Application Note

IPsec VPN Between RobustOS

Document Type:	**Application Note**
Date:	**2016-11-30**
Status:	**Confidential**
Doc ID:	**RT_AN002_ROS_IPsec VPN Between RobustOS_v.1.0.0**
Author:	**Tim Zhao**

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. The configuration web interface of the ROS is a little different from the existing old platform of R3000 series.

VPN (Virtual Private Network) is a technology establishing private network tunnels on the public network. IPsec VPN is a kind of LAN to LAN communication or remote access VPN technology with the IPsec protocol, offering end-to-end encryption and authentication service for public and private network.

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 the IPsec VPN between two local area networks, with both sides using Robustel R2000s.

This application note applies to the ROS firmware of R2000 and R3000. However, the followings will take R2000 as an example

1.2 Assumptions

The features of IPsec 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: R2000 standard industrial cellular VPN router
- Firmware Version: R2000_ROS_V2.0.6.fs
- 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.

  R2000_Remote works with wired network (static public IP address) and **R2000_Local** connects to cellular network (i.e. GPRS, EDGE, UMTS, HSDPA or HSUPA). **R2000_Local** connecting to cellular networks is usually allocated a dynamic private IP address, in this case, **R2000_Local** need to be assigned a public IP address from ISP carrier. This is because the IPsec initiator always needs to know where to connect, and the ROS only support to specify remote IPsec Gateway in IPsec common part.

  The IPsec initiator and IPsec responder router must be assigned a public IP address to their WAN interfaces. The IP address can be dynamic or static. If R2000 working with dynamic public IP address, a DNS service must be used to park dynamic public IP address to static domain.

1.3 Rectifications

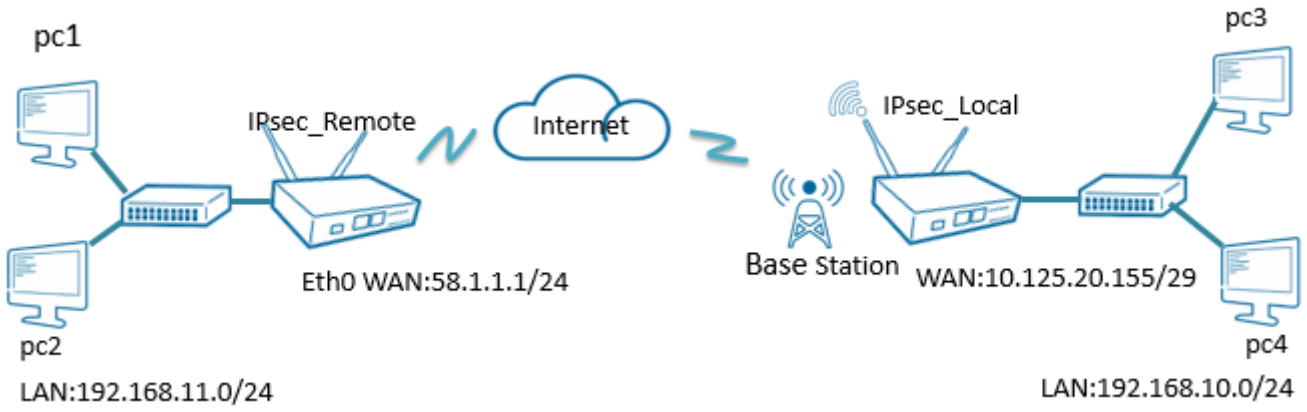
Appreciate for corrections or rectifications to this application note, and if there are any request for new application notes please email to: support@robustel.com.

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
2016-11-30	v.1.0.0	Initial Release

Chapter 2 Topology

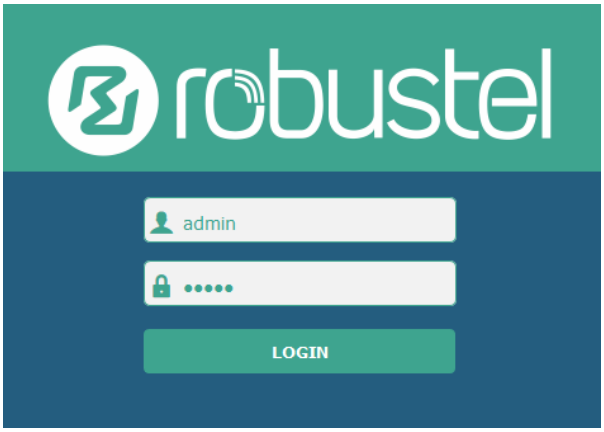


1. R2000_Remote runs as central router which has a static public IP address or a domain name.
2. R2000_Local works on cellular network with any kind of IP which can access the Internet and communicate with central R2000_Remote successfully.
3. IPsec VPN will be established between R2000_Remote and R2000_Local, and the interesting traffic from R2000_Remote side (192.168.11.0/24) to R2000_Local side (192.168.10.0/24) will be encrypted and vice versa.

Chapter 3 Configuration

3.1 R2000_ROS (IPsec Remote) Configuration

Connect the power supply, access the Internet via eth0, and log-in the Web GUI of R2000.



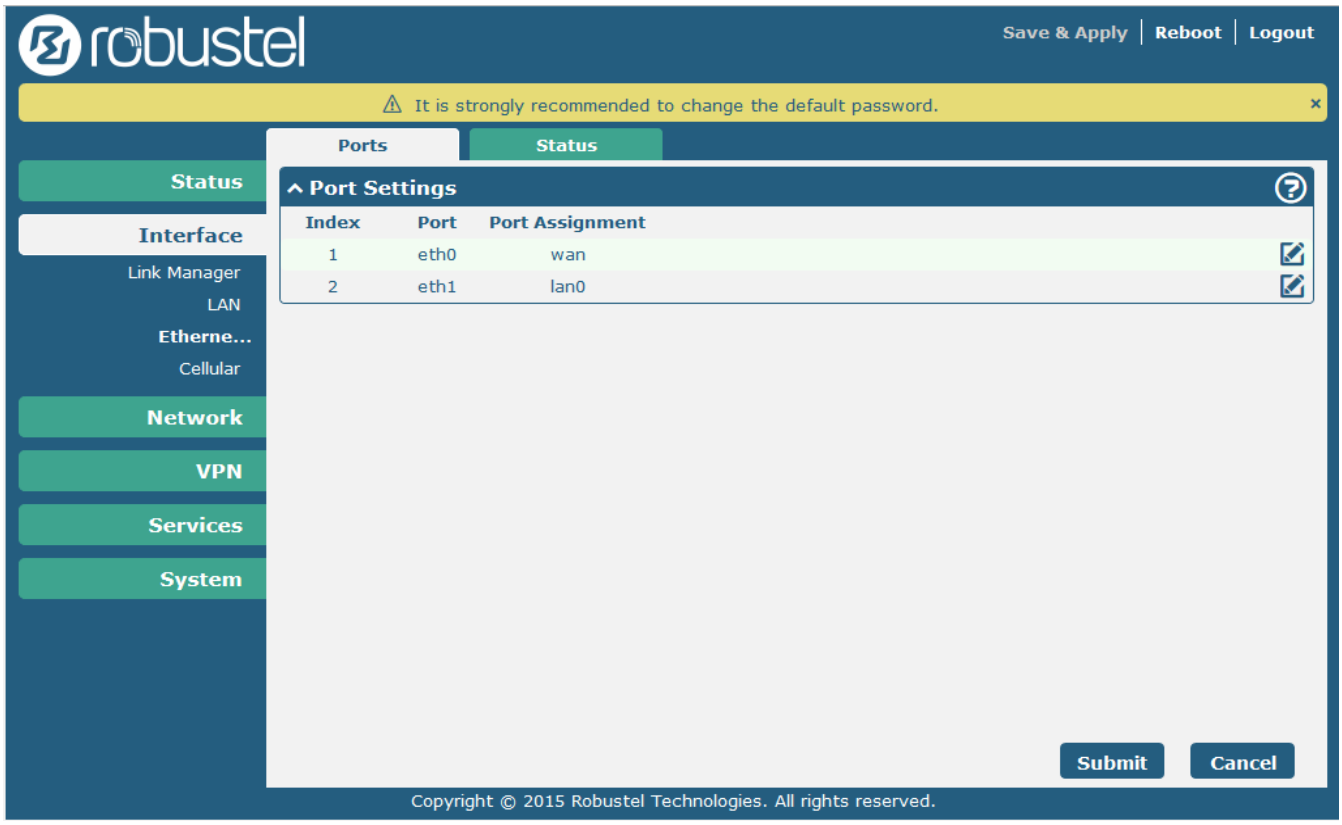
Note: You need to know the following factory settings before you have logged in the Web GUI.

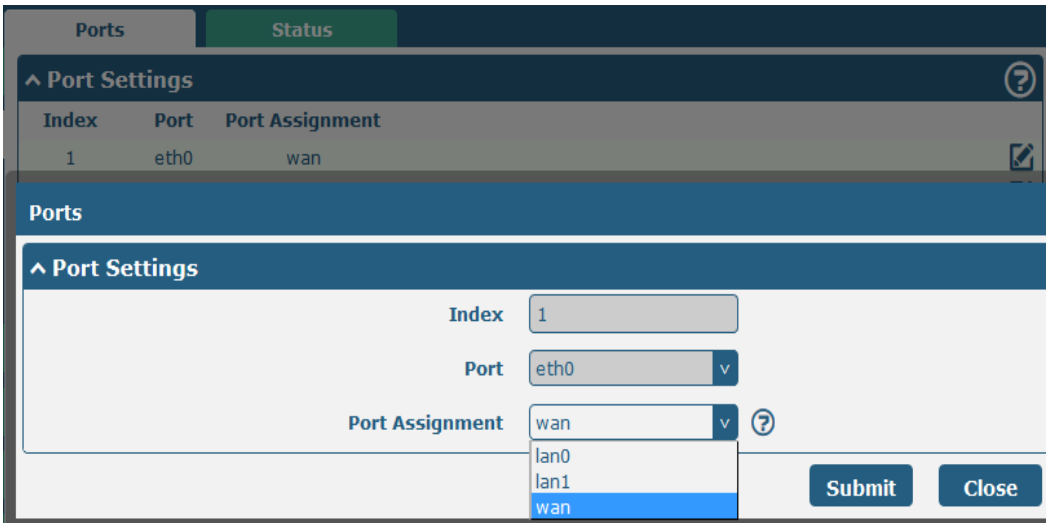
Item	Description
Username	Admin
Password	Admin
ETH0	192.168.0.1/255.255.255.0, LAN Mode
ETH1	192.168.0.1/255.255.255.0, LAN Mode
DHCP Server	Enabled

3.1.1 Configure WAN Link

1. Browse **Interface > Ethernet > Ports > Port Settings**.

- Click the edit button of eth0.
- Click the drop-down list of **Port Assignment** and choose **wan**.
- Click **Submit**.
- Click **Save & Apply**.

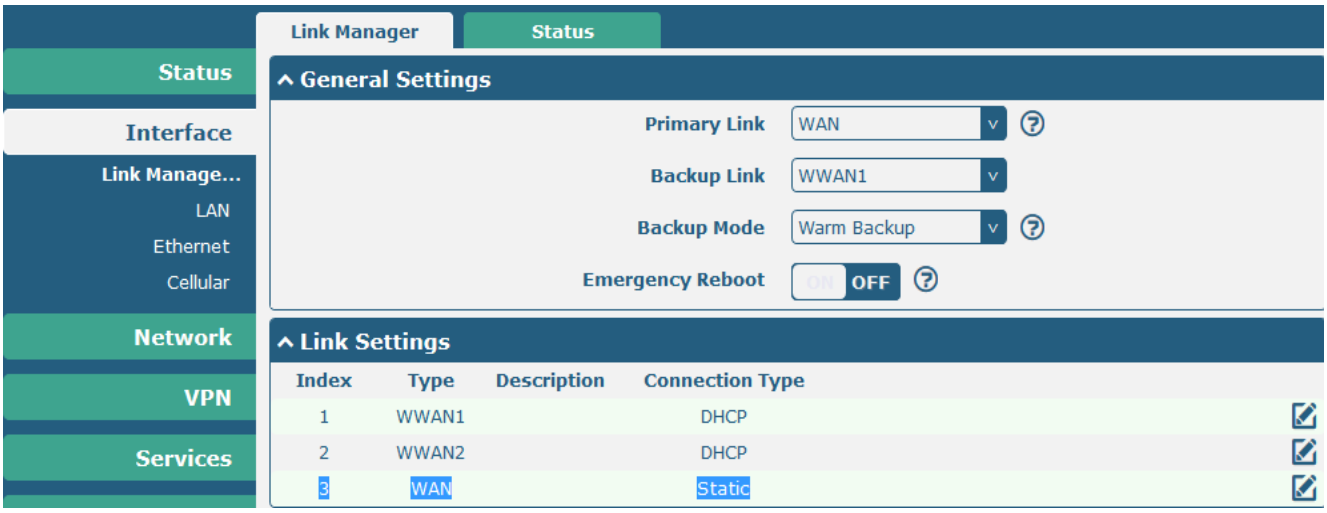


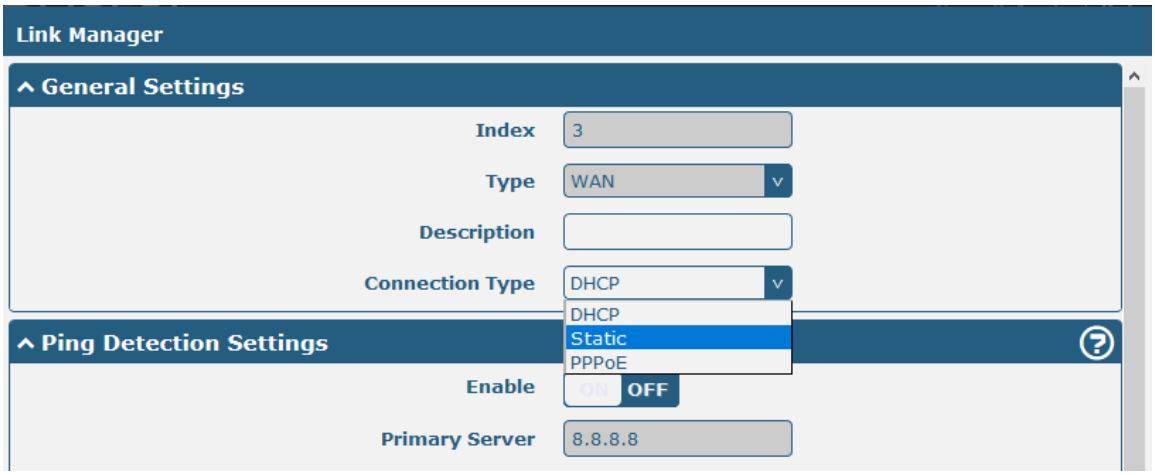


Item	Description	Setting
Port	Choose “eth0” or “eth1”, but one port should be assigned to lan0 at least.	eth0
Port Assignment	Choose “lan0”, “lan1” or “wan”.	wan

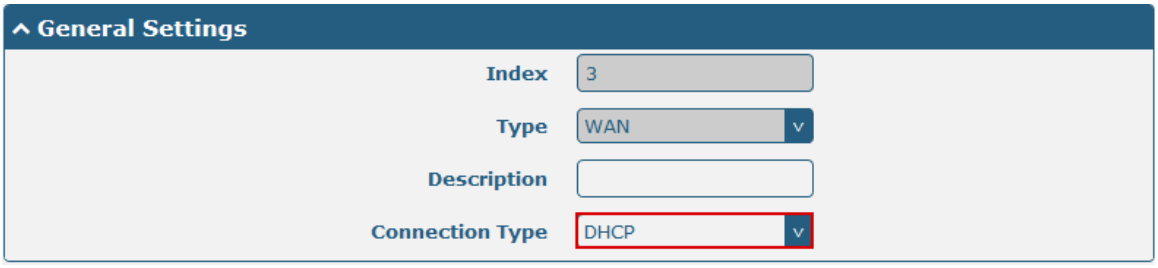
2. Browse **Interface > Link Management > Link Settings**.

- Click the edit button of **WAN**.
- Enter the related parameters in **Static Address Settings.**
- Enter the related parameters in **Ping Detection Settings**.
- Click **Submit**.
- Click **Save & Apply**.





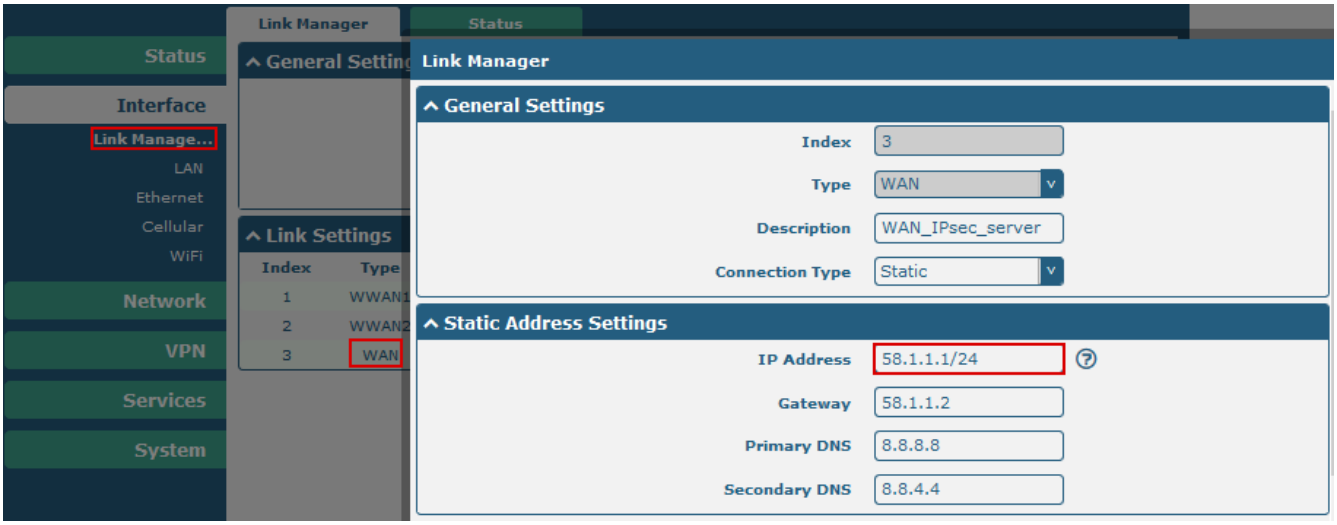
R2000 will obtain IP automatically from DHCP server when choosing **DHCP** as the connection type.



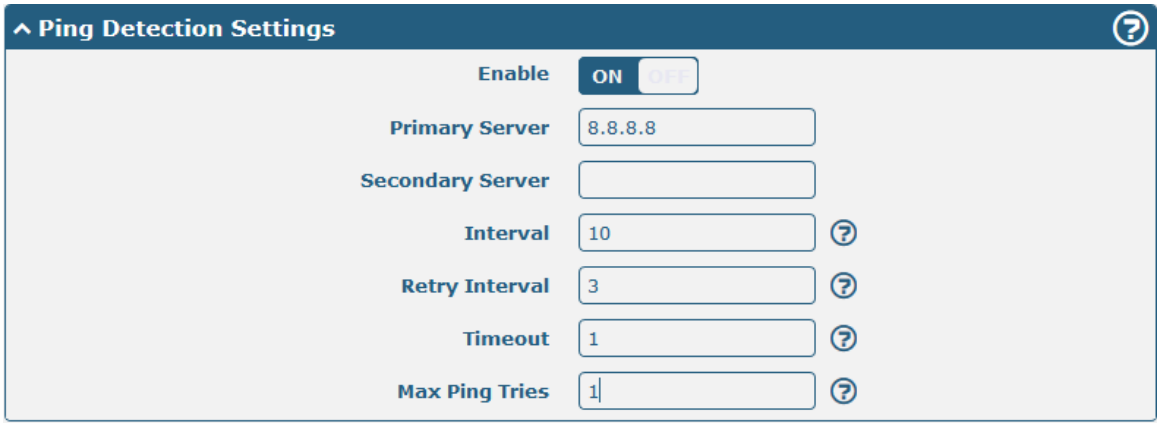
The window is displayed as below when choosing **PPPoE** as the connection type.

Item	Description	Setting
Username	Enter the username provided by your Internet Service Provider.	Null
Password	Enter the password provided by your Internet Service Provider.	Null
Authentication Type	Choose “Auto”, “PAP” or “CHAP” as the local Internet Service Provider required.	Auto
PPP Expert Options	PPP Expert options are used for PPPoE dialup. You can enter some other PPP initialization strings in this field. Each string can be separated by a semicolon (;).	Null

Here we chose **Static** as the connection type that makes it easier to test.



Item	Description	Setting
IP Address	Set the IP address with Netmask which can access the Internet.	172.16.5.227/16
Gateway	Set the gateway of the WAN IP.	172.16.5.1
Primary DNS	Set the Primary DNS.	172.16.5.1
Secondary DNS	Set the Secondary DNS.	Null



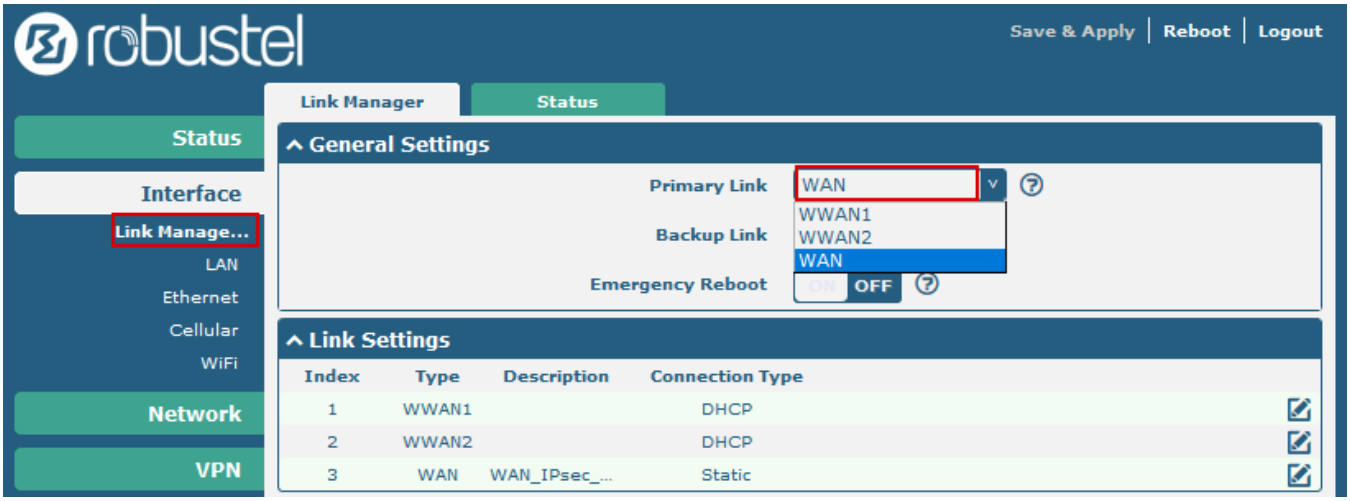
Item	Description	Setting
Primary Server	Router will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8

Secondary Server	Router will ping this secondary address/domain name to check if the current connectivity is active.	Null
Interval	Set the ping interval.	10
Retry Interval	Set the ping retry interval.	3
Timeout	Set the ping timeout.	1
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	1

3.1.2 Configure Link Management Settings

Browse **Interface > Link Management > Link Manager > General Settings**.

- Click the drop-down list of **Primary Link** and choose **WAN**.
- Click the drop-down list of **Backup Link** and choose **WWAN1**.
- Click the drop-down list of **Backup Mode** and choose **Warm Backup**.
- Click **Submit**.
- Click **Save & Apply**.



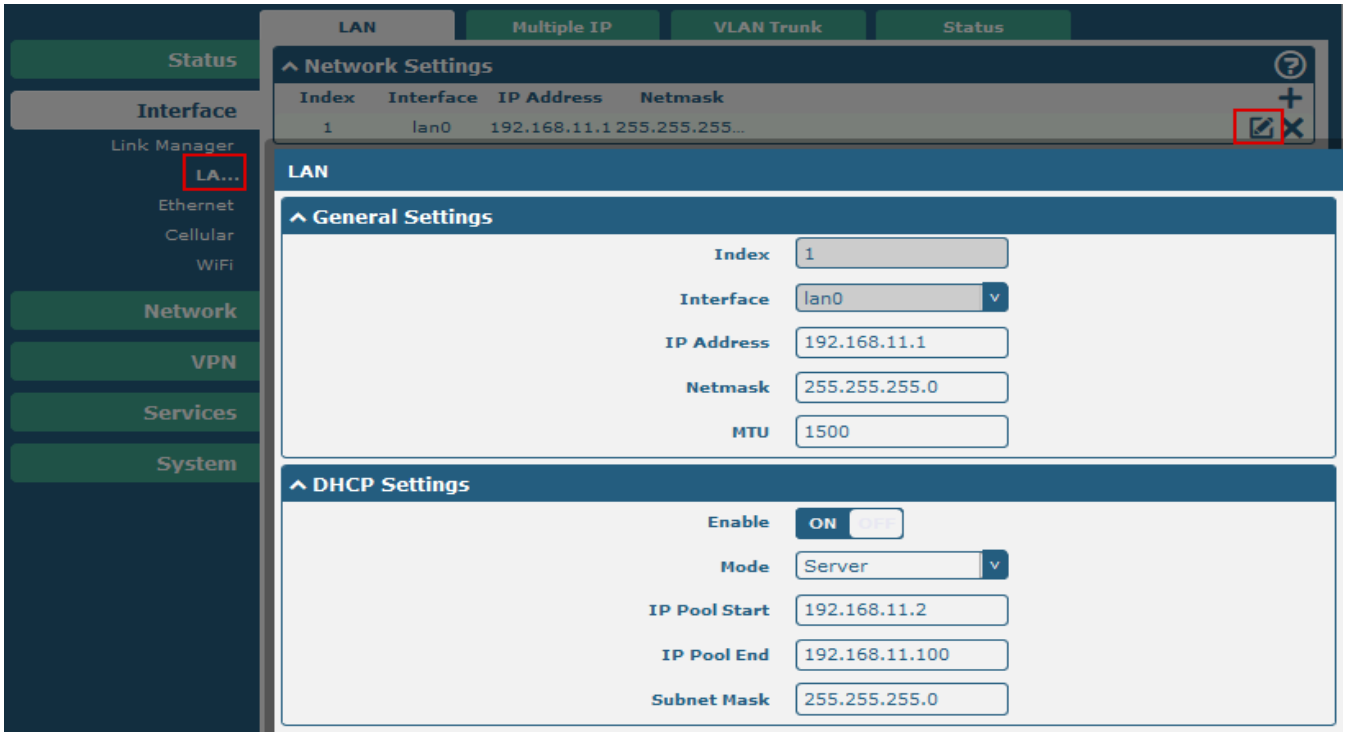
Item	Description	Setting
Primary Link	Select “WWAN1”, “WWAN2” or “WAN” as the primary connecting interface.	WAN
Backup Link	Select “WWAN1”, “WWAN2” or “WAN” as the backup connecting interface.	WWAN1
Backup Mode	Select “Cold Backup”, “Warm Backup” or “Load Balancing” as the backup mode.	Warm Backup

3.1.3 Configure LAN IP Address

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

- Click the edit button of **lan0**.
- Set its **IP address** and **Netmask**, and the parameters of **DHCP Settings** are set accordingly.

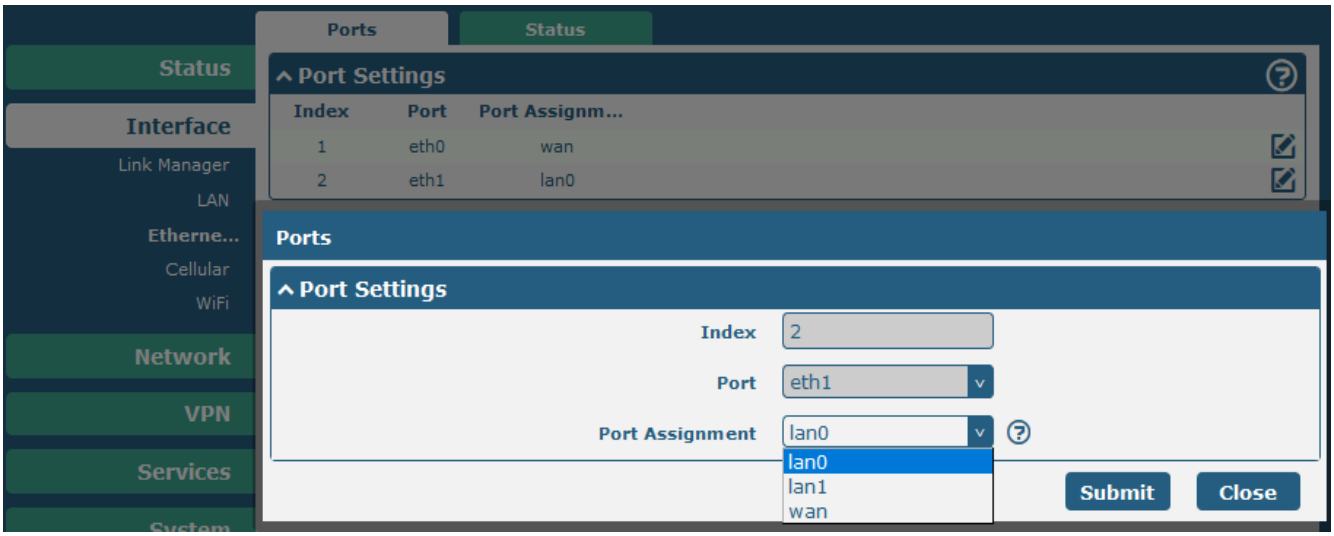
- Click **Submit**.
- Click **Save & Apply**.



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 **Interface > Ethernet > Ports**.

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



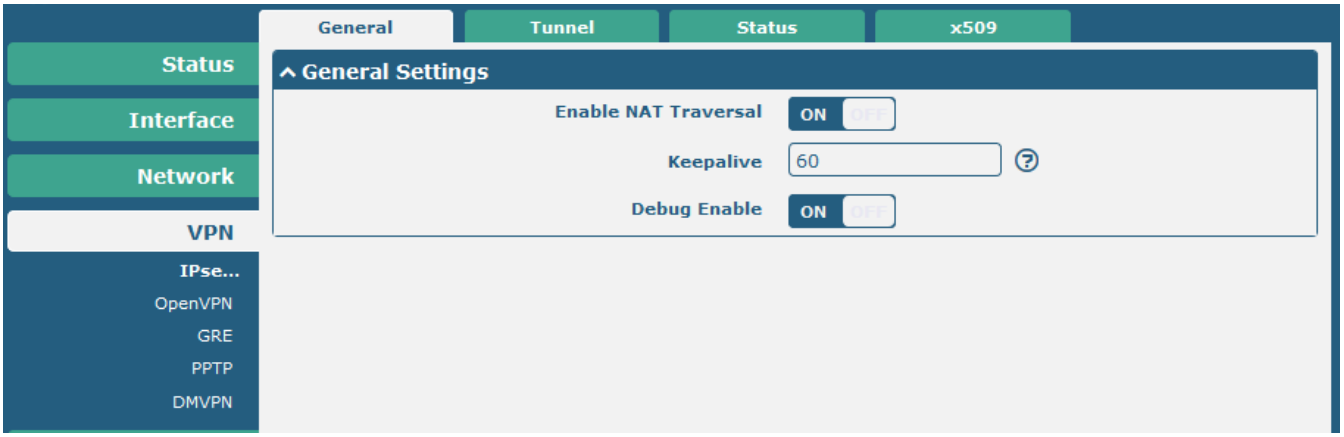
3.1.4 IPsec Configuration

The following sections are related to the IPsec VPN parameters.

1. Browse **VPN > IPsec > General**, and enable NAT traversal feature.

- Click the button of **Enable NAT Traversal**.

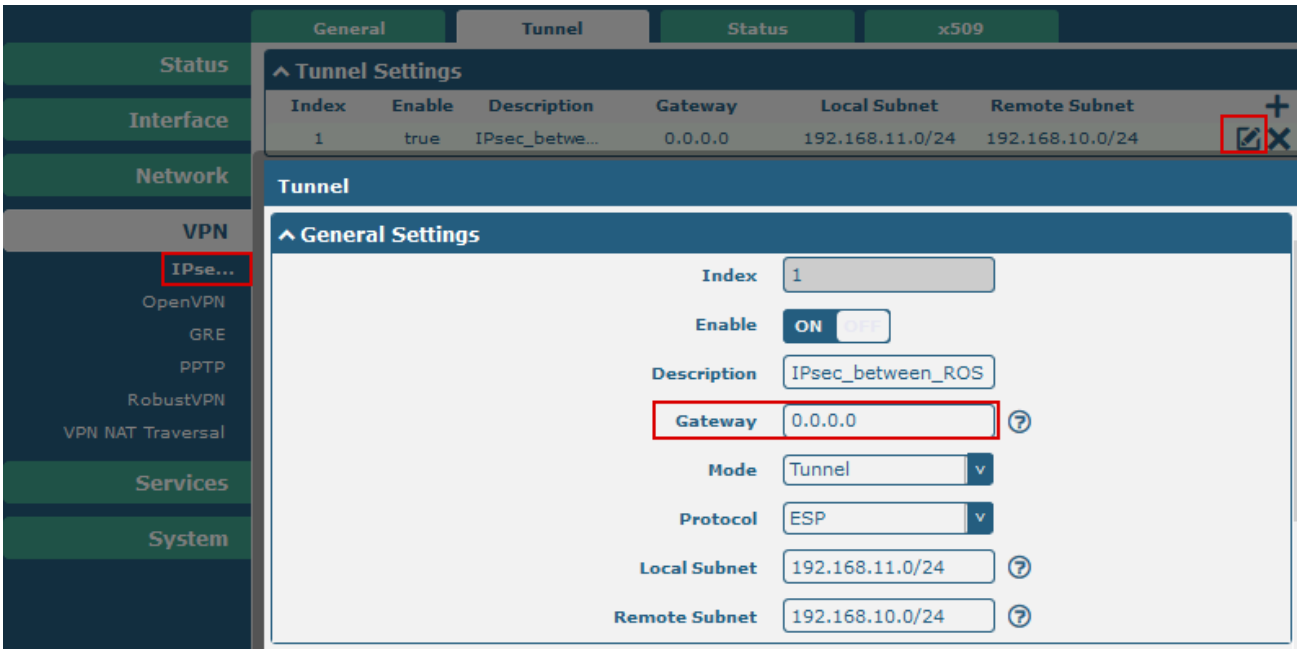
  Note: This item must be enabled when router under a NAT environment.
- Enter the value about **Keepalive** Interval (s).
- Click the button of **Debug Enable**.
- Click **Submit**.
- Click **Save & Apply**.



Item	Description	Setting
Enable NAT Traversal	Click to enable NAT Traversal for IPsec.	Enable
Keepalive Interval	Set the interval that router sends keepalive packets to NAT box to avoid actively removing the NAT mapping.	60
Debug Enable	Enable this feature, which will output IPsec information to the debug port.	OFF

2. Browse **VPN > IPsec > Tunnel**.

- Click the add button to enter the settings window of IPsec Tunnel.
- Set IPsec gateway address and subnets accordingly



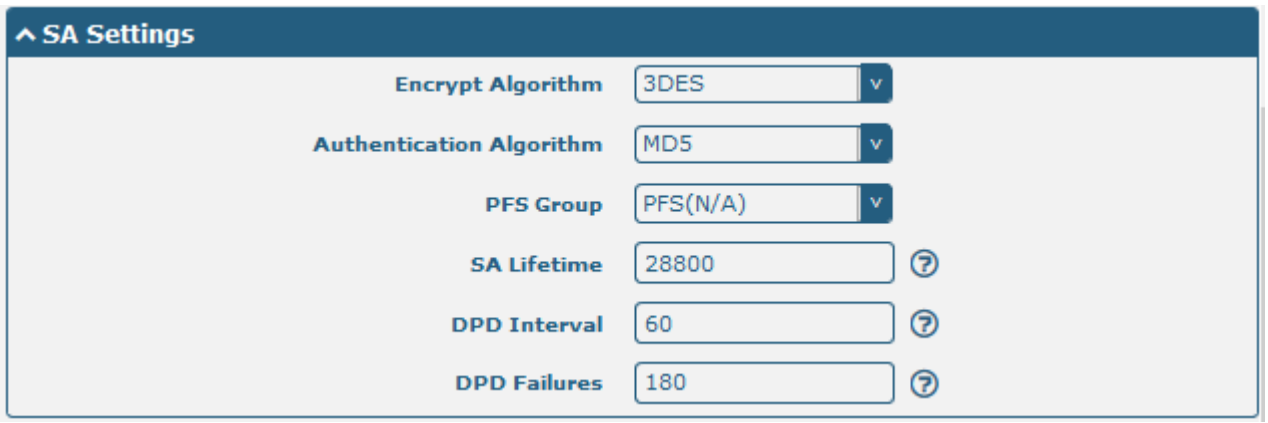
Item	Description	Setting
Gateway	Enter the address of remote side IPsec VPN server.	Enter accordingly
Mode	Select from “Tunnel” or “Transport”. Tunnel: Use the Tunnel protocol Transport: Use the Transport protocol	Select accordingly
Protocol	Select from “ESP” or “AH” as the security protocol. ESP: Use the ESP protocol AH: Use the AH protocol	Select accordingly
Local Subnet	Enter protected subnet address of local IPsec.	Enter accordingly
Remote Subnet	Enter protected subnet address of remote IPsec.	Enter accordingly

- Configure **IKE Settings**

Item	Description	Setting
Negotiation Mode	Select from “Main” or “aggressive” as the IKE negotiation mode.	Select accordingly
Authentication Algorithm	Select from “MD5” or “SHA1”to be used in IKE negotiation. MD5: Use HMAC-SHA1 SHA1: Use HMAC-MD5	Select accordingly
Encryption Algorithm	Select from “DES”, “3DES”, “AES128”, “AES192” or “AES256”to be used in IKE negotiation.	Select accordingly
IKE DH Group	Select from “MODP768_1”, “MODP1024_2” or “MODP1536_5”to be used in key negotiation.	Select accordingly
Authentication Type	Select from “PSK”, “CA”, “XAUTH Init PSK” or “XAUTH Init CA” to be used in IKE negotiation.	Select accordingly
PSK Secret	Enter the Pre-shared Key.	Enter accordingly
Local ID Type	Select from “IP Address”, “FQDN” or “User FQDN” for IKE negotiation. “Default” stands for “IP Address”.	Default
Remote ID Type	Select from “IP Address”, “FQDN” or “User FQDN” for IKE negotiation. “Default” stands for “IP Address”.	Default
IKE Lifetime	Set the lifetime in IKE negotiation.	3600

Note: The server’s PSK Secret must be the same as the client’s PSK.

- Configure **SA Settings**

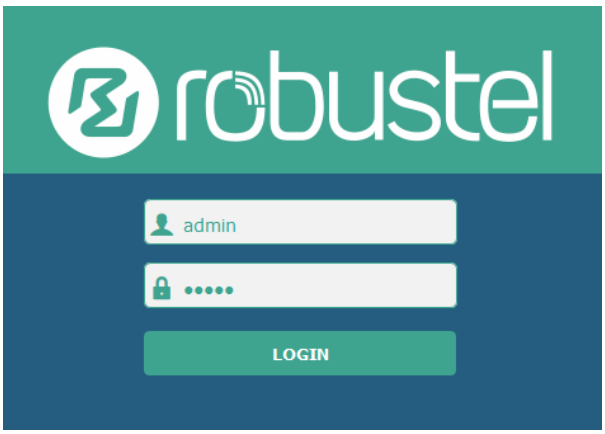


Item	Description	Setting
Encrypt Algorithm	Select from “3DES”, “AES128” or “AES256”.	Select accordingly
Authentication Algorithm	Select from “MD5” or “SHA1”to be used in SA negotiation.	Select accordingly
PFS Group	Select from “PFS_NULL”, “MODP768_1”, “MODP1024_2” or “MODP1536_5”.	Select accordingly
SA Lifetime	Set the lifetime of IPsec SA.	28800
DPD Interval	Set the interval time. If not received IPsec protected packets from the peer, DPD will be triggered after the specified interval time.	60
DPD Failures	Set the timeout of DPD packets.	180

3.2 R2000_ROS (IPsec Local) Configuration

3.2.1 Configure Link Manager

1. Install the antenna, insert the SIM cards, connect the power supply, and log-in the Web GUI of R2000.

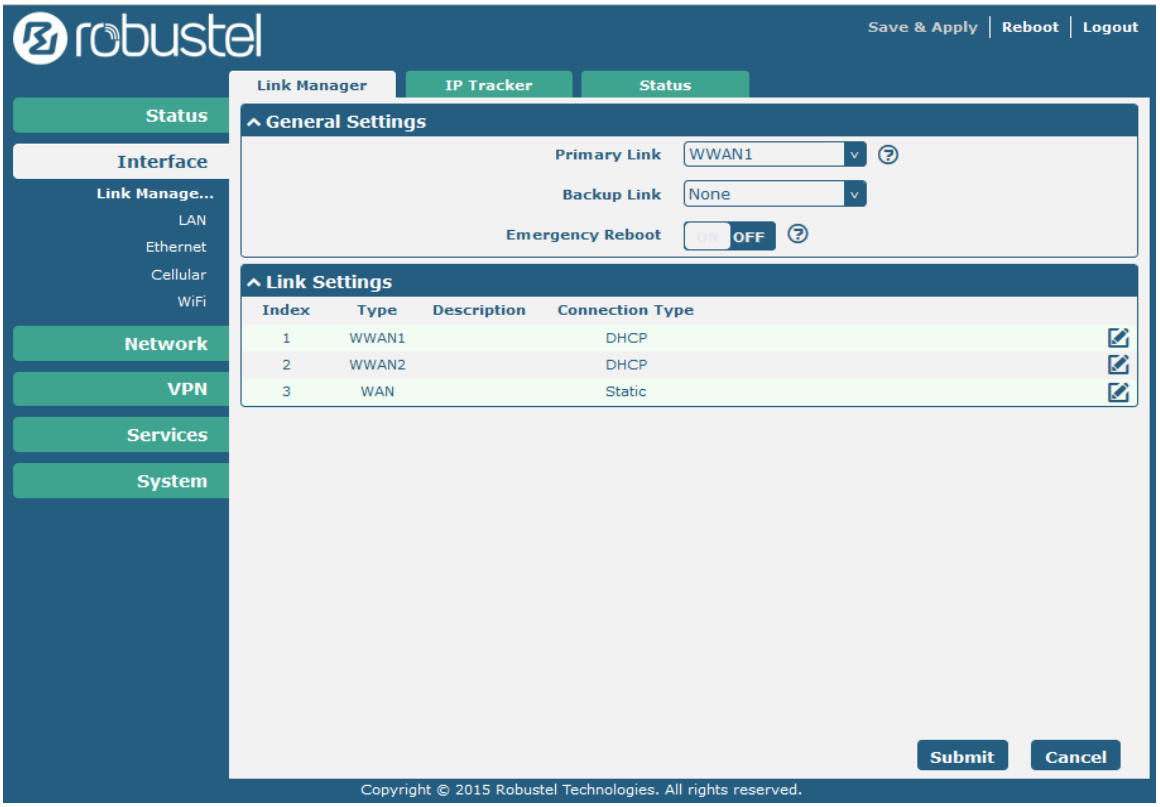


Note: You need to know the following factory settings before you have logged in the Web GUI.

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 **Interface > Link Management**.

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

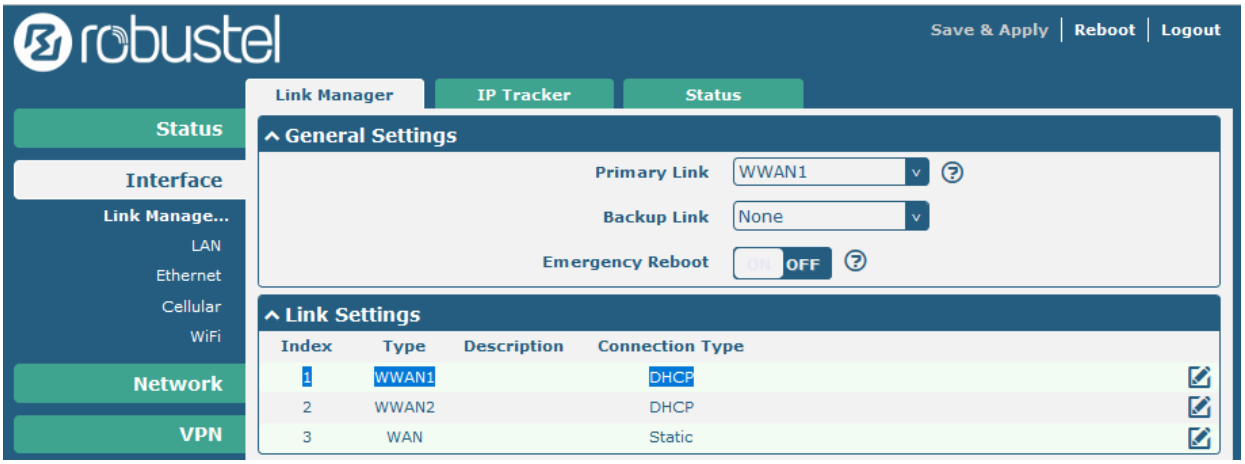


Item	Description	Setting
Primary Link	Select “WWAN1”, “WWAN2” or “WAN” as the primary connecting interface.	WWAN1

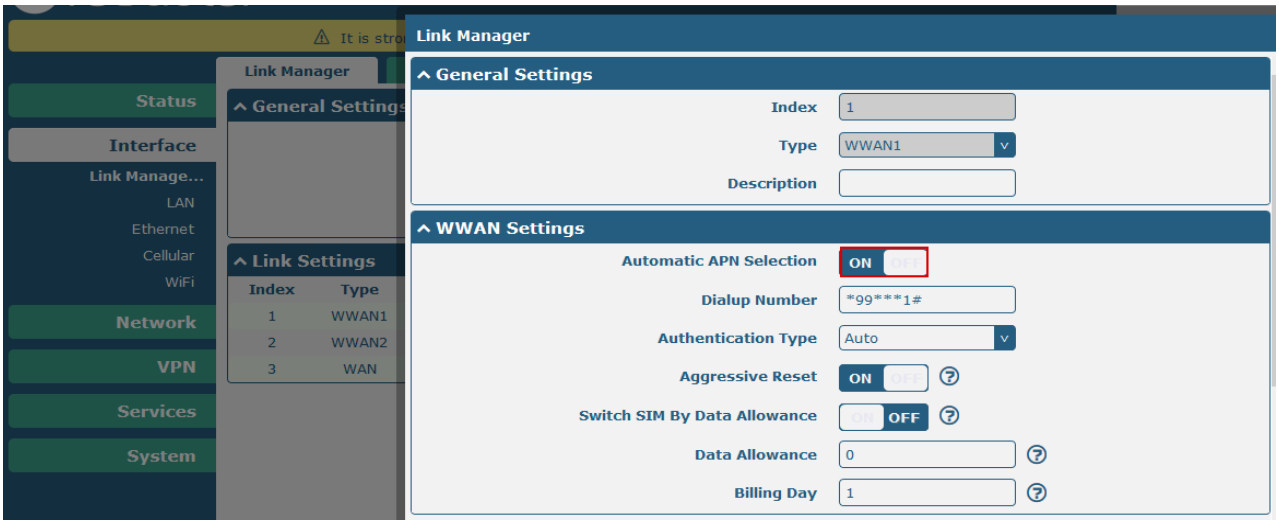
3.2.2 Configure Cellular WAN

Browse **Interface > Link Management > Link Settings**.

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

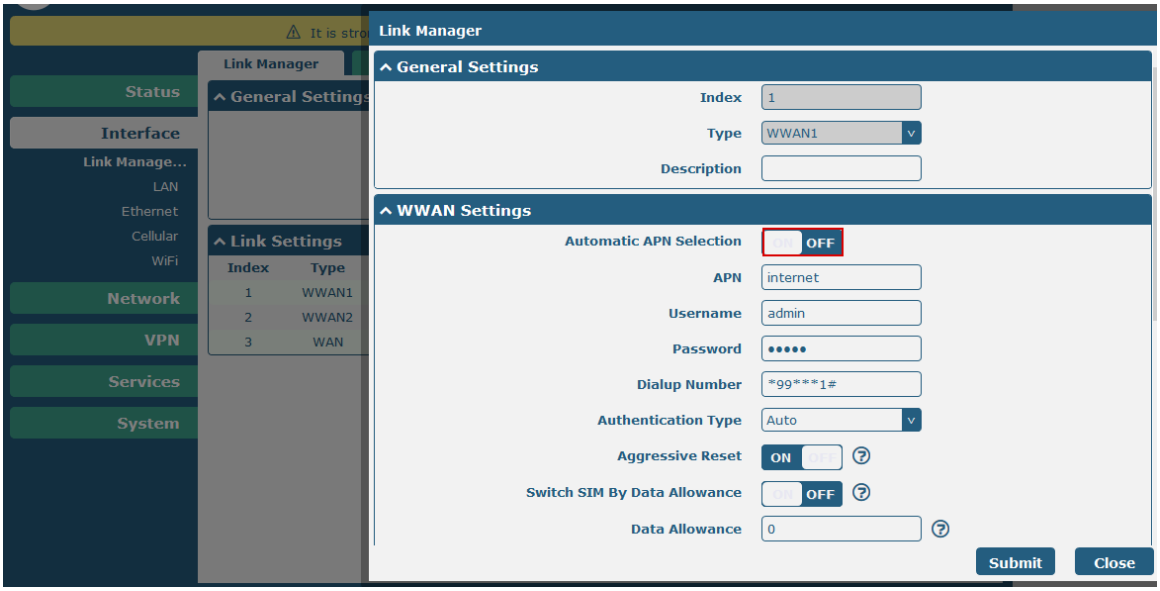


The window is displayed as below when enabling the **Automatic APN Selection**.

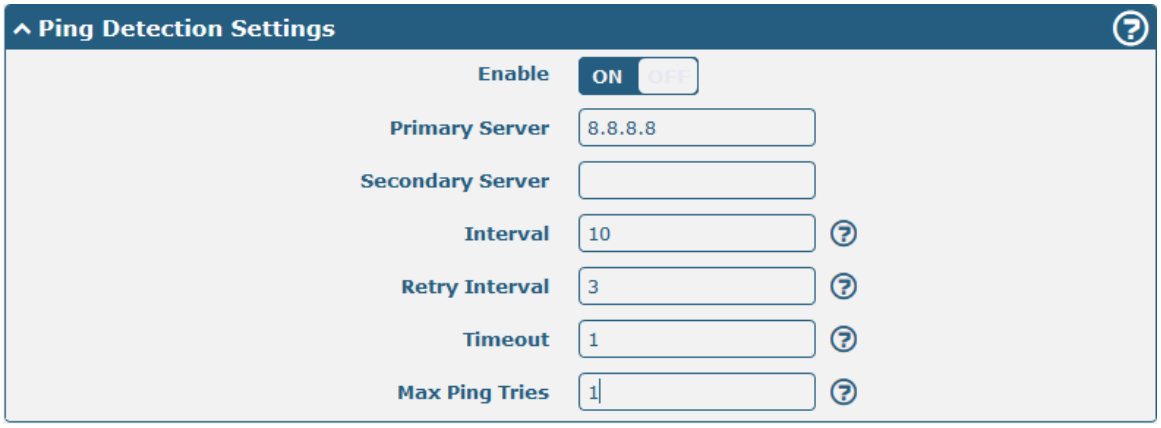


Item	Description	Setting
Dialup Number	Set the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Data Allowance	Set the monthly data traffic limitation.	0
Billing Day	Specify the monthly billing day, and the data traffic statistics will be recalculated from this day.	1

The window is displayed as below when disabling the **Automatic APN Selection**.



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

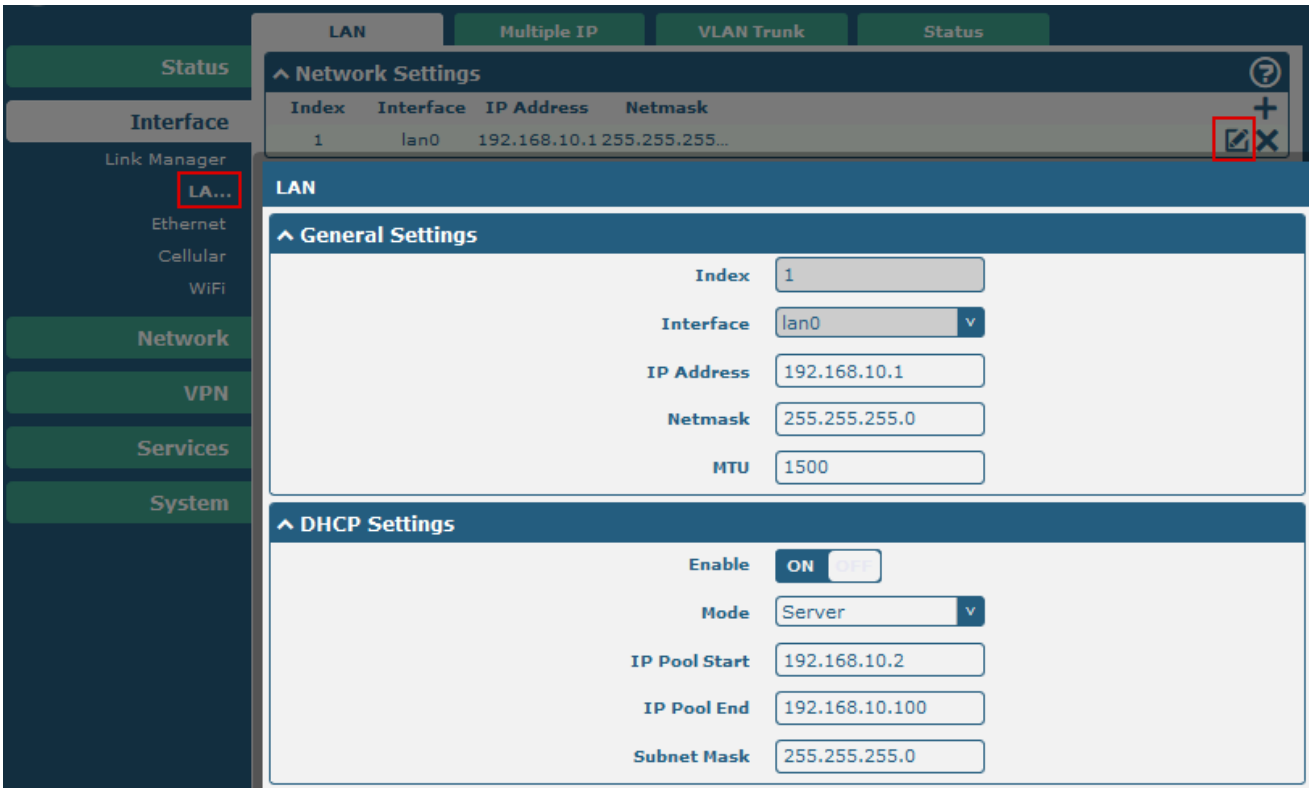


Item	Description	Setting
Primary Server	Router will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check if the current connectivity is active.	Null
Interval	Set the ping interval.	10
Retry Interval	Set the ping retry interval.	3
Timeout	Set the ping timeout.	1
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	1

3.2.3 Configure IP Address of LAN

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

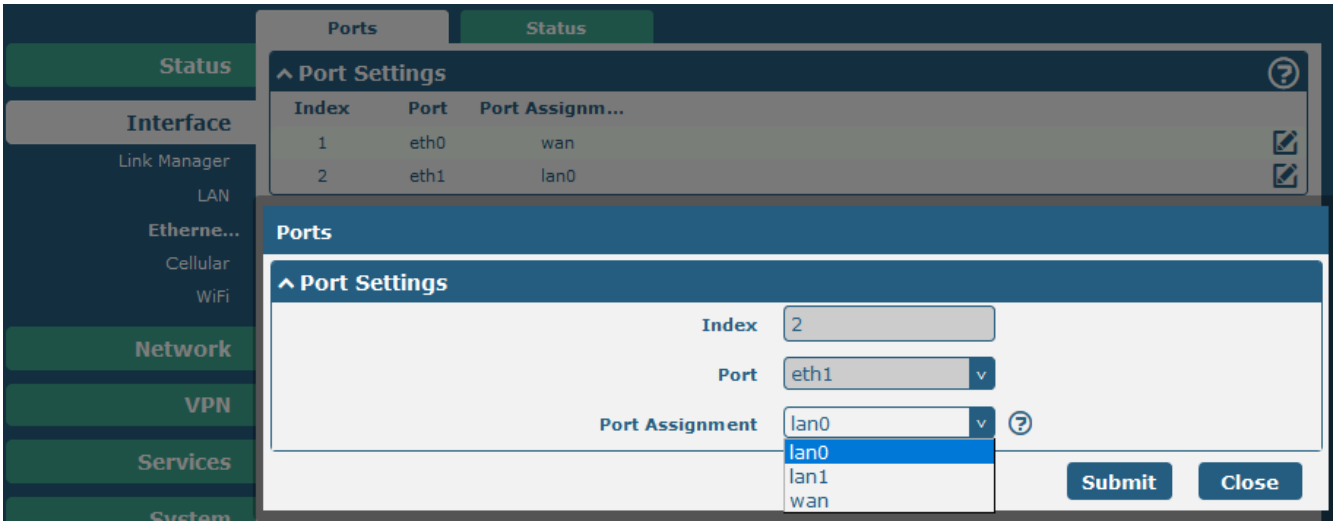
- Click the edit button of **lan0**.
- Set its **IP address** and **Netmask**, and the parameters of **DHCP Settings** are set accordingly.
- Click **Submit**.
- Click **Save & Apply**.



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 **Interface > Ethernet > Ports**.

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



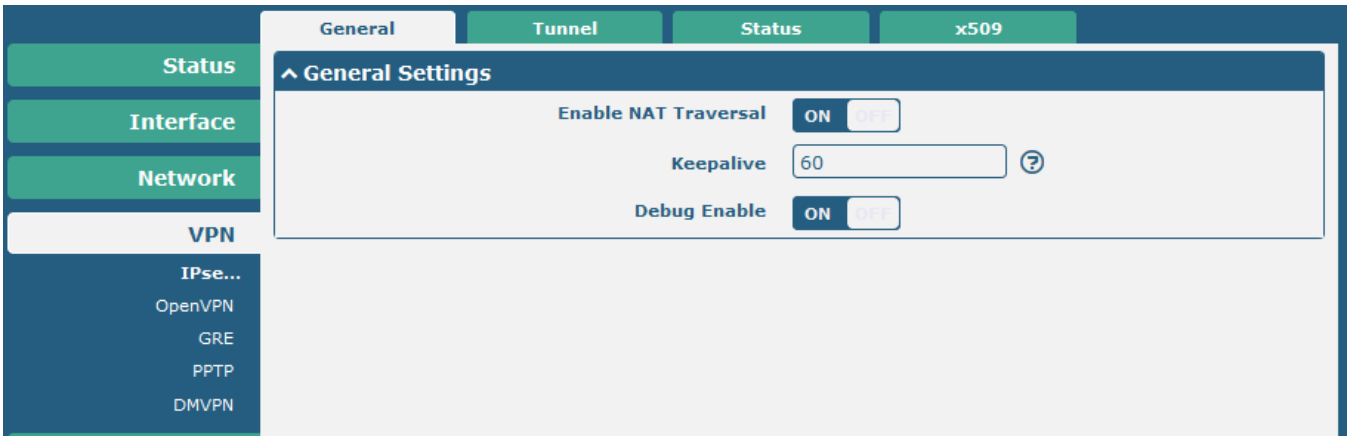
3.2.4 IPsec Configuration

The following sections are related to the IPsec VPN parameters.

1. Browse **VPN > IPsec > General**, and enable NAT traversal feature.

- Click the button of **Enable NAT Traversal**.

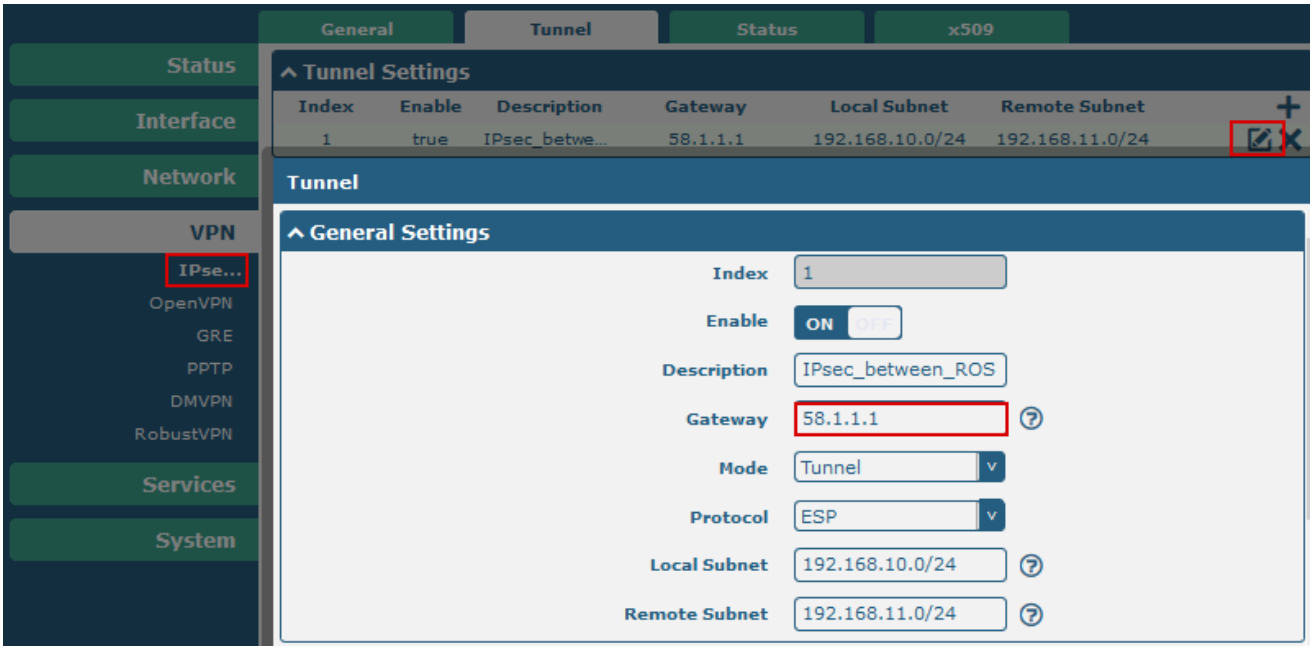
  Note: This item must be enabled when router under a NAT environment.
- Enter the value about **Keepalive** Interval(s).
- Click the button of **Debug Enable**.
- Click **Submit**.
- Click **Save & Apply**.



Item	Description	Setting
Enable NAT Traversal	Click to enable NAT Traversal for IPsec.	Enable
Keepalive Interval	Set the interval that router sends keepalive packets to NAT box to avoid actively removing the NAT mapping.	60
Debug Enable	Enable this feature, which will output IPsec information to the debug port.	OFF

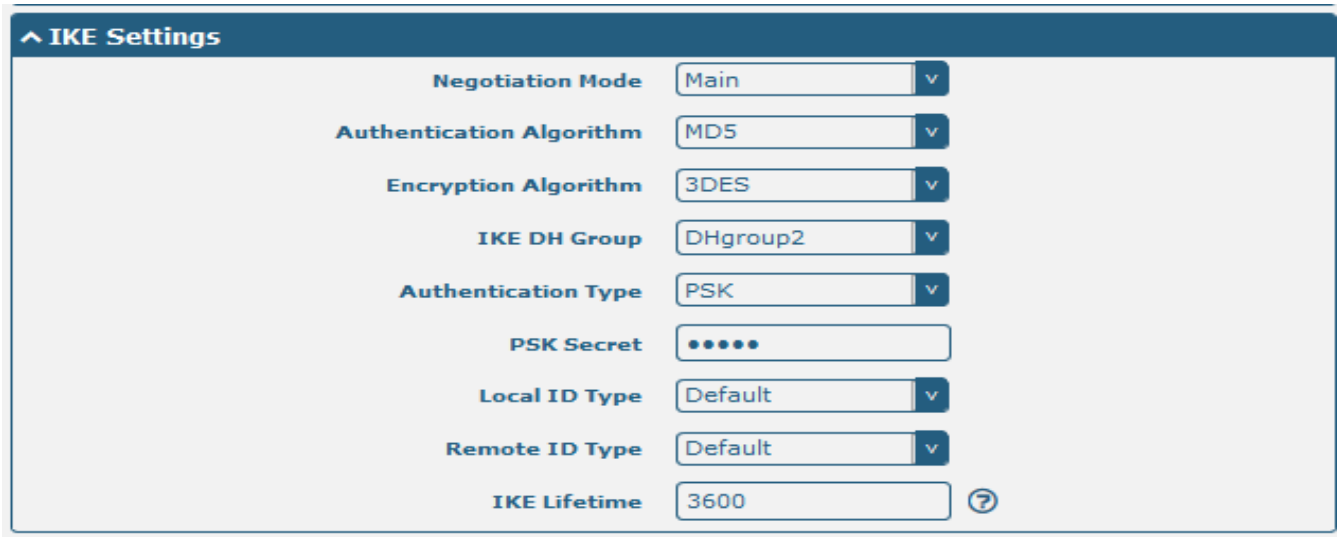
2. Browse **VPN > IPsec > Tunnel**.

- Click the add button to enter the settings window of IPsec Tunnel.
- Set IPsec Gateway address and subnets accordingly.



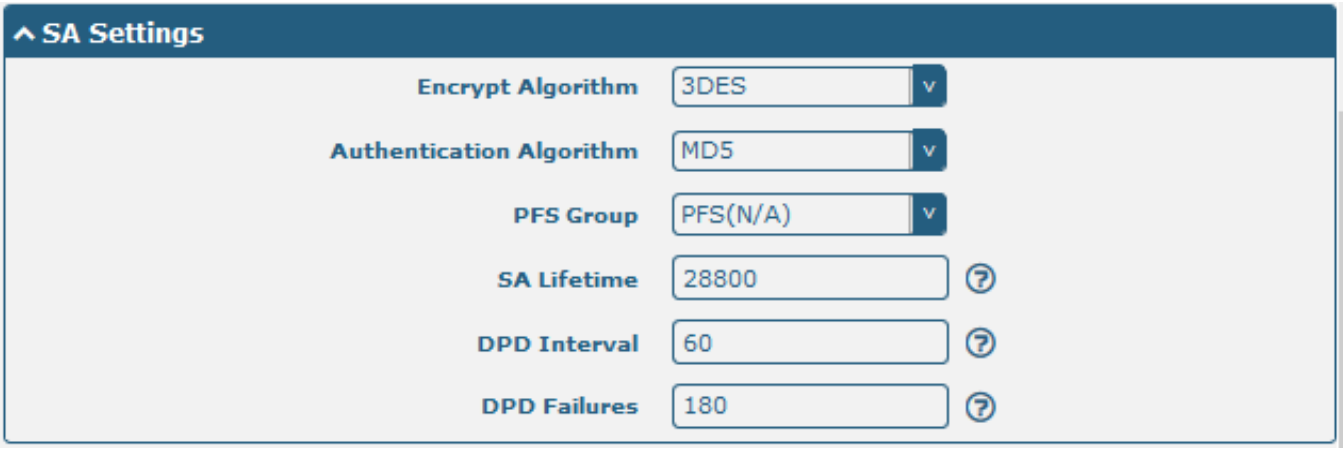
Item	Description	Setting
Gateway	Enter the address of remote side IPsec VPN server.	Enter accordingly
Mode	Select from “Tunnel” or “Transport”. Tunnel: Use the Tunnel protocol Transport: Use the Transport protocol	Select accordingly
Protocol	Select from “ESP” or “AH” as the security protocol. ESP: Use the ESP protocol AH: Use the AH protocol	Select accordingly
Local Subnet	Enter protected subnet address of local IPsec.	Enter accordingly
Remote Subnet	Enter protected subnet address of remote IPsec.	Enter accordingly

- Configure **IKE Settings**



Item	Description	Setting
Negotiation Mode	Select from “Main” or “aggressive” for the IKE negotiation mode.	Select accordingly
Authentication Algorithm	Select from “MD5” or “SHA1”to be used in IKE negotiation. MD5: Use HMAC-SHA1 SHA1: Use HMAC-MD5	Select accordingly
Encryption Algorithm	Select from “DES”, “3DES”, “AES128”, “AES192” or “AES256”to be used in IKE negotiation.	Select accordingly
IKE DH Group	Select from “MODP768_1”, “MODP1024_2” or “MODP1536_5”to be used in key negotiation.	Select accordingly
Authentication Type	Select from “PSK”, “CA”, “XAUTH Init PSK” or “XAUTH Init CA” to be used in IKE negotiation.	Select accordingly
Local ID Type	Select from “IP Address”, “FQDN” or “User FQDN” for IKE negotiation. “Default” stands for “IP Address”.	Default
Remote ID Type	Select from “IP Address”, “FQDN” or “User FQDN” for IKE negotiation. “Default” stands for “IP Address”.	Default
PSK Secret	Enter the Pre-shared Key.	Enter accordingly
IKE Lifetime	Set the lifetime in IKE negotiation.	3600

- Configure **SA Settings**



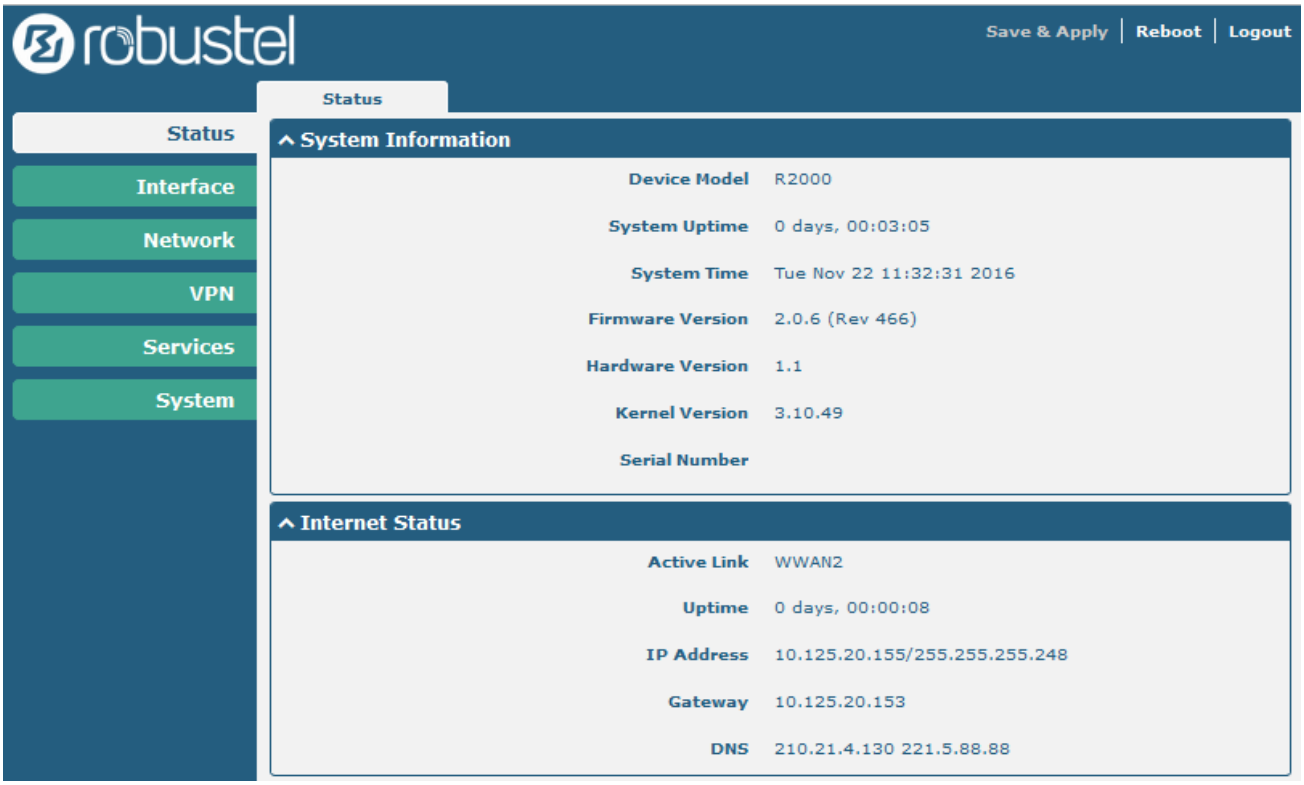
Item	Description	Setting
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256”.	Select accordingly
Authentication Algorithm	Select from “MD5” or “SHA1”to be used in SA negotiation.	Select accordingly
PFS Group	Select from “PFS_NULL”, “MODP768_1”, “MODP1024_2” or “MODP1536_5”.	Select accordingly
SA Lifetime	Set the lifetime of IPsec SA.	28800
DPD Interval	Set the interval time. If not received IPsec protected packets from the peer, DPD will be triggered after the specified interval time.	60
DPD Failures	Set the timeout of DPD packets.	180

- Click **Submit**.
- Click **Save & Apply**.

Chapter 4 Testing

4.1 Network Status

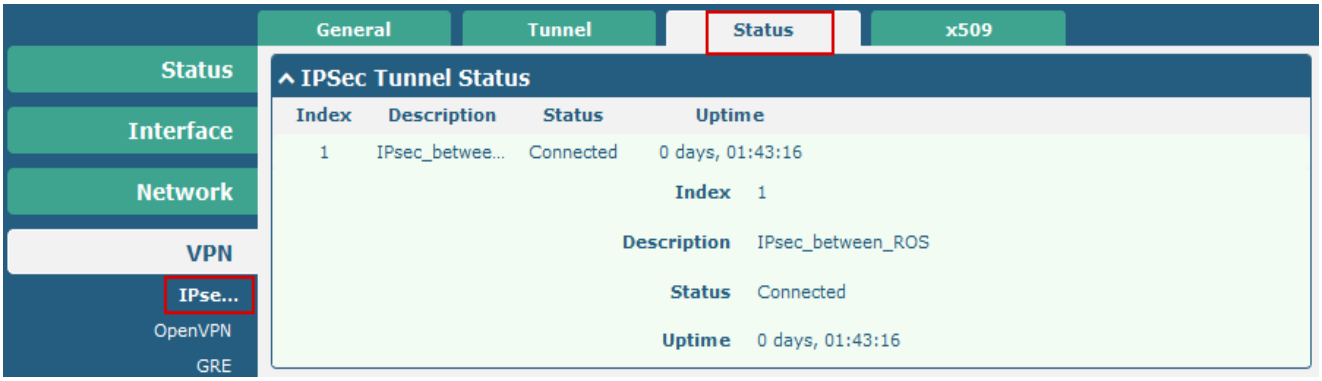
1. Browse **Status**.
2. Check whether R2000 Remote has obtained the assigned static IP address.
3. Check whether R2000 Local has used SIM card to register to network, dial up to get IP address and get access to the Internet.

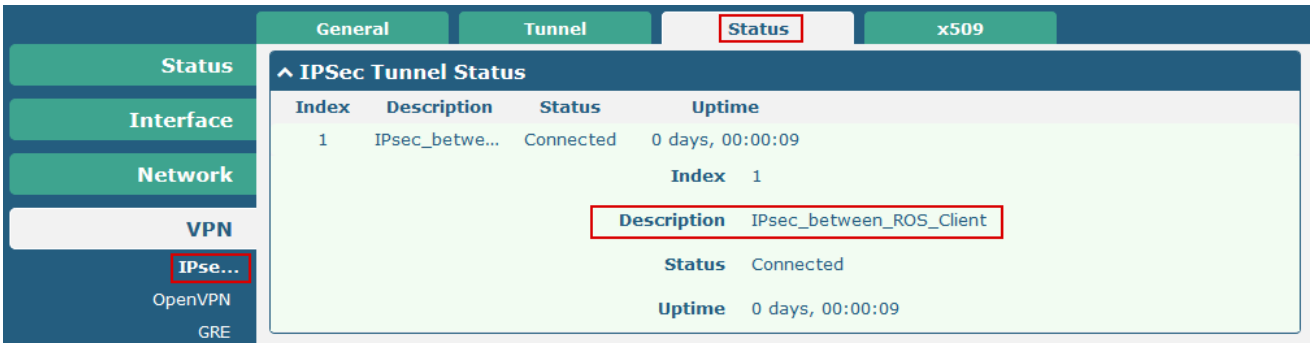


4.2 VPN Status and Communication

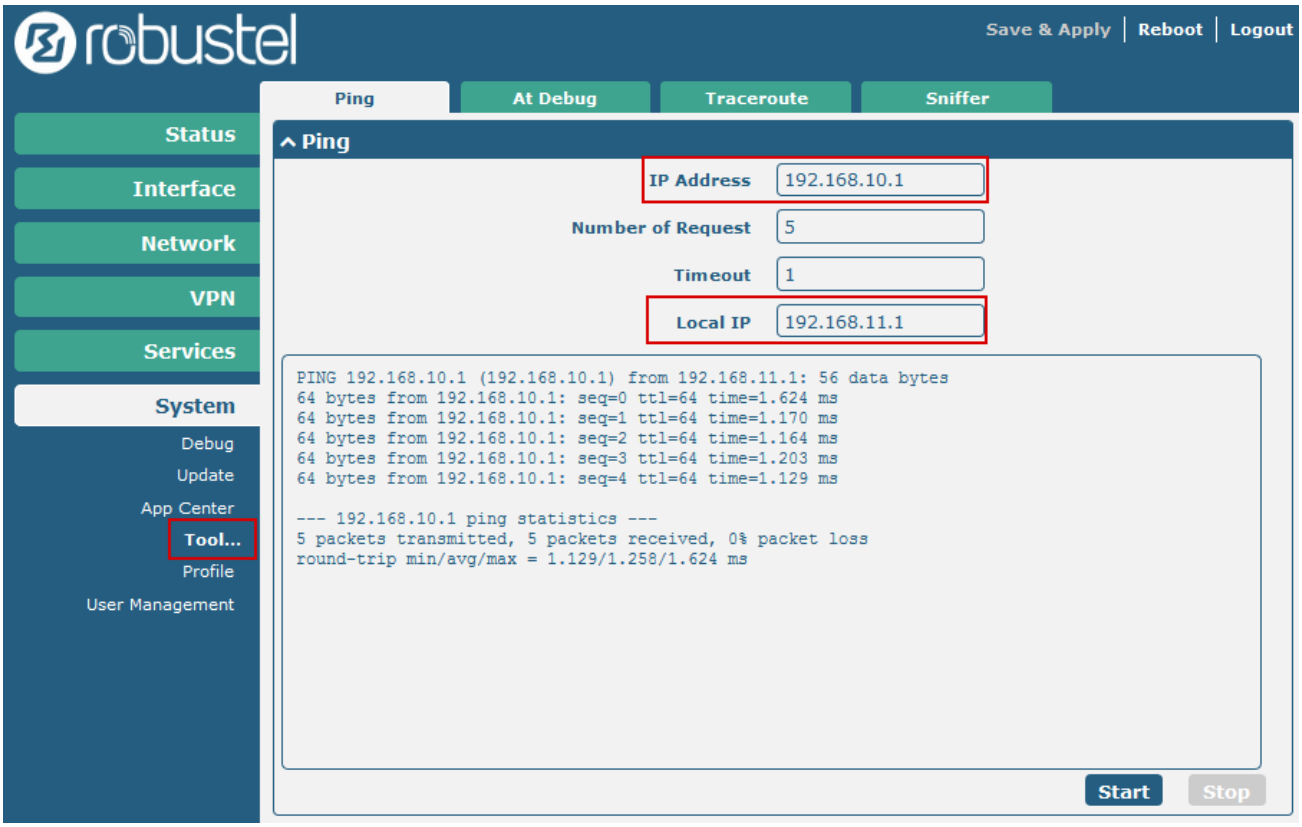
Browse **VPN > IPsec > Status**.

- Check whether the ROS has established IPsec VPN with Cisco router.



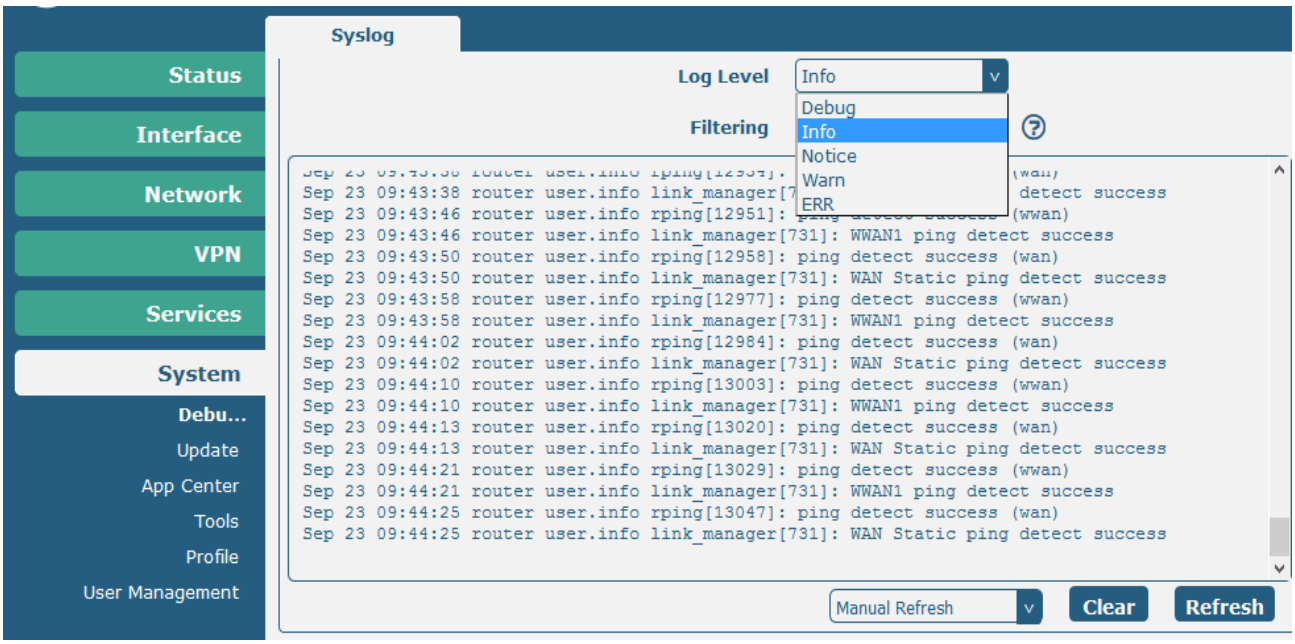


- Browse **System > Tools > Ping**.
  Ping from 192.168.11.1 to 172.16.10.1 and get ICMP reply from Cisco router. LAN to LAN communication is working correctly.



4.3 Event/Log

Event/Log shows the running process and the ROS status. Only the information is relevant to the configuration above will be explained below:



```
router daemon.err ipsec_setup: ...Openswan IPsec started
router daemon.err ipsec_setup: ...Openswan IPsec started
router user.notice init[1]: IPSec started
router    authpriv.debug pluto[1008]: | Added new connection IPSec_TUN_1 with policy
                    PSK+ENCRYPT+TUNNEL+PFS+IKEv2ALLOW+SAREFTRACK
router authpriv.warn pluto[1008]: added connection description "IPSec_TUN_1"
router daemon.err ipsec__plutorun: 002 added connection description "IPSec_TUN_1"
router daemon.err ipsec__plutorun: 002 added connection description "IPSec_TUN_1"
router authpriv.debug pluto[1008]: | ike_life: 86400s; ipsec_life: 28800s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0; policy:
PSK+ENCRYPT+TUNNEL+PFS+IKEv2ALLOW+SAREFTRACK
router authpriv.warn pluto[1008]: loading secrets from "/etc/ipsec.secrets"
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | Queuing pending Quick Mode with 58.1.1.1 "IPSec_TUN_1"
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: initiating Main Mode
router daemon.err ipsec__plutorun: 104 "IPSec_TUN_1" #1: STATE_MAIN_I1: initiate
router daemon.err ipsec__plutorun: 104 "IPSec_TUN_1" #1: STATE_MAIN_I1: initiate
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: |        DOI: ISAKMP_DOI_IPSEC
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: received Vendor ID payload [Openswan (this version) 2.6.42 ]
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: received Vendor ID payload [Dead Peer Detection]
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: received Vendor ID payload [RFC 3947] method set to=115
router authpriv.debug pluto[1008]: | ****parse IPsec DOI SIT:
router authpriv.debug pluto[1008]: |        IPsec DOI SIT: SIT_IDENTITY_ONLY
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: enabling possible NAT-traversal with method RFC 3947 (NAT-Traversal)
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: STATE_MAIN_I2: sent MI2, expecting MR2
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike (MacOS X): no NAT detected
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike (MacOS X): no NAT detected
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: STATE_MAIN_I3: sent MI3, expecting MR3
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: received Vendor ID payload [CAN-IKEv2]
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: Main mode peer ID is ID_IPV4_ADDR: '58.1.1.1'
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY
cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp1024}
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: Dead Peer Detection (RFC 3706): enabled
router authpriv.debug pluto[1008]: | unqueuing pending Quick Mode with 58.1.1.1 "IPSec_TUN_1" import:admin initiate
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
```

```
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW+SAREFTRACK
{using isakmp#1 msgid:2238bc3d proposal=3DES(3)_192-MD5(1)_128 pfsgroup=OAKLEY_GROUP_MODP1024}
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | install_ipsec_sa() for #2: inbound and outbound
router authpriv.debug pluto[1008]: | route owner of "IPSec_TUN_1" prospective erouted: self; eroute owner: self
router authpriv.debug pluto[1008]: | could_route called for IPSec_TUN_1 (kind=CK_PERMANENT)
router authpriv.debug pluto[1008]: | cmd( 800): ipsec_updown 1:
router user.debug ipsec_updown[1543]: ----------
router authpriv.debug pluto[1008]: | route_and_eroute: instance "IPSec_TUN_1", setting eroute_owner {spd=0x78283a04,sr=0x78283a04}
to #2 (was #0) (newest_ipsec_sa=#0)
router authpriv.debug pluto[1008]: | route_and_eroute: instance "IPSec_TUN_1", setting eroute_owner {spd=0x78283a04,sr=0x78283a04}
to #2 (was #0) (newest_ipsec_sa=#0)
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #2: Dead Peer Detection (RFC 3706): enabled
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #2: transition from state STATE_QUICK_I1 to state STATE_QUICK_I2
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP=>0x7f1d339d
<0xba8e862c xfrm=3DES_0-HMAC_MD5 NATOA=none NATD=none DPD=enabled}
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP=>0x7f1d339d
<0xba8e862c xfrm=3DES_0-HMAC_MD5 NATOA=none NATD=none DPD=enabled}
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: received Delete SA payload: replace IPSEC State #2 in 10 seconds
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: received Delete SA payload: replace IPSEC State #2 in 10 seconds
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: received and ignored informational message
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: |        DOI: ISAKMP_DOI_IPSEC
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #1: received Delete SA payload: deleting ISAKMP State #1
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #2: replacing stale IPsec SA
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #2: replacing stale IPsec SA
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.debug pluto[1008]: | Queuing pending Quick Mode with 58.1.1.1 "IPSec_TUN_1"
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: initiating Main Mode
router authpriv.debug pluto[1008]: |        DOI: ISAKMP_DOI_IPSEC
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: received Vendor ID payload [Openswan (this version) 2.6.42 ]
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: received Vendor ID payload [Dead Peer Detection]
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: received Vendor ID payload [RFC 3947] method set to=115
router authpriv.debug pluto[1008]: | ****parse IPsec DOI SIT:
router authpriv.debug pluto[1008]: |        IPsec DOI SIT: SIT_IDENTITY_ONLY
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: enabling possible NAT-traversal with method RFC 3947 (NAT-Traversal)
router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: STATE_MAIN_I2: sent MI2, expecting MR2
```

router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1

router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike (MacOS X): no NAT detected

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike (MacOS X): no NAT detected

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: STATE_MAIN_I3: sent MI3, expecting MR3

router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: received Vendor ID payload [CAN-IKEv2]

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: Main mode peer ID is ID_IPV4_ADDR: '58.1.1.1'

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp1024}

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #3: Dead Peer Detection (RFC 3706): enabled

router authpriv.debug pluto[1008]: | unqueuing pending Quick Mode with 58.1.1.1 "IPSec_TUN_1" import:admin initiate

router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #4: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW+SAREFTRACK {using isakmp#3 msgid:00f45449 proposal=3DES(3)_192-MD5(1)_128 pfsgroup=OAKLEY_GROUP_MODP1024}

router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1

router authpriv.debug pluto[1008]: | processing connection IPSec_TUN_1

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #4: Dead Peer Detection (RFC 3706): enabled

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #4: transition from state STATE_QUICK_I1 to state STATE_QUICK_I2

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #4: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP=>0xa2dc96fc <0x9f8a0876 xfrm=3DES_0-HMAC_MD5 NATOA=none NATD=none DPD=enabled}

router authpriv.warn pluto[1008]: "IPSec_TUN_1" #4: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP=>0xa2dc96fc <0x9f8a0876 xfrm=3DES_0-HMAC_MD5 NATOA=none NATD=none DPD=enabled}

Chapter 5 Appendix

5.1 Firmware Version

The configuration above was tested on the ROS with firmware version 2.0.6.

System Information

Device Model	R2000
System Uptime	0 days, 05:24:46
System Time	Fri Jan 1 05:24:36 2016 (NTP not updated)
Firmware Version	2.0.6 (Rev 466)
Hardware Version	1.1
Kernel Version	3.10.49
Serial Number	12345678901234

System Information

Device Model	R2000
System Uptime	0 days, 02:25:11
System Time	Fri Jan 1 02:24:59 2016 (NTP not updated)
Firmware Version	2.0.6 (Rev 466)
Hardware Version	1.1
Kernel Version	3.10.49
Serial Number	01440215100006