NR100 5G Router User Manual

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

Version History

Date	Version	Content	By
2020-4-17	V1.0.0	**First Version**	XRC
2020-4-20	V1.0.1	Modify picture	LJH
2020-4-29	V1.0.2	Delete Duplicate content	XRC
2020-4-29	V1.0.3	Modify Package Content	Fish_yan
2020-09-18	V1.0.4		

5G
Yifan
NR100
Industrial Router
Voltage
+9~36VDC
IP
192. 168. 1. 1
Username
admin
Password
admin
www.yifanwireless.com

Content

Chapter 1 Product Introduction 6
Chapter 2 Installation 8
2.4 Power supply 11
2.5 Indicators 11
2.6 Reset Button 12
Chapter 3 Configuration and Management 13
3.1 Configuration Connection 13
3.2 Access the Configuration Web Page 13
3.3 Management and configuration 15
3.3.1 Setting 15
3.3.1.1 Basic Setting 15
3.3.1.2 Dynamic DNS 21
3.3.1.3 Clone MAC Address 23
3.3.1.4 Advanced Router 23
3.3.1.5 VLANs 24
3.3.1.6 Networking 25
3.3.2 Wireless 28
3.3.2.1 Basic Settings 28
3.3.2.2 Wireless Security 31
3.3.3 Services 33
3.3.3.1 Services 33
3.3.4 VPN 36
3.3.4.1 PPTP 36
3.3.4.2 L2TP 37
3.3.4.3 OPENVPN 38
3.3.4.4 IPSEC 43
3.3.4.5 GRE 45
3.3.5 Security 47
3.3.5.1 Firewall 47
3.3.6 Access Restrictions 49
3.3.6.1 WAN Access 49
3.3.6.2 URL Filter 52
3.3.6.3 Packet Filter 53
3.3.7 NAT 54
3.3.7.1 Port Forwarding 54
3.3.7.2 Port Range Forward 55
3.3.7.3 DMZ 56

3.3.8 QoS Setting 56
3.3.8.1 Basic 56
3.3.8.2 Classify 57
3.3.9 Applications 58
3.3.9.1 Serial Applications 58
3.3.10 Administration 59
3.3.10.1 Management 59
3.3.10.2 Keep Alive 61
3.3.10.3 Commands 62
3.3.10.4 Factory Defaults 63
3.3.10.5 Firmware Upgrade 63
3.3.10.6 Backup 64
3.3.11 Status 65
3.3.11.1 Router 65
3.3.11.2 WAN 68
3.3.11.3 LAN 69
3.3.11.4 Wireless 72
3.3.11.5 Bandwidth 74
3.3.11.6 Sys-Info 75
Appendix 78

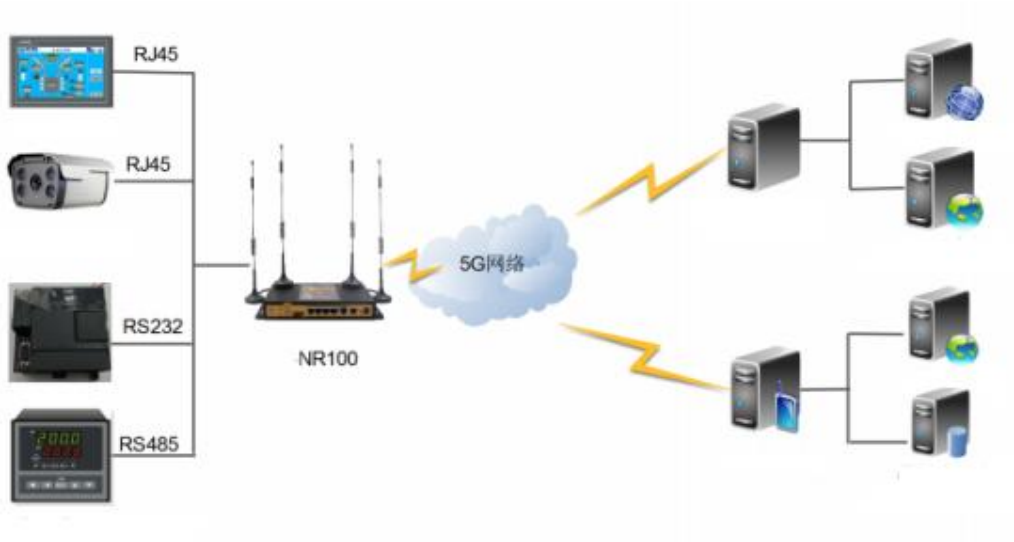
Chapter 1 Product Introduction

1.1 Product overview

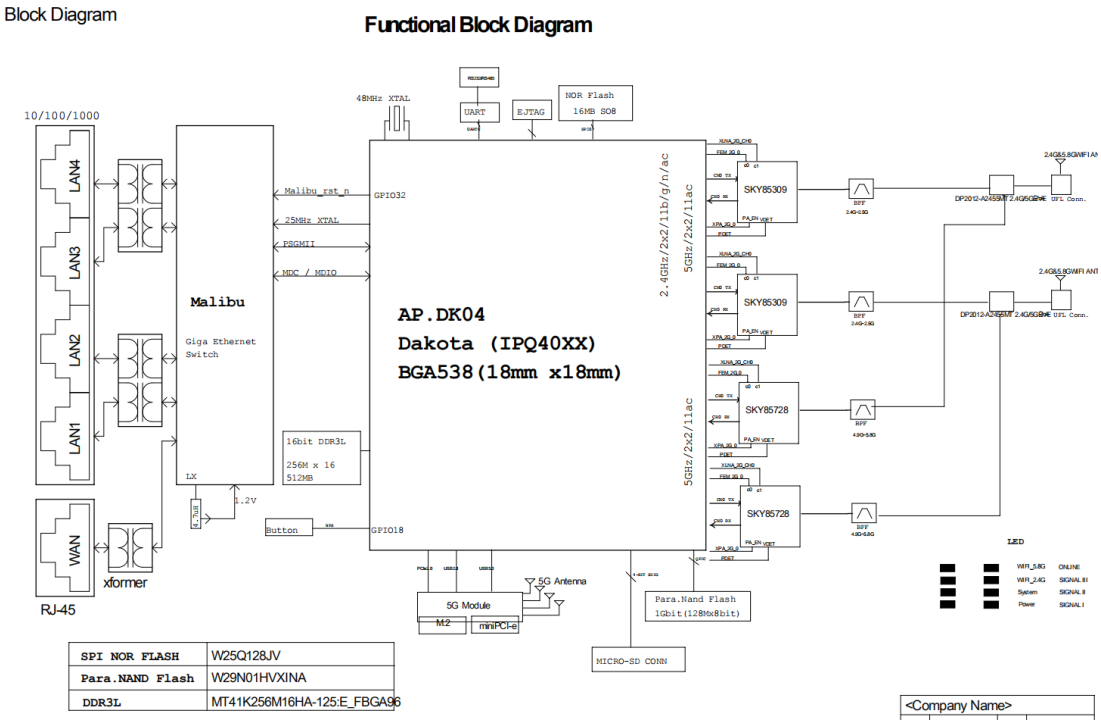
NR100 is a wireless communication router for the Internet of Things, which uses public 3G/4G/5G networks to provide users with wireless long-distance big data transmission functions.

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 1 RS232 (or RS485) + 4 Ethernet LAN + 1 Ethernet WAN + 2 WIFI interfaces, 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 in 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.



1.2 Block diagram of working principle



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

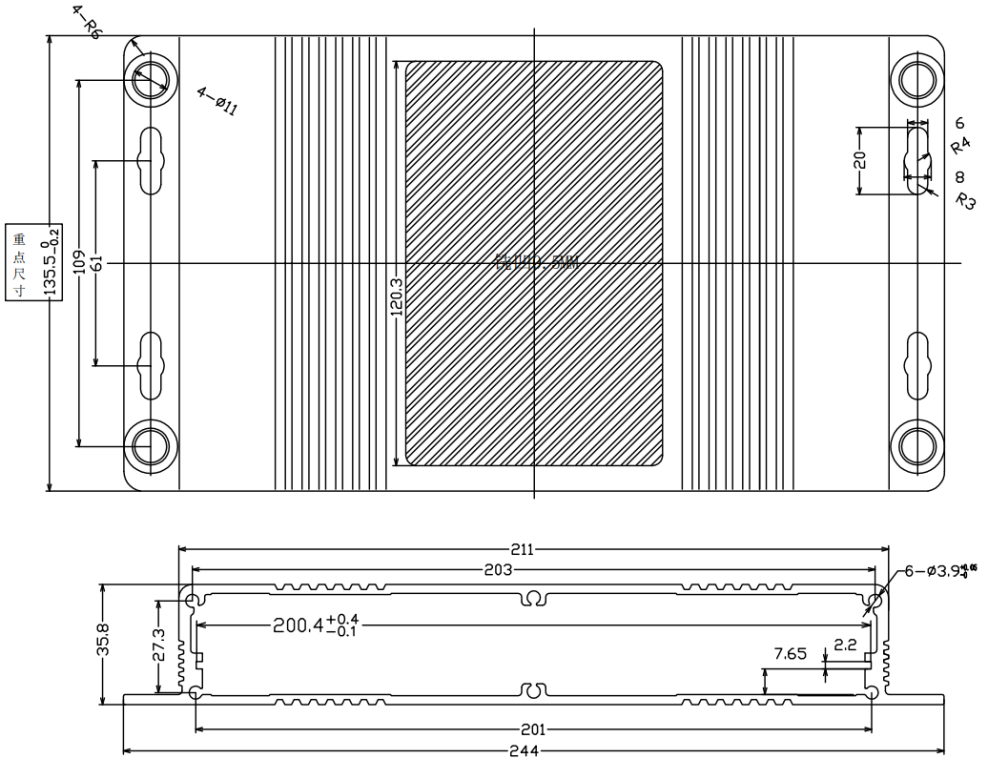
When you open the box, please keep the packing materials, so that you can use it when you need to transfer in the future.

The list is as follows:

·5G router host x 1
·5G wireless cellular antennas (SMA male) x 4
·WIFI antenna (SMA female) x2
·Matching power supply x 1
·Ethernet direct connection x 1

2.3 Installation and cable connection

Size(mm)：



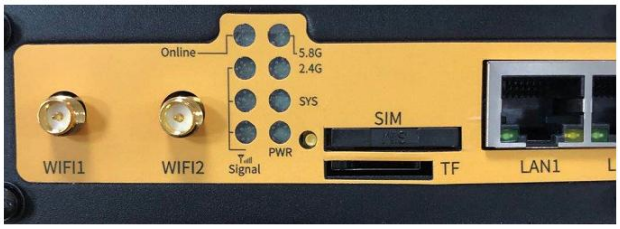
Antenna installation:

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. In order 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 wifi antenna, it is recommended that the two wifi are placed at a 90 degree angle.

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. Put the SIM/UIM card into the card holder first, and make sure that the metal contact surface of the SIM/UIM card is facing outward, then insert the SIM/UIM card holder into the drawer .

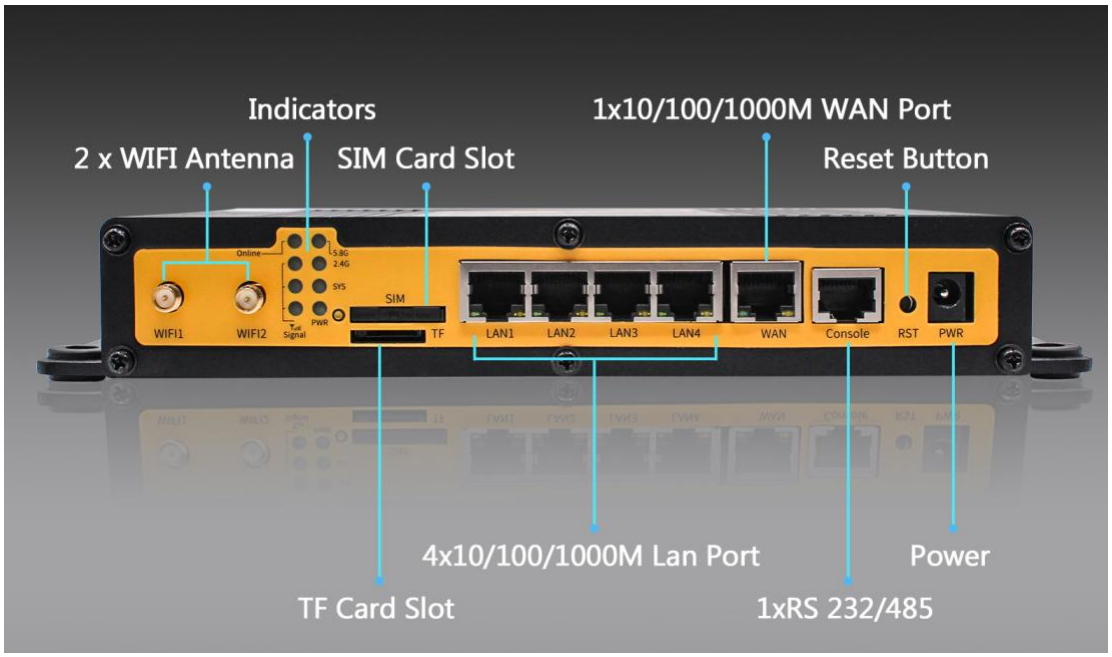


Connect Console cable：

Plug the RJ45 end of the Console line into the Console interface (RS232) of the Router, and plug the DB9 end into the RS232 serial interface of the user device. The signal connections of the Console are as follows:

Console (RS232)				
RJ45	color	Pin map	DB9F	Content
1	white/Orange	A	8	RS485-A（optional）
2	Orange	B	6	RS485-B（optional）
3	White/Green	RXD	2	RS232 RX

4	Blue	--	1	--
5	white/blue	GND	5	GND
6	green	TXD	3	RS232 TX
7	White/brown	--	4	--
8	brown	--	7	--



2.4 Power supply

5G routers are usually used in complex external environments. In order 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.

2.5 Indicators

5G Router provide indicators as below：“Power”、“System”、“2.4G”、“5.8G”、“ONLINE”、“Signal”：

indicator	status	Content
Power	On	Device powered on

	Off	Device powered off
System	Blank	System running normally
	Off	System not running
Online	on	Device is online on internet
	off	Device not online
2.4G	on	2.4GWIFI is on
	off	2.4GWIFIis off
5.8G	on	5.8GWIFI is on
	off	5.8GWIFI is off
WAN	off	WAN port not connected
	on/blank	WAN port connected/communicating
LAN1~LAN4	off	LAN port not connected
	on/blank	LAN port connected/communicating
Signal strength	One light on	weak(<-90dbm)
	Two lights on	medium(-70dbm~-90dbm)
	Three lights on	good(>-70dbm)

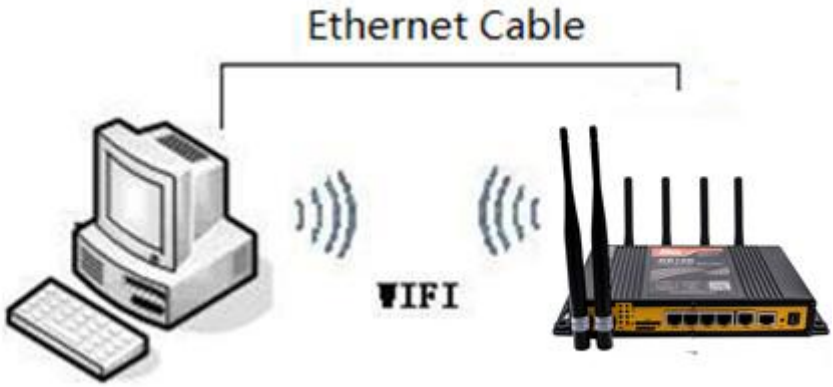
2.6 Reset Button

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.

Chapter 3 Configuration and Management

3.1 Configuration Connection

Before configuration, you should connect the Router and your configuration PC with the supplied network cable. Plug the cable's one end into the Local Network port of the Router, and another end into your configure PC's Ethernet port. The connection diagram is as following:

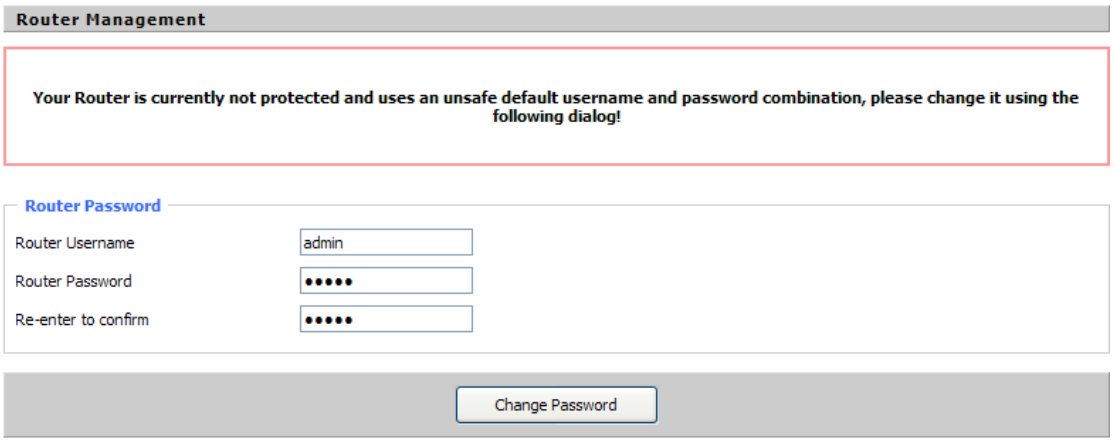


Please modify the IP address of PC as the same network segment address of the Router, for instance, 192.168.1.9. Modify the mask code of PC as 255.255.255.0 and set the default gateway of PC as the Router's IP address (192.168.1.1).

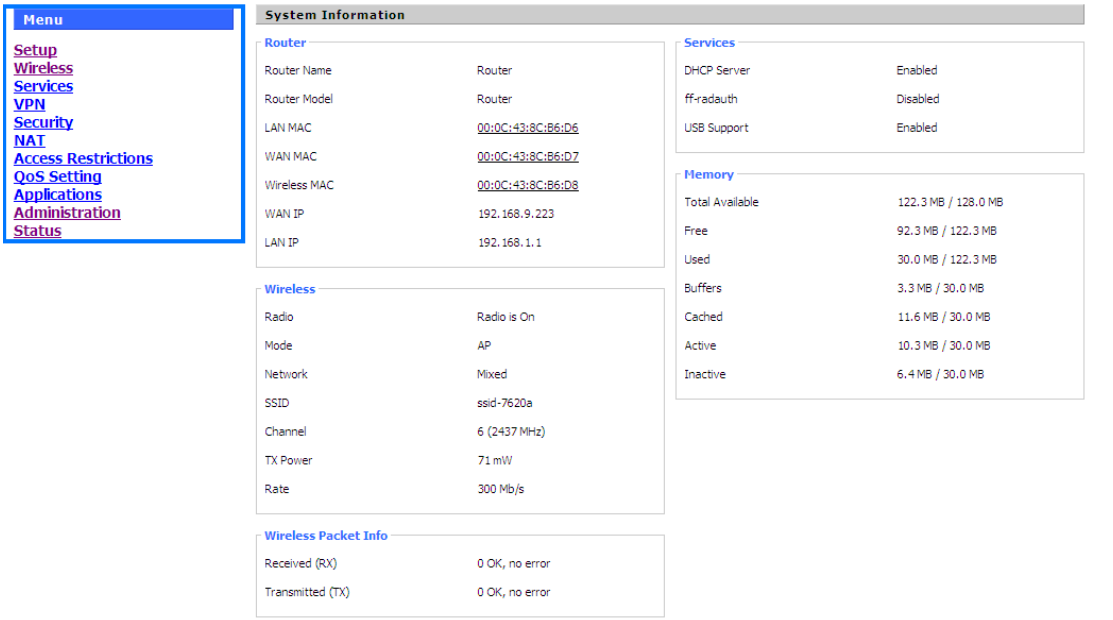
3.2 Access the Configuration Web Page

The chapter is to present main functions of each page. Users visit page tool via web browser after connect 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.

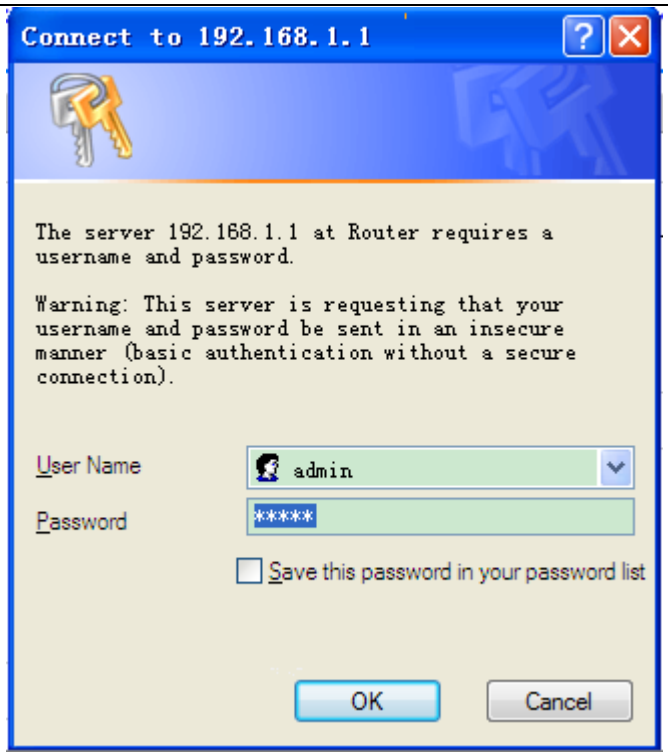
Users can open IE or other explorers and enter the Router's default IP address of 192.168.1.1 on address bar, then press the bottom of Enter to visit page Web management tool of the Router. The users login in the web page at the first name, there will display a page shows as blow to tip users to modify the default user name and password of the Router. Users have to click "change password" to make it work if they modify user name and password.



After access to the information main page



Users need to input user name and password if it is their first time to login.



Input correct user name and password to visit relevant menu page. Default user name is admin, password is admin. (available to modify user name and password on management page, then click submit)

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 User Name, Password, IP Address, Default Gateway Address, or DNS IP Address. These information can be obtained from your ISP, if required.

3.3.1.1Basic Setting

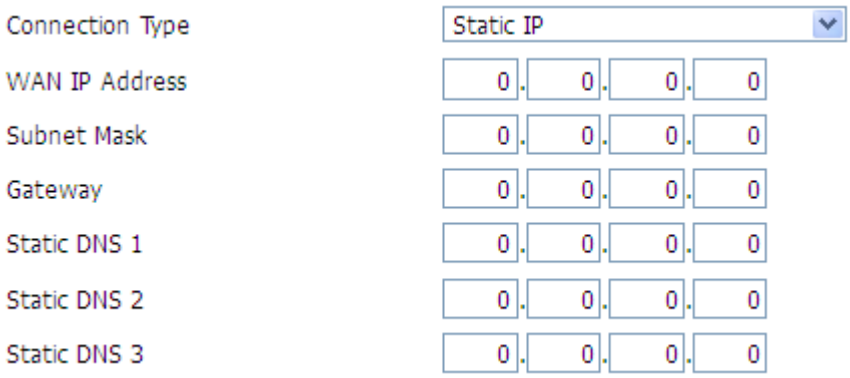
WAN Connection Type

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

Disabled

Forbid the setting of WAN port connection type

Static IP

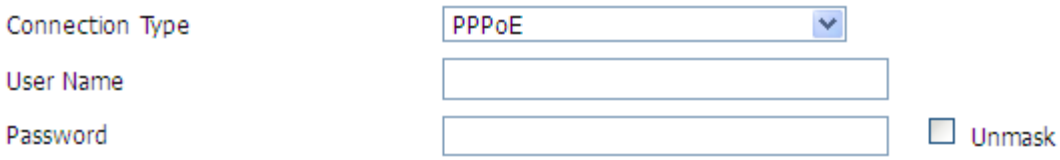


WAN IP Address: Users set IP address by their own or ISP assigns
Subnet Mask: Users set subnet mask by their own or ISP assigns
Gateway: Users set gateway by their own or ISP assigns
Static DNS1/DNS2/DNS3: Users set static DNS by their own or ISP assigns

Automatic Configuration-DHCP

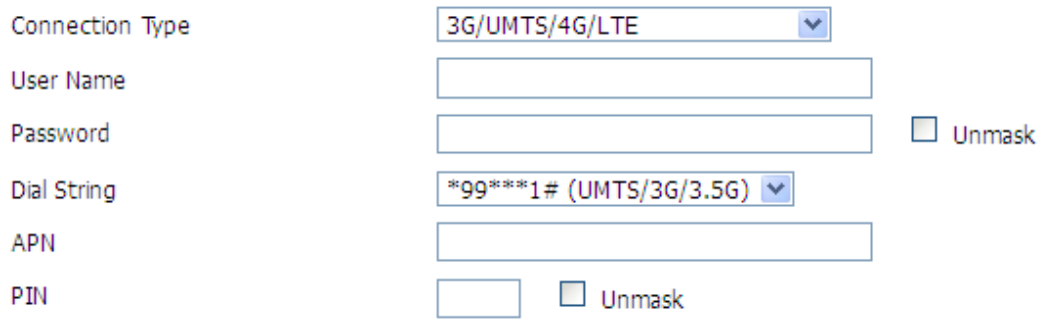
IP address of WAN port gets automatic via DHCP

PPPOE



User Name: login the Internet
Password: login the Internet

3G/UMTS/4G/LTE



User Name: login users' ISP(Internet Service Provider)
Password: login users' ISP
Dial String: dial number of users' ISP
APN: access point name of users' ISP
PIN: PIN code of users' SIM card

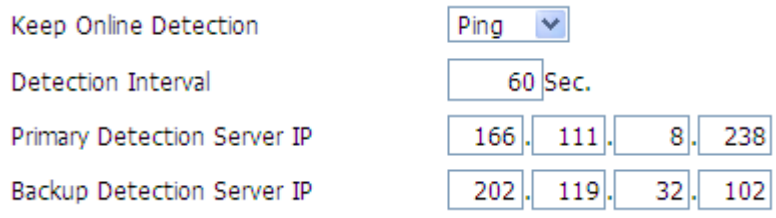
Connection type

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

DHCP-4G/5G

IP address of WAN port gets automatic via DHCP-4G/5G.

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.

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 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 response the 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

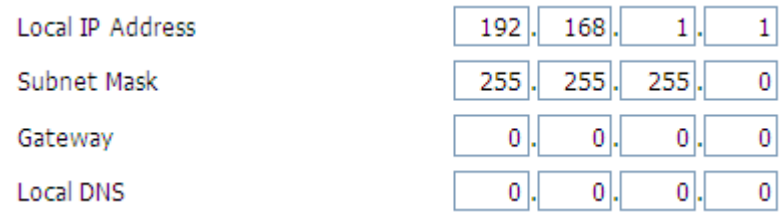
STP

STP (Spaning 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

Optional Configuration

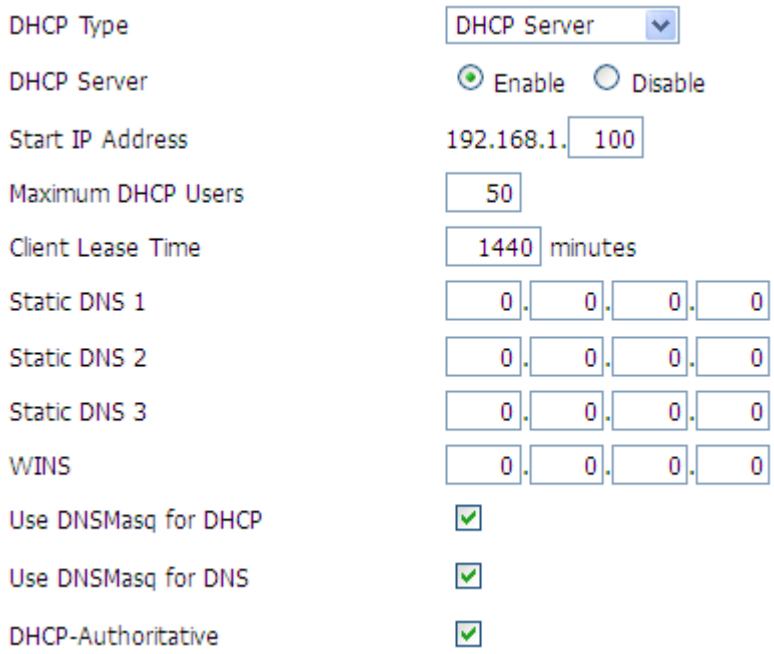
Router Name: set Router name
Host Name: ISP provides
Domain Name: ISP provides
MTU: auto (1500) and manual (1200-1492 in PPPOE/PPTP/L2TP mode, 576-16320 in other modes)

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

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.



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 have 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

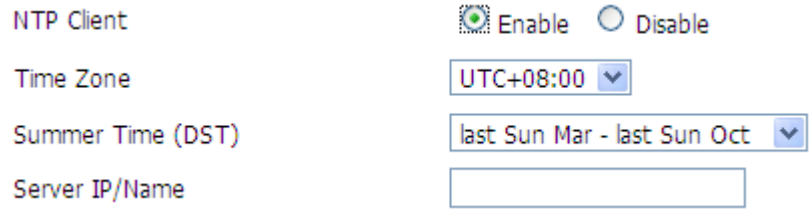
one of these fields. Users can enter up to three DNS Server IP addresses here. The Router will utilize them for quicker access to functioning DNS servers.

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.

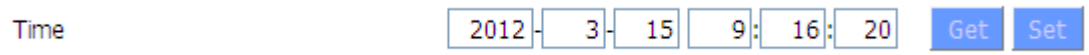
Time Settings

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

Adjust Time



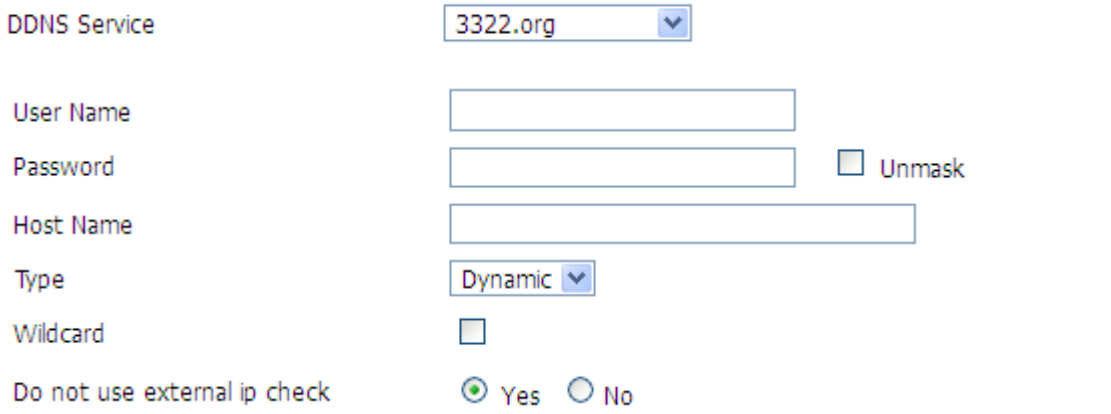
To adjust time by the system and refresh to get the time of the web, user can set to modify the time of the system. They can change to adjust time by manual to achieve adjust time by the system if the system fails to get NTP server

3.3.1.2 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 what their IP address will be, and the address can change frequently. In this case, users can use a commercial dynamic DNS service, which allows them to register their domain to their IP address, and will

forward traffic directed at their domain to their frequently-changing IP address.

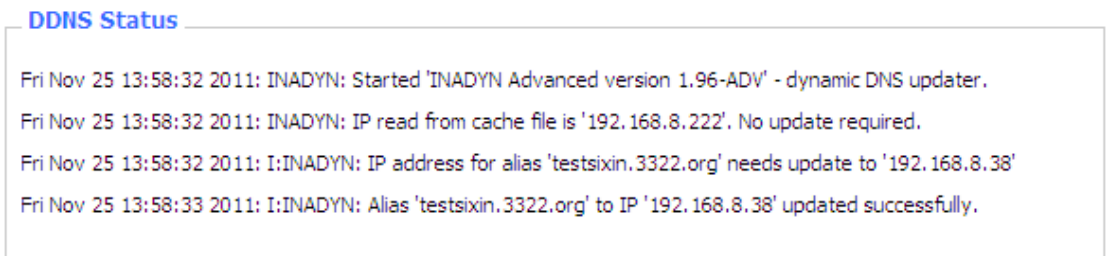
DDNS Service: Router currently support DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP and Custom based on the user.



User Name: users register in DDNS server, up to 64 characteristic
Password: password for the user name that users register in DDNS server, up to 32 characteristic
Host Name: users register in DDNS server, no limited for input characteristic for now
Type: depends on the server
Wildcard: support wildcard or not, the default is OFF. ON means *.host.3322.org is equal to host.3322.org
Do not use external ip check: enable or disable the function of 'do not use external ip check'

Force Update Interval: unit is day, try forcing the update dynamic DNS to the server by setted days

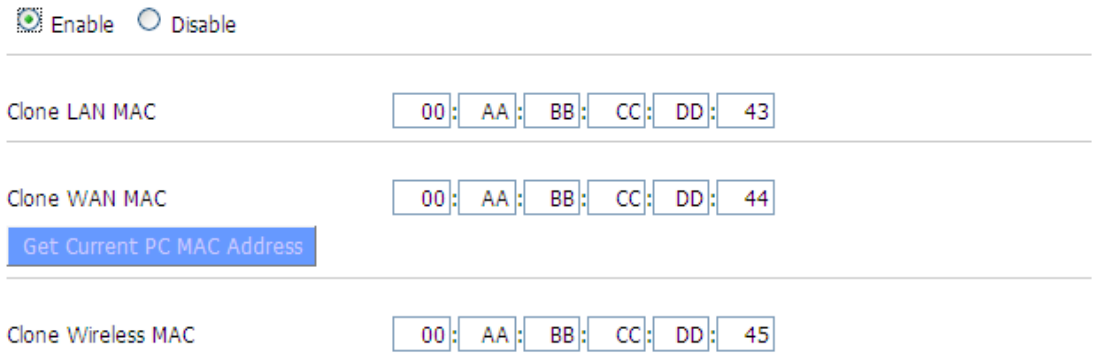
Status



DDNS Status shows connection log information

3.3.1.3 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

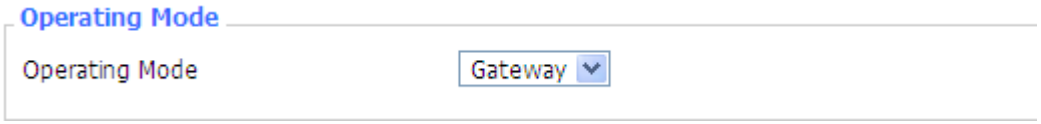


Clone MAC address can clone three parts: Clone LAN MAC, Clone WAN MAC, Clone Wireless MAC.

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

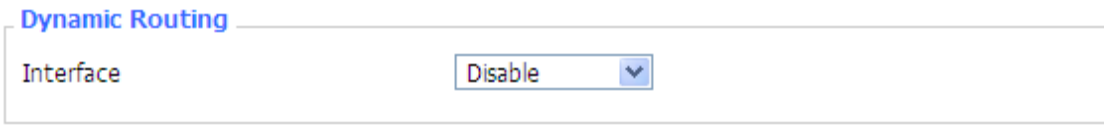
3.3.1.4 Advanced Router

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.

Dynamic Routing



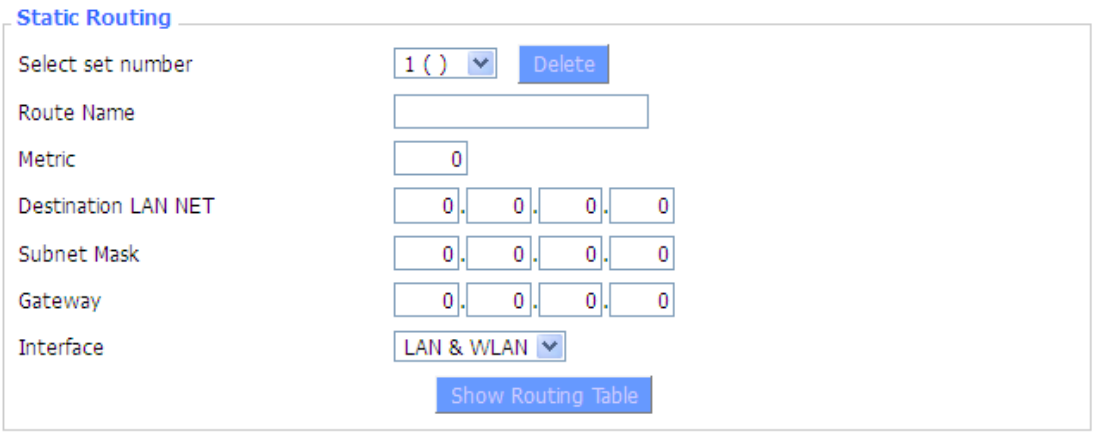
Dynamic Routing enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with other Routers. The Router determines the network packets' route based on the fewest number of hops between the source and destination.

To enable the Dynamic Routing feature for the WAN side, select WAN. To enable this feature for the LAN and wireless side, select LAN&WLAN. To enable the feature for both

the WAN and LAN, select Both. To disable the Dynamic Routing feature for all data transmissions, keep the default setting, Disable.

Note： Dynamic Routing is not available in Gateway mode

Static Routing



Select set number: 1-50

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

Metric: 0-9999

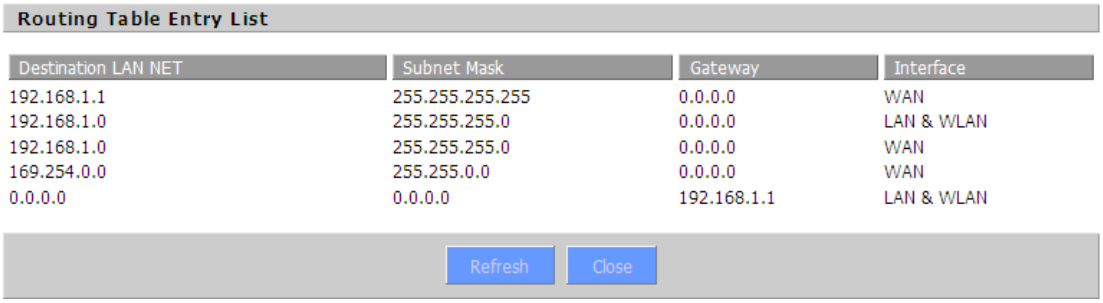
Destination LAN NET: the Destination IP Address is the address of the network or host to which users want to assign a static route

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

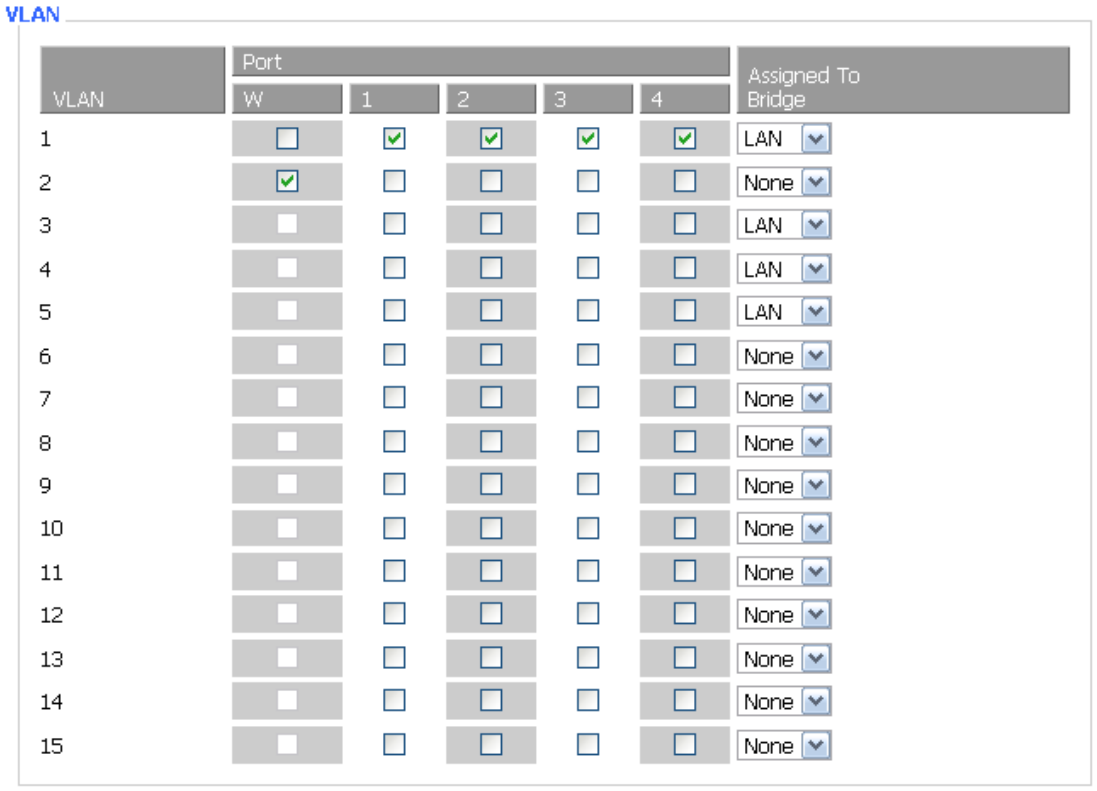
Gateway: IP address of the gateway device that allows for contact between the Router and the network or host.

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

Show Routing Table

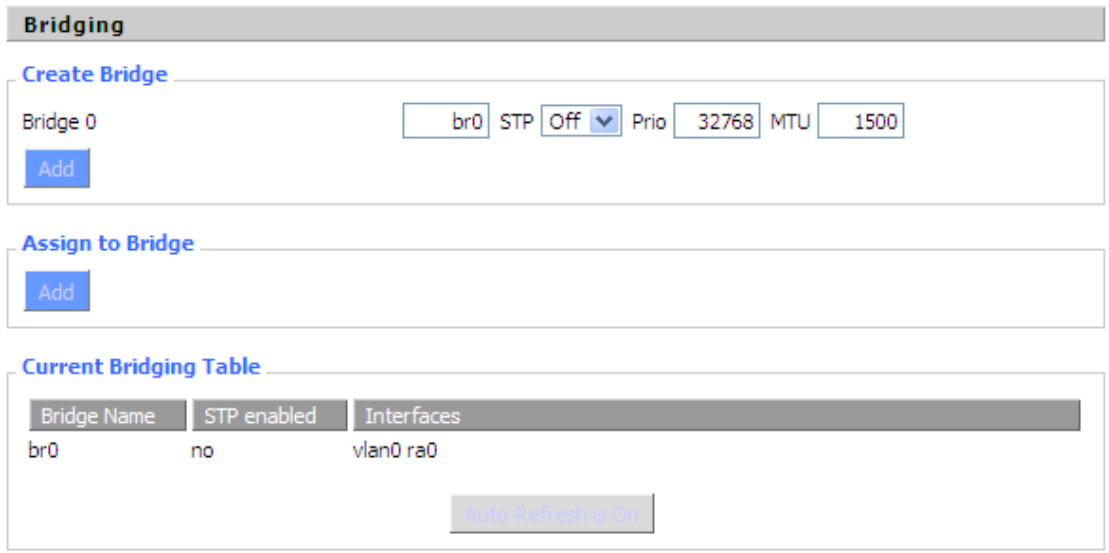


3.3.1.5 VLANs



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.

3.3.1.6 Networking



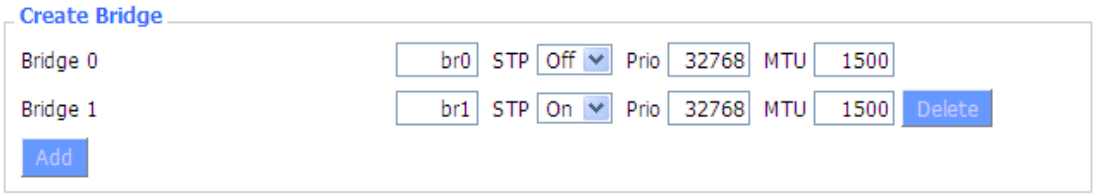
Bridging-Create Bridge: creates a new empty network bridge for later use. STP means Spanning Tree Protocol and with PRIO users are able to set the bridge priority order. The lowest number has the highest priority.

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.

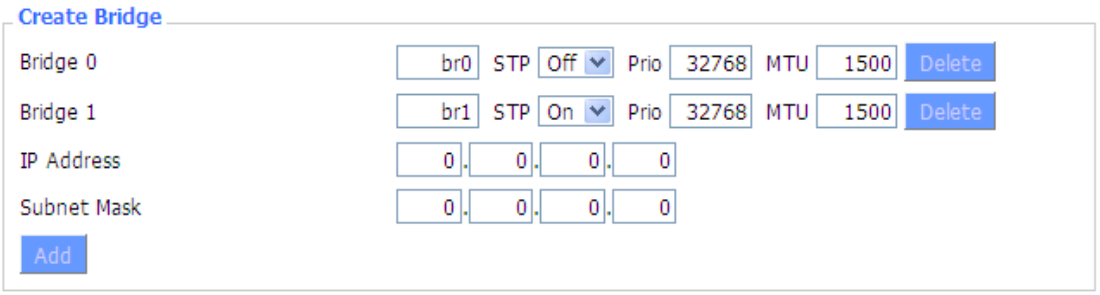
Current Bridging Table: shows current bridging table

Create steps as below:

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

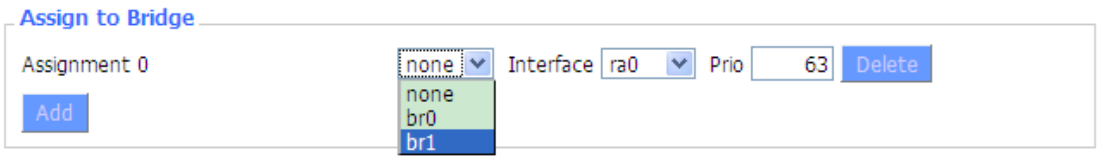


Create bridge option: the first br0 means bridge name. STP means to on/off spanning tree protocol. Prio means priority level of STP, the smaller the number, the higher the level. MTU means maximum transfer unit, default is 1500, delete if it is not need. And then click 'Save' or 'Add'. Bride properties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



Enter relewant 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:

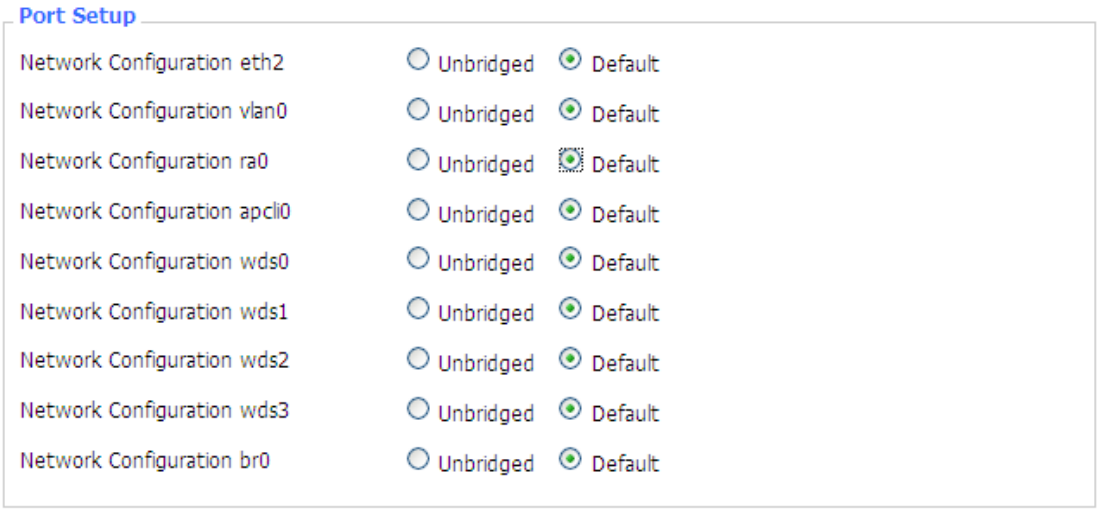
Prio means priority level: work if multiple ports are within the same bridge. The smaller the number, the higher the level. Click 'Add' to take it effect.

Note: corresponding interface of WAN ports interface should not be binding, this bridge

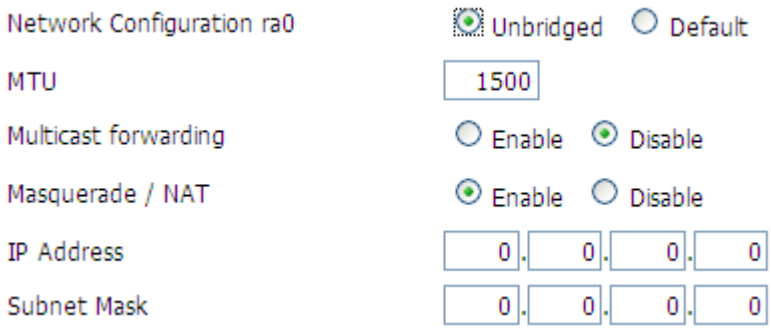
function is basically used for LAN port, and should not be binding with WAN port

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

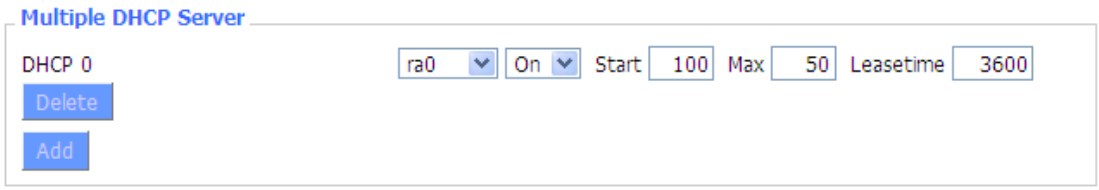
To make br1 bridge has the same function with DHCP assigned address, users need to set multiple DHCP function, see the introduction of multi-channel DHCPD:



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

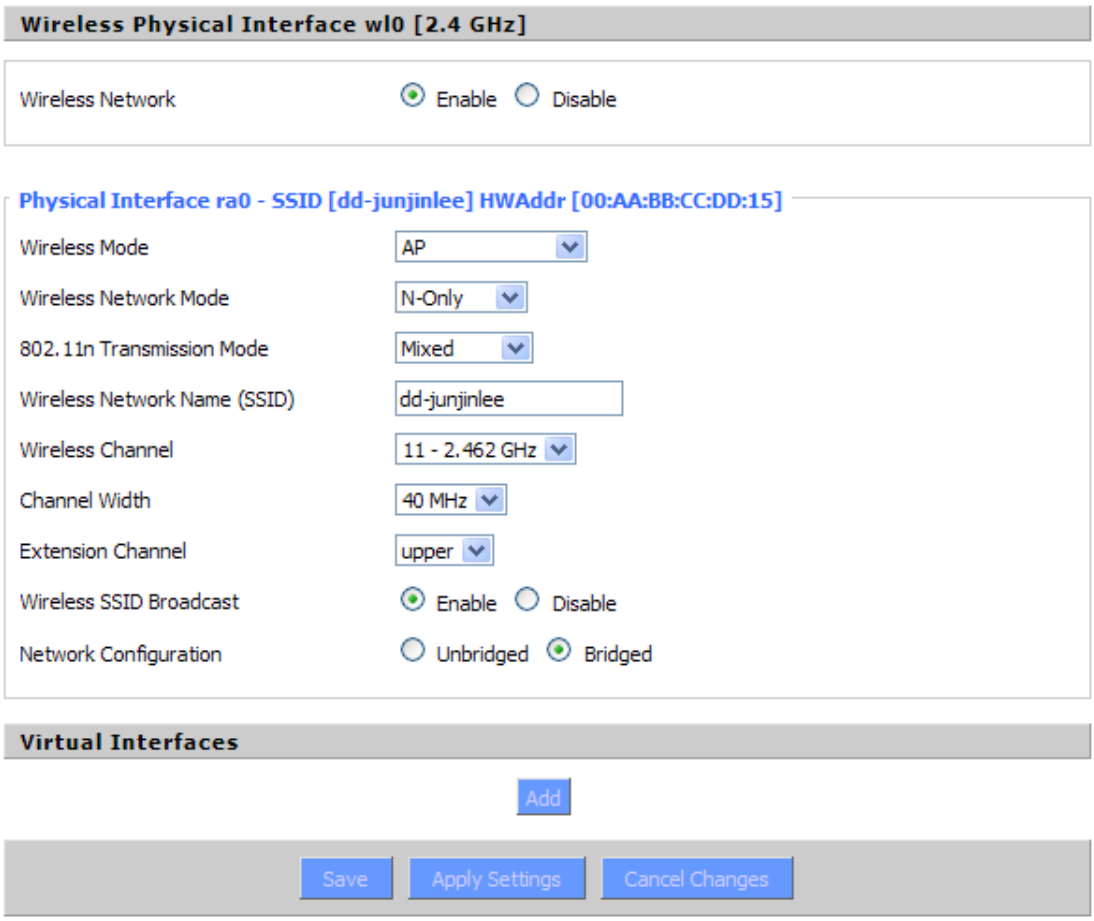


Multiple DHCPD: using multiple DHCP service. Click 'Add' in multiple DHCP server to appear relevant configuration. The first means the name of port or bridge (do not be configured as eth0), the second means whether to on DHCP. Start means start address, Max means maximum assigned DHCP clients, Leasetime 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, can not configure multiple DHCP at the same time.

3.3.2 Wireless

3.3.2.1 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.

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.

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

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：

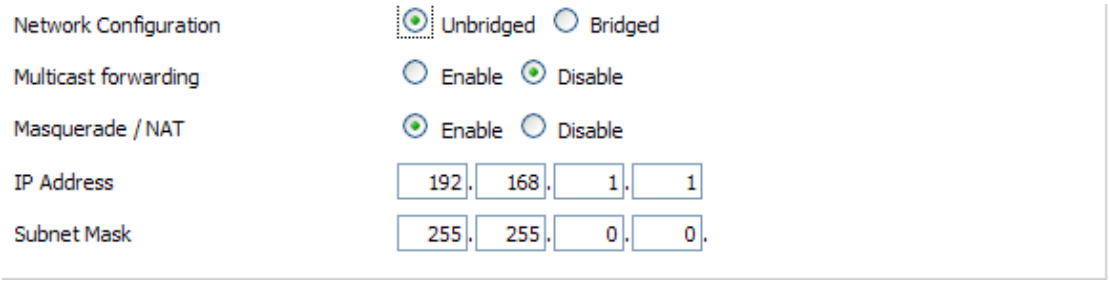
Enable：SSID broadcasting.

Disable：Hidden SSID.

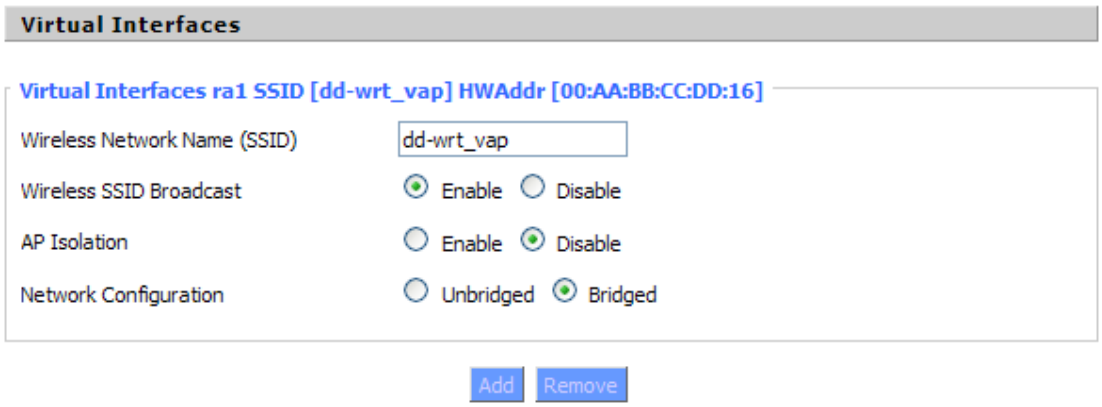
Network Configuration：

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。

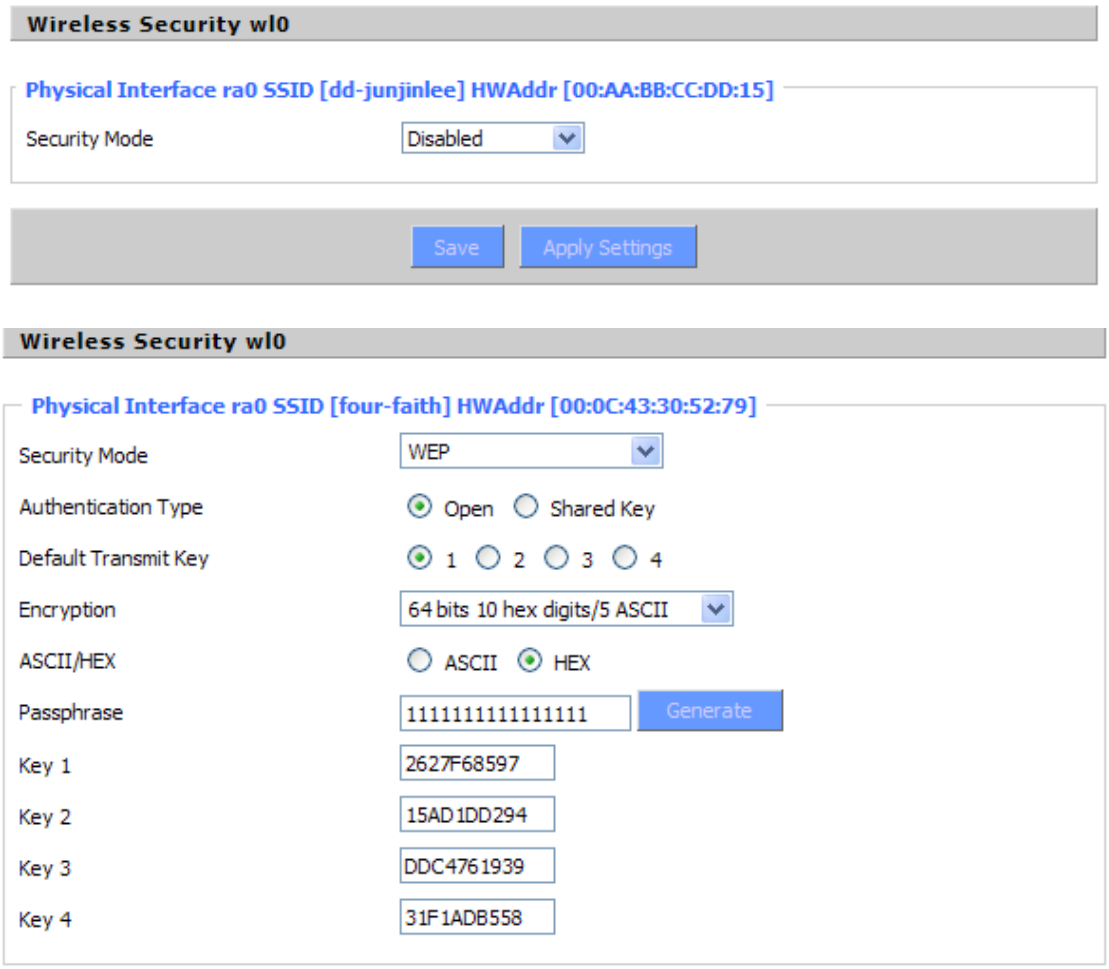


AP Isolation：This setting isolates wireless clients so access to and from other wireless clients are stopped.

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.

3.3.2.2 Wireless Security

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



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

Authentication Type：Open or shared key。

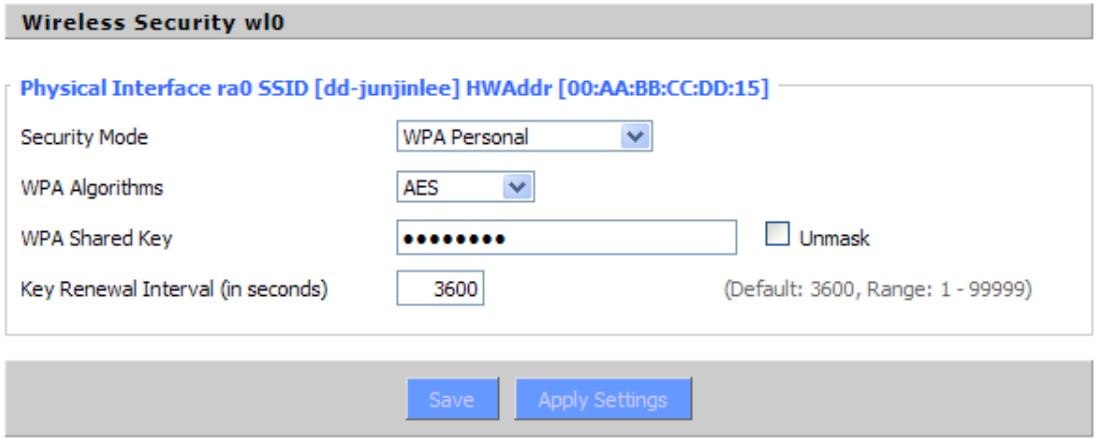
Default Transmit Key：Select the key form Key 1 - Key 4 key.

Encryption：There are two levels of WEP encryption, 64-bit (40-bit) and 128-bit. To utilize WEP, select the desired encryption bit, and enter a passphrase or up to 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 charceters. 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.

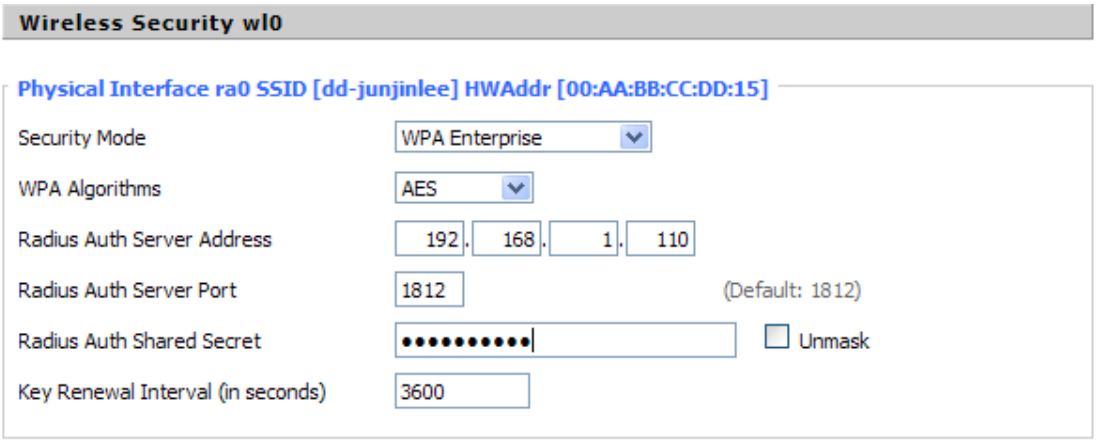
Key1-Key4：Manually fill out or generated according to input the pass phrase.



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。



WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed: WPA Enterprise uses an external RADIUS server to perform user authentication.

WPA Algorithms: AES/TKIP/TPIP+AES.

Radius Auth Sever Address：The IP address of the RADIUS server.

Radius Auth Server Port：The RADIUS Port (default is 1812)。

Radius Auth Shared Secret：The shared secret from the RADIUS server。

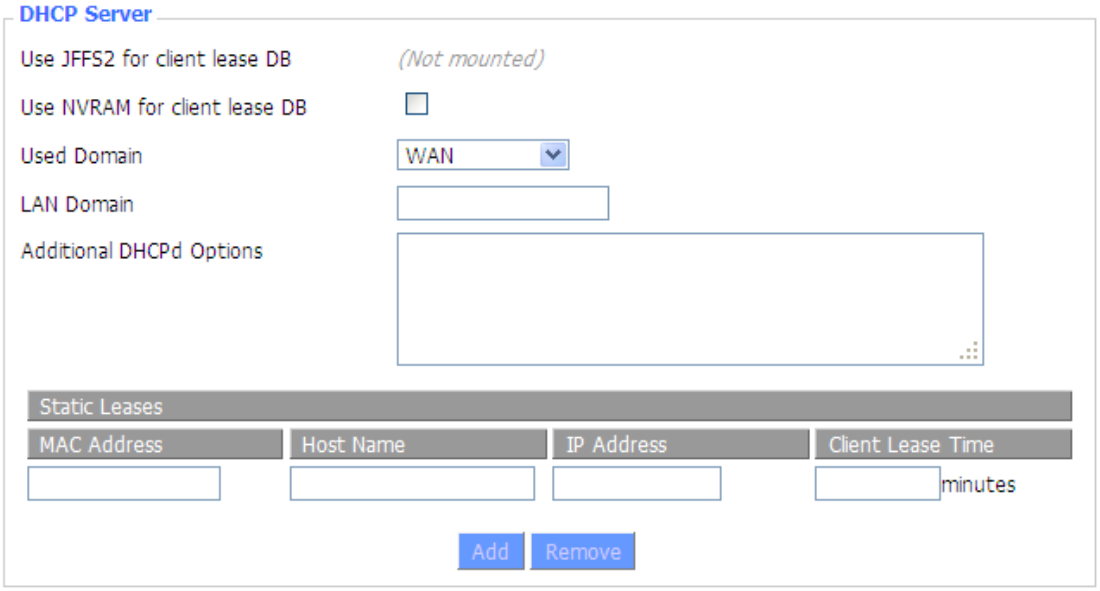
Key Renewal Interva(in seconds): 1-99999。

3.3.3 Services

3.3.3.1 Services

DHCP Server

DHCPd 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.

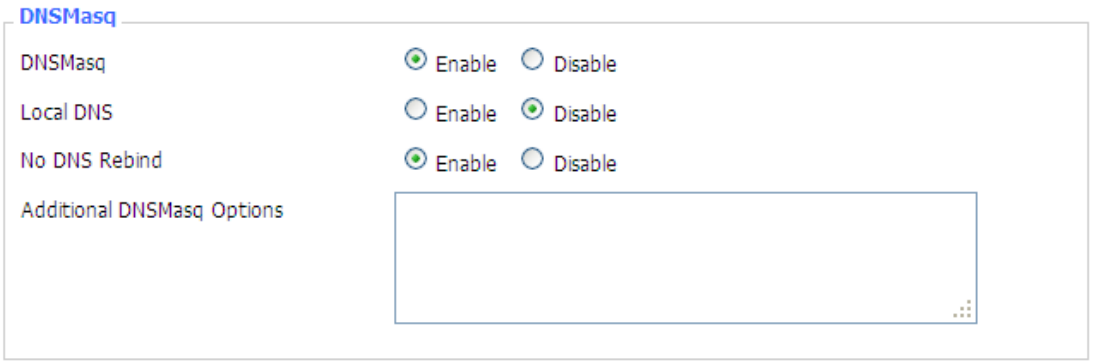
LAN Domain: users can define here their local LAN domain which is used as local domain for DNSmasq and DHCP service if chose above.

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.



Local DNS: enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames

No DNS Rebind:

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

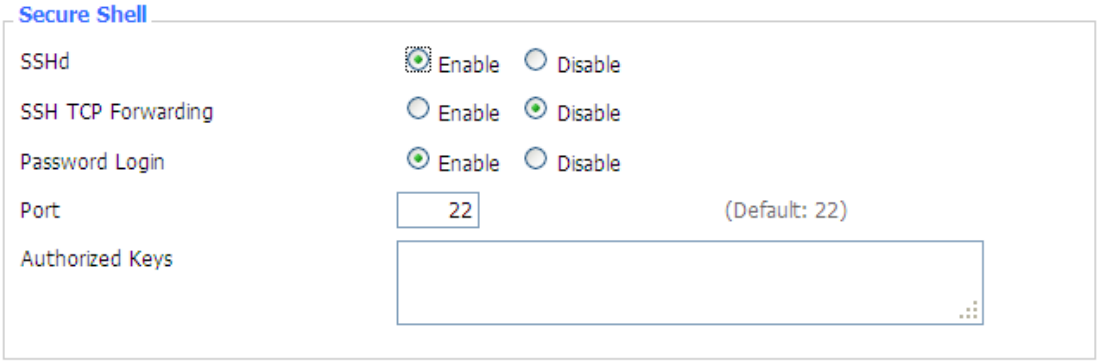
Name: device name

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

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

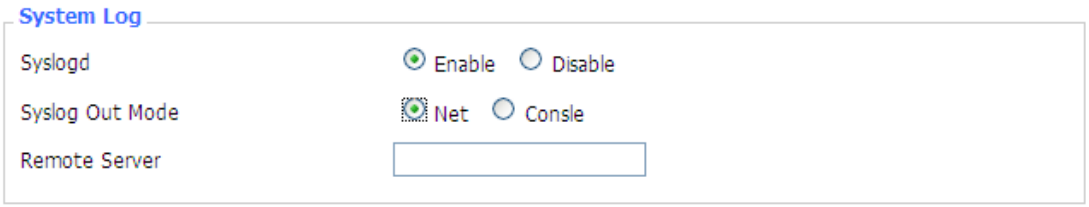
Password Login: allows login with the Router password (username is admin)

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 Syslogd 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.



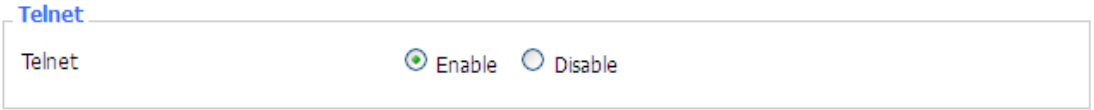
Syslog Out Mode: two log mode

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.

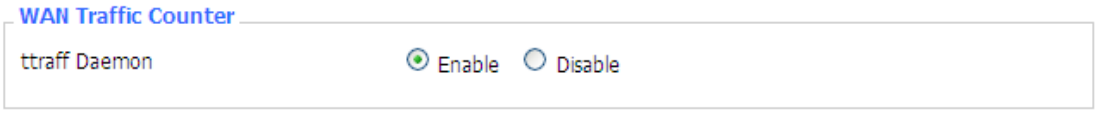
Telnet



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

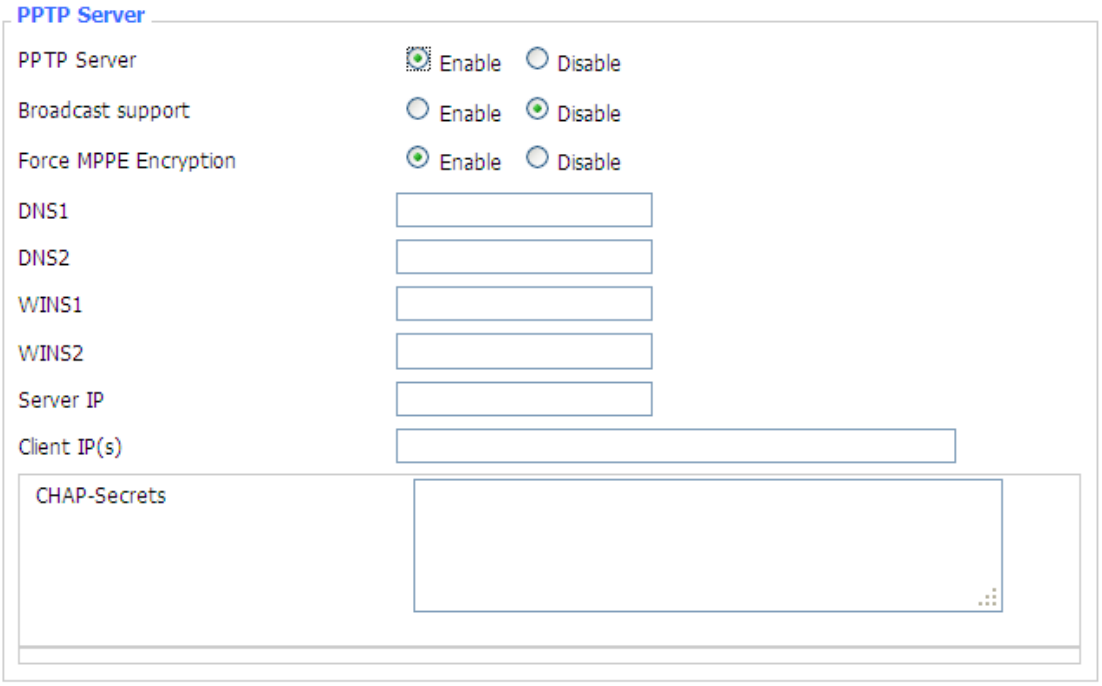


Ttraff Daemon: enable or disable wan traffic counter function

3.3.4 VPN

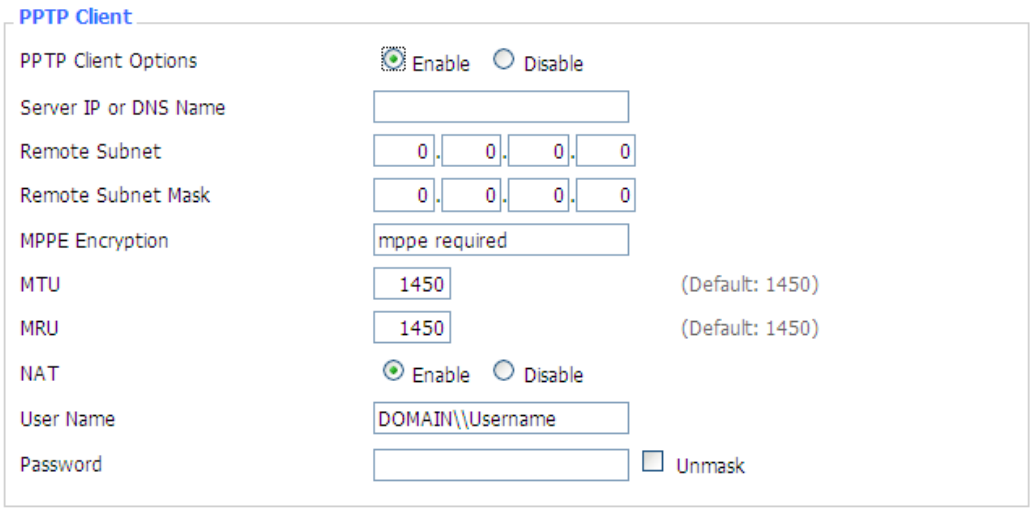
3.3.4.1 PPTP

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: user name 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 *.

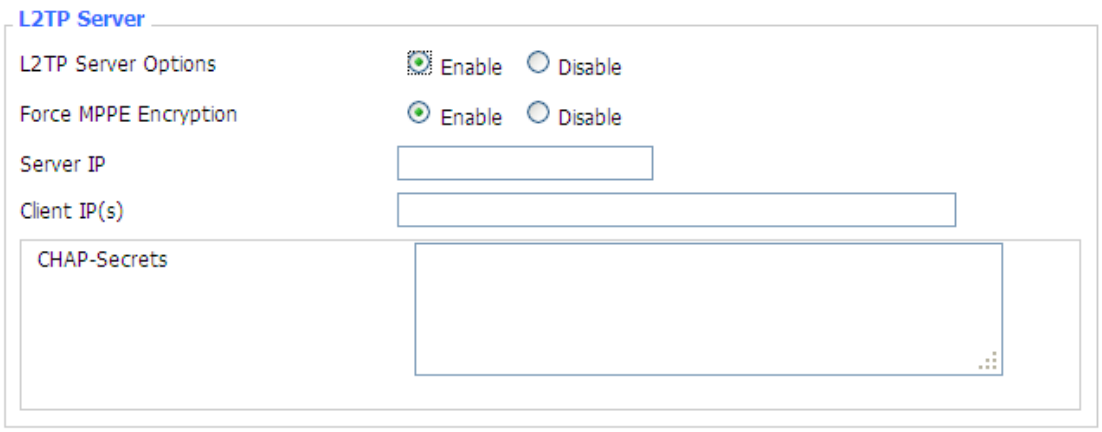
PPTP Client



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
User Name: user name to login PPTP Server.
Password: password to log into PPTP Server.

3.3.4.2 L2TP

L2TP Server



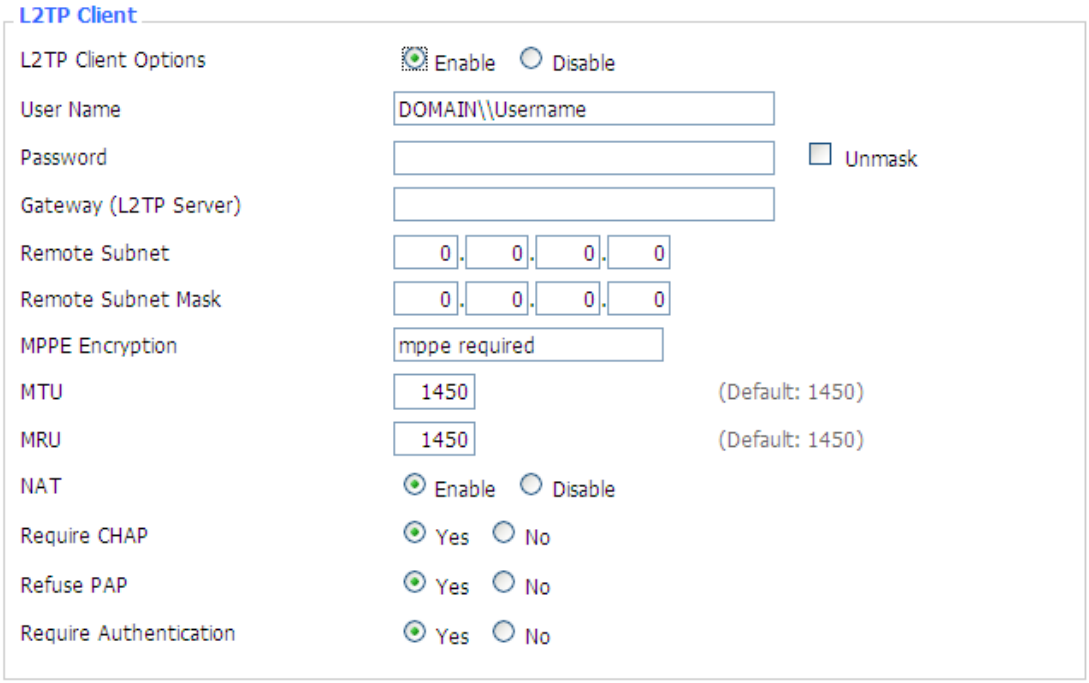
Force MPPE Encryption: enable or disable force MPPE encryption of L2TP data
Server IP: input IP address of the Router as PPTP server, differ from LAN address
Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx

CHAP Secrets: user name and password of the client using L2TP service

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

User Name: user name 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

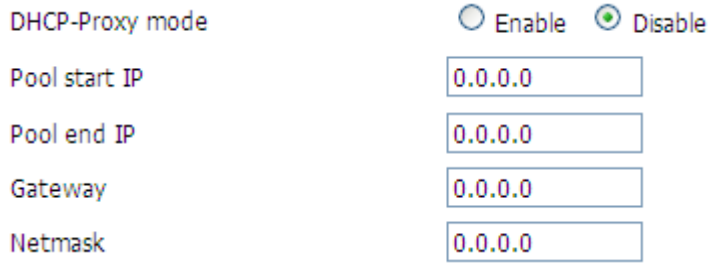
3.3.4.3 OPENVPN

OPENVPN Server

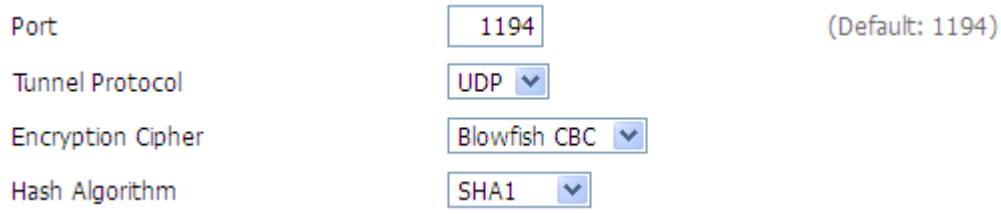
Start Type: WAN UP----start after on-line, System----start when boot up

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):



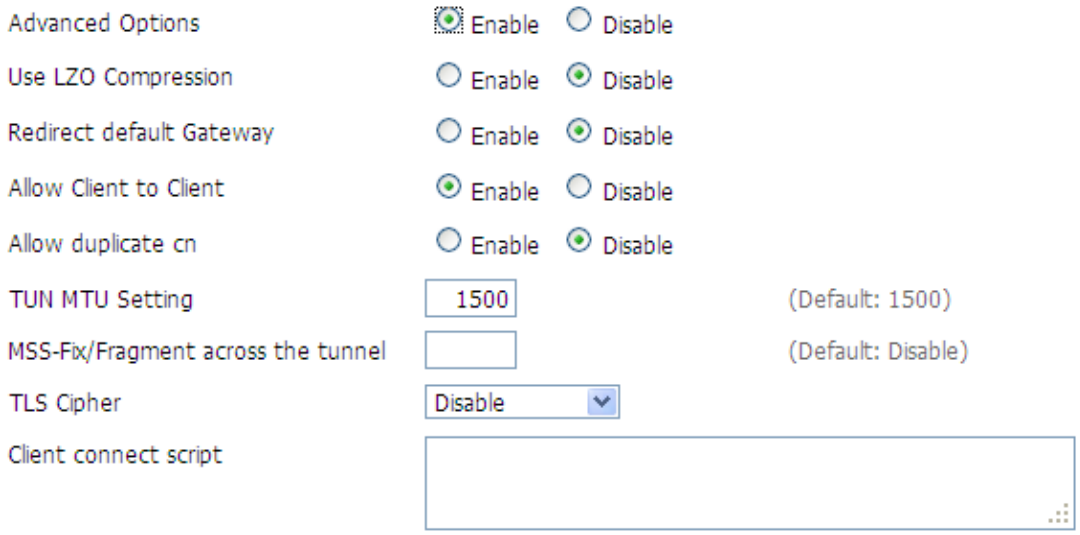
DHCP-Proxy mode: enable or disable DHCP-Proxy mode
Pool start IP: pool start IP of the client allowed by OPENVPN server
Pool end IP: pool end IP of the client allowed by OPENVPN server
Gateway: the gateway of the client allowed by OPENVPN server
Netmask: netmask of the client allowed by OPENVPN server



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

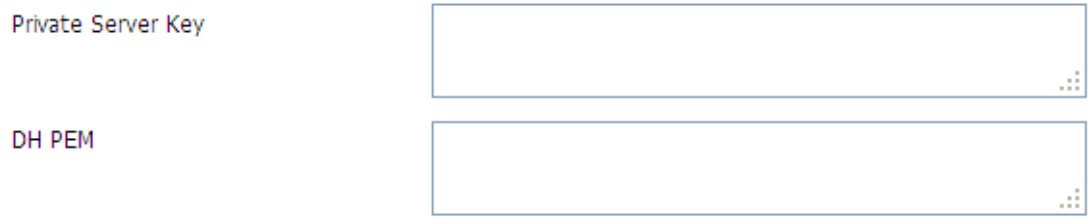
Advanced Options



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

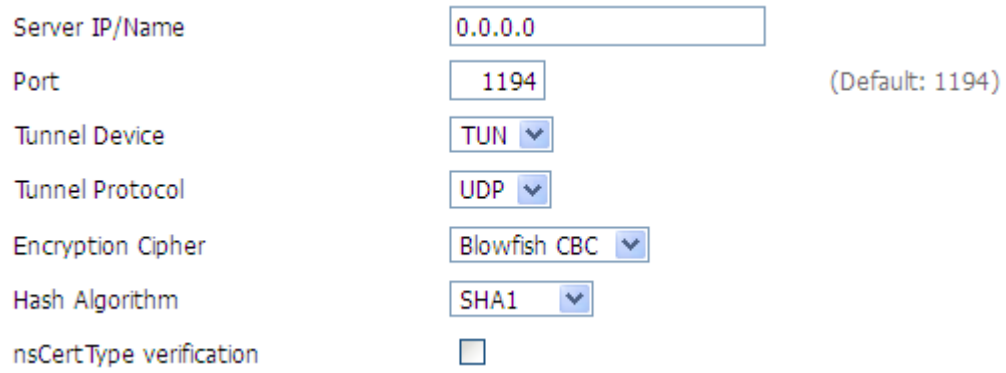
Public Server Cert: server certificate



Private Server Key: the key seted by the server
DH PEM: PEM of the server

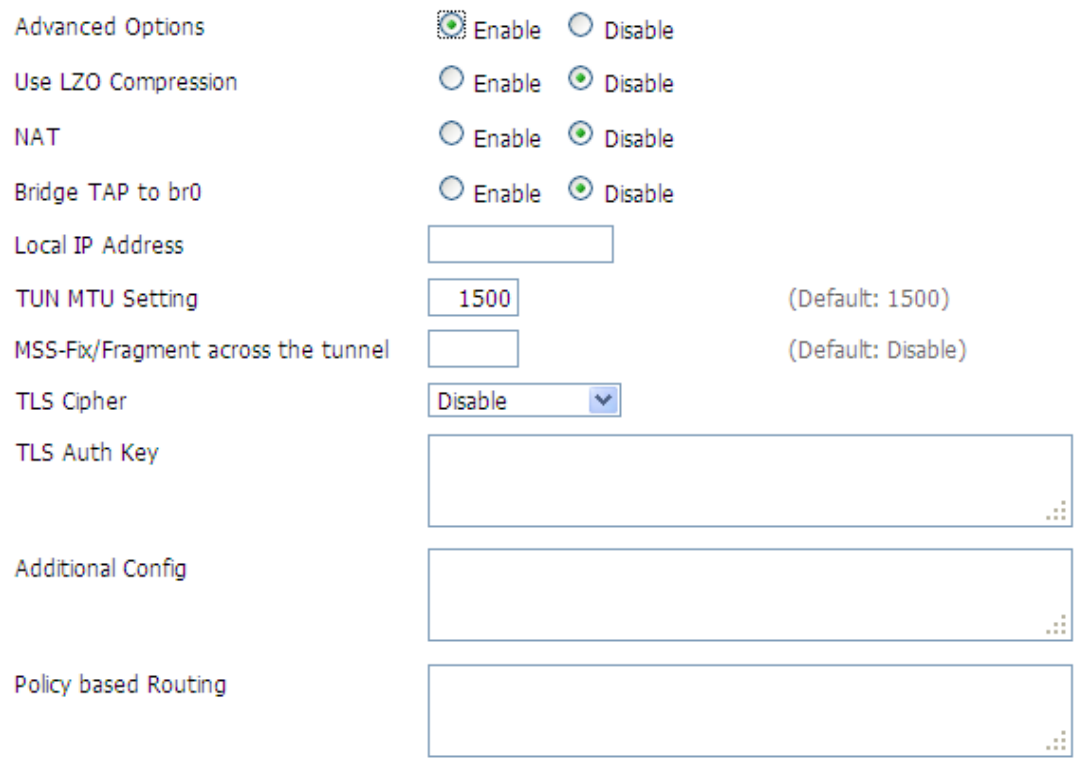
Additional Config: additional configurations of the server
CCD-Dir DEFAULT file: other file approaches
TLS Auth Key: authority key of Transport Layer Security
Certificate Revoke List: configure some revoke certificates

OPENVPN Client



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

CA Cert: CA certificate

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

3.3.4.4 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

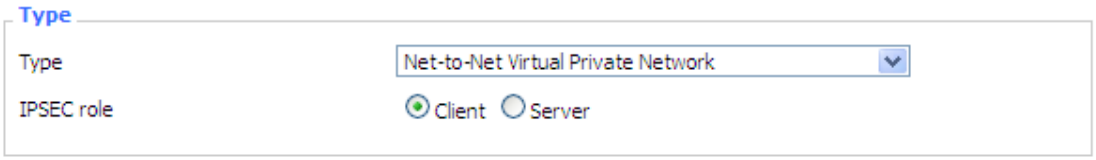
Reconnect: this action will remove current tunnel, and re-launch tunnel establish request

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

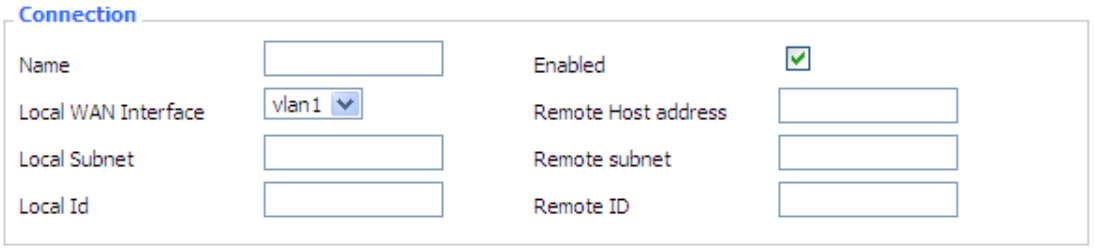
Add: to add a new IPSEC connection

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 can not fill in if using tunnel mode server

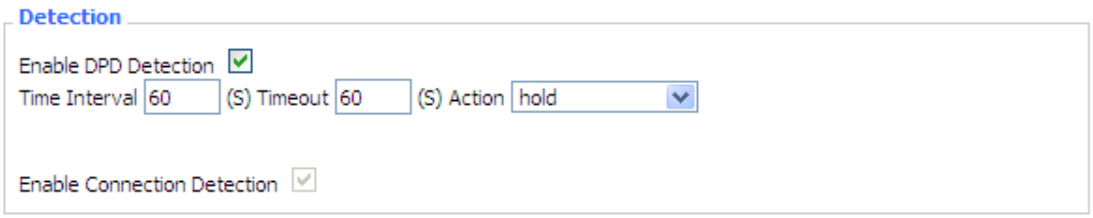
Local Subnet: IPSec local protects subnet and subnet mask, i.e. 192.168.1.0/24; this option can not fill in if using transfer mode

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

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

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

Detection: this part contains configure information of connection detection



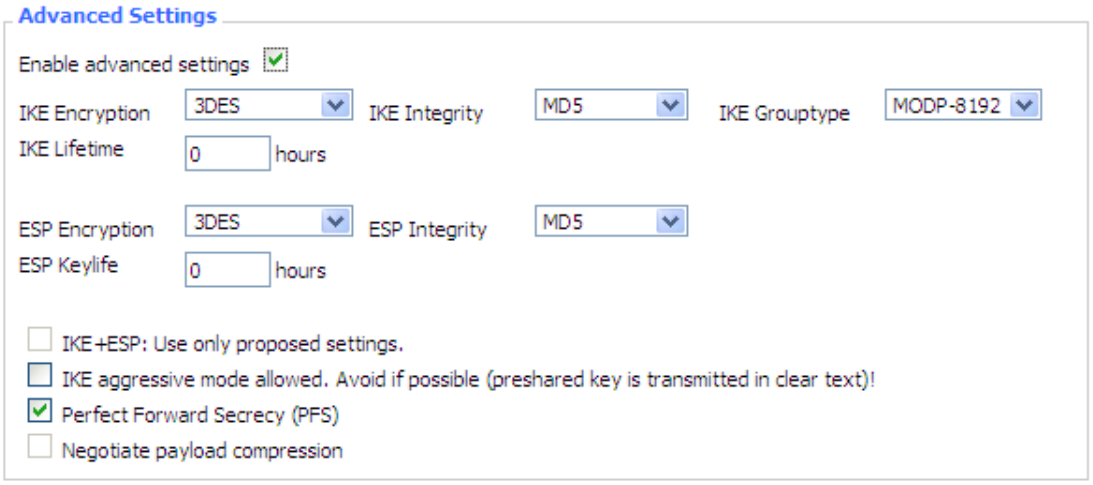
Enable DPD Detection: enable or disable this function, tick means enable

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.



Enable Advanced Settings: enable to configure 1st and 2nd phase information, otherwise it

will automic 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

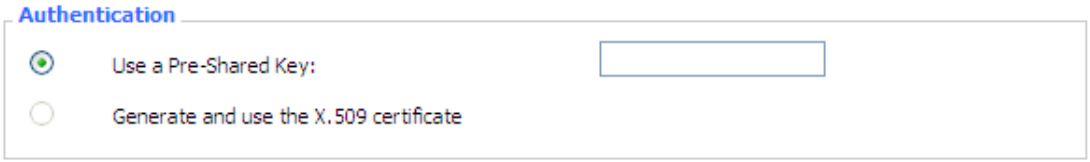
ESP Keylife: set ESP keylife, current unit is hour, the default is 0

IKE aggressive mode allowed: negotiation mode adopt aggressive mode if tick; it is main

mode if non-tick

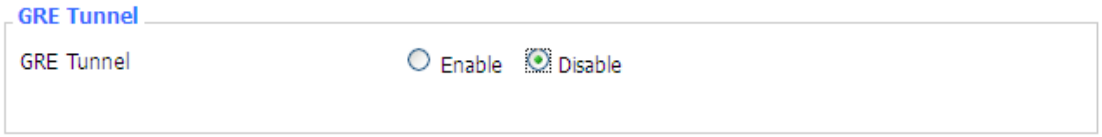
Negotiate payload compression: Tick to enable PFS, non-tick to diable PFS

Authentication: choose use share encryption option or certificate authentication option. Current is only to choose use share encryption option.

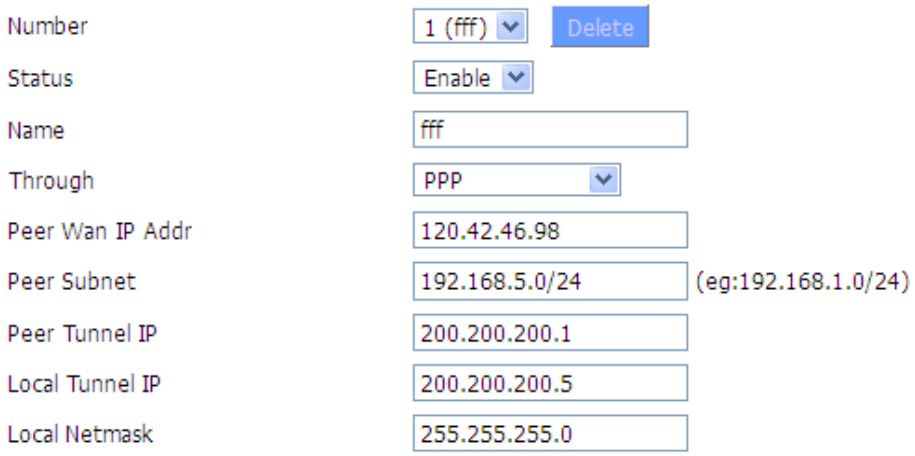


3.3.4.5 GRE

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).



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

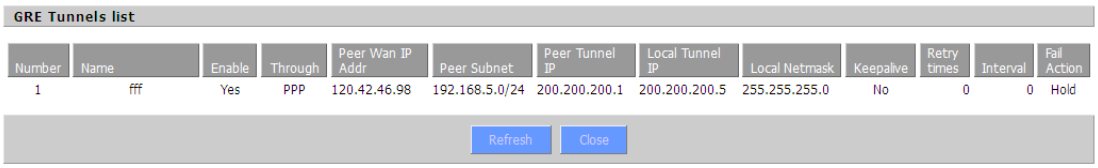
Keepalive：Enable or disable GRE Keepalive function

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

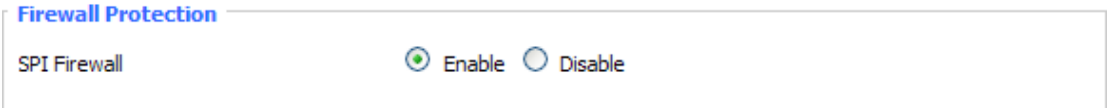


3.3.5 Security

3.3.5.1 Firewall

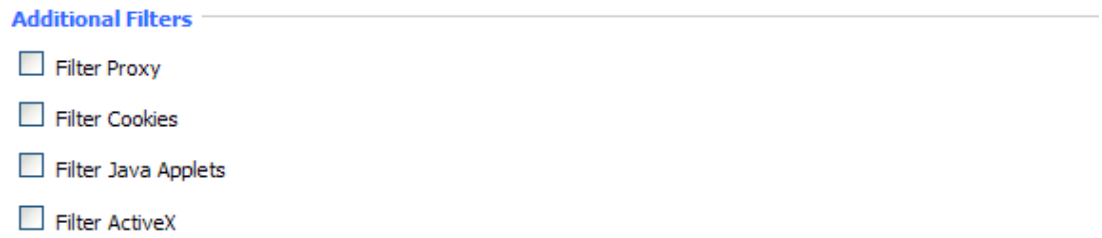
You can enable or disable the firewall, filter specific Internet data types,and prevent anonymous Internet requests,ultimately enhance network security.

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



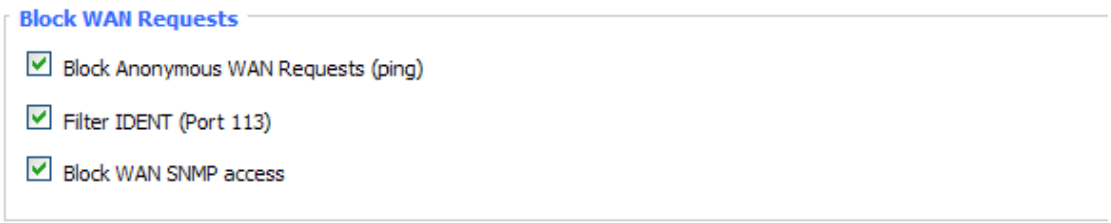
Filter Proxy: Wan proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

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 from the Ping or

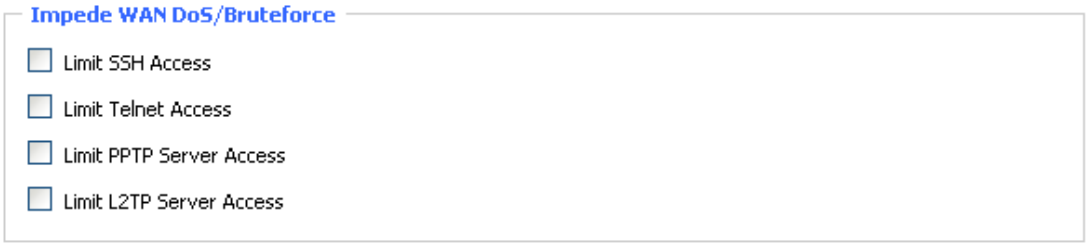
detection of other Internet users. so that make More difficult to break into your network. The default state of this feature is enabled ,choose to disable allow anonymous Internet requests.

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.

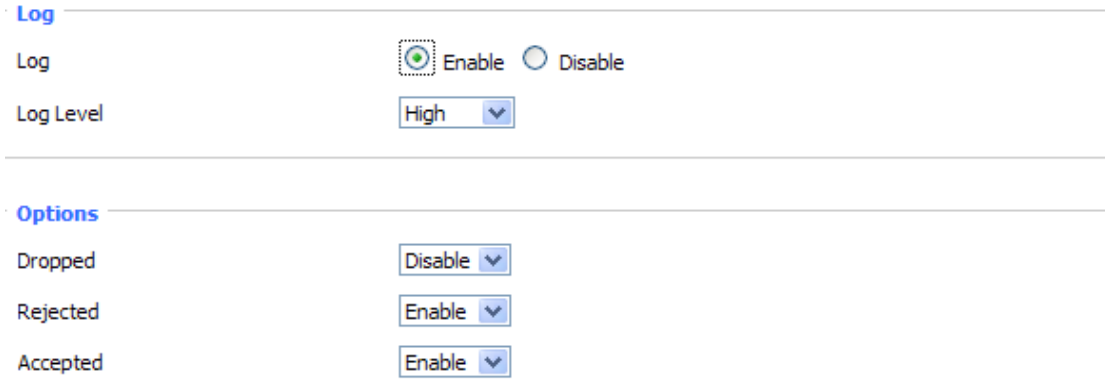
Limit PPTP Server Access: When build a PPTP Server in the Router,this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP . Any new access request will be automatically dropped.

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.

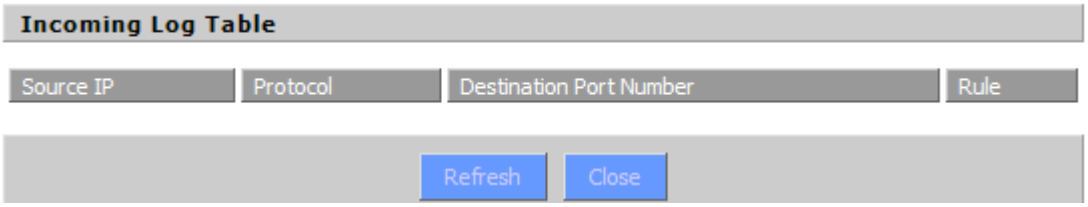
Log Management

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

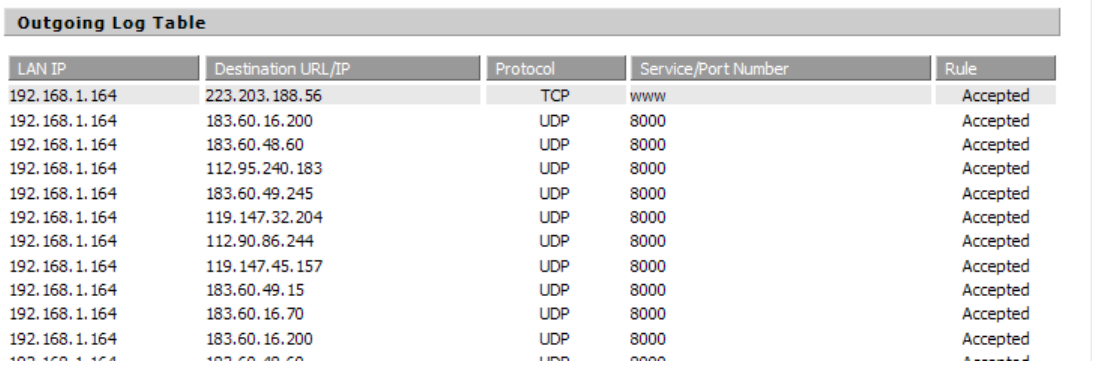
Log: To keep activity logs, select Enable. To stop logging, select Disable. When select enable, the following page will appear.



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

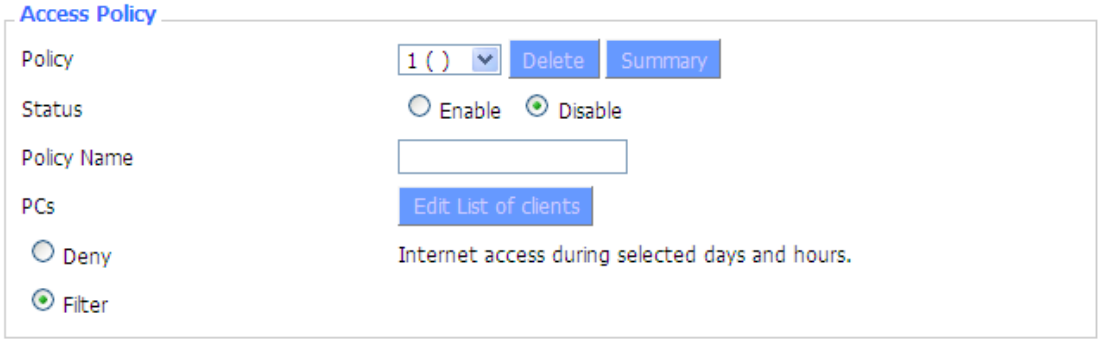
LAN IP	Destination URL/IP	Protocol	Service/Port Number	Rule
192.168.1.164	223.203.188.56	TCP	www	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted
192.168.1.164	112.95.240.183	UDP	8000	Accepted
192.168.1.164	183.60.49.245	UDP	8000	Accepted
192.168.1.164	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.

3.3.6 Access Restrictions

3.3.6.1 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.



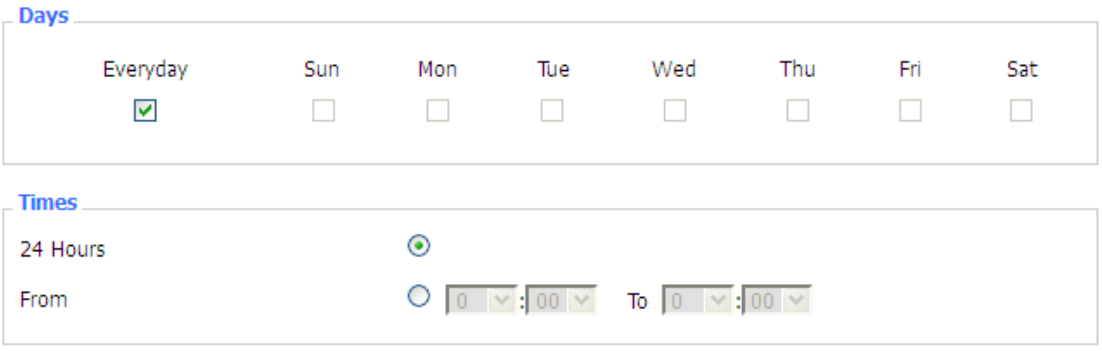
Two options in the default policy rules: "Filter" and "reject". If select "Deny", you will deny specific computers to access any Internet service at a particular time period. If you choose to "filter", It will block specific computers to access the specific sites at a specific time period. You can set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

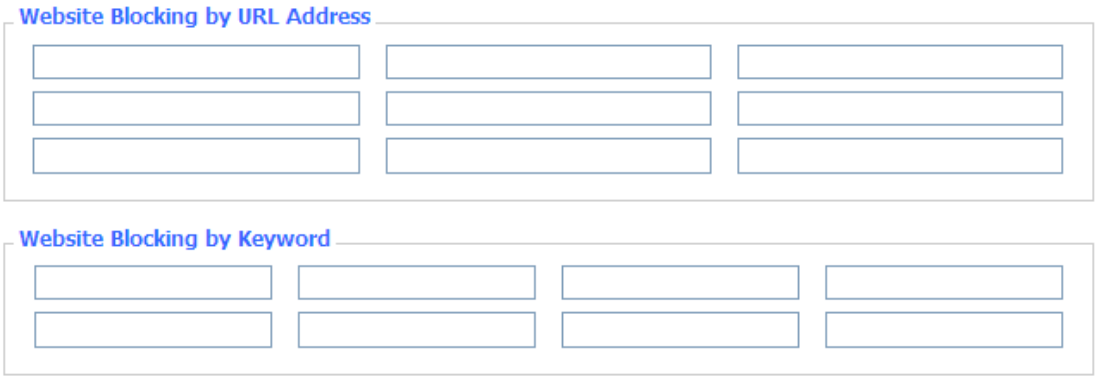
Policy Name: You may assign a name to your policy.

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



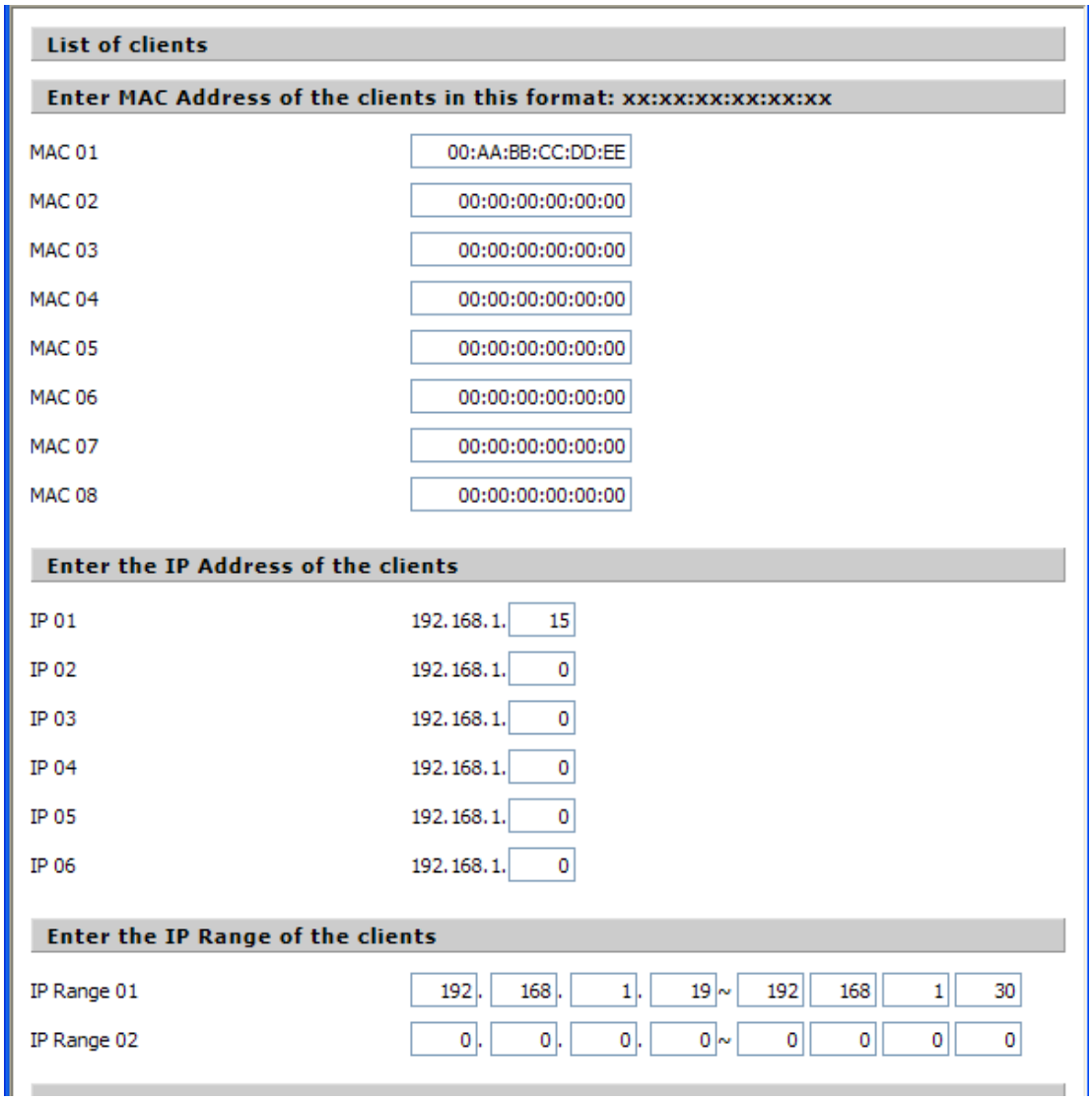
Days: Choose the day of the week you would like your policy to be applied.

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



set up Internet access policy

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

For this policy is enabled, click the radio button next to "Enable"

Enter a name in the Policy Name field.

Click the Edit List of PCs button.

On the List of PCs screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the IP fields. If you have a range of IP addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC addresses into the MAC fields.

Click the Apply button to save your changes. Click the Cancel button to cancel your unsaved changes. Click the Close button to return to the Filters screen.

If you want to block the listed PCs from Internet access during the designated days and time, then keep the default setting, Deny. If you want the listed PCs to have Internet filtered during the designated days and time, then click the radio button next to Filter.

Set the days when access will be filtered. Select Everyday or the appropriate days of the week.

Set the time when access will be filtered. Select 24 Hours, or check the box next to From and use the drop-down boxes to designate a specific time period.

Click the Add to Policy button to save your changes and active it.

To create or edit additional policies, repeat steps 1-9.

To delete an Internet Access Policy, select the policy number, and click the Delete button.

Note:

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

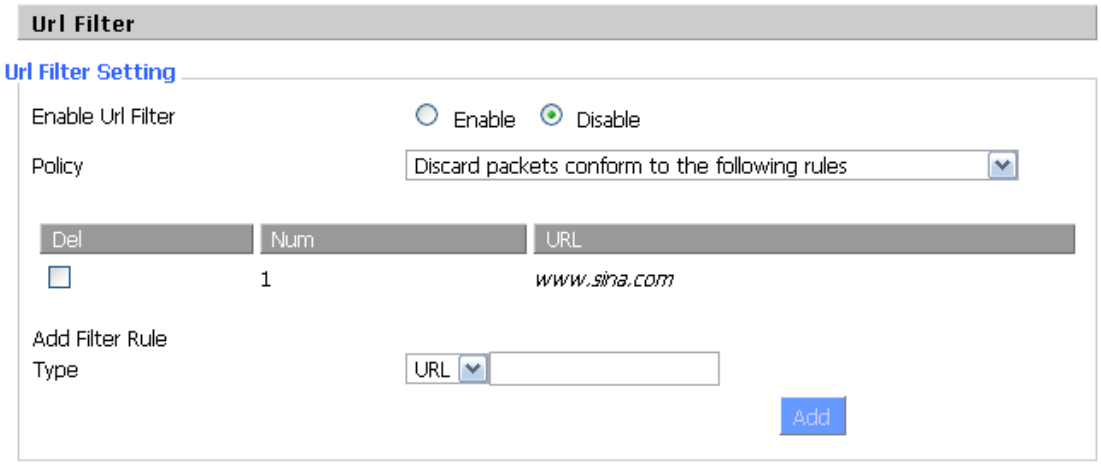
Turn off the power of the Router or reboot the Router can cause a temporary failure。

After the failure of the Router, if can not automatically synchronized NTP time server, you need to recalibrate to ensure the correct implementation of the relevant period control function.

3.3.6.2 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 .

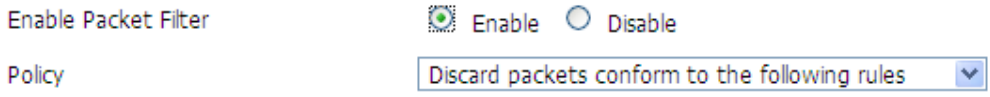
Accept only the data packets conform to the following rules: receive only with custom rules of network address, discarded all other URL address.

3.3.6.3 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.

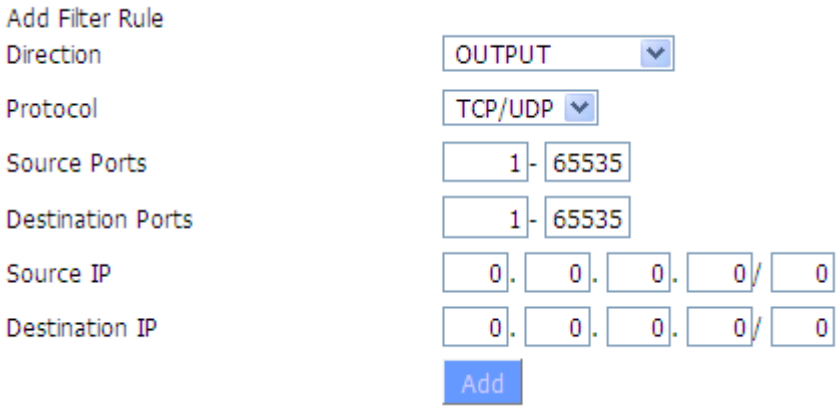


Enable Packet Filter: Enable or disable “packet filter” function

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

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

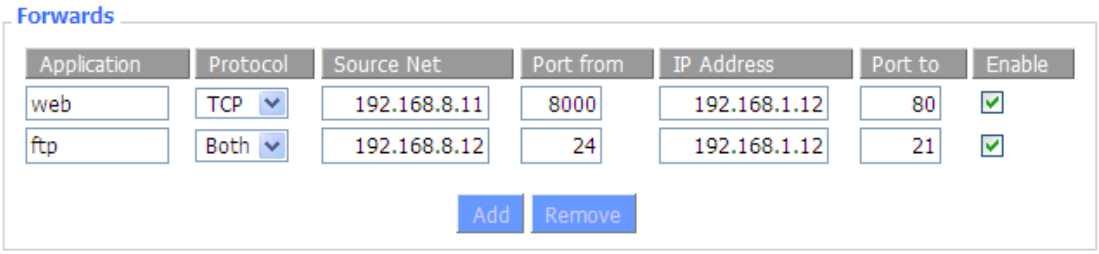
Protocol: packet protocol type
Source Ports: packet's source port
Destination Ports: packet's destination port
Source IP: packet's source IP address
Destination IP: packet's destination IP address

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.

3.3.7 NAT

3.3.7.1 Port Forwarding

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

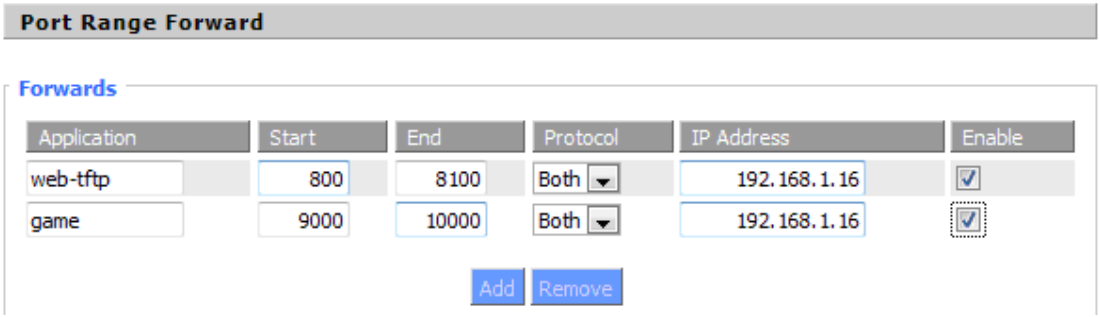


Application: Enter the name of the application in the field provided.
Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.
Source Net: Forward only if sender matches this ip/net (example 192.168.1.0/24).
Port from: Enter the number of the external port (the port 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.

3.3.7.2 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 seen by users on the Internet and forwarded to your PC.
End: Enter the number of the last port of the range you want to seen by users on the Internet and forwarded to your PC.
Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application

requires.

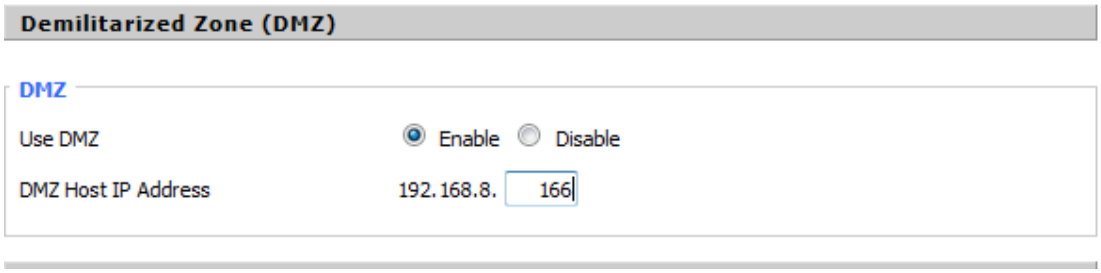
IP Address: Enter the IP Address of the PC running the application.

Enable: Click the Enable 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.

3.3.7.3 DMZ

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



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

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

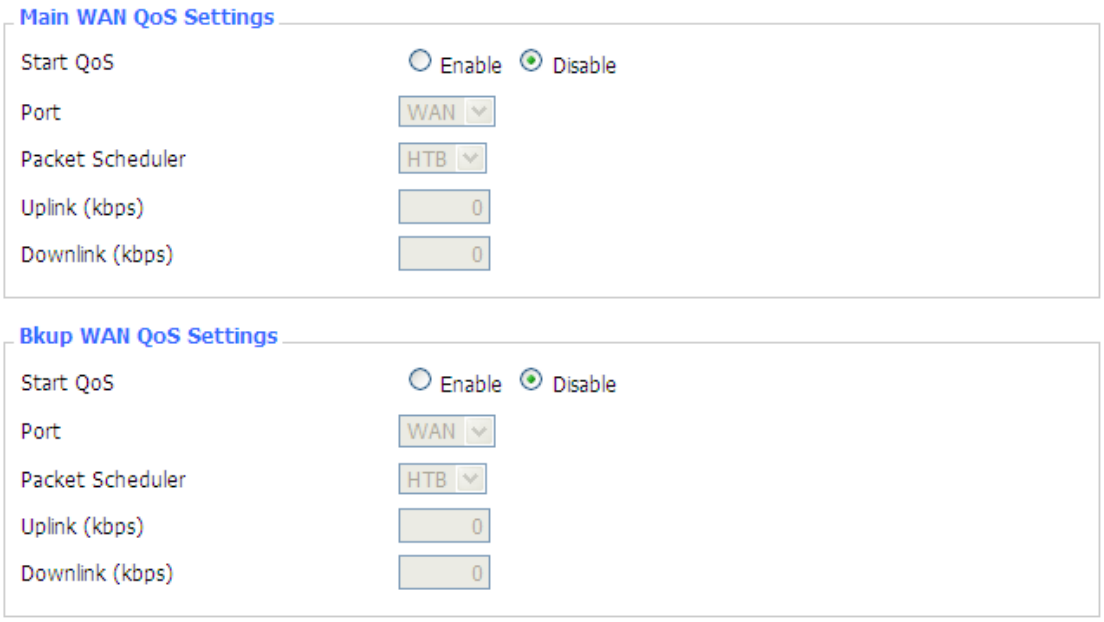
Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.8 QoS Setting

3.3.8.1 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 more or less automatic.

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

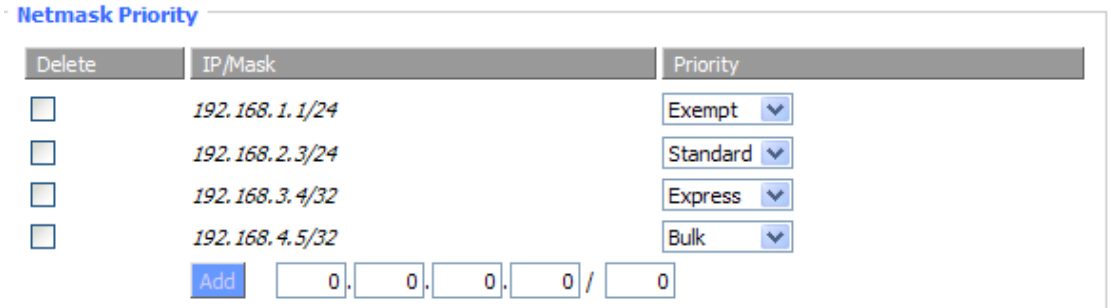


Uplink (kbps)： In order to use bandwidth management (QoS) you must enter bandwidth values for your uplink. These are generally 80% to 90% of your maximum bandwidth.

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.

3.3.8.2 Classify

Netmask Priority



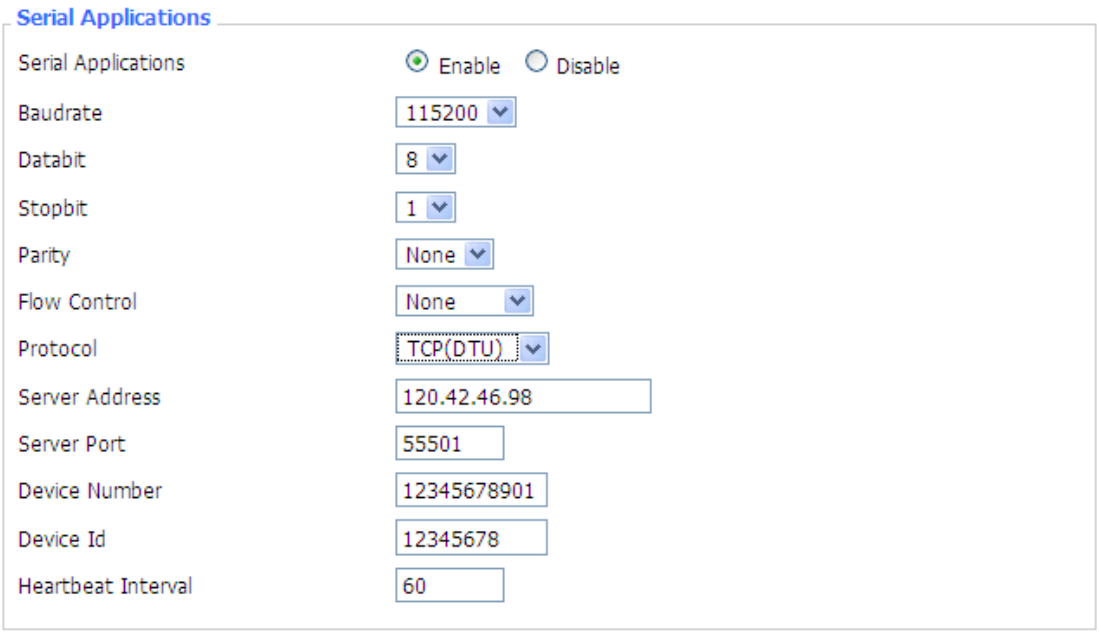
You may specify priority for all traffic from a given IP address or IP Range.

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

3.3.9.1 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).



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 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 IP 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 heart beat packet. This item is valid only when you choose UDP(DTU) or TCP(DTU) protocol type.

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

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

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

3.3.10 Administration

3.3.10.1 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:

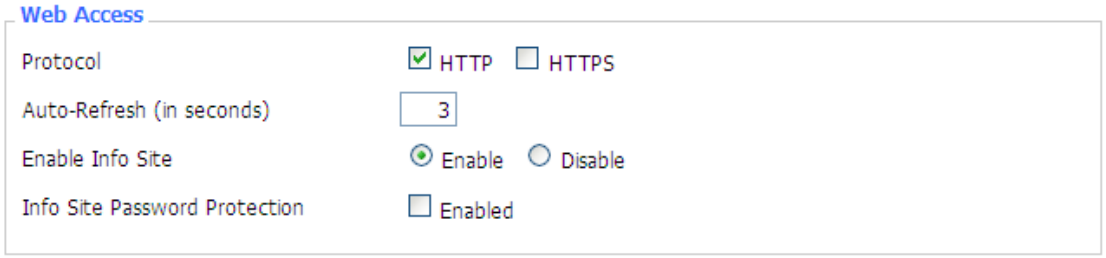
Default username is admin.

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).

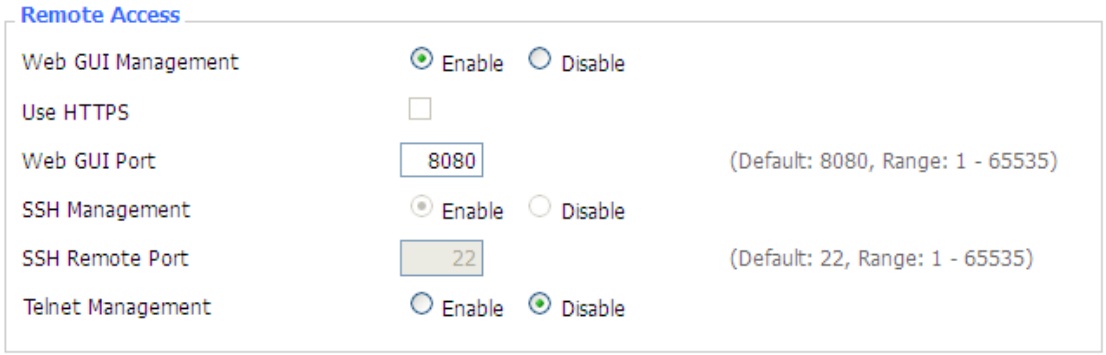


Protocol：This feature allows you to manage the Router using either HTTP protocol or the HTTPS protocol

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



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.

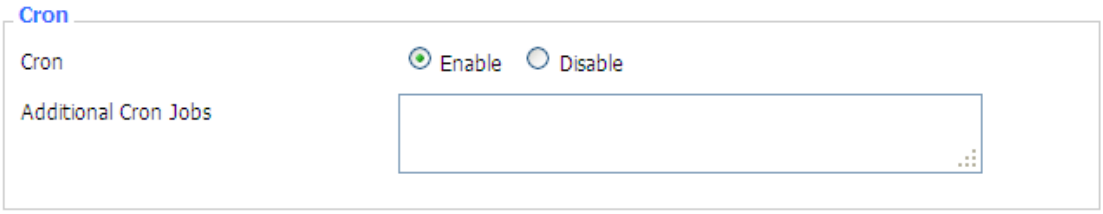
If you use https you need to specify the url as https://xxx.xxx.xxx.xxx:8080 (not all firmwares does support this without rebuilding with SSL support).

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.

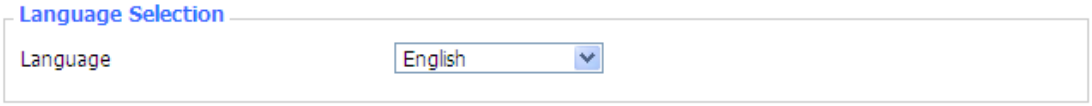
Note：

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.

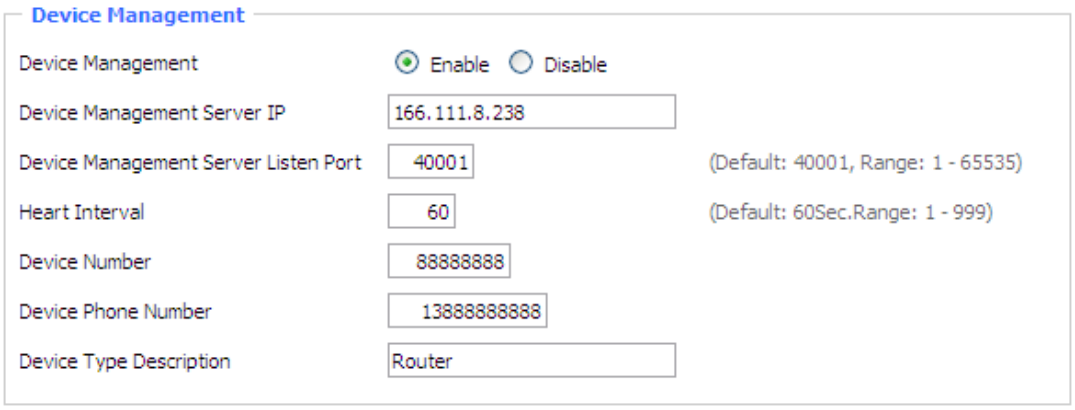
Telnet Management：Enable or disable remote Telnet function



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



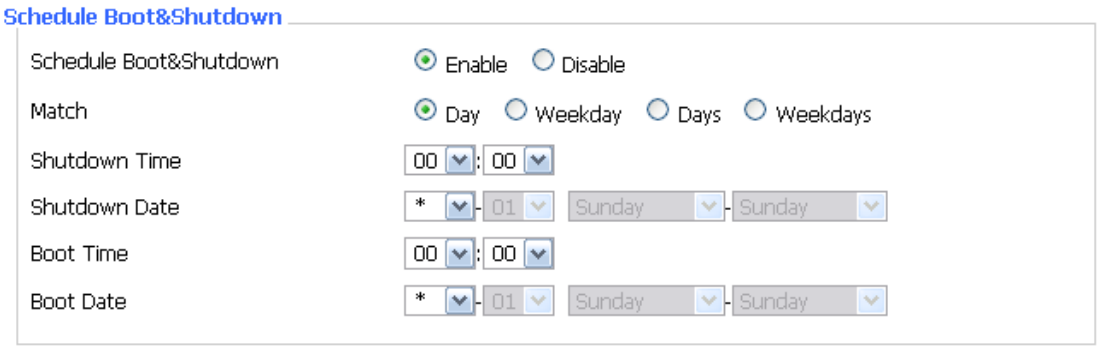
Language： Set up the Router page shows the type of language, including simplified Chinese and English.



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

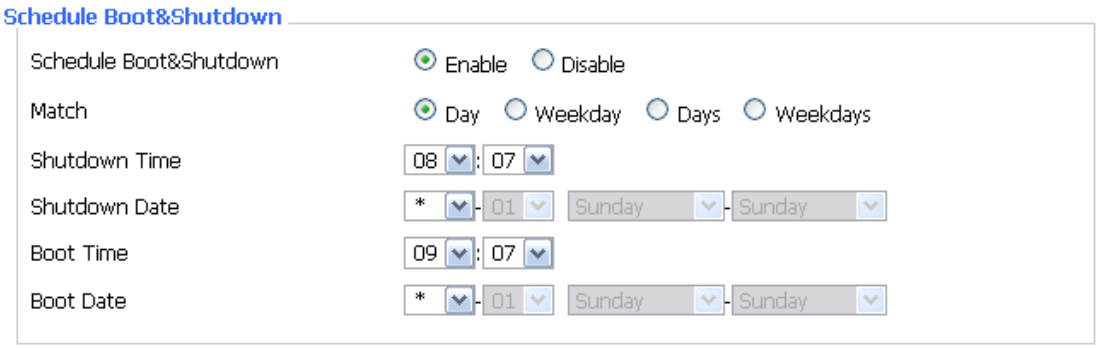
3.3.10.2 Keep Alive

Schedule Boot&Shutdown

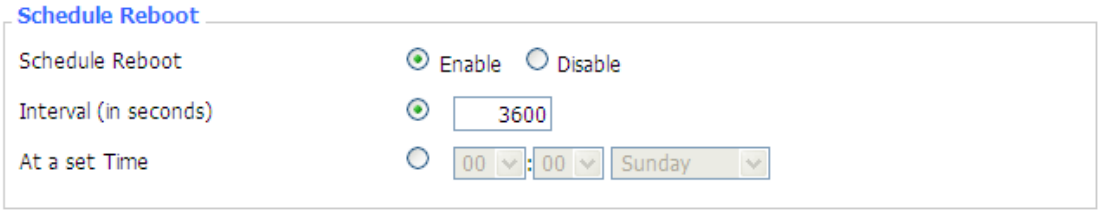


The user can set the startup or shutdown time:

For example,the user want to set the start time at 8:07 and boot time at 9:07.



Schedule Reboot



You can schedule regular reboots for the Router :

Regularly after xxx seconds.

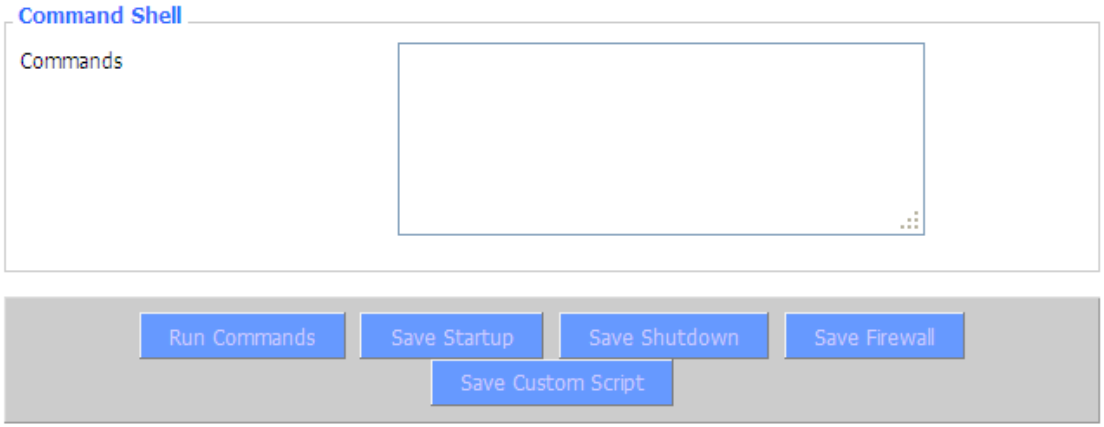
At a specific date time each week or everyday.

Note：

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

3.3.10.3 Commands

Commands： You are able to run command lines directly via the Webinterface.



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

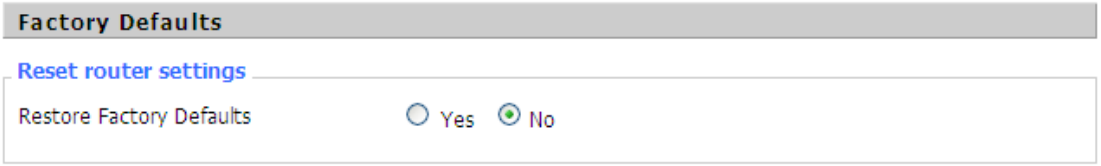
Startup： You can save some command lines to be executed at startup's Router. Fill the text area with commands (only one command by row) and click Save Startup.

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.

3.3.10.4 Factory Defaults

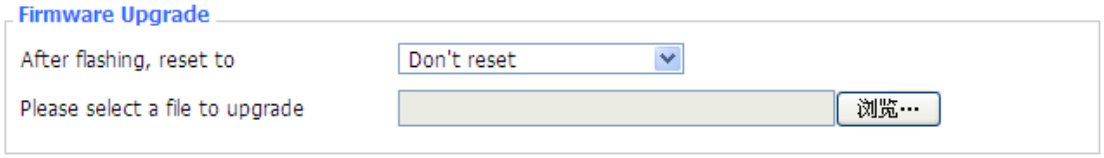


Reset Router settings： Click the Yes button to reset all configuration settings to their default values. Then click the Apply Settings button.

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.

3.3.10.5 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.

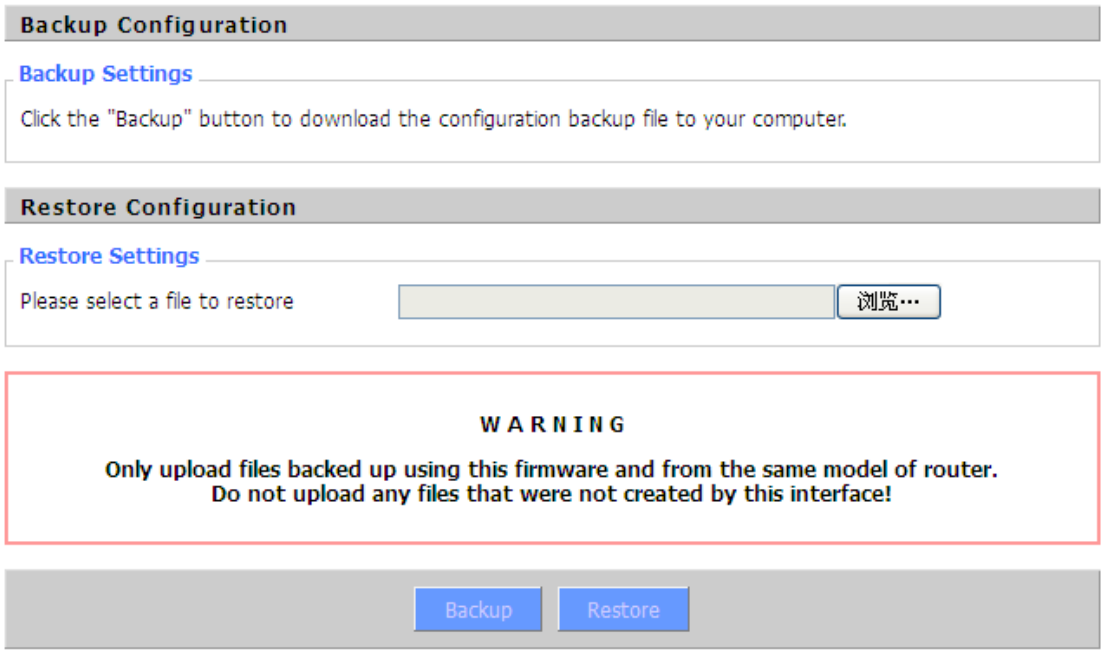
Note：

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.

3.3.10.6 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 backup your

current configuration.

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

Note：

Only restore configurations with files backed up using the same firmware and the same model of Router.

3.3.11 Status

3.3.11.1 Router

Router Name: name of the Router, setting→basic setting to modify

Router Model: model of the Router, unavailable to modify

Firmware Version: software version information

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

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

WAN Domain Name: domain name of WAN, setting→basic setting to modify

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

Current Time: local time of the system

Uptime: operating uptime as long as 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

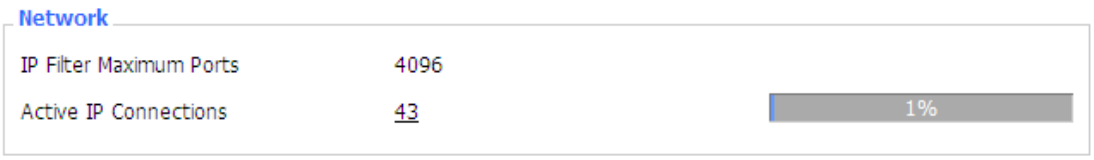
Used: used memory, total available memory minus free memory

Buffers: used memory for buffers,

Cached: the memory used by high-speed cache memory

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

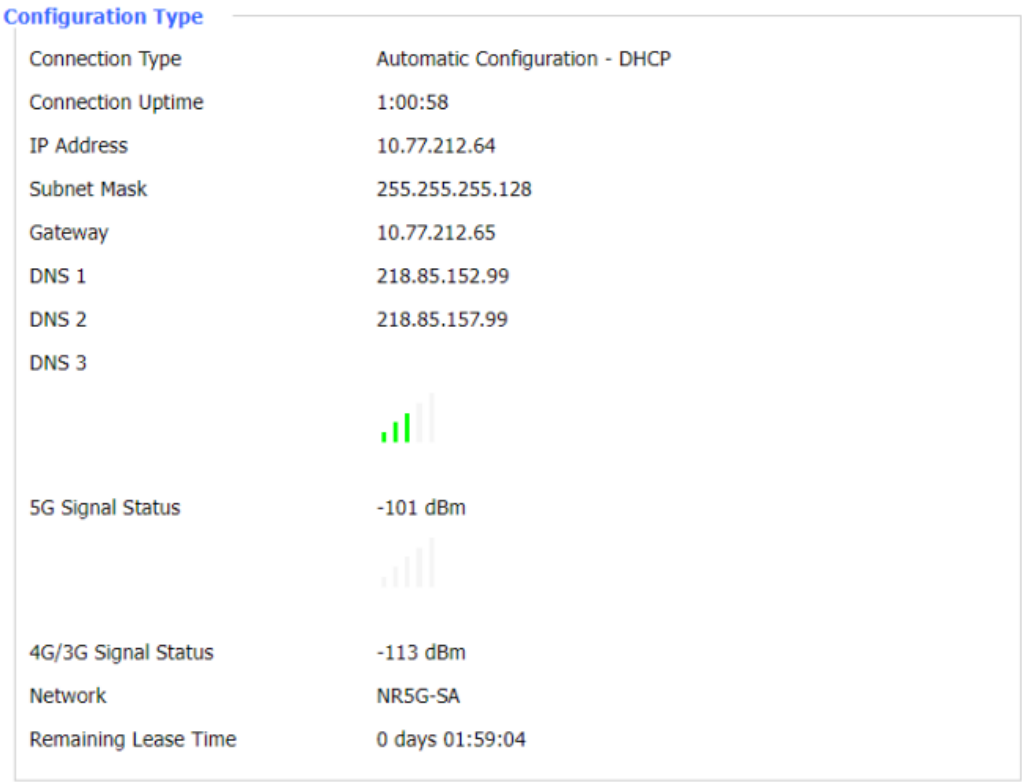
Source Address: source IP address

Remote Address: remote IP address

Service Name: connecting service port

Status: displayed status

3.3.11.2 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

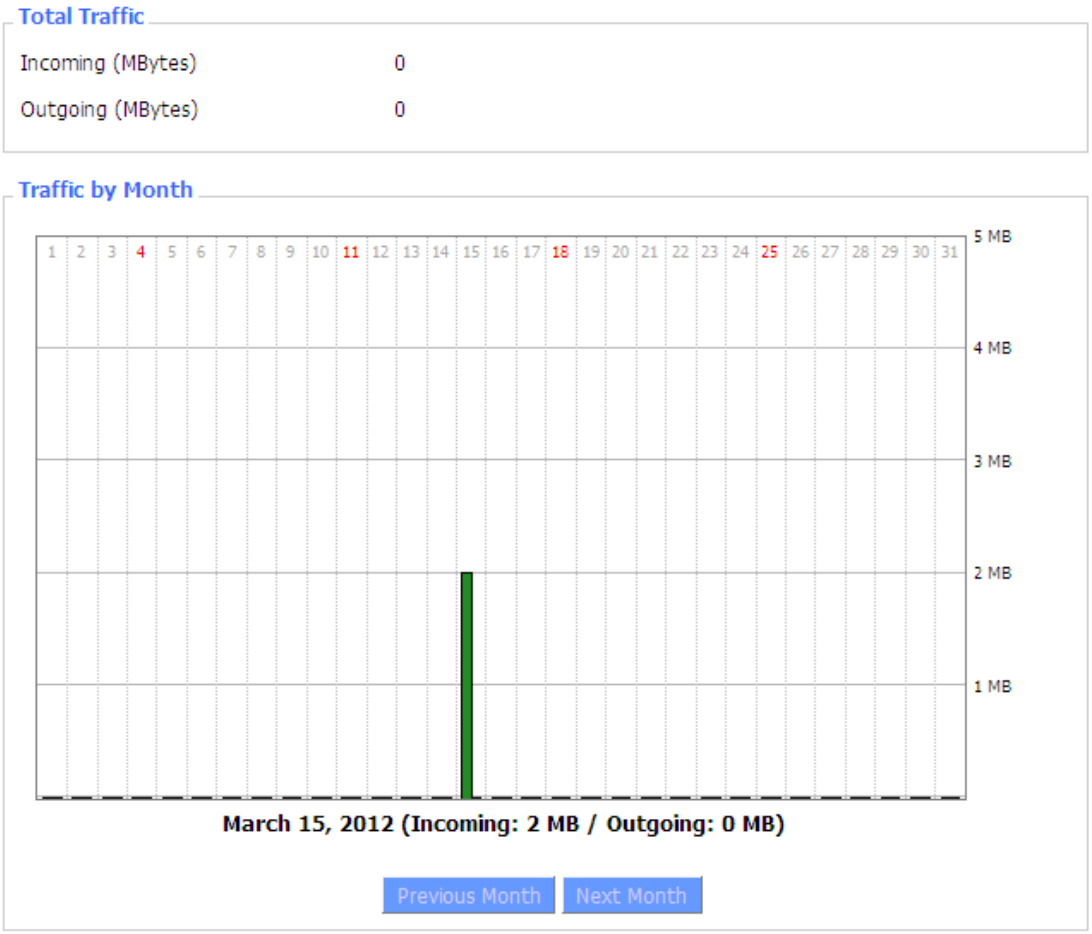
IP Address: IP address of router WAN

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



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

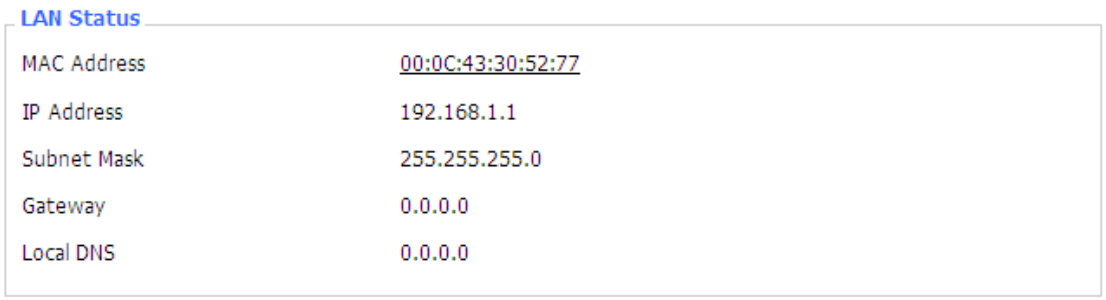
Next Month: the flow of next month

Backup: backup data administration

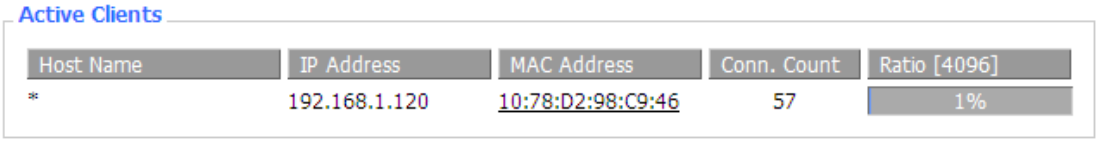
Restore: restore data administration

Delete: delete data administration

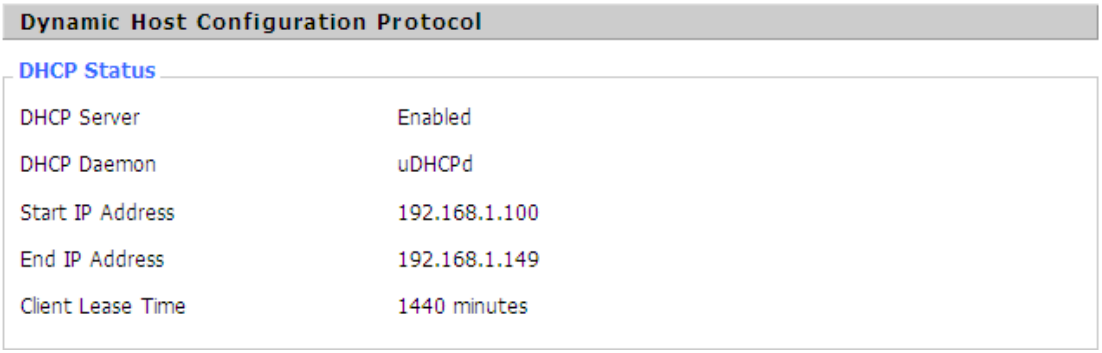
3.3.11.3 LAN



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



DNCP 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
Client Lease Time: the lease time of DHCP client

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time	Delete
PC-201011161332	192.168.1.142	00:21:5C:33:4D:29	1 day 00:00:00	
jack-lincw	192.168.1.117	44:37:E6:3F:45:54	1 day 00:00:00	
*	192.168.1.149	00:0C:E7:00:00:00	1 day 00:00:00	

Host Name: host name of LAN client
IP Address: IP address of the client
MAC Address: MAC address of the client
Expires: the expiry the client rents the IP address
Delete: click to delete DHCP client

Connected PPPOE Clients

Interface	User Name	Local IP	Delete
ppp0	hometest	192.168.10.10	

Interface: the interface assigned by dial-up system
User Name: user name 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
User Name: user name 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

Connected PPTP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.5.1	120.42.46.98	

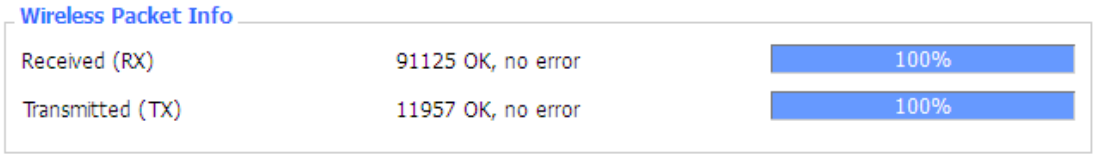
Interface: the interface assigned by dial-up system
User Name: user name of the client
Local IP: tunnel IP address of PPTP client
Remote IP: IP address of PPTP client
Delete: click to delete PPTP client

3.3.11.4 Wireless

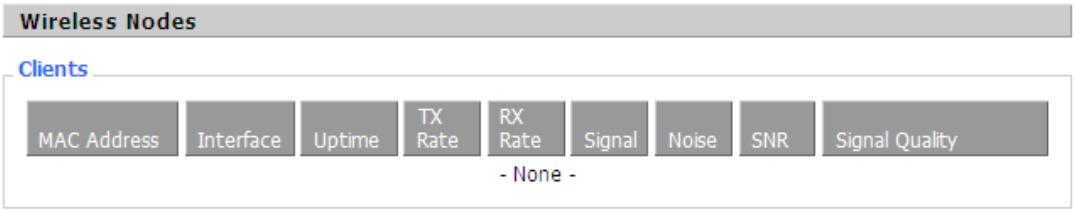
Wireless Status

MAC Address	00:0C:43:30:52:79
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	Yifan
Channel	6 (2437 MHz)
TX Power	71 mW
Rate	72 Mb/s
Encryption - Interface wl0	Disabled
PPTP Status	Disconnected

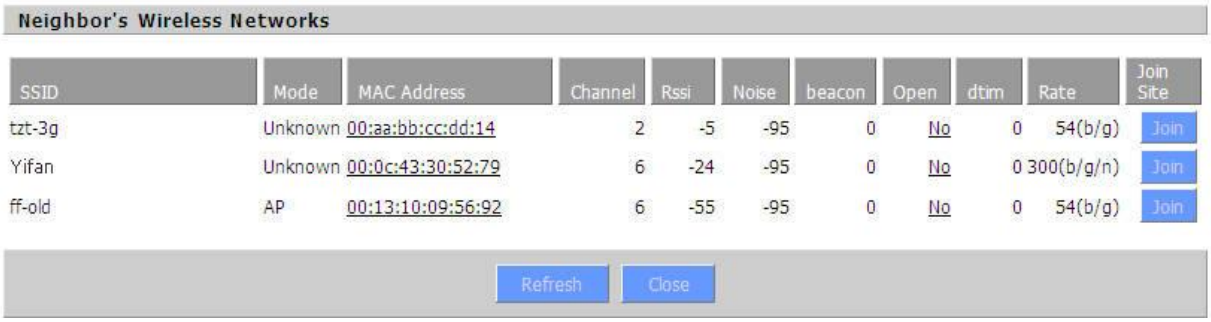
MAC Address: MAC address of wireless client
Radio: display whether radio is on or not
Mode: wireless mode
Network: wireless network mode
SSID: wireless network name
Channel: wireless network channel
TX Power: reflection power of wireless network
Rate: reflection rate of wireless network
Encryption-Interface wl0: enable or diasbal Encryption-Interface wl0
PPTP Status: show wireless pptp status



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



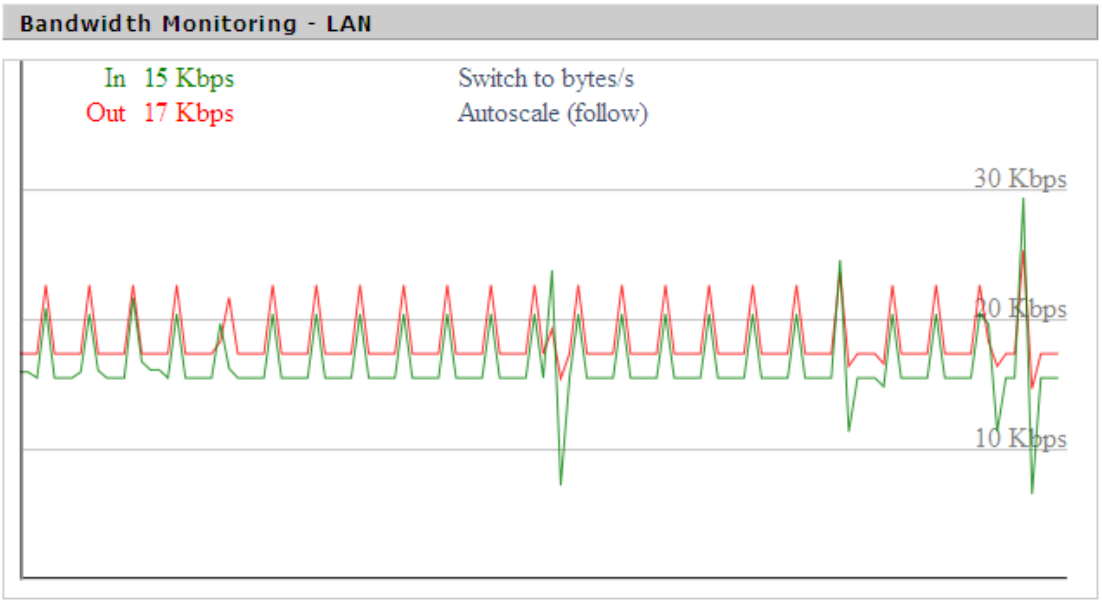
MAC Address: MAC address of wireless client
Interface: interface of wireless client
Uptime: connecting uptime of wireless client
TX Rate: transmit rate of wireless client
RX Rate: receive rate of wireless client
Signal: the signal of wireless client
Noise: the noise of wireless client
SNR: the signal to noise ratio of wireless client
Signal Quality: signal quality of wireless client



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

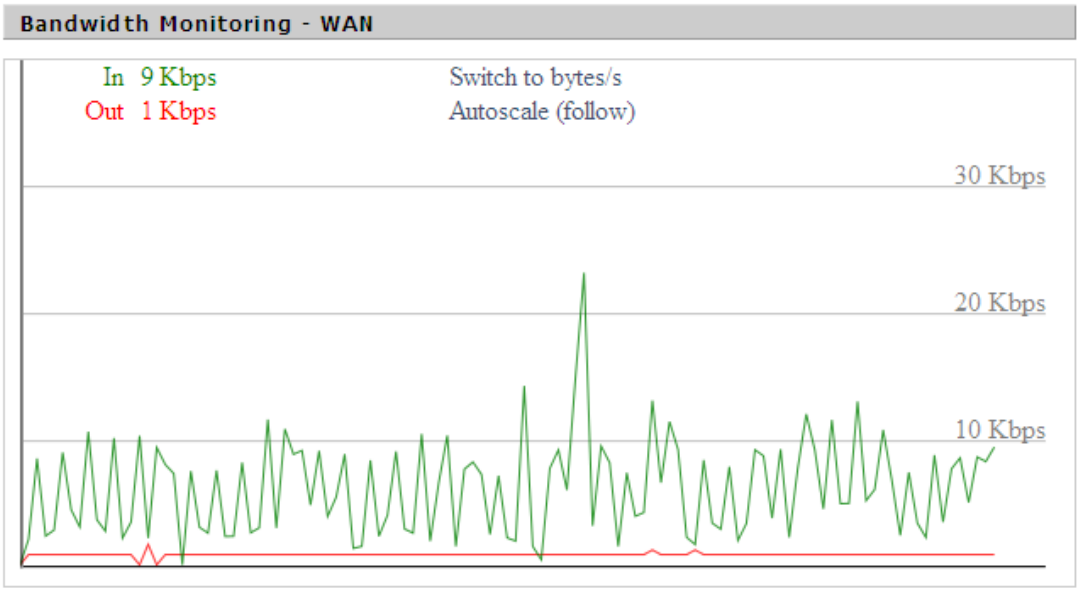
3.3.11.5 Bandwidth



Bandwidth Monitoring-LAN Graph

abscissa axis: time

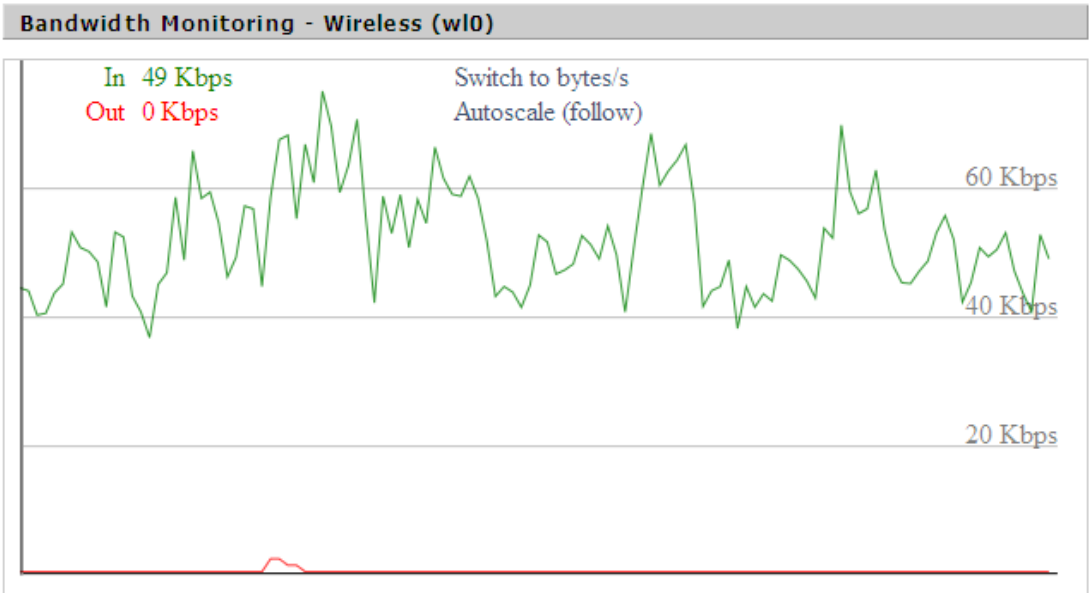
vertical axis: speed rate



Bandwidth Monitoring-WAN Graph

abscissa axis: time

vertical axis: speed rate

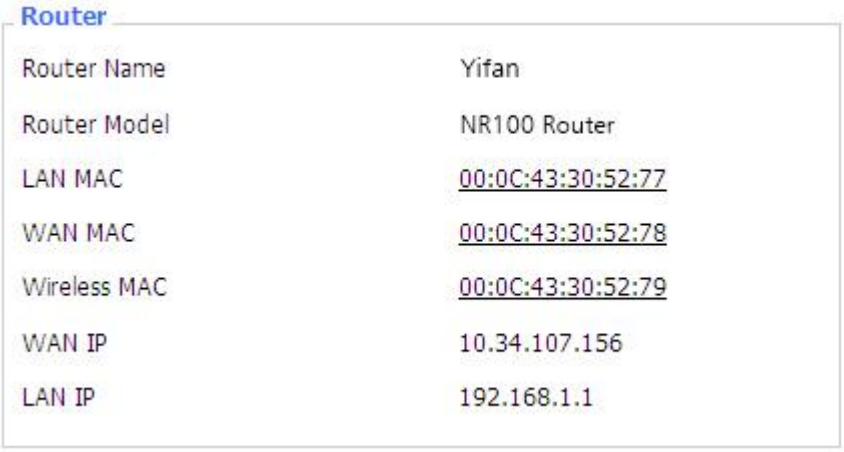


Bandwidth Monitoring-Wireless (W10) Graph

abscissa axis: time

vertical axis: speed rate

3.3.11.6 Sys-Info



Router Name: the name of the Router

Router Model: the model of the Router

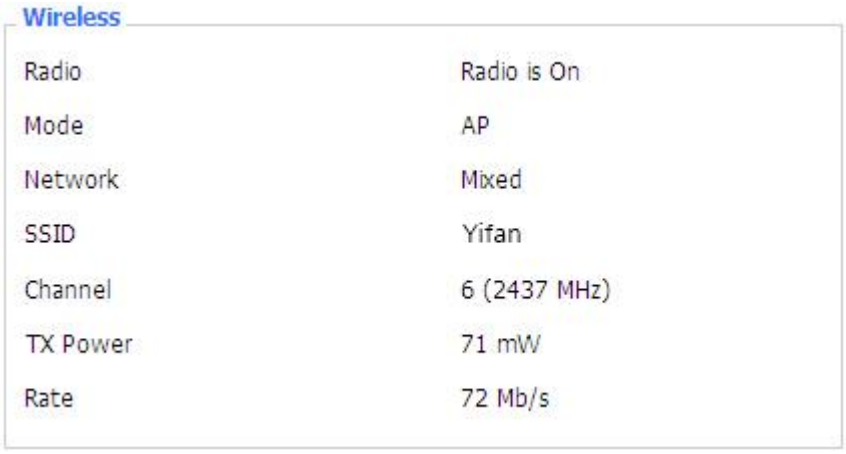
LAN MAC: MAC address of LAN port

WAN MAC: MAC address of WAN port

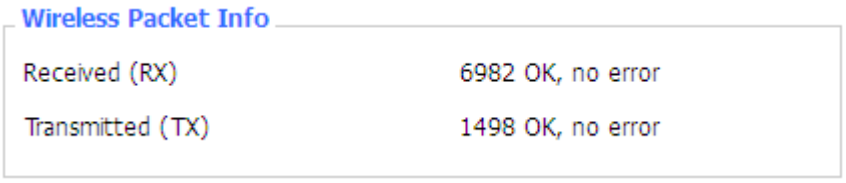
Wireless MAC: MAC address of the wireless

WAN IP: IP address of WAN port

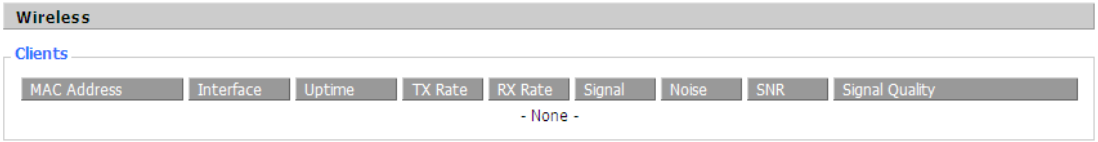
LAN IP: IP address of LAN port



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

Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Disabled

DHCP Server: enabled or disabled
ff-radauth: enabled or disabled
USB Support: enabled or disabled

Memory

Total Available	122.3 MB / 128.0 MB
Free	92.6 MB / 122.3 MB
Used	29.6 MB / 122.3 MB
Buffers	3.3 MB / 29.6 MB
Cached	11.7 MB / 29.6 MB
Active	10.3 MB / 29.6 MB
Inactive	6.4 MB / 29.6 MB

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

DHCP

DHCP Clients

Host Name	IP Address	MAC Address	Expires
*	192.168.1.143	xx:xx:xx:xx:DD:45	1 day 00:00:00
four-488e1df5fa	192.168.1.125	xx:xx:xx:xx:D8:F7	1 day 00:00:00
Mycenae-PC	192.168.1.116	xx:xx:xx:xx:5E:30	1 day 00:00:00

Host Name: host name of LAN client
IP Address: IP address of the client
MAC Address: MAC address of he client
Expires: the expiry the client rents the IP address

Appendix

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

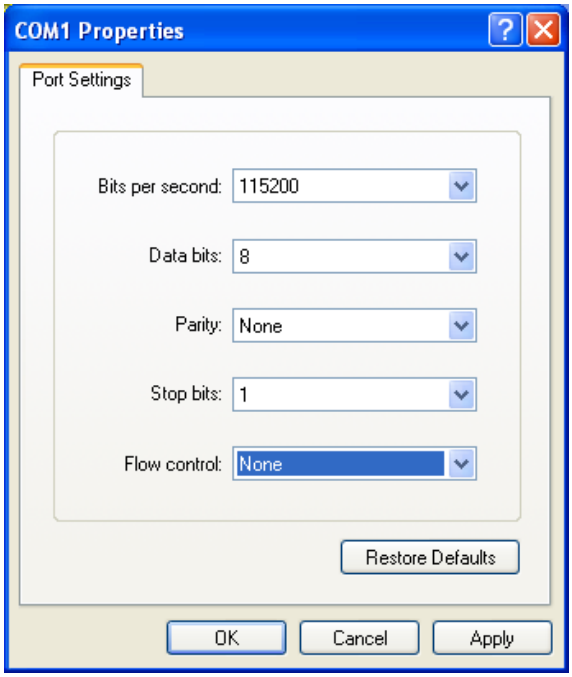
3.3.2.1 Press “Start”→”Programs”→”Accessories”→”Communications”→”Hyper Terminal”

3.3.2.2 Input connection name, choose “OK”

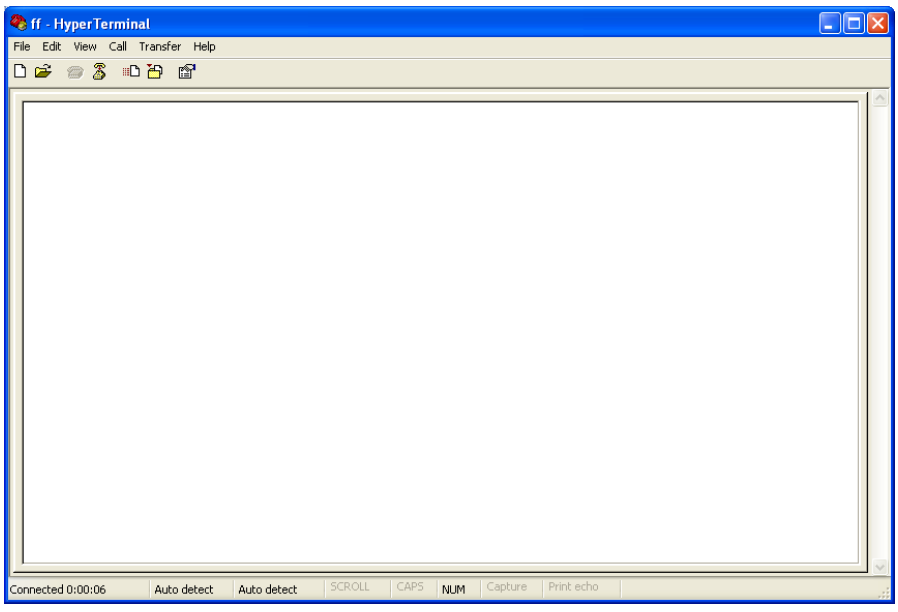
3.3.2.3 Choose the correct COM port which connects to modem, choose “OK”

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

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



3.3.2.5 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.