multimax
HSPA+ Dual Port M2M Router | MA-2040

multimax+
4G Dual Port Router | MA-2040-4G

Dual Port, Dual SIM Industrial Cellular Router + 4G

User Guide V1.03

Table of Contents

CONTACT INFORMATION

In keeping with Maxon's dedicated customer support policy, we encourage you to contact us.

TECHNICAL:

Hours of Operation: Monday to Friday 8.30am to 5.30pm*
Telephone: +61 2 8707 3000
Facsimile: +61 2 8707 3001
Email: support@maxon.com.au * Public holidays excluded

SALES:

Hours of Operation: Monday to Friday 8.30am to 5.30pm*
Telephone: +61 2 8707 3000
Facsimile: +61 2 8707 3001
Email: sales@maxon.com.au * Public holidays excluded

WEBSITE: www.maxon.com.au

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the router are used in a normal manner with a well-constructed network, the router should avoid situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Maxon accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data.

Safety Precautions

General

- The router generates radio frequency (RF) power. When using the router care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your router in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Ensure that the router does not interfere with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, or any large obstacles such as concrete walls etc.
- An external antenna must be connected to the router for proper operation.
- Always keep the antenna with minimum safety distance of 26.6 cm or more from the human body. Do not put the antenna inside metallic box, containers, etc.

***Note**: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. The router may be used at this time.*

Using the router in a vehicle

- Check for any regulation or law authorising the use of cellular equipment in vehicles in your country, territory or state before installing the router.
- The driver or operator of any vehicle must refrain from operating the router while in control of a vehicle.
- Installation of the router should be performed by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the router.
- The router should be connected to the vehicle's supply system by using a fuse-protected terminal in the vehicle's fuse box.
- Use caution when powering the router by the vehicle's main battery. The battery may be drained after an extended period of using the router.

Protecting your router

- To ensure error-free usage, please install and operate your router with care.
- Avoid exposing the router to extreme conditions such as high humidity / rain, high temperatures, direct sunlight, caustic / harsh chemicals, dust, or water.
- There are no user serviceable parts inside. Do not try to disassemble or modify the router. Doing so would void the warranty.

- Avoid dropping, hitting or shaking the router. Please refrain from using the router under extreme vibrating conditions.
- When removing the antenna or power supply cables, you must first hold the connection before you do so.
- Connect the router only according to the instruction manual. Failure to do so would void the warranty.
- In the event of any problems, please contact Maxon Australia Pty Ltd.

RF EXPOSURE COMPLIANCE

The use of this device in any other type of host configuration may not comply with the RF exposure requirements and should be avoided. During operation, a 20 cm separation distance should be maintained between the antenna, (whether extended or retracted), and the user's/bystander's body excluding hands, wrists, feet, and ankles to ensure RF exposure compliance.

Caution

Change or modification without the express consent of Maxon Australia Pty Ltd voids the user's authority to use the device. These limits are designed to provide reasonable protection against harmful interference in an appropriate installation. The modem is a transmitting device with similar output power to a mobile phone. This device can generate, use, and radiate radio frequency energy, if not used in accordance with instructions it can cause harmful radiation to radio communication. The device is approved for use with the antenna: **ANT-SMA**. Unauthorized antennas, modifications, or attachments could impair call quality, damage the device, or result in violation of RF exposure regulations.

There is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference in radio and television reception, which can be determined by turning the equipment on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving radio or TV antenna
- Increase the separation distance between the equipment and the receiver
- Contact Maxon Australia Technical Support for assistance

Notes The user is cautioned that changes or modifications not expressly approved by Maxon Australia could void the warranty.

* The product must be used by a limited power source or appropriate power supply provided. Otherwise, safety will not be ensured.

Potentially Unsafe Areas

Posted Facilities: Turn off this device in any facility or area where posted notices require you to do so.

Blasting Areas: Turn off your device where blasting is in progress. Observe restrictions and follow any regulations or rules.

Potentially Explosive Atmospheres: Turn off your device when you are in any area with a potentially explosive atmosphere. Obey all signs and instructions. Sparks in such areas could cause an explosion or fire, resulting in bodily injury or death.

Areas with a potentially explosive atmosphere are often but not always clearly marked. They include:

- Fuelling areas such as gas or petrol stations
- Below deck on boats
- Transfer or storage facilities for fuel or chemicals
- Vehicles using liquefied petroleum gas, such as propane or butane
- Environments that contain chemicals or particles such as grain, dust or metal powders
- Avoid using the router in areas that emit electromagnetic waves or enclosed metallic structures, e.g. lifts or any other area where you would normally be advised to turn off your engine

Document Version Control

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Product	Multimax Industrial Ethernet Router
Model	MA-2040, MA-2040-4G
Document Type	PDF
Current Version Number	1.03
Status of the Document	Public Release
Revision Date	July 2014
Total Number of Pages	135

Release Date	Firmware Version	Details
2013-01-24	1.00	First Release.
2013-03-15	1.01	Update firmware; Add configuration examples.
2014-05-19	1.02	4G additions/changes
2014-06-02	1.03	Added new features introduced in new firmware. Screenshots updated accordingly.

Chapter 1. Product Introduction

1.1 Overview

The Maxon Multimax MA-2040 / MA-2040-4G is a rugged cellular router offering state-of-the-art mobile connectivity for (M2M) machine-to-machine applications. It includes the following specifications;

- Dual SIM redundancy for continuous cellular connection supports 2G/3G/4G[1].
- Optional diversity antenna for improved fringe performance.
- Two Ethernet ports can be configured as two LANs or (one LAN, one WAN) , supports wireless WAN and wired WAN backup.
- One RS232, one RS485, one console port, two digital inputs, two digital outputs, one high speed USB host up to 480 Mbps.
- Six LED indicators provide status and signal strength (RSSI).
- Wide range input voltages from 9 to 60 VDC and wide operating temperature range from-40 to 85 °C.
- The metal enclosure can be mounted on a DIN-rail or on the wall, with extra ground screw.
- Network protocols including PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, DMZ, RIP, OSPF, DDNS, VRRP, HTTP, HTTPs.
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP client/server, GRE.
- Management via Web, CLI, SNMP.
- Supports Modbus/RTU to Modbus/TCP gateway.
- Auto reboot during a preset time of day.
- Firmware upgrade via web interface and supports FOTA.

[1] 4G is available with MA2040-4G Model.

1.2 Packing List

Check your package to make certain it contains the following items:

- Maxon Multimax MA-2040 or MA-2040-4G router (x 1)

- SMA antenna (x 2)

- 3-pin pluggable terminal block with lock for power connector (x 1)

- 7-pin pluggable terminal block with lock for I/O (x 1)

- Ethernet cable (x 1)

- CAB-4475 Phoenix Connector to DB9 Cable

- Wall Mounting Kit

- CD with user guide (x 1)

***Note**: Please notify your sales representative if any of the above items are missing or damaged.*

Optional accessories (can be purchased separately):

- 35mm Din-Rail mounting kit

- AC/DC Power Supply Adapter (12VDC, 1.5A) x 1
  (AU plug standard, EU, US, UK plugs optional)

1.3 Specifications

Cellular Interface

- Standards: GSM/GPRS/EDGE/UMTS/HSPA/FDD LTE[1]
- GSM/GPRS/EDGE: 850/900/1800/1900 MHz
- HSPA: 850/900/1900/2100 MHz, DL 7.2,UL 5.76 Mbps, fall-back to 2G
- HSPA+: 850/900/1900/2100 MHz, DL 21,UL5.76 Mbps, fall-back to 2G
- FDD LTE[1]: 800/900/1800/2100/2600 MHz, DL, 100 UL 50 Mbps, fall-back to 3G/2G
- DUAL SIM: 2 x (3V & 1.8V)
- Antenna Interface: SMA Female, 50 ohms impedance

[1] FDD LTE for MA-2040-4G model only

Ethernet Interface

- Ports: 2 x (10/100 Mbps), can be used as (2x LANs) or (1x LAN, 1x WAN)
- Magnet Isolation Protection: 1.5kV

Serial Interface

- Ports: 1 x RS-232, 1 x RS-485
- ESD Protection: 15kV
- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- Baud Rate: 2000bps to 115200bps
- Flow Control: RTS/CTS, XON/XOFF
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B), GND
- Interface: 3.5mm terminal block with lock

Digital Input

- Type: 2 x DI, Dry Contact
- Dry Contact: (On: short to GND/V-), (Off: open)
- Isolation: 3kVDC or 2kVRMS
- Digital Filtering Time Interval: Software selectable
- Over-voltage Protection: 36VDC
- Interface: 3.5mm terminal block with lock

Digital Output

- Type: 2 x DO, Sink
- Over-voltage Protection: 40VDC
- Over-current Protection: 0.5 A
- Isolation: 3kVDC or 2kVRMS
- Interface: 3.5mm terminal block with lock

System

- LED Indicators: 6 indicators include, (RUN, PPP, USR, RSSI, NET, SIM)
- Built-in RTC, Watchdog, Timer
- Expansion: 1 x USB 2.0 high speed host, (up to 480Mbps)
- Storage: 1 x Micro SD, (up to 2GB)

Software

- Network protocols: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, DMZ, RIP v1/v2, OSPF, DDNS, VRRP, HTTP, HTTPs, DNS, ARP, SSH, SNTP, Telnet
- LinkGo: PPP LCP (Echo/Reply), ICMP to keep always online
- VPN tunnel: IPSec, OpenVPN, PPTP, L2TP, GRE
- Firewall: SPI, anti-DoS, Filter, Access Control
- Management: Web, CLI, Telnet, SNMP (v1/v2/v3)
- Serial Port: TCP client/server, UDP, Virtual COM

Power Supply and Consumption

- Power Supply Interface: 5mm terminal block with lock
- Input Voltage: 9 to 60 VDC
- Power Consumption: Idle: 180 mA (@ 12 V)
  Data Link: 500 to 1000 mA @ 12 V

Physical Characteristics

- Housing & Weight: Metal, 500g
- Dimension: (L x W x H): 125 x 108 x 45 mm
- Installation: 35mm Din-Rail or wall mounting or desktop

Environmental Limits

- Operating Temperature & Humidity:
  MA-2040: (-40 to 85°C), (5 to 95% RH)
  MA-2040-4G: (-40 to 85°C), (5 to 95% RH)
- Storage Temperature: (-40 to 85°C)

Regulatory and Type Approvals

- Approvals & Directives: CE, FCC, PTCRB, A-Tick, RoHS, WEEE
- EMC: EN 61000-4-2 (ESD) Level 4, EN 61000-4-3 (RS) Level 4
  EN 61000-4-4 (EFT) Level 4, EN 61000-4-5 (Surge) Level 3
  EN 61000-4-6 (CS) Level 3, EN 61000-4-8, EN 61000-4-12

1.4 Selection and Ordering Information

Please refer to MA-2040 / MA-2040-4G Specifications and Packing List above.

2.1 LED Indicators

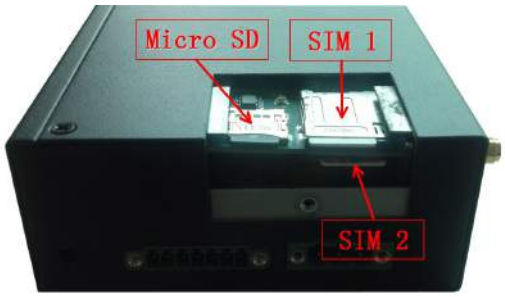
Name	Colour	Function
RUN	Green	Indicates the system status. Blinking: Router is up and running. On: Router is starting. Off: Router is powered off.
PPP	Green	Indicates the PPP connection status. On: PPP connection is established. Off: PPP connection has dropped or failed.
USR	Green	Indicates the status of VPN, PPPoE, or DynDNS by user selection. On: the selected function is active. Off: the selected function is inactive.
RSSI	Green	Signal level: 21-31 (Perfect signal level)
	Yellow	Signal level: 11-20 (Normal signal level)
	Red	Signal level: 1-10 (Bad signal level)
NET	Green	Operating on 4G (4G model only).
	Yellow	Operating on 3G.
	Red	Operating on 2G.
	Off	Not registered to any network
SIM	Green	SIM 1 inserted. On: SIM1 works normally. Blinking: SIM 1 inserted but failing to work, e.g. incorrect PIN code
	Yellow	SIM 2 inserted. On: SIM 2 works normally. Blinking: SIM 2 inserted but failing to work, e.g. incorrect PIN code
	Off	No SIM inserted.

2.2 Mounting the Router

Use 2 x M3 screw to mount the router on the wall.

Or mount the router on a DIN rail with optional kit.

2.3 Installing SIM Card/s and Micro SD Card



- **Inserting SIM Card or Micro SD Card**

1. Make sure the power supply is disconnected.
2. Unscrew and remove the cover for SIM and Micro SD Card to find the SIM and Micro SD slot.
3. Insert the SIM card or Micro SD card and press the card with fingers until you hear a “clicking” sound.
4. Put the cover back on and screw firmly.

- **Removing SIM Card or Micro SD Card**

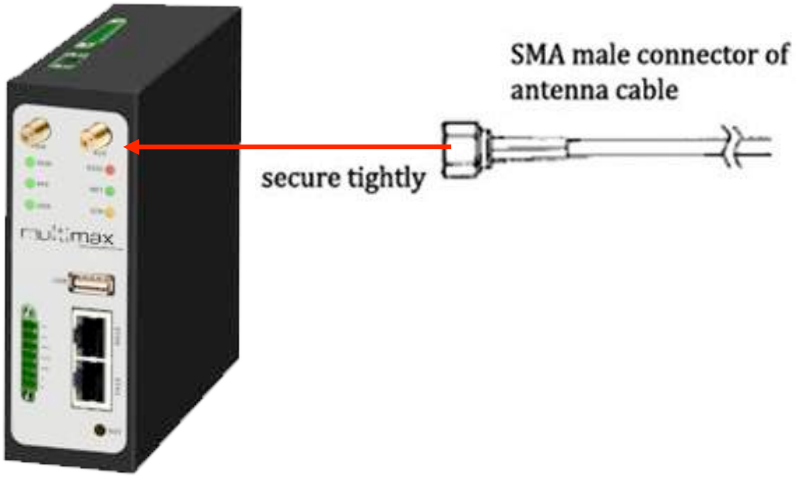
1. Make sure the router is powered off.
2. Unscrew and remove the cover for SIM and Micro SD Card.
3. Press the card until you hear “a clicking sound” and the card will pop out for removal from the slot.

Note:

1. Never operate the router without the SIM card cover installed.
2. Avoid touching the metal surface of the SIM card to avoid damage or loss of information in the card.
3. Avoid bending or scratching your SIM card. Keep the card away from any strong electromagnetic fields.
4. Make sure to disconnect the power source from your router before inserting or removing SIM or Micro SD cards.

2.4 Connecting the External Antenna (SMA Type)

Connect this to an external antenna with an SMA male connector. Make sure the antenna is for the correct frequencies as specified by your GSM/3G/4G operator (and supported by the modem) with an impedance of 50 ohms, and also that connector is secure and tight. Auxiliary antenna connection is optional but recommended.

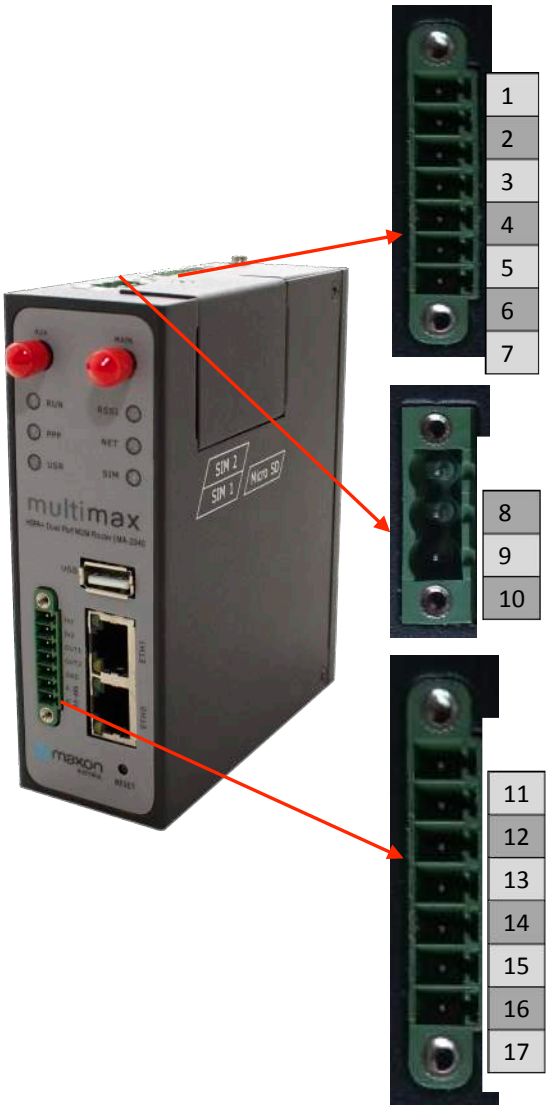


2.5 Grounding

Grounding and cable routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the grounding screw to the grounding point prior to the connection of devices.

Note: This product is intended to be mounted to a well-grounded mounting surface, such as a metal panel.

2.6 PIN assignments



PIN	Debug	RS232	Power	Digital I/O	RS485
1	RXD				
2	TXD				
3	GND	GND			
4		TXD			
5		RXD			
6		RTX			
7		CTX			
8			Positive		
9			Negative		
10			GND		
11				Input 1	
12				Input 2	
13				Output 1	
14				Output 2	
15				GND	
16					Data+(A)
17					Data- (B)

Note: The power supply range is 9 to 60 VDC. Be aware of the polarity and refrain from reversing it.

2.7 Reset Button

Function	Operation
Reboot	Press and hold the button for 5 seconds when router is operating.
Restore to factory default settings	When router is operating, press and hold the button for 60 seconds until the three LEDs at the left side (RUN, PPP, USR) blink 5 times.

Chapter 3. Configuration settings over web browser

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Vista/7/8, etc. The product provides an easy and user-friendly interface for configuration.

There are various ways to connect the router, either through an external repeater/hub or connect directly to your PC. Ensure that your PC has an Ethernet interface properly installed prior to connecting the router.

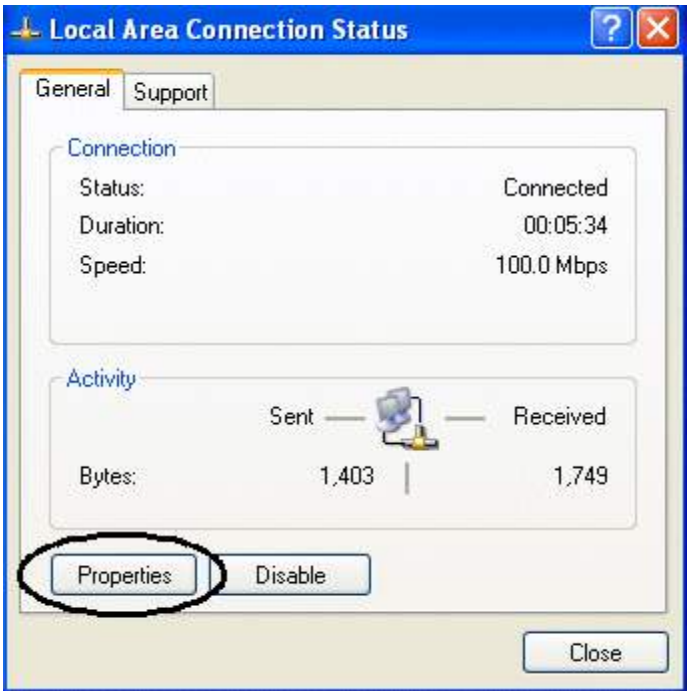
You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router web interface it is advisable to disable the firewall on your PC, as the firewall can disable access to the router.

3.1 Configuring PC in Windows

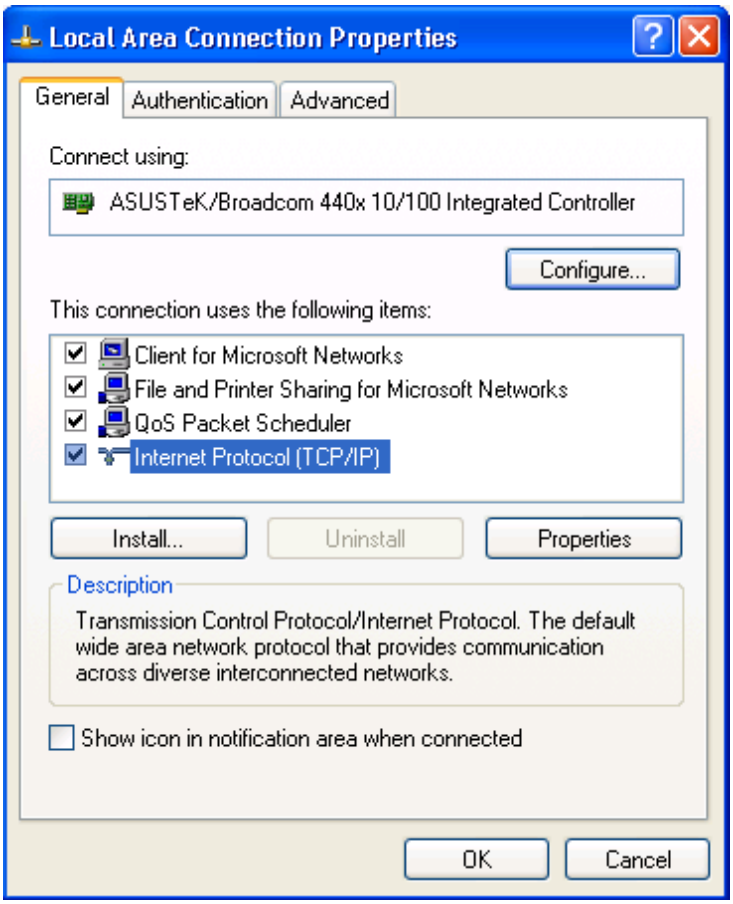
1. Go to Start / Control Panel (in Classic View). In the Control Panel, double-click Network Connections.

2. Double-click Local Area Connection.

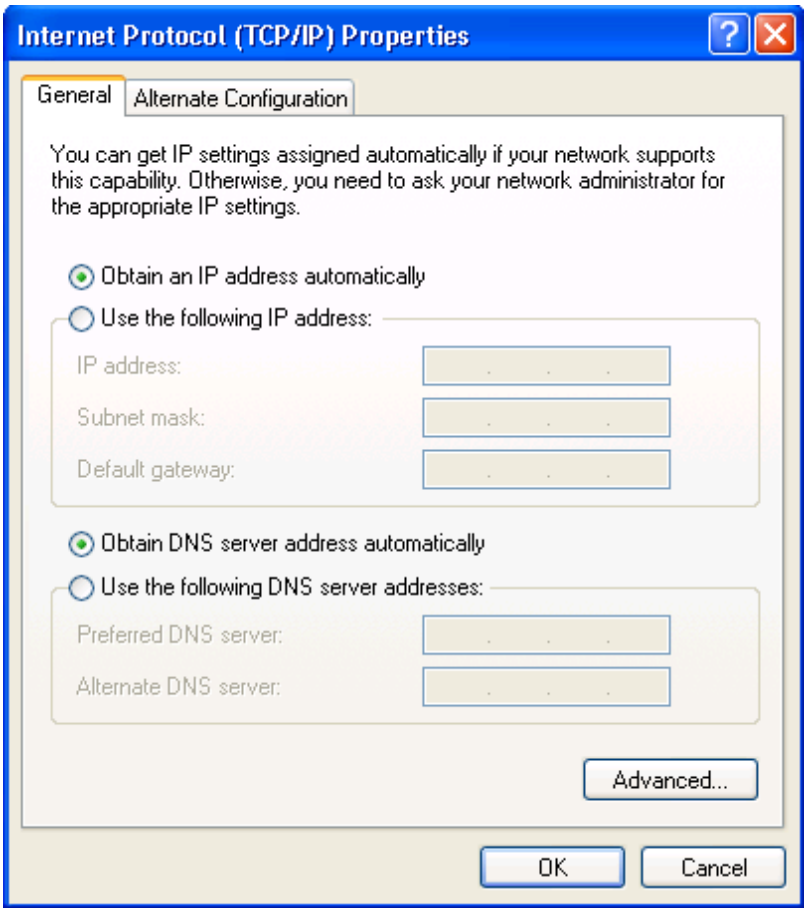
3. In the LAN Area Connection Status window, click Properties.



4. Select Internet Protocol (TCP/IP) and click Properties.



5. Select the “Obtain an IP address automatically” and “Obtain DNS server address automatically” radio buttons.



6. Click OK to finish the configuration.

3.2 Factory Default Settings of Multimax Ethernet Port

Before configuring your router, please familiarise yourself with following default settings.

Item	Description
Username	admin
Password	admin
Eth0	192.168.0.1/255.255.255.0, LAN mode
Eth1	192.168.0.1/255.255.255.0, LAN mode (Bridged)
DHCP Server	Enabled.

3.3 Control Panel

This section allows users to save configuration, reboot router, logout and select language.

Control Panel		
Item	Description	Button
Save	Click to save the current configuration into router's flash.	• Save
Reboot	Click to manually reboot the router. This is required after saving the modified configuration for the changes to take full effect.	• Reboot
Logout	Click to return to the login page.	• Logout
Language	Language Selection. English only.	• English
Refresh	Click to refresh the status.	Refresh
Apply	Click to apply the modifications on every configuration page.	Apply
Cancel	Click to cancel the modifications on every configuration page.	Cancel

Note: How to modify the device configuration:

1. Modify the configurations in the relevant page;
2. Click Apply within the page;
3. Repeat steps 1 & 2 for more modifications in the relevant pages if required;
4. After completing all modifications, Click • Save ;
5. Click • Reboot .

3.4 Status -> System

This section displays the router system status, which shows useful pieces of information such as the LED information, Router information, Current WAN Link and Cellular Information.

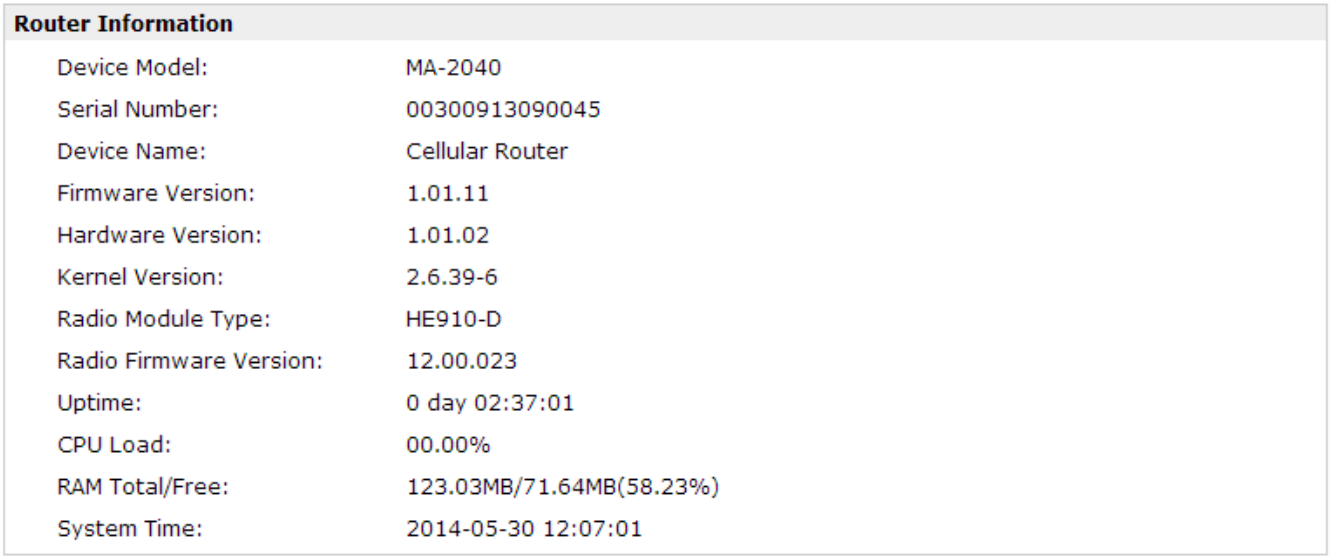
LED Information

For a detailed description, please refer to 2.1 LED Indicators.

Name	Color	Function
RUN	Green	Indicating the system status. Blinking: Router is up and running. On: Router is starting. Off: Router is power off.
PPP	Green	Indicating the PPP connection status. On: PPP connection is established. Off: PPP connection has dropped or failed.
USR	Green	Indicating the status of VPN, PPPoE, or DynDNS by user selection. On: the selected function is active. Off: the selected function is inactive.
RSSI	Green	Signal level: 21-31 (Perfect signal level)
	Yellow	Signal level: 11-20 (Normal signal level)
	Red	Signal level: 1-10 (Bad signal level)
NET	Green	Operating on the 4G network.
	Yellow	Operating on the 3G network.
	Red	Operating on the 2G network.
	Off	Not registered to any network
SIM	Green	SIM 1 inserted. On: SIM1 works normally. Blinking: SIM 1 inserted but fails to work, e.g. incorrect PIN code
	Yellow	SIM 2 inserted. On: SIM 2 works normally. Blinking: SIM 2 inserted but fails to work, e.g. incorrect PIN code
	Off	No SIM inserted.

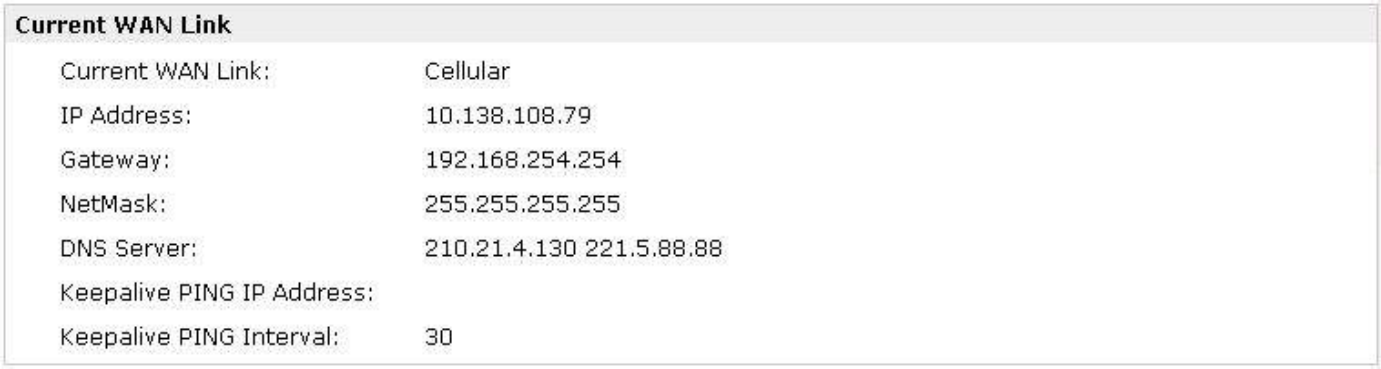
Router Information

Item	Description
Device Model	Model name of this device
Serial Number	Serial number of this device
Device Name	Device name to distinguish different devices you have installed.
Firmware Version	Current firmware version
Hardware Version	Current hardware version
Kernel Version	Current kernel version
Radio Module Type	Current radio module type
Radio Firmware Version	Current radio firmware version
Uptime	How long the router has been working since being powered on
CPU Load	Current CPU load
RAM Total/Free	Total capacity /Free capacity of RAM
System Time	Current system time



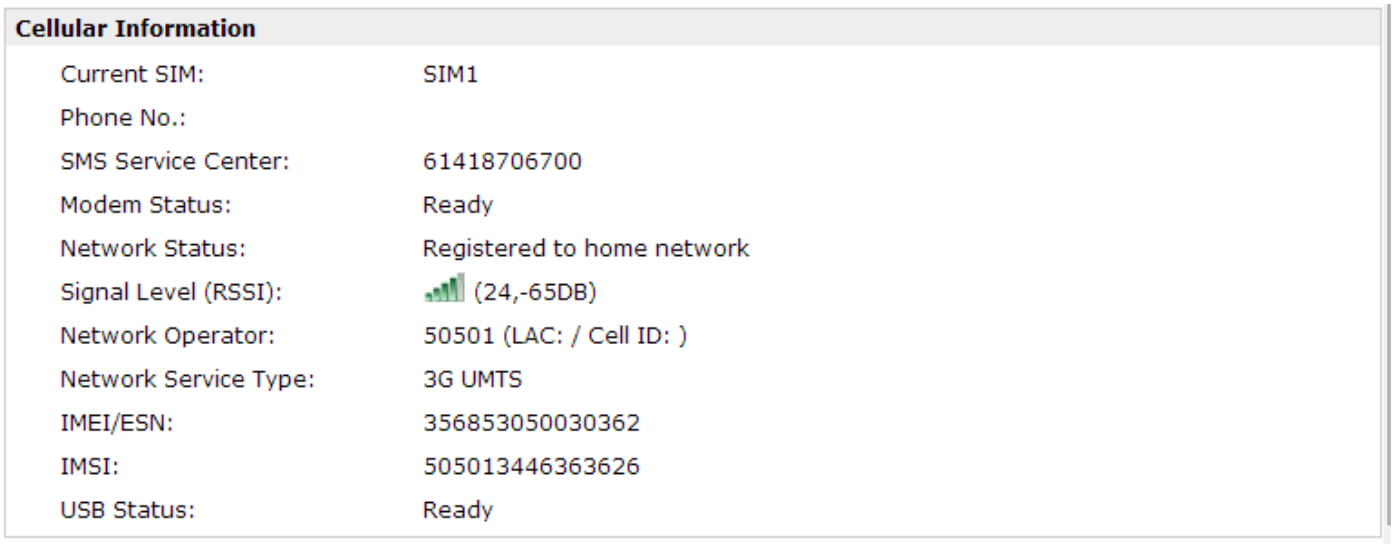
Current WAN Link

Item	Description
Current WAN Link	Current WAN link: Cellular or Eth
IP Address	Current WAN IP address
Gateway	Current gateway
Netmask	Current netmask
DNS Server	Current primary DNS server and Secondary server
Keeping PING IP Address	Current ICMP detection server which you can set in “Configuration->Link Management”.
Keeping PING Interval	ICMP Detection Interval (s) which can be set in “Configuration->Link Management”.



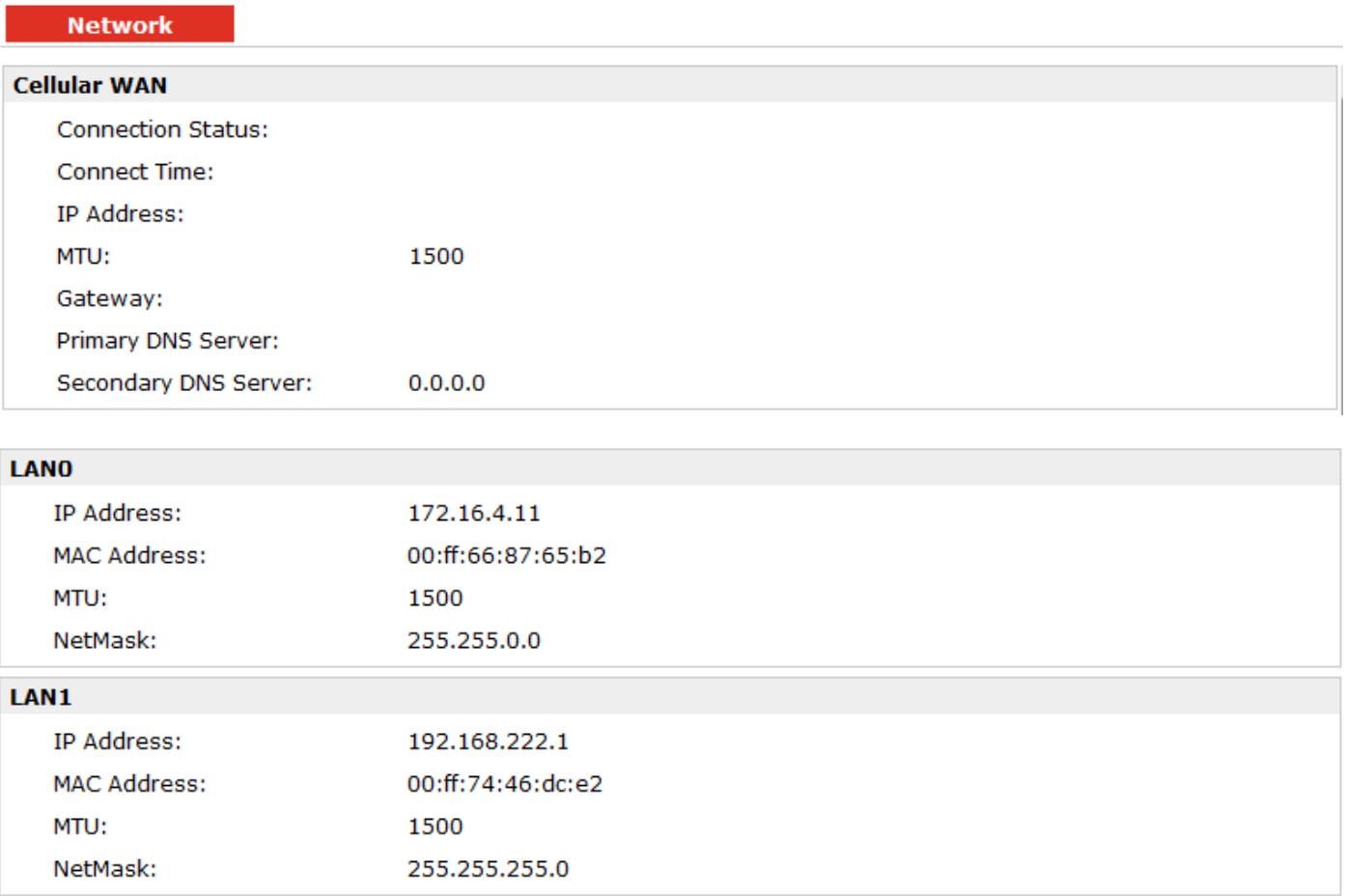
Cellular Information

Item	Description
Current SIM	The SIM card which the router currently uses: SIM1 or SIM2
Phone Number	Phone number of the current SIM
SMS Service Center	The SMS Service Center
Modem Status	Status of the modem. There are 8 different statuses: 1. Unknown. 2. Ready. 3. Checking AT. 4. Need PIN. 5. Need PUK. 6. Signal level is low. 7. No registered. 8. Initialize APN failed
Network Status	Current network state. There are 6 different states: 1. Not registered, ME is currently not searching for new operator! 2. Registered to home network. 3. Not registered, but ME is currently searching for a new operator. 4. Registration denied. 5. Registered, roaming. 6. Unknown.
Signal Level (RSSI)	Current signal level
Network Operator	Mobile Country Code (MCC) +Mobile Network Code (MNC), e.g. 46001. Also it will show the Location Area Code (LAC) and Cell ID
Network Service Type	Current network service type, e.g. UMTS.
IMEI/ESN	IMEI/ESN number of the radio module
IMSI	IMSI number of the current SIM
USB Status	Current status of USB host



3.5 Status -> Network

This section displays the route Network status, which includes status of Cellular, Eth0 and Eth1.



Note: ETH0 WAN information will not be shown if you select “Cellular Only” in “Configuration”->”Link Management”->”WAN Link”.

3.6 Status -> Route

This section displays the router's route table.

Route Table

Destination	NetMask	Gateway	Interface	Metric
172.16.0.0	255.255.0.0	0.0.0.0	eth0	0
192.168.1.0	255.255.255.0	0.0.0.0	eth1	0

3.7 Status -> VPN

This section displays the router VPN status, which includes IPsec, L2TP, PPTP and OpenVPN.

IPsec | L2TP | PPTP | OpenVPN

IPsec Status

No.	Tunnel name	Status	Connect Time
1		LINK_DOWN	
2		LINK_DOWN	
3		LINK_DOWN	

IPsec Detail Status

Show Detail Status

IPsec | L2TP | PPTP | OpenVPN

L2TP Client

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

L2TP Server

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

IPsec | L2TP | PPTP | OpenVPN

PPTP Client

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

PPTP Server

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

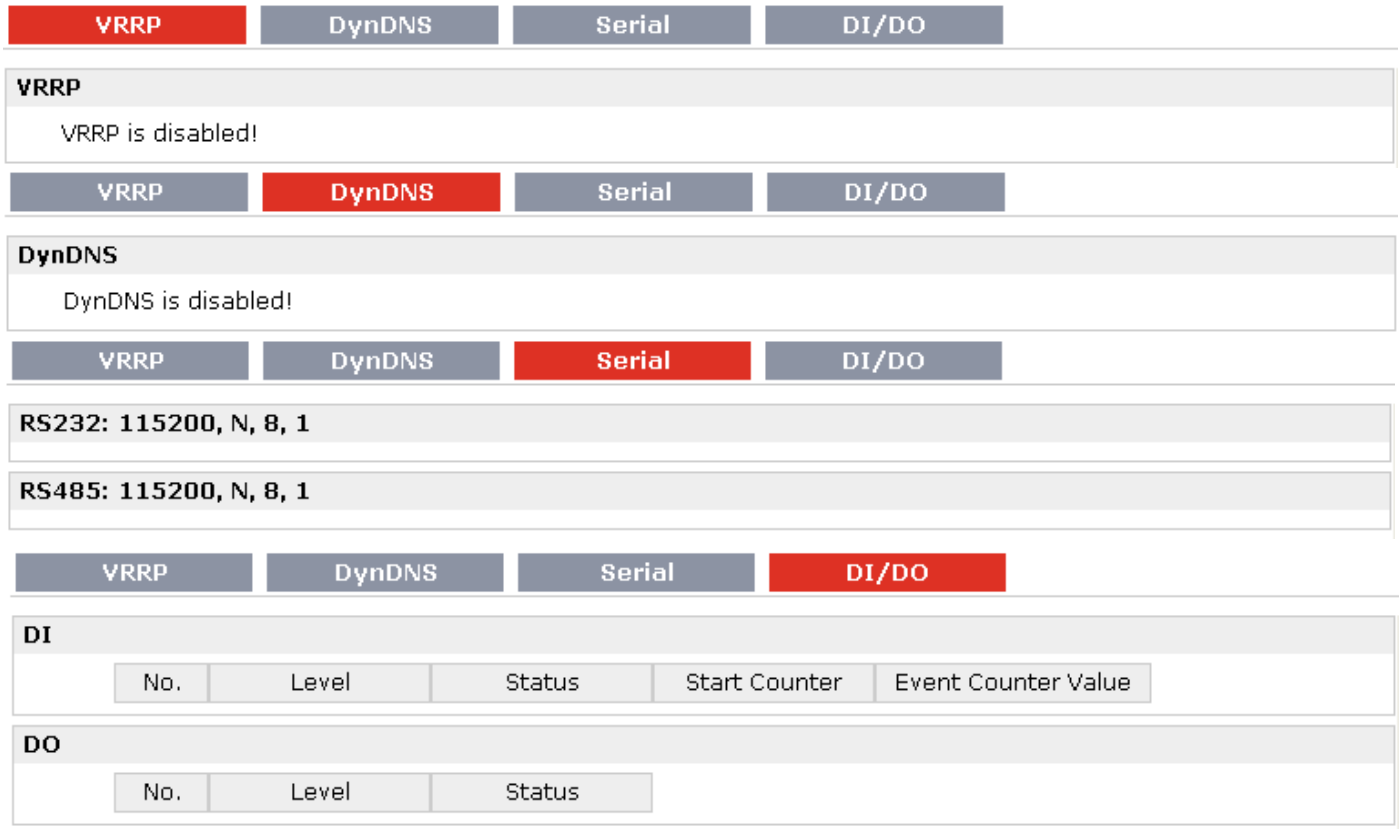
IPsec | L2TP | PPTP | OpenVPN

VPN Status

No.	Tunnel name	Status

3.8 Status -> Services

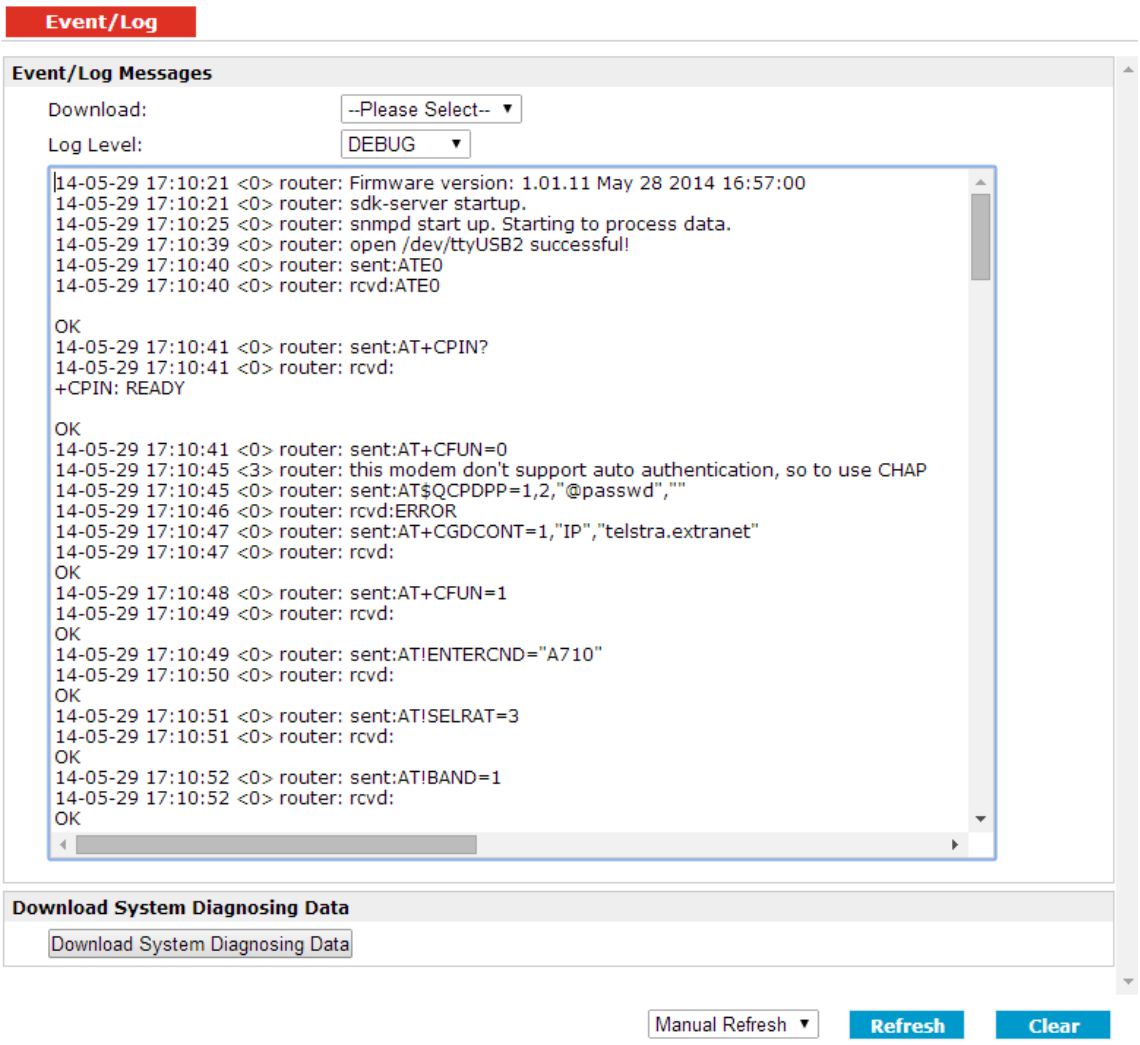
This section displays the router Services' status, including VRRP, DynDNS, Serial and DI/DO.



3.9 Status -> Event/Log

This section displays the router event/log information. You need to enable the router to output the log and select the log level first, then you can view the log information here.

Item	Description
Download	Select the log messages you want to download
Log Level	Select the Log level in the drop-down menu: DEBUG, INFO, NOTICE, WARNING, ERR, CRIT, ALERT, and EMERG.
Download System Diagnosing Data	Click "*Download System Diagnosing Data*" to download diagnostic file
Manual Refresh	Select from "5 Seconds", "10 Seconds", "15 Seconds", "30 Seconds" and "1 Minute". User can select these intervals to refresh the log information



3.10 Configuration -> Link Management

This section allows users to set the WAN link and the related parameters.

Link Management		
Item	Description	Default
Primary Interface	Selected from “Cellular”, “Eth0”. Cellular: Select Cellular as the primary WAN link. Eth0: Select Eth0 as the primary WAN link.	Cellular
Backup Interface	Selected from “None”, “Cellular”, “Eth0”. None: Do not use backup interface. Cellular: Select Cellular as the backup WAN link. Eth0: Select Eth0 as the backup WAN link. **Note**: Drop down list will not show the option that is already used for primary interface.	None
ICMP Detection Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	Null
ICMP Detection Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	Null
ICMP Detection Interval	Set the ping interval.	Null
ICMP Detection Timeout	Set the ping timeout.	30
ICMP Detection Retries	If the router pings the preset address/domain name time out continuously for Max Retries time, it will consider that the connection has been lost.	3
Reset The Interface	Enable to reset the cellular/ETH0 interface after the max ICMP detection retries.	3

Link Management

Link Management Settings

Primary Interface:	Cellular
Backup Interface:	None
ICMP Detection Primary Server:	8.8.8.8
ICMP Detection Secondary Server:	8.8.4.4
ICMP Detection Interval (s):	30
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3

☐ Reset The Interface

**It is recommended to use an ICMP detection server to keep router always online.*

**The ICMP detection increases the reliability and also cost data traffic.*

**DNS example: Google DNS Server 8.8.8.8 and 8.8.4.4*

3.11 Configuration -> Cellular WAN

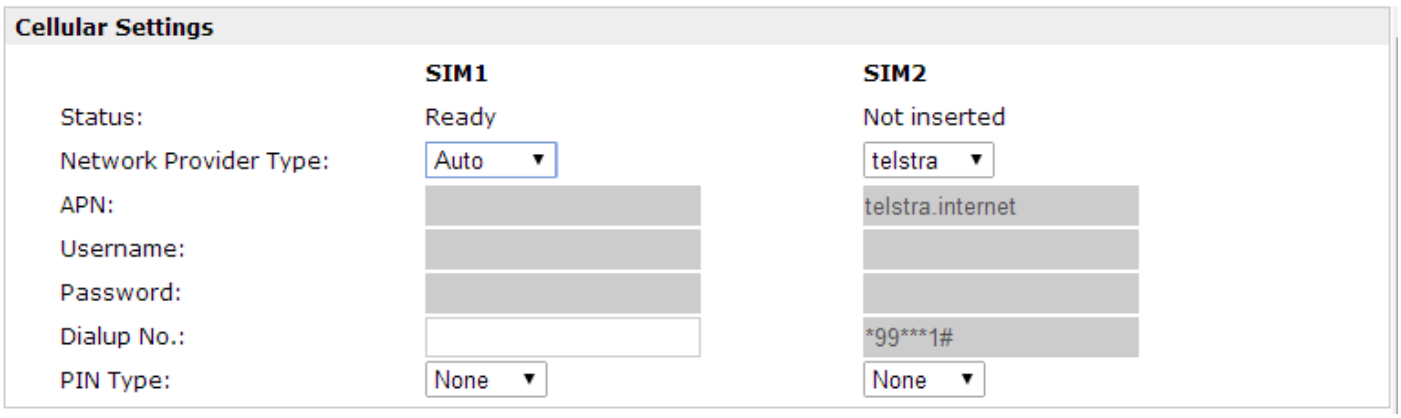
This section allows users to set the Cellular WAN and the related parameters.
Note: This section will not be displayed if you select “Eth0” as primary interface and no backup in “Configuration”->”Link Management”->”WAN Link”.

Basic Settings

Cellular WAN Settings		
Item	Description	Default
Network Provider Type	Select from “Auto”, “Custom” or the ISP name you preset in *“Configuration”->”Cellular WAN”->”ISP Profile”.* Auto: Router will get the ISP information from the SIM card, and set the APN, username and password automatically. This option only works when the SIM card is from well-known ISPs. Custom: Users need to set the APN, username and password manually.	Auto
APN	Access Point Name for cellular dial-up connection, provided by local ISP.	Null
Username	Username for cellular dial-up connection, provided by local ISP.	Null
Password	Password for cellular dial-up connection, provided by local ISP.	Null
Dialup No.	Dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
PIN Type	Select from “None”, “Input”, “Lock”, and “Unlock”. None: Select when SIM card does not enable PIN lock or PUK lock. Input: Select when SIM card has enabled with PIN lock or PUK. Correct PIN/PUK code need to be entered. Lock: Select when user needs to lock the SIM card with PIN or PUK code. Unlock: Select when user needs to unlock the SIM card with PIN or PUK code. **Note**: Please refer to your local ISP to see whether your SIM card requires PIN or not. If you wish to change the SIM PIN, please click the button to enable it, and then input the new PIN. You can go to tab “Status” -> “Event/Log” and search “AT+CPIN?” to check the status of SIM card.	Null

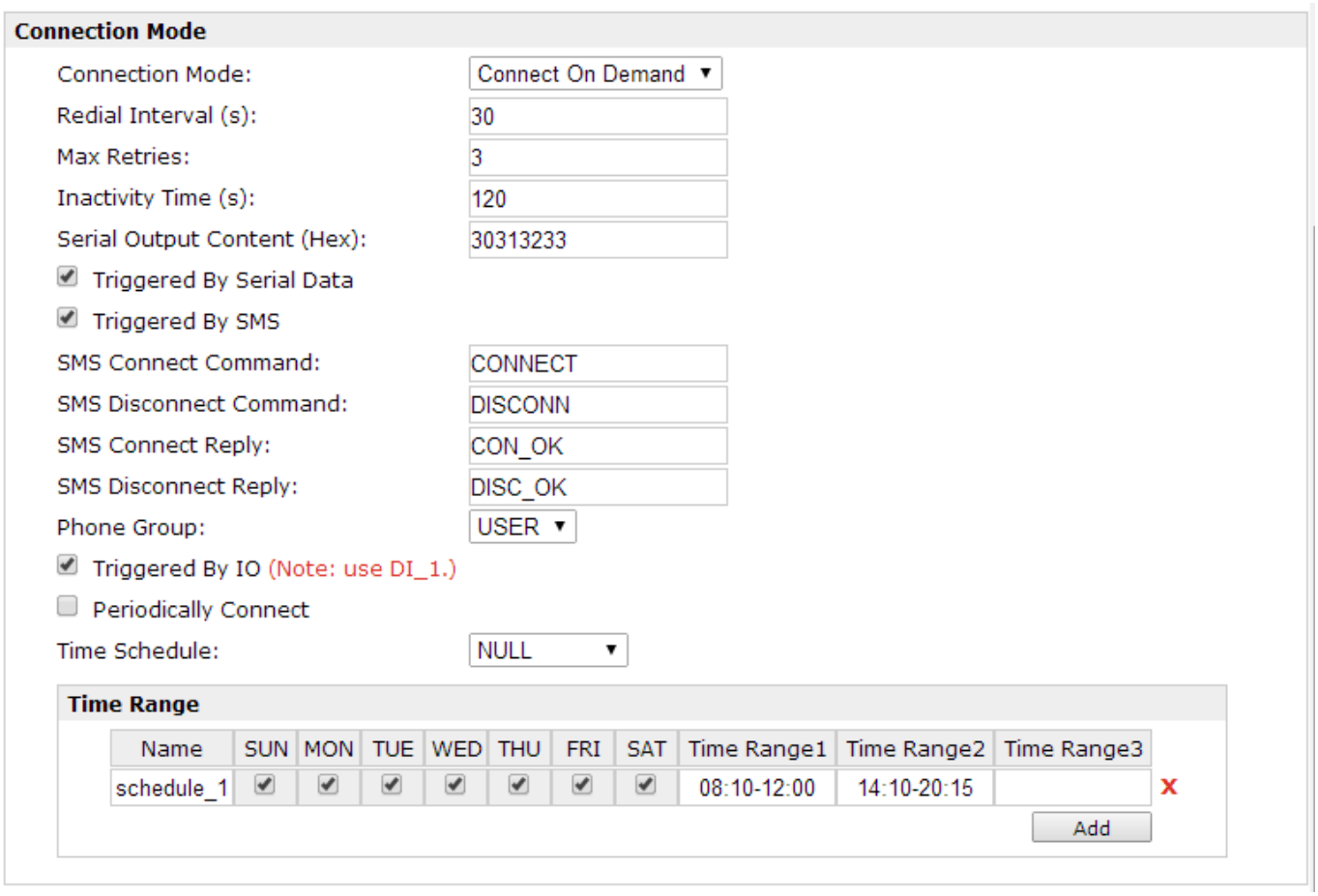
Connection Mode		
Connection Mode	Select from “Always Online” and “Connect On Demand”. Always Online: Auto activates PPP and keeps the link up after power on. Connect On Demand: After selecting this option, the user can choose from the following On Demand Connection Rules: Triggered by Serial Data, Triggered by SMS, Triggered by I/O, Triggered by Periodically Connect, and Triggered by Time Schedule. **Note**: If you select multiple on demand rules, the router only has to meet one of them to be triggered.	Always Online
Redial Interval (s)	Router will automatically re-connect with this interval (in seconds) when it fails to communicate with peer via TCP or UDP	30
Max Retries	The maximum number of retries for automatic re-connection in case the router fails to dial up. After the number is reached, the router will reboot the cellular module. If it still fails to dial up, the router will switch to the backup SIM card for re-connection and the maximum number of retries still applies. Once connection is successful, the Max Retries counter will be reset.	3
Inactivity Time (s)	Configurable under “Connect On Demand” mode. This field specifies the idle time in seconds for cellular auto-disconnection and reverting back to preferred SIM card. 0 means timeless.	0
Serial Output Content	The content that is sent by the serial device connected to the router to trigger PPP connection/disconnection under “Connect On Demand” mode. The content must be in HEX values.	Null
Triggered by Serial Data	Tick this checkbox to allow PPP connection or disconnection when data comes into the serial port and matches the preset Content.	Disabled
Triggered by Tel	Tick this checkbox to allow PPP connection or disconnection when making a voice call to router. **Note**: This function is not supported by the 4G model.	Disabled
Triggered by SMS	Tick this checkbox to allow PPP connection or disconnection when a specific SMS is received.	Disabled
SMS Connect Command	Users shall send this specific SMS to trigger PPP connection.	Null
SMS Disconnect Command	Users shall send this specific SMS to trigger PPP disconnection.	Null
SMS Connect Reply	When PPP is connected, an SMS specified here will be sent to preset users (set in the Phone Group).	Null
SMS Disconnect Reply	When PPP is disconnected, an SMS specified here will be sent to preset users (set in the Phone Group).	Null

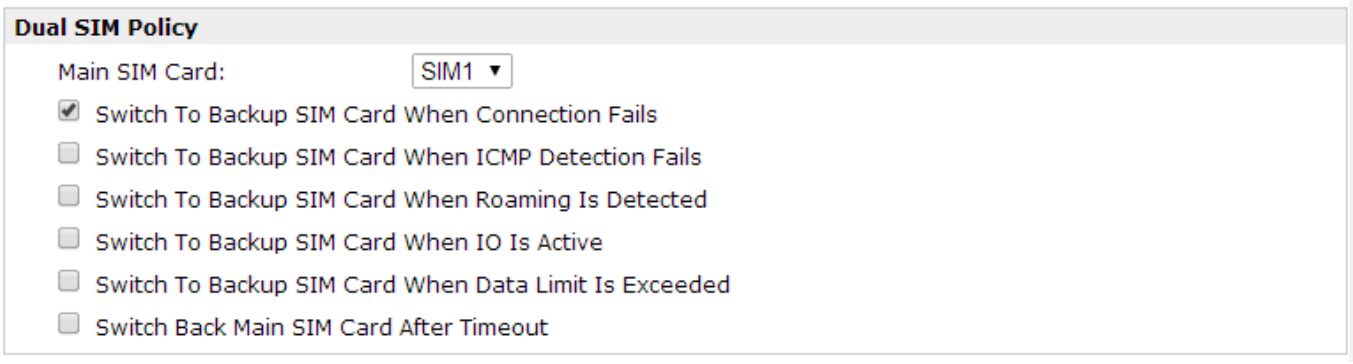
Phone Group	Click to add Phone Group to Set specific users' Phone Book and which Phone Group they are belonged to.	
Trigger By IO	Tick this checkbox to allow PPP connection/disconnection when there is a DI alarm. Only DI_1 can be used for this trigger and if selected, DI_1 cannot be used for any other purposes.	Disabled
Periodically Connect	Tick this checkbox to allow the router to automatically connect to the cellular network with an interval pre-set in *Periodical Connect Interval*.	Disabled
Periodically Connect Interval (s)	The Interval in seconds for Periodical Connect.	300
Time Schedule	Select the Time Range to allow the router to automatically connect to cellular network during specified time range.	NULL
Time Range	Adding the Time Range used for Time Schedule. You can set the days in the week and up to three time slots in one day. You can also add more than one schedule in the table and name them.	Null
Dual SIM Policy		
Main SIM Card	Set the preferred SIM card from SIM 1 or SIM 2.	SIM1
Switch to backup SIM Card When Connection Fails	If the router consistently fails to dialup or ping the preset WAN address and exceeds the Max Retries, it will switch to the backup SIM card.	Enabled
Switch to backup SIM Card When Roaming is Detected	The router will switch to backup SIM card when preferred SIM card is roaming.	Disabled
Preferred PLMN	The identifier for the router to check if it is in the home location area or in a roaming area, and to decide if it needs to switch back to the preferred SIM card.	Null
Switch to backup SIM card when IO is active	Router will switch to another SIM card if it detects there is a DI alarm. Only DI_2 can be used for this function and if selected, DI_2 cannot be used for any other purposes.	
Switch to backup SIM card when data limit is exceeded	If the active SIM card has reached the preset data limit, it will switch to the backup SIM card.	Disabled
Max Data limitation (MB)	Set the monthly data traffic limit in MB.	100
Date of Month to Clean	Set the day in a month to reset the data usage.	1
Already used	Show the amount of data been used.	0
Switch back Main SIM card after timeout	Enable to Switch back topreferred SIM card after the Initial timeout.	Disabled
Initial Timeout(min)	Set the initial timeout in minutes.	60



Invalid PPP password characters list:

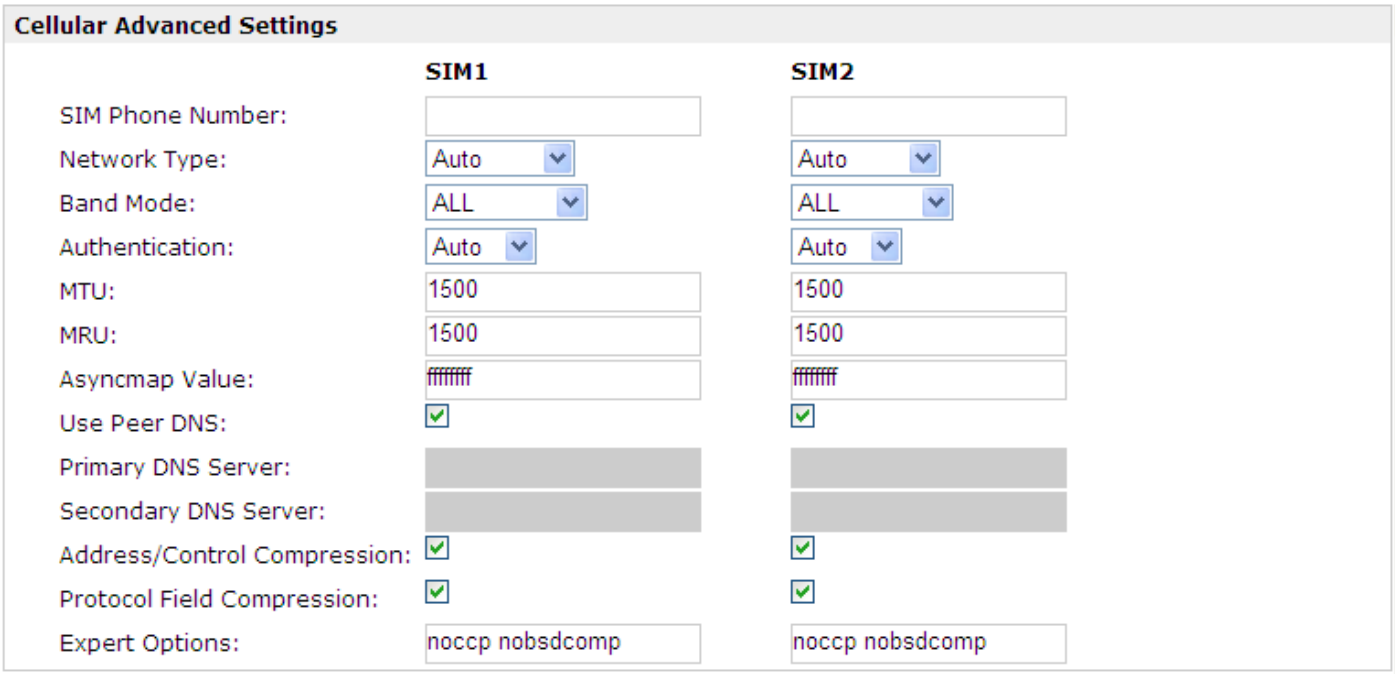
- " (double quotation mark)
- ' (quotation mark)
- ? (question mark)
-) (bracket)
- @ (at sign)
- ; (semi colon)
- | (pipe sign)
- I (upper case I)





Advanced

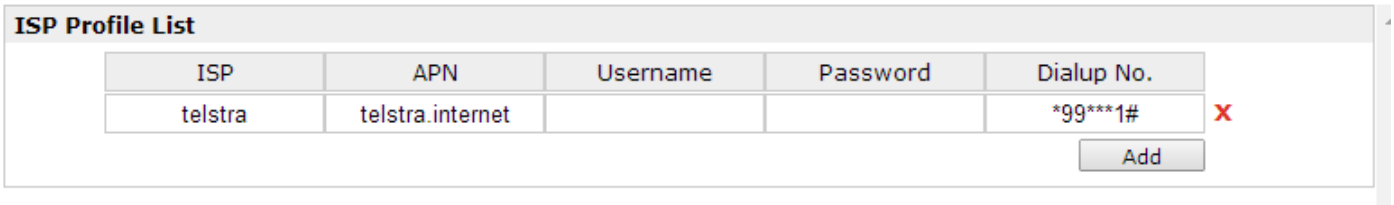
Cellular WAN – Advanced Settings		
Item	Description	Default
Phone No.	Set the phone number associated with the SIM card; will be shown in “Status”->”System”->”System”->”Cellular WAN Information”-“SIM Phone Number”. Normally, you don’t have to enter this number because the router will get it from the SIM card automatically.	Null
Network Type	Select from “auto” or the specific network type that the wireless module supports.	Auto
Band Mode	Select from “ALL” or the specific band which the wireless module supports.	ALL
Authentication	Select from “Auto”, “PAP” and “CHAP” as the local ISP required.	Auto
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which can be transferred in certain environments. In most cases, you don’t need to modify this value.	1500
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which can be received in certain environments. In most cases, you don’t need to modify this value.	1500
Asyncmap Value	One of the PPP initialization strings. In most cases, you don’t need to modify this value.	ffffffff
Use Peer DNS	Enable to obtain the DNS server address from the ISP.	Enabled
Primary DNS Server	Set the primary DNS server address. This item will be unavailable if you enable “Use Peer DNS”.	Null
Secondary DNS Server	Set the secondary DNS server address. This item will be unavailable if you enable “Use Peer DNS”.	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enabled
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enabled
Expert Options	You can enter some extra PPP initialization strings in this field. Each string can be separated by a space.	noccpnobsdcomp



ISP Profile

This section allow users to preset some ISP profiles which will be shown in the selection list of "Configuration"->"Cellular WAN"->"Network Provider Type".

Cellular WAN – ISP Profiles		
Item	Description	Default
ISP	Input the ISP's name which will be shown in the selection list of "Configuration"->"Cellular WAN"->"Network Provider Type".	Null
APN, Username, Password, Dialup No.	All these parameters provided by the ISP.	Null

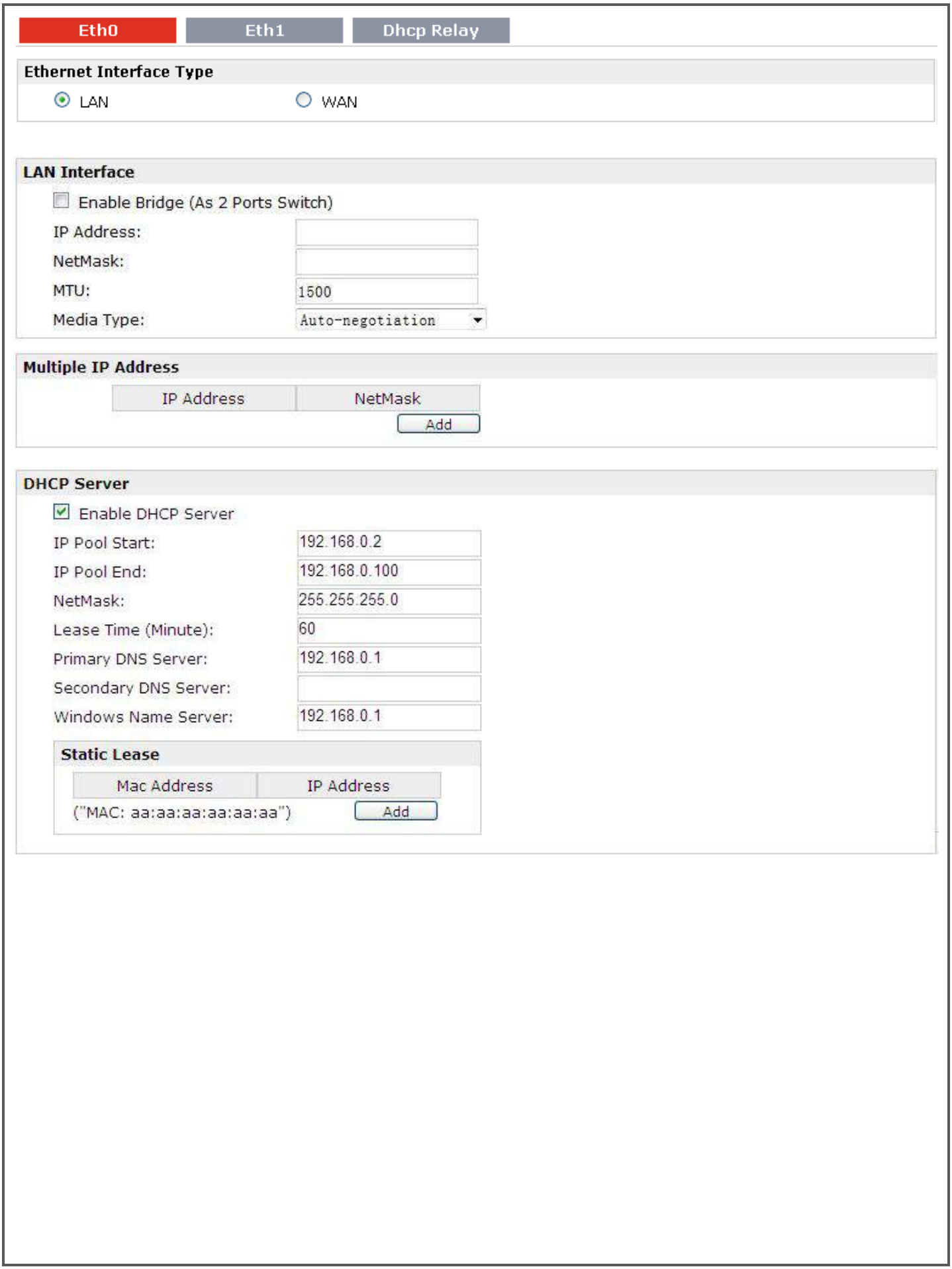


3.12 Configuration -> Ethernet

This section allows users to set the Ethernet WAN and LAN parameters.

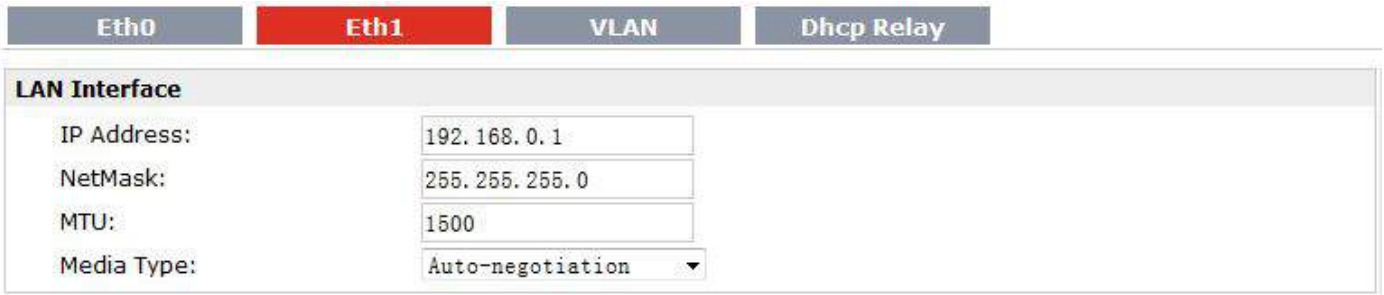
Eth0/Eth1

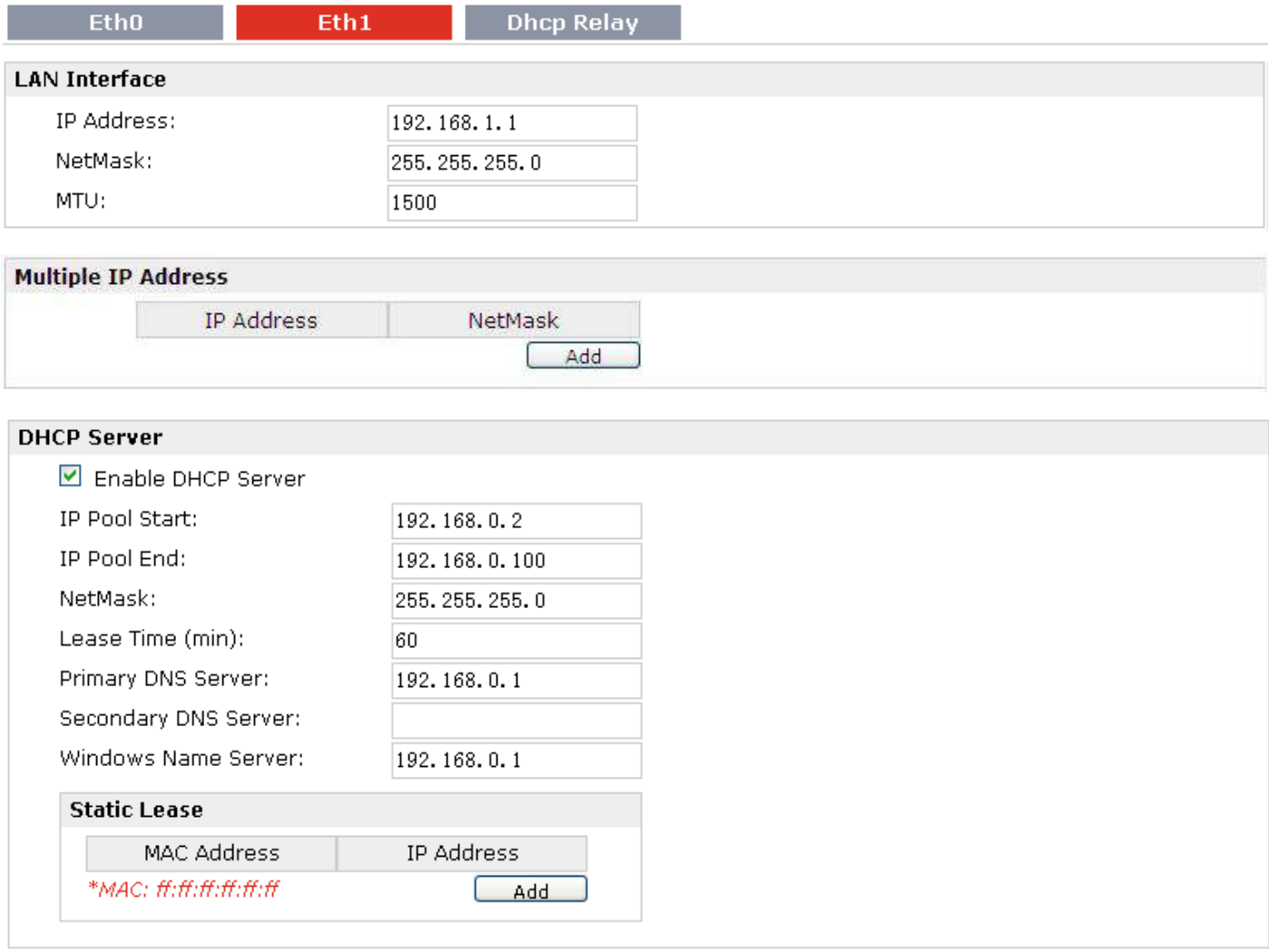
Ethernet - Eth0		
Item	Description	Default
Ethernet Interface Type	Eth0 can work under two different kinds of modes: LAN and WAN.	LAN
Enable Bridge @ LAN Interface	Enable to make Eth0 work under bridge mode with Eth1. Eth0 and Eth1 will have the same IP address under this mode.	Enable
IP Address, Netmask, MTU @ LAN Interface	Set the IP address, netmask and MTU of Eth0. These parameters will be un-configurable if you enable Bridge mode.	192.168.0.2/ 192.168.0.100 / 1492
Media Type @ LAN Interface	Set up media type for Eth0. There are five types in the drop down list to choose from: Auto-negotiation 10Mbps Half Duplex 10Mbps Full Duplex 100Mbps Half Duplex 100Mbps Full Duplex	Auto-negotiation
Multiple IP Address @ LAN Interface	Assign multiple IP addresses for Eth0.These parameters will be un-configurable if you enable Bridge mode.	Null
Enable DHCP Server @ DHCP Server	Enable to make the router lease IP address to DHCP clients which connect to Eth0.These parameters will be un-configurable if you enable Bridge mode.	Enable
IP Pool Start, IP Pool End @ DHCP Server	Define the beginning (IP Pool Start) and end (IP Pool End) of the pool of IP addresses that will be leased to DHCP clients.	192.168.0.2/ 192.168.0.100
Netmask @ DHCP Server	Define the netmask that the DHCP clients will get from DHCP server.	255.255.255.0
Lease Time @ DHCP Server (min)	Define how long (in minutes) the client can use the IP address acquired from DHCP server.	60
Primary/Secondary DNS Server @ DHCP Server	Define the primary and secondary DNS Server that the DHCP clients will get from DHCP server.	192.168.0.1/ 0.0.0.0
WINS Server @ DHCP Server	Define the WINS Server that the DHCP clients will get from DHCP server.	192.168.0.1
Static Lease @ DHCP Server	Define the IP Addresses that are dedicatedly allocated to the equipment with the specified MAC Addresses.	Null


Eth0
Eth1
Dhcp Relay
Ethernet Interface Type
LAN
WAN
LAN Interface
Enable Bridge (As 2 Ports Switch)
IP Address:
NetMask:
MTU:
1500
Media Type:
Auto-negotiation
Multiple IP Address
IP Address
NetMask
Add
DHCP Server
Enable DHCP Server
IP Pool Start:
192.168.0.2
IP Pool End:
192.168.0.100
NetMask:
255.255.255.0
Lease Time (Minute):
60
Primary DNS Server:
192.168.0.1
Secondary DNS Server:
Windows Name Server:
192.168.0.1
Static Lease
Mac Address
IP Address
("MAC: aa:aa:aa:aa:aa:aa")
Add

LAN Settings for Eth1 will be common for both Ethernet ports when bridge mode is enabled.

Ethernet – Eth1		
Item	Description	Default
IP Address, Netmask, MTU @ LAN Interface	Set the IP address, netmask, MTU and Media Type of Eth1.	192.168.0.2 / 192.168.0.100 / 1492
Media Type @ LAN Interface	Set up media type for Eth0. There are five types in the drop down list to choose from: Auto-negotiation 10Mbps Half Duplex 10Mbps Full Duplex 100Mbps Half Duplex 100Mbps Full Duplex	Auto-negotiation
Enable DHCP Server @ DHCP Server	Enable to allow the router to lease IP addresses to DHCP clients that connect to Eth1.	Enabled
IP Pool Start, IP Pool End @ DHCP Server	Define the beginning (IP Pool Start) and end (IP Pool End) of the pool of IP addresses thatwill lease to DHCP clients.	192.168.0.2/ 192.168.0.100
Netmask @ DHCP Server	Define the netmask that the DHCP clients will obtain from DHCP server.	255.255.255.0
Lease Time @ DHCP Server(min)	Define the time that the client can use the IP address which obtained from DHCP server.	60
Primary/Secondary DNS Server @ DHCP Server	Define the primary/secondary DNS Server that the DHCP clients will obtain from DHCP server.	192.168.0.1/ 0.0.0.0
Windows Name Server @ DHCP Server	Define the WINS Server that the DHCP clients will obtain from DHCP server.	192.168.0.1
Static Lease @ DHCP Server	Define to lease static IP Addresses, which conform to MAC Address of the connected equipment.	Null

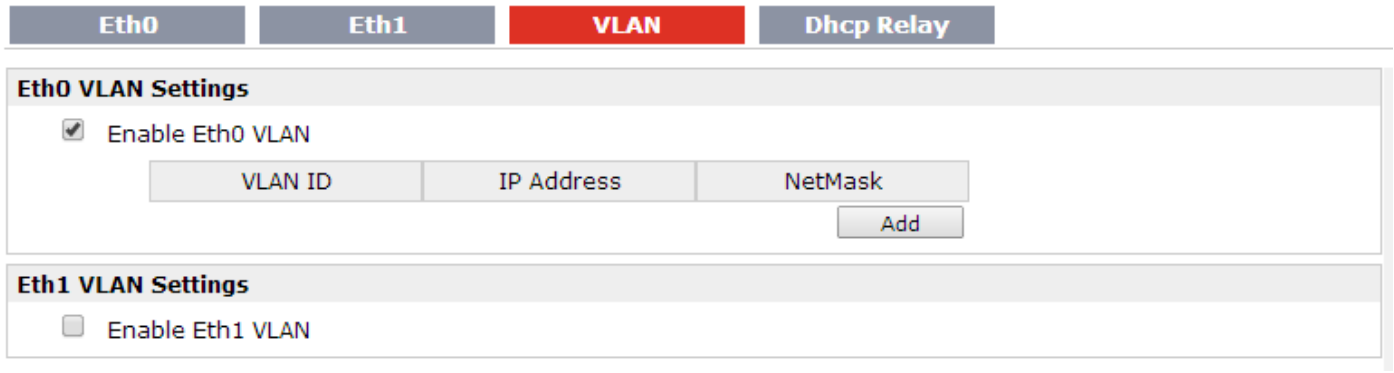




VLAN

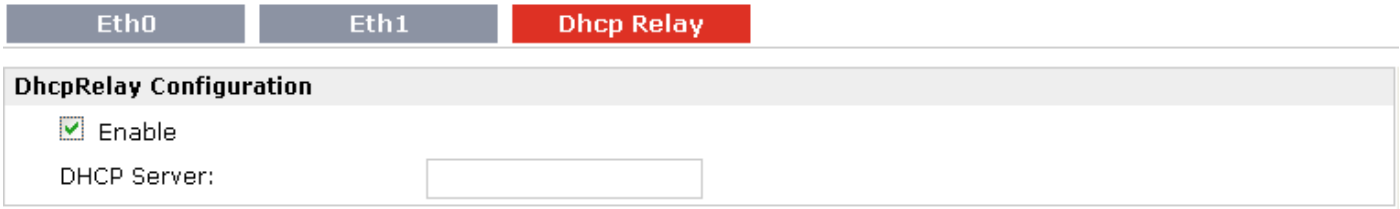
Ethernet - VLAN		
Item	Description	Default
Enable Eth0/1 VLAN@Eth0/1 VLAN Settings	Enable to make router encapsulate and de-encapsulate the VLAN tag.	Disabled
VLAN ID@Eth0/1 VLAN Settings	Set the Tag ID for VLAN	Null
IP Address, NetMask @Eth0/1 VLAN Settings	Set the IP address, Netmask for VLAN interface	Null

Note: Virtual LAN is not available when in bridge mode.



DHCP Relay

The Router can be a DHCP Relay, which will provide a relay tunnel when the DHCP Client and DHCP Server are not in the same subnet. This section allows users to configure DHCP Relay settings.



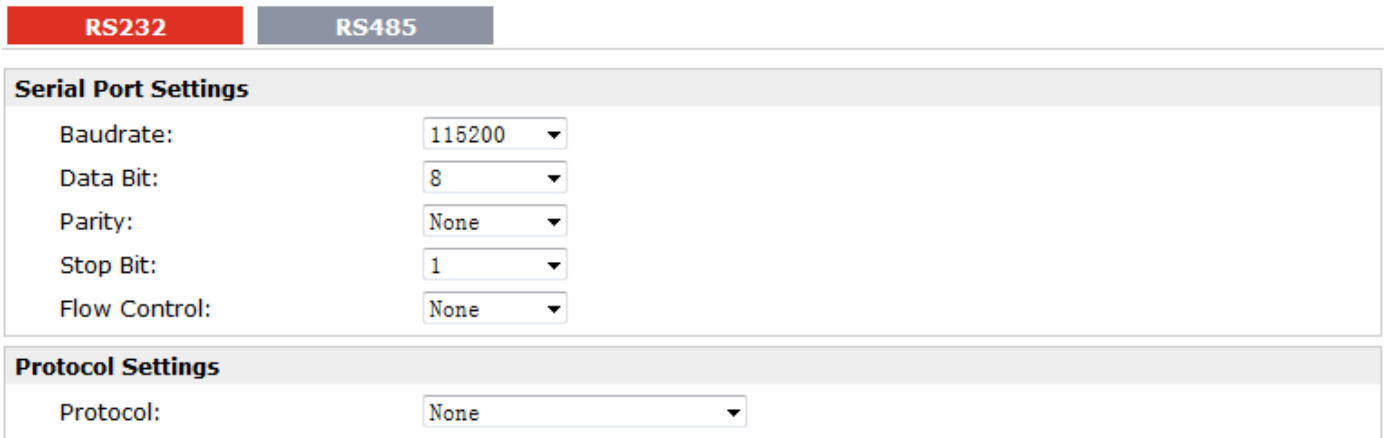
3.13 Configuration -> Serial

This section allows users to set the serial (RS232/RS485) parameters.

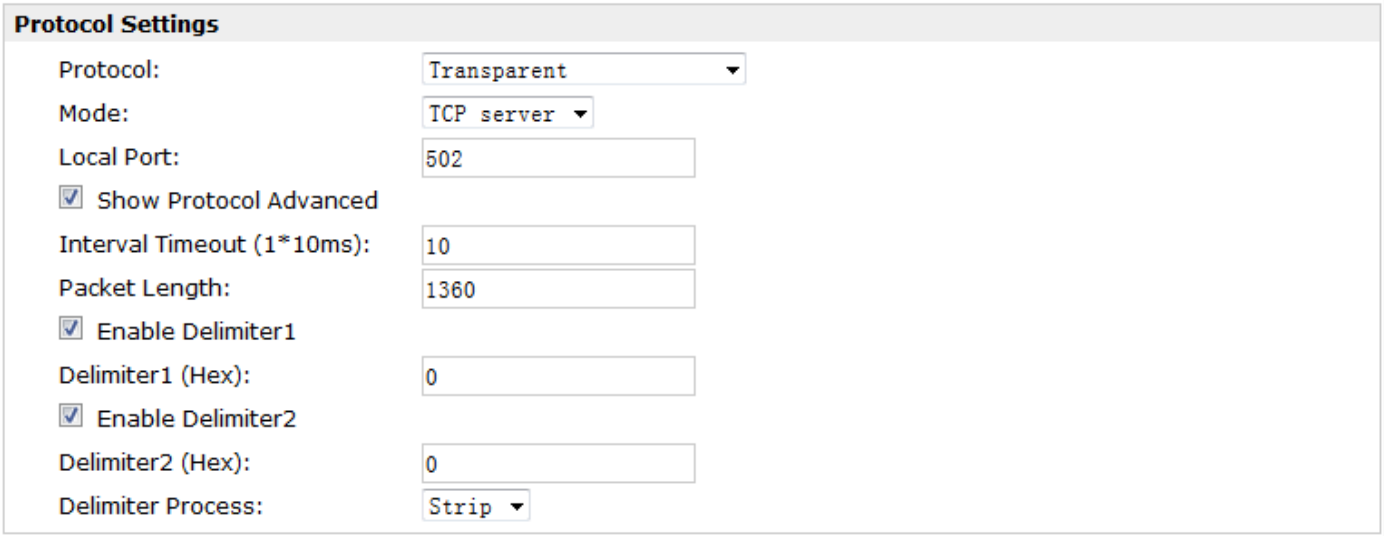
Serial – RS232		
Item	Description	Default
Baud-rate	Select from “300”, “600”, “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600” , “115200”and “230400”.	115200
Data bit	Select from “7” and “8”.	8
Parity	Select from “None”, “Odd” and “Even”.	None
Stop bit	Select from “1” and “2”.	1
Flow control	Select from “None”, “Software” and “Hardware”.	None
Protocol	Select from “None”, “Transparent”, “Modbus”, and “AT Over COM”. 1. None: Router will do nothing with the RS232 serial port. 2. Transparent: Router will transmit the serial data transparently without any protocols. 3. Modbus: Router will translate the Modbus RTU data to Modbus TCP data and vice versa. 4. AT Over COM: select to operate router via RS232 COM port. Enter AT commands to router via RS232 COM port.	None
Mode @Transparent	Select from “TCP Server”, “TCP Client” and “UDP”. TCP Client: the router works as TCP client, initiating a TCP connection to a TCP server. Server address supports both IP and domain name. TCP Server: the router works as TCP server, listening for connection request from TCP client. UDP: the router works as a UDP client.	TCP Client
Local Port @Transparent	Enter the local port for TCP or UDP.	0
Multiple Server @Transparent	Click “Add” button to add multiple servers. You need to enter the server’s IP and port, and enable or disable “Send data to serial”. If you disable “Send data to serial”, router will not transmit the data from this server to serial port. **Note**: This section will not be displayed if you select “TCP server” in “Mode”.	None
Show Protocol Advanced @ Transparent	Tick to enable protocol advanced setting.	Disabled
Local IP @ Transparent	This item will show up when you enable any VPN tunnel in the router, it means that serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. **Note**: when you do not enable any VPN tunnel, this item will not show up.	Null

Interval Timeout @Transparent	The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. **Note**: Data will also be sent as specified by the packet length or delimiter settings even when data is not reaching the interval timeout in the field.	10
Packet Length @Transparent	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. Setting 0 for packet length means that data in the buffer will be sent as specified by the interval timeout or delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length. **Note**: Data will also be sent as specified by the interval timeout or delimiter settings even when data is not reaching the preset packet length.	1360
Enable Delimiter1/2	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	Disabled
Delimiter1/2 (Hex) @Transparent	Enter the delimiter in Hex.	0
Delimiter Process @Transparent	The Delimiter process field determines how the data is handled when a delimiter is received. None: Data in the buffer will be transmitted when the delimiter is received; the data also includes the delimiter characters. Strip: Data in the buffer is first stripped of the delimiter before being transmitted.	Strip
Local IP @ Modbus	This item will show up when you enable any VPN tunnel in the router, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. **Note**: when you do not enable any VPN tunnel, this item will not be shown.	0
Local Port @ Modbus	Enter the Local port for Modbus.	0
Attached serial device type @Modbus	Select From “Modbus RTU slave”, “Modbus ASCII slave”, “Modbus RTU master” and “Modbus ASCII master”. Modbus RTU slave: router connects to a Modbus slave device that works under Modbus RTU protocol. Modbus ASCII slave: router connects to a Modbus slave device that works under Modbus ASCII protocol.	Modbus RTU slave

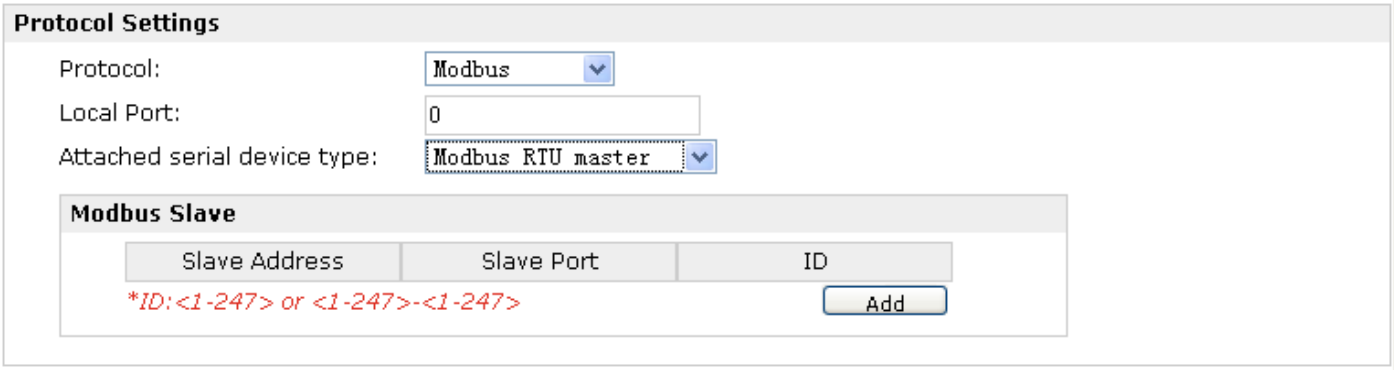
	Note: When “Modbus RTU slave” or “Modbus ASCII slave” protocol is selected, the router is acting as a TCP Server so the user needs to enter a local port number in “Local Port @Modbus” field and the router will listen to the port for connection. Modbus RTU master: router connects to a Modbus master device that works under Modbus RTU protocol. Modbus ASCII master: router connects to a Modbus master device that works under Modbus ASCII protocol. **Note**: When “Modbus RTU master” or “Modbus ASCII master” protocol is selected, the router is acting as a TCP Client so the user needs to enter slave address and slave port number in “Slave Address @ Modbus Slave” and “Slave Port @ Modbus Slave” fields. The router will then try to connect to the server using the specified address and port.	
Modbus Slave @Modbus	Add the Modbus slaves that will be polled by Modbus master. This section will be shown only when you select “Modbus RTU master” or “Modbus ASCII master” in “Attached serial device type”.	Null
Slave Address @ Modbus Slave	Enter the address of the Modbus slave that is acting as a TCP sever.	Null
Slave Port @ Modbus Slave	Enter the port number of the Modbus slave that is acting as a TCP sever.	Null
ID @ Modbus Slave	Enter the ID number of the Modbus slave.	Null
Display all com @ AT Over COM	Enable to display all virtual com ports of the cellular inside the router. Generally, /dev/ttyUSB0 and /dev/ttyUSB2 are used for cellular network connection. **Note**: Enabling this function could result in loss of Cellular WAN function.	Disabled
COM Name	Show the available virtual com ports of the cellular module.	/dev/ttyUSB1



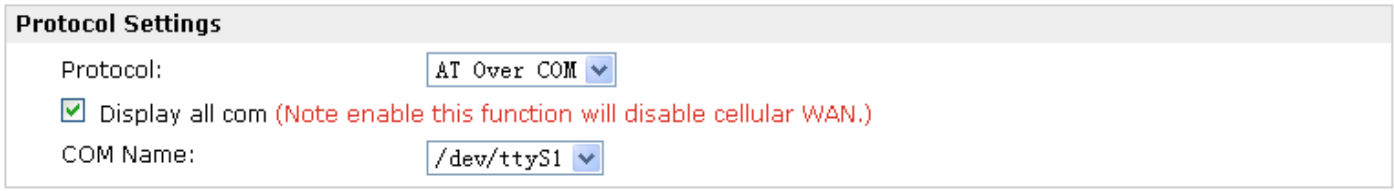
- When Selecting the Protocol “Transparent”:



- When Selecting the Protocol “Modbus”:



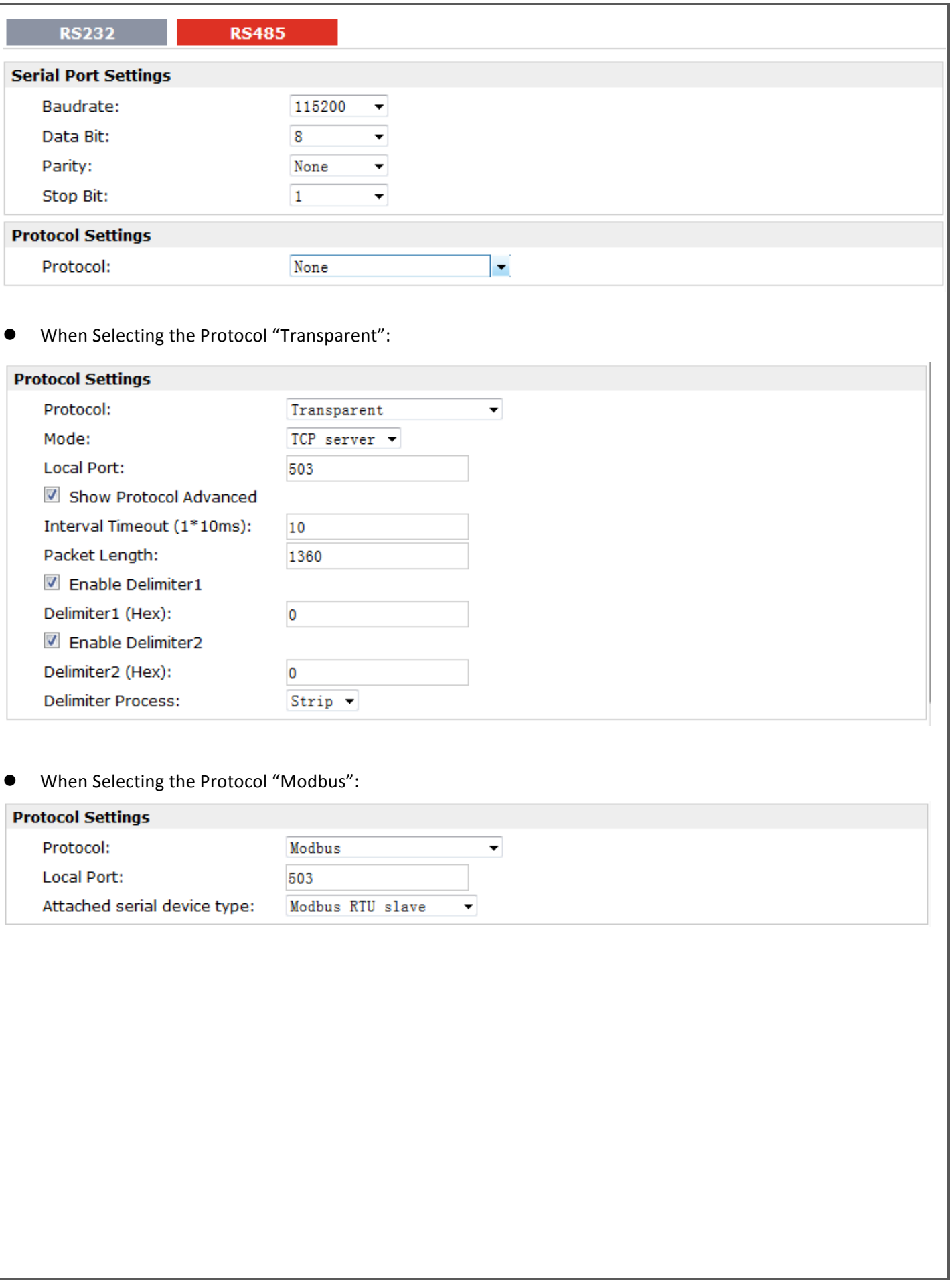
- When Selecting the Protocol “AT Over COM”:



Serial – RS485		
Item	Description	Default
Baud-rate	Select from “300”, “600”, “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600” , “115200”and “230400”.	115200
Data bit	Select from “7” and “8”.	8
Parity	Select from “None”, “Odd” and “Even”.	None
Stop bit	Select from “1” and “2”.	1

Protocol	Select from “None”, “Transparent” and “Modbus”. Transparent: Router will transmit the serial data transparently without any protocols. Modbus: Router will transmit the serial data with Modbus protocol.	Transparent
Mode @ Transparent	Select from “TCP Server”, “TCP Client” and “UDP”.	TCP Client
Local Port @ Transparent	Enter the Local port for TCP or UDP.	0
Multiple Server @ Transparent	Click “Add” button to add multiple servers. You need to enter the server’s IP and port, and enable or disable “Send data to serial”. If you disable “Send data to serial”, router will not transmit the data from this server to serial port. **Note:** This section will not be displayed if you select “TCP server” in “Mode”.	Null
Enable Protocol @ Transparent	Tick to enable protocol advanced settings.	Disabled
Local IP @ Transparent	This item will show up when you enable any VPN tunnel in the router, it means that serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. **Note**: when you do not enable any VPN tunnel, this item will not show up.	0
Interval Timeout @Transparent	The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. **Note**: Data will also be sent as specified by the packet length or delimiter settings even when data is not reaching the interval timeout in the field.	10
Packet Length @Transparent	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. Setting 0 for packet length means that data in the buffer will be sent as specified by the interval timeout or delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length. **Note**: Data will also be sent as specified by the interval timeout or delimiter settings even when data is not reaching the preset packet length.	1360
Enable Delimiter	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when a specific character, entered in HEXADECIMAL format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	Disabled

Delimiter(Hex) @ Transparent	Enter the delimiter in Hex.	0
Delimiter Process @ Transparent	The Delimiter process field determines how the data is handled when a delimiter is received. None: Data in the buffer will be transmitted when the delimiter is received; the data also includes the delimiter characters. Strip: Data in the buffer is first stripped of the delimiter before being transmitted.	Strip
Local IP @ Modbus	This item will be configurable when you enable any VPN tunnel in the router, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. **Note**: when you have not enabled any VPN tunnel, this item will not be shown.	0
Local Port @ Modbus	Enter the Local port for Modbus.	0
Attached serial device type @Modbus	Select From “Modbus RTU slave”, “Modbus ASCII slave”, “Modbus RTU master” and “Modbus ASCII master”. Modbus RTU slave: router connects to slave device that works under Modbus RTU protocol. Modbus ASCII slave: router connects to slave device that works under Modbus ASCII protocol. Modbus RTU master: router connects to master device that works under Modbus RTU protocol. Modbus ASCII master: router connects to master device that works under Modbus ASCII protocol.	Modbus RTU slave
Modbus Slave @ Modbus	Add the Modbus slaves that will be polled by Modbus master. This section will be shown only when you select “Modbus RTU master” or “Modbus ASCII master” in “Attached serial device type”.	Null
Slave Address @ Modbus Slave	Enter the address of the Modbus slave that is acting as a TCP sever.	Null
Slave Port @ Modbus Slave	Enter the port number of the Modbus slave that is acting as a TCP sever.	Null
ID @ Modbus Slave	Enter the ID number of the Modbus slave.	Null



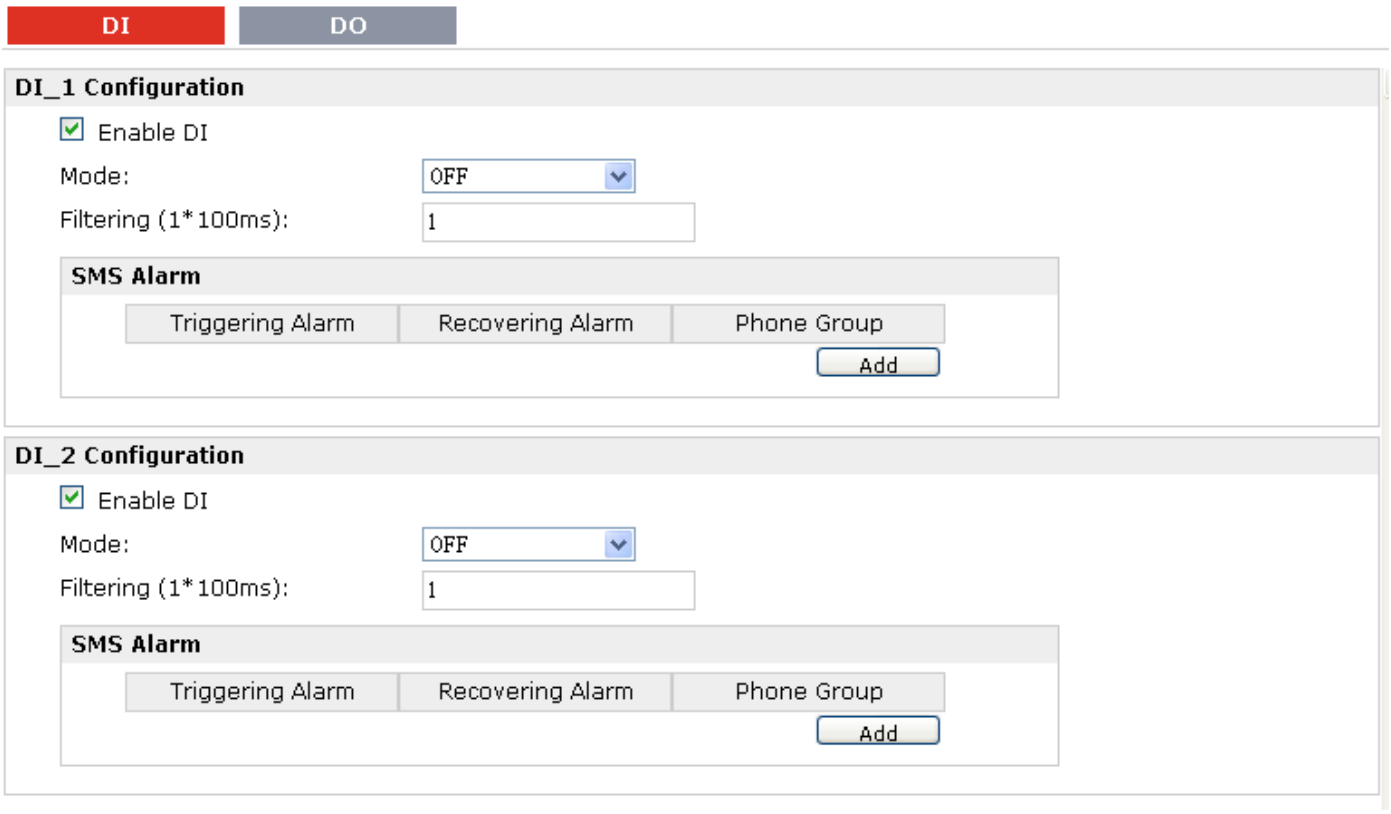
- When Selecting the Protocol “Transparent”:

- When Selecting the Protocol “Modbus”:

3.14 Configuration -> DI/DO

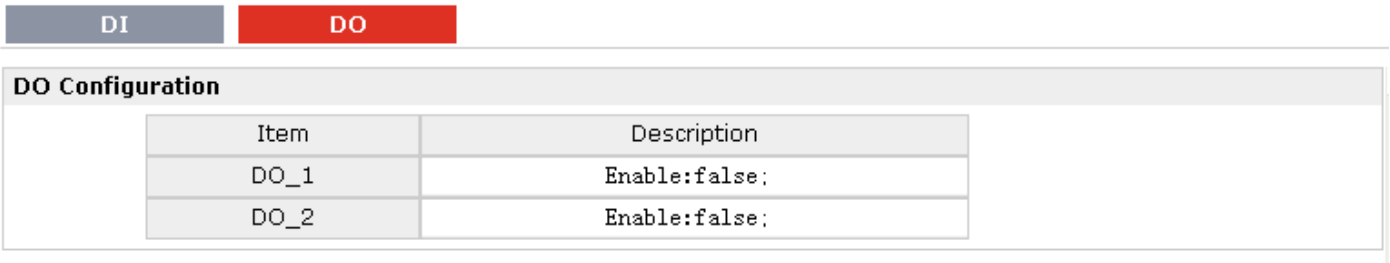
This section allows users to set the Digital IO parameters.

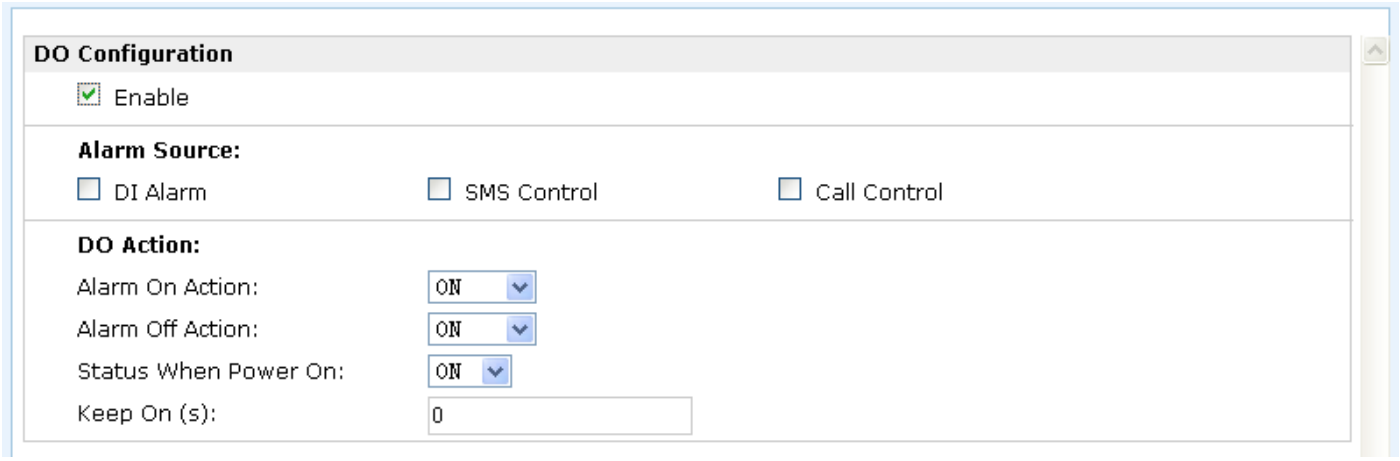
DI/DO - DI		
Item	Description	Default
Enable DI	Click to Enable digital input (DI).	Disabled
Mode	Select from “OFF”, “ON”, “EVENT_COUNTER”. OFF: Connect to GND (logic 0). When DI is connected to GND, Multimax will trigger a DI alarm. ON: Open from GND (logic 1). When DI is disconnected from GND, Multimax will trigger a DI alarm. EVENT_COUNTER: DI works in the Event Counter mode.	OFF
Filtering	Software filtering is used to eliminate the switching noises (debouncing).Input range from 0 to 100 in a unit of 100ms.	1
Count Trigger	Available when DI is in the Event Counter mode. Input range from 0 to 100. (0=will not trigger alarm) The router will trigger alarm when counter reaches the value. After alarm is triggered, DI will keep counting but not alarm will be triggered again.	0
Counter Active	Available when DI is in the Event Counter mode. Select from “Hi to Lo” or “Lo to Hi”. In the Event Counter mode, the input accepts limit or proximity switches and counts the number of events according to the state changes defined.	Lo to Hi
Counter Start When Power On	Available when DI is in the Event Counter mode. When enabled, the event counting will start counting once the router is powered on. Normally users shall enable this option when DI is used for Event Counter. Alternatively, the router will start counting when a SMS command is received. Refer to section 4.1.3 for details.	Disabled
Triggering Alarm	The SMS to send when alarm is triggered. (70 ASICII char max)	Null
Recovering Alarm	The SMS to send when alarm is cleared. (70 ASICII char max)	Null
Phone Group	Specify phone group that will receive alarm SMS. Each phone group can include up to 10 phone numbers.	Null



DI/DO - DO		
Item	Description	Default
Enable	Click to enable Digital Output (DO).	Disable
Alarm Source	Digital Output will operate based on the alarm sources, which can be "DI Alarm", "SMS Control", and "Call Control". More than one source can be selected. DI Alarm: Digital Output will take the defined action when there is alarm from Digital Input. SMS Control: Digital Output will take the defined action when getting an SMS from a number in the phone book. Call Control: Digital Output will take the defined action when getting a phone call from a number in the phone book. **Note**: Call Control is not supported by the 4G model.	Null
Alarm On Action	The action that the Digital Output will take when there is an alarm. Selected from "OFF", "ON", and "Pulse". OFF: Disconnected from GND. ON: Connected to GND. Pulse: Generates a square wave specified in the pulse mode parameters.	ON
Alarm Off Action	The action that the Digital Output will take when alarm is cleared. Selected from "OFF", "ON", "Pulse". OFF: Disconnected from GND. ON: Connected to GND. Pulse: Generates a square wave specified in the pulse mode parameters.	ON

Status When Power On	Specify the Digital Output status when power on. Selected from “OFF”, “ON”. OFF: Disconnected from GND. ON: Connected to GND.	ON
Keep On (s)	Available when Digital Output Alarm On/Off Action is enabled, Enter the time the Digital Output should keep the state after an action is taken. Input range from 0 to 255 seconds. (0=keep on until the next action)	0
Delay	Available when enabling “Pulse” option in Alarm On/Off Action. The first pulse will be generated after a “Delay”. Input range from 0 to 3000 in the unit of 10ms. (0=without delay)	0
Low	Available when enabling “Pulse” option in Alarm On/Off Action. This value specifies the time period of low level (connected to GND) in the square wave form. Input range from 1 to 3000 in the unit of 10ms.	10
High	Available when enabling “Pulse” option in Alarm On/Off Action. This value specifies the time period of high level (disconnected from GND) in the square wave form. Input range from 1 to 3000 in the unit of 10ms.	10
Output	Available when enabling “Pulse” option in Alarm On/Off Action. The value defines the number of pulses that will be generated from Digital Output. Input range from 0 to 30000. (0 for continuous pulse output)	0
SMS Content On	Available when enabling the SMS Control in Alarm Source. Input the SMS content to be received by router to trigger an alarm action (70 ASIC II char max).	Null
SMS Content Off	Available when enabling SMS Control in Alarm Source. Input the SMS content to be received by router to trigger an alarm cleared action (70 ASIC II char max)	Null
SMS Content On Reply	Input the SMS content that will be sent out by the router after an alarm action is taken. (70 ASIC II char max)	Null
SMS Content Off Reply	Input the SMS content that will be sent out by the router after an alarm cleared action is taken. (70 ASIC II char max)	Null
Phone Group	Click to add phone groups.	Null





3.15 Configuration -> USB

This section allows users to configure the USB port.

Note: Users can insert a USB storage device, such as a USB flash Disk, into the router's USB interface. If there is valid configuration file or firmware of Multimax in the USB device, the Multimax will automatically update the configuration or firmware. Please refer to a separate application note for details on how to do USB automatic updates.

USB		
Item	Description	Default
Enable automatic update of configuration	Tick to enable the automatic update of Multimax configuration when inserting a USB storage device containing a valid configuration file.	Disabled
Enable automatic update of firmware	Tick to enable the automatic update of Multimax firmware when inserting a USB storage device containing a valid firmware file.	Disabled

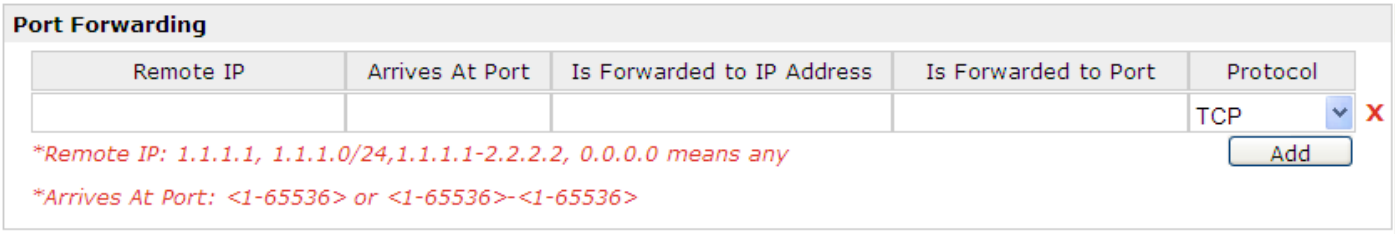
3.16 Configuration -> NAT/DMZ

This section allows users to set the NAT/DMZ parameters.

NAT (Port Forwarding)

Port forwarding is to manually define rules in the router to send all data received from a range of ports on the WAN side to a port and IP address on the LAN side.

NAT/DMZ - Port Forwarding		
Item	Description	Default
Remote IP	Set the remote IP address.	Null
Arrives At Port	The port of the internet side that you want to forward to LAN side.	Null
Is Forwarded to IP Address	The device's IP on the LAN side that you want to forward the data to.	Null
Is Forwarded to Port	The device's port on the LAN side that you want to forward the data to.	Null
Protocol	Select from "TCP", "UDP" or "TCP&UDP" which depends on the application.	TCP



DMZ

DMZ host is a host on the local network that has all ports exposed, except those otherwise forwarded.

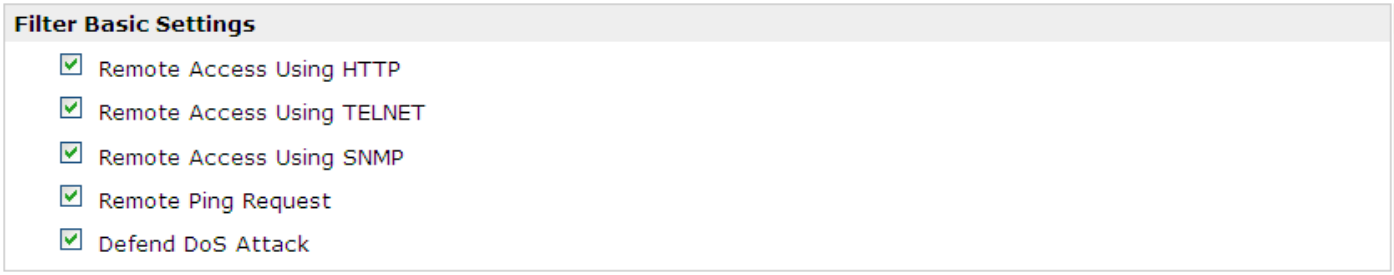
NAT/DMZ - DMZ		
Item	Description	Default
Enable DMZ	Select to enable the DMZ function.	Disabled
DMZ Host	Enter the IP address of the DMZ host on the internal network.	0.0.0.0
Source Address	Set the address that can talk to the DMZ host. Null means for any addresses. "0.0.0.0" means any IP addresses.	0.0.0.0

3.17 Configuration -> Firewall

This section allows users to set the firewall parameters.

Basic Settings

Firewall – Basic Settings		
Item	Description	Default
Remote Access Using HTTP	Tick to allow users to access the router remotely from the internet using HTTP.	Enabled
Remote Access Using TELNET	Tick to allow users to access the router remotely from the internet using Telnet.	Enabled
Remote Access Using SNMP	Tick to allow users to access the router remotely on the internet using SNMP.	Enabled
Remote Ping Request	Tick to allow the router reply Ping requests from the internet.	Enabled
Defend DoS Attack	DoS (Deny of Services) attack is an attempt to make a machine or network resource unavailable to its intended users. Tick to enable protection from DoS attacks.	Enabled

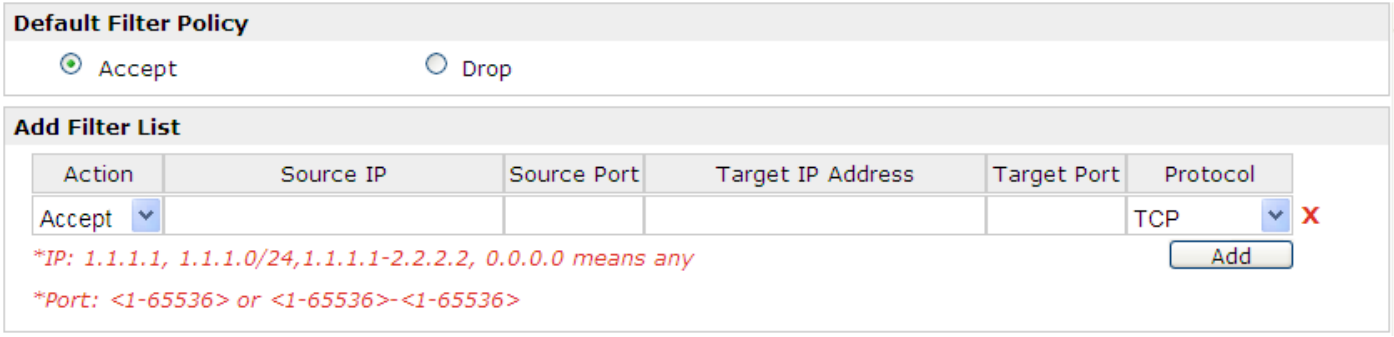


Filtering

Firewall - Filtering		
Item	Description	Default
Default Filter Policy	Select from “Accept” and “Drop”. Accept: Router will only reject the connecting requests from the hosts that match the filter list. Drop: Router will only accept the connecting requests from the hosts that fit the filter list.	Accept
Add Filter List	Click “Add” to add a filter list.	Null
Action	Select from “Accept” and “Drop”. Accept: Router will accept the connection request that matches the definition in the table.	Accept

	Drop: Router will reject the connection request that matches the definition in the table.	
Source IP	Defines if access is allowed from one or a range of IP addresses that are defined by Source IP Address, or every IP address.	Null
Source Port	Defines if access is allowed from one or a range of ports that is defined by Source Port.	Null
Target IP Address	Defines if access is allowed to one or a range of IP addresses that are defined by Target IP Address, or every IP address.	Null
Target Port	Defines if access is allowed tone or a range of port that is defined by Target Port.	Null
Protocol	Select from "TCP", "UDP", "TCP&UDP", "ICMP" or "ALL". If you don't know what kinds of protocol of your application, we recommend you select "ALL".	TCP

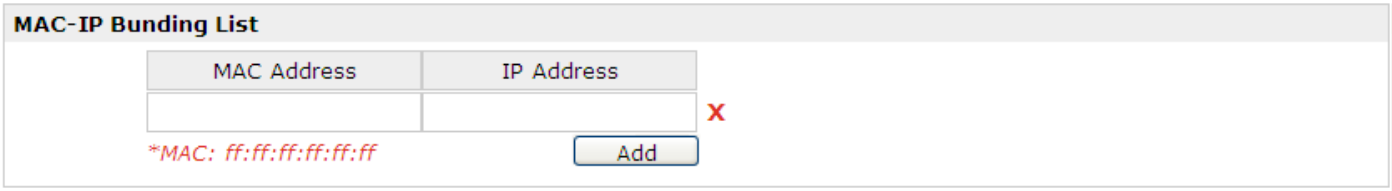
***Note**: You can use "-" to define a range of IP addresses or ports, e.g. 1.1.1.1-2.2.2.2, 10000-12000.*



Mac-IP Bounding

By MAC-IP bounding, the defined host (MAC) on the LAN side can only use the defined IP address to communicate with the router, others will be rejected.

Firewall - Mac-IP Bounding		
Item	Description	Default
Mac Address	Enter the defined host's Mac Address.	Null
IP Address	Enter the defined host's IP Address.	Null



3.18 Configuration ->QoS

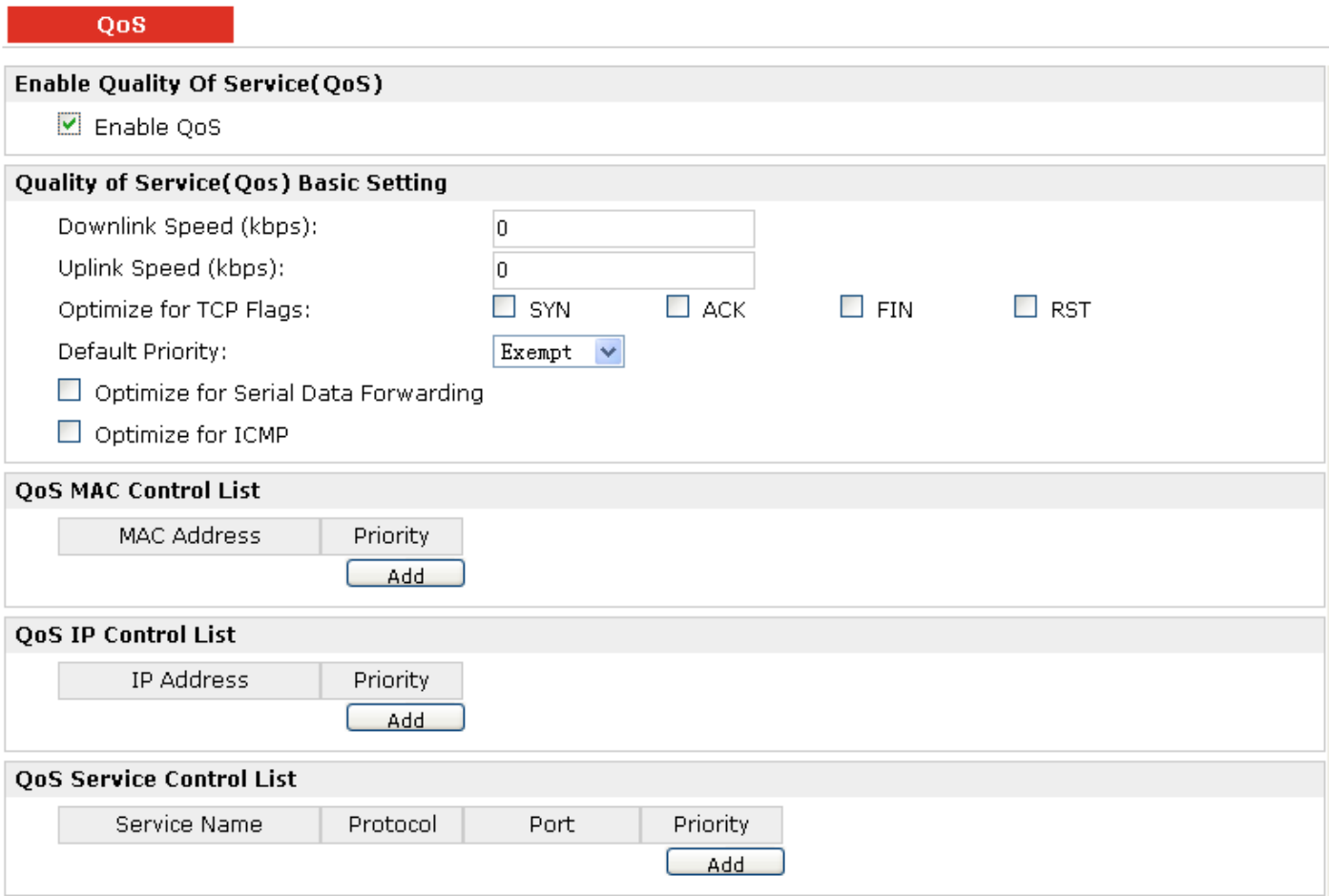
This section allows users to set up the QoS(Quality of Service) configurations.

QoS		
Item	Description	Default
Enable QoS	Tick to enable “QoS” function.	Disabled
Downlink Speed (kbps)	Prescribe downlink speed of router. **Note**: Default setting of “0” means that there is no limitation of downlink speed.	0
uplink Speed (kbps)	Prescribe uplink speed of router. **Note**: Default setting of “0” means that there is no limitation of uplink speed.	0
Optimize for TCP Flags	Users can choose to enable TCP flags: “SYN”, “ACK”, “FIN”, “RST”, which means that data with the above TCP Flags will get the highest priority to occupy the bandwidth. After being enabled, the router will enhance the response of TCP control in case of data resending frequently.	Disabled
Default Priority	Selectable from “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”. Users (Services) without other pre-priority setting will use this default priority. Exempt: this is the highest priority that guarantees that the minimum global rate of the router is 50% of the “Downlink Speed”, and the maximum rate can be 100%. Premium: guarantees that the minimum global rate of the router is 25% of the “Downlink Speed”, and the maximum rate can be 100%. Express: guarantees that the minimum global rate of the router is 15% of “Downlink Speed”, and the maximum rate can be 100%. Normal: guarantees that the minimum global rate of the router is 10% of “Downlink Speed”, and the maximum rate can be 100%. Bulk: guarantees that the minimum global rate of the router is 1% of “Downlink Speed”, and the maximum rate can be 100%.	Normal
Optimize for Serial Data Forwarding	Enable to optimize for serial data forwarding, meaning that serial data forwarding will get the highest priority to occupy the bandwidth. If using this option, a local port number for controlling is required. Therefore, it will need to set up a local port number for the router even if the router is a TCP Client.	Disabled
Optimize for ICMP	Enable to optimize for ICMP, meaning that ICMP will get the highest priority to occupy the bandwidth. After being enabled, response of PING control will be faster. **Note**: if enabling “Optimize for TCP Flags”, “Optimize for Serial Data Forwarding”, and “Optimize for ICMP” at the same time (meaning that these three services are in the same priority level), router will automatically start Stochastic Fairness Queuing (SFQ) strategy to make	Disabled

	a fair bandwidth allocation to avoid one service occupying all the bandwidth.	
MAC Address @ QoS MAC Control List	Enter the MAC address of a user device (for example, a PC) that requires QoS. The Multimax can support up to 20 devices with QoS MAC Control. Priority of QoS MAC Control is higher than that of QoS IP control.	Null
Priority @ QoS MAC Control List	Select from “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”. Select the priority of user device(s) (for example, a PC) which are set with QoS Control. Exempt: this is the highest priority that guarantees that the minimum global rate of the router is 50% of “Downlink Speed”, and the maximum rate can be 100%. Premium: guarantees that the minimum global rate of the router is 25% of “Downlink Speed”, and the maximum rate can be 100%. Express: guarantees that the minimum global rate of the router is 15% of “Downlink Speed”, and the maximum rate can be 100%. Normal: guarantees that the minimum global rate of the router is 10% of “Downlink Speed”, and the maximum rate can be 100%. Bulk: guarantees that the minimum global rate of the router is 1% of “Downlink Speed”, and the maximum rate can be 100%.	Exempt
IP Address @ QoS IP Control List	Enter the IP address of a user device (for example, a PC) that requires QoS. Multimax can support up to 20 devices with QoS IP Control. If requires to set upa network segment, users can set “IP Address” in format of “x.x.x.x/x” or “x.x.x.x/netmask”. For example, for network “172.16.x.x”, users can use “172.16.0.0/16” or “172.16.0.0/255.255.0.0” in “IP Address” field.	Null
Priority @ QoS IP Control List	Select from “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”. Select the priority of user device(s), “for example, a PC” which is set with QoS Control. Exempt: this is the highest priority that guarantees that the minimum global rate of the router is 50% of “Downlink Speed”, and the maximum rate can be 100%. Premium: guarantees that the minimum global rate of the router is 25% of “Downlink Speed”, and the maximum rate can be100%. Express: guarantees that the minimum global rate of the router is 15% of “Downlink Speed”, and the maximum rate can be 100%. Normal: guarantees that the minimum global rate of the router is 10% of “Downlink Speed”, and the maximum rate can be 100%. Bulk: guarantees that the minimum global rate of the router is 1% of “Downlink Speed”, and the maximum rate can be 100%.	Exempt
Service Name @ QoS Service Control List	Set the name of the service that requires QoS. The Multimax can support up to 20 services with QoS. Priority of QoS Service Control is higher than that of both QoS IP control and QoS MAC control.	Null
Protocol @ QoS Service Control	Select from “TCP”, “UDP” and ”TCP & UDP”.	TCP

List		
Port @ Service Control List	Enter the port number of the service that requires QoS.	Null
Priority @ QoSService Control List	Select from “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”. Select the priority of the service(s) that require QoS. Exempt: this is the highest priority thatguarantees that the minimum global rate of the router is 50% of “Downlink Speed”, and the maximum rate can be 100%. Premium: guarantees that the minimum global rate of the router is 25% of “Downlink Speed”, and the maximum rate can be100%. Express: guarantees that the minimum global rate of the router is 15% of “Downlink Speed”, and the maximum rate can be 100%. Normal: guarantees that the minimum global rate of the router is 10% of “Downlink Speed”, and the maximum rate can be 100%. Bulk: guarantees that the minimum global rate of the router is 1% of “Downlink Speed”, and the maximum rate can be 100%.	Exempt

Note: If devices or services are in the same priority level, the router will automatically start Stochastic Fairness Queuing (SFQ) strategy to make a fair bandwidth allocation.



3.18 Configuration -> IP Routing

This section allows users to set the IP routing parameters.

Static Route

To manually add, delete or modify static route rules.

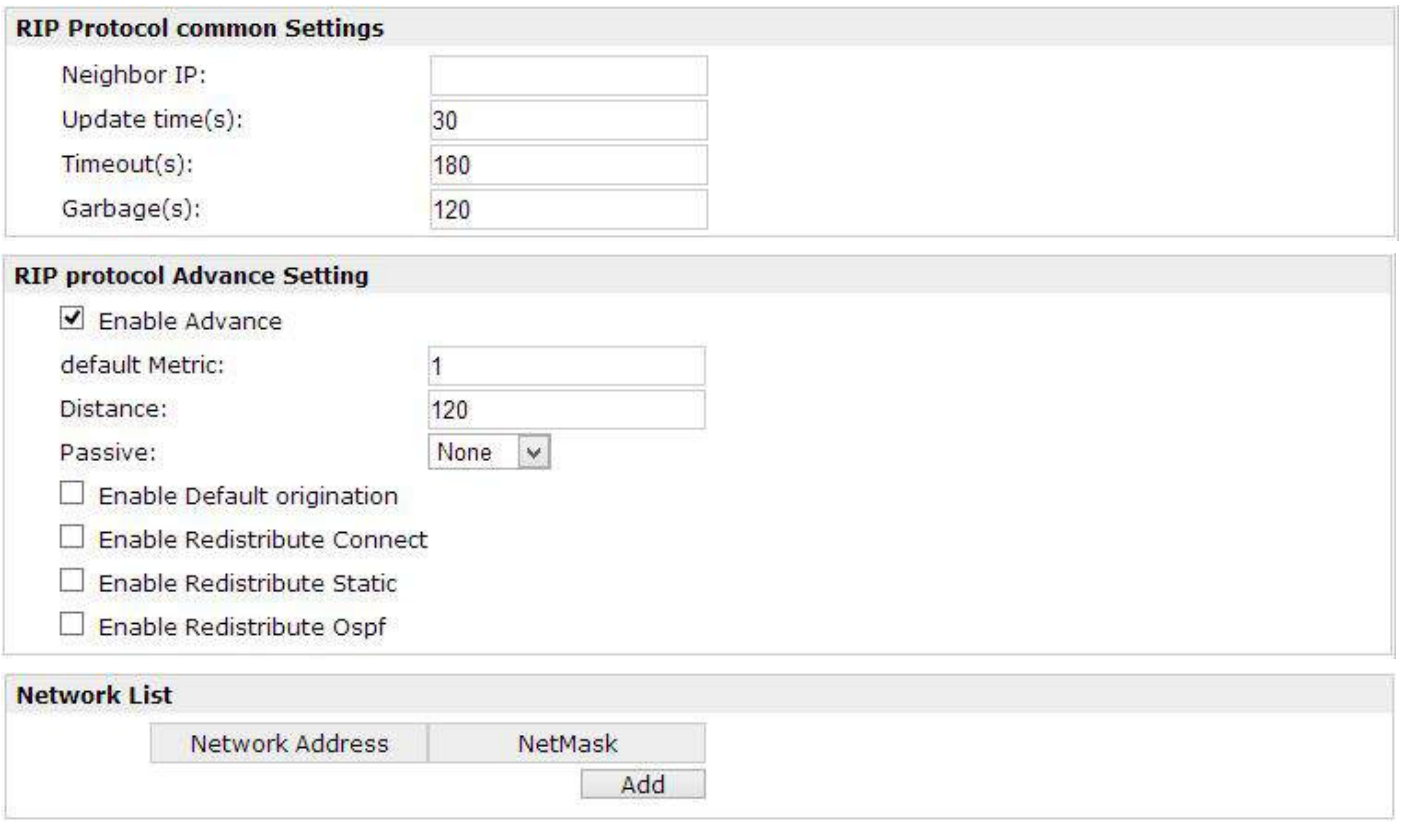
IP Routing - Static Route		
Item	Description	Default
Static Route Table	The table for static routing rule(s).	Null
Interface	Select from “WAN”, “LAN_0” or “LAN_1”.	WAN
Destination	Enter the destination host’s IP address or destination network.	Null
NetMask	Enter the netmask of the destination or destination network.	Null
Gateway	Enter the gateway’s IP address of this static route rule. Router will forward all the data that fits the destination and netmask to this gateway.	Null

RIP

RIP (Routing Information Protocol) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.

IP Routing - RIP		
Item	Description	Default
Enable RIP Protocol Setting	Tick to enable RIP function.	Disabled
RIP Protocol Version	Select from “RIPv1” and “RIPv2”.	RIPv1
Neighbor IP	If you input this neighbor IP, router will only send RIP request message to this IP instead of broadcast. This item only needs to be set in some unicast network.	0.0.0.0
Update times	Defines the interval in seconds between routing updates.	30
Timeout	Defines the aging time of a route (in seconds). If no update for a route is	180

	received, the metric of the route will be set to 16 in the routing table after the aging time elapses.	
Garbage	Defines the Garbage-Collect time (in seconds) from when the metric of a route becomes 16 to when it is deleted from the routing table. During the time, RIP advertises the route with the routing metric set to 16. If no update is announced for that route after the time period, the route will be deleted from the routing table.	120
Enable Advance	Tick to enable RIP protocol Advanced Settings.	Disabled
Default Metric	This value is used for redistributed routes.	1
Distance	The first criterion for a router to determine which routing protocol to use if two protocols provide route information for the same destination.	120
Passive	Select from “None”, “Eth0”, “Eth1” and “Default”. This command sets the specified interface to passive mode. When the interface is in passive mode, all receiving packets are processed as normal and RIP message will not be sent except to the RIP neighbours specified in the Neighbour field. The default is to be passive on all interfaces.	None
Enable Default Origination	Enable to make the router send the default route to other routers within one Autonomous System (AS) using Interior Gateway Protocol (IGP).	Disabled
Enable Redistribute Connect	Redistribute the connected routes into the RIP tables.	Disabled
Enable Redistribute Static	Enable to redistribute routing information from static route entries into the RIP tables.	Disabled
Enable Redistribute OSPF	Enabling to redistribute routing information from OSPF route entries into the RIP tables.	Disabled
Network List	The router will only report the RIP information in this list to its neighbour.	Null
Network Address	Enter the Network address which Eth0 or Eth1 is directly connected to.	Null
NetMask	Enter the Network’s netmask which Eth0 or Eth1 is directly connected to.	Null



OSPF

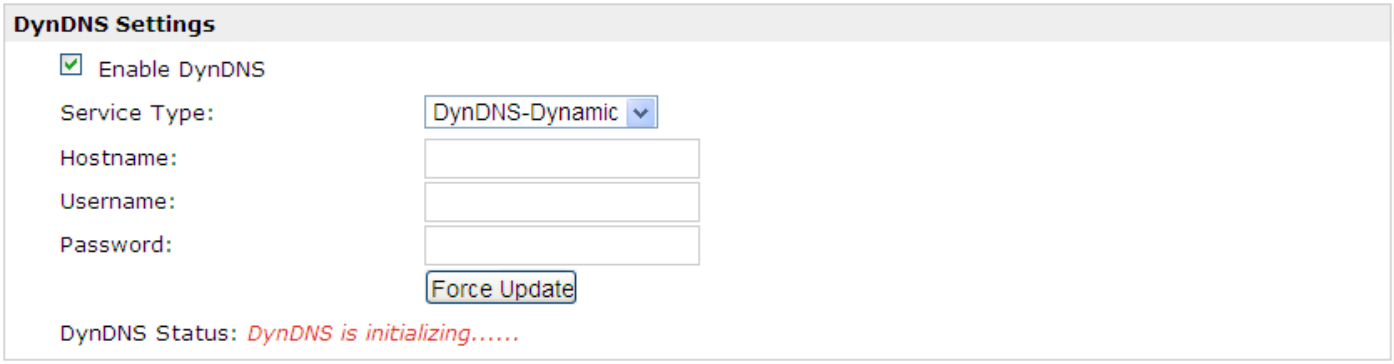
OSPF (Open Shortest Path First) is a link-state routing protocol for IP network. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within an Autonomous System (AS).

IP Routing - OSPF		
Item	Description	Default
Enable OSPFv2	Tick to enable OSPF function.	Disabled

3.19 Configuration ->DynDNS

This section allows users to set up the dynamic DNS service. This service allows you to alias a dynamic IP address to a static hostname, allowing users whose Internet Service Provider (ISP) do not supply them a static IP address. This is especially useful for hosting servers via dynamic IP connections, so that anyone wishing to connect to the server may use a domain name rather than having to know the IP address, which will change from time to time.

DynDNS		
Item	Description	Default
Enable DynDNS	Tick to enable dynamic DNS function.	Disabled
Service Type	Select the dynamic DNS service provider. Multimax supports "DynDNS–Dynamic", "QDNS (3322)" and "NOIP", with which you have to set up an account in advance.	DynDNS–Dynamic
Hostname	Enter the Host name that you get from the service provider.	Null
Username	Enter the user name of your service account.	Null
Password	Enter the password of your service account.	Null
Force Update	Click to force the router to update the current WAN IP to the selected dynamic DNS server.	Null
DynDNS Status	Show the current service status.	Null



3.20 Configuration ->IPsec

This section allows users to set the IPsec (Internet Protocol Security) parameters. IPsec is a protocol for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

IPsec Basic

@ IPsec - Basic		
Item	Description	Default
Enable NAT Traversal	Tick to enable NAT Traversal for IPsec. This item must be enabled when router under NAT environment.	Enabled
Keep alive Interval	The interval that router sends keep alive packets to NAT box so that to avoid being removed from NAT mapping.	30

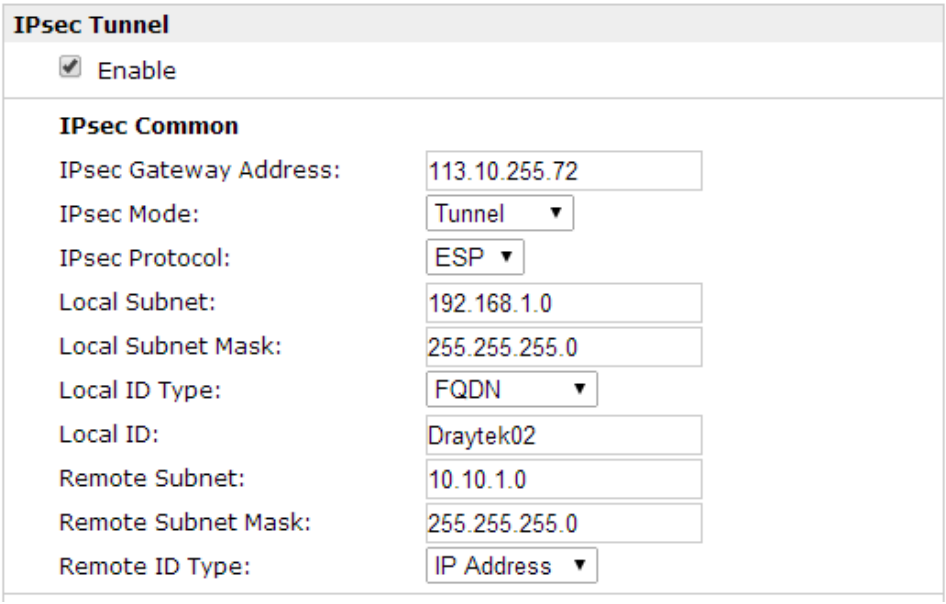
IPsec Tunnel

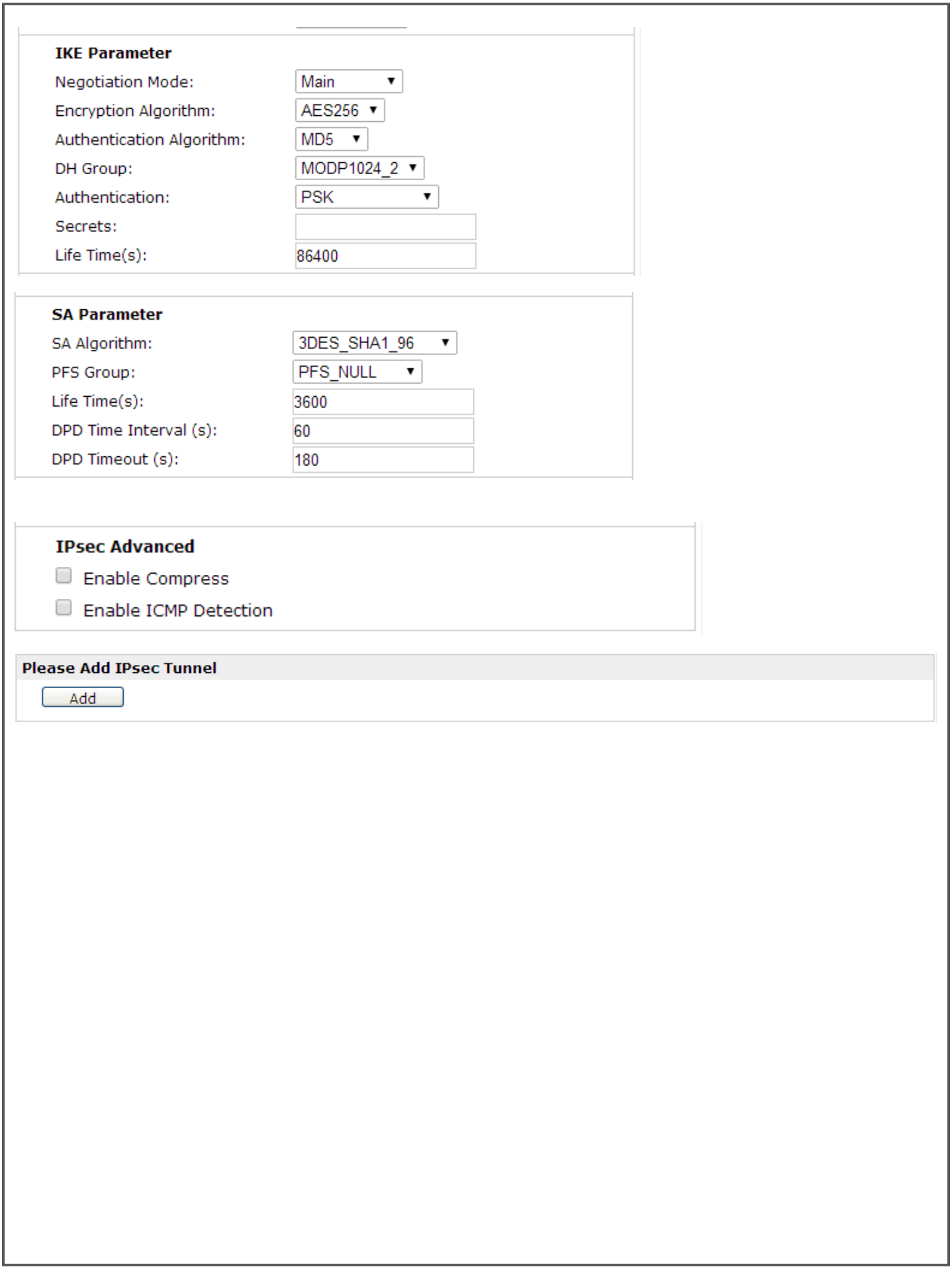
IPsec - Tunnel		
Item	Description	Default
Enable	Enable IPsec Tunnel, the maximum tunnel account is 3	Null
Disable	Disable IPsec Tunnel.	Null
IPsec Gateway Address	Enter the address of the remote IPsec VPN server.	Null
IPsec Mode	Select from “Tunnel” and “Transport”. Tunnel: Commonly used between gateways, or an end-station to a gateway. The gateway is acting as a proxy for the hosts behind it. Transport: Used between end-stations or an end-station and a gateway. If a gateway is acting as a host, for example, an encrypted Telnet session from a workstation to a router, the router is the actual destination.	Tunnel
IPsec Protocol	Select the security protocols from “ESP” and “AH”. ESP: Uses the ESP (Encapsulating Security Payload) protocol. AH: Uses the AH (Authentication Header) protocol.	ESP
Local Subnet	Enter IPsec Local Protected subnet’s address.	Null
Local Subnet Mask	Enter IPsec Local Protected subnet’s mask.	Null
Local ID Type	Select from “Default”, “IP Address”, “FQDN” (Fully Qualified	Default

	Domain Name) and “User FQDN” in IKE (Internet Key Exchange) negotiation. “Default” stands for “IP Address”. IP Address: Uses IP address as the ID in IKE negotiation. FQDN: Uses FQDN type as the ID in IKE negotiation. With this option, a name for the local security gateway (with no “@”in between) is required as the Local ID, e.g., test.maxon.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. With this option, a name for the local security gateway (containing an“@”symbol) is required as the Local ID, e.g., test@maxon.com.	
Remote Subnet	Enter IPsec Remote Protected subnet’s address.	Null
Remote Subnet Mask	Enter IPsec Remote Protected subnet’s mask.	Null
Remote ID Type	Select from “Default”, “IP Address”, “FQDN” and “User FQDN” in IKE negotiation. IP Address: Uses IP address as the ID in IKE negotiation. FQDN: Uses FQDN type as the ID in IKE negotiation. With this option, a name for the remote security gateway (with no “@” in between) is required as the Remote ID, e.g., test.maxon.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. With this option, a name for the remote security gateway (containing an “@” symbol) is required as the Remote ID, e.g., test@maxon.com.	Default
Negotiation Mode	Select from “Main” and “Aggressive” modes, which will be used for IKE negotiation in Phase 1. If the IP address at one end of an IPsec tunnel is dynamic, the IKE negotiation mode must be aggressive. In this case, SA (Security Association) can be established once the username and password are correct.	Main
Encryption Algorithm	Select from “DES”, “3DES”, “AES128”, “AES192” and “AES256”to be used in IKE negotiation. DES: Uses the DES algorithm in CBC mode and 56-bit key. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key. AES192: Uses the AES algorithm in CBC mode and 192-bit key. AES256: Uses the AES algorithm in CBC mode and 256-bit key.	3DES
Authentication Algorithm	Select from “MD5” and “SHA1”to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
DH Group	Select from “MODP768_1”, “MODP1024_2” and “MODP1536_5”to be used in IKE negotiation phase 1. MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	MODP1024_2

Authentication	Select from “PSK”, “CA”, “XAUTH Init PSK” and “XAUTH Init CA” to be used in IKE negotiation. PSK: Pre-shared Key. CA: Certification Authority. XAUTH: Extended Authentication to AAA server.	PSK
Secrets	Enter the Pre-shared Key.	Null
Life Time @ IKE Parameter	Set the lifetime (in seconds) for IKE negotiation. Before an SA expires, IKE negotiates a new SA. Once a new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
SA Algorithm	Select from “DES_MD5_96”, “DES_SHA1_96”, “3DES_MD5_96”, “3DES_ SHA1_96”, “AES128_MD5_96”, “AES128_ SHA1_96”, “AES192_MD5_96”, “AES192_ SHA1_96”, “AES256_MD5_96” and “AES256_ SHA1_96” when “ESP” is selected for IPSec protocol; Select from “AH_MD5_96” and “AH_ SHA1_96” when “AH” is selected for IPSec protocol; **Note**: Higher security means more complexity in implementation and slower speed. In general, DES is enough to meet general requirements. Use 3DES when higher security level is required.	3DES_MD5_96
PFS Group	Select from “PFS_NULL”, “MODP768_1”, “MODP1024_2” and “MODP1536_5”. PFS_NULL: Disable PFS Group MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	PFS_NULL
Life Time @ SA Parameter	Set the IPsec SA lifetime (in seconds). **Note**: During negotiation of setting up an IPsec SA, IKE will use the smaller value between the locally set lifetime and the one proposed by the peer.	28800
DPD Time Interval	Set the interval in seconds after which DPD (Dead Peer Detection) is triggered if no IPsec protected packets are received from the peer. Dead peer detection (DPD) is a method that network devices use to verify the current existence and availability of other peer devices. When the local device is sending out an IPsec packet, DPD will check the time when the last IPsec packet was received from the peer. If the time period exceeds the specified interval, DPD will send a DPD notification to the peer. If no DPD acknowledgement is received within the DPD packet retransmission interval, it will retransmit the DPD hello. If still no DPD acknowledgement is received after a maximum number of retransmission attempts, DPD will consider the peer as dead, and remove the IKE SA and those IPSec SAs based on the IKE SA for that peer.	180
DPD Timeout	Set the interval (in seconds) for DPD packet re transmission.	60

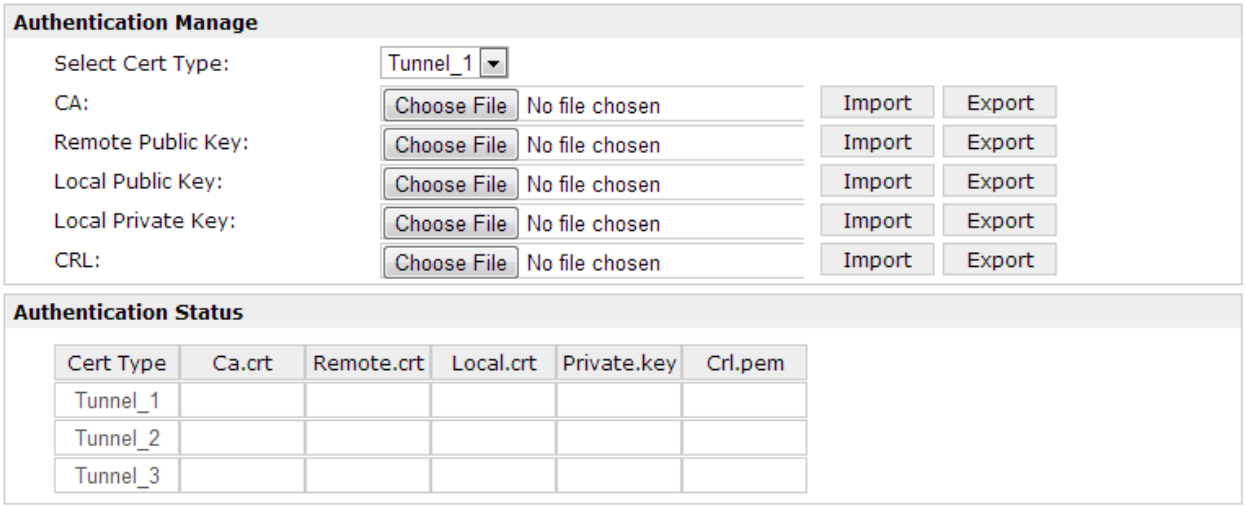
VPN Over IPsec Type	Select from “None”, “L2TP” and “GRE”. L2TP Over IPsec: Encrypt theL2TP tunnels using IPsec. GRE Over IPsec: Encrypt the GRE tunnels using IPsec.	None
Enable Compress	Tick to enable compressing the inner headers of IP packets.	Disabled
Enable ICMP Detection	Click to enable ICMP detection.	Disabled
ICMP Detection Server	Enter the IP address or domain name or remote server. Router will ping this address/domain name to check that if the current connectivity is active.	Null
ICMP Detection Local IP	Set the local IP address.	Null
ICMP Detection Interval	Set the ping interval time.	30
ICMP Detection Timeout	Set the ping timeout.	5
ICMP Detection Retries	If Router ping the preset address/domain name times out continuously for Max Retries time, it will try to re-establish the VPN tunnel.	3
Please Add IPsec Tunnel	Click “Add” to add the defined IPsec Tunnel	Null




IKE Parameter
Negotiation Mode: Main
Encryption Algorithm: AES256
Authentication Algorithm: MD5
DH Group: MODP1024_2
Authentication: PSK
Secrets:
Life Time(s): 86400
SA Parameter
SA Algorithm: 3DES_SHA1_96
PFS Group: PFS_NULL
Life Time(s): 3600
DPD Time Interval (s): 60
DPD Timeout (s): 180
IPsec Advanced
Enable Compress
Enable ICMP Detection
Please Add IPsec Tunnel
Add

X.509

IPSec – X.509		
Item	Description	Default
Select Cert Type	Select the IPsec tunnel to set up the certificates.	None
CA	Click “Browse” to select the appropriate CA file from your PC, and then “Import” to load it to the router. Click “Export” to save the CA file to your PC.	Null
Remote Public Key	Click “Browse” to select the appropriate Remote Public Key file from your PC, and then “Import” to load it to the router. Click “Export” to save the Remote Public Key file to your PC.	Null
Local Public Key	Click “Browse” to select the appropriate Local Public Key file from your PC, and then “Import” to load it to the router. Click “Export” to save the Local Public Key file to your PC.	Null
Local Private Key	Click “Browse” to select the appropriate Local Private Key file from your PC, and then “Import” to load it to the router. Click “Export” to save the Local Private Key file to your PC.	Null
CRL	Click “Browse” to select the correct CRL file from your PC, and then click “Import” to load it to the router. Click “Export” to save the CRL file to your PC.	Null
Authentication Status	Show the current authentication status of IPsec tunnels.	Null



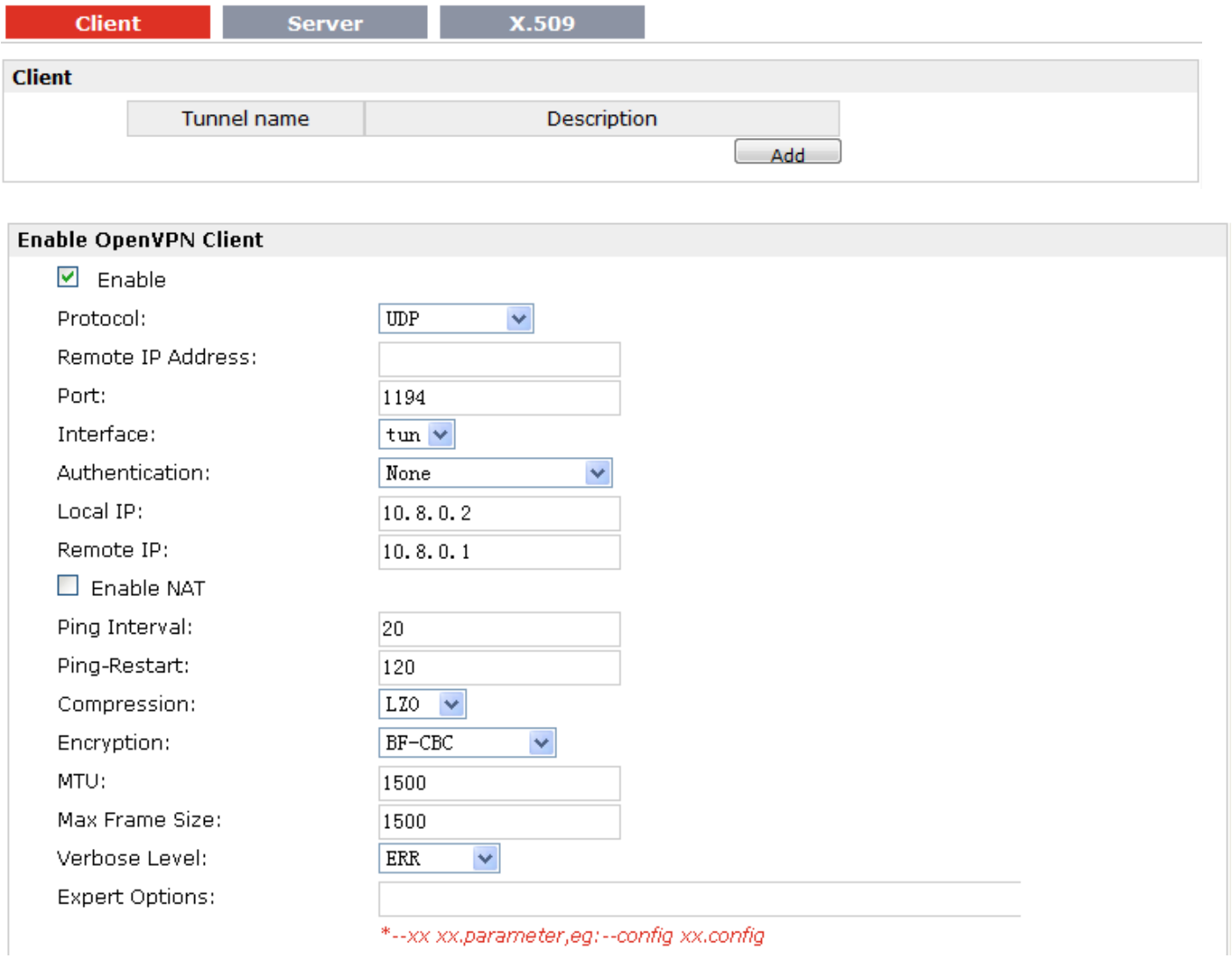
3.21 Configuration -> Open VPN

This section allows users to set the Open VPN parameters.

Client

Open VPN - Client		
Item	Description	Default
Enable	Enable OpenVPN Client, the maximum tunnel account is 3.	Null
Protocol	Select from “UDP” and “TCP Client” which depends on the application.	UDP
Server Address	Enter the IP address or domain name of the remote OpenVPN server.	Null
Port	Enter the listening port of the remote OpenVPN server.	1194
Interface	Select from “tun” and “tap”, which are two different types of device interface for OpenVPN. The difference between “tun” and “tap” device is that, a “tun” device is a virtual IP point-to-point device and a “tap” device is a virtual Ethernet device.	tun
Authentication	Select from four different types of authentication methods: “Pre-shared”, “Username/Password”, “X.509 cert”, and “X.509 cert+user”.	None
Local IP	Define the local IP address of the OpenVPN tunnel.	10.8.0.2
Remote IP	Define the remote IP address of the OpenVPN tunnel.	10.8.0.1
Enable NAT	Tick to enable NAT Traversal for OpenVPN tunnel. This item must be enabled when the router is under NAT environment.	Disabled
Ping Interval	Set ping interval (in seconds) to check if the tunnel is active.	20
Ping -Restart	Re-establish the OpenVPN tunnel if constantly fails for the specified time period (in seconds).	120
Compression	Select “None” for no compression, or “LZO” for using the LZO compression library to compress the data stream.	LZO
Encryption	Select from “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES128-CBC”, “AES192-CBC”, and “AES256-CBC”. BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key. DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key. AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key. AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.	BF-CBC
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Maximum Frame Size for transmission.	1500

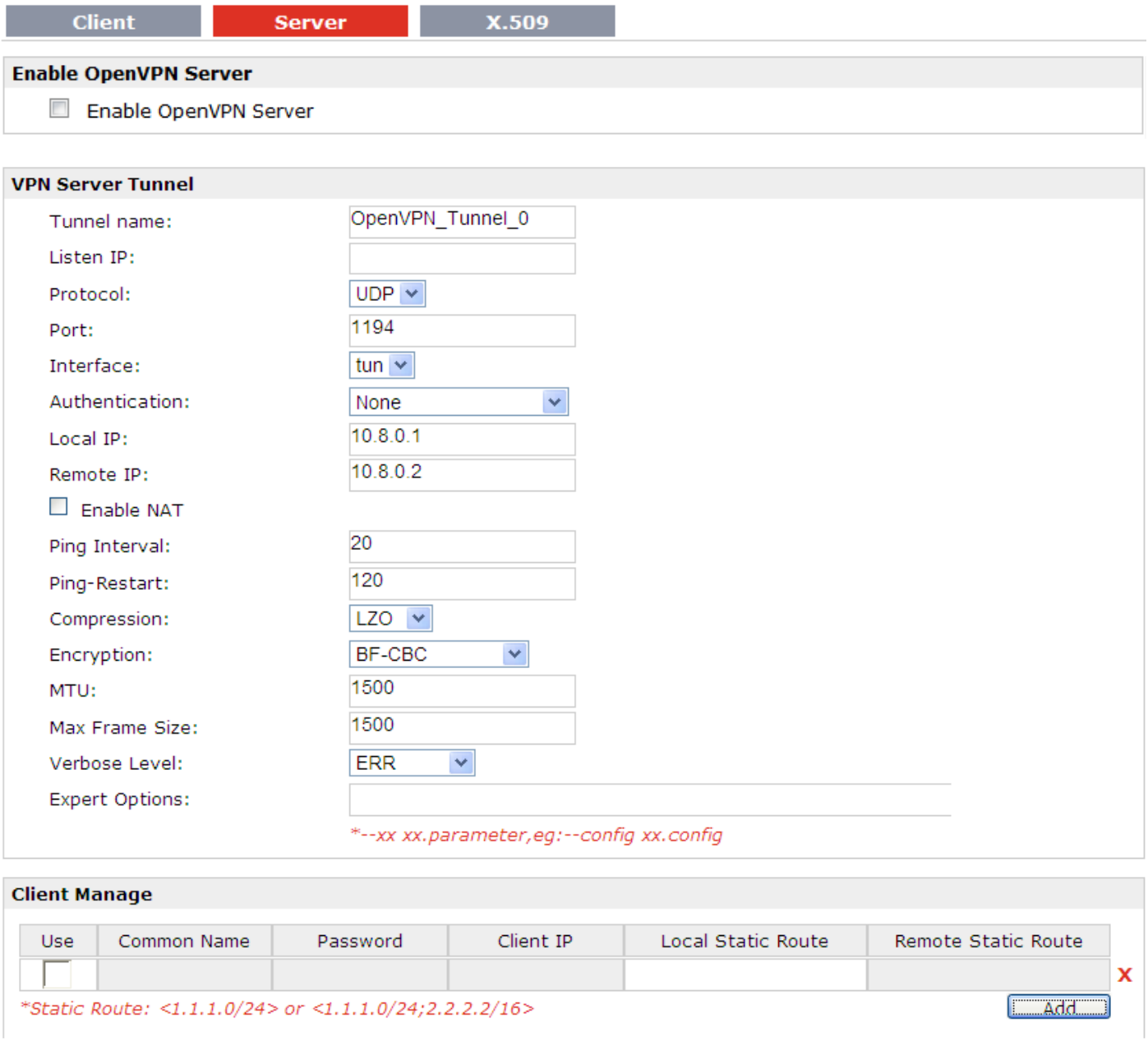
Verbose Level	Select the log output level which from low to high: “ERR”, “WARNING”, “NOTICE” and “DEBUG”. Higher level will output more log information.	ERR
Expert Options	Users can enter some PPP initialization strings in this field. Each string can be separated by a space.	Null



Server

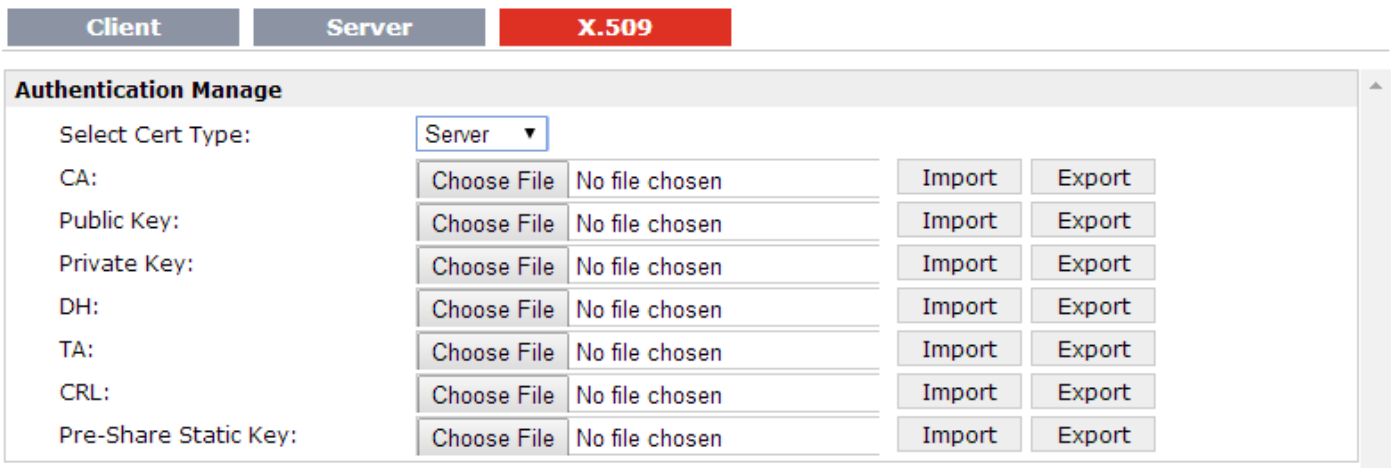
Open VPN - Server		
Item	Description	Default
Enable OpenVPN Server	Tick to enable OpenVPN server tunnel.	Disabled
Tunnel name	The name of the OpenVPN server. The name is generated automatically and not user configurable	Tunnel_OpenVPN_0
Listen IP	You can enter the IP address of cellular WAN, Ethernet WAN or Ethernet LAN. Null or 0.0.0.0 stands for using the active WAN link -cellular WAN or Ethernet WAN.	0.0.0.0
Protocol	Select from “UDP” and “TCP” which depends on the application.	UDP
Port	Set the local listening port	1194
Interface	Select from “tun” and “tap” which are two different types of device interface for OpenVPN.	tun
Authentication	Select from four different types of authentication ways: “Pre-shared”, “Username/Password”, “X.509 cert” and “X.509 cert+user”.	None
Local IP	Define the local IP address of OpenVPN tunnel.	10.8.0.1
Remote IP	Define the remote IP address of OpenVPN tunnel.	10.8.0.2
Enable NAT	Tick to enable NAT Traversal for OpenVPN. This item must be enabled when the router is under NAT environment.	Disabled
Ping Interval	Set ping interval (in seconds) to check if the tunnel is active.	20
Ping -Restart	Re-establish the OpenVPN tunnel if ping constantly fails for the specified time period (in seconds).	120
Compression	Select from “None” and “LZO”, select “LZO” to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES128-CBC”, “AES192-CBC” and “AES256-CBC”. BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key. DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key. AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key. AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.	BF-CBC
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Maximum Frame Size for transmission.	1500

Verbose Level	Select the log output level which from low to high: “ERR”, “WARNING”, “NOTICE” and “DEBUG”. The higher level will output more log information.	ERR
Expert Options	Users can enter some PPP initialization strings in this field. Each string can be separated by a space.	Null
Client Manage	Click “Add” to add a OpenVPN client, including “Common Name”, “Password”, “Client IP”, “Local Static Route” and “Remote Static Route”. This field can be configured only when you select “Username/Password” in“ Authentication”.	Null



X.509

Open VPN – X.509		
Item	Description	Default
Select Cert Type	Select the OpenVPN client or server to set up the certificates.	Null
CA	Click “Browse” and then “Import” for the router to get the appropriate CA file from your PC. Click “Export” to save the CA file to your PC.	Null
Public Key	Click “Browse” and then “Import” for the router to get the appropriate Public Key file from your PC. Click “Export” to save the Public Key file to your PC.	Null
Private Key	Click “Browse” and then “Import” for the router to get the appropriate Private Key file from your PC. Click “Export” to save the Private Key file to your PC.	Null
DH	Click “Browse” and then “Import” for the router to get the appropriate DH file from your PC. Click “Export” to save the DH file to your PC.	Null
TA	Click “Browse” and then “Import” for the router to get the appropriate TA file from your PC. Click “Export” to save the TA file to your PC.	Null
CRL	Click “Browse” and then “Import” for the router to get the appropriate CRL file from your PC. Click “Export” to save the CRL file to your PC.	Null
Pre-Share Static Key	Click “Browse” and then “Import” for the router to get the appropriate Pre-Share Static Key file from your PC. Click “Export” to save the Pre-Share Static Key file to your PC.	Null



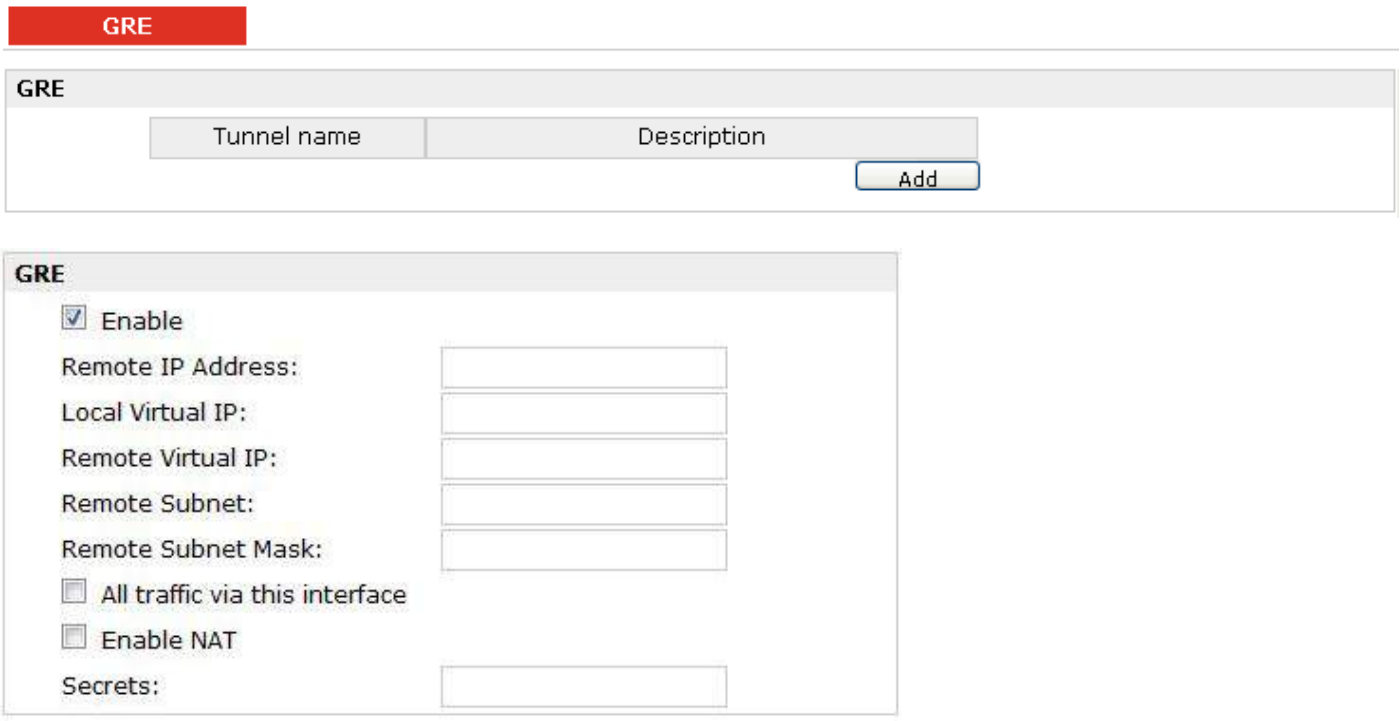
Authentication Status

Cert Type	CA	Public Key	Private Key	DH	TA	CRL	PKCS12	Pre-Share
Server								
Client_1	OK	OK	OK					OK
Client_2								
Client_3								

3.22 Configuration -> GRE

This section allows users to set up the GRE (Generic Routing Encapsulation) parameters. GRE is a protocol that encapsulates packets in order to route other protocols over IPnetworks.

GRE		
Item	Description	Default
Add	Click “Add” to add a GRE tunnel.	
Enable	Click to enable GRE tunnel.	Disabled
Remote IP Address	Set remote IP Address of the GRE Server.	Null
Local Virtual IP	Set local IP Address of the virtual GRE tunnel.	Null
Remote virtual IP	Set remote IP Address of the virtual GRE tunnel.	Null
Remote Subnet	Add a static route to the remote subnet so that the remote network is known to the local network.	Null
Remote Subnet Mask	Set the remote subnet netmask.	Null
All traffic via this interface	After enabling this feature, all data traffic will be sent via GRE tunnel.	Disabled
Enable NAT	Tick to enable NAT for GRE. The source IP address of the host behind the Multimax will be disguised for accessing the remote GRE server.	Disabled
Secrets	Set Tunnel Key of GRE.	Null



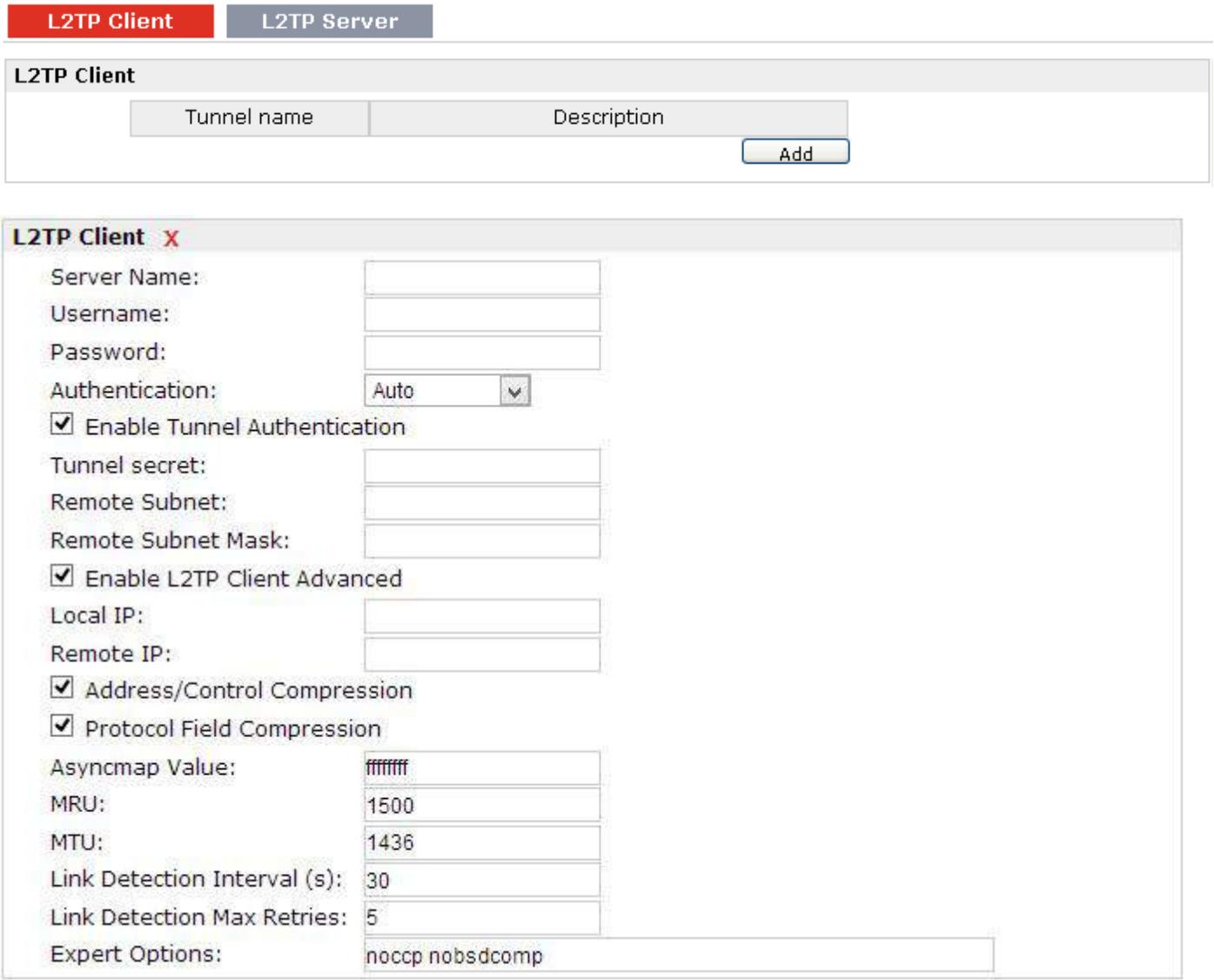
3.23 Configuration -> L2TP

This section allows users to set up the L2TP tunnel (Server or Client).

Client

L2TP - Client		
Item	Description	Default
Add L2TP Client	Click “Add” to add a L2TP client. You can add up to 3 L2TP clients. Click “ ” to delete an existing L2TP client.	Null
Server Name	Enter your L2TP server’s public IP or domain name.	Null
Username	Enter the username that is required by the L2TP server.	Null
Password	Enter the password that is required by the L2TP server.	Null
Authentication	Select from “Auto”, “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. You need to select the correct authentication method based on the server’s configuration. When you select “Auto”, the router will automatically select the correct method based on the server’s setting.	Disabled
Enable Tunnel Authentication	Tick to enable tunnel authentication and enter the tunnel secret provided by the L2TP server.	Disabled
Remote Subnet	Enter the L2TPremote protected subnet.	Null
Remote Subnet Mask	Enter the L2TPremote Protected netmask.	Null
Show L2TP Client Advanced	Tick to enable the L2TP client advanced setting.	Disabled
Local IP	Set the IP address of the L2TP client. You can enter the IP that assigned by L2TP server. Null means L2TP client will obtain an IP address automatically from L2TP server’s IP pool.	Null
Remote IP	Enter the peer’s private IP address or remote subnet’s gateways address.	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as a default.	Enabled
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as a default.	Enabled
Asyncmap Value	One of the L2TP initialization strings. In general, you don’t need to change this value.	ffffffff
MRU	Maximum Receiving Unit. The identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between L2TP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no	30

	response from the peer within a specified period of time, it will retransmit the PPP echo. If no response from the peer is received after the set number of maximum retries, it is considered that the L2TP tunnel is down and the client will try to re-establish a tunnel with the peer.	
Link Detection Max Retries	Specify the maximum retries for L2TP link detection.	5
Expert Options	Users can enter some extra PPP initialization strings in this field. Each string can be separated by a space.	noccpno bsdcom p



Server

L2TP - Server		
Item	Description	Default
Enable L2TP Server	Tick to enable L2TP server.	Disabled
Username	Set the username that will be used by L2TP client.	Null
Password	Set the password that will be used by L2TP client.	Null
Authentication	Select from “Auto”, “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. You need to make sure the same authentication method used by the client.	CHAP
Enable Tunnel Authentication	Tick to enable tunnel authentication and enter the tunnel secret that will provide to L2TP client.	Disabled
Local IP	Set the IP address of L2TP server.	10.0.0.1
IP Pool Start	Set the IP pool start IP address that will assign to the L2TP clients.	10.0.0.2
IP Pool End	Set the IP pool end IP address that will assign to the L2TP clients.	10.0.0.100
Enable L2TP Server Advanced	Tick to show the L2TP server advanced setting.	Disabled
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enabled
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enabled
Asyncmap Value	One of the L2TP initialization strings. In general, you don’t need to modify this value.	ffffffff
MRU	Maximum Receiving Unit. The identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. The identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between L2TP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo requests to each other. If the client or server receives no response from the peer within a specified period of time, it will retransmit the PPP echo. If no response from the peer is received after the set number of maximum retries, it is considered that the L2TP tunnel is down and the client will try to re-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the maximum retries for L2TP link detection.	5
Expert Options	You can enter some extra PPP initialization strings in this field. Each string can be separated by a space.	noccpnobsdcomp
Route Table List	Click “Add” to add a route rule from L2TP server to L2TP client.	Null

L2TP Client | L2TP Server

Enable L2TP Server

☐ Enable L2TP Server

L2TP Common Settings

Username:	
Password:	
Authentication:	Auto

☑ Enable Tunnel Authentication

Tunnel secret:	
Local IP:	
IP Pool Start:	10.0.0.2
IP Pool End:	10.0.0.100

L2TP Server Advanced

☑ Enable L2TP Server Advanced

☑ Address/Control Compression

☑ Protocol Field Compression

Asyncmap Value:	ffffffff
MRU:	1500
MTU:	1436
Link Detection Interval (s):	30
Link Detection Max Retries:	5
Expert Options:	noccp nobsdcomp

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask

("0.0.0.0" means any) Add

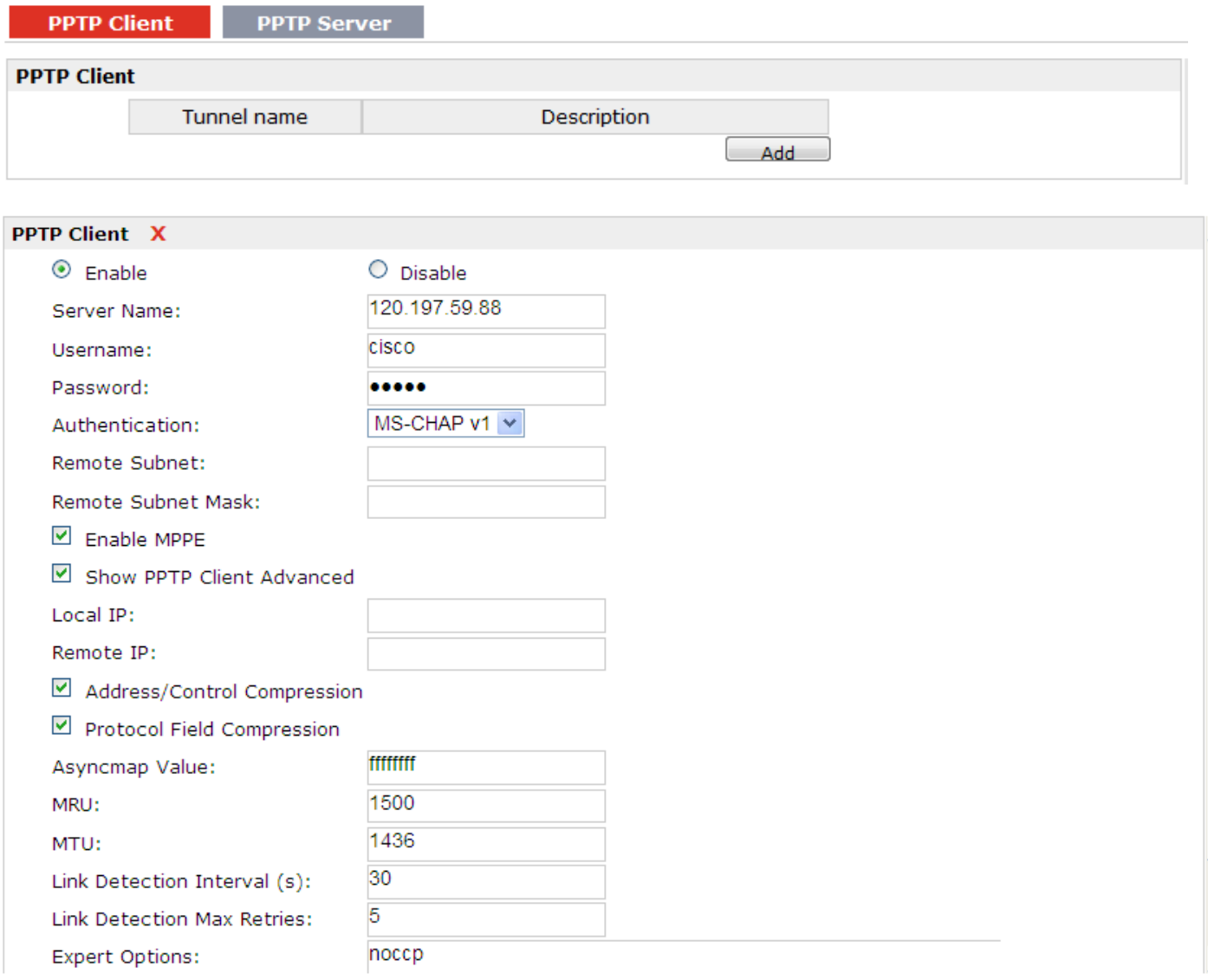
3.24 Configuration -> PPTP

This section allows users to set up the L2TP tunnel (Server or Client).

Client

PPTP - Client		
Item	Description	Default
Add	Click “Add” to add a PPTP client	N/A
Enable	Enable the PPTP Client. The max tunnel accounts are 3.	Null
Disable	Disable PPTP Client.	Null
Remote IP Address	Enter the PPTP server’s public IP address or domain name.	Null
Username	Enter the username that was provided by your PPTP server.	Null
Password	Enter the password that was provided by your PPTP server.	Null
Authentication	Select from “Auto”, “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. You need to select the correct authentication method based on the server’s configuration. When you select “Auto”, the router will automatically select the correct method based on the server’s setting.	Auto
Remote Subnet	Enter PPTP remote protected subnet.	Null
Remote Subnet Mask	Enter PPTP remote Protected netmask.	Null
Enable MPPE	Tick to enable MPPE (Microsoft Point-to-Point Encryption). It’s a protocol for encrypting data across PPP and VPN links.	Disabled
Enable PPTP Client Advanced	Tick to enable the PPTP client advanced setting.	Disabled
Local IP	Set the IP address of the PPTP client. You can enter the IP that assigned by PPTP server. Null means PPTP client will obtain an IP address automatically from PPTP server’s IP pool.	Null
Remote IP	Enter the remote peer’s private IP address or remote subnet’s gateways address.	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as a default.	Enabled
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as a default.	Enabled
Asyncmap Value	One of the PPTP initialization strings. In general, you don’t need to modify this value.	ffffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection	Specify the interval between PPTP client and server.	30

Interval	To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it will retransmit the PPP echo. If no response from the peer is received after the set number of maximum retries, it is considered that the PPTP tunnel is down and the client will try to re-establish a tunnel with the peer.	
Link Detection Max Retries	Specify the maximum retries for PPTP link detection.	5
Expert Options	You can enter some extra PPP initialization strings in this field. Each string can be separated by a space.	noccpnobs dcomp



Server

PPTP - Server		
Item	Description	Default
Enable PPTP Server	Tick to enable PPTP server.	Disabled
Username	Set the username that will assign to PPTP client.	Null
Password	Set the password that will assign to PPTP client.	Null
Authentication	Select from “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. PPTP client need to select the same authentication method based on this server’s authentication method.	CHAP
Local IP	Set the IP address of PPTP server.	10.0.0.1
IP Pool Start	Set the IP pool start IP address that will assign to the PPTP clients.	10.0.0.2
IP Pool End	Set the IP pool end IP address that will assign to the PPTP clients.	10.0.0.100
Enable MPPE	Tick to enable MPPE (Microsoft Point-to-Point Encryption). It’s a protocol for encrypting data across PPP and VPN links.	Disabled
Enable PPTP Server Advanced	Tick to show the PPTP server advanced setting.	Disabled
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enabled
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enabled
Asyncmap Value	One of the PPTP initialization strings. In general, you don’t need to modify this value.	ffffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between PPTP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it will retransmit the PPP echo. If no response from the peer is received after the set number of maximum retries, it is considered that the PPTP tunnel is down and the client will try to re-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the maximum retries for PPTP link detection.	5
Expert Options	You can enter some extra PPP initialization strings in this field. Each string can be separated by a space.	noccpnobs dcomp
Route Table List	Click “Add” to add a route rule from PPTP server to PPTP client.	Null

PPTP Client | PPTP Server

Enable PPTP Server

☑ Enable PPTP Server

PPTP Common Settings

Username:	
Password:	
Authentication:	CHAP
Local IP:	10. 0. 0. 1
IP Pool Start:	10. 0. 0. 2
IP Pool End:	10. 0. 0. 100

☐ Enable MPPE

PPTP Server Advanced

☑ Enable PPTP Server Advanced
☑ Address/Control Compression
☑ Protocol Field Compression

Asyncmap Value:	ffffffff
MRU:	1500
MTU:	1436
Link Detection Interval (s):	30
Link Detection Max Retries:	5
Expert Options:	noccp nobsdcomp

Route Table List

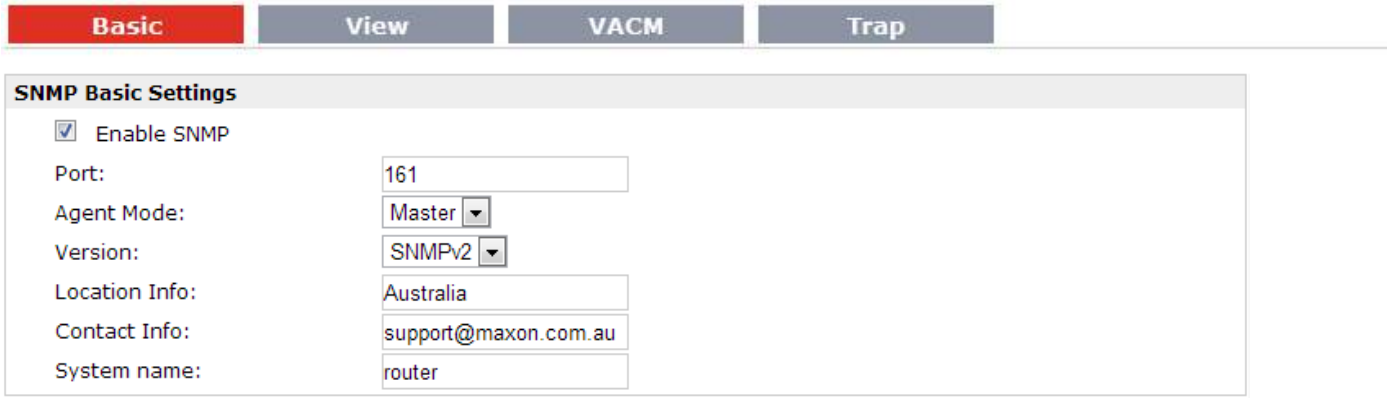
Client IP	Remote Subnet	Remote Subnet Mask
("0.0.0.0" means any)		Add

3.25 Configuration -> SNMP

This section allows users to set up the SNMP (Simple Network Management Protocol) parameters.

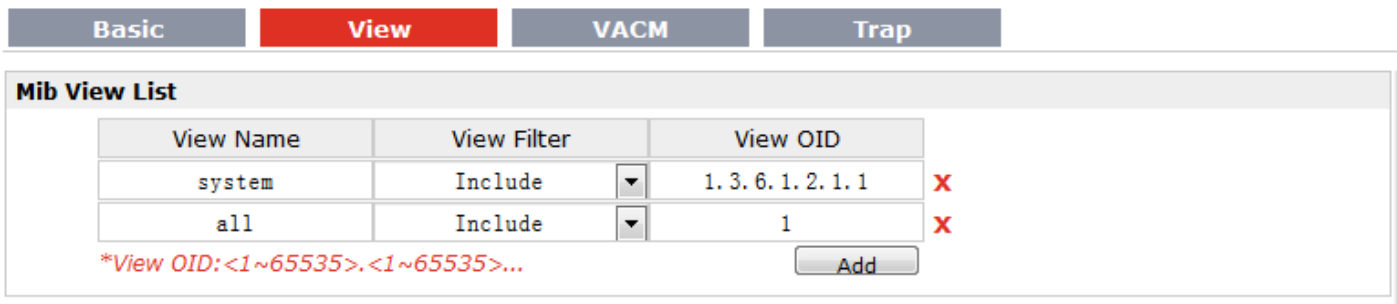
Basic

SNMP - Basic		
Item	Description	Default
Port	UDP port for sending and receiving SNMP requests.	161
Agent Mode	Select the proper agent mode.	Master
Version	Select from “SNMPv1”, “SNMPv2” and “SNMPv3”.	SNMPv2
Location Info	Enter the router’s location info that will be sent to an SNMP client.	Australia
Contact Info	Enter the router’s contact info that will be sent to an SNMP client.	support@maxon.com.au
System name	Enter the router’s system name that will be sent to an SNMP client.	router



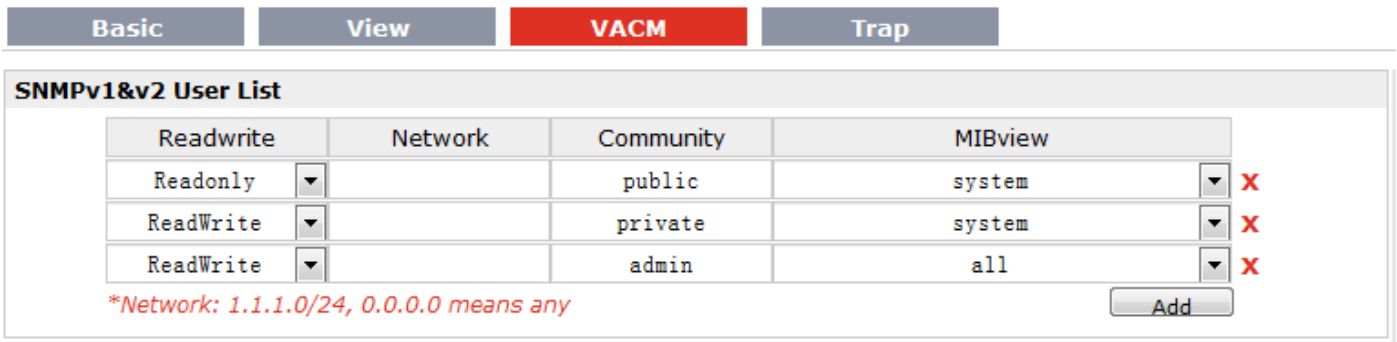
View

SNMP - View		
Item	Description	Default
View Name	Enter the View Name	Null
View Filter	Select from “Include” and “Exclude”.	Include
View OID	Enter the Object Identifiers (OID)	Null



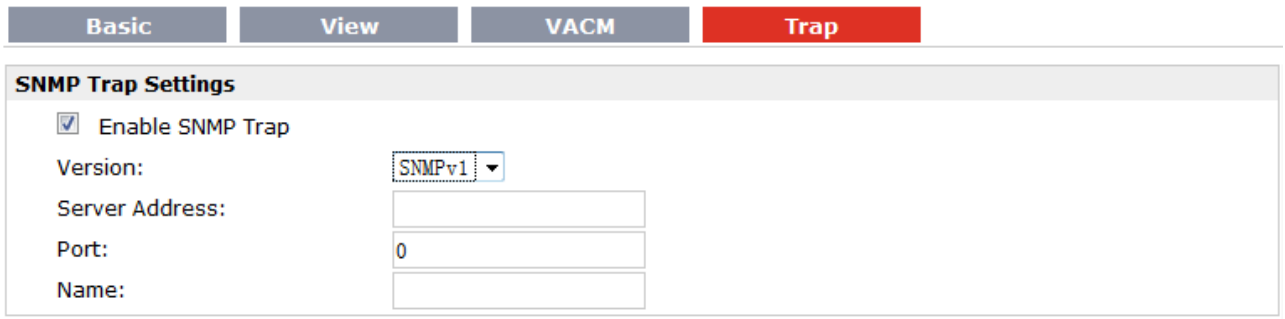
VACM

SNMP - VACM		
Item	Description	Default
Readwrite	Select the access rights from “Readonly” and “ReadWrite”.	Readonly
Network	Define the network from which is allowed to access. E.g. 172.16.0.0.	Null
Community	Enter the community name.	Null
MIBview	Select from “none”, “system” and “all”	none



Trap

SNMP - Trap		
Item	Description	Default
Enable SNMP Trap	Click to enable SNMP Trap feature.	Disable
Version	Select from “SNMPv1”, “SNMPv2” and “SNMPv3”.	SNMPv1
Server Address	Enter the SNMP trap server’s IP address.	Null
Port	Enter SNMP trap server’s port number	0
Name	Enter SNMP server’s name.	Null



3.26 Configuration -> VRRP

This section allows users to set up the VRRP (Virtual Router Redundancy Protocol) service. VRRP is an Internet protocol that provides a way to have one or more backup routers when using a statically configured router on a local area network (LAN).

VRRP		
Item	Description	Default
Enable VRRP	Tick to enable the VRRP protocol.	Disabled
Group ID	Specify which VRRP group of this router belongs to.	1
Priority	Enter the priority value from 1 to 255. The larger value has higher priority.	100
Interval	The interval at which the master router sends keep alive packets to backup routers.	10
Virtual IP	A virtual IP address is shared among the routers as the gateway IP in the LAN. The router with the same IP as the virtual IP is the master router and the others are backups. In case the master fails, the virtual IP address is mapped to a backup router's IP address according to its priority and this backup router becomes the master router.	192.168.0.1

3.27 Configuration -> IP Passthrough

This section allows users to set up the IP Pass through parameters. In IP Passthrough mode, Multimax acts as a PPPoE server and will pass its WAN IP address to PPPoE client directly. Packets received from the WAN interface are delivered directly to the LAN interface. Similarly, packets received for the LAN interface (everything except broadcasts/multicasts) are sent to the WAN interface.

IP Passthrough		
Item	Description	Default
Enable IP Passthrough	Tick to enable IP Passthrough feature. **Note**: To be able to use this feature, "Cellular" has to be selected as" Primary Interface" in tab "Configuration"->"Link Management".	Disabled
Mode	"PPPoE" is the only option for mode.	PPPoE
Ethernet Interface	Set the LAN interface from "LAN_0" and"LAN_1". PPPoE client dials up to Multimax (PPPoE server) on the LAN interface selected. For example when LAN_0 is selected and connected to aPPPoE client, e.g. a PC, the PC will dial up to Multimax (PPPoE server) through LAN_0. **Note**: It doesn't matter whether you select "LAN_0" or "LAN_1"If enabling bridge mode in tab "Configuration" ->"Ethernet" ->"LAN Interface".	LAN_0
Username	Set the username of the PPPoE server.	Null
Password	Set the password of the PPPoE server.	Null
AC Name	Set the AC (Access Concentrator) name of the PPPoE server.	Null
Service Name	Set the service name of the PPPoE server. **Note**: the PPPoE client needs to use the same username, password, AC name, and service name of the PPPoE server, or it will fail to dial up to the server.	Null
Authentication	Set up the PPP authentication method by selecting one of the following: "Auto", "PAP", and "CHAP".	Auto
Link Detection Interval(s)	When the PPPoE client dials up to Multimax (PPPoE server), the Multimax will send a "LCP Echo Request" to PPPoE client with this interval. The interval can be configured from 3 to 30 seconds.	30
Link Detection Max Retries	If the Multimax does not get response after sending "LCP Echo Request", it will do retries. If still fails to get a response after a maximum retires, the Multimax will send a "LCP Terminal Request" packet to disconnect the connection between PPPoE server and client. The maximum retries can be from 3 to 5 times.	5

IP Passthrough

IP Passthrough Settings

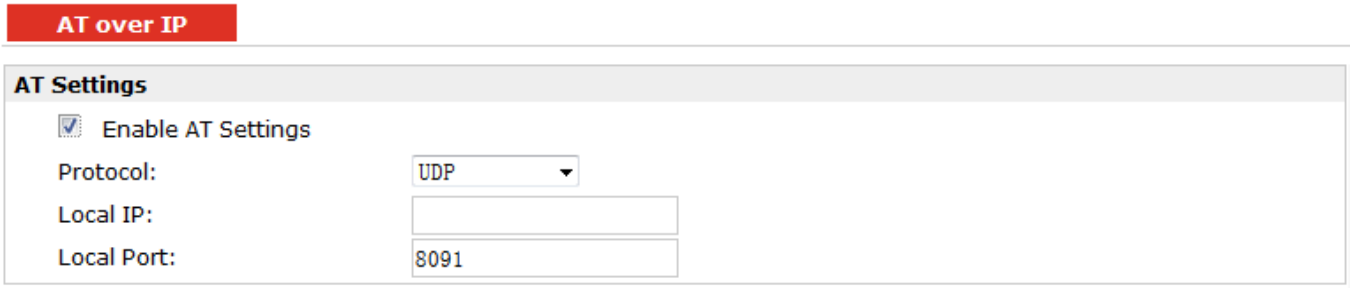
- [x] Enable IP Passthrough

Mode:	PPPoE
Ethernet Interface:	LAN_0
Username:	
Password:	
AC Name:	
Service Name:	
Authentication:	Auto
Link Detection Interval(s):	30
Link Detection Max Retries:	5

3.28 Configuration -> AT over IP

This section allows users to set up the AT over IP parameters.

AT over IP		
Item	Description	Default
Enable AT Settings	Tick to enable the AT over IP function for remotely controlling the cellular module via AT command.	Disabled
Protocol	Select from “TCP server” or “UDP”	UDP
Local IP	You can enter the IP address of the cellular WAN, Ethernet WAN or Ethernet LAN. Null or 0.0.0.0 stands for all these three IP addresses.	0.0.0.0
Local Port	Enter the local TCP or UDP listening port.	8091

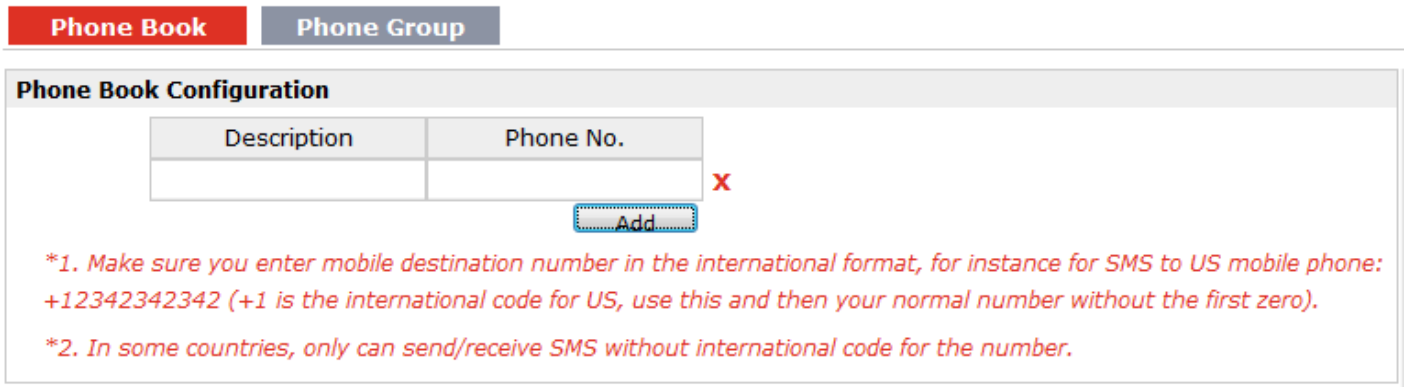


3.29 Configuration -> Phone Book

This section allows users to set up the Phone Book.

Phone Book

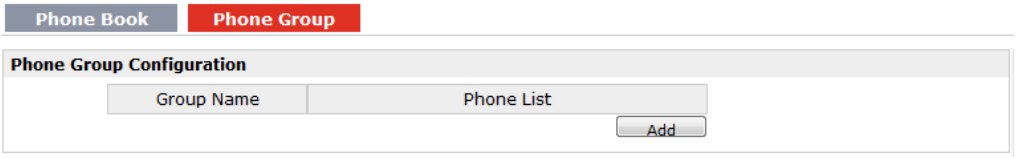
Phone Book – Phone Book		
Item	Description	Default
Description	Set up a name for corresponding phone No.	Null
Phone No.	Enter the phone No. **Note**: Please use international format; This begins with a "+" followed by the country code and number.	Null

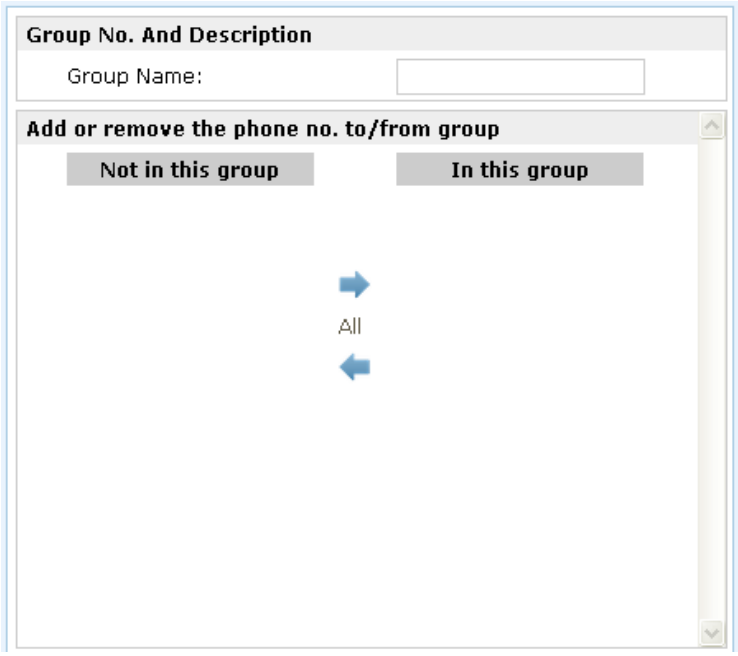


Phone Group

Phone Book – Phone Group		
Item	Description	Default
Group Name	Name of the phone group.	Null
Phone List	Show the phone list in the group.	Null
Add	Click "Add" to create a new phone group.	N/A
Add or remove the phone No. to/from group	This box will appear when users click either a phone group or "Add" button. Click right arrow to add a selected phone No.to the group, or Click left arrow to remove a selected phone No. from the group.	Null

Note: Phone group cannot be set up if there are no phone numbers in the phone book.

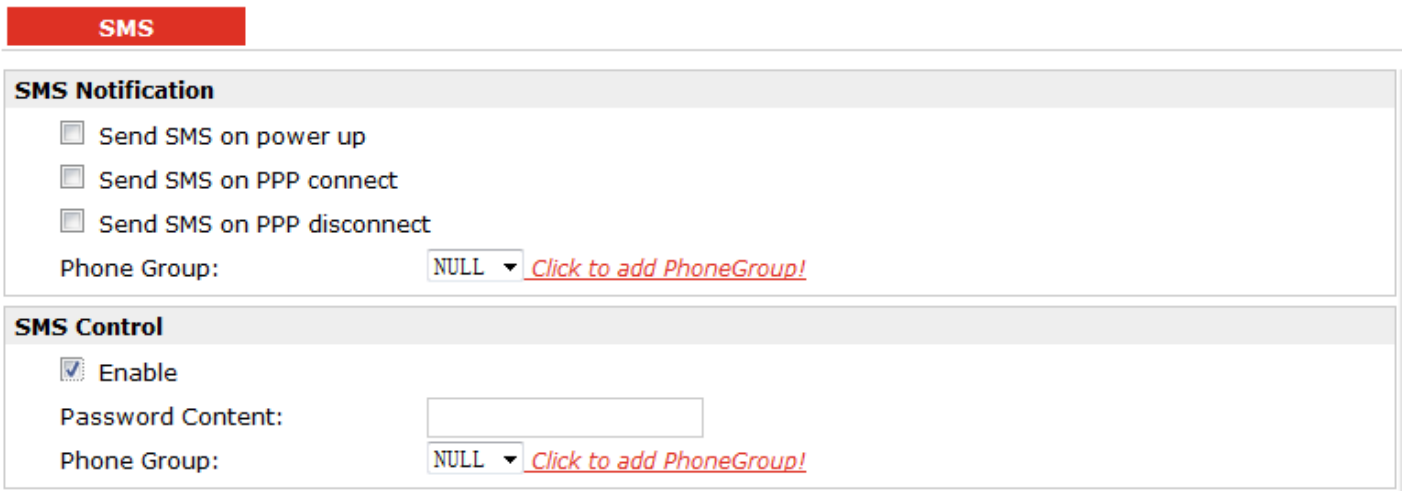



Group No. And Description
Group Name:
Add or remove the phone no. to/from group
Not in this group
In this group
All

3.30 Configuration -> SMS

This section allows users to set the SMS Notification and SMS Controls.

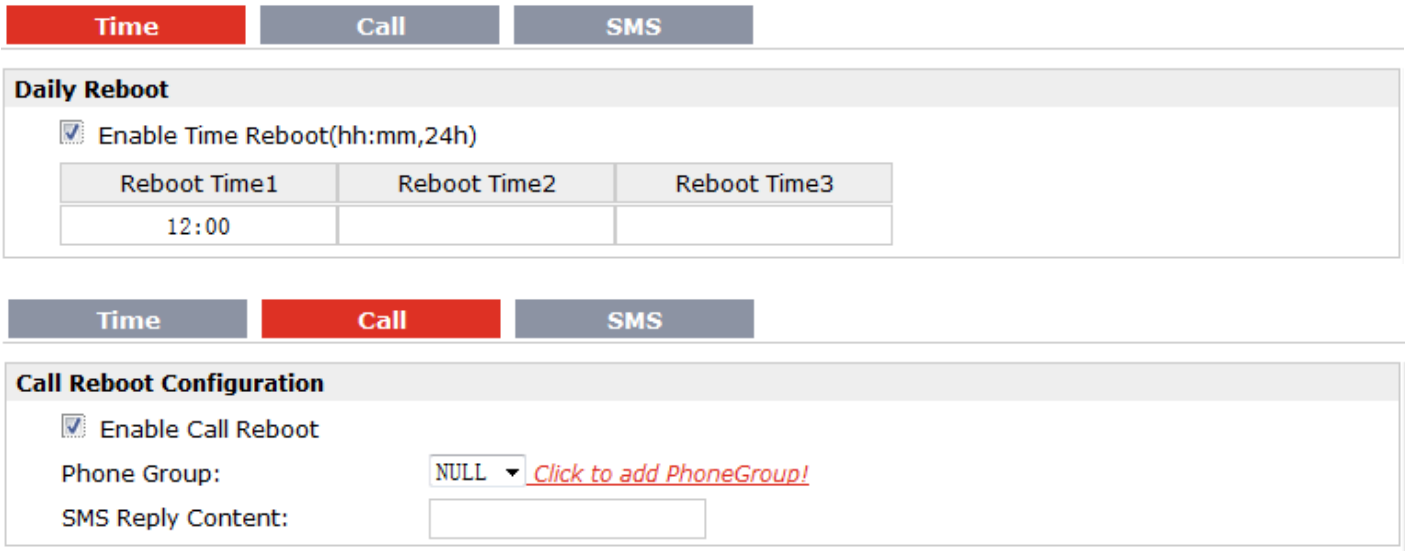
SMS		
Item	Description	Default
Send SMS on power up	Enable to send SMS to a specified phone group after the router is powered up.	Disabled
Send SMS on PPP connect	Enable to send SMS to a specified phone group after PPP is up.	Disabled
Send SMS on PPP disconnect	Enable to send SMS to a specified phone group after PPP is down.	Disabled
Phone Group	Select the Phone Group who wish to receive the SMS(s).	Null
Enable @ SMS Control	Click to enable SMS remote control feature.	Disabled
Password Content	Set the password content for SMS control. **Note**: Only supports text format. For example 123 or ABC123.	Null
Phone Group	Select the Phone Group who can use SMS control feature.	Null

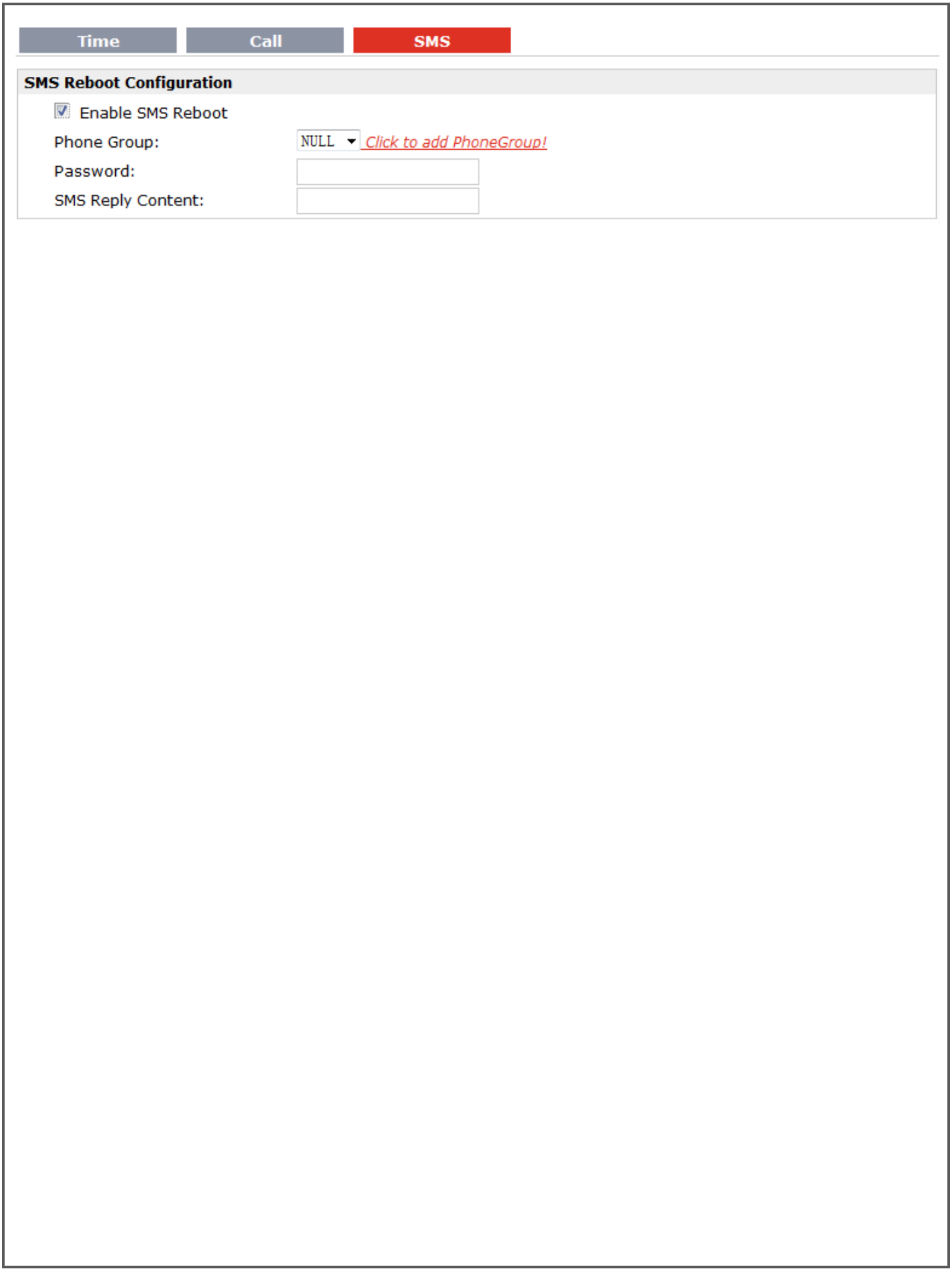


3.31 Configuration -> Reboot

This section allows users to set up the reboot policies for the router.

Reboot - Time		
Item	Description	Default
Enable(ahh:mm,24h)	Enable daily reboot. Up to three time points can be configured. The time has to be inhh:mm, 24h time format.	Disabled
Reboot Time1	Specify time1 when the router will reboot.	Null
Reboot Time2	Specify time2 when the router will reboot.	Null
Reboot Time3	Specify time3 when the router will reboot.	Null
Reboot - Call		
Enable Call Reboot	Click to enable call reboot function **Note**: This feature is not supported by 3G or 4G model.	Disabled
Phone Group	Set the Phone Group which is allowed to reboot the router by call.	Null
SMS Reply Content	Set up the reply SMS after reboot by call is performed, e.g. Reboot ok! **Note**: Only support text format SMS.	Null
Reboot - SMS		
Enable SMS Reboot	Click to enable SMS reboot function	Disabled
Phone Group	Set the Phone Group that is allowed to reboot the router by SMS.	Null
Password	Password for triggering the reboot.	Null
SMS Reply Content	Set up the reply SMS after reboot by SMS is performed, e.g. Reboot ok! **Note**: Only support text format SMS.	Null

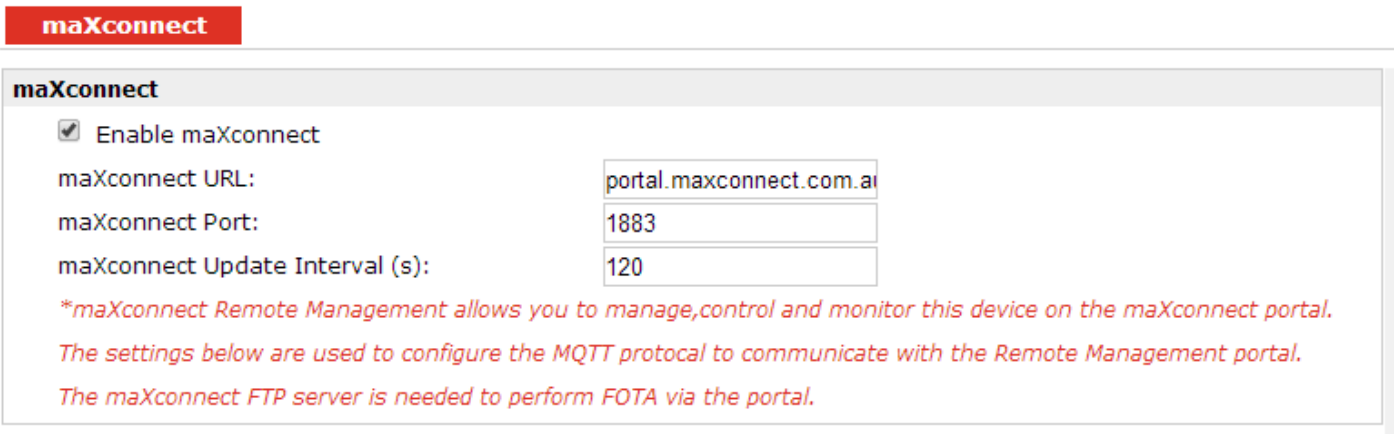



Time
Call
SMS
SMS Reboot Configuration
Enable SMS Reboot
Phone Group:
NULL
Click to add PhoneGroup!
Password:
SMS Reply Content:

3.32 Configuration -> maXconnect

This section allows users to configure parameters for maXconnect. MaXconnect is Maxon's modem management portal, a cloud based M2M management portal which allows you to access, monitor and control 3G/4G Maxon devices securely. With maXconnect you can access real-time data from your devices, monitor their status and location. Utilise complete functionality by controlling your devices anywhere, anytime. This one stop portal is an access point to manage your 3G/4G assets securely and remotely.

maXconnect		
Item	Description	Default
Enable maXconnect	Click to enable maXconnect feature.	Disabled
Server address	Enter the IP address or URL of the maXconnect Server for the device status update. When an Internet connection is used, please enter: portal.maxconnect.com.au. When using maXwan, please use IP: 10.0.0.1	Null
Port	Enter port number for maXconnect service.	1883
maXconnect Update Interval (s)	The status update interval in seconds	120

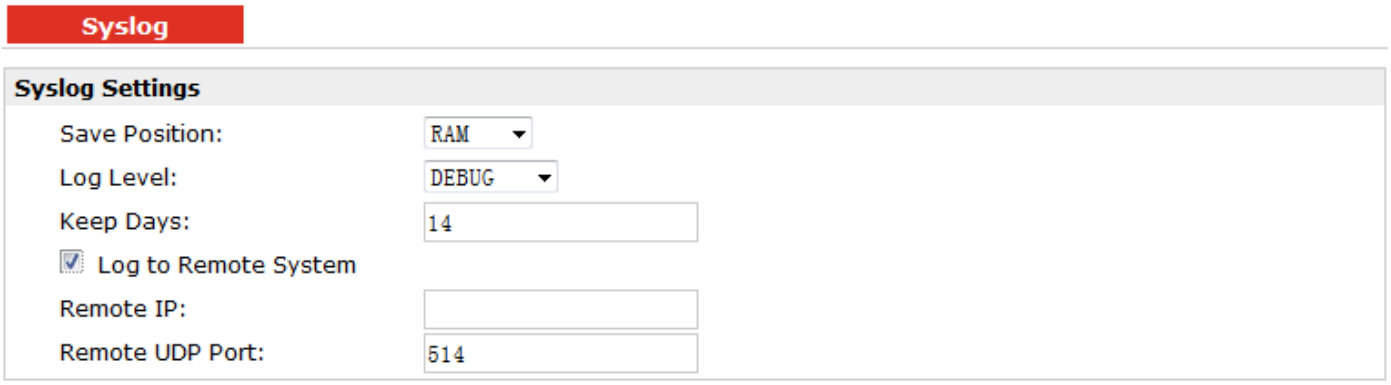


Note: FTP server access will be available in future.

3.33 Configuration -> Syslog

This section allows users to set up the parameters for Syslog function. Syslog is a standard for computer message logging which allow system and debug information of a device to be saved to a storage media device or sent to a remote syslog server.

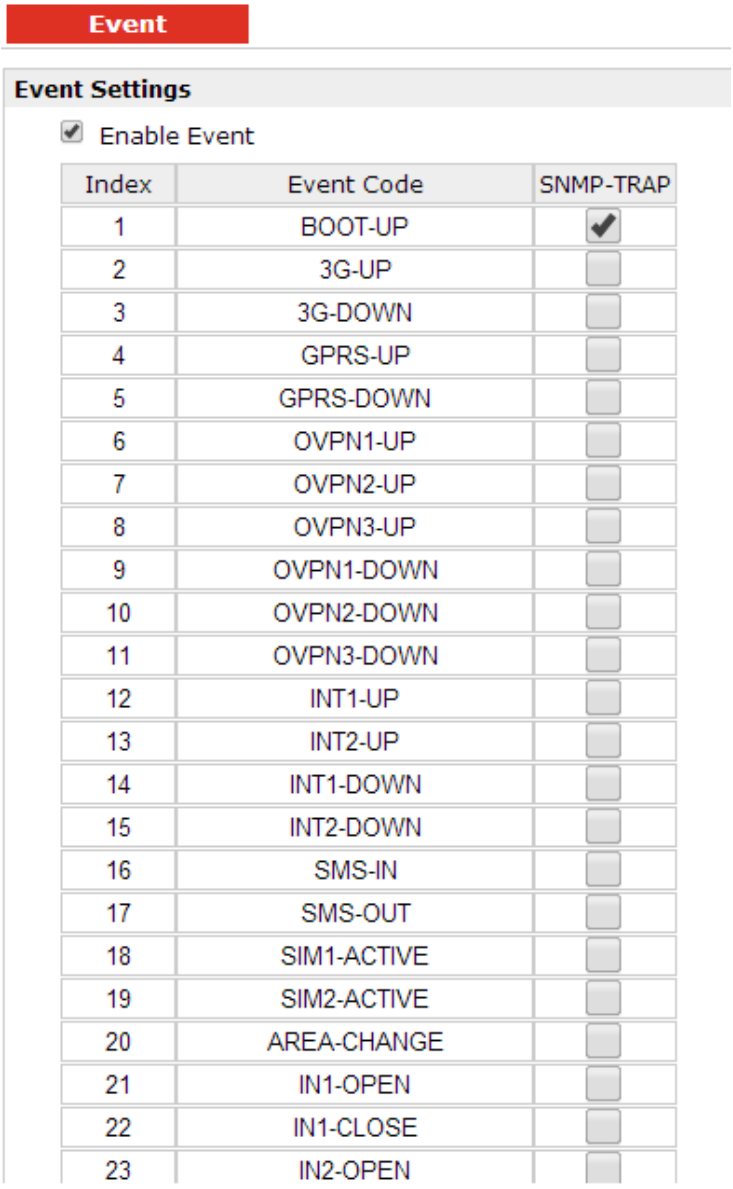
Syslog		
Item	Description	Default
Save Position	Select the save position from “None”, “Flash” and “SD”. “None” means syslog is only saved in RAM, and will be cleared after reboot.	NONE
Log Level	Select form “DEBUG”, “INFO”, “NOTICE”, “WARNING”, “ERR”, “CRIT”, “ALERT” and “EMERG” which from low to high. The lower level will output more syslog in detail.	DEBUG
Keep Days	Specify the syslog “keep Days” for router to clear the old syslog.	14
Log to Remote System	Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	Disabled



3.34 Configuration -> Event

This section allows users to select the events that will be reported via SNMP-Trap.

Event		
Item	Description	Default
Enable Event	Click to enable Event feature. This feature is used to report Multimax's major running events to SNMP-TRAP. There are numbers of Event code that can be selected, such as "BOOT-UP", "3G-UP", "3G-DOWN", etc.	Disabled



3.35 Configuration -> USR LED

This section allows users to configure how the USR LED is used for display.

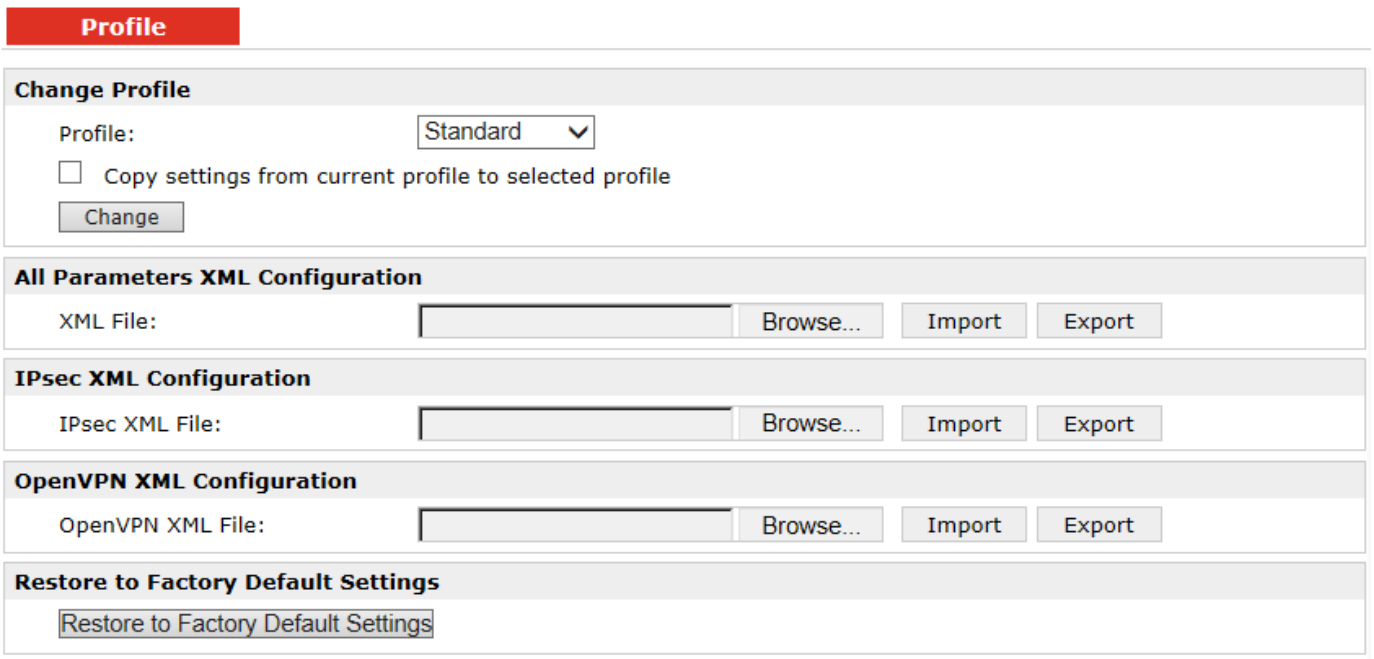
Note: Please refer to “Status” -> “System” -> “LEDs Information” -> “USR”.

USR LED		
Item	Description	Default
USR LED Type	Select from “VPN”, “PPPoE”, and “DynDNS”	VPN
Indication	Select from “ON”, “Blink”. For example, if “USR LED Type” is set as “VPN” and “Indication” is set as “Blink”, when any VPN tunnel is up USR LED will blink.	ON

3.36 Administration -> Profile

This section allows users to set up profiles, import or export the device configuration, and restore the factory default settings.

Profile		
Item	Description	Default
Profile	This item allows users to save different configuration profiles into different positions for easier change over later; or to save one configuration profile into different positions just for configuration backup. Selected from "Standard", "Alternative 1", "Alternative 2", "Alternative 3".	Standard
XML Configuration	Import: Click "Browse" to select a saved device configuration file (XML file) and then click "Import" to load the file into the router. Export: Click "Export" and the device configuration will be shown in a new browser window, you can then save it as a XML file. The configuration of IPSec and OpenVPN can be loaded and saved separately if needed.	Null
Restore to Factory Default Settings	Click the "Restore to Factory Default Settings" button to load factory default settings to the router. A reboot is required for the settings to take effect.	Null

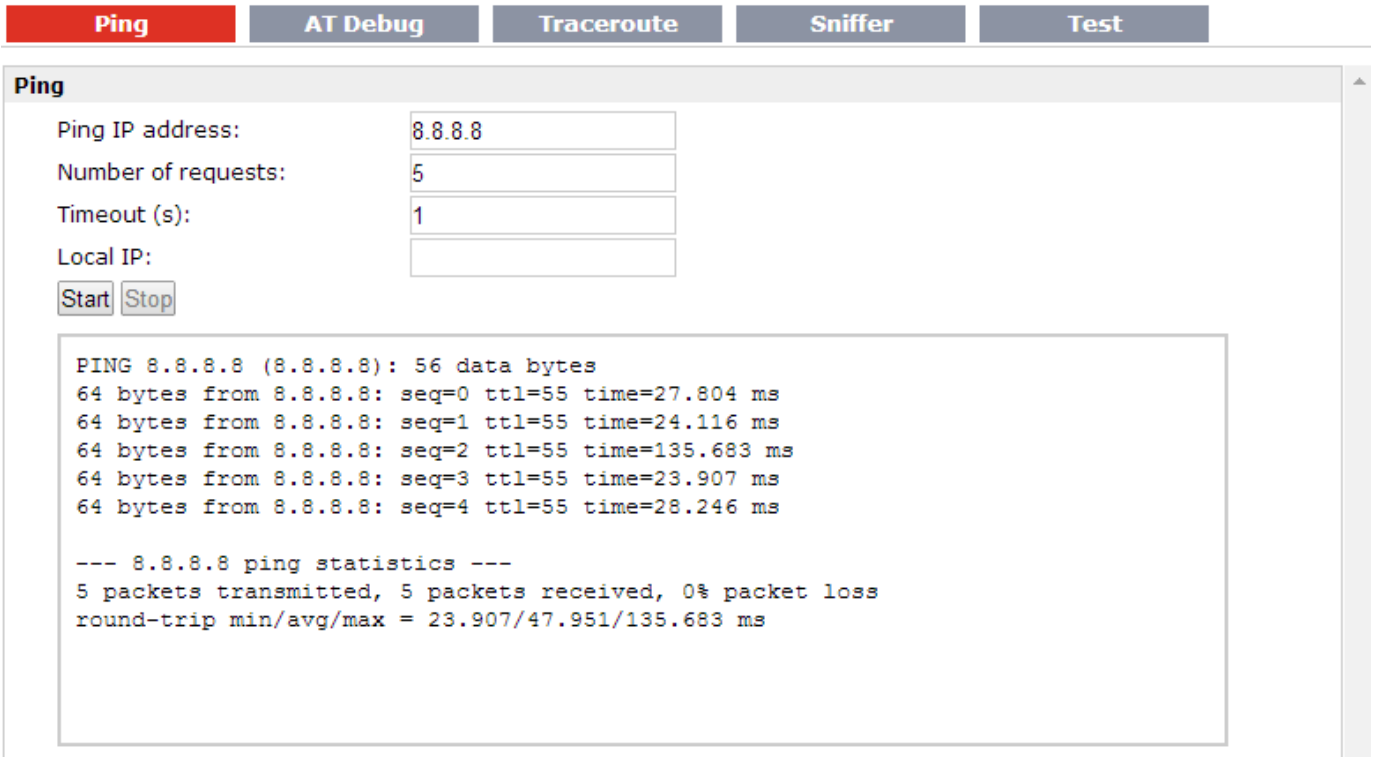


3.37 Administration -> Tools

Five useful tools are provided for users to do some debugging: Ping, AT Debug, Traceroute, Sniffer, and Test.

Ping

Tool - Ping		
Item	Description	Default
Ping IP address	Enter the ping destination IP address or domain name.	Null
Number of requests	Specify the number of requests.	5
Timeout	Specify timeout of ping request.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting the local IP address from these three automatically.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	Null

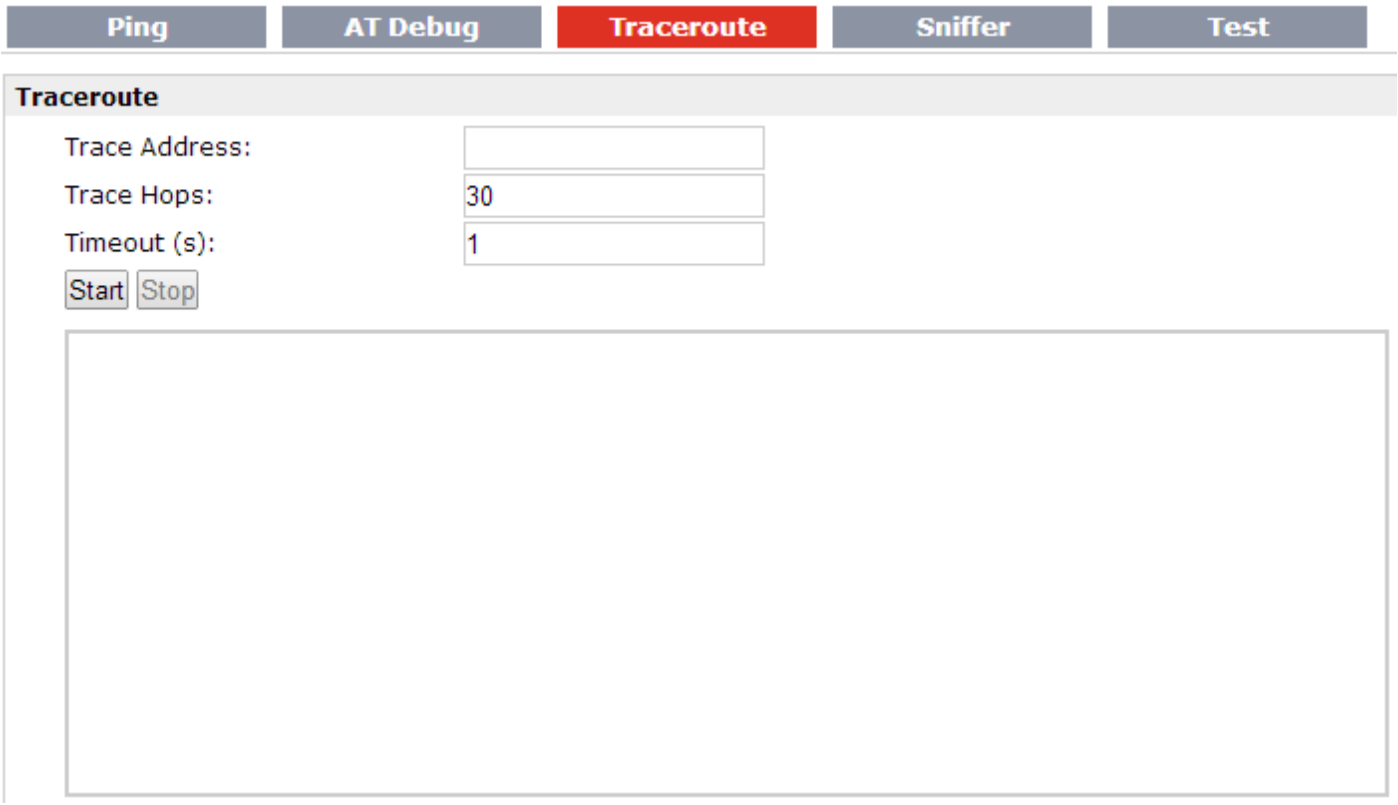


AT Debug

Tool - AT Debug		
Item	Description	Default
Send AT Commands	Enter the AT commands which will be sent to the cellular module in this box.	Null
Send	Click this button to send the AT commands.	Null
Receive AT Commands	The router will display the response from the cellular module in this box.	Null

Traceroute

Tool - Traceroute		
Item	Description	Default
Trace Address	Enter the destination IP address or domain name for the trace route command.	Null
Trace Hops	Specify the maximum trace hops. Router will stop tracing if the trace hops has reached the value regardless of whether the destination has been reached or not.	30
Timeout	Specify the timeout (in minutes) of Trace route request.	1
Send	Click this button to launch the Trace route request, and the log will be displayed in the box below.	Null



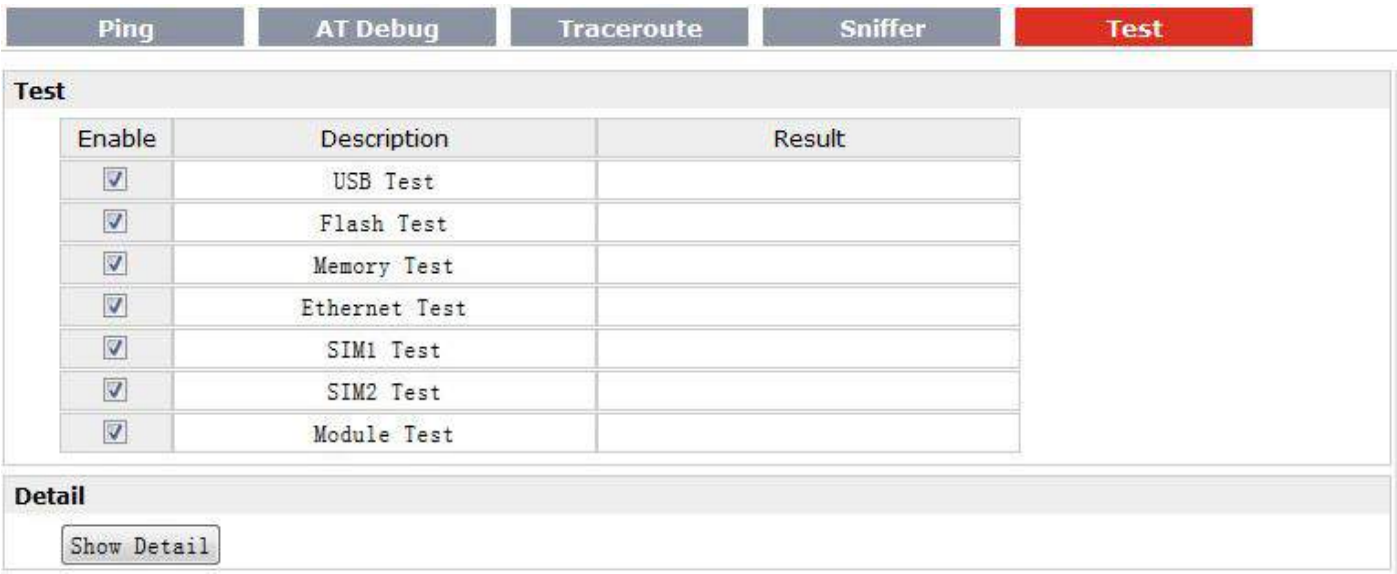
Sniffer

Tools - Sniffer		
Item	Description	Default
Interface	Select form “all”, “lo”, “imq0”, “imq1”, “eth0”, “gre0”, and “ppp0”: all: All the interfaces; lo: Local Loopback interface; imq0/1: virtual interface for QoS, which used to limit the download and upload speed; eth0: Ethernet interface; gre0: GRE tunnel interface; ppp0: Cellular PPP interface;	All
Host	Filter the packets that contain the specify IP address.	Null
Protocol	Select from “all”, “ip”, “arp”, “tcp” and “udp”.	All
Start	Click this button to start the sniffer, and the log will be displayed in the follow box.	Null

Test

Test @ Tools		
Item	Description	Default
Enable	Click “Enable” to select the hardware component to check.	Enable
Description	Show the list of components that can be tested: “SD Test”, “USB Test”, “Flash Test”, “Memory Test”, “Ethernet Test”, “SIM1 Test”, “SIM2 Test”, and “Module Test”.	N/A
Result	Show the current status of the selected hardware component. There are 3 status “Testing”, “Success” and “Failure”. Testing: the router is testing the selected hardware component. Success: Correspond hardware component is properly inserted and detected. Failure: Correspond hardware component is not inserted into the router or the router fails to detect.	Null
Show Detail	Show the latest test details of the hardware component.	Null

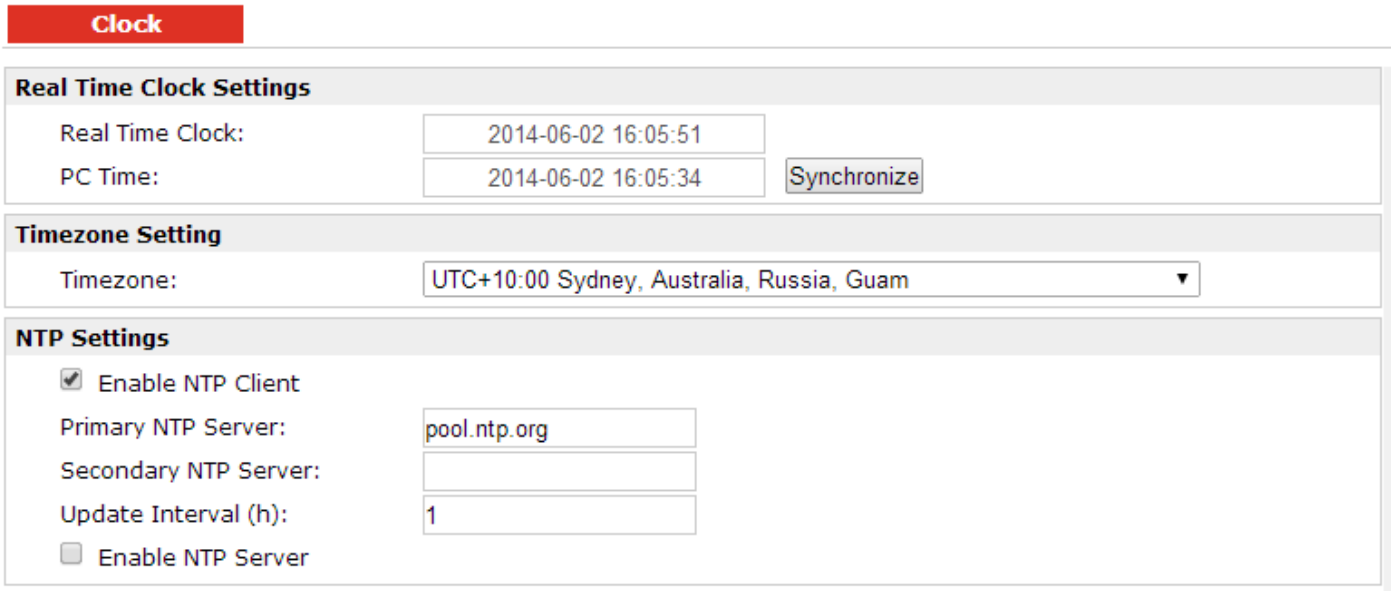
Note: Please click “Apply” to start testing.



3.38 Administration -> Clock

This section allows users to set up the Real Time Clock (RTC) of the router and NTP Service.

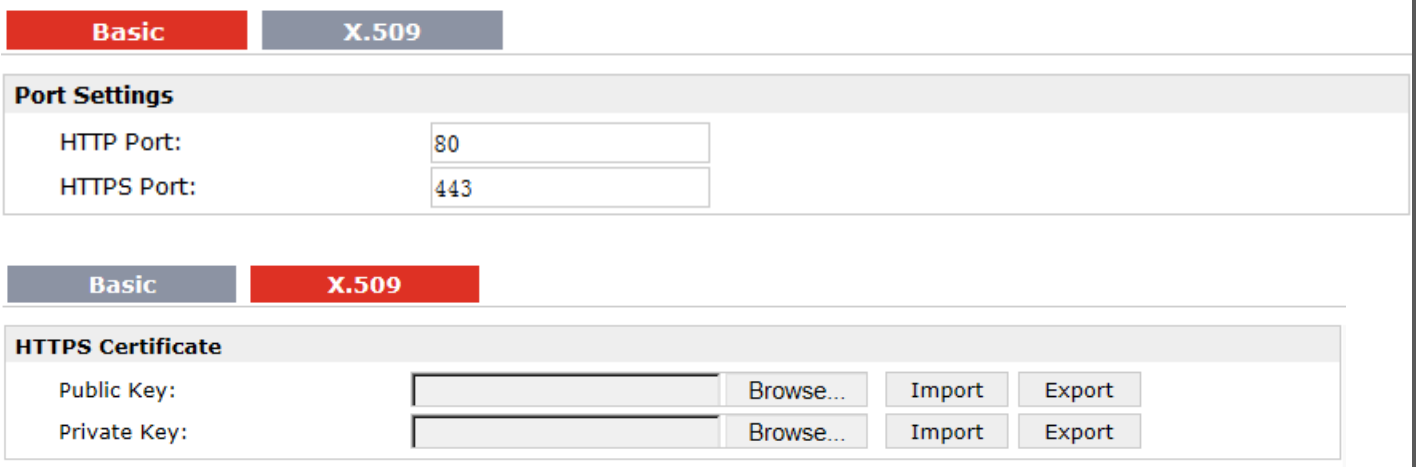
Clock		
Item	Description	Default
Real Time Clock	Router's RTC is shown and can be modified in this field.	Null
PC Time	The time of the PC that connects to the router is shown here.	Null
Synchronize	Synchronize the router's RTC with PC time.	Null
Enable NTP Client	Click to enable NTP client, which synchronizes the time from an NTP server.	Disabled
Timezone @ Client	Select your local time zone.	UTC +10:00
Primary NTP Server	Enter the primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter the secondary NTP Server's IP address or domain name.	Null
Update interval (h)	Enter the interval (in hours) which the NTP client will synchronize the time from NTP server.	1
Enable NTP Server	Click to enable the NTP server service in the router.	Disabled



3.39 Administration -> Web Server

This section allows users to modify the parameters of Web Server.

Web Server - Basic		
Item	Description	Default
HTTP Port	Enter the HTTP port number to be used in Multimax's Web Server. By default, port 80 is the port that the Web server "listens to" or expects to receive from a Web client using HTTP. If you wish to configure the router with another HTTP Port number other than the port 80, just enter the port number in the field.	80
HTTPS Port	Enter the HTTPS port number to be used in Multimax's Web Server. By default, port 443 is the port that the Web server "listens to" or expects to receive from a Web client using HTTPS. If you wish to configure the router with another HTTPS Port number other than the port 443, just enter the port number in the field. **Note**: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTPS was deployed to allow authorization and secured transactions.	443
Web Server – X.509		
HTTPS Certificate	In this tab, user can import or export "Public Key" and "Private Key" for HTTPS certificate.	Null



3.40 Administration -> User Management

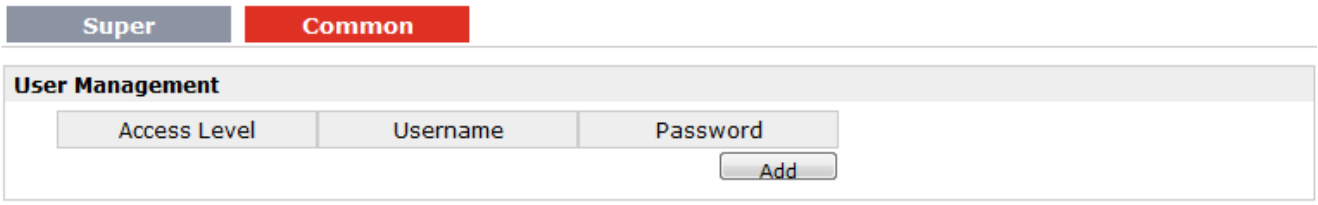
This section allows users to add and modify user accounts.

Super User

User Management - Super		
Item	Description	Default
Super	Each router has only one super user account. With this account the user has the highest authority of managing all user accounts.	Admin
User Management	Set Username and Password.	Null
Login Timeout	Specify the login timeout (in seconds). User needs to re-login after the inactive time exceeds the setting.	1800

Common

User Management - Common		
Item	Description	Default
Common	Each router can have up to 9 common user accounts. There are two access levels for the common user account: “ReadWrite” and “ReadOnly”.	Null
Access Level	Select from “ReadWrite” and “ReadOnly”. ReadWrite: Users can view and change the configuration of the router; ReadOnly: Users only can view the configuration of the router.	Null
Username/ Password	Set Username and Password.	Null
Add	Click this button to add a new account.	N/A

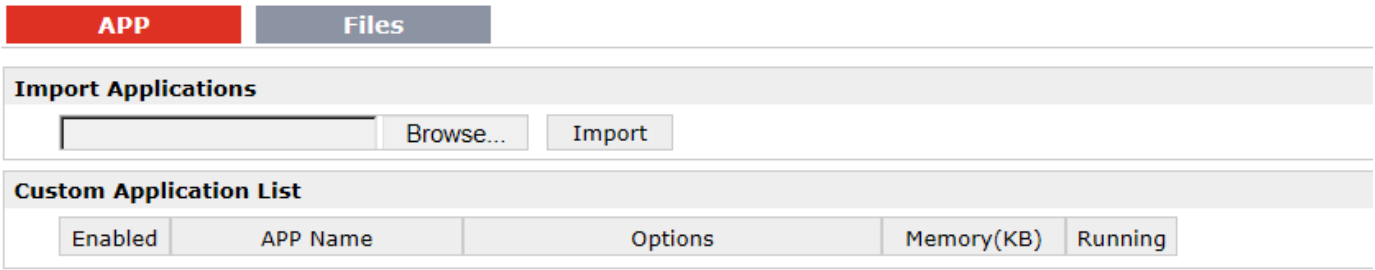


3.41 Administration -> SDK Management

This section allows users to set up SDK Management parameters for the router.

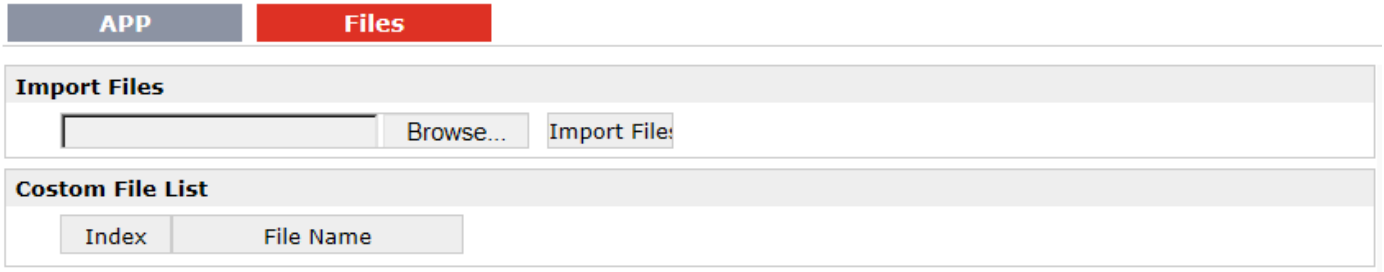
Applications

SDK Management -APP		
Item	Description	Default
Firmware Version	Show the current firmware version.	Null
Import Files	Click to import application files.	Null
Custom Application List	The list shows which application files have been imported to the router, which application files that need to be run, as well as the running information. Enable: Click to enable the application. APP Name: Shows the name of the application. Options: Optional setting, in which users can configure the startup parameters. Memory (KB): Shows the memory resources allocated for the applications. Running: Shows whether the applications are running.	Null



Configuration Files

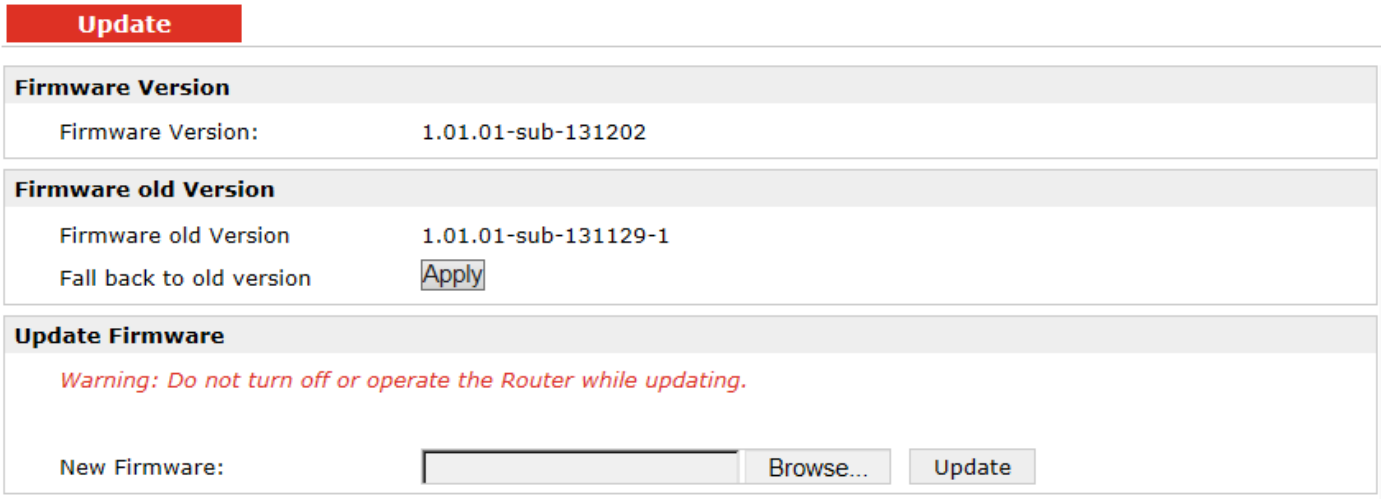
SDK Management - Files		
Item	Description	Default
Import Files	Click to import configuration files.	Null
Custom File List	This list shows which Configuration files that have been imported to the router.	Null



3.42 Administration -> Update Firmware

This section allows users to update the firmware of the router locally or remotely. The Multimax supports FOTA (Firmware Over The Air).

Update Firmware		
Item	Description	Default
Firmware Version	Show the current firmware version.	Null
Firmware Old Version	Show the previous firmware version if there is one. Click the "Apply" button to will tell the router to roll back to a previous firmware. A Reboot will be required for this operation. This feature is very useful if something goes wrong after a firmware upgrade.	Null
Update firmware	Click the "Select File" button to select the correct firmware in your PC, and then click the "Update" button" to upload. After uploading successfully, the router will reboot for the new firmware to take effect.	Null



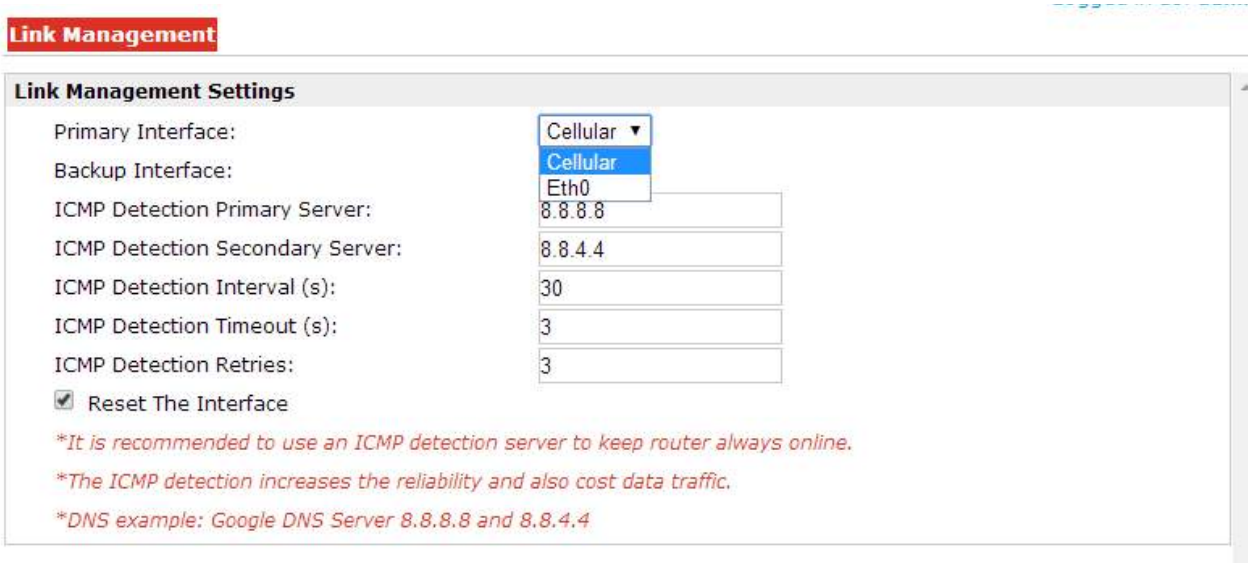
Chapter 4. Examples of configuration

4.1 Cellular Dial-Up

This section describes how to configure the Cellular Dial-up parameters. Two different policies “Always Online” and “Connect on Demand” are explained.

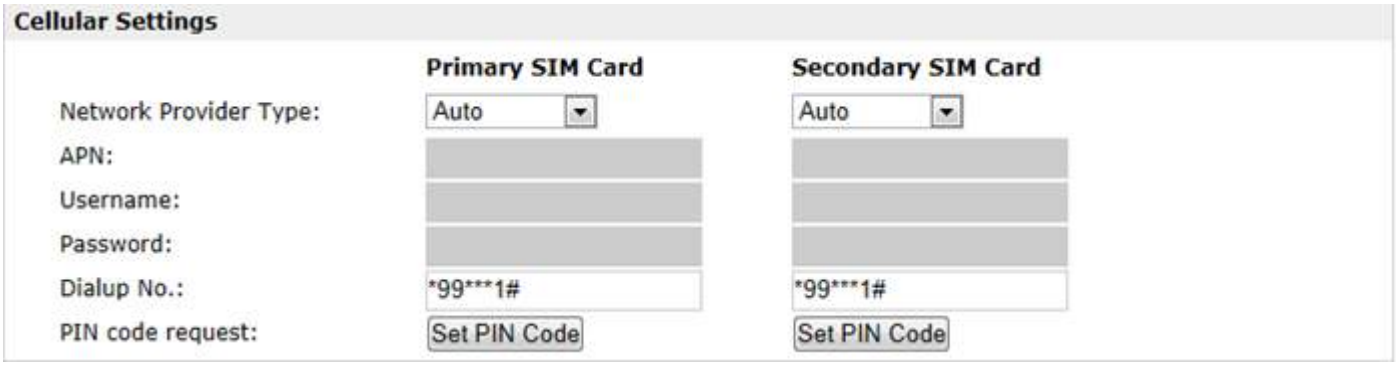
4.1.1 Always Online:

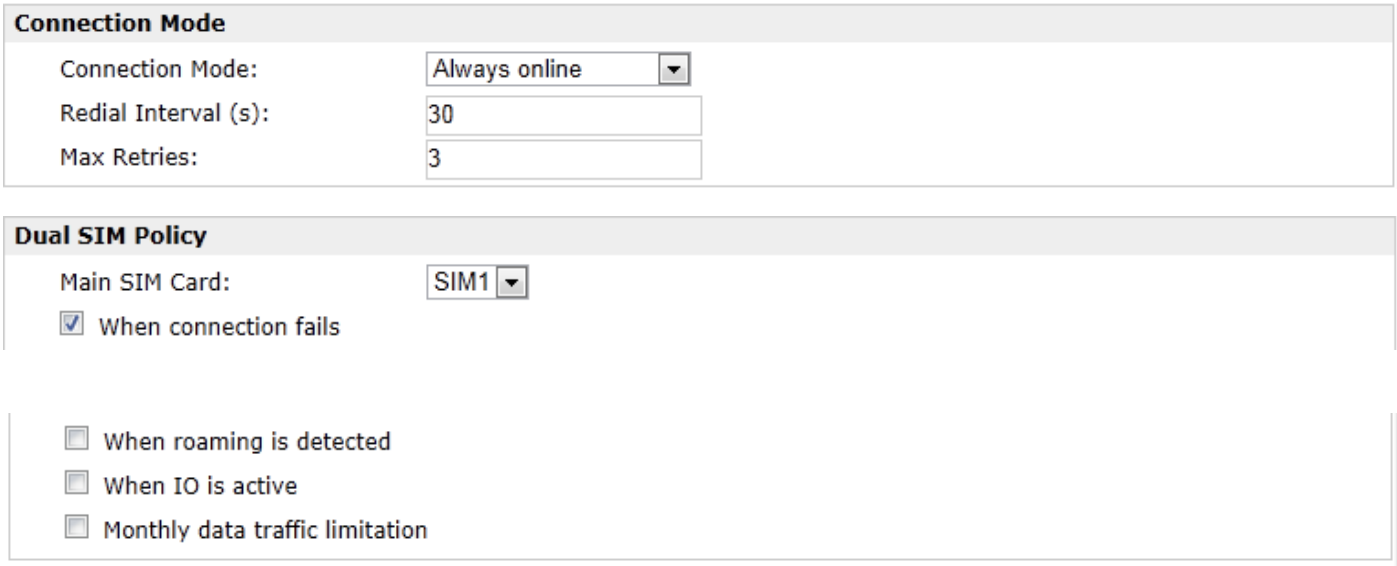
Configuration-->Link Management-->Cellular Only



The change will take effect after clicking the “Apply” button.

Configuration-->Cellular WAN -->Basic



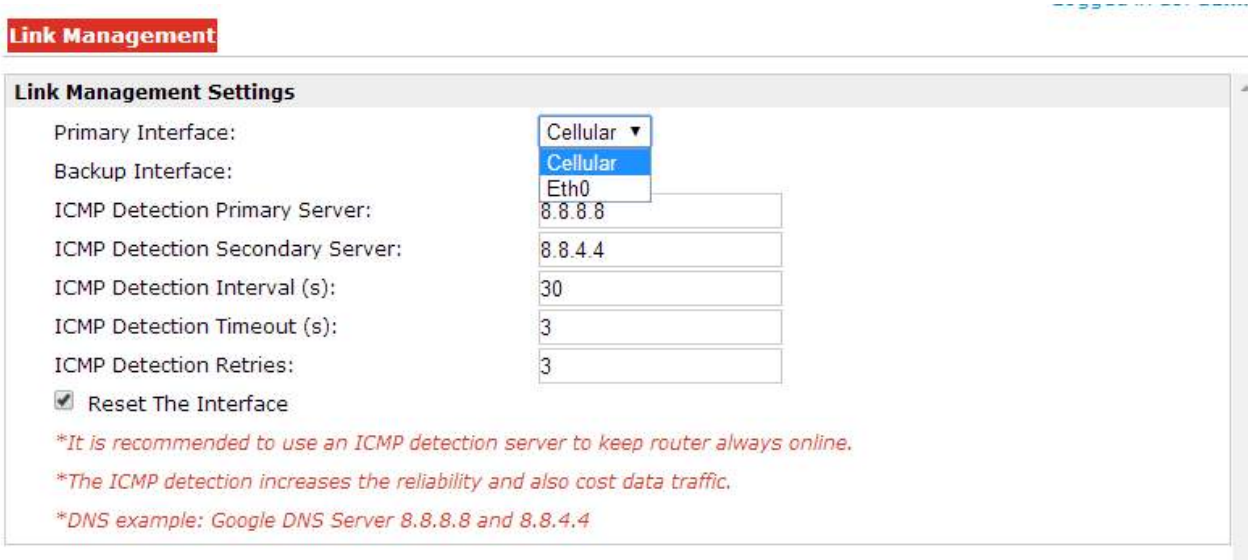


The change will take effect after clicking the “Apply” button.
If a customized SIM card is used, please select “Custom” instead of “Auto” in “Network Provider Type”, and “APN”, “username”, and “password” will need to be configured accordingly.

Note: Cellular WAN settings page will not be shown if users select “Eth0 Only” in “Configuration -> Link Management”.

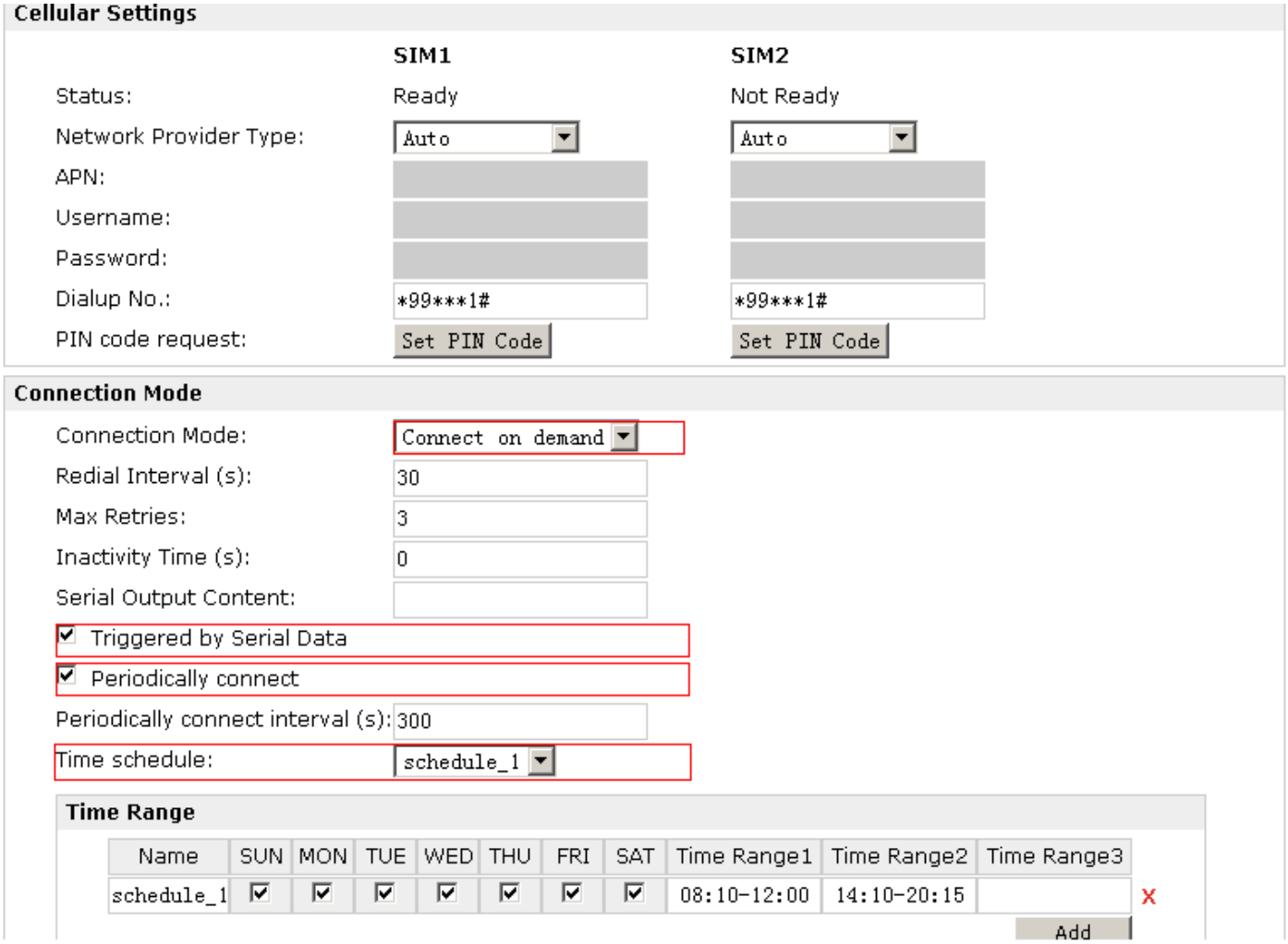
4.1.2 Connect on Demand:

Configuration-->Link Management-->Cellular Only



Changes will take effect after clicking the “Apply” button.

Configuration-->Cellular WAN -->Basic



Select the trigger policy required.

Note: If multiple trigger policies are selected, the PPP will be triggered with any of them matched.

4.1.3 SMS Remote Status Reading

The Multimax supports remote status reading via SMS using the commands in the table below to get the status of the router.

SMS command syntax:

Password: cmd1,a,b,c;cmd2,d,e,f;cmd3,g,h,i;...;cmdn,j,k,n

SMS command Explanation:

1. Password: The SMS command password is configurable via **Basic->SMS Control->Password**, and it is optional.

a) When there is no password, the SMS command has the following structure:
cmd1;cmd2;cmd3;…;cmdn

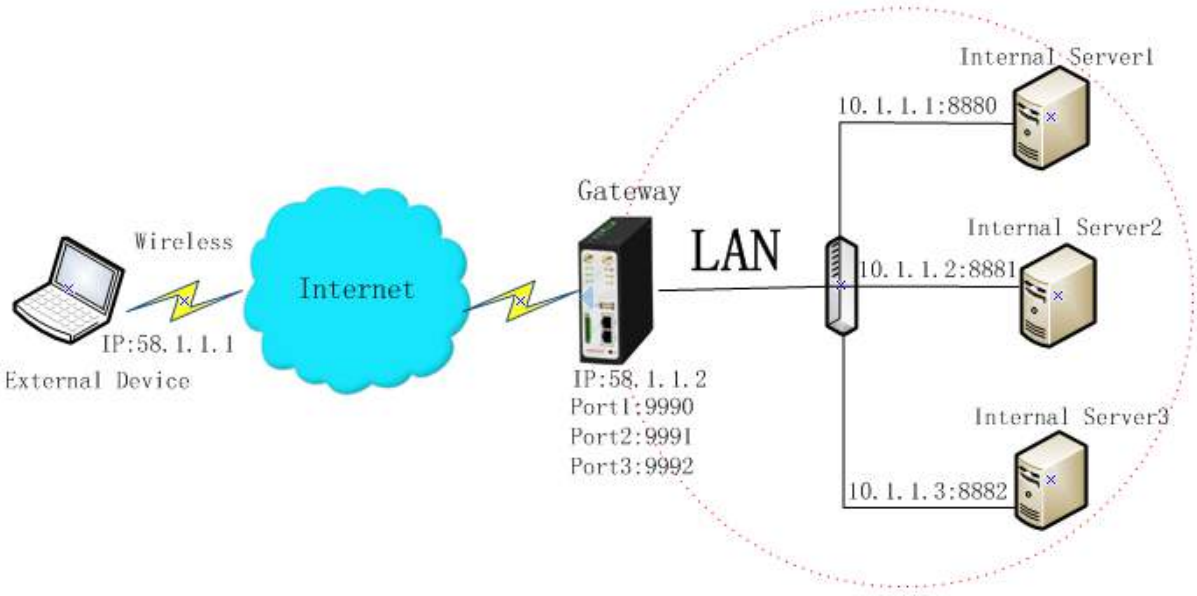
b) When there is a password, SMS command has the following structure:
Password:cmd1;cmd2;cmd3;…;cmdn

2. cmd1, cmd2, cmd3 to Cmdn, command identification numbers 0001 – 0010.
3. a, b, c to n, are command parameters.
4. The semicolon character (';') is used to separate more than one command packed in a single SMS.
5. E.g., 1234:0001, in this command, password is 1234, 0001 is the command to reset the Multimax.

Cmd	Description	Syntax	Comments
SMS Commands			
0001	Reset Device	cmd	
0002	Save Parameters	cmd	
0003	Save Parameters and Reset Device	cmd	
0004	Start PPP Dialup	cmd	
0005	Stop PPP	cmd	
0006	Switch Sim Card	cmd	
0007	Enable/Disable Event Counter	cmd,channel,flag	channel: 1 - DI_1 2 - DI_2 flag: 0 - disable 1 - enable
0008	Get Event Count Value	cmd,channel	channel: 1 - DI_1 2 - DI_2
0009	Clear Event Count	cmd,channel	channel: 1 - DI_1 2 - DI_2
0010	Clear SIM Card's Data Limitation	cmd,simNumber	simNumber: 1 - SIM_1 2 - SIM_2

4.2 NAT (Port Forwarding)

This section explains how to set up the NAT configuration of the router.
Remote IP defines if access from the IP is allowed to route to the forwarded IP and associated Port via the WAN IP with the associated port.



Configuration--->NAT/DMZ--->Port Forwarding

Port Forwarding

Remote IP	Arrives At Port	Is Forwarded to IP Address	Is Forwarded to Port	Protocol	
58.1.1.1	9990	10.1.1.1	8880	TCP	X
58.1.1.1	9991	10.1.1.2	8881	UDP	X
58.1.1.1	9992	10.1.1.3	8882	TCP&UDP	X

*Remote IP: 1.1.1.1, 1.1.1.0/24,1.1.1.1-2.2.2.2, 0.0.0.0 means any

Add

*Arrives At Port: <1-65536> or <1-65536>-<1-65536>

Note: This section will be hidden if the user selects "Cellular as primary and if fail use Eth0" in "Configuration ->Link Management".

Explanations for above diagram:
If there are two IP addresses 58.1.1.1 and 59.1.1.1 for the External Devices, then the result will be different from the test when the NAT is working at the router.
58.1.1.1----------access to--------->58.1.1.2:9990----------be forwarded to------->10.1.1.1:8000 TCP
58.1.1.1----------access to--------->58.1.1.2:9991----------be forwarded to------->10.1.1.2:8001 UDP
58.1.1.1----------access to--------->58.1.1.2:9992----------be forwarded to------->10.1.1.3:8002 TCP&UDP

4.3 L2TP

Note:

In the following diagrams the red coloured numbers mean that these should be matched between server and client, and those with the blue coloured numbers mean that they must be set up locally for the tunnel.

L2TP_SERVER:

Configuration--->L2TP--->L2TP Server

Enable L2TP Server

☐ Enable L2TP Server

Tick "Enable L2TP Server", and enter the proper settings:

L2TP Common Settings

Username:	l2tp	1
Password:	••••	2
Authentication:	PAP	3
☐ Enable Tunnel Authentication		
Local IP:	10.1.2.1	
IP Pool Start:	10.1.2.2	
IP Pool End:	10.1.2.254	

L2TP Server Advanced

☐ Show L2TP Server Advanced

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask	
0.0.0.0	192.168.1.0	255.255.255.0	X

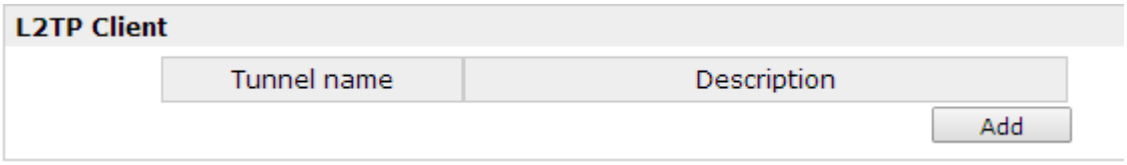
"0.0.0.0" means any

Add

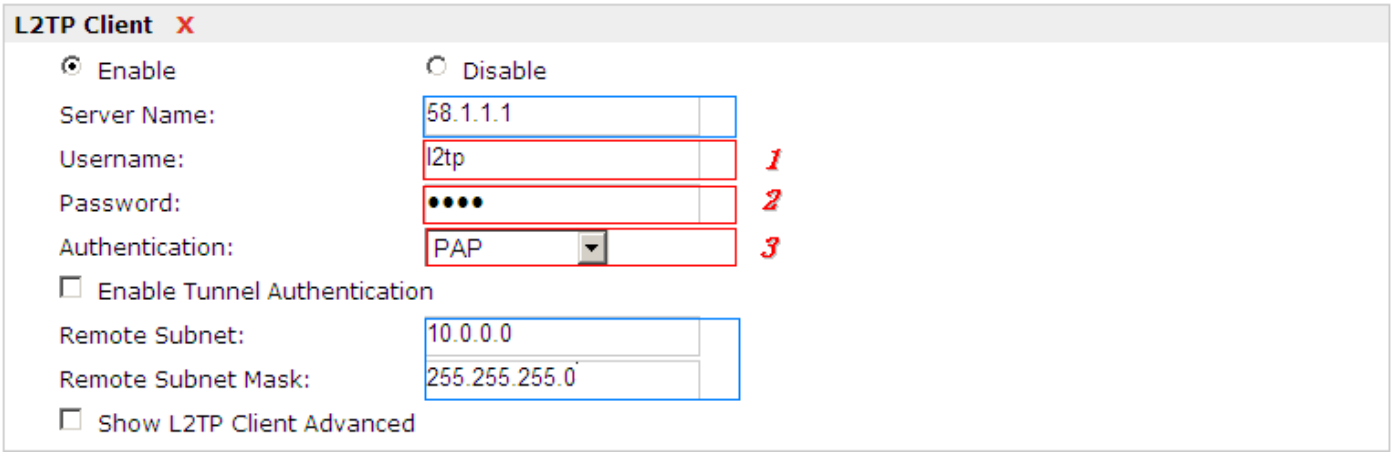
The changes will take effect after doing “Apply-->Save-->Reboot”.

L2TP_CLIENT:

Configuration--->L2TP--->L2TP Client



Click “Add” button, and enter the proper settings:



The changes will take effect after doing “Apply-->Save-->Reboot”.

4.4 PPTP

Note:

In the following diagrams, the red coloured numbers mean that these should be matched between server and client, and those with the blue coloured numbers mean that they must be set up locally for the tunnel.

PPTP_SERVER:

Configuration--->PPTP--->PPTP Server

Enable PPTP Server

☐ Enable PPTP Server

Tick "Enable PPTP Server", and enter the proper settings:

PPTP Common Settings

Username:	pptp	1
Password:	••••	2
Authentication:	PAP	3
Local IP:	10.0.0.1	
IP Pool Start:	10.0.0.2	
IP Pool End:	10.0.0.254	

☐ Enable MPPE

PPTP Server Advanced

☐ Show PPTP Server Advanced

Route Table List

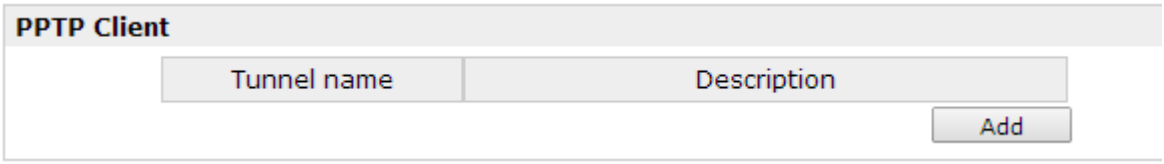
Client IP	Remote Subnet	Remote Subnet Mask	
0.0.0.0	192.168.1.0	255.255.255.0	X

"0.0.0.0" means any Add

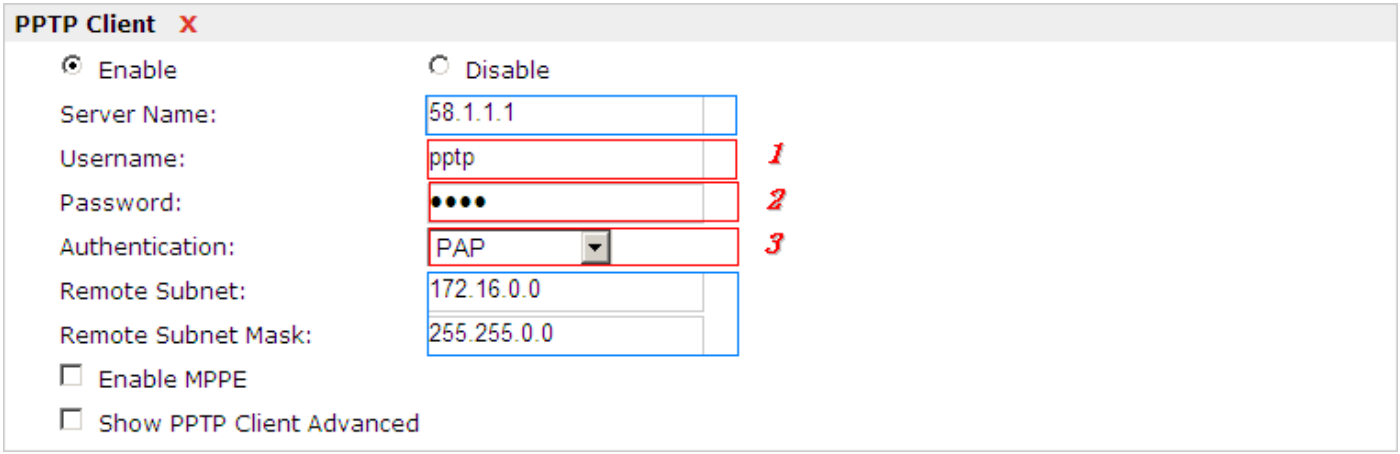
The changes will take effect after doing "Apply-->Save-->Reboot".

PPTP_CLIENT:

Configuration--->PPTP--->PPTP Client



Click “Add” button, and enter the proper settings:



The changes will take effect after doing “Apply-->Save-->Reboot”.

4.5 IPSEC VPN

Note:

In the following diagrams the red coloured numbers mean that these should be matched between server and client, and those with the blue coloured numbers mean that they must be set up locally for the tunnel.

IPsecVPN_SERVER:

Cisco 2811:

```
crypto isakmp policy 10
 encr aes 256                                   8
 hash md5                                       9
 authentication pre-share                       11
 group 2                                        10
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
                 12
!
crypto ipsec transform-set trans esp-3des esp-md5-hmac   2, 13
!
crypto dynamic-map dyn 10
  set transform-set trans
  match address 101
!
crypto map map1 10 ipsec-isakmp dynamic dyn
!
interface FastEthernet0/0
  crypto map map1
!
access-list 101 permit ip 10.0.0.0 0.0.0.255 any   3, 5
!
```

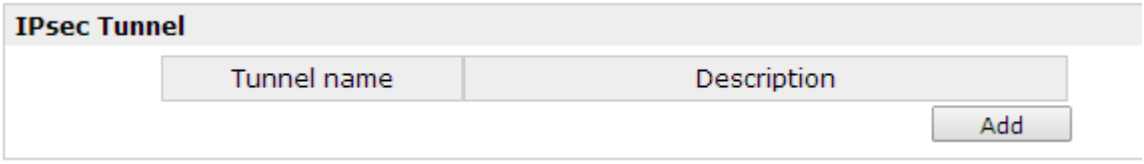
Note: Polices 1,4,6,7 are default for Cisco router and are shown here.

IPsecVPN_CLIENT:

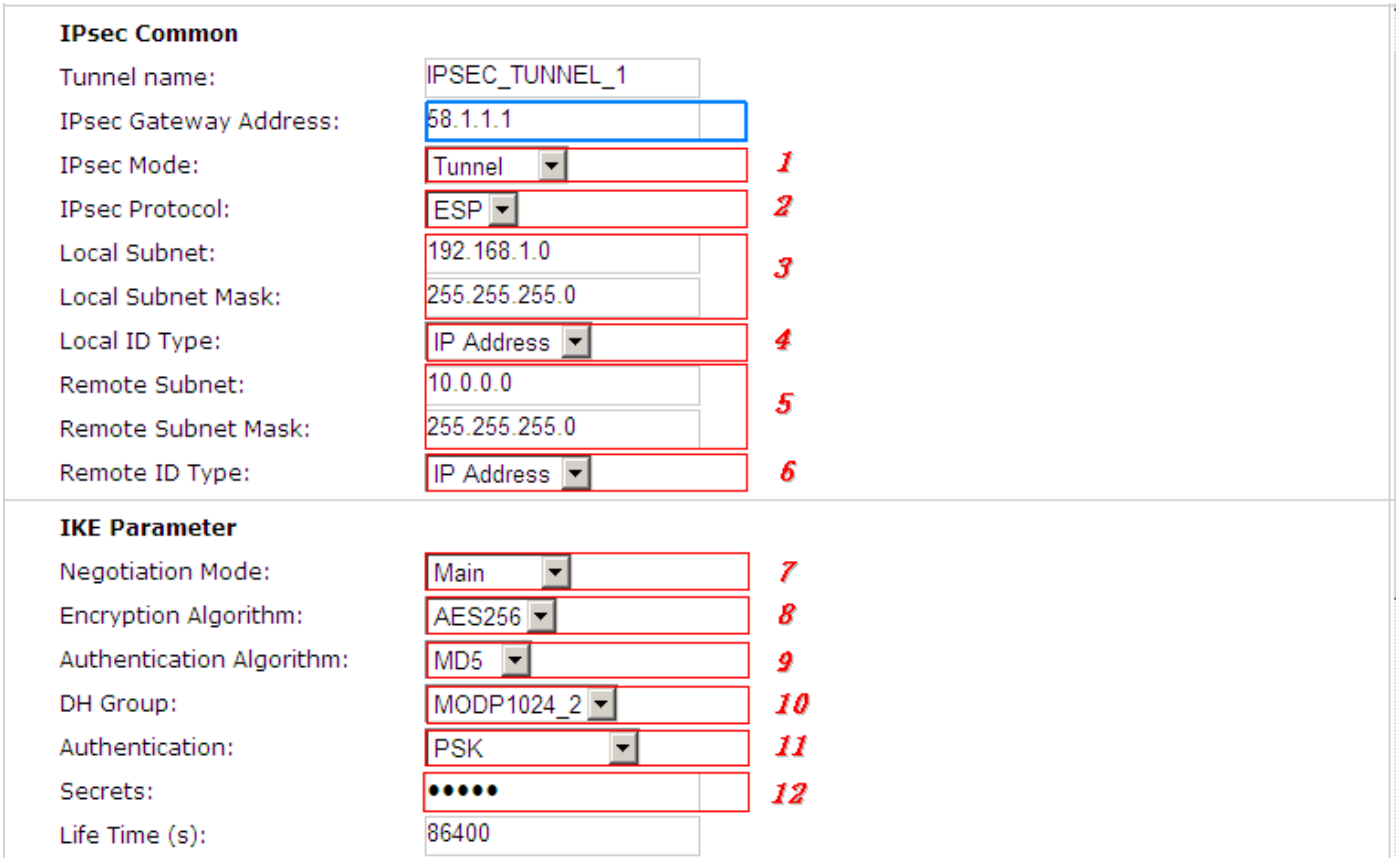
Configuration--->IPsec--->IPsec Basic

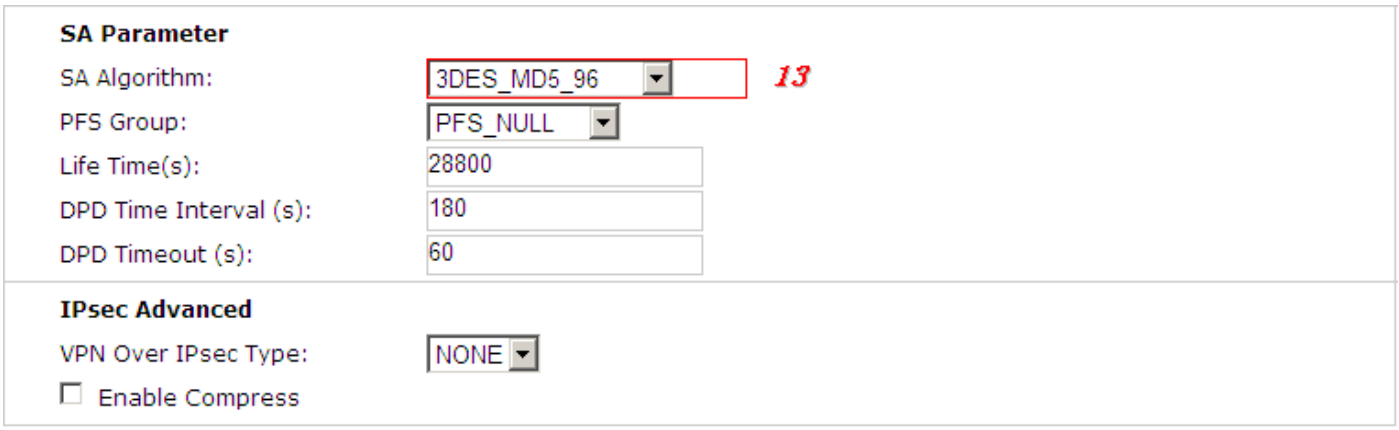
Then click “Apply”.

Configuration--->IPsec--->IPsec Tunnel



Click “Add” button, and enter the proper settings:





The changes will take effect after doing “Apply-->Save-->Reboot”.

4.6 OPENVPN

Note:
In the following diagrams the red coloured numbers mean that these should be matched between server and client, and those with the blue coloured numbers mean that they must be set up locally for the tunnel.

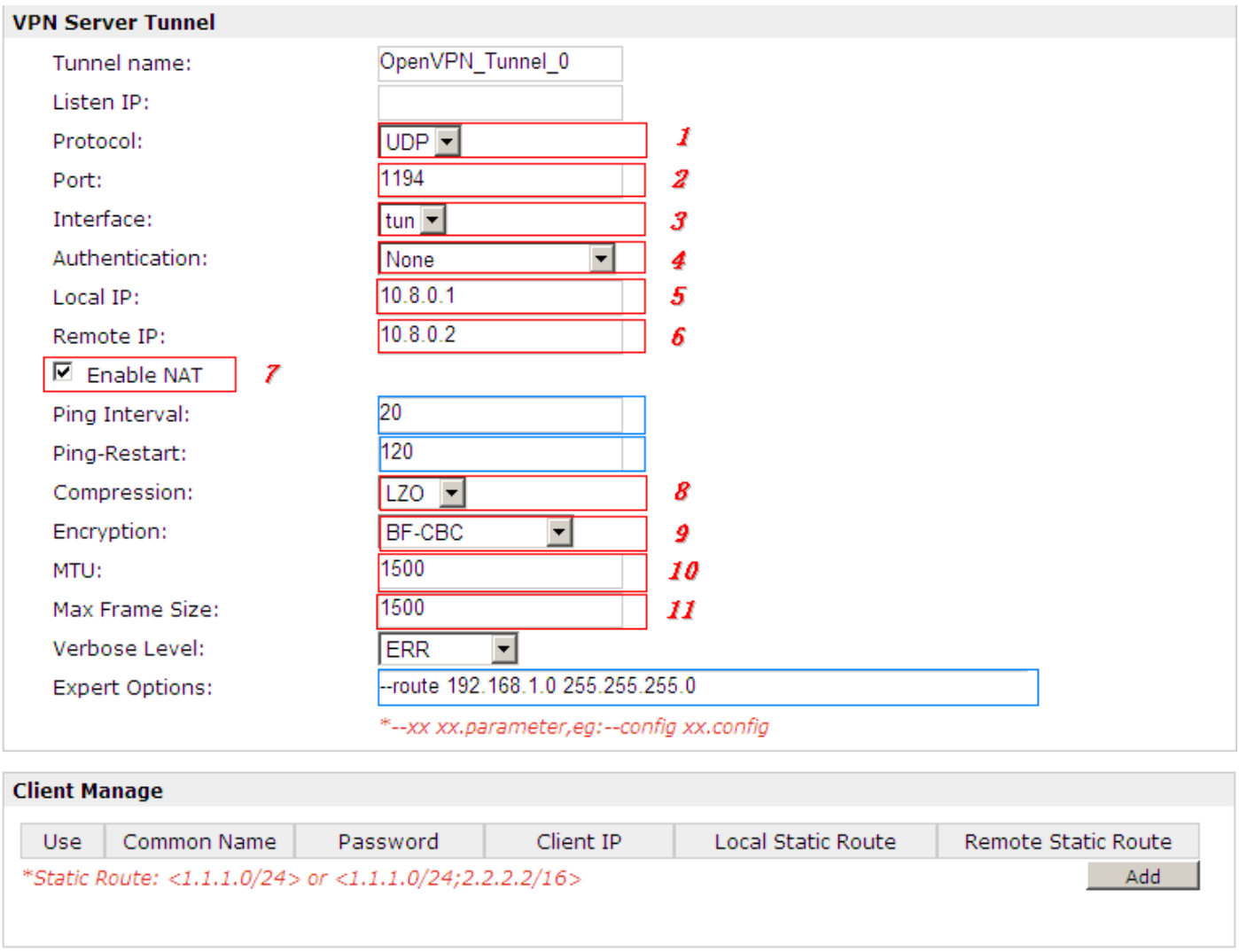
OPENVPN_SERVER:

Configuration--->OpenVPN--->Server

Enable OpenVPN Server

☐ Enable OpenVPN Server

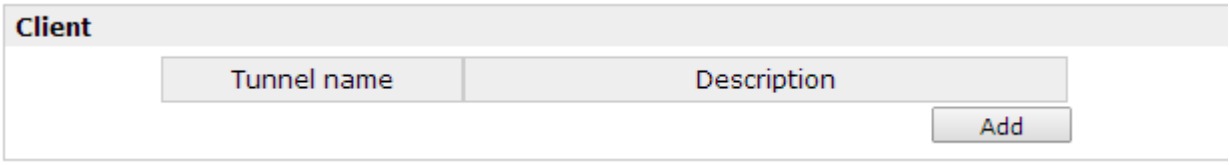
Tick “Enable OpenVPN Server”, and enter the proper settings:



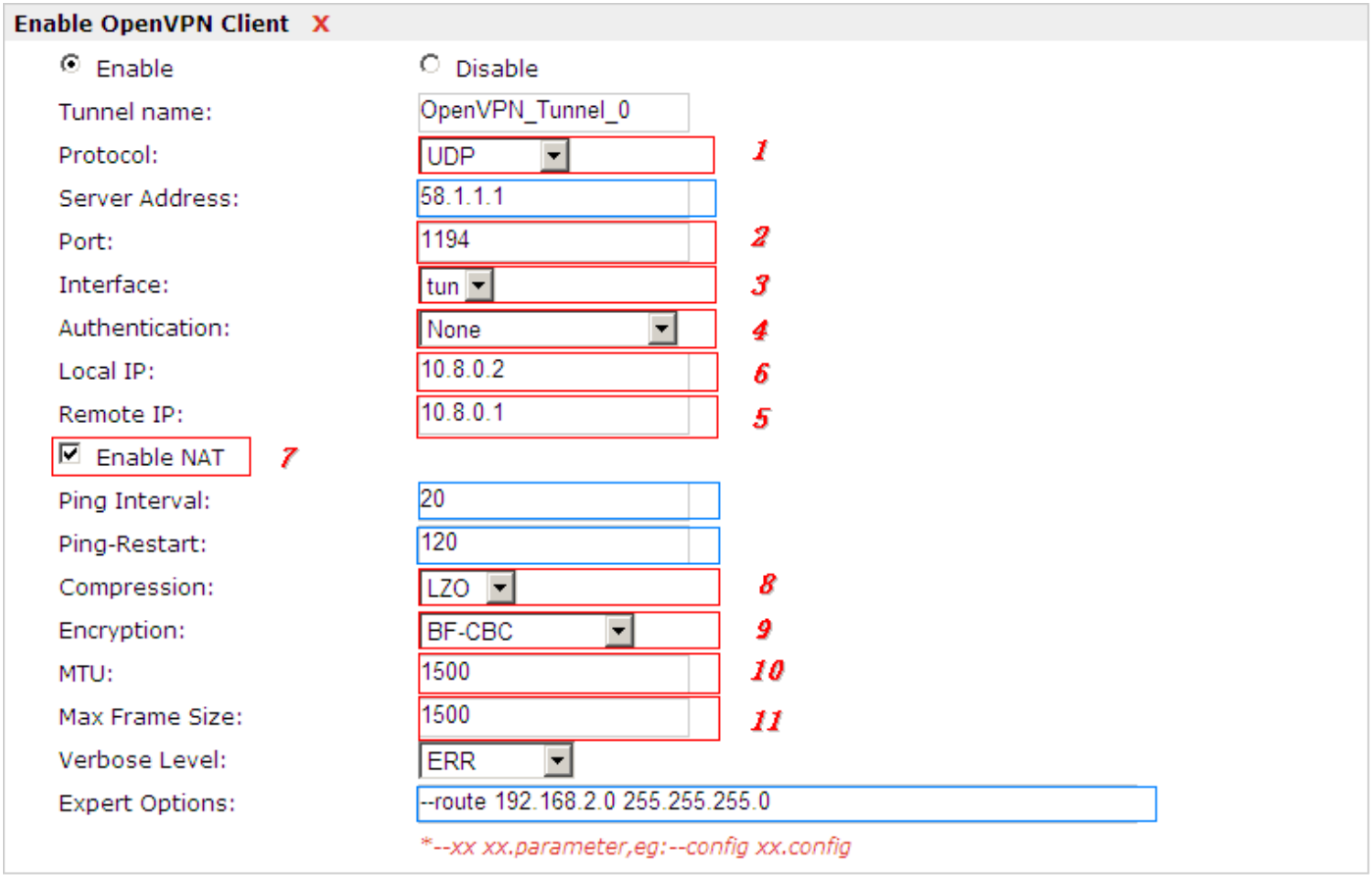
The changes will take effect after doing “Apply-->Save-->Reboot”.

OPENVPN_CLIENT:

Configuration--->OpenVPN--->Client



Click “Add” button, and enter the proper settings:



The modification will take effect after doing “Apply-->Save-->Reboot”.

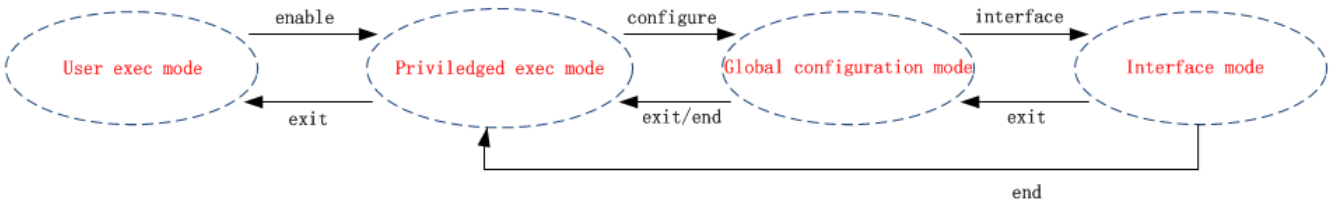
Chapter 5. Introductions for CLI

5.1 What is the CLI and hierarchy level Mode?

The MA-2040 Command-Line Interface (CLI) is a software interface providing another way to set up the device configurations from the serial console port or through a telnet connection. To use the CLI properly, it is necessary to understand the four different CLI hierarchy level modes, which have different access privileges:

- **User exec mode**—the command prompt ">" shows that you are in the user exec mode. Under this mode, users can only use some simple commands to view the current configuration and the device status, or to use the "Ping" command to check the network connectivity.
- **Privileged exec mode**—when entering the privileged exec mode, the command prompt will change to "#",under which users can use all those allowed in the user exec mode plus the addition commands, such as importing and exporting files, system logs, and debug, etc.
- **Global configuration mode**—the global configuration mode is with command prompt "<config>#", which allows users to view and change the current device configurations.
- **Interface mode**— the global configuration mode is with command prompt "<config-xx>", where "xx" indicates the particular interface. Under this mode, users are to set IP address and MTU for this interface.

The following chart shows how to access or quit among these modes:



USER EXEC MODE:

MA-2040 Configure Environment

Username: admin

Password: *****

MA-2040 > ? Use "?" to check available commands in **user exec mode**

Enable	Turn on privileged commands
Exit	Exit from current mode
Ping	Ping test
Reload	Halt and perform a cold restart
Tracert	Traceroute test
Show	Show running system information

PRIVILEDGED EXEC MODE:

MA-2040> enable

Password: *****

MA-2040# ?Use “?” to check available commands in **priviledged exec mode**

Debug	Debug configure information
Exit	Exit from current mode
Export	Export file using tftp
Syslog	Export system log
import	Import file using tftp
load	Load configure information
ping	Ping test
reload	Halt and perform a cold restart
tracert	Traceroute test
write	Write running configuration
tftp	Copy from tftp: file system
show	Show running system information
configure	Enter configuration mode
end	Exit to normal mode

GLOBAL CONFIGURATION MODE:

MA-2040# configure

MA-2040 (config)# ? Use “?” to check available commands **global configuration mode**

exit	Exit from current mode
end	Exit to normal mode
interface	Configure an interface
set	Set system parameters
add	Add system parameters list
modify	Modify system parameters list
delete	Delete system parameters list

INTERFACE MODE:

MA-2040(config)# interface Ethernet 0

MA-2040(config-e0)# ? Use "?" to check available commands in **interface mode**

exit	Exit from current mode
end	Exit to normal mode
ip	Set the IP address of an interface
mtu	Set the mtu of an interface

5.2 How to configure the CLI

The following is a list of the help and errors that can be encountered in the configuring program.

Commands /tips	Description
?	Typing a question mark "?" whenever needed for displaying the help information.
Ctrl+c	Pressing the both keys at the same time to perform a "copy" function, or to exit from a running program.
Invalid command "xxx"	An invalid or unsupported command. Please use "?" to find out the correct command and its usage.
Incomplete command	One for more parameters are expected for the command entered. Please use "?" to find out the proper usage of the command.
% Invalid input detected at '^' marker	The '^' marker indicates the location where is incorrect within the command entered.

Note*:* Most of the configurations are able to be set in the Global configuration mode. **Set** and **Add** commands are very important under this mode. If any parameters cannot be found in the Global configuration mode, please use **Privileged exec mode** or **Interface mode**.

Important: Understanding the **CLI modes hierarchy level** is essential before doing configuration using the CLI. If you are not familiar with it, please read **Section 5.1** first!

5.2.1 Configuration Examples by using CLI

The best and quickest way to make the best use of CLI is to know all the device features from the web interface in advance, then to get familiar with the CLI commands and learn to use them by looking at some examples.

Example 1 : Show current version

```
MA-2040> show version
    software version :      1.01.00
    kernel version    :     v2.6.39
    hardware version :      1.01.00
```

Example 2 : Update firmware via tftp

```
MA-2040> enable
    Password:               *****
    MA-2040#
    MA-2040# tftp 172.16.3.3 get rootfsMultimax_V1.01.11

tftptransferring
tftp succeeded downloaded


MA-2040# write                              //save current configuration
Building configuration...
OK

MA-2040# reload
!Reboot the system ?'yes'or 'no':yes        //reboot the device for the new firmware to take effect
```

Example 3: Set link-management

```
MA-2040> enable
    Password:           *****
    MA-2040#
    MA-2040#            configure
    MA-2040(config)# set link-management
    wan link :
                        1.Cellular Only
                        2.Eth0 Only
                        3.Eth0 as primary and if fail use Cellular
                        4.Cellular as primary and if fail user Eth0
                            ->please select mode(1-4)[1]:2          //select “Eth0 Only” as wan-link
                            ->ICMP detection primary server[]:8.8.8.8
                            ->ICMP detection second server[]:8.8.8.4
                            ->ICMP detection interval(3-1800)[30]:
                            ->ICMP detection timeout(1-10)[3]:
```

```
                    ->ICMP detection retries(1-20)[3]:
                    ->reset the interface?'yes'or'no'[no]:

This parameter will take effect after reboot!
Really want to modify[yes]:
MA-2040# write                          //save current configuration
Building configuration...
OK
MA-2040# reload
!Reboot the system ?'yes'or 'no':yes//reboot the device for the new configuration to take
effect
```

Example 4: Set IP address, Gateway and DNS for Eth0

```
MA-2040> enable
        Password:       *****
        MA-2040#
        MA-2040# show link-management                   //show the current link-management

*****************************************
wan link                : Eth0 Only                     //"Eth0 Only" as the current wan-link
  ICMP primary server   : 8.8.8.8
  ICMP second server    : 8.8.8.4
  ICMP detection interval   : 30 seconds
  ICMP detection timeout    : 3 seconds
  ICMP detection retries    : 3
reset the interface     : no
*****************************************

MA-2040# configure
MA-2040 (config)        # set eth0
Ethernet interface type:    WAN
Type select:
            1. Static IP
            2. DHCP
            3. PPP0E
                ->please select mode(1-3)[1]:
                ->IP address[192.168.0.1]:58.1.1.1              //set IP address for eth0
                ->netmask[255.255.255.0]:255.0.0.0
                ->gateway[192.168.0.254]:58.1.1.254             //set gateway for eth0
                ->mtu value(1024-1500)[1500]:
                ->input primary DNS[192.168.0.254]:58.1.1.254   //set dns for eth0
                ->input secondary DNS[0.0.0.0]:

This parameter will take effect after reboot!
```

really want to modify[yes]:

MA-2040(config)# end

MA-2040# write //save current configuration

Building configuration...

OK

MA-2040# reload

!Reboot the system ?'yes'or 'no':yes //reboot the device for the new configuration to take effect

Example 5: CLI for Cellular dialup

MA-2040> enable

Password: *****

MA-2040#

MA-2040# show link-management

****

wan link : Cellular Only //“Cellular Only” as the current wan-link

ICMP primary server : 8.8.8.8

ICMP second server : 8.8.8.4

ICMP detection interval : 30 seconds

ICMP detection timeout : 3 seconds

ICMP detection retries : 3

Reset the interface : no

****

MA-2040(config)# set cellular

1. set SIM_1 parameters

2. set SIM_2 parameters

->please select mode(1-2)[1]:

SIM 1 parameters:

Network provider

1. Auto

2. Custom

3. china-mobile

->please select mode(1-3)[1]:

->dial out using numbers[*99***1#]:

->pin code[]:

Connection Mode:

```
        1. Always online
        2. Connect on demand
                ->please select mode(1-2)[1]:
                ->redial interval(1-120)[30]:
                ->max connect try(1-60)[3]:
MA-2040(config)# end
        MA-2040#        write                                   //save current configuration
Building configuration...
OK

MA-2040# show cellular
************************************************
   Cellular enable              : yes
        1. show SIM_1 parameters
        2. show SIM_2 parameters
                ->please select mode(1-2)[1]:
SIM 1 parameters:
network provider                : Auto
dial numbers                    : *99***1#
pin code                        : NULL
connection Mode                 : Always online
redial interval                 : 30 seconds
max connect try                 : 3
main SIM select                 : SIM_1
when connect fail               : yes
when roaming is detected        : no
month date limitation           : no
SIM phone number                :
network select Type             : Auto
authentication type             : Auto
mtu value                       : 1500
mru value                       : 1500
asyncmap value                  : 0xffffffff
use peer DNS                    : yes
primary DNS                     : 0.0.0.0
secondary DNS                   : 0.0.0.0
address/control compression     : yes
protocol field compression      : yes
expert options                  : noccpnobsdcomp
************************************************

MA-2040# reload
!Reboot the system ?'yes'or 'no':yes        //reboot the device for the new configuration to take
effect
```

5.3 Commands reference

Commands	Syntax	Description
Debug	Debug *parameters*	Turn on or turn off debug function
Export	Export *parameters*	Export vpn CA certificates
Import	Import *parameters*	Import vpn CA certificates
Syslog	syslog	Export log information to tftp server
Load	Load default	Restores default values
Write	Write	Save current configuration parameters
tftp	tftp*IP-address* get {cfg|rootfs} *file-name*	Import configuration file or update firmware via tftp
Show	Show *parameters*	Show current configuration of each function, if need to see all the configurations, please use "show *running*"
Set	Set *parameters*	All the function parameters are set by commands set and add. The difference is that (set) is for the single parameter and (add) is for the list parameter
Add	Add *parameters*	