5G Industrial Router NR130

User Manual

V2.0.0

Xiamen Yifan Communicaton Technology Co., Ltd.

Add：Floor 14th, A06 Building, No. 370, ChengYi Street,
Jimei District, XiaMen, China Zip Code: 361000

Tel：+86 592-6101492

Fax:+86 592-5222813

http://www.yifanwireless.com

Document Revision History

Date	Version	Note	Author
2022.5.17	V2.0.0	First Version	Alvin

Note: There may be differences between models of accessories and interfaces, actual products shall prevail.

Copyright Notice

All contents in the files are protected by copyright law, and all copyrights are reserved by Xiamen Yifan Communication Technology Co., Ltd.

Without written permission, all commercial use of the files from Yifan 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.

Content

Chapter 1 Product Introduction 1
1.1 Product Overview 1
1.2 Diagram of Working Principle 2

Chapter 2 Installation 3
2.1 Overview 3
2.2 Packing List 3
2.3 Installation and Cable Connection 4
2.4 Power Supply 6
2.5 Indicators 7
2.6 Reset Button 7

Chapter 3 Configuration and Management 8
3.1 Configuration Connection 8
3.2 Access the Configuration on Web Page 9
3.3 Management and Configuration 11
3.3.1 Setting 11
Basic Setting 11
Dynamic DNS 17
Clone MAC Address 18
Advanced Router 18
VLANS 19
Networking 20
3.3.2 Wireless 23
Basic Setting 23
Wireless Security 25
3.3.3 Services 27
Services 27
3.3.4 VPN 30
PPTP 30
L2TP 31
OPEN VPN 33
IPSEC 37

GRE 39
3.3.5 Security 41
Firewall 41
3.3.6 Access Restrictions 44
WAN Access 44
URL Filter 47
Packet Filter 47
3.3.7 NAT 49
Port Forwarding 49
Port Range Forward 50
DMZ 50
3.3.8 QoS Setting 51
Basic 51
Classify 52
3.3.9 Applications 52
Serial Applications 52
3.3.10 Administration 54
Management 54
Keep Alive 56
Commands 57
Factory Defaults 58
Firmware Upgrade 58
Backup 59
3.3.11 Status 60
Router 59
WAN 62
LAN 64
Wireless 66
Bandwidth 68
Sys-Info 69

Appendix 72

Chapter 1 Product Introduction

1.1 Product Overview

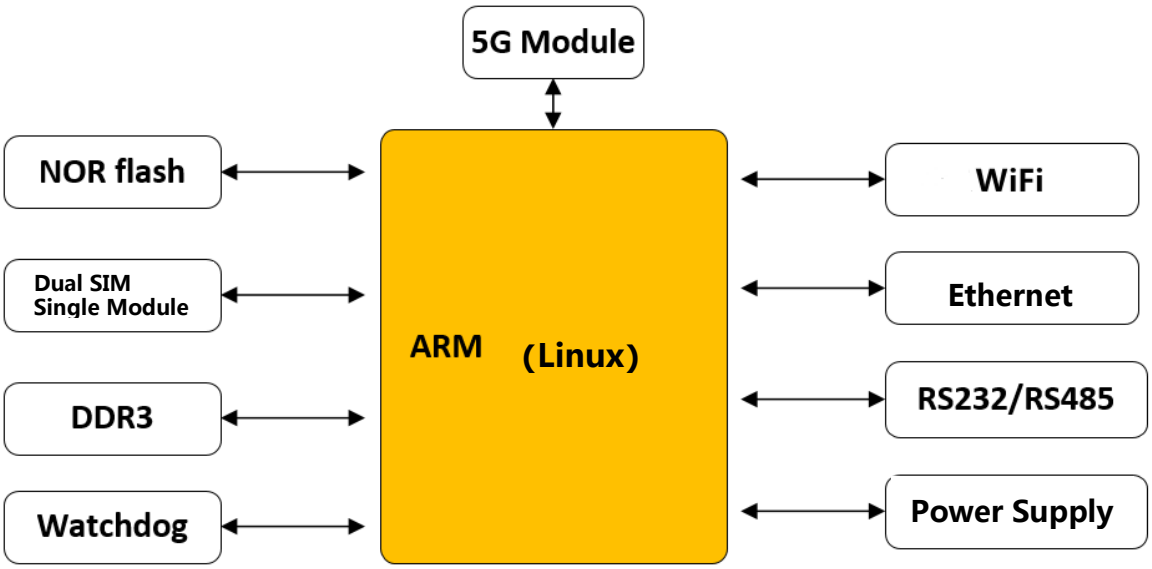
NR130 is a wireless communication router for the Internet of Things, which uses public 3G/4G/5G networks to provide users with wireless long-distance big data transmission functions.

The product adopts high-performance industrial-grade 32-bit communication processor and industrial-grade wireless module, with embedded real-time operating system as the software support platform, and provides 1xRS232, 1xRS485, 1xEthernet LAN and 1 Ethernet WAN/LAN(Default for the LAN), which can connect serial devices, Ethernet devices and WIFI devices at the same time to realize data transparent transmission and routing functions.

This product has been widely used in the M2M industry on the Internet of Things industry chain, such as smart grid, smart transportation, smart home, finance, mobile POS terminals, supply chain automation, industrial automation, smart buildings, fire protection, public safety, environmental protection, meteorology, Digital medical treatment, remote sensing survey, military, space exploration, agriculture, forestry, water affairs, coal mine, petrochemical and other fields.

 Copyright @ Yifan 2021

1.2 Block Diagram of Working Principle



 Copyright @ Yifan 2021

Chapter 2 Installation

2.1 Overview

5G routers must be installed correctly to achieve the designed functions. Usually, the installation of the equipment must be carried out under the guidance of qualified engineers approved by the company.

2.2 Packing List

When you open the box, please keep the packing materials, so that you can use it when you need to transfer in the future.

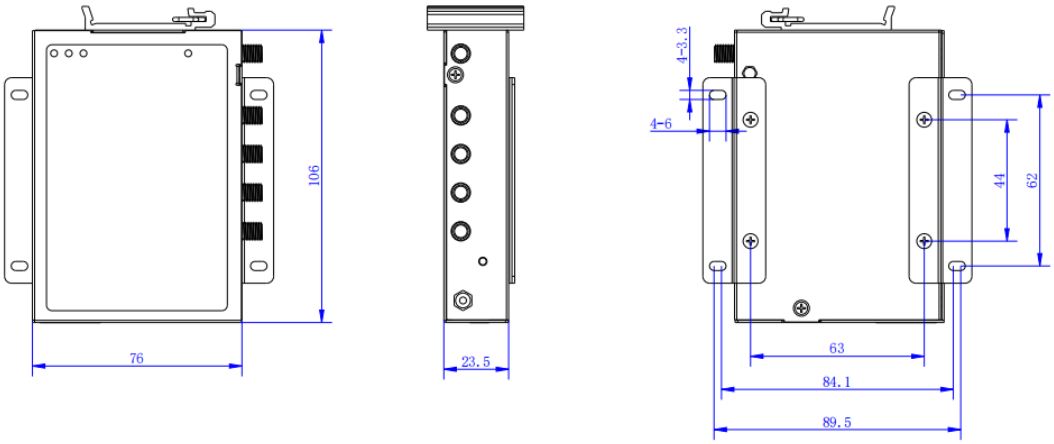
The list is as follows:

- 1 x 5G router
- 4 x 5G wireless cellular antennas (SMA male)
- 1 x WIFI antenna (SMA female)
- 1 x Matching power supply
- 1 x Ethernet cable
- 1 x Warranty card
- 1 x terminal block

 Copyright @ Yifan 2021

2.3 Installation and Cable Connection

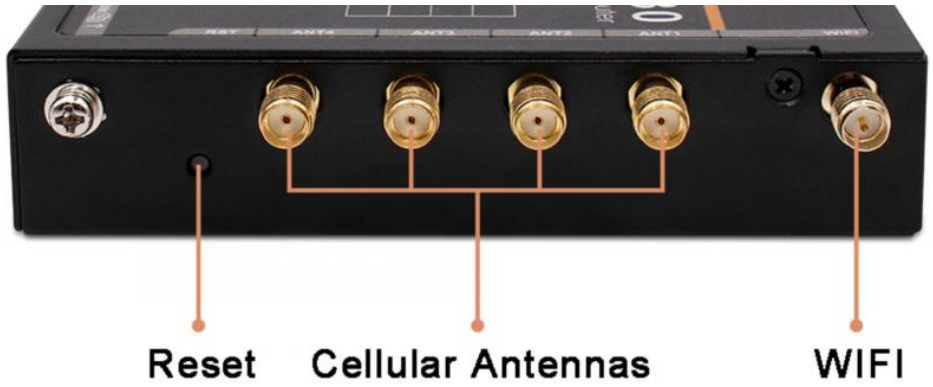
Dimension (mm):



Antenna Installation:

The 5G antenna interface is an SMA female socket. Screw the SMA male of the matching wireless cellular antenna to the antenna interface and make sure to tighten it. To increase the isolation of the 5G antenna, try to keep the antenna at an angle of 30 degrees to enhance signal quality.

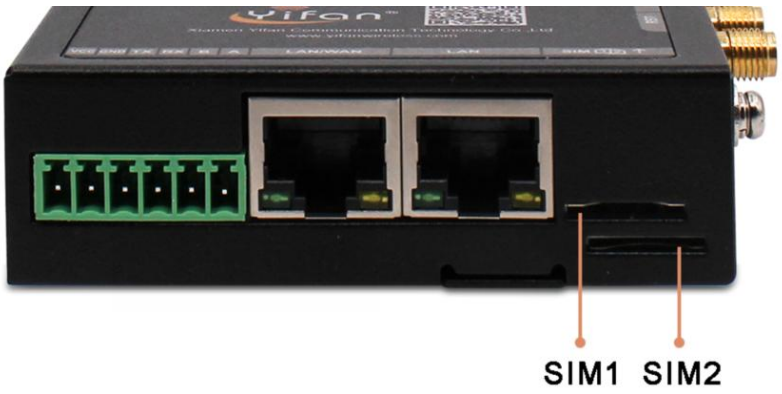
The WIFI antenna interface is an SMA male socket. Screw the SMA female of the matching WIFI antenna to the antenna interface and make sure to tighten it. In addition, to increase the isolation of the Wi-Fi antenna, it is recommended that the two Wi-Fi are placed at a 90-degree angle.



 Copyright @ Yifan 2021

SIM/UIM installation：

When installing or removing the SIM/UIM card, first use a pointed object to gently hold the eject button, and the SIM/UIM card sleeve will pop out. Ensure that the metal contact surface of the SIM/UIM card is facing correctly. Above is the position of SIM1: the missing angle is inward, and the contact surface of the SIM/UIM card is downward. Below is the position of SIM2: missing angle is inward, metal contact surface of the SIM/UIM card is downward.



Ethernet Cable:

Insert the network connection cable at one end of the straight to 5G router LAN/WAN or LAN, and on the other end into the Ethernet interface on the user's device. The direct network signal connection 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

 Copyright @ Yifan 2021

3.5 mm Terminal Interface Definition:

Using 5 pin terminal 3.5 mm of the interface, POWER, and function of RS232 and RS485. Specific definitions are as follows:

5 PIN 3.5 mm Terminal Interface Signal Definition			
Number	**Definition**	**Signal Description**	**Extended Function**
1	VCC	Positive of devices power supply terminal	
2	GND	Negative of devices power supply terminal	RS232 common ground
3	TXD	RS232 transmitting end	
4	RXD	RS232 receiving end	
5	B	RS485 B end	
6	A	RS485 A end	

Serial Port:

To use a serial port connection, the stripping end of the terminal serial port to receive the 3.5 mm terminal of the Router interface (GND TX RX), the DB9 end plug on the RS232 serial interface to the user equipment, terminal serial port signal connection is as follows:

Definition of Terminal Serial Cable Signal (RS232)					
Number	**Color**	**Signal Definition**	**DB9F**	**Signal Description**	**Description**
1	Brown	TXD	2	Send data	Output
2	Blue	RXD	3	Receive data	Input
3	Black	GND	5	Ground	

2.4 Power Supply

5G routers are usually used in complex external environments. To adapt to the complex application environment and improve the stability of the system, the router adopts advanced power supply technology. Users can use the standard 12VDC/1.5A power adapter to power the 5G router, or directly use the DC 9~36V power supply to power the router. When the user uses an external power supply to power the router, the stability of the power supply must be ensured (the ripple is less than 300mV, and the instantaneous voltage does not exceed 36V), and the power supply must be greater than 8W.

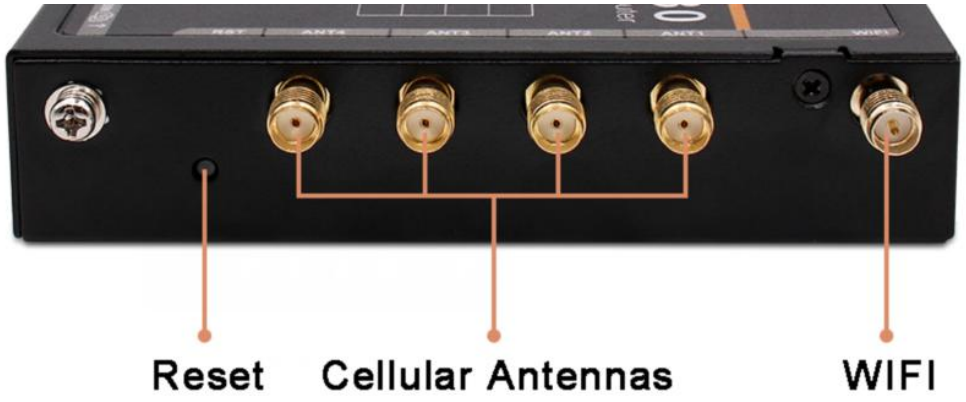
 Copyright @ Yifan 2021

2.5 Indicators

5G Router provide indicators as below：“PWR”,“SyS”,“Online”, “WiFi”：

Indicator	Status	Content
PWR	On	Device powered on
SYS	Blinking	System running normally
	Off	System not running
WiFi	On	WiFi turn on
	On	WiFi turn off
Online	Blinking	Connect with 4G network
	On	Connect with 5G network
	Off	Device offline

2.6 Reset Button



The 5G router has a reset button, marked as "RST"

The function of this button is to restore the parameter configuration of the 5G router to factory values

Methods as below: Power on device, let it running for 30 seconds, use a pen keep pressing the reset button for about 15 seconds, until all led turn off, the device will restart and reset to factory.

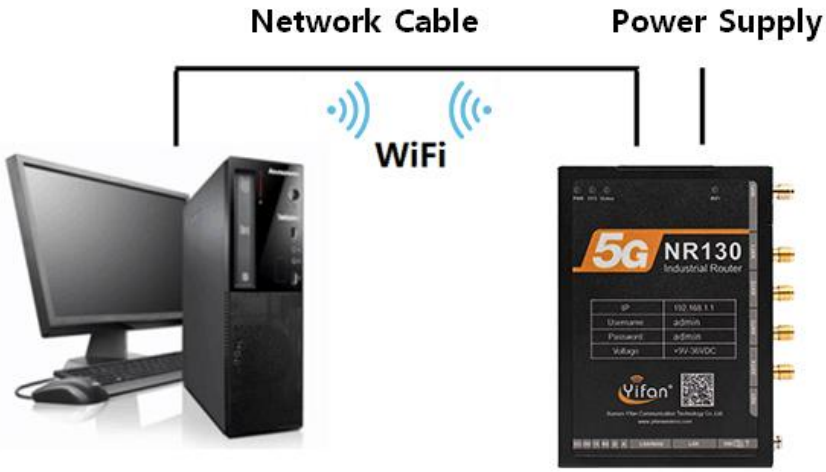
 Copyright @ Yifan 2021

Chapter 3 Configuration and Management

This chapter describes how to configure and manage the Router.

3.1 Configuration Connection

Before configuring a 5G router, connect the 5G router to the PC using a factory configured network cable or WiFi. When using a network cable, one end of the network cable is connected to any Ethernet port of a 5G router, LAN/WAN, or LAN, and the other end is connected to the Ethernet port of a PC. When WIFI is used, the default SSID of 5G industrial routers is "YIFAN", which does not require password verification. Please modify the IP address of PC as the same 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).



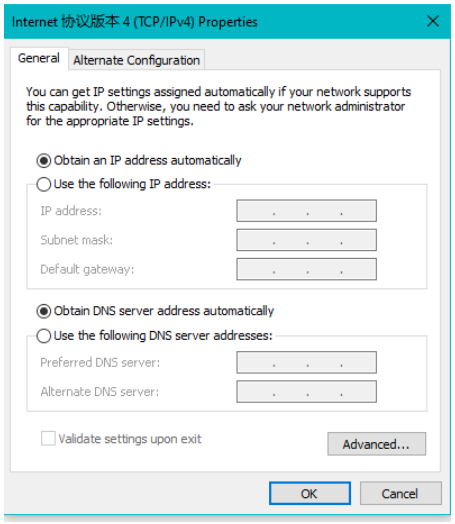
 Copyright @ Yifan 2021

3.2 Access the Configuration Web Page

The chapter is to present main functions of each page. Users visit page tool via web browser after connecting users' PC to the Router. There are eleven main pages: Setting, Wireless, Service, VPN, Security, Access Restrictions, NAT, QoS Setting, Applications, Management and Status. Users enable to browse slave pages by click one main page.

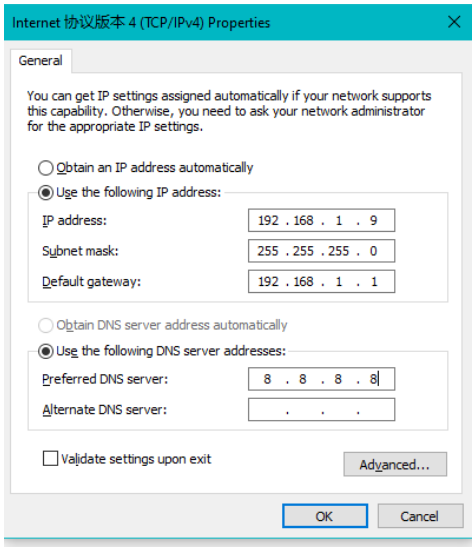
3.2.1 IP configurations in PC

The first method: Obtain an IP address automatically:



The second way: specify the IP address

Set the IP address of the PC to 192.168.1.9 (or other IP addresses in the 192.168.1 network segment), the subnet mask is set to: 255.255.255.0, and the default gateway is set to: 192.168.1.1. DNS is set to gateway address or local available DNS server.

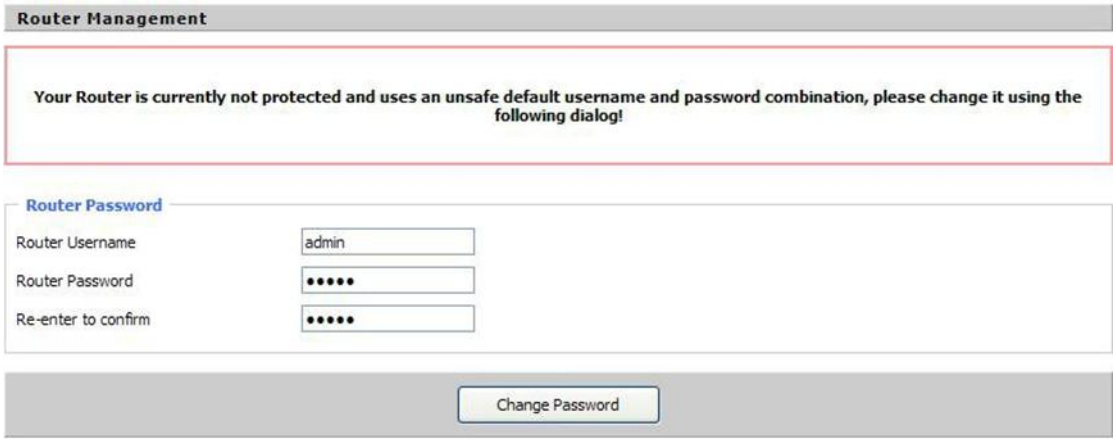


 Copyright @ Yifan 2021

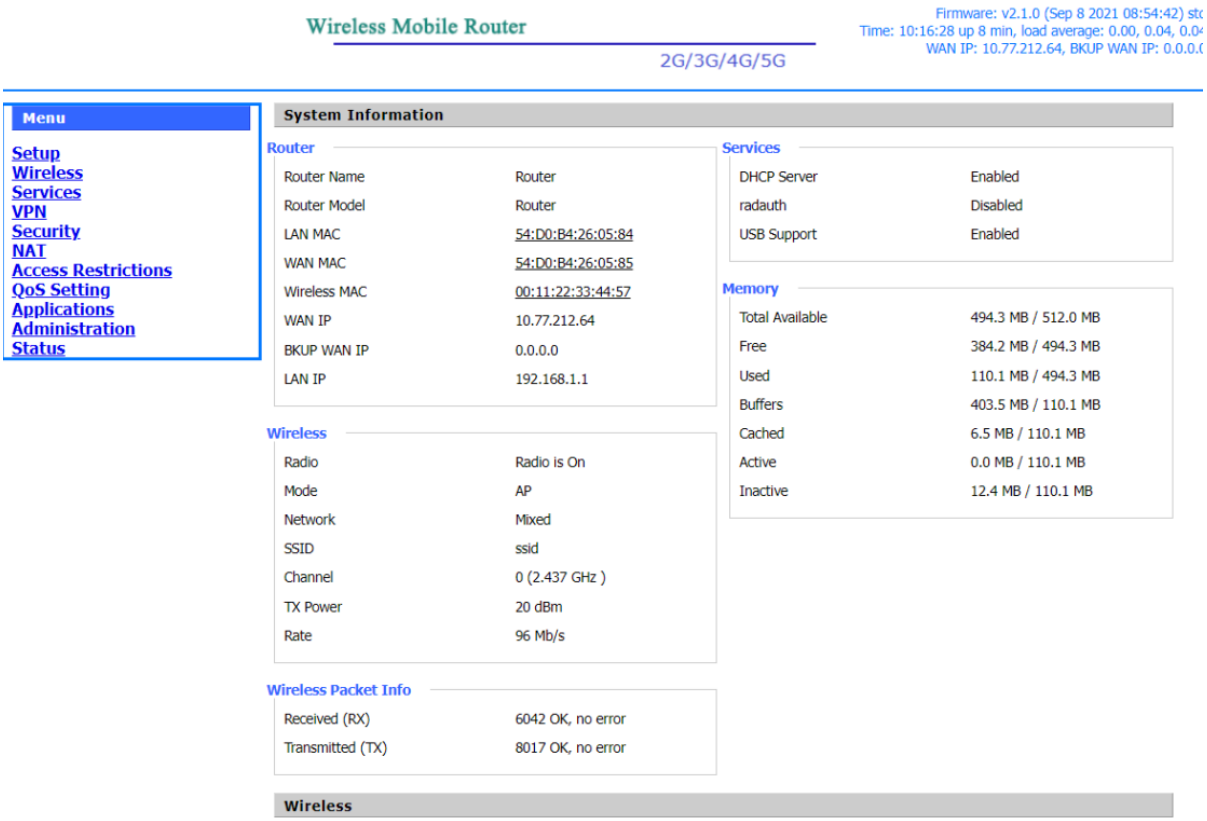
3.2.2 Log in to the configuration page

To access the web-based web management tool of the 5G industrial router, start IE or other browsers, and enter the default IP address 192.168.1.1 of the 5G industrial router in the "Address" field. Press the Enter key.

If you log in to the Web page for the first time, you can see the page shown below, prompting the user whether to modify the default username and password of the 5G industrial router. If you need to enter the user-defined username and password, click the "Change Password" button to apply.



If you click the main menu for the first time, you need to enter the corresponding username and password.



 Copyright @ Yifan 2021

If you click the main menu for the first time, you need to enter the corresponding username and password

Enter the correct user and password to access the corresponding menu page. The default username is **admin** and the default password is **admin**.

3.3 Management and Configuration

3.3.1 Setting

The Setup screen is the first screen users will see when accessing the Router. Most users will be able to configure the Router and get it work properly using only the settings on this screen. Some Internet Service Providers (ISPs) will require users to enter specific information, such as Username, Password, IP Address, Default Gateway Address, or DNS IP Address. This information can be obtained from your ISP, if required.

Basic Setting

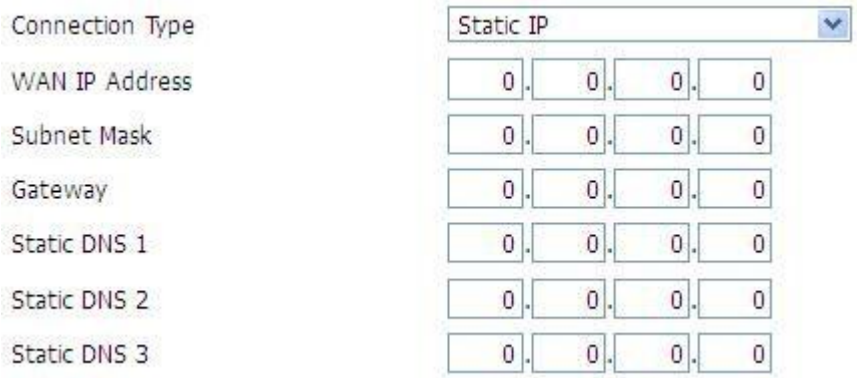
WAN Connection Type
Seven Ways: Disabled, Static IP, Automatic Configuration-DHCP, PPPOE, 3G/UNMTS/4G/LTE, DHCP-4G/5G.

1. Disabled

Forbid the setting of WAN port connection type

 Copyright @ Yifan 2021

2. Static IP

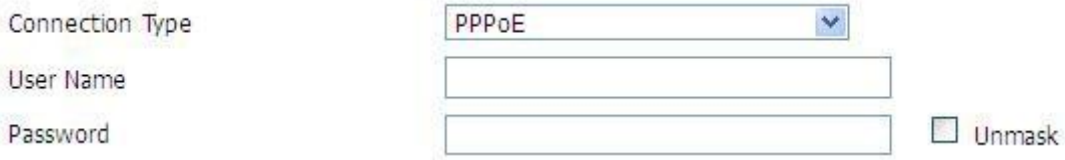


WAN IP Address: Users set IP address by their own or ISP assigns
Subnet Mask: Users set subnet mask by their own or ISP assigns
Gateway: Users set gateway by their own or ISP assigns
Static DNS1/DNS2/DNS3: Users set static DNS by their own or ISP assigns

3. Automatic Configuration-DHCP

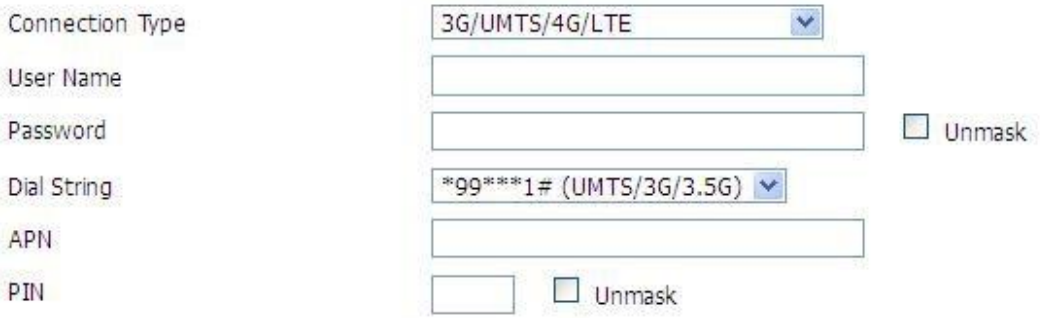
IP address of WAN port gets automatic via DHCP

4. PPPOE



Username: login the Internet
Password: login the Internet

5. 3G/UMTS/4G/LTE



 Copyright @ Yifan 2021

Username: Login users' ISP (Internet Service Provider)
Password: Login users' ISP
Dial String: Dial number of users' ISP
APN: Access point name of users' ISP
PIN: PIN code of users' SIM card

6. Connection Type

Connection type: Auto, Force 3G, Force 2G, prefer 3G, Prefer 2G options. If using 4G module, there has 4G network option. Users select different mode depending on their need

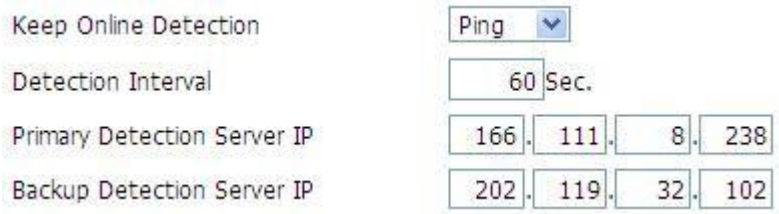
7. DHCP-4G

IP address of WAN port gets automatic via DHCP-4G

8. DHCP-4G/5G

The IP address of the WAN port is obtained in DHCP-4G/5G mode. The default Auto network type selection, namely, at the same time support the NSA and SA. This option is best set to separate SA or separate NSA according to the actual network environment.

9. Keep Online



This function is used to detect whether the Internet connection is active, if users set it and when the Router detect the connection is inactive, it will redial to users' ISP immediately to make the connection active. If the network is busy or the user is in private network, we recommend that Router mode will be better.

10. Detection Method

None: Do not set this function
Ping: Send ping packet to detect the connection, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.
Route: Detect connection with route method, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.
PPP: Detect connection with PPP method, when choose this method, users should also

 Copyright @ Yifan 2021

configure "Detection Interval" item.
Detection Interval: Time interval between two detections, unit is second
Primary Detection Server IP: The server used to response the Router's detection packet. This item is only valid for method "Ping" and "Route".

Backup Detection Server IP: The server used to response the Router's detection packet. This item is valid for method "Ping" and "Route".
Note: When users choose the "Route" or "Ping" method, it's quite important to make sure that the "Primary Detection Server IP" and "Backup Detection Server IP" are usable and stable, because they have to responsethe detection packet frequently.

Force Reconnect: This option schedules the PPPOE or 3G reconnection by killing the PPPD daemon and restart it.
Time: Needed time to reconnect

11. STP

STP (Spanning Tree Protocol) can be applied to loop network. Through certain algorithm achieves path redundancy, and loop network cuts to tree-based network without loop in the meantime, thus, to avoid the hyperplasia and infinite circulation of a message in the loop network

12. Optional Configuration

Router Name: Set Router name

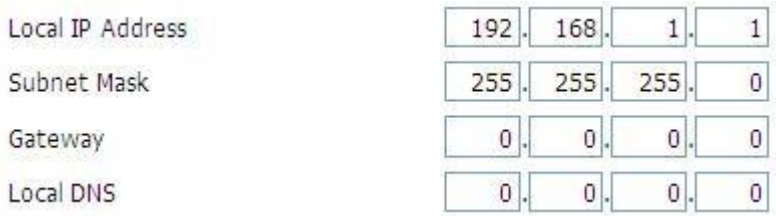
Host Name: ISP provides

Domain Name: ISP provides
MTU: Auto (1500) and manual (1200-1492 in PPPOE/PPTP/L2TP mode, 576-16320 in other modes)

 Copyright @ Yifan 2021

13. Router Internal Network Settings

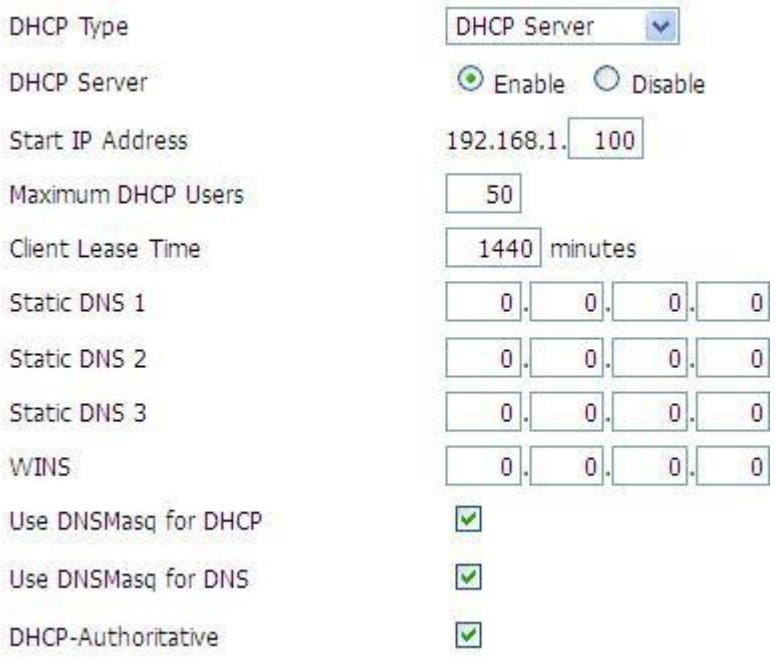
Router IP



Local IP Address: IP address of the Router
Subnet Mask: The subnet mask of the Router
Gateway: Set internal gateway of the Router. If default, internal gateway is the address of the Router
Local DNS: DNS server is auto assigned by network operator server. Users enable to use their own DNS server or other stable DNS servers, if not, keep it default.

14. Network Address Server Settings (DHCP)

These settings for the Router's Dynamic Host Configuration Protocol (DHCP) server functionality configuration. The Router can serve as a network DHCP server. DHCP server automatically assigns an IP address for each computer in the network. If they choose to enable the Router's DHCP server option, users can set all the computers on the LAN to automatically obtain an IP address and DNS, and make sure no other DHCP server in the network.



 Copyright @ Yifan 2021

DHCP Type: DHCP Server and DHCP Forwarder
Enter DHCP Server if set DHCP Type to DHCP Forwarder as blow:

DHCP Server: Keep the default Enable to enable the Router's DHCP server option. If users have already had a DHCP server on their network or users do not want a DHCP server, then select Disable
Start IP Address: Enter a numerical value for the DHCP server to start with when issuing IP addresses. Do not start with 192.168.1.1 (the Router's own IP address).
Maximum DHCP Users: Enter the maximum number of PCs that users want the DHCP server to assign IP addresses to. The absolute maximum is 253 if 192.168.1.2 is users' starting IP address.
Client Lease Time: The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.
Static DNS (1-3): The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Users' ISP will provide them with at least one DNS Server IP address. If users wish to utilize another, enter that IP address in one of these fields. Users can enter up to three DNS Server IP addresses here. The Router will utilize them for quicker access to functioning DNS servers.
WINS: The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If users use a WINS server, enter that server's IP address here. Otherwise, leave it blank.
DNSMasq: Users' domain name in the field of local search, increase the expansion of the host option, to adopt DNSMasq can assign IP addresses and DNS for the subnet, if select DNSMasq, DHCPD service is used for the subnet IP address and DNS.

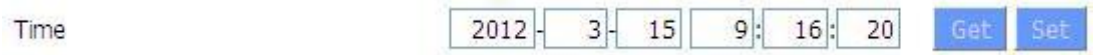
15. Time Settings

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

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

 Copyright @ Yifan 2021

16. Adjust 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.

Dynamic DNS

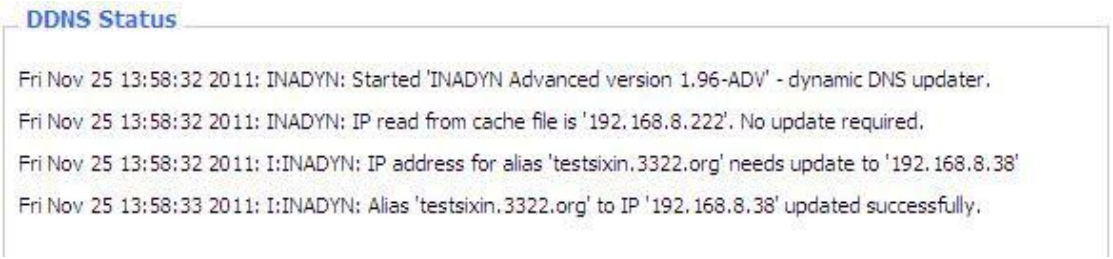
If user's network has a permanently assigned IP address, users can register a domain name and have that name linked with their IP address by public Domain Name Servers (DNS). However, if their Internet account uses a dynamically assigned IP address, users will not know in advance whattheir IP address 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 directedat their domain to their frequently-changing IP address.
DDNS Service: Router currently support DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP and Custom based on the user.

Username: Users register in DDNS server, up to 64 characteristic **Password:** password for the username that users register in DDNSserver, 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

 Copyright @ Yifan 2021

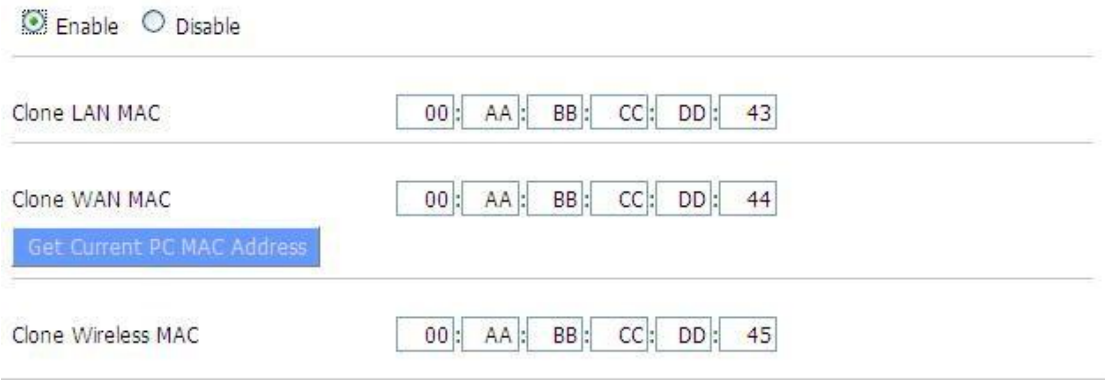
Status



DDNS Status shows connection log information

Clone MAC Address

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: Can clone three parts: Clone LAN MAC, Clone WAN MAC, Clone Wireless MAC.

Noted: That one MAC address is 48 characteristics, cannot 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.

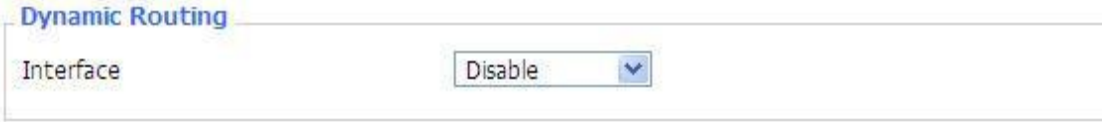
Advanced Router

Operating Mode: Gateway and Router

If the Router is hosting users' Internet connection, select Gateway mode. If another Router exists on their network, select Router mode.

 Copyright @ Yifan 2021

Dynamic Routing

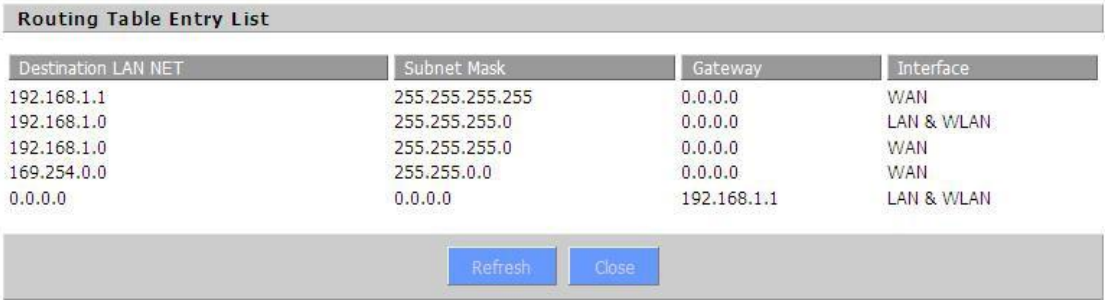


Subnet Mask: The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion

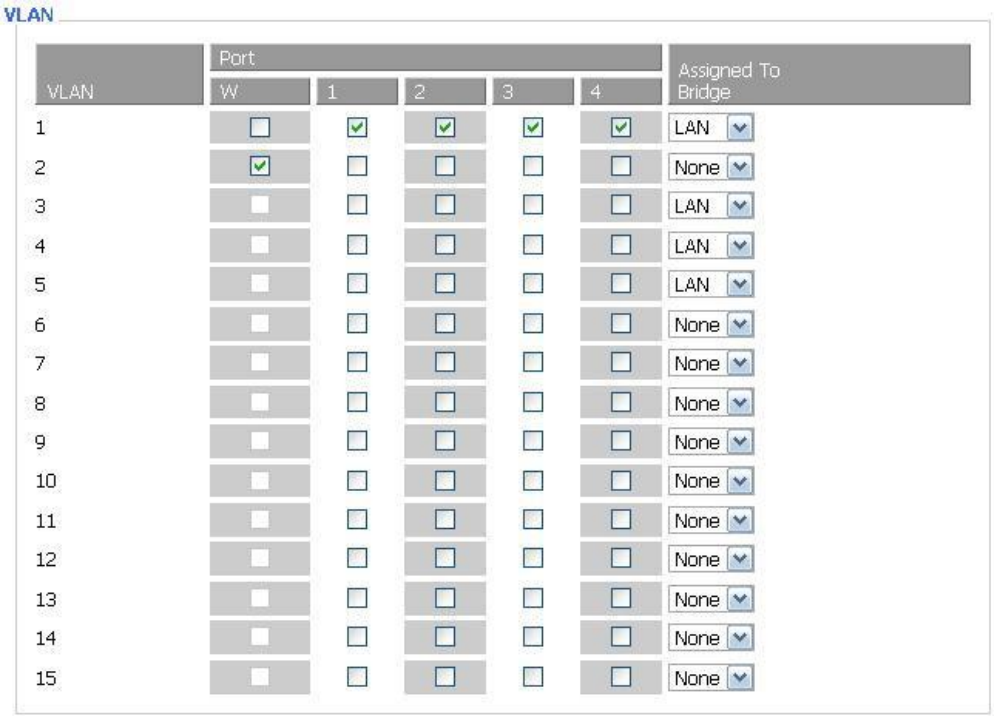
Gateway: IP address of the gateway device that allows for contact between the Router and the network or host.

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)

Show Routing Table:



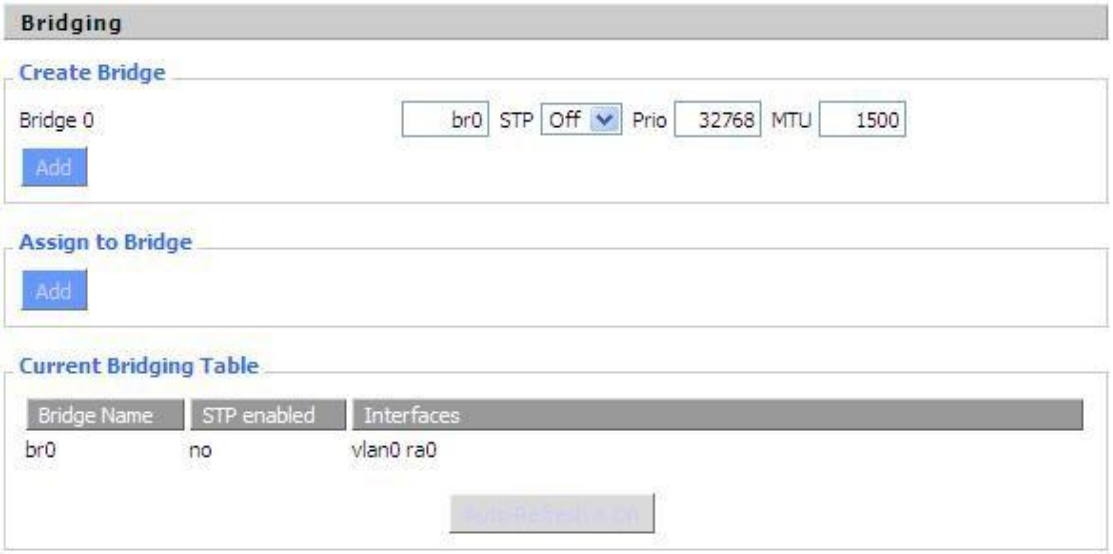
VLANs



VLANs function is to divide different VLAN ports by users' will. The system supports 15 VLAN port from VLAN1-VLAN15. However, there is only 5-time ports (1 WAN port and 4 LAN port) divided by users themselves, and LAN port and WAN port disable to divide into one VLAN port meanwhile.

 Copyright @ Yifan 2021

Networking



Bridging-Create Bridge: Creates a new empty network bridge for later use. STP means Spanning Tree Protocol and with PRIO users can set the bridge priority order. The lowest number has the highest priority.

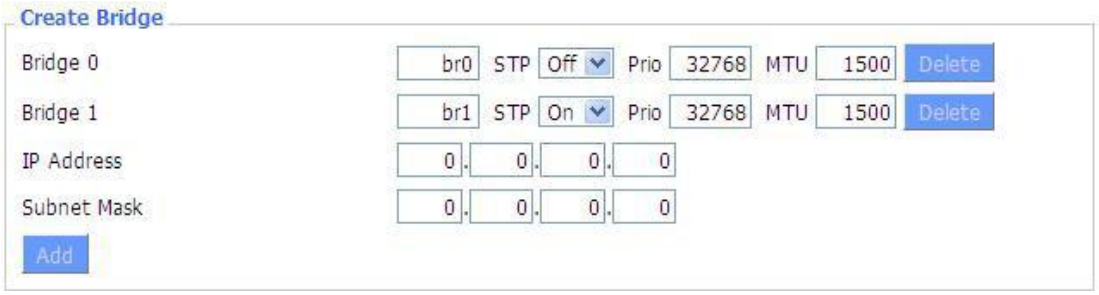
Bridging - Assign to Bridge: Allows users to assign any valid interface to a network bridge. Consider setting the Wireless Interface options to Bridged if they want to assign any Wireless Interface here. Any system specific bridge setting can be overridden here in this field.

Current Bridging Table: Shows current bridging table

Create steps as below:

Click 'Add' to create a new bridge, configuration is as below:

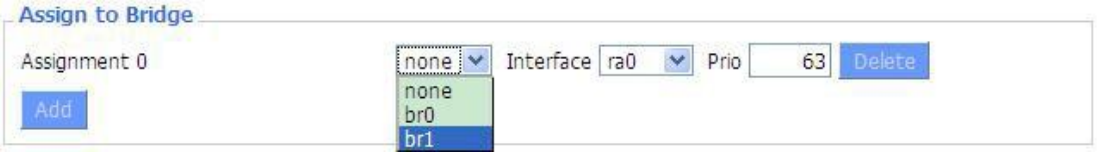
Create bridge option: the first br0 means bridge name. STP means to on/off spanning tree protocol. Prio means priority level of STP, the smaller the number, the higher the level. MTU means maximum transfer unit, default is 1500, delete if it is not need. And then click 'Save' or 'Add'. Brideproperties is as below:



 Copyright @ Yifan 2021

Enter relevant bridge IP address and subnet mask, click 'Add' to create a bridge.

Note: Only create a bride can apply it.



Assign to Bridge option: to assign different ports to created bridge. For example: assign port (wireless port) is ra0 in br1 bridge as below:

Prio means priority level: work if multiple ports are within the same bridge. The smaller the number, the higher the level. Click 'Add' to take it effect.

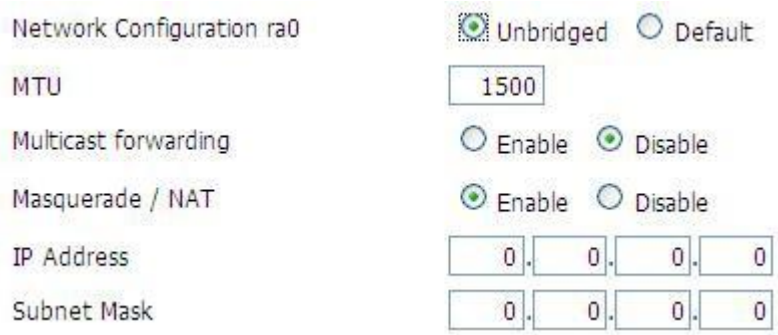
Note: corresponding interface of WAN ports interface should not bebinding, this bridge function is basically used for LAN port, and should not be binding with WAN port

If bind success, bridge binding list in the list of current bridging table is as below:

To make br1 bridge has the same function with DHCP assigned address, users need to set multiple DHCP function, see the introduction of multi-channel DHCPD:

 Copyright @ Yifan 2021

Port Setup: Set the port property, the default is not set



Choose not bridge to set the port's own properties, detailed properties are as below:
MTU: Maximum transfer unit
Multicast Forwarding：Enable or disable multicast forwarding Masquerade/NAT: enable or disable Masquerade/NAT
IP Address: Set ra0's IP address, and do not conflict with other ports or bridge Subnet
Mask: set the port's subnet mask

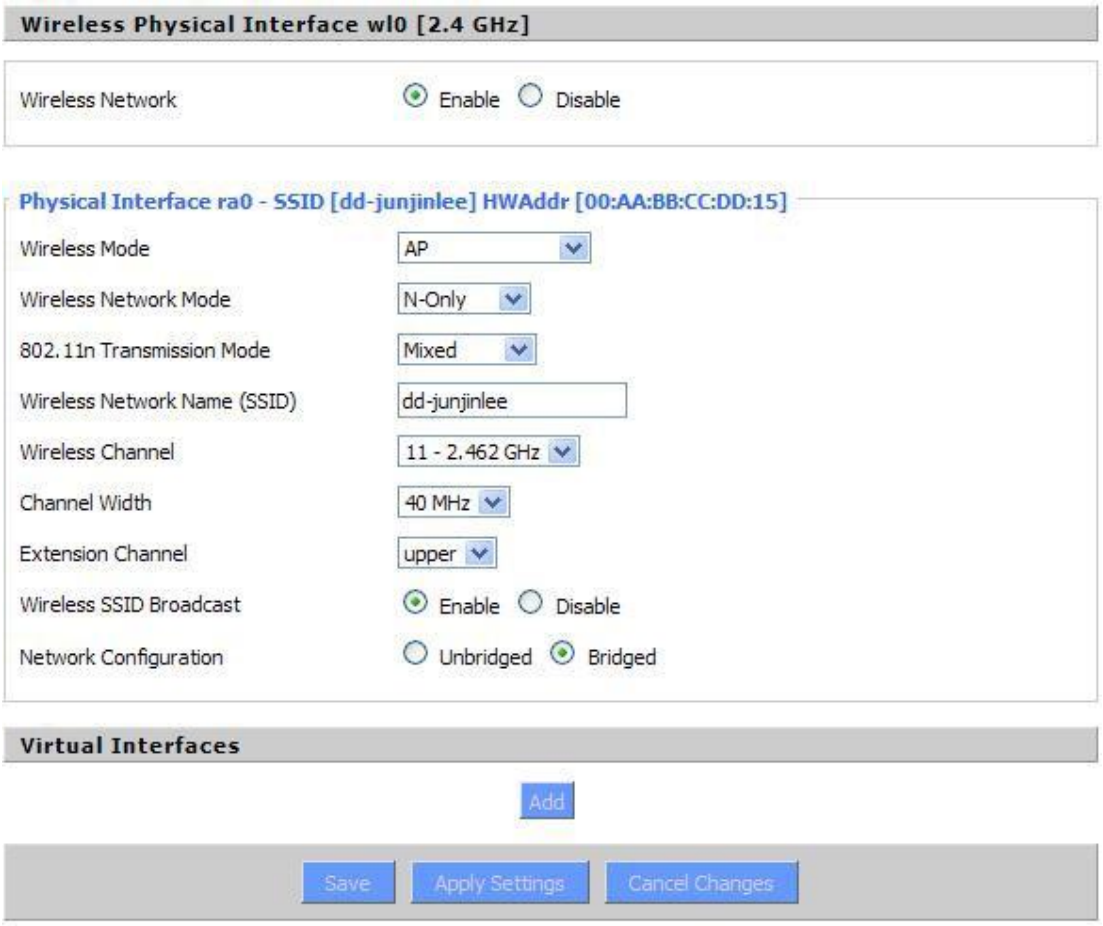
Multiple DHCPD: Using multiple DHCP service. Click 'Add' in multiple DHCP server to appear relevant configuration. The first means the name of port or bridge (do not be configured as eth0), the second means whether to on DHCP. Start means start address, Max means maximum assigned DHCP clients, Lease time means the client lease time, the unit is second, click 'Save' or 'Apply' to put it into effect after setting.

Note: Only configure and click 'Save' can configure the next, cannot configure multiple DHCP at the same time.

 Copyright @ Yifan 2021

3.3.2 Wireless

Basic Settings



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

Wireless Mode：AP, Client, Adhoc, Repeater, Repeater Bridge four options。

Wireless 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.

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.

5.8G: Support ac/na mode

8021.11n Transmission Mode ： In the wireless network mode to "N-only" choose to transfer its transmission mode.

 Copyright @ Yifan 2021

Greenfield: When you determine the surrounding environment, there is no other 802.11a/b/g devices use the same channel, use this mode to increase throughput. Other 802.11a/b/g devices use the same channel in the environment, the information you send may generate an error, re-issued.

Mixed This mode is contrary to the green mode but will reduce the throughput.

Wireless Network Name (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.

Wireless 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.

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

Wireless SSID Broadcast：

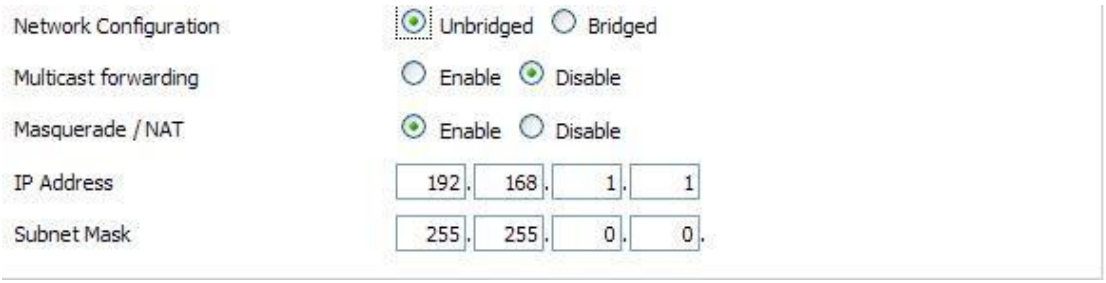
Enable：SSID broadcasting.

Disable：Hidden SSID.

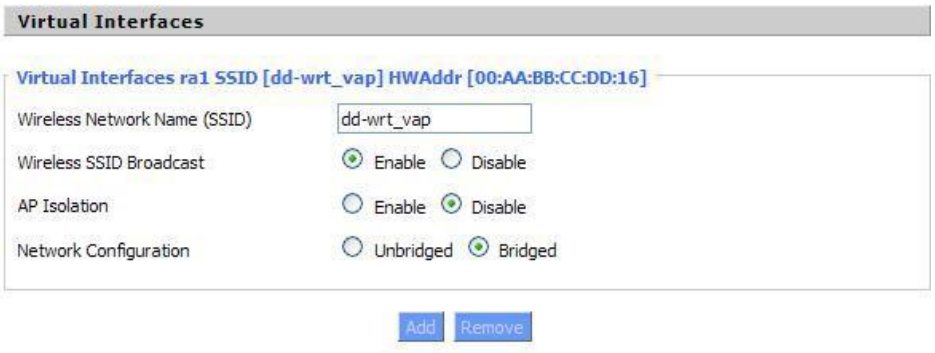
Network Configuration：

Bridged：Bridge to the Router, under normal circumstances, please select the bridge.

Unbridged：There is no bridge to the Router, IP addresses need to manually configure.



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



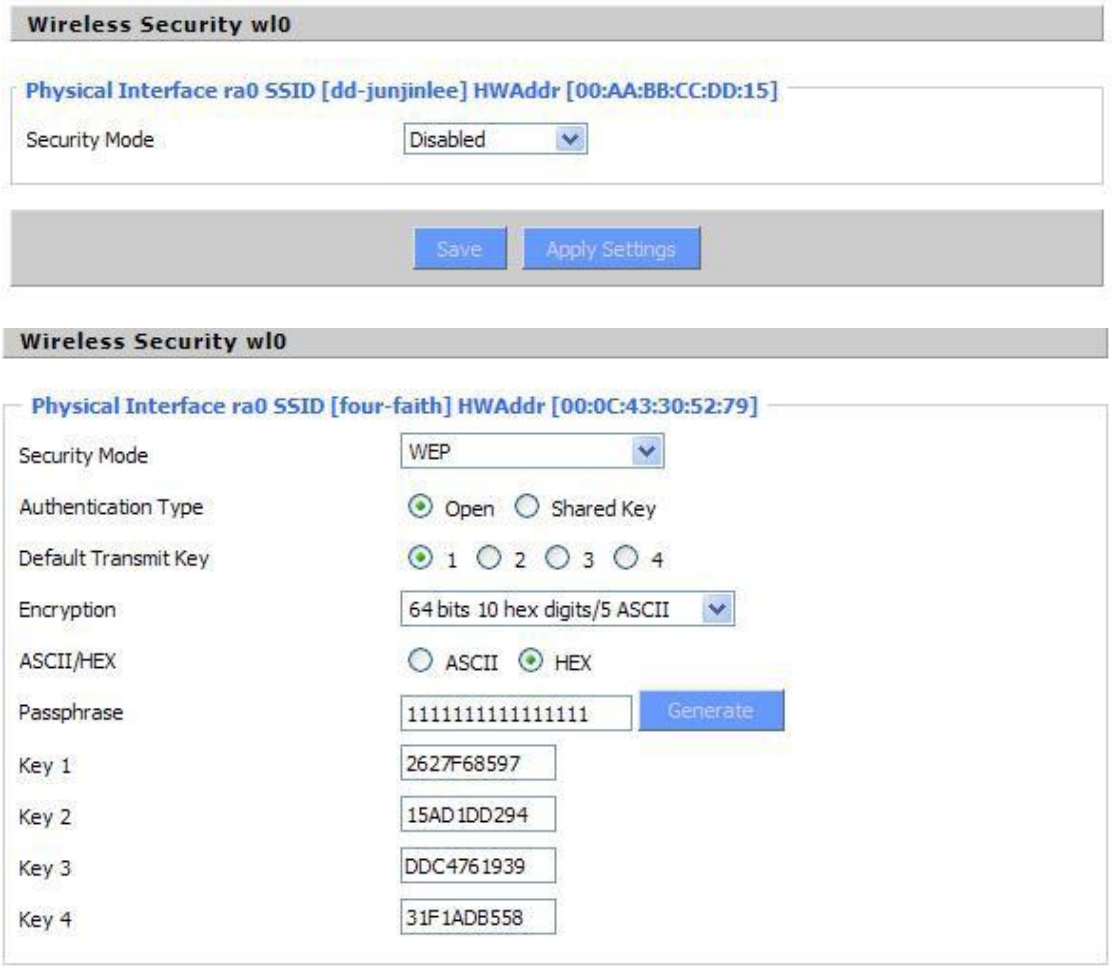
AP Isolation：This setting isolate wireless clients so access to and from other wireless clients are stopped.

 Copyright @ Yifan 2021

Note： Save your changes, after changing the "Wireless Mode", "Wireless Network Mode", "wireless width", "broadband" option, please click on this button, and then configure the other options.

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: It's a basic encryption algorithm is less secure than WPA. Use of WEP is discouraged due to security weaknesses, and one of the WPA modes shouldbe 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.

 Copyright @ Yifan 2021

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 four 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.

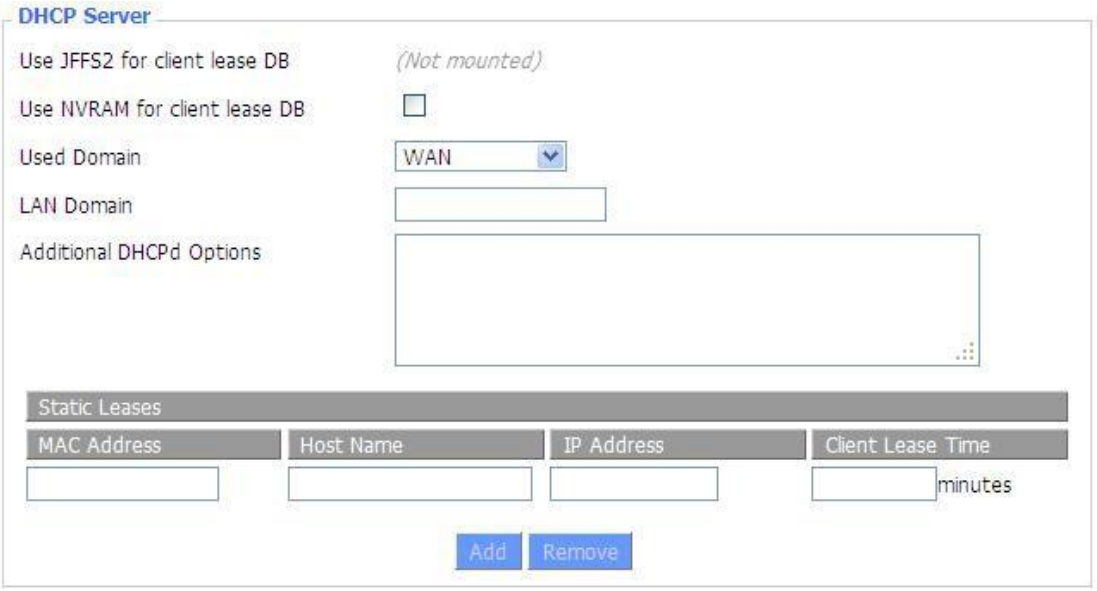
 Copyright @ Yifan 2021

3.3.3 Services

Services

DHCP Server

DHCP assigns IP addresses to users' local devices. While the main configuration is on the setup page users can program some nifty special functions here.



Use NVRAM for Client Lease DB: Users can store data to the system NVRAM area is enabled.

Used domain: Users can select here which domain the DHCP clients should get as their local domain. This can be the WAN domain set on the Setup screen or the LAN domain which can be set here.

LAN Domain: Users can define here their local LAN domain which is used as local domain for DNSmasq and DHCP service if chose above.

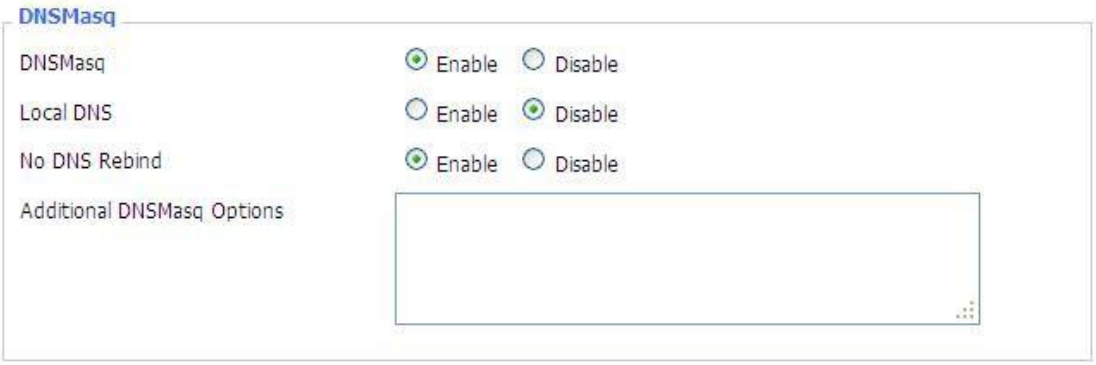
Static Leases: If users want to assign certain hosts a specific address, then they can define them here. This is also the way to add hosts with a fixed address to the Router's local DNS service (DNSmasq).

Additional DHCPd Options: Some extra options users can set by entering them

DNSMasq

DNSmasq is a local DNS server. It will resolve all host names known to the Router from dhcp (dynamic and static) as well as forwarding and caching DNS entries from remote DNS servers. Local DNS enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.

 Copyright @ Yifan 2021



Local DNS: Enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.
No DNS Rebind: When enabled, it can prevent an external attacker to access the Router's internal Web interface. It is a security measure
Additional DNSMasq Options: Some extra options users can set by entering them in Additional DNS Options.
For example:

Static Allocation: Dhcp-host=AB:CD: EF:11:22:33,192.168.0.10,myhost,myhost.domain,12h
Max Lease Number: Dhcp-lease-max=2
DHCP Server IP Range: Dhcp-range=192.168.0.110,192.168.0.111,12h

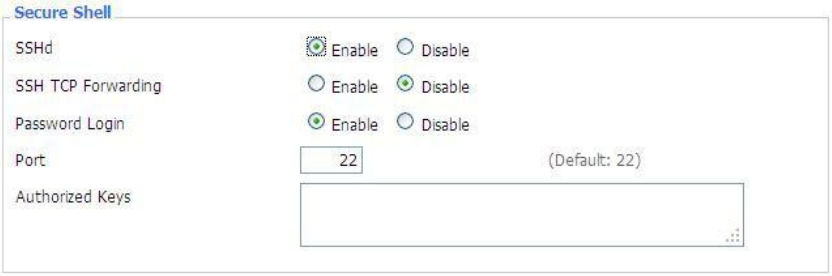
SNMP

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

 Copyright @ Yifan 2021

SSHD

Enabling SSHd allows users to access the Linux OS of their Router with an SSH client



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)

System log

Enable Syslog to capture system messages. By default they will be collected in the local file /var/log/messages. To send them to another system, enter the IP address of a remote syslog server.

Syslog Out Mode: Two log mode

Net: The log information output to a syslog server

Console: The log information output to console port

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

Telnet

Telnet: Enable a telnet server to connect to the Router with telnet. The username is admin and the password is the Router's password.

Note: If users use the Router in an untrusted environment (for example as a public hotspot), it is strongly recommended to use SSHd and deactivate telnet.

WAN Traffic Counter

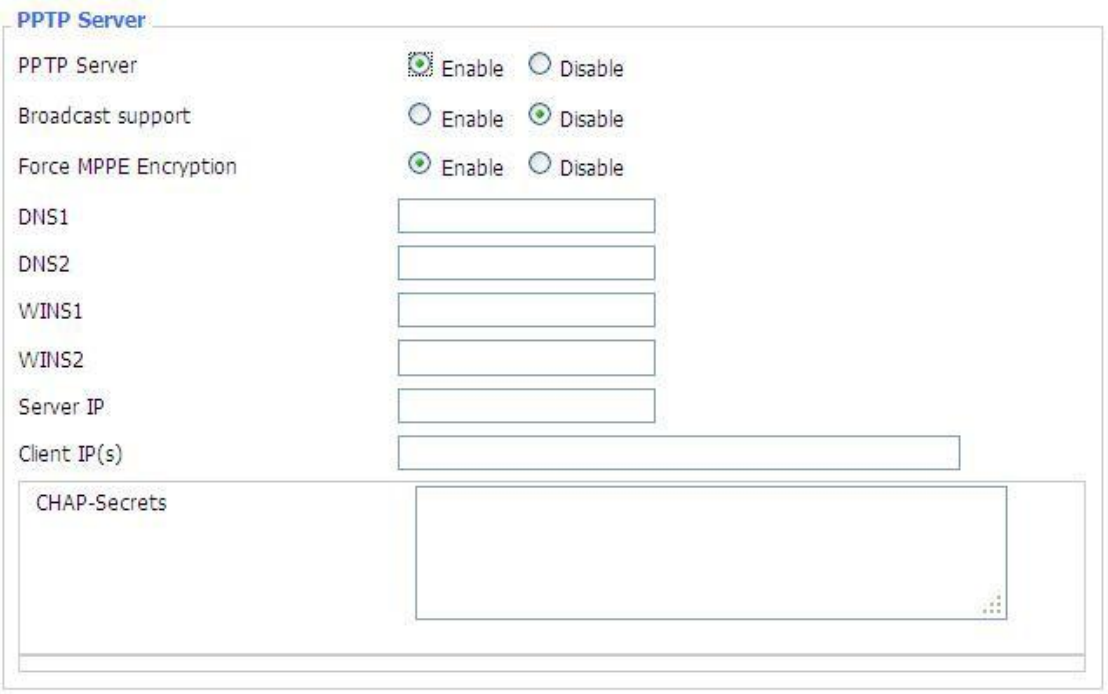
 Copyright @ Yifan 2021

Ttraff Daemon: Enable or disable wan traffic counter function

3.3.4 VPN

1. PPTP

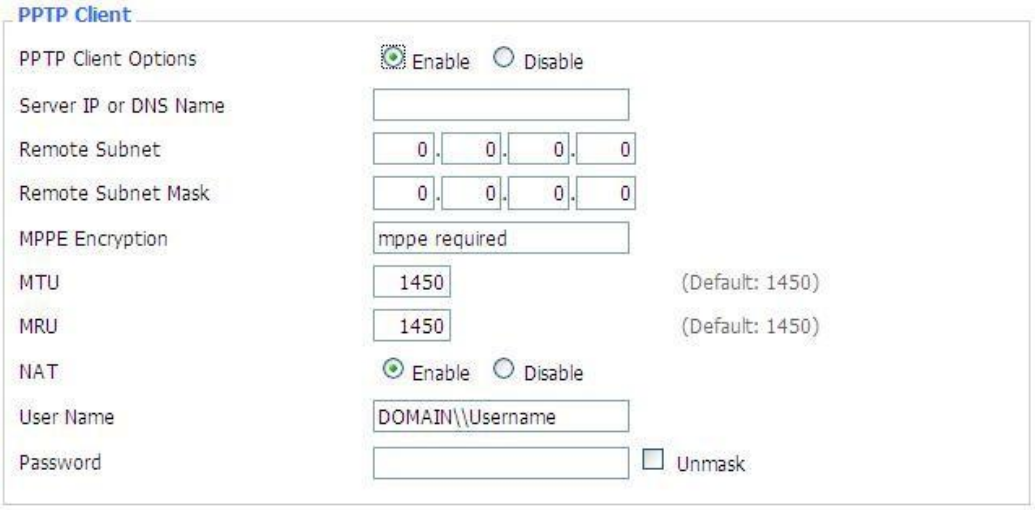
PPTP Server



Broadcast Support: Enable or disable broadcast support of PPTP server
Force MPPE Encryption: Enable of disable force MPPE encryption of PPTP data
DNS1/DNS2/WINS1/WINS2: Set DNS1/DNS2/WINS1/WINS2
Server IP: Input IP address of the Router as PPTP server, differ from LAN address
Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx
CHAP Secrets: Username and password of the client using PPTP service
Note: Client IP must be different with IP assigned by Router DHCP. The format of CHAP Secrets is user * password *.

 Copyright @ Yifan 2021

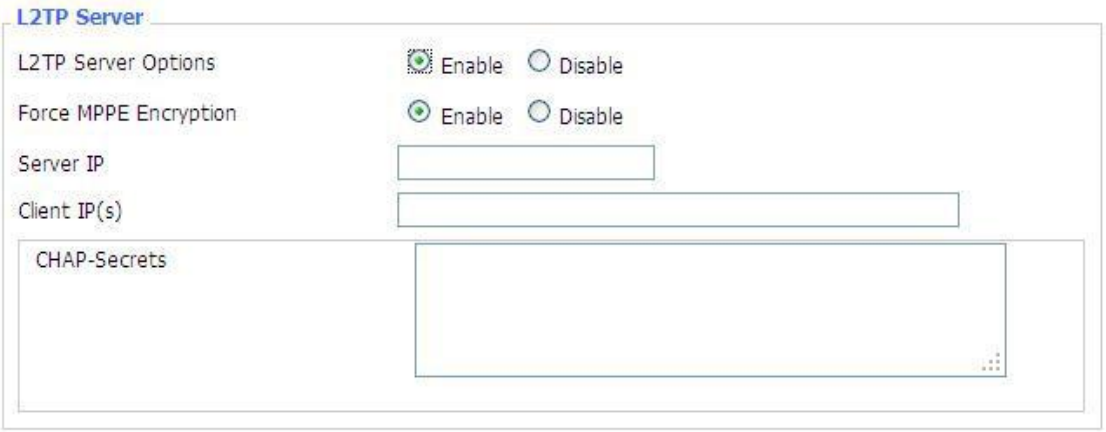
PPTP Client



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
MPPE Encryption: Enable or disable Microsoft Point-to-Point Encryption。
MTU: Maximum Transmission Unit
MRU: Maximum Receive Unit
NAT: Network Address Translation
Username: User name to login PPTP Server.
Password: Password to log into PPTP Server.

2. L2TP

L2TP Server



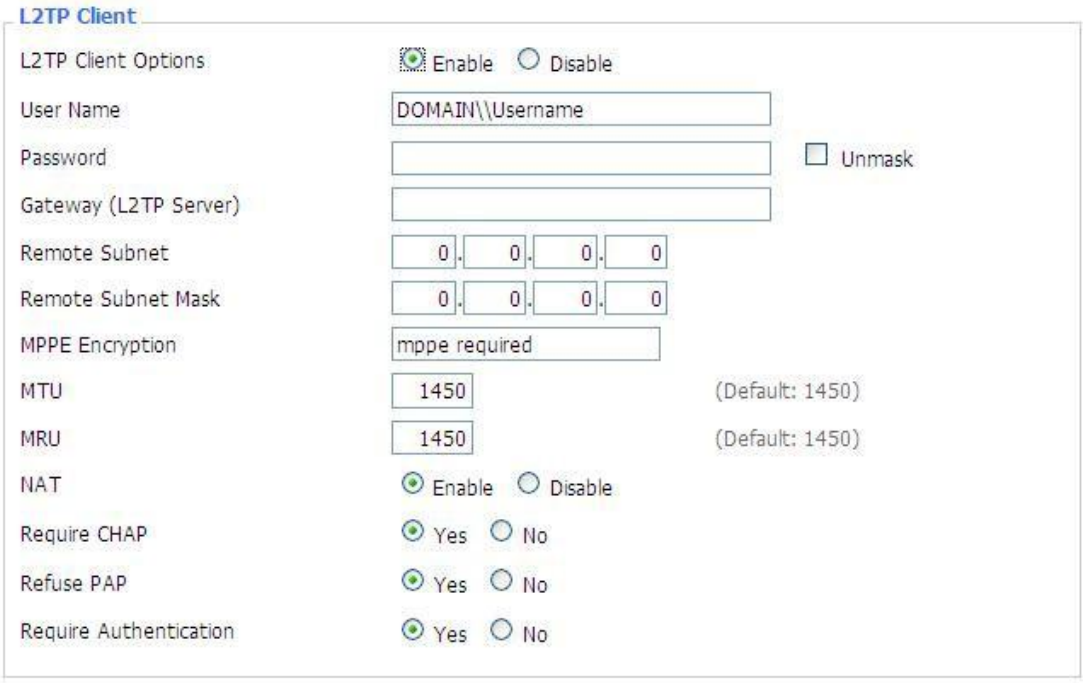
Force MPPE Encryption: Enable or disable force MPPE encryption of L2TP data
Server IP: Input IP address of the Router as PPTP server, differ from LAN address
Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx
CHAP Secrets: Username and password of the client using L2TP service

 Copyright @ Yifan 2021

Note: Client IP must be different with IP assigned by Router DHCP.

The format of CHAP Secrets is user * password *.

L2TP Client



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
MPPE Encryption: Enable or disable Microsoft Point-to-Point Encryption
MTU: Maximum transmission unit
MRU: Maximum receive unit
NAT: Network address translation
Username: Username to login L2TP Server
Password: Password to login L2TP Server
Require CHAP: Enable or disable support chap authentication protocol
Refuse PAP: Enable or disable refuse to support the pap authentication
Require Authentication: Enable or disable support authentication protocol

 Copyright @ Yifan 2021

3. OPENVPN

OPENVPN Server

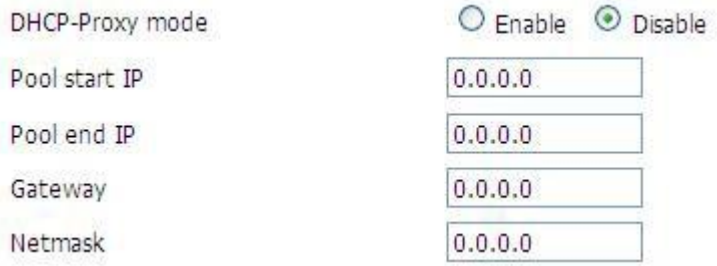
Start Type: WAN UP----start after on-line, System----------start when boot up

Config via: GUI----Page configuration, Config File---------- config File configuration
Server Mode: Router (TUN)-route mode, Bridge (TAP)---------- bridge mode

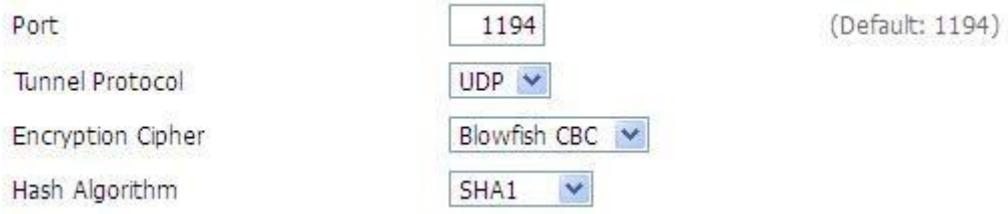
Router (TUN):

Network: Network address allowed by OPENVPN server
Netmask: Netmask allowed by OPENVPN server

Bridge (TAP):



DHCP-Proxy mode: Enable or disable DHCP-Proxy mode
Pool start IP: Pool start IP of the client allowed by OPENVPN server
Pool end IP: Pool end IP of the client allowed by OPENVPN server
Gateway: The gateway of the client allowed by OPENVPN server



 Copyright @ Yifan 2021

Netmask: Netmask of the client allowed by OPENVPN server

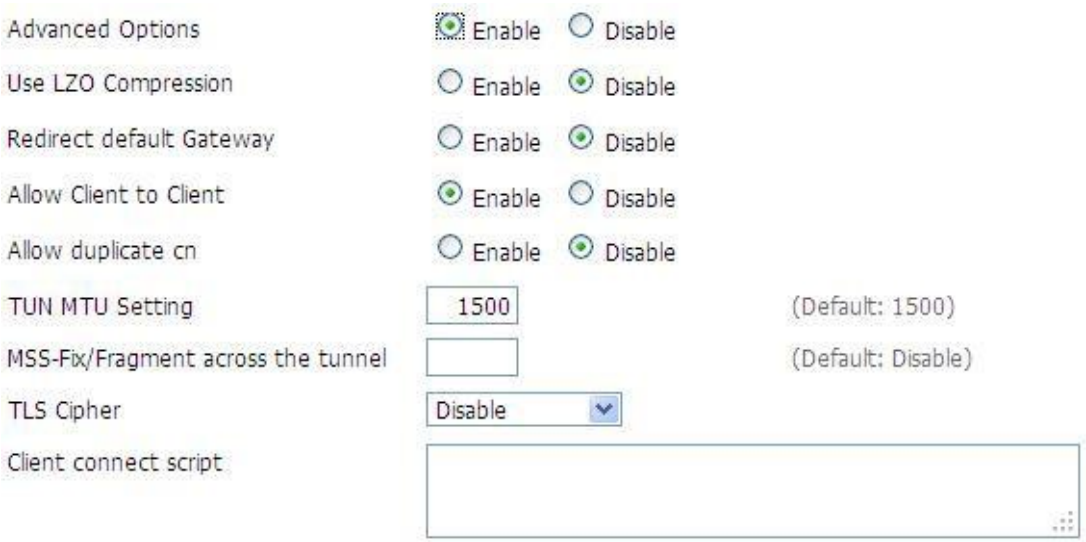
Port: Listen port of OPENVPN server

Tunnel Protocol: UCP or TCP of OPENVPN tunnel protocol

Encryption Cipher: Blowfish CBC，AES-128 CBC，AES-192 CBC，AES-256 CBC， AES-512 CBC

Hash Algorithm: Hash algorithm provides a method of quick access to data, including SHA1，SHA256，SHA512，MD5

Advanced Options



Use LZO Compression: Enable or disable use LZO compression for data transfer

Redirect Default Gateway: Enable or disable redirect default gateway

Allow Client to Client: Enable or disable allow client to client

Allow Duplicate cn: Enable or disable allow duplicate cn

TUN MTU Setting: Set the value of TUN MTU

TCP MSS: MSS of TCP data

TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA

Client Connect Script: Define some client script by user self

CA Cert: CA certificate

 Copyright @ Yifan 2021

Public Server Cert: Server certificate

Private Server Key: The key selected by the server
DH PEM: PEM of the server

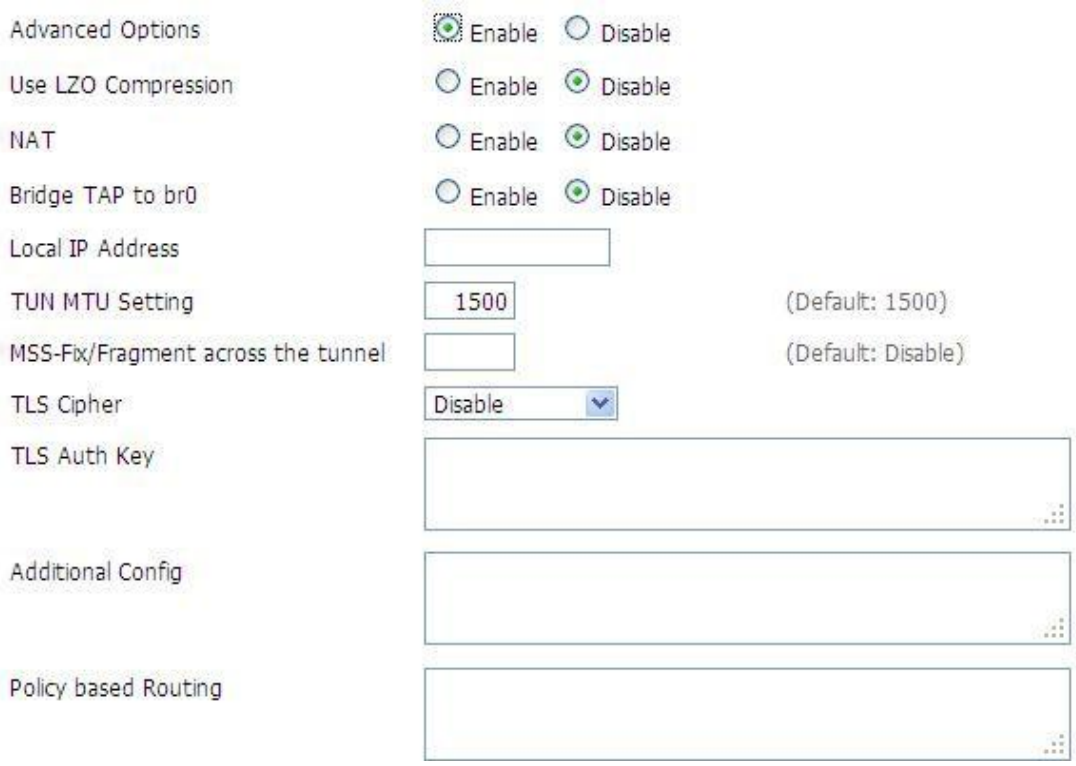
Additional Config: Additional configurations of the server
CCD-Dir DEFAULT file: Other file approaches
TLS Auth Key: Authority key of Transport Layer Security
Certificate Revoke List: Configure some revoke certificates

OPENVPN Client

Server IP/Name: IP address or domain name of OPENVPN server
Port: Listen port of OPENVPN client

 Copyright @ Yifan 2021

Tunnel Device: TUN----Router mode, TAP ---------- Bridge mode
Tunnel Protocol: UDP and TCP protocol
Encryption Cipher: Blowfish CBC，AES-128 CBC，AES-192 CBC，AES-256 CBC， AES-512 CBC
Hash Algorithm: Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, MD5
NsCertType Verification: Support ns certificate type



Use LZO Compression: Enable or disable use LZO compression for data transfer
NAT: Enable or disable NAT through function
Bridge TAP to br0: Enable or disable bridge TAP to br0
Local IP Address: Set IP address of local OPENVPN client
TUN MTU Setting: Set MTU value of the tunnel
TCP MSS: Mss of TCP data
TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA
TLS Auth Key: Authority key of Transport Layer Security
Additional Config: Additional configurations of OPENVPN server
Policy Based Routing: Input some defined routing policy

 Copyright @ Yifan 2021

CA Cert: CA certificate
Public Client Cert: Client certificate
Private Client Key: Client key

4. IPSEC

Connect Status and Control

Show IPSEC connection and status of current Router on IPSEC page.

Name: The name of IPSEC connection
Type: The type and function of current IPSEC connection
Common Name: Local subnet, local address, opposite end address and opposite end subnet of current connection
Status: Connection status: closed, negotiating, establish

Closed: This connection does not launch a connection request to opposite end

Negotiating: This connection launch a request to opposite end, is under negotiating, the connection has not been established yet

Establish: The connection has been established, enabled to use this tunnel
Action: The action of this connection, current is to delete, edit, reconnect and enable

Delete: To delete the connection, also will delete IPSEC if IPSEC has set up

Edit: To edit the configure information of this connection, reload this connection to make the configuration effect after edit

Reconnect: This action will remove current tunnel, and re-launch tunnel establish request

Enable: When the connection is enabled, it will launch tunnel establish request when the system reboot or reconnect, otherwise the connection will not do it

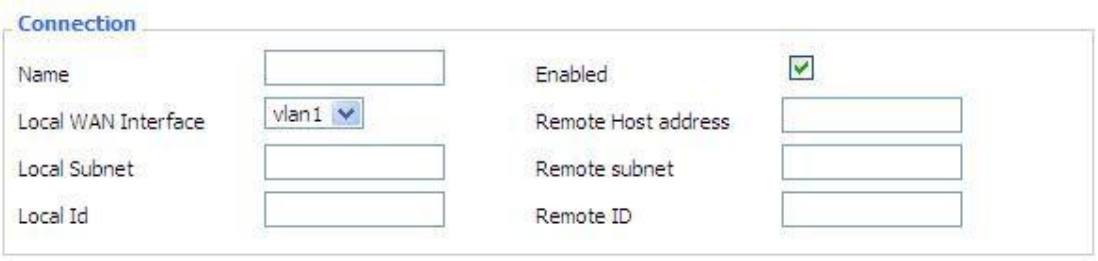
Add: To add a new IPSEC connection

 Copyright @ Yifan 2021

Add IPSEC connection or edit IPSEC connection

Type: To choose IPSEC mode and relevant functions in this part, supports tunnel mode client, tunnel mode server and transfer mode currently

Connection: This part contains basic address information of the tunnel



Name: To 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 cannot 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 cannot 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 cannot 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
Detection: This part contains configure information of connection detection

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
Advanced Settings: This part contains relevant setting of IKE, ESP, negotiation mode, etc.

 Copyright @ Yifan 2021

Enable Advanced Settings: Enable to configure 1st and 2nd phase information, otherwise it will automatic negotiation according to opposite end
IKE Encryption: IKE phased encryption mode
IKE Integrity: IKE phased integrity solution
IKE Grouptype: DH exchange algorithm
IKE Lifetime: Set IKE lifetime, current unit is hour, the default is 0
ESP Encryption: ESP encryption type
ESP Integrity: ESP integrity solution
ESP 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

Negotiate Payload Compression: Tick to enable PFS, non-tick to disable PFS
Authentication: choose use share encryption option or certificate authentication option. Current is only to choose use share encryption option.

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).

 Copyright @ Yifan 2021

GRE Tunnel: Enable or disable GRE function

Number：Switch on/off GRE tunnel app

Status：Switch on/off someone GRE tunnel app

Name：GRE tunnel name

Through：The GRE packet transmit interface

Peer Wan IP Addr：The remote WAN address

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

Peer Tunnel IP：The remote tunnel IP address

Local Tunnel IP：The local tunnel IP address

Local Netmask：Netmask of local network

Keepalive：Enable or disable GRE Keepalive function

Retry times：GRE keepalive detect fail retries

Interval：The time interval of GRE keepalive packet sent

Fail Action：The action would be exec after keeping alive failed Click on "**View GRE tunnels**" keys can view the information of GRE

 Copyright @ Yifan 2021

3.3.5 Security

Firewall

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

Firewall Protection

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.

Additional Filters

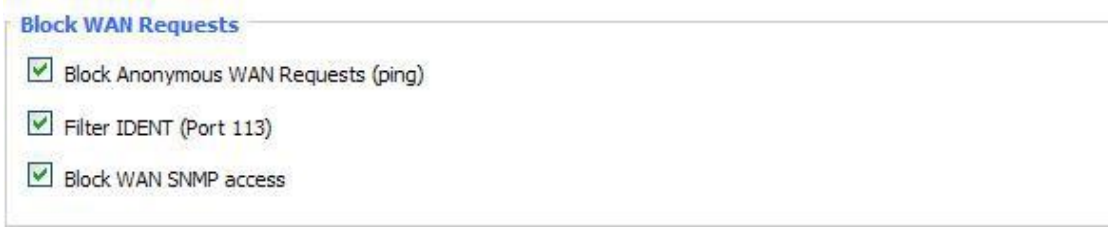
Filter Proxy: Wan proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

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.

Prevent WAN Request



Block Anonymous WAN Requests (ping): By selecting “Block Anonymous WAN Requests (ping)” box to enable this feature, you can prevent your network

 Copyright @ Yifan 2021

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.

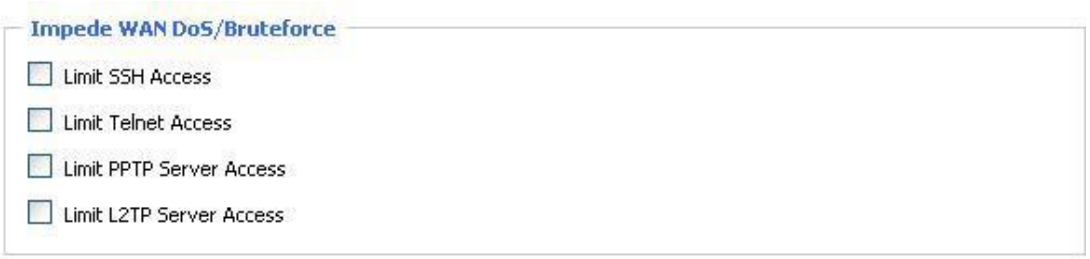
Filter IDENT (Port 113): Enable this feature can prevent port 113 from being scaned from outside. Click the check box to enable the function otherwise disabled.

Block WAN SNMP Access: This feature prevents the SNMP connection requests from the WAN. After Complete the changes, click the

Save Settings: Button to save your changes. Click the

Cancel Changes: Button to cancel unsaved changes.

Impede WAN DoS/Bruteforce



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.

Limit PPTP Server Access: When build a PPTP Server in the Router, 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.

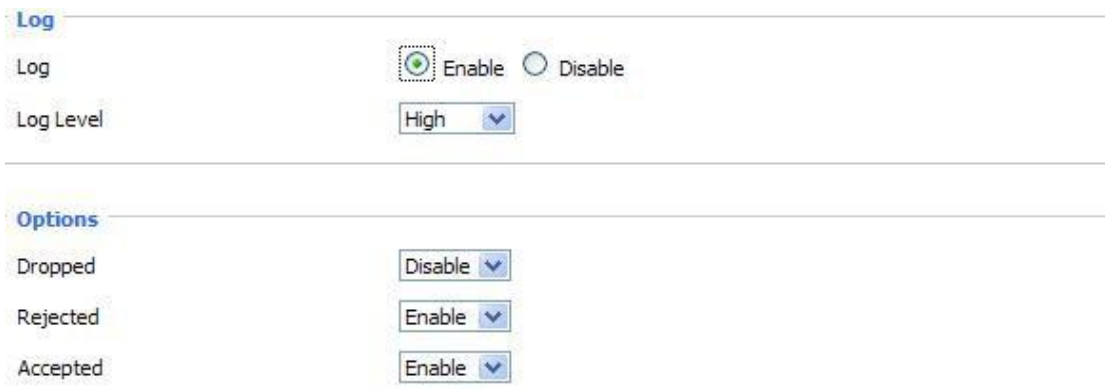
Limit L2TP Server Access: When build a L2TP Server in the Router, this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Log Management

The Router can keep logs of all incoming or outgoing traffic for your Internet connection.

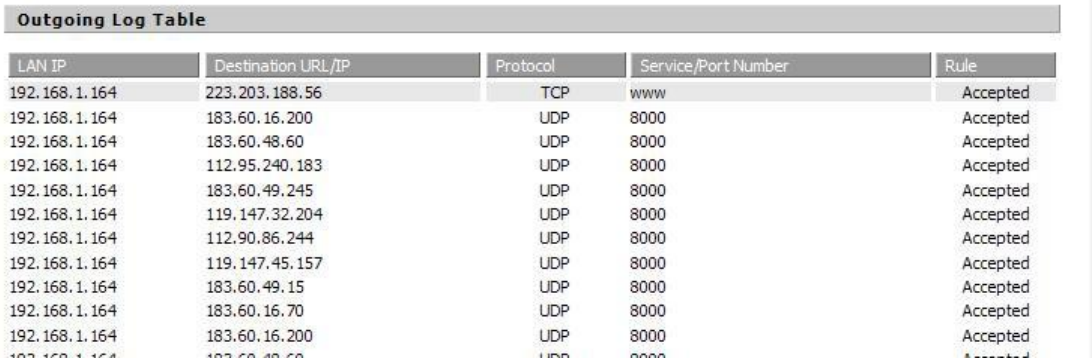
Log: To keep activity logs, select Enable. To stop logging, select Disable.When select enable, the following page will appear.

 Copyright @ Yifan 2021



Log Level: Set this to the required log level. Set Log Level higher to log more actions.
Options: When select Enable, the corresponding connection will be recorded in the journal, the disabled are not recorded.
Incoming Log: To see a temporary log of the Router's most recent incoming traffic, click the Incoming Log button.

Outgoing Log: To see a temporary log of the Router's most recent outgoing traffic, click the Outgoing Log button.



Outgoing Log Table

LAN IP	Destination URL/IP	Protocol	Service/Port Number	Rule
192.168.1.164	223.203.188.56	TCP	www	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted
192.168.1.164	112.95.240.183	UDP	8000	Accepted
192.168.1.164	183.60.49.245	UDP	8000	Accepted
192.168.1.164	119.147.32.204	UDP	8000	Accepted
192.168.1.164	112.90.86.244	UDP	8000	Accepted
192.168.1.164	119.147.45.157	UDP	8000	Accepted
192.168.1.164	183.60.49.15	UDP	8000	Accepted
192.168.1.164	183.60.16.70	UDP	8000	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted

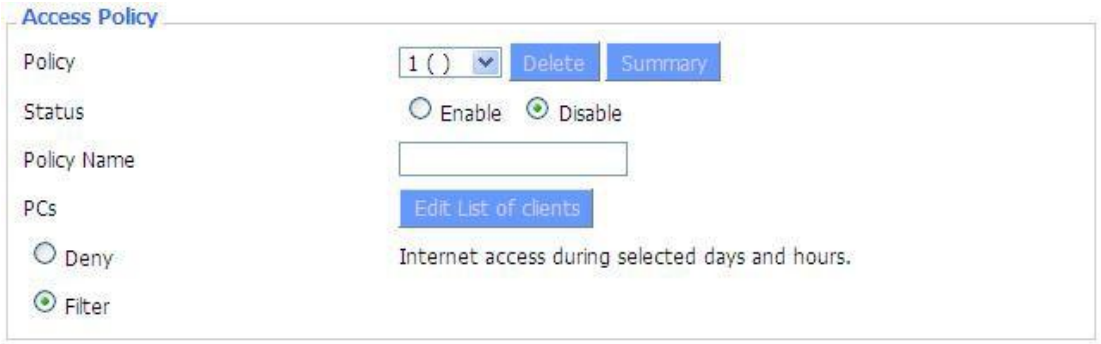
Click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

 Copyright @ Yifan 2021

3.3.6 Access Restrictions

WAN Access

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.

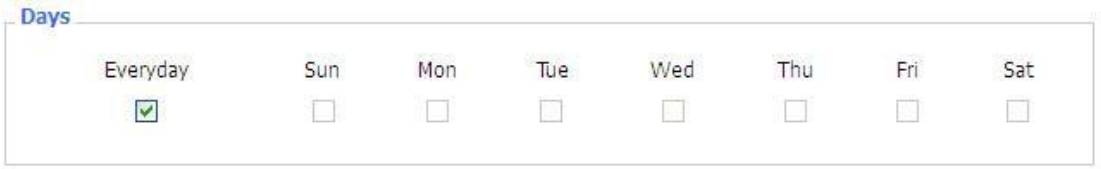
Two options in the default policy rules: "Filter" and "reject". If select "Deny", you will deny specific computers to access any Internet service at a particular time period. If you choose to "filter"， It will block specific computers to access the specific sites at a specific time period. You can set 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.

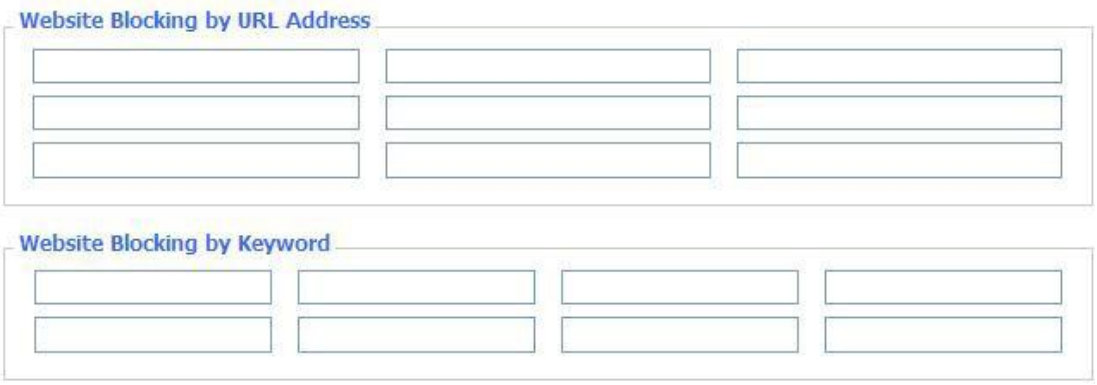
PCs: The part is used to edit client list, the strategy is only effective for the PC in the list.

Days: Choose the day of the week you would like your policy to be applied.



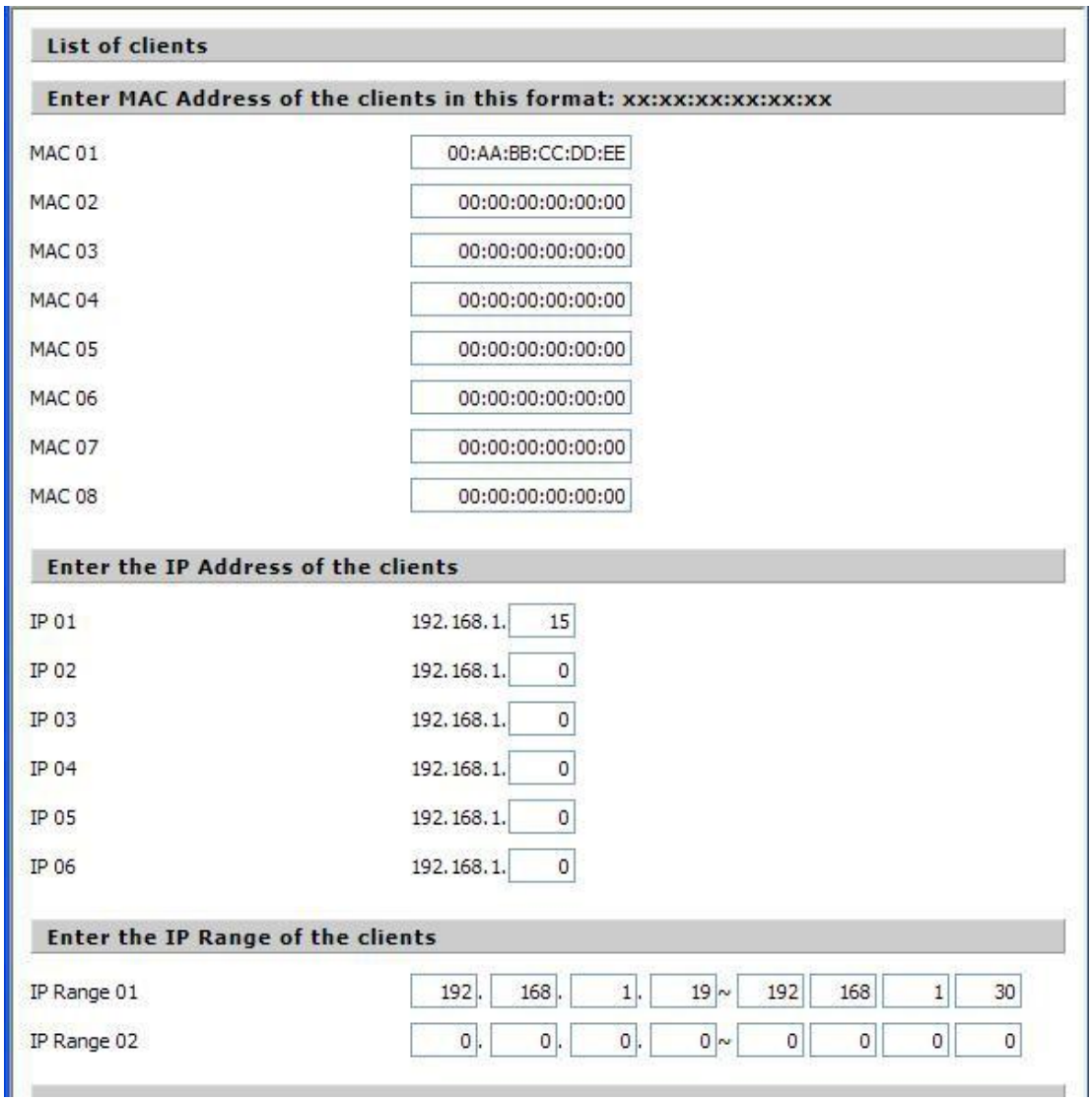
 Copyright @ Yifan 2021

Times: Enter the time of the day you would like your policy to be applied.



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 their webpage



 Copyright @ Yifan 2021

Set up Internet access policy

1. Select the policy number (1-10) in the drop-down menu.
2. For this policy is enabled, click the radio button next to "Enable"
3. Enter a name in the Policy Name field.
4. Click the Edit List of PCs button.
5. 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.
6. 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.
7. 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.
8. Set the days when access will be filtered. Select Everyday or the appropriate days of the week.
9. 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.
10. Click the Add to Policy button to save your changes and active it.
11. To create or edit additional policies, repeat steps 1-9.
12. To delete an Internet Access Policy, select the policy number, and click the Delete button.

Note:

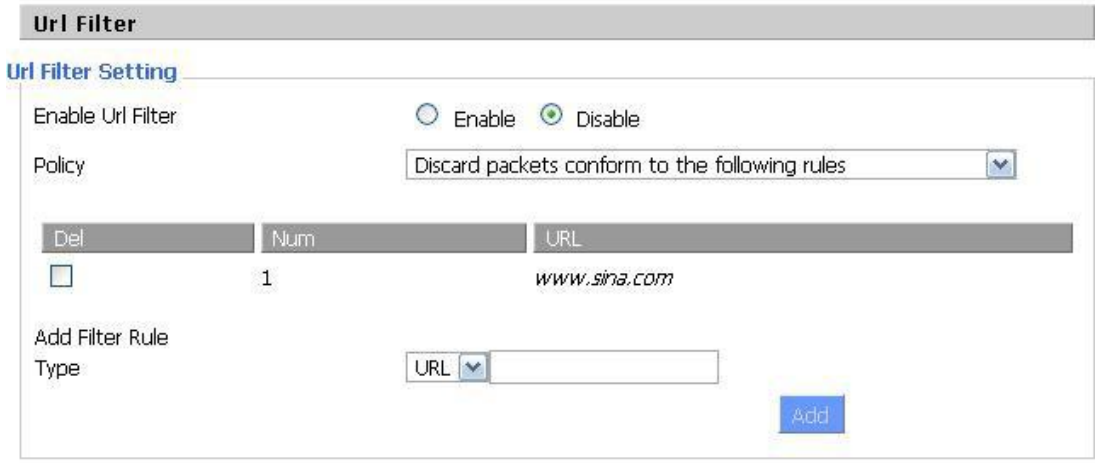
1. The default factory value of policy rules is "filtered". If the user chooses the default policy rules for "refuse", and editing strategies to save or directly to save the settings. If the strategy edited is the first, it will be automatically saved into the second, if not the first, keep the original number.
2. 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 recalibrate to ensure the correct implementation of the relevant period control function.

 Copyright @ Yifan 2021

URL Filter

If you want to prevent certain client access to specific network domain name, such as www.sina.com. We can achieved it through the function of URL filter.

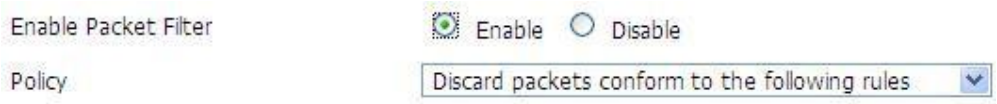
URL filtering function



Discard packets conform to the following rules: Only discard the matching URL address in the list.

Accept only the data packets conform to the following rules: Receive only with custom rules of network address, discarded all other URL address.

Packet Filter



To block some packets getting Internet access or block some Internet packets getting local network access, you can configure filter items to block these packets. Packet Filter Packet filter function is realized based on IP address or port of packets.

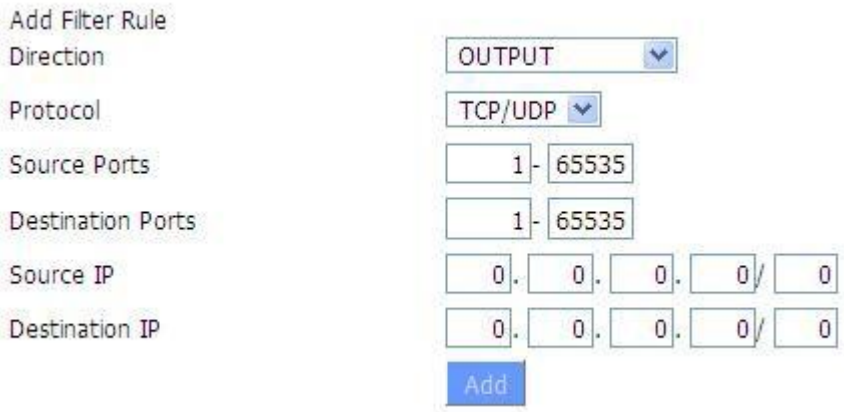
Enable Packet Filter: Enable or disable “packet filter” function

Policy: The filter rule’s policy, you can choose the following options

Discard The Following--Discard packets conform to the following rules, Accept all other packets

 Copyright @ Yifan 2021

Only Accept The Following-- Accept only the data packets conform to the following rules, Discard all other packets



Direction

input: Packet from WAN to LAN

output: Packet from LAN to WAN

Protocol: Packet protocol type

Source Ports: Packet's source port

Destination Ports: Packet's destination port

Source IP: Packet's source IP address

Destination IP: Packet's destination IP address

Note: "Source Port","Destination Port" ,"Source IP" ,"Destination IP" could not be all empty ,you have to input at least one of these four parameters.

 Copyright @ Yifan 2021

3.3.7 NAT

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. If you want to forward a whole range of ports, see Port Range Forwarding.

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 checkbox to enable port forwarding for the application. Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

 Copyright @ Yifan 2021

Port Range Forward

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. If you only want to forward a single port, see Port Forwarding.

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 see by users on the Internet and forwarded to your PC.

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

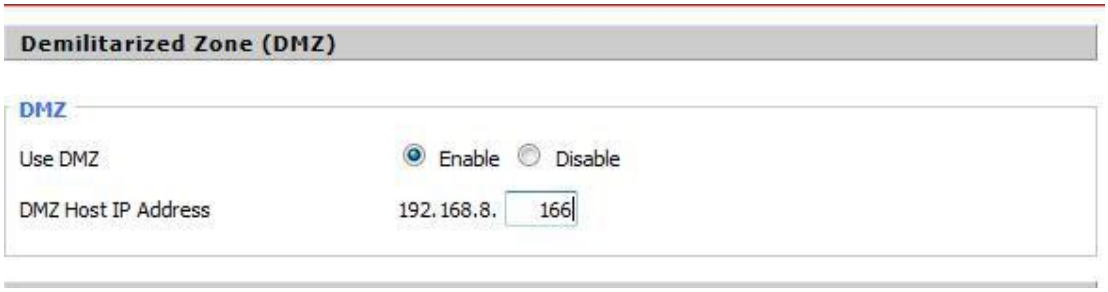
Protocol: Chose the right protocol TCP, UDP or Both. Set this to what the application requires.

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

Enable: Click the Enable checkbox to enable port forwarding for the application. Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

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 video conferencing. 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 should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

 Copyright @ Yifan 2021

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

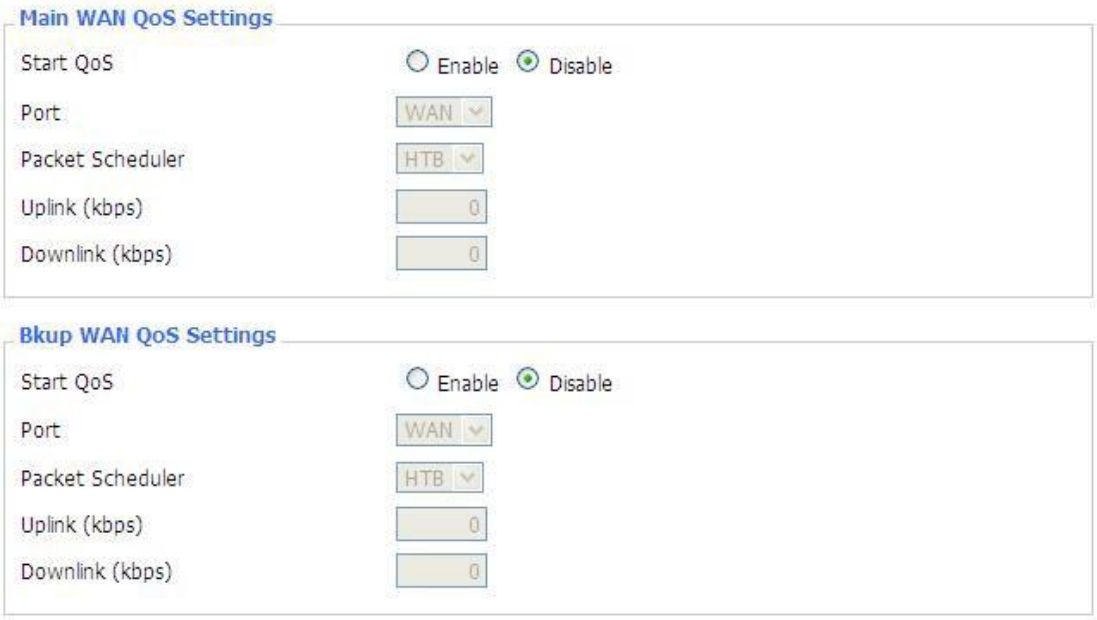
Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.8 QoS Setting

Basic

Bandwidth management prioritizes the traffic on your Router. Interactive traffic (telephony, browsing, telnet, etc.) gets priority and bulk traffic (file transfer, P2P) gets low priority. The main goal is to allow both types to live side-by side without unimportant traffic disturbing more critical things. All of this is automatic.

QoS allows control of the bandwidth allocation to different services, netmasks, MAC addresses and the four LAN ports.



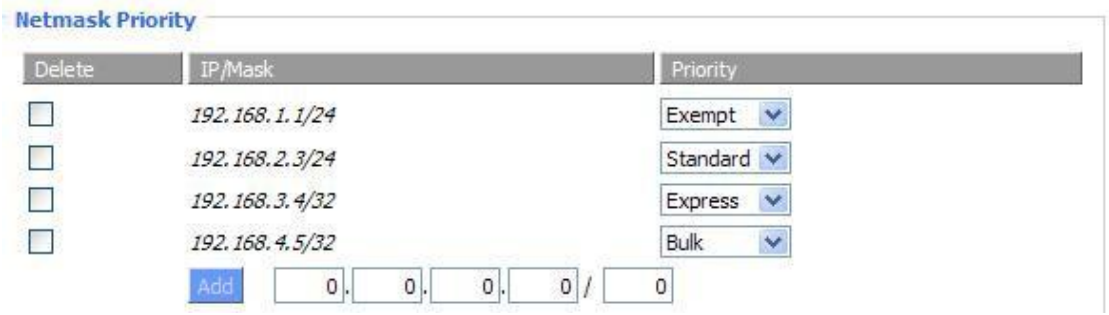
Uplink (kbps)： In order to use bandwidth management (QoS) you must enter bandwidth values for your uplink. These are generally 80% to 90% of your maximum bandwidth.

Downlink (kbps)： 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.

 Copyright @ Yifan 2021

Classify

Netmask Priority

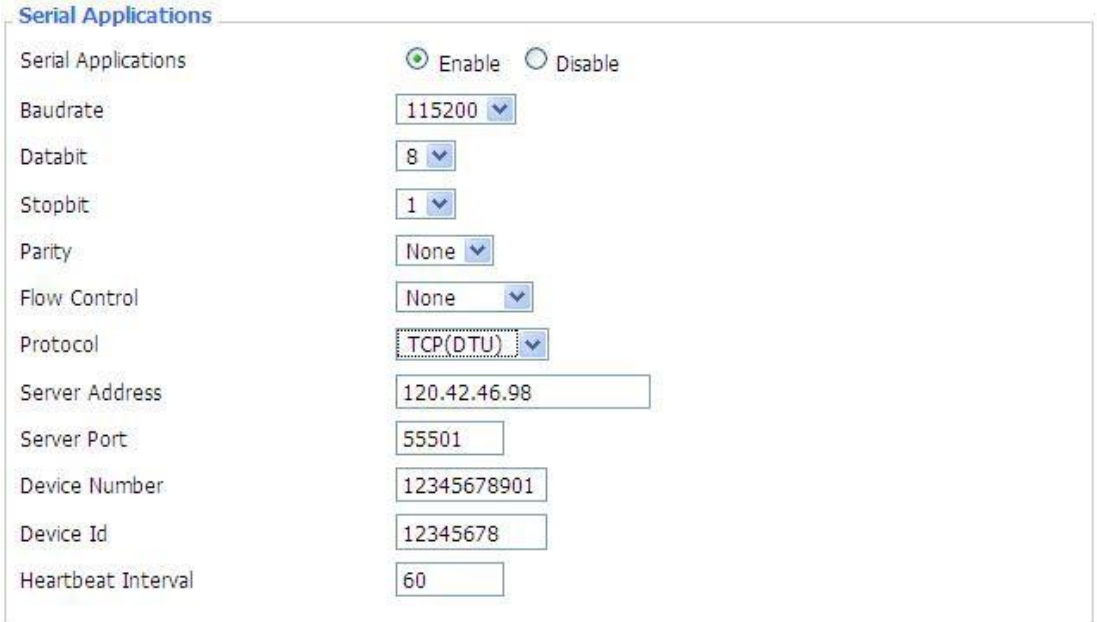


You may specify priority for all traffic from a given IP address or IP Range. Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.9 Applications

Serial Applications

There is a console port on router. Normally, this port is used to debug the router. This port 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).



 Copyright @ Yifan 2021

Baudrate: Baud rate indicates the number of bytes per second transported by device, commonly used baud rate is115200, 57600, 38400, 19200.

Databit: The data bits can be 4, 5, 6, 7, 8, constitute a character. The ASCII code is usually used. Starting from the most significant bit is transmitted.

Stopbit: It marks the end of a character data. It is a high level of 1, 1.5, 2.

Parity: Use a set of data to check the data error.

Flow Control: Including the hardware part and software part in two ways.

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 Yifan IP MODEM device 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 Yifan P MODEM device 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 ID: The router's identity ID.

Device Number: The router's phone number.

Heartbeat Interval: The time interval to send heartbeat 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"

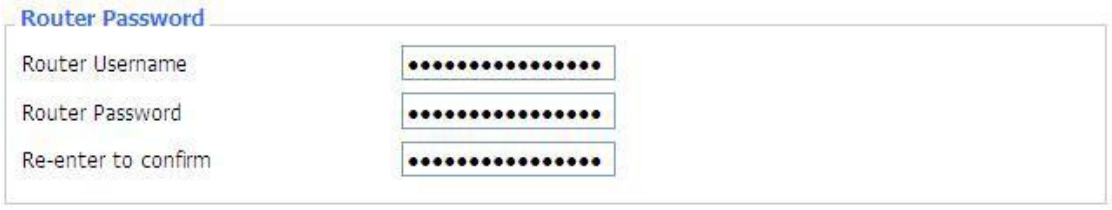
Custom Registration Packets: This item is valid when Protocol Type is "TCST"

 Copyright @ Yifan 2021

3.3.10 Administration

Management

The Management screen allows you to change the Router's settings. On this page you will find most of the configurable items of the router code.



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：

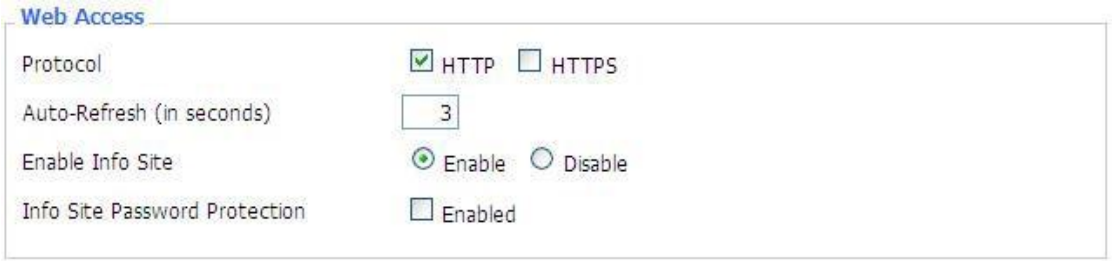
Default username is admin.

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.

Web Access

This feature allows you to manage the router using either HTTP protocol or the HTTPS protocol. If you choose to disable this feature, a manual reboot will be required. You can also activate or not the router information web page. It's now possible to password protect this page (same username and password than above).

Protocol ：



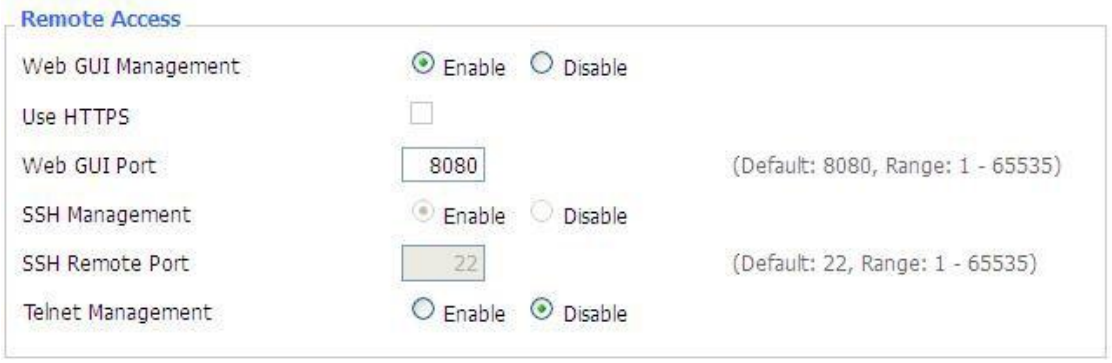
This feature allows you to manage the Router using either HTTP protocol or the HTTPS protocol

Auto-Refresh： Adjusts the Web GUI automatic refresh interval. 0 disables this feature completely

Enable Info Site： Enable or disable the login system information page

Info Site Password Protection： Enable or disable the password protection feature of the system information page

 Copyright @ Yifan 2021



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 to one of your own, if you haven't already.

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 your web browser's address field. You will be asked for the Router's password.

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

SSH Management： You can also enable SSH to remotely access the Router by Secure Shell. Note that SSH daemon needs to be enable in Services page.

Note：

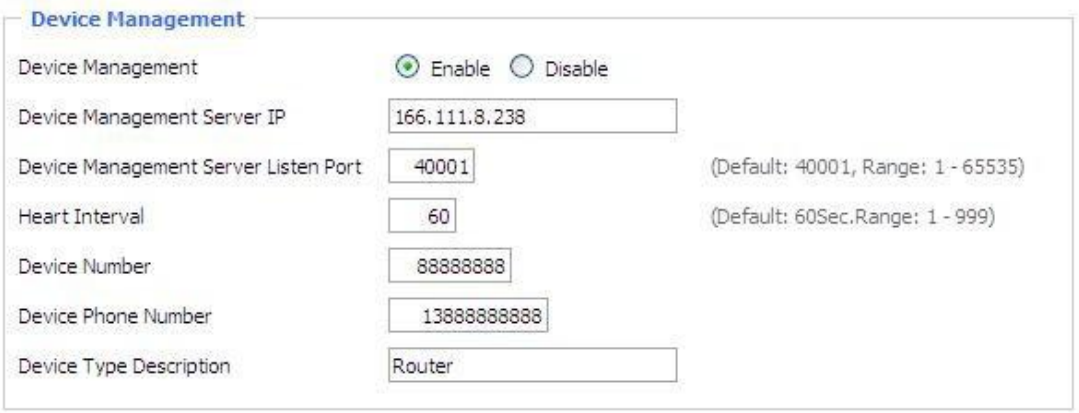
If the Remote Router Access feature is enabled, anyone who knows the Router's Internet IP address and password will be able to alter the Router's settings.

Telnet Management： Enable or disable remote Telnet function

Cron： The cron subsystem schedules execution of Linux commands. You'll need to use the command line or startup scripts to use this.

Language： Set up the Router page shows the type of language, including simplified Chinese and English.

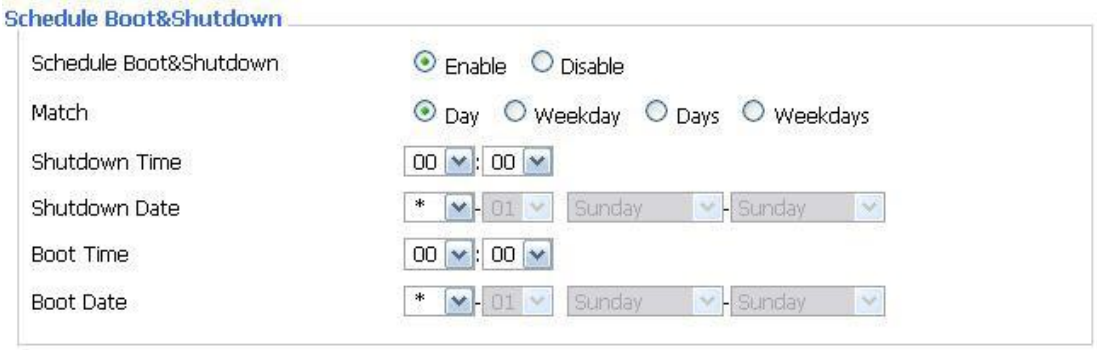
 Copyright @ Yifan 2021



Remote Upgrade: Custom-developed remote management server for this station router monitoring and management, configuration parameters, WIFI advertising updates.

Keep Alive

Schedule Boot & Shutdown



The user can set the startup or shutdown time:
For example, the user wants to set the start time at 8:07 and boot time at 9:07.

 Copyright @ Yifan 2021

Schedule Reboot

You can schedule regular reboots for the router:

Regularly after xxx seconds.

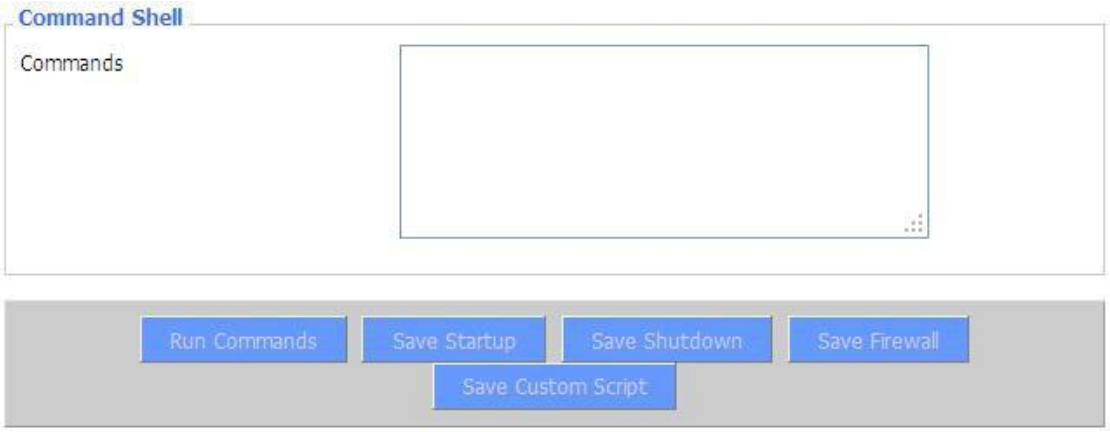
At a specific date time each week or every day.

Note：

For date-based reboots Cron must be activated. See Management for Cron activation.

Commands

Commands： You can run command lines directly via the Web interface.



Run Command： You can run command lines via the web interface. Fill the text area with your command and click Run Commands to submit.

Startup： You can save some command lines to be executed at startup's Router. Fill the text area with commands (only one command by row) and click Save Startup.

Shutdown： You can save some command lines to be executed at shutdown's Router. Fill the text area with commands (only one command by row) and click Save Shutdown.

Firewall： Each time the firewall is started, it can run some custom iptables instructions. Fill the text area with firewall's instructions (only one command by row) and click Save Firewall.

Custom Script： Custom script is stored in /tmp/custom.sh file. You can run it manually or use cron to call it. Fill the text area with script's instructions (only one command by row) and click Save Custom Script.

 Copyright @ Yifan 2021

Factory Defaults

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.

Firmware Upgrade

Firmware Upgrade： New firmware versions are posted at www..com and can be downloaded. 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:

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

Note：

Upgrading firmware may take a few minutes.

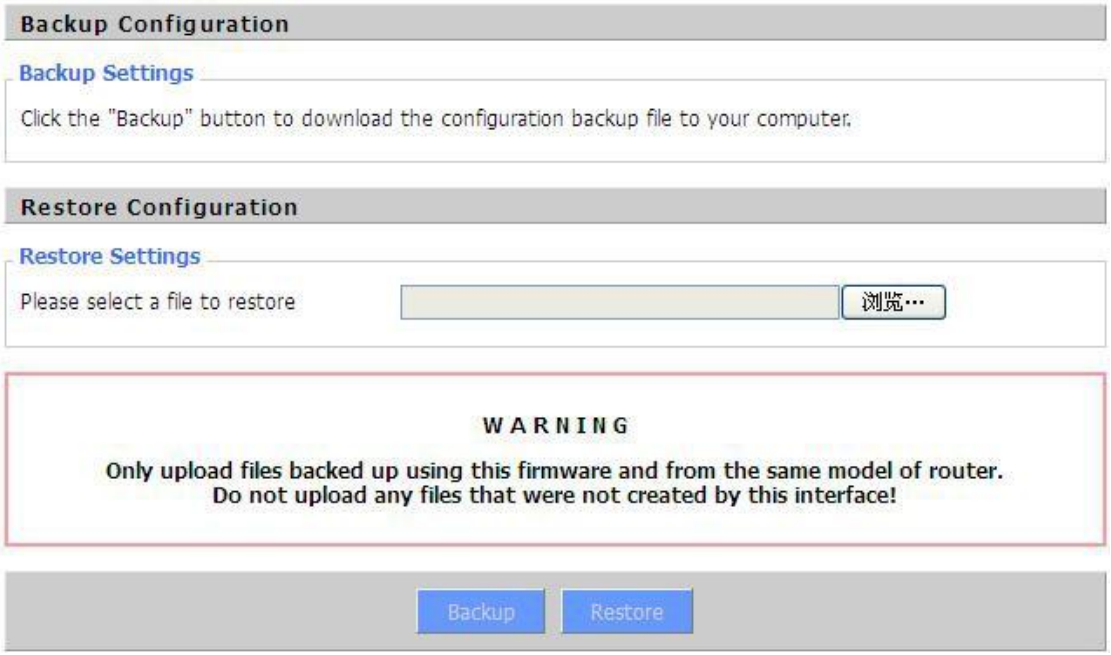
Do not turn off the power or press the reset button!

After flashing, reset to：

If you want to reset the Router to the default settings for the firmware version you are upgrading to, click the Firmware Defaults option.

 Copyright @ Yifan 2021

Backup



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 back up 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.

 Copyright @ Yifan 2021

3.3.11 Status

Router

Router Name: Name of the router, setting too basic setting for modify

Router Model: Model of the Router, unavailable to modify

Firmware Version: software version information

MAC Address: MAC address of WAN, setting to Clone MAC Address for modify

Host Name: Host name of the Router, setting to basic setting for modify

WAN Domain Name: Domain name of WAN, setting to basic setting for modify

LAN Domain Name: Domain name of LAN, unavailable to modify

Current Time: Local time of the system

Uptime: Operating uptime if the system is powered on

Total Available: The room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: Free memory, the router will reboot if the memory is less than 500kB

Used: Used memory, total available memory minus free memory

Buffers: Used memory for buffers,

Cached: The memory used by high-speed cache memory

 Copyright @ Yifan 2021

Active: Active use of buffer or cache memory page file size

Inactive: Not often used in a buffer or cache memory page file size

IP Filter Maximum Ports: Preset is 4096, available to re-management

Active IP Connections: Real time monitor active IP connections of the system, click to see the table as blow:

Active IP Connections 53

No.	Protocol	Timeout (s)	Source Address	Remote Address	Service Name	State
1	TCP	60	192.168.1.120	192.168.1.1	80	TIME_WAIT
2	TCP	30	192.168.1.120	192.168.1.1	80	TIME_WAIT
3	TCP	65	192.168.1.120	192.168.1.1	80	TIME_WAIT
4	TCP	96	192.168.1.120	192.168.1.1	80	TIME_WAIT
5	TCP	99	192.168.1.120	192.168.1.1	80	TIME_WAIT
6	TCP	70	192.168.1.120	192.168.1.1	80	TIME_WAIT
7	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
8	TCP	115	192.168.1.120	192.168.1.1	80	TIME_WAIT
9	TCP	84	192.168.1.120	192.168.1.1	80	TIME_WAIT
10	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
11	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
12	TCP	108	192.168.1.120	192.168.1.1	80	TIME_WAIT
13	TCP	3600	192.168.1.120	192.168.1.1	80	ESTABLISHED
14	TCP	93	192.168.1.120	192.168.1.1	80	TIME_WAIT
15	TCP	102	192.168.1.120	192.168.1.1	80	TIME_WAIT
16	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
17	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
18	TCP	15	192.168.1.120	192.168.1.1	80	TIME_WAIT
19	TCP	25	192.168.1.120	192.168.1.1	80	TIME_WAIT
20	TCP	90	192.168.1.120	192.168.1.1	80	TIME_WAIT
21	UDP	26	192.168.8.119	255.255.255.255	1947	UNREPLIED
22	TCP	77	192.168.1.120	192.168.1.1	80	TIME_WAIT
23	TCP	35	192.168.1.120	192.168.1.1	80	TIME_WAIT
24	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
25	TCP	40	192.168.1.120	192.168.1.1	80	TIME_WAIT
26	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
27	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
28	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
29	TCP	4	192.168.1.120	192.168.1.1	80	TIME_WAIT
30	UDP	31	192.168.8.160	224.0.0.1	9166	UNREPLIED

Active IP Connections: Total active IP connections

Protocol: Connection protocol

Timeouts: Connection timeouts, unit is second

Source Address: Source IP address

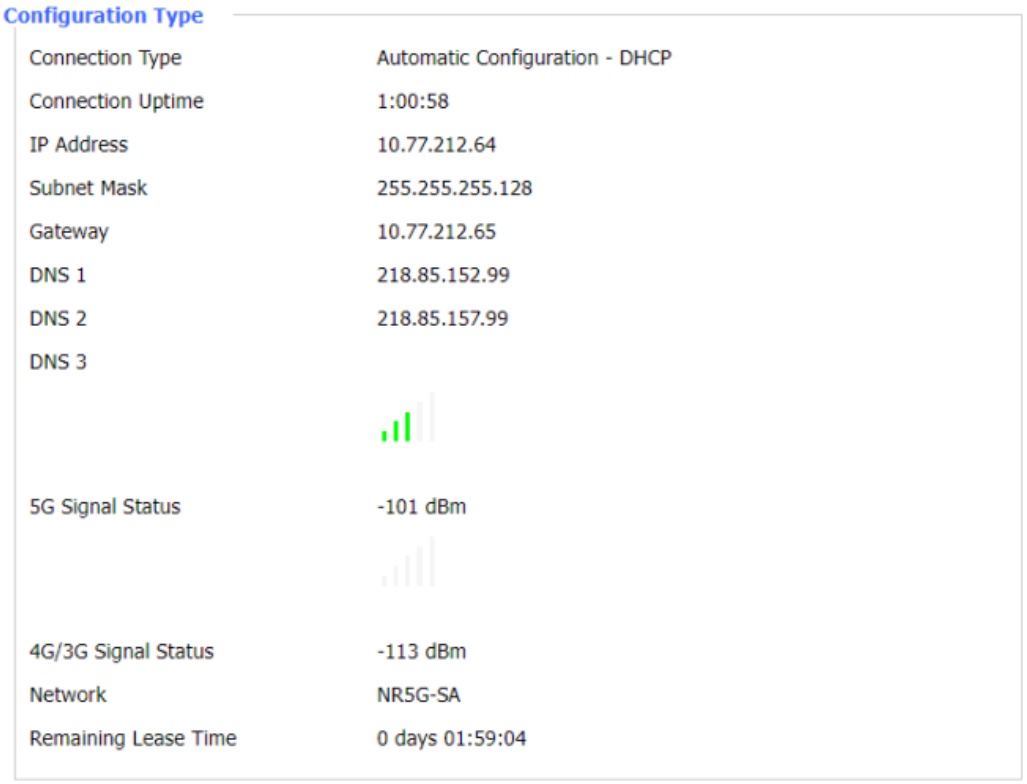
Remote Address: Remote IP address

Service Name: Connecting service port

Status: Displayed status

 Copyright @ Yifan 2021

WAN



Connection Type: Disabled, static IP, automatic configuration-DHCP, PPPOE, PPTP, L2TP, 3G/UMTS, DHCP-4G/5G

Connection Uptime: Connecting uptime; If disconnect, display Not available

IP Address: IP address of router WAN

Subnet Mask: Subnet mask of router WAN

Gateway: The gateway of router WAN

DNS1, DNS2, DNS3: DNS1/DNS2/DNS3 of Router WAN

Signal Status: Signal intensity of the module in 3G/4G/5G mode

Network: Network type of the module in 3G/4G/5G mode

 Copyright @ Yifan 2021

Total Flow: Flow from power-off last time until now statistics, download and upload direction

Monthly Flow: The flow of a month, unit is MB

Last Month: The flow of last month

Next Month: The flow of next month

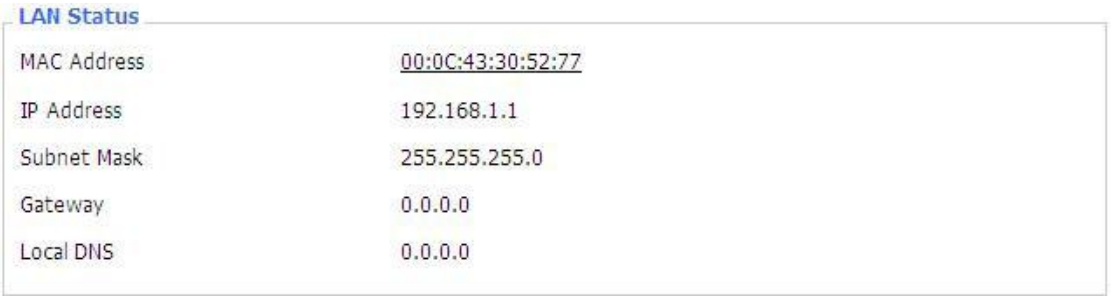
Backup: Backup data administration

Restore: Restore data administration

Delete: Delete data administration

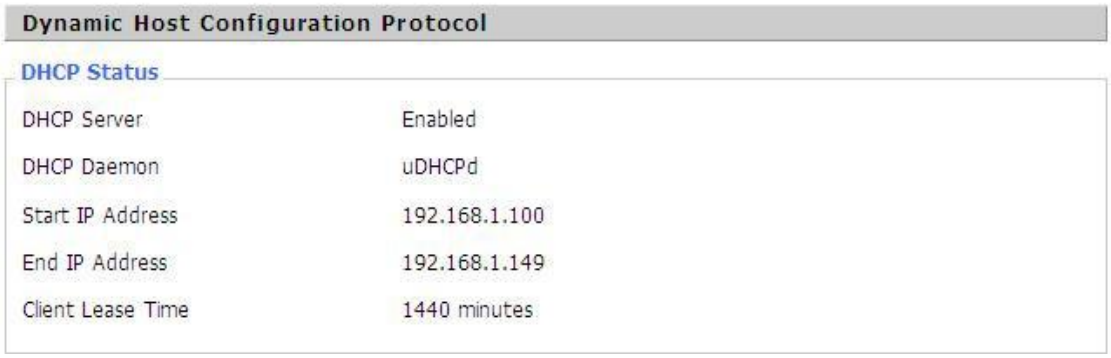
 Copyright @ Yifan 2021

LAN

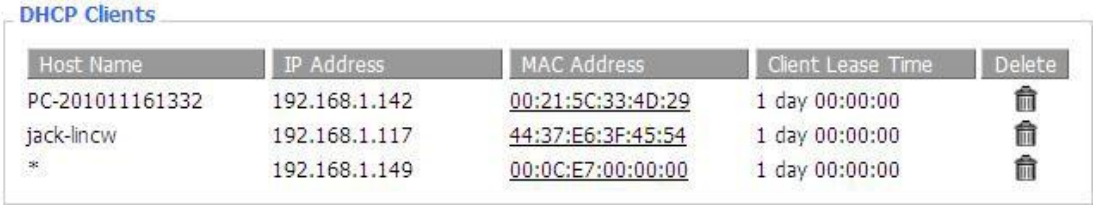


MAC Address: MAC Address of the LAN port ethernet
IP Address: IP Address of the LAN port
Subnet Mask: Subnet Mask of the LAN port
Gateway: Gateway of the LAN port
Local DNS: DNS of the LAN port

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 Server: Enable or disable the Router work as a DHCP server
DHCP Daemon: The agreement allocated using DHCP including DNSMasq and uDHCPd 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



 Copyright @ Yifan 2021

Client Lease Time: The lease time of DHCP client

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

Connected PPPOE Clients

Interface	User Name	Local IP	Delete
ppp0	hometest	192.168.10.10	

Delete: Click to delete DHCP client

Interface: The interface assigned by dial-up system
Username: Username of PPPoE client
Local IP: IP address assigned by PPPoE client
Delete: Click to delete PPPoE client

Connected L2TP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	

Interface: The interface assigned by dial-up system
Local IP: Tunnel IP address of local L2TP

Remote IP: Tunnel IP address of L2TP server
Delete: Click to disconnect L2TP

Connected L2TP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.50.2	120.42.46.98	

Interface: The interface assigned by dial-up system
Username: Username of the client

Local IP: Tunnel IP address of L2TP client
Remote IP: IP address of L2TP client

Delete: Click to delete L2TP client

Connected PPTP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	

Interface: The interface assigned by dial-up system
Local IP: Tunnel IP address of local PPTP

Remote IP: Tunnel IP address of PPTP server
Delete: Click to disconnect PPTP

 Copyright @ Yifan 2021

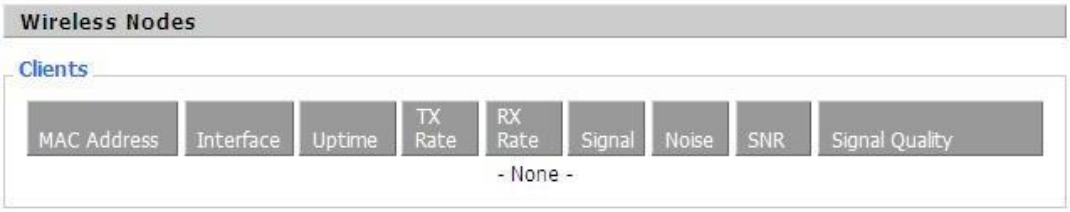
Interface: The interface assigned by dial-up system
Username: Username of the client
Local IP: Tunnel IP address of PPTP client
Remote IP: IP address of PPTP client
Delete: Click to delete PPTP client

Wireless

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 diasbal Encryption-Interface wl0
PPTP Status: Show wireless pptp status

 Copyright @ Yifan 2021

Received (RX): Received data packet
Transmitted (TX): Transmitted data packet

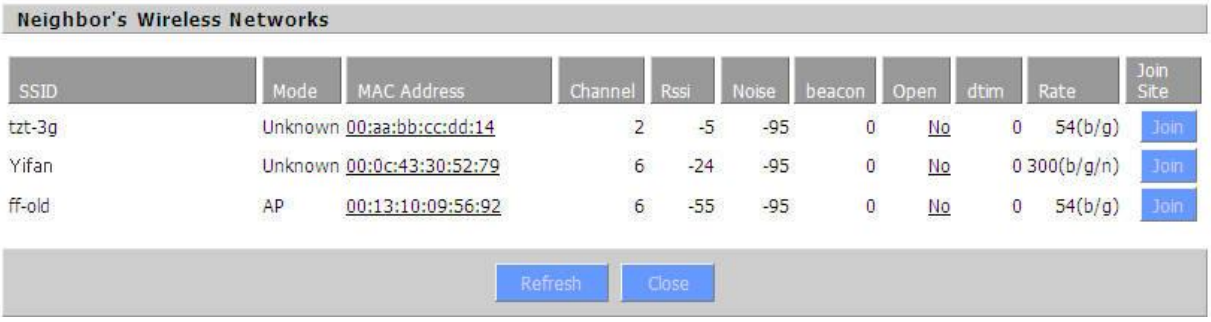


MAC Address: MAC address of wireless client
Interface: Interface of wireless client

Uptime: Connecting 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 Qua lity: Signal quality of wireless client



Neighbor's Wireless Network: Display other networks nearby
SSID: The name of wireless network nearby
Mode: Operating mode of wireless network nearby

MAC Address: MAC address of the wireless nearby
Channel: The channel of the wireless nearby
Rssi: Signal intensity of the wireless nearby
Noise: The noise of the wireless nearby
Beacon: Signal beacon of the wireless nearby
Open: The wireless nearby is open or not
Dtim: Delivery traffic indication message of the wireless nearby
Rate: Speed rate of the wireless nearby
Join Site: Click to join wireless network nearby

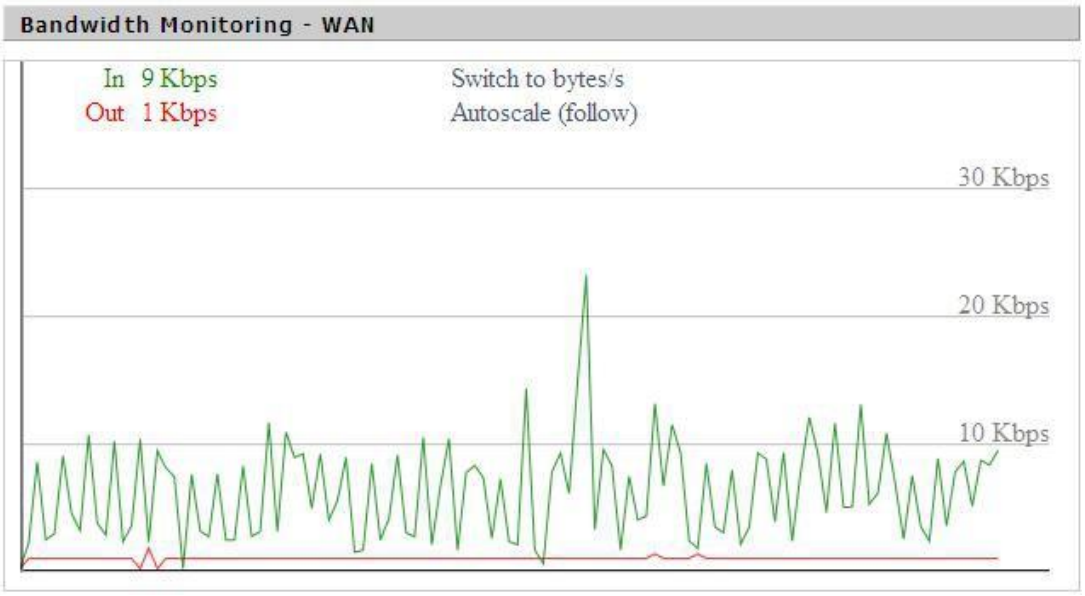
 Copyright @ Yifan 2021

Bandwidth

Bandwidth Monitoring-LAN Graph

Abscissa axis: Time

Vertical axis: Speed rate

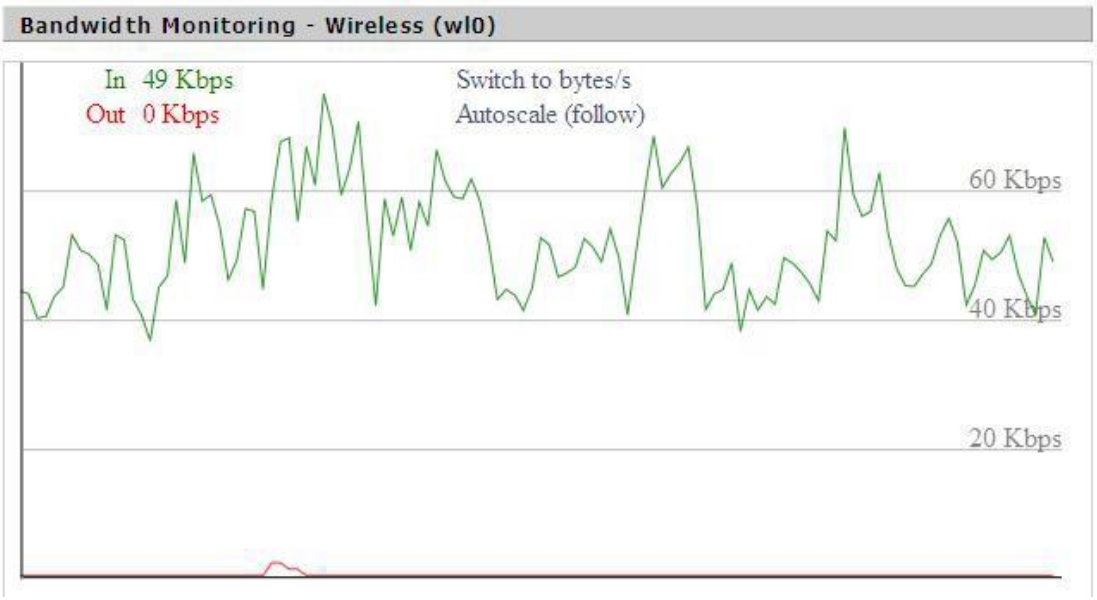


Bandwidth Monitoring-WAN Graph

Abscissa axis: Time

Vertical axis: Speed rate

 Copyright @ Yifan 2021



Bandwidth Monitoring-Wireless (W10) Graph

Abscissa axis: Time

Vertical axis: Speed rate

Sys-Info

Router

Router Name	Router
Router Model	Router
LAN MAC	54:D0:B4:26:05:84
WAN MAC	54:D0:B4:26:05:85
Wireless MAC	00:11:22:33:44:57
WAN IP	10.77.212.64
BKUP WAN IP	0.0.0.0
LAN IP	192.168.1.1

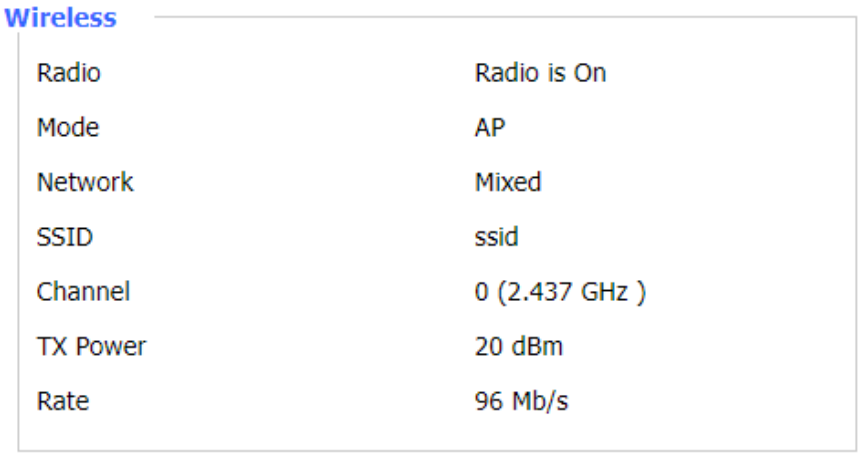
Router Name: The name of the Router
Router Model: The model of the Router

LAN MAC: MAC address of LAN port

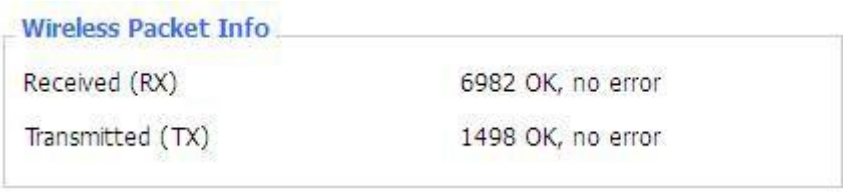
WAN MAC: MAC address of WAN port

 Copyright @ Yifan 2021

Wireless MAC: MAC address of the wireless
WAN IP: IP address of WAN port
LAN IP: IP address of LAN port



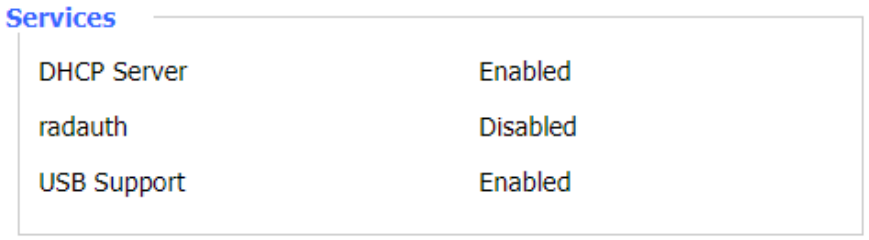
Radio: Display whether radio is on or not
Mode: Wireless mode
Network: Wireless network mode
SSID: Wireless network name
Channel: Wireless network channel
TX Power: Reflection power of wireless network
Rate: Reflection rate of wireless network



Received (RX): Received data packet
Transmitted (TX): Transmitted data packet

MAC Address: MAC address of wireless client
Interface: Interface of wireless client
Uptime: Connecting 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

 Copyright @ Yifan 2021



DHCP Server: Enabled or disabled

radauth: Enabled or disabled

USB Support: Enabled or disabled

Total Available: The room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: Free memory, the Router will reboot if the memory is less than 500kB

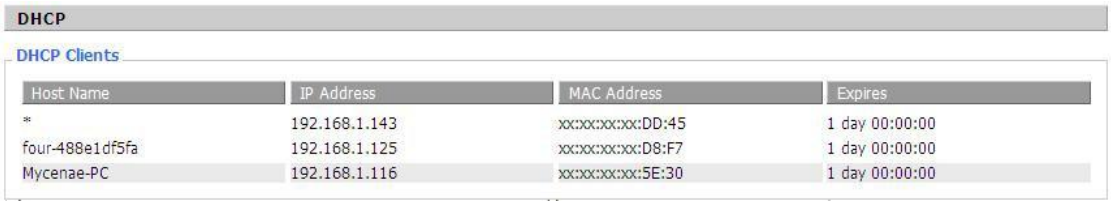
Used: Used memory, total available memory minus free memory

Buffers: Used memory for buffers, total available memory minus allocated memory

Cached: The memory used by high-speed cache memory

Active: Active use of buffer or cache memory page file size

Inactive: Not often used in a buffer or cache memory page file size



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

 Copyright @ Yifan 2021

Appendix

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

1. Press Start→Programs→Accessories→Communications→Hyper Terminal

2. Input connection name, choose “OK”

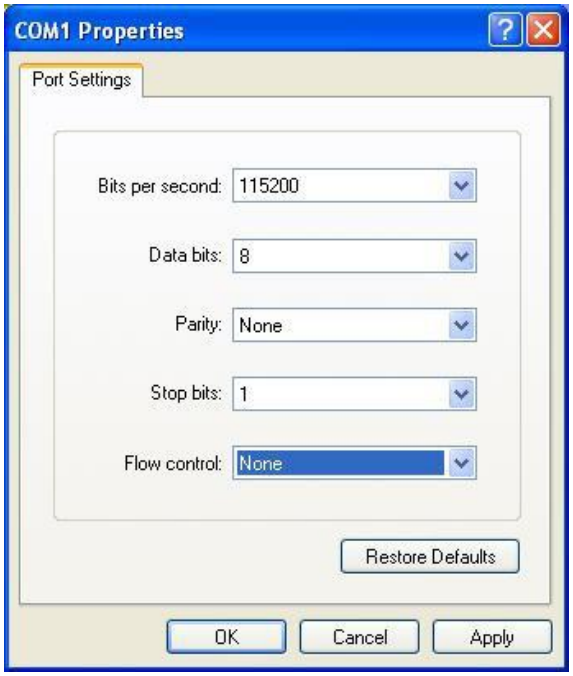
3. Choose the correct COM port which connects to modem, choose “OK”

4. Configure the serial port parameters as following, choose “OK” Bits per

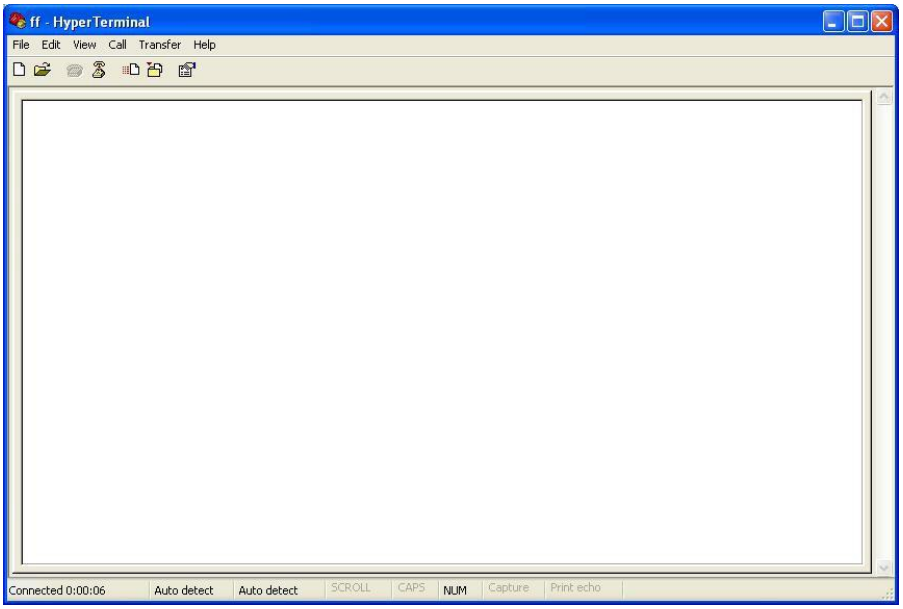
Second: 115200
Data bits: 8

 Copyright @ Yifan 2021

Parity: None Stop
bits: 1
Flow control: None



5. Complete Hyper Terminal operation, it runs as following



Note: If the user is using the win7 system, you can download a win7 super terminal on the internet. Universal serial interface or other similar software.

 Copyright @ Yifan 2021