

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

Contents

Chapter 1	Introduction.....	2
1.1	Overview.....	2
1.2	Assumptions	2
1.3	Rectifications	3
1.4	Version	3
Chapter 2	Topology	4
Chapter 3	Configuration	5
3.1	Cisco Configuration.....	5
3.2	R2000 Configuration.....	7
3.2.1	Configure Link Manager	7
3.2.2	Configure Cellular WAN	8
3.2.3	Configure IP Address of LAN	11
3.2.4	Configure PPTP Client	12
Chapter 4	Testing.....	15
4.1	VPN Status and Communication of R2000	15
4.2	VPN Status and Communication of Cisco	17
4.3	Event/Log.....	18

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.

^ System Information	
Device Model	R2000
System Uptime	0 days, 00:10:45
System Time	Wed Nov 23 11:58:52 2016
Firmware Version	2.0.6 (Rev 466)
Hardware Version	1.1
Kernel Version	3.10.49
Serial Number	16011401210001

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

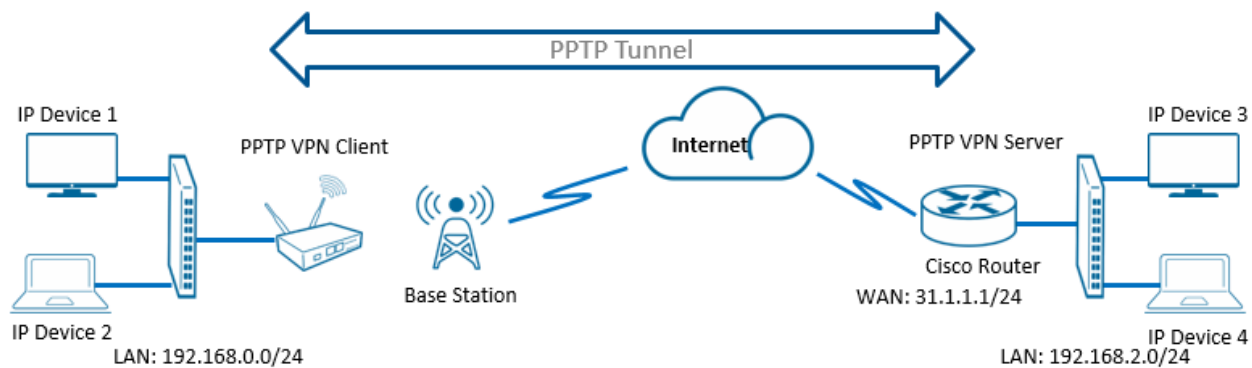
Requests for corrections or rectifications to this application note will be appreciated, and if there are any request for new application notes please email to: support@robustel.com.

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
```

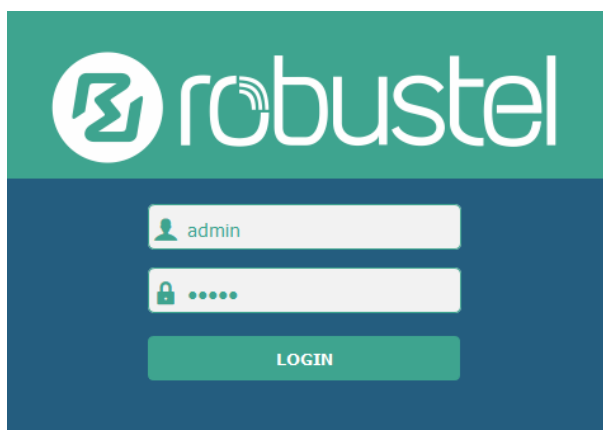
Save the configuration for Cisco router.

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

3.2 R2000 Configuration

3.2.1 Configure Link Manager

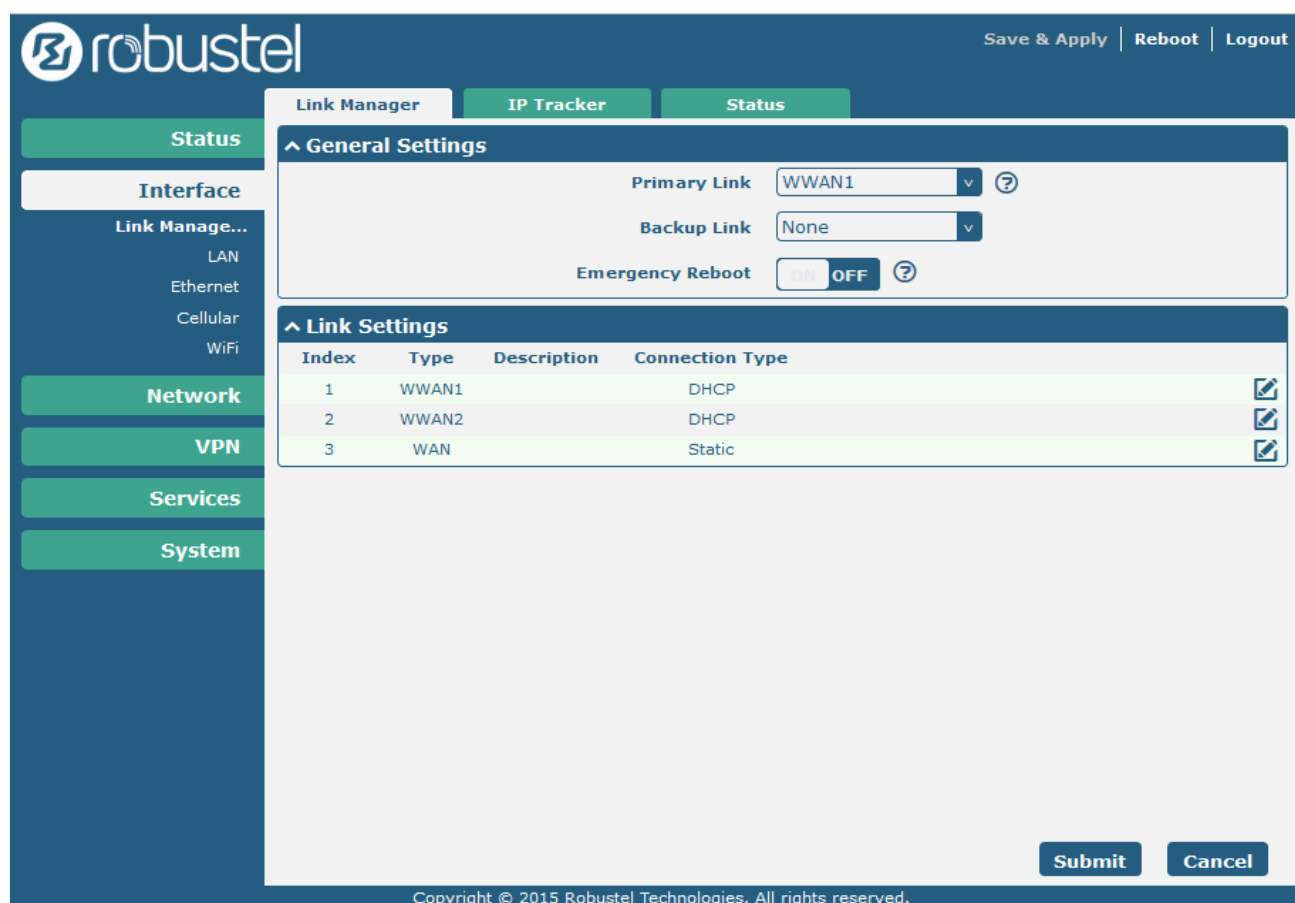
1. Follow these steps before configuring the router:
 - Attach the external antenna to the router's connector and twist tightly
 - Insert the SIM card into the router
 - Connect the power supply correctly
 - Log in the Web GUI of the router



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".



robustel

Save & Apply | Reboot | Logout

Link Manager IP Tracker Status

Status

Interface

Link Manage...

LAN

Ethernet

Cellular

WiFi

Network

VPN

Services

System

^ General Settings

Primary Link WWAN1 ?

Backup Link None

Emergency Reboot ON OFF ?

^ Link Settings

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

Submit Cancel

Copyright © 2015 Robustel Technologies. All rights reserved.

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

3.2.2 Configure Cellular WAN

- 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 screenshot shows the 'Link Manager' interface with the 'Status' tab selected. The left sidebar contains 'Status', 'Interface', 'Link Manager', 'Network', and 'VPN'. The 'Link Manager' section is expanded, showing 'LAN', 'Ethernet', 'Cellular', and 'WiFi'. The main content area has two sections: 'General Settings' and 'Link Settings'.

General Settings:

- Primary Link: WWAN1
- Backup Link: None
- Emergency Reboot: OFF

Link Settings:

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

Each row in the Link Settings table has a red square icon with a pencil, indicating an edit option.

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

The screenshot shows the 'Link Manager' interface with the 'Link Settings' tab selected for Index 1. The left sidebar is the same as the previous screenshot. The main content area has two sections: 'General Settings' and 'WWAN Settings'.

General Settings:

- Index: 1
- Type: WWAN1
- Description:

WWAN Settings:

- Automatic APN Selection: ON
- Dialup Number: *99***1#
- Authentication Type: Auto
- Aggressive Reset: OFF
- Switch SIM By Data Allowance: OFF
- Data Allowance: 0
- Billing Day: 1

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.

The screenshot shows the 'Link Manager' configuration window. On the left is a sidebar with navigation options: Status, Interface, Link Manager (selected), LAN, Ethernet, Cellular, WiFi, Network, VPN, Services, and System. The main area is titled 'Link Manager' and contains two sections: 'General Settings' and 'WWAN Settings'. In 'General Settings', 'Index' is 1, 'Type' is WWAN1, and 'Description' is empty. In 'WWAN Settings', 'Automatic APN Selection' is set to OFF (highlighted with a red box). Other settings include APN: internet, Username: admin, Password: masked with dots, Dialup Number: *99***1#, Authentication Type: Auto, Aggressive Reset: ON, Switch SIM By Data Allowance: OFF, and Data Allowance: 0. 'Submit' and 'Close' buttons are at the bottom right.

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

The screenshot shows the 'Ping Detection Settings' window. It has a title bar with a question mark icon. The 'Enable' toggle is set to OFF. Below are input fields for: Primary Server (8.8.8.8), Secondary Server (empty), Interval (300), Retry Interval (5), Timeout (3), and Max Ping Tries (3). Each of the last four fields has a help icon (question mark) to its right.

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

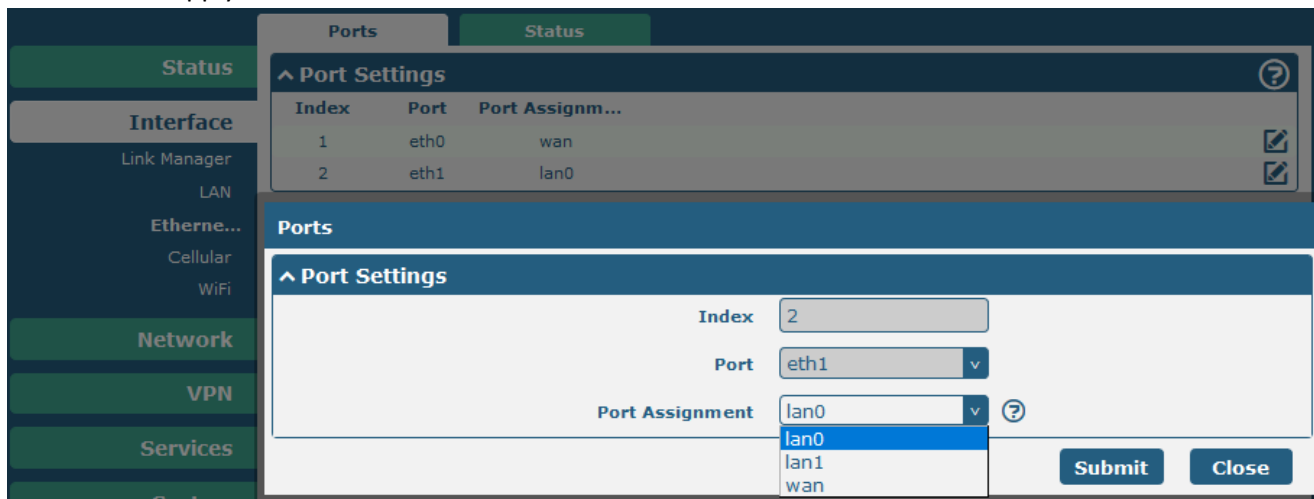
1. Browse to **Interface > LAN > LAN**.
 - Click the edit button of lan0.
 - Set its IP address and Netmask, and the parameters in the “DHCP Settings” window are set accordingly.
 - Click “Submit”.
 - Click “Save & Apply”.

The screenshot displays the MikroTik WinBox configuration page for the LAN interface. The left sidebar shows the navigation menu with 'Interface' selected. The main panel is titled 'LAN' and contains two sections: 'General Settings' and 'DHCP Settings'. In 'General Settings', the Index is 1, the Interface is lan0, the IP Address is 192.168.0.1, the Netmask is 255.255.255.0, and the MTU is 1500. In 'DHCP Settings', the Enable checkbox is checked (ON), the Mode is set to Server, the IP Pool Start is 192.168.0.2, the IP Pool End is 192.168.0.100, and the Subnet Mask is 255.255.255.0.

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:

 r2000-pptp-2.0.0.rpk

12/12/2016 4:23 PM RPK File

60 KB

- Path of installation:



- Installed:

The screenshot shows the 'App Center' interface. On the left is a sidebar with navigation options: Status, Interface, Network, VPN, Services, System, Debug, Update, App Center, and Tools. The 'App Center' option is selected. The main area is titled 'App Center' and contains two sections: 'App Install' and 'Installed Apps'. The 'App Install' section has a 'File' input field with a '选择文件' button and an 'Install' button. The 'Installed Apps' section contains a table with the following data:

Index	Name	Version	Status	Description	
1	robustvpn	test201..	Stopped	RobustVPN Client	✕
2	captive_portal	2.0.0	Stopped	captive_portal	✕
3	dmvpn	2.0.0	Stopped	DMVPN	✕
4	language_chinese	2.0.0	Stopped	Chinese language	✕
5	dynamic_route	test123..	Stopped	dynamic_route	✕
6	robustlink	2.0.0	Stopped	RobustLink Client	✕
7	pptp	2.0.0	Stopped	PPTP	✕

The row for 'pptp' (Index 7) is highlighted with a red box.

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

The screenshot shows the 'PPTP Client Settings' interface. The left sidebar has 'VPN' selected, and the 'PPTP' option is highlighted. The main area has three tabs: 'PPTP Server', 'PPTP Client', and 'Status'. The 'PPTP Client' tab is active. Below the tabs is a section titled 'PPTP Client Settings' containing a table with the following columns: Index, Enable, Description, Server Address, Authenticat..., Remote Subnet, and Remote Subne... A red box highlights the '+' button in the top right corner of the table.

Index	Enable	Description	Server Address	Authenticat...	Remote Subnet	Remote Subne...
+						

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

The screenshot shows the PPTP Client configuration page. On the left is a navigation menu with options: Status, Interface, Network, VPN (selected), Services, and System. Under VPN, there are sub-options: IPsec, OpenVPN, GRE, PPTP (selected), DMVPN, and RobustVPN. The main content area has tabs for PPTP Server, PPTP Client, and Status. The PPTP Client tab is active, showing a table of PPTP Client Settings. The table has columns: Index, Enable, Description, Server Address, Authentication, Remote Subnet, and Remote Subnet Mask. The first row is selected, showing Index 1, Enable true, Description, Server Address 31.1.1.1, Authentication pap, Remote Subnet 192.168.2.0, and Remote Subnet Mask 255.255.255.0. Below the table, the configuration fields for the selected client are shown. A red box highlights the following fields: Server Address (31.1.1.1), Username (admin123), Password (masked with dots), and Remote Subnet (192.168.2.0) and Remote Subnet Mask (255.255.255.0). Other fields include Index (1), Enable (ON), Description, Authentication (pap), Enable NAT (ON), All Traffic via This Interface (OFF), and Expert Options (noaccomp nopcomp no). At the bottom right are buttons for Submit and Close.

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.

Status

Interface

Network

VPN

IPsec

OpenVPN

GRE

PPTP

PPTP Server

PPTP Client

Status

^ PPTP Server Status

Index	Remote IP Address	Uptime
-------	-------------------	--------

^ PPTP Client Status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime
1		Connected	100.1.1.100	100.1.1.1	0 days, 00:09:42

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

	Static Route	Status				
Status	^ Route Table					
Interface						
Network						
Route						
Firewall						
Dynamic Route						
IP Passthrough						
	Index	Destination	Netmask	Gateway	Interface	Metric
	1	0.0.0.0	0.0.0.0	172.16.88.91	wan	0
	2	100.0.0.0	255.0.0.0	100.1.1.1	ppp0	0
	3	100.1.1.1	255.255.255.255	0.0.0.0	ppp0	0
	4	172.16.0.0	255.255.0.0	0.0.0.0	wan	0
	5	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0
	6	192.168.2.0	255.255.255.0	100.1.1.1	ppp0	0

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.

The screenshot shows the 'Ping' tool interface. The 'IP Address' field is set to '100.1.1.1'. The 'Number of Request' is set to '5', and the 'Timeout' is set to '1'. The 'Local IP' field is empty. The output shows a successful ping to 100.1.1.1 with 5 data bytes and a round-trip time of approximately 19.452 ms. The statistics show 5 packets transmitted, 5 packets received, and 0% packet loss.

Field	Value
IP Address	100.1.1.1
Number of Request	5
Timeout	1
Local IP	

```
PING 100.1.1.1 (100.1.1.1): 56 data bytes
64 bytes from 100.1.1.1: seq=0 ttl=255 time=19.452 ms
64 bytes from 100.1.1.1: seq=1 ttl=255 time=20.552 ms
64 bytes from 100.1.1.1: seq=2 ttl=255 time=25.977 ms
64 bytes from 100.1.1.1: seq=3 ttl=255 time=21.732 ms
64 bytes from 100.1.1.1: seq=4 ttl=255 time=19.868 ms

--- 100.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 19.452/21.516/25.977 ms
```

The screenshot shows the 'Ping' tool interface. The 'IP Address' field is set to '192.168.2.2'. The 'Number of Request' is set to '5', and the 'Timeout' is set to '1'. The 'Local IP' field is empty. The output shows a failed ping to 192.168.2.2 with 56 data bytes and a round-trip time of approximately 26.069 ms. The statistics show 5 packets transmitted, 4 packets received, and 20% packet loss.

Field	Value
IP Address	192.168.2.2
Number of Request	5
Timeout	1
Local IP	

```
PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: seq=1 ttl=254 time=85.262 ms
64 bytes from 192.168.2.2: seq=2 ttl=254 time=35.792 ms
64 bytes from 192.168.2.2: seq=3 ttl=254 time=26.069 ms
64 bytes from 192.168.2.2: seq=4 ttl=254 time=35.688 ms

--- 192.168.2.2 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 26.069/45.702/85.262 ms
```

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 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 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
C       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.

The screenshot displays the Syslog interface with the following details:

- Log Level:** Debug
- Filtering:** pptp
- Log Entries:**

```

Jan 1 00:32:57 router user.debug pptpa[5019]: pptp PPTP_TUNNEL_1 timeout, so restarting
Jan 1 00:32:57 router user.debug pptpa[5019]: start pptp PPTP_TUNNEL_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 00:33:02 router user.debug pptpa[5019]: rcv action connected from ppp
Jan 1 00:33:02 router user.debug pptpa[5019]: rcv msg "action": "connected"; "tunnel_name": "PPTP_TUNNEL_1"; "local_ip": "100.1.1.100"; "remote_ip": "100.1.1.1"; "interface": "ppp0" from ppp
Jan 1 00:33:02 router user.debug pptpa[5019]: deleting evtimer PPTP_TUNNEL_1
Jan 1 00:33:02 router user.debug pptpa[5019]: pptp evtimer delete (PPTP_TUNNEL_1)
Jan 1 00:33:02 router user.debug pptpa[5019]: add static route (192.168.2.0 255.255.255.0 100.1.1.1 ppp0)
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 00:35:48 router daemon.notice pptp[5046]: anon log[logecho:pptp_ctrl.c:696]: Echo Request received.
Jan 1 00:35:48 router daemon.notice pptp[5046]: anon log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 6 'Echo-Reply'
Jan 1 00:36:48 router daemon.notice pptp[5046]: anon log[logecho:pptp_ctrl.c:696]: Echo Request received.
Jan 1 00:36:48 router daemon.notice pptp[5046]: anon log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 6 'Echo-Reply'
Jan 1 00:37:47 router daemon.notice pptp[5046]: anon log[logecho:pptp_ctrl.c:696]: Echo Request received.
Jan 1 00:37:47 router daemon.notice pptp[5046]: anon log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 6 'Echo-Reply'
Jan 1 00:38:46 router daemon.notice pptp[5046]: anon log[logecho:pptp_ctrl.c:696]: Echo Request received.
Jan 1 00:38:46 router daemon.notice pptp[5046]: anon log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 6 'Echo-Reply'
Jan 1 00:39:46 router daemon.notice pptp[5046]: anon log[logecho:pptp_ctrl.c:696]: Echo Request received.
Jan 1 00:39:46 router daemon.notice pptp[5046]: anon log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 6 'Echo-Reply'
Jan 1 00:40:45 router daemon.notice pptp[5046]: anon log[logecho:pptp_ctrl.c:696]: Echo Request received.

```

```

.....
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

.....