RELIABLE SECURE CONNECTIVITY

XWR3400G

User Guide

Copyright Notice

All contents in the files are protected by copyright law, and all copyrights are reserved byAgatel Ltd.. Without written permission, all commercial use of the files from Agatel Ltd. are forbidden, such as copy, distribute, reproduce the files, etc., but non-commercial purpose, downloaded or printed by individual (all files shall be not revised, and the copyright and other proprietorship notice shall be reserved) are welcome.



Note: There may be different components and interfaces in different model, please in kind prevail.

Contents

Chapter 1 Brief Introduction of Product 7
1.1 General 7
1.2 Working Principle 8
Chapter 2 Installation Introduction 9
2.1 General 9
2.2 Encasement List 9
2.3 Installation and Cable Connection 9
2.4 Power 14
2.5 Indicator Lights Introduction 14
2.6 Reset Button Introduction 15
Chapter 3 Configuration and Management 16
3.1 Configuration Connection 16
3.2 Login the Router Web GUI 16
3.2.1 Configure the PC IP address(There are two ways) 16
3.2.2 Login the router Web GUI 18
3.3 Management and Configuration 19
3.3.1 Network 19
3.3.1.1 Internet Setting 19
3.3.1.2 LAN Setting 24
3.3.1.3 Wireless Setting 25
3.3.2 Firewall 27
3.3.2.1 Port Forwarding 28
3.3.2.2 DMZ 28
3.3.2.3 URL Filter 29
3.3.4 VPN 29
3.3.4.1 L2TP 29
3.3.4.2 PPTP 31
3.3.4.3 GRE 32
3.3.4.4 IPsec 34
3.3.4.5 OpenVPN 38
3.3.5 Advanced 39
3.3.5.1 FTP Server 39
3.3.5.2 Dynamic DNS 39
3.3.5.3 QoS Setting 40
3.3.5.4 Remote Management Settings 41
3.3.5.5 SNMP 42
3.3.5.6 Static Routes 44
3.3.5.7 GPS Setting 45
3.3.5.8 Serial Setting 46
3.3.6 Management 47

3.3.6.1 Admin Password....47
3.3.6.2 System Log Setting....48
3.3.6.3 Backup/Restore....49
3.3.6.4 Flash Firmware....49
3.3.6.5 Sys Log....50
3.3.6.6 Attached Setting....50
3.3.6.7 Time Setting....51
3.3.6.8 Reboot....52
3.3.6.9 Logout....52
3.3.7 Appendix....52

Chapter 1 Brief Introduction of Product

1.1 General

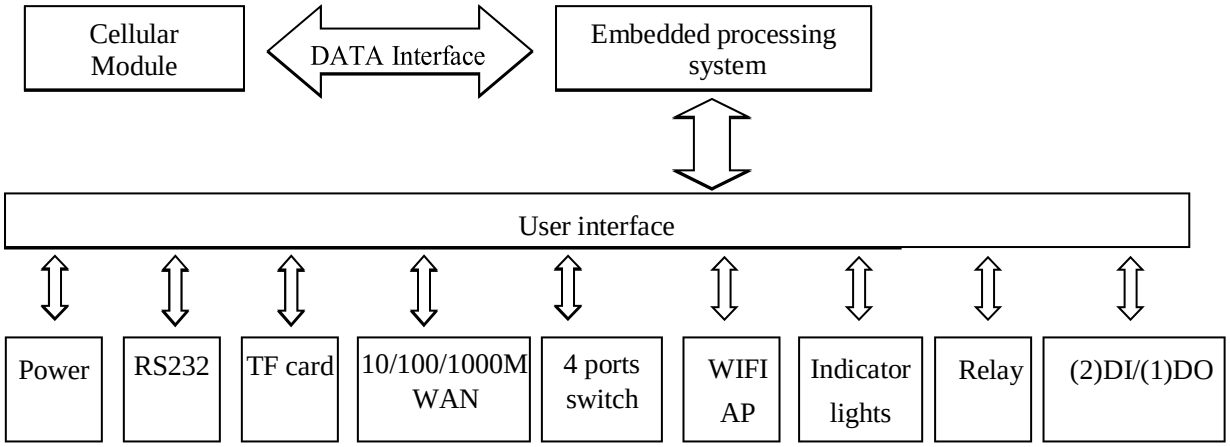
Agatel Ltd. Industrial Router XWR3400Gis an intelligent 3G/4G routers to provide the necessary M2M applications for all types of terminals.

It adopts high-powered industrial 32-bits CPU and embedded real time operating system. It supports RS232 (or RS485/RS422), Ethernet and WIFI port that can conveniently and transparently connect one device to a cellular network, allowing you to connect to your existing serial, Ethernet and WIFI devices with only basic configuration.

It has been widely used on M2M fields, such as self-service terminal industry, intelligent transportation, smart grid, smart home, industrial automation, intelligent building, public security, fire protection, environment protection, telemetry, finance, POS, water supply, meteorology, remote sensing, digital medical, military, space exploration, agriculture, forestry, petrochemicaland other fields etc..

1.2 Working Principle

The principle chart of the router is as following:



Chapter 2 Installation Introduction

2.1 General

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

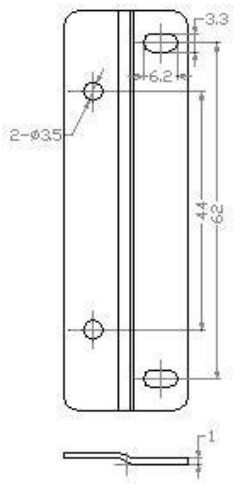
Warning: Forbid to install the router when powered!

2.2 Encasement List

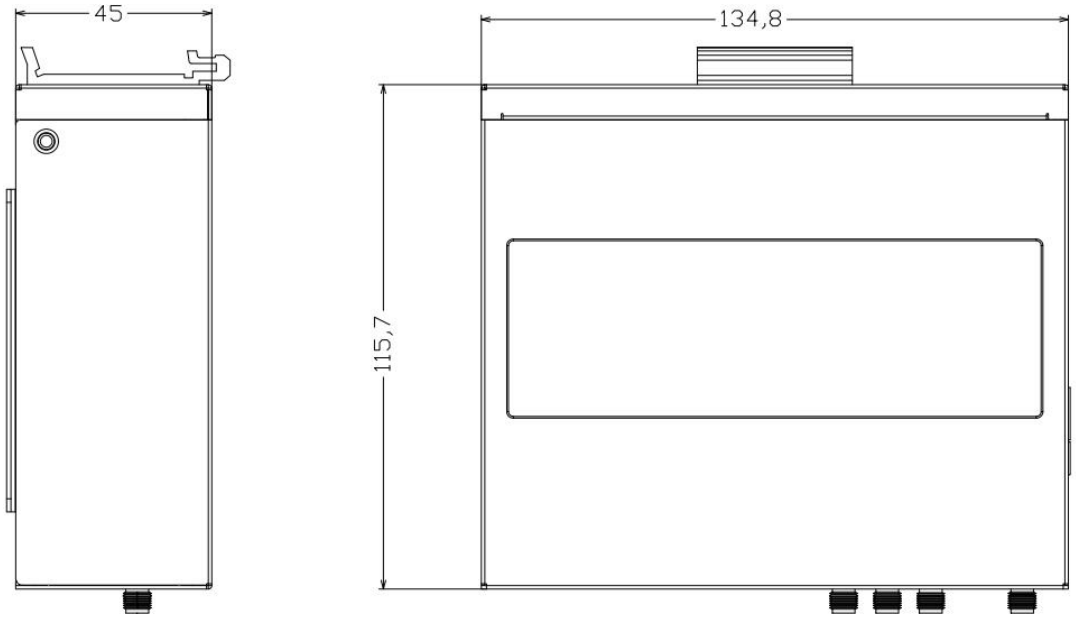
Name	Quantity	Remark
Router host	1	
Cellular antenna (Male SMA)	2	
WIFI Dual band antenna (Female SMA)	1	
GPS antenna(Male SMA)	1	optional
Network cable	1	
Console cable	1	
RS485 Console cable	1	optional
3PIN Terminal Block	2	
2PIN Terminal Block	1	
Power adapter	1	
Manual CD	1	
Certification card	1	
Maintenance card	1	

2.3 Installation and Cable Connection

Stator and routing equipment of screw specification for: M3 * 5 mm countersunk head screws(black)（optional）



Fixed Size



Router Size

Installation of SIM/UIM card:

1、Firstly power off the router

2、Unscrewed the screw

3、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

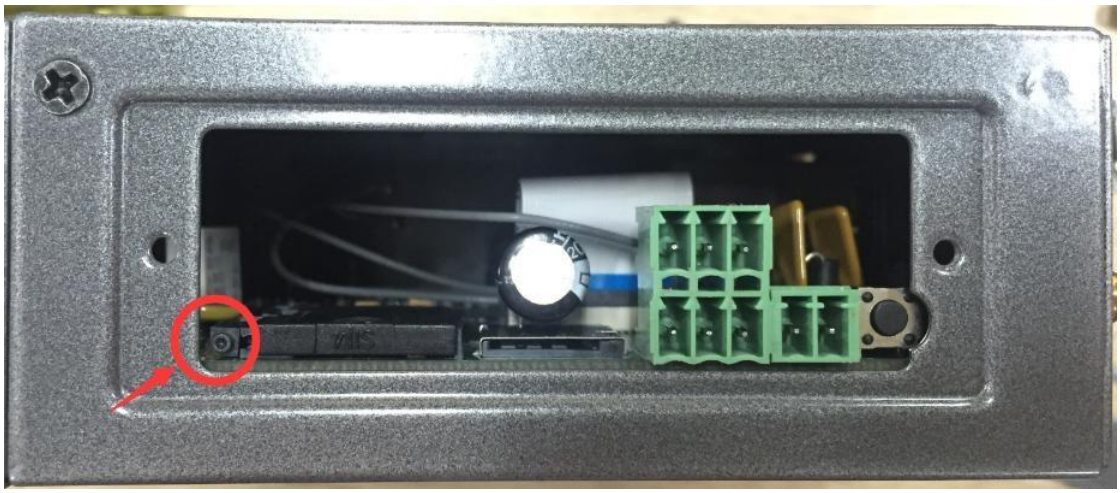
4、Put SIM/UIM card into the card sheath (Pay attention to put the side which has metal point outside), and insert card sheath back to the SIM/UIM card outlet.

5、Screwed the screw

Warning: Forbid to install SIM/UIM card when powered!



Step 2



Step 3



Step 4



Step 5

Installation of antenna:

Screw the SMA male pin of the cellular antenna to the female SMA interface of the Router with sign “ANT-1” and “ANT-2”.

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

Screw the SMA female pin of the GPS antenna to the female SMA interface of the router with sign “GPS”.(optional)

Warning: The cellular antenna and the WIFI antenna can not be connected wrongly. And the antennas must be screwed tightly, or the signal quality of antenna will be influenced!

Installation of cable:

Insert one end of the network cable into the switch interface with sign“LAN1/LAN2/LAN3/ LAN4”, and insert 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	Color
1	1	White/Orange
2	2	Orange
3	3	White/Green
4	4	Blue
5	5	White/Blue
6	6	Green
7	7	White/Brown
8	8	Brown

Insert the RJ45 end of the console cable into the RJ45 outlet with sign “console”, and insert the DB9F end of the console cable into the RS232 serial interface of user’s device.

The signal connection of the console cable is as follows:

Console line definition (RS232)					
RJ45	Color	Signal	DB9F	Description	Dir (Router
1	White/ Orange	A	8	RS485-A	Input/Output
2	Orange	B	6	RS485-B	Input/Output
3	White/ Green	RXD	2	Receive Data	Output
4	Blue	DCD	1	Data Carrier Detect	Output
5	White/ Blue	GND	5	System Ground	
6	Green	TXD	3	Transmit Data	Input
7	White/ Brown	DTR	4	Data Terminal Ready	Input
8	Brown	RTS	7	Request To Send	Input



2.4 Power

The power range of the router is DC 5~36V.

Warning: When we use other power, we should make sure that the power can supply power above 8W.

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

2.5 Indicator Lights Introduction

The router provides following indicator lights: “PWR”, “SYS”, “Online”, “SIM”, “LAN”, “WAN”, “WIFI”, “Signal Strength”.

Indicator Light	State	Introduction
PWR	ON	Router is powered on
	OFF	Router is powered off
SYS	BLINK	System works properly
	OFF	System does not work
Online	ON	Router has logged on network
	OFF	Router hasn’t logged on network
SIM	ON	The SIM card has been identified
	OFF	The SIM card is not recognized
LAN	OFF	The corresponding interface of switch is not connected
	ON / BLINK	The corresponding interface of switch is connected /Communicating
WAN	OFF	The interface of WAN is not connected

	ON / BLINK	The interface of WAN is connected /Communicating
WIFI	OFF	WIFI is not active
	ON	WIFI is active
Signal Strength	One Light ON	Signal strength is weak
	Two Lights ON	Signal strength is medium
	Three Lights ON	Signal strength is good

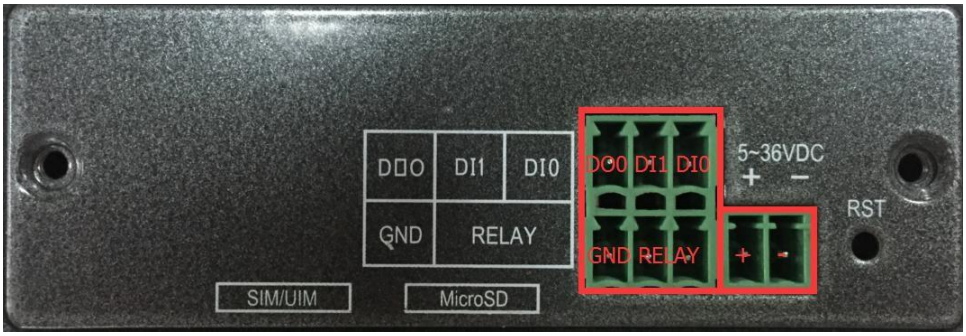
2.6 Reset Button Introduction

The router has a “RST” button to restore it to its original factory default settings. When user press the “Reset” button for up to 10s, the router will restore to its original factory default settings and restart automatically.

2.7 Flank Interface

Flank Interface as picture below,The router provides 2 Direct Input,1 Direct Output,1 Relay control .

DI	Input ON	5 to 30 VDC
	Input OFF	0 to 3 VDC
DO	Output	< 50mA @ 30VDC
RELAY	Load capability	1A 250VAC/30VDC



Chapter 3 Configuration and Management

This chapter describes that how to configure and manage the router.

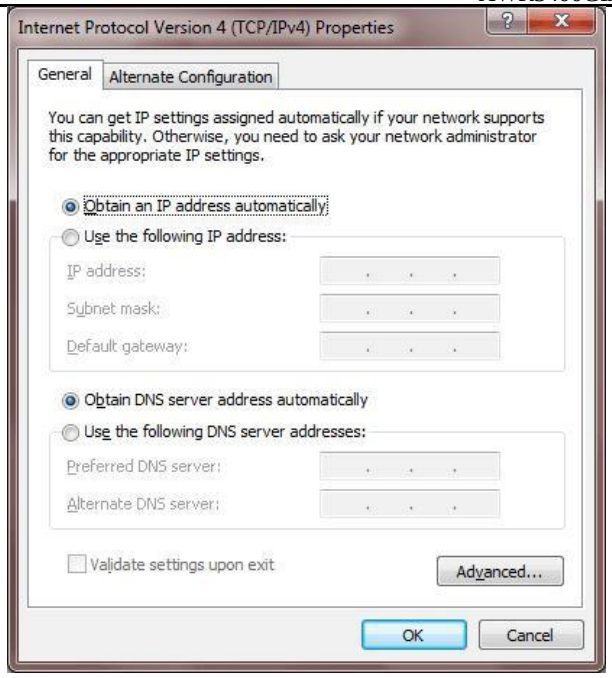
3.1 Configuration Connection

Before configuration, you should connect the router to the PC by the provided Ethernet cable or WIFI to configure the router. Connect one side of the Ethernet cable to the router LAN port, and the other side to PC ETH port. If you connect by WIFI, connect to SSID “AGATEL LTD._XXXX”(XXXX stands for the last four letters of the default Wireless MAC address in the router) without password.

3.2 Login the Router Web GUI

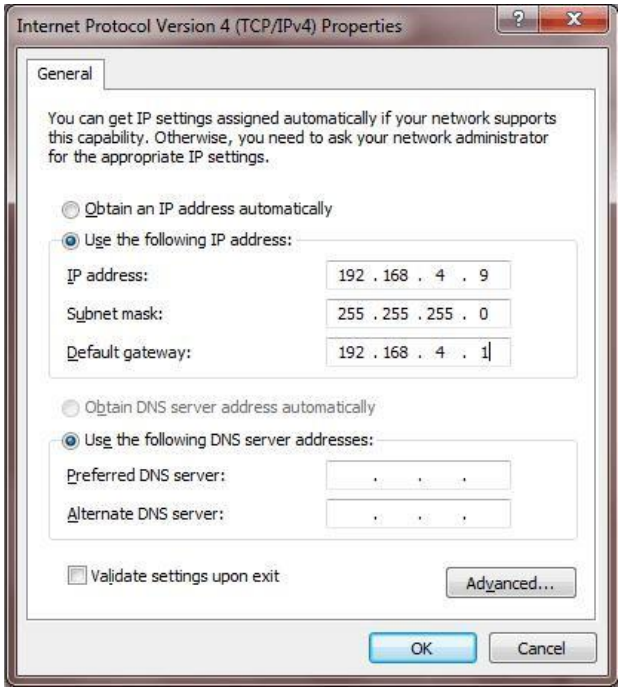
3.2.1 Configure the PC IP address(There are two ways)

(1) Obtain an IP address automatically



(2) Use a given IP address

Configure the PC IP address as 192.168.4.9 (or other IP address in the same subnet), subnet mask as 255.255.255.0 and default gateway as 192.168.4.1. Configure the DNS server as the local DNS server.



3.2.2 Login the router Web GUI

The main functions of each menu are described in this chapter. You can access to the router Web GUI through the web browser on the PC. Main menus are as below: Status, Network, Firewall, VPN Setting, Advanced Setting and Management. Click the main menu and you will see the sub menu.



Start IE explorer or other web browser, input the router default IP address 192.168.4.1:90 and press the enter button to access router login Web GUI. You will get the following prompt box to remind you to enter the router default login username and password when you access the Web GUI for the first time.

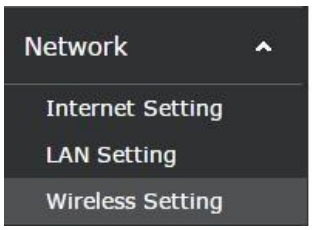
Then you will enter the Status page.



3.3 Management and Configuration

3.3.1 Network

The first sub menu in “Network” menu is “Internet Setting”, And you can change the Internet setting according to the instructions. Click “Save & Apply” button and the changes will take effect. Click “Save” button to save the settings but the changes don’t take effect. Click “Reset” button to cancel changes.



3.3.1.1 Internet Setting

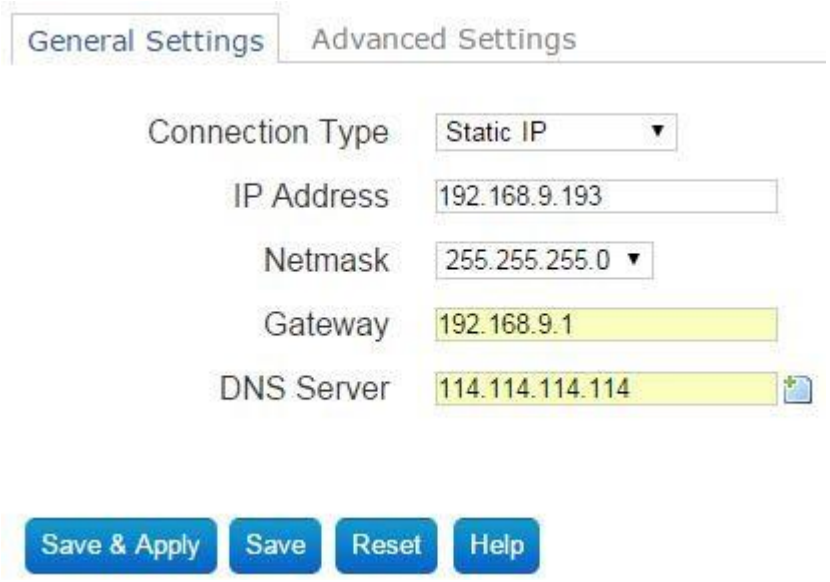
Configure “WAN Connection type” to make the router connect to the Internet. And you can get the parameters from the ISP.

WAN Connection Type:

Select the corresponding Internet connection type which is provided. WAN connection type includes Static IP, DHCP, PPPoE, 3G connection and LTE connection.

Mode One: Static IP

Use this mode if you subscribe optical network or other wired network and configure the IP address, netmask, gateway, DNS server provided by the ISP.

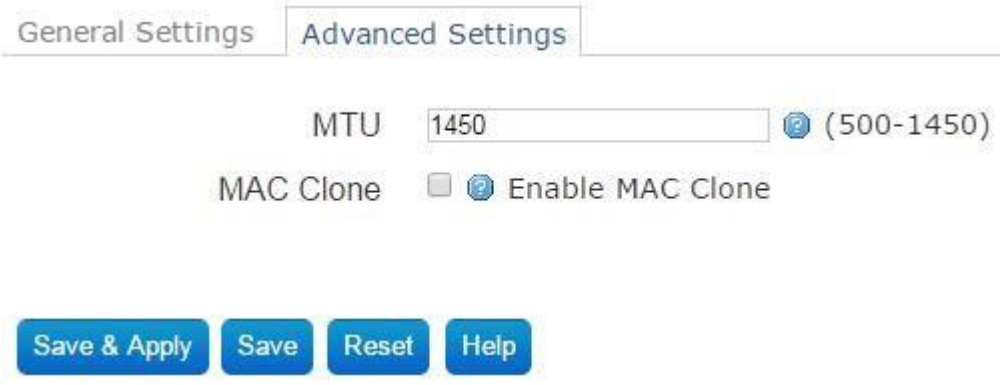


IP Address: IP address assigned by the ISP or one you set by your own

Netmask: Netmask assigned by the ISP or one you set by your own

Gateway: Gateway assigned by the ISP or one you set by your own

DNS Server: IP address assigned by the ISP or one you set by your own. Click "+" button to add more.

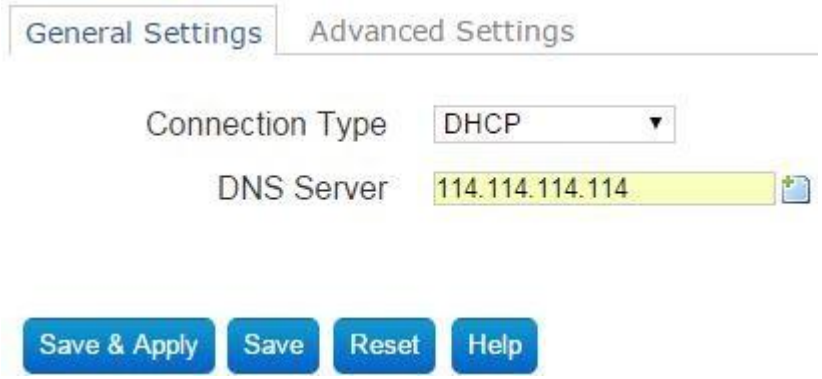


MTU: Set the appropriate MTU value to make full use of internet throughout.

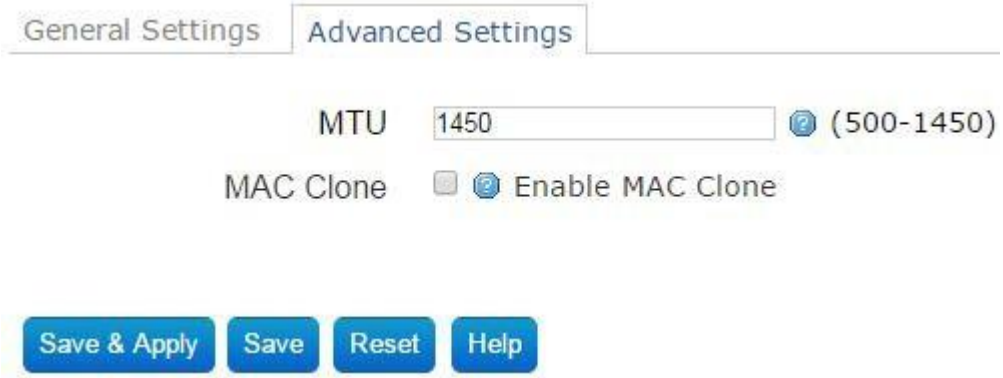
MAC Clone: The selection enable MAC Clone.

Mode Two: DHCP

DHCP is the default WAN connection type.



Router obtains the WAN IP address by DHCP and you can set the static DNS server.

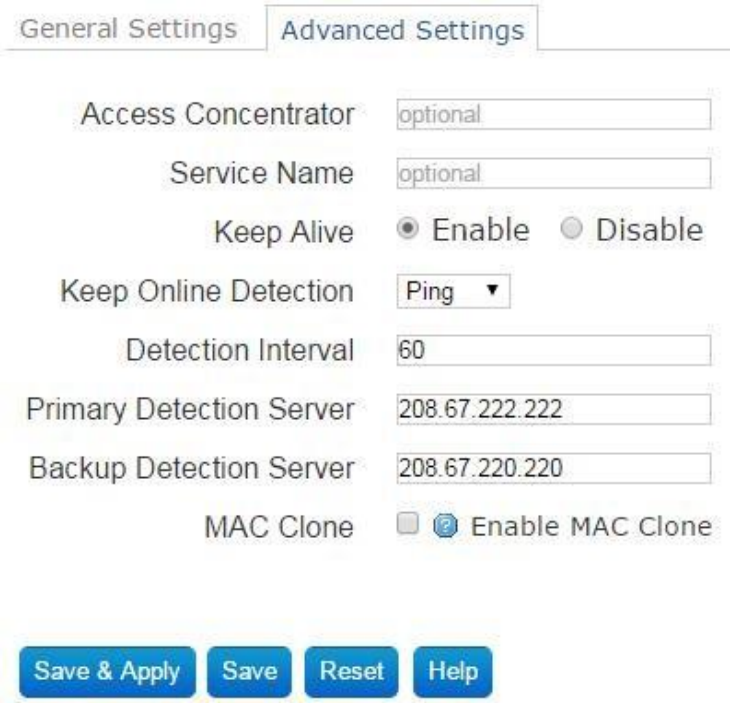


The advanced setting of this mode is the same with static IP mode

Mode Three: PPPOE

Use this mode if you subscribe ADSL broadband service. Configure username and password provided by the ISP.

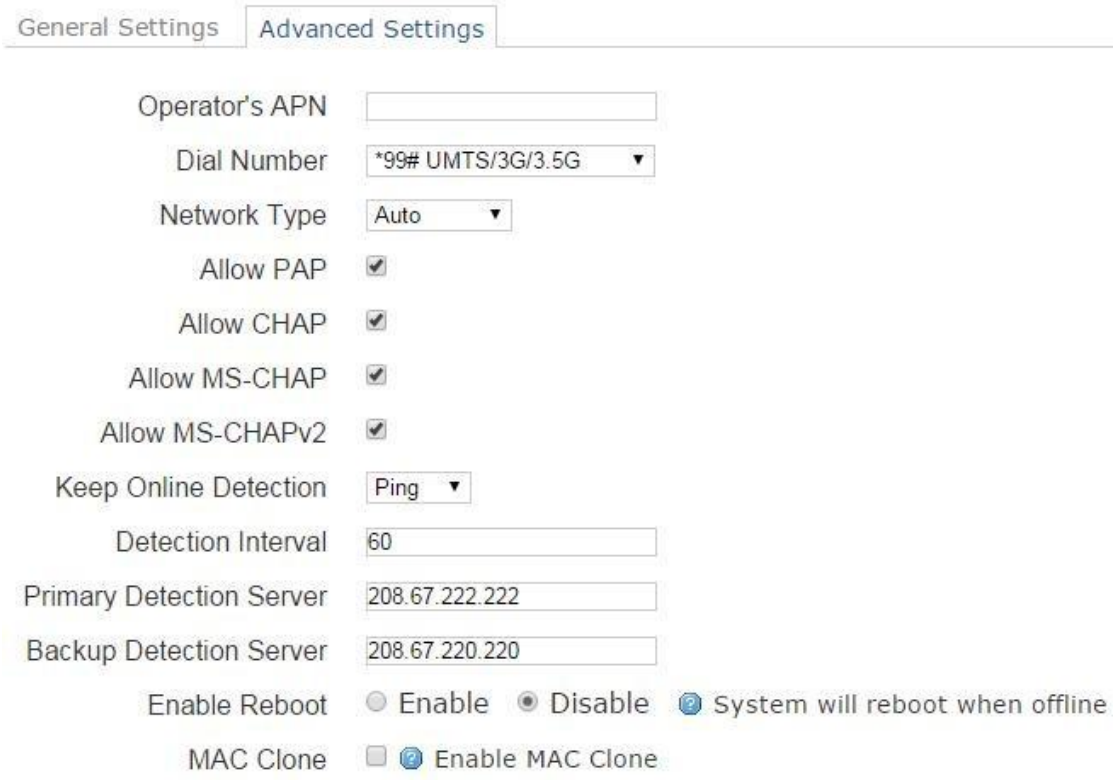




Access Concentrator and Server Name, are optional. The other options will be explained below.

Mode Four: 3G Connection





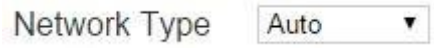
User Name: login the Internet

Password: login the Internet

Dial Number: dial number of users' ISP

Operator's APN: access point name of users' ISP

Network Type:



Network type includes Auto, Force 3G, Force 2G, Prefer 3G, Prefer 2G, 3G/2G, Force 4G and 4G/3G/2G.

Keep Online Detection



This function is used to detect whether the Internet connection is active. if users set it, router will detect the Internet connection automatically. The router will redial immediately to make the obtain active connection When it detects the connection is inactive.

Keep Online Connection Type:

None: No online detection

Ping: Send ping packet to detect the connection. when choosing this method, you should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

Route: Detect connection with route method. When choosing this method, you should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

PPP: Detect connection with PPP method. When choosing this method. You should also configure "Detection Interval" item.

Detection Interval:

Time interval between two detection , and unit is second.

Primary Detection Server:

The server used to response to the router's detection packet. This item is only valid for method "Ping" and "Route".

Backup Detection Server:

The backup server used to response to the router's detection packet. This item is only valid for method "Ping" and "Route".

3.3.1.2 LAN Setting

Local Network

Configure the local area network setting



Local Address: The router IP in the local network

Netmask: Netmask assigned by the ISP or one you set by your own

DHCP Server Setting(DHCP)

These functions are used to configure dynamic host configuration protocol server setting. The XWR3400Grouter can be a DHCP server. The DHCP server provides a dynamic IP address for every pc automatically. You can configure all of computers to get IP addresses and DNS automatically while DHCP function of the router is selected, and make sure that there is only one DHCP serverin the network.



DHCP Server: DHCP Sever is enabled by default. If users already have a DHCP server on their network or do not want a DHCP server, select disable. If the DHCP server is enabled, enter the IP address please.

Start IP Address: Enter a numerical value for the DHCP server as the starting IP addresses. Please do not start with 192.168.4.1 (the router's own IP address). The start ip of the network must be great than or equal to 192.168.4.2, but less than 192.168.4.254. The default start IP is 192.168.4.100.

Maximum DHCP Users: Enter the maximum number of the PCs which users want to assign IP addresses to. The absolute maximum is 253 if 192.168.4.2 is users' starting IP address. The default number is 50.

Leasetime: The Leasetime is the amount of time that the dynamic IP address allowed to be used. Enter the leasetime, in minutes, so that the user could "lease" this dynamic IP address. New IP address will be assigned after the leasetime is expired.The default setting is 1440 minutes, which is one day. The configurable value ranges from 0 to 99999.

3.3.1.3 Wireless Setting

Basic Setting



Enable: Enable WIFI

Disable: Disable WIFI

Wireless Mode:

802.11b: Only supports the 802.11b standard wireless devices.

802.11g: Only supports the 802.11g standard wireless devices.

802.11bg: Support 802.11b, 802.11g wireless devices.

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

Channel: There are 13 channels in total, from channel 1 to channel 13. Don't use the same channel with other routers.

Network Name(SSID): The SSID is the network name shared in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters.

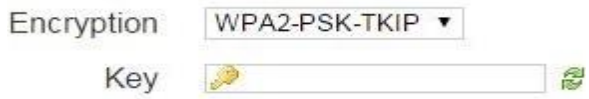
Encryption: The XWR3400Grouter contains 6 security modes in total. Encryption is disabled by default. If the mode is changed, click "Save & Apply" to make it effect immediately.

Hide SSID:

Uncheck: Broadcast SSID

Check: Hide SSID

Configure wireless network security.

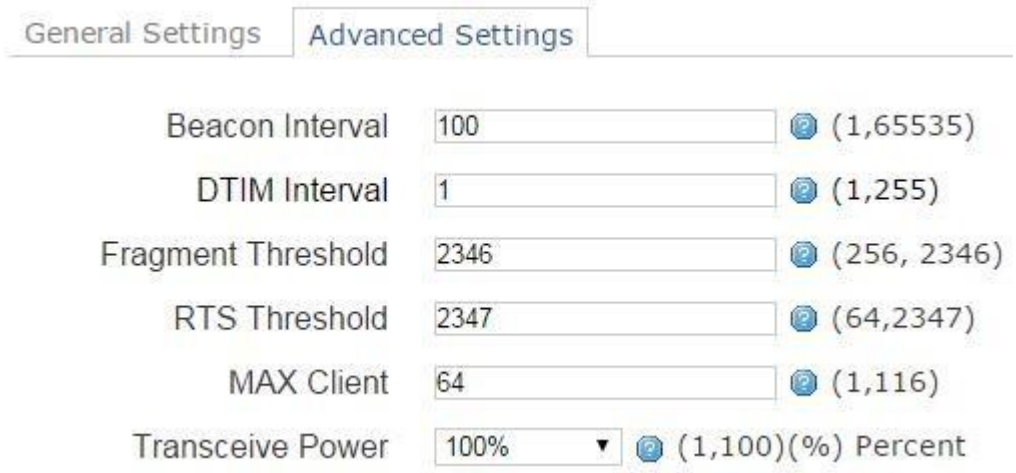


WEP: WEP is a basic encryption algorithm, which is less secure than WPA. Using of WEP is discouraged due to the weaknesses security, and one of the WPA modes should be used whenever possible. Only use WEP if you have clients that can only support WEP (usually older, 802.11b-only clients).

WPA Personal/WPA2 Personal/WPA2 Person Mixed: XWR3400Gprovides 3 types of WPA security protocols,TKIP/AES/TKIP+AES,dynamic encryption keys. TKIP + AES, self-applicable TKIP or AES. WPA Person Mixed, allows WPA Personal and WPA2 Personal client mixed.

Advanced Settings:

Please be careful of these configurations, the router will degrade performance because of the incorrect configuration.



Beacon Interval: The default is 100. You can enter the value ranges from 1 to 65535, in milliseconds.

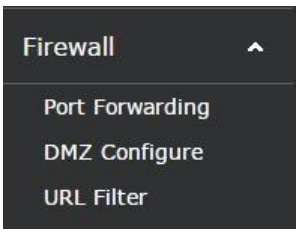
DTIM Interval: Thedefault is 1.it ranges from 1 to 255, which indicates that the interval of message transmission. The DTIM field is counted down. he rooter will inform the customer to get the broadcast and multicast messages, then the latest DTIM and DTIM interval will be sent. The clients will be waked up and get the broadcast and multicast messages from the transmitting stations.

Fragment Threshold: Keep the value 2346 by default, which ranges from 256 to 2346 Bytes. It indicates the maximum amount of data without division. You should increase Fragment Threshold when the higher packet loss rate occurs. The low fragment threshold may lead to the degrade performance. s a result, we advice you not to change fragment threshold.

RTS Threshold: Keep the value 2347 as default setting, which is range from 0 to 2347. A slight modification is allowed if you are in trouble of inconsistent data stream. The RTS/CTS mechanism will not take effect for the amount of network packets is less than preset Threshold. The router sends the RTS frame and data frame to the specific receiving station. After getting the RTS frame, The wireless terminals obtain the specific CTS frame, then transmission is starting.

MAX Client: The maximum number of clients, 1-128.

3.3.2 Firewall



3.3.2.1 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 which use Internet access to perform functions such as video conferencing or online gaming.



Names: Enter the application name in the field.

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

External IP Address: Forward only if sender matches this ip/net (example 192.168.4.0/24).

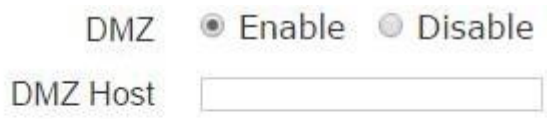
Internal IP Address: Enter the IP Address of the PC which is running the application.

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

Click “Save” or “Save & Apply”to complete modification. Click “Reset” to roll back the changes. The shortcut “Help” locates on the lower right corner of the page, click it for more details.

3.3.2.2 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.





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.

Check all values and click **“Save & Apply”** or “**Save**” to save your settings. Click the “**Reset**” to cancel your changes.

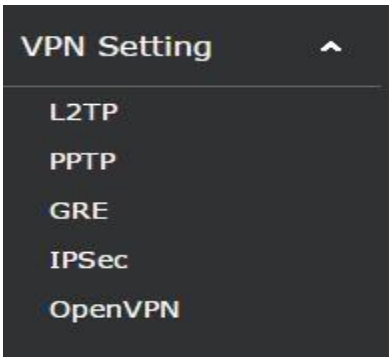
3.3.2.3 URL Filter

It filters some specific domain address. If you visit the domain address, firewall intercept it.



Click “Add” to add more key words.

3.3.4 VPN



3.3.4.1 L2TP

L2TP Server



L2TP Server Local IP: Enter the L2TP Server IP address, make sure that the Sever IP is different from LAN IP address.

Clients IP Address Range: IP addresses assigned to the Clinets, **xxx.xxx.xxx.xxx-xxx**

Enable MPPE Encryption：Use MPPE Force Encryption.

DNS1，**DNS2**，**WINS1**，**WINS2**：Set your first DNS, second DNS, first wins, second wins.

CHAP Secrets：The usernames and passwords of the clients.

NOTE：The Clients IP can't be the same with the IP of DHCP, but outside of the range.

CHAP Secrets format: user blank*blank password blank*

L2TP Clinet



L2TP Server: The IP address of L2TP server

User Name: The user name which is recognized by the server

Password: The password which is corresponding to user name

remote local ip mask: The remote local ip address

remote local netmask: Netmask assigned by the ISP of remote local ip;

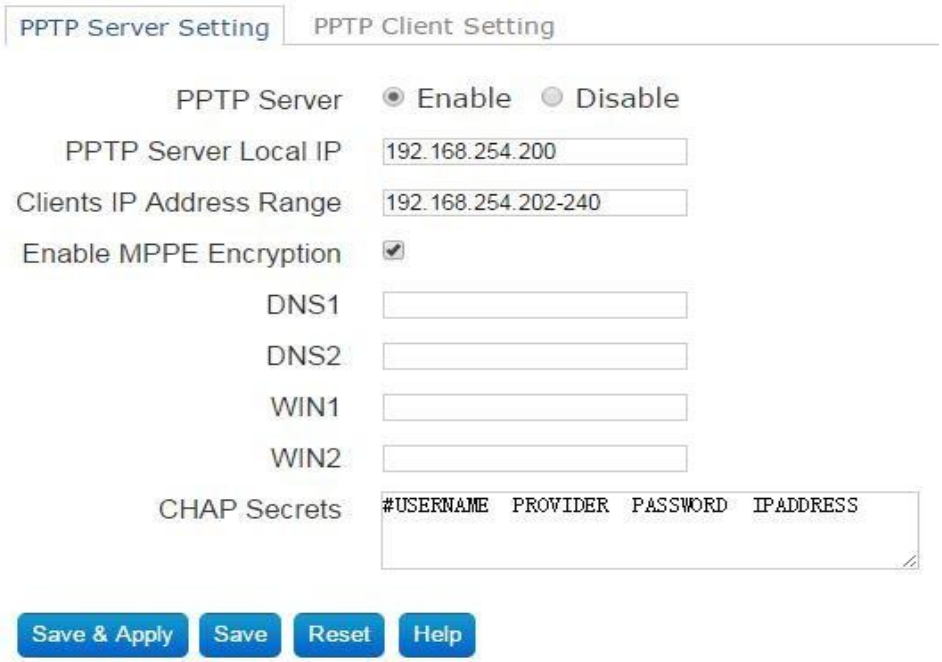
Nat: Allow network address translation

Enable MPPE Encryption: Use MPPE force encryption.

Enable Manual Setup: Configure the IP address manually.

3.3.4.2 PPTP

PPTP Server



PPTP Server Local IP: Enter the PPTP Server IP address, different with LAN IP address.

Clients IP Address Range: IP addresses assigned to the clients, **xxx.xxx.xxx.xxx-xxx**

Enable MPPE Encryption: Use MPPE Force Encryption.

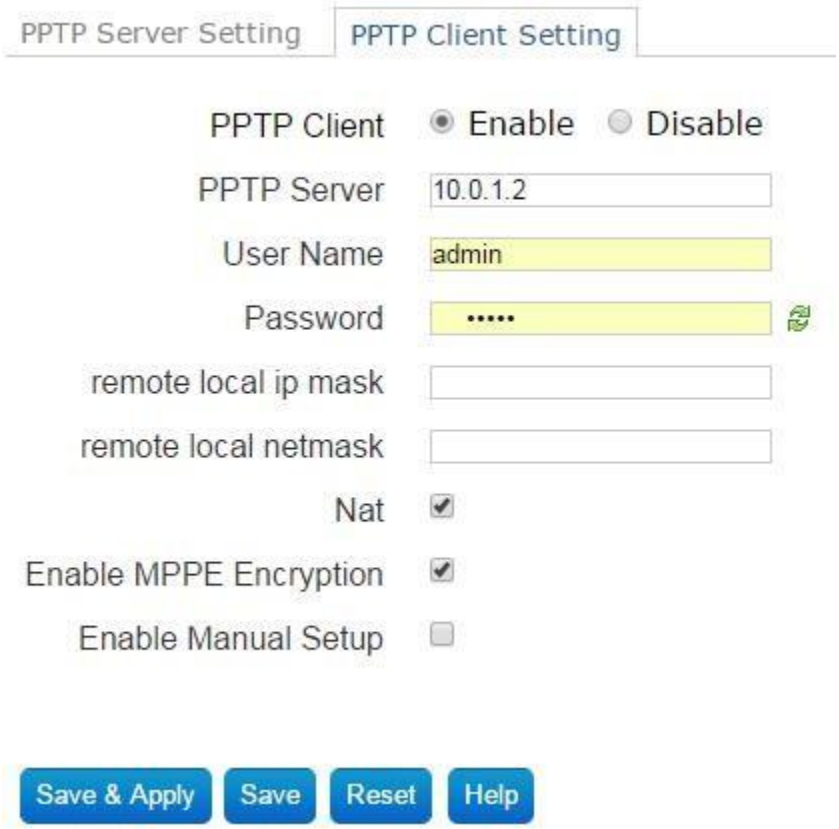
DNS1,DNS2,WINS1,WINS2: Set your first DNS, second DNS, first wins, second wins.

CHAP Secrets: The usernames and passwords of the clients.

NOTE: The Clients IP can't be the same with the IP of DHCP, but outside of the range.

CHAP Secrets format: user blank*blank password blank*

PPTP Client



PPTP Server: The IP address of PPTP server
User Name: The user name which is recognized by the server
Password: The password which is corresponding to user name
remote local ip mask: The remote local ip address
remote local netmask: Netmask assigned by the ISP of remote local ip;
Nat: Allow network address translation
Enable MPPE Encryption: Use MPPE Force Encryption.
Enable Manual Setup: Assign the IP address manually.

3.3.4.3 GRE

GRE (Generic Routing Encapsulation) encapsulates the network layer protocol(IP , IPX) data packets, it makes these packets can be transferred in the other network layer protocol. GRE uses tunnel technology, which is the third layer protocol of VPN(Virtual Private Network). With GRE you can setup VPN tunnel through GRE protocol. You can setup max 12 tunnels.



Click “Add” to add rules, just like below.



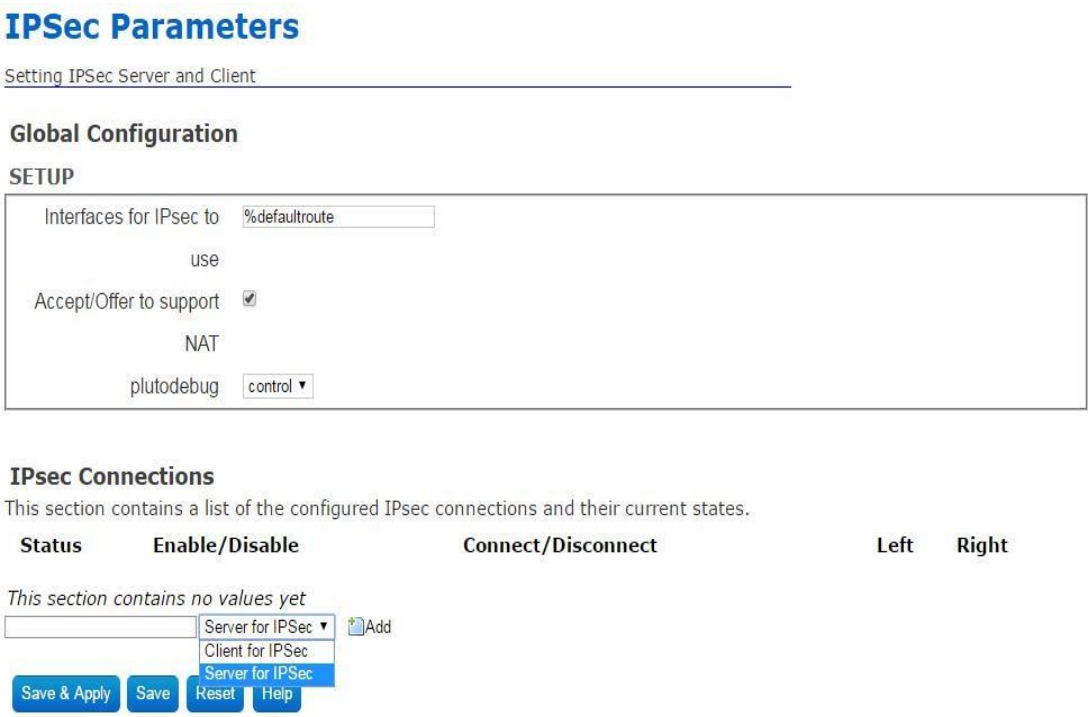
Name: The name of GRE rule

Peer Wan IP: Enter the GRE Wan IP of peer side

Peer Tunnel IP: The GRE tunnel IP of peer side

Peer Subnet: The Subnet of peer side， it can not be the same with the local subnet

3.3.4.4 IPsec



There are two modes are provided, which are “Server for IPSec” and “Client for IPSec”.

Server for IPSec:

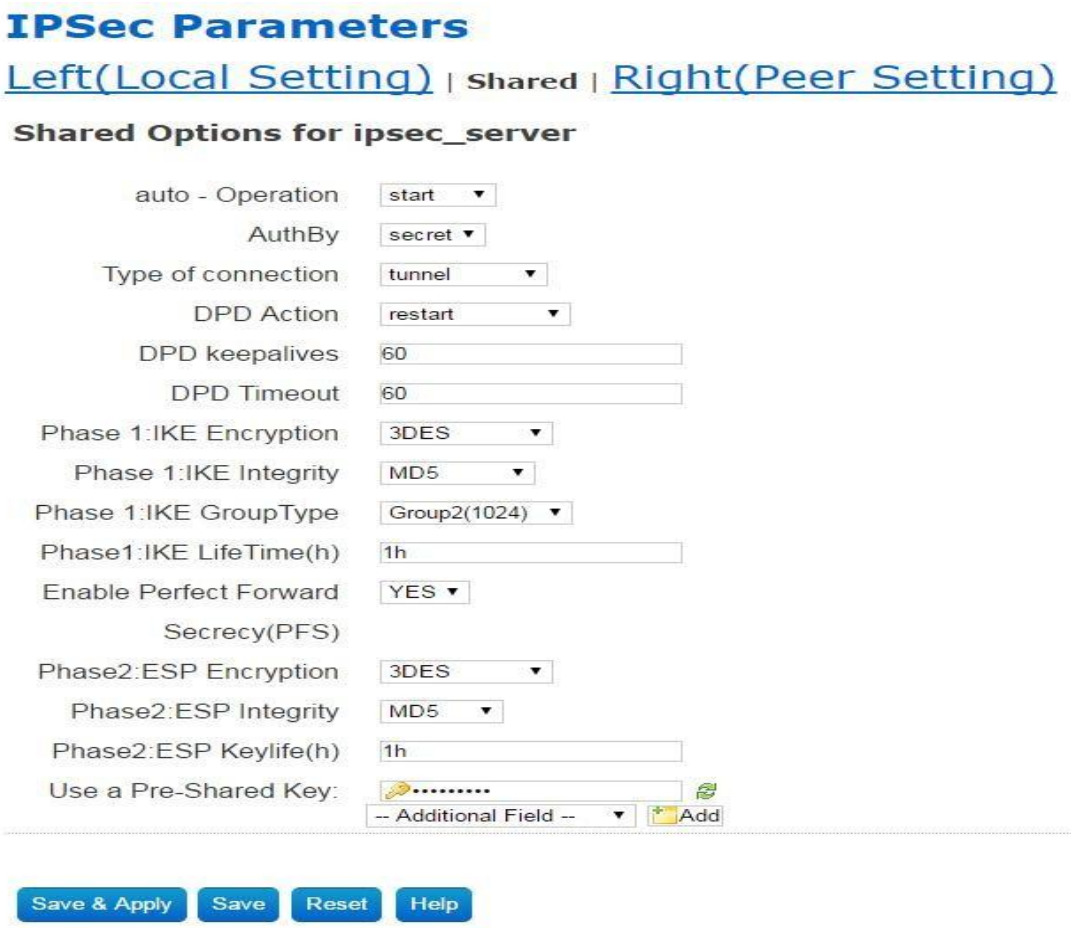
Left(Local Setting)



leftid: this is the sign of the local side, you can the id just like “@123”

leftsubnets: it is the subnet of the local side, just like “192.168.4.0/24”

shared:



Auto – Operation : Fine options are provided, add, ignore, manual,route,start.

AuthBy: there are three manners, sercret, rsasig, nerver.

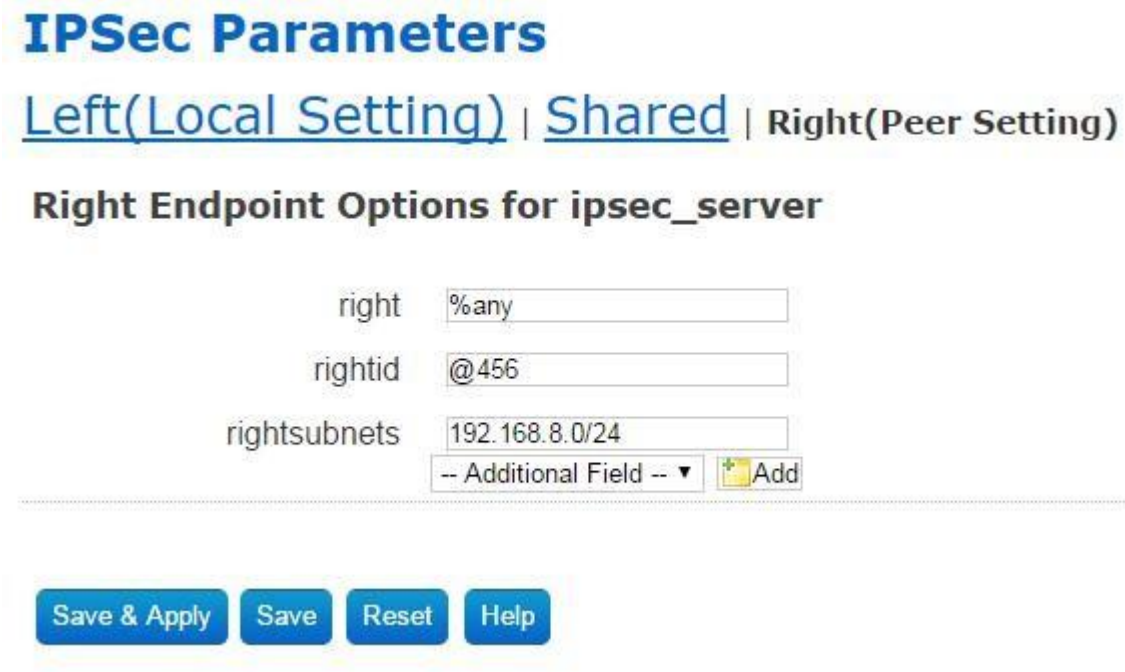
Type of connect: There are 5 kinds of connect type, drop, passthrough, reject, transport, and tunnel.

DPD Action: clear, hold, restart, restart by peer.

DPD keepalives: The default is 60s, you can change it by yourself.

DPD Timeout: The timeout setting, default is 60s

Right(Peersetting)

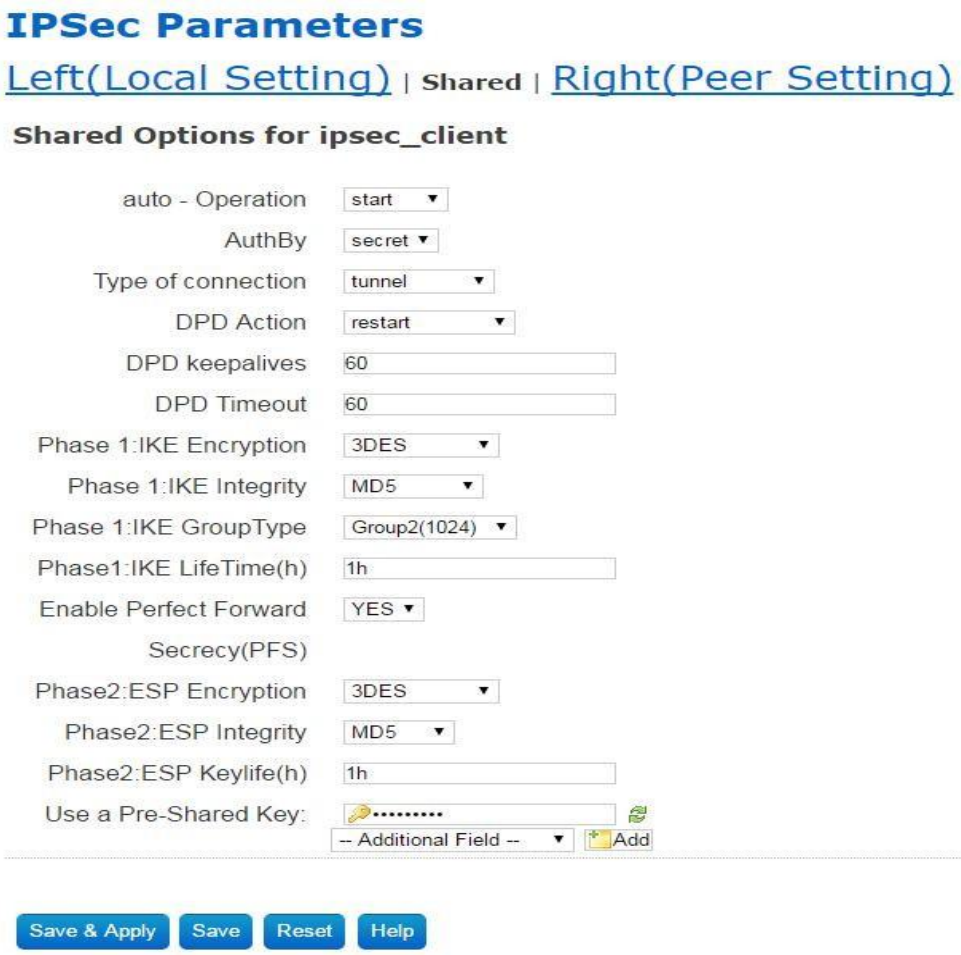


Right: %any, means for any client is ok.
Rightid: the Sign of opposite side.
Right subnets: the opposite subnet, for example: 192.168.8.0/24

Client for IPSec settings are similar with Server for IPSec settings



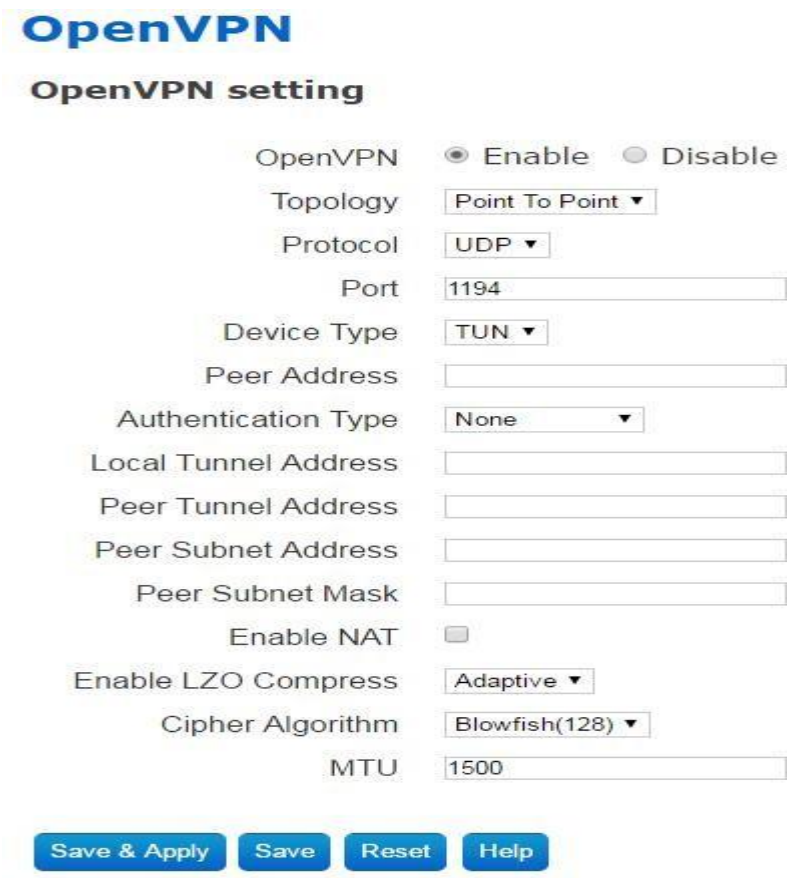
Shard



Right(Peer Setting)

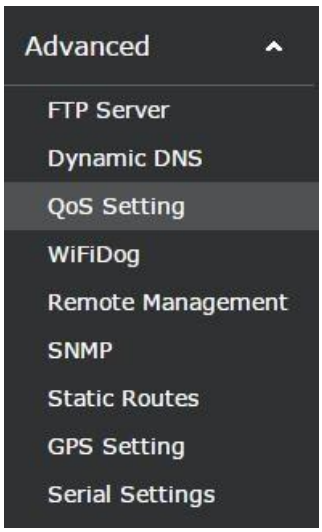


3.3.4.5 OpenVPN



Topology: Point To Point and Subnet are selectable.
Protocal: The protocol would be TCP or UDP.
Port: The port which is listened to.
Device Type: TUN and TAP.
Peer Address: The opposite side IP address.
Authentication Type: The Authentication type would be Static Secret and Certificate.
Local Tunnel Address: The ip address of local tunnel.
Peer Tunnel Address: the ip address of peer tunnel.
Peer Subnet Address: the subnet of peer address;
Peer Subnet Mask: the mask of peer subnet
Enable NAT: The NAT is enabled or not
Enable LZO Compress: It could be YES, NO, or Adaptive.
Cipher Algorithm: Blowfish(128), DES(128), 3DES(192), AES(128),AES(192), AES2 (56).

3.3.5 Advanced



3.3.5.1 FTP Server

In this page, you can config the FTP server setting.



FTP Service: FTP Service is enabled by default, select “Disable” if you want to disable this function.

Resource Path: The path of your resource, you can select other option in the drop-down box.

FTP Account: The FTP account of the service, do not use admin or root

FTP Password: The password according to FTP Account.

3.3.5.2 Dynamic DNS

Because of the allocation of dynamic IP addresses, wan IP addresses always change when the routers connect to the internet. In that case, you should use dynamic DNS. The domain name providers allows you to register a domain name which is signing up with current ip of the routers.

As a result, you can access to the latest internet IP address.



Service Type: XWR3400Grouter supports several DDNS server, such as DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP. User-defined server is allowed either.

User Name: The user name which is registered on the DDNS server. The maximum length is 64 characters.

User Password: The password according to the user name. The maximum length is 32 characters.

Host Name: The subdomain which is registered on the DDNS server. There is no limit to the length of host name.

Not USE Internet IP detect: The approach to access wan IP address. Router should detect the wan IP itself when it is selected.

Bind Status: The running state of DDNS. “Bind Failed” or “Bind success”

3.3.5.3 QoS Setting

QoS function controls the upload traffic and download traffic to balance the traffic, and it also can assign priority for specific IP address or MAC.

Basic Setup



Download speed(kbit/s): In order to use bandwidth management (QoS) you must enter bandwidth values for your downlink. These are generally 80% to 90% of your maximum bandwidth.

Upload speed(kbit/s): In order to use bandwidth management (QoS) you must enter bandwidth values for your uplink. These are generally 80% to 90% of your maximum bandwidth.

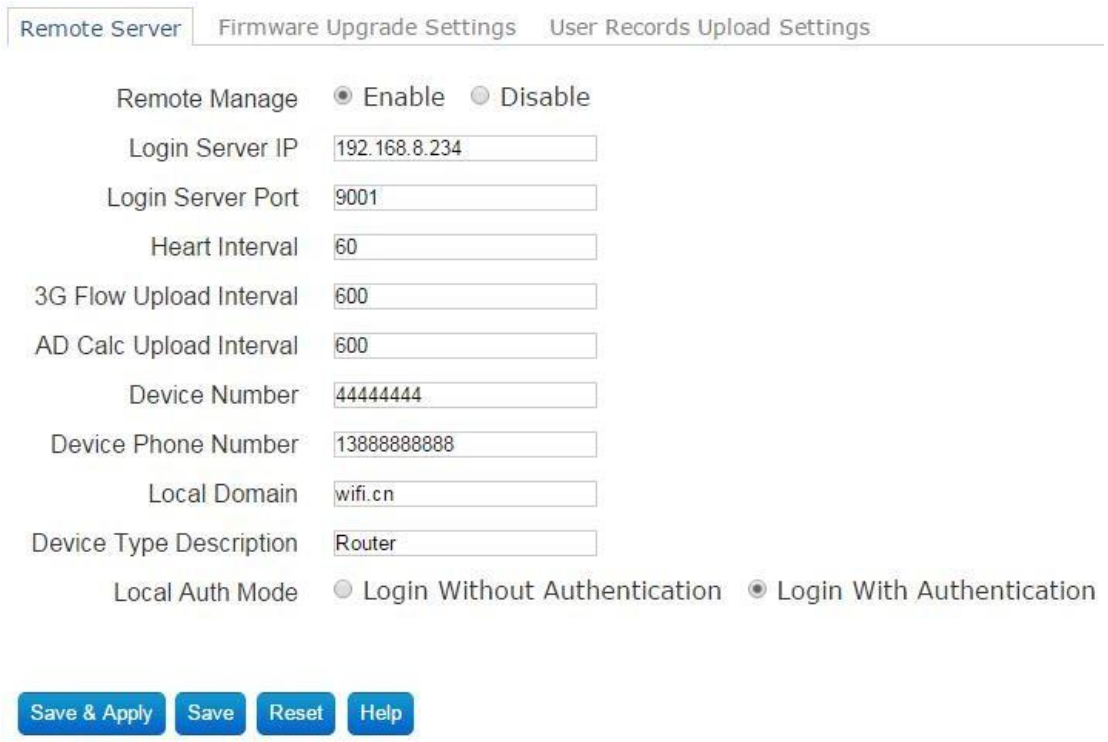
Max Upload per user:you can enter max upload bandwidth values for per user.

Max Download per user:you can enter max download bandwidth values for per user.

3.3.5.4 Remote Management Settings

Remote management function can manage all of the routes by the cloud platform. Users can control all devices by the cloud platform, including routine configuration, firmware upgrade and User records upload.

Remote Server:



Remote Manage:

Enable: Enable the Remote Manage function.

Disable: Disable the Remote Manage function.

Login Server IP: The IP address of cloud platform server.

Login Server Port: The port of cloud platform server

Heart Interval: The heartbeat interval to keep connection alive., 600 seconds by default

3G Flow Upload Interval: The interval of 3G flow, 600 seconds by default

Device Number: Device number is the only identification, which is a eight-digit number. Make sure that the device number is different from other devices. The defaut is 44444444.

Device Phone Number: Enter the phone number of the sim card.

Local Domain: The domain name of the router.

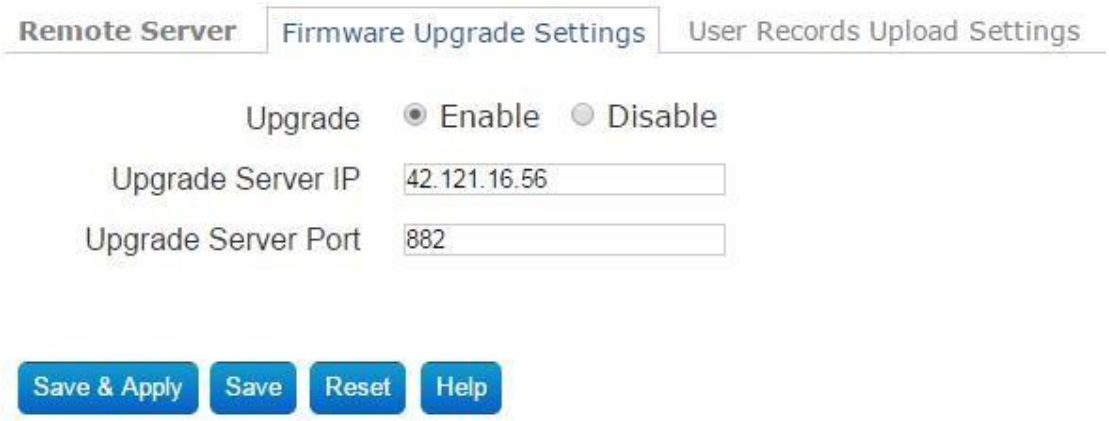
Device Type Description: The type description of the device.

Local Auth Mode:

Login With Authentication: Enable the local authentication.

Login Without Authentication: Disable the local authentication.

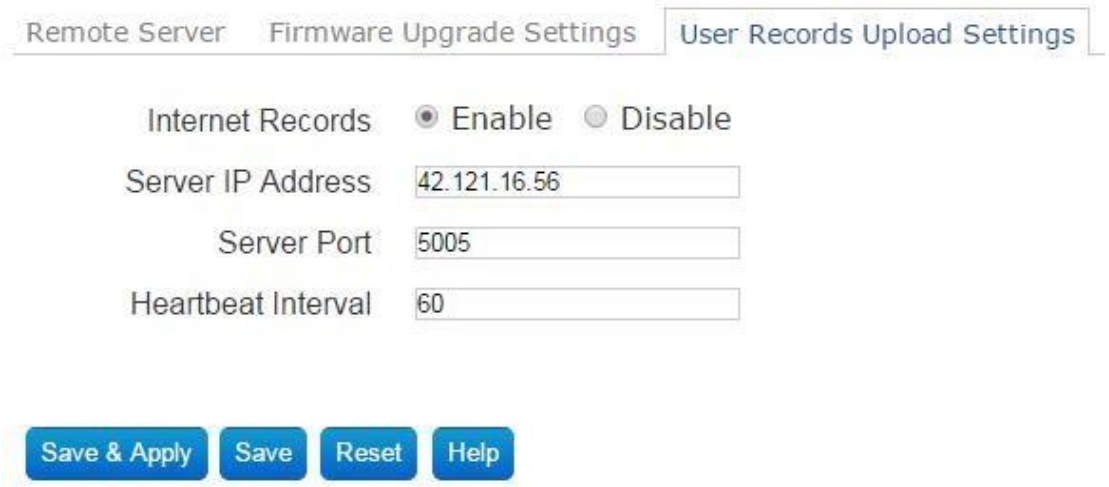
Firmware Upgrade Settings:



Upgrade Server IP: The remote upgrade server IP address.

Upgrade Server Port: The remote upgrade server port.

User Records Upload Settings: This feature is used to upload user records.



Server IP Address: The remote user records server IP address.

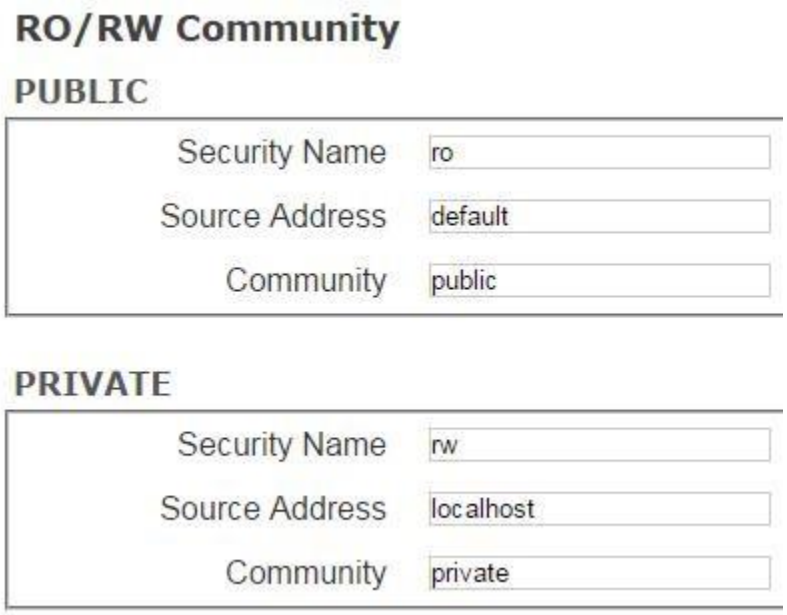
Server Port: The remote user records server port.

3.3.5.5 SNMP

Simple **N**etwork **M**anagement **P**rotocol (**SNMP**) is a widely used protocol for monitoring the health and welfare of network equipment (eg. routers), computer equipment and even devices like UPSs.



Location: The location of the equipment.
Contact: Contact this equipment management
Name: Device name, The default name is Agatel Ltd.



PUBLIC:
Security Name: The security name is RO, means only to read.
Source Address: The source address is default.
Community: The community is public by default

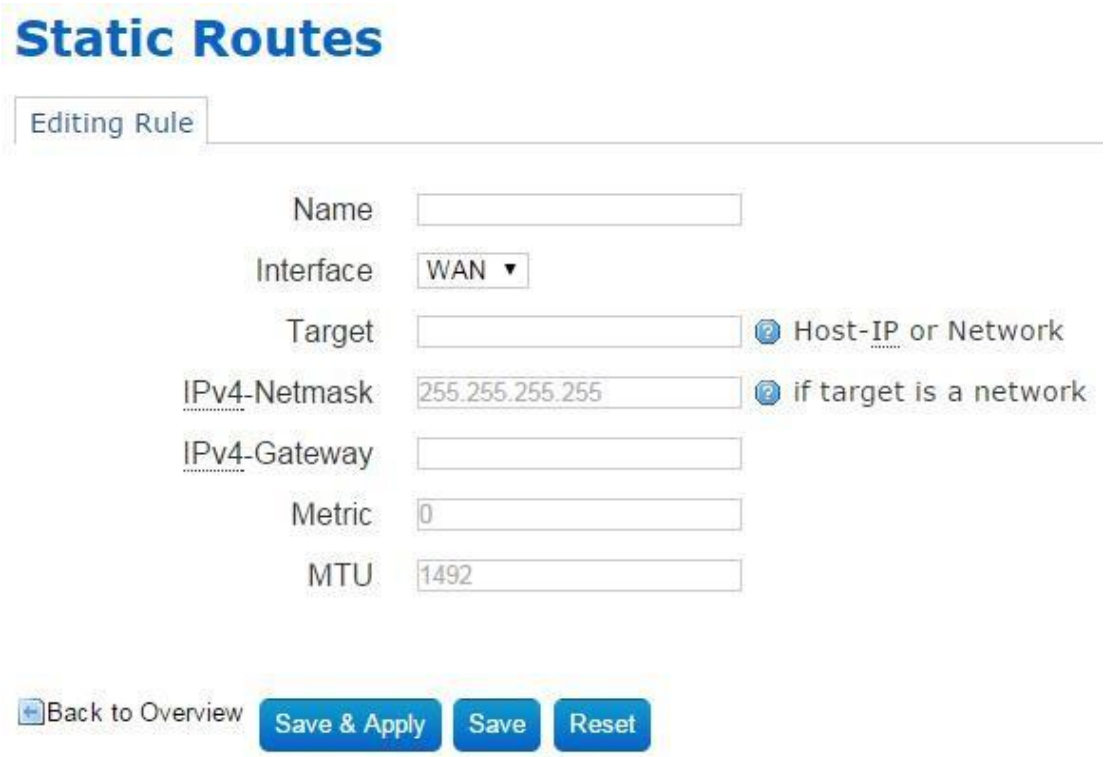
PRIVATE:
Security Name: The security name is rw, means read-write permissions
Source Address: The source address is localhost.
Community: The community is private by default

Click “Save & Apply” to make it effect and click “Save” just to save it but not apply, or you also can click “Reset” to turn to default value.

3.3.5.6 Static Routes



If you want to set static routing between the router and the other network, Click "Add" on the bottom-left corner of the page, and you will see below, then edit the rule please.



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

Interface: It indicates that users whether the Destination IP Address is on the LAN (internal wired and wireless networks) or the WAN (Internet). Select the appropriate interface optionin the drop-down box.

Target: The destination IP address, which is the address that users want to assign a static route.

IPv4-Netmask: The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion

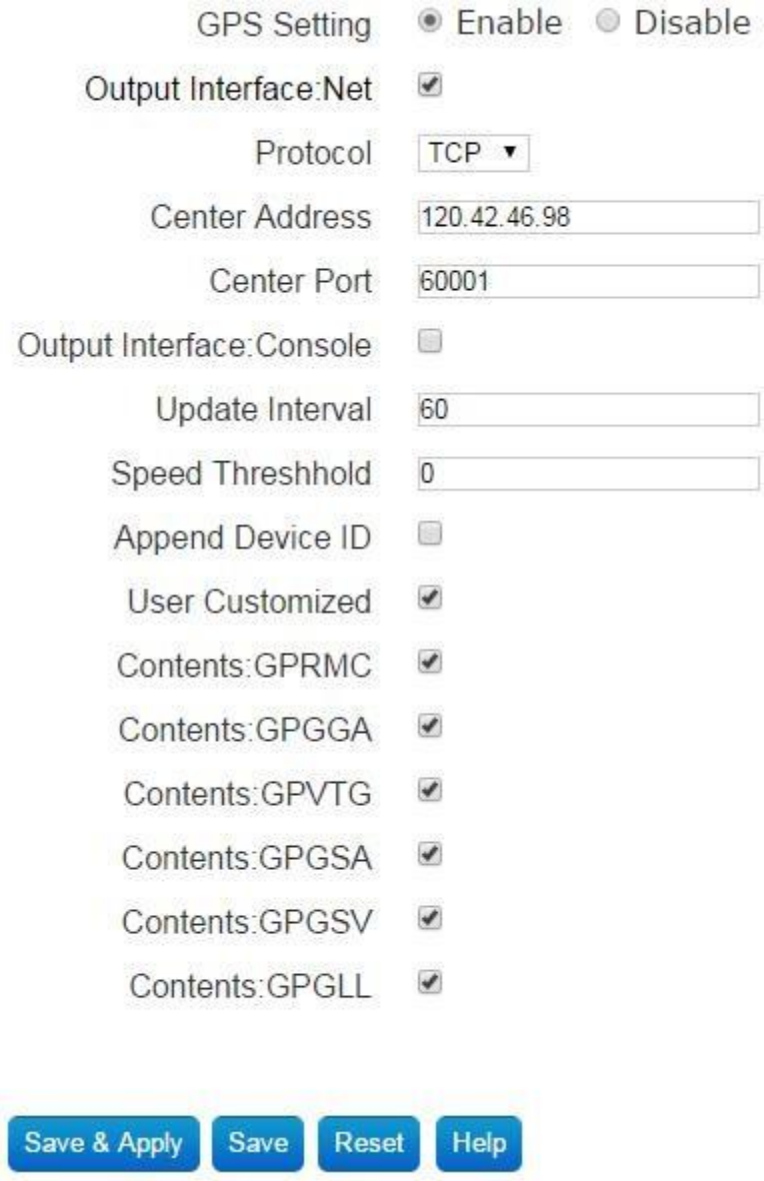
IPv4-Gateway: IP address of the gateway device that allows for contact between the router and the network or host.

Metric: 0-9999, the same as the ttl.

MTU: Maximum Transmission Unit, set the value according to the local MTU and the internet MTU, to make full use of the internet throughout.

3.3.5.7 GPS Setting

GPS setting allows you to set the GPS configuration. The user customized feature is provided.



Gps Setting: Enable or disable GPS function.

Output Interface:

Net: This item selects the network output interface.

Console: This item selects the GPS serial port output interface.

Protocol: TCP mode or UDP mode.

Center Address: The GPS center's IP Address or domain name.

Center Port: The GPS center's listening port.

Update Interval: The time interval between two GPS information update, unit is second.

Speed Threshold: The GPS speed threshold of update gps information.

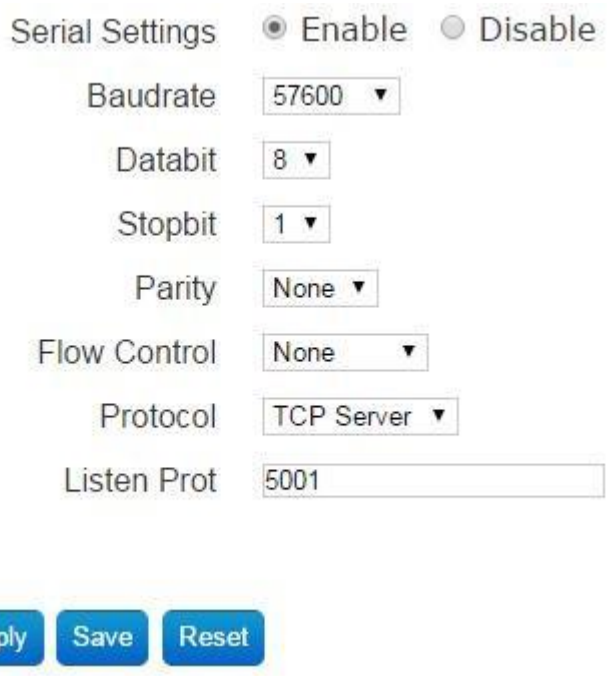
Append Device ID: The item selects the device ID.

Device ID: The device ID.

User Customized: GPS contents selection, including GPRMC, GPGGA, GPVTG, GPGSA, GPGSV, GPGLL.

3.3.5.8 Serial Setting

There is a console port on XWR3400Grouter. Normally, this port is used to debug the router. it can also be used as a serial port. 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 DTU (Data Terminal Unit).



Baudrate: The serial port's baudrate, there are several options, such as: 115200, 57600, 38400, 19200, 9600, 4800, 2400, etc.

Databit: The databit of the serial port

Stopbit: The stopbit of the serial port

Parity: The parity of the serial port

Flow Control: The flow control type of the serial port

Protocol: 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.

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 Number: The router's phone number.

Device ID: The router's identity ID.

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.

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"

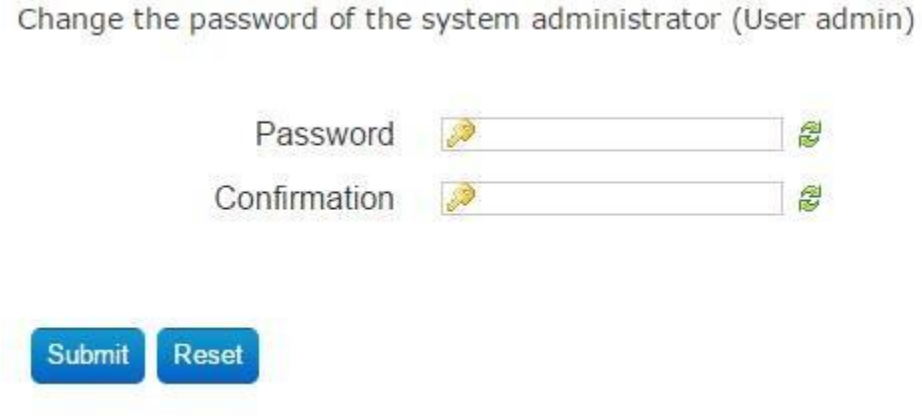
3.3.6 Management

The Management screen allows you to change the system settings of the XWR3400Grouter. Onthis page you will find most of the configurable items of the router.



3.3.6.1 Admin Password

In this part, user can modify the password and submit it to make it effect.



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.

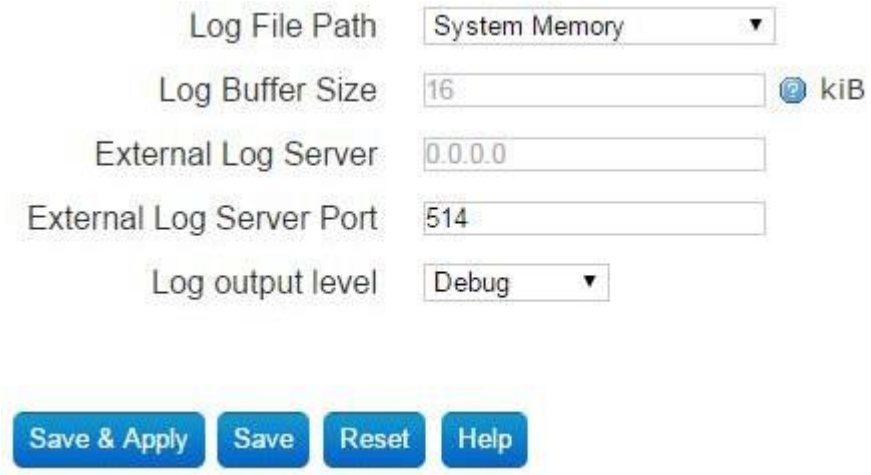
Note:

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.

3.3.6.2 System Log Setting

System Log Setting is used to modify the system log configuration.



Log File Path: Select the storage path in the drop-down box, which are “System memory”, “Console”,”KINGSTON(mmcblk0p1:)”,”Volume(sda1:)”, Please be attention that system log would be lost when the system is power failures if “System memory” is selected.

Log Buffer Size: Enter the buffer length of log file, in KB. The Log file will be clean when the data length is over the threshold you have defined.

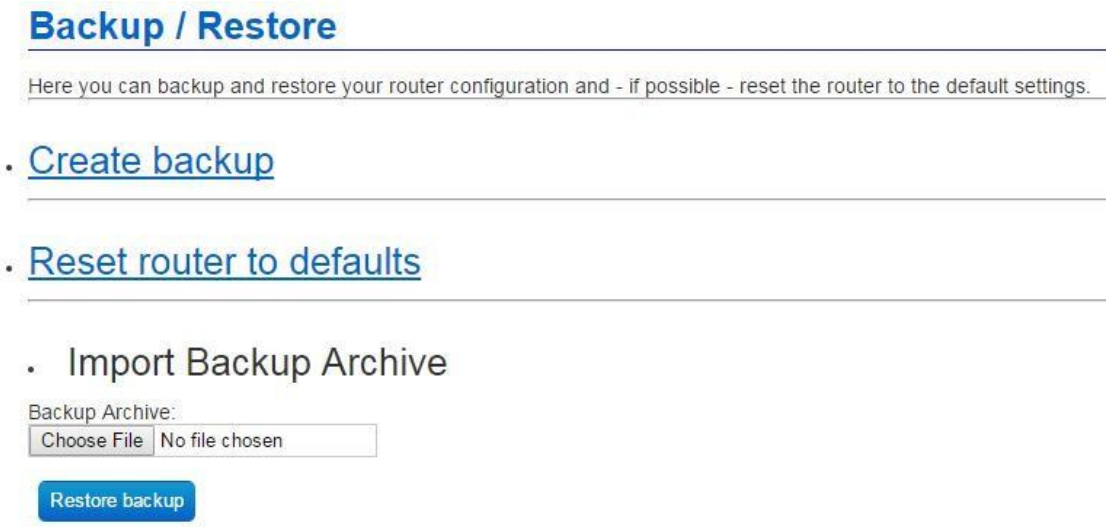
External Log Server: If you have an external log server, enter the IP address.

Log output level: Select the debug level in the drop-down box. The debug levels contain Debug,

Info, Notice, Warning, Error, Critical, Alert, Emergency. Debug is the lowest priority level while "Emergency" is the highest. Select the appropriate level. The lower the priority is, the more output. Click the "Save & Apply" to make it effect.

3.3.6.3 Backup/Restore

Backup/Restore functions, as the name, is used to backup the current configurations, and restore the settings at anytime if necessary.



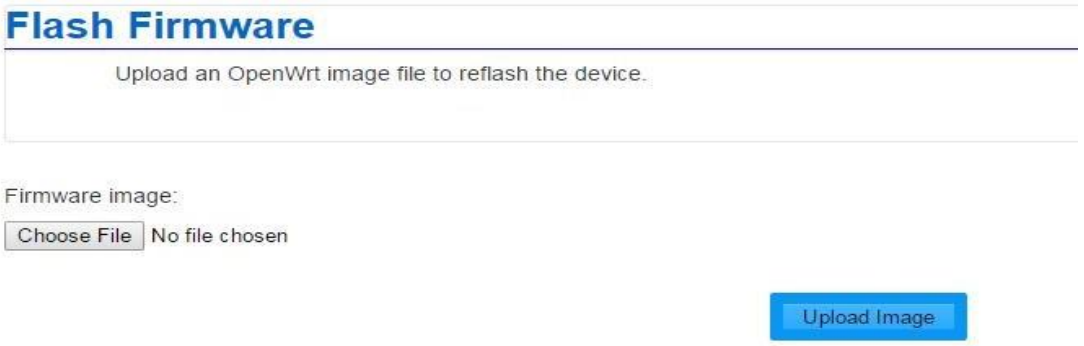
create backup: In case you need to reset the router back to the factory default settings, click "Create backup" to backup the current configurations, which maybe take several minutes. Some of configuration files, which are under the directory /lib and /ete, are compressed to backup-Agatel Ltd.-xxxx-xx-xx.tar.gz.

Reset router to defaults: It is used to reset all configurations to their default values.

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 192.168.4.1 and the default password is "admin".

3.3.6.4 Flash Firmware



Flash Firmware: New firmware versions are posted at www.four- faith.com and can be downloaded. If the Router is not experiencing difficulties, then there is no need to download a 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 that you have backup the current router settings before you upgrade the firmware.

To upgrade the Router's firmware:

1. Download the firmware upgrade file from the website.
2. Click the Browse... button and chose the firmware upgrade file.
3. Click the “Upgrade Image” button and wait until the upgrade is finished.

Note:

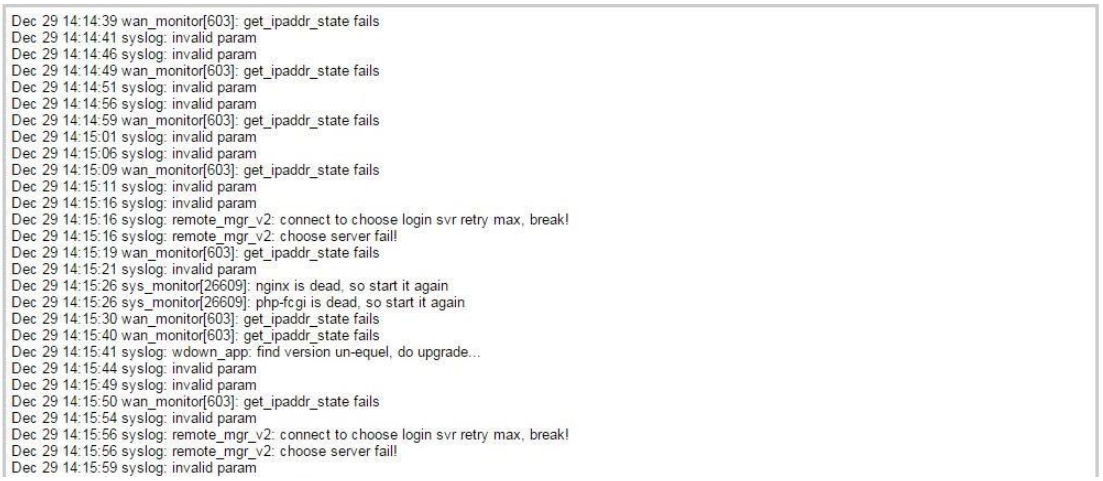
Upgrading firmware may take a few minutes.

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

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

3.3.6.5 Sys Log

Sys Log shows the system log information to user . You can get the system running state of the router, and diagnose system problems.



3.3.6.6 Attached Setting

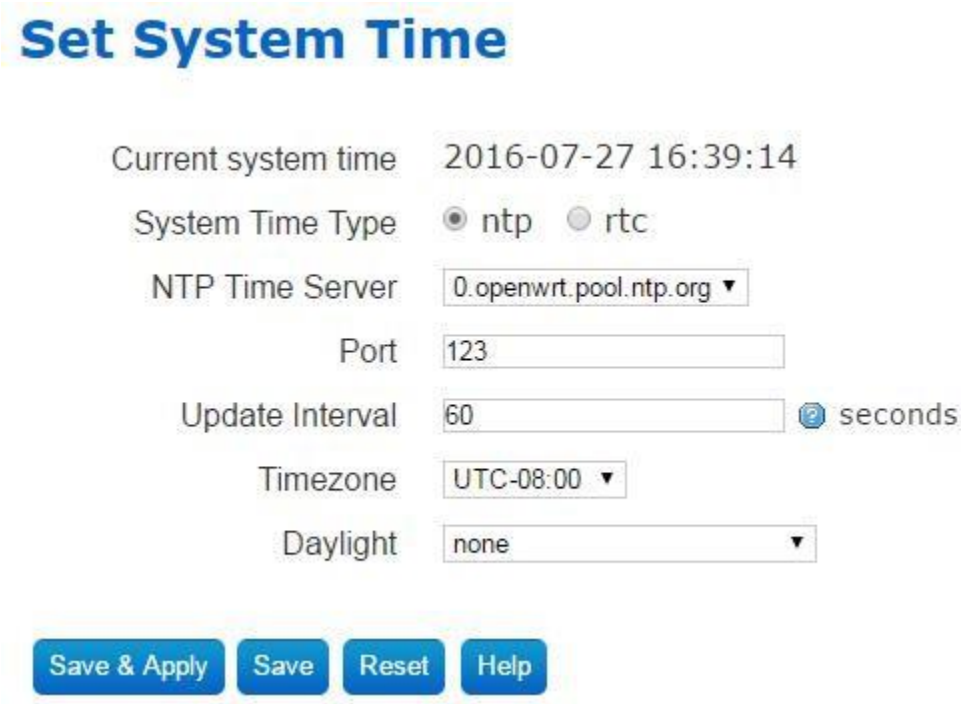
Attached Setting functions to show the attached devices in the tables, Which shows the “IP Address”, “Mac”, “Hostname”. Click “Refresh” to update the attached device table information.





3.3.6.7 Time Setting

This function allows you to setting the system time.



Current system time: Show the current system time.

System Time Type: The optional time type of the system are RTC and NTP. If RTC selected, the hardware RTC time is used. If ntp selected, it can synchronize to the **NTP time server:** As shown, The current time type is ntp.

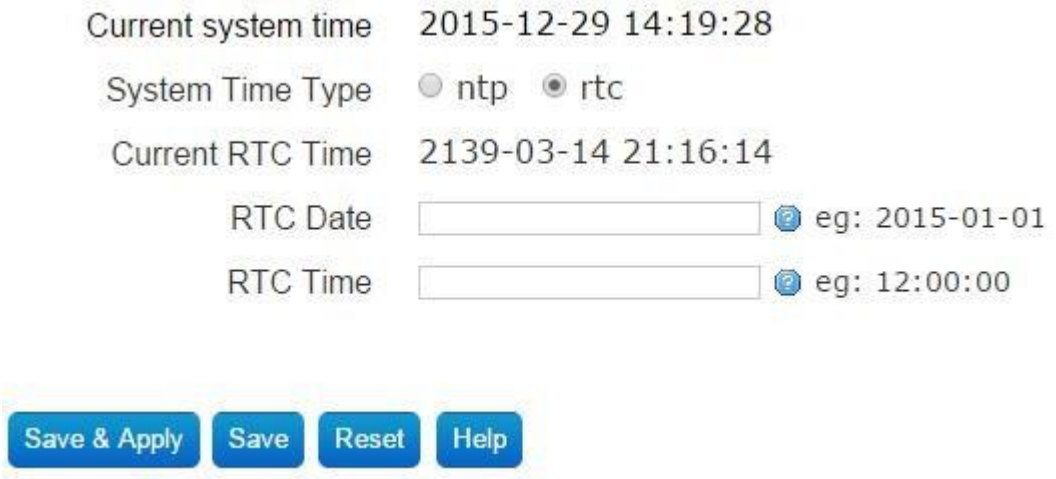
NTP Time Server: Select the optional time server which you want to synchronize to. You also can select the custom option, and enter the time server by yourself.

Port: The listening port of the time server.

Update Interval: It specifies the interval of NTP time updating.

Time zone: Users should select the proper time zome according to longitude and latitude.

Daylight: It specifies the daylight time according to the longitude and latitude.



If the RTC is selected, the RTC clock time is shown as above.

RTC Date: Enter the RTC date into the field if you want to modify it. Please pay attention to the date format, separated with "-";

RTC Time: Enter the RTC date into the field if you want to modify it. Please pay attention to the date format, separated with ":";

3.3.6.8 Reboot

This feature is used to reboot the operating system of your device. Click the "Perform reboot" as below.



3.3.6.9 Logout

This function allows you to logout from the web GUI, and turn to the login page.

3.3.7 Appendix

The following steps describe how to setup Windows XP Hyper Terminal.

Press "Start"→"Programs"→"Accessories"→"Communications"→"Hyper Terminal"



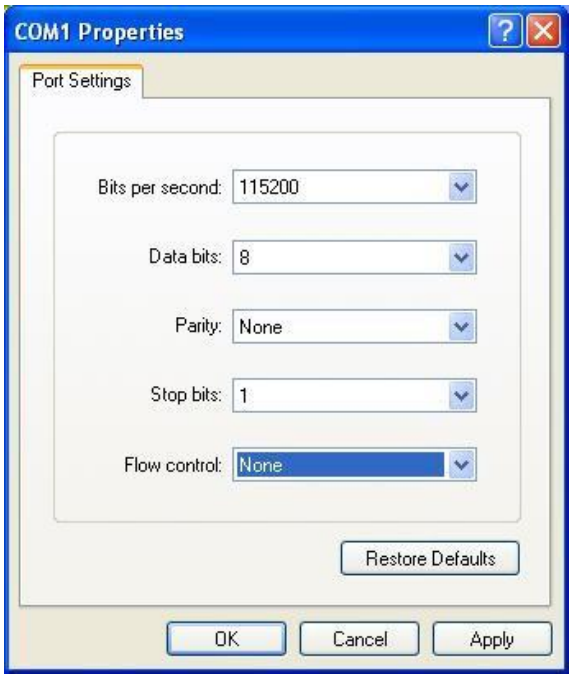
Input connection name, choose “OK”

Choose the correct COM port which connects to modem, choose “OK”



Configure the serial port parameters as following, choose “OK”

Bits per second: 115200
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None



Complete Hyper Terminal operation, It runs as following

