

User Manual



GW-632FW

Active Ethernet IAD with VoIP
Wireless LAN and Gigabit Ethernet Switch



CTC UNION TECHNOLOGIES CO., LTD.

CTC Union Technologies Co., Ltd.

Far Eastern Vienna Technology Center (Neihu Technology Park)

8F, No. 60 Zhouzi St.

Neihu District

Taipei 114

Taiwan

Tel: +886-2-26591021

Fax: +886-2-27991355

Email: sales@ctcu.com

techsupport@ctcu.com

URL: <http://www.ctcu.com>

GW-632FW User Manual

Fiber Ethernet IAD Gateway

Version 1.0 October, 2013

We make no warranties with respect to this documentation and disclaim any implied warranties of merchant-ability, quality, or fitness for any particular purpose,. The information in this document is subject to change without notice. We reserve the right to make revisions to this publication without obligation to notify an person or entity of any such changes.

Trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective companies,

Table of Contents

1	Introduction	1
	Features	1
	Device Requirements	2
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 the fiber network or broadband device like DSL modem, cable modem or fiber modem</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 and connect Wireless PCs if the device is with wireless interface</i>	<i>7</i>
	<i>Next step.....</i>	<i>7</i>
4	Getting Start with the Web pages	8
	Accessing the Web pages.....	8
	Testing your Setup.....	11
	Default device settings.....	11
5	Device Information	13
	Summary.....	13
	WAN	14
	Statistic.....	14
	Route	14
	ARP	15
	DHCP	15
	Voice.....	15
6	Advanced Setup.....	17
	Layer2 Interface	17
	WAN Service.....	18
	<i>PPP over Ethernet (PPPoE).....</i>	<i>20</i>
	<i>IP over Ethernet.....</i>	<i>22</i>
	<i>Bridging.....</i>	<i>23</i>
	LAN.....	24
	<i>IPv6 Autoconfig.....</i>	<i>25</i>
	NAT (Network Access Translation).....	25
	<i>Virtual Server</i>	<i>26</i>
	<i>Port Triggering</i>	<i>27</i>

	<i>DMZ Host</i>	28
	Security	28
	<i>IP Address Filter</i>	28
	Parental Control	31
	<i>URL Filter</i>	32
	Quality of Service.....	33
	<i>QoS Queue</i>	33
	<i>QoS Classification</i>	34
	Routing.....	36
	<i>Default Gateway</i>	36
	<i>Static Route</i>	37
	<i>Policy Routing</i>	37
	<i>RIP</i>	38
	DNS.....	39
	<i>DNS Server</i>	39
	<i>Dynamic DNS</i>	40
	Print Server	41
	DLNA.....	41
	Storage Service	42
	<i>Storage Device Info</i>	42
	<i>User Accounts</i>	42
	Interface Grouping	43
	IP Tunnel.....	44
	<i>IPv6 in IPv4 Tunnel</i>	45
	<i>IPv4 in IPv6 Tunnel</i>	45
	IPSec.....	46
	Certificate	48
	<i>Local</i>	48
	<i>Trusted CA</i>	50
	Power Management	51
	Multicast	52
7	Wireless Setup	53
	Basic.....	53
	Security	54
	MAC Filter	58
	Wireless Bridge.....	59
	Advanced	60
	Station Information.....	61
8	Voice Setup	62
	Interface Setup.....	62
	SIP Basic Setting	63
	SIP Advanced Setting.....	65
9	Diagnostic.....	67
	Diagnostic.....	67

10	Management.....	68
	Settings	68
	System Log	69
	Security Log	70
	TR-069 Client.....	70
	Internet Time	71
	Access Control.....	72
	<i>IP Address</i>	72
	<i>Service</i>	73
	<i>Password</i>	73
	Update Software	74
	Reboot.....	74
	Logout	75
	Appendix A - Configuring the Internet Settings	76
	Configuring Ethernet PCs.....	76
	<i>Assigning static Internet information to your PCs</i>	76
	Configuring Wireless PCs.....	77
	<i>Positioning the wireless PCs</i>	77
	<i>Wireless PC cards and drivers</i>	77
	<i>Configuring PC access to your Wireless device</i>	77
	Appendix B - Troubleshooting	78
	Troubleshooting Suggestions.....	78
	Diagnosing Problem using IP Utilities	79
	<i>Ping</i>	79
	<i>Nslookup</i>	80
	Appendix C - Specification	81
	Appendix D - Regulation	83

1 Introduction

Congratulations on becoming the owner of the **GW-632FW**, Active Ethernet IAD. You will now be able to access the Internet using your high-speed connection.

The **GW-632FW** is an IAD integrating wireless, VoIP, and Ethernet interfaces into one device which provides the most flexibility and efficiency way to you. You could connect devices like PCs, Set-Top-Box, servers, phone, and so on easily by Ethernet, wireless, and VoIP interfaces to enjoy data, voice, and video services immediately through high speed connection.

This User Guide will show you how to connect your **GW-632FW** Active Ethernet IAD 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 (**GW-632FW**) 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:

- Active Ethernet interface (Fiber) automatic speed-sensing and crossover correction supports up to 1000 Mbps downstream and 1000 Mbps upstream rates
- AE 1310 nm TX . 1490/1550 nm RX
- Integrated four-port 10/100/1000BaseTX Ethernet switch with speed-sensing and crossover detection automatically
- 802.11b/g/n WLAN supports up to 300 Mbps transmission rate
- Provides wireless secure transmitting encryption by either 802.1x; WEP; WEP2; WPA; WPA2; TKIP; AES; 802.11i
- Supports 2 FXS ports for VoIP application including call waiting, call forward, call transfer and so on
- Support voice CODECs like G.711, G.726, G.729AB, BV16, ILBC, T.38 etc.; programmable G.168 echo cancellation, adaptive jitter buffer and packet loss concealment
- Supports Voice activity detection (VAD), comfort noise generation (CNG) and caller ID
- Supports DTMF tone detection and generation; Fax / Modem detection and pass-through
- Support SIP signaling protocol and bonus services like call forwarding, call waiting, call transfer, call busy, call return, enquiry service, CLIP/CLIR and three way conference
- Support Networking protocols such as PPP, Routing, DHCP server / relay / client
- Network address translation (NAT) functions to provide security for your LAN and multiple PCs surfing Internet simultaneously.
- Configuration and management by Web-browser through the Ethernet interface and remotely through WAN interface
- Firmware Support TR-069
- Upgradeable through HTTP / TFTP

Device Requirements

In order to use the **GW-632FW**, you must have the following:

- ▶ High speed broadband service with Active Ethernet Fiber
- ▶ 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 or wireless card.
- ▶ For system configuration a web browser such as Internet Explorer.



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 (GW-632FW)***
- ▶ ***Ethernet cable***
- ▶ ***Phone cable***
- ▶ ***Power adapter***


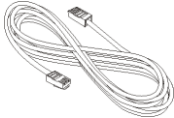
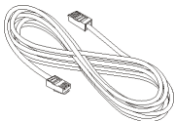

	GW-632FW device
	RJ-45 Cable
	RJ-11 Cable
	Power adapter

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.



Figure 2: Front Panel and LEDs

Connector and LED definitions from left to right:

Label	Color	Function
Power	Green Red	GREEN off: No power GREEN on: Power on RED on: Self-test fails
WAN	Green Yellow	GREEN on: Physical layer sync up 1Gbps YELLOW on: Physical layer sync up 100Mbps Off: No connection or no signal
Ethernet	Green	On: LAN link established and active Off: No LAN link
WiFi	Green	On: WLAN service is enabled Off: WLAN service is disabled
TEL1	Green	On: make or receive a phone call Off: disconnect the phone call Slow blink: SIP registration failure Fast blink: incoming call (ringing)
TEL2	Green	On: make or receive a phone call Off: disconnect the phone call Slow blink: SIP registration failure Fast blink: incoming call (ringing)
Internet	Green Red	GREEN on: device gets an IP RED on: device is getting an IP Off: Device is in Bridge mode or power off
USB	Green	On: detects an USB device Off: no USB link
WPS	Green	On: device is in WPS mode Off: device is not in WPS mode

Rear Panel

The rear panel of this device will be described here which cover all rear panel definitions of other models.

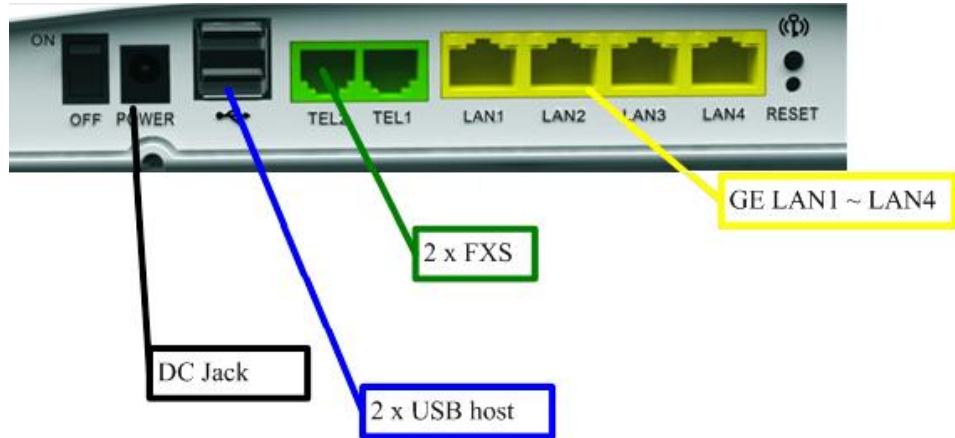


Figure 3: Rear Panel Connections

Connector definition:

Label	Function
Power Switch	ON/OFF switch
Power Jack	Connects to the supplied power adapter
USB	Connects to the USB devices
TEL 1 ~ TEL2	Connects to analog telephones for VoIP service
LAN1 ~ LAN4	Connects the device via Ethernet to your devices in LAN
WPS	Press to enter wireless WPS mode
RES	A reset button to reset the device or reset to default settings
SFP	Connects to the fiber broadband network
WAN Jack 2	Connects to the broadband network

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:

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.

Step 1. Connect the WAN port to the fiber network or broadband device like DSL modem, cable modem or fiber modem

Connect the WAN port to fiber network or the broadband device like DSL modem, cable modem or fiber modem which has the high speed internet connection.

Step 2. Connect the Ethernet cable

Connect up to four single Ethernet computers to the device via Ethernet cable(s).

Note that the cable does not need to be crossover cable, 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 the device and PCs.

Step 4. Configure your Ethernet PCs

You must also configure the Internet properties on your Ethernet PCs. See Appendix A.

Or, step 5. Install a Wireless card and connect Wireless PCs if the device is with wireless interface

You can attach a Wireless LAN that enables Wireless PCs to access the Internet via the device.

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

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. The minimum browser version requirement is Internet Explorer v4 or Netscape v4. For the best display quality, use latest version of Internet Explorer, Netscape or Mozilla Firefox. From any of the LAN computers, launch your web browser, type the URL, <http://192.168.1.1> in the web address (or location) box, and press [Enter]. The default IP address of the device is 192.168.1.1. 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, DHCP and Voice.

Device Info

Summary

WAN

Statistics

Route

ARP

DHCP

Voice

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 Proxy, Print Server, DLNA, Storage service, Interface Grouping, IP Tunnel, IPSec, Certificate, Power Management and Multicast.

Advanced Setup

Layer2 Interface

WAN Service

LAN

NAT

Security

Parental Control

Quality of Service

Routing

DNS

UPnP

DNS Proxy

Print Server

DLNA

Storage Service

Interface Grouping

IP Tunnel

IPSec

Certificate

Power Management

Multicast

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 the VoIP Setup. It includes the sub menus, Interface Setup, SIP Basic Setting and SIP Advanced Setting.

Voice

Interface Setup

SIP Basic Setting

SIP Advanced Setting

Diagnostic: provides the diagnostic utility to check the LAN and Wireless physical connection and WAN connection as well.

Diagnostics

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

Management

Settings

System Log

Security Log

TR-069 Client

Internet Time

Access Control

Update Software

Reboot

Logout

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 green 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.
Ethernet	Solid green to indicate that the device can communicate with your LAN.
Internet	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 is enabled	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

Voice.

Summary

The Summary Page of the device shows the following information, Board ID, Build Timestamp, Software version, Bootloader version, Wireless driver version, Voice driver version and device uptime. Besides, more information is supported like LAN IP, Default gateway, Primary DNS server, Secondary DNS server, LAN IPv6, default IPv6 gateway (if you have configured the device to use IPv6 to connect to ISP) and current system time.

Device Info

Board ID:	96816PVWM
Build Timestamp:	110518_2330
Software Version:	MSG2110-GE-FXS_4.10RCT01.04
Bootloader (CFE) Version:	1.0.37-110.4
Wireless Driver Version:	5.100.96.0.cpe4.10L01a.4
Voice Service Version:	FG500_1.6.7
Uptime:	6D 4H 27M 36S

This information reflects the current status of your WAN connection.

LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Wed Jan 7 04:27:36 1970

Figure 6: Device Information

WAN

The WAN information of the device shows detailed information about the WAN connection such as VLAN ID, WAN port service information, Protocol, IPv6 enabled or disabled, IGMP enabled or disabled, Quality of Service enabled or disabled, IP address of WAN port and so on.

WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address
eth4.1	ipoe_eth4	IPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	Unconfigured	0.0.0.0

Figure 7: WAN Port Information

Statistic

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

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN1	38559	257	0	0	130597	195	0	0
LAN2	365696150	798948	0	0	87135503	190343	0	0
LAN3	21511	141	0	0	100546	528	0	0
LAN4	0	0	0	0	0	0	0	0
wl0	0	0	2	0	0	0	184910	0
(null)	0	0	0	0	0	0	0	0

Reset Statistics

Figure 8: Device LAN Port Statistic Information

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth4.1	ipoe_eth4	0	0	0	0	0	0	0	0

Reset Statistics

Figure 9: Device WAN Port 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, I - 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 10: 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
192.168.1.199	Complete	00:13:72:17:e7:98	br0

Figure 11: 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
EricChangNB	90:4c:e5:7c:5a:6f	192.168.1.2	0 seconds
android_f500f6107464d2b3	f4:c7:14:21:0c:01	192.168.1.3	0 seconds
android-tattoo	00:23:76:57:f4:f8	192.168.1.4	11 hours, 22 minutes, 40 seconds
android-c82b0c4fd0dd3d99	40:fc:89:e5:b5:64	192.168.1.5	0 seconds
X-MAN	00:03:25:0f:1a:b4	192.168.1.7	0 seconds

Figure 12: Device DHCP Table Information

Voice

The Voice Page of the device shows the SIP account information such as extension and user status of TEL port1 and 2.

Voice -- VoIP Status

SIP Account	0	1
Extension		
User status		

Figure 13: Device Voice Status

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 Proxy, Print Server, DLNA, Storage service, Interface Grouping, IP Tunnel, IPSec, Certificate, Power Management and Multicast.

Layer2 Interface

WAN Service

LAN

NAT

Security

Parental Control

Quality of Service

Routing

DNS Proxy

Print Server

DLNA

Storage Service

Interface Grouping

IP Tunnel

IPSec

Certificate

Power Management

Multicast

Layer2 Interface

The WAN configuration is divided by two steps, one is to setup the Layer 2 interface and the other is to setup the WAN service including protocols. In this page, you could add an Ethernet WAN interface via clicking “add” to continue the setup.

ETH WAN Interface Configuration

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

Interface/(Name)	Connection Mode	Remove
------------------	-----------------	--------

Figure 14: Layer 2 Interface Setup Page

In this page, please select an ETH port from the list, usually select the “eth4/WAN” as WAN layer2 interface.

ETH WAN Configuration
This screen allows you to configure a ETH port .

Select a ETH port:

eth4/WAN ▼

Select Connection Mode

☒ Default Mode - Single service over one connection

☐ VLAN MUX Mode - Multiple Vlan service over one connection

Back Apply/Save

Figure 15: Add a Layer 2 WAN Interface Page

To configure ETH WAN (Layer 2 interface) configuration:

- ▶ Select an *ETH port* from the list.
- ▶ Check the *connection mode*:
 - Default Mode*: Single service over one connection
 - VLAN MUX Mode*: Multiple VLAN service over one connection such as data, voice, and video services simultaneously with different VLAN IDs.
- ▶ Click *Apply/Save* to save the configuration

WAN Service

You can configure your internet connection from this page. This page displays the details of existing internet connection and also allows you to add more WAN service. There are three connection types can be configured including PPP over Ethernet (PPPoE), IP over Ethernet, and Bridging.

Wide Area Network (WAN) Service Setup
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
-----------	-------------	------	-----------	-----------	------	-----	----------	------	-----	--------	------

Add Remove

Figure 16: WAN Service Setup Page

Click “Add” to add a new WAN service and then select the WAN Layer 2 interface from the list.

WAN Service Interface Configuration

Select a layer 2 interface for this service

eth4/WAN ▾

[Back](#) [Next](#)

Figure 17: WAN Service Setup – Select a layer 2 interface

Click “Next” to continue the configuration. The parameters of each following page will be varied and depended on the WAN layer 2 interface (default mode or VLAN MUX mode). Most of cases the VLAN MUX mode covers the settings of default mode. The VLAN MUX mode will be introduced and described in details.

WAN Service Configuration

Select WAN service type:

- ☒ PPP over Ethernet (PPPoE)
- ☐ IP over Ethernet
- ☐ Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

☐ Enable IPv6 for this service

[Back](#) [Next](#)

Figure 18: WAN Service Configuration

To configure WAN Service Configuration:

- ▶ Select the *WAN service type*: PPPoE, IPoE or Bridge
- ▶ Enter the *Service Description*
- ▶ Enter *802.1P priority [0-7]*, set -1 for untagged service
- ▶ Enter *802.1Q VLAN ID [0-4094]*, set -1 for untagged service
- ▶ Check to *enable IPv6 service* if necessary
- ▶ Click *Next*

PPP over Ethernet (PPPoE)

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: **AUTO** ▼

☐ Enable Fullcone NAT

☐ Dial on demand (with idle timeout timer)

☐ PPP IP extension

☐ Use Static IPv4 Address

☐ Enable PPP Debug Mode

☐ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

☐ Enable IGMP Multicast Proxy

Figure 19: WAN Connection, PPPoE Configuration

To configure the PPPoE settings:

- ▶ Enter the User's *PPP Username* and *Password*
- ▶ Enter the *Service Name* if any
- ▶ Select the *Authentication Method* used during negotiation, default is **AUTO**.
- ▶ Check to *Enable Fullcone NAT*. The device will process all requests from the same internal IP address and port are mapped to the same external IP address and port
- ▶ Check *Dial On Demand* if you do not need PPPoE connection always ON and enter the timeout value (1-4320 minutes) to disconnect the PPPoE connection when connection is idle and timeout.
- ▶ Check the *PPP IP extension* if your 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 IP 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* to get more debug message for analysis if necessary
- ▶ Check to *Enable Bridge PPPoE frames between WAN and local ports* if necessary
- ▶ Check to *Enable Multicast IGMP Proxy* if necessary
- ▶ Click *Next*

Configure the default routing (gateway) WAN interface and click “Next”.

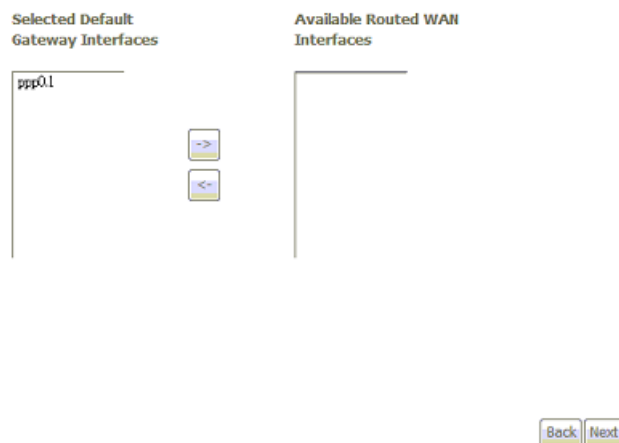


Figure 20: WAN Service Default Routing Configuration

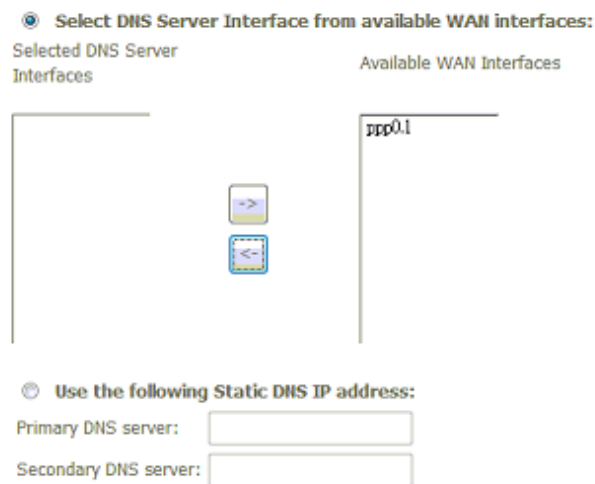


Figure 21: WAN Service DNS server Configuration

To configure WAN DNS Server Configuration:

- ▶ Check to use *Select DNS server interface from the available WAN interfaces* or “*use the following Static DNS IP address*”
- ▶ Enter the *Primary DNS server* and/or *Secondary DNS server* IP address.
- ▶ Click *Next*

WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Enabled
Multicast VLAN Filter:	
Quality Of Service:	Disabled

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

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

Figure 22: WAN Setup Summary

The *WAN Setup Summary* page as previous WAN Setup Summary figure shows all of parameters. Click Apply/Save if correct or click *Back* to restart the configuration again.

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 IPoE 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

Option 66: ☒ Disable ☐ Enable

Option 67: ☒ Disable ☐ Enable

Option 43: ☒ Disable ☐ Enable

Option 128: ☒ Disable ☐ Enable

Option 121: ☒ Disable ☐ Enable

Option 132: ☒ Disable ☐ Enable

☐ Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Figure 23: WAN Connection, IP over Ethernet Configuration

To configure the IP over Ethernet settings:

- ▶ Select *Obtain an IP address automatically* or *User the following (fixed) IP address* and then also enter the *WAN IP address* and *WAN Subnet Mask*.
- ▶ Enter the *DHCP Vendor Class Identifier (option 60)*, *Option 61 IAID*, and *Option 61 DUID* if necessary
- ▶ Check to enable or disable the following *options*, 125/66/67/43/128/121/132
- ▶ 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 Firewall

IGMP Multicast

☐ Enable IGMP Multicast

[Back](#) [Next](#)

Figure 24: Network Address Translation Configuration

Global Settings:

- ▶ Check to *Enable NAT* if PCs in the LAN share the same WAN port IP address to surf Internet
- ▶ Check to *Enable Firewall* if you need the device to do the first firewall protection
- ▶ Check to *Enable IGMP Multicast*
- ▶ Click *Next*

Then keep configuring the Default routing (Gateway) and DNS server configuration pages as described in the PPPoE section. After these, the *WAN Setup Summary* page shows all of parameters. Click *Apply/Save* if correct or click *Back* to restart the configuration again.

Bridging

WAN Setup - Summary

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

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Multicast VLAN Filter:	
Quality Of Service:	Disabled

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

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

Figure 25: WAN Bridge Setup Summary

The *WAN Setup Summary* page shows all of parameters. Click *Apply/Save* if correct or click *Back* to restart the configuration again.

LAN

Local Area Network (LAN) Setup

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

IP Address:

Subnet Mask:

☒ Enable IGMP Snooping

☒ 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

Figure 26: LAN Configuration

Global Settings:

- ▶ Select the Group Name 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 the LAN site 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.
- ▶ Besides the dynamic assignment of IP address, you can configure the static IP address too which will be reserved for the device with specified MAC address only. Click *Add Entries* to enter MAC address of the device and fixed IP address. You could check the entry and click *Remove Entries* to remove it.
- ▶ Check to enable and configure the *second IP address and subnet mask for LAN*

interface if there are two separated networks in the LAN sharing the device to surf Internet. Then enter the *second IP address* and *subnet mask*.

- ▶ Click *Apply/Save* to save setting or *Save/Reboot* to save and then reboot the device

IPv6 Autoconfig

IPv6 is supported in this device. Below page allows to configure the LAN site of device with IPv6 settings.

IPv6 LAN Auto Configuration
Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::".
information. For example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration
Interface Address (prefix length is required):

IPv6 LAN Applications

☒ Enable DHCPv6 Server

☒ Stateless

☐ Stateful

Start interface ID:

End interface ID:

Leased Time (hour):

☒ Enable RADVD

☒ Enable ULA Prefix Advertisement

Prefix:

Preferred Life Time (hour):

Valid Life Time (hour):

☐ Enable MLD Snooping

Figure 27: LAN IPv6 Auto Configuration

Global Settings:

- ▶ Enter the *IPv6 address*
- ▶ Check to enable/disable *IPv6 DHCP server*. If enable IPv6 DHCP server, choose "stateless" or "stateful" with *start interface ID*, *end interface ID* and *leased time*.
- ▶ Check to enable *RADVD* with *Prefix*, *Preferred Lift Time*, and *Valid Life Time* if enable ULA Prefix Advertisement.
- ▶ Check to enable *MLD snooping* with *standard mode* or *blocking mode*
- ▶ Click *Save/Apply* to save the settings.

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 28: 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
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		

Figure 29: Add A Rule Of Virtual Server

Global Setting

- ▶ Select *Use Interface* from the list
- ▶ Select a *service name* 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
- ▶ Click *Apply/Save* to save configuration
- ▶ 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 *Apply/Save*

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.

NAT -- Port Triggering Setup

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

Add
Remove

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

Figure 30: Port Triggering Setup

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

Use Interface: ipoe_eth4/eth4.1

Application Name: Select One

☒ Select an application: Select One

☐ Custom application:

Save/Apply

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Save/Apply

Figure 31: Add a Rule Of Port Triggering

Global Setting

- ▶ Select *Use Interface* from the list
- ▶ Select a *Application Name* from the predefined list or enter the name of *Custom Application*
- ▶ 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 port # to secure the service.
- ▶ Select the *Open Protocol*
- ▶ Click *Save/Apply*

DMZ Host

A DMZ (DeMilitarized Zone) host is a computer on your network that can be accessed from the Internet. The de-militarised 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 Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

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

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

DMZ Host IP Address:

Save/Apply

Figure 32: DNS Host Configuration

Global Setting

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

Security

The Security feature provides two more setting pages including IP filtering in Routed mode 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	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<div>Add Remove</div>							

Figure 33: Outgoing IP Filter Settings

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

Filter Name:	<input type="text"/>
IP Version:	<input type="text" value="IPv4"/>
Protocol:	<input type="text"/>
Source IP address[/prefix length]:	<input type="text"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address[/prefix length]:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>
<div>Apply/Save</div>	

Figure 34: Add - Outgoing IP Filter Configuration

Global Setting

- ▶ Enter the *Filter Name*
- ▶ Select the *IP version*, IPv4 or IPv6
- ▶ 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 *Apply/Save*

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

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

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<div> Add Remove </div>								

Figure 35: Incoming IP Filter Status

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

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

Add IP Filter -- Incoming

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

Filter Name:

IP Version:

Protocol:

Source IP address/prefix length:

Source Port (port or port:port):

Destination IP address/prefix length:

Destination Port (port or port:port):

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

☒ Select All

☒ ipoe_eth4/eth4.1

☒ br0/br0

Apply/Save

Figure 36: Incoming IP Filter Configuration

Global Setting

- ▶ Enter the *Filter Name*
- ▶ Select the IP version, IPv4 or IPv6
- ▶ 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 *Apply/Save*

Parental Control

This feature allows you to configure some of PCs in LAN to surf Internet in specific time period. The URL filter feature also allows you to build up a list of URLs up to 100 entries. You could set to exclude those URLs which mean PCs can not access those URLs which packets to those URLs will be discarded by the device automatically. Or you could set to include those URLs which mean PCs can only access those URLs.

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

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<div>Add Remove</div>											

Figure 37: Parental Control Configuration

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

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

Access Time Restriction

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

User Name	<input type="text"/>														
<input checked="" type="radio"/> Browser's MAC Address	<input type="text"/>														
<input type="radio"/> Other MAC Address	<input type="text"/>														
(xx:xx:xx:xx:xx:xx)															
Days of the week	<table><tr><td>Mon</td><td>Tue</td><td>Wed</td><td>Thu</td><td>Fri</td><td>Sat</td><td>Sun</td></tr><tr><td>Click to select</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td></tr></table>	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"/>
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"/>									
Start Blocking Time (hh:mm)	<input type="text"/>														
End Blocking Time (hh:mm)	<input type="text"/>														

Apply/Save

Figure 33: 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 Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ☒ Exclude ☐ Include

Address	Port	Remove
		<input type="button" value="Add"/> <input type="button" value="Remove"/>

Figure 38: URL Filter

The URL filter feature also allows you to build up a list of URLs up to 100 entries. You could set to exclude those URLs which mean PCs can not access those URLs which packets to those URLs will be discarded by the device automatically. Or you could set to include those URLs which mean PCs can only access those URLs.

Global Setting:

- ▶ Check the URL List Type, *Exclude* or *Include*.
- ▶ Click *Add* to add entries as below.

Parental Control -- URL Filter Add

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

URL Address:

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

Figure 39: URL Filter Configuration

Global Setting

- ▶ Enter the *URL Address*
- ▶ Enter the *Port Number*, the default port number is 80 which is a WEB application.
- ▶ Click *Apply/Save*

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.

QoS -- Queue Management Configuration

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

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

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

☒ Enable QoS

Select Default DSCP Mark: No Change(-1)

Apply/Save

Figure 40: 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 *Apply/Save*

QoS Queue

QoS Queue Setup

In ATM mode, maximum 8 queues can be configured.

For each Ethernet interface, maximum 4 queues can be configured.

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

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

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

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

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

Name	Key	Interface	Scheduler Alg	Precedence	DSL Latency	Enable	Remove
------	-----	-----------	---------------	------------	-------------	--------	--------

Add **Enable** **Remove**

Figure 41: Quality of Service Queue Setup

Click *Add* to add a QoS queue. The Enable button will scan through the every rule in the table. Rule with Enable-checkbox checked will be enabled.

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

QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.
Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others
 Click 'Apply/Save' to save and activate the queue.

Name:

Enable:

Interface:

Figure 42: Add a QoS Queue

Global Setting

- ▶ Enter the *Name* of QoS Queue
- ▶ Set *Enable* or *Disable* the QoS Queue
- ▶ Select the LAN or WAN *Interface* and select the *Precedence* (1 to 4)
- ▶ Click *Apply/Save* to add this QoS queue

QoS Classification

You need to define one or more *classes* of data traffic and set the priority for each of classes.

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

To add a rule, click the **Add** button.
 To remove rules, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

CLASSIFICATION CRITERIA														CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Limit (kbps)	Enable	Remove	
<div style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/> </div>																				

Figure 43: Quality of Service Classification Setup

Click *Add* to add a class of Quality of Service. The Enable button will scan through the every rule in the table. Rule with Enable-checkbox checked will be enabled.

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

Add Network Traffic Class Rule

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

Traffic Class Name:	<input type="text"/>
Rule Order:	Last ▾
Rule Status:	Disable ▾
Specify Classification Criteria	
A blank criterion indicates it is not used for classification.	
Class Interface:	LAN ▾
Ether Type:	<input type="text"/>
Source MAC Address:	<input type="text"/>
Source MAC Mask:	<input type="text"/>
Destination MAC Address:	<input type="text"/>
Destination MAC Mask:	<input type="text"/>
Specify Classification Results	
Note- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to a queue at the interface, whose priority is equal to or lower than the class queue.	
A blank mark or tag value means no change.	
Specify Class Queue (Required):	<input type="text"/>
Mark Differentiated Service Code Point (DSCP):	<input type="text"/>
Mark 802.1p priority:	<input type="text"/>
Tag VLAN ID [0-4094]:	<input type="text"/>
Set Rate Limit(kbps):	<input type="text"/>
<input type="button" value="Apply/Save"/>	

Figure 44: Add a QoS Classification

The screen creates a traffic class rule to classify the upstream 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 'Apply/Save' to save and activate the rule.

Global Setting

- ▶ Enter the *Traffic Class Name*
- ▶ Select the *Rule Order* and *Rule Status* from the list
- ▶ Select the *Class Interface* from the list
- ▶ Select the *Ether Type* from the list
- ▶ Enter the *Source MAC Address*, *Source MAC Mask*, *Destination MAC Address* and *Destination MAC Mask*
- ▶ Select the *Specify Class Queue* from the list
- ▶ Select *Differentiated Service Code Point (DSCP) Mark* from the list. If the field is not empty, the corresponding DSCP byte in the IP header of packet will be overwritten by the selected value.
- ▶ Select the *802.1p Priority* from the list
- ▶ Set the *Tag VLAN ID (0-4094)*

- ▶ Set *Rate Limit (Kbps)*
- ▶ Click *Apply/save* 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 four more setting pages including Default Gateway, Static Route, Policy Routing and RIP. Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Default Gateway

Routing -- Default Gateway

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

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
eth4.1	

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

Selected WAN Interface: NO CONFIGURED INTERFACE ▼

Apply/Save

Figure 45: Default Gateway Configuration

Global Setting

- ▶ Select WAN interfaces in the *Available Routed WAN Interfaces* and move them into *Selected Default Gateway Interfaces*.
- ▶ Set *Selected WAN Interface* from the list
- ▶ Click *Apply/Save* to save the configuration

Static Route

You could create your own routing entry by the destination network address and interface to configure the data traffic in the network. Click Add to add entry.

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

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
<div>Add Remove</div>					

Figure 46: Static Route Configuration

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.

IP Version:

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

Figure 47: Add a Static Route

Global Setting

- ▶ Select the *IP Version* (IPv4 or IPv6)
- ▶ Enter the *Destination Network Address* and *prefix length* (range)
- ▶ Select the *Interface* from the list
- ▶ Enter the *Gateway IP Address* where packet will be forwarded to.
- ▶ Enter the number of *Metric*
- ▶ Click *Apply/Save* to save the configuration

Policy Routing

You could create your own routing entry by the LAN interface or source IP address and WAN interface to configure the data traffic in the network. Click Add to add entry.

Policy Routing Setting -- A maximum 8 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
<div>Add Remove</div>					

Figure 48: Policy Route Configuration

Policy Routing Setup

Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.

Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

Use Interface:

Default Gateway IP:

Apply/Save

Figure 49: Add a Policy Route

Global Setting

- ▶ Enter the *Policy Name* of this configuration
- ▶ Select the *physical LAN interface (port)* from the list
- ▶ Enter the *Source IP Address*
- ▶ Select the *Use Interface* from the list
- ▶ Enter the *Gateway IP Address* where packet will be forwarded to.
- ▶ Click *Apply/Save* to save the configuration

RIP

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to start/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
eth4.2	2	Passive	<input type="checkbox"/>

Apply/Save

Figure 50: RIP Configuration

Global Setting

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

DNS

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

DNS Server

DNS Server Configuration

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

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

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

Available WAN Interfaces

Selected DNS Server Interfaces	Available WAN Interfaces
eth4.1	

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

TODO: IPV6 ***** Select the configured WAN interface for IPV6 DNS server information OR enter the static IPV6 DNS server Addresses.
Note that selecting a WAN interface for IPV6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPV6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPV6 DNS address:

Primary IPV6 DNS server:

Secondary IPV6 DNS server:

Figure 51: DNS Configuration

Global Setting

- ▶ Check *Select DNS Server Interface from available WAN interfaces* or *Use the following Static DNS IP Address*.
- ▶ If set the DNS server interface from available WAN interface, select the available WAN interface and move them to the selected DNS interfaces table.
- ▶ If set to use the static DNS server, enter the IP addresses of *primary DNS server*

and/or *secondary DNS server*.

- ▶ If there is IPv6 WAN interface, the DNS server interface can be obtained from the selected WAN interface via checking *Obtain IPv6 DNS info from a WAN interface* or by enter static IP address of *Primary IPv6 DNS server* and/or *Secondary IPv6 DNS server*.
- ▶ Click *Apply/Save* 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
<div><div>Add</div><div>Remove</div></div>				

Figure 52: Dynamic DNS Configuration

Click *Add* to add Dynamic DNS setting.

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

Add Dynamic DNS

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

D-DNS provider	<div>DynDNS.org ▾</div>
Hostname	<div></div>
Interface	<div>ipoe_eth4.1 ▾</div>
DynDNS Settings	
Username	<div></div>
Password	<div></div>

Apply/Save

Figure 53: Add a 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 *Apply/Save* to save the configuration

Print Server

The Print Server feature provides you to setup a network printer in your LAN environment.

Print Server settings

This page allows you to enable / disable printer support.

☒ Enable on-board print server.

Printer name

Make and model

Apply/Save

Figure 54: Print Server Configuration

Global Setting

- ▶ Check *Enable On-Board Print Server* checkbox
- ▶ Enter the *Printer Name* which you like others to see it while searching network printer.
- ▶ Enter the *maker* and *model* name..
- ▶ Click *Apply/Save* to save the configuration

DLNA

The DLNA feature provides you to setup a digital media server to store the picture, video and so on for sharing in your LAN environment.

Digital Media Server settings

This page allows you to enable / disable digital media server support.

☒ Enable on-board digital media server.

Interface Default ▾

Media Library Path

Apply/Save

Figure 55: DLNA Configuration

Global Setting

- ▶ Check *Enable On-Board digital media server* checkbox

- ▶ Select the *Interface* from the list
- ▶ Set the *Media Library Path* where stores the files
- ▶ Click *Apply/Save* to save the configuration

Storage Service

The Storage Service feature allows you to use USB storage device as a sharing storage device.

Storage Device Info

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volumename	FileSystem	Total Space	Used Space
------------	------------	-------------	------------

Figure 56: Storage Device Information

User Accounts

Storage UserAccount Configuration

Choose Add, or Remove to configure User Accounts.

Username	HomeDir	Remove
----------	---------	--------

Figure 57: User Accounts Configuration

Storage User Account Setup

In the boxes below, enter the user name, password and volume name on which the home directory is to be created.

Username:
 Password:
 Confirm Password:
 volumeName:

Figure 58: Add a Storage User Account

Global Setting

- ▶ Enter the *Username* and *Password* who is allowed to access the storage device

- ▶ Enter the password again in the *Confirm Password* field
- ▶ Enter the *Volumename*
- ▶ Click *Apply/Save* to save the configuration

Interface Grouping

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

Interface Grouping -- A maximum 16 entries can be configured

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

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		eth4.1	LAN1	
		eth4.2	LAN2	
			LAN3	
			LAN4	
			wlan0	

Figure 59: Interface Grouping Configuration

Click *Add* to add a Group.

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

Interface grouping Configuration

To create a new interface group:

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

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

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces	Available LAN Interfaces
<div style="border: 1px solid black; height: 100px; width: 100%;"></div>	<div style="border: 1px solid black; padding: 5px;">LAN1 LAN2 LAN3 LAN4 wan0</div>

<-> <->

Automatically Add Clients With the following DHCP Vendor IDs

Figure 60: Add a Group Configuration

Global Setting

- ▶ Enter the *Group Name*
- ▶ Select the *WAN Interface used in this group* from the list
- ▶ 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.
- ▶ Enter DHCP vendor IDs if necessary
- ▶ Click *Apply/Save* to save the configuration.

IP Tunnel

The IP Tunnel feature allows you to create two tunnels, IPv6 in IPv4 tunnel or IPv4 in IPv6 tunnel.

IPv6 in IPv4 Tunnel

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
<div>Add Remove</div>							

Figure 61: IPv6 in IPv4 Tunnel Information

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

☒ Manual ☐ Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

Figure 62: IPv6 in IPv4 Tunnel Configuration

Global Setting

- ▶ Enter the *Tunnel Name*
- ▶ Select the *Mechanism* from the list
- ▶ Select the *Associated WAN Interface* from the list
- ▶ Select the *Associated LAN interface* from the list
- ▶ Check *Manual* or *Automatic*
- ▶ Set the *IPv4 Mask Length*, *6rd Prefix with Prefix Length*
- ▶ Set the *Border Relay IPv4 Address*
- ▶ Click *Apply/Save* to save the configuration.

IPv4 in IPv6 Tunnel

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	Remote IPv6 Address	Remove
<div>Add Remove</div>					

Figure 63: IPv4 in IPv6 Tunnel Information

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name:

Mechanism: DS-Lite ▼

Associated WAN Interface: ▼

Associated LAN Interface: LAN/br0 ▼

☒ Manual ☐ Automatic

Remote IPv6 Address:

Apply/Save

Figure 64: IPv4 in IPv6 Tunnel Configuration

Global Setting

- ▶ Enter the *Tunnel Name*
- ▶ Select the *Mechanism* from the list
- ▶ Select the *Associated WAN Interface* from the list
- ▶ Select the *Associated LAN interface* from the list
- ▶ Check *Manual* or *Automatic*
- ▶ Set the *Remote IPv6 Address*
- ▶ Click *Apply/Save* to save the configuration.

IPSec

The IPSec feature allows you to create IPSec VPN tunnel with remote site.

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
<div> Add New Connection Remove </div>				

Figure 65: IPSec Tunnel Connection Information

IPSec Settings

IPSec Connection Name

Tunnel Mode

Remote IPSec Gateway Address (IPv4 address in dotted decimal)

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 66: IPSec Tunnel Configuration

Global Setting

- ▶ Enter the *IPSec Connection Name*
- ▶ Select the *Tunnel Mode*
- ▶ Enter the *Remote IPSec Gateway Address*
- ▶ Select the *Tunnel Access from Local IP Address* from the list (subnet or single address) and enter the *IP address for VPN* and *Subnetmask*
- ▶ Select the *Tunnel Access from Remote IP Address* from the list (subnet or single address) and enter the *IP address for VPN* and *Subnetmask*
- ▶ Select the *Key Exchange Method* from the list
- ▶ Select the *Authentication Method* from the list
- ▶ Enter the *Pre-Shared Key*
- ▶ Click *Show Advanced Setting* button if necessary
- ▶ Click *Apply/Save* to save the configuration

The image shows a web-based configuration interface for Advanced IKE Settings. It is divided into two sections: Phase 1 and Phase 2. Each section contains dropdown menus for Mode, Encryption Algorithm, Integrity Algorithm, and Select Diffie-Hellman Group for Key Exchange, along with a text input for Key Life Time. A 'Hide Advanced Settings' button is located at the top right.

Section	Mode	Encryption Algorithm	Integrity Algorithm	Select Diffie-Hellman Group for Key Exchange	Key Life Time
Phase 1	Main	3DES	MD5	1024bit	3600
Phase 2		3DES	MD5	1024bit	3600

Figure 67: Advanced IPSec Tunnel Configuration

There are two phases, phase 1 and phase 2 in the Advanced IKE settings.

Global Setting

- ▶ Select *Mode* of phase 1 from the list
- ▶ Select *Encryption Algorithm* of phase 1 from the list
- ▶ Select *Integrity Algorithm* of phase 1 from the list
- ▶ Select *Diffle-Hellman Group for Key Exchange* of phase 1 from the list
- ▶ Enter the *Key Life Time* of phase 1
- ▶ Select *Encryption Algorithm* of phase 2
- ▶ Select *Integrity Algorithm* of phase 2 from the list
- ▶ Select *Diffle-Hellman Group for Key Exchange* of phase 2 from the list
- ▶ Enter the *Key Life Time* of phase 2
- ▶ Click *Apply/Save* to save the configuration

Certificate

The Certificate feature allows you to verify the identity. .

Local

The image shows a web-based interface for managing local certificates. It includes a title 'Local Certificates', a descriptive text, and a table with columns: Name, In Use, Subject, Type, and Action. Below the table are two buttons: 'Create Certificate Request' and 'Import Certificate'.

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
------	--------	---------	------	--------

Create Certificate Request Import Certificate

Figure 68: Local Certificate

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 69: Create Certificate Request Configuration

Global Setting

- ▶ Enter the *Certificate Name*
- ▶ Enter the *Common Name*
- ▶ Enter the *Organization Name*
- ▶ Enter the *State/Province Name*
- ▶ Select *Country/Region Name* from the list
- ▶ Click *Apply* to save the configuration.

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 Configuration

Global Setting

- ▶ Enter the *Certificate Name*
- ▶ Enter the *Certificate*
- ▶ Enter the *Private Key*
- ▶ Click *Apply* to save the configuration.

Trusted CA

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 Information

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

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

Figure 72: Import Trusted CA Configuration

Global Setting

- ▶ Enter the *Certificate Name*
- ▶ Enter the *Certificate*
- ▶ Click *Apply* to save the configuration.

Power Management

The Power management feature provides you the control of hardware modules to evaluate power consumption.

Power Management

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

MIPS CPU Clock divider when Idle

☒ Enable Status: Enabled

Wait instruction when Idle

☒ Enable Status: Enabled

DRAM Self Refresh

☒ Enable Status: Enabled

Ethernet Auto Power Down Number of ethernet interfaces in:

☒ Enable Status: Enabled Full power mode: 1
Low power mode: 4

Apply refresh

Figure 73: Power Management Configuration

Global Setting

- ▶ Check to enable *MIPS CPU Clock divider when Idle*
- ▶ Check to enable *Wait instruction when Idle*
- ▶ Check to enable *DRAM Self Reflash*
- ▶ Check to enable *Ethernet Auto Power Down*
- ▶ Click *Apply/Save* to save the configuration
- ▶ Click *Reflash* to update the status

Multicast

The Multicast feature provides you to configure detailed parameters of IGMP protocol.

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	3
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:	<input type="checkbox"/>

Figure 74: Multicast IGMP Configuration

Global Setting

- ▶ Enter the *Default Version*
- ▶ Enter the *Query Interval*
- ▶ Enter the *Query Response Interval*
- ▶ Enter the *Last Member Query Interval*
- ▶ Enter the *Robustness Value*
- ▶ Enter the *Maximum Multicast Groups*
- ▶ Enter the *Maximum Multicast Data Source*
- ▶ Enter the *Maximum Multicast Group Member*
- ▶ Check to enable *Fast Leave Enable*
- ▶ Check to enable *LAN to LAN (Intra LAN) Multicast Enable*
- ▶ Click *Apply/Save* to save the configuration

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, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

☒ Enable Wireless

☐ 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"/>	16	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A

Figure 75: 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 enable *Clients Isolation* that wireless clients can not share information

to each other.

- ▶ Check to disable WMM Advertise where WMM stands for WiFi Multimedia. This technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are handled in lower priority.
- ▶ Check to enable the Wireless Multicast Forwarding (WMF)
- ▶ Enter the *wireless network name (SSID)*
- ▶ The *BSSID* is the MAC address of device
- ▶ Select the *Country* from the list
- ▶ Enter the *Maximum Wireless Client Number* allowed to associate with the device
- ▶ Check to enable *Wireless Guest Network* to create a virtual wireless AP. There are three more guests available for configuration.
- ▶ Click *Apply/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.

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)

WPS Setup

Enable WPS

Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
☐ Push-Button ☐ Enter STA PIN ☐ Use AP PIN

Set WPS AP Mode

Setup AP (Configure all security settings with an external registrar)

Device PIN [Help](#)

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

Figure 76: Wireless Setting – Security

Global Setting

- ▶ 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:	Open
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

- ▶ 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

- ▶ 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

- ▶ 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:	<input type="text"/> Click here to display
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP
WEP Encryption:	Disabled

Save/Apply

- ▶ 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:	WPA2
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	AES
WEP Encryption:	Disabled

Save/Apply

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

- ▶ 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:	Mixed WPA2/WPA	
WPA2 Preauthentication:	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:	TKIP+AES	
WEP Encryption:	Disabled	

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

- ▶ Click *Save/Apply* to save the configuration.

MAC Filter



Wireless -- MAC Filter

Select SSID: Intero_68

MAC Restrict Mode: ☒ Disabled ☐ Allow ☐ Deny

MAC Address	Remove
-------------	--------

Figure 77: Wireless Setting – Input MAC Address



Wireless -- MAC Filter

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

MAC Address:

Figure 78: Wireless Setting – Define the action plan for those MAC address

Global Setting

- ▶ 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) or Deny (only those PCs with MAC addresses in the table can not surf Internet).
- ▶ Click Add to add more wireless MAC address or click Remove to remove the specified entry.
- ▶ Enter the *MAC Address* of wireless client
- ▶ Click *Apply/Save* to save the configuration.

Wireless Bridge

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

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.

Click "Apply/Save" to configure the wireless bridge options.

AP Mode:	<input type="text" value="Access Point"/>
Bridge Restrict:	<input type="text" value="Enabled"/>
Remote Bridges MAC Address:	<input type="text"/> <input type="text"/>

Figure 79: 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 Bridge Restrict* determine where it can communicate with all other wireless bridges and also wireless clients (set *Bridge Restrict* is Disabled) or just the specified MAC addresses of below wireless bridge devices (set *Bridge Restrict* is Enable).
- ▶ Click *Reflash* to get the updated information
- ▶ Click *Apply/Save* to save the configuration

Advanced

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

Band:	2.4GHz	
Channel:	1	Current: 1 (interference: acceptable)
Auto Channel Timer(min):	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz in 2.4G Band and 40MHz in 5G Band	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Off	
OBSS Co-Existence:	Enable	
RX Chain Power Save:	Disable	Power Save status: Full Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Apply/Save

Figure 80: 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
- ▶ Set the *Wireless Communication Rate*, AUTO means to use the highest rate if possible
- ▶ Set the *Wireless Bandwidth*
- ▶ Set the *Control Sideband*
- ▶ Set the *802.11n Rate and Protection*
- ▶ Set the *support the 802.11n client only*
- ▶ Set the *RIFS Advertisement*
- ▶ Set the *OBSS Co-Existence*
- ▶ Set *RX Chain Power Save*, *RX Chain Power Save Quiet Time*, *RX Chain Power Save PPS*
- ▶ Set *54G Rate*
- ▶ 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 Global *Maximum Client*
- ▶ Set *XPress Technology* enabled or disabled.
- ▶ Set *Transmission Power*. Larger value means more coverage.
- ▶ Set *WMM (Wireless Multimedia)*
- ▶ Set *WMM No Acknowledgement*. Enabling no-acknowledge can result in more efficient throughput but high error rates
- ▶ Set *WMM APSD (Automatic Power Save Delivery)*
- ▶ Click *Apply/Save* to save the configuration

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 81: Wireless Setting – Station Information

Global Setting

- ▶ Click *Refresh* to get the latest updated information

8 Voice Setup

The Voice Setup web page menu comprises:

Interface Setup

SIP Basic Setting

SIP Advanced Setting

Interface Setup

This page allows you to specify the voice packets to pass through the specific interface and to choose different country code to pre-set voice related parameters including ringing type, ringing frequency, tone type, tone frequency, cadence, etc..



Global parameters

Global parameters

Bound Interface Name: Any_WAN ▼

Locale selection: SWE-SWEDEN ▼

SIP listen port: 5060

Start SIP client

Stop SIP client

Figure 82: Voice Configuration – Interface Setup

Global Setting:

- ▶ Select *Interface Name* that voice packet go through
- ▶ Select *Location* where you are located
- ▶ Set the *SIP Listen Port*
- ▶ Click button to *Start SIP client* or *Stop SIP client*

SIP Basic Setting

This page allows you to setup the SIP protocols (parameters).

Service Provider 0

Voice -- SIP configuration

Enter the SIP parameters and click Apply to save the parameters and restart the voice application.

SIP domain name:

Voip Dialplan Setting:

☒ Use SIP Proxy.

SIP Proxy:

SIP Proxy port:

☒ Use SIP Outbound Proxy.

SIP Outbound Proxy:

SIP Outbound Proxy port:

☒ Use SIP Registrar.

SIP Registrar:

SIP Registrar port:

SIP Account	0	1
Account Enabled	<input type="checkbox"/>	<input type="checkbox"/>
Physical Endpt Id	<input type="text" value="0"/>	<input type="text" value="1"/>
Extension	<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.711MuLaw"/>	<input type="text" value="G.711MuLaw"/>
Preferred codec 2	<input type="text" value="G.711ALaw"/>	<input type="text" value="G.711ALaw"/>
Preferred codec 3	<input type="text" value="G.729a"/>	<input type="text" value="G.729a"/>
Preferred codec 4	<input type="text" value="G.723.1"/>	<input type="text" value="G.723.1"/>
Preferred codec 5	<input type="text" value="G.726_24"/>	<input type="text" value="G.726_24"/>
Preferred codec 6	<input type="text" value="G.726_32"/>	<input type="text" value="G.726_32"/>

Apply

Figure 83: Voice Basic SIP Protocol Configuration

Global Setting:

- ▶ Enter the *SIP domain name*
- ▶ Enter the *VoIP dial plan*
- ▶ Check to *Use SIP Proxy* if necessary and then enter address of *SIP Proxy* and *SIP Proxy Port number*
- ▶ Check to *Use SIP Outbound Proxy* if necessary and then enter address of *SIP Outbound Proxy* and *SIP Outbound Proxy Port number*

- ▶ Check to *Use SIP Registrar* if necessary and then enter address of *SIP Registrar* and *SIP Registrar Port number*
- ▶ There are two SIP accounts can be configured with following parameters, Account Enabled, Physical Endpt Id, Extension, Authentication name, Password, Preferred ptime, Preferred codec 1 to 6.
- ▶ Click *Apply* to save the configuration.

SIP Advanced Setting

This page allows you to setup the advanced parameters of the SIP protocols.

Service Provider 0

Voice -- SIP Advanced configuration

Enter the SIP parameters and click Apply to save the parameters and restart the voice application.

Call Features

Line	1	2
Call waiting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Call forwarding number	<input type="text"/>	<input type="text"/>
Forward unconditionally	<input checked="" type="checkbox"/>	<input checked="" 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"/>
Three-way conference	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Anonymous calling (CLIR)	<input type="checkbox"/>	<input type="checkbox"/>

Feature Access Codes

CFWD Unconditional Activation	: *21* [number]#	CFWD Unconditional Deactivation	: #21#
CFWD No Answer Activation	: *61* [number]#	CFWD No Answer Deactivation	: #61#
CFWD On Busy Activation	: *67* [number]#	CFWD On Busy Deactivation	: #67#
Call Waiting Activation	: *43#	Call Waiting Deactivation	: #43#
Internal Call	: ###	Call Return	: *69#
CCBS Cancel	: #37#	Unattended Call Transfer	: *90*
CLIR Next Call	: *31#	CLIP Next Call	:
Permanent CLIR	:	Permanent CLIP	:

SIP

CLIR Method ☒ Anonymous URI ☐ Use Privacy Header

Registration Expire Timeout:

DSCP for SIP:

Hook Flash Relay setting:

SIP Transport protocol:

RTP/Codec

☐ Enable T38 support

☐ Enable V18 support

RTP Base Port:

DSCP for RTP:

Dtmf Relay setting:

Line	1	2
VAD support	<input type="checkbox"/>	<input type="checkbox"/>
Ingress gain	<input type="text" value="0"/>	<input type="text" value="0"/>
Egress gain	<input type="text" value="0"/>	<input type="text" value="0"/>

Apply

Figure 84: Voice Advanced SIP Protocol Configuration

Global Setting:

- ▶ There are two SIP accounts with call features separately. Check to enable those call features, Call waiting, Call forwarding number, Forward unconditionally, Forward on “busy”, Forward on “no answer”, Message waiting indication (MWI), Three-way conference, and Anonymous calling (CLIR).
- ▶ Set the Feature Access Codes for CFWD unconditional activation, CFWS unconditional deactivation, CFWD no answer activation, CFWD on busy activation, CFWD on busy deactivation, Call waiting activation, Call waiting deactivation, Internal call, Call return, CCBS cancel, unattended call transfer, CLIR next call, CLIP next call, permanent CLIR, and Permanent CLIP.
- ▶ Check to select CLIP Method, Anonymous URI or Use Privacy Header.
- ▶ Set Registration Expire Timeout
- ▶ Select the DSCP for SIP from the list
- ▶ Select the Hook Flash Relay Setting from the list
- ▶ Select the SIP Transport Protocol from the list
- ▶ Check to enable T.38 support and V18 support
- ▶ Enter the number of RTP Base Port
- ▶ Select the DSCP for RTP from the list
- ▶ Select the DTMF relay setting from the list
- ▶ Check and set the VAD support, Ingress gain and Egress gain for Tel1 and Tel2.
- ▶ Click *Apply* to save the configuration.

9 Diagnostic

Diagnostic

This page allows you to diagnostic the connections of LAN, Wireless and WAN ports.

Diagnostics

The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN1 Connection:	FAIL	Help
Test your LAN2 Connection:	PASS	Help
Test your LAN3 Connection:	FAIL	Help
Test your LAN4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Rerun Diagnostic Tests

Figure 85: Diagnostic

Click *Run Diagnostic* to run the test script and get the diagnostic result.

10 Management

The Management web page menu comprises:

Settings

System Log

Security Log

TR-069 Client

Internet Time

Access Control

Update Software

Reboot

Logout

Settings

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

Settings - Backup

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

Backup Settings

Figure 86: Backup Settings

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

Tools -- Update Settings

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

Settings File Name:

Update Settings

Figure 87: Restore Default Settings

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

Tools -- Restore Default Settings

Restore VoIP router settings to the factory defaults.

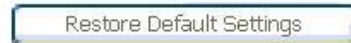


Figure 88: Restore Default Settings

To 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 89: 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 'Apply/Save' to configure the system log options.

Log: ☒ Disable ☐ Enable

Log Level:

Display Level:

Mode:



Figure 90: 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 *Apply/Save* to save the configuration.

Security Log

This page allows you to view security log.

Security Log

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

Click "View" to view the Security Log.

Click "Reset" to clear and reset the Security Log.

Right-click [here](#) to save Security Log to a file.

Figure 91: Management Configuration – Security Log

Global Setting

- ▶ Click *View* to view the security log
- ▶ Click *Reset* to clear and rest the security log

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 92: Management Configuration – TR-069 client

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*
- ▶ Select the *WAN interface used by TR-069 client* from the list
- ▶ Select to enable or disable *displaying SOAP messages on serial console*
- ▶ Check to select *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

First NTP time server:	Other	ntp1.sth.netnod.se
Second NTP time server:	Other	ntp1.gbg.netnod.se
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	

Time zone offset: (GMT+01:00) Amsterdam, Berlin, Bonn, Rome, Stockholm, Vienna

Apply/Save

Figure 93: Internet Time Configuration

Global Setting

- ▶ Check to *Automatically synchronize with Internet time servers*
- ▶ Select the *first, second, third, fourth, and fifth NTP time servers*. You could select the pre-defined time server from the list. Or select *Other* to enter your own name of NTP server
- ▶ Select the *Time zone offset* from the list
- ▶ Click *Save* to save your settings

Access Control

This submenu provides you local (LAN) or remote (WAN) access to the device. This may help the IT support staff to configure the router locally or remotely.

IP Address

Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Access Control Mode: ☒ Disable ☐ Enable

IP Address	Remove

Figure 94: Access Control: IP Address

Click to enable or disable Access Control by IP address.

Click *Add* to add IP address.

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

Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

Subnet Mask:

Figure 95: Add a Access Control: IP Address

Global Setting:

- ▶ Add the *IP Address* and *subnet mask* which is permitted to access the device and execute the management service.
- ▶ Click *Save/Apply* to save the settings.

Service

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
ICMP	Enable	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Save/Apply

Figure 96: Access Control: Service

Global Setting:

- ▶ Specify the method by which you wish to access the router locally or remotely by selecting it. The following are the methods available for local and remote access:
 - FTP
 - HTTP
 - ICMP (Ping)
 - SSH
 - TELNET
 - TFTP
- ▶ Click *Save/Apply* to save the configuration.

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 update the device software.

Access Control -- Passwords

Access to your broadband router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

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

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

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

Apply/Save

Figure 97: Access Control: Password

Global Setting:

- ▶ Enter the *Username*
- ▶ Enter the *Old Password*
- ▶ Enter the *New Password* and *Confirm Password*
- ▶ Click *Apply/Save* 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 98: 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 save current configuration and reboot to use the settings.

Click the button below to reboot the router.



Figure 99: Reboot

Global Setting

- ▶ Click *Reboot* to reboot the device

Logout

This page allows you to save current configuration and reboot to use the settings.

Click the button below to logout.



Figure 100: Logout

Global Setting

- ▶ Click *Logout* to leave the device's configuration page

Appendix A - Configuring the Internet Settings

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

Configuring Ethernet PCs

Assigning static Internet information to your PCs

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

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

You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).

You maintain different subnets on your LAN (subnets are described in Appendix B).

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

The IP address and subnet mask of each PC

The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the device. By default, the LAN port is assigned the IP address 192.168.1.1. (You can change this number or another number can be assigned by your ISP.)

The IP address of your ISP's Domain Name System (DNS) server.

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



Note

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

Configuring Wireless PCs

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

Positioning the wireless PCs

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

Wireless PC cards and drivers

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

Configuring PC access to your Wireless device

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

A Wireless access card for each of the PCs

Corresponding wireless access card driver software files

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

To configure Wireless PCs:

- Install the wireless access card.
- Install the wireless driver software files.
- Configure the following wireless parameters on each of the wireless PCs:
- Set the adapter to use infrastructure mode. This configures the PCs to access each other and the Internet via the device.
- Configure the SSID and channel to match the SSID and channel previously configured on the device.

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

Appendix B - Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the device, and provides instructions for using several IP utilities to diagnose problems.

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

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 cable provided with the device and that it is securely connected to the device and a wall socket/power strip.
<i>LINK LAN LED does not illuminate after Ethernet cable is attached.</i>	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the device. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.
Internet Access	
My PC cannot access the Internet	Run a health check on your device. Use the ping utility (discussed in the following section) to check whether your PC can communicate with the device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: <ul style="list-style-type: none"> ● Check that the gateway IP address on the computer is your public IP address (see Current Status on page 1 for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. ● Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.
<i>My LAN PCs cannot display web pages on the Internet.</i>	Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the device is correct, and then you can use the ping utility, discussed on page 79, to test connectivity with your ISP's DNS server.
Web pages	

Problem	Troubleshooting Suggestion
<i>I forgot/lost my user ID or password.</i>	If you have not changed the password from the default, try using "admin" as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing three times the Reset Default button on the front panel of the device. Then, type the default User ID and password shown above. WARNING: Resetting the device removes any custom settings and returns all settings to their default values.
<i>I cannot access the web pages from my browser.</i>	Use the ping utility, discussed in the following section, to check whether the PC can communicate with the device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the device.
<i>My changes to the web pages are not being retained.</i>	Be sure to use the <i>Confirm Changes</i> function after any changes.

Diagnosing Problem using IP Utilities

Ping

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

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

```
ping 192.168.1.1
```

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

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

```

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

```

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

Using the ping command, you can test whether the path to the device is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

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

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

Nslookup

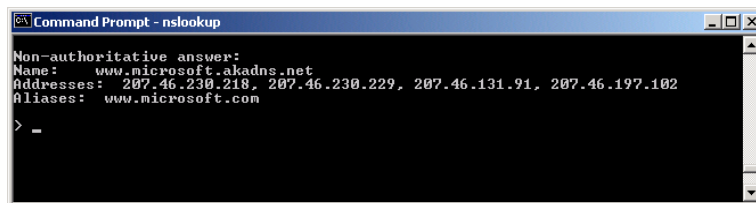
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

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

Nslookup

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

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



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

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

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

Appendix C - Specification

A1. Hardware Specifications

- LAN Interface
 - Four port 10/100BaseT Ethernet Switch (4 * RJ-45 connectors), IEEE 802.3u with MDI/MDIX auto-detection
 - Integrated 802.11b/g WLAN Access Point
- WAN Active Ethernet Optical Interface
 - SFF BiDi with 1310 nm TX.. 1490/1550 nm RX
- Analog Voice Interface
 - 2 FXS ports (2 * RJ-11 connectors) for analog phone sets
- Indicators
 - PWR – Green LED indicates power and operation. Red LED indicates failure.
 - WAN – Green LED indicates broadband connection
 - Internet – Green LED indicates PPP connection and RED indicates PPP failure or device in BRIDGE mode.
 - TEL1 – Green LED indicates phone connection
 - TEL2 – Green LED indicates phone connection
 - LAN – Green LED indicates LAN connection
 - WLAN – Green LED indicates wireless AP enabled
- OAM&P
 - Local: Telnet and Web management
 - Remote: Telnet Web Management
- Environment
 - Operation Temperature: 0°C ~ 45°C
 - Operation Humidity: 5% ~ 95%
 - Storage Temperature: -20 ~ +85°C
 - Storage Humidity: 5%~95%
- Power
 - AC Adapter: Input 110/220VAC, 50/60Hz; Output 12VDC 1.50A
- 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
 - ▶ DHCP client, server and relay agent
- Wireless LAN
 - ▶ Supports 802.1x; WEP; WEP2; WPA; WPA2; TKIP; AES; 802.11i
 - ▶ Hidden SSID
 - ▶ WMM for advanced Quality of Service
 - ▶ Multiple SSIDs

- Firewall
 - ▶ Support NAT and DMZ
 - ▶ Virtual server (port mapping) and IP filters
 - ▶ Protection against IP and MAC address spoofing
 - ▶ UPnP NAT traversal and VPN / IPSec pass-through
- Voice
 - ▶ Support voice CODECs like G.711, G.726, G.729A/B, BV16, ILBC, T.38 etc
 - ▶ DTMF tone detection / generation, fax / modem detection and pass-through
 - ▶ Adaptive jitter buffer, packet loss concealment (PLC), voice activity detection (VAD), comfort noise generation (CNG) and Caller ID
 - ▶ Support SIP (RFC3261)
 - ▶ Supports Call Waiting, Call Transfer, Call Forward and so on.
 - ▶ G.168 line echo cancellation with programmable tail
- VoIP and Telephone service
 - ▶ Supports SIP (RFC3261), SDP (RFC2327, RFC3264) as well as both TCP and UDP transport
 - ▶ Supports User Agent Client (UAC) - User Agent Server (UAS) call, or proxy call routing
 - ▶ Supports SIP and telephone URL addressing
 - ▶ Supports in-band DTMF tone sending / receiving and out-band DTMF signaling with RTP, as per RFC2833
 - ▶ Bonus services include:
 - Call Forwarding: Unconditional, No Response, On Busy
 - Call Waiting: Force Busy, Pickup and Release Old, Pickup and Put Old on Hold, Switch between two calls
 - Call Transfer, Call Back busy subscriber, Call Back last number called (call return)
 - Enquiry service
 - Three way conference
 - ▶ Provisioning through TFTP client with configuration profile
- Configuration and Network Management Features
 - ▶ 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
 - ▶ Embedded syslog; SNTP with DHCP options
 - ▶ 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 - Regulation

FCC Part 15 Notice

Warning: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 to the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is unlikely to cause harmful interference. But if it does, the user will be required to correct the interference at his or her own expense. The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless CTC Union expressly approves the changes or modifications.

FCC Part 15 Notice with Wireless

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/ TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Warning:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Part 68 Notice

This equipment complies with Part 68 of FCC Rules. On the base unit of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. IF REQUESTED, THIS INFORMATION MUST BE GIVEN TO THE TELEPHONE COMPANY.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to you line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in it is facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, Please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

NOTICE: The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or an electronic device to send any message via a telephone fax machine, unless such a message clearly contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission the following information:

- ✓ The date and time of transmission
- ✓ Identification of either business, business entity or individual sending message
- ✓ Telephone number of either the sending machine, business entity or individual

Warning: Users should not attempt to make such connections themselves, but should contact appropriate electric inspection authority, or electrician, as appropriate. Do not use any other power adapter except the one that accompanies the unit. Use of other adapter could result in damage to the unit. To prevent electronic shock, please do not open the cover.

UL Safety Regulations

- ✓ Disconnect TNV circuit connector or before removing cover or equivalent.
- ✓ Disconnect TNV circuit connector(s) before disconnecting power.
- ✓ Do not use this product near water for example, near a bathtub, washbowl, and kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- ✓ Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening.
- ✓ Do not use the telephone to report a gas leak in the vicinity of the leak.
- ✓ Use only the power cord batteries indicated in this manual. Do not dispose of batteries in a fire, as they may explode. Check with local codes for possible special disposal instructions.

No. 26 AWG Telephone Line Cord shall either be provided with the equipment or shall be described in the safety instruction. If fuse (F1) is not present, see the caution statement listed below:

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.



www.ctcu.com

T +886-2 2659-1021 F +886-2 2659-0237 E sales@ctcu.com



ISO 9001 Quality System Certified CTC Union Technologies Co.,LTD.

All trademarks are the property of their respective owners. Technical information in this document is subject to change without notice.