Connection #1 Phase 1

Mode	○ Disable ● Enable
Name	
Protocol	IKEv1
Aggressive mode	Disable
Auth Type	RSA
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Host	
Local ID	ID#1: remote.ipsec (RSA)
Remote Host	10.0.0.1
Remote ID	<empty> (allow any)

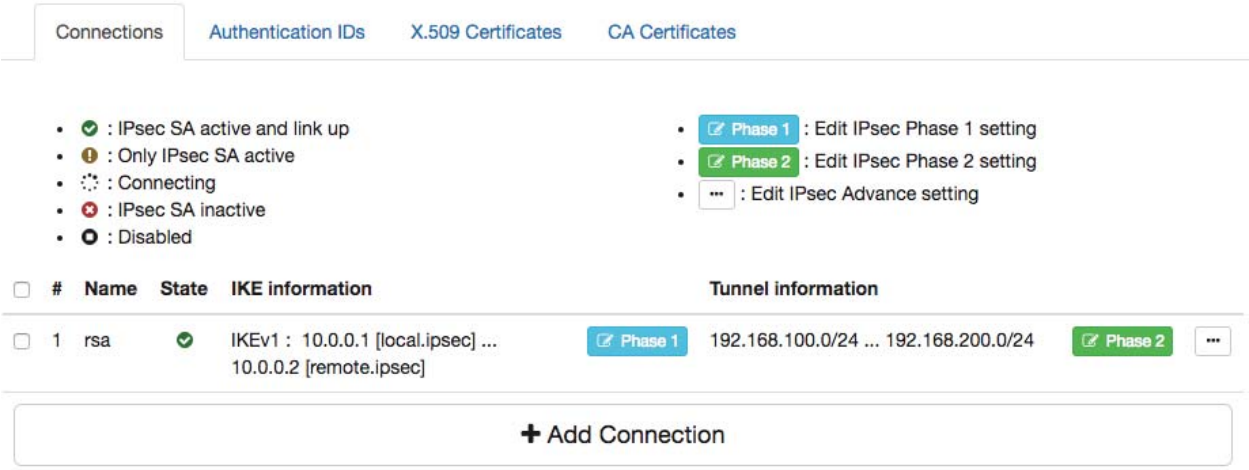
Back Save

Connection #1 Phase 2

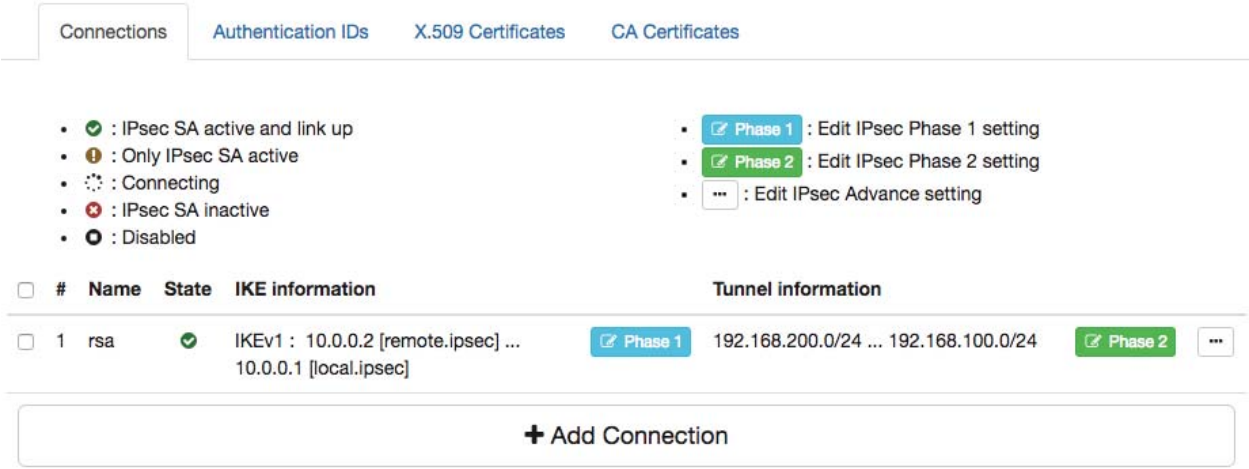
Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Subnet	192.168.200.0/24
Remote Subnet	192.168.100.0/24
Service	Any

Back Save

- **IPsec Net-to-Net with RSA authentication result**
  - Server



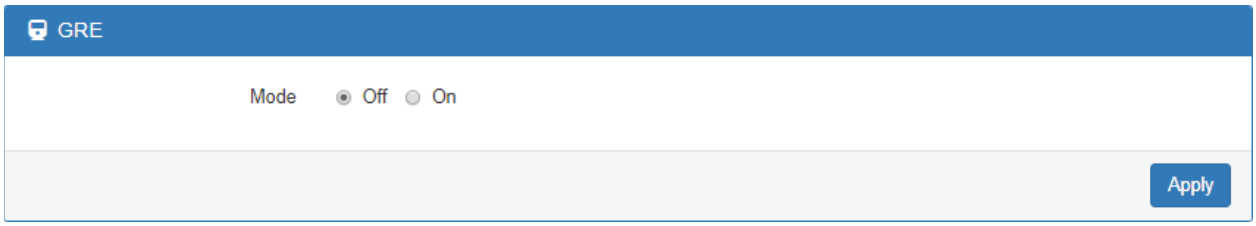
  - Client



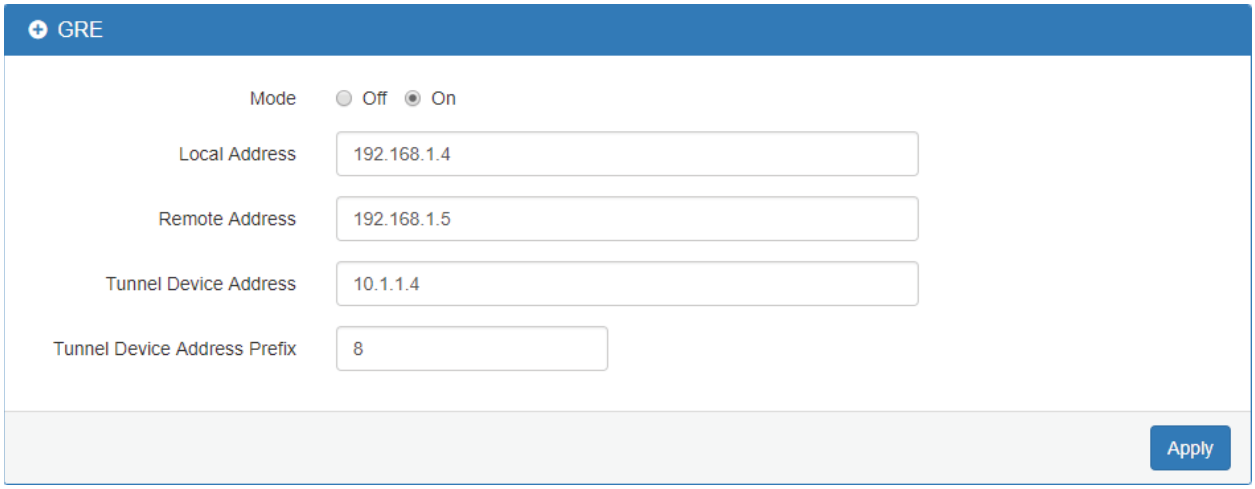
11.3 VPN > GRE

This section allows you to set **GRE configuration**. The default mode is off.

Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.



The GRE Mode is on.

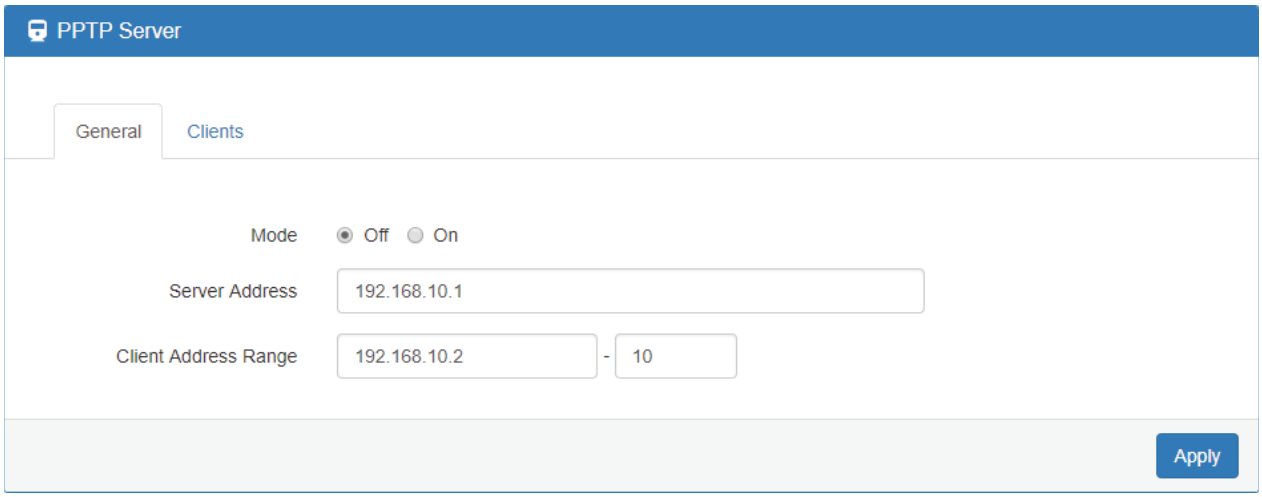


VPN > GRE	
Item	**Description**
Mode	Select from Off or On to enable GRE.
Local Address	Set local address of the GRE tunnel.
Remote Address	Set remote address of the GRE tunnel.
Tunnel Device Address	Set IP address of this GRE tunnel device.
Tunnel Device Address Prefix	Set Prefix of the Tunnel Device Address.

11.4 VPN > PPTP Server

This section provides 2 sub configurations, including General Configuration and Clients Configuration.

(1) General Configuration



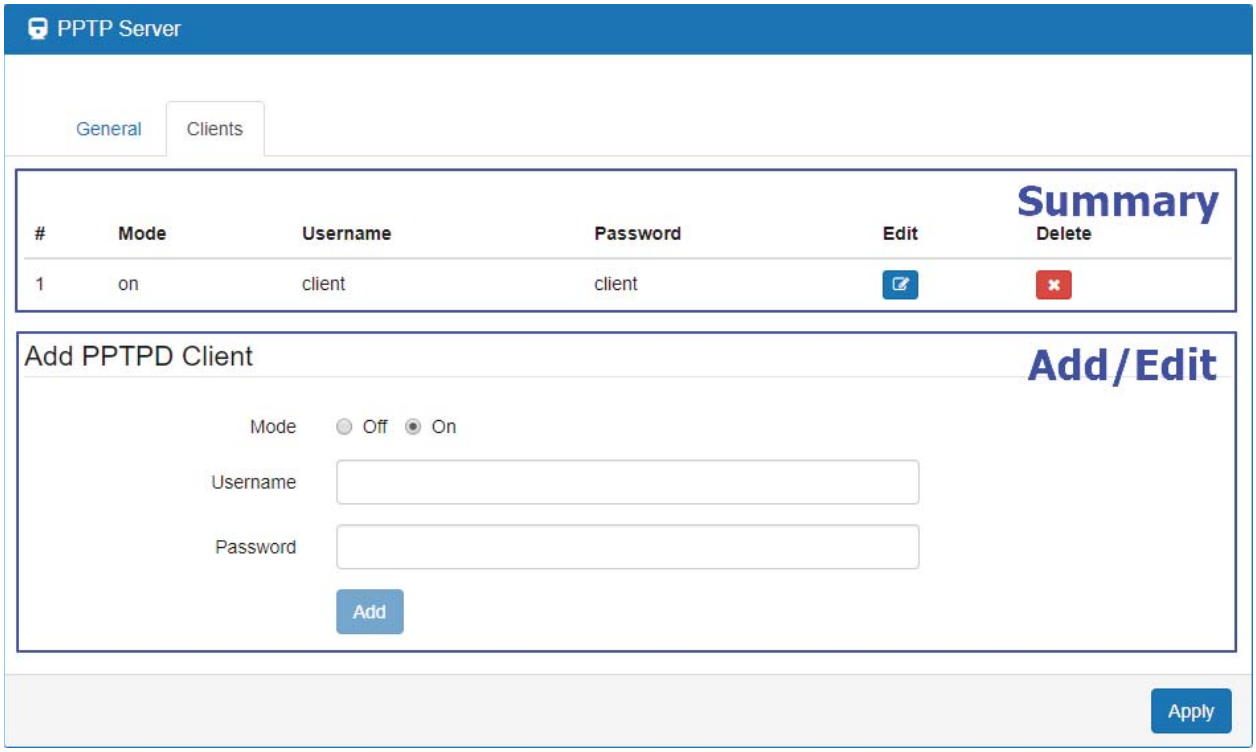
VPN > PPTP Server > General	
Item	**Description**
Mode	Select from Off or On to enable PPTP Server.
Server Address	IP addresses to be used at the local end of the tunneled PPP links between the server and the client.
Client Address Range	A list of IP addresses to assign to remote PPTP clients.

(2) Clients Configuration

There are two parts for Clients configuration.

- Summary part: User can delete and edit the existed PPTP clients.
- Add/Edit part:

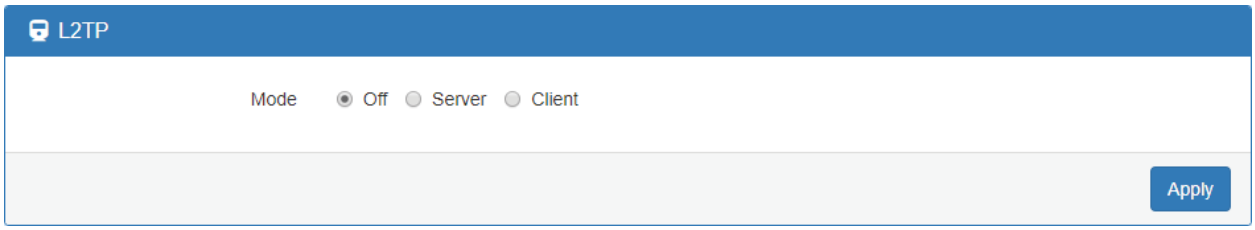
VPN > PPTP Server > Clients	
Item	**Description**
Mode	Select from Off or On to set the client setting.
Username	The username of this client.
Password	The password of this client.


PPTP Server
General
Clients
Summary
Mode Username Password Edit Delete
1 on client client
Add PPTPD Client
Add/Edit
Mode Off On
Username
Password
Add
Apply

11.5 VPN > L2TP

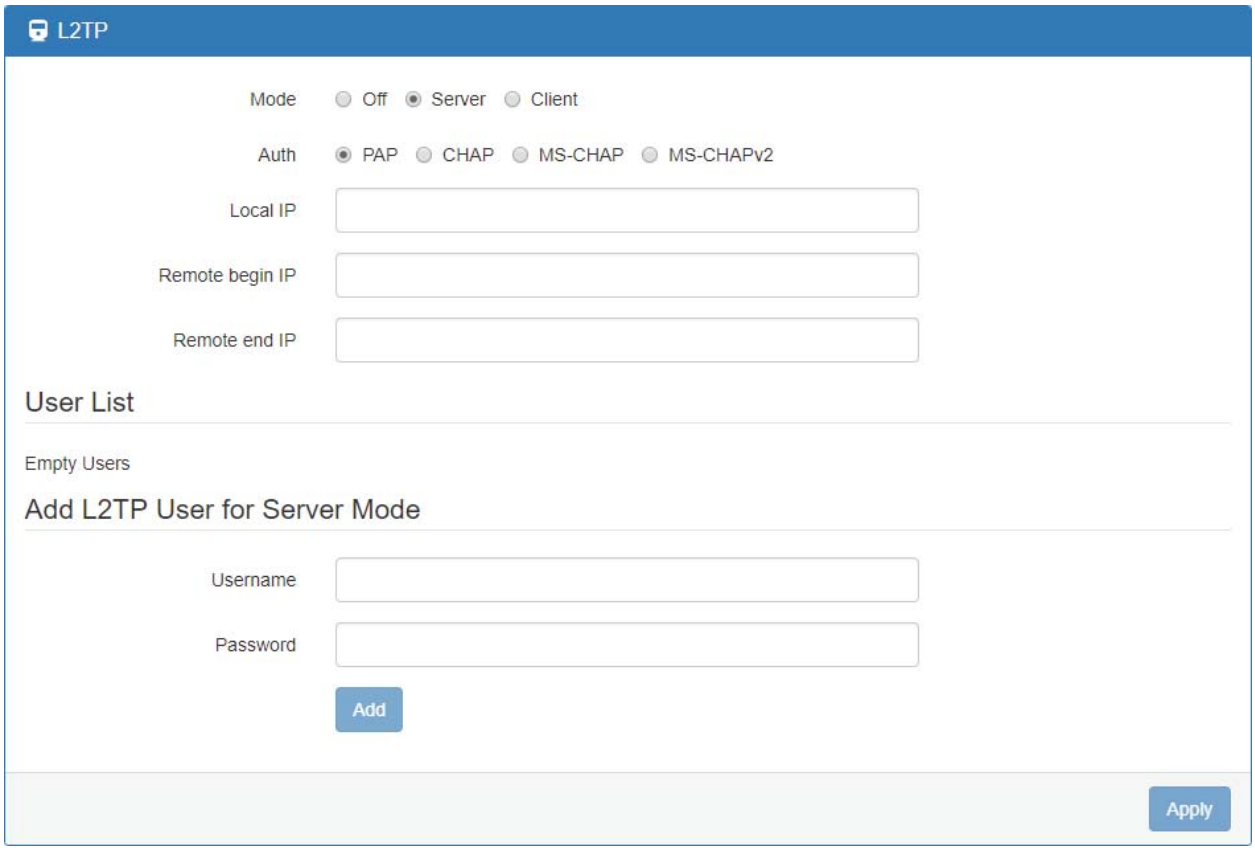
This section allows you to set up L2TP and provides three modes for configuration, including Off, Server, and Client Mode.

(1) General Mode: The default mode is Off as shown in the following interface.



(2) Server Mode:

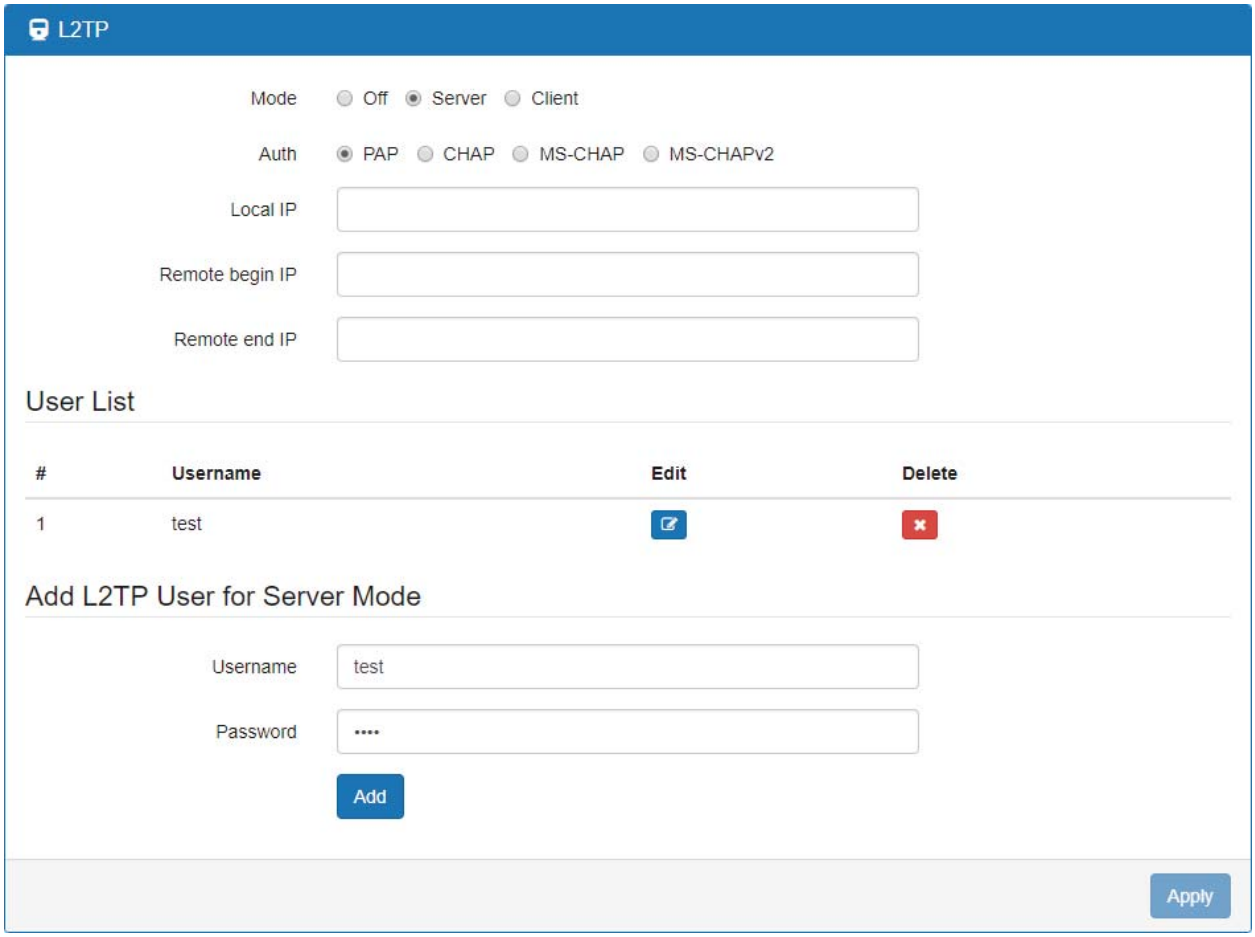
Choose the Server mode and the interface will be changed as below.



VPN> L2TP > Server Mode	
Item	**Description**
Mode	Select from Off or On to set the client setting.
Auth	The authentication method for L2TP connection. Available options: PAP, CHAP, MS-CHAP, MS-CHAPv2
Local IP	The virtual IP for L2TP server.
Remote begin IP	The begin address of L2TP client's IP pool.
Remote end IP	The end address of L2TP client's IP pool.
Username	The L2TP client's username. Could be used to add the newly client or update existed client.

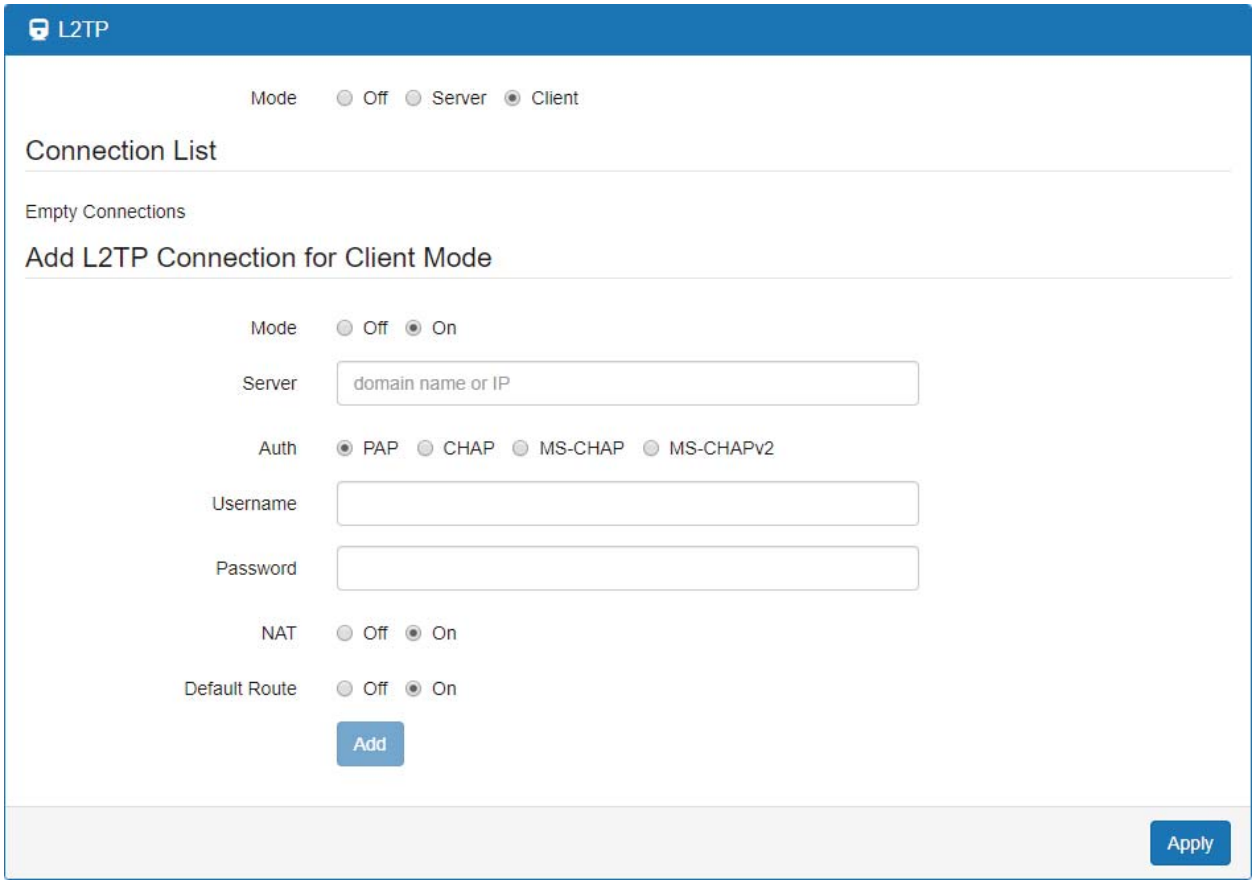
Password	The L2TP client's password. Could be used to add the newly client or update existed client.

Fill in the username and password and click the Add button, you can create the L2TP client and manage them under server mode.



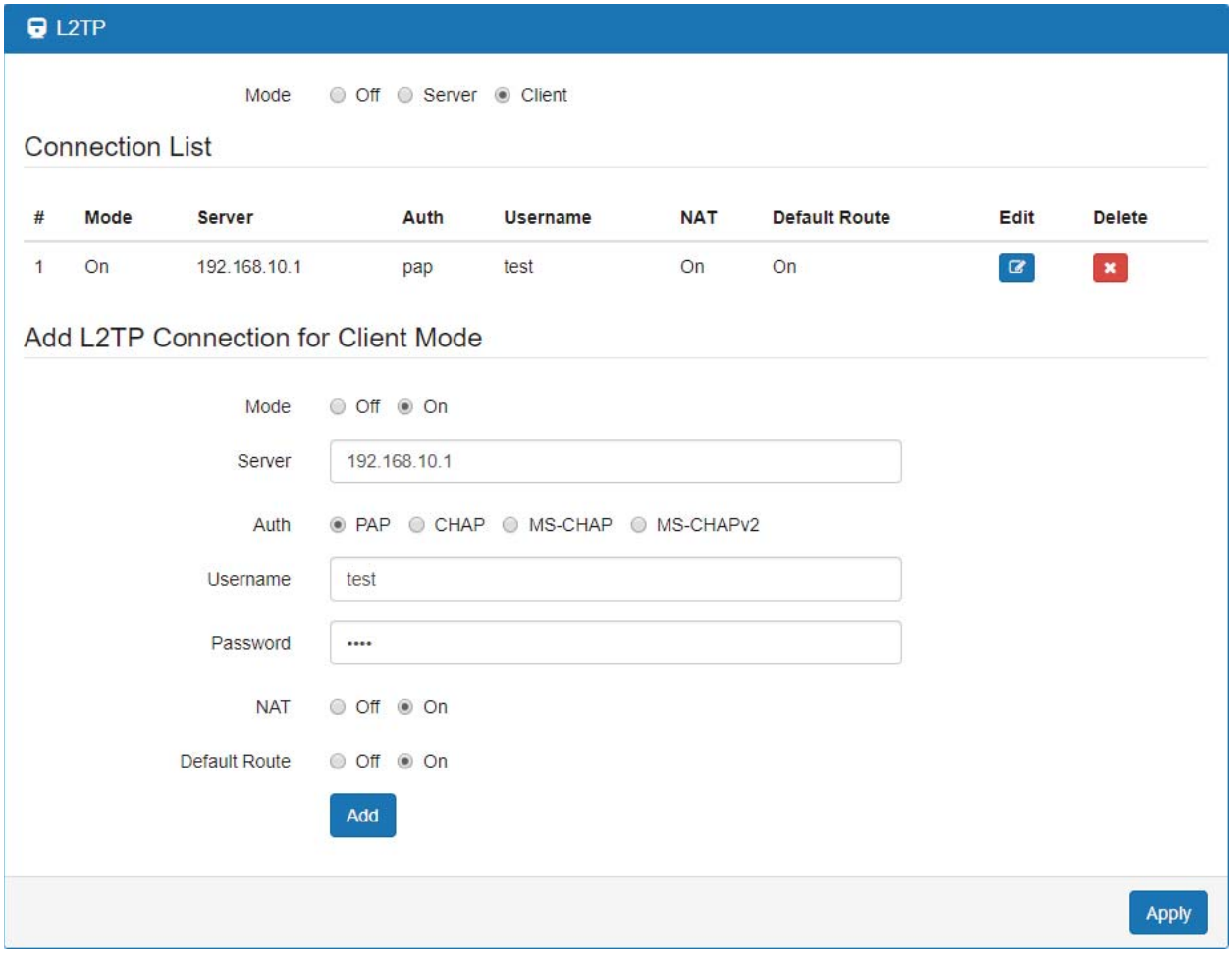
(3) Client Mode:

Choose the Client mode and the interface will be changed as below.



VPN> L2TP > Client Mode	
Item	**Description**
Mode	Turn on/off this L2TP connection
Server	The L2TP server address or hostname.
Auth	The authentication method for L2TP connection. Should same as L2TP server's auth type.
Username	The username for L2TP authentication.
Password	The password for L2TP authentication.
NAT	Turn on to translate the LAN subnet IP to L2TP virtual IP.
Default route	Turn on to redirect all traffic to L2TP tunnel.

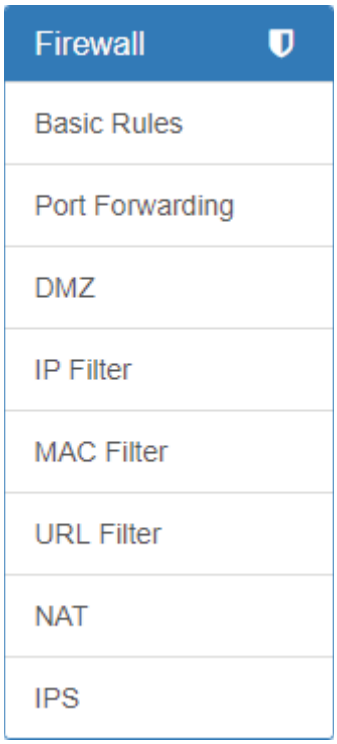
Fill in the required parameters and click the Add button to create the L2TP connection and manage the L2TP connection under client mode.



Click the button and edit the parameters to update the L2TP connection.

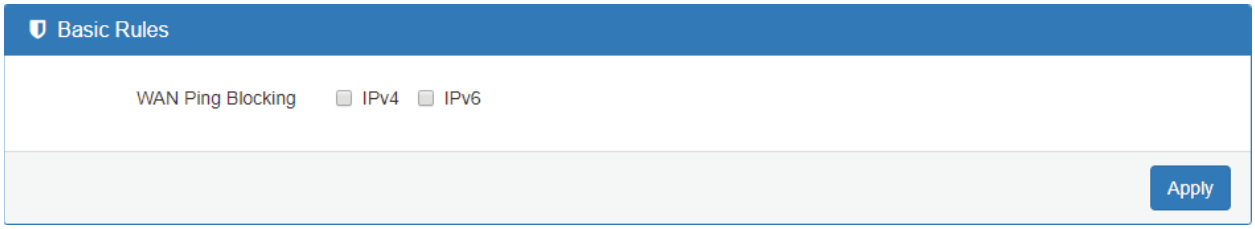
12 Configuration > Firewall

This section allows you to configure Basic Rules, Port Forwarding, DMZ, IP Filter, MAC Filter, URL Filter, NAT and IPS.



12.1 Firewall > Basic Rules

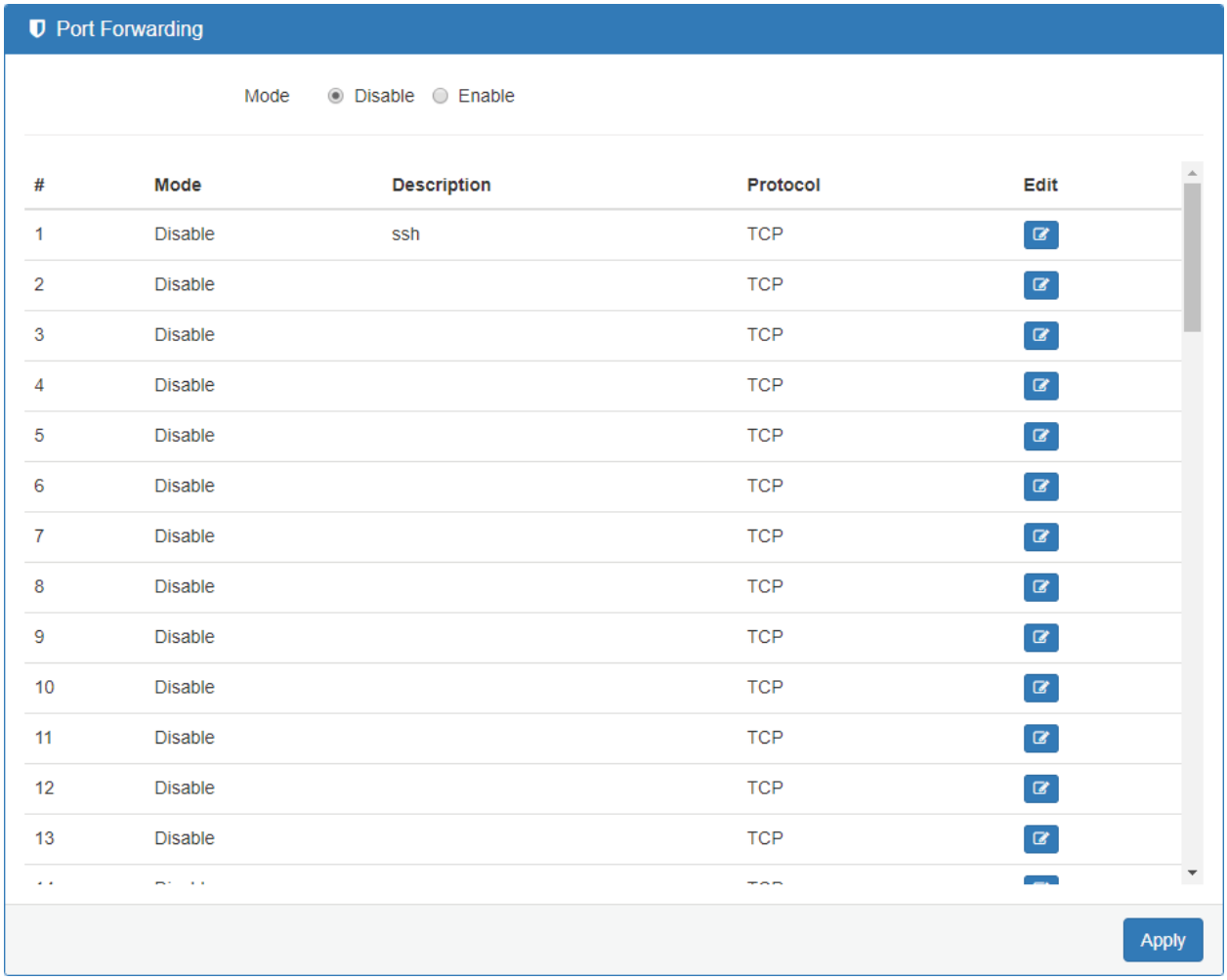
This section allows you to set the Basic Rules configuration.



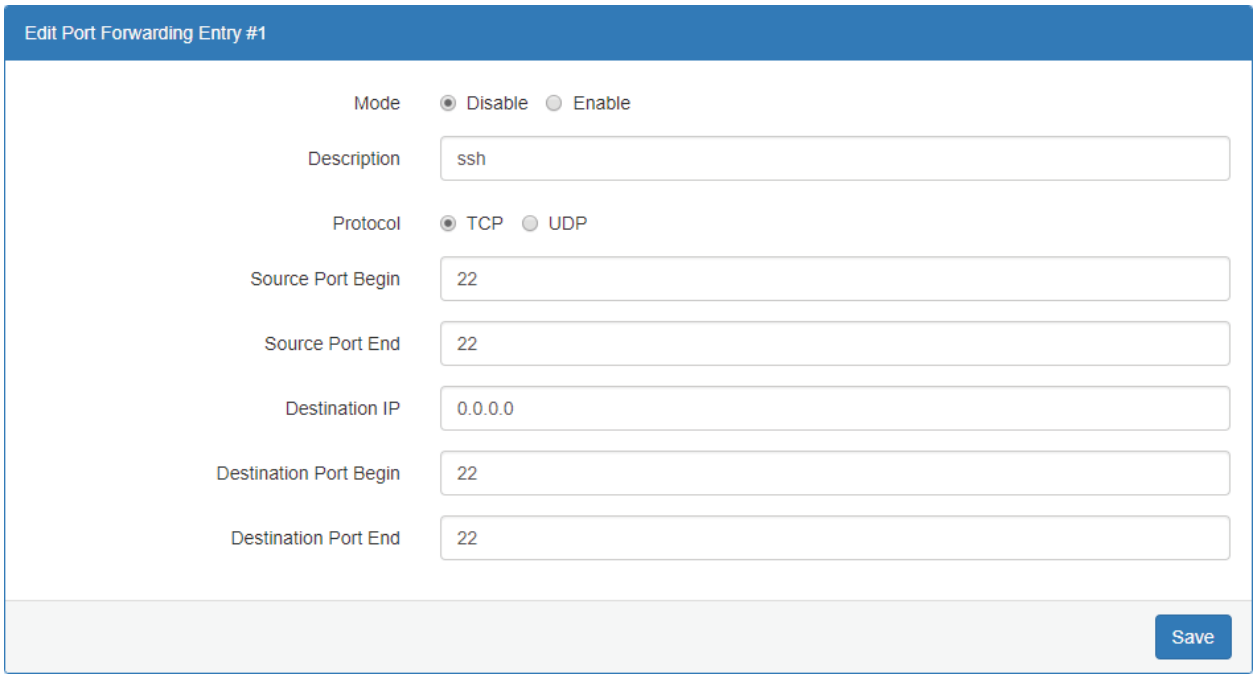
Firewall > Basic Rules	
Item	**Description**
WAN Ping Blocking	Check IPv4 or IPv6 for blocking

12.2 Firewall > Port Forwarding

This section allows you to set up **Port Forwarding** and click edit button to configure.



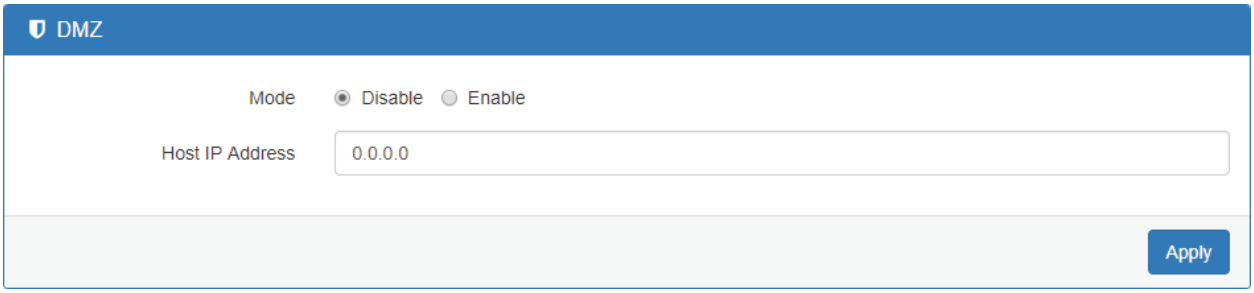
#	Mode	Description	Protocol	Edit
1	Disable	ssh	TCP	
2	Disable		TCP	
3	Disable		TCP	
4	Disable		TCP	
5	Disable		TCP	
6	Disable		TCP	
7	Disable		TCP	
8	Disable		TCP	
9	Disable		TCP	
10	Disable		TCP	
11	Disable		TCP	
12	Disable		TCP	
13	Disable		TCP	



Firewall > Port Forwarding	
Item	**Description**
Mode	Turn on/off Port Forwarding to select Disable or Enable. The default is Disable.
Description	Descript the name of Port Forwarding.
Protocol	Select from UDP or TCP Client which depends on the application.
Source Port Begin	Fill in the beginning of source port.
Source Port End	Fill in the end of source port.
Destination IP	Fill in the current private destination IP.
Destination Port Begin	Fill in the beginning of private destination port.
Destination Port End	Fill in the end of private destination port.

12.3 Firewall > DMZ

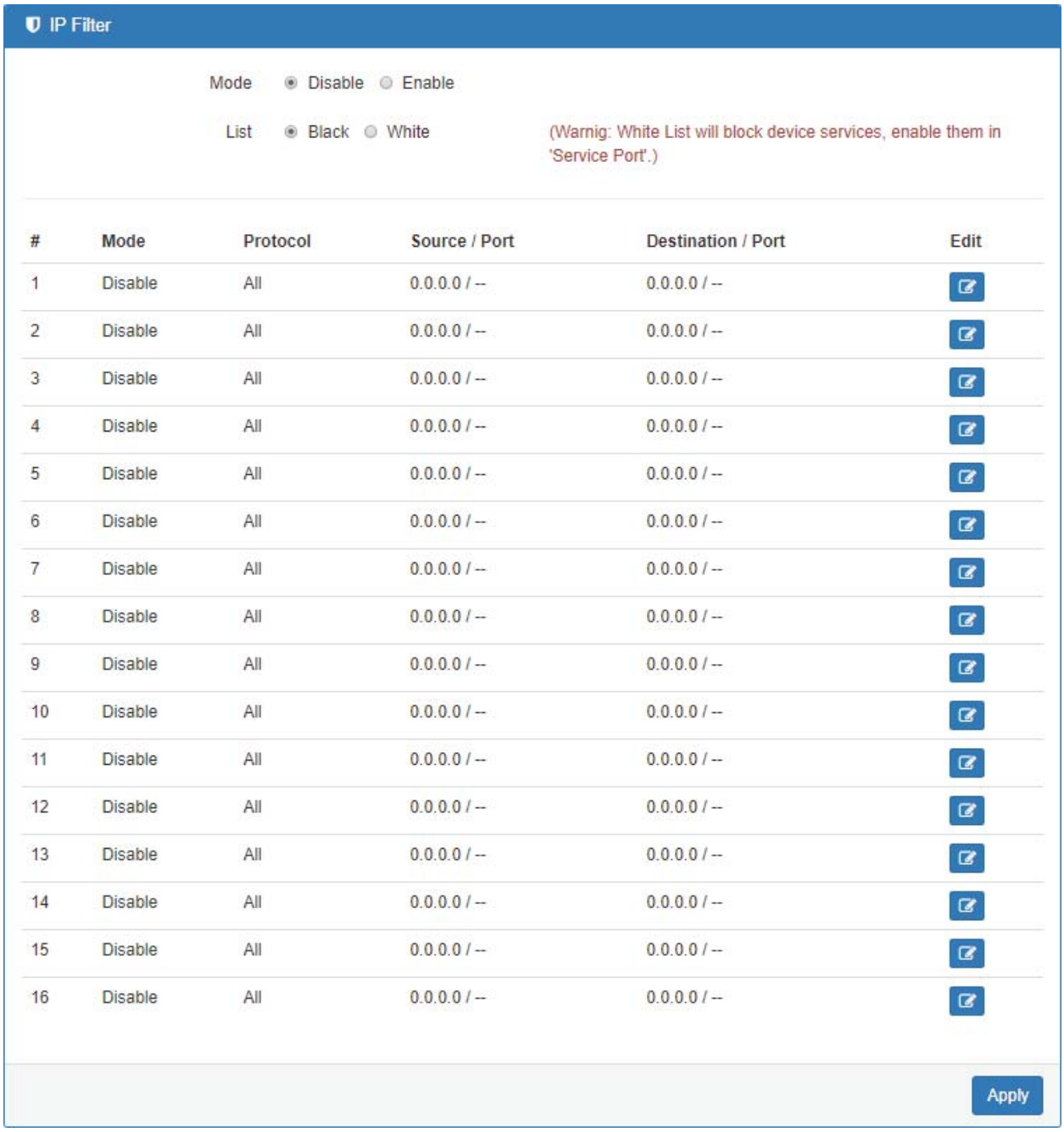
This section allows you to set the DMZ configuration.



Firewall > DMZ	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Host IP Address	Fill in your Host IP Address.

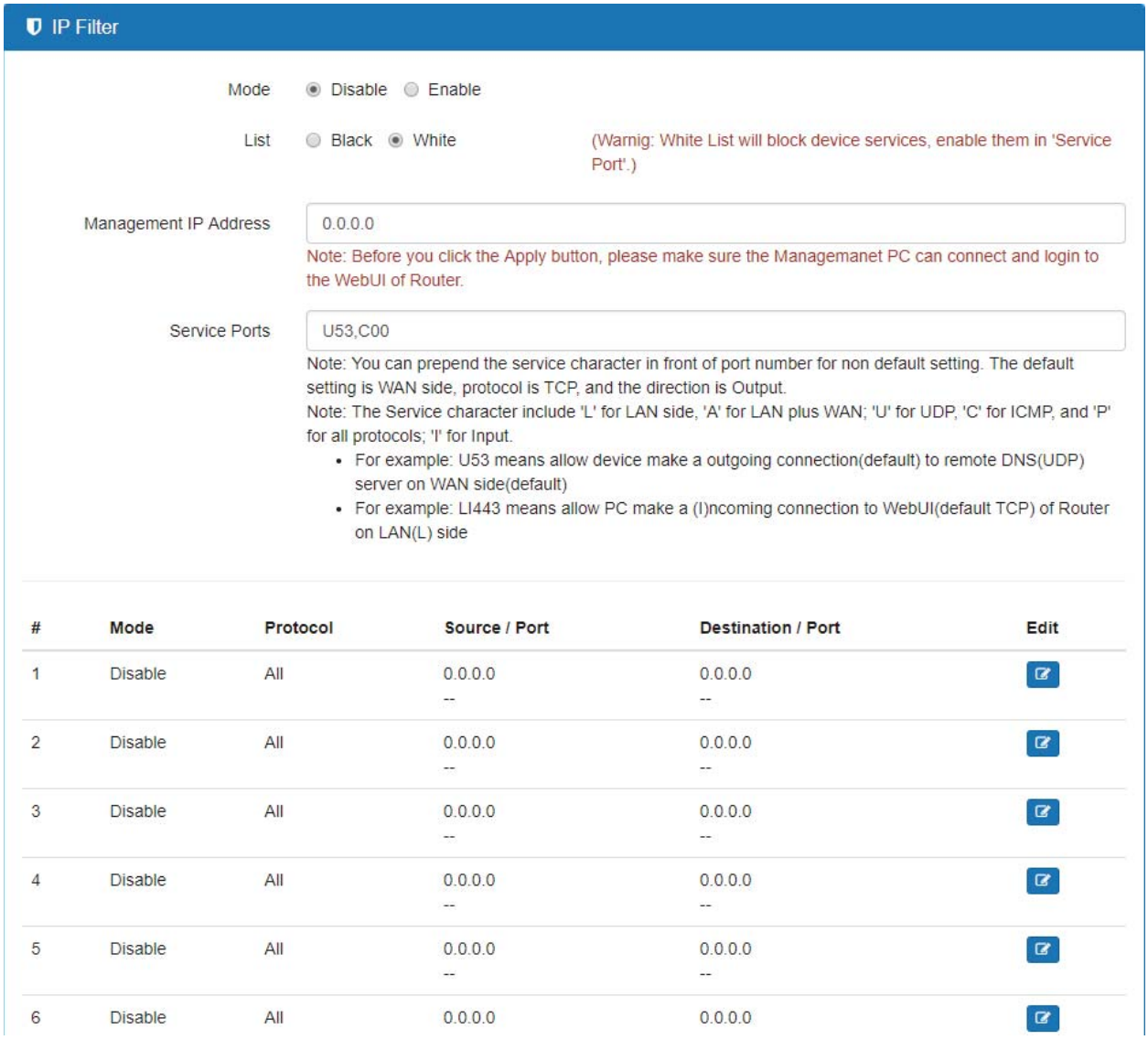
12.4 Firewall > IP Filter

This section allows you to configure IP Filter. After clicking button, you can edit your IP protocol, source/port and destination/port. The default is **Disable** mode and **Black** list.



#	Mode	Protocol	Source / Port	Destination / Port	Edit
1	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
2	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
3	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
4	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
5	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
6	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
7	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
8	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
9	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
10	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
11	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
12	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
13	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
14	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
15	Disable	All	0.0.0.0 / --	0.0.0.0 / --	
16	Disable	All	0.0.0.0 / --	0.0.0.0 / --	

- **Black List:** When set as Black List, the specific IP address/port in rule will be blocked.
- **White List:** When set as White List, the specific IP address/port in rule will be accepted.



Management IP Address:

For White List only. Since White List will block all user communication except those has been assigned by rules, it is better to assign a specific IP address for the administrator to access the Router which is Management IP Address.

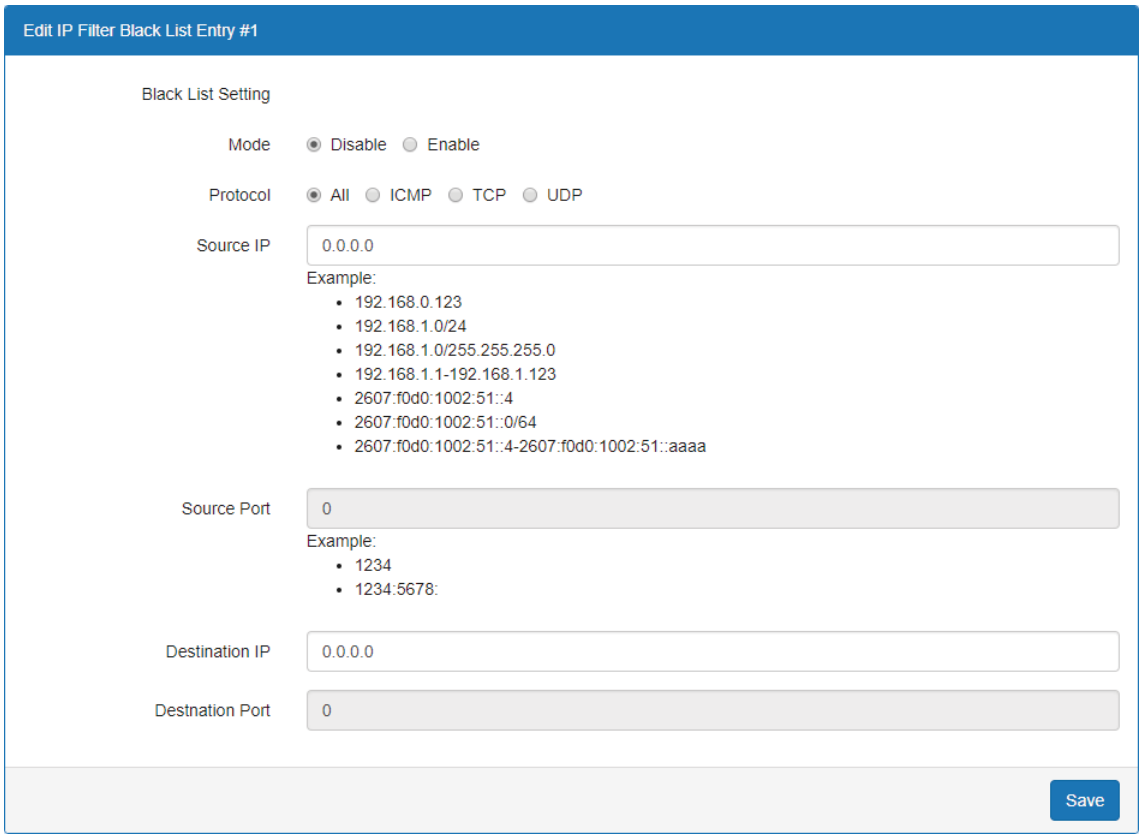
Service Ports:

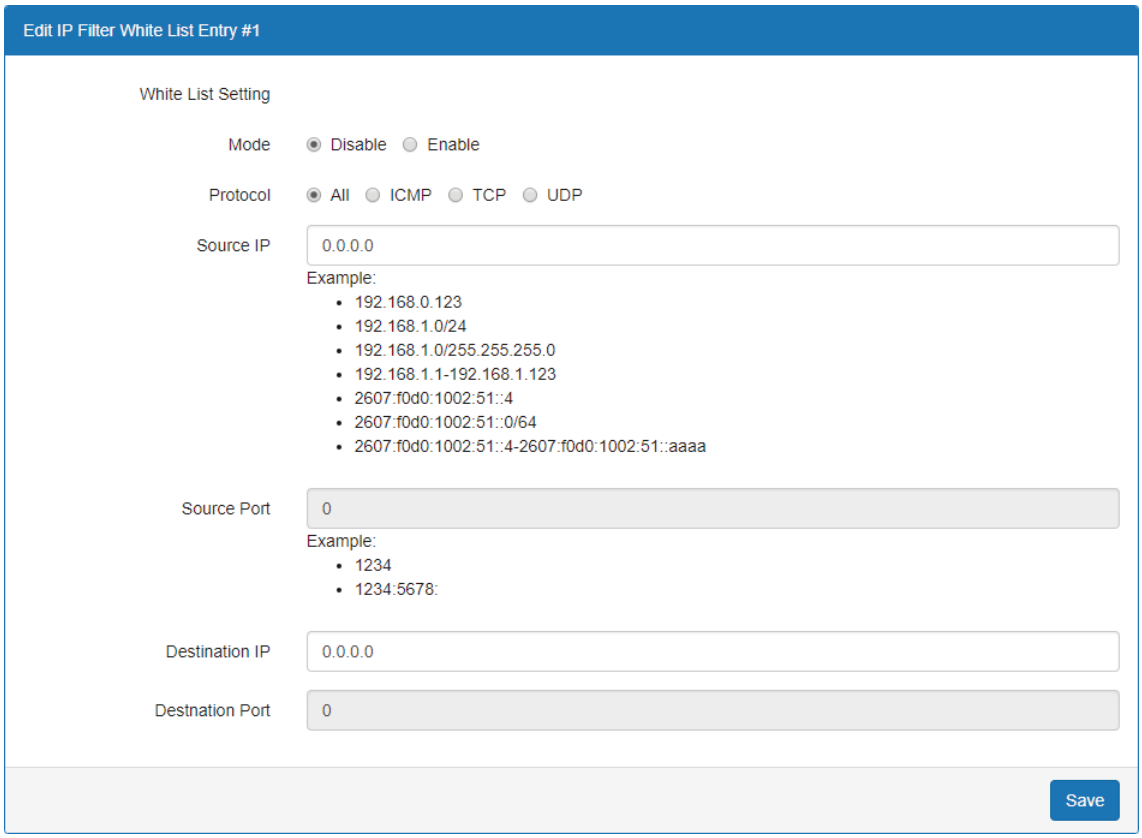
For White List only. The setting is specified for Router access only. The user can set it to allow Router access outside WAN or inside LAN Service. For example, access outside WAN DNS service. It also allows user to access Router service from outside WAN or inside LAN. For example, access Router Web service.

Edit Black/White List

(1) Click button to edit Black/White list.

(2) The default is **Disable** mode as the following interface (Black/White).





Firewall > IP Filter	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Protocol	Select from All, ICMP, TCP or UDP.
Source IP	Fill in your source IP address.
Source Port	Fill in your source port.
Destination IP	Fill in your destination IP address.
Destination Port	Fill in your destination port.

(3) When selecting Enable Mode, the protocol is TCP. The source IP has IPv4 and IPv6 setting formats.

(4) For Source IP, there are three types to input your source IP that depends on your requirement, including single IP, IP with Mask or giving a range of IP. The following table provides some examples.

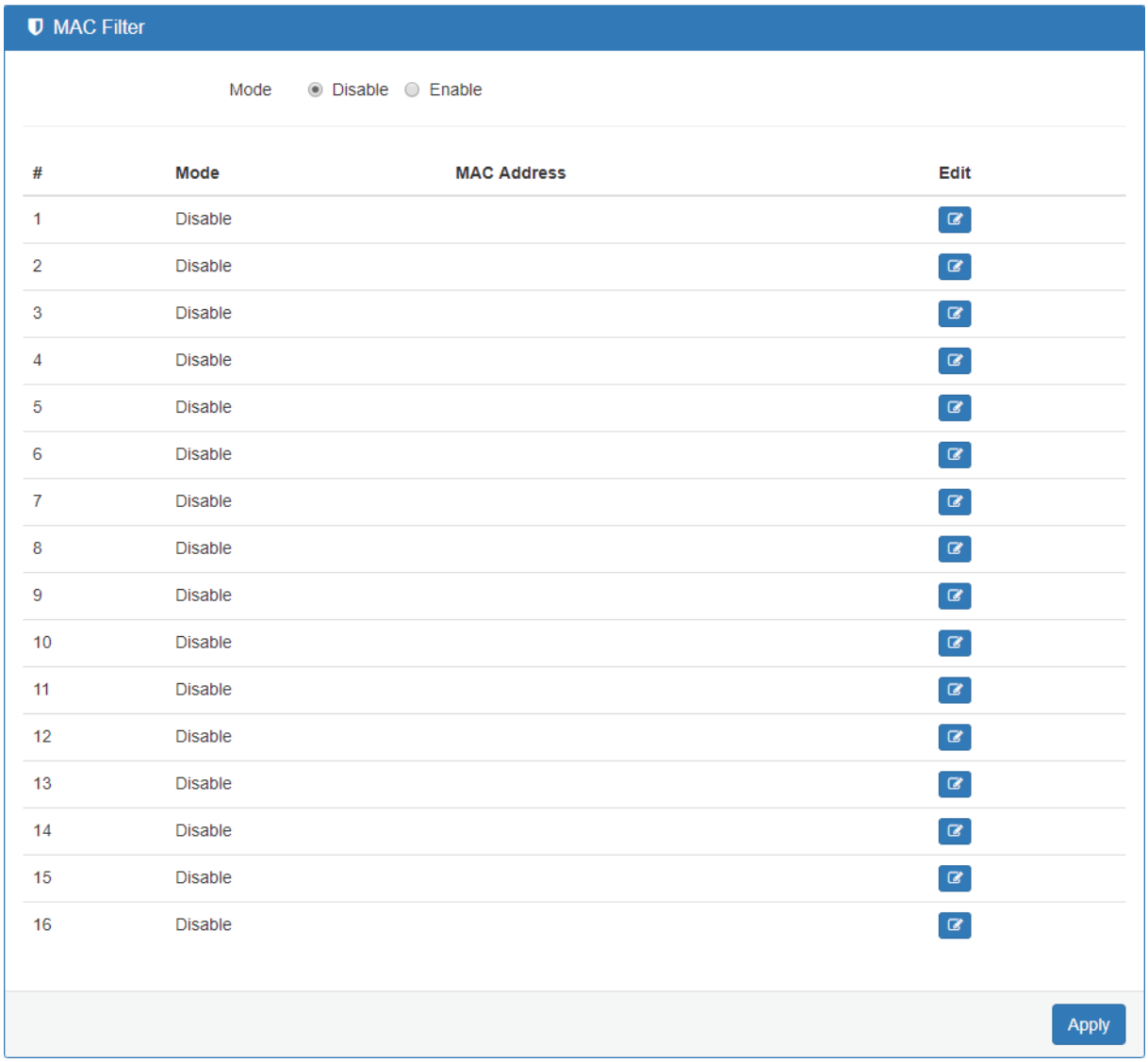
Firewall > Edit IP Filter > Source IP			
IP Format	**Single IP**	**IP with Mask**	**Ranged IP**
IPv4	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	192.168.1.1- 192.168.1.123
IPv6	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4- 2607:f0d0:1002:51::aaaa
Note: Setting up a range of IP, please use **–** hyphen symbol to mark your ranged IP.			

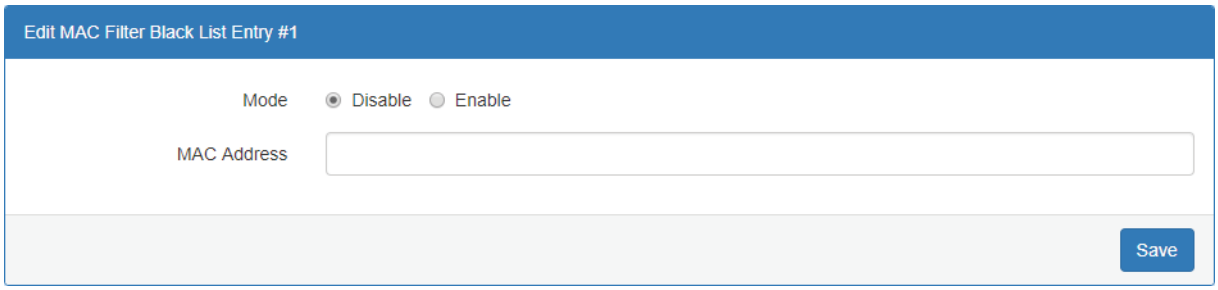
(5) For Source Port, there are two types to input your source port that depends on your requirement, including single port (e.g.1234) or giving a range of ports (e.g.1234:5678).

Note: Setting up a range of source ports, please use: colon symbol to mark your ranged ports.

12.5 Firewall > MAC Filter

This section allows you to set up MAC Filter. After clicking button, you can edit your MAC address.





Service > MAC Filter	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
MAC Address	Fill in your MAC address.

Note: Setting up MAC address, please use ":" colon symbol (e.g. xx : xx : xx : xx) or "-" hyphen symbol to mark (e.g. xx - xx - xx - xx).

12.6 Firewall > URL Filter

This section allows you to set up URL Filter. After clicking button, you can edit the type of filter and information.

URL Filter

Mode ◉ Disable ○ Enable

#	Mode	Filter	Key/Full	Edit
1	Disable	Key		
2	Disable	Key		
3	Disable	Key		
4	Disable	Key		
5	Disable	Key		
6	Disable	Key		
7	Disable	Key		
8	Disable	Key		
9	Disable	Key		
10	Disable	Key		
11	Disable	Key		
12	Disable	Key		
13	Disable	Key		
14	Disable	Key		
15	Disable	Key		
16	Disable	Key		

Apply

Edit URL Filter Black List Entry #1

Mode ○ Disable ◉ Enable

Filter ○ Key ◉ Full

Key/Full tw.yahoo.com

Hint About the 'Full' filter:

- Please NOT include 'http://' or 'https://' inside the URL
- It only works at LTE Net Modes 'Router Only' and 'Dual Router'

Save

Note: Please not include "**https://**" or "**http://**" for the URL address in the **Full** Filter.

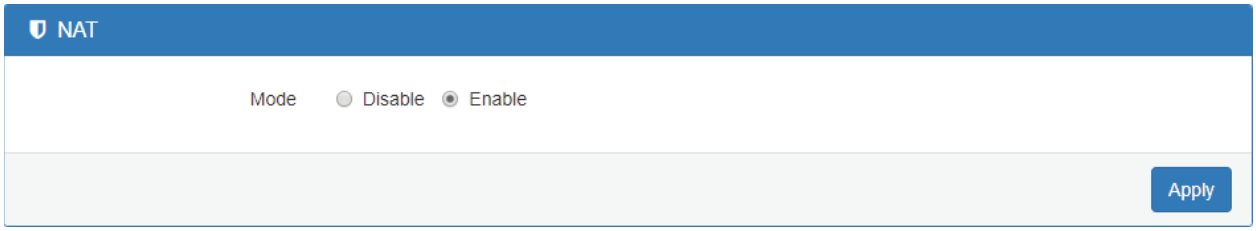
Firewall > URL Filter	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Filter	Select from Key or Full. The default is Key.
Key / Full	Fill in your Key / Full information.

12.7 Firewall > NAT

This section allows you to set NAT configuration.

When NAT mode is **Enable**, the router will replace the source private IP address by its Internet public address for outgoing packets, and replace the destination Internet public address by private IP address for incoming packets.

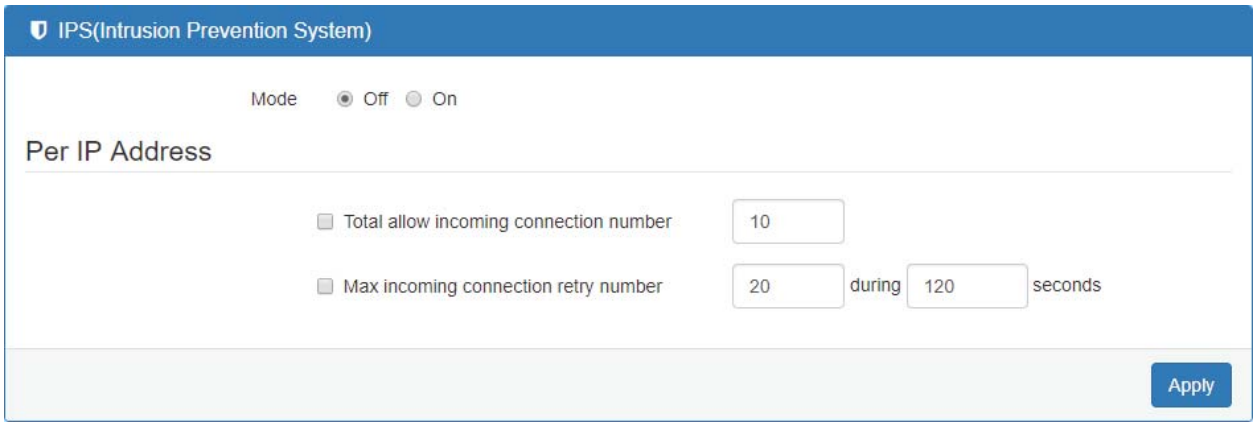
When NAT mode is **Disable**, the router will send the source LAN private IP address for outgoing packets and allow to receive the destination LAN private IP address for incoming packets.



12.8 Firewall > IPS

This section allows you to set IPS configuration. IPS prevents the system from being attacked by the Internet.

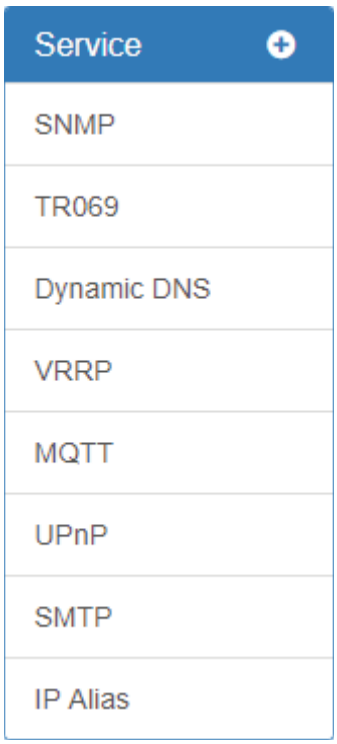
The system allows to limit the max incoming connection number from WAN per source IP address to prevent system resource exhausted. Also, the system allows to limit the max incoming connection retry number during a specific time period from WAN per source IP address to prevent too many unexpected connections retry event from causing system busy.



Firewall > IPS	
Item	**Description**
Mode	Turn on / off IPS function (default: Off)
Total allow incoming connection number	Select the checkbox to enable or disable the function. The default number is 10.
Max incoming connection retry number	Select the checkbox to enable or disable the function. The default number is 20.
Duration time	The default time is 120 seconds.

13 Configuration > Service

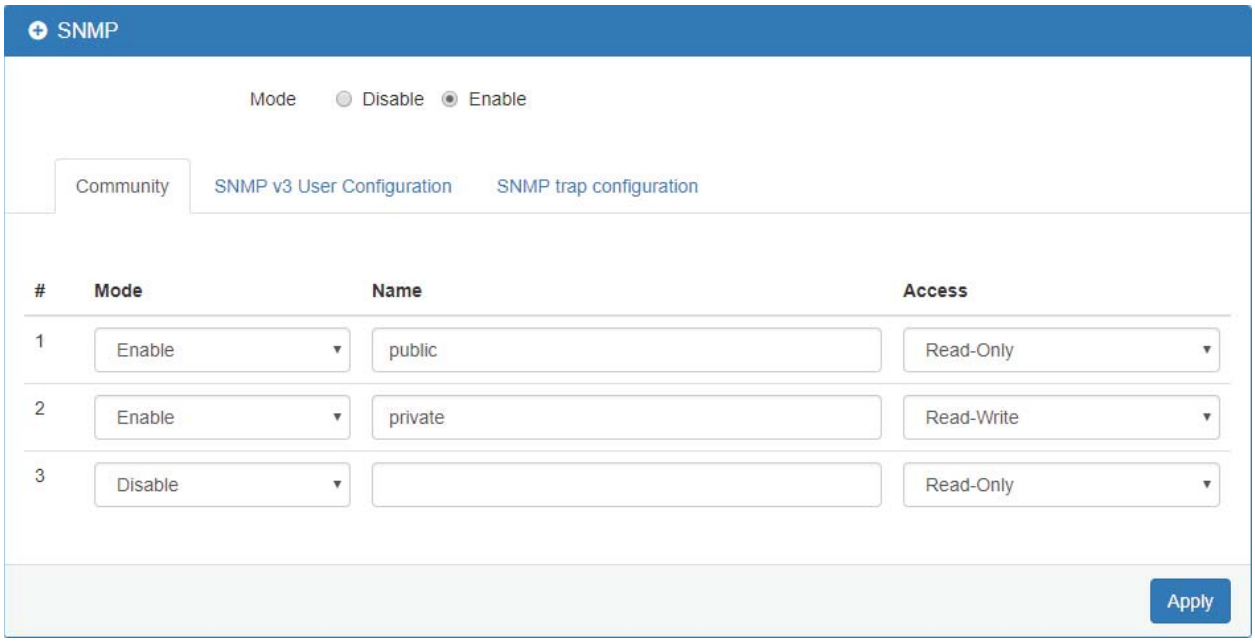
This section allows you to configure the SNMP, TR069, Dynamic DNS, VRRP, MQTT, UPnP, SMTP, and IP Alias.



13.1 Service > SNMP

This section allows you to set the SNMP configuration.

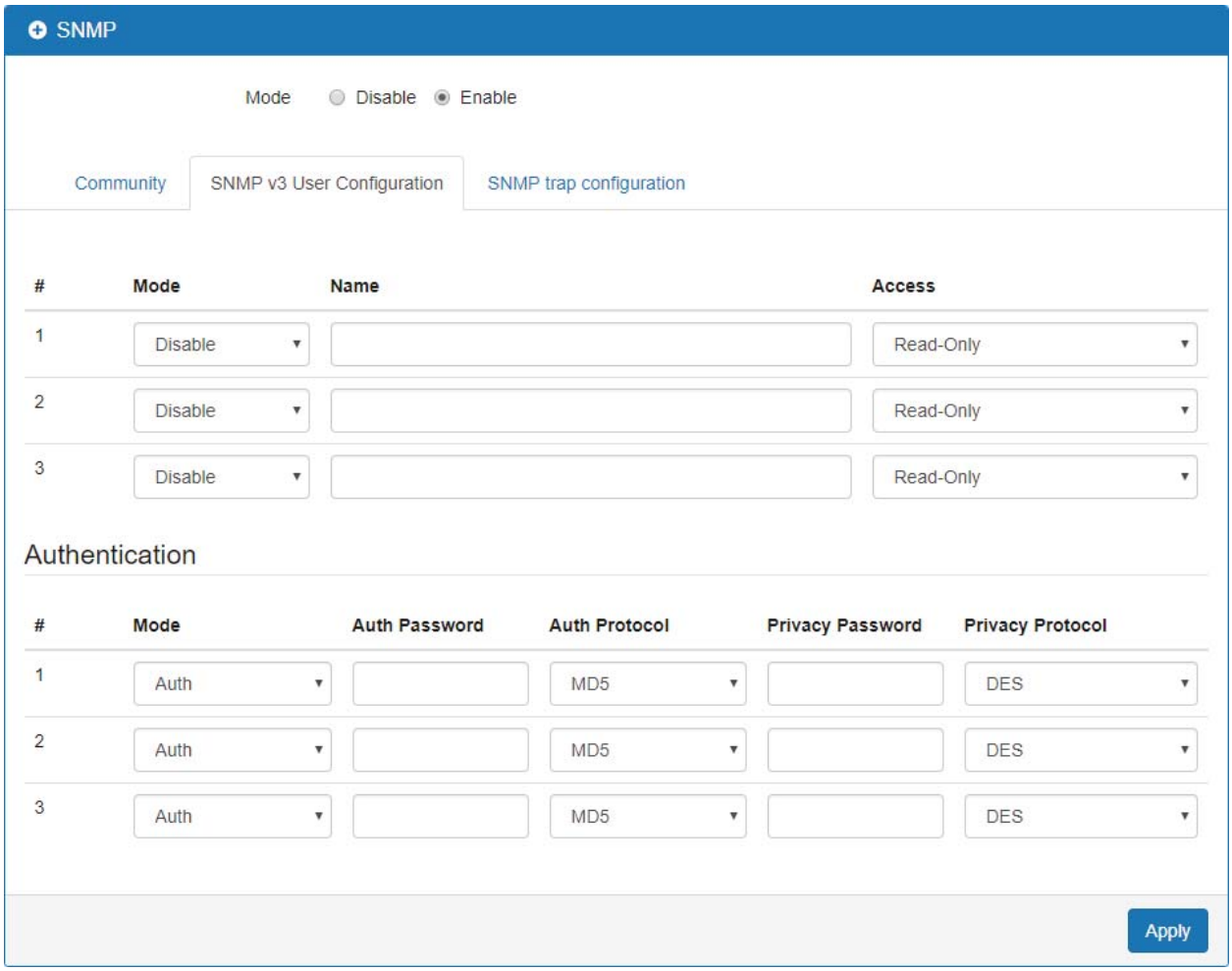
13.1.1 Community



Service > SNMP > Community	
Item	**Description**
Mode	Select from Disable or Enable to configure SNMP.
Community	Configure community setting with three options, including # 1, # 2 and #3.
Mode	Select from Disable or Enable.
Name	Name each community.
Access	Select from Read-Only or Read-Write.

13.1.2 SNMP v3 User Configuration

For SNMP v3 User Configuration, you need to register authentication and allow a receiver that confirm the packet was not modified in transit. There are three options to set up SNMP v3 Configuration.

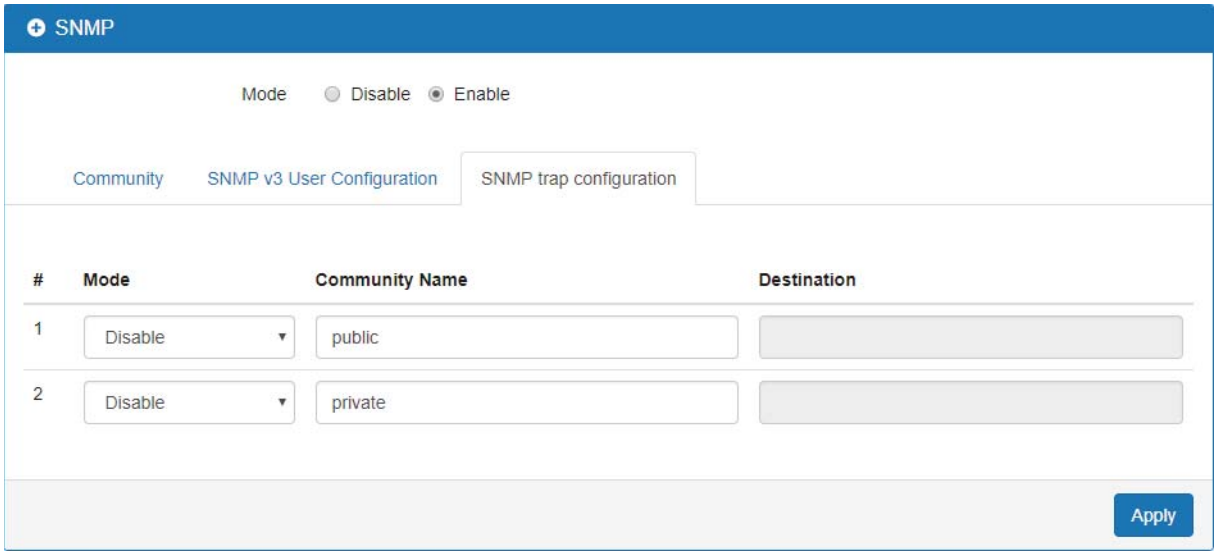


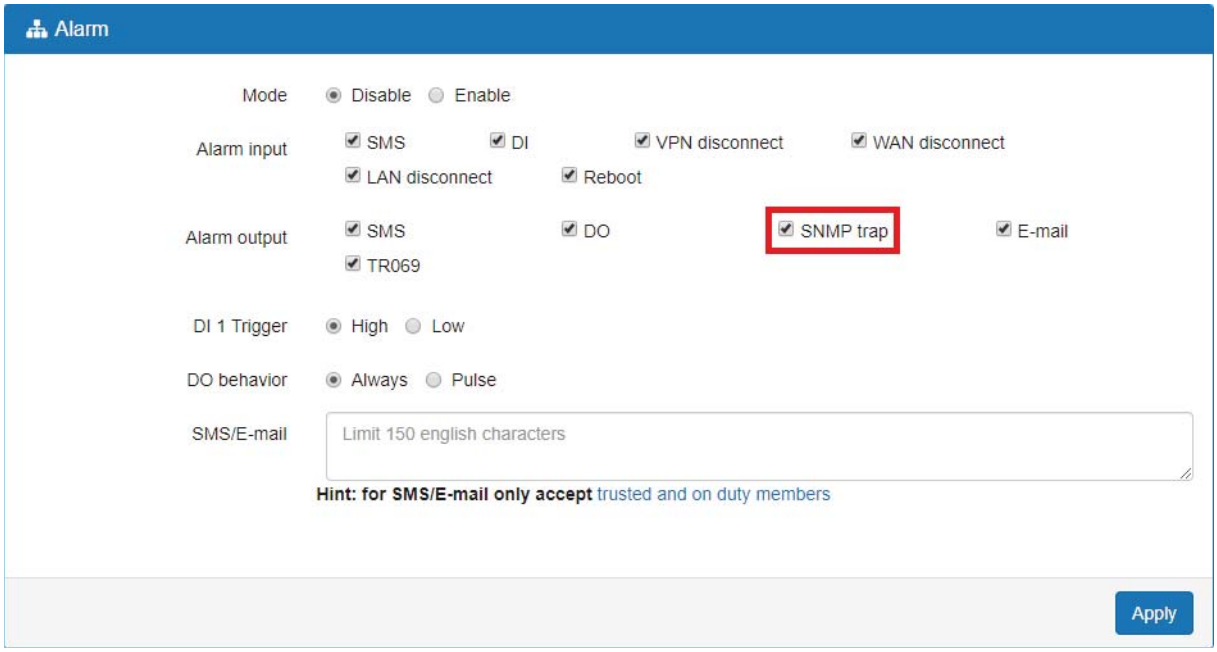
Service > SNMP > SNMP v3 User configuration	
Item	**Description**
Mode	Select from Disable or Enable to configure SNMP. The default is Disable.
Name	Fill in your name.
Auth Mode	Select from Authentication or Privacy.
Authentication Password	Fill in your authentication password.

Authentication Protocol	Select from MD5 or SHA.
Privacy Password	Fill in your privacy password.
Privacy Protocol	Select from DES or AES.
Access	Select from Read-Only or Read-Write.

13.1.3 SNMP trap configuration

This section allows you to set up the SNMP trap configuration when you select the SNMP trap function from Alarm output of system for your router. With SNMP trap setting, you can know the status of remote device.

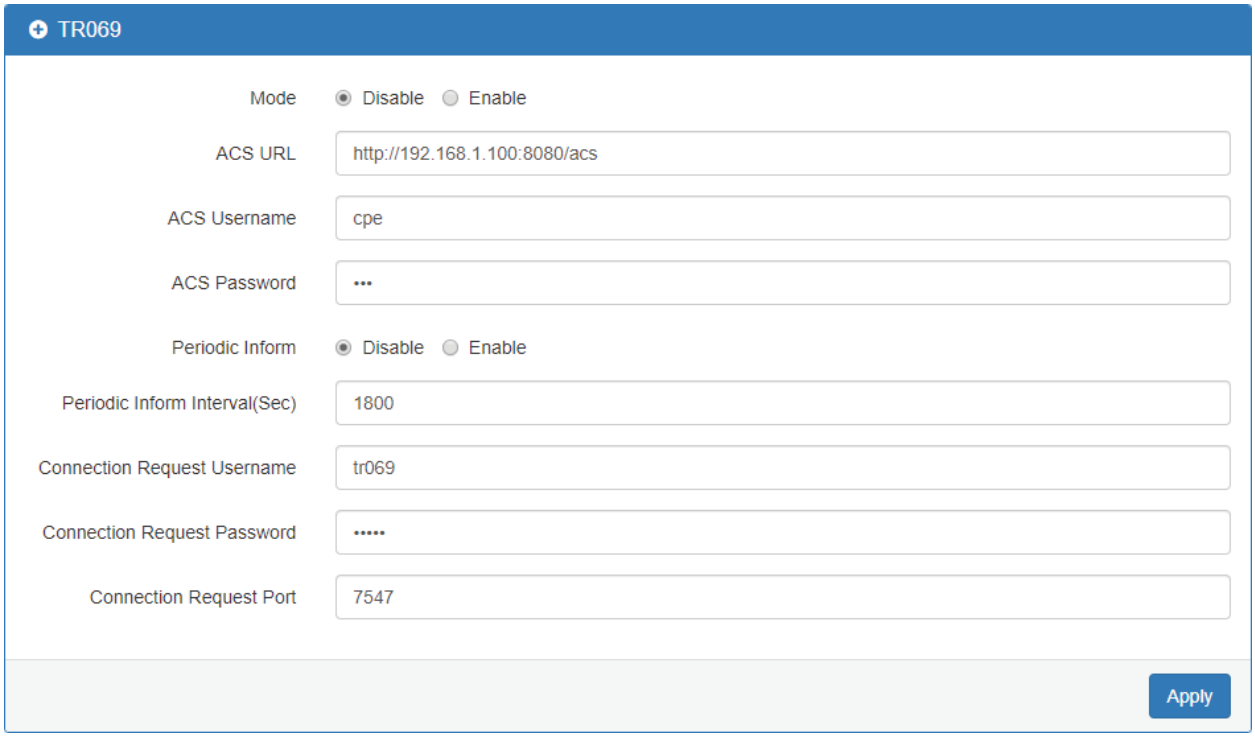




Service > SNMP > SNMP trap configuration	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Community Name	Fill in your community name.
Destination	The destination (domain name/IP) of remote SNMP trap server.

13.2 Service > TR069

This section allows you to set up TR069 client configuration. You can get information how to install TR069 Server (GenieACS Installation) from the application configuration chapter.



Service > TR069	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
ACS URL	Fill in the URL address of ACS (Auto-Configuration Server).
ACS Username	Fill in the ACS username to authenticate the CPE (this router) when connecting to the ACS.
ACS Password	Fill in the ACS password to authenticate the CPE (this router) when connecting to the ACS.
Periodic Inform	Select from Disable or Enable. The default is Disable. The CPE reports the status to the ACS when enabling a period of time set.
Periodic Inform Interval (Sec)	Fill in the periodic time. The CPE reports to ACS the status according to your duration in seconds of the interval set.
Connection Request Username	Fill in the connection request username to authenticate the ACS if the ACS attempts to communicate with the CPE.
Connection Request Password	Fill in the connection request password to authenticate the ACS if the ACS attempts to communicate with the CPE.
Connection Request Port	Fill in the connection request port to authenticate the ACS if the ACS attempts to communicate with the CPE.

13.3 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.

Service > Dynamic DNS	
Item	**Description**
Mode	Turn on/off this function to select Disable or Enable. The default is Disable.
Service Provider	Select the Service Provider of Dynamic DNS.
Host Name	Fill in your registered Host Name from Service Provider.
Token ID	Fill in your Token ID from Service Provider.
Host Secret ID	Fill in your Secret ID from Service Provider.
Username	Fill in your registered username from Service Provider.
Password	Fill in your registered password from Service Provider.
Update Period Time (Sec)	Fill in “0” to mean 30 days.
IP Address Selection	Select either Internet IP or WAN IP.

Note: There are six options of Service Provider as below to explain the information.

Service Provider	**dynv6.com**
Host Name	Register hostname, e.g. tester.dynv6.net
Token ID	The token ID, e.g. v_ABjMMQxeAnWv5UwtuVn1QBriynzq

Service Provider	**www.nsupdate.info**
Host Name	Register hostname, e.g. tester.nsupdate.info
Host Secret ID	The Host Secret ID, e.g. e2AMDsLmVF

Service Provider	**www.duckdns.org**
Host Name	Register hostname, e.g. tester.duckdns.org
Token ID	The token ID, e.g.12345678-de49-4e97-a33c-98b159aead2b

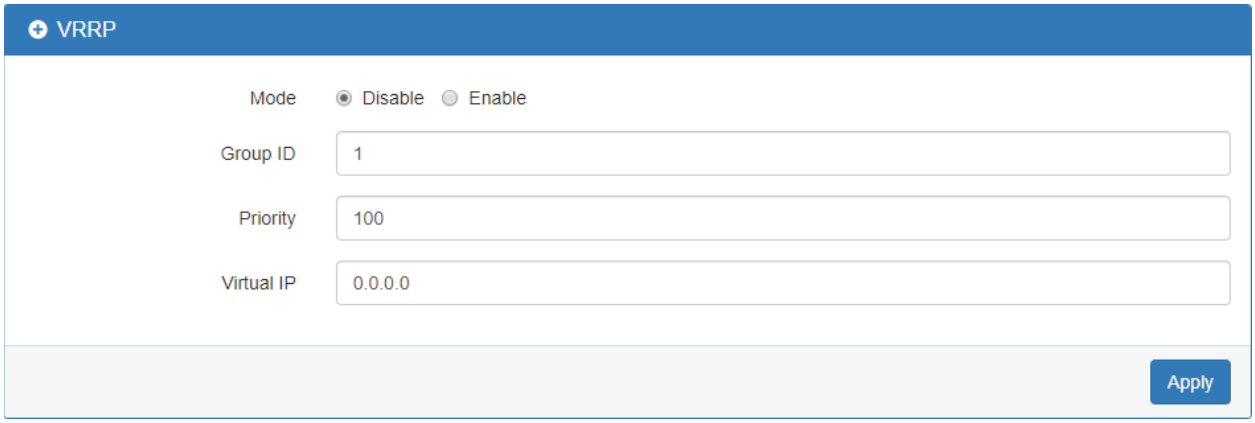
Service Provider	**no-ip.com**
Host Name	Register hostname, e.g. tester.hopto.org
Username	Register username.
Password	Register password.

Service provider	**freedns.afraid.org**
Host Name	Register hostname, e.g. tester.mooo.com
Username	Register username.
Password	Register password.

Service provider	**dyndns.org**
Host Name	Register hostname, e.g. tester.dyns.com
Username	Register username.
Password	Register password.

13.4 Service > VRRP

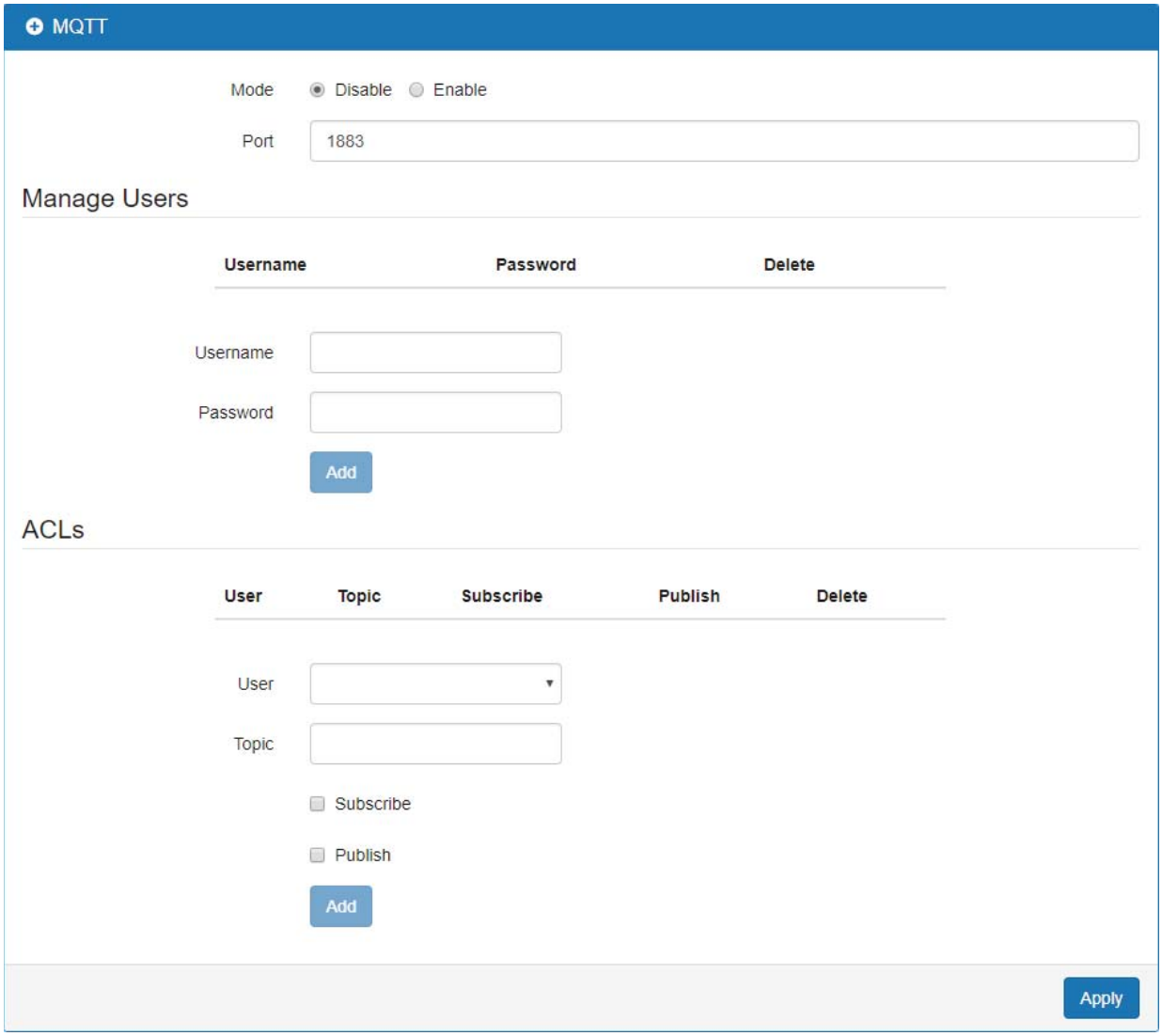
This section allows you to configure VRRP.



Service > VRRP	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Group ID	Specify which VRRP group of this router belong to (1-255). The default is 1.
Priority	Enter the priority value from 1 to 254. The larger value has higher priority. The default is 100.
Virtual IP	● Each router in the same VRRP group must have the same virtual IP address. The default is 0.0.0.0. ● This virtual IP address must belong to the same address range as the real IP address of the interface.

13.5 Service > MQTT

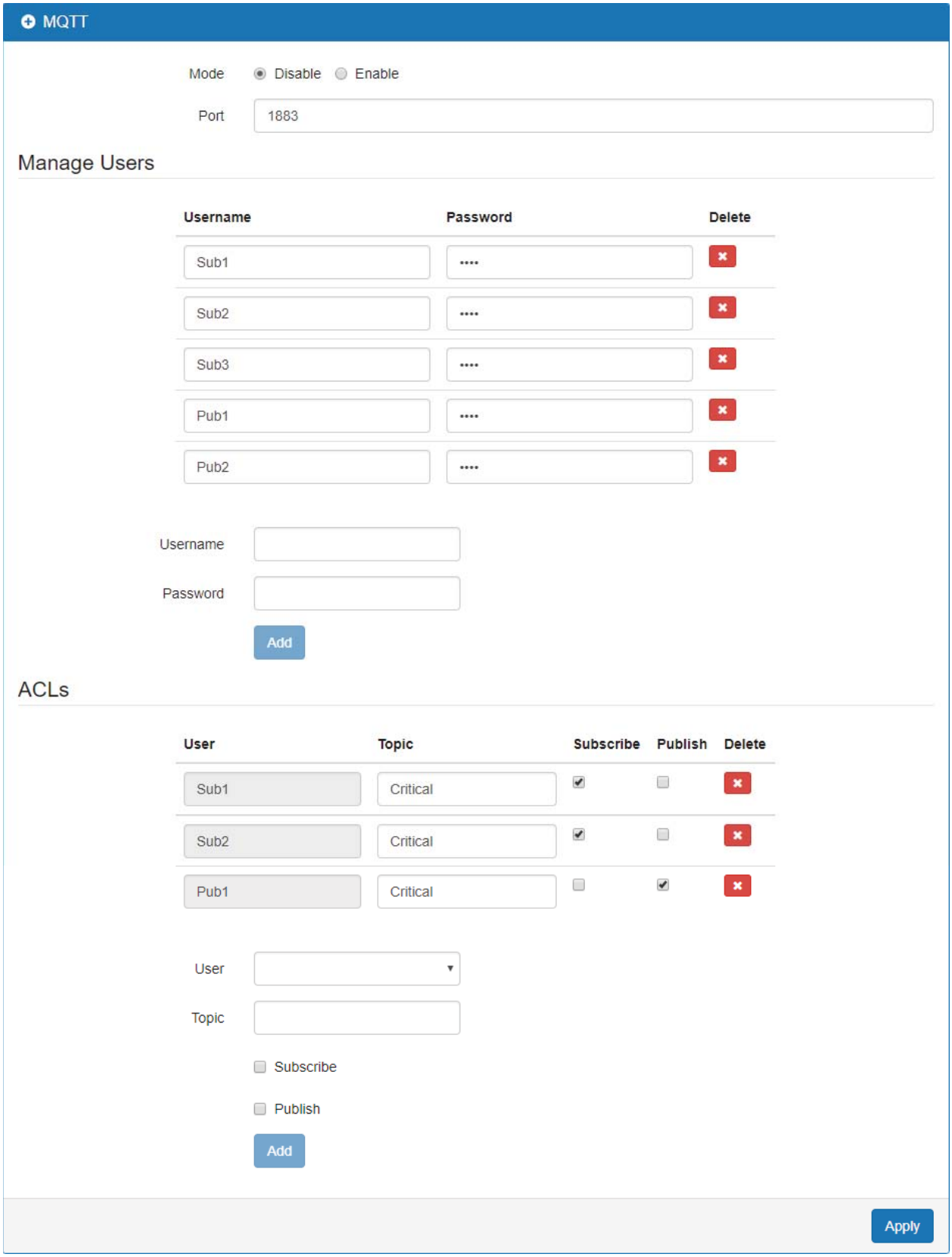
This section makes you configure MQTT which allows the MQTT client to send the message within specific topic or channel. By default, the router does not allow anonymous to read/write the MQTT topic or channel. Thus, you need to create the account with username and password for MQTT client in the web UI.



Service > MQTT	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Port	Fill in the port number of MQTT application.
Manage Users	Create the users and show all users' names. Allow each user to delete their name.
Username	Fill in the username of manage user.
Password	Fill in the password of manage user.
ACLs	Allow to specify what topic should be limited.
User	Select the users and identify their authority to read or write the MQTT topic/channel.
Topic	Name the topic of MQTT message.

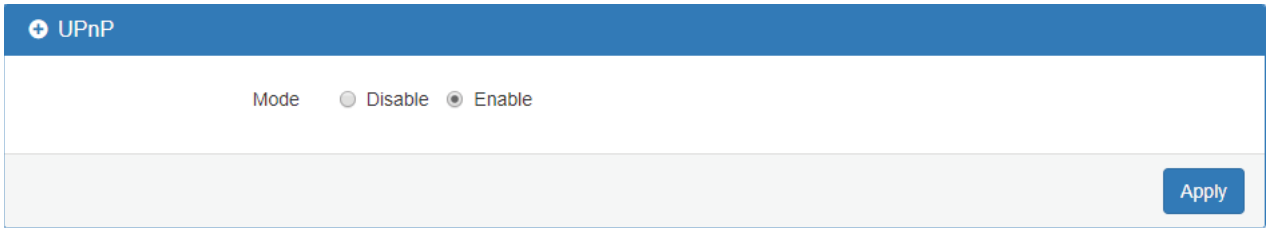
Take for example, the interface is shown as below.

The **Manage Users** section will show all users that you create. Moreover, each user can use the delete button to delete it. For the **ACLs** control, user can specify what topic should be limited. In this case, we set up the publisher **pub1** to write the critical topic. Additionally, we also allow the subscribers **sub1** and **sub2** to read the critical topic. Thus, only the sub1 and sub2 can receive it when **pub1** sending the message.


MQTT
Mode
Disable
Enable
Port
1883
Manage Users
Username
Password
Delete
Sub1
Sub2
Sub3
Pub1
Pub2
Username
Password
Add
ACLs
User
Topic
Subscribe
Publish
Delete
Sub1
Critical
Sub2
Critical
Pub1
Critical
User
Topic
Subscribe
Publish
Add
Apply

13.6 Service > UPnP

This section allows you to set up UPnP confirguration to select the mode from Disable or Enable. The default UPnP is enabled for the cellular router.



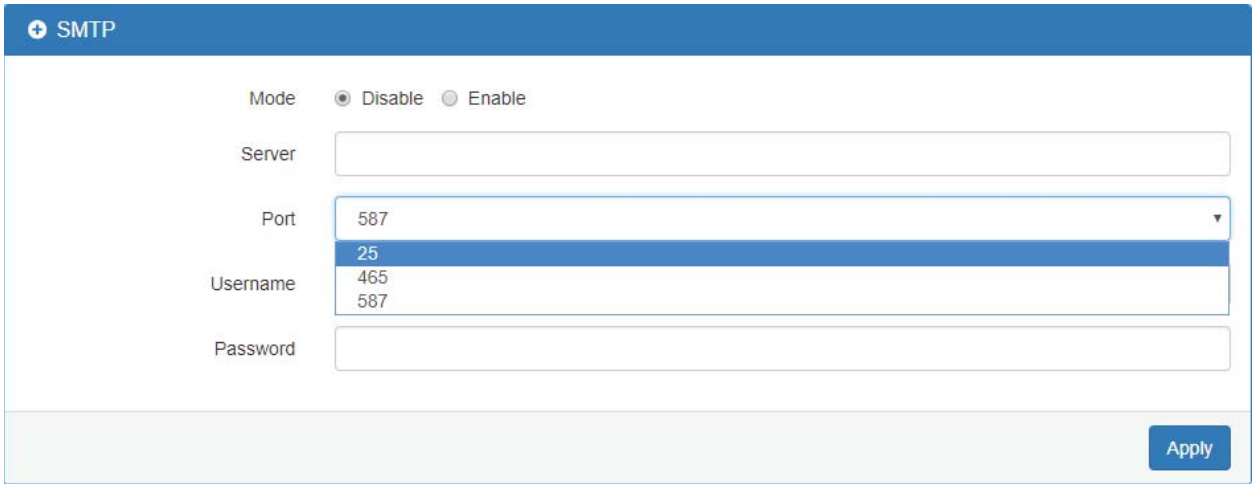
Note:

UPnP™ (Universal Plug and Play) is a set of protocols that allows a PC to automatically discover other UPnP devices (anything from an Internet gateway device to a light switch), retrieve an XML description of the device and its services, control the device, and subscribe to real-time event notification.

PCs using UPnP can retrieve the cellular router's WAN IP address, and automatically create NAT port maps. This means that applications that support UPnP, and are used with UPnP enabled cellular router, will not need application layer gateway support on the cellular router to work through NAT.

13.7 Service > SMTP

This section provides you to send your email for the server. For instance, the email will be sent to notify when the Alarm has a nofitication by the server.



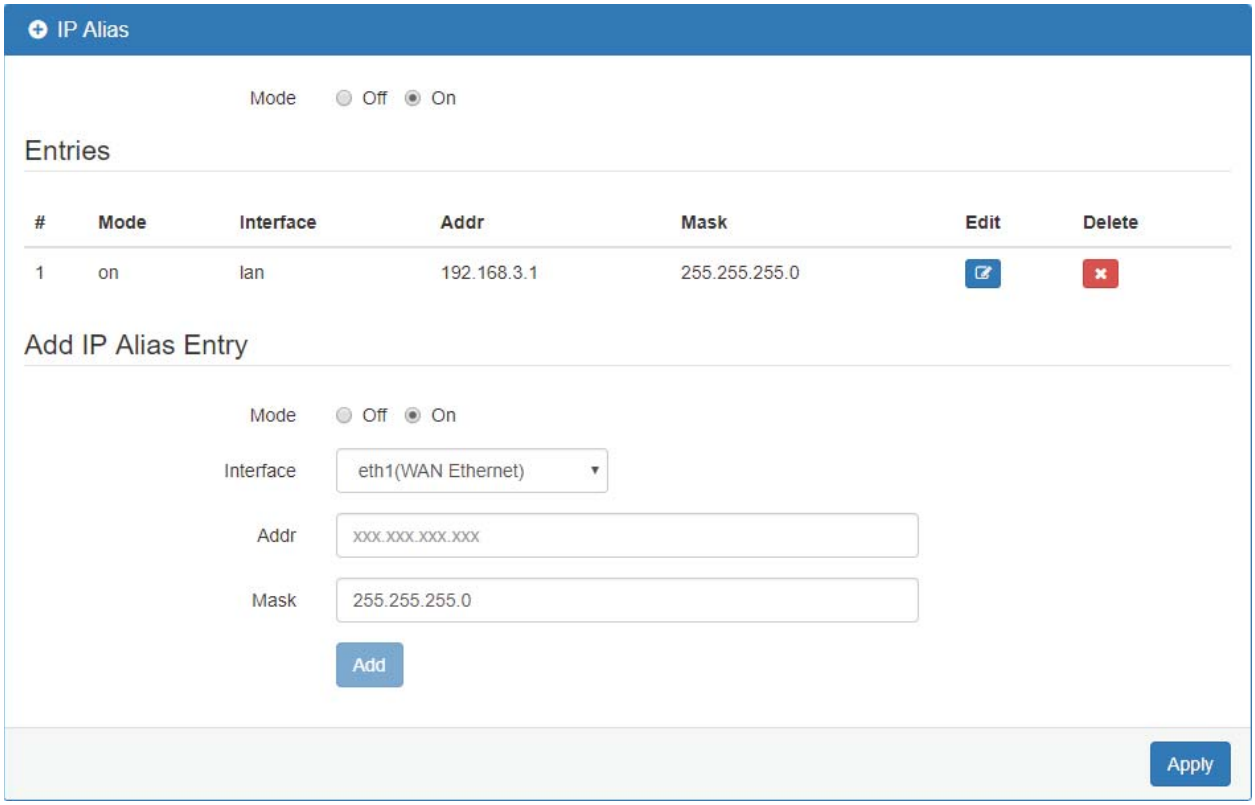
Service > SMTP	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Server	The email will be sent through the server.
Port	There are three ports for SMTP communication between mail servers. ● **Port 25**：Use TCP port 25 without encryption. ● **Port 465**：SMTP connections secured by SSL. ● **Port 587**：SMTP connections secured by TLS.
Username / Password	Fill in your username and password as the same your server.

13.8 Service > IP Alias

This section allows you to set **IP Alias** configuration.

IP Alias is associating more than one IP address to a network interface. With IP Alias, one node on a network can build multiple connections with the network, each serving a different purpose.

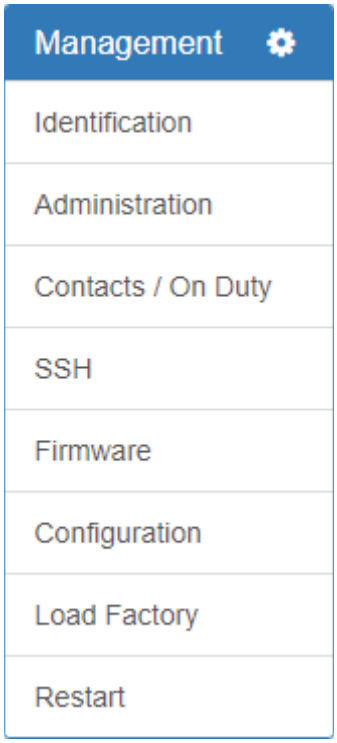
IP Alias can be used to provide multiple network addresses on a single physical interface.



Service > IP Alias	
Item	**Description**
Mode	Select from Off or On to enable the IP Alias.
Entries	The setting can be edited or deleted the existed entries.
Add / Edit IP Alias Entry	● **Mode:** select from Off or On to use or not use this entry. ● **Interface:** the interface you want to provide the additional address. ● **Addr:** the IP address. ● **Mask:** the network mask.

14 Configuration > Management

This section provides you to manage the router, set up your administration and know about the status of current software and firmware. Also, you can back up and restore the configuration.



14.1 Management > Identification

This section allows you to confirm the profile of router, current software, firmware version and system uptime.

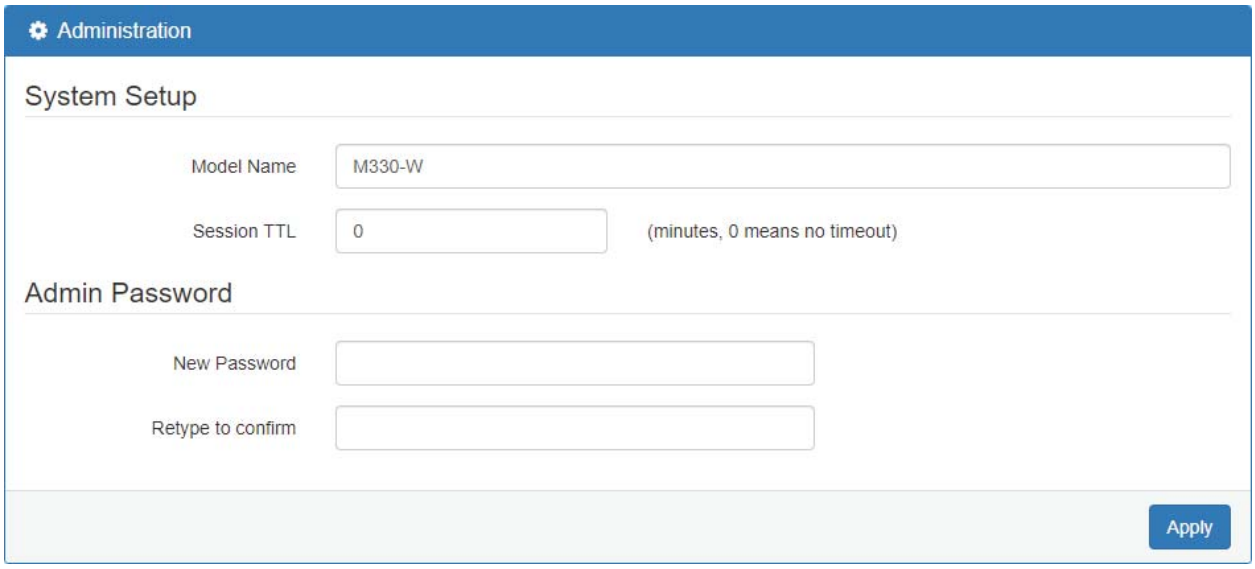
Identification

Attr.	Value
Active Image Partition	a
Model Name	M330-W
LAN Ethernet MAC Address	00:03:79:06:2F:BD
WAN Ethernet MAC Address	00:03:79:06:2F:BE
Software Version	3.3.8
Firmware Version	V0.02
Hardware Version	
Software MCSV	014B00000022E82C
Hardware MCSV	014B000000000000
Serial Number	BL9U43VZ0005
Modem Firmware Version	EC25EFAR06A03M4G
IMEI	866758043832480
Uptime	6:42:38

Management > Identification	
Item	**Description**
Model Name	The model name of cellular router.
LAN Ethernet MAC Address	The LAN Ethernet MAC address.
WAN Ethernet MAC Address	The WAN Ethernet MAC address.
Software Version	The software version currently running on the device.
Firmware Version	The firmware version of the device.
Hardware Version	The hardware version of the device.
Software MCSV	Show the software MCSV of the running firmware
Hardware MCSV	Show the current hardware MCSV of the device.
Serial Number	Show the product serial number.
Modem Firmware Version	Show the modem firmware version of the device
IMEI	Show the IMEI (International Mobile Equipment Identity number).
Uptime	Show the current system uptime.

14.2 Management > Administration

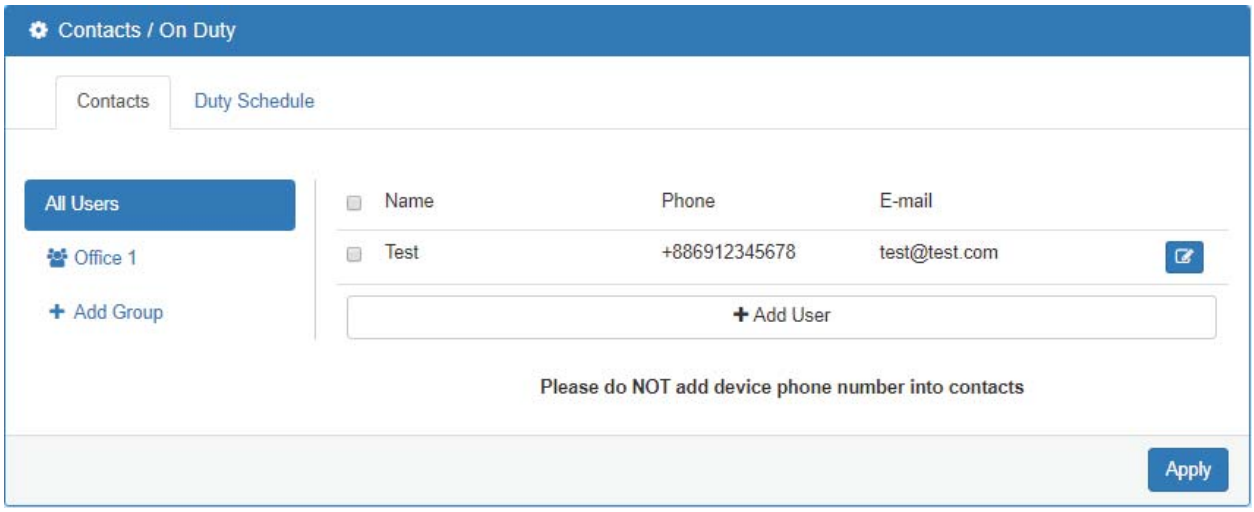
This section allows you to set up the name of the device and change your new password. For the **Session TTL**, you can set up what duration of time will be logout. If you don't need to have this timeout limitation, you can fill in "0"(Zero). The default timeout is 5 minutes.



14.3 Management > Contacts / On Duty

This section allows you to create the groups, add the usersFor more detailed instruction, please navigate to System > Alarm.

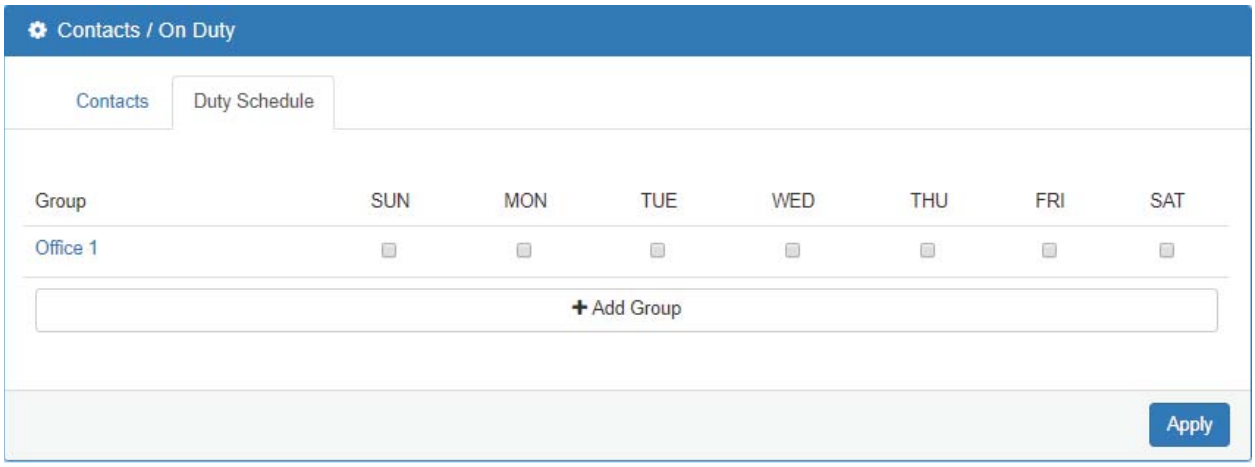
14.3.1 Contacts



+ Add Group: Please fill out group name.

+ Add User: Please fill out Name/Phone/E-Mail/Groups.

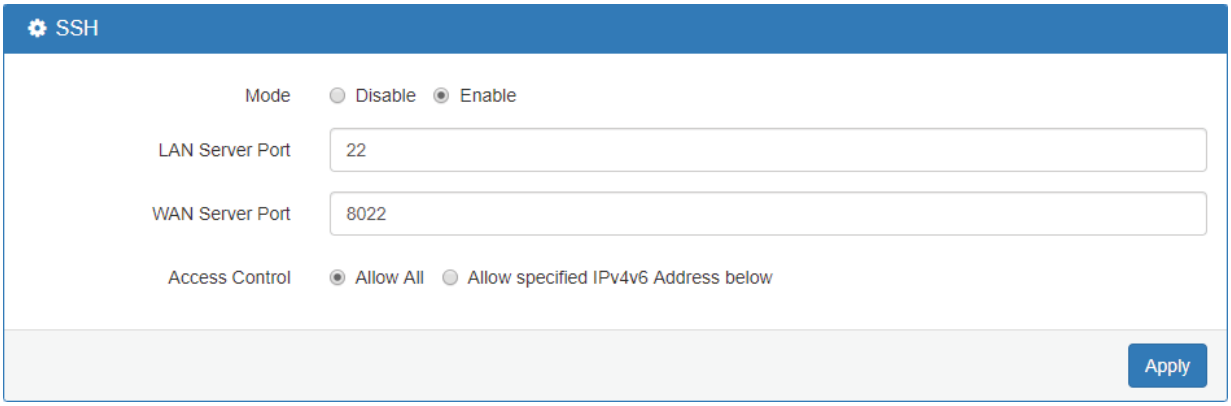
14.3.2 Duty Schedule

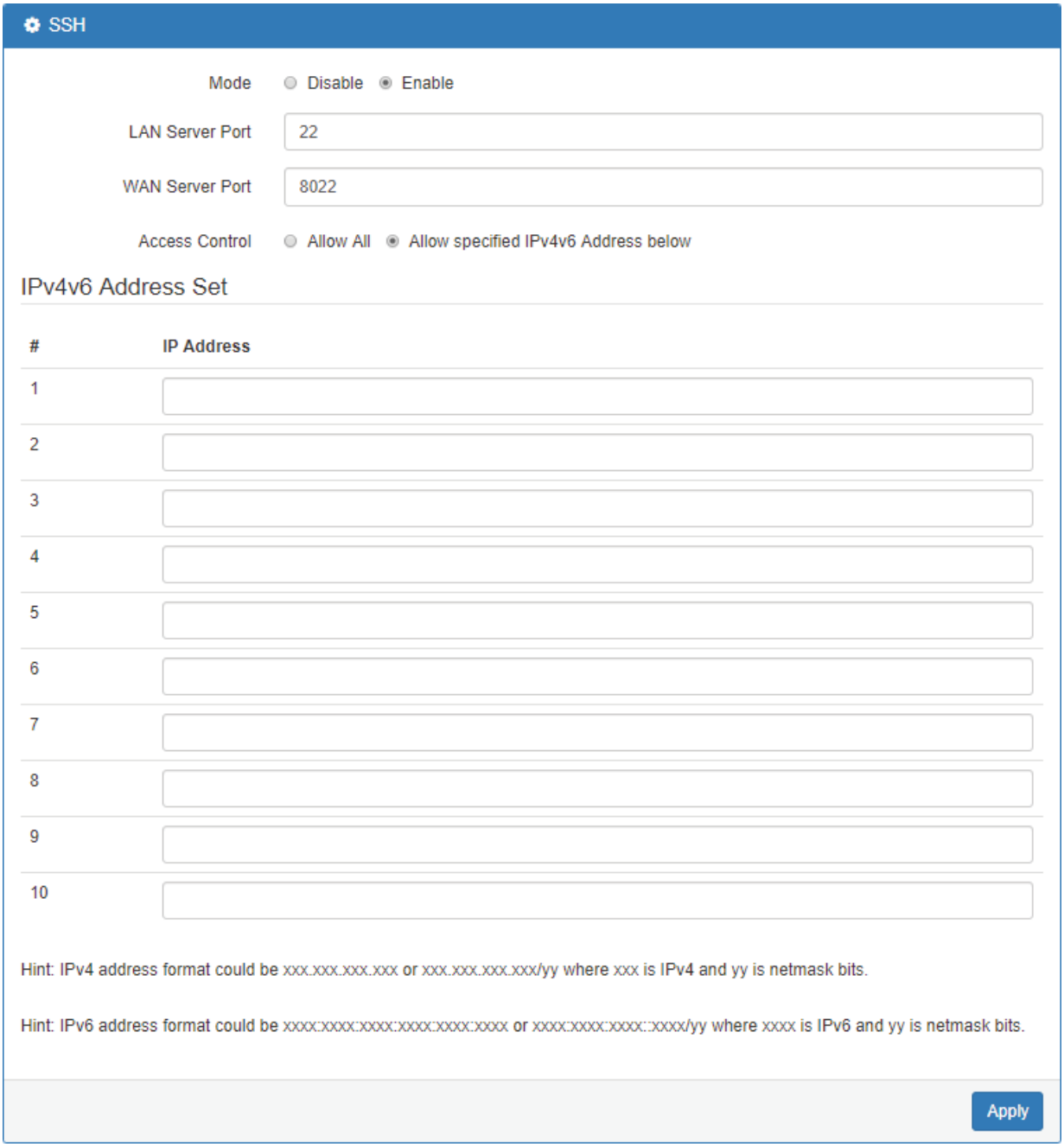


Please select duty date for every group. The trust and responsible groups can control/receive alarms and SMS.

14.4 Management > SSH

Secure Shell (SSH) allows user to configure system via a secure channel. User can configure system from either public domain or local LAN.





Management > SSH	
Item	**Description**
Mode	Select from Disable or Enable SSH function.
LAN Server Port	The LAN side TCP port number listened by SSH server.
WAN Server Port	The WAN side TCP port number listened by SSH server.
Access Control	● **Allow All:** Any client who own the IPv4v6 Address can reach system is able to connect system. ● **Allow specified IPv4v6 Address below:** Only those configured IPv4v6 Address client are allowed to connect system.

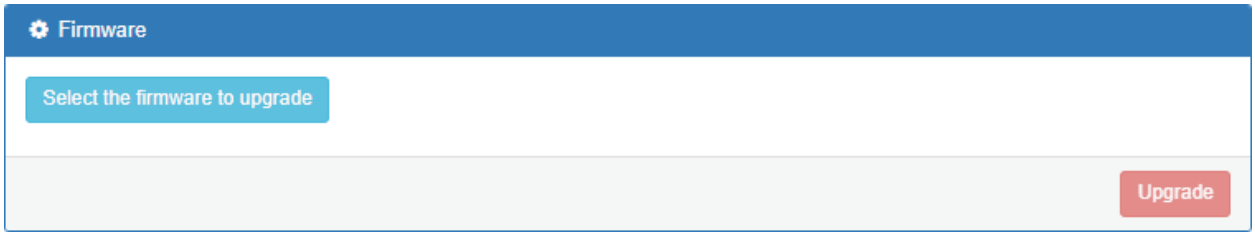
14.5 Management > Firmware

This section provides you to upgrade the firmware of router.

(1) Click Select the firmware to upgrade button to choose your current firmware version in your PC.

(2) Select Upgrade button to update.

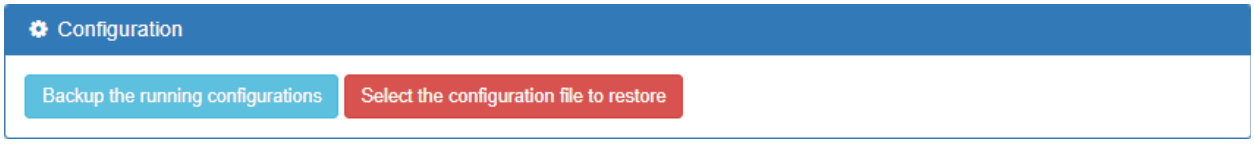
(3) After upgrading successfully, please reboot the router.



14.6 Management > Configuration

This section supports you to export or import the configuration file.

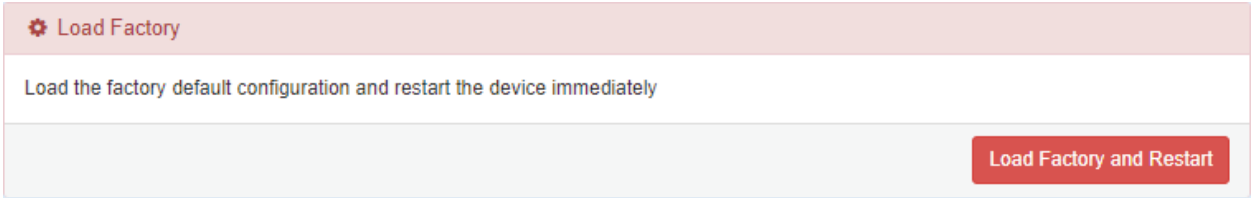
(1) Click Backup the running configurations button to export your current configurations.



(2) Click Select the configuration file to restore button to import the configuration file.

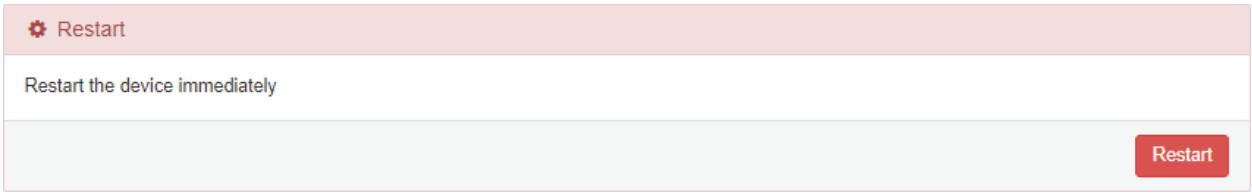
14.7 Management > Load Factory

This section supports you to load the factory default configuration and restart the device immediately. You can click the Load Factory and Restart button.



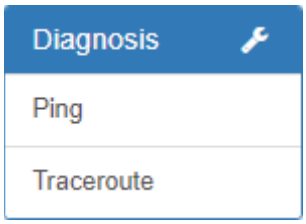
14.8 Management > Restart

This section allows you to click Restart button and the router will restart immediately.



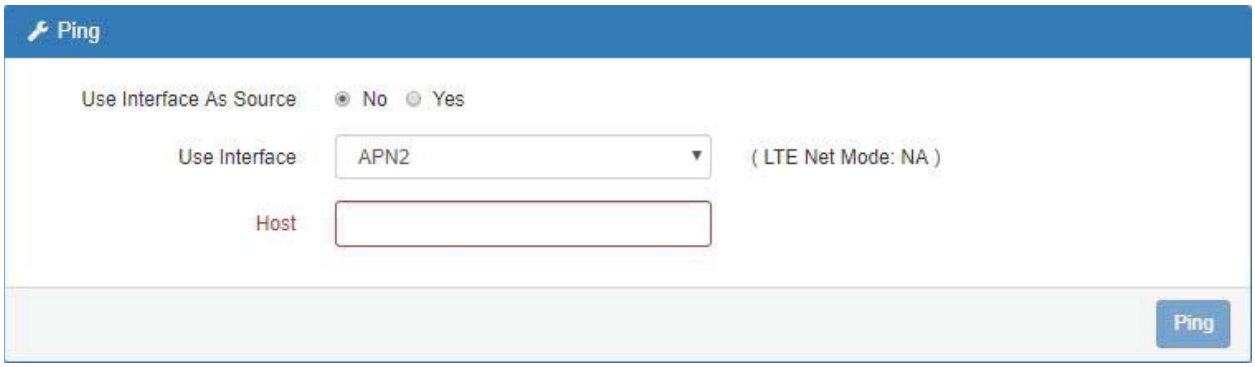
15 Configuration > Diagnosis

This section allows you to diagnose Ping and Traceroute for your Host (IP address or Domain Name).



15.1 Diagnosis > Ping

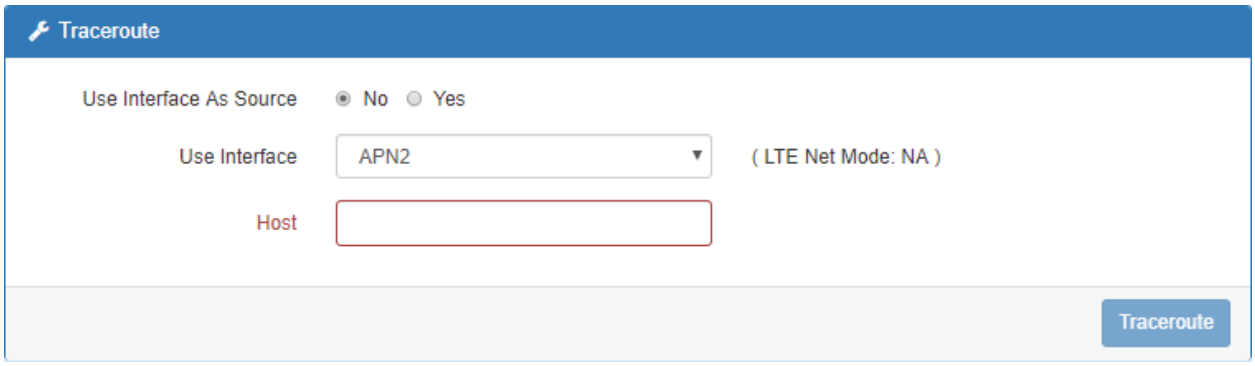
Please assign the Host you want to ping.



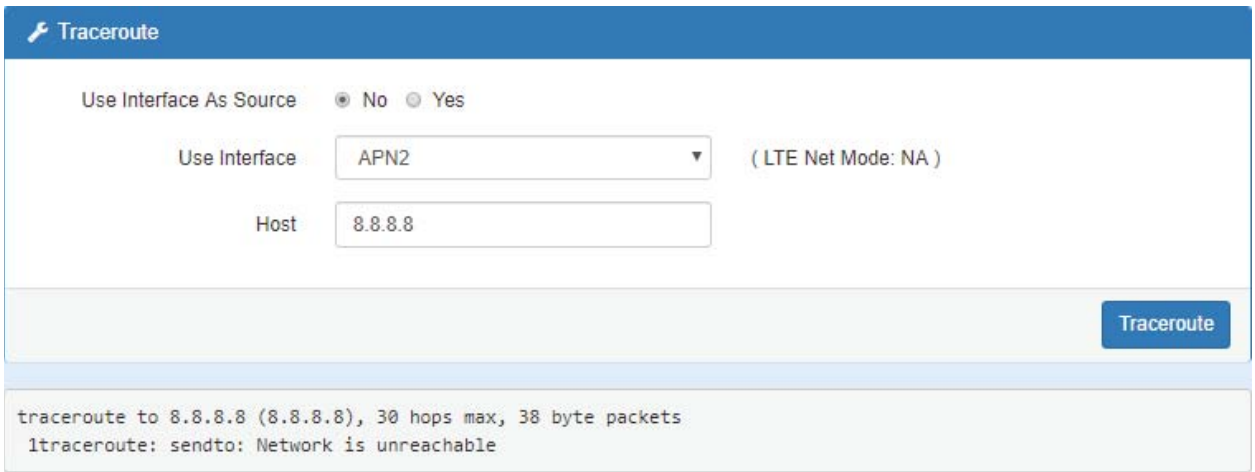
Diagnosis > Ping	
Item	**Description**
Use Interface As Source	Use or not use the Interface as source
Use Interface	APN1 / APN2
Host	The host name or the host IP address

15.2 Diagnosis > Traceroute

Please assign the Host **you want to** traceroute.



The result of the traceroute is as below.



Diagnosis > Ping	
Item	**Description**
Use Interface As Source	Use or not use the Interface as source
Use Interface	APN1 / APN2
Host	The host name or the host IP address

16 Configuration Applications

This section explains specific examples how to configure your applications.

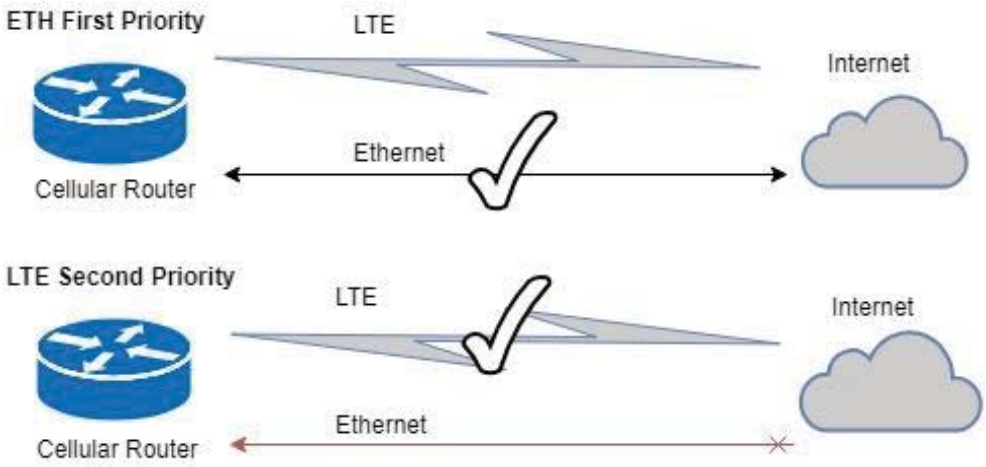
16.1 WAN Priority

You can select from ETH First, LTE Only, ETH Only or LTE First.

(1) WAN Priority > ETH First:

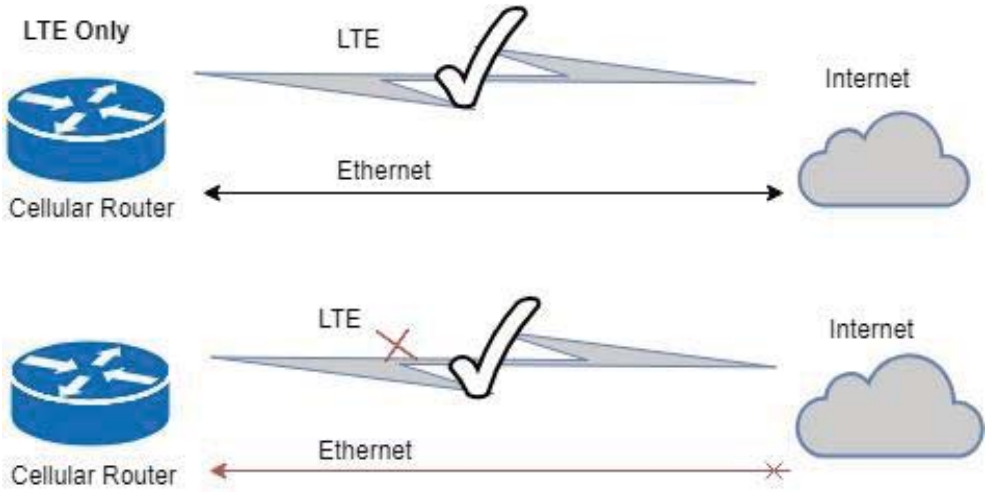
In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.

However, in case Ethernet is unplug or not able to access Internet (check by ping), the router would route network packages through LTE network.



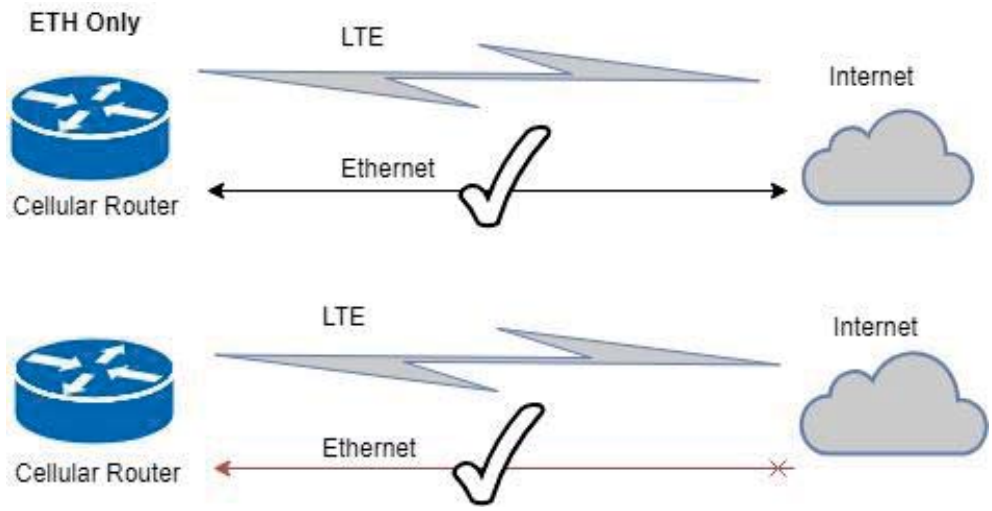
(2) WAN Priority > LTE Only:

In this mode, the router only routes network packages through LTE.



(3) WAN Priority > ETH Only:

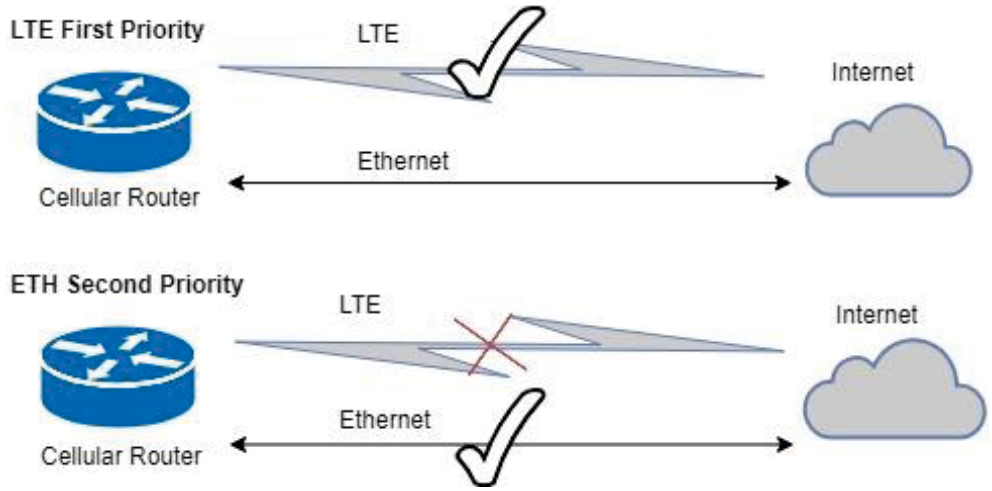
In this mode, the router only routes network packages through Ethernet.



(4) WAN Priority > LTE First:

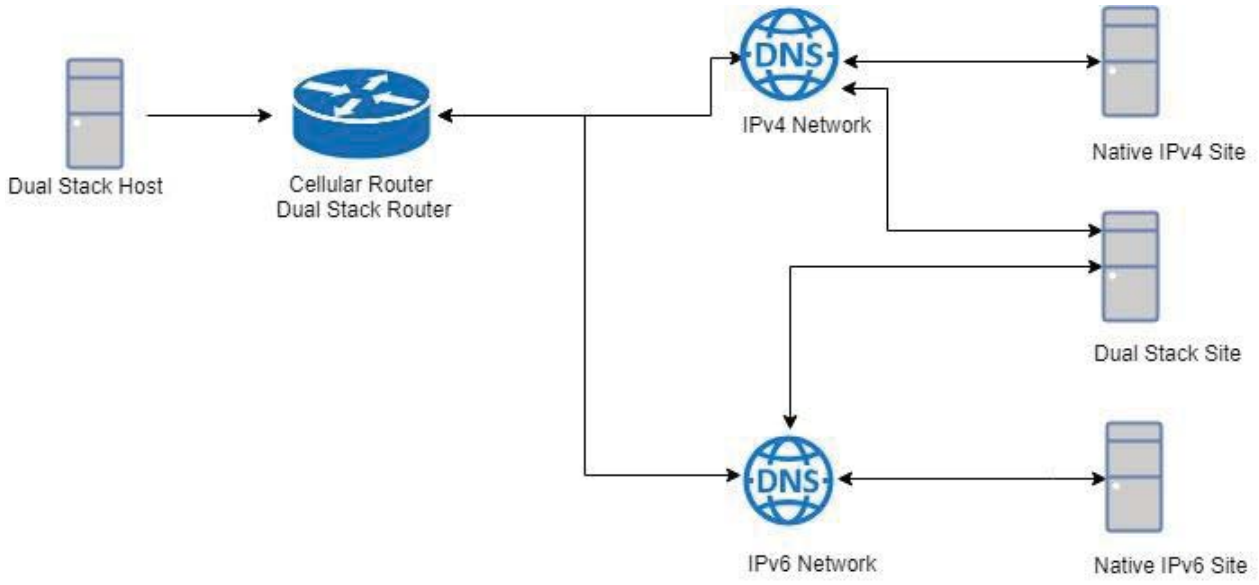
In case both Ethernet and LTE can access Internet, the router would route network packages through LTE.

However, in case LTE is unplug or not able to access Internet (check by ping), the router would route network packages through Ethernet network.



16.2 LAN > IPv4/IPv6 Dual Stack

The router supports IPv4/IPv6 dual stack by default, it means IPv4 packages route to IPv4 network and IPv6 route to IPv6 network.



Since IPv6 is global IP, there is no NAT between WAN site and LAN site. One device only needs one global IPv6. There is IPv6 firewall protection in the router by default. Only the IPv6 packages come from LAN site device and got reply back.

Status

Attr.	Current SIM	Backup SIM
SIM Card	SIM1	SIM2
Modem Status	Ready	Not Inserted
Operator	Chunghwa Telecom	
Modem Access	FDD LTE	
IMSI	466924290307730	
Phone Number		
Band	LTE BAND 7	
Channel ID	3050	0
IPv4 Address	10.167.236.11	
IPv4 Mask	255.255.255.255	

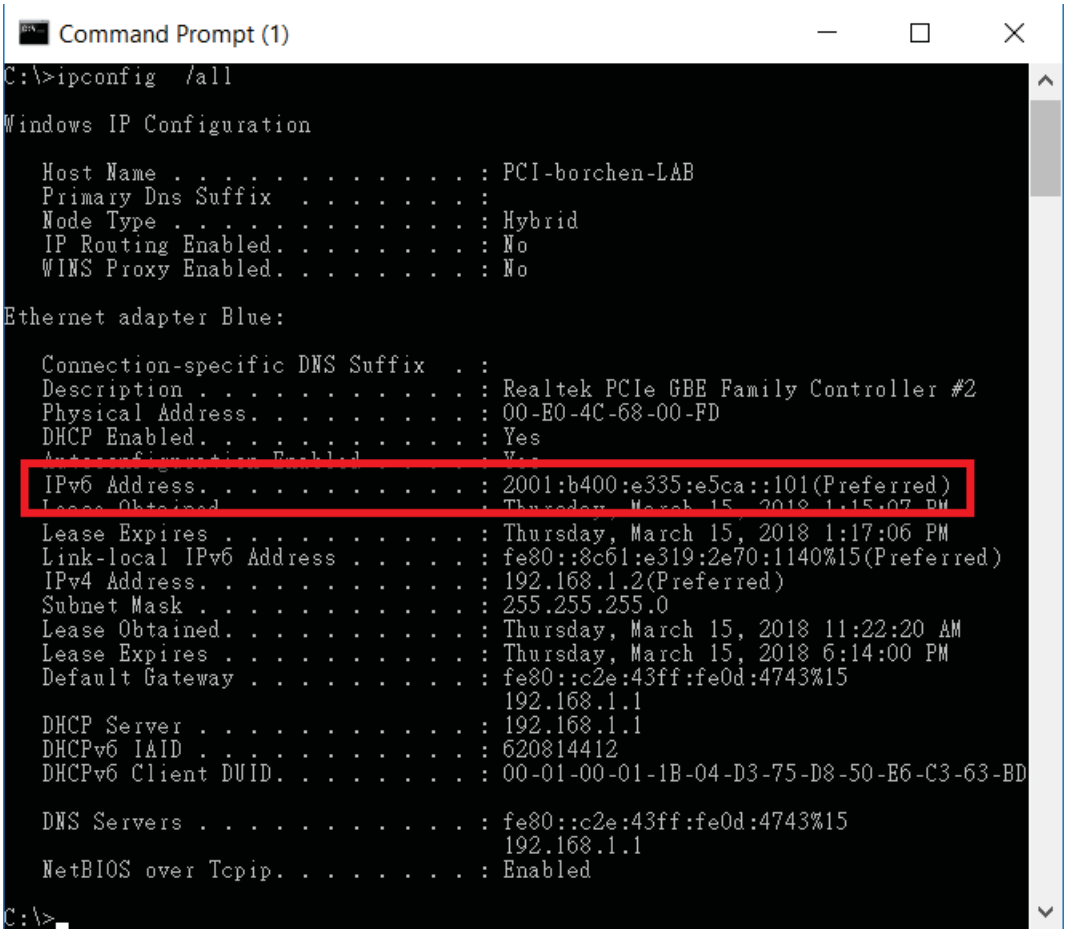
Ethernet WAN

Attr.	Value
IPv4 Address	192.168.11.176
IPv4 Mask	255.255.255.0

Ethernet LAN

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b021:4a::100

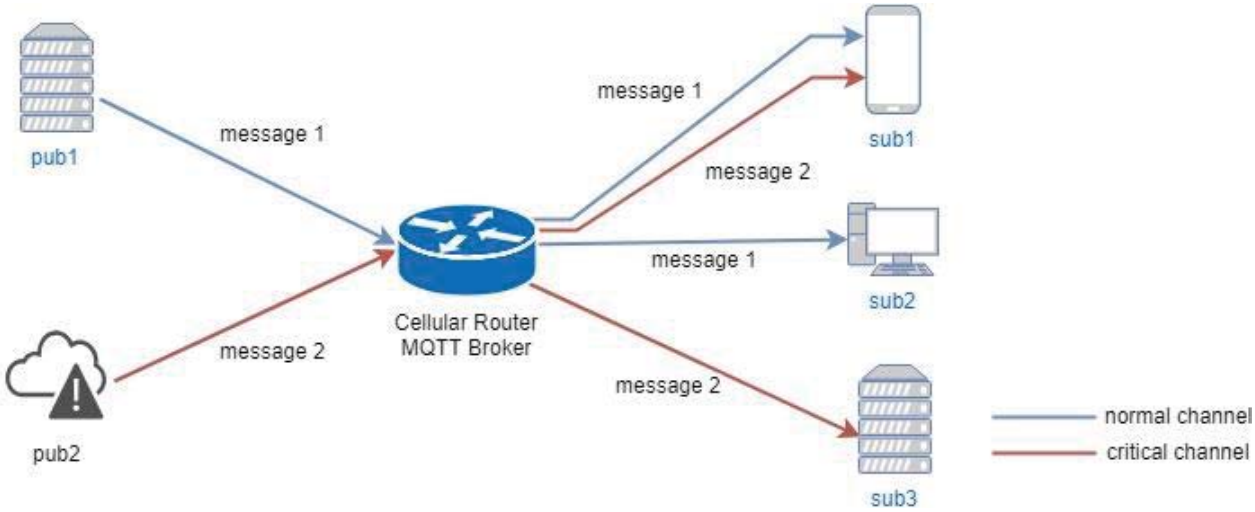
The router automatically detects IPv6 environment and query IP. After the IP is obtained successfully, it will distribute to LAN site hosts.



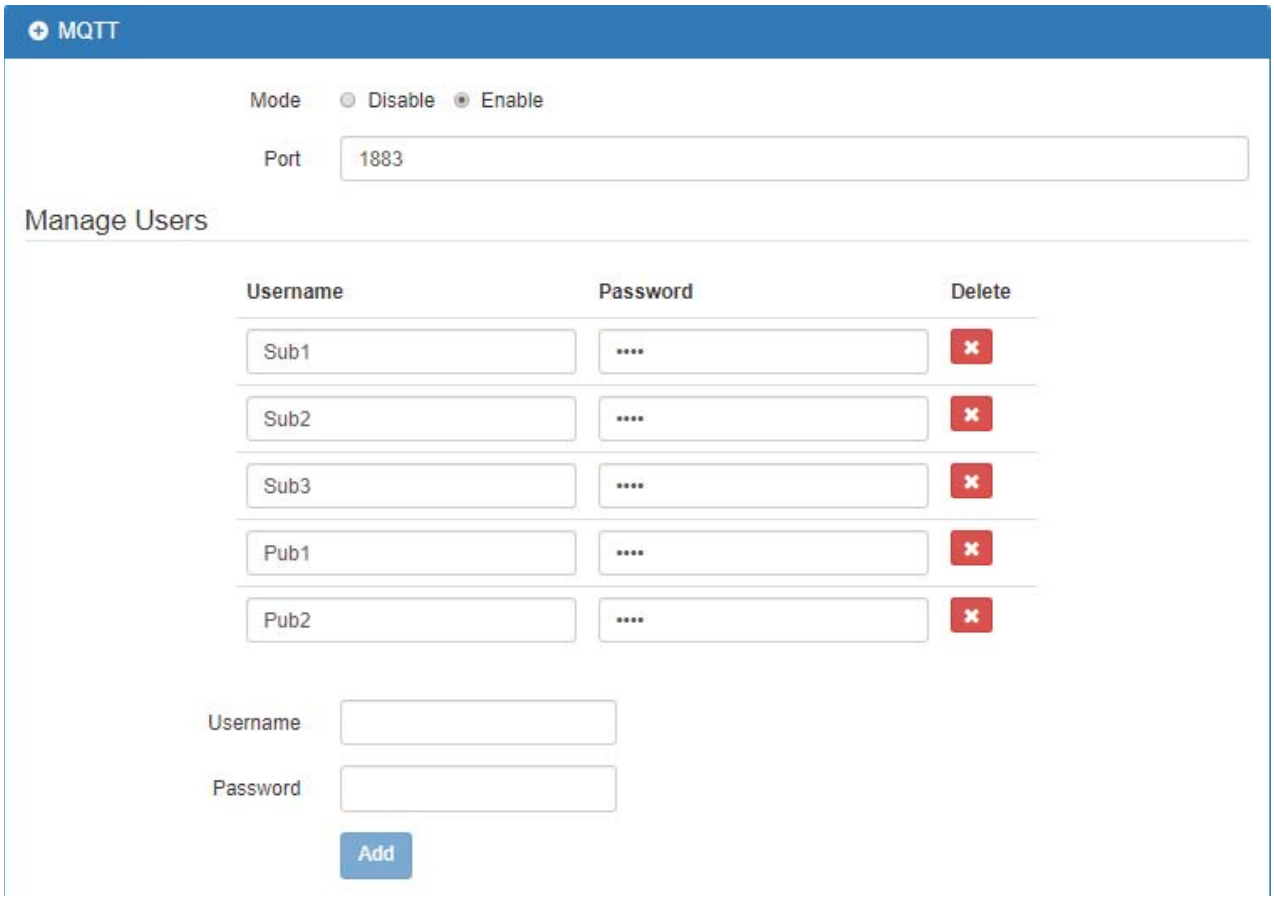
16.3 MQTT Broker

The cellular router provides the MQTT broker feature which allow the MQTT client sending the message within specific topic (channel).

By default, the cellular router does not allow anonymous to read/write the MQTT topic (channel).



Thus, you need to create the account with username and password for MQTT client in the web UI.

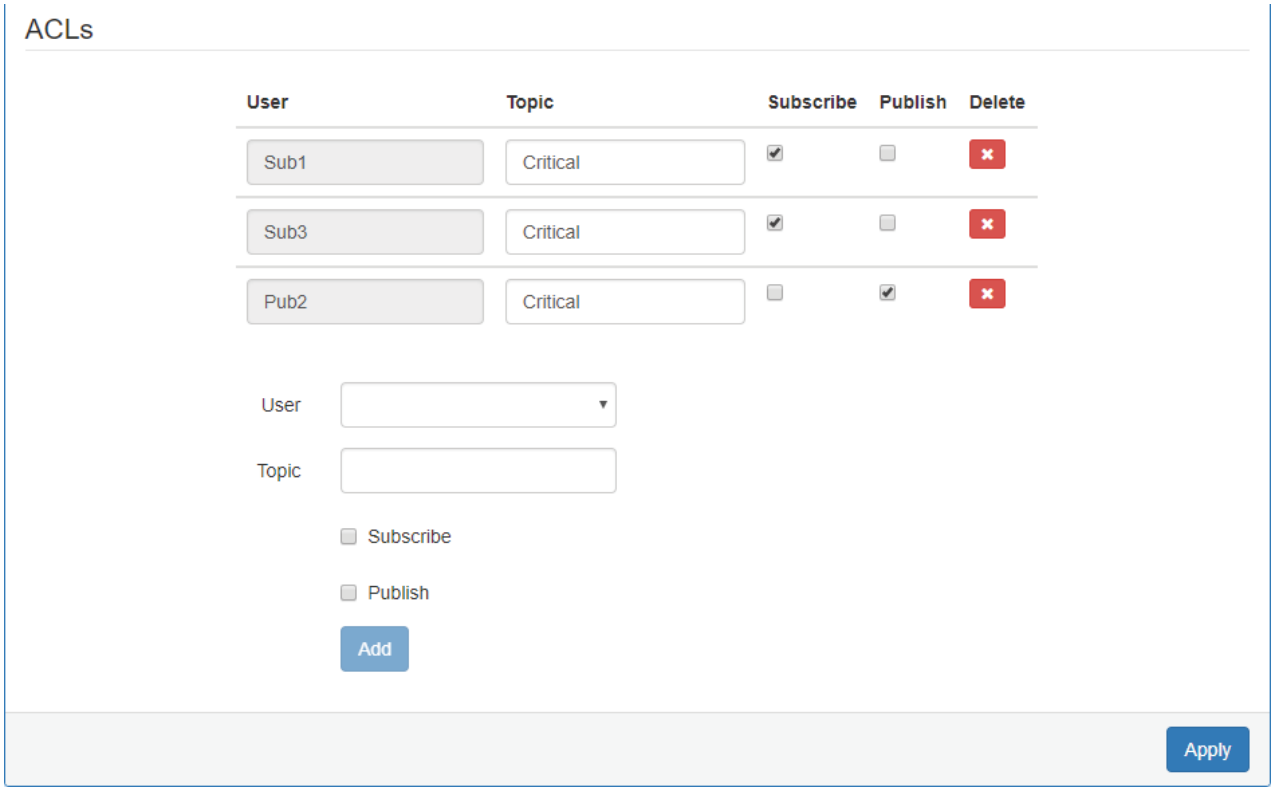


The **Manage Users** section will show all created users. Each user can use the **delete** button to delete it. For the ACL control, you can specify what topic should be limited.

For example, we set the publisher **pub2** to write the critical topic.

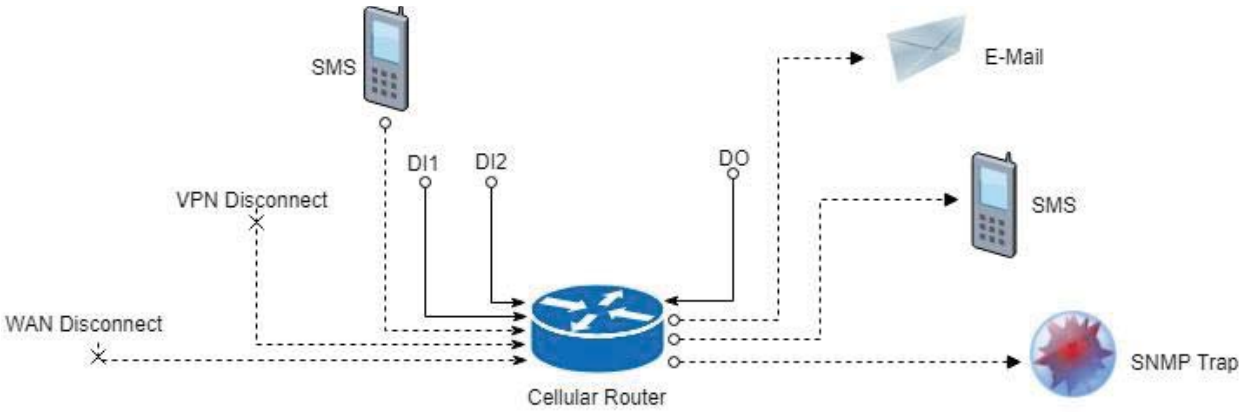
Additionally, we also the subscribers **sub1** and **sub3** can read the critical topic.

Thus, when **pub2** is sending the message only the **sub1**, the **sub3** can receive it.



16.4 Alarm Configuration

After you enable alarm, all the selected alarm input events would trigger selected alarm output.

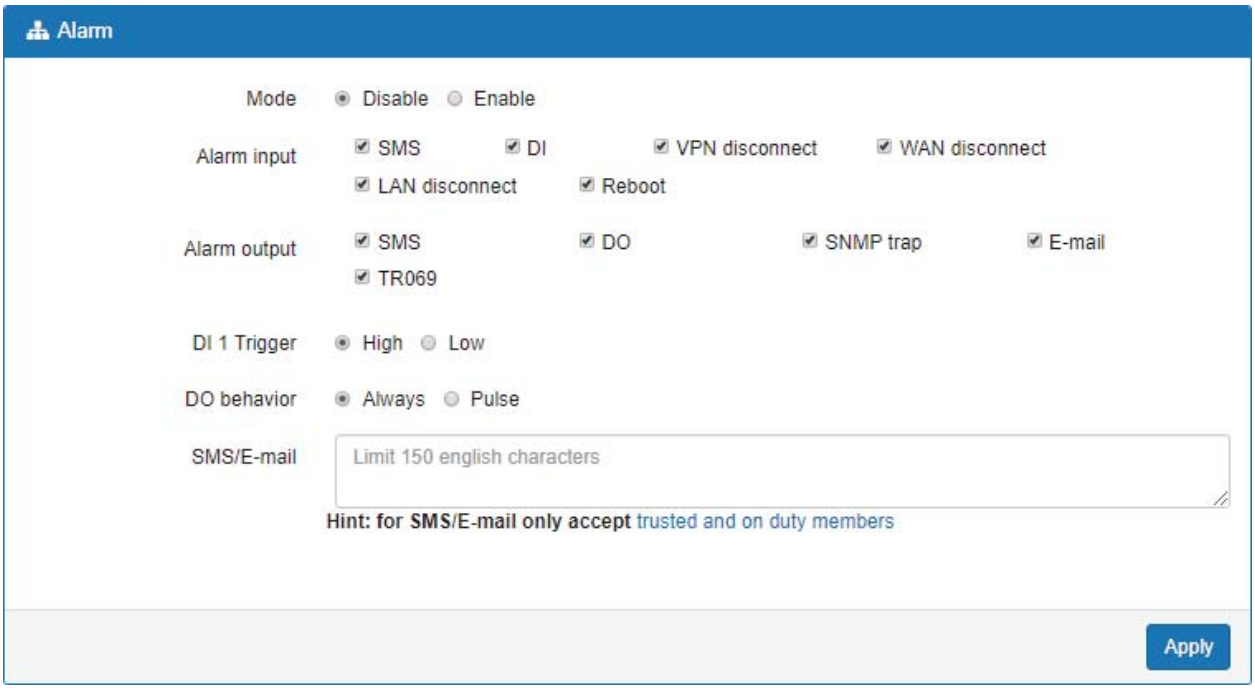


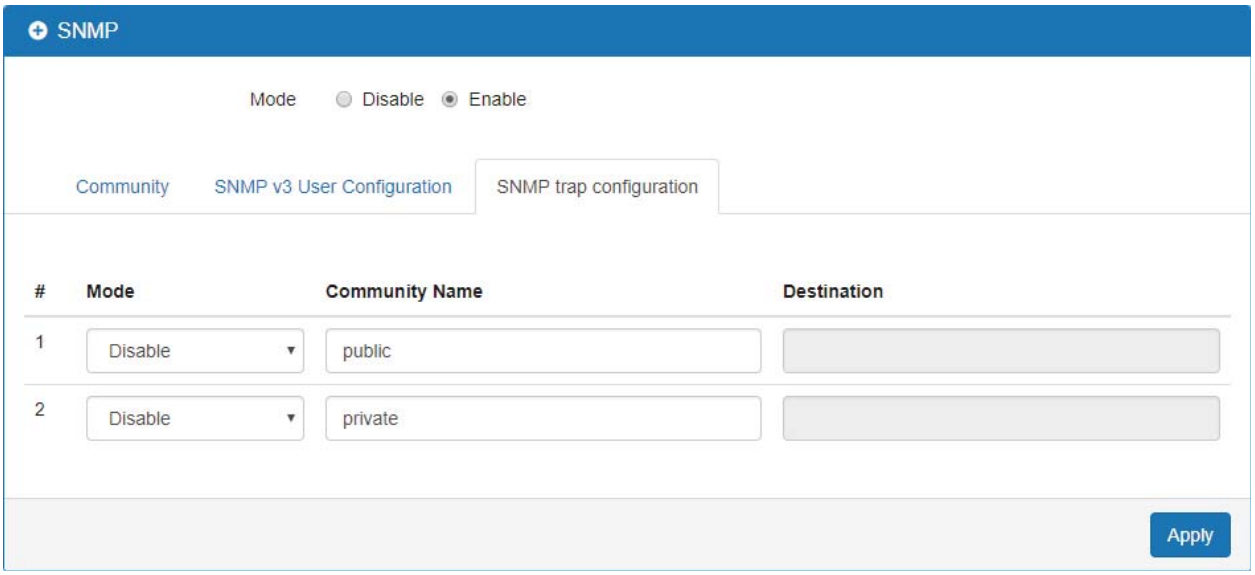
(1) Alarm Input:

- The alarm would be triggered when DI1/DI2 show(s) high signal.
- The user's phone number is in device contact phone book can send a SMS to device SIM card to trigger alarm.
- VPN / WAN disconnect would trigger alarm no matter which interface is currently using.

(2) Alarm Output:

- In case of SMS is selected then only user's phone number is in selected group and on selected working day would receive alarm SMS.
- In case of DO is selected, please make sure your DO is connected to your alarm device.
- In case of SNMP trap is selected, please make sure you enable SNMP trap (**Service -> SNMP**) and fill our server IP.





16.5 Open VPN Configuration

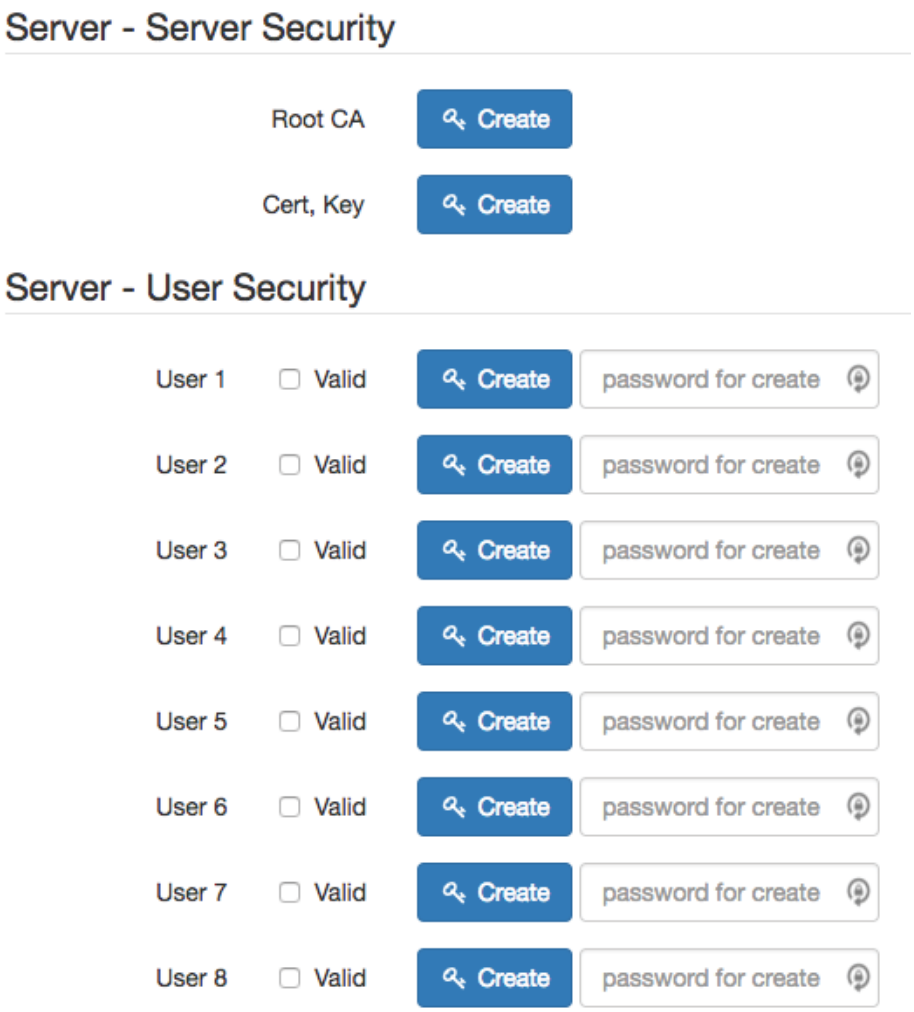
Generic setup

For Open VPN configuration, use the certificate to authenticate the VPN connection.

Thus, you need to generate the required files for Open VPN server or import the required file to Open VPN client.

16.5.1 Open VPN Server Mode

Open VPN server certificate generation

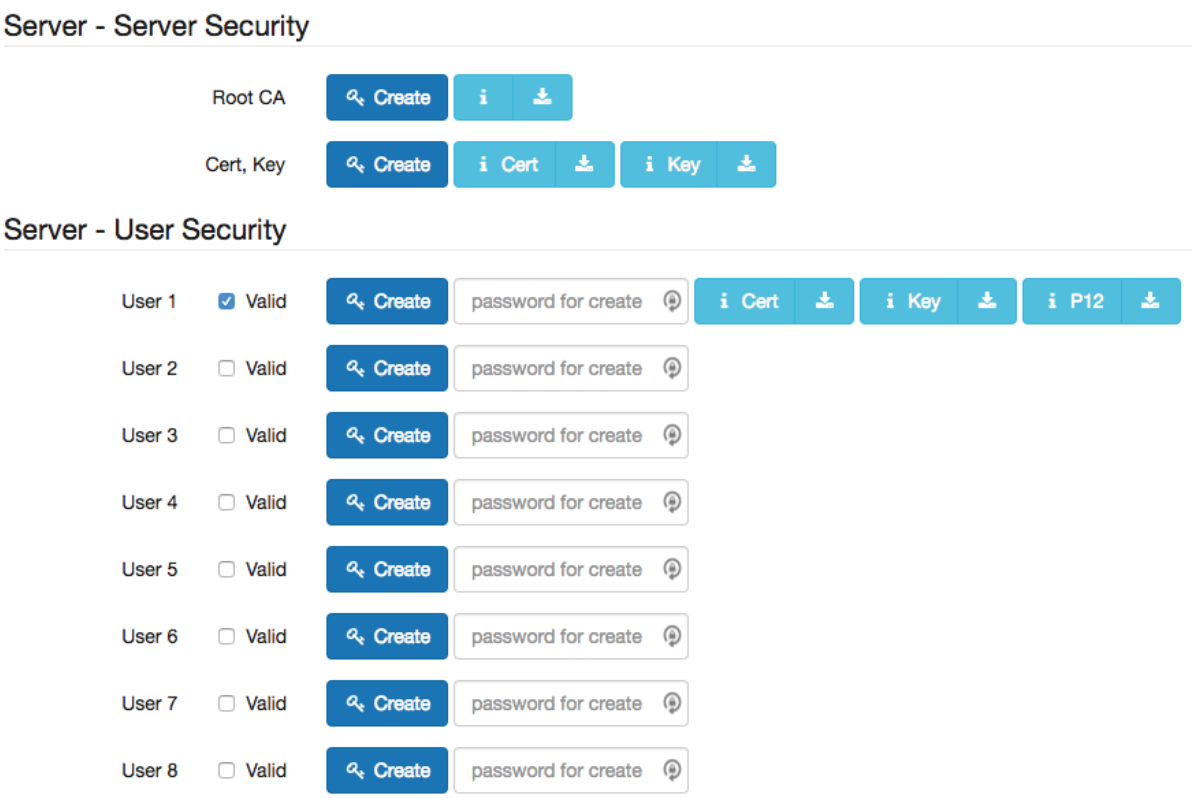


For the Open VPN server mode, the Open VPN web UI provides the buttons to generate the required files. The files include **Root CA**, **Cert**, **Key** and **Open VPN** client files. The file will be generated when you click the corresponded **Create** button.

Note: The **Cert**, **Key** generation will take around 10 minutes.

To generate the Open VPN client files, you need to type the password to create it.

The password will be used in the Open VPN client when the client uses **PKCS#12** to authenticate the VPN connection. After the generation, the web UI shows the below picture.



And you can click the info button to show the detail for each files, or click the download button to download the file to PC.

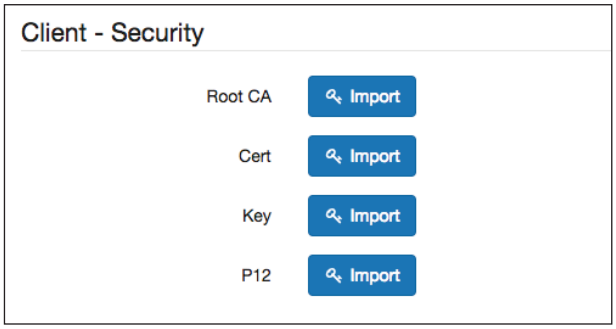
16.5.2 Open VPN Client Mode

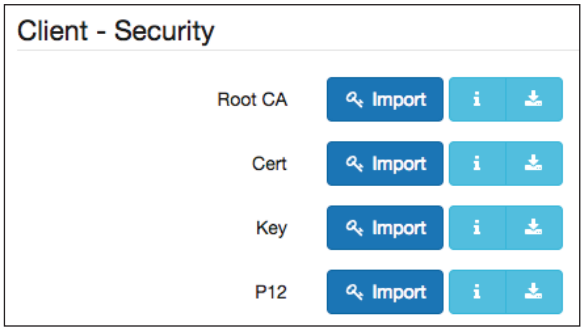
Open VPN client certificate import

For the Open VPN client mode, the Open VPN web UI provides the buttons to import the required files. The Open VPN client can use the **Root CA**, **User Key** and **User Cert** files from Open VPN server to authenticate the VPN tunnel. Or just only use the **PKCS#12 (P12)** file from Open VPN server to authenticate it.

Note: The PKCS#12 files will contain the Root CA, User Key and User Cert.

When the files are imported, the web UI is as shown in the right-bottom picture.

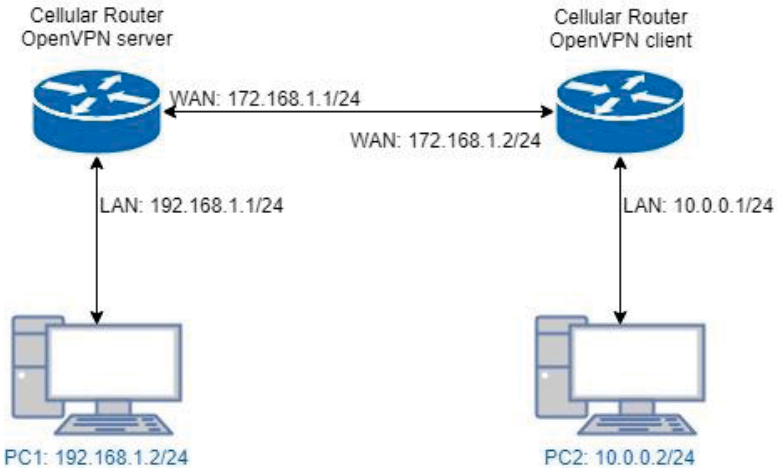




Same as Open VPN server part, you can use the info/download buttons to get the information of file or download the file to PC.

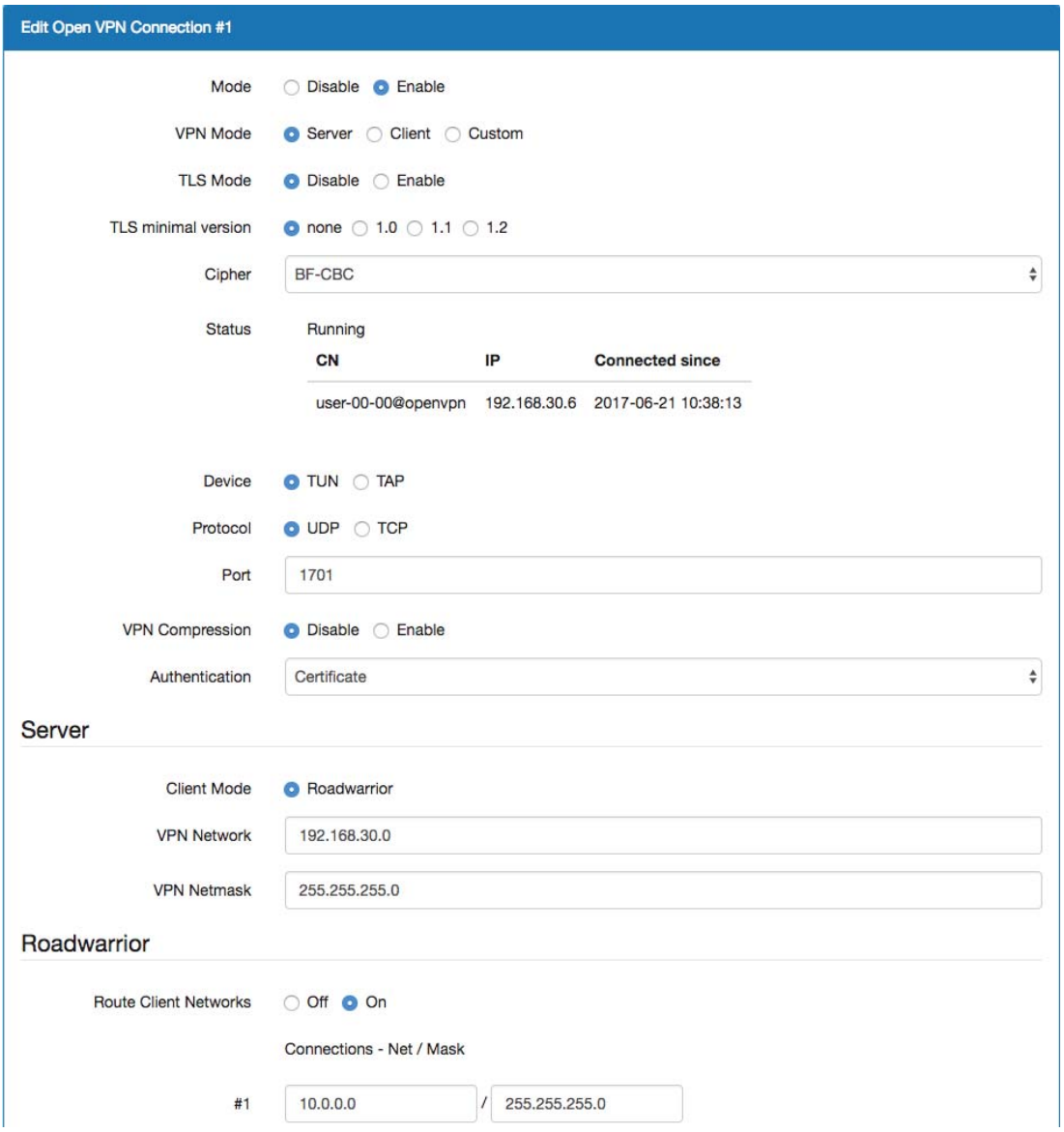
16.5.3 Open VPN Net-to-Net

You can use the Open VPN VPN tunnel to make the PC1 and PC2 communicate each other.



(1) Open VPN server configuration

For the Open VPN server side, the basic setting is as shown in below figure.



The **VPN Network** and **VPN Netmask** are required fields.

Note: The **VPN Network** should be network ID (e.g. **192.168.30.1** is invalid setting.)

When PC1 and PC2 communicate each other, the Route Client Networks should be enabled.

And add the LAN information of Open VPN client side, in this case the **#1** route will be **10.0.0.0** and **255.255.255.0**

Note: The **#1** route means the routing information for **User 1**.

If all settings set up properly, the web UI will show the **Apply OK** and the Open VPN server status should be **Running**. When Open VPN Client mode is connected, the status will show the information which client is connected, IP address and connected time.

Status Running

CN	IP	Connected since
user-00-00@openvpn	192.168.30.6	2017-06-21 10:38:13

In the status, the **CN** field will indicate which client is connected and the **user-00-00@Open VPN** value is from the **User 1** certificate information. You can check it by clicking the information button, the web UI will display the window as the below figure.

192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_i...

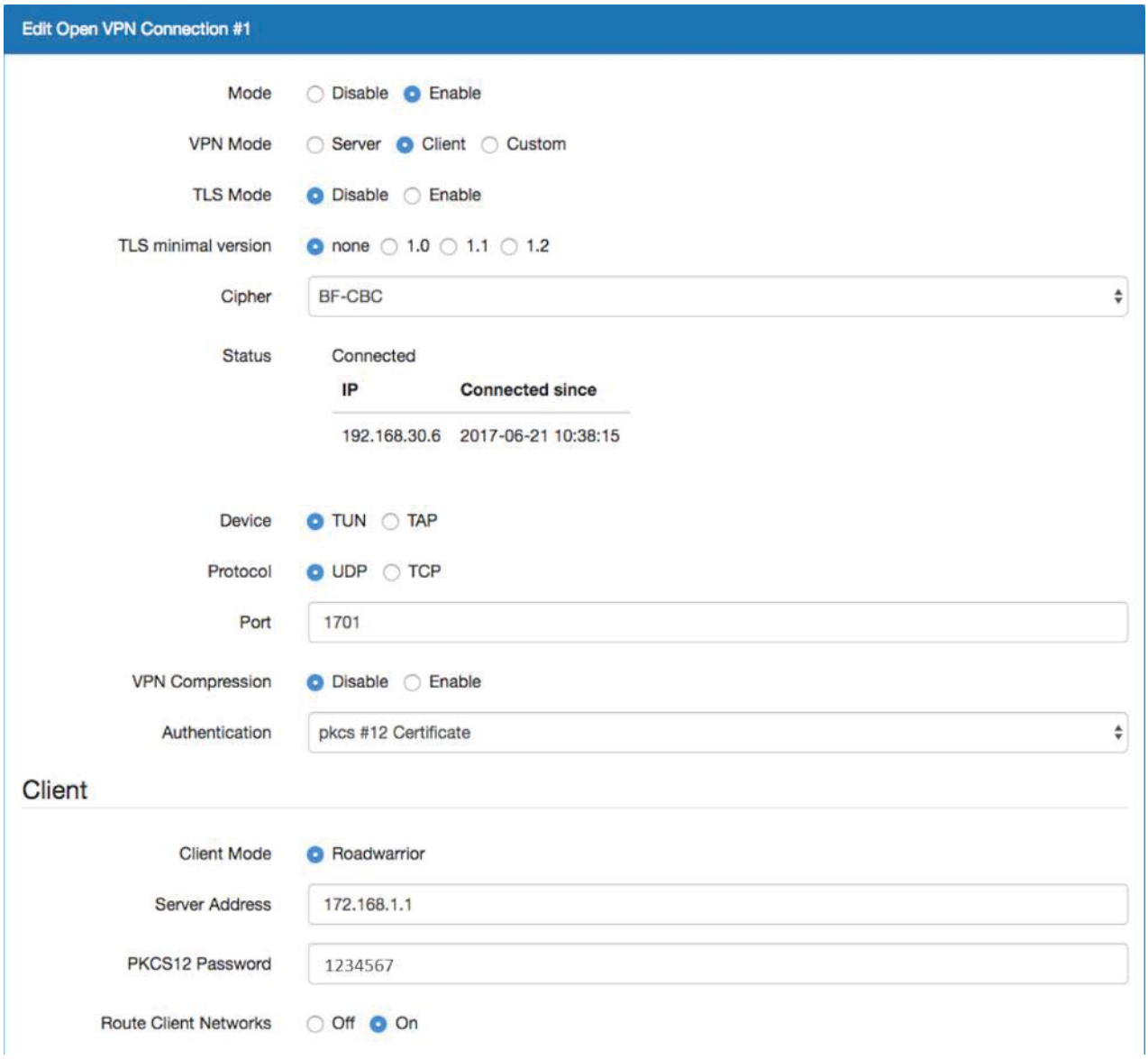
192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_id...

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CH, O=strongSwan, CN=OpenVPN
        Validity
            Not Before: May  9 06:34:08 2017 GMT
            Not After : May  7 06:34:08 2027 GMT
        Subject: C=CH, O=strongSwan, CN=user-00-00@openvpn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:b1:ca:c7:74:18:70:ed:71:88:9e:c4:ba:d1:
                    c4:09:52:b8:11:d7:17:00:e4:dd:e5:a7:f4:e1:f6:
                    1c:10:b5:0c:d2:27:e7:f8:63:cb:e2:30:78:6c:ab:
                    e3:eb:bd:08:a0:64:ed:1c:6d:97:8f:75:be:21:0d:
                    47:1f:ca:66:6e:52:a8:c2:40:98:01:21:73:73:b5:
                    62:c7:ab:a7:39:6b:94:7b:db:b4:a4:45:33:39:00:
                    5b:92:f6:05:4c:18:e1:7d:1b:0b:35:ed:3b:da:0e:
                    1c:f3:0e:db:04:e0:90:53:da:f5:87:91:d9:af:0f:
                    3d:82:c3:12:ec:4a:e2:ed:77:d9:ca:89:2a:73:c9:
                    e7:4f:a3:97:ff:97:f1:c4:f0:de:12:c0:ae:12:73:
                    3f:63:30:dd:e8:87:97:59:34:e7:a7:1f:a0:53:c5:
                    b1:f6:4d:10:2f:96:bd:f1:80:cc:62:5a:66:d8:30:
                    29:c6:f3:fa:7a:69:4a:6a:67:0b:85:e7:8f:76:a4:
                    fc:47:af:e5:1e:76:96:1c:f0:2b:64:d7:d0:02:50:
                    63:43:ae:65:ad:88:73:b0:19:67:08:a4:60:6a:f1:
                    03:93:62:f1:e3:0a:b3:70:82:dc:8b:85:a4:95:98:
                    fb:f5:f8:81:2b:a5:55:8a:f7:1c:15:41:c2:f5:8b:
                    ae:ed
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         54:fd:09:0b:23:5b:d1:22:e3:17:1e:de:5c:48:1c:30:30:c7:
         01:d8:6d:46:f4:91:4c:84:16:35:ea:79:91:67:dc:91:63:88:
         6a:23:7b:fe:8c:e0:93:14:a1:1e:1d:32:c2:22:84:af:22:ff:
         a9:9d:2f:aa:b2:0c:8b:86:c3:bc:46:8e:9d:5c:f8:55:39:91:
         cc:03:17:40:e9:d5:bb:df:e9:34:aa:89:71:f7:ea:1c:78:78:
         99:38:ba:7b:ec:d7:de:1a:d0:a0:07:58:cc:8a:4a:cc:2e:54:
         b3:d9:46:03:8e:58:cb:ef:de:95:61:01:33:9f:40:4c:cb:1b:
         3e:3e:70:4a:07:62:8c:d4:f0:53:86:42:c7:13:30:a8:3a:76:
         d3:bf:9d:33:7b:50:c3:98:fd:f0:ed:2a:c3:00:b8:dc:e0:80:
         a9:4b:0c:e1:ad:fc:32:76:03:b8:2f:9f:2a:d1:bb:1b:e7:cb:
         62:d2:63:be:7c:21:ac:b5:91:14:55:96:fc:67:94:cc:1f:7b:
         82:12:e6:84:da:fe:12:3e:73:bf:62:bb:1a:14:57:45:ce:28:
         95:e1:1f:d9:86:cb:36:c6:4d:b8:04:af:f6:0e:f4:f4:31:ba:
         6d:ef:cc:75:bc:0e:db:19:c7:c2:2c:b3:62:60:c2:88:d9:a3:
         cf:d4:8b:25
-----BEGIN CERTIFICATE-----
MIIC5zCCAc8CAQEwDQYJKoZIhvcNAQELBQAwNDELMAkGA1UEBhMCQ0gxEzARBgNV
BAoMCnN0cm9uZ1N3YW4xEDAOBgNVBAMMB09wZW5WUE4wHhcNMTcwNTA5MDYzNDA4
WhcNMjcwNTA3MDYzNDA4WjA/MOswCOYDVOOGEwJDSDETMBEGA1UECgwKc3Rvb25n
```

The CN information of user certificate is as shown in the subject field.

(2) Open VPN client configuration

For the Open VPN client side, the basic setting is as below figure.



The **Server Address** is required field, which indicate the Open VPN server address which Open VPN client try to connect. And the **PKCS12 Password** only works when selected the **pkcs #12 Certificate** authentication option.

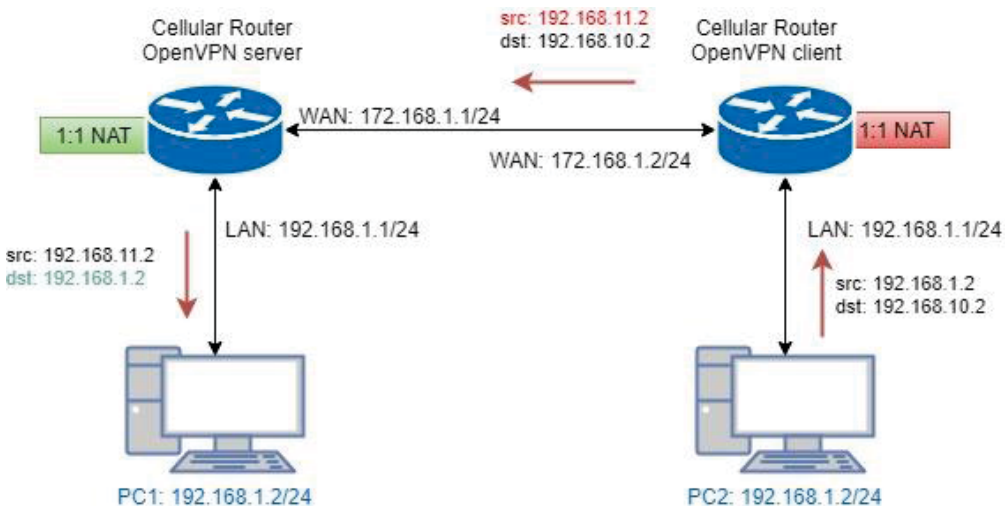
This option requires the P12 file which generated from Generic Setup Open VPN server part.

The password also be set on the Generic Setup Open VPN server part.

If you use the Certificate authentication option, the Open VPN client will require the **Root CA**, **User cert** and **User key** files.

Same as the Open VPN server configuration part, Open VPN client web UI also provides the status information. When all settings set up properly, the status will change from **Idle** to **Running**. When Open VPN tunnel is created, the status shows **Connected** and the information for IP address and the time.

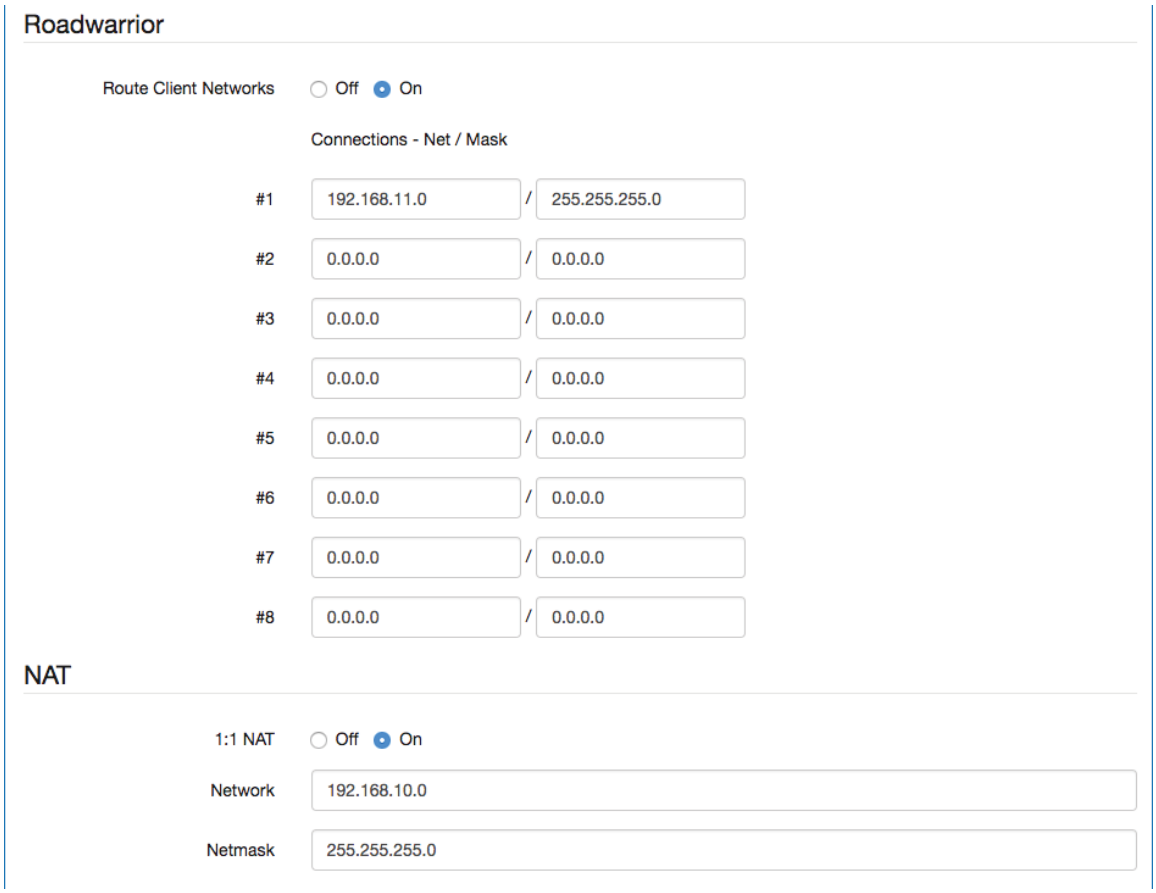
16.5.4 Open VPN 1:1 NAT



For the net-to-net part, the Open VPN server LAN network and the Open VPN client LAN network are different. But some time, the LAN network will be same for both sides.

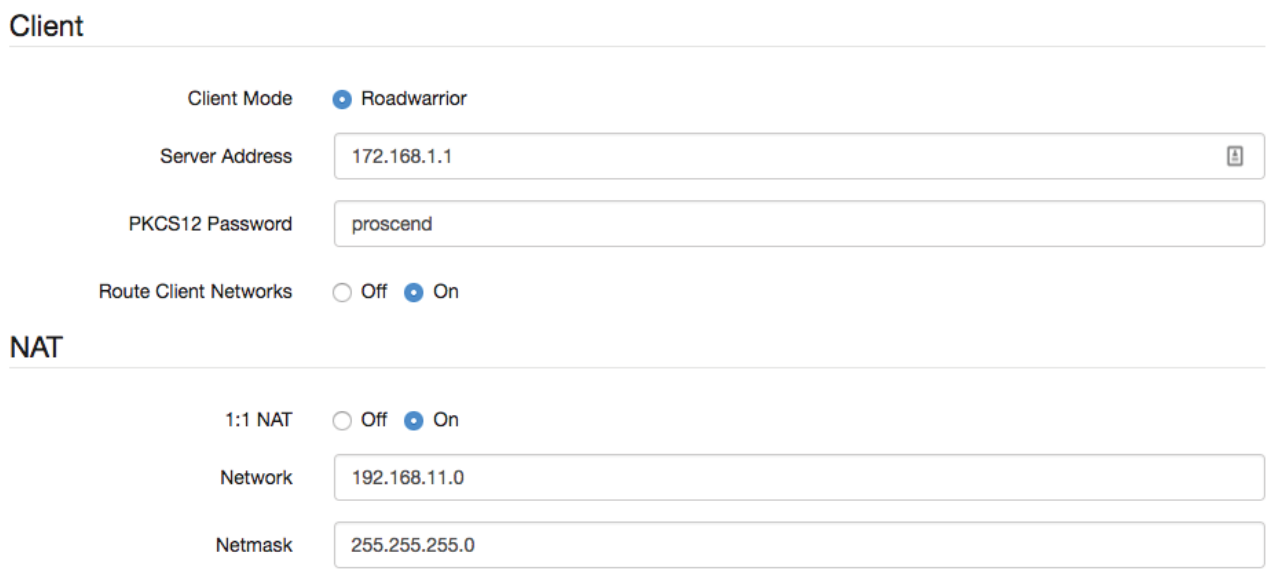
When this situation occurred, the routing rules will be ambiguous that will result in the PC1 and the PC2 can't communicate each other. Thus, the router Open VPN provides the 1:1 NAT feature. The feature will convert the conflict subnet to different subnet. In this case, you can use 1:1 NAT feature to convert the Open VPN server and client side LAN network.

For the Open VPN server side, we fill up the Network be **192.168.10.0** and Netmask **255.255.255.0**. The setting will make the router convert the Open VPN server side LAN network from **192.168.1.0/24** to **192.168.10.0/24** when the VPN traffic is coming.

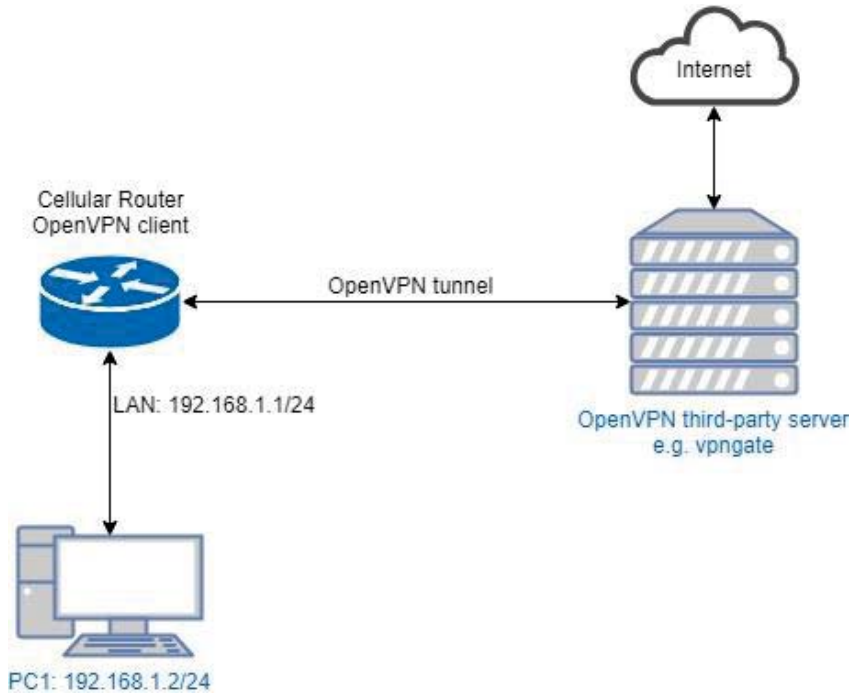


For the Open VPN client side, same as server side but we fill up the Network as **192.168.11.0**.

The setting will make router convert the Open VPN client side LAN network from **192.168.1.0/24** to **192.168.11.0/24** when the VPN traffic is coming.



16.5.5 Open VPN with third-party server



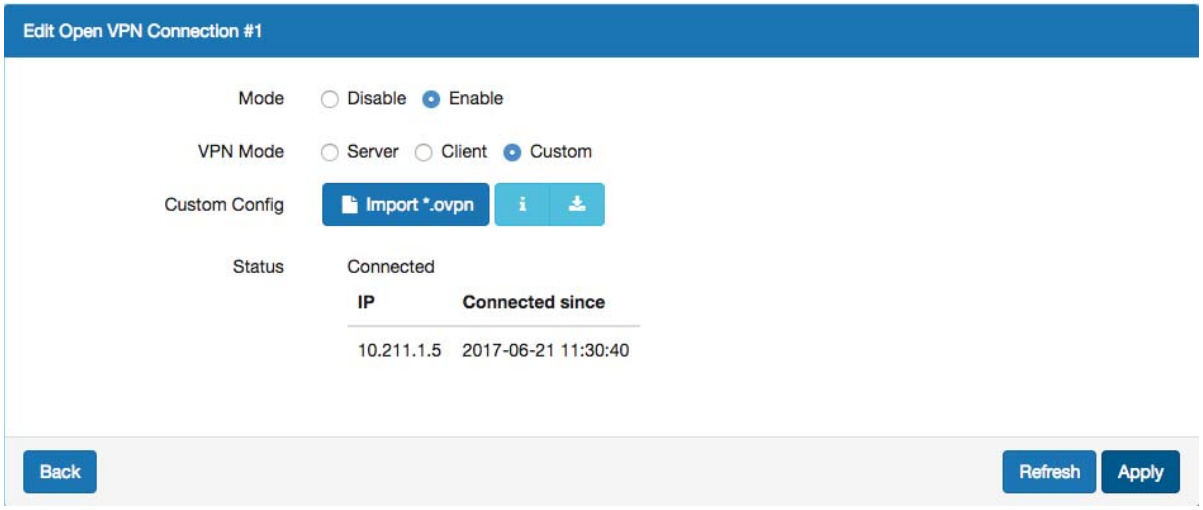
A VPN enables you to send and receive data across shared networks.

For some users, they will use the VPN to access the limited network service from the different country. But normally, the third-party Open VPN server will provide the **.ovpn** configuration files for the Open VPN client. The **.ovpn** is hard to convert to the cellular router Open VPN client configuration. So, we provide the **Custom** mode to make the user can easy use the **.ovpn** to set up the cellular router Open VPN client. The **Custom** mode provide the import button to allow user import the third-party Open VPN server **.ovpn** configurations file.

For example, use the Japan Open VPN server which provided by http://www.vpngate.net/en/.

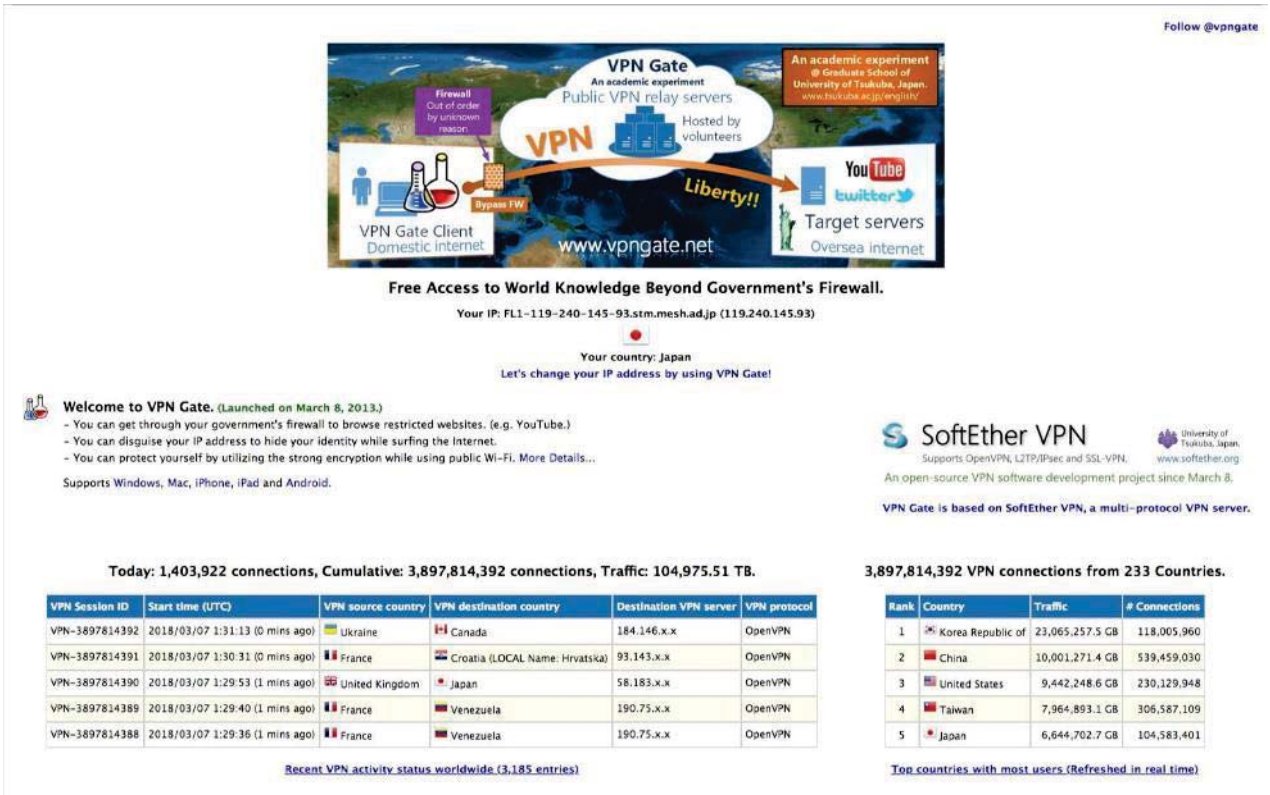
Firstly, download the ovpn configuration files from vpngate.net.

Additionally, use the Open VPN custom import button to import it. The result is as the below figure. If the **.ovpn** configuration file is correct, the web UI will show **Apply OK**.



If the third-party Open VPN server is reachable, the VPN tunnel will be established.

When the Open VPN VPN tunnel is established, the status shows **Connected** and the information for IP address and the time. In this moment, the PC1 can visit the http://www.vpngate.net and the web UI should indicate the PC1 in the Japan at now as the below figure.



16.5.6 Install Open VPN Access Server on Docker

Open VPN Access Server on Docker installation

Open VPN Access Server is a full featured secure network tunneling VPN software solution that integrates Open VPN server capabilities, enterprise management capabilities, simplified Open VPN Connect UI, and Open VPN Client software packages that accommodate Windows, MAC, Linux, Android, and iOS environments. Open VPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/ or private cloud network resources and applications with fine-grained access control.

All Open VPN Access Server downloads come with 2 free client connections for testing purposes.

$15.00 License Fee Per Client Connection Per Year. Support & Updates included. 10 Client minimum purchase.

The detail please look https://Open VPN.net/index.php/access-server/pricing.html

Quick Installation

- **Prerequisites**
- Ubuntu 16.04
- curl or wget should be installed

Install via curl

```
sh -c "$(curl -fsSL https://bit.ly/2GrzYyS)"
```

Install via wget

```
sh -c "$(wget https://bit.ly/2GrzYyS -O -)"
```

Install Docker on Ubuntu 16.04 64bit

Reference: https://docs.docker.com/engine/installation/linux/docker-ce/ubuntu/

Set up the repository

```
sudo apt-get remove docker docker-engine docker.io
sudo apt-get update
sudo apt-get install \
    apt-transport-https \
    ca-certificates \
    curl \
    software-properties-common
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository \
   "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
   $(lsb_release -cs) \
   stable"
```

Install Docker CE

sudo apt-get update

sudo apt-get install docker-ce

Install Open VPN Access Server by docker image

Reference: https://hub.docker.com/r/linuxserver/Open VPN-as/

```
sudo mkdir -p /Open VPN-as
sudo docker create --name=Open VPN-as \
    -v /Open VPN-as:/config \
    -e TZ="Asia/Taipei" \
    -e INTERFACE=enp3s0 \
    --net=host --privileged linuxserver/Open VPN-as
sudo docker start Open VPN-as
```

Check the Open VPN Access Server by visiting https://<server_ip_or_domain>:943

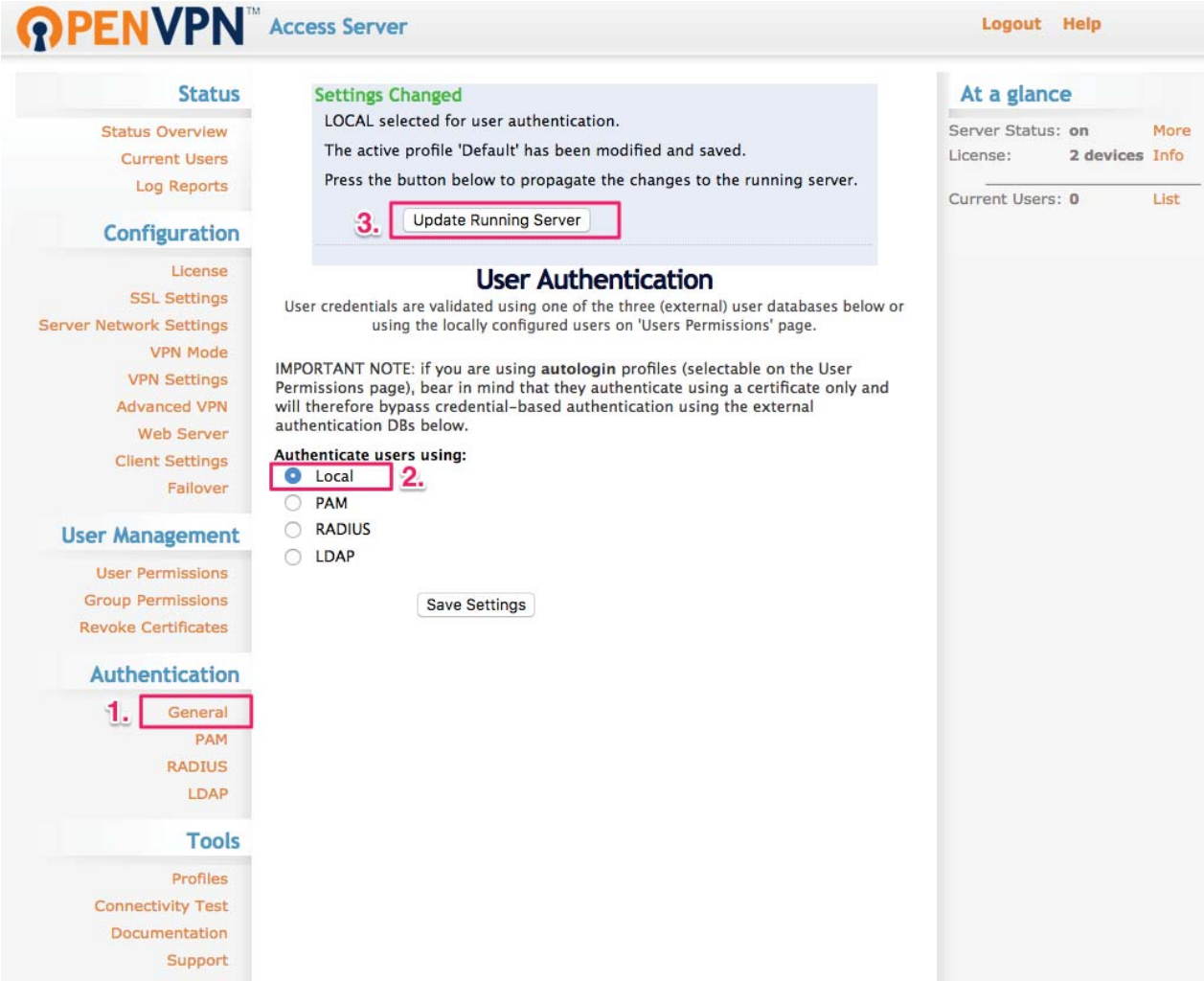
Setup Open VPN Access Server for Cellular Router

The admin page is https://<server_ip_or_domain>:943/admin

The default administrator username and password is admin/password.

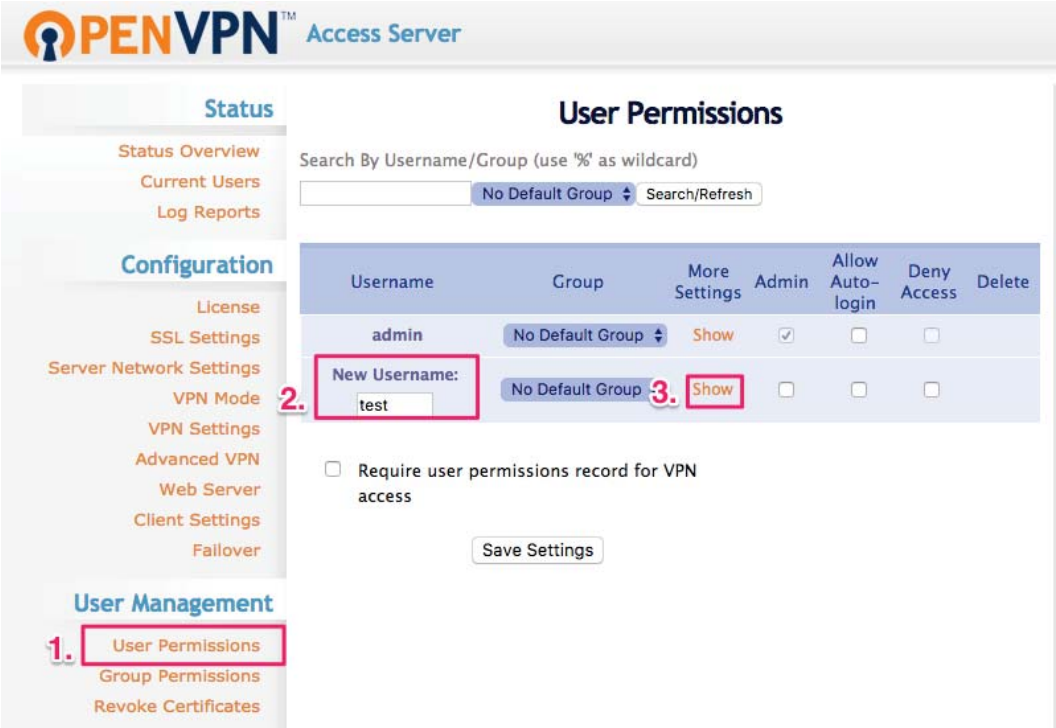
Login page:

After logged, please change the user authentication type to Local like the following figure.

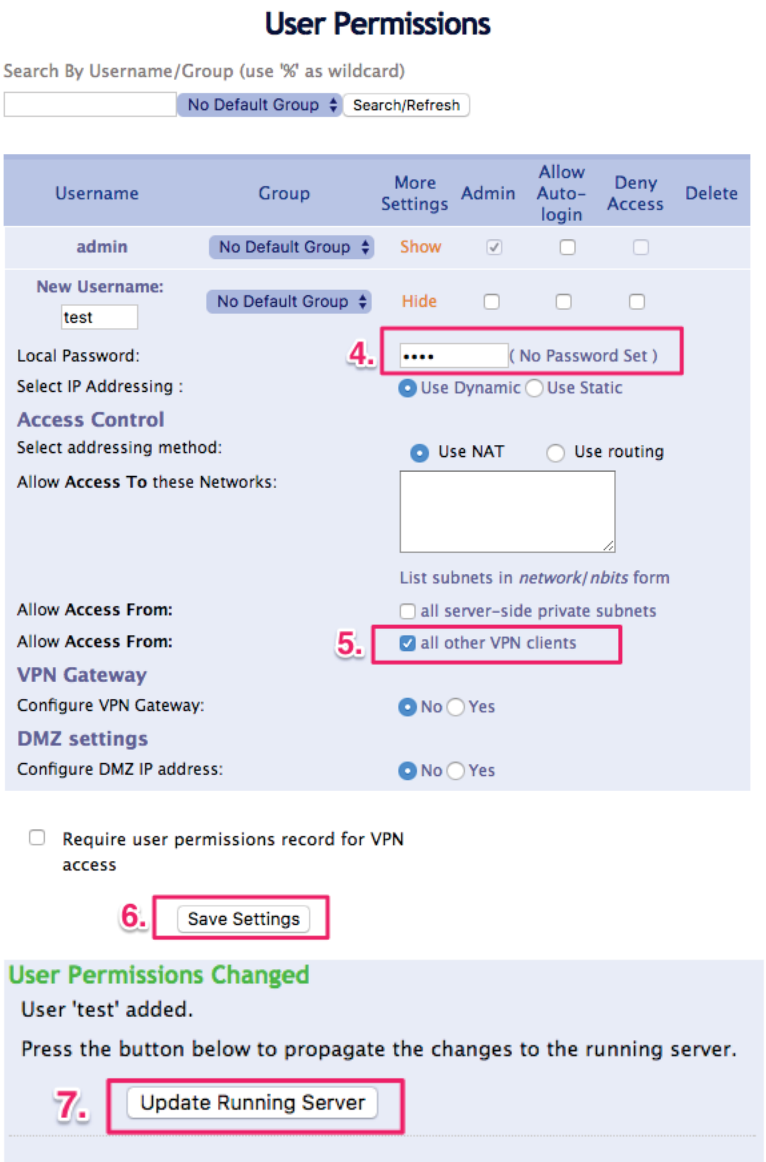


And switch to the User Permission page to create the user for Cellular Router.

(In this case, we use the test/test to be the example.)



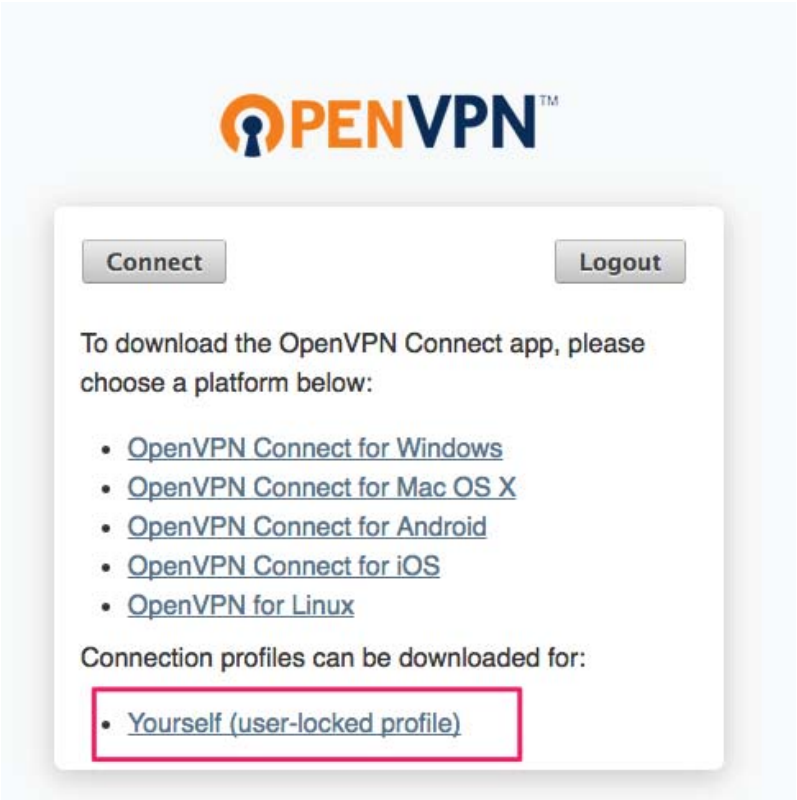
Also check the Access from all other VPN clients to make the Cellular Router could be reachable.



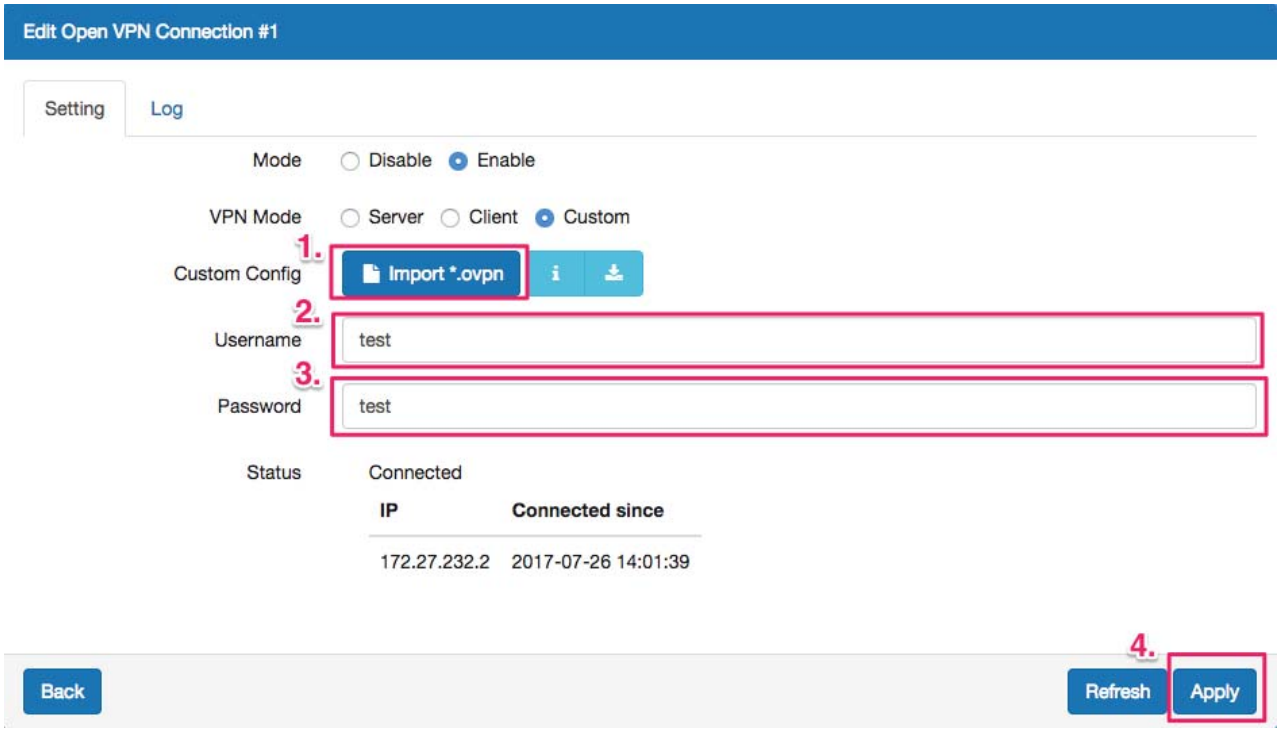
Setup Cellular Router Open VPN client

Use the user test/test to login https://<server_ip_or_domain>:943

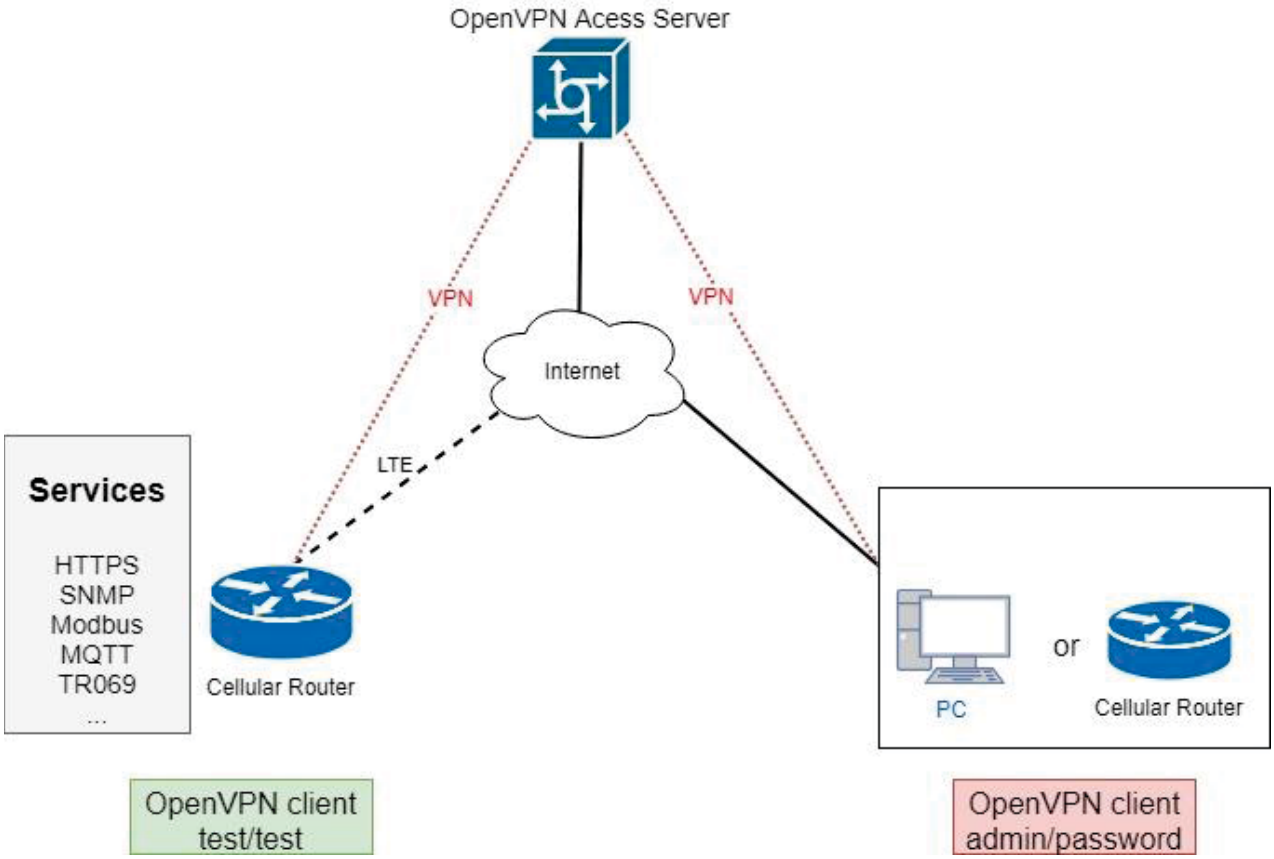
Please make sure to change the type from Connect to Login.



After logged, please download the .ovpn configuration by click the user-locked profile.



Upload the .ovpn configuration to Cellular Router Open VPN custom mode, and input the username and password.



When the VPN tunnel established, the Cellular Router can be managed/accessed by the other VPN clients.

16.5.7 Install Pritunl Open VPN server on Docker

Pritunl Open VPN server on Docker installation

Pritunl is a distributed enterprise vpn server built using the Open VPN protocol.

Quick Installation

- **Prerequisites**

- Ubuntu 16.04
- curl or wget should be installed

- **Install via curl**

sh -c "$(curl -fsSL https://bit.ly/2IpJN1X)"

- **Install via wget**

sh -c "$(wget https://bit.ly/2IpJN1X -O -)"

Install Docker on Ubuntu 16.04 64bit

Reference: https://docs.docker.com/engine/installation/linux/docker-ce/ubuntu/

Set up the repository

sudo apt-get remove docker docker-engine docker.io

```
sudo apt-get update
sudo apt-get install \
    apt-transport-https \
    ca-certificates \
    curl \
    software-properties-common
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository \
   "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
   $(lsb_release -cs) \
   stable"
```

Install Docker CE

```
sudo apt-get update
sudo apt-get install docker-ce
```

Install Docker compose

```
sudo apt-get install docker-compose
```

Install Pritunl Open VPN Server by docker compose

(1) Set up the basic environment by the following commands.

```
mkdir ~/pritunl
cd ~/pritunl
touch docker-compose.yml
```

(2) Copy and paste the following content to docker-compose.yml.

```
version: '2'
services:
  pritunl:
    image: jippi/pritunl
    volumes:
      - pritunl:/var/lib/pritunl
      - mongo:/var/lib/mongodb
    privileged: true
    network_mode: "host"
    ports:
      - "1194:1194/tcp"
      - "1194:1194/udp"
      - "80:80/tcp"
```

```
    - "443:443/tcp"
volumes:
  mongo:
  pritunl:
```

(3) Run the command docker-compose up -d to start the server

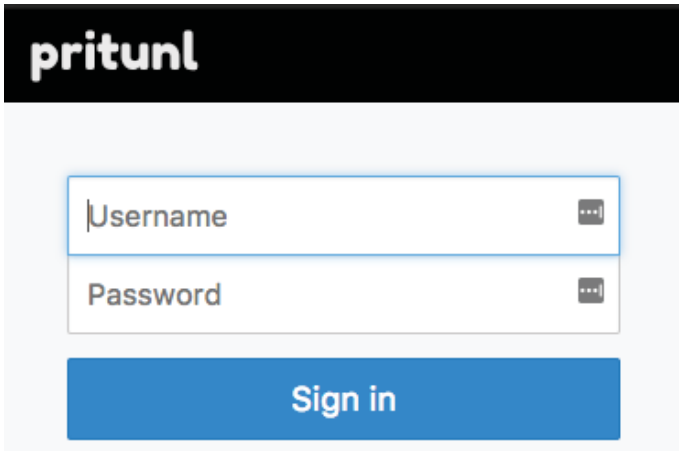
(4) Check the Pritunl Open VPN Server by visiting https://<server_ip_or_domain>

Setup Pritunl Open VPN Server for Cellular Router

The server will running on https://<server_ip_or_domain>.

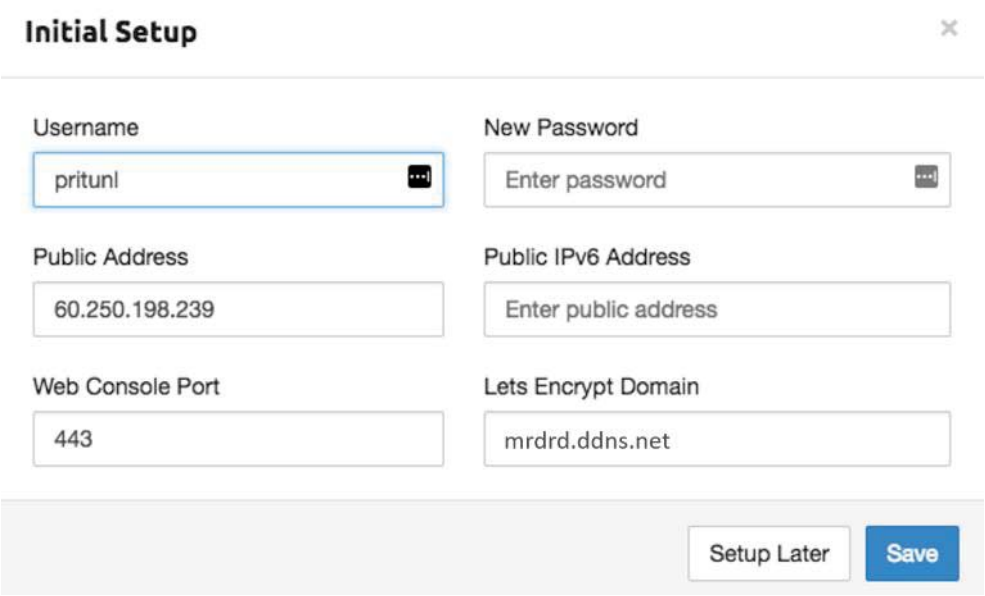
The default username/password is pritunl/pritunl.

Login Page:



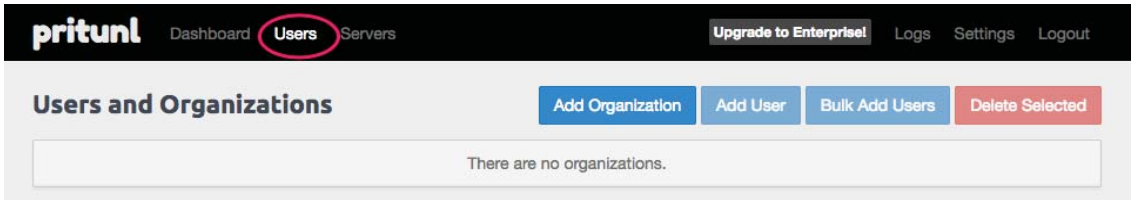
After logged, the server will ask you to do the initial setup. You can change the username and the password setting in this page.

Initial Setup:

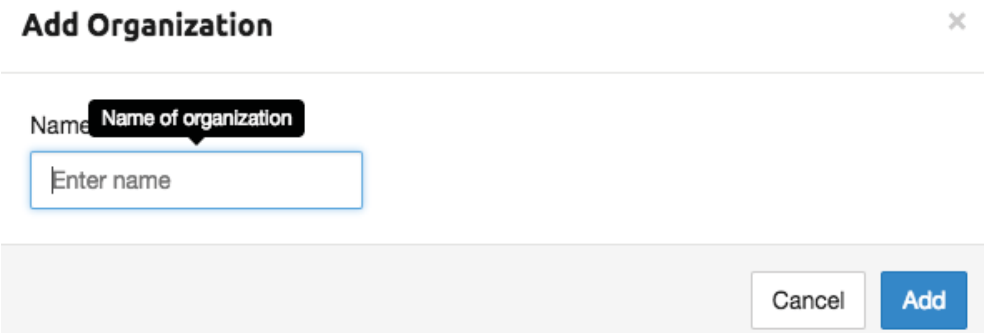


Open VPN user setup

Please navigate to the User page to setup the Open VPN user account.

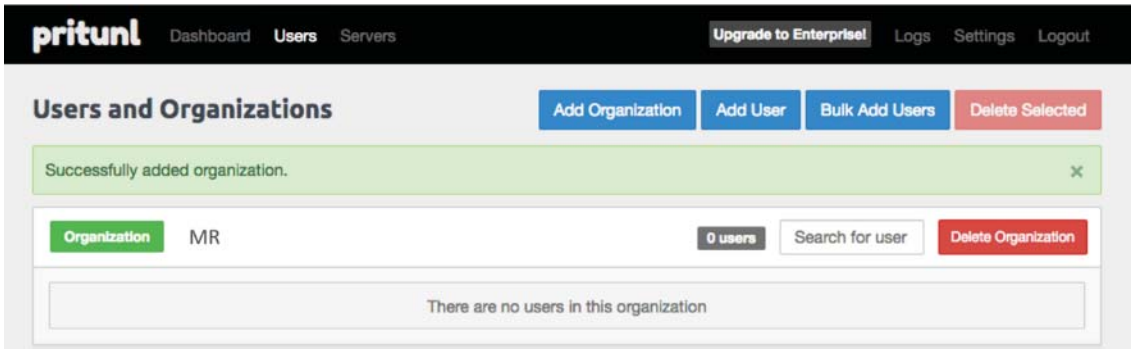


Add the organization by click the Add Organization button.

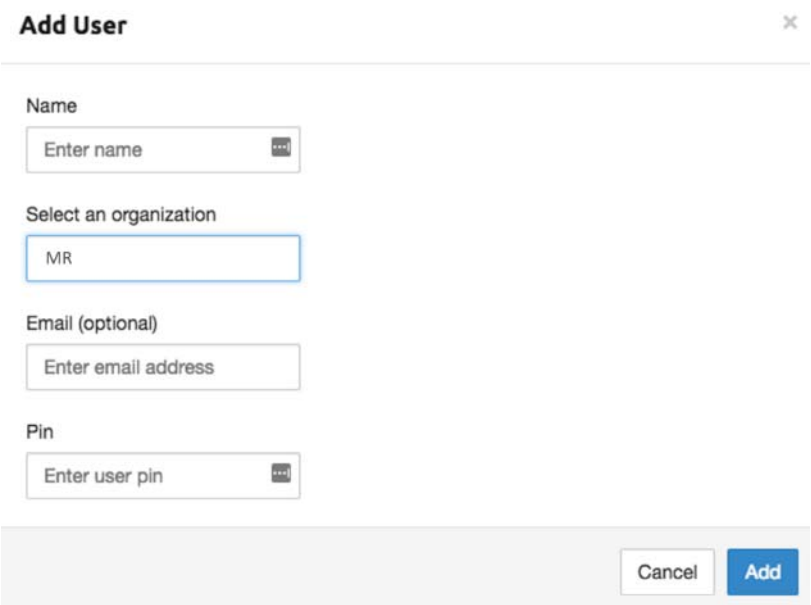


(In this document, we use the MR to be the organization example.)

When the organization be created, the Users page should be like the following figure.

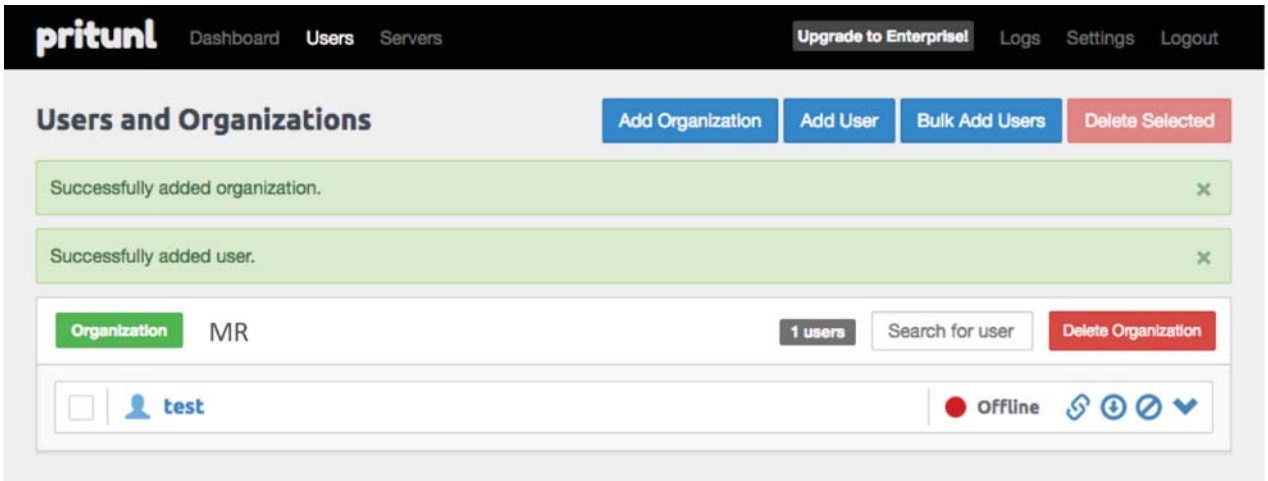


Then add the Open VPN user by click the Add User button.



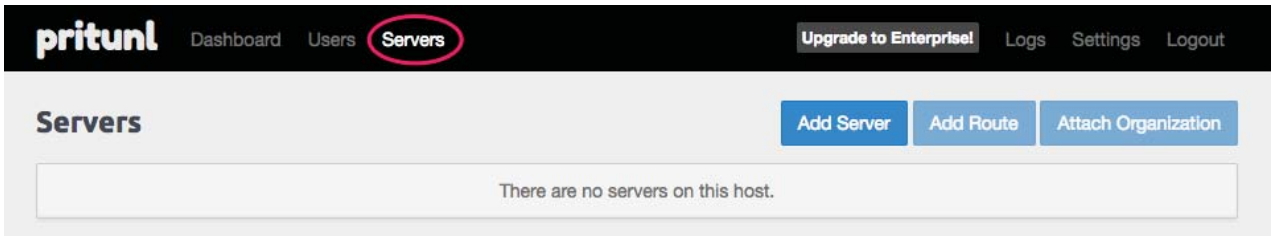
Note: In this Open VPN server, the PIN must contain only digits.

Note: In this document, we use the test/123456 Open VPN user to be the example.

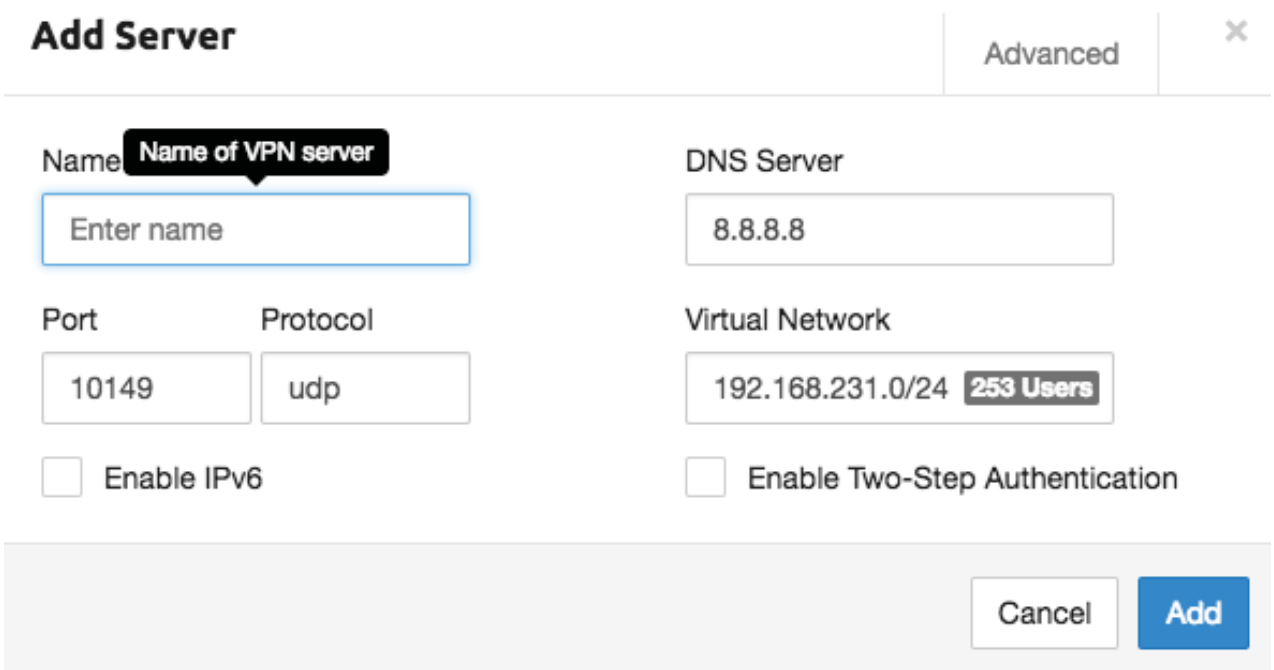


Open VPN server setup

Please navigate to the Server page to setup the Open VPN server.

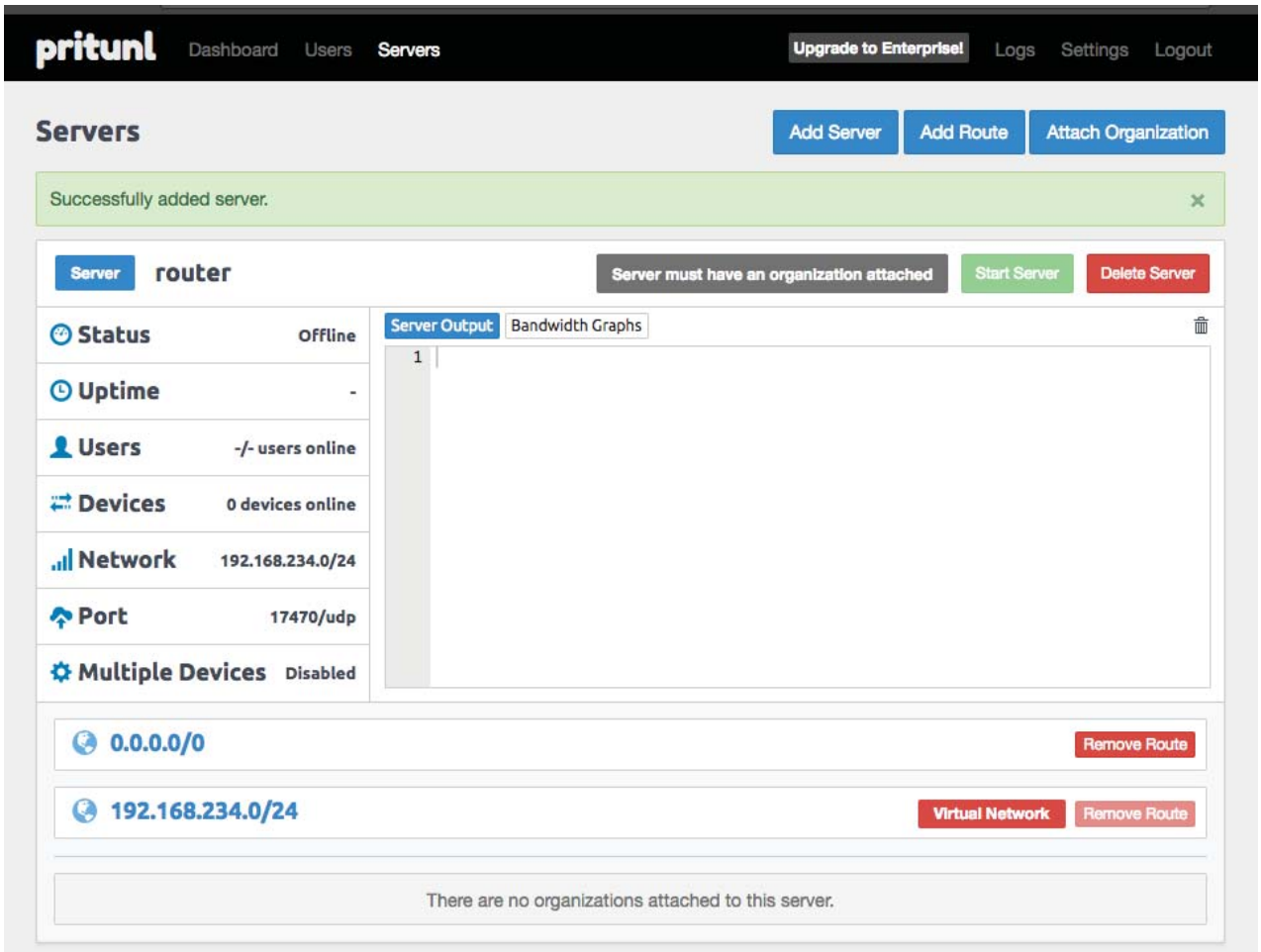


And click the Add Server button to create the Open VPN server.

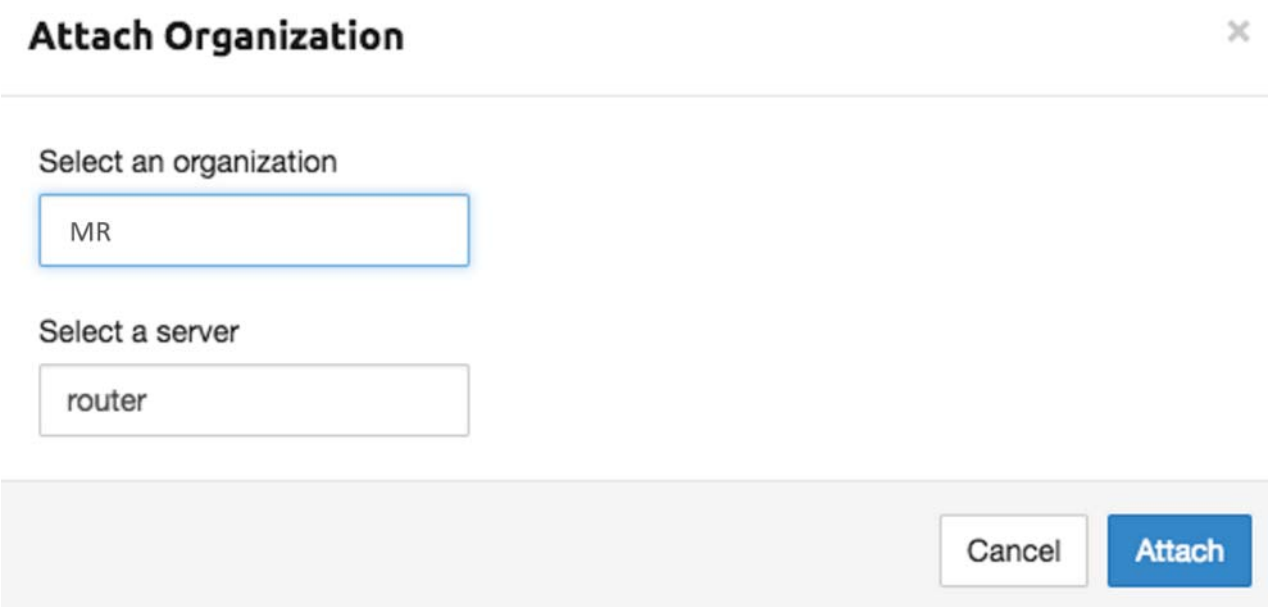


Note: Please click the Advanced tab and make sure the Inter-Client Communication be checked

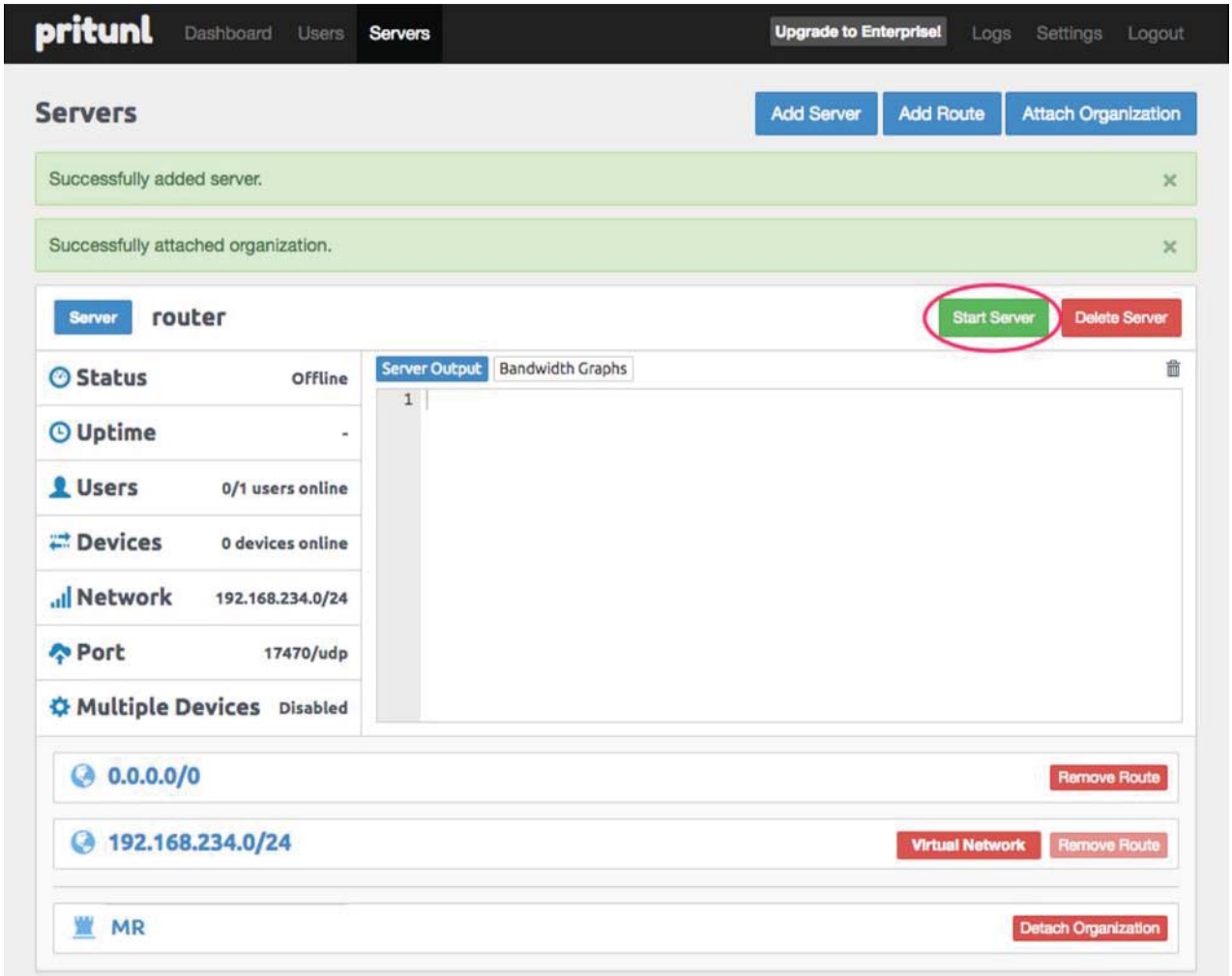
When the Open VPN server created, the Servers page should like the following figure.



And click Attach Organization button to setup the Open VPN server.

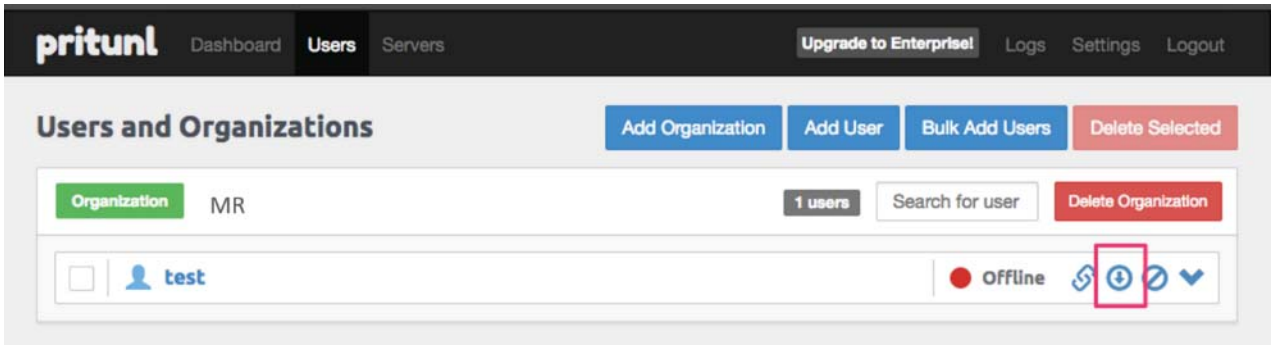


Start the Open VPN server by click Start Server button.



Cellular Router setup

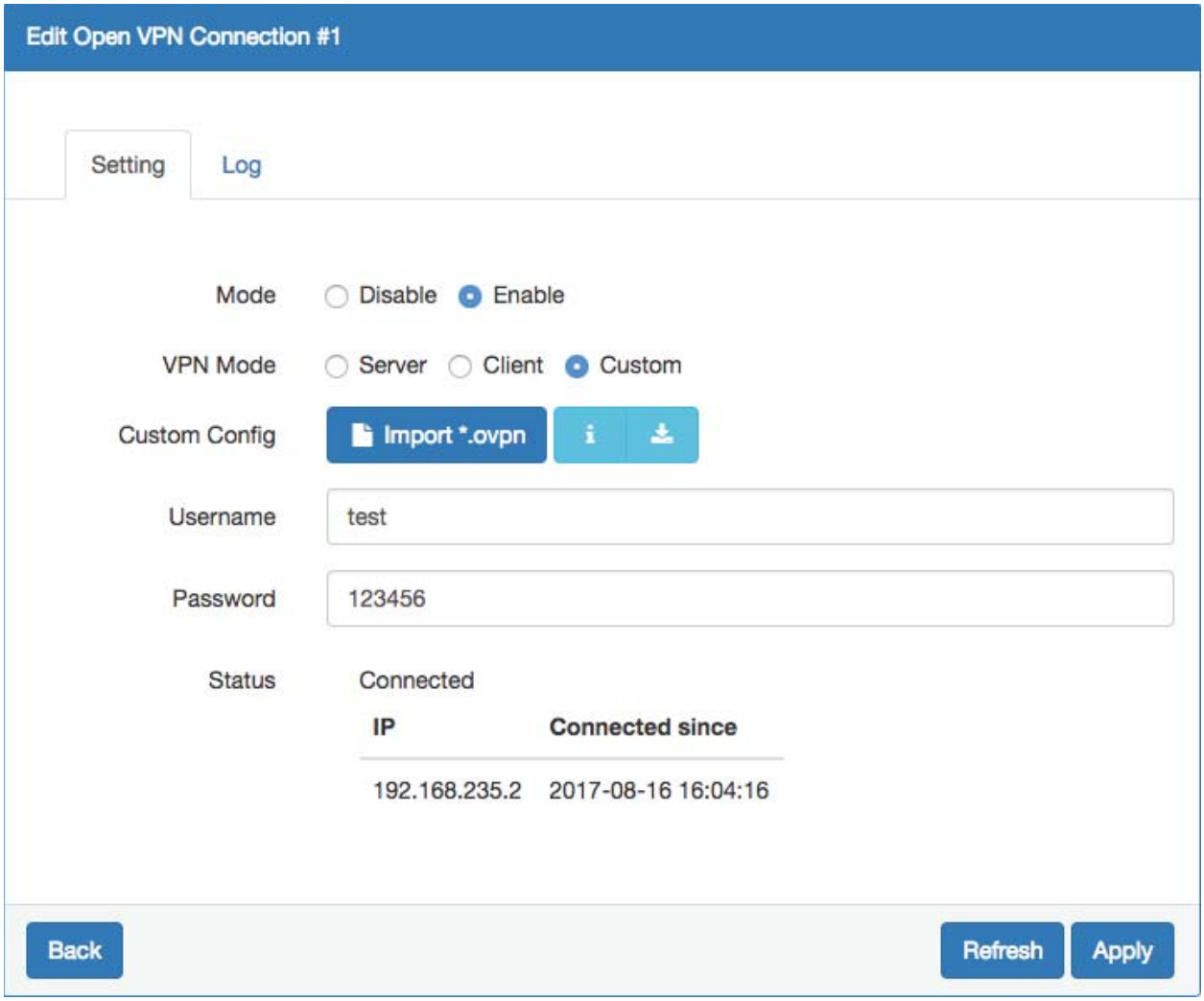
First, please navigate to the Users page and download the user configuration file and extract it.



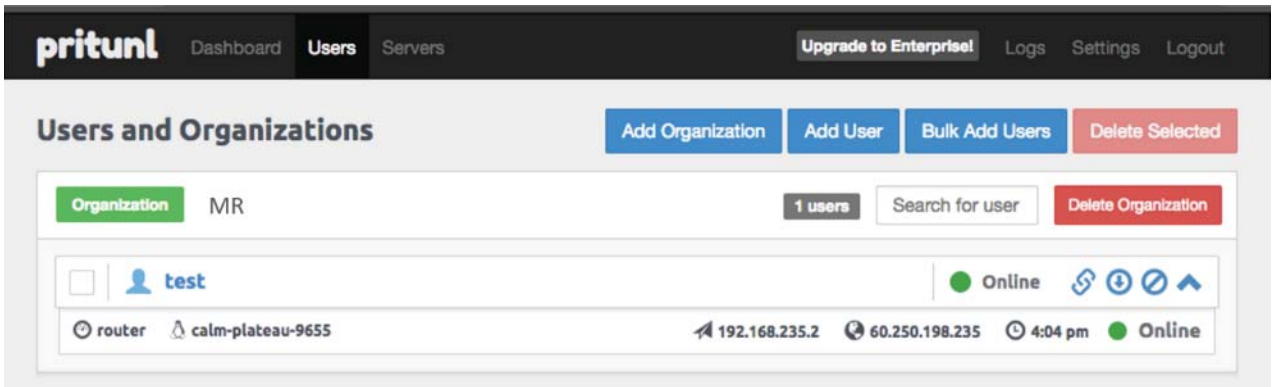
Note: In this document, you should get the MR_test_router.ovpn file.

And visit the Cellular Router Open VPN custom page then import the .ovpn file.

Fill up the username/password which be setup in Open VPN user setup part.

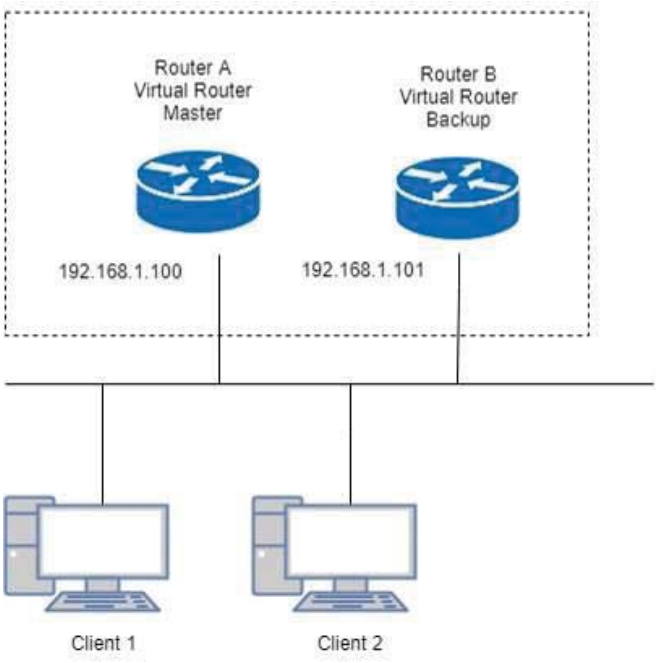


When the Cellular Router Open VPN connected, the Pritunl Open VPN server also update the user status.



16.6 VRRP Topology

Basic VRRP Topology



Base on this topology and VRRP Parameter settings, Router A and Router B will offer a virtual router service with virtual IP = 192.168.1.200 for the client.

16.7 TR069 Server (GenieACS Installation)

Server OS: Ubuntu 14.04 on Virtualbox

Installation:

1) Login ubuntu
2) Change to root by 'su -' and enter your root password.
3) Install required package as below command:
   >apt install gcc openssl-devel zlib-devel readline-devel sqlite-devel
4) Make a directory for application installation
   >mkdir /opt
5) Install yaml
cd /opt
wget http://pyyaml.org/download/libyaml/yaml-0.1.7.tar.gz
tar xvzf yaml-0.1.7.tar.gz
cd yaml-0.1.7
./configure
make && make install
6) Install ruby
cd /opt
wget http://cache.ruby-lang.org/pub/ruby/2.4/ruby-2.4.1.tar.gz
tar xvzf uby-2.4.1.tar.gz
cd ruby-2.4.1

```
./configure
make && make install
ruby   -v
ruby 2.4.1p111 (2017-03-22 revision 58053) [i686-linux]

cd /opt
gem install rails --no-ri --no-rdoc
gem install bundle --no-ri --no-rdoc

7) Install node.js
cd /opt
wget http://nodejs.org/dist/v8.2.1/node-v8.2.1.tar.gz
tar zxvf node-v8.2.1.tar.gz
cd node-v8.2.1
./configure
make && make install
node -v
v8.2.1

8) Install redis
cd /opt
wget http://download.redis.io/releases/redis-4.0.1.tar.gz
tar zxvf redis-4.0.1.tar.gz
cd redis-4.0.1
make
make test
All tests passed without errors!
make install
#Start redis server
redis-server

9) Install mongodb
cd /opt
wget https://fastdl.mongodb.org/linux/mongodb-linux-i686-3.3.3.tgz
tar zxvf mongodb-linux-i686-3.3.3.tgz
cd mongodb-linux-i686-3.3.3
mkdir -p /data/db

10) Install genieACS
cd /opt
git clone https://github.com/zaidka/genieacs.git
cd genieacs
npm install
npm run configure
npm run compile
```

Modify FS_HOSTNAME field in genieacs/config/config.json for device retrieve firmware file

Original configuration:
"FS_HOSTNAME" : "acs.example.com"

New configuration example.:
"FS_HOSTNAME" : "192.168.0.199"

Note: It is the place where the device firmware file stored. Generally, it is the IP address on where your GenieACS server installed.

Modify connect request username/password in genieacs/config/auth.js to stimulate connection

Original configuration:

```
function connectionRequest(deviceId, url, username, password, callback) {
    return callback(username || deviceId, password || "");
}
```

New configuration example:

```
function connectionRequest(deviceId, url, username, password, callback) {
    return callback('tr069','tr069');
}
```

Note: The hard code username/password MUST same with device's connection request username/password, otherwise the ACS stimulate connection will fail.

11) Install genieACS-Gui

```
git clone https://github.com/zaidka/genieacs-gui
cd genieacs-gui
bundle

gem install json
bundle update

rm -f db/*.sqlite3
rake db:create
RAILS_ENV=development rake db:migrate

cd /opt
cd genieacs-gui/config
cp index_parameters-sample.yml index_parameters.yml
cp parameter_renderers-sample.yml parameter_renderers.yml
cp parameters_edit-sample.yml parameters_edit.yml
cp roles-sample.yml roles.yml
cp summary_parameters-sample.yml summary_parameters.yml
cp users-sample.yml users.yml
cp graphs-sample.json.erb graphs.json.erb
```

GenieACS startup script:

```
#!/bin/sh

GENIE_PATH=/opt/genieacs/bin
GENIE_GUI_PATH=/opt/genieacs-gui

echo "start mongod."
pidof mongod
if [ $? != 0 ]; then
/opt/mongodb-linux-i686-3.3.3/bin/mongod --dbpath /data/db --journal --storageEngine=mmapv1
--fork --syslog
fi

echo "start North Bound/RESTful Interface service."
$GENIE_PATH/genieacs-nbi &

echo "start ACS/CWMP service."
$GENIE_PATH/genieacs-cwmp &

echo "start HTTP/File streaming service."
$GENIE_PATH/genieacs-fs &

echo "start GenieACS/WebUI."
cd $GENIE_GUI_PATH
rails server -b 0.0.0.0
```

GenieACS stop:

Ctrl-C

Usage:

1) Device Configuration

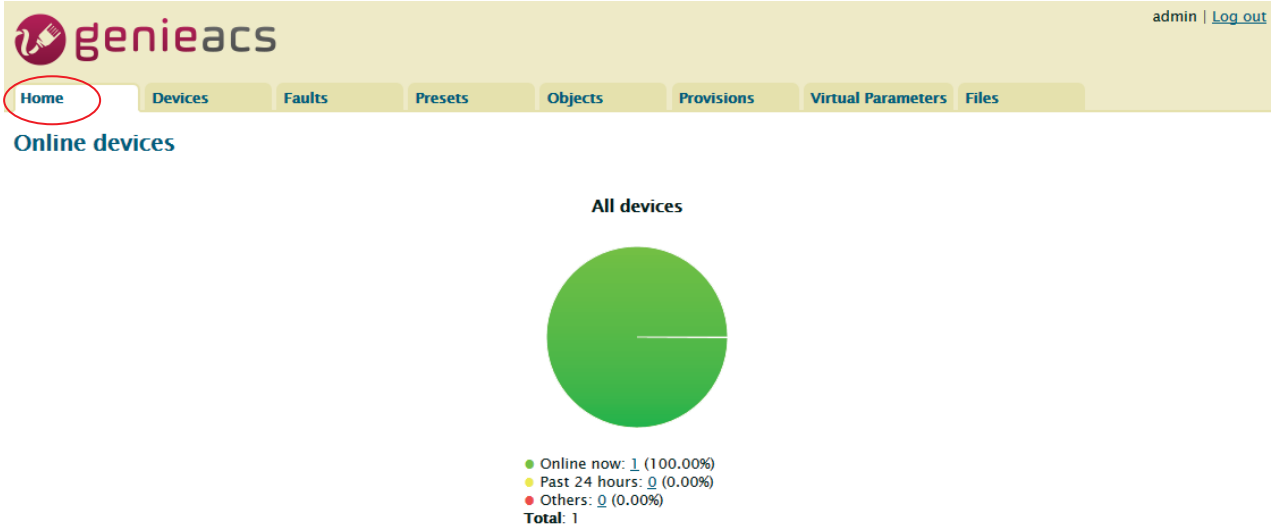
Fill in the ACS URL field as http://GenieACS server IP:7547

Fill in the Connection Request Username and Connection Request Password fields to same with the configuration in genieacs/config/auth.js.

2) GenieACS Operation

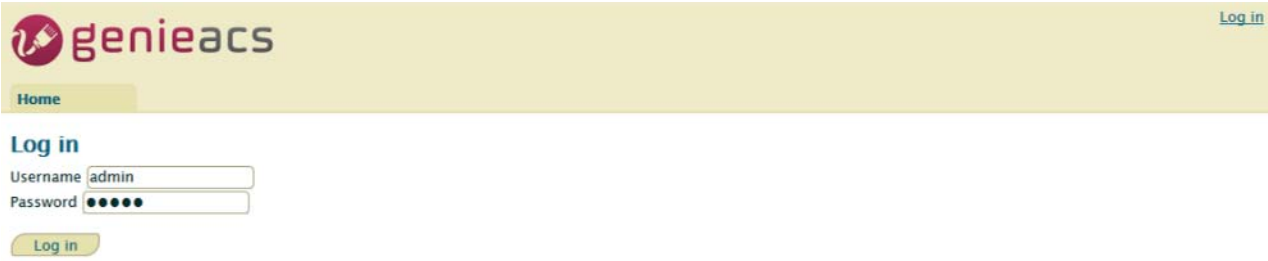
Input http://GenieACS server IP:3000 on browser url bar and Enter.

Press Home tab to refresh Online devices status.



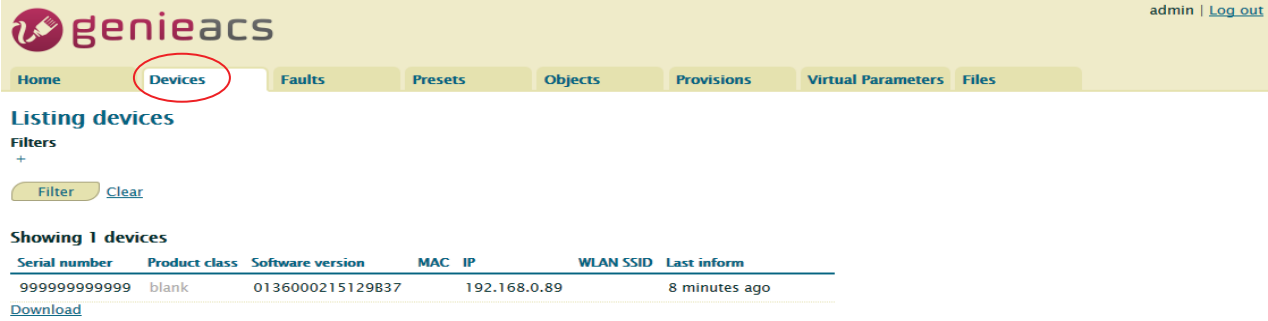
2.1) Login

Username and Password are admin/admin.

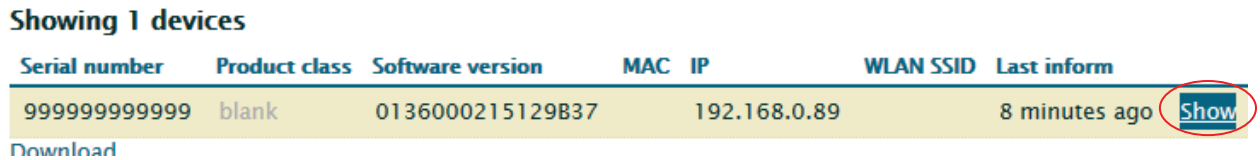


3) Device information

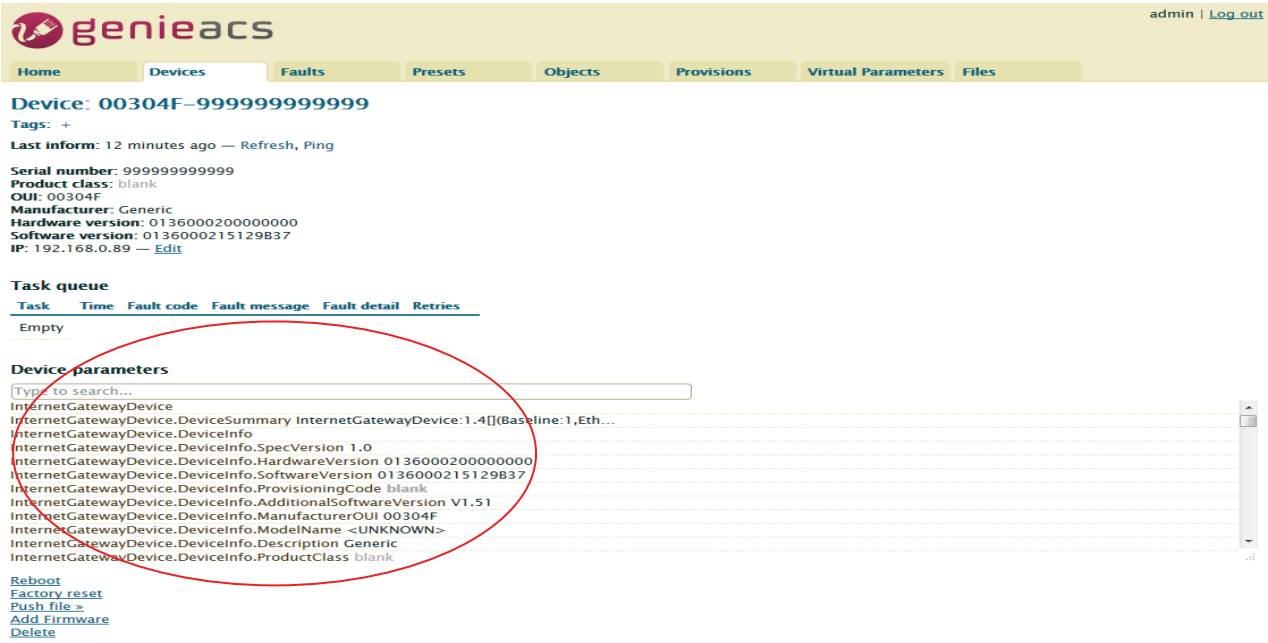
Press Devices tab



Move mouse to line end of your device, the Show link show up.



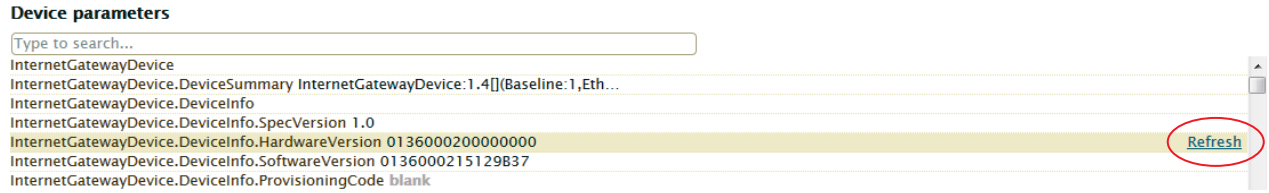
Press Show link, the device information shows up.



4) Access parameters

Scroll up/down on Device parameters list, the Refresh and Edit link show up at line end of parameter.

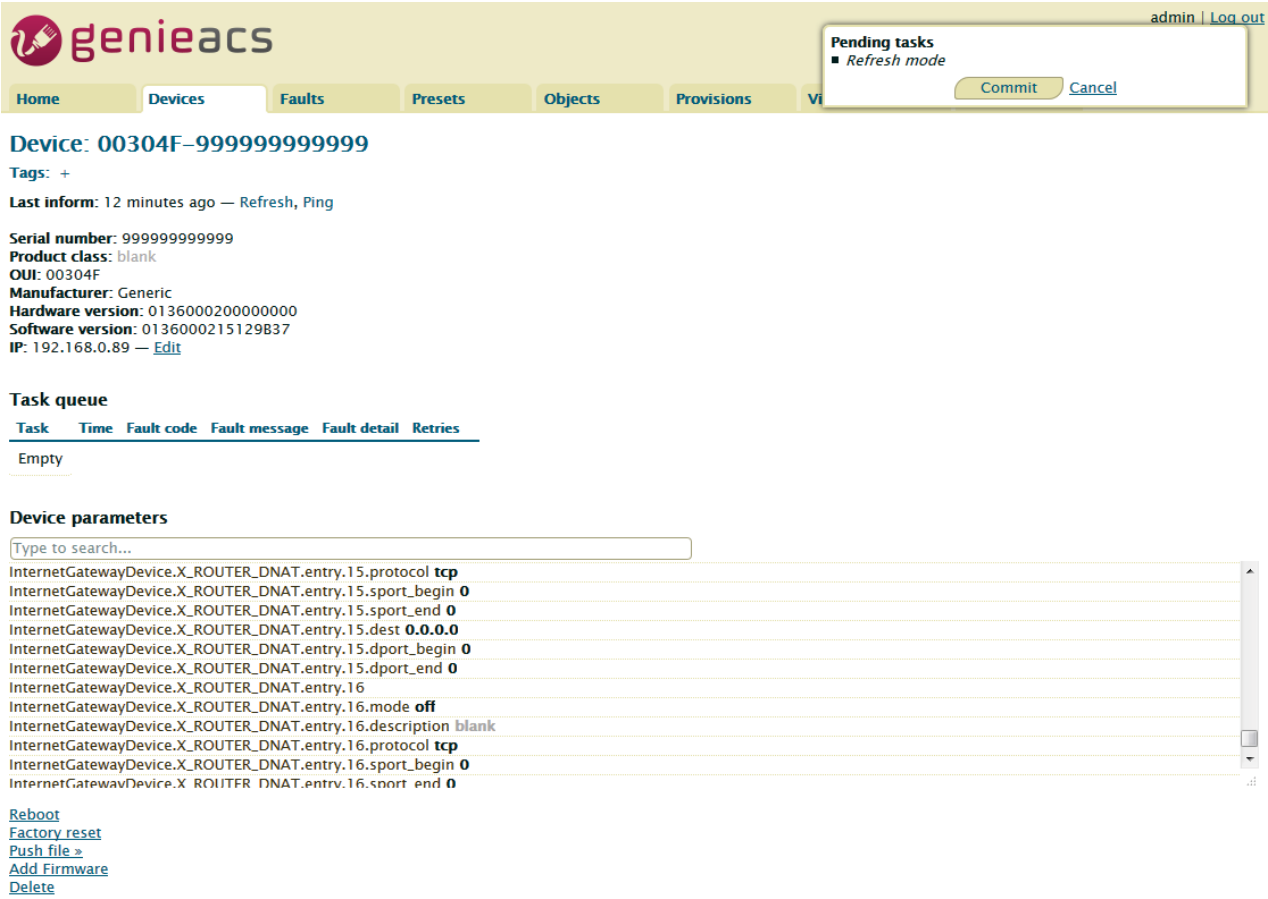
For Readable parameter



For Readable and Writable parameter

4.1) Get parameter value

Press on the Refresh link, the Pending tasks window will pop up on right top to ask you to allow or Cancel this action.



Press Commit to get this parameter value.

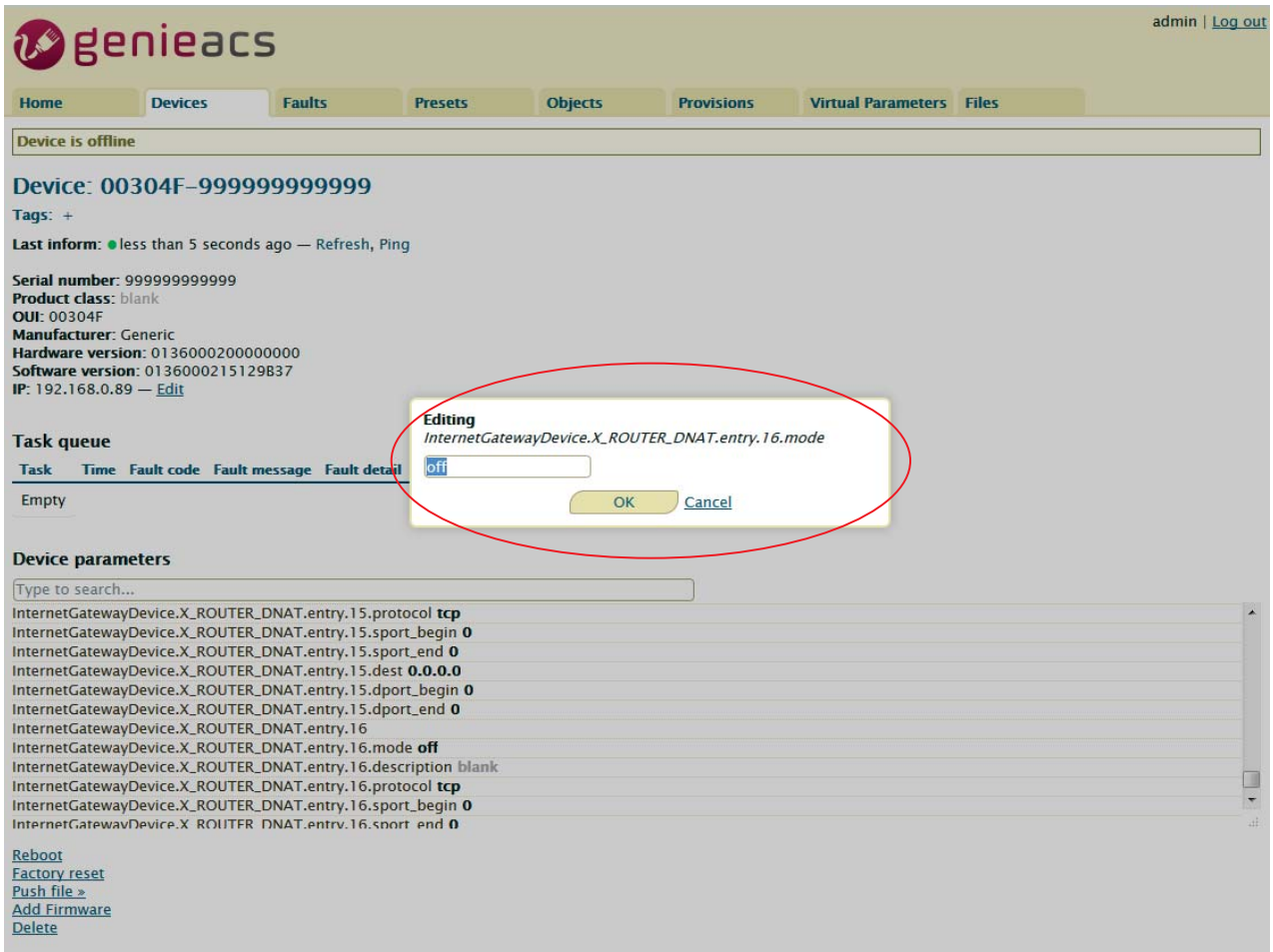
Note: *If the GenieACS can reach the device, the parameter value will be updated immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

Note: To update the whole tree, refresh the root parameter (InternetGatewayDevice.).

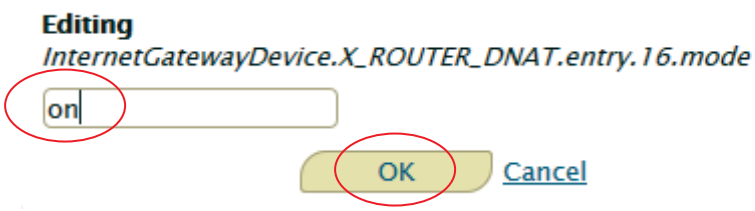
Note: To update partial tree, refresh the parent node of the partial tree.

4.2) Set parameter value

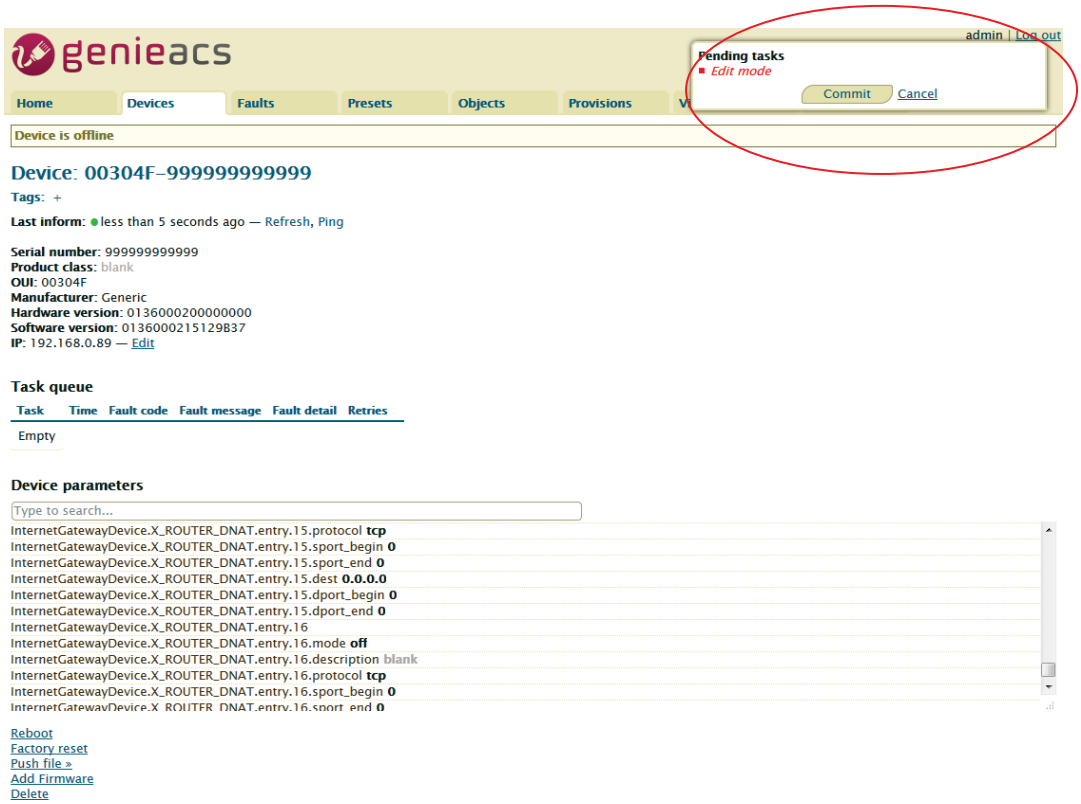
Press on the Edit link, editing window will pop up to ask you to change the value of this parameter.



Input new value and press OK.



The Pending tasks window will pop up to ask you to allow or Cancel this action.

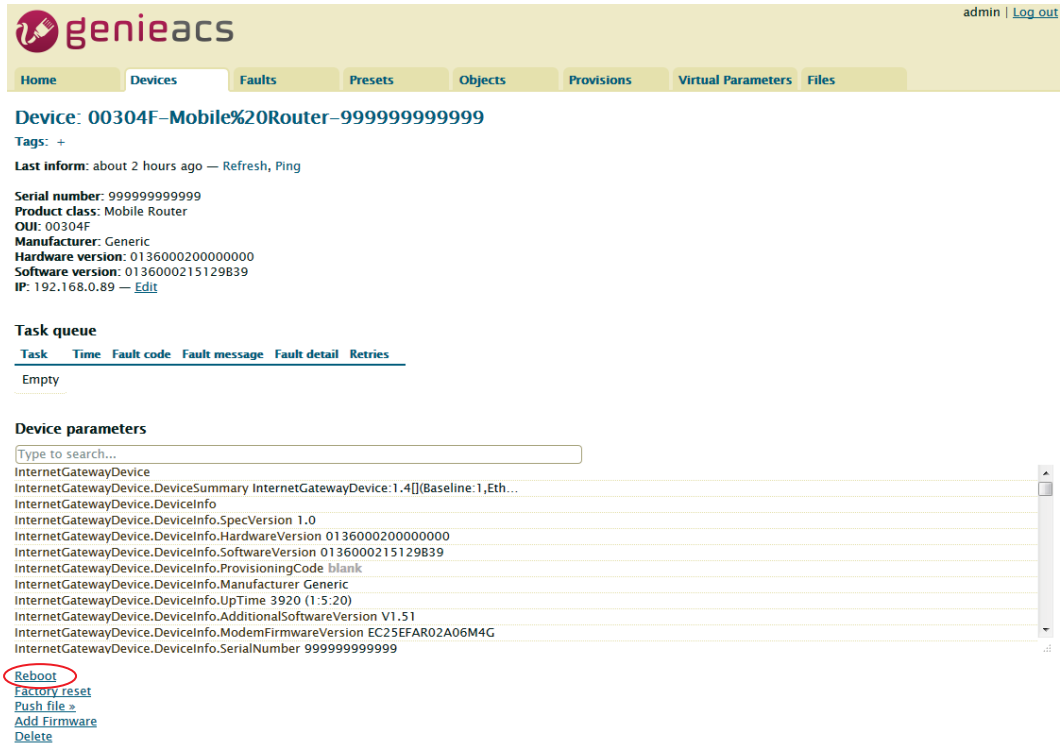


Press Commit to set this parameter value.

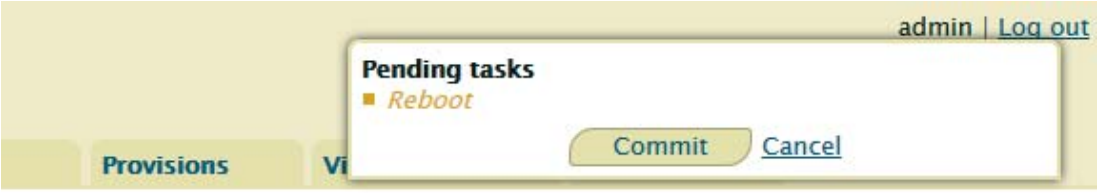
Note: *If the GenieACS can reach the device, the parameter value will be set immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

5) Reboot device

Press on Reboot link.



The Pending tasks window will pop up to ask you to allow or Cancel this action.



Press Commit to reboot device.

Note: *If the GenieACS can reach the device, the device will reboot immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

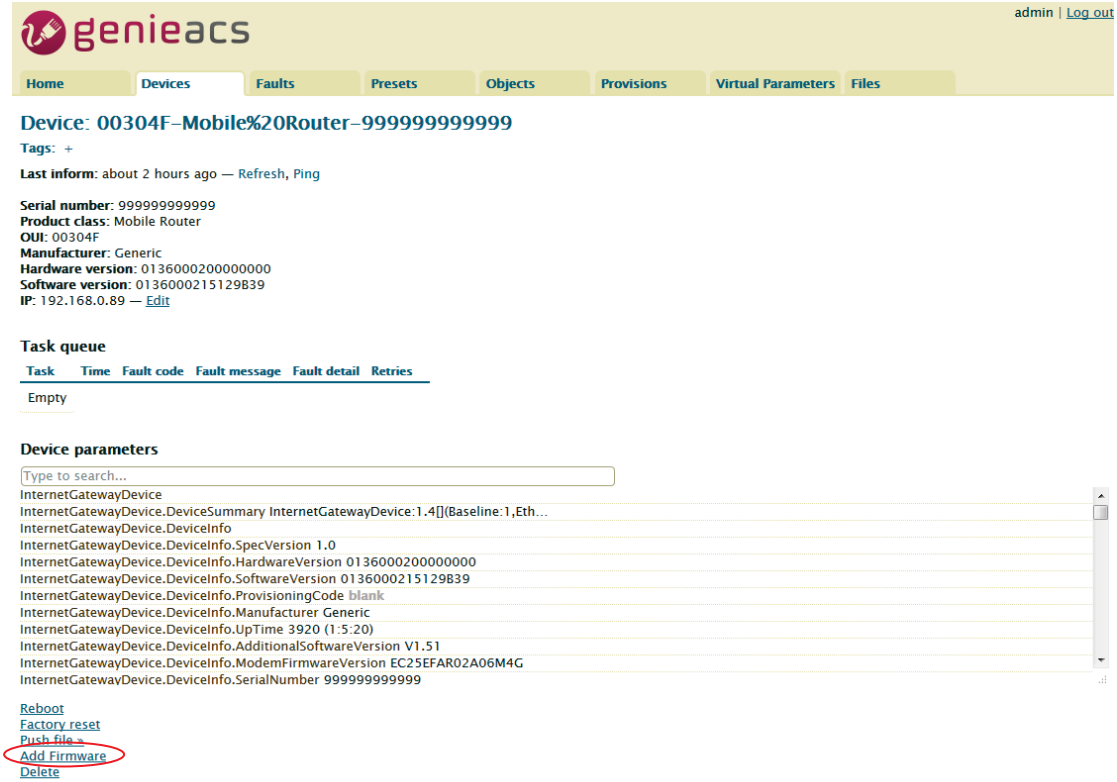
6) Reset to default

Similar to Reboot device except pressing on Factory reset link.

7) Firmware Upgrade

7.1) Upload Firmware

Press Add Firmware link



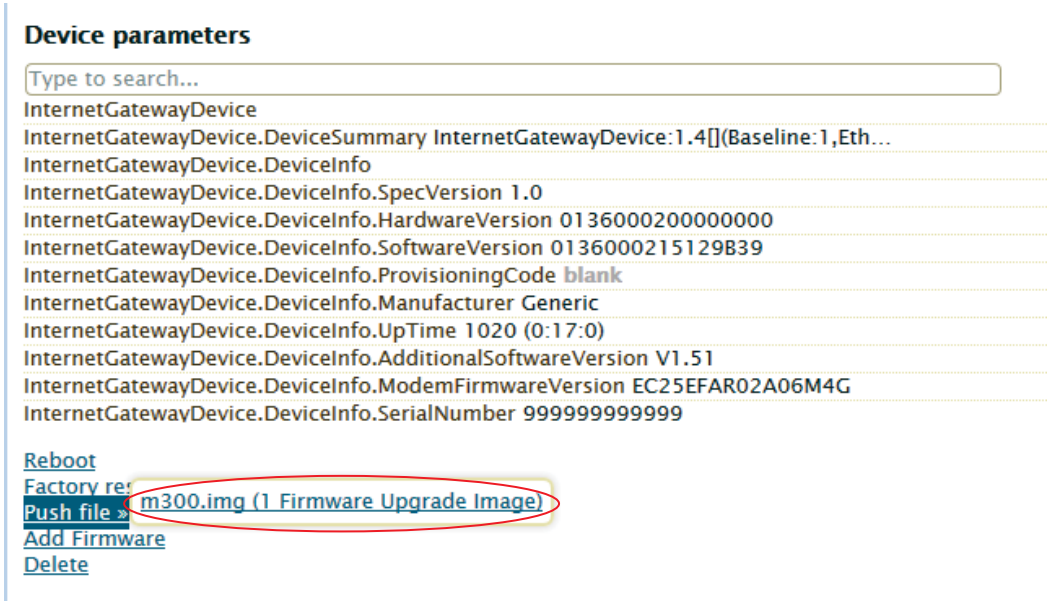
The link will redirect to Files tab

Press File: browse button, select the firmware, and then press Upload button.

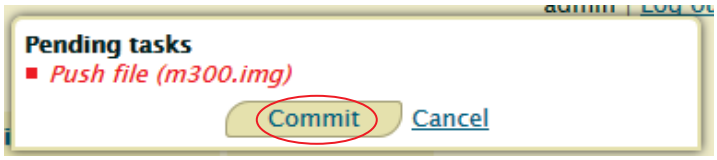
The firmware will be added to listing files as below.

7.2) Upgrade

Move mouse to the Push file>> link, the upgrade firmware name will pop up as below picture.



Move mouse to the upgrade firmware name and press it. The Pending tasks window will pop up to ask you to allow or Cancel this action.

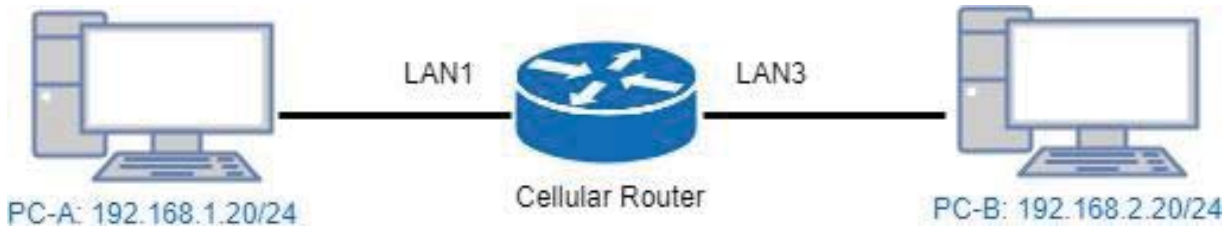


Press Commit, then firmware upgrade started.

Note: *If the GenieACS can reach the device, the firmware upgrade will be started immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

17 Test Case Example

17.1 VLAN Topology



This VLAN Topology for **3-port LANs** shows different PCs how to configure VLAN settings with different LAN ports and has two results for this configuration.

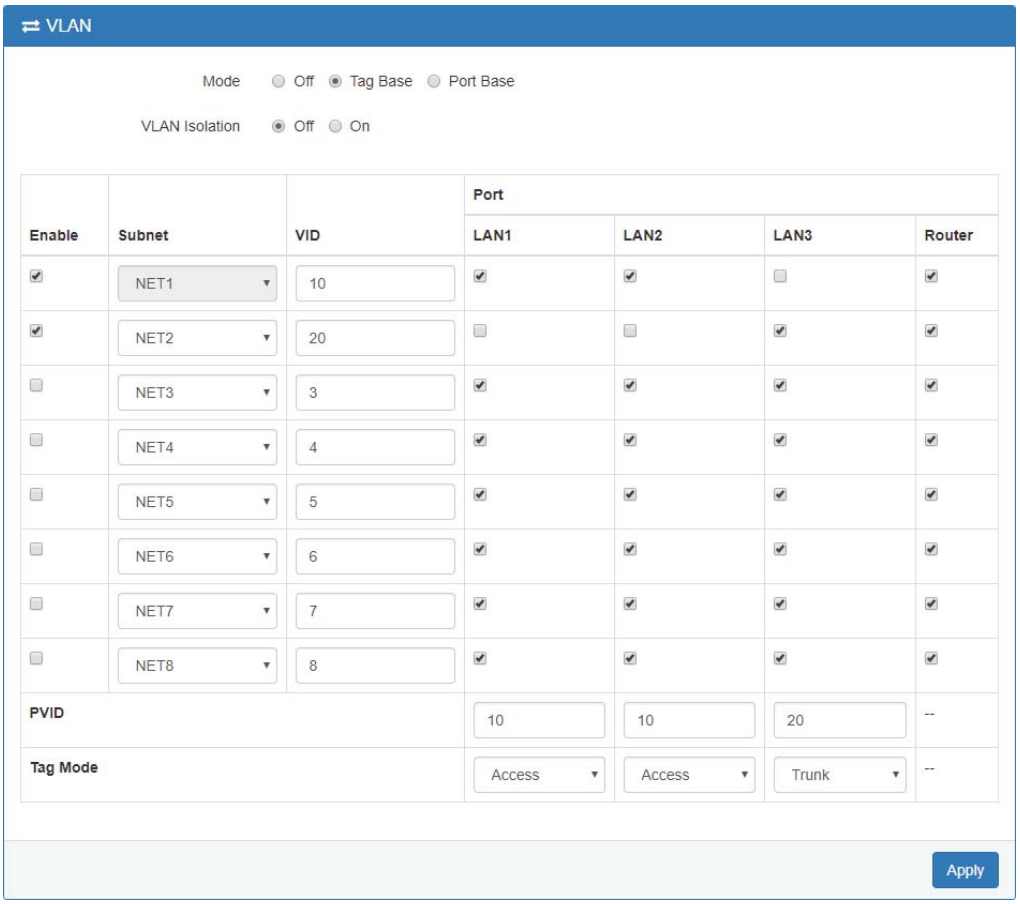
(1) PC-A sends ICMP packet to PC-B IP (192.168.2.20) and captures traffic on PC-B. Thus, PC-B will receive Tag20 traffic.

(2) PC-B sends ICMP packet to PC-A IP (192.168.1.20) and captures traffic on PC-A. Thus, PC-A will receive untag traffic.

Note:

- PC-A and PC-B are on Ubuntu OS.
- PC-A and PC-B should install vlan on Ubuntu.
- PC-A and PC-B should command this order “sudo apt-get install vlan”.

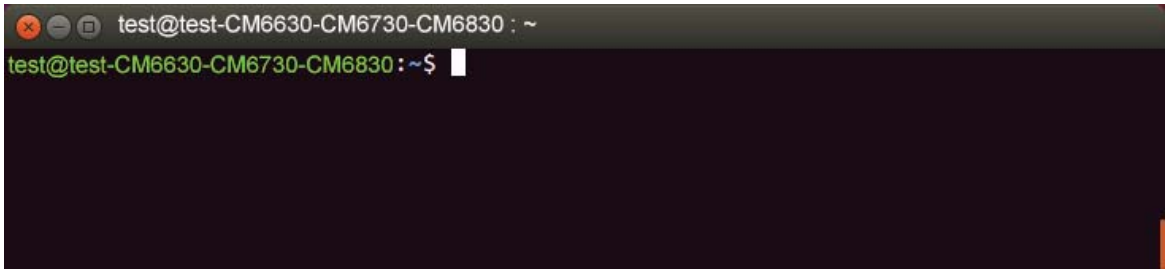
The following interface shows VLAN settings for the cellular router.



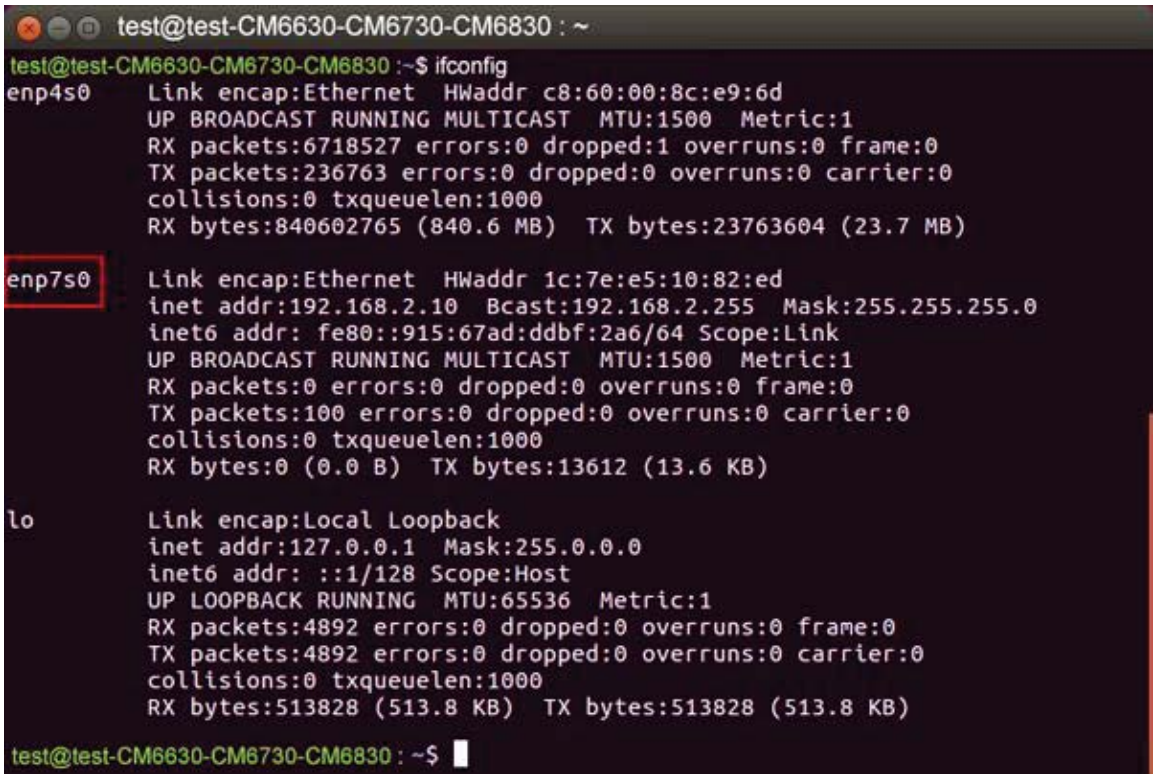
Note:

- Different PCs have different interface of network cards, like PC-A network card is eth1.10 for example 1 and PC-B network card is eth1.20 for example 2.
- How to find out the terminal and the interface of network cards based on different PCs.
  - From the following picture, you can click *the finding your computer icon* and input the terminal letters. Then, the interface will show *the terminal icon* and click to open it.

  - Next, it shows the information when you click *the terminal icon*.



  - From the following picture, it shows the interface of network card, enp7s0.



There are two examples to explain how configure VLAN settings.

Example 1: PC-A pings PC-B (Access to Trunk)

For PC-A, add default gateway and LAN's MAC to ARP.

- Load VLAN and create VLAN interface, command as below:
  - sudo modprobe 8021q
  - sudo vconfig rem eth1.20
  - sudo vconfig add eth1.10
- Configure VLAN interface as below:
  - sudo ifconfig eth1.10 192.168.1.20 netmask 255.255.255.0 up
  - sudo ifconfig eth1 0.0.0.0
- sudo route add default gw 192.168.1.1 eth1.10
- sudo arp -s 192.168.1.1 LAN's MAC
- eth1 is network interface on PC-A

Therefore, PC-B will receive Tag20 traffic when PC-A sends ICMP packet to PC-B IP (192.168.2.20) and captures traffic on PC-B.

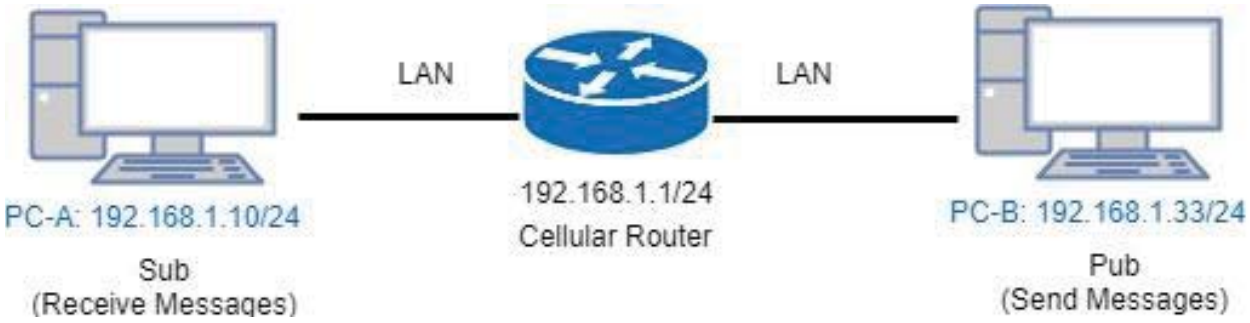
Example 2: PC-A ping PC-B (Trunk to Access)

For PC-B, add default gateway and LAN's MAC to ARP

- Load VLAN and create VLAN interface, command as below:
  - sudo modprobe 8021q
  - sudo vconfig rem eth1.10
  - sudo vconfig add eth1.20
- Configure VLAN interface as below:
  - sudo ifconfig eth1.20 192.168.2.20 netmask 255.255.255.0 up
  - sudo ifconfig eth1 0.0.0.0
- sudo route add default gw 192.168.2.1 eth1.20
- sudo arp -s 192.168.2.1 LAN's MAC
- eth1 is network interface on PC-B

Therefore, PC-A will receive untag traffic when PC-B sends ICMP packet to PC-A IP (192.168.1.20) and captures traffic on PC-A.

17.2 MQTT Topology



This MQTT Topology shows the cellular router to connect PC-A and PC-B's LANs and have two results are as below.

Expect Result:

(1) PC-A sends message to PC-B and PC-B should not receive any message.

(2) PC-B sends message to PC-A and PC-A should receive message.

Note: PC-A and PC-B should install MQTT Client software.

There is a process to explain the steps and result.

- Step1: Install mosquitto-clients on ubuntu or windows.

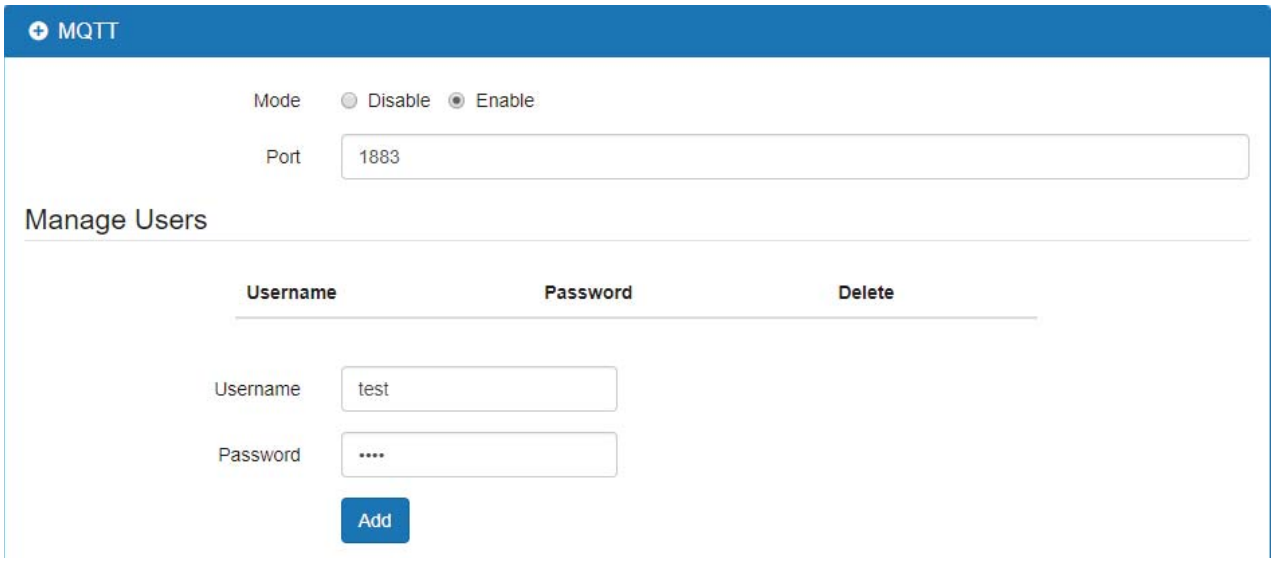
If your OS system is Ubuntu, you should install as below steps:

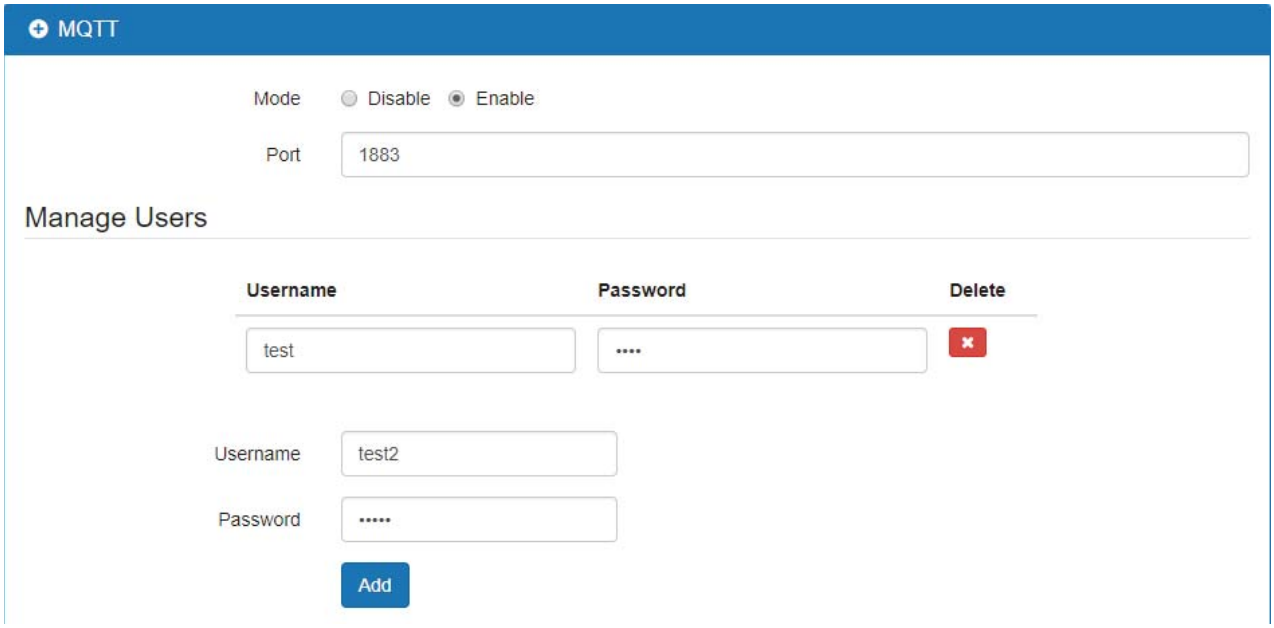
```
test@test: ~
test@test:~$ sudo apt-get install mosquitto-clients
sudo: unable to resolve host test
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  geoip-database-extra javascript-common libjs-openlayers libnghttp2-14
  libnl-route-3-200 libqgsttools-p1 libqt5multimedia5-plugins
  libqt5multimediawidgets5 libsmi2ldbl libssh-gcrypt-4 libwireshark-data
  libwiretap6 libwscodecs1 libwsutil7 linux-headers-4.10.0-28
  linux-headers-4.10.0-28-generic linux-headers-4.10.0-42
  linux-headers-4.10.0-42-generic linux-headers-4.13.0-26
  linux-headers-4.13.0-26-generic linux-image-4.10.0-28-generic
  linux-image-4.10.0-42-generic linux-image-4.13.0-26-generic
  linux-image-extra-4.10.0-28-generic linux-image-extra-4.10.0-42-generic
  linux-image-extra-4.13.0-26-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libc-ares2 libmosquitto1
The following NEW packages will be installed:
  libc-ares2 libmosquitto1 mosquitto-clients
0 upgraded, 3 newly installed, 0 to remove and 119 not upgraded.
Need to get 65.3 kB/96.4 kB of archives.
After this operation, 330 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

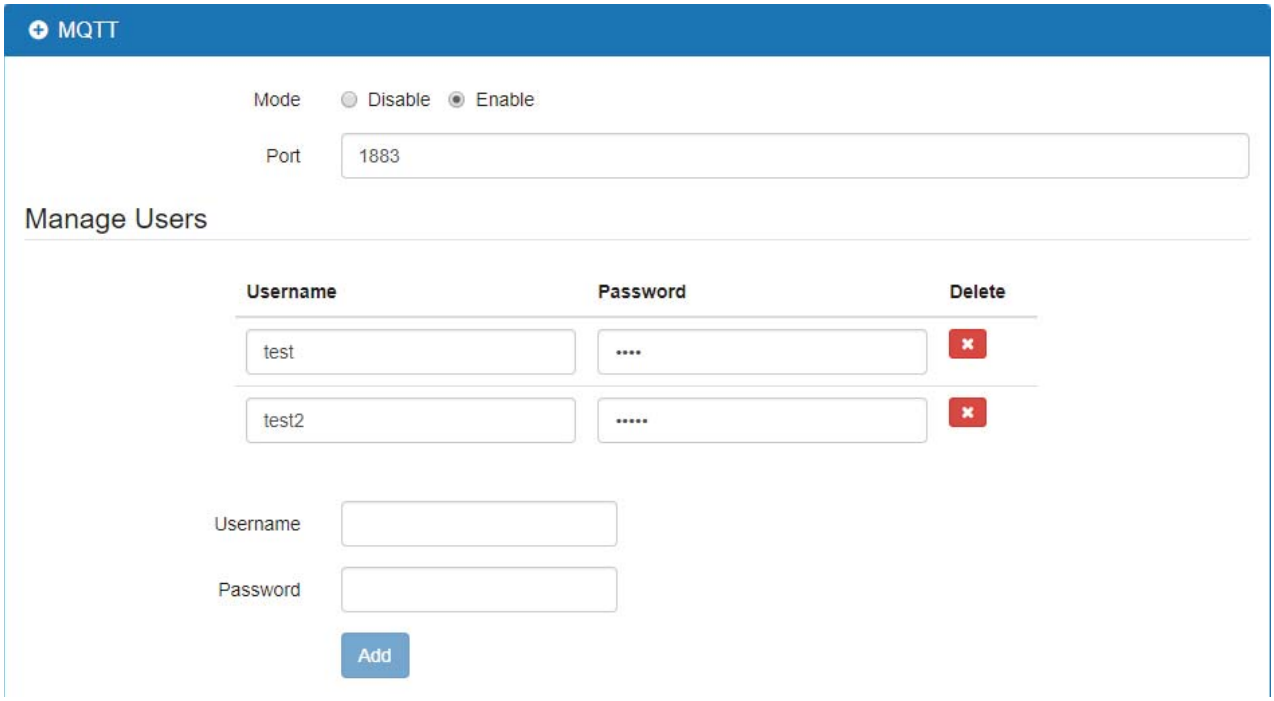
```
test@test: ~
After this operation, 330 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://tw.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libc-ares2 amd
64 1.10.0-3ubuntu0.2 [34.1 kB]
Get:2 http://tw.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 libmosquit
to1 amd64 1.4.8-1ubuntu0.16.04.2 [31.3 kB]
Fetched 65.3 kB in 0s (201 kB/s)
Selecting previously unselected package libc-ares2:amd64.
(Reading database ... 319360 files and directories currently installed.)
Preparing to unpack .../libc-ares2_1.10.0-3ubuntu0.2_amd64.deb ...
Unpacking libc-ares2:amd64 (1.10.0-3ubuntu0.2) ...
Selecting previously unselected package libmosquitto1:amd64.
Preparing to unpack .../libmosquitto1_1.4.8-1ubuntu0.16.04.2_amd64.deb ...
Unpacking libmosquitto1:amd64 (1.4.8-1ubuntu0.16.04.2) ...
Selecting previously unselected package mosquitto-clients.
Preparing to unpack .../mosquitto-clients_1.4.8-1ubuntu0.16.04.2_amd64.deb ...
Unpacking mosquitto-clients (1.4.8-1ubuntu0.16.04.2) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libc-ares2:amd64 (1.10.0-3ubuntu0.2) ...
Setting up libmosquitto1:amd64 (1.4.8-1ubuntu0.16.04.2) ...
Setting up mosquitto-clients (1.4.8-1ubuntu0.16.04.2) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
test@test:~$
```

- Step2: Configure MQTT for the Cellular Router

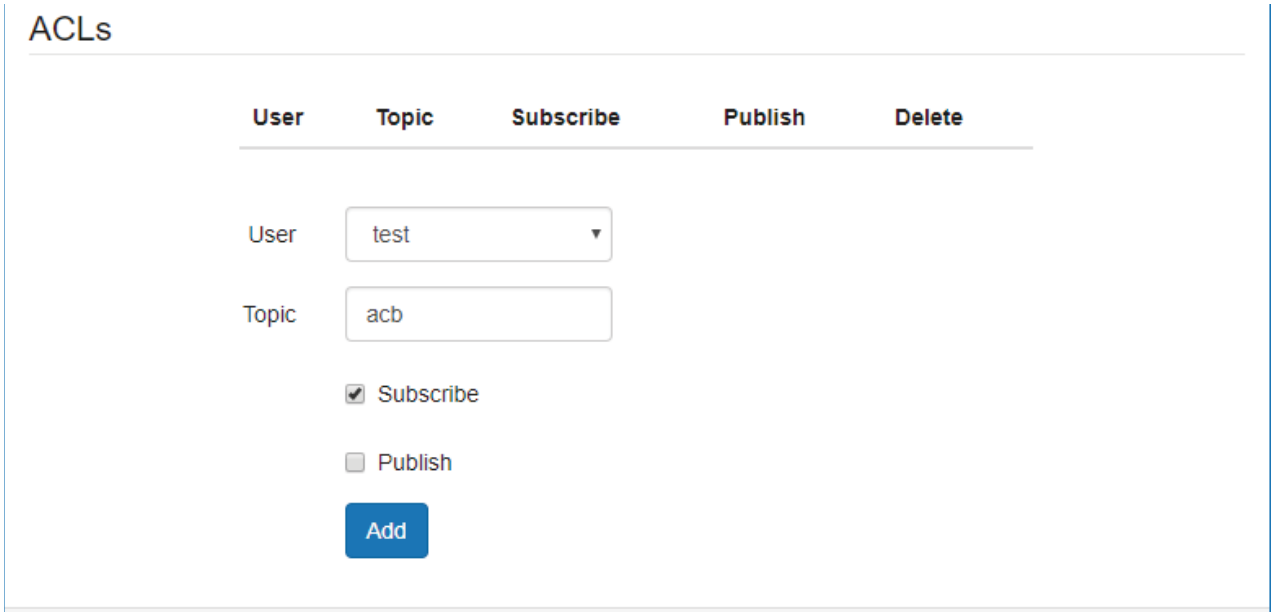
You need to add two users. For example, we create the users for test and test2.

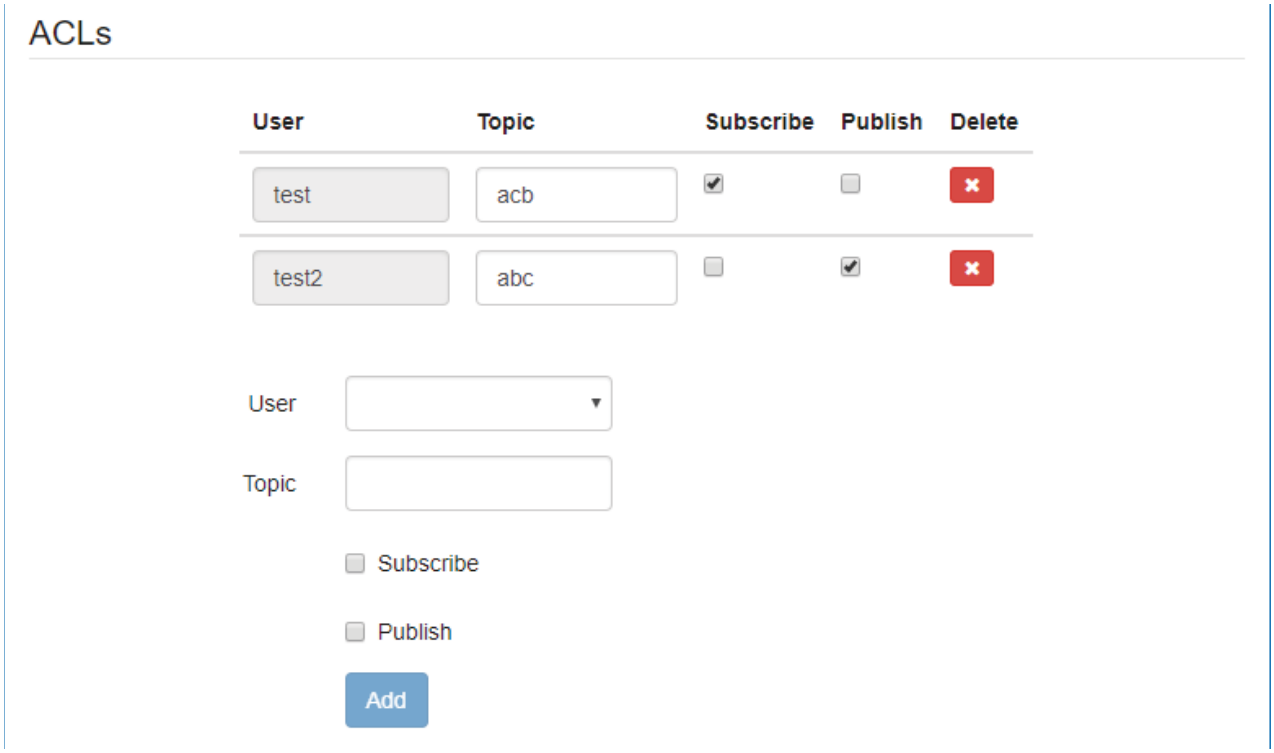






You need to add two ACLs based on the users you created. For instance, we create two ACLs for test user and test2 user.





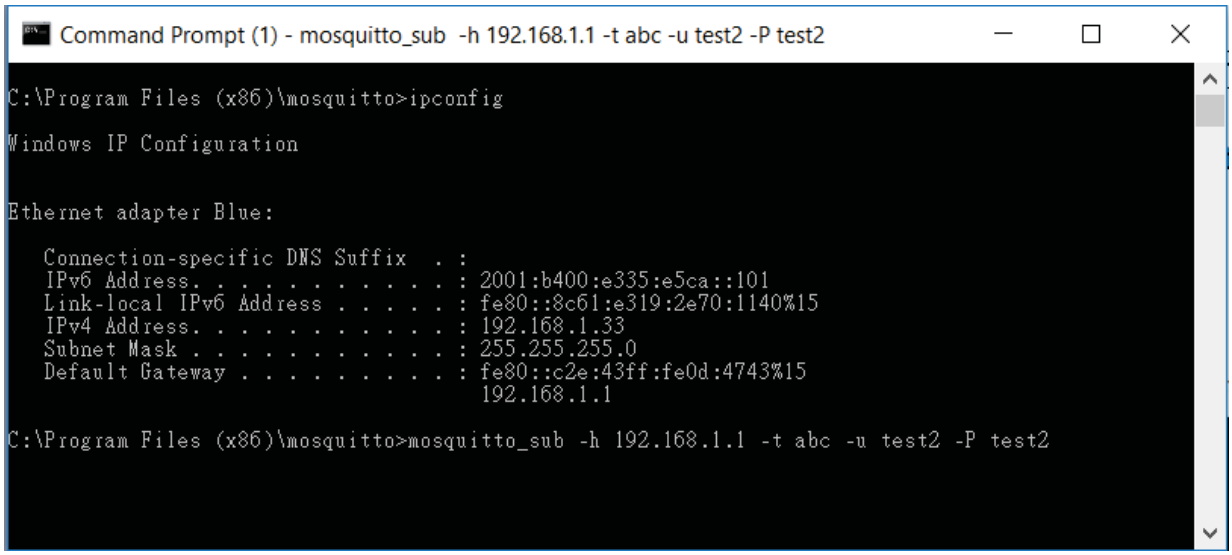
Note:

- For Receive message command format:
  Mosquitto_sub -h <M300 IP> -t <Topic> -u <username> -P <password>
- For Send message command format:
  Mosquitto_pub -h <M300 IP> -t <Topic> -u <username> -P <password> -m <message>

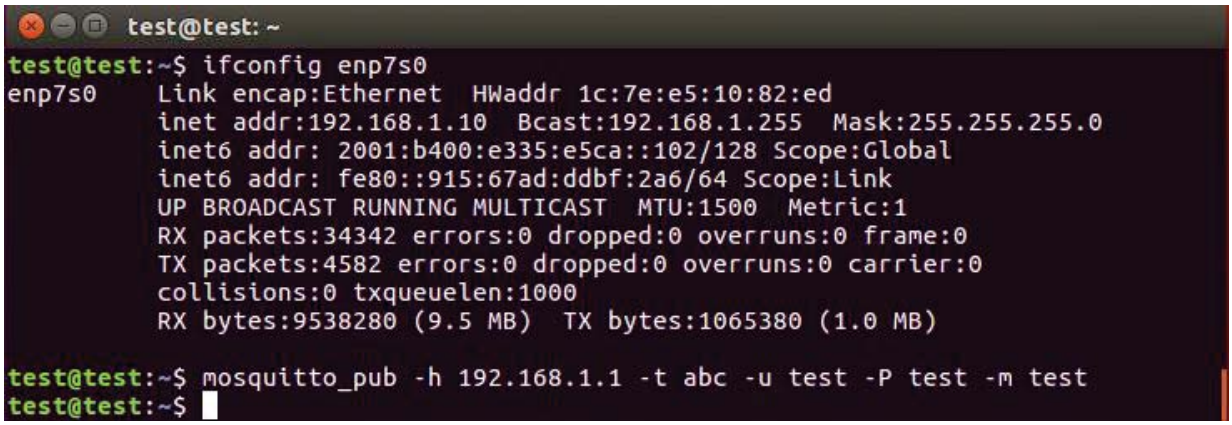
- Step3: There are two test MQTT examples.

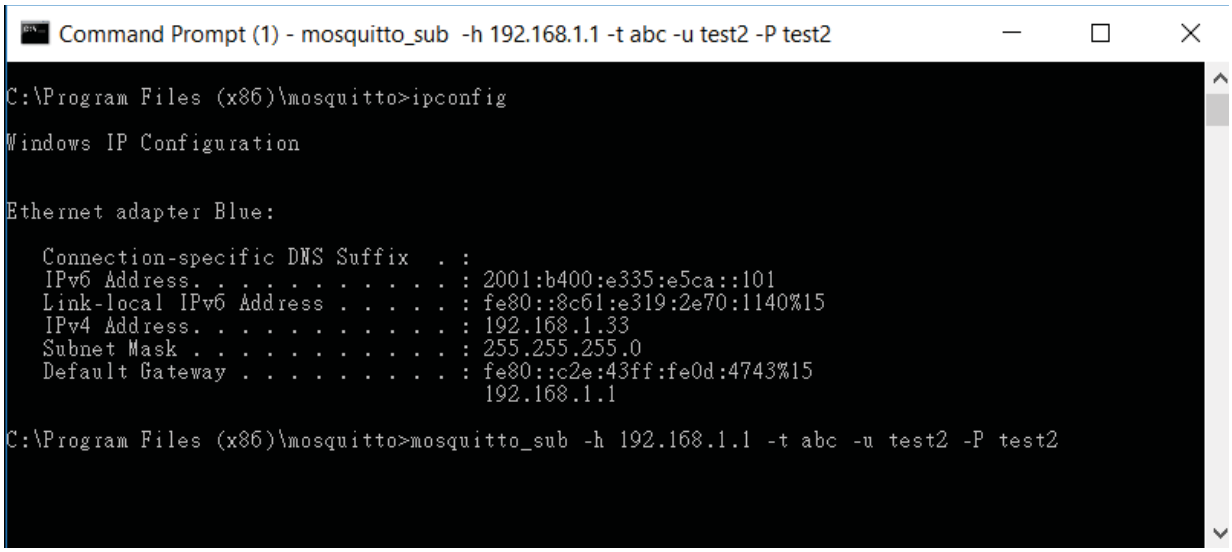
Example 1: PC-A sends message to PC-B and PC-B should not receive any message.

For PC-B, command "mosquitto_sub -h 192.168.1.1 -t abc -u test2 -P test2".



For PC-A, command "mosquitto_pub -h 192.168.1.1 -t abc -u test -P test -m test" and confirm the message on PC-B. It won't receive any message on PC-B.





Example 2: PC-B sends message to PC-A and PC-A should receive message.

For PC-A, command "mosquitto_sub -h 192.168.1.1 -t abc -u test -P test"

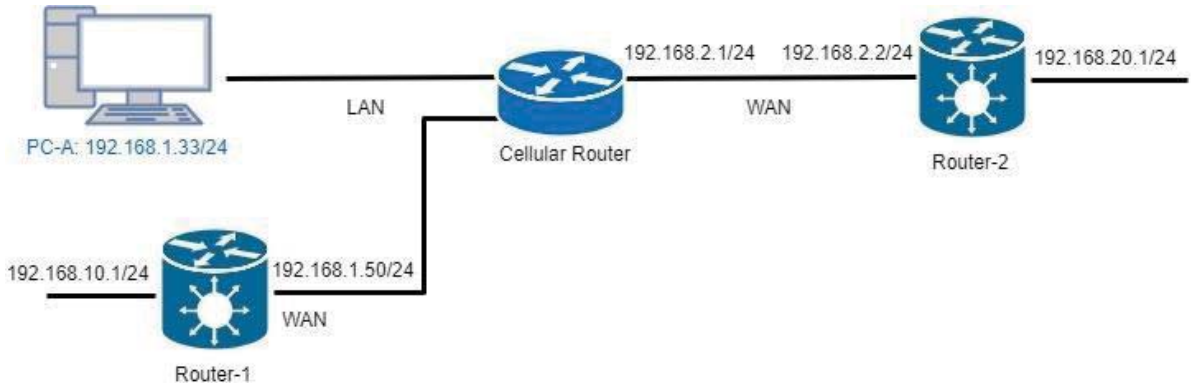
```
test@test: ~
test@test:~$ ifconfig enp7s0
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50690 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4831 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10908302 (10.9 MB)  TX bytes:1150596 (1.1 MB)

test@test:~$ mosquitto_sub -h 192.168.1.1 -t abc -u test -P test
```

For PC-B, command "mosquitto_pub -h 192.168.1.1 -t abc -u test2 -P test2 -m test" and confirm the message on PC-A. It will receive test message on PC-A.

```
Command Prompt (1)

C:\Program Files (x86)\mosquitto>ipconfig

Windows IP Configuration


Ethernet adapter Blue:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b400:e335:e5ca::101
   Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15
   IPv4 Address. . . . . . . . . . . : 192.168.1.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c2e:43ff:fe0d:4743%15
                                       192.168.1.1

C:\Program Files (x86)\mosquitto>mosquitto_pub -h 192.168.1.1 -t abc -u test2 -P test2 -m test

C:\Program Files (x86)\mosquitto>
```

```
test@test: ~
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50690 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4831 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10908302 (10.9 MB)  TX bytes:1150596 (1.1 MB)

test@test:~$ mosquitto_sub -h 192.168.1.1 -t abc -u test -P test
test
```

17.3 IP Routing Topology



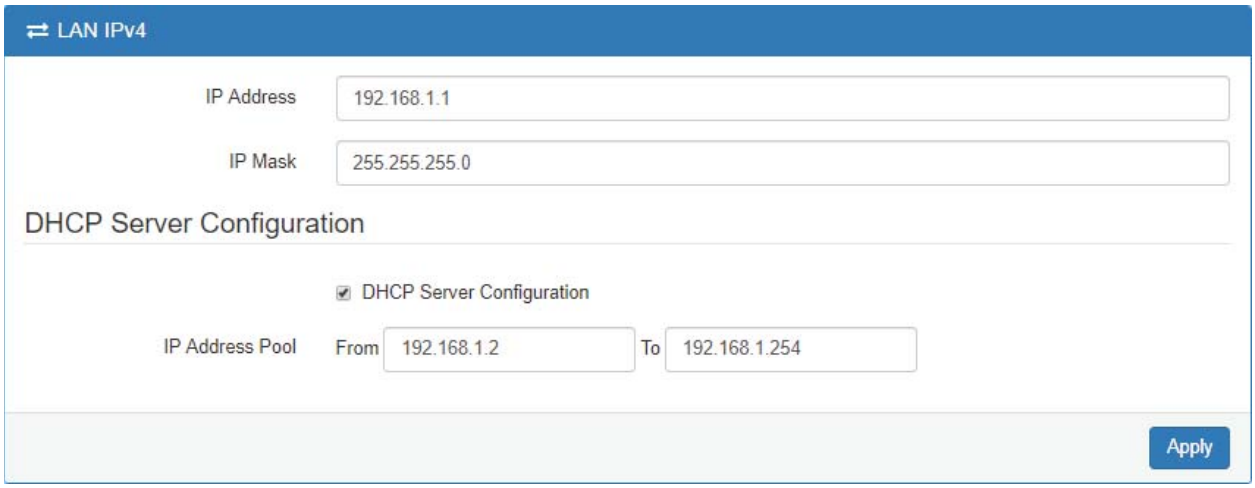
This IP Routing topology that the cellular router connects Router-1 and Router-2 will have two results.

(1) PC-A sends ICMP packet to Router-1 LAN and WAN IP and they should have response.

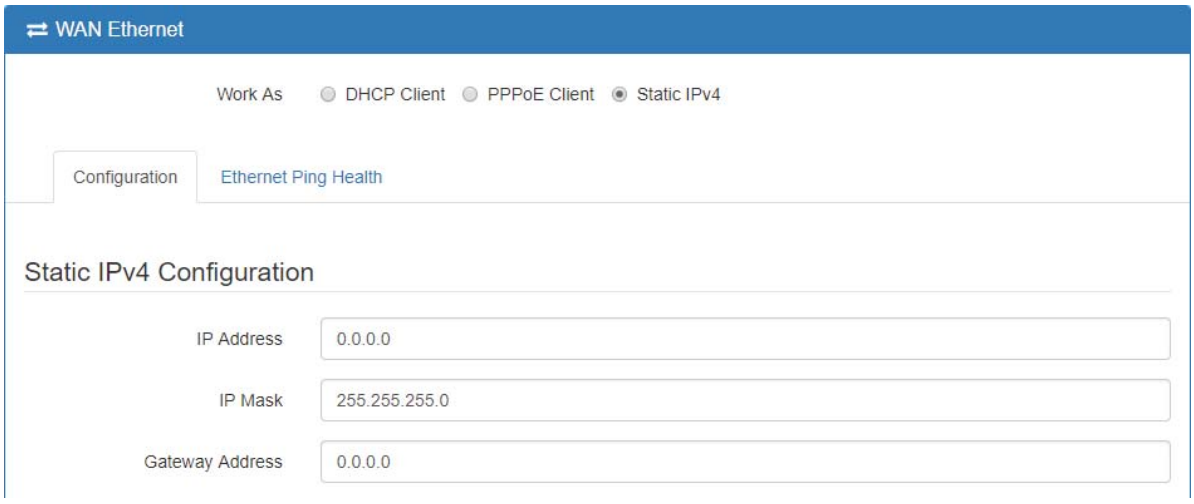
(2) PC-A sends ICMP packet to Router-2 LAN and WAN IP and they should have response.

Note: Router-1 and Router-2 are pure routers and should be supported "NAT enable / disable".

- LAN configuration:



- WAN configuration:

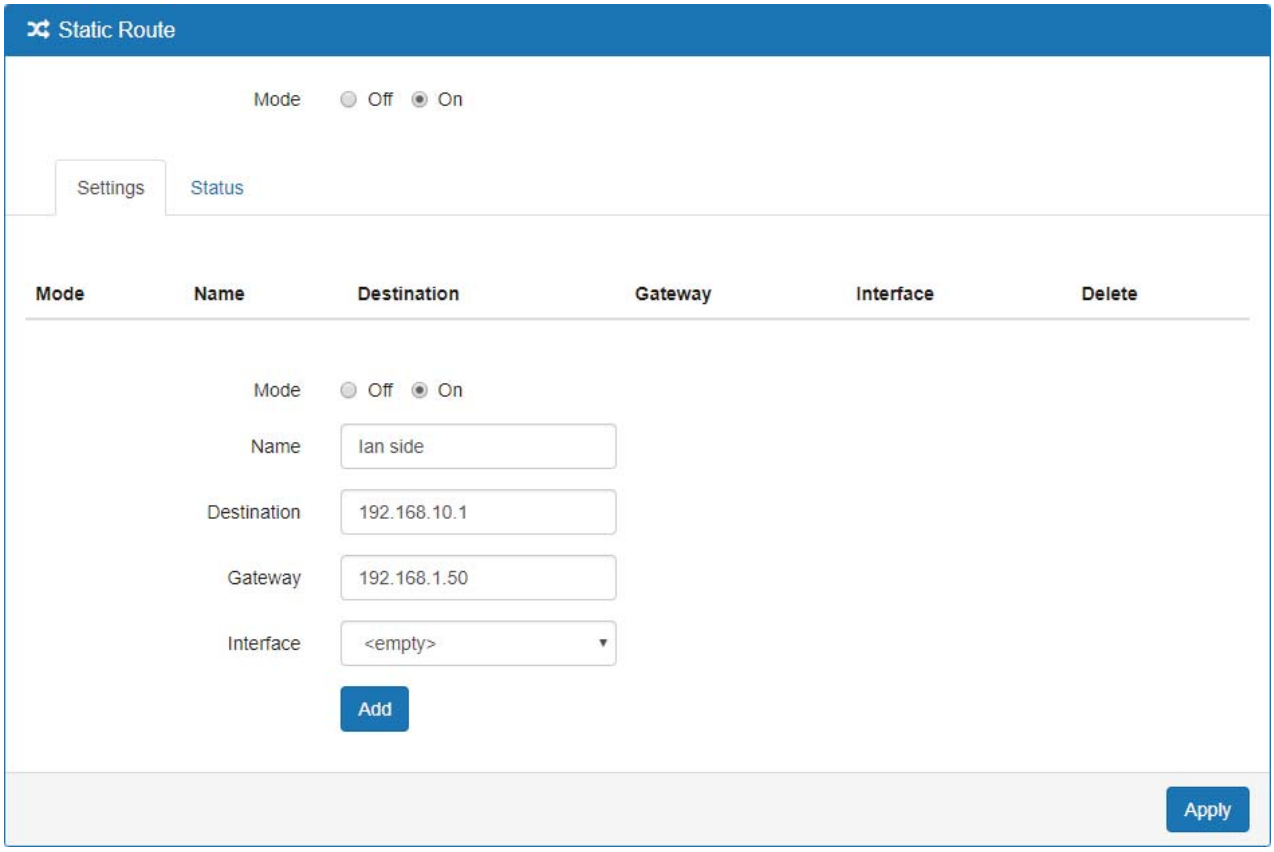


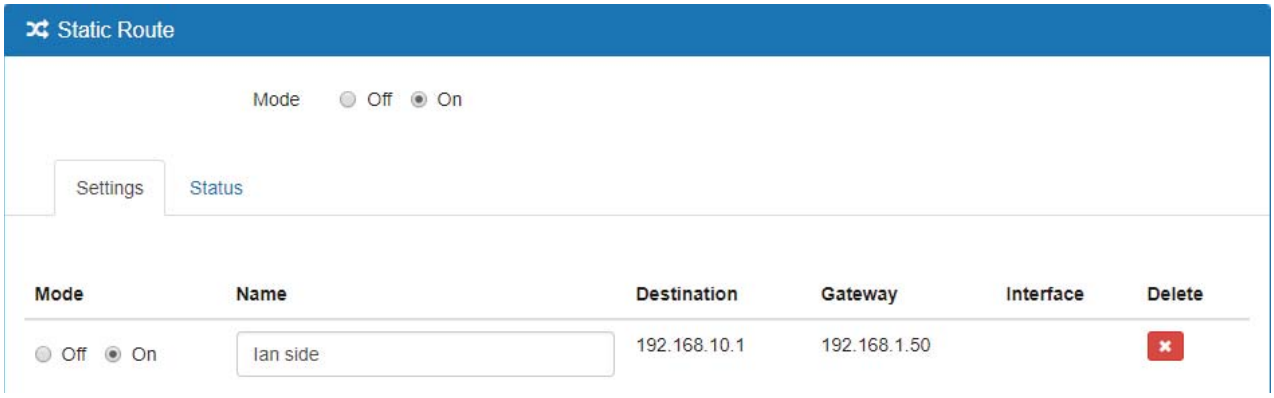
There are two examples to introduce how to work for routing.

Example 1: Add IP Routing on LAN interface

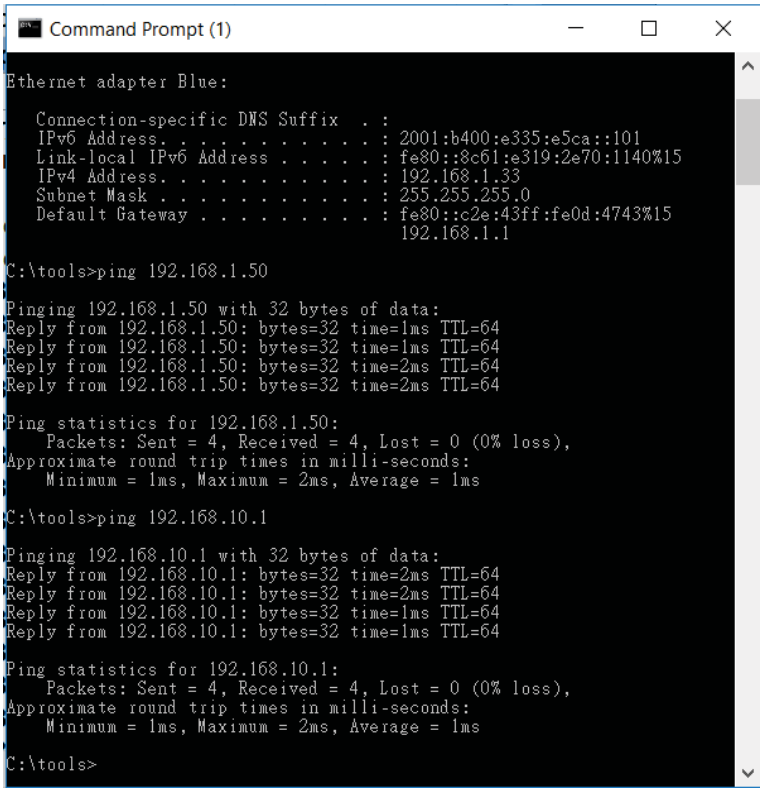
- Step 1: The cellular router for Static Route configuration
  The Mode is on at the settings section and add the routing.
- Step 2: Router-1 configuration is as below.

(1) Login to the Router-1 web site, and then "NAT disable".
(2) Configure LAN IP: 192.168.10.1
(3) Configure WAN IP: 192.168.1.50





- Result: PC-A sends ICMP packet to Router-1 LAN and WAN IP and they should have response.



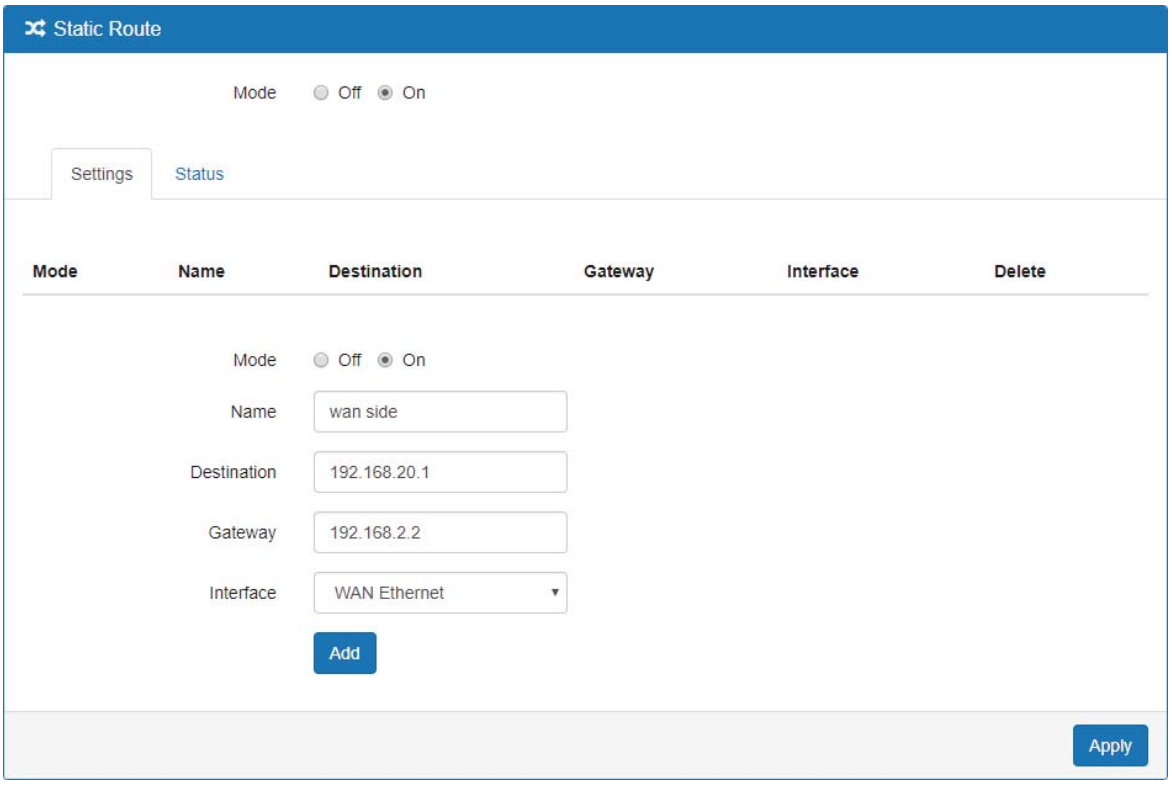
Example 2: Add IP Routing on WAN interface

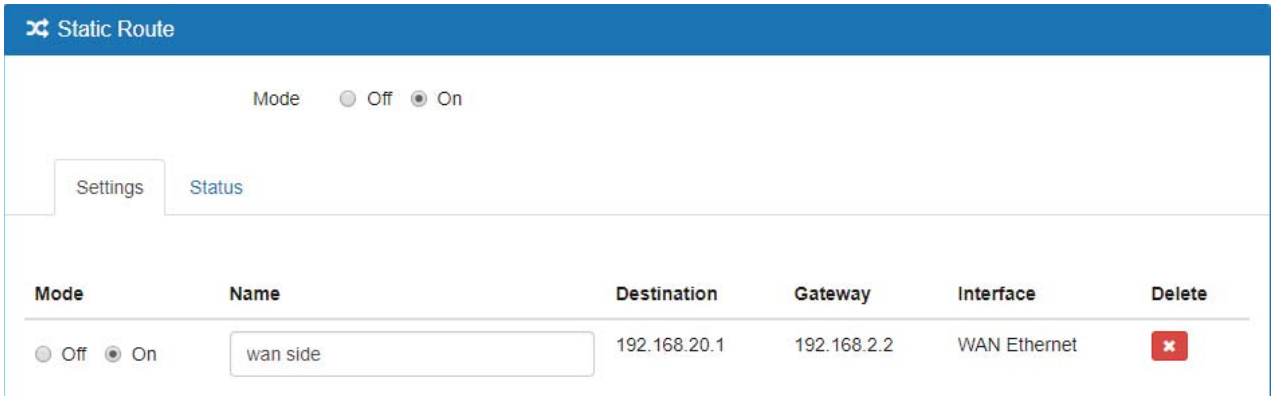
- Step1: The cellular router for Static Route configuration
  The Mode is on at the settings section and add the routing.
- Step2: Router-2 configuration is as below.

(1) Login to the Router-2 web site, and then "NAT disable".

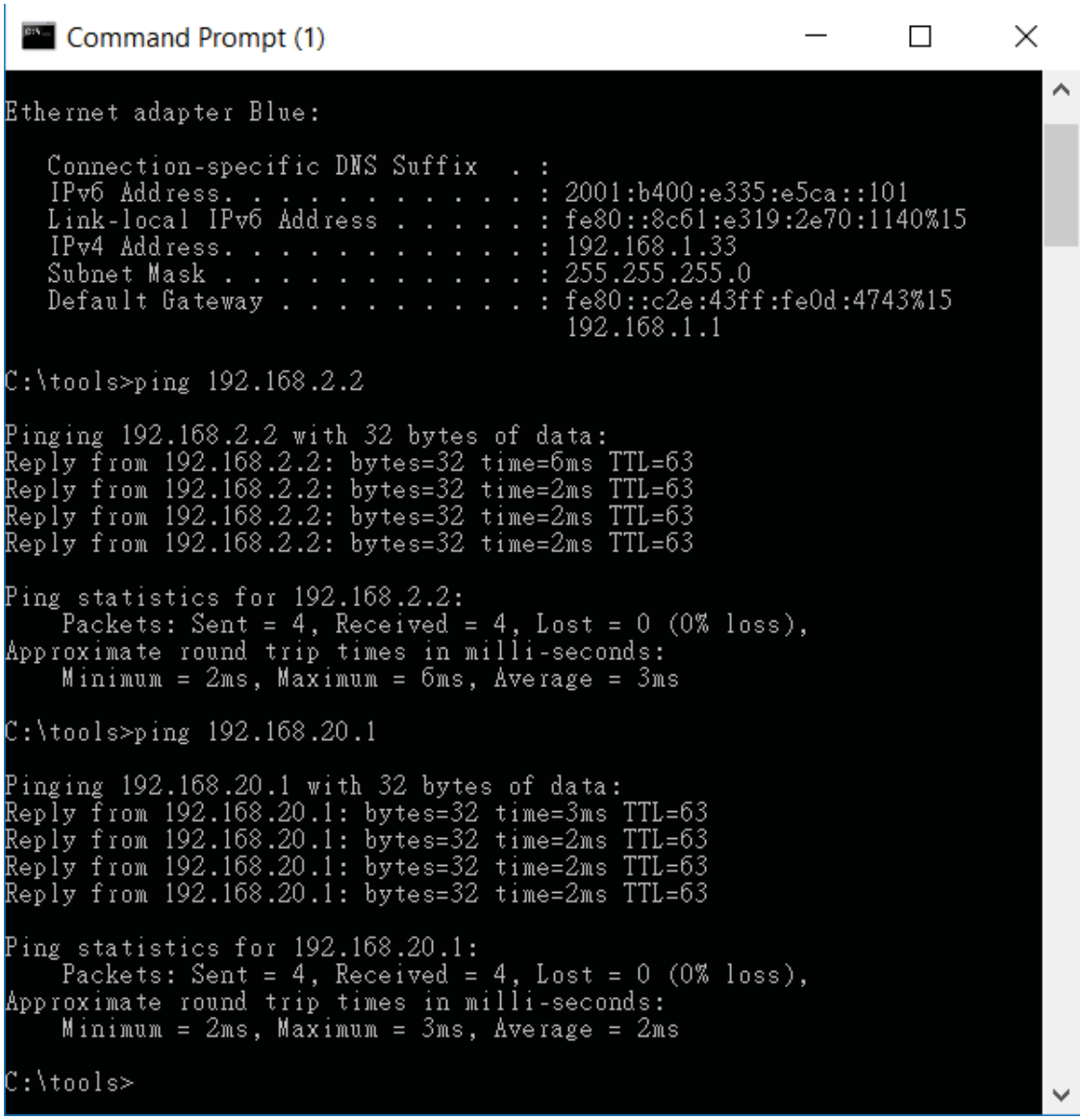
(2) Configure LAN IP: 192.168.20.1

(3) Configure WAN IP: 192.168.2.2





- Result: PC-A sends ICMP packet to Router-2 LAN and WAN IP and they should have response.



Warning:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.
NOTE: This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter

RF Exposure Statement

To maintain compliance with FCC's RF Exposure guidelines, This equipment should be installed and operated with minimum distance of 20Cm the radiator your body. This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter