Application Note

PPTP Client with Cisco Router

Version:	**v.1.0.0**
Date:	**2017-03-10**
Status:	**Confidential**
Doc ID:	**RT_AN013_ROS_PPTP Client with Cisco Router_v.1.0.0**
Author:	**Singson Chen**

www.robustel.com

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.

PPTP is one of VPN supporting multiprotocol network technology. It can use password authentication protocol (PAP) and extensible authentication protocol (EAP) to enhance the network security. Users can dial into the ISP, by directly connecting the Internet or other networks to visit the enterprise private network safely.

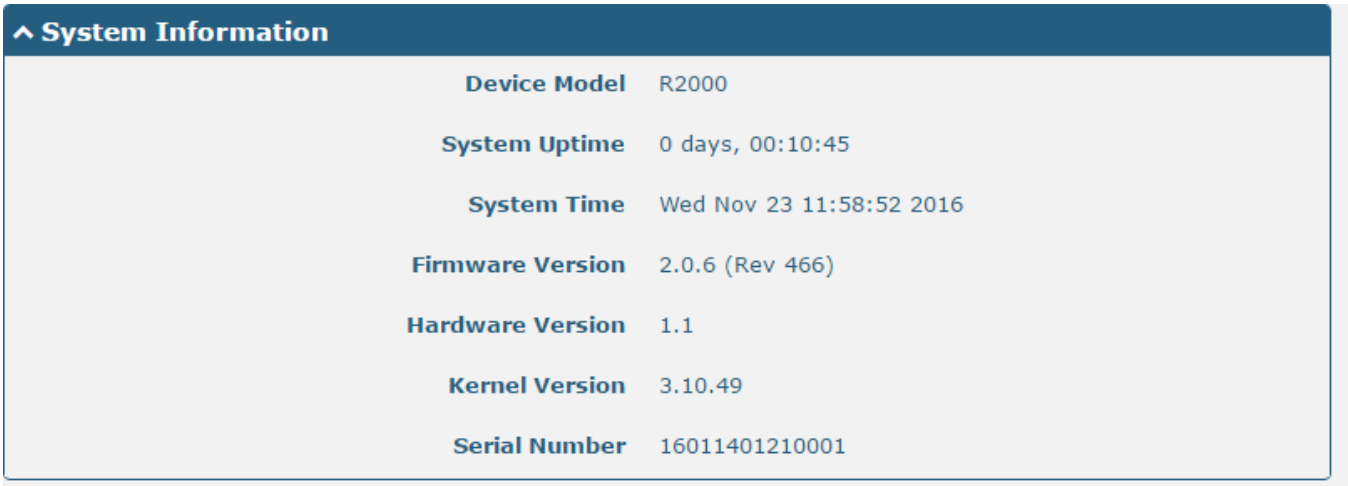
This application note has been written for customer with a good understanding of Robustel products and a basic experience of VPN. It shows customer how to configure and test the PPTP VPN between a R2000 router and a Cisco router through the cellular network.

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 PPTP VPN have been fully tested. 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 cellular WAN port of R2000 can be dynamic or static, and its IP address can be public or private with NAT. The R2000 working with a dynamic private IP address still could work for PPTP client.

It must assign a public IP address to the WAN port of the central Cisco router. This public IP address can be dynamic or static. If the central Cisco router working with a dynamic public IP address, a DNS service must be used to park dynamic public IP address to a static domains.

1.3 Rectifications

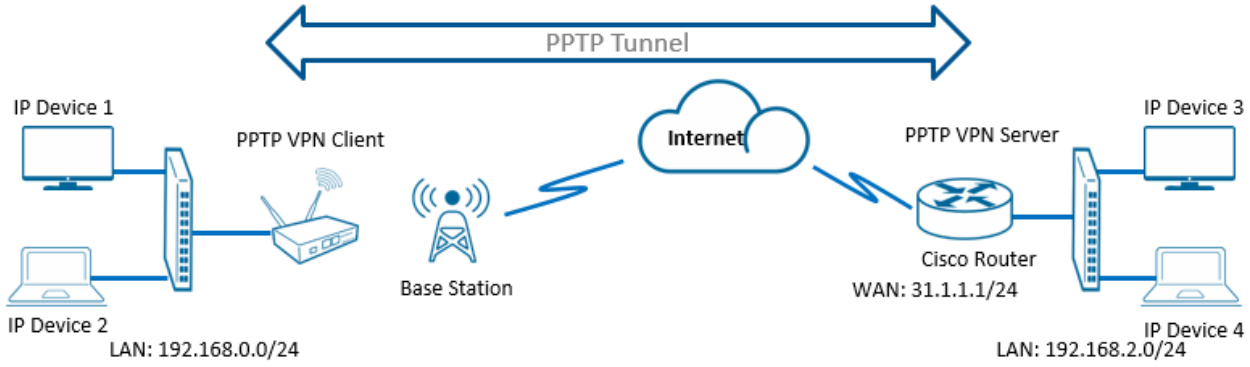
Requests for corrections or rectifications to this application note will be appreciated, and if there are any request for new application notes please email to: support@robustel.com.

1.4 Version

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

Release Date	Doc Version	Change Description
2017-03-10	v.1.0.0	Initial Release

Chapter 2 Topology



1. The Cisco Router runs as a border router in enterprise which has a fixed public IP address or a domain name.
2. The GoRugged R2000 works on wireless network with any kind of IP which can access Internet.
3. PPTP VPN will be established between the central Cisco Router and the GoRugged R2000.

Chapter 3 Configuration

3.1 Cisco Configuration

Enter the configuration mode and check the IOS version of 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 following entries set the host name of the Cisco router.

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

The following vpdn entries show the feature on Cisco Router, which using dial-in policy for PPTP server and encapsulation with PPTP protocol. Invoke virtual-temp 1 as PPTP server’s interface.

```
vpdn enable
vpdn-group PPTP
   accept-dialin
   protocol pptp
   virtual-temp 1
```

The following entry configures for connection authentication.

```
username admin123 password 0 admin123
```

The following entry defines the ip pool for PPTP subnet.

```
ip local pool robustel 100.1.1.100 100.1.1.200
```

The following entries define the virtual-template 1 interface, including the IP address, authentication mode and ip pool for PPTP subnet.

```
int virtual-template 1
  ip address 100.1.1.1 255.255.255.0
  peer default ip address pool robustel
  ppp authentication pap
```

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 interfaces.

```
interface FastEthernet0/0
ip address 31.1.1.1 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  duplex auto
  speed auto
!
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly
  duplex auto
  speed auto
!
access-list 100 permit ip 192.168.2.0 0.0.0.255 any
!
ip nat inside source list 100 interface FastEthernet0/0 overload
```

The following entry configures the default gateway for Cisco router.

```
ip route 0.0.0.0 0.0.0.0 31.1.1.3
```

Set the LAN IP of R2000 into the PPTP tunnel.

```
ip route 192.168.0.0 255.255.255.0 100.1.1.100
```

Save the configuration for Cisco router.

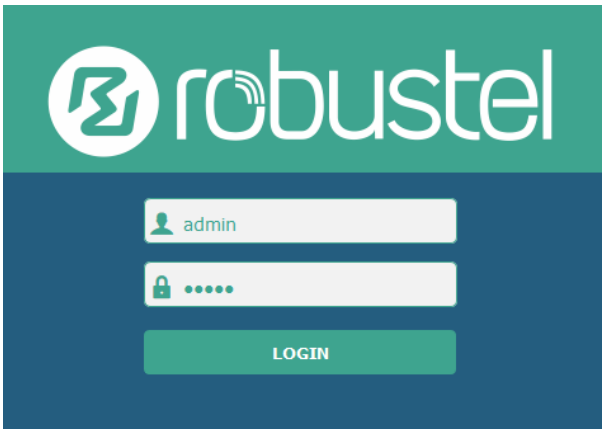
```
copy running-config startup-config
```

3.2 R2000 Configuration

3.2.1 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 card into the router
- Connect the power supply correctly
- Log in the Web GUI of the router

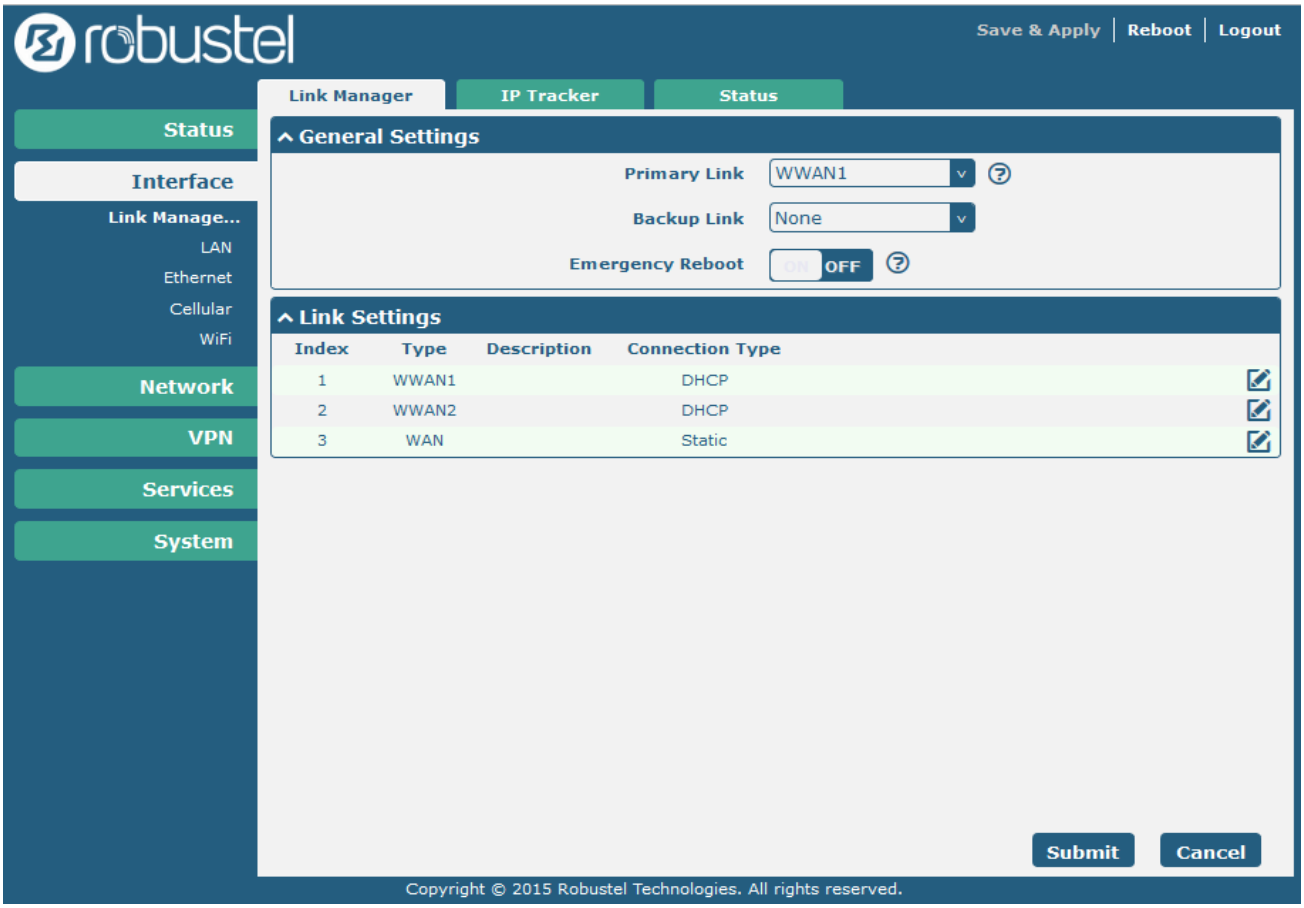


You need to know the following factory settings before you have logged in the Web GUI.

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".

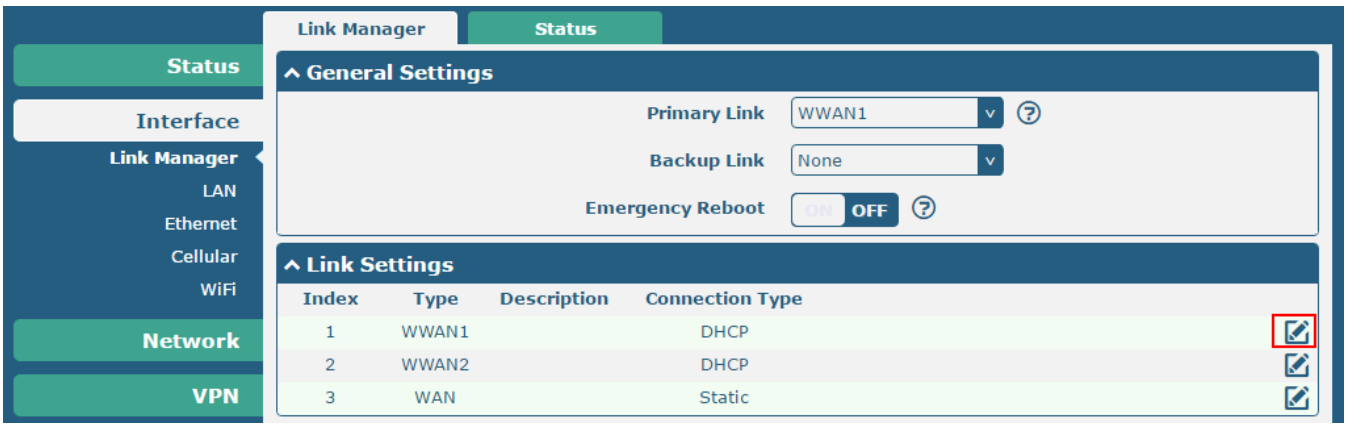


Item	Description	Setting
Primary Link	Select “WWAN1”, “WWAN2” or “WAN” as the primary connecting interface.	WWAN1

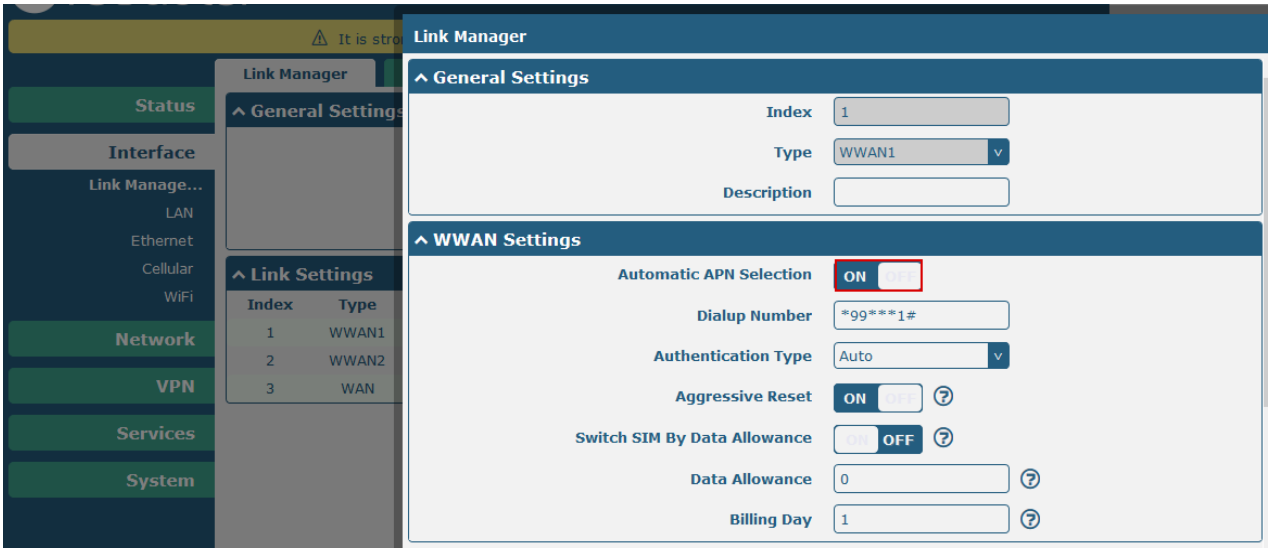
3.2.2 Configure Cellular WAN

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”.

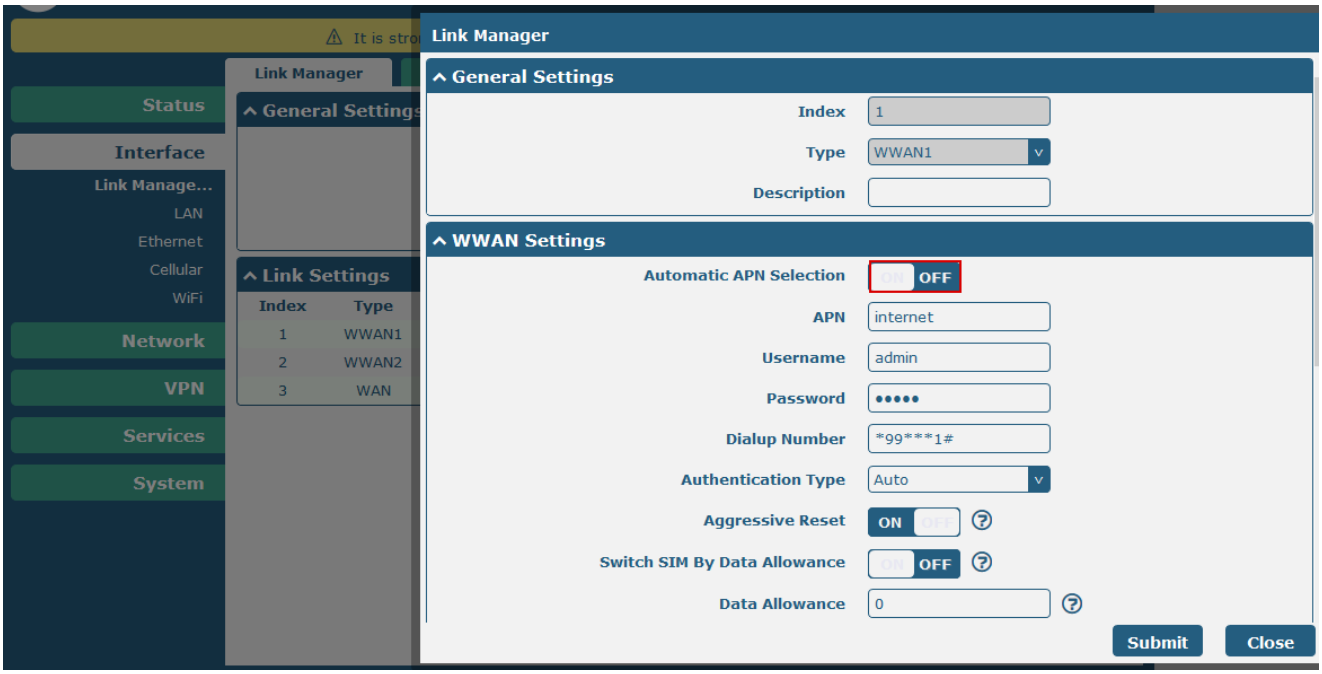


2. The window is displayed as below when enabling the “Automatic APN Selection” option.

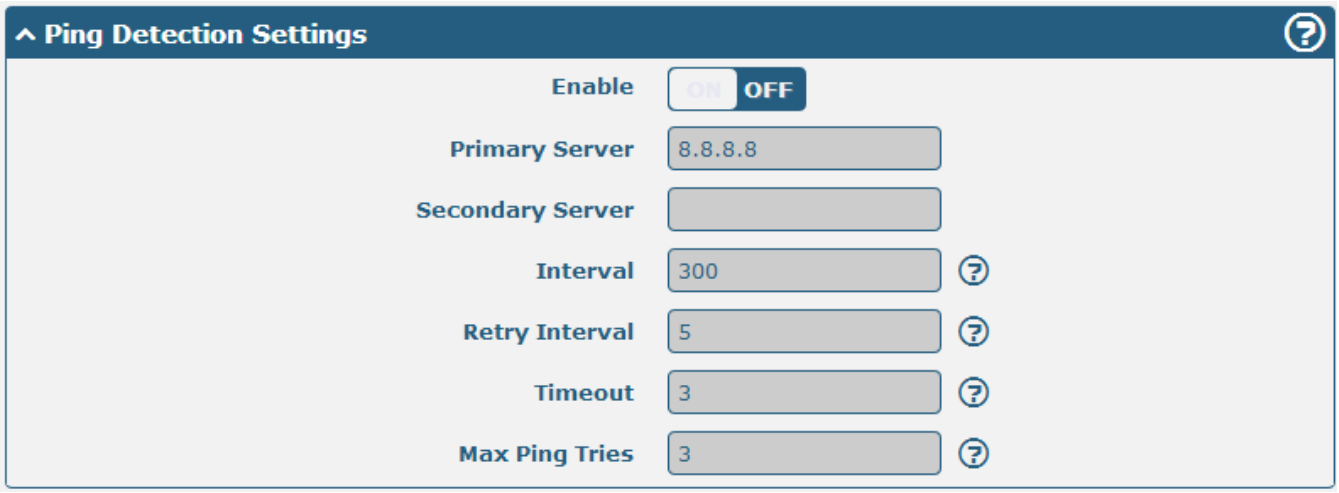


Item	Description	Setting
Dialup Number	Set the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Data Allowance	Set the monthly data traffic limitation.	0
Billing Day	Specify the monthly billing day, and the data traffic statistics will be recalculated from this day.	1

3. 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



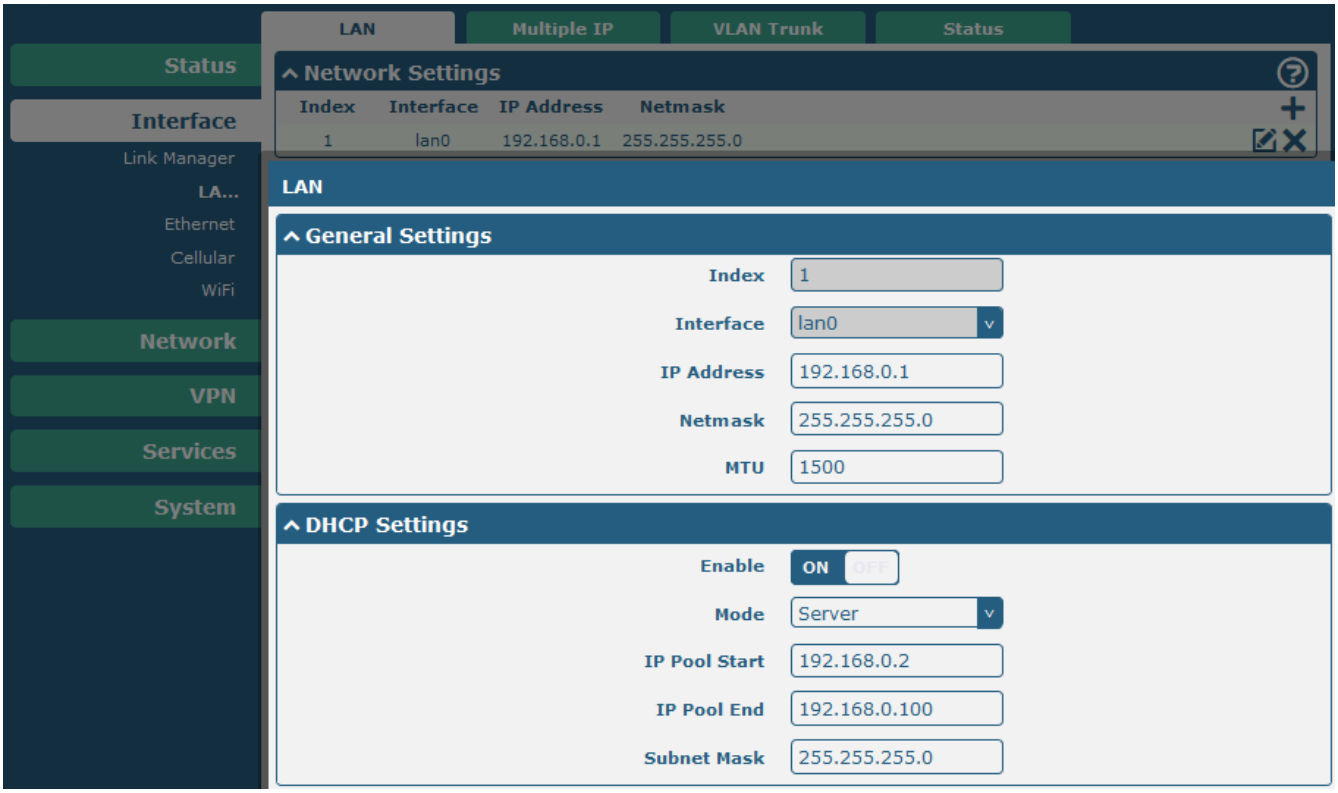
Item	Description	Setting
Enable	Click the toggle button to enable the ping detection, a keepalive policy of R2000 router.	OFF
Primary Server	Router will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain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

	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

3.2.3 Configure IP Address of LAN

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

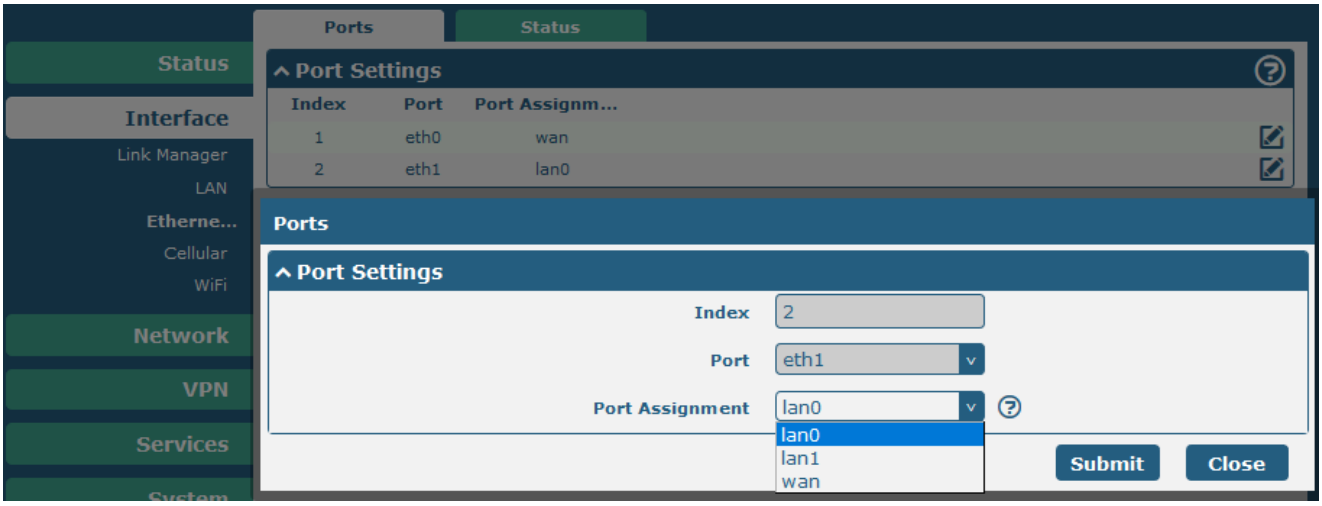
- Click the edit button of lan0.
- Set its IP address and Netmask, and the parameters in the “DHCP Settings” window are set accordingly.
- Click “Submit”.
- Click “Save & Apply”.



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”.



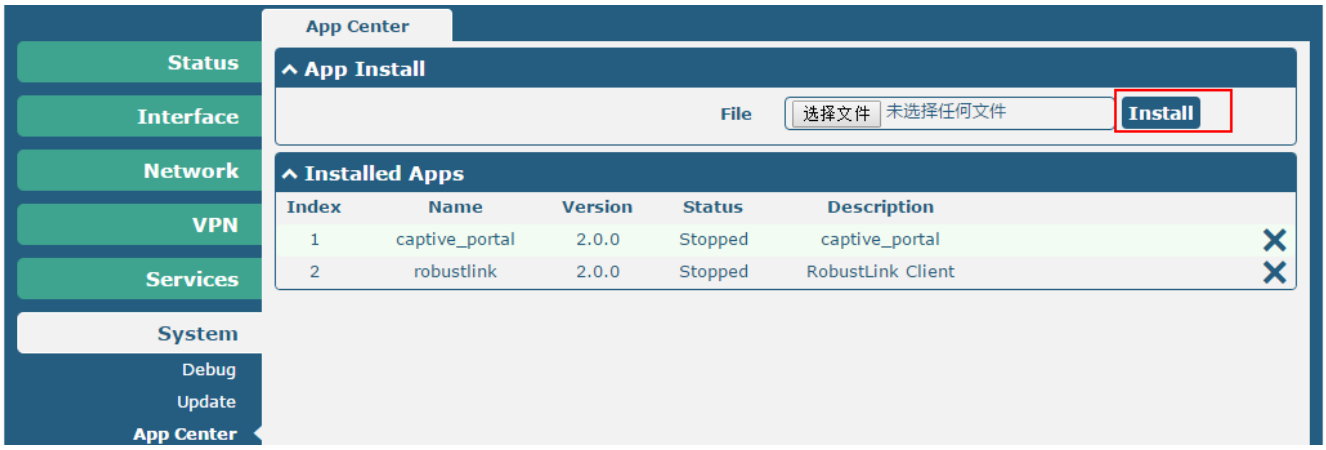
3.2.4 Configure PPTP Client

This section allows you to set the related parameters of PPTP Client.

1. PPTP needs to be installed first in the APP Center since PPTP is not the default setting in the ROS. Kindly contact us when you need this function.

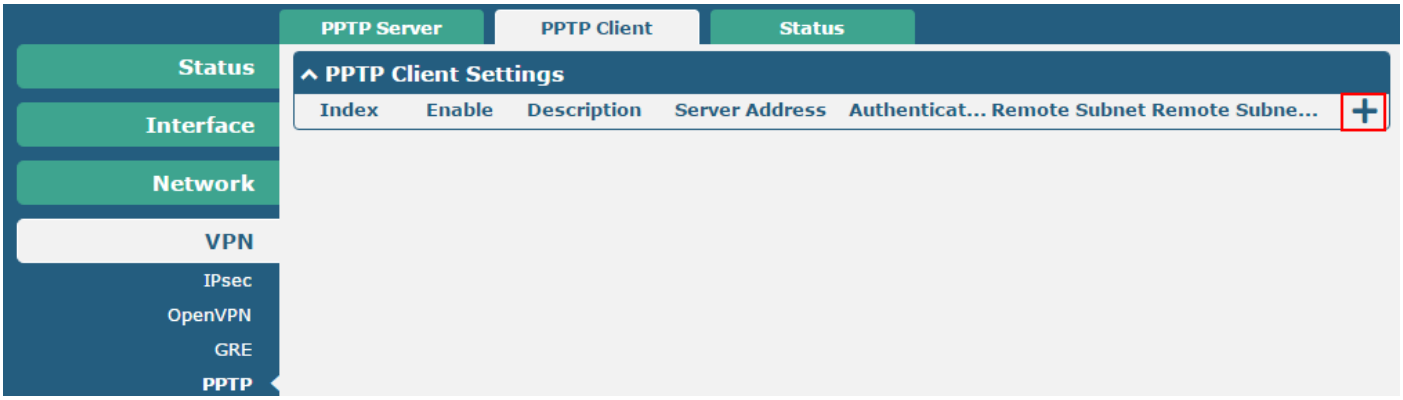
- APP:

- Path of installation:

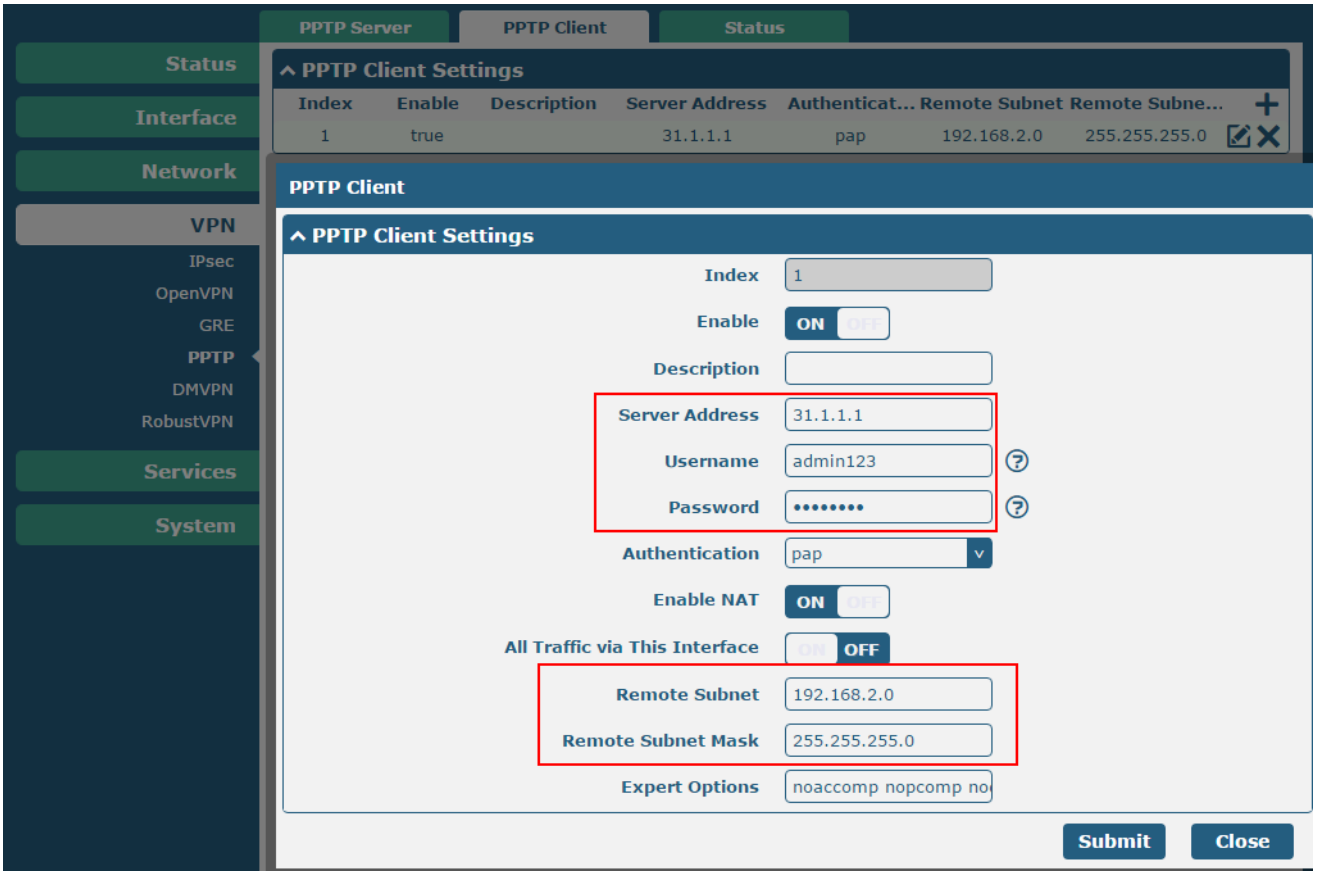


- Installed:

2. Browse to **VPN > PPTP**, and add the PPTP client.



3. Configure the related parameters to match the PPTP server, and click **Submit > Save & Apply**.



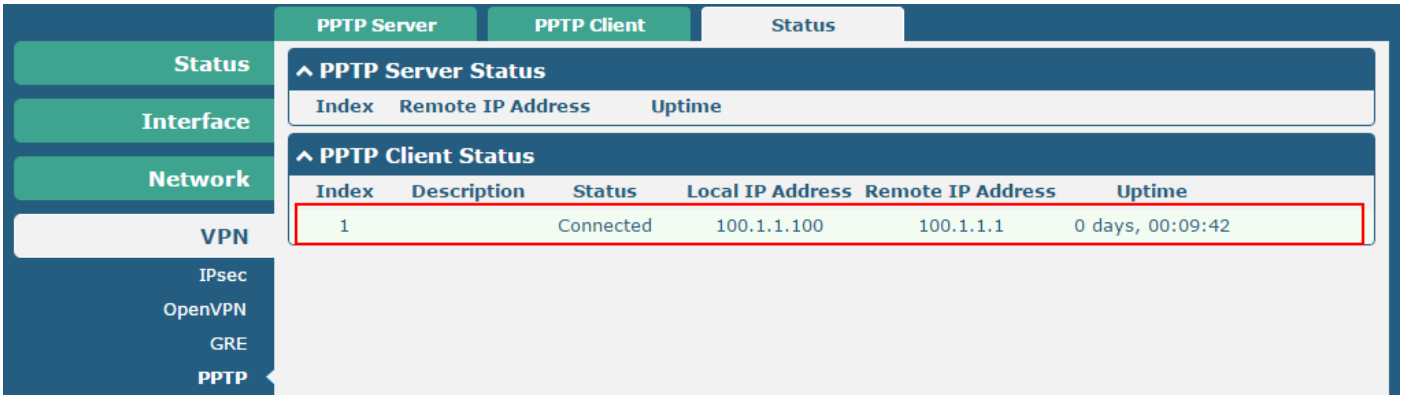
PPTP Client		
Item	Description	Default
Enable	Click the toggle button to enable the PPTP Client option.	Null
Server Address	Enter the public IP or domain name of your PPTP server.	Null
Username	Enter the username provided by your PPTP server.	Null
Password	Enter the password provided by your PPTP server.	Null
Authentication	Select from “Auto”, “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. You need to select the corresponding authentication method based on the server’s authentication method. When the “Auto” selected, the router will auto select the correct method based on server’s method.	Auto
Enable NAT	Click the toggle button to enable NAT feature of PPTP. The source IP address of host Behind R2000 will be disguised before accessing the remote PPTP server.	OFF
All traffic via this interface	Click the toggle button to enable this option. When enabled, all data traffic will be sent via PPTP tunnel.	OFF
Remote Subnet	Enter the remote peer’s private IP address or the remote subnet’s gateways address.	Null
Remote Subnet Mask	Enter the subnet mask of the remote peer.	Null
Expert Options	Enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp

Chapter 4 Testing

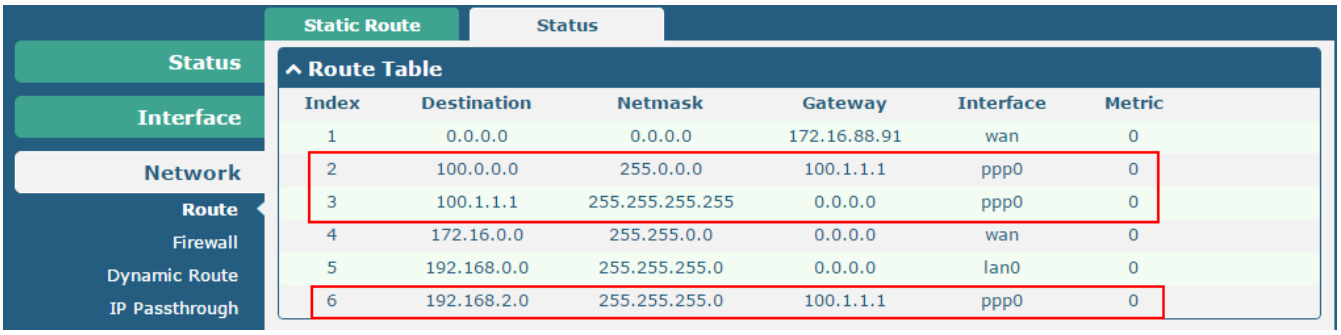
4.1 VPN Status and Communication of R2000

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

2. Check whether R2000 has established a PPTP VPN tunnel with Server side.

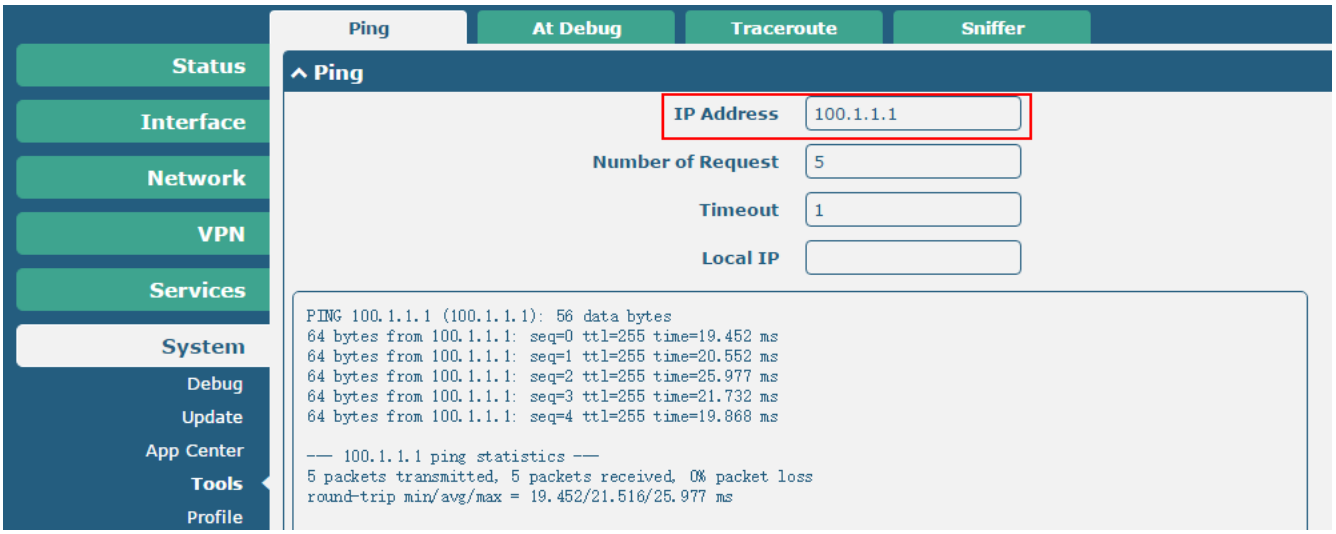


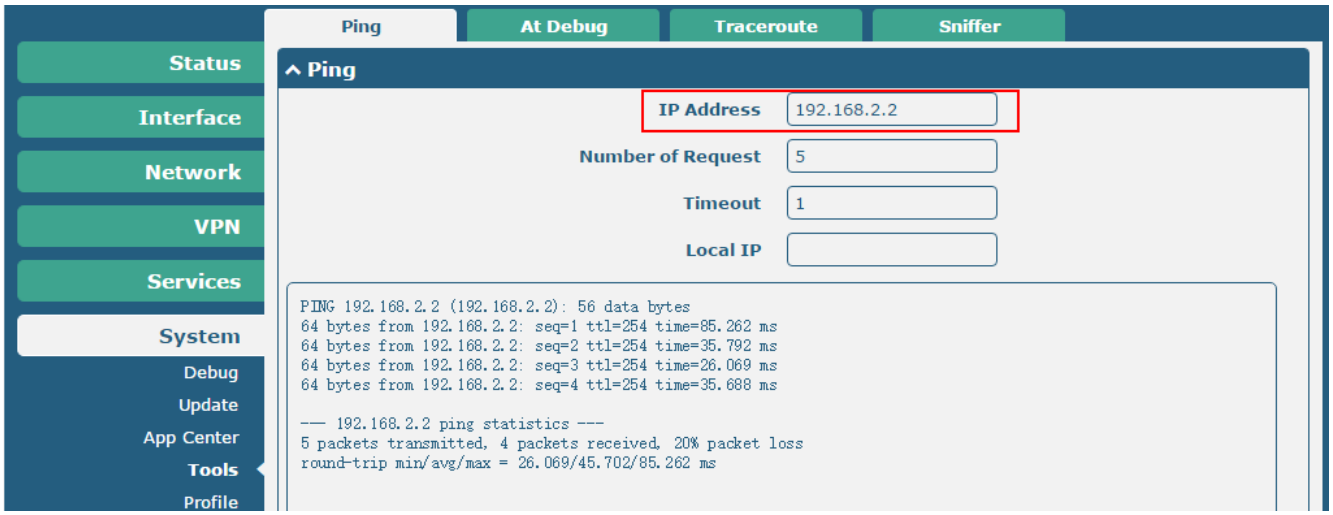
3. Browse to **Network > Route > Status**, and check the virtual tunnel on Route table.



4. Browse to **System > Tools > Ping**.

   Ping the virtual IP of PPTP VPN Server and LAN IP address behind Server, and get ICMP reply from remote end.





4.2 VPN Status and Communication of Cisco

1. Input “show ip route” command to check the route-table in Cisco router.

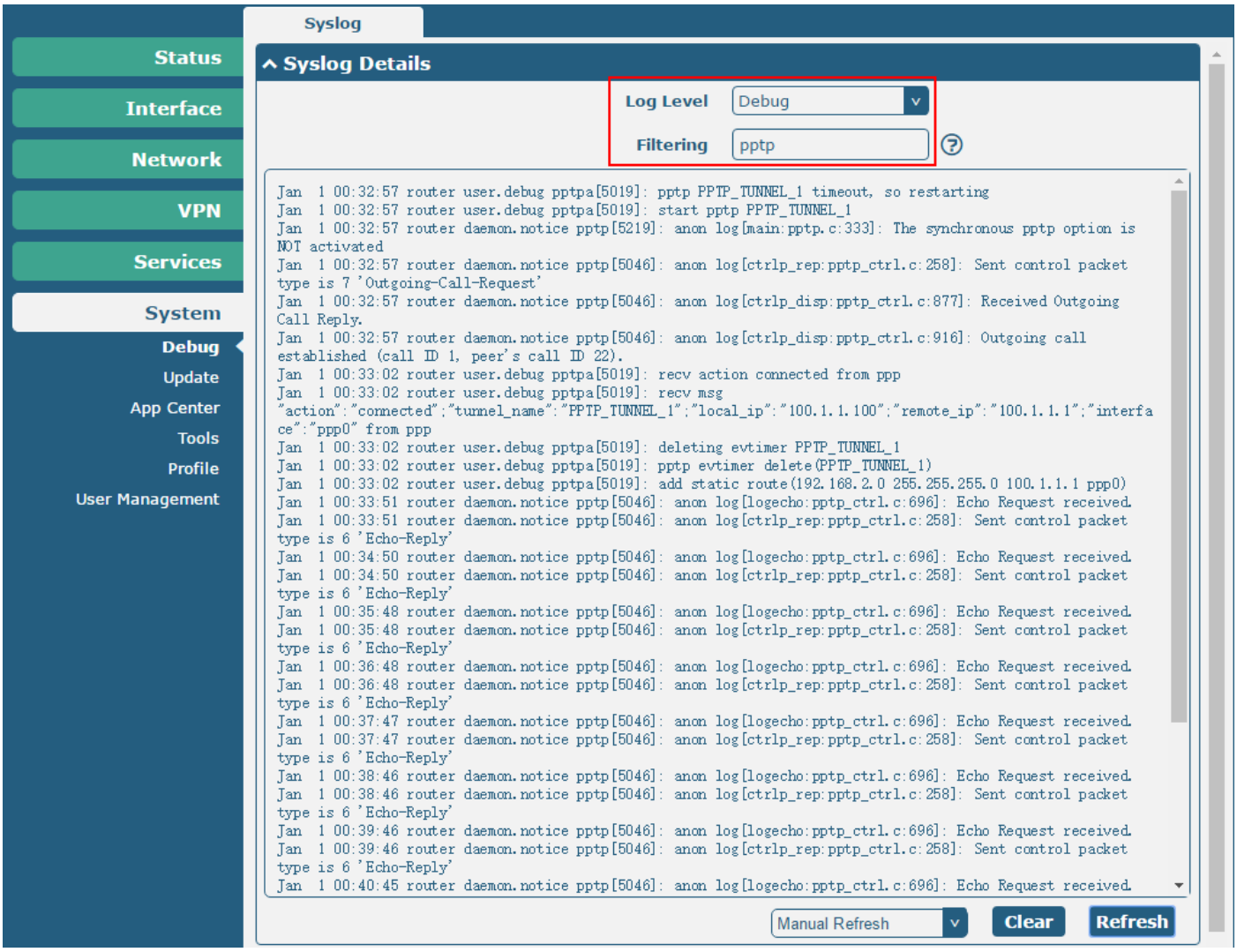
```
cisco2811#sho ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i -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

Gateway of last resort is 31.1.1.3 to network 0.0.0.0

     100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       100.1.1.100/32 is directly connected, Virtual-Access3
C       100.1.1.0/24 is directly connected, Virtual-Access3
S    192.168.0.0/24 [1/0] via 100.1.1.100
C    192.168.2.0/24 is directly connected, FastEthernet0/1
     31.0.0.0/24 is subnetted, 1 subnets
C       31.1.1.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 31.1.1.3
```

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

```
cisco2811#ping 100.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.1.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/23/32 ms
cisco2811#


cisco2811#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/28/36 ms
```

4.3 Event/Log

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



……

Jan 1 00:32:57 router daemon.notice pppd[5215]: pppd 2.4.7 started by root, uid 0

Jan 1 00:32:57 router daemon.info pppd[5215]: Using interface ppp0

Jan 1 00:32:57 router daemon.notice pppd[5215]: Connect: ppp0 <--> /dev/pts/1

Jan 1 00:32:57 router daemon.notice pptp[5219]: anon log[main:pptp.c:333]: The synchronous pptp option is NOT activated

Jan 1 00:32:57 router daemon.notice pptp[5046]: anon log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 7 'Outgoing-Call-Request'

Jan 1 00:32:57 router daemon.notice pptp[5046]: anon log[ctrlp_disp:pptp_ctrl.c:877]: Received Outgoing Call Reply.

Jan 1 00:32:57 router daemon.notice pptp[5046]: anon log[ctrlp_disp:pptp_ctrl.c:916]: Outgoing call established (call ID 1, peer's call ID 22).

Jan 1 00:32:58 router daemon.warn pppd[5215]: Warning - secret file /etc/ppp/pap-secrets has world and/or group

```
access
Jan    1 00:32:58 router daemon.warn pppd[5215]: Warning - secret file /etc/ppp/pap-secrets has world and/or group
access
Jan    1 00:33:01 router daemon.notice pppd[5215]: PAP authentication succeeded
Jan    1 00:33:02 router daemon.notice pppd[5215]: local    IP address 100.1.1.100
Jan    1 00:33:02 router daemon.notice pppd[5215]: remote IP address 100.1.1.1
Jan    1 00:33:02 router daemon.info pppd[5215]: CCP terminated by peer
Jan    1 00:33:51 router daemon.notice pptp[5046]: anon log[logecho:pptp_ctrl.c:696]: Echo Request received.
Jan    1 00:33:51 router daemon.notice pptp[5046]: anon log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 6
'Echo-Reply'
Jan    1 00:34:50 router daemon.notice pptp[5046]: anon log[logecho:pptp_ctrl.c:696]: Echo Request received.
Jan    1 00:34:50 router daemon.notice pptp[5046]: anon log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 6
'Echo-Reply'
Jan    1 00:35:09 router user.notice ntpc_mgmt[1004]: ntp client starts to update
……
```