robustel | Application Note

GRE between RobustOS and Cisco

Version:	**v.1.0.0**
Date:	**2017-03-06**
Status:	**Confidential**
Doc ID:	**GRE between RobustOS and Cisco**
Author:	**Singson Chen**

www.robustel.com

robustOS

Contents

Chapter 1 Introduction

1.1 Overview

RobustOS (hereinafter referred to as “the ROS”) is a new operating system for Robustel's IoT gateway released in 2015. It is a modular and open software platform which could support third party development based on SDK/API. Meanwhile, it supports different routing and VPN protocols for different application scenarios. This newer platform provides a different web configuration interface than the existing platform.

VPN (Virtual Private Network) is a technology establishing private network tunnel on the public network. GRE is one of tunnel protocols for transmitting the data packets from one network to another network. GRE tunnel supports the multicast and can be used to connect with the enterprise private network, but lacks of strong enough security mechanism.

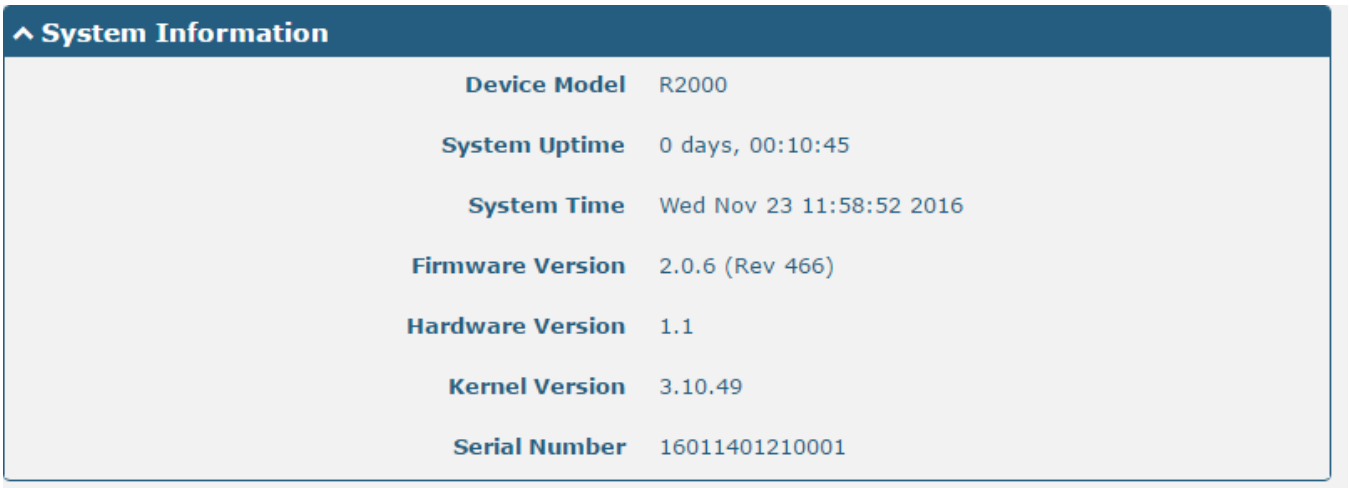
This application note has been written for customer with a good understanding of Robustel products and a basic experienced of VPN. It shows customer how to configure and test the GRE VPN between the R2000 and Cisco router through the cellular network.

This application note applies to the ROS firmware of R2000 and R2000. However, the followings will take R2000 as an example

1.2 Assumptions

The features of GRE VPN have been fully tested and this application note has been written by technically competent engineer who is familiar with the Robustel products and the application requirements.
This application note is based on:

- Product model: Robustel GoRugged R2000, an industrial cellular VPN router
- Firmware version: R2000_ROS_ v2.0.6
- Configuration: This application note assumes the Robustel products are set to factory default. Most of configuration steps are only shown if they are different from the factory default settings.



The R2000 router must be assigned a public IP address to its WAN port. The IP address can be dynamic or static. If the R2000 working with dynamic public IP address, a DNS service must be used to park dynamic public IP address to a static domain.

1.3 Rectifications

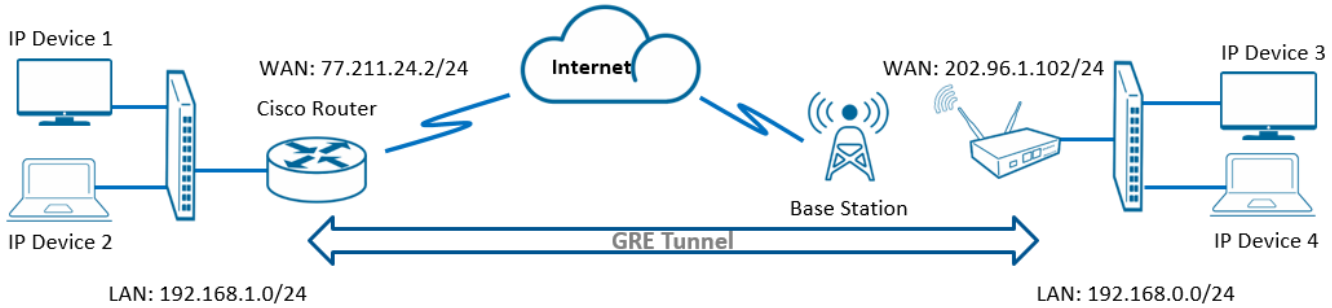
Requests for corrections or rectifications to this application note will be appreciated, and if there are any request for new application notes please email to: support@robustel.com.

1.4 Version

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Release Date	Firmware Version	Change Description
2017-03-06	v.1.0.0	Initial Release

Chapter 2 Topology



1. Cisco router runs as central router which has a static public IP address, or a dynamic public IP address with domain name.
2. The R2000 works with static public IP address.
3. GRE VPN will be established between the central Cisco router and the R2000, and the internal network can be visited by each other.

Note: *The two peer devices should have a fixed public IP address because it needs to specify the peer public IP when establishing GRE tunnel, and make sure the data packets can be transmitted through the public network.*

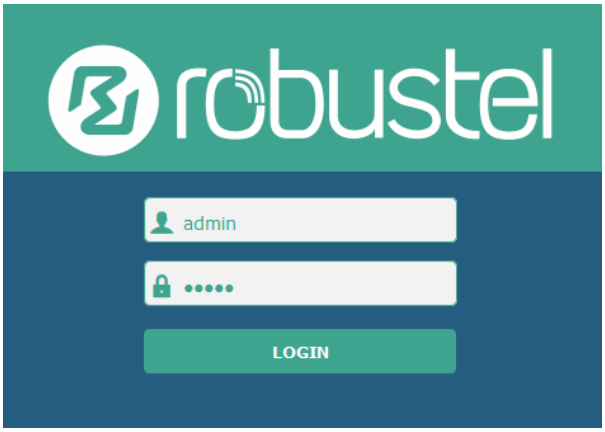
Chapter 3 Configuration

3.1 GRE VPN Configuration on R2000

3.1.1 Configure Link Manager

1. Follow these steps before configuring the router:

- Attach the external antenna to the router's connector and twist tightly
- Insert the SIM cards into the router
- Connect the power supply correctly
- Log in the Web GUI of the router

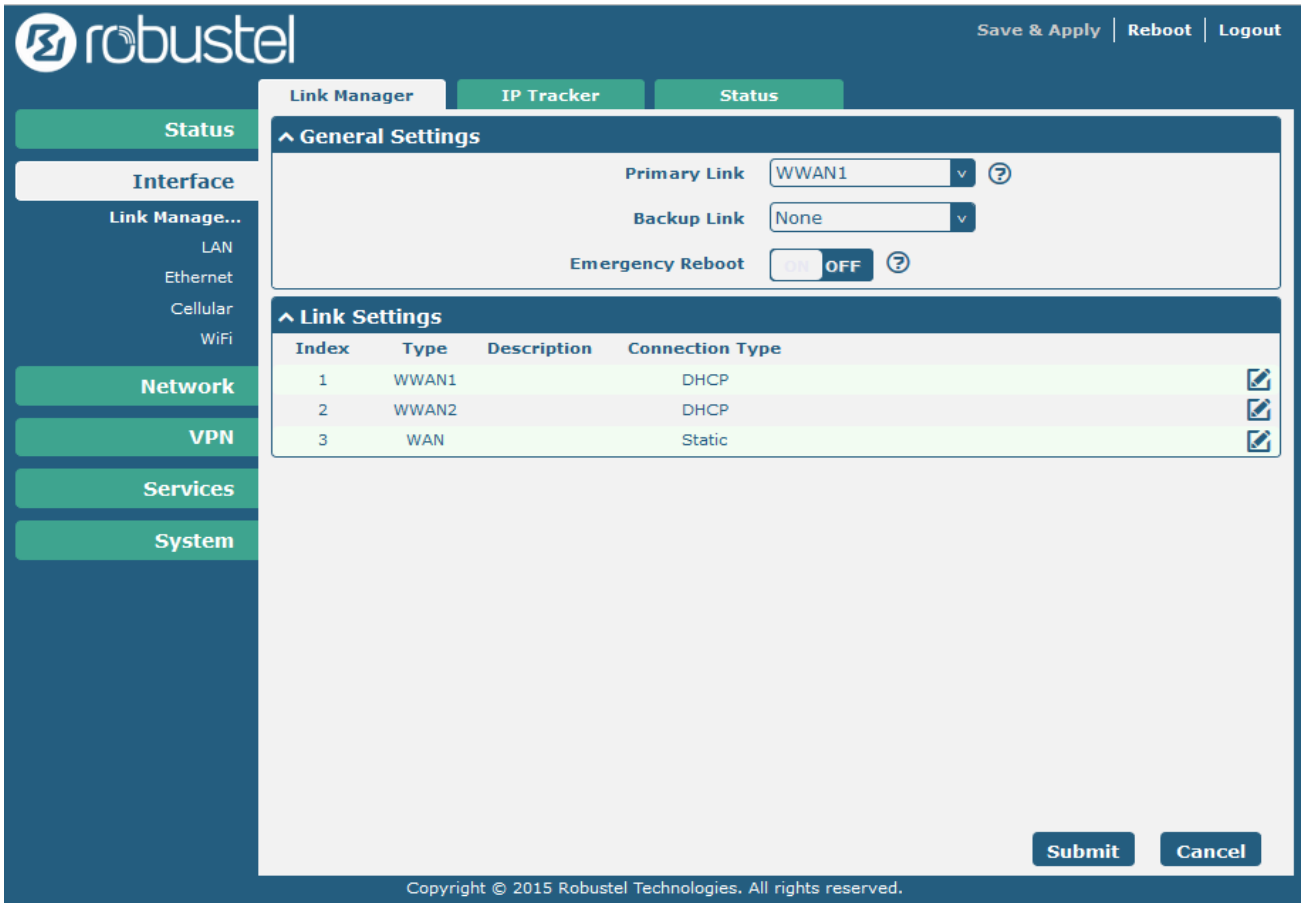


You need to know the following factory settings before you have logged in the Web GUI.

Item	Description
Username	Admin
Password	Admin
Eth0	192.168.0.1/255.255.255.0, LAN mode
Eth1	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

2. Browse to **Interface > Link Manager**.

- Click the drop-down list of "Primary Link" and select "WWAN1".
- Click "Submit".
- Click "Save & Apply".

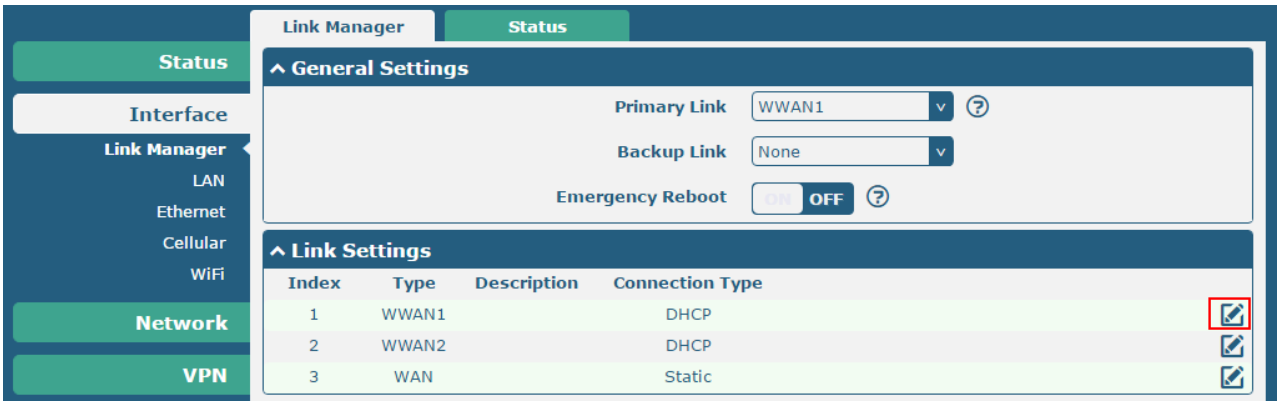


Item	Description	Setting
Primary Link	Select “WWAN1”, “WWAN2” or “WAN” as the primary connecting interface.	WWAN1

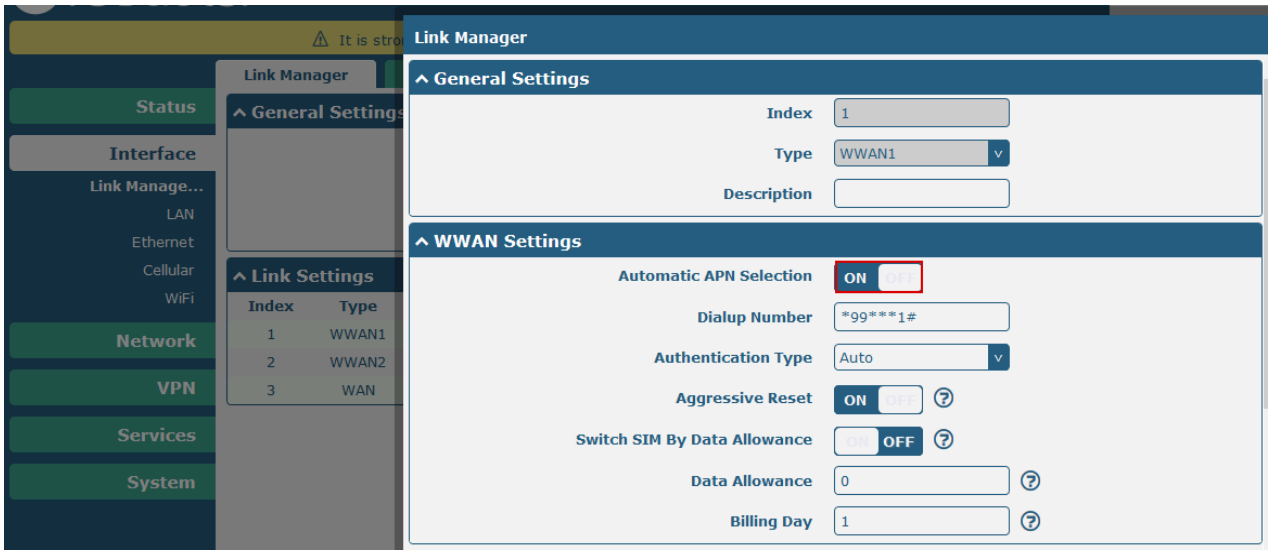
3.1.2 Configure Cellular WAN

1. Browse to **Interface > Link Manager > Link Settings**.

- Click the edit button of “WWAN1”.
- Enter the related parameters in the “WWAN Settings” window.
- Enter the related parameters in the “Ping Detection Settings” window.
- Click “Submit”.
- Click “Save & Apply”.

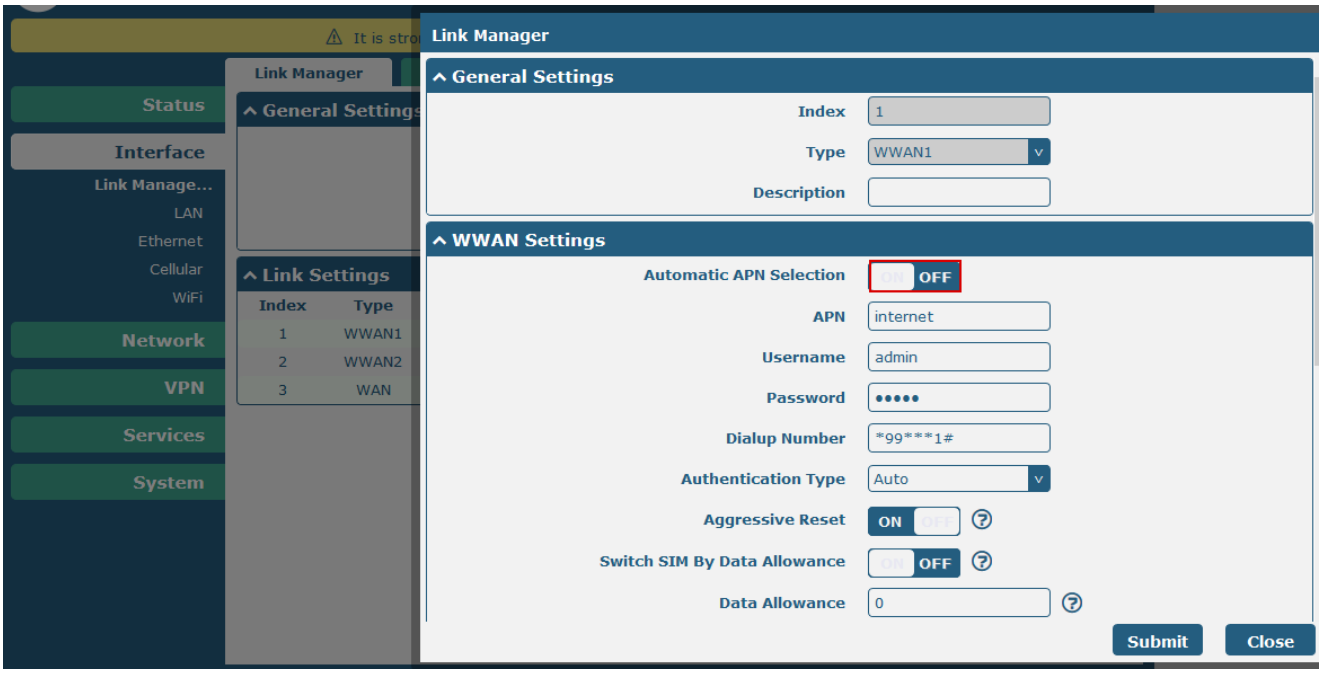


The window is displayed as below when enabling the “Automatic APN Selection” option.

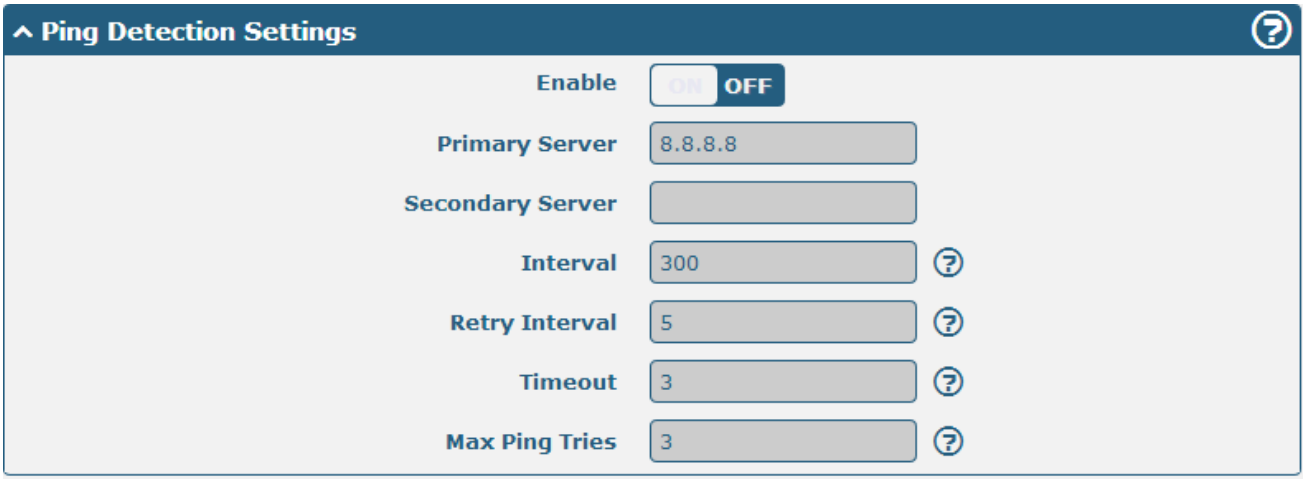


Item	Description	Setting
Dialup Number	Set the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Data Allowance	Set the monthly data traffic limitation.	0
Billing Day	Specify the monthly billing day, and the data traffic statistics will be recalculated from this day.	1

The window is displayed as below when disabling the “Automatic APN Selection” option.



Item	Description	Setting
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	Internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null



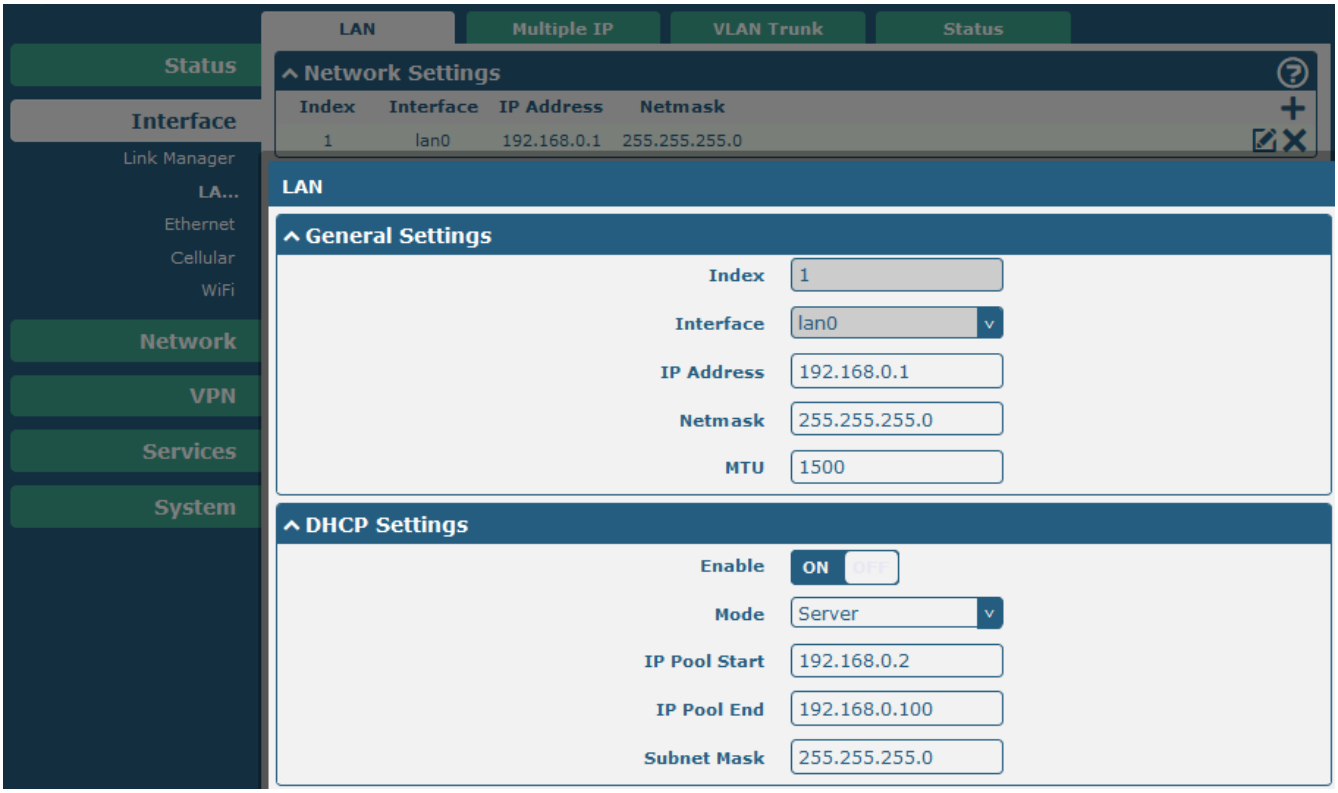
Item	Description	Setting
Enable	Click the toggle button to enable the ping detection, a keepalive policy of R2000 router.	OFF
Primary Server	Router will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check	Null

	if the current connectivity is active.	
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	3

3.1.3 Configure IP Address of LAN

1. Browse to **Interface > LAN > LAN**.

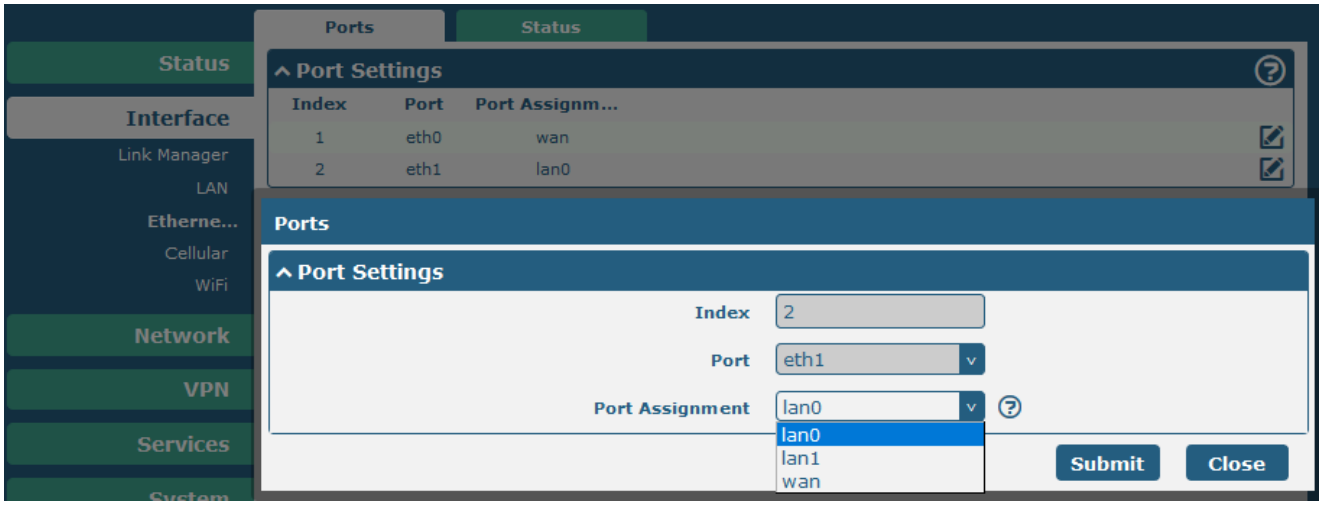
- Click the edit button of “lan0”.
- Set its IP address and Netmask, and the parameters of “DHCP Settings” are set accordingly.
- Click “Submit”.
- Click “Save & Apply”.



Item	Description	Setting
IP Address	Set the IP address of lan0.	Enter accordingly
Netmask	Set the Netmask of lan0.	Enter accordingly
MTU	Set the MTU of lan0.	1500

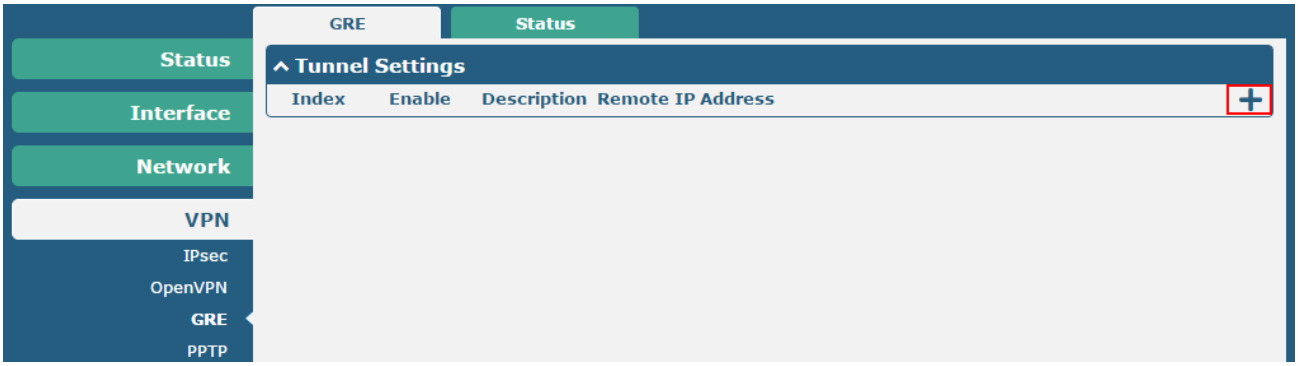
2. Browse to **Interface > Ethernet > Ports**.

- Click the edit button of “eth1”.
- Assign lan0 to the eth1 port.
- Click “Submit”.
- Click “Save & Apply”.



3.1.4 GRE server Configuration

1. Browse to **VPN > GRE**, add and enable the GRE tunnel.



2. Configure the parameters of GRE, and click “Submit > Save & Apply”.

Item	Description	Setting
Index	Show the index of the tunnel.	1
Enable	Click the toggle button to enable the GRE tunnel. GRE (Generic Routing Encapsulation) is a protocol encapsulating packets in order to route other protocols over IP networks.	ON
Description	Enter a description for this GRE Tunnel.	Null
Remote IP Address	Set remote IP Address of the virtual GRE tunnel.	Null
Local Virtual IP	Set local IP Address of the virtual GRE tunnel.	Null
Remote virtual IP	Set remote IP Address of the virtual GRE tunnel.	Null
Enable Default Route	All the traffics of R2000 router will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable the NAT feature of GRE. The source IP address of host Behind R2000 will be disguised before accessing the remote GRE server.	Disable
Secrets	Set Tunnel Key of GRE.	Null

3.2 GRE VPN Configuration on Cisco router

Enter configuration mode and check the IOS version of the Cisco router. In this case, the mode needs to be “enable mode” in advance (e.g. typing “configure terminal”).

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

The entries below sets the host name of the Cisco router.

```
hostname cisco2811
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$ROMx$RGJMeV3dfHuOQu0z7Ffjh.
```

The entries below sets the GRE VPN of Cisco router.

```
Interface Tunnel1
Ip address 123.1.1.2 255.255.255.0        //Virtual IP address for GRE VPN
Tunnel source 77.211.24.2
Tunnel destination 202.96.1.102
Tunnel key 123456
!
```

The Cisco router is connected to the Internet and LAN side is connected to its FastEthernet0/1. The Crypto map must be applied to the WAN interface. And enable NAT feature on both Ethernet interface.

```
interface FastEthernet0/0
  ip address 77.211.24.2 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  duplex auto
  speed auto
!
interface FastEthernet0/1
ip address 192.168.1.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly
  duplex auto
  speed auto
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
!
```

```
ip nat inside source list 100 interface FastEthernet0/0 overload
```

The following entry configure the default gateway and remote GRE subnet for Cisco router.

```
ip route 0.0.0.0 0.0.0.0 77.211.24.1
ip route 192.168.0.0 255.255.255.0 Tunnel1        // Set data flow into GRE tunnel
```

Save the configuration for Cisco router.

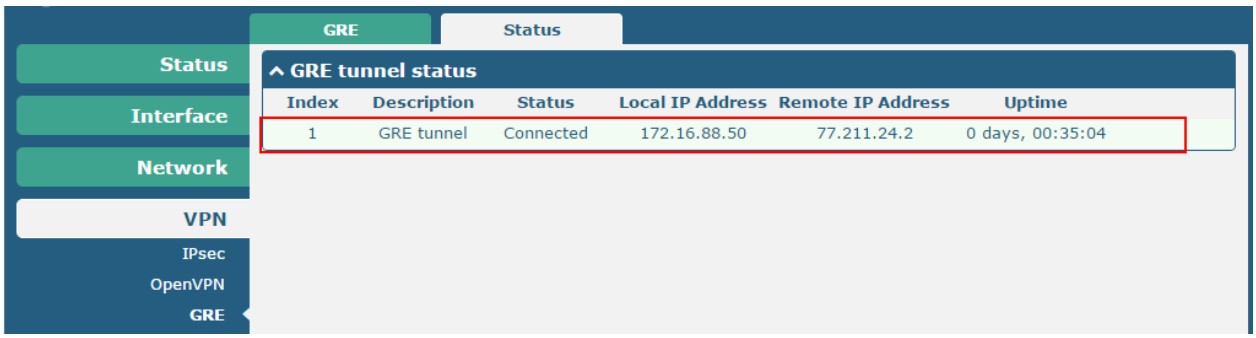
```
copy running-config startup-config
```

Chapter 4 Testing

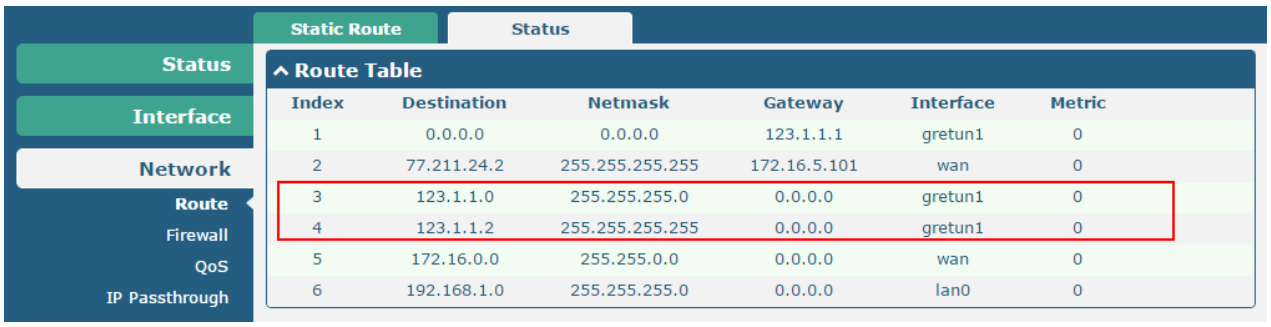
4.1 VPN Status and Communication of R2000

1. Browse to **VPN > GRE > Status**.

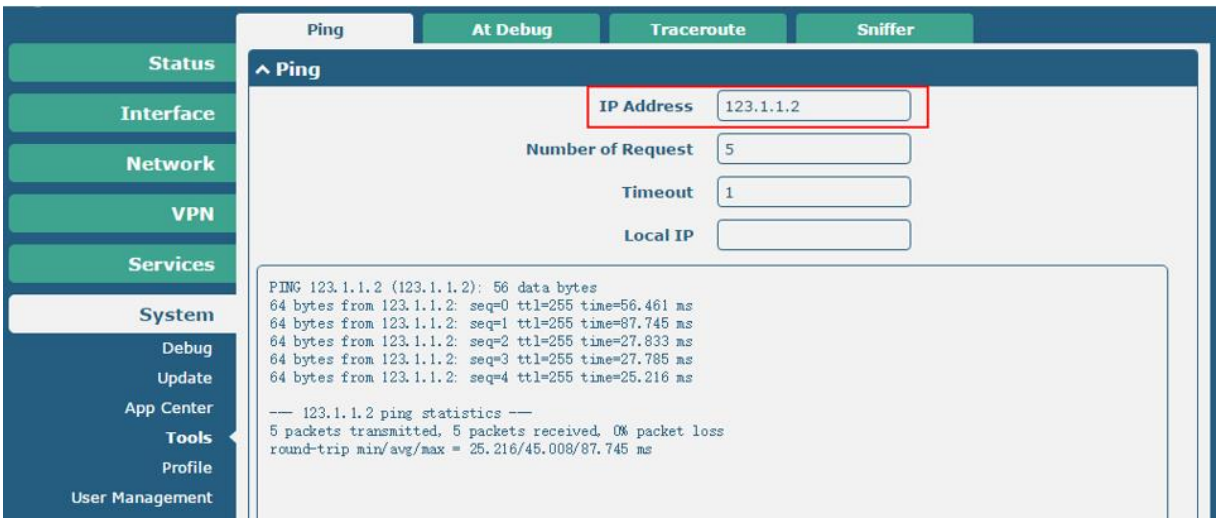
- Check whether R2000 has connected to the GRE VPN.

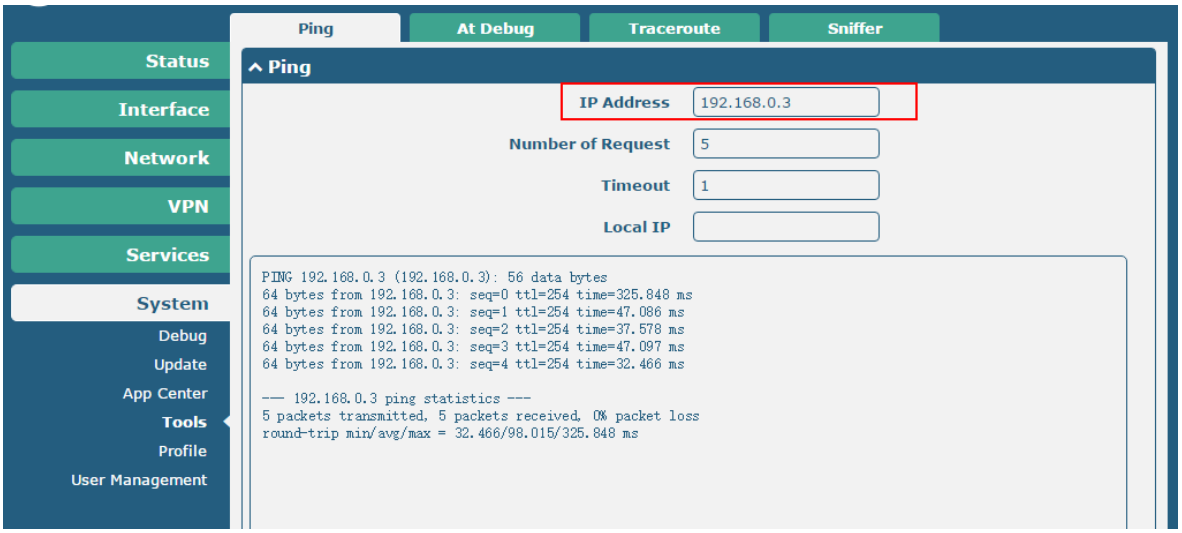


- Browse to **Network > Route > Status**, and check the virtual tunnel on Route table.



- Browse to **System > Tools > Ping**.
  Ping the virtual IP of GRE VPN and get ICMP reply from remote end.





4.2 VPN Status and Communication of Cisco

1. Run the CLI and type “show ip route” command to check the route-table in Cisco router.

```
cisco2811#sho ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 77.211.24.1 to network 0.0.0.0

     77.0.0.0/24 is subnetted, 1 subnets
C       77.211.24.0 is directly connected, FastEthernet0/0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
     123.0.0.0/24 is subnetted, 1 subnets
C       123.1.1.0 is directly connected, Tunnel1
S    192.168.1.0/24 is directly connected, Tunnel1
S*   0.0.0.0/0 [1/0] via 77.211.24.1
cisco2811#
```

2. Ping the virtual IP of GRE VPN and LAN IP address behind R2000, and get ICMP reply from remote end.

```
cisco2811#ping 123.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/66/68 ms
cisco2811#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/64 ms
cisco2811#
```

4.3 Event/Log

Event/Log shows the running process and the status of R2000. Only the information that specifically relate to the configuration above will be explained below.