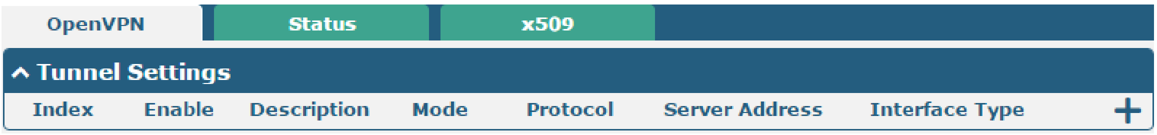
x509		
Item	**Description**	**Default**
PKCS # 12 Certificate	Select the PKCS # 12 certificate file to import into the route	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate's name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

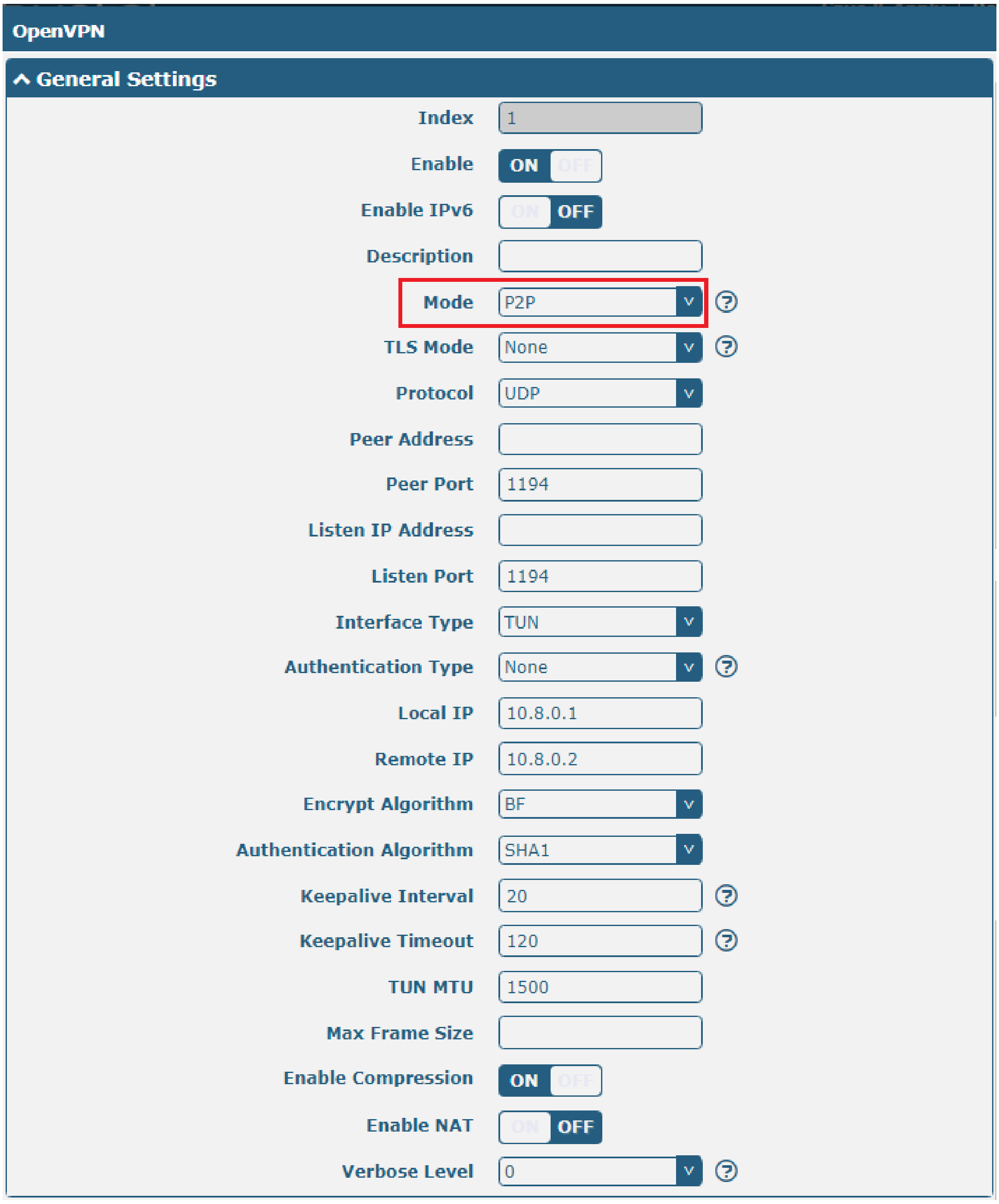
3.15 VPN>OpenVPN

This section allows you to set the OpenVPN and the related parameters.OpenVPNis an open-source software application that implementsvirtual private network(VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.Router supports point-to-point and point-to-points connections.
Click **Virtual Private Network> OpenVPN> OpenVPN**. The following information is displayed:

OpenVPN



Click + to add tunnel settings. The maximum count is 3.The window is displayed as below when choosing "None" as the authentication type.By default, the mode is "P2P".

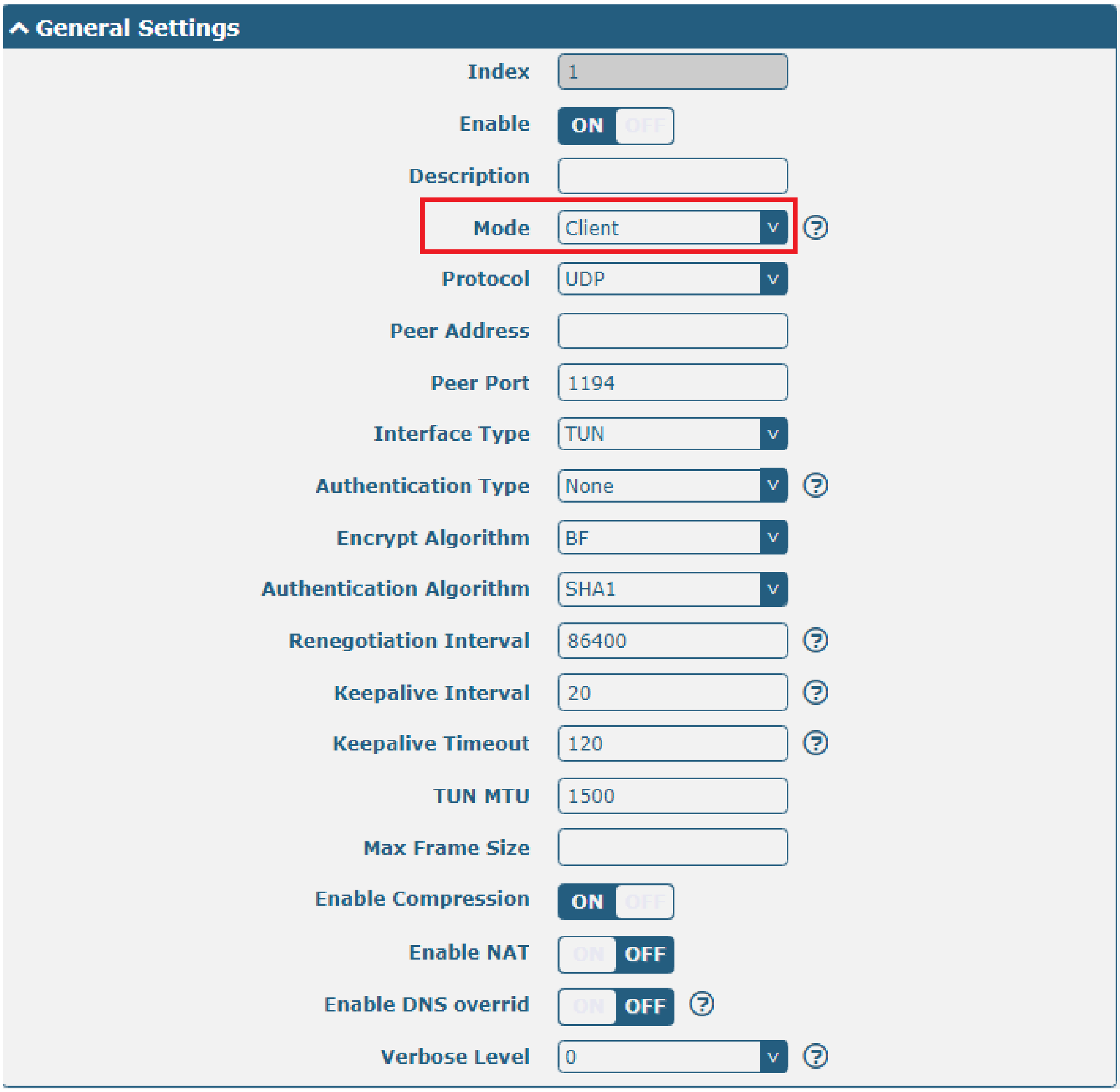


OpenVPN

General Settings

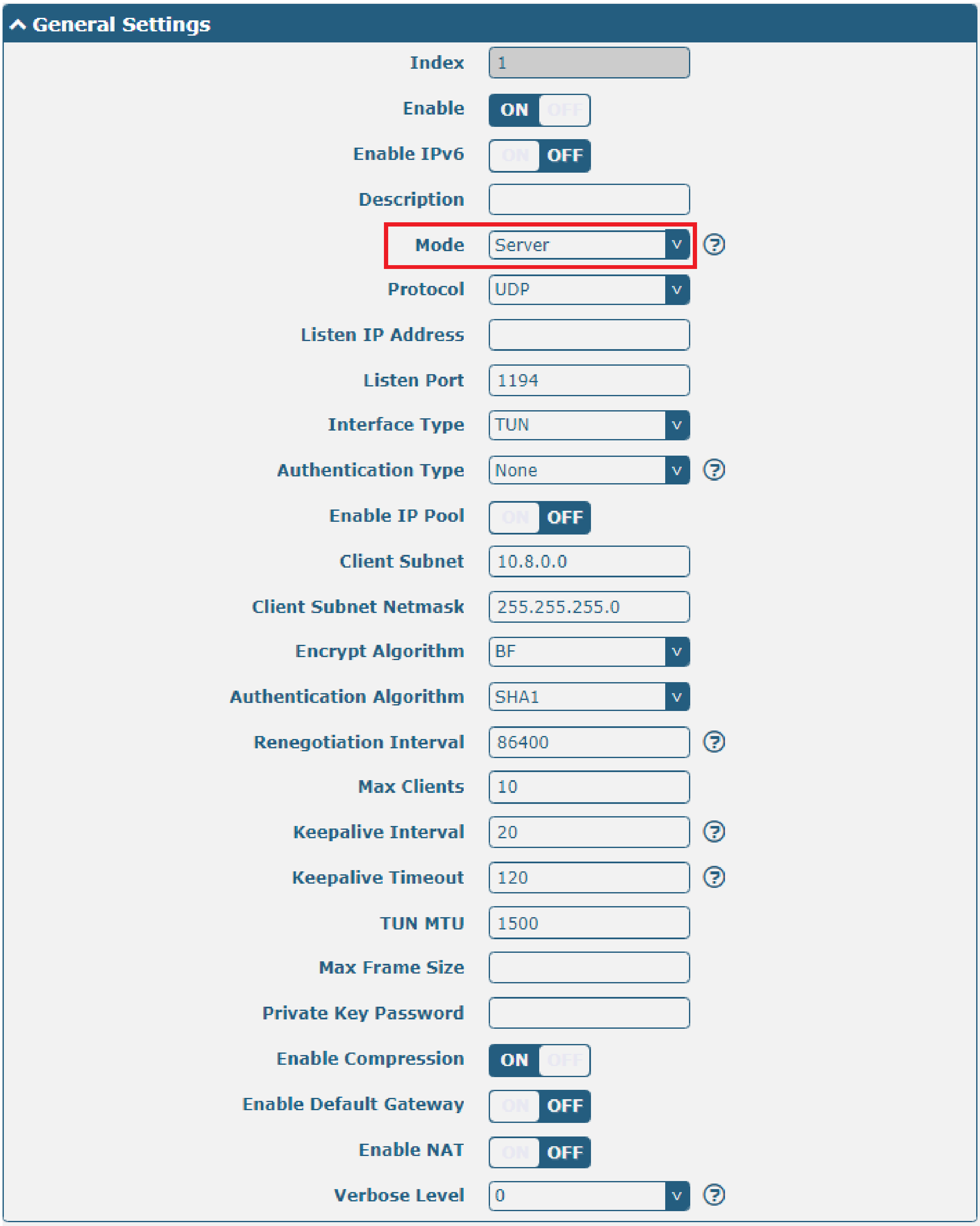
Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

The window is displayed as below when choosing “Client” as the mode.



Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	None
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	0

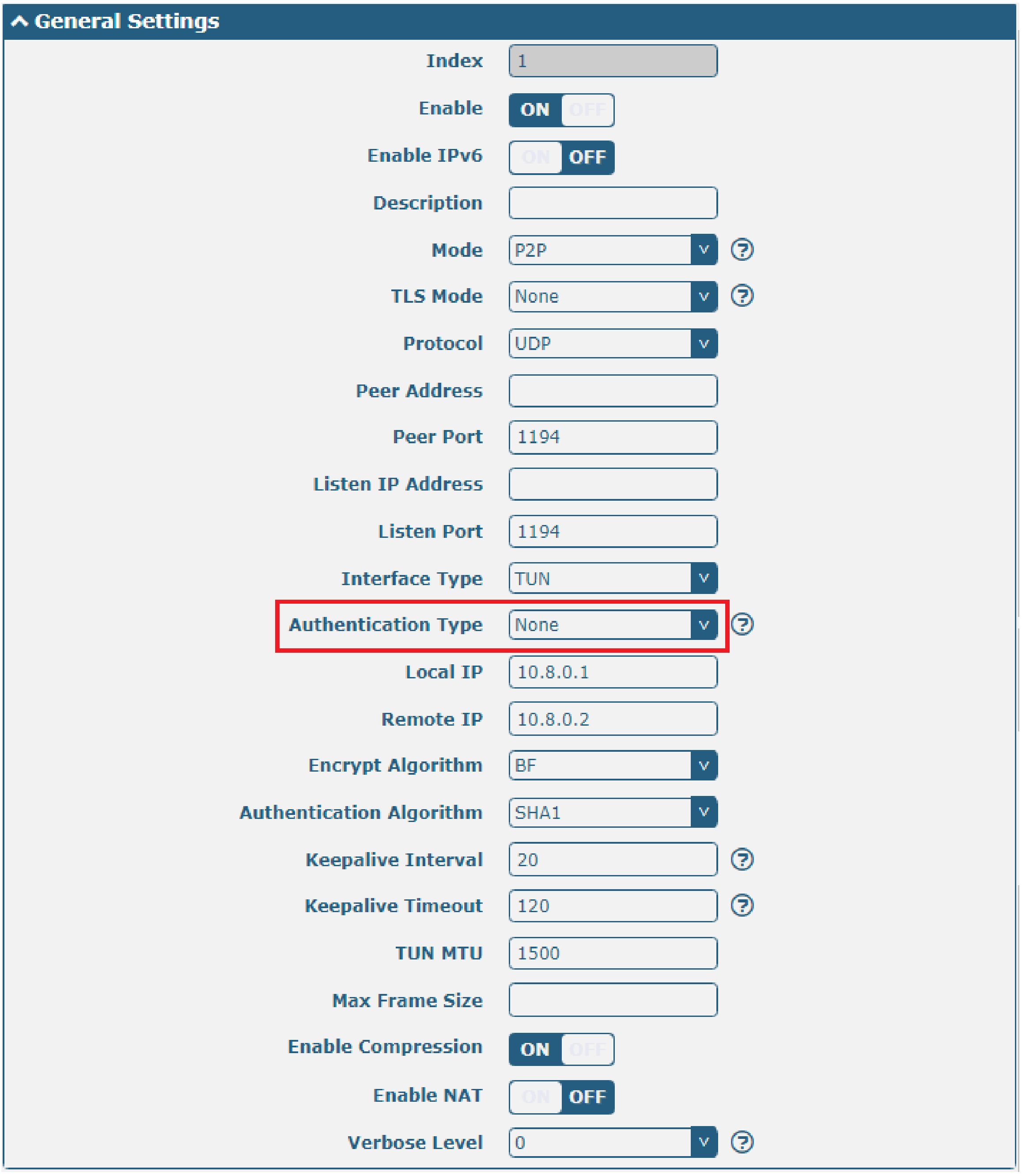
The window is displayed as below when choosing “Server” as the mode.



General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	Server
Protocol	UDP
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Enable IP Pool	OFF
Client Subnet	10.8.0.0
Client Subnet Netmask	255.255.255.0
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Max Clients	10
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON
Enable Default Gateway	OFF
Enable NAT	OFF
Verbose Level	0

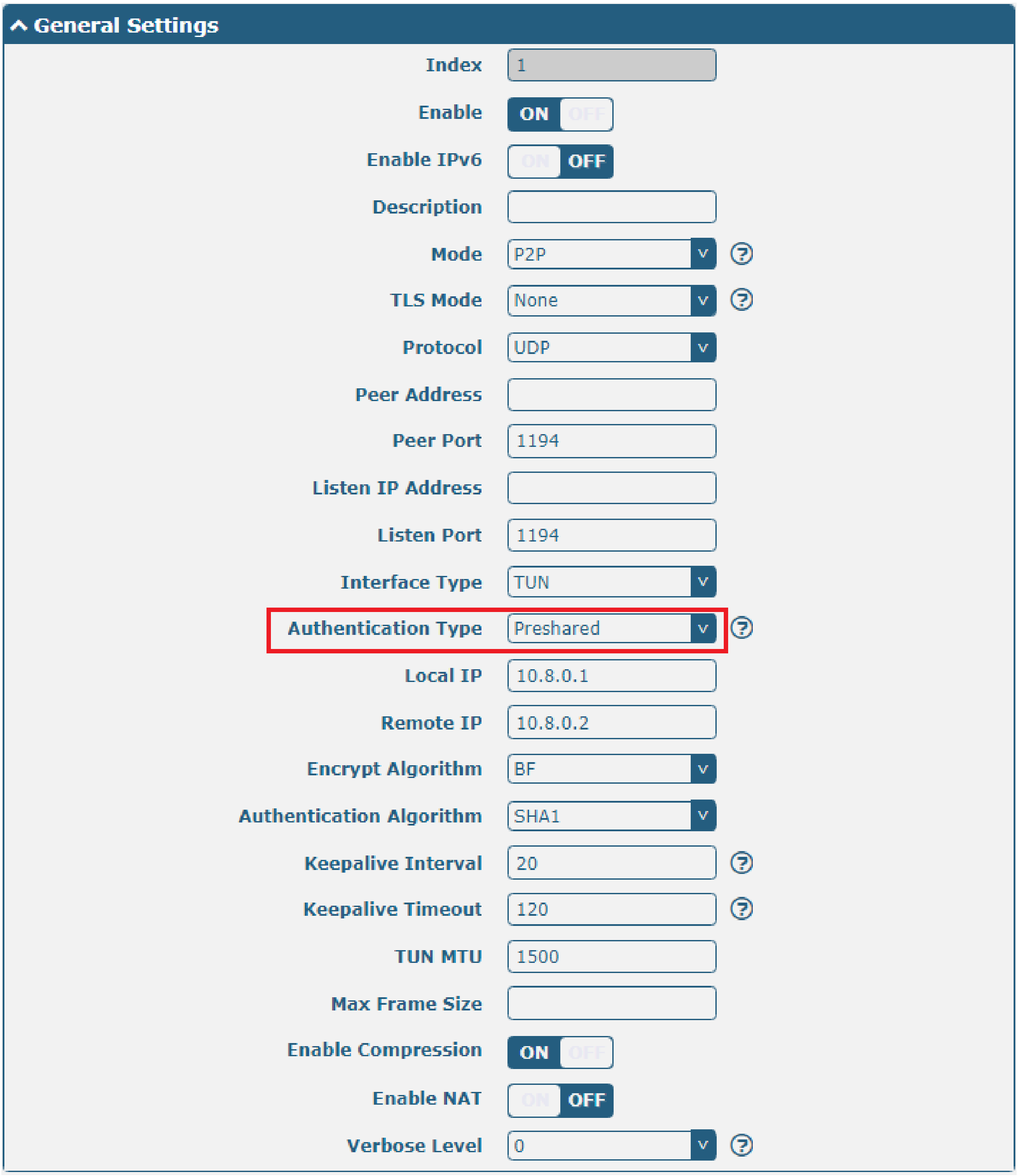
The window is displayed as below when choosing “None” as the authentication type.



General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

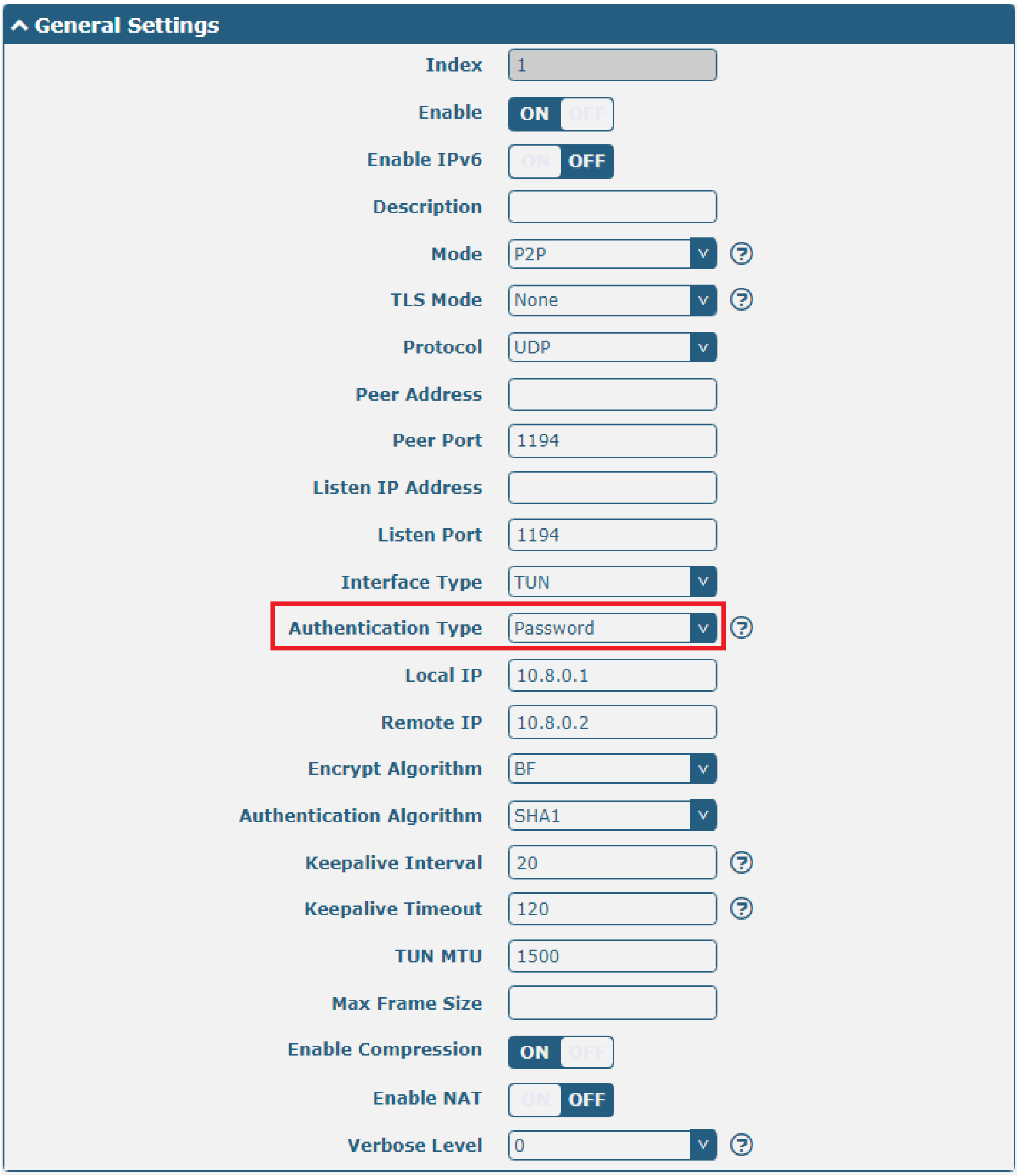
The window is displayed as below when choosing “Preshared” as the authentication type.



^ General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	Preshared
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

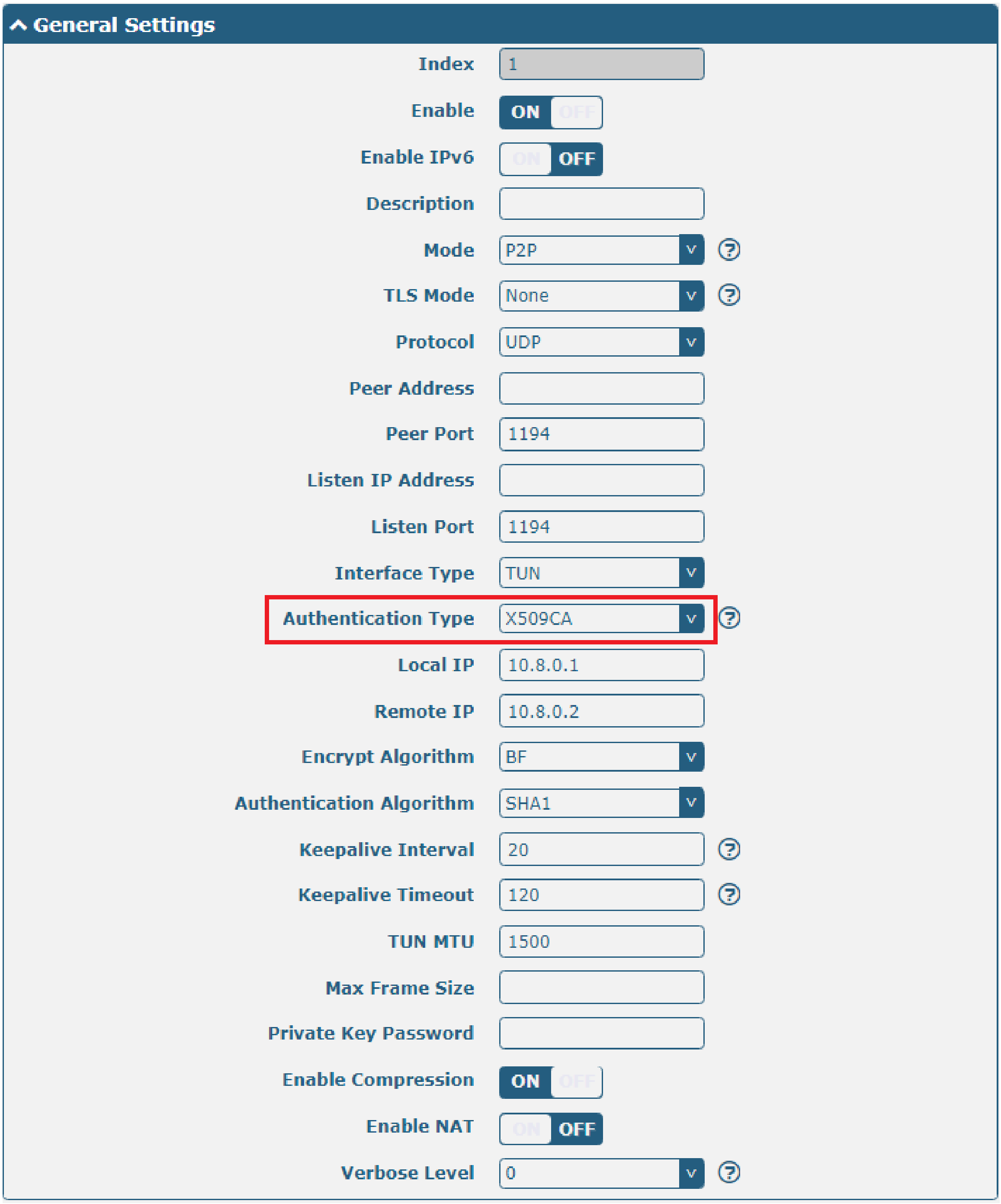
The window is displayed as below when choosing “Password” as the authentication type.



General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	Password
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

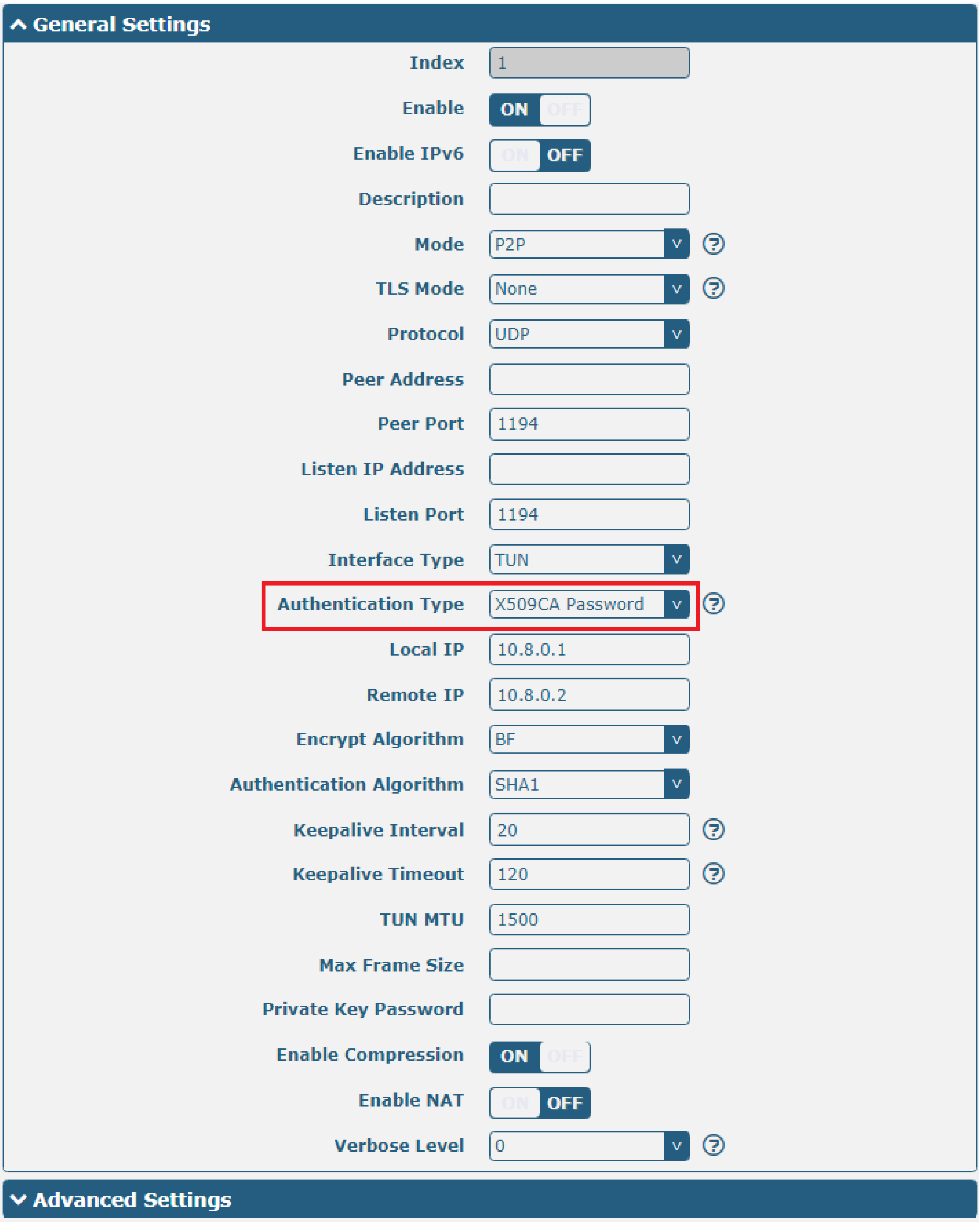
The window is displayed as below when choosing “X509CA” as the authentication type.



General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	X509CA
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

The window is displayed as below when choosing “X509CA Password” as the authentication type.

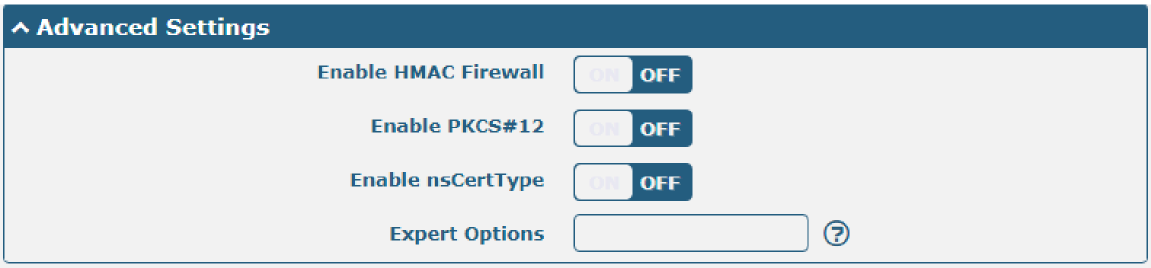


General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	X509CA Password
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

Advanced Settings

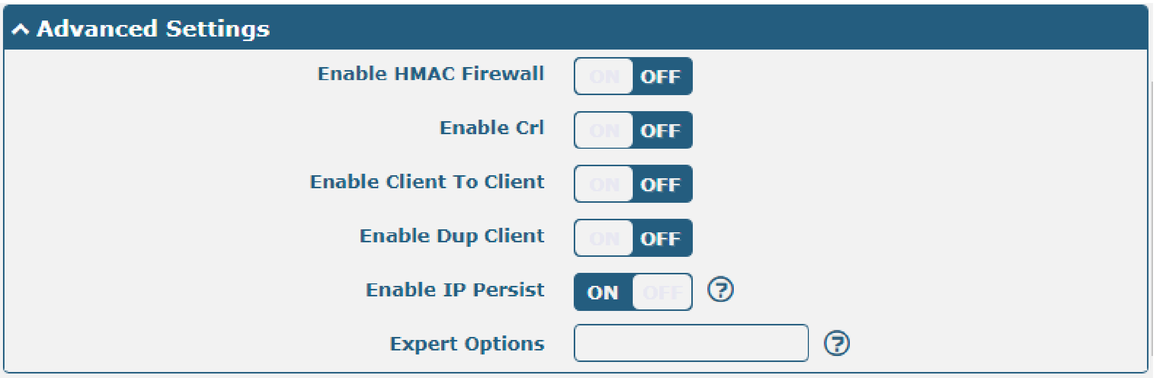
The window is displayed as below when choosing “Client” as the mode.



Advanced Settings

Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Enable nsCertType	OFF
Expert Options	

The window is displayed as below when choosing “Server” as the mode.



Advanced Settings

Enable HMAC Firewall: ON OFF

Enable Crl: ON OFF

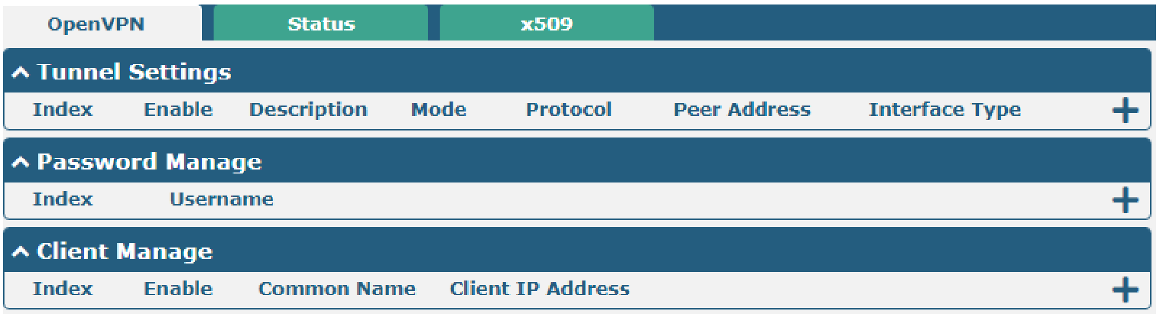
Enable Client To Client: ON OFF

Enable Dup Client: ON OFF

Enable IP Persist: ON OFF ?

Expert Options: ?

The window of "Virtual Private Network> OpenVPN> OpenVPN" is displayed as below when choosing “Server” as the modeand choosing “X509CA Password” as the authentication type.



Tunnel Settings

Index	Enable	Description	Mode	Protocol	Peer Address	Interface Type	+

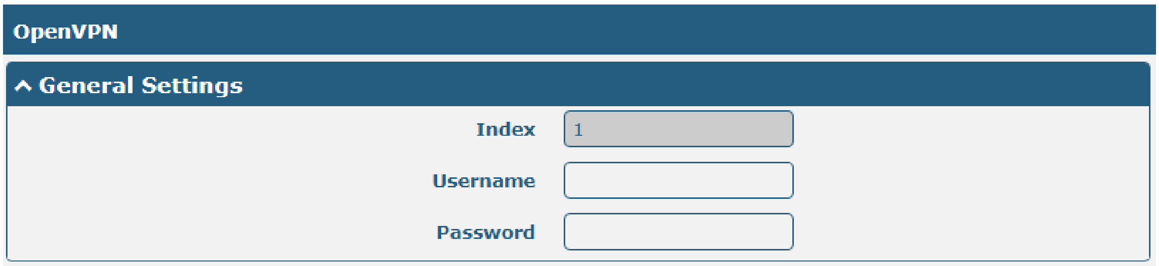
Password Manage

Index	Username	+

Client Manage

Index	Enable	Common Name	Client IP Address	+

Click User Password Management + to add username and password, as shown below:



OpenVPN

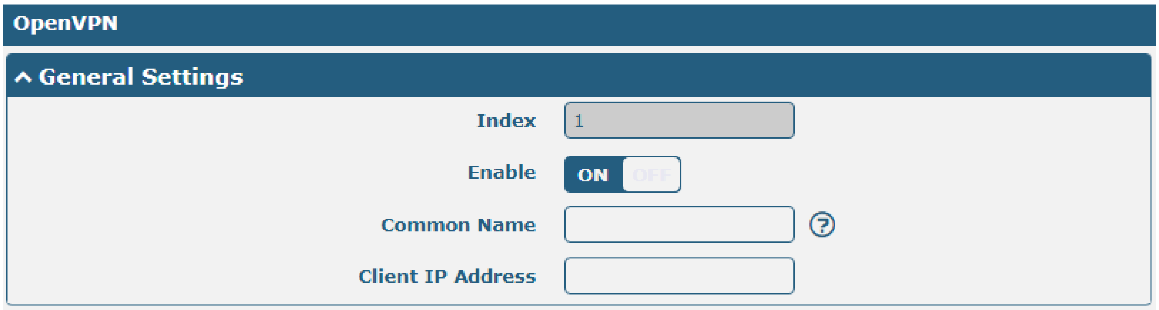
General Settings

Index: 1

Username:

Password:

Click Client Management + to add client information, as shown below:



OpenVPN

General Settings

Index: 1

Enable: ON OFF

Common Name: ?

Client IP Address:

General Settings @ OpenVPN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Enable Ipv6	Click the toggle button to enable / disable OpenVPN using IPv6.	OFF
Description	Enter a description for this OpenVPN tunnel.	Null

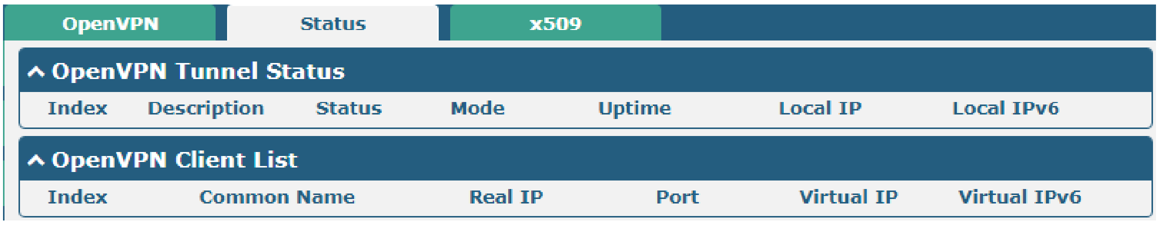
General Settings @ OpenVPN		
Item	**Description**	**Default**
Mode	Select from "P2P" or "Client".	Client
TLS Mode	Select from "None", "Client" or "Server".	None
Protocol	Select from "UDP", "TCP-Client" or "TCP-Server".	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listening port of the OpenVPN server.	1194
Listening Address	Local server address.	Null
Listening Port	Local server port.	1194
Interface Type	Select from "TUN" or "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
Authentication Type	Select from "None", "Preshared", "Password", "X509CA" and "X509CA Password". **Note**: "None" and "Preshared" authentication type are only working with P2P mode.	None
Enable IP Address Pool	Click the toggle button to enable / disable the IP address pool allocation function.	OFF
Starting Address	Defines the beginning of an IP address pool that assigns addresses to OpenVPN clients.	10.8.0.5
End Address	Defines the end of the IP address pool for assigning addresses to OpenVPN clients.	10.8.0.254
Client Network	Enter the client network IP.	10.8.0.0
Client Netmask	Enter the client netmask.	255.255.255.0
Username	Enter the username used for "Password" or "X509CA Password"authentication type.	Null
Password	Enter the password used for"Password" or "X509CA Password" authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES128", "AES192" and "AES256". • BF: Use 128-bit BF encryption algorithm in CBC mode • DES: Use 64-bit DES encryption algorithm in CBC mode • DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES192: Use 192-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	BF
Renegotiation Interval	Set the renegotiation interval. If connection failed, OpenVPN will renegotiate when the renegotiation interval reached.	86400

General Settings @ OpenVPN		
Item	**Description**	**Default**
Maximum Number of Clients	Set the maximum number of clients allowed to access the OpenVPN server.	10
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
MTU	Set the maximum transmission unit.	1500
Data Fragmentation	Set the maximum frame length.	Null
Private Key Password	Enter the private key password under the “X509CA” and “X509CA Password” authentication type.	Null
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the data stream of the header.	ON
Enable Default Gateway	Standalone switch button to enable / disable the default gateway function. After enabling, push the local tunnel address as the default gateway of the peer device.	OFF
Receive DNS Push	Standalone switch button to enable / disable receiving DNS push function.After enabling, it is allowed to receive DNS information pushed by the peer.	OFF
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled,the source IP address of host behind router will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log and values from 0 to 11. • 0: No output except fatal errors • 1~4: Normal usage range • 5: Output R and W characters to the console for each packet read and write • 6~11: Debug info range	0
Advanced Settings @ OpenVPN		
Enable HMAC Firewall	Click the toggle button to enable/disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Click the toggle button to enable/disable the PKCS#12 certificate. It is an exchange of digital certificate encryption standard, used to describe personal identity information.	OFF
Enable nsCertType	Click the toggle button to enable/disable nsCertType. Require that peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Enable Crl	Click the toggle button to enable / disable the option. When enabled, client certificates can be revoked.	OFF
Enable Client to Client	Click the toggle button to enable / disable the option. When enabled, clients can communicate with each other.	OFF

General Settings @ OpenVPN		
Item	**Description**	**Default**
Enable Dup Client	Click the toggle button to enable / disable the option. After being enabled, the tunnel IPs obtained by multiple clients are different, and the tunnel IP of the client and the tunnel IP of the server are interoperable.	OFF
Enable IP Address Hold	Click the toggle button to enable / disable the option. When enabled, the IP in the address pool is obtained automatically.	ON
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ‘;’.	Null
Advanced Settings @ User Password Management		
Username	Custom tunnel connection username.	Null
Password	Custom tunnel connection password.	Null
Client Management		
Enable	Click the toggle button to enable / disable this option. When enabled, the client IP address can be managed.	OFF
Common Name	Set the certificate name.	Null
Client IP Address	Set a fixed client virtual IP.	Null

Status

This section allows you to view the status of the OpenVPN tunnel.



^ OpenVPN Tunnel Status

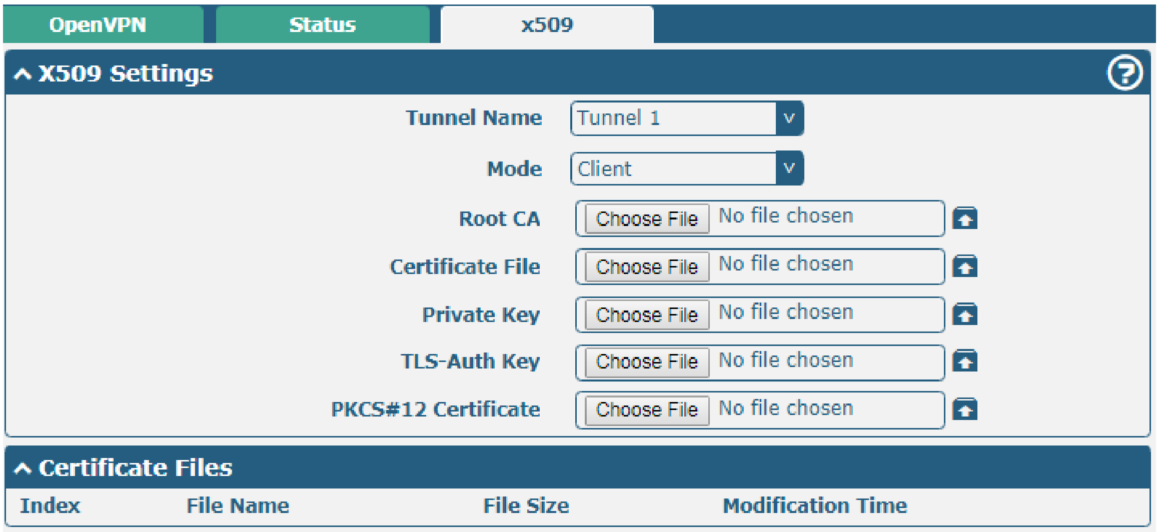
Index	Description	Status	Mode	Uptime	Local IP	Local IPv6

^ OpenVPN Client List

Index	Common Name	Real IP	Port	Virtual IP	Virtual IPv6

x509

User can upload the X509 certificates for the OpenVPN in this section.



X509 Settings

Tunnel Name: Tunnel 1

Mode: Client

Root CA: Choose File No file chosen

Certificate File: Choose File No file chosen

Private Key: Choose File No file chosen

TLS-Auth Key: Choose File No file chosen

PKCS#12 Certificate: Choose File No file chosen

Certificate Files

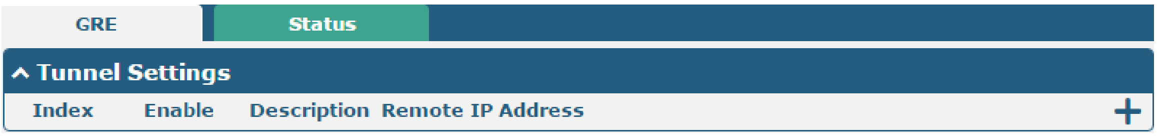
Index	File Name	File Size	Modification Time

x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5"or "Tunnel 6".	Tunnel 1
Tunnel mode	Select "P2P Mode", "Client Mode" or "Server Mode".	Client mode
Root certificate	Select the root certificate file to import into the router.	--
Certificate Files	Click on “Choose File” to locate the certificate file from your computer, and then import this file into your router.	--
Private Key	Select the private key file to import into the router.	--
TLS-Auth Key	Select the TLS-Auth key file to import into the router.	--
PKCS # 12 Certificate	Select the PKCS # 12 certificate file to import into the router.	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate’s name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

3.16 VPN > GRE

This section allows you to set the GRE and the related parameters.Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layerprotocols inside virtual point-to-point links over an Internet Protocol network.There are two main uses of the GRE protocol: enterprise internal protocol encapsulation and private address encapsulation.

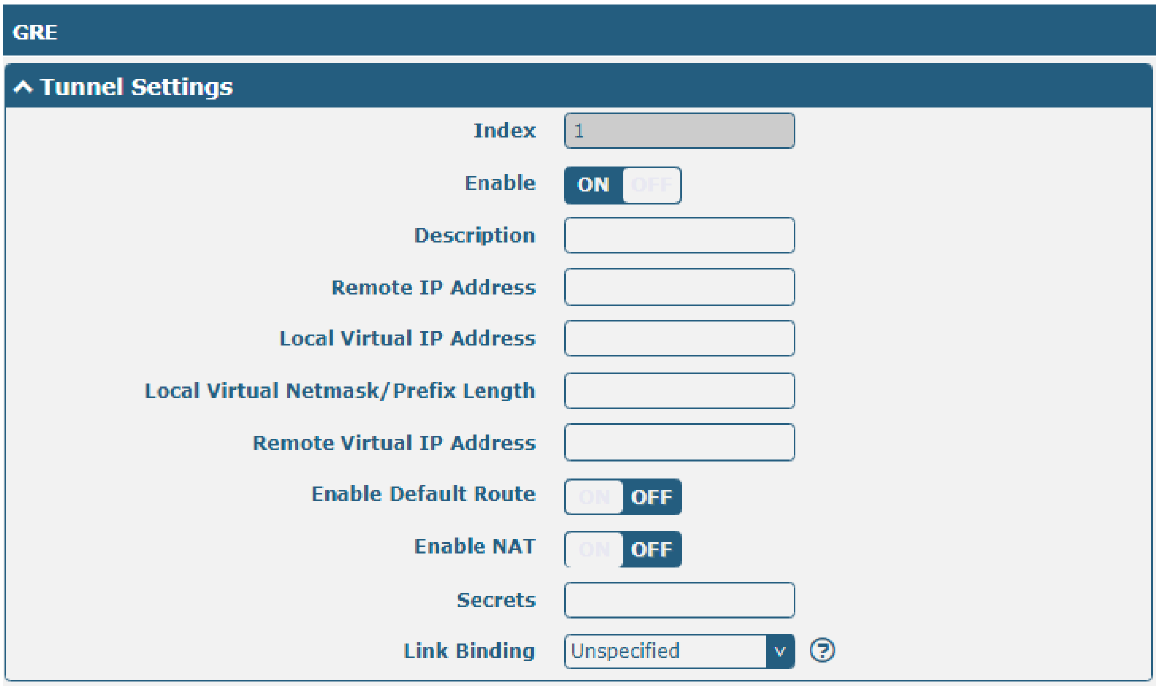
GRE



Tunnel Settings

Index	Enable	Description	Remote IP Address	+

Click + to add tunnel settings. The maximum count is 3.



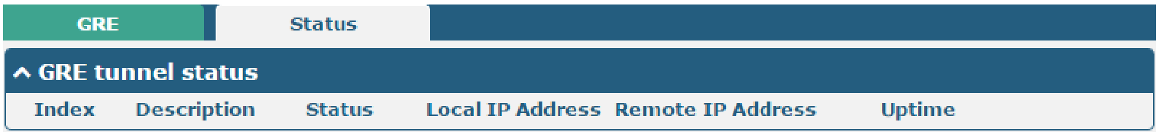
Tunnel Settings

Index	1
Enable	ON
Description	
Remote IP Address	
Local Virtual IP Address	
Local Virtual Netmask/Prefix Length	
Remote Virtual IP Address	
Enable Default Route	OFF
Enable NAT	OFF
Secrets	
Link Binding	Unspecified

Tunnel Settings @ GRE		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the localvirtual IP address of the GRE tunnel.	Null
Local Virtual Netmask/ IPv6 prefix length	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set the remotevirtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all the traffics of the router will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when router under NAT environment.	OFF
Secrets	Set the key of the GRE tunnel.	Null
Link Binding	Select from "WWAN1", "WWAN2", "WAN", or "WLAN".	Not bound

Status

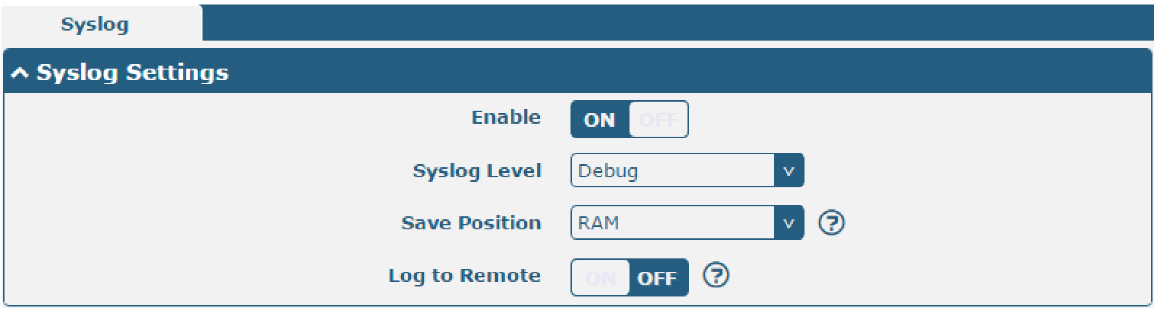
This section allows you to view the status of GRE tunnel.



Index | Description | Status | Local IP Address | Remote IP Address | Uptime

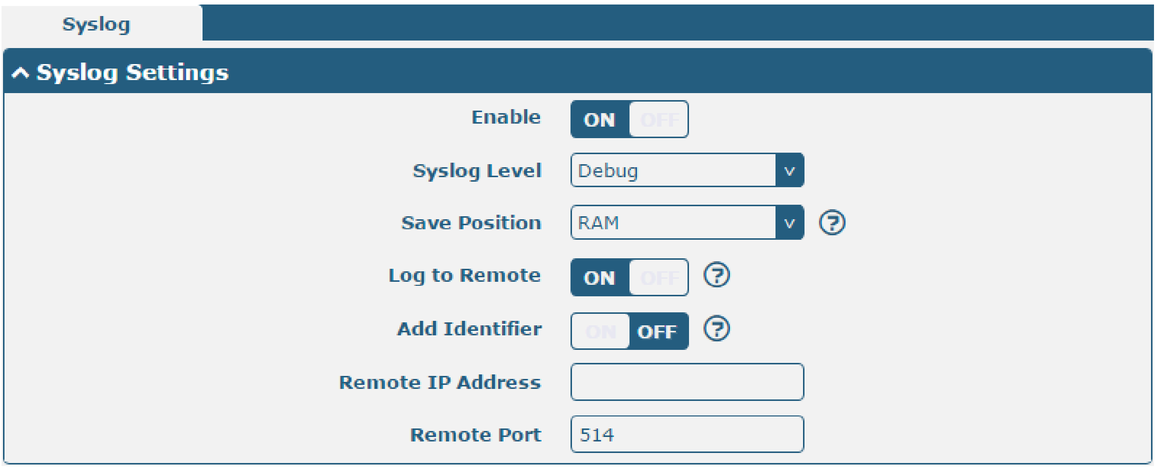
3.17 Services> Syslog

This section allows you to set the syslog parameters. The system log of the router can be saved in the local, also supports to be sent to remote log server and specified application debugging. By default, the “Log to Remote” option is disabled.



Enable: ON
Syslog Level: Debug
Save Position: RAM
Log to Remote: OFF

The window is displayed as below when enabling the “Log to Remote” option.



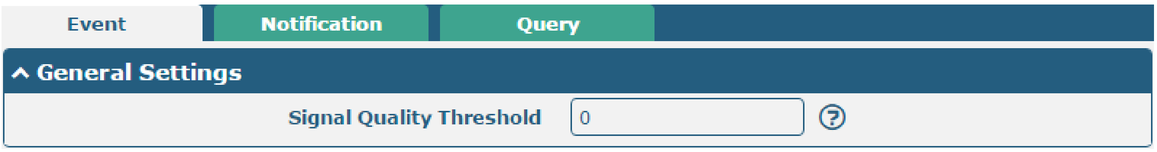
Enable: ON
Syslog Level: Debug
Save Position: RAM
Log to Remote: ON
Add Identifier: OFF
Remote IP Address:
Remote Port: 514

Syslog Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Syslog settings option.	OFF
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in details.	Debug
Save Position	Select the save position from “RAM”, “NVM” or “Console”. The data will be cleared after reboot when choose “RAM”. **Note**: It's not recommended that you save syslog to NVM (Non-Volatile Memory)	RAM

	for a long time.	
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	OFF
Add Identifier	Click the toggle button to enable/disable this option. When enabled, you can add serial number to syslog message which used for loading Syslog to RobustLink.	OFF
Remote IP Address	Enter the IP address of syslog server when enabling the “Log to Remote” option.	Null
Remote Port	Enter the port of syslog server when enabling the “Log to Remote” option.	514

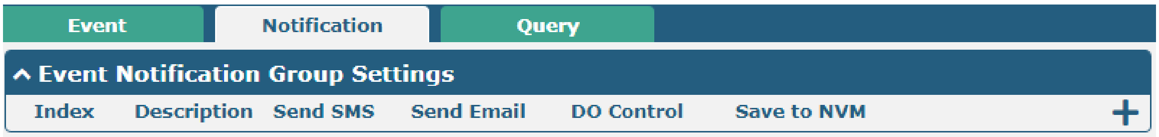
3.18 Services> Event

This section allows you to set the event parameters. Event feature provides an ability to send alerts by SMS or Email when certain system events occur.

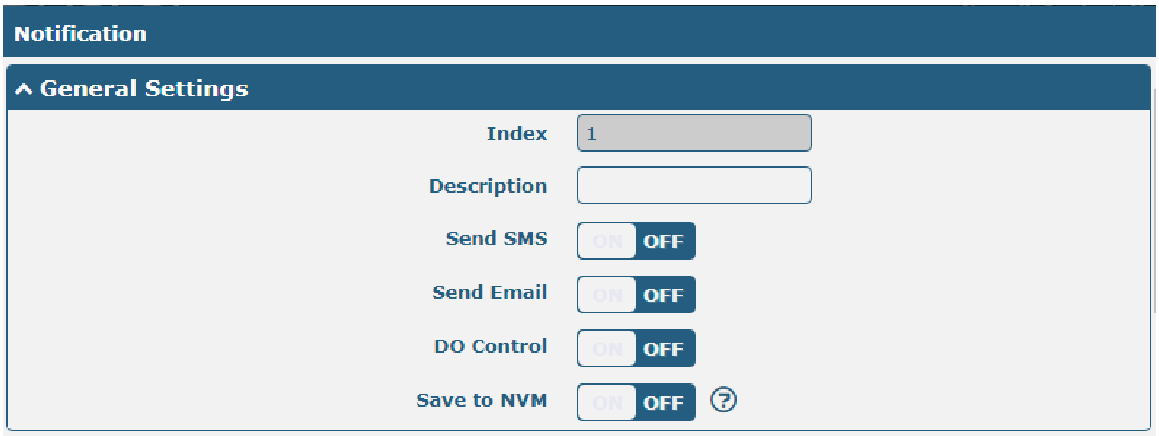


Signal Quality Threshold: 0

General Settings @ Event		
Item	**Description**	**Default**
Signal Quality Threshold	Set the threshold for signal quality. Router will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0



Click + button to add an Event parameters.



Index: 1

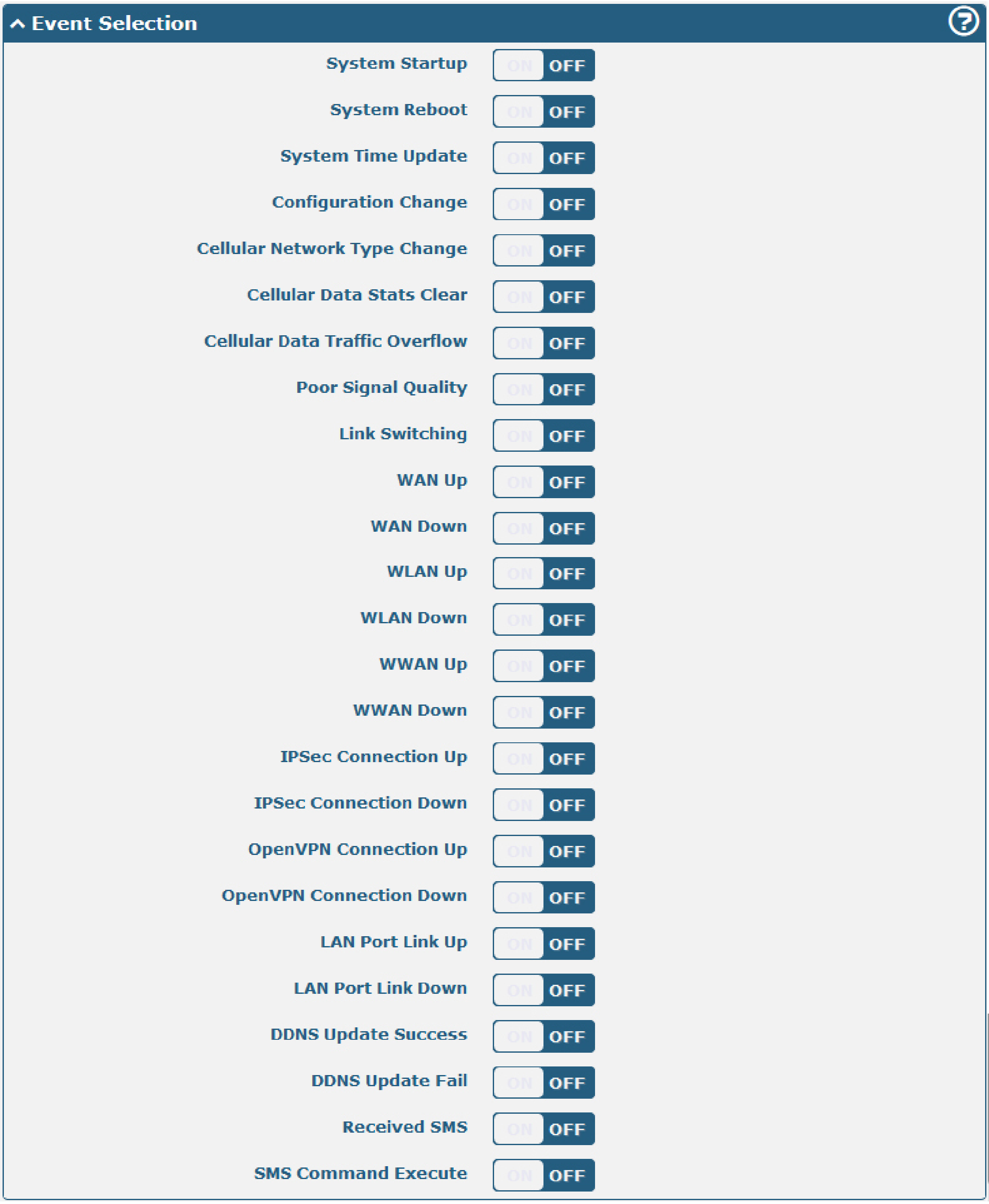
Description:

Send SMS: OFF

Send Email: OFF

DO Control: OFF

Save to NVM: OFF



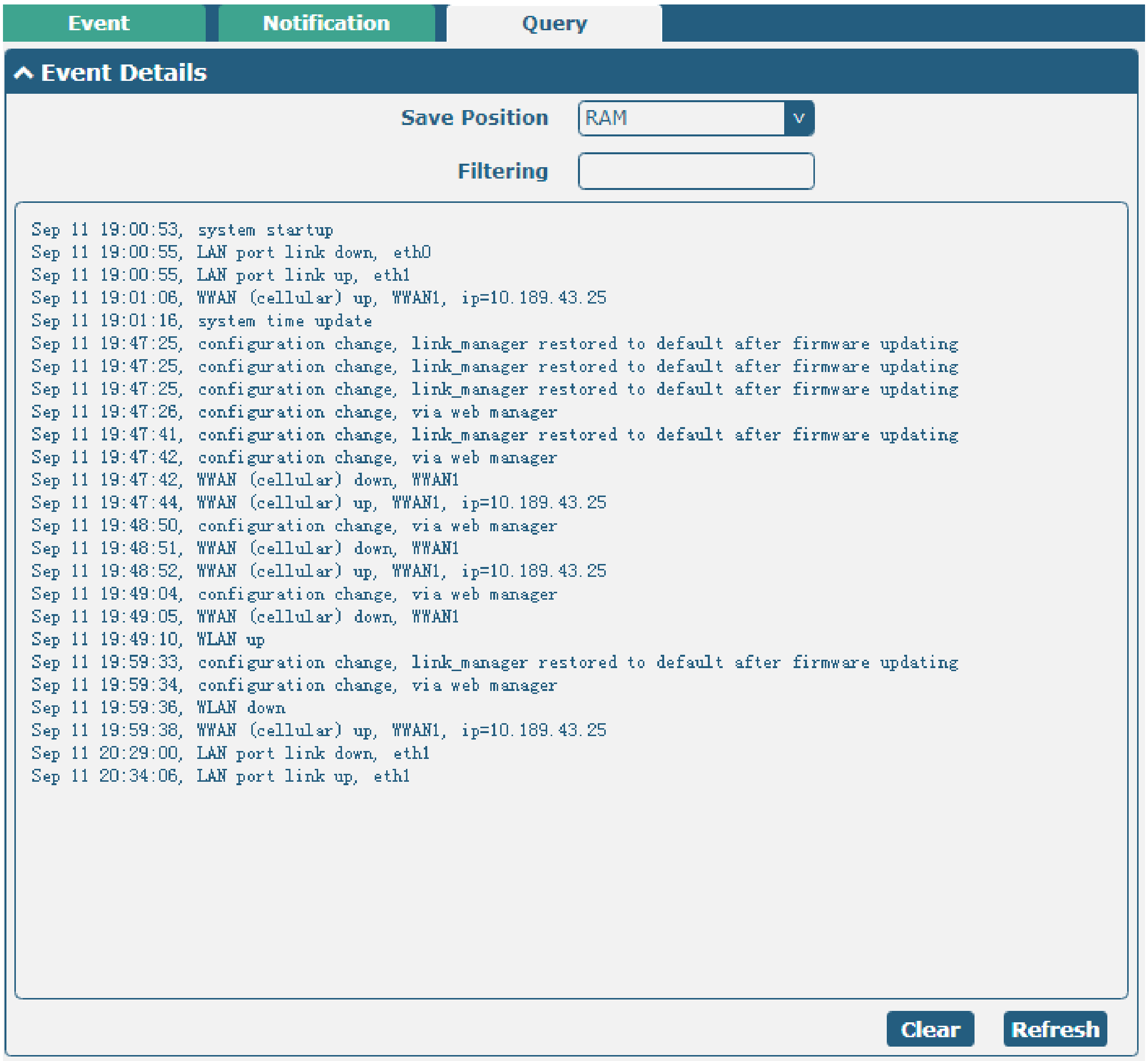
^ Event Selection

System Startup	OFF
System Reboot	OFF
System Time Update	OFF
Configuration Change	OFF
Cellular Network Type Change	OFF
Cellular Data Stats Clear	OFF
Cellular Data Traffic Overflow	OFF
Poor Signal Quality	OFF
Link Switching	OFF
WAN Up	OFF
WAN Down	OFF
WLAN Up	OFF
WLAN Down	OFF
WWAN Up	OFF
WWAN Down	OFF
IPSec Connection Up	OFF
IPSec Connection Down	OFF
OpenVPN Connection Up	OFF
OpenVPN Connection Down	OFF
LAN Port Link Up	OFF
LAN Port Link Down	OFF
DDNS Update Success	OFF
DDNS Update Fail	OFF
Received SMS	OFF
SMS Command Execute	OFF

General Settings @ Notification		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in “3.21 Services > Email”,and use ‘;’to separate each number.	OFF
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email addressin “3.21 Services > Email”.	OFF

DO Control	Click the toggle button to enable / disable this option. After it is turned on, the event router will send it to the corresponding DO in the form of Low / High level.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

In the following window you can query various types of events record. Click Refresh to query filtered events while click Clear to clear the event records in the window.



Save Position: RAM

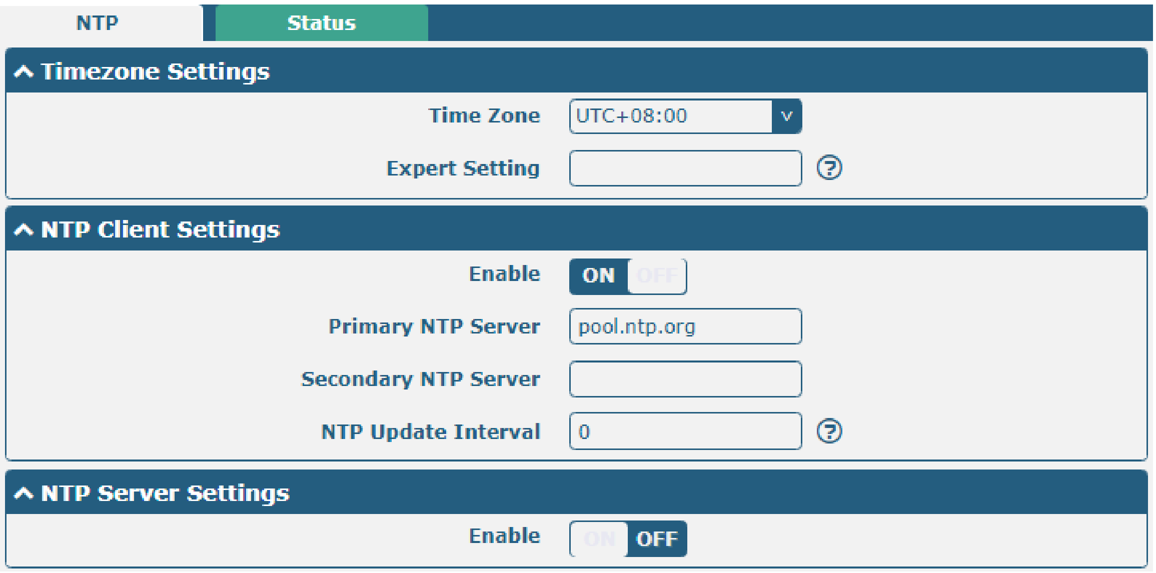
Filtering:

```
Sep 11 19:00:53, system startup
Sep 11 19:00:55, LAN port link down, eth0
Sep 11 19:00:55, LAN port link up, eth1
Sep 11 19:01:06, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:01:16, system time update
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:26, configuration change, via web manager
Sep 11 19:47:41, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:42, configuration change, via web manager
Sep 11 19:47:42, WWAN (cellular) down, WWAN1
Sep 11 19:47:44, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:48:50, configuration change, via web manager
Sep 11 19:48:51, WWAN (cellular) down, WWAN1
Sep 11 19:48:52, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:49:04, configuration change, via web manager
Sep 11 19:49:05, WWAN (cellular) down, WWAN1
Sep 11 19:49:10, WLAN up
Sep 11 19:59:33, configuration change, link_manager restored to default after firmware updating
Sep 11 19:59:34, configuration change, via web manager
Sep 11 19:59:36, WLAN down
Sep 11 19:59:38, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 20:29:00, LAN port link down, eth1
Sep 11 20:34:06, LAN port link up, eth1
```

Event Details		
Item	**Description**	**Default**
Save Position	Select the events' save position from"RAM" or "NVM". • RAM: Random-access memory • NVM: Non-Volatile Memory	RAM
Filter Message	Enter the filtering message based on the keywords set by users. Click the "Refresh" button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

3.19 Services > NTP

This section allows you to set the related NTP (Network Time Protocol) parameters, including Time zone, NTP Client and NTP Server.



^ Timezone Settings

Time Zone: UTC+08:00

Expert Setting:

^ NTP Client Settings

Enable: ON

Primary NTP Server: pool.ntp.org

Secondary NTP Server:

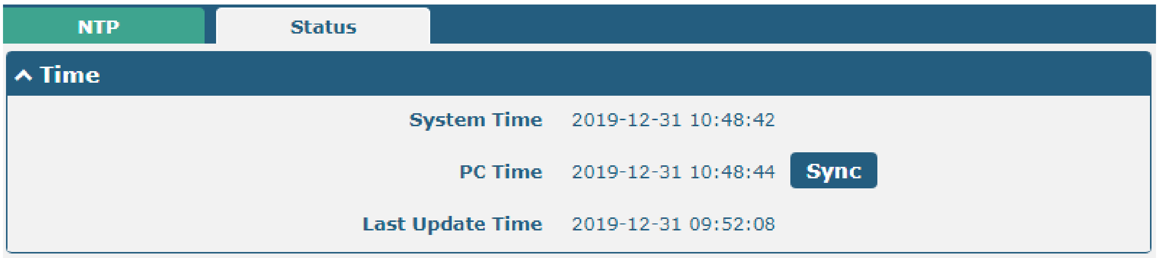
NTP Update Interval: 0

^ NTP Server Settings

Enable: OFF

NTP		
Item	**Description**	**Default**
	Timezone Settings	
Time Zone	Click the drop down list to select the time zone you are in.	UTC +08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
	NTP Client Settings	
Enable	Click the toggle button to enable/disable this option. Enable to synchronize time with the NTP server.	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
NTP Updateinterval	Enter the interval (minutes)synchronizing the NTP client time with the NTP server's. Minutes wait for next update, and 0 means update only once.	0
	NTP Server Settings	
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

This window allows you to view the current time of router and also synchronize the router time. Click Sync button to synchronize the router time with the PC's.



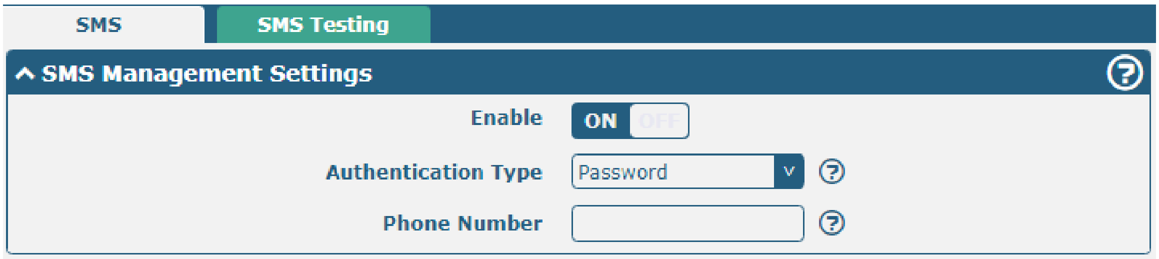
System Time 2019-12-31 10:48:42

PC Time 2019-12-31 10:48:44 Sync

Last Update Time 2019-12-31 09:52:08

3.20 Services> SMS

This section allows you to set SMS parameters. Router supports SMS management, and user can control and configure their routers by sending SMS.For more details about SMS control, refer to **4.1.2 SMS RemoteControl**.



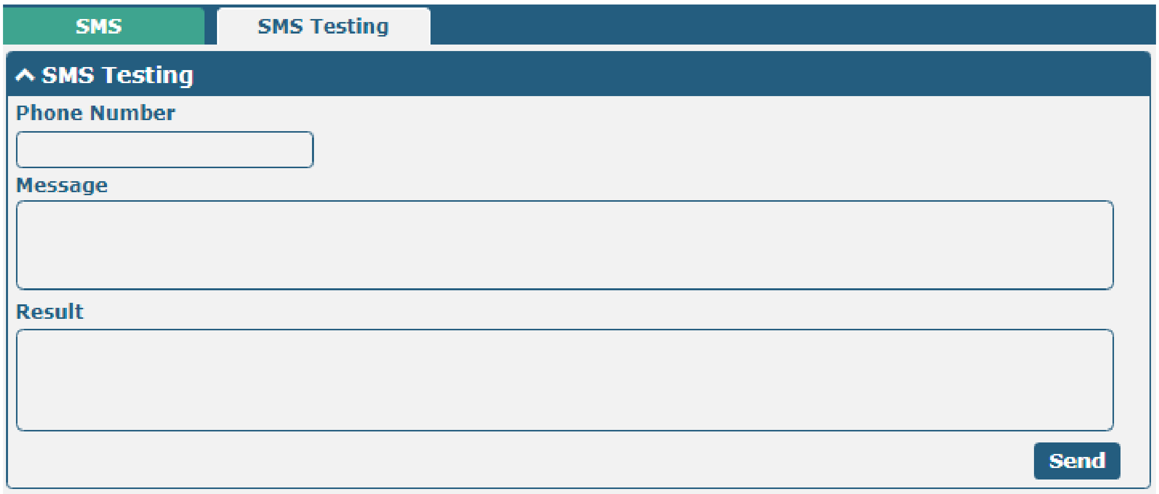
Enable ON OFF

Authentication Type Password

Phone Number

SMS Management Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from “Password”, “Phonenum” or “Both”. • Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be “username: password; cmd1; cmd2; …” **Note:** Set the WEB manager password in **System > User Management** section. • Phonenum: Use the Phone number for authentication, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “cmd1; cmd2; …” • Both: Use both the “Password” and “Phonenum” for authentication. User should set the Phone Number that is allowed for SMS management.The format of the SMS should be “username: password; cmd1; cmd2; …”	Password
Phone Number	Set the phone number used for SMS management, and use‘; ‘to separate each number. **Note**: It can be null when choose “Password” as the authentication type.	Null

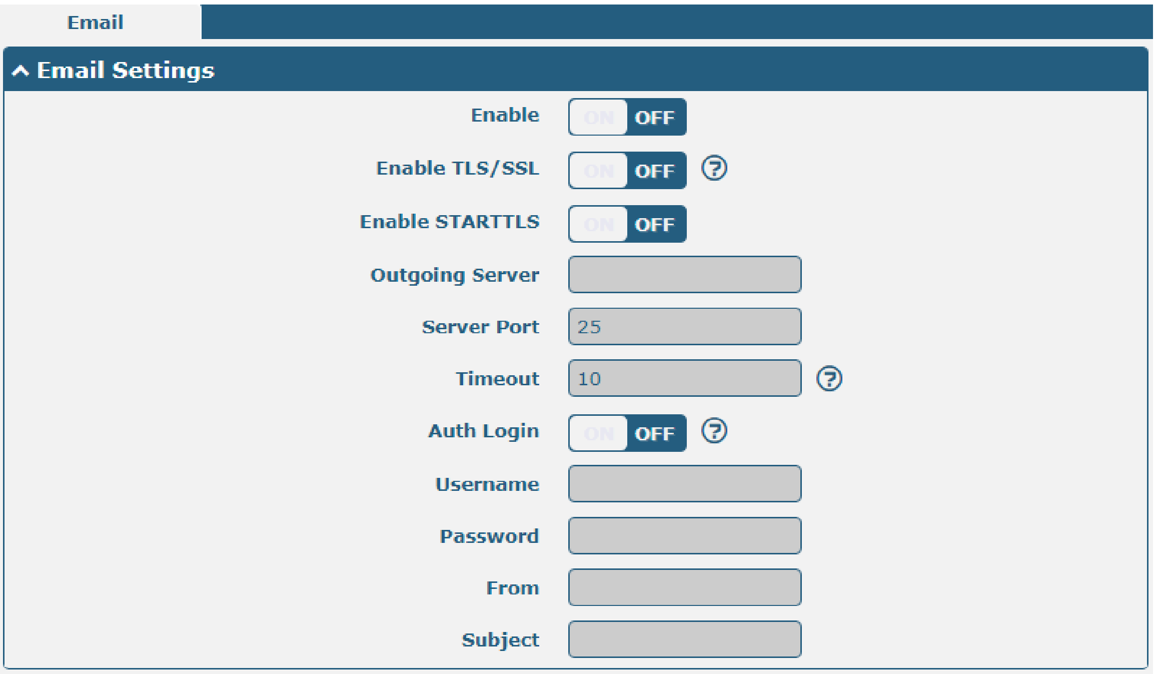
User can test the current SMS service whether it is available in this section.



SMS Testing		
Item	**Description**	**Default**
Phone Number	Enter the specified phone number which can receive the SMS from router.	Null
Message	Enter the message that router will send it to the specified phone number.	Null
Result	The result of the SMS test will be displayed in the result box.	Null
Send	Click the button to send the test message.	--

3.21 Services > Email

Email function supports to send the event notifications to the specified recipient by ways of email.

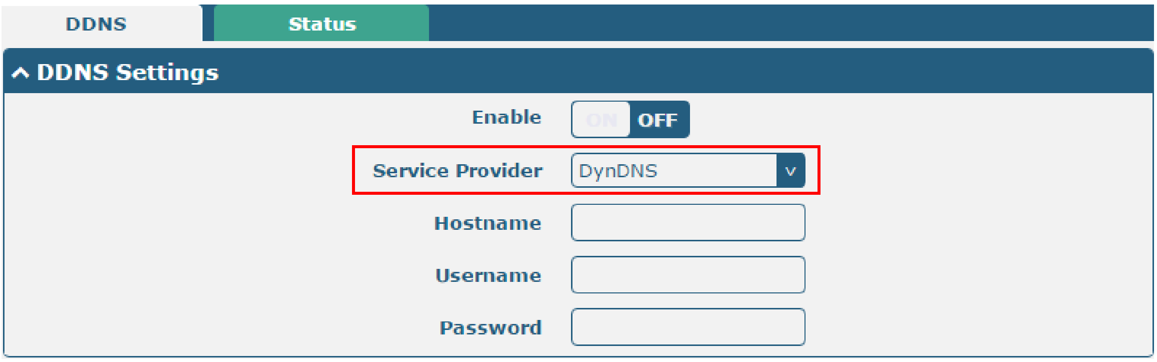


Enable: ON OFF
Enable TLS/SSL: ON OFF ?
Enable STARTTLS: ON OFF
Outgoing Server:
Server Port: 25
Timeout: 10 ?
Auth Login: ON OFF ?
Username:
Password:
From:
Subject:

Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disablethe Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable / disable STARTTLS encryption.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn't receive the email over this time, it will try to resend.	10
Auth Login	If the mail server supports AUTH login, you must enable this button and set a username and password.	OFF
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

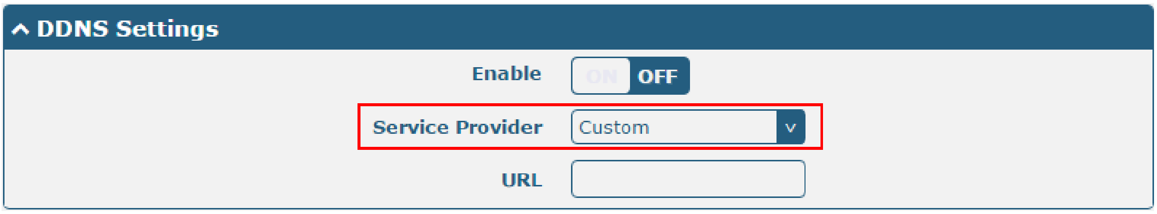
3.22 Services > DDNS

This section allows you to set the DDNS parameters.The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.The service provider defaults to "DynDNS", as shown below.



Service Provider: DynDNS

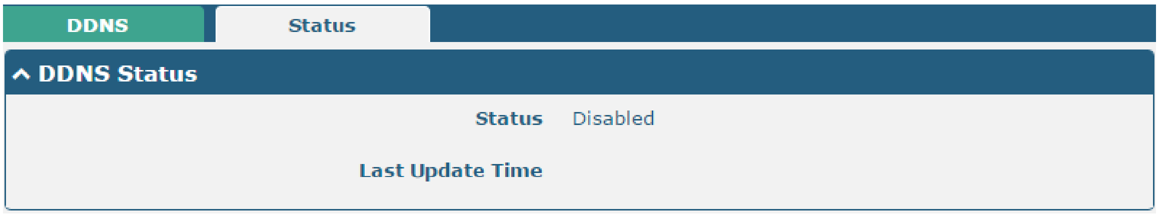
When "Custom" service provider chosen, the window is displayed as below.



Service Provider: Custom

DDNS Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disablethe DDNS option.	OFF
Service Provider	Select the DDNS service from “DynDNS”,“NO-IP”, “3322” or “Custom”. **Note:**The DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null

Click “Status” bar to view the status of the DDNS.



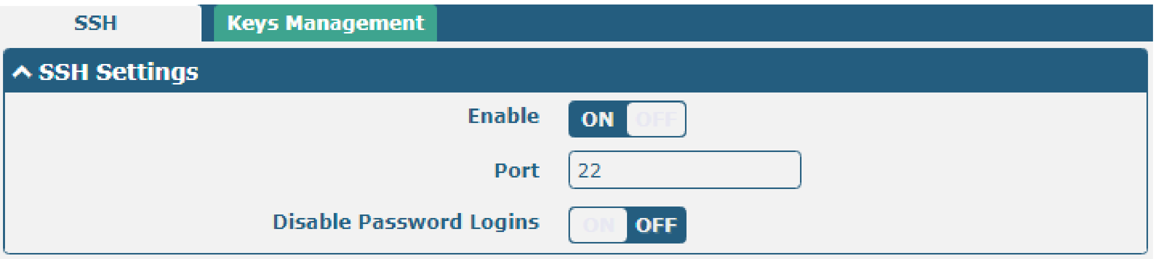
Status Disabled

Last Update Time

DDNS Status	
Item	**Description**
Status	Display the current status of the DDNS.
Last Update Time	Display the date and time for the DDNS was last updated successfully.

3.23 Services > SSH

Router supports SSH password access and secret-key access.



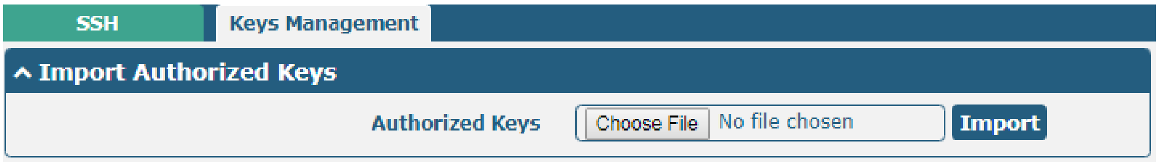
Enable ON OFF

Port 22

Disable Password Logins ON OFF

SSH Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the router via SSH.	ON
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/disable this option. When enabled, you cannot use username and password to access the router via SSH. In this	OFF

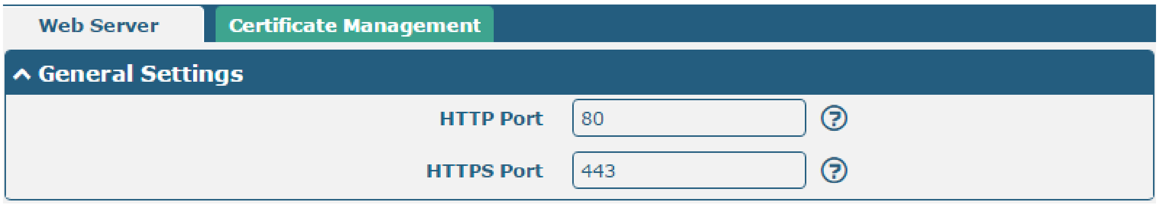
	case, only the key can be used for login.	



Import Authorized Keys	
Item	**Description**
Authorized Keys	Click on “Choose File” to locate anauthorized keyfrom your computer, and then click “Import” to import this key into your router. **Note**: This option is valid when enabling the password logins option.

3.24 Services > Web Server

This section allows you to modify the parameters of Web Server.

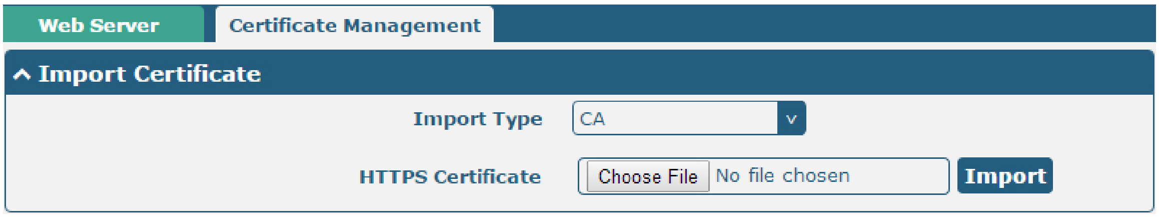


HTTP Port 80

HTTPS Port 443

General Settings @ Web Server		
Item	**Description**	**Default**
HTTP Port	Enter the HTTP port number you want to change in router’s Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login router’s Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in router’s Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login router’s Web Server. **Note**: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.	443

This section allows you to importthe certificate file into the router.



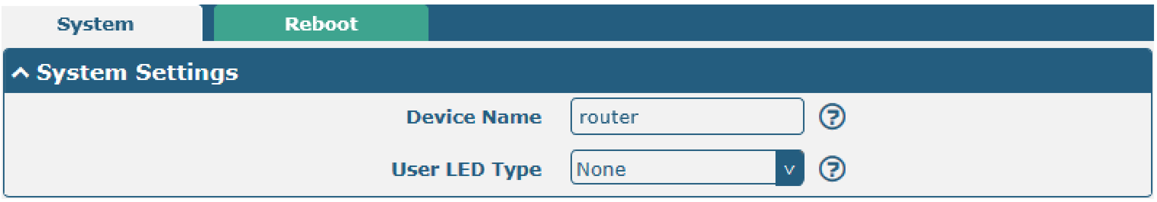
Import Type: CA

HTTPS Certificate: No file chosen

Import Certificate		
Item	**Description**	**Default**
Import Type	Select from "CA" and "Private Key". • CA: a digital certificate issued by CA center • Private Key: a private key file	CA
HTTPS Certificate	Click on "Choose File" to locate the certificate file from your computer, and then click "Import" to import this file into your router.	--

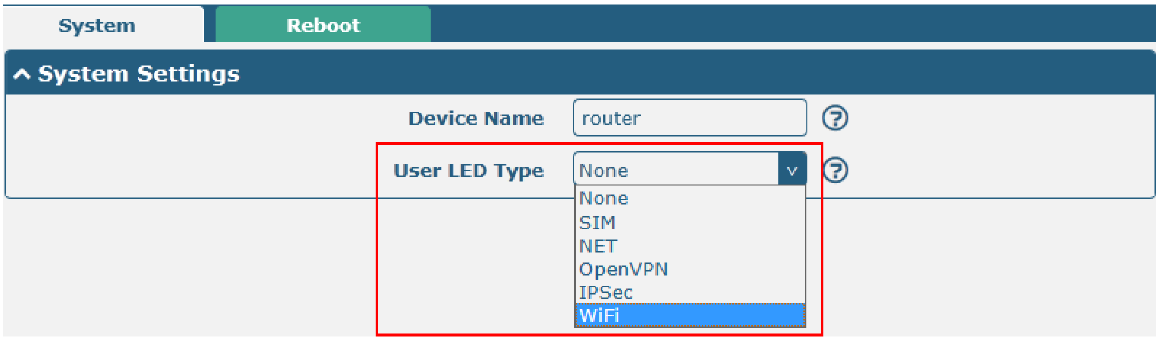
3.25 Services > Advanced

This section allows you to set the Advanced and parameters.



Device Name: router

User LED Type: None

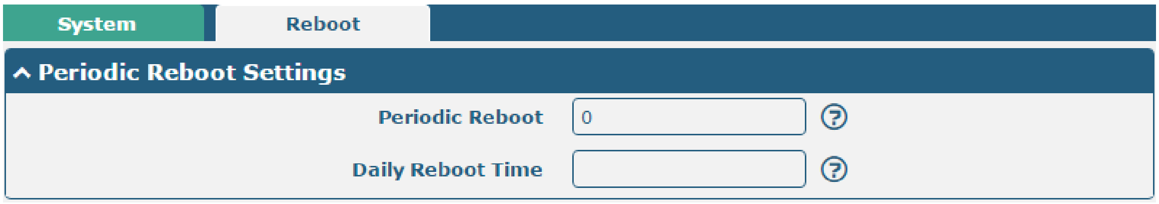


Device Name: router

User LED Type: None

System Settings		
Item	**Description**	**Default**
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	router
User LED Type	Specify the display type of your USR LED.Select from "None", "SIM", "NET", "OpenVPN", "IPSec" or "WiFi". • None: Meaningless indication, and the LED is off • SIM: USR indicator showing the SIMstatus • NET: USR indicator showing the NETstatus • OpenVPN: USR indicator showing the OpenVPN status • IPSec: USR indicator showing the IPsecstatus	None

	• WiFi: USR indicator showing the WiFi status **Note**: For more details about USR indicator, see “2.2 LED Indicators”.	



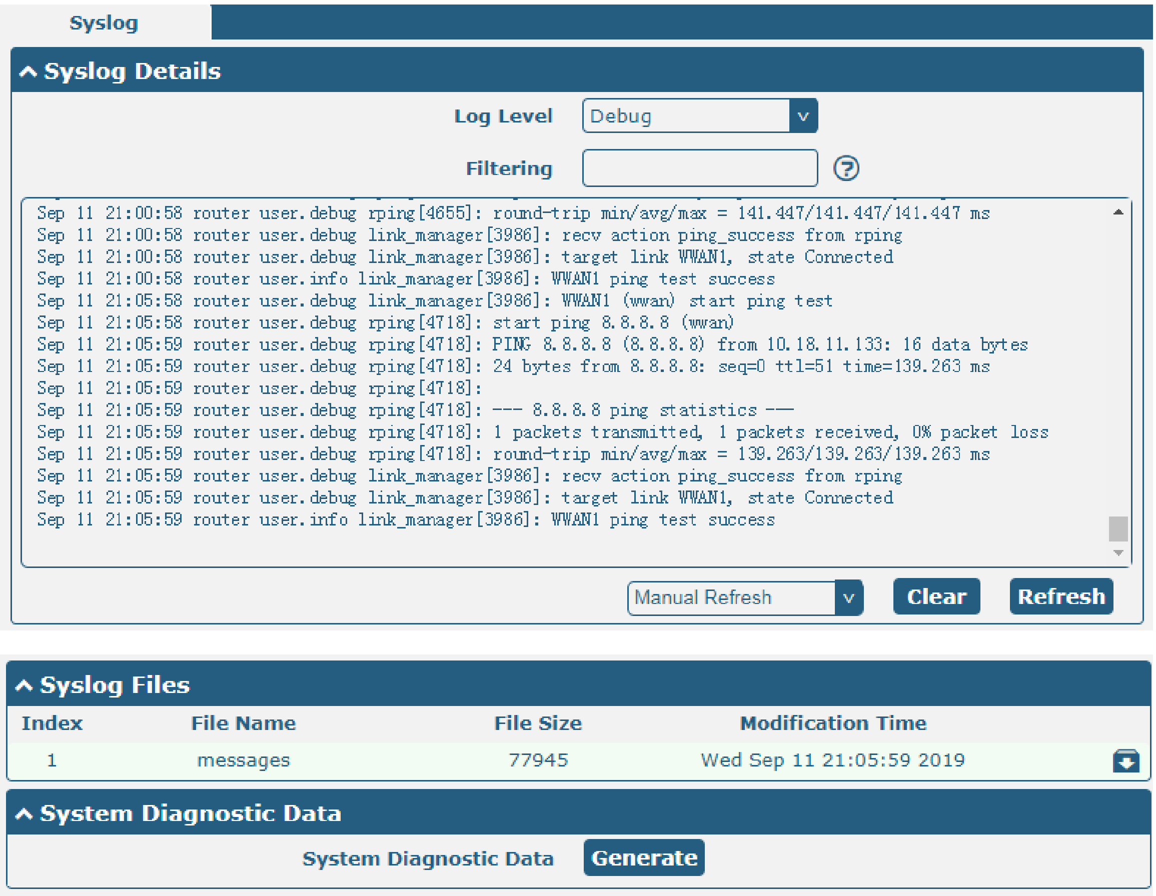
Periodic Reboot: 0

Daily Reboot Time:

Periodic Reboot Settings		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the router. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router. You should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid.Leave it empty means disable.	Null

3.26 System>Debug

This section allows you to check and download the syslog details.



Log Level: Debug

Filtering:

```
Sep 11 21:00:58 router user.debug rping[4655]: round-trip min/avg/max = 141.447/141.447/141.447 ms
Sep 11 21:00:58 router user.debug link_manager[3986]: recv action ping_success from rping
Sep 11 21:00:58 router user.debug link_manager[3986]: target link WWAN1, state Connected
Sep 11 21:00:58 router user.info link_manager[3986]: WWAN1 ping test success
Sep 11 21:05:58 router user.debug link_manager[3986]: WWAN1 (wwan) start ping test
Sep 11 21:05:58 router user.debug rping[4718]: start ping 8.8.8.8 (wwan)
Sep 11 21:05:59 router user.debug rping[4718]: PING 8.8.8.8 (8.8.8.8) from 10.18.11.133: 16 data bytes
Sep 11 21:05:59 router user.debug rping[4718]: 24 bytes from 8.8.8.8: seq=0 ttl=51 time=139.263 ms
Sep 11 21:05:59 router user.debug rping[4718]:
Sep 11 21:05:59 router user.debug rping[4718]: --- 8.8.8.8 ping statistics ---
Sep 11 21:05:59 router user.debug rping[4718]: 1 packets transmitted, 1 packets received, 0% packet loss
Sep 11 21:05:59 router user.debug rping[4718]: round-trip min/avg/max = 139.263/139.263/139.263 ms
Sep 11 21:05:59 router user.debug link_manager[3986]: recv action ping_success from rping
Sep 11 21:05:59 router user.debug link_manager[3986]: target link WWAN1, state Connected
Sep 11 21:05:59 router user.info link_manager[3986]: WWAN1 ping test success
```

Manual Refresh

Index	File Name	File Size	Modification Time
1	messages	77945	Wed Sep 11 21:05:59 2019

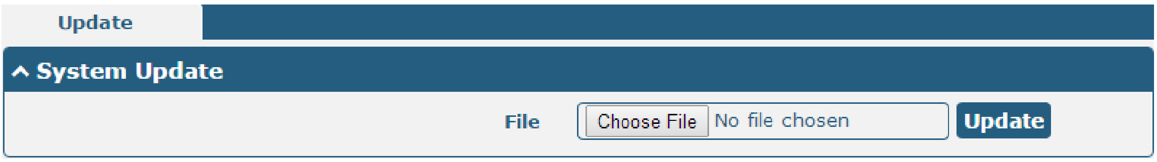
System Diagnostic Data

Syslog		
Item	**Description**	**Default**
Syslog Details		
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, “Error” which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Enter the filtering message based on the keywords. Use “&” to separate more than one filter message, such as “keyword1&keyword2”.	Null
Refresh	Select from “Manual Refresh”, “5 Seconds”, “10 Seconds”, “20 Seconds” or “30 Seconds”. You can select these intervals to refresh the log informationdisplayed in the follow box. If selecting “manual refresh”, you should click the refresh button to refresh the syslog.	Manual Refresh
Clear	Click the button to clear the syslog.	--
Refresh	Click the button to refresh the syslog.	--
Syslog Files		
Syslog Files List	It can show at most 5 syslog files in the list, the files’ name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.	--
System Diagnosing Data		
Generate	Click to generate the syslog diagnosing file.	--
Download	Click to downloadsystem diagnosing file.	--

3.27 System>Update

This section allows you to upgrade the router system and implement system update by importing and updating firmware files. Import a firmware file from the computer to the router, click Update and restart the device as prompted to complete the firmware update.

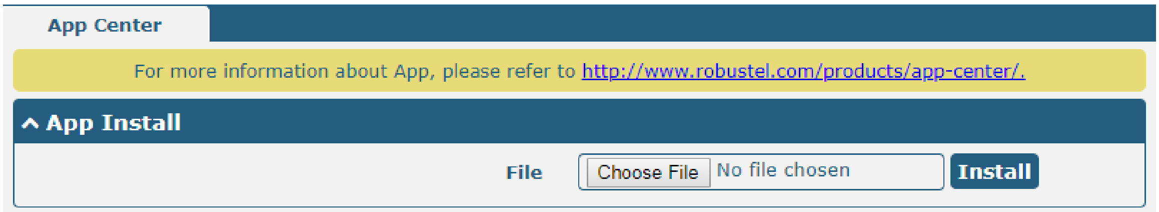
Note: To access the latest firmware file, please contact your technical support engineer.



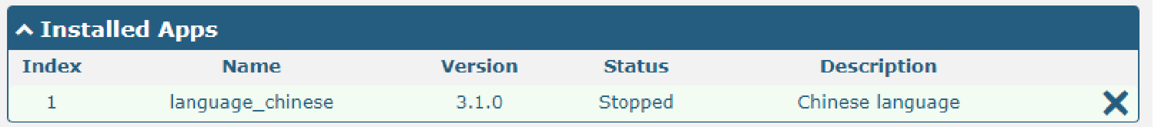
3.28 System>App Center

This section allows you to add some required or customized applications to the router. Import and install your applicationsto the App Center, andreboot the device according to the system prompts. Each installed application will be displayed under the “Services” menu, while other applications related to VPN will be displayedunder the “VPN” menu.

Note: After importing the applications to the router, the page display may have a slight delay due to the browsercache. It is recommended that you clear the browser cache first and log in the router again.


App Center
For more information about App, please refer to http://www.robustel.com/products/app-center/.
^ App Install
File
Choose File
No file chosen
Install

The successfully installed app will be displayed in the following list. Click ✕ to uninstall the app.



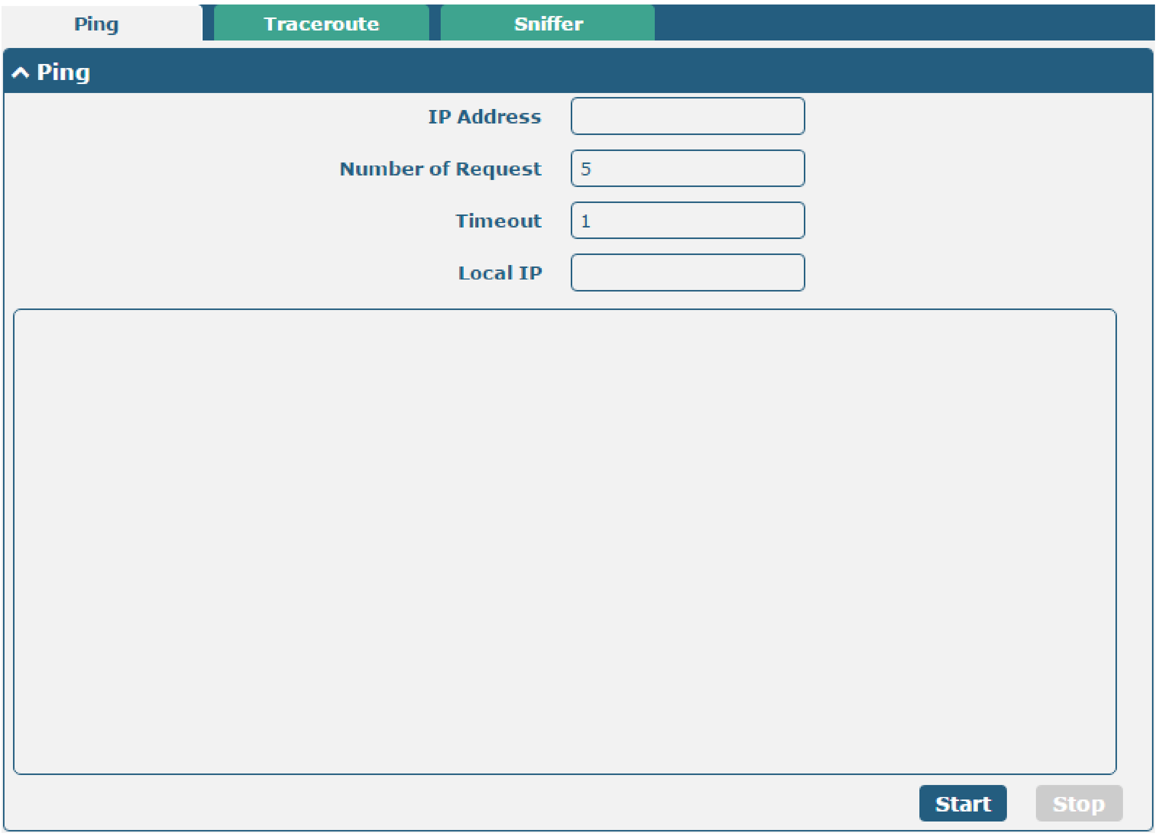
^ Installed Apps

Index	Name	Version	Status	Description	
1	language_chinese	3.1.0	Stopped	Chinese language	✕

App Center		
Item	**Description**	**Default**
App Install		
File	Click on “Choose File” to locate the App file from your computer, and then click Install to import this file into your router. **Note**: File format should be *xxx.rpk*, e.g.*R2000-robustlink-1.0.0.rpk*.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

3.29 System> Tools

This section provides users three tools: Ping, Traceroute and Sniffer.



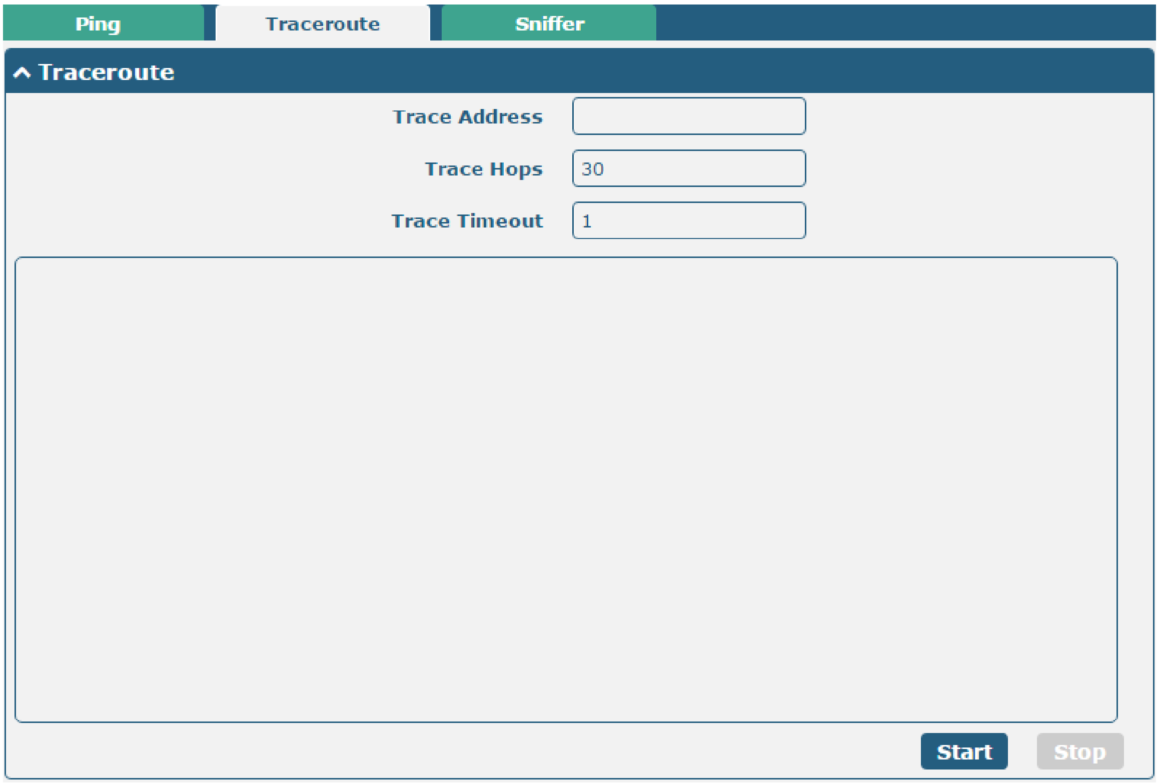
IP Address

Number of Request 5

Timeout 1

Local IP

Ping		
Item	**Description**	**Default**
IP address	Enter the ping's destination IP address or destination domain.	Null
Number of Requests	Specify the number of ping requests.	5
Timeout	Specify the timeout of ping requests.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting local IP address from these three automatically.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	--
Stop	Click this button to stop ping request.	--

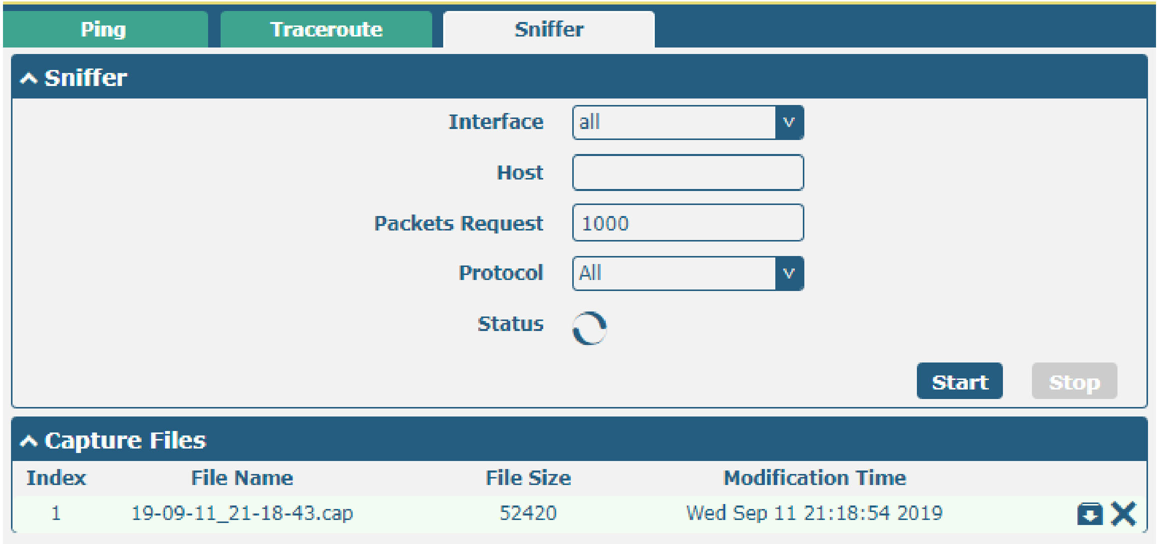


Trace Address

Trace Hops 30

Trace Timeout 1

Traceroute		
Item	**Description**	**Default**
Trace Address	Enter the trace’s destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify the timeout of Traceroute request.	1
Start	Click this button to start Traceroute request, and the log will be displayed in the follow box.	--
Stop	Click this button to stop Traceroute request.	--



Interface all

Host

Packets Request 1000

Protocol All

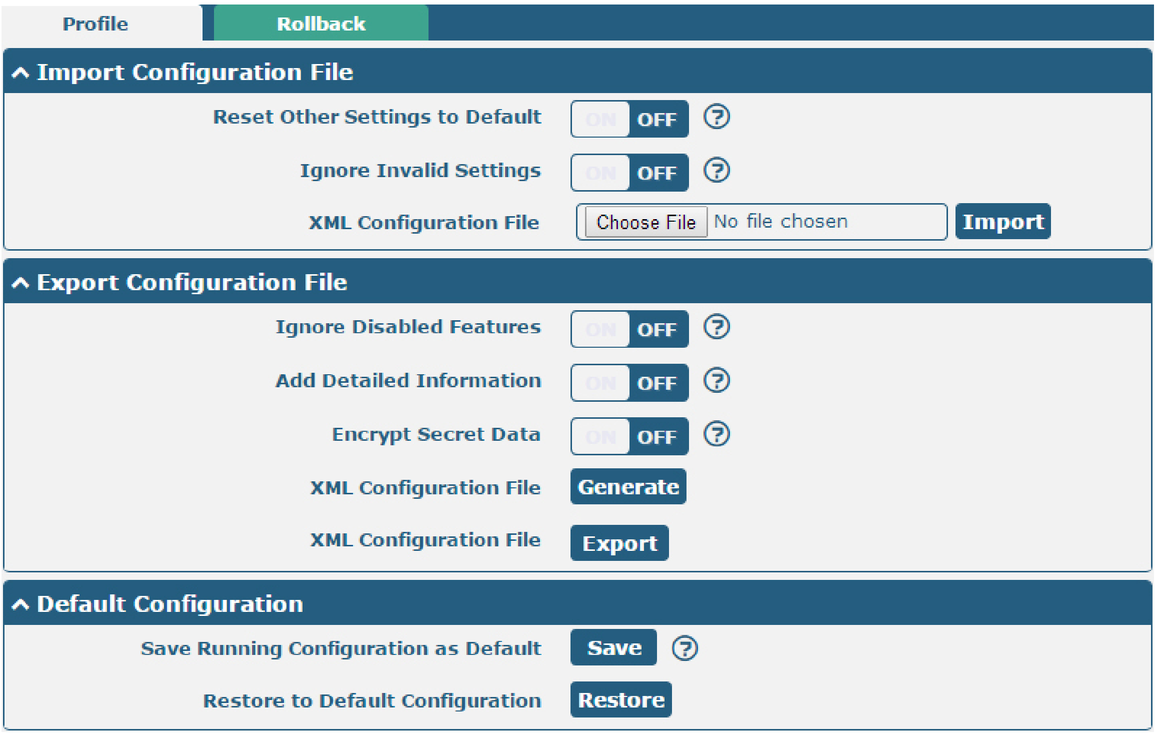
Status

Index	File Name	File Size	Modification Time
1	19-09-11_21-18-43.cap	52420	Wed Sep 11 21:18:54 2019

Sniffer		
Item	**Description**	**Default**
Interface	Choose the interface according to your Ethernet configuration.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from “All”, “IP”, “TCP”, “UDP” and “ARP”.	All
Status	Show the current status of sniffer.	--
Start	Click this button to start the sniffer.	--
Stop	Click this button to stopthe sniffer. Once you click this button, a new log file will be displayed in the following List.	--
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click ⬇ to download the log, click ✕to delete the log file. It can cache a maximum of 5 files.	--

3.30 System> Profile

This section allows you to import or export the configuration file, and restore the router to factory default setting.



^ Import Configuration File

Reset Other Settings to Default: OFF

Ignore Invalid Settings: OFF

XML Configuration File: Choose File No file chosen Import

^ Export Configuration File

Ignore Disabled Features: OFF

Add Detailed Information: OFF

Encrypt Secret Data: OFF

XML Configuration File: Generate

XML Configuration File: Export

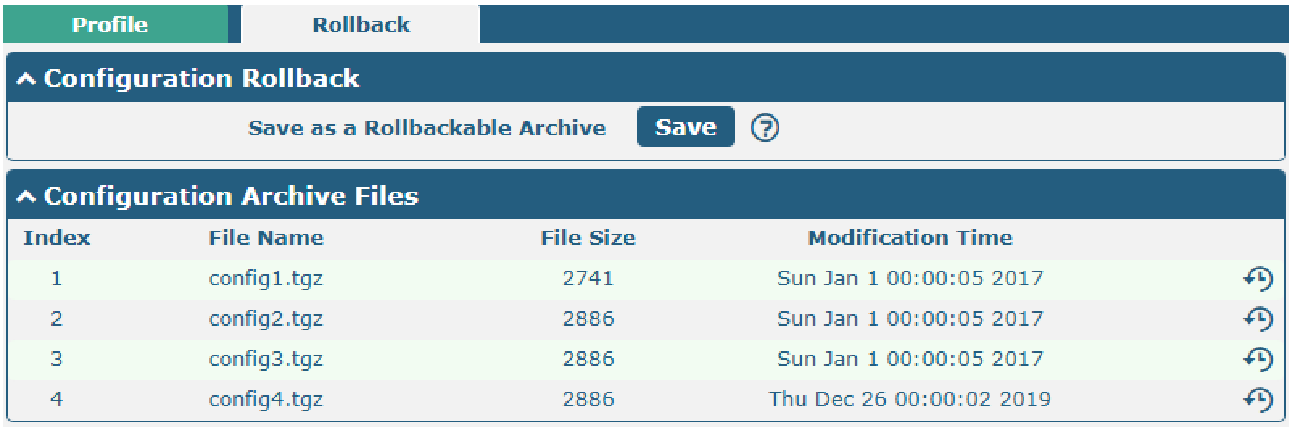
^ Default Configuration

Save Running Configuration as Default: Save

Restore to Default Configuration: Restore

Profile		
Item	**Description**	**Default**
	Import Configuration File	
Reset Other Settings to Default	Click the toggle button as “ON” to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as “OFF” to ignore invalid settings.	OFF
XML Configuration File	Click on Choose File to locate the XML configuration file from your computer, and then click Import to import this file into your router.	--

Export Configuration File		
Ignore Disabled Features	Click the toggle button as “OFF” to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as “On” to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as “ON” to encrypt the secret data.	OFF
XML Configuration File	Click Generate button to generate the XML configuration file, and click Export to export the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click Save button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click Restore button to restore the factory defaults.	--



Configuration Rollback

Save as a Rollbackable Archive Save ?

Configuration Archive Files

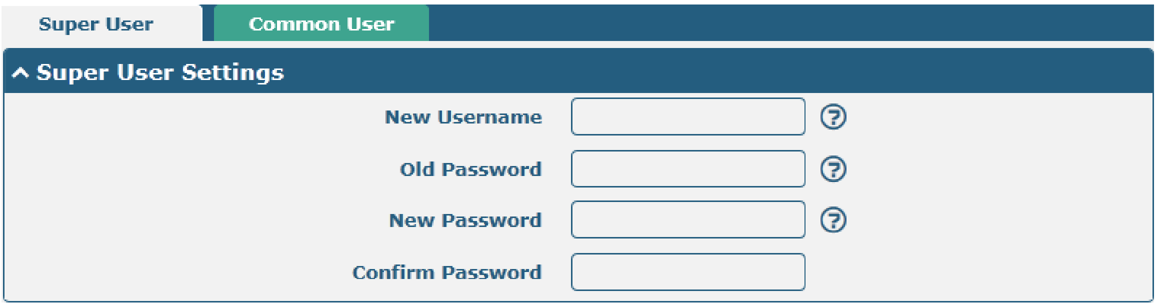
Index	File Name	File Size	Modification Time	
1	config1.tgz	2741	Sun Jan 1 00:00:05 2017	↺
2	config2.tgz	2886	Sun Jan 1 00:00:05 2017	↺
3	config3.tgz	2886	Sun Jan 1 00:00:05 2017	↺
4	config4.tgz	2886	Thu Dec 26 00:00:02 2019	↺

Rollback		
Item	**Description**	**Default**
Configuration Rollback		
Save as a Rollbackable Archive	Create a savepoint manually. Additionally, the system will create a savepoint every day automatically if configuration changes.	--
Configuration Archive Files		
Configuration Archive Files	View the related information about configuration archive files, including name, size and modification time.	--

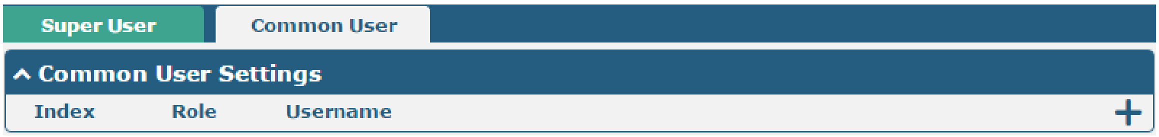
3.31 System> User Management

This section allows you to changeyour username and password, and create or manage user accounts.One router has only one super user who has the highest authority to modify, add and manage other common users.

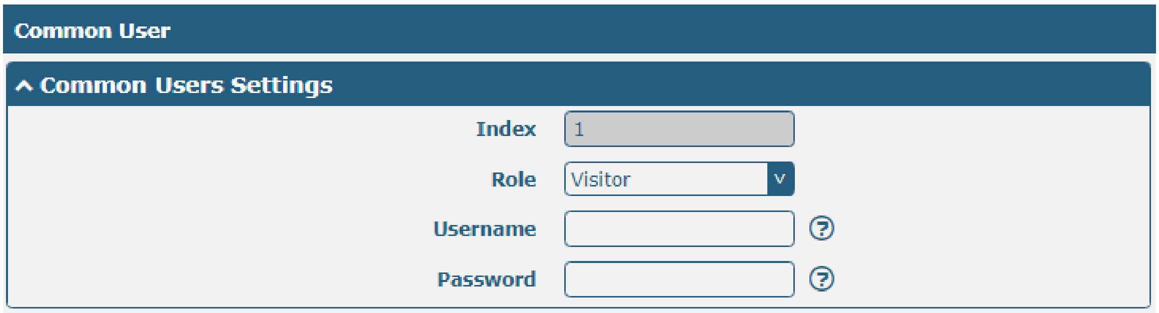
Note: Your new password must be more than 5 character and less than 32 characters and may contain numbers, upper and lowercase letters, and standard symbols.



Super User Settings		
Item	**Description**	**Default**
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Old Password	Enter the old password of your router. The default is “admin”.	Null
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Confirm Password	Enter the new password again to confirm.	Null



Click + button to add a new common user.The maximum rule count is 5.



Index 1

Role Visitor

Common User Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Role	Select from “Visitor” and “Editor”. • Visitor: Users only can view the configuration of router under this level	Visitor

	- Editor: Users can view and set the configuration of router under this level	
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null

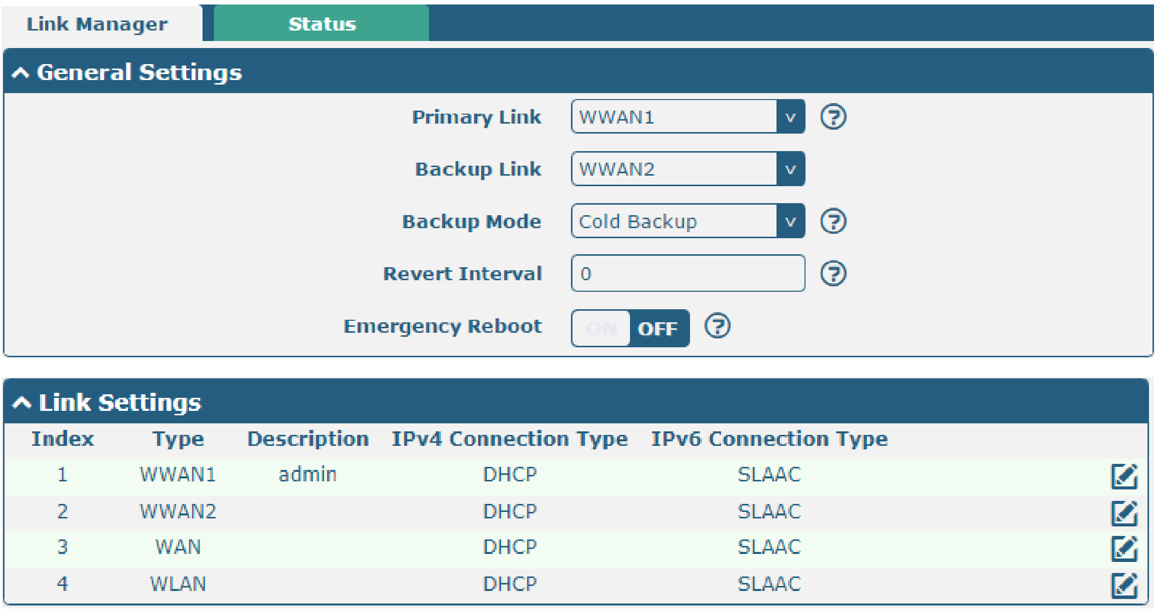
Chapter 4 Configuration Examples

4.1 Cellular

4.1.1 Cellular Dial-Up

This section shows you how to configure the primary and backup SIM cardfor Cellular Dial-up. Connect the router correctly and insert two SIM, then open the configuration page. Under the homepage menu, click **Interface > Link Manager > Link Manager > General Settings**, choose “WWAN1” as the primary link and “WWAN2” as the backup link, and set “Cold Backup” as the backup mode, then click “Submit”.

Note: All data will be transferred via WWAN1 when choose WWAN1 as the primary link and set backup mode as cold backup. At the same time, WWAN2 is always offline as a backup link. All data transmission will be switched to WWAN2 when the WWAN1 is disconnected.



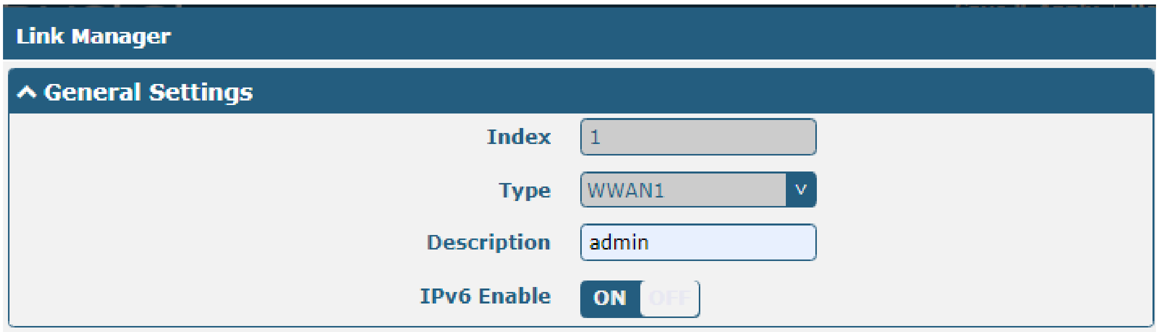
General Settings

Primary Link	WWAN1
Backup Link	WWAN2
Backup Mode	Cold Backup
Revert Interval	0
Emergency Reboot	ON OFF

Link Settings

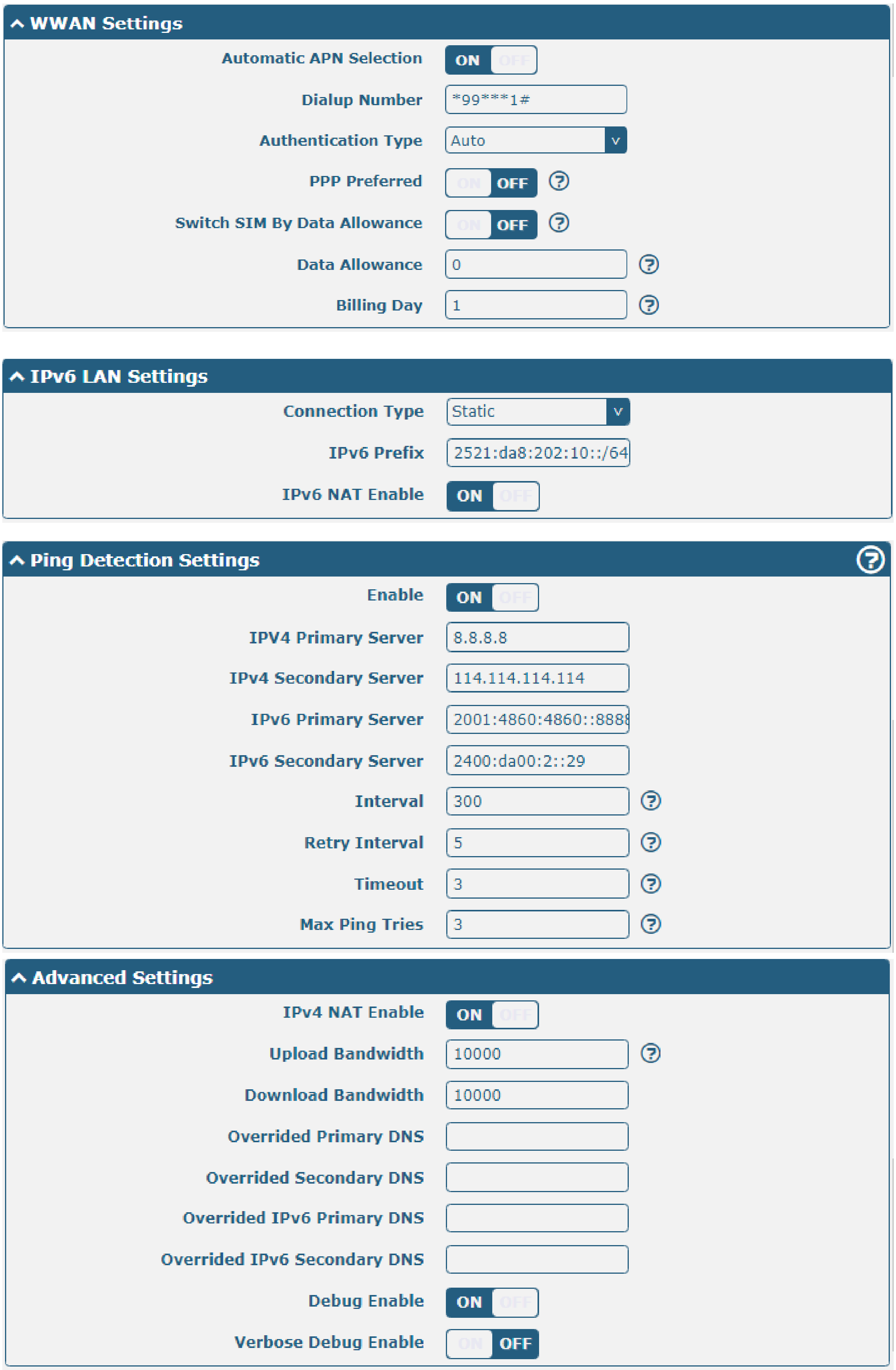
Index	Type	Description	IPv4 Connection Type	IPv6 Connection Type	
1	WWAN1	admin	DHCP	SLAAC	✎
2	WWAN2		DHCP	SLAAC	✎
3	WAN		DHCP	SLAAC	✎
4	WLAN		DHCP	SLAAC	✎

Click the ✎ button of WWAN1 to set its parameters according to the current ISP.



General Settings

Index	1
Type	WWAN1
Description	admin
IPv6 Enable	ON OFF



WWAN Settings

Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
PPP Preferred	OFF
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

IPv6 LAN Settings

Connection Type	Static
IPv6 Prefix	2521:da8:202:10::/64
IPv6 NAT Enable	ON

Ping Detection Settings

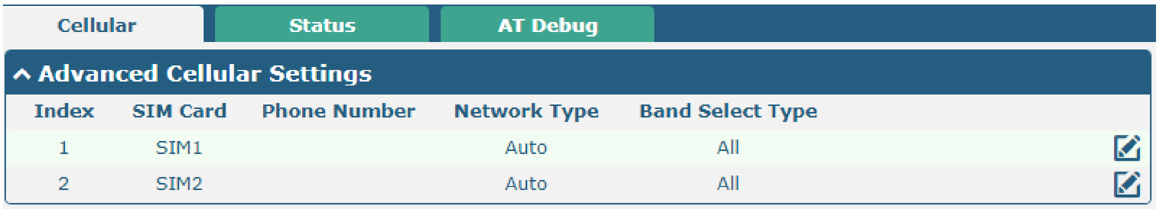
Enable	ON
IPV4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::888
IPv6 Secondary Server	2400:da00:2::29
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3

Advanced Settings

IPv4 NAT Enable	ON
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Overrided IPv6 Primary DNS	
Overrided IPv6 Secondary DNS	
Debug Enable	ON
Verbose Debug Enable	OFF

When finished, click **Submit > Save & Apply** for the configuration to take effect.

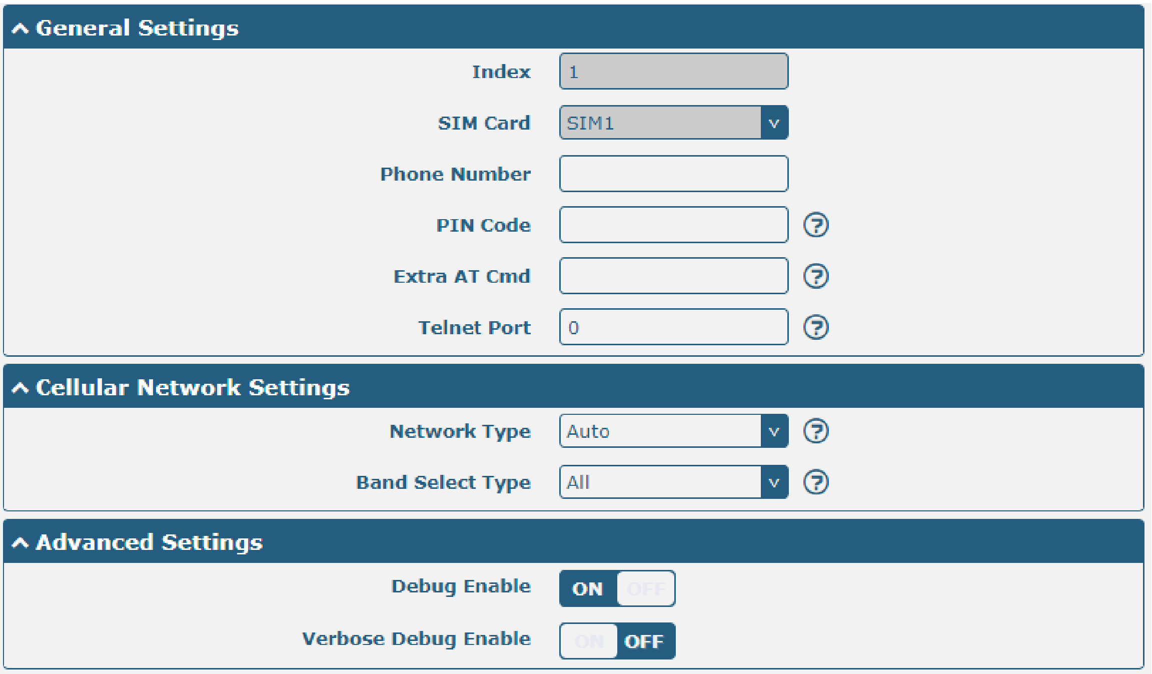
The window is displayed below by clicking **Interface > Cellular > Advanced Cellular Settings**.



^ Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type
1	SIM1		Auto	All
2	SIM2		Auto	All

Click the edit button of SIM1 to set its parameters according to your application request.



^ General Settings

Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0

^ Cellular Network Settings

Network Type	Auto
Band Select Type	All

^ Advanced Settings

Debug Enable	ON
Verbose Debug Enable	OFF

When finished, click **Submit > Save & Apply** for the configuration to take effect.

4.1.2 SMS Remote Control

R2000supports remote control via SMS. You can use following commands to get the status of the router, and set all the parameters of the router.There are three authentication types for SMS control. You can select from “Password”, “Phonenum” or “Both”.

An SMS command has the following structure:

1. Password mode—Username: **Password;cmd1;cmd2;cmd3; …cmdn** (available for every phone number).
2. Phonenum mode-- **Password; cmd1; cmd2; cmd3; … cmdn** (available when the SMS was sent from the phone number which had been added in router’s phone group).
3. Both mode-- **Username: Password;cmd1;cmd2;cmd3; …cmdn**(available when the SMS was sent from the phone number which had been added in router’s phone group).

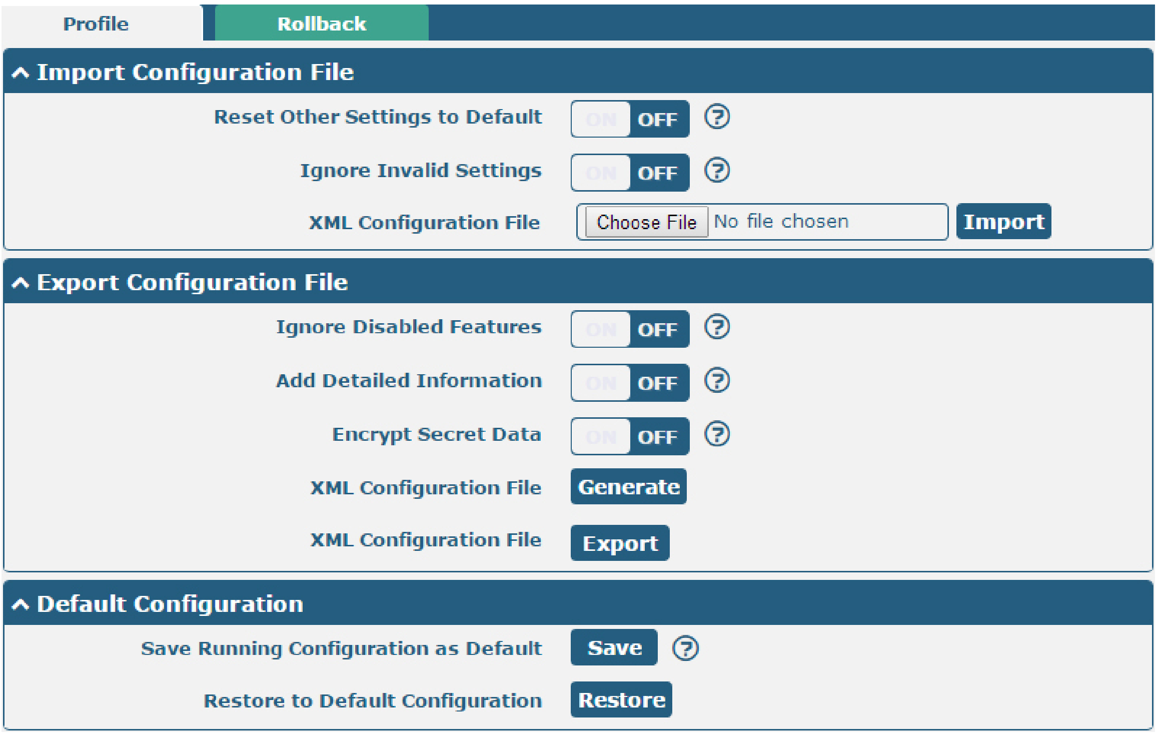
SMS command Explanation:

1. User name and Password: Use the same username and password as WEB manager for authentication.

2. **cmd1, cmd2, cmd3 to Cmdn**, the command format is the same as the CLI command, more details about CLI cmd please refer to **Chapter 5 Introductions for CLI**.

   Note: Download the configure XML file from the configured web browser. The format of SMS control command can refer to the data of the XML file.

   Go to **System > Profile > Export Configuration File**, click **Generate** to generate the XML file and click **Export** to export the XML file.



Import Configuration File

Reset Other Settings to Default: ON OFF

Ignore Invalid Settings: ON OFF

XML Configuration File: Choose File No file chosen Import

Export Configuration File

Ignore Disabled Features: ON OFF

Add Detailed Information: ON OFF

Encrypt Secret Data: ON OFF

XML Configuration File: Generate

XML Configuration File: Export

Default Configuration

Save Running Configuration as Default: Save

Restore to Default Configuration: Restore

XML command:

```
<lan >
<network max_entry_num="2" >
<id > 1</id >
<interface > lan0</interface >
<ip > 172.16.10.67</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >
```

SMS cmd:

set lan network 1 interface lan0
set lan network 1 ip 172.16.10.67
set lan network 1 netmask 255.255.0.0
set lan network 1 mtu 1500

3. The semicolon character (‘;’) is used to separate more than one commands packed in a single SMS.
4. E.g.

   admin:admin;status system

   In this command, username is “admin”, password is “admin”, and the function of the command is to get the system status.

   SMS received:

   hardware_version = 1.0

```
firmware_version = "3.0.0"
kernel_version = 3.10.49
device_model = R2000
serial_number = 111111111
system_uptime = "0 days, 06:17:32"
system_time = "Thu Jul617:28:51 2017"
```

admin:admin;reboot

In this command, username is “admin”, password is “admin”, and the command is to reboot the Router.

SMS received:

```
OK
```

admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false

In this command, username is “admin”, password is “admin”, and the command is to disable the remote_ssh and remote_telnet access.

SMS received:

```
OK
OK
```

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.99.11;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

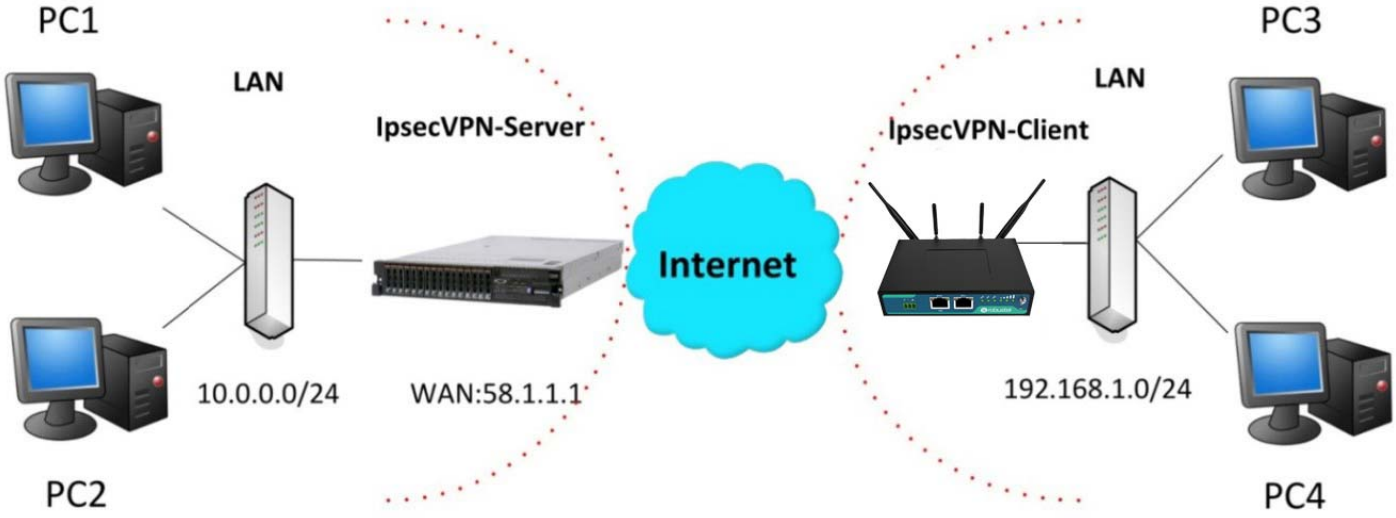
In this command, username is “admin”, password is “admin”, and the commands is to configure the LAN parameter.

SMS received:

```
OK
OK
OK
OK
```

4.2 Network

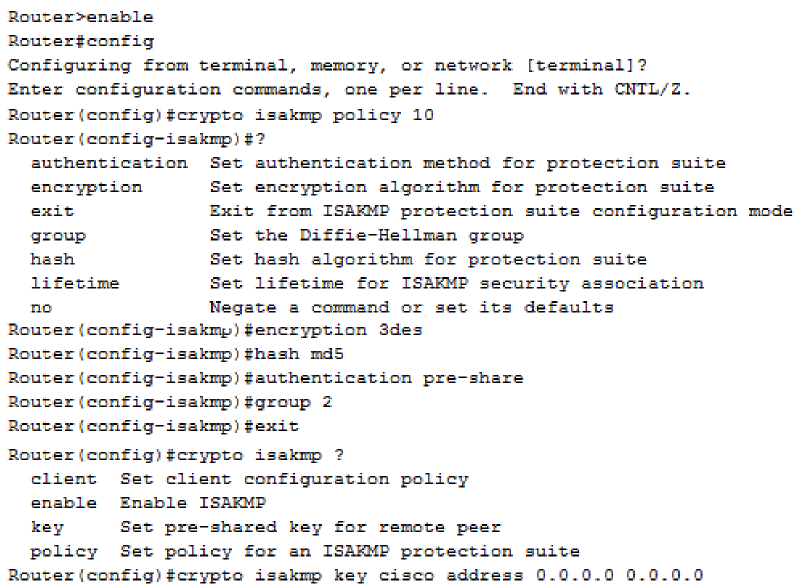
4.2.1 IPsec VPN



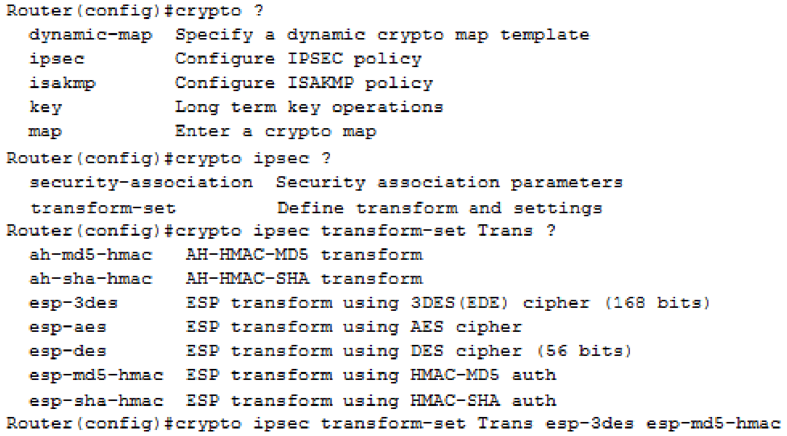
The configuration of server and client is as follows.

IPsecVPN_Server:

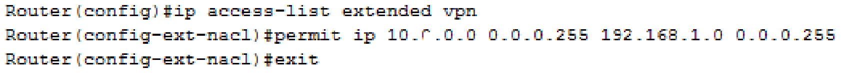
Cisco 2811:



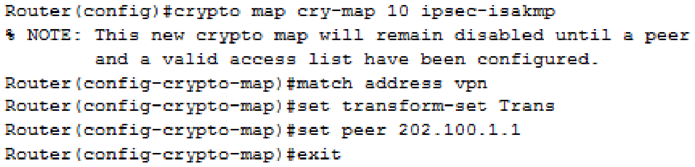
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```



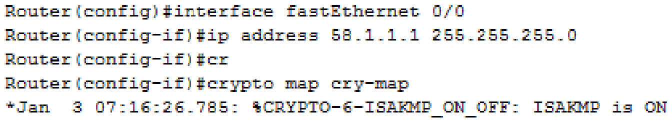
```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac
```



```
Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit
```



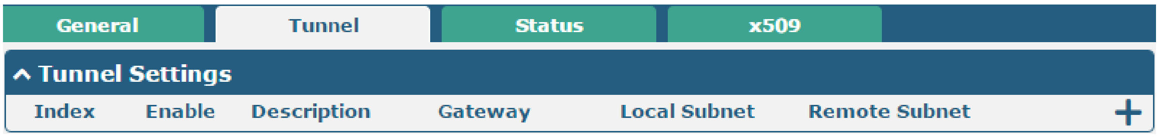
```
Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit
```



```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

IPsecVPN_Client:

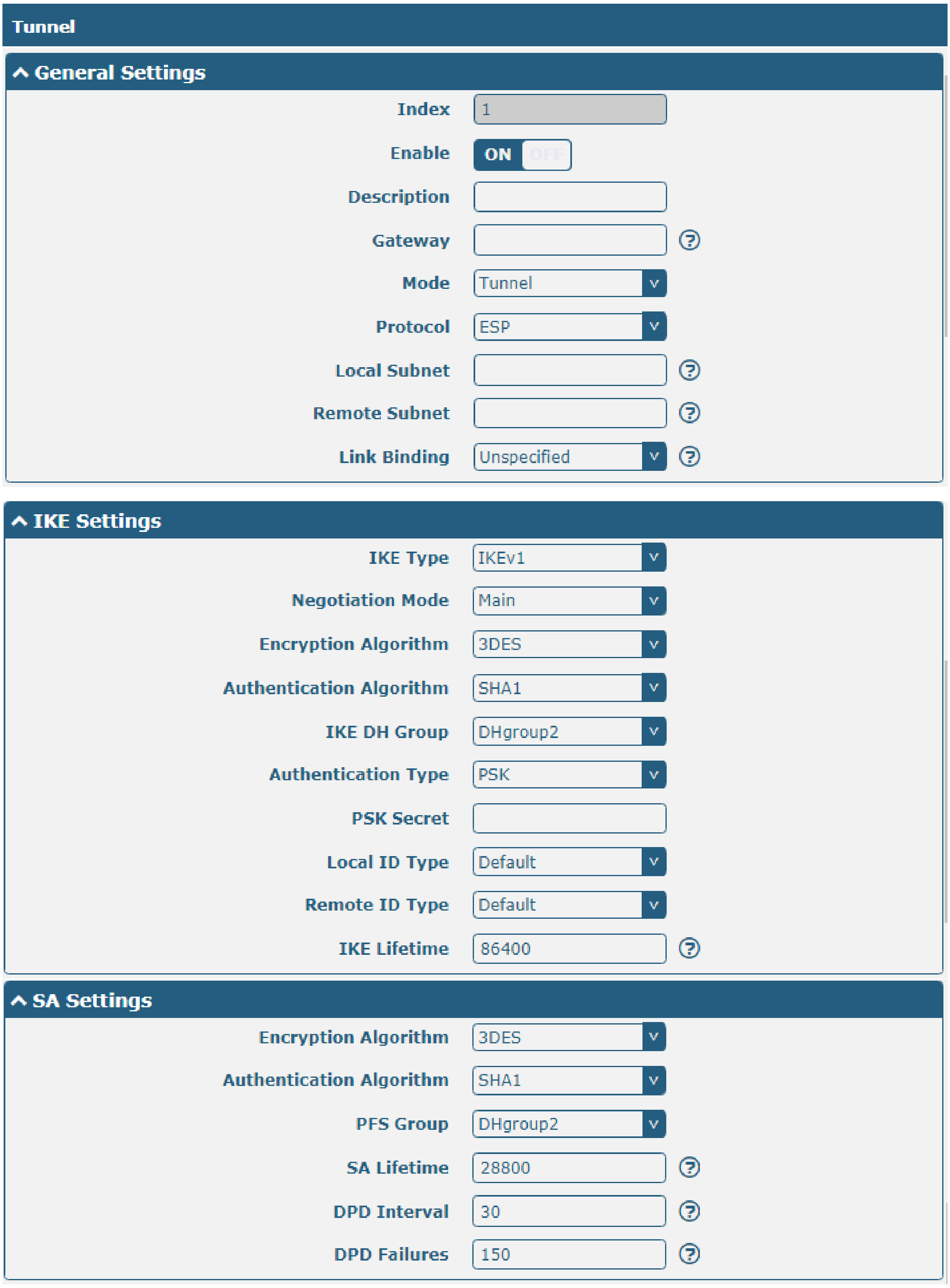
The window is displayed as below by clicking **VPN > IPsec > Tunnel**.



^ Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet

Click + buttonand set the parameters of IPsec Client as below.



^ General Settings

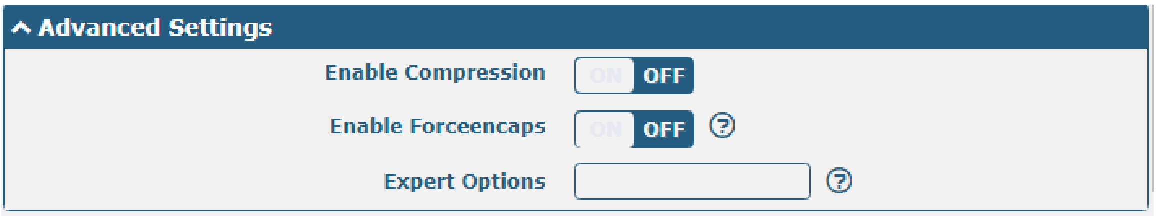
Index	1
Enable	ON OFF
Description	
Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Remote Subnet	
Link Binding	Unspecified

^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

^ SA Settings

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	30
DPD Failures	150



^ Advanced Settings

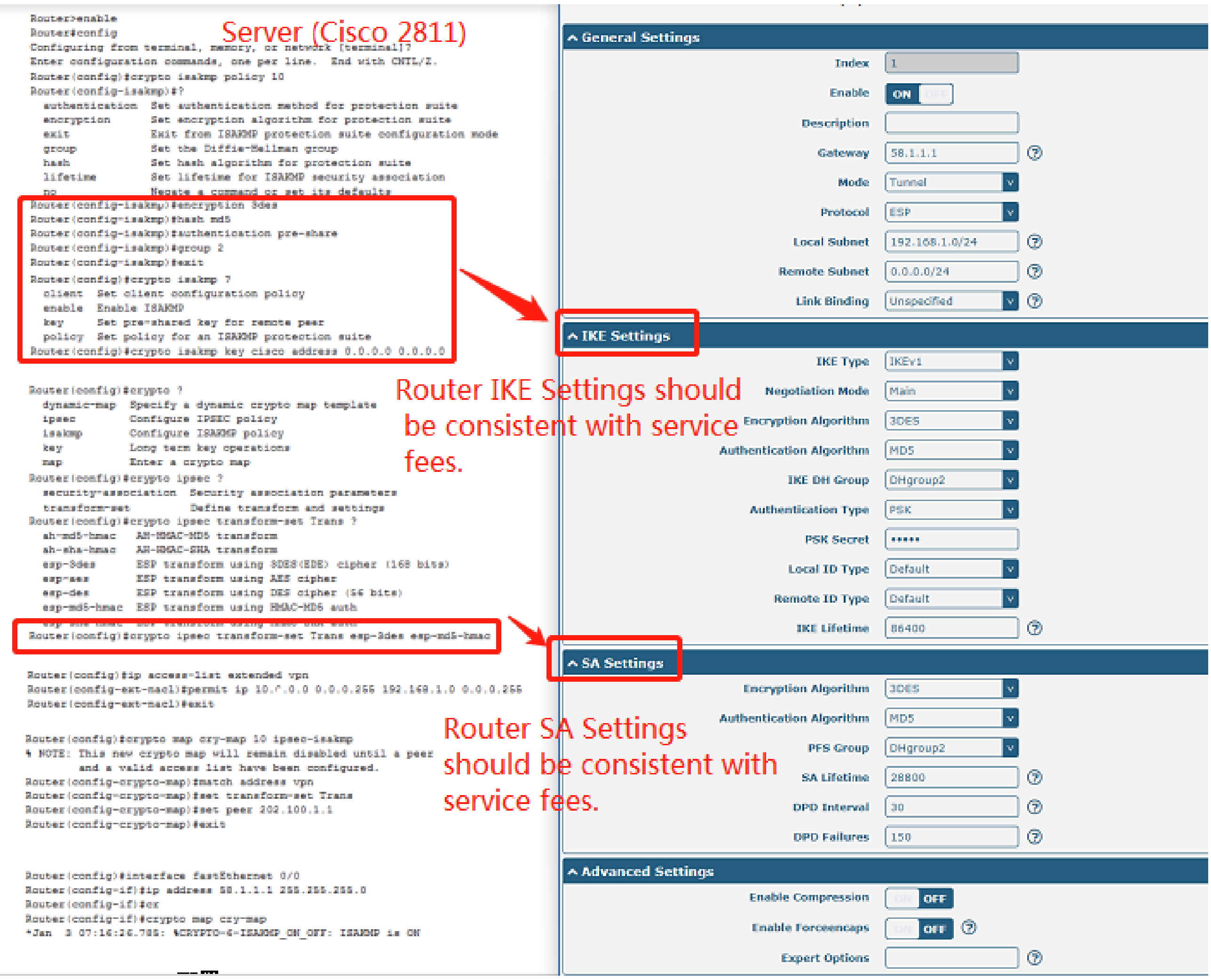
Enable Compression: ON OFF

Enable Forceencaps: ON OFF

Expert Options:

When finished, click **Submit > Save & Apply** for the configuration to take effect.

The comparison between server and client is as below.



Server (Cisco 2811)

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0

Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac

Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.*.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit

Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit


Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#ex
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Router IKE Settings should be consistent with service fees.

Router SA Settings should be consistent with service fees.

^ General Settings

Index: 1

Enable: ON OFF

Description:

Gateway: 58.1.1.1

Mode: Tunnel

Protocol: ESP

Local Subnet: 192.168.1.0/24

Remote Subnet: 0.0.0.0/24

Link Binding: Unspecified

^ IKE Settings

IKE Type: IKEv1

Negotiation Mode: Main

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

IKE DH Group: DHgroup2

Authentication Type: PSK

PSK Secret: •••••

Local ID Type: Default

Remote ID Type: Default

IKE Lifetime: 86400

^ SA Settings

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

PFS Group: DHgroup2

SA Lifetime: 28800

DPD Interval: 30

DPD Failures: 150

^ Advanced Settings

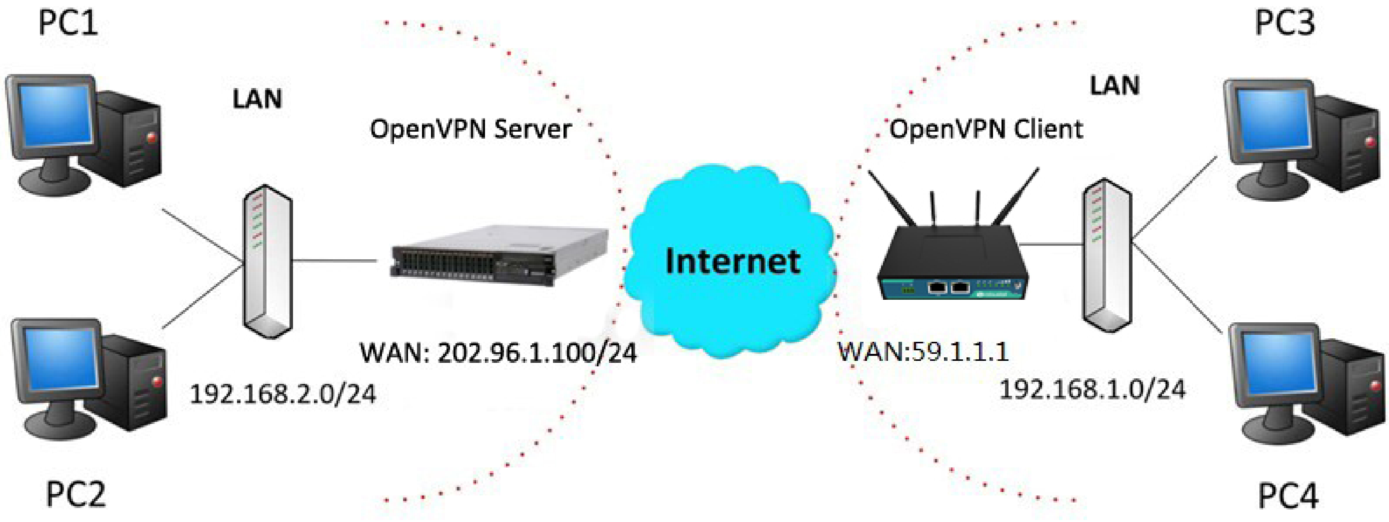
Enable Compression: ON OFF

Enable Forceencaps: ON OFF

Expert Options:

4.2.2 OpenVPN

OpenVPN supports two modes, including Client and P2P. Here takes Client as an example.



OpenVPN_Server:

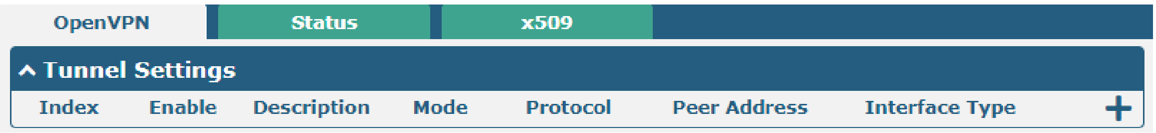
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

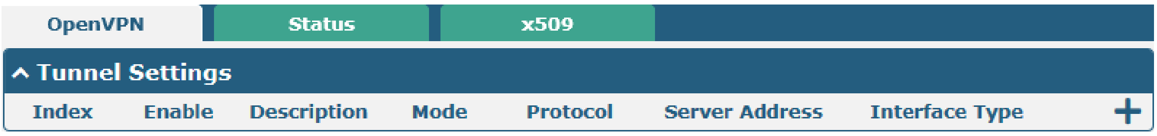
Note: For more configuration details, please contact your technical support engineer.

OpenVPN_Client:

Click **VPN > OpenVPN > OpenVPN** as below.

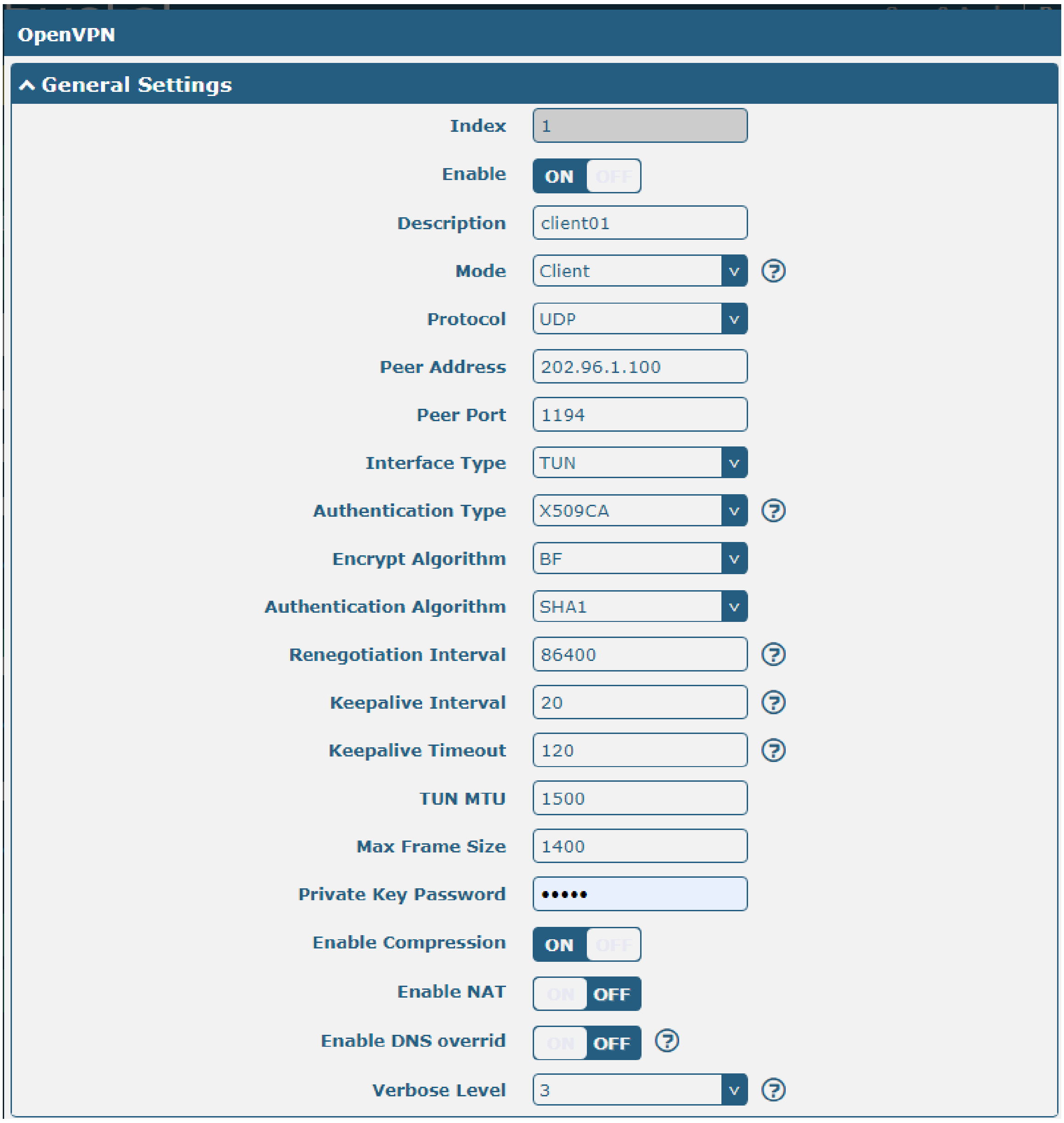


Index	Enable	Description	Mode	Protocol	Peer Address	Interface Type

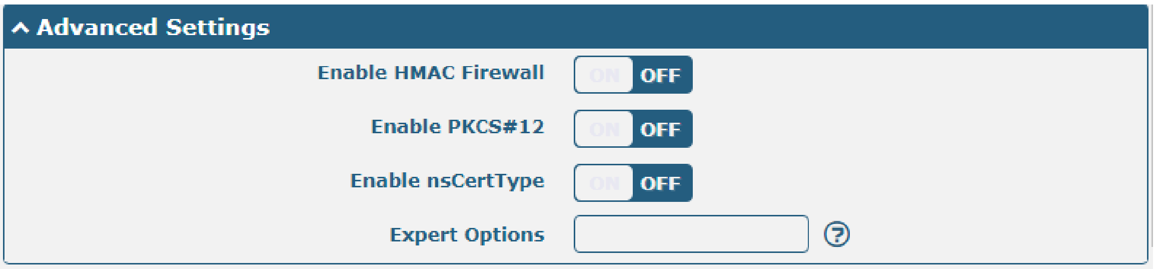


Index	Enable	Description	Mode	Protocol	Server Address	Interface Type

Click + to configure the Client01 as below.



Index	1
Enable	ON
Description	client01
Mode	Client
Protocol	UDP
Peer Address	202.96.1.100
Peer Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	1400
Private Key Password	•••••
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	3

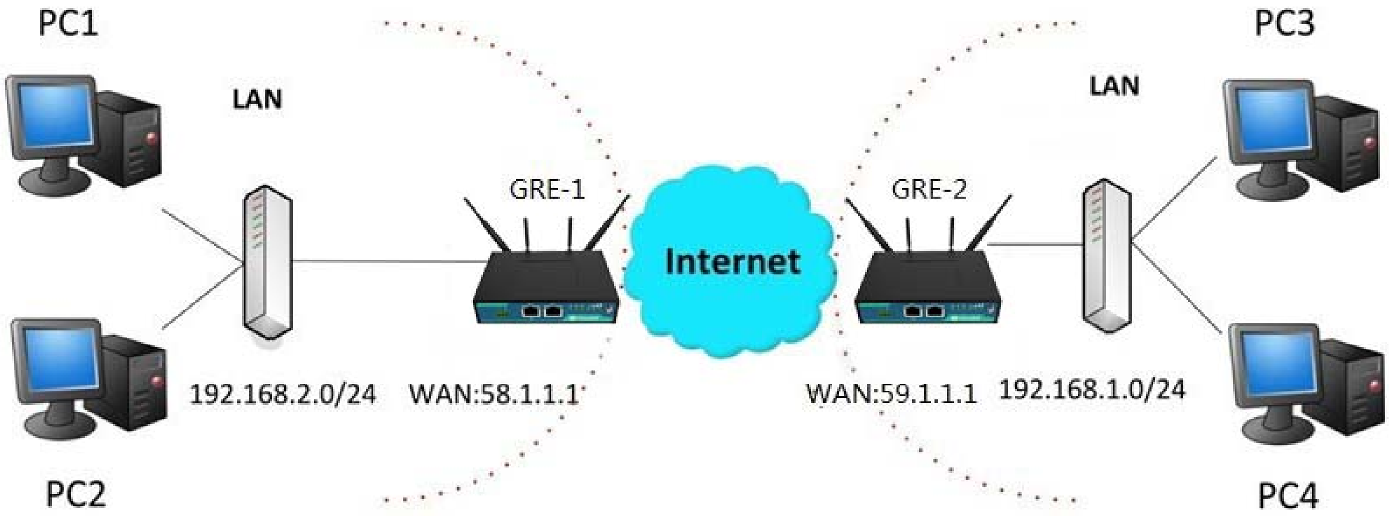


^ Advanced Settings

Enable HMAC Firewall	ON OFF
Enable PKCS#12	ON OFF
Enable nsCertType	ON OFF
Expert Options	?

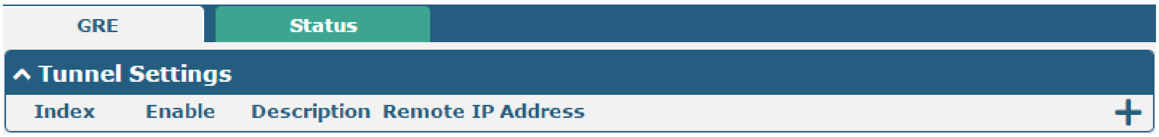
When finished, click **Submit > Save & Apply** for the configuration to take effect.

4.2.3 GRE VPN



The configuration of two points is as follows.

The window is displayed as below by clicking **VPN > GRE > GRE**.



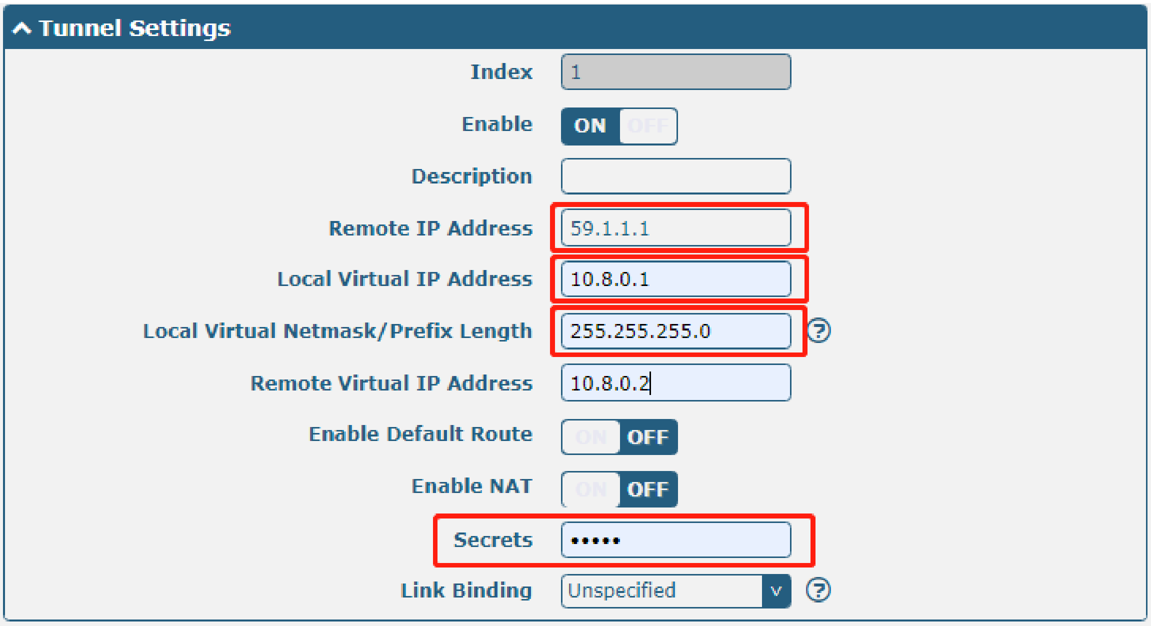
GRE | Status

^ Tunnel Settings

Index	Enable	Description	Remote IP Address	+

GRE-1：

Click + buttonand set the parameters of GRE-1 as below.



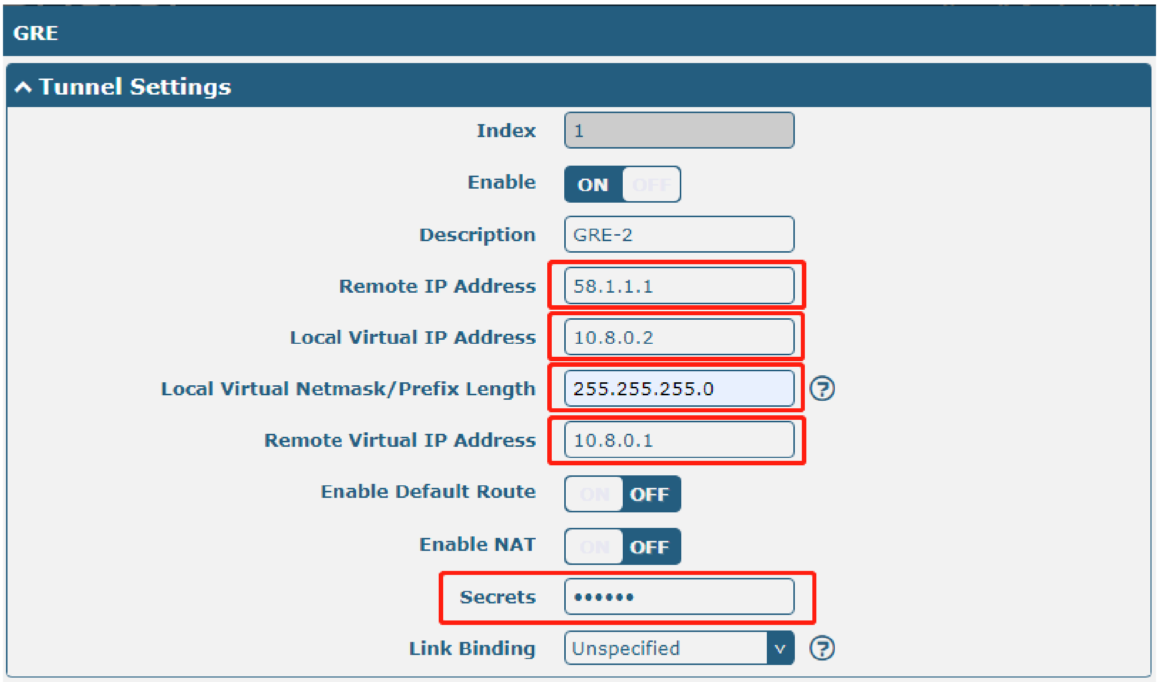
Tunnel Settings

Index	1
Enable	ON
Description	
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.1
Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.2
Enable Default Route	OFF
Enable NAT	OFF
Secrets	•••••
Link Binding	Unspecified

When finished, click **Submit > Save & Apply** for the configuration to take effect.

GRE-2:

Click ➕ buttonand set the parameters of GRE-1 as below.



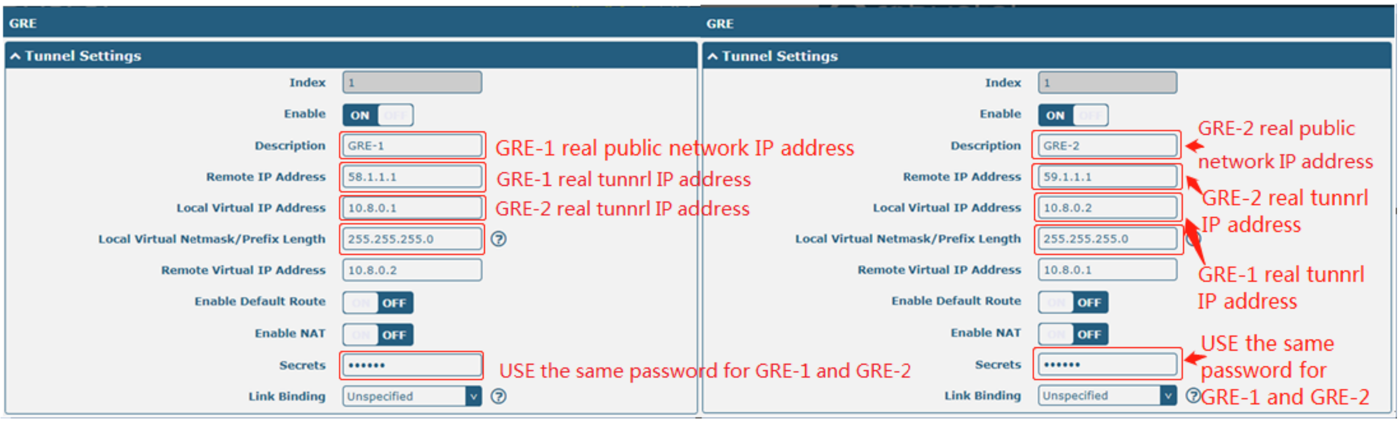
GRE

Tunnel Settings

Index	1
Enable	ON
Description	GRE-2
Remote IP Address	58.1.1.1
Local Virtual IP Address	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.1
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••
Link Binding	Unspecified

When finished, click **Submit > Save & Apply** for the configuration to take effect.

The comparison between GRE-1 and GRE-2 is as below.



GRE

Tunnel Settings

Index: 1

Enable: ON

Description: GRE-1

Remote IP Address: 58.1.1.1

Local Virtual IP Address: 10.8.0.1

Local Virtual Netmask/Prefix Length: 255.255.255.0

Remote Virtual IP Address: 10.8.0.2

Enable Default Route: OFF

Enable NAT: OFF

Secrets: ••••••

Link Binding: Unspecified

GRE-1 real public network IP address

GRE-1 real tunnrl IP address

GRE-2 real tunnrl IP address

USE the same password for GRE-1 and GRE-2

GRE

Tunnel Settings

Index: 1

Enable: ON

Description: GRE-2

Remote IP Address: 59.1.1.1

Local Virtual IP Address: 10.8.0.2

Local Virtual Netmask/Prefix Length: 255.255.255.0

Remote Virtual IP Address: 10.8.0.1

Enable Default Route: OFF

Enable NAT: OFF

Secrets: ••••••

Link Binding: Unspecified

GRE-2 real public network IP address

GRE-2 real tunnrl IP address

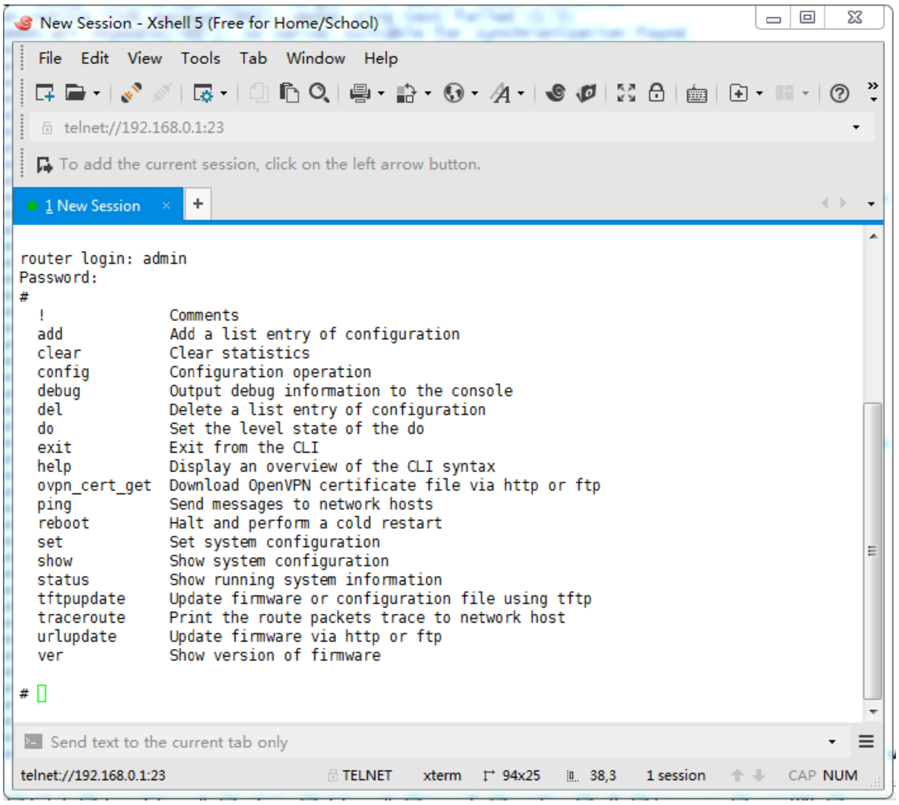
GRE-1 real tunnrl IP address

USE the same password for GRE-1 and GRE-2

Chapter 5 Introductions for CLI

5.1 What Is CLI

Command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the SSH or through a telnet network connection.


New Session - Xshell 5 (Free for Home/School)
File Edit View Tools Tab Window Help
telnet://192.168.0.1:23
To add the current session, click on the left arrow button.
1 New Session
Send text to the current tab only
telnet://192.168.0.1:23 TELNET xterm 94x25 38,3 1 session CAP NUM

```
router login: admin
Password:
#
  !             Comments
  add           Add a list entry of configuration
  clear         Clear statistics
  config        Configuration operation
  debug         Output debug information to the console
  del           Delete a list entry of configuration
  do            Set the level state of the do
  exit          Exit from the CLI
  help          Display an overview of the CLI syntax
  ovpn_cert_get Download OpenVPN certificate file via http or ftp
  ping          Send messages to network hosts
  reboot        Halt and perform a cold restart
  set           Set system configuration
  show          Show system configuration
  status        Show running system information
  tftpupdate    Update firmware or configuration file using tftp
  traceroute    Print the route packets trace to network host
  urlupdate     Update firmware via http or ftp
  ver           Show version of firmware

#
```

Route login:

Router login: admin

Password: admin

#

CLI commands:

#? (**Note**: the '?' won't display on the page.)

!	Comments
add	Add a list entry of configuration
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
exit	Exit from the CLI

help	Display an overview of the CLI syntax
ovpn_cert_get	Download OpenVPN certificate file via http or ftp
ping	Send messages to network hosts
reboot	Halt and perform a cold restart
route	Static route modify dynamically, this setting will not be saved
set	Set system configuration
show	Show system configuration
status	Show running system information
tftpupdate	Update firmware using tftp
traceroute	Print the route packets trace to network host
urlupdate	Update firmware using http or ftp
ver	Show version of firmware

5.2 How to Configure the CLI

Following is a table about the description of help and the error should be encountered in the configuring program.

Commands /tips	Description
?	Typing a question mark "?" will show you the help information. eg. # config（Press '?'） config Configuration operation # config（Press spacebar +'?'） commit Save the configuration changes and take effect changed configuration save_and_apply Save the configuration changes and take effect changed configuration loaddefault Restore Factory Configuration
Ctrl+c	Press these two keys at the same time, except its "copy" function but also can be used for "break" out of the setting program.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	It can help you finish you command. Example: # config (tick enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault
#config commit	When your setting finished, you should enter those commands to make

# config save_and_apply	your setting take effect on the device. **Note:**Commit and save_and_apply plays the same role.

5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug *parameters*	Turn on or turn off debug function
Show	Show *parameters*	Show current configuration of each function , if we need to see all please using "show running "
Set	Set *parameters*	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add *parameters*	

Note: Download the config.XML file from the configured web browser. The command format can refer to the config.XML file format.

5.4 Quick Start with Configuration Examples

The best and quickest way to master CLI is firstly to view all features from the webpage and then read all CLI commands at a time,finally learn to configure it with some reference examples.

Example 1: Show current version

```
# status system
hardware_version = 1.0
firmware_version = "3.0.0"
kernel_version = 3.10.49
device_model = R2000
serial_number = 111111111
system_uptime = "0 days, 06:17:32"
system_time = "Thu Jul 6 17:28:51 2017"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
  firmware    New firmware
# tftpupdate firmware (space+?)
  String    Firmware name
# tftpupdate firmwarefilename R2000-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new firmware name
Downloading
R2000-firmware-s 100% |*******************************|    5018k    0:00:00 ETA
```

```
Flashing
Checking 100%
Decrypting 100%
Flashing 100%
Verifying 100%
Verfify Success
upgrade success                          //update success
# config save_and_apply
OK                       // save and apply current configuration, make you configuration effect
```

Example 3: Set link-manager

```
# set
# set
  at_over_telnet         AT Over Telnet
  cellular               Cellular
  ddns                   Dynamic DNS
  ethernet               Ethernet
  event                  Event Management
  firewall               Firewall
  gre                    GRE
  ipsec                  IPsec
  lan                    Local Area Network
  link_manager           Link Manager
  ntp                    NTP
  openvpn                OpenVPN
  reboot                 Automatic Reboot
RobustLink               RobustLink
  route                  Route
  sms                    SMS
  snmp                   SNMP agent
  ssh                    SSH
  syslog                 Syslog
  system                 System
  user_management        User Management
  vrrp                   VRRP
  web_server             Web Server
# set link_manager
  primary_link           Primary Link
  backup_link            Backup Link
  backup_mode            Backup Mode
  emergency_reboot       Emergency Reboot
  link                   Link Settings
# set link_manager primary_link (space+?)
Enum    Primary Link (wwan1/wwan2/wan)
# set link_manager primary_link wwan1 //select “wwan1” as primary_link
```

```
OK                                                          //setting succeed
# set link_manager link 1
   type                  Type
   desc                  Description
   connection_type       Connection Type
   wwan                  WWAN Settings
   static_addr           Static Address Settings
   pppoe                 PPPoE Settings
   ping                  Ping Settings
   mtu                   MTU
   dns1_overrided        Overrided Primary DNS
   dns2_overrided        Overrided Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
   auto_apn                      Automatic APN Selection
   apn                           APN
   username                      Username
   password                      Password
   dialup_number                 Dialup Number
   auth_type                     Authentication Type
   aggressive_reset              Aggressive Reset
   switch_by_data_allowance      Switch SIM By Data Allowance
   data_allowance                Data Allowance
   billing_day                   Billing Day
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100            //open cellular switch_by_data_traffic
OK                                                           //setting succeed
# set link_manager link 1 wwan billing_day 1                 //settingspecifies the day of month for billing
OK                                                           // setting succeed
…
# config save_and_apply
OK                                   // save and apply current configuration, make you configuration effect
```

Example 4: Set Ethernet

```
# set Ethernet port_setting 2 port_assignmEnt lan0           //Set Table 2 (eth1) to lan0
OK
# config save_and_apply                                      //setting succeed
OK
```

Example 5: Set LAN IP address

```
# show lan all
network {
        id = 1
        interface = lan0
        ip = 192.168.0.1
        netmask = 255.255.255.0
        mtu = 1500
        dhcp {
                enable = true
                mode = server
                relay_server = ""
                pool_start = 192.168.0.2
                pool_end = 192.168.0.100
                netmask = 255.255.255.0
                gateway = ""
                primary_dns = ""
                secondary_dns = ""
                wins_server = ""
                lease_time = 120
                expert_options = ""
                debug_enable = false
        }
}
multi_ip {
        id = 1
        interface = lan0
        ip = 172.16.10.67
        netmask = 255.255.0.0
}
#
# set lan
    network         Network Settings
    multi_ip        Multiple IP Address Settings
    vlan            VLAN
# set lan network 1(space+?)
    interface       Interface
    ip              IP Address
    netmask         Netmask
    mtu             MTU
    dhcp            DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.10.67                  //set IP address for lan
OK                                                   //setting succeed
```

Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
CE	Conformité Europóene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EDGE	Enhanced Data rates for Global Evolution of GSM and IS-136
EMC	Electromagnetic Compatibility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
EVDO	Evolution-Data Optimized
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
kbps	kbits per second
L2TP	Layer 2 Tunneling Protocol

Abbr.	Description
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio

Abbr.	Description
WAN	Wide Area Network

Guangzhou Robustel LTD

Add:	3rd Floor, Building F, Kehui Park, No.95 Daguan Road, Guangzhou, China 510660
Tel:	86-20-29019902
Email:	info@robustel.com
Web:	www.robustel.com