



# MTX-ROUTER-HELIOS II

## • HARDWARE • USER **GUIDE**



[www.mtxm2m.com](http://www.mtxm2m.com)

# Index

<b>COPYRIGHT &amp; TRADEMARKS .....</b>	<b>8</b>
<b>INTRODUCTION .....</b>	<b>9</b>
1. Hardware Installation .....	9
1.1 WARNING .....	9
1.2 System Requirements.....	10
1.3 Hardware Configuration.....	10
1.4 Led Indication.....	11
<b>GETTING STARTED.....</b>	<b>12</b>
1. Hardware Installation .....	12
1.1 Mount the Unit.....	12
1.2 Insert the SIM Card.....	12
1.3 Connecting Power .....	13
1.4 Connecting DI/DO Devices .....	13
1.5 Connecting Serial Devices.....	15
1.6 Connecting to the Network or a Host.....	15
2. Easy Setup by Configuring WEB UI .....	16
2.1 Network Status.....	16
2.2 WiFi Status.....	17
2.3 LAN Client List .....	18
2.4 Firewall Status.....	18
2.5 VPN Status.....	19
2.6 System Management Status.....	20
2.7 GNSS Status.....	21
<b>MAKING CONFIGURATIONS.....</b>	<b>22</b>
1. Basic Network .....	23
1.1 WAN Setup.....	23
1.1.1 Internet Setup .....	23
1.1.1.1 3G/4G WAN-3G/4G.....	24

1.1.2 Physical Interface .....	28
1.1.2.2 Ethernet WAN .....	30
1.1.2.2.1 Dynamic IP Address .....	30
1.1.2.2.2 Static IP Address .....	33
1.1.2.2.3 PPP over Ethernet .....	35
1.1.2.2.4 PPTP .....	37
1.1.2.2.5 L2TP .....	40
1.1.3 Load Balance .....	42
1.2 LAN Setup .....	45
1.2.1 Ethernet LAN .....	45
1.2.2 DHCP Server .....	45
1.2.2.1 DHCP Server List .....	45
1.2.2.2 DHCP Server Configuration .....	46
1.2.2.3 Fixed Mapping .....	48
1.2.3 VLAN .....	49
1.2.3.1 VLAN Scenarios .....	50
1.2.3.2 Port-Based VLAN .....	55
1.2.3.3 Tag-Based VLAN .....	57
1.3 WiFi Setup .....	58
1.3.1 WiFi Configuration .....	58
1.3.1.1 AP Router Mode .....	59
1.3.1.2 WDS Only Mode .....	63
1.3.1.3 WDS Hybrid Mode .....	65
1.3.1.4 WPS Setup .....	67
1.3.2 Wireless Client List .....	70
1.3.3 Advanced Configuration .....	70
1.3.4 Captive Portal .....	72
1.3.5 External Servers .....	72
1.3.5.1 External Server List .....	73
1.3.5.2 External Server Configuration .....	74

1.4 IPv6 Setup .....	75
1.4.1 6 to 4 .....	75
1.4.2 6 in 4 .....	76
1.5 NAT/DMZ .....	78
1.5.1 Configuration.....	78
1.5.2 DMZ .....	78
1.6 Routing Setup.....	79
1.6.1 Static Routing.....	80
1.6.2 Routing Information.....	81
2. Advanced Network.....	82
2.1 Firewall .....	82
2.1.1 Configuration.....	82
2.1.2 Packet Filters .....	82
2.1.2.1 Configuration .....	82
2.1.2.2 Packet Filter List.....	83
2.1.2.3 Packet Filter Rule Configuration.....	83
2.1.3 URL Blocking.....	85
2.1.3.1 Configuration .....	85
2.1.3.2 URL Blocking Rule List.....	86
2.1.3.3 URL Blocking Rule Configuration.....	86
2.1.4 Web Content Filters .....	87
2.1.4.1 Configuration .....	87
2.1.4.2 Web Content Filter Rule List .....	88
2.1.4.3 Web Content Filter Configuration .....	88
2.1.5 MAC Control .....	89
2.1.5.1 Configuration .....	89
2.1.5.2 MAC Control Rule List.....	89
2.1.5.3 MAC Control Rule Configuration .....	90
2.1.6 IPS.....	91
2.1.7 Options .....	91

2.2 QoS & BWM .....	92
2.2.1 Configuration.....	93
2.2.2 Rule-based QoS .....	94
2.2.2.1 Configuration .....	95
2.2.2.2 QoS Rule List .....	95
2.2.2.3 QoS Rule Configuration.....	96
2.3 VPN Setup.....	100
2.3.1 Configuration.....	101
2.3.2 IPsec .....	101
2.3.2.1 IPsec VPN Tunnel Scenarios .....	102
2.3.2.2 IPsec Configuration.....	103
2.3.2.3 Tunnel List & Status.....	104
2.3.2.4 Tunnel Configuration .....	105
2.3.2.5 Local & Remote Configuration .....	106
2.3.2.6 Authentication .....	107
2.3.2.7 IKE Phase .....	107
2.3.2.8 IKE Proposal Definition .....	108
2.3.2.9 IPsec Phase.....	109
2.3.2.10 IPsec Proposal Definition .....	109
2.3.2.11 Manual Proposal .....	110
2.3.3 PPTP .....	111
2.3.3.1 PPTP/L2TP VPN Tunnel Scenarios.....	111
2.3.3.2 PPTP Server Configuration.....	113
2.3.3.3 PPTP Server Status .....	114
2.3.3.4 User Account List .....	114
2.3.3.5 User Account Configuration .....	115
2.3.3.6 PPTP Client .....	115
2.3.3.7 PPTP Client List & Status.....	116
2.3.3.8 PPTP Client Configuration.....	116

2.3.4 L2TP .....	118
2.3.4.1 L2TP Server Configuration .....	119
2.3.4.2 L2TP Server Status .....	120
2.3.4.3 User Account List .....	120
2.3.4.4 User Account Configuration .....	121
2.3.4.5 L2TP Client .....	121
2.3.4.6 L2TP Client List & Status .....	121
2.3.4.7 L2TP Client Configuration .....	122
2.3.5 GRE .....	124
2.3.5.1 GRE VPN Tunnel Scenario .....	124
2.3.5.2 GRE Configuration .....	124
2.3.5.3 GRE Tunnel Definitions .....	125
2.3.5.4 GRE Rule Configuration .....	125
2.4 Redundancy .....	127
2.4.1 VRRP .....	127
2.5 System Management .....	128
2.5.1 TR-069 .....	128
2.5.2 SNMP .....	129
2.5.3 Telnet with CLI .....	131
2.5.4 UPnP .....	131
2.6 Certificate .....	131
2.6.1 My Certificates .....	132
2.6.1.1 Root CA .....	132
2.6.1.2 Local Certificate List .....	133
2.6.2 Trusted Certificates .....	134
2.6.2.1 Trusted CA Certificate List .....	134
2.6.2.2 Trusted Client Certificate List .....	134
2.6.3 Issue Certificates .....	135
2.7 Serial Port Settings .....	135
2.7.1 Port Configuration .....	135
2.7.2 Virtual COM .....	136
2.7.3 Modbus .....	142

3. SMS Remote Management.....	145
3.1 SMS Remote Management .....	145
3.1.1 SMS .....	145
3.1.4 Remote Management.....	148
3.2 IO Management.....	150
3.2.1 Configuration.....	150
4. Location Tracking.....	151
4.1 GNSS.....	152
4.1.1 Scenario of location tracking for fleet management.....	154
5. System.....	160
5.1 System Related.....	160
5.1.1 Change Password .....	160
5.1.2 System Tools .....	161
5.2 Scheduling.....	163
5.3 MMI .....	164
5.3.1 Web UI .....	164
<b>APPENDIX A: LICENSING INFORMATION.....</b>	<b>165</b>

# COPYRIGHT & TRADEMARKS

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.



# INTRODUCTION

Congratulations on your purchase of this outstanding product: Modbus Cellular Gateway. For M2M (Machine-to-Machine) applications, the MTX-Router-Helios II is absolutely the right choice. With built-in world-class 4G module, you just need to insert SIM card from local mobile carrier to get to Internet. The redundant SIM design provides a more reliable WAN connection for critical applications. By VPN tunneling technology, remote sites easily become a part of Intranet, and all data are transmitted in a secure (256-bit AES encryption) link..

This MTX-Router-Helios II is loaded with luxuriant security features including VPN, firewall, NAT, port forwarding, DHCP server and many other powerful features for complex and demanding business and M2M (Machine-to-Machine) applications. The redundancy design in fallback 9-48 VDC power terminal, dual SIM cards and VRRP function makes the device as a back-up in power, network connection and data transmission without lost.

Main Features:

- Provide various and configurable WAN connection
- Support dual SIMs for the redundant wireless WAN connection
- Provide Ethernet ports for comprehensive LAN connection and LAN-1 port can be configured to be another WAN interface
- Feature with VPN and NAT firewall to have powerful security
- Support the robust remote or local management to monitor network
- Designed by solid and easy-to-mount metal body for business and M2M environment to work with a variety M2M (Machine-to-Machine) applications

Before you install and use this product, please read this manual in detail for fully exploiting the functions of this product.

## ● 1. Hardware Installation

### 1.1 WARNING

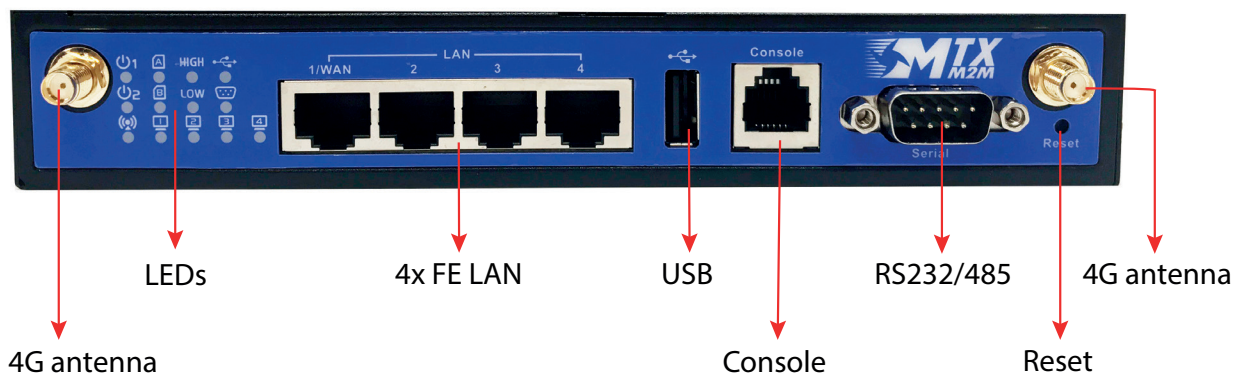
- Do not use the product in high humidity or high temperatures
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor is dangerous and may damage the product
- Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have it repaired at a qualified service center
- Place the product on a stable surface and avoid using this product and all accessories outdoors

## 1.2 System Requirements

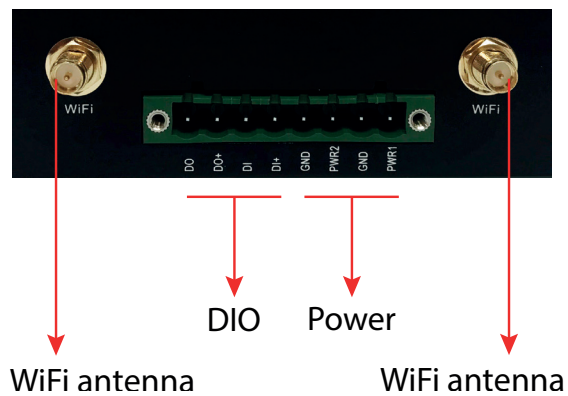
SYSTEM REQUIREMENTS	
Network requirements	<ul style="list-style-type: none"><li>• An Ethernet RJ45 cable or DSL modem</li><li>• 3G cellular service subscription</li><li>• IEEE 802.11n or 802.11b/g wireless clients</li><li>• 10/100 Ethernet adapter on PC</li></ul>
Web-based configuration utility requirements	<p>Computer with the following:</p> <ul style="list-style-type: none"><li>• Windows®, Macintosh, or Linux-based operating system</li><li>• An installed Ethernet adapter</li></ul> <p>Browser Requirements:</p> <ul style="list-style-type: none"><li>• Internet Explorer 6.0 or higher</li><li>• Chrome 2.0 or higher</li><li>• Firefox 3.0 or higher</li><li>• Safari 3.0 or higher</li></ul>
CD installation wizard requirements	<p>Computer with the following:</p> <ul style="list-style-type: none"><li>• Windows® 7, Vista®, or XP with Service Pack 2</li><li>• An installed Ethernet adapter</li><li>• CD-ROM drive</li></ul>

## 1.3 Hardware Configuration

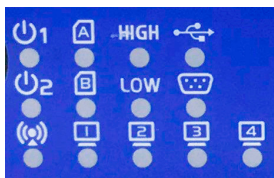
Front view:



Power input and DIO connector:



## 1.4 Led Indication



ICON	DESCRIPTION
Power source 1	Steady ON: device is powered on by power source 1
Power source 2	Steady ON: device is powered on by power source 2
WLAN (WiFi)	Steady ON: wireless radio is enabled Flash: data packets are transferred OFF: wireless radio is disabled
SIM A	Steady ON: SIM card A is chosen for connection
SIM B	Steady ON: SIM card B is chosen for connection
LAN 1/WAN - LAN 4	Steady ON: Ethernet connection of LAN/WAN is established Flash: data packets are transferred
High cellular signal	Steady ON: the signal strength of cellular is good
Low cellular signal	Steady ON: the signal strength of cellular is weak
USB	Steady ON: if USB dongle is attached
Serial port	Steady ON: if serial device is attached

# GETTING STARTED

This chapter describes how to install and configure the hardware and how to use the setup wizard to configure the network with the web GUI of MTX-Router-Helios II series.

## 1. Hardware Installation

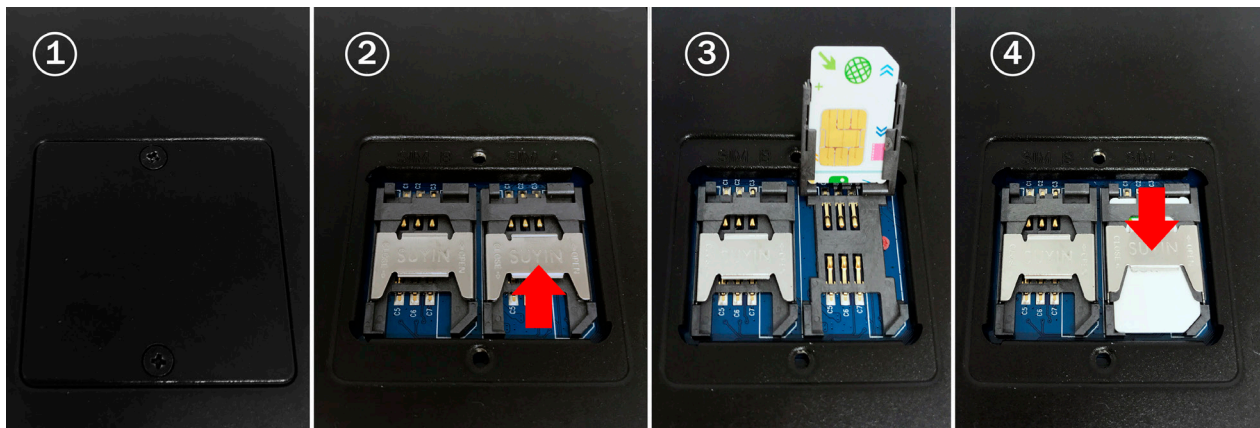
### 1.1 Mount the Unit

The MTX-Router-Helios II series can be placed on a desktop, mounted on the wall, or mounted on a DIN-rail. It has designed with “ears” for attaching to the wall or the inside of a cabinet. The wall-mount kits and DIN-rail bracket are not screwed on the product when out of factory. Please screw the wall-mount kits and DIN-rail bracket on the product first.

### 1.2 Insert the SIM Card

**WARNING: BEFORE INSERTING OR CHANGING THE SIM CARD, PLEASE MAKE SURE THAT POWER OF THE DEVICE IS SWITCHED OFF.**

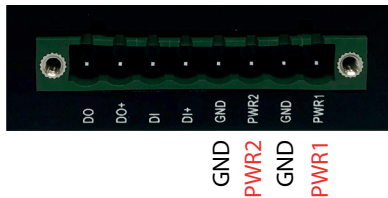
The SIM card slots are located at the bottom side of Helios II housing in order to protect the SIM card. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert a SIM card. After SIM card is well placed, screw back the outer SIM card cover.



- Step 1: Remove the security cover
- Step 2: slide SIM holder to unlock
- Step 3: lift up SIM holder, insert SIM card
- Step 4: place back SIM holder, slide to lock

## 1.3 Connecting Power

The MTX-Router-Helios II series can be powered by connecting a power source to the terminal block. It supports dual 9 to 48VDC power inputs. Following picture is the power terminal block pin assignments. Please check carefully and connect to the right power requirements and polarity.



There are a DC converter and a DC12V/2A power adapter in the package for you to easily connect DC power adapter to this terminal block.



\*Note : If both of power source 1 and power source 2 are connected, the device will choose power source 1 first. If power outage occurred from power source 1, this device will switch to power source 2 automatically and seamlessly.

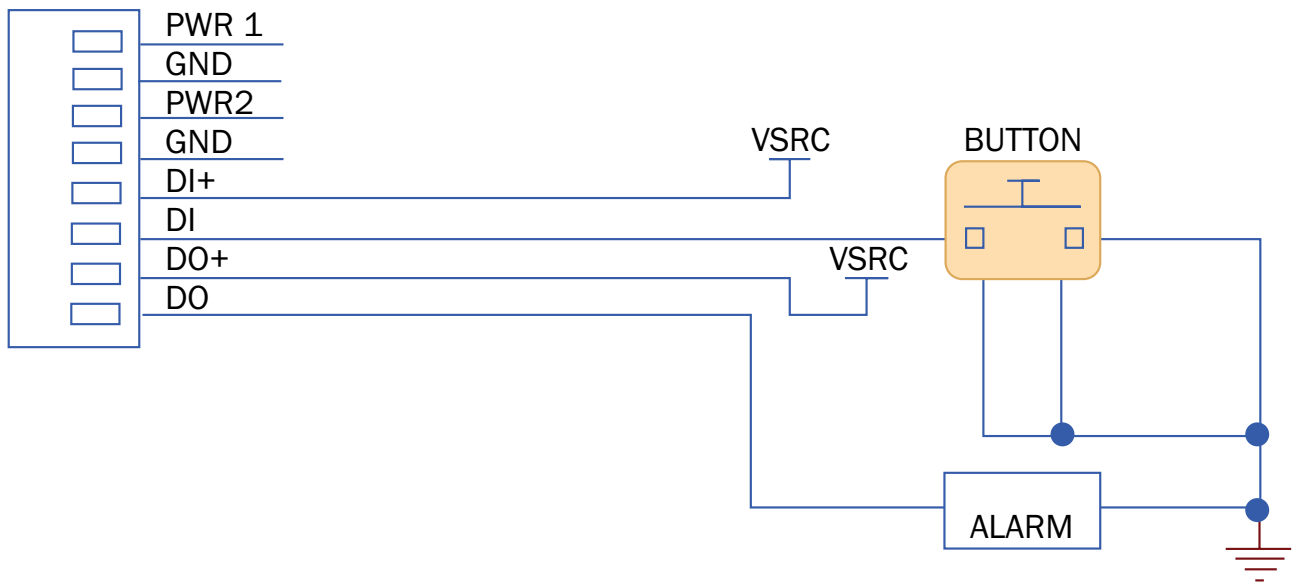
The maximum power consumption of Helios II is 15.5W.

## 1.4 Connecting DI/DO Devices

There are a DI and a DO ports together with power terminal block. Please refer to following specification to connect DI and DO devices.

MODE	SPECIFICATION	
Digital input	Trigger voltage (high)	Logic level 1: 3.3V~30V
	Normal voltage (low)	Logic level 0: 0V~3.0V
Digital output	Voltage (relay mode)	Depends on external device maximum voltage is 30V
	Maximum current	1A

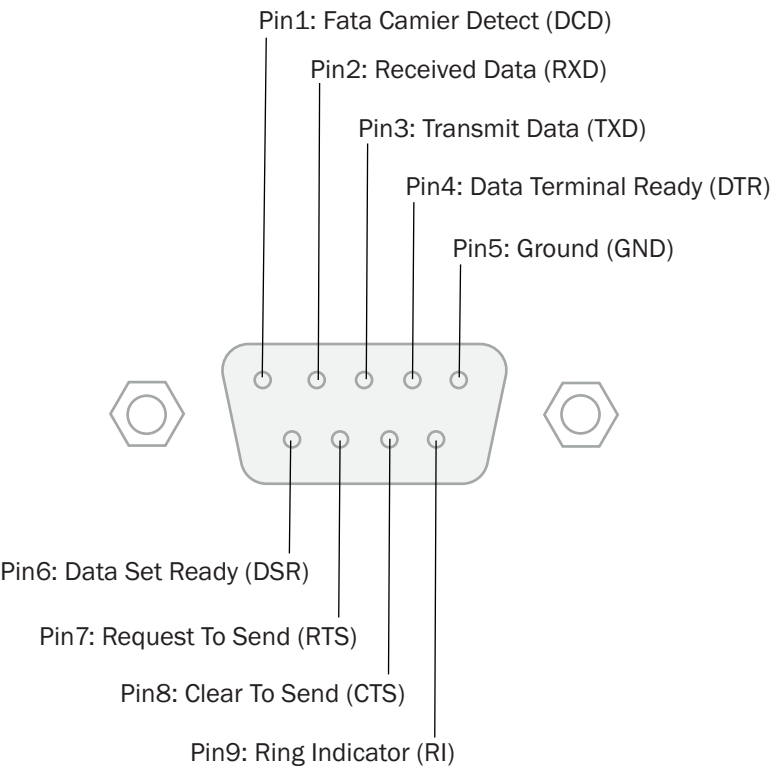
Example of connection diagram:



## 1.5 Connecting Serial Devices

The Helios II provides one standard serial port DB-9 male connector. Connect the serial device to the unit DB-9 male port with the right pin assignments of RS-232/485 are shown as below.

RS232 pinout



	PIN1	PIN2	PIN3	PIN4	PIN5	PIN6	PIN7	PIN8	PIN9
RS-232	DCD	RXD	TXD	DTR	GND	DSR	RTS	CTS	RI
RS-485			DATA+	DATA-	GND				

## 1.6 Connecting to the Network or a Host

The Helios II series provides four RJ45 ports to connect 10/100Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect the Ethernet cable to the RJ45 ports of the device. Plug one end of an Ethernet cable into your computer's network port and the other end into one of Helios II series for LAN ports on the front panel. If you need to configure or troubleshoot the device, you may need to connect the Helios II series directly to the host PC. In this way, you can also use the RJ45 Ethernet cable to connect the Helios II series to the host PC's Ethernet port.

## ● 2. Easy Setup by Configuring WEB UI

You can browse web UI to configure the device. First you need to launch the Setup Wizard browser and then the Setup Wizard will guide you step-by-step to finish the setup process.

### Browse to Activate the Setup Wizard

To start the configuration of the MTX-Router-Helios II, plug an Ethernet cable to any of the 4 Ethernet ports of the router and the other side of the cable directly to the Ethernet port of your computer. Your computer must get the IP by DHCP or fixed IP into the same range of the router 192.168.1.x.

After this, open your web explorer and type the default IP Address <http://192.168.1.2>

To login into the device please use:

Username: admin

Password: admin

You will access to the configuration page. The first screen you will see is the status of the system where you will get the information about network status.

## 2.1 Network Status

In Network Status page, you can review lots information of network status, WAN IPv4 status, WAN IPv6 status, LAN status, and 3G/4G modem status. You can also check the device time at the bottom of this page.

### WAN Interface IPv4 Network Status

Display WAN type, IPv4 information, MAC information, and connection status of multiple WAN interfaces in IPv4 networking. Press “Edit” button if you want to change settings.

WAN Interface IPv4 Network Status									
WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Connecting...	<a href="#">Edit</a>

### WAN Interface IPv6 Network Status

Display WAN type, IPv6 information, and connection status of multiple WAN interfaces in IPv6 networking. Press “Edit” button if you want to change settings.

WAN Interface IPv6 Network Status						
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1			Disable			<a href="#">Edit</a>

### LAN Interface Status

Display IPv4 and IPv6 information of local network. Press “Edit” button if you want to change settings.

LAN Interface Status		
IPv4 Address	IPv4 Subnet Mask	Actions
192.168.0.85	255.255.255.0	<a href="#">Edit IPv4</a>



## 3G/4G Modem Status

Display modem information, link status, signal strength, and network (carrier) name of 3G/4G connection.

3G/4G Modem Status						Refresh
Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions	
3G/4G		Connecting...	N/A		Detail	
USB 3G/4G	N/A	Disconnected	N/A	N/A	Detail	

## Internet Traffic Statistics

Display number of transmitted packets and received packets of each WAN interface.

Internet Traffic Statistics			
WAN ID	Physical Interface	Received Packets	Transmitted Packets
WAN-1	3G/4G	0	0

## Device Time

Display current time information of device.

Device Time: Mon, 11 Jan 2016 10:05:06 +0000

## 2.2 WiFi Status

WiFi Virtual AP List: In order to view the basic information of WiFi virtual APs, it will display operation band, virtual AP ID, WiFi activity, operation mode, SSID, channel, WiFi system, WiFi security approach and MAC address of all virtual APs on status page. Besides, there is an additional Edit command button for each virtual AP to link to the configuration page of that dedicated virtual AP.

WiFi Virtual AP List									
Op. Band	VAP ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.&Security	MAC Address	Action
2.4G	VAP-1	<input checked="" type="checkbox"/>	AP Router	JP.75	Auto	B/G/N Mixed	Auto(None)	00:50:18:96:63:53	Edit
2.4G	VAP-2	<input type="checkbox"/>	AP Router	default	Auto	B/G/N Mixed	Auto(None)	02:50:18:96:63:53	Edit
2.4G	VAP-3	<input type="checkbox"/>	AP Router	default	Auto	B/G/N Mixed	Auto(None)	06:50:18:96:63:53	Edit
2.4G	VAP-4	<input type="checkbox"/>	AP Router	default	Auto	B/G/N Mixed	Auto(None)	0A:50:18:96:63:53	Edit
2.4G	VAP-5	<input type="checkbox"/>	AP Router	default	Auto	B/G/N Mixed	Auto(None)	0E:50:18:96:63:53	Edit
2.4G	VAP-6	<input type="checkbox"/>	AP Router	default	Auto	B/G/N Mixed	Auto(None)	12:50:18:96:63:53	Edit
2.4G	VAP-7	<input type="checkbox"/>	AP Router	default	Auto	B/G/N Mixed	Auto(None)	16:50:18:96:63:53	Edit
2.4G	VAP-8	<input type="checkbox"/>	AP Router	default	Auto	B/G/N Mixed	Auto(None)	1A:50:18:96:63:53	Edit

WiFi Traffic Statistics: In order to view the traffic statistics of WiFi virtual APs, it will display operation band, virtual AP ID and the numbers of received packets and transmitted packets of all virtual APs on status page. Besides, there is an additional Reset command button for each virtual AP to clear the traffic statistics.

WiFi Traffic Statistics <span>Refresh</span>				
Op. Band	VAP ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	660	197	<button>Reset</button>
2.4G	VAP-2	0	0	<button>Reset</button>
2.4G	VAP-3	0	0	<button>Reset</button>
2.4G	VAP-4	0	0	<button>Reset</button>
2.4G	VAP-5	0	0	<button>Reset</button>
2.4G	VAP-6	0	0	<button>Reset</button>
2.4G	VAP-7	0	0	<button>Reset</button>
2.4G	VAP-8	0	0	<button>Reset</button>

## 2.3 LAN Client List

In order to view the connection of current active wired/wireless clients, it will display LAN interface, IP address configuration, host name, MAC address and remaining lease time of all client devices on status page.

LAN Client List				
LAN Interface	IP Address Configuration	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 10.0.75.100	amit-alpha	20-6A-6A-6A-6A-B6	23:21:54
WiFi	Dynamic / 10.0.75.101	android-4bd032267756f548	00-37-6D-26-A2-1C	23:32:50

## 2.4 Firewall Status

In Firewall Status page, you can review lots information of filter status, including Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and other options of firewall.

### Packet Filters

Display all detected contents of firing activated packet filter rules.

Packet Filters <span>Edit</span> <span>[ + ]</span>			
Activated Filter Rule	Detected Contents	IP	Time

### URL Blocking

Display all blocked URLs of firing activated URL blocking rules.

URL Blocking <span>Edit</span> <span>[ + ]</span>			
Activated Blocking Rule	Blocked URL	IP	Time

## Web Content Filters

Display all detected contents of firing activated Web content filter rules.

Web Content Filters <span>Edit</span> <span>[+]</span>			
Activated Filter Rule	Detected Contents	IP	Time

## MAC Control

Display all blocked MAC addresses of firing activated MAC control rules.

MAC Control <span>Edit</span> <span>[+]</span>			
Activated Control Rule	Blocked MAC Addresses	IP	Time

## Application Filters

Display all activated rules of application filters

Application Filters <span>Edit</span> <span>[+]</span>			
Filtered Application Category	Filtered Application Name	IP	Time

## IPS

Display all events of firing activated rules of IPS.

IPS <span>Edit</span> <span>[+]</span>		
Detected Intrusion		Time

## Options

Display option settings of firewall.

Options <span>Edit</span> <span>[+]</span>			
Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

## 2.5 VPN Status

In VPN Status page, you can review lots information of VPN status, including IPSec status, PPTP Server status, PPTP Client status, L2TP Server status and L2TP Client status.

### IPSec Status

Display the status of all activated tunnels of IPSec.

IPSec Status <span>Edit</span>							
Tunnel Name	Tunnel Scenario	Local Subnet	Local Subnet Mask	Remote IP/FQDN	Remote Subnet	Remote Subnet Mask	Status

## PPTP Server Status

Display the status of all activated accounts of PPTP server.

PPTP Server Status <span>Edit</span>				
User Name	Peer IP/FQDN	Peer Virtual IP	Peer Call ID	Status

## PPTP Client Status

Display the status of all activated PPTP clients.

PPTP Client Status <span>Edit</span>					
PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status

## L2TP Server Status

Display the status of all activated accounts of L2TP server.

L2TP Server Status <span>Edit</span>				
User Name	Peer IP/FQDN	Virtual IP	Peer Call ID	Status

## L2TP Client Status

Display the status of all activated L2TP clients.

L2TP Client Status <span>Edit</span>					
L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status

## 2.6 System Management Status

In System Management Status page, you can review lots information of SNMP and TR-069 status.

### SNMP Linking Status

Display information of SNMP linking.

SNMP Linking Status						
User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

### SNMP Trap Information

Display information of SNMP traps.

SNMP Trap Information		
Trap Level	Time	Trap Event

TR-069 Status

Display link status of TR-069.

TR-069 Status	
Link Status	
Off	

2.7 GNSS Status

Go to Status > Administration > GNSS tab.

The GNSS Information screen shows the status for current GNSS positioning information for the gateway.

GNSS Information						
Condition	No. of Satellites	Satellites ID / Signal Strength (dBm)	Position (Lat, Long)	Altitude (meters)	True Course	Ground Speed (km/h)
Not Fixed						


The available GNSS information includes GNSS Condition, No. of Satellites, Satellites ID / Signal Strength, Position (Lat., Long.), Altitude (meters), True Course, and the equivalent Ground Speed (km/h).

# MAKING CONFIGURATIONS

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web browser and typing in the IP Address of the device. The default IP Address is: 192.168.1.2 In the configuration section you may want to check the connection status of the device, to do Basic or Advanced Network setup or to check the system status. These task buttons can be easily found in the cover page of the UI (User Interface).

Enter the default password “admin” in the Password and then click ‘Login’ button.

Afterwards, you can go Basic Network, Advanced Network, SMS Remote Management, System or Status respectively on left hand side of webpage.



Firmware rev: BUTE0.1008\_12101122  
Date: 2015\_12\_10  
Copyright Matrix Electronica S.L

- Basic Network
  - WAN
  - LAN
  - WiFi
  - IPv6
  - NAT/DMZ
  - Routing
- Advanced Network
  - Firewall
  - QoS & BWM
  - VPN
  - Redundancy
  - System Management
  - Certificate
  - Serial Port Settings
- SMS Remote Management
  - SMS Remote Management
  - I/O Management
- System
  - System Related
  - Scheduling
  - MMI
- Status
  - Network Status
  - WiFi Status
  - LAN Client List
  - Firewall Status
  - VPN Status
  - System Mgmt. Status

### WAN Interface IPv4 Network Status

WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Connecting...	Edit

### WAN Interface IPv6 Network Status

WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1			Disable			Edit

### LAN Interface Status

IPv4 Address	IPv4 Subnet Mask	Actions
192.168.0.65	255.255.255.0	Edit IPv4

### 3G/4G Modem Status

Refresh

Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
3G/4G	D18Q1	Connecting...	N/A	Emergency Only	Detail
USB 3G/4G	N/A	Disconnected	N/A	N/A	Detail

### Internet Traffic Statistics

WAN ID	Physical Interface	Received Packets	Transmitted Packets
WAN-1	3G/4G	0	0

Device Time: Mon, 11 Jan 2016 10:22:25 +0000

Note: You can see the first screen is located at Status >> Network Status after you logged in and the screen shows the Network Connection Status below.

## ● 1. Basic Network

You can enter Basic Network for WAN, LAN, WiFi, IPv6, NAT/DMZ, and Routing settings as the icon shown here.

### 1.1 WAN Setup

This device is equipped with three WAN Interfaces to support different WAN types of connection. You can configure one by one to get proper Internet connection setup.

3G/4G WAN: The gateway has one 3G/4G modem built-in, please plug in SIM card and follow UI setting to setup.

#### CAUTION

- Please MUST POWER OFF the gateway before you insert or remove SIM card
- It will damage SIM card if you insert or remove SIM card during gateway is in operation
- Please follow instructions at section 2.1.2

USB 3G/4G WAN: The gateway has one USB port that can support USB 3G/4G modem dongle . Please plug 3G/LTE USB dongle and follow UI setting to setup.

Ethernet WAN: The 1st Ethernet port (noted as LAN-1/WAN) can be configured as WAN connection. Please plug in RJ45 cable from your external DSL modem and follow UI setting to setup.

#### 1.1.1 Internet Setup

There are three physical WAN interfaces that you can configure one by one to get proper Internet connection setup. They include the 3G/4G and Ethernet WAN types. For 3G/4G WAN type, the WAN interface is 3G/4G or USB 3G/4G and the ISP is a mobile operator that can provide LTE, HSPA+, HSPA, WCDMA, EDGE, GPRS data services. However, for Ethernet WAN interface, a fixed line ISP provides xDSL or cable modem with Dynamic IP, Static IP, PPPoE, PPTP and L2TP connection types. Especially, for 3G/4G WAN interface, the device product supports Dual-SIM failover mechanism.

Hereafter are some details of WAN type options:

3G/4G: If you have subscribed 3G/LTE data services from mobile operators. This gateway can support LTE/3G/2G depends on respective specifications. However, if your 3G data plan is not with a flat rate, it's recommended to set Connection Control mode to Connect-on-demand or Manually.

Dynamic IP Address: You may choose this WAN type if you connects a cable modem or a fiber (VDSL modem) for Internet connection. The assigned IP address may be different every time.

Static IP Address: If you get a fixed IP address from your ISP.

PPP over Ethernet: As known as PPPoE. This WAN type is widely used for ADSL connection.

PPTP: This WAN type is more popular in Russia.

L2TP: This WAN type is more popular in Israel.

### 1.1.1.1 3G/4G WAN-3G/4G

Click on the “Edit” button for the 3G/4G WAN interface and you can get the detail WAN settings and then configure the settings as well.

Internet Setup				
Physical Interface				
Load Balance				
Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	<a href="#">Edit</a>
WAN-2	-	Disable	-	<a href="#">Edit</a>
WAN-3	-	Disable	-	<a href="#">Edit</a>

WAN Type: 3G/4G

### Internet Connection Configuration ( WAN - 1 )

WAN Type 3G/4G

### 3G/4G WAN Type Configuration

Preferred SIM Card SIM-A First

#### Preferred SIM card

Choose “SIM-A First”, “SIM-B First”, “SIM-A Only” or “SIM-B Only” for 3G/4G connection. There are two SIM card slots attached to each cellular modem and with four kinds of SIM card usage scenarios, including “SIM-A First”, “SIM-B First”, “SIM-A Only” and “SIM-B Only”. By default, “SIM-A First” scenario is used to connect to mobile system for data transferring. If using “SIM-A First” scenario, the gateway will try to connect to the Internet by using SIM-A card first. And when the connection is broken, gateway system will switch to use SIM-B card for an alternate automatically. System will not switch back to use SIM-A card unless SIM-B connection is also broken. That is, SIM-A and SIM-B are used iteratively, but either one will keep being used for data transferring when current connection is still alive. In the same way, the gateway will try to connect to the Internet by using SIM-B card first if choosing “SIM-B First”. However, when “SIM-A Only” or “SIM-B Only” is used, that means the specified SIM slot of card is the ONLY one to be used for negotiation parameters between gateway device and mobile base station.

When you select “SIM-A First” or “SIM-A Only”, there will be a configuration window of “Connection with SIM-A Card” beneath the “3G/4G WAN Type Configuration” window. However, when you select “SIM-B First” or “SIM-B Only”, there will be a configuration window of “Connection with SIM-B Card” beneath the “3G/4G WAN Type Configuration” window. All configuration items are the same in SIM-A and SIM-B configuration. Furthermore, there is also a common configuration window for 3G/4G connection after “3G/4G WAN Type Configuration” window, “Connection with SIM-A Card” window and “Connection with SIM-B Card” window.



## Connection with SIM-A Card

Dial-up Profile	<input type="radio"/> Auto-detection <input checked="" type="radio"/> Manual-configuration
Country	<input type="text" value="Spain"/>
Service Provider	<input type="text" value="Movistar"/>
APN	<input type="text" value="movistar.es"/> (Optional)
PIN Code	<input type="text"/> (Optional)
Dial Number	<input type="text"/>
User	<input type="text" value="MOVISTAR"/> (Optional)
Password	<input type="text" value="****"/> (Optional)
Authentication	<input type="text" value="Auto"/>
Primary DNS	<input type="text"/> (Optional)
Secondary DNS	<input type="text"/> (Optional)
Roaming	<input type="checkbox"/> Enable

### Dial-up profile

After you subscribe 3G/4G data service, your operator will provide some information for you to setup connection, such as APN, dialed number, account or password. If you know this information exactly, you can choose “Manual-configuration” option and type in that information by your own. Otherwise, you can select “Auto-detection” to let this gateway detect automatically. Even you choose “Manual” setting, this gateway will show responding information for your reference to setup the dial-up profile after you select country and service provider.

If you choose “SIM-A First” or “SIM-A Only” for Preferred SIM Card, you need to input dial-up profile for SIM-A. Similarly, you need to input dial-up profile for SIM-B when you choose “SIM-B First” or “SIM-B Only” as your preferred one.

### Country & Service Provider

When you choose “Manual-configuration” option for the Dial-up Profile, you must select the country and service provider to retrieve related parameters from system for dialing up to connect to Internet. Once system doesn’t store related parameters or stores not-matched parameters, you must specify them one by one manually.

### APN

When you select the target country and service provider for manual dial-up profile, system will show related APN value. Change it if it is not correct for you.

### PIN Code

Enter PIN code of SIM card if your SIM card needs it to unlock.

## Dial Number

Enter the dialed number that is provided by your ISP.

## Account & Password

Enter Account and Password that is provided by your ISP.

## Authentication

Choose “Auto”, “PAP”, or “CHAP” according to your ISP’s authentication approach. Just keep it with “Auto” if you can’t make sure.

## Primary/Secondary DNS

Enter IP address of Domain Name Server. You can keep them in blank, because most ISP will assign them automatically.

### Connection Common Configuration

Connection Control	Auto-reconnect (Always on) ▼
Time Schedule	(0) Always ▼
MTU	0 (0 is Auto)
NAT	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Enable
	<input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking
	<input checked="" type="checkbox"/> Loading Check
	Check Interval 3 (seconds)
	Check Timeout 3 (seconds)
	Latency Threshold 3000 (ms)
	Fail Threshold 10 (Times)
	Target1 DNS1 ▼
	Target2 None ▼
Network Monitoring	
IGMP	Disable ▼
WAN IP Alias	<input type="checkbox"/> Enable 10.0.0.1
	<input type="button" value="Save"/> <input type="button" value="Undo"/>

## Connection Control

Select your connection control scheme from the drop list: “Auto-reconnect (Always on)”, “Dial-on-demand” or “Connect Manually”. If selecting “Auto-reconnect (Always on)”, this gateway will start to establish Internet connection automatically since it’s powered on. It’s recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing “Dial-on-demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. During normal operation, this gateway will disconnect WAN connection if idle time reaches the value of “Maximum Idle Time”. If choosing “Connect Manually”, this gateway won’t start to establish

WAN connection until you press “Connect” button on web UI. During normal operation, this gateway will disconnect WAN connection if idle time reaches the value of “Maximum Idle Time”.

### Time Schedule

This option allows you to limit WAN connection available in a certain time period. You can select “Always” option or a time schedule object from the schedule object list that you can find them in [System]-[Scheduling].

### MTU

MTU refers to “Maximum Transmit Unit”. Different WAN types of connection will have different value. You can leave it with 0 (Auto) if you are not sure about this setting.

### NAT

By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.

### Network Monitoring

You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

1. Enable: check the box to do Network Monitoring. By default, it is checked.
2. DNS Query/ICMP Checking: do the keep alive through DNS query packets or ICMP packets.
3. Loading Checking: The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection. By default, the Loading Checking is enabled.
4. Check Interval: indicate how often to send keep-alive packet.
5. Check Timeout: set allowance of time period to receive response of keep-alive packet. If this gateway doesn't receive response within this time period, this gateway will record this keep alive is failed.
6. Latency Threshold: set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.
7. Fail Threshold: times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.
8. Target1/Target2: set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

## IGMP

Enable or disable multicast traffics from Internet. You may enable as auto mode or select by the option list of IGMP v1, IGMP v2, IGMP v3 and Auto.

## WAN IP Alias

The device supports 2 WAN IP addresses for a physical interface, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this.

### 1.1.2 Physical Interface

Click on the “Edit” button for each WAN interface and you can get the detail physical interface settings and then configure the settings as well. By default, the WAN-1 interface is forced to “Always on” mode, and operates as the primary internet connection; the interfaces WAN-2 and WAN-3 are disabled.

Internet SetupPhysical InterfaceLoad Balance

Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	3G/4G	Always on	0 (Mbps) / 0 (Mbps)	<div>Edit</div>
WAN-2	-	Disable	0 (Mbps) / 0 (Mbps)	<div>Edit</div>
WAN-3	-	Disable	0 (Mbps) / 0 (Mbps)	<div>Edit</div>

## WAN-1

The operation mode of this interface is forced to “Always on” mode, and operates as the primary Internet connection. You can click on the respective “Edit” button and configure the rest items for this interface.

## WAN-2~WAN-3

The operation mode of this interface is disabled by default, you can click on the respective “Edit” button to configure.

### Interface Configuration ( WAN- 1 )

Physical Interface	<input type="text" value="Ethernet"/>
Operation Mode	<input type="text" value="Always on"/>
Line Speed	<input type="text" value=""/> Mbps / <input type="text" value=""/> Mbps (Upload / Download)
VLAN Tagging	<input type="checkbox"/> Enable <input type="text" value="0"/> (1-4095)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

## Physical Interface

Select the WAN interface from the available list. For this gateway, there are “Ethernet”, “3G/4G”, and “USB 3G/4G” items. If you want to use embedded 3G/4G modem to operate as the primary Internet connection (WAN-1), please choose “3G/4G” for configuring the embedded 3G/4G modem as primary WAN connection. Or you can select “USB 3G/4G” if you want to use attached 3G/LTE USB dongle as an Internet connection. Otherwise, you can choose “Ethernet” if you would like the RJ45 port to be the primary Internet connection.

## Operation Mode

There are three options for this item.

1. Always on: set this WAN interface to be active all the time. It means two or more Internet connections will be established simultaneously, and outgoing data will be transferred through these WAN connections base on load balance policies. This mode is especially suitable for high bandwidth requirement, such as video stream transmission.
2. Failover: set this WAN interface to be a backup WAN connection. This WAN interface won't be active until other WAN connection is failed. If you specified a certain WAN interface as a “Failover” WAN, you have to further identify which WAN interface is to be failover and fallback.

▶ Operation Mode	Failover ▼	WAN-1 ▼	Seamless <input type="checkbox"/> Enable
------------------	------------	---------	--

For the example above, if WAN-1 connection is broken, this gateway will try to failover the Internet connection to this WAN interface automatically. When WAN-1 connection becomes available again, the Internet connection will switch back to WAN-1 automatically.

Besides, for some mission-critical applications, this gateway supports “Seamless failover” to shorten switch time between WAN interface failover and fallback. That is, if an interface serves as a “Seamless Failover” WAN, the WAN connection will be activated after system has operated normally, even without data flow in it. When the primary connection is broken, fast switching data flow to the WAN interface is the major concern for “Seamless Failover”.

3. Disable: deactivate this WAN interface.

## Line Speed

You can specify the upstream / downstream speed (Mbps) for the corresponding WAN connection. Such information will be referred in QoS and load balance function to manage the traffic load for each WAN connection.

## VLAN Tagging

If your ISP required a VLAN tag to be inserted into the WAN packets, you can enable this setting, and enter the specified tag value.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

### 1.1.2.2 Ethernet WAN

Click on the “Edit” button for the Ethernet WAN interface and you can get the detail WAN settings and then configure the settings as well. The device provides “Static IP Address”, “Dynamic IP Address”, “PPP over Ethernet”, “PPTP” and “L2TP” WAN types for the Ethernet WAN interface to connect to the Internet.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Static IP	<a href="#">Edit</a>
WAN-2	3G/4G	Always on	3G/4G	<a href="#">Edit</a>
WAN-3	USB 3G/4G	Failover	3G/4G	<a href="#">Edit</a>

#### 1.1.2.2.1 Dynamic IP Address

##### Internet Connection Configuration ( WAN - 1 )

WAN Type Dynamic IP ▼

##### Dynamic IP WAN Type Configuration

Host Name  (Optional)

▶ ISP Registered MAC Address  [Clone](#)

Connection Control Auto-reconnect (Always on) ▼

MTU  (0 is Auto)

NAT ☒ Enable  
☒ Enable  
☐ DNS Query ☒ ICMP Checking  
☒ Loading Check  
Check Interval  (seconds)  
Check Timeout  (seconds)  
Latency Threshold  (ms)  
Fail Threshold  (Times)  
Target1 DNS1 ▼  
Target2 None ▼

IGMP Disable ▼

WAN IP Alias ☐ Enable

[Save](#) [Undo](#)

#### WAN Type

Choose “Dynamic IP” from the drop list.

#### Host Name

Optional, required by some ISPs, for example, @Home.

## ISP registered MAC Address

Some ISP would ask you to register a MAC address for Internet connection. In this case, you need to enter the registered MAC address here, or simply press “Clone” button to copy MAC address of your PC to this field.

## Connection Control

Select your connection control scheme from the drop list: “Auto-reconnect (Always on)”, “Dial-on-demand” or “Manually”. If selecting “Auto-reconnect (Always on)”, this gateway will start to establish Internet connection automatically since it’s powered on. It’s recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing “Dial-on-demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

## MTU

Most ISP offers MTU value to users. The default value is 0 (auto).

## NAT

By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.

## Network Monitoring

You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

1. Enable: check the box to do Network Monitoring.
2. DNS Query/ICMP Checking: do the keep alive through DNS query packets or ICMP packets.
3. Loading Checking: the response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.
4. Check Interval: indicate how often to send keep-alive packet.
5. Check Timeout: set allowance of time period to receive response of keep-alive packet. If this gateway doesn’t receive response within this time period, this gateway will record this keep alive is failed.
6. Latency Threshold: set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.

7. Fail Threshold: times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

8. Target1/Target2: set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

## **IGMP**

Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.

## **WAN IP Alias**

In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.



### 1.1.2.2.2 Static IP Address

Select this option if ISP provides a fixed IP address to you. You will need to enter in the IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The gateway will not accept the IP address if the format is not correct.

#### Internet Connection Configuration ( WAN - 1 )

WAN Type	<div>Static IP ▼</div>	
<b>Static IP WAN Type Configuration</b>		
WAN IP Address	<input type="text"/>	
WAN Subnet Mask	<input type="text"/>	
WAN Gateway	<input type="text"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	
MTU	<input type="text" value="0"/>	(0 is Auto)
NAT	<input checked="" type="checkbox"/> Enable	
	<input checked="" type="checkbox"/> Enable	
	<input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking	
	<input checked="" type="checkbox"/> Loading Check	
	Check Interval	<input type="text" value="5"/> (seconds)
	Check Timeout	<input type="text" value="3"/> (seconds)
	Latency Threshold	<input type="text" value="3000"/> (ms)
	Fail Threshold	<input type="text" value="5"/> (Times)
	Target1	<div>DNS1 ▼</div>
	Target2	<div>None ▼</div>
Network Monitoring		
IGMP	<div>Disable ▼</div>	
WAN IP Alias	<input type="checkbox"/> Enable <input type="text" value="10.0.0.1"/>	
<div>Save Undo</div>		

#### WAN Type

Choose “Static IP” from the drop list.

#### WAN IP address/Subnet Mask/Gateway

Enter the IP address, subnet mask, and gateway address which is provided by your ISP.

#### Primary DNS/Secondary DNS

Input the IP address of primary and secondary DNS server that is provided by your ISP. Secondary DNS can be ignored if only one DNS server is provided by your ISP.

## MTU

Most ISP offers MTU value to users. The default value is 0 (auto).

## NAT

By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.

## Network Monitoring

You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

1. Enable: check the box to do Network Monitoring.
2. DNS Query/ICMP Checking: do the keep alive through DNS query packets or ICMP packets.
3. Loading Checking: the response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.
4. Check Interval: indicate how often to send keep-alive packet.
5. Check Timeout: set allowance of time period to receive response of keep-alive packet. If this gateway doesn't receive response within this time period, this gateway will record this keep alive is failed.
6. Latency Threshold: set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.
7. Fail Threshold: times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.
8. Target1/Target2: set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

## IGMP

Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.

## WAN IP Alias

In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

### 1.1.2.2.3 PPP over Ethernet

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for ADSL services.

#### Internet Connection Configuration ( WAN - 1 )

WAN Type	PPPoE ▼	
<b>PPPoE WAN Type Configuration</b>		
IPv6 Dual Stack	<input type="checkbox"/> Enable	
PPPoE Account	<input type="text"/>	
PPPoE Password	<input type="password"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	
Connection Control	Auto-reconnect (Always on) ▼	
Service Name	<input type="text"/>	(Optional)
Assigned IP Address	<input type="text"/>	(Optional)
MTU	<input type="text" value="0"/>	(0 is Auto)
NAT	<input checked="" type="checkbox"/> Enable	
	<input checked="" type="checkbox"/> Enable	
	<input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking	
	<input checked="" type="checkbox"/> Loading Check	
	Check Interval	<input type="text" value="5"/> (seconds)
	Check Timeout	<input type="text" value="3"/> (seconds)
	Latency Threshold	<input type="text" value="3000"/> (ms)
	Fail Threshold	<input type="text" value="5"/> (Times)
	Target1	DNS1 ▼
	Target2	None ▼
Network Monitoring		
IGMP	Disable ▼	
WAN IP Alias	<input checked="" type="checkbox"/> Enable	<input type="text" value="10.0.0.1"/>
<div>Save Undo</div>		

#### WAN Type

Choose “PPPoE” from the drop list.

#### IPv6 Dual Stack

You can enable this option if your ISP provides not only one IPv4 but also one IPv6 address.

#### PPPoE Account and Password

The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security concern, the password you input won't be displayed on web UI.

#### Primary DNS/ Secondary DNS

In most cases, ISP will assign DNS server automatically after PPPoE connection is established. Input the

IP address of primary and secondary DNS server manually if required.

### Connection Control

Select your connection control scheme from the drop list: “Auto-reconnect (Always-on)”, “Dial-on-demand” or “Manually”. If selecting “Auto-reconnect (Always-on)”, this gateway will start to establish Internet connection automatically since it’s powered on. It’s recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing “Dial-on-demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

### Service Name/Assigned IP Address

ISP may ask you to use a specific service name when connecting PPPoE connection. In some cases, ISP can also provide you a fixed IP address with PPPoE connection. For these cases, you need to add that information in this field.

### MTU

Most ISP offers MTU value to users. The default MTU value is 0 (auto).

### NAT

By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.

### Network Monitoring

You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

1. Enable: check the box to do Network Monitoring.
2. DNS Query/ICMP Checking: do the keep alive through DNS query packets or ICMP packets.
3. Loading Checking: the response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.
4. Check Interval: indicate how often to send keep-alive packet.
5. Check Timeout: set allowance of time period to receive response of keep-alive packet. If this gateway doesn’t receive response within this time period, this gateway will record this keep alive is failed.

6. Latency Threshold: set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.

7. Fail Threshold: times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

8. Target1/Target2: set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

## IGMP

Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.

## WAN IP Alias

In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

### 1.1.2.2.4 PPTP

Choose PPTP (Point-to-Point Tunneling Protocol) if your ISP used a PPTP connection. Your ISP will provide you with a username and password.

#### Internet Connection Configuration ( WAN - 1 )

WAN Type	<input type="text" value="PPTP"/>
<b>PPTP WAN Type Configuration</b>	
IP Mode	<input type="text" value="Dynamic IP Address"/>
Server IP Address / Name	<input type="text"/>
PPTP Account	<input type="text"/>
PPTP Password	<input type="text"/>
Connection ID	<input type="text"/> (Optional)
Connection Control	<input type="text" value="Auto-reconnect (Always on)"/>
MTU	<input type="text" value="0"/> (0 is Auto)
MPPE	<input type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable
	<input checked="" type="checkbox"/> Enable
	<input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking
	<input checked="" type="checkbox"/> Loading Check
Network Monitoring	Check Interval <input type="text" value="5"/> (seconds)
	Check Timeout <input type="text" value="3"/> (seconds)
	Latency Threshold <input type="text" value="3000"/> (ms)
	Fail Threshold <input type="text" value="5"/> (Times)
	Target1 <input type="text" value="DNS1"/>
	Target2 <input type="text" value="None"/>
IGMP	<input type="text" value="Disable"/>
WAN IP Alias	<input type="checkbox"/> Enable <input type="text" value="10.0.0.1"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

## WAN Type

Choose “PPTP” from the drop list.

## IP Mode

Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “WAN IP Address”, “WAN Subnet Mask”, and “WAN Gateway” settings provided by your ISP.

▶ IP Mode	<div>Static IP Address ▼</div>
▶ WAN IP Address	<input type="text"/>
▶ WAN Subnet Mask	<input type="text"/>
▶ WAN Gateway	<input type="text"/>

## Server IP Address/Name

IP address of the PPTP server provided by ISP.

## PPTP Account and Password

The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security concern, the password you input won’t be displayed on web UI.

## Connection ID

Optional, input the connection ID if your ISP requires it.

## Connection Control

Select your connection control scheme from the drop list: “Auto-reconnect (Always on)”, “Dial-on-demand” or “Manually”. If selecting “Auto-reconnect (Always on)”, this gateway will start to establish Internet connection automatically since it’s powered on. It’s recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing “Dial-on-demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

## MTU

Most ISP offers MTU value to users. The default MTU value is 0 (auto).

## MPPE (Microsoft Point-to-Point Encryption)

Enable this option to add encryption on transferred and received data packets. Please check with your ISP to see if this feature is supported or not.

## NAT

By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.

## Network Monitoring

You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

1. Enable: check the box to do Network Monitoring.
2. DNS Query/ICMP Checking: do the keep alive through DNS query packets or ICMP packets.
3. Loading Checking: the response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.
4. Check Interval: indicate how often to send keep-alive packet.
5. Check Timeout: set allowance of time period to receive response of keep-alive packet. If this gateway doesn't receive response within this time period, this gateway will record this keep alive is failed.
6. Latency Threshold: set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.
7. Fail Threshold: times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.
8. Target1/Target2: set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

## IGMP

Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.

## WAN IP Alias

In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

### 1.1.2.2.5 L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP used a L2TP connection. Your ISP will provide you with a username and password.

#### Internet Connection Configuration ( WAN - 1 )

WAN Type	<div>L2TP ▼</div>
<b>L2TP WAN Type Configuration</b>	
IP Mode	<div>Dynamic IP Address ▼</div>
Server IP Address / Name	<div></div>
L2TP Account	<div></div>
L2TP Password	<div></div>
Connection Control	<div>Auto-reconnect (Always on) ▼</div>
MTU	<div>0 (0 is Auto)</div>
Service Port	<div>User-defined ▼ 1702</div>
MPPE	<div><input type="checkbox"/> Enable</div>
NAT	<div><input checked="" type="checkbox"/> Enable</div>
	<div><input checked="" type="checkbox"/> Enable</div>
	<div><input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking</div>
	<div><input checked="" type="checkbox"/> Loading Check</div>
	<div>Check Interval 5 (seconds)</div>
	<div>Check Timeout 3 (seconds)</div>
	<div>Latency Threshold 3000 (ms)</div>
	<div>Fail Threshold 5 (Times)</div>
	<div>Target1 DNS1 ▼</div>
	<div>Target2 None ▼</div>
Network Monitoring	
IGMP	<div>Disable ▼</div>
WAN IP Alias	<div><input type="checkbox"/> Enable 10.0.0.1</div>
<div>Save Undo</div>	

#### WAN Type

Choose “L2TP” from the drop list.

#### IP Mode

Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “IP Address”, “Subnet Mask”, and “WAN Gateway IP” settings provided by your ISP.

▶ IP Mode	<div>Static IP Address ▼</div>
▶ WAN IP Address	<div></div>
▶ WAN Subnet Mask	<div></div>
▶ WAN Gateway	<div></div>

#### Server IP Address/Name

IP address of the L2TP server provided by ISP.



## L2TP Account and Password

The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security concern, the password you input won't be displayed on web UI.

## Connection Control

Select your connection control scheme from the drop list: "Auto-reconnect (Always on)", "Dial-on-demand" or "Manually". If selecting "Auto-reconnect (Always on)", this gateway will start to establish Internet connection automatically since it's powered on. It's recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing "Dial-on-demand", this gateway won't start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing "Manually", this gateway won't start to establish WAN connection until you press "Connect" button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

## MTU

Most ISP offers MTU value to users. The default MTU value is 0 (auto).

## MPPE (Microsoft Point-to-Point Encryption)

Enable this option to add encryption on transferred and received data packets. Please check with your ISP to see if this feature is supported or not.

## NAT

By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.

## Network Monitoring

You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

1. Enable: check the box to do Network Monitoring.
2. DNS Query/ICMP Checking: do the keep alive through DNS query packets or ICMP packets.
3. Loading Checking: the response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.
4. Check Interval: indicate how often to send keep-alive packet.
5. Check Timeout: set allowance of time period to receive response of keep-alive packet. If this gateway

doesn't receive response within this time period, this gateway will record this keep alive is failed.

6. Latency Threshold: set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.

7. Fail Threshold: times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

8. Target1/Target2: set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

## IGMP

Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.

## WAN IP Alias

In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

### 1.1.3 Load Balance

This device support multi-WAN load balance function and more than one WAN interface can access to Internet at a time. The load balance function can help you to manage the outbound traffics and to maximize the utilization of available bandwidth.

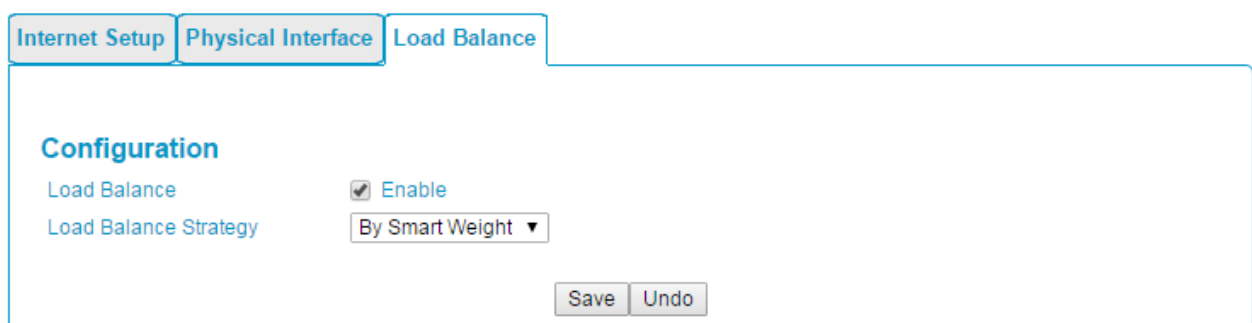
## Load Balance

Enable or disable the load balance function.

## Load Balance Strategy

Once you enabled the load balance function, you have to further configure which strategy is to be applied for load balancing the outbound traffics. There are three load balance strategy: "By Smart Weight", "By Priority", and "By User Policy."

### 1. By Smart Weight



Internet Setup Physical Interface Load Balance

**Configuration**

Load Balance ☒ Enable

Load Balance Strategy By Smart Weight ▼

Save Undo

If you choose the “By Smart Weight” strategy, No any other setting is required. This device will automatically allocate the outbound traffics to each WAN interface.

## 2. By Priority

Internet Setup

Physical Interface

Load Balance

**Configuration**

Load Balance ☒ Enable

Load Balance Strategy By Priority ▼

**Priority Definition**

WAN ID	Priority (%)	Action
WAN - 1	100%	<div>Edit</div>

Save

Undo

If you choose the “By Priority” strategy, you have to further specify the outbound traffic percentage for each WAN interface. The load balancing mechanism will follow these settings to allocate proper connection traffics for each WAN to access the internet.

## 3. By User Policy

Internet Setup

Physical Interface

Load Balance

**Configuration**

Load Balance ☒ Enable

Load Balance Strategy By User Policy ▼

**User Policy List**

Add

Delete

Save

Undo

If you choose the “By User Policy” strategy, you have to create the expected policies one by one. Click the “add” button to add your load balance policy.

You can manage the outbound traffic flows and force specific traffics to access Internet through designated WAN interface. For those traffics not covered in the user policy rules, the device will allocate the WAN interface by applying “Smart Weight” mechanism simultaneously.

## Source IP Address

Enter the expected Source IP Address for the load balance policy. It can be “Any”, “Subnet”, “IP Range”, or “Single IP”. Just choose one type of the source IP address, and specify its value as well. If you don't

want to specify a certain source IP address for this policy, just leave it as “Any.”

### **Destination IP Address**

Enter the expected Destination IP Address for the load balance policy. It can be “Any”, “Subnet”, “IP Range”, “Single IP”, or “Domain Name”. Just choose one type of the destination IP address, and specify its value as well. If you don’t want to specify a certain destination IP address for this policy, just leave it as “Any.”

### **Destination Port**

Enter the expected Destination Port number for the load balance policy. It can be “All”, “Port Range”, “Single Port”, or “Well-known Applications”. Just choose one type of the destination port, and specify its value as well. If you don’t want to specify a certain destination port for this policy, just leave it as “All.”

### **Protocol**

Enter the expected protocol type for the load balance policy. It can be “TCP”, “UDP” or “Both”. If you don’t want to specify a certain protocol type for this policy, just leave it as “Both.”

### **WAN Interface**

Identify which WAN interface is to be selected for accessing the Internet if all of above source and destination criteria are matched for the outbound traffics.

### **Policy**

Enable or disable this user policy.

## 1.2 LAN Setup

This device is equipped with four Fast Ethernet LAN ports as to connect your local devices via Ethernet cables at “Reset to Default” state. But for the first Ethernet LAN, noted as LAN-1/WAN, it can be configured an Ethernet WAN interface for Internet connection. Please see the Basic Network >> WAN settings. Besides, VLAN function is provided to organize your local networks.

Ethernet LAN

VLAN

Dynamic DNS

Configuration

LAN IP Address

192.168.0.65

Subnet Mask

255.255.255.0 (/24)

DHCP Server List

Add

Delete

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Server Enable	Actions
DHCP 1	192.168.0.65	255.255.255.0	192.168.0.100-192.168.0.200	86400		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<div>Edit</div>
DHCP 2	192.168.10.1	255.255.255.0	192.168.10.2-192.168.10.253	86400		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<div>Edit</div> <div>Select</div>

Fixed Mapping...

Save

Undo

### 1.2.1 Ethernet LAN

Please follow the following instructions to do IPv4 Ethernet LAN Setup.

#### LAN IP Address

The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI.

#### Subnet Mask

Input your Subnet mask. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.

### 1.2.2 DHCP Server

#### 1.2.2.1 DHCP Server List

The gateway supports up to 4 DHCP servers to serve the DHCP requests from different VLAN groups. And there is one default one whose LAN IP Address is the same one of gateway LAN interface, Subnet Mask is “255.255.255.0,” and IP Pool ranges from .100 to .200 as shown at following DHCP Server List. You can add or edit one DHCP server configuration by clicking on the “Add” button behind “DHCP Server List”

or the “Edit” button at the end of DHCP server information.

There are two additional buttons can be used to show the DHCP client list and the fixed mapping between MAC address and IP address of local client hosts as following diagram.

**DHCP Server List**

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Server Enable	Actions
DHCP 1	192.168.0.65	255.255.255.0	192.168.0.100-192.168.0.200	86400		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="button" value="Edit"/>
DHCP 2	192.168.10.1	255.255.255.0	192.168.10.2-192.168.10.253	86400		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Select"/>

### 1.2.2.2 DHCP Server Configuration

Ethernet LAN **VLAN** Dynamic DNS

**DHCP Server Configuration**

DHCP Server Name

LAN IP Address

Subnet Mask

IP Pool  
Starting Address:   
Ending Address:

Lease Time  seconds

Domain Name

Primary DNS

Secondary DNS

Primary WINS

Secondary WINS

Gateway

Server ☐ Enable

### DHCP Server

Choose DHCP Server to Enable. If you enable the DHCP Server function, this gateway will assign IP address to LAN computers or devices through DHCP protocol. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.

### LAN IP Address

Specify the local IP address of the enabled DHCP Server. It's the LAN IP address of this gateway for DHCP-1 server. Normally, this IP address will be also the default gateway of local computers and devices.

## Subnet Mask

Select the subnet mask for the specific DHCP-n server. Subnet Mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0/24, and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.

## IP Pool Starting/Ending Address

Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool. Please note the number of IP address in this IP pool must less than the maximum number of subnet network that according to the subnet mask you set.

## Lease Time

DHCP lease time to the DHCP client.

## Domain Name

Optional, this information will be passed to the clients.

## Primary DNS/Secondary DNS

Optional. This feature allows you to assign DNS Servers.

## Primary WINS/Secondary WINS

Optional. This feature allows you to assign WINS Servers.

## Gateway

Optional. Gateway address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your local computer when DHCP server offers IP address. For an example, this gateway will assign IP address to local computers, but local computers will go to Internet through another gateway.

### 1.2.2.3 Fixed Mapping

Press “Fixed Mapping ...” button at the bottom of the DHCP server list page and you can specify a certain IP address for designated local device (MAC address) by manual, so that the DHCP Server will reserve the special IPs for designated devices. For internal servers, you can use this feature to ensure each of them receives same IP address all the time.

Fixed Mapping

DHCP clients

-- select one --

Copy to

ID

--

[ Help ]

ID	MAC Address	IP Address	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

<<Previous

Next>>

Save

Undo

Back



## 1.2.3 VLAN

This section provides a brief description of VLANs and explains how to create and modify virtual LANs which are more commonly known as VLANs. A VLAN is a logical network under a certain switch or router device to group lots of client hosts with a specific VLAN ID. This device supports both Port-based VLAN and Tag-based VLAN. In Port-based VLAN, all client hosts belong to the same group by transferring data via some physical ports that are tagged with same VLAN ID in the device. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN. However, in Tag-based VLAN, all packets with same VLAN ID will be treated as the same group of them and own same access property and QoS property. It is especially useful when individuals of a VLAN group are located at different location.

The VLAN function allows you to divide local network into different “virtual LANs”. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV) to work properly. In some cases, SMB departments are separated and located at any floor of building. All client hosts in same department should own common access property and QoS property. You can select either one operation mode, port-based VLAN or tag-based VLAN, and then configure according to your network configuration.

Ethernet LAN VLAN Dynamic DNS

Configuration [ Help ]

VLAN Type Port-based ▼

**Port-based VLAN List**

Port	NAT/Bridge	VLAN ID	Tx TAG	DHCP Server	Available WAN	WAN VID	Action
Port1	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
Port2	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
Port3	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
Port4	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
VAP1	NAT	2	X	DHCP 2/Disable 192.168.10.0/24	X	0	<a href="#">Edit</a>
VAP2	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
VAP3	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
VAP4	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
VAP5	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
VAP6	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
VAP7	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>
VAP8	NAT	1	X	DHCP 1/Disable 192.168.0.0/24	X	0	<a href="#">Edit</a>

**Port-based VLAN Summary**

VLAN IDs	Members	NAT/Bridge	DHCP Server	Bridged WAN	Tx Tag
1	Port1, Port2, Port3, Port4, VAP-2, VAP-3, VAP-4, VAP-5, VAP-6, VAP-7, VAP-8	NAT	DHCP 1	X	No
2	VAP-1	NAT	DHCP 2	X	No

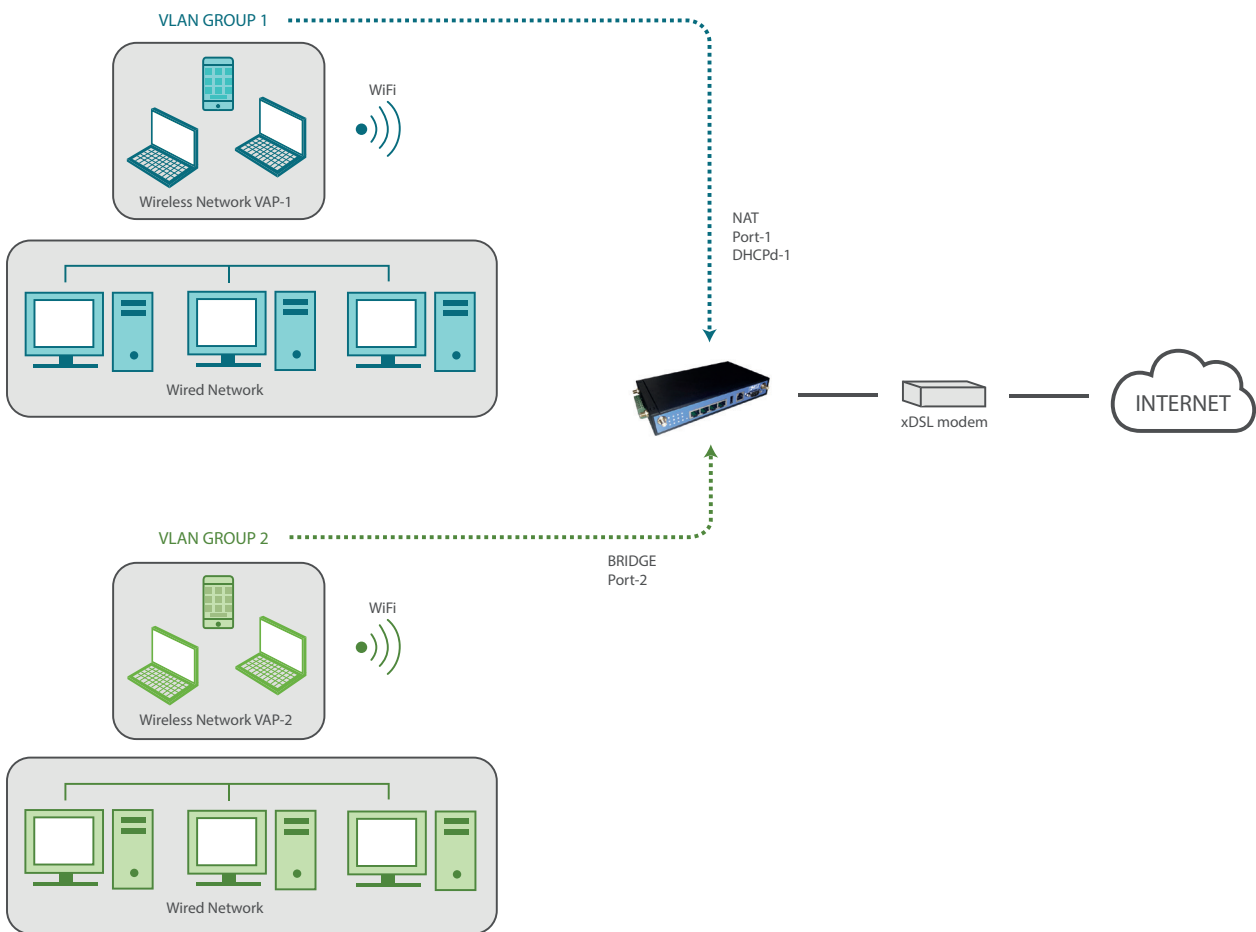
[Save](#) [VLAN Routing Group](#)

### 1.2.3.1 VLAN Scenarios

There are some common VLAN scenarios as follows:

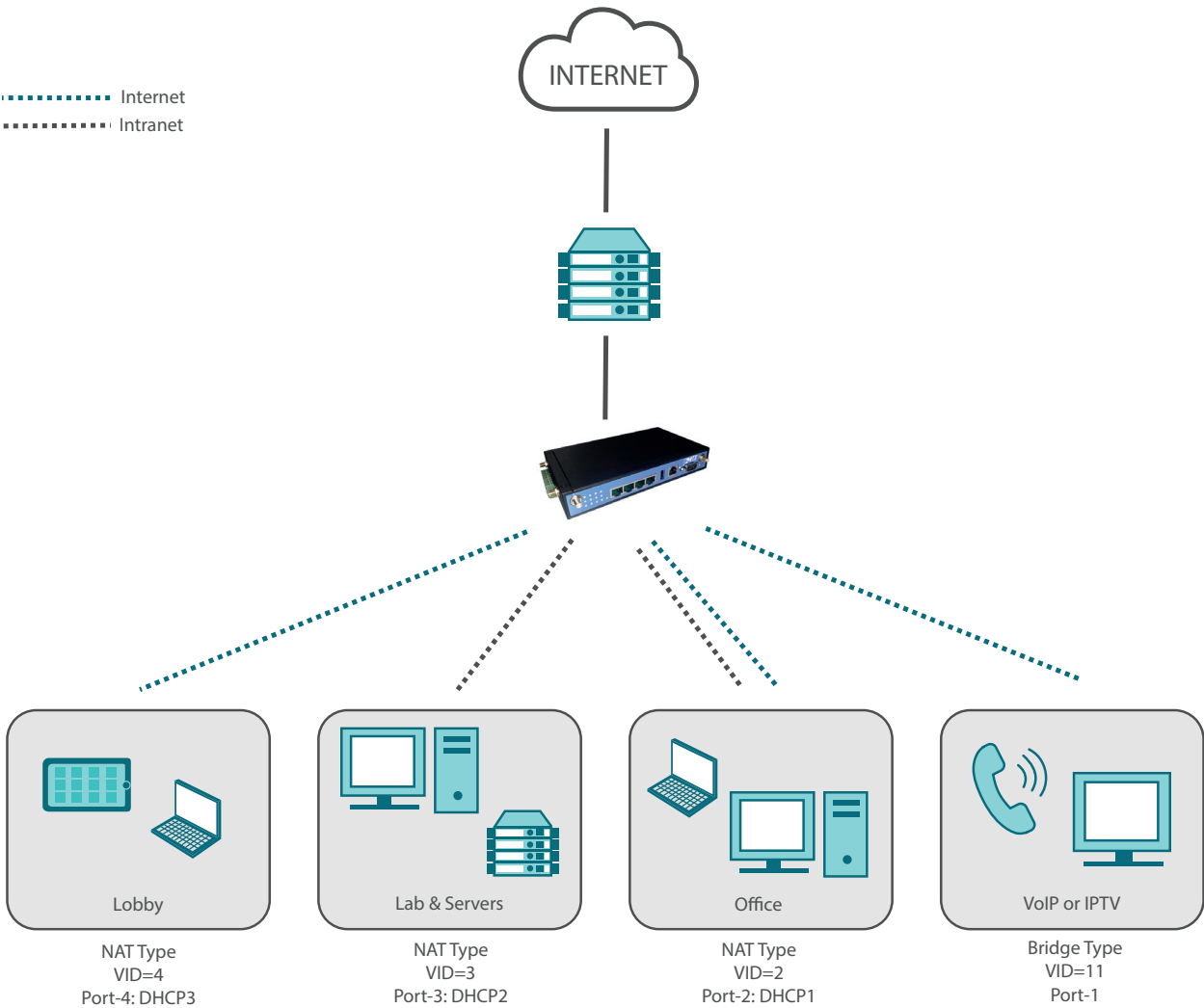
#### Port-Based VLAN Tagging for Differentiated Services

Port-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together for differentiated services like Internet surfing, multimedia enjoyment, VoIP talking, and so on. Two operation modes, NAT and Bridge, can be applied to each VLAN group. One DHCP server is allocated for an NAT VLAN group to let group host member get its IP address. Thus, each host can surf Internet via the NAT mechanism of business access gateway. At bridge mode, Intranet packet flow was delivered out WAN trunk port with VLAN tag to upper link for different services.



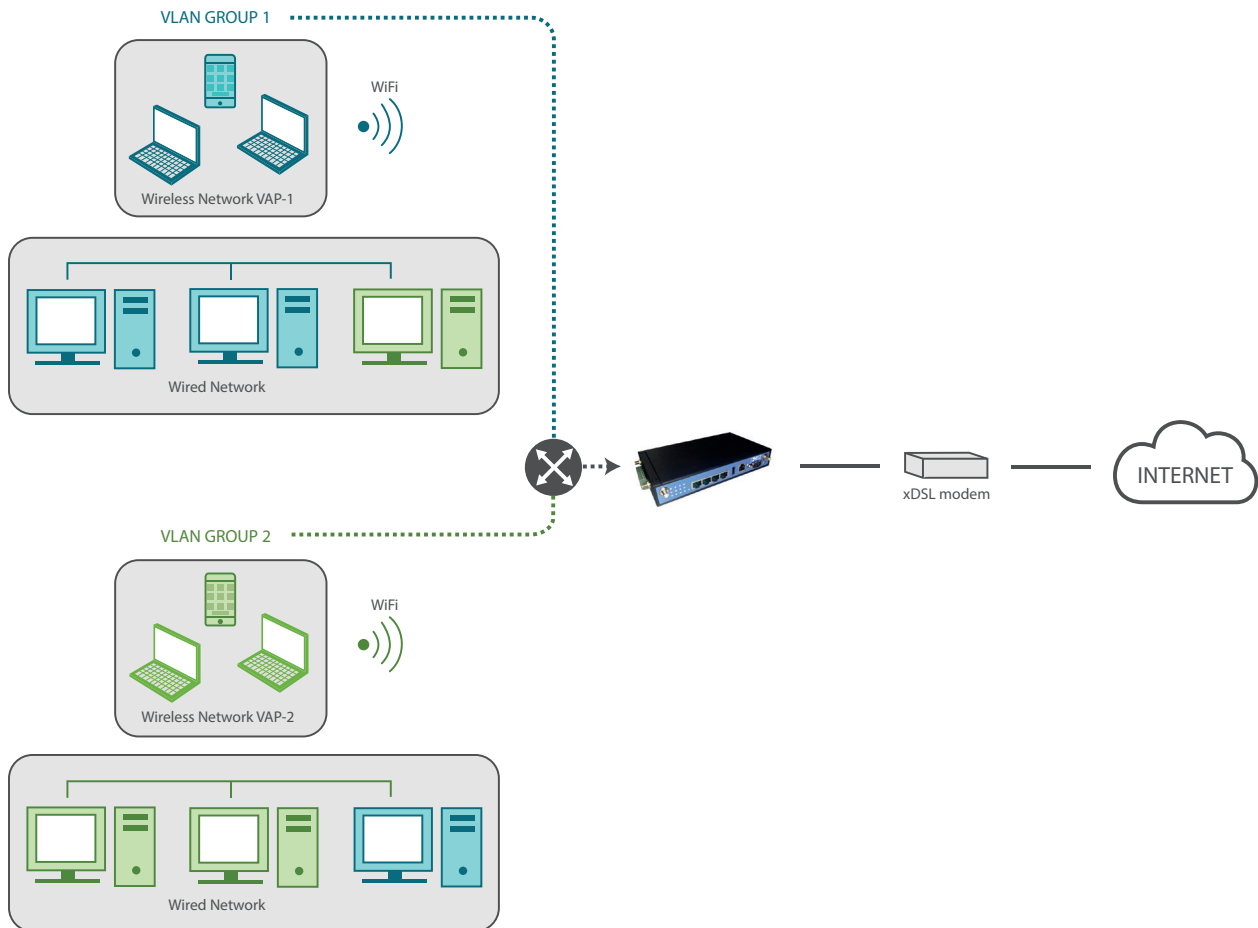
A port-based VLAN is a group of ports on an Ethernet or Virtual APs of Wired or Wireless Gateway that form a logical Ethernet segment. Following is an example. In SMB or a company, administrator schemes out 4 segments, Lobby, Lab & Servers, Office and VoIP & IPTV. In a Wireless Gateway, administrator can configure Lobby segment with VLAN ID 4. The VLAN group includes Port-4 and VAP-8 (SSID: Guest) with NAT mode and DHCP-3 server equipped. He also configure Lab & Servers segment with VLAN ID 3. The VLAN group includes Port-3 with NAT mode and DHCP-2 server equipped. However, he configure Office segment with VLAN ID 2. The VLAN group includes Port-2 and VAP-1 (SSID: Staff) with NAT mode and DHCP-1 server equipped. At last, administrator also configure VoIP & IPTV segment with VLAN ID 11. The

VLAN group includes Port-1 with bridge mode to WAN interface as shown at following diagram.

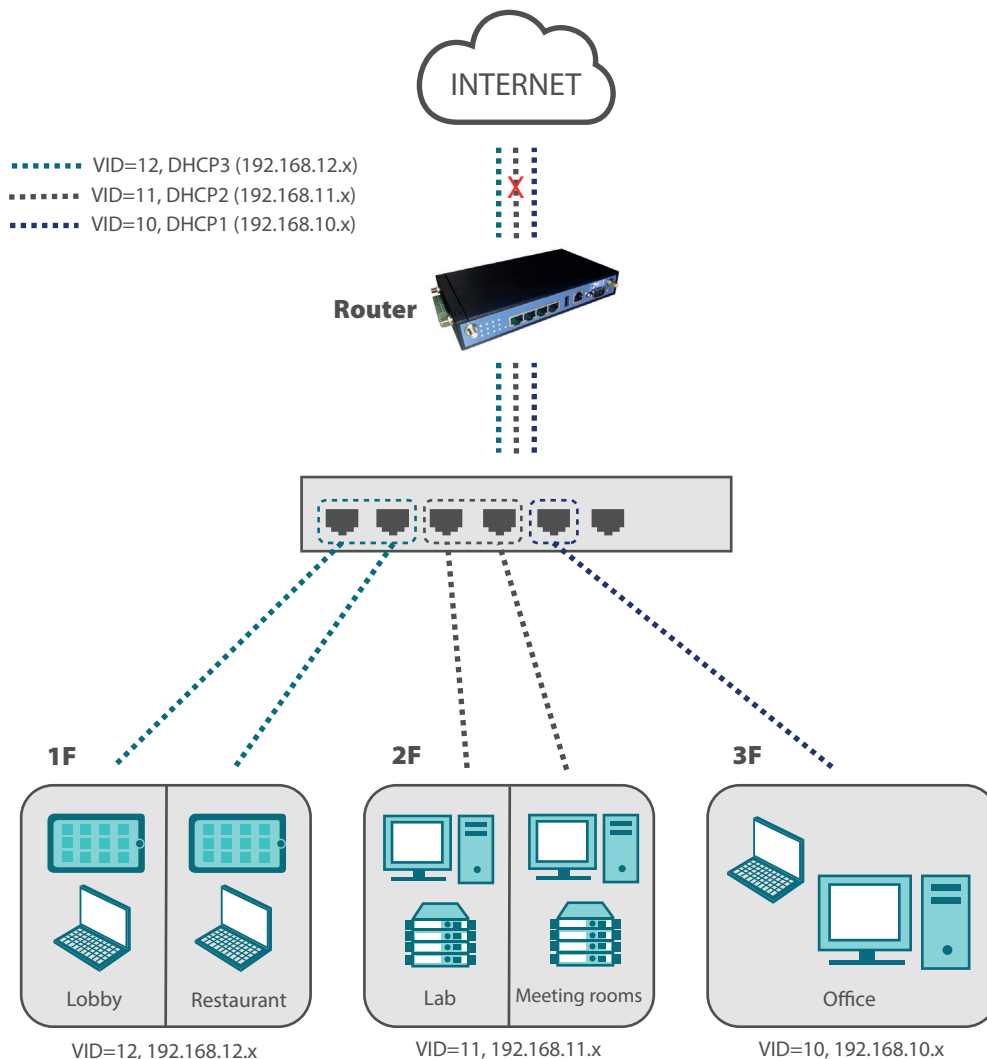


## Tag-based VLAN Tagging for Location-free Departments

Tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together with different VLAN tags for deploying department subnets in Intranet. All packet flows can carry with different VLAN tags even at the same physical port for Intranet. These flows can be directed to different destination because they have differentiated tags. The approach is very useful to group some hosts in different geographic location to be a same department.



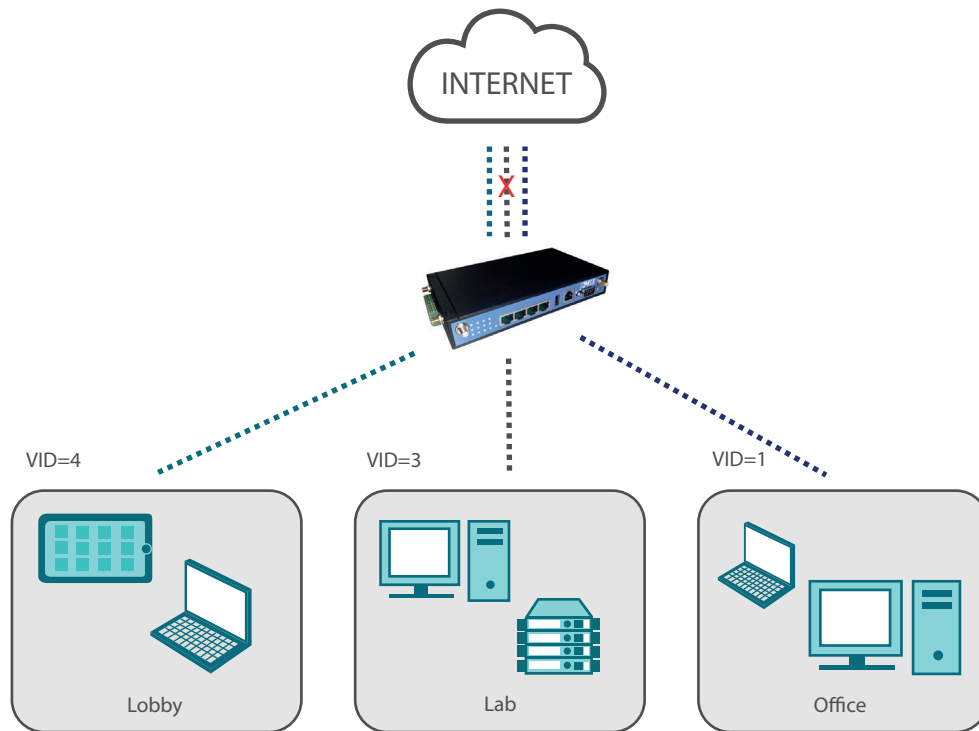
Tag-based VLAN is also called a VLAN Trunk. The VLAN Trunk collects all packet flows with different VLAN IDs from Router device and delivers them in the Intranet. VLAN membership in a tagged VLAN is determined by VLAN ID information within the packet frames that are received on a port. Administrator can further use a VLAN switch to separate the VLAN trunk to different groups based on VLAN ID. Following is an example. In SMB or a company, administrator schemes out 3 segments, Lobby & Restaurant, Lab & Meeting Rooms and Office. In a Security VPN Gateway, administrator can configure Lobby & Restaurant segment with VLAN ID 12. The VLAN group is equipped with DHCP-3 server to construct a 192.168.12.x subnet. He also configure Lab & Meeting Rooms segment with VLAN ID 11. The VLAN group is equipped with DHCP-2 server to construct a 192.168.11.x subnet for Intranet only. That is, any client host in VLAN 11 group can't access the Internet. However, he configure Office segment with VLAN ID 10. The VLAN group is equipped with DHCP-1 server to construct a 192.168.10.x subnet. In this example, VLAN 10 and 12 groups can access the Internet as following diagram.



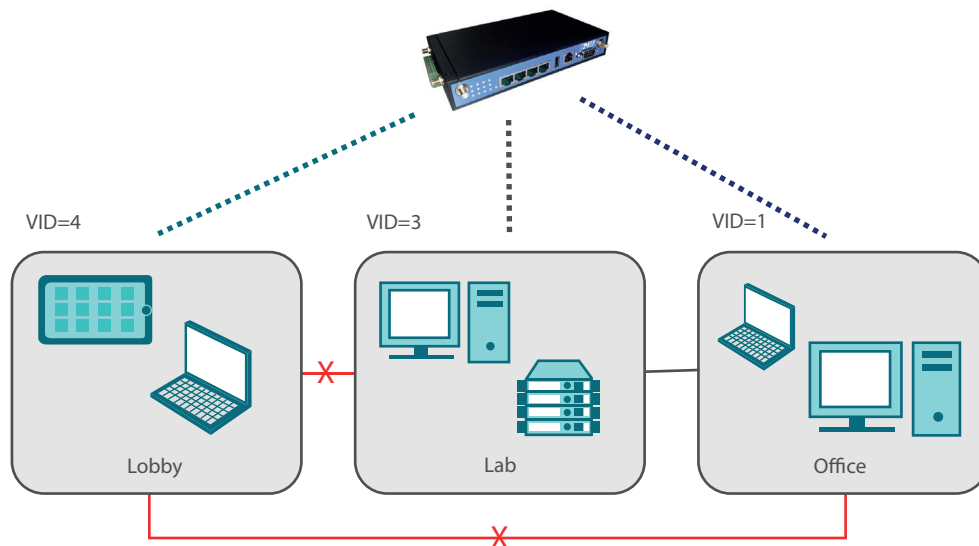
## VLAN Group Access Control

Administrator can specify the Internet access right for all VLAN groups. He also can configure which VLAN groups can communicate each other.

1. VLAN Group Internet Access: administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 1 and 4 can access Internet but the one with VID is 3 can't. That is, visitors in Lobby and staffs in office can access Internet. But ones in Lab can't since security issue. Servers in Lab serve only for trusted staffs or are accessed in secure tunnels.



2. Inter VLAN Group Routing: in Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair has not the transitive property. That is, A can communicate with B, and B can communicate with C, that doesn't mean A can communicate with C. An example is shown at following diagram. VLAN groups of VID is 1 and 3 can access each other but the ones between VID 3 and VID 4 and between VID 1 and VID 4 can't.



### 1.2.3.2 Port-Based VLAN

A port-based VLAN is a group of ports on an Ethernet switch or router that form a logical Ethernet segment. There are four LAN ports and up to eight virtual APs in this device, so you can have various VLAN configurations to organization the available LAN ports and virtual APs if required.

By default, all the 4 LAN ports and 8 virtual APs belong to one VLAN, and this VLAN is a NAT type network, all the local device IP addresses are allocated by DHCP server 1. If you want to divide them into different VLANs, click on the “Edit” button related to each port.

#### Type

Select “NAT” or “Bridge” to identify if the packets are directly bridged to the WAN port or processed by NAT mechanism.

#### LAN VID

Specify a VLAN identifier for this port. The ports with the same VID are in the same VLAN group.

#### Tx TAG

If ISP requests a “VLAN Tag” with your outgoing data, please check the checkbox of “Tx TAG.”

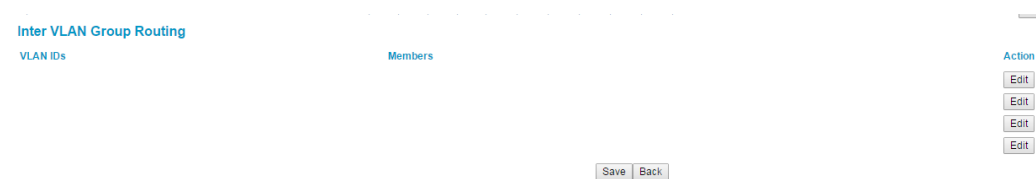
## DHCP Server

Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.

## WAN VID

The VLAN Tag ID that come from the ISP service. For NAT type VLAN, no WAN VLAN tag is allowed and the value is forced to “0”; For Bridge type VLAN, You have to specify the VLAN Tag value that is provided by your ISP.

## VLAN Routing Group



Above configuration example supports 3 access policies. The first one is Internet Access Policy that includes Port-1, Port-2, VAP-1 ~ VAP-4. All client hosts via these interfaces can access the Internet. The second policy is Intranet access Policy that includes Port-3 and VAP-5~ VAP-8. All client hosts via these interfaces can't access the Internet. But the Ethernet client hosts of VLAN 1 and 2 groups can communicate each other. About the configuration of inter-VAP routing, please refer to Basic Network >> WiFi section. The last one policy is the Bridge to WAN Policy that includes only Port-4.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.



### 1.2.3.3 Tag-Based VLAN

The second type of VLAN is the tag-based VLAN. VLAN membership in a tagged VLAN is determined by VLAN information within the packet frames that are received on a port. This differs from a port-based VLAN, where the port VIDs assigned to the ports determine VLAN membership.

When the device receives a frame with a VLAN tag, referred to as a tagged frame, the device forwards the frame only to those ports that share the same VID.

By default, all the LAN ports and virtual APs belong to one VLAN, and this VLAN ID is forced to “1”. It is a special tag based VLAN for device to operated, there is no tag required for this default VLAN ID.

**Ethernet LAN** **VLAN** **Dynamic DNS**

**Configuration** [ Help ]

VLAN Type Tag-based ▼

**Tag-based VLAN List** Add Delete

VLAN ID	Internet	Port	VAP	DHCP Server	Actions
None	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8	DHCP 1	<span>Edit</span>

Previous Next

**Tag-based VLAN Summary**

Port	VLAN IDs
Port1	
Port2	
Port3	
Port4	

Apply

If you want to configure your own tag-based VLANs, click on the “Edit” checkbox on a new VLAN ID row.

#### VLAN ID

Specify a VLAN tag for this VLAN group. The ports with the same VID are in the same VLAN group.

#### Internet

Specify whether this VLAN group can access Internet or not. If it is checked, all the packet will be un-tagged before it is forward to Internet, and all the packets from Internet will be tagged with the VLAN ID before it is forward to the destination belongs to this configuring VLAN group in the Intranet.

#### Port-1~Port-4, VAP-1~VAP-8

Specify whether they belong to the VLAN group or not. You just have to check the boxes for dedicated ports.

## DHCP Server

Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

## 1.3 WiFi Setup

The gateway supports 2.4GHz 802.11n 2Tx2R MIMO WiFi, and also can be back compatible to 802.11b/g clients. WiFi settings allow you to set the wireless LAN configuration items. When the wireless configuration is done, your WiFi LAN is ready to support your local WiFi devices such as your laptop PC, smart phone, tablet, wireless printer and some portable wireless devices.

Configuration

Wireless Client List

Advanced Configuration

Captive Portal

External Servers

Basic Configuration

[ Help ]

Operation Band

2.4G Single Band

WPS

2.4G WPS Setup

2.4G WiFi Configuration

WiFi Module

☒ Enable

WiFi Operation Mode

AP Router Mode

Green AP

☐ Enable

Multiple AP Names

VAP 1

☒ Enable

Max.STA :

☐ Enable

Time Schedule

(0) Always

Network ID (SSID) & Broadcast

Portal cautivo

Broadcast

☒ Enable

WLAN Partition

☒ Enable

Channel

Auto

WiFi System

802.11b/g/n Mixed

Authentication

Auto

802.1x

☐ Enable

Encryption

None

Save

Undo

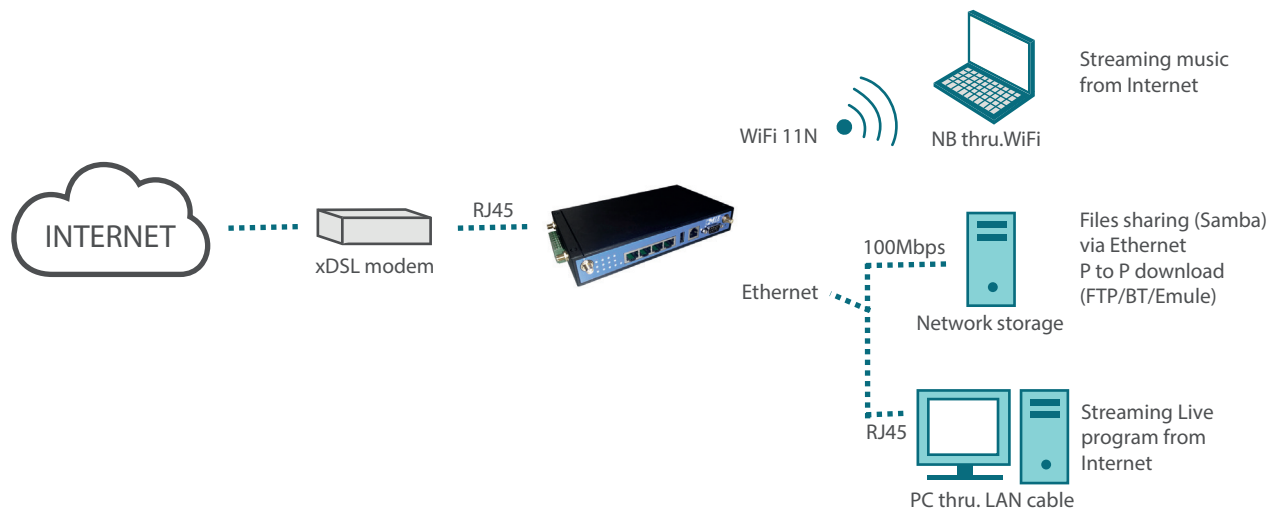
### 1.3.1 WiFi Configuration

This device is equipped with IEEE802.11b/g/n 2Tx2R wireless radio, you have to configure 2.4G Hz operation band's wireless settings and then activate your WLAN.

There are several wireless operation modes provided by this device. They are: “AP Router Mode”, “WDS Hybrid Mode”, and “WDS Only Mode”. You can choose the expected mode from the wireless operation mode list.

### 1.3.1.1 AP Router Mode

This mode allows you to get your wired and wireless devices connected with NAT.



In this mode, this gateway is working as a WiFi AP, but also a WiFi hotspot. It means local WiFi clients can associate to it, and go to Internet. With its NAT mechanism, all of wireless clients don't need to get public IP addresses from ISP.

#### Basic Configuration

[\[ Help \]](#)

Operation Band

2.4G Single Band ▼

WPS

2.4G WPS Setup

#### Operation Band

Select the WiFi operation band that you want to configure. But the device supports only 2.4G single WiFi band.

#### WPS

Click on the button to setup WPS.

## 2.4G WiFi Configuration

WiFi Module	<input checked="" type="checkbox"/> Enable
WiFi Operation Mode	AP Router Mode ▼
Green AP	<input type="checkbox"/> Enable
Multiple AP Names	VAP 1 ▼ <input checked="" type="checkbox"/> Enable Max.STA: <input type="checkbox"/> Enable
Time Schedule	(0) Always ▼
Network ID (SSID) & Broadcast	Portal cautivo Broadcast <input checked="" type="checkbox"/> Enable
WLAN Partition	<input checked="" type="checkbox"/> Enable
Channel	Auto ▼
WiFi System	802.11b/g/n Mixed ▼
Authentication	Auto ▼ 802.1x <input type="checkbox"/> Enable
Encryption	None ▼

Save Undo

### Wireless Module

Enable the wireless function.

### Wireless Operation Mode

Choose “AP Router Mode” from the drop list.

### Green AP

Enable the Green AP function to reduce the power consumption when there is no wireless traffic. By default, it is disabled.

### Multiple AP Names

This device supports up to 8 SSIDs for you to manage your wireless network. You can select VAP-1 ~ VAP-8 and configure each wireless network if it is required.

### Time Schedule

The wireless radio can be turn on according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled. If you want to add a new schedule rule, please go to System -> Scheduling menu.

### Network ID (SSID)

Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)

### SSID Broadcast

The router will broadcast beacons that have some information, including SSID so that wireless clients

can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can’t find the device from beacons.

## WLAN Partition

You can check the WLAN Partition function to separate the wireless clients. The wireless clients can’t communicate each other, but they can access the internet and other Ethernet LAN devices.

## Channel

The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection. It’s recommended to choose a channel that is not used in your environment to reduce radio interference.

## WiFi System

This gateway supports 2.4GHz 802.11b/g/n modes, so you can choose adequate WiFi system from the option list of “802.11b Only”, “802.11g Only”, “802.11n Only”, “802.11b/g Mixed”, “802.11g/n Mixed” and “802.11b/g/n Mixed” according to your requirement. The factory default setting is “802.11b/g/n Mixed.”

## Authentication & Encryption

You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA/WPA2.

1. Open: open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router (WiFi gateway) containing a success or failure message. An example of when a failure may occur is if the client’s MAC address is explicitly excluded in the AP/router configuration. In this mode you can enable 802.1x feature if you have another RADIUS server for user authentication. You need to input IP address, port and shared key of RADIUS server here.

Authentication	Open ▼	802.1x <input checked="" type="checkbox"/> Enable
RADIUS Server	RADIUS Server IP	0.0.0.0
	RADIUS Server Port	1812
	RADIUS Shared Key	

In this mode, you can only choose “None” or “WEP” in the encryption field.

2. Shared: shared key authentication relies on the fact that both stations taking part in the authentication process have the same “shared” key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

3. Auto: the gateway will select appropriate authentication method according to WiFi client’s request

automatically.

4. WPA-PSK: select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don’t need additional RADIUS server for user authentication.

5. WPA: select Encryption mode and enter RADIUS Server related information. You have to specify the IP address and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”.

6. WPA2-PSK: select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don’t need additional RADIUS server for user authentication.

7. WPA2: select Encryption mode and enter RADIUS Server related information. You have to specify the IP address and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”.

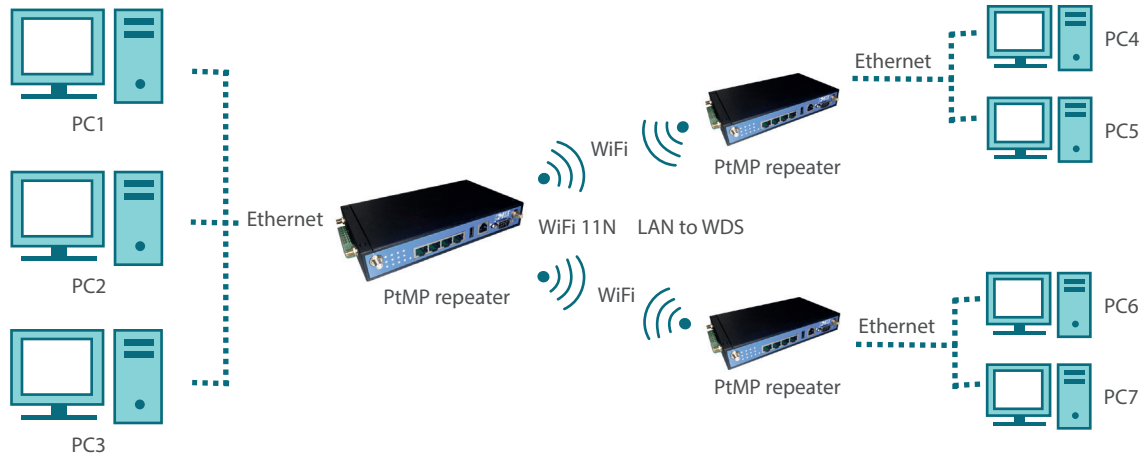
8. WPA-PSK/WPA2-PSK: if some of wireless clients can only support WPA-PSK, but most of them can support WPA2-PSK. You can choose this option to support both of them. Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. In this mode, you don’t need additional RADIUS server for user authentication.

9. WPA/WPA2: if some of wireless clients can only support WPA, but most of them can support WPA2. You can choose this option to support both of them. Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

### 1.3.1.2 WDS Only Mode

While acting as a wireless bridge, Wireless Repeater 1 and Wireless Repeater 2 can communicate with each other through wireless interface (with WDS). Thus all stations can communicate each other.



### 2.4G WiFi Configuration

WiFi Module	<input checked="" type="checkbox"/> Enable
WiFi Operation Mode	WDS Only Mode ▼
Green AP	<input type="checkbox"/> Enable
Channel	Auto ▼
Authentication	Auto ▼
Encryption	None ▼
Scan Remote AP's MAC List	Scan
Remote AP MAC 1	<input type="text"/>
Remote AP MAC 2	<input type="text"/>
Remote AP MAC 3	<input type="text"/>
Remote AP MAC 4	<input type="text"/>

### Wireless Module

Enable the wireless function.

### Wireless Operation Mode

Choose “WDS Only Mode” from the drop list.

### Lazy Mode

This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers' MAC address filled.

## Green AP

Enable the Green AP function to reduce the power consumption when there are no wireless traffics.

## Channel

The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.

## Authentication & Encryption

You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK and WPA2-PSK.

1. Open: open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router (WiFi gateway) containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration. In this mode, you can only choose "None" or "WEP" in the encryption field.
2. Shared: shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.
3. Auto: the gateway will select appropriate authentication method according to WiFi client's request automatically.
4. WPA-PSK: select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are "TKIP", "AES", or "TKIP/AES". In this mode, you don't need additional RADIUS server for user authentication.
5. WPA2-PSK: select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are "TKIP", "AES", or "TKIP/AES". In this mode, you don't need additional RADIUS server for user authentication.

## Scan Remote AP's MAC List

If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one. Click on the "Scan" button to get the available AP's MAC list automatically and select the expected item and copy its MAC address to the Remote AP MAC 1~4 one by one.



Scan Remote AP's MAC List Scan

Remote AP MAC 1  ☒ Copy MAC to Here

Remote AP MAC 2  ☐ Copy MAC to Here

Remote AP MAC 3  ☐ Copy MAC to Here

Remote AP MAC 4  ☐ Copy MAC to Here

Save Undo

### Wireless AP List

SSID	Channel	Quality	Authentication	Encryption	MAC Address	Select
PLANTA_2	2	18%	WPA-PSK	AES	00:17:9a:b1:7b:a8	<span>Copy to</span>

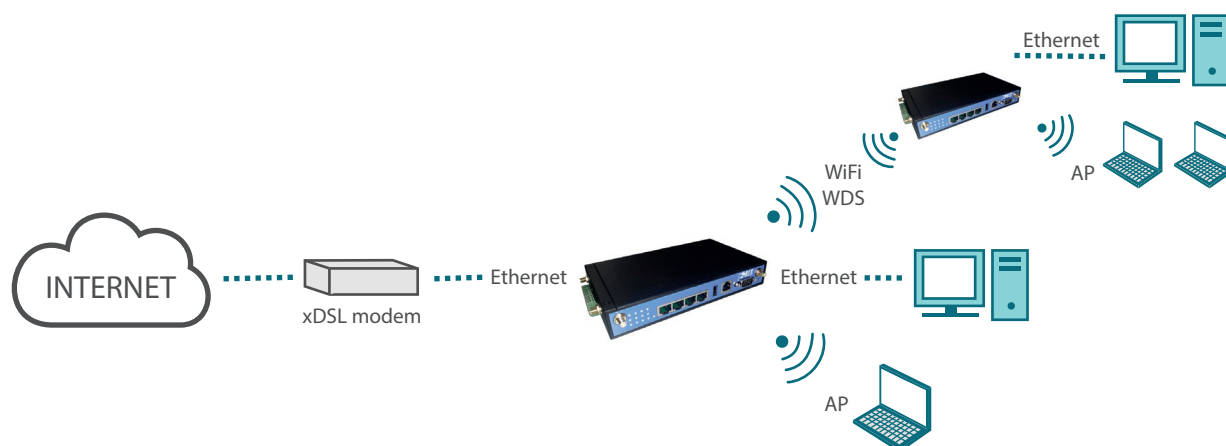
### Remote AP MAC 1~Remote AP MAC 4

If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

### 1.3.1.3 WDS Hybrid Mode

WDS (Wireless Distributed System) Hybrid function let this access point acts as a wireless LAN access point and a repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools, etc.



## 2.4G WiFi Configuration

WiFi Module	<input checked="" type="checkbox"/> Enable
WiFi Operation Mode	WDS Hybrid Mode ▼
Lazy Mode	<input checked="" type="checkbox"/> Enable
Green AP	<input type="checkbox"/> Enable
Multiple AP Names	VAP 1 ▼ <input checked="" type="checkbox"/> Enable Max.STA: <input type="checkbox"/> Enable
Time Schedule	(0) Always ▼
Network ID (SSID) & Broadcast	Portal cautivo <input type="text"/> Broadcast <input checked="" type="checkbox"/> Enable
WLAN Partition	<input checked="" type="checkbox"/> Enable
Channel	Auto ▼
WiFi System	802.11b/g/n Mixed ▼
Authentication	Auto ▼ 802.1x <input type="checkbox"/> Enable
Encryption	None ▼

Save Undo

### Wireless Module

Enable the wireless function.

### Wireless Operation Mode

Choose “WDS Hybrid Mode” from the drop list.

### Lazy Mode

This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy Mode simultaneously; at least there must be one AP with all the WDS peers' MAC address filled.

### Green AP

Enable the Green AP function to reduce the power consumption when there is no wireless traffic.

### Multiple AP Names

This device supports up to 8 SSIDs for you to manage your wireless network. You can select VAP-1 ~ VAP-8 and configure each wireless network if it is required.

### Time Schedule

The wireless radio can be turn on according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled. If you want to add a new schedule rule, please go to System -> Scheduling menu.

### Network ID (SSID)

Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”).

### SSID Broadcast

The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can’t find the device from beacons

### Channel

The radio channel number. The permissible channels depend on the Regulatory Domain. This channel number needs to be same as the channel number of peer AP.

### Authentication & Encryption

You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK and WPA2-PSK.

1. Open: open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router (WiFi gateway) containing a success or failure message. An example of when a failure may occur is if the client’s MAC address is explicitly excluded in the AP/router configuration.

In this mode, you can only choose “None” or “WEP” in the encryption field.

2. Shared: shared key authentication relies on the fact that both stations taking part in the authentication process have the same “shared” key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

3. Auto: the gateway will select appropriate authentication method according to WiFi client’s request automatically.

4. WPA-PSK: select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don’t need additional RADIUS server for user authentication.

5. WPA2-PSK: select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don’t need additional RADIUS server for user authentication.

#### 1.3.1.4 WPS Setup

Once you finished the wireless settings for the following sub-sections, you can configure and enable the WPS (Wi-Fi Protection Setup) easy setup feature for your wireless network by clicking on the “2.4G WPS Setup” button.

Configuration
Wireless Client List
Advanced Configuration
Captive Portal
External Servers

### 2.4G Wi-Fi Protected Setup [ Help ]

WPS
☒ Enable

Configuration Status
CONFIGURED
Release

Configuration Mode
Registrar ▼

Allowed STA PIN Code

WPS Trigger
WPS Trigger

WPS Status
NOUSED

Save
Undo
Back

**WPS** (only one wireless client is allowed to proceeding WPS connecion at the same time)

You can enable this function by checking “Enable” box. WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.

### Configuration Status

This configuration status will be “CONFIGURED” or “UNCONFIGURED”. “CONFIGURED” means WPS connection is following WiFi settings on this gateway. If it’s released to “UNCONFIGURED”, the WPS connection will generate a new profile.

### Configuration Mode

Select your Configuration Mode from “Registrar” or “Enrollee”. In most cases, for an AP router or AP, it should be in “Registrar” mode, so that other wireless clients in “Enrollee” mode can connect to the discovered “Registrar”. Briefly specking, “Enrollee” is the initiator of WPS connection.

#### Registrar Mode

Configuration Mode
Registrar ▼

Allowed STA PIN Code

WPS Trigger
WPS Trigger

#### Enrollee Mode

Configuration Mode
Enrollee ▼

AP PIN Code & New Generate
22209122
New Generate

### Push-button WPS Trigger [Registrar Mode]

Press this button to simulate you have push WPS button and let wireless clients to connect to this gateway in WPS PBC mode.

### Allowed STA PIN Code [Registrar Mode]

Fill the PIN code of device, so all STA clients can operate the WPS process to the device with the certificated code.

### **AP PIN Code & New Generate [Enrollee Mode]**

This PIN number is required for WiFi client during WPS connection. You can press “New Generate” to get a new AP PIN.

### **WPS status**

According to your setting and activity, the status will show “IDLE”, “STARTPROCESS”, or “NOT USED”. The status is “IDLE” by default. If you want to start a WPS connection, you need to push “Trigger” button to change its status to “STARTPROCESS”. Only one wireless client is allowed for each WPS connection.

If you want to start a WPS connection, you can click on the “Trigger” button of this device to change the WPS status to “STARTPROCESS” and then initiate the WPS process on other wireless client devices in two minutes to make the client device connected to the activated WLAN.

### 1.3.2 Wireless Client List

In “Wireless Client List” page, the list of connected wireless clients will be shown consequently. You can choose to see “All” of connected wireless clients, or you can indicate which virtual AP (SSID) you want to browse. You can check wireless clients of VAP-1~VAP-8 individually.

Configuration

Wireless Client List

Advanced Configuration

Captive Portal

External Servers

Target WiFi

[ Help ]

Operation Band

2.4G ▾

Multiple AP Names

All ▾

Client List

Address

Host Name

MAC Address

Mode

Rate

Signal

Interface

Refresh

### 1.3.3 Advanced Configuration

This device provides advanced wireless configuration for professional user to optimize the wireless performance under the specific installation environment.

Configuration

Wireless Client List

Advanced Configuration

Captive Portal

External Servers

Target WiFi

[ Help ]

Operation Band

2.4G ▾

Advanced Configuration

Regulatory Domain

(1-13)

Beacon Interval

100

Range: (1~1000 msec)

DTIM Interval

3

Range: (1~255)

RTS Threshold

2347

Range: (1~2347)

Fragmentation

2346

Range: (256~2346)

WMM

☒ Enable

Short GI

400ns ▾

TX Rate

Best ▾

RF Bandwidth

Auto ▾

Transmit Power

100% ▾

Save

Undo

### Operation Band

Select the WiFi operation band that you want to configure. But the device supports only 2.4G single WiFi band.

## Regulatory Domain

Indicate number of Wi-Fi channel. It depends on regional government regulations.

## Beacon interval

Beacons are broadcast packets that are sent by a wireless AP/router. The main purpose of beacon packet is let wireless clients know this AP (SSID) when doing wireless network scan.

## DTIM interval

A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value.

## RTS Threshold

If an excessive number of wireless packet collision occurred, the wireless performance will be affected. It can be improved by adjusting the RTS/CTS (Request to Send/Clear to Send) threshold value.

## Fragmentation

Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage.

## WMM Capable

WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

## Short GI

Time setting of Guard Interval between two Wi-Fi packets. Decrease this time interval will increase Wi-Fi data throughput. But it may cause some side-effects when the quality of Wi-Fi signal is not good. 800ns is the standard time setting of GI.

## TX Rate

For WiFi transmit rate, you can choose “Best” for auto-adjustment according to WiFi signal quality in your environment, or you can fix it in certain TX rate. Please note the WiFi connection may be dropped if you fix at a higher data rate but in a noisy (poor RF signal quality) environment. Besides, there is only one “Best” option if following “RF Bandwidth” parameter is set to “Auto”.

## RF Bandwidth

Select Auto, HT20 or HT40 to define the RF bandwidth for a channel. By default, it is Auto for the device.

## Transmit Power

Normally the wireless transmission power operates at 100% out power specification of this device. You can lower down the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

### 1.3.4 Captive Portal

Configuration

Wireless Client List

Advanced Configuration

Captive Portal

External Servers

#### Captive Portal Configuration

Captive Portal

☒ Enable

WAN Interface

WAN-1

LAN Subnet

Authentication Server

External RADIUS Server

Radius

UAM Server

☒ Enable

Select from External Server List:

hotspotsystem

Save

Refresh

The gateway supports the Captive Portal function, including external captive portal. For external captive portable, you must specify external RADIUS (Remote Authentication Dial In User Service) server and external UAM (Universal Access Method) server.

#### External Captive Portal

Before enabling external Captive Portal function, please go to System >> External Servers to define some external server objects, like RADIUS server and UAM server. Then configure Captive Portal function in this page to specific WAN Interface, select external Authentication Server and UAM Server from the pre-defined external server object list.

NOTE: All Internet Packets will forward to Captive Portal Web site of the gateway when enabled this feature. Please make sure that you had one account and password.

### 1.3.5 External Servers

This device supports six types of external server objects to be created. They are Email Server objects, Syslog Server objects, RADIUS Server objects, Active Directory Server objects, LDAP Server objects and UAM Server objects. These objects can be used in other applications of system, like system log emailing to email server or sending to syslog server in [System]-[System Related]-[System Status], captive portable function in [Applications]-[Captive Portable], SMS forwarding to email server or syslog server in [Applications]-[Mobile Applications]-[SMS], AP Management alerting system in [Applications]-[AP Management], and IO Management alerting handler in [Applications]-[IO Management]. Above usage examples depend on the provided functions of different product models.



Configuration
Wireless Client List
Advanced Configuration
Captive Portal
External Servers

External Server List
Add
Delete

ID	Server Name	Server IP/FQDN	Server Port	Server Type	Enable	Setting
1	hotspotsystem	www.hotspotsystem.com	3990	UAM Server	<input checked="" type="checkbox"/>	Edit <input type="checkbox"/> Select
2	Radius	radius.hotspotsystem.com	1812	RADIUS Server	<input checked="" type="checkbox"/>	Edit <input type="checkbox"/> Select

Refresh

### 1.3.5.1 External Server List

External Server List can show the list of all defined external server objects and their attributes in this window. You can add one new external server object by clicking on the “Add” command button. But also you can modify some existed external server objects by clicking corresponding “Edit” command buttons at the end of each object record in the External Server List. Besides, unnecessary objects can be removed by checking the “Select” box for those objects and then clicking on the “Delete” command button at the External Server List caption.

#### Add

Click on the button to add one external server object.

#### Delete

Click on the button to delete the external server objects that are specified in advance by checking on the “Select” box of those objects.

#### Edit

Click on the button to edit the external server object.

#### Select

Select the external server object to delete.

### 1.3.5.2 External Server Configuration

#### External Server Configuration

Server Name	<input type="text" value="hotspotsystem"/>
Server IP/FQDN	<input type="text" value="www.hotspotsystem.com"/>
Server Port	<input type="text" value="3990"/>
	<input type="text" value="UAM Server"/>
	Login URL: <input type="text" value="https://customer.hotspotsys"/>
Server Type	Shared Secret: <input type="text" value="Juntos11"/>
	NAS/Gateway ID: <input type="text" value="Danimatrix"/>
	Location ID: <input type="text" value="1"/>
	Location Name: <input type="text" value="Matrix"/>
Server	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/>	
<input type="button" value="Refresh"/>	

#### Server Name

Define the name of external server object.

#### Server IP/FQDN

Specify the IP address or domain name of external server.

#### Server Port

Specify the service port of external server.

#### Server Type

Select one server type from the option list of “Email Server”, “Syslog Server”, “RADIUS Server”, “Active Directory Server”, “LDAP Server” and “UAM Server”. Based on your selection, there are several parameters need to specify. When you select “Email Server” option for the Server Type, you must specify two more parameters, “User Name” and “Password”. When “Syslog Server”, no more parameter is required. When “RADIUS Server”, you can specify primary RADIUS server and secondary RADIUS server for redundancy. For each server, following parameters need to be specified: Shared Key, Authentication Protocol (CHAP or PAP), Session Timeout (1~60 Mins) and Idle Timeout (1~15 Mins). When “Active Directory” Server, you must specify one more parameter, “Domain”. When “LDAP” Server, one more parameter, Base Domain Name. When “NT Domains” Server, one more parameter: “Workgroup”. When “UAM” Server, following parameters must be provided: “Login URL”, “Shared Secret”, “NAS/Gateway ID”, “Location ID” and “Location Name”. Among them, Location Name is optional.

## Server

Check the “Enable” box to activate the external server object.

## 1.4 IPv6 Setup

The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 (Internet Protocol version 6) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. This gateway supports two types of IPv6 connection (6to4/6in4). Please ask your ISP of what type of IPv6 is supported before you proceed with IPv6 setup.

Configuration

**IPv6 Configuration** [Help]

IPv6 ☐ Enable

WAN Connection Type 6to4 ▼

**6to4 WAN Type Configuration**

6 to 4 Address

Primary DNS

Secondary DNS

MLD Snooping ☐ Enable

**LAN Configuration**

Global Address 2002:0:0::1

Link-local Address

**Address Auto-configuration**

Auto-configuration ☒ Enable

Auto-configuration Type Stateless ▼

Router Advertisement Lifetime 200 (seconds)

Save Undo

### 1.4.1 6 to 4

Configuration

**IPv6 Configuration**

IPv6 ☒ Enable

WAN Connection Type 6to4 ▼

When “6 to 4” is selected for the WAN Connection Type, you need to do the following settings:

#### 6to4 WAN Type Configuration

**6to4 WAN Type Configuration**

6 to 4 Address

Primary DNS

Secondary DNS

MLD Snooping ☒ Enable

1. 6 to 4 Address: you may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.

2. Primary/Secondary DNS: please enter IPv6 primary DNS address and secondary DNS address.
3. MLD Snooping: MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

## LAN Configuration

### LAN Configuration

Global Address 2002:0:0: :1  
Link-local Address

1. Global Address: please enter IPv6 global address for LAN interface.
2. Link-local Address: to show the IPv6 Link-local address of LAN interface.

## Address Auto-configuration

### Address Auto-configuration

Auto-configuration ☒ Enable  
Auto-configuration Type Stateless  
Router Advertisement Lifetime 200 (seconds)

1. Auto-configuration: disable or enable this auto configuration setting.
2. Auto-configuration type: you may set stateless or stateful (Dynamic IPv6).
3. Router Advertisement Lifetime: you can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements

## 1.4.2 6 in 4

When “6 in 4” is selected for the WAN Connection Type, you need to do the following settings:

### IPv6 Configuration

IPv6 ☒ Enable  
WAN Connection Type 6in4

## 6in4 WAN Type Configuration

## 6in4 WAN Type Configuration

Remote IPv4 Address	<input type="text"/>
Local IPv4 Address	0.0.0.0
Local IPv6 Address	<input type="text"/> /64
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
MLD Snooping	<input type="checkbox"/> Enable

1. Remote/Local IPv4 and IPv6 Address: you may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
2. DNS: please enter IPv6 primary DNS address and secondary DNS address.
3. MLD Snooping: MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

## LAN Configuration

### LAN Configuration

Global Address	<input type="text"/> /64
Link-local Address	

1. Global Address: please enter IPv6 global address for LAN interface.
2. Link-local Address: to show the IPv6 Link-local address of LAN interface.

## Address Auto-configuration

### Address Auto-configuration

Auto-configuration	<input checked="" type="checkbox"/> Enable
Auto-configuration Type	Stateless ▾
Router Advertisement Lifetime	<input type="text" value="200"/> (seconds)

1. Auto-configuration: disable or enable this auto configuration setting.
2. Auto-configuration Type: you may set stateless or stateful (Dynamic IPv6).
3. Router Advertisement Lifetime: you can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link

partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

## 1.5 NAT/DMZ

This part includes NAT related settings, such as NAT loopback, Virtual Server, Virtual Computer, Special AP, ALG, and DMZ.

The screenshot shows a configuration window with two tabs: 'NAT Loopback' and 'DMZ'. The 'NAT Loopback' tab is active, showing a table with columns: ID, Public Port, Server IP, Private Port, Protocol, Time Schedule, Enable, and Actions. A single entry is shown with ID 1, Public Port 25500, Server IP 192.168.0.70, Private Port 80, Protocol Both, Time Schedule (0) Always, and Enable checked. Below the table are buttons for 'Add' and 'Delete'. The 'DMZ' tab is also visible, showing fields for 'IP Address of DMZ Host' and 'DHCP Relay' (192.168.123.254), both with 'Enable' checkboxes. A 'Save' button is at the bottom right.

### 1.5.1 Configuration

#### NAT Loopback

NAT Loopback

☒ Enable

#### NAT Loopback

Allow you to access the WAN IP address from inside your local network. This is useful when you run a server inside your network. For an example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's WAN IP address. You don't need to change IP address of mail server no matter you are at local side or go out. This is useful when you run a server inside your network.

### 1.5.2 DMZ

#### DMZ

DMZ IP Address of DMZ Host:  ☐ Enable

Relay DHCP Relay:  ☐ Enable

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications. Otherwise, if specific application is blocked by NAT mechanism, you can indicate that LAN computer as a DMZ host to solve this problem.

#### IP Address of DMZ Host

Enter IP address of Server or Host.

## DHCP Relay

DHCP Relay Agent component relays DHCP messages between DHCP clients and DHCP servers on different IP networks. Because DHCP is a broadcast-based protocol, by default its packets do not pass through routers. If you need this feature in the environment, please enable it.

NOTE: This feature should be used only when needed.

## 1.6 Routing Setup

If you have more than one router and subnet, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing

Routing Information

Static Configuration

[ Help ]

Static Routing

☐ Enable

Static Routing Rule List

AddDelete

RIP Configuration

[ Help ]

RIP

Disable ▼

OSPF Configuration

OSPF

☐ Enable

Backbone Subnet

OSPF Area List

AddDelete

BGP Configuration

BGP

☐ Enable

Self ID

BGP Neighbor List

AddDelete

Save

Undo

### 1.6.1 Static Routing

For static routing, you can specify up to 32 routing rules. The routing rules allow you to determine which physical interface addresses are utilized for outgoing IP data grams. You can enter the destination IP address, Subnet Mask, Gateway, and Metric for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

Please click Add or Edit button to configure a static routing rule:

Routing

Routing Information

#### Static Routing Rule Configuration

Destination IP

Subnet Mask

Gateway IP

Interface

Auto ▾

Metric

Rule

☐ Enable

Save

Undo

Back

#### Destination IP

Enter the subnet network of routed destination.

#### Subnet Mask

Input your subnet mask. Subnet mask defines the range of IP address in destination network.

#### Gateway

The IP address of gateway that you want to route for this destination subnet network. The assigned gateway is required to be in the same subnet of LAN side or WAN side.

#### Metric

The router uses the value to determine the best possible route. It will go in the direction of the gateway with the lowest metric.

#### Rule

Check the Enable box to enable this static routing rule.



1.6.2 Routing Information

Routing

Routing Information

Routing Table

Destination IP	Gateway IP	Subnet Mask	Metric	Interface
37.12.154.128	0.0.0.0	255.255.255.252	0	WAN-1
192.168.0.0	0.0.0.0	255.255.255.0	0	LAN
192.168.10.0	0.0.0.0	255.255.255.0	0	tun0
192.168.10.0	0.0.0.0	255.255.255.0	0	LAN
169.254.0.0	0.0.0.0	255.255.0.0	0	LAN
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN
127.0.0.0	0.0.0.0	255.0.0.0	0	lo
0.0.0.0	37.12.154.130	0.0.0.0	0	WAN-1

Policy Routing Information

Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

Refresh

A routing table, or routing information base (RIB), is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it.

This page displays the routing table maintained by this device. It is generated according to your network configuration.

## ● 2. Advanced Network

This device also supports many advanced network features, such as Firewall, QoS & Bandwidth Management, VPN, Redundancy, System Management, Certificate and Serial Port Settings. You can finish those configurations in this section.

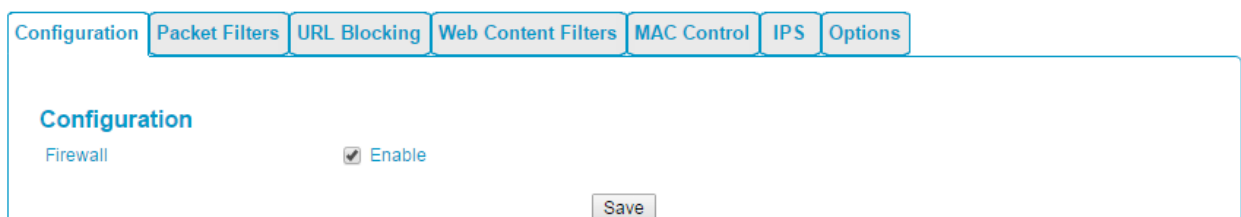


### 2.1 Firewall

The firewall functions include Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and some firewall options.

#### 2.1.1 Configuration

One Firewall Enable check box lets you activate all firewall functions that you want.



#### 2.1.2 Packet Filters

Packet Filters function can let you define both outbound filter and inbound filter rules by specifying the source IP and destination IP in a rule. It enables you to control what packets are allowed or blocked to pass the router. Outbound filters are applied to all outbound packets. However, inbound filters are applied to packets that destined to virtual servers or DMZ host/port only.

##### 2.1.2.1 Configuration

You can enable packet filter function here. And select one of the two filtering policies as follows. The first one is to define the black list. System will block the packets that match the active filter rules. However, the second one is the white list. System will allow the packets to pass the gateway, which match the active filter rules.

- Allow all to pass except those match the specified rules (black list)
- Deny all to pass except those match the specified rules (white list)

Configuration
Packet Filters
URL Blocking
Web Content Filters
MAC Control
IPS
Options

### Configuration

[ Help ]

Packet Filters
☒ Enable

Black List / White List
Allow all to pass except those match the following rules. ▼

Log Alert
☐ Enable

Besides, you also can enable the log alerting so that system will record packet blocking events when filter rules are fired. At the right upper corner of screen, one “[Help]” command let you see the on-line help message about Packet Filter function.

### 2.1.2.2 Packet Filter List

It is a list of all packet filter rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed packet filter rules by clicking corresponding “Edit” command buttons at the end of each filter rule in the Packet Filter List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the Packet Filter List caption.

Packet Filter List <div> Add Delete </div>										
ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Destination Port	Protocol	Time Schedule	Enable	Actions
1	Block 75.2 Telnet	Any	Any	10.0.75.2	0.0.0.0	23-23	TCP	(0) Always	<input checked="" type="checkbox"/>	<div>Edit</div> <div>Select</div>

### 2.1.2.3 Packet Filter Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one packet filter rule. They are Rule Name, From Interface, To Interface, Source IP, Destination IP, Destination Port, Protocol, Time Schedule and finally, the rule enable.

Configuration
Packet Filters
URL Blocking
Web Content Filters
MAC Control
IPS
Options

### Packet Filter Rule Configuration

Rule Name

Rule1

From Interface

Any ▼

To Interface

Any ▼

Source IP

Specific IP Address ▼ 192.168.0.1

Destination IP

Specific IP Address ▼ 192.168.0.5

Destination Port

User-defined Service ▼ -

Protocol

TCP ▼

Time Schedule

(0) Always ▼

Rule

☒ Enable

Save

Undo

Back

#### Rule Name

The name of packet filter rule.

### From Interface

Any interface or someone LAN interface or someone WAN interface.

### To Interface

Any interface or someone LAN interface or someone WAN interface.

### Source IP

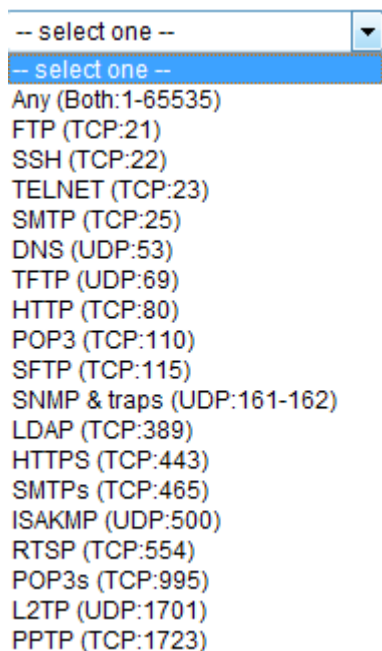
Specify the Source IP address of packets that want to be filtered out in the packet filter rule. You can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). A "0.0.0.0" implies all IP addresses.

### Destination IP

Specify the Destination IP address of packets that want to be filtered out in the packet filter rule. You can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). A "0.0.0.0" implies all IP addresses.

### Destination Port

Choose "User-defined Service" to let you specify manually the destination service port of packets that want to be filtered out in the packet filter rule. You can define a single port (80) or a range of ports (1000-1999). A "0" implies all ports are used. You also can choose one well-known service instead so that the chosen service will provide its destination port and protocol number for the rule. The supported well-known services include:



## Protocol

Specify which packet protocol is to be filtered. It can be TCP, UDP, or Both.

## Time Schedule

The rule can be turned on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the System -> Scheduling menu.

## Rule Enable

Check the enable box if you want to activate the rule. Each rule can be enabled or disabled individually.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

### 2.1.3 URL Blocking

URL Blocking will block the webs containing pre-defined key words. This feature can filter both domain input suffix (like .com or .org, etc) and a keyword “bct” or “mpe.”

Configuration Packet Filters URL Blocking Web Content Filters MAC Control IPS Options

**Configuration** [ Help ]

URL Blocking ☒ Enable

Black List / White List Allow all to pass except those match the following rules. ▼

Log Alert ☐ Enable

Invalid Access Web Redirection ☒ Enable

**URL Blocking Rule List** Add Delete

Save Undo

#### 2.1.3.1 Configuration

##### URL Blocking

Check the enable box if you want to activate URL Blocking function.

##### Black List/White List

Select one of the two filtering policies for the defined rules in URL Blocking Rule List.

- Allow all to pass except those match the specified rules (black list)
- Deny all to pass except those match the specified rules (white list)

## Log Alert

Enable the log alerting so that system will record URL blocking events when blocking rules are fired.

## Invalid Access Web Redirection

Users will see a specific web page to know their access is blocked by rules.

## [Help]

At the right upper corner of screen, one “[Help]” command let you see the on-line help message about URL Blocking function.

### 2.1.3.2 URL Blocking Rule List

It is a list of all URL Blocking rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed URL blocking rules by clicking corresponding “Edit” command buttons at the end of each blocking rule in the URL Blocking Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the URL Blocking Rule List caption.

### 2.1.3.3 URL Blocking Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one URL blocking rule. They are Rule Name, URL / Domain Name / Keyword, Destination Port, Time Schedule and finally, the rule enable.

Configuration Packet Filters **URL Blocking** Web Content Filters MAC Control IPS Options

**URL Blocking Rule Configuration**

Rule Name Rule1

URL / Domain Name / Keyword

Destination Port -

Time Schedule (0) Always ▼

Rule ☐ Enable

Save Undo Back

#### Rule Name

The name of URL blocking rule.

#### URL/Domain Name/Keyword

If any part of the Website’s URL matches the pre-defined words, the connection will be blocked. You can enter up to 10 pre-defined words in a rule and each URL keyword is separated by “,”, e.g., “google, yahoo,

org”; In addition to URL keywords, it can also block the designated domain name, like “www.xxx.com”, “www.123aaa.org, mma.com.”

### Destination Port

Specify the destination port in URL requests that want to be blocked in the URL blocking rule. You can define a single port (80) or a range of ports (1000-1999). An empty or “0” implies all ports are used.

### Time Schedule

The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the System -> Scheduling menu.

### Rule Enable

Check the enable box if you want to activate the rule. Each rule can be enabled or disabled individually. Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

## 2.1.4 Web Content Filters

Web Content Filters can block HTML requests with the specific extension file name, like “.exe”, “.bat” (applications), “mpeg” (video), and block HTML requests with some script types, like Java Applet, Java Scripts, cookies and Active X.

The screenshot shows a web management interface with a top navigation bar containing tabs: Configuration, Packet Filters, URL Blocking, Web Content Filters (selected), MAC Control, IPS, and Options. The main content area is titled 'Configuration' and includes a '[ Help ]' link. It contains three sections: 'Web Content Filters' with an 'Enable' checkbox, 'Popular File Extension List' with checkboxes for 'Cookie', 'Java', and 'ActiveX', and 'Log Alert' with an 'Enable' checkbox. Below these is a 'Web Content Filter List' section with 'Add' and 'Delete' buttons. At the bottom right are 'Save' and 'Undo' buttons.

### 2.1.4.1 Configuration

#### Web Content Filters

Check the Enable box if you want to enable Web Content Filters function.

#### Popular File Extension List

Check which extension types, Cookie, Java, ActiveX, are to be blocked.

## Log Alert

Enable the log alerting so that system will record Web content filtering events when filtering rules are fired.

### 2.1.4.2 Web Content Filter Rule List

It is a list of all Web Content Filter rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed Web Content Filter rules by clicking corresponding “Edit” command buttons at the end of each filtering rule in the Web Content Filter List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the Web Content Filter List caption.

#### Web Content Filter Configuration

Rule Name	User-defined File Extension List (Use ; to Concatenate)	Time Schedule	Enable
<input type="text" value="Rule1"/>	<input type="text"/>	<input type="text" value="(0) Always"/> ▼	<input type="checkbox"/>
<div>Save Undo</div>			

### 2.1.4.3 Web Content Filter Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one Web Content Filter rule. They are Rule Name, User-defined File Extension List, Time Schedule and finally, the rule enable.

#### Rule Name

The name of Web Content Filter rule.

#### User-defined File Extension List

You can enter up to 10 file extensions to be blocked in a rule by using ‘;’ to concatenate these file extensions.

#### Schedule

The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the System -> Scheduling menu.

#### Enable

Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.



## 2.1.5 MAC Control

MAC Control allows you to assign different access right for different users based on device's MAC address.

Configuration [ Help ]

MAC Control ☐ Enable

Black List / White List Allow all to pass except those match the following rules. ▼

Log Alert ☐ Enable

Known MAC from LAN PC List -- select one -- Copy to

MAC Control Rule List Add Delete

Save Undo

### 2.1.5.1 Configuration

#### MAC Control

Check the “Enable” box to activate the MAC Control function. All of the settings in this page will take effect only when “Enable” is checked.

#### Black List/White List

Select one of the two filtering policies for the defined rules.

- Allow all to pass except those match the specified rules (black list)
- Deny all to pass except those match the specified rules (white list)

#### Log Alert

Enable the log alerting so that system will record MAC control events when control rules are fired.

#### Known MAC from LAN PC List

You can see all of connected clients from this list, and copy their MAC address to the MAC Control Rule Configuration window below.

### 2.1.5.2 MAC Control Rule List

It is a list of all MAC Control rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed MAC control rules by clicking corresponding “Edit” command buttons at the end of each control rule in the MAC Control Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the MAC Control Rule List caption.

### 2.1.5.3 MAC Control Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one MAC Control rule. They are Rule Name, MAC Address, Time Schedule and finally, the rule enable.

#### MAC Control Rule Configuration

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
<input type="text" value="Rule1"/>	<input type="text"/>	<input type="text" value="(0) Always"/>	<input type="checkbox"/>
<input type="button" value="Save"/>			

#### Rule Name

The name of Web Content Filter rule.

#### MAC Address

Input the MAC address of local device. You can input manually or copy it from Known MAC from LAN PC List. Please note the format of MAC address is like "xx:xx:xx:xx:xx:xx". "x" is a hexadecimal digit.

#### Schedule

The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the System -> Scheduling menu.

#### Enable

Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

## 2.1.6 IPS

IPS (Intrusion Prevention Systems) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it and report it.

You can enable the IPS function and check the listed intrusion activities if necessary. There are some intrusion prevention items need a further Threshold parameter to work properly for intrusion detection. Besides, you can enable the log alerting so that system will record Intrusion events when corresponding intrusions are detected.

Configuration

Packet Filters

URL Blocking

Web Content Filters

MAC Control

IPS

Options

**Configuration**

[ Help ]

IPS☐ Enable

Log Alert☐ Enable

**Intrusion Prevention**

SYN Flood Defense

☐ Enable

Packets/second (10~10000)

UDP Flood Defense

☐ Enable

Packets/second (10~10000)

ICMP Flood Defense

☐ Enable

Packets/second (10~10000)

Port Scan Detection

☐ Enable

Packets/second (10~10000)

Block Land Attack

☐ Enable

Block Ping of Death

☐ Enable

Block IP Spoof

☐ Enable

Block TCP Flag Scan

☐ Enable

Block Smurf

☐ Enable

Block Traceroute

☐ Enable

Block Fraggle Attack

☐ Enable

ARP Spoofing Defence

☐ Enable

Packets/second (10~10000)

Save

Undo

## 2.1.7 Options

Configuration

Packet Filters

URL Blocking

Web Content Filters

MAC Control

IPS

Options

**Firewall Options**

[ Help ]

Stealth Mode☐ Enable

SPI☒ Enable

Discard Ping from WAN☐ Enable

Remote Administrator Hosts (IP / Mask : Port)

/  :

☒ Enable

Save

Undo

### Stealth Mode

Enable this feature, this device will not respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet.

## SPI

When this feature is enabled, the router will record the outgoing packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

## Discard PING from WAN

If this feature is enabled, this gateway won't reply any ICMP request packet from WAN side. It means any remote host can't get response when "ping" to this gateway. "Ping" is a useful command that we use to detect if a certain host is alive or not. But it also let hacker know about this. Therefore, many Internet servers will be set to ignore IGMP request.

## Remote Administrator Hosts (IP/Mask: Port)

In general, only local clients (LAN users) can browse the device's built-in web pages for device administration setting. This feature enables you to perform administration task from a certain remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be configured to 80 as default. You also can change web server port to other port

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

## 2.2 QoS & BWM

The total amount of data traffic increases nowadays as the higher demand of mobile devices, like Game/Chat/VoIP/P2P/Video/Web access. In order to pose new requirements for data transport, e.g. low latency, low data loss, the entire network must ensure them via a connection service guarantee.

The main goal of QoS & BWM (Quality of Service and Bandwidth Management) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows. So, QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.

To utilize your network throughput completely, administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. It is indeed required that an access gateway satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management. Helios Security Gateway provides a Rule-based QoS to carry out the requirements.

Configuration

System Resource Configuration

Total Priority Queues of All WANs

6

WAN Interface

WAN - 1

WAN Interface Resource

Bandwidth of Upstream

0

Mbps

Bandwidth of Downstream

0

Mbps

Total Connection Sessions

30000

Configuration

Rule-based Qos Enable

Enable

Flexible Bandwidth Management

Enable

QoS Rule List

Add

Delete

Clear

Restart

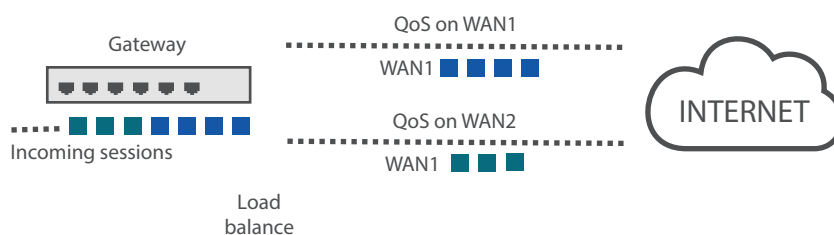
Save

Undo

## 2.2.1 Configuration

### QoS on Multiple WAN Interfaces

- QoS on all WAN interfaces satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management in a more flexible approach
- Integrated with Multi-WAN load balance function to maximize the total network throughput



### Flexible Bandwidth Management (FBM)

- Adjust the bandwidth distribution dynamically based on current bandwidth usage situation to get the maximum system network performance, and it is transparent to all users

Before QoS & BWM function can work correctly, this gateway needs to define the resource for each WAN interface. First one is the available bandwidth of WAN connection. It was set in the Basic Network -> WAN -> Physical Interface menu and shown here. Second one is the maximum number of connection sessions that the WAN interface supports. The last is the maximum number of priority queues that the

WAN interface supports.

1. WAN Interface: Select the WAN interface to configure.
2. Bandwidth of Upstream: The maximum bandwidth of uplink in Mbps.
3. Bandwidth of Downstream: The maximum bandwidth of downlink in Mbps.
4. Total Connection Sessions: Input the maximum number of connection sessions for the WAN interface.

### 2.2.2 Rule-based QoS

This gateway provides lots of flexible rules for you to set QoS policies. Basically, you need to know three parts of information before you create your own policies. First, “who” needs to be managed? Second, “what” kind of service needs to be managed? The last part is “how” you prioritize. Once you get this information, you can continue to learn more details in this section.

#### Flexible QoS Rule Definition

- Multiple Group Categories
  - Specify the group category in a QoS rule for the target objects that rule to be applied on
  - Group Category can bases on VLAN ID, MAC Address, IP Address, Host Name or Packet Length. Category depends on model
- Differentiated Services
  - Specify the service type in a QoS rule for the target packets that rule to be applied on.
  - Differentiated services can be base on 802.1p, DSCP, TOS, VLAN ID, User-defined Services and Well-known Services
  - Well-known services include FTP(21), SSH(TCP:22), Telnet(23), SMTP(25), DNS(53), TFTP(UDP:69), HTTP(TCP:80), POP3(110), Auth(113), SFTP(TCP:115), SNMP&Traps(UDP:161-162), LDAP(TCP:389), HTTPS(TCP:443), SMTPs(TCP:465), ISAKMP(500), RTSP(TCP:554), POP3s(TCP:995), NetMeeting(1720), L2TP(UDP:1701) and PPTP(TCP:1723)
- Available Control Functions
  - There are 4 resources can be applied in a QoS rule: bandwidth, connection sessions, priority queues and DiffServ Code Point (DSCP). Control function that acts on target objects for specific services of packet flow is based on these resources
  - For bandwidth resource, control functions include guaranteeing bandwidth and limiting bandwidth. For priority queue resource, control function is setting priority. For DSCP resource, control function is DSCP marking. The last resource is Connection Sessions; the related control function is limiting connection sessions.
- Individual/Group Control
  - One QoS rule can be applied to individual member or whole group in the target group. This feature depends on model
- Outbound/Inbound Control

- One QoS rule can be applied to the outbound or inbound direction of packet flow, even them both. This feature depends on model

### 2.2.2.1 Configuration

It supports the activation of Rule-based QoS.

#### Rule-based QoS Enable

Check the box if you want to enable the QoS & BWM function.

Besides, at the right upper corner of screen, one “[Help]” command let you see the on-line help message about Rule-based QoS function.

### 2.2.2.2 QoS Rule List

It is a list of all QoS rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed QoS rules by clicking corresponding “Edit” command buttons at the end of each rule in the QoS Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the QoS Rule List caption. One “Clear” command button can let you clear all rules and “Restart” command button can let you restart the operation of all QoS rules.

QoS Rule List <span>Add</span> <span>Delete</span> <span>Clear</span> <span>Restart</span>									
Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
All WANs	10.0.75.8/29	ALL	Bandwidth	10-15	Outbound	Group	(0) Always	<input checked="" type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> <span>Select</span>
All WANs	10.0.75.196/30	DSCP:CS4	DSCP	AF23	Inbound	Group	(0) Always	<input checked="" type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> <span>Select</span>
WAN - 1	10.0.75.16/28	ALL	SESSION	20000	Outbound	Group	(0) Always	<input checked="" type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> <span>Select</span>

#### Add

After you enabled the rule-based QoS function, you can click on the “Add” button to create a new QoS rule.

#### Delete

After you selected some QoS rules by checking the “Select” box for each rule, you can click on the “Delete” button to remove those rules from the list.

#### Clear

Delete all existed QoS rules.

## Restart

Press “Restart” button to re-initiate all QoS rules again.

## Edit

Configure the specific QoS rule again.

### 2.2.2.3 QoS Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one QoS rule. They are Interface, Group, Service, Resource, Control Function, QoS Direction, Sharing Method, Time Schedule and finally, the rule enable.

**Configuration**

**QoS Rule Configuration**

Interface

Group

Service

Resource

Control Function

QoS Direction

Sharing Method

Time Schedule

Rule

All WANs ▾

Src. MAC Address ▾

All ▾

Bandwidth ▾

Set MINR & MAXR ▾  ---  Mbps ▾

Outbound ▾

Group Control ▾

(0) Always ▾

☐ Enable

Save

Undo

Back

## Interface

Select the WAN interface for the QoS rule.

## Group

Specify the target client members for the rule by their VLAN ID, MAC Address, IP Address, Host Name or Group Object. These base categories depend on product models. Besides, “IP Address” group can be defined as an IP range with an IP address and its subnet mask. And “Group Object” is defined in the System -> Grouping menu. But what kinds of groups to use depend on product models.



## Service

There are 5 options for service, including All, DSCP, TOS, User-defined Services and Well-known Service as below.

ALL
DSCP
TOS
User-defined Services
Well-known Service

By default, it is “All”. It defines “what” kinds of service packets need to be managed. When “DSCP” is selected, another “DiffServ CodePoint” value must be specified. DSCP means DiffServ Code Point, as known as advanced TOS. You can choose this option if your local service gateway supports DSCP tags. The DSCP categories that this gateway can detect are as below.

Default
IP Precedence 1(CS1)
IP Precedence 2(CS2)
IP Precedence 3(CS3)
IP Precedence 4(CS4)
IP Precedence 5(CS5)
IP Precedence 6(CS6)
IP Precedence 7(CS7)
AF Class1(Low Drop)
AF Class1(Medium Drop)
AF Class1(High Drop)
AF Class2(Low Drop)
AF Class2(Medium Drop)
AF Class2(High Drop)
AF Class3(Low Drop)
AF Class3(Medium Drop)
AF Class3(High Drop)
AF Class4(Low Drop)
AF Class4(Medium Drop)
AF Class4(High Drop)
EF class

You need to choose a correct one according to your device’s specification. When “TOS” is selected for Service, TOS value must be chosen from a list of 4 options. For example:

Minimize-Cost
Maximize-Reliability
Maximize-Throughput
Minimize-Delay

When “User-defined Services” is selected, two more parameters, Protocol Number and Service Port Range, must be defined. Protocol Number is either TCP or UDP or Both. Finally, when “Well-known Service” is selected, you can choose the well-known from a list like:

Any(Both 1-65535)
FTP(21)
SSH(TCP:22)
Telnet(23)
SMTP(25)
DNS(53)
TFTP(UDP:69)
HTTP(TCP:80)
POP3(110)
Auth(113)
SFTP(TCP:115)
SNMP&Traps(UDP:161-162)
LDAP(TCP:389)
HTTPS(TCP:443)
SMTPs(TCP:465)
ISAKMP(500)
RTSP(TCP:554)
POP3s(TCP:995)
NetMeeting(1720)
L2TP(UDP:1701)
PPTP(TCP:1723)

## Resource

There are 4 resources can be chosen to control in the QoS rule. They are “Bandwidth”, “Connection Sessions”, “Priority Queues” and “DiffServ Code Points”.

## Control Function

It depends on the chosen resource. For “Bandwidth” resource, the control function is “Set MINR & MAXR”. For “Connection Sessions”, the control function is “Set Session Limitation”. For “Priority Queues”, it is “Set Priority”. However, for “DiffServ Code Points”, it is “DSCP Marking” and you need specify the DSCP value additionally.

## QoS Direction

Select the traffic direction to be applied for this rule.

DIRECTION	
IN	For inbound data
OUT	For outbound data
BOTH	Inbound and outbound

## Sharing Method

If you want to apply the value of control setting on each selected host in the “Group”, you need to select “Individual Control” for Sharing Method. On the other hand, if the value of control setting wants to be applied on all selected hosts in the “Group”, you need to select “Group Control”. For example, you define Control Function as “Set Session Limitation” and the limited sessions are 2000 sessions. You also define Sharing Method as “Individual Control”. Then, that means the maximum connection sessions of each selected host can’t exceed 2000 sessions. On the contrary, changing to “Group Control”, it means that group of client hosts totally can’t use over 2000 connection sessions.

## Schedule

The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the System -> Scheduling menu.

## Enable

Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

## Example #1 for adding a “DSCP” type QoS rule

### QoS Rule Configuration

Interface	All WANs ▼		
Group	IP ▼	10.0.75.106	Subnet Mask : 255.255.255.255 (/32) ▼
Service	DSCP ▼	DiffServ CodePoint	IP Precedence 4(CS4) ▼
Resource	DiffServ Code Points ▼		
Control Function	DSCP Marking ▼	AF Class1(High Drop) ▼	
QoS Direction	Inbound ▼		
Sharing Method	Group Control ▼		
Time Schedule	(0) Always ▼		
Rule	<input checked="" type="checkbox"/> Enable		

- Interface: select “All WANs”
- Group: select “IP” and enter IP range: 10.0.75.196/30
- Service: select “DSCP” with DiffServ CodePoint is CS4
- Resource: select “DiffServ Code Points”
- Control Function: select “DSCP Marking” with “AF Class 2(High Drop)”
- QoS Direction: select “Inbound” for inbound traffic only
- Sharing Method: select “Group Control”
- Schedule: leave the default value of “(0) Always” as it is

This rule means IP packets from all WAN interfaces to LAN IP address 10.0.75.196 ~ 10.0.75.199 which have DiffServ code points with “IP Precedence 4(CS4)” value will be modified by “DSCP Marking” control function with “AF Class 2(High Drop)” value at any time.

## Example #2 for adding a “Connection Sessions” type QoS rule

### QoS Rule Configuration

Interface	WAN - 1 ▼		
Group	IP ▼	10.0.75.106	Subnet Mask : 255.255.255.240 (/28) ▼
Service	All ▼		
Resource	Connection Sessions ▼		
Control Function	Set Session Limitation ▼	20000	
QoS Direction	Outbound ▼		
Sharing Method	Group Control ▼		
Time Schedule	(0) Always ▼		
Rule	<input checked="" type="checkbox"/> Enable		

- Interface: Select “WAN-1”
- Group: Select “IP” and enter IP range: 10.0.75.16/28
- Service: Select “ALL”
- Resource: Select “Connection Sessions”
- Control Function: Select “Set Session Limitation”, and set session number to 20000
- QoS Direction: Select “Outbound” for outbound traffic only. It is for the client devices under the gateway to establish multiple sessions with servers in the Internet
- Sharing Method: Select “Group Control”
- Schedule: Leave the default value of “(0) Always” as it is

This rule defines that all client hosts, whose IP address is in the range of 10.0.75.16~31, can access to the Internet and keep a maximum 20000 connection sessions totally at any time.

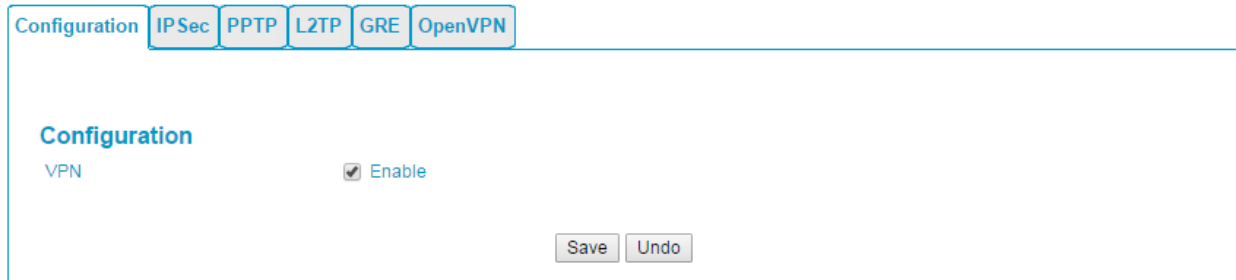
## 2.3 VPN Setup

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

The product series supports following tunneling technologies to establish secure tunnels between multiple

sites for data transferring, including IPSec, PPTP, L2TP (over IPSec) and GRE. Advanced functions include Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN.

### 2.3.1 Configuration



To enable the VPN function, you should go to Configuration before any setting.

### 2.3.2 IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

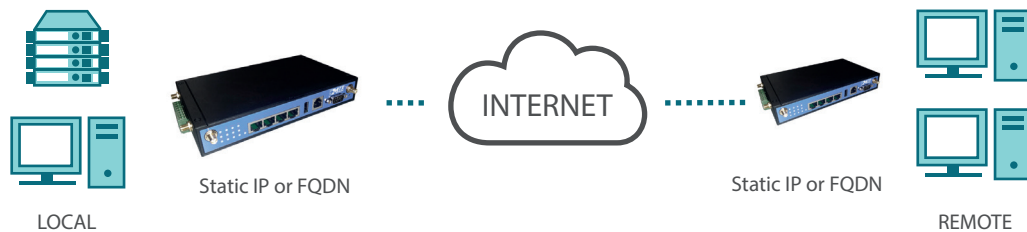
An IPSec VPN tunnel is established between IPSec client and server. Sometimes, we call the IPSec VPN client as the initiator and the IPSec VPN server as the responder. There are two phases to negotiate between the initiator and responder during tunnel establishment, IKE phase and IPSec phase. At IKE phase, IKE authenticates IPSec peers and negotiates IKE SAs (Security Association) during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2. At IPSec phase, IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. After these both phases, data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

### 2.3.2.1 IPSec VPN Tunnel Scenarios

There are some common IPSec VPN connection scenarios as follows:

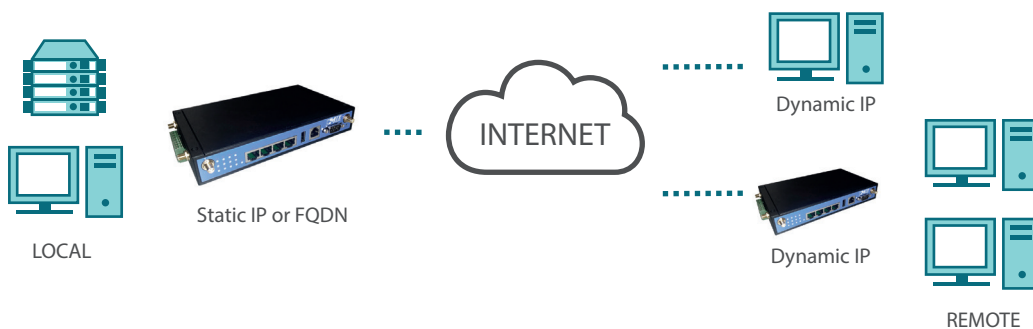
#### Site to Site

The device establishes IPSec VPN tunnels with security gateway in headquarters or branch offices. Either local or remote peer gateway which can be recognized by a static IP address or a FQDN can initiate the establishing of an IPSec VPN tunnel. Two peers of the tunnel have their own Intranets and the secure tunnel serves for data communication between these two subnets of hosts.



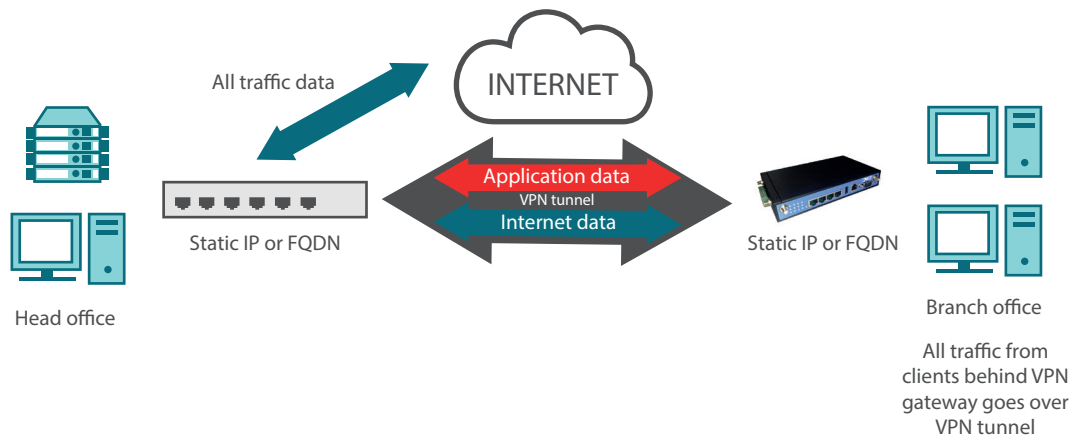
#### Dynamic VPN

Business Security Gateway can ignore IP information of clients when using Dynamic VPN, so it is suitable for users to build VPN tunnels with Business Security Gateway from a remote mobile host or mobile site. Remote peer is a host or a site will be indicated in the negotiation packets, including what remote subnet is. It must be noted that the remote peer has to initiate the tunnel establishing process first in this application scenario.



## Site to Site–Support Full Tunnel Application

When Full Tunnel function of remote Business Security Gateway is enabled, all data traffic from remote clients behind remote Business Security Gateway will go over the VPN tunnel. That is, if a user is operating at a PC that is in the Intranet of remote Business Security Gateway, all application packets and private data packets from the PC will be transmitted securely in the VPN tunnel to access the resources behind local Business Security Gateway, including surfing the Internet. As a result, every time the user surfs the web for shopping or searching data on Internet, checking personal emails, or accessing company servers, all are done in a secure way through local Business Security Gateway.



### 2.3.2.2 IPSec Configuration

#### Configuration

IPSec	<input checked="" type="checkbox"/> Enable
NetBIOS over IPSec	<input type="checkbox"/> Enable
NAT Traversal	<input type="checkbox"/> Enable
Max. Concurrent IPSec Tunnels	32

#### IPSec

You could trigger the function of IPSec VPN if you check “Enable” box.

#### NetBIOS over IPSec

If you would like two Intranets behind two Business Security Gateways to receive the NetBIOS packets from Network Neighborhood, you have to check “Enable” box.

## NAT Traversal

Some NAT routers will block IPSec packets if they don't support IPSec pass through. If your Business Security Gateway connects to this kind of NAT router which doesn't support IPSec pass through, you need to activate this option in your Business Security Gateway.

## Max. Tunnels

The device supports up to 32 IPSec tunnels, but you can specify it with the number of maximum current activated IPSec tunnels that is smaller or equal to 32.

You can add new, edit or delete some IPSec tunnels in Tunnel List & Status as follows.

### 2.3.2.3 Tunnel List & Status

Tunnel List & Status <span>Add</span> <span>Delete</span> <span>Refresh</span>								
ID	Interface	Tunnel Scenario	Tunnel Name	Remote Address	Gateway	Status	Enable	Actions
1	WAN 1	Site to Site	IPSec #1	/			<input type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> <span>Select</span>

#### Add

You can add one new IPSec tunnel with Site to Site scenario by clicking the “Add” button.

#### Delete

Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking the “Delete” button.

#### Refresh

To refresh the Tunnel List & Status each 2 seconds by clicking on the “Refresh” button.

#### Tunnel

Check the “Enable” box to activate the IPSec tunnel.

#### Edit

You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.



### 2.3.2.4 Tunnel Configuration

#### Tunnel Configuration

Tunnel	<input type="checkbox"/> Enable
Tunnel Name	<input type="text" value="IPSec #2"/>
Interface	<input type="text" value="WAN 1"/>
Tunnel Scenario	<input type="text" value="Site to Site"/>
Operation Mode	<input type="text" value="Always on"/>
Encapsulation Protocol	<input type="text" value="ESP"/>
Keep-alive	<input type="checkbox"/> Enable
	<input type="text" value="Ping IP"/> <input type="text" value="Interval 30"/> (seconds)

#### Tunnel Name

Enter the name of tunnel.

#### Interface

Decide the WAN Interface to establish the tunnel.

#### Tunnel Scenario

Support “Site to Site”, “Site to Host”, “Host to Site”, “Host to Host” and “Dynamic VPN”. Select one from them.

#### Operation Mode

Default is “Always on” and other options depend on product models.

#### Encapsulation Protocol

Default is ESP and other options depend on product models.

#### Keep-alive

Check “Enable” box to keep alive the tunnel. By default, keep-alive method is “Ping IP” and other options depend on product models. Input the IP address of remote host that exists in the opposite side of the VPN tunnel (Ex. You can input the LAN IP address of remote Business Security Gateway). The Interval is specified with the time interval between two ping requests, and by default, it is 30 seconds. Now, the device will start to ping remote host when there is no traffic within the VPN tunnel. If the device can’t get ICMP response from remote host anymore, it will terminate the VPN tunnel automatically.

### 2.3.2.5 Local & Remote Configuration

#### Local & Remote Configuration

Local Subnet	<div>192.168.0.0</div> <div></div> <div></div> <div></div> <div></div>
Local Netmask	<div>-- select one -- ▼</div> <div>-- select one -- ▼</div> <div>-- select one -- ▼</div> <div>-- select one -- ▼</div> <div>-- select one -- ▼</div>
Full Tunnel	<input type="checkbox"/> Enable
Remote Subnet	<div></div> <div></div> <div></div> <div></div> <div></div>
Remote Netmask	<div>-- select one -- ▼</div> <div>-- select one -- ▼</div> <div>-- select one -- ▼</div> <div>-- select one -- ▼</div> <div>-- select one -- ▼</div>
Remote Gateway	<div></div> (IP Address/FQDN)

#### Local Subnet

The subnet of LAN site of local Business Security Gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of local gateway. There are 5 entries for Local Subnet.

#### Local Netmask

The local netmask and associated local subnet can define a subnet domain for the local devices connected via the VPN tunnel. There are 5 entries for Local Netmask.

#### Full Tunnel

All traffic from Intranet of Business Security Gateway goes over the IPSec VPN tunnel if these packets don't match the Remote Subnet of other IPSec tunnels. That is, both application data and Internet access packets land up at the VPN concentrator.

#### Remote subnet

The subnet of LAN site of remote Business Security Gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway. There are 5 entries for Remote Subnet.

## Remote Netmask

The remote netmask and associated remote subnet can define a subnet domain for the remote devices connected via the VPN tunnel. There are 5 entries for Remote Netmask.

## Remote Gateway

Enter the IP address or FQDN of remote Business Security Gateway.

### 2.3.2.6 Authentication

#### Authentication

Key Management

IKE+Pre-shared Key  (Min. 8 characters)

Local ID

Type: User Name  ID:

Remote ID

Type: User Name  ID:

## Key Management

Select “IKE+Pre-shared Key” or “Manually”. Other options depend on product models. By default, “IKE+Pre-shared Key” method is adopted for key management. It is the first key used in IKE phase for both VPN tunnel initiator and responder to negotiate further security keys to be used in IPSec phase. The pre-shared key must be the same for both VPN tunnel initiator and responder. When “Manually” key management is adopted, the Pre-shared is not necessary.

## Local ID

The Type and the Value of the local Business Security Gateway must be the same as that of the Remote ID of the remote VPN peer. There are 4 types for Local ID: User Name, FQDN, User@FQDN and Key ID.

## Remote ID

The Type and the Value of the local Business Security Gateway must be the same as that of the local ID of the remote VPN peer. There are also 4 types for Remote ID: User Name, FQDN, User@FQDN and Key ID.

### 2.3.2.7 IKE Phase

#### IKE Phase

Negotiation Mode

Main Mode

X-Auth

None  X-Auth Account

User Name :  Password :

Dead Peer Detection (DPD)

☐ Enable  
Timeout : 180 (seconds) Delay : 30 (seconds)

Phase1 Key Life Time

3600 (seconds) (Max. 86400)

## Negotiation Mode

Choose Main Mode or Aggressive Mode: main Mode provides identity protection by authenticating peer identities when pre-shared keys are used. The IKE SA's are used to protect the security negotiations. Aggressive mode will accelerate the establishing speed of VPN tunnel, but the device will suffer from less security in the meanwhile. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.

## X-Auth

For the extended authentication function (XAUTH), the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or Business Security Gateway). The VPN server would reject the connect request from VPN clients because of invalid user information, even though the pre-shared key is correct. This function is suitable for remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users, but you can also designate account / password for specific users that are permitted to establish VPN connection with VPN server. There are 3 roles to let Business Security Gateway behave as for X-Auth authentication, including None, Server and Client. For None role, there is no X-Auth authentication happens during VPN tunnel establishing. For Server role, click "X-Auth Account" button to modify 10 user accounts for user validation during tunnel establishing to VPN server. Finally, for Client role, there are two additional parameters to fill: "User Name" and "Password" for valid user to initiate that tunnel.

## Dead Peer Detection

This feature will detect if remote VPN peer still exists. Delay indicates the interval between detections, and Timeout indicates the timeout of detected to be dead.

## Phase 1 Key Life Time

The value of life time represents the life time of the key which is dedicated at Phase 1 between both end gateways.

### 2.3.2.8 IKE Proposal Definition

#### IKE Proposal Definition

ID	Encryption	Authentication	DH Group	Definition
1	AES-auto ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-auto ▼	MD5 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
4	3DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable

There are 4 IKE proposals can be defined by you and used in IKE phase of negotiation between two VPN peers.

## Encryption

There are six algorithms can be selected: DES, 3DES, AES-auto, AES-128, AES-192, and AES-256.

## Authentication

There are five algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.

## DH Group

There are nine groups can be selected: None, Group 1 (MODP768), Group 2 (MODP1024), Group 5 (MODP1536) and Group14 ~ 18.

## Enable

Check this box to enable the IKE Proposal during tunnel establishing.

### 2.3.2.9 IPsec Phase

#### IPsec Phase

Phase2 Key Life Time  (seconds) (Max. 86400)

#### Phase 2 Key Life Time

The value of life time represents the life time of the key which is dedicated at Phase 2 between two VPN peers.

### 2.3.2.10 IPsec Proposal Definition

#### IPsec Proposal Definition

ID	Encryption	Authentication	PFS Group	Definition
1	<input type="text" value="AES-auto"/>	<input type="text" value="SHA1"/>	<input type="text" value="Group 2"/>	<input checked="" type="checkbox"/> Enable
2	<input type="text" value="AES-auto"/>	<input type="text" value="MD5"/>		<input checked="" type="checkbox"/> Enable
3	<input type="text" value="DES"/>	<input type="text" value="SHA1"/>		<input checked="" type="checkbox"/> Enable
4	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>		<input checked="" type="checkbox"/> Enable

There are 4 IPsec proposals can be defined by you and used in IPsec phase of negotiation between two VPN peers.

## Encryption

There are six algorithms can be selected: DES, 3DES, AES-auto, AES-128, AES-192, and AES-256.

## Authentication

There are five algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.

## PFS Group

There are nine groups can be selected: None, Group 1 (MODP768), Group 2 (MODP1024), Group 5 (MODP1536) and Group14 ~ 18. Once the PFS Group is selected in one IPSec proposal, the one in other 3 IPSec proposals uses the same choice.

## Enable

Check this box to enable the IKE Proposal during tunnel establishing.

### 2.3.2.11 Manual Proposal

#### Manual Proposal

Outbound SPI	0x	<input type="text"/>
Inbound SPI	0x	<input type="text"/>
Encryption	<input type="text" value="DES"/>	<input type="text"/>
Authentication	<input type="text" value="None"/>	<input type="text"/>

When “Manually” key management is used, there are 4 further parameters need to be specified by you and used in IPSec tunnel establishing.

## Outbound SPI

SPI is an important parameter during hashing. Outbound SPI will be included in the outbound packet transmitted from local gateway. The value of outbound SPI should be set in hex formatted.

## Inbound SPI

Inbound SPI will be included in the inbound packet transmitted from remote VPN peer. It will be used to de-hash the coming packet and check its integrity. The value of inbound SPI should be set in hex formatted.

## Encryption Algorithm

There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. Encryption key is used by the encryption algorithm. Its length is 16 in hex format if encryption algorithm is DES or 48

if 3DES. However, AES-128 uses 32 length of hex format, AES-192 uses 48 length of hex format, and AES-256 uses 64 length of hex format. The key value should be set in hex formatted here.

## Authentication

There are five algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512. Authentication key is used by the authentication algorithm and its length is 32 in hex format if authentication algorithm is MD5 or 40 if SHA1. However, SHA2-256 uses 64 length of hex format. Certainly, its length will be 0 if no authentication algorithm is chosen. The key value should be also set in hex formatted.

### 2.3.3 PPTP

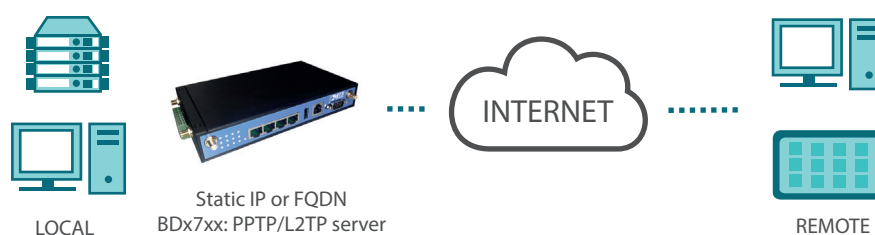
The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality. However, the most common PPTP implementation shipping with the Microsoft Windows product families implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

#### 2.3.3.1 PPTP/L2TP VPN Tunnel Scenarios

There are some common PPTP/L2TP VPN connection scenarios as follows:

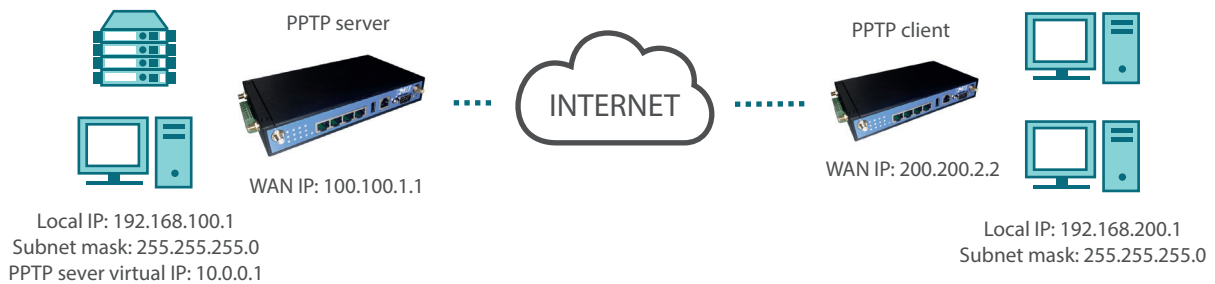
##### PPTP/L2TP Server for Remote Mobile Users

The device acts as Server role for remote users to dial in and shares some services in Intranet for them.



## PPTP/L2TP Server/Client Application

The device acts as Server or Client role in SMB Headquarters or Branch Office.



The Business Security Gateway can behave as a PPTP server and a PPTP client at the same time.

**Configuration** | **IPSec** | **PPTP** | **L2TP** | **GRE** | **OpenVPN**

**Configuration** [ Help ]

PPTP ☐ Enable

Client/Server

**PPTP Server Configuration**

PPTP Server ☐ Enable

Server Virtual IP

IP Pool Starting Address

IP Pool Ending Address

Authentication Protocol ☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2

MPPE Encryption ☐ Enable

**PPTP Server Status**

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

**User Account List**

1. PPTP: check the “Enable” box to activate PPTP client and server functions.
2. Client/Server: choose Server or Client to configure corresponding role of PPTP VPN tunnels for the Business Security Gateway beneath the choosing screen



### 2.3.3.2 PPTP Server Configuration

The Business Security Gateway can behave as a PPTP server, and it allows remote hosts to access LAN servers behind the PPTP server. The device can support four authentication methods: PAP, CHAP, MS-CHAP and MS-CHAP v2. Users can also enable MPPE encryption when using MS-CHAP or MS-CHAP v2.

#### PPTP Server Configuration

PPTP Server	<input type="checkbox"/> Enable
Server Virtual IP	<input type="text" value="192.168.0.1"/>
IP Pool Starting Address	<input type="text" value="10"/>
IP Pool Ending Address	<input type="text" value="100"/>
Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable <input type="text" value="40 bits"/>

#### PPTP Server

Enable or disable PPTP server function.

#### Server Virtual IP

It is the virtual IP address of PPTP server used in PPTP tunneling. This IP address should be different from the gateway one and members of LAN subnet of Business Security Gateway.

#### IP Pool Starting Address

This device will assign an IP address for each remote PPTP client. This value indicates the beginning of IP pool.

#### IP Pool Ending Address

This device will assign an IP address for each remote PPTP client. This value indicates the end of IP pool.

#### Authentication Protocol

You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2.

#### MPPE Encryption

Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication method. In the meantime, you also can choose encryption length of MPPE encryption, 40 bits, 56 bits or 128 bits.

### 2.3.3.3 PPTP Server Status

The user name and connection information for each connected PPTP client to the PPTP server of the Business Security Gateway will be shown in this table.

PPTP Server Status <span>Refresh</span>				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

#### Refresh

To refresh the PPTP Server Status each 2 seconds by clicking on the “Refresh” button.

#### Disconnect

To terminate the connection between PPTP server and remote dialing in PPTP clients by clicking on the “Disconnect” button.

### 2.3.3.4 User Account List

You can input up to 10 different user accounts for dialing in PPTP server.

#### Add

You can add one new user account by clicking on the “Add” button.

#### Delete

Delete selected user accounts by checking the “Select” box at the end of each user account list and then clicking on the “Delete” button.

#### Account

Check the “Enable” box to validate the user account.

#### Edit

You can edit one user account configuration by clicking on the “Edit” button at the end of each user account list.

### 2.3.3.5 User Account Configuration

Add or edit one user account will activate the “User Account Configuration” screen.

#### User Account Configuration

User Name	Password	Enable
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Enable

#### User Name

Enter the user name of user account.

#### Password

Enter the password of user account.

#### Account

Check the “Enable” box to validate the user account.

#### Save

To save the user account configuration.

### 2.3.3.6 PPTP Client

The Business Security Gateway also can behave as a PPTP client except PPTP server, and PPTP client tries to establish a PPTP tunnel to remote PPTP server. All client hosts in the Intranet of Business Security Gateway can access LAN servers behind the PPTP server.

#### PPTP Client Configuration

PPTP Client	<input checked="" type="checkbox"/> Enable
-------------	--

#### PPTP Client

Enable or disable PPTP client function.

### 2.3.3.7 PPTP Client List & Status

You can add new up to 22 different PPTP client tunnels by clicking on the “Add” button, and modify each tunnel configuration by clicking on the corresponding “Edit” button at the end of each existed tunnel.

#### Add

You can add one new PPTP client tunnel by clicking on the “Add” button.

#### Delete

Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.

#### Tunnel

Check the “Enable” box to activate the tunnel.

#### Edit

You can edit one PPTP client tunnel configuration by clicking on the “Edit” button at the end of each tunnel list.

### 2.3.3.8 PPTP Client Configuration

#### PPTP Client Configuration

PPTP Client Name	<input type="text" value="PPTP #1"/>
Interface	<input type="text" value="WAN 1"/>
Operation Mode	<input type="text" value="Always on"/>
Remote IP/FQDN	<input type="text"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>
Default Gateway/Remote Subnet	<input type="text" value="Remote Subnet"/> <input type="text"/>
Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable
NAT before Tunneling	<input type="checkbox"/> Enable
LCP Echo Type	<input type="text" value="Auto"/>
	Interval <input type="text" value="30"/> seconds Max. Failure Time <input type="text" value="6"/> times
Tunnel	<input type="checkbox"/> Enable

#### PPTP Client Name

The name of this tunnel.

## Operation Mode

Default is “Always on” and other options depend on product models.

## Peer IP/Domain

The IP address or Domain name of remote PPTP server.

## User Name

The user name which can be validated by remote PPTP server.

## Password

The password which can be validated by remote PPTP server.

## Default Gateway/Peer Subnet

You can choose “Default Gateway” option or “Peer Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this PPTP tunnel if these packets don’t match the Peer Subnet of other PPTP tunnels. There is only one PPTP tunnel to own the “Default Gateway” property. However, when “Peer Subnet” is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote PPTP server. If an Intranet packet wants to go to this peer subnet, the PPTP tunnel will be established automatically.

Connection Control: There are three connection control options for users to choose when the PPTP tunnel is established. You can choose “Connect-on-Demand”, “Auto Reconnect (always-on)”, or “Manually”. By default, it is “Auto Reconnect (always-on)”.

## Authentication Protocol

You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2. The protocol you choose must be supported by remote PPTP server.

## MPPE Encryption

Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication methods.

## NAT before Tunneling

Check the “Enable” box to let hosts in the Intranet of Business Security Gateway can go to access Internet via remote PPTP server. By default, it is enabled. However, if you want the remote PPTP Server to monitor the Intranet of local Business Security Gateway, the option can’t be enabled.

### LCP Echo Type

Choose the way to do connection keep alive. By default, it is “Auto” option that means system will automatically decide the time interval between two LCP echo requests and the times that system can retry once system LCP echo fails. You also can choose “User-defined” option to define the time interval and the retry times by yourself. The last option is “Disable”.

### Tunnel

Check the “Enable” box to activate the tunnel.

## 2.3.4 L2TP

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

The Business Security Gateway can behave as a L2TP server and a L2TP client at the same time.

### Configuration

L2TP	<input type="checkbox"/> Enable
Client/Server	Server ▼

### L2TP

Check the “Enable” box to activate L2TP client and server functions.

### Client/Server

Choose Server or Client to configure corresponding role of L2TP VPN tunnels for the Business Security Gateway beneath the choosing screen.

### 2.3.4.1 L2TP Server Configuration

The Business Security Gateway can behave as a L2TP server, and it allows remote hosts to access LAN servers behind the L2TP server. The device can support four authentication methods: PAP, CHAP, MS-CHAP and MS-CHAP v2. Users can also enable MPPE encryption when using MS-CHAP or MS-CHAP v2.

#### L2TP Server Configuration

L2TP Server	<input type="checkbox"/> Enable
L2TP over IPsec	<input type="checkbox"/> Enable Preshare Key <input type="text"/> (Min. 8 characters)
Server Virtual IP	<input type="text" value="192.168.10.1"/>
IP Pool Starting Address	<input type="text" value="10"/>
IP Pool Ending Address	<input type="text" value="100"/>
Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable <input type="text" value="40 bits"/>
Service Port	<input type="text" value="1701"/>

#### L2TP Server

Enable or disable L2TP server function.

#### L2TP over IPsec

L2TP over IPsec VPNs allow you to transport data over the Internet, while still maintaining a high level of security to protect data. Enter a Pre-shared key that system will use it in IPsec tunneling. And when you use some devices, like Apple related mobile devices, you should also know that key to establish L2TP over IPsec tunnels.

#### Server Virtual IP

It is the virtual IP address of L2TP server used in L2TP tunneling. This IP address should be different from the gateway one and members of LAN subnet of Business Security Gateway.

#### IP Pool Starting Address

This device will assign an IP address for each remote L2TP client. This value indicates the beginning of IP pool.

#### IP Pool Ending Address

This device will assign an IP address for each remote L2TP client. This value indicates the end of IP pool.

#### Authentication Protocol

You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2.

## MPPE Encryption

Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication method. In the meantime, you also can choose encryption length of MPPE encryption, 40 bits, 56 bits or 128 bits.

### 2.3.4.2 L2TP Server Status

The user name and connection information for each connected L2TP client to the L2TP server of the Business Security Gateway will be shown in this table.

L2TP Server Status <span>Refresh</span>				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

#### Refresh

To refresh the L2TP Server Status each 2 seconds by clicking on the “Refresh” button.

#### Disconnect

To terminate the connection between L2TP server and remote dialing in L2TP clients by clicking on the “Disconnect” button

### 2.3.4.3 User Account List

You can input up to 10 different user accounts for dialing in L2TP server.

#### Add

You can add one new user account by clicking on the “Add” button.

#### Delete

Delete selected user accounts by checking the “Select” box at the end of each user account list and then clicking on the “Delete” button.

#### Account

Check the “Enable” box to validate the user account.



## **Edit**

You can edit one user account configuration by clicking on the “Edit” button at the end of each user account list.

### **2.3.4.4 User Account Configuration**

Add or edit one user account will activate the “User Account Configuration” screen.

#### **User Name**

Enter the user name of user account.

#### **Password**

Enter the password of user account.

#### **Account**

Check the “Enable” box to validate the user account.

#### **Save**

To save the user account configuration.

### **2.3.4.5 L2TP Client**

The Business Security Gateway also can behave as a L2TP client except L2TP server, and L2TP client tries to establish a L2TP tunnel to remote L2TP server. All client hosts in the Intranet of Business Security Gateway can access LAN servers behind the L2TP server.

#### **L2TP Client Configuration**

Enable or disable L2TP client function.

### **2.3.4.6 L2TP Client List & Status**

You can add new up to 22 different L2TP client tunnels by clicking on the “Add” button, and modify each tunnel configuration by clicking on the corresponding “Edit” button at the end of each existed tunnel.

#### **Add**

You can add one new L2TP client tunnel by clicking on the “Add” button.

## Delete

Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.

## Tunnel

Check the “Enable” box to activate the tunnel.

## Edit

You can edit one L2TP client tunnel configuration by clicking on the “Edit” button at the end of each tunnel list.

### 2.3.4.7 L2TP Client Configuration

#### L2TP Client Configuration

L2TP Client Name	<input type="text" value="L2TP #1"/>		
Interface	<input type="text" value="WAN 1"/>		
Operation Mode	<input type="text" value="Always on"/>		
L2TP over IPsec	<input type="checkbox"/>	Enable Preshare Key	<input type="text" value=""/> (Min. 8 characters)
Remote LNS IP/FQDN	<input type="text"/>		
Remote LNS Port	<input type="text" value="1701"/>		
User Name	<input type="text"/>		
Password	<input type="password"/>		
Tunneling Password (Optional)	<input type="password"/>		
Default Gateway/Remote Subnet	<input type="text" value="Remote Subnet"/>	<input type="text"/>	
Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2		
MPPE Encryption	<input type="checkbox"/> Enable		
NAT before Tunneling	<input type="checkbox"/> Enable		
LCP Echo Type	<input type="text" value="Auto"/>		
Interval	<input type="text" value="30"/>	seconds	Max. Failure Time <input type="text" value="6"/> times
Service Port	<input type="text" value="Auto"/>	<input type="text" value="0"/>	
Tunnel	<input type="checkbox"/> Enable		

#### L2TP Client Name

The name of this tunnel.

#### Operation Mode

Default is “Always on” and other options depend on product models.

**Peer IP/Domain**

The IP address or Domain name of remote L2TP server.

**User Name**

The user name which can be validated by remote L2TP server.

**Password**

The password which can be validated by remote L2TP server.

**Default Gateway/Peer Subnet**

You can choose “Default Gateway” option or “Peer Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this L2TP tunnel if these packets don’t match the Peer Subnet of other L2TP tunnels. There is only one L2TP tunnel to own the “Default Gateway” property. However, when “Peer Subnet” is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote L2TP server. If an Intranet packet wants to go to this peer subnet, the L2TP tunnel will be established automatically.

**Connection Control**

There are three connection control options for users to choose when the L2TP tunnel is established. You can choose “Connect-on-Demand”, “Auto Reconnect (always-on)”, or “Manually”. By default, it is “Auto Reconnect (always-on)”.

**Authentication Protocol**

You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2. The protocol you choose must be supported by remote L2TP server.

**MPPE Encryption**

Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication methods.

**NAT before Tunneling**

Check the “Enable” box to let hosts in the Intranet of Business Security Gateway can go to access Internet via remote PPTP server. By default, it is enabled. However, if you want the remote PPTP Server to monitor the Intranet of local Business Security Gateway, the option can’t be enabled.

## LCP Echo Type

Choose the way to do connection keep alive. By default, it is “Auto” option that means system will automatically decide the time interval between two LCP echo requests and the times that system can retry once system LCP echo fails. You also can choose “User-defined” option to define the time interval and the retry times by yourself. The last option is “Disable”.

## Tunnel

Check the “Enable” box to activate the tunnel.

### 2.3.5 GRE

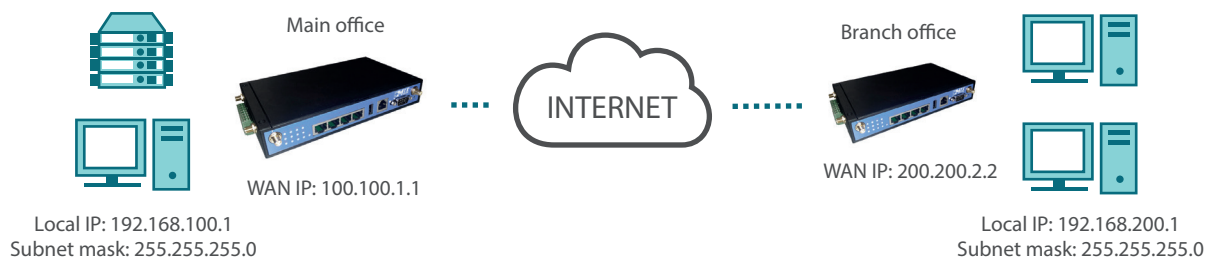
Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

#### 2.3.5.1 GRE VPN Tunnel Scenario

There is one common GRE VPN connection scenario as follows:

#### GRE Server/Client Application

The Business Security Gateway acts as GRE Server or Client role in SMB Headquarters or Branch Office.



#### 2.3.5.2 GRE Configuration

##### Configuration

GRE Tunnel

☒ Enable

#### GRE Tunnel

Check the “Enable” box to activate the GRE tunnel function.

2.3.5.3 GRE Tunnel Definitions

**GRE Tunnel List** Add Delete

ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	Key	TTL	Keep-alive	Default Gateway/ Remote Subnet	Enable	Actions
1	GRE #1	WAN 1	Always on	100.100.1.1	200.200.2.2	1234	255	<input type="checkbox"/>	0.0.0.0/0	<input type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> <span>Select</span>

Add

You can add one new GRE tunnel by clicking on the “Add” button.

Delete

Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.

Tunnel

Check the “Enable” box to activate the GRE tunnel.

Edit

You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

2.3.5.4 GRE Rule Configuration

**GRE Rule Configuration**

Tunnel Name

GRE #1

Interface

WAN 1 ▾

Operation Mode

Always on ▾

Tunnel IP

100.100.1.1

Remote IP

200.200.2.2

Key

1234

TTL

255

Keep-alive

☐ Enable

Ping IP ▾

Interval

0

(seconds)

Default Gateway/Remote Subnet

Default Gateway ▾

0.0.0.0/0

DMVPN Spoke

☐ Enable

IPSec Pre-shared Key

(Min. 8 characters)

Tunnel

☐ Enable

Tunnel

Enable or disable this GRE tunnel.

**Tunnel Name**

The name of this GRE tunnel.

**Tunnel IP**

The gateway IP address of Business Security Gateway.

**Peer IP**

Enter the IP address of remote peer that you want to connect.

**Key**

Enter the password to establish GRE tunnel with remote host.

**TTL**

Time-To-Live for packets. The value is within 1 to 255. If a packet passes number of TTL routers and still can't reach the destination, then this packet will be dropped.

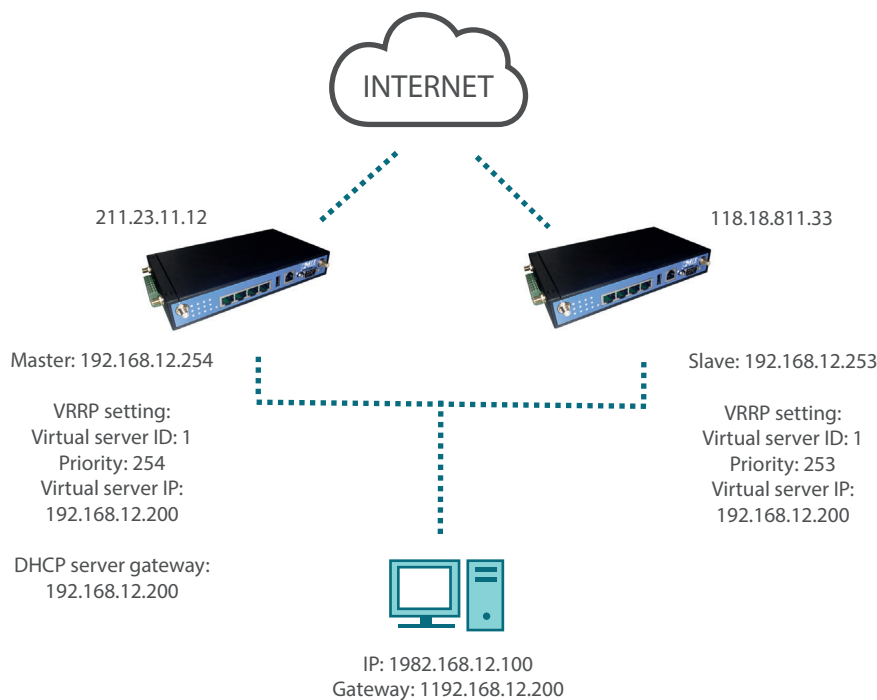
**Default Gateway/Peer Subnet**

You can choose "Default Gateway" option or "Peer Subnet" option here. When "Default Gateway" is chosen, all traffic from Intranet of Business Security Gateway goes over this GRE tunnel if these packets don't match the Peer Subnet of other GRE tunnels. There is only one GRE tunnel to own the "Default Gateway" property. However, when "Peer Subnet" is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote GRE server. If an Intranet packet wants to go to this peer subnet, the GRE tunnel will be established automatically.

## 2.4 Redundancy

### 2.4.1 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol providing device redundancy. It allows a backup router or switch to automatically take over if the primary (master) router or switch fails. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP network.



The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group. The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.

**VRRP**

**Configuration**

VRRP

☐ Enable

Virtual Server ID

(1-255)

Priority of Virtual Server

(Lowest 1 ~ 254 Highest)

Virtual Server IP Address

Save

Undo

## VRRP

Enable or disable the VRRP function.

## Virtual Server ID

Means Group ID. Specify the ID number of the virtual server. Its value ranges from 1 to 255.

## Priority of Virtual Server

Specify the priority to use in VRRP negotiations. Valid values are from 1 to 254, and a larger value has higher priority.

## Virtual Server IP Address

Specify the IP address of the virtual server.

Click on “Save” to store what you just select or “Undo” to give up.

## 2.5 System Management

This device supports many system management protocols, such as TR-069, SNMP and Telnet with CLI. You can finish those configurations in this sub-section.

### 2.5.1 TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices, like this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The Security Gateway is such CPE.

TR-069

SNMP

Telnet with CLI

UPnP

Configuration

[ Help ]

TR-069

☐ Enable

Interface

WAN-1

ACS URL

ACS UserName

ACS Password

ConnectionRequest Port

8099

ConnectionRequest UserName

ConnectionRequest Password

Inform

☒ Enable Interval 900

Save

Undo



TR-069 is a customized feature for ISP; it is not recommend that you change the configuration for this. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help. At the right upper corner of TR-069 Setting screen, one “[Help]” command let you see the same message about that.

## 2.5.2 SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow:

Supported MIBs:

- MIB-II (RFC 1213, Include IPv6)
- IF-MIB, IP-MIB, TCP-MIB, UDP-MIB
- SMIv1 and SMIv2
- SNMPv2-TM and SNMPv2-MIB
- AMIB (Matrix Private MIB)

TR-069

SNMP

Telnet with CLI

UPnP

Configuration

SNMP Enable

Supported Versions

Get / Set Community

Trap Event Receiver 1

Trap Event Receiver 2

Trap Event Receiver 3

Trap Event Receiver 4

WAN Access IP Address

LAN

WAN

v1


v2c

/

User Privacy Definition

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	Enable	Actions
1			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<div>Edit</div>
2			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<div>Edit</div>
3			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<div>Edit</div>
4			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<div>Edit</div>
5			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<div>Edit</div>

[ Help ]



MTX-ROUTER-HELIOS II | 2018/3  
 MTX © by MATRIX ELECTRONICA S.L.U.  
 SUPPORT: [iotsupport@mtxm2m.com](mailto:iotsupport@mtxm2m.com) | SALES: [info@mtxm2m.com](mailto:info@mtxm2m.com) | [mtxm2m.com](http://mtxm2m.com)

129

## SNMP Enable

You can check “Local(LAN)”, “Remote(WAN)” or both to enable SNMP function. If “Local(LAN)” is checked, this device will respond to the request from LAN. If “Remote(WAN)” is checked, this device will respond to be request from WAN.

## WAN Access IP Address

If you want to limit the remote SNMP access to specific computer, please enter the PC`s IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.

## SNMP Version

Supports SNMP V1 and V2c.

## Get Community

The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.

## Set Community

The community of SetRequest that this device will accept.

## Trap Event Receiver 1~4

Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify it, so that the device can send SNMP Trap message to the management PCs consequently.

## WAN Access IP Address

The IP address of remote control site to manage the device by using SNMP protocol.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

### 2.5.3 Telnet with CLI

A command-line interface (CLI), also known as command-line user interface, console user interface, and character user interface (CUI), is a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH CLI with default service port 2300 and 22, respectively. And it also accepts commands from both LAN and WAN sides.

#### Configuration

Telnet with CLI	LAN <input checked="" type="checkbox"/> Enable	WAN <input type="checkbox"/> Enable
Connection Type	Telnet : Service Port	<input type="text" value="23"/> <input checked="" type="checkbox"/> Enable
	SSH : Service Port	<input type="text" value="22"/> <input type="checkbox"/> Enable

### 2.5.4 UPnP

UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some NAT routers. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming, and remote assistance programs need a way to communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming.

TR-069	SNMP	Telnet with CLI	UPnP
<div>Configuration <span>[ Help ]</span></div> <div>UPnP <input type="checkbox"/> Enable</div> <div>Save Undo</div>			

This device supports the UPnP Internet Gateway Device (IGD) feature. By default, it is enabled.

## 2.6 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users ("endorsements") whom the person examining the certificate might know and trust. The device also plays as a CA role.

Certificates are an important component of Transport Layer Security (TLS, sometimes called by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing. Here, it can be used in IPsec tunneling for user authentication.

### 2.6.1 My Certificates

My Certificates include Root CA and Local Certificate List. Root CA is the top certificate of the tree, the private key used to “sign” other certificates. Local Certificate is generated in the router. it can be self-signed by its Root CA or just generate a CSR which can be signed by another external Root CA.

**My Certificates**

**Root CA**

**Local Certificate List**

**Trusted CA Certificate List**

**Trusted Client Certificate List**

**Certificate Signing Request (CSR) Import from a File**   
 Ningún archivo seleccionado

**Certificate Signing Request (CSR) Import from a PEM**

#### 2.6.1.1 Root CA

The device can serve as the Root CA. Root CA can sign local certificate when generated by selected self-signed or the Certificate Signing Request (CSR).

You can generate it by clicking on the “Generate” button.

##### Name

Enter the name of root CA.

## Key

Key Type is RSA. Key length: The size of the private key in bits. There are five key length can be selected: 512-bits, 765-bits, 1024-bits, 1536-bits, 2048-bits.

## Subject Name

The Subject Name include seven information. Country(C): The two character country code of the certificate authority is located. State(ST): The state where the certificate authority is located. Location(L): The city where the certificate authority is located. Organization(O): The company whom the certificate authority belongs to. Organization Unit(OU): The company department whom the certificate authority belongs to. Common Name(CN): The common name for certificate authority. It's important as the common name for certificate authority. E-mail: The email address of a contact for the certificate authority.

## Validity

The expiration date. There are four time period can be selected: 3-years, 5-years, 10-years, 20-years.

After successful generating the root CA, you also can delete it by checking the Select box and clicking on the "Delete" button.

You also can view its PEM codes by checking the "View" button.

You can download the local certificate file by clicking on the "Download" button.

### 2.6.1.2 Local Certificate List

This feature can show the list of all certificates which contain information identifying the applicant. Each certificate involves field of the certificate name, subject, issuer and valid to.

You can generate one certificate by clicking on the "Generate" button.

## Name

Enter the name of certificate.

## Key

Key Type is RSA. Key length: The size of the private key in bits. There are five key length can be selected: 512-bits, 765-bits, 1024-bits, 1536-bits, 2048-bits.

## Subject Name

The Subject Name include seven information. Country(C): The two character country code of the certificate is located. State(ST): The state where the certificate is located. Location(L): The city where the certificate is located. Organization(O): The company whom the certificate belongs to. Organization Unit(OU): The company department whom the certificate belongs to. Common Name(CN): The common

name for certificate. It's important as the common name for certificate. E-mail: The email address of a contact for the certificate.

You also can import one certificate from your backup ones by clicking on the "Import" button. There are two approaches to import it. One is from a file and another is copy-paste the PEM codes in Web UI, and then click on the "Apply" button.

Certainly, you also can delete one local certificate by checking corresponding Select box and clicking on the "Delete" button.

You can view its PEM codes by checking the "View" button.

You can download the local certificate file by clicking on the "Download" button.

## 2.6.2 Trusted Certificates

Trusted Certificates include Trusted CA Certificate List and Trusted Client Certificate List. The Trusted CA Certificate List which places the external trusted CA. The Trusted Client Certificate List which place the certificates what you trust.

**Trusted CA Certificate List**

**Trusted Client Certificate List**

### 2.6.2.1 Trusted CA Certificate List

The device can let you import the certificate of trusted external CA by clicking on the "Import" button.

There are two approaches to import it. One is from a file and another is copy-paste the PEM codes in Web UI, and then click on the "Apply" button.

After successful importing the trusted external CA, you also can delete it by checking the Select box and clicking on the "Delete" button.

You can view its PEM codes by checking the "View" button.

You can download the trusted CA file by clicking on the "Download" button.

### 2.6.2.2 Trusted Client Certificate List

This feature can show the list of all certificates information. Each Certificate involve field of certificate name, subject, issuer and valid to.

You can import one trusted external client certificate by clicking on the "Import" button.

There are two approaches to import it. One is from a file and another is copy-paste the PEM codes in Web UI, and then click on the "Apply" button.

You also can delete one trusted client certificate by checking corresponding Select box and clicking on

the “Delete” button.

You can view its PEM codes by checking the “View” button.

You can download the trusted client certificate file by clicking on the “Download” button.

### 2.6.3 Issue Certificates

When you have a Certificate Signing Request (CSR) that needs to be certificated by the root CA of the device, you can issue the request here and let Root CA sign it. There are two approaches to issue it. One is from a file and another is copy-paste the CSR codes in Web UI, and then click on the “Sign” button.

After signing, the Issuer information can be show which is Root ca subject.

You also can view its PEM codes by checking the “View” button and download the issued certificate file by clicking on the “Download” button.

## 2.7 Serial Port Settings

The Helios II series provides the DB-9 male port for various serial communication use through connecting the RS-232 or RS-485 serial device to an IP-based Ethernet LAN. These communication protocols make user access serial devices anywhere over a local LAN or the Internet easily.

You can finish all related configurations of serial port in this section.

### 2.7.1 Port Configuration

Before using the function of Virtual COM or Modbus, you need to configure the DB-9 male port first.

Serial Port Modbus

**Port Configuration**

Operation Mode Disable ▼

Interface RS-232 ▼

Baud Rate 19200 ▼

Data Bits 8 ▼

Stop Bits 1 ▼

Flow Control None ▼

Parity None ▼

**Functionality**

Operation Mode Select One ▼

#### Operation Mode

Choose the purpose of serial port. It can be “Virtual COM” or “Modbus”. You can also disable it to prevent anyone connects a unknown serial device to this gateway.

### Interface

Choose RS-232 or RS-485.

### Baud Rate

Set the baud rate (bps) of serial port. The value can be 9600, 19200, 38400, 57600, or 115200.

### Data Bits

Choose 7 or 8 as the data bit.

### Stop Bits

Choose 1 or 2 as the stop bit.

### Flow Control

Choose RTS/CTS, DTS/DSR for flow control, or none.

### Parity

Choose None, Even or Odd.

## 2.7.2 Virtual COM

Create a virtual COM port on user's PC/Host and provide access to serial device connected to serial port on Helios gateway. Therefore, users can access, control, and manage serial devices through Internet (fixed line, or cellular network) no matter where they are. There are four modes for virtual com connection: TCP Client, TCP Server, UDP, and RFC2217.



## TCP Client Mode

In TCP Client mode, Helios can actively establish a TCP connection to a pre-defined host computer when serial data arrives. After the data has been transferred, Helios can automatically disconnect from the host computer by using the TCP alive check timeout or idle timeout settings.

### Functionality

Operation Mode	TCP Client ▼
Connection Control	Always on ▼
Connection Idle Timeout	0 (0-60)min
Alive Check Timeout	0 (0-60)min

### Legal IP/FQDN Definition (TCP Client)

ID	To Host	Remote Port	Definition	Action
1		4001		Edit
2		4001		Edit
3		4001		Edit
4		4001		Edit

1. Operation Mode: choose TCP Client.
2. Connection Control: choose “Always on” if you want to keep TCP connection with TCP server all the time. Otherwise, you can choose “ON-Demand” if you want to establish TCP connection only when data is required to transmit.
3. Connection Idle Timeout: input the time period of idle timeout. The TCP connection will be terminated if it idles longer than this timeout setting. This option is only available when connection control is set to “ON-Demand”.
4. Alive Check Timeout: input the time period of alive check timeout. The TCP connection will be terminated if it doesn’t receive response of alive-check longer than this timeout setting.
5. To Host: press “Edit” button at right side, and you can enter IP address or FQDN of remote host (TCP server) that you want to communicate.
6. Remote Port: enter the TCP port that remote host (TCP server) is listening.
7. Definition: check this checkbox to enable this rule.

## TCP Server Mode

In TCP Server mode, Helios provides a unique IP:Port address on a TCP/IP network. Helios waits passively to be contacted by the host computer, allowing the host computer to establish a connection with and get data from the serial device. This operation mode also supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device – at the same time.

### Functionality

Operation Mode	<input type="text" value="TCP Server"/>
WAN interface	<input type="text" value="All WANs"/>
Listen Port	<input type="text" value="4001"/>
Trust Type	<input checked="" type="radio"/> Allow All <input type="radio"/> Specific IP
Max Connection	<input type="text" value="1"/>
Connection Idle Timeout	<input type="text" value="0"/> (0-60)min
Alive Check Timeout	<input type="text" value="0"/> (0-60)min

1. Operation Mode: choose TCP Server.
  2. Listen Port: indicate the listening port of TCP connection.
  3. Trust Type: you can choose “Allow All” to allow all TCP clients to connect, or choose “Specific IP” to limit to certain TCP clients.
  4. Max Connection: set the maximum number of concurrent TCP connections. Up to 4 TCP connections can be established at the same time.
  5. Connection Idle Timeout: input the time period of idle timeout. The TCP connection will be terminated if it idles longer than this timeout setting.
  6. Alive Check Timeout: input the time period of alive check timeout. The TCP connection will be terminated if it doesn’t receive response of alive-check longer than this timeout setting.
- If choosing “Specific IP” in Trust Type, you need to enter the IP address range of allowed TCP clients. Then check the checkbox in “Definition” to enable this rule.

UDP Mode

In the UDP mode, you can multicast data from the serial device to multiple host computers, and the serial device can also receive data from multiple host computers, making this mode ideal for message display applications.

Functionality

Operation Mode

UDP

WAN interface

All WANs

Listen Port

4001

Legal IP Definition (UDP)

ID	Host	Remote Port	Definition	Action
1	-	4001		Edit
2	-	4001		Edit
3	-	4001		Edit
4	-	4001		Edit

- 1. Operation Mode: choose UDP.
- 2. Listen Port: indicate the listening port of UDP connection.
- 3. Host: press “Edit” button, and enter IP address range of remote UDP hosts.
- 4. Remote Port: indicate the UDP port of peer UDP hosts.
- 5. Definition: check this checkbox to enable this rule.

## RFC2217 Mode

In the RFC2217 mode, it is a standard driver that provides Virtual COM function. RFC2217 defines general COM port control options based on telnet protocol. Any 3rd party driver supporting RFC2217 can be used to implement Virtual COM on the gateway. The driver establishes a transparent connection between host and serial device by mapping the IP:Port of the gateway's serial port to a local COM port on the host computer.

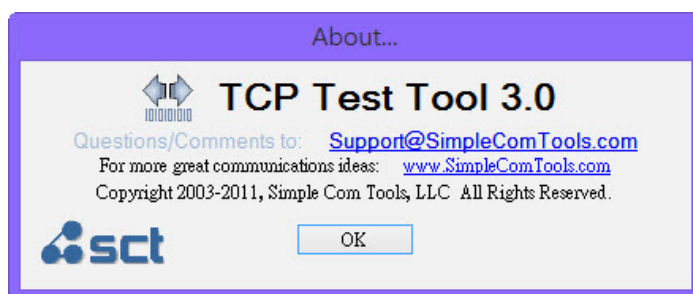
### Functionality

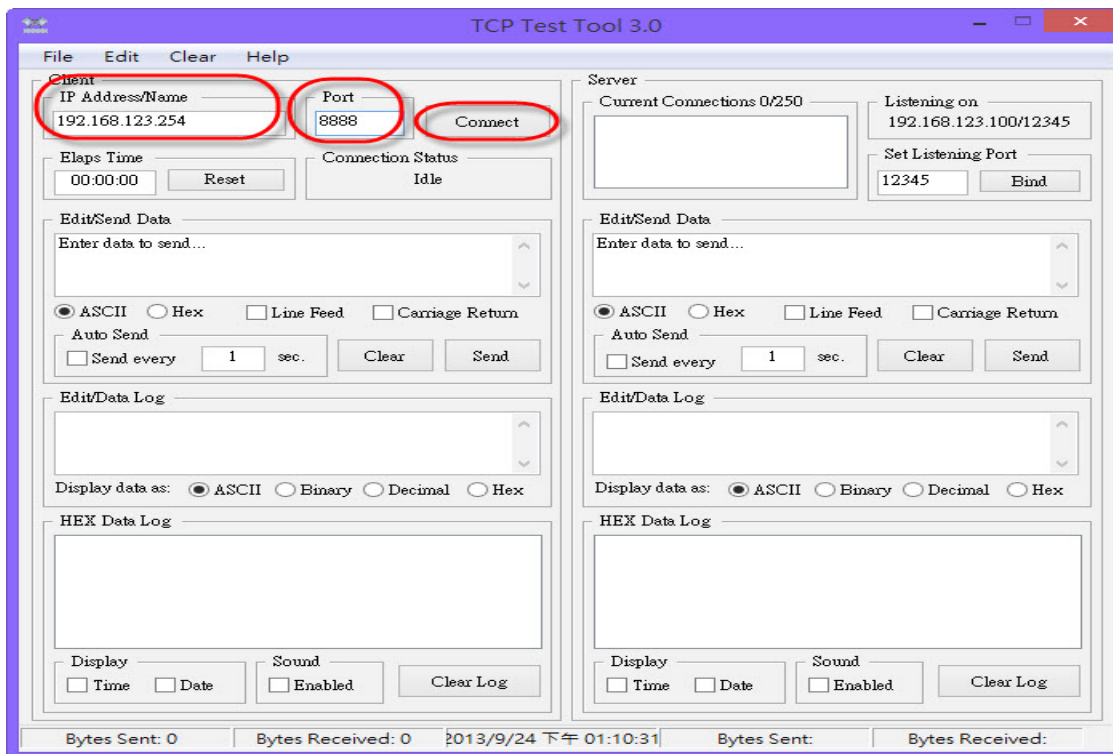
Operation Mode	<input type="text" value="RFC-2217"/>
WAN interface	<input type="text" value="All WANs"/>
Listen Port	<input type="text" value="4001"/>
Trust Type	<input checked="" type="radio"/> Allow All <input type="radio"/> Specific IP
Connection Idle Timeout	<input type="text" value="0"/> (0-60)min
Alive Check Timeout	<input type="text" value="0"/> (0-60)min

1. Operation Mode: choose RFC-2217.
2. Listen Port: indicate the listening port of RFC-2217 connection.
3. Trust Type: you can choose "Allow All" to allow all hosts to connect, or choose "Specific IP" to limit to certain hosts.
4. Connection Idle Timeout: input the time period of idle timeout. The connection will be terminated if it idles longer than this timeout setting.
5. Alive Check Timeout: input the time period of alive check timeout. The connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting.

If choosing "Specific IP" in Trust Type, you need to enter the IP address range of allowed hosts. Then check the checkbox in "Definition" to enable this rule.

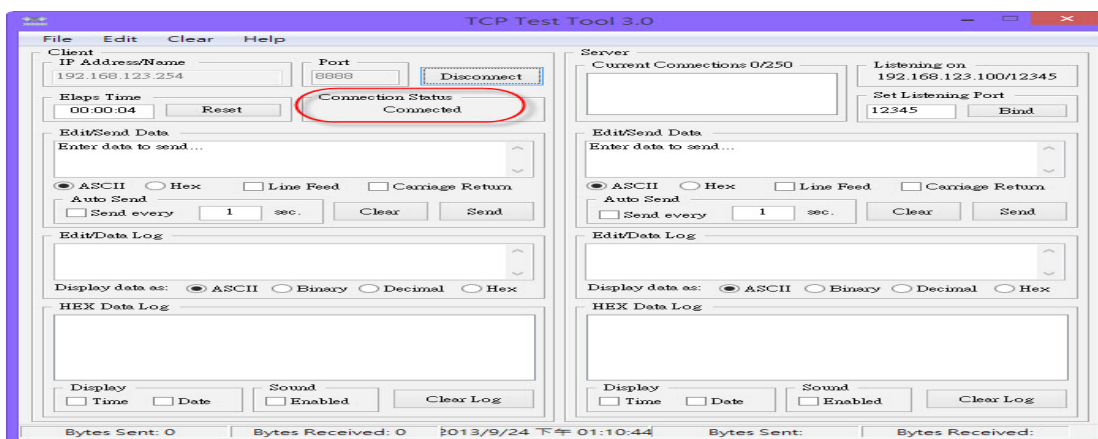
There is another approach to verify whether the Virtual COM setting is correct or not. You can install the "TPC Test Tool" in another LAN computer.

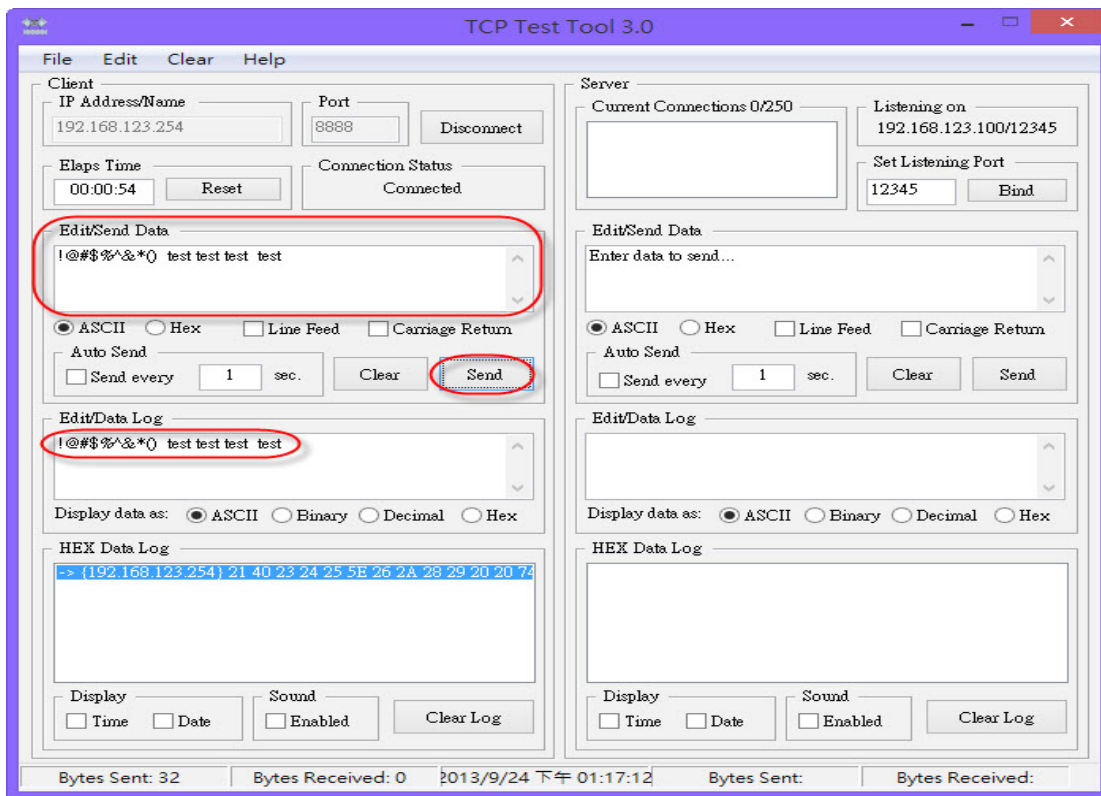




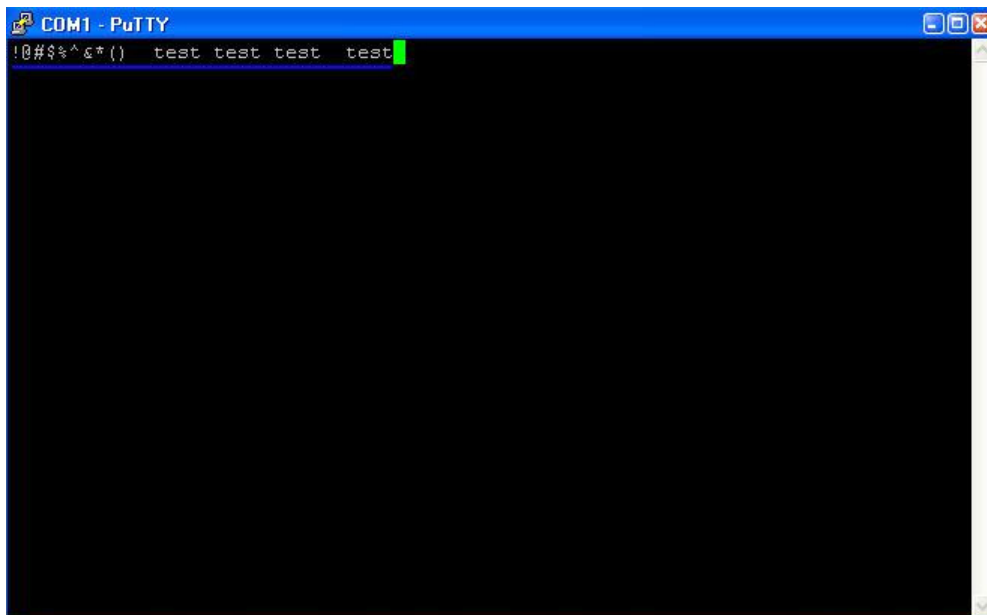
TCP Test Tools can be configured the following steps:

- IP Address: setting the Helios II address (ex. 192.168.123.254)
- Port: should be same as the listen port of Helios II
- Click the “Connect” button
- The Connecting Status should be shown as “Connected”





In the Edit/Send Data, you can try to text some information, and then click the “Send” button. Then, you can see the same information in the PuTTY.



### 2.7.3 Modbus

Modbus is one of the most popular automation protocols in the world, supporting traditional RS-232/485 devices and recently developed Ethernet devices. Many industrial devices, such as PLCs, DCSs, HMIs, instruments, and meters, use Modbus as the communication standard. It is used to

establish master-slave/client-server communication between intelligent devices.

However, the Ethernet-based Modbus protocol is so different from the original serial-based protocols. In order to integrate Modbus networks, the Helios series, including a serial ports that support RS-232 and RS-485 communication interface, can automatically and intelligently translate between Modbus TCP (Ethernet) and Modbus ASCII/RTU (serial) protocols, allowing Ethernet-based PLCs to control instruments over RS-485 without additional programming or effort.

- Integration of Modbus TCP and Modbus RTU/ASCII networks
- Software-selectable RS-232/485 communication
- High speed serial interface supporting 460.8Kbps

NOTE: All devices that are connected to a single serial port must use the same protocol (i.e., either Modbus RTU or Modbus ASCII).

Serial Port

Modbus

Gateway Configuration

Gateway

Response Timeout

Timeout Retries

Message Buffering

0Bh Exception

Tx Delay

☒ Enable

(1-65535)ms

(0-5)times

☐ Enable

☐ Enable

☐ Enable

Slave Configuration

Slave

Slave ID

Interface

☒ Enable

(1-247)

☒ Serial ☐ TCP Network

Modbus Serial Definition

Serial Port	Serial Mode	Serial Protocol	Enable	Action
SPort-1	Slave	RTU	<input type="checkbox"/>	<div>Edit</div>

Modbus TCP Configuration

Listen Port

TCP Connection Idle Time

Maximum TCP Connections

TCP Keep-alive

Trusted IP Access

(1-65535)

(1-65535)sec

(1-4)

☐ Enable

Modbus Remote Slave List

Add

Delete

1. Gateway: the definition of Modbus Gateway is an adapter application enables conversions between Serial and Network Modbus protocols.

2. Serial Response Timeout: if the serial side does not response within the specific time, data would be dropped and not transmitted over TCP even if the gateway receives it later (if the response is not received, the gateway can generate and return the Master exception).

3. Serial Timeout Retries: if “0” is set, the gateway would not store TCP packets in the buffer. If the number is greater than “0”, the gateway would store the TCP packets in the buffer and retries the

specified time when the Modbus device on the serial side does not response.

4. Serial Message Buffering: if this option is selected, the gateway will buffer TCP up to 32 requests. If this option is unselected, the gateway will respond with a 06h if it has a message out on the port with no response yet.

5. 0Bh Exception: modbus protocol defines that the 0Bh is “an error code which means error message of the interconnected gateway, or no response of the access device”. When the Modbus slave device does not respond before the timeout has been reached or has a bad response (check sum does not match), the 0Bh exception code is transmitted to the master that initiated the Modbus message.

6. Tx Delay: this is the minimum amount of time after receiving a response before the next message can be sent out.

### **Slave Configuration**

7. Slave: enable this functionality if the gateway is going to be used as Modbus slave device.

8. Slave ID: select the ID of the gateway into the Modbus bus with a number between 1-247.

9. Interface: select the interface of the Slave profile of the gateway, Serial or TCP Network if the the gateway will be slave device on the Ethernet side.

### **Modbus Serial Definition**

10. Serial Mode: we can select if the Serial port of the gateway will be master or slave in the bus.

11. Serial Protocol: defines the RTU or ASCII for the serial protocol.

12. Enable: we can enable or disable the serial interface.

### **Modbus TCP Configuration**

13. Listen port: select the TCP port where the gateway will be waiting for connection.

14. TCP Connection Idle Timeout: idle timeout in seconds for the Modbus /TCP connection. If the gateway doesn't receive any Modbus /TCP query within the specific time, the connection will be closed.

15. Maximum TCP Connection: maximum of four simultaneous Modbus /TCP connections is allowed.

16. TCP Keep-alive: enable the connection testing enabled for TCP network communication.

17. Trusted IP Access: defines the IP that is allowed to connect to the gateway.

### **Modbus Remote Slave List**

18. Remote Slave IP: when the router is working as TCP master, here we have to select the the IP of the Modbus Slave.

19. Remote Slave Port: TCP port for the connection.

20. Remote Slave ID Range: range of ID for the slaves connected to the gateway.



## ● 3. SMS Remote Management

In this section you can finish the Mobile Application and Captive Portal settings. For Mobile Application, this device is equipped with a 3G/4G module as WAN interface, and it also provide the SMS, USSD, Network Scan, and Remote Management by SMS. Besides, it also serves as an Internet access gateway. Any client host in the Intranet wants to surf the Internet, the device will redirect the Internet surfing request to an external captive portal Web server for user authentication. If the authentication is successful, the requested client host will be allowed to access Internet by the device.

### 3.1 SMS Remote Management

#### 3.1.1 SMS

SMS

Remote Management

#### Configuration

Physical Interface

3G/4G-1 ▼

SMS

☒ SIM Status: SIM\_A

SMS Storage

SIM Card Only ▼

#### Alert Rule List

Add

Delete

#### SMS Summary

New SMS

SMS Inbox

Unread SMS	7
Received SMS	17
Remaining SMS	33

Save

Refresh

You can compose new SMS message and check received SMS message on this gateway.

#### Configuration

Physical Interface

3G/4G-1 ▼

SMS

☒ SIM Status: SIM\_A

SMS Storage

SIM Card Only ▼

1. Physical Interface: indicate which 3G/LTE modem is used for SMS feature.
2. SMS: indicate which SIM card is used for SMS feature.
3. SMS Storage: select storage for SMS message. This gateway only supports “SIM Card Only” for SMS storage.

This gateway can forward received SMS message automatically. Press “Add” to add new rule.

## Alert Rule List

[Add](#)[Delete](#)

### Alert Rule Configuration

[Save](#)

From Phone Number

Alert Approach

Auto-forward ▼

Destination

Enable

☐

1. From Phone Number: indicate phone number of sender.
2. Alert Approach: decide the way to forward message. You can forward this message to another phone number, or to a mail address, or to a syslog server.
3. Destination: please enter the phone number of receiver if you choose “Auto-forward”. Or enter a mail address if choosing “By Email”. Or enter the IP address of syslog server if choosing “By Syslog”.
4. Enable: enable this rule.

## SMS Summary

### SMS Summary

[New SMS](#)[SMS Inbox](#)

Unread SMS

7

Received SMS

17

Remaining SMS

33

1. Unread SMS: indicate number of unread SMS message.
2. Received SMS: indicate number of total received SMS message.
3. Remaining SMS: indicate number of new message can be received because of SMS storage limit.

## Create New SMS Message

You can create a new SMS message on this page. After finishing the content of message, and filling with phone number of receiver(s), you can press the “Send” button to send this message out. You can see “Send OK” if the new message has been sent successfully.

**New SMS**

Receivers

(Use '+' for International Format and ';' to Compose Multiple Receivers)

Text Message

Length of Current Input : 0

Result

## Read New SMS Message

You can read, delete, reply, and forward messages in this inbox section.

SMS Inbox List <input type="button" value="Refresh"/> <input type="button" value="Delete"/> <input type="button" value="Close"/>				
ID	From Phone Number	Timestamp	SMS Text Preview	Actions
1	2116	2015/11/26,16:45:59		<input type="button" value="Detail"/> <input type="checkbox"/> <input type="button" value="Reply"/> <input type="button" value="Forward"/>
2	2116	2015/11/26,16:46:21		<input type="button" value="Detail"/> <input type="checkbox"/> <input type="button" value="Reply"/> <input type="button" value="Forward"/>
3	2116	2015/11/26,17:05:10		<input type="button" value="Detail"/> <input type="checkbox"/> <input type="button" value="Reply"/> <input type="button" value="Forward"/>
4	2116	2015/12/23,11:38:48		<input type="button" value="Detail"/> <input type="checkbox"/> <input type="button" value="Reply"/> <input type="button" value="Forward"/>
5	2116	2015/12/23,11:42:52		<input type="button" value="Detail"/> <input type="checkbox"/> <input type="button" value="Reply"/> <input type="button" value="Forward"/>
6	222000	2015/12/23,11:49:06	El mensaje.....	<input type="button" value="Detail"/> <input type="checkbox"/> <input type="button" value="Reply"/> <input type="button" value="Forward"/>
7	222000	2016/01/11,11:05:02	El mensaje.....	<input type="button" value="Detail"/> <input type="checkbox"/> <input type="button" value="Reply"/> <input type="button" value="Forward"/>
8	222000	2016/01/11,11:05:08	El mensaje.....	<input type="button" value="Detail"/> <input type="checkbox"/> <input type="button" value="Reply"/> <input type="button" value="Forward"/>

1. Refresh: you can press “Refresh” button to renew SMS lists.
2. Delete, Reply, Forward Messages: after reading message, you can check the checkbox on the right of each message to delete, reply, or forward this message.

### 3.1.4 Remote Management

This part is for remote management functions that are done by text SMS (Short Message Service). Users can send certain SMS to this gateway to activate some actions, such as connect/disconnect/reconnect WAN connection or reboot the system. Besides, gateway can also send SMS to users to alert some events automatically.

SMS

Remote Management

**Management Settings**

Remote Management via SMS  
Delete SMS for Remote Management  
Security Key

☒ Enable ☐ Disable  
☐ Enable ☒ Disable  
123456

**Command Settings**

Status  
Connect  
Disconnect  
Reconnect  
Reboot

☒ Enable ☐ Disable  
☐ Enable ☒ Disable  
☐ Enable ☒ Disable  
☐ Enable ☒ Disable  
☒ Enable ☐ Disable

**Notification Settings**

WAN Link Up  
WAN Link Down

☒ Enable ☐ Disable  
☐ Enable ☒ Disable

**Access Control List**

Access Control  
Phone 1  
Phone 2  
Phone 3  
Phone 4  
Phone 5

+34681319911

☒ Enable ☐ Disable  
☒ Management ☒ Notification  
☐ Management ☐ Notification  
☐ Management ☐ Notification  
☐ Management ☐ Notification  
☐ Management ☐ Notification

Save

Undo

Reboot

#### Management Settings

1. Remote Management via SMS: check this to enable this function.
2. Delete SMS for Remote Management: this device will delete received SMS message that is for remote management purpose if enabling this option. This option can prevent storage space of SIM card from being occupied continuously. If SIM storage is full, this gateway can't receive any new SMS.
3. Security Key: this security key will be used for authentication when this gateway receives SMS command. Users need to type this key first and then followed by a command. There should be a "blank" between key and command (e.g. 1234 reboot). If this field is empty, users just need to type command without adding any key information.

Note: if security key is empty, access control needs to be activated. The security key can be empty if access control is activated.

#### Command Settings

1. Status: enable it, and you can send command "status" to query WAN connection status. For 3G/

LTE WAN, router will send back WAN IP address, network name, network type, and connection time via SMS. For Ethernet WAN, router will send back WAN IP address and connection time via SMS. The content would be similar to following format:

WAN IP: [xxx.xx.xxx.xx]

Network: [carrier name] (for wireless WAN only)

Type: [GPRS, WCDMA, HSPA, HSPA+, LTE] (for wireless WAN only)

Conn. Time: [connection time]

2. Connect: enable it, and you can send command “connect” to start WAN connection.
3. Disconnect: enable it, and you can send command “disconnect” to disconnect WAN connection.
4. Note: if this gateway receives “disconnect” command from SMS, it won’t try to connect again no matter WAN connection mode is set to auto-reconnect.
5. Reconnect: enable it, and you can send command “reconnect” to disconnect WAN connection, and start WAN connection again immediately.
6. Reboot: enable it, and you can send command “reboot” to restart router.

**\*\*All management commands are not case sensitive\*\***

### Notification Settings

1. WAN Link Down: enable it, and this gateway will send a message to users if primary WAN connection is dropped.
2. WAN Link Up: enable it, and this gateway will send a message to users if WAN connection is established. This message will also include WAN IP address.
3. Secondary WAN is Up: enable it, and this gateway will send a message to users if secondary WAN is connected. This message will also include WAN IP address.
4. Secondary WAN is Down: enable it, and this gateway will send a message to users if secondary WAN is disconnected.

### Access Control List

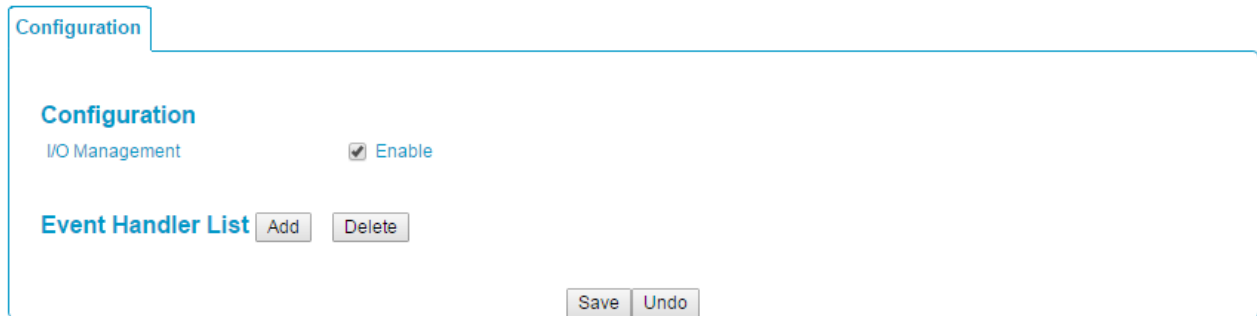
1. Access Control: users can decide which phone number can send commands to this gateway or receive notifications when enable this option.
2. Phone 1~5: for security concern, this gateway won’t deal with the command if that phone number is not in the list even the security key is correct. The phone number must be with the international prefix (i.e. +886939123456). You can also assign specific phone number can send command and/or also can receive notifications.

## 3.2 IO Management

This IO management is to help user to define DIDO events/ handler behavior, once you enable the IO management, you can add Event/ Handler to follow your definition.

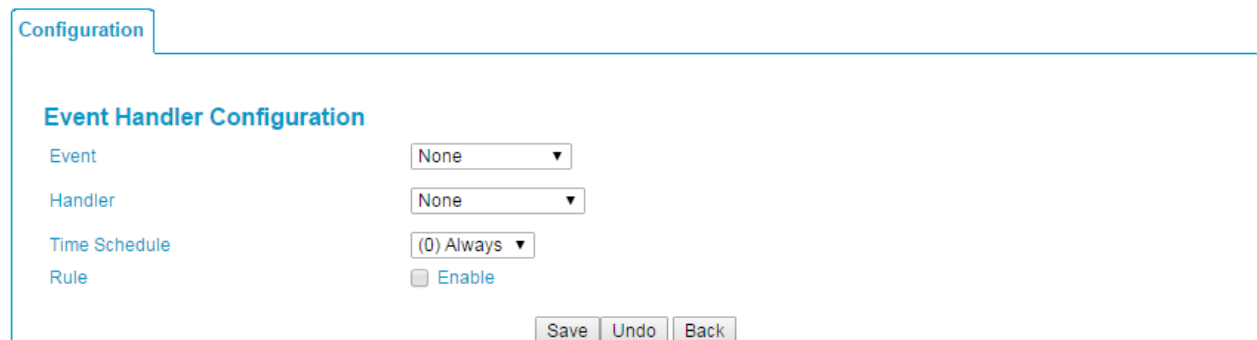
### 3.2.1 Configuration

To press 'Add' button, you can enter the following page, and define your event as DI/SMS/Power Change/Modbus Event. Some event categories depend on product models.



The screenshot shows a web interface with a 'Configuration' tab. Below the tab, there is a section titled 'Configuration' with a sub-label 'I/O Management'. To the right of this sub-label is a checkbox labeled 'Enable' which is checked. Below this, there is a section titled 'Event Handler List' with two buttons: 'Add' and 'Delete'. At the bottom right of the configuration area, there are two buttons: 'Save' and 'Undo'.

Then, you can define the handler behavior for None/ DO/SMS/Syslog/SNMP Trap/Email Alert / Reboot/ Modbus Handler. Some handler categories depend on product models.



The screenshot shows a web interface with a 'Configuration' tab. Below the tab, there is a section titled 'Event Handler Configuration'. It contains four rows of configuration options: 'Event' with a dropdown menu set to 'None', 'Handler' with a dropdown menu set to 'None', 'Time Schedule' with a dropdown menu set to '(0) Always', and 'Rule' with a checkbox labeled 'Enable' which is checked. At the bottom right of the configuration area, there are three buttons: 'Save', 'Undo', and 'Back'.

As for the Time schedule, it is to allow Event/ Handler to active by the Time Schedule Rule. The feature depends on product models.

## ● 4. Location Tracking

Location tracking applications are usually referred to applications that take benefits from Global Navigation Satellite System (GNSS). GNSS is the infrastructure that allows devices to determine its position, velocity, and time by processing satellites signals from outer space. GNSS includes varieties of satellite systems and Satellite-Based Augmentation Systems (SBAS). SBAS is usually used for improving positioning accuracy. The tables below show 4 major GNSS system in the world, and SBAS system in different areas.

Major GNSS System in the world:

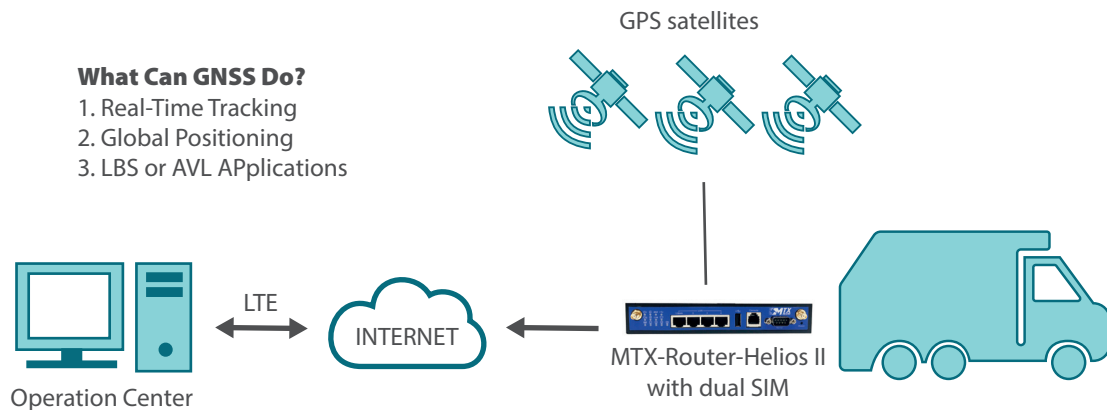
GNSS System	OWNER
GPS	USA
GLONASS	Russia
Galileo	European Union
BeiDou (COMPASS)	China

Satellite-Based Augmentation System (SBAS):

SBAS	AREA COVERAGE
EGNOS	Europe
WAAS	North America
GAGAN	India
MSAS	Japan

Position applications are widely-used by varieties of industrial applications, including Location-Based Services (LBS), Automatic Vehicle Location (AVL), Fleet Management, or assets tracking. However, in most case, GNSS is a one-way communication. That means GNSS-compatible device can only locate its location by receiving GNSS signal, but it can't forward its location data to any other identity through GNSS system. According to this limitation by GNSS system, devices usually need to equip other technology to transmit their location data to back-end server for track or further analysis. Furthermore, as the position applications are more applied on moving objects, a kind of wireless technology would be more suitable to be adopted to transmit location data. Nowadays, thanks to popularity and wide coverage of cellular technology (GSM, 3G, 4G/LTE), transmitting location data to remote center in real time is no longer a hurdle. In addition, the data format of location data is NMEA 0183 compatible, so the back-end server will be easy to interpret the collected location data.

Hereunder are the main features of GNSS function in cellular gateway, if optional GNSS function is supported.



- Retrieve GNSS data from satellites and send to remote operation center periodically or save in local storage
- Global positioning with multiple GNSS systems, including GPS, and optional for GLONASS, Galileo, or BeiDou
- Mandatory for varieties of LBS (Location-Based Service) applications, such as advertisement, emergent call
- Easy integration with AVL (Automatic Vehicle Location) applications, for managing fleet of service vehicles
- Other value-added applications, such as asset tracking, electronic toll collection, intelligent transport system

## 4.1 GNSS

With GNSS configuration page, you can configure those functions that are mentioned above. Please note the available GNSS features on different models may be different. Please check product datasheet for details.

The configuration steps include following items.

- Activate GNSS feature in gateway and finish settings of cellular WAN
- Support NMEA 0183 (compatible to 3.0) protocol, and allow customized prefix and suffix
- Configurable GPS data logging on local microSD card storage for route record tracking
- Indicate remote host, time interval, TCP/UDP, and type of GPS data that would be sent

### GPS Message Type

This item shows all supported types of NMEA 0183 data format. NMEA 0183 data format was defined and maintained by National Marine Electronics Association (NMEA). Select one or more types that



you want to use for transmitting GPS data. In most case, this configuration depends on which data format that your central server can recognize. Only select the type you need, otherwise it will consume unnecessary network bandwidth. The table below shows more information for different types of NMEA 0183 message.

TYPE	DESCRIPTION	EXAMPLE
GGA	Fix Information	\$GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47
GLL	Lat/Lon Data	\$GPGLL,4916.45,N,12311.12,W,225444,A,*1D
GSA	Overall Satellite Data	\$GPGSA,A,3,04,05,,09,12,,,24,,,,,2.5,1.3,2.1*39
GSV	Detailed Satellite Data	\$GPGSV,2,1,08,01,40,083,46,02,17,308,41,12,07,344,39,14,22,228,45*75
RMC	Recommended Minimum Data	\$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A
VTG	Vector Track and Speed Over the Ground	\$GPVTG,054.7,T,034.4,M,005.5,N,010.2,K*48

Please note this option is hardware dependent. The available options of GPS message type show on this page is according to product specification. You may not see all options if your product doesn't support all of them.

## SBAS

SBAS is Satellite-Based Augmentation Systems that is used to improve accuracy of location data. There are several SBAS systems for different areas in the world.

SBAS	AREA COVERAGE
EGNOS	Europe
WAAS	North America
GAGAN	India
MSAS	Japan

Please note this option is hardware dependent. You may not see this option if your product doesn't support it.

### Assisted GPS

Assisted GPS (as known as A-GPS) is used for speeding up location fix, especially when satellite signal is weak. If activating this option, gateway will download almanac data from A-GPS server through IP network instead of from satellite. You can also choose different valid period of almanac data. The shorter almanac data will get higher accuracy. However, the almanac data with shorter valid period needs to be updated more frequently. It will consume more network bandwidth. Please note this option is hardware dependent. You may not see this option if your product doesn't support it.

### Data to Storage

Besides transmitting location data to remote server, you can also store location data into internal storage (e.g. microSD card) or external storage (e.g. USB drive) if any. Regarding to data format, either can be NMEA 0183 raw data format or save it as GPX file format. The location data will be saved to a new file if the original file size is bigger than the pre-defined file size. The "Download log file" button allows you to browse all saved log files and download to your personal devices.

#### 4.1.1 Scenario of location tracking for fleet management

A fleet owner would like to see the locations of his trucks in real time. He also likes to know where his trucks have been passed through with time information. In his operation office, there is a server (IP: 100.100.100.1) which can interpret NMEA RMC data format and shows truck's location and track on map. This server is listening on TCP port 888 to receive NMEA RMC packet from trucks. IMEI number will be added before NMEA RMC data for identification of each truck. Hereunder is the configuration on each truck.

#### Basic Settings:

CONFIGURATION PATH	[GNSS]-[CONFIGURATION]
GNSS	Enable
GNSS Type	GPS
GPS Message Types	RMC
SBAS	Enable
Assisted GPS	Enable, 1
Data to Storage	Disable

### Settings for Remote Host:

CONFIGURATION PATH	[GNSS]-[REMOTE HOST CONFIGURATION]
Host Name	Truck-1
Host IP	100.100.100.1
Protocol Type	TCP
Port Number	888
Interval(s)	15
Prefix Message	123456789012345
Suffix Message	[blank]
Enable Checkbox	[Checked]

Go to Service > Location Tracking > GNSS Tab.

The GNSS allows user to set the configuration of GNSS, log NMEA data to storage, and send data to remote host. Ensure GNSS is enabled and saved.

### Setup GNSS Configuration

Configuration	
Item	Setting
▶ GNSS	<input type="checkbox"/> Enable
▶ GNSS Type	GPS ▼
▶ GNSS Message Types	<input type="checkbox"/> GGA <input type="checkbox"/> GLL <input type="checkbox"/> GSA <input type="checkbox"/> GSV <input type="checkbox"/> RMC <input type="checkbox"/> VTG
▶ SBAS	<input checked="" type="checkbox"/> Enable
▶ Assisted GPS	<input checked="" type="checkbox"/> Enable 1 ▼ day Differential Almanac Corrections
▶ Data to Storage	<input type="checkbox"/> Enable    Select Device: Internal ▼ Interval: 5 (s) Data format: GPX ▼ Data file name: GPX_yyyyMMddhhmm Split file: <input type="checkbox"/> Enable    Size: 200 KB ▼ ▼    Download log file

GNSS CONFIG. ITEM	VALUE SETTING	DESCRIPTION
GNSS Enable	The box is unchecked by default	Check Enable box to activate GNSS functions.
GNSS Type	GPS is selected by default	Select a GNSS Type (GNSS System) that you want to use. Please note this option is hardware dependent. The available options of GNSS type show on this page is according to product specification. You may not see all of these four options if your product doesn't support all of them.
GPS Message Types	The box is unchecked by default	Select one or more GNSS Message Types that you want to use for transmitting or recording GPS data. There are many sentences in the NMEA standard for selecting, GGA, GLL, GSA, GSV, RMC and VTG. ALL Other includes DTM, GNS, GRS, GST, ZDA, and GBS sentences. Only select the type you need, otherwise it will consume unnecessary network bandwidth.
SBAS	The box is unchecked by default	Check Enable box to activate satellite-based augmentation system (SBAS). Note: Some devices do not support this function.
Assisted GPS	The box is checked by default	Check Enable box to activate Assisted GPS (A-GPS). Select the duration for downloading the Differential Almanac Corrections data from A-GPS server through IP network. Note: Some devices may not support this function.

Data to Storage	The box is unchecked by default	<ul style="list-style-type: none"> <li>• Enable (The box is unchecked by default Check Enable box to activate data to storage function.</li> <li>• Select Device (A Must filled setting)Select Internal or External device to store log data.</li> <li>• Interval (A Must filled setting). Specify the time interval between two continuous data log. By default, 5 second is set. Value Range: 5 ~ 60 seconds.</li> <li>• Data Format (A Must filled setting). Select data format (RAW, or GPX) to store.</li> <li>• Data file name(A Must filled setting).Define file name to store.</li> <li>• Split Enable. Check Enable box to activate file splitting function.</li> <li>• Split Size&amp; Unit. Define file size and unit for log file. By default, 200 KB is defined. Value Range: &gt;= 10KB (Minimum file size is 10 KB).</li> <li>• Download log file. Select a log file and Click Download log file to download through Web GUI. If the log format which is specified to download is GPX, we will convert standard GPX format for used.</li> </ul>
Save	NA	Click the Save button to save the configuration.

### Create/Edit Remote Host

The Remote Host allows you to customize your rules for sending NMEA data to specific IP address and Port. The router supports up to a maximum of 10 rule sets.

Remote Host List <span>Add</span> <span>Delete</span>									
ID	Host Name	Host IP	Protocol Type	Port Number	Interval(s)	Prefix Message	Suffix Message	Enable	Actions

When Add button is applied, Remote Host Configuration screen will appear.

Remote Host Configuration	
Item	Setting
▶ Host Name	<input type="text"/>
▶ Host IP	<input type="text"/>
▶ Protocol Type	TCP ▼
▶ Port Number	<input type="text"/>
▶ Interval(s)	1 <input type="text"/>
▶ Prefix Message	<input type="text"/>
▶ Suffix Message	<input type="text"/>
▶ Enable	<input type="checkbox"/>

REMOTE HOST CONFIG. ITEM	VALUE SETTING	DESCRIPTION
Host Name	String format: any text	Enter the host name for the designated remote host. Value Range: -1 ~ 64 characters.
Host IP	A Must filled setting	Specify the IP Address of remote host. It will be use as destination IP for sending NMEA packets.
Protocol Type	TCP is selected by default	Specify the Protocol (TCP or UDP) to use for sending NMEA packets.
Port Number	A Must filled setting	Specify a Port Number as destination port for sending NMEA packets. Value Range: 1 ~ 65535.
Interval(s)	A Must filled setting	Check Enable box to activate Assisted GPS (A-GPS). Select the duration for downloading the Differential Almanac Corrections data from A-GPS server through IP network. Note: Some devices may not support this function.
Prefix Message	String format: any text	Specify optional prefix string with specific information if your backend server can recognize. For example, you can input the IMEI code of this device here, and then your backend server can recognize this GPS data is sent from this device. You can also leave this field blank.

Suffix Message	String format: any text	Specify optional suffix string with specific information if your backend server can recognize.
Enable	The box is unchecked by default	Check Enable box to activate this remote host rule.
Save	NA	Click the Save button to save the configuration.

## ● 5. System

In the System section you can check system related information and execute some system operations, define some time schedule rules, make object grouping, define external server objects and configure the operation parameters on Web UI surfing.

About system related, you can see system related information and system logs, use system tools for system update and do some network tests.

About Scheduling, you can define some time scheduling rules here to be applied at various applications in the device system. Whatever one application needs a time schedule, like the “Work Hours” is defined as AM8:00~PM5:00 from Monday to Friday, the time schedule object can be defined in the [System]-[Scheduling] section.

About Grouping, except for user group, the device also provides you to group some kinds of objects to be several groups. It supports three types of objects to be grouped. They are host objects, file extension objects and L7 Application objects. The grouping object can be defined in the [System]-[Grouping] section.

About External Servers, you can define some external server objects here to be applied at various applications in the device system. Whatever one application needs an external server, like a RADIUS server, the external server object can be defined in the [System]-[External Servers] section. These server objects include Email Server objects, Syslog Server objects, RADIUS Server objects, Active Directory Server objects, LDAP Server objects and UAM Server objects.

About MMI (Man-Machine Interface), it means the Web-based GUI. User can set the administrator timeout of Web UI surfing during configuring the device by the administrator.

### 5.1 System Related

System Related section includes “Change Password”, “System Information”, “System Status” and “System Tools”. Change Password is to change the password of administrator for configuring the device by using Web UI. System Tools support system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup. You also can check the system information and system status log here.

Change Password System Tools

**Change Password** [ Help ]

Old Password

New Password

New Password Confirmation

Save Undo

#### 5.1.1 Change Password

You can change the System Password here. We strongly recommend you to change the system password for security reason. Click on “Save” to store your settings or click “Undo” to give up the changes.



## Old Password

Input the old password of administrator.

## New Password

Input the new password of administrator for future logging in. Certainly, once the password is changed successfully, system will ask you login again with new password.

## New Password Confirmation

Re-type new password again here. It must be the same as the one in “New Password”; otherwise, an error message will be shown out.

### 5.1.2 System Tools

The device supports many system tools, including system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup.

Change Password

System Tools

System Web Log

View

Email Now

Web Log

Email Alert

☒ System ☒ Attacks ☒ Drop ☐ Debug Categories

☐ Enable

Server List: --- Option --- 

AddObject

E-mail Addresses:

E-mail Subject:

Syslogd

☐ Enable Server List: --- Option --- 

AddObject

System Tools

System Time

Configure

Sync with Time Server

Sync with my PC (Monday January 11, 2016 17:53:38)

Firmware Upgrade

Via Web UI 

Firmware Upgrade

Ping Test

Host IP:

Interface: Auto 

Ping

Tracert Test

Host IP:

Interface: Auto 

UDP

Traceroute

Reboot

Now 

Reboot

Reset to Default

Reset

Wake on LAN

Wake up

Backup Configuration Settings

Backup

Logout

Logout

## System Time

There are three approaches to setup the system time. Before the process, some basic information must be filled by clicking on the “Configure” command button. Basic information includes following items:

- Time Zone: Select a time zone where this device locates.
- Auto-Synchronization: Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time from the available list and by default, it is 132.163.4.102.
- Daylight Saving Time: Check the “Enable” checkbox to enable this function.
- Set Date & Time Manually: Set the date and time for system by manual. But Auto-Synchronization must be unchecked beforehand to do it.

Above is the first way to setup system date and time. That is, it is the manual way. The second way is “Sync with Timer Server”. Based on your selection of time server in basic information configuration, system will communicate with time server by NTP Protocol to get system date and time after you click on the button. The last way is “Sync with my PC”. Click on the button to let system synchronizes its date and time to the ones of the configuration PC.

## FW Upgrade

If new firmware is available, you can upgrade router firmware through the WEB GUI here. After clicking on the “FW Upgrade” command button, you need to specify the file name of new firmware by using “Browse” button, and then click “Upgrade” button to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.

NOTE: PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS PROCEEDING.

## Ping Test

This allows you to specify an IP / FQDN and the test interface, so system will try to ping the specified device to test whether it is alive after clicking on the “Ping” button. A test result window will appear beneath it. There is a “Close” command button there can let the test result windows disappear.

## Tracert Test

Trace route command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point. First, you need to specify an IP / FQDN, the test interface and used protocol number. Used protocol number is either “UDP” or “ICMP”, and by default, it is “UDP”. Then, system will try to trace the specified device to test whether it is alive after clicking on the “Traceroute” button. A test result window will appear beneath it. There is a “Close” command button there can let the test result windows disappear.

## Reboot

You can also reboot this device by clicking the “Reboot” button.

## Reset to Default

You can also reset this device to factory default settings by clicking the “Reset” button.

## Wake on LAN

Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the “Wake up” command button.

## Backup Configuration Settings

You can backup your settings by clicking the “Backup” button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

## 5.2 Scheduling

You can set the schedule time to decide which service will be turned on or off. The added rules will be listed as below and they can be up to 100 rules.

The screenshot displays the 'Schedule Settings' configuration page. At the top, there's a tab labeled 'Schedule Settings'. Below it, the 'Configuration' section contains a 'Time Scheduling' option with a checkbox that is currently checked, labeled 'Enable'. Underneath, the 'Time Schedule List' section is visible, featuring 'Add' and 'Delete' buttons. At the bottom right of the configuration area, there are 'Save' and 'Refresh' buttons.

### Enable

Enable or disable the scheduling function.

## Add New Rule

To create a schedule rule, click the “Add New” button or the “Add New Rule” button at the bottom. When the next dialog popped out you can edit the Name of Rule, Policy, and set the schedule time (Week day, Start Time, and End Time). In a schedule rule, it collects 8 time periods to organize it. You also can specify the rule is to define the enable timing (“Inactive except the selected days and hours below”) or disable timing (“Active except the selected days and hours below”).

**Schedule Settings**

**Time Schedule Configuration**

Rule Name

Rule Policy Inactivate ▼ the Selected Days and Hours Below.

**Time Period Definition**

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
2	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
3	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
4	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
5	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
6	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
7	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
8	-- choose one -- ▼	<input type="text"/>	<input type="text"/>

Afterwards, click “save” to store your settings or click “Undo” to give up the changes.

## 5.3 MMI

### 5.3.1 Web UI

**Web UI**

**Others** [ Help ]

Administrator Time-out  seconds (0 to disable)

You can set UI administration time-out duration in this page. If the value is “0”, means the time-out is unlimited.

# APPENDIX A: LICENSING INFORMATION

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

## Availability of source code

Please visit our web site or contact us to obtain more information.

## GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program

proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License (exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement).

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- Accompany it with the information you received as to the offer to distribute corresponding source code (this alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above).

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies,

or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may



differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,

INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## END OF TERMS AND CONDITIONS