

User Manual
DG200 Series

VDSL2 & Gigabit Ethernet
Residential Gateway

Issue 1.0
24th June 2009

Inteno Broadband Technology AB

Tel: +46 8 579 190 00

Drivhjulsvägen 22, SE-126 30, Hägersten, Sweden

Copyright © 2008, Inteno Broadband Technology AB

Information in this manual is subject to change without notice. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or scanning, for any purpose, without the written permission of Inteno Broadband Technology AB.

Inteno Broadband Technology AB provides this documentation without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Table of Contents

1	Introduction	1
	Features	1
	Device Requirements	1
2	Getting to know the device.....	3
	Parts Check	3
	Front Panel	4
	Rear Panel.....	5
3	Connecting your device.....	6
	Connecting the Hardware	6
	<i>Step 1. Connect the WAN port to ADSL network</i>	<i>7</i>
	<i>Step 2. Connect the Ethernet cable.....</i>	<i>7</i>
	<i>Step 3. Attach the power connector.....</i>	<i>7</i>
	<i>Step 4. Configure your Ethernet PCs</i>	<i>7</i>
	<i>Or, step 5. Install a Wireless card or dongle to the PCs if these machines do not have Ethernet port, or wireless connection is preferred.....</i>	<i>7</i>
	Next step.....	7
4	Getting Start with the Web pages.....	8
	Accessing the Web pages	8
	Testing your Setup	10
	Default device settings	10
5	Device Information	12
	Summary	12
	WAN.....	12
	Statistic.....	13
	Route.....	14
	ARP	15
	DHCP.....	15
6	Advanced Setup	16
	Layer2 Interface.....	16
	<i>DSL ATM Interface.....</i>	<i>16</i>
	<i>ETH WAN Interface.....</i>	<i>18</i>
	<i>DSL PTM Interface.....</i>	<i>19</i>
	WAN Service	20
	<i>PPP over Ethernet (PPPoE)</i>	<i>21</i>
	<i>IPoE (IP over Ethernet)</i>	<i>23</i>
	<i>Bridging.....</i>	<i>24</i>
	LAN	25

	NAT (Network Access Translation)	26
	<i>Virtual Server</i>	26
	<i>Port Triggering</i>	28
	<i>DMZ</i>	29
	Security	29
	<i>IP Address Filter</i>	29
	Parental Control	32
	<i>Time Restriction</i>	32
	<i>URL Filter</i>	33
	Quality of Service	33
	<i>Queue Configuration</i>	34
	<i>QoS Classification</i>	35
	Routing	36
	<i>Default Gateway</i>	36
	<i>Static Route</i>	37
	<i>RIP</i>	37
	DNS	38
	<i>DNS Server</i>	38
	<i>Dynamic DNS</i>	38
	DSL	40
	UPnP	41
	DNS Proxy	41
	Print Server	42
	Interface Grouping	42
	IPSec	44
	Certificate	45
	<i>Local Certificates</i>	45
	<i>Trusted CA Certificate</i>	47
7	Wireless Setup	49
	Basic	49
	Security	50
	MAC Filter	54
	Wireless Bridge	55
	Advanced	56
	Station Information	57
8	Voice Setup	58
	SIP Basic Setting	58
	Line Setting	60
	RTP/Codec Setting	61
	SIP Advanced Setting	63
9	Voice Supplementary Service	65

Call Forward	65
<i>Call Forward Unconditional</i>	65
<i>Call Forward No Response</i>	65
<i>Call Forward on Busy</i>	65
Secret Number, Calling Line Identification Restriction (CLIR)	65
<i>Static Configuration</i>	66
<i>On per call basis</i>	66
Call Waiting	66
<i>Call Waiting customer configuration</i>	66
Call Transfer	66
Call Back Busy Subscriber (Busy)	66
Call Back last number called (Call Return)	67
10 Diagnostic.....	68
Diagnostics	68
Fault Management	69
11 Management.....	70
Settings	70
<i>Backup</i>	70
<i>Update</i>	70
<i>Restore Default</i>	71
System Log	71
TR-069 Client	72
Internet Time	73
Access Control	73
<i>Password</i>	73
Update Software	74
Reboot	74
Appendix A - Configuring the Network Settings	75
Configuring Ethernet (LAN) Card	75
<i>Before you begin</i>	75
<i>Windows XP PCs</i>	75
<i>Assigning static IP addresses to your PCs</i>	75
Configuring Wireless LAN card	76
<i>Wireless card and drivers</i>	76
<i>Configuring wireless device</i>	76
Appendix B - Troubleshooting	77
Troubleshooting Suggestions	77
IP Utilities for diagnostic	78
<i>Ping</i>	78
<i>Nslookup</i>	78
Appendix C - Specification	80

Appendix D - Warranties 82
Appendix E - Contact information 84

1 Introduction

Congratulations on becoming the owner of the **DG200 series**, an advanced VDSL2 VoIP and wireless gateway. You will now be able to access the Internet using your high-speed connection.

The **DG200 series** is a gateway integrating VDSL2, 2 USB host ports, 2 Giga Ethernet ports, 2 VoIP ports, 4 Ethernet ports switch and 802.11b/g/n wireless interfaces into one device which provides the most flexibility and efficiency way to you. You could connect devices like PCs, Set-Top-Box, ATA, servers, IP phone and so on easily by Ethernet and wireless interfaces to enjoy data, voice, and video services immediately through high speed connection.

This User Guide will show you how to connect your **DG200 series** gateway and how to customize its configuration to get the most out of your new product.

Features

The list below contains the main features of the device (**DG200 series**) and may be useful to users with knowledge of networking protocols. The chapters throughout this guide will provide you with enough information to get the most out of your device.

The features include:

- Support up to VDSL2 (G.993.2) with 100 Mbps downstream and 50 Mbps upstream rates* as well as fallback to ADSL2 (* in short loop, the actual loop performance may vary depending on network configuration and link conditions.)
 - Integrated four-port Ethernet switch with automatic speed-sensing and crossover correction
 - Giga Ethernet ports for high-speed local network connections.
 - 802.11n WLAN supports up to 300 Mbps transmission rate and air traffics are secured by either 802.1X, WEP, WPA/WPA2
 - Two USB 2.0 host ports to support specific plug-and-play functionalities such as print sharing and storage sharing.
 - Support Networking protocols such as PPP, NAT, Routing, DHCP server / relay / client
 - Configuration and management by Web-browser through the Ethernet interface and remotely through WAN interface
 - Support TR-064, TR-069 or SNMP for remote management, and firmware is upgradeable through HTTP or TFTP

Device Requirements

In order to use the device, you must have the following:

- ▶ High speed broadband service
- ▶ Instructions from your ISP on what type of Internet access you will be using, and the IP addresses needed to set up access
- ▶ One or more computers, each containing an Ethernet card (10Base-T/100Base-TX network interface card (NIC)).
- ▶ For system configuration a web browser such as Internet Explorer v4 or later, or Netscape v4 or later, or Firefox is required.



Note

You do not need to use a hub or switch in order to connect more than one Ethernet PC to the device. Instead, you can connect up to four Ethernet PCs directly to the device using the ports labeled LAN1 to LAN4 on the rear panel.

2 Getting to know the device

Parts Check

In addition to this document, your package should arrive containing the following:

- ▶ **The device (DG200 series)**
- ▶ **Ethernet cable**
- ▶ **Standard phone line cable**
- ▶ **Power adapter**


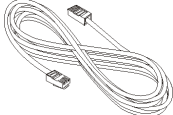
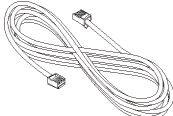


	<p>DG200 series device</p>
	<p>RJ-45 Cable</p>
	<p>RJ-11 Cable</p>
	<p>Power adapter</p>
	<p>User Manual CD (Optional)</p>

Figure 1: Package Contents

Front Panel

The front panel of this device will be described here which cover all front panel definitions of other models. (NOTE: Picture is not actual housing)

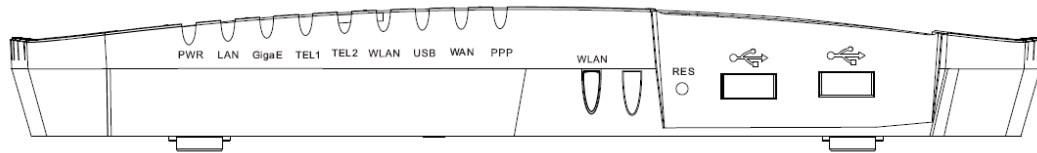


Figure 2: Front Panel and LEDs

LED definitions from left to right:

Name	Color	Function
Power	Green or Red	Off : Power off On (Green) : Power on ON (Red) : Self-test fails
Ethernet	Green	Off : No LAN link On : LAN link established and active Blink : Data being transmitted
Giga Ethernet	Green or Orange	Off : No LAN link On (Green) : Link speed is 100Mbps On (Orange) : Link speed is 1000Mbps Blink : Data being transmitted
TEL1 and TEL2	Green or Orange	Off : SIP Not Enabled On : SIP registered Flashing : Incoming call Slow Blink: SIP Register Fail
WLAN	Green	Off : WLAN service is disabled On : WLAN service is enabled Blink : Data being transmitted
USB	Green	On : LAN link established and active Off : No LAN link Blink: Data being transmitted
WAN	Green	Off : No connection or no signal On : Physical layer sync up successfully. Blink : Physical sync up progress
Internet	Green or Red	Off (Green) : Bridge mode On (Green) : The device gets an IP address successfully in Router mode Red on : It can not get an IP address in Router mode.

Front Panel Connector definition

Name	Function
Wireless Switch	Wireless ON/OFF switch
Reset	A reset button to reset the device or reset to default settings.
USB Host 1 ~ 2	Connects to a supported USB client device

Rear Panel

The rear panel of this device will be described here which cover all rear panel definitions of other models. (NOTE: Picture is not actual housing)

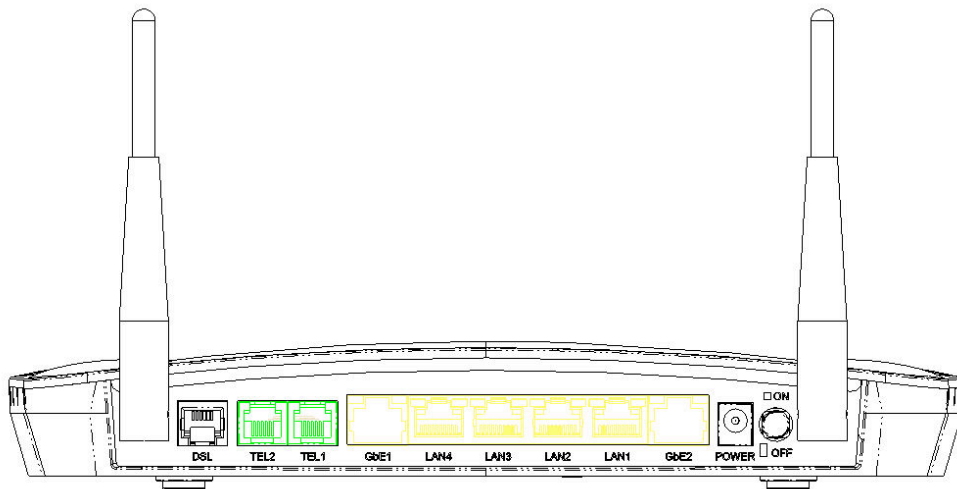


Figure 3: Rear Panel Connections

Rear Panel Connector definition:

Name	Function
Antenna	Connects to the 802.11b/g/n enabled wireless devices in LAN
DSL Jack	Connects to the ADSL network
TEL1 ~ TEL2	Connects to the analog telephone set
Giga Ethernet	Connects the device via Giga Ethernet to your device in LAN
LAN1 ~ LAN4	Connects the device via Ethernet to your devices in LAN
Giga Ethernet	Connects the device via Giga Ethernet to your device in LAN
Power Jack	Connects to the supplied power adapter
Power Switch	ON/OFF switch
Antenna	Connects to the 802.11b/g/n enabled wireless devices in LAN

3 Connecting your device

This chapter provides basic instructions for connecting the device to a computer or LAN and to the Internet.

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

Configuring Ethernet PCs section

Configuring Wireless PCs section

This chapter assumes that you have already subscribed a broadband service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

Connecting the Hardware

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



WARNING

Before you begin, turn the power off for all devices. These include your computer(s), your LAN hub/switch (if applicable), and the device.

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

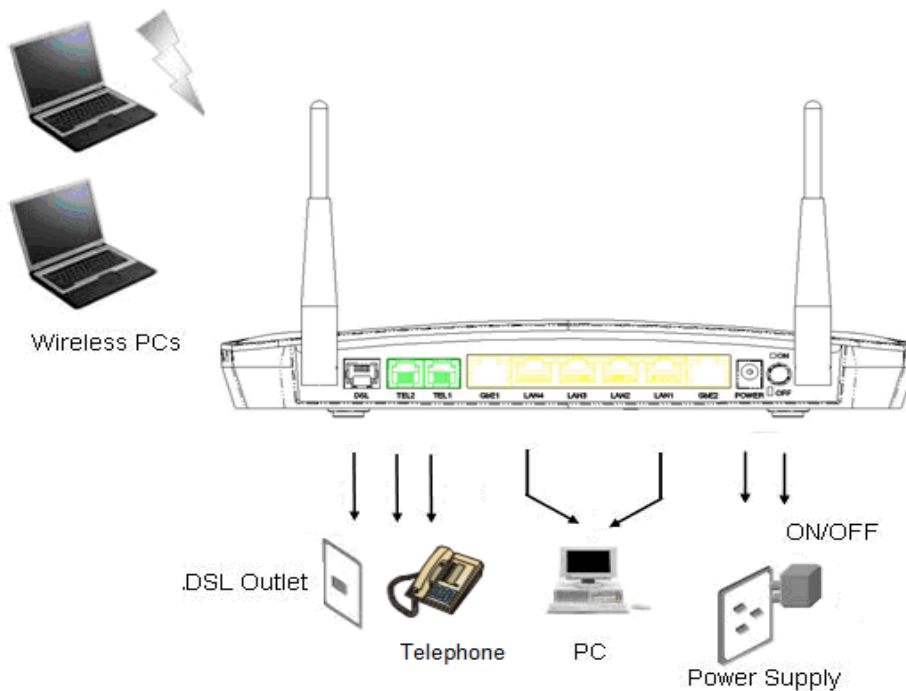


Figure 4: Overview of Hardware Connections (NOTE: Picture is not actual housing)

Step 1. Connect the WAN port to ADSL network

Connect the WAN port to the DSL network which has the high speed internet connection.

Step 2. Connect the Ethernet cable

Connect up to four Ethernet-equipped computers or hubs/switches directly to the device via Ethernet cable(s).

Note that the cables do not need to be crossover cables; the switch provides MDI and MDIX auto-detection.

Step 3. Attach the power connector

Connect the AC power adapter to the Power connector on the back of the device and plug the adapter into a wall outlet or power strip. Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Step 4. Configure your Ethernet PCs

You must also configure the Internet properties on your Ethernet PCs. See Configuring Ethernet PCs section.

Or, step 5. Install a Wireless card or dongle to the PCs if these machines do not have Ethernet port, or wireless connection is preferred.

You can attach a wireless LAN client (card or dongle) that enables PCs to access the Internet via the device through air connection.

You must configure your Wireless computer(s) in order to access your device. For complete instructions, see Configuring Wireless PCs section.

Next step

After setting up and configuring the device and PCs, you can log on to the device by following the instructions in "Getting Started with the Web pages" on chapter 4. The chapter includes a section called Testing your Setup, which enables you to verify that the device is working properly.

4 Getting Start with the Web pages

The device includes a series of Web pages that provide an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through a web browser on a PC connected to the device.

Accessing the Web pages

To access the web pages, you need the following:

A laptop or PC connected to the LAN or WLAN port on the device.

A web browser installed on the PC. You launch the web browser, type the URL, <http://192.168.1.1> in the web address (or location) box, and press [Enter]. You need to enter different IP address if the default IP address of the device was changed. Then enter the default username and password: admin/admin to access the configuration web page, if you have not changed the username and password. Please be informed that strings of username and password are case-sensitive.



Figure 5: Login Page

The Menu comprises:

Device Information: provides the basic information of the system. It includes sub menus, Summary, WAN, Statistics, Route, ARP and DHCP.

- Device Info
- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP

Advanced Setup: provides information about the current configuration of various system features with options to change the configuration. It includes the sub menus Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, Dns Proxy, Print Server, Interface Grouping, IPSec and Certificate.

Advanced Setup

- Layer2 Interface
- WAN Service
- LAN
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- Upnp
- Dns Proxy
- Print Server
- Interface Grouping
- IPSec
- Certificate

Wireless Setup: provides wireless SSID, security, key and various options to change the configuration. It includes the sub menu, Basic, Security, MAC Filter, Wireless Bridge, Advanced, and Station Info.

Wireless

- Basic
- Security
- MAC Filter
- Wireless Bridge
- Advanced
- Station Info

Voice Setup: provides VoIP SIP configuration. It includes the sub menu, SIP Basic Setting, Line Setting, RTP/Codec Setting, and SIP Advanced Setting.

Voice

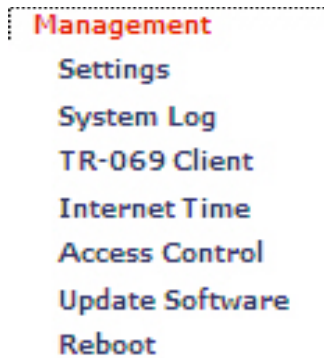
- SIP Basic Setting
- Line Setting
- RTP/Codec Setting
- SIP Advanced Setting

Diagnostic: provides the diagnostic utility to check the LAN and Wireless physical connection and VDSL/ADSL connection as well. It includes Diagnostics and Fault Management.

Diagnostics

- Diagnostics
- Fault Management

Management: provides the administration utilities. It includes the sub menus, Settings, System Log, TR-069 Client, Internet Time, Access Control, Update Software, and Reboot.



Testing your Setup

Once you have connected your hardware and configured your PCs, any computer on your LAN should be able to use the device to access the Internet.

To test the connection, turn on the device, wait seconds till device booting up and then verify that the LEDs are illuminated as follows:

LED	Behavior
Power (PWR)	Solid red to indicate that the device is turned on. If this light is not on, check the power cable attachment.
Wireless (WLAN)	Solid green to indicate that the Wireless LAN function is operational.
LAN	Solid green to indicate that the device can communicate with your LAN.
WAN (DSL)	Solid green to indicate that the device has successfully established a connection with your ISP.

Table 1: LED Indicators

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

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. If the LEDs still do not illuminate as expected or the web page is not displayed, see Troubleshooting section or contact your ISP for assistance.

Default device settings

The device is preconfigured with default settings for use with a typical home or small office network.

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



WARNING

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

Option	Default Setting	Explanation/Instructions
User/Password	admin/admin	User name and password to access the device
LAN Port IP Address	Assigned static IP address: 192.168.1.1 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See <i>Local Network</i> section.
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.2 through 192.168.1.254 (Please be noted that the default DHCP IP address pool may be different in each firmware version.)	The device maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in <i>DHCP Server</i> section.

Table 2: Values of Default Settings

5 Device Information

The Device Information web page menu includes the following submenus:

Summary

WAN

Statistics

Route

ARP

DHCP

Summary

The Summary Page of the device shows the following information, Board ID, Software version, Bootloader version, Wireless driver version, and MAC address. Besides, LAN IP, Default gateway, Primary DNS server and Secondary DNS server are shown too.

Device Info

Board ID:	96368MVWG
Software Version:	VI580_4.02L.03XAT01
Bootloader (CFE) Version:	1.0.37-102.6
Wireless Driver Version:	5.10.85.0.cpe4.402.0

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps)	
Line Rate - Downstream (Kbps)	
LAN IPv4 Address	192.168.1.1
Default Gateway:	
Primary DNS Server:	
Secondary DNS Server:	

Figure 6: Device Information

WAN

The WAN information of the device shows detailed information about the WAN connection such as Interface name, Description, Encapsulation Type, VLAN MuxID, IGMP, NAT, Firewall, Connection Status and IP address of WAN port.

WAN Info

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
ppp0	pppoe_0_0_35	PPPoE	Disabled	Disabled	Enabled	Enabled	Connecting	(null)

Figure 7: WAN Port Information

Statistic

The Statistic Page of the device shows the following information, Interfaces, data transmitting (Received and Transmitted directions) in that interface such as total bytes, packets, error count and drop count of LAN port, WAN port, xTM, and xDSL.

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	85564	581	0	0	255995	452	0	0
eth1	736638	5015	0	0	2102659	4529	0	0
eth2	0	0	0	0	1280	20	0	0
eth3	0	0	0	0	1216	19	0	0
eth4	0	0	0	0	0	0	0	0
eth5	0	0	0	0	0	0	0	0
usb0	0	0	0	0	0	0	0	0
wl0	0	0	8	0	0	0	10	0

Reset Statistics

Figure 8: Device LAN Port Statistic Information

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0	pppoe_0_0_35	0	0	0	0	2143079712	716781240	6278440	2143079788

Reset Statistics

Figure 9: Device WAN Port Statistic Information

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
-------------	-----------	------------	------------	-------------	--------------	---------------	--------------	---------------	------------------	----------------

Reset

Figure 10: Device xTM Statistic Information

Statistics -- xDSL

Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test
Reset Statistics

Figure 11: Device xDSL Statistic Information

Route

The Route Page of the device shows the route table. It contains Destination IP address, Gateway, Subnet Mask, Flag, Metric, Service and Interface.

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 12: Device Route Table Information

ARP

The ARP Page of the device shows the ARP table mapping the IP address and related MAC address. The ARP table contains IP address, Flag, MAC address, Device Interface.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.44	Complete	00:0C:76:C4:D1:2F	br0

Figure 13: Device ARP Table Information

DHCP

The DHCP Page of the device shows the DHCP table which DHCP server of device assigns the IP address to the PC requesting an IP address. The DHCP table contains Hostname, MAC address, IP address and Expires In.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
----------	-------------	------------	------------

Figure 14: Device DHCP Table Information

6 Advanced Setup

The Advance Setup menu includes the sub menus Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, Dns Proxy, Print Server, Interface Grouping, IPSec and Certificate.

Layer2 Interface

WAN Service

LAN

NAT

Security

Parental Control

Quality of Service

Routing

DNS

DSL

UPnP

DNS Proxy

Print Server

Interface Grouping

IPSec

Certificate

Layer2 Interface

You can configure the DSL ATM and ETH WAN layer2 interfaces from this page.

DSL ATM Interface

This page displays the details of existing DSL ATM interface including interface name, VPI/VCI, latency, Category, link type, connection mode, ATM QoS enable/disable. You may click *Add* to create a specific Layer2 Interface.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Disabled	<input type="checkbox"/>
atm1	0	33	Path0	UBR	EoA	DefaultMode	Enabled	<input type="checkbox"/>

Figure 15: Layer2 Interface DSL ATM Page

Global settings:

- ▶ Check the *Remove option* and click *Remove* button to remove the specific entry
- ▶ Click *Add* to create a new ATM Layer2 Interface.

ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category, enable it.

VPI: [0-255]

VCI: [32-65535]

Select DSL Latency

Path0

Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA

PPPoA

IPoA

Encapsulation Mode:

Service Category:

Select Connection Mode

Default Mode - Single service over one connection

VLAN MUX Mode - Multiple Vlan service over one connection

MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. the number of PVCs will be reduced. Use *Advanced Setup/Quality of Service* to assign priorities for the applications.

Enable Quality Of Service

Figure 16: Add a Layer2 Interface Page

Global settings:

- ▶ Enter *VPI/VCI* values
- ▶ Select *DSL Latency*: Path 0 or Path 1.
- ▶ Select the DSL link type, EoA, PPPoA or IPoA. The EoA type is for PPPoE, IPoE and Bridge.
- ▶ Select the *Encapsulation Mode* from the list (LLC/SNAP-BRIDGING, LLC/SNAP-Routing or VC/MUX)
- ▶ Select the Service Category from the list (UBR without PCR, UBR with PCR, CBR, Non Realtime VBR, Realtime VBR). Please leave it as default, UBR with PCR, if ISP does not give you any information of this setting.

Service Category:

UBR Without PCR
UBR With PCR
CBR
Non Realtime VBR
Realtime VBR

Figure 17: Service Category Configuration

PCR stands for Peak Cell Rate (ATM cells per second). It is the maximum allowable rate which cells can be transferred in the connection.

SCR stands for Sustainable Cell Rate (ATM cells per second). It is an average allowable rate which cells can be transferred in the connection.

MRS stands for Maximum Burst Size (ATM cells). It is the maximum allowable burst size of cells which cells can be transferred in the connection.

- ▶ Select *Connection Mode*:
 - Default Mode: single service over one connection
 - VLAN MUX Mode: multiple VLAN service over one connection
 - MSC Mode: multiple service over one connection
- ▶ Check to enable the *Qualify of Service* if Service Category is UBR without PCR, URB with PCR or Non Realtime VBR and you like this service. Use the Advanced Setup -> Qualify of Service to assign priorities for the applications.
- ▶ Click *Save/Apply*

ETH WAN Interface

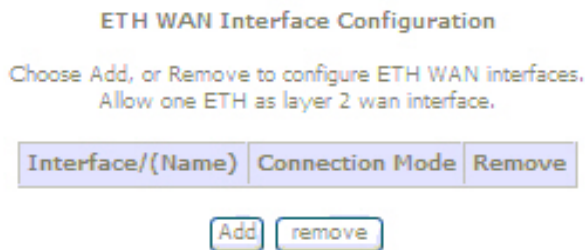


Figure 18: ETH WAN Interface Page

Global settings:

- ▶ Check the *Remove option* and click *Remove* button to remove the specific entry
- ▶ Click *Add* to create a new ETH WAN Interface.

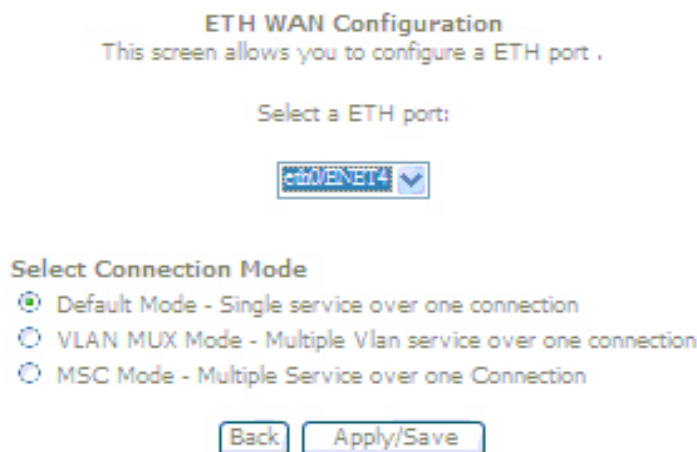


Figure 19: Add ETH WAN Interface Page

Global settings:

- ▶ Select the *specific Ethernet port* from the list as WAN port
- ▶ Select the *Connection Mode*, Default Mode, VLAN Mux Mode or MSC Mode.
 Default Mode: Single service over one connection
 VLAN MUX Mode: Multiple VLAN service over one connection
 MSC Mode: Multiple service over one connection
- ▶ Click *Apply/Save*.

DSL PTM Interface

This page displays the details of existing DSL PTM interface including interface name, DSL Latency, PTM Priority, Connection Mode, QoS enable/disable. You may click *Add* to create a specific Layer2 Interface.

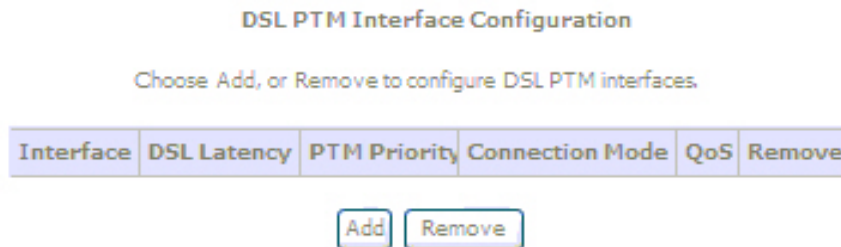


Figure 20: DSL PTM Interface Page

Global settings:

- ▶ Check the *Remove option* and click *Remove* button to remove the specific entry
 Click *Add* to create a new DSL PTM WAN Interface.

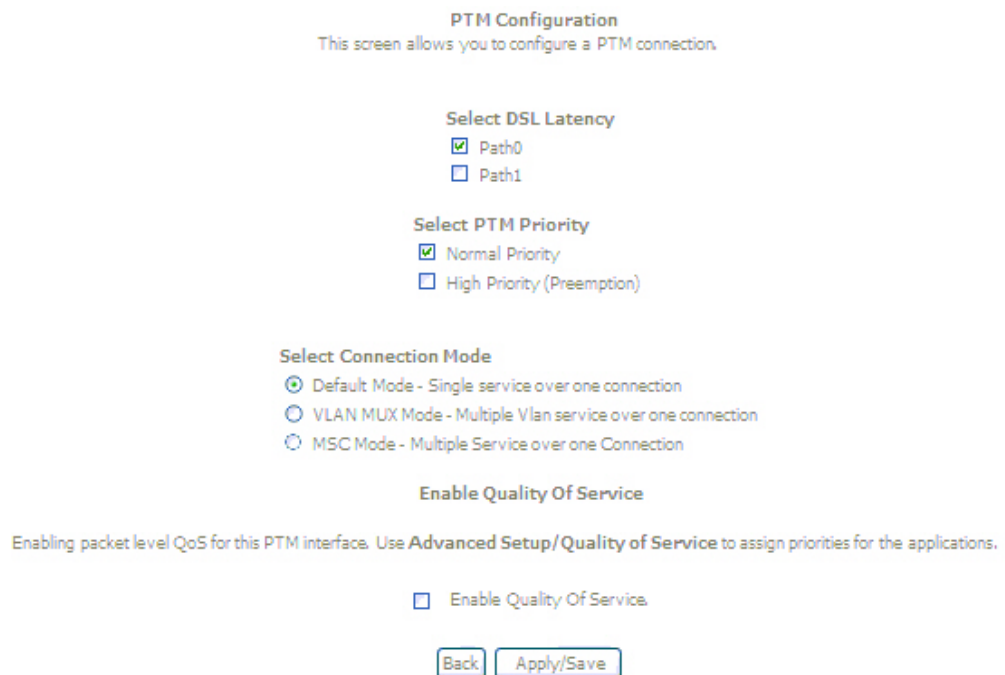


Figure 21: Add DSL PTM WAN Interface Page

Global settings:

- ▶ Select the *DSL Latency*, Path 0 or Path 1.
- ▶ Select the *DSL Priority*, Normal Priority or High Priority.
- ▶ Select the *Connection Mode*, Default Mode, VLAN Mux Mode or MSC Mode.
 Default Mode: Single service over one connection
 VLAN MUX Mode: Multiple VLAN service over one connection
 MSC Mode: Multiple service over one connection
- ▶ Check to enable the *Quality of Service*. Use the Advanced Setup -> Quality of Service to assign priorities for the applications.
- ▶ Click *Apply/Save*.

WAN Service

You can configure your internet connection from this page. This page displays the details of existing internet connection.

Wide Area Network (WAN) Service Setup

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

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>

Figure 22: WAN Setup Page

Global settings:

- ▶ Check the *Remove option* and click *Remove* button to remove the specific entry
- ▶ Click *Add* to create a new WAN Service

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 -> DSL Latency PATH0
 portId=1 -> DSL Latency PATH1
 portId=4 -> DSL Latency PATH0&1
 low =0 -> Low PTM Priority not set
 low =1 -> Low PTM Priority set
 high =0 -> High PTM Priority not set
 high =1 -> High PTM Priority set

Figure 23: Create WAN Service Interface Page

- ▶ Select one of available *Layer2 Interface* and click *Next*

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

Figure 24: WAN Service Configuration

- ▶ Select *WAN Service Type*: PPPoE, IPoE or Bridging.
- ▶ Enter a name as a *Service Description*.
- ▶ Click *Next* to continue the configuration

PPP over Ethernet (PPPoE)

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

Enable MLD Multicast Proxy

Figure 25: WAN Connection, PPPoE Configuration

To configure the PPPoE settings:

- ▶ Enter the User's *PPP Username* and *Password*

- ▶ Enter the *Service Provider Name* if any
- ▶ Select the *Authentication Method* used during negotiation, default is AUTO.
- ▶ Check to *enable Fullcore NAT* if necessary
- ▶ Check “*Dial On Demand*” if you do not need PPPoE connection always ON and enter the timeout value to disconnect the PPPoE connection when connection is idle and timeout. If you enter “0”, zero for the timeout value, it means always ON.
- ▶ Check the “*PPP IP extension*” if ISP requests to enable it, otherwise do not select it. This is a special service to forward IP address assigned by remote to the local device in the LAN.
- ▶ Check the “*Use Static IPv4 address*” and enter the IP address if your ISP assigns a fixed IP address to you. Otherwise, do not select it.
- ▶ Check to enable “*PPP Debug Mode*”
- ▶ *Check Bridge PPP frames between WAN and Local Ports* if you want to pass PPP frame between WAN and LAN.
- ▶ Check to enable *IGMP Multicast* to avoid the multicast packet flooding to other LAN ports where do not need this IGMP packet to get better efficiency in Ethernet port.
- ▶ Check to enable *MLD (Multicast Listener Discovery) Multicast Proxy*
- ▶ Click *Next* to configure the default gateway

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

Figure 26: WAN Service, Default Gateway

- ▶ Select a preferred WAN interface from the list as the device default path to route the packets.
- ▶ Click *Next* to configure the DNS servers

Obtain DNS info from a WAN interface:
 WAN Interface selected:

Use the following Static DNS IP address:
 Primary DNS server:
 Secondary DNS server:

Figure 27: WAN Service, DNS Settings

- ▶ Select to obtain DNS info from a WAN interface or set static DNS IP addresses to enter IP address of Primary DNS server and/or Secondary DNS server.
- ▶ Click *Next* to view the Summary of current settings

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 33
Connection Type:	PPPoE
Service Name:	pppoe_0_0_33
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Enabled
Quality Of Service:	Enabled

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

Figure 28: WAN Service, Summary

- ▶ Click *Apply/Save* to save the configuration or click *Back* to reconfigure it again.

IPoE (IP over Ethernet)

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 MER mode.
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically
 Option 60 Vendor ID:
 Option 61 IAID: (8 hexadecimal digits)
 Option 61 DUID: (hexadecimal digit)
 Option 125: Disable Enable
 Use the following Static IP address:
 WAN IP Address:
 WAN Subnet Mask:
 WAN gateway IP Address:

Figure 29: WAN Service, IPoE Configuration

To configure the IP over Ethernet settings:

- ▶ Select "Obtain an IP address automatically" or "Use the following (fixed) IP address" and then also enter the WAN IP address, WAN Subnet Mask and WAN Gateway IP Address.
- ▶ If you choose to obtain an IP address automatically, please input the DHCP Option 60, 61 and 125 if ISP provides such information to you, otherwise leave it as default (blank).
- ▶ Click *Next*

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 Fullcone NAT
- Enable Firewall

IGMP Multicast

- Enable IGMP Multicast
- Enable MLD Multicast Proxy

Figure 30: WAN Service, IPoE NAT Configuration

WAN service setting:

- ▶ Check to enable *NAT* that allows multiple PCs surfing Internet simultaneously by using the same WAN IP address.
- ▶ Check to enable *Firewall*
- ▶ Check to enable *IGMP Multicast* to avoid the multicast packet flooding to other LAN ports where do not need this IGMP packet to get better efficiency in Ethernet port.
- ▶ Check to enable *MLD (Multicast Listener Discovery) Multicast Proxy*
- ▶ Click *Next*

The *Default Gateway configuration*, *DNS Server configuration*, and *WAN Setup Summary* page will show up. Please refer related pages above for reference. Click *Save* if correct and click *Back* to restart the configuration again.

Bridging

You configure the WAN service as a Bridging function between WAN and LAN ports. The *WAN Setup Summary* page is shown. Click *Save* if correct and click *Back* to restart the configuration again.

LAN

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. GroupName Default ▼

IP Address:
 Subnet Mask:

Enable IGMP Snooping

Standard Mode

Blocking Mode

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

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

MAC Address	IP Address	Remove
<input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/>		

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:
 Subnet Mask:

Figure 31: LAN Configuration

To configure LAN:

- ▶ Select the *GroupName* from the list
- ▶ Enter the *IP address* which the CPE in the LAN will use to connect to the device. For example, enter 192.168.1.1
- ▶ Enter the *Subnet Mask*. For example, enter 255.255.255.0
- ▶ Check to *Enable IGMP Snooping*. This feature will snoop all of IGMP packets and record related information. Therefore, multicast packets will be generated to the related LAN ports only to avoid the packet flooding on all of LAN ports. Select one of two modes, *Standard mode* or *Blocking mode*.
- ▶ Check to *enable LAN side firewall*
- ▶ Select to *Enable or Disable DHCP server*. If it is enabled, please enter the DHCP IP pool of *Start IP address* and *End IP address*. Enter the value of *leased time* in hour about the valid period of assigned IP address. The DHCP server ON (enabled) feature will enable this device to assign IP address automatically to PC in LAN if PC requests an IP address by DHCP client protocol.
- ▶ Click *Add Entries* button to add IP address excluded in the IP pool.

DHCP Static IP Lease

Enter the Mac address and Static IP address then click "Apply/Save".

MAC Address:

IP Address:

Figure 32: LAN DHCP Static IP Lease Configuration

- ▶ Enter the MAC address and static IP address which a dedicated PC uses this fixed IP address already. This IP address will be excluded from the IP pool. Click Apply/Save to save configuration.
- ▶ Check to *Enable DHCP Server Relay* and then input the IP address of DHCP server.
- ▶ The device can handle second IP address and subnet of LAN interface. You may check this feature to configure the second IP address and subnet for LAN port to meet your LAN environment.
- ▶ Click *Save* to save the configuration

NAT (Network Access Translation)

The NAT feature provides the basic firewall feature to avoid hacker attacks from remote site. There are three more setting pages including virtual server, port trigger, and DMZ to provide specified service for remote users.

Virtual Server

Virtual Server enables you to run a server on your local network that can be accessed from the remote parties. You need to set up a rule to tell the device on which computer the server is held. When port virtual server is enabled, your router (the device) routes all the inbound traffic on a particular port to the chosen computer on your network.

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.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

Figure 33: Virtual Server Setup Configuration

Click Add to add a rule of virtual server.

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>

Figure 34: Add Rule Of Virtual Server

Global Setting:

- ▶ Select the WAN Interface from the list which applies to this rule.
- ▶ Select a *service* from the predefined list or enter the name of *Custom Server*. The presetting will be imported if you select the predefined service.
- ▶ Enter the *Server IP Address* located in the LAN to provide the service to remote party
- ▶ Enter the *Start External Port #* and *End External Port #* that open to remote to access the service
- ▶ Select the *Protocol* from the list
- ▶ Enter the *Start Internal Port #* and *End Internal Port #* that may use different port # to secure the service. If you use the same port # as *external port #*, please leave *Internal Port #* as blank.
- ▶ Click *Save/Apply*

Port Triggering

The feature is similar to the virtual server, but provides a more secure way to provide your device. It opens up the port hole temporary and allows CPE in LAN to establish a connection with remote parties. Those ports are open only if a specified request from a PC in LAN is received, and then the device allows the remote parties to access to establish a connection with that PC in LAN.

FIAT -- 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 35: Port Triggering Setup

Click *Add* to add a rule of port triggering.

Use Interface:

Application Name:

Select an application:

Custom application:

Save/Apply

Trigger Port	Start	Trigger Port	End	Trigger Protocol	Open Port	Start	Open Port	End	Open Protocol
<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"/>	<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

Save/Apply

Figure 36: Add Rule Of Port Triggering

Global Setting

- ▶ Select the WAN Interface from the list which applies to this rule.
- ▶ Select a *service* from the predefined list or enter the name of *Custom Server*
- ▶ Enter the *Server IP Address* located in the LAN to provide the service to remote party
- ▶ Enter the *Start Trigger Port #* and *End Trigger Port #* that open to remote to access the service
- ▶ Select the *Trigger Protocol*
- ▶ Enter the *Start Open Port #* and *End Open Port #* that may use different port # to secure the service. If you use the same port # as *Trigger port #*, please leave *Open Port #* as blank.

- ▶ Select the *Open Protocol*
- ▶ Click *Save/Apply*

DMZ

A DMZ (De-Militarized Zone) host is a computer on your network that can be accessed from the Internet. The de-militarized zone (DMZ) is for forwarding IP packets from the remote parties that are not fixed to any of the applications configured in the virtual server. These packets are forwarded to a designated DMZ host device. A DMZ is often used to host Web servers, FTP servers etc that need to be accessible from the Internet

NAT -- DMZ Host

The DSL 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:

Save/Apply

Figure 37: DMZ Configuration

Global Setting

- ▶ Enter the *DMZ Host IP address*
- ▶ Click *Save/Apply*

Security

The Security feature provides two more setting pages including MAC filtering and Parental Control.

IP Address Filter

The device can block the packet in outgoing and incoming directions. By default, all outgoing IP packets from LAN is allowed to surf Internet, but some IP packets can be blocked by setting up filters.

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	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

Add Remove

Figure 38: Outgoing IP Filter Setup

Click *Add* to add a rule of Outgoing IP Filtering.

Check *Remove* and click *Remove* to remove the specified entry.

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 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Figure 39: Add - Outgoing IP Filter Setup

Global Setting

- ▶ Enter the *Filter Name*
- ▶ Select the *Protocol* from the selection list.
- ▶ Enter the *Source IP Address* and *Subnet Mask (range of IP addresses)* of packet
- ▶ Enter the *one port or multi ports (port range)*
- ▶ Enter the *Destination IP Address* and *Subnet Mask (range of IP addresses)* of packet
- ▶ Enter the *one port or multi ports (port range)*
- ▶ Click *Save/Apply*

By default, all incoming IP packets from WAN are blocked to access PCs in LAN, but some IP packets can be accepted by setting up filters.

Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

Figure 40: Incoming IP Filter Setup

Click *Add* to add a rule of Incoming IP Filtering.

Check *Remove* and click *Remove* to remove the specified entry.

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, rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

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 br0/br0

Figure 41: Add - Incoming IP Filter Setup

Global Setting

- ▶ Enter the *Filter Name*
- ▶ Select the *Protocol* from the selection list.
- ▶ Enter the *Source IP Address* and *Subnet Mask (range of IP addresses)* of packet
- ▶ Enter the *one port or multi ports (port range)*
- ▶ Enter the *Destination IP Address* and *Subnet Mask (range of IP addresses)* of packet
- ▶ Enter the *one port or multi ports (port range)*
- ▶ Select the *WAN interfaces* which will be applied with this incoming IP filter rule.
- ▶ Click *Save/Apply*

Parental Control

This feature allows you to configure some of PCs in LAN to surf Internet in specific time period and filter the specific URLs.

Time Restriction

Time of Day Restrictions -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<div style="display: flex; justify-content: center; gap: 10px;"> Add Remove </div>											

Figure 42: Parental Control Configuration

Click *Add* to add a rule of schedule for parental control.

Check *Remove* and click *Remove* to remove the specified entry.

Time of Day 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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Save/Apply

Figure 43: Time of Day Restriction Configuration

Global Setting

- ▶ Enter the *Username*
- ▶ Select the *Browser's MAC Address* or *Other MAC Address* to enter the specific PC MAC address.
- ▶ Check *those days* you want to block above PC to surf Internet.
- ▶ Enter the *Start Blocking Time* and *End Blocking Time*
- ▶ Click *Save/Apply*.

URL Filter

URL List Type: Exclude Include

Address	Port	Remove
		<input type="checkbox"/>

Figure 44: URL Filter Configuration

Global Setting

- ▶ Select the URL List Type, Exclude or Include
- ▶ Click Add to add URL. Maximum 100 entries can be configured. Check the remove box and click Remove to remove the entry.

Parental Control -- URL Filter Add

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

URL Address:

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

Figure 45: Add URL Filter Configuration

- ▶ Enter the URL address and port number then click Save/Apply to save the configuration.

Quality of Service

The Quality of Service feature provides a method to prioritize the packet and arrange a better efficiency of bandwidth. In other words, some traffic such as voice or video has handled as higher priority than others such as data to get near real time response.

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:

Figure 46: Quality of Service Configuration

Global Setting

- ▶ Check Enable QoS (Quality of Service)
- ▶ Select “Default DSCP Mark” from the list if the egress packets that do not match any classification rules.
- ▶ Click Save/Apply

Queue Configuration

You could configure a maximum 16 QoS queues to provide different service levels.

QoS Queue Setup -- A maximum 16 entries can be configured.

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

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	1			Enabled	
WMM Voice Priority	2	wl0	2			Enabled	
WMM Video Priority	3	wl0	3			Enabled	
WMM Video Priority	4	wl0	4			Enabled	
WMM Best Effort	5	wl0	5			Enabled	
WMM Background	6	wl0	6			Enabled	
WMM Background	7	wl0	7			Enabled	
WMM Best Effort	8	wl0	8			Enabled	

Figure 47: Quality of Service Queue Configuration

Click *Add* to add a class of Quality of Service.

The screen allows to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be user by the classifier to place ingress packets appropriately. Note: lower integer values for precedence imply higher priority for this queue relative to others.

Name:

Enable: ▼

Interface:

Precedence: ▼

Figure 48: Add QoS Queue

Global Setting

- ▶ Enter the name of this queue

- ▶ Select Enable or Disable this queue
- ▶ Select the *queue* attaching to a specific network *Interface*
- ▶ Select the *Queue Precedence* (1, 2, 3), lower integer values for precedence imply higher priority for this queue relative to others.
- ▶ Click *Save/Apply* to save it.

QoS Classification

You need to define one or more *classes* of data traffic and set the priority for each of classes. A maximum 32 entries can be configured.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Remove

Figure 49: Quality of Service Classification Setup

Click *Add* to add a class of Quality of Service.

Check *Remove* and click *Remove* to remove the specified entry.

Traffic Class Name:

Rule Order:

Rule Status:

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

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Tag VLAN ID:

Figure 50: Add Quality of Service Classification

The screen creates a traffic class rule to classify the traffic, assign queue priority which defines the precedence and type of service. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for

the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Global Setting

- ▶ Enter the *Traffic Class Name*
- ▶ Select the *Rule Order* and *Rule Status* from the list
- ▶ Enter the specific classification criteria including Class Interface, Ether Type, Source MAC Address, Source MAC Mask, Destination MAC Address and Destination MAC Mask. A blank criterion indicates it is not used for classification.
- ▶ Enter the specific classification result including Assign Classification Queue, Mark Differentiated Service Code Point (DSCP), Mark 802.1p Priority, and Tag VLAN ID. A blank mark or tag means no change.
- ▶ Click *Apply* to add this QoS class

Routing

The section shows the IP addresses or address routes for the computers connected to the gateway to reach different destinations, such as the local network, the gateway, or the Internet. The Routing feature provides three more setting pages including Default Gateway and Static Route.

Default Gateway

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

Save/Apply

Figure 51: Default Gateway Configuration

Global Setting

- ▶ Select the WAN Interface from the list to be the system default gateway.
- ▶ Click *Save/Apply* to save the configuration

Static Route

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

Destination	Subnet Mask	Gateway	Interface	Remove
-------------	-------------	---------	-----------	--------

Add Remove

Figure 52: Static Route Configuration

Click Add to add the static route path.

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

Destination Network Address:

Subnet Mask:

Use Interface: ▼

Use Gateway IP Address:

Apply/Save

Figure 53: Add Static Route Configuration

Global Setting

- ▶ Enter the *Destination Network Address* and *Subnet Mask* (range)
- ▶ Select the *Use Interface* from the list
- ▶ Enter the *Use Gateway IP Address* where packet will be forwarded to.
- ▶ Click *Save* to save the configuration

RIP

Interface	Version	Operation	Enabled
atm1	2 ▼	Passive ▼	<input type="checkbox"/>

Save/Apply

Figure 54: RIP Configuration

Global Setting

- ▶ Select the desired *RIP version* and *operation*, followed by placing a check in the 'Enabled' checkbox for the interface.
- ▶ Click *Save* to save the configuration

The RIP can not be configured if the WAN interface has NAT enabled.

DNS

The DNS feature provides two more setting pages including DNS server setting and Dynamic DNS.

DNS Server

Obtain DNS info from a WAN interface:
 WAN Interface selected:

Use the following Static DNS IP address:
 Primary DNS server:
 Secondary DNS server:

Figure 55: DNS Server Configuration

Global Setting

- ▶ Select to obtain DNS information from a WAN interface then select the WAN interface from the list.
- ▶ Or select to use the static DNS IP addresses then enter the IP addresses of primary DNS server and/or secondary DNS server.
- ▶ Click Save/Apply to save the configuration.

Dynamic DNS

The Dynamic DNS feature allows you to bind the dynamic assigned WAN IP address into a specified domain name. You could pass this domain name to friends to access your service in your site instead of informing them every times if WAN IP address is changed.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>				

Figure 56: Dynamic DNS Configuration

Click *Add* to add Dynamic DNS setting.

Check *Remove* and click *Remove* to remove the specified entry.

Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider	<input type="text" value="DynDNS.org"/>
Hostname	<input type="text"/>
Interface	<input type="text" value="eth_0_1/eth0.2"/>
DynDNS Settings	
Username	<input type="text"/>
Password	<input type="text"/>

Figure 57: Add Dynamic DNS

Global Setting

- ▶ Select the Dynamic DNS service provider from the list
- ▶ Enter the your Hostname
- ▶ Select the *Interface* from the list where the device can reach it for registration
- ▶ Enter the *Username* and *Password*
- ▶ Click *Save/Apply* to save the configuration

DSL

The DSL feature provides basic and advance configuration to set the DSL parameters. Please contact technician for details before changing any parameters.

DSL Settings

Select the modulation below.

Select the profile below.

<input checked="" type="checkbox"/> G.Dmt Enabled	<input checked="" type="checkbox"/> 8a Enabled
<input checked="" type="checkbox"/> G.lite Enabled	<input checked="" type="checkbox"/> 8b Enabled
<input checked="" type="checkbox"/> T1.413 Enabled	<input checked="" type="checkbox"/> 8c Enabled
<input checked="" type="checkbox"/> ADSL2 Enabled	<input checked="" type="checkbox"/> 8d Enabled
<input checked="" type="checkbox"/> AnnexL Enabled	<input checked="" type="checkbox"/> 12a Enabled
<input checked="" type="checkbox"/> ADSL2+ Enabled	<input checked="" type="checkbox"/> 12b Enabled
<input type="checkbox"/> AnnexM Enabled	<input checked="" type="checkbox"/> 17a Enabled
<input checked="" type="checkbox"/> VDSL2 Enabled	<input checked="" type="checkbox"/> 30a Enabled
	US0
	<input checked="" type="checkbox"/> Enabled

Select the phone line pair below.

Inner pair

Outer pair

Capability

Bitswap Enable

SRA Enable

Figure 58: DSL Basic Configuration

Global Setting

- ▶ Check to select the *DSL modulation* modes.
- ▶ Select the *DSL phone line pair*, inner pair or outer pair. The inner pair is default setting.
- ▶ Check to select the *Capabilities*, Bitswap and SRA (Seamless Rate Adaption).
- ▶ Click *Apply* to save the configuration
- ▶ Click *Advanced Settings* to get details, please contact technician for support.

UPnP

The page provides UPnP configuration to pass UPnP traffic automatically such as MSN messenger voice, video and so on.

Upnp Configuration

Enable or disable Upnp protocol.

Apply/Save

Figure 59: UPnP Configuration

Global Setting

- ▶ Check to *Enable or Disable UPnP protocol*.
- ▶ Click *Save/Apply* to save the configuration

DNS Proxy

The page provides DNS Proxy configuration. To enable DNS Proxy can take DNS queries from the local network and forward them to an Internet Domain Name Server

Dns Proxy Configuration

Enable or disable Dns proxy.

Host name of the modem:

Domain name of the LAN network:

Apply/Save

Figure 60: DNS Proxy Configuration

Global Setting

- ▶ Check to *Enable or Disable DNS Proxy*.
- ▶ Enter the Host name of the modem and Domain name of the LAN network.
- ▶ Click *Save/Apply* to save the configuration

Print Server

The page provides Print Server configuration. You could enable this feature to use the service of on-board printer server. Please refer Chapter Print Server Setup.

Print Server settings

This page allows you to enable / disable printer support.

Enable on-board print server.

Printer name

Make and model

Figure 61: Print Server Configuration

Global Setting

- ▶ Check to *Enable on-board print server* if you like to use this feature. Then enter the Printer Name, Make and Model Name.
- ▶ Click *Save/Apply* to save the configuration

Interface Grouping

The page provides Interface Grouping configuration. In default, the LAN1 to LAN4, wireless, virtual wireless guest and Routed PVC are grouped together as a single Ethernet environment. Interface grouping supports multiple ports to VLAN groups. Each VLAN group will perform as an independent network. To support this feature, you must create interface groups with appropriate LAN and WAN interfaces.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		atm0	eth0	
		atm1	eth1	
			eth2	
			eth3	
			eth4	
			eth5	
			USB	
			wlan0	
			wl0_Guest1	
			wl0_Guest2	
			wl0_Guest3	

Figure 62: Port Mapping Configuration

Click *Add* to add VLAN setting.

Check *Remove* and click *Remove* to remove the specified entry.

Group Name:

WAN Interface used in the grouping

Grouped LAN Interfaces

Available LAN Interfaces

- eth0
- eth1
- eth2
- eth3
- eth4
- eth5
- USB
- wlan0
- wl0_Guest1
- wl0_Guest2

>

<

Automatically Add Clients
With the following DHCP
Vendor IDs

Figure 63: Add Port Mapping Configuration

Global Setting

- ▶ Enter the *Group Name*
- ▶ Select the *WAN Interface used in the grouping*.
- ▶ Select the available *LAN ports* from available LAN interfaces into grouped interface. The selected LAN interface will be removed from its original group and joined this new group.
- ▶ If you like to add LAN clients to a PVC automatically 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.
- ▶ Click *Save/Apply* to save the configuration.

IPSec

The page provides IPSec VPN configuration to establish a VPN tunnel.

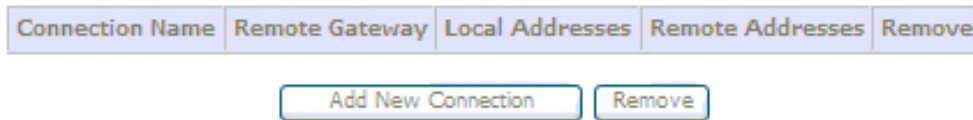


Figure 64: IPSec VPN Configuration

Click Add New Connection to create a IPSec VPN profile.

Check the Remove box and click Remove button to remove the IPSec VPN profile.

IPSec Settings

IPSec Connection Name

Remote IPSec Gateway Address (IP or Domain Name)

Tunnel access from local IP addresses

IP Address for VPN

IP Subnetmask

Tunnel access from remote IP addresses

IP Address for VPN

IP Subnetmask

Key Exchange Method

Authentication Method

Pre-Shared Key

Perfect Forward Secrecy

Advanced IKE Settings

Figure 65: IPSec VPN Settings

Global Setting

- ▶ Enter *IPSec Connection Name*
- ▶ Enter the *IP address of remote IPSec Gateway*
- ▶ Select *Tunnel access from local IP address*: subnet or single IP address
- ▶ Enter the local *IP address of VPN tunnel*
- ▶ Enter the local *IP subnet mask*
- ▶ Select the *Key exchange method*: IKE or Manual
- ▶ Select the *Authentication Method*: Pre-shared Key or Certificate (X.509)
- ▶ Enter the *Pre-shared key* if chooses Pre-shared key as the authentication method
- ▶ Select to enable or disable the *Perfect Froward Secrecy*.

- ▶ Click Show Advanced Settings for more settings.

Figure 66: IPsec VPN Advanced Settings

- ▶ There are two phases in advanced settings. There are five parameters in phase 1 and four parameters in phase 2.
- ▶ Select *Mode* from the list in phase 1: Main or Aggressive
- ▶ Select *Encryption Algorithm* from the list in phase 1 and 2: DES, 3DES, AES-128, AES-192, AES-255
- ▶ Select *Integrity Algorithm* in phase 1 and 2: MD5 or SHA1
- ▶ Set *Diffie-Hellman Group* in phase 1 and 2 for Key Exchange:
- ▶ Enter the *Key life time* in phase 1 and 2 to change the key again.
- ▶ Click *Save/Apply* to save the configuration

Certificate

The page provides the Certificate configuration. There are two sub-menu (Local and Trusted CA) are provided. “Local” means local certificates and “Trusted CA” means trusted certificate Authority certificates. Local Certificates preserve the identity of the modem. CA certificates are used by the device to verify certificates from the other hosts.

Local Certificates

Local certificates are used by peers to verify your identity.

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
<input type="button" value="Create Certificate Request"/> <input type="button" value="Import Certificate"/>				

Figure 67: Local Certificate Configuration

Click *Create Certificate Request* to generate a certificate.

Check *Import Certificate* to get a certificate from file.

Create New Certificate Request:

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

Figure 68: Create New Certificate Request

Global Setting

- ▶ Enter *Certificate Name*, *Common Name*, *Organization Name*, and *State/Province Name*.
- ▶ Select *Country/Region Name* from the list.
- ▶ Click *Apply* to create new certificate request. The generated certificate will be shown as below.

Certificate signing request

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	Test
Type	request
Subject	CN=Test/O=Xavi/ST=CA/C=US
Signing Request	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBdzCB4QIBADAAMQ0wCwYDVQQDEwRUZKXNOMQ0wCwYDVQQKEwRYYXZpMQswCQYD VQQIEwJDQTElMAkGA1UEBhMCVVMwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB AM6FwVw8BMn5zka8bkTwyjTZVNL8WOKxBDCVuAaccelnHoZO7zY4SDdp+urDyfo UV/TriMwpb6Up1TlQJ3YO2d44e9jY/JCQrxkkti5pgdo+pkCWdBtUuVdsZtODH5B Z7W26hqe7buCbB91h3sKi6uA98yRVWtWNmeK5/TAKzBhAgMBAAGgADANBgkqhkiG 9w0BAQQAFAA0BgQAEg/tTNx5rb33FqK.r.rZKH6KJ5i.rqvey3TgkHJDagV+9qzNgKo gV5hPkaAos0EuTPbGCvmOnj1P7JoKA5WmumoWYA9ucakdndfdj3k48p1oQGfkFu0 Eg1HNbTW7Ah1A7TKiGeL+gt103rUJjvjzklORGS+9qoeLKT4fkPuTDAYGA== -----END CERTIFICATE REQUEST----- </pre>

Figure 69: Generated Certificate

The certificate request needs to be submitted to a certificate authority, which would sign the request. Then the signed certificate needs to be loaded into modem. Click "Load Signed Certificate" button to load the certificate and then a new certificate is created.

Import Certificate:

Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----  
<insert private key here>  
-----END RSA PRIVATE KEY-----
```

Figure 70: Import Certificate

Global Setting

- ▶ Enter *Certificate Name*
- ▶ Enter the *Certificate* and Private Key
- ▶ Click *Apply*

Trusted CA Certificate

CA (Certificate Authority) are used by you to verify peer's certificate. It can be imported only.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

Name	Subject	Type	Action
------	---------	------	--------

Figure 71: Trusted CA (Certificate Authority) Certificates Configuration

Click Import Certificate to set certificate.

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Figure 72: Import CA Certificate

Global Setting

- ▶ Enter *Certificate Name*.
- ▶ Enter the *Certificate*.
- ▶ Click *Apply*.

7 Wireless Setup

The Wireless Setup web page menu comprises:

Basic

Security

MAC Filter

Wireless Bridge

Advanced

Station Information

Basic

The device provides wireless connection to wireless clients. This page allows you to enable the wireless service, hide the network from active scan and set the SSID (Service Set Identifier). Besides, it allows you to create a virtual wireless AP which could use different SSID and security key.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, 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

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

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 73: Wireless Setting – Basic

Global Setting

- ▶ Check to enable *Wireless feature*
- ▶ Check to enable *Hide Access Point* to hide from active scan of wireless client
- ▶ Check to isolate the wireless clients that each wireless client can not communicate

others by the device directly.

- ▶ Check to disable WMM (WiFi Multi-Media) feature. WMM takes the audio, voice, and video data stream as prioritized packet to support better performance for such applications.
- ▶ Check to enable *Wireless Multicast Forwarding*
- ▶ Enter the *wireless network name (SSID)*
- ▶ The *BSSID* is the MAC address of the device
- ▶ Select the *Country* from the list
- ▶ Input to set the maximum wireless clients the device wants to provide service.
- ▶ Check to enable *Wireless Guest Network* to create a virtual wireless AP with different SSID and security key
- ▶ Enter the Guest SSID and check necessary features such as hiding the SSID, isolating the clients, disable WMM, and maximum # of supported clients.
- ▶ Click *Save* to save the configuration

Security

The device provides wireless connection with security including authentication method and data encryption to protect your data in the air. There are two ways to configure the WiFi security, WSC (WiFi Simple Configuration) or setup manually.

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)

WSC Setup

Enable WSC: ▾

Set WSC AP Mode: ▾

Setup AP (Configure all security settings with an external registrar)
 Push-Button PIN

Device PIN: [Help](#)

WSC Add External Registrar:

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 "Save/Apply" when done.

Select SSID: ▾

Network Authentication: ▾

WEP Encryption: ▾

Figure 74: Wireless Setting – Security

Global Setting

- ▶ Select from the list to *Enable* or *Disable* the WSC (WiFi Simple Configuration).
- ▶ Select Configured or Unconfigured for *WSC AP mode* if there is an external registrar.
- ▶ Select Push-Button or PIN methods to allow Wireless client to access the device. The WPS push button is located at the rear panel of the device. You may select Push-Button and press the button to start the WPS procedure. The wireless client must start the WPS procedure within two minutes, the wireless client will be securely added into your wireless network. If you choose PIN, please enter the wireless client PIN #. Then click *Enroll* to start the process. The wireless client must start the WPS procedure within two minutes, the wireless client will be securely added into your wireless network.
- ▶ If there is an external registrar, please select *Configured* in the “Set WSC AP Mode” and then click *Start Adder* button to process the “WSC Add External Registrar”.
- ▶ To manually set the security, select the SSID from the list, then set the related security parameters
- ▶ Select the method of Network Authentication. It could be OPEN (none), Shared, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, Mixed WPA2/WPA-PSK
- ▶ Select the method of *WEP Encryption* if *Network Authentication* is Open. Select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary if WEP Encryption is enabled.

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

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

Figure 75: Wireless Setting – OPEN and WEP Security

- ▶ If the *Network Authentication* is Shared. Select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary as the same as *Network Authentication* is Open and *WEP Encryption* is enabled.
- ▶ If the *Network Authentication* is 802.1X, enter the *IP address* and *Port number* of Radius server, *Radius Key*, enable or disable *WEP encryption*. If *WEP Encryption* is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.

Network Authentication: 802.1X

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 2

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

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

Save/Apply

Figure 76: Wireless Setting – 802.1x Security

- ▶ If the *Network Authentication* is WPA, enter *WPA Group Rekey Interval*, the *IP address* and *Port number* of Radius server, *Radius Key*, WPA Encryption Method (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.

Network Authentication: WPA

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WPA Encryption: TKIP

WEP Encryption: Disabled

Save/Apply

Figure 77: Wireless Setting – WPA Security

- ▶ If the *Network Authentication* is WPA-PSK (pre-shared key), enter the WPA Pre-Shared Key and enter *WPA Group Rekey Interval*, *WPA Encryption Method* (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.

Network Authentication: WPA-PSK

WPA Pre-Shared Key: [Click here to display](#)

WPA Group Rekey Interval: 0

WPA Encryption: TKIP

WEP Encryption: Disabled

Save/Apply

Figure 78: Wireless Setting – WPA-PSK Security

- ▶ If the *Network Authentication* is WPA2, select Enable or Disable for *WPA2 Pre-authentication*, enter value of *Network Re-Auth Interval*, enter value of *WPA Group Rekey Interval*, the *IP address* and *Port number* of Radius server, *Radius Key*, WPA Encryption Method (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.

Network Authentication:	<input type="text" value="WPA2"/>
WPA2 Preauthentication:	<input type="text" value="Disabled"/>
Network Re-auth Interval:	<input type="text" value="36000"/>
WPA Group Rekey Interval:	<input type="text" value="0"/>
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Key:	<input type="text"/>
WPA Encryption:	<input type="text" value="AES"/>
WEP Encryption:	<input type="text" value="Disabled"/>

Figure 79: Wireless Setting – WPA2 Security

- ▶ If the *Network Authentication* is WPA2-PSK (pre-shared key), enter the WPA Pre-Shared Key and enter *WPA Group Rekey Interval*, *WPA Encryption Method* (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.

Network Authentication:	<input type="text" value="WPA2-PSK"/>
WPA Pre-Shared Key:	<input type="text"/> Click here to display
WPA Group Rekey Interval:	<input type="text" value="0"/>
WPA Encryption:	<input type="text" value="AES"/>
WEP Encryption:	<input type="text" value="Disabled"/>

Figure 80: Wireless Setting – WPA2-PSK Security

- ▶ If the *Network Authentication* is mixed WPA2/WPA, select Enable or Disable for *WPA2 Pre-authentication*, enter value of *Network Re-Auth Interval*, enter value of *WPA Group Rekey Interval*, the *IP address* and *Port number* of Radius server, *Radius Key*, WPA Encryption Method (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.

Network Authentication:

WPA2 Preauthentication:

Network Re-auth Interval:

WPA Group Rekey Interval:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WPA Encryption:

WEP Encryption:

Figure 81: Wireless Setting – Mixed WPA2/WPA Security

- ▶ If the *Network Authentication* is Mixed WPA2/WPA-PSK (pre-shared key), enter the WPA Pre-Shared Key and enter *WPA Group Rekey Interval*, *WPA Encryption Method* (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary

Network Authentication:

WPA Pre-Shared Key: [Click here to display](#)

WPA Group Rekey Interval:

WPA Encryption:

WEP Encryption:

Figure 82: Wireless Setting – Mixed WPA2/WPA-PSK Security

- ▶ Click Save/Apply to save the configuration.

MAC Filter

With this configuration, you could allow or deny wireless to access the device by wireless MAC address filtering feature. It is disabled as default.

Wireless -- MAC Filter

Select SSID:

MAC Restrict Mode: Disabled Allow Deny

Figure 83: Wireless MAC Filter Configuration

Global Setting

- ▶ To manually set the security, select the SSID from the list.
- ▶ Select the *MAC Restrict Mode* from one of Disable (no MAC filter), Allow (only those PCs with MAC addresses in the table can surf Internet) and Deny (only those PCs with MAC addresses in the table can not surf Internet).
- ▶ Click *Add* to add an entry or *Remove* to remove the specified entry.

Wireless – MAC Filter

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:

Figure 84: Add Wireless MAC Address

Global Setting

- ▶ Enter the *MAC Address of wireless client*
- ▶ Click *Save/Apply* to save the configuration.

Wireless Bridge

The wireless bridge feature is also known as WDS, Wireless Distribution System).

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Figure 85: Wireless Bridge Configuration

Global Setting

- ▶ Set the *AP mode* as Access Point or Wireless Bridge
- ▶ When the *AP mode* is set to Wireless Bridge, the *Wireless Restrict* determine where it can communicate with all other wireless bridges (set *Bridge Restrict* is Disabled) or just the specified MAC addresses of remote wireless bridge devices (set *Bridge Restrict* is Enable or Enable (scan)).
- ▶ Click *Refresh* to get the updated information
- ▶ Click *Save/Apply* to save the configuration

Advanced

This page allows you to configure advanced parameters for wireless communication.

The screenshot shows a configuration interface for wireless settings. The parameters and their current values are as follows:

- Band: 2.4GHz
- Channel: 1 (Current: 1)
- 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: None)
- 802.11n Rate: Auto
- 802.11n Protection: Auto
- Support 802.11n Client Only: Off
- 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
- Transmit Power: 100%
- WMM(Wi-Fi Multimedia): Enabled
- WMM No Acknowledgement: Disabled
- WMM APSD: Enabled

A 'Save/Apply' button is located at the bottom right of the configuration area.

Figure 86: Wireless Setting – Advanced

Global Setting

- ▶ Set the *Wireless Communication Band*. If you do not know it, please it as default.
- ▶ Select the *channel* from the list
- ▶ Enter the value of *Auto Channel Timer*
- ▶ Select *AUTO* or *Disable* in *802.11n/EWC* (Enhanced Wireless Consortium).
- ▶ Select the bandwidth from the list
- ▶ Set the *802.11n Rate* (Wireless Communication Rate), *AUTO* means to use the highest rate if possible)
- ▶ Set *802.11n Protection*, *AUTO* or *Disable*.
- ▶ Set *Support 802.11n client only*, *OFF* or *ON*.
- ▶ Set the *54g Rate* (Wireless Communication Rate), *AUTO* means to use the highest rate if possible)
- ▶ Set the *Rate for Multicast Packets*, *AUTO* means to use the highest if possible.
- ▶ Set the *Basic Rate*
- ▶ Set the *Fragmentation Threshold* values from 256 to 2364 bytes. If the value is too small, it may cause a result in poor performance.
- ▶ Set the *RTS (Ready to Send) Threshold*
- ▶ Set *DTIM Interval*. *DTIM* stands for *Delivery Traffic Indication Message*. This is a beacon and is a countdown informing wireless clients of the next window for listening to broadcast and multicast messages. It is a wake-up interval for clients in power-saving mode.
- ▶ Set *Beacon Interval*. The interval in milliseconds between beacon transmissions.
- ▶ Set the *Maximum Associated Wireless Client*

- ▶ Set *XPress Technology* enabled or disabled.
- ▶ Set *Transmission Power*. Larger value means more coverage.
- ▶ Select to enable or disable *WMM (Wi-Fi Multimedia)*
- ▶ Select to enable or disable *WMM No Acknowledgement*. Enabling no-acknowledge can result in more efficient throughput but high error rates
- ▶ Select to enable or disable the WMM APSD (Auto Power Saving Delivery).

Station Information

The table shows up whole associated wireless clients the device and their status.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

Refresh

Figure 87: Wireless Setting – Station Information

Global Setting

- ▶ Click Refresh to get the latest updated information

8 Voice Setup

The Voice Setup web page menu comprises:

SIP Basic Setting

Line Setting

RTP/Codec Setting

SIP Advanced Setting

SIP Basic Setting

This page allows you to configure the VoIP settings to enable the Voice service in Broadband network.

Voice -- SIP configuration

Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.

Bound Interface Name: (Note: Requires vodsl restart to take affect)

Locale selection: (Note: Requires vodsl restart to take affect)

SIP domain name:

SIP Transport Protocol: UDP TCP

Listen Port:

Maximum Redirect:

Fallover Retries: seconds.

External IP: Port:

Keep-Alive Interval: (>=30)seconds.

SIP Proxy Require:

Session Expires: seconds.

Enable Session Timer Feature.

Figure 88: SIP Basic Setting

Global Setting

- ▶ Select the *Bound Interface Name* from the list where the VoIP service is enabled.
- ▶ Select the *Location* from the list where VoIP service is enabled.
- ▶ Enter *SIP Domain Name* given by service provider.
- ▶ Check *SIP Transport Protocol*, UDP or TCP.

- ▶ Enter the *SIP Listen Port Number* which is a port number of UDP or TCP, default is 5060.
- ▶ Enter the value for *Maximum Redirect* which is the number that VoIP packet may allow to redirect or forward to.
- ▶ Enter the *Failover retrial* which service provider requests to retransmit if there is no response received.
- ▶ Enter the *External SIP IP address and Port number*.
- ▶ Enter the *Keep-alive Interval* which the device will send packet to SIP server to keep the connection alive.
- ▶ Enter the *SIP Proxy IP address* if required.
- ▶ Enter the value of *Session Expires* in seconds. The device will close the session in seconds after the call is disconnected.
- ▶ Check to enable *Session Timer* feature
- ▶ Click *Start SIP Client* to activate SIP service.
- ▶ Click *Stop SIP Client* to stop SIP service.
- ▶ Click *Restore Default Setting* to restore system default SIP settings.
- ▶ Check *Apply* to save the configuration.

Line Setting

This page allows you to configure the telephone line interfaces (TEL1 and/or TEL2) of the device.

Voice -- Line configuration

Use SIP Proxy.
SIP Proxy: Port:

Use SIP Alternate Proxy.
SIP Alternate Proxy: Port:

Use SIP Outbound Proxy.
SIP Outbound Proxy: Port:

Use SIP Registrar.
SIP Registrar: Port:

SIP Account	1	2
Account Enabled	<input type="checkbox"/>	<input type="checkbox"/>
Physical Endpt Id	<input type="text" value="0"/>	<input type="text" value="1"/>
User Id	<input type="text"/>	<input type="text"/>
Display name	<input type="text"/>	<input type="text"/>
Authentication name	<input type="text"/>	<input type="text"/>
Password	<input type="text"/>	<input type="text"/>
Preferred ptime	<input type="text" value="20"/>	<input type="text" value="20"/>
Preferred codec 1	<input type="text" value="G.711ALaw"/>	<input type="text" value="G.711ALaw"/>
Preferred codec 2	<input type="text" value="G.729a"/>	<input type="text" value="G.729a"/>
Preferred codec 3	<input type="text" value="G.723.1"/>	<input type="text" value="G.723.1"/>
Preferred codec 4	<input type="text" value="G.726_24"/>	<input type="text" value="G.726_24"/>
Preferred codec 5	<input type="text" value="G.726_32"/>	<input type="text" value="G.726_32"/>
Preferred codec 6	<input type="text" value="G.726_32"/>	<input type="text" value="G.726_32"/>
Ingress gain	<input type="text" value="0"/>	<input type="text" value="0"/>
Egress gain	<input type="text" value="0"/>	<input type="text" value="0"/>
VAD	<input type="checkbox"/>	<input type="checkbox"/>

Support VIA rport
 Use DNS SRV

Figure 89: Line Setting

Global Setting

- ▶ Check to use SIP Proxy, its IP address and Port number if necessary.
- ▶ Check to use SIP Alternate Proxy, its IP address and Port number if necessary.
- ▶ Check to use SIP Outbound Proxy, its IP address and Port number if necessary.
- ▶ Check to use SIP Registrar, its IP address and Port number is necessary.
- ▶ Check to enable SIP Account for TEL1 and TEL2 separately.
- ▶ Enter the physical Endpoint ID for TEL1 and TEL2 separately.
- ▶ Enter User ID, Display Name, Authentication Name and Password for TEL1 and TEL2

separately.

- ▶ Select the *Preferredptime* from the list.
- ▶ Select the *Preferred Codec 1 to 6* in sequence from the list for TEL1 and TEL2 separately. The preferred codec will be negotiated with peer in sequence.
- ▶ Select *Ingress Gain* and *Egress Gain* from the list separately.
- ▶ Check to enable *VAD (Voice Activation Detection)* feature separately.
- ▶ Check to enable *Support VIA rport* and *Use DNS SRV*.
- ▶ Click *Start SIP Client* to activate SIP service.
- ▶ Click *Stop SIP Client* to stop SIP service.
- ▶ Check *Apply* to save the configuration.

RTP/Codec Setting

This page allows you to RTP and Codec parameters.

Voice -- RTP/Codec configuration

DTMF Method : Inband DTMF

RFC2833 DTMF Payload Type : 101

RTP Base Port : 10000

Jitter Buffer : 5

ECHO Cancellation : Disable milliseconds

Enable FAX Pass Through

Fax Passthrough Codec : G.711 A-Law

Enable CED Tone Detection

Enable T.38 FAX

Start SIP client

Stop SIP client

Apply

Figure 90: RTP/Codec Setting

Global Setting

- ▶ Check to set the *DTMP Method*, Inband DTMF or Outband DTMF which DTMF signal is sent in the voice channel or by SIP protocol.
- ▶ Enter the *RFC2833 DTMF Payload Type*.
- ▶ Enter the *RTP Base Port number*.
- ▶ Select the *Jitter Buffer* from the list.
- ▶ Select the *Echo Cancellation* from the list.
- ▶ Check to enable *FAX Pass Through* and select the *Fax Passthrough Codec* from the list

- ▶ Check to enable *CED Tone Detection* feature
- ▶ Check to enable *T.38 Fax* feature
- ▶ Click *Start SIP Client* to activate SIP service.
- ▶ Click *Stop SIP Client* to stop SIP service.
- ▶ Check *Apply* to save the configuration.

SIP Advanced Setting

This page allows you to configure more SIP parameters and access code for more voice services.

Voice -- SIP Advanced configuration

Line	1	2
Call waiting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Forward unconditionally	<input type="checkbox"/>	<input type="checkbox"/>
Forward on "busy"	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Forward on "no answer"	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MWI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Anonymous calling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Three-way Conference	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Call Back Busy Subscriber	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unattended Call Transfer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Attended Call Transfer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Caller ID	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Registration Expire Timeout:

Registration Retry Interval:

Voip Dialpan Setting:

DSCP for SIP:

DSCP for RTP:

Feature Timer

Redial duration: minutes

Retry interval: seconds

Onhook delay: seconds

Call waiting ring timeout: seconds

Signal Timer

Call Waiting Period: seconds

Reorder Delay: seconds

Ring Timeout: seconds

No Answer Timeout: seconds

Min. Hook Flash Time: milliseconds

Max. Hook Flash Time: milliseconds

Operational Flags

Enable Call Forwarding On Server

Enable Call Return On Server

Enable Call Waiting On Server

CLIR Method: Anonymous URI Use Privacy Header

Feature Access Codes

CFWD Unconditional Activation: <input type="text" value="*21*"/>	[number]#CFWD Unconditional Deactivation: <input type="text" value="#21#"/>
CFWD No Answer Activation: <input type="text" value="*61*"/>	[number]#CFWD No Answer Deactivation: <input type="text" value="#61#"/>
CFWD On Busy Activation: <input type="text" value="*67*"/>	[number]#CFWD On Busy Deactivation: <input type="text" value="#67#"/>
Call Waiting Activation: <input type="text" value="*43#"/>	Call Waiting Deactivation: <input type="text" value="#43#"/>
Internal Call: <input type="text" value="###"/>	Call Return: <input type="text" value="69#"/>
CCBS Cancel: <input type="text" value="*37#"/>	Unattended Call Transfer: <input type="text" value="*90*"/>
CLIR: <input type="text" value="*31#"/>	CLIP: <input type="text" value="#31#"/>

Figure 91: SIP Advanced Setting

Global Setting

- ▶ Check to enable those services, *Call waiting*, *Forward unconditionally*, *Forward on "busy"*, *Forward on "no answer"*, *MWI*, *Anonymous calling*, *3-way conference*, *Call back busy subscriber*, *Unattended call transfer*, *Attended call transfer* and *Caller ID* for TEL1 and TEL2 separately if service provider provides those service in your accounts.
- ▶ Enter the value of *Registration Expired Timeout*. The device will try to register and enable SIP account in this duration until timeout.
- ▶ Enter the value of *Registration Retrial Interval*.
- ▶ Enter the *VoIP Dial Plan Setting*.
- ▶ Select the packet priority of SIP and RTP from the DSCP priority selection list.
- ▶ Enter the feature timer value for each timer, Redial duration, Retry Interval, On Hook Delay and Call Waiting Ring Timeout.
- ▶ Enter the signal timer value for each signal, Call Waiting Period, Reorder Delay, Ring Timeout, No Answer Timeout, Min. Hook Flash Time, Max. Hook Flash Time.
- ▶ Check to enable Operation Flags, Call Forwarding On Server, Call Return On Server, and Call Waiting On Server if necessary.
- ▶ Check to CLIR (Calling Line Identification Restriction) Method, Anonymous URI or Use Privacy Header
- ▶ Enter feature access code for each access feature, CFWD unconditional activation, CFWD no answer activation, CFWD on busy activation, Call waiting activation, Internal call, CCBS cancel, CLIR, CFWD unconditional deactivation, CFWD no answer deactivation, CFWD on busy deactivation, Call waiting deactivation, Call return, Unattended call transfer, and CLIP.
- ▶ Click *Start SIP Client* to activate SIP service.
- ▶ Click *Stop SIP Client* to stop SIP service.
- ▶ Check *Apply* to save the configuration.

9 Voice Supplementary Service

Call Forward

There are three types of call forward, call forward unconditional, call forward no response and call forward on busy. You could activate and deactivate these features by press keypad in the phone.

Call Forward Unconditional

Call Forward Unconditional (CFU), this enables the customer to have all incoming calls, which are addressed to his number, forwarded to another number. For the duration that Call Forward Unconditional is enabled, a stuttering dial tone shall be played instead of the normal dial tone when picking up the phone.

To configure CFU to any number:

Activation: * 21 * number #

Deactivation: # 21 #

Call Forward No Response

Call Forward No Response (CFNR) enables the customer to have all incoming calls, which meet with no reply and are addressed to his number, forwarded to another number.

To configure CFNR to any number:

Activation: * 61 * number # (forwarding after 30 s)

or: * 61 * number * ss # where ss (5-60 s) is the time until forwarding

Deactivation: # 61 #

Call Forward on Busy

Call Forward Busy Subscriber (CFBS) enables the customer to have all incoming calls, which meet with busy and are addressed to his number, forwarded to another number.

To configure CFBS to any number :

Activation: * 67 * number #

Deactivation: # 67 #

Secret Number, Calling Line Identification Restriction (CLIR)

This is a phone service that called party will not see the incoming caller phone number.

Static Configuration

Secret Number is usually an extra service and customers are charged an additional monthly fee. It must be possible to provision from remote if CLIR is enabled or disabled for each outgoing phone call.

On per call basis

Caller Line Identification Restriction (CLIR) enables a calling party to prevent presentation, on a call by call basis, of his number to the called party. This is in Sweden a regulatory requirement for an operator to provide.

Activation: # 31 # is dialed immediately before the called party number.

Call Waiting

Call Waiting (CW) enables a busy customer to be notified of a new incoming call that is in a waiting position. Then customer has the choice of accepting, rejecting or ignoring the waiting call, making use of switching orders based on R (**R means the hook flash button**).

Call Waiting customer configuration

Call Waiting is permanently enabled or disabled until disabled / enabled again. It is not on a per call basis.

Activation: * 43 #

Deactivation: # 43 #

Call Transfer

The Call Transfer enables the customer to transfer the current call to another third party.

Procedure: When A and B are engaged in a call, if A wants to transfer the call to C, so B and C can make a conversation. A presses R and dial *90*Number#, when B hear the ring back tone, the call with A will be disconnected and A hears the reorder tone and hangs up the call. The call is transferred.

Call Back Busy Subscriber (Busy)

Call Back Busy Subscriber (CCBS) enables a calling customer (A), encountering a busy destination (B), to have the retry dialing automatically until destination becomes idle, without having to make a new call attempt.

Activation: press 5 when encountering a busy tone

Deactivation: # 37 # deactivates all CCBS

The device will reattempt the last made call every 60 seconds if CCBS is activated.

The B Party alerts the original calling customer (A) with a ringing signal when the busy destination (B) becomes idle, if within 30 minutes. When the original calling customer answers the request, the former busy called party will start ringing.

After the call back ring signal timeout both sides must be disconnected from the call. B has the possibility to make a new call before A answers the call back.

Call Back last number called (Call Return)

The customer has the possibility to press *69# to call back the last number that called. It is not possible to call secret numbers. This call will be screened through the dial plans to screen any call blocking functionality enabled.

10 Diagnostic

The Diagnostic web page provides the connection check in physical layer and upper layer. The result is helpful to figure out the problem if you have a problem surfing the Internet. The Diagnostic web page menu comprises:

Diagnostics

Fault Management

Diagnostics

This page will show up the result of diagnostic in physical layer like WAN port and also upper layer of PPP if ISP provides the PPP access protocol.

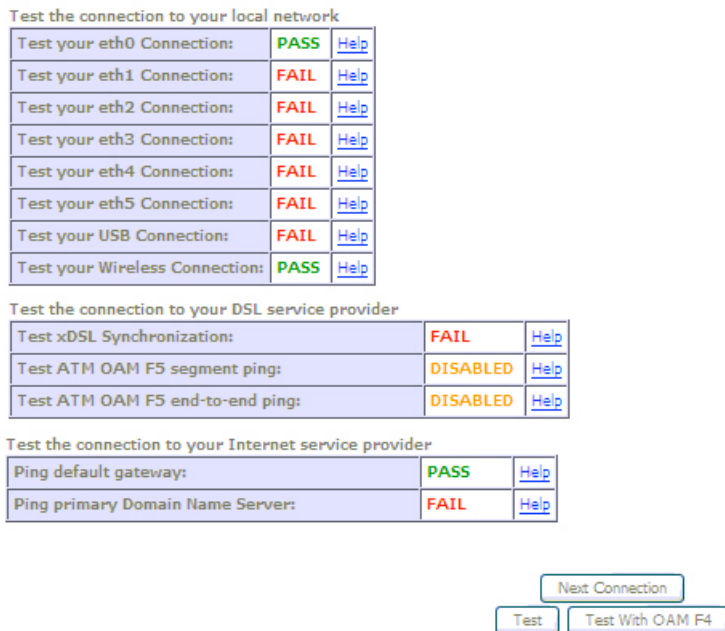


Figure 92: Diagnostic Result

Global Setting:

- ▶ Click the *Test* to test it again
- ▶ If you have setup more than one WAN service, click *Next Connection* to test next available WAN connection.
- ▶ Click *Test with OAM F4* to verify the DSL link.

Fault Management

This diagnostic page is used for VDSL PTM mode only. The 802.1ag allows an operator to detect, locate and verify faults for an Ethernet service. The connectivity check protocol is able to monitor the services continuously through periodically exchanging message to verify connectivity at a maintenance domain.

802.1ag Connectivity Fault Management

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level:

Destination MAC Address:

802.1Q VLAN ID: [0-4095]

VDSL Traffic Type:

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):

Find Maintenance End Points (MEPs)

Linktrace Message (LTM):	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 93: Fault Management

Global Setting:

- ▶ Select the Maintenance Domain (MD) Level from the list. The MD level determines the device that is interested in the contents of the CFM (Connectivity Fault Management) frame and which the CFM frame is allowed to pass through.
- ▶ Enter the Destination MAC Address
- ▶ Enter the 802.1Q VLAN ID
- ▶ Click Set MD Level.
- ▶ Click Send Loopback. It is used to do the fault verification and provides the on-demand or proactive Ethernet network topology information
- ▶ Click Send Linktrace. It is used to do the fault isolation and provides on-demand or proactive indication about the address of remote defected device

11 Management

The Management web page menu comprises:

Settings

System Log

TR-069 Client

Internet Time

Access Control

Update Software

Reboot

Settings

This page allows you to backup the current configuration of the device, update the configuration, and restore default configuration (factory setting).

Backup

Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

Backup Settings

Figure 94: Backup Settings

Click Backup Settings to backup the current settings of the device into file in PC.

Update

Tools -- Update Settings

Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

Update Settings

Figure 95: Restore Default Settings

Click *Browser* to specify the configuration file (settings) in PC and click *Update Settings* to upload the settings to the device.

Restore Default

Tools -- Restore Default Settings

Restore VoIP router settings to the factory defaults.



Figure 96: Restore Default Settings

Click Restore Default Settings to restore the factory default settings.

System Log

This page allows you to view system log and also configure system log that way you want to see.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.



Figure 97: Management Configuration – System Log

Global Setting

- ▶ Click *View System Log* to view system log
- ▶ Click *Configure System Log* to configure the way you want to see

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 'Save/Apply' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

Mode:



Figure 98: Management Configuration – Configure System Log

Global Setting

- ▶ Select to *Enable Log* function or not
- ▶ Select *Log Level* from the list
- ▶ Select *Display Level* from the list
- ▶ Select *Mode* from the list
- ▶ Click *Save/Apply* to save the configuration.

TR-069 Client

This page allows you to access TR-069 ACS (Auto-Configuration Server). The ACS can provision, configure, and diagnostic the device from remote site.

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:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

Figure 99: Management Configuration – Firmware Upgrade

Global Setting

- ▶ Select to *Enable* or *Disable* to send *Inform* packet to ACS.
- ▶ Enter the *Inform Interval* number of seconds. The Inform packet will be sent to ACS periodically.
- ▶ Enter the *ACS URL* to reach ACS
- ▶ Enter the *ACS User Name* and *Password*
- ▶ Enter the *WAN interface* used by TR-069 client to send TR-069 packets
- ▶ Select to *Enable* or *Disable* to send the TR-069 SOAP messages to serial console port. This is usually used for trouble shooting purpose.
- ▶ Check to enable *Connection Request Authentication*
- ▶ Enter the *Connection Request User Name* and *Password*
- ▶ Click *Save/Apply* to save the configuration

Internet Time

This page allows you to sync up the real time clock from Internet. .

Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

Save/Apply

Figure 100: Internet Time Configuration

Global Setting

- ▶ Check to enable *Automatically synchronize with Internet time servers*
- ▶ Click **Save** to save your settings

Access Control

This submenu provides you to configure the change the passwords of admin, support and user accounts.

Password

There are three levels of access accounts: admin, support, and user. The user name "admin" has unrestricted access to change and view configuration of the device. The user name "support" is used to allow an ISP technician to access the device for maintenance and to run diagnostics. The user name "user" can access the device, view configuration settings and statistics, as well as updaet the device software.

Access Control -- Passwords

Access to your DSL 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 DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL 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" to change or create passwords. Note: Password cannot contain a space.

Username:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

Save/Apply

Figure 101: Management Configuration – Access Control: Password

Global Setting:

- ▶ Select the level of *Username*
- ▶ Enter the *Old Password*
- ▶ Enter the *New Password* and *Confirm Password*
- ▶ Click *Save/Apply* to save the configuration.

Update Software

This page allows you to upgrade the software (firmware).

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 DSL Router will reboot.

Software File Name:

Figure 102: Management Configuration – Update Software

Global Setting:

- ▶ First of all, you have to get the updated software (firmware) from ISP or manufacture.
- ▶ Click *Browser* to specify the location and filename
- ▶ Click *Update Software* to start the process. It could take minutes to complete it.

Reboot

This page allows you to reboot the device.

Click the button below to reboot the router.

Figure 103: Management Configuration – Reboot

Global Setting

- ▶ Click *Reboot* to reboot the device

Appendix A - Configuring the Network Settings

To surf Internet through the device, you need to configure the network settings of your PC correctly. This appendix provides the guide for a reference.

Configuring Ethernet (LAN) Card

Before you begin

By default, the device automatically assigns the required Internet settings to your PCs. You need to check your PCs to get the information automatically. If you need to set the information manually, please make sure you get enough information from service provider and configure the network settings of PC correctly.

If you have connected your LAN PCs via Ethernet to the device, please follow the instructions to configure the network settings in Windows XP (for example). The instructions for different Windows system are very similar, please refer its manual separately.

Windows XP PCs

Click the *Start* button, and then click *Control Panel*, and then click the *Network connection icon*. In the *LAN* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

Make sure that the check box of *Internet Protocol TCP/IP* is checked and click *Properties*. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled Obtain an IP address automatically and also click the radio button labeled Obtain DNS server address automatically. The PC will send inquiry packet to the device to get an IP address, gateway IP address, DNS IP address and son on automatically.

Click *OK* to confirm your changes, and then close the Control Panel.

Assigning static IP addresses to your PCs

If you are professional in networking and subscribe to public IP addresses from service provider, you need to assign the public IP address and associated information to the PCs manually. For example, you may provide public WEB server in your LAN environment, you need to assign public IP address in the WEB server. Basically, you need the information from your service provider.

1. The IP address and subnet mask of each your PC.
2. The gateway IP address for PC to send packets to.
3. The DNS server IP address.

With above information, you are ready to configure your PCs.

Click the *Start* button, and then click *Control Panel*, and then click the *Network connection icon*. In the *LAN* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

Make sure that the check box of *Internet Protocol TCP/IP* is checked and click *Properties*. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button to enter the LAN IP address, subnet and gateway IP address manually. Besides, click the radio button to enter DNS IP address manually.

Click *OK* to confirm your changes, and then close the Control Panel.

Configuring Wireless LAN card

If your PC is connected to the device through wireless link, you need to configure the network setting of wireless LAN card in stead of LAN card. The steps to configure the network settings of wireless LAN card are the same procedure described in previous section, Configuring Ethernet LAN cardf section.

Wireless card and drivers

You need to install the wireless card and drivers correctly. Please check the information of installation and security of wireless card provided by the wireless card vendor or notebook vendor.

Configuring wireless device

The following steps provide a basic guide line to configure the wireless card to establish a wireless connection to the device.

To configure wireless card to establish a connection to the device:

1. Make sure the wireless access card is installed.
2. Make sure the wireless driver is installed.
3. Scan the available wireless AP (Access Point) and find the SSID of the device
4. Connect to the AP
5. Enter the security code (WPA, WEP or others) if necessary

Then you have a connection to the device through wireless link.

Appendix B - Troubleshooting

During the installing or using the device, you may encounter problem, this appendix provides the solution and instructions to solve the issues. In case, the problem can not be solved, please contact Customer Support for further support.

Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
LEDs	
<i>Power LED does not illuminate after product is turned on.</i>	Verify that you are using the power adapter provided with the device and that it is securely connected to the device and a wall socket/power strip.
<i>LAN LED does not illuminate after Ethernet cable is attached to your PC.</i>	Verify that the Ethernet cable is securely connected to your LAN switch or PC and to the device. Make sure the PC and/or hub is turned on.
Internet Access	
<i>Cannot access the Internet</i>	Use the ping utility provided by PC's system to check whether your PC can communicate with the device. Command: ping device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you assigned a private IP address to your PC, (not a public address), please check the IP addresses of gateway and DNS server in your PC network settings. Those IP addresses should be given by service provider. Otherwise, configure the PC to receive the IP, gateway IP and DNS IP automatically.
<i>Cannot surf web pages on the Internet.</i>	Verify that the DNS server IP address in the PCs is correct for your ISP. If you configured that the DNS server be assigned automatically from a server, then verify with your ISP that the address configured on the device is correct.
Device's Web pages	
<i>Forgot my user ID or password.</i>	The default setting of username and password is "admin". If you failed to access the device by enter this. You can reset the device to the default configuration by pressing the Reset Default button on the front or rear panel of the device. Then, type the default Username (admin) and password (admin). WARNING: Reset Default means the device returns all settings to their default values.

Problem	Troubleshooting Suggestion
<i>Cannot access the web pages</i>	<p>Verify the Ethernet connection by using ping utility. Command: ping device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.</p> <p>Verify that you are using latest Internet Explorer or Netscape Navigator or other browsers.</p> <p>Verify that subnet mask: the PC's IP address should be defined as being on the same subnet as the IP address of the LAN port on the device.</p>
<i>Changes/settings to the web pages are not being saved.</i>	Be sure to save the configuration after any changes.

IP Utilities for diagnostic

Ping

Ping is a simple command and easy way to check remote PC or device on your network and the Internet. Besides, this is a command supported in most of IP-based network operation system like Windows, Linux and so on. To use it, you must know the IP address of the PC or device which you like to send a message to. If the remote PC or device gets this message, the PC or device will send back a message in reply. If you saw the reply, you know the communication link to remote PC or device is OK. In Windows system, you can execute a ping command from the Start menu by clicking the Start button, and then clicking Run and then enter below statement in the open box: (the 192.168.1.1 is an IP address which you like to check the device is on line or not.)

ping 192.168.1.1

Click OK.

If the communication link is OK, you will see the message and a Command Prompt window is displayed as an example:

```

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

If not, you will receive the message Request timed out.

You could also use this ping tool to verify the Internet connection by entering an external address, such as www.yahoo.com. If you do not know the IP address of a particular Internet location, you can use the nslookup command as described in the following section.

Please be noted that some of PCs or devices may reject to reply message requesting by ping command. At that time, you won't get message in reply, but message timeout.

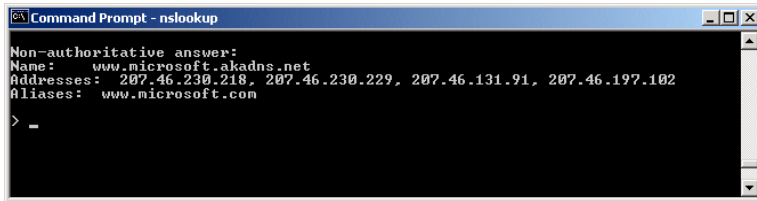
Nslookup

There is another useful command provided by Windows system. You can use the nslookup command to get the IP address associated with a domain name like www.yahoo.com or www.microsoft.com. The nslookup command looks up the domain name in on your DNS server located in your service provider. The server then returns the associated IP address. In Windows system, you can execute the nslookup command by clicking the Start button and then clicking Run and then entering below statement in the open box.

Nslookup

Click OK.

A Command Prompt window is prompted. Enter the domain name like www.yahoo.com or www.microsoft.com. The associated IP address will be shown as below



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

In this case, you see multiple IP addresses associated with that domain name. It is common for Web server. System engineers prepare multiple and redundant servers to handle the heavy traffic and also balance the load in each server.

Appendix C - Specification

A1. Hardware Specifications

- Local Interface
 - Four port 10Base-T/100Base-TX Ethernet Switch (4 * RJ-45 connectors), IEEE 802.3u with MDI/MDIX auto-detection
 - Two USB 2.0 Host Port
 - 10/100/1000Base-T Gigabit Ethernet port
 - Integrated 802.11b/g/n WLAN Access Point
- WAN DSL Line Interface
 - Compliant with ITU-T G.993.1, G.993.2 with profile 8x, 12x and 17a. ANSI T1.424 trial use standard, ETSI TS 101270, IEEE 802.3ah 10 PASS TS D2.1, China's national VDSL standards.
 - Compliant with ITU-T G.992.1, G.992.2, G.992.3, G.992.5 and ANSI T1.413 Issue 2
 - Annex A (over PSTN) or B (over ISDN) is supported by different model.
 - Line Impedance: 100 Ω
 - Connection Loops: One (pair wire)
 - Connector: RJ-11
 - Optional 10/100/1000Base-T Gigabit Ethernet WAN port in RJ-45, comply with IEEE 802.3/802.3u/802.3ab
- Indicators
 - PWR – Green LED indicates power and operation. Red LED indicates failure.
 - LAN – Green LED indicates LAN connection
 - GE LAN – Orange LED indicates 1000Mbps connection speed and Green LED indicates 100Mbps
 - TEL1 and TEL2 – Green LED indicates SIP registered and Orange LED indicates off-hook.
 - WLAN – Green LED indicates wireless AP enabled
 - USB – Green LED indicates USB connection
 - DSL – Green LED indicates broadband connection
 - Internet – Green LED indicates PPP connection and Red LED indicates PPP failure or device in BRIDGE mode.
- OAM&P
 - Local: Telnet and Web management
 - Remote: Telnet and Web Management
- Environment
 - Operation Temperature: 0°C ~ 40°C
 - Operation Humidity: 5% ~ 95%
 - Storage Temperature: -20 ~ +70°C
 - Storage Humidity: 5%~95%
- Power
 - AC Adapter: Input 100~240VAC, 50/60Hz; Output 12VDC 2A
- Certificates
 - CE, CB (TBD)

A2. Software Specifications

- Bridging
 - Transparent Bridging and spanning (IEEE 802.1D) with at least 32 MAC addresses
 - RFC2684 (RFC 1483) Bridged
 - Bridge filtering with per-port extensions

- Routing
 - IP routing and PPP supported
 - PAP and CHAP for user authentication in PPP connection
 - RFC2684 (RFC1483) Routed
 - MAC Encapsulated Routing (MER)
 - DHCP client, server and relay agent
 - DNS relay
- Wireless LAN
 - Supports 802.1x; WEP; WEP2; WPA; WPA2; TKIP; AES; 802.11i
 - Hidden SSID
 - WMM for advanced Quality of Service
 - Hardware based AES
- Firewall
 - Support NAT and DMZ
 - Protection against IP and MAC address spoofing
 - UPnP NAT traversal and VPN / IPSec pass-through
- USB 2.0 Host
 - Support printer server
 - Support mass storage device and Samba for file sharing inside local network
- Voice Features
 - Support voice codecs like G.711, G.726, G.729ab, BV16, ILBC, T.38 and etc
 - G.168 line echo cancellation with programmable tail.
 - Adaptive jitter buffer, packet loss concealment (PLC), voice activity detection (VAD), comfort noise generation (CNG) and Caller ID.
 - DTMF tone detection and generation, Fax/modem detection and pass-through
 - Support in-band DTMF tone sending/receiving and out-band DTMF signaling with RTP.
 - Support SIP and telephone URL addressing
 - Bonus services: call forwarding, call waiting, call transfer, and etc.
- Configuration and Network Management Features
 - SNMP GETs, SETs and TRAPs for four groups in MIB-II
 - DHCP client and server for IP management
 - UPnP Internet Gateway Device (IGD) compliance
 - WEB for local or remote management
 - HTTP or TFTP for firmware upgrade and configuration
 - Support TR-069, TR-104 and with parameters: DeviceInfo, ManagementServer, Time, IPPingDiagnostic, etc

Note: The hardware and software specifications are subjected to change without notices.

Appendix D - Warranties

B1. Product Warranty

Inteno Broadband Technology AB warrants that the unit will be free from defects in material and workmanship for a period of twelve (12) months from the date of shipment.

Inteno Broadband Technology AB shall incur no liability under this warranty if

- The allegedly defective goods are not returned prepaid to Inteno Broadband Technology AB within thirty (30) days of the discovery of the alleged defect and in accordance with Inteno Broadband Technology AB ' repair procedures; or
- Inteno Broadband Technology AB ' tests disclose that the alleged defect is not due to defects in material or workmanship.

Inteno Broadband Technology AB liability shall be limited to either repair or replacement of the defective goods, at Inteno Broadband Technology AB option.

Inteno Broadband Technology AB MARKS NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE USER'S DOCUMENTATION. INTENO SHALL NOT BE RESPONSIBLE FOR CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES.

B2. Warranty Repair

1. During the first three (3) months of ownership, Inteno Broadband Technology AB will repair or replace a defective product covered under warranty within twenty-four (24) hours of receipt of the product. During the fourth (4th) through twelfth (12th) months of ownership, Inteno Broadband Technology AB will repair or replace a defective product covered under warranty within ten (10) days of receipt of the product. The warranty period for the replaced products shall be ninety (90) days or the remainder of the warranty period of the original unit, whichever is greater. Inteno Broadband Technology AB will ship surface freight. Expedited freight is at customer's expense.
2. The customer must return the defective product to Inteno Broadband Technology AB within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, Inteno Broadband Technology AB will bill the customer for the product at list price.

B3. Out-of-Warranty Repair

Inteno Broadband Technology AB will either repair or, at its option, replace a defective product not covered under warranty within ten (10) working days of its receipt. Repair charges are available from the Repair Facility upon request. The warranty on a serviced product is thirty (30) days measured from date of service. Out-of-warranty repair charges are based upon the prices in effect at the time of return.

Appendix E - Contact information

You can help us serve you better by sending us your comments and feedback. Listed below are the addresses, telephone and fax numbers of our offices. You can also visit us on the World Wide Web at www.inteno.se for more information. We look forward to hearing from you!

HEADQUARTER

Inteno Broadband Technology AB

Drivhjulsvägen 22, SE-126 30, Hägersten, Sweden
Tel: +46 8 579 190 00

NORWAY OFFICE

Inteno Broadband Technology AS

Solheimveien 36, N-1473, Lørenskog, Norway
Tel: +47 67 91 19 30

FINLAND OFFICE

Vaasa

Oy Netmedia Finland Ab
Vaasanpuistikko 18, 3.kerros
PL 98, 65101 VAASA
Tel: +358 6 3181 300

Helsinki

Oy Netmedia Finland Ab
Rälssintie 10
00720 HELSINKI
Tel: +358 9 347 8540

DENMARK OFFICE

Inteno Denmark AS

Højbyvej 19
DK-4320 Lejre, Denmark
Telephone +45 51 555 936