

Custom Iptables Rule		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this rule.	Null
Rule	Specify one iptables rule. e.g -I INPUT -s 192.168.0.2 -j ACCEPT	Null

DMZ

Filtering
Port Mapping
Custom Rules
DMZ
Status

^ DMZ Settings

Enable DMZ ON OFF

Host IP Address

Source IP Address ?

DMZ Settings		
Item	Description	Default
Enable DMZ	Click the toggle button to enable/disable DMZ. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	OFF
Host IP Address	Enter the IP address of the DMZ host on your internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. Null means for any addresses.	Null

Status

Click the "Status" column to view the

Filtering
Port Mapping
Custom Rules
DMZ
Status

^ Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	all	wwan	*	0.0.0.0/0	!10.244.165.242
2	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
4	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
5	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	50	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0

^ Chain Forward

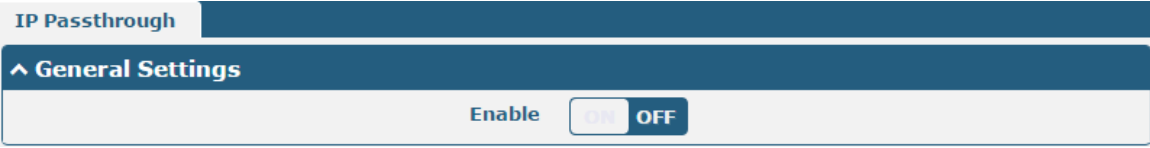
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0

^ Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination
-------	---------	--------	----------	----	-----	--------	-------------

3.16 Network > IP Passthrough

Click **Network > IP Passthrough > IP Passthrough** to enable or disable the IP Pass-through option.

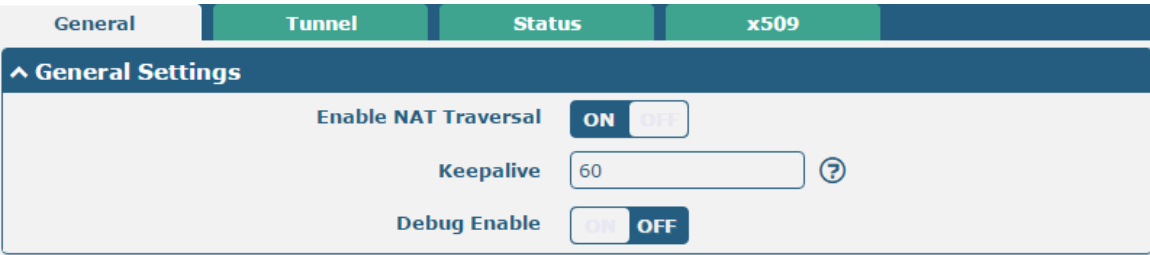


If gateway enables the IP Pass-through, the terminal device (such as PC) will enable the DHCP Client mode and connect to LAN port of the gateway; and after the gateway dial up successfully, the PC will automatically obtain the IP address and DNS server address which assigned by ISP.

3.17 VPN > IPsec

This section allows you to set the IPsec and the related parameters. Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.

General



General Settings @ General		
Item	Description	Default
Enable NAT Traversal	Click the toggle button to enable/disable the NAT Traversal function. This option must be enabled when gateway under NAT environment.	ON
Keepalive	Set the keepalive time, measured in seconds. The gateway will send packets to NAT server every keepalive time to avoid record remove from the NAT list.	60
Debug Enable	Click the toggle button to enable/disable this option. Enable for IPsec VPN information output to the debug port.	OFF

Tunnel

General	Tunnel	Status	x509			
^ Tunnel Settings						
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

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

Tunnel

^ General Settings

Index

Enable ON OFF

Description

Gateway ?

Mode v

Protocol v

Local Subnet ?

Remote Subnet ?

General Settings @ Tunnel		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter the address of remote IPsec VPN server. 0.0.0.0 represents for any address.	Null
Mode	Select from "Tunnel" and "Transport". <ul style="list-style-type: none"> Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a gateway, in which the gateway is the actual destination 	Tunnel
Protocol	Select the security protocols from "ESP" and "AH". <ul style="list-style-type: none"> ESP: Use the ESP protocol AH: Use the AH protocol 	ESP
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null

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

^ IKE Settings

IKE Type	<input type="text" value="IKEv1"/>	<input type="button" value="v"/>
Negotiation Mode	<input type="text" value="Main"/>	<input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="MD5"/>	<input type="button" value="v"/>
Encryption Algorithm	<input type="text" value="3DES"/>	<input type="button" value="v"/>
IKE DH Group	<input type="text" value="DHgroup2"/>	<input type="button" value="v"/>
Authentication Type	<input type="text" value="PSK"/>	<input type="button" value="v"/>
PSK Secret	<input type="text"/>	
Local ID Type	<input type="text" value="Default"/>	<input type="button" value="v"/>
Remote ID Type	<input type="text" value="Default"/>	<input type="button" value="v"/>
IKE Lifetime	<input type="text" value="86400"/>	<input style="float: right;" type="button" value="?"/>

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

^ IKE Settings

IKE Type	<input type="text" value="IKEv1"/>	<input type="button" value="v"/>
Negotiation Mode	<input type="text" value="Main"/>	<input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="MD5"/>	<input type="button" value="v"/>
Encryption Algorithm	<input type="text" value="3DES"/>	<input type="button" value="v"/>
IKE DH Group	<input type="text" value="DHgroup2"/>	<input type="button" value="v"/>
Authentication Type	<input type="text" value="CA"/>	<input type="button" value="v"/>
Private Key Password	<input type="text"/>	
IKE Lifetime	<input type="text" value="86400"/>	<input style="float: right;" type="button" value="?"/>

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

^ IKE Settings

IKE Type	<input type="text" value="IKEv1"/>	<input type="button" value="v"/>
Negotiation Mode	<input type="text" value="Main"/>	<input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="MD5"/>	<input type="button" value="v"/>
Encryption Algorithm	<input type="text" value="3DES"/>	<input type="button" value="v"/>
IKE DH Group	<input type="text" value="DHgroup2"/>	<input type="button" value="v"/>
Authentication Type	<input type="text" value="xAuth PSK"/>	<input type="button" value="v"/>
PSK Secret	<input type="text"/>	
Local ID Type	<input type="text" value="Default"/>	<input type="button" value="v"/>
Remote ID Type	<input type="text" value="Default"/>	<input type="button" value="v"/>
Username	<input type="text"/>	<input style="float: right;" type="button" value="?"/>
Password	<input type="text"/>	<input style="float: right;" type="button" value="?"/>
IKE Lifetime	<input type="text" value="86400"/>	<input style="float: right;" type="button" value="?"/>

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

^ IKE Settings

IKE Type: IKEv1

Negotiation Mode: Main

Authentication Algorithm: MD5

Encryption Algorithm: 3DES

IKE DH Group: DHgroup2

Authentication Type: xAuth CA

Private Key Password:

Username: ?

Password: ?

IKE Lifetime: 86400 ?

IKE Settings		
Item	Description	Default
IKE Type	Select from “IKEv1” or “IKEv2” as IKE version.	IKEv1
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in IKE negotiation.	MD5
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256” to be used in IKE negotiation. <ul style="list-style-type: none"> 3DES: Use 168-bit 3DES encryption algorithm in CBC mode AES128: Use 128-bit AES encryption algorithm in CBC mode AES256: Use 256-bit AES encryption algorithm in CBC mode 	3DES
IKE DH Group	Select from “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from “PSK”, “CA”, “xAuth PSK” and “xAuth CA” to be used in IKE negotiation. <ul style="list-style-type: none"> PSK: Pre-shared Key CA: x509 Certificate Authority xAuth: Extended Authentication to AAA server 	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from “Default”, “FQDN” and “User FQDN” for IKE negotiation. <ul style="list-style-type: none"> Default: Use an IP address as the ID in IKE negotiation FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign “@” for the local 	Default

IKE Settings		
Item	Description	Default
	security gateway, e.g., test@robustel.com	
Remote ID Type	Select from “Default”, “FQDN” and “User FQDN” for IKE negotiation. <ul style="list-style-type: none"> Default: Use an IP address as the ID in IKE negotiation FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign “@” for the local security gateway, e.g., test@robustel.com 	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key under the “CA” and “xAuth CA” authentication types.	Null
Username	Enter the username used for the “xAuth PSK” and “xAuth CA” authentication types.	Null
Password	Enter the password used for the “xAuth PSK” and “xAuth CA” authentication types.	Null

If click **VPN > IPsec > Tunnel > General Settings**, and choose **ESP** as protocol. The specific parameter configuration is shown as below.

^ General Settings

Index

Enable ON OFF

Description

Gateway ?

Mode v

Protocol v

Local Subnet ?

Remote Subnet ?

v IKE Settings

^ SA Settings

Encryption Algorithm v

Authentication Algorithm v

PFS Group v

SA Lifetime ?

DPD Interval ?

DPD Failures ?

If choose **AH** as protocol, the window of SA Settings is displayed as below.

^ **General Settings**

Index

Enable ON OFF

Description

Gateway ?

Mode v

Protocol v

Local Subnet ?

Remote Subnet ?

v **IKE Settings**

^ **SA Settings**

Authentication Algorithm v

PFS Group v

SA Lifetime ?

DPD Interval ?

DPD Failures ?

^ **Advanced Settings**

Enable Compression ON OFF

Expert Options ?

SA Settings		
Item	Description	Default
Encrypt Algorithm	Select from "3DES", "AES128" or "AES256" when you select "ESP" in "Protocol". Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from "MD5", "SHA1", "SHA2 256" or "SHA2 512" to be used in SA negotiation.	MD5
PFS Group	Select from "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating set up IPsec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives	60

SA Settings		
Item	Description	Default
	no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	180
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

Status

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

General	Tunnel	Status	x509
^ IPsec Tunnel Status			
Index	Description	Status	Uptime

x509

User can upload the X509 certificates for the IPsec tunnel in this section.

General	Tunnel	Status	x509
^ X509 Settings ?			
Tunnel Name		Tunnel 1 v	
Certificate Files		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.	Tunnel 1
Certificate Files	Click on "Choose File" to locate the certificate file from your computer, and then import this file into your gateway. The correct file format is displayed as follows: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null

x509		
Item	Description	Default
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

3.18 VPN > OpenVPN

This section allows you to set the OpenVPN and the related parameters. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. Gateway supports point-to-point and point-to-points connections.

OpenVPN

The screenshot shows the OpenVPN configuration interface. At the top, there are tabs for 'OpenVPN', 'Status', and 'x509'. Below the tabs is a section titled '^ Tunnel Settings' which contains a table with the following columns: Index, Enable, Description, Mode, Protocol, Server Address, Interface Type, and a '+' icon for adding new settings.

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 “Client”.

The screenshot shows the 'General Settings' form for an OpenVPN tunnel. The fields are as follows:

- Index:** 1
- Enable:** ON (toggle)
- Description:** (empty text field)
- Mode:** Client (dropdown menu, highlighted with a red box)
- Protocol:** UDP (dropdown menu)
- Server Address:** (empty text field)
- Server Port:** 1194
- Interface Type:** TUN (dropdown menu)
- Authentication Type:** None (dropdown menu with a help icon)
- Renegotiation Interval:** 86400 (text field with a help icon)
- Keepalive Interval:** 20 (text field with a help icon)
- Keepalive Timeout:** 120 (text field with a help icon)
- Enable Compression:** ON (toggle)
- Enable NAT:** OFF (toggle)
- Verbose Level:** 0 (dropdown menu with a help icon)

The window is displayed as below when choosing “P2P” as the mode.

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="P2P"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="None"/> v ?
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="Preshared"/> v ?
Encrypt Algorithm	<input type="text" value="BF"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="Password"/> v ?
Username	<input type="text"/>
Password	<input type="text"/>
Encrypt Algorithm	<input type="text" value="BF"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="X509CA"/> v ?
Encrypt Algorithm	<input type="text" value="BF"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/>
Protocol	<input type="text" value="UDP"/>
Server Address	<input type="text"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/>
Authentication Type	<input type="text" value="X509CA Password"/>
Username	<input type="text"/>
Password	<input type="text"/>
Encrypt Algorithm	<input type="text" value="BF"/>
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> ?

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
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P” or “Client”.	Client
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
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

General Settings @ OpenVPN		
Item	Description	Default
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA” and “X509CA Password”. Note: “None” and “Preshared” authentication type are only working with P2P mode.	None
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”. <ul style="list-style-type: none"> 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
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
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 NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of host behind gateway 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. <ul style="list-style-type: none"> 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

Enable HMAC Firewall OFF

Enable PKCS#12 OFF

Enable nsCertType OFF

Expert Options ?

Advanced Settings @ OpenVPN		
Item	Description	Default
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
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ‘;’.	Null

Status

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

OpenVPN | **Status** | x509

^ OpenVPN Tunnel Status

Index	Description	Status	Uptime	Local IP
-------	-------------	--------	--------	----------

x509

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

OpenVPN | Status | **x509**

^ X509 Settings ?

Tunnel Name v

Certificate Files No file chosen

^ Certificate Files

Index	File Name	File Size	Modification Time
-------	-----------	-----------	-------------------

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1

Certificate Files	Click on "Choose File" to locate the certificate file from your computer, and then import this file into your gateway. The correct file format is displayed as follows: @ca.crt @remote.crt @local.crt @private.key @crl.pem @client.p12	Null
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

3.19 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 layer protocols inside virtual point-to-point links over an Internet Protocol network.

GRE

GRE
Status

^ Tunnel Settings

Index	Enable	Description	Remote IP Address
			+

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

GRE

^ Tunnel Settings

Index

Enable ON OFF

Description

Remote IP Address

Local Virtual IP Address

Local Virtual Netmask

Remote Virtual IP Address

Enable Default Route ON OFF

Enable NAT ON OFF

Secrets

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 local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set the remote virtual 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 gateway will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when gateway under NAT environment.	OFF
Secrets	Set the key of the GRE tunnel.	Null

Status

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

GRE		Status			
^ GRE tunnel status					
Index	Description	Status	Local IP Address	Remote IP Address	Uptime

3.20 Services > Syslog

This section allows you to set the syslog parameters. The system log of the gateway 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.

Syslog	
^ Syslog Settings	
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Syslog Level	Debug <input type="button" value="v"/>
Save Position	RAM <input type="button" value="v"/> <input style="float: right;" type="button" value="?"/>
Log to Remote	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input style="float: right;" type="button" value="?"/>

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

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. Note: The lower level will output more syslog in details.	Debug
Save Position	Select the save position from “RAM”, “NVM” or “Console”. Choose “RAM”. The data will be cleared after reboot. Note: It's not recommended that you save syslog to NVM for a long time.	RAM
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow gateway 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

3.21 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.

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

Event Notification Query

^ Event Notification Group Settings

Index Description Send SMS Send Email Save to NVM +

Click **+** button to add an Event parameters.

Notification

^ General Settings

Index

Description

Send SMS ON OFF

Phone Number ?

Send Email ON OFF

Email Addresses ?

Save to NVM ON OFF ?

^ Event Selection ?

System Startup ON OFF

System Reboot ON OFF

System Time Update ON OFF

Configuration Change ON OFF

Cellular Network Type Change ON OFF

Cellular Data Stats Clear ON OFF

Cellular Data Traffic Overflow ON OFF

Poor Signal Quality ON OFF

Link Switching ON OFF

WAN Up ON OFF

WAN Down ON OFF

WWAN Up ON OFF

WWAN Down ON OFF

IPSec Connection Up ON OFF

IPSec Connection Down ON OFF

OpenVPN Connection Up ON OFF

OpenVPN Connection Down ON OFF

LAN Port Link Up ON OFF

LAN Port Link Down ON OFF

USB Device Connect ON OFF

USB Device Remove ON OFF

DDNS Update Success ON OFF

DDNS Update Fail ON OFF

Received SMS ON OFF

SMS Command Execute ON OFF

DI 1 ON ON OFF

DI 1 OFF ON OFF

DI 1 Counter Overflow ON OFF

DI 2 ON ON OFF

DI 2 OFF ON OFF

DI 2 Counter Overflow ON 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 gateway will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in "3.24 Services > Email", and use ';' to separate each number.	OFF
Phone Number	Enter the phone numbers used for receiving event notification. Use a semicolon (;) to separate each number.	Null
Send Email	Click the toggle button to enable/disable this option. When enabled, the gateway will send notification to the specified email box via Email if event occurs. Set the related email address in "3.24 Services > Email".	OFF
Email Address	Enter the email addresses used for receiving event notification. Use a space to separate each address.	Null
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.

Event
Notification
Query

^ Event Details

Save Position RAM v

Filtering

```

Oct 11 15:40:39, system startup
Oct 11 15:40:41, LAN port link up, eth0
Oct 11 15:41:21, WWAN (cellular) up, WWAN1, ip=10.244.165.242
Oct 11 15:41:33, system time update
                    
```

Clear
Refresh

Event Details		
Item	Description	Default
Save Position	Select the events' save position from "RAM" or "NVM". <ul style="list-style-type: none"> 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

3.22 Services > NTP

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

NTP
Status

^ Timezone Settings

Time Zone

UTC+08:00 v

Expert Setting ?

^ NTP Client Settings

Enable

ON

OFF

Primary NTP Server

Secondary NTP Server

NTP Update Interval ?

^ NTP Server Settings

Enable

ON

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 Update interval	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 gateway and also synchronize the gateway time. Click **Sync** button to synchronize the gateway time with the PC's.

NTP

Status

^ Time

System Time 2017-10-11 16:56:27

PC Time 2017-10-11 16:58:16 **Sync**

Last Update Time 2017-10-11 15:41:33

3.23 Services > SMS

This section allows you to set SMS parameters. Gateway supports SMS management, and user can control and configure their gateways by sending SMS. For more details about SMS control, refer to **4.2.2 SMS Remote Control**.

SMS

SMS Testing

^ SMS Management Settings

Enable ON OFF

Authentication Type Password v ?

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". <ul style="list-style-type: none"> 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
SMS Testing

^ SMS Testing

Phone Number

Message

Result

Send

SMS Testing		
Item	Description	Default
Phone Number	Enter the specified phone number which can receive the SMS from gateway.	Null
Message	Enter the message that gateway 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.	--

3.24 Services > Email

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

Email

^ Email Settings

Enable

ON
OFF

Enable TLS/SSL

ON
OFF
?

Outgoing Server

Server Port

Timeout

?

Username

Password

From

Subject

Email Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF

Email Settings		
Item	Description	Default
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
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

3.25 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 gateway, which is assigned to you by your ISP. The service provider defaults to "DynDNS", as shown below.

The screenshot shows the 'DDNS Settings' form. At the top, there are tabs for 'DDNS' and 'Status'. Below the tabs, there is a section titled '^ DDNS Settings'. Inside this section, there is an 'Enable' toggle switch currently set to 'OFF'. Below the toggle, there is a 'Service Provider' dropdown menu with 'DynDNS' selected. Below the dropdown, there are three input fields: 'Hostname', 'Username', and 'Password', all of which are currently empty.

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

The screenshot shows the 'DDNS Settings' form with the 'Service Provider' dropdown menu set to 'Custom'. Below the dropdown, there is a 'URL' input field which is currently empty. The 'Enable' toggle switch remains 'OFF'.

DDNS Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the 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	DynDNS

	Corresponding service provider.	
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.

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.

3.26 Services > SSH

Gateway supports SSH password access and secret-key access.

SSH Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the gateway 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 gateway via SSH. In this case, only the key can be used for login.	OFF

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

3.27 Services > GPS

This section allows you to set the GPS setting parameters.

GPS
Status
Map

^ General Settings

Enable GPS ON OFF

Sync GPS Time ON OFF

^ RS232 Report Settings

Report to RS232 ON OFF

Report GGA Sentence ON OFF

Report VTG Sentence ON OFF

Report RMC Sentence ON OFF

Report GSV Sentence ON OFF

^ GPS Servers

Index	Enable	Protocol	Local Address	Local Port	Server Address	Server Port	
+							

GPS		
Item	Description	Default
General Settings		
Enable GPS	Click the toggle button to enable/disable the GPS option.	OFF
Sync GPS Time		OFF
RS232 Report Settings		
Report to RS232	Submit the GPS information via RS232.	OFF
Report GGA Sentence	Submit the GGA information.	OFF
Report VTG Sentence	Submit the VTG information.	OFF
Report RMC Sentence	Submit the RMC information.	OFF
Report GSV Sentence	Submit the GSV information.	OFF

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

GPS

^ Server Settings

Index

Enable ON OFF

Protocol v

Server Address

Server Port

Send GGA Sentence ON OFF

Send VTG Sentence ON OFF

Send RMC Sentence ON OFF

Send GSV Sentence ON OFF

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

^ Server Settings

Index

Enable ON OFF

Protocol v

Local Address

Local Port

Send GGA Sentence ON OFF

Send VTG Sentence ON OFF

Send RMC Sentence ON OFF

Send GSV Sentence ON OFF

The window is displayed as below when choosing “UDP” as the protocol.

^ Server Settings

Index

Enable ON OFF

Protocol v

Server Address

Server Port

Send GGA Sentence ON OFF

Send VTG Sentence ON OFF

Send RMC Sentence ON OFF

Send GSV Sentence ON OFF

Server Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable the GPS server settings.	ON
Protocol	Select from "TCP Client", "TCP Server" or "UDP".	TCP Client
Server Address @TCP Client	Set the address of the TCP Client.	Null
Server Port @TCP Client	Set the port of the remote TCP Server.	Null
Local Address	Set the local address when the gateway set as a TCP Server.	Null
Local Port	Set the local port when the gateway set as a TCP Server.	Null
Server Address @ UDP	Set the address of the TCP Server.	Null
Server Port @ UDP	Set the port of the remote TCP Server.	Null
Send GGA Sentence	Send GGA information in NMEA format.	OFF
Send VTG Sentence	Send VTG information in NMEA format.	OFF
Send RMC Sentence	Send RMC information in NMEA format.	OFF
Send GSV Sentence	Send GSV information in NMEA format.	OFF

Click the "Status" column to view the current status.

GPS
Status
Map

^ GPS Status

Status Not Fixed

UTC Time 2017-09-15 07:18:23

Last Fixed Time 2017-09-14 12:36:58 UTC

Satellites In Use 4

Satellites In View 12

Latitude 23.1534988

Longitude 113.4013826

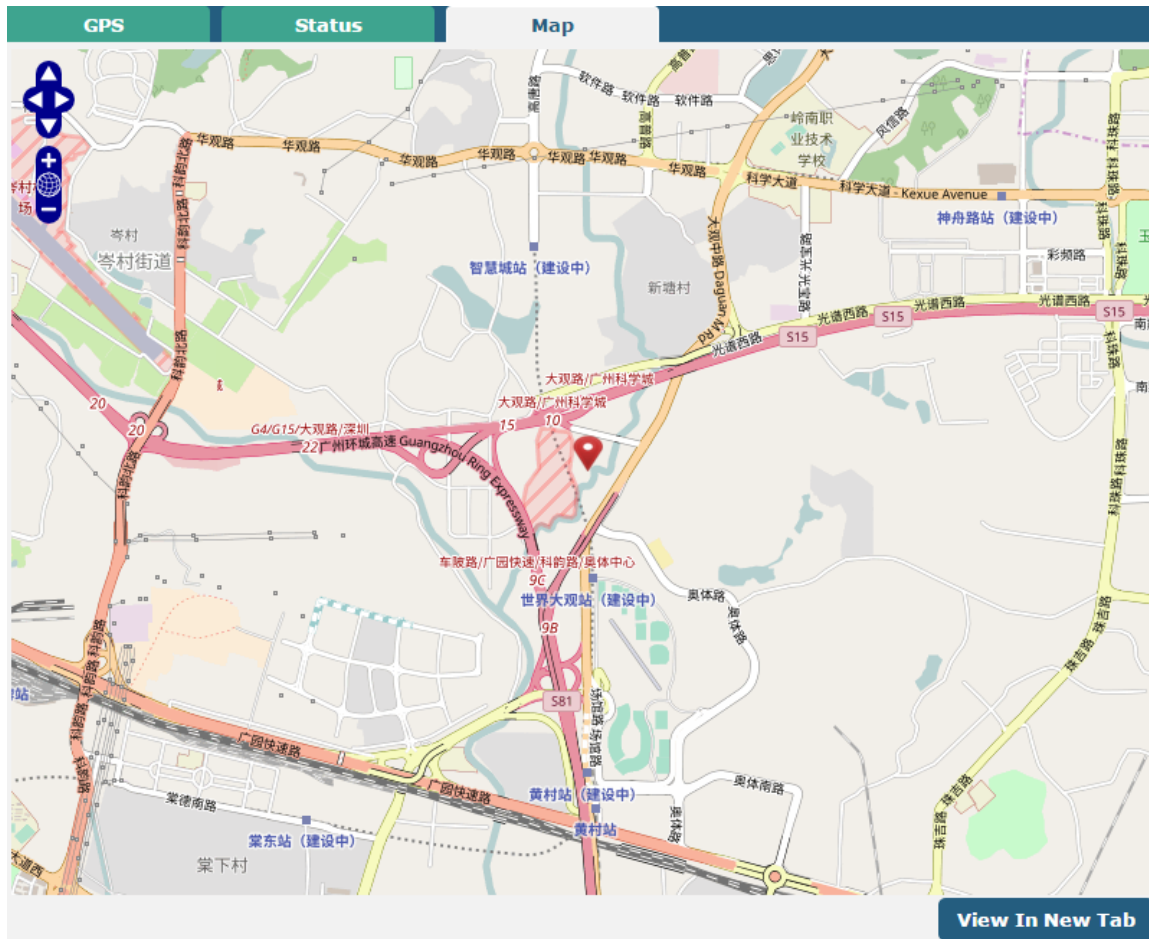
Altitude 29.0 m

Speed 1.947 m/s

GPS Status	
Item	Description
Status	Show the GPS Status. GPS status includes "NO Fix", "2D Fix" and "3D Fix".
UTC Time	Show the UTC of satellites, which is world unified time, not local time.
Last Fixe Time	Show the last positioning time.
Satellites In Use	Show the satellite quantity in use.
Satellites In View	Show the satellite quantity in view.
Latitude	Show the latitude status of gateway.
Longitude	Show the longitude status of gateway.
Altitude	Show the altitude status of gateway.

GPS Status	
Item	Description
Speed	Show the horizontal speed of gateway.

Click "Map" column to view the current location of the gateway.



3.28 Services > Web Server

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

Web Server	Certificate Management
General Settings	
HTTP Port	<input type="text" value="80"/> ?
HTTPS Port	<input type="text" value="443"/> ?

General Settings @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in gateway'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 gateway with other HTTP Port number except 80, only adding that port number then you can login gateway's	80

	Web Server.	
HTTPS Port	<p>Enter the HTTPS port number you want to change in gateway’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 gateway with other HTTPS Port number except 443, only adding that port number then you can login gateway’s Web Server.</p> <p>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.</p>	443

This section allows you to import the certificate file into the gateway.

Import Certificate		
Item	Description	Default
Import Type	Select from “CA” and “Private Key”. <ul style="list-style-type: none"> 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 gateway.	--

3.29 Services > Advanced

This section allows you to set the Advanced and parameters.

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 *.	gateway
User LED Type	Specify the display type of your USR LED. Select from “None”, “OpenVPN” or “IPSec”. <ul style="list-style-type: none"> None: Meaningless indication, and the LED is off OpenVPN: USR indicator showing the OpenVPN status IPSec: USR indicator showing the IPsec status Note: For more details about USR indicator, see “2.2 LED Indicators”.	None

System

Reboot

^ Periodic Reboot Settings

Periodic Reboot ?

Daily Reboot Time ?

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

3.30 System > Debug

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

Syslog
^ Syslog Details

Log Level

Filtering ?

```

Oct 11 16:46:28 router user.debug link_manager[732]: rcv action ping_success from rping
Oct 11 16:46:28 router user.debug link_manager[732]: target link WWAN1, state Connected
Oct 11 16:46:28 router user.info link_manager[732]: WWAN1 ping test success
Oct 11 16:51:28 router user.debug link_manager[732]: WWAN1 (wwan) start ping test
Oct 11 16:51:28 router user.debug rping[2977]: start ping 8.8.8.8 (wwan)
Oct 11 16:51:29 router user.debug rping[2977]: PING 8.8.8.8 (8.8.8.8) from 10.244.165.242: 16 data bytes
Oct 11 16:51:29 router user.debug rping[2977]: 24 bytes from 8.8.8.8: seq=0 ttl=248 time=183.775 ms
Oct 11 16:51:29 router user.debug rping[2977]:
Oct 11 16:51:29 router user.debug rping[2977]: --- 8.8.8.8 ping statistics ---
Oct 11 16:51:29 router user.debug rping[2977]: 1 packets transmitted, 1 packets received, 0% packet loss
Oct 11 16:51:29 router user.debug rping[2977]: round-trip min/avg/max = 183.775/183.775/183.775 ms
Oct 11 16:51:29 router user.debug link_manager[732]: rcv action ping_success from rping
Oct 11 16:51:29 router user.debug link_manager[732]: target link WWAN1, state Connected
Oct 11 16:51:29 router user.info link_manager[732]: WWAN1 ping test success
Oct 11 16:56:29 router user.debug link_manager[732]: WWAN1 (wwan) start ping test
Oct 11 16:56:29 router user.debug rping[3105]: start ping 8.8.8.8 (wwan)
Oct 11 16:56:29 router user.debug rping[3105]: PING 8.8.8.8 (8.8.8.8) from 10.244.165.242: 16 data bytes
Oct 11 16:56:29 router user.debug rping[3105]: 24 bytes from 8.8.8.8: seq=0 ttl=248 time=179.991 ms
Oct 11 16:56:29 router user.debug rping[3105]:
Oct 11 16:56:29 router user.debug rping[3105]: --- 8.8.8.8 ping statistics ---
Oct 11 16:56:29 router user.debug rping[3105]: 1 packets transmitted, 1 packets received, 0% packet loss
Oct 11 16:56:29 router user.debug rping[3105]: round-trip min/avg/max = 179.991/179.991/179.991 ms
Oct 11 16:56:29 router user.debug link_manager[732]: rcv action ping_success from rping
Oct 11 16:56:29 router user.debug link_manager[732]: target link WWAN1, state Connected
Oct 11 16:56:29 router user.info link_manager[732]: WWAN1 ping test success
                    
```

Manual Refresh
Clear
Refresh

^ Syslog Files

Index	File Name	File Size	Modification Time
1	messages	26328	Wed Oct 11 16:56:29 2017

^ System Diagnostic Data

System Diagnostic Data Generate

System Diagnostic Data Download

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 information displayed 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.	--

RT_UG_R3000 LG_v.1.1.0

13 Aug., 2020

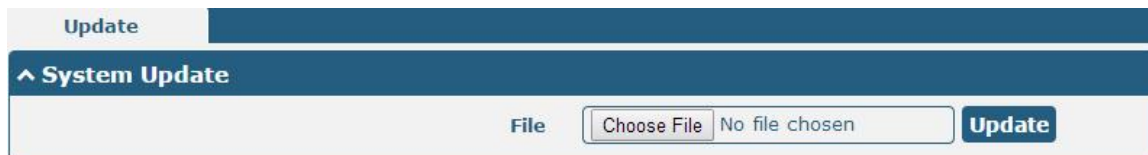
103/135

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 download system diagnosing file.	--

3.31 System > Update

This section allows you to upgrade the firmware of your gateway. Click **System > Update > System Update**, and click on "Choose File" to locate the firmware file to be used for the upgrade. Once the latest firmware has been chosen, click "Update" to start the upgrade process. The upgrade process may take several minutes. Do not turn off your Gateway during the firmware upgrade process.

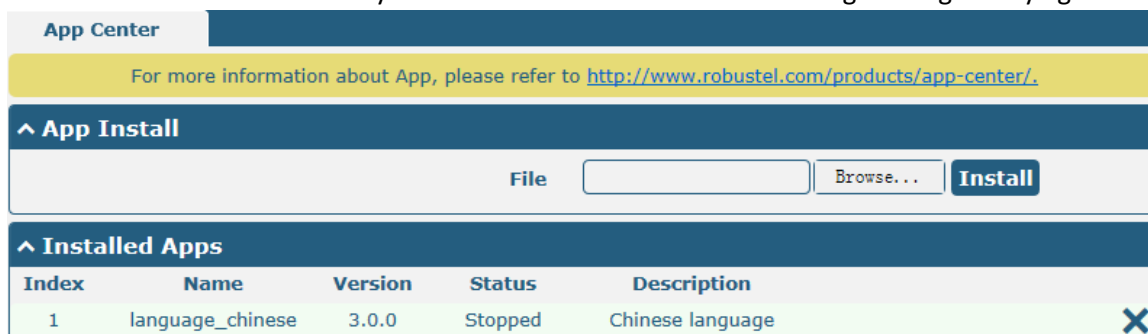
Note: To access the latest firmware file, please contact your technical support engineer.



3.32 System > App Center

This section allows you to add some required or customized applications to the gateway. Import and install your applications to the App Center, and reboot 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 displayed under the "VPN" menu.

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



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 gateway.	--

App Center		
Item	Description	Default
	Note: File format should be <i>xxx.rpk</i> , e.g. <i>R3000 LG-robustlink-1.0.0.rpk</i> .	
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

3.33 System > Tools

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

Ping
Traceroute
Sniffer

^ Ping

IP Address

Number of Request

Timeout

Local IP

Start
Stop

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.	Null
Stop	Click this button to stop ping request.	--

Ping | Traceroute | Sniffer

Traceroute

Trace Address
 Trace Hops
 Trace Timeout

Start Stop

Traceroute		
Item	Description	Default
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Gateway 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.	--

Ping | Traceroute | Sniffer

Sniffer

Interface v
 Host
 Packets Request
 Protocol v
 Status

Start Stop

Capture Files

Index	File Name	File Size	Modification Time
1	17-10-11_17-02-11.cap	24	Wed Oct 11 17:02:12 2017

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 gateway can sniffer at a time.	1000
Protocol	Select from "All", "IP", "TCP", "UDP" and "ARP".	All
Port	Set the port number for TCP or UDP that is used in sniffer.	Null
Status	Show the current status of sniffer.	Null
	Click this button to start the sniffer.	--
	Click this button to stop the 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.	Null

3.34 System > Profile

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

Profile

Rollback

^ Import Configuration File

Reset Other Settings to Default OFF

Ignore Invalid Settings OFF

XML Configuration File No file chosen

^ Export Configuration File

Ignore Disabled Features OFF

Add Detailed Information OFF

Encrypt Secret Data OFF

XML Configuration File

XML Configuration File

^ Default Configuration

Save Running Configuration as Default

Restore to Default Configuration

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 gateway.	--
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 this button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click this button to restore the factory defaults.	--

Profile
Rollback

^ Configuration Rollback

Save as a Rollbackable Archive
Save
?

^ Configuration Archive Files

Index	File Name	File Size	Modification Time
-------	-----------	-----------	-------------------

Rollback		
Item	Description	Default
Configuration Rollback		
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point 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.	--

3.35 System > User Management

This section allows you to change your username and password, and create or manage user accounts. One gateway 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
Common User

^ Super User Settings

New Username	<input type="text"/>	?
Old Password	<input type="password"/>	?
New Password	<input type="password"/>	?
Confirm Password	<input type="password"/>	

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 gateway. 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

Super User
Common User

^ Common User Settings

Index	Role	Username

+

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

Common User

^ Common Users Settings

Index	<input style="width: 80%;" type="text" value="1"/>
Role	<input style="border-bottom: 1px solid #ccc;" type="text" value="Visitor"/> v
Username	<input style="width: 80%;" type="text"/> ?
Password	<input style="width: 80%;" type="password"/> ?

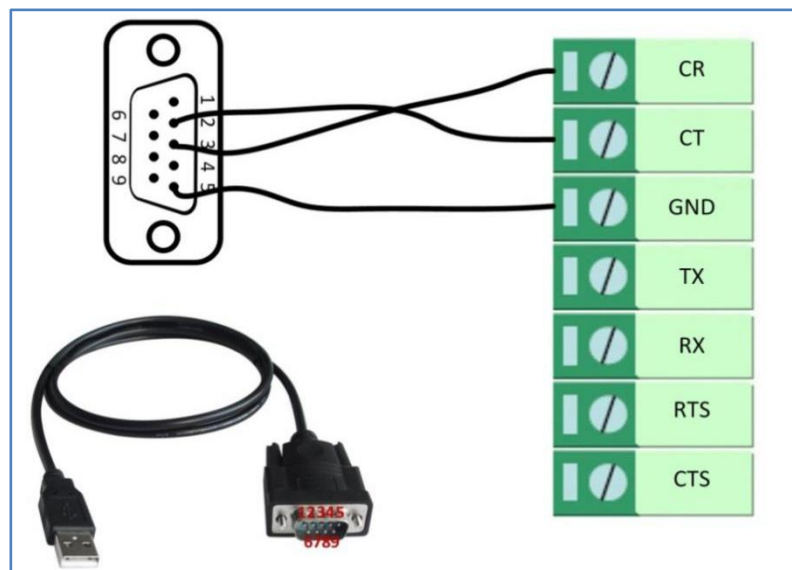
Common User Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Role	Select from "Visitor" and "Editor". <ul style="list-style-type: none"> Visitor: Users only can view the configuration of gateway under this level Editor: Users can view and set the configuration of gateway under this level 	Visitor
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 Interface

4.1.1 Console Port

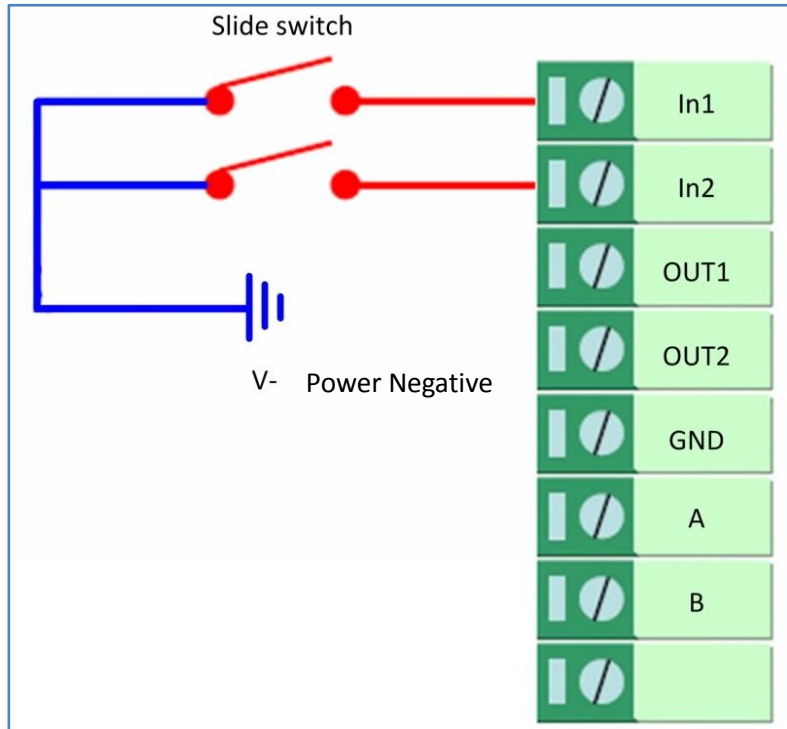
You can use the console port to manage the gateway via CLI commands, please refer to **Chapter 5 Introductions for CLI**.



4.1.2 Digital Input

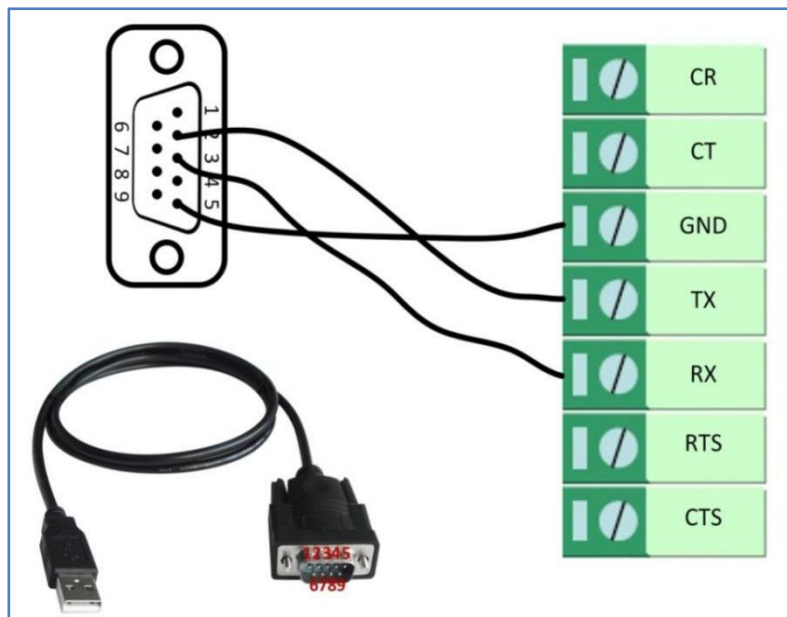
R3000 LG supports digital input with dry contact. Please check the connector interface of the gateway, you can easily find a mark “V-” at one pin of the power connector.

Note: Do not connect In1/In2 directly and do not slide the switch to the port marked “GND” on the terminal block. Otherwise, the DI cannot work properly.



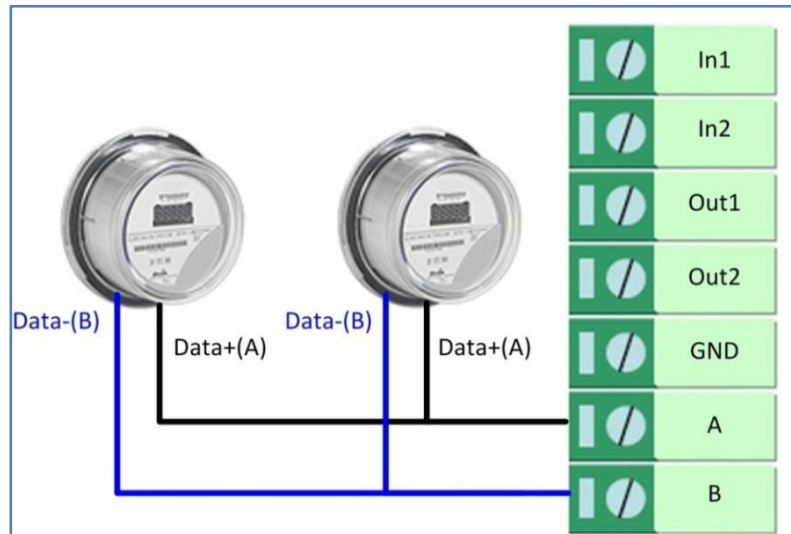
4.1.3 RS-232

R3000 LG supports one RS-232 for serial data communication. Please refer to the connection diagram at the right side.



4.1.4 RS-485

R3000 LG supports one RS-485 for serial data communication. Please refer to the connection diagram at the right side.



4.2 Cellular

4.2.1 Cellular Dial-Up

This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the gateway 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, “WWAN2” as the backup link and “Cold Backup” as the backup mode.

Link Manager
Status

^ General Settings

Primary Link WWAN1 v ?

Backup Link WWAN2 v

Backup Mode Cold Backup v ?

Revert Interval 0 ?

Emergency Reboot ON OFF ?

^ Link Settings

Index	Type	Description	Connection Type	
1	WWAN1		DHCP	
2	WWAN2		DHCP	
3	WAN		DHCP	

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

Link Manager

^ **General Settings**

Index	<input type="text" value="1"/>
Type	<input style="border-bottom: 1px solid #ccc;" type="text" value="WWAN1"/> v
Description	<input type="text"/>

^ **WWAN Settings**

Automatic APN Selection	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Dialup Number	<input type="text" value="*99***1#"/>
Authentication Type	<input style="border-bottom: 1px solid #ccc;" type="text" value="Auto"/> v
Switch SIM By Data Allowance	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Data Allowance	<input type="text" value="0"/> ?
Billing Day	<input type="text" value="1"/> ?

^ **Ping Detection Settings** ?



Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Primary Server	<input type="text" value="8.8.8.8"/>
Secondary Server	<input type="text" value="114.114.114.114"/>
Interval	<input type="text" value="300"/> ?
Retry Interval	<input type="text" value="5"/> ?
Timeout	<input type="text" value="3"/> ?
Max Ping Tries	<input type="text" value="3"/> ?

^ **Advanced Settings**

NAT Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Upload Bandwidth	<input type="text" value="10000"/> ?
Download Bandwidth	<input type="text" value="10000"/>
Overrided Primary DNS	<input type="text"/>
Overrided Secondary DNS	<input type="text"/>
Debug Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Verbose Debug Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> 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**.

Cellular	Status	AT Debug			
^ 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.

Cellular

^ General Settings

Index:

SIM Card: v

Phone Number:

PIN Code: ?

Extra AT Cmd: ?

Telnet Port: ?

^ Cellular Network Settings

Network Type: v ?

Band Select Type: v ?

^ Advanced Settings

Debug Enable: ON OFF

Verbose Debug Enable: ON OFF

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

4.2.2 SMS Remote Control

The gateway supports remote control via SMS. You can use following commands to get the status of the gateway, and set all the parameters. 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--cmd1; cmd2; cmd3; ... cmdn (available when the SMS was sent from the phone number which had been added in gateway’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 gateway’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.



XML command:

```
<lan >
<network max_entry_num="2" >
<id > 1</id >
<interface > lan0</interface >
<ip > 172.16.7.29</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >
```

SMS cmd:

```
set lan network 1 interface lan0
set lan network 1 ip 172.16.7.29
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 = "1.0.0"
kernel_version = 4.1.0
```

```
device_model = R3000 LG
serial_number = 102017111101533
system_uptime = "0 days, 01:39:50"
system_time = "Wed Oct 11 17:20:07 2017"
```

admin:admin;reboot

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

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

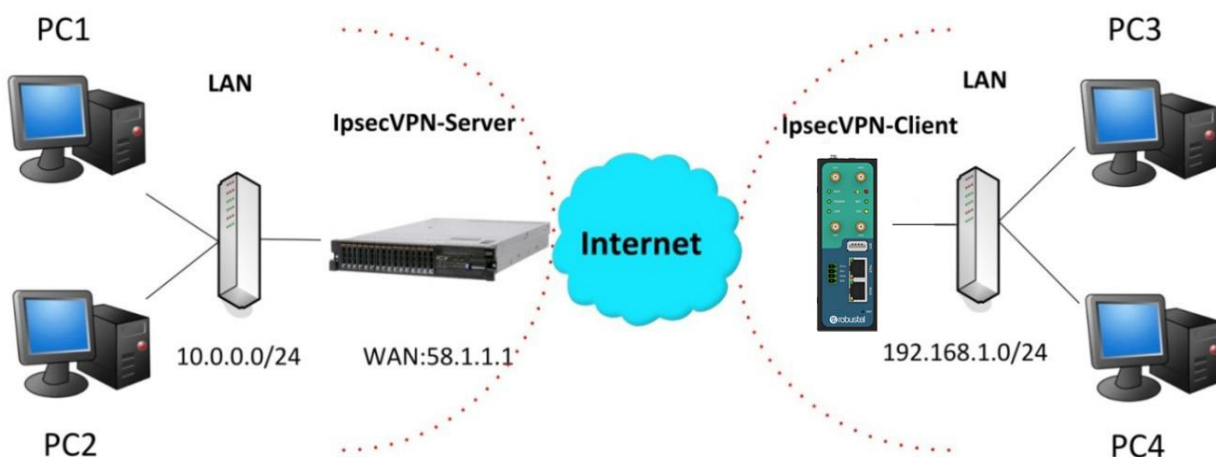
OK

OK

OK

4.3 Network

4.3.1 IPsec VPN



The configuration of server and client is as follows.

IPsec VPN_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

```

IPsec VPN_Client:

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

General	Tunnel	Status	x509			
^ Tunnel Settings						
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

Click **+** button and set the parameters of IPsec Client as below.

Tunnel

^ General Settings

Index

Enable ON OFF

Description

Gateway ?

Mode v

Protocol v

Local Subnet ?

Remote Subnet ?

^ IKE Settings

IKE Type v

Negotiation Mode v

Authentication Algorithm v

Encryption Algorithm v

IKE DH Group v

Authentication Type v

PSK Secret

Local ID Type v

Remote ID Type v

IKE Lifetime ?

^ SA Settings

Encrypt Algorithm	<input type="text" value="3DES"/>	v	
Authentication Algorithm	<input type="text" value="MD5"/>	v	
PFS Group	<input type="text" value="DHgroup2"/>	v	
SA Lifetime	<input type="text" value="28800"/>	?	
DPD Interval	<input type="text" value="60"/>	?	
DPD Failures	<input type="text" value="180"/>	?	

^ Advanced Settings

Enable Compression	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF		
Expert Options	<input type="text"/>	?	

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

The comparison between server and client is as below.

```

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 ?
  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 07:16:26.786: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
    
```

Server (Cisco 2811)

Client (R3000 LG)

^ Tunnel Settings

Index	<input type="text" value="1"/>		
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF		
Description	<input type="text"/>		
Gateway	<input type="text" value="58.1.1.1"/>	?	
Mode	<input type="text" value="Tunnel"/>	v	
Protocol	<input type="text" value="ESP"/>	v	
Local Subnet	<input type="text" value="192.168.1.0"/>	?	
Remote Subnet	<input type="text" value="255.255.255.0"/>	?	

^ IKE Settings

IKE Type	<input type="text" value="IKEv1"/>	v	
Negotiation Mode	<input type="text" value="Main"/>	v	
Authentication Algorithm	<input type="text" value="MD5"/>	v	
Encryption Algorithm	<input type="text" value="3DES"/>	v	
IKE DH Group	<input type="text" value="DHgroup2"/>	v	
Authentication Type	<input type="text" value="PSK"/>	v	
PSK Secret	<input type="text"/>		
Local ID Type	<input type="text" value="Default"/>	v	
Remote ID Type	<input type="text" value="Default"/>	v	
IKE Lifetime	<input type="text" value="86400"/>	?	

^ SA Settings

Encrypt Algorithm	<input type="text" value="3DES"/>	v	
Authentication Algorithm	<input type="text" value="MD5"/>	v	
PFS Group	<input type="text" value="MODP(1024)"/>	v	
SA Lifetime	<input type="text" value="28800"/>	?	
DPD Interval	<input type="text" value="60"/>	?	
DPD Failures	<input type="text" value="180"/>	?	

^ Advanced Settings

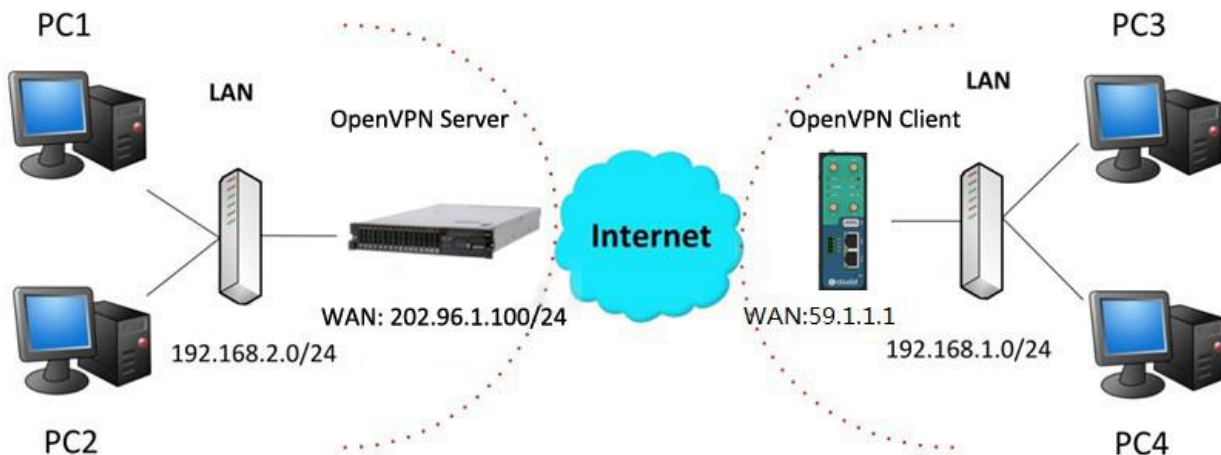
Enable Compression	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF		
--------------------	---	--	--

IKE Setting in Client must be consistent with server.

SA Setting in Client must be consistent with server.

4.3.2 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.

OpenVPN	Status	x509					
^ Tunnel Settings							
Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

Click **+** to configure the Client01 as below.

^ General Settings

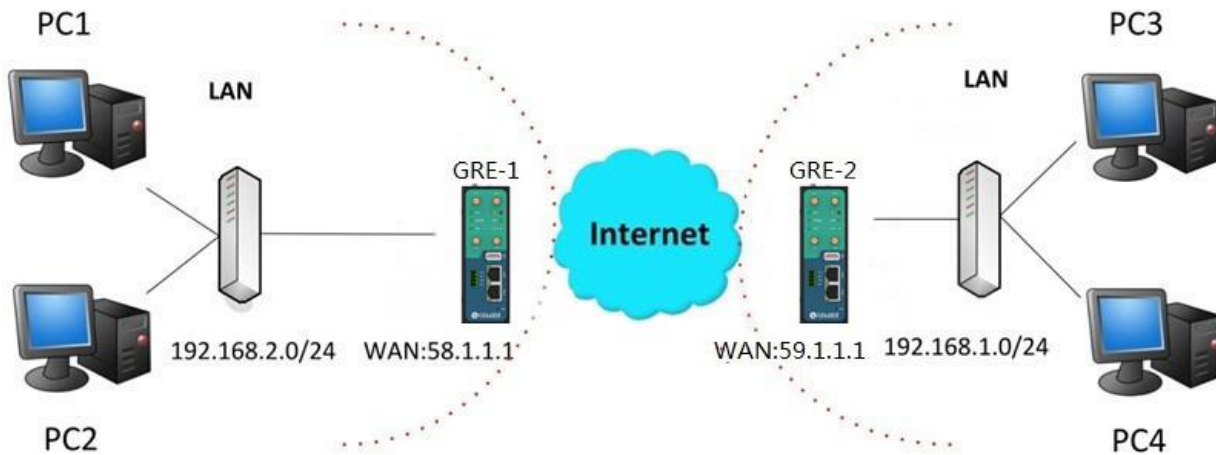
Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text" value="Client01"/>
Mode	<input type="text" value="Client"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text" value="202.96.1.100"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="X509CA"/> v ?
Encrypt Algorithm	<input type="text" value="BF"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Private Key Password	<input type="password" value="•••••"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Verbose Level	<input type="text" value="3"/> v ?

^ Advanced Settings

Enable HMAC Firewall	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable PKCS#12	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable nsCertType	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Expert Options	<input type="text" value="fragment 1500"/> ?

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

4.3.3 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 **+** button and set the parameters of GRE-1 as below.

^ Tunnel Settings	
Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text" value="GRE-1"/>
Remote IP Address	<input type="text" value="59.1.1.1"/>
Local Virtual IP Address	<input type="text" value="10.8.0.1"/>
Remote Virtual IP Address	<input type="text" value="10.8.0.2"/>
Enable Default Route	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets	<input type="password" value="*****"/>

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

GRE-2:

Click **+** button and set the parameters of GRE-2 as below.

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

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

GRE-1	GRE-2
Remote IP Address: 59.1.1.1 (GRE-1 public IP)	Remote IP Address: 58.1.1.1 (GRE-2 public IP)
Local Virtual IP Address: 10.8.0.1 (GRE-1 tunnel IP)	Local Virtual IP Address: 10.8.0.2 (GRE-2 tunnel IP)
Remote Virtual IP Address: 10.8.0.2 (GRE-2 tunnel IP)	Remote Virtual IP Address: 10.8.0.1 (GRE-1 tunnel IP)
Enable NAT: OFF (set the same secret as GRE-2)	Enable NAT: OFF (set the same secret as GRE-1)
Secrets: *****	Secrets: *****

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.

Route login:

Gateway 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
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.
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 save_and_apply / #config commit	When your setting finished, you should enter those commands to make your setting take effect on the device. Note: Commit and save_and_apply plays the same role.

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 = "1.0.0"
kernel_version = 4.1.0
device_model = R3000 LG
serial_number = 10201711101533
system_uptime = "0 days, 01:39:50"
system_time = "Wed Oct 11 17:20:07 2017"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
firmware    New firmware
# tftpupdate firmware (space+?)
String    Firmware name
# tftpupdate firmware filename R3000 LG-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new
firmware name
Downloading
```

R3000 LG-firmware-s 100% |*****| 5018k 0:00:00 ETA

Flashing

Checking 100%

Decrypting 100%

Flashing 100%

Verifying 100%

Verify 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_overridden Overridden Primary DNS
  dns2_overridden Overridden 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 //setting specifies 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 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 = 172.16.7.29
    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 172.16.99.22           //set IP address for lan
OK                                             //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
...
# config save_and_apply
OK                                             // save and apply current configuration, make you configuration effect

```

Example 5: CLI for setting Cellular

```
# show cellular all
```

```
sim {
    id = 1
    card = sim1
    phone_number = ""
    extra_at_cmd = ""
    network_type = auto
    band_select_type = all
    band_gsm_850 = false
    band_gsm_900 = false
    band_gsm_1800 = false
    band_gsm_1900 = false
    band_wcdma_850 = false
    band_wcdma_900 = false
    band_wcdma_1900 = false
    band_wcdma_2100 = false
    band_lte_800 = false
    band_lte_850 = false
    band_lte_900 = false
    band_lte_1800 = false
    band_lte_1900 = false
    band_lte_2100 = false
    band_lte_2600 = false
    band_lte_1700 = false
    band_lte_700 = false
    band_tdd_lte_2600 = false
    band_tdd_lte_1900 = false
    band_tdd_lte_2300 = false
    band_tdd_lte_2500 = false
}
sim {
    id = 2
    card = sim2
    phone_number = ""
    extra_at_cmd = ""
    network_type = auto
    band_select_type = all
    band_gsm_850 = false
    band_gsm_900 = false
    band_gsm_1800 = false
    band_gsm_1900 = false
    band_wcdma_850 = false
    band_wcdma_900 = false
    band_wcdma_1900 = false
    band_wcdma_2100 = false
    band_lte_800 = false
    band_lte_850 = false
```

```

band_lte_900 = false
band_lte_1800 = false
band_lte_1900 = false
band_lte_2100 = false
band_lte_2600 = false
band_lte_1700 = false
band_lte_700 = false
band_tdd_lte_2600 = false
band_tdd_lte_1900 = false
band_tdd_lte_2300 = false
band_tdd_lte_2500 = false
}
# set(space+?)
at_over_telnet    cellular          ddns             dhcp             dns
event            firewall         ipsec           lan              link_manager
ntp              openvpn         reboot          route           serial_port
sms              snmp            syslog          system           user_management
vrrp
# set cellular(space+?)
  sim    SIM Settings
# set cellular sim(space+?)
  Integer  Index (1..2)

# set cellular sim 1(space+?)
  card          SIM Card
  phone_number  Phone Number
  extra_at_cmd  Extra AT Cmd
  network_type  Network Type
  band_select_type  Band Select Type
  band_gsm_850  GSM 850
  band_gsm_900  GSM 900
  band_gsm_1800 GSM 1800
  band_gsm_1900 GSM 1900
  band_wcdma_850 WCDMA 850
  band_wcdma_900 WCDMA 900
  band_wcdma_1900 WCDMA 1900
  band_wcdma_2100 WCDMA 2100
  band_lte_800   LTE 800 (band 20)
  band_lte_850   LTE 850 (band 5)
  band_lte_900   LTE 900 (band 8)
  band_lte_1800  LTE 1800 (band 3)
  band_lte_1900  LTE 1900 (band 2)
  band_lte_2100  LTE 2100 (band 1)
  band_lte_2600  LTE 2600 (band 7)
  band_lte_1700  LTE 1700 (band 4)
  band_lte_700   LTE 700 (band 17)

```

```

band_tdd_lte_2600 TDD LTE 2600 (band 38)
band_tdd_lte_1900 TDD LTE 1900 (band 39)
band_tdd_lte_2300 TDD LTE 2300 (band 40)
band_tdd_lte_2500 TDD LTE 2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
...
# config save_and_apply
OK // save and apply current configuration, make you configuration effect

```

5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug <i>parameters</i>	Turn on or turn off debug function
Show	Show <i>parameters</i>	Show current configuration of each function
Set	Set <i>parameters</i>	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 <i>parameters</i>	

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

Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (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
LoRa	Long Range
LoRaWAN	LoRa Wide Area Network
LPWAN	Low Power Wide Area Network
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

Abbr.	Description
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Guangzhou Robustel LTD

Add: ROOM F315, NO.95 DAGUAN MIDDLE ROAD, TIANHE
DISTRICT, Guangzhou,

Tel: 86-20-29019902

Email: info@robustel.com

Web: www.robustel.com