

Televes®



Ref. 769501
Ref. 769502

User's Manual

EN GPON ONT OFFICE
GPON ONT HOME

Índice

1.	Summary	10
2.	Technical Description	11
2.1	Refs. 769501-769502 Gateway Main Functionalities	11
2.2	Application Scenario	11
2.3	Interoperability	12
2.4	Interfaces	13
2.5	General Features	13
2.6	General Architecture.....	16
2.7	GPON	16
2.8	Ethernet.....	16
2.9	IPTV	16
2.10	RF Video Overlay	16
2.11	Voice	17
2.12	WI-FI.....	17
2.12.1	Operational description	17
2.12.2	Block Diagram	18
2.12.3	Refs. 769501-769502 WI-FI Antennas	19
2.13	Multiple QoS per VLAN	19
2.14	Policing/Rate Limiting.....	19
2.14.1	Downstream QoS.....	19
2.14.2	Upstream QoS.....	19
2.14.3	Dynamic Bandwidth Allocation (DBA)	20
2.14.4	Upstream QoS scenarios	21
3.	General Specifications.....	22
3.1	Interfaces	22
3.1.1	GPON.....	22
3.1.2	Ethernet.....	23

3.1.3	RF Overlay.....	23
3.1.4	FXS.....	24
3.1.5	WI-FI.....	25
3.2	General Features	26
3.3	General Service Description.....	27
3.4	Optical metering	28
3.5	Wavelength filtering	28
3.6	GPON/Ethernet characteristics	28
3.7	GPON management.....	29
3.8	Standards.....	30
4.	Setup	31
4.1	Before installing Refs. 769501-769502 device.....	31
4.2	Connections.....	31
4.3	How to Setup Refs. 769501-769502.....	33
4.4	Interface connection	35
4.4.1	Optical cable connection	35
4.4.2	General Overview of Refs. 769501-769502 Connections	35
5.	Configuration	37
5.1	Refs. 769501-769502 activation.....	37
5.2	Customization.....	37
5.2.1	Software download from the OLT.....	37
5.3	Network Setup.....	37
5.4	Refs. 769501-769502 General Management Configuration.....	38
5.5	Device Info.....	39
5.5.1	Summary.....	40
5.5.2	WAN	41
5.5.3	Statistics	42
5.5.4	Route	45
5.5.5	ARP	46
5.5.6	DHCP	46
5.5.7	Voice	47
5.6	Advanced Setup.....	48
5.6.1	Layer2 Interface.....	48

5.6.2	WAN Service/	49
5.6.3	LAN.....	78
5.6.4	NAT	84
5.6.5	Security.....	89
5.6.6	Parental Control.....	96
5.6.7	Quality of Service	99
5.6.8	Routing	104
5.6.9	DNS	113
5.6.10	UPnP	117
5.6.11	DNS Proxy	117
5.6.12	Storage Service	118
5.6.13	Interface Grouping	118
5.6.14	IP Tunnel.....	120
5.6.15	Power Management	124
5.6.16	Multicast.....	124
5.7	Wireless.....	126
5.7.1	Basic.....	126
5.7.2	Security.....	128
5.7.3	MAC Filter.....	131
5.7.4	Advanced.....	132
5.7.5	Station Info.....	133
5.8	Voice	133
5.8.1	SIP Basic Settings	134
5.8.2	SIP Advanced Settings	137
5.8.3	SIP Debug Settings.....	140
5.9	Diagnostics.....	141
5.10	Management.....	141
5.10.1	Settings.....	142
5.10.2	System Log	144
5.10.3	Security Log	147
5.10.4	TR-069 Client	148
5.10.5	Internet Time	150
5.10.6	Access Control.....	152

5.10.7	Update Software	153
5.10.8	Reboot	154
5.11	Logout.....	154
6.	Operation Indicators.....	155
6.1	Refs. 769501-769502	155
6.1.1	LED Indicators Status.....	155
6.1.2	Troubleshooting.....	157
7.	CLI.....	158
7.1	Overview	158
7.2	Nodes and Commands	158
7.2.1	“wan” node	158
7.2.2	“lan” node.....	163
7.2.3	“nat” node	166
7.2.4	“dns” node.....	170
7.2.5	“qos” node.....	172
7.2.6	“voice” node	176
7.2.7	“security” node.....	178
7.2.8	“routing” node.....	180
7.2.9	“multicast” node.....	182
7.2.10	“diagnostics” node	183
7.2.11	“arp” node	184
7.2.12	“device-info” node	184
7.2.13	“statistics” node.....	185
7.2.14	“dhcp” node.....	185
7.2.15	“upnp” node.....	186
7.2.16	“intf-grouping” node.....	186
7.2.17	“management” node	188
7.3	VoIP configuration using CLI.....	192
7.3.1	IPoE Service Configuration	192
7.3.2	VoIP Configuration	193

Glossary of Acronyms and Definitions

Acronyms and abbreviations

3G	Third generation mobile telecommunications
AAA	Authentication, Authorization, and Accounting
AC	Alternating Current
AC	Access Concentrator
ACL	Access Control List
ACS	Auto Configuration Server
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AS	Autonomous System
AUTO-MDIX	Medium Dependent Interface Crossover Automatic Choice
BBF	Broadband Forum
BGP	Border Gateway Protocol
CAT5E	Category 5 Cable
CATV	Cable TV
CIFS	Common Internet File System
CLI	Command-line interface
CO	Central Office
CPE	Customer-Premises Equipment
CRC	Cyclic Redundancy Check
DC	Direct Current
DDNS	Dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
EAP-SIM	Extensible Authentication Protocol Method for GSM Subscriber Identity Module
FTP	File Transfer Protocol
FTTH	Fiber-To-The-Home
FXS	Foreign eXchange Station
GbE	Gigabit Ethernet
GEM	GPON Encapsulation Module
GEPON	Gigabit Ethernet Passive Optical Network
GPON	Gigabit-capable Passive Optical Network
GSM	Global System for Mobile Communications
GW	Gateway
HG	Home Gateway
HSI	High Speed Internet
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol

IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ITU-T	Telecommunications International Telecommunication Union
L2	OSI Layer 2
L3	OSI Layer 3
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MAN	Metropolitan Area Network
MAP	Mobile Application Part
ME	Managed Entity
MEGACO	Media Gateway Control Protocol
MRU	Maximum Receive Unit
MTBF	Mean Time Between Failures
NAS	Network Access Server
NAT	Network Address Translation
NGN	Next Generation Network
NMS	Network Management System
OLT	Optical Line Terminal
OMCI	ONT Management Control Interface
ONT	Optical Network Terminal
OPEX	Operational Expenditure
OSI	Open Systems Interconnection
PC	Personal Computer
PON	Passive Optical Network
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PSK	Phase-Shift Keying
PWLAN	Public Wireless LAN
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
RGW	Residential Gateway
RIP	Routing Information Protocol
RJ11	Registered Jack model 11
RJ45	Registered Jack model 45
SAMBA	SMB/CIFS implementation
SC/APC	SC/APC optical connector
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIP	Session Initiation Protocol
SMB	Server Message Block
SNTP	Simple Network Time Protocol
SS7	Signalling System No. 7

SSID	Service Set IDentifier
STB	Set Top Box
SW	Software
T-CONT	Transmission Container
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
TR-069	Technical Report 069
TTL	Time to Live
TV	Television
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VAD	Voice Activity Detection
VAP	Virtual Access Point
VID	VLAN Identifier
VLAN	Virtual Local Area Networks
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WI-FI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	WI-FI Protected Setup
xBASE-T	Ethernet over twisted pair technologies

1. Summary

The Refs. 769501-769502 is an Optical Terminal Equipment (ONT) unit for Passive Optical Networks (PON) termination in a FTTH (Fiber-To-The-Home) service delivery architecture. Refs. 769501-769502 communicates with the OLT (Optical Line Terminal) for the PON side and with the customer's premises for the client side. This equipment supports triple-play services - high speed internet (HSI), voice (VoIP), video (IPTV and RF Overlay) and WPS (Wi-Fi Protected Setup). The use of the GPON fiber access technology does allow a significant service delivery increase when compared with traditional xDSL technologies.

The Refs. 769501-769502 equipment technology is based on GEM (GPON Encapsulation Method), and complies with ITU-T G.984.x. recommendation as like as G.984.4 (OMCI) ensuring interoperability with major GPON OLT vendors (BBF.247).

These base functionalities, together with the support for bit rates of up to 2.5 Gbps (downstream) and 1.24 Gbps (upstream), an optical network splitting ratio of up to 1:64 in a single fiber and a distance range of up to 60 km, make the GPON technology and the Refs. 769501-769502 the most efficient option for passive optical network topologies, when integrated service delivery is an issue.

Together with multi-vendor OLT interoperability (BBF.247 certified), other differentiated features of the Refs. 769501-769502 product are the embedded RF Video Overlay as well as the chance to have several TV channel packs by means of using remote managed analog RF video overlay filters. The use of an embedded optical reflective component also increases probing resolution in case of FTTH probing. The Refs. 769501-769502 is also one of the first single household integrated CPE solution (ONT+GATEWAY).

As opposed to the point-to-point architecture, in which there is one physical port per client in the Central Office, in GPON point-to-multipoint architecture there is only a single laser and photo-detector in the Central Office (CO) to serve up to 64 CPEs. All the Optical Distribution Network is built by means of passive equipment modules with a long live MTBF standards and very low OPEX.

2. Technical Description

2.1 Refs. 769501-769502 Gateway Main Functionalities

The Refs. 769501-769502 Gateway is aimed for customer premises and complies with the ITU-T G.984.x recommendation in order to transport (over GPON) and deliver (to premises domain) the full broadband service pack.

Broadband service applications are commonly referred as below:

- High speed internet (HSI);
- Voice (VoIP) services (SIP/MEGACO H.248);
- TV (whether IPTV or analog RF video overlay);
- WI-FI.

The multiplay environment is thus reinforced when combining the upper referred services.

2.2 Application Scenario

The next figure shows a possible gateway scenario for Refs. 769501-769502 equipments when in an end-to-end PON architecture.

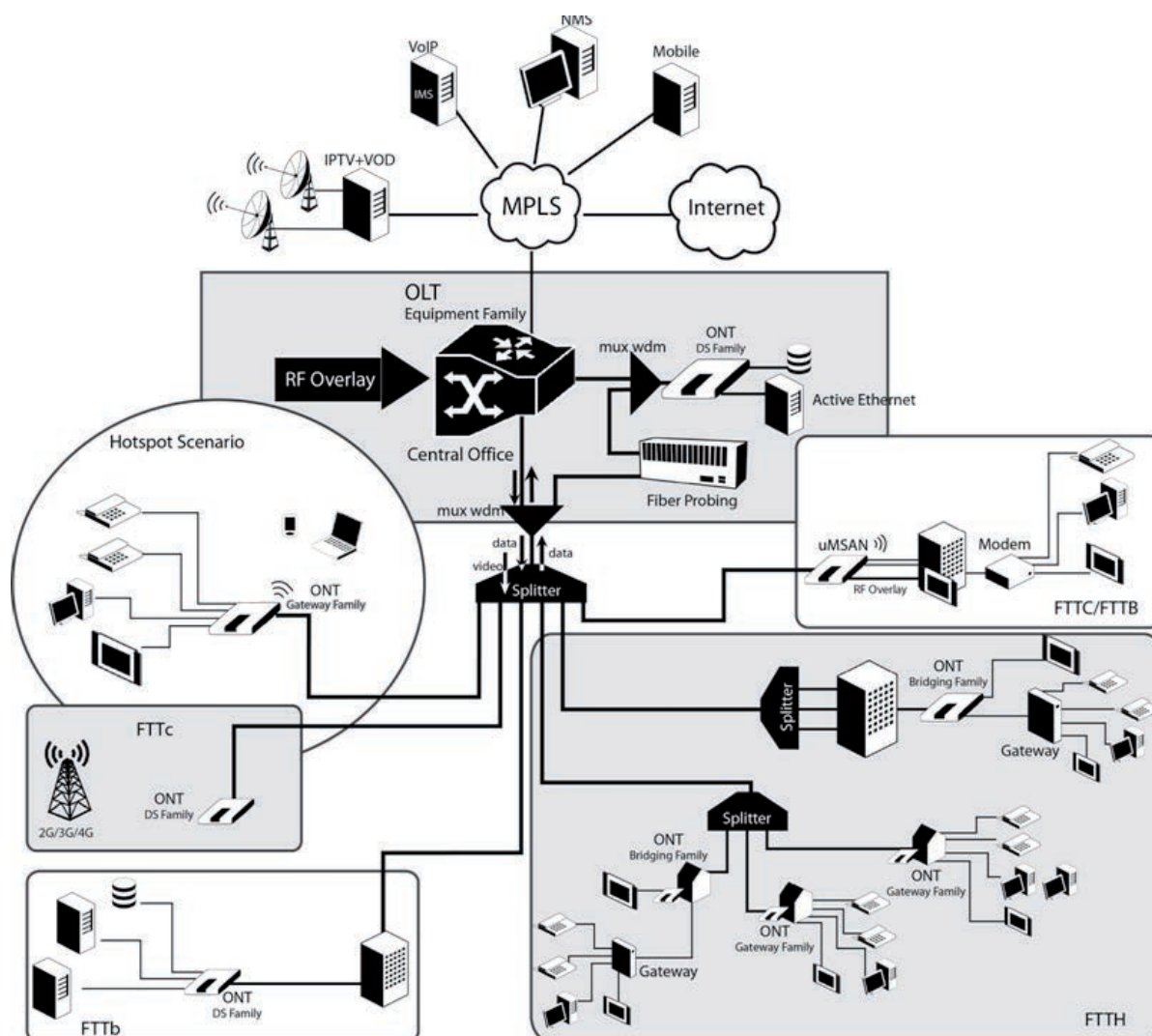


Figure 2-1: Refs. 769501-769502 equipment application scenario

2.3 Interoperability

The ONT gateway family equipment complies with ITU-T G.984.x. Recommendation as like as G.984.4 (OMCI) ensuring multi-vendor OLT interoperability with major GPON OLT vendors, as defined in BBF.247 ONU certification program.

BBF.247 ONU certification program certifies ONT link layer configuration and management protocol, OMCI, Figure 2-2, as defined by ITU-T G.984.3, ITU-T G.984.4 and ITU-T G.988.

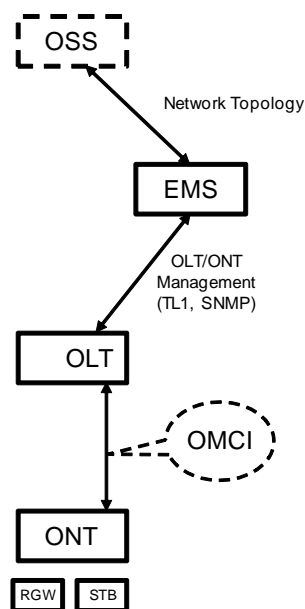


Figure 2-2: Link Layer Configuration and Management

IP-based services configuration and management is achieved by means of the TR-069 protocol as defined by Broadband Forum. This procedure takes for granted that previously the link layer connectivity has been achieved.

TR-069 is then transparent to the OLT, since the TR-069 connections are established between the ACS and the ONTs, Figure 2-4.

ONT gateway family equipments integrate gateway functionalities. Link layer configuration and management is achieved by the use of OMCI, while IP-based services (RG functionality and Voice over IP) are configured and managed by TR-069, Figure 2-3.

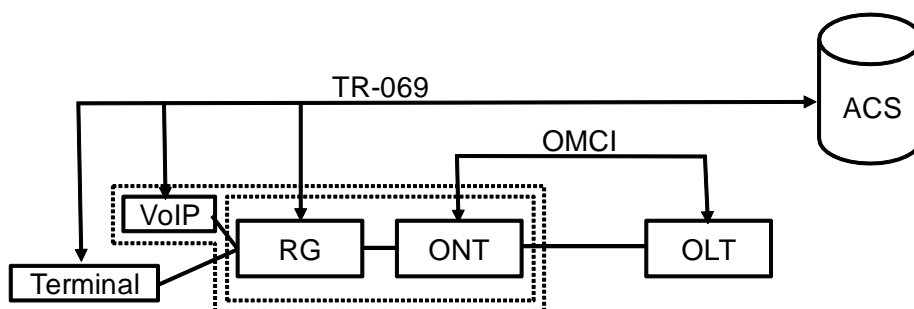


Figure 2-3: ONT gateway family equipment configuration

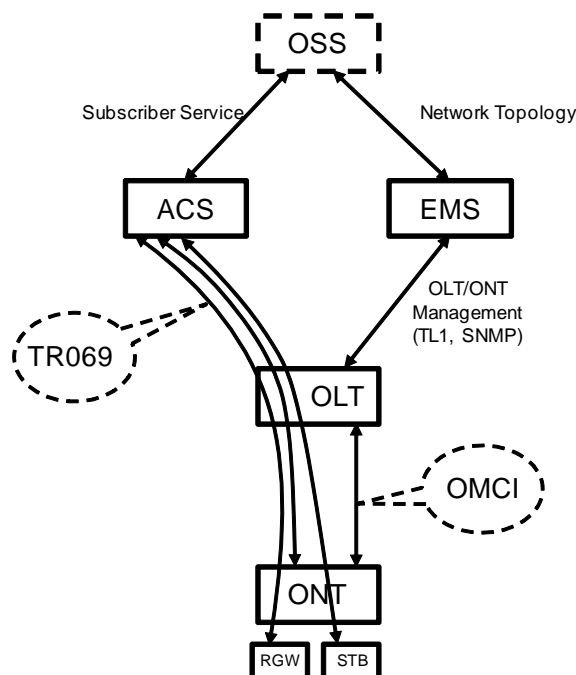


Figure 2-4: IP Based services-TR069 configuration

2.4 Interfaces

Client interface options are of type:

- 4x 100/1000Base-T for Ethernet network connection (RJ45 connectors);
- 2x FXS channels (RJ11 connectors);
- 2x2 @ 2.4/5.0 GHz wireless interfaces (802.11 b/g/n);
- 2x USB 2.0 Masters for printer sharing, media sharing and for 3G/4G backup uplink;
- RF Overlay interface;
- Control switches for power and WI-FI;

Network interface option is of type:

- GPON SC/APC Optical connector (B+/C+).

2.5 General Features

GPON is a point-to-multipoint passive optical network, in which unpowered optical splitters are used to enable a single optical fiber to serve multiple premises, typically 1-64.

A PON consists of an optical line terminal (OLT) at the central office and a number of optical network terminals (ONT) at the customer premises. Downstream signals are broadcasted to all premises sharing multiple fibers. Encryption can prevent eavesdropping. Upstream signals are combined using a multiple access protocol (Time Division Multiple Access- TDMA). The OLT queues data to the various ONT terminals in order to provide time slot assignments for upstream communication.

In Figure 2-5 it is shown a scenario for a multi-service user domain basic architecture through an ISP network.

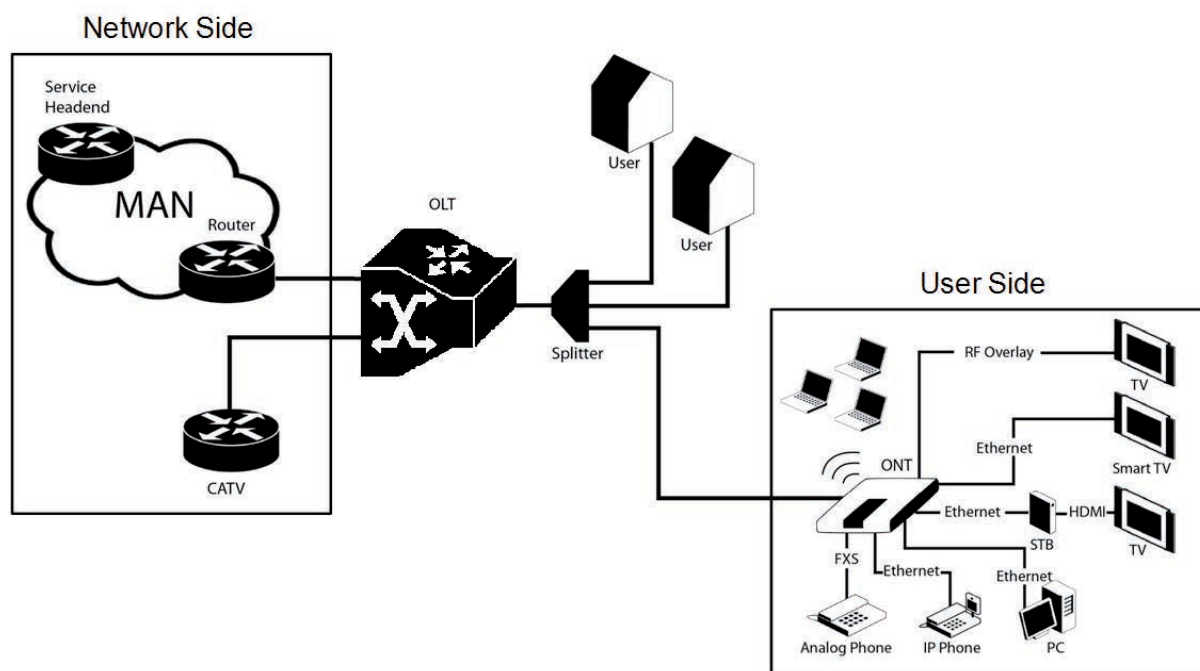


Figure 2-5: Optical fiber Internet service user access

In the upstream direction, the Refs. 769501-769502 is connected to the optical splitter and respectively to the OLT through the PON port to provide integrated access services through the service headend.

In the downstream direction, the Refs. 769501-769502 is connected to various terminals through the following LAN-side ports to implement multi-play services:

- Four 10/100/1000M Base-T Ethernet ports, which can be connected to terminals such as PCs, STBs, and video phones to provide the high-speed data and video services;
- Two FXS ports, which can be connected to telephone sets to provide VoIP services;
- Two Wi-Fi antennas, which can connect to Wi-Fi terminals wirelessly to provide a secure and reliable high-speed wireless network;
- Two USB ports, which can be connected to a USB storage device to provide convenient storage and file sharing services within a home network;
- One RF Overlay port, which can be connected to a TV set to provide high-quality CATV service.

The communication between client equipment (ONT) and the ISP access routers (MAN edge) is made by an optical fiber-based passive architecture (ITU-T G.984 Recommendation). The GPON network acts as a Layer 2 Ethernet metropolitan network. Access network assures and controls the media (MAC) communication through a TDMA scheme, introducing GEM (GPON Encapsulation Method) in between to adapt TDM layer to Ethernet.

The used protocol stack is shown in Figure 2-6.

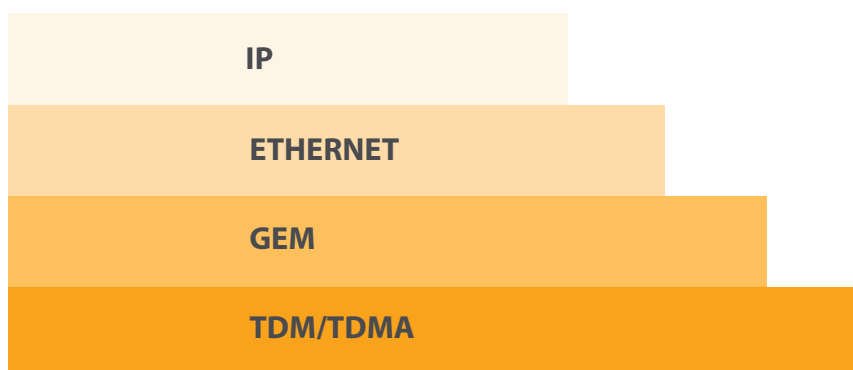


Figure 2-6: Stack of protocols for GPON architecture

Several transmission containers (T-CONT) are assigned to each user. Each T-CONT has an associated GEM port and each GEM port has a VLAN identifier and an 802.1p priority level.

The ONT classifies the traffic depending on the VLAN and the marked priority, and routes it over the corresponding T-CONT/GEM port. Thus for frame multiplexing, GEM and T-CONT ports are used for uplink while the downlink only use the GEM ports feature.

ONT7-RGW complies with Broadband Forum TR-142 Technical Report, which defines a framework for the remote configuration and management of IP-based services over PON (Passive Optical Network) and fiber access technology.

TR-142 framework uses TR-069 which is the protocol of choice for the remote management and configuration of IP services over PON and fiber access networks. TR-069 is intended to be used for the remote configuration and management of IP services running over ONT, as well as for some aspects of ONT management.

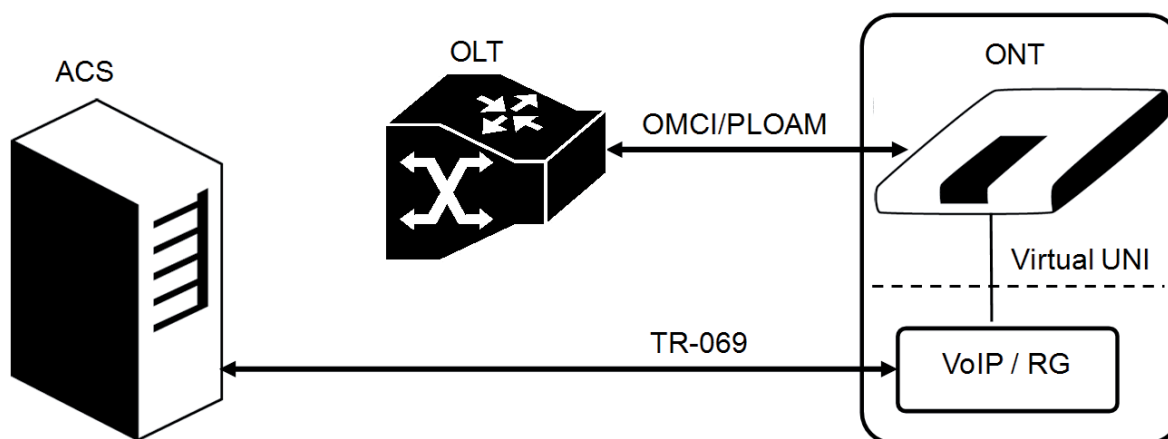


Figure 2-7: TR-142 Framework

TR-142 framework defines a virtual UNI between the OMCI (ONT Management Control Interface) and TR-069 management domains.

This framework allows PON CPE with L3 layer capabilities to be mass remotely configured, troubleshoot and managed by an ACS (Auto Configuration Server) using TR-069 CPE WAN Management Protocol.

2.6 General Architecture

The Refs. 769501-769502 basic system architecture is hereafter presented.

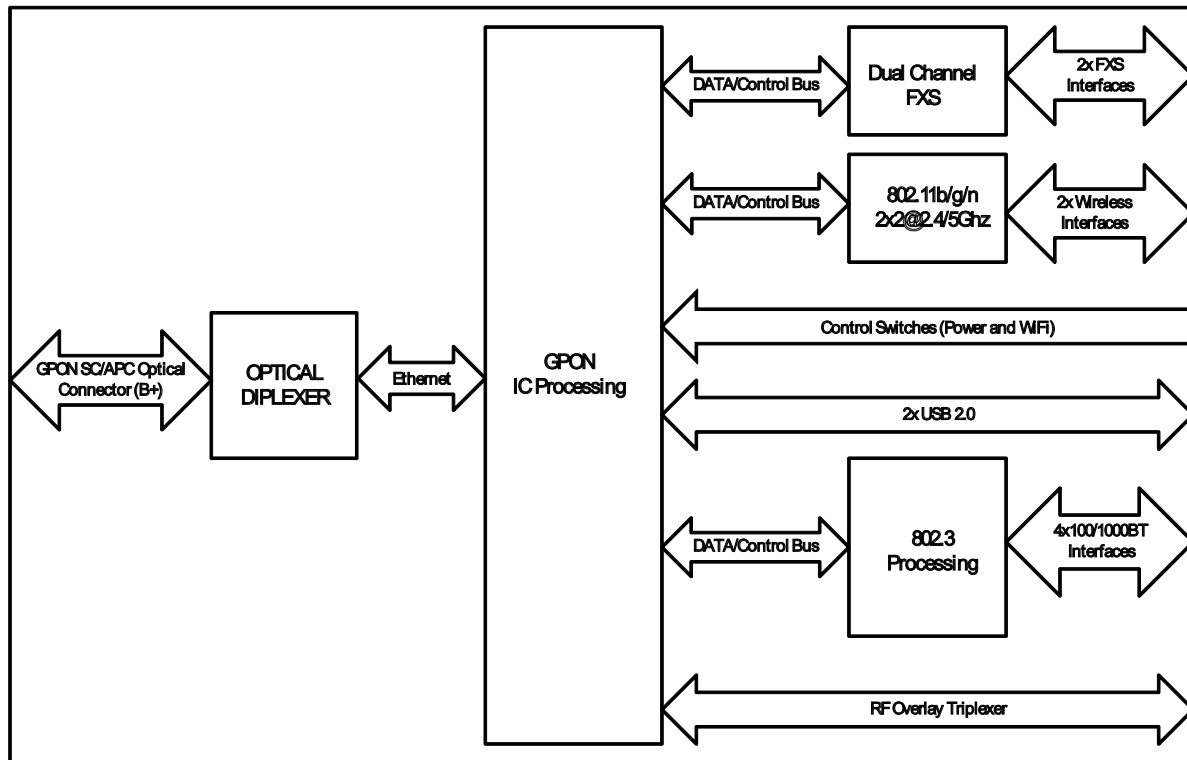


Figure 2-8: Refs. 769501-769502 system architecture

The GPON IC Processing unit is the core component inside Refs. 769501-769502. It is responsible for the interconnection and processing between client side interfacing and optical GPON Uplink interface.

2.7 GPON

The Refs. 769501-769502 GPON layer as G.984.x uses 1490nm downstream and 1310nm upstream of the optical wavelength, with 2,488Gbps downstream and 1,244Gbps upstream by using an SC/APC protected optical connector.

2.8 Ethernet

Ethernet is the wired LAN technology and is revised in the IEEE 802.3 standard. At the OSI reference system, Ethernet is at the Data Link layer. In the Refs. 769501-769502 equipment both WAN and LAN type of physical interfaces are 10/100/1000BASE-T AUTO-MIX Ethernet type over RJ45 connectors.

2.9 IPTV

For the IPTV service the Refs. 769501-769502 also behaves like a Layer 2 bridging device. For this service, the Refs. 769501-769502 has a specific GEM PORT for Multicast. This same GEM PORT is requested by the user in order to have access to the various IPTV channels. Every time a user requests a new channel, the Refs. 769501-769502 will send to OLT a IGMP packet requesting that Channel. The Refs. 769501-769502 is also responsible for implementing the snooping for the channels that the user requests.

2.10 RF Video Overlay

Broadcast video signal travels over fiber from the central office in the 1550nm wavelength and is demuxed and converted in the Refs. 769501-769502 to a F connector (75 Ohm) RF Overlay interface to deliver a RF TV signal going from 47MHz up to 862MHz bandwidth. Refs. 769501-769502 may also implement multiple analog filtering on the RF Interface in order to turn the open RF Spectrum in a group of sliced TV channel packs that are remotely enabled from the NMS.

PON RF video overlay service is the way to deliver a broadcast TV service over a PON fiber network. This video overlay service is foreseen to provide mainly broadcast video transmission in contrast to unicast and/or multicast IP video transmission which is used for IPTV and/or Video-On-Demand having the need for a Set-Top-Box or a Smart TV at the customer premises.

Standardization bodies (ITU for GPON and IEEE for GEAPON) have excluded the use of the 1550 -1560nm wavelength window for IP transmission on PONs and have even continued with this approach for the upcoming 10GPON and 10GEAPON standards. The 1550-1560nm wavelength window is thus exclusively reserved for the video overlay transmission and by that mean an option to offload unicast and/or multicast video transmission from the IP PON transmission link.

Typically an extra fiber testing signal (1650nm) for optical network probing is also added to the PON optical communication link.

EN

2.11 Voice

Refs. 769501-769502 voice service provisioning could be made through OLT configurations over OMCI messages or could be downloaded (FTP) from the OLT up to the Refs. 769501-769502 after the Refs. 769501-769502 registration on the PON network. The Refs. 769501-769502 gateway family equipments have the ability to deliver the Voice service over two types of interface:

Logical interface (VLAN encapsulation)

If the Refs. 769501-769502 has no FXS ports and the VoIP service is transparently forwarded from the OLT up to the Home Gateway (and vice versa) within a previously defined voice VLAN. Refs. 769501-769502 respects the defined priority and implements the traffic encapsulation from its own Ethernet interface into a specific T-CONT/GEM-Port over the PON interface and up to the OLT equipment.

Physical interface (FXS ports)

The Refs. 769501-769502 has physical RJ11 FXS interfaces. In this version of the Refs. 769501-769502 equipment, voice interfaces are terminated in the equipment by means of FXS (RJ11) connections. The RJ11 analog terminals adapter function is auto/self-configured, integrated (analog/VoIP) and associated with a defined SIP or Megaco (H.248) user.

The Refs. 769501-769502 will allow VoIP or NGN (Next Generation Network) traffic from devices connected to the RJ11 or RJ45 interfaces, towards the same internal VLAN.

Apart of the SIP and Megaco (H.248) self-configuration, it is also possible to make modifications in the voice service configurations by updating the Refs. 769501-769502 SW through download from the OLT via OMCI.

The Refs. 769501-769502 equipment has a DHCP client to get an IP address, alternatively the Refs. 769501-769502 could be configured with a static IP. The configuration of the static IP or DHCP client is related to the WAN side and is enabled by the OLT.

2.12 WI-FI

2.12.1 Operational description

The Refs. 769501-769502 supports WI-FI, with an WI-FI interface currently operating in the 2.4GHz frequency.

The Refs. 769501-769502 complies with the following standards:

- IEEE 802.11b (2.4GHz, 11 to 22 Mbps)
- IEEE 802.11g (2.4Ghz, up 54 Mbps)
- IEEE 802.11n (MIMO-OFDM 2.4GHz, 65Mbps to 300Mbps)

The ONT supports the following wireless security features:

- WEP encryption (64/128 bits)
- WPA (Wireless Protect Access) TKIP
- WPA2 AES

- WPA2 mixed
- 02.1x Authentication
- Client access control through media access control (MAC) filter
- Dynamic cryptography (TKIP and AES)

2.12.2 Block Diagram

The Refs. 769501-769502 circuit block diagram is presented in the figure below showing all oscillators in the device and its frequencies, Figure 9. Intentional radiators in the circuit and radio signal path between circuit blocks are also shown.

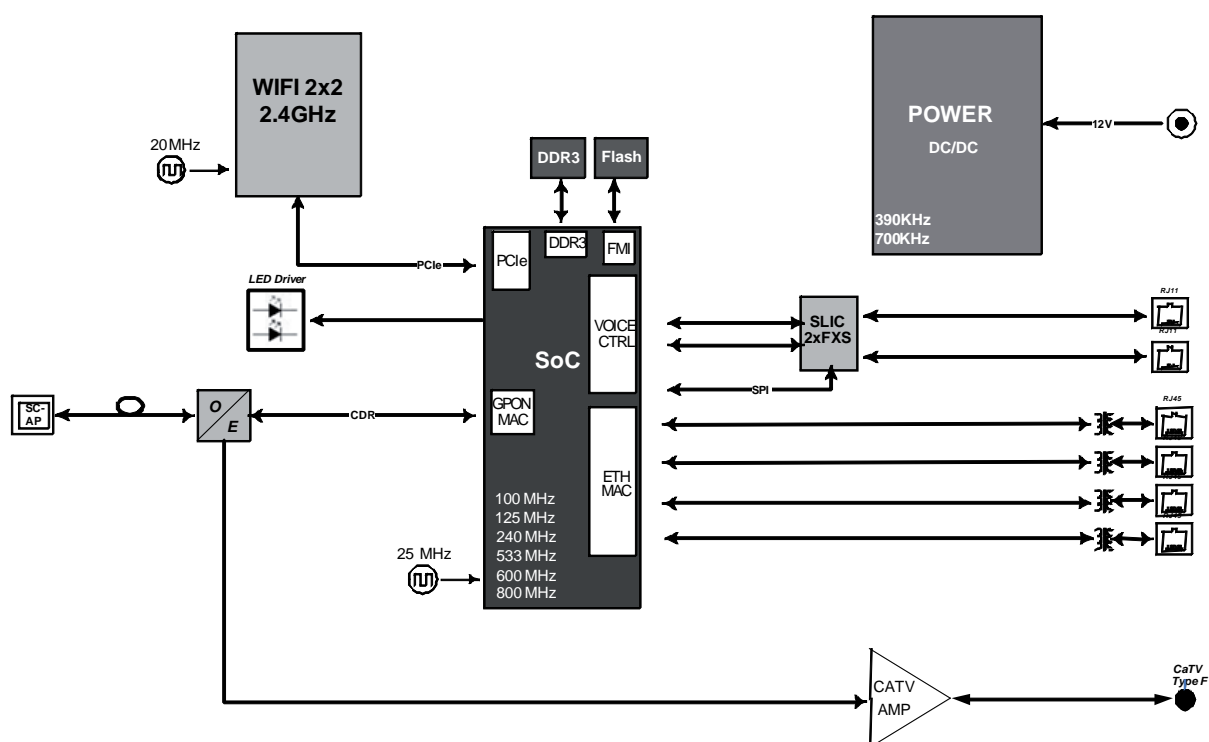


Figure 2-9: Refs. 769501-769502 circuit block diagram

2.12.3 Refs. 769501-769502 WI-FI Antennas

The ONT provides a MIMO 2x2 topology Wireless antenna capability.

The ONT has internal, Omni-directional antennas with a gain of 1.6dBi.

2.13 Multiple QoS per VLAN

The Refs. 769501-769502 supports 802.1p QoS per VLAN services in which several flows (one per allowed pbit) are embedded in the same VLAN. According to the applied configuration, the Refs. 769501-769502 performs a per-flow QoS policy: dropping traffic marked with not allowed pbits and limiting to the configured value the data rate of the allowed flows.

The Refs. 769501-769502 performs transparent VLAN translation. It is transparent to upper layer protocols, such as ARP, RIP, DHCP, IGMP, PPP, etc.

2.14 Policing/Rate Limiting

2.14.1 Downstream QoS

The OLT system provides several QoS mechanisms, that can be targeted to the flow characterized by one or two VLAN according with the type of service, or can be targeted to the packets priority, where each p-bit is mapped in one of eight queues of each port.

For each OLT ports are associated eight queues, for each of these queues is possible to configure the p-bit mapping in one of the queues, the scheduler type (Strict Priority or Weighted Fair Queuing) and the minimum and maximum bandwidth of each queue.

In the downstream direction the ingress traffic first passes by a policer configured to each ONT service, which is defined by one or two tags. After this the traffic is put in a queue according with the p-bit/queue mapping. Each of these queues is associated with a scheduler and a policer. Then the traffic flows to the GPON interface and when it arrives to the ONT it will pass by a mapping block which will map the traffic in one of the eight queues according with the p-bits, these queues have a Strict Priority scheduler in order to guarantee that the most prioritized traffic passes first.

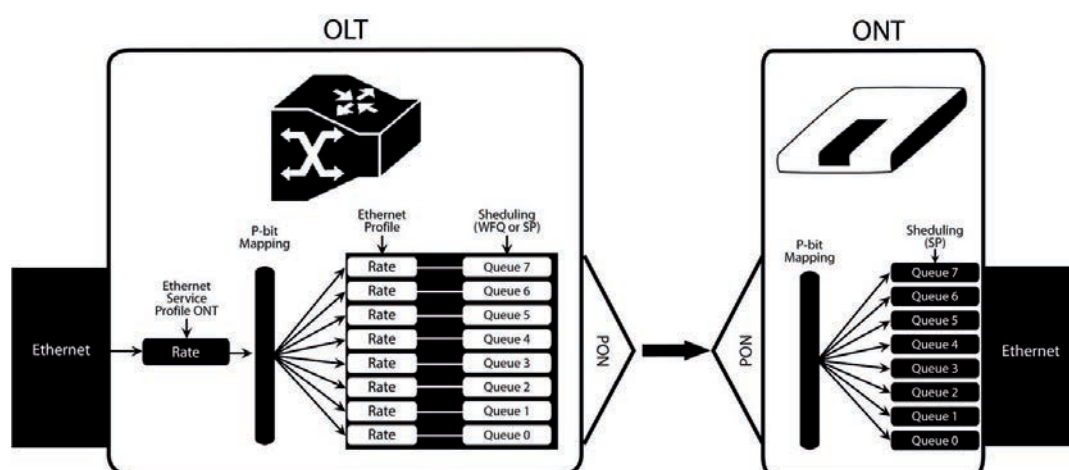


Figure 2-10: Downstream QoS Diagram

2.14.2 Upstream QoS

In the upstream direction, for each T-CONT the ingress traffic in the ONT passes by a mapping block that maps the traffic in one of the eight queues according with the p-bit, these queues have a Strict Priority Scheduler. The ONT “waits” until the OLT assigns a transmission timeslot for that T-CONT, so that the most prioritized queues are the ones that transmit first. In the OLT ingress, the traffic is put into a queue according with what is defined in the queue/p-bit mapping. Each of these queues has an associated scheduler and policer that control the traffic sent to the uplink.

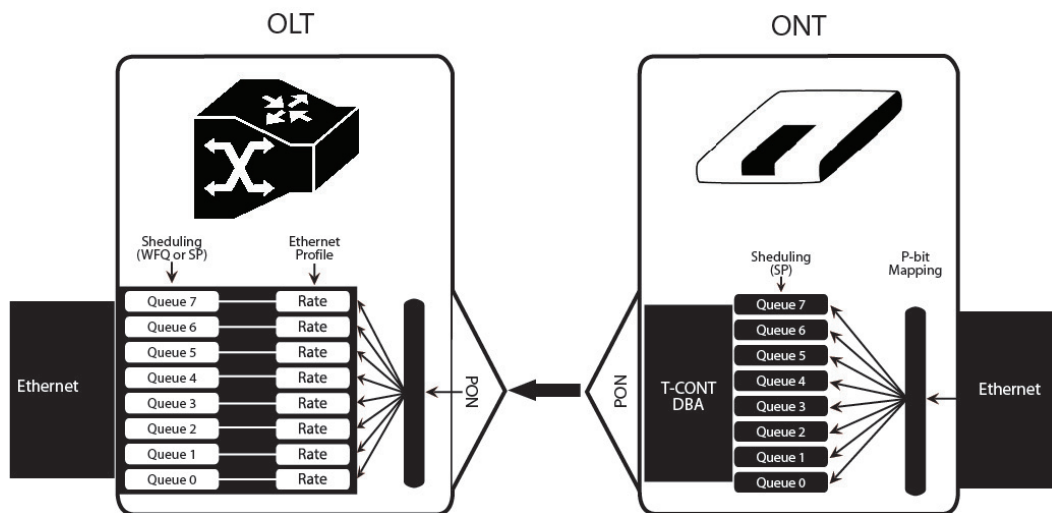


Figure 2-11: Upstream QoS Diagram

2.14.3 Dynamic Bandwidth Allocation (DBA)

The DBA (Dynamic Bandwidth Allocation) is available in order to optimize the upstream bandwidth. This mechanism consists in defining an adequate T-CONT to the service traffic in question. There are five types of T-CONT, defined by the Fixed, Assured and Maximum Parameters:

- Type 1: Only fixed Bandwidth;
- Type 2: Only Assured Bandwidth;
- Type 3: Assured+Maximum Bandwidth;
- Type 4: Only Maximum Bandwidth (Best Effort);

Type 5: Fixed+Assured+Maximum Band

T-CONT	Type 1	Type 2	Type 3	Type 4	Type 5	Units
Fixed BW- R_F	R_{F1}	0	0	0	R_{F5}	[b/s]
Assured BW- RA	0	R_{A2}	R_{A3}	0	R_{A5}	[b/s]
Max Bw - RM	$R_{M1} = R_{F1}$	$R_{M2} = R_{A2}$	$R_{M3} > R_{A3}$	R_{M4}	$R_{M5} >$ $R_{F5} + R_{A5}$	[b/s]
Bandwidth Eligibility	0	0	Non-Assured BW - R_{NA}	Best-Effort - R_{BE}	R_{NA} / R_{BE}	

Table 2-1: T-CONT types definition

In each GPON interface there are 1024 Alloc-ID (T-CONT identifiers) available, provided to manage ONT services. They are distributed in the following way:

Alloc-ID	Allocation Type
0-127	Default Alloc-ID (Dynamic or Static)
128-255	Reserved
256-639	Dynamic or Static
640-1023	Static

Table 2-2: Alloc-ID's distribution by T-CONT type

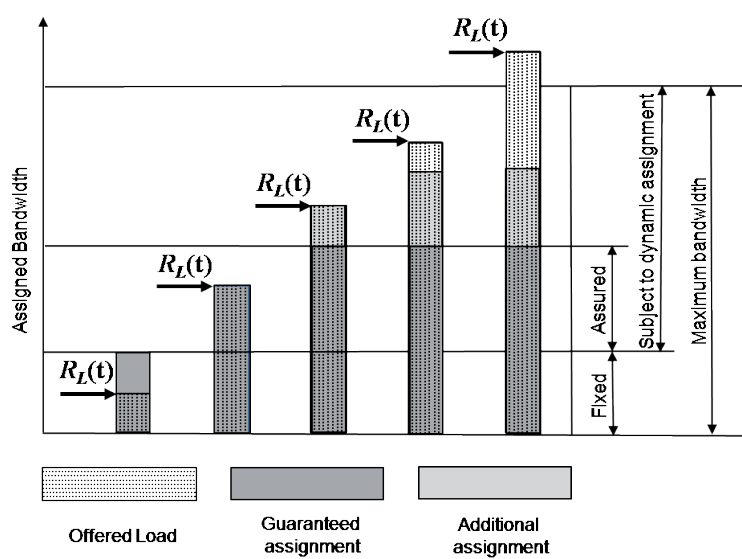


Figure 2-12: Traffic distribution by service/client

2.14.4 Upstream QoS scenarios

- 8 priority queues
- Strict-priority
- Upstream Scheduling:
 - Strict Priority (currently supported)
 - Strict Priority + rate controller (currently supported)
 - Strict Priority + WFQ (can be SW supported)

3. General Specifications

3.1 Interfaces

3.1.1 GPON

The Refs. 769501-769502 GPON G.984.x layer uses 1490nm downstream and 1310nm upstream optical wavelengths, with 2,488Gbps downstream and 1,244Gbps upstream by using an SC/APC protected optical connector.

3.1.1.1 Optical interfaces

Items	Unit	B+	C+
		ONT Tx	ONT Tx
Nominal bit rate	Mbps	1244.16	1244.16
Operating wavelength	nm	1260-1360	1260-1360
Line code	--	Scrambled NRZ	Scrambled NRZ
Minimum ORL of ODN	dB	>32	>32
Mean launched power MIN	dBm	+0.5	+0.5
Mean launched power MAX	dBm	+5	+5
Launched optical power without input to the Tx	dBm	Less than Min sensitivity -10	Less than Min sensitivity -10
Maximum Tx Enable		16	16
Maximum Tx Disable		16	16
Extinction ratio	dB	>8.2	>8.2
Tolerance to the Tx incident light power	dB	>-15	>-15
SLM Laser – MAX –20 dB width	nm	1	1
SLM Laser – MIN SMSR	dB	30	30
		ONT Rx	ONT Rx
Receiving bit rate	Mbps	2488.32	2488.32
Receiving wavelength	nm	1480-1500	1480-1500
Max reflectance of equipment, measured at Rx wavelength	dB	<-20	<-20
Bit error ratio	--	<-10 ⁻¹⁰	<-10 ⁻¹⁰
Minimum sensitivity	dBm	-27	-30*
Minimum overload	dBm	-8	-8*
Upstream optical penalty	dB	0.5	0.5
Consecutive identical digit immunity	bit	>72	>72
Tolerance to reflected optical power	dB	<10	<10
		ONT Rx Video	
Receiving wavelength	nm	1550-1560	

Table 3-1: Optical interfaces specifications

* ONT RX= -8~-30 dBm (The ONT7-RGW sensitivity assumes the use of the optional RS (255,239) FEC capability of the G-PON TC layer with the current class B+ ONU detector technology; The ONU overload is set at -8 dBm to be common with the class B+ value, even though in this application -10 dBm is sufficient).

Optical solution: B+ and C+.

Connector type: SC/APC.

IEC 60825-1: "Class 1 Laser Product".

The B+ and C+ triplexer is embedded on the ONT7-RGW equipment version.

ONU Single Fiber - G.984.2 (03/2003) + G.984.2 Amd 1 (02/2006) and 2 (03/2008), G.983.3 (03/2001).

Optical Metering – G.984.2 Amd 2 Table IV.1/G.984.2 – Optical Line Supervision related measurement specifications (the accuracy of the measurement is +/-3dBm maximum).

EN

3.1.2 Ethernet

Ethernet is the wired LAN technology and is revised in the IEEE 802.3 standard. At the OSI reference system, Ethernet is at the Data Link layer. In the ONT7-RGW equipment the LAN type of physical interfaces is 10/100/1000BASE-T AUTO-MIX Ethernet type over RJ45 connectors.

3.1.3 RF Overlay

Broadcast video signal travels over fiber from the CO in the 1550nm wavelength and is demuxed and converted in the Refs. 769501-769502 to a F connector (75 Ohm) RF Overlay interface to deliver a RF TV signal going from 47MHz up to 1GHz of bandwidth.

3.1.4 FXS

Items	State	Description	
Pulse Dialling	Pulse Frequency: 10 Hz (8 Hz to 12 Hz) Pulse Relation: 66,6% (33% to 75%) Interdigital Pause and Pre-Dialling: 400 ms (min)	-	
DTMF	-	According to ETSI CTR 21 [1]	
Clip	-	According to ETSI 300 659-1	
Clip on Call Waiting	-	According to ETSI 300 659-2	
DC voltage (V)	-48V (-46 to -54)	-	
Loop Current Characteristics (A)	20mA (min) to 60mA (max)	-	
I _{feed} Max. (A)	45mA	-	
Impedance and Transmission Requirements (Ω)	Q.552 [4] (11/96) of ITU-T 220 Ω +820 Ω //115nF.	A telephone that comply with transmission requirements defined in CTR 38, should comply with SLR, RLR and STMR (4.2.2.1, 4.2.2.2 and 4.2.3) standard requisites, when connected to a FXS interface.	
ILA (A)	20 – 45 mA	5 bit parameter which sets the current limit for DC feed (DC feed and battery switch are programmed and calibrated to ILA=26mA, VOC=48V, VAS=3V, bshv=5V).	
Ringer voltage (V)	DC offset: 48V AC voltage: 75V _{rms} +/- 0.5% Frequency: 25Hz +/- 3%	-	
Ringing signal	normal ringing	1 sec ring / 5 sec pause (interval = 6 sec).	
Hook flash	on-hook - register recall/hook flash	100 msec	Minimum time of recognition of "on-hook" when hook-flash feature does not exist
	on-hook - register recall/hook flash	1000 msec	Minimum time "on-hook" recognition when hook-flash feature does exist
	off-hook	40 msec	minimum time "off-hook" recognition
	intervall	160msec - 400msec	Time calibrated break pulse duration for register recall recognition

NOTE:

FXS interface specific parameter values vary according to country adopted standards. Refs. 769501-769502 FXS interface specifications table values are configurable at the web management interface at the menu Voice, item SIP basic settings, by selecting the local(Country) where the Refs. 769501-769502 will be used. Please refer to section SIP BASIC SETTING, for details on this configuration.

Table 3-2: FXS interface specifications

3.1.5 WI-FI

Items	Compliance	Description
	IEEE 802.11 b/g/n	-
Bit Rates	802.11 b/g	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54Mb/s
	802.11 n	Up to 300Mb/s over two spatial streams
SSID	-	Up to 8
Operation Frequencies	-	2.4GHz (ISM) or 5GHz (U-NII)
Channels	-	20MHz and 40MHz channels
MIMO	-	2x2
MCS	-	supported values: 0-15 and 32
Wireless Security	WEP	40bit secure key and 24 bit as defined in 802.11-2007
	WPA	
	WPA2	
	AES	encryption/de-encryption coupled to TKIP (as defined in 802.11-2007 and 802.1X)
Short Guard Interval	SGL support	-
Space-Time Block Coding	STBC support	-
Transmit Power	-	Up to +18dBm
Receive Sensitivity	Mode b (8% PER)	1Mb/s: -96dBm
		11Mb/s: -88dBm
	Mode g (10% PER)	6Mb/s: -90dBm
		12Mb/s: -89dBm
		54Mb/s: -75dBm
	Mode n/2.4GHz (10% PER)	1Mb/s: -96dBm
		54Mb/s: -75dBm
		M0/20MHz: -86 dBm
		M0/40MHz: -83 dBm
		M15/20MHz: -69 dBm
	Mode n/5GHz (10% PER)	M15/40MHz: -69 dBm
		6Mb/s: -89 dBm
		54Mb/s: -74 dBm
		M0/20MHz: -85 dBm
		M0/40MHz: -82 dBm
		M15/20MHz: -68 dBm
		M15/40MHz: -68 dBm

Table 3-3: WI-FI specification

3.2 General Features

Features	Refs. 769501-769502
GPON	1x Singlemode Optical Fiber Cable (SC/APC Connector)
Ethernet 10/100/1000Base-T	4x Ethernet UTP CAT5E direct or crossover AUTO-MDIX cable (RJ45)
RF Video Overlay ⁽¹⁾	1x Coaxial F type connector (75 Ohm)
FXS Ports	2x voice / fax RJ11 connector
USB Ports	2x USB 2.0
WI-FI (802.11b/g/n)	Yes
ON/OFF button	Yes
RESET button	Yes
OLT Interoperability (BBF.247)	Yes
DHCP Client	Yes
Number of GEM ports	256
Number of T-CONT	32
Primary Power Connection (VDC)	12 (± 15%)
Primary Power Connection (VAC)	230V AC 50Hz ±2Hz 110V AC 60Hz ±2Hz
Power Supply (W) ⁽²⁾	19
MTBF (h)	404660
Size (mm)	210x210x40
Temperature (°C)	-5 to 45
Humidity (%)	0 to 95

Table 3-4: General Features

NOTES:

(1) Optional ; Dependent on the Refs. 769501-769502 specific model

(2) An LPS power source is used to power the ONT equipment:

US/Canada:

The ONT must be powered by an external Listed Limited Power Source (LPS) or Class 2 Power source. The external power adapter must be LPS certified.

Rest of the World:

The ONT must be powered by an External CB approved Limited Power Source (LPS).

3.3 General Service Description

GPON layer per G984.x	<ul style="list-style-type: none"> > Comply with GPON standard: ITU-T G984.1/ G984.2/G984.3/G984.4; > GPON Encapsulation Method (GEM) supports Ethernet; > Configurable AES Downstream and FEC Downstream and Upstream; > Bitrates: 2488 Gbps (downstream) / 1244 Gbps (upstream). 	<ul style="list-style-type: none"> > Class B+ optics (28 dB); > T-CONT:32; > GEM-Port-IDs: 32.
L2/L3 layer	<ul style="list-style-type: none"> > VLAN-ID to GEM port-ID mapping (per WT-156): N:1 VLAN; 1:1; > Transparent VLAN; > Classification: IDSCP/TOS, 802.1p TCI, VLAN ID, MAC address; > Traffic Management: up to 8 queues per T-CONT in Priority-controlled mode or up to 16 queues per T-CONT in Rate-controlled scheduling mode. 	<ul style="list-style-type: none"> > 802.1q VLAN processing: Q-in-Q, tagging, removing tag, replacing tag or transparent forwarding; > Routing: Network Access Translation (NAT) and Network Access Port Translation (NAPT); > Firewall; > VPN; > DHCP Client and Server; > PPPoE Client; > Performance: 1000 Mbps Bidirectional.
IPTV	<ul style="list-style-type: none"> > IGMP v1/v2/v3 snooping; > IGMP processing per VLAN ID to support group of channels; > Interactive services (Video On Demand); > IPTV streams forwarding simultaneous: 128; > IPTV prioritization using Quality of Service (QoS) using 802.1p. 	-
VoIP	<ul style="list-style-type: none"> > T.38 Fax Relay; > Fax/Data Bypass; > Echo Canceller; > Echo Canceller Length; > Jitter Buffer; > Caller ID Generation; > G.711 PLC; > G.711 VAD and CNG; > G.723.1; > G.726 ADPCM; > G.729 Annex A. 	<ul style="list-style-type: none"> > G.729 Annex B; > Caller ID and Call waiting; > RTP/RTCP packet encapsulation; > RFC 2833 support; > In-band Signaling Detection and Generation (dial, busy, ring-back, stutter, distinctive ring); > 3-Way Conferencing; > RFC 3261 support (SIP).
Ethernet	<ul style="list-style-type: none"> > RJ-45 10/100/1000BASE-T; > Support Auto-negotiation; > Support auto MDI/MDIX. 	-
Video Overlay	<ul style="list-style-type: none"> > One port on a F Connector; > 75 Ohm impedance (nominal). 	<ul style="list-style-type: none"> > TV overlay: 1550nm -8dBm < Pin < +2dBm; > Analog bandwidth: minimum 47 MHz and maximum 1000 MHz; > Channel number depends on PAL B/G, PAL M, etc, systems.
WI-FI	<ul style="list-style-type: none"> > IEEE 802.11 b/g/n 	<ul style="list-style-type: none"> > 802.11 b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54Mb/s; > 802.11 n: Up to 300Mb/s over 2 spatial streams.
Management	<ul style="list-style-type: none"> > Web-based with GUI; > Remote management over the OMCI, PLOAM, OAM and TR-069, TR-104, TR-111, TR-142. 	<ul style="list-style-type: none"> > Secure software download upgrade via OMCI or TR-069; > Embedded Telnet server for remote management.

Table 3-5: Services

3.4 Optical metering

The equipment measures the downstream received power from the OLT in 1490nm and reports this value through OMCI. The accuracy of the measurement is +/- 3dBm, maximum. Optionally, Refs. 769501-769502 has also the chance to have an embeded optical reflective component in order to increase the FTTH probing capabilities in a 50 centimeters resolution factor, which turns to have a single probing system to probe all GPON network ONTs even when its number increases over Million customers.

3.5 Wavelength filtering

The optical interface has WDM filters that allow GPON coexistence with RF video services (1550-1560nm) and the new generation of NGPON1 technology, according to G.984.5 Recommendation.

ITU-T Rec. G987.1 is also granted for XGPON, (following FSAN NG-PON2).

In order to face the final user's demands, current GPON networks have to confront the first evolution in terms of terminal equipments and actual infrastructure. Migration will be available through a new wavelength planning, by allowing the co-existence of two different technologies over the same fiber. The ITU-T Rec. G987.1 provides a mechanism for GPON to XGPON migration with the possibility to achieve 2.5Gbps upstream path. Nominally downstream will be 10 Gbps.

The next figure depicts the wavelength planning of ITU-T Rec. G987.1:

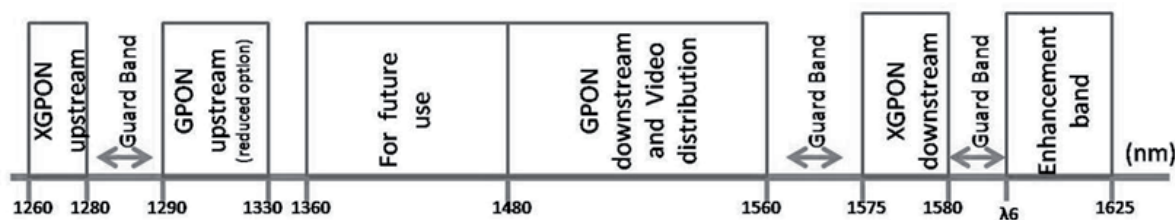


Figure 3-1: Wavelength planning

In order to accomplish to that plan, the upstream wavelength for GPON must be restricted to ONU (ONT) equipment based on the ordinary DFB lasers, while the XGPON downstream signal range is defined from 1575 nm to 1580 nm and the XGPON upstream signal from 1260 nm to 1280 nm. For the coexistence of XGPON and GPON over the same fiber, the CO requires a WDM filter that combines the downstream signal (1490 nm, 1555 nm and 1577 nm), isolating the 1310 nm and 1270 nm upstream signal, with the video signal. Also the wavelength of 1650 nm, used for fiber monitoring, has to be handled.

In addition, ONT devices require the use of a triplexer type transceiver that include an integrated filter or a discrete WDM filter to distinguish the different signals that may be present on the fiber. The current networks, equipped with ONT in accordance with the current ITU-T Rec. G984.5, will be easily updated to XGPON.

Class B+ optical budget are the nominal requirement for coexistence of GPON and XGPON over the same optical fiber. Taking this requirement into account, the fiber network architecture will not limit the future of the service provider business since GPON architectures, respecting B+ class of the GPON, are easily updated by placing newest terminal equipments, namely XOLT and XONT, and by replacing the current WDM filter by the new one in order to handle the new XGPON signals.

XGPON must support/emulate all GPON legacy services in case of total migration.

Like GPON, XGPON is required to support triple play services (data, voice and video), as well as mobile backhauling (accurate frequency/phase/time synchronization) application through its high quality of service and high bit rate feature capabilities. Access to Ethernet services such as point-to-point, multipoint-to-multipoint and rooted-multipoint Ethernet Virtual Connection services should be provided. Finally, as a global requirement, XG-PON needs to support IPv6.

3.6 GPON/Ethernet characteristics

GPON/Ethernet characteristics supported, both functional level and GTC-OMCI configuration, corresponds with the general mandatory characteristics defined in ITU-T G.984.3, G.984.4 and G.988 Recommendation:

- PON interface: downstream operating rate 2.488 Gbits/s, upstream operating rate 1.244 Gbits/s;
- 32 T-CONT and 256 simultaneous GEM ports;

- 1:64 SR is granted once optical power transmission from the OLT side is up from -27/30dBm;
- Unmarked or marked bandwidth management;
- Upstream and downstream FEC;
- Downstream AES encryption;
- Ethernet flow control in client's port: 802.3x and 802.3ab;
- Ability to classify and modify VLAN labels (single or double labeling);
- Ability to support multiple VLAN tags per service (Internet, IPTV, VoIP, ACS, etc) from Residencial Gateway. And ability to translate those VLAN to one specific service VLAN on OLT side, like, IPTV service VLAN, Internet Service VLAN (SVLAN and CVLAN), and VoIP Service VLAN;
- 802.1 DSCP for CoS support;
- IEEE 802.1Q and 802.1p support;
- Multicast snooping support IGMPv2 and IGMPv3;
- Firmware upgrade through the PON interface following the mechanisms specified in the ITU-T G.984.4 and G.988, including a safe dual firmware updates image system and the ability of back-up, allowing the SINGLE PORT Refs. 769501-769502 start in case the software download fails, to enable a new software update.

3.7 GPON management

The system supports the configuration according to the recommendations described in ITU-T, G.984, G.988 and BBF TR-156.

Specifically the next functionalities are obtained via OMCI for diagnostic (counters and alarms):

- Refs. 769501-769502 configuration checking of the services provisioned;
- Acquisition of the physical parameters of the SINGLE PORT GPON Refs. 769501-769502 interface;
- Traffic counters, statistics, errors, GPON interface status: by VLAN, by traffic type, by priority;
- Traffic counters, statistics, errors, GbE interface status are only available by port;
- Configuration parameters of services provisioned in the Refs. 769501-769502: T-CONT, GEMPORT, VLAN and GPON MAC tables;
- Alarms/events included in the standards mentioned above.

3.8 Standards

EMC	Standards	EMC Directive 89/336/EEC, EMC Addendum Directive 92/31/EEC, EMC Addendum Directive 91/263/EEC (Telecommunications Terminal Equipment Directive)
	Emissions	EN50081-1, EN55022
	Immunity	EN50082-1, EN61000-4-2, EN61000-4-3, EN61000-4-4
Operating Limits	Temperature	EN300019
	Relative humidity, maximum	EN300019
Environmental Standards	Acoustic noise	ISO 3743 (<45dBa)
Power and Grounding		ETSI EN 300 132-2 V2.1.1 (2003-01)
		ETSI ETS 300 253: January 1995
Energy Consumption		European Code of Conduct on Energy Consumption of Broadband Equipment V3
Safety and Protection		EN/IEC 60950-1
Mechanical Resistance		EN300019
Quality		CE - Conformité Européenne
RoHS 2002/95/EC Directive Compliance		
Certification		BBF.247 G-PON

Table 3-6: Standards compliance

4.2 Connections

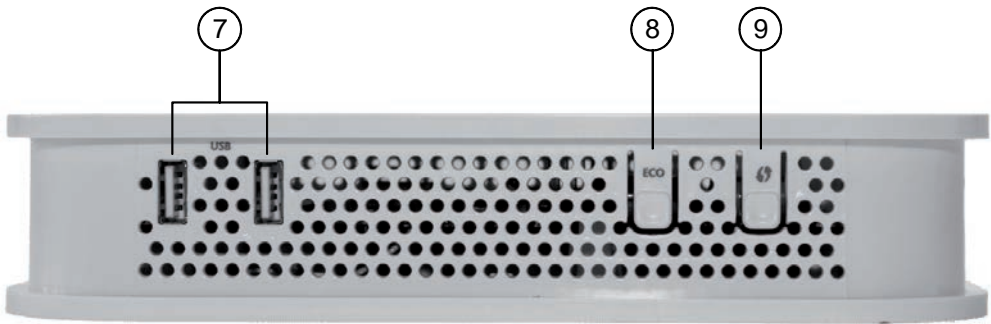


Figure 4-3: Refs. 769501-769502 connections 2





Number	Name	Description
1	12V 	12V DC Power Supply Connector
2		ON/OFF button
3	FXS (1, 2)	2x RJ11 – FXS Ports
4	LAN (1, 2, 3, 4)	4x RJ45 Ports - 10/100/1000Base-T Ethernet with AUTO-MDIX
5 ⁽¹⁾	RF Video ⁽¹⁾	Video RF Connector, F type ⁽¹⁾
6	RST	Configurations RESET button
7	USB (1, 2)	2x USB 2.0 ports
8	ECO	Energy saving button. In order to verify the status of all LEDS press the button. If not pressed only POWER and RADIO SIGNAL LEDs have up- dated status information.
9		WPS - WI-FI Protected Set-up
7	12V 	12V DC Power Supply Connector

Table 4-1: Refs. 769501-769502 connections description

NOTES:

(1) Optional ;

Dependent on the Refs. 769501-769502 specific model

4.3 How to Setup Refs. 769501-769502

The Refs. 769501-769502 may be installed horizontally on a flat surface or wall mounted. Quick steps for these setups are described below.

Wall-mount

Refs. 769501-769502 wall mounting kit consists of two AGL. ZN. CC. PZ. 3,5X30mm screws, standard DIN 7505-B and two Nylon M 6X30 wall anchors.

EN

- On the back of the Refs. 769501-769502 there are two mounting hole. Refer to Figure 4-4- a) to locate the mounting holes for your installation;
- Mark on the wall the two Refs. 769501-769502 holding screws' locations;
- Drill the holes on the wall with a drill bit size that matches the screws or wall anchors' size if you are using wall anchors;
- Secure the screws on the wall leaving a distance of about 3mm between the screw nut and the wall;
- Remove the Refs. 769501-769502 optical adaptor protection cap, Figure 4-4- b);
- Clean the Refs. 769501-769502 optical connector face within the optical adaptor with an appropriate optical connector cleaning material;
- Remove the protection cap of one of optical SC/APC connector of optical patchcord;
- Clean the optical SC/APC connector face with an appropriate optical connector cleaning material;
- Plug the patchcord cleaned SC/APC optical connector on the Refs. 769501-769502 SC/APC adaptor, observing the alignment mechanism, Figure 4-4- c);
- You will hear a click when the connector is secure into place;
- Pass the optical patchcord, in a counter- clockwise direction, round the storage circular guide on the back of the equipment, wrapping it round as many times as necessary, Figure 4-4- d). Please avoid small bend radius on the patchcord (30mm minimum bend radius);
- Pass the other end of the optical patchcord to the outside of the equipment using the passing hole, Figure 4-4- f);
- Fix the optical patchcord with plastic clamps to the Refs. 769501-769502 the appropriate fixing support fastening the plastic clamp just enough to secure the optical patchcord, Figure 4-4- e);
- Hold the Refs. 769501-769502 vertically and align the center of the equipment mounting holes Figure 4-4- a) with the holding screws in the wall;
- Assure the screws enter the mounting holes, Figure 4-4- a);
- Slide the equipment vertically down to hold it in place.

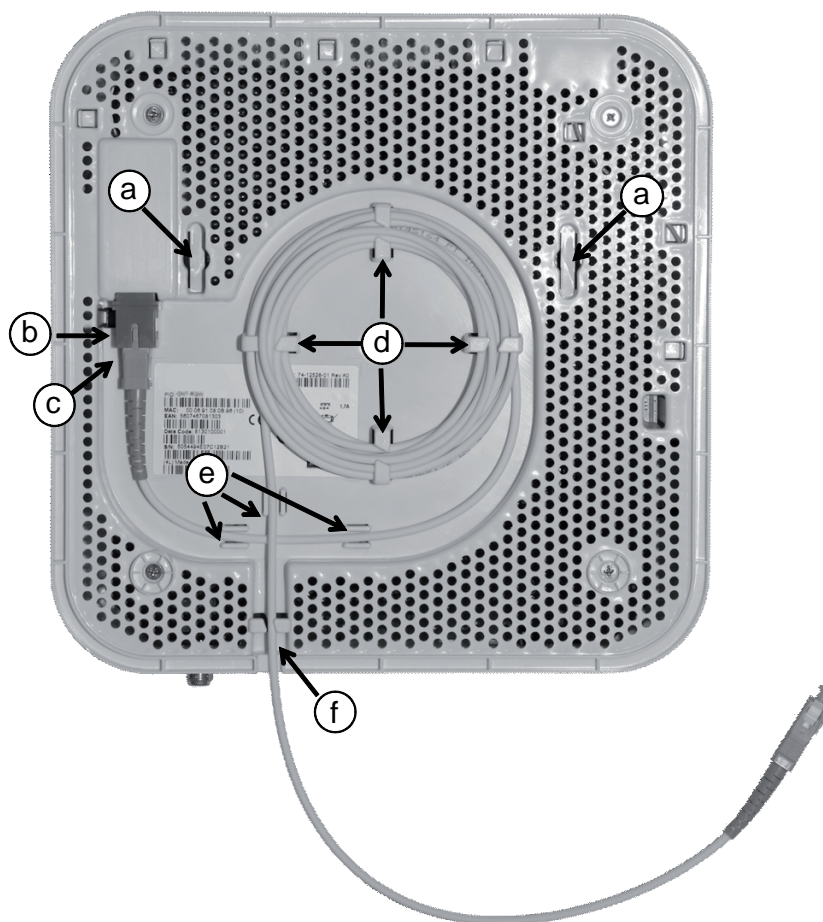


Figure 4-4: Refs. 769501-769502 back side –optical patch cord installation

Horizontal position

- Remove the Refs. 769501-769502 optical adaptor protection cap, Figure 4-4- b);
- Clean the Refs. 769501-769502 optical connector face within the optical adaptor with an appropriate optical connector cleaning material;
- Remove the protection cap of one of optical SC/APC connector of optical patchcord;;
- Clean the optical SC/APC connector face with an appropriate optical connector cleaning material;
- Plug the patchcord cleaned SC/APC optical connector on the Refs. 769501-769502 SC/APC adaptor, observing the alignment mechanism, Figure 4-4- c);
- You will hear a click when the connector is secure into place;
- Pass the optical patchcord, in a counter- clockwise direction, round the storage circular guide on the back of the equipment, wrapping it round as many times as necessary, Figure 4-4- d). Please avoid small bend radius on the patchcord (30mm minimum bend radius);
- Pass the other end of the optical patchcord to the outside of the equipment using the passing hole, Figure 4-4- f);
- Fix the optical patchcord with plastic clamps to the Refs. 769501-769502 the appropriate fixing support fastening the plastic clamp just enough to secure the optical patchcord, Figure 4-4- e).

4.4 Interface connection

4.4.1 Optical cable connection

Connect the optical cable (C1) from the Refs. 769501-769502 to the optical socket, Figure 4-5;

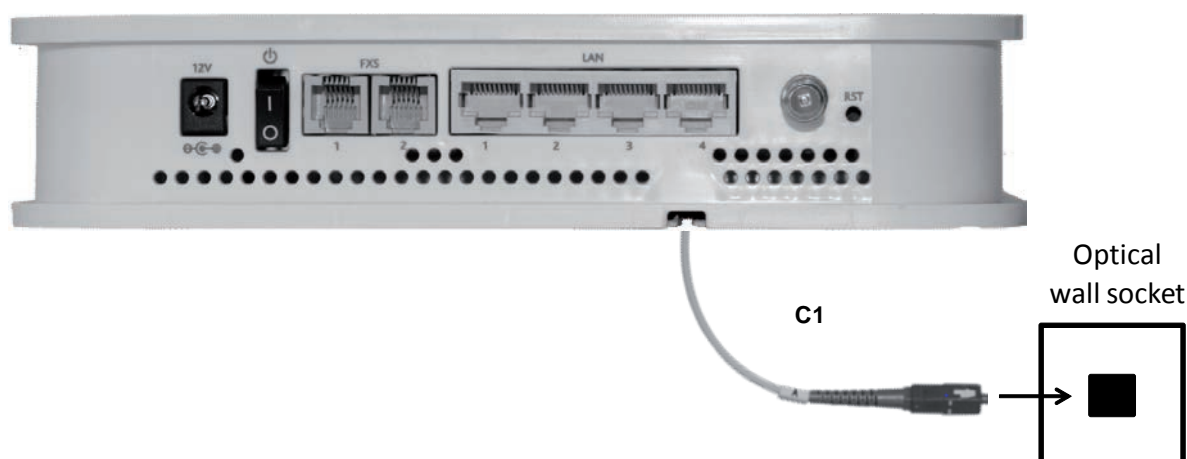


Figure 4-5: Interfaces connection (PON Interface)

4.4.2 General Overview of Refs. 769501-769502 Connections

Figure 4-6 below shows the connections to be made between the Refs. 769501-769502 and the home network devices. Please refer to Figure 4-1 and 4-1 for the Refs. 769501-769502 connector description and to Table 4-2 for the description of the connecting cables that must be used.

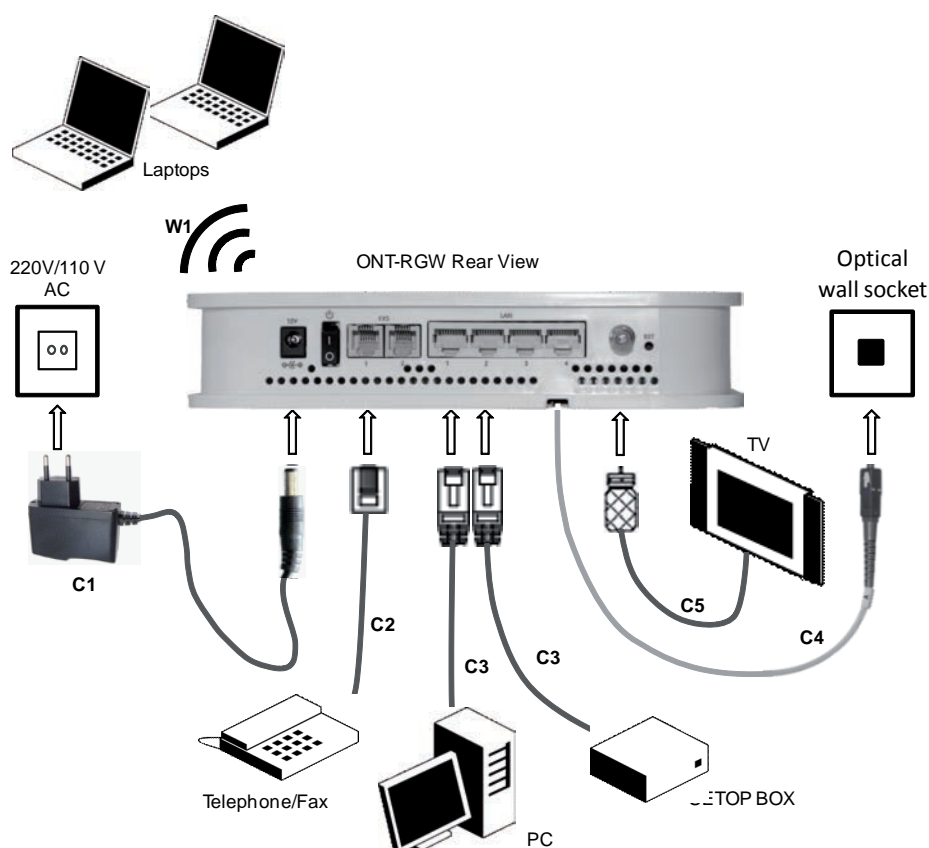


Figure 4-6: Refs. 769501-769502 connections

Connection	Description
C1	12V DC Adapter
C2	RJ11 Telephone cable
C3	Ethernet Cable UTP CAT56 cable (direct or crossover)
C4	Single-mode Optical Cable with SC/APC Connector (GPON)
C5 (1)	Cable with F-type Connectors, Coaxial 75 Ohm
W1	WI-FI

NOTES:

(1) Optional ;

Dependent on the Refs. 769501-769502 specific model

Table 4-2: Refs. 769501-769502 connections

5. Configuration

5.1 Refs. 769501-769502 activation

The Refs. 769501-769502 activation process has a distributed set of procedures that allow the connection of an inactive equipment to a PON network. This configuration is done following the procedure described in the OMCI protocol.

5.2 Customization

EN

For customization process, the requirements specified in the G.984.4, G.984.5 and 'Implementer's Guide' in the G.984.4 v1 are taken into account.

5.2.1 Software download from the OLT

The software download is made following the OMCI-based procedure included in the 'Implementer's Guide' of the G.984.4 Recommendation.

The Managed Entity (ME) in charge of managing the software download is named Software Image. Per each ME containing independently-manageable software, the Refs. 769501-769502 creates two software images. Each image will have three attributes:

- Valid - if it has been verified that its content is an image with executable code;
- Committed - if once the Refs. 769501-769502 is rebooted, it is loaded and executed;
- Active - if it is loaded and it is being executed in the Refs. 769501-769502.

There can be only one active image and only one committed image at a given moment. The Refs. 769501-769502 goes through a series of states in order to download and activate a software image. Each state is defined according to the states of the variables of both images. The OLT controls the Refs. 769501-769502 state through a series of commands:

- Start download
 - It starts the software download sequence. This action is only valid for inactive and non-committed software images;
- Download section
 - It downloads a section of a software image. This action is only valid for an image that is being downloaded;
- End download
 - It indicates the end of a download sequence, providing the CRC and information about version for the final verification of the downloaded software image. This action is only valid for a software image that is being downloaded;
- Activate image
 - It loads/executes a valid software image. When this action is applied to an inactive software image, the execution of the current code image is suspended, the associated software image is loaded from the non-volatile memory and the execution of the new code image is started. When this action is applied over a software image that is active, a reboot is executed;
- Commit image
 - It selects a valid SW image to be loaded and executed by default when the Refs. 769501-769502 is restarted;
- Composition of the Software Image
 - A software image is divided into sections of 31 bytes, with one section per OMCC message and each section protected by the CRC of the OMCC. A group of sections makes up a window, and a group of windows constituting the image.

5.3 Network Setup

Refs. 769501-769502 is the link between the modem and all of the peripherals in the LAN. The following figure shows a possible network setup containing three wireless computers and two wired computers.

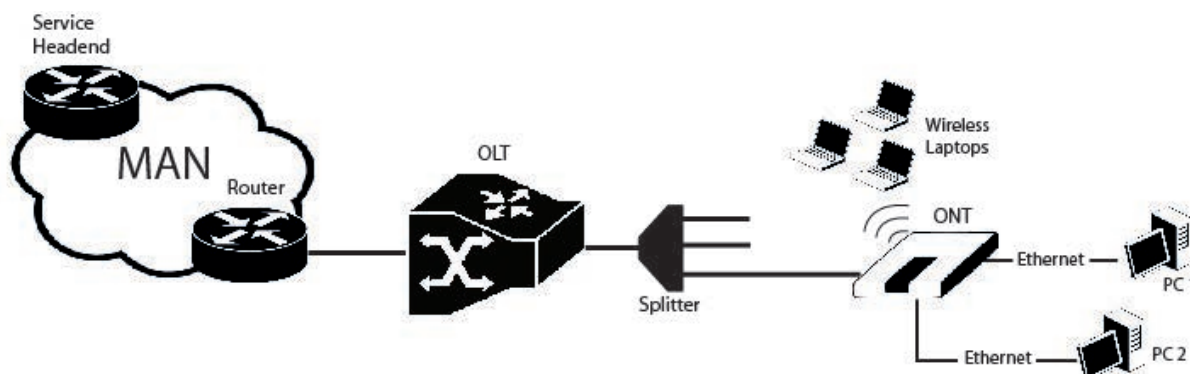


Figure 5-1: Refs. 769501-769502 Network Setup

5.4 Refs. 769501-769502 General Management Configuration

To configure the Refs. 769501-769502, enter the URL address **http://192.168.1.1** address in an internet browser.

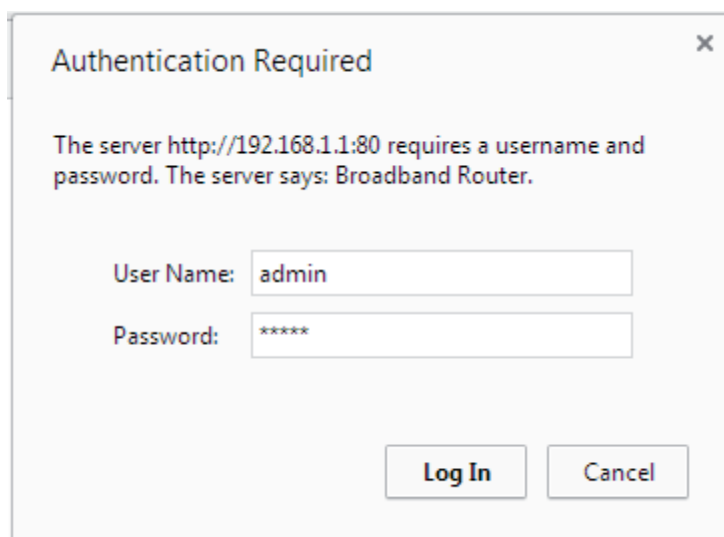


Figure 5-2: Refs. 769501-769502 management login

The administrative user and password is:

- User: admin
- Password: admin

After logging in, the main window is as shown in the next figure. The shown main window is device info summary window..

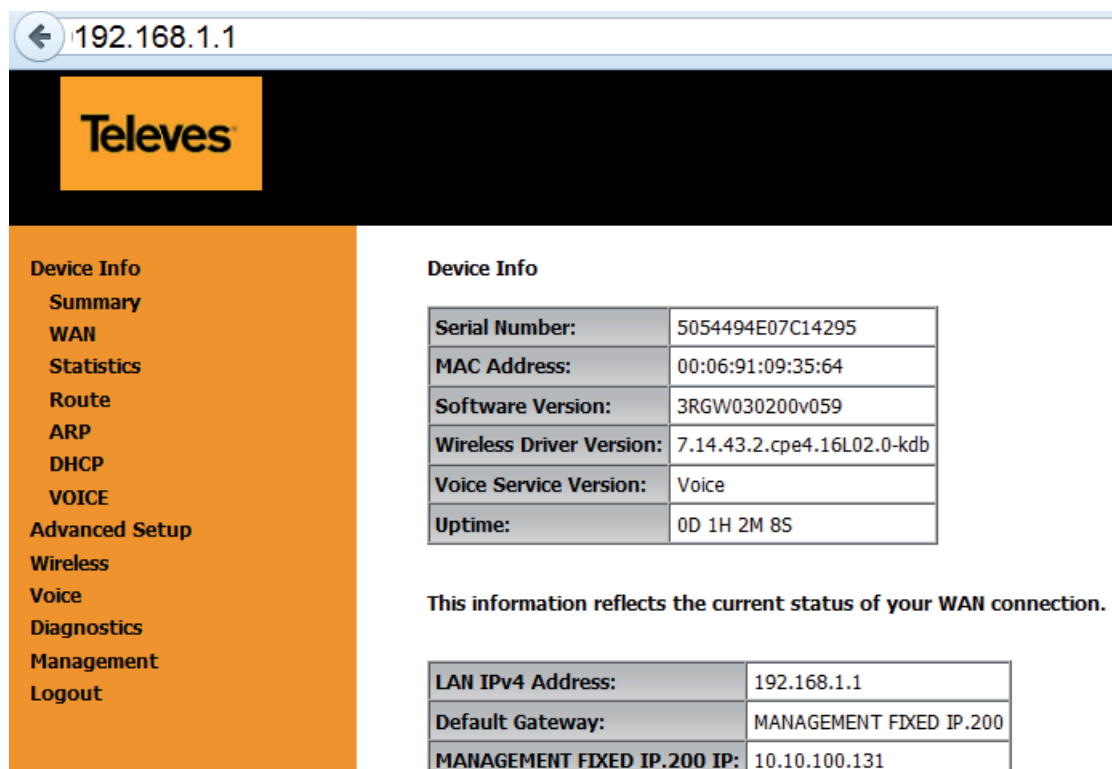


Figure 5-3: Refs. 769501-769502 management main screen

The Refs. 769501-769502 Management lets the user configure these categories by clicking the folder icons in the Control Menu pane.

- Device Info
- Advanced Setup
- Wireless
- Voice
- Diagnostics
- Management

5.5 Device Info

Selecting Device Info menu item, expands Device Info sub-menu into listed items, Figure 5-4:

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- VOICE



Figure 5-4 : Refs. 769501-769502 Graphic User Interface main menu

5.5.1 Summary

Selection of Device Info sub-menu item Summary, displays in the main window the initial device info configuration details, Figure 5-5. The initial displayed information will be updated to the current device info details by the performed configuration settings of the ONT. Description of the Device Info window parameters can be found in Table 5-1

Device Info	
Serial Number:	5054494E072894AF
Symmetric CPU Threads:	2
Software Version:	3RGW030000r760
Wireless Driver Version:	6.37.14.4803.cpe4.14L04.0-kdb
Voice Service Version:	Voice

LAN IPv4 Address:	192.168.1.1
Date/Time:	Thu Jan 1 00:25:42 1970

Figure 5-5: Device Info details – initial configuration

Parameter	Description
Serial Number	ONT serial number
Symmetric CPU Threads	Number of ONT Symmetric CPU Threads
Software Version	Installed ONT software version
Wireless Driver Version	Installed ONT Wireless Driver version
LAN IPv4 Address	ONT LAN initial IPv4 Address; corresponds to the ONT IPV4 address used to access the ONT HTTP GUI
Date/Time	Initial ONT date; this value will be updated the ONT has access to an NTP server, upon an IPoE configuration

Table 5-1: Device Info window parameters

5.5.2 WAN

Selection of the Device Info sub-menu item WAN displays in the main window the current WAN configuration details, Figure 5-6.

The window is composed of two tables:

- WAN info;
- GRE Tunnels Status

Description of the WAN Info Table parameters can be found in Table 5-2 and GRE Tunnels Status table parameters in Table 5-3.

WAN Info														
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Enable/Disable

GRE Tunnels Status									
Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Tunnel Mode	Status	

Figure 5-6: WAN current configuration details window – initial window

WAN Info														
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Enable/Disable
veip0.2	ipoe_veip0.15	IPoE	15	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Connected	172.22.107.126	(null)	Enable
ppp0.1	pppoe_veip0.11	PPPoE	11	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	172.22.190.70		Enable

GRE Tunnels Status									
Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Tunnel Mode	Status	
gre_tunnel	172.22.107.5	190.20.20.4	10.10.10.1	10.10.10.2	255.255.255.0	128	Layer 2	Enabled	

Figure 5-7: WAN current configuration details window – example of 2 WAN interfaces and a GRE Tunnel configured

Parameter	Description
Interface	WAN interface identification (string); attributed on the Wan interface configuration; if not set by the user, the system names the interface automatically as "xxx0.n/", where xxx is the type of interface (eg ppp stands for pppoe) n is number indicating order of interface creation, starting in 1
Description	WAN service description; String that can be entered by the user; default values indicates type of WAN service (pppoe/ipoe/gre/br), used layer 2 interface (eg. veip0/eth1) interface and used vlan id (eg. 11)
Type	Identifies Wan service Type (PPPoE/IPoE/gre/br)
VlanMuxId	Used 802.1Q VLAN ID (0-4094)
IPv6	Flag (enable/disable) ; indicates if IPv6 is enabled
Igmp Pxy	Flag (enable/disable) ; indicates if IGMP proxy is enabled; to use for multicast configuration in the case of IPv4.
Igmp Src Enbl	Flag (enable/disable); indicates if IGMP source is enabled; to use for multicast configuration in the case of IPv4.
MLD Pxy	Flag (enable/disable) ; indicates if MLD proxy is enabled; to use for multicast configuration in the case of IPv6.
MLD Src Enbl	Flag (enable/disable) ; indicates if MLD source is enabled; to use for multicast configuration in the case of IPv6.
NAT	Flag (enable/disable); Indicates if NAT is enabled

Table 5-2: WAN Info Table parameters

Parameter	Description
Tunnel Name	Gre Tunnel identification (string) configured when gre tunnel is created
Local IP	IP address of the local end interface of the GRE tunnel
Remote IP	IP address of the local end interface of the GRE tunnel
Tunnel IP	Tunnel IP Address
Peer IP	Peer IP Address
Tunnel Mask	Tunnel mask
TTL	Time To Live in seconds
Tunnel Mode	Indicates if this is a Layer 2 mode tunnel
Status	Flag (enable/disable); indicate the Tunnel is administratively enabled

Table 5-3: GRE Tunnels Status Table parameters

5.5.3 Statistics

When selected the Device Info sub-menu item Statistics expands into a statistics sub-menu, composed of the following items:

- LAN
- WAN Service

The main window shows the LAN statistics information.

5.5.3.1 LAN

Selection of the Device Info, Statistics submenu, item LAN displays in the main window the current LAN (Local Area Network) statistics information, Figure 5-8.

Received and Transmitted Total and per type of traffic Statistics will be displayed for each LAN interface with traffic. LAN statistics parameter description can be found in Table 5-4.

Statistics -- LAN

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
eth0	685124	5840	0	0	0	255	5585	0	2359645	5631	0	0	0	157	5474	0
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Reset Statistics

Figure 5-8: LAN Statistics

Parameter	Description
Interface	<p>LAN interface Identification (string).</p> <p>eth #, # - number : 0 to 3 – Refs. 769501-769502 ETH port number</p> <p>wl0, Wireless interface</p>
Total Received/transmitted	<p>Total values (Multicast+Unicast+Broadcast) of:</p> <p>Bytes – Total number of Received /Transmitted Bytes</p> <p>Pkts – Total number of Received/transmitted Packets</p> <p>Errs– Total number of Received/transmitted Errors</p> <p>Drops – Total number of Received/transmitted Drops</p>
Multicast Received/transmitted	<p>Number of received/transmitted Multicast:</p> <p>Bytes</p> <p>Pkts – Packets</p> <p>Errs– Errors</p> <p>Drops</p>
Unicast Received/transmitted	<p>Number of received/transmitted Unicast:</p> <p>Bytes</p> <p>Pkts – Packets</p> <p>Errs– Errors</p> <p>Drops</p>
Broadcast Received/transmitted	<p>Number of received/transmitted Broadcast:</p> <p>Bytes</p> <p>Pkts – Packets</p> <p>Errs– Errors</p> <p>Drops</p>

Table 5-4: LAN Statistics Table parameters

5.5.3.2 WAN Service

Selection of the Device Info, Statistics sub-menu Item WAN service displays in the main window the Wide Area Network statistics information per configured Wan service, Figure 2-1.

WAN Service statistics parameter description can be found in Table 5-2.

Statistics -- WAN

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
veip0.1	ipoe_veip0.15	23154	234	0	0	0	0	231	3	46296	358	0	0	0	0	358	0
veip0.3	br_veip0.12	588	14	0	0	0	0	13	1	160887	1654	0	0	24309	251	1031	372
ppp0.2	pppoe_veip0.11	195387898	148409	0	0	0	0	148409	0	48682762	87123	0	0	0	0	87123	0

Reset Statistics

Figure 5-9: WAN Statistics

Parameter	Description
Interface	WAN interface identification (string)
Description	WAN service description; String that can be entered by the user at the Wan service creation ; default values indicates type of WAN service (pppoe/ipoe/gre/br), used layer 2 interface (eg. veip0/eth1) interface and used vlan id (eg. 11)
Total Received/transmitted	<p>Total values (Multicast+Unicast+Broadcast) of:</p> <p>Bytes – Total number of Received /Transmitted Bytes</p> <p>Pkts – Total number of Received/transmitted Packets</p> <p>Errs– Total number of Received/transmitted Errors</p> <p>Drops – Total number of Received/transmitted Drops</p>
Multicast Received/transmitted	<p>Number of received/transmitted Multicast:</p> <p>Bytes</p> <p>Pkts – Packets</p> <p>Errs– Errors</p> <p>Drops</p>
Unicast Received/transmitted	<p>Number of received/transmitted Unicast:</p> <p>Bytes</p> <p>Pkts – Packets</p> <p>Errs– Errors</p> <p>Drops</p>

Parameter	Description
Broadcast Received/transmitted	Number of received/transmitted Broadcast: Bytes Pkts – Packets Errs– Errors Drops

Table 5-5: WAN Statistics Table parameters

5.5.4 Route

Selection of the Device Info sub-menu Route item, compresses the open Device info sub-menu if expanded (eg Statistics) and shows in the main window the Device Routing information, Figure 5-10. In the example bellow the destination address is the address of the Refs. 769501-769502 bridge (br0 Interface) and the route status is up.

Route Table parameter description can be found in Table 5-6.

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Figure 5-10: Device Route Info

Parameter	Description
Destination	IP Destination Address
Gateway	Used Gateway IP Address, if configured
Subnet Mask	Used sub network mask, if configured
Flag	Route status indication flag: U – UP ! – reject G - gateway H – host R – Reinstate D – Dynamic (redirect) M - modified
Metric	Used metric
Service	Service using the route
Interface	Interface used by the Route

Table 5-6: Device Routing information Table parameters

5.5.5 ARP

Selection of the Device Info sub-menu ARP item, compresses the open Device Info sub-menu if expanded (eg Statistics) and shows in the main window the Device ARP information, Figure 5-11.

Device ARP information parameter description can be found in Table 5-7.

ARP is used to convert an IP address to a Physical address. The ARP table

In the example bellow the IP Address is the allocated IP address by the Refs. 769501-769502 the latop connected to one of the device ETH LAN ports and used to access the device GUI (Graphic User Interface) for Device configuration. The HW address corresponding to this IP address is the laptop MAC, the ARP flags value is complete since the IP address was successfully resolved to the Laptop MAC address . The logical device the laptop is connected is the Refs. 769501-769502 bridge br0. This is the ARP table for this device.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.2	Complete	38:ea:a7:fc:4c:41	br0

Figure 5-11: Device ARP Info

Parameter	Description
IP Address	External Device IP Address
Flags	ARP status indication flag: Complete Incomplete...
HW address	External device Hardware address
Device	Used Device Interface
Metric	Used Metric
Service	Service using the route
Interface	Interface used by the route

Table 5-7: Device ARP information Table parameters

5.5.6 DHCP

Selection of the Device Info sub-menu DHCP item, compresses the open Device Info sub-menu if expanded (eg Statistics) and shows in the main window the Device DHCP Leases information, Figure 5-12.

Device DHCP information parameter description can be found in Table 5-8.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
p-cfmacedo2	38:ea:a7:fc:4c:41	192.168.1.2	23 hours, 45 minutes, 17 seconds
p-almeida2	64:27:37:76:23:1e	192.168.1.4	23 hours, 45 minutes, 28 seconds

Figure 5-12: Device DHCP Leases Info

Parameter	Description
Hostname	External Device(with an IP Address was attributed by DHCP lease by the Refs. 769501-769502) Name
MAC Address	External Device (with an IP Address was attributed by DHCP lease by the Refs. 769501-769502) MAC Address
IP Address	External Device IP Address attributed by DHCP lease by the Refs. 769501-769502
Expires in	Remaining validity time of DHCP leased External Device IP address

Table 5-8: Device DHCP Leases information Table parameters

5.5.7 Voice

Selection of the Device Info sub-menu VOICE item, compresses the open Device Info sub-menu if expanded (eg Statistics) and shows in the main window the Device Voice Status information, Figure 5-13

Device Voice Status information parameter description can be found in Table 19

Status -- Voice

SIP Account	User Name	User Status	Registration Status
1	undefined	Enabled	Disabled
2	undefined	Enabled	Disabled

Figure 5-13: Device Voice Status information table

Parameter	Description
SIP Account	SIP account identifier; two SIP account can be configured at the Refs. 769501-769502:
User Name	SIP Account Access Data Information: Username
User Status	SIP Account Access Data Information: User Status (enabled/disabled)e
Registration Status	Information of the status of SIP Account Registration process: (enabled/disabled)

Table 5-9:Device Voice Status information Table parameters

5.6 Advanced Setup

Selection of the main menu item Advanced Setup expands Advanced Setup sub-menu, Figure 5-14.



Figure 5-14: Advanced Setup Expanded Menu

The main Windows shows the Layer2 interface menu, GPON interface configuration window.

5.6.1 Layer2 Interface

This menu item allows the configuration of the wan ONT-wan interface (uplink interface) as GPON wan interface or ETH wan interface (physical electrical ETH interface). In the last case the Refs. 769501-769502 is configured simply as a conventional RGW.

Selection of Advanced Setup sub-menu item Layer2 Interface expands Layer2 Interface submenu items than allow the configuration of the WAN interface (uplink interface):

- GPON Interface
- Ethernet Interface

5.6.1.1 GPON Interface

Selection of Advanced Setup, Layer2 Interface sub-menu item GPON interface displays in the main window GPON WAN Interface Configuration window which is the default configuration for WAN interface, Figure 5-15. In this window it is possible to add or remove GPON WAN interface.

Device DHCP information parameter description can be found in Table 5-10.

GPON WAN Interface Configuration

Choose Add, or Remove to configure GPON WAN interfaces.
Allow one GPON as layer 2 wan interface.

NOTE: Create interfaces in order (example - create veip0 first, then veip1 and so on).

Interface/(Name)	Connection Mode	Remove
veip0/veip0	VlanMuxMode	<input type="checkbox"/>

Add Remove

Figure 5-15: GPON WAN Interface Configuration- initial window

Parameter	Description
Interface/(Name)	Refs. 769501-769502 WAN interface Identification. In the case of GPON Wan interface – veip0/veip0
Connection Mode	Value: VlanMuxMode
Remove	If selected, the WAN interface can be removed with Remove button

Table 5-10: GPON WAN interface configuration Table parameters

5.6.2 WAN Service

Selection of Advanced Setup submenu item Wan Service will display in the main window two configuration tables, Figure 5-20:

- Wan service setup
- GRE tunnels setup

Table parameters' description can be found in tables Table 5-12 and Table 5-13.

In this window it is possible the Addition and Removal of WAN services.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit	Enable/Disable
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------	----------------

GRE Tunnels Setup

Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Remove	Tunnel Mode	Enable/Disable
-------------	----------	-----------	-----------	---------	-------------	-----	--------	-------------	----------------

Add Remove

Figure 5-20: Advanced Setup WAN Service main window

Parameter	Description
Interface	WAN interface identification (string); attributed on the Wan interface configuration; if not set by the user, the system names the interface automatically as "xxx0.n/", where xxx is the type of interface (eg ppp stands for pppoe) n is number indicating order of interface creation, starting in 1

Parameter	Description
Description	WAN service description; String that can be entered by the user; default values indicates type of WAN service (pppoe/ipoe/gre/br), used layer 2 interface (eg. veip0/eth1) interface and used vlan id (eg. 11)
Type	Identifies Wan service Type (PPPoE/IPoE/gre/br)
Vlan8021p	IEEE 802.1P Priority value (0 to 7)- to use for tagged services Set to "-1" for Untagged services
VlanMuxId	Used 802.1Q VLAN ID (0-4094) for tagged services; for untagged services use value "-1"
VlanTpid	VLAN Tag Protocol Identifier;
Igmp Proxy	Flag (enable/disable) ; indicates if IGMP proxy is enabled; to use for multicast configuration in the case of IPv4.
Igmp Source	Flag (enable/disable); indicates if IGMP source is enabled; to use for multicast configuration in the case of IPv4.
Igmp Src Enbl	Flag (enable/disable); indicates if IGMP source is enabled; to use for multicast configuration in the case of IPv4.
NAT	Flag (enable/disable); Indicates if NAT is enabled
Firewall	Flag (enable/disable); Indicates if Firewall is enabled
IPv6	Flag (enable/disable) ; indicates if IPv6 is enabled
MLD Pxy	Flag (enable/disable) ; indicates if MLD proxy is enabled; to use for multicast configuration in the case of IPv6.
MLD Src	Flag (enable/disable) ; indicates if MLD source is enabled; to use for multicast configuration in the case of IPv6.
Remove	If selected, the WAN Service can be removed with Remove button
Edit	Flag (enable/disable) ; indicates if IPv6 is enabled
Enable/Disable	Flag (enable/disable); indicate if the interface is administratively enabled

Table 5-12: WAN Service Setup Table parameters

Parameter	Description
Tunnel Name	GRE Tunnel identification (string) configured when gre tunnel is created
Local IP	IP address of the local end interface of the GRE tunnel
Remote IP	IP address of the local end interface of the GRE tunnel
Tunnel IP	Tunnel IP Address
Peer IP	Peer IP Address
Tunnel Mask	Tunnel mask
TTL	Time To Live in seconds
Remove	If selected, the GRE Tunnel can be removed with Remove button
Tunnel Mode	Indicates if this is a Layer 2 mode tunnel
Enable/Disable	Flag (enable/disable); indicate the Tunnel is administratively enabled

Table 5-13: GRE Tunnels Setup Table parameters

5.6.2.1 WAN Service Creation

To create a WAN service, use the ADD button in the Advanced Setup WAN service Main window, Figure 5-20. A new window will be displayed where is possible to select on a combo box the Refs. 769501-769502 WAN interface associated to the service to create, Figure 5-21. Once selected the WAN interface use the Next Button, Figure 5-22, to progress to the next WAN service configuration window – Type of service selection and service configuration, Figure 5-23.

Four types of WAN services can be created and configured:

- PPP over Ethernet (PPPoE)
- IP over Ethernet (IPoE)
- GRE Tunneling (over Layer 2)
- Bridging.

WAN Service Interface Configuration

Select a layer 2 interface for this service

veip0/veip0 ▼

Back

Next

Figure 5-22: WAN service Interface selection for the WAN service to setup

5.6.2.1.1 PPPoE Type of Service Creation

After the selection of the WAN interface associated to the service to create, Figure 5-21 and Figure 5-22, use the Next button Figure 5-22, to progress to the next WAN Service setup window- Wan service Configuration, Figure 5-23

At this window execute the following steps:

STEP 1. Select the PPP over Ethernet (PPPoE) WAN service type.

STEP 2. At the Field Service Description enter a string for the service description; the default service description is a string automatically filled in when the type of device is selected (Step 1) and composed by the type of Service followed by underscore and the WAN interface name, e.g. pppoe_veip0

Next fields of the WAN service configuration are related to VLAN tagging configuration:

- 802.1P priority; definition of the upstream traffic classification by attributing a Pbit value (0->7; 0 being the lowest priority traffic)
- 802.1Q VLAN ID, Specifies the VLAN identifier; values from 0 to 4096
- VLANTPID; Tag Protocol Identifier (TPID) is a 16-bit field of the IEEE 802.1Q header, that is used to identify the frame as a tagged frame;

Possible values are:

- 0x8100, TPID default value; Used for single tagged frames or for double tagged frames as the inner or customer VLAN tag (802.1ad conventions)
- 0x88A8, Used in double tagged frames, for the outer or service VLAN tag (802.1ad conventions); in this case the inner VLAN (C-VLAN) tag TPID has the default value of 0x8100;
- 0x9100, Used in double tagged frames, for the outer or service VLAN tag (older version of 802.1Q); in this case the inner VLAN (C-VLAN) tag TPID has the default value of 0x8100;

5.6.2.1.2 VLAN Tagging Configuration Procedure

STEP 3. For tagged service, at the field 802.1P priority, enter the pbit value (0-7) to mark the upstream traffic according to the desired CoS for the service to create; a higher value corresponds to a higher priority CoS; For untagged service leave the field with the default value of -1;

STEP 4. For tagged service, at the VLAN ID field enter the VLAN ID value (0-4094) of the VLAN used by the service.

For untagged service leave the field with the default value of -1;

STEP 5 For tagged service select a TPID value from the selection combo box, Figure 5-23.

0x8100, TPID default value; if selected a single tagged service is configured.

0x88A8 or 0x9100, TPID used for the outer VLAN (S-VLAN) for double tagged services; if selected a double VLAN tagged service is configured; in this case the inner VLAN (C-VLAN) tag TPID has the default value of 0x8100;

STEP 6 At the field Network Protocol Selection use the selection combo box to choose one of the available options:

- IPv4 Only (default value);
- IPv4 & IPv6 (Dual Stack);
- IPv6 Only;

Figure 5-23: WAN service setup – type of service selection and service configuration – PPPoE service

STEP 7. Once the WAN service setup parameters are configure use Next button, Figure 5-26, to progress to the next WAN Service setup window- Connection establishment parameters configuration, Figure 5-27

WAN Service Configuration

Select WAN service type:

- ☒ PPP over Ethernet (PPPoE)
- ☐ IP over Ethernet
- ☐ GRE Tunneling (over Layer 2)
- ☐ Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Network Protocol Selection:

7

Figure 5-26: WAN service setup– type of service selection and service configuration – finalize type of service configuration

The WAN Service Setup window– Connection establishment configuration, Figure 5-27, allows the configuration of the PPoE connection establishment parameters, as explained below.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

☐ Enable Fullcone NAT

☐ Dial on demand (with idle timeout timer)

☐ PPP IP extension

☐ Use Static IPv4 Address

☐ Enable PPP Debug Mode

☐ Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast Proxy

☐ Enable IGMP Multicast Proxy

☐ Enable IGMP Multicast Source

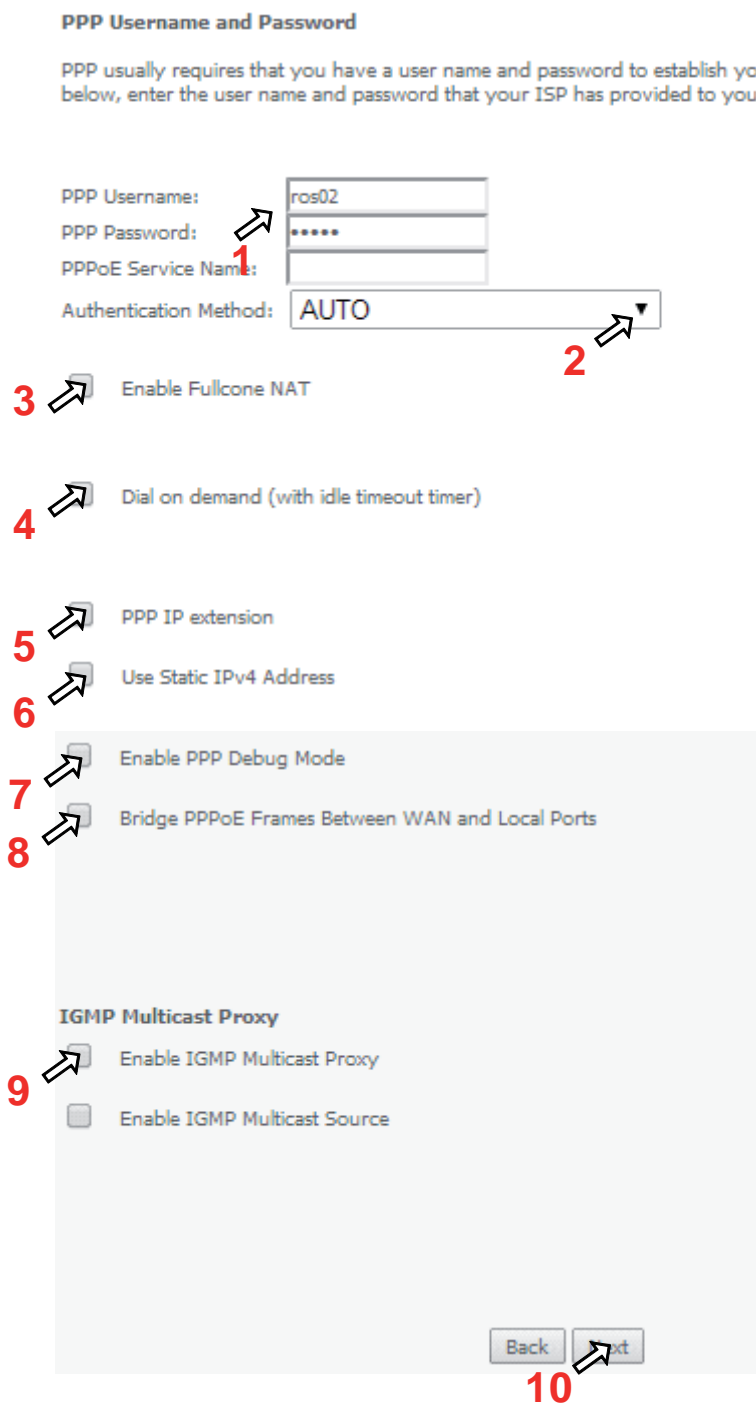


Figure 5-27: WAN Service Setup – Connection establishment configuration window

5.6.2.1.3 PPPoE Connection Establishment Parameters Configuration

STEP 1. Select the PPP username and password and use the access data provided by your ISP (Username and password) to establish the PPPoE connection, Figure 5-27;

STEP 2. At the authentication method selection combo box select one of the available option, Figure 5-28:

- AUTO;
- PAP, Password Authentication Protocol, simple unsecure method of authentication since password are send unencrypted over the network; the authentication is done once upon link establishment.
- CHAP, Challenge-Handshake Authentication Protocol, secure authentication method, uses a secret known by the client and the authentication server; the authenticator sends a challenge to which the client must answer to by using the secret. The answer is compared against the result obtained by the authenticator itself using the secret. CHAP periodically verifies the identity of the client by sending a new challenge.
- MSCHAP, Microsoft extension to the CHAP protocol – is a modified CHAP.

STEP 3. If Fullcone NAT is to be used select the option Enable Fullcone NAT; If enabled a warning message on the disadvantages of its use is shown, Figure 5-29

FullCone NAT is also known as one-to-one NAT: An LAN internal address, port pair is mapped to an external address, port pair so that any packets from the internal address, port pair will be sent through the external address, port pair and any external host can send packets to the internal Address, Port pair by sending packets to external Address, Port pair. Once established a fullcone NAT mapping for LAN internal address and port, it can be reached by any external host without the need of any request from the LAN internal address.

STEP 4. If Dial on Demand is selected inactivity timeout period in minutes must be specified, Figure 5-30. This corresponds to the time of inactivity (without traffic) after which the PPPoE connection goes down; the connection recovers when activity is detected.

STEP 5. Selected if PPP IP extension is to be used, Figure 5-27

STEP 6. If Use Static IPv4 is selected, the IPv4 address must be entered, Figure 5-31

STEP 7. Selection of Enable PPP debug mode, Figure 5-27, allows to see the packets exchanged in the PPP connection.

STEP 8. Bridge PPPoE Frames between WAN and local ports configures bridging mode

STEP 9. IGMP multicast proxy configuration allows the configuration as either IGMP proxy or IGMP source and enable/disable Multicast VLAN filter, Figure 5-32.

STEP 10. Once the Connection establishment parameters are configured use Next button, Figure 5-27, to progress to the next WAN Service setup - Routing Default Gateway configuration window, Figure 5-33.

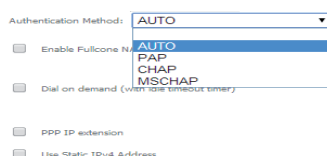


Figure 5-28: WAN Service Setup - Connection establishment configuration window- ppp authentication method available options



Figure 5-29: WAN Service Setup – Connection establishment configuration window- Enable fullcone NAT warning message

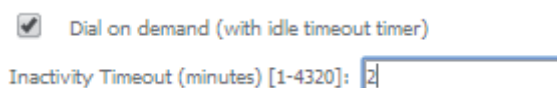


Figure 5-30: WAN Service Setup – Connection establishment configuration window- Dial on demand Configuration

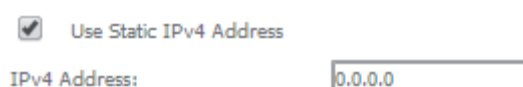


Figure 5-31: WAN Service Setup – Connection establishment configuration window- Use of static IPv4 Configuration



Figure 5-32: WAN Service Setup – Connection establishment configuration window- IGMP Multicast Proxy configuration

5.6.2.1.4 Routing Default Gateway Configuration

The Routing Default Gateway configuration window presents two lists:

- Selected Default Gateway Interfaces: the WAN interfaces that can be used as default gateway interfaces are listed here; only one interface will be used as default gateway interface- this interface will be the highest priority interface of the connected WAN interfaces in this list;

WAN interface priority is based on its position on the list, the first one of the list being the highest priority interface.

To change WAN interface priority, its position in the list must be changed; that can be achieved by removing all from the Selected Default Gateway Interfaces list and adding them back in the desired order.

- Available Routed WAN Interfaces: all defined available routed WAN interfaces are listed here; these interfaces can be moved to the Selected Default Gateway interfaces list

If there is only one WAN interface defined in the system, as in the example presented, this will be selected by the system as the default gateway interface thus being presented in the Selected default gateway list on the left.

If more WAN interfaces are shown in the list on the right (available routed WAN interfaces) one or more can be moved to the list on the left and be selectable as default gateway routed interface according to its priority in the list.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

ppp0.1

->

<-

Available Routed WAN Interfaces

Back

Next

EN

Figure 5-33: WAN Service setup - Routing Default Gateway configuration window

After default gateway interface configuration, use the Next button, Figure 5-33, to progress to the next WAN Service setup – DNS Server configuration parameters window, Figure 5-34.

5.6.2.1.5 DNS Server Configuration

DNS server interface can

- either be selected from available WAN interfaces, Figure 5-34, 1, from the list Selected DNS Server Interfaces, according to its priority (please see description below),
- or use a Static DNS IP address, in which case this option must be selected, Figure 5-34, 2, and the Static DNS servers (primary and secondary) IP addresses must be entered.

5.6.2.1.5.1 Selection of DNS Server Interfaces from Available WAN interfaces

The DNS Server Configuration window presents two lists:

- **Selected DNS Server Interfaces:** the WAN interfaces that can be used as system DNS Server interfaces are listed here; only one interface will be used as DNS server interface- this interface will be the highest priority interface of the connected WAN interfaces in this list;

WAN interface priority is based on its position on the list, the first one of the list being the highest priority interface.

To change WAN interface priority, its position in the list must be changed; that can be achieved by removing all from the Selected DNS Server Interfaces list and adding them back in the desired order.

- Available WAN Interfaces: all defined available routed WAN interfaces are listed here; these interfaces can be moved to the Selected DNS Server interfaces list

If there is only one WAN interface defined in the system, as in the example presented, this will be selected by the system as the default gateway interface thus being presented in the Selected DNS Server list on the left.

If more WAN interfaces are shown in the list on the right (available WAN interfaces) one or more can be moved to the list on the left and be selectable as Selected DNS Server interface according to its priority in the list.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

1 **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces

ppp0.1

->

<-

Available WAN Interfaces

2 **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

Figure 5-34: WAN Service setup – DNS Server configuration window

Once the DNS server configuration is done the PPPoE WAN service configuration is complete. Use the Next button to progress to the WAN Service Setup Summary window, Figure 5-35. This table should reflect the configuration for the WAN service setup parameters that have been entered on the successive WAN service setup configuration windows. Network Address Translation flag and Firewall flag default configurations are enabled. Please verify the presented configuration matches the settings provided by the ISP for this service.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back
Apply/Save

Figure 5-35: WAN Service Setup Summary window

To finalize the configuration use the Save/Apply button, Figure 5-35. The next displayed window is initial window, the WAN Service Window, where the service configured is displayed in the corresponding table, Figure 5-36.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit	Enable/Disable
ppp0.1	pppoe_veip0.11	PPPoE	0	11	0x8100	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit	Disable

GRE Tunnels Setup

Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Remove	Tunnel Mode	Enable/Disable
<input type="button" value="Add"/> <input type="button" value="Remove"/>									

Figure 5-36: WAN Service Setup Initial Window- service configuration displayed

It is now possible to view the configured WAN service parameters as well as obtained IP address by Selecting the Device Info sub-menu item WAN, Figure 5-37. Date and Hour are updated at the Device Info window, Figure 5-38.

WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Enable/Disable
ppp0.1	pppoe_veip0.11	PPPoE	11	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	172.22.190.70		Enable

GRE Tunnels Status

Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Tunnel Mode	Status

Figure 5-37: Device Info- WAN Service Current configuration and IP Address

After WAN service configuration, the Routing table, Figure 5-39, DNS table, Figure 5-40 and Interfacer Grouping information, Figure 5-41, are updated reflecting the configurations done, in this example the configured ppp0.1 interface appears in the Routing and DNS tables as the default WAN interface and in the Interface Grouping and the default WAN interface.

Device Info

Serial Number:	5054494E072894AF
Symmetric CPU Threads:	2
Software Version:	3RGW030000r760
Wireless Driver Version:	6.37.14.4803.cpe4.14L04.0-kdb
Voice Service Version:	Voice

This information reflects the current status of your WAN connection.

LAN IPv4 Address:	192.168.1.1
Default Gateway:	ppp0.1
Primary DNS Server:	192.168.122.82
Date/Time:	Fri Feb 14 09:34:02 2014

Figure 5-38: Device Info- Date and hour update

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

ppp0.1

->

<-

Available Routed WAN Interfaces

TODO: IPV6 ***** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface

NO CONFIGURED INTERFACE ▼

Apply/Save

Figure 5-39: Advanced Setup / routing - current routing table

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces

Available WAN Interfaces

Selected DNS Server Interfaces		Available WAN Interfaces
ppp0.1	<div>-></div> <div><-</div>	

☐ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

TODO: IPV6 ***** Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

☐ Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

☒ **Use the following Static IPv6 DNS address:**

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Apply/Save

Figure 5-40: Advanced Setup / DNS- current DNS server table

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	eth0.0	
			eth2.0	
			eth3.0	
			wlan0	

Figure 5-41: Advanced Setup /Interface Grouping- current Interface Grouping table

5.6.2.2 IPoE Type of Service Creation

After the selection of the WAN interface associated to the service to create, Figure 5-21 and Figure 5-22 , use the Next button at Figure 5-22, to progress to the next WAN Service setup window- Wan service Configuration, Figure 5-42.

At this window execute the following steps:

- STEP 1.** Select the IP over Ethernet (IPoE) WAN service type.
- STEP 2.** At the Field Service Description enter a string for the service description; the default service description is a string automatically filled in when the type of device is selected(Step1) and composed by the type of Service followed by underscore and the WAN interface name , e.g. ipoe_veip0.
- STEP 3 to 6.** Next fields of the WAN service configuration are related to VLAN tagging configuration; please refer to section: 5.6.2.1.2 VLAN Tagging Configuration Procedure.
- STEP 7.** Once the WAN service setup parameters are configured use Next button, Figure 5-42, to progress to the next WAN Service setup window- WAN IP Settings configuration, Figure 5-43.

WAN Service Configuration

Select WAN service type:

- ☐ PPP over Ethernet (PPPoE)
- ☒ IP over Ethernet
- ☐ GRE Tunneling (over Layer 2)
- ☐ Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Network Protocol Selection:

Figure 5-42: WAN service setup-type of service selection and service configuration – IPoE service

5.6.2.2.1 WAN IP Settings

WAN IP Settings should use the information provided by the ISP.

IP address can be obtained automatically via DHCP or can be statically configured.

5.6.2.2.1.1 Obtain IP Address Automatically

STEP 1. Select the option "Obtain an IP address automatically, option 1 of Figure 5-43.

STEP 2. DHCP will be used to obtain an IP address; there are 4 DHCP options that can be configured:

Option 60 Vendor ID: String value; this option allows the identification of the vendor by the DHCP server and is used in this context to identify in the DHCP server the IP Address pool to use by the configured service.

Option 61- IAID (Identity Association Identifier): value-8 hexadecimal digits; IAID is a binding between an interface and one or more IP addresses – this option used with DUID allows to identify an interface in a client to which will be attributed a temporary IP address by DHCPv6

Option 61- DUID (DHCP Unique Identifier): value -1 hexadecimal digit; this option identifies a DHCPv6 participant; each allocation in the DHCPv6 server is identified by a DUID and an IAID

Option 125 Vendor Identifying – Vendor Options: Flag –Enable/disable; the definition of the information carried in this option is vendor specific. Use of vendor-specific information allows enhanced operation, utilizing additional features in a vendor's DHCP implementation.

5.6.2.2.1.2 Use of Static IP Address

- STEP 1. Select the option "Use the following Static IP address", option 2 of Figure 5-43.
- STEP 2. Enter WAN IP address to be used
- Enter WAN Subnet Mask to be used;
- Enter WAN gateway IP Address to be used
- STEP 3. Use the Next button to progress to the WAN Service setup window- Network Address Translation Settings configuration

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

1

☒

Obtain an IP address automatically

Option 60 Vendor ID:

XPTQGR24xxG_VoIP

(8 hexadecimal digits)

Option 61 IAID:

(hexadecimal digit)

Option 61 DUID:

(hexadecimal digit)

Option 125:

☒ Disable

☐ Enable

2

☐

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Figure 5-43: WAN Service setup window- WAN IP Settings configuration

5.6.2.2.2 Network Address Translation Settings

To use NAT, option "Enable NAT" must be selected, Figure 5-44; If NAT option is selected, the option Fullcone NAT is available; if selected a warning message on the disadvantages of its use is shown, Figure 5-45.

To use Firewall option "Enable Firewall" must be selected, Figure 5-44.

In this window is also possible to configure IGMP Multicast as Proxy by selecting option "Enable IGMP Multicast Proxy" or as a Source by selecting option "Enable IGMP Multicast Source" and enable/disable Multicast VLAN filter, Figure 5-46.

ArPing Setup allows ArPing to be enabled and the number of repetitions and timeout to be configured. To configure ArPing "Enable ArPing" Option must be selected, Figure 5-47, and the values for number o repetitions and timeout interval (seconds) must be entered. ArPing is similar to Ping as given an IP address it test to find out if this is in use on the local network, and can get additional information about the device using that address.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☐ Enable NAT☐ Enable Firewall**IGMP Multicast**☐ Enable IGMP Multicast Proxy☐ Enable IGMP Multicast Source**ArpPing Setup**☐ Enable ArpPing

Number of Repetitions:

Timeout (sec):

Back

Next

Figure 5-44: WAN Service setup window- NAT, IGMP and Arping Settings configuration

☒ Enable NAT☒ Enable Fullcone NAT

ONLY IF REQUIRED -- DISABLES NETWORK ACCELERATION AND SOME SECURITY

☐ Enable Firewall

Figure 5-45: WAN Service setup window- Network Address Translation Settings configuration Enable fullcone NAT warning message

IGMP Multicast☒ Enable IGMP Multicast Proxy☒ Enable IGMP Multicast Source☐ No Multicast VLAN Filter

Figure 5-46: WAN Service setup window- IGMP Multicast configuration options

ArpPing Setup☒ Enable ArpPing

Number of Repetitions: 3

Timeout (sec): 3600

Figure 5-47: WAN Service setup window- ArPing Setup

Once the NAT, IGMP and Arping Settings are configured use Next button Figure 5-44, to progress to the next WAN Service setup - Routing Default Gateway configuration window, Figure 5-48.

The actual default gateway configuration is presented in this window, with the ppp0.1 WAN interface previously configured shown as the default Gateway interface. In the list of available WAN routed interfaces the veip0.2 used in this IPoE service configuration is shown, Figure 5-48, and can be used to change/update default Routing Default Gateway current configuration.

Please refer to section 5.6.2.1.4 Routing Default Gateway Configuration, for the explanation of the configuration.

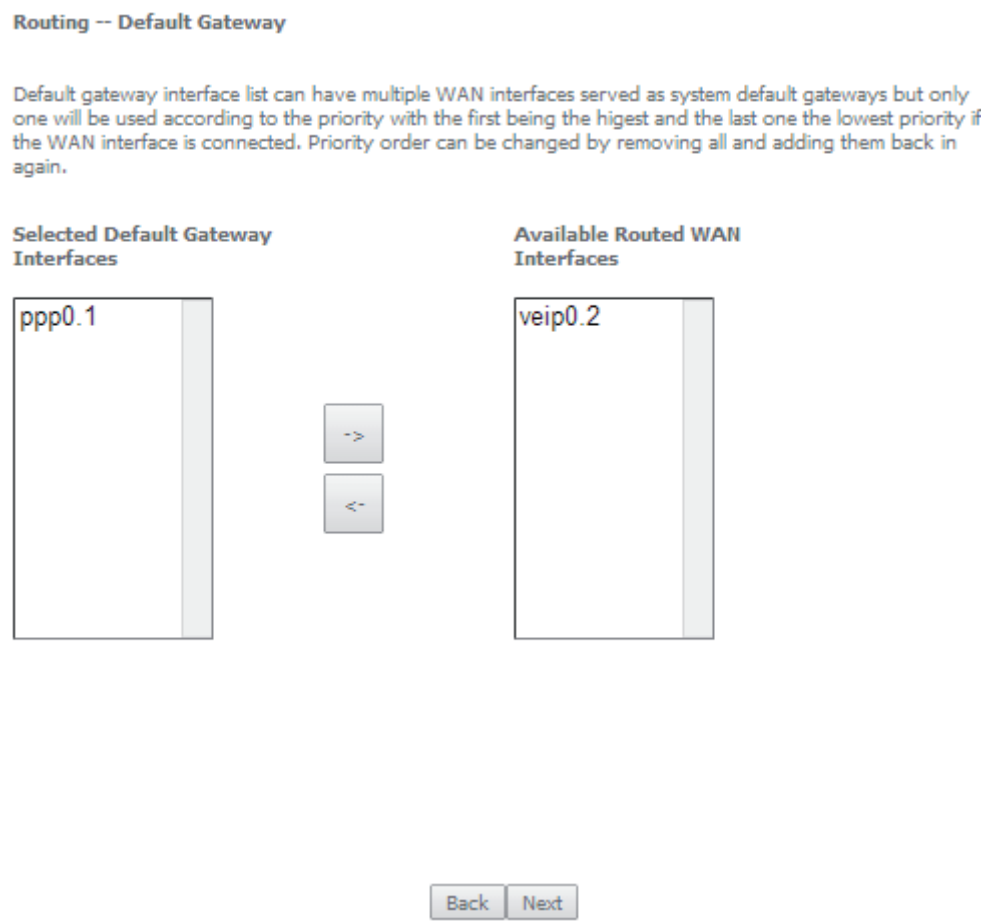


Figure 5-48: WAN Service setup - Routing Default Gateway configuration window

After default gateway interface configuration, use the Next button, Figure 5-48, to progress to the next WAN Service setup – DNS Server configuration parameters window, Figure 5-49.

DNS table, as well as previously shown Routing table, is in accordance with current Default Gateway configuration, Figure 67: ppp0.1 is thus shown as the current DNS server interface, but veip0.2 WAN interface is available for changing/updating DNS server interface if desired.

Please refer to section 5.6.2.1.5 DNS Server Configuration, for the explanation of the configuration.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces

ppp0.1

->

<-

Available WAN Interfaces

veip0.2

☐ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

Figure 5-49: WAN Service setup – DNS Server configuration parameters window

Once the DNS server configuration is done the IPoE WAN service configuration is complete. Use the Next button to progress to the WAN Service Setup Summary window, Figure 5-50. This table should reflect the configuration for the WAN service setup parameters than have been entered on the successive WAN service setup configuration windows. Network Address Translation flag and Firewall flag default configurations are enabled. Please verify the presented configuration match the settings provided by the ISP for this service.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Figure 5-50: WAN Service Setup Summary window- IPoE service configured

To finalize the configuration use the Save/Apply button, Figure 5-50. The next displayed window is initial window, the WAN Service Window, where the service configured is displayed in the corresponding table, Figure 5-51.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit	Enable/Disable
veip0.2	ipoe_veip0.15	IPoE	0	15	0x8100	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit	Disable
ppp0.1	pppoe_veip0.11	PPPoE	0	11	0x8100	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit	Disable

GRE Tunnels Setup

Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Remove	Tunnel Mode	Enable/Disable
<div>Add Remove</div>									

Figure 5-51: WAN Service Setup Initial Window- service configuration displayed

It is now possible to view the currently configured WAN services' parameters as well as obtained IP addresses by Selecting the Device Info sub-menu item WAN, Figure 5-52.

WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Enable/Disable
veip0.2	ipoe_veip0.15	IPoE	15	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Connected	172.22.107.126	(null)	Enable
ppp0.1	pppoe_veip0.11	PPPoE	11	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	172.22.190.70		Enable

GRE Tunnels Status

Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Tunnel Mode	Status

Figure 5-52: Device Info-WAN Service Current configuration and IP Addresses

5.6.2.3 GRE Type of Service Creation

A GRE tunnel configuration example will be given, showing the GRE tunnel settings configuration at the Network A Refs. 769501-769502.

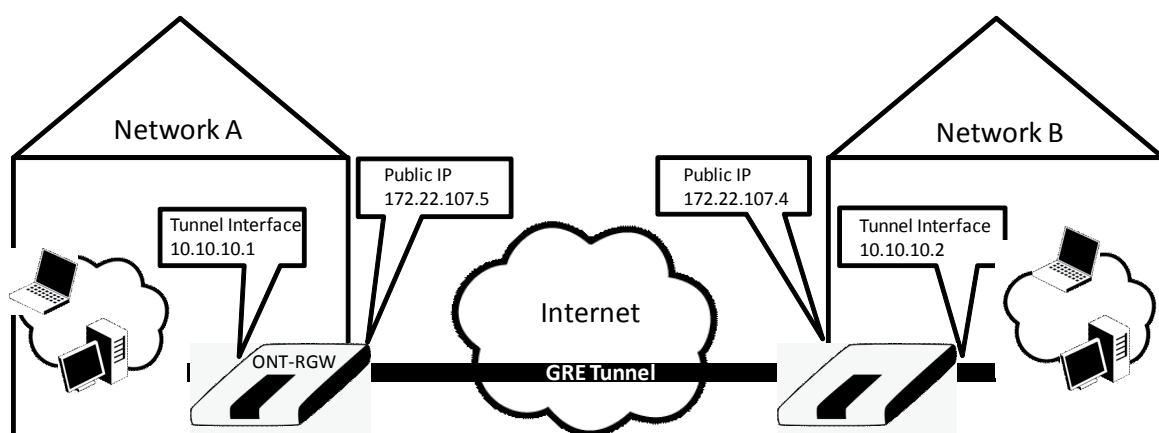


Figure 5-53: GRE Tunnel configuration example at the Network A Refs. 769501-769502

After the selection of the WAN interface associated to the service to create, Figure 5-21 and Figure 5-22, use the Next button at Figure 5-22, to progress to the next WAN Service setup window- Wan service Configuration, Figure 5-54.

At this window execute the following steps:

- STEP 1.** Select the IP over Ethernet (GRE) WAN service type, Figure 5-54.
- STEP 2.** In the Field Service Description enter a string for the service description; the default service description is a string automatically filled in when the type of device is selected (Step1) and composed by the type of Service followed by underscore and the WAN interface name, e.g. gre_veip0.
- STEP 3.** Use the Next button, Figure 5-54, to progress to the WAN Service setup window- GRE Tunneling Settings, Figure 5-55.

In this window two GRE configuration modes are available from a configuration mode combo box selection, ; The detail of the required information for setting the GRE will vary according to the configuration mode selected:

- Basic
- Advanced

WAN Service Configuration

Select WAN service type:

- ☐ PPP over Ethernet (PPPoE)
- ☐ IP over Ethernet
- ☒ GRE Tunneling (over Layer 2)
- ☐ Bridging

Enter Service Description:

Figure 5-54: WAN service setup – type of service selection and service configuration – GRE service

GRE Tunneling Settings

Configuration Mode:

Enable GRE Tunnel ☐

Tunnel Name

Remote IP:

Figure 5-55: WAN Service setup window- GRE Tunneling Settings

5.6.2.3.1 GRE Tunnel Setting – Basic Configuration Mode

In the basic configuration mode only Tunnel Name and Remote IP are required for setting the GRE Tunnel, Figure 5-56. Remote IP is the Public IP address of the routing device terminating the GRE Tunnel in the other extreme of the tunnel (Refs. 769501-769502 of network B in the shown example), Figure 5-53.

GRE Tunneling Settings

Configuration Mode:

Basic

Enable GRE Tunnel

☒

Tunnel Name

xpto

Remote IP:

172.22.107.8

Back

Next

Figure 5-56: WAN Service setup window - GRE Tunneling Settings – Basic configuration mode

After entering the required information, use Next button to progress to the next window, WAN Service setup window- GRE Tunneling Settings – GRE Summary, Figure 5-57. This table should reflect the configuration for the GRE-Tunnel service setup parameters than have been configured. Please verify the presented configuration match the settings provided by the ISP for this service.

WAN Setup - GRE Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	GRE
Local IP:	
Remote IP:	172.22.107.8
Tunnel Name:	gre_xpto
Tunnel IP:	
Peer IP:	
Tunnel Mask:	
TTL:	
Tunnel Mode:	Layer 2

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back

Apply/Save

Figure 5-57: WAN Service setup window- GRE Tunneling Settings – GRE Summary

To finalize the configuration use the Save/Apply button, Figure 5-57. The next displayed window is initial window, the WAN Service Window, where the service configured is displayed in the corresponding table, Figure 5-58.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit	Enable/Disable
veip0.2	ipo_e_veip0.15	IPoE	0	15	0x8100	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit	Disable
ppp0.1	pppoe_veip0.11	PPPoE	0	11	0x8100	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit	Disable

GRE Tunnels Setup

Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Remove	Tunnel Mode	Enable/Disable
gre_xpto		172.22.107.8					<input type="checkbox"/>	Layer 2	Disable

Figure 5-58: WAN Service Setup Initial Window- service configuration displayed

It is now possible to view the currently configured WAN services' parameters as well as obtained IP addresses by Selecting the Device Info sub-menu item WAN, Figure 5-59.

WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Enable/Disable
veip0.2	ipo_e_veip0.15	IPoE	15	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Connected	172.22.107.126	(null)	Enable
ppp0.1	pppoe_veip0.11	PPPoE	11	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	172.22.190.70		Enable

GRE Tunnels Status

Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Tunnel Mode	Status
gre_xpto		172.22.107.8					Layer 2	Enabled

Figure 5-59: Device Info- WAN service Current configuration

5.6.2.3.2 GRE Tunnel Setting – Advanced Configuration Mode

In the Advanced configuration mode the following information is required for setting the GRE Tunnel, Figure 5-56, Figure 5-60, and Table 5-14.

GRE Tunneling Settings

Configuration Mode: Advanced ▼

Enable GRE Tunnel ☒

Tunnel Name:

Remote IP:

Local IP: (optional)

GRE Tunnel IP: (optional)

GRE Peer IP: (optional)

GRE Tunnel Mask: (optional)

TTL: (optional)

Figure 5-60: WAN Service setup window- GRE Tunn

Parameter	Description
Local IP	Public IP address of the routing device where the tunnel is being configured, (Refs. 769501-769502 of network A in the shown example), Figure 5-53.
Remote IP	Public IP address of the routing device terminating the GRE Tunnel in the other extreme of the tunnel (Refs. 769501-769502 of network B in the shown example), Figure 5-53.
Tunnel Name	GRE Tunnel Identification (string)
GRE Tunnel IP	IP address of GRE Tunnel interface, on the routing device being configured (Refs. 769501-769502 of network A in the shown example), Figure 5-53.
GRE Tunnel Mask	IP address of GRE Tunnel interface, on the routing device terminating the GRE Tunnel in the other extreme of the tunnel (Refs. 769501-769502 of network B in the shown example), Figure 5-53.
TTL	Time to Live value

Table 5-14:GRE Tunneling Settings – Advanced configuration mode parameters

After entering the required information, use Next button to progress to the next window, WAN Service setup window- GRE Tunneling Settings – GRE Summary, Figure 5-61. This table should reflect the configuration for the GRE-Tunnel service setup parameters than have been configured. Please verify the presented configuration match the settings provided by the ISP for this service.

WAN Setup - GRE Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	GRE
Local IP:	172.22.107.5
Remote IP:	190.20.20.4
Tunnel Name:	gre_tunnel
Tunnel IP:	10.10.10.1
Peer IP:	10.10.10.2
Tunnel Mask:	255.255.255.0
TTL:	128
Tunnel Mode:	Layer 2

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.







[Back](#) [Apply/Save](#)

Figure 5-61: WAN Service setup window- GRE Tunneling Settings – GRE Summary



To finalize the configuration use the Save/Apply button, Figure 5-61. The next displayed window is initial window, the WAN Service Window, where the service configured is displayed in the corresponding table, Figure 5-62.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit	Enable/Disable
veip0.2	ipoe_veip0.15	IPoE	0	15	0x8100	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled		 Edit	 Disable
ppp0.1	pppoe_veip0.11	PPPoE	0	11	0x8100	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled		 Edit	 Disable

GRE Tunnels Setup

Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Remove	Tunnel Mode	Enable/Disable
gre_tunnel	172.22.107.5	190.20.20.4	10.10.10.1	10.10.10.2	255.255.255.0	128		Layer 2	 Disable



 Add  Remove

Figure 5-62: WAN Service Setup Initial Window- service configuration displayed

It is now possible to view the currently configured WAN services' parameters as well as obtained IP addresses by Selecting the Device Info sub-menu item WAN, Figure 5-63.

WAN Info														
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Enable/Disable
veip0.2	ipoe_veip0.15	IPoE	15	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Connected	172.22.107.126	(null)	Enable
ppp0.1	pppoe_veip0.11	PPPoE	11	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	172.22.190.70		Enable

GRE Tunnels Status									
Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Tunnel Mode	Status	
gre_tunnel	172.22.107.5	190.20.20.4	10.10.10.1	10.10.10.2	255.255.255.0	128	Layer 2	Enabled	

Figure 5-63:Device Info- WAN Service Current configuration

5.6.2.3.3 Interface Grouping for GRE

After the GRE tunnel creation, association between the WAN and the desired interfaces must be done.

At the Advanced Setup menu the item Interface Grouping must be selected. An Interface Grouping Configuration window will be displayed.

An on-line help on interface grouping is available at the configuration window:

- STEP 1.** Name the interfaces group, Figure 5-64, 1;
- STEP 2.** At the Wan interface used in the group selection combo box, select the wan interface for the grouping, in this case the GRE previously configured interfaces, Figure 5-64, 2 and Figure 5-67 To finalize the configuration use the Save/Apply button, Figure 5-65-6. The next displayed window is initial window, the Advanced Setup- Interface grouping initial window where the newly configured group, brgre in this example, Figure 5-67;
- STEP 3.** Figure 5-64; From the list of available WAN interfaces select the desired wan interface, in this example wlan0, Figure 5-66-3;
- STEP 4.** Click on the left pointing arrow, Figure 5-66-4, to move the selected interface (wlan0 in this example) from the Available LAN Interfaces List to the Grouped LAN Interfaces, Figure 5-65-5;
- STEP 5.** Wlan0, the selected interface for interface grouping is now show at the grouped LAN interfaces list, Figure 5-65-5;
- STEP 6.** To finalize the configuration use the Save/Apply button, Figure 5-65-6. The next displayed window is initial window, the Advanced Setup- Interface grouping initial window where the newly configured group, brgre in this example, Figure 5-67.

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Apply/Save button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name: 1 →

WAN Interface used in the grouping 2 →

Grouped LAN Interfaces

wlan0

5 →

->

<-

Available LAN Interfaces

eth0.0
eth2.0
eth3.0
wl0_Guest12GA/wl0.1
wl0_Guest12GA/wl0.2
wl0_Guest12GA/wl0.3

Automatically Add Clients With the following DHCP Vendor IDs

6 →

Figure 5-64: Advanced Setup- interface grouping configuration window

WAN Interface used in the grouping ▼

ipoe_veip0.15/veip0.2

pppoe_veip0.11/ppp0.1

gre_xpto/gre_xpto

No Interface/None

Figure 5-65: Wan interface used in the grouping selection combo box

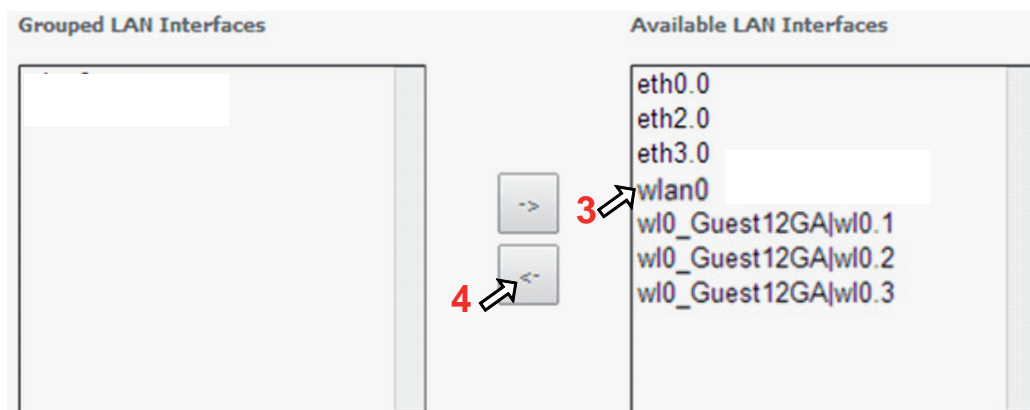


Figure 5-66: Advanced Setup- interface grouping configuration window

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	eth0.0	
		veip0.2	eth2.0	
			eth3.0	
			wlo_Guest12GA wlo.1	
			wlo_Guest12GA wlo.2	
			wlo_Guest12GA wlo.3	
brgre	<input type="checkbox"/>	gre_xpto	wlan0	

Add Remove

Figure 5-67: Advanced Setup- Interface grouping configuration initial Window: Current interface grouping configuration

5.6.2.4 Bridging Service Configuration

After the selection of the WAN interface associated to the service to create, Figure 5-21 and Figure 5-22 , use the Next button at Figure 5-22, to progress to the next WAN Service setup window- Wan service Configuration, figure 5-68.

The image shows a 'WAN Service Configuration' window with the following elements and numbered annotations:

- 1**: Points to the 'Bridging' radio button under 'Select WAN service type:'.
- 2**: Points to the 'Allow as IGMP Multicast Source' checkbox.
- 3**: Points to the 'Enter Service Description' text field containing 'br_veip0'.
- 4**: Points to the 'Enter 802.1P Priority [0-7]' spin box set to '0'.
- 5**: Points to the 'Enter 802.1Q VLAN ID [0-4094]' spin box set to '12'.
- 6**: Points to the 'Select VLAN TPID' dropdown menu set to '0x8100'.
- 7**: Points to the 'Next' button at the bottom right.

Text in the window includes: 'Select WAN service type:', 'PPP over Ethernet (PPPoE)', 'IP over Ethernet', 'GRE Tunneling (over Layer 2)', 'Bridging', 'Allow as IGMP Multicast Source', 'Allow as MLD Multicast Source', 'Enter Service Description: br_veip0', 'For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.', 'Enter 802.1P Priority [0-7]:', 'Enter 802.1Q VLAN ID [0-4094]:', 'Select VLAN TPID:', 'Back', and 'Next'.

Figure 5-68: WAN service setup – type of service selection and service configuration – Bridging service

At this window execute the following steps:

STEP 1. Select the Bridging WAN service type, Figure 5-68-1;

Multicast source options are displayed for selection: IGMP or MLD

STEP 2. Select which multicast source protocol to use, if any, (IGMP or MLD) Figure 5-68-2;

STEP 3. At the Field Service Description enter a string for the service description ; the default service description is a string automatically filled in when the type o device is selected(Step1) and composed by the type of Service followed by underscore and the WAN interface name , e.g. br_veip0, Figure 5-68-3;

STEP 4. For tagged service, at the field 802.1P priority, enter the pbit value (0-7) to mark the upstream traffic according to the desired CoS for the service to create; a higher value corresponds to a higher priority CoS, Figure 5-68-4;

For untagged service leave the filed with the default value of -1;

STEP 5. For tagged service, at the VLAN ID field enter the VLAN ID value (0-4094) of the VLAN used by the service, , Figure 5-68-5

For untagged service leave the field with the default value of -1;

STEP 6. For tagged service select a TPID value from the selection combo box, , Figure 5-68-6.

0x8100, TPID default value; if selected a single tagged service is configured

0x88A8 or 0x9100, TPID used for the outer VLAN (S-VLAN) for double tagged services; if selected a double VLAN tagged service is configured; in this case the inner VLAN (C-VLAN) tag TPID has the default value of 0x8100;

STEP 7. Once the WAN service setup parameters are configured use Next button,, Figure 5-68-7 on to progress to the WAN Service Setup Summary window, Figure 87. This table should reflect the configuration for the WAN service setup parameters than have been entered. Please verify the presented configuration match the settings provided by the ISP for this service.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Enabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

Figure 5-69: WAN Service Setup Summary window

To finalize the configuration use the Save/Apply button, Figure 5-69. The next displayed window is initial window, the WAN Service Window, where the service configured is displayed in the corresponding table, Figure 5-70.

Wide Area Network (WAN) Service Setup															
Choose Add, Remove or Edit to configure a WAN service over a selected interface.															
Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpId	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit	Enable/Disable
veip0.2	ipoe_veip0.15	IPoE	0	15	0x8100	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit	Disable
veip0.3	br_veip0.12	Bridge	0	12	0x8100	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit	Enable/Disable
ppp0.1	pppoe_veip0.11	PPPoE	0	11	0x8100	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit	Disable

GRE Tunnels Setup										
Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Remove	Tunnel Mode	Enable/Disable	
gre_tunnel	172.22.107.5	190.20.20.4	10.10.10.1	10.10.10.2	255.255.255.0	128	<input type="checkbox"/>	Layer 2	Disable	

Add Remove

Figure 5-70: WAN Service Setup Initial Window- service configuration displayed

It is now possible to view the configured WAN service parameters by Selecting the Device Info sub-menu item WAN, Figure 5-71.

WAN Info														
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Enable/Disable
veip0.2	ipoe_veip0.15	IPoE	15	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Connected	172.22.107.126	(null)	Enable
veip0.3	br_veip0.12	Bridge	12	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Connected	0.0.0.0	(null)	Enable
ppp0.1	pppoe_veip0.11	PPPoE	11	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	172.22.190.70		Enable

GRE Tunnels Status								
Tunnel Name	Local IP	Remote IP	Tunnel IP	Peer IP	Tunnel Mask	TTL	Tunnel Mode	Status
gre_tunnel	172.22.107.5	190.20.20.4	10.10.10.1	10.10.10.2	255.255.255.0	128	Layer 2	Enabled

Figure 5-71: Device Info- WAN Service Current configuration and IP Address

Service statistics can be obtained by selecting at the menu Device Info the submenu Statistics, item Wan; a Services-WAN statistics window will be displayed, Figure 5-72. Please refer to Table 5-5 for the description of the statistics window display parameters.

Statistics -- WAN

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
veip0.1	ipoe_veip0.15	23154	234	0	0	0	0	231	3	46296	358	0	0	0	0	358	0
veip0.3	br_veip0.12	588	14	0	0	0	0	13	1	160887	1654	0	0	24309	251	1031	372
ppp0.2	pppoe_veip0.11	195387898	148409	0	0	0	0	148409	0	48682762	87123	0	0	0	0	87123	0

Figure 5-72: Device Info/Statistics/WAN-- WAN Services Statistics Information

5.6.3 LAN

Selection of Advanced Setup submenu item LAN will display a LAN submenu with two items, Figure 5-73:

- Lan VLAN Setting
- IPv6 Autoconfig

In the main window a Local Area Network (LAN) Setup window is displayed, Figure 5-74.

This window allows the configuration Multicast, firewall and DHCP in the LAN.

Device Info
 Advanced Setup
 Layer2 Interface
 WAN Service
 LAN
 LAN Port Config
 Lan VLAN Setting
 LAN LLDP Config
 IPv6 Autoconfig

Figure 5-73: Advanced Setup LAN Sub-menu

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default ▾

1 → IP Address:

2 → Subnet Mask:

3 → ☒ Enable IGMP Snooping

4 → ☐ Standard Mode

5 → ☒ Blocking Mode

Enable IGMP LAN to LAN Multicast: Disable ▾ 6 →

(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

7 → ☐ Enable LAN side firewall

8 → ☐ Disable DHCP Server

9 → ☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

10 →

MAC Address	IP Address	Remove
Add Entries Remove Entries		

11 → ☐ Enable secondary Server (for DHCP Option 60)

12 → Apply/Save

Figure 5-74: Advanced Setup - LAN Setup window

At this window execute the following steps:

STEP 1. IP Address –This is the Refs. 769501-769502 IP Address, default value 192.168.1.1, Figure 5-74-1;

STEP 2. Refs. 769501-769502 sub network Mask ; default value is 255.255.255.0, Figure 5-74-2;

STEP 3. In order to enable IGMP Snooping select this option, Figure 5-74-2;

In the case IGMP snooping is not selected multicast packets are send to all bridge ports. If this option is selected an IGMP Snooping mode must be selected (see step 4 and step 5)

There are two modes of IGMP snooping, that establish the way groups multicast packets are forwarded by the bridge Figure 5-74- 4 and 5:

STEP 4. Standard Mode, Figure 5-74-4,

- Group multicast packets are forwarded to all ports if there was no previous IGMP Group report by any port:
- In the case there were previous IGMP Group reports, multicast packets are only forwarded to the ports that previously send

IGMP group reports.

STEP 5. Blocking mode, Figure 5-74 , 5.

- In this mode multicast packets are only forwarded if there were previous IGMP reports, for the ports that send these reports. Packets are not forwarded if there were no IGMP reports

STEP 6. In order to have a multicast data source on LAN side and IGMP snooping enabled, then LAN-2-LAN multicast option must be enabled, Figure 5-74-6;

LAN-2-LAN multicast is enabled (even if this option is set to disable) until the first WAN service is connected.

STEP 7. This option must be selected in order to enable LAN side firewall; if LAN side firewall is enabled, Figure 5-74-7,

STEP 8. If selected Refs. 769501-769502 DHCP server is disabled, Figure 5-74-8;

STEP 9. If selected Refs. 769501-769502 DHCP server is enabled, Figure 5-74-9; the pool of IP address to use must be defined by indicating:

- start IP address; default value is 192.168.1.2
- end IP addresses; default value is 192.168.1.254
- Leased Time: amount of time (in hours) then the LAN user will be allowed the dynamic IP address that has been allocated to him; default value is 24.

Static IP lease settings allow the reservation of static IPs for PCs in the LAN that will therefore obtain the same static IP address each time they request an IP address from the Refs. 769501-769502 DHCP server . For the Refs. 769501-769502 DHCP Server up to 32 Static IP leases can be configured

STEP 10. To configure static IP leases, Figure 5-74-10, use the Add entries button ;

Each entry will consists of a MAC address of the PC to which the static IP address will be reserved and the Static IP reserved for this PC; enter the MAC address and the reserved IP address for this MAC.

STEP 11. If Option "Enable secondary Sever (for DHCP option 60)" is selected, Figure 5-75, fields requesting information for configuration of this option will be shown (DHCP option 60 is vendor ID);Enabling this option allows to add LAN clients on a WAN interface requesting DHCP with option 60

IP Address: DHCP Server (Refs. 769501-769502) IP Address;

Subnet Mask: Refs. 769501-769502 sub network Mask ; default value is 255.255.255.0;

Start IP address: First IP address to use by DHCP server for allocation;

End IP addresses: Last IP address to use by DHCP server for allocation;

Leased Time: amount of time (in minutes) then the LAN user will be allowed the dynamic IP address that has been allocated to him;

Vendor ID: String identifier for vendor ID (DHCP option 60);

Primary DNS Server: Primary DNS Server IP address;

Secondary DNS server: Secondary DNS Server IP address;

NTP server: NTP server IP Address

TFTP Server: TFTP Server IP Address

11 ☒ Enable secondary Server (for DHCP Option 60)

IP Address:	192.168.5.1
Subnet Mask:	255.255.255.0
Start IP Address:	192.168.5.2
End IP Address:	192.168.5.10
Leased Time (minutes):	10
Vendor ID:	xpto
Primary DNS Server:	192.168.123.123
Secondary DNS Server:	192.168.123.124
NTP Server:	192.168.123.200
TFTP Server:	192.168.123.120

Figure 5-75: Advanced Setup - LAN Setup window- Enable Secondary server (for DHCP Option 60)

STEP 12. To finalize the configuration use the Save/Apply button, Figure 5-74, -12; the displayed window will show the LAN settings current configuration

5.6.3.1 LAN VLAN Settings

Selection of Advanced Setup submenu LAN, item will Lan VLAN Setting a Local Area Network (LAN) VLAN Setup window is displayed in the main window Figure 5-74.

In order to create Lan VLANs, a LAN port must be chosen at the Selection combo box, Figure 5-76.

To create a Lan VLAN use the Add button and at the table entry created, Figure 5-77, type in the:

- VLAN Id : Specifies the VLAN identifier; values from 0 to 4096;
- Pbits: assigned priority value (0-7).

To finalize the configuration use the Save/Apply button, Figure 5-77; the displayed window will show the LAN settings current configuration.

Local Area Network (LAN) VLAN Setup

Select a LAN port:

☐ Enable VLAN Mode

Vlan Id	Pbits	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Apply/Save"/>		

Figure 5-76: Advanced Setup –LAN/ Lan VLAN setup window

Local Area Network (LAN) VLAN Setup

Select a LAN port: eth0/eth0 ▾

☐ Enable VLAN Mode

Vlan Id	Pbits	Remove
<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>

Add Remove Apply/Save

Figure 5-77: Advanced Setup –LAN/ Lan VLAN setup window- Add and configure a Lan VLAN

Lan VLAN can be configured in advance as described before and not enabled. To Enable Lan VLAN afterwards, option “Enable VLAN Mode” must be selected, and then the Save/Apply button used to finalize the configuration.

5.6.3.2 IPv6 Autoconfig

Selection of Advanced Setup submenu LAN, item will IPv6 Autoconfig an IPv6 VLAN Auto Configuration window is displayed in the main window Figure 5-78. A short on line help text is provided in the configuration window.

For a typical IPv6 VAN Auto Configuration setting, shown in Figure 5-78, execute the following Steps, Figure 5-78:

- STEP 1. Select Option “Enable DHCPv6 Server;
- STEP 2. Selectthe option “Stateless”;
- STEP 3. Select the option “Enable RADVD”;
- STEP 4. Select the option “MLD Snooping”;
- STEP 5. Select the option “Blocking Mode”;
- STEP 6. To finalize the configuration use the Save/Apply button


IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

1  ☒ Enable DHCPv6 Server

Prefix Delegation:

2  ☐ Stateless

☒ Stateful

Start interface ID:

End interface ID:

Leased Time (hour):

3  ☒ Enable RADVD

☐ Enable ULA Prefix Advertisement


☐ Randomly Generate

☒ Statically Configure

Prefix:

Preferred Life Time (hour):

Valid Life Time (hour):

4  ☒ Enable MLD Snooping

☐ Standard Mode

5  ☒ Blocking Mode

Enable MLD LAN to LAN Multicast:

Disable ▼

(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

6 

Figure 5-78: Advanced Setup –LAN/ IPv6 VLAN Auto Configuration window

5.6.4 NAT

Selection of Advanced Setup submenu item NAT will display a NAT submenu with three items, Figure 5-79:

- Virtual Servers
- Port Triggering
- DMZ Host

In the main window a NAT-Virtual Servers Setup window is displayed, Figure 5-80, showing the current NAT-Virtual servers configuration.

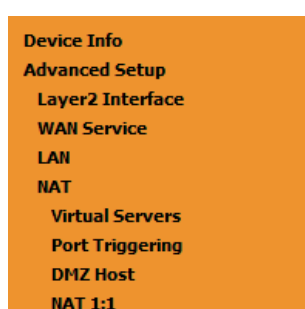


Figure 5-79: Advanced Setup NAT Sub-menu

5.6.4.1 Virtual Servers

Selection of Advanced Setup submenu NAT, item Virtual Servers a NAT-Virtual Servers Setup window is displayed in the main window Figure 5-80, showing the current NAT-Virtual servers configuration.

This window allows inserting and configuring port forwarding, redirecting a network port from one network mode to another network mode. This allows a user from the WAN side of the network to reach a PC on the LAN side of the network for which ports were opened. The WAN interface used must have NAT enabled. A short on line help text is provided in the configuration window.

To insert and configure a new NAT-Virtual server use the Add Button, Figure 5-80; a new window is displayed, Figure 5-81, allowing the configuration of a new Nat- virtual Server entry, Figure 5-82. A short on line help text is provided in the configuration window.

The first part of the configuration consists on choosing the Wan interface, the Service name and the server IP address.

To save and apply this configuration, use the Apply/Save button, Figure 5-81-1. The port forwarding table will be updated with the chosen service predefined port forwarding configuration, Figure 5-81.

To finalize the configuration use the Apply/Save button below the table, Figure 5-81-2. The next displayed window is the initial window, showing the current NAT - virtual servers' configuration, Figure 5-83.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Teredo	51331	51331	UDP	51331	51331	192.168.1.5	ppp0.1	<input type="checkbox"/>

Figure 5-80: Advanced Setup/NAT-Virtual Servers Setup window

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured:31

Use Interface:

Service Name:

☒ Select a Service:

☐ Custom Service:

Server IP Address:

1

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text" value="47624"/>	<input type="text" value="47624"/>	TCP ▼	<input type="text" value="47624"/>	<input type="text" value="47624"/>
<input type="text" value="6073"/>	<input type="text" value="6073"/>	TCP ▼	<input type="text" value="6073"/>	<input type="text" value="6073"/>
<input type="text" value="2300"/>	<input type="text" value="2400"/>	TCP ▼	<input type="text" value="2300"/>	<input type="text" value="2400"/>
<input type="text" value="2300"/>	<input type="text" value="2400"/>	UDP ▼	<input type="text" value="2300"/>	<input type="text" value="2400"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>

2

Figure 5-81: Advanced Setup/NAT-Virtual Servers Setup window - Wan port, Service and Server IP Address Configuration

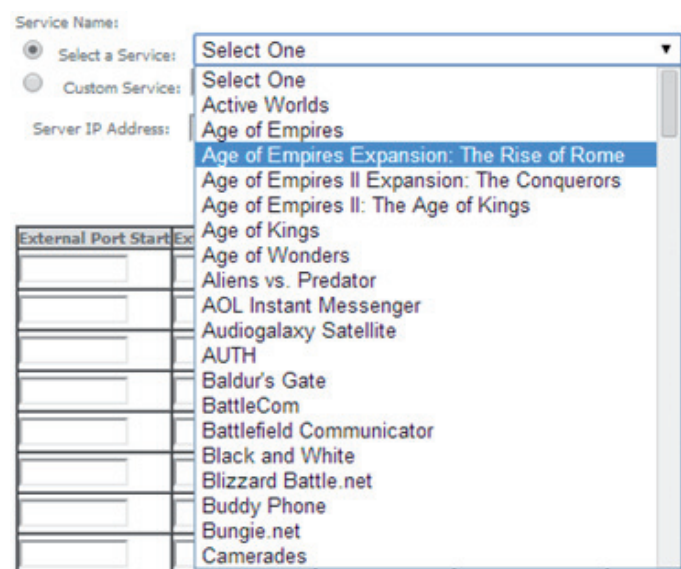


Figure 5-82: Advanced Setup/NAT-Virtual Servers Setup window - Service Selection Combo box

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

AddRemove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Teredo	51331	51331	UDP	51331	51331	192.168.1.5	ppp0.1	<input type="checkbox"/>
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.4	ppp0.1	<input type="checkbox"/>
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.4	ppp0.1	<input type="checkbox"/>
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.4	ppp0.1	<input type="checkbox"/>
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.4	ppp0.1	<input type="checkbox"/>

Figure 5-83: Advanced Setup/NAT-Virtual Servers Setup window - Current NAT Virtual Server Configuration

5.6.4.2 Port Triggering

Selection of Advanced Setup submenu NAT, item Port Triggering, a NAT-Port Triggering Setup window is displayed in the main window Figure 5-84, showing the current NAT- Port Triggering configuration. A short on line help text is provided in the setup window.

This window allows inserting and configuring port triggering, for defined applications. This redirects a network port from one network mode to another network mode. This configuration allows opening ports of a PC in the LAN for a user on the WAN side only when the session on the Lan side is active- this is always initiated by the PC in the network LAN side, being safer then port forwarding.

To insert and configure a new NAT-Port Triggering entry use the Add Button, Figure 5-84; a new window is displayed, Figure 5-85. A short on line help text is provided in the configuration window.

This window allows the configuration of Port Triggering by choosing the Wan interface and the Application Name, Figure 5-85. The WAN interface to use must have NAT enabled.

To apply and save this configuration use the Apply/Save button, below Figure 5-85-1.

The port triggering table will be updated with the chosen application predefined port Triggering configuration, Figure 5-84.

To finalize the configuration use the Apply/Save button below the table, Figure 85-2. The next displayed window is the initial window, showing the current NAT - Port Triggering configuration, Figure 5-86.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Add Remove

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

Figure 5-84: Advanced Setup/NAT-Port Triggering Setup window

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured:32

Use Interface:

Application Name:

- ☒ Select an application:

☐ Custom application:

1 Save/Apply

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
4099	4099	TCP	5191	5191	TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

2 Save/Apply

Figure 5-85: Advanced Setup/NAT-Port Triggering Setup window -Add port triggering for specified application

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger		Open			WAN Interface	Remove	
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	<input type="checkbox"/>

Figure 5-86: Advanced Setup/NAT-Port Triggering Setup window -Current configuration

5.6.4.3 DMZ Host

Selection of Advanced Setup submenu NAT, item DMZ Host, a NAT-DMZ Host Setup window is displayed in the main window Figure 5-87, allowing the DMZ Host configuration by Providing the DMZ Host IP address. A short on line help text is provided in the setup window.

A DMZ Host is a host exposed to the internet. All incoming IP packets from the WAN network side, if not belong to any Service or application configured on the NAT- Virtual server or Port Triggering (for the application) are forwarded to the DMZ Host. DMZ Host must have a static IP address assigned to it.

To finalize the configuration use the Save/ Apply button.

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

Figure 5-87: Advanced Setup/NAT-DMZ Host Setup window

5.6.5 Security

Selection of Advanced Setup submenu item Security will display a Security submenu with two items, Item IP Filtering is a submenu composed of two items, Outgoing and Incoming, Figure 5-88:

- IP Filtering,
 - Outgoing
 - Incoming
- MAC Filtering

EN

In the main window an Outgoing IP Filtering Setup window is displayed, Figure 5-89.

This window allows the creation and configuration a filter rule to identify outgoing IP traffic.



Figure 5-88: Advanced Setup Security Sub-menu5.6.5.1 IP Filtering

Selection of Advanced Setup submenu Security, submenu IP Filtering, will display in the main window, an Outgoing IP filtering Setup window, Figure 5-89, showing the current Outgoing IP Filtering configuration. A short on line help text is provided in the configuration window.

5.6.5.1.1 Outgoing

Selection of Advanced Setup submenu Security, submenu IP Filtering, item Outgoing, an Outgoing IP filtering Setup window is displayed , Figure 5-89, showing the current Outgoing IP Filtering configuration. A short on line help text is provided in the configuration window.

To insert and configure a new Outgoing IP Filter entry use the Add Button, Figure 5-89; a new window is displayed, Figure 108. A short on line help text is provided in the configuration window.

This window allows the configuration of Outgoing IP Filter. Figure 5-90 provides an outgoing filter configuration example

In order to configure the Outgoing IP Filter, Figure 5-90:

- STEP 1.** Enter the Filter name;
- STEP 2.** Select the IP version to use from the IP version selection combo box;
- STEP 3.** Select the Protocol to use from the Protocol Selection combo box;
- STEP 4.** Enter the Source IP address;

- STEP 5. Enter the Source Port;
- STEP 6. Enter the Destination IP address;
- STEP 7. Enter the Destination Port;

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the current Outgoing IP Filtering configuration, Figure 5-91.

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	----------	---------------------	---------	---------------------	---------	--------

Add

Remove

Figure 5-89: Advanced Setup, Security - Outgoing IP filtering Setup window

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

pc_isabel

IP Version:

IPv4

Protocol:

TCP

Source IP address[/prefix length]:

192.168.1.122

Source Port (port or port:port):

80

Destination IP address[/prefix length]:

142.20.23.120

Destination Port (port or port:port):

80

Apply/Save

Figure 5-90:Advanced Setup, Security - Outgoing IP filtering Setup –Add Filter window

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
pc_isabel	4	TCP	192.168.1.122	80	142.20.23.120	80	<input type="checkbox"/>

Add

Remove

Figure 5-91: Advanced Setup, Security - Outgoing IP filtering Setup window –Current Configuration

5.6.5.1.2 Incoming

Selection of Advanced Setup submenu Security, submenu IP Filtering, item Incoming, will display an Incoming IP filtering Setup window, Figure 5-92, showing the current Incoming IP Filtering configuration. A short on line help text is provided in the configuration window.

To insert and configure a new Incoming IP Filter entry use the Add Button, Figure 110; a new window is displayed, Figure 5-93. A short on line help text is provided in the configuration window.

This window allows the configuration of Incoming IP Filter. In order to configure the Incoming IP Filter, Figure 5-93:

EN

- STEP 1.** Enter the Filter name;
- STEP 2.** Select the IP version to use from the IP version selection combo box, Figure 5-94;
- STEP 3.** Select the Protocol to use from the Protocol Selection combo box;
- STEP 4.** Enter the Source IP address;
- STEP 5.** Enter the Source Port;
- STEP 6.** Enter the Destination IP address;
- STEP 7.** Enter the Destination Port;
- STEP 8.** Select the WAN and/or LAN interfaces to apply this rule

Figure 5-95 provides an incoming filter configuration example

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the current Incoming IP Filtering configuration, Figure 5-96.

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is **BLOCKED**. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
aaaaVoiceFilter13c4	veip0.2	6	TCP or UDP				5060:5060	<input type="checkbox"/>

Add Remove

Figure 5-92: Advanced Setup, Security - Incoming IP filtering Setup window- Current Configuration

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☐ Select All ☐ pppoe_veip0.11/ppp0.1 ☐ gre_tunnel/gre_tunnel ☐ br0/br0 ☐ br0:0/br0:0

Figure 5-93: Advanced Setup, Security - Incoming IP filtering Setup – Add Filter window

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

TCP/UDP
TCP
UDP
ICMP

Figure 5-94: Advanced Setup, Security - Incoming IP filtering Setup- Add Filter window – Protocol selection combo box

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☐ Select All ☒ pppoe_veip0.11/ppp0.1 ☐ gre_tunnel/gre_tunnel ☐ br0/br0 ☐ br0:0/br0:0

Figure 5-95: Advanced Setup, Security - Incoming IP filtering Setup- Add Filter window - Configuration exemple

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is **BLOCKED**. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/PrefixLength	SrcPort	DstIP/PrefixLength	DstPort	Remove
xpto	ppp0.1	4	TCP					<input type="checkbox"/>

Add Remove

Figure 5-96: Advanced Setup, Security - Incoming IP filtering Setup window – Current Configuration

5.6.5.2 MAC Filtering

Selection of Advanced Setup submenu Security, item MAC Filtering displays a MAC filtering Setup window, Figure 5-97, showing the current MAC Filtering configuration: Policy and rules.

A short on line help text is provided in the configuration window.

This window allows changing the policy of rules applied: Forwarded/Blocked

If current configuration of policy is forward, all MAC layer frames are forwarded except those matching with any of the specified rules in the MAC filtering rules table.

If current configuration of policy is blocked, all MAC layer frames are blocked except those matching with any of the specified rules in the MAC filtering rules table.

The policy can be changed by selecting the change and afterwards use the Change policy button. The policy table will change the value to the opposite value (from forward to blocked and vice-versa), Figure 5-98.

Changing from one policy to another of an interface will cause all defined rules for that interface to be removed automatically; therefore rules for the new policy have to be created.

To insert and configure a new MAC filtering rule entry use the Add Button, Figure 115; a new window is displayed, Figure 5-99.

This window allows the configuration of MAC Filtering rule. A short on line help text is provided in the configuration window. Figure 5-99 provides an outgoing filter configuration example

In order to configure the MAC Filtering rule, Figure 5-99:

- STEP 1.** Select the Protocol to use from the Protocol Selection combo box;
- STEP 2.** Type in the destination MAC address;
- STEP 3.** Type in the Source MAC address;
- STEP 4.** Select the frame direction from the selection combo box;
- STEP 5.** Select the WAN interfaces from the selection combo box;

To finalize the configuration use the Save/Apply button. The next displayed window is the initial window, showing the current MAC Filtering configuration, Figure 5-100.

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
veip0.3	FORWARD	<input type="checkbox"/>

Change Policy

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

Add Remove

Figure 5-97: Advanced Setup, Security – MAC filtering Setup window

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
veip0.3	FORWARD	<input checked="" type="checkbox"/>

2 Change Policy

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Fra
-----------	----------	-----------------	------------	-----

Add Remove

Interface	Policy	Change
veip0.3	BLOCKED	<input type="checkbox"/>

Change Policy

Figure 5-98: Advanced Setup, Security – MAC filtering Setup window –Change policy

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Figure 5-99: Advanced Setup, Security – MAC filtering – Add MAC Filter window

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
veip0.3	BLOCKED	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
veip0.3	IGMP	84:3a:4b:14:b2:92	84:3a:4b:14:b5:22	BOTH	<input type="checkbox"/>

Figure 5-100: Advanced Setup, Security – MAC filtering Setup window –Current Configuration

5.6.6 Parental Control

Selection of Advanced Setup submenu item Parental Control will display a Parental Control submenu with two items, Figure 5-101:

- Time Restriction,
- Url Filter

In the main window an Access time Restriction Configuration window is displayed, Figure 5-102.

This window allows the creation and configuration Access Time Restriction Rules.

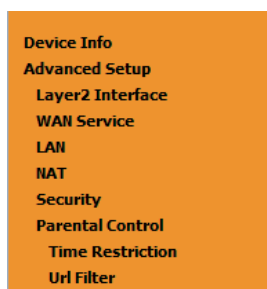


Figure 5-101: Advanced Setup Parental Control Sub-menu

5.6.6.1 Time Restriction

Selection of Advanced Setup submenu Parental Control, item Time Restriction will display an Access Time Restriction configuration window showing the current Access Time Restriction configuration table, Figure 5-102.

A short on line help text is provided in the configuration window.

To insert and configure a new Access Time Restriction rule use the Add Button, Figure 5-102; a new window is displayed, Figure 5-103. A short on line help text is provided in the configuration window. Figure 5-103. Provides a configuration example for an Access Time Restriction rule.

In order to setup a new Access Time Restriction rule, Figure 5-103:

- STEP 1.** Enter the user name;
- STEP 2.** Enter the Browser's MAC address;
- STEP 3.** Select the week days to apply the restriction;
- STEP 4.** Enter the Start Blocking time;
- STEP 5.** Enter the End Blocking time;

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the current Access Time Restriction configuration, Figure 5-104.

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<div> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>											

Figure 5-102: Advanced Setup, Parental Control – Time Restriction Configuration window

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

☒ Browser's MAC Address
☐ Other MAC Address
(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Figure 5-103: Advanced Setup, Parental Control, Time Restriction -Add Time Restriction rule window

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
carla	64:27:37:76:23:1e	x	x	x	x	x			21:0	22:0	<input type="button" value="Remove"/>
<div> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>											

Figure 5-104: Advanced Setup, Parental Control – Time Restriction Configuration window - Current configuration

5.6.6.2 URL Filter

Selection of Advanced Setup submenu Parental Control, item Url Filter will display an URL Filter configuration window showing the current URL Filter configuration table, Figure 5-105. This window allows the creation and configuration of an URL Filter list.

A short on line help text is provided in the configuration window Figure 5-105.

To create a URL filter list the URL list Type to create must be defined as Exclude or Include, Figure 5-105.

To create a new entry in the URL filter list, use the Add button, Figure 123; an URL Filter Add window will be displayed, Figure 5-106.

In this window enter the URL address. Default port number 80 will be used if Port number entry is left blank.

To finalize the add URL entry to the URL filter list use the Apply/Save button, Figure 124. The next displayed window is the initial window, showing the current URL Filter configuration, Figure 5-107.

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ☒ Exclude ☐ Include

Address	Port	Remove
---------	------	--------

Figure 5-105: Advanced Setup, Parental Control – URL Filter Configuration window

Parental Control -- URL Filter Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

Figure 5-106: Advanced Setup, Parental Control – URL Filter – Add Filter window

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ☒ Exclude ☐ Include

Address	Port	Remove
http://www.facebook.com	80	<input type="checkbox"/>

Figure 5-107: Advanced Setup, Parental Control – URL Filter Configuration window- Current Configuration

5.6.7 Quality of Service

Selection of Advanced Setup submenu item Quality of Service will display a Quality of Service submenu with two items, Figure 5-108:

- QoS Queue,
- QoS Classification

This Submenu allows QoS configuration. It is assumed that the Refs. 769501-769502 has the following services already configured: IPoE with NAT and PPPoE services.

EN

In the main window a QoS Queue Management Configuration window will be displayed, Figure 5-109

QoS is disabled by default - it must be enabled by selecting the Enable QoS option, Figure 5-109. Default DSCP mark can be selected from a selection combo box, Figure 5-110. Use the button Apply/Save to apply this configuration and progress to the next window,



Figure 5-108: Advanced Setup Quality of Service Sub-menu

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☒ Enable QoS

Select Default DSCP Mark No Change(-1) ▼

Apply/Save

Figure 5-109: Advanced Setup Quality of Service -Queue Management Configuration

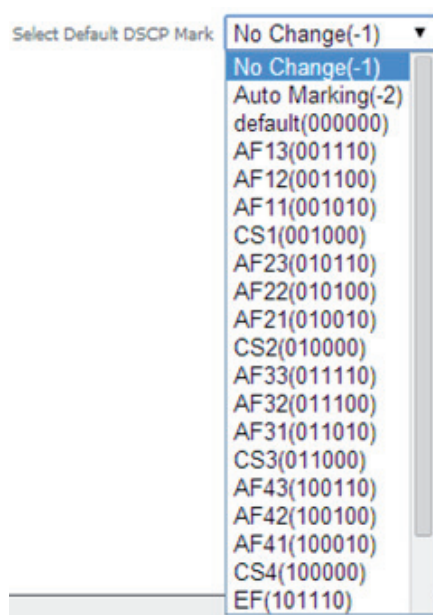


Figure 5-110: Advanced Setup Quality of Service- Queue Management Configuration- Select Default DSCP mark combo box

5.6.7.1 QoS Queue

Selection of Advanced Setup submenu Quality of Service, item QoS Queue will display a QoS Queue Setup Configuration window, Figure 5-111.

This window displays the current QoS configured queues.

A short on line help text is provided in the configuration window.

To insert and configure a new QoS queue entry use the Add Button, Figure 5-111; a new window is displayed, Figure 5-112. A short on line help text is provided in the configuration window. Figure 5-113 provides a configuration example.

In order to configure a new QoS queue, Figure 5-113:

- STEP 1.** Enter the QoS queue name;
- STEP 2.** Select Enable/Disable from the Enable selection combo box; a queue configured as disable can be later on enabled at the current QoS queue configuration window, Figure 5-114 and Figure 5-118
- STEP 3.** Select the Interface for the QoS queue from a selection combo box;
- STEP 4.** Select the queue precedence from a selection combo box;

The Lower is the selected value for queue precedence the higher is the priority; along with the precedence level, the scheduler algorithm for each precedence level is show; queues with the same precedence will bw scheduled based on the algorithm; queues with unequal precedence will be scheduled based on SP (Strict Priority).

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the current Access QoS queue configuration, Figure 5-114.

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.

For each Ethernet interface, maximum 8 queues can be configured.

For each Ethernet WAN interface, maximum 8 queues can be configured.

To add a queue, click the **Add** button.

To remove queues, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the queue after page reload.

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	Min Bit Rate(bps)	Enable	Remove
WMM Voice Priority	1	wl0	8	1/SP		Enabled	
WMM Voice Priority	2	wl0	7	2/SP		Enabled	
WMM Video Priority	3	wl0	6	3/SP		Enabled	
WMM Video Priority	4	wl0	5	4/SP		Enabled	
WMM Best Effort	5	wl0	4	5/SP		Enabled	
WMM Background	6	wl0	3	6/SP		Enabled	
WMM Background	7	wl0	2	7/SP		Enabled	
WMM Best Effort	8	wl0	1	8/SP		Enabled	

Add **Enable** **Remove**

Figure 5-111: Advanced Setup Quality of Service- QoS Queue Setup

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface

Name:

Enable:

Interface:

Figure 5-112: Advanced Setup Quality of Service- QoS Queue Configuration

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)

- The precedence list shows the scheduler algorithm for each precedence level.
- Queues of equal precedence will be scheduled based on the algorithm.
- Queues of unequal precedence will be scheduled based on SP.

Figure 5-113: Advanced Setup Quality of Service- QoS Queue enable example configuration

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.

For each Ethernet interface, maximum 8 queues can be configured.

For each Ethernet WAN interface, maximum 8 queues can be configured.

To add a queue, click the **Add** button.

To remove queues, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the queue after page reload.

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	Min Bit Rate(bps)	Enable	Remove
WMM Voice Priority	1	wl0	8	1/SP		Enabled	
WMM Voice Priority	2	wl0	7	2/SP		Enabled	
WMM Video Priority	3	wl0	6	3/SP		Enabled	
WMM Video Priority	4	wl0	5	4/SP		Enabled	
WMM Best Effort	5	wl0	4	5/SP		Enabled	
WMM Background	6	wl0	3	6/SP		Enabled	
WMM Background	7	wl0	2	7/SP		Enabled	
WMM Best Effort	8	wl0	1	8/SP		Enabled	
xyz_o	38	eth2	6	3/SP		<input type="checkbox"/>	<input type="checkbox"/>

Figure 5-114: Advanced Setup Quality of Service- QoS Queue Setup window- current configuration

5.6.7.2 QoS Classification

Selection of Advanced Setup submenu Quality of Service, item QoS Classification will display a QoS Classification Setup window Figure 5-115.

A short on line help text is provided in the configuration window.

To insert and configure a new QoS classification rule use the Add Button, Figure 5-115; a new window is displayed, Figure 5-116. A short on line help text is provided in the configuration window.

In order to configure a new QoS classification rule, Figure 5-113 (not all the configuration fields are mandatory):

STEP 1. Enter the Traffic class name;

STEP 2. Select the rule order from the selection combo box;

STEP 3. Select the rule status (enable/disable) from the selection combo box; a rule status configured as disable can be later on enabled at the current QoS classification configuration window, Figure 5-117 and Figure 5-118

Specify the classification criteria

STEP 4. Select the class interface from the selection combo box;

STEP 5. Select the Ether Type from the selection combo box;

STEP 6. Enter the Source MAC address;

STEP 7. Enter the Source MAC mask;

STEP 8. Enter the Destination MAC address;

STEP 9. Enter the Destination MAC mask;

Specify Classification Results

STEP 10. Specify the Class Queue;

STEP 11. Specify the Mark Differentiated Service Code (DSCP)

STEP 12. Specify the Mark 802.1p Priority

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the current QoS Classification configuration, Figure 5-117.

EN

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.

To remove rules, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the rule after page reload.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS				
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Enable	Remove

Figure 5-115: Advanced Setup Quality of Service- QoS Classification Setup window

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:

Ether Type:

802.1p Priority Check:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.

- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.

- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.

- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Figure 5-116: Advanced Setup Quality of Service- QoS Classification – Add Network Traffic Class Rule Window –configuration exemple

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.

To remove rules, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the rule after page reload.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS				
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Enable	Remove

xpto_2	1	eth2	8021Q									0	1	auto	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
--------	---	------	-------	--	--	--	--	--	--	--	--	---	---	------	---	-------------------------------------	--------------------------

Figure 5-117: Advanced Setup Quality of Service- QoS Classification Setup window- Current Configuration

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.

For each Ethernet interface, maximum 8 queues can be configured.

For each Ethernet WAN interface, maximum 8 queues can be configured.

To add a queue, click the **Add** button.

To remove queues, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the queue after page reload.

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	Min Bit Rate(bps)	Enable	Remove
WMM Voice Priority	1	wl0	8	1/SP		Enabled	
WMM Voice Priority	2	wl0	7	2/SP		Enabled	
WMM Video Priority	3	wl0	6	3/SP		Enabled	
WMM Video Priority	4	wl0	5	4/SP		Enabled	
WMM Best Effort	5	wl0	4	5/SP		Enabled	
WMM Background	6	wl0	3	6/SP		Enabled	
WMM Background	7	wl0	2	7/SP		Enabled	
WMM Best Effort	8	wl0	1	8/SP		Enabled	
xyz_o	38	eth2	6	3/SP		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add **Enable** **Remove**

Figure 5-118: Advanced Setup Quality of Service- QoS Queue Setup window- current configuration-Queue Enable

5.6.8 Routing

Selection of Advanced Setup submenu item Routing will display a Routing submenu with six items, Figure 5-119:

- Default Gateway,
- Static Routing,
- BGP,
- Policy Routing,
- RIP/OSFP.

In the main window a Routing-Default Gateway Configuration window will be displayed, Figure 5-120.

Device Info
 Advanced Setup
 Layer2 Interface
 WAN Service
 LAN
 NAT
 Security
 Parental Control
 Quality of Service
 Routing
 Default Gateway
 Static Route
 BGP
 LDP
 Policy Routing

Figure 5-119: Advanced Setup Routing Sub-menu

5.6.8.1 Default Gateway

Selection of Advanced Setup submenu Routing, item Default Gateway will display a Routing-Default Gateway configuration window, Figure 5-120.

A short on line help text is provided in the configuration window.

The Routing Default Gateway configuration window presents two lists:

- **Selected Default Gateway Interfaces:** the WAN interfaces that can be used as default gateway interfaces are listed here; only one interface will be used as default gateway interface- this interface will be the highest priority interface of the connected WAN interfaces in this list;

WAN interface priority is based on its position on the list, the first one of the list being the highest priority interface.

To change WAN interface priority, its position in the list must be changed; that can be achieved by removing all from the Selected Default Gateway Interfaces list and adding them back in the desired order.

- **Available Routed WAN Interfaces:** all defined available routed WAN interfaces are listed here; these interfaces can be moved to the Selected Default Gateway interfaces list

If there is only one WAN interface defined in the system, as in the example presented, this will be selected by the system as the default gateway interface thus being presented in the selected default gateway list on the left.

If more WAN interfaces are shown in the list on the right (available routed WAN interfaces) one or more can be moved to the list on the left and be selectable as default gateway routed interface according to its priority in the list.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

ppp0.1



Available Routed WAN Interfaces

veip0.2
gre_tunnel

TODO: IPV6 ***** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface **gre_tunnel/gre_tunnel ▼**

Apply/Save

Figure 5-120: Advanced Setup, Routing-Default Gateway Configuration window

Use the Select WAN Interface selection combo box Figure 5-120, to choose a preferred wan interface as the System default IPv6 gateway.

To finalize the configuration use the Apply/Save button.

5.6.8.2 Static Routing

Selection of Advanced Setup submenu Routing, item Static Routing will display a Routing-Static Route configuration window, Figure 5-121.

This window displays the current static routing configuration and allows the insertion/removal of static routes.

A short on line help text is provided in the configuration window.

To insert and configure a new Static Route use the Add Button, Figure 5-121; a new window is displayed, Figure 5-122. A short on line help text is provided in the configuration window.

In order to configure the new static route, Figure 5-121:

- STEP 1.** Select the IP version from the selection combo box;
- STEP 2.** Enter the Destination IP address /prefix length;
- STEP 3.** Select the Interface from the selection combo box;
- STEP 4.** Enter the metric value (optional)

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the current Static Routing configuration, Figure 5-122.

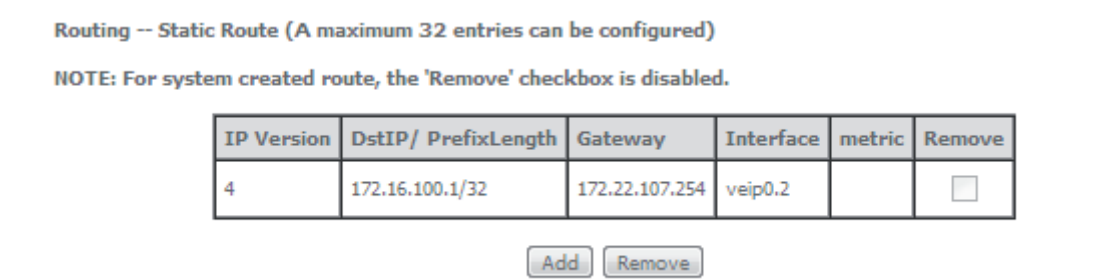


Figure 5-121: Advanced Setup, Static Routing-Configuration window

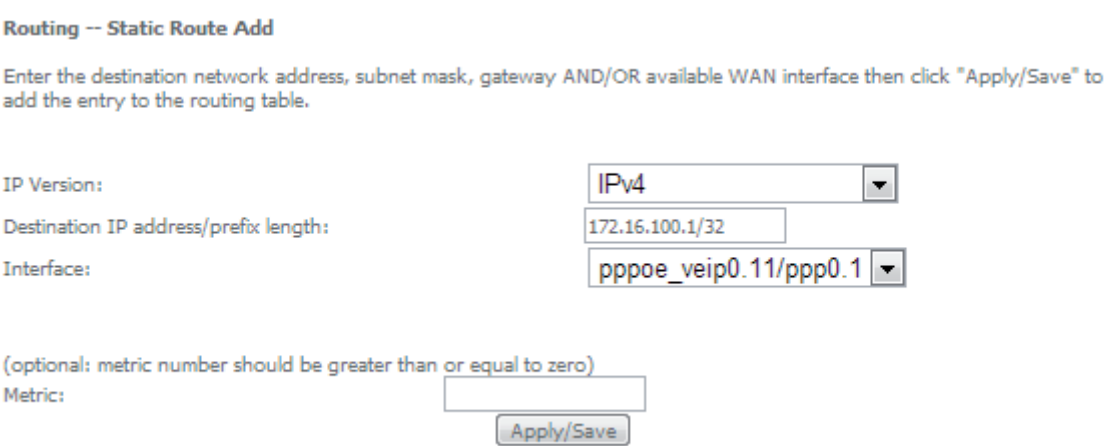


Figure 5-122: Advanced Setup, Routing- Static Route Add window

Routing -- Static Route (A maximum 32 entries can be configured)

NOTE: For system created route, the 'Remove' checkbox is disabled.

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
4	172.16.100.1/32		ppp0.1		<input type="checkbox"/>
4	172.16.100.1/32	172.22.107.254	veip0.2		<input type="checkbox"/>

EN

Figure 5-123: Advanced Setup, Static Routing-Configuration window- Current configuration

5.6.8.3 BGP

Selection of Advanced Setup submenu Routing, item BGP will display a Routing-BGP configuration window, Figure 5-124. This window allows the configuration of the:

- BGP router,
- Neighbors,
- Networks.

A short on line help text is provided in the configuration window.

To be able to configure the BGP router you must have the following information on the router parameters:

- Autonomous System Number (Number: 0 to 65535)
- Router ID (Optional) - IP address of one of the router interfaces

In order to configure the BGP Router, Figure 5-124:

- STEP 1.** Select the Enable BGP option;
- STEP 2.** Type in the Autonomous System Number;
- STEP 3.** Type in the Router ID (optional)

To finalize the BGP Router configuration use the Apply/Save button.

In order to configure the Neighbors, at the neighbors configuration table, Figure 5-124:

- STEP 1.** Type in the Neighbor IP address;
- STEP 2.** Type in the Neighbor Autonomous System (the Remote AS column);
- STEP 3.** Use the Add Entry button; a new line will be added to the table under the entered neighbor configuration.

To finalize the Neighbor configurations use the Add Entry button; the neighbor just configured is now shown at the table and a new line is added.

If the configured Neighbor is announcing BGP routes, these are added to the system and can be viewed at the Device Info menu, item Route window, Figure 5-125.

For the configured neighbors a selection box under the Remove column allows the removal of neighbors.

In order to remove a neighbor from the table:

STEP 1. For the neighbor to remove, select the box under the remove column;

STEP 1. Use the Remove entries button; the selected neighbor is removed from the table

A removed neighbor the learned routes associated to this neighbor are eliminated from the system and are no longer visible at the Device Info menu, item, Route.

To be able to configure the networks to announce you must have the following information on the Network parameters:

- Network IP Address,
- Network Mask.

In order to configure the Networks to announce the, at the networks configuration table, Figure 5-124:

STEP 1. Type in Network address/Mask;

To finalize the Network configuration use the Add Entry button; the network just configured is now shown at the table and a new line is added.

For the configured networks a selection box under the Remove column allows the removal of networks.

In order to remove a network from the table:

STEP 1. For the network to remove, select the box under the remove column;

STEP 2. Use the Remove entries button; the selected network is removed from the table

A removed Network is no longer announced to the neighbors.

Routing -- BGP Configuration

BGP router configuration

Enable BGP



AS Number:

1

Router ID:

10.10.10.1

Neighbors Configuration

IP Address	Remote AS	Remove
10.10.10.2	2	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Add Entry

Remove Entries

Networks Configuration

Net Address	Remove
20.20.20.1/24	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>

Add Entry

Remove Entries

Apply/Save

Figure 5-124: Advanced Setup, Routing- BGP Configuration window

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
0.0.0.0	172.22.107.254	0.0.0.0	UG	0	ipoe_veip0.10	veip0.1
172.22.8.0	172.22.107.254	255.255.255.0	UG	0	ipoe_veip0.10	veip0.1
172.22.9.1	172.22.107.254	255.255.255.255	UGH	0	ipoe_veip0.10	veip0.1
172.22.9.254	172.22.107.254	255.255.255.255	UGH	0	ipoe_veip0.10	veip0.1
172.22.10.0	172.22.107.254	255.255.255.0	UG	0	ipoe_veip0.10	veip0.1
172.22.11.0	172.22.107.254	255.255.255.0	UG	0	ipoe_veip0.10	veip0.1
172.22.11.110	172.22.107.254	255.255.255.255	UGH	0	ipoe_veip0.10	veip0.1
172.22.11.111	172.22.107.254	255.255.255.255	UGH	0	ipoe_veip0.10	veip0.1
172.22.11.112	172.22.107.254	255.255.255.255	UGH	0	ipoe_veip0.10	veip0.1
172.22.12.0	172.22.107.254	255.255.255.0	UG	0	ipoe_veip0.10	veip0.1
172.22.55.0	172.22.107.254	255.255.255.0	UG	0	ipoe_veip0.10	veip0.1
172.22.56.0	172.22.107.254	255.255.255.0	UG	0	ipoe_veip0.10	veip0.1
172.22.58.0	172.22.107.254	255.255.255.0	UG	0	ipoe_veip0.10	veip0.1
172.22.69.0	172.22.107.254	255.255.255.0	UG	0	ipoe_veip0.10	veip0.1
172.22.107.0	0.0.0.0	255.255.255.0	U	0	ipoe_veip0.10	veip0.1

Figure 5-125: Device Info -Route information window – example of BGP routes announced

5.6.8.4 Policy Routing

Selection of Advanced Setup submenu Routing, item Policy Routing will display a Policy Routing Setting window, Figure 5-126.

This window displays the current Policy routing configuration and allows the insertion/removal of new Policy routing rules.

A short on line help text is provided in the configuration window.

To insert and configure a new Policy routing rule use the Add Button, Figure 5-126; a new window is displayed, Figure 144. A short on line help text is provided in the configuration window.

In order to configure the new Policy Routing rule, Figure 5-127:

- STEP 1. Enter the policy name;
- STEP 1. Select the Physical LAN port from the selection combo box;
- STEP 1. Enter the Source IP address;
- STEP 1. Select the Use Interface from the WAN selection combo box;
- STEP 1. If the selected interface is "IPoE", enter the default gateway IP.

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the current Policy Routing configuration, Figure 5-128.



Figure 5-126: Advanced Setup, Routing- Policy Routing Setting window

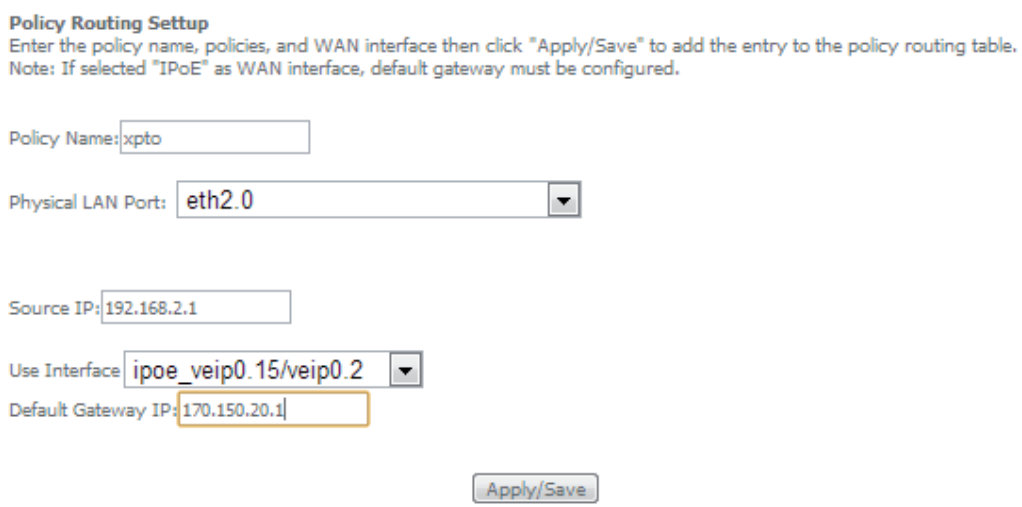


Figure 5-127: Advanced Setup, Routing- Policy Routing Setting – Add and configure Policy window

Policy Routing Setting -- A maximum 7 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
xpto	192.168.2.1	eth2.0	veip0.2	170.150.20.1	<input type="checkbox"/>

Figure 5-128: Advanced Setup, Routing- Policy Routing Setting window- current configuration

5.6.8.5 RIP/OSPF

Selection of Advanced Setup submenu Routing, item RIP/OSPF will display a Routing-RIP Configuration window, Figure 5-129.

This window allows the configuration of the:

- RIP
- OSPF

A short on line help text is provided in the configuration window.

Figure 5-130 provides a RIP and OSPF configuration example.

In order to configure RIP for the WAN Interface, Figure 5-130:

STEP 1. Select the desired RIP version at the column "Version" from the combo box

STEP 2. Select the desired operation mode at the column "Operation" from the combo box;

If the selected interface has NAT enabled, the only operation mode that can be configured is Passive;

STEP 3. At the column enabled select the Enabled checkbox

To finalize the RIP configuration use the Apply/Save button at the bottom of the window.

In order to configure and activate the OSPF, at the OSPF configuration table, Figure 5-130:

Note: OSPF cannot be configured on the WAN interface which has NAT enabled (such as PPPoE)

STEP 1. Select the option Enabled OSPF;

STEP 2. Type in the Router IP address at the box Router id;

STEP 3. Type in the Network IP address and Mask;

STEP 4. Type in the OSPF area ID at the Area ID column;

To finalize the OSPF configuration use the Apply/Save button at the bottom of the window.

To add a new OSPF configuration, use the Add Entry button; a new line is added to the table.

For the configured OSPF a selection box under the Remove column allows the removal of OSPF configuration.

In order to remove an OSPF configuration from the table:

- STEP 1.** For the OSPF configuration to remove, select the checkbox under the remove column;
- STEP 2.** Use the Remove button; the selected OSPF configuration is removed from the table

Routing -- RIP Configuration

NOTE: If selected interface has NAT enabled, only Passive mode is allowed.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
veip0.2	2	Passive	<input type="checkbox"/>

Routing -- OSPF Configuration

NOTE: OSPF CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate OSPF dynamic routing, place a check in the 'Enabled' checkbox. To stop OSPF, uncheck the 'Enabled' checkbox. Click the 'Add' or 'Remove' button to add or remove OSPF Areas and Networks. Click the 'Apply/Save' button to star/stop OSPF and save the configuration.

☐ Enabled OSPF

Router-id: 0.0.0.0

Network [IP/mask]	Area ID	Remove
		<input type="checkbox"/>

AddRemove

Apply/Save

Figure 5-129: Advanced Setup, Routing- RIP and OSPF Configuration window

Routing -- RIP Configuration

NOTE: If selected interface has NAT enabled, only Passive mode is allowed.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to start/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
veip0.2	2	Passive	<input checked="" type="checkbox"/>

Routing -- OSPF Configuration

NOTE: OSPF CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate OSPF dynamic routing, place a check in the 'Enabled' checkbox. To stop OSPF, uncheck the 'Enabled' checkbox. Click the 'Add' or 'Remove' button to add or remove OSPF Areas and Networks. Click the 'Apply/Save' button to start/stop OSPF and save the configuration.

☒ Enabled OSPF

Router-id:

Network [IP/mask]	Area ID	Remove
<input type="text" value="10.10.10.1/24"/>	<input type="text" value="2"/>	<input type="button" value="Remove"/>

Figure 5-130: Advanced Setup, Routing- RIP and OSPF Configuration example

5.6.9 DNS

Selection of Advanced Setup submenu item DNS will display a DNS submenu with two items, Figure 5-131:

- DNS Server,
- Dynamic DNS.

In the main window a DNS Server Configuration window will be displayed, Figure 5-132.



Figure 5-131: Advanced Setup DNS Sub-menu

5.6.9.1 DNS Server

Selection of Advanced Setup submenu DNS, item DNS Server will display a DNS Server configuration window, Figure 5-132.

A short on line help text is provided in the configuration window.

The DNS Server configuration window presents two lists:

- **Selected DNS Server Interfaces:** the WAN interfaces that can be used as DNS Server interfaces are listed here; only one interface will be used as DNS Server interface- this interface will be the highest priority interface of the connected WAN interfaces in this list;

WAN interface priority is based on its position on the list, the first one of the list being the highest priority interface.

To change WAN interface priority, its position in the list must be changed; that can be achieved by removing all from the Selected DNS server Interfaces list and adding them back in the desired order.

- **Available WAN Interfaces:** all defined available WAN interfaces are listed here; these interfaces can be moved to the Selected DNS Server interfaces list

Figure 5-132 provides a DNS Server Configuration example;

In order to configure DNS server, Figure 5-132:

- STEP 1.** Select the option "Select DNS Server Interface from available WAN Interfaces " to use one of the available WAN interfaces as the DNS server interface:
- STEP 2.** Select the WAN interface to use from the available Wan interfaces list on the right and move it to the Selected DNS Server Interfaces list on the left;
- STEP 3.** If Static DNS IP address is to be used select this option in the window and Type in the DNS primary and secondary IP addresses; otherwise go to the following step;
- STEP 4.** To obtain IPv6 DNS info from a WAN interface Select this option and choose the WAN interface from the selection combo box;
- STEP 5.** If Static DNS IPv6 address is to be used select this option in the window and Type in the DNS primary and secondary IPv6 addresses;

To finalize the configuration use the Apply/Save button.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces		Available WAN Interfaces
ppp0.1	<div style="text-align: center;"> <div style="border: 1px solid #ccc; padding: 2px 10px; margin: 2px;">→</div> <div style="border: 1px solid #ccc; padding: 2px 10px; margin: 2px;">←</div> </div>	veip0.2 gre_tunnel

☐ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

TODO: IPV6 ***** Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

☒ **Obtain IPv6 DNS info from a WAN interface:**

WAN Interface selected:

☐ **Use the following Static IPv6 DNS address:**

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Figure 5-132: Advanced Setup, DNS Server Configuration Window

5.6.9.2 Dynamic DNS

Selection of Advanced Setup submenu DNS, item Dynamic DNS will display a Dynamic DNS configuration window, Figure 5-133.

This window displays the current Dynamic DNS configuration.

A short on line help text is provided in the configuration window.

To insert and configure a new Dynamic DNS entry use the Add Button, Figure 5-133; a new window is displayed, Figure 5-134. A short on line help text is provided in the configuration window. Figure 5-134 provides a configuration example.

In order to configure a new Dynamic DNS entry, Figure 5-134:

- STEP 1.** Select the Dynamic DNS provider from the D-DNS provider selection combo box;
- STEP 2.** Type in the Hostname;
- STEP 3.** Select the Interface from the selection combo box;

- STEP 4.** At the DynDNS Settings type in the username;
- STEP 5.** At the DynDNS Settings type in the Password;

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the current Access Dynamic DNS configuration, Figure 5-135.

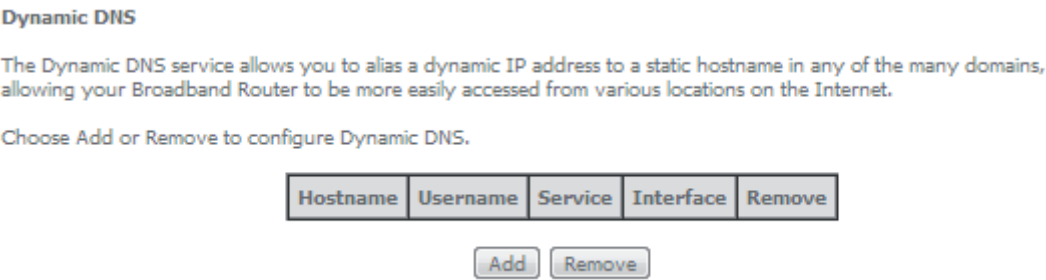


Figure 5-133: Advanced Setup, DNS-Dynamic DNS Configuration window

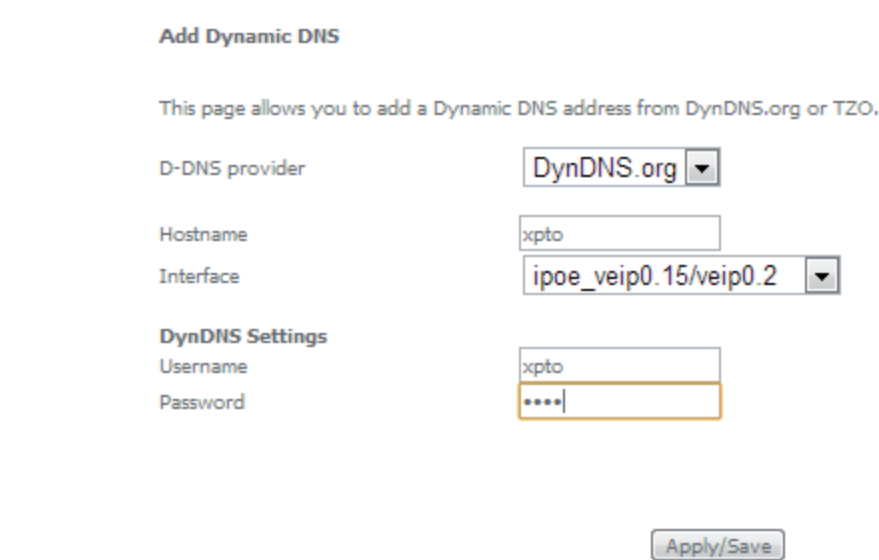


Figure 5-134: Advanced Setup, DNS-Add Dynamic DNS window

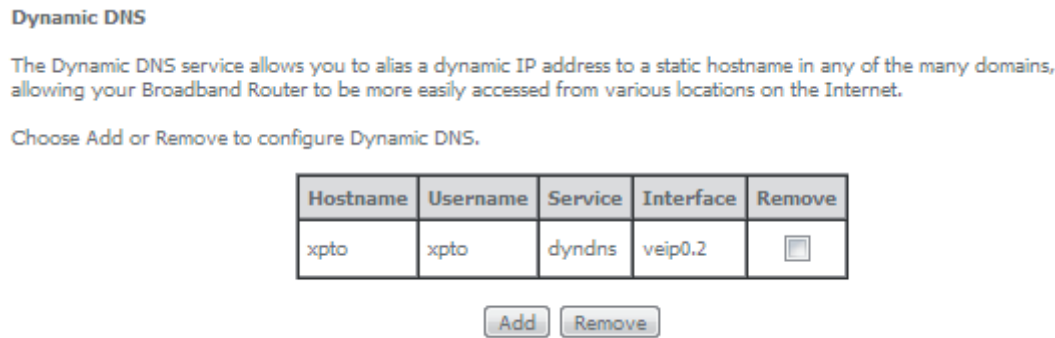


Figure 5-135: Advanced Setup, DNS-Dynamic DNS Configuration window-current configuration

5.6.10 UPnP

Selection of Advanced Setup submenu item UPnP will display a UPnP Configuration window, Figure 5-136.

To enable UPnP select the option “Enable UPnP” and use the Apply/Save button to finalize de configuration.

Note: UPnP is activated only where there is a live WAN service with NAT enabled.

UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☒ Enable UPnP

Apply/Save

Figure 5-136: Advanced Setup, UPnP Configuration Window

5.6.11 DNS Proxy

Selection of Advanced Setup submenu item DNS Proxy will display a DNS proxy Configuration window, Figure 5-137.

To configure DNS Proxy:

STEP 1. Select the option “Enable DNS Proxy”

STEP 2. Type in the Host name of the RGW Router;

STEP 3. Type in the Domain name of the LAN network;

To finalize de configuration use the Apply/Save button.

DNS Proxy Configuration

☒ Enable DNS Proxy

Host name of the RGWRouter:

ONT-RGW

Domain name of the LAN network:

Home

Apply/Save

Figure 5-137:Advanced Setup, DNS Proxy Configuration window

5.6.12 Storage Service

Selection of Advanced Setup submenu item Storage Service will show A Storage Device Info submenu item, Figure 5-138 and display a Storage Service Device Information window, Figure 5-139

This window displays information on the current Storage connected to the USB Ports.



Figure 5-138:Advanced Setup Storage Service Sub-menu

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volumename	FileSystem	Total Space	Used Space
usb1_1	fat	1919	1621

Figure 5-139: Advanced Setup Storage Service configuration window

5.6.13 Interface Grouping

Selection of the Advanced Setup menu item Interface Grouping will display an Interface Grouping Configuration window, Figure 5-140. This window allows establishing an association between a WAN interface and desired LAN interfaces.

An on-line help on interface grouping is available at the configuration window:

Figure 5-140 provides an interface grouping example.

In order to setup an interface grouping, execute the following steps, Figure 5-140:

- STEP 1.** Name the interfaces group, Figure 5-140-1
- STEP 2.** At the Wan interface used in the group selection combo box, select the wan interface for the grouping, Figure 5-140-2;
- STEP 3.** From the list of available WAN interfaces select the desired wan interface, in this example wlan0, Figure 5-140-3
- STEP 4.** Click on the left pointing arrow, Figure 5-141-4, to move the selected interface (wlan0 in this example) from the Available LAN interfaces List to the Grouped LAN Interfaces, Figure 5-140-5
- STEP 5.** Wlan0, the selected interface for interface grouping is now show at the grouped LAN interfaces list, Figure 5-140-5

STEP 6. To finalize the configuration use the Save/Apply button, Figure 5-140-6. The next displayed window is initial window, the Advanced Setup- Interface grouping initial window showing the current configuration, Figure 5-142

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**

4. Click Apply/Save button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name: 1

WAN Interface used in the grouping 2

Grouped LAN Interfaces
 5

Available LAN Interfaces
eth0.0
eth2.0
eth3.0
wl0_Guest12GA|wl0.1
wl0_Guest12GA|wl0.2
wl0_Guest12GA|wl0.3

Automatically Add Clients With the following DHCP Vendor IDs

6

Figure 5-140: Advanced Setup- interface grouping configuration window- Setup on an Interface grouping example

Grouped LAN Interfaces

Available LAN Interfaces
eth0.0
eth2.0
eth3.0
 3
wl0_Guest12GA|wl0.1
wl0_Guest12GA|wl0.2
wl0_Guest12GA|wl0.3

4

Figure 5-141: Advanced Setup- interface grouping configuration window

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	eth0.0	
		veip0.2	eth2.0	
			eth3.0	
			wl0_Guest12GA wl0.1	
			wl0_Guest12GA wl0.2	
			wl0_Guest12GA wl0.3	
brgre	<input type="checkbox"/>	gre_xpto	vlan0	

Add

Remove

Figure 5-142: Advanced Setup- Interface grouping configuration initial Window: Current interface grouping configuration

5.6.14 IP Tunnel

Selection of Advanced Setup submenu, item IP Tunnel item will display an IP Tunnel submenu with two items, Figure 5-143:

- IPv6inIPv4,
- IPv4inIPv6

In the main window an IP Tunneling-6in4 Tunnel Configuration window will be displayed, Figure 5-144.



Figure 5-143: Advanced Setup IP Tunnel Sub-menu

5.6.14.1 IPv6inIPv4

Selection of Advanced Setup, IP Tunnel submenu, IPv6inIPv4 item, will display an IP Tunneling-6in4 Tunnel Configuration window, Figure 5-144.

This window displays the current IP Tunneling-6in4 Tunnel Configuration.

To insert and configure a new IPv6 into IPv4 tunnel entry use the Add Button, Figure 5-144; a new window is displayed, Figure 5-145. A short on line help text is provided in the configuration window. Figure 5-146 provides a configuration example.

In order to configure new IPv6 into IPv4 tunnel entry, Figure 5-146:

STEP 1. Type in the Tunnel Name;

STEP 2. Select the Mechanism to use from the selection combo box;

Note: Currently only 6RD configuration is supported;

STEP 3. Select the Associated WAN interface to use from the selection combo box;

STEP 4. Select the Associated LAN interface to use from the selection combo box;

STEP 5. Select the option Manual or Automatic;

In the case of Manual option selection the following steps are required, Figure 5-145:

STEP 6. Type in the IPv4 Mask length (manual configuration only);

STEP 7. Type in the 6RD Prefix with Prefix length (manual configuration only);

STEP 8. Type in the Relay IPv4 Address (manual configuration only).

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the IP Tunneling-6in4 Tunnel Configuration, Figure 5-147.

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove

Figure 5-144: Advanced Setup, IP tunnel IP- Tunneling-6in4 Tunnel Configuration window

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name

Mechanism:

6RD

Associated WAN Interface:

Associated LAN Interface:

LAN/br0

☒ Manual

☐ Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

Apply/Save

Figure 5-145: Advanced Setup, IP tunnel IP- Tunneling-6in4 Tunnel: Add Tunnel Configuration window

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name

xpto_tunnel

Mechanism:

6RD

Associated WAN Interface:

ipoe_veip0.15/veip0.2

Associated LAN Interface:

LAN/br0

☐ Manual

☒ Automatic

Apply/Save

Figure 5-146: Advanced Setup, IP tunnel IP- Tunneling-6in4 Tunnel Add Tunnel Configuration window example

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
xpto_tunnel	veip0.2	br0	Dynamic	0			<input type="checkbox"/>

Remove

Figure 5-147: Advanced Setup, IP tunnel IP- Tunneling-6in4 Tunnel Configuration window- current configuration

5.6.14.2 IPv4inIPv6

Selection of Advanced Setup, IP Tunnel submenu, IPv4inIPv6 item, will display an IP Tunneling-4in6 Tunnel Configuration window, Figure 5-148.

This window displays the current IP Tunneling-4in6 Tunnel Configuration.

To insert and configure a new IPv4 into IPv6 tunnel entry use the Add Button, Figure 5-148; a new window is displayed, Figure 5-149. A short on line help text is provided in the configuration window. Figure 5149 provides a configuration example.

In order to configure new IPv6 into IPv4 tunnel entry, Figure 5-149:

STEP 1. Type in the Tunnel Name;

STEP 2. Select the Mechanism to use from the selection combo box;

Note: Currently only DS-Lite configuration is supported;

STEP 3. Select the Associated WAN interface to use from the selection combo box;

STEP 4. Select the Associated LAN interface to use from the selection combo box;

STEP 5. Select the option Manual or Automatic;

To finalize the configuration use the Apply/Save button. The next displayed window is the initial window, showing the IP Tunneling-6in4 Tunnel Configuration, Figure 5-150.

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	AFTR	Remove
<div><div>Add</div><div>Remove</div></div>					

Figure 5-148: Advanced Setup, IP tunnel IP- Tunneling-4in6 Tunnel Configuration window

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name	<input type="text" value="xpto_tunnel4in6"/>
Mechanism:	<div>DS-Lite ▼</div>
Associated WAN Interface:	<div>gre_tunnel/gre_tunnel ▼</div>
Associated LAN Interface:	<div>LAN/br0 ▼</div>
<div><input type="radio"/> Manual <input checked="" type="radio"/> Automatic</div>	
<div>Apply/Save</div>	

Figure 5-149:Advanced Setup, IP tunnel IP- Tunneling-4in6 Tunnel: Add Tunnel Configuration window exemple

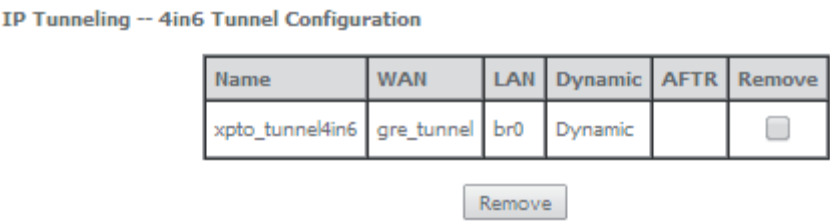


Figure 5-150: Advanced Setup, IP tunnel IP- Tunneling-4in6 Tunnel Configuration window- current configuration

5.6.15 Power Management

Selection of Advanced Setup, Power Management item, will display Power Management control and information window, Figure 5-151.

This window allows the control of Hardware modules to evaluate power consumption. Hardware modules can be enabled by selecting the corresponding checkbox and use the enabled button. The Apply button will finalize the power management configuration. Refresh button allows the updating of module power consumption status, that can be consulted by selecting the module respective status button.

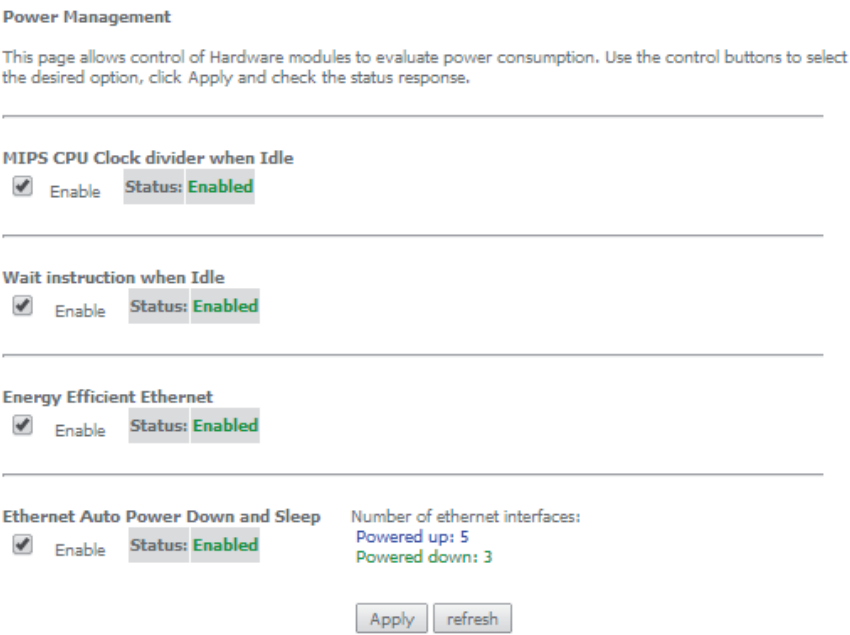


Figure 5-151: Advanced Setup, Power Management Configuration window

5.6.16 Multicast

Selection of Advanced Setup menu, item Multicast will display a Multicast (IGMP and MLD) Configuration window, Figure 5-152. This window allows the configuration of the:

- IGMP
- MLD

A short on line help text is provided in the configuration window.

Figure 5152 provides a Multicast configuration example.

In order to configure Multicast, Figure 5-152

STEP 1. Configure Multicast Precedence from the Selection combo box; Options available are:

- Disable
- Precedence value (lower value, higher priority)

IGMP and MLD configurations are filled with default values, Figure 5-152, that can be modified if desired. In order to proceed with Multicast default configuration values just go to the bottom of the window and use the Apply/Save to finalize the configuration.

Otherwise, if other than default values should be used for the multicast configuration change the default values by typing in the corresponding parameter field the desired value and finalize the configuration by using the Apply/Save button at the bottom of the window.

EN

Multicast Precedence: Disable ▾ lower value, higher priority

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	2
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	<input checked="" type="checkbox"/>

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	2
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	10
Maximum Multicast Data Sources (for mldv2):	10
Maximum Multicast Group Members:	10
Fast Leave Enable:	<input checked="" type="checkbox"/>

Apply/Save

Figure 5-152: Advanced Setup, Multicast (IGMP and MLD) Configuration window – configuration example

5.7 Wireless

Selection of Advanced Setup submenu item Wireless will display a Wireless submenu with six items, Figure 5-153:

- Basic,
- Security,
- MAC Filter,
- Wireless Bridge,
- Advanced,
- Station Info.

In the main window a Wireless-Basic Configuration window will be displayed, Figure 5-154.

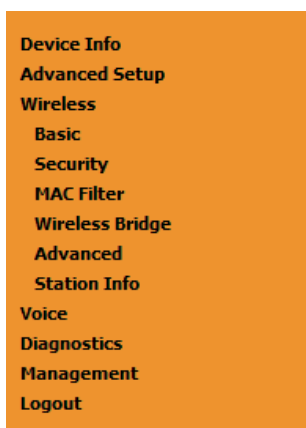


Figure 5-153: Wireless submen

5.7.1 Basic

Selection of Advanced Setup submenu Wireless, item Basic will display a Wireless-Basic configuration window, Figure 5-154.

A short on line help text is provided in the configuration window.

In order to configure Wireless LAN interface basic features:

- STEP 1.** To Enable the Wireless LAN interface select the “Enable Wireless” checkbox;
- STEP 2.** To Enable the Wireless Hotspot 2.0 e select the corresponding checkbox;
- STEP 3.** To Hide Access Pointe from active scans select the corresponding checkbox;
- STEP 4.** To configure Clients Isolation select the corresponding checkbox;
- STEP 5.** To disable WMM Advertise select the corresponding checkbox;
- STEP 6.** To Enable Wireless Multicast Forwarding (WMF) select the corresponding checkbox;
- STEP 7.** Type in the Wireless network Name (SSID) ;
- STEP 8.** Select the country from the selection combo box in order to restrict the channel set based on country requirements

STEP 9. Type in Country RegRev

STEP 10. Type in the maximum number of clients

STEP 11. At the wireless-guest/virtual Access Points configuration table use the checkboxes to configure Virtual access points

To finalize the configuration use the Apply/Save button at the bottom of the window.

EN

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

- ☒ Enable Wireless
- ☐ Enable Wireless Hotspot2.0
- ☐ Hide Access Point
- ☐ Clients Isolation
- ☐ Disable WMM Advertise
- ☐ Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Country RegRev

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

Figure 5-154: Wireless -Basic configuration window –configuration exemple

5.7.2 Security

Selection of Advanced Setup submenu Wireless, item Security will display a Wireless-Security configuration window, Figure 5-155.

A short on line help text is provided in the configuration window.

Wireless Security can be configured:

- Manually - Figure 5-155 configuration example
- Through WI-FI Protected Setup (WPS) - Figure 5-158 configuration example.

In order to configure Wireless LAN interface Security features manually, Figure 5-155:

STEP 1. Select "Disable" from the WPS selection combo box;

STEP 2. Select SSID from the selection combo box;

STEP 3. Select Network Authentication Method from the selection combo box, Figure 5-156;

STEP 4. At the WEP encryption selection combo box select:

- Disabled, Figure 5-155, to disable WEP encryption; in this case configuration is complete- use the Apply/Save to finalize the security configuration
- Enabled, Figure 5-157, to enable WEP encryption; in this case proceed with WEP encryption configuration (following steps)

WEP encryption configuration (WEP encryption is set to Enabled) Figure 5-157:

STEP 5. Select Encryption Strength value from the selection combo box;

STEP 6. Select Current Network Key from the selection combo box;

STEP 7. Type in Network Key values for Keys 1 to 4;

To finalize the configuration use the Apply/Save button at the bottom of the window.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS Disabled ▼

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID: Cisco-072894AF ▼

Network Authentication: Open ▼

WEP Encryption: Disabled ▼

Apply/Save

Figure 5-155: Wireless --Security configuration window –configuration example

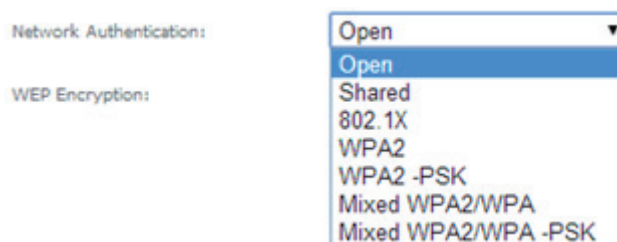


Figure 5-156: Wireless –Security configuration window –Network authentication available methods

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID: Cisco-072894AF ▼

Network Authentication: Open ▼

WEP Encryption: Enabled ▼

Encryption Strength: 128-bit ▼

Current Network Key: 1 ▼

Network Key 1: 1234567890123

Network Key 2: 1234567890123

Network Key 3: 1234567890123

Network Key 4: 1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

Figure 5-157: Wireless –Security configuration window –Manual Setup AP configuration (if WEP enabled selected)

In order to configure Wireless LAN interface Security features through WPS, Figure 5-158:

- STEP 1.** Select "Enabled" from the WPS selection combo box;
- STEP 2.** To use Add Client feature (available only for WPA-PSK(WPS1)):
 - Select the desired option use STA PIN /use AP PIN by selecting the corresponding checkbox;
 - Use the Add Enrollee to finalize Add client configuration
- STEP 3.** Select WPS AP Mode from the selection combo box;
- STEP 4.** Setup AP (Configure all security settings with an external register), by entering the Device PIN;

Help on Device PIN configuration is available at the Help link, Figure 5-159

To finalize the configuration use the Apply/Save button at the bottom of the window.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.

You may setup configuration manually

OR

through WiFi Protected Setup(WPS)

Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS

Enabled ▼

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)



Use STA PIN



Use AP PIN

Add Enrollee

Set WPS AP Mode

Configured ▼

Setup AP (Configure all security settings with an external registrar)

Device PIN

90150104

[Help](#)

Figure 5-158: Wireless --Security configuration window --WPS Setup configuration

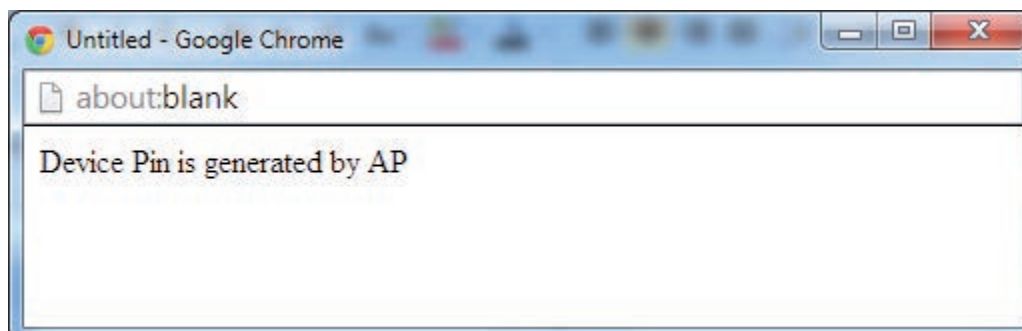


Figure 5-159: Wireless --Security configuration window --WPS Setup -- Device PIN Help window

5.7.3 MAC Filter

Selection of Advanced Setup submenu Wireless, item MAC Filter will display a Wireless-MAC Filter configuration window, Figure 5-160.

A short on line help text is provided in the configuration window.

In order to configure MAC filter:

STEP 1. Select SSID from the selection combo box;

STEP 2. Choose the MAC Restrict Mode by selecting the desired Mode at the corresponding checkbox;

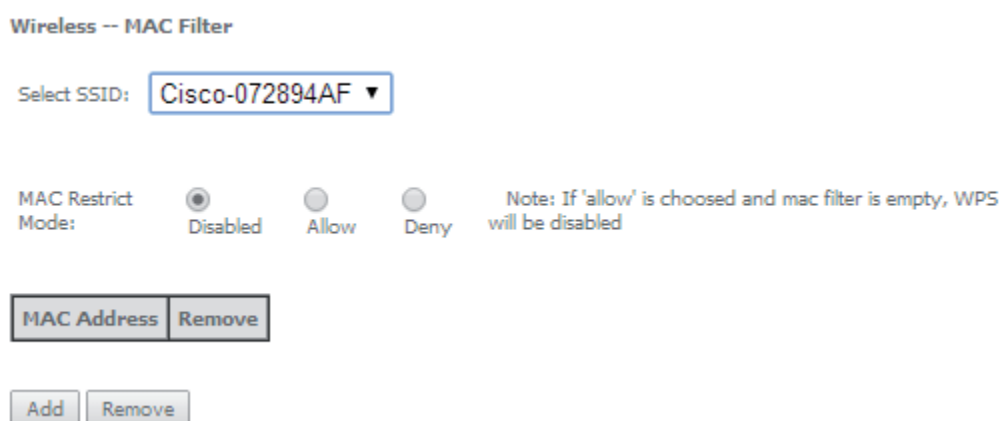
STEP 3. If disabled selected, the configuration is finalized

STEP 4. If allow or deny selected MAC addresses to be filtered must be entered at the MAC address table;

Note: If "Allow" option is selected and the MAC address table is empty WPS will be disa

STEP 5. To enter the MAC addresses to filter in the MAC address table use the Add button;

STEP 6. To remove MAC addresses from the table, select the checkbox on the Remove Column for the desired MAC address and use the Remove button.



The screenshot shows the 'Wireless -- MAC Filter' configuration window. At the top, the title is 'Wireless -- MAC Filter'. Below it, there is a 'Select SSID:' label followed by a dropdown menu showing 'Cisco-072894AF' with a downward arrow. Underneath, the 'MAC Restrict Mode:' is set to 'Disabled', indicated by a selected radio button. There are also unselected radio buttons for 'Allow' and 'Deny'. To the right of these options, a note states: 'Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled'. Below the mode selection, there is a table with two columns: 'MAC Address' and 'Remove'. At the bottom of the window, there are two buttons: 'Add' and 'Remove'.

Figure 5-160: Wireless –MAC Filter configuration window –configuration exemple

5.7.4 Advanced

Selection of Advanced Setup submenu Wireless, item Advanced will display a Wireless-Advanced configuration window, Figure 5-161.

A short on line help text is provided in the configuration window.

This window allows the selection of a particular Channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wake up interval for clients in power-save mode, set the beacon interval for the access point, set the Xpress mode and set whether short or long preambles are used.

Figure 5-161 provides a Wireless - Advanced features configuration example; Default values are available and auto configuration mode dependent on the parameters, and can be used as is or modified as desired.

To finalize the configuration the Apply/Save button must be used.

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply/Save" to configure the advanced wireless options.

Band:

2.4GHz

Channel:

Auto

Current: 11 (interference: acceptable)

Auto Channel Timer(min)

0

802.11n/EWC:

Auto

Bandwidth:

20MHz in 2.4G Band and 40MHz in 5G Band

Current: 20MHz

Control Sideband:

Lower

Current: N/A

802.11n Rate:

Auto

802.11n Protection:

Auto

Support 802.11n Client Only:

Off

RIFS Advertisement:

Auto

OBSS Coexistence:

Enable

RX Chain Power Save:

Enable

Power Save status: Full Power

RX Chain Power Save Quiet Time:

10

RX Chain Power Save PPS:

10

54g[™] Rate:

1 Mbps

Multicast Rate:

Auto

Basic Rate:

Default

Fragmentation Threshold:

2346

RTS Threshold:

2347

DTIM Interval:

1

Beacon Interval:

100

Global Max Clients:

16

XPress[™] Technology:

Disabled

WMM(Wi-Fi Multimedia):

Enabled

WMM No Acknowledgement:

Disabled

WMM APSD:

Enabled

Beamforming Transmission (BFR):

Disabled

Beamforming Reception (BFE):

Disabled

Apply/Save

Figure 5-161: Wireless –Advanced configuration window

5.7.5 Station Info

Selection of Advanced Setup submenu Wireless, item Station Info will display a Wireless-Authenticated Stations Information window Figure 5-162, listing currently authenticated wireless stations and providing information on its status.

Information can be updated by using the button Refresh.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
84:3A:4B:14:B2:92	Yes		Cisco-072894AF	wl0
64:27:37:76:23:1E	Yes		Cisco-072894AF	wl0

Refresh

Figure 5-162: Wireless –Authentication Stations configuration window

5.8 Voice

Configuration of Voice on the Refs. 769501-769502 requires an IPoE service on the WAN interface to be used for VoIP. To create an IPoE service on a WAN interface, please refer to section IPoE .

Selection of menu item Voice will display Voice submenu, Figure 5-163, with three items:

- SIP Basic Setting,
- SIP Advanced Setting,
- SIP Debug setting

In the main window a SIP Basic Settings–Global Parameters configuration window will be displayed, Figure 5-164.

Device Info
Advanced Setup
Wireless
Voice
 SIP Basic Setting
 SIP Advanced Setting
 SIP Debug Setting
Diagnostics
Management
Logout

Figure 5-163: Voice Submenu

5.8.1 SIP Basic Settings

Selection of Voice menu, item SIP Basic Settings will display a SIP Basic Settings–Global Parameters configuration window, Figure 5-164

A short on line help text is provided in the configuration window.

In order to configure Global Parameters:

STEP 1. Select the Bound Interface Name from the selection combo box, Figure 5-165;

STEP 2. Select the IP address Family from the selection combo box;

To finalize the configuration use the Apply button at the bottom of the window.

Using the “Start SIP client” button will unregister the SIP accounts as can be seen by consulting the Voice status information, through Device Info menu, item Voice, Figure 5-166.

The UP value on the Registration Status column indicates the account registration was successful, the accounts are active and VoIP is operational.

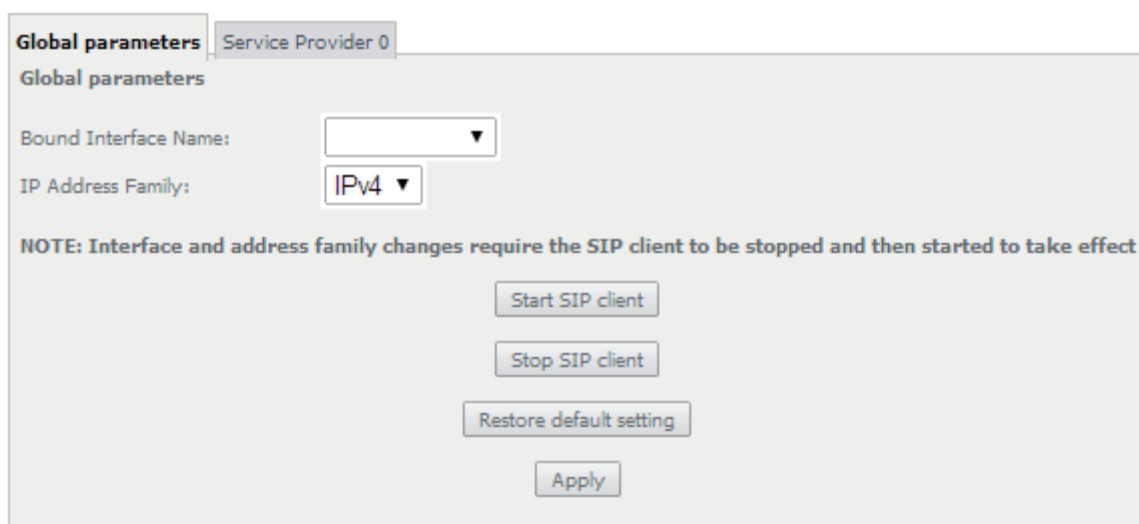


Figure 5-164: Voice, SIP Basic Settings–Global Parameters configuration window

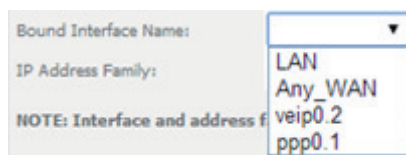


Figure 5-165: Voice, SIP Basic Settings–Global Parameters–Bound Interface Name selection combo box

Status -- Voice

SIP Account	User Name	User Status	Registration Status
1	1002	Enabled	Up
2	1003	Enabled	Up

Figure 5-166: Device Info, Voice- Registered Sip Accounts information and Status

EN

Figure 5-167 provides a configuration example for the SIP provider parameters (Basic Settings)

In order to configure Service Provider, Figure 5-167:

STEP 1. Select the Local from the selection combo box, Figure 5-168;

This will change service provider parameters dependent on local specific applicable standards, such as Ring tone,

Change of local to take effect will require the SIP client to be stopped and then restarted.

STEP 2. Type in Voice Dialplan;

STEP 3. To Use SIP Proxy select the corresponding checkbox;

STEP 4. If Use SIP Proxy selected configure SIP proxy to use by entering:

- SIP Proxy
- SIP Proxy Port

STEP 5. To Use SIP Outbound Proxy select the corresponding checkbox;

STEP 6. If Use SIP Outbound Proxy selected configure SIP Outbound Proxy to use by entering:

- SIP Outbound Proxy
- SIP Outbound Proxy Port

STEP 7. To Use SIP Registrar select the corresponding checkbox;

STEP 8. If Use SIP Registrar selected configure SIP Registrar to use by entering:

- SIP Registrar
- SIP Registrar Port

Configure two SIP accounts "0" and "1", at the SIP account table:

STEP 9. Enable the accounts by selecting the respective Enable Account checkbox;

STEP 10. Type in for each account the extension number;

STEP 11. Type in for each account the account display name;

STEP 12. Type in for each account the account authentication name;

STEP 13. Type in for each account the account password;

STEP 14. Select for each account the Physical Terminal Assignment, i.e., the FXS port to use, by using the FXS ports checkboxes;

STEP 15. Select the account Preferred time value at the respective selection combo box;

STEP 16. Select the account set of Preferred codecs to use, from the respective selection combo boxes;

To finalize the configuration use the Apply button at the bottom of the window.

To make effective the configuration just done, use the Start SIP client button.

Global parameters **Service Provider 0**

Voice -- SIP configuration

Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.

Locale selection*: **ETS - ETSI** (Note: Requires the SIP client to be stopped and then started to take affect)

Voip Dialpan Setting: **x+T**

☒ Use SIP Proxy.

SIP Proxy: **sip-proxy.qilu.voip.oi**

SIP Proxy port: **5060**

☒ Use SIP Outbound Proxy.

SIP Outbound Proxy: **sip-proxy.qilu.voip.oi**

SIP Outbound Proxy port: **5060**

☒ Use SIP Registrar.

SIP Registrar: **sip-proxy.qilu.voip.oi**

SIP Registrar port: **5060**

SIP Account	0	1
Account Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Extension	13022014	13022015
Display name	13022014	13022015
Authentication name	13022014	13022015
Password	valentine	romeu
Physical Terminal Assignment	<input checked="" type="checkbox"/> FXS 0 <input type="checkbox"/> FXS 1	<input type="checkbox"/> FXS 0 <input checked="" type="checkbox"/> FXS 1
Preferred ptime	20	20
Preferred codec 1	G.711ALaw	G.711ALaw
Preferred codec 2	G.729a	G.729a
Preferred codec 3	G.723.1	G.723.1
Preferred codec 4	G.726_24	G.726_24
Preferred codec 5	G.726_32	G.726_32
Preferred codec 6	PCMWIDEBAND	PCMWIDEBAND

Start SIP client

Stop SIP client

Restore default setting

Apply

* Changing this parameter for one service provider affects all other service providers.

Figure 5-167: Voice, SIP Basic Settings--Service Provider configuration window

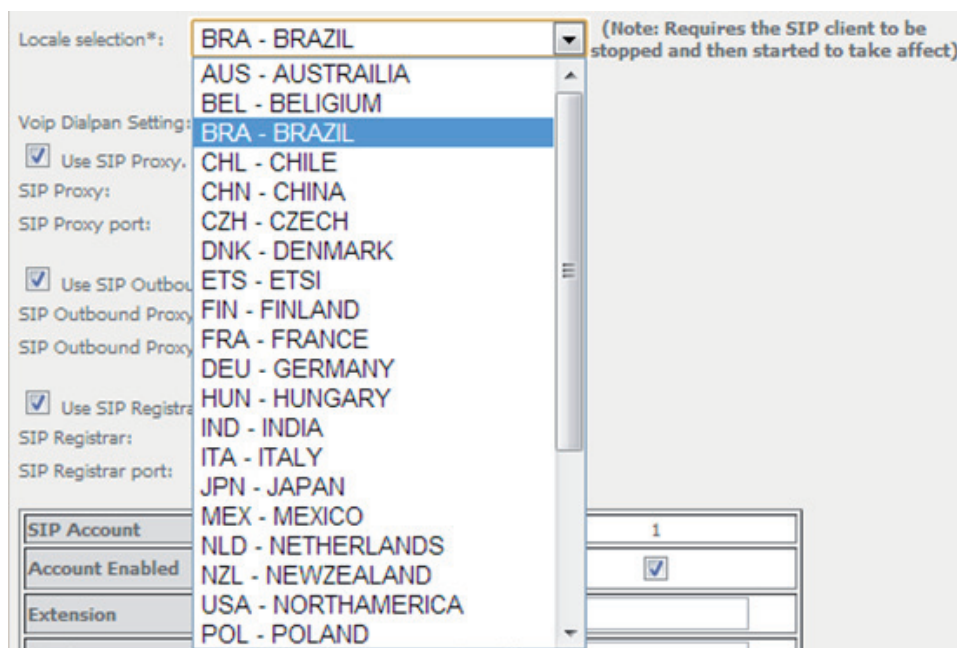


Figure 5-168: Voice, SIP Basic Settings– Service Provider configuration window- Local Selection combo box

5.8.2 SIP Advanced Settings

Selection of Voice menu, item SIP Advanced Settings will display a SIP Advanced Settings–Service Provider configuration window, Figure 5-169 and Figure 5-170.

Figure 5-169 and Figure 5-170, provide a configuration example for the SIP provider parameters (Advanced settings)

In order to configure Service Provider-Advanced Settings Figure 5-169 and Figure 5-170:

STEP 1. Configure Enable SIP Call Features for the two SIP accounts “0” and “1”, at the “ Enable Call Features” table, Figure 5-169,

In order to enable a desired advanced sip call feature for an account, at the account column, for the desired feature select the respective Checkbox. Activation instructions for the enabled feature are provided at the column “Activation Instructions”

STEP 2. Type in the Registration Expire Timeout;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 3. Type in the Registration Retry Interval;

STEP 4. Select DSCP for SIP option from the selection combo box;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 5. Select DSCP for RTP option from the selection combo box;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 6. Select Dtmf Relay settings option from the selection combo box;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 7. Select Hook Flash Relay setting option from the selection combo box;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 8. Select SIP Transport protocol option from the selection combo box;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 9. Select SRTP Configuration option from the selection combo box;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 10. To Enable SIP tag matching select the respective checkbox;

Note1: Must be uncheck for Vonage Interop;

Note2: Changing this parameter for one service provider affects all other service providers;

STEP 11. Type in the Music Server IP address;

Note: Changing this parameter for one service provider affects all other service providers;

In order to configure a Music Server:

STEP 12. Type in the Music Server Port;

Note: Changing this parameter for one service provider affects all other service providers;

In order to configure Conference :

STEP 13. Type in the Conference URI;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 14. Select Conference Option from the respective selection combo box;

Note: Changing this parameter for one service provider affects all other service providers;

To finalize the configuration use the Apply button at the bottom of the window.

To make effective the configuration just done, use the Start SIP client button.

Global parameters | **Service Provider 0**

Voice -- SIP Advanced configuration

Enabled SIP Call Features			
Feature	Account 0	Account 1	Activation Instructions
Call waiting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	When enabled, dial *61 to activate, *60 to deactivate
Call forwarding number			
Forward unconditionally	<input type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *71 to activate, *75 to deactivate
Forward on "busy"	<input type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *71 to activate, *75 to deactivate
Forward on "no answer"	<input type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *71 to activate, *75 to deactivate
Call barring	<input type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *85[PIN]0/*85[PIN]1/*85[PIN]2 to deactivate/activate/activate per digitmap
Call barring pin	9999	9999	
Call barring digit map			
Warm line	<input type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *78 to activate, *79 to deactivate
Warm line number			
Anonymous call blocking	<input type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *80 to activate, *81 to deactivate
Anonymous calling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	When enabled, dial *82 to activate for current call
DND	<input type="checkbox"/>	<input type="checkbox"/>	When enabled, dial *86 to activate, *87 to deactivate

☐ Enable T38 support

☒ Enable V18 support

☒ Enable DHCP Option 120 (SIP Servers)

Figure 5-169: Voice, SIP Advanced Settings–Service Provider configuration window -1

Registration Expire Timeout*: 0

Registration Retry Interval: 20

DSCP for SIP*: EF (101110)

DSCP for RTP*: EF (101110)

Dtmf Relay setting*: InBand

Hook Flash Relay setting*: None

SIP Transport protocol*: UDP

SRTP Configuration*: Disabled

☒ Enable SIP tag matching* (Uncheck for Vonage Interop).

Music Server*: 0.0.0.0

Music Server port*: 0

Conference URI*:

Conference Option*: Local

Start SIP client

Stop SIP client

Apply

* Changing this parameter for one service provider affects all other service providers.

Figure 5-170: Voice, SIP Advanced Settings–Service Provider configuration window -2

5.8.3 SIP Debug Settings

Selection of Voice menu, item SIP Debug Settings will display a SIP Debug Settings–Service Provider configuration window, Figure 5-171.

Figure 5-171, provides a configuration example for the Service provider parameters (SIP Debug Configuration)

In order to configure Service Provider- SIP Debug Configuration, Figure 5-171:

STEP 1. Type in the SIP log server IP Address;

Note: Changing this parameter for one service provider affects all other service providers;

STEP 2. Type in the SIP log server port;

Note: Changing this parameter for one service provider affects all other service providers;

Configure line debug option at the Line table:

STEP 3. To enable VAD support for a line select the respective checkbox;

STEP 4. To configure Ingress gain for a line select Ingress Gain Value from the respective selection combo box;

STEP 5. To configure Egress gain for a line select Egress Gain Value from the respective selection combo box;

To finalize the configuration use the Apply button at the bottom of the window.

To make effective the configuration just done, use the Start SIP client button.

Global parameters

Service Provider 0

Voice -- SIP Debug configuration

SIP log server IP Address*:

0.0.0.0

SIP log server port*:

0

Line	1	2
VAD support	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ingress gain	0 ▾	0 ▾
Egress gain	0 ▾	0 ▾

Start SIP client

Stop SIP client

Apply

* Changing this parameter for one service provider affects all other service providers.

Figure 5-171: Voice, SIP Debug Settings configuration window

5.9 Diagnostics

Selection of menu item Diagnostics will display a Diagnostics Information window, Figure 5-172.

This window lists the individual test results. In case of fail, Troubleshooting procedures will be available at the Help link for the respective failed test.

Rerun diagnostic tests button allows running the tests and for confirmation of the persistence of the fail result. The window will be updated with the results of the Diagnostics tests rerun.

EN

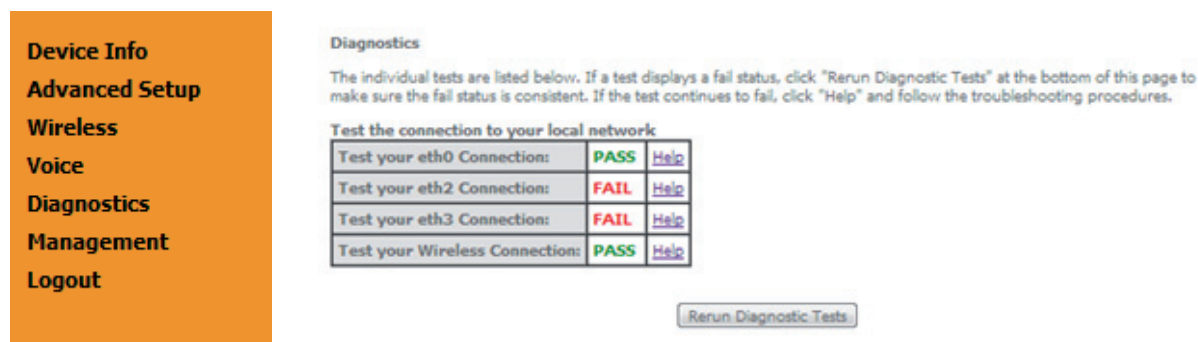


Figure 5-172: Diagnostics information window

5.10 Management

Selection of menu item Management will display management submenu, Figure 5-173, with eight items:

- Settings,
- System Log,
- Security Log,
- TR-069 Client,
- Internet Time,
- Access Control,
- Update Software,
- Reboot.

In the main window a Management, Settings–Backup window will be displayed, Figure 5-175.

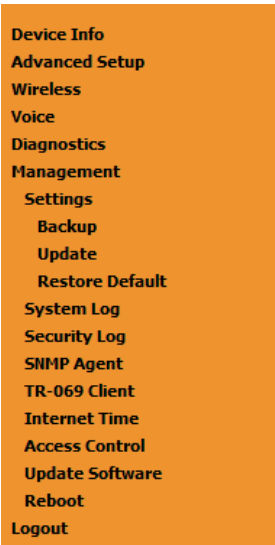


Figure 5-173: Management Submenu

5.10.1 Settings

Selection of Management Submenu, item Settings will display a Settings submenu, Figure 5-174, with four items:

- Backup,
- Update,
- Restore Default.

In the main window a Management, Settings–Backup window will be displayed, Figure 5-175.

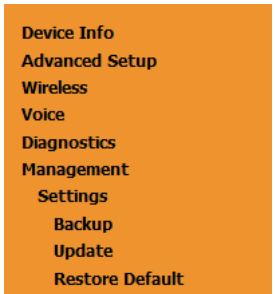


Figure 5-174: Management, Settings Submenu

5.10.1.1 Backup

Selection of Management, Settings submenu, item Backup will display a Settings–Backup window will be displayed, Figure 5-175.

A short on line help text is provided in the window. This window allows saving the current Refs. 769501-769502 configurations to a PC.

In order to Backup the current Refs. 769501-769502 configurations use the button Backup Settings, Figure 5-175. A Save file window will open at your PC allowing to choose the folder where to save the backup file and the renaming of the file.

Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Backup Settings

Figure 5-175: Management, Settings–Backup window

5.10.1.2 Update

Selection of Management, Settings submenu, item Update will display a Tools–Update Settings window Figure 5-176.

A short on line help text is provided in the window. This window allows updating the Refs. 769501-769502 configurations with a Backup file previously saved to a PC.

In order to update Refs. 769501-769502 configuration with a saved backup file, Figure 5-176:

STEP 1. Use the button Select file. An open file window will open at your PC allowing to choose a previously backed up file to use;

STEP 2. Use the Update Settings button and the Refs. 769501-769502 configurations will be updated with the selected file.

Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

Select File

No file is selected.

Update Settings

Figure 5-176: Management, Settings–Tools- Update window

5.10.1.3 Restore Default

Selection of Management, Settings submenu, item Restore Default will display a Tools-Restore Default Settings window Figure 5-177.

A short on line help text is provided in the window. This window allows restore Refs. 769501-769502 configurations to default setting.

In order to restore Refs. 769501-769502 configuration to Default Settings use the Restore Default Settings button.

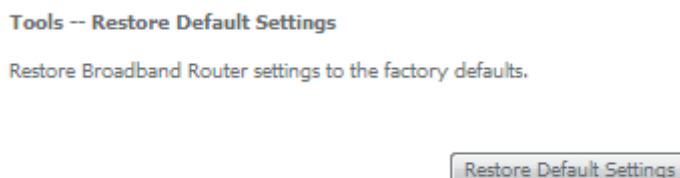


Figure 5-177: Management, Settings–Tools –Restore Default Settings window

5.10.2 System Log

Selection of Management menu item System Log, will display a System Log window Figure 5-179.

A short on line help text is provided in the window. This window allows viewing and configuring System Log.

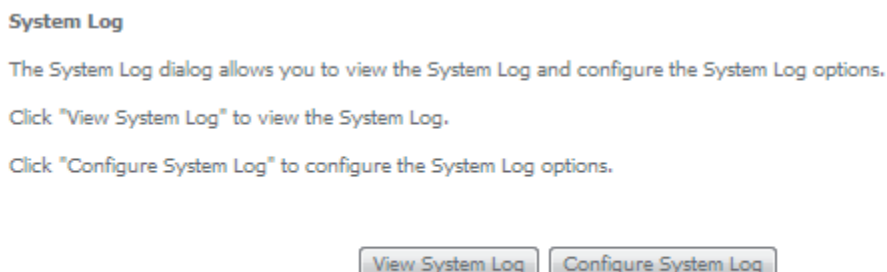


Figure 5-178: Management–System Log window

In order to view System Log use the View System Log button, Figure 5-179. A window will display showing Refs. 769501-769502 debug information on the mode selected on the System Log configuration, with events' date and time displayed, Figure 5-179.

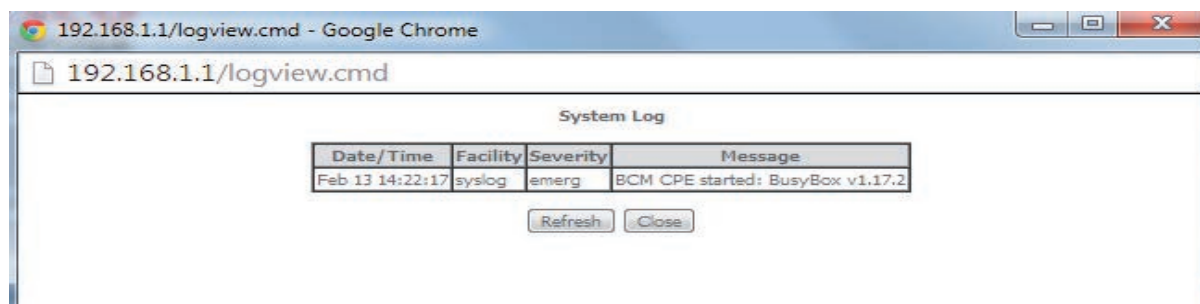


Figure 5-179: Management–System Log Configuration: View System Log

In order to configure System Log Options use the Configure System Log button, Figure 5-178; a System Log Configuration window will be displayed, Figure 5-180.

Figure 5-183 provides a System Log configuration example.

A short on line help text is provided in the window.

In order to configure System Log options:

- STEP 1.** To enable System Log select the Log Enable checkbox, Figure 5-180;
- STEP 2.** Select the Log Level from the respective selection combo box, Figure 5-180;
- STEP 3.** Select the Display Level from the respective selection combo box, Figure 5-181;
- STEP 4.** Select the Mode from the respective selection combo box, Figure 5-182;

To finalize the configuration use the Apply/save Button, Figure 5-183.

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ☐ Disable ☒ Enable

Log Level: Debugging

Display Level: Emergency

Mode: Alert

Apply/Save

Figure 5-180: Management–System Log Configuration window –Log level options

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ☐ Disable ☒ Enable

Log Level: Debugging

Display Level: Warning

Mode: Emergency
Alert
Critical
Error
Warning
Notice
Informational
Debugging

Apply/Save

Figure 5-181: Management-System Log Configuration window -Display level options

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ☐ Disable ☒ Enable

Log Level: Debugging

Display Level: Warning

Mode: Local
Local
Remote
Both
Support Mode

Apply/Save

Figure 5-182: Management-System Log Configuration window -Mode level options

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ☐ Disable ☒ Enable

Log Level:

Display Level:

Mode:

Apply/Save

Figure 5-183: Management-System Log Configuration window –Configuration Example

5.10.3 Security Log

Selection of Management menu item Security Log, will display a Security Log window Figure 5-184.

A short on line help text is provided in the window. This window allows viewing and resetting Security Log.

In order to view Security Log use the View button, Figure 5-184. A window will display showing Refs. 769501-769502 security log information on the mode selected on the Security Log configuration, with events' date and time displayed, Figure 5-185.

Security Log

The Security Log dialog allows you to view the Security Log and configure the Security Log options.

Click "View" to view the Security Log.

Click "Reset" to clear and reset the Security Log.

Right-click [here](#) to save Security Log to a file.

View Reset

Figure 5-184: Management-Security Log window

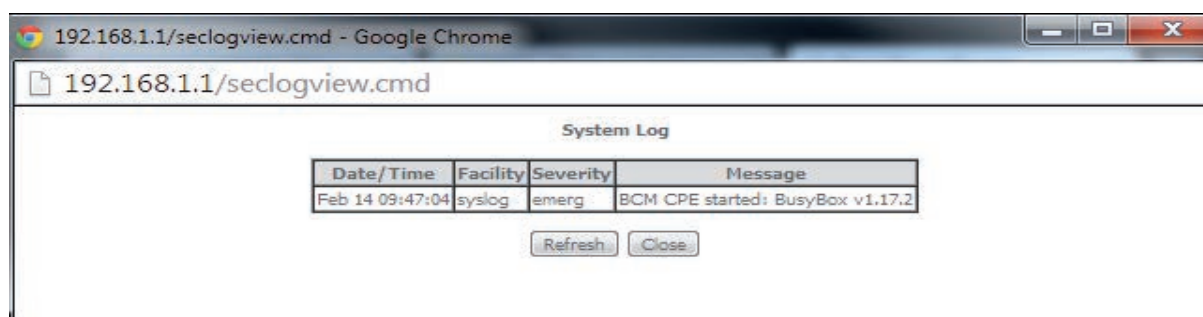


Figure 5-185: Management- Security Log window: View

In order to reset Security Log use the Reset Button, Figure 5-184. A Reset information window will be displayed, Figure 5-186.



Figure 5-186: Management-Security Log window: Reset

5.10.4 TR-069 Client

Selection of Management menu item TR-069 Client, will display a TR-069 Client Configuration window, Figure 5-187.

A short on line help text is provided in the window. TR-069 Client configuration allows the connection to an Auto configuration Server (ACS) for Refs. 769501-769502 configuration, provisioning, collection and diagnostics.

Figure 5-187 provides a TR-069 client configuration example.

In order to Configure TR-069 Client, Figure 5-187:

STEP 1. Configure Inform Option to be Disabled or Enabled by selecting the respective Checkboxes;

STEP 2. Type in Inform Interval Value for the Inform Enabled option;

Time Interval between Refs. 769501-769502 and ACS communications

STEP 3. Type in the ACS URL;

STEP 4. Type in the ACS User Name;

STEP 5. Type in the ACS Password;

STEP 6. Select the WAN Interface used by the TR-069 Client from the respective selection combo box, Figure 5-188;

STEP 7. Configure "Display SOAP messages on serial console" Option to be Disabled or Enabled by selecting the respective Checkboxes;

If enabled the messages exchanged between the Refs. 769501-769502 and the ACS can be viewed via serial port.

STEP 8. To use Connection Request Authentication select the respective checkbox;

This option is enabled by default; ACS will send answer messages to connection Request if enabled and configured;

If Connection Request authentication is to be used, configure it:

STEP 9. Type in the Connection Request User Name;

STEP 10. Type in Connection Request Password;

STEP 11. Type in Connection Request URL;

This URL is the selected WAN interface URL with port and serial number information (Connection Request URL Format - `http://IP:port/serialNumber`)

Use the Apply/Save Button to Finalize the Configuration.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Inform Interval:	<input type="text" value="900"/>
ACS URL:	<input type="text" value="http://vodka.lipptr69"/>
ACS User Name:	<input type="text" value="admin"/>
ACS Password:	<input type="password" value="*****"/>
WAN Interface used by TR-069 client:	<input type="text" value="bronu1.14"/> ▼
Display SOAP messages on serial console	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input checked="" type="checkbox"/> Connection Request Authentication	
Connection Request User Name:	<input type="text" value="admin"/>
Connection Request Password:	<input type="password" value="*****"/>
Connection Request URL:	<input type="text" value="http://172.22.169.71:30005/5054494E072894AF"/>
<input type="button" value="Apply/Save"/> <input type="button" value="GetRPCMethods"/>	

Figure 5-187: Management, TR-069 Client Configuration window

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform ☒ Disable ☐ Enable

Inform Interval: 900

ACS URL: http://vodka.lipp.tr69

ACS User Name: admin

ACS Password:

WAN Interface used by TR-069 client: bronu1.14

Display SOAP messages on serial console

☒ Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL: http://172.22.169.71:30005/5054494E072894AF

Apply/Save GetRPCMethods

Figure 5-188: Management, TR-069 Client Configuration window – WAN Interface Options

15.10.5 Internet Time

Selection of Management menu item Internet Time, will display an Internet Time-Time settings window, Figure 5-189.

A short on line help text is provided in the window. Internet Time Settings allows the configuration of time servers to enable updating 769501-Refs. 769502 date and time.

Figure 5-189 provides an Internet Time Settings configuration example.

In order to Configure Internet Time Settings, Figure 5-189:

STEP 1. Configure "Automatically Synchronize with Internet Time Servers" by selecting the respective Checkbox;

STEP 2. Select "First NTP Time Server" Option from the respective selection combo box, Figure 5-190;

If other was specified, Type in the IP address of the server to use Figure 5-190;

STEP 3. Select "Second NTP Time Server" Option from the respective selection combo box;

If other was specified, Type in the IP address of the server to use;

Up to five NTP servers can be specified if desired.

STEP 4. Select "Time zone offset" Option from the respective selection combo box, Figure 5-191;

Use the Apply/Save Button to Finalize the Configuration.

Time settings

This page allows you to the modem's time configuration.

☒ Automatically synchronize with Internet time servers

First NTP time server:	Other	192.168.123.200
Second NTP time server:	Other	213.13.16.235
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	
Time zone offset:	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London	

Apply/Save

Figure 5-189: Management, Internet Time-Time settings window

Time settings

This page allows you to the modem's time configuration.

☒ Automatically synchronize with Internet time servers

First NTP time server:	Other	192.168.123.200
Second NTP time server:	clock.fmt.he.net	213.13.16.235
Third NTP time server:	clock.nyc.he.net	
Fourth NTP time server:	clock.sjc.he.net	
Fifth NTP time server:	clock.via.net	
	ntp1.tummy.com	
	time.cachenetworks.com	
	time.nist.gov	
Time zone offset:	Other	n Time: Dublin, Edinburgh, Lisbon, London

Apply/Save

Figure 5-190: Management, Internet Time-Time settings window: NTP server options

Time settings

This page allows you to the modem's time configuration.

☒ Automatically synchronize with Internet time servers

First NTP time server:

Other

192.168.123.200

Second NTP time server:

Other

213.13.16.235

Third NTP time server:

None

Fourth NTP time server:

None

Fifth NTP time server:

None

Time zone offset:

(GMT-07:00) Mountain Time

(GMT-07:00) Mountain Time

(GMT-06:00) Central America

(GMT-06:00) Central Time

(GMT-06:00) Guadalajara, Mexico City, Monterrey

(GMT-06:00) Saskatchewan

(GMT-05:00) Bogota, Lima, Quito

(GMT-05:00) Eastern Time

(GMT-05:00) Indiana

(GMT-04:00) Atlantic Time

(GMT-04:00) Caracas, La Paz

(GMT-04:00) Santiago

(GMT-03:30) Newfoundland

(GMT-03:00) Brasilia

(GMT-03:00) Buenos Aires, Georgetown

(GMT-03:00) Greenland

(GMT-02:00) Mid-Atlantic

(GMT-01:00) Azores

(GMT-01:00) Cape Verde Is.

(GMT-00:00) Casablanca, Monrovia

(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Apply/Save

Figure 5-191: Management, Internet Time-Time settings window: Time zone options

5.10.6 Access Control

Selection of Management Submenu, item Access Control will display an Access Control submenu, Figure 5-192, with one item, Passwords. In the main window an Access Control-Passwords window will be displayed, Figure 5-193.

- Device Info
- Advanced Setup
- Wireless
- Voice
- Diagnostics
- Management
 - Settings
 - System Log
 - Security Log
 - SNMP Agent
 - TR-069 Client
 - Internet Time
 - Access Control
 - Passwords
 - Users Configuration
 - Update Software
 - Reboot
 - Logout

Figure 5-192: Management, Access Control Submenu

5.10.6.1 Passwords

Selection of Management, Access Controls submenu, item Passwords will display an Access Control-Passwords window, Figure 5-193.

A short on line help text is provided in the window. This window allows the definition of Refs. 769501-769502 user accounts.

Three user accounts can be defined:

- Admin: account with unrestricted access to view and change Refs. 769501-769502 configurations;
- Support: account for maintenance and diagnostics purposes;
- User: account to view Refs. 769501-769502 configurations and statistics and update Refs. 769501-769502 software.

NOTE: Only an admin user can view set up user accounts;

Access Control -- Passwords

Access to your broadband router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

User Name:

Old Password:

New Password:

Confirm Password:

Figure 5-193: Management, Access Control-Passwords configuration window

5.10.7 Update Software

Selection of Management menu item Update Software, will display a Tools- Update Software window, Figure 5-194.

This window allows the update of the Refs. 769501-769502 with an update file from the ISP.

A Step by Step on line help text is provided in the window.

Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: No file is selected.

Figure 5-194: Management, Tools- Update Software window

5.10.8 Reboot

Selection of Management menu item Reboot, will display a Reboot window, Figure 5-195.

This window allows the reboot of the Refs. 769501-769502.

A short on line help text is provided in the window.

To Reboot the Refs. 769501-769502 use the button Reboot.

Click the button below to reboot the router.

Reboot

Figure 5-195: Management, Reboot window

5.11 Logout

Selection of menu item Logout, Figure 5-196, will allow ending the user account session on the Refs. 769501-769502. A logout confirmation window will be displayed, Figure 5-197. Selection of Yes will confirm logout and terminate user session.

Device Info
Advanced Setup
Wireless
Voice
Diagnostics
Management
Logout

Figure 5-196: Logout menu item

Logout

Are you sure you want to log out?

Yes

No

Figure 5-197: Logout window

6. Operation Indicators

6.1 Refs. 769501-769502

The Refs. 769501-769502 has fifteen LEDs to indicate the equipment operational status.

6.1.1 LED Indicators Status

EN

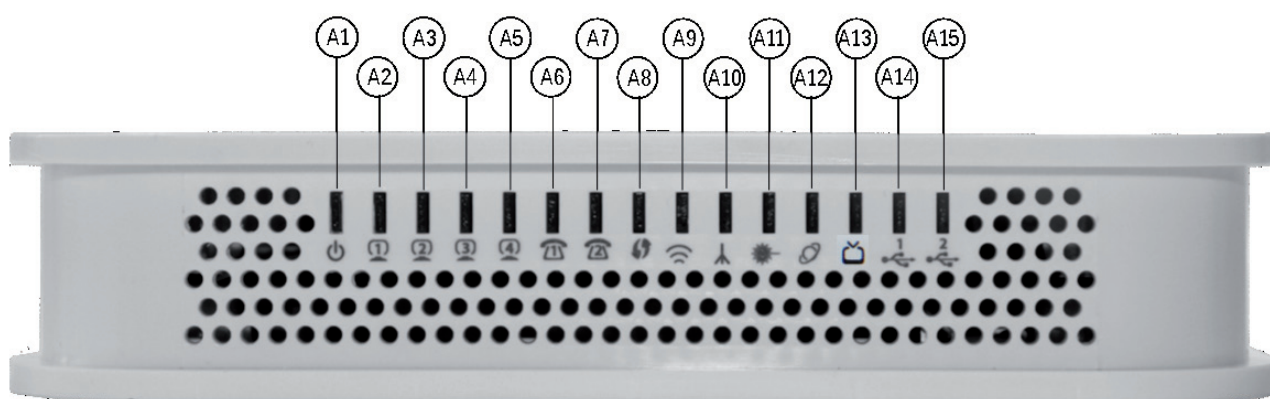


Figure 6-1: Refs. 769501-769502 status LEDs

LED	ID	LED Status	Description
A1 ⁽¹⁾	POWER	ON	Power supply ON (green)
		OFF	Power supply OFF
A2 to A5 ⁽²⁾	ETHERNET	ON	With Ethernet connection (green)
		OFF	No Ethernet connection
		Flashing	Ethernet IN/OUT activity (green)
A6, A7 ⁽²⁾	VOIP	ON	Service configured and authenticated (green)
		OFF	Service not configured or registration failure
		Flashing	Telephone off the hook
A8 ⁽²⁾	WPS	ON	WPS active (blinking green)
		OFF	WPS inactive
A9 ⁽¹⁾	RADIO SIGNAL	ON	Radio signal active
		OFF	Radio signal inactive
A10 ⁽²⁾	GPON LINK	See Table 62	
A11 ⁽²⁾	GPON AUTH		
A12 ⁽²⁾	PPPoE	ON	PPPoE active
		OFF	PPPoE inactive

LED	ID	LED Status	Description
A13 ⁽³⁾	CATV ⁽³⁾	ON	Port administratively connected
		OFF	Port administratively disconnected
		Flashing	Port administratively connected to CATV
A14, A15	USB	ON	USB ON (green)
		OFF	USB OFF

Table 6-1: LED status

NOTES:

- (1) These status LEDs are always update (pressing ECO button is not required).
- (2) To obtain these status LEDs information ECO button must be pressed.
- (3) Optional; Dependent on the Refs. 769501-769502 specific model.

The following combination of GPON LINK (A10) and AUTH (A11) LEDs reflects the various states that the Refs. 769501-769502 is in during the process of configuration and communication with the OLT (Optical Line Terminal).

Refs. 769501-769502 Status	LED Status		Description
	GPON LINK (A10)	GPON AUTH (A11)	
1 - Initial	OFF	OFF	Initial State
2 - Standby	Flashing	OFF	Refs. 769501-769502 is waiting for initial configuration by the OLT
3 - Serial-Number	Flashing	Flashing	The OLT is configuring the Refs. 769501-769502
4 - Ranging	Flashing	ON	Refs. 769501-769502 and OLT synchronisation
5 - Operational	ON	ON	Refs. 769501-769502 normal operational status
6 - POPUP	Flashing	OFF	Loss of optical signal detected
7 - Emergency-Stop	ON	OFF	Anomalous event

Table 6-2: LED states

6.1.2 Troubleshooting

The table below, according to the LEDs status, identifies a possible cause and describes the procedure to fix the problem.

LED	State	Possible Cause	Solution
POWER (A1)	OFF	No power supply to the Refs. 769501-769502	- Check that the power cable is correctly connected to both the Refs. 769501-769502 and the adapter at the electrical socket.
ETHERNET (A2 to A5)	OFF	ETHERNET cable incorrectly connected	- Check that the ETHERNET cable is properly connected to the Refs. 769501-769502's ETHERNET port and the Home Gateway's WAN port and not, for example, to a LAN port. - Change the ETHERNET cable.
GPON LINK (A10)	OFF	Anomaly in the optical fibre signal	- Check that the optical cable is correctly inserted in both the Refs. 769501-769502's internal optical connector and the optical socket. - Check that the fibre is intact, is not dirty and has not been cut or twisted.
AUTH (A11)	OFF		
GPON LINK (A10)	ON	Refs. 769501-769502 deactivated by the administrator	Contact the technical support.
AUTH (A11)	OFF		
CATV (A13) ⁽¹⁾	OFF	CATV deactivated in the 769501-769502	
VOIP (A6 to A7)	OFF	VoIP deactivated in the Refs. 769501-769502	
GPON LINK (A10)	Blinking	Error in Refs. 769501-769502 authentication	

NOTES:

(1) Optional ;

Dependent on the 769501-769502 specific model

Table 6-3: Troubleshooting

7.CLI

7.1 Overview

The aim of this chapter is to describe the commands available from the ONT Gateway CLI.

The CLI has a `/cli>` prompt character, and it is available from the serial console, telnet login, and ssh logins.

CLI has a “directory-like” structure and the command `cd` should be used to navigate through the various nodes.

In order to see a list of available CLI commands, the user can type `tree` (to see all nodes within the current node and respective commands) or `dir` (to see the available commands of the given node).

The command that the user wants to type may need arguments; in order to check the arguments of one command, the user can type `?` after it (ex: `/cli/wan/gre> create ?`).

The same logic can be used with some arguments, for instance, the command `/cli/wan/ipoe> create --interface=?` will return the list of the available interfaces that can be used. (Note that when there is more than one mandatory argument, all of those arguments must be fulfilled, even if the user wants to type `?` in one of them).

The `show` command has a screen output depending on the usage context: node or sub-node current configuration or information is displayed on the screen.

To see the CLI basic usage, type `help`.

To logout/quit CLI, type `quit`.

Some command have restricted availability depending on the user profile permissions.

7.2 Nodes and Commands

7.2.1 “wan” node

This node allows a user to see, to add and/or to delete wan services. The available wan services are: IPoE, PPPoE, Bridging and GRE.

In order to configure one service, the user should enter the respective node (ex: `/cli> cd ipoe`) and then type the desired command.

The user can see the configured wan interfaces by typing `show` on the interfaces node.

```
+ wan[@show]
  + bridge[@create, @remove, @show]
  + gre[@create, @remove, @show]
  + interfaces[@show]
  + ipoe[@create, @remove, @show]
  + pppoe[@create, @remove, @show]
```

Figure 7-1: wan node tree

7.2.1.1 Permissions

Command	Admin	Support	User
/wan/show	Yes	Yes	Yes
/wan/ipoe/create	Yes	Yes	No
/wan/ipoe/remove	Yes	Yes	No
/wan/ipoe/show	Yes	Yes	Yes
/wan/pppoe/create	Yes	Yes	No
/wan/pppoe/remove	Yes	Yes	No
/wan/pppoe/show	Yes	Yes	Yes
/wan/gre/create	Yes	Yes	No
/wan/gre/remove	Yes	Yes	No
/wan/gre/show	Yes	Yes	Yes
/wan/bridge/create	Yes	Yes	No
/wan/bridge/remove	Yes	Yes	No
/wan/bridge/show	Yes	Yes	Yes
/wan/interfaces/show	Yes	Yes	No

Table 7-1: wan node and sub-node tree command permissions

7.2.1.2 “bridge” sub-node

7.2.1.2.1 “create” command

Name	create	
Description	Creates a new bridging service	
Full path	/wan/bridge/create	
Arguments		
<MANDATORY>	--interface	WAN L2 Interface
[OPTIONAL]	--igmp-mcast	IGMP Multicast <enable disable> (disable by default)
	--mld-mcast	MLD Multicast <enable disable> (disable by default)
	--pbit	802.1P Priority [0-7] (-1 by default)
	--service-name	Service description
	--vlan	802.1Q VLAN ID [0-4094] (-1 by default)

Table 7-2: “create” command information

7.2.1.2.2 “remove” command

Name	remove	
Description	Removes an existing bridging service	
Full path	/wan/bridge/remove	
Arguments		
<MANDATORY>	--if-to-rmv	WAN Interface

Table 7-3: “remove” command information

7.2.1.3 “gre” sub-node

7.2.1.3.1 “create” command

Name	create	
Description	Creates a new GRE service	
Full path	/wan/gre/create	
Arguments		
<MANDATORY>	--interface	Interface
	--remote-ip	Remote IP
	--tunnel-name	Tunnel Name
[OPTIONAL]	--local-ip	Local IP
	--peer-ip	Peer IP
	--ttl	TTL [0, 255]
	--tunnel-ip	Tunnel IP
	--tunnel-mask	Tunnel mask

Table 7-4: “create” command information

7.2.1.3.2 “remove” command

Name	remove	
Description	Removes an existing GRE service	
Full path	/wan/gre/remove	
Arguments		
<MANDATORY>	--tunnel-name	Tunnel Name

Table 7-5: “remove” command information

7.2.1.4 “interfaces” sub-node

7.2.1.5 “ipoe” sub-node

7.2.1.5.1 “create” command

Name	create	
Description	Creates a new IPoE service	
Full path	/wan/ipoe/create	
Arguments		
<MANDATORY>	--interface	Interface

[OPTIONAL]

--arping	ArpPing <enable disable> (disable by default)
--dhcp-client	DHCP Client <enable disable> (enable by default)
--dhcp-op125	DHCP Option 125 <enable disable> (disable by default)
--dhcp-op60-vid	DHCP Option 60 Vendor ID
--dhcp-op61-duid	DHCP Option 61 DUID (hexadecimal digit)
--dhcp-op61-iaid	DHCP Option 61 IAID (8 hexadecimal digits)
--dhcp6c-iana	Launch Dhcp6c for Address Assignment (IANA) <enable disable> (disable by default)
--dhcp6c-iapd	Launch Dhcp6c for Prefix Delegation (IAPD) <enable disable> (enable by default)
--firewall	Firewall <enable disable> (disable by default)
--fullcone	Fullcone NAT <enable disable> (disable by default)
--igmp	IGMP Multicat Proxy <enable disable> (disable by default)
--igmp-mcast-src	IGMP Multicast Source <enable disable> (disable by default)
--ip-version	Network Protocol <ipv4 ipv6 dual> (IPv4 by default)
--mld	MLD Multicat Proxy <enable disable> (disable by default)
--mld-mcast-src	MLD Multicast Source <enable disable> (disable by default)
--nat	NAT <enable disable> (disable by default)
--nat-mask	Subnet mask
--nat-masquerade	NAT Masquerade <enable disable> (disable by default)
--nat-max-add	End IP Address
--nat-min-add	Start IP Address
--no-mcast-vlan-filter	Multicast VLAN Filter <enable disable> (disable by default)
--nr-rep	ArpPing number of repetitions [1, 255] (3 by default)
--pbit	802.1P Priority [0-7] (No PBIT by default)
--service-name	Service description
--timeout	ArpPing timeout (sec) [30, 3600] (3600 by default)
--tpid	VLAN TPID <0x8100 0x88A8 0x9100> (No VLAN TPID by default)
--vlan	802.1Q VLAN ID [0-4094] (No VLAN by default)
--wan-gw	WAN gateway IP Address
--wan-ip-add	WAN IP Address
--wan-ipv6-add	Static IPv6 Address <WAN IPv6 Address/Prefix Length>. If the address prefix length is not specified, it will be default to /64.
--wan-ipv6-next-hop	WAN Next-Hop IPv6 Address
--wan-mask	WAN subnet mask

Table 7-6: "create" command information

7.2.1.5.2 “remove” command

Name	remove
Description	Removes an existing IPoE service
Full path	/wan/ipoe/remove
Arguments	
<MANDATORY>	--if-to-rmv WAN Interface

Table 7-7: “remove” command information

7.2.1.6 “pppoe” sub-node

7.2.1.6.1 “create” command

Name	create
Description	Creates a new PPPoE service
Full path	/wan/pppoe/create
Arguments	
<MANDATORY>	--interface Interface
[OPTIONAL]	--auth-error-retry Authentication error retry <enable disable> (disable by default)
	--auth-method Authentication method <AUTO PAP CHAP MSCHAP> (AUTO by default)
	--debug PPP Debug Mode <enable disable> (disable by default)
	--dhcp6c-iana Launch Dhcp6c for Address Assignment (IANA) <enable disable> (disable by default)
	--dhcp6c-iapd Launch Dhcp6c for Prefix Delegation (IAPD) <enable disable> (enable by default)
	--firewall Firewall <enable disable> (disable by default)
	--fullcone Fullcone NAT <enable disable> (disable by default)
	--igmp IGMP Multicat Proxy <enable disable> (disable by default)
	--igmp-mcast-src IGMP Multicast Source <enable disable> (disable by default)
	--ipv4-add Static IPv4 Address
	--ipv6-add Static IPv6 Address
	--ipv6-unnumbered-model IPv6 Unnumbered model <enable disable> (enable by default)
	--mld MLD Multicat Proxy <enable disable> (disable by default)
	--mld-mcast-src MLD Multicast Source <enable disable> (disable by default)
	--ip-version Network Protocol <ipv4 ipv6 dual> (IPv4 by default)
	--no-mcast-vlan-filter Multicast VLAN Filter <enable disable> (disable by default)
	--on-demand Dial on demand (with idle timeout timer) <enable disable>
	--password PPP Password
	--pbit 802.1P Priority [0-7] (-1 by default)
	--server-name PPPoE server name
	--service-name Service description
	--timeout Inactivity Timeout (minutes) [1-4320]
	--to-bridge Bridge PPPoE Frames Between WAN and Local Ports <enable disable> (disable by default)
	--tpid VLAN TPID <0x8100 0x88A8 0x9100> (-1 by default)
	--username PPP Username
	--vlan 802.1Q VLAN ID [0-4094] (-1 by default)

Table 7-8: “create” command information

7.2.1.6.2 “remove” command

Name	remove
Description	Removes an existing PPPoE service
Full path	/wan/pppoe/remove
Arguments	
<MANDATORY>	--if-to-rmv WAN Interface

Table 7-9: “remove” command information

7.2.2 “lan” node

This node allows a user to configure the LAN settings. It allows the configuration of generic LAN settings, as well as setup the LAN VLAN and the configuration of the available Ethernet LAN ports.

```
+ lan[@config, @show]
  + interfaces[@config, @show]
  + static-lease[@create, @remove, @show]
  + vlan[@create, @remove, @show]
```

Figure 7-2: lan node tree

7.2.2.1 Permissions

Command	Admin	Support	User
/lan/show	Yes	Yes	Yes
/lan/config	Yes	Yes	Yes
/lan/interfaces/show	Yes	Yes	No
/lan/interfaces/config	Yes	Yes	No
/lan/static-lease/create	Yes	Yes	No
/lan/static-lease /remove	Yes	Yes	No
/lan/static-lease /show	Yes	Yes	No
/lan/vlan/create	Yes	Yes	No
/lan/vlan /remove	Yes	Yes	No
/lan/vlan/show	Yes	Yes	No

Table 7-10: lan node and sub-node tree command permissions

7.2.2.2 “config” command

Name	config	
Description	Configures the LAN	
Full path	/lan/config	
Arguments		
[OPTIONAL]	--default-gw	Default gateway (0.0.0.0 by default)
	--dhcp-end	DHCP End IP address (192.168.1.254 by default)
	--dhcp-server	DHCP Server <enable disable> (enable by default)
	--dhcp-start	DHCP Start IP address (192.168.1.2 by default)
	--dns-primary	Primary DNS (0.0.0.0 by default)
	--dns-sec	Secondary DNS
	--firewall default)	LAN side firewall <enable disable> (disable by default)
	--igmp-mode default)	IGMP mode <standard blocking> (blocking by default)
	--igmp-snoop default)	IGMP Snooping <enable disable> (enable by default)
	--ip-add	IP address (192.168.1.1 by default)
	--lan-to-lanMcast	IGMP LAN to LAN Multicast
		<enable disable> (disable by default)
	--lan2	Secondary Server (for DHCP Option 60)
		<enable disable> (disable by default)
	--lan2-dns-prim	Sec. server primary DNS
	--lan2-end	Sec. server end IP address
	--lan2-ip	Sec. server IP address
	--lan2-leased-time	Sec. server leased time (minutes)
	--lan2-mask	Sec. server subnet mask
	--lan2-ntp	NTP server
	--lan2-sec-dns	Sec. server secondary DNS
	--lan2-start	Sec. server start IP address
	--lan2-tftp	TFTP server
	--lan2-vendor-id	Sec. server vendor ID
	--leased-time	Leased Time (hours) (24 by default)
	--mask	Subnet mask (255.255.255.0 by default)

Table 7-11: “config” command information

7.2.2.3 “interfaces” sub-node

7.2.2.3.1 “config” command

Name	config
Description	Configure the state of the Ethernet LAN ports
Full path	/lan/interfaces/config
Arguments	
<MANDATORY>	--interface LAN Interface
[OPTIONAL]	--admin-status Admin status <UP DOWN> (UP by default)
	--speed Speed (Mb/s) <AUTO 10 100> (AUTO by default)

Table 7-12: “config” command information

7.2.2.4 “static-lease” sub-node

7.2.2.4.1 “create” command

Name	create
Description	Creates a new entry on the static IP lease list
Full path	/lan/static-lease/create
Arguments	
<MANDATORY>	--ip IP address
	--mac MAC address

Table 7-13: “create” command information

7.2.2.4.2 “remove” command

Name	remove
Description	Removes an existing entry on the static IP lease list
Full path	/lan/static-lease/remove
Arguments	
<MANDATORY>	--mac-to-rmv MAC address to remove

Table 7-14: “remove” command information

7.2.2.5 “vlan” sub-node

7.2.2.5.1 “create” command

Name	create	
Description	Creates a new LAN VLAN entry	
Full path	/lan/vlan/create	
Arguments		
<MANDATORY>	--interface	LAN interface
[OPTIONAL]	--taglist	vid1/pbit1 ... vidN/pbitN
	--vlan-mode	VLAN Mode ON/OFF

Table 7-15: “create” command information

7.2.2.5.2 “remove” command

Name	remove	
Description	Removes an existing entry on the LAN VLAN list	
Full path	/lan/vlan/remove	
Arguments		
<MANDATORY>	--interface	LAN interface
[OPTIONAL]	--id	Table Entry ID

Table 7-16: “remove” command information

7.2.3 “nat” node

This node allows a user to configure the NAT (Network Address Translation) settings.

```
+ nat[]
+ dmz-host[@config, @show]
+ nat1:1[@create, @remove, @show]
+ port-triggering[@create, @remove, @show]
+ virtual-servers[@create, @remove, @show]
```

Figure 7-3: nat node tree

7.2.3.1 Permissions

Command	Admin	Support	User
/nat/dmz-host/show	Yes	No	No
/nat/dmz-host/config	Yes	No	No
/nat/nat1:1/create	Yes	No	No
/nat/nat1:1/remove	Yes	No	No
/nat/nat1:1/show	Yes	No	No
/nat/port-triggering /create	Yes	No	No
/nat/port-triggering /remove	Yes	No	No
/nat/port-triggering /show	Yes	No	No
/lan/virtual-servers/create	Yes	Yes	Yes
/lan/virtual-servers/remove	Yes	Yes	Yes
/lan/virtual-servers/show	Yes	Yes	Yes

Table 7-17: nat node and sub-node tree command permissions

7.2.3.2 “dmz-host” sub-node

The Refs. 769501-769502 will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer. The user should pass the DMZ Host IP address as a parameter.

7.2.3.2.1 “config” command

Name	config
Description	Configure the state of the Ethernet LAN ports
Full path	/nat/dmz-host/config
Arguments	
<MANDATORY>	--ip-address DMZ Host IP Address

Table 7-18: “config” command information

7.2.3.3 “nat1:1” sub-node

1:1 NAT is a mode of NAT that maps one internal address to one external address

7.2.3.3.1 “create” command

Name	create	
Description	Creates a new entry on the NAT 1:1 list	
Full path	/nat/nat1:1/create	
Arguments		
<MANDATORY>	--lan-ip	LAN IP
	--name	Name
	--public-ip	Public IP
	--wan-interface	WAN interface

Table 7-19: “create” command information

7.2.3.3.2 “remove” command

Name	remove	
Description	Removes an existing entry on the NAT 1:1 list	
Full path	/nat/nat1:1/remove	
Arguments		
<MANDATORY>	--name	Name

Table 7-20: “remove” command information

7.2.3.4 “port-triggering” sub-node

Some applications require that specific ports in the Router’s firewall be opened for access by the remote parties. Port Trigger dynamically opens up the ‘Open Ports’ in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the ‘Triggering Ports’. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the ‘Open Ports’.

7.2.3.4.1 “create” command

Name	create	
Description	Creates a new entry on the Port-triggering list	
Full path	/nat/port-triggering/create	
Arguments		
<MANDATORY>	--name	Application Name
	--open-port-end	Open port end
	--open-port-start	Open port start
	--open-proto	Open Protocol <TCP/UDP TCP UDP>
	--trigger-port-end	Trigger port end
	--trigger-port-start	Trigger port start
	--trigger-proto	Trigger Protocol <TCP/UDP TCP UDP>
	--wan-intf	Interface

Table 7-21: “create” command information

7.2.3.4.2 “remove” command

Name	remove	
Description	Removes an existing entry on the port triggering list	
Full path	/nat/port-triggering/remove	
Arguments		
<MANDATORY>	--open-port-end	Open port end
	--open-port-start	Open port start
	--open-proto	Open Protocol <TCP/UDP TCP UDP>
	--trigger-port-end	Trigger port end
	--trigger-port-start	Trigger port start
	--trigger-proto	Trigger Protocol <TCP/UDP TCP UDP>
	--wan-intf	Interface

Table 7-22: “remove” command information

7.2.3.5 “virtual-servers” sub-node

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

7.2.3.5.1 “create” command

Name	create	
Description	Creates a new entry on the Virtual-Servers list	
Full path	/nat/virtual-servers/create	
Arguments		
<MANDATORY>	--ext-port-end	External port end
	--ext-port-start	External port start
	--int-port-start	Internal port start
	--protocol	Protocol <TCP/UDP TCP UDP>
	--server-ip	Server IP address
	--server-name	Service Name
	--wan-intf	Interface
[OPTIONAL]	--int-port-end	Internal port end
	(if not set it will have the same value as External Port End)	

Table 7-23: “create” command information

7.2.3.5.2 “remove” command

Name	Remove	
Description	Removes an existing entry on the Virtual-Servers list	
Full path	/nat/virtual-servers/remove	
Arguments		
<MANDATORY>	--ext-port-end	External port end
	--ext-port-start	External port start
	--int-port-start	Internal port start
	--protocol	Protocol <TCP/UDP TCP UDP>
	--server-ip	Server IP address
[OPTIONAL]	--int-port-end	Internal port end
	(if not set it will have the same value as External Port End)	

Table 7-24: “remove” command information

7.2.4 “dns” node

This node allows a user to configure the DNS (Domain Name Server) server, as well as the the DNS proxy and the dynamic DNS service provider account information.

+ dns[]
+ dynamic[@create, @remove, @show]
+ proxy[@config, @show]
+ server[@config, @show]

Figure 7-4: dns node tree

7.2.4.1 Permissions

Command	Admin	Support	User
/dns/server/show	Yes	Yes	No
/dns/server/config	Yes	Yes	No
/dns/proxy/show	Yes	Yes	No
/dns/proxy/config	Yes	Yes	No
/dns/dynamic/show	Yes	Yes	No
/dns/dynamic /create	Yes	Yes	No
/dns/dynamic /remove	Yes	Yes	No

Table 7-25: dns node and sub-node tree command permissions

7.2.4.2 “server” sub-node

This subnode is used to select a DNS Server Interface from available WAN interfaces or to enter a static DNS server IP addresses for the system.

DNS Server Interfaces can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

7.2.4.2.1 “config” command

Name	config
Description	Configures a new entry on the DNS server interfaces list
Full path	/dns/server/config
Arguments	
[OPTIONAL]	--dns-primary Primary DNS server
	--dns-secondary Secondary DNS server
	--dns-server DNS server interfaces list <intf1,...,intfN>
	--dnsv6-primary Primary IPv6 DNS server
	--dnsv6-secondary Secondary IPv6 DNS server
	--dnsv6-wan WAN IPv6 DNS interface

Table 7-26: “config” command information

7.2.4.3 “proxy” sub-node

This subnode can be used by the user to enable/disable and to configure a DNS proxy.

7.2.4.3.1 “config” command

Name	config
Description	Configures the DNS proxy
Full path	/dns/proxy/config
Arguments	
<MANDATORY>	--enable Enable DNS Proxy <yes no>
[OPTIONAL]	--domain-name Domain name of the LAN network (Home by default)
	--hostname Host name of the Broadband Router (Broadcom by default)

Table 7-27: “config” command information

7.2.4.4 “dynamic” sub-node

The Dynamic DNS service allows the user to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

7.2.4.4.1 “create” command

Name	create	
Description	Creates a new entry	
Full path	/dns/dynamic/create	
Arguments		
<MANDATORY>	--hostname	Hostname
	--interface	Interface
	--password	Password
	--service	D-DNS provider <DynDNS.org/TZO>
	--username	Username

Table 7-28: “create” command information

7.2.4.4.2 “remove” command

Name	remove	
Description	Removes an existing entry	
Full path	/dns/dynamic/remove	
Arguments		
<MANDATORY>	--hostname	Hostname

Table 7-29: “remove” command information

7.2.5 “qos” node

This node allows a user to configure some Qos (Quality of Service) traffic rules. If the QoS option is disabled, then all QoS will be disabled for all interfaces. Besides, the default DSCP mark is used to mark all egress packets that do not match any classification rules.



Figure 7-5: qos node tree

7.2.5.1 Permissions

Command	Admin	Support	User
/qos/config	Yes	Yes	No
/qos/show	Yes	Yes	No
/qos/policer/create	Yes	Yes	No
/qos/policer/remove	Yes	Yes	No
/qos/policer/show	Yes	Yes	No
/qos/queue/create	Yes	Yes	No
/qos/queue /remove	Yes	Yes	No
/qos/queue /show	Yes	Yes	No

Table 7-30: qos node and sub-node tree command permissions

7.2.5.2 “config” command

Name	config	
Description	Configures the QoS	
Full path	/qos/config	
Arguments		
<MANDATORY>	--qos	QoS <enable disable>
[OPTIONAL]	--dscp	Default DSCP Mark (-1 by default)

Table 7-31: “config” command information

7.2.5.3 “policer” sub-node

This sub-node is used to add a QoS policer.

7.2.5.3.1 “create” command

Name	create
Description	Creates a new policer
Full path	/qos/policer/create
Arguments	
<MANDATORY>	--committed-burst-size Committed Burst Size (bytes)
	--committed-rate Committed Rate (kbps)
	--enable Enable <yes no>
	--meter Meter type <Simple Token Bucket(1) Single Rate Three Color(2) TwoRate Three Col- or(3)>
	--name Name
[OPTIONAL]	--conform-action Conforming Action <Null DSCP> (Null by default)
	--dscp DSCP Mark
	--excess-burst-size Excess Burst Size (bytes)
	--non-conform-action Nonconforming Action <Null Drop DSCP> (Null by default)
	--partial-conform-action Partial Conforming Action <Null Drop DSCP> (Null by default)
	--peek-burst-size Peak Burst Size (bytes)
	--peek-rate Peak Rate (kbps)

Table 7-32: “create” command information

7.2.5.3.2 “remove” command

Name	remove
Description	Removes an existing policer
Full path	/qos/policer/remove
Arguments	
<MANDATORY>	--key Key of entry to remove

Table 7-33: “remove” command information

7.2.5.4 “queue” sub-node

This sub-node allows the user to setup a QoS queue.

7.2.5.4.1 “create” command

Name	create
Description	Creates a new QoS queue
Full path	/qos/queue/create
Arguments	
<MANDATORY>	--enable[=STRING] Enable <yes no>
	--interface Interface
	--name Name
	--queue-precedence Queue Precedence (lower value, higher priority) [1-8]
	--sched-alg Scheduler Algorithm <Strict Priority(SP) Weighted Round Robin(WRR)>
[OPTIONAL]	--min-rate Minimum Rate [1-100000 Kbps] (-1 indicates no shaping) (-1 by default)
	--queue-weigth Queue weight [1-63]

Table 7-34: “create” command information

7.2.5.4.2 “remove” command

Name	remove
Description	Removes an existing QoS queue
Full path	/qos/queue/remove
Arguments	
<MANDATORY>	--key Key of entry to remove

Table 7-35: “remove” command information

7.2.6 “voice” node

This node can be used to configure the voice-related parameters. Only SIP is supported and there are two SIP accounts available.

This command also allows the start/stop of the voice application, as well as restoring the settings to their default values.

NOTE: At this point, only the configuration of basic voice parameters is supported. Full support must be available in the next versions.

```
+ voice[@restore-default, @show, @start, @stop]
+ sip[@config, @show]
+ account0[@config, @show]
+ account1[@config, @show]
```

Figure 7-6: voice node tree

7.2.6.1 Permissions

Command	Admin	Support	User
/voice/restore-default	Yes	Yes	No
/voice/show	Yes	Yes	Yes
/voice/start	Yes	Yes	No
/voice/stop	Yes	Yes	No
/voice/sip/show	Yes	Yes	No
/voice/sip/config	Yes	Yes	No
/voice/sip /account0/show	Yes	Yes	No
/voice/sip /account0/config	Yes	Yes	No
/voice/sip /account1/show	Yes	Yes	No
/voice/sip /account1/config	Yes	Yes	No

Table 7-36: voice node and sub-node tree command permissions

7.2.6.2 “sip” sub-node

This sub-node is used to configure the basic SIP settings (non-account-related).

7.2.6.2.1 “config” command

Name	config
Description	Configures basic SIP settings
Full path	/voice/sip/config
Arguments	
[OPTIONAL]	--bound-if Bound Interface Name <LAN Any_WAN (WAN IfName, e.g. veip0.1)
	--dialplan Voip Dialplan Setting (x+T by default)
	--ip-version IP Address Family <IPv4 IPv6> (IPv4 by default)
	--locale Locale selection (PRT by default)
	--outbound-proxy SIP Outbound Proxy <hostname IP> (0.0.0.0 by default)
	--outbound-proxy-port SIP Outbound Proxy Port (5060 by default)
	--proxy SIP Proxy <hostname IP> (0.0.0.0 by default)
	--proxy-port SIP Proxy Port (5060 by default)
	--registrar SIP Registrar <hostname IP> (0.0.0.0 by default)
	--registrar-port SIP Registrar Port (5060 by default)

Table 7-37: “config” command information

7.2.6.2.2 “account0/1” sub-nodes

These sub-nodes allows a user to setup the proper SIP account.

7.2.6.2.2.1 “config” command

Name	config
Description	Configures SIP accounts
Full path	/voice/sip/account0/config /voice/sip/account1/config
Arguments	
[OPTIONAL]	--account Activate line <on off> (on by default)
	--auth-name SIP authentication name
	--codec-list Codec priority list <codec(1)[,codec(2)]>
	--disp-name SIP Display Name
	--extension SIP extension
	--password SIP authentication password
	--phys-endpt Physical Terminal Assignment <0 1 0,1>
	--pref-time Packetization period <10 20 30> (20 by default)

Table 7-38: “config” command information

7.2.7 “security” node

This node allows the configuration of some security settings.

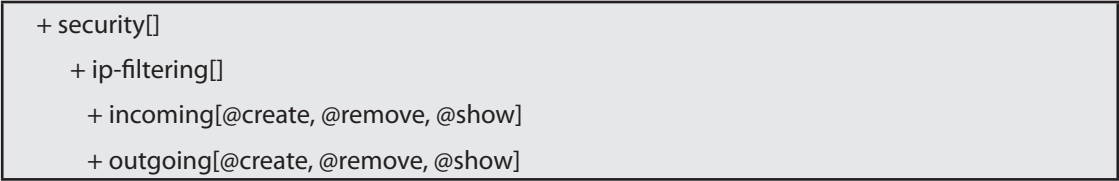


Figure 7-7: security node tree

7.2.7.1 Permissions

Command	Admin	Support	User
/security/ip-filtering/incoming/create	Yes	No	No
/security /ip-filtering/incoming/remove	Yes	No	No
/security /ip-filtering/incoming/show	Yes	No	No
/security /ip-filtering/outgoing/create	Yes	No	No
/security /ip-filtering/outgoing/remove	Yes	No	No
/security /ip-filtering/outgoing/show	Yes	No	No

Table 7-39: security node and sub-node tree command permissions

7.2.7.2 “ip-filtering” sub-node

7.2.7.2.1 “incoming” sub-node

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be ACCEPTED by setting up filters. The aim of this sub-node is to allow the configuration of those filters.

EN

7.2.7.2.1.1 “create” command

Name	create	
Description	Creates a filter	
Full path	/security/ip-filtering/incoming/create	
Arguments		
<MANDATORY>	--dest-ip	Destination IP address
	--dest-port	Destination port
	--interfaces	WAN Interfaces (configured in Routing mode and with firewall enabled) and LAN interfaces <ALL or intf1[intf2 ...]>
	--ip-version	IP version <IPv4 IPv6>
	--name	Filter name
	--protocol	Protocol <TCP UDP TCP UDP ICMP>
	--src-ip	Source IP address
	--src-port	Source port

Table 7-40: “create” command information

7.2.7.2.2 “remove” command

Name	remove	
Description	Removes an existing filter	
Full path	/security/ip-filtering/incoming/remove	
Arguments		
<MANDATORY>	--name-to-rmv	Filter name to remove

Table 7-41: “remove” command information

7.2.7.2.3 “outgoing” sub-node

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. The aim of this sub-node is to allow the configuration of those filters.

7.2.7.2.3.1 “create” command

Name	create	
Description	Creates a filter	
Full path	/security/ip-filtering/outgoing/create	
Arguments		
<MANDATORY>	--dest-ip	Destination IP address
	--dest-port	Destination port
	--ip-version	IP version <IPv4 IPv6>
	--name	Filter name
	--protocol	Protocol <TCP UDP TCP UDP ICMP>
	--src-ip	Source IP address
	--src-port	Source port

Table 7-42: “create” command information

7.2.7.2.4 “remove” command

Name	remove	
Description	Removes an existing filter	
Full path	/security/ip-filtering/ougoing/remove	
Arguments		
<MANDATORY>	--name-to-rmv	Filter name to remove

Table 7-43: “remove” command information

7.2.8 “routing” node

This node allows the configuration of some routing settings.

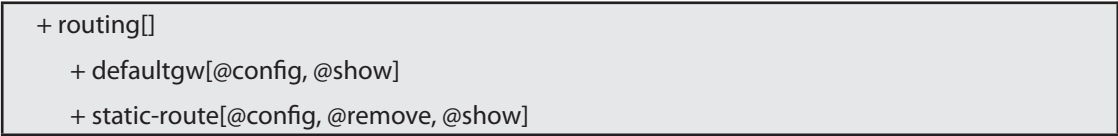


Figure 7-8: routing node tree

7.2.8.1 Permissions

Command	Admin	Support	User
/routing/defaultgw/config	Yes	Yes	No
/routing /defaultgw /show	Yes	Yes	No
/routing /static-route/config	Yes	Yes	No
/routing /static-route/remove	Yes	Yes	No
/routing /static-route/show	Yes	Yes	Yes

Table 7-44: routing node and sub-node tree command permissions

7.2.8.2 “defaultgw” sub-node

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

7.2.8.2.1 “config” command

Name	config	
Description	Enters the default gateway interface list	
Full path	/routing/defaultgw/config	
Arguments		
<MANDATORY>	--default-mode	Default gateway mode <WAN/LAN>
[OPTIONAL]	--default-gw6-ifc	Default WAN IPv6 gateway
	--default-list	Selected Default Gateway Interfaces <intf1,...intfN>
	--lan-address	Default Gateway IP Address
	--lan-bridge	LAN Interface (Default by default)

Table 7-45: “config” command information

7.2.8.3 “static-route” sub-node

This sub-node allows the user to configure static routes.

7.2.8.3.1 “config” command

Name	config	
Description	Creates a static route	
Full path	/routing/static-route/config	
Arguments		
<MANDATORY>	--dest-ip	Destination IP address/prefix length
	--gw-address	Gateway IP address
	--interface	Interface
[OPTIONAL]	--ip-version	IP Version <IPv4 IPv6> (IPv4 by default)
	--metric	Metric

Table 7-46: “config” command information

7.2.8.3.2 “remove” command

Name	remove	
Description	Removes an existing static route	
Full path	/routing/static-route/remove	
Arguments		
<MANDATORY>	--dest-ip	Destination IP address/prefix length

Table 7-47: “remove” command information

7.2.9 “multicast” node

This node allows the user to setup multicast. It can be configured some IGMP and MLD parameters.

```
+ multicast[@config, @show]
```

Figure 7-9: multicast node tree

7.2.9.1 Permissions

Command	Admin	Support	User
/multicast/config	Yes	Yes	No
/multicast/show	Yes	Yes	No

Table 7-48: multicast node command permissions

7.2.9.2 “config” command

Name	config	
Description	Configures multicast	
Full path	/multicast/config	
Arguments		
[OPTIONAL]	--igmp-fast-leave	IGMP Fast Leave <enable disable> (enable by default)
	--igmp-last-member-query-int	IGMP Last Member Query Interval (10 by default)
	--igmp-max-groups	IGMP Maximum Multicast Groups (25 by default)
	--igmp-max-members default)	IGMP Maximum Multicast Group Members (25 by default)
	--igmp-max-sources	IGMP Maximum Multicast Data Sources (for IGMPv3) (10 by default)
	--igmp-query-int	IGMP Query Interval (125 by default)
	--igmp-query-resp-int	IGMP Query Response Interval (10 by default)
	--igmp-rv	IGMP Robustness value (2 by default)
	--igmp-version	IGMP Default Version <1 2 3> (2 by default)
	--mld-fast-leave	MLD Fast Leave <enable disable> (enable by default)
	--mld-last-member-query-int	MLD Last Member Query Interval (10 by default)
	--mld-max-groups	MLD Maximum Multicast Groups (10 by default)
	--mld-max-members default)	MLD Maximum Multicast Group Members (10 by default)
	--mld-max-sources	MLD Maximum Multicast Data Sources (for MLDv2) (10 by default)
	--mld-query-int	MLD Query Interval (125 by default)
	--mld-query-resp-int	MLD Query Response Interval (10 by default)
	--mld-rv	MLD Robustness value (2 by default)
	--mld-version	MLD Default Version <1 2> (2 by default)
	--precedence	Multicast precedence <Disable [1,8]> (lower value, higher priority) (Disable by default)

Table 7-49: “config” command information

7.2.10 “diagnostics” node

This node allows the user to check the current status of the equipment LAN and WLAN interfaces.

```
+ diagnostics[@show]
```

Figure 7-10: diagnostics node tree

7.2.10.1 Permissions

Command	Admin	Support	User
/diagnostics/show	Yes	Yes	Yes

Table 7-50: diagnostics node command permissions

7.2.11 “arp” node

This node displays the ARP (Address Resolution Protocol) table.



Figure 7-11: arp node tree

7.2.11.1 Permissions

Command	Admin	Support	User
/arp/show	Yes	Yes	Yes

Table 7-51: arp node command permissions

7.2.12 “device-info” node

This node displays general info about the device (such as serial number, MAC address, software version).



Figure 7-12: device-info node tree

7.2.12.1 Permissions

Command	Admin	Support	User
/device-info/show	Yes	Yes	Yes

Table 7-52: device-info node command permissions

7.2.13 “statistics” node

This node allows the user to view and reset the current WAN/LAN/optical statistics on the device.

The `-option` argument is a mandatory argument to all the commands in this tree and is used to select the type of packets to show, Received, Transmitted or all. The following argument values can be used: `<received|transmitted|all>`.

```
+ statistics[]  
  + lan[@reset, @show]  
  + optical[@reset, @show]  
  + wan[@reset, @show]
```

Figure 7-13: statistics node tree

7.2.13.1 Permissions

Command	Admin	Support	User
/statistics/lan/reset	Yes	Yes	Yes
/statistics/lan/show	Yes	Yes	Yes
/statistics/optical/reset	Yes	Yes	Yes
/statistics/optical/show	Yes	Yes	Yes
/statistics/wan/reset	Yes	Yes	Yes
/statistics/wan/show	Yes	Yes	Yes

Table 7-53: Statistics node and sub-node tree command permissions

7.2.14 “dhcp” node

A DHCP-enabled client obtains a lease for an IP address from a DHCP server. Before the lease expires, the DHCP server must renew the lease for the client or the client must obtain a new lease. This node shows the DHCP leases table.

```
+ dhcp[@show]
```

Figure 7-14: dhcp node tree

7.2.14.1 Permissions

Command	Admin	Support	User
/dhcp/show	Yes	Yes	Yes

Table 7-54: dhcp node command permissions

7.2.15 “upnp” node

This node is used to enable/disable UPnP (Universal Plug and Play). UPnP is activated only when there is a live WAN service with NAT enabled.

```
+ upnp[@config, @show]
```

Figure 7-15: upnp node tree

7.2.15.1 Permissions

Command	Admin	Support	User
/upnp/config	Yes	Yes	No
/upnp/show	Yes	Yes	No

Table 7-55: upnp node command permissions

7.2.15.2 “config” command

Name	config
Description	Configures UPnP
Full path	/upnp/config
Arguments	
<MANDATORY>	--enable Enable UPnP <yes no>

Table 7-56: “config” command information

7.2.16 “intf-grouping” node

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network.

```
+ intf-grouping[@config, @remove, @show]
```

Figure 7-16: intf-grouping node tree

7.2.16.1 Permissions

Command	Admin	Support	User
/intf-grouping/config	Yes	No	No
/intf-grouping/remove	Yes	No	No
/intf-grouping/show	Yes	No	No

Table 7-57: intf-grouping node command permissions

7.2.16.2 “config” command

Name	config	
Description	Configures interface grouping	
Full path	/intf-grouping/config	
Arguments		
<MANDATORY>	--group-name	Group name
	--lan-intf	LAN interfaces to group <intf1[intf2 ...]>
[OPTIONAL]	--routing-mode	Routing mode <enable disable> (disable by default)
	--vendor-id0	Automatically Add Clients With the following DHCP Vendor ID 0
	--vendor-id1	Automatically Add Clients With the following DHCP Vendor ID 1
	--vendor-id2	Automatically Add Clients With the following DHCP Vendor ID 2
	--vendor-id3	Automatically Add Clients With the following DHCP Vendor ID 3
	--vendor-id4	Automatically Add Clients With the following DHCP Vendor ID 4
	--wan-intf	WAN Interface used in the grouping (None by default)

Table 7-58: “config” command information

7.2.16.3 “remove” command

Name	remove	
Description	Removes an existing Interface Grouping entry	
Full path	/intf-grouping/remove	
Arguments		
<MANDATORY>	--group-name-to-rmv	Group name to remove

Table 7-59: “remove” command information

7.2.17 “management” node

The aim of this section is to allow users to perform management functions over the Refs. 769501-769502.

```
+ management[@backup, @reboot, @restore-default, @update-settings, @update-software]
+ access-control[@change-pw]
+ new-users[@create, @remove, @show]
+ security-log[@reset, @show]
+ snmp[@config, @show]
+ system-log[@config, @show]
```

Figure 7-17: management node tree

7.2.17.1 Permissions

Command	Admin	Support	User
/management/reboot	Yes	Yes	No
/management /restore-default	Yes	Yes	No
/management /backup	Yes	Yes	No
/management /update-settings	Yes	Yes	No
/management /update-software	Yes	Yes	No
/management /access-control/change-pw	Yes	Yes	Yes
/management /access-control/new-users/create	Yes	Yes	No
/management /access-control/ new-users/remove	Yes	Yes	No
/management /access-control/ new-users/show	Yes	Yes	No
/management /security-log/reset	Yes	Yes	No
/management /security-log/show	Yes	Yes	No
/management /snmp/config	Yes	Yes	No
/management /snmp/show	Yes	Yes	No
/management /system-log/config	Yes	Yes	Yes
/management /system-log/show	Yes	Yes	Yes

Table 7-60: manegement node and sub-nodes command permissions

7.2.17.2 “backup” command

Name	backup
Description	Backups settings (saves a file named backupsettings.conf on the TFTP address)
Full path	/management/backup
Arguments	
<MANDATORY>	--tftp-server-ip TFTP server IP address

Table 7-61: “backup” command information

7.2.17.3 “update-settings” command

Name	update-settings	
Description	Update settings	
Full path	/management/update-settings	
Arguments		
<MANDATORY>	--config-file	Settings file name
	--tftp-server-ip	TFTP server IP address

Table 7-62: “update-settings” command information

7.2.17.4 “update-software” command

Name	update-software	
Description	Updates software	
Full path	/management/update-software	
Arguments		
<MANDATORY>	--sw-image	Software image name
	--tftp-server-ip	TFTP server IP address

Table 7-63: “update-software” command information

7.2.17.5 “access-control” sub-node

7.2.17.5.1 “change-pwd” command

Name	change-pwd	
Description	Changes the user’s current password	
Full path	/management/access-control/change-pwd	
Arguments		
<MANDATORY>	--new-pw	New password
	--old-pw	Old password
	--username	User name

Table 7-64: “change-pwd” command information

7.2.17.5.2 “new-users” sub-node

This sub-node allows the creation and removal of new users. It also allows viewing new users already configured.

7.2.17.5.2.1 “create” command

Name	create
Description	Creates a new user
Full path	/management/access-control/new-users/create
Arguments	
<MANDATORY>	--password Password
	--permissions-level Permissions level <admin support user>
	--username User name

Table 7-65: “create” command information

7.2.17.5.2.2 “remove” command

Name	remove
Description	Removes existing users
Full path	/management/access-control/new-users/remove
Arguments	
<MANDATORY>	--user-to-rmv List of usernames to remove <name1[,name2,...]>

Table 7-66: “remove” command information

7.2.17.5.3 “security-log” sub-node

This sub-node allows the user to see and to reset the security log.

7.2.17.5.4 “system-log” sub-node

This sub-node allows the user to see and to reset the system log.

EN

7.2.17.5.5 “snmp” sub-node

This sub-node allows the user to see the configured SNMP client parameters, as well as configure those parameters.

7.2.17.5.5.1 “config” command

Name	config
Description	Configures the SNMP client
Full path	/management/snmp/config
Arguments	
<MANDATORY>	--agent SNMP Agent <enable disable> --auth-mode SNMPv3 Authentication Mode <MD5 SHA> (MD5 by default) --auth-passphrase SNMPv3 Authentication Passphrase (password by default) --auth-trap SNMPv3 Authentication Trap <Enable Disable> (Disable by default) --permissions SNMPv3 Permissions <R RW> (R by default) --priv-mode SNMPv3 Privacy Mode <None DES AES> (None by default) --priv-passphare SNMPv3 Privacy Passphrase [OPTIONAL] --read-community SNMPv2 Read community (public by default) --set-community SNMPv2 Set community (private by default) --system-contact System contact --system-location System location --system-name System name --trap-manager-ip SNMPv3 Trap Manager IP Address (0.0.0.0 by default) --trap-manager-ip SNMPv2 Trap Manager IP (0.0.0.0 by default) --username SNMPv3 Username (default by default)

Table 7-67: “config” command information

7.3 VoIP configuration using CLI

Configuration of Voice on the Refs. 769501-769502 requires an IPoE service on the WAN interface to be used for VoIP. To configure an IPoE service, you must be logged in as admin or support user.

7.3.1 IPoE Service Configuration

STEP 1. Configuration example sequence:

```
/cli> /wan/ipoe/create --interface=veip0 --vlan=11 --pbit=0 --tpid=0x8100 --nat=enable --nat-  
masquerade=enable --dhcp-client=enable  
/cli> /routing/defaultgw/config --default-mode=WAN --default-list=veip0.2
```

STEP 2. To view the current interface configuration

```
/cli> /wan/ipoe/show  
-----  
IPoE Info  
-----  
Interface:          veip0.2  
Description:        ipoe_veip0.11  
Vlan 802.1p:        0  
Vlan Mux ID:        11  
Vlan TPID:          0x8100  
IPv6:               Disabled  
IGMP Proxy:         Disabled  
IGMP Source:        Disabled  
MLD Proxy:          Disabled  
MLD Source:         Disabled  
NAT:                Enabled  
NAT Type:           Masquerade  
Firewall:           Disabled  
Status:             Connected  
IPv4 address:       172.22.211.118  
IPv6 address:       (null)  
-----
```


STEP 3. To view the current default gateway configuration

```
/cli> /routing/defaultgw/show --default-mode=WAN
```

```
+-----+
```

```
|Default Gateway Interfaces |
```

```
+-----+
```

```
|Priority   |Interface |
```

```
+-----+
```

```
|1         |veip0.2  |
```

```
+-----+
```

STEP 4. To view the current DNS server configuration

```
cli> /dns/server/show
```

```
+-----+
```

```
|DNS Server Interfaces |
```

```
+-----+
```

```
|Priority   |Interface |
```

```
+-----+
```

```
|1         |veip0.2  |
```

```
+-----+
```

```
+-----+
|Static DNS Server IPv6                |
```

```
+-----+
```

```
|Primary           |Secondary           |
```

```
+-----+
```

```
|                  |                  |
```

```
+-----+
```

7.3.2 VoIP Configuration

To configure voice on the Refs. 769501-769502 you must be logged in as admin or support user

STEP 1. Voice basic settings configuration example sequence

```
/cli> /voice/sip/config --outbound-proxy=192.168.126.50 --outbound-proxy-port=5060
--proxy=192.168.126.50 --proxy-port=5060 --registrar=192.168.126.50 --registrar-port=5060
/cli> /routing/defaultgw/config --default-mode=WAN --default-list=veip0.2
```

STEP 2. To view the voice current configuration

To configure accounts you must activate the line, provide the display name, authentication name and password, and indicate the Refs. 769501-769502 FXS port to use

```
/cli> /voice/sip/show
```

Global Parameters:

-----BoundIfName : undefined

IP address family : IPv4

Vodsl logLevel : Error

Management Protocol : TR69

Service Provider 0:

Associated Voice Profile : 1

Locale : PRT

DTMFMethod : InBand

HookFlashMethod : None

DigitMap : x+T

Log Server Addr : 0.0.0.0

Log Server Port : 0

T38 : off

V18 : on

RTPDSCPMark : 46

SIP:

Domain :

Port : 5060

Transport : UDP

RegExpires : 0

RegRetryInterval : 20

DSCPMark : 46

Registrar Addr : 192.168.126.50

Registrar Port : 5060

Proxy Addr : 192.168.126.50

Proxy Port : 5060

OutBoundProxy Addr : 192.168.126.50

OutBoundProxy Port : 5060

Music Server Addr : 0.0.0.0

Music Server Port : 0

Conferencing URI : 0

Conferencing Option : Local

To Tag Matching : On

Timer B (in ms) : 32000

Timer F (in ms) : 32000

SRTP Usage Option : Disabled

STEP 3. Voice Account configuration example sequence:

```
cli> /voice/sip/account0/config --auth-name=1010 --disp-name=1010 --extension=1010
--password=andre --phys-endpt=0
```

STEP 4. To view the voice account current configuration

```
cli> /voice/sip/account0/show

Account 0:
-----
  ActivationStatus      : Enabled
  VoipServiceStatus    : Disabled
  CallStatus           : Idle
  Associated LineIns    : 1
  PhysEndpt            : 0
  Extension             : 1010
  DisplayName          : 1010
  AuthName             : 1010
  AuthPwd              : andre
  TxGain               : 0 dB
  RxGain               : 0 dB
  CALLFEATURES:
    MWI                : off
    CallWaiting         : on
    CFWDNum            :
    CallFwdAll          : off
    CallFwdBusy         : off
    CallFwdNoans        : off
    AnonymousOutgoingCall : on
    AnonymousCallRcvBlock : off
    DoNotDisturb        : off
    CallCompOnBusy      : off
    SpeedDial           : off
    WarmLine           : off
    WarmLineNum         :
    CallBarring         : off
    CallBarringMode     : None
    CallBarringPin      : 9999
    CallBarringDigitMap :
    NetPrivacy          : on
    VMWI               : on
  CODECSETTINGS:
    VAD                : on
    pTime              : 20
    CodecList          : (0) G.711ALaw
                      (1) G.729a
                      (2) G.723.1
                      (3) G.726_24
                      (4) G.726_32
                      (5) PCMWIDEBAND
```

STEP 5. Configuration To make effective the configuration just done

```
/cli> /voice/sip/config --bound-if=veip0.2
/ccli> /voice/start
```

European technology **Made in  EU rope**