R102 Industrial Router

User Manual

Version: 1.5

© Vantron Technology, Inc. All rights reserved.

Revision History:

No.	Software Version	Description	Date
V1.0	V200R003	First release, software version: V200R003	Feb. 10, 2022
V1.1	V200R003	Replaced screenshots Added 3.6.2 Manufacturer Info Customization	Mar. 9, 2022
V1.2	V200R003	Added more details for configuration of the pre-certified 4G module in 3.5.3	Mar. 23, 2022
V1.3	V200R003	Updated hardware connection	Nov. 17, 2022
V1.4	V200R003	System integration, updated file accordingly	Mar. 14, 2023
V1.5	V200R003	1. Deleted the Networking section under quick start as per system change; 2. Modified the wording as per the system change	Nov. 14, 2023

Table of Contents

Foreword 1
CHAPTER 1 HARDWARE DESCRIPTION 5
1.1 Product Overview 6
1.2 Unpackaging 7
1.3 Specifications 8
1.4 Definition of Interfaces 9
1.5 Serial Port Introduction 11
CHAPTER 2 GETTING STARTED 12
2.1 Setting up the Router 13
2.2 Router Login 15
2.3 Password Change 16
2.4 Language Change 16
2.5 Interfacing with Vantron Gateway Management Platform 17
CHAPTER 3 ROUTER SETUP VIA VANTRONOS 18
3.1 Introduction to VantronOS 19
3.2 Status 20
3.3 Quick Start— Auto Routing 22
3.4 Virtual Tunnel 25
3.4.1 OpenVPN Server 25
3.4.2 VPN Client 27
3.5 IPSec Connection 28
3.5.1 Prerequisites 28
3.5.2 Certificate Setup 29
3.5.3 Secret Setup 31
3.5.4 IPSec Connection Setup 33
3.6 Network 56
3.6.1 Interfaces 56
3.6.1.1 LAN 57
3.6.1.2 WAN 60
3.6.2 Wireless (WIFI) 64
3.6.2.1 Wi-Fi – AP Mode (General settings) 64
3.6.2.2 Wi-Fi – AP Mode (Advanced setting) 65
3.6.2.3 Wi-Fi – Client Mode 66
3.6.3 4G/LTE 69
3.6.4 Static Routes 73
3.6.5 Firewall 75
3.6.5.1 Firewall – General Settings 75
3.6.5.2 Firewall – Zones 76
3.6.5.3 Firewall – Port Forwards 77
3.6.5.4 Firewall – Custom Rules 77
3.6.6 VTShark 78

3.7 User Management 81
3.8 Customization 82
3.8.1 Custom Program 82
3.8.2 IPK Installer 83
3.8.3 Manufacturer Info Customization 84
3.8.4 DMP Agent 85
3.9 Hardware 86
3.9.1 Ser2TCP 86
3.9.2 Ser2net environment setup and verification 86
3.9.3 Protocol comparison 92
3.10 Services 93
3.10.1 Dynamic DNS 93
3.10.2 RC to PLC 93
3.11 System 95
3.11.1 System 95
3.11.2 Netlink Bandwidth Monitor (NBM) Setting 97
3.11.3 Administration 99
SSH Access 99
3.11.4 Terminal 101
3.11.5 Mount Points 102
3.11.6 Backup/Flash Firmware 104
3.11.7 Reboot 107
3.12 Logout 107
CHAPTER 4 DISPOSAL AND PRODUCT WARRANTY 108
4.1 Disposal 109
4.2 Warranty 110
Appendix Regulatory Compliance Statement 111

Foreword

Thank you for purchasing R102 Industrial Router ("the Router" or "the Product"). This manual intends to provide guidance and assistance necessary on setting up, operating or maintaining the Product. Please read this manual and make sure you understand the structure and functionality of the Product before putting it into use.

Intended Users

This manual is intended for:

- Network architects
- Network administrators
- Technical support engineers
- Other users

Copyright

Vantron Technology, Inc. ("Vantron") reserves all rights of this manual, including the right to change the content, form, product features, and specifications contained herein at any time without prior notice. An up-to-date version of this manual is available at www.vantrontech.com.

The trademarks in this manual, registered or not, are properties of their respective owners. Under no circumstances shall any part of this user manual be copied, reproduced, translated, or sold. This manual is not intended to be altered or used for other purposes unless otherwise permitted in writing by Vantron. Vantron reserves the right of all publicly released copies of this manual.

Disclaimer

While all information contained herein has been carefully checked to assure its accuracy in technical details and typography, Vantron does not assume any responsibility resulting from any error or features of this manual, nor from improper uses of this manual or the software.

It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without notice.

Technical Support and Assistance

Should you have any question about the Product that is not covered in this manual, contact your sales representative for solution. Please contain the following information in your question:

- Product name and PO number;
- Complete description of the problem;
- Error message you received, if any.

Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538
Tel: (650) 422-3128
Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- Part 15 of the FCC Rules
- PTCRB

Please refer to **Appendix** for Regulatory Compliance Statement.

Symbology

This manual uses the following signs to prompt users to pay special attention to relevant information.

	Caution for latent damage to system or harm to personnel
	Attention to important information or regulations

General Safety Instructions

The Product is supposed be installed by knowledgeable, skilled persons familiar with local and/or international electrical codes and regulations. For your safety and prevention of damage to the Product and other equipment connected to it, please read and observe carefully the following safety instructions prior to installation and operation. Keep this manual well for future reference.

- Do not disassemble or otherwise modify the Product. Such action may cause heat generation, ignition, electronic shock, or other damages including human injury, and may void your warranty.
- Keep the Product away from heat source, such as heater, heat dissipater, or engine casing.
- Do not insert foreign materials into any opening of the Product as it may cause the Product to malfunction or burn out.
- To ensure proper functioning and prevent overheating of the Product, do not cover or block the ventilation holes of the Product.
- Follow the installation instructions with the installation tools provided or recommended.
- The use or placement of the operation tools shall comply with the code of practice of such tools to avoid short circuit of the Product.
- Cut off the power before inspection of the Product to avoid human injury or product damage.

Precautions for Power Cables and Accessories

⚠ Use proper power source only. Make sure the supply voltage falls within the specified range.

⚠ Place the power cable properly at places without extrusion hazards.

⚠ Cleaning instructions:

- Power off before cleaning the Product
- Do not use caustic or aggressive liquids, vapor, or spray
- Clean with a damp cloth
- Do not try to clean exposed electronic components unless with a dust collector

⚠ Power off and contact Vantron technical support engineer in case of the following faults:

- The Product is damaged
- The temperature is excessively high
- Fault is still not solved after troubleshooting according to this manual

⚠ Do not use in combustible and explosive environment:

- Keep away from combustible and explosive environment
- Keep away from all energized circuits
- Unauthorized removal of the enclosure from the device is not allowed
- Do not change components unless the power cable is unplugged
- In some cases, the device may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the device before replacement of the components.

CHAPTER 1 HARDWARE DESCRIPTION

1.1 Product Overview

Vantron R102 industrial wireless router is designed for industrial IoT that combines dual SIM LTE, Wi-Fi, Ethernet, and virtual private network to meet diversified networking requirements. R102 industrial router applies a communication tactic that uses multiple channels with failover protocol, which together with the high-reliability watchdog maintains a secure and stable network access. As is compact in size, R102 supports panel mount, DIN rail mount, and wall mount to meet the requirements of varying sites. Meanwhile it provides access to Vantron BlueSphere cloud platform for unified management to ease the efforts of users by real-time monitoring and tracking, remote maintenance and OTA updates, task assignment and follow-up.

Featuring high stability and reliability, excellent cost performance, and convenient networking deployment, Vantron R102 industrial router is especially suitable for large-scale distributed networking in the following scenarios:

Intelligent business: parcel lockers, meal delivery cabinets, charging piles, ATM machines, digital signages, etc.;

Smart city: supply of heat, water, gas and oil, etc.;

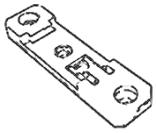
Intelligent security and intelligent transportation;

Monitoring of cranes and other devices on construction sites;

Monitoring of environmental protection devices, water conservancy devices etc.

1.2 Unpackaging

The Product has been carefully packed with special attention to quality. However, should you find any component damaged or missing, please contact your sales representative in due time.

Standard accessories		Optional accessories	
	1 x R102 router		1 x Power adapter
	2 x Wi-Fi antenna		1 x DC power connector
	1 x DIN rail mounting bracket		2 x 4G LTE antenna

Actual accessories might vary slightly from the list above as the customer order might be different from the standard configuration options.

1.3 Specifications

R102		
System	Memory	128MB DDR2
	Storage	32MB Flash
Communication	Ethernet	2 x RJ45, 10/100Mbps
	Wi-Fi	2.4GHz, IEEE 802.11 b/g/n, 300Mbps, AP & Client
	4G LTE	CAT M/4
	WAN protocol	PPP, PPPoE, DHCP
I/Os	Serial port	1 x RS485 (default)
	SIM slot	2 x Drawer-type SIM slot
	Antenna	2 x LTE antenna, 2 x Wi-Fi antenna
	Grounding	Enclosure & PCB
System Control	Reset button	1 x Reset button
	LED indicator	3 x Signal strength indicator 1 x Power indicator 1 x Status indicator 1 x Internet indicator 1 x WLAN indicator
Mechanical	Dimensions	93.8mm x 93.3mm x 29mm
	Enclosure	Metal
	Installation	DIN rail mounting
	IP rating	IP30
	Cooling mode	Fanless
Power	Input	9-36V DC, over-current protection, reverse polarity protection
Software	OS	VantronOS based on Linux
	Network management	SNMP v1/v2c/v3
	Device management platform	Vantron BlueSphere
Security	Firewall	Supported
	Data security	PPTP, L2TP, GRE, IPSec, OpenVPN
	Link detection	Heartbeat detection, automatic reconnection
	Network reliability	Multi-channel failover, Ethernet, Wi-Fi, 4G LTE backup
	Dual SIM switch	Dual backup, automatic switch
	IP application	Ping, Traceroute, DHCP Server/Client, DDNS
	IP Routing	Static routing
	NAT	Supported
Environment Condition	Temperature	Operating: -20℃~+60℃ Storage: -40℃~+70℃
	Humidity	Storage: RH 5%~95% (non-condensing)
	Certification	CCC, CE, FCC, PTCRB

1.4 Definition of Interfaces

1.4.1 LED Indicators

1. 4G LTE signal strength indicator

Signal strength	Description
≥66.67%	The three indicators turn solid green
Between 33.34% and 66.66%	The bottom two indicators turn solid green
≤33.33%	The bottom indicator blinks

2. Power indicator

When the Router is powered on, the power indicator will turn solid green.

3. Status indicator

System action	Description
System bootup	The indicator blinks
System running properly	The indicator turns solid green
System upgrade or settings clear-up	The indicator blinks

4. Internet indicator

Network connectivity of the Router	Description
Yes	The indicator blinks
No	The indicator is off

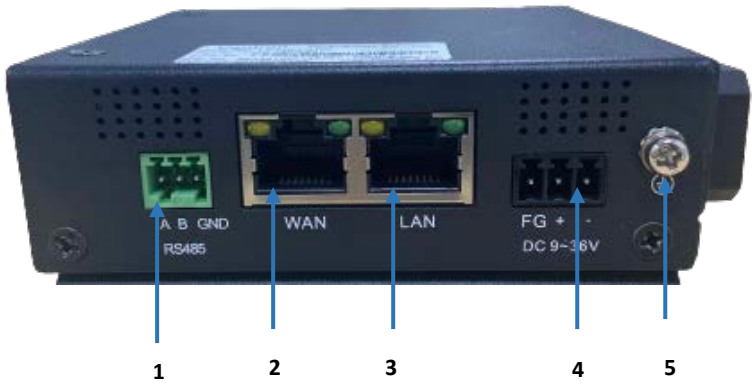
5. Wi-Fi indicator

Wi-Fi module status	Description
A client is connecting to the Router via Wi-Fi	The indicator blinks quickly
A client is connected to the Router via Wi-Fi	The indicator blinks slowly, and turns solid green in the end
The Wi-Fi network is not in use	The indicator is off

1.4.2 Left Side View

Interface	Description
1	WLAN antenna connector 1
2	Micro SIM slot 1
3	4G LTE antenna connector 1
4	Micro SIM slot 2
5	4G LTE antenna connector 2 (reserved)
6	Micro SD card slot (reserved)
7	WLAN antenna connector 2
8	Reset button Press the button and hold for 3-10 seconds, the Router will be factory reset. The system will reboot after the factory reset.

1.4.3 Right Side View



Interface	Description
1	RS485
2	WAN port, set as eth0.2 in VantronOS
3	LAN port, set as eth0.1 in VantronOS
4	9-36V DC power terminal
5	Grounding screw

1.5 Serial Port Introduction

The serial port is in RS485 mode. Pinout description of the port is as follows:

No.	Pin	Node name	Port	Type	Definition
1	A	/dev/ttyS1	COM1	I/O	RS485 A signal
2	B			I/O	RS485 B signal
3	GND			NC	Isolated ground

Input the following command line to open the serial port with a serial port communication program (e.g., microcom):

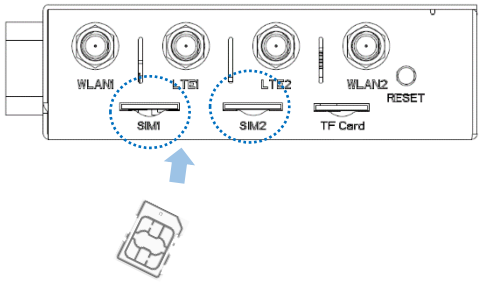
```
~# microcom /dev/ttyS1 -s 115200
```

CHAPTER 2 GETTING STARTED

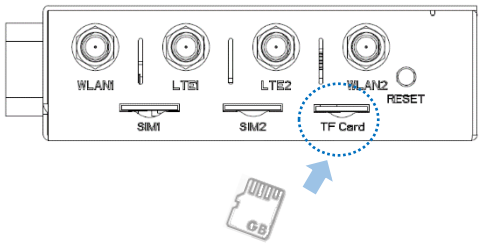
2.1 Setting up the Router

Before you proceed with configuration of the Router, follow the steps below to finish hardware connection.

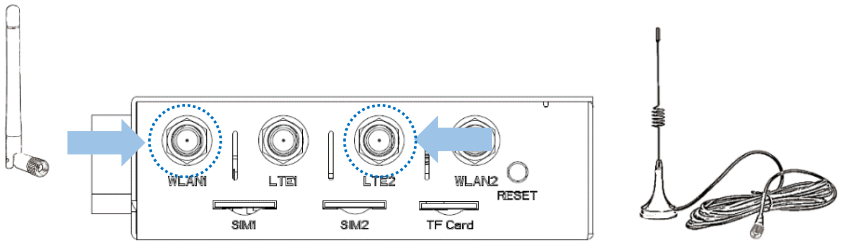
1. Use the mounting bracket and screws provided to install the Router to a secure place;
2. Insert an activated Micro SIM card into either of the SIM slots with the gold-colored contacts facing up and the clipped side inward (dual SIM supported);



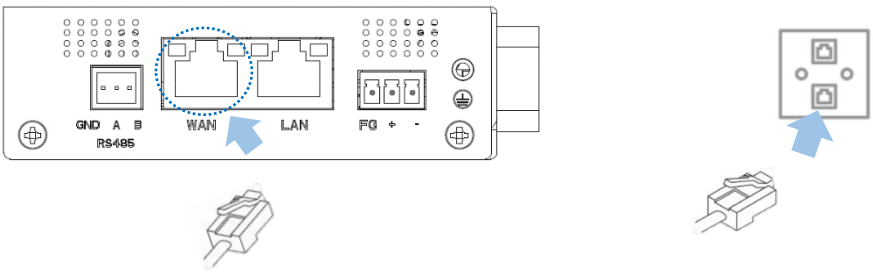
3. Push the Micro SIM card to secure it;
4. Insert a Micro SD card into the TF card slot with the gold-colored pins facing up;



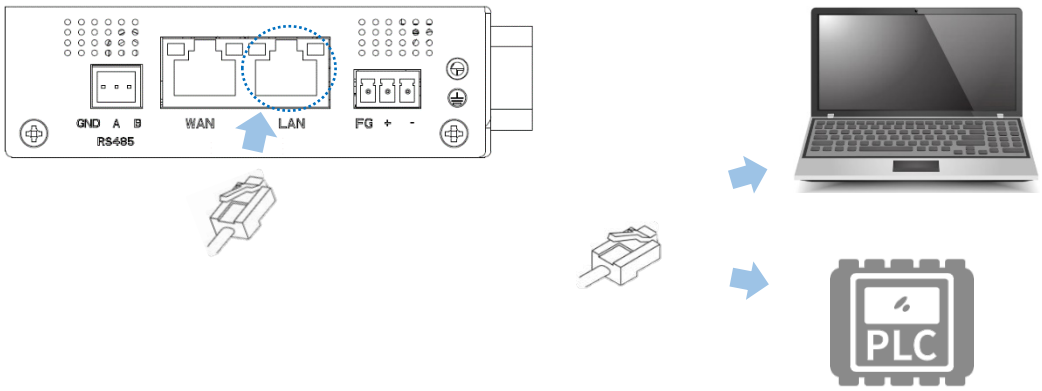
5. Install the round head antennas to WLAN antenna connector and the sucker antennas to the LTE antenna connectors, then tighten the rotating heads to secure the antennas in proper position;



6. Connect one end of an Ethernet cable to the WAN port of the Router and the other to a live Ethernet port;

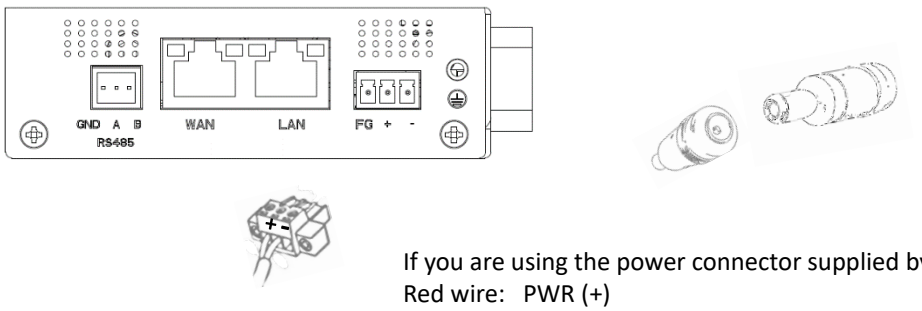


7. Connect one end of another Ethernet cable to a LAN port of the Router and the other to a host computer or client device depending on your use;;



Skip the Ethernet connection steps if you choose wireless network connection.

8. Connect the terminal end of the female DC power connector to the power terminal of the Router and the round end to the adapter;



If you are using the power connector supplied by Vantron:
Red wire: PWR (+)
Black wire: GND (-)

9. Plug the adapter to a power outlet that meets the supply voltage requirement (9V to 36V) to turn on the Router;

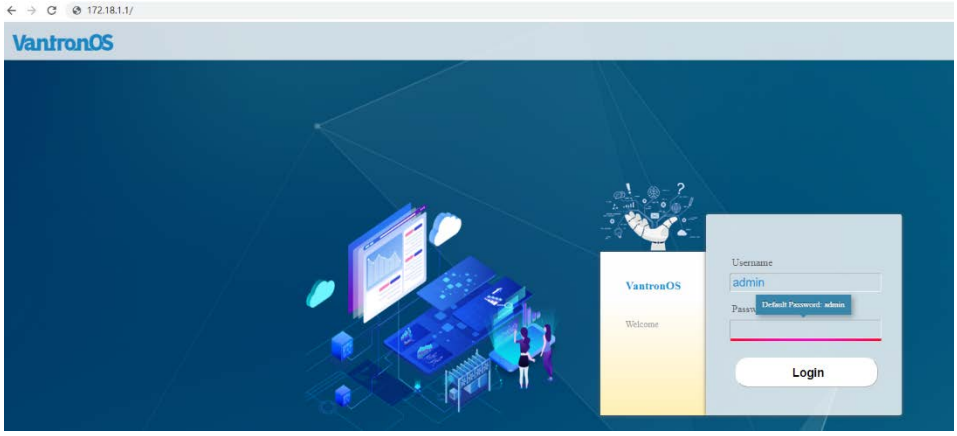
10. The power indicator will turn solid green upon power application.

The antennas might be different from what used for illustration here. Should you have any trouble installing the antennas, please contact the sales executive for solution.

2.2 Router Login

The Router is designed to allow network connectivity with minimal configuration. That said, you can configure the network settings and customize the Router from VantronOS interface.

1. Input the LAN port IP address of the Router in your browser to log in the VantronOS web interface (default: http://172.18.1.1/).
   - Default user: **admin** / Super user: **root**
   - Default password: **admin** / Super user password: **rootpassword**



2. For SSH login, use the LAN port IP address (default: http://172.18.1.1/).
   - Port: **22**
   - Account: **root**
   - Password: **rootpassword**

The web login address coincides with the LAN port IP address of the Router, so you might have to change the login address when you reset the IP address.

*SSH login is disabled by default, refer to **SSH Access** included in 3.10.3 for more details.*

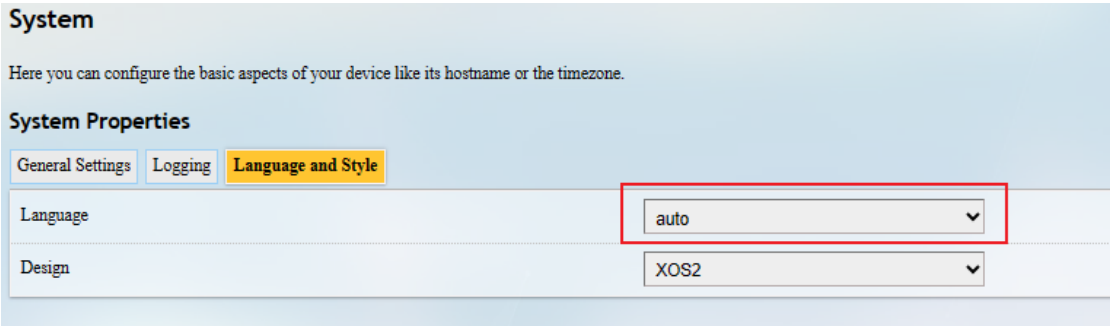
2.3 Password Change

It is up to you to decide whether you would like to change the login password after logging in VantronOS.

1. Navigate to **System > Administration**;
2. Input the original password for the current user;
3. Input a new password and confirm the password;
4. Save the settings and apply;
5. The system will log out automatically;
6. Log in with the new password.

2.4 Language Change

Currently the system supports simplified Chinese and English. The system language is set to automatically follow your browser language by default. You can change the system language by navigating to **System > System > Language and Style**.



Auto: System language based on the browser language (default)

English: English interface

Simplified Chinese: Simplified Chinese interface

2.5 Interfacing with Vantron Gateway Management Platform

BlueSphere Gateway Management Platform ("GWM") is a cloud-based management portal that empowers organizations to seamlessly provision, monitor, and manage Vantron IoT communication devices, including gateways, routers, and DTUs. By leveraging BlueSphere GWM, organizations can streamline device setup, ensure real-time visibility into device performance, and effortlessly control device configurations. This contributes to enhanced operational efficiency and improved decision-making.

Before you can use the BlueSphere GWM for remote management of Vantron IoT devices, please make sure the following prerequisites are met:

- You have obtained a license for login to the BlueSphere GWM
- The DMP agent is installed on the device for remote management
- The DMP agent is “enabled” (Refer to 3.10.4 DMP Agent for the configuration)
- The serial number of the device is added to the BlueSphere GWM

CHAPTER 3 ROUTER SETUP VIA VANTRONOS

3.1 Introduction to VantronOS

VantronOS is an intelligent operating system developed by the Vantron team, featuring independent system and function development. It is built upon the Linux system and optimized for embedded hardware. The operating system follows a modular design and plug-in expansion approach, utilizing the Linux kernel with a built-in firewall to ensure secure internet connectivity for Vantron IoT communication devices, protecting them from potential attacks.

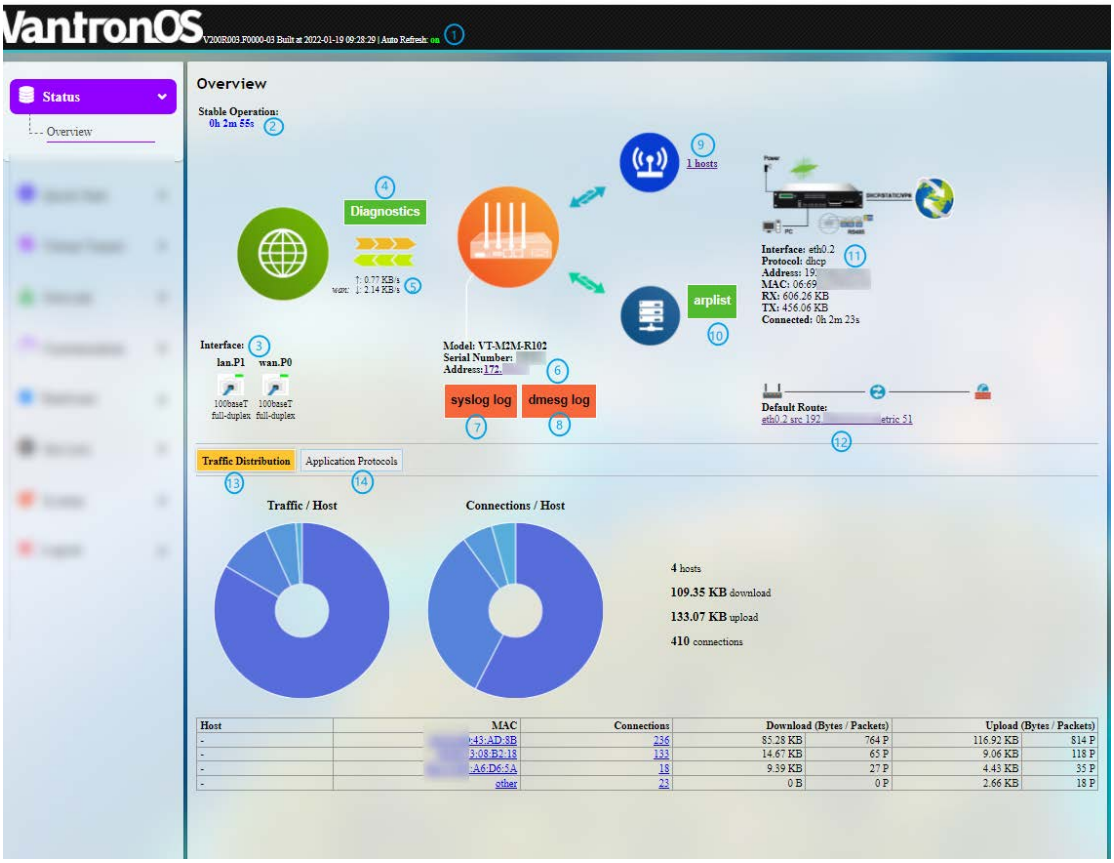
VantronOS incorporates a user-friendly UI interface based on the MVC framework, providing a simple and efficient setting entry for users. Additionally, it offers seamless interfacing with various cloud management platforms, including the self-developed BlueSphere GWM, as well as popular platforms like Azure, Alibaba Cloud, Huawei Cloud, and RootCloud. This enables users to remotely monitor, operate, and diagnose devices without the need for on-site technical support engineers. VantronOS facilitates the interconnection and interaction between users and the Industrial Internet of Things, enhancing the overall efficiency and convenience of device management.

In the following sections, should you find any features not displayed in the VantronOS interface as an 'admin' user, please log in with the root account.

Make sure to save all settings and changes before exit to let them take effect.

3.2 Status

This page provides the overall information of the Router, including stable operation duration, number of devices connected to the Router via wireless or Ethernet connection, default routing, hardware information, traffic statistics, etc.



Description of the numbered areas

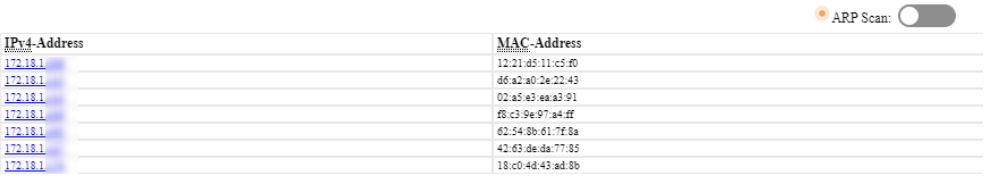
1. Firmware version and auto refresh on/off
2. Stable running time of the Router since network connection
3. Current working status of Ethernet ports

(Both the LAN port and WAN port are connected in this case)

4. A collection of network diagnostic tools
5. Instant default exit traffic
6. The model, serial number, and management address of the router in use
7. System log information
8. Kernel log information
9. Number of clients connected to the Router via Wi-Fi

You will access Wi-Fi settings upon a click of the number.

10. Address information of clients connected to the Router



11. Details of the router connectivity

The illustrative image varies with the communication module on the Router.

12. Default route currently used by the Router
13. Traffic distribution of clients connected to the Router displayed by MAC addresses

Clicking on each MAC address in the table at the page bottom will get the detailed traffic information of the clients.

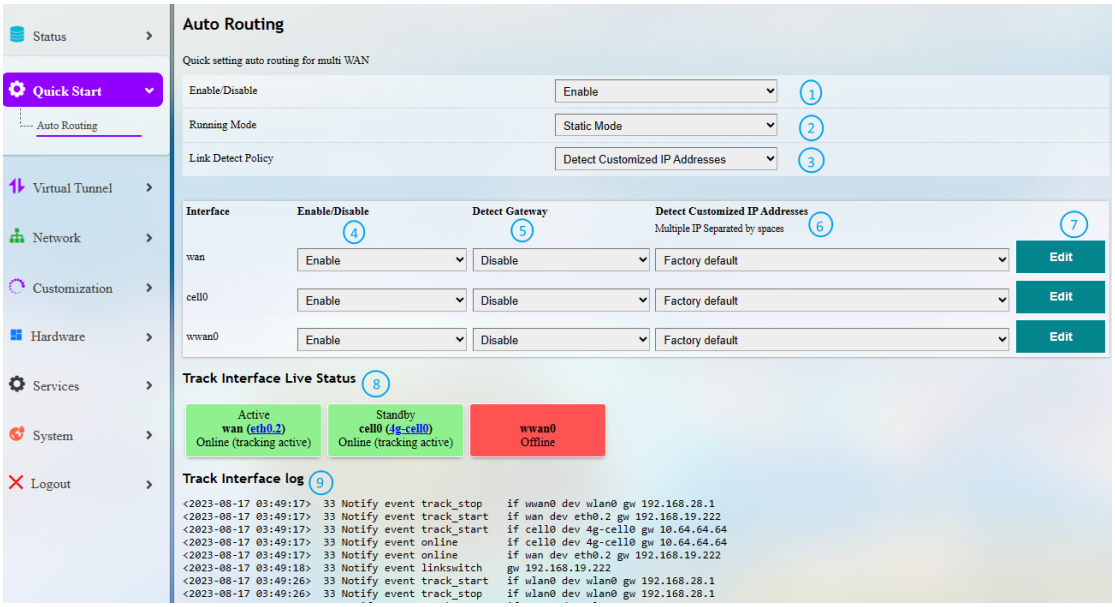
14. Application layer protocols

HTTPS, HTTP, and POP3S represent the top 3 protocols for data download and upload. HTTPS, HTTP and DNS represent the top 3 protocols for device connection.

3.3 Quick Start— Auto Routing

Automatic routing ensures that the Router maintains Internet access when multiple links are available. It features automatic link detection, automatic route switching, and recovery.

The default link detection and data forwarding are prioritized based on the following rule: Ethernet > Wi-Fi > LTE > others.



Description of the numbered areas

1. Enable/Disable route tracking
2. Mode of the automatic routing (refer to the details below)
3. Automatic link detection policy (refer to the details below)
4. Enable/Disable link detection for a specific network interface

   In the screenshot above, wan stands for Ethernet connection, cell0 for cellular connection, and wwan0 for Wi-Fi connection.
5. Enable/Disable gateway detection
6. Customized IP address detection (heartbeat or gateway address)
7. Edit the auto routing rule of a specific network interface (refer to the details below)
8. Link status
9. Link detection log and service running log

Mode of the automatic routing

Mode	Description
Static mode (Default)	1. The user-designated link priority takes precedence; 2. If the user does not designate the link priority, the default rule will apply.
Dynamic mode	1. The default rule governs the entire routing policy; 2. The user-designated link priority will be disabled. This is not recommended when special applications are installed on the Router that rely on the designated link priority.

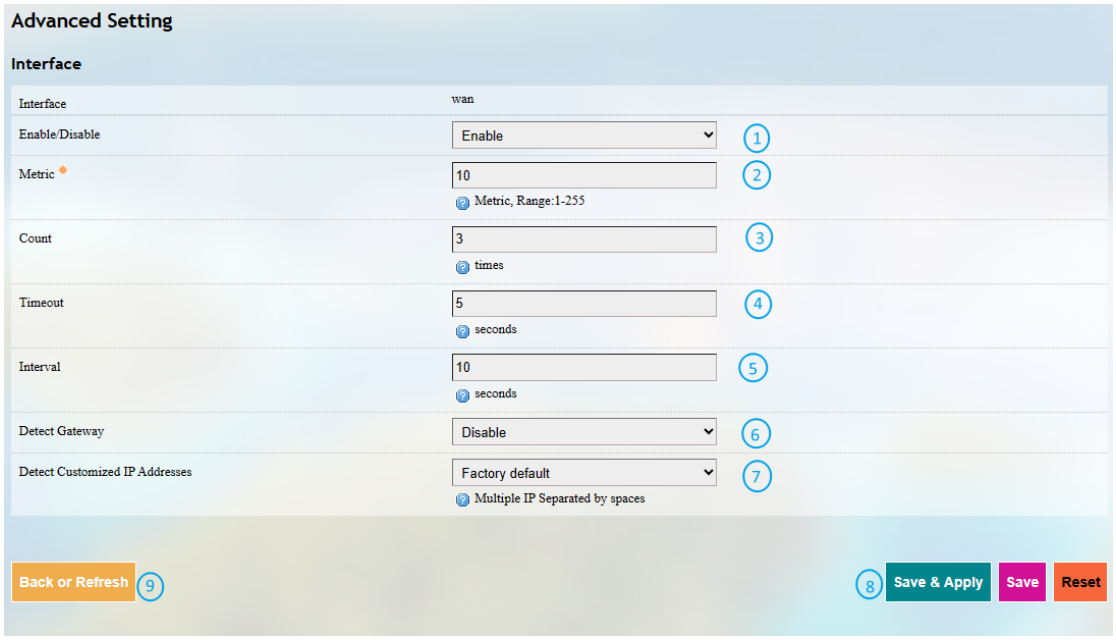
Automatic link detection policy

Policy	Description
Detect customized IP addresses (Default)	1. You can set IP addresses for a specific network interface. If these IP addresses have packets received and transmitted, the interface is active and set “Online”; 2. If the Router is located at a place without access to external network, please change the policy to “Detect gateway” or add some IP addresses that the Router can detect.
Detect gateway	This policy is to identify the IP address of the gateway on the current network. You are recommended not to apply this policy for P2P/PPP connection scenarios, in which circumstance, verifying the public network IP address (such as 8.8.8.8) is recommended.

Note:

1. Please choose an appropriate policy based on the device’s network position and the network access protocol used by the network interface.
2. If you have configured for both “Detect customized IP addresses” and “Detect gateway”, the gateway detection will take precedence.
3. If you have selected “Detect customized IP addresses” but have not provided any IP address, it will automatically switch to gateway detection.
4. Refer to the next page on editing the routing rules for more details.

Clicking on the **Edit** button behind an interface will direct you to the rule editing page as follows.



Description of the numbered areas

1. Enable/Disable the route tracking on this interface
2. Gateway metric (The smaller the number, the higher the priority)
3. The count of total messages sent in case of a detection timeout (3 by default)
4. The timeout for a single tracking (5s by default)
5. Tracking interval, defined as from the completion of one tracking to the initiation of the next tracking (10s by default)
6. Enable/disable gateway detection
7. Select the default IP addresses (‘factory default’) or customized IP addresses (‘custom’) for IP detection
8. **Save & Apply** the settings
9. Go back to the automatic routing page

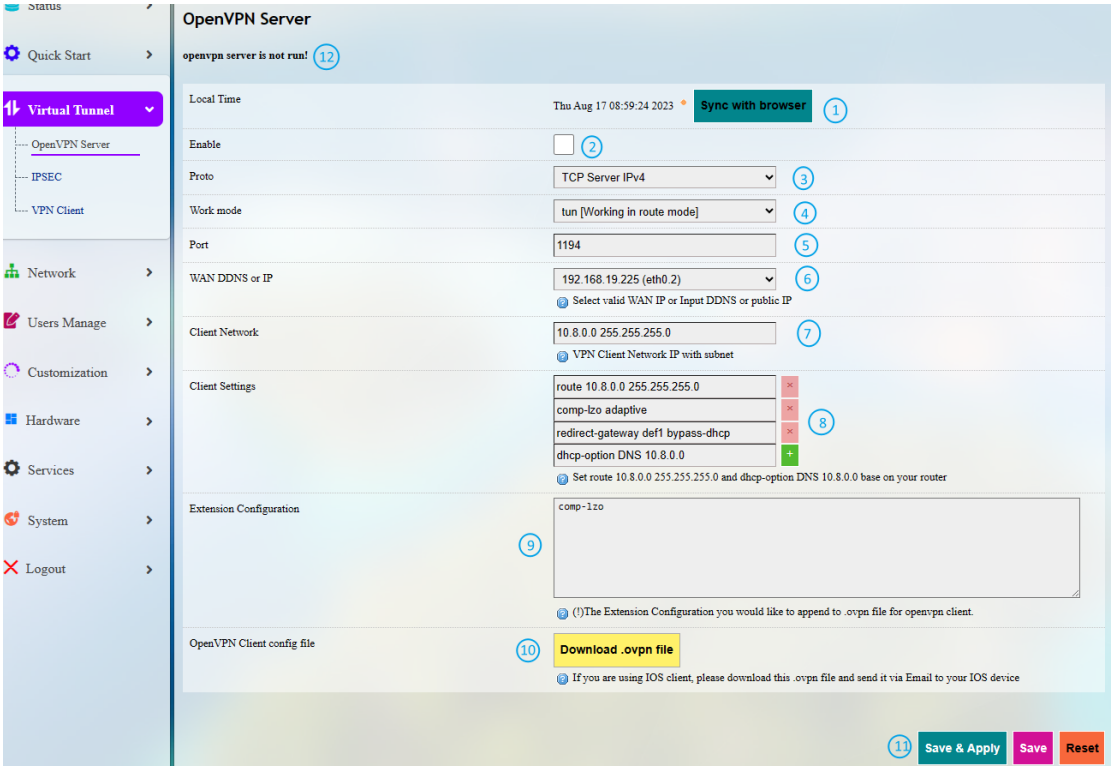
3.4 Virtual Tunnel

A virtual private network (VPN) lets you use the Internet to securely access your network remotely. The Router supports such VPN protocols as PPTP, L2TP, GRE, Ipsec, and OpenVPN to ensure data confidentiality and undisturbedness.

You can configure the Router either as an OpenVPN server or an OpenVPN client based on needs.

3.4.1 OpenVPN Server

Basic and advanced settings for OpenVPN server are accessible on this page.



Follow the steps below to build an OpenVPN Server:

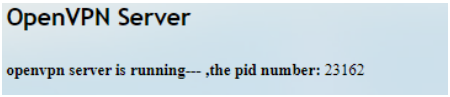
1. Synchronize the Router time with the browser (local) time;
2. Enable the server;
3. Select a protocol;

TCP provides an ordered delivery of data from user to server (and vice versa), whereas UDP is not dedicated to end-to-end communications, nor does it check the readiness of the receiver.

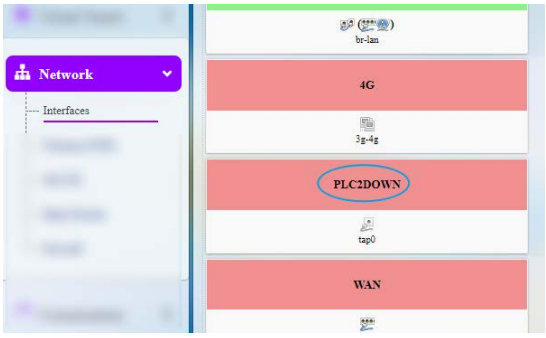
4. Select a working mode between **tap** and **tun**;

*Tap bridges two ethernet segments at different locations, so use **tap** if you need to connect to remote network (remote desktops, PLCs, controllers, etc.). If you only need network connection, then use **tun**.*

5. Set a port that the server is to monitor;
6. Choose the WAN port IP or DDNS or public IP that the server is to monitor;
7. Assign a virtual IP network for the clients;
8. The basic configurations sent to the clients (not applicable to the tap working mode);
9. The extension configurations sent to the clients;
10. Download the configuration file for client connection (not necessary for server setup);
11. **Save & Apply** the settings;
12. Status of the OpenVPN server after the setup.



Once the OpenVPN server is set up, an interface named PLC2DOWN will be added automatically so that users could make further changes.



Advanced Setting allows you to set the authentication method, certificate authentication options, and renew the system certificate.

Run Log displays the details after the server setup.

3.4.2 VPN Client

To connect the Router to a VPN server and use it as a client, navigate to **Virtual Tunnel > VPN Client** for specific settings.

Description of the numbered areas

1. Synchronize your VPN time with the browser (local) time
2. Select a WAN protocol for the virtual line (OPENVPN & PPTP available)
3. Click to switch to the protocol
4. Check or uncheck the box to enable/disable the protocol

Only when the protocol is enabled will subsequent options be displayed. The subsequent options correspond to the type of WAN protocol selected.

5. If you select OpenVPN as the WAN protocol, you'll have to continue with the configuration using a .ovpn file

If you select PPTP as the WAN protocol, you shall input the PPTP server IP, user name and password as indicated.

6. Select the local .ovpn file for configuration
7. Upload the local profile
8. Select to use a certification or username & password for the authentication

The mode will update automatically, leave it as is.

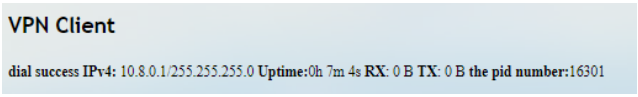
9. Set the MTU
10. Set the gateway metric (between 1 and 255)

The smaller the number, the higher the priority.

11. Disable/Enable heartbeat detection

*Select **custom** and enter the IP address for heartbeat detection to enable the mechanism.*

12. Enter a custom DNS Server
13. **Save & Apply** the settings
14. Status of the VPN client after the setup



3.5 IPSec Connection

3.5.1 Prerequisites

- An R102 industrial router ('G1' for short)
- A supporting device (gateway/router) that runs on VantronOS and supports IPSec ('G2' for short)
- Certificates for the router and the supporting device:

1. Assume that the IP addresses of the G1 and G2 are as follows:

   G1— LAN IP: 172.18.2.1, WAN IP: 192.168.9.78

   G2— LAN IP: 172.18.3.1, WAN IP: 192.168.9.82

2. Assume the certificates of the two devices are as follows:

   G1—

   X509 root certificate: rootca.cert

   X509 certificate: 78.cert

   Private key: 78.priv.key

   Public key: 78.pub.key

   G2—

   X509 root certificate: rootca.cert

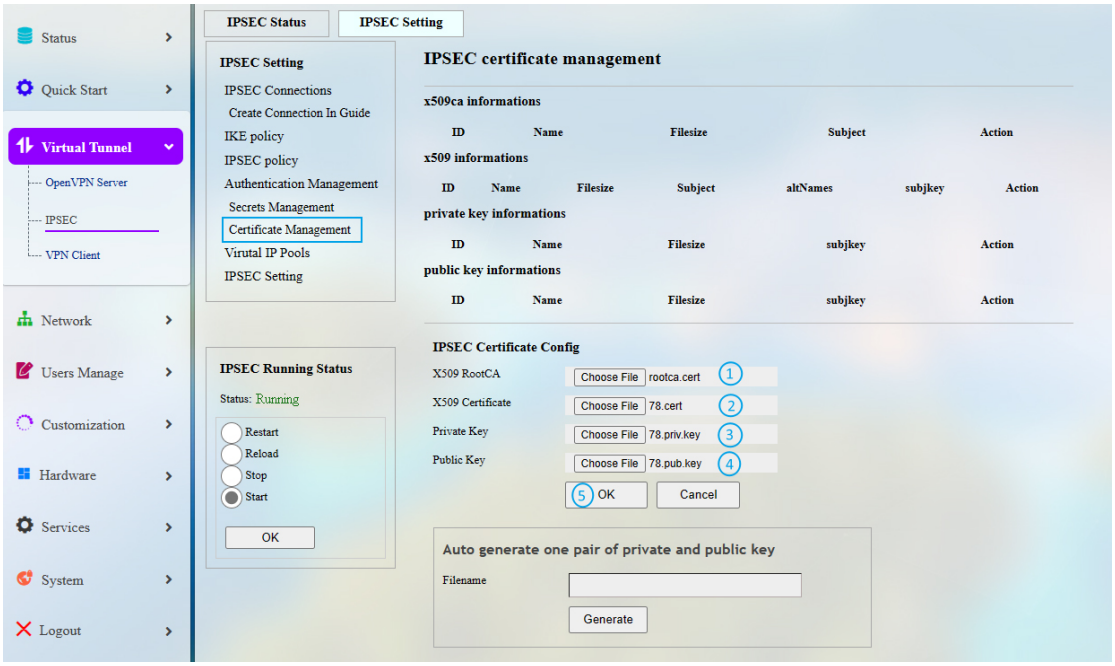
   X509 certificate: 82.cert

   Private key: 82.priv.key

   Public key: 82.pub.key

3.5.2 Certificate Setup

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Certificate Management** to upload the certificates (take G1 as an example):

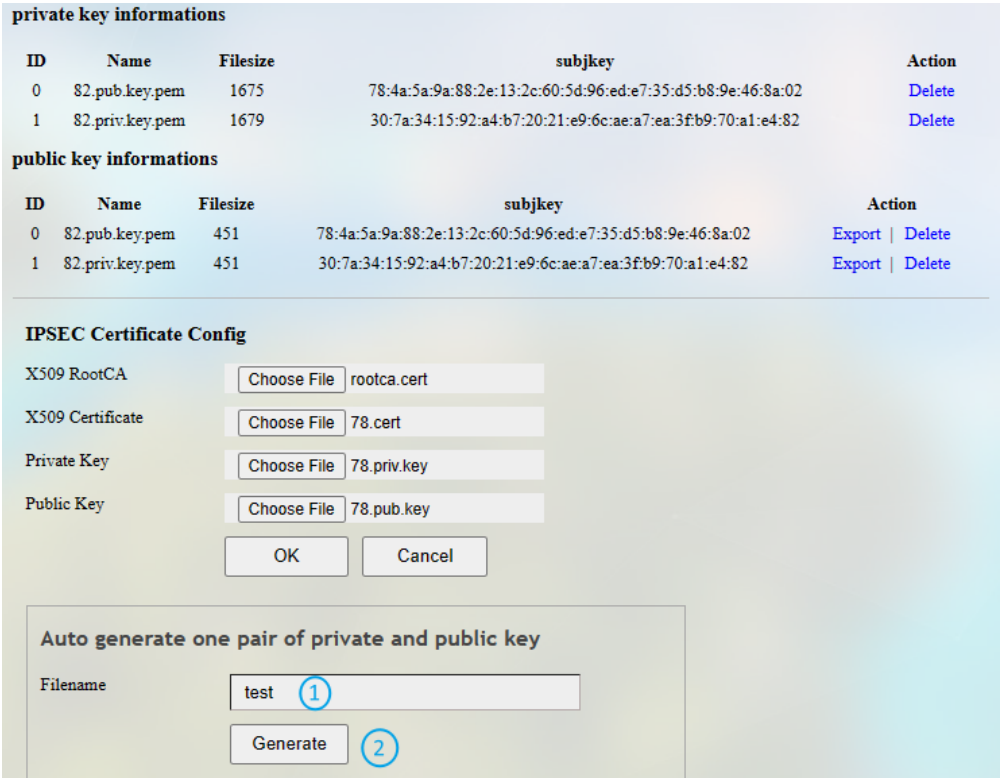


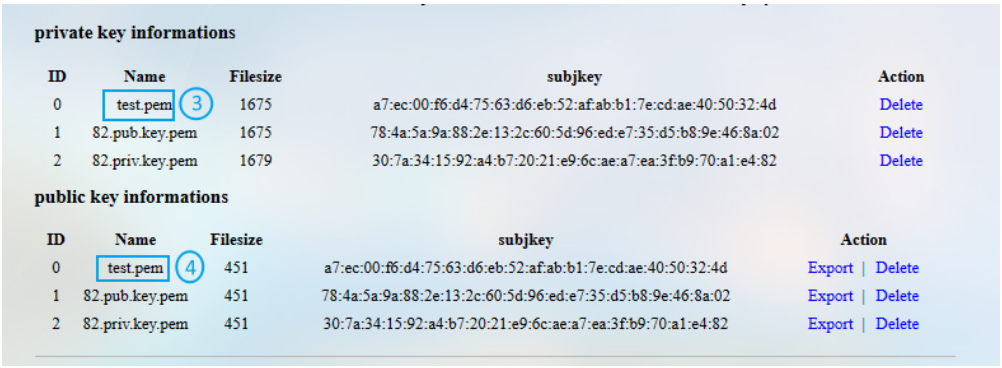
Follow the steps below to upload the certificates.

1. Select the X509 root certificate;
2. Select the X509 certificate;
3. Select the private key;
4. Select the public key;
5. Click **OK** to upload the certificates for G1.

The above screenshot only illustrates how to upload the certificates for G1. Please follow the same way to upload the certificates for G2.

You can use the tool located at the bottom of the page to generate a pair of private and public keys, which, however, can only be used as public key authentication.





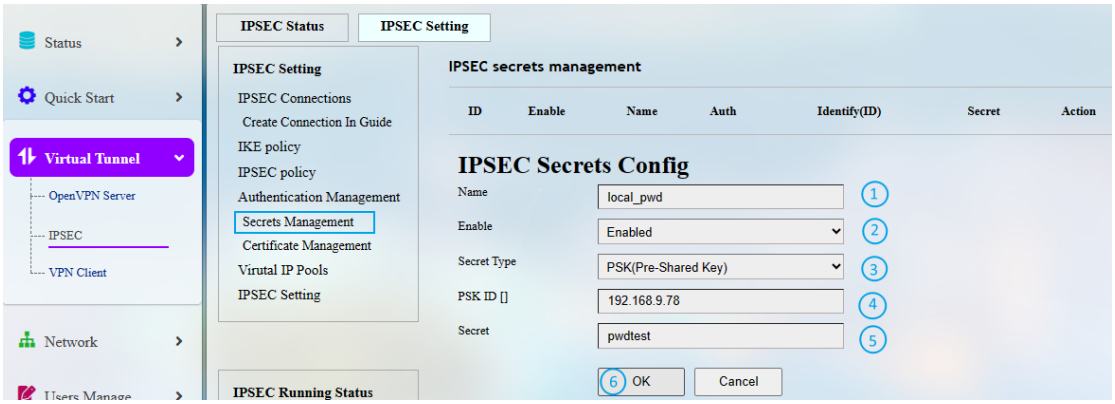
Description of the numbered areas

1. Input a file name for the keys
2. Click **Generate** to generate the keys
3. Newly generated private key
4. Newly generated public key

3.5.3 Secret Setup

This configuration only applies when pre-shared key (PSK) is selected as the secret type.

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Secretes Management** to configure a local secret (take G1 as an example):



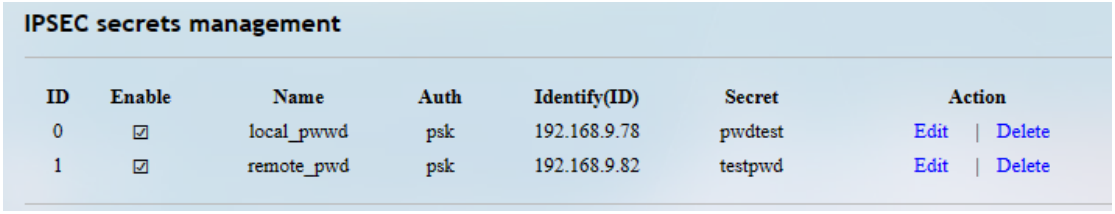
Follow the steps below to set a local secret**.**

1. Assign a name for the secrete;
2. Select **Enabled** from the dropdown list to enable the secret;
3. Select **PSK** as the secret type;
4. Input the PSK ID: 192.168.9.78 (WAN IP of G1);
5. Input a password;
6. Click **OK** to save the secret.

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Secretes Management** to configure a remote secret (take G1 as an example):

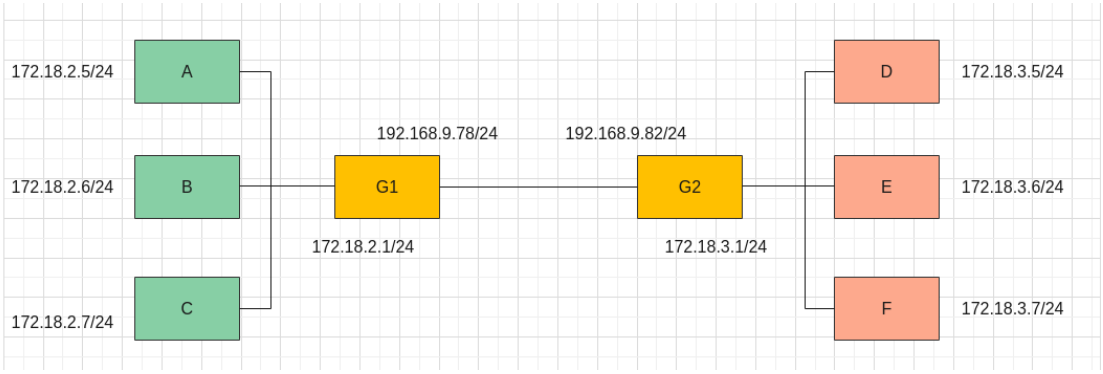
Follow the steps below to set a remote secret**.**

1. Assign a name for the secrete;
2. Select **Enabled** from the dropdown list to enable the secret;
3. Select **PSK** as the secret type;
4. Input the PSK ID: 192.168.9.82 (WAN IP of G2);
5. Input a password;
6. Click **OK** to save the secret.



The local secret of G1 acts as the remote secret of G2, and the remote secret of G1 acts as the local secret of G2.

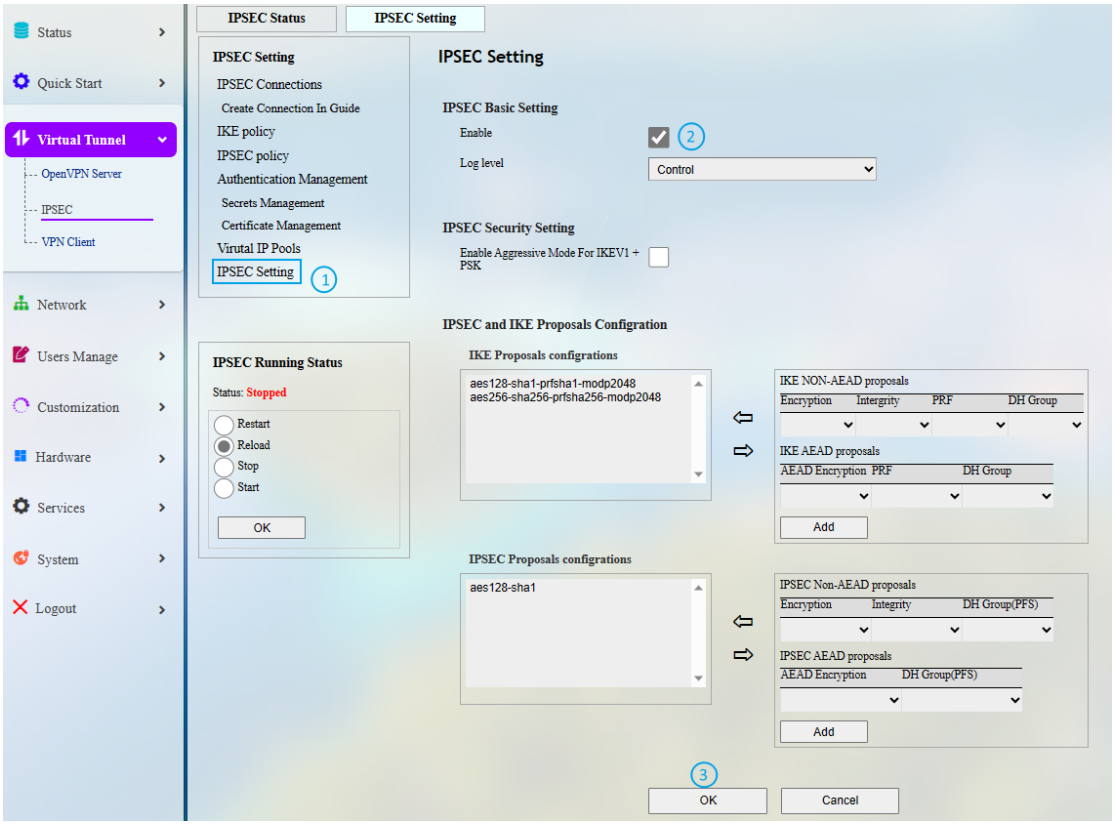
3.5.4 IPSec Connection Setup



Introduction to the above scenarios

- Scenario 1: Host-to-Host, G1 connects with G2 via IPSec, and subnets are not connected
- Scenario 2: Site-to-Site, G1 connects with G2 via IPSec, and subnets are connected
- Scenario 3: Remote access (Server), D connects to G1 via IPSec with access to subnets of G1
- Scenario 4: Remote access (Client), A connects to G2 via IPSec with access to subnets of G2

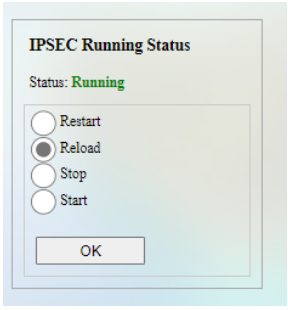
STEP 1: Enabling IPSec



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Setting**
2. Enable IPSec settings
3. Click **OK** to save the setting

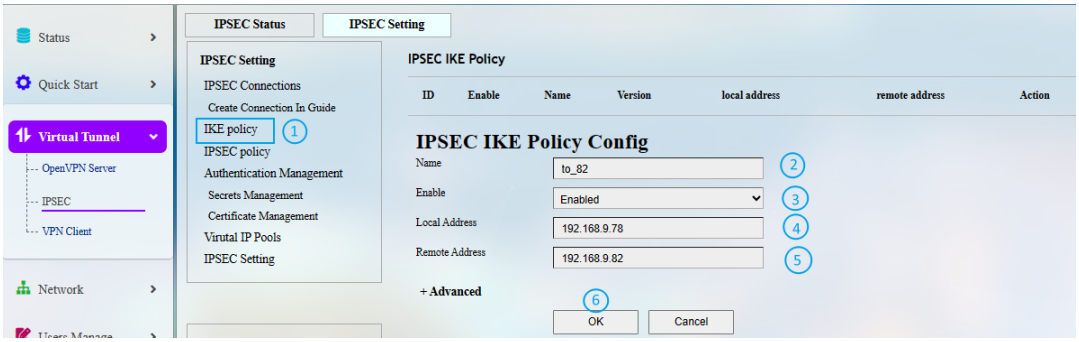
After the settings are loaded, the status of IPSec will change to ‘running’ as follows.



STEP 2: IKE policy configuration

Configurations for scenarios 1 and 2:

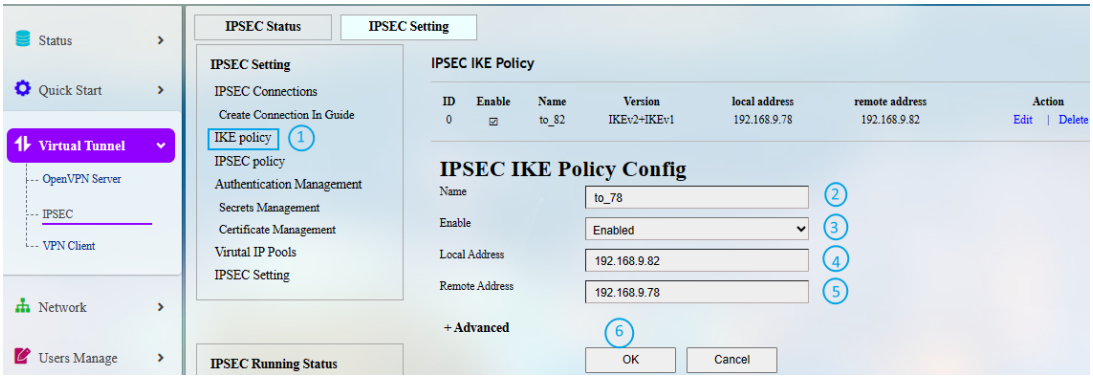
G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.78
5. Input the remote address: 192.168.9.82
6. Click **OK** to save the settings

G2 setup

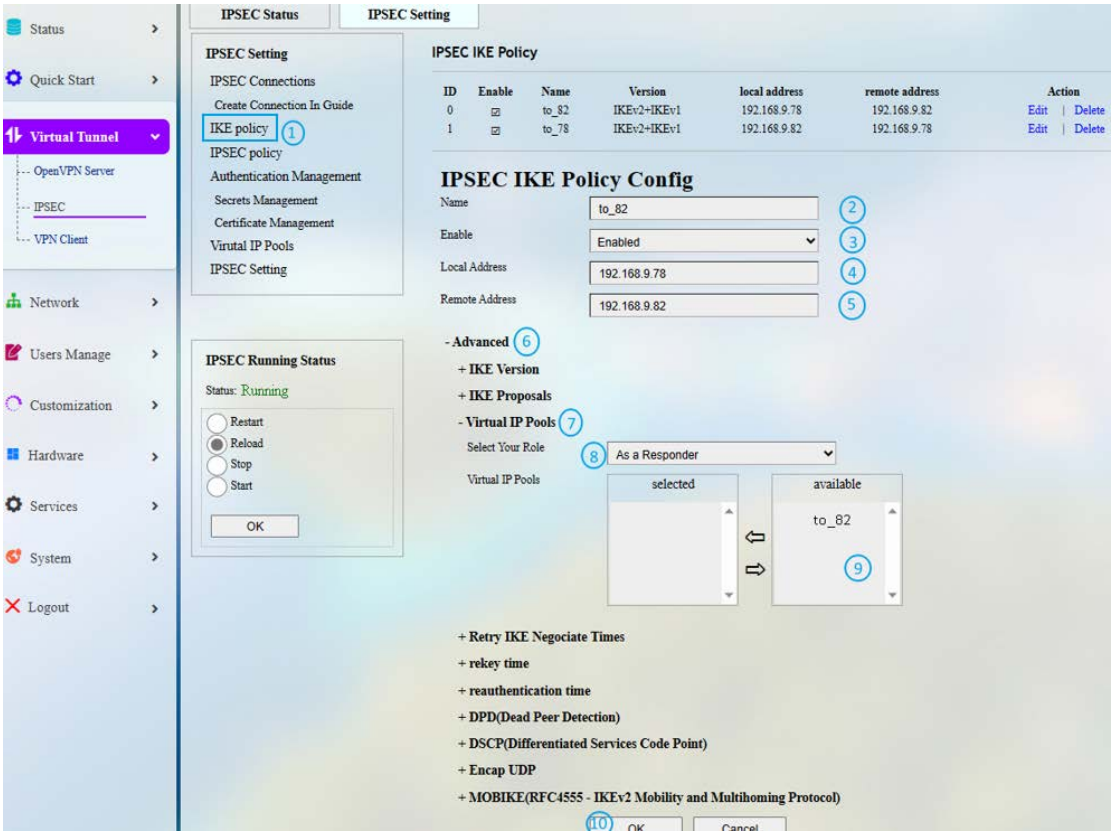


Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.82
5. Input the remote address: 192.168.9.78
6. Click **OK** to save the settings

Configurations for scenario 3 (swapping the configurations of G1 and G2 will get you the configurations for scenario 4):

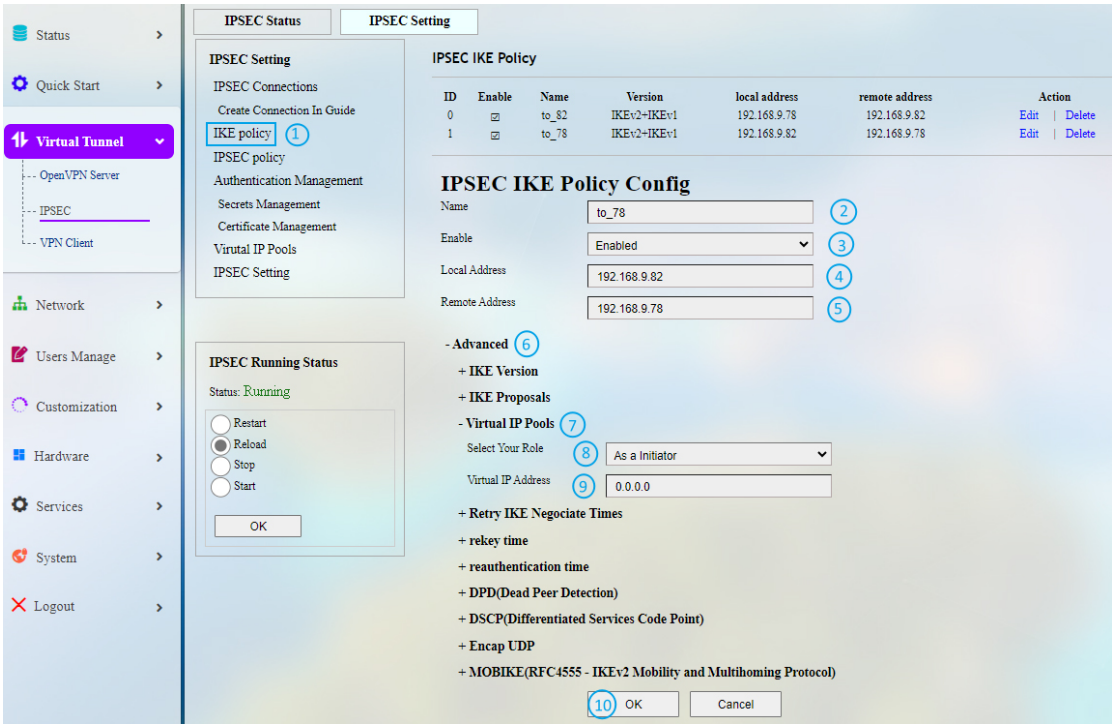
G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.78
5. Input the remote address: 192.168.9.82
6. Click **Advanced** to access the advanced settings
7. Click **Virtual IP Pools**
8. Select 'Responder' as the role of G1
9. Double click the available 'to_82' IP to select it
10. Click **OK** to save the settings

G2 setup



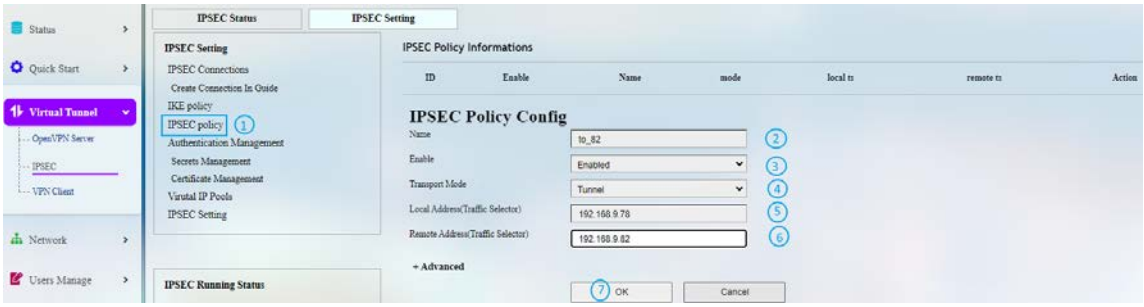
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy (to_78)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.82
5. Input the remote address: 192.168.9.78
6. Click **Advanced** to access the advanced settings
7. Click **Virtual IP Pools**
8. Select 'Initiator' as the role of G2
9. Input a virtual IP (0.0.0.0)
10. Click **OK** to save the settings

STEP 3: IPSec policy configuration

Configurations for scenario 1:

G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 192.168.9.78
6. Input the remote address: 192.168.9.82
7. Click **OK** to save the settings

G2 setup

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_78)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 192.168.9.82
6. Input the remote address: 192.168.9.78
7. Click **OK** to save the settings

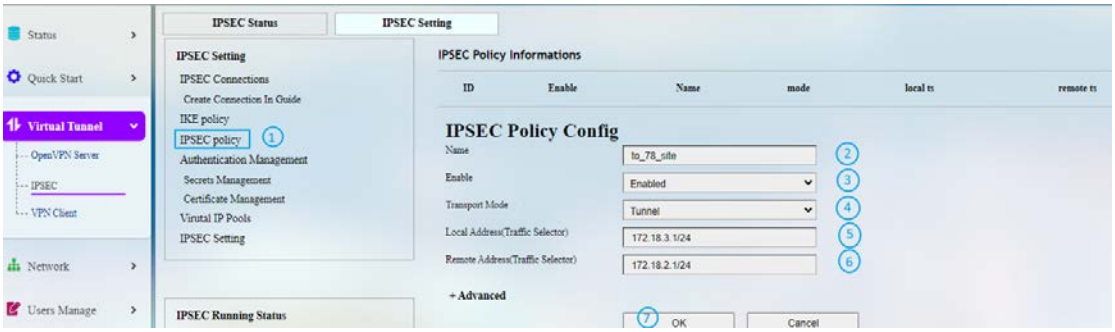
Configurations for scenario 2:

G1 setup

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82_site)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 172.18.2.1/24 (LAN IP of G1)
6. Input the remote address: 172.18.3.1/24 (LAN IP of G2)
7. Click **OK** to save the settings

G2 setup

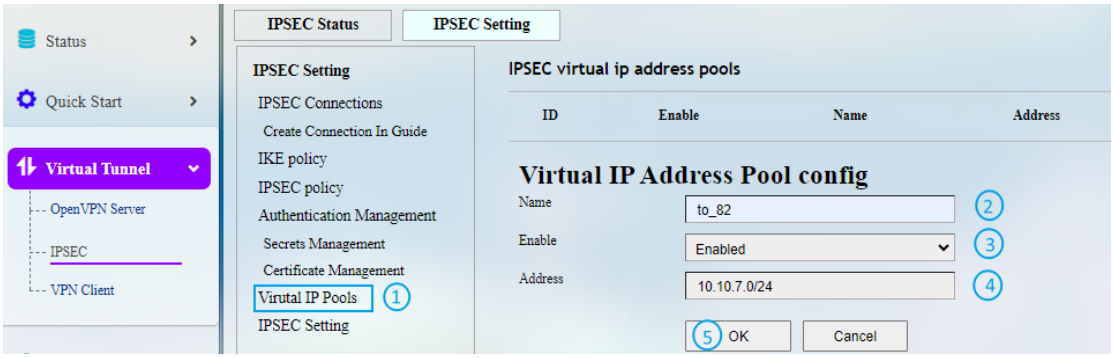


Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_78_site)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 172.18.3.1/24 (LAN IP of G2)
6. Input the remote address: 172.18.2.1/24 (LAN IP of G1)
7. Click **OK** to save the settings

Configurations for scenario 3 (swapping the configurations of G1 and G2 will get you the configurations for scenario 4):

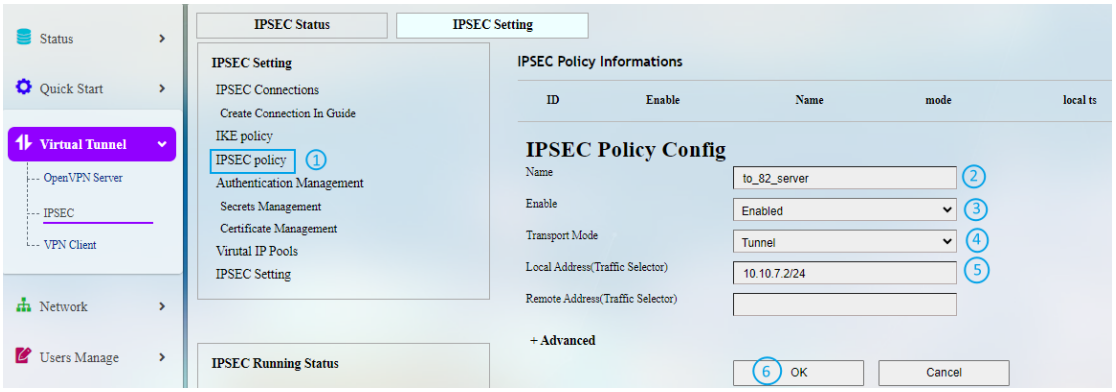
Virtual IP setup of G1



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Virtual IP Pools**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input a virtual address: 10.10.7.0/24
5. Click **OK** to save the settings

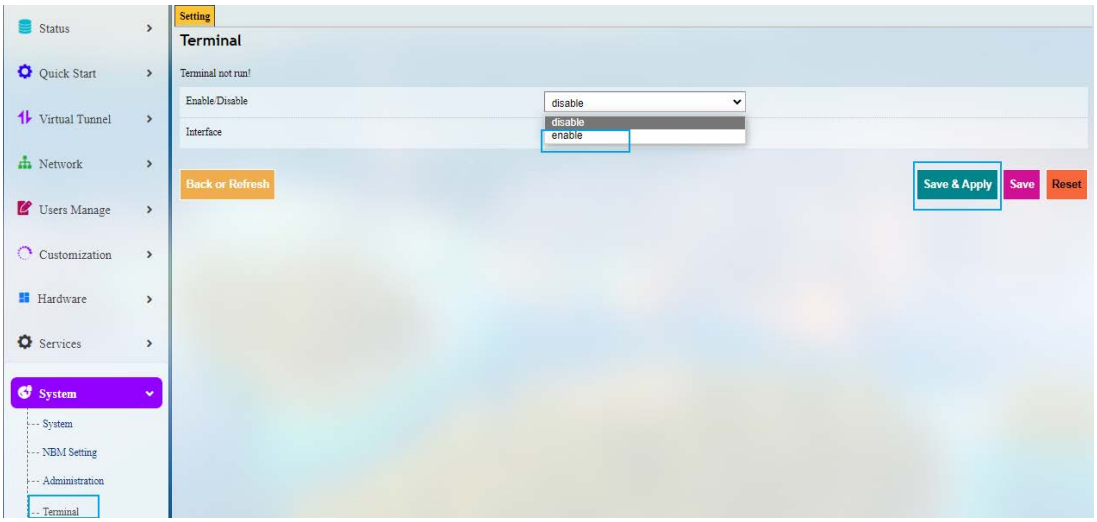
IPSec policy of G1



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82_server)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 10.10.7.0/24
6. Click **OK** to save the settings

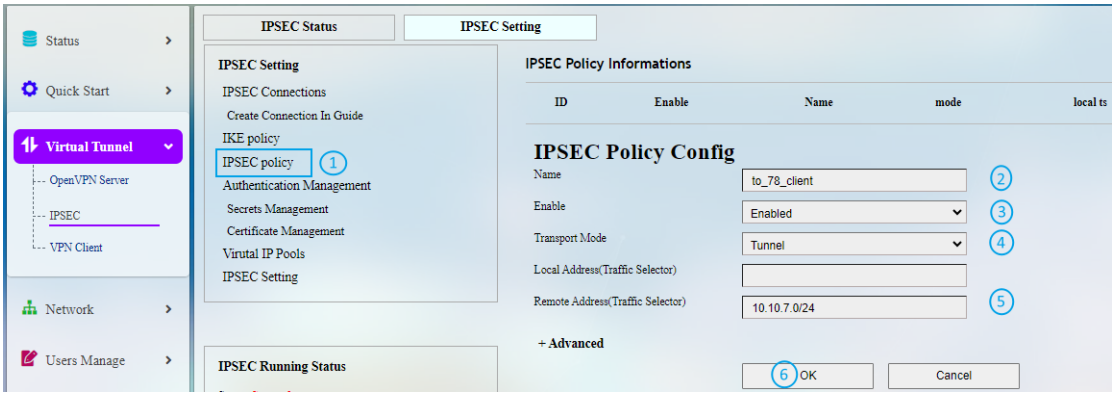
Navigate to **System > Terminal > Settings** to enable the terminal.



Log in with root account (default password: rootpassword), and input the following command to add the IP to G1.

```
ip address add 10.10.7.2/24 dev eth0
```

IPSec policy of G2



Description of the numbered areas

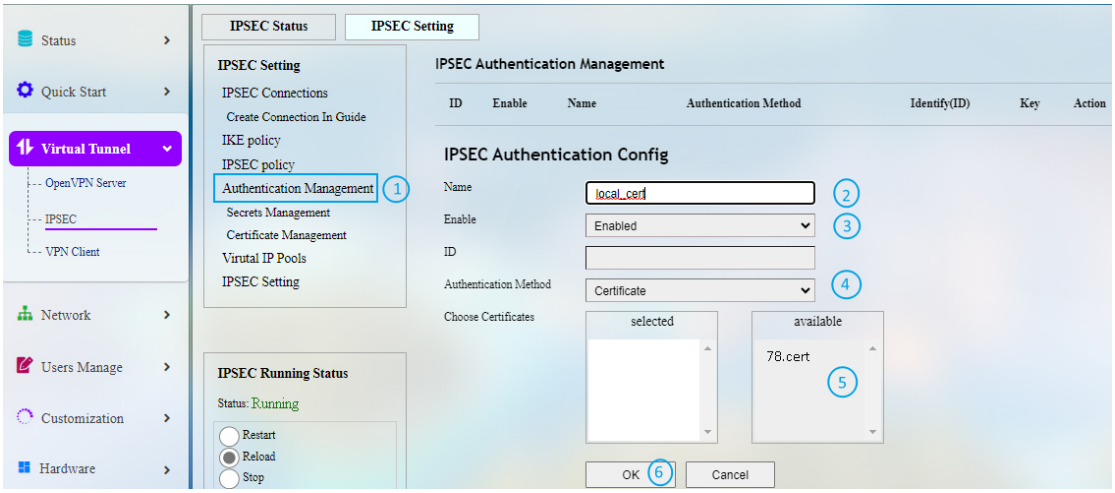
1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC policy**
2. Assign a name to the policy (to_78_client)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the remote address: 10.10.7.0/24
6. Click **OK** to save the settings

STEP 4: Authentication management

Three ways are available for the authentication: certificate, PSK, and public key.

Certificate authentication

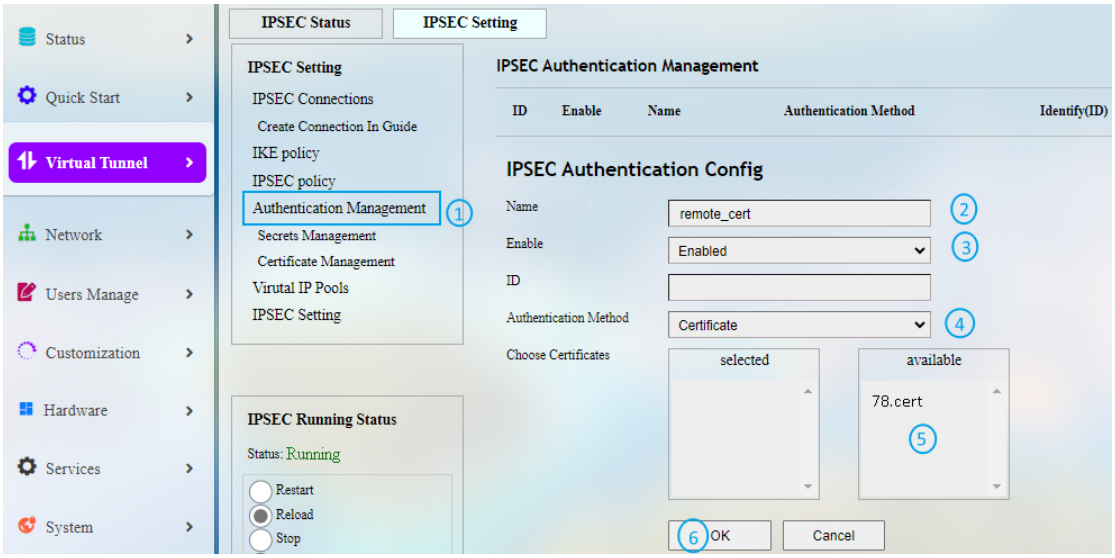
Configurations of G1 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available ’78.cert’ certificate to select it
6. Click **OK** to save the settings

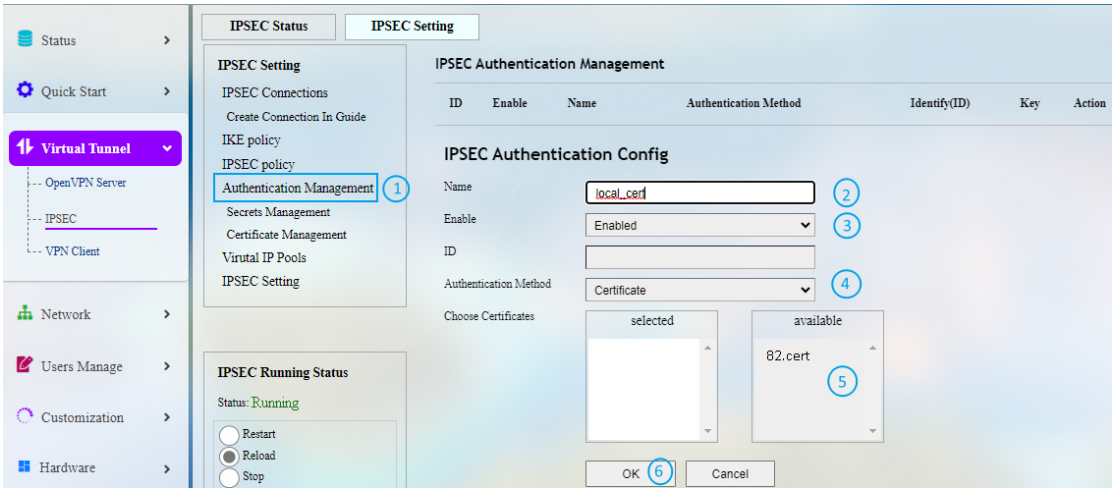
Configurations of G1 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available ’78.cert’ certificate to select it
6. Click **OK** to save the settings

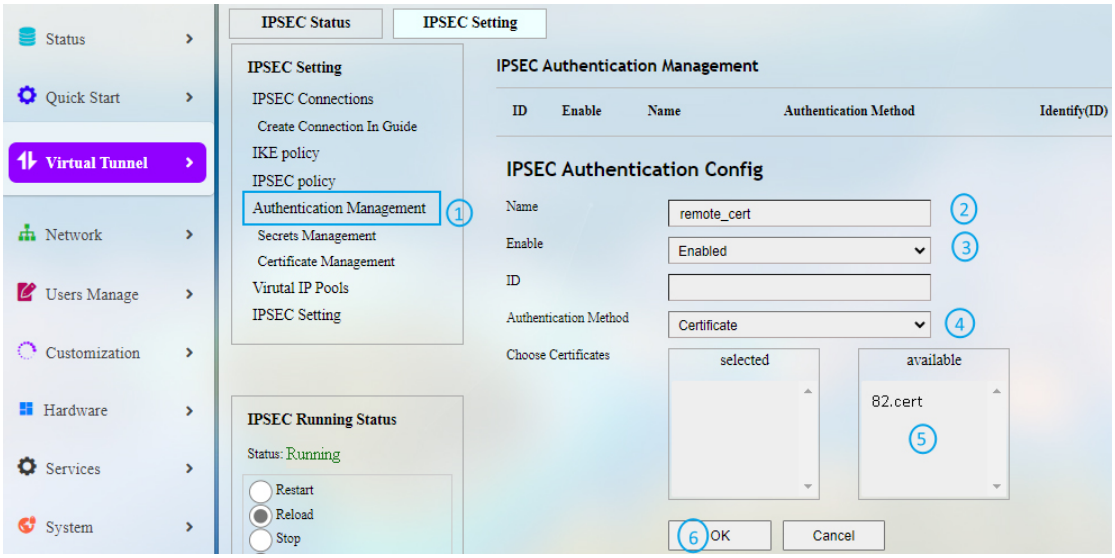
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available '82.cert' certificate to select it
6. Click **OK** to save the settings

Configurations of G2 for remote authentication

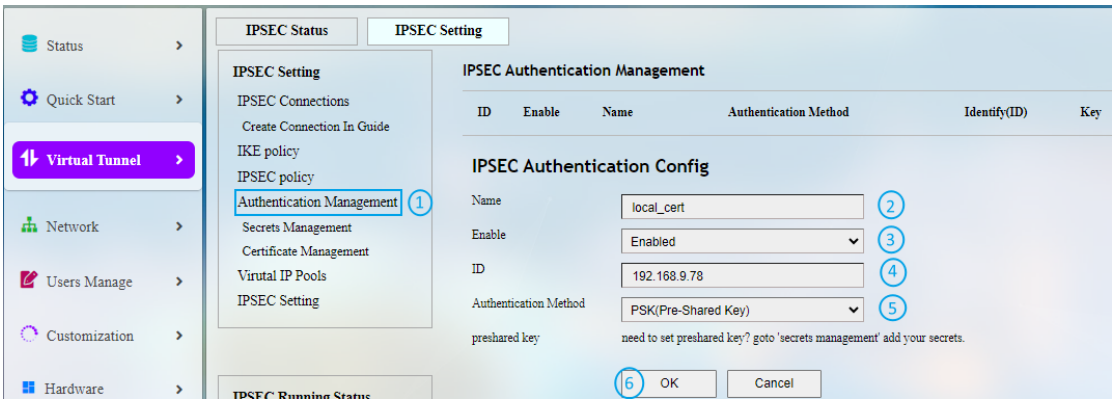


Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available ’82.cert’ certificate to select it
6. Click **OK** to save the settings

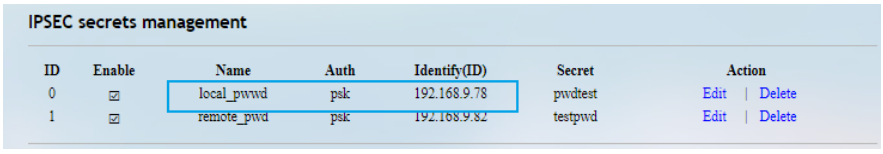
PSK authentication

Configurations of G1 for local authentication



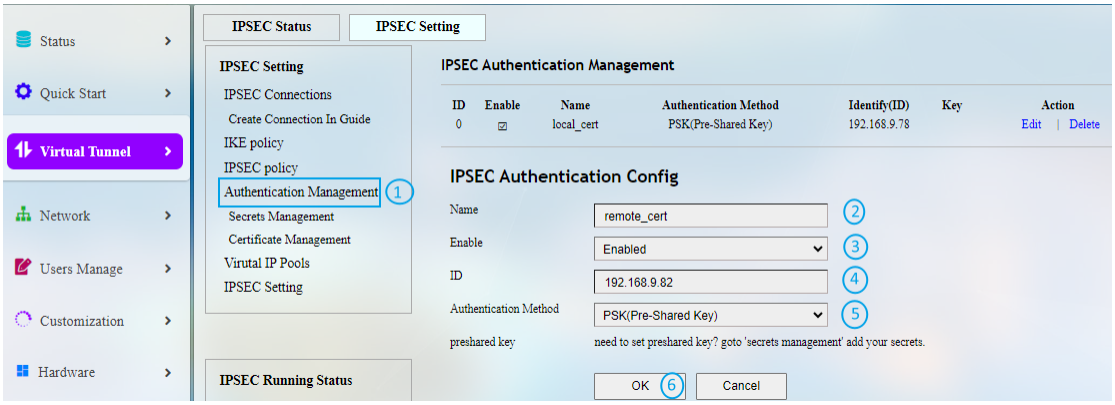
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.78)



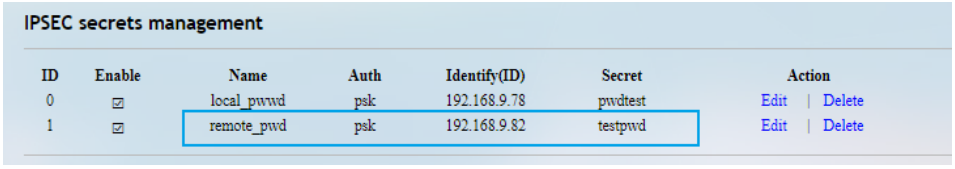
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Configurations of G1 for remote authentication



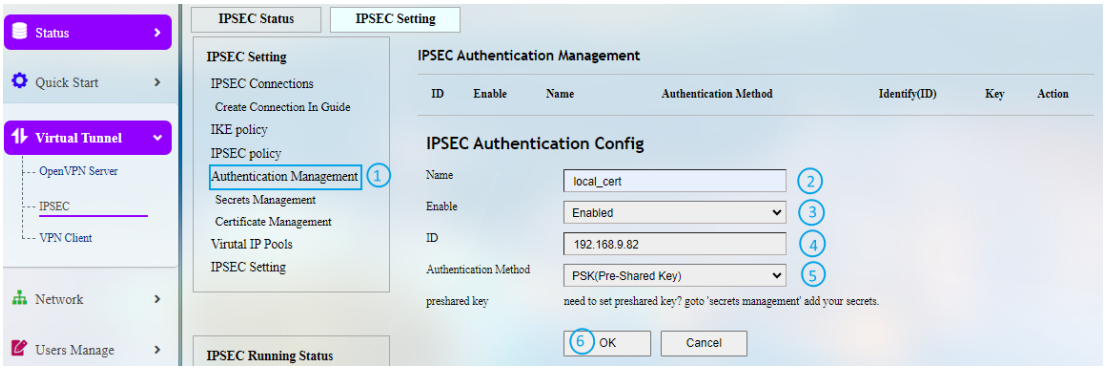
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.82)



5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

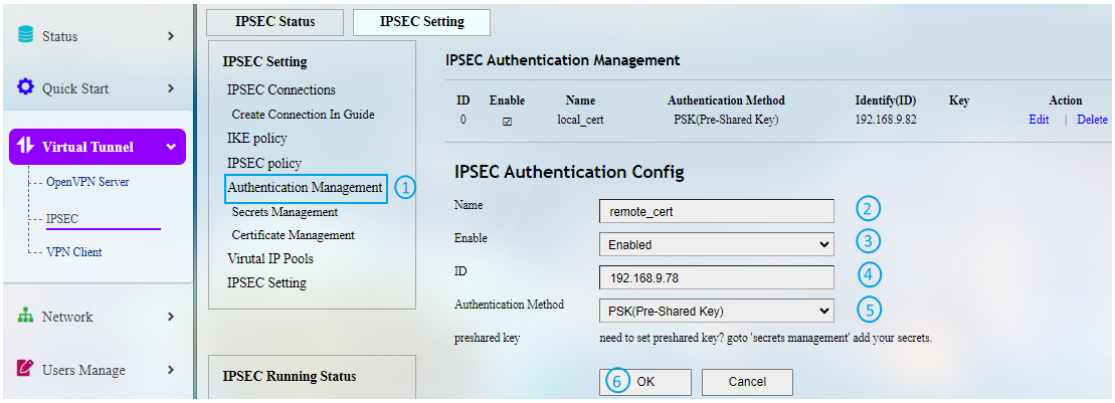
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.82)
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Configurations of G2 for remote authentication



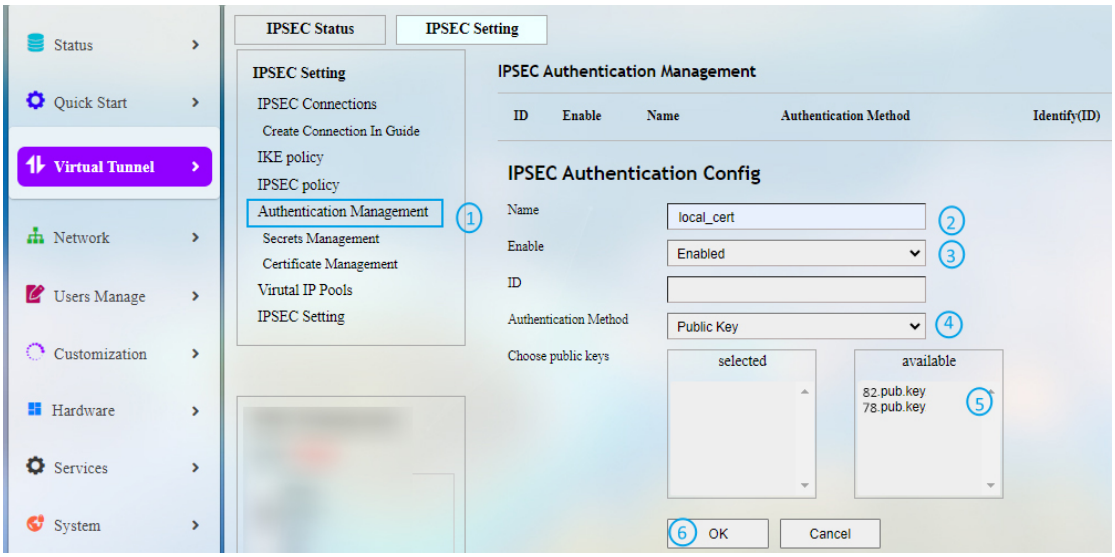
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.78)
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Public key authentication

This authentication requires to upload the public key of G1 (78.pub.key) to G2 and upload the public key of G2 (82.pub.key) to G1.

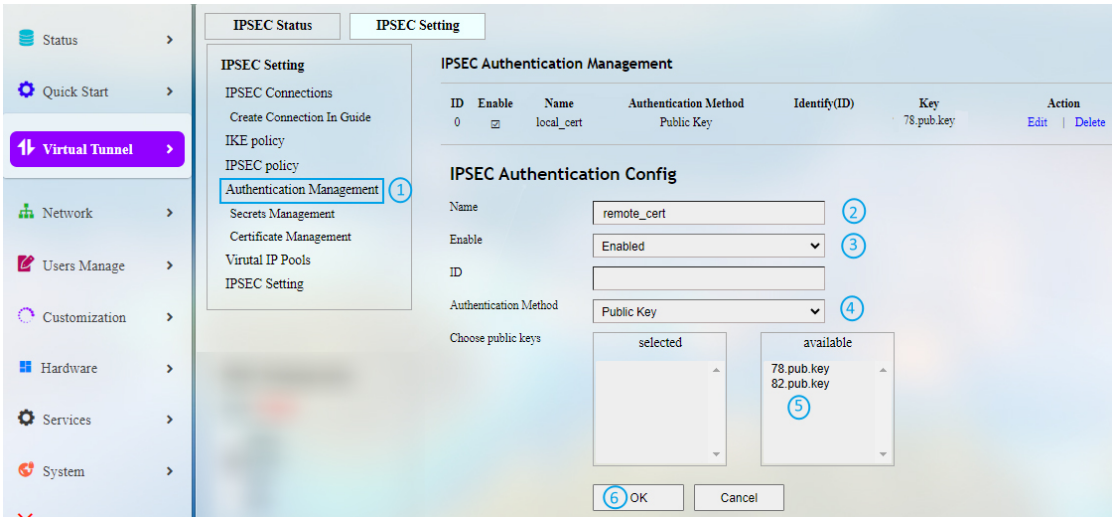
Configurations of G1 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select '78.pub.key'
6. Click **OK** to save the settings

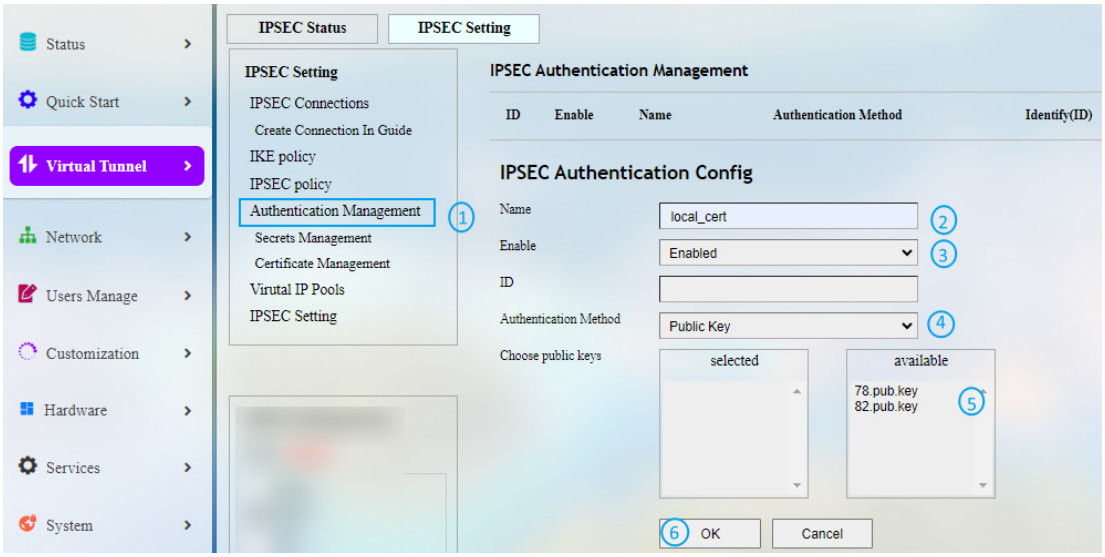
Configurations of G1 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select ’82.pub.key’
6. Click **OK** to save the settings

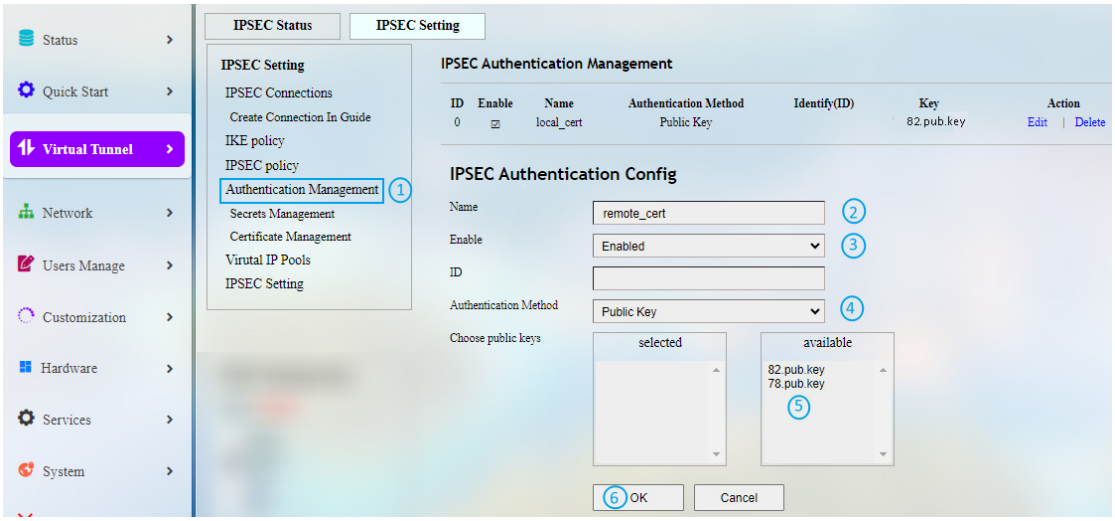
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select ’82.pub.key’
6. Click **OK** to save the settings

Configurations of G2 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select ’78.pub.key’
6. Click **OK** to save the settings

STEP 5: Configurations for IPSec connection

G1 setup

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Connection**
2. Assign a name for the connection (to_82)
3. The certificate is **Enabled** by default
4. Select a previously created IKE policy ('to_82' in this case) from the drop-down list
5. Double click a previously created local authentication policy ('local_cert' in this case) to select the policy
6. Double click a previously created remote authentication policy ('remote_cert' in this case) to select the policy
7. Double click a previously created IPSec policy ('to_82' in this case) to select the policy
8. Click **OK** to save the settings

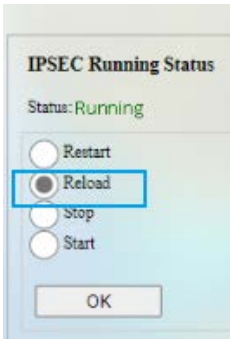
G2 setup

Description of the numbered areas

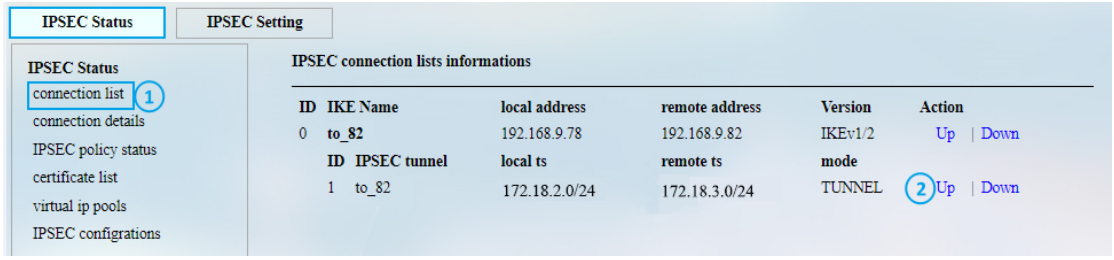
1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Connection**
2. Assign a name for the connection (to_78)
3. The certificate is **Enabled** by default
4. Select a previously created IKE policy ('to_78' in this case) from the drop-down list
5. Double click a previously created local authentication policy ('local_cert' in this case) to select the policy
6. Double click a previously created remote authentication policy ('remote_cert' in this case) to select the policy
7. Double click a previously created IPSec policy ('to_78' in this case) to select the policy
8. Click **OK** to save the settings

STEP 6: Reloading the IPSec program

Click the radio button before **Reload** and then **OK** to reload the program.



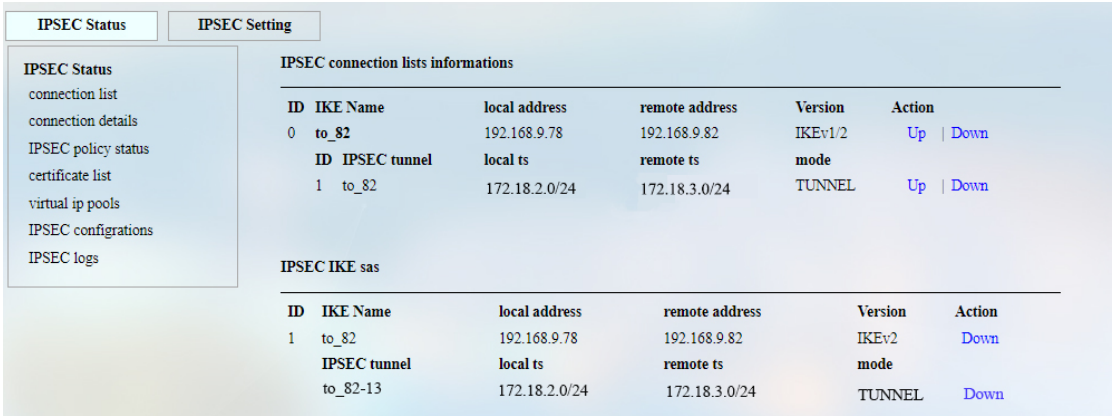
STEP 7: IPSec connection



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Status> Connection list**
2. Select the connection setting and click **Up**

When the connection is added to **IPSEC IKE SAS**, the connection is established successfully.

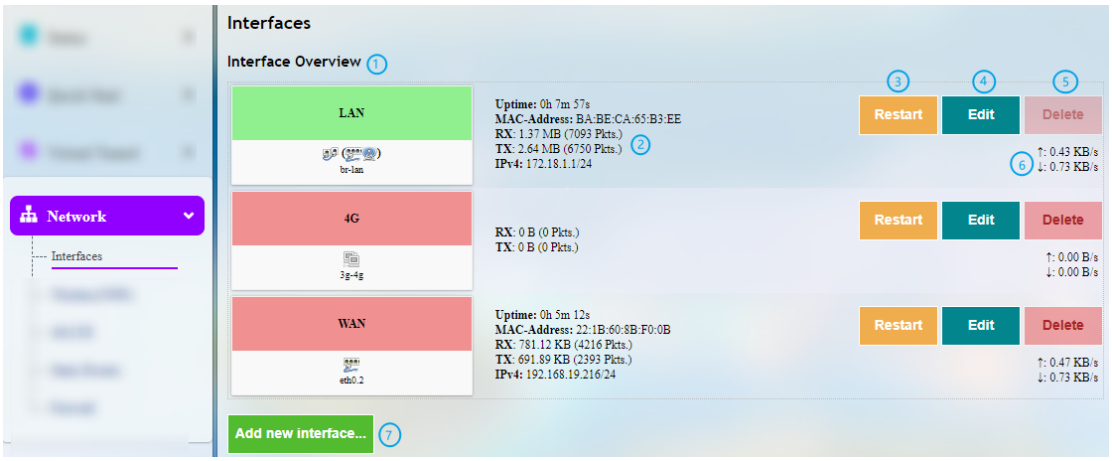


3.6 Network

Users can change the settings related to the available network interfaces in the **Network** page.

3.6.1 Interfaces

All the network interfaces currently available and configurable are displayed under **Network > Interfaces**.



Description of the numbered areas

1. Interface overview
2. Interface traffic details
3. Restart the interface manually
4. Edit the interface settings
5. Delete the interface (available only when you log in as a root user)
6. Instantaneous traffic of the interface
7. Add a new interface (available only when you log in as a root user)

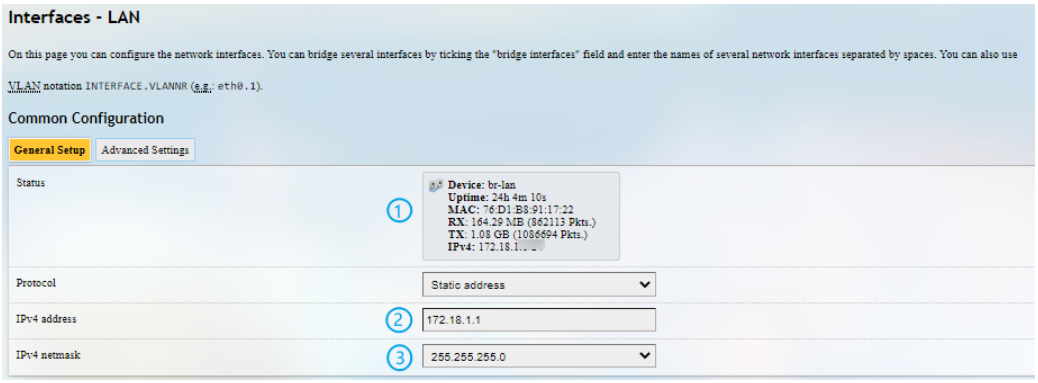
The interfaces may differ from what is shown above as certain devices do/do not have the module that makes corresponding interface available.

The following section illustrates on how to edit the LAN port and WAN port settings of the Router.

3.6.1.1 LAN

- **Common Configurations**

Clicking on the **Edit** button behind the **LAN** port will allow you to access the configurations of the LAN port, and **General Setup** is displayed by default.



Description of the numbered areas

1. Status of the interface
2. Enter the IP address of the LAN port
3. Select a LAN port subnet mask

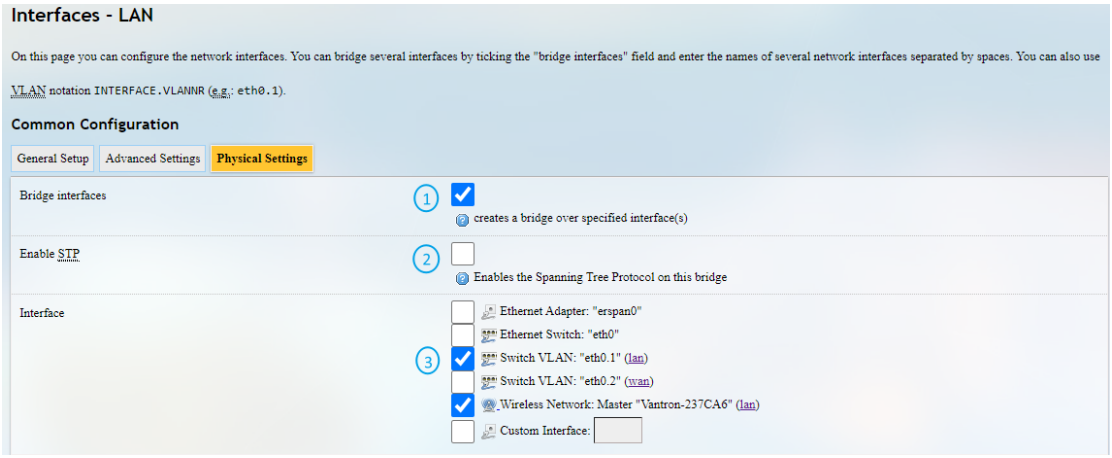
In the **Advanced Settings** next to the general setup:

Description of the numbered areas

1. MAC address cloning
2. Set the MTU (keep the default setting)
3. Set a gateway metric (keep the default setting)

Be sure to save the settings before you exit the page.

There is a **Physical Settings** tab next to **Advanced settings** when you log in with the root account, allowing you to configure the LAN port for network bridge.



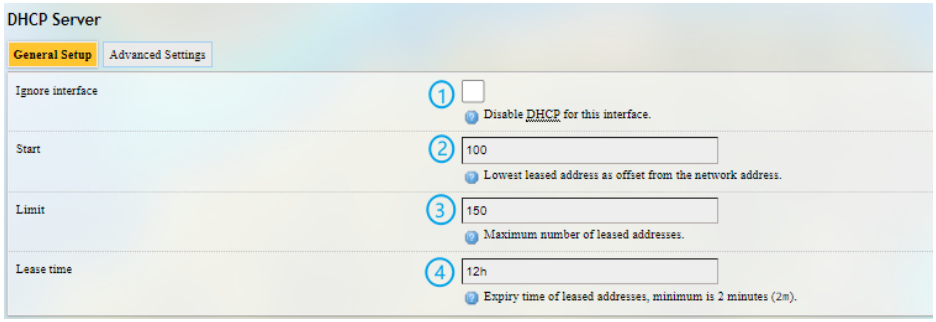
Description of the numbered areas

1. Enable the interface for network bridge
2. Enable STP protocol
3. Select the interface for bridge connection

Be sure to save the settings before you exit the page.

- **DHCP server**

In the **General Setup** page of **DHCP Server**, DHCP could be set up with more details:



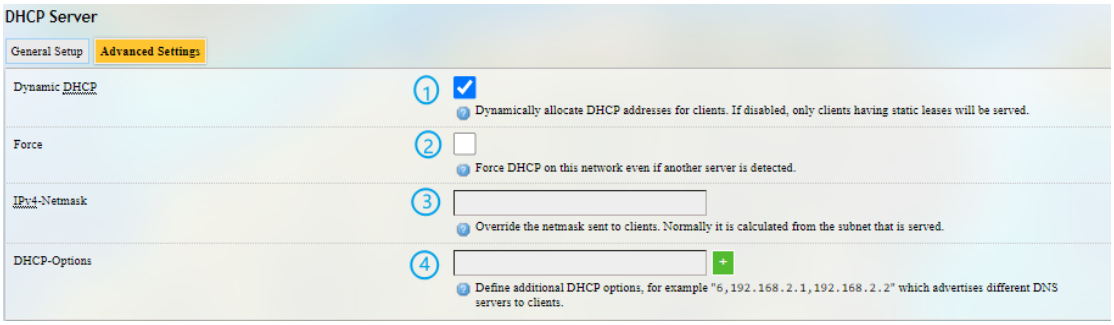
Description of the numbered areas

1. Disable the DHCP service

If disabled, the DHCP service will not be available to the client devices connected to the LAN port of the Router.

2. DHCP start address
3. Maximum number of leased addresses (up to 150)
4. Expiry time of leased addresses (min. 2m)

Advanced Settings of DHCP Server:



Description of the numbered areas

1. Enable allocation of DHCP addresses for clients
2. Force enablement of DHCP service (to bypass other servers)
3. Override the netmask sent to clients

Normally it is calculated from the subnet that is served

4. Add different DNS servers for clients

*Be sure to save the settings before you exit the page. Clicking on **Back or Refresh** will get you back to **WAN** interface settings.*

3.6.1.2 WAN

- **General DHCP settings**

Clicking on the **Edit** button behind the **WAN** port will allow you to access the configurations of the WAN port, and **General Setup** is displayed by default.

Description of the numbered areas

1. Status of the WAN port
2. Select a WAN protocol (DHCP client by default)
3. Input a hostname of the Router for requesting DHCP

Be sure to save the settings before you exit the page.

- **Advanced DHCP settings**

If you have selected DHCP client protocol, advanced settings are available after you have finished the setup as mention above.

Description of the numbered areas

1. Check the box to bring up the port upon device boot
2. Force link (once the box is checked, hotplug handlers will not be invoked after a link change)
3. Enable **Use default gateway**
4. Enable **Use DNS server advertised by peer**

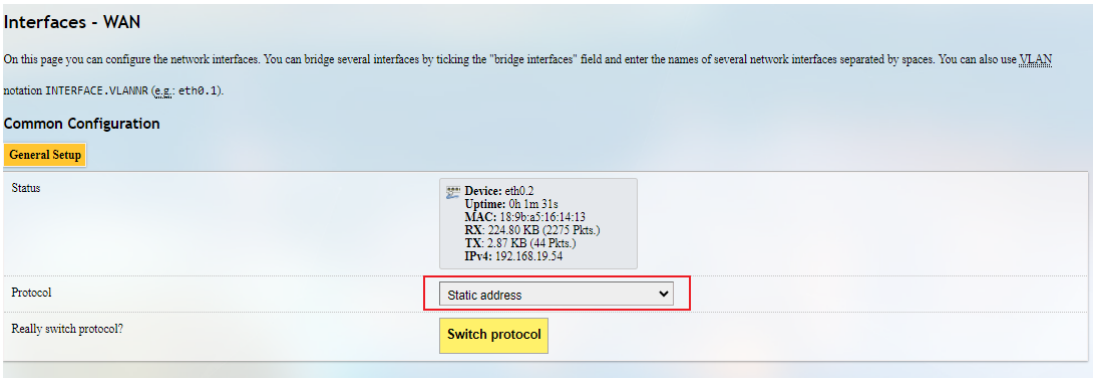
If this option is disabled, you will need to define a DNS server.

5. Set a gateway metric
6. MAC address cloning
7. Set the MTU

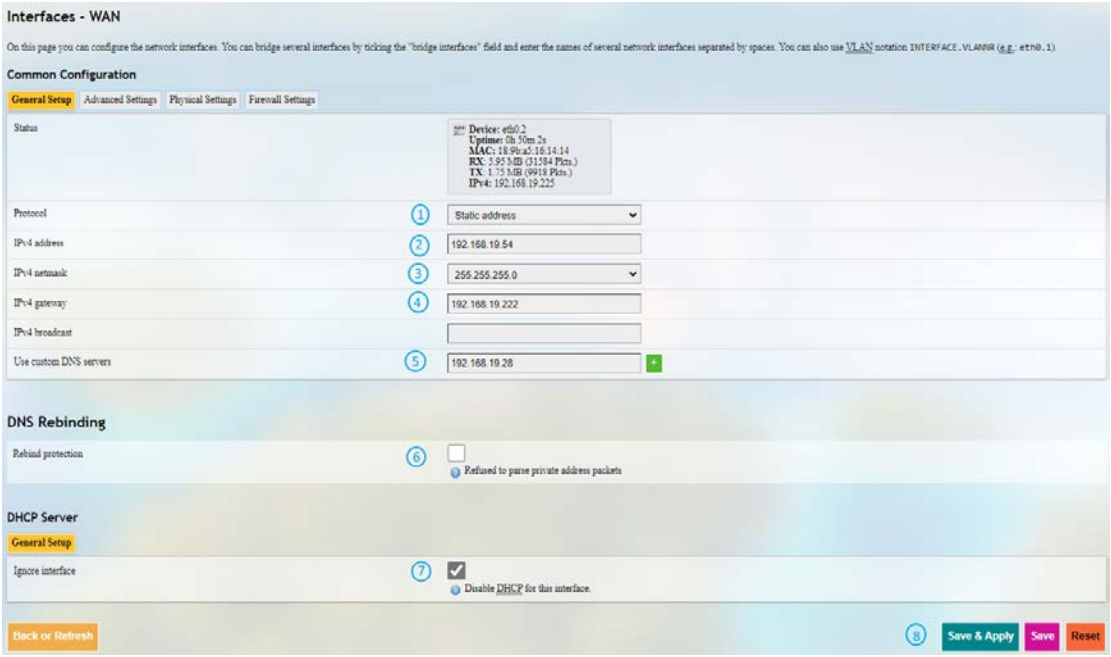
Be sure to save the settings before you exit the page.

- **General Static protocol settings**

To activate static address protocol, select **Static address** from the protocol drop-down list under **General Setup** of the WAN port and click **Switch protocol**.



Upon a click of **Switch protocol**, you'll need to input the IPv4 address, subnet mask, IPv4 gateway, and the IPv4 broadcast.



Description of the numbered areas

1. Current protocol
2. Input an IPv4 address
3. Input an IPv4 netmask
4. Input the IPv4 gateway
5. Set a custom DNS server (can be provided by the carrier or self-defined)
6. DNS re-binding protection (if enabled, parsing of private IP data will be refused)
7. Disable DHCP service (keep the default settings)

8. Save & apply the settings

Leave the field as is if not applicable.

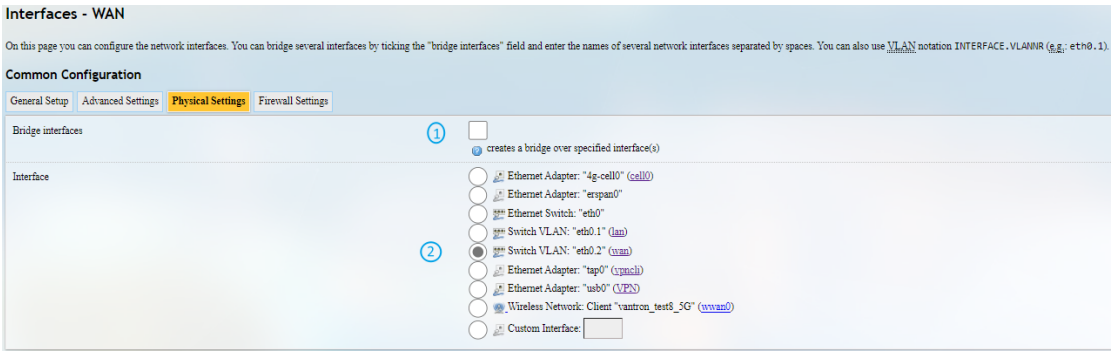
When static address protocol is selected, DHCP server will be automatically disabled.

The advanced settings are basically same as those for DHCP protocol.

Be sure to save the settings before you exit the page.

Other available WAN protocols include PPPoE, GRE tunnel over IPv4, and relay bridge. The settings are dependent on the specific protocols. Clicking on **Back or Refresh** allows you to return to interface settings.

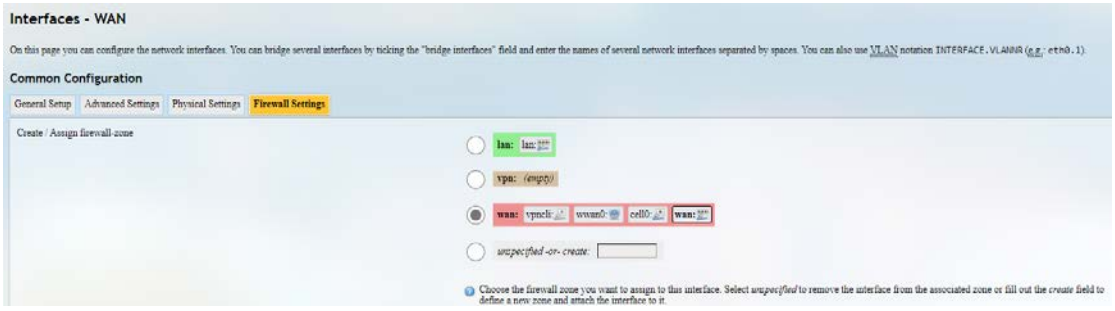
There is a **Physical Settings** tab next to **Advanced settings** when you log in with the root account, allowing you to configure the WAN port for network bridge.



Description of the numbered areas

1. Enable the interface for network bridge
2. Select the interfaces for bridge connection

There is a **Firewall Settings** tab next to the **Physical settings** tab when you log in with the root account, allowing you to create or designate a firewall zone.

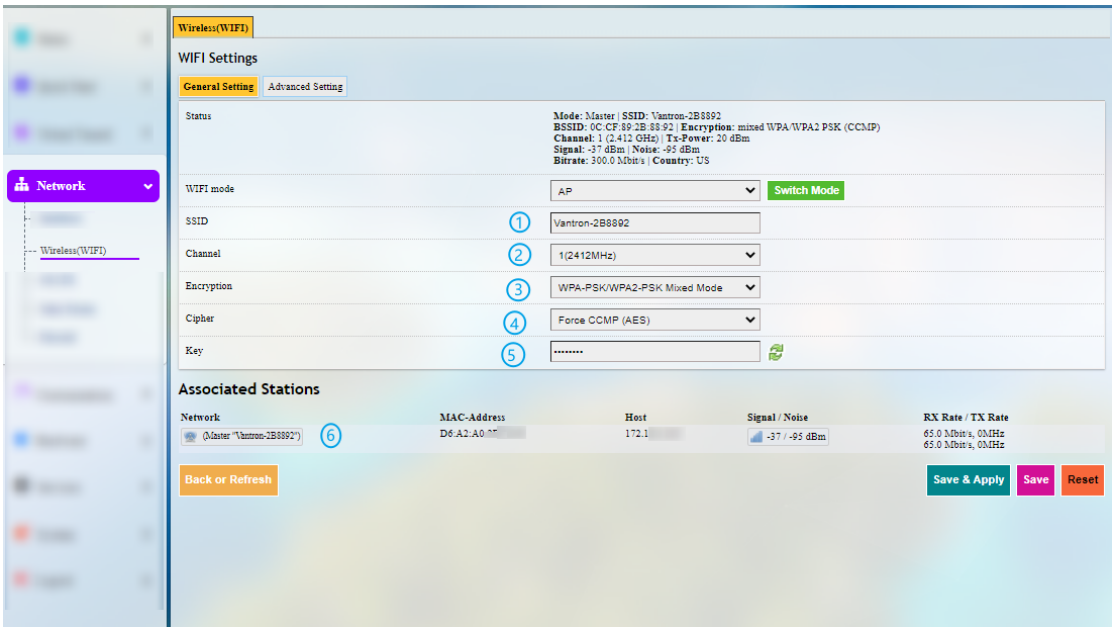


When ‘unspecify or create’ is selected, you can remove the interface from the associated firewall zone or create a new zone.

3.6.2 Wireless (WIFI)

You can switch between AP and client modes for wireless connection.

3.6.2.1 Wi-Fi – AP Mode (General settings)



Description of the numbered areas

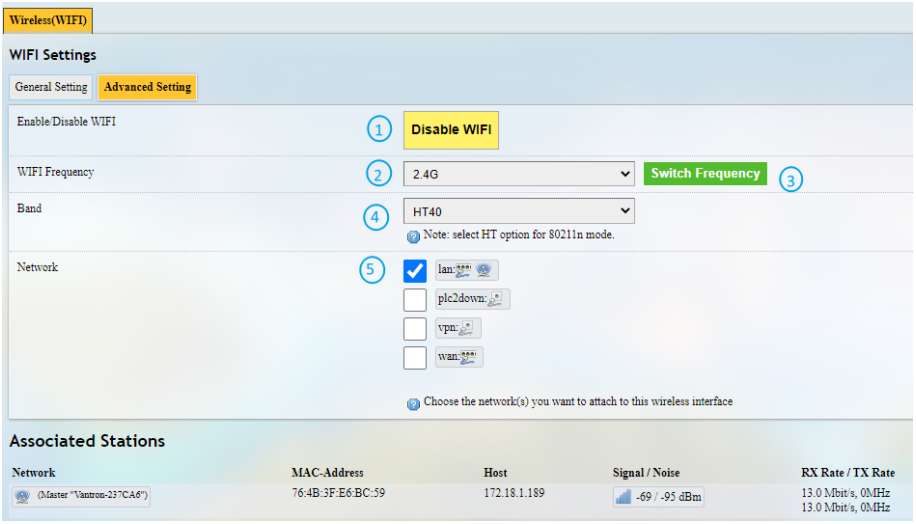
1. Set an SSID for the Router

The ID name shall not contain characters including $, `, \.

2. Select a Wi-Fi channel
3. Select an encryption method (the following options vary with the encryption method)
4. Select an encryption algorithm
5. Assign a Wi-Fi password (no less than 8 characters)
6. List of currently connected devices

Be sure to save the settings before you exit the page.

3.6.2.2 Wi-Fi – AP Mode (Advanced setting)



Description of the numbered areas

1. Turn on/off Wi-Fi
2. Set Wi-Fi frequency (determined by hardware)
3. Click to switch the frequency
4. Select the frequency band
5. The network interface to which Wi-Fi belongs

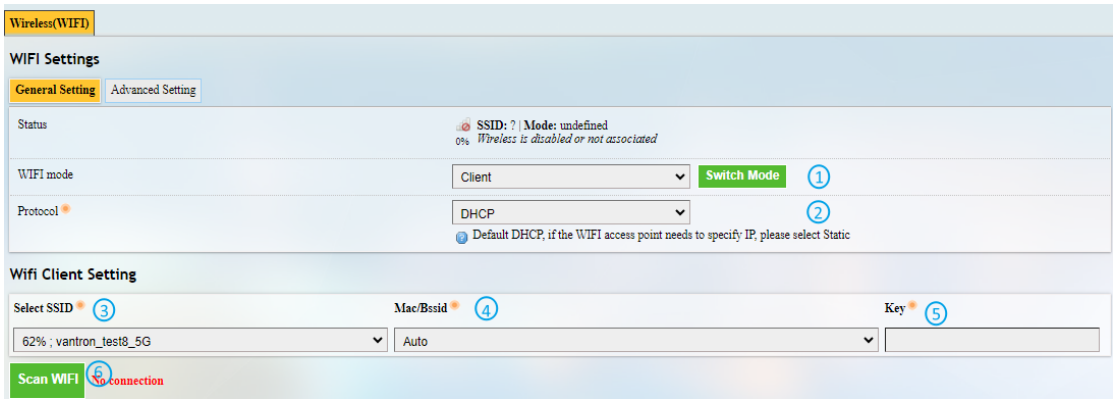
As modification of field 2 will have impact on the Wi-Fi signal, the web interface will return to the general settings page upon a click of the switch button.

Be sure to save the settings before you exit the page.

3.6.2.3 Wi-Fi – Client Mode

When the Router is set as a client on a wireless network, the page below allows you to make changes to the network settings.

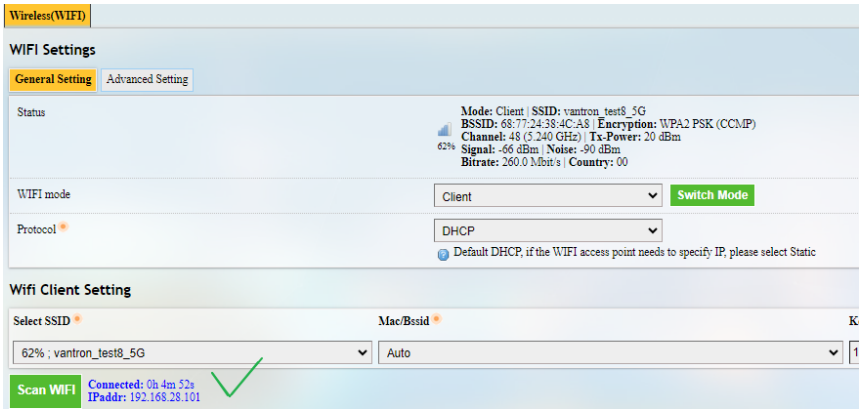
*A wwan0 port will be added (as shown in the **Interface** page) when the Wi-Fi client mode is enabled.*



Description of the numbered areas

1. Switch to **Client mode**
2. Select DHCP protocol to automatically get an IP or Static protocol to specify an IP for the Router
3. Select a wireless network for internet access
4. Select the MAC address of the access point, or leave it to Auto if not clear
5. Input the password of the access point
6. Click **Scan WIFI** to refresh the Wi-Fi list if the target SSID is not identified

When the Router is successfully connected as a client, there will be the network information next to the **Scan WIFI** button.

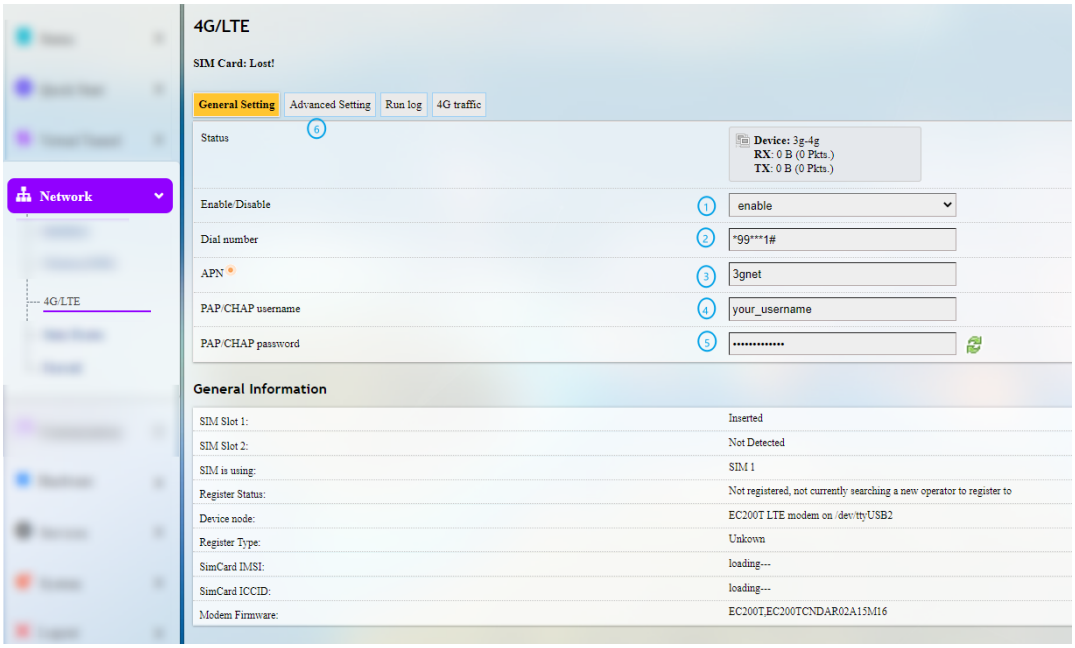


3.5.3 4G/LTE

Before you configure for 4G/LTE, be sure to install the activated SIM card and the LET antennas. After installation, the SIM card information will display on the top of the page, including signal strength, IP, and IMEI. While register status and other general information will display at the bottom of the page.

Confirm with your sales executive whether the 4G module is AT&T and Verizon pre-certified. If so, when you apply for SIM cards from the carriers,

- provide Verizon with the pre-certified module name **VT-MOB-CELL-mPCIe**.
- provide AT&T with the pre-certified module name **VT-MOB-MPCIE-4G**.



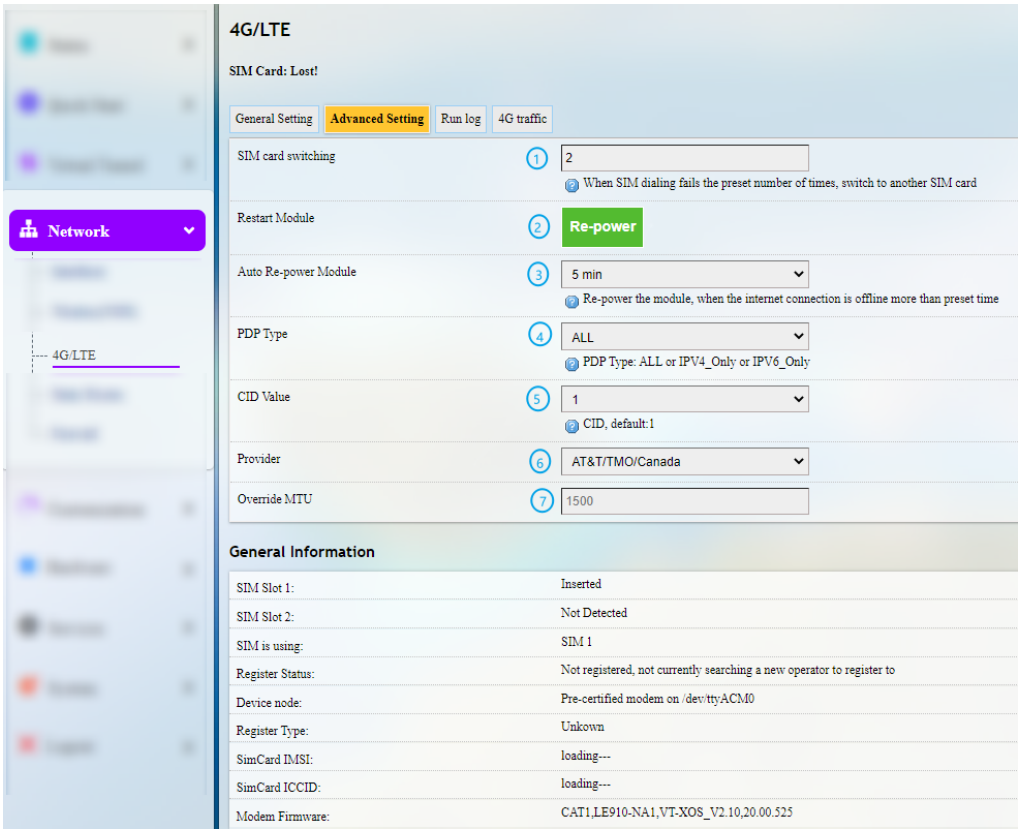
Description of the numbered areas

1. Enable/disable 4G/LTE service
2. Input ***99***1#** for AT&T SIM cards and ***99***3#** for Verizon SIM cards
3. Input the APN provided by the carrier
4. Enter the username provided by the carrier for PAP/CHAP authentication
5. Enter the password provided by the carrier for PAP/CHAP authentication
6. Click **Advanced Setting** for more configuration options

Leave the field as is if not applicable.

PAP/CHAP username and password are to be specified only if your carrier has setup APN with user name and password.

In the **Advanced Setting** page, you can further configure the cellular network.



Description of the numbered areas

1. Maximum number of dial failures allowed for current SIM card (only for devices with dual SIM cards, better to leave it as is)
2. Click to restart the 4G module
3. Time scheduled for automatic restart of the 4G module when it is offline
4. Select a PDP type (leave it as is)
5. Select **custom** from the drop-down list, input **1** for AT&T SIM cards and **3** for Verizon SIM cards
6. Select **AT&T/TMO/Canada** or **Verizon** from the drop-down list for AT&T SIM cards and Verizon SIM cards, respectively
7. Default MTU value (1500)

Remember to save the settings to have the configurations take effect.

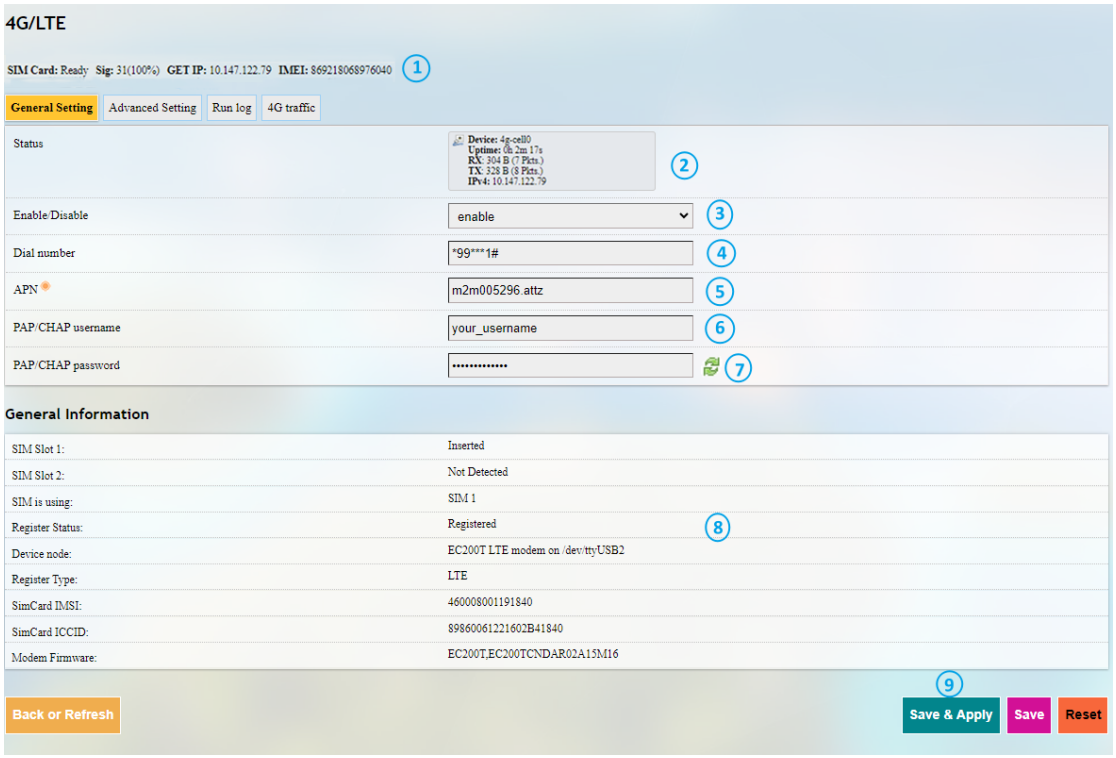
3.6.3 4G/LTE

Before you configure for 4G/LTE, be sure to install the activated SIM card and the LET antennas following the steps set out in 2.1.

Confirm with your sales executive whether the 4G module is AT&T or Verizon pre-certified. If so, when you apply for SIM cards from the carriers,

- provide Verizon with the pre-certified module name **VT-MOB-CELL-mPCIe**.
- provide AT&T with the pre-certified module name **VT-MOB-MPCIE-4G**.

After installation, the 4G signal indicators on the Router will light up to indicate the signal strength. Navigate to **Network > 4G/LTE** for more settings.



Description of the numbered areas

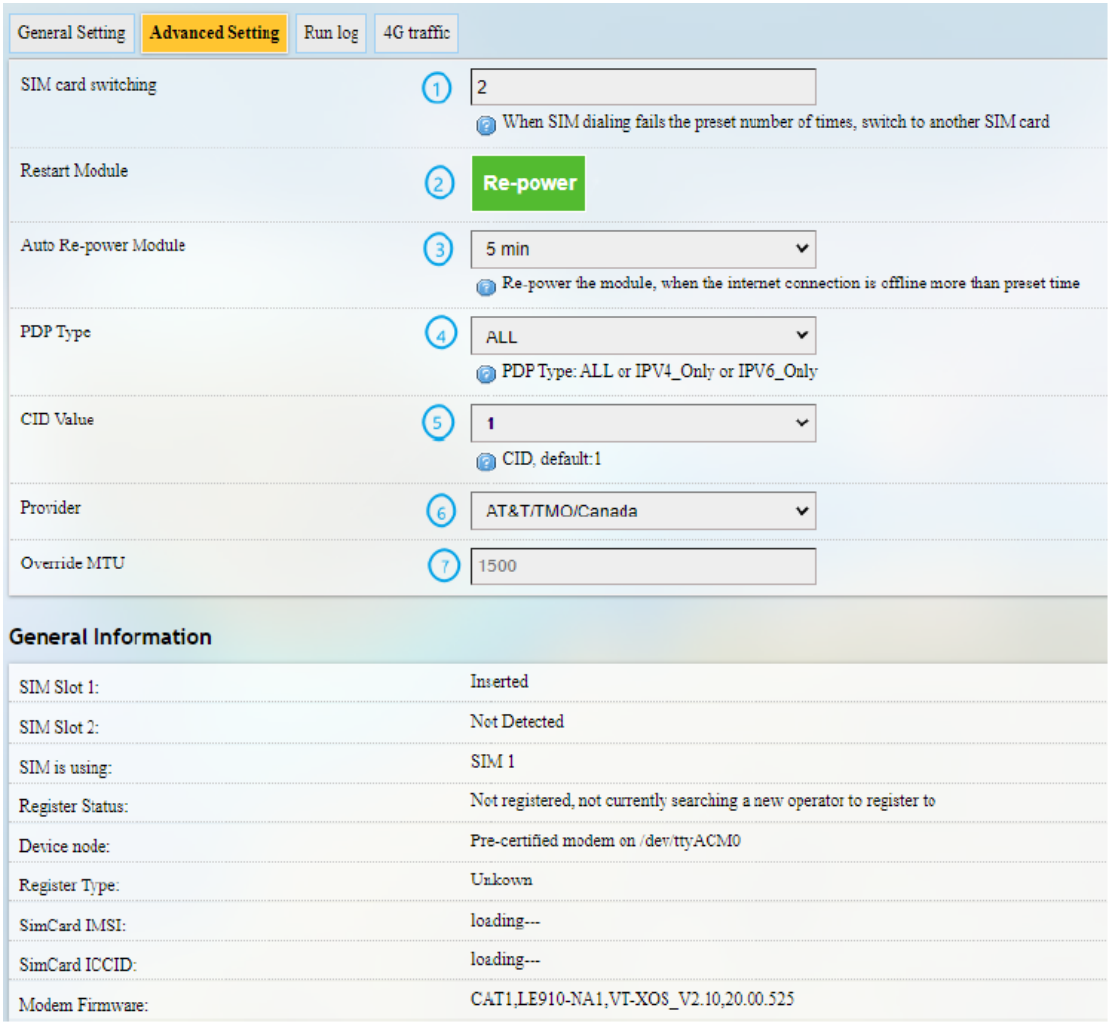
1. Connection status information (including SIM card status, signal strength, IP, and IMEI)
2. Status of the SIM card
3. Enable/Disable the SIM card
4. The Dial number is automatically populated (in case it does not work, ***99#** is applicable to all carriers)
5. The APN is automatically populated, you can replace it with the one provided by your carrier when necessary
6. Enter the username provided by the carrier for PAP/CHAP authentication
7. Enter the password provided by the carrier for PAP/CHAP authentication
8. Detailed information of the SIM cards
9. Make sure to save and apply the settings before you exit.

Leave the field as is if not applicable or if you are not sure.

PAP/CHAP username and password are to be specified only if your carrier has setup APN with user name and password.

*If you have inserted a SIM card into SIM slot 2, you can click the **SIM2 Card Setting** tab for more settings.*

In the **Advanced Setting** page, you can further configure the cellular network.

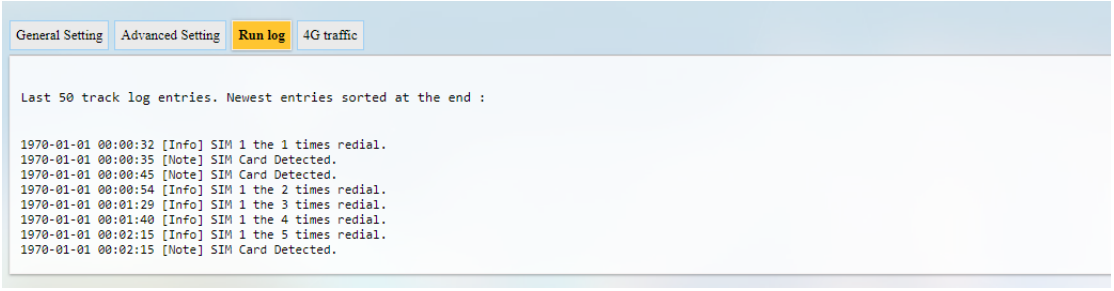


Description of the numbered areas

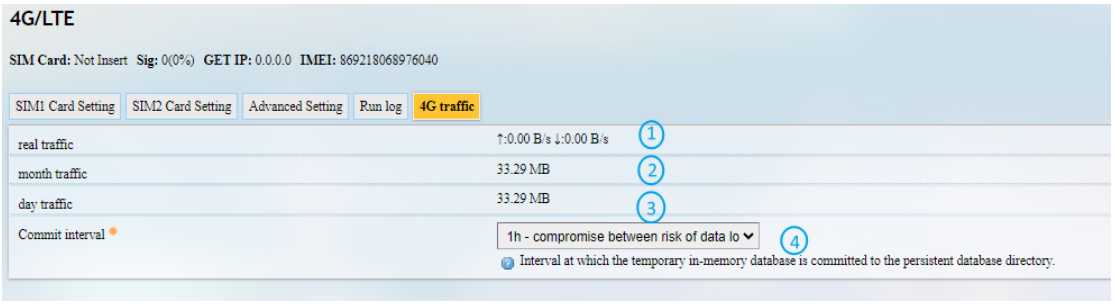
1. Maximum number of dial failures allowed for current SIM card (only for devices with dual SIM cards, better to leave it as is)
2. Click to restart the 4G module
3. Time scheduled for automatic restart of the 4G module when it is offline
4. Select a PDP type (leave it as is)
5. Select custom from the drop-down list, input 1 for AT&T SIM cards and 3 for Verizon SIM cards
6. Select AT&T/TMO/Canada or Verizon from the drop-down list for AT&T SIM cards and Verizon SIM cards, respectively
7. Default MTU value (1500)

Be sure to save the settings before you exit the page.

The **Run Log** tab next to the **Advanced Setting** tab displays the last 50 log entries of the module.



Under the **4G traffic** tab, traffic information measured in real time or on the monthly and daily basis is available. You can also set the interval for submitting the temporary in-memory database to the persistent database directory.



Description of the numbered areas

1. Real-time traffic
2. Data used in the current month
3. Data used in the day
4. Time interval for submitting the temporary database to the persistent database

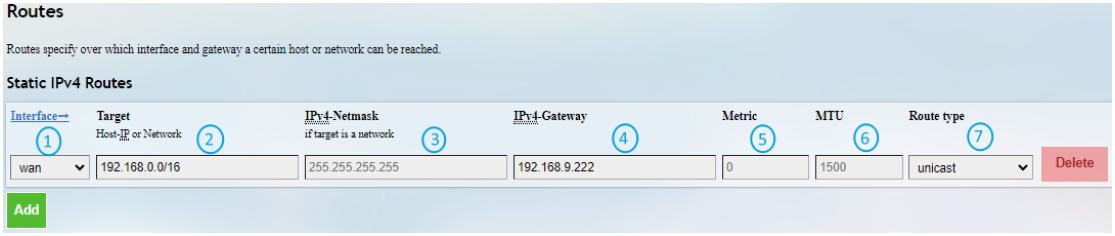
3.6.4 Static Routes

This is an advanced function allowing you to specify interface rules for route access.

Example:

Requirement: When the Router has 4G and WAN network interfaces, the internal network (192.168.0.0 - 192.168.255.254) is accessed via the WAN interface by the internal server. Other data access is realized via the 4G interface.

Click **Add** to set a new static route.



Description of the numbered areas

1. Select an interface to configure the route
2. Input the IP address of the host
3. Input the subnet mask (255.255.255.255 by default)
4. Input the address of IPv4 gateway
5. Gateway metric (The smaller the number, the higher the priority)
6. Set the MTU
7. Select a route type (refer to the details next page)

Be sure to save the settings before you exit the page.

Description of the route type:

Type	Description
Unicast	The route entry describes real paths to the destinations covered by the route prefix.
Local	The destinations are assigned to this host. The packets are looped back and delivered locally.
Broadcast	The destinations are broadcast addresses. The packets are sent as link broadcasts.
Multicast	IP datagrams are sent to a group of interested receivers in a single transmission. It is not present in normal routing tables.
Unreachable	The destinations are unreachable. Packets are discarded and the ICMP message of host unreachable is generated. The local senders will receive an EHOSTUNREACH error.
Type	Description
Prohibit	The destinations are unreachable. Packets are discarded and the ICMP message of communication administratively prohibited is generated. The local senders will receive an EACCES error.
Blackhole	The destinations are unreachable. Packets are discarded silently. The local senders will receive an EINVAL error.
Anycast	The destinations are any cast addresses assigned to this host. They are mainly equivalent to local with one difference that such addresses are invalid when used as the source address of any packet.

3.6.5 Firewall

3.6.5.1 Firewall – General Settings

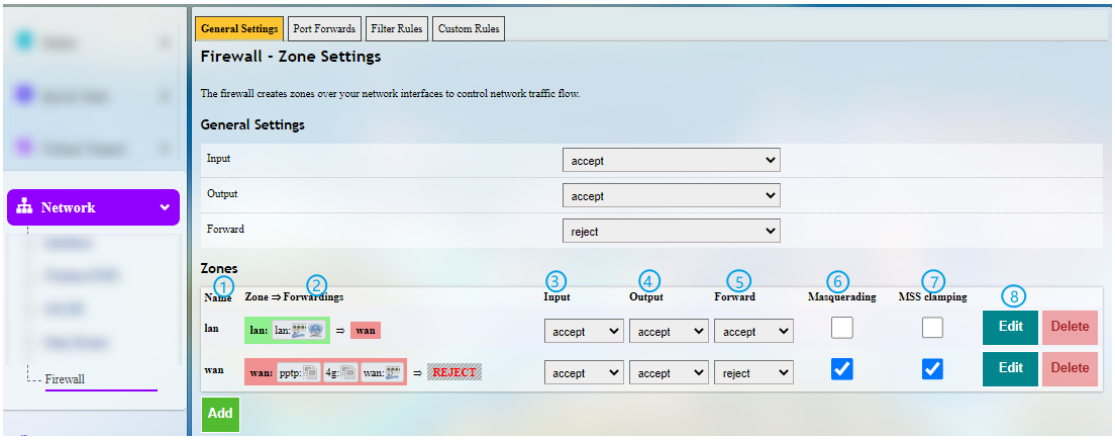
The following is a summary of the configuration items that the firewall can define. The minimum firewall configurations usually contain a basic setting item, at least two zones (LAN and WAN) and a forwarding to allow packets to be forwarded from LAN to WAN.

General Settings define the global settings that do not depend on a specific area. The following options can be defined:

Name	Type	Mandatory or not	Default value	Description
Input	String	N	ACCEPT	INPUT chain default strategy (ACCEPT, REJECT, DROP)
Forward	String	N	REJECT	FORWARD chain default strategy (ACCEPT, REJECT, DROP)
Output	String	N	ACCEPT	OUTPUT chain default strategy (ACCEPT, REJECT, DROP)

3.6.5.2 Firewall – Zones

A zone section groups multiple interfaces and serves as a source or destination for forwardings, rules and redirects. Masquerading (NAT) of outgoing traffic is controlled on a per-zone basis.



Description of the numbered areas

1. Unique zone name

At least LAN and WAN shall be listed under the zone name.

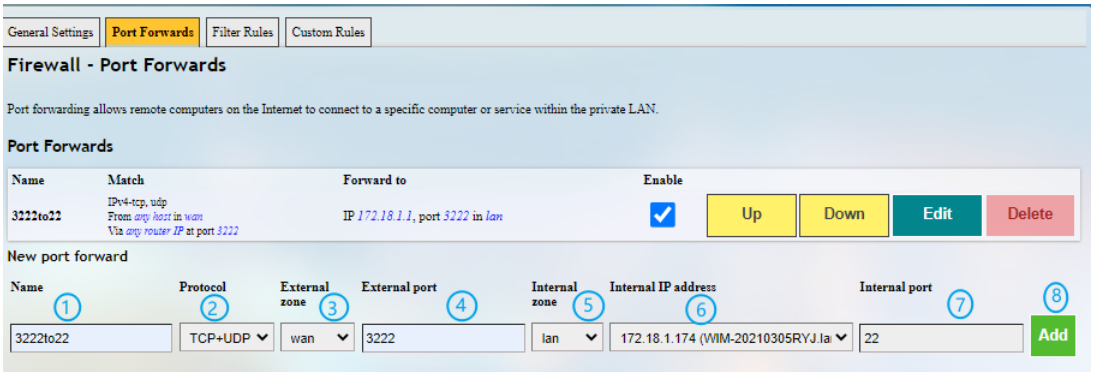
2. Zone forwarding model description
3. Default policy (ACCEPT, REJECT, DROP) for incoming zone traffic
4. Default policy (ACCEPT, REJECT, DROP) for outgoing zone traffic
5. Default policy (ACCEPT, REJECT, DROP) for forwarded zone traffic
6. Masquerading (NAT)
7. MSS clamping
8. Zone editing

A click of the **Edit** button following each zone will direct you to the detailed zone setting page where general settings, advanced settings and forwarding rules are available.

3.6.5.3 Firewall – Port Forwards

The forwarding sections control the traffic flow between zones and may enable MSS clamping for specific directions. Only one direction is covered by a forwarding rule. To allow bidirectional traffic flows between two zones, two forwardings are required, with src and dest reversed in each.

Illustrative example on port forwarding (Forwarding port 3222 (WAN) to port 22 of LAN host 172.18.1.174):



Description of the numbered areas

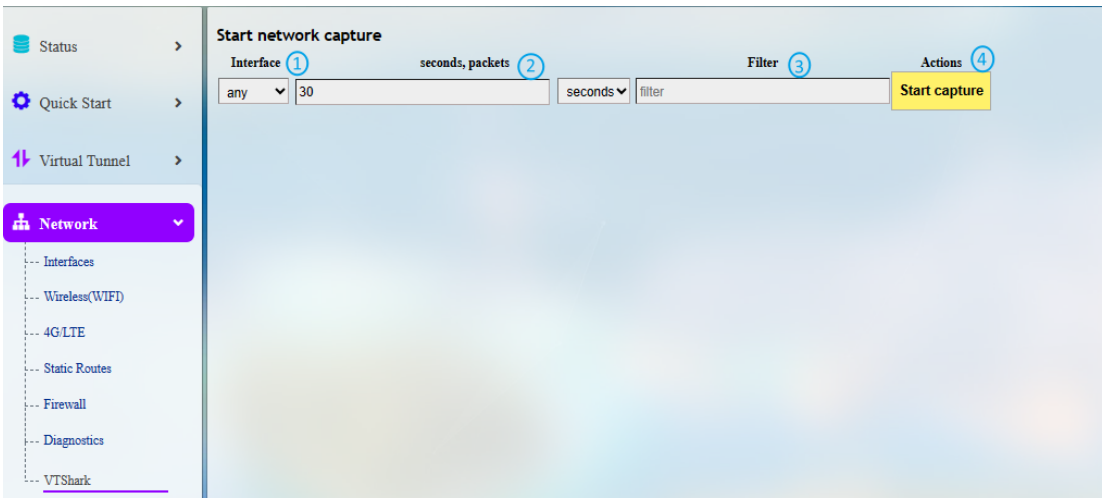
1. Rule name
2. Protocol (TCP/UDP/TCP + UDP are supported)
3. External zone: WAN
4. External port: 3222
5. Internal zone: Select the LAN port
6. LAN host: 172.18.1.174
7. Target host port number of the internal zone: 22
8. Add rules (mandatory)

3.6.5.4 Firewall – Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default rule settings have been loaded.

3.6.6 VTShark

The **VTShark** feature provides a flexible way to follow up and verify network issues. You can use wireshark to open and check the packets captured.



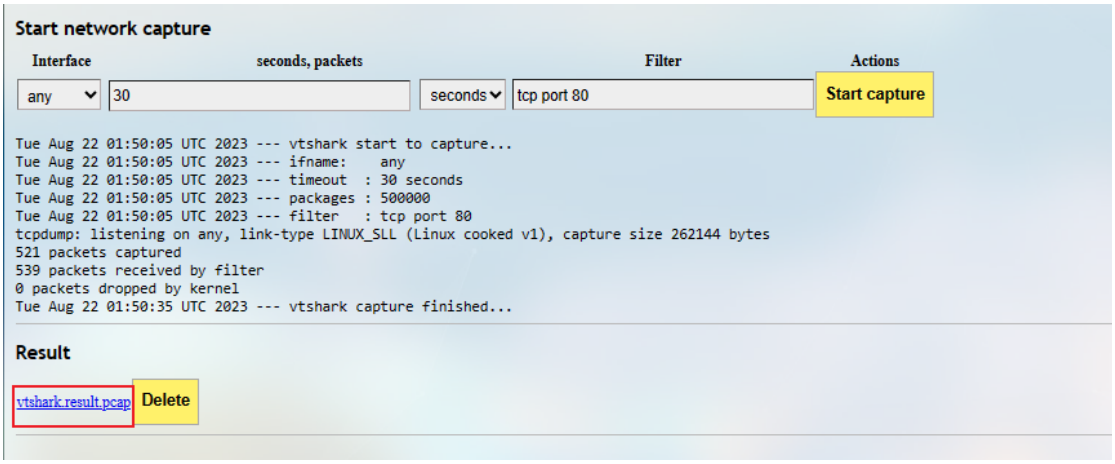
Description of the numbered areas

1. The interface from which the packets are captured (all interfaces are selected by default)
2. The measurement by which the data packets are captured (by seconds or by packet counts as explained below)
3. The filter for capturing the designated packets (more details are available at https://www.tcpdump.org/manpages/pcap-filter.7.html for advanced filtering)
4. Start the data capturing

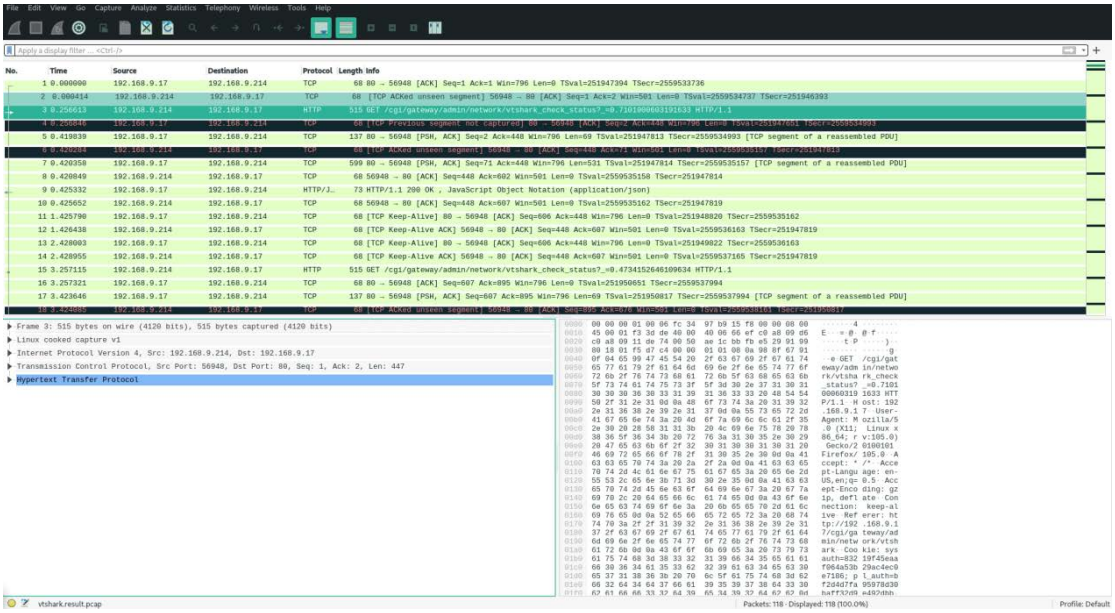
Packets capturing by seconds and by packet counts:

Measurement	Description
Seconds	To specify a time duration for data capturing. For instance, you can input '10/20/30…' for the data capturing, which indicates that the capture will stop in 10/20/30 seconds.
	The system supports up to 500,000 packets for the time-based data capturing. The capture stops after reaching this limit, even if it has not reached the preset time duration.
Packets	To specify the count of packets for data capturing. For instance, you can input '100/200/500…' for the data capturing, which indicates that the capture will stop when 100/200/500 packets have been captured.
	The system supports up to 10 minutes (600 seconds) for the packet-based data capturing. The capture stops after reaching this limit, even if it has not reached the preset packet counts.

In the following scenario, the capture targets at all interfaces for the http packets from 'tcp port 80' for 30 seconds.



Clicking the result will download it to the local directory and you can open it with wireshark.

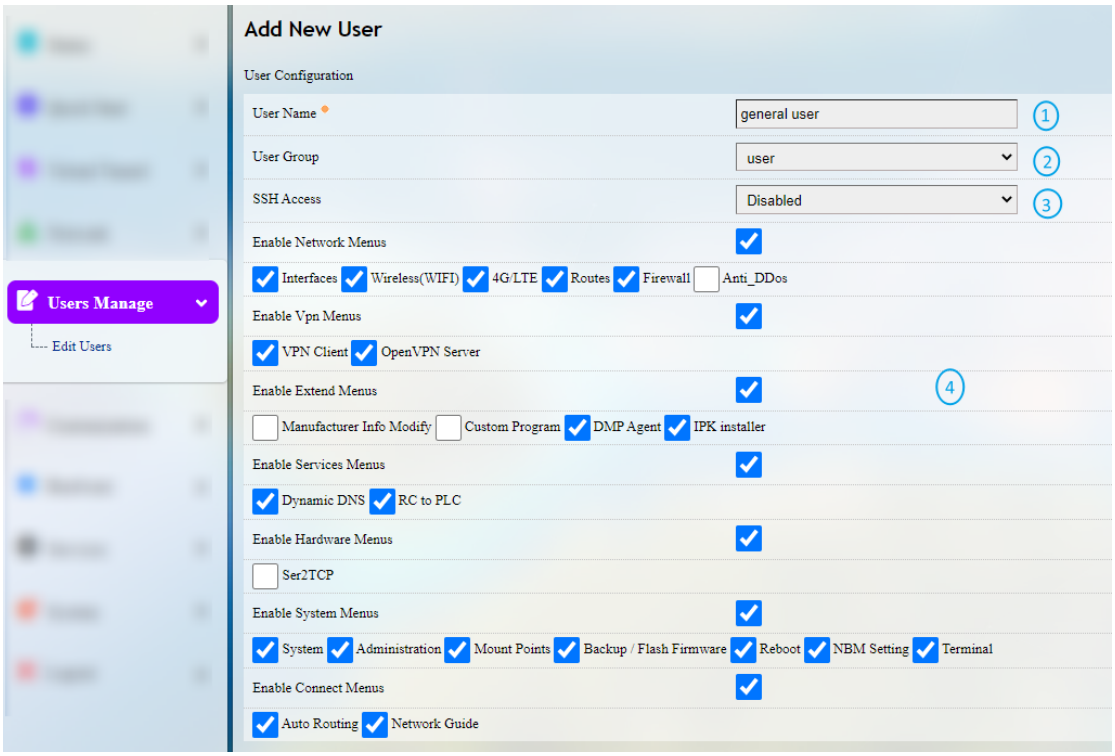


3.7 User Management

As this function may change system settings, you need log in with the root account (Refer to 2.2 for the username and password) to enable the function.

In the **Edit Users** page, you can add new users or edit the existing users.

To add a new user, click the button below the existing user information：

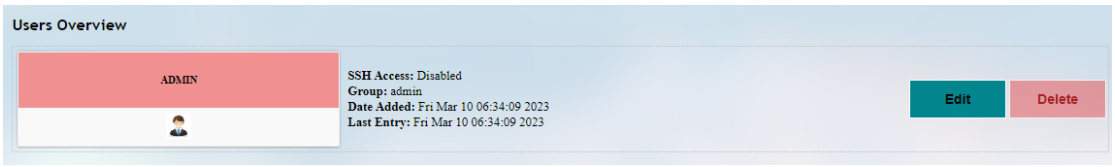


Description of the numbered areas

1. Input a username
2. Select a group for the new user
3. Enable SSH access or not for the new user
4. Enable the specific functions for the new user

Be sure to save the settings before you exit the page.

After creating the user, it will be added to the user list. The **Edit** and **Delete** buttons behind a user allow you to enable/disable certain functions for this user or delete this user.

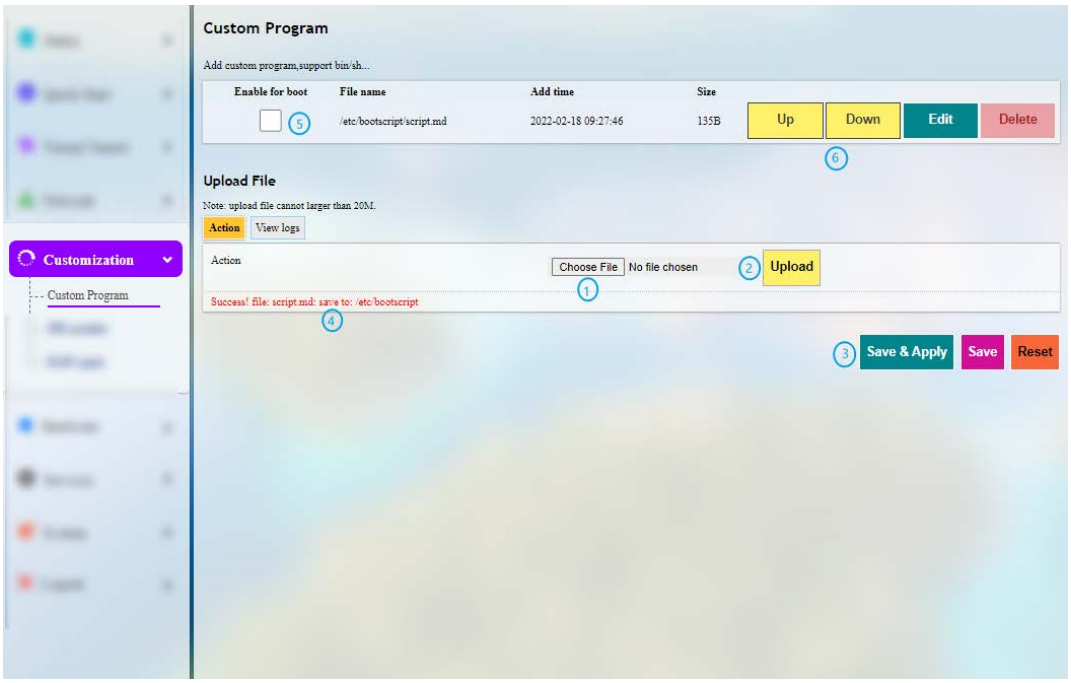


3.8 Customization

As certain functions under this tab may change system settings, you need log in with the root account (Refer to 2.2 for the username and password) to enable the function.

3.8.1 Custom Program

Custom program allows users to upload scripts or programs (sh/bin) to the Router and run them at the startup.

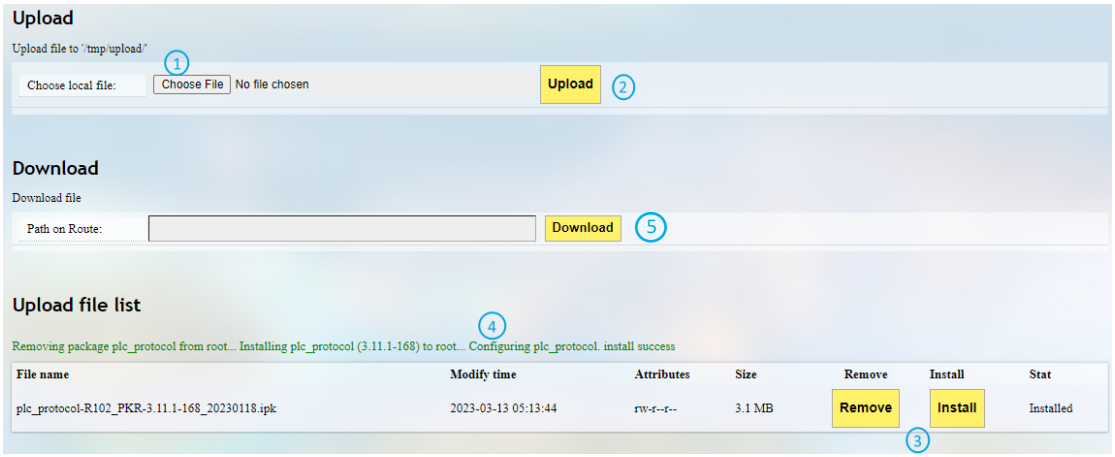


Description of the numbered areas

1. Select a script to upload
2. Upload the script to the Router
3. **Save & Apply** the settings
4. When the script is uploaded successfully, the file name and file directory will be displayed
5. Enable the script, and it will run next time when the router starts up
6. If more than one script is uploaded, you can move any of them up or down to rearrange the script order, and edit/delete the script

3.8.2 IPK Installer

With IPK Installer, customers can install self-compiled IPK packages to the Router. Vantron industrial protocol packages are also uploaded from here.

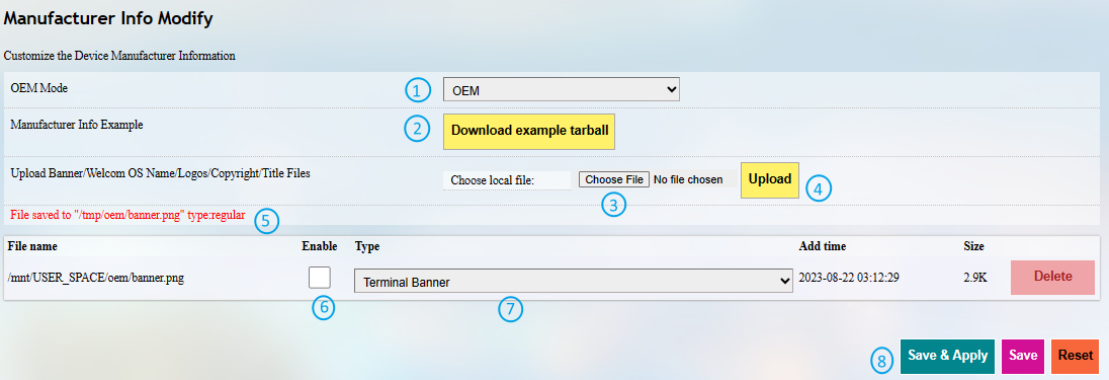


Description of the numbered areas

1. Select an .ipk file from the local directory
2. Click **Upload** to upload the file to the device
3. You can delete or install the file after the .ipk file is uploaded
4. Install the file and wait a moment, there will be a prompt for the installation status
5. You can also input a file path on the device to download the specific file

3.8.3 Manufacturer Info Customization

Once you need to customize the manufacturer information for logging in the system, navigate to **Customization > Manufacturer Info Modify**, and select **OEM** from the **OEM Mode** drop-down list.



Description of the numbered areas

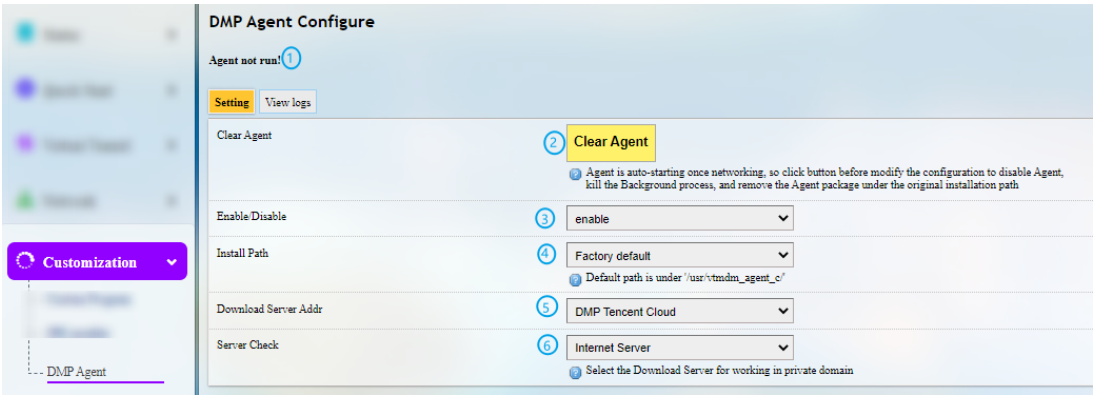
1. Select the **OEM** mode
2. Download the illustrative .tar file to the local directory and replace the files with your own as necessary
3. Select the target file from the local directory
4. Upload the file to the Router
5. The path of the file will be displayed here
6. Choose to enable the file or not for next startup
7. Select the type of the file
8. **Save & Apply** the settings

The three modes that customers can choose from the drop-down list based on needs are explained as follows.

Mode	Description
Vantron	All the information displayed in VantronOS will be Vantron-related
Standard	Some of the information displayed in VantronOS will be “Gateway” by default, and some information like the copyright will be left blank.
OEM	All the information displayed will be user tailored

3.8.4 DMP Agent

Gateways/routers are interfacing with BlueSphere GWM via DMP Agent. You can modify the settings of the DMP agent here.



Description of the numbered areas

1. Status of DMP Agent
2. Click **Clear Agent** before changing any configurations

Provided that the remaining prerequisites (refer to 2.5 Interfacing with Vantron Gateway Management Platform) are met, the DMP Agent, once enabled, will run automatically when there is internet access. Clicking this button will disable DMP Agent, kill all the processes running at the background, and remove the Agent package from the original installation directory.

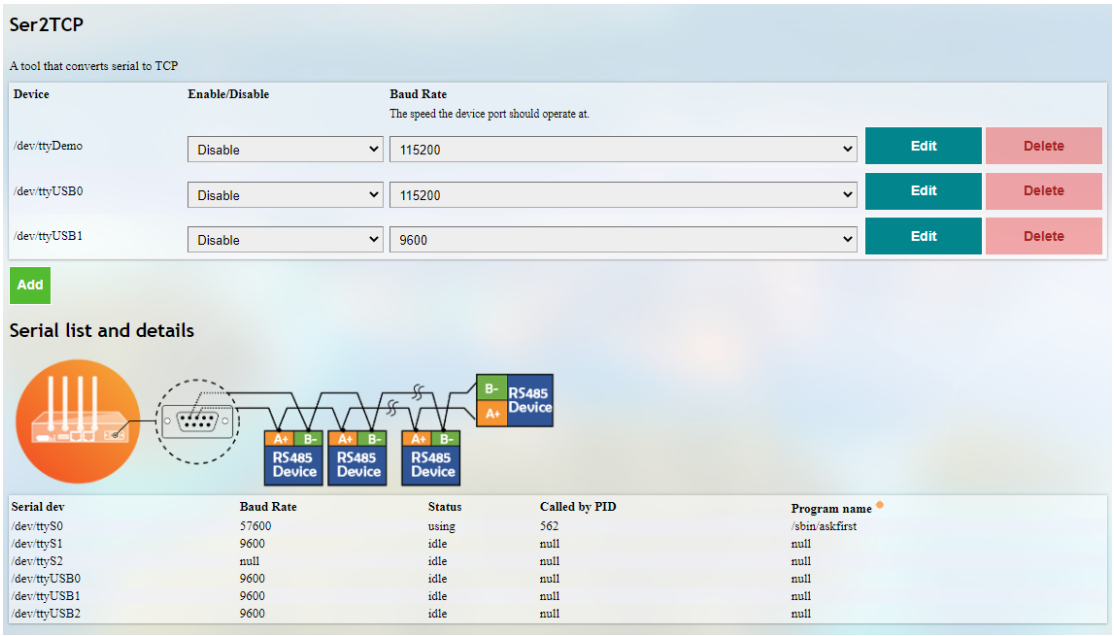
3. Enable/Disable the Agent
4. You can customize the installation path of the Agent here (default path: '/usr/vtmdm_agent_c/')
5. Set up the download address of the Agent server (better to keep the default setting)
6. Internet server for public domain and download server for private domain

*Factory reset of the Router will deactivate the device on the BlueSphere GWM platform. If you wish to activate it again on the GWM, please click **Clear Agent** in the VantronOS portal, then **enable** the agent and wait a moment to allow the device to come online on the BlueSphere GWM platform.*

3.9 Hardware

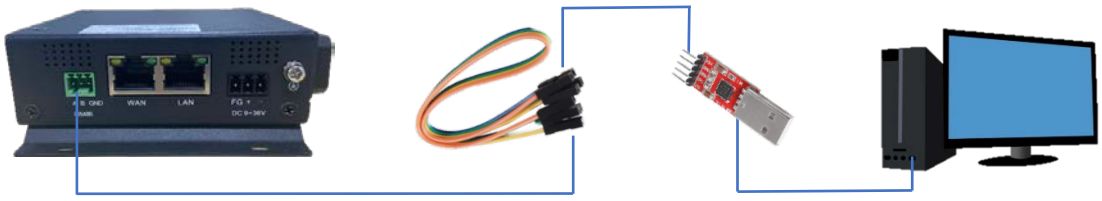
3.9.1 Ser2TCP

Serial to TCP provides an easy way to convert local serial data into Ethernet data and enables two-way communication with remote devices. Each conversion rule can be independently configured to server-side or client-side mode. You can also add, edit or delete a conversion rule on this page.



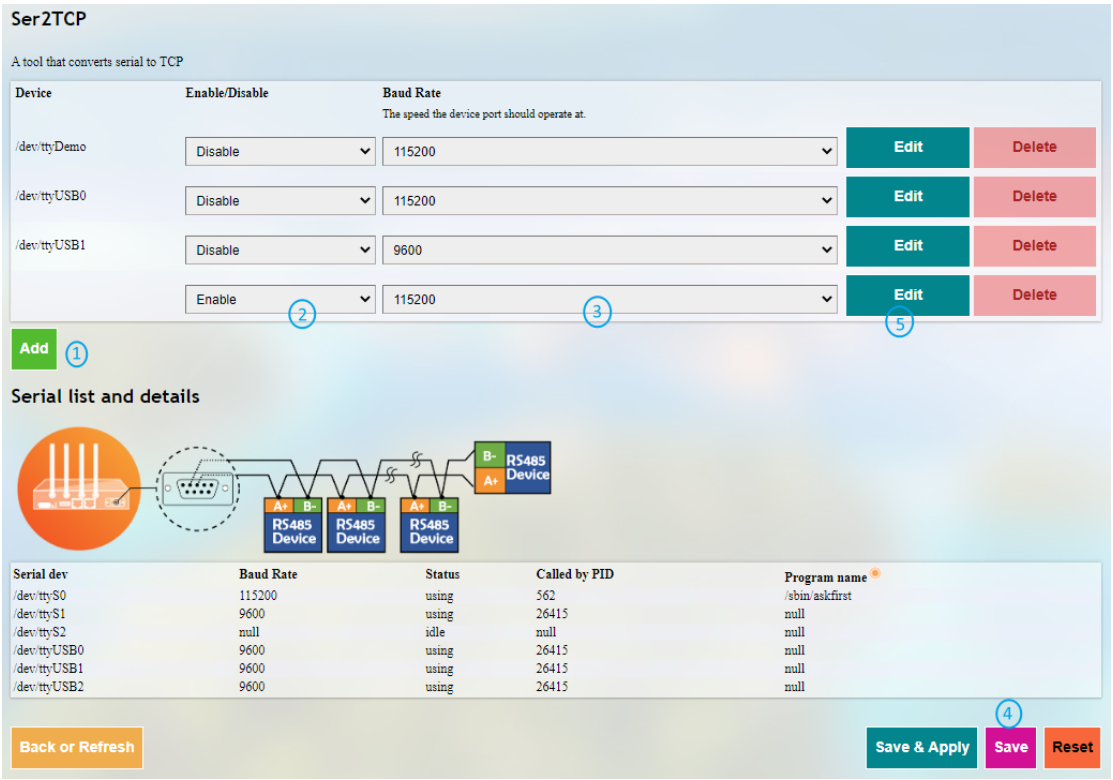
3.9.2 Ser2net environment setup and verification

- Prerequisites
  - An R102 router
  - An Ubuntu host
  - A USB to TTL serial adapter
  - A DuPont cable
  - Connect the serial port of the router to the host as follows



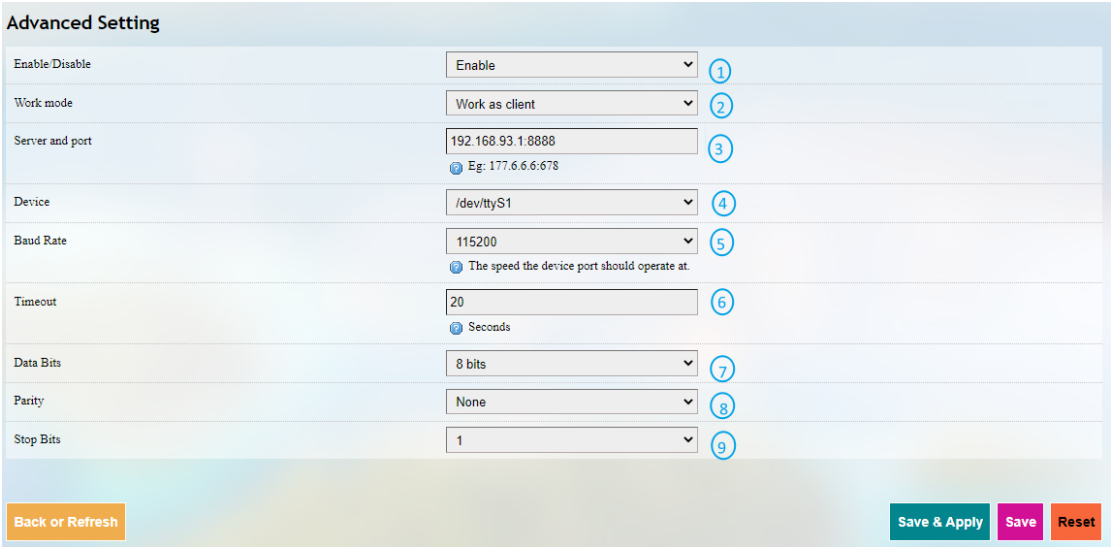
- Client mode

(1) Settings on VantronOS web interface



Description of the numbered areas

1. Click **Add** to add a conversion rule
2. Select **Enable** from the drop-down
3. Set the Baud rate to 115200
4. Save the settings
5. Click **Edit** after the rule to enter the advanced settings page



Description of the numbered areas

1. **Enable** the rule
2. Select the **Work as client** mode
3. Input the server address and port number (Ubuntu host shall be the server, and port number is user-defined)
4. Select the serial device from the drop-down (software node is /dev/ttyS1 as described in 1.5)
5. Select 115200 as the baud rate (the default value will be the one selected when setting up the rule)
6. Set a timeout value
7. Select “8 bits” for the data bit
8. Select “None” for parity
9. Select “1” as the stop bit

Save and Apply above settings before you exit.

(2) The Ser2net process is running as follows:

```
uart2net -c -d 192.168.93.1 -p 8888 -t /dev/ttyS1 -b 115200 -a 8 -r none -s 1 -o 20
```

(3) Settings on the Ubuntu host

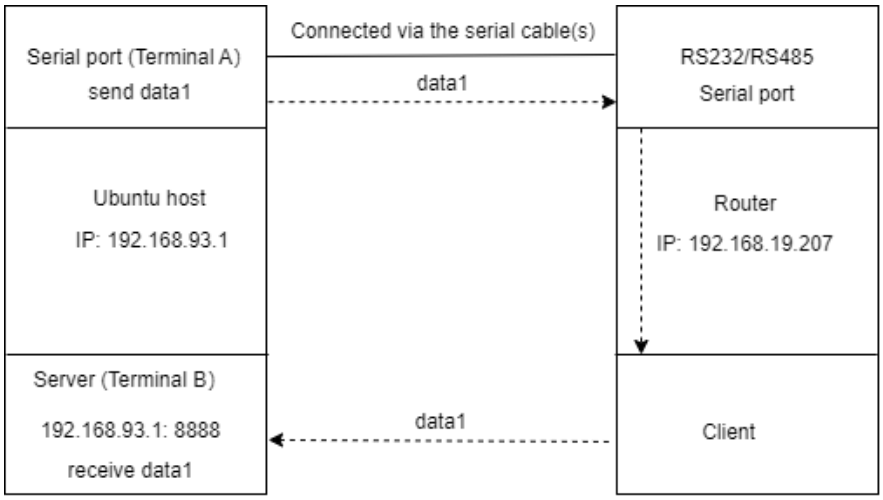
- Use microcom to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- Monitor the designated port (8888 as assigned in prior steps)

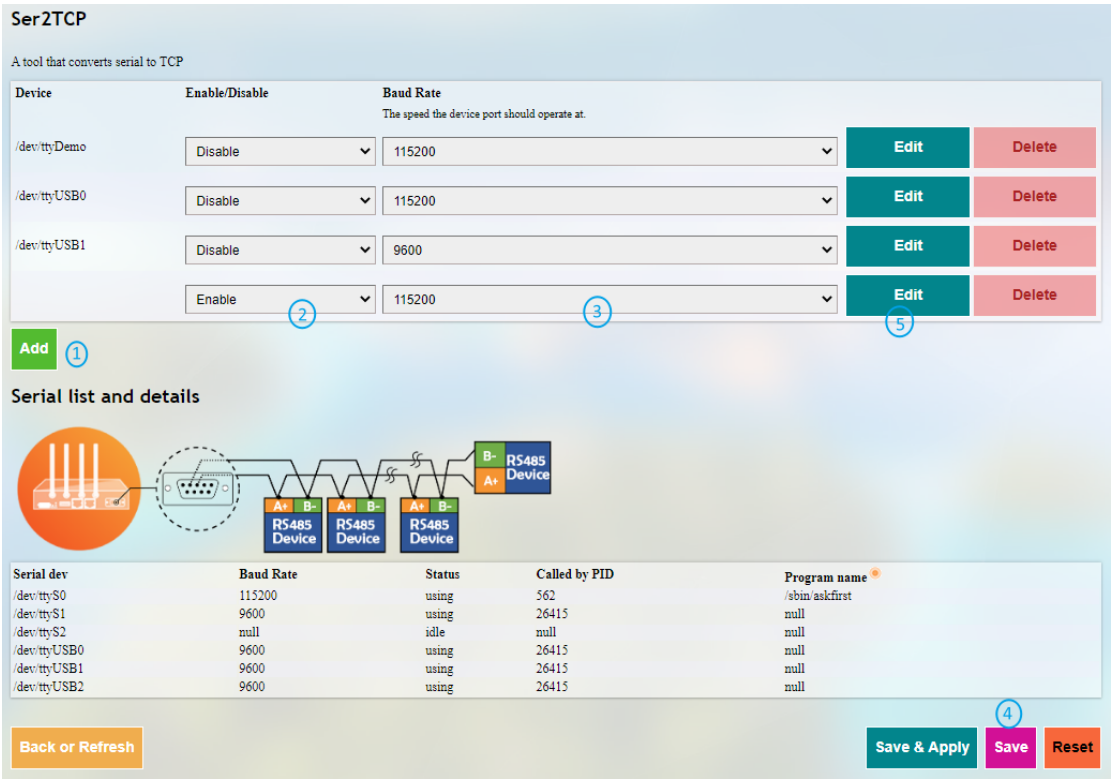
```
tcpudp_test tcp server:tcpudp_test -p 8888
```

- Input data in terminal A and receive in terminal B (the topology is as follows)



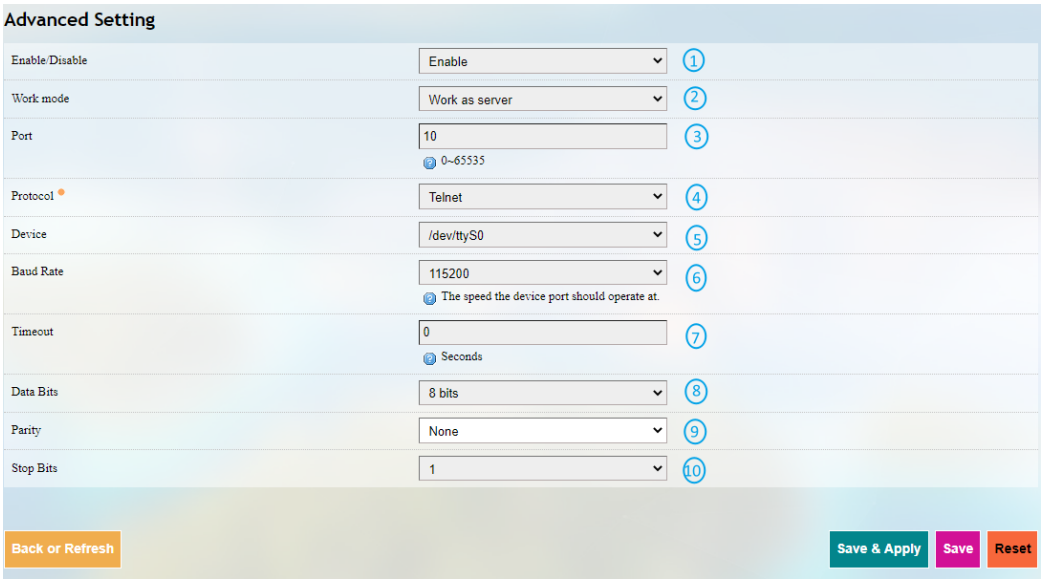
- Server mode

(1) Settings on VantronOS web interface



Description of the numbered areas

1. Click **Add** to add a conversion rule
2. Select **Enable** from the drop-down
3. Set the Baud rate to 115200
4. Save the settings
5. Click **Edit** after the rule to enter the advanced settings page



Description of the numbered areas

1. **Enable** the rule
2. Select the **Work as server** mode
3. Input the port number (user-defined)
4. Select a protocol from the drop-down (**Telnet** for instance, see 3.8.3 for the difference between the protocols)
5. Select the serial device from the drop-down (software node is /dev/ttyS1 as described in 1.5)
6. Select 115200 as the baud rate (the default value will be the one selected when setting up the rule)
7. Set a timeout value
8. Select “8 bits” for the data bit
9. Select “None” for parity
10. Select “1” as the stop bit

Save and Apply above settings before you exit.

(2) The Ser2net process is running as follows:

```
/usr/sbin/ser2net -n -c /tmp/ser2net.conf
```

(3) Settings on the Ubuntu host

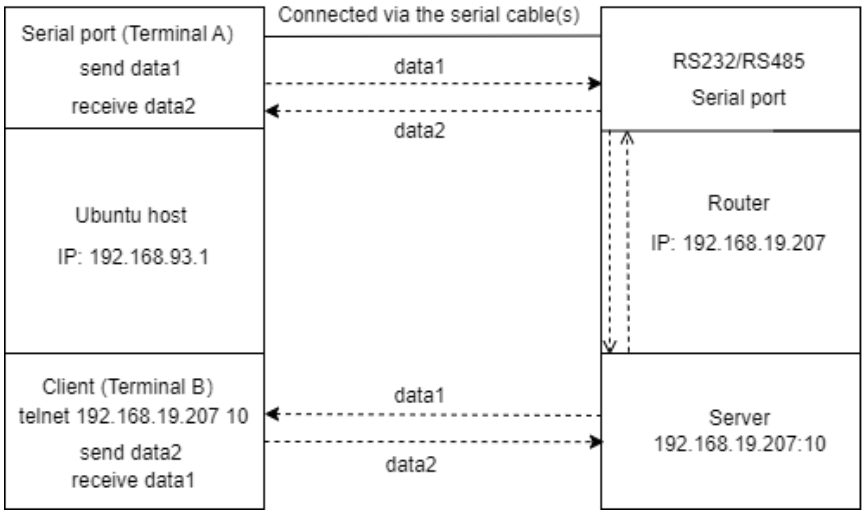
- Use microcom to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- Monitor the designated port (10 as assigned in prior steps) in terminal B using Telnet protocol

```
telnet 192.168.19.207 10
```

- Terminals A and B can send and receive data in both directions (the topology is as follows)



3.9.3 Protocol comparison

Under the server mode, three protocols are available which are differentiated as below:

1) Raw: enables the port and transfers all data as-is between the port and the long integer.

2) Rawlp: enables the port and transfers all input data to a gateway that is open without any Termios settings, allowing to use /dev/lpx devices and printers connected.

3) Telnet: enables the port and runs the telnet protocol on the port to set up telnet parameters (less used).

3.10 Services

3.10.1 Dynamic DNS

Dynamic DNS is a technology in domain name system (DNS) that automatically updates the content of Name Server, often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information.

Input a name of the subdomain or root domain and click **Add** button, and you will be directed to the setup page of the dynamic DNS. Then you can edit the service as needed.

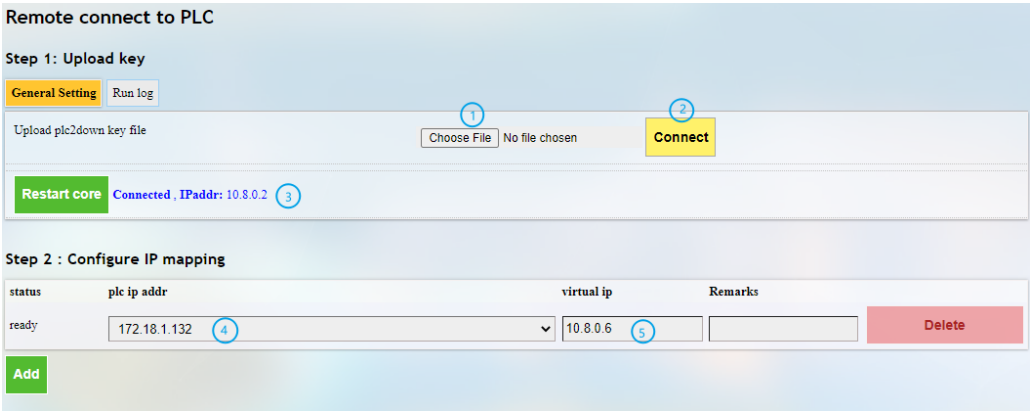
3.10.2 RC to PLC

For remote access and control of PLC devices via OpenVPN protocol, you will need two R105 routers and a Windows host computer ('Windows PC') that are on the same network. One router ('R1') is for building an OpenVPN server, and the other ('R2') is for connecting the OpenVPN server built by R1.

Prerequisites:

1. Prepare the R1, R2, Windows PC, and PLC device
2. Connect R1 and R2 to the same network via Wi-Fi or Ethernet
3. Install an OpenVPN client program (such as OpenVPN-2.5.2-I601-amd64.msi) and a PLC programming software (such as STEP7 depending on the device) on the Windows PC
4. Refer to 3.4.1 OpenVPN Server to build an OpenVPN server in the **tap** working mode on R1 and download the .ovpn file
5. Connect the Windows PC to the OpenVPN server built by R1 via the OpenVPN client program
6. Connect R2 to the OpenVPN server built by R1 (see below)
7. Connect the PLC device to a LAN port of R2 and set a static IP address for the PLC (see details below)
8. Connect the PLC device to the Windows PC via Ethernet and control the PLC with the PLC programming software (STEP7)

VantronOS offers a platform for connecting R2 to R1 and configuring the PLC and R2. For other settings, please download the related software program and finish the setup.



Description of the numbered areas

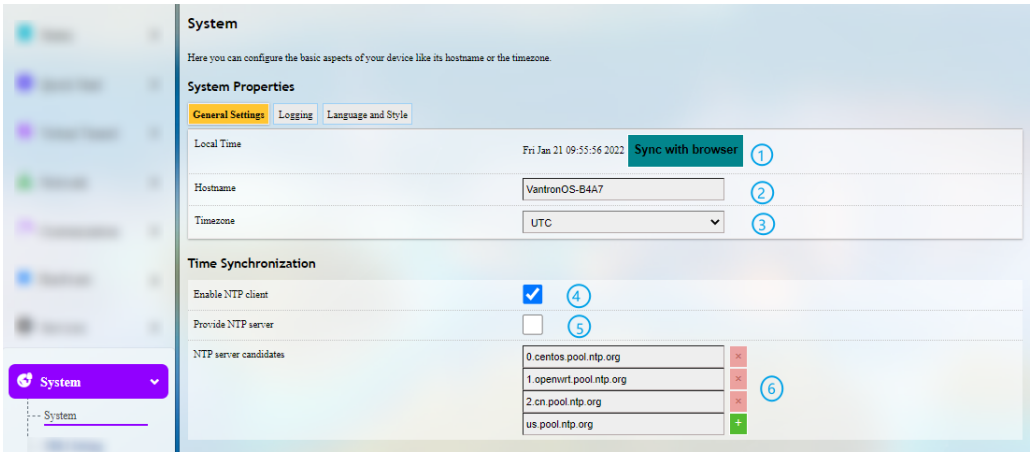
1. Download and save the .ovpn file after setting up the OpenVPN server on R1, then click this button to open the directory of the file
2. Click **Connect** to connect R2 to the OpenVPN server built by R1
3. After connection, an IP address assigned by the OpenVPN server will be displayed here
4. Input a static IP address for the PLC (on the same IP network as the LAN port of R2)
5. Input a virtual IP for the PLC (on the same IP network as the one assigned by the OpenVPN server and not occupied by other clients)

Be sure to save above settings to allow them to take effect.

3.11 System

3.11.1 System

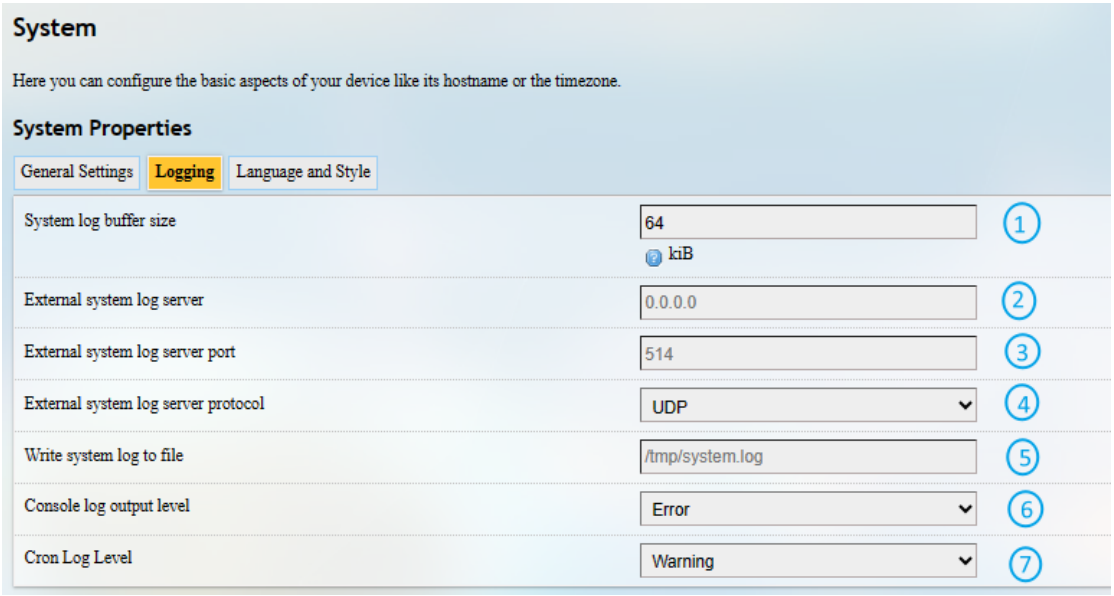
Apart from the device settings you might make in the previous sections, here you can configure your Router in more details, including host name, time zone, administrative password and so on.



Description of the numbered areas

1. Synchronize the router time with the browser (local) time
2. Change the name of the host
3. Select a time zone
4. Enable NTP online time adjustment
5. Start the NTP server
6. NTP online time server

For log-related settings, click **Logging** tab next to the **General settings** tab.

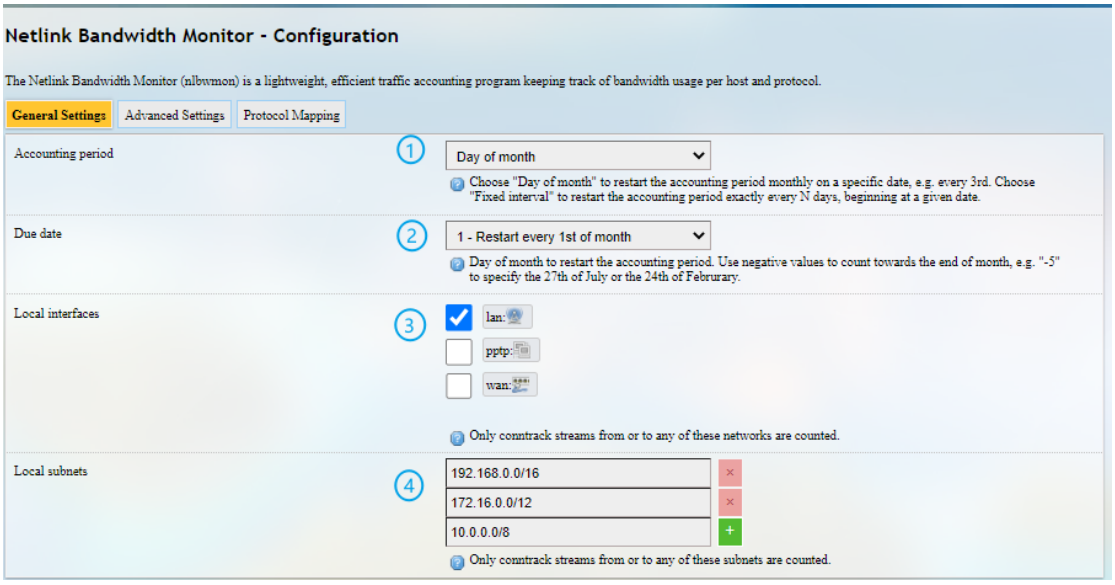


Description of the numbered areas

1. Buffer size of the system log
2. Address of the log server
3. Port of the log server
4. Protocol used by the log server
5. Path of the file for the system log
6. Output level of the console log
7. Cron log level

3.11.2 Netlink Bandwidth Monitor (NBM) Setting

- **General Settings**



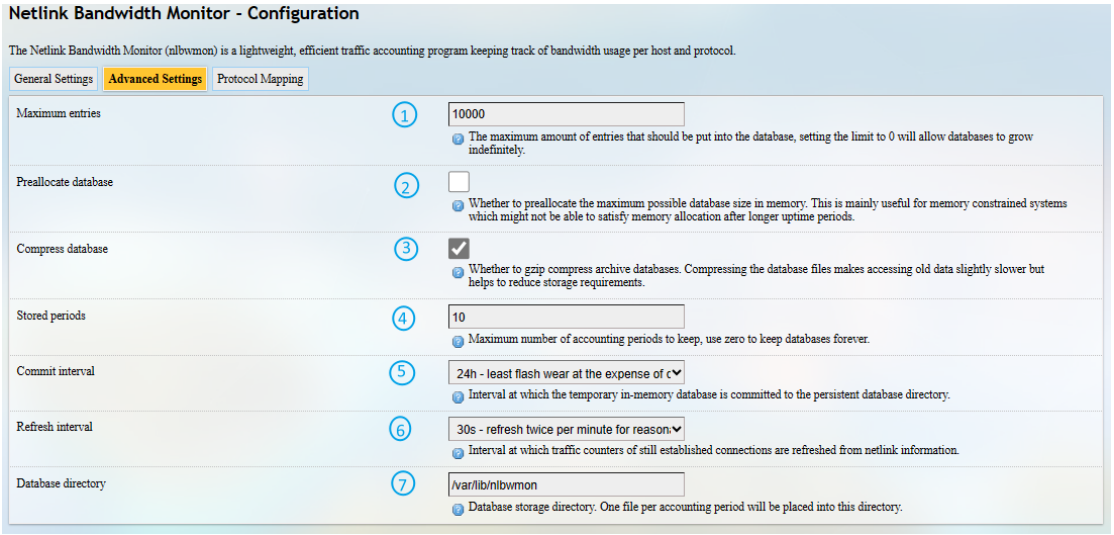
Description of the numbered areas

1. Set how long you would like the monitoring activities to be reported
2. Specify a date in a month for restarting another round of monitoring activities

Applicable when Day of month is selected in 1

3. Select the interfaces to monitor
4. Local subnets

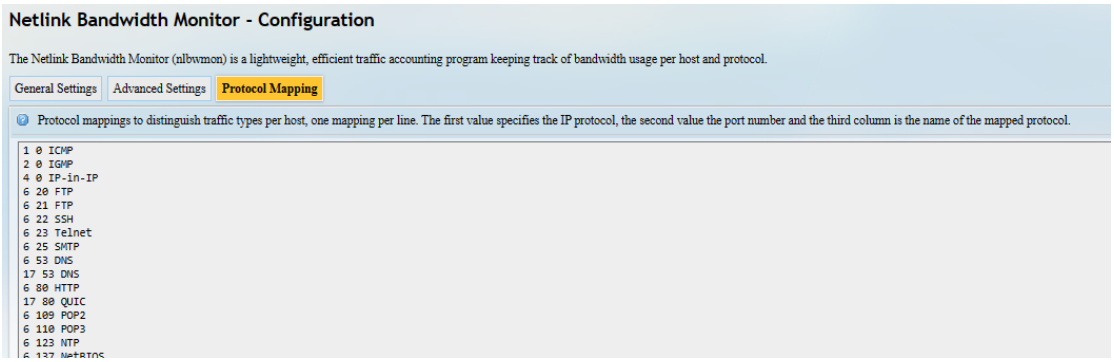
Under **Advanced Settings** tab, you can further set up the monitoring activities.



Description of the numbered areas

1. Set the maximum count of entries to store in the database (‘0’ for no limit)
2. Check the box to pre-allocate a database (more frequently applicable to devices with less memory space)
3. Check the box to compress the database
4. Maximum count of reporting periods to store (‘0’ for no limit)
5. Time interval for submitting the temporary database to the persistent database
6. Time interval for refreshing the traffic counters from the netlink information
7. Directory of the database

Protocol Mapping can be used to distinguish traffic types per host. Each mapping takes one line, with the first value being the IP protocol, the second value being the port number, and the third value being the name of the mapping protocol.



3.11.3 Administration

On this page, you can set a password for accessing the Router.

SSH Access

As this function might compromise the security of the network, you have to log in the web interface with a root account.

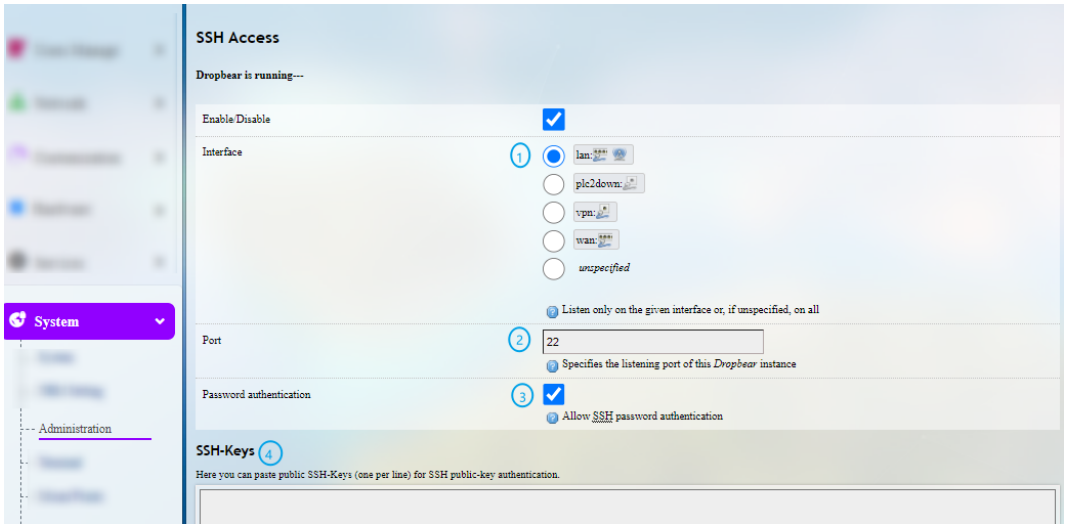
Step 1: Log out the interface by clicking **Logout** at the left bottom corner;

Step 2: Log in with the account and password;

Account: root

Password: rootpassword

Step 3: Navigate to **System > Administration**, and enable dropbear.



Description of the numbered areas

1. Select a port to access (LAN by default)

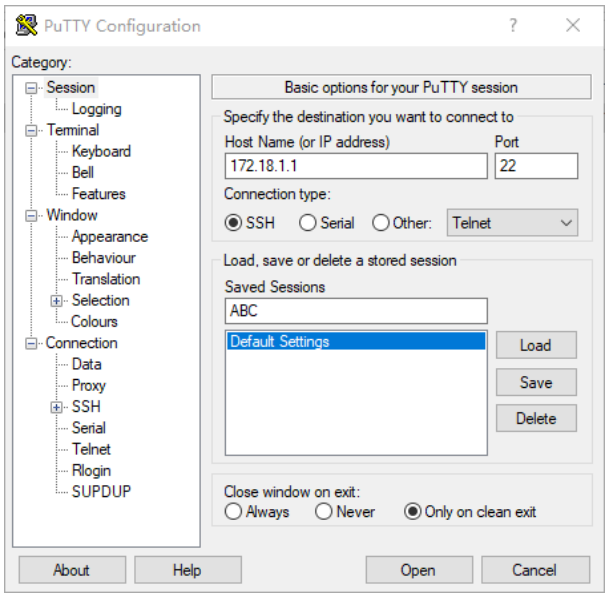
When "unspecified" is selected, all the ports will be monitored.

2. Specify a port for monitoring (port 22 by default)
3. Allow SSH password authentication
4. Add SSH-Keys for public key authentication

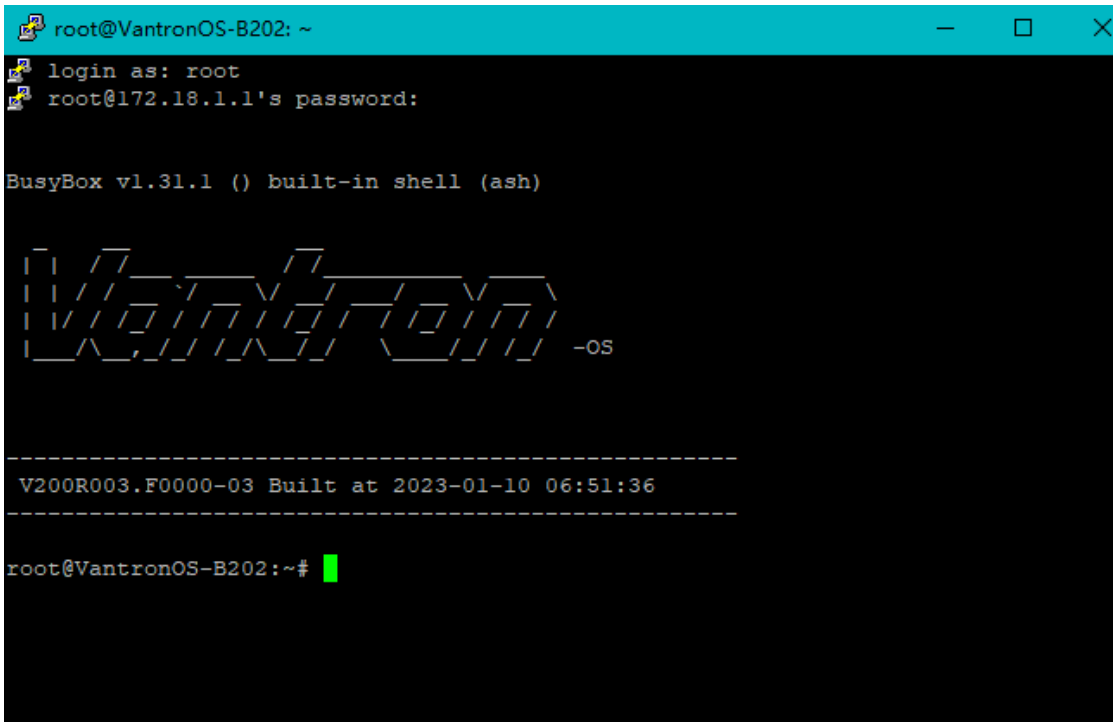
Step 4: Open an SSH client (PuTTY or MobaXterm recommended) in the Windows host;

Step 5: Input the host name or IP address (LAN port address by default: 172.18.1.1), keep the default port No. (22), and select **SSH** for the connection type;

Step 6: Set the session name and **Save**, keep the other settings unchanged, then click **Open**;

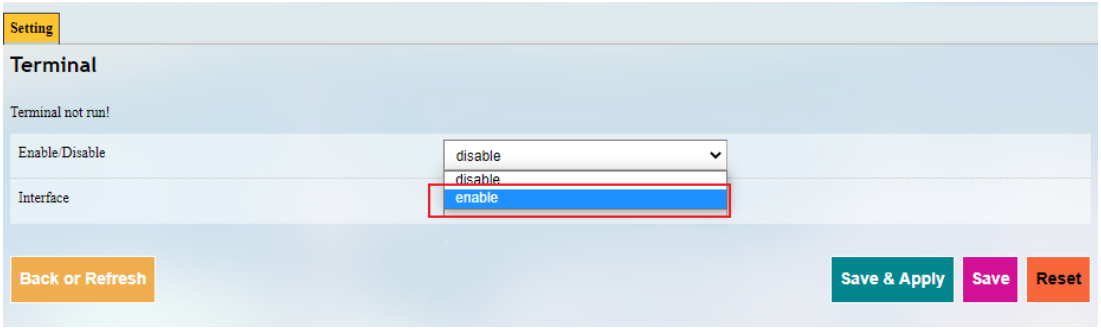


Step 7: Log in to the root account (password same as the router login password as shown above), and start an SSH remote session.



3.11.4 Terminal

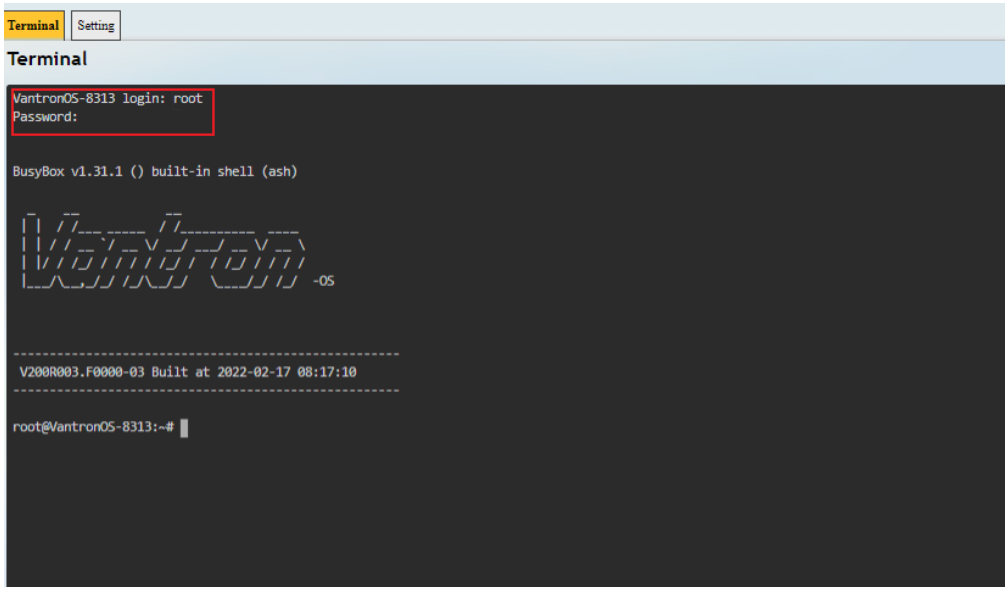
Under the **Setting** tab, users can click **enable** from the drop-down box and **Save & Apply** to enable the web terminal for router debugging.



After the web Terminal is enabled, the **Terminal** tab will be available next to the **Setting** tab.

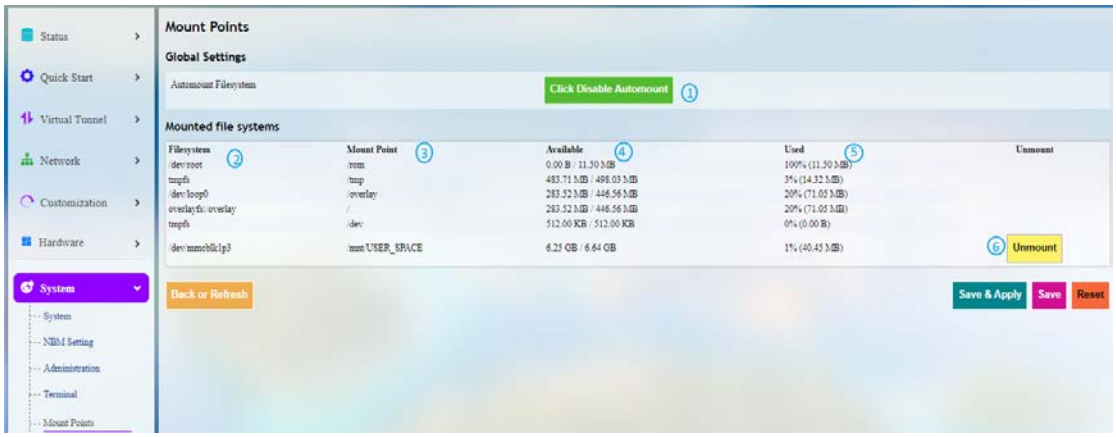
Login name: root

Login password: rootpassword (invisible while typing)



3.11.5 Mount Points

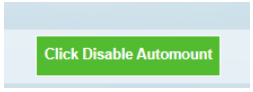
You can enable/disable automount and check the mounting information here.

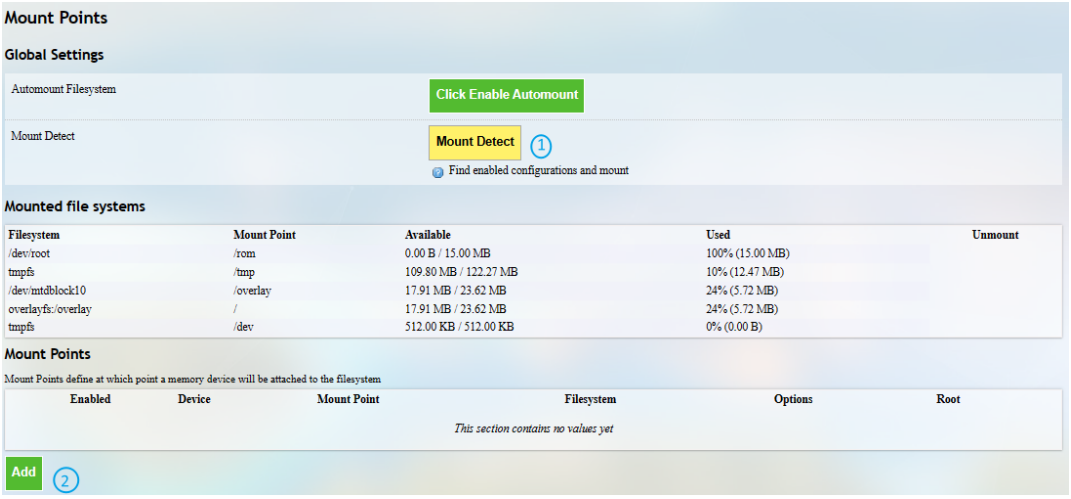


Description of the numbered areas

1. Disable/Enable automatic mount
2. File path on the Router
3. Mount point
4. Available space in the mount point
5. Space used in percentage
6. If you have previously mounted a file to the device, you can manually unmount the file here

To manually mount a file, click the **Click Disable Automount** button first and then proceed with the settings.

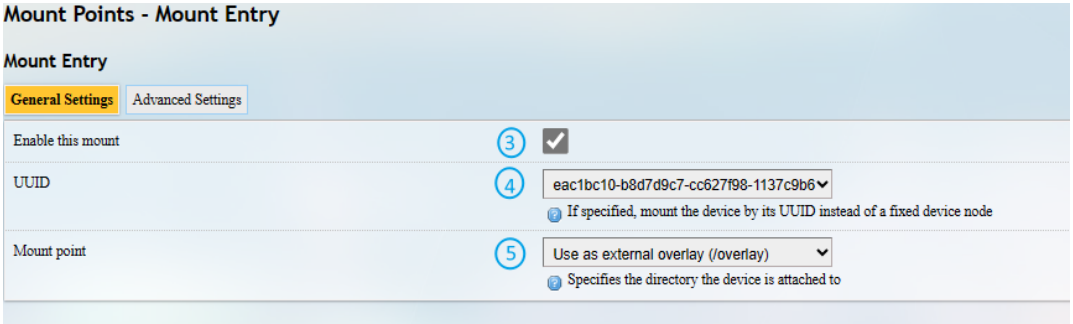




Description of the numbered areas

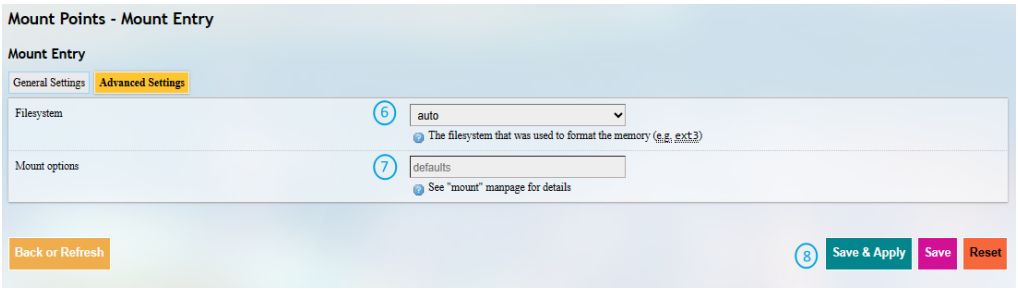
1. Detect the available mount points
2. Click **Add** to add a mount point

Click the **Edit** button behind the newly added mount point for more settings.

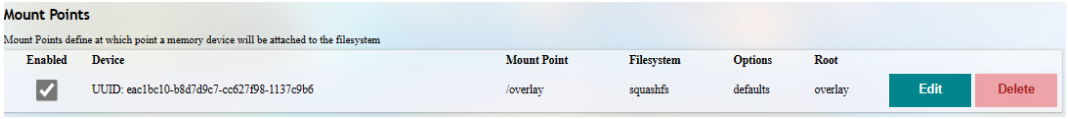


3. Check the box to enable the mount point after creation
4. Select the UUID of the device
5. Select the mount point

Then click the **Advanced Settings** tab to access advanced settings.



6. Select the file system for formatting the memory
7. Input the mount options
8. Save the settings and click the **Back or Refresh** button to return to the general settings

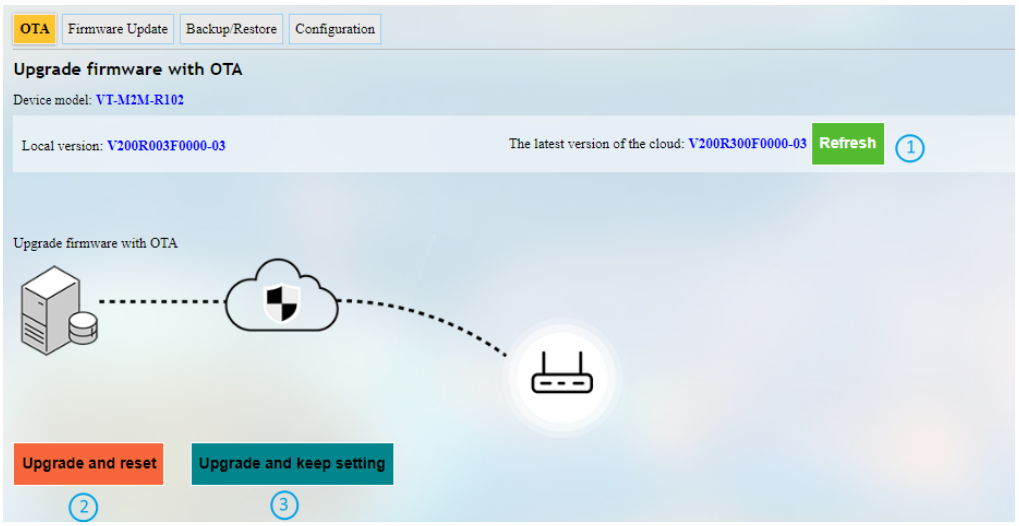


The mount point is created as above.

3.11.6 Backup/Flash Firmware

On this page, you can backup/restore parameters, restore factory settings (clear user settings), and update firmware from local or with OTA.

OTA Upgrade

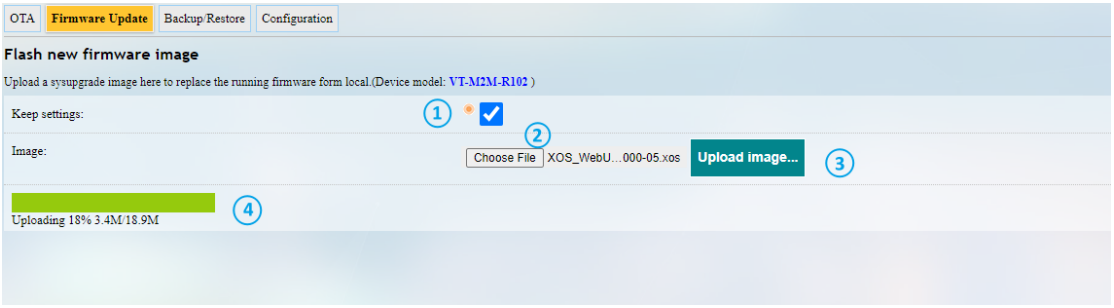


Description of the numbered areas

1. Refresh the cloud version to the latest
2. Upgrade the Router and reset to default settings
3. Upgrade the Router and keep the existing settings unchanged

*If the cloud version is shown **Failure**, the Router is not activated from the cloud, please contact your sales executive for solution.*

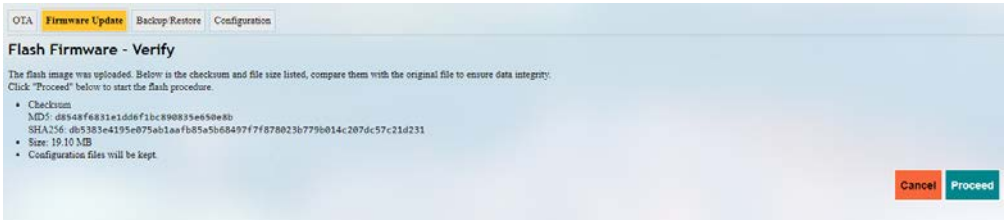
Firmware Update



Description of the numbered areas

1. Check the box to keep the user settings while upgrading the device (not recommended)
2. Select the firmware from the local directory
3. Click the button to upload the firmware
4. Upload progress of the package

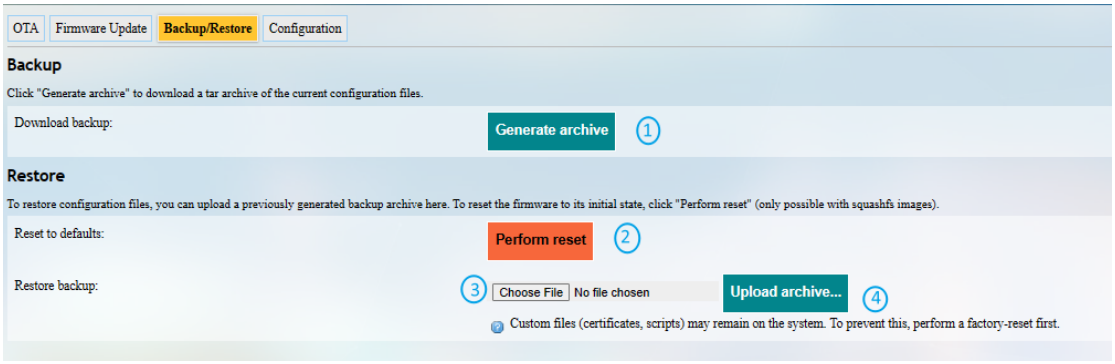
When the detailed information of the firmware is displayed, check if the firmware is correct, then click **Proceed** to start the upgrading;



It will take some time for the upgrade and DO NOT power off the Router when firmware upgrading is in process;

The login page will be refreshed once the upgrading finishes and you can login to check the firmware version on the homage.

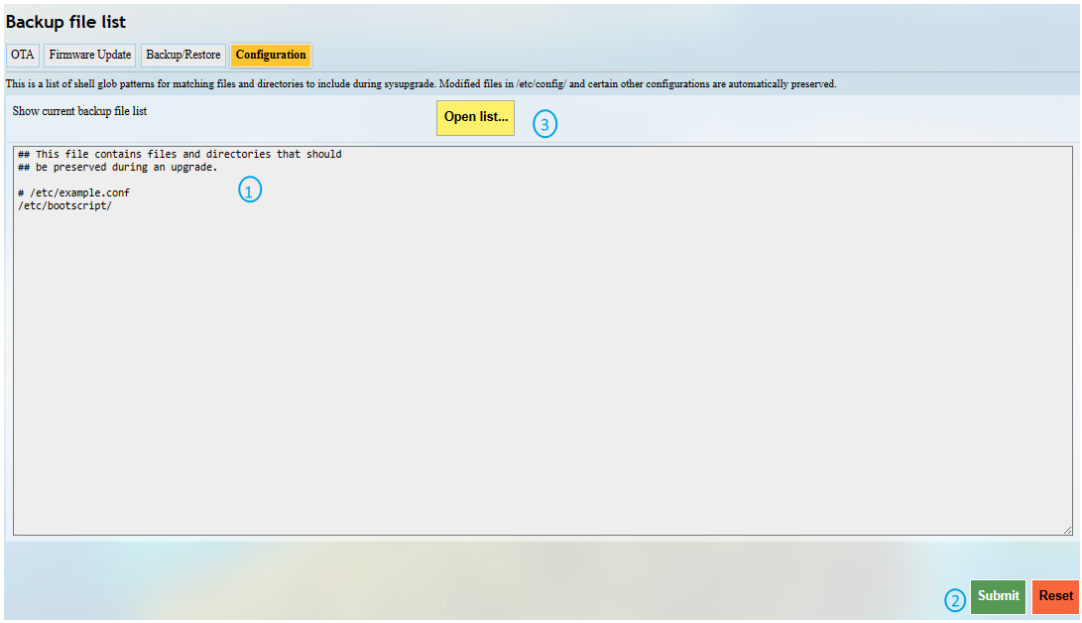
Under the **Backup/Restore** tab, you can download the backup package of your settings, including configuration files and pre-set folders, restore the factory settings of the Router, and upload the backup package saved before.



Description of the numbered areas

1. Click the button to back up the system configurations (include only the configuration files and preset files other than client files or programs)
2. Factory reset the Router (user configurations will be cleared)
3. Select the backup file from the local directory to restore the backup settings
4. Upload the file

Under the **Configuration** tab, you can customize the configuration files or directories to be retained during the upgrade.



Description of the numbered areas

1. Input the configuration file or directory to be retained during the upgrade
2. Click **Submit** to confirm the setting
3. Open the list of configuration files kept during the upgrade

3.11.7 Reboot

Make sure you don't have any ongoing process before rebooting the Router.

3.12 Logout

You will exit the web interface with a click on the **Logout** tab. If you need make changes to any of your settings, you can log in the web again with default password: **admin**. Make sure you have saved the changes before logout.

CHAPTER 4 DISPOSAL AND PRODUCT WARRANTY

4.1 Disposal

When the device comes to end of life, you are suggested to properly dispose of the device for the sake of the environment and safety.

Before you dispose of the device, please back up your data and erase it from the device.

It is recommended that the device is disassembled prior to disposal in conformity with local regulations. Please ensure that the abandoned batteries are disposed of according to local regulations on waste disposal. Do not throw batteries into fire or put in common waste canister as they are explosive. Products or product packages labeled with the sign of “explosive” should not be disposed of like household waste but delivered to specialized electrical & electronic waste recycling/disposal center.

Proper disposal of this sort of waste helps avoid harm and adverse effect upon surroundings and people’s health. Please contact local organizations or recycling/disposal center for more recycling/disposal methods of related products.

4.2 Warranty

Product warranty

VANTRON warrants to its CUSTOMER that the Product manufactured by VANTRON, or its subcontractors will conform strictly to the mutually agreed specifications and be free from defects in workmanship and materials (except that which is furnished by the CUSTOMER) upon shipment from VANTRON. VANTRON's obligation under this warranty is limited to replacing or repairing at its option of the Product which shall, within **24 months** after shipment, effective from invoice date, be returned to VANTRON's factory with transportation fee paid by the CUSTOMER and which shall, after examination, be disclosed to VANTRON's reasonable satisfaction to be thus defective. VANTRON shall bear the transportation fee for the shipment of the Product to the CUSTOMER.

Out-of-Warranty Repair

VANTRON will furnish the repair services for the Product which are out-of-warranty at VANTRON's then-prevailing rates for such services. At customer's request, VANTRON will provide components to the CUSTOMER for non-warranty repair. VANTRON will provide this service as long as the components are available in the market; and the CUSTOMER is requested to place a purchase order up front. Parts repaired will have an extended warranty of 3 months.

Returned Products

Any Product found to be defective and covered under warranty pursuant to Clause above, shall be returned to VANTRON only upon the CUSTOMER's receipt of and with reference to a VANTRON supplied Returned Materials Authorization (RMA) number. VANTRON shall supply an RMA, when required within three (3) working days of request by the CUSTOMER. VANTRON shall submit a new invoice to the CUSTOMER upon shipping of the returned products to the CUSTOMER. Prior to the return of any products by the CUSTOMER due to rejection or warranty defect, the CUSTOMER shall afford VANTRON the opportunity to inspect such products at the CUSTOMER's location and no Product so inspected shall be returned to VANTRON unless the cause for the rejection or defect is determined to be the responsibility of VANTRON. VANTRON shall in turn provide the CUSTOMER turnaround shipment on defective Product within **fourteen (14) working days** upon its receipt at VANTRON. If such turnaround cannot be provided by VANTRON due to causes beyond the control of VANTRON, VANTRON shall document such instances and notify the CUSTOMER immediately.

Appendix Regulatory Compliance Statement

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate this equipment.