

9. VPN configuration

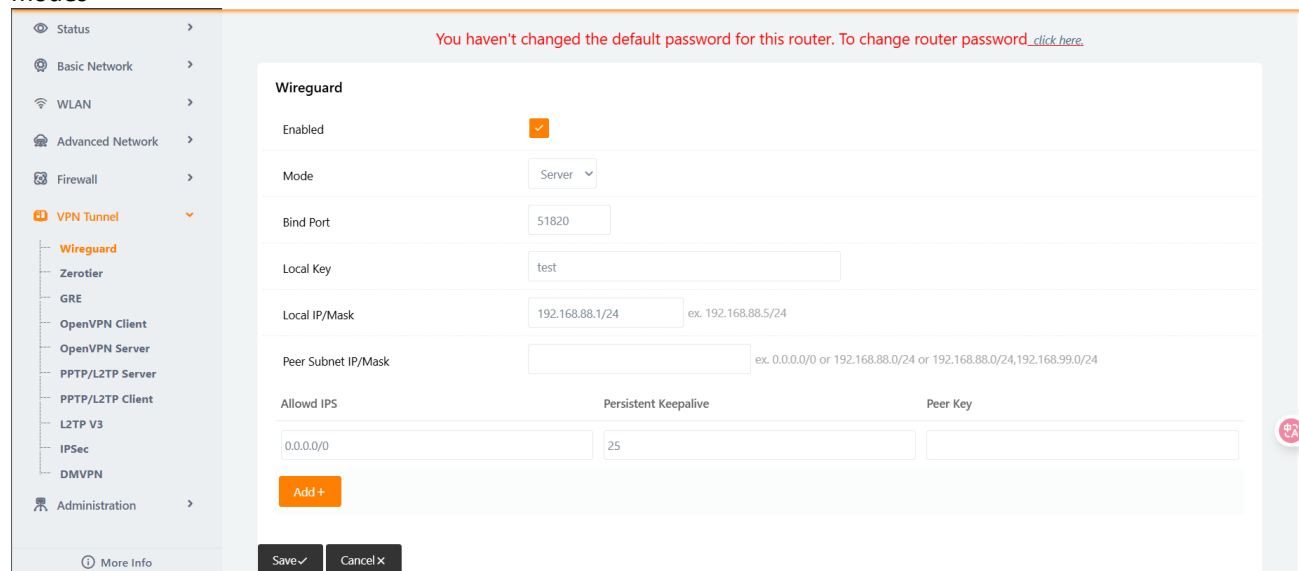
Virtual Private Network (VPN) is a secure Internet-based local area network (LAN) that currently supports Wireguard/Zerotier/L2TP/PPTP/GRE/openvpn/IPSEC/L2TP V3/DMVPN are used separately.

9.1. Wireguard

WireGuard is an easy-to-configure, fast, and secure open-source VPN that leverages the latest encryption technology. The goal is to provide a faster, simpler, and leaner general-purpose VPN that can be easily deployed on low-end devices like Raspberry Pi to high-end servers.

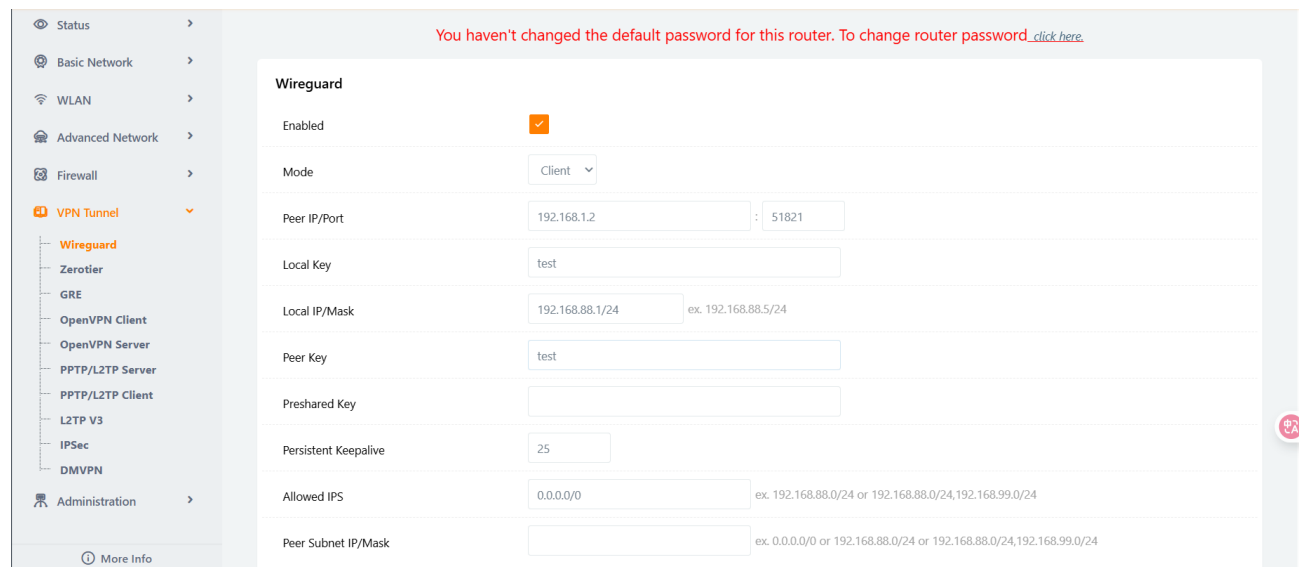
Since most other solutions like IPsec and OpenVPN were developed decades ago, realize that they are slow and difficult to configure and manage properly; Multi-platform support for Linux, Windows, macOS, BSD, iOS, and Android; Although wireguard is simple, it supports all the latest encryption technologies, such as the Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF, and secure trusted fabrics; And because WireGuard runs in kernel space, it provides a secure network at high speeds.

Step 1: Select "VPN Tunnel > Wireguard" in the navigation bar as shown in the image, which contains both server and client modes



The screenshot shows the router's web interface with the 'VPN Tunnel' menu expanded and 'Wireguard' selected. The configuration page for Wireguard is displayed, showing the 'Server' mode. The 'Enabled' checkbox is checked. The 'Mode' is set to 'Server'. The 'Bind Port' is 51820. The 'Local Key' is 'test'. The 'Local IP/Mask' is 192.168.88.1/24. The 'Peer Subnet IP/Mask' is empty. The 'Allowed IPS' is 0.0.0.0/0. The 'Persistent Keepalive' is 25. The 'Peer Key' is empty. There is an 'Add +' button at the bottom left of the configuration area. A red warning message at the top says: 'You haven't changed the default password for this router. To change router password [click here](#).' The left sidebar shows the navigation menu with 'VPN Tunnel' expanded and 'Wireguard' selected. The bottom of the sidebar has a 'More Info' link.

Figure 9-1



The screenshot shows the router's web interface with the 'VPN Tunnel' menu expanded and 'Wireguard' selected. The configuration page for Wireguard is displayed, showing the 'Client' mode. The 'Enabled' checkbox is checked. The 'Mode' is set to 'Client'. The 'Peer IP/Port' is 192.168.1.2 : 51821. The 'Local Key' is 'test'. The 'Local IP/Mask' is 192.168.88.1/24. The 'Peer Key' is 'test'. The 'Preshared Key' is empty. The 'Persistent Keepalive' is 25. The 'Allowed IPS' is 0.0.0.0/0. The 'Peer Subnet IP/Mask' is empty. There is an 'Add +' button at the bottom left of the configuration area. A red warning message at the top says: 'You haven't changed the default password for this router. To change router password [click here](#).' The left sidebar shows the navigation menu with 'VPN Tunnel' expanded and 'Wireguard' selected. The bottom of the sidebar has a 'More Info' link.

Figure 9-2

Step 2: Configure the wireguard parameter

The name of the parameter	meaning	How to configure
Enable Wireguard	Enable/disable the Wireguard feature	Click Enable to enable the feature
Mode	There are two modes: server and client	Select the appropriate mode for each application
Bind Port	In server mode, the listening port of the server	The default is 51820
Local key	In server mode, the private key of the server	Default: test The server's private key is paired with the public key
Local IP/Mask	In server mode, one wireguardVPN subnet and mask of the server are supported	Format: A.B.C.D/M Default: 192.168.88.1/24
Peer Subnet IP/Mask	In server mode, the client can have multiple WireGuard VPN subnets and masks	格式: A.B.C.D/M, E. F.G.H/N Default is empty
Allowd IPS	In server mode, the local subnet and mask of the client and the VPN subnet and mask of the client	格式: A.B.C.D/M, E. F.G.H/N Default: 0.0.0.0/0
Persistent Keepalive	Every once in a while, it will be checked if the connection is dropped	Default: 25 Unit: seconds
Peer key	In server mode, the client's public key	Default is empty The client's private key is paired with the public key
Peer IP/port	In client mode, the WAN port IP address and port number of the server	Port default: 192.168.1.2 Port default: 51821
Local key	In client mode, the private key of the client	Default: test It is paired with the public key set by the server
Local IP/Mask	In client mode, the VPN address and subnet of the client	Default: 192.168.88.1/24 The VPN address must be on the same network segment as the VPN address of the server, but the IP address is different
Peer key	In client mode, the server matches the public key	Default: test
Preshared key	The password of the client	Default is empty
Allowd IPS	In client mode, you can allow other IP addresses to access or connect to the device	Default: 0.0.0.0/0 The default setting means that all devices can access or connect
Peer Subnet IP/Mask	In client mode, the local IP address of the server or the local IP address and subnet of other clients	Default is empty Format: A.B.C.D/M, E. F.G.H/N

Table 9-1 WireGuard parameters

Step 3: Set other parameters for server mode

You haven't changed the default password for this router. To change router password [click here](#).

WAN / Internet

Type	Static Address
IP Address	192.168.10.155
Subnet Mask	255.255.255.0
Gateway	192.168.10.1
MTU	0 (0 for default)
Primary DNS	192.168.10.1
Secondary DNS	114.114.114.114

Figure 9-3

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440	✗	

1

Add +

DNS

Use Custom DNS ☐

Figure 9-4

Step 4: Configure the wireguard parameter in server mode

You haven't changed the default password for this router. To change router password [click here](#).

Wireguard

Enabled ☒

Mode: Server

Bind Port: 51820

Local Key: 0NFyuzEY5nNEkg0TYaPSmy1uPD8fc9AU7nCs8pEIGY= Server private key

Local IP/Mask: 192.168.88.1/24 ex. 192.168.88.5/24

Peer Subnet IP/Mask: 192.168.3.0/24, 192.168.4.0/24 Server VPN tunnel address (note: cannot be the same as LAN port address)

Allowed IPS: 192.168.68.2/32, 192.168.3.0/24 subnet of Client 1

192.168.68.4/32, 192.168.4.0/24 subnet of Client 2

Persistent Keepalive: 25

Peer Key: xQWzk3nq9vUeagkmdINzyFK1p/Sb6tBhX9toc1F7Byc= public key of Client 1

Mzto7A2ShKyslnNFDz+FsaGRRLung9ci8IqismWkGFK= public key of Client 2

0.0.0.0/0 public key of Client 1

Add +

Figure 9-5

Step 5: Set other parameters in client mode

Route Client 1:

WAN / Internet

Type: Static Address

IP Address: 192.168.10.125

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.1

MTU: 0 (0 for default)

Primary DNS: 192.168.10.1

Secondary DNS: 114.114.114.114

Figure 9-6

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.168.3.1	255.255.255.0	✓	192.168.3.2 - 254	1440	✗	

1

Add +

DNS

Use Custom DNS: ☐

Figure 9-7

Routing Client 2:

WAN / Internet

Type: Static Address

IP Address: 192.168.10.127

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.1

MTU: 0 (0 for default)

Primary DNS: 192.168.10.1

Secondary DNS: 114.114.114.114

Figure 9-1

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.168.4.1	255.255.255.0	✓	192.168.4.2 - 254	1440	✗	

1

Add +

DNS

Use Custom DNS

Figure 9-2

Step 6: Configure the wireguard parameter of the client (the mask of the client must be set to /24, which cannot be in the same subnet range as /32 set by the server).

Route Client 1:

Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Wireguard
ZeroTier
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration

You haven't changed the default password for this router. To change router password [click here](#).

Wireguard

Enabled

Mode
Client

Peer IP/Port
192.168.10.155 : 51820
Server WAN port IP/port

Local Key
/AAHE1BuHtpCgv/LGL9uKV5hFP2E1SHieq5ilUjgB30=
Client 1 Private Key

Local IP/Mask
192.168.88.2/24 ex. 192.168.88.5/24
VPN tunnel address for client 1

Peer Key
6KVbpd/or90D1xQ7og58trVfmdlgh+=UFGM4c5oGZ4Gc=
Server public key

Preshared Key

Persistent Keepalive
25

Allowed IPS
0.0.0.0/0 ex. 192.168.88.0/24 or 192.168.88.0/24, 192.168.99.0/24
Service terminal network

Peer Subnet IP/Mask
192.168.1.0/24 , 192.168.4.0/24
Subnet of Client 2

Figure 9-3

Routing Client 2:

Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Wireguard
ZeroTier
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration

You haven't changed the default password for this router. To change router password [click here](#).

Wireguard

Enabled

Mode
Client

Peer IP/Port
192.168.10.155 : 51820
Server WAN port IP/port

Local Key
QL64lgayFKuwWYHfSyzlHHfr2LTb+YpMltoonUJks2Y=
Client 2 Private Key

Local IP/Mask
192.168.88.4/24 ex. 192.168.88.5/24
VPN tunnel address for client 2

Peer Key
6KVbpd/or90D1xQ7og58trVfmdlgh+=UFGM4c5oGZ4Gc=
Server public key

Preshared Key

Persistent Keepalive
25

Allowed IPS
0.0.0.0/0 ex. 192.168.88.0/24 or 192.168.88.0/24, 192.168.99.0/24
Service terminal network

Peer Subnet IP/Mask
192.168.1.0/24 192.168.3.0/24
Subnet of Client 2

Figure 9-4

Step 7: The connection is as follows

<https://www.wtiwireless.com/>

109 /

WTIwireless

The telnet of the server enters the background and you can view the connection status and route table information

```

21/08/2024 10:07:04 /home/mobaxterm telnet 192.168.1.1 2323
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Router login: root
Password:

root@Router:/tmp/home/root# wg
interface: wg0
  public key: 6KVbpd/oz90D1zQ7og58trVFmdbjh+UFGX4c5oGZ4Gc=
  private key: (hidden)
  listening port: 51820

peer: aQWzk3nq9vUeqpkmdINzyFk1p/SbeIbBhXHoc1F78yc=
  endpoint: 192.168.10.125:19880
  allowed ips: 192.168.88.2/32, 192.168.3.0/24
  latest handshake: 1 minute, 45 seconds ago
  transfer: 3.55 KiB received, 2.48 KiB sent
  persistent keepalive: every 25 seconds

peer: Mzto7A2ShKyslnNFDz+FsA6RRUng9cI8JqislmWkGFk=
  endpoint: 192.168.10.127:3077
  allowed ips: 192.168.88.4/32, 192.168.4.0/24
  latest handshake: 1 minute, 55 seconds ago
  transfer: 69.77 KiB received, 26.40 KiB sent
  persistent keepalive: every 25 seconds

```

Client1

Client2

Figure 9-5

```

root@Router:/tmp/home/root# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.2.240.1 0.0.0.0 UG 0 0 0 usb0
10.2.240.0 0.0.0.0 255.255.255.0 U 0 0 0 usb0
10.2.240.1 0.0.0.0 255.255.255.255 UH 0 0 0 usb0
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 lo
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 br0
192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0
192.168.4.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0
192.168.10.0 0.0.0.0 255.255.255.0 U 0 0 0 vlan2
192.168.88.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0

```

Figure 9-6

In server mode, you can ping the vpn addresses, gateways, and subnet IPs of both clients on the PC side

```

root@Router:/tmp/home/root# ping 192.168.88.2
PING 192.168.88.2 (192.168.88.2): 56 data bytes
64 bytes from 192.168.88.2: seq=0 ttl=64 time=1.243 ms
64 bytes from 192.168.88.2: seq=1 ttl=64 time=1.002 ms
64 bytes from 192.168.88.2: seq=2 ttl=64 time=0.972 ms
64 bytes from 192.168.88.2: seq=3 ttl=64 time=0.963 ms
64 bytes from 192.168.88.2: seq=4 ttl=64 time=0.975 ms
64 bytes from 192.168.88.2: seq=5 ttl=64 time=1.004 ms
^C
--- 192.168.88.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.963/1.026/1.243 ms

root@Router:/tmp/home/root# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: seq=0 ttl=64 time=1.171 ms
64 bytes from 192.168.3.1: seq=1 ttl=64 time=0.975 ms
64 bytes from 192.168.3.1: seq=2 ttl=64 time=0.942 ms
64 bytes from 192.168.3.1: seq=3 ttl=64 time=0.943 ms
64 bytes from 192.168.3.1: seq=4 ttl=64 time=0.977 ms
^C
--- 192.168.3.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.942/1.001/1.171 ms

root@Router:/tmp/home/root# ping 192.168.3.195
PING 192.168.3.195 (192.168.3.195): 56 data bytes
64 bytes from 192.168.3.195: seq=0 ttl=127 time=1.566 ms
64 bytes from 192.168.3.195: seq=1 ttl=127 time=1.262 ms
64 bytes from 192.168.3.195: seq=2 ttl=127 time=1.276 ms
64 bytes from 192.168.3.195: seq=3 ttl=127 time=1.310 ms

```

Client 1 VPN Address

Subnet and Gateway of Client 1

Figure 9-7

```

root@Router:/tmp/home/root# ping 192.168.88.4
PING 192.168.88.4 (192.168.88.4): 56 data bytes
64 bytes from 192.168.88.4: seq=0 ttl=64 time=1.103 ms
64 bytes from 192.168.88.4: seq=1 ttl=64 time=0.984 ms
64 bytes from 192.168.88.4: seq=2 ttl=64 time=0.992 ms
64 bytes from 192.168.88.4: seq=3 ttl=64 time=0.988 ms
^C
--- 192.168.88.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.984/1.016/1.103 ms

root@Router:/tmp/home/root# ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1): 56 data bytes
64 bytes from 192.168.4.1: seq=0 ttl=64 time=1.177 ms
64 bytes from 192.168.4.1: seq=1 ttl=64 time=2.672 ms
64 bytes from 192.168.4.1: seq=2 ttl=64 time=0.919 ms
64 bytes from 192.168.4.1: seq=3 ttl=64 time=0.973 ms
64 bytes from 192.168.4.1: seq=4 ttl=64 time=0.950 ms
^C
--- 192.168.4.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.919/1.338/2.672 ms

root@Router:/tmp/home/root# ping 192.168.4.195
PING 192.168.4.195 (192.168.4.195): 56 data bytes
64 bytes from 192.168.4.195: seq=0 ttl=127 time=1.599 ms
64 bytes from 192.168.4.195: seq=1 ttl=127 time=1.344 ms
64 bytes from 192.168.4.195: seq=2 ttl=127 time=1.298 ms
64 bytes from 192.168.4.195: seq=3 ttl=127 time=1.305 ms
^C
--- 192.168.4.195 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss

```

Client 2 VPN address

Client 2 subnet and gateway

Figure 9-8

The telnet client enters the background and can view the connection status and route table information

Client 1:

```

root@Router:/tmp/home/root# wg show
interface: wg0
  public key: aQWzk3nq9vUeqpkmdINzyFk1p/SbeIbBhXHoc1F78yc=
  private key: (hidden)
  listening port: 26277

peer: 6KVbpd/oz90D1zQ7og58trVFmdbhj+UFGX4c5oGZ4Gc=
  endpoint: 192.168.10.155:51820
  allowed ips: 0.0.0.0/0
  latest handshake: 1 minute, 36 seconds ago
  transfer: 4.43 KiB received, 6.20 KiB sent
  persistent keepalive: every 25 seconds
root@Router:/tmp/home/root#

```

Figure 9-9

```

root@Router:/tmp/home/root# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.10.1 0.0.0.0 UG 0 0 0 wlan2
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 lo
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0
192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 br0
192.168.4.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0
192.168.10.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan2
192.168.10.1 0.0.0.0 255.255.255.255 UH 0 0 0 wlan2
192.168.88.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0

```

Figure 9-10

Client 1 can ping the VPN address, gateway and subnet IP address of the server (including the ping packet on the PC)

```

root@Router:/tmp/home/root# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1): 56 data bytes
64 bytes from 192.168.88.1: seq=0 ttl=64 time=1.288 ms
64 bytes from 192.168.88.1: seq=1 ttl=64 time=0.958 ms
64 bytes from 192.168.88.1: seq=2 ttl=64 time=1.016 ms
64 bytes from 192.168.88.1: seq=4 ttl=64 time=1.079 ms
64 bytes from 192.168.88.1: seq=5 ttl=64 time=0.997 ms
^C
--- 192.168.88.1 ping statistics ---
5 packets transmitted, 5 packets received, 16% packet loss
round-trip min/avg/max = 0.958/1.067/1.288 ms

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.156 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.000 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.933 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.966 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.935 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.933/0.998/1.156 ms

root@Router:/tmp/home/root# ping 192.168.1.37
PING 192.168.1.37 (192.168.1.37): 56 data bytes
64 bytes from 192.168.1.37: seq=0 ttl=127 time=1.415 ms
64 bytes from 192.168.1.37: seq=1 ttl=127 time=1.301 ms
64 bytes from 192.168.1.37: seq=2 ttl=127 time=1.247 ms
64 bytes from 192.168.1.37: seq=3 ttl=127 time=1.285 ms
64 bytes from 192.168.1.37: seq=4 ttl=127 time=1.302 ms
^C

```

Server VPN address

Server subnet and gateway

Figure 9-11

Client 2:

```

root@Router:/tmp/home/root# wg
interface: wg0
  public key: Mzto7A2ShKyslnNFDz+FsA6RRUng9cI8JqislMwKGFk=
  private key: (hidden)
  listening port: 47384

peer: 6KVbpd/oz90D1zQ7og58trVFmdbjh+UFGX4c5oGZ4Gc=
  endpoint: 192.168.10.155:51820
  allowed ips: 0.0.0.0/0
  latest handshake: 1 minute, 22 seconds ago
  transfer: 9.18 KiB received, 34.07 KiB sent
  persistent keepalive: every 25 seconds
root@Router:/tmp/home/root#

```

Figure 9-12

```

root@Router:/tmp/home/root# route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          192.168.10.1   0.0.0.0        UG    0      0      0   wlan2
127.0.0.0        0.0.0.0        255.0.0.0      U      0      0      0    lo
192.168.1.0       0.0.0.0        255.255.255.0  U      0      0      0   wg0
192.168.3.0       0.0.0.0        255.255.255.0  U      0      0      0   wg0
192.168.4.0       0.0.0.0        255.255.255.0  U      0      0      0   br0
192.168.10.0      0.0.0.0        255.255.255.0  U      0      0      0   wlan2
192.168.10.1     0.0.0.0        255.255.255.255 UH     0      0      0   wlan2
192.168.88.0     0.0.0.0        255.255.255.0  U      0      0      0   wg0

```

Figure 9-13

Client 2 can ping the VPN address, gateway and subnet IP address of the server (including the ping packet on the PC).

```

root@Router:/tmp/home/root# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1): 56 data bytes
64 bytes from 192.168.88.1: seq=0 ttl=64 time=1.288 ms
64 bytes from 192.168.88.1: seq=1 ttl=64 time=0.958 ms
64 bytes from 192.168.88.1: seq=2 ttl=64 time=1.016 ms
64 bytes from 192.168.88.1: seq=4 ttl=64 time=1.079 ms
64 bytes from 192.168.88.1: seq=5 ttl=64 time=0.997 ms
^C
--- 192.168.88.1 ping statistics ---
5 packets transmitted, 5 packets received, 16% packet loss
round-trip min/avg/max = 0.958/1.067/1.288 ms

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.156 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.000 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.933 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.966 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.935 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.933/0.998/1.156 ms

root@Router:/tmp/home/root# ping 192.168.1.37
PING 192.168.1.37 (192.168.1.37): 56 data bytes
64 bytes from 192.168.1.37: seq=0 ttl=127 time=1.415 ms
64 bytes from 192.168.1.37: seq=1 ttl=127 time=1.301 ms
64 bytes from 192.168.1.37: seq=2 ttl=127 time=1.247 ms
64 bytes from 192.168.1.37: seq=3 ttl=127 time=1.285 ms
64 bytes from 192.168.1.37: seq=4 ttl=127 time=1.302 ms
^C

```

Server VPN address

Server subnet and gateway

Figure 9-14

Client 1 or Client 2 pings the peer (including the PC side).

Client 1:

```

PING 192.168.88.4 (192.168.88.4): 56 data bytes
64 bytes from 192.168.88.4: seq=0 ttl=63 time=1.652 ms
64 bytes from 192.168.88.4: seq=1 ttl=63 time=1.594 ms
64 bytes from 192.168.88.4: seq=2 ttl=63 time=1.549 ms
64 bytes from 192.168.88.4: seq=3 ttl=63 time=1.576 ms
^C
--- 192.168.88.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.549/1.642/1.852 ms

root@Router:/tmp/home/root# ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1): 56 data bytes
64 bytes from 192.168.4.1: seq=0 ttl=63 time=1.987 ms
64 bytes from 192.168.4.1: seq=1 ttl=63 time=1.638 ms
64 bytes from 192.168.4.1: seq=2 ttl=63 time=1.587 ms
^C
--- 192.168.4.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.587/1.737/1.987 ms

root@Router:/tmp/home/root# ping 192.168.4.195
PING 192.168.4.195 (192.168.4.195): 56 data bytes
64 bytes from 192.168.4.195: seq=0 ttl=126 time=2.962 ms
64 bytes from 192.168.4.195: seq=1 ttl=126 time=2.155 ms
64 bytes from 192.168.4.195: seq=2 ttl=126 time=2.112 ms
64 bytes from 192.168.4.195: seq=3 ttl=126 time=2.082 ms
^C
--- 192.168.4.195 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.082/2.327/2.962 ms

```

Client2 VPN address

Client2 subnet and gateway

Figure 9-15

Client 2:

```

root@Router:/tmp/home/root# ping 192.168.88.2
PING 192.168.88.2 (192.168.88.2): 56 data bytes
64 bytes from 192.168.88.2: seq=0 ttl=63 time=1.901 ms
64 bytes from 192.168.88.2: seq=1 ttl=63 time=1.591 ms
64 bytes from 192.168.88.2: seq=2 ttl=63 time=1.667 ms
64 bytes from 192.168.88.2: seq=3 ttl=63 time=1.657 ms
^C
--- 192.168.88.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.591/1.704/1.901 ms

root@Router:/tmp/home/root# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: seq=0 ttl=63 time=1.912 ms
64 bytes from 192.168.3.1: seq=1 ttl=63 time=1.716 ms
64 bytes from 192.168.3.1: seq=2 ttl=63 time=1.705 ms
^C
--- 192.168.3.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.705/1.777/1.912 ms

root@Router:/tmp/home/root# ping 192.168.3.195
PING 192.168.3.195 (192.168.3.195): 56 data bytes
64 bytes from 192.168.3.195: seq=0 ttl=126 time=2.461 ms
64 bytes from 192.168.3.195: seq=1 ttl=126 time=2.211 ms
64 bytes from 192.168.3.195: seq=2 ttl=126 time=2.028 ms
^C
--- 192.168.3.195 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.028/2.233/2.461 ms

root@Router:/tmp/home/root#

```

Figure 9-16

9.2. Zerotier

ZeroTier is a software-defined networking (SDN) solution that enables users to create and manage virtual networks across physical devices and locations. It enables seamless connection of devices on the Internet, suitable for remote work, Internet of Things and other scenarios, providing secure and efficient network connectivity.

Step 1: Select "VPN Tunnel > Zerotier" in the navigation bar

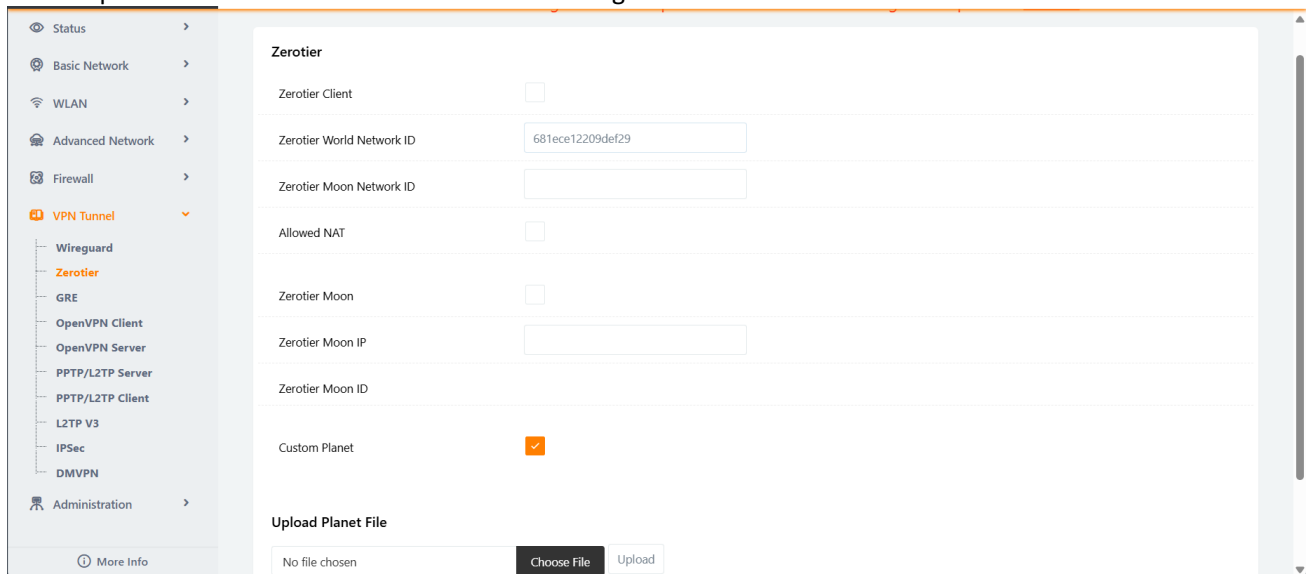


Figure 9-17

Zerotier Parameter Description:

parameter	meaning	How to configure
Enable Zerotier	Enable/disable the Zerotier feature	Click 'Enable' to enable the feature save to
Zerotier World Network ID	The network ID of the root node of the ZeroTier	
Zerotier Moon Network ID	This is the network ID of the ZeroTier proxy node	

Automatically allow client NAT	To enable this function, you need to use it in conjunction with the IP management table of ZeroTier to allow access to other ZeroTier clients, and the IP address is the LAN CIDR block address of other ZeroTier clients. The gateway is the vpn address of the other ZeroTier client, and the IP address and gateway must correspond to the same route.	
Enable the ZeroTier Moon server	Enable/disable the Zerotier Moon server feature	Click 'Enable' to enable the feature save to
ZeroTier Moon Server IP	Enter the IP address of the Moonnode	
ZeroTier Moon server ID	Enter the ID of the Megaonnode	
Customize Planet	Enable/Disable indicates whether or not to use the custom Planet service	Click Enable to save to enable the feature
Upload the Planet file	Uploading a Planet file means uploading a Planet file on a custom server, and not uploading a file means that the official root node is used by default	

Table 9-1

Example of using a custom Planet:

Step 1: The first time you use a custom Planet, you need to import the Planet file, and you need to enable the custom Planet function, after importing the file, you need to re-save the settings to make the Planet file take effect, after the first import is successful, enter the background `cd /tmp/etc/storage` directory, you can view the Planet file, after the power is off and restarted, the Planet file has been written into the nvram parameter.

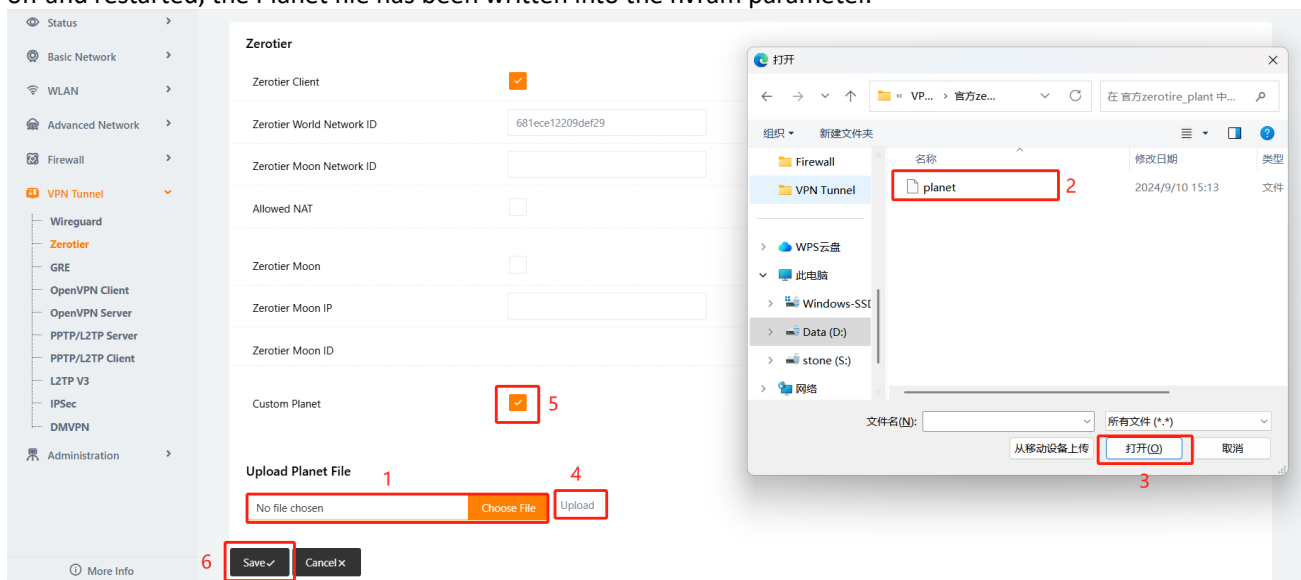


Figure 9-18

```

root@Router:/tmp/home/root#
root@Router:/tmp/home/root# cd /tmp/etc/
root@Router:/tmp/etc# ls
TZ
Wireless      dnsmasq      group         igmp.conf     iptables      openssl.cnf   resolv.conf   shadow        swanctl       zebra.conf
cli.conf      dnsmasq.conf gshadow       iproute2      ld.so.conf    passwd        resolv.dnsmasq storage        vpn           wg_cli_pub.key
detran.cfg    ethertypes   hosts         ipsec.conf    ld.so.conf    profile       rpd.conf     strongswan.conf wg_cli_pub.key
root@Router:/tmp/etc#
root@Router:/tmp/etc# cd storage/
root@Router:/tmp/etc/storage# ls
planet        zerotier-one
root@Router:/tmp/etc/storage#
root@Router:/tmp/etc/storage#
root@Router:/tmp/etc/storage#
root@Router:/tmp/etc/storage#

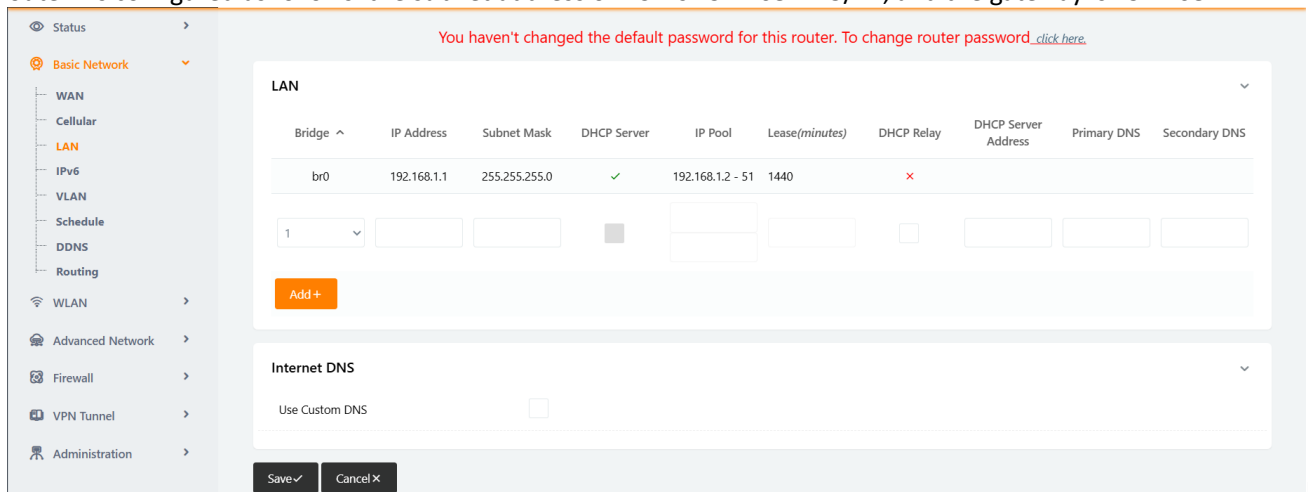
```

Figure 9-19

Step 2: Use two routers, Router1 and Router2. Two PCs, PC1 and PC2;

Router1 is connected to PC1, and Router2 is connected to PC2.

Router1 is configured as follows: the subnet address of PC1 is 192.168.1.25/24, and the gateway is 192.168.1.1



Figure

9-20

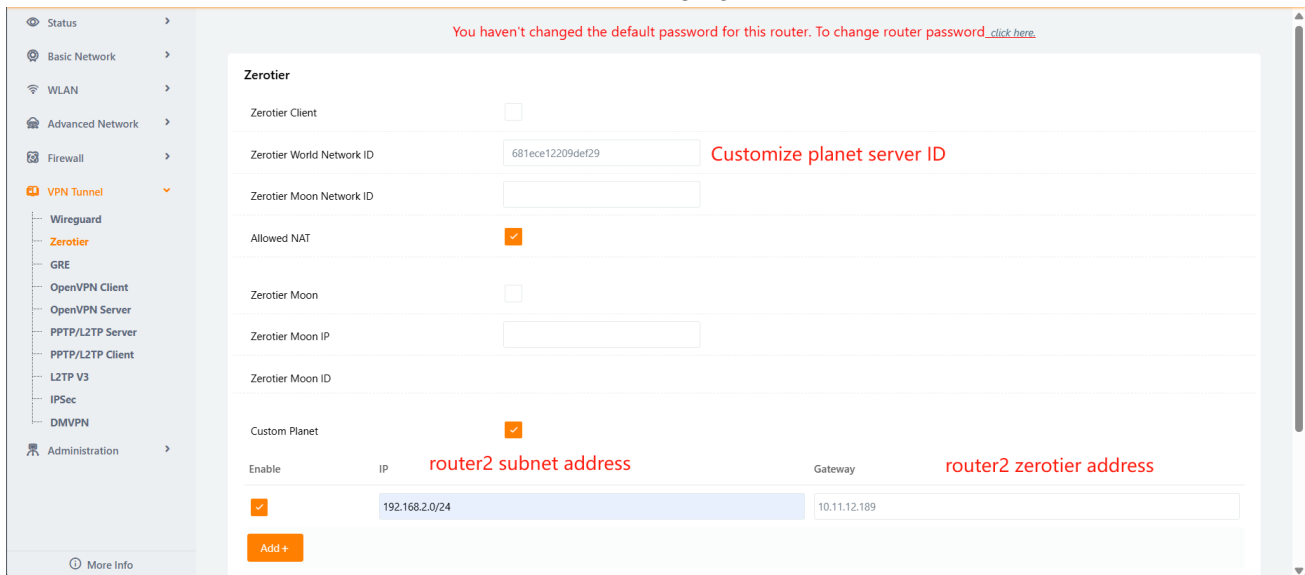


Figure 9-21

Router2 is configured as follows: PC2 has a subnet address of 192.168.2.35/24 and a gateway of 192.168.2.1

You haven't changed the default password for this router. To change router password [click here](#).

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address	Primary DNS	Secondary DNS
br0	192.168.2.1	255.255.255.0	✓	192.168.2.2 - 51	1440	✗			

1 ☐ ☐

[Add +](#)

Internet DNS

Use Custom DNS ☐

[Save ✓](#) [Cancel ✗](#)

Figure

9-22

You haven't changed the default password for this router. To change router password [click here](#).

Zerotier

Zerotier Client ☒

Zerotier World Network ID [Customize planet server ID](#)

Zerotier Moon Network ID

Allowed NAT ☒

Zerotier Moon ☐

Zerotier Moon IP

Zerotier Moon ID

Custom Planet ☒

Enable	IP	Gateway
✓	192.168.1.0/24	10.11.12.37

[Add +](#)

Figure 9-23

Step 3: Check the connection status

Enter the backend of Router1 and Router2 respectively, and ifconfig can also view and obtain the address

```
usb0      Link encap:Ethernet  HWaddr DE:07:B4:3D:02:30
          inet addr:10.66.55.31  Mask:255.255.255.192
          UP RUNNING NOARP MULTICAST  MTU:1400  Metric:1
          RX packets:78290 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60320 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:92205309 (87.9 MiB)  TX bytes:6437284 (6.1 MiB)

vlan1     Link encap:Ethernet  HWaddr 34:0A:51:32:33:61
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:217012 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21416 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17288035 (16.4 MiB)  TX bytes:7244639 (6.9 MiB)

ztpi7fh7ij Link encap:Ethernet  HWaddr 2A:C5:C6:CF:35:B8      Router1
          inet addr:10.11.12.37  Bcast:10.11.12.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:2800  Metric:1
          RX packets:1468 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1084 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:1553048 (1.4 MiB)  TX bytes:125833 (122.8 KiB)

root@Router:/tmp/home/root#
```

Figure 9-24

```
usb0      Link encap:Ethernet  HWaddr 9E:C4:C8:48:22:D7
          inet addr:10.18.75.234  Bcast:10.18.75.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7794 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18027 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2393128 (2.2 MiB)  TX bytes:4498395 (4.2 MiB)

vlan1     Link encap:Ethernet  HWaddr 30:3D:51:11:B2:55
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:32689 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13317 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3351346 (3.1 MiB)  TX bytes:3530408 (3.3 MiB)

ztpi7fh7ij Link encap:Ethernet  HWaddr 2A:5B:39:34:B1:59      Router2
          inet addr:10.11.12.189  Bcast:10.11.12.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:2800  Metric:1
          RX packets:1147 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1466 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:132091 (128.9 KiB)  TX bytes:1568220 (1.4 MiB)

root@Router:/tmp/home/root#
```

Figure 9-25

After NAT is configured, both devices can ping the peer gateway and subnet addresses on the PC and the router Router1, PC1 ping:

```

root@Router:/tmp/home/root#
root@Router:/tmp/home/root#
root@Router:/tmp/home/root#
root@Router:/tmp/home/root# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=64 time=118.049 ms
64 bytes from 192.168.2.1: seq=1 ttl=64 time=115.918 ms
64 bytes from 192.168.2.1: seq=2 ttl=64 time=157.476 ms
64 bytes from 192.168.2.1: seq=3 ttl=64 time=97.071 ms
64 bytes from 192.168.2.1: seq=4 ttl=64 time=95.434 ms
^C
--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 95.434/116.789/157.476 ms

root@Router:/tmp/home/root# ping 192.168.2.35
PING 192.168.2.35 (192.168.2.35): 56 data bytes
64 bytes from 192.168.2.35: seq=0 ttl=127 time=131.753 ms
64 bytes from 192.168.2.35: seq=1 ttl=127 time=89.171 ms
64 bytes from 192.168.2.35: seq=2 ttl=127 time=69.050 ms
64 bytes from 192.168.2.35: seq=3 ttl=127 time=115.275 ms
64 bytes from 192.168.2.35: seq=4 ttl=127 time=112.699 ms
^C
--- 192.168.2.35 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 69.050/103.589/131.753 ms

root@Router:/tmp/home/root#

```

Router1

Figure 9-26

```

19/06/2024 10:23.27 /home/mobaxterm ping 192.168.2.1

正在 Ping 192.168.2.1 具有 32 字节的数据:
来自 192.168.2.1 的回复: 字节=32 时间=152ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=78ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=83ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=147ms TTL=63

192.168.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 78ms, 最长 = 152ms, 平均 = 115ms

19/06/2024 11:45.41 /home/mobaxterm ping 192.168.2.35

正在 Ping 192.168.2.35 具有 32 字节的数据:
来自 192.168.2.35 的回复: 字节=32 时间=97ms TTL=126
来自 192.168.2.35 的回复: 字节=32 时间=102ms TTL=126
来自 192.168.2.35 的回复: 字节=32 时间=76ms TTL=126
来自 192.168.2.35 的回复: 字节=32 时间=77ms TTL=126

192.168.2.35 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 76ms, 最长 = 102ms, 平均 = 88ms

```

PC1

Figure 9-27

Router2, PC2 ping:

```

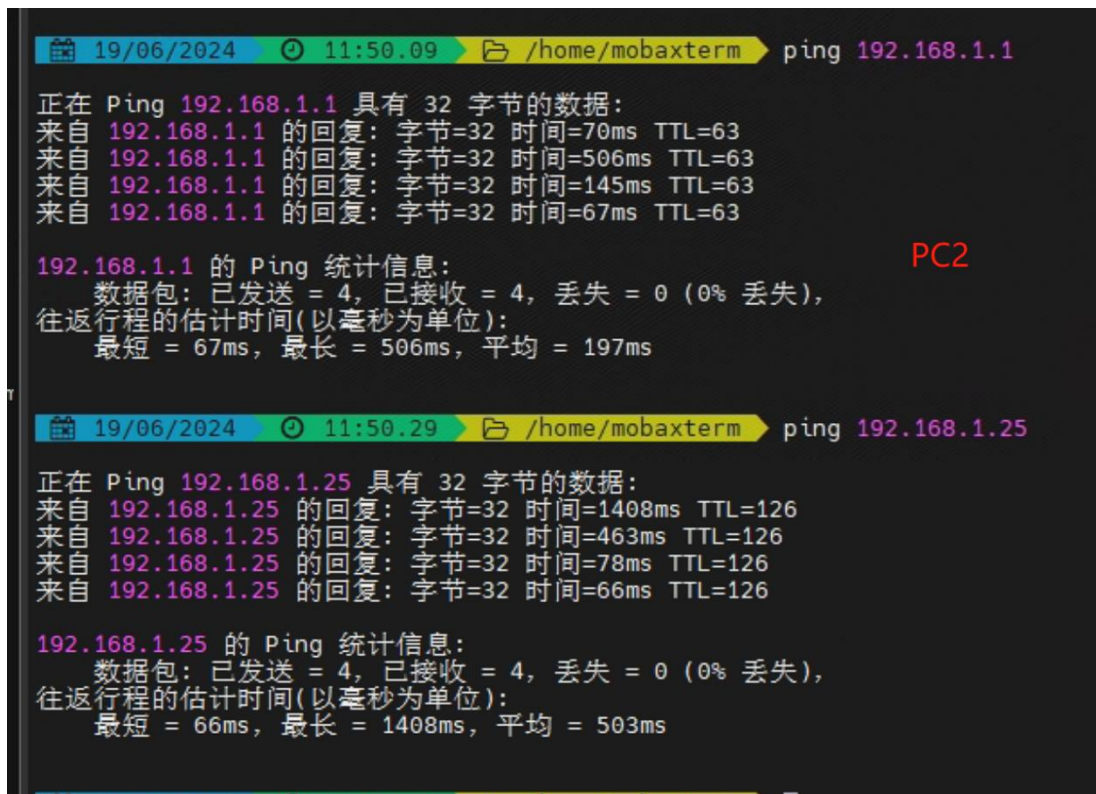
root@Router:/tmp/home/root#
root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=95.862 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=72.544 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=122.445 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=58.510 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 58.510/87.340/122.445 ms

root@Router:/tmp/home/root# ping 192.168.1.25 Router2
PING 192.168.1.25 (192.168.1.25): 56 data bytes
64 bytes from 192.168.1.25: seq=0 ttl=127 time=152.327 ms
64 bytes from 192.168.1.25: seq=1 ttl=127 time=142.216 ms
64 bytes from 192.168.1.25: seq=2 ttl=127 time=76.966 ms
64 bytes from 192.168.1.25: seq=3 ttl=127 time=111.470 ms
64 bytes from 192.168.1.25: seq=4 ttl=127 time=698.566 ms
^C
--- 192.168.1.25 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 76.966/236.309/698.566 ms

root@Router:/tmp/home/root#

```

Figure 9-28



```

19/06/2024 11:50.09 /home/mobaxterm ping 192.168.1.1
正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=70ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=506ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=145ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=67ms TTL=63

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 67ms, 最长 = 506ms, 平均 = 197ms

19/06/2024 11:50.29 /home/mobaxterm ping 192.168.1.25
正在 Ping 192.168.1.25 具有 32 字节的数据:
来自 192.168.1.25 的回复: 字节=32 时间=1408ms TTL=126
来自 192.168.1.25 的回复: 字节=32 时间=463ms TTL=126
来自 192.168.1.25 的回复: 字节=32 时间=78ms TTL=126
来自 192.168.1.25 的回复: 字节=32 时间=66ms TTL=126

192.168.1.25 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 66ms, 最长 = 1408ms, 平均 = 503ms

```

Figure 9-29

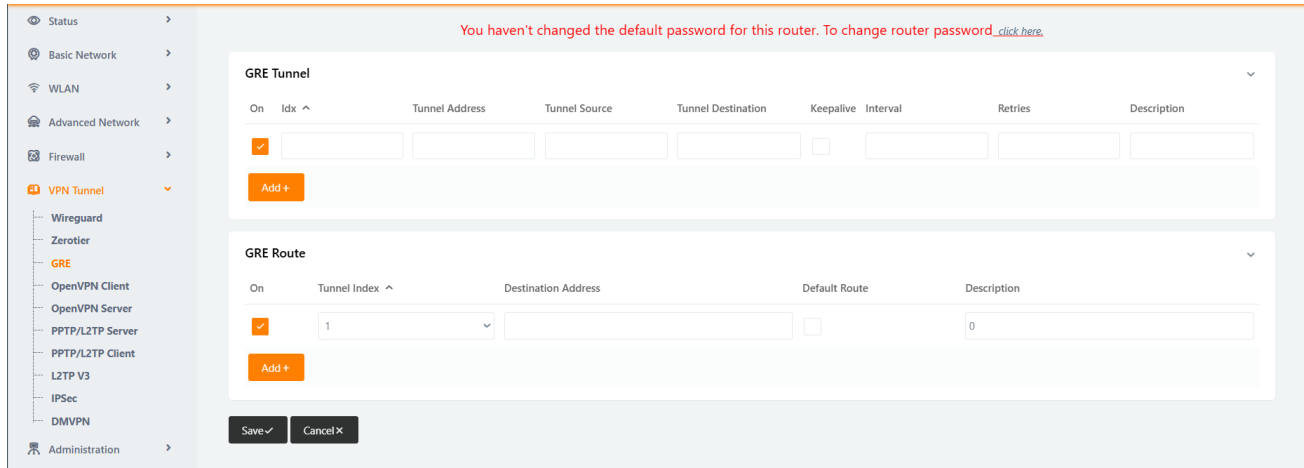
9.3. GRE setting

Tunneling technology is a way of passing data between networks through an interconnected network infrastructure. The <https://www.wtiwireless.com/> 120 / WTIwireless

logical path that the encapsulated packet travels through as it travels over the public Internet throughout the delivery process is called a tunnel.

GRE (Generic Routing Encapsulation) specifies how one network protocol is used to encapsulate another. There are two main uses of the GRE protocol: internal protocol encapsulation and private address encapsulation.

Step 1: Select "VPN Tunnel > GRE Settings" in the navigation bar, as shown in Figure 9-1



The screenshot shows the router's configuration page for GRE settings. On the left is a navigation menu with options like Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel (selected), Wireguard, ZeroTier, GRE, OpenVPN Client, OpenVPN Server, PPTP/L2TP Server, PPTP/L2TP Client, L2TP V3, IPSec, DMVPN, and Administration. The main content area has a red warning at the top: "You haven't changed the default password for this router. To change router password [click here](#)." Below this are two sections: "GRE Tunnel" and "GRE Route". The "GRE Tunnel" section has a table with columns: On, Idx, Tunnel Address, Tunnel Source, Tunnel Destination, Keepalive, Interval, Retries, and Description. The "On" checkbox is checked. Below the table is an "Add +" button. The "GRE Route" section has a table with columns: On, Tunnel Index, Destination Address, Default Route, and Description. The "On" checkbox is checked, "Tunnel Index" is set to 1, and "Description" is 0. Below the table is an "Add +" button. At the bottom are "Save ✓" and "Cancel ✕" buttons.

Figure 9-30

Step 2: GRE Mode Parameters

parameter	meaning	How to configure
ON/OFF GRE	ON/OFF the IP Tunnel Service	Click Enable to enable the tunnel rule
Tunnel address	The virtual IP address of the local tunnel	Enter the virtual IP address of the local GRE tunnel. Format: Interface A.B.C.D
Tunnel Source	Set the IP address of the public network or WAN port of the machine	Enter the IP address of the external interface of the local network of the tunnel. Format: A.B.C.D
Tunnel Destination	The external interface IP address of the tunnel peer network is usually the public IP (Internet) address, but it can also be the internal IP address of the enterprise	Enter the IP address of the external interface of the tunnel peer network Format: A.B.C.D. interface type
Destination address	Set the destination address of the peer	Format: A.B.C.D/M

Table 9-2 GRE Mode Parameter Configuration

Step 3: Once the configuration is complete, click the "Save Settings" button for the configuration to take effect.

Example:

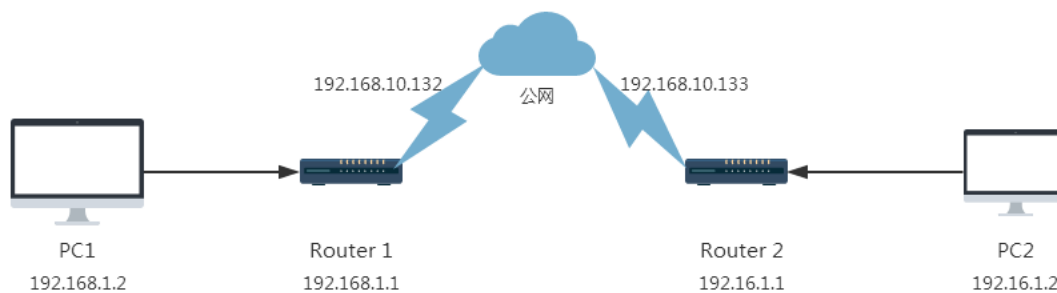


Figure 9-31

Router1 configuration:

GRE Tunnel

On	Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	3	192.168.1.1	192.168.10.69	192.168.10.67	✓	3	10	

☒ ☐

Add +

GRE Route

On	Tunnel Index ^	Destination Address	Default Route	Description
✓	3	192.168.2.0/24	✓	0

☒ 1 ☐ 0

Add +

Figure 9-32

Router2 configuration:

GRE Tunnel

On	Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	3	192.168.2.1	192.168.10.67	192.168.10.69	✓	3	10	

☒ ☐

Add +

GRE Route

On	Tunnel Index ^	Destination Address	Description
✓	3	192.168.1.0/24	

☒ 1

Add +

Figure 9-33

Router1 can be pinged from PC2

```
root@LTE_Quectel:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.828 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.661 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.642 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.629 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.636 ms
^C
```

Figure 9-34

Router1 can be pinged from PC2

```
23/08/2024 16:08.04 /home/mobaxterm ping 192.168.2.1

正在 Ping 192.168.2.1 具有 32 字节的数据:
来自 192.168.2.1 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=3ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63

192.168.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 3ms, 平均 = 1ms
```

Figure 9-35

9.4. OpenVPN client

OpenVPN is an application-layer VPN implementation based on the OpenSSL library, which is a virtual private tunnel that provides a secure data transmission between enterprises or between individuals and companies. OpenVPN allows a single point of participation in the establishment of a VPN using a shared key, e-certificate, or username/password for authentication.

Step 1: Select "VPN Tunnel > OpenVPN Client" in the navigation bar.

Step 2: Openvpn configuration is divided into four configurations

Basic settings

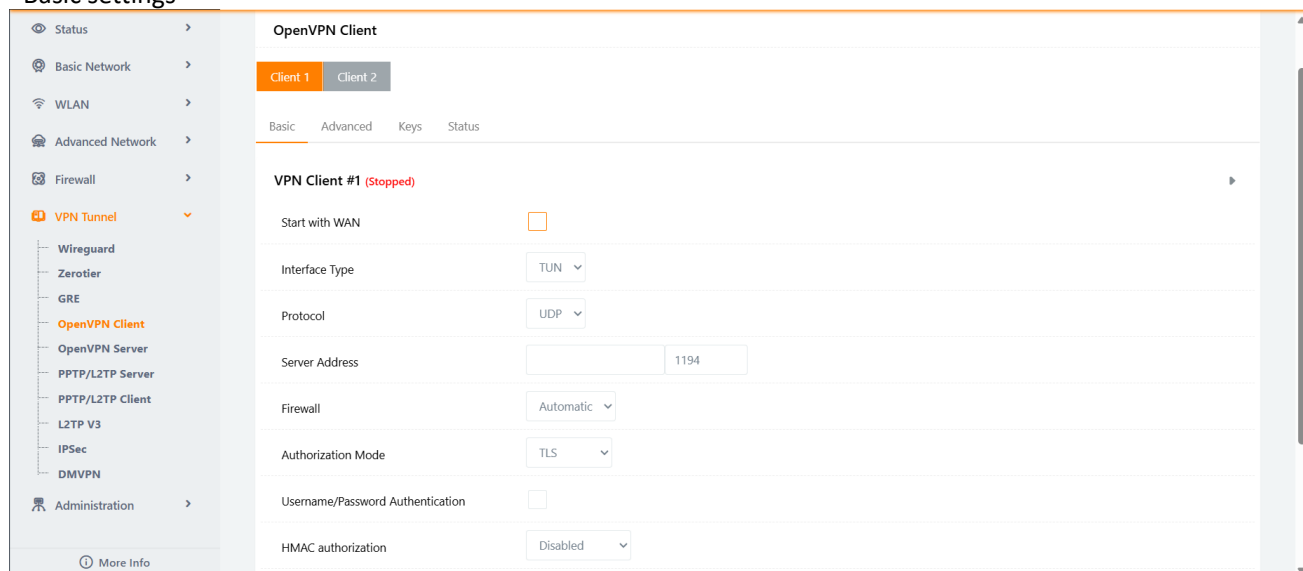


Figure 9-36

Basic Parameter Configuration Description:

The name of the parameter	meaning	How to configure
Start with WAN	Whether the network is over a WAN port	ON/OFF

Interface type	The difference between TUN and TAP is that a TUN device is a point-to-point virtual appliance at the network layer, while TAP is a virtual appliance at the Ethernet link layer. TAP mode: Openvpn bridging mode TUN mode: openvpn tunnel mode	Drop-down to select TAP mode or TUN mode
Protocol	TCP mode or UDP mode	Select TCP mode or UDP mode from the drop-down list
Server address/port	Server subnet configuration, including IP address and port	You need to fill in the subnet address and port of the server. Format: A.B.C.D; port number
firewall	Firewall modes, including automatic and custom	Select Automatic or Custom from the drop-down list
Authorization Mode	The authentication types include TLS, static key, and custom	Select TLS, static key, or custom from the drop-down drop-down
Username/password authentication	Whether to enable username/password authentication	Enabled or not enabled
Username	Appears when the username/password feature is enabled	Enter the username configured on the server
password	Appears when the username/password feature is enabled	Enter the password configured on the server
Username Authen. Only	If the server does not have a password, it can be enabled without entering the password	Enable or disable
HMAC Certified	Hash message authentication: Default: Disabled, Bi- directional Incoming Outgoing	Enable or select one of the modes
Server is on the same subnet	Appears when TAP is selected for Interface Type	Enable or disable
Create NAT on tunnel	When the interface type is selected as TUN, click the toggle button to enable/disable the NAT (Network Address Translation) feature. When enabled, the host IP address behind the router will be encapsulated.	Enable or disable

Table 9-3 OpenVPN parameter configuration

Advanced settings:

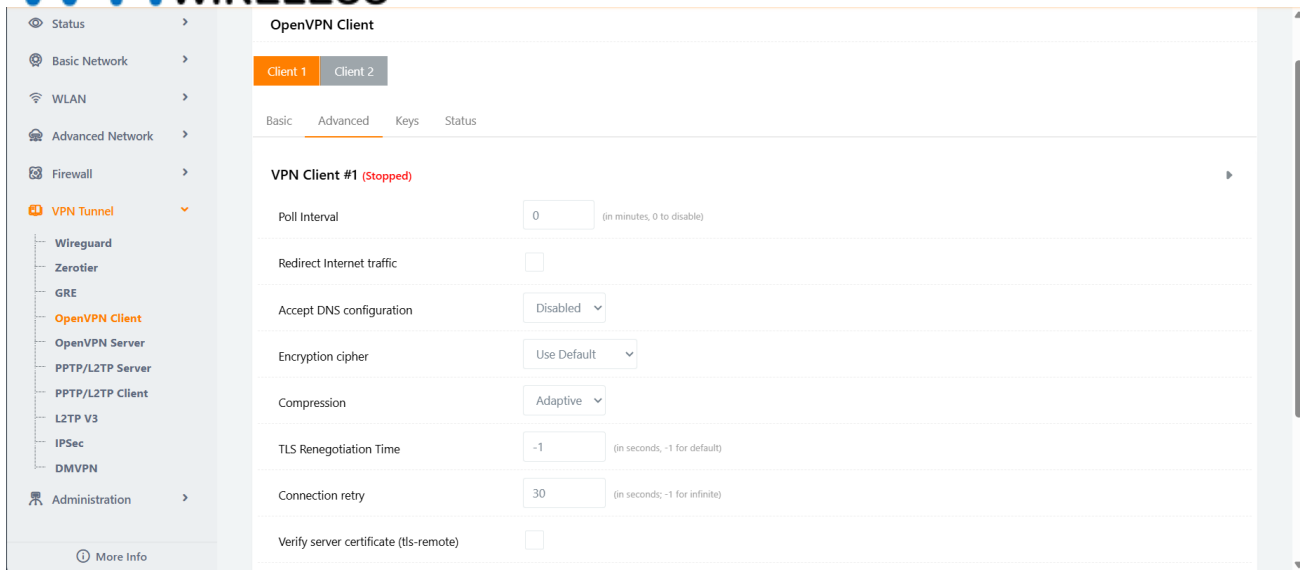


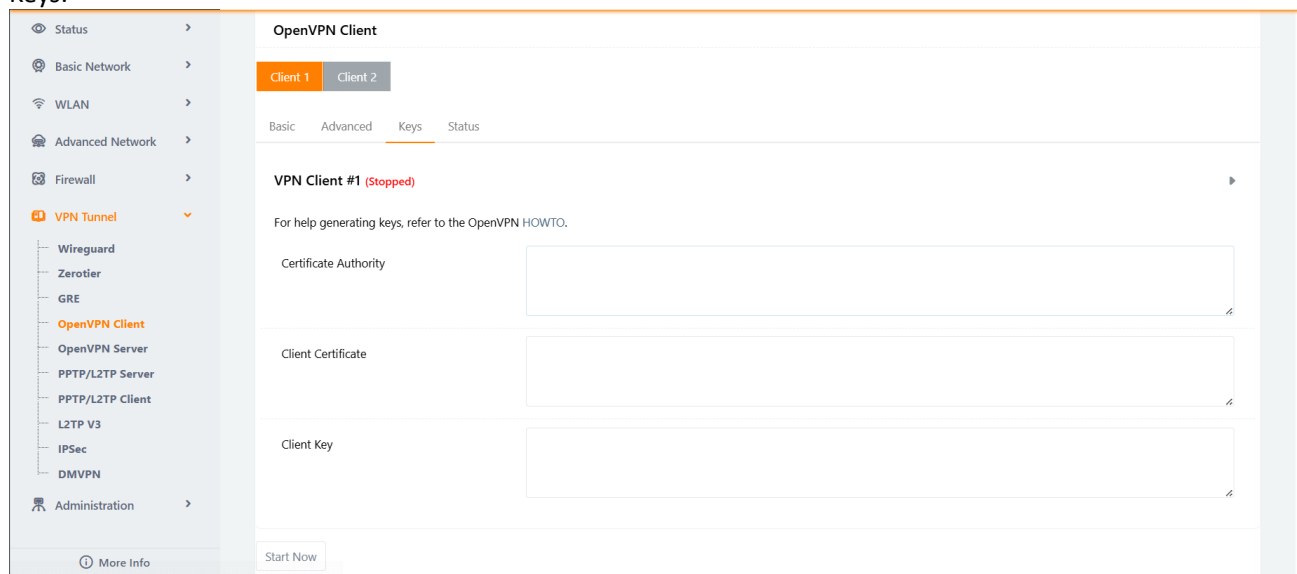
Figure 9-37

Advanced Setup Instructions:

parameter	meaning	How to configure
Polling interval	0 is not disabled and is in minutes	0 is not enabled, and 0 is enabled
Redirect Internet traffic	Whether to allow OpenVPN as the default route	Enable or Disable
Receives the peer DNS configuration	4 types of end-to-end DNS configurations: disabled, relaxed, strict, exclusive	Select any one of the four modes from the dropdown menu
Encryption cipher	Choose from "BF", "DES", "DES-EDE3", "AES128", "AES192", and "AES256". BF: 128-bit encryption algorithm using BF in CBC mode DES: Use DES's 64-bit encryption algorithm in CBC mode DES-EDE3: 192-bit encryption algorithm using 3DES in CBC mode AES128: Use AES's 128-bit encryption algorithm in CBC mode AES192: Use AES's 192-bit encryption algorithm in CBC mode AES256: Uses AES's 256-bit encryption algorithm in CBC mode	Select any one from the drop-down list
Compression	4 compression modes: disabled, none, enabled, adaptive	
TLS Renegotiation time	d-1 is the default in seconds	-1 is the default Enter 0 or higher to enable
Connection retry	Set the number of reconnections of OpenVPN, -1 is an unlimited number of reconnections	-1 is an unlimited number of times, fill in the number above 0 as the number of reconnections, and the default is 30
Verify server certificate (tls-remote)	After checking the box, the common name input box appears	Enable or disable
Custom Configuration	Reservation settings	

Table 9-4

Keys:



The screenshot shows the 'OpenVPN Client' configuration page with the 'Keys' tab selected. The left sidebar lists various network settings, with 'VPN Tunnel' expanded and 'OpenVPN Client' selected. The main content area shows the 'Keys' tab for 'Client 1'. It includes a 'Status' section indicating 'VPN Client #1 (Stopped)' and a note: 'For help generating keys, refer to the OpenVPN HOWTO.' Below this are three text input fields: 'Certificate Authority', 'Client Certificate', and 'Client Key'. A 'Start Now' button is at the bottom left of the main content area.

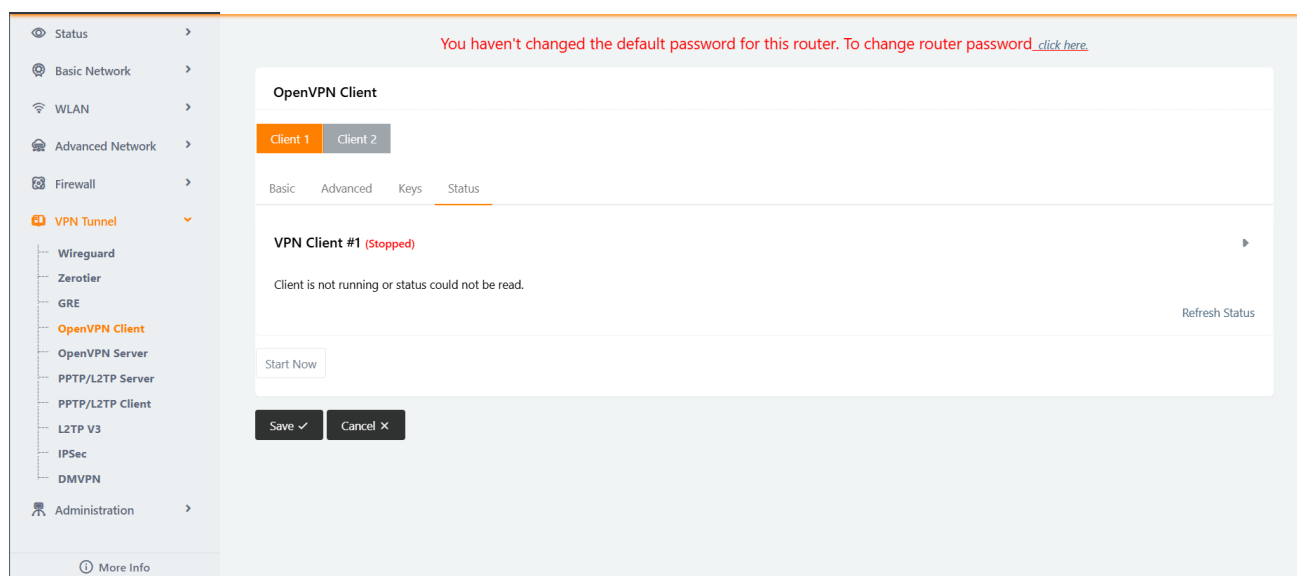
Figure 9-38

Key Setup Instructions:

The name of the parameter	meaning	How to configure
Certificate Authority	Configure the corresponding certificate authorization	Enter the corresponding authorization certificate
Client certificate	Configure the corresponding client certificate	Enter the corresponding client certificate
Client Key	Configure the corresponding client secret	Enter the corresponding client secret

Table 9-5

Status:



The screenshot shows the 'OpenVPN Client' configuration page with the 'Status' tab selected. At the top, a red message states: 'You haven't changed the default password for this router. To change router password [click here](#).' Below this, the 'OpenVPN Client' section shows 'Client 1' selected. The 'Status' tab is active, displaying 'VPN Client #1 (Stopped)' and a message: 'Client is not running or status could not be read.' There is a 'Refresh Status' button on the right. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 9-39

Status Description:

<https://www.wtiwireless.com/>

The name of the parameter	meaning	How to configure
Start now	Launch OpenVPN now	Enable or disable
Refresh the state	Manually refresh the OpenVPN link status	To click or not to click

Table 9-6

9.5. OpenVPN server

OpenVPN is an application-layer VPN implementation based on the OpenSSL library, which is a virtual private tunnel that provides a secure data transmission between enterprises or between individuals and companies. OpenVPN allows a single point of participation in the establishment of a VPN using a shared key, e-certificate, or username/password for authentication.

Step 1: Select "VPN Tunnel > OpenVPN Server" in the navigation bar.

Step 2: Openvpn configuration is divided into four configurations
basic setting

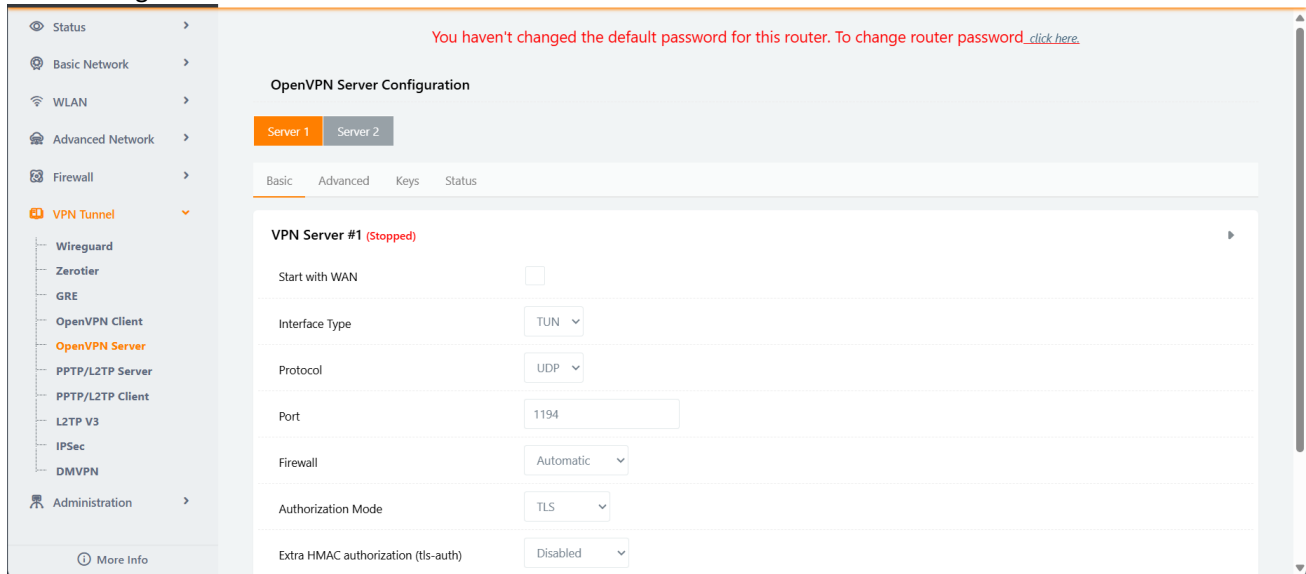


Figure 9-40

Basic Parameter Configuration Description:

parameter	meaning	How to configure
Start with WAN	Whether the network is over a WAN port	ON/OFF
Interface type	The difference between TUN and TAP is that a TUN device is a point-to-point virtual appliance at the network layer, while TAP is a virtual appliance at the Ethernet link layer. TAP mode: Openvpn bridging mode TUN mode: openvpn tunnel mode	Drop-down to select TAP mode or TUN mode
Protocol	TCP mode or UDP mode	Select TCP mode or UDP mode from the drop-down list
Port	Server port configuration	The default port is 1194
Firewall	Firewall modes, including automatic, External Only, and custom	Select automatic, External Only, or custom from the drop-down drop-down
Authorization Mode	The authentication types include TLS, static key, and custom	Select TLS, static key, or custom from the drop-down drop-down
Extra HMAC authorization	Hash message authentication: Default:	

(tls-auth)	Disabled, Bi- directional Incoming (0) Outgoing (1)	Enable or select one of the modes
VPN subnet/netmask	Server subnet address and mask assignment	Format: A.B.C.D/M Default: 10.8.0.0/24

Table 9-7 OpenVPN parameter configuration

Advanced :

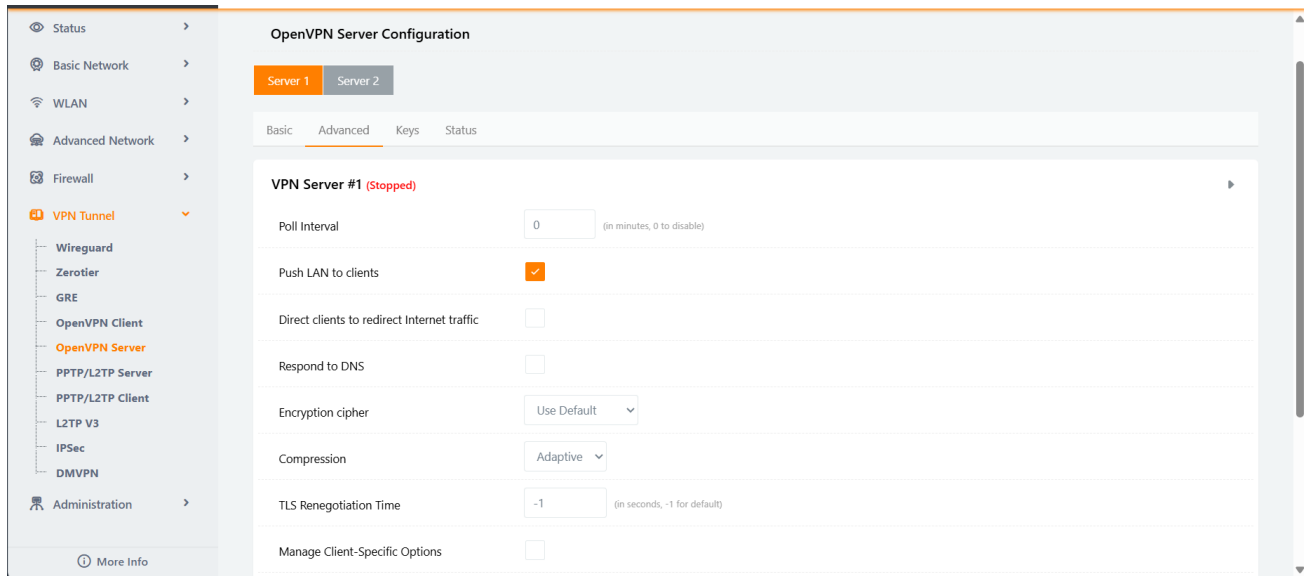


Figure 9-41

Advanced Setup Instructions:

parameter	meaning	How to configure
Polling interval	0 is not disabled and is in minutes	0 is disabled, and 0 or greater is enabled
Push the LAN to the client	Push the LAN port route of the server to the client	Enable or disable Enabled by default
Direct the client to redirect network traffic	The server responds to the DNS to the client	Enable or disable Not enabled by default
Respond to DNS	Whether the server will respond to DNS	Enable or disable Not enabled by default
Advertise DNS to clients	The server sends DNS to the client	Enable or disable Not enabled by default
Encryption cipher	Choose from "BF", "DES", "DES-EDE3", "AES128", "AES192", and "AES256". BF: 128-bit encryption algorithm using BF in CBC mode DES: Use DES's 64-bit encryption algorithm in CBC mode DES-EDE3: uses the 192-bit encryption algorithm of 3DES in CBC mode AES128: Use AES's 128-bit encryption algorithm in CBC mode AES192: Use AES's 192-bit encryption algorithm in CBC mode AES256: Uses AES's 256-bit encryption algorithm in CBC mode	Select any one from the drop-down list
Compression	4 compression modes: disabled, none, enabled, adaptive	Adaptive by default

TLS renegotiation time	-1 is the default in seconds	-1 is the default Enter 0 or higher to enable
Manage client-specific options	After enabled, you can configure whether clients or clients communicate with each other	Enable or disable Not enabled by default
Allow Client < - > Client	Whether client-to-client communication is allowed	Enable or disable Not enabled by default
Allow Only These Clients	configure which clients the server is allowed to push; Configurations include CommonName, subnet, netmask, and push	Enable or disable Not enabled by default
Allow User/Pass Auth	When enabled, you can configure which users require authentication, The configuration includes a username and password	Enable or disable Not enabled by default
Custom Configuration	Reservation settings	Default is empty

Table 9-8

Key Settings:

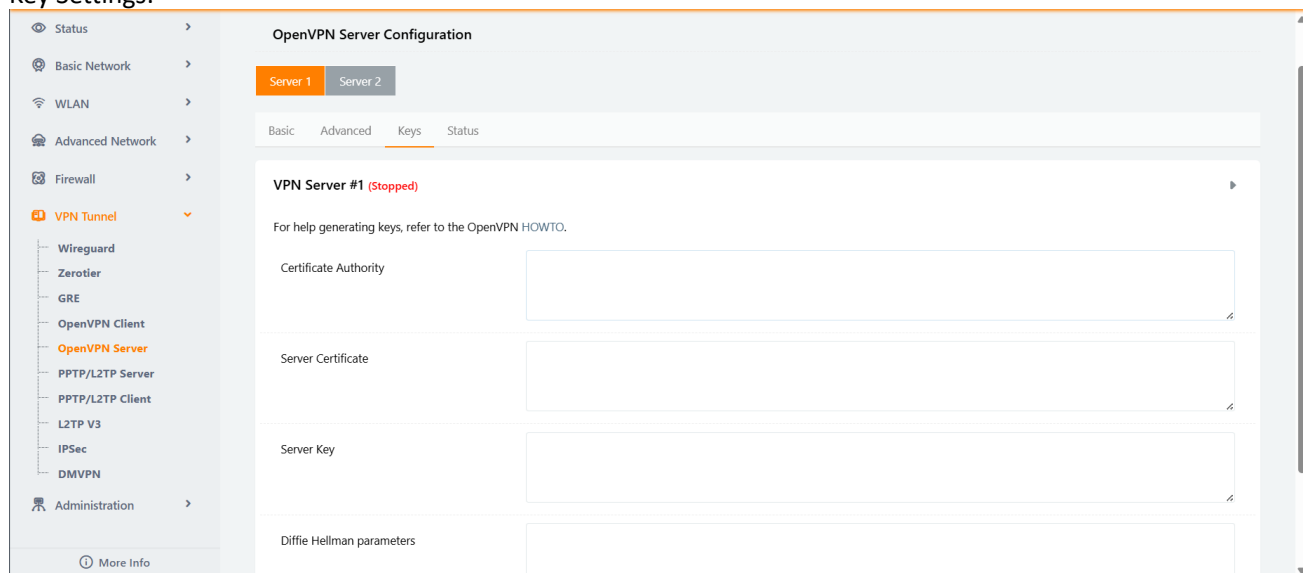


Figure 9-42

Key Setup Instructions:

The name of the parameter	meaning	How to configure
Certificate Authority	Configure certificate authority	Fill in the authorization certificate
Server Certificate	Configure a server-side certificate	Enter the server certificate
Server key	Configure a server key	Enter the server key
Diffie Hellman parameters	Configure the DH parameter of the server	Enter the DH parameter of the server

Table 9-9

Status:

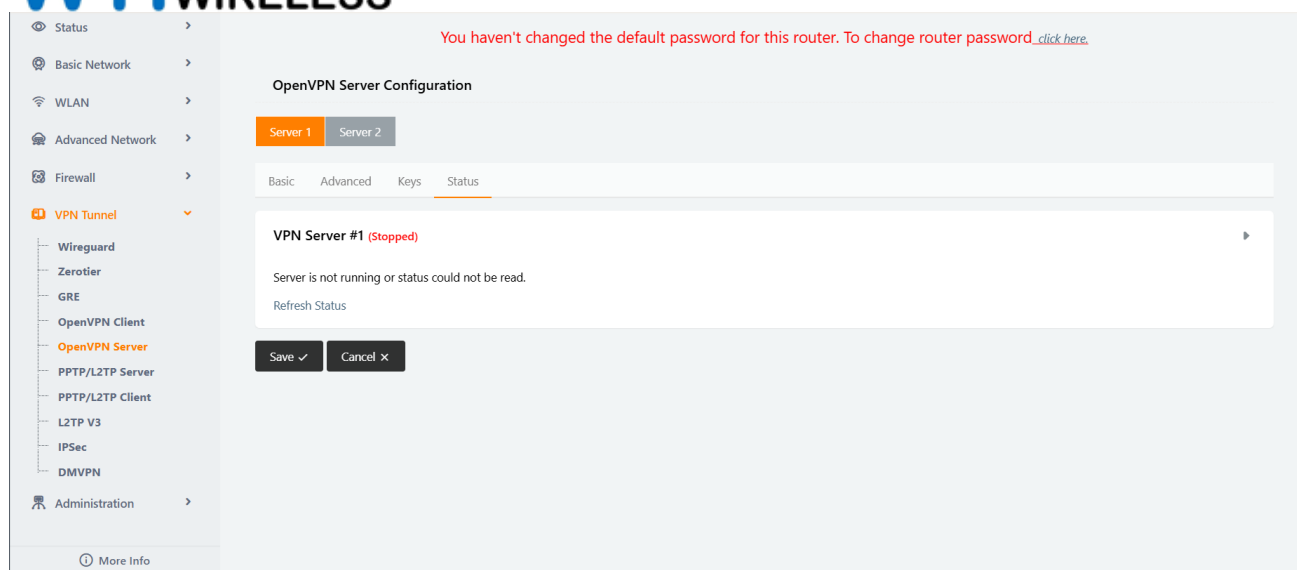


Figure 9-43

Status Description:

The name of the parameter	meaning	How to configure
Start now	Launch OpenVPN now	Enable or disable
Refresh the state	Manually refresh the OpenVPN link status	To click or not to click

Table 9-10

Example 1:

Example configuration of TUN-TCP

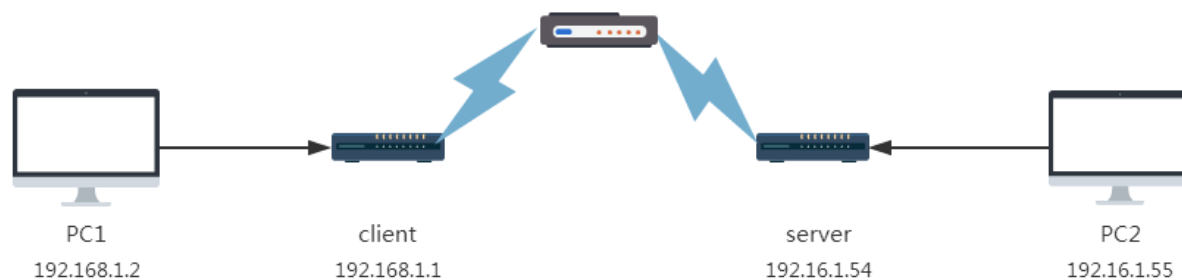


Figure 9-44

Server configuration:

OpenVPN Server Configuration

Server 1 Server 2

Basic Advanced Keys Status

VPN Server #1 (Running)

Start with WAN ☒

Interface Type TUN

Protocol UDP

Port 1194

Firewall Automatic

Authorization Mode TLS

Extra HMAC authorization (tls-auth) Disabled

VPN subnet/netmask 10.8.0.0 255.255.255.0

Figure 9-45

Basic Advanced Keys Status

VPN Server #1 (Running)

Poll Interval 0 (in minutes, 0 to disable)

Push LAN to clients ☒

Direct clients to redirect Internet traffic ☐

Respond to DNS ☐

Encryption cipher Use Default

Compression Adaptive

TLS Renegotiation Time -1 (in seconds, -1 for default)

Manage Client-Specific Options ☐

Allow User/Pass Auth ☐

Custom Configuration

Figure 9-46

Client Configuration (check Allow Tunnel NAT):

OpenVPN Client

Client 1
Client 2

Basic
Advanced
Keys
Status

VPN Client #1 (Running)

Start with WAN ☒

Interface Type TUN

Protocol UDP

Server Address 192.168.10.69 1194

Firewall Automatic

Authorization Mode TLS

Username/Password Authentication ☐

HMAC authorization Disabled

Figure 9-47

After the link is successful:

OpenVPN Server Configuration

Server 1
Server 2

Basic
Advanced
Keys
Status

VPN Server #1 (Running)

Data current as of Tue Sep 3 11:19:15 2024.

Client List

Common Name	Real Address	Virtual Address	Virtual IPv6 Address	Bytes Received	Bytes Sent	Connected Since	Connected Since (time_t)	Username	Client ID
client	192.168.10.70:50908	10.8.0.6		29301	29060	Tue Sep 3 09:11:22 2024	1725325882	UNDEF	0

Routing Table

Virtual Address	Common Name	Real Address	Last Ref
10.8.0.6	client	192.168.10.70:50908	Tue Sep 3 09:11:24 2024

General Statistics

Name	Value
Max bcast/mcast queue length	0

Refresh Status

Figure 9-48

Select Allow tunnel NAT, which can ping the same server IP address, but cannot ping the subnet IP address

```

03/09/2024 14:52.40 /home/mobaxterm ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=63

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 2ms, 平均 = 1ms

03/09/2024 14:53.06 /home/mobaxterm ping 192.168.1.37

正在 Ping 192.168.1.37 具有 32 字节的数据:
来自 192.168.1.37 的回复: 字节=32 时间=4ms TTL=126
来自 192.168.1.37 的回复: 字节=32 时间=2ms TTL=126
来自 192.168.1.37 的回复: 字节=32 时间=3ms TTL=126
来自 192.168.1.37 的回复: 字节=32 时间=2ms TTL=126

192.168.1.37 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 4ms, 平均 = 2ms

```

Figure 9-49

Client configuration (uncheck Allow Tunnel NAT):

Basic	Advanced	Keys	Status
VPN Client #1 (Running)			
Start with WAN	☒		
Interface Type	TUN		
Protocol	UDP		
Server Address	192.168.10.95 1194		
Firewall	Automatic		
Authorization Mode	TLS		
Username/Password Authentication	☐		
HMAC authorization	Disabled		
Create NAT on tunnel	☐ Routes must be configured manually.		

Figure 9-50

If you do not select Allow tunnel NAT, you can ping the server IP address and the subnet IP address

TAP-TCP configuration example:

Server:

Server 1Server 2

BasicAdvancedKeysStatus

VPN Server #1 (Running)

Start with WAN

Interface Type

TAP

Bridge TAP with

LAN (br0)*

* default

Protocol

UDP

Port

1194

Firewall

Automatic

Authorization Mode

TLS

Extra HMAC authorization (tls-auth)

Disabled

Client address pool

DHCP

Figure 9-51

Client Configuration:

Client 1Client 2

BasicAdvancedKeysStatus

VPN Client #1 (Running)

Start with WAN

Interface Type

TAP

Protocol

UDP

Server Address

192.168.10.95

1194

Firewall

Automatic

Authorization Mode

TLS

Username/Password Authentication

HMAC authorization

Disabled

Server is on the same subnet

Figure 9-52

After the link is successful, PC1 can ping the server gateway

```

06/09/2024 10:01.58 /home/mobaxterm ping 192.168.1.254

正在 Ping 192.168.1.254 具有 32 字节的数据:
来自 192.168.1.254 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=3ms TTL=64

192.168.1.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3ms, 最长 = 5ms, 平均 = 3ms

06/09/2024 10:11.17 /home/mobaxterm ping 192.168.1.254

正在 Ping 192.168.1.254 具有 32 字节的数据:
来自 192.168.1.254 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=4ms TTL=64

192.168.1.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3ms, 最长 = 5ms, 平均 = 3ms

```

Figure 9-53

9.6. PPTP/L2TP server

PPTP is an extension of the End-to-End Protocol (PPP) that uses the authentication, compression, and encryption mechanisms provided by PPP, and PPTP can be automatically installed along with the TCP/IP protocol. PPTP and Microsoft End-to-End Encryption (MPPE) technology provide VPN services for encapsulating and encrypting confidential data. MPPE encrypts PPP frames with encryption keys generated by the MS-CHAP and MS-CHAP v2 authentication processes. In order to encrypt valid data contained in PPP frames, the VPN client must use the MS-CHAP, MS-CHAP v2 authentication protocol.

Step 1: Select "VPN Tunnel > PPTP/L2TP Server" in the navigation bar. The specific page is as follows:

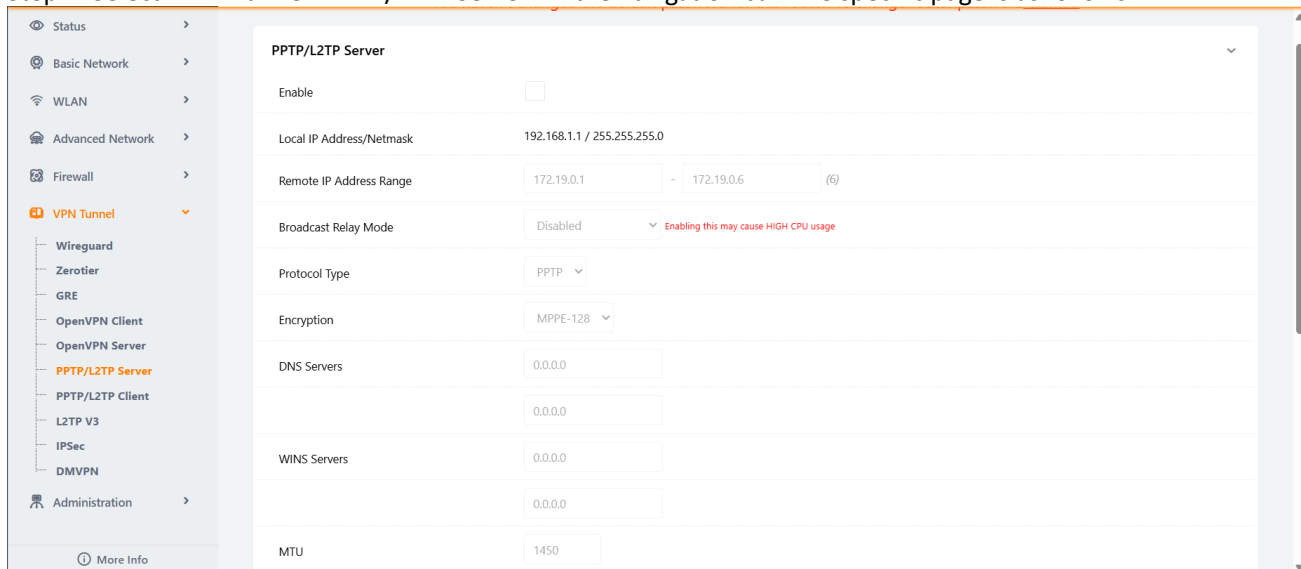


Figure 9-54

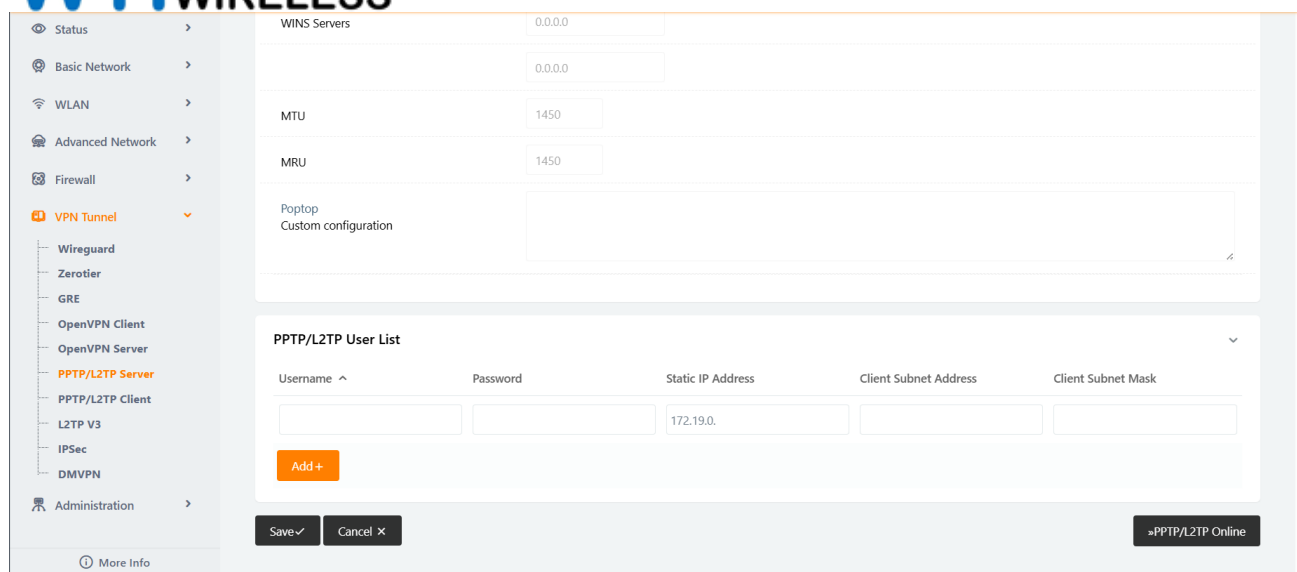


Figure 9-55

Step 2: Parameters

name	meaning	How to configure
Enable	Click Enable	enable
Local IP address/netmask	The LAN port IP address and subnet of the router	Varies based on router LAN parameters
Remote IP address range	The VPN address of the server	The default value is 172.19.0.1-172.19.0.6
Broadcast relay mode	Trunk mode configuration	The default value is Disabled Disabled, LAN to VPN client, VPN client to LAN, Both
Protocol Type	Protocol type	Default PTP PPTP/L2TP optional
Encryption	Data is encrypted against the VPN	Default MPPE-128 Optional MPPE-128/NONE
DNS server	The domain name resolution server settings of the VPN	Default 0.0.0.0, 0.0.0.0
WINS server	The VPN's domain name resolution server settings work based on the computer's NetBIOS name	Default 0.0.0.0, 0.0.0.0
MTU	The maximum transmission unit of data, which represents the outgoing traffic processing	Default 1450
MRU	The maximum transmission unit of data, which represents the incoming traffic processed	Default 1450
Poptop Customize the settings	User-defined	Default is empty
List of PPTP/L2TP users	/	/

Username	Username configuration for the server	Default is empty
password	Password configuration for the server	Default is empty
Static IP address	The VPN address assigned by the server to the client (within the range of remote IP addresses)	The default value is 172.19.0
Client subnet address	Subnet IP configuration of the client	Default is empty
Client subnet mask	The mask IP configuration of the client	Default is empty

Table 9-11 PPTP/L2TP server parameters

Step 3: Set the parameters as follows:

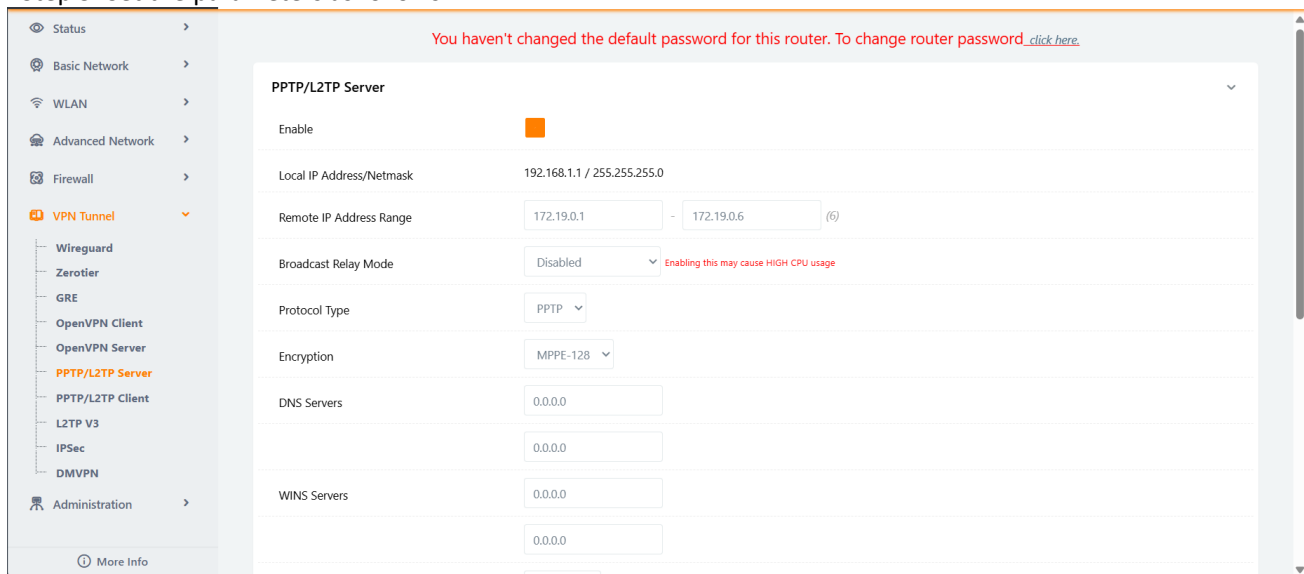


Figure 9-56

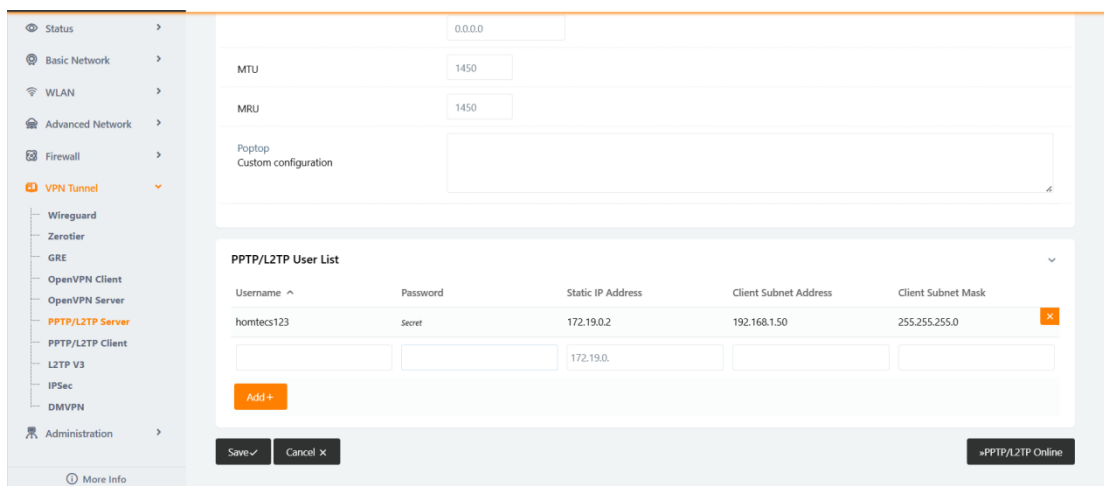


Figure 9-57

Step 4: After the client is successfully connected, you can click the PPTP/L2TP online page at the bottom of the server configuration page to view the connection status

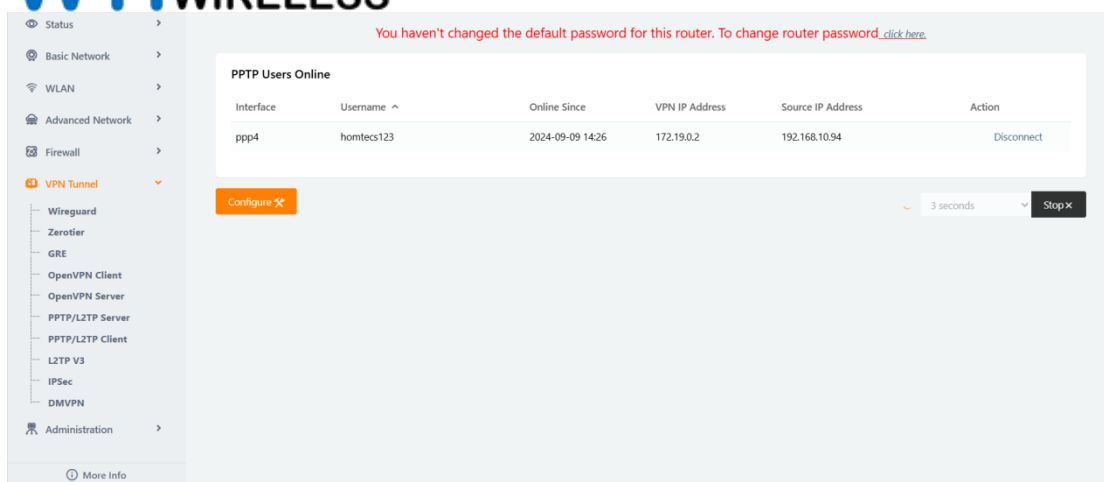


Figure 9-58

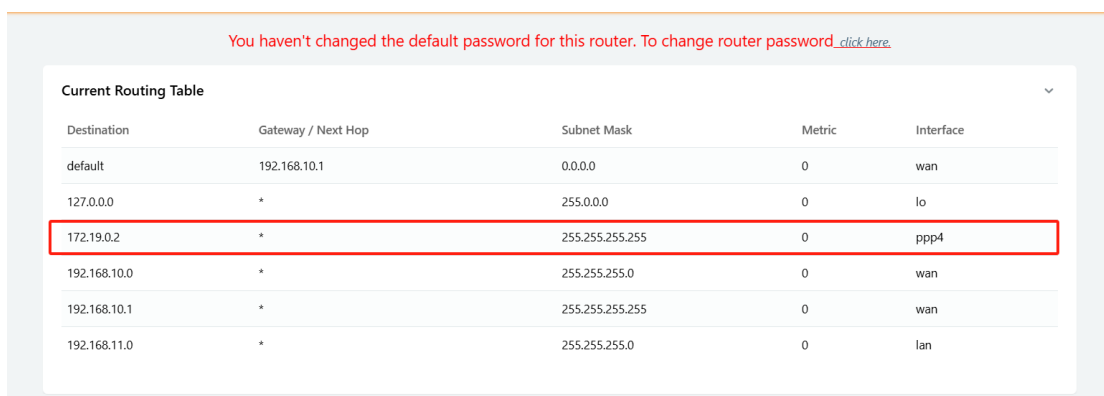


Figure 9-59

telnet enters the backend of the server and can ping the VPN address of the client

```
root@Router:/tmp/home/root#
root@Router:/tmp/home/root# ping 172.19.0.2
PING 172.19.0.3 (172.19.0.3): 56 data bytes
64 bytes from 172.19.0.3: seq=0 ttl=64 time=1.669 ms
64 bytes from 172.19.0.3: seq=1 ttl=64 time=1.442 ms
64 bytes from 172.19.0.3: seq=2 ttl=64 time=1.439 ms
64 bytes from 172.19.0.3: seq=3 ttl=64 time=1.444 ms
64 bytes from 172.19.0.3: seq=4 ttl=64 time=1.449 ms
^C
--- 172.19.0.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.439/1.488/1.669 ms
```

Figure 9-60

The client page is connected to the following link, and you can ping the IP address of the server

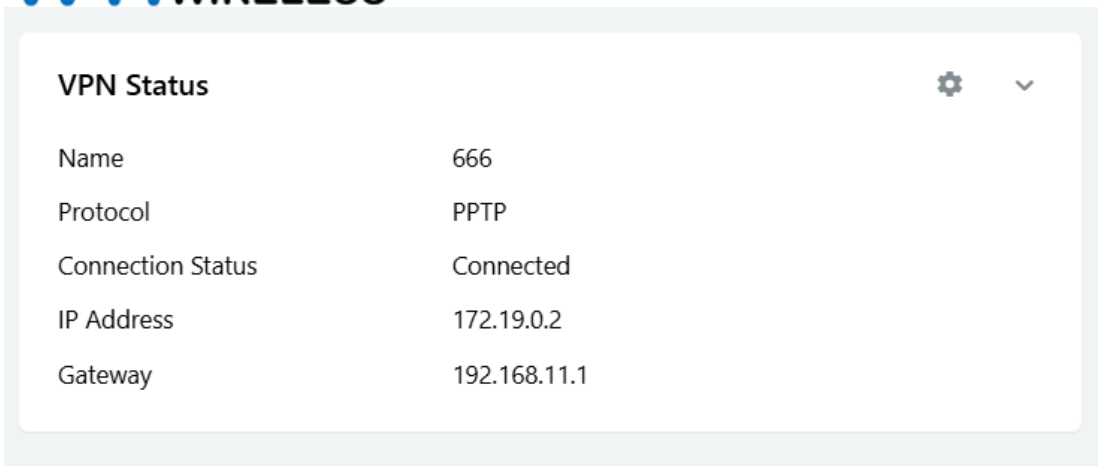


Figure 9-61

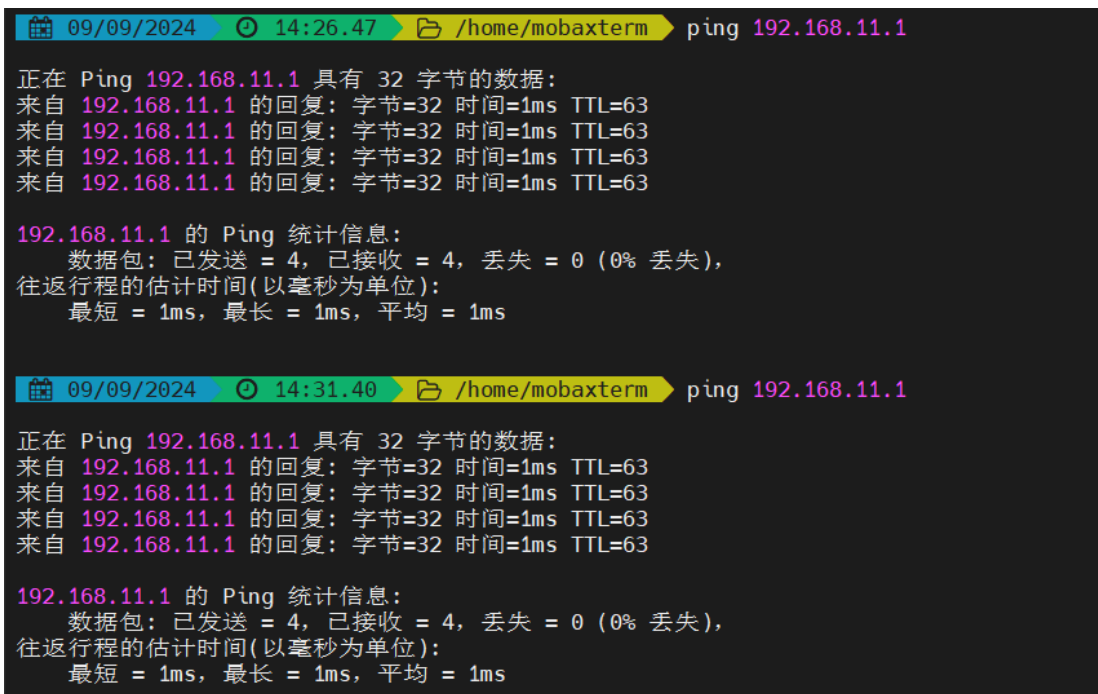


Figure 9-62

9.7. L2TP/PPTP client

Point to Point Tunneling Protocol (PPTP) is a network technology that supports multi-protocol virtual private networks, and it is also a layer 2 protocol. Through this protocol, remote users can securely access the corporate network through the mainstream Windows operating system and other systems with point-to-point protocols, and can dial up to the local ISP to securely connect to the corporate network over the Internet.

L2TP (Layer Two Tunneling Protocol) is an abbreviation for Layer 2 Tunneling Protocol, which is a type of VPDN (Virtual Private Dial-up Network) technology, which is specially used for Layer 2 data channel transmission. L2TP provides a means of remote access access control, and its typical application scenario is that an employee of a company dials in to the company's local network access server (NAS) through PPP to access the company's internal network and obtain an IP address and access the network resources with the appropriate permissions. The employee dials in to the corporate network as securely and conveniently as they would on the corporate LAN.

L2TP protocol configuration:

Step 1: Select "VPN Tunnel > VPN Client" in the navigation bar. In the page that opens, you can select an L2TP client from the drop-down list and modify the relevant parameters.

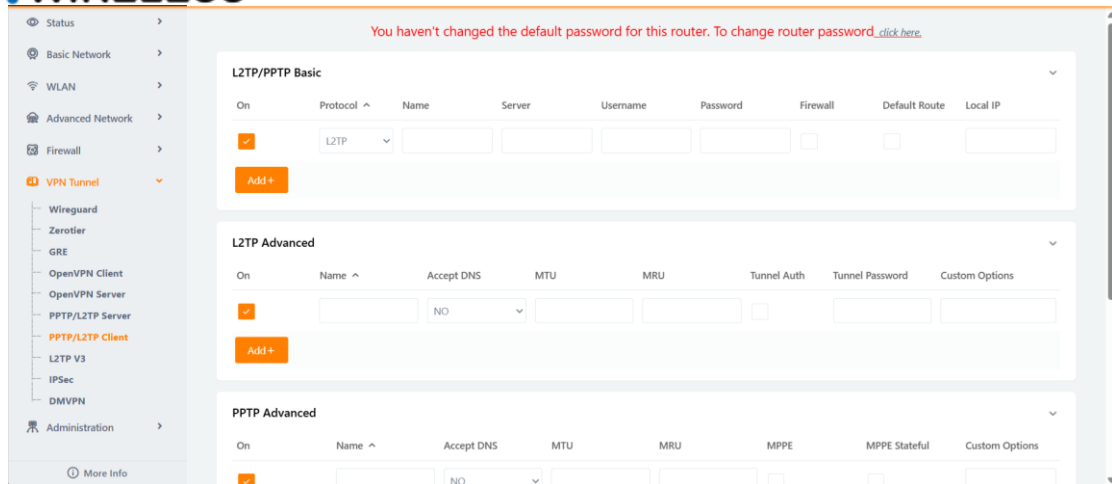


Figure 9-63

Step 2: L2tp configuration description

name	meaning	How to configure
ON\OFF	Click Enable	ON\OFF
Protocol	Select the client mode	Select L2TP/PPTP
name	Set the name of the client	Null
Server	The IP address or domain name of the server used for access.	Fill in the IP address or domain name of the server
Username	A legitimate user who has been authorized to access the access server.	Fill in the username that the server has authorized
password	The access server has authorized a valid user password.	Fill in the password that the server has authorized
Firewall	Set up a firewall	Tick/Unchecked
Default Route	Set the default route	Tick/Unchecked
Local IP	Set the local IP address	Null
Receives the peer DNS	Accept L2TP Server to assign DNS addresses	YES/NO
MTU	Set the MTU parameters	1500
MRU	Set MRU parameters	1500
Tunnel authentication	Configure tunnel authentication	Tick/Unchecked
Tunnel password	Set a tunnel password	Null
Customize options	Set up custom dialing content	Null

Table 9-12 L2TP configuration

PPTP protocol configuration:

Step 1: Select "VPN Tunnel > VPN Client" in the navigation bar. In the page that opens, you can select an L2TP client from the drop-down list and modify the relevant parameters.

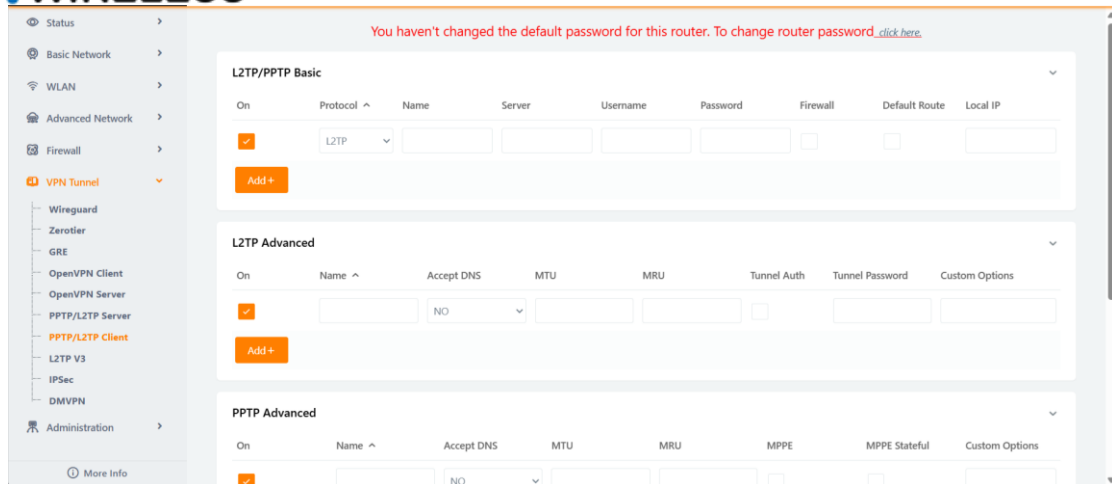


Figure 9-64

Step 2: Configure PPTP parameters.

parameter	meaning	How to configure
Client-side mode	Select the client mode	L2TP or PPTP
name	Set the name of the client	Null
Service	The IP address or domain name of the server used for access.	Fill in the IP address or domain name of the server
Username	A legitimate user who has been authorized to access the access server.	Fill in the username that the server has authorized
password	The access server has authorized a valid user password.	Fill in the password that the server has authorized
Firewall	Set up a firewall to allow the VPN to channel the NAT	Tick/unchecked
Default route	Set the default route for all data to go through VPN	Tick/Unchecked
Local IP	Set the local IP address of the specified V PN client	Null
Accept the peer DNS configuration	Accept the DNS Server Address assigned by the PPTP Server	Disable or enable
MTU	Set the MTU parameters	1500
MRU	Set MRU parameters	1500
MPPE	Encryption options	Tick/Unchecked
MPPE stateful	Set the MPPE connection status	Tick/Unchecked
Custom Options	Set custom dialing options	If you need this option, you must contact our technical support

Table 9-13 VPN PPTP Parameter Configuration

Step 3: Save the settings and complete the VPN rule settings.

Example:

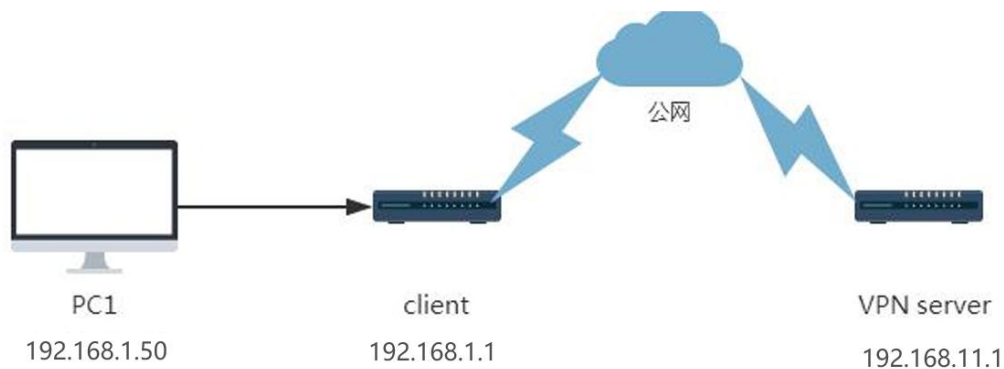


Figure 9-65

Configure PPTP, bring the router 3G/4G online, and link to the PPTP server

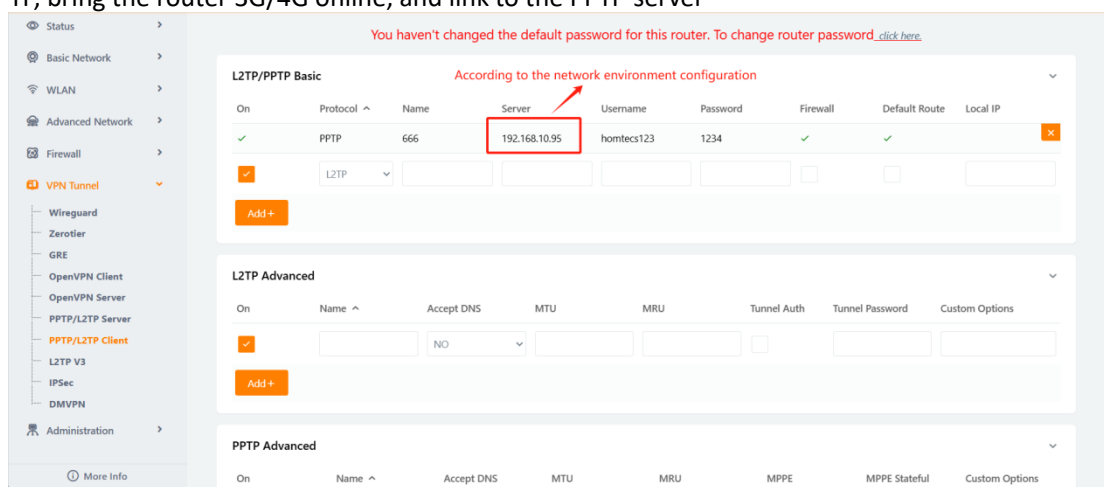


Figure 9-66

Configure PPTP, bring the router 3G/4G online, and link to the PPTP server

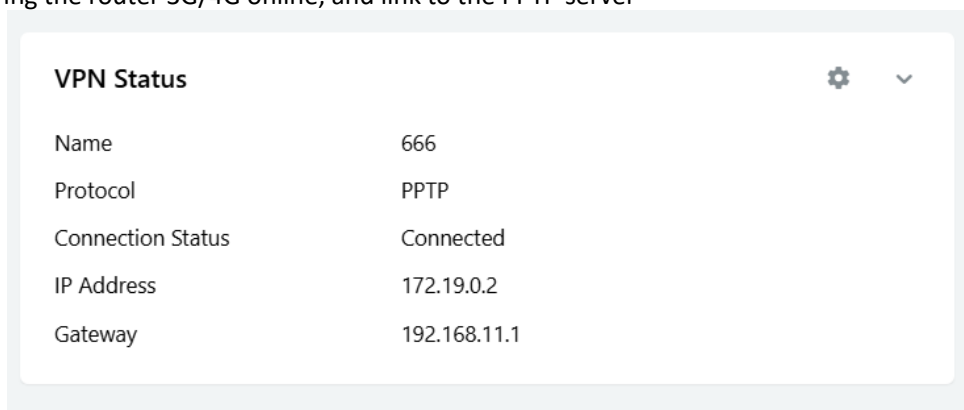


Figure 9-67

The PC can ping the PPTP server gateway through the router Internet access

```

09/09/2024 14:26.47 /home/mobaxterm ping 192.168.11.1

正在 Ping 192.168.11.1 具有 32 字节的数据:
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63

192.168.11.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 1ms, 平均 = 1ms

09/09/2024 14:31.40 /home/mobaxterm ping 192.168.11.1

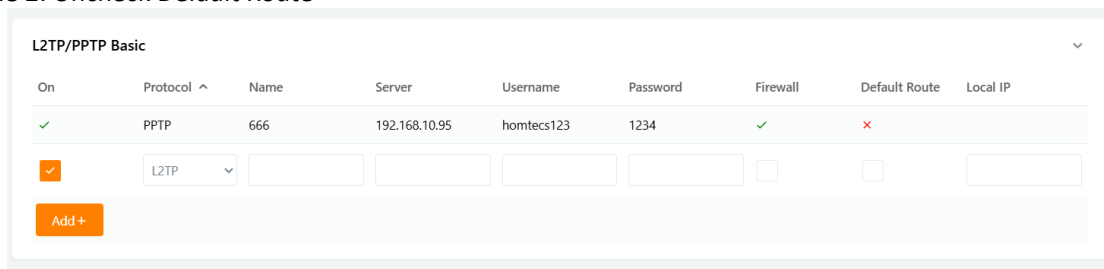
正在 Ping 192.168.11.1 具有 32 字节的数据:
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63

192.168.11.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 1ms, 平均 = 1ms

```

Figure 9-68

Example 2: Uncheck Default Route



On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
✓	PPTP	666	192.168.10.95	homtects123	1234	✓	✗	
☒	L2TP					☐	☐	

Add +

Figure 9-69

9.8. L2TP V3

L2TPv3 (Layer Two Tunneling Protocol - Version 3) is a Layer 2 tunneling technology that transparently transmits multiple Layer 2 packets (such as PPP, Ethernet, HDLC, and ATM) and transparently transmits Layer 2 access links on the user side in packet-switched networks.

L2TPv3 is an L2VPN solution for IP-based networking. L2TPv3 is formerly Cisco's proprietary protocol, --- Universal Transport Protocol (UTI).

Step 1: Select "VPN Tunnel%3EL2TP V3" in the navigation bar.

You haven't changed the default password for this router. To change router password [click here](#).

Status >
Basic Network >
WLAN >
Advanced Network >
Firewall >
VPN Tunnel ▾
Wireguard
Zerotier
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration >
More Info

Tunnel Setting

On
Local Tunnel ID
Remote Tunnel ID
Server Address

☒

Add+

Session Setting

On
Index
Tunnel ID
Local Session ID
Remote Session ID
Local Address And Mask
Remote Address And Mask
Work Mode

☒

ROUTER

Add+

Save ✓
Cancel ✕

Figure 9-70

Step 2: Configure parameters

Parameter	meaning	How to configure
Local tunnel ID	Local tunnel ID	Default is empty
Remote Tunnel ID	Remote Tunnel ID	Default is empty
Server address	The address of the peer WAN port	Default is empty Format: A.B.C.D,
Session setting sequence number (Index)	serial number	Default is empty
Session Setup Tunnel ID	Tunnel ID	Default is empty
Local session ID	Local session ID	Default is empty
The ID of the peer session	The ID of the peer session	Default is empty
Local tunnel address and mask	Local tunnel address and subnet	Format: A.B.C.D/M Default is empty
Remote Address And Mask	The address and subnet of the peer tunnel	Format: A.B.C.D/M Default is empty
Working mode	It is divided into routing, gateway and bridging	The route mode is selected by default

Table 9-14 L2TP V3 parameters

Step 3: Set the parameters as follows:

R1: local IP address 192.168.1.1/32, WAN port IP address 192.168.10.77

You haven't changed the default password for this router. To change router password [click here](#).

Status >
Basic Network >
WLAN >
Advanced Network >
Firewall >
VPN Tunnel >
Wireguard
Zerotier
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration >

Tunnel Setting

On	Local Tunnel ID	Remote Tunnel ID	Server Address
✓	1	1	192.168.10.95
✓			
Add +			

Session Setting

On	Index	Tunnel ID	Local Session ID	Remote Session ID	Local Address And Mask	Remote Address And Mask	Work Mode
✓	1	1	11	11	10.5.1.1/32	10.5.1.2/32	ROUTER
✓							ROUTER
Add +							

Save ✓ Cancel ✕

Figure 9-71

R2: local IP address 192.168.2.1/32, WAN port IP address 192.168.10.169

You haven't changed the default password for this router. To change router password [click here](#).

Status >
Basic Network >
WLAN >
Advanced Network >
Firewall >
VPN Tunnel >
Wireguard
Zerotier
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration >

Tunnel Setting

On	Local Tunnel ID	Remote Tunnel ID	Server Address
✓	1	1	192.168.10.94
✓			
Add +			

Session Setting

On	Index	Tunnel ID	Local Session ID	Remote Session ID	Local Address And Mask	Remote Address And Mask	Work Mode
✓	1	1	11	11	10.5.1.2/32	10.5.1.1/32	ROUTER
✓							ROUTER
Add +							

Save ✓ Cancel ✕

Figure 9-72

After the connection is established, you can view the information through the route tables of R 1 and R 2, and ping the tunnel address and gateway IP address of the peer end

R1 :

Current Routing Table				
Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	192.168.10.1	0.0.0.0	0	wan
10.4.168.0	*	255.255.255.0	0	modem
10.5.1.2	*	255.255.255.255	0	l2tpeth1
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	lan
192.168.2.0	*	255.255.255.255	0	l2tpeth1
192.168.10.0	*	255.255.255.0	0	wan
192.168.10.1	*	255.255.255.255	0	wan

Figure 9-73

```

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.553 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.824 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.727 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.792 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.845 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.727/0.948/1.553 ms

root@Router:/tmp/home/root# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=64 time=0.324 ms
64 bytes from 192.168.2.1: seq=1 ttl=64 time=0.252 ms
64 bytes from 192.168.2.1: seq=2 ttl=64 time=0.232 ms
64 bytes from 192.168.2.1: seq=3 ttl=64 time=0.293 ms
64 bytes from 192.168.2.1: seq=4 ttl=64 time=0.310 ms
^C
--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.232/0.282/0.324 ms

```

Figure 9-74

R2:

Current Routing Table				
Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	192.168.10.1	0.0.0.0	0	wan
10.5.1.1	*	255.255.255.255	0	l2tpeth1
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	l2tpeth1
192.168.2.0	*	255.255.255.0	0	lan
192.168.10.0	*	255.255.255.0	0	wan
192.168.10.1	*	255.255.255.255	0	wan

Figure 9-75

```

root@Router:/tmp/home/root# ping 10.5.1.1
PING 10.5.1.1 (10.5.1.1): 56 data bytes
64 bytes from 10.5.1.1: seq=0 ttl=64 time=1.041 ms
64 bytes from 10.5.1.1: seq=1 ttl=64 time=0.829 ms
64 bytes from 10.5.1.1: seq=2 ttl=64 time=0.805 ms
64 bytes from 10.5.1.1: seq=3 ttl=64 time=0.818 ms
64 bytes from 10.5.1.1: seq=4 ttl=64 time=0.807 ms
^C
--- 10.5.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.805/0.860/1.041 ms

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.919 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.687 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.660 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.690 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.660/0.739/0.919 ms

```

Figure 9-76

9.9. IPSec configuration

IPSec is a protocol built on top of the Internet Protocol (IP) layer that enables two or more hosts to communicate in a secure manner. IPSec is the long-term direction for secure networking. It provides proactive protection against attacks on private networks and the Internet through end-to-end security.

Step 1: Select "VPN Tunnel > IPSec" in the navigation bar.

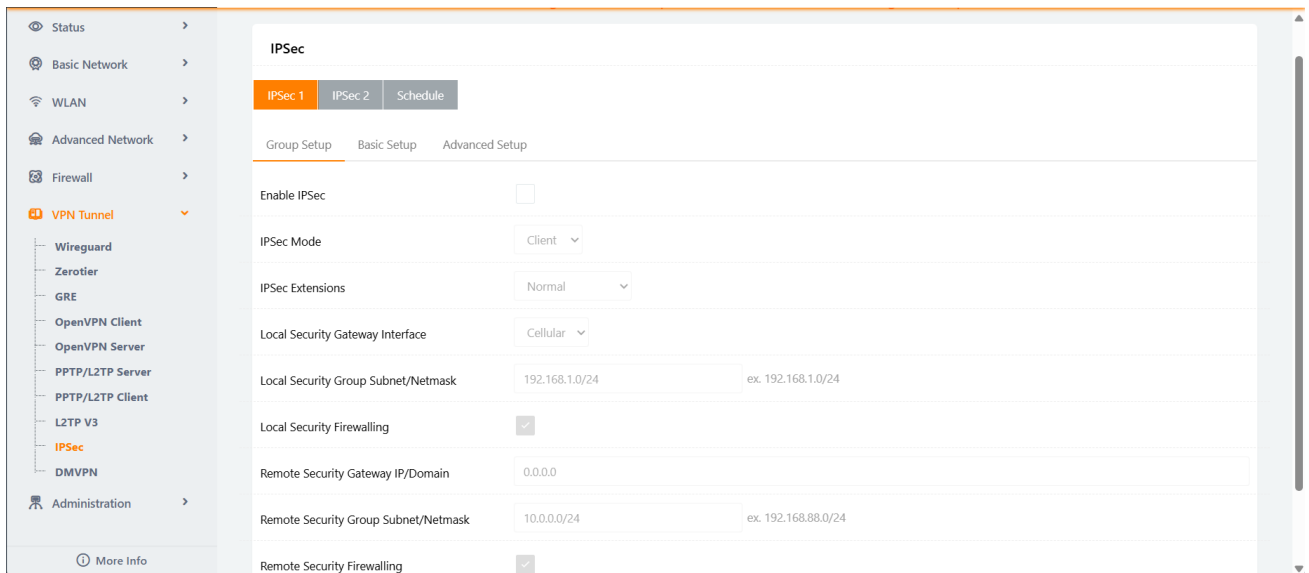


Figure 9-77

Step 2: This IPSec page is divided into two phases of configuration.

1. The first stage parameter configuration interface is shown in the following figure:

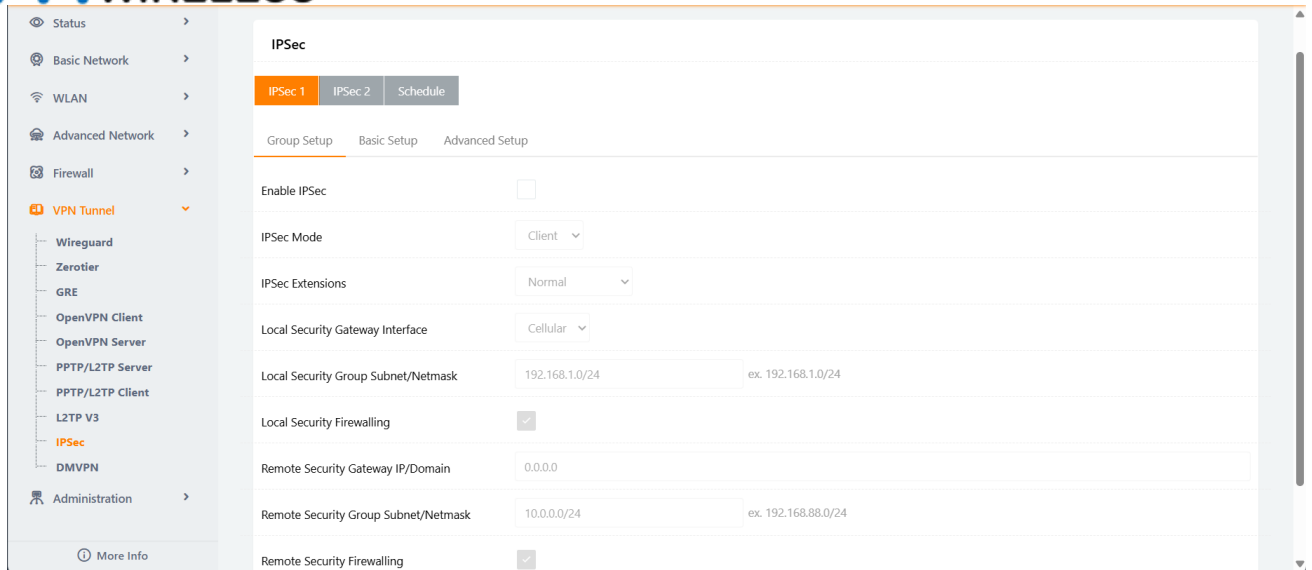


Figure 9-78

Parameter configuration description of the first stage:

The name of the parameter	meaning	How to configure
Enable IPsec	Specifies whether to enable IPsec configuration	Enabled or not enabled
IPsec Extension	Three IPsec networking methods: NormalIPsec/GRE Over IPsec/L2TP Over IPsec	Configure the networking mode of the server corresponding to the Yess
Local security group Subnet/Netmask	Local subnet configuration	You do not need to configure subnets in transmission mode, but you need to configure them in automatic and tunnel modes. Enter the local subnet address. Format: A.B.C.D/M,
On-premise security firewall	Whether the firewall is enabled	Enabled or not enabled
Remote Security Gateway IP/Domain	IPsec server IPO or domain name	
Remote Security Group Subnet/Netmask	Remote subnet configuration	You do not need to configure subnets in transmission mode, but you need to configure them in automatic and tunnel modes. Enter the remote subnet address. Format: A.B.C.D/M,
Remote Security Firewall	Whether the firewall is enabled	Enabled or not enabled

Table 9-15 IPsec Phase 1 Parameter Configuration

After the configuration is complete, click the Save Settings button for the configuration to take effect.

2. Figure 9-30 shows the parameters in the second stage.

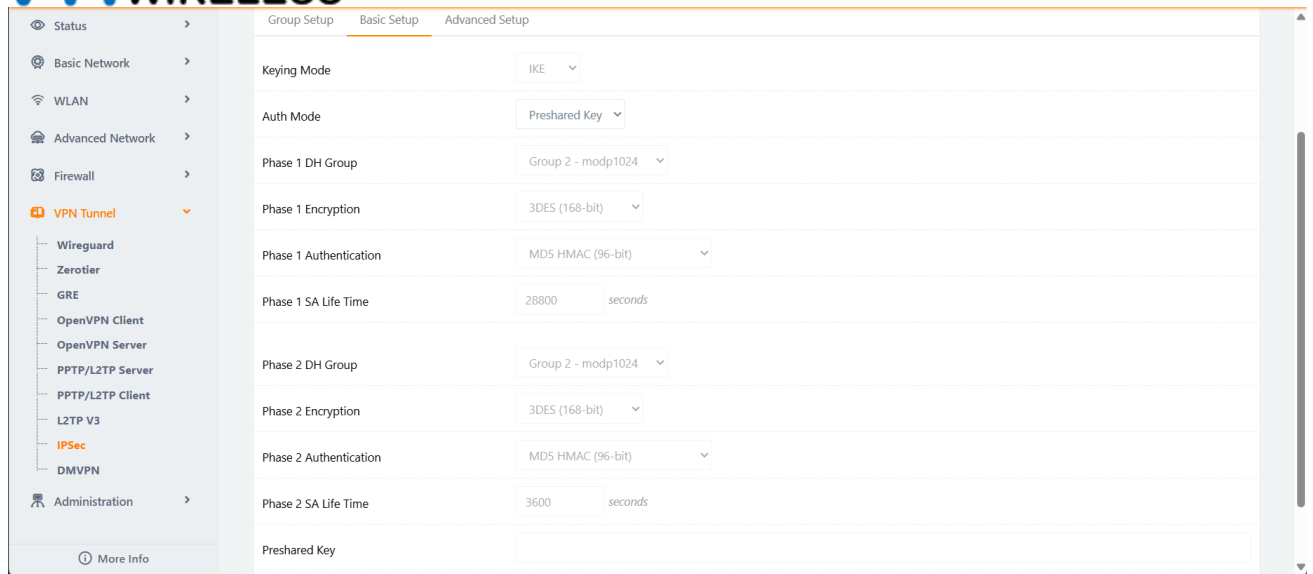


Figure 9-79

Parameter configuration description of the second stage:

Parameter	Meaning	How to configure
DH Group	Used when enabling Perfect Forward Encryption, this is configured as the key length for IPSec Phase 2 SA negotiation	Select from the dropdown table Select the appropriate group name from the dropdown table
Encryption	Supports DES, 3DES, and AES encryption methods	Dropdown table selection Select the appropriate group name from the dropdown table
SA Life Time	IPSec SA (IPSec Security Alliance) key lifetime	Fill in the appropriate key lifecycle Value range: 120~86400 Unit: seconds

Table 9-16 IPSet Phase II parameters

Configuration example:

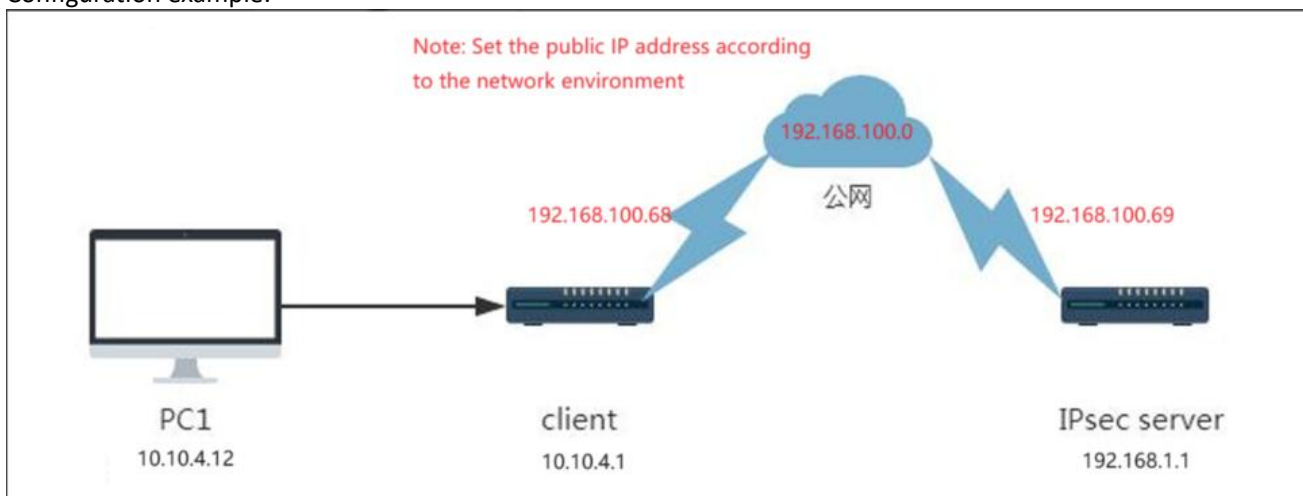


Figure 9-80

Group Setup:

IPSec

IPSec 1

IPSec 2

Schedule

Group Setup

Basic Setup

Advanced Setup

Enable IPSec

☒

IPSec Mode

Server

IPSec Extensions

Normal

Local Security Gateway Interface

Cellular

Local Security Group Subnet/Netmask

192.168.1.0/24

ex. 192.168.1.0/24

Local LAN port IP

Local Security Firewalling

☒

Remote Security Gateway IP/Domain

0.0.0.0

Remote Security Group Subnet/Netmask

10.10.4.0/24

ex. 192.168.88.0/24

LAN IP of the remote device

Remote Security Firewalling

☒

Figure 9-81

Basic Setup:

Default parameters

Group Setup

Basic Setup

Advanced Setup

Keying Mode

IKE

Auth Mode

Preshared Key

Phase 1 DH Group

Group 2 - modp1024

Phase 1 Encryption

3DES (168-bit)

Phase 1 Authentication

MD5 HMAC (96-bit)

Phase 1 SA Life Time

28800

seconds

Phase 2 DH Group

Group 2 - modp1024

Phase 2 Encryption

3DES (168-bit)

Phase 2 Authentication

MD5 HMAC (96-bit)

Phase 2 SA Life Time

3600

seconds

Preshared Key

Figure 9-82

IPSec client:

Group Setup:

IPSec

IPSec 1 | IPSec 2

Group Setup | Basic Setup | Advanced Setup

Enable IPSec ☒

IPSec Extensions

Local Security Gateway Interface

Local Security Group Subnet/Netmask ex. 192.168.1.0/24

Local Security Firewalling ☒

Remote Security Gateway IP/Domain WAN port IP of remote device

Remote Security Group Subnet/Netmask ex. 192.168.88.0/24 or 192.168.88.0/24, 192.168.89.0/24

Remote Security Firewalling ☒

Note: The public IP address shown in the figure is set based on the current network environment

Basic Setup:

Default parameters

IPSec 1 | IPSec 2

Group Setup | Basic Setup | Advanced Setup

Keying Mode

Phase 1 DH Group

Phase 1 Encryption

Phase 1 Authentication

Phase 1 SA Life Time seconds

Phase 2 DH Group

Phase 2 Encryption

Phase 2 Authentication

Phase 2 SA Life Time seconds

Preshared Key

Advanced Setup:

Default parameters

IPSec 1

IPSec 2

Group Setup

Basic Setup

Advanced Setup

Aggressive Mode
☐

Compress(IP Payload Compression)
☐

Dead Peer Detection(DPD)
☐

ICMP Check
☐

IPSec Custom Options 1

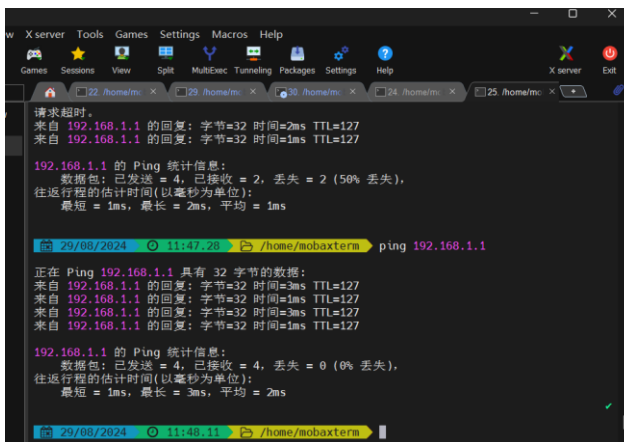
IPSec Custom Options 2

IPSec Custom Options 3

IPSec Custom Options 4

After the configuration is completed and the connection is successful, the IP addresses of the client and server can ping each other, increasing the amount of incoming and outgoing traffic through Ipsec.

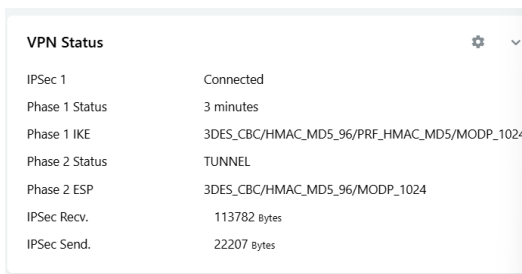
Client ping sever:



VPN Status

VPN Mode	Openvpn Client1
Local IP Address	0.0.0.0
Remote IP Address	0.0.0.0
Connection Status	Disconnected
VPN Mode	Openvpn Client2
Local IP Address	0.0.0.0
Remote IP Address	0.0.0.0
Connection Status	Disconnected
IPSec 1	Connected
Phase 1 Status	11 seconds
Phase 1 IKE	3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
Phase 2 Status	TUNNEL
Phase 2 ESP	3DES_CBC/HMAC_MD5_96
IPSec Recv.	780 Bytes
IPSec Send.	780 Bytes

Sever ping client:





Note: The usage of IPsec server is based on data transmission between clients with limited access.

9.10. DMVPN

DMVPN is a highly scalable IPsec VPN solution, and the so-called high scalability refers to the solution suitable for

large-scale deployment at the enterprise level, for example, for a network environment where an enterprise has hundreds of branch offices.

Due to the limitations of the traditional IPsec VPN star network topology, the central site configuration is large, the traffic delay between branch sites is large, the maintenance cost is too large, and each branch site requires a fixed IP address, so the traditional IPsec is no longer applicable. DMVPN has simple configuration, good performance, supports dynamic IP addresses, provides a fully interconnected topology, zero packet loss, and supports multicast from branch structure to center. It consists of four basic components, namely mGRE, NHRP, Dynamic Routing Protocol, and IPsec.

Step 1: Select "VPN Tunnel>DMVPN" in the navigation bar.

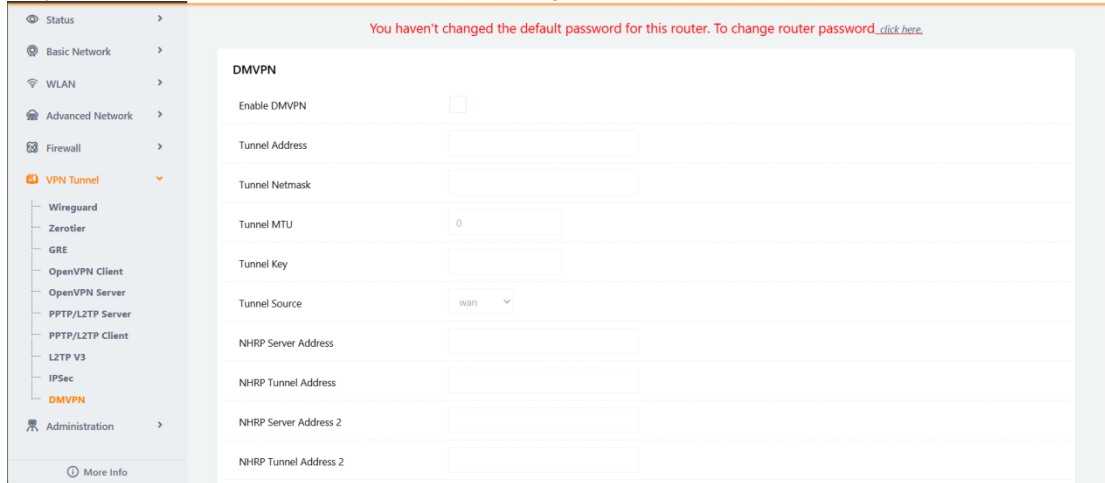


Figure 9-83

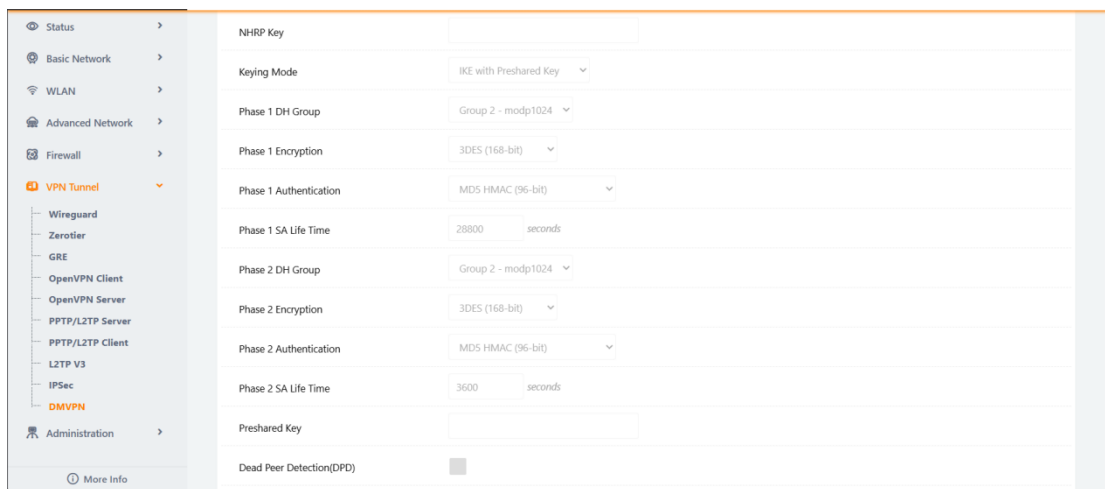
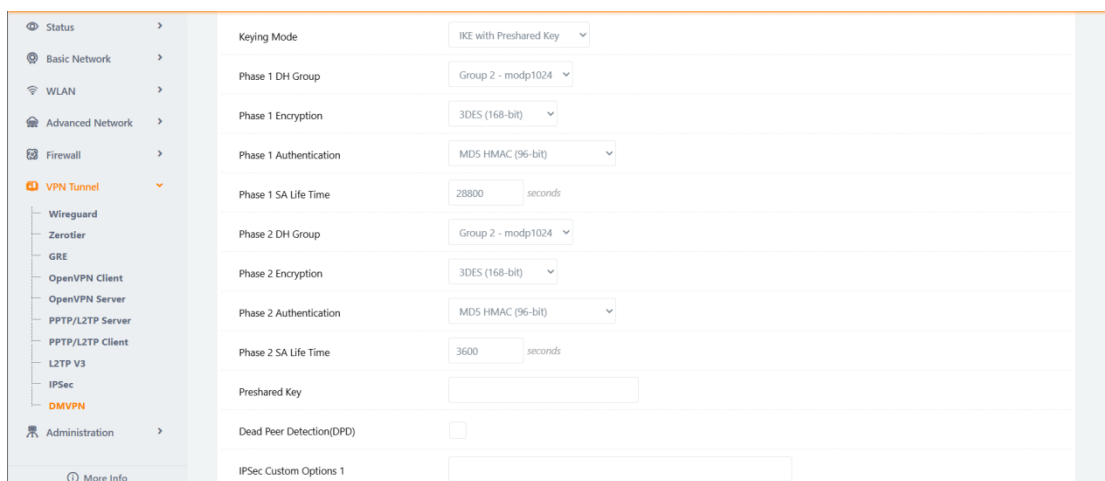


Figure 9-84



Step 2: The DMVPN parameters page is divided into two pages: DMVPN and BGP configuration:

The parameters of D MVPN are described as follows:

parameter	meaning	How to configure
Enable DMVPN	D Enabling and disabling MVPN	The default is disabled
Tunnel address	The tunnel address of the GRE	Default is empty; Format: A. B.C.D/M
Tunnel mask	Tunnel mask for GRE	Default is empty; Format: A. B.C.D/M
Tunnel MTU	GRE tunnel MTU value	The default is 0; Range: 0-2000
Tunnel key	GRE tunnel key	Default is empty;
Tunnel Source	Contains modem, wan, sta, sta2	Default: modem
Key mode	I KE/IKE v2 with Preshared Key	Default IKE
DH Group	Group 1, Group2, Group5 are supported	Default Group2
Encryption	Supports 3DES,AS-128, AES-192, AES-256	Default 3DES
Authentication	Support NONE, MD5, SHA1, SHA2	Default MD5
Phase 1 SA Life Time	The duration of the SA in Phase 1	The default is 28800 Unit: seconds Range: 1-86400
Phase 2 SA Life Time	The duration of the SA in Phase 2	The default is 28800 Unit: seconds Range: 1-86400
Preshared key	The key of the IPSec must be the same as that of the server	Default is empty
DPD (Dead Peer Detection)	Enabling and disabling digital distortion detection	Default: Disabled

Check Period Time Interval	The interval between the tests once	Default: 30 Unit: seconds Range: 1-86400
Check Timeout Interval	IPSec detection timeout period	Default: 150 Unit: seconds Range: 1-86400
IPSec Custom Options 1-4	IPSec custom content	Default is empty

Table 9-17 DMVPN parameters

Step 3:D configure the parameters on the MVPN page (including the BGP parameters on the Route Table Settings page).

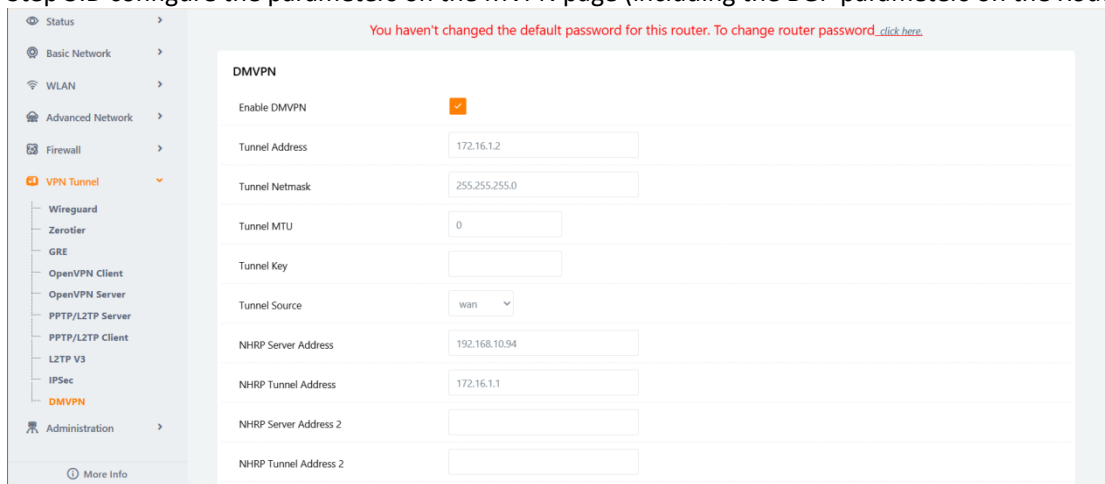


Figure 9-85

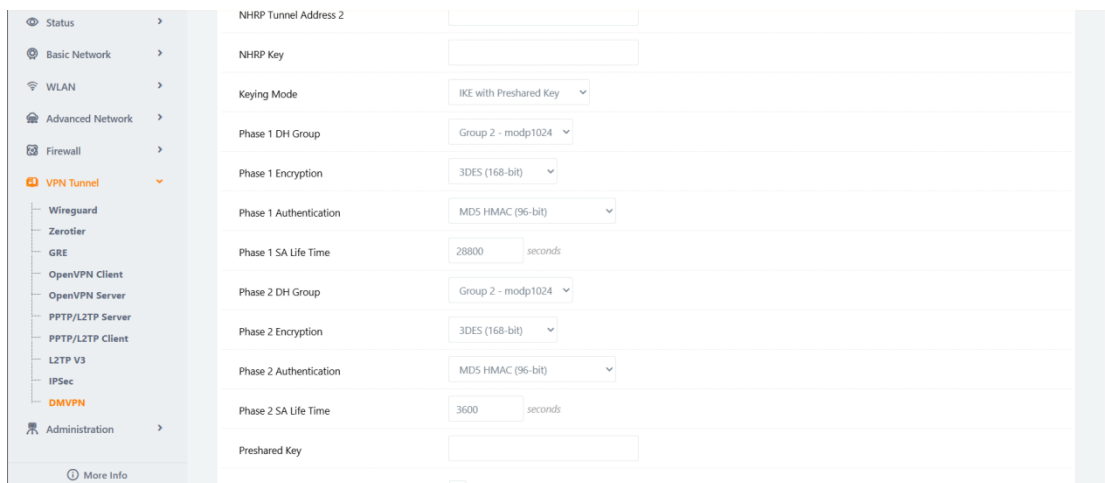


Figure 9-86

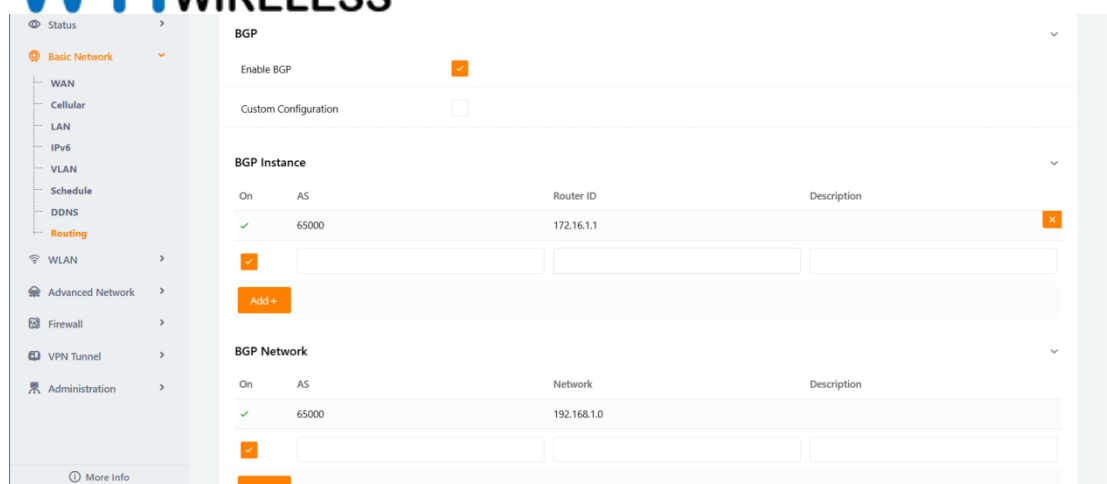


Figure 9-87

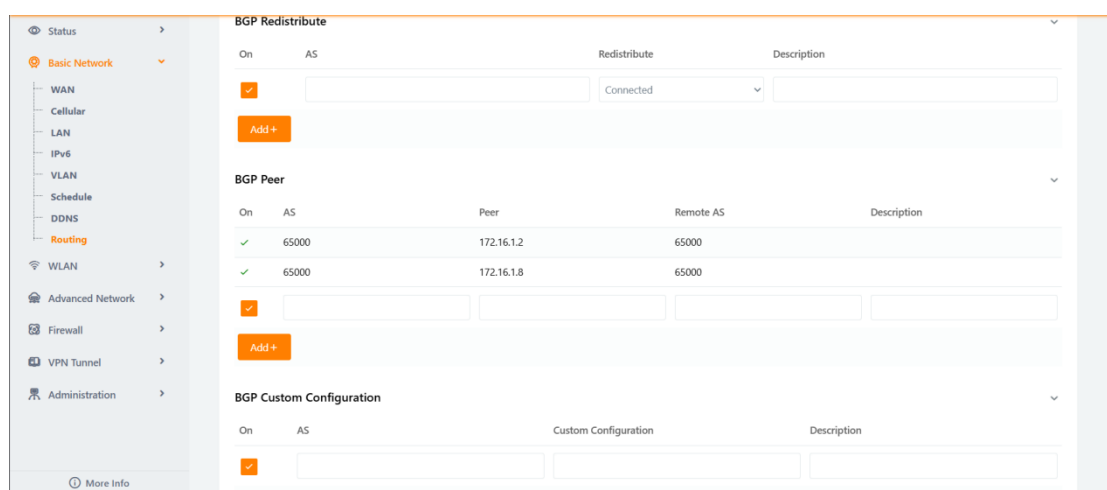


Figure 9-88

Figure 9-89

Step 4: After the configuration is complete, view the information about the route table, as follows:

R1