C365-4G-H900

COMMS365 H900 4G Router

(and C365-5G-H900 Options where applicable)

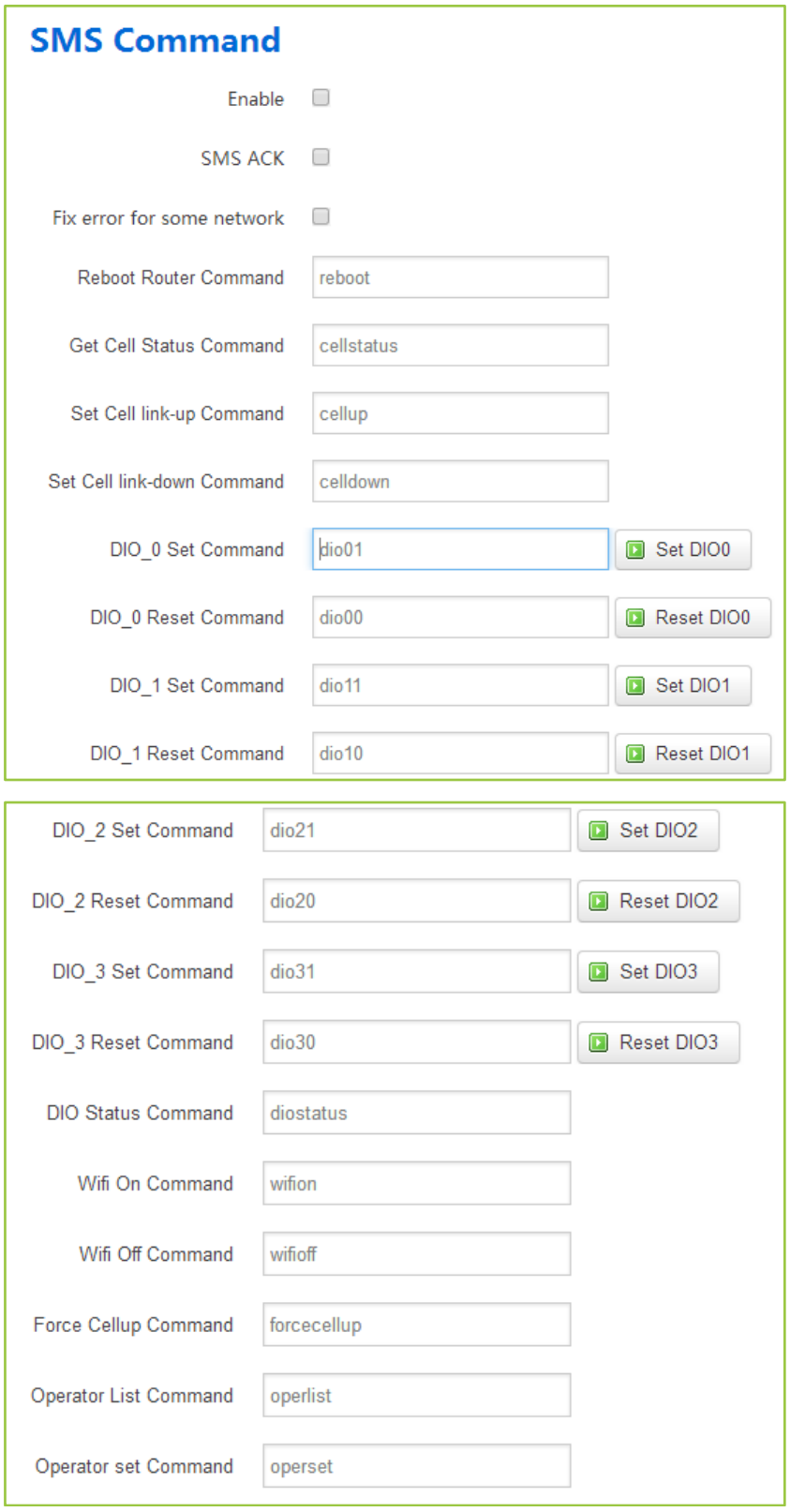
PART 2

USER MANUAL

Contents

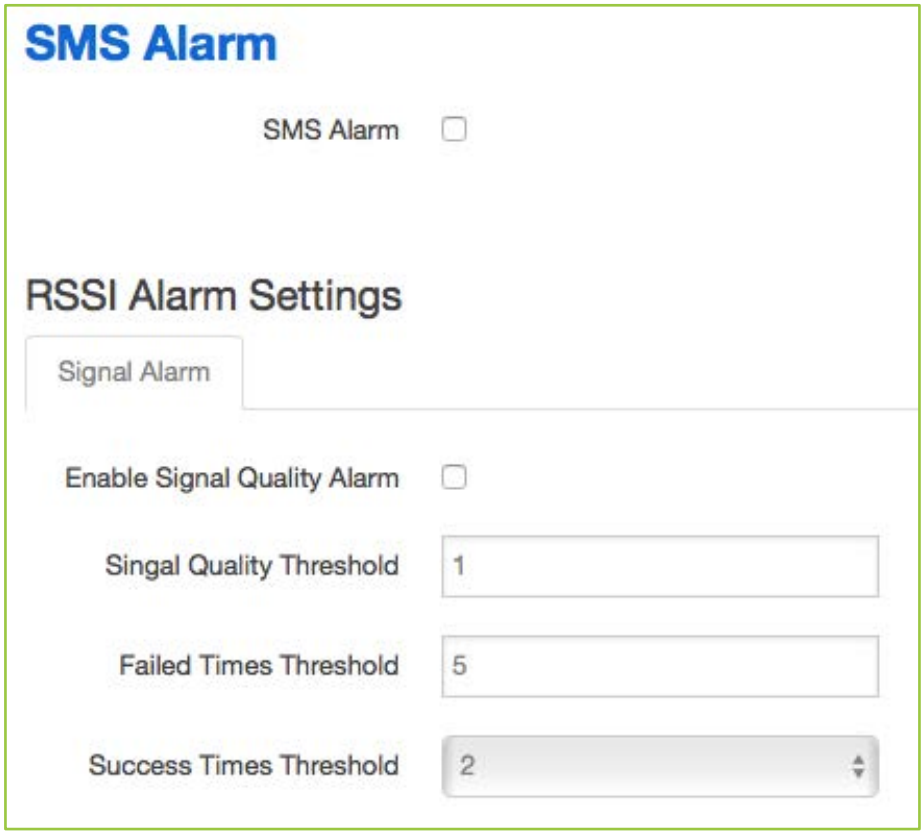
3.5.7 SMS

SMS Command



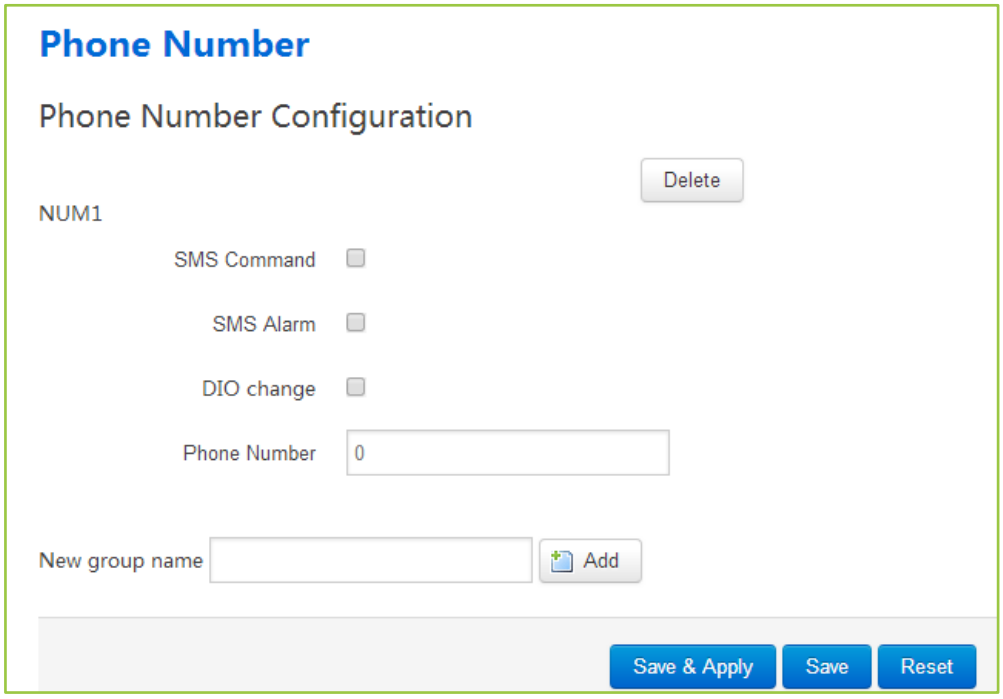
- **Enable:** Check the box to enable the SMS command feature.
- **SMS ACK:** If checked, the router will send the command feedback to the sender's phone number. If unchecked, the router will not send the command feedback to the sender's phone number.
- **Reboot Router Command:** Input the command for **"reboot"** operation, default is **"reboot".**
- **Get Cell Status Command:** Input the command for **"router cell status checking"** operation, default is **"cell status".** For example, if we send **"cell status"** to the router, the router will feedback the status to the sender such as "Router SN: 086412090002 cell_link_up", which identifies the router SN number and Cell Working Status.
- **Set cell link-up Command**: Input the command for the **"router cell link up"** operation, default is **"cell up".** If the router receives this command, the Router Cell will be online.
- **Set cell link-down Command:** Input the command for **"router cell link down"** operation, default is **"cell down".** If router gets this command, the Router Cell will be offline.
- **DIO_0 Set Command:** set I/O port 0 to high (1). For the SMS feature, please keep the parameter as default.
- **DIO_0 Reset Command**: set I/O port 0 to low (0). For the SMS feature, please keep the parameter as default.
- **DIO_1 Set Command:** set I/O port 1 to high (1). For the SMS feature, please keep the parameter as default.
- **DIO_1 Reset Command**: set I/O port 1 to low (0). For the SMS feature, please keep the parameter as default.
- **DIO_2 Set Command:** set I/O port 2 to high (1). For the SMS feature, please keep the parameter as default.
- **DIO_2 Reset Command:** set I/O port 2 to low (0). For the SMS feature, please keep the parameter as default.
- **DIO_3 Set Command:** set I/O port 3 to high (1). For the SMS feature, please keep the parameter as default.
- **DIO_3 Reset Command:** set I/O port 3 to low (0). For the SMS feature, please keep the parameter as default.
- **Button Set/Reset DIO:** Set the DIO to high or low immediately.
- **DIO Status Command:** Input the command for I/O port status. For the SMS feature, please keep the parameter as default.
- **Wi-Fi on Command:** Input the command for turning on the Wi-Fi. For the SMS feature, please keep the parameter as default.
- **Wi-Fi off Command:** Input the command for turning off the Wi-Fi. For the SMS feature, please keep the parameter as default.
- **Force Cellup Command:** If the cell is down due to traffic limitation, then it can be brought up by this command.
- **Operator List Command:** Send the modem operator list as SMS, it is only supported by some specific modems.
- **Operator set Command:** Set the modem to operator manually, it is only supported by some specific modems.

SMS Alarm



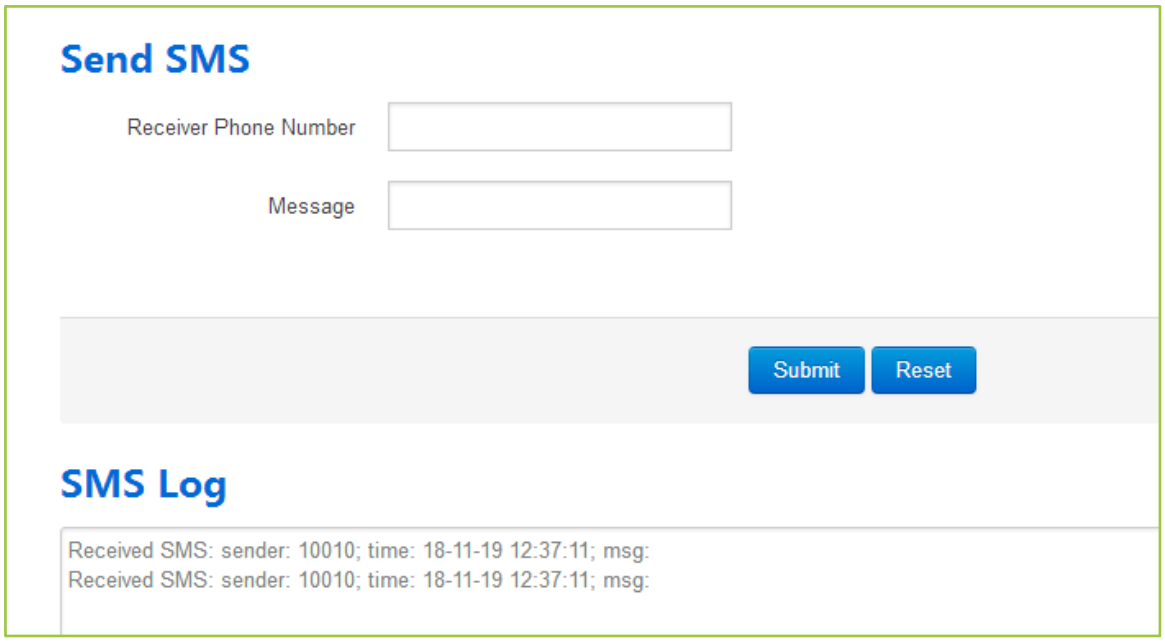
- **SMS Alarm:** Enable SMS alarm feature.
- **Enable Signal Quality Alarm:** Enable the signal quality alarm feature.
- **Signal Quality Threshold:** When the signal alarm is generated and the real time signal strength is lower than the signal quality threshold, then reset the success counter to 0. If the real time signal strength is bigger than this threshold, the success counter will add one.
- When the signal alarm is not generated and the real time signal strength is lower than the signal quality threshold, the failed counter will add one. If the real time signal strength is bigger than this threshold, reset the failed counter to 0.
- **Failed Times Threshold:** If the failed counter is more than this threshold, a signal alarm will be generated.
- **Success Times Threshol**d: If a signal alarm is generated, and the success counter is bigger or equal to the success times threshold, a clear signal will alarm.

Phone Number



- **Add Phone number:** Input a name and click the **"Add"** button to add a new Phone number.
- **Delete Phone number:** Click the **"Delete"** button.
- **SMS command:** Enable the SMS command feature on this phone number.
- **SMS alarm:** This phone number can receive an SMS Alarm.
- **DIO change:** DIO change alarm can be sent to this phone number.

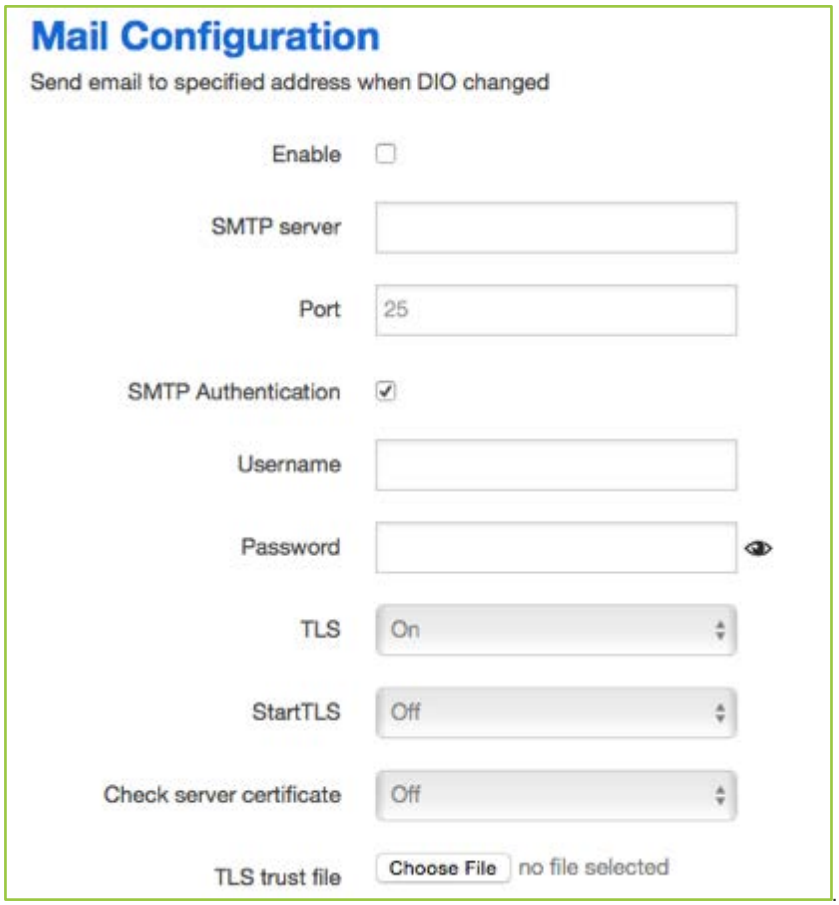
SMS Number



- **Receiver Phone Number:** The Phone number that receives the message.
- **Message:** The content of the message.
- **Submit:** Click the "**Submit**" button to send the message immediately.
- **SMS Log:** The SMS send and receive log.

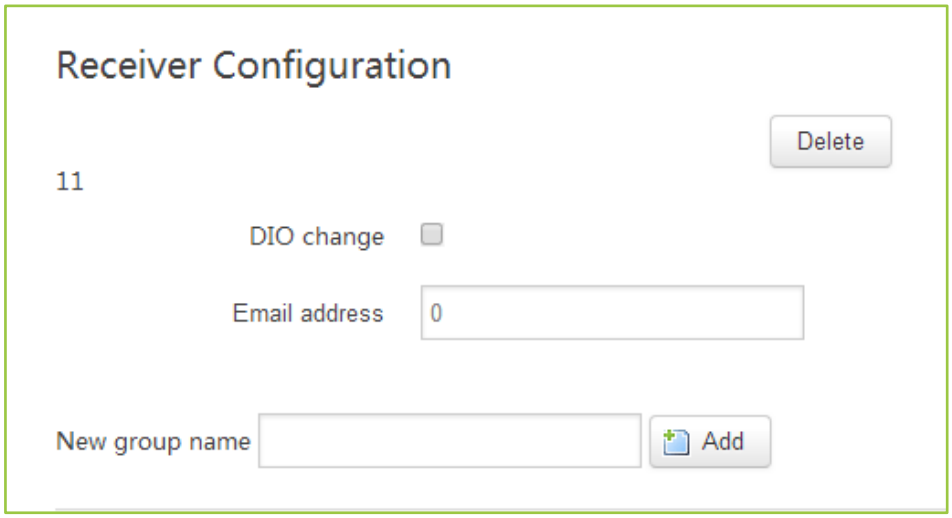
DIO Mail

Send the email to the receiver when the DIO is changed.

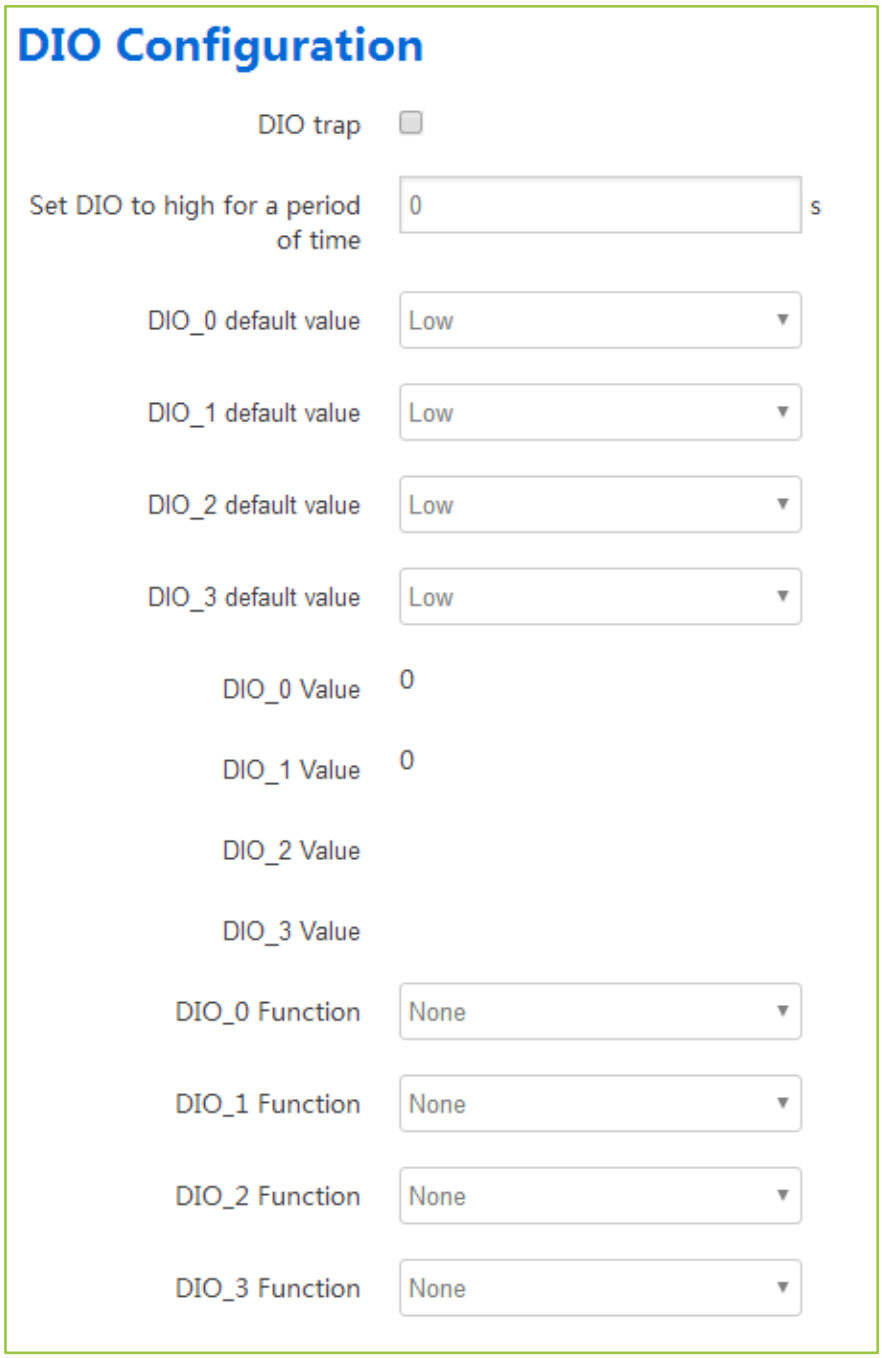


- **Enable:** Activate the DIO Mail functionality.
- **SMTP server:** SMTP server IP address or URL.
- **Port:** SMTP server port.
- **SMTP Authentication:** If SMTP server requires SMTP Authentication, enable it.
- **Username:** Username for the SMTP authentication.
- **Password:** Password for the SMTP authentication.
- **TLS:** Enable or disable TLS (also known as SSL) for secured connections.
- **StartTLS:** Choose the TLS variant: start TLS from within the session ('on', default), or tunnel the session through TLS ('off')..
- **Check server certificate:** Activate server certificate verification using a list of trusted Certification Authorities (CAs).
- **TLS trust file:** Activate server certificate verification using trusted Certification Authorities (CAs).

The default email title is "**[DIOx] changed**", and content is SN:8600000000, [DIOx] is changed from [value0] to value [1]. Configure the email title and content, replace string in [ ].



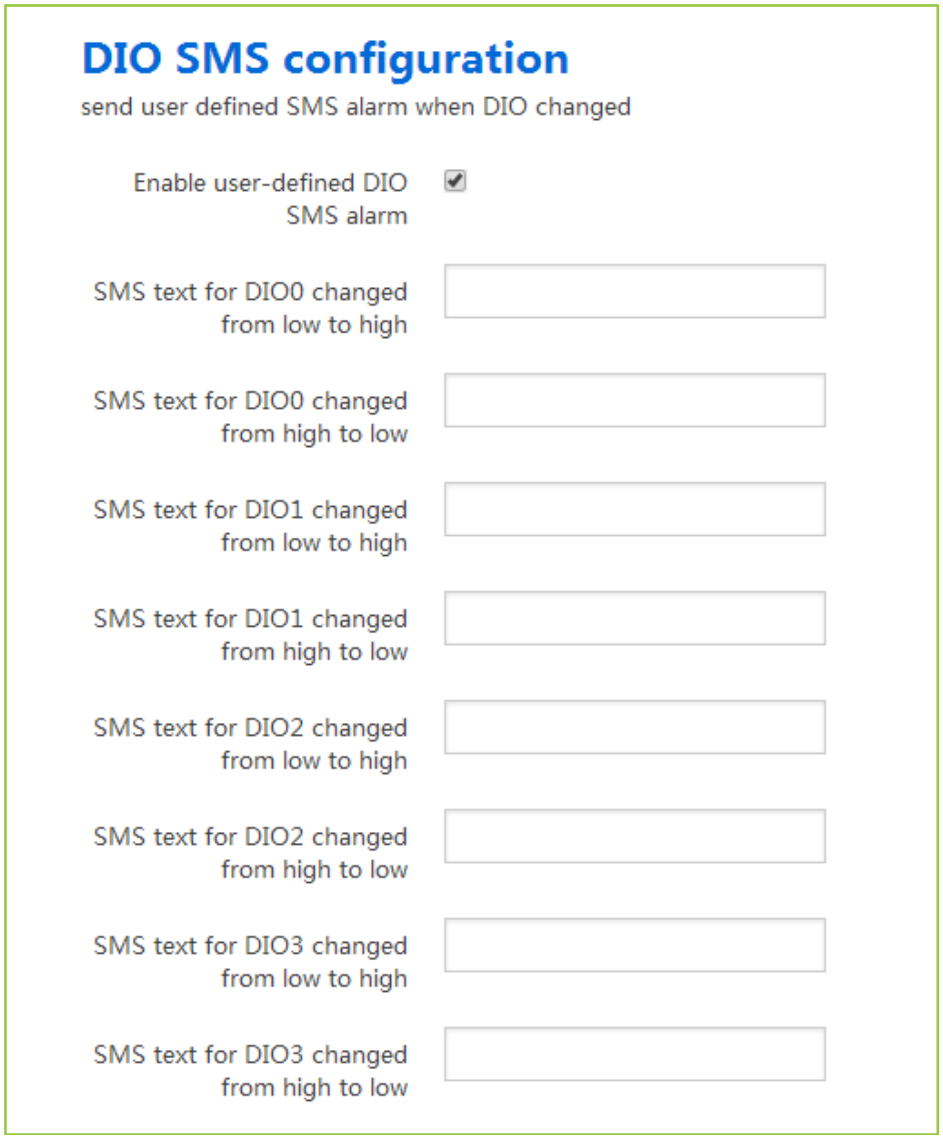
DIO Default



- **DIO trap:** Send SNMP trap when DIO is changed from 1 to 0, or 0 to 1.
- Set DIO to high for a period of time: If setting DIO to high after a period of time, DIO will change to low automatically, value 0 means disable.
- **DIO_0 default value:** DIO default value is low (0). If set to high (1), when device is up, it will be set to high automatically.
- **DIO_1 default value:** DIO default value is low (0). If set to high (1), when device is up, it will be set to high automatically.
- **DIO_2 default value:** DIO default value is low (0). If set to high (1), when device is up, it will be set to high automatically.
- **DIO_3 default value:** DIO default value is low (0). If set to high (1), when device is up, it will be set to high automatically.

- **DIO_0 Value:** DIO current value, 0 means low, and 1 means high.
- **DIO_1 Value:** DIO current value, 0 means low, and 1 means high.
- **DIO_2 Value:** DIO current value, 0 means low, and 1 means high.
- **DIO_3 Value:** DIO current value, 0 means low, and 1 means high.
- **DIO_0 Function:** DIO function can be set to None, GPS and Wi-Fi. DIO value is set to high to turn on functionality, set it to low to turn it off. If the value is None, it will do nothing.
- **DIO_1 Function**: DIO function can be set to None, GPS and Wi-Fi. DIO value is set to high to turn on functionality, set it to low to turn it off. If the value is None, it will do nothing.
- **DIO_2 Function:** DIO function can be set to None, GPS and Wi-Fi. DIO value is set to high to turn on functionality, set it to low to turn it off. If the value is None, it will do nothing.
- **DIO_3 Function**: DIO function can be set to None, GPS and Wi-Fi. DIO value is set to high to turn on functionality, set it to low to turn it off. If the value is None, it will do nothing.

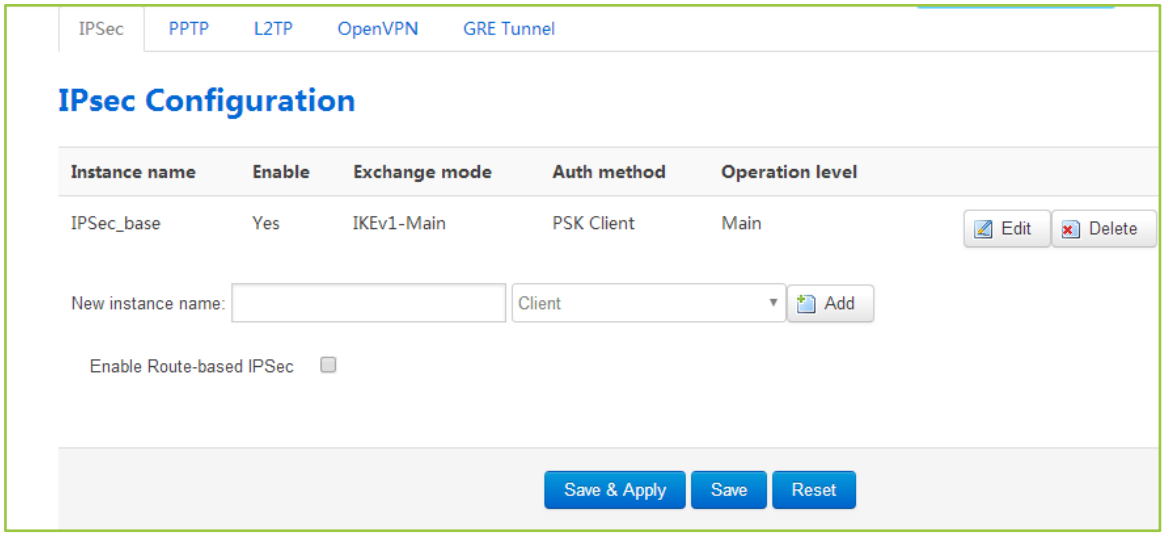
DIO SMS



When the DIO value is changed, it sends an SMS text accordingly. It must enable the DIO change on the phone number. If the user-defined text is empty, it will send a system default SMS to the phone number. The default format is SN:[86000000000], [DIOx] is changed from [value1] to [value0].

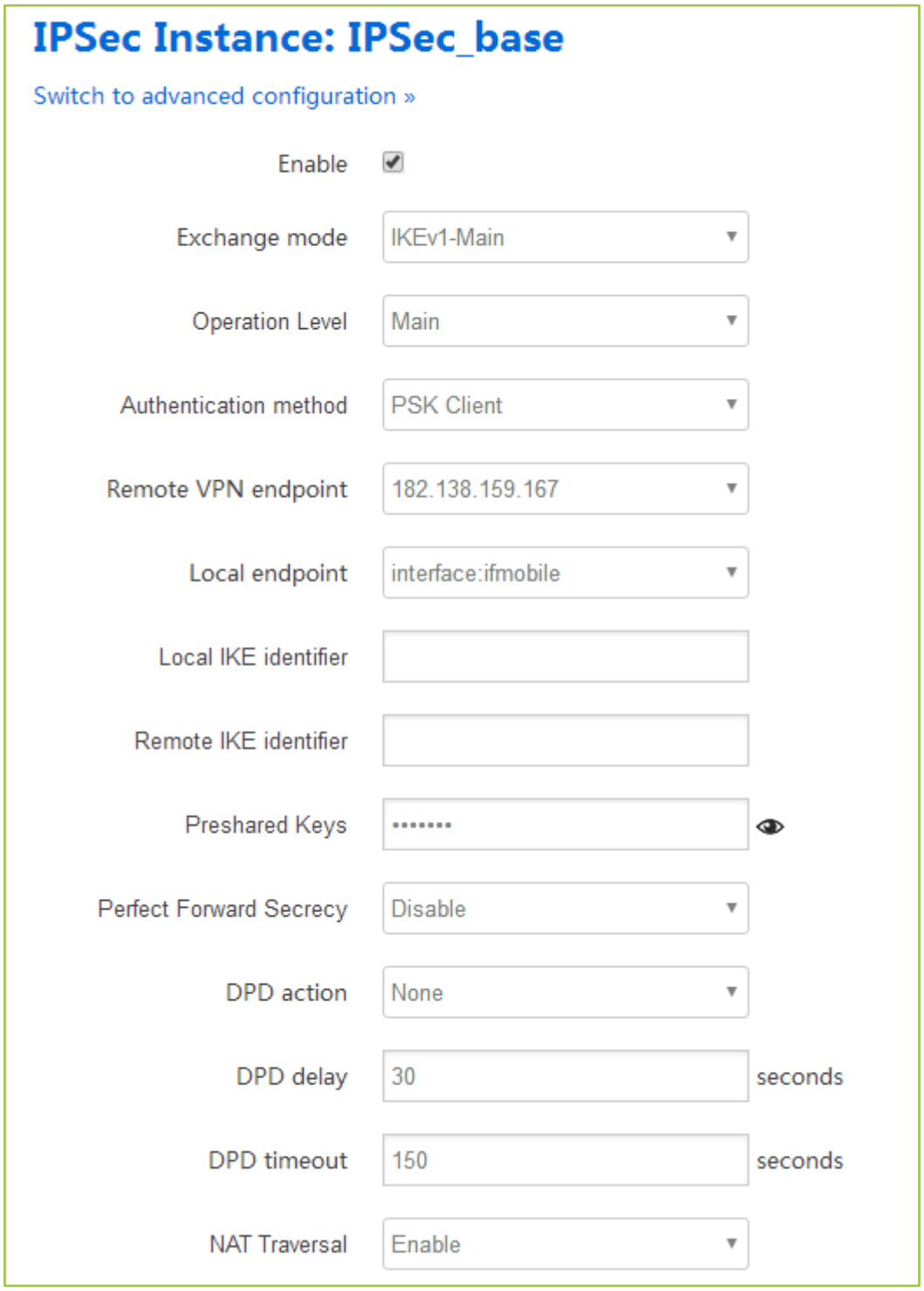
3.5.8 VPN

3.5.8.1 ISPEC

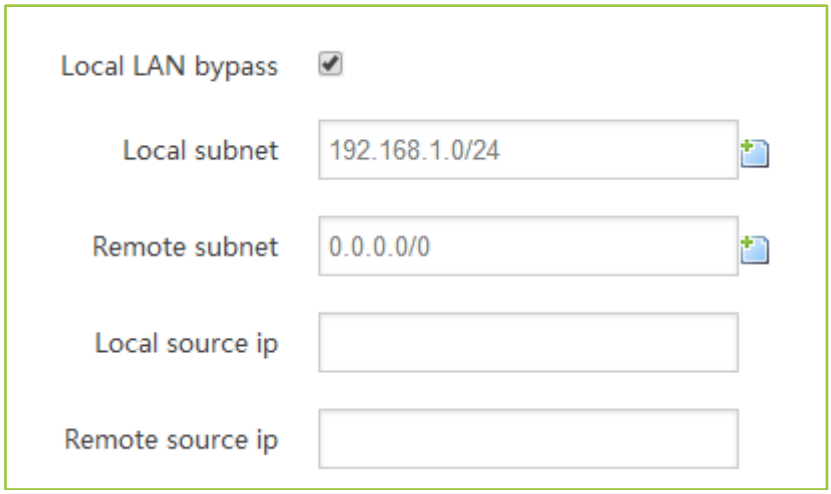


This page is a list of configured IPSec instances and their state. Click the **"Edit"** button to modify it or click the **"Delete"** button to delete an instance.

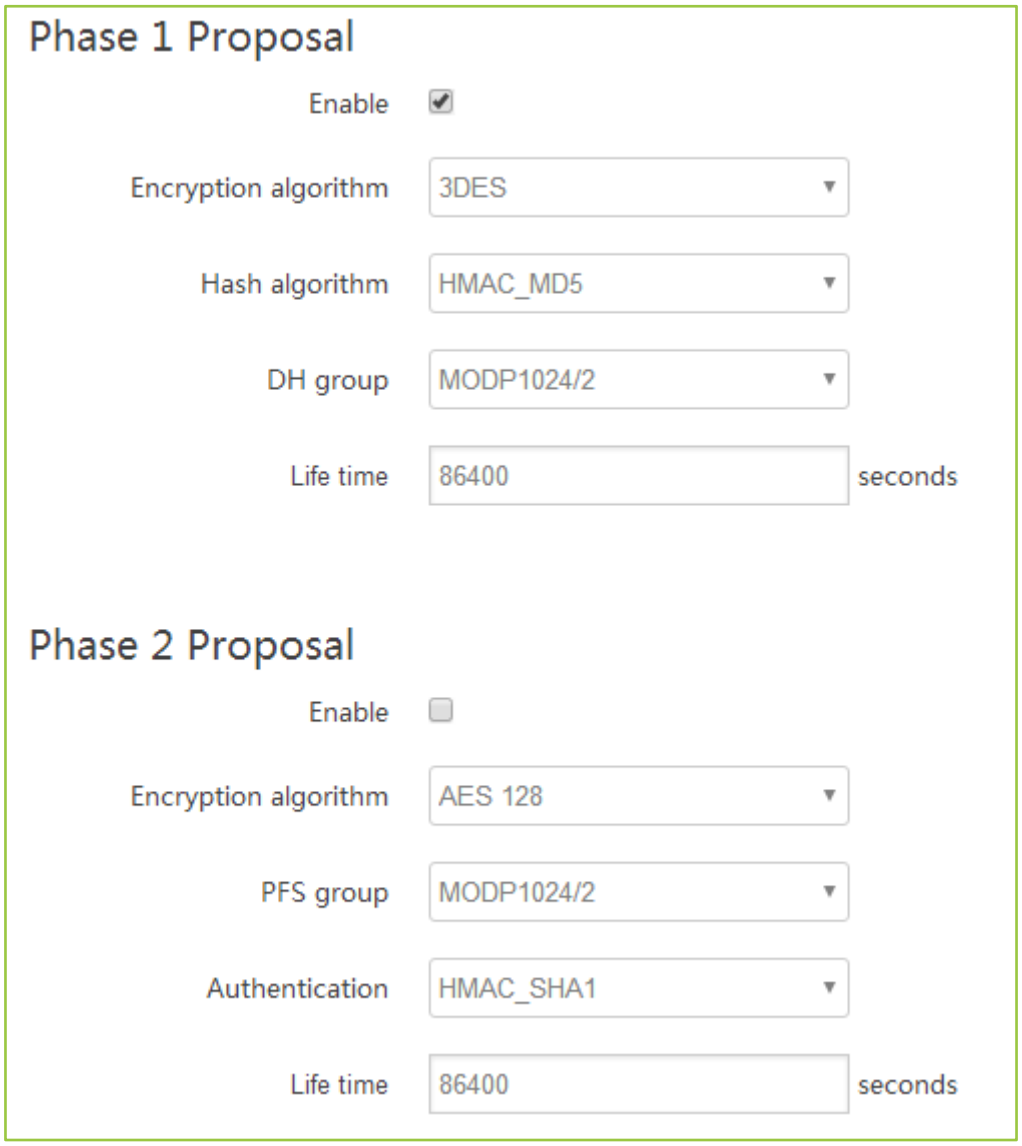
The default setting is Policy-based IPSec, if Enabled the Route-based IPSec box is ticked, after click **"Save & Apply"**, it will then switch to Route-based IPSec.


IPSec Instance: IPSec_base
Switch to advanced configuration »
Enable
Exchange mode
IKEv1-Main
Operation Level
Main
Authentication method
PSK Client
Remote VPN endpoint
182.138.159.167
Local endpoint
interface:ifmobile
Local IKE identifier
Remote IKE identifier
Preshared Keys
Perfect Forward Secrecy
Disable
DPD action
None
DPD delay
30
seconds
DPD timeout
150
seconds
NAT Traversal
Enable

- **Enable:** Enable the IPSEC feature.
- **Exchange mode:** IKEv1-Main, IKEv1-Aggressive, and IKEv2-Main modes are supported.
- **Operation Level:** For IPSec backup. One level is Main and the other is Backup. If the Main instance is down then switch to the backup instance.
- **Authentication method:** PSK Client, PSK Server, RSA X.509 Client and RSA X.509 Server. Client is the device which starts the IPSEC connection.
- **Remote VPN endpoint:** Domain name or IP address of the remote endpoint. It can be visited from the Internet.
- **Local endpoint:** Domain name or IP address or interface name of this device.
- **Local IKE identifier:** Identity the use of the local device authentication.
- **Remote IKE identifier:** Identity the use of the remote device authentication.
- **Preshared Keys:** Pre-shared key authentication, known as PSK.
- **Perfect Forward Secrecy:** Confirm whether Perfect Forward Secrecy of keys is desired on the connection's keying channel.
- **DPD action:** Controls the use of the Dead Peer Detection protocol (DPD, RFC 3706) where R_U_THERE notification messages (IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically sent in order to check the activeness of the IPsec peer. The values are clear, hold, and restart, all of which activate the DPD and determine the action to perform on a timeout. Clear: The connection is closed with no further actions taken. Hold: Installs a trap policy, which will catch matching traffic and tries to re-negotiate the connection on demand. Restart: Immediately triggers an attempt to re-negotiate the connection. The default is none which disables the active sending of DPD messages
- **DPD delay:** Defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer.
- **DPD timeout:** Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.
- **NAT Traversal:** Indicates whether the device is behind a NAT device or not.

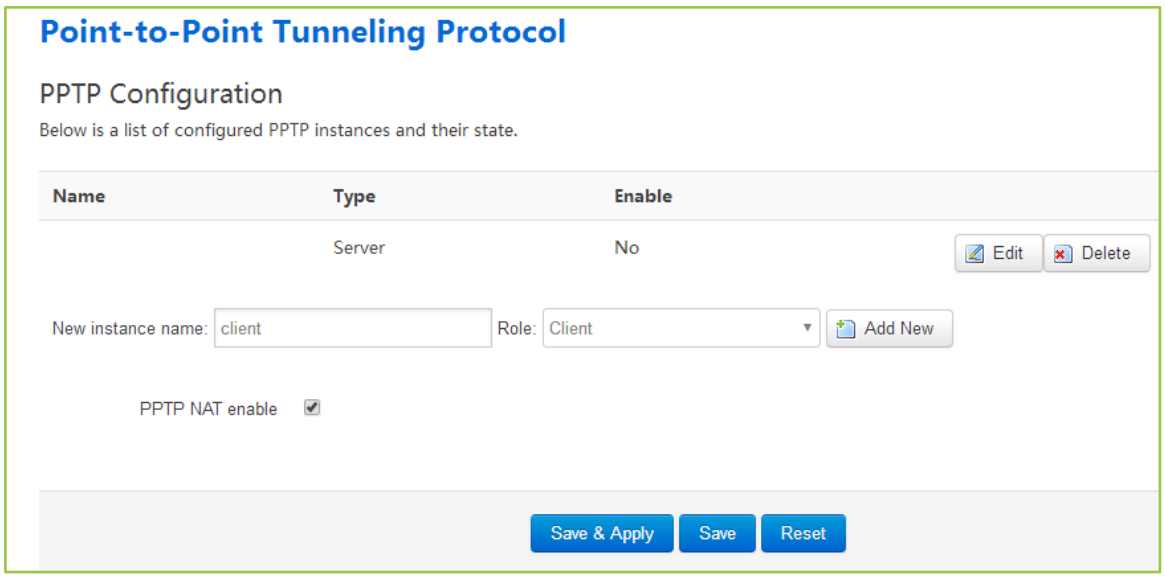


- **Local subnet:** The local subnet which connects to the IPSEC VPN.
- **Remote subnet:** The remote subnet which connects to the IPSEC VPN.
- **Local source ip:** The internal source IP of the local device to use in a tunnel, also known as virtual IP.
- **Remote source ip:** The internal source IP of the remote device to use in a tunnel, also known as virtual IP.



Note: All the configurations in the Phase 1 Proposal and Phase 2 Proposal must match the remote endpoint to establish an IPSEC connection.

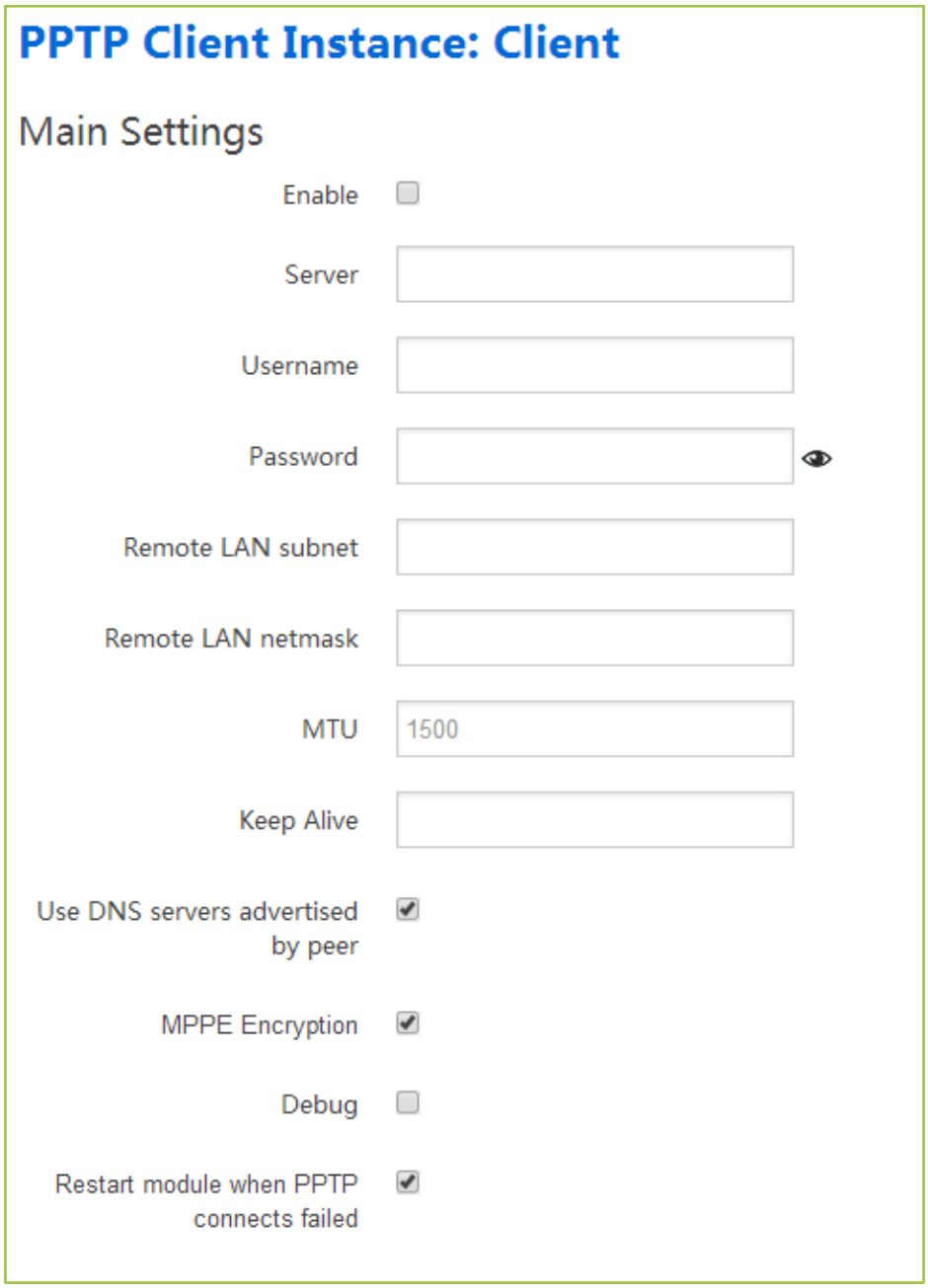
3.5.8.2 PPTP



This page is a list of configured PPTP instances and their state. Click the **"Edit"** button to modify it or click the **"Delete"** button to delete an instance.

PPTP NAT enable: Enable PPTP interface NAT.

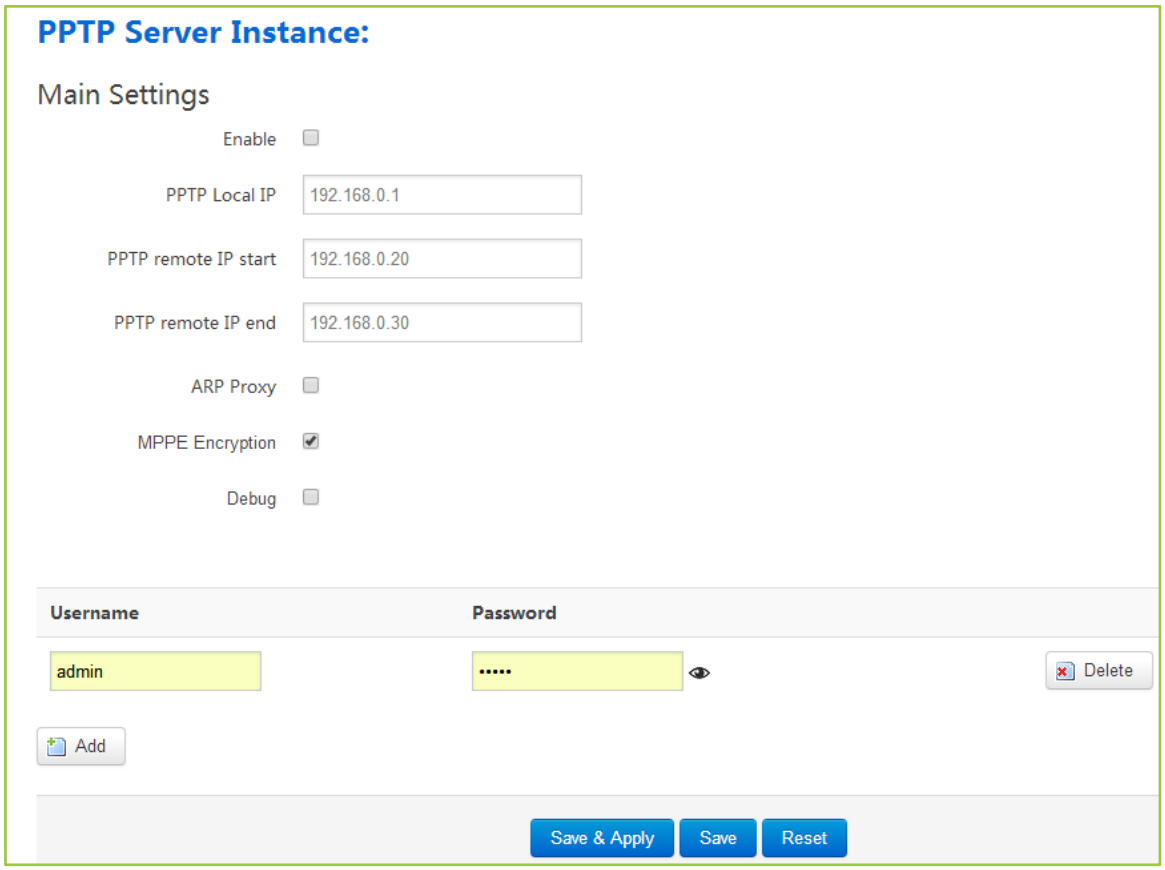
PPTP Client configuration



- **Enable:** Enable this instance.
- **Server:** The domain name or IP address of the PPTP server.
- **Username:** Server authentication username.
- **Password:** Server authentication password.
- **Remote LAN subnet:** The remote subnet which can be accessed via the PPTP tunnel, such as 192.168.10.0
- **Remote LAN netmask:** The netmask for the remote LAN subnet, such as 255.255.255.0
- **MTU:** Maximum transmission unit.
- **Keep Alive:** Number of unanswered echo requests before considering the peer is dead. The interval between the echo requests is 5 seconds.
- **Use DNS servers advertised by peer:** If unchecked, the advertised DNS server addresses are ignored.

- **MPPE Encryption:** Microsoft Point-to-Point Encryption.
- **Debug:** Add verbose PPTP log in the system log.
- **Restart module when PPTP connects failed:** Some network PPTP cannot connect until module is restarted.

PPTP Server Configuration

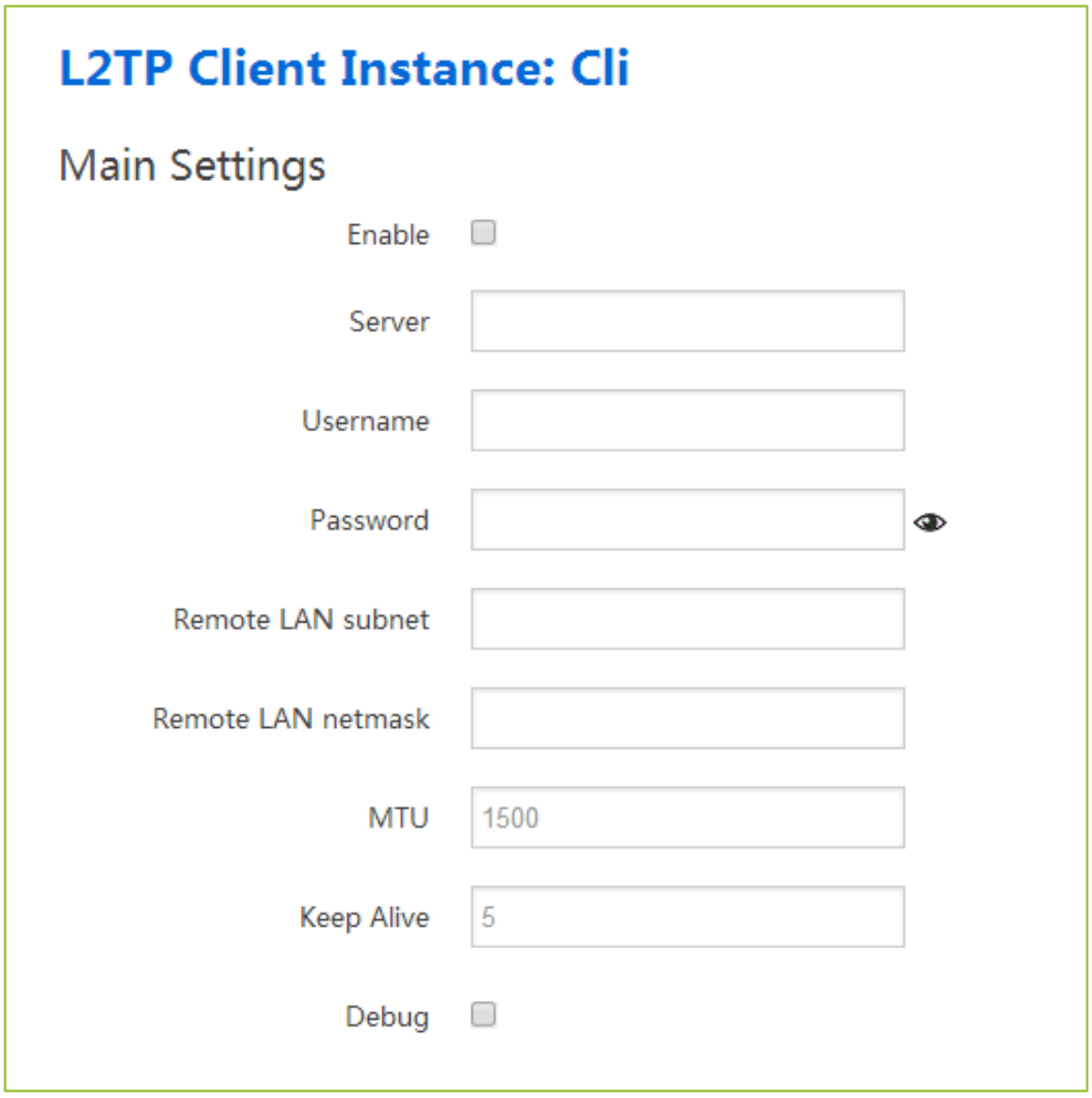


- **PPTP Local IP:** Indicate server's IP address.
- **PPTP remote IP start:** The remote IP address leases start.
- **PPTP remote IP end:** The remote IP address lease end.
- **ARP Proxy:** If the remote IP has the same subnet as the LAN, check it for connecting one another.
- **MPPE Ecryption:** Microsoft Point-to-Point Encryption.
- **Debug:** Add verbose PPTP log in the system log.
- **Username:** Server authentication username.
- **Password:** Server authentication password.

3.5.8.3 L2TP

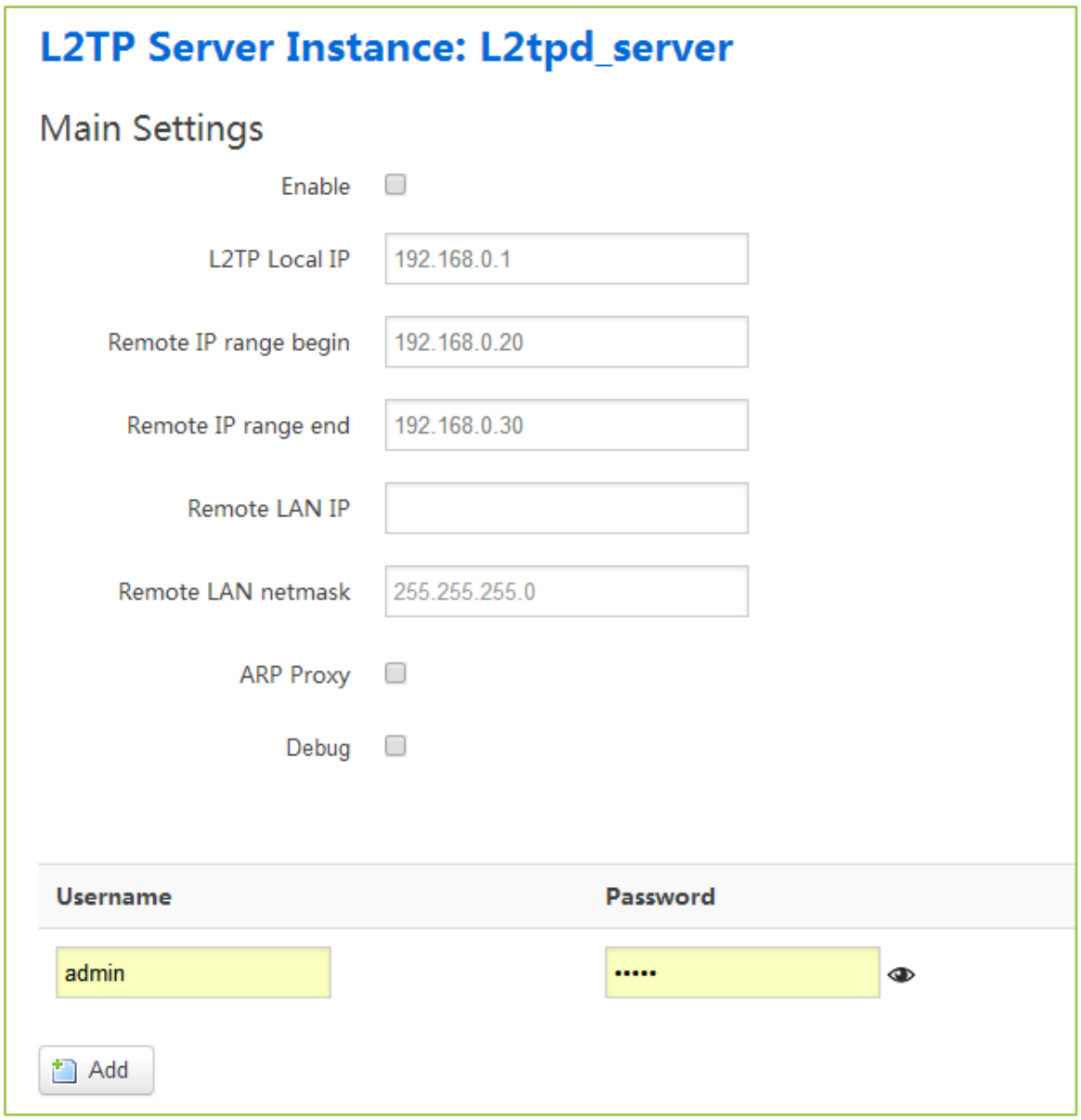
This page is a list of configured L2TP instances and their state. The user can click the **"Edit"** button to modify it or click the **"Delete"** button to delete an instance.

L2TP Client configuration



- **Enable:** Enable this L2TP instance.
- **Server:** Domain name or IP address of L2TP server.
- **Username:** Server authentication username.
- **Password:** Server authentication password.
- **Remote LAN subnet:** The remote LAN subnet can be accessed via the L2TP tunnel, such as 192.168.10.0.
- **Remote LAN netmask:** The netmask for remote LAN subnet, such as 255.255.255.0
- **MTU:** Maximum transmission unit.
- **Keep Alive:** Number of unanswered echo requests before considering the peer is dead. The interval between the echo requests is 5 seconds.
- **Checkup Interval:** Number of seconds passed before checking if the interface is not up since the last setup attempt and retrying the connection. Set it to a value sufficient for a successful L2TP connection for you. It's because the netifd sent the connect request yet the xl2tpd failed to complete it without the notice of netifd.
- **Debug:** Add L2TP verbose log into the system log.

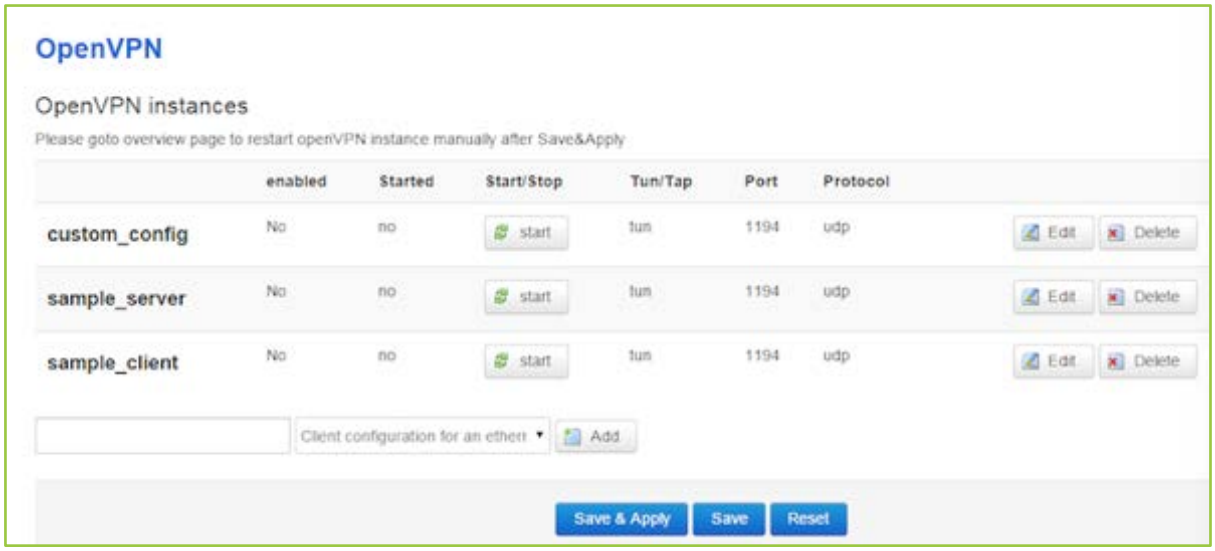
L2TP Server configuration



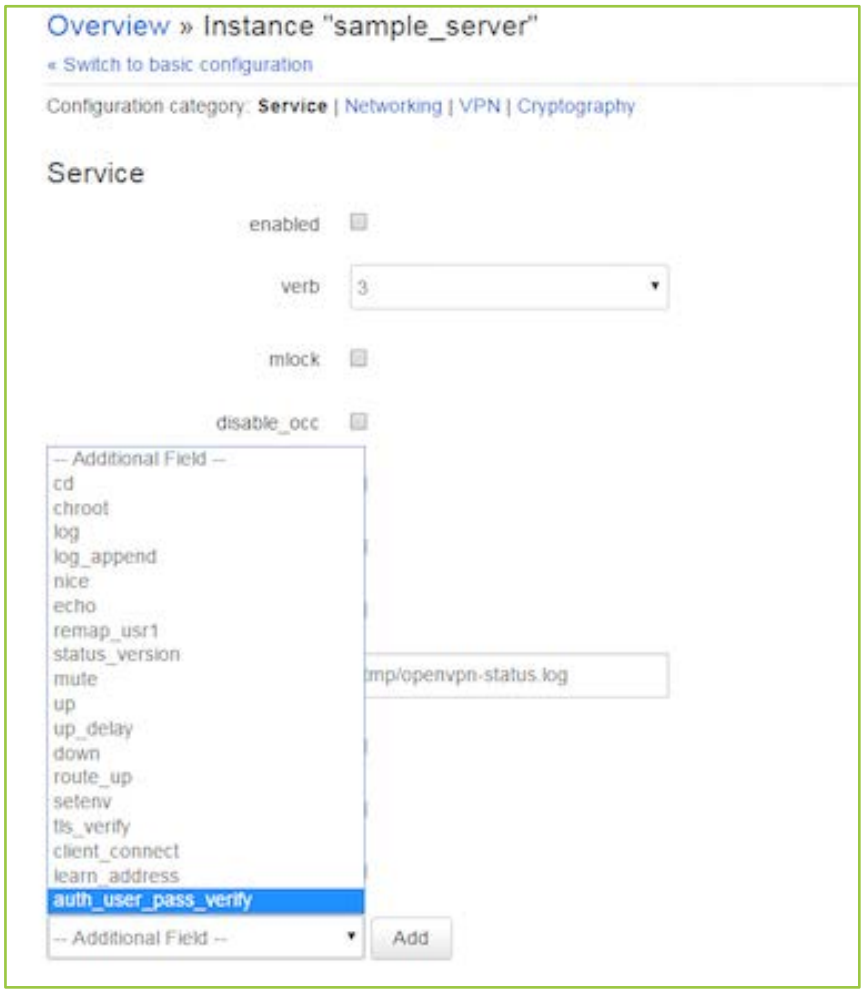
- **Local IP:** Indicate the server's IP address.
- **Remote IP range begin:** The remote IP address leases start.
- **Remote IP range end:** The remote IP address lease end.
- **Remote LAN IP:** The remote LAN subnet can be accessed via the L2TP tunnel, such as 192.168.10.0.
- **Remote LAN netmask:** The mask of the L2TP client IP, the default value is 255.255.255.0.
- **ARP Proxy:** It allows the remote L2TP client to access the local LAN subnet. The remote IP range should be included in the LAN subnet, for example if the local LAN subnet is 192.168.1.0/24, then configure the remote IP range starting with 192.168.1.20 and the remote IP range ending in 192.168.1.30, and enable the ARP Proxy.
- **Debug:** Add the L2TP verbose log into system log.
- **Username:** Server authentication username
- **Password:** Server authentication password.

3.5.8.3 Open VPN

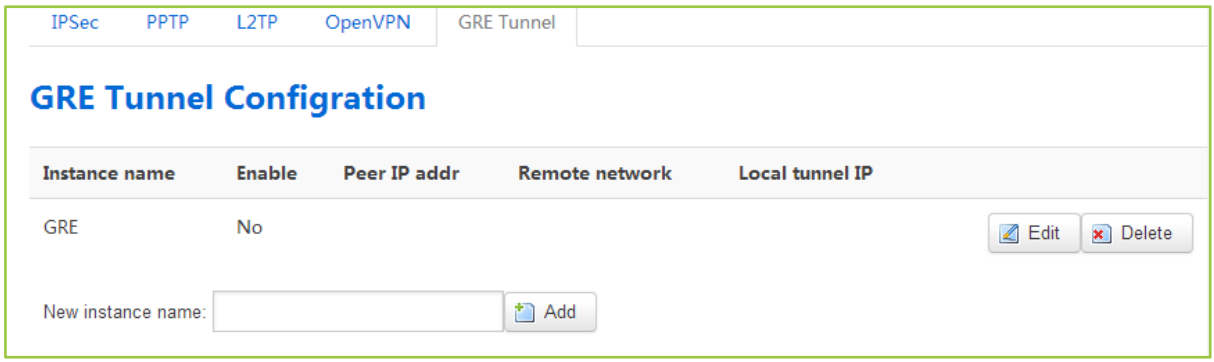
This page is a list of the configured OpenVPN instances and their states. You can click the "**Edit**" button to modify it or click the "**Delete**" button to delete an instance.
You can click the "**Start**" button to start or "**Stop**" button stop a specific instance.

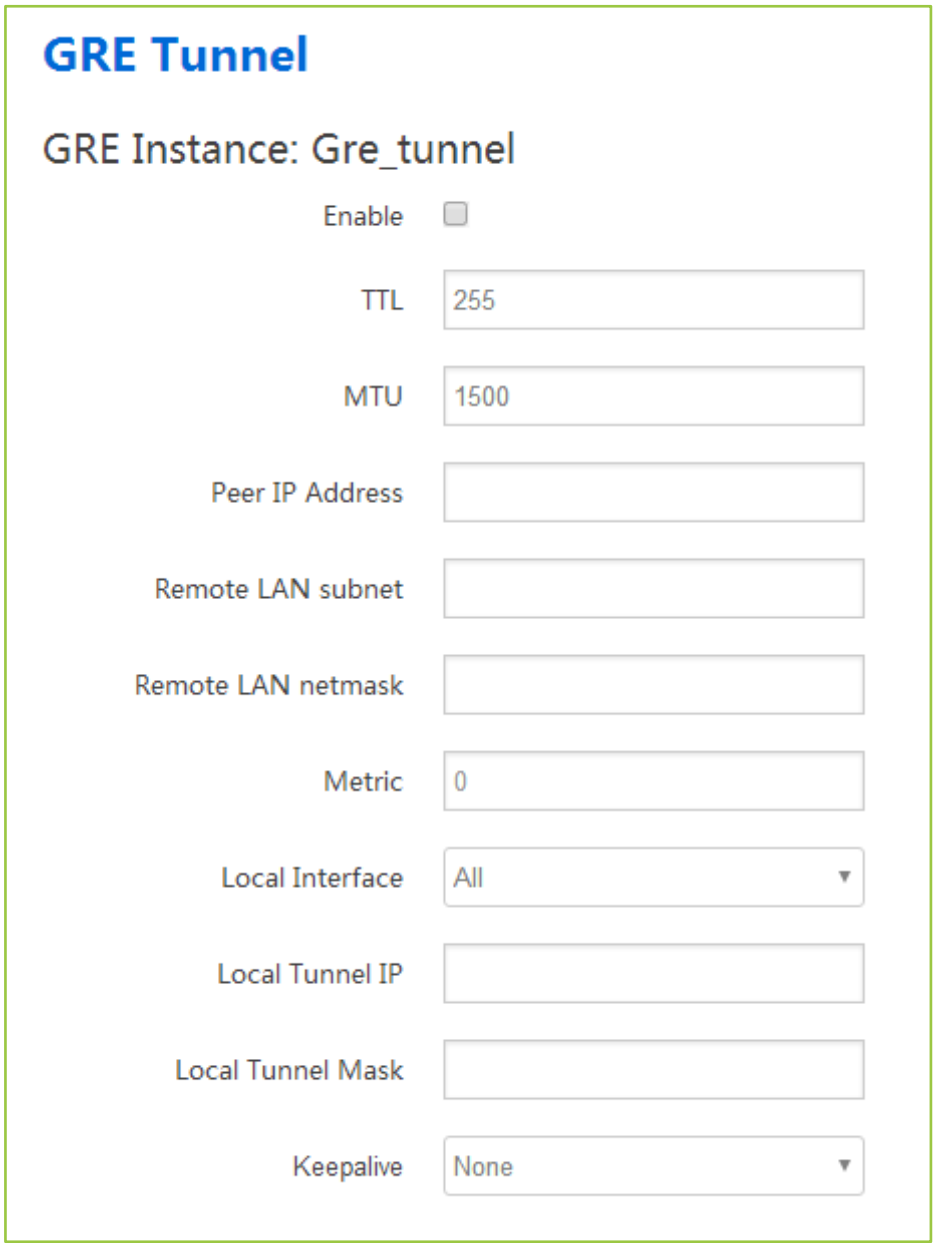


Note: For the OpenVPN configuration page, you can put the mouse on the title of the item to get more help information.
If the item you needed is not shown on the main page, please check the "**Additional Field**" dropdown list at the bottom of the page.



3.5.8.5 GRE Tunnel

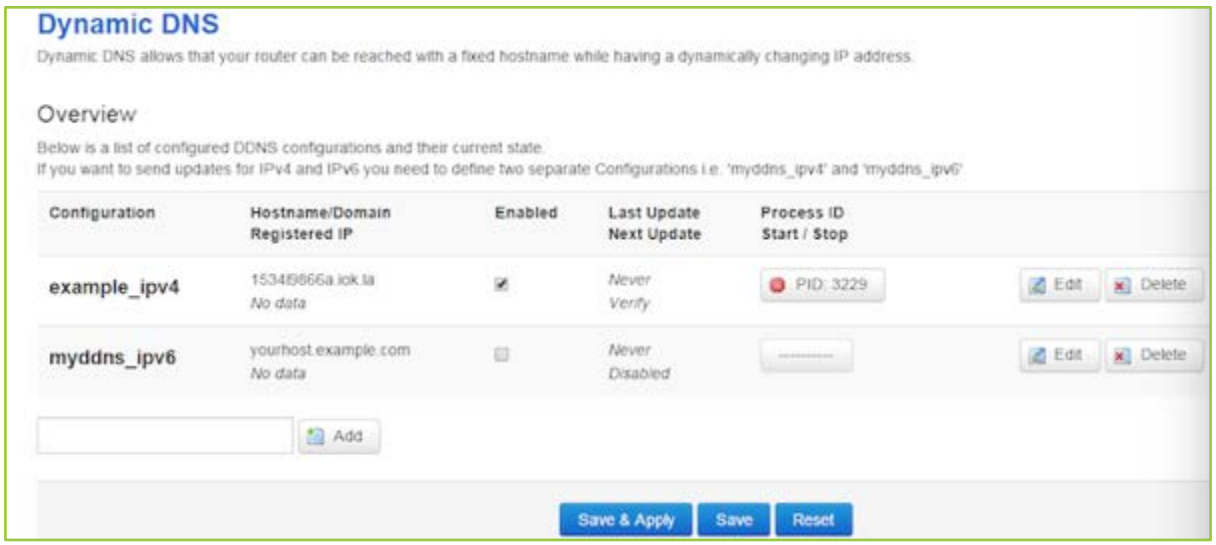


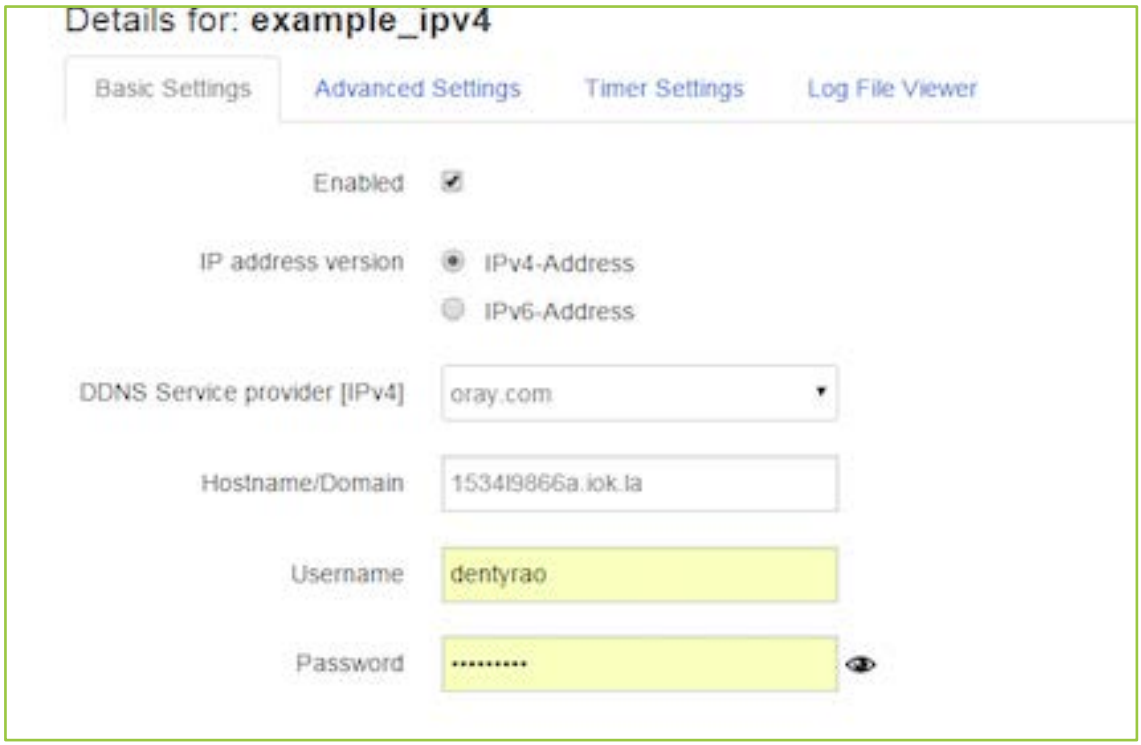


- **Enable:** Enable the GRE tunnel feature.
- **TTL:** Time-to-live.
- **MTU:** Maximum transmission unit.
- **Peer IP address:** The remote WAN IP address.
- **Remote Network IP:** The remote LAN subnet address that can be accessed via the GRE tunnel, such as 192.168.10.0.
- **Remote Netmask:** The remote LAN subnet mask. Such as 255.255.255.0.
- **Local Tunnel IP:** Virtual IP address. It cannot be in the same subnet as the LAN network.
- **Local Tunnel Mask:** Virtual IP mask.
- **Local Interface:** Bond a specific interface for the GRE tunnel.
- **Keepalive:** Options are None, receive only, send and receive. If the value is None, the GRE tunnel will remain up, if the value is receive only and if no GRE keepalive message is received for the peer device, it will set the tunnel to up. If the value is send and receive, it will send a keepalive message to the remote peer and it will receive a keepalive message from the peer.

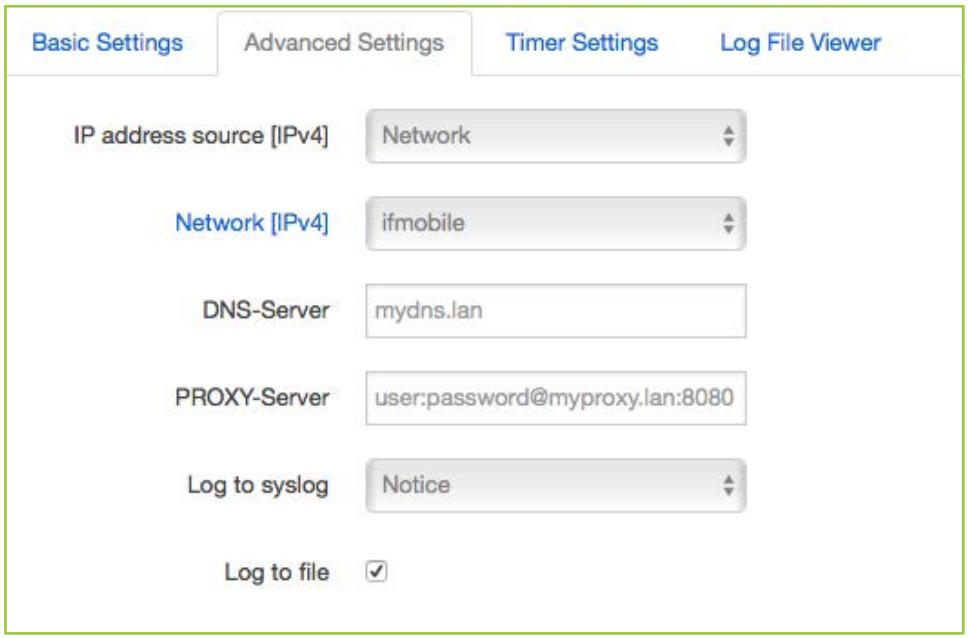
3.5.9 DDNS

DDNS allows the router to be reached with a fixed domain name while having a dynamically changing IP address.

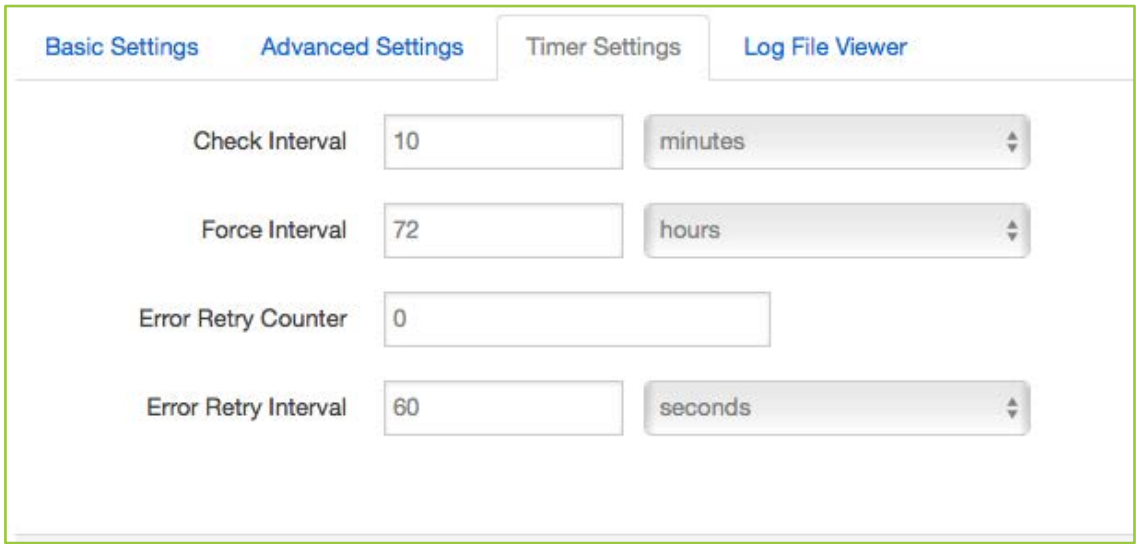




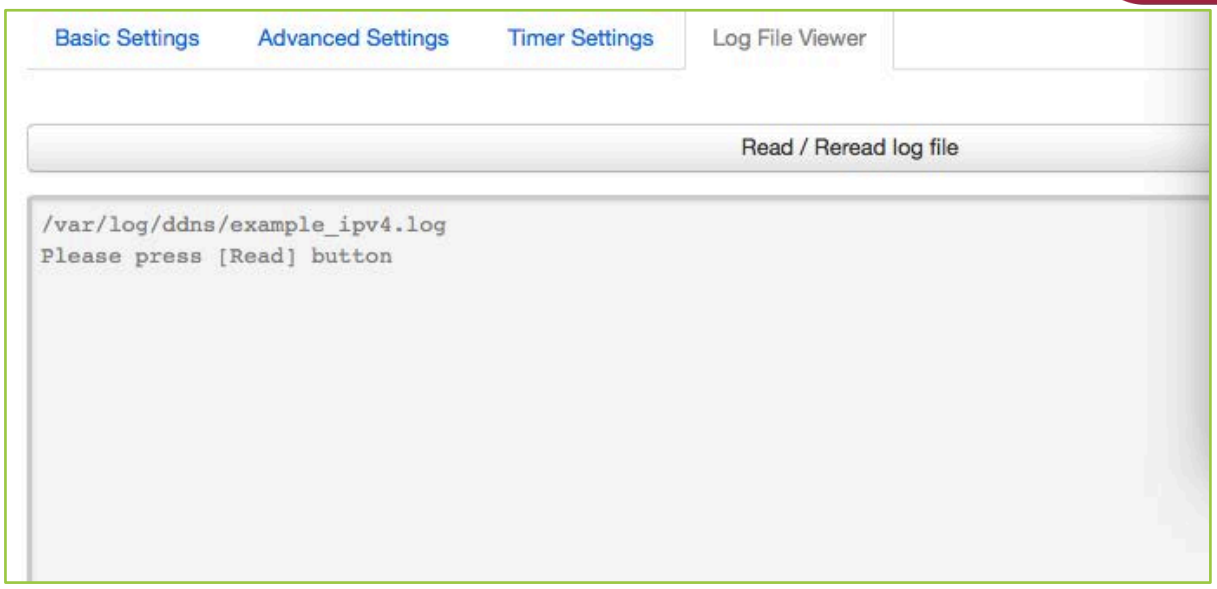
- **Enabled:** Enable this instance.
- **IP address version:** IPv4 and IPv6 supported.
- **DDNS Service provider:** Select a suitable provider.
- **Hostname/Domain:** The domain name that you can access the router by.



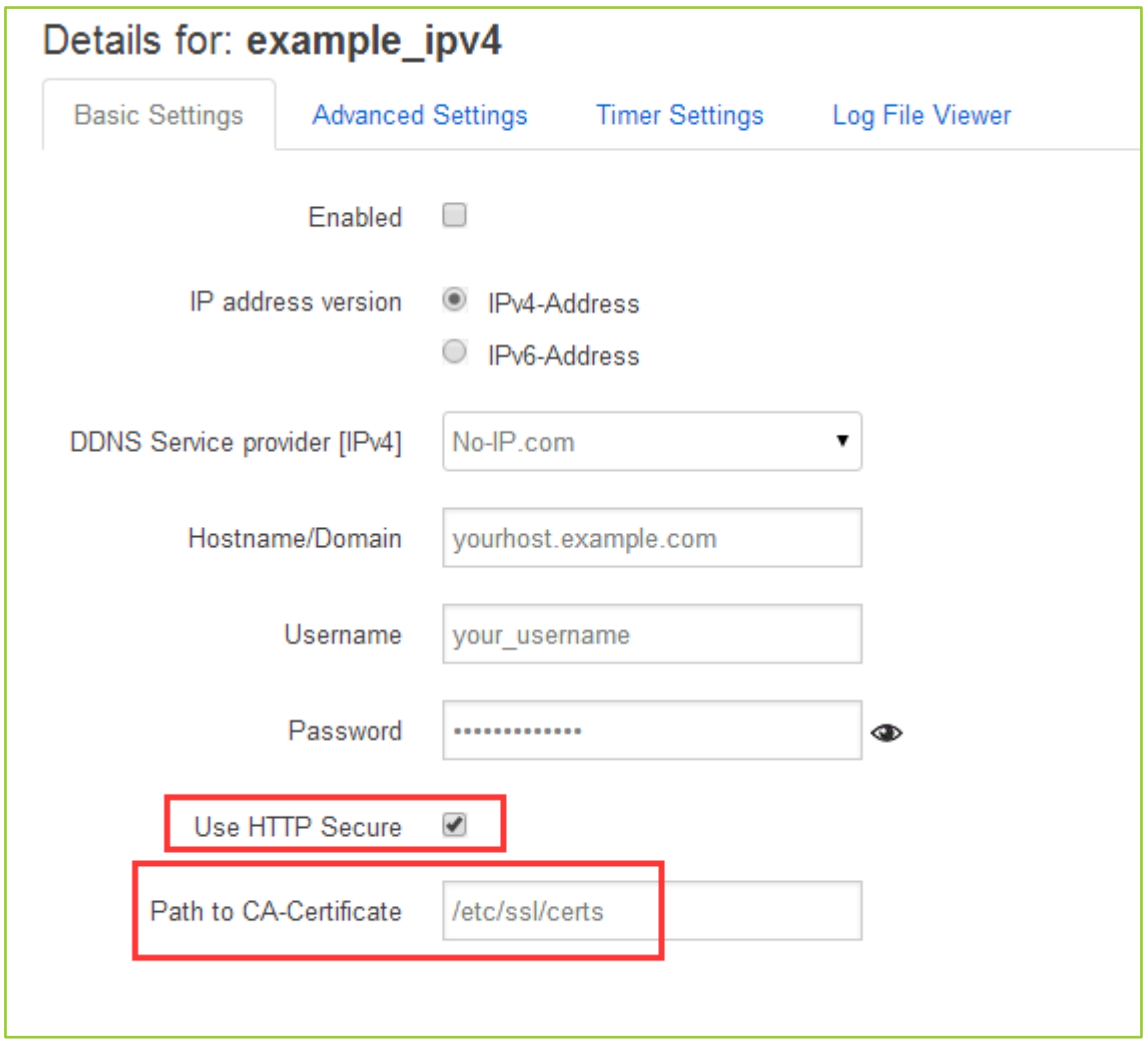
- **IP address source:** Defines the source that reads the systems IPv4-Address from and that will be sent to the DDNS provider. The recommended option is network.
- **Network:** Defines the network that reads the systems IPv4-Address from.
- **DNS-server:** OPTIONAL: Use the non-default DNS-Server to detect 'Registered IP'. IP address and domain name is required.
- **Log to syslog:** Writes log messages to syslog. Critical Errors will always be written to syslog.
- **Log to file:** Writes detailed messages to the log file. The file will be truncated automatically.

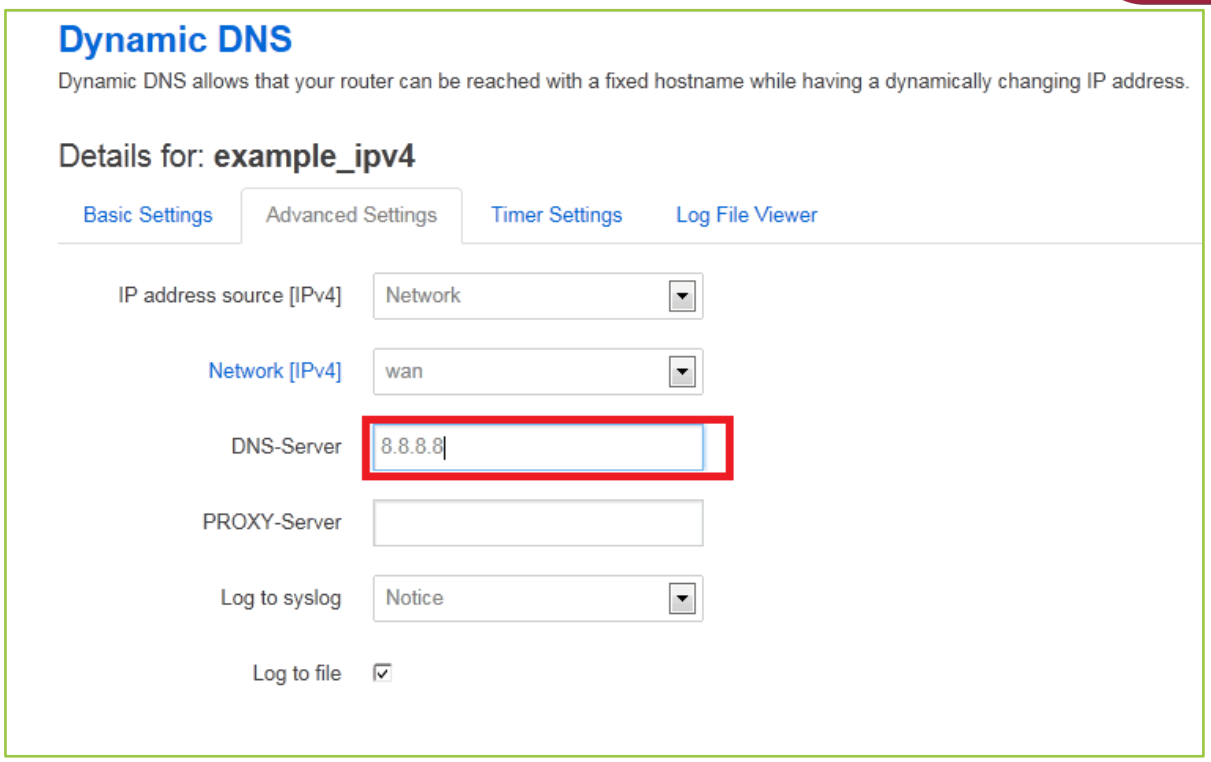


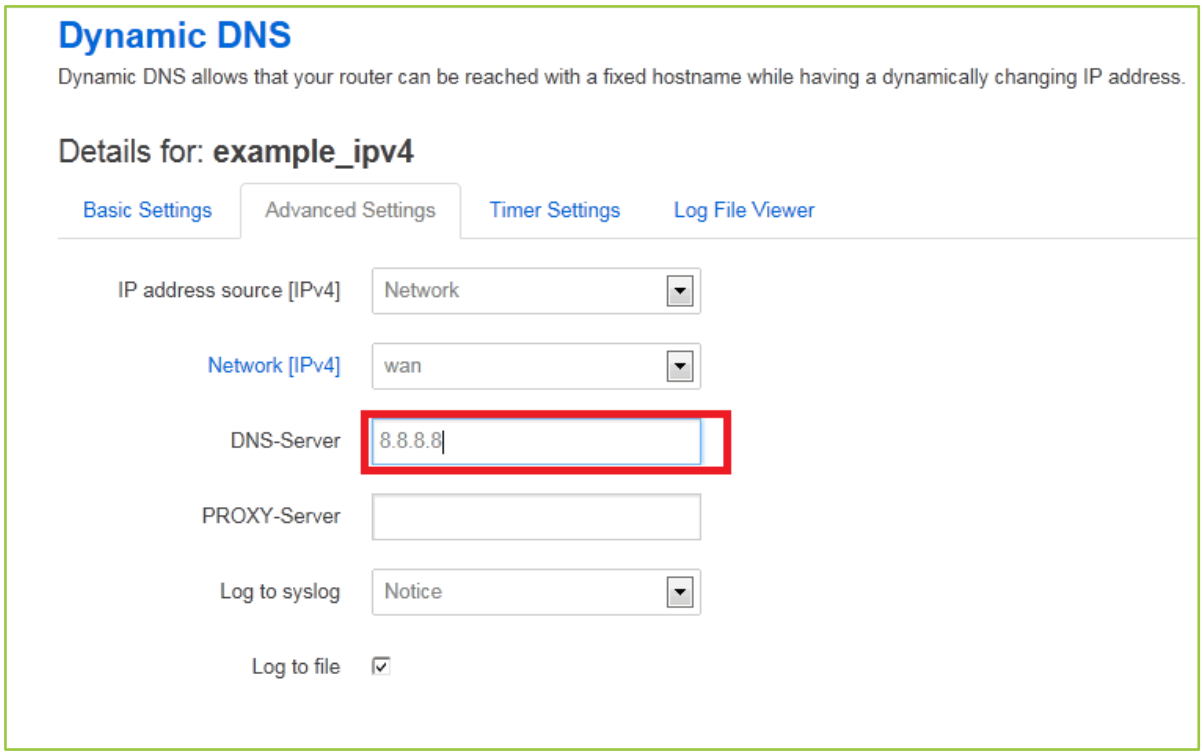
- **Check Interval:** The minimum check interval is 1 minute=60seconds.
- **Force interval:** The minimum check interval is 1 minute=60seconds.
- **Error Retry Counter:** On Error the script will stop execution after a given number of retries. The default setting of '0' will retry infinitely.



Note: If using the DDNS server no-ip.com, please check that the **"Use HTTP Secure" b**ox and put "8.8.8.8" for the DNS-Server, referring to the following picture.



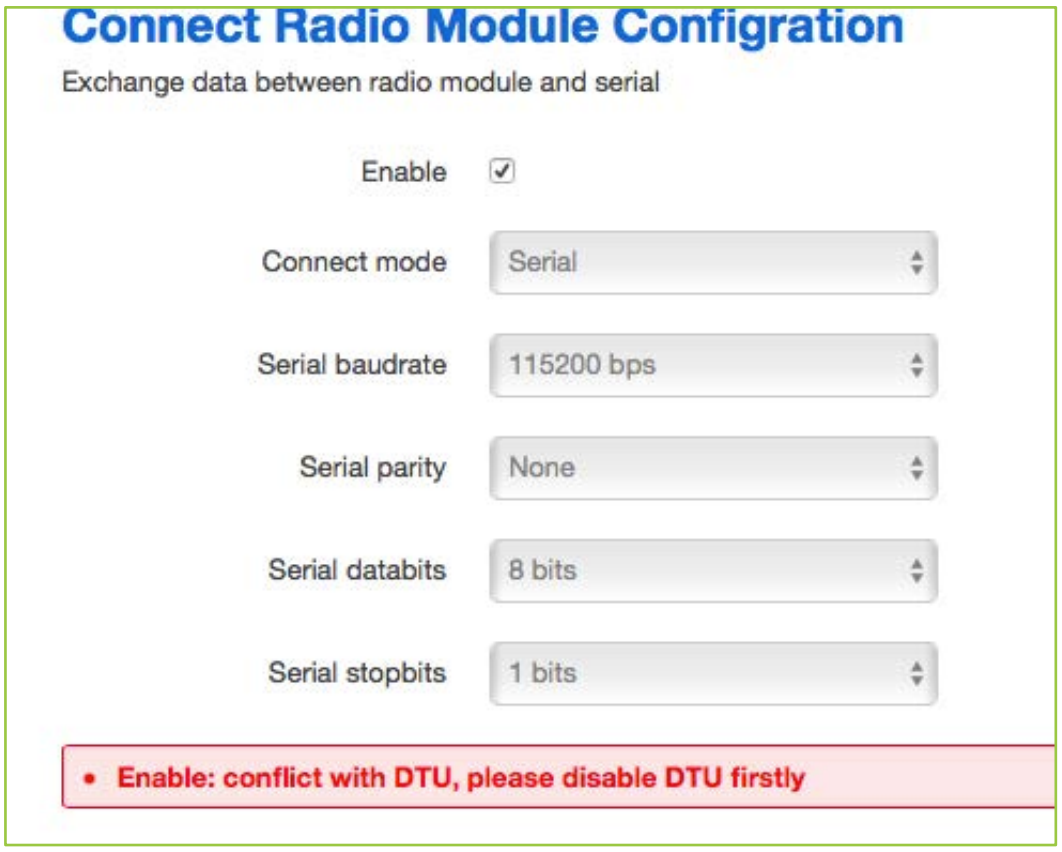

Dynamic DNS
Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.
Details for: example_ipv4
Basic Settings
Advanced Settings
Timer Settings
Log File Viewer
IP address source [IPv4]
Network
Network [IPv4]
wan
DNS-Server
8.8.8.8
PROXY-Server
Log to syslog
Notice
Log to file


Dynamic DNS
Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.
Details for: example_ipv4
Basic Settings
Advanced Settings
Timer Settings
Log File Viewer
IP address source [IPv4]
Network
Network [IPv4]
wan
DNS-Server
8.8.8.8
PROXY-Server
Log to syslog
Notice
Log to file

3.5.10 Connect Radio Module

Connect the Radio Module feature is used for exchanging data between the Radio module and the serial.

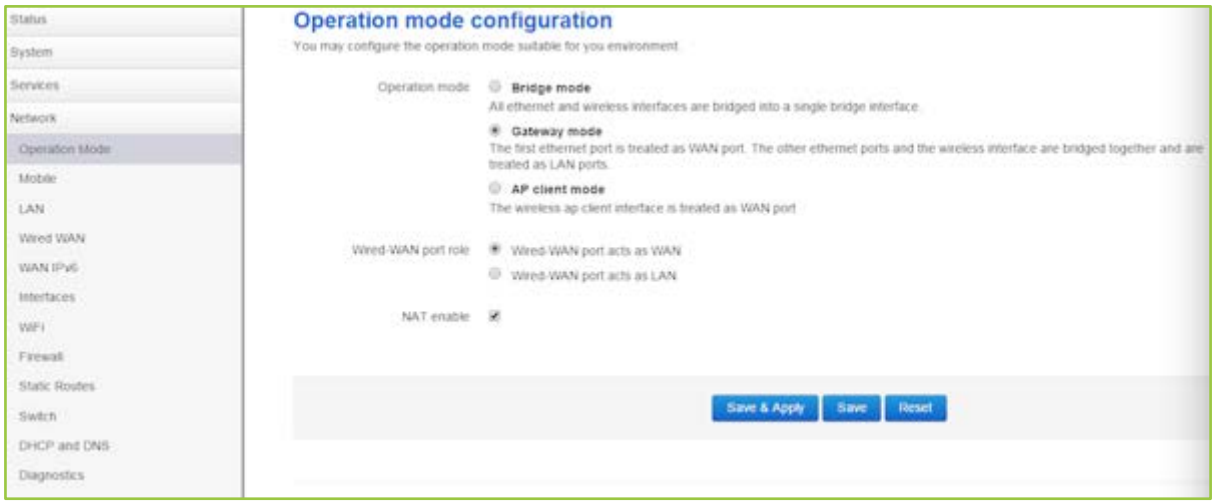
Notes: This feature conflicts with the DTU and **"GPS sent to serial".** Please make sure that the other two features are disabled before enabling the Connect Radio Module. Otherwise this error will occur.



- **Connect Mode:** Serial only.
- Modem to Serial Settings
- **Serial baudrate:** Supports 9600/19200/38400/57600/115200bps
- **Serial parity:** Supports none/odd/even
- **Serial databits:** Supports 7 bits and 8 bits
- **Serial stopbit**: Supports 1 bits and 2 bits
- **Serial Flow Control:** Supports none/hardware/software

3.6 Network Configuration

3.6.1 Operation Mode



Operation mode

- **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface.
- **Gateway:** The first Ethernet port is treated as a WAN port. The other Ethernet ports and the wireless interface are bridged together and are treated as LAN ports.
- **AP Client:** The wireless apcli interface is treated as a WAN port and the wireless AP interface and the Ethernet ports are LAN ports.

NAT Enabled
Network Address Translation. Default is Enabling.
Ethernet wan port role:
Wired-WAN port acts as WAN.
The Ethernet WAN port is used as the WAN. Default is Checked.
Wired-WAN port acts as LAN.
The Ethernet WAN port is used as the LAN port to get 2 LAN Ethernet ports. If the WAN RJ45 Ethernet port is used for the WAN, please do not check this feature.

Default setting is **"Gateway mode".** Keep all other parameters as default.

3.6.1.1 LAN Ethernet Ports

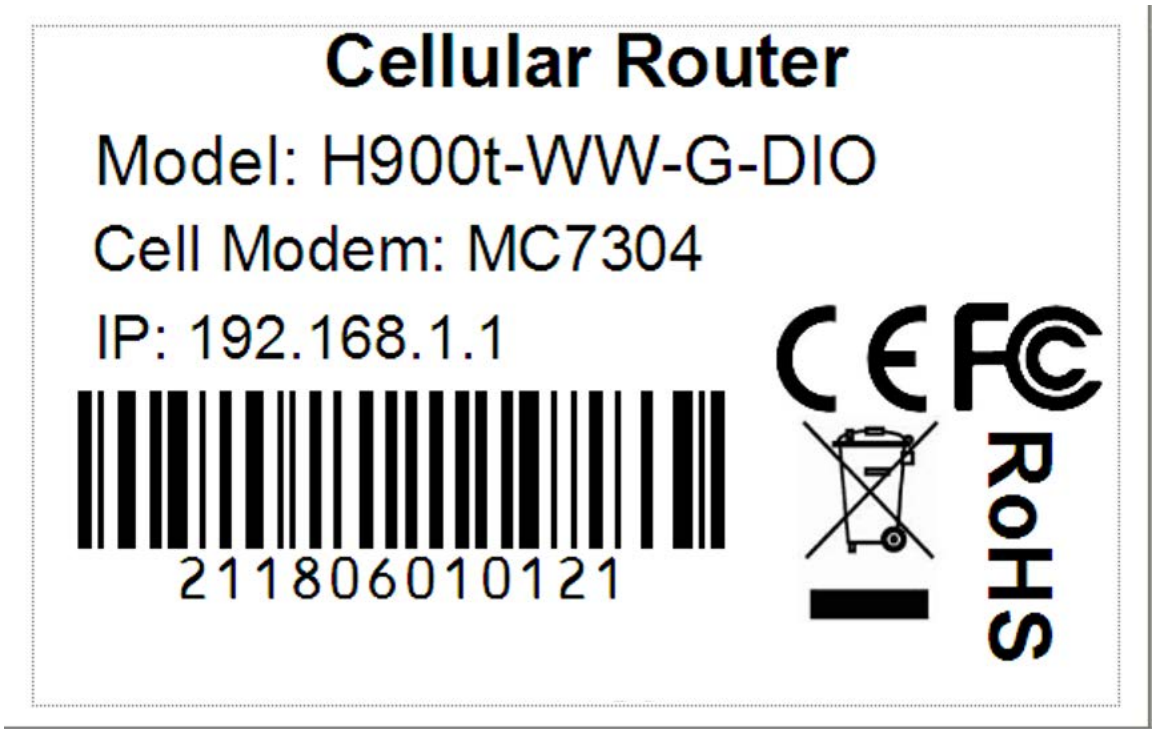
Check the " Wired-WAN port acts as LAN ".

Note:
1) If checked the **"Wired-WAN port acts as LAN",** the C365-4G-H900 will not have a WAN RJ45 port.
2) Please do not use any features for WAN RJ45 if the **"Wired-WAN port acts as LAN"** is checked.

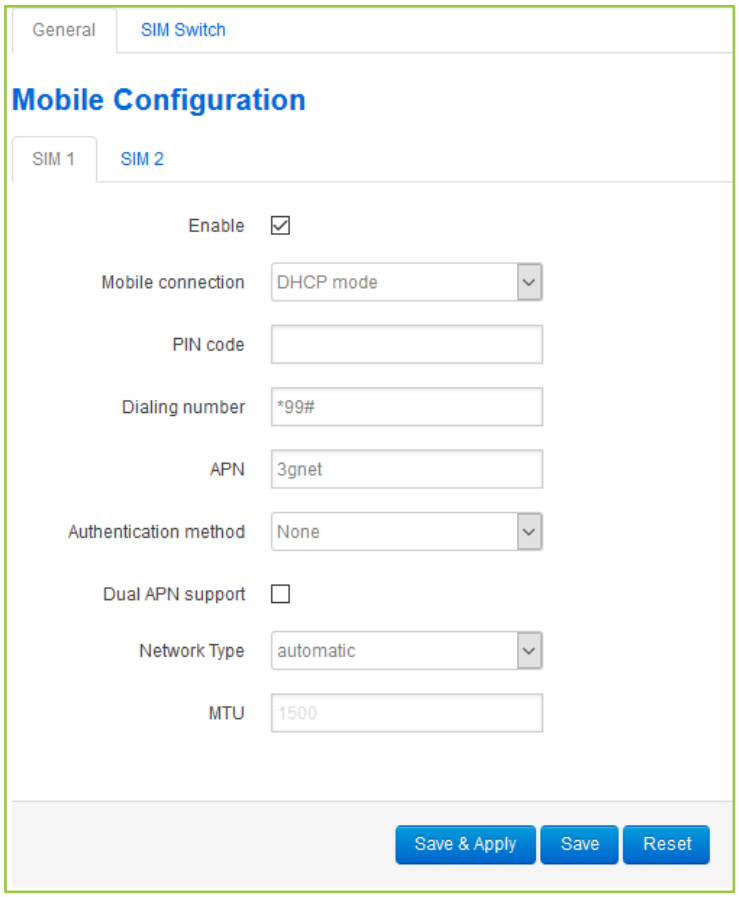
3.6.2 Mobile Configuration

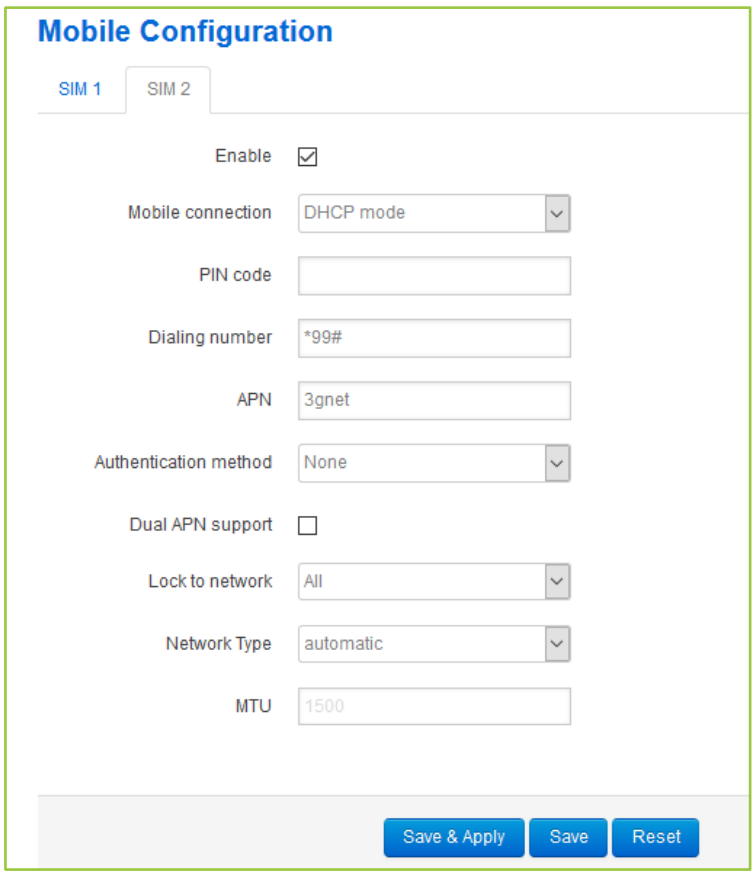
Systems support different cell modems. By default, the router is set to the correct Cell Modem name before shipment. If you replace it with another Cell Modem and it is not supported, the router will automatically detect the Cell Modem.

Note: The Cell Modem Type was marked on the back of the router.
For example, it shows the following picture. H900 is the router series name, H900t-WW-G-DIO is the part number name. And the MC7304 Cell Modem is the Cell Modem name.



Configure the parameters for SIM1 and SIM2.


General
SIM Switch
Mobile Configuration
SIM 1
SIM 2
Enable
Mobile connection
DHCP mode
PIN code
Dialing number
*99#
APN
3gnet
Authentication method
None
Dual APN support
Network Type
automatic
MTU
1500
Save & Apply
Save
Reset

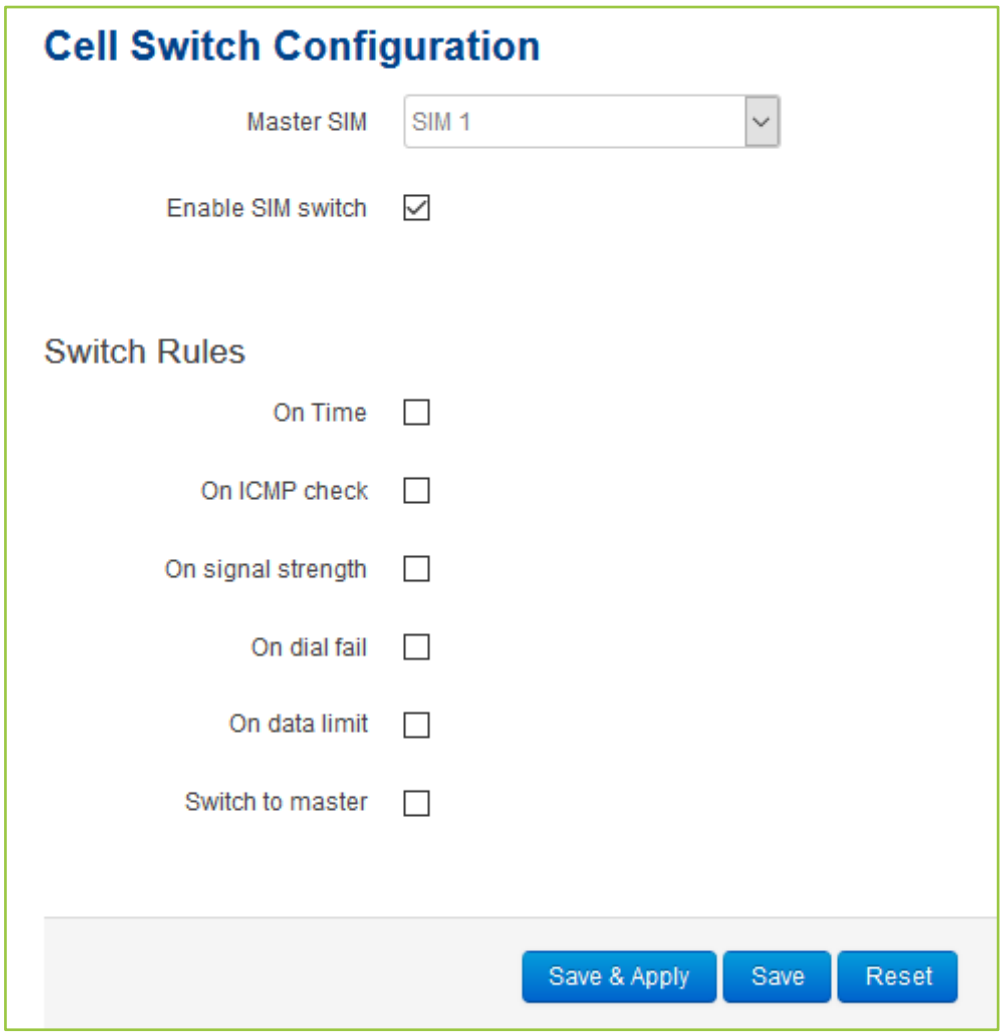

Mobile Configuration
SIM 1
SIM 2
Enable
Mobile connection
DHCP mode
PIN code
Dialing number
*99#
APN
3gnet
Authentication method
None
Dual APN support
Lock to network
All
Network Type
automatic
MTU
1500
Save & Apply
Save
Reset

Item	Description	
Enable	Check it	
Mobile connection	DHCP mode or PPP mode. Normally system will be automatically selected.	
PIN code	If the SIM card uses a PIN code, please put it here. The wrong PIN code will prevent the router from working. If the SIM card doesn't use a PIN code, please keep it blank.	
Dialing number	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier. With experience, most of the time, 2G/3G/4G uses *99#, and CDMA/EVDO use #777.	
APN	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier;	
Authentication method	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier;	
	None	No more settings.
	CHAP	Username and Password required.
	PAP	Username and Password required.
Dual APN support	Most of the SIM cards or Carriers/Operators use just one APN, but some use two APNs. Check this feature to before use. Second APN: configure it referring to APN; Second Authentication method: configure it referring to Authentication method;	
Lock to network	Normally keep default settings.	
Network Type	Select the network you want to use or use default settings.	
Demand	Use default settings.	
MTU	Use default settings.	
Item	Description.	
Enable	Check it.	
Mobile connection	DHCP mode or PPP mode. The system will automatically select.	
PIN code	If the SIM card uses a PIN code, please put it here. The wrong PIN code will prevent the router from working. If the SIM card doesn't use the PIN code, please keep blank.	
Dialing number	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier. With experience, most of the time, 2G/3G/4G uses *99#, and CDMA/EVDO use #777.	
APN	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier;	
Authentication method	Fill in the right parameters. Get this parameter from the Sim Card Provider or Carrier;	
	None	No more settings
	CHAP	Username and Password required.
	PAP	Username and Password required.
Dual APN support	Most of the SIM cards or Carriers/Operators use just one APN, but some use two APNs. Check this feature to use. Second APN: configure it referring to APN; Second Authentication method: configure it referring to Authentication method	
Lock to network	Normally keep default settings. For some models, there is no this option.	
Network Type	Select the network you want to use. Normally keep default settings	
Demand	Use default settings.	
MTU	Use default settings.	

Click the Save button for the next step;

Click the SIM Switch to configure the SIM working mode.


General
SIM Switch
Mobile Configuration
SIM 1
SIM 2


Cell Switch Configuration
Master SIM
SIM 1
Enable SIM switch
Switch Rules
On Time
On ICMP check
On signal strength
On dial fail
On data limit
Switch to master
Save & Apply
Save
Reset

Item	Description	
Master SIM	Choose the SIM1 or SIM2 for the master SIM, the other SIM will automatically be a backup SIM.	
Enable SIM switch	Check this to enable the SIM switch feature. If unchecked, the router works with a single SIM.	
Switch Rules	On Time	Check this, the two SIMs switch with trigger at a scheduled time.
	On ICMP check	Check this, the two SIMs switch with trigger of cell alive. The data traffic goes via the Master SIM, once the Master SIM has failed, switch to the backup SIM. Once the backup SIM has failed, the data traffic switches to the Master SIM.
	On Signal strength	Set the signal ASU value from 1 to 30. For example, set the value as 10, the data traffic will switch from the Master SIM to the backup SIM if the master SIM signal value is less than 10.
	On dial fail	Master SIM and backup SIM switch with trigger, dialling a number of retries. For example, set the value as 5, the data traffic will switch from Master SIM to backup SIM if master SIM dial failure reaches 5.
	On data limit	Master SIM and backup SIM switch with trigger of SIM data limit.
	Switch to master	For example, check this feature and set the value as 3 minutes. With some issues, the data traffic goes via the backup SIM. The router will check the master SIMs working status. If the master SIM is working, the data traffic will switch to the master SIM after 3 minutes.
Notes: some trigger rules can be selected and used at the same time to meet different applications.		

- **Enable:** Enable mobile network;
- **Mobile connection:** Select a suitable mode for the mobile to connect, if the cell modem only supports 3G, the default mode is pppd mode, otherwise the default value is DHCP mode;
- **APN:** Fill in the related parameters. Get this parameter from the Sim Card Provider or Carrier;
- **PIN number:** If necessary, fill in the related parameters. If the SIM card has no PIN code, and then keep it as blank;
- **Dialing number:** Fill in the related parameters. Get this parameter from the SIM Card Provider or Carrier;
- **Authentication method:** Three options (None, PAP, CHAP). Please confirm your carrier, provide the types of authentication. Normally select None. If it is not working then try to use PAP or CHAP;
- **Username:** Fill in the related parameters. Get this parameter from the SIM Card Provider or Carrier. Notes: If your SIM card has no username, please input out default value, otherwise the router may not dialup. Note: if the authentication method is None, this parameter will not be displayed.
- **Password:** Fill in the related parameters. Get this parameter from the Sim Card Provider or Carrier.

Note: If your SIM card has no username, please input out default value, otherwise the router may not dialup.

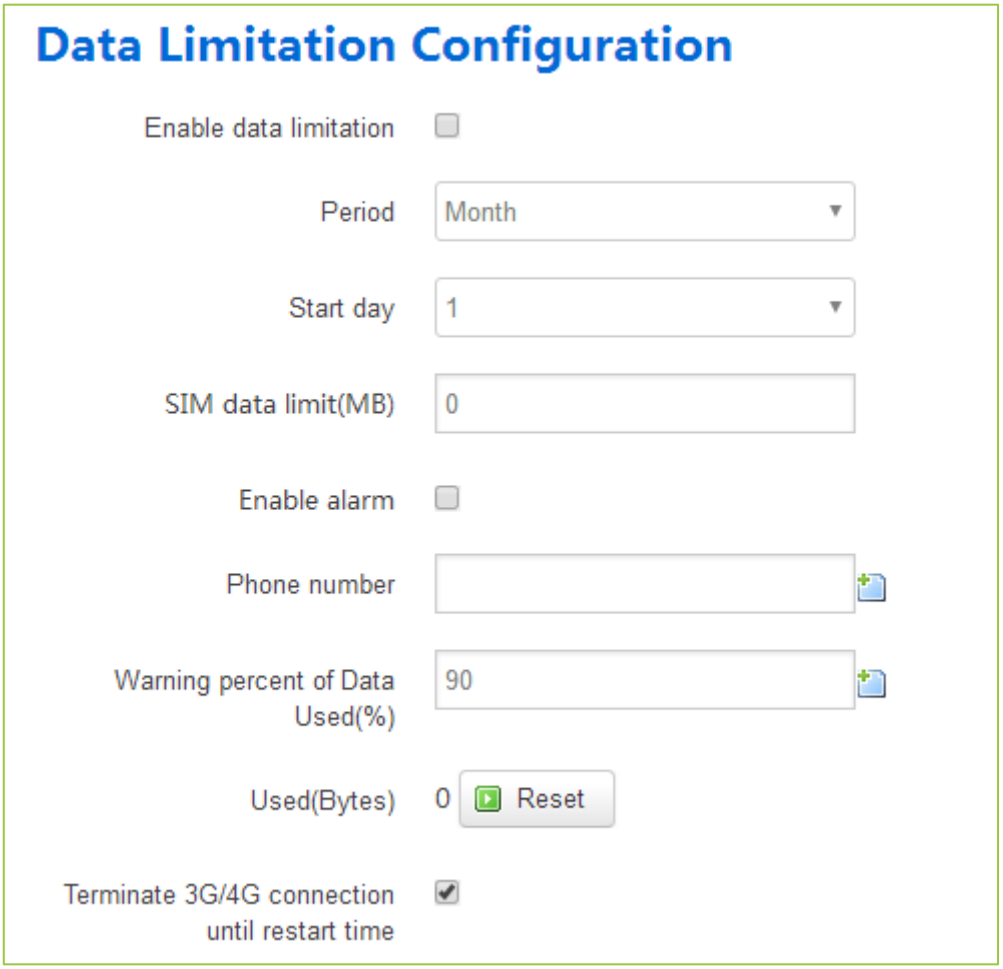
Note: if the authentication method is None, this parameter will not be displayed.

- **Network Type:** Select the type. Different Cell Modems support different types. The default value is Automatic.
- **MTU:** Maximum Transmission Unit. This is the max size of packet transmitted on the network. The default value is 1500. Please configure it to optimize your own network.
- **Online Mode**
- **Keep Alive:** means always online. The router will keep online whenever there is data for transmission or not.
- **On Demand:** The router will dialup when there is data for transmission.
- **Idle time (minutes):** Fill in the time. For example, enter 5 and the router will be offline after 5 minutes

if there is no data for transmission.

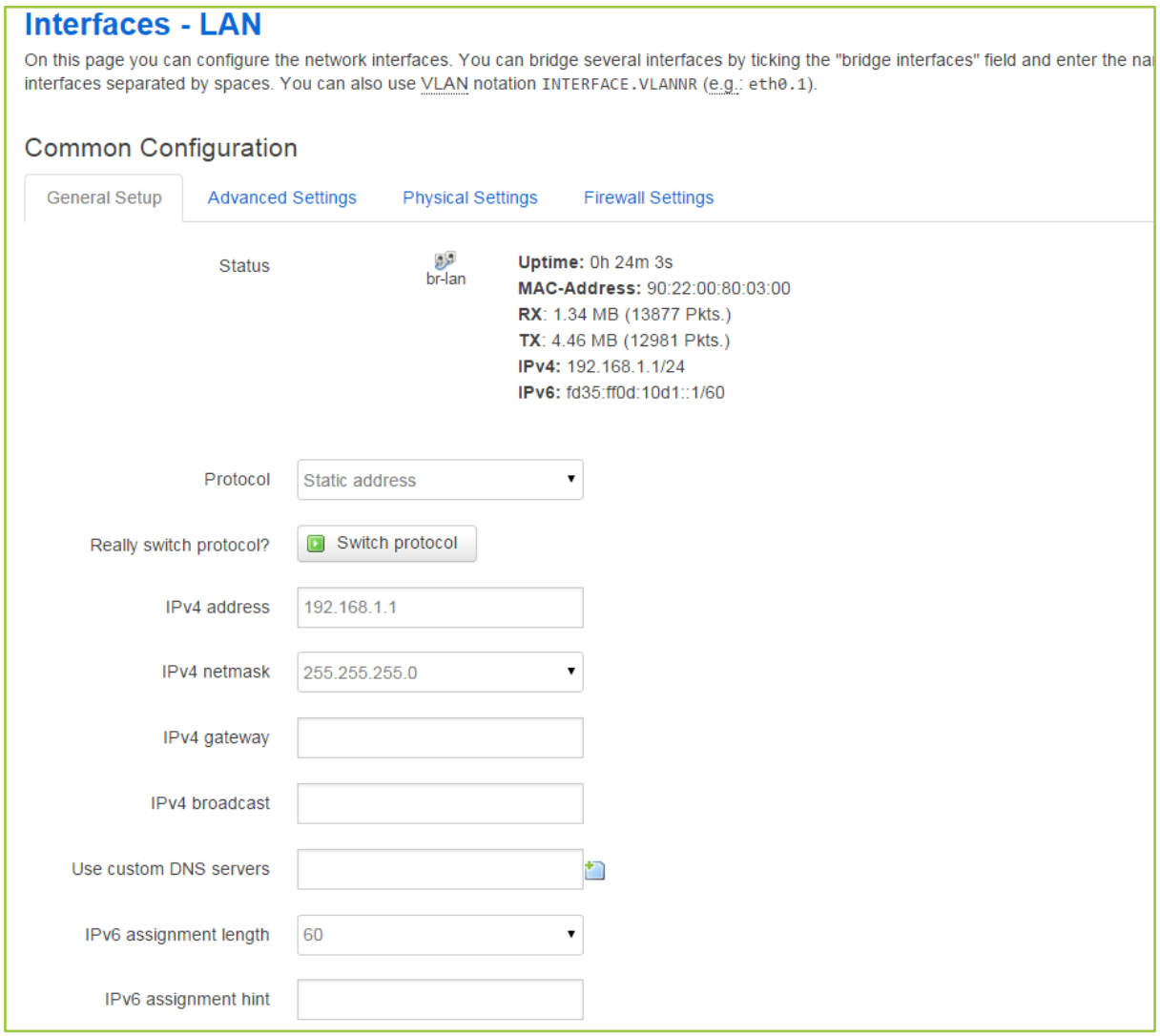
- Scheduled: Router dialup or offline with schedule. One group is supported.

3.6.3 Cell Mobile Data Limitation

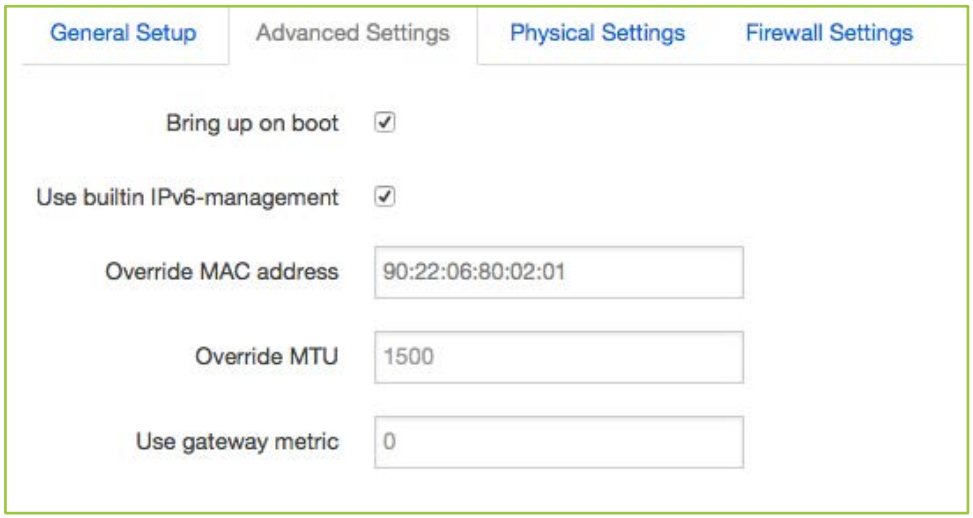


- **Enable data limitation:**
- **Period:** Support periods are Month, Week and Day.
- **Start day:** The beginning day of period.
- **SIM data limit(MB):** The maximum data that can be used during this period. If it exceeds, the router will disable the cell mobile network during this period.
- **Enable alarm:** Enable the data limitation alarm.
- **Phone number:** The phone number that receives the data limitation alarm SMS.
- **Warning percent of data used:** If the used data arrives at this limit, a data limitation alarm SMS will be sent.
- **Used(MB):** The amount of data consumed during this period.
- **Reset**: Press this button to clear all used data.
- **Terminate 3G/4G connection until restart time:** If the max data is exceed, set the cell interface to down.

3.6.4 LAN Settings

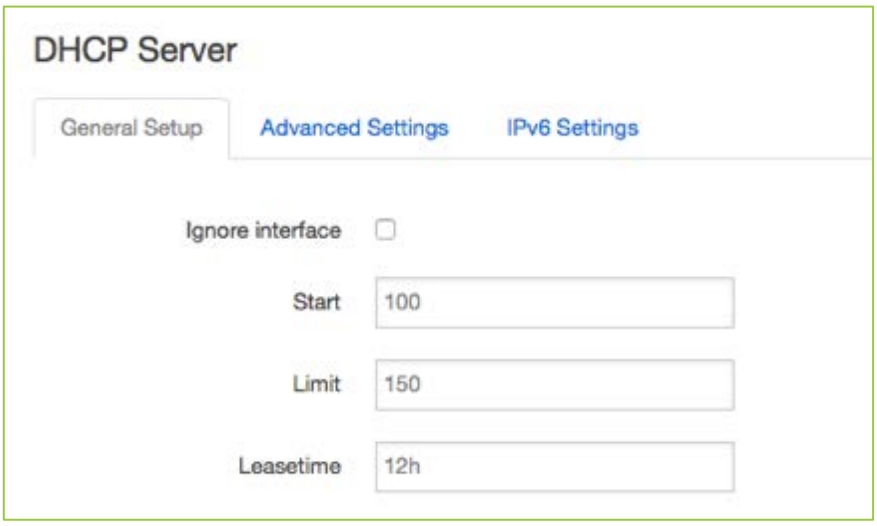


- **Protocol:** Only static addresses are supported for LAN
- **Use custom DNS servers:** Multiple DNS server supported.
- **IPv6 assignment length:** Assign a part of a given length of every public IPv6-prefix to LAN interface.
- **IPv6 assignment hint:** Assign prefix parts using this hexadecimal subprefix ID for LAN interface.

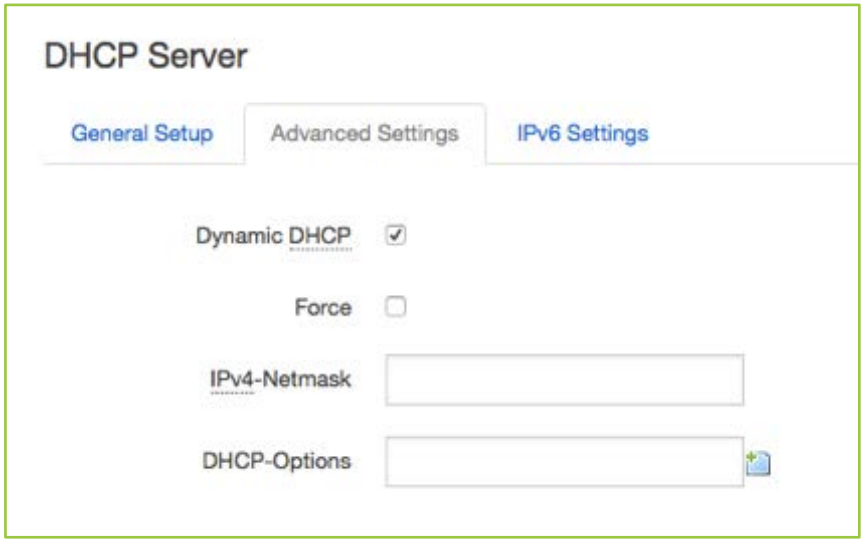


- **Bring up on boot:** If checked, the LAN interface will be set to up to when the system boots up. If unchecked, the LAN interface will be down. Don't set it to be unchecked if you don't have a specific purpose.
- Use built-in IPv6-management: The default is checked. If IPv6 is not needed, it can be set to unchecked.
- **Override MAC address:** Override LAN MAC address.
- **Override MTU:** Maximum Transmission Unit.
- **Use gateway metric:** The LAN subnet's metric gateway.

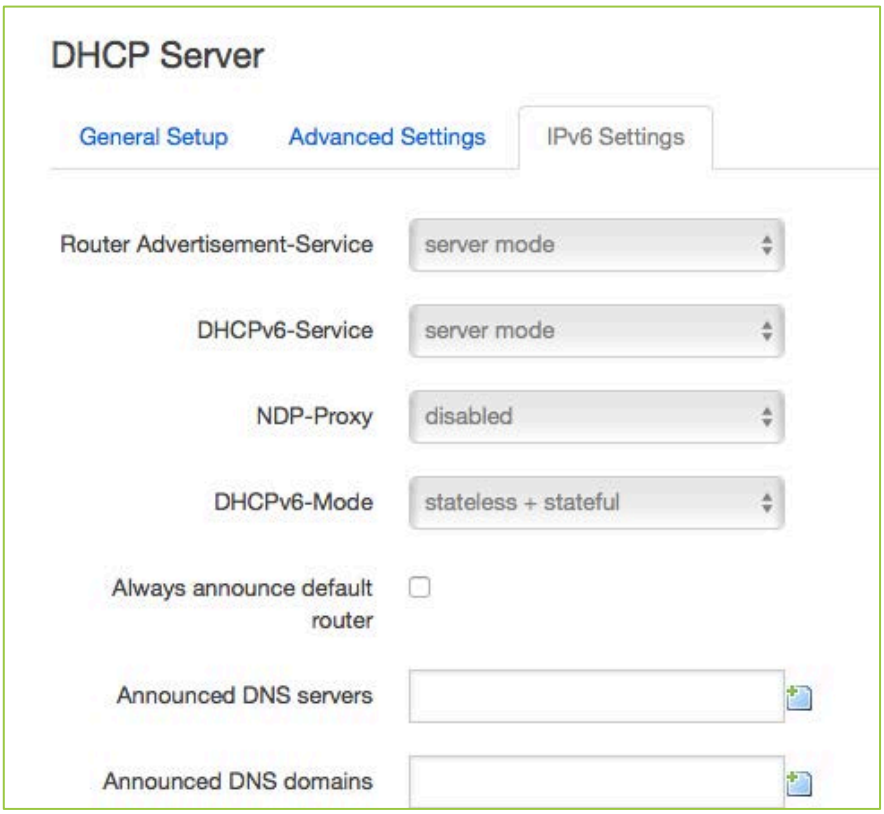
- **Bridge interfaces:** LAN bridges wired-LAN and Wi-Fi in a same LAN subnet.
- **Enable STP:** Enable the Spanning Tree Protocol on the LAN. The default value is unchecked.



- **Ignore interface:** If it is unchecked, Disable DHCP on LAN.
- **Start:** Lowest leased address as offset from the network address.
- **Limit**: Maximum number of leased addresses.
- **Lease time:** Expiry time of leased addresses, minimum is 2 minutes(2m). 12H means 12 hours.

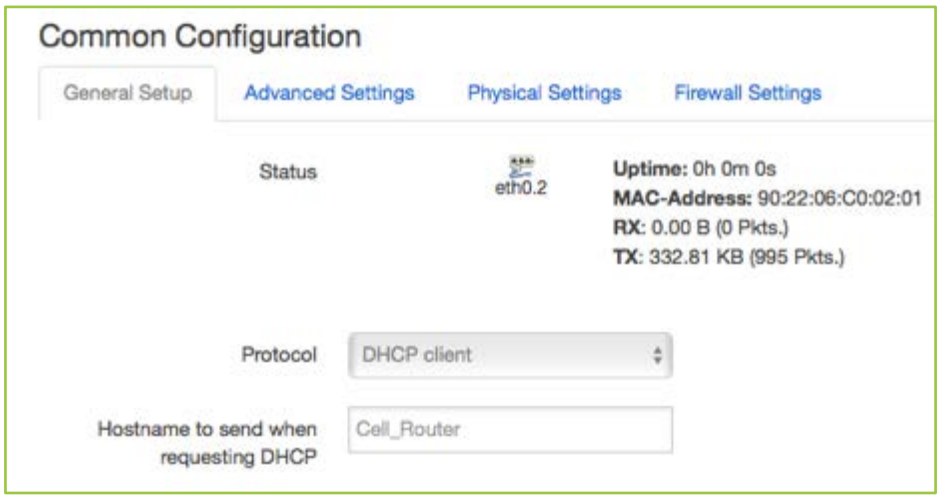


- **Dynamic DHCP:** Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
- **Force:** Force DHCP on this network even if another server is detected.
- **IPv4-Netmask:** Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
- **DHCP-Options:** Define additional DHCP options, for example '6,192.168.2.1,192.168.2.2' which advertises different DNS servers to clients.

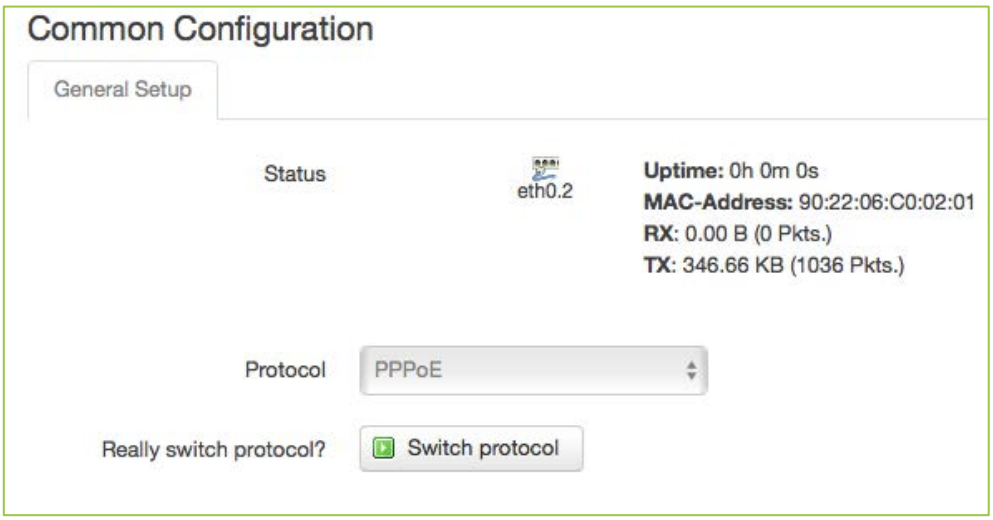


- **Router Advertisement-Service:** Four options: disabled, server mode, relay mode and hybrid mode.
- **DHCPv6-Service:** Has the same options with Router Advertisement-Service.
- **NDP-Proxy: three options:** Disabled, relay mode and hybrid mode.
- **Always announce default router:** Announce as the default router even if no public prefix is available.

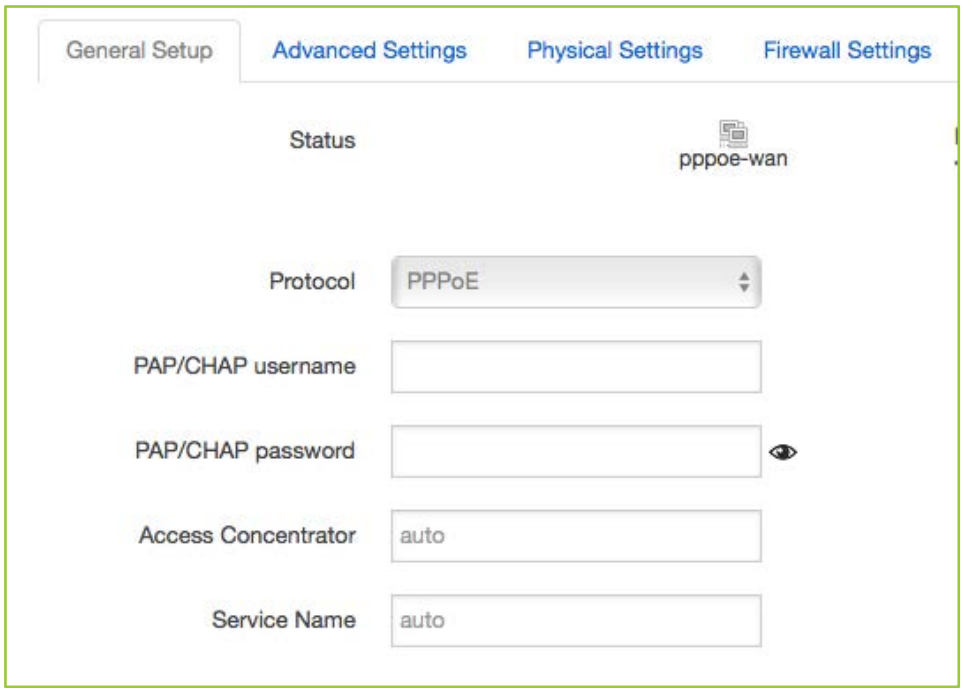
3.6.5 Wired WAN



Protocol: the default protocol is DHCP client. If it should be changed to another protocol, such as PPPoE, select protocol PPPoE, then click button the **"Switch protocol".**



After, click the **"Switch protocol"** button, the below screen appears:

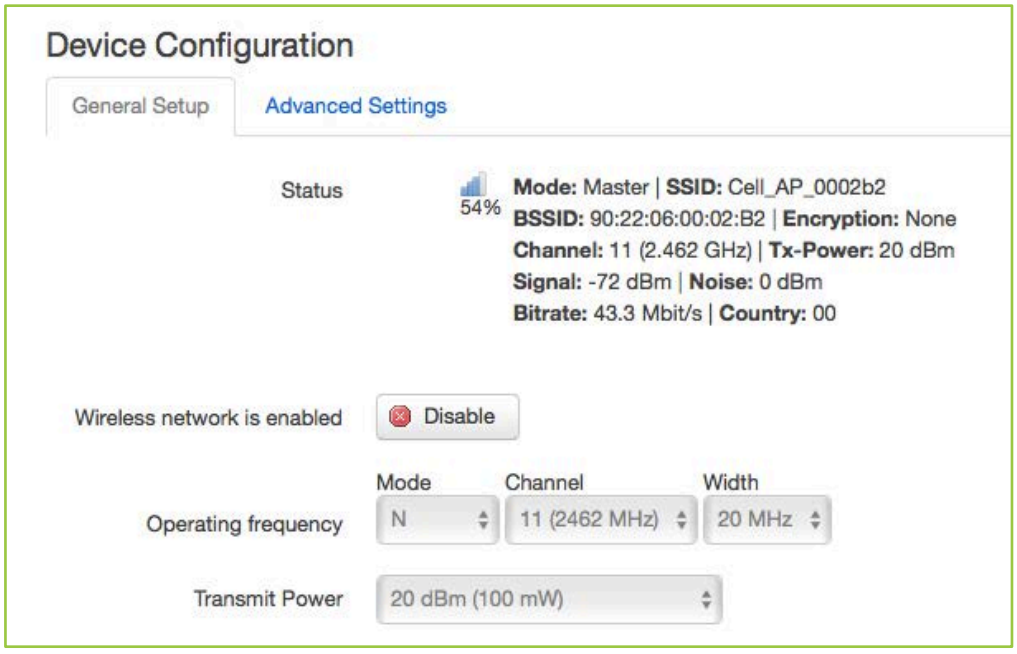


Note: for different protocols the Advanced Settings are different, please put the mouse over the title to receive help information, the recommend web browser is Google Chrome.

3.6.6 Wi-Fi Settings

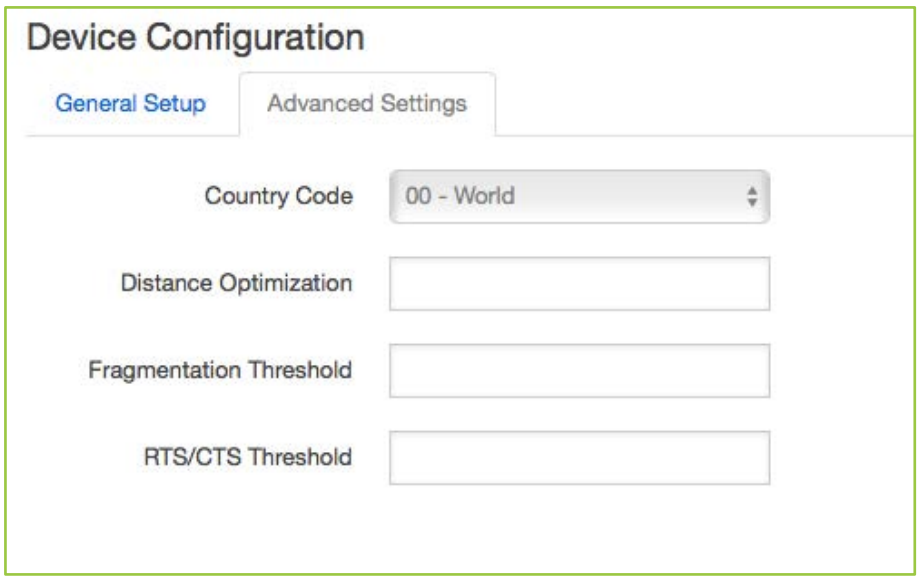
- **Wi-Fi Restart:** Turn off Wi-Fi, and then turn it on again.
- **AP Client:** Scan all frequencies to get the Wi-Fi network information.
- **Add:** Add a new Wireless network.
- **Disable:** Set the wireless network to down.
- **Edit:** Modify the detailed information of the wireless network.
- **Remove:** Delete a wireless network.
- **Associated Stations:** This is a list of connected wireless stations.

3.6.6.1. Wi-Fi General Configuration



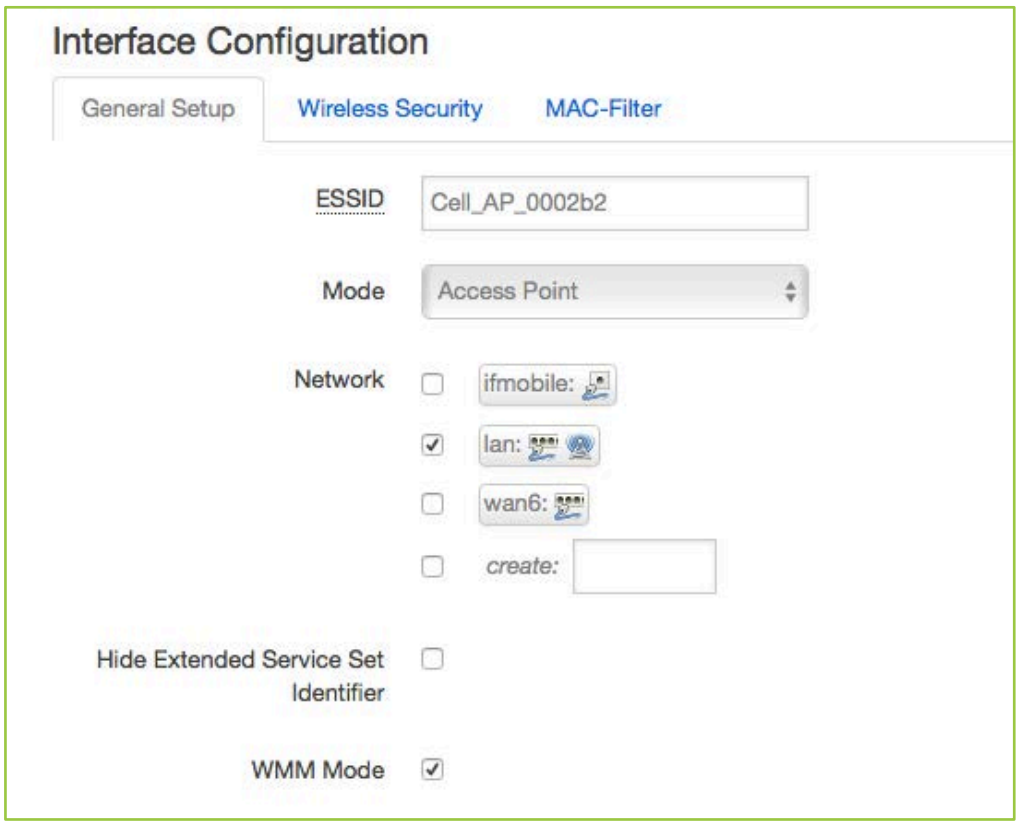
- **Status:** Show the Wi-Fi signal strength, mode, SSID and so on.
- **Operating frequency Mode:** supports 802.11b/g/n/ac. the Legacy means 802.11b/g. "N" means 802.11n. "ac" means 802.11ac.
- **Channel:** Channel 1-11 supported.
- **Width:** 20MHz and 40MHz.
- **Transmit Power:** From 0dBm to 20dBm supported.

3.6.6.2 Wi-Fi Advanced Configuration

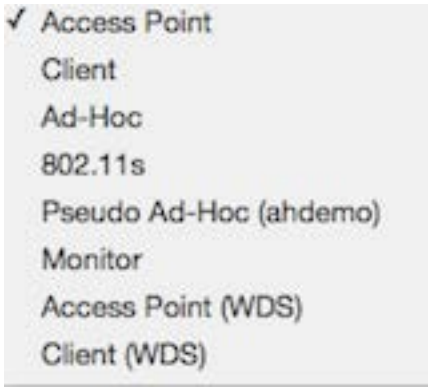


- **Country Code:** Use ISO/IEC 3166 alpha2 country codes.
- **Distance Optimization:** Distance to the farthest network member in meters.
- **Fragmentation Threshold:**
- **RTS/CTS Threshold:**

3.6.6.3 Wi-Fi Interface Configuration



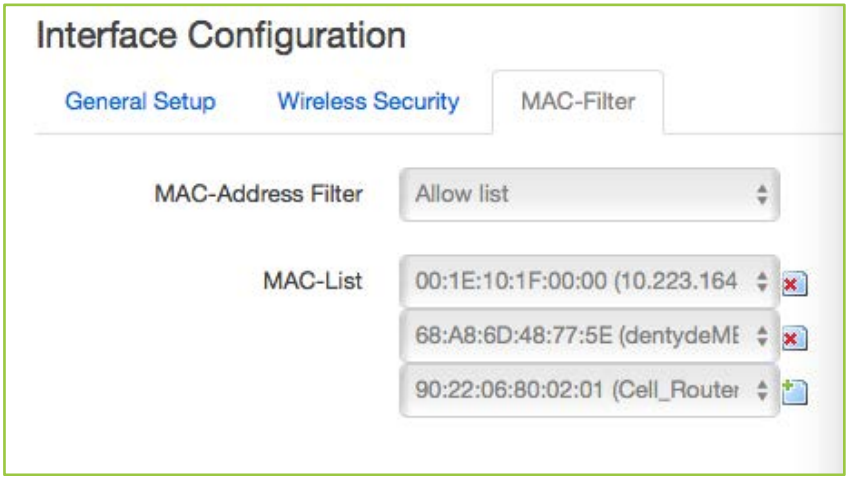
- **ESSID:** Extended Service Set Identifier. This is the broadcast name.
- **Mode:** Supported options.



- **Network:** Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
- **Hide Extended Service Set Identifier:** Hide SSID means this Wi-Fi cannot be scanned by others.
- **WMM Mode:**

- **Encryption:**

- **Key:** This is the password to join a wireless network. If the Encryption is set to "**No Encryption**", no password is required.

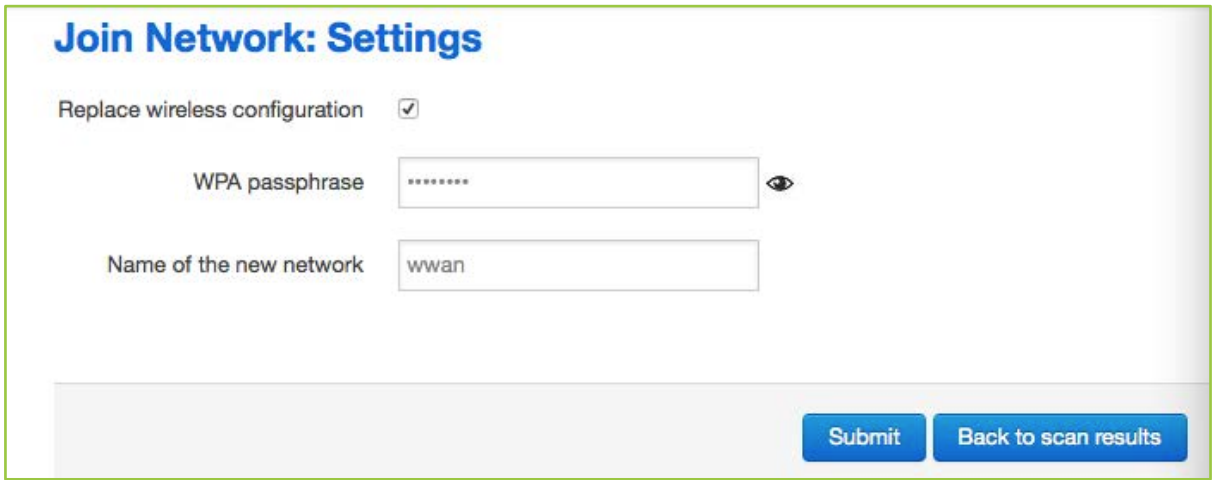


  - **MAC-Address Filter:** MAC address access policy. Disabled: disable MAC-address filter functionality. Allow list: only the MAC address in the list is allowed to proceed. Deny list: all packets are allowed to proceed except the MAC address on the list.
  - **MAC-List:** click button the button to delete the MAC address from the list, click the button to add to a new MAC address onto the list.

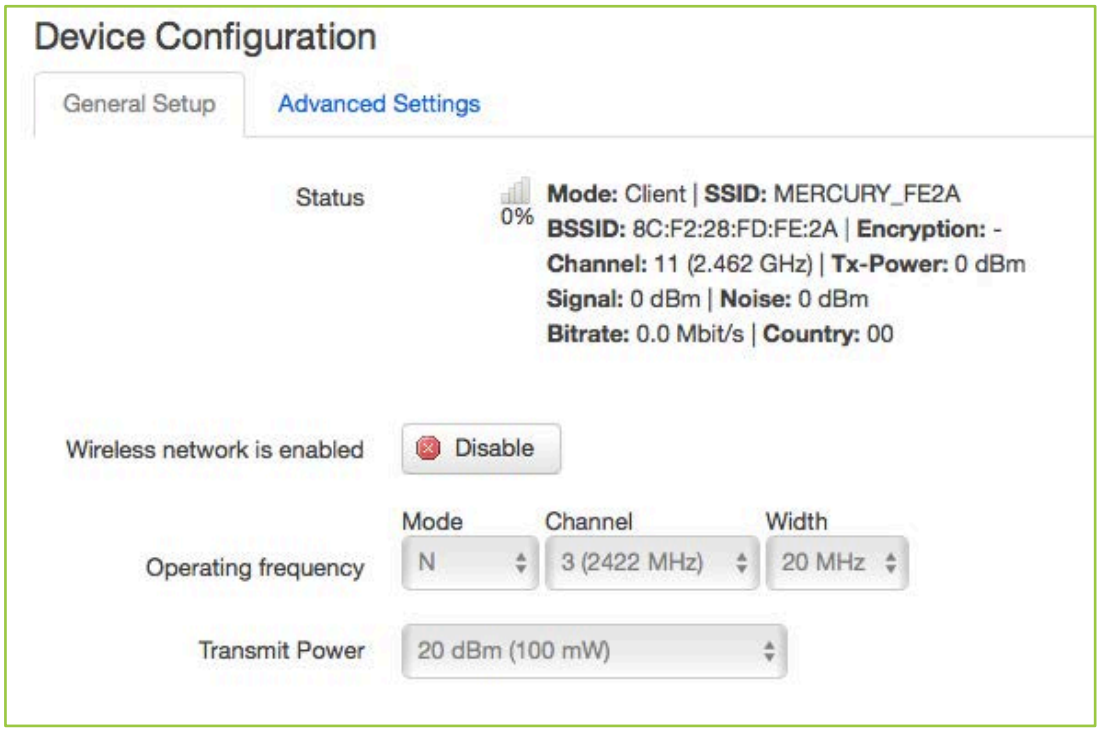
3.6.6.4 Wi-Fi AP Client

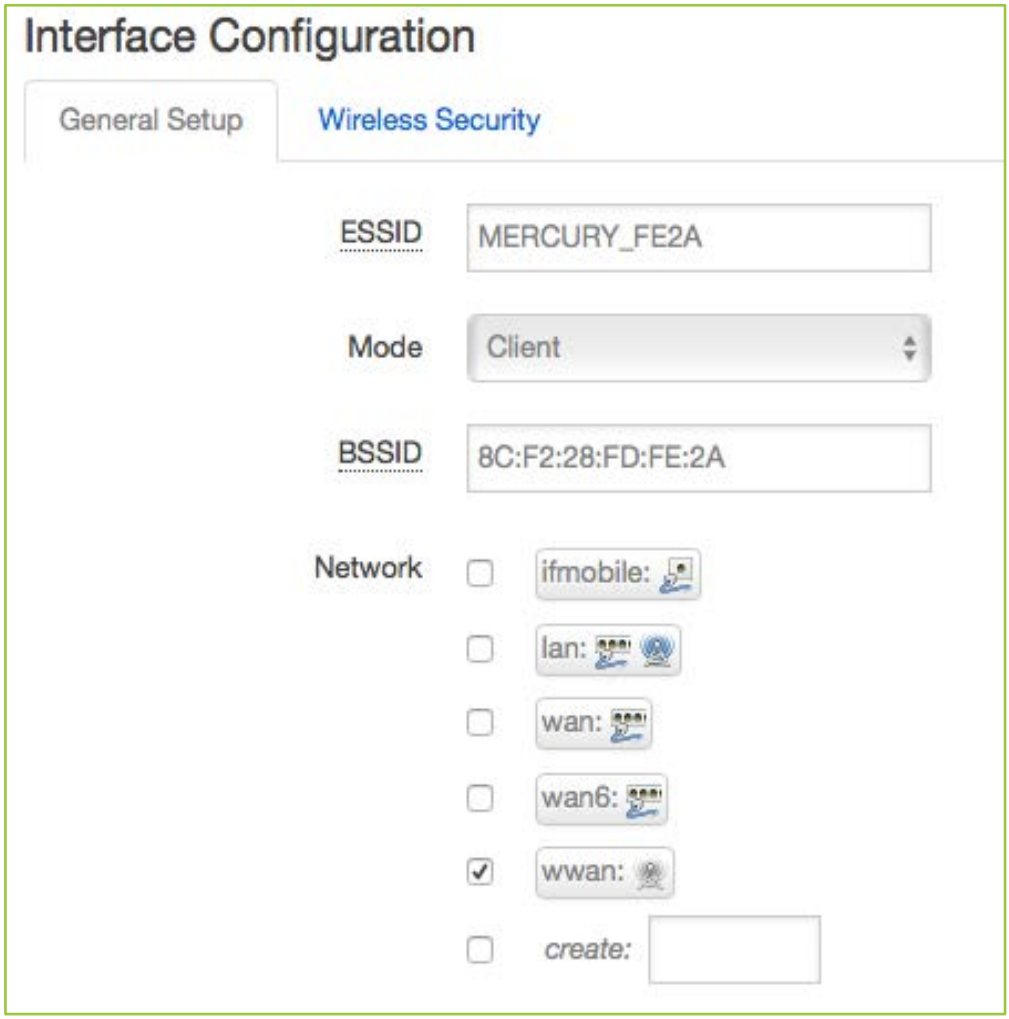
- **Step 1)** click the **"AP Client"** button on the wireless overview page, then the system will start to scan all Wi-Fi signals.

- **Step 2)** If the Wi-Fi you want to join is on the list, then click the **"Join Network"** button accordingly. If it is not, click **"Repeat Scan"** until you find the Wi-Fi that you want to join.



- **Step 3)** Join Network Settings
  Replace wireless configuration**:** An additional wireless network will be created if it is unchecked. Otherwise it will replace the old configuration.
  WPA passphrase: Specify the secret encryption key here.
  Name of the new network: The default value is wwan. If it conflicts with other interfaces, please change it. Otherwise don't change it.
- **Step 4)** Click Submit if everything is configured. The below is the Wi-Fi configuration page. Don't change the operating frequency, make sure the ESSID and BSSID is from the Wi-Fi you want to join.

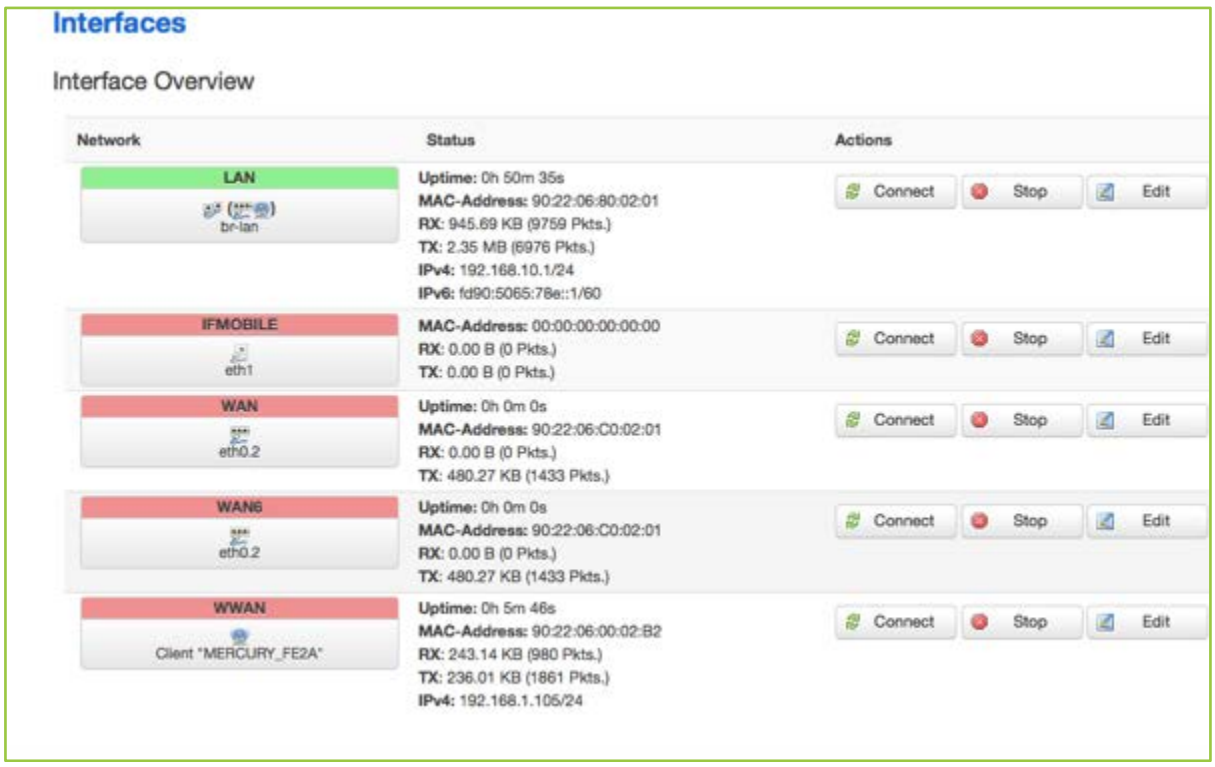

Device Configuration
General Setup
Advanced Settings
Status
0%
Mode: Client | SSID: MERCURY_FE2A
BSSID: 8C:F2:28:FD:FE:2A | Encryption: -
Channel: 11 (2.462 GHz) | Tx-Power: 0 dBm
Signal: 0 dBm | Noise: 0 dBm
Bitrate: 0.0 Mbit/s | Country: 00
Wireless network is enabled
Disable
Mode
Channel
Width
Operating frequency
N
3 (2422 MHz)
20 MHz
Transmit Power
20 dBm (100 mW)


Interface Configuration
General Setup
Wireless Security
ESSID
MERCURY_FE2A
Mode
Client
BSSID
8C:F2:28:FD:FE:2A
Network
ifmobile:
lan:
wan:
wan6:
wwan:
create:

- **Step 5)** Click the "**Save & Apply**" button to start the AP client.

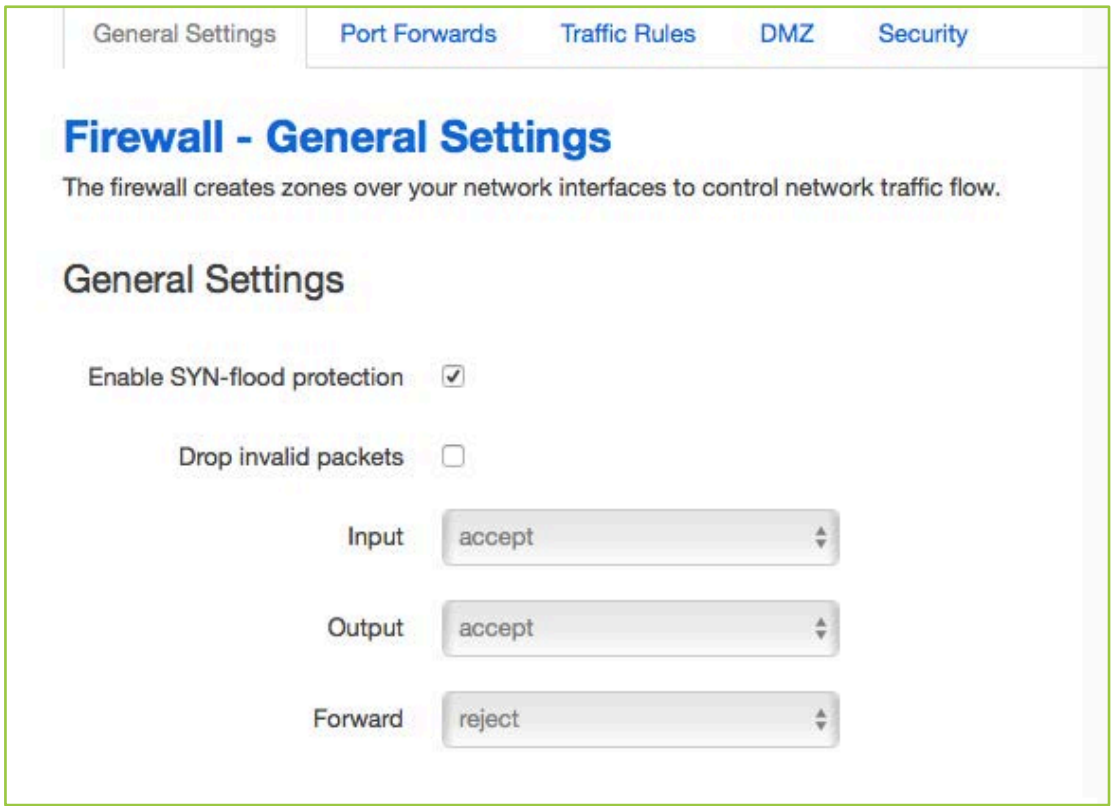
3.6.7 Interfaces Overview

Interfaces overview shows all interfaces status, including uptime, MAC-address, RX, TX and IP address.



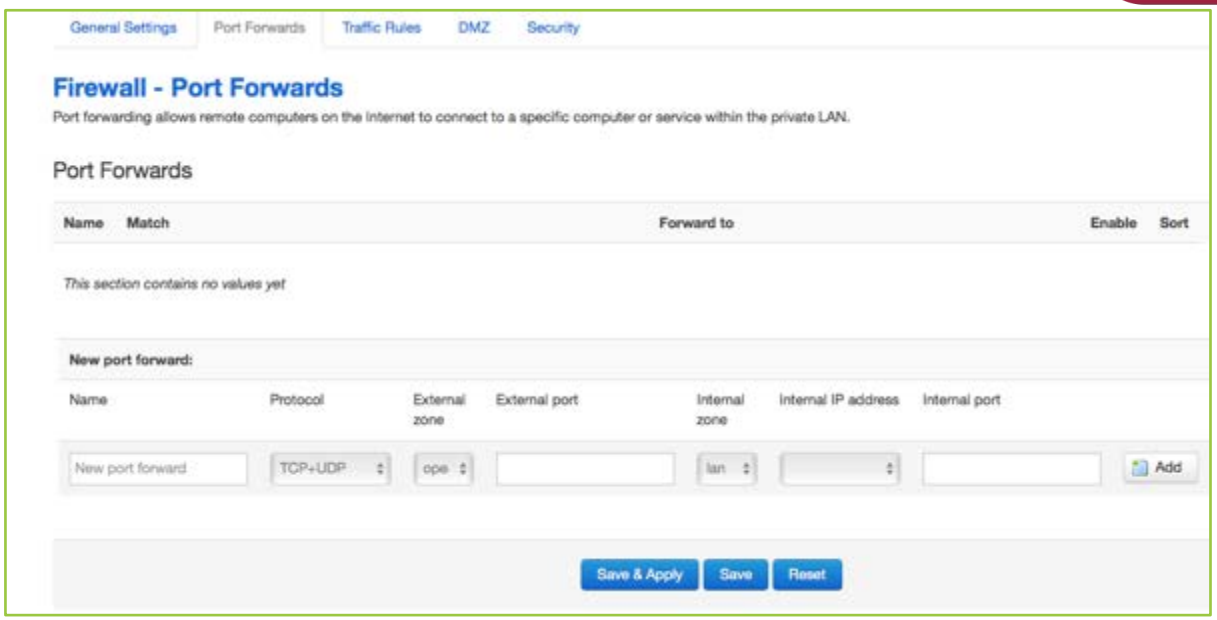
3.6.8 Firewall

3.6.8.1 General Settings



3.6.8.2 Port Forwards

This page includes the port forwards list and the add new port forwards rule functionality.

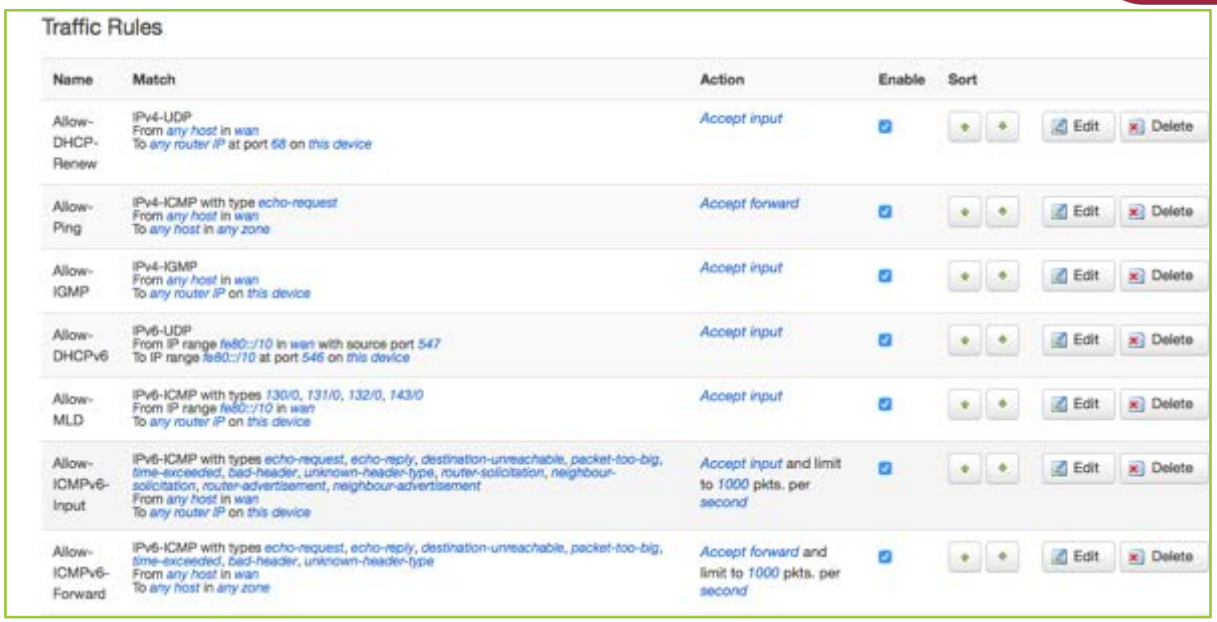


- **Name:** Port forward instance name.
- **Protocol:** TCP+UDP, UDP and TCP can be chosen.
- **External zone:** The recommended option is wan.
- **External port:** Match incoming traffic directed at the given destination port on this host.
- **Internal zone:** The recommended zone is lan.
- **Internal IP address**: Redirect matched incoming traffic to the specific host.
- **Internal port:** Redirect matched incoming traffic to the given port on the internal host.

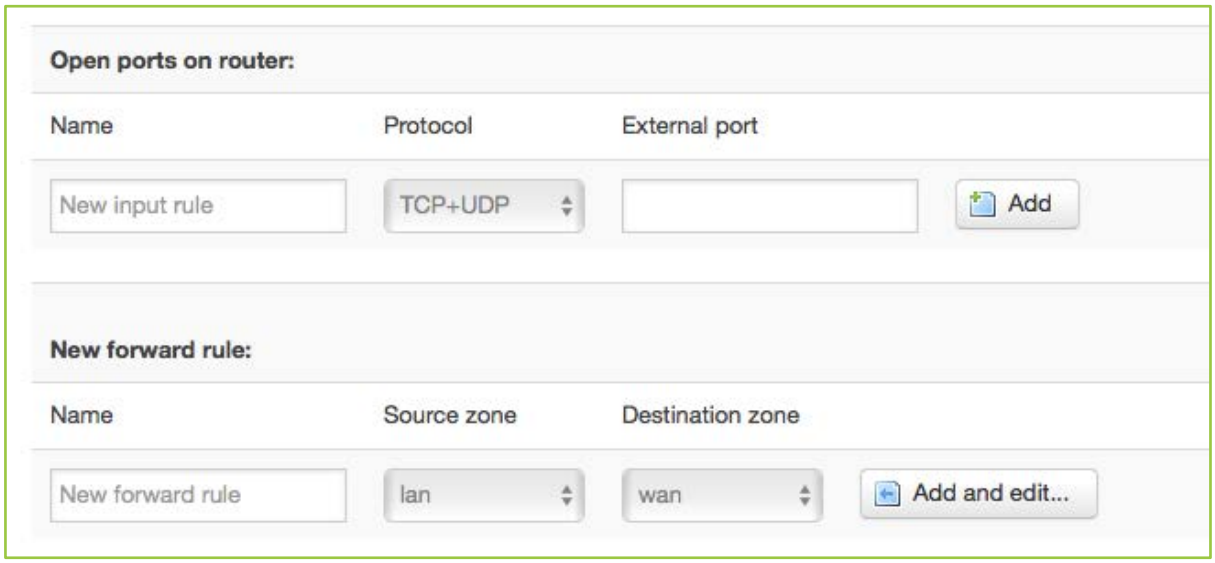
3.6.8.3 Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.
The traffic rules overview page content provides the following functionalities.

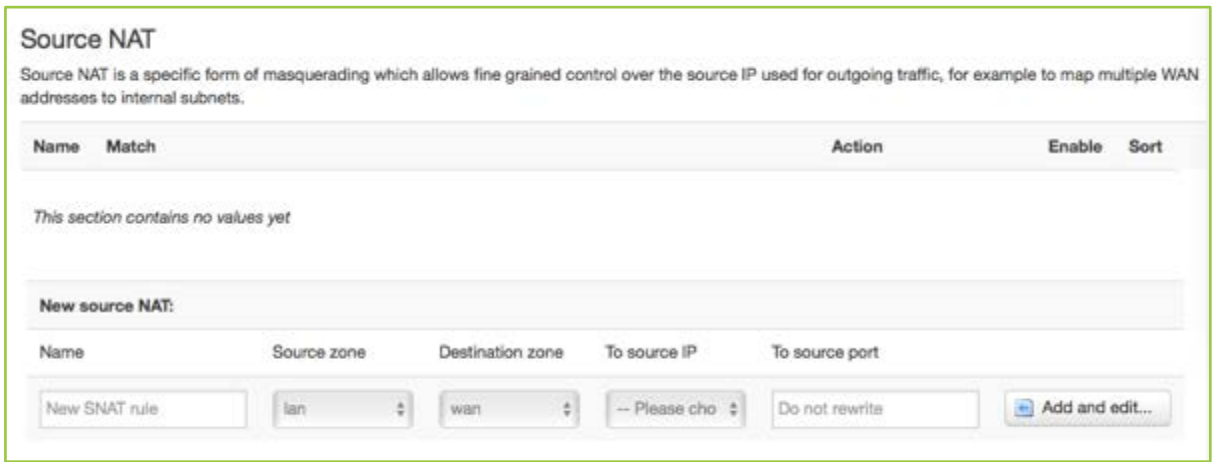
Traffic rules list:



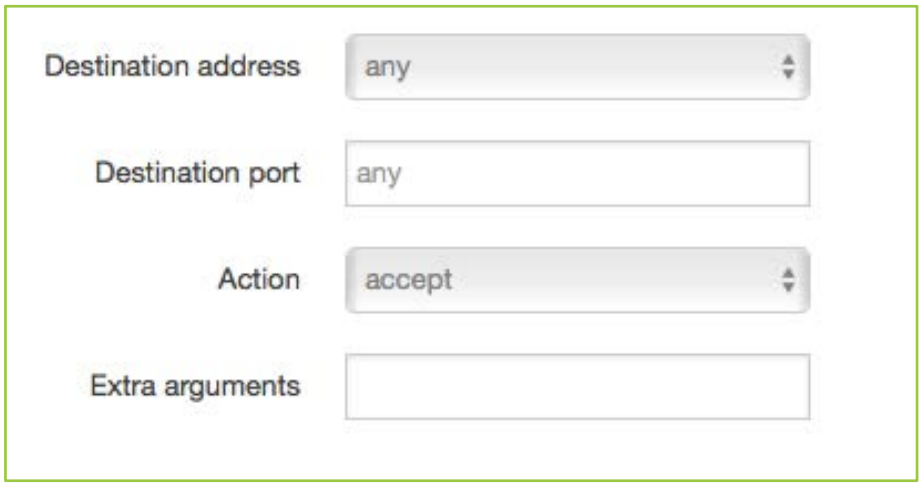
Open ports on the router and create new forward rules:



Source the NAT list and create the source NAT rule:

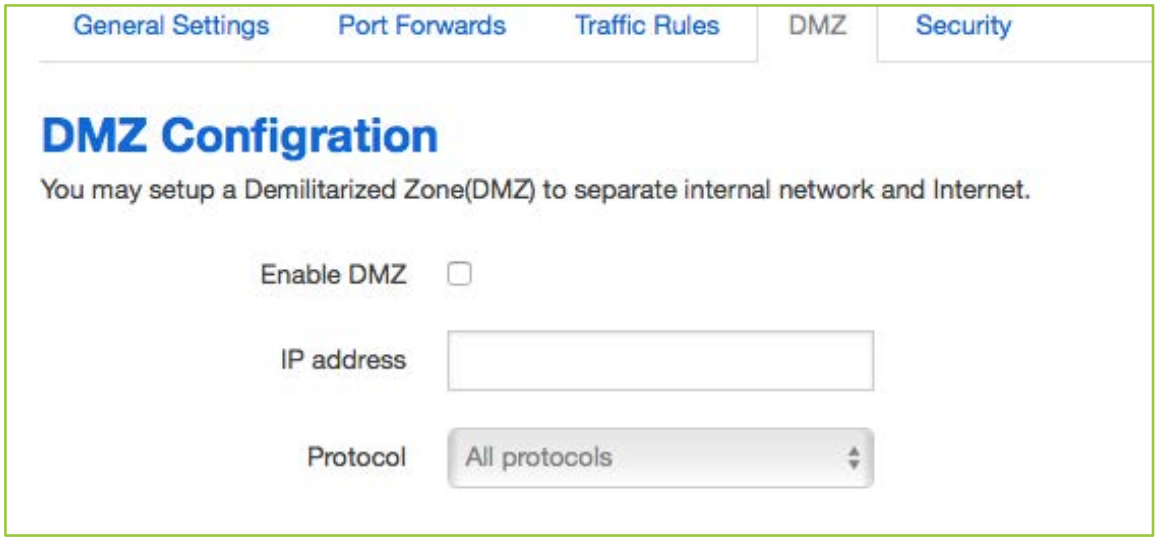


Traffic rule configuration page: This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.



- **Name:** Traffic rule entry name
- **Restrict to address family:** IPv4+IPv6, IPv4 and IPv6 can be selected. Specify the matched IP address family.
- **Protocol:** Specify the protocol matched in this rule. "Any" means any protocol is matched.
- **Source zone:** This is the zone that the traffic comes from.
- **Source MAC address:** Traffic rule checks if the incoming packet's source MAC address is matched.
- **Source address:** Traffic rule checks if the incoming packet's source IP address is matched.
- **Source port:** Traffic rule checks if the incoming packet's TCP/UDP port is matched.
- **Destination zone:** The zone that the traffic will go to.
- **Destination address:** Traffic rule checks if the incoming packet's destination IP address is matched.
- **Destination port:** Traffic rule checks if the incoming packet's TCP/UDP port is matched.
- **Action:** If traffic is matched, the system will handle traffic according to the Action (accept, drop, reject, don't track).
- **Extra argument:** Passes additional arguments to iptable, use with care!

3.6.8.4 DMZ

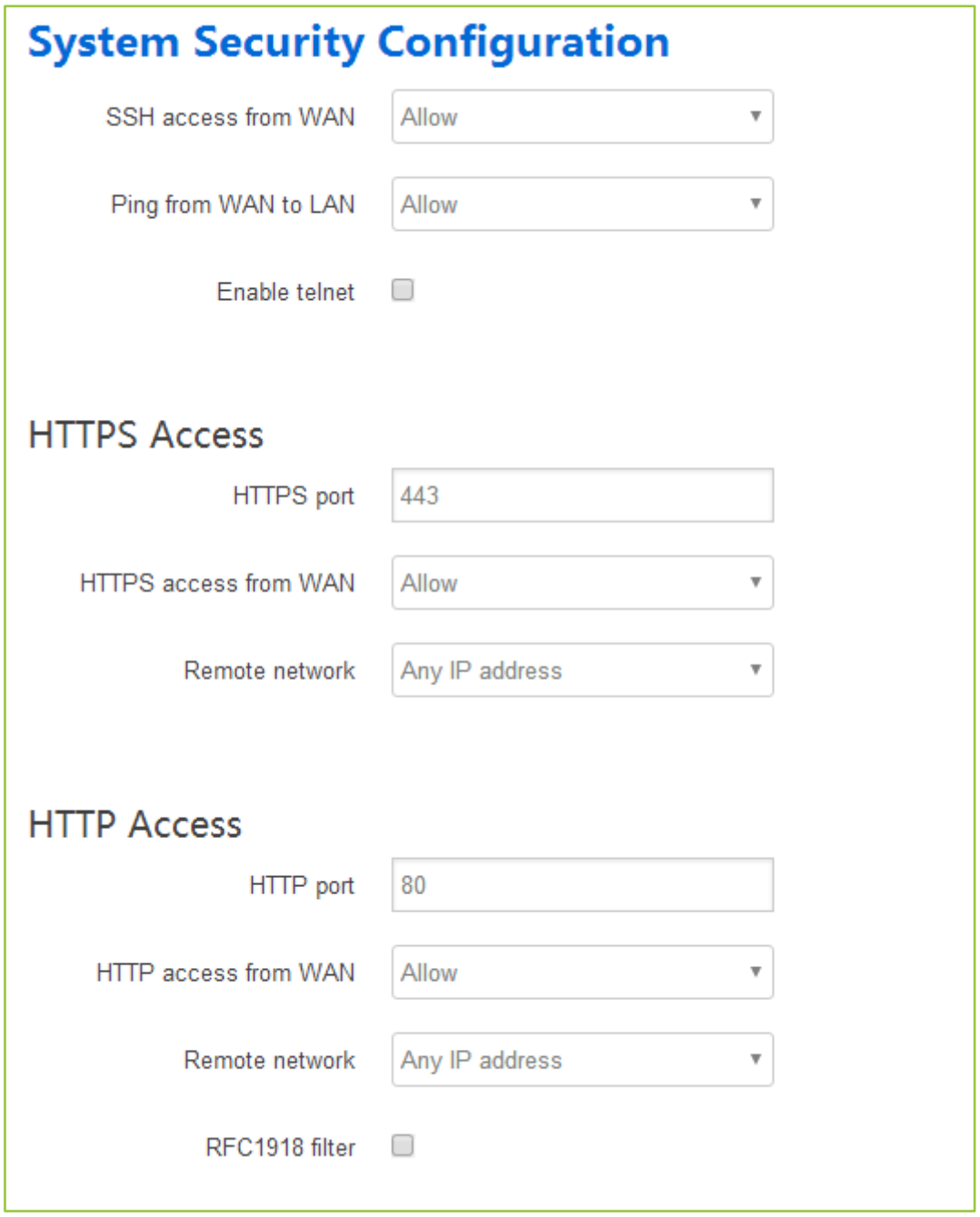


In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).

- **IP Address:** Please Enter the IP address of the computer which you want to set as DMZ host
- **Protocol:** All protocols, TCP+UDP, TCP, UDP.

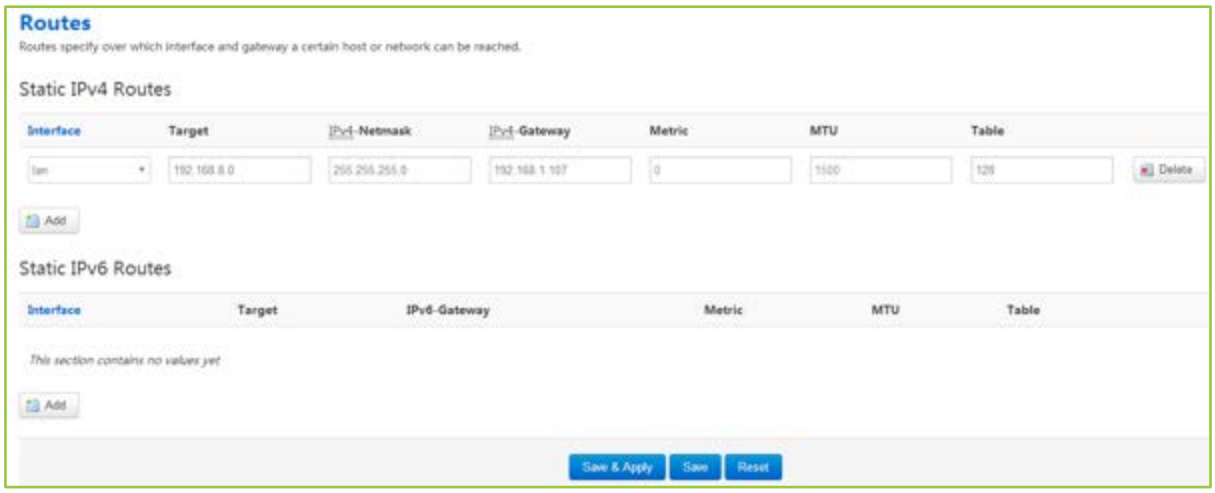
Note: When DMZ host is settled, the computer is completely exposed to the external network; the firewall will not influence this host.

3.6.8.5 Security



- **SSH access from WAN:** Allow or deny users access to the router from remote side.
- **Ping from WAN to LAN:** Allow or deny ping from remote side to internal LAN subnet.
- **Enable telnet:** Enable telnet connect. The default setting is disabled for security.
- **HTTPS port:** Set HTTPS port, the default port is 443.
- **HTTPS access from WAN:** Allow or deny access router web management page from remote side.
- **Remote network:** Any IP Address, Single IP address, Subnet.
- **IP address:** Fill a remote IP address that can access the router web management page.
- **Netmask:** 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the legal value is from 1 to 32.
- **HTTP port:** Set HTTP port, the default port is 80.
- **HTTP access from WAN:** Allow or deny access router web management page from remote side.
- **Remote network:** Any IP Address, Single IP address, Subnet.
- **IP address:** Fill a remote IP address that can access router web management page.
- **Netmask:** 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the legal value is from 1 to 32.
- **RFC1918 filter:** Reject requests from RFC1918 IPs to public server IPs

3.6.9 Static Routes

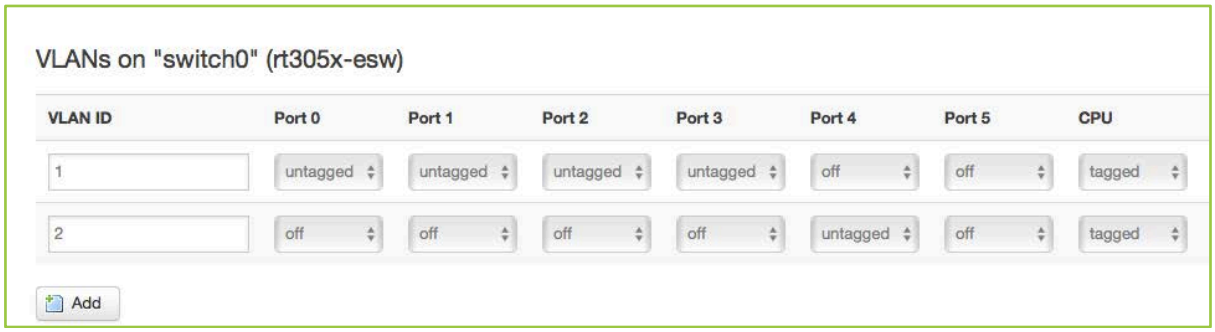


- **Interface:** You can choose the corresponding interface type.
- **Target:** The destination host IP or network.
- **IPv4-Netmask:** The destination IP mask.
- **IPv4-Gateway:** IP address of the next hop.
- **Metric:** Used by router to make routing decisions.
- **MTU:** Maximum transmission unit
- **Table:** The route table ID, the default value is 254, valid table ID 1-254.

  Notice:

  - Gateway and LAN IP of this router must belong to the same network segment.
  - If the destination IP address is the one of a host, and then the Netmask must be 255.255.255.255.
  - If the destination IP address is IP network segment, it must match with the Netmask. For example, if the destination IP is 10.0.0.0, and the Netmask is 255.0.0.0.

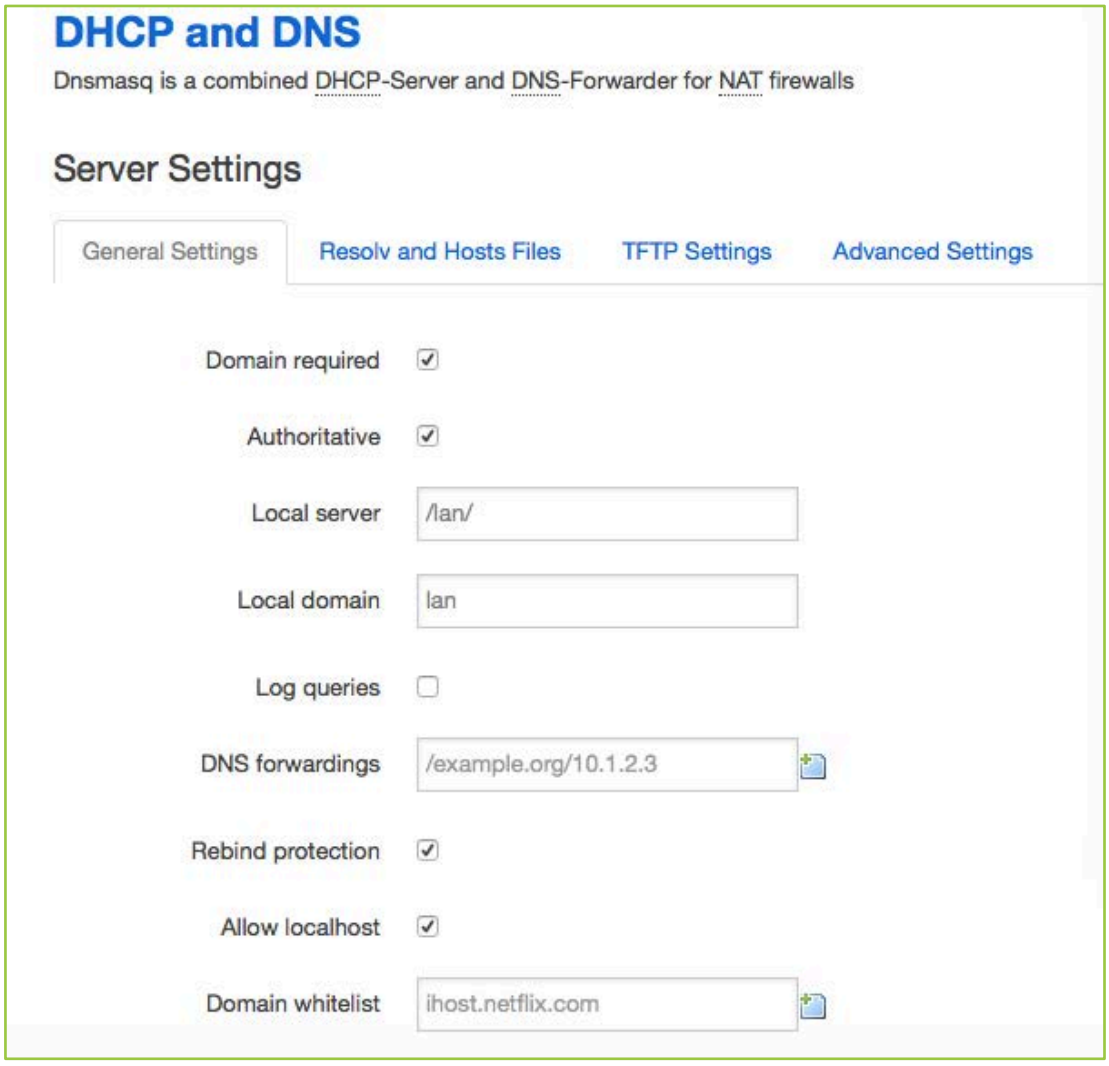
3.6.10 Switch



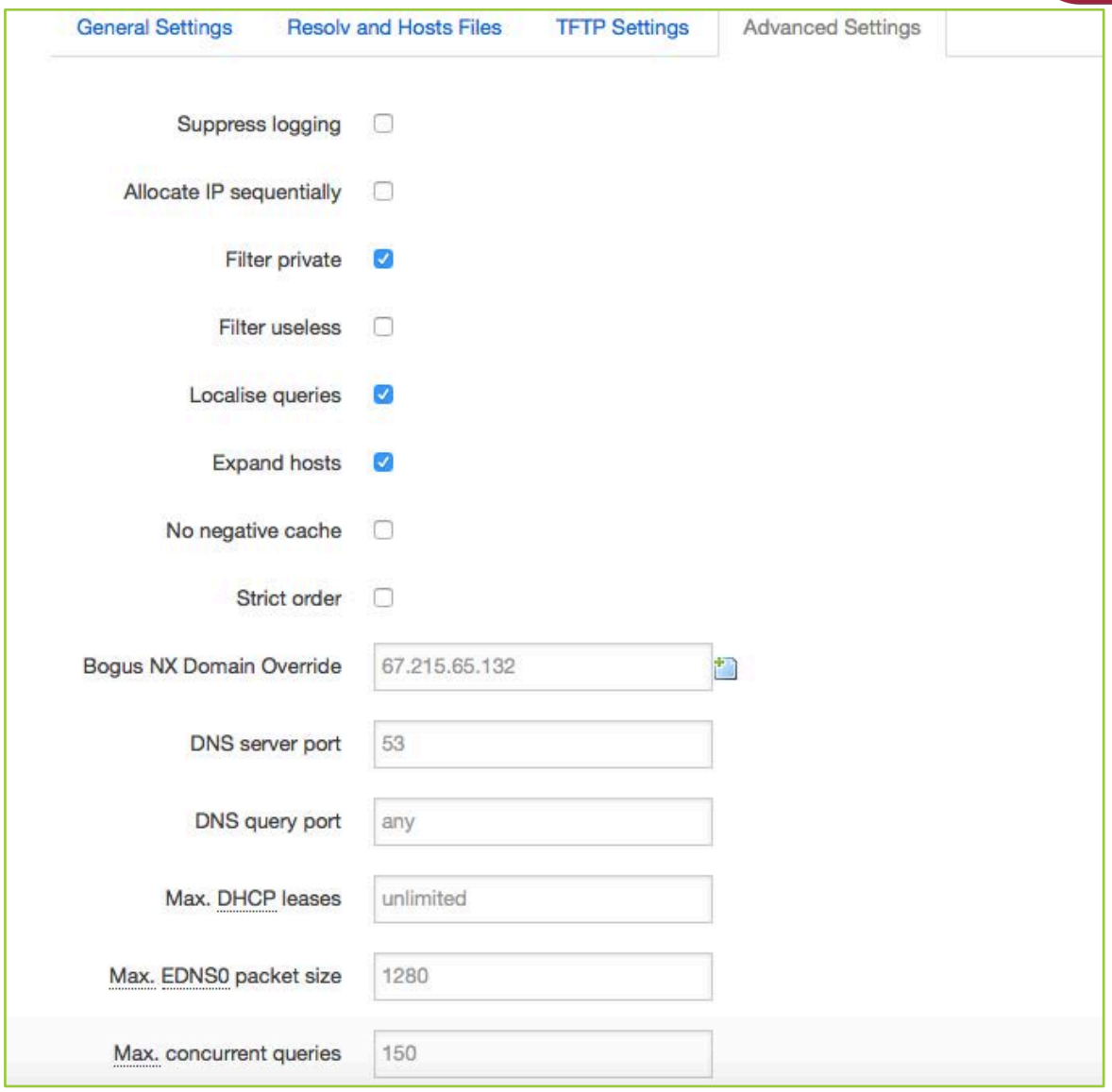
Note:

1. Port 4 is a Wired-WAN port, port 0, port 1, port 2, port 3 are LAN port.
2. **"Untagged"** means the Ethernet frame transmits from this port without VLAN tag.
3. **"Tagged"** means the Ethernet frame transmits from this port is with VLAN tag.
4. **"Off"** means this port does not belong to VLAN. For default setting, port 0 belongs to VLAN1, but not belong to VLAN 2.

3.6.11 DHCP and DNS



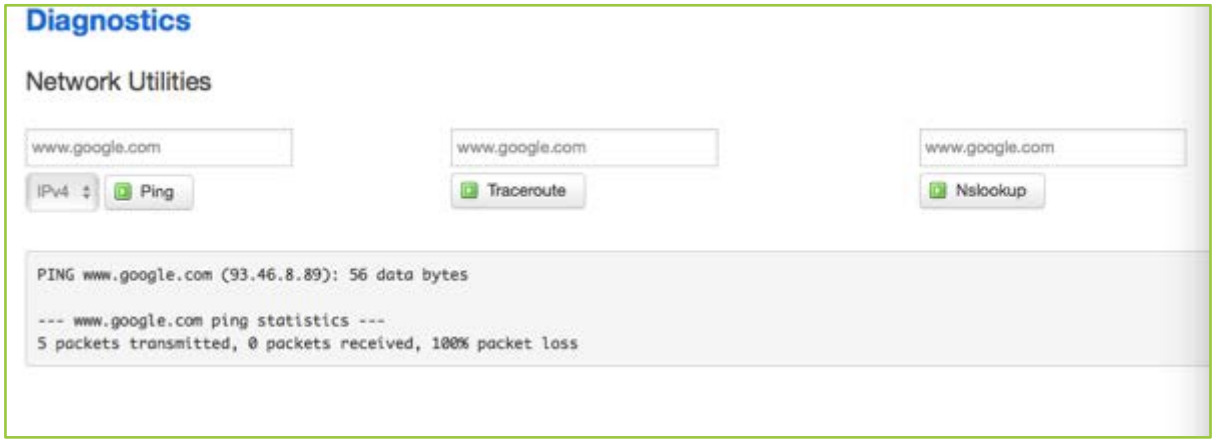
- **Domain required:** Don't forward DNS-requests without DNS-Name.
- **Authoritative:** This is the only DHCP on the local network.
- **Local server:** Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only.
- **Local domain:** Local domain suffix appended to DHCP names and hosts file entries.
- **Log queries**: Write received DNS requests to syslog.
- **DNS forwarding:** List of DNS servers to forward requests to.
- **Rebind protection**: Discard upstream RFC1918 responses.
- **Allow localhost:** Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services.
- **Domain whitelist:** List of domains to allow RFC1918 responses for.



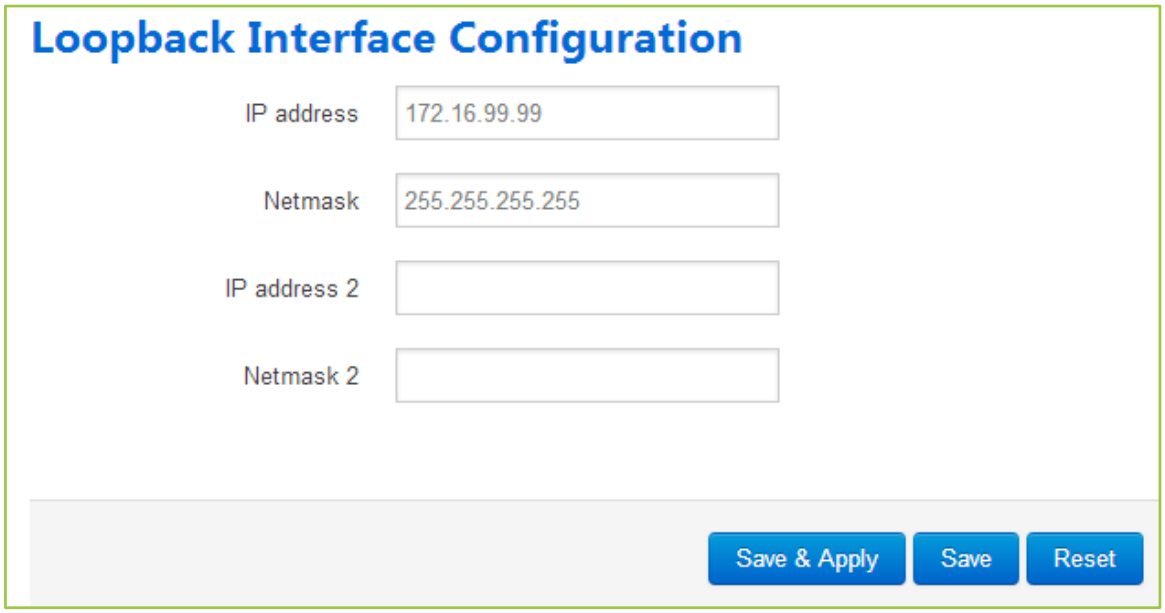
- **Suppress logging:** Suppress logging of the routine operation of these protocols.
- **Allocate IP sequentially:** Allocate IP addresses sequentially, starting from the lowest available address.
- **Filter private:** Do not forward reverse lookups for local networks.
- **Filter useless:** Do not forward requests that cannot be answered by public name servers.
- **Localize queries:** Localize hostname depending on the requesting subnet if multiple IPs are available.
- **Expand hosts:** Add local domain suffix to names served from hosts files.
- **No negative cache:** Do not cache negative replies, e.g. for not existing domains.
- **Strict order:** DNS servers will be queried in the order of the resolve file.
- **Bogus NX Domain Override:** List of hosts that supply bogus NX domain results.
- **DNS server port:** Listening port for inbound DNS queries
- **DNS query port:** Fixed source port for outbound DNS queries
- **Max DHCP leases:** Maximum allowed number of active DHCP leases
- **Max edns0 packet size:** Maximum allowed size of EDNS.0 UDP packets.
- **Max concurrent queries:** Maximum allowed number of concurrent DNS queries.

3.6.12 Diagnostics

- **Ping :** This is a tool that is used to test the reachability of a host on an Internet Protocol (IP) network.
- **Traceroute:** it is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.
- **Nslookup:** This is a network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
- For example if you want to ping www.google.com, type the target domain name or IP address, then click the "**Ping**" button. Wait a couple of seconds, then the result will be shown below.



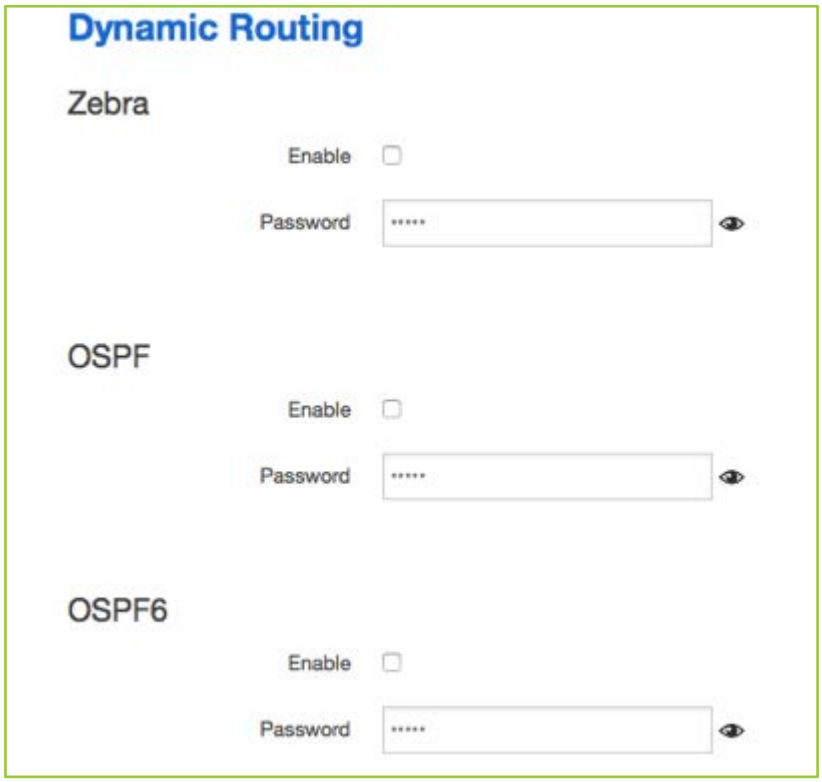
3.6.13 Loopback Interface

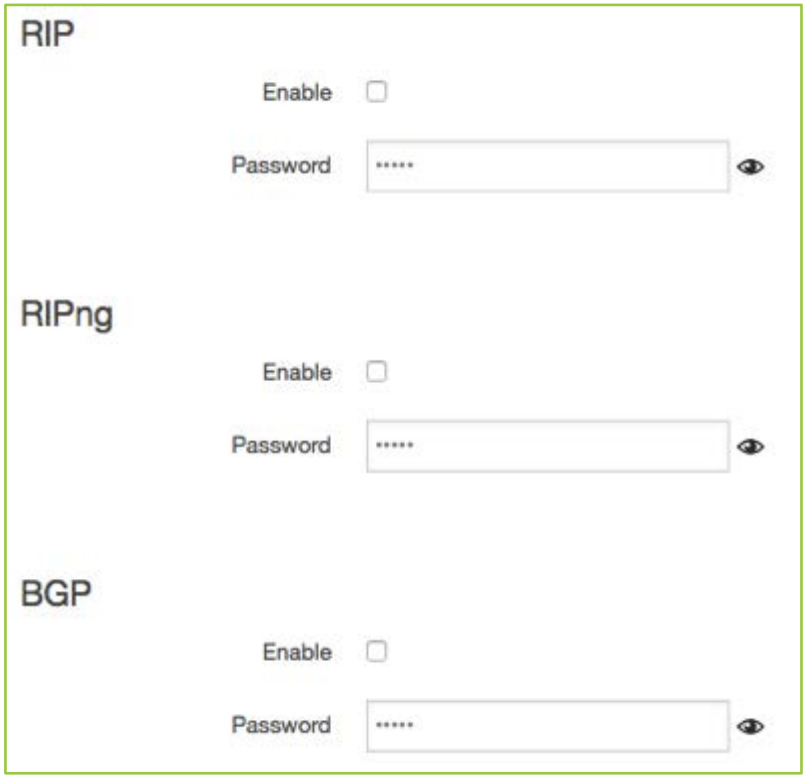


The default Loopback interface has the IP address 127.0.0.1, the user can change it here. The first IP address can be used in IPSec. The secondary can be used as management.

3.6.14 Dynamic Routing

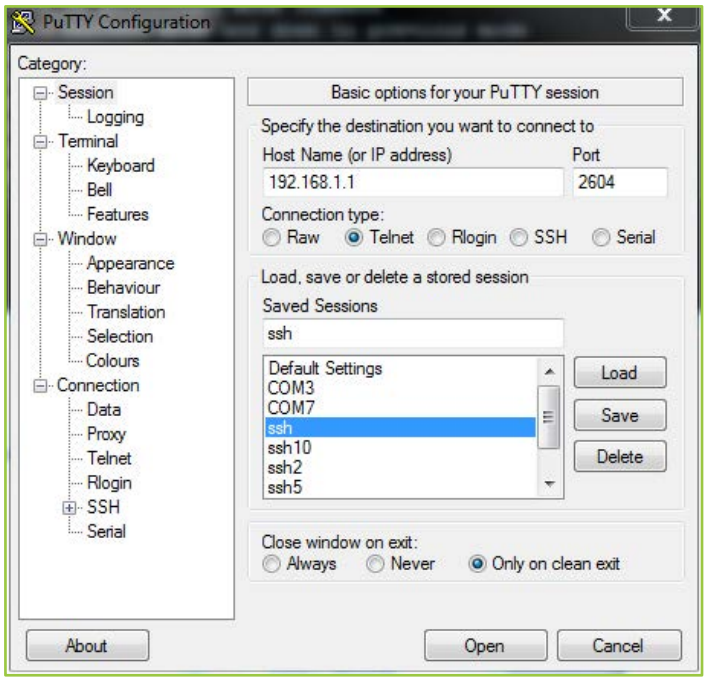
Dynamic Routing is implemented by quagga-0.99.22.4. Dynamic Routing services can be enabled here:


Dynamic Routing
Zebra
Enable
Password
OSPF
Enable
Password
OSPF6
Enable
Password


RIP
Enable
Password
RIPng
Enable
Password
BGP
Enable
Password

- **Zebra:** Zebra is an IP routing manager. Telnet port number is 2601.
- **OSPF:** Open Shortest Path First. Telnet port number is 2604.
- **OSPF6:** Open Shortest Path First for IPv6. Telnet port number is 2606.
- **RIP:** Routing Information Protocol. Telnet port number is 2602.
- **RIPng:** This is an IPv6 reincarnation of the RIP protocol. Telnet port number is 2603.
- **BGP:** Border Gateway Protocol. Telnet port number is 2605.

Note: How to configure these services? For example, the router's LAN IP is 192.168.10.1. If we want to configure OSPF, we need to set OSPF to "**Enable**" firstly, then open putty in windows:

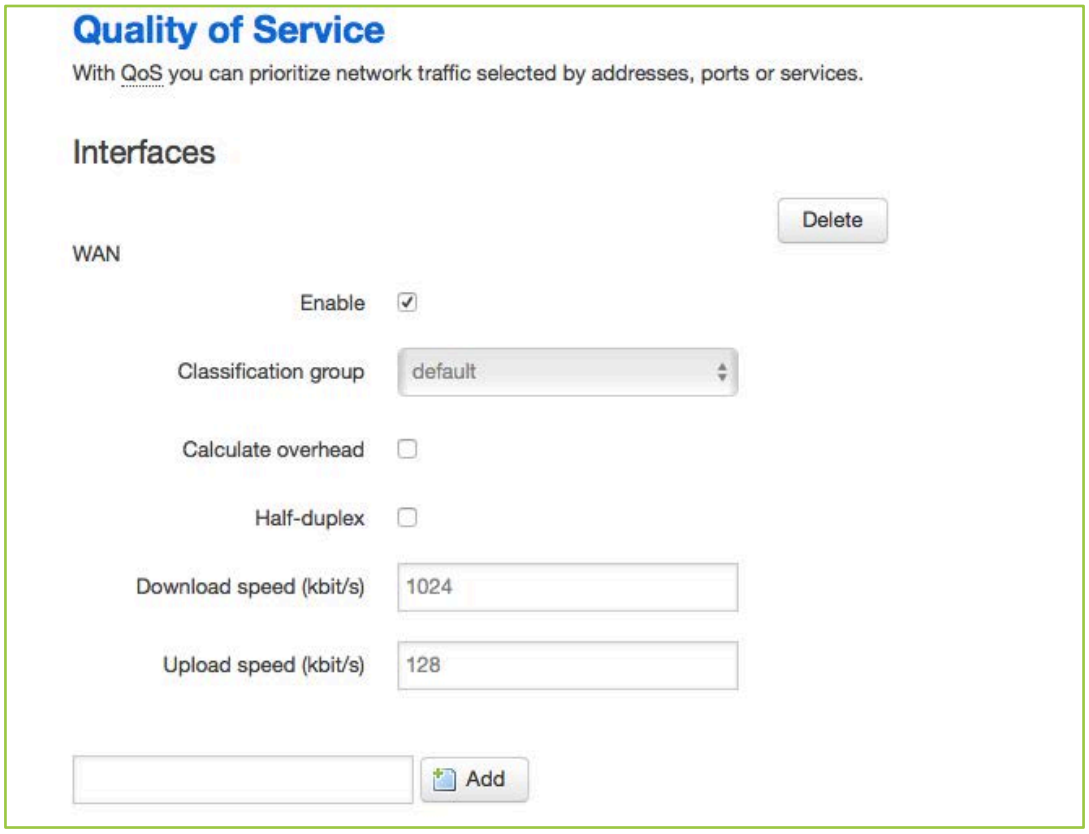


Input the password of OSPF. Then press the"**?**" for help.

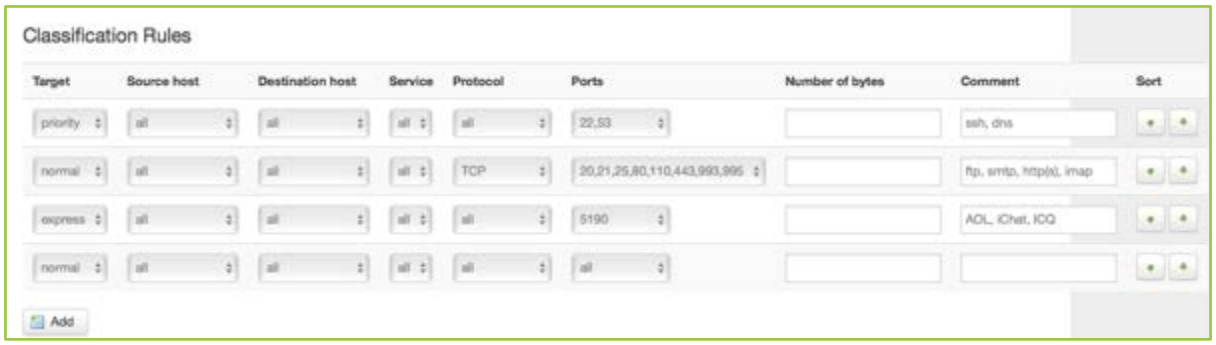
```
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

Password:
Cell_Router>
Cell_Router>
  echo      Echo a message back to the vty
  enable    Turn on privileged mode command
  exit      Exit current mode and down to previous mode
  help      Description of the interactive help system
  list      Print command list
  quit      Exit current mode and down to previous mode
  show      Show running system information
  terminal  Set terminal line parameters
  who       Display who is on vty
Cell_Router>
```

3.6.15 QoS

QoS (Quality of Service) can prioritize network traffic selected by addresses, ports or services.



- **Enable:** Enable QoS on this interface.
- **Classification group:** Specify class group used for this interface.
- **Calculate overhead**: Decrease upload and download ratio to prevent link saturation.
- **Download speed:** Download limit in kilobits/second.
- **Upload speed:** Upload limit in kilobits/second.

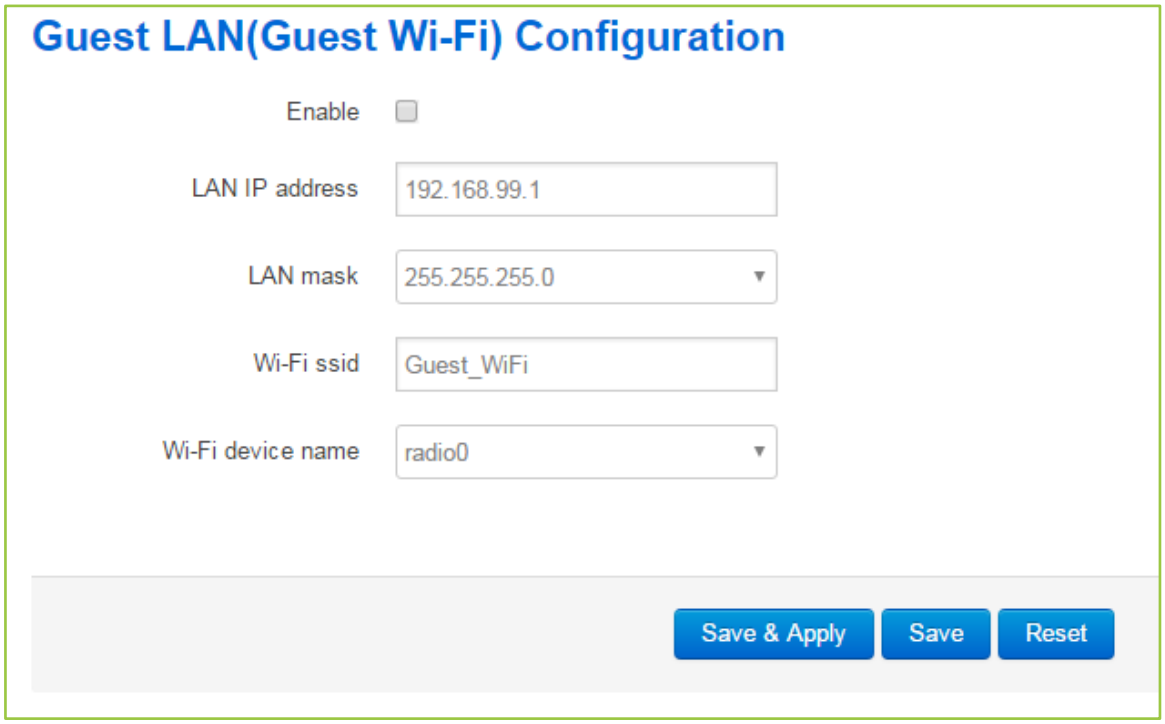


Each classification section defines one group of packets and which target (i.e. bucket) this group belongs to. All the packets share the bucket specified.

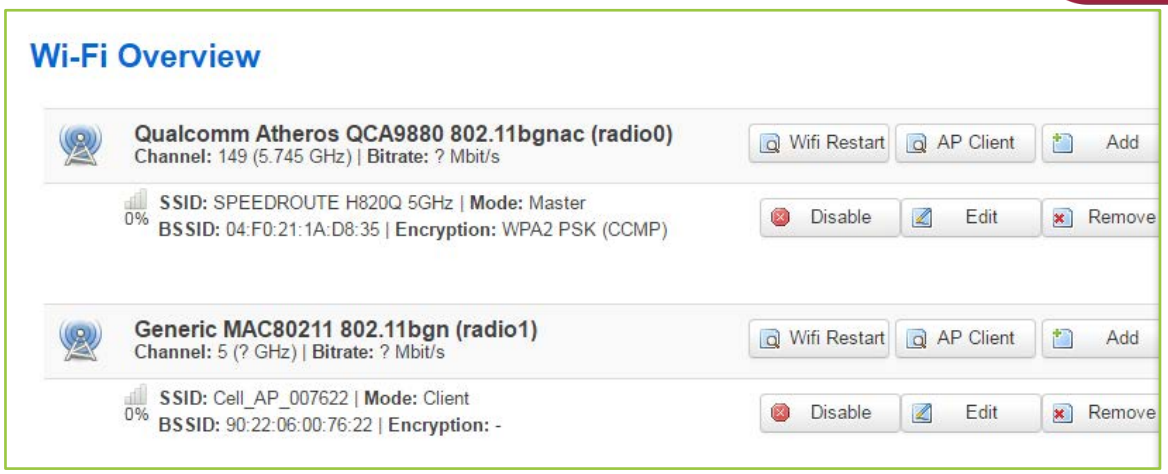
- **Target:** The four defaults are: priority, express, normal, low.
- **Source host:** Packets matching this source host(s) (single IP or in CIDR notation) belong to the bucket defined in the target.
- **Destination host:** Packets matching this destination host(s) (single IP or in CIDR notation) belong to the bucket defined in the target.
- **Protocol:** Packets matching this protocol belong to the bucket defined in the target.
- **Ports:** Packets matching this, belong to the bucket defined in the target. If more than 1 port is required, they must be separated by a comma.
- **Number of bytes:** Packets matching this, belong to the bucket defined in target.

3.6.16 Guest LAN (Guest Wi-Fi)

Guest Wi-Fi is a specific Wi-Fi that can only access internet bots not the local LAN.



- **Enable:** Enable Guest Wi-Fi.
- **LAN IP address:** This LAN IP address must be different than the LAN interface IP address.
- **LAN mask:** Packets matching this destination host(s) (single IP or in CIDR notation) belong to the bucket defined in the target。
- **Wi-Fi ssid**: The ssid of the guest Wi-Fi.
- **Wi-Fi device name:** Choose one Wi-Fi device to carry the Guest Wi-Fi, the available device name is radio0 and radio1. Check the Wi-Fi overview page for the device name. for example:


Wi-Fi Overview
Qualcomm Atheros QCA9880 802.11bgnac (radio0)
Channel: 149 (5.745 GHz) | Bitrate: ? Mbit/s
Wifi Restart
AP Client
Add
0%
SSID: SPEEDROUTE H820Q 5GHz | Mode: Master
BSSID: 04:F0:21:1A:D8:35 | Encryption: WPA2 PSK (CCMP)
Disable
Edit
Remove
Generic MAC80211 802.11bgn (radio1)
Channel: 5 (? GHz) | Bitrate: ? Mbit/s
Wifi Restart
AP Client
Add
0%
SSID: Cell_AP_007622 | Mode: Client
BSSID: 90:22:06:00:76:22 | Encryption: -
Disable
Edit
Remove