Check VPN Status on RV016 RV042 RV042G and RV082 VPN Routers

Objective

A Virtual Private Network (VPN) is a secure connection between two end points. The VPN creates a secure tunnel between these two end points and provides security to the data traffic along the tunnel. A Virtual Private Network (VPN) is a secure connection established within a network or between networks. In order for this tunnel to work properly, the VPN configuration on both sides of the connection must be performed carefully and some information must match. The objective of this document is to explain how to check VPN status on RV016, RV042, RV042G, and RV082 VPN Routers. VPNs serve to isolate traffic between specified hosts and networks from the traffic of unauthorized hosts and networks.

Applicable Devices

- RV016
- RV042
- RV042G
- RV082

Software Version

- 4.2.1.02

Common VPN Parameters to Check

In order for a VPN connection to work properly, the two ends of the connection must meet the same requirements. When there is a failure in the VPN connection, there are two things you can check that can make the difference. These are:

- The local IP address conflicts between the two VPN endpoints.

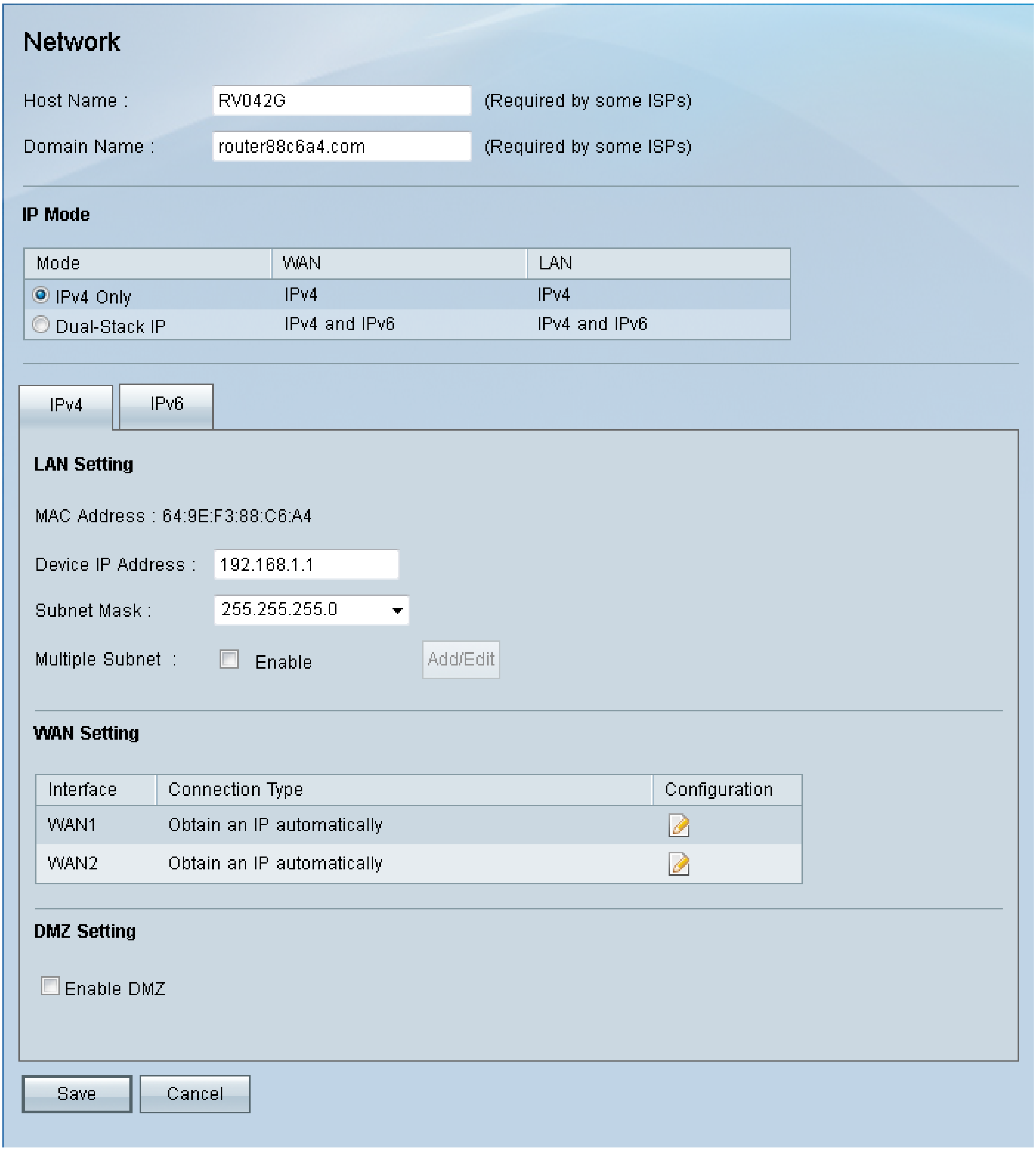
- There are differences in the encryption and authentication settings of the two end points.

The next section will explain how to check the IP address scheme of a VPN and how to make the correct changes.

Change the LAN IP Address of the Router

The LAN interface of both ends of the VPN connection must be part of a different network address. If both parts belong to the same network address, the VPN connection will not work. The following steps explain how to make changes on your LAN IP address on RV042, RV042G, and RV082 VPN Routers.

Step 1. Log in to the web based configuration utility and choose **Setup > Network**. The *Network* page opens:



Network

Host Name : RV042G (Required by some ISPs)

Domain Name : router88c6a4.com (Required by some ISPs)

IP Mode

Mode	WAN	LAN
● IPv4 Only	IPv4	IPv4
○ Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

LAN Setting

MAC Address : 64:9E:F3:88:C6:A4

Device IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

Multiple Subnet : □ Enable

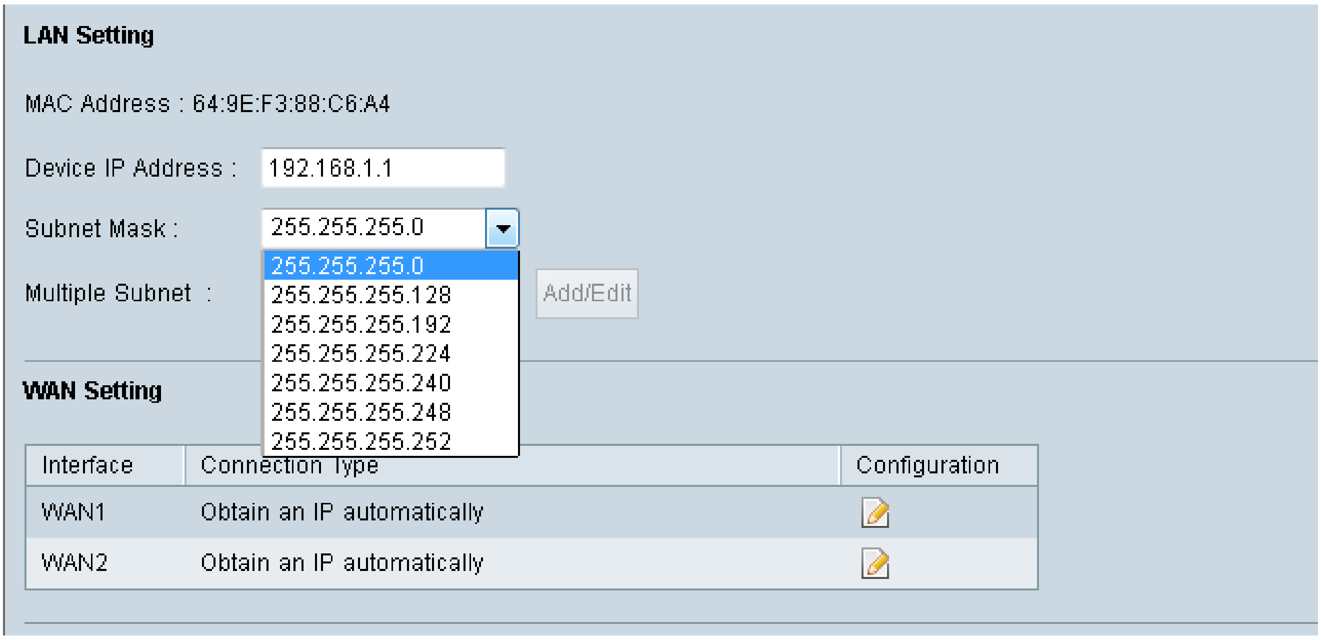
WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	✎
WAN2	Obtain an IP automatically	✎

DMZ Setting

□ Enable DMZ

Step 2. Under LAN Setting, in the Device IP Address field, enter an IP address that belongs to a different network address of the other end of the VPN connection.



LAN Setting

MAC Address : 64:9E:F3:88:C6:A4

Device IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	✎
WAN2	Obtain an IP automatically	✎

Step 3. In the Subnet Mask drop-down list, choose the appropriate subnet mask for your VPN connection.

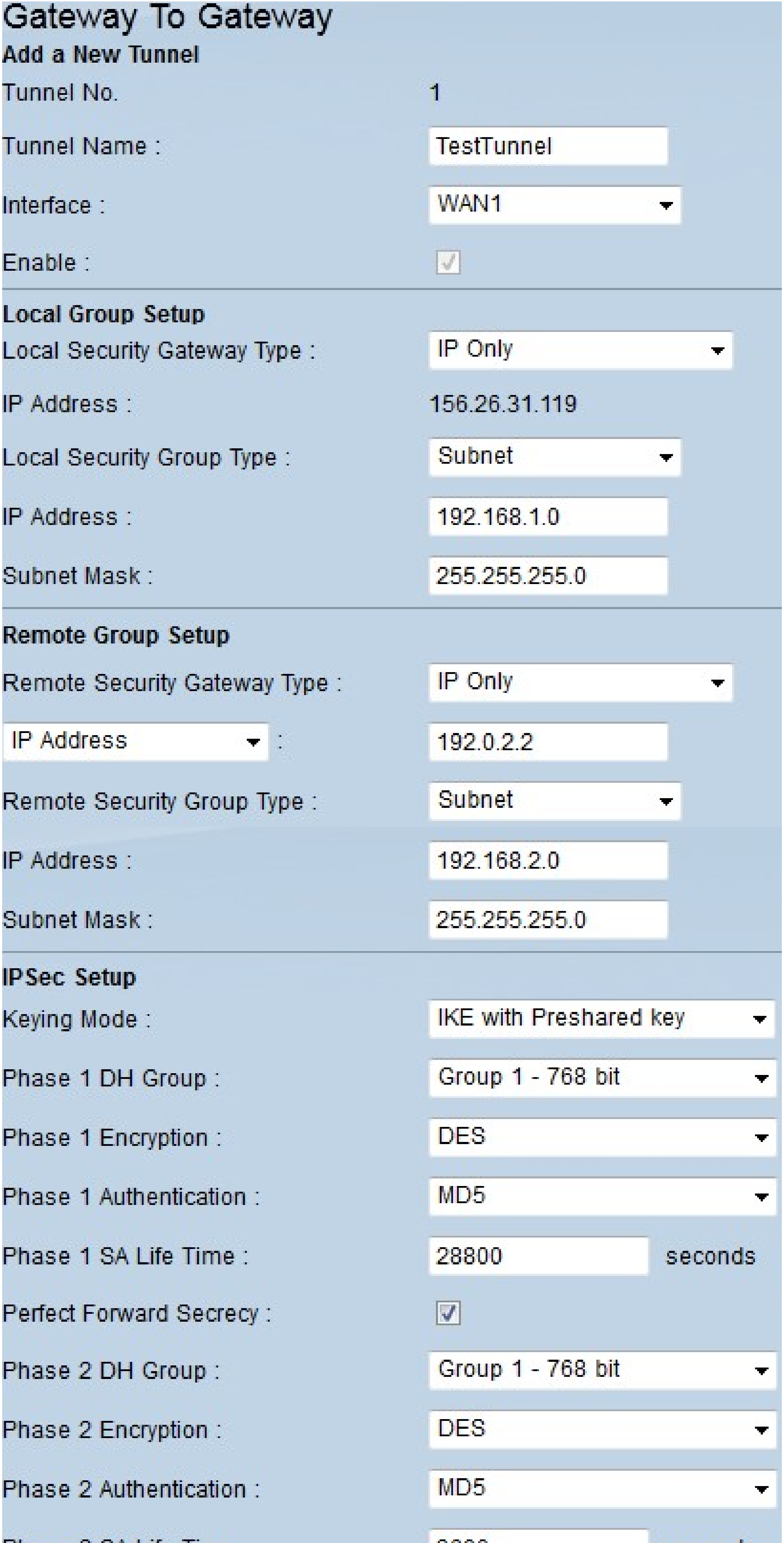
Step 4. (Optional) To enable the use of multiple subnets, in the Multiple Subnet field, check the Enable checkbox.

Step 5. Click **Save** to apply your new settings.

Check the Security Parameters of the VPN Connection

The security setup of the VPN connection must be the same on each end of the connection. The next steps explains how to check these parameters on RV042, RV042G, and RV082 VPN Routers.

Step 1. Log in to the web based configuration utility and choose **VPN > Gateway to Gateway**. The *Gateway to Gateway* page opens.



Gateway To Gateway

Add a New Tunnel

Tunnel No.	1
Tunnel Name :	TestTunnel
Interface :	WAN1
Enable :	☑

Local Group Setup

Local Security Gateway Type :	IP Only
IP Address :	156.26.31.119
Local Security Group Type :	Subnet
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Remote Group Setup

Remote Security Gateway Type :	IP Only
IP Address :	192.0.2.2
Remote Security Group Type :	Subnet
IP Address :	192.168.2.0
Subnet Mask :	255.255.255.0

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 1 - 768 bit
Phase 1 Encryption :	DES
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	☑
Phase 2 DH Group :	Group 1 - 768 bit
Phase 2 Encryption :	DES
Phase 2 Authentication :	MD5

Step 2. Check the following parameters. Make sure both ends of the VPN connection have the same settings:

- Local Security Group Type is the same as the local router's LAN segment.

- Remote Security Group Type is the same as the remote router's LAN segment.

- Remote Security Gateway Type is the WAN/Internet IP address of the remote router.

- IPSec Setup fields must match on both sides of the VPN tunnel.

- Pre-shared Key must be the same on both sides of the VPN tunnel.

Step 3. (Optional) Click **Advanced+** for more security properties. As before, these settings must be the same in both sides of the connection.

Step 4. Click **Save** to apply the new settings if anything was changed.