webdyn
flexitron group

MTX-Router-EOS

User Manual

www.webdyn.com

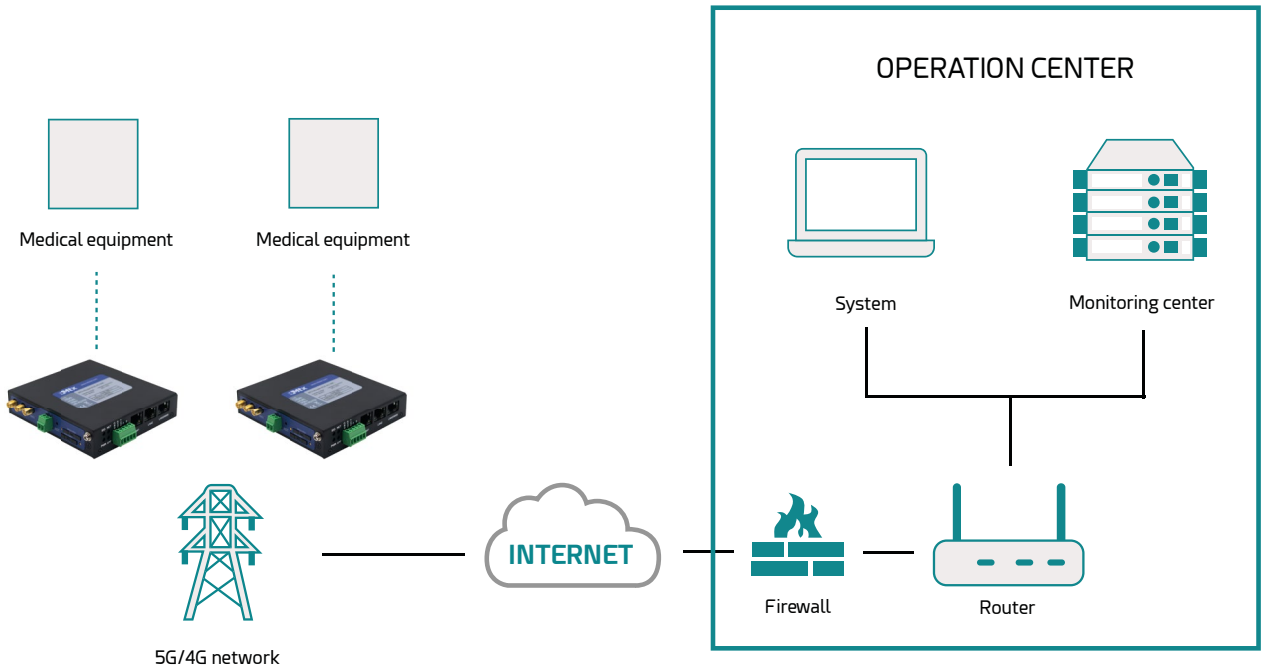
Index

Brief Introduction

1. General

MTX-Router-EOS is a kind of terminal device that developed based on 2G/3G/4G/5G, WiFi, VPN technology. It adopts high-powered industrial 32-bits CPU and embedded real time operating system. It supports RS232 and RS485, Ethernet and WiFi port that can conveniently and transparently connect one device to a cellular network, allowing to connect to your existing serial, Ethernet and WiFi devices with only basic configuration.

It has been widely used on M2M fields, such as intelligent transportation, smart grid, postal services,industrial automation, telemetry, finance, POS, water supply, environment protection, post, weather, and so on.

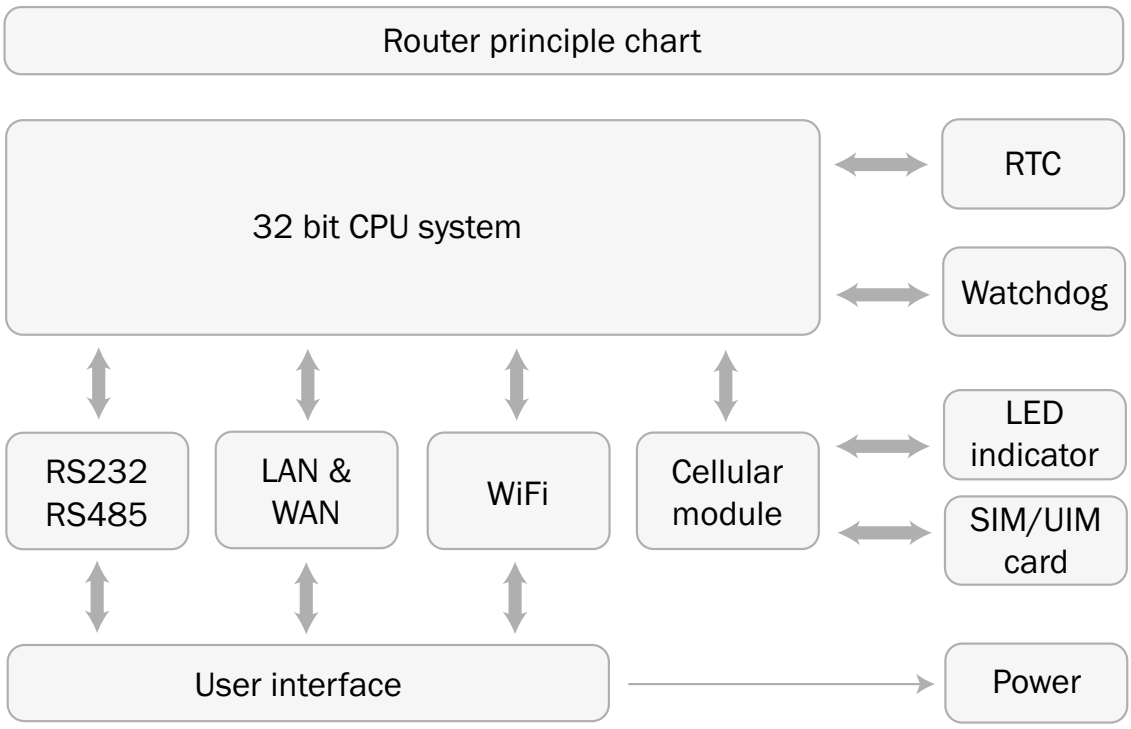


2. Product Feature

ITEMS	CONTENTS
Industrial design	High-powered industrial cellular module High-powered industrial 32bits CPU Housing: Iron, providing IP30 protection. Power range: DC 9~35V
High reliability	Support hardware and software WDT Support auto recovery mechanism to make router always online Ethernet port: 1.5KV magnetic isolation protection RS232/RS485 port: 15KV ESD protection SIM/UIM port: 15KV ESD protection Power port: reverse-voltage and over voltage protection Antenna port: lightning protection (optional)
Standard and convenience	Support hardware and software WDT Support auto recovery mechanism to make router always online Ethernet port: 1.5KV magnetic isolation protection RS232/RS485 port: 15KV ESD protection SIM/UIM port: 15KV ESD protection Power port: reverse-voltage and over voltage protection Antenna port: lightning protection (optional)

High-performance and security	Support multiple WAN access methods, including static IP, DHCP, PPPOE, 2.5G/3G/4G/5G. Support double link backup between 2.5G/3G/4G/5G and WAN (optional). Support VPN client(PPTP, L2TP, IPSEC and GRE). Support remote management, SYSLOG, SNMP, TELNET, SSH, HTTPS, etc. Support local and remote firmware upgrade,import and export configure file. Support NTP, RTC embedded. Support multiple DDNS provider service. Support MAC address cloning. WiFi support 802.11b/g/n. support AP, client. (optional) WiFi support WEP,WPA,WPA2 encryption. (optional) Support multiple online trigger ways, including SMS, ring and data. Support link disconnection when timeout. Support APN/VPDN. Support multiple DHCP server and DHCP client, DHCP binding MAC address, DDNS, Firewall, NAT, DMZ host, QoS, traffic statistics, real-time display data transfer rate etc. Support TCP/IP, UDP, FTP(optional), HTTP, etc. Supports SPI firewall, VPN pass-through, access control, URL filtering,etc. Support local log storage. Support GPS/Beidou (optional). Support Dual SIM(optional).

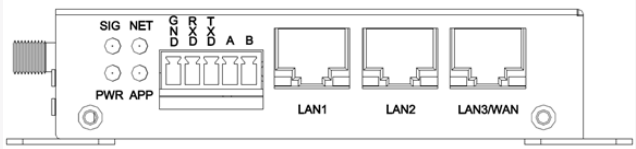
3. Block Diagram



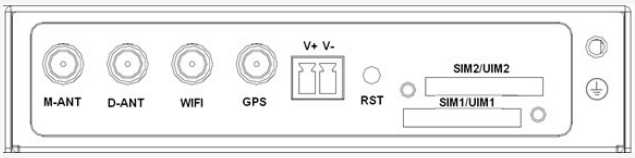
4. Product Specifications

ITEMS		CONTENTS
Hardware System	CPU	Industrial 32 bits CPU
	FLASH	16MB (Extendable to 64MB)
	SDRAM	128MB
Interface	Serial	1 RS232 and 1 RS485, 15KV ESD protection Serial port: 5 PIN industrial terminal, 3.5mm pitch Data bits: 5, 6 ,7, 8 Stop bits: 1, 1.5(optional), 2 Parity: none, even, odd, space, mark Baud rate: 110~230400 bps Large serial port data cache:10MB
	WAN/LAN	1 10/100Mbps WAN(RJ45,can configurable as LAN) port, auto MDI/MDIX, 1.5KV magnetic isolation protection
	LAN	2 10/100Mbps Ethernet ports(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
	Antenna	Cellular/GPS: Standard SMA female interface, 50 ohm WiFi: Standard SMA male interface, 50 ohm
	SIM/UIM	Standard 3V/1.8V user card interface, 15KV ESD protection
	Power	2 PIN industrial terminal, 3.81mm pitch, reverse- voltage and over voltage protection
	Reset	Press this key for 8 seconds to restore the Router to its original factory default settings
	Indicator	“PWR”, ”SIG”, ”NET”, ”APP”, ”Link”(RJ45)

Router front interface diagram:



Router side interface diagram:



Network	Wireless network	GSM/GPRS/EDGE: 850/900/1800/1900MHz CDMA: 800/1900MHz WCDMA/HSUPA/HSPA+: 850/900/1900/2100MHz CDMA2000 1x/ EVDO Rev. A: 800/1900MHz TD-SCDMA: 1880-1920/2010-2025MHz(A/F) TDD-LTE:Band 38/39/40/41& Band 61/62 (Private Network) FDD-LTE:Band1/2/3/4/5/7/8/12/13/17/18/19/20/21/25/26/28/66
	PPP protocol	Support PPP protocol
	PPP heartbeat	Maintaining links with the cellular network to prevent forced sleep, to ensure the stability of dial-up link.
	Network authentication	Support CHAP/PAP authentication
	TCP heartbeat	Monitor the server connection
WiFi (optional)	Standard	IEEE802.11b/g/n
	Bandwidth	IEEE802.11b/g: 54Mbps (max.) IEEE802.11n: 150Mbps (max.)
	Security	WEP, WPA, WPA2, etc. WPS (optional)

Power supply	Power range	DC 9~35V, recommended 12VDC/1.5A
	Communication current	<500mA (@12VDC)
	Standby current	<250mA (@12VDC)
Physical	Dimensions	107x98x24mm
	Weight	350g
	Installation	Mount Kit or DIN Rail 35mm (optional)
Environmental limits	Operating temperature	-35~+75°C (-31~+167°F)
	Storage temperature	-40~+85°C (-40~+185°F)
	Operating humidity	95% (unfreezing)

Installation Introduction

1. General

The router must be installed correctly to make it work properly.

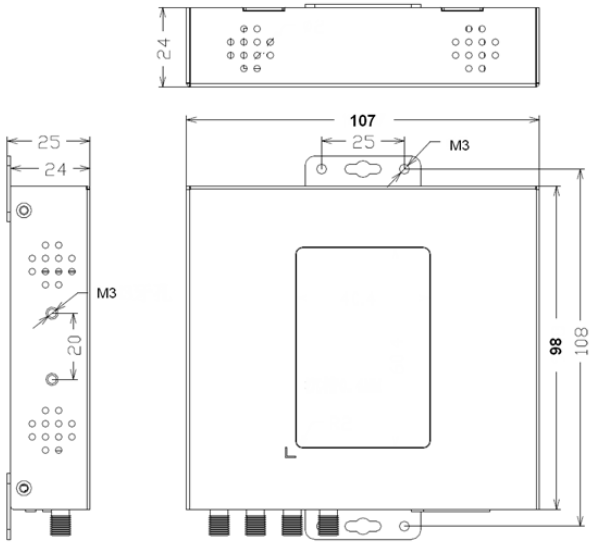
Warning: Forbid to install the router when powered!

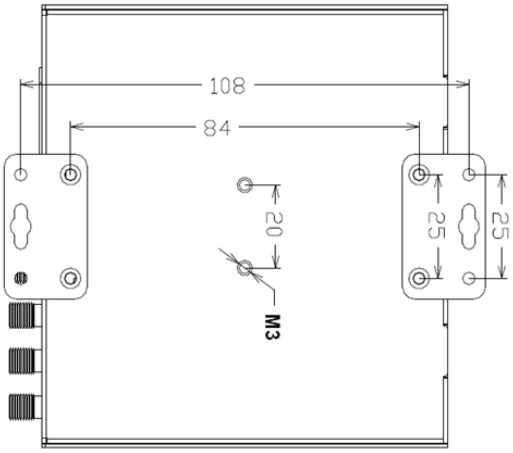
2. Encasement List

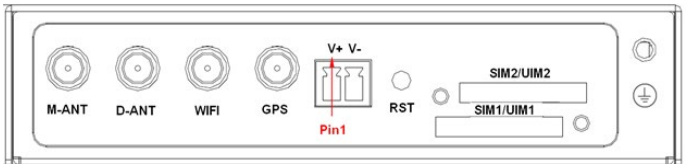
NAME	QUANTITY	REMARK
Router host	1	
Cellular antenna (male SMA)	1 or 2	
Network cable	1	
Power terminal	1	
Serial terminal	1	
WiFi antenna (female SMA)	1	Optional
Power adapter	1	Optional
RS232 cable	1	Optional
RS485 cable	1	Optional
GPS antenna	1	Optional
35mm din-rail buckle	1	Optional

3. Installation and Cable Connection

Dimensions in mm (the fixing piece is detachable):

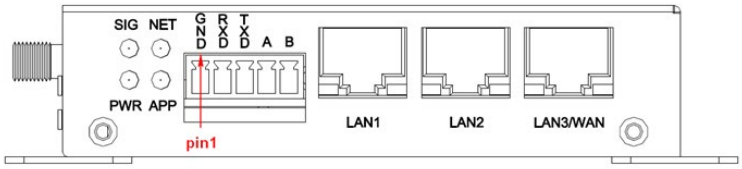






PIN NUMBER	SIGNAL NAME	DESCRIPTION
1	V+	Positive power supply
2	V-	Negative power supply

Communication interface definition:



5 pin 3.5mm pitch industrial terminal is defined as follows:

PIN NUMBER	SIGNAL NAME	DESCRIPTION
1	GND	System ground
2	RXD	RS232 receive
3	TXD	RS232 transmit
4	A	RS485+(A)
5	B	RS485-(B)

Product accessories:

RS232 cable (optional)

Cellular antenna (standard)

Power terminal (standard)

(2 pin 3.81mm pitch)

Serial terminal (standard)

(5 pin 3.5mm pitch)

Adapter (optional)

Network cable (standard)

35mm din-rail buckle (optional)

RS485 cable (optional)

WiFi antenna (optional)

GPS antenna (optional)

Installation of antenna:

Cellular antenna (standard)

WiFi antenna (optional)

GPS antenna (optional)

Screw the SMA male pin of the cellular/GPS antenna to the female SMA interface of the router with sign “ANT” and “GPS”(some models are two antennas, namely “M-ANT”, “D-ANT”).

Screw the SMA female pin of the WiFi antenna to the male SMA interface of the router with sign “WiFi”.

Warning: the cellular/GPS antenna and the WiFi antenna cannot be connected wrongly. And the antennas must be screwed tightly, or the signal quality of antenna will be influenced.

Installation of SIM/UIM card:

SIM/UIM Card Installation:

Firstly power off the router, and press the out button of the SIM/UIM card outlet with a needle object. Then the SIM/UIM card sheath will flick out at once. Put SIM/UIM card into the card sheath (Pay attention to put the side which has metal point outside), and insert card sheath back to the SIM/UIM card outlet.

Warning: forbid to install SIM/UIM card when powered.

Installation of cable:

Network Cable (Standard)

RS232 Cable (optional)

RS485 Cable (optional)

Insert one end of the network cable into the switch interface with sign “WAN” or “LAN”, and the other end into the Ethernet interface of user’s device. The signal connection of network direct cable is as follows:

RJ45-1	RJ45-2
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

RS232 and RS485 cable should be screwed into the serial terminal, ensure the signal connection is correct. The RS232 cable is as follows:

DB9F PIN NUMBER	WIRE COLOR
2	Blue
3	Brown
5	Black

4. Power Adapter (optional)

The power range of the router is DC 9~35V. Warning: when we use other power, we should make sure that the power can supply power above 7W.

We recommend user to use the standard DC 12V/1.5A power.

5. Indicator Lights Introduction

The router provides following indicator lights: “Power”, “SIG”, “NET”, “APP”, “LINK”.

INDICATOR	STATE	INTRODUCTION
Power	OFF	Router is powered off
	ON	Router is powered on
SIG	OFF	The signal is terrible
	BLINK	Signal strength is weak
	ON	Signal strength is good
NET	OFF	SIM/UIM card is not recognized
	BLINK	SIM/UIM card is recognized but not dialed
	ON	Router has logged on network
APP	OFF	Serial port application is closed
	BLINK	Serial port application is connecting
	ON	Serial port application connection is normal
Link (yellow) (RJ45)	OFF	WAN/LAN is not connected
	ON/BLINK	WAN/LAN is connected/communicating

6. Reset Button Introduction

The router has a “Reset” button to restore it to its original factory default settings. When user press the “Reset” button for up to 8 seconds, the router will restore to its original factory default settings and restart automatically. (The auto-restart is as follows: The “RUN” indicator turns off for about 10 seconds and then functions normally).

The auto-restart is as follows: the “POWER” indicator turns off for about 10 seconds and then functions normally.

Configuration and Management

This chapter describes how to configure and manage the router.

1. Configuration Connection

Before configuration, you should connect the router and your PC with the supplied network cable. Plug the cable's one end into the Local Network port of the router, and another end into your PC's Ethernet port.

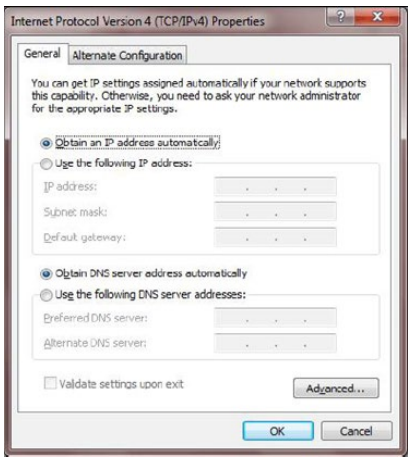
The connection diagram is as following:

Please modify the IP address of PC the same as network segment address of the router, for instance, 192.168.1.9. Modify the mask code of PC as 255.255.255.0 and set the default gateway of PC as the router's IP address (192.168.1.1).

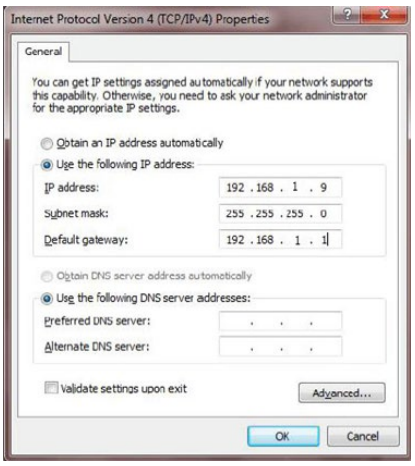
2. Access the Configuration Web Page

2.1 IP Address Setting

IP Address - DHCP



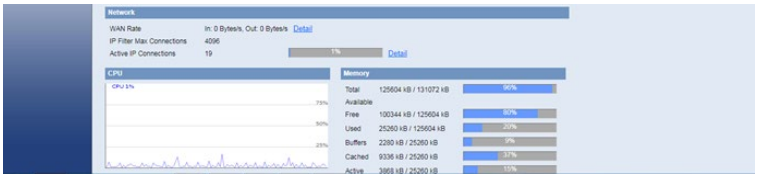
IP Address - Static. Set the IP PC address to 192.168.1.9. Set the subnet mask to 255.255.255.0. Set the default gateway to 192.168.1.1.



2.2 Access the Configuration Web Page

The chapter is to present main functions of each page. Users visit page tool via web browser after connect users' PC to the router.

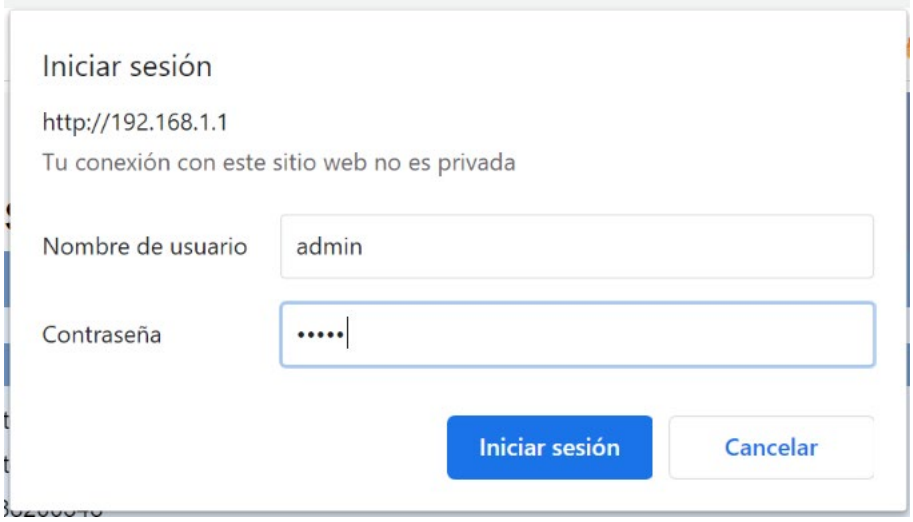
Start a web browser and type 192.168.1.1 in the Address (URL) field (The Default IP Address of the Ethernet port is 192.168.1.1). It will prompt the Web management tool of the router. The users login in the web page, there will display a page shows as blow. Users have to click "Continue" to make it work if they modify language.



After access to the information main page.

The operation data and state of each module can be completely observed in the information main page, which including basic information of routing, WAN, LAN, wireless, network, CPU, memory and other basic information.

Access other pages. It will prompt a login page. The default username and password are both “admin”. Please input the username and password login to access the configuration pages.



Input correct user name and password to visit relevant menu page.

3. Basic

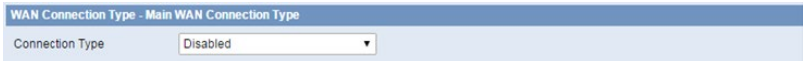
3.1 WAN

Select the appropriate wide area networking mode according to different requirements. Set the corresponding parameters according to different connection modes.

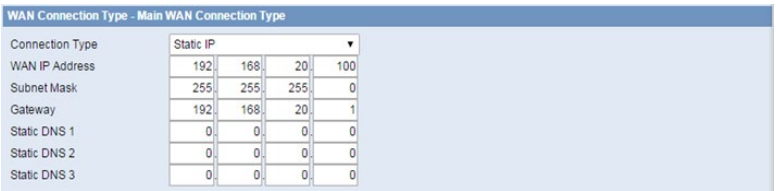
Dual Both Online: WAN and Bkup WAN are both online.The system will automatically switch back to the main chain when the main link is available if enabled.

Link Fail to Restart: Time of restart system for all link fail.

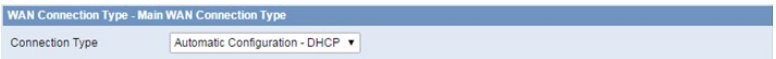
Disable WAN connection



Put in the IP address, subnet mask, default gateway, and DNS Server(optional) assigned by the provider.

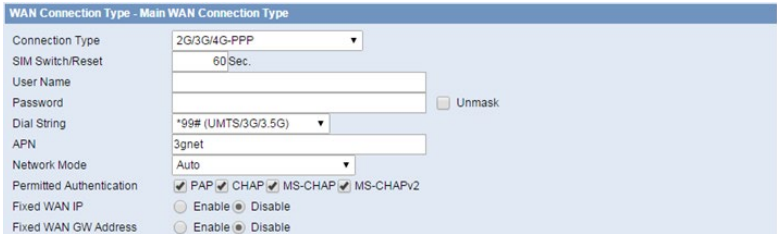


Normally, The Internet IP Address of the router is allocated by the ISP automatically.



You may choose “PPPoE” if you connect the WAN port to a PPPoE server. Input the correct username and password provided by ISP or administrator.

If you want to access to 2G/3G/4G network, you can choose “2G/3G/4G-PPP” or “2G/3G/4G-DHCP” mode.



SIM Switch/Reset: Time of restart SIM card for dial fail.

User Name: Login users' ISP(Internet Service Provider)

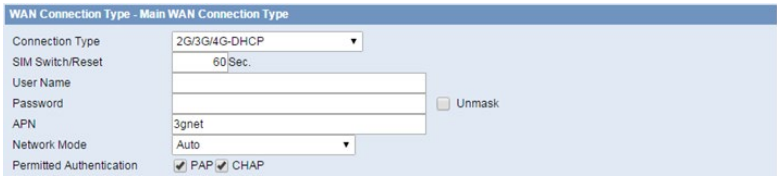
Password: Login users' ISP

Dial String: Dial number of users' ISP

APN: Access point name of users' ISP

Network Mode: Select the appropriate network model according to the environment.

Permitted Authentication:Select the authentication protocol according to the requirements.



Refer to 2G/3G/4G-PPP mode.

Force reconnect: Reset the connection according to the set time.

Connect Fail: Switch to Backup WAN after link failure times.

Dial Fail to Restart: Time of restart system for this link fail.

Keep Alive: This function is used to detect whether the Internet connection is active. It will redial to users' ISP immediately to make the connection active if users set it and when the router detect the connection is inactive. Specifies how many seconds to wait before reconnect the link after it terminates.

None: do not set this function

Ping: Send ping packet to detect the connection, when choose this method. Users should also configure "Keep Alive Interval", "Keep Alive Server IP" and "Keep Alive Server IP2" items.

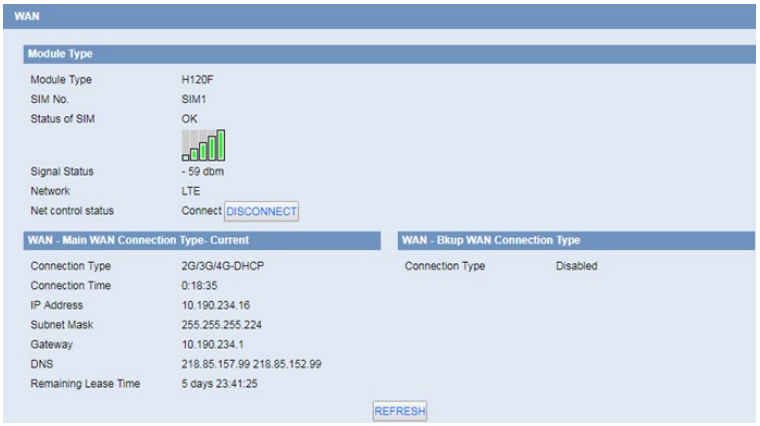
Route: Detect connection with route method, when choose this method. Users should also configure "Keep Alive Interval", "Keep Alive Server IP" and "Keep Alive Server IP2" items.

PPP: Detect connection with PPP method, when choose this method. Users should also configure "Detection Interval" item.

Keep Alive Fail: Switch to Backup WAN after keep alive fail times.

NOTE: When users choose the "Route" or "Ping" method, it's quite important to make sure that the "Keep Alive Server IP" and "Keep Alive Server IP2" are usable and stable, because they have to response the detection packet frequently.

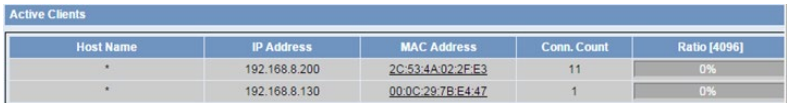
3.2 WAN Status



The page show the specific connection details, including module information, network operators, as well as the connection of the IP address and DNS, etc.., according to the different connection types.

3.3 LAN Status

LAN port MAC, IP and DNS and other information.



Host Name	IP Address	MAC Address	Conn. Count	Ratio [4096]
*	192.168.8.200	2C:53:4A:02:2F:E3	11	0%
*	192.168.8.130	00:0C:29:7B:E4:47	1	0%

Host Name: Host name of LAN client.

IP Address: IP address of the client.

MAC Address: MAC address of the client.

Conn. Count: Connection count caused by the client.

Ratio: The ratio of 4096 connection.

DHCP Status	
DHCP Server	Enabled
Start IP Address	192.168.1.100
End IP Address	192.168.1.149
Client Lease Time	1440 minutes

DNCP Server: Enable or disable the router work as a DHCP server.

Starting IP Address: The starting IP Address of the DHCP server's Address pool.

Ending IP Address: The ending IP Address of the DHCP server's Address pool.

Client Lease Time: The lease time of DHCP client.

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time	Delete
		- None -		

Host Name: Host name of LAN client.

IP Address: IP address of the client.

MAC Address: MAC address of the client.

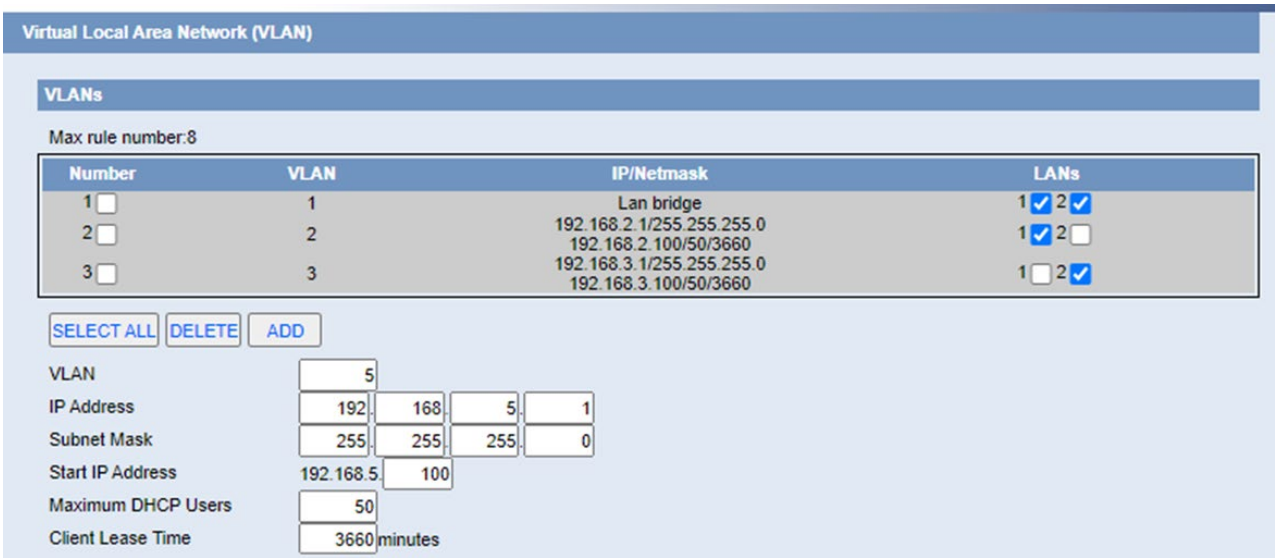
Expires: The expiry the client rents the IP address.

Delete: Click to delete DHCP client.

4. Advanced

4.1 VLANs

The device has up to 3 LAN ports according to the hardware, and each physical interface can support independent VLAN configuration.

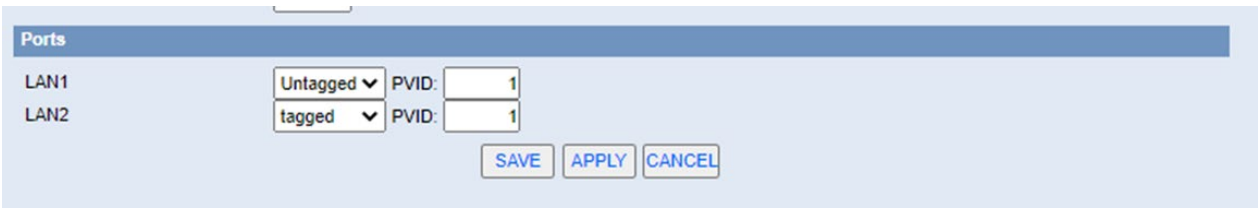


VLAN: VLAN ID

IP Address: IP Address of VLAN

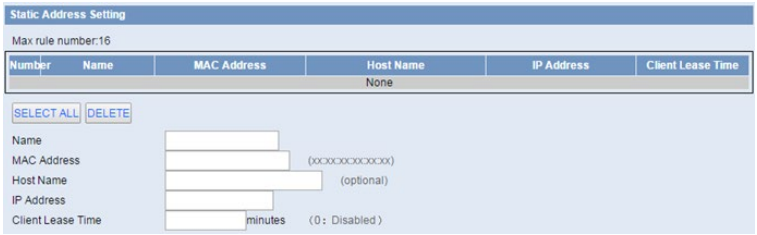
Subnet Mask: Subnet Mask of VLAN

Start IP Address/Maximum DHCP Users/Client Lease Time: DHCP Server of VLAN.



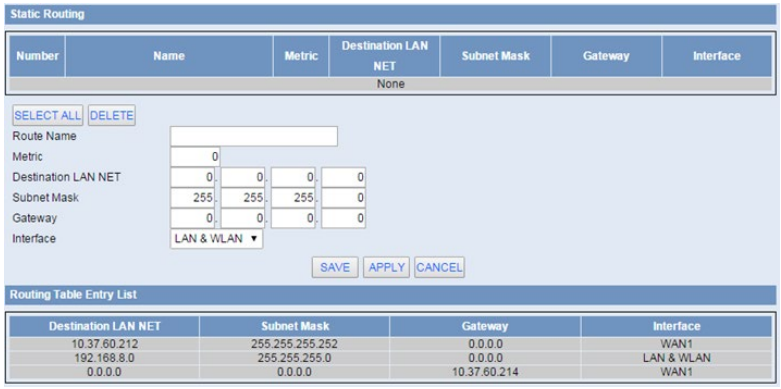
Configure the VLAN TAG attributes of the packets on each physical port and the PVID of the port.

4.2 Statically Assigned



Statically Assigned: Assign the static IP address to the specified client according to MAC address.

4.3 Advanced Router



Route Name: Defined routing name by users, up to 25 characters.

Metric: 0-9999.

Destination LAN NET: The Destination IP Address is the address of the network or host to which users want to assign a static route.

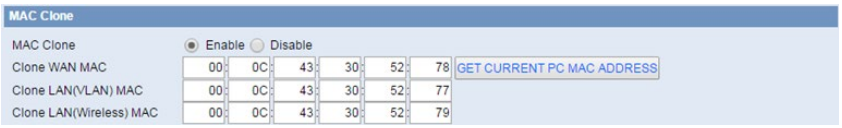
Subnet Mask: The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.

Gateway: IP address of the gateway device that allows for contact between the router and the network or host.

Interface: Indicate users whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), the WAN (Internet), or Loopback (a dummy network in which one PC acts like a network, necessary for certain software programs).

4.4 MAC Address Clone

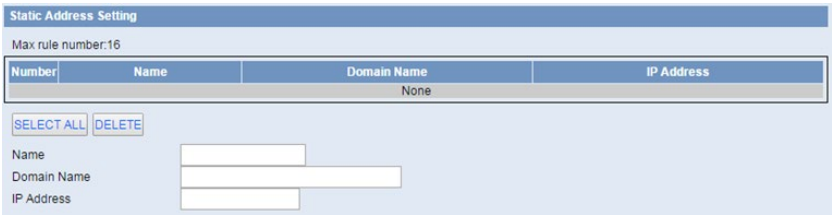
Some ISP need the users to register their MAC address. The users can clone the router MAC address to their MAC address registered in ISP if they do not want to re-register their MAC address.



Clone MAC address: It can clone three parts: Clone LAN MAC, Clone WAN MAC, Clone Wireless MAC.

NOTE: One MAC address is 48 characteristic. MAC address can not be set to the multicast address, the first byte must be even. And MAC address value of network bridge br0 is determined by the smaller value of wireless MAC address and LAN port MAC address.

4.5 SDNS



When users host their domain names on free or commercial servers, they usually get a static IP (non-changeable IP) address for their websites, which involves the use of static name servers, or static DNS, as well. Static DNS settings will never update on their own and will remain the same, until you decide to update them. Static DNS settings are very useful, since they provide a stable service with no interruptions, and can increase the overall speed of the website.

4.6 VRRP

Virtual Interface: The binding runtime interface.

Related to Wan: When the WAN port linkage work is enabled, when the WAN port is unable to access

the internet, the VRRP status value shows Down, and automatically quits the VRRP backup group. The remaining VRRP routers run for Master router router.

Virtual Gateway: The default gateway address for external communication.

Serial Numbers: The MAC address of the client who is currently logged in to the WEB management page, click the button, and fill the MAC address of the PC that can get the current management device into the MAC address of the cloned WAN port.

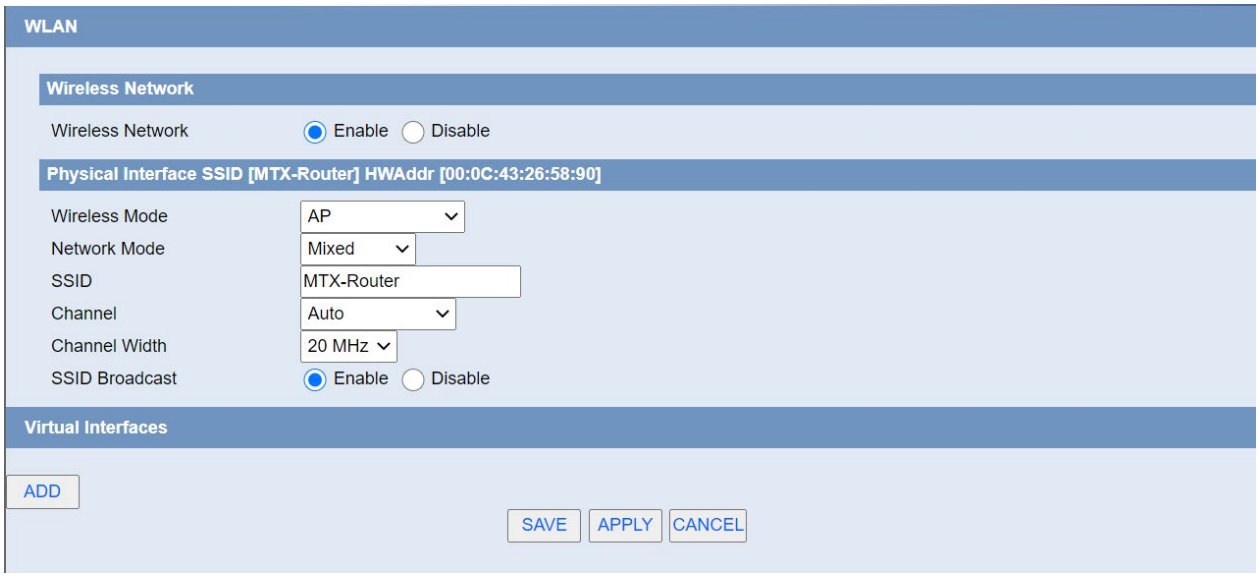
Priority: The higher priority is master.

Notice Timers: If the backup machine does not receive advertisement messages from the host every X seconds, a new round of elections will take place.

Run State: Displays whether the current router is in standby or host state.

5. Wireless

5.1 Basic Settings



Wireless Network: “Eanble”, radio on. “Disable”, radio off.

Wireless Mode: AP.

Network Mode:

Mixed: Support 802.11b, 802.11g, 802.11n wireless devices.

BG-Mixed: Support 802.11b, 802.11g wireless devices.

B-only: Only supports the 802.11b standard wireless devices.

B-only: Only supports the 802.11b standard wireless devices.

G-only: Only supports the 802.11g standard wireless devices.

NG-Mixed: Support 802.11g, 802.11n wireless devices.

N-only: Only supports the 802.11g standard wireless devices.

SSID: The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all devices in your wireless network.

Channel: A total of 1-13 channels to choose more than one wireless device environment, please try to avoid using the same channel with other devices.

Channel Width: 20MHZ and 40MHZ.

Channel: Channel for 40MHZ, you can choose upper or lower.

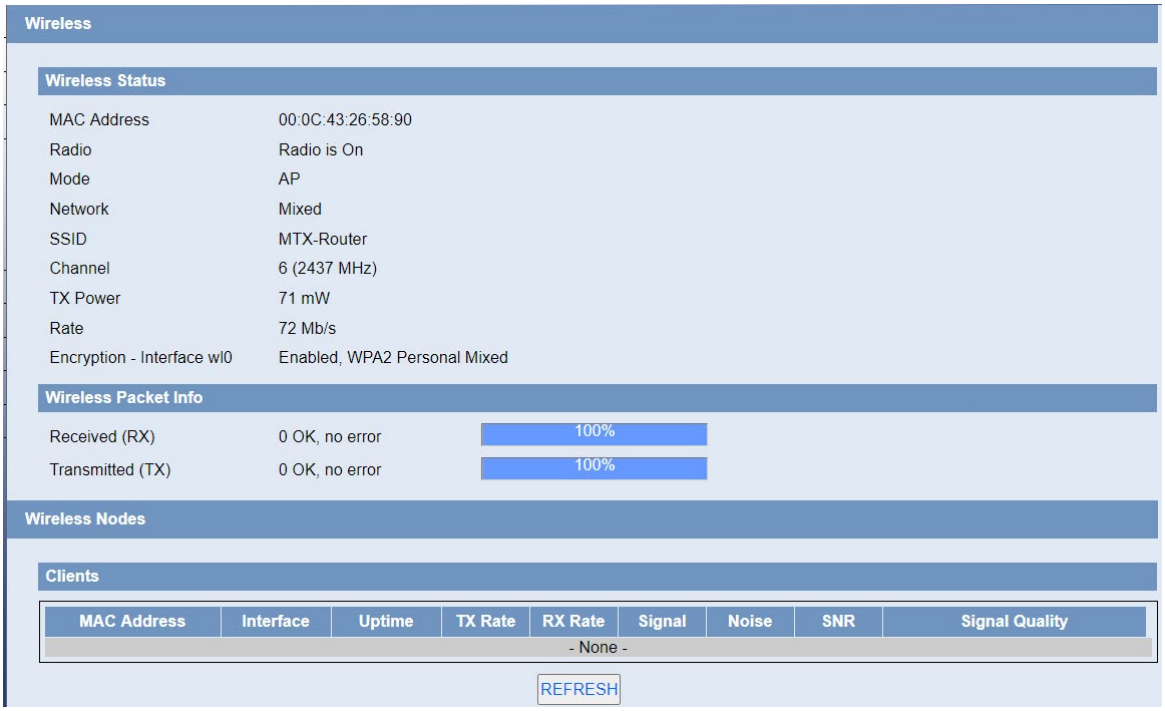
Wireless SSID Broadcast: Enable, SSID broadcasting; Disable, Hidden SSID.

Virtual Interfaces: Click Add to add a virtual interface. Add successfully, click on the remove, you can remove the virtual interface.

AP Isolation: This setting isolates wireless clients so access to and from other wireless clients are stopped.

5.2 Wireless Security

Wireless security options used to configure the security of your wireless network. This route is a total of seven kinds of wireless security mode. Disabled by default, not safe mode is enabled. Such as changes in Safe Mode, click Apply to take effect immediately.



WEP: Is a basic encryption algorithm is less secure than WPA. Use of WEP is discouraged due to security weaknesses, and one of the WPA modes should be used whenever possible. Only use WEP if you have clients that can only support WEP (usually older, 802.11b-only clients).

Authentication Type: Open or shared key

Default Transmit Key: Select the key form Key 1 - Key 4 key.

Encryption: There are two levels of WEP encryption, 64-bit (40-bit) and 128-bit. To utilize WEP, select the desired encryption bit, and enter a Passphrase or up to WEP key in hexadecimal format. If you are using 64-bit (40-bit), then each key must consist of exactly 10 hexadecimal characters or 5 ASCII characters. For 128-bit, each key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are “0”-”9” and “A”-”F”.

ASCII/HEX: ASCII, the keys is 5 bit ASCII characters/13bit ASCII characters. HEX, the keys is 10bit/26 bit hex digits.

Passphrase: The letters and numbers used to generate a key.

Key1-Key4: Manually fill out or generated according to input the pass phrase.

WPA Personal/WPA2 Personal/WPA2 Person Mixed:TKIP/AES/TKIP+AES, dynamic encryption keys. TKIP + AES, self-applicable TKIP or AES. WPA Person Mixed, allow WPA Personal and WPA2 Personal client mix.

WPA Shared Key: Between 8 and 63 ASCII character or hexadecimal digits.

Key Renewal Interval (in seconds):1-99999.

5.3 Wireless Status

MAC Address: MAC address of wireless client.

Radio: Display whether radio is on or not.

Mode: Wireless mode.

Network: Wireless network mode.

SSID: Wireless network name.

Channel: Wireless network channel.

TX Power: Reflection power of wireless network.

Rate: Reflection rate of wireless network.

Encryption-Interface wl0: Enable or disable Encryption-Interface wl0.

Wireless Packet Info		
Received (RX)	622820 OK, no error	100%
Transmitted (TX)	7452 OK, no error	100%

Received (RX): received data packet.

Transmitted (TX): transmitted data packet.

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

MAC Address: MAC address of wireless client.

Interface: Interface of wireless client.

Uptime: Uptime of wireless client.

TX Rate: Transmit rate of wireless client.

RX Rate: Receive rate of wireless client.

Signal: The signal of wireless client.

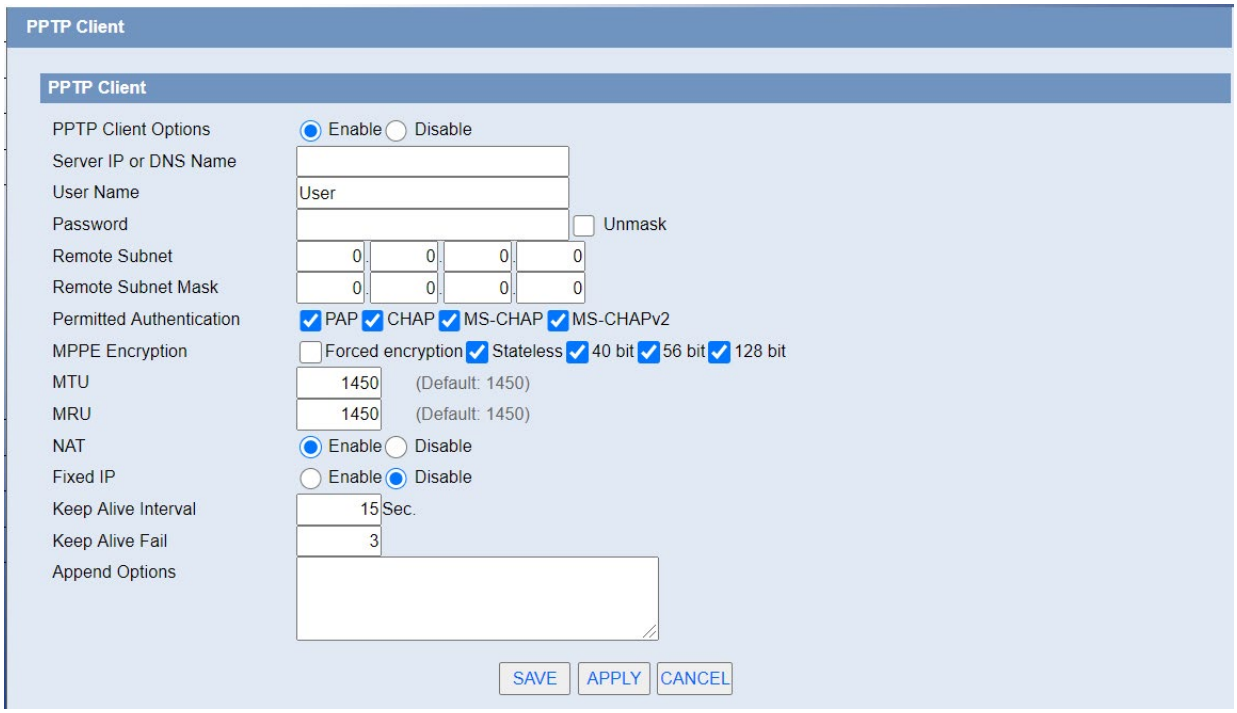
Noise: The noise of wireless client.

SNR: The signal to noise ratio of wireless client.

Signal Quality: Signal quality of wireless client.

6. VPN

6.1 PPTP



Server IP or DNS Name: PPTP server's IP Address or DNS Name.

Remote Subnet: The network of the remote PPTP server.

Remote Subnet Mask: Subnet mask of remote PPTP server.

Permitted Authentication: Select permitted authentication.

MPPE Encryption: Enable or disable Microsoft Point-to-Point Encryption.

MTU: Maximum Transmission Unit.

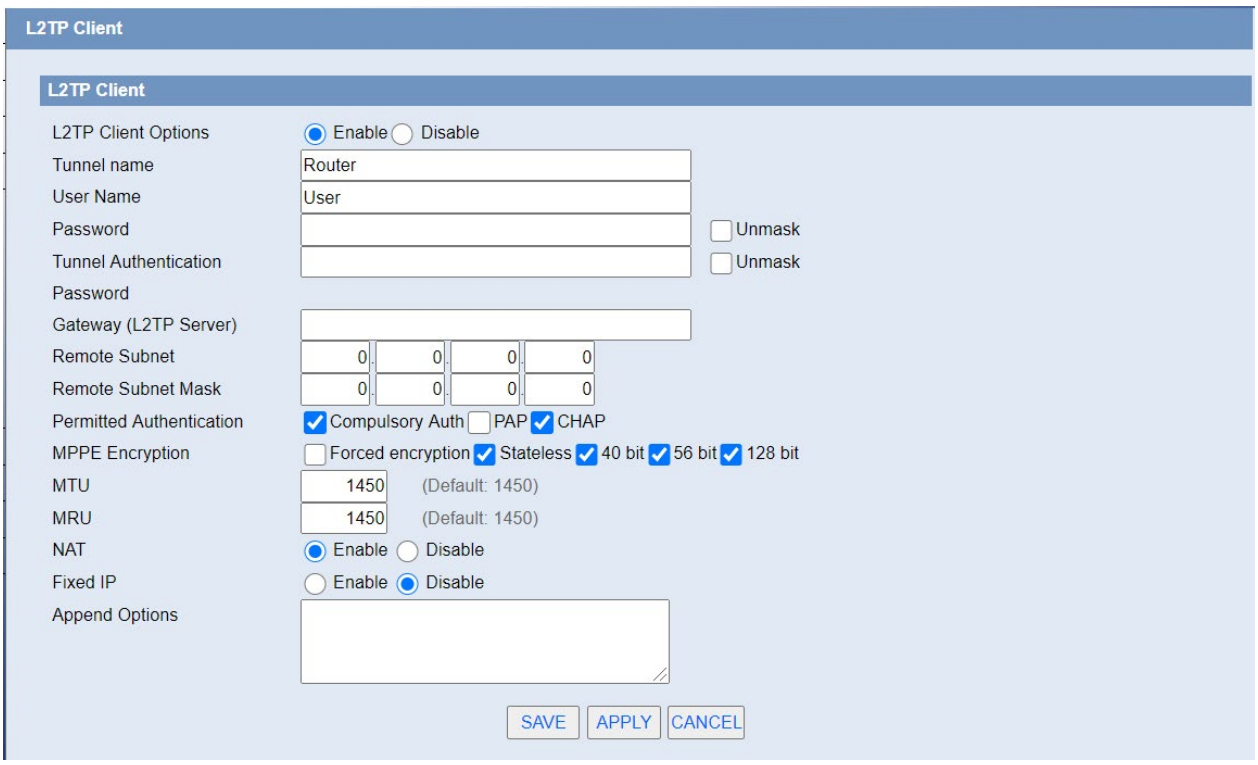
MRU: Maximum Receive Unit.

NAT: Network Address Translation.

User Name: User name to login PPTP Server.

Password: Password to log into PPTP Server.

6.2 L2TP



User Name: User name to login L2TP Server.

Password: Password to login L2TP Server.

Gateway(L2TP Server): L2TP server's IP Address or DNS Name.

Remote Subnet: The network of remote PPTP server.

Remote Subnet Mask: Subnet mask of remote PPTP server.

Permitted Authentication: Select permitted authentication.

MPPE Encryption: Enable or disable Microsoft Point-to-Point Encryption.

MTU: Maximum transmission unit.

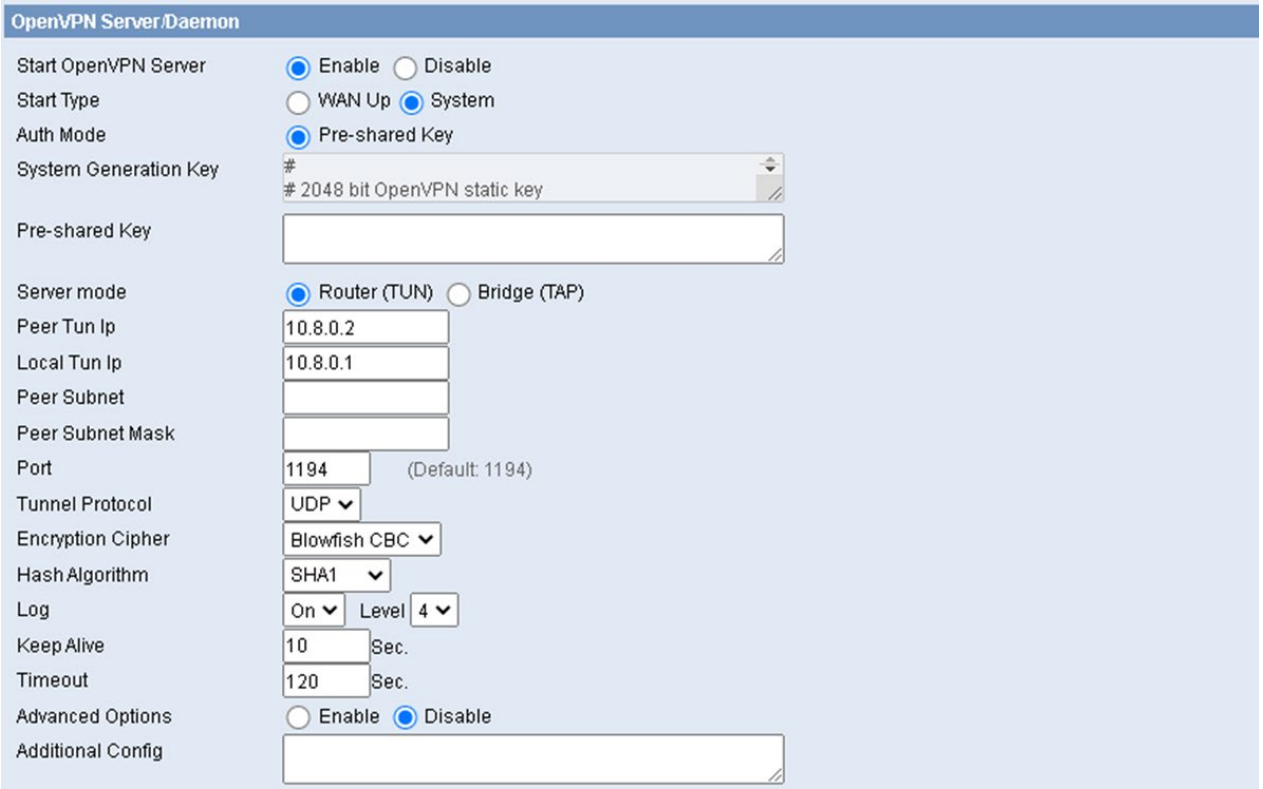
MRU: Maximum receive unit.

NAT: Network address translation.

6.3 OpenVPN

Please refer to Aplication Note from our website “AN2- OpenVPN configuration on MTX-Router-EOS”.

Server



Start Type: Startup while wan is up or system is up.

Auth Mode: Support pre-shared key authentication

System Generation Key: Randomly generated by the system

Pre-shared Key: Configure pre-shared key

Server mode: Tunnel mode or bridge mode

Peer Tun Ip/ Local Tun Ip: Tunnel ip address.

Peer Subnet/Peer Subnet Mask: Tunnel Subnet Mask

Port: Network port.

Tunnel Protocol: UDP or TCP.

Encryption Cipher: Standard of channel encryption

Hash Algorithm: Standard of hash algorithm

Client

Server IP/Name: IP/Name of server.

Port: Server port.

Auth Mode: Support pre-shared key authentication

Pre-shared Key: Configure pre-shared key

Server mode: Tunnel mode or bridge mode

Peer Tun Ip/ Local Tun Ip: Tunnel ip address.

Peer Subnet/Peer Subnet Mask: Tunnel Subnet Mask

Tunnel Protocol: UDP or TCP.

Encryption Cipher: Standard of channel encryption

Hash Algorithm: Standard of hash algorithm

6.4 IPSEC

Please refer to Aplication Note from our website “AN1- IPSec configuration on MTX-Router-EOS”.

Name: Indicate this connection name, must be unique.

Enabled: If enable, the connection will send tunnel connection request when it is reboot or re-connection, otherwise it is no need if disable.

Local WAN Interface: Local addresss of the tunnel.

Remote Host Address: IP/domain name of end opposite; this option can not fill in if using tunnel mode server

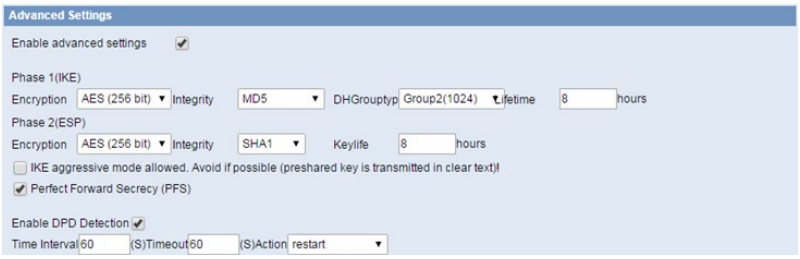
Local Subnet: IPSec local protects subnet and subnet mask, i.e. 192.168.1.0/24; this option can not fill in if using transfer mode.

Remote Subnet: IPSec opposite end protects subnet and subnet mask, i.e.192.168.7.0/24; this option can not fill in if using transfer mode.

Local ID: Tunnel local end identification, IP and domain name are available.

Remote ID: Tunnel opposite end identification, IP and domain name are available.

Use a Pre-Shared Key: Choose use share encryption option.



Enable Advanced Settings: Enable to configure 1st and 2nd phase information, otherwise it will auto negotiation according to opposite end.

Phase 1(IKE)

Encryption: IKE phased encryption mode.

Integrity: IKE phased integrity solution.

DHGrouptype: DH exchange algorithm.

Lifetime: Set IKE lifetime, current unit is hour, the default is 0.

Phase 2(ESP)

Encryption: ESP encryption type.

Integrity: ESP integrity solution.

Keylife: Set ESP keylife, current unit is hour, the default is 0.

IKE aggressive mode allowed: Negotiation mode adopt aggressive mode if tick; it is main mode if non-tick.

Perfect Forward Secrecy: Tick to enable PFS, non-tick to disable PFS.

Enable DPD Detection: Enable or disable this function, tick means enable.

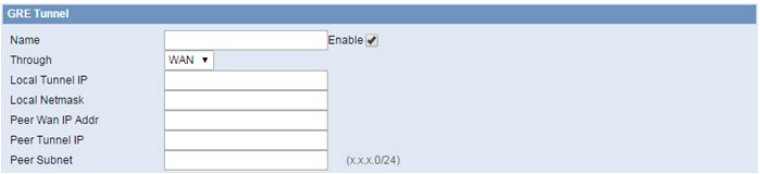
Time Interval: Set time interval of connect detection (DPD).

Timeout: Set the timeout of connect detection.

Action: Set the action of connect detection.

6.5 GRE

GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) protocol is a network layer protocol (such as IP and IPX) data packets are encapsulated, so these encapsulated data packets to another network layer protocol (IP)transmission. GRE Tunnel (tunnel) technology, Layer Two Tunneling Protocol VPN (Virtual Private Network).



Name: GRE tunnel name.

Through: The GRE packet transmit interface.

Local Tunnel IP: The local tunnel ip address.

Local Netmask: Netmask of local network.

Peer Wan IP Addr: The remote WAN address.

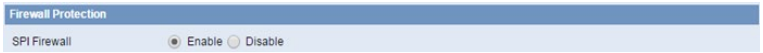
Peer Tunnel IP: The remote tunnel ip address.

Peer Subnet: The remote gateway local subnet, eg: 192.168.1.0/24.

7. Security

7.1 Firewall

You can enable or disable the firewall, filter specific Internet data types, and prevent anonymous Internet requests, ultimately enhance network security.

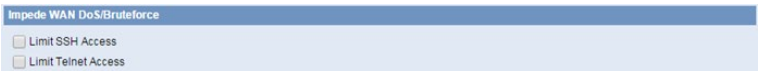


Firewall enhance network security and use SPI to check the packets into the network.To use firewall protection, choose to enable otherwise disabled. Only enable the SPI firewall, you can use other firewall functions: filtering proxy, block WAN requests, etc.

Block Anonymous WAN Requests (ping): By selecting “Block Anonymous WAN Requests (ping)” box to enable this feature, you can prevent your network from the Ping or detection of other Internet users. so that make More difficult to break into your network. The default state of this feature is enabled ,choose to disable allow anonymous Internet requests.

Filter IDENT (Port 113): Enable this feature can prevent port 113 from being scanned from outside. Click the check box to enable the function otherwise disabled.

Block WAN SNMP access: This feature prevents the SNMP connection requests from the WAN.



Limit ssh Access: This feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit Telnet Access: This feature limits the access request from the WAN by Telnet, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Filter Proxy: Wan proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

Filter Cookies: Cookies are the website of data the data stored on your computer.When you interact with the site ,the cookies will be used. Click the check box to enable the function otherwise disabled.

Filter Java Applets: If refuse to Java, you may not be able to open web pages using the Java programming. Click the check box to enable the function otherwise disabled.

Filter ActiveX: If refuse to ActiveX, you may not be able to open web pages using the ActiveX programming. Click the check box to enable the function otherwise disabled.

7.2 Access Restriction

Use access restrictions, you can block or allow specific types of Internet applications. You can set specific PC-based Internet access policies. This feature allows you to customize up to ten different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses.

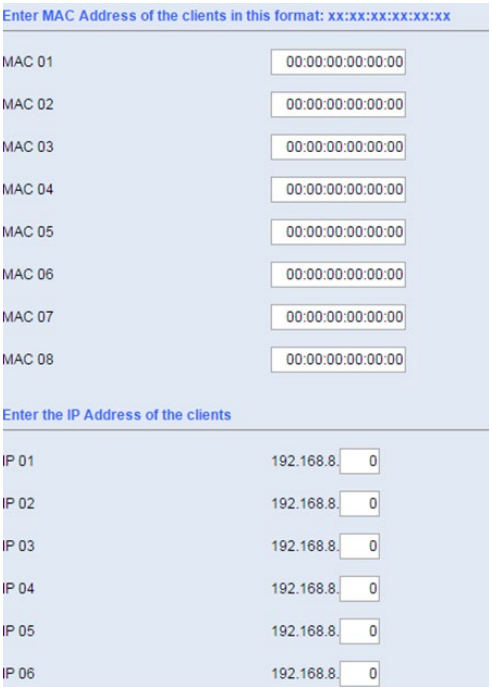
Two options in the default policy rules: “Filter” and “reject”. If select “Deny”, will deny specific computers to access any Internet service at a particular time period. If choose “filter”, it will block specific computers to access the specific sites at a specific time period. You can set up 10 Internet access policies filtering specific PCs access Internet services at a particular time period.

Access Policy: You may define up to 10 access policies. Click Delete to delete a policy or Summary to see a summary of the policy.

Status: Enable or disable a policy.

Policy Name: You may assign a name to your policy.

PCs: The part is used to edit client list, the strategy is only effective for the PC in the list.

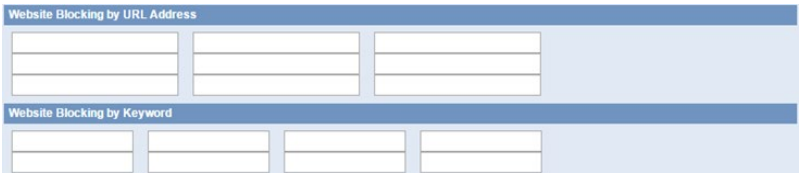


Set up Internet access policy:

Select the policy number (1-10) in the drop-down menu.

- For this policy is enabled, click the radio button next to “Enable”
- Enter a name in the Policy Name field.

- Click the Edit List of PCs button.
- On the List of PCs screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the IP fields. If you have a range of IP addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC addresses into the MAC fields.
- Click the Apply button to save your changes. Click the Cancel button to cancel your unsaved changes. Click the Close button to return to the Filters screen.
- If you want to block the listed PCs from Internet access during the designated days and time, then keep the default setting, Deny. If you want the listed PCs to have Internet filtered during the designated days and time, then click the radio button next to Filter.
- Set the days when access will be filtered. Select Everyday or the appropriate days of the week.
- Set the time when access will be filtered. Select 24 Hours, or check the box next to From and use the drop-down boxes to designate a specific time period.
- Click the Add to Policy button to save your changes and active it.
- To create or edit additional policies, repeat steps 1-9.
- To delete an Internet Access Policy, select the policy number, and click the Delete button.



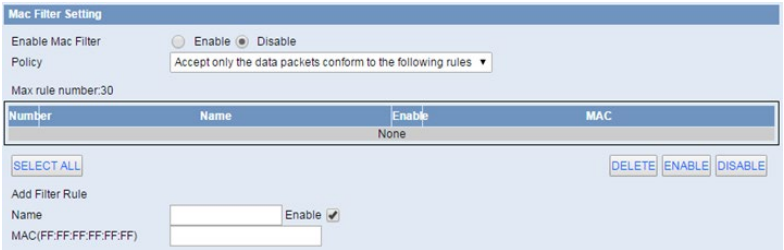
Website Blocking by URL Address: You can block access to certain websites by entering their URL.

Website Blocking by Keyword: You can block access to certain website by the keywords contained in the web page.

NOTE: The default factory value of policy rules is “filtered”. If the user chooses the default policy rules for “refuse”, and editing strategies to save or directly to save the settings. If the strategy edited is the first, it will be automatically saved into the second, if not, please keep the original number.

Turn off the power of the router or reboot the router can cause a temporary failure. After the failure of the router, if can not automatically synchronized NTP time server, you need to ensure the correct implementation of the relevant period control function.

7.3 MAC Filter



Using MAC address for data filtering.

7.4 Packet Filter

Firewall rules to protect your network from malicious attacks on Internet network viruses.

Packet filter: Enable or disable packet filtering.

Policy: Select the action of the data package that does not conform to the setting rules.

Accept only the data packets conform to the following rules: Only access to match the address.

Discard packets conform to the following rules: Only receive the network address that complies with the custom rules, and drop all other addresses.

NOTE: Add filter matching rules. Source port, destination port, source address, destination address must be filled in at least one item.

INPUT: Data packets from WAN port to LAN port.

OUTPUT: Data packets from the LAN port to the WAN port.

Pro: Protocol type for a data packet.

Sport: The source port of the data package.

Dport: Port of destination.

Source IP: The source IP address of the data package.

Destination IP: Destination IP address.

8. Forwarding

8.1 Port Forwarding

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, the router will forward those requests to the appropriate PC.

Application: Enter the name of the application in the field provided.

Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.

Source Net: Forward only if sender matches this ip/net (example 192.168.1.0/24).

Port from: Enter the number of the external port (the port number seen by users on the Internet).

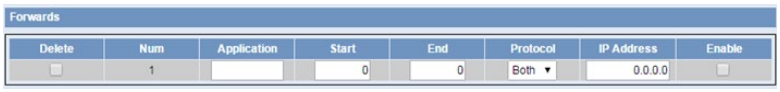
IP Address: Enter the IP Address of the PC running the application.

Port to: Enter the number of the internal port (the port number used by the application).

Enable: Click the Enable check box to enable port forwarding for the application.

8.2 Port Range

Port Range Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, the router will forward those requests to the appropriate PC.



Application: Enter the name of the application in the field provided.

Start: Enter the number of the first port of the range you want to seen by users on the Internet and forwarded to your PC.

End: Enter the number of the last port of the range you want to seen by users on the Internet and forwarded to your PC.

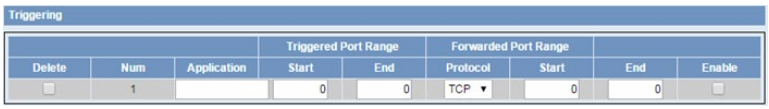
Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.

IP Address: Enter the IP Address of the PC running the application.

Enable: Click the Enable check box to enable port forwarding for the application.

8.3 Port Triggering

Port Triggering allows you to do port forwarding without setting a fixed PC. By setting Port Triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.



Application: Enter the name of the application in the field provided.

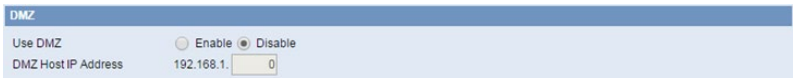
Triggered Port Range: Enter the number of the first and the last port of the range, which should be triggered. If a PC sends outbound traffic from those ports, incoming traffic on the Forwarded Range will be forwarded to that PC.

Forwarded Port Range: Enter the number of the first and the last port of the range, which should be forwarded from the Internet to the PC, which has triggered the Triggered Range.

Enable :Click the Enable check box to enable port triggering for the application.

8.4 DMZ

The DMZ (DeMilitarized Zone) hosting feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.

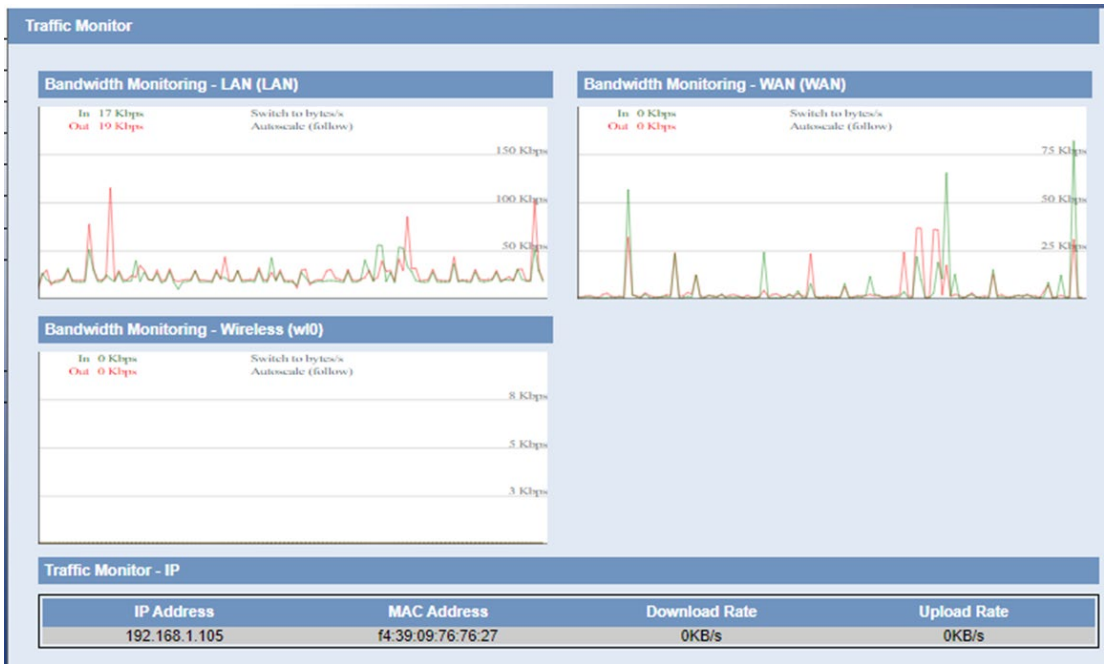


Any PC whose port is being forwarded must should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ Host IP Address: To expose one PC to the Internet, select Enable and enter the computer's IP address in the DMZ Host IP Address field. To disable the DMZ, keep the default setting: Disable.

9. Traffic Monitoring

9.1 Bandwidth State

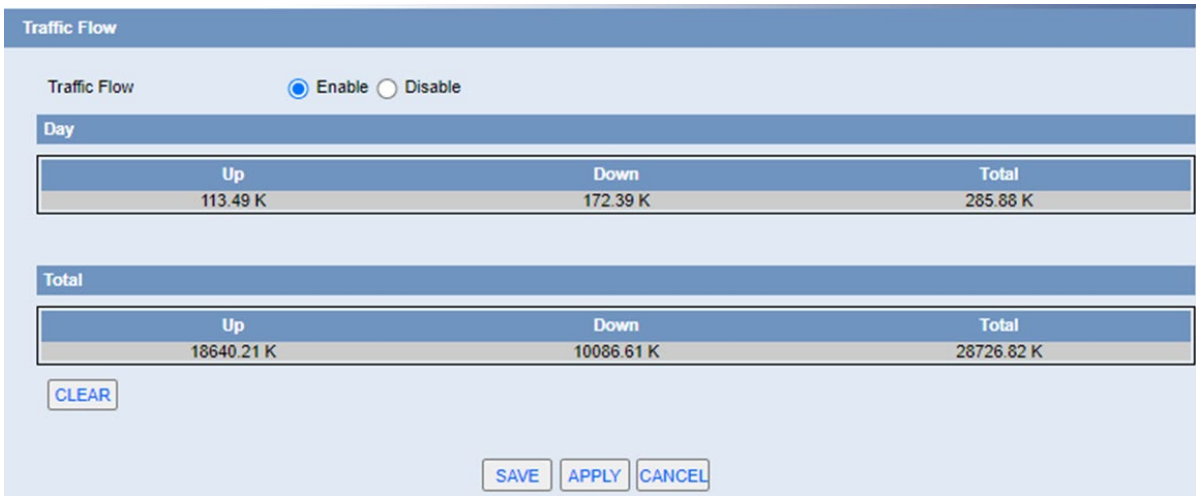


Show the bandwidth of WAN, LAN, WIFI.

Abscissa axis: Time.

Vertical axis: Speed rate.

9.2 Traffic Flow

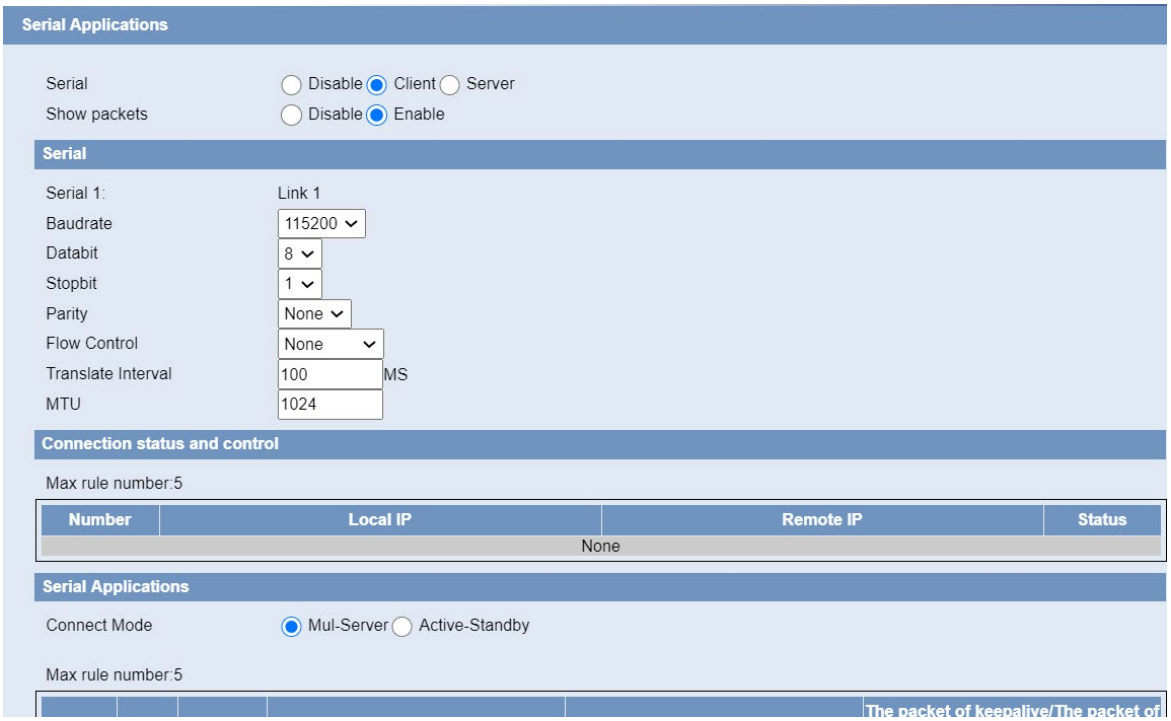


Visual display of statistics of the upstream and downstream, as well as the total traffic.

10. Serial and Remote Management

10.1 Serial

There is a console port on the router. Normally, this port is used to debug. This port can also be used for serial transmission. The router has embedded a serial to TCP program. The data sent to the serial port is encapsulated by TCP/IP protocol stack and then is sent to the destination server. This function can work as a IP Modem.



Baudrate: The serial port's baud rate.

Databit: The serial port's data bit.

Parity: The serial port's parity.

Stopbit: The serial port's stopbit.

Flow Control: The serial port's flow control type.

Enable Serial TCP Function: Enable the serial to TCP function.

Protocol Type: The protocol type to transmit data.

UDP(DTU): Data transmit with UDP protocol , work as a DTU which has application protocol and hear beat mechanism.

Pure UDP: Data transmit with standard UDP protocol.

TCP(DTU): Data transmit with TCP protocol , work as a DTU which has application protocol and hear beat mechanism.

Pure TCP: Data transmit with standard TCP protocol, router is the client.

TCP Server: Data transmit with standard TCP protocol, router is the server.

Modbus TCP Server: MODBUS TCP and MODBUS RTU conversion.

TCST: Data transmit with TCP protocol, Using a custom data.

Server Address: The data service center's IP Address or domain name.

Server Port: The data service center's listening port.

Device ID: The router's identity ID.

Device Number: The router's phone number.

Heartbeat Interval: The time interval to send heart beat packet. This item is valid only when you choose UDP(DTU) or TCP(DTU) protocol type.

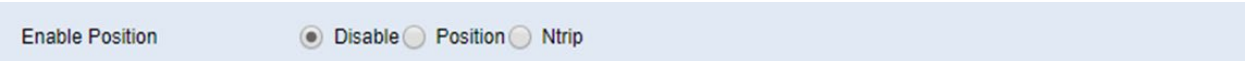
TCP Server Listen Port: This item is valid when Protocol Type is "TCP Server".

Custom Heartbeat Packet : This item is valid when Protocol Type is "TCST".

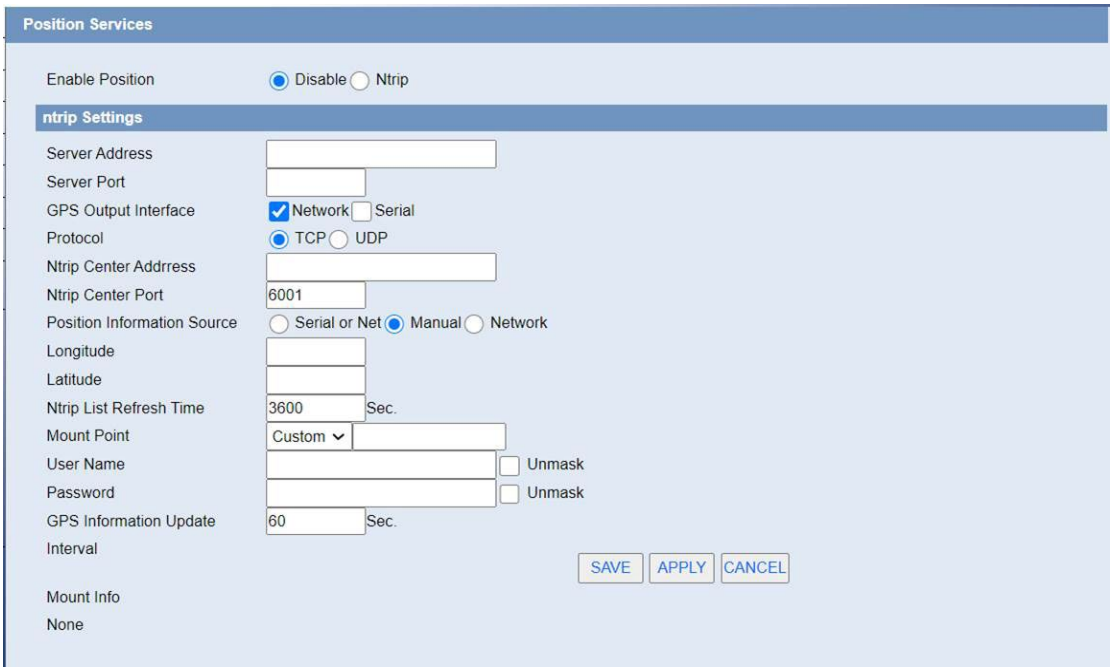
Custom Registration Packets: This item is valid when Protocol Type is "TCST".

10.2 Position

This menu is only valid for GPS versions.



Configure the output port to output positioning data or differential data.



GPS Output Interface: Choose the way of data output

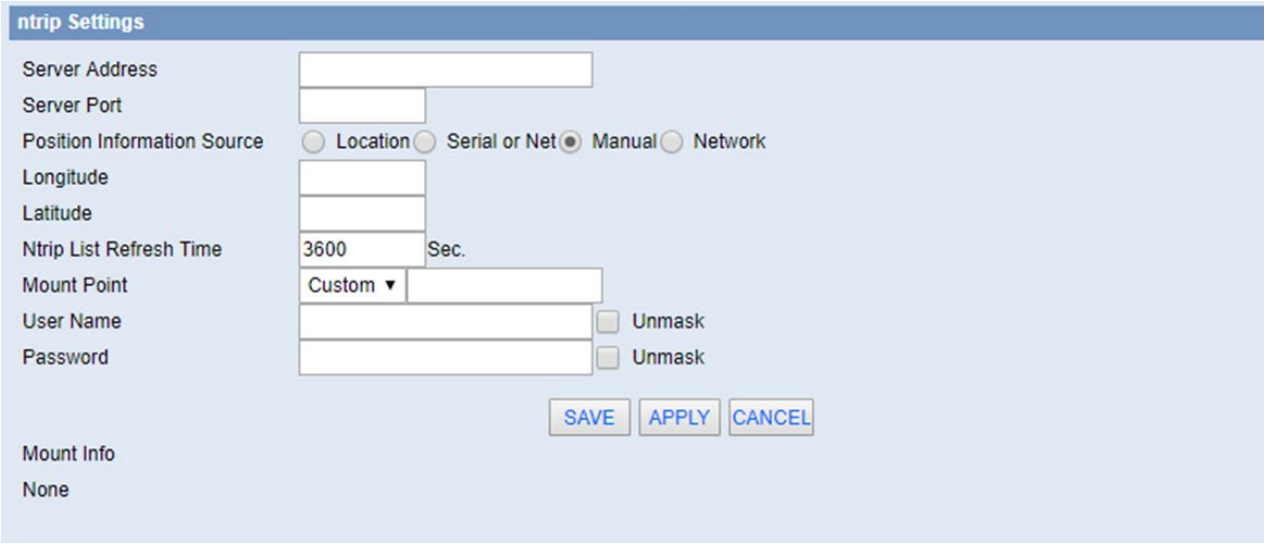
Protocol, GPS Center Address, GPS Center Port: Network Output Configuration

GPS Information Contents: After checking, the output location information will contain the corresponding type data.

ID of device: Users can customize it to identify which device it is.

GPS Information Update: Time interval of data output.

Baudrate, Databit, Stopbit, Parity, Flow Control: Serial port output configuration.



Server Address,Server Port: IP and Port Number of Ntrip Service Provider

Position Information Source: In automatic mode, GGA information is read regularly from GPS module. Serial port, get GGA data from serial port.Manually, pack the latitude and longitude set below into GGA data format. Network, Getting GGA Data from Network

Ntrip List Refresh Time: Seeing the name of a thing one thinks of its function

Mount Point: The name of the mountpoint provided by the Ntrip service provider

User Name: The account provided by Ntrip service provider

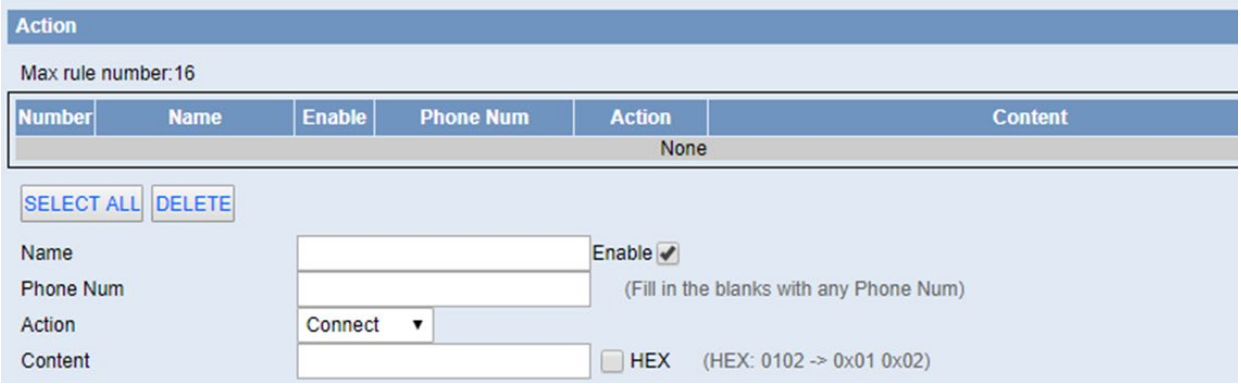
Password: Ntrip Service Provides Account Password

Mount Info: All mountable point information provided by the operator will be displayed in this column.

10.3 SMS Control

For more detailed information about SMS control please refer to the application note AN5 “MTX-Router-EOS management via SMS”.

SMS center: Used to forward received information.



Name: Name of control brake operation.

Phone Num: Designate to receive the mobile phone number control, if it is empty, receive any mobile phone number control.

Action: Includes connecting, disconnecting, restarting the router and configuring the router.

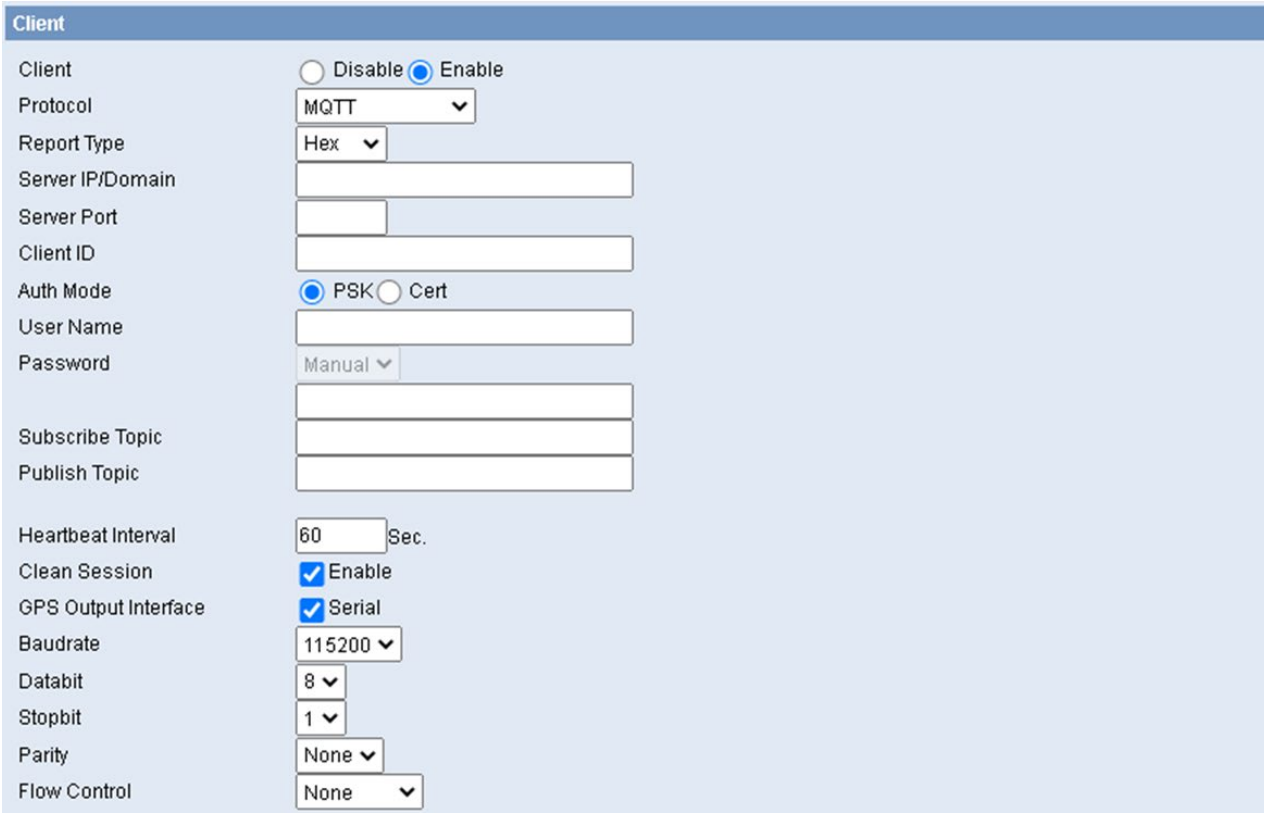
Content: Receiving the short message of the content, the corresponding operation will be performed.

10.4 MQTT

To configure MQTT in MTX-Router EOS please refer to the application notes of our website AN3 “MTX-Router EOS management from Cervello Stem” and AN4 “MQTT connection to Cervello Stem”.

MQTT is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth.

Client



Protocol, Support protocols: MQTT/Ali/Huawei/ONENET/CTWing

Report Type:Support Hex/String

Server IP/Domain: Server IP/Domain

Server Port: Server listen port

Client ID: Connection requires a unique client ID

Auth Mode: Support PSK/CERT

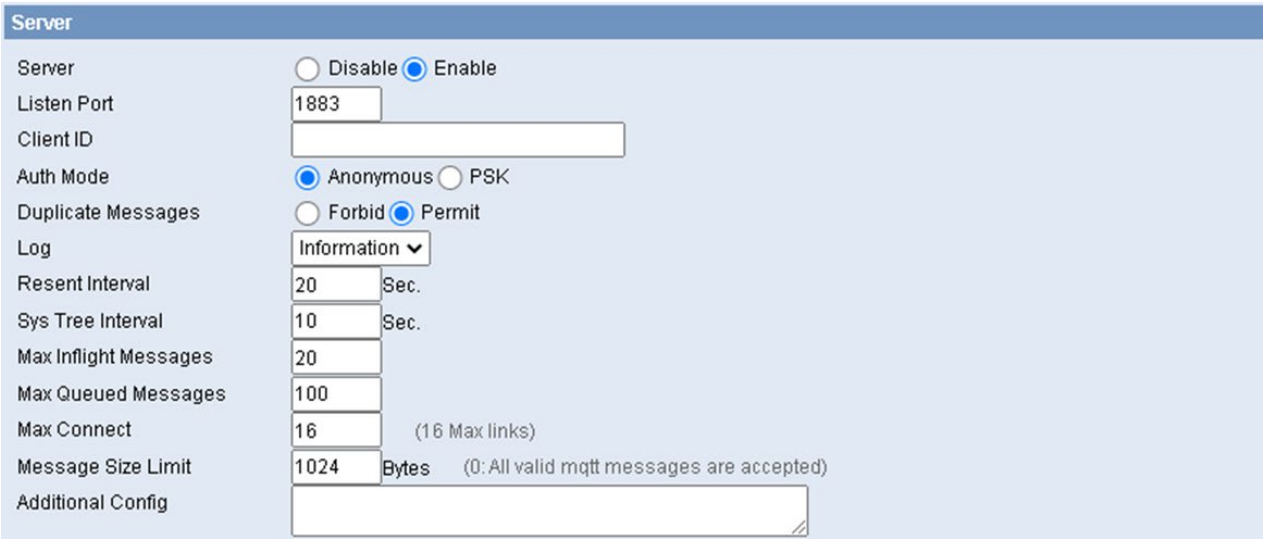
User Name: MQTT name

Password: MQTT password

Subscribe Topic/Publish Topic: MQTT topic

Clean Session: Clean messages posted during disconnection

Server



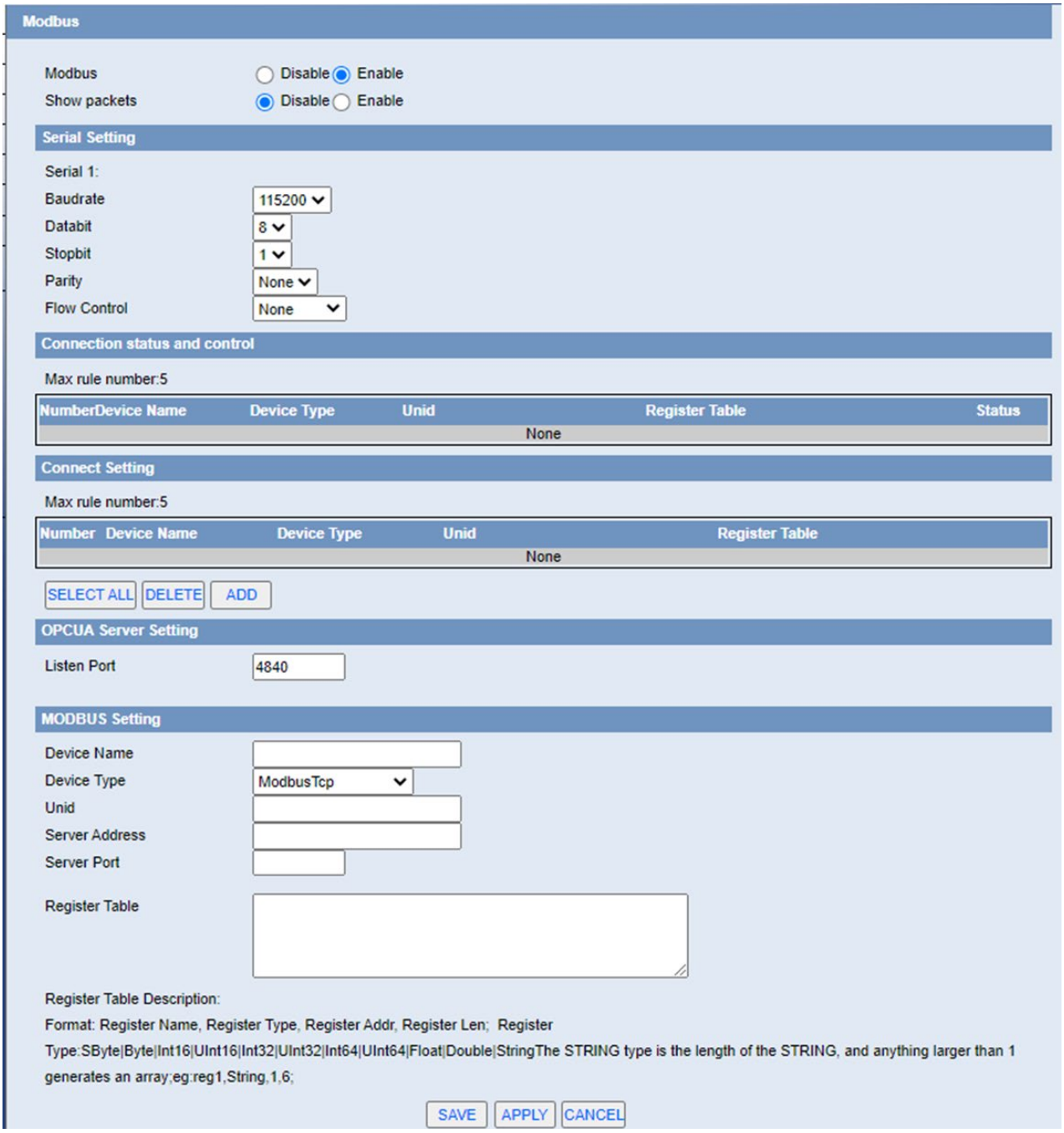
Listen Port: Server listen port

Client ID: Connection requires a unique client ID

Auth Mode: Support PSK/CERT

Duplicate Messages: Whether to receive duplicate messages

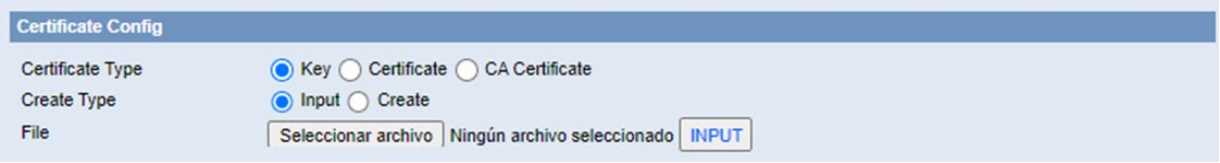
10.5 Modbus


Modbus
Modbus
Disable
Enable
Show packets
Disable
Enable
Serial Setting
Serial 1:
Baudrate
115200
Databit
8
Stopbit
1
Parity
None
Flow Control
None
Connection status and control
Max rule number:5
NumberDevice Name
Device Type
Unid
Register Table
Status
None
Connect Setting
Max rule number:5
Number
Device Name
Device Type
Unid
Register Table
None
SELECT ALL
DELETE
ADD
OPCUA Server Setting
Listen Port
4840
MODBUS Setting
Device Name
Device Type
ModbusTcp
Unid
Server Address
Server Port
Register Table
Register Table Description:
Format: Register Name, Register Type, Register Addr, Register Len; Register Type:SByte|Byte|Int16|UInt16|Int32|UInt32|Int64|UInt64|Float|Double|StringThe STRING type is the length of the STRING, and anything larger than 1 generates an array;eg:reg1,String,1,6;
SAVE
APPLY
CANCEL

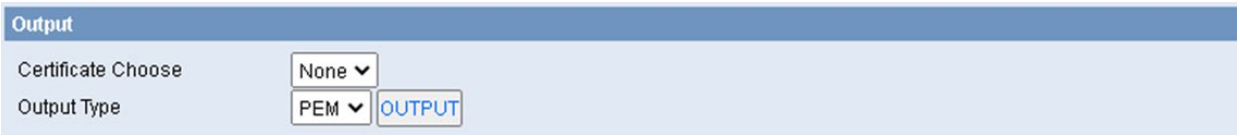
11. Administration

11.1 Certificate

Unified management of device certificates, such as http certificates, mqtt certificates, ipsec certificates, and openvpn certificates.



Certificate import: Users can import externally certificates



Certificate create: Users can create certificates on the device

Certificate Request: Export the certificate request file based on the existing certificate.

11.2 Password

Set the user name and password, to support the input of 32 characters.

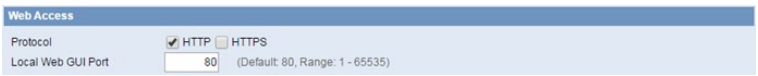
The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.

NOTE: Default username is admin.

It is strongly recommended that you change the factory default password of the router, which is admin. All users who try to access the router's web-based utility or Setup Wizard will be prompted for the router's password.

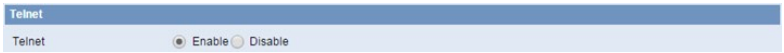
11.3 Management

Configure WEB server parameters.



Protocol: This feature allows you to manage the router using either HTTP protocol or the HTTPS protocol.

Local Web GUI port: Set the access port of the WEB server. For example, when the gateway address is 192.168.1.1 and set the server port 1010, you will enter the address bar in the http://192.168.1.1:1010 to access the WEB configuration page. The default port for the server is 80.



Telnet: Enable or disable Telnet server.

SSH TCP Forwarding: Enable or disable to support the TCP forwarding.

Password Login: Allows login with the router password (username is admin).

Port: port number for SSHd (default is 22).

Authorized Keys: Here users paste their public keys to enable key-based login (more secure than a simple password).

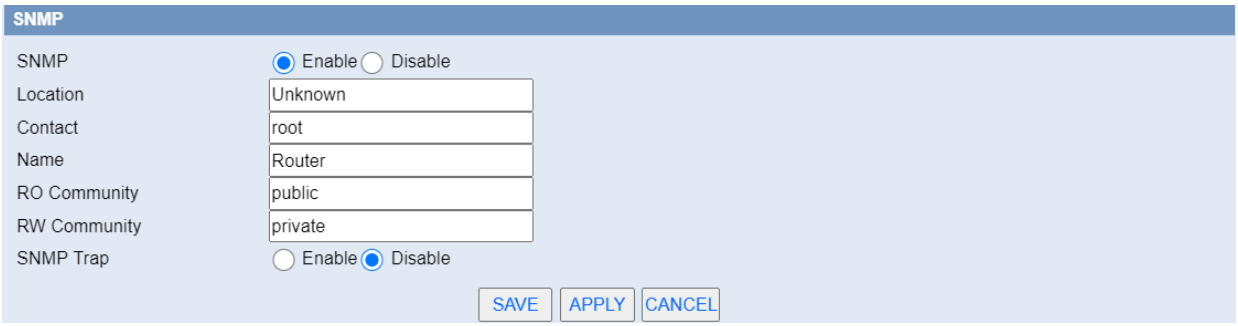
Remote Access: This feature allows you to manage the router from a remote location, via the Internet. To disable this feature, keep the default setting, Disable. To enable this feature, select Enable, and use the specified port (default is 8080) on your PC to remotely manage the router. You must also change the router's default password, if you haven't . To remotely manage the router, enter http://xxx.xxx.xxx.xxx:8080 (the x's represent the router's Internet IP address, and 8080 represents the specified port) in web browser's address field. You will be asked for the router's password.

If use https, need to specify the url as https://xxx.xxx.xxx.xxx:8080 (not all firmwares does support this without rebuilding with SSL support).

SSH Management: Enable SSH to remotely access the router by Secure Shell.

Telnet Management: Enable SSH to remotely access the router.

NOTE: If the Remote Router Access feature is enabled, anyone who knows the router's Internet IP address and password will be able to alter the router's settings.



Location: Equipment location.

Contact: Contact this equipment management.

Name: Device name.

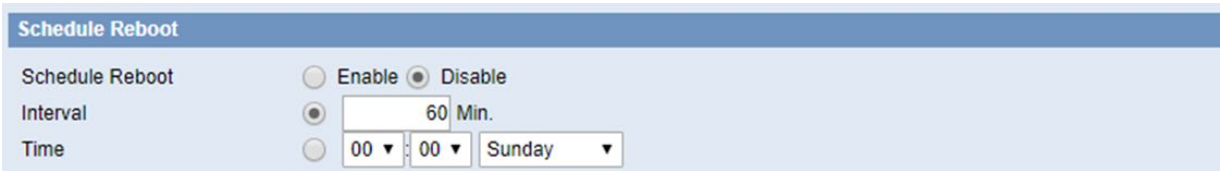
RO Community: SNMP RO community name, the default is public, Only to read.

RW Community: SNMP RW community name, the default is private, Read-write permissions.

11.4 Reboot

Reboot The upper right corner of the page provides the language switch button and reset button to set the WEB configuration page.

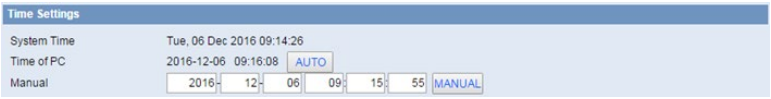
You can also set a schedule reboot:



Timing reboot can be set or router can be restarted immediately.

11.5 System Time

Select time zone of your location. To use local time, leave the check mark in the box next to Use local time.



To adjust time by the system and refresh to get the time of the web, user can set to modify the time of the system. They can change to adjust time by manual to achieve adjust time by the system if the system fails to get NTP server.

NTP Client: Get the system time from NTP server.

Time Zone: Time zone options.

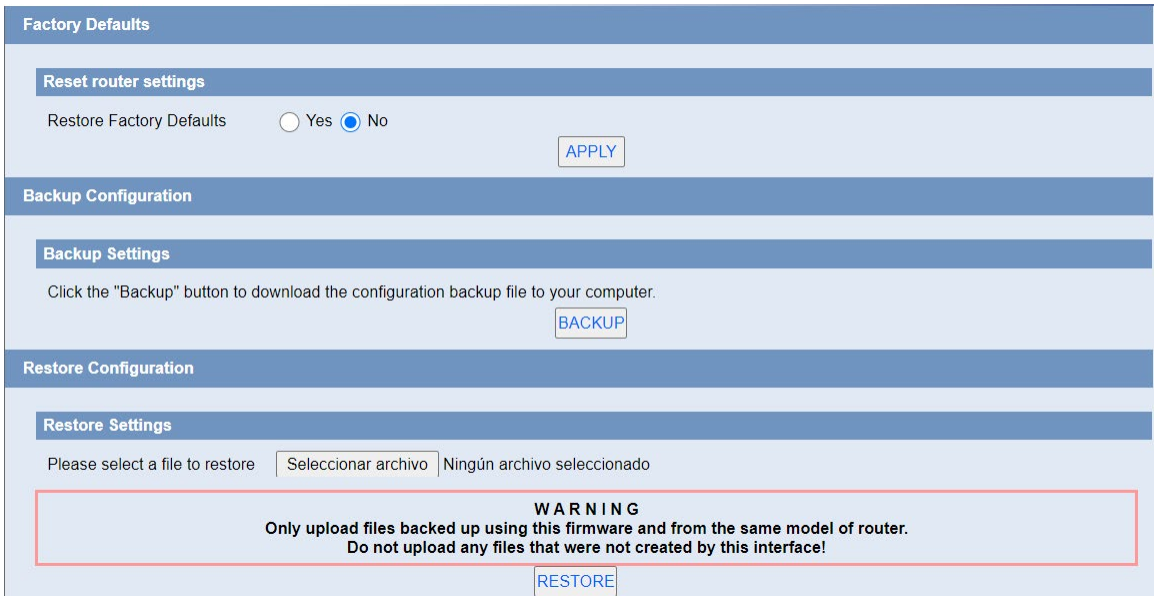
Summer Time (DST): Set it depends on users' location.

Server IP/Name: IP address of NTP server, up to 32 characters. If blank, the system will find a server by default.

11.6 Configure

Reset router settings: Click the Yes button to reset all configuration settings to their default values. Then click the Apply Settings button.

NOTE: Any settings you have saved will be lost when the default settings are restored. After restoring the router is accessible under the default IP address 192.168.1.1 and the default password admin.



Backup Settings: You may backup your current configuration in case you need to reset the router back to its factory default settings.Click the Backup button to backup your current configuration.

Restore Settings: Click the Browse button to browse for a configuration file that is currently saved on your PC.Click the Restore button to overwrite all current configurations with the ones in the configuration file.

NOTE: Only restore configurations with files backed up using the same firmware and the same model of router.

11.7 Upgrade

Update software to get new features.

Firmware Upgrade: Contact us for New firmware versions. If the Router is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

NOTE: When you upgrade the Router's firmware, you lose its configuration settings, so make sure you

write down the Router settings before you upgrade its firmware.

To upgrade the Router's firmware:

- Download the firmware upgrade file.
- Click the Browse... button and chose the firmware upgrade file.
- Click the Upgrade button and wait until the upgrade is finished.

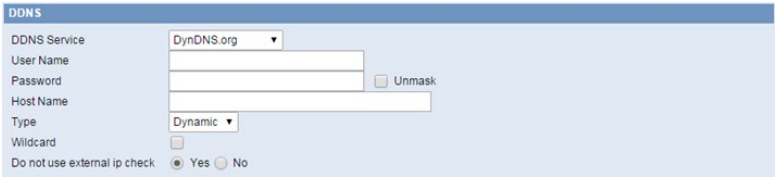
NOTE: Upgrading firmware may take a few minutes.

Do not turn off the power or press the reset button!

After flashing, reset to default: If you want to reset the router to the default settings for the firmware version you are upgrading to, click the YES option.

11.8 DDNS

If user's network has a permanently assigned IP address, users can register a domain name and have that name linked with their IP address by public Domain Name Servers (DNS). However, if their Internet account uses a dynamically assigned IP address, users will not know in advance what their IP address will be, and the address can change frequently. In this case, users can use a commercial dynamic DNS service, which allows them to register their domain to their IP address, and will forward traffic directed at their domain to their frequently-changing IP address.



User Name: Users register in DDNS server, up to 64 characteristic.

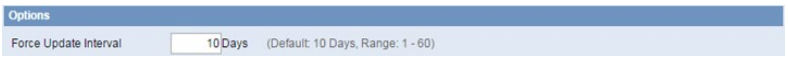
Password: Password for the user name that users register in DDNS server, up to 32 characteristic.

Host Name: Users register in DDNS server, no limited for input characteristic for now.

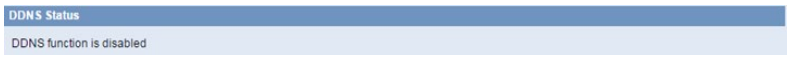
Type: Depends on the server.

Wildcard: Support wildcard or not, the default is OFF. ON means *.host.3322.org is equal to host.3322.org.

Do not use external ip check: Enable or disable the function of 'do not use external ip check.



Force Update Interval: Unit is day, try forcing the update dynamic DNS to the server by settled days.



DDNS Status shows connection log information.

11.9 Syslog

Enable Syslog to capture system messages. To send them to another system, enter the IP address of a remote syslog server.

Syslog Out Mode: 3 mode options.

Net: The log information output to a syslog server.

Console: The log information output to console port. (The log from the console is the most detailed, so if need to debug, could run serial port software to read and save the log).

Web: The log information output to local web page.

Remote Server: If choose net mode, users should input a syslog server's IP Address and run a syslog server program on it.

11.10 NetTest

Test the connection status with other IP or domain names.

Offices & Support Contact

SPAIN

C/ Alejandro Sánchez 109
28019 Madrid

Phone: +34.915602737
Email: contact@webdyn.com

FRANCE

26 Rue des Gaudines
78100 Saint-Germain-en-Laye

Phone: +33.139042940
Email: contact@webdyn.com

INDIA

803-804 8th floor, Vishwadeep Building
District Centre, Janakpurt, 110058 Delhi

Phone: +91.1141519011
Email: contact@webdyn.com

PORTUGAL

Av. Coronel Eduardo Galhardo 7-1ºC
1170-105 Lisbon

Phone: +351.218162625
Email: comercial@lusomatrix.pt

TAIWAN

5F, No. 4, Sec. 3 Yanping N. Rd.
Datong Dist. Taipei City, 103027

Phone: +886.965333367
Email: contact@webdyn.com

SUPPORT

Madrid Offices

Phone: +34.915602737
Email: iotsupport@mtxm2m.com

Saint-Germain-en-Laye Offices

Phone: +33.139042940
Email: support@webdyn.com

Delhi Offices

Phone: +91.1141519011
Email: support-india@webdyn.com

Taipei City Offices

Phone: +886.905655535
Email: iotsupport@mtxm2m.com