



robustel R2000S-MHI Dual-SIM LTE IoT Gateway User Guide

[Home](#) » [robustel](#) » robustel R2000S-MHI Dual-SIM LTE IoT Gateway User Guide 



Contents

- [1 R2000S-MHI Dual-SIM LTE IoT Gateway](#)
- [2 Status](#)
- [3 Chapter 4 Configuration Examples](#)
- [4 Chapter 5 Introductions for CLI](#)
- [5 Documents / Resources](#)
- [6 Related Posts](#)

R2000S-MHI Dual-SIM LTE IoT Gateway

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. 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. The router supports point-to-point and point-to-point connections.

Click Virtual Private **Network> OpenVPN> OpenVPN**. The following information is displayed:

OpenVPN

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

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

OpenVPN

^ General Settings

Index

1

Enable

ON

OFF

Enable IPv6

ON

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

OFF

Enable NAT

ON

OFF

Verbose Level

0

?

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

^ General Settings

Index

1

Enable

ON OFF

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 OFF

Enable NAT

ON OFF

Enable DNS overrid

ON OFF

?

Verbose Level

0

?

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

^ General Settings

Index

1

Enable

ON

OFF

Enable IPv6

ON

OFF

Description

Mode

Server

v

?

Protocol

UDP

v

Listen IP Address

Listen Port

1194

Interface Type

TUN

v

Authentication Type

None

v

?

Enable IP Pool

ON

OFF

Client Subnet

10.8.0.0

Client Subnet Netmask

255.255.255.0

Encrypt Algorithm

BF

v

Authentication Algorithm

SHA1

v

Renegotiation Interval

86400

?

Max Clients

10

Keepalive Interval

20

?

Keepalive Timeout

120

?

TUN MTU

1500

Max Frame Size

Private Key Password

Enable Compression

ON

OFF

Enable Default Gateway

ON

OFF

Enable NAT

ON

OFF

Verbose Level

0

v

?

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

^ General Settings

Index

1

Enable

ON OFF

Enable IPv6

ON 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 OFF

Enable NAT

ON OFF

Verbose Level

0

?

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

^ General Settings

Index

1

Enable

ON

OFF

Enable IPv6

ON

OFF

Description

Mode

P2P

v

?

TLS Mode

None

v

?

Protocol

UDP

v

Peer Address

Peer Port

1194

Listen IP Address

Listen Port

1194

Interface Type

TUN

v

Authentication Type

Preshared

v

?

Local IP

10.8.0.1

Remote IP

10.8.0.2

Encrypt Algorithm

BF

v

Authentication Algorithm

SHA1

v

Keepalive Interval

20

?

Keepalive Timeout

120

?

TUN MTU

1500

Max Frame Size

Enable Compression

ON

OFF

Enable NAT

ON

OFF

Verbose Level

0

v

?

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

^ General Settings

Index

1

Enable

ON OFF

Enable IPv6

ON OFF

Description

Mode

P2P

v

?

TLS Mode

None

v

?

Protocol

UDP

v

Peer Address

Peer Port

1194

Listen IP Address

Listen Port

1194

Interface Type

TUN

v

Authentication Type

Password

v

?

Local IP

10.8.0.1

Remote IP

10.8.0.2

Encrypt Algorithm

BF

v

Authentication Algorithm

SHA1

v

Keepalive Interval

20

?

Keepalive Timeout

120

?

TUN MTU

1500

Max Frame Size

Enable Compression

ON OFF

Enable NAT

ON OFF

Verbose Level

0

v

?

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

^ General Settings

Index

1

Enable

ON

OFF

Enable IPv6

ON

OFF

Description

Mode

P2P

v

?

TLS Mode

None

v

?

Protocol

UDP

v

Peer Address

Peer Port

1194

Listen IP Address

Listen Port

1194

Interface Type

TUN

v

Authentication Type

X509CA

v

?

Local IP

10.8.0.1

Remote IP

10.8.0.2

Encrypt Algorithm

BF

v

Authentication Algorithm

SHA1

v

Keepalive Interval

20

?

Keepalive Timeout

120

?

TUN MTU

1500

Max Frame Size

Private Key Password

Enable Compression

ON

OFF

Enable NAT

ON

OFF

Verbose Level

0

v

?

The window is displayed as below when choosing "X 509CA Password" as the authentication type.

^ General Settings

Index
1

Enable
ON OFF

Enable IPv6
ON 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 OFF

Enable NAT
ON OFF

Verbose Level
0

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

^ Advanced Settings

Enable HMAC Firewall
ON OFF

Enable PKCS#12
ON OFF

Enable nsCertType
ON OFF

Expert Options

The window is displayed 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” mode and choosing “X509CA A Password” is displayed as the auth notification type.

OpenVPN

Statusx509

^ 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 the user’s name and past 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

ONOFF

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

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 interfaces for OpenVPN. The difference between TUN and TAP devices is that a TUN device is a point-to-point virtual device on the 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 types 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 the "Password" or "X509CA Password" authentication type.	Null
Password	Enter the password used for the "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 the connection failed, OpenVPN will renegotiate when the renegotiation interval is reached.	86400

Maximum Number of Clients	Set the maximum number of clients allowed to access the OpenVPN server	10
Keepalive Interval	Set a 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 types.	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 the host behind the 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 standards, used to describe personal identity information.	OFF
Enable nsCertType	Click the toggle button to enable/disable nsCertType. Require that the peer certificate was signed with an explicit serotype 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

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's 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 allows you to view the status of the OpenVPN tunnel.

OpenVPN	Status	x509				
^ 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

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

OpenVPN	Status	x509
<div> <div>^ X509 Settings</div> <div> <div>Tunnel Name</div> <div>Tunnel 1</div> <div>v</div> </div> <div> <div>Mode</div> <div>Client</div> <div>v</div> </div> <div> <div>Root CA</div> <div>Choose File</div> <div>No file chosen</div> <div>+</div> </div> <div> <div>Certificate File</div> <div>Choose File</div> <div>No file chosen</div> <div>+</div> </div> <div> <div>Private Key</div> <div>Choose File</div> <div>No file chosen</div> <div>+</div> </div> <div> <div>TLS-Auth Key</div> <div>Choose File</div> <div>No file chosen</div> <div>+</div> </div> <div> <div>PKCS#12 Certificate</div> <div>Choose File</div> <div>No file chosen</div> <div>+</div> </div> </div>		

^ 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 layer protocols 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

Status

^ Tunnel Settings

Index

Enable

Description

Remote IP Address

+

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

GRE

^ Tunnel Settings

Index

1

Enable

ON OFF

Description

Remote IP Address

Local Virtual IP Address

Local Virtual Netmask/Prefix Length

Remote Virtual IP Address

Enable Default Route

ON OFF

Enable NAT

ON OFF

Secrets

Link Binding

Unspecified v ?

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/ IP v6 prefix length	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Addresses	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 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 the router is under a NAT environment.	OFF
Secrets	Set the key to 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 the GRE tunnel.

GRE	Status				
^ GRE tunnel status					
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.

Syslog

^ Syslog Settings

Enable

ON OFF

Syslog Level

Debug v

Save Position

RAM v ?

Log to Remote

ON OFF ?

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

Syslog

^ Syslog Settings

Enable

ON OFF

Syslog Level

Debug v

Save Position

RAM v ?

Log to Remote

ON OFF ?

Add Identifier

ON 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
Sy log Level	Select from “Debug”, “Info”, “Notice”, “Warning”, or “Error”, which from low to high. The lower level will output more Syslog in detail.	Debug
Save Position	Select the save position from “RAM”, “NVM” or “Console”. The data will be cleared after reboot when choosing “RAM”. Note: It's not recommended that you save Syslog to NVM (Non-Volatile Memory) for a long time.	RAM

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 a serial number to the Syslog message which is used for loading Syslog to RobustLink.	OFF
Remote IP Address	Enter the IP address of the Syslog server when enabling the "Log to Remote" option.	Null
Remote Port	Enter the port of the Syslog server when enabling the "Log to Remote" option.	514

3.18 Services> Event

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

Event

Notification

Query

^ General Settings

Signal Quality Threshold
?

General Settings @ Event		
Item	Description	Default
Signal Quality Threshold	Set the threshold for signal quality. The router 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

IndexDescriptionSend SMSSend EmailDO ControlSave to NVM+

Click + button to add Event parameters.

Notification

^ General Settings

Index

Description

Send SMS
☐ ON ☒ OFF

Send Email
☐ ON ☒ OFF

DO Control
☐ ON ☒ OFF

Save to NVM
☐ ON ☒ OFF ?

System Startup	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
System Reboot	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
System Time Update	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Configuration Change	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Network Type Change	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Data Stats Clear	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Data Traffic Overflow	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Poor Signal Quality	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Link Switching	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WLAN Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WLAN Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec Connection Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec Connection Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN Connection Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN Connection Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN Port Link Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN Port Link Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DDNS Update Success	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DDNS Update Fail	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Received SMS	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
SMS Command Execute	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

General Settings @ Notification		
Item	Description	Default
In ex	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 notifications to the specified phone numbers via SMS if an 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 a notification to the specified email box via Email if an event occurs. Set the related email address in "3.21 Services > Email".	OFF

D 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 the event to nonvolatile memory.	OFF

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

Event

Notification

Query

^ Event Details

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

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 following box. Use "&" to separate more than one filter message, such as message & 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.

NTP

Status

^ Timezone Settings

Time Zone

UTC+08:00

v

Expert Setting

?

^ NTP Client Settings

Enable

ON

OFF

Primary NTP Server

pool.ntp.org

Secondary NTP Server

NTP Update Interval

0

?

^ 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 the primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter the secondary NTP Server's IP address or domain name.	Null
NTP Updateinterval	Enter the interval (minutes)synchronizing the NTP client time with the NTP servers. Minutes wait for the 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 the router and also synchronize the router time. Click the **Sync** button to synchronize the router time with the PCs.

NTP

Status

^ Time

System Time

2019-12-31 10:48:42

PC Time

2019-12-31 10:48:44

Sync

Last Update Time

2019-12-31 09:52:03

3.20 Services> SMS

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

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 the WEB manager for authentication. For example, the format of the SMS should be “username: password; cmd; cmd2; ...” • Phonenum: Use the Phone number for authentication, and the user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “cmd; cmd2; ...” • Both: Use both the “Password” and “Phonenum” for authentication. The user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “username: password; cmd; cmd2; ...” 	Password
Phone Number	Set the phone number used for SMS management, and use `;` to separate each number. Note: It can be null when choosing “Password” as the authentication type.	Null

Users 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 the router.	Null
Message	Enter the message that the router will send 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

The email function supports sending the event notifications to the specified recipient by way of an email.

^ Email Settings

Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable TLS/SSL	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Enable STARTTLS	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Outgoing Server	<input type="text"/>
Server Port	<input type="text" value="25"/>
Timeout	<input type="text" value="10"/> ?
Auth Login	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Username	<input type="text"/>
Password	<input type="password"/>
From	<input type="text"/>
Subject	<input type="text"/>

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
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 the SMTP server. When the server does n'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 the 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, and 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.

DDNS

Status

^ DDNS Settings

Enable

ONOFF

Service Provider

DynDNS

v

Hostname

Username

Password

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

^ DDNS Settings

Enable

ONOFF

Service Provider

Custom

v

URL

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 being registered by the 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 the user.	Null

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

DDNS

Status

^ DDNS Status

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

The router supports SSH password access and secret-key access

SSH

Keys Management

^ SSH Settings

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 a username and password to access the router via SSH. In this case, only the key can be used for login.	OFF

SSH

Keys Management

^ Import Authorized Keys

Authorized Keys

Choose File

No file chosen

Import

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 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 the Web Server.

Web Server

Certificate Management

^ General Settings

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 the 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 numbers except 80, only adding that port number then you can log in router's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in the 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 numbers except 443, only adding that port number then you can log in 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 import the certificate file into the router.

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 the 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.

System

Reboot

^ System Settings

Device Name

?

User LED Type

None

v

?

System

Reboot

^ System Settings

Device Name

?

User LED Type

None

v

?

None
SIM
NET
OpenVPN
IPSec
WiFi

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	<p>Specify the display type of your USB LED. Select from “None”, “SIM”, “NET”, “OpenVPN”, “IPSec”, or “WiFi”.</p> <ul style="list-style-type: none"> None: Meaningless indication and the LED is off SIM: USB indicator showing the SIM status NET: USB indicator showing the NET status OpenVPN: USB indicator showing the OpenVPN status IPSec: USB indicator showing the IPsec status WiFi: USB indicator showing the WiFi status <p>Note: For more details about the USB indicators, see “2.2 LED Indicators”.</p>	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 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.

Syslog

^ 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]: rcv 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]: rcv 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

Clear

Refresh

^ Syslog Files

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

^ System Diagnostic Data

System Diagnostic Data

Generate

Syslog		
Item	Description	Default
Syslog Details		
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, and “Error” 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 “3 Seconds”. You can select these intervals to refresh the log information displayed in the following 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' names range from message0 to message 4. And the newest Syslog file will be placed at the top of the list.	--
System Diagnosing Data		
Generate	Click to generate the Syslog diagnosing file.	--
Download	Click to download the system diagnosing file.	--

3.27 System>Update

This section allows you to upgrade the router system and implement system updates by importing and updating firmware files. Import a firmware file from the computer to the router, and 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.

Update

^ System Update

File

Choose File No file chosen

Update

3.28 System>App Center

This section allows you to add some required or customized applications to the router. Import and install your application 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 router, 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 to 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 **X** 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		
In ex	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 with 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 a local IP address from these three automatically.	Null
Start	Click this button to start a ping request, and the log will be displayed in the following box.	--
Stop	Click this button to stop the ping requests.	--

Ping

Traceroute

Sniffer

^ Traceroute

Trace Address

Trace Hops

30

Trace Timeout

1

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. The router will stop tracing if the trace hops have met the max value no matter whether the destination has been reached or not.	30
Trace Timeout	Specify the timeout of the Traceroute request.	1
Start	Click this button to start the Traceroute request, and the log will be displayed in the following box.	--
Stop	Click this button to stop the Traceroute request.	--

Ping
Traceroute
Sniffer


^ Sniffer

Interface
all
v

Host



Packets Request
1000





Protocol
All
v

Status


Start
Stop

^ Capture Files

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 contains the specified 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 the sniffer.	--
	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 time of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List click  to download the log and 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 the factory default setting.

Profile

Rollback

^ Import Configuration File

Reset Other Settings to Default

ONOFF?

Ignore Invalid Settings

ONOFF?

XML Configuration File

Choose FileNo file chosen

Import

^ Export Configuration File

Ignore Disabled Features

ONOFF?

Add Detailed Information

ONOFF?

Encrypt Secret Data

ONOFF?

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 the button to generate the XML configuration file, and click Export to export the XML configuration file.	--
Default Configuration		
Save the Running configuration as Default	Click Save the button to save the current running parameters as the default configuration.	--
Restore to Default Configuration	Click Restore the 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	
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 change your 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 characters 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

?

Old Password

?

New Password

?

Confirm 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 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

Super User

Common User


^ Common User Settings

Index

Role

Username

+

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

Common User

^ Common Users Settings

Index

1

Role

Visitor

v

Username

?

Password

?

Common User S things		
Item	Description	Default
In ex	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 the router under this level • Editor: Users can view and set the configuration of the router 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 Cellular

4.1.1 Cellular Dial-Up

This section shows you how to configure the primary and backup SIM card for 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 choosing WWAN1 as the primary link and set the backup mode as a 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.

Link Manager

Status

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.

Link Manager

^ General Settings

Index

Type v

Description

IPv6 Enable ☒ ON ☐ OFF

^ WWAN Settings

Automatic APN Selection ☒ ON ☐ OFF

Dialup Number

Authentication Type v

PPP Preferred ☐ ON ☒ OFF ?

Switch SIM By Data Allowance ☐ ON ☒ OFF ?

Data Allowance ?

Billing Day ?

^ IPv6 LAN Settings

Connection Type v

IPv6 Prefix

IPv6 NAT Enable ☒ ON ☐ OFF

^ Ping Detection Settings
?

Enable

ON OFF

IPv4 Primary Server

8.8.8.8

IPv4 Secondary Server

114.114.114.114

IPv6 Primary Server

2001:4860:4860::8888

IPv6 Secondary Server

2400:da00:2::29

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Max Ping Tries

3

?

^ Advanced Settings

IPv4 NAT Enable

ON OFF

Upload Bandwidth

10000

?

Download Bandwidth

10000

Overridden Primary DNS

Overridden Secondary DNS

Overridden IPv6 Primary DNS

Overridden IPv6 Secondary DNS

Debug Enable

ON OFF

Verbose Debug Enable

ON OFF

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.

^ 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 OFF
Verbose Debug Enable
ON OFF

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

4.1.2 SMS Remote Control

R2000 supports remote control via SMS. You can use the 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; ...code (available for every phone number).
2. phonenum mode-- Password; cmd1; cmd2; cmd3; ... code (available when the SMS was sent from the phone number which had been added to the router's phone group).
3. Both modes-- Username: Password;cmd1;cmd2;cmd3; ...code(available when the SMS was sent from the phone number which had been added in the router's phone group).

SMS command Explanation:

1. User name and Password: Use the same username and password as the 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 configured 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.

Profile
Rollback

^ 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
```

- The semicolon character (;) is used to separate more than one command packed in a single SMS.
- E.g.

admin:admin;status system

In this command, the username is "admin", the 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, the username is "admin", the 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, the username is "admin", the 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, the username is "admin", the password is "admin", and the command is to configure the LAN parameter.

SMS received:

OK

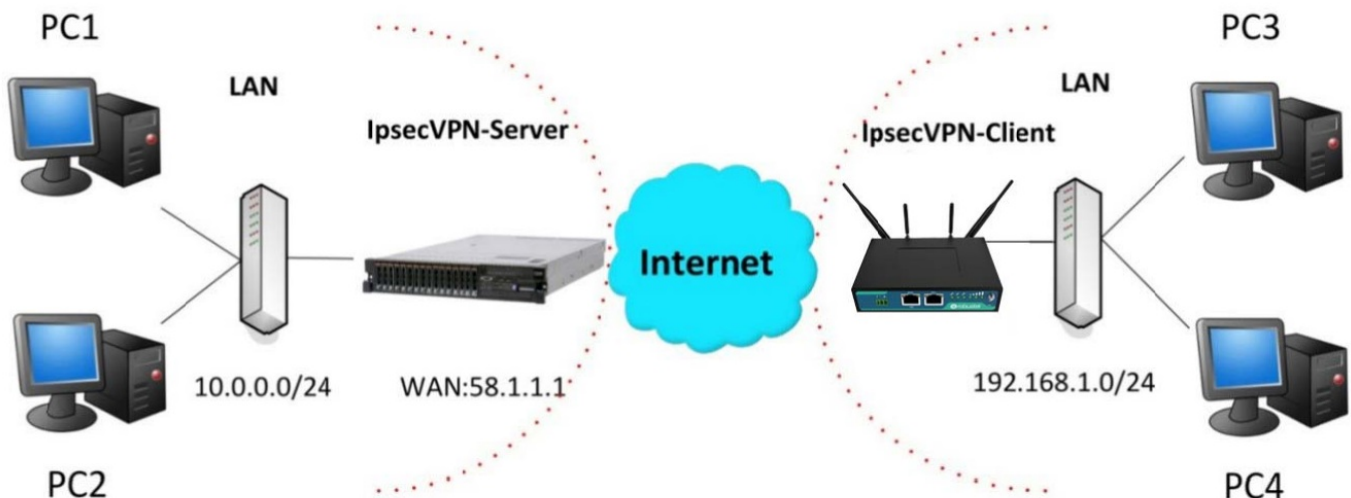
OK

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
```

```

hash          Set hash algorithm for protection suite
lifetime      Set lifetime for ISAKMP security association
no            Negate a command or set its defaults
Router(config)#encryption 3des
Router(config)#hash md5
Router(config)#authentication pre-share
Router(config)#group 2
Router(config)#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

```

General


Tunnel

Status

x509

^ Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+
-------	--------	-------------	---------	--------------	---------------	---

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

Tunnel

^ General Settings

Index

1

Enable

ON OFF

Description

Gateway

?

Mode

Tunnel

v

Protocol

ESP

v

Local Subnet

?

Remote Subnet

?

Link Binding

Unspecified

v

?

^ IKE Settings

IKE Type

IKEv1

v

Negotiation Mode

Main

v

Encryption Algorithm

3DES

v

Authentication Algorithm

SHA1

v

IKE DH Group

DHgroup2

v

Authentication Type

PSK

v

PSK Secret

Local ID Type

Default

v

Remote ID Type

Default

v

IKE Lifetime

86400

?

^ SA Settings

Encryption Algorithm

3DES

v

Authentication Algorithm

SHA1

v

PFS Group

DHgroup2

v

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.


```

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 (128 bits)
esp-des ESP transform using DES cipher (64 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 202.96.1.1
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)#no
Router(config-if)#crypto map cry-map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

```

General Settings

Index: 1

Enable: ☒

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: ☐

Enable Forceencaps: ☐

Expert Options:

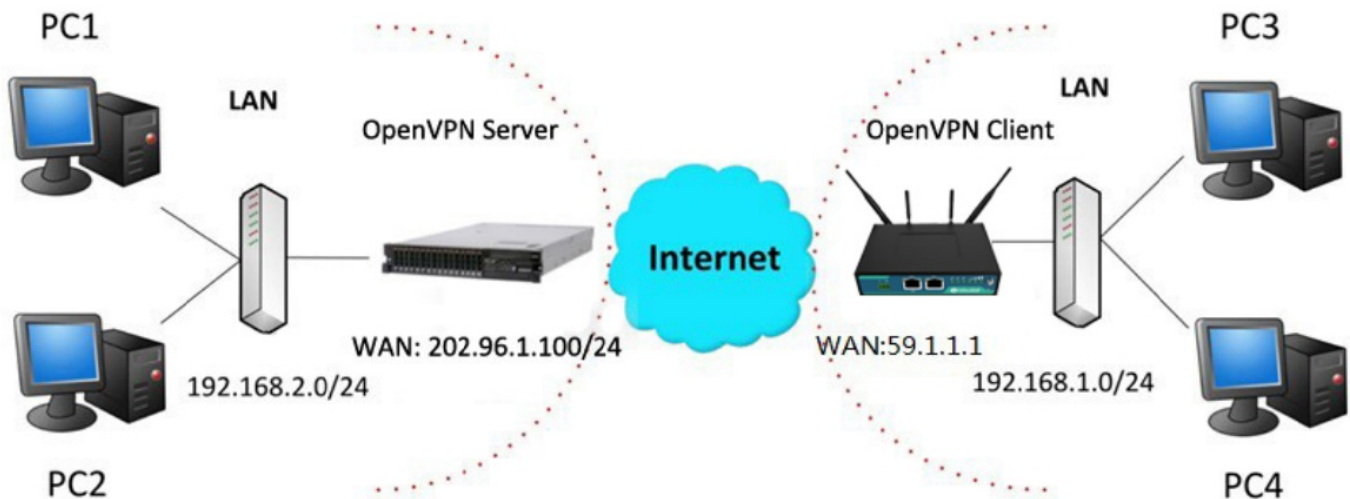
Server (Cisco 2811)

Router IKE Settings should be consistent with service fees.

Router SA Settings should be consistent with service fees.

4.2.2 OpenVPN

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



OpenVPN_Server:

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

```

local 202.96.1.100
mode server
port 1194
proto UDP
dev tun-
MTU 1500
fragment 1500

```

ca ca. crt
cert Server01.crt
key Server01.key
DH dh1024.poem
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	Peer Address	Interface Type	+

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

Click  to configure the Client01 as below.

OpenVPN

^ General Settings

Index

1

Enable

ON

OFF

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

OFF

Enable NAT

ON

OFF

Enable DNS overrid

ON

OFF

?

Verbose Level

3

?

^ Advanced Settings

Enable HMAC Firewall

ON

OFF

Enable PKCS#12

ON

OFF

Enable nsCertType

ON

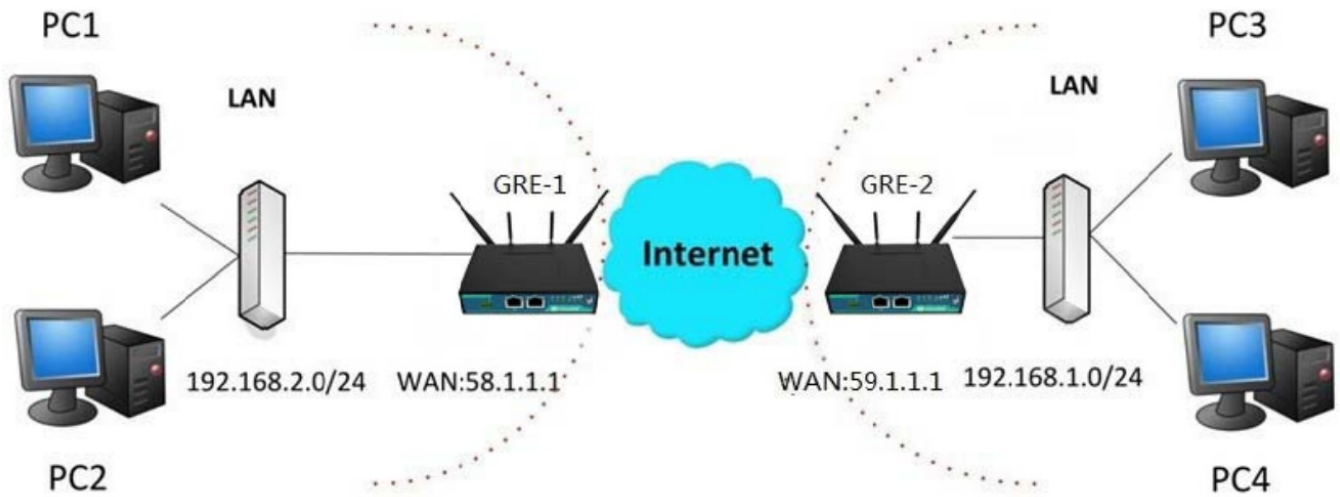
OFF

Expert Options

?

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

4.2.3 GRE VPN



The configuration of the two points is as follows.
The window is displayed 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	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
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	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets
Link Binding	Unspecified v ?

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

GRE-2:

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

GRE

^ Tunnel Settings

Index

1

Enable

ON OFF

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

ON OFF

Enable NAT

ON OFF

Secrets

Link Binding

Unspecified

v

?

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

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

GRE

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

v

?

GRE-1 real public network IP address

GRE-1 real tunnlr IP address

GRE-2 real tunnlr IP address

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

^ 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

v

?

GRE-2 real public network IP address

GRE-2 real tunnlr IP address

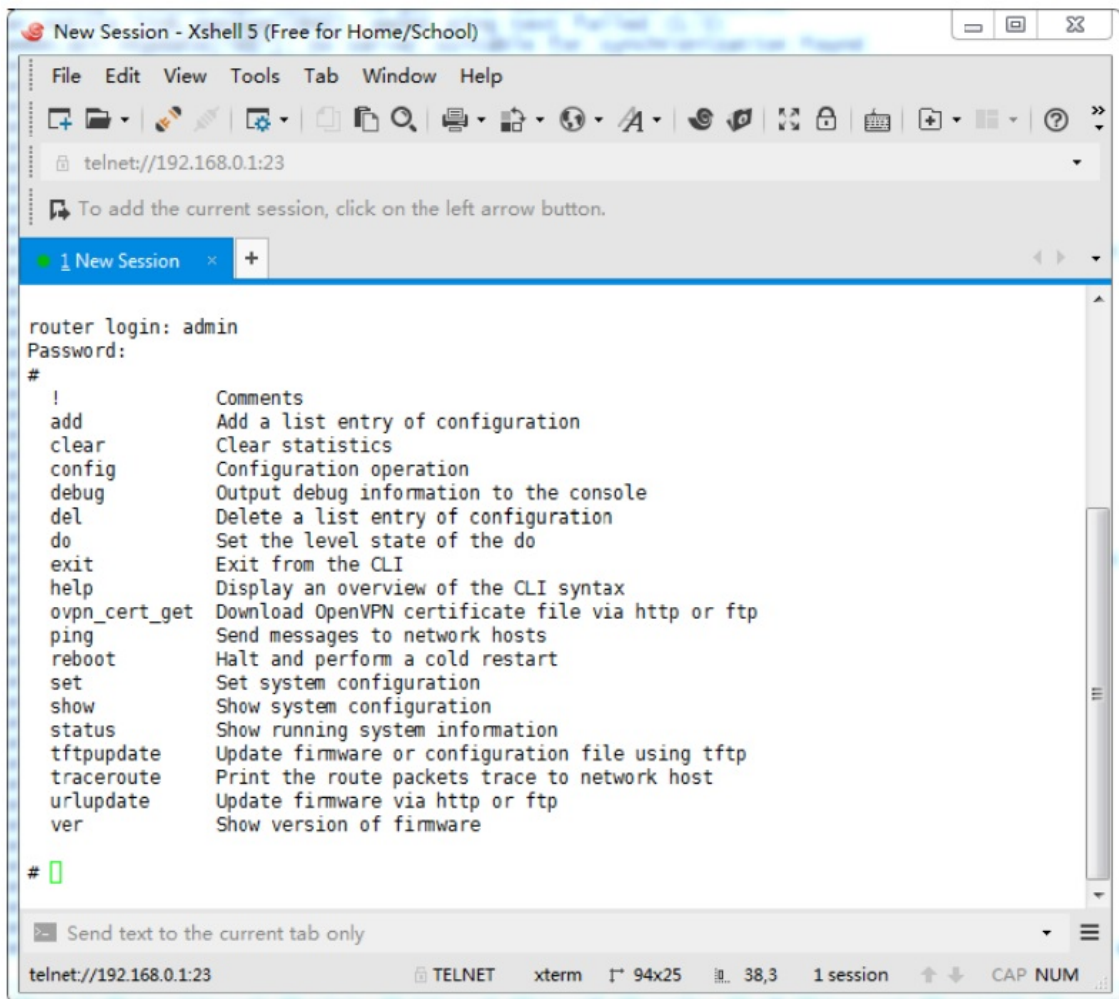
GRE-1 real tunnlr IP address

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 x +
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 the 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
TFTP update	Update firmware using TFTP
tracert	Print the route packets trace to the network host
URL update	Update firmware using HTTP or FTP
ver	Show version of the firmware

5.2 How to Configure the CLI

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

Commands /tips	Description
?	Typing a question mark “?” will show you the helpful 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 load default Restore Factory Configuration
Ctrl+c	Press these two keys at the same time, except its “copy” function but also can be used to “break” out of the setting program.
Syntax error: The command is not completed	The command is not completed.
Tick space key+ Tab key	It can help you finish your command. Example: # config (tick enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply load default
#config commit	When your setting is finished, you should enter those commands to make

# config save_and_apply	your setting takes effect on the device. Note: Commit and save_and_apply play 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 Add 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		

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 learning to configure it with some reference examples.

Example 1: Show the 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 firmware filename 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%
Verify Success
upgrade success
# config save_and_apply
OK
//update success
// save and apply current configuration, make your configuration effect
```

Example 3: Set link-manager

set

set

at_over_telnet	AT Over Telnet
cellular	Cellular
DNS	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
very	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 desc connection_type wwan static_addr pppoe ping mtu dnsl_overridden dns2_overridden	Type Description Connection Type WWAN Settings Static Address Settings PPPoE Settings Ping Settings MTU Override Primary DNS Override Secondary DNS
--	--

```
# set link_manager link 1 type wwan1
OK
#set link_manager link 1 wwan
```

auto_apn apn username password dialup_number auth_type aggressive_reset switch_by_data_allowance data allowance billing_day	Automatic APN Selection APN Username Password Dialup Number Authentication Type Aggressive Reset Switch SIM By Data Allowance Data Allowance Billing Day
--	---

```
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan billing_data_allowance 100
OK
# set link_manager link 1 wwan billing_day 1
OK
...
# config save_and_apply
OK
//open cellular switch_by_data_traffic
//setting succeed
// setting specifies the day of the month for billing
// setting succeed
```

```
// save and apply the current configuration, and make your configuration effect
```

Example 4: Set Ethernet

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

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
```



```

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 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	bits per second
L2TP	Layer 2 Tunneling Protocol

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

WAN	Wide Area Network
-----	-------------------

Guangzhou Robustel LTD

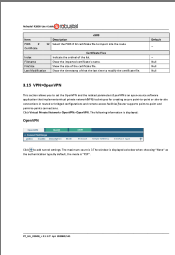
Add: 3rd Floor, Building F, Kehui Park, No.95 Daguan Road, Guangzhou, China 510660

Tel: 86-20-29019902

Email: info@robustel.com

Web: www.robustel.com

Documents / Resources

	<p>robustel R2000S-MHI Dual-SIM LTE IoT Gateway [pdf] User Guide</p> <p>R2000S-MHI, R2000SMHI, 2AAJGR2000S-MHI, 2AAJGR2000SMHI, R2000S-MHI Dual-SIM L TE IoT Gateway, R2000S-MHI, Dual-SIM LTE IoT Gateway</p>
--	--