

User's Manual



5-Port 10/100/1000T VPN Security Router

▶ VR-100



Copyright

Copyright (C) 2019 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology. This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means, electronic or mechanical including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements and/or changes to this User's Manual at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Compliance Statement

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment 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.

CE mark Warning



The is a class A device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of  electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

Revision

User's Manual of PLANET 5-Port 10/100/1000T VPN Security Router

Model: VR-100

Rev.: 1.0 (September, 2019)

Part No. EM-VR-100_v1.0

Table of Contents

Chapter 1. Product Introduction.....	6
1.1 Package Contents.....	6
1.2 Overview	6
1.3 Topology.....	10
1.4 Features	11
1.5 Product Specifications	13
Chapter 2. Hardware Introduction	15
2.1 Physical Descriptions	15
2.1.1 Front View.....	15
2.1.2 Rear View	15
2.1.3 Diagrams.....	16
2.2 Hardware Installation	17
2.2.1 Desktop Installation	17
2.2.2 Rack Mounting (optional).....	17
Chapter 3. Preparation	20
3.1 Requirements.....	20
3.2 Setting TCP/IP on your PC	21
3.2.1 Windows 7/8	21
3.2.2 Windows 10	25
3.3 Planet Smart Discovery Utility.....	28
Chapter 4. Web-based Management	30
4.1 Introduction	30
4.2 Logging in to the VPN Router	30
4.3 Main Web Page.....	31
4.4 System	33
4.4.1 Wizard.....	34
4.4.2 Dashboard	40
4.4.3 Status.....	41
4.4.4 Statistics.....	42
4.4.5 Connection Status	42
4.4.6 SNMP.....	43
4.5 Network.....	44
4.5.1 WAN.....	45
4.5.2 WAN Advanced.....	46

4.5.3	LAN Setup.....	47
4.5.4	Routing.....	48
4.5.5	WAN IPv6 Setting	50
4.5.6	DHCP.....	50
4.5.7	DDNS.....	52
4.5.8	MAC Address Clone	54
4.6	Security	55
4.6.1	Firewall.....	56
4.6.2	MAC Filtering	58
4.6.3	IP Filtering.....	59
4.6.4	Web Filtering.....	60
4.6.5	Port Forwarding	61
4.6.6	DMZ	62
4.7	VPN 64	
4.6.7	IPsec.....	65
4.6.8	GRE	68
4.6.9	PPTP Server.....	70
4.6.10	L2TP Server.....	72
4.6.11	SSL VPN.....	74
4.6.12	VPN Connection	75
4.7	Maintenance.....	76
4.7.1	Administrator.....	76
4.7.2	Date and Time	77
4.7.3	Saving/Restoring Configuration	78
4.7.4	Upgrading Firmware	79
4.7.5	Reboot / Reset.....	79
4.7.6	Diagnostics	80
Appendix A: DDNS Application		82

Chapter 1. Product Introduction

1.1 Package Contents

The package should contain the following:

- VR-100 x 1
- Quick Installation Guide x 1
- Power Cord x 1
- Feet Pads x 4



Note

If any of the above items are missing, please contact your dealer immediately.

1.2 Overview

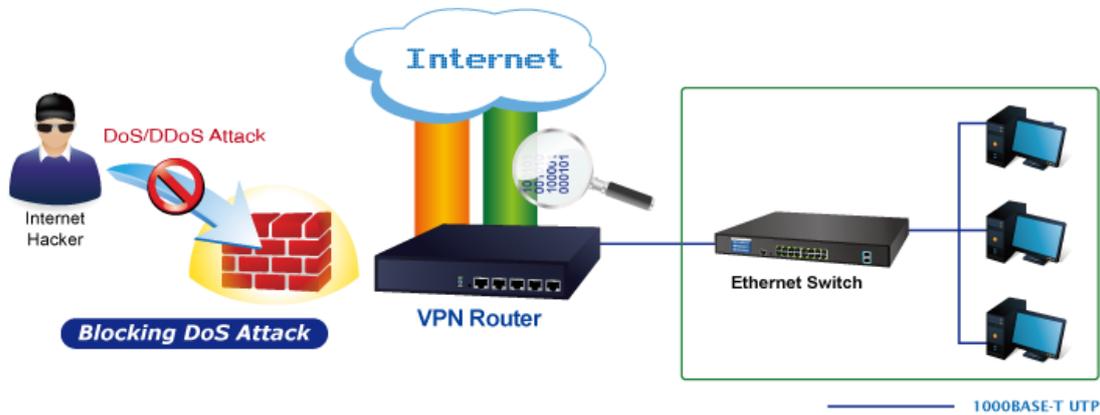
Powerful VPN Security Solution

The innovation of the Internet has created tremendous worldwide opportunities for e-business and information sharing. It has become essential for businesses to focus more on network security issues. The demand for information security has become the primary concern for the enterprises. To fulfill this demand, PLANET has launched the VR-100 VPN Security Router, an all-in-one appliance that carries several main categories across your network security deployments: SPI firewall security protection, policy auditing (Content Filtering, VPN Tunnel and MAC/IP Filtering), and easy management (Setup Wizard, DHCP Server and Dashboard). Furthermore, its Dual-WAN Failover and Outbound Load Balance features can improve the network efficiency while the web-based interface provides friendly and consistent user experience.



Excellent Ability in Threat Defense

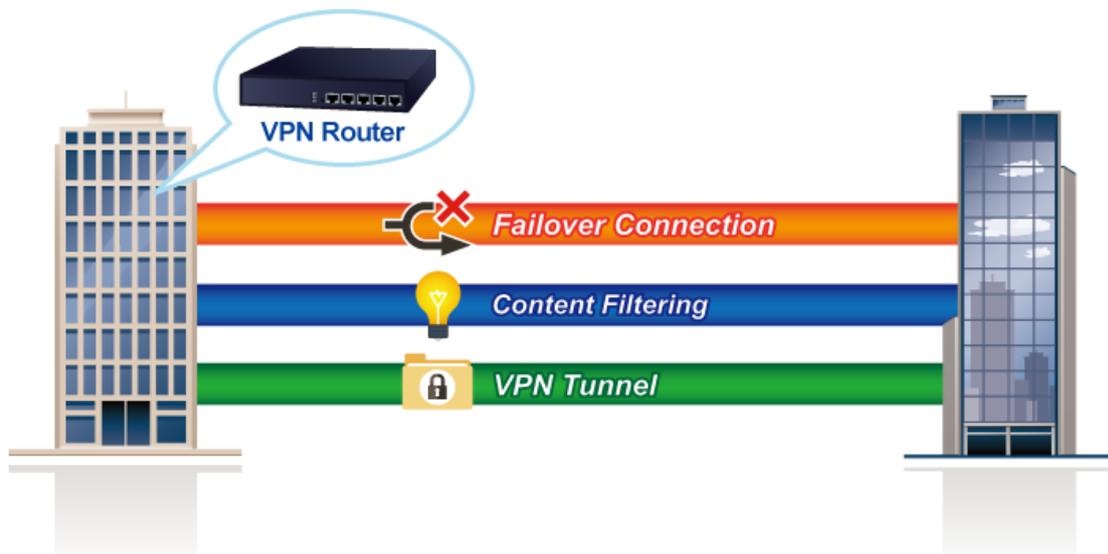
The VR-100 built-in SPI (Stateful Packet Inspection) firewall and Blocking DoS/DDoS attack functions provide high efficiency and extensive protection for your network. Virtual Server and DMZ functions can let you setup servers in the Intranet and still provide services to the Internet users.



Ideal VPN Security Router Solution for SMBs

The VR-100 provides complete data security and privacy for accessing and exchanging most sensitive data, built-in IPSec VPN function with DES/3DES/AES encryption and MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication, and GRE, SSL, PPTP and L2TP server mechanism. The full VPN capability in the VR-100 makes the connection solid secure, more flexible, and more capable.

The VR-100 supports many popular security features including Content Filtering to block specific URL, MAC/IP filtering, outbound load-balancing and more. Furthermore, it provides higher performance with all Gigabit Ethernet interfaces which offer faster speeds for your network applications. The Gigabit user-defined interfaces flexibly fulfill the network requirement nowadays, and the Dual-WAN interfaces enable the VR-100 to support outbound load balancing and WAN fail-over features.



Cybersecurity Network Solution to Minimize Security Risks

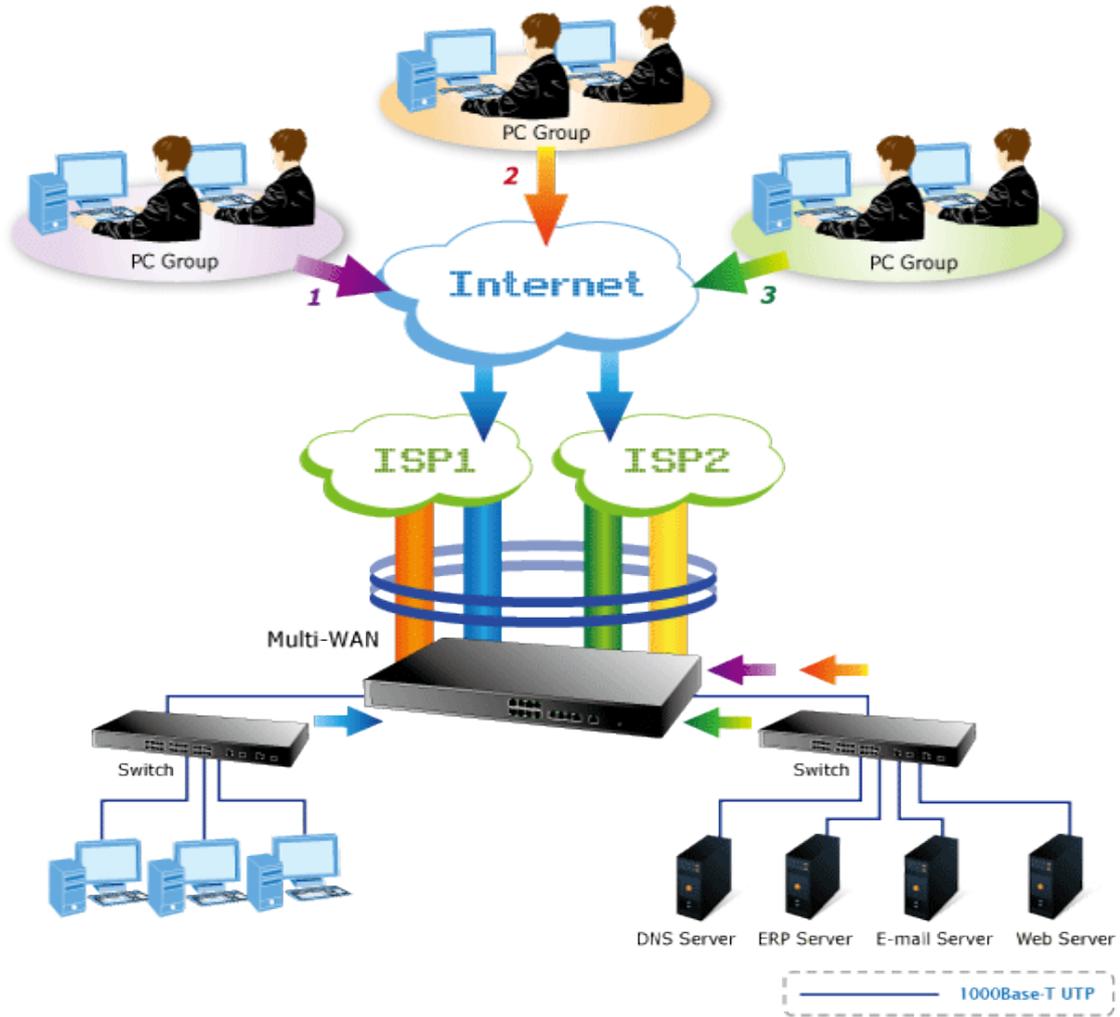
The cybersecurity feature included to protect the switch management in a mission-critical network virtually needs no effort and cost to install. For efficient management, the VR-100 is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the VR-100 offers an easy-to-use, platform independent management and configuration facility. The VR-100 supports SNMP and it can be managed via any management software based on the standard SNMP protocol.

Improving Network Efficiency

The VR-100 has link redundancy, Content Filtering and many more functions to make the entire network system better. It is applicable to the small-scale sector (from 10 to 50 people), using a 9-inch desktop design, with five Gigabit ports (WAN/LAN). The VR-100's economical price with complete cable management features make it an inevitable choice for the next-generation office network load balancer.

The VR-100's built-in Content Filtering feature can automatically resolve the IP address corresponding to all. Users' network can be easily managed by just typing the URL of the websites like Facebook, YouTube and Yahoo.

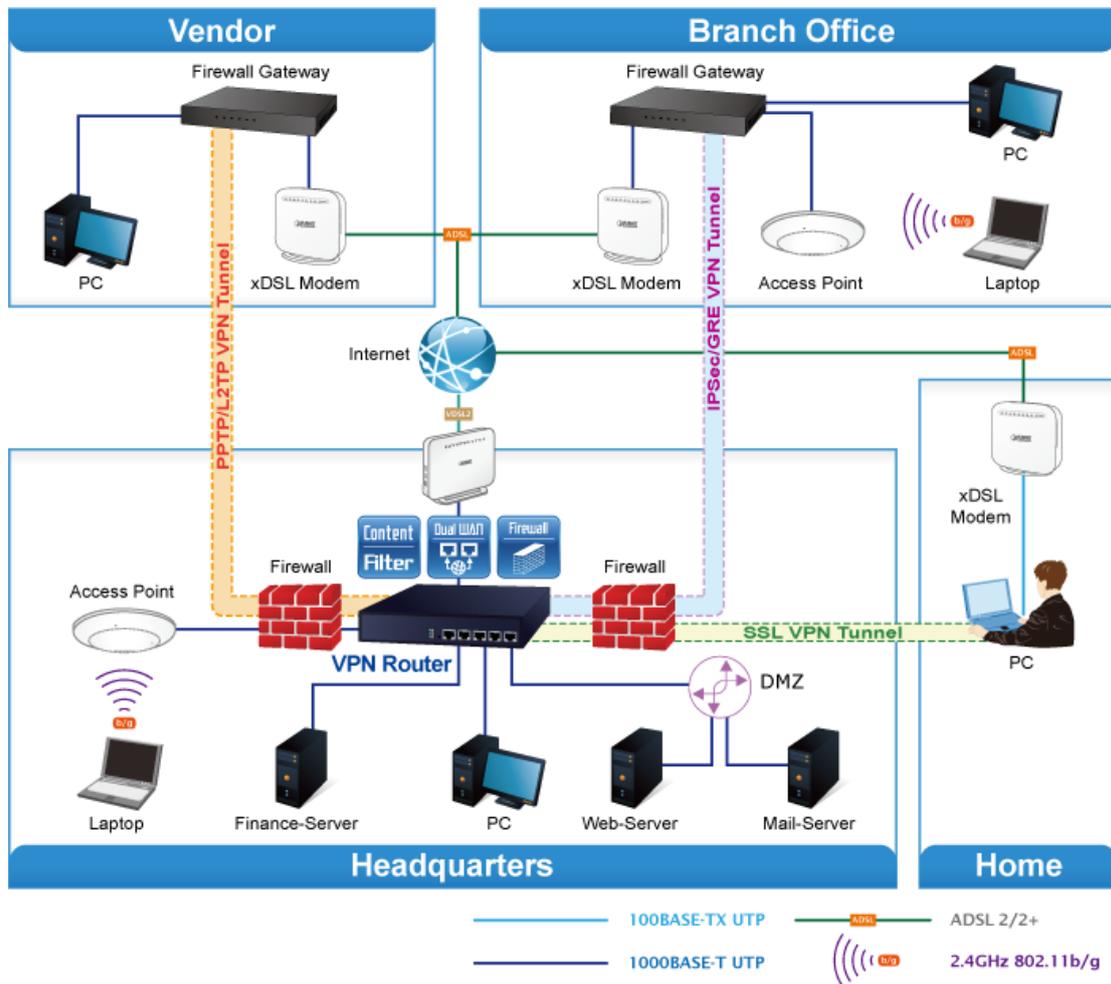
The VR-100 can connect dual WANs with up to two different ISPs. It creates a stable and qualified VPN connection for many important applications such as VoIP, video conferencing and data transmission.



1.3 Topology

PLANET VR-100 VPN security router has an SPI firewall with DoS detection. Through the Content Filtering function, it can easily block the websites like Facebook, YouTube, Gmail, etc. With IPSec/GRE/PPTP/L2TP/SSL VPN solutions, the VR-100 provides secured data communication for branches, vendors, and mobile workers with a flexible way to connect back to the headquarters.

The VR-100 connects dual WANs with up to two different ISPs. It creates a stable and qualified VPN connection for many important applications such as VoIP, video conferencing and data transmission.



1.4 Features

➤ Hardware

- 5 10/100/1000BASE-T RJ45 ports
- 1 undefined Ethernet port (LAN/WAN)
- Dual-WAN function
- 1 USB 3.0 port for system configuration backup and restore
- Reset button
- Desktop installation or rack mounting (optional)
- Fanless design

➤ IP Routing Feature

- Static Route
- Dynamic Route

➤ Firewall Security

- Stateful Packet Inspection (SPI) firewall
- Blocks DoS/DDoS attack
- Content filtering
- MAC/IP filtering
- Blocks SYN/ICMP flooding

➤ VPN Features

- IPSec (Host to Host)/GRE/PPTP server/L2TP/SSL(Open VPN)
- Max. Connection Tunnel Entries: 60 VPN tunnels,
- Encryption methods: DES, 3DES, AES, AES-128/192/256
- Authentication methods: MD5, SHA-1, SHA-256, SHA-384, SHA-512

➤ Networking

- Outbound load balancing
- Failover for dual-WAN
- Static IP/DHCP client for WAN
- Protocols: TCP/IP, UDP, ARP, IPv4, IPv6
- Port forwarding
- DMZ
- SNMP
- DHCP server/NTP client

- MAC address clone
- DDNS: PLANET DDNS, PLANET Easy DDNS, DynDNS and No-IP
- Cybersecurity

➤ **Others**

- Setup wizard
- Dashboard for real time system overview
- Supported access by HTTP or HTTPS
- Auto reboot
- PLANET Smart Discovery utility/UNI-NMS supported

1.5 Product Specifications

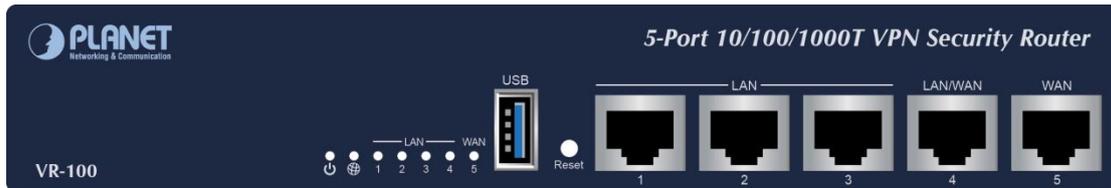
Product	VPN security router
Model	VR-100
Hardware	
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including <ul style="list-style-type: none"> ■ 3 LAN ports ■ 1WAN port ■ 1 LAN/WAN port
USB Port	1 USB 3.0 port for system configuration backup and restore
Reset Button	Reset to factory default
Thermal Fan	Fanless
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green)
Installation	Desktop installation or rack mounting (optional)
Power Requirements	100-240V AC, 1A max.
Power Consumption	13W max.
Weight	0.85kg
Dimensions (W x D x H)	215.2 x 135 x 42.6 mm
Software	
Management	Web browser
Operation Mode	Routing mode
Routing Protocol	Static route: 32 Dynamic route: 4096
NAT Throughput	Max. 900Mbps
Firewall Security	Stateful packet inspection (SPI) Blocks DoS/DDoS attack
Outbound Load Balancing	Supported algorithms: Weight
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, SNMP,
Content Filtering	MAC filtering IP filtering Web filtering
Log	System Operation Log

Others	<p>Outbound load balancing</p> <p>Failover for dual-WAN</p> <p>Port forwarding</p> <p>DMZ</p> <p>Cybersecurity</p> <p>Dashboard</p> <p>Setup wizard</p> <p>Auto reboot</p> <p>PLANET Smart Discovery utility/UNI-NMS supported</p>
VPN	
VPN Function	<ul style="list-style-type: none"> ■ IPsec (Host to Host) ■ GRE ■ PPTP server ■ L2TP ■ SSL (Open VPN)
VPN Tunnels	Max. 60
VPN Throughput	Max. 60Mbps
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm
Standards Conformance	
Regulatory Compliance	CE, FCC
Environment Specifications	
Operating	<p>Temperature: 0 ~ 50 degrees C</p> <p>Relative Humidity: 5 ~ 95% (non-condensing)</p>
Storage	<p>Temperature: -10 ~ 60 degrees C</p> <p>Relative Humidity: 5 ~ 95% (non-condensing)</p>
Standard Accessories	
Packet Contents	<ul style="list-style-type: none"> ■ VR-100 x 1 ■ Quick Installation Guide x 1 ■ Power Cord x 1 ■ Feet Pads x 4

Chapter 2. Hardware Introduction

2.1 Physical Descriptions

2.1.1 Front View



LED		
PWR		Lights up when the power is on.
Internet	Green	Lights up when the router connects to internet successfully.
Port 1-5		“Steady on” indicates the port is connected to other network device. “Blink” to indicate there is traffic on the port.
Ports		
USB Port	USB 3.0 port for system configuration backup and restoration.	
Reset Button	Power on the device and press the reset button for ten seconds to restore it to factory default settings.	
Port 1-3	It is a LAN port for connecting to a switch.	
Port 4	Default is LAN port. It can be defined as LAN port or WAN port.	
Port 5	It is a WAN port for connecting to a perimeter router.	

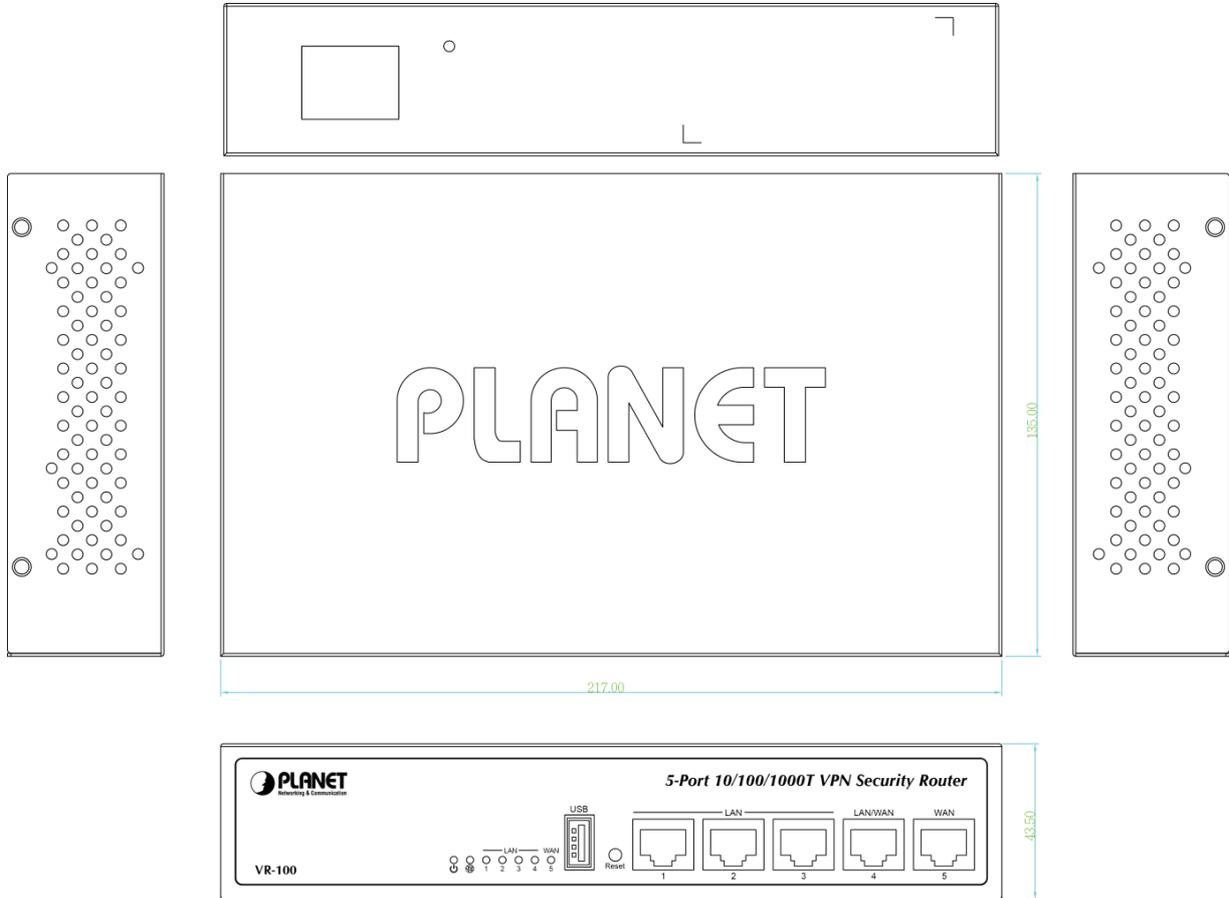
2.1.2 Rear View



Interface	
AC Power Receptacle	For compatibility with electrical outlet standard in most areas of the world, the device’s power supply automatically adjusts to line power in the range of 100-240V AC and 50/60Hz. Plug the female end of the power cord firmly into the receptacle on the rear

panel of the device and the other end into an electrical outlet, and the power will be ready.

2.1.3 Diagrams



Unit: mm

2.2 Hardware Installation

2.2.1 Desktop Installation

To install the VR-100 on desktop, simply follow the following steps:

Step 1: Place the device on desktop.

Step 2: Keep enough ventilation space between the device and the surrounding objects.



When choosing a location, please keep in mind the environmental restrictions should be under the specifications of the VR-100.

Step 3: Connect your device to hub / switch.

A. Connect one end of a standard network cable to the LAN port (port 1) of the device.

B. Connect the other end of the cable to the hub / switch.



The UTP Category 5, 5e or 6 network cabling with RJ45 tips is recommended.

Step 4: Connect your device to internet.

A. Connect one end of a standard network cable to the WAN port (port 5) of the device.

B. Connect the other end of the cable to the LAN port of ISP network device (such as a modem).



If there is only one line connected to the outer network in your network environment, it is suggested that you use WAN port (port 5).

Step 5: Power on the device. When the device receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting (optional)

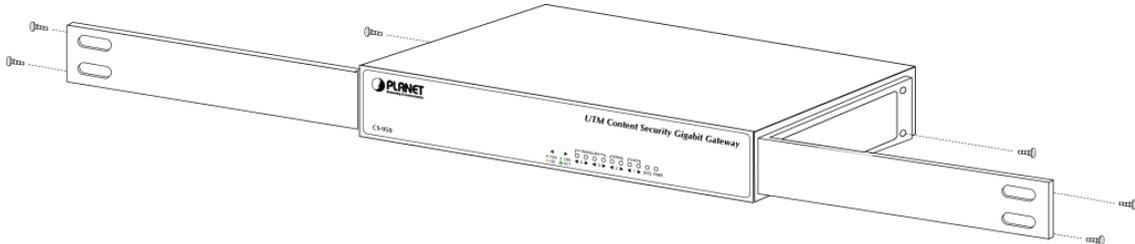
If you need install the VR-100 in a 19-inch standard rack, please contact your dealer first and order the accessories -- **RKE-10B**, a rack mounting kit not included in the package.

Please follow the instructions described below.

(The device shown on this chapter is just a representation of the said device.)

Step 1: Place your device on a hard flat surface, with the front panel positioned towards your front side.

Step 2: Attach a rack-mount bracket to each side of the device with supplied screws attached to the package. In the picture below, it shows how to attach brackets to one side of the device.

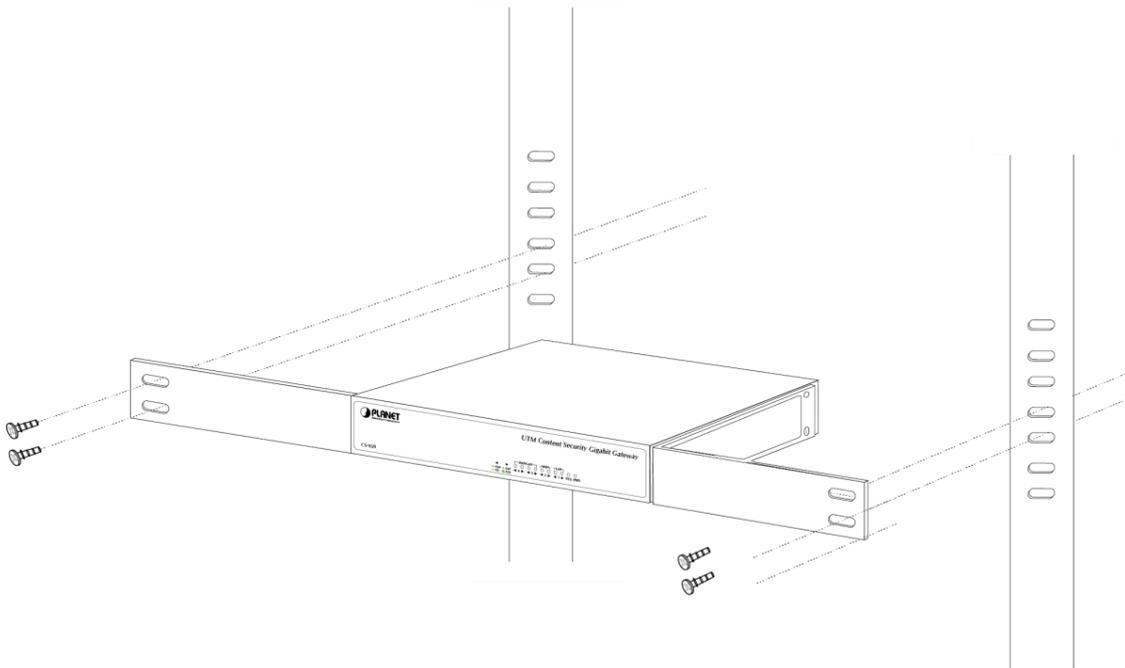


You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step 3: Secure the brackets tightly.

Step 4: Follow the same steps to attach the second bracket to the opposite side.

Step 5: After the brackets are attached to the device, use suitable screws to securely attach the brackets to the rack, as shown in the picture below.



The width of the rack should be at least 453 mm.

Step 6: Proceed with Steps 4 and 5 in Section 2.2.1 Desktop Installation to connect the network cabling and power on the device.

Chapter 3. Preparation

Before getting into the device's web UI, user has to check the network setting and configure PC's IP address.

3.1 Requirements

User is able to confirm the following items before configuration:

1. Please confirm the network is working properly; it is strongly suggested to test your network connection by connecting your computer directly to ISP.
2. Suggested operating systems: Windows 7 / 8 / 10.
3. Recommended web browsers: IE / Firefox / Chrome.

3.2 Setting TCP/IP on your PC

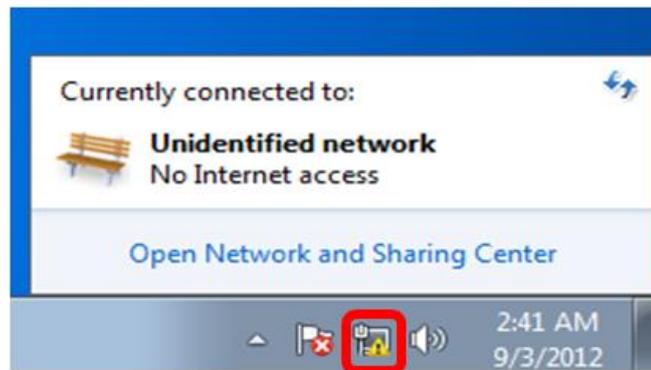
The default IP address of the VR-100 is 192.168.1.1, and the DHCP Server is on. Please set the IP address of the connected PC as DHCP client, and the PC will get IP address automatically from the VR-100.

Please refer to the following to set the IP address of the connected PC.

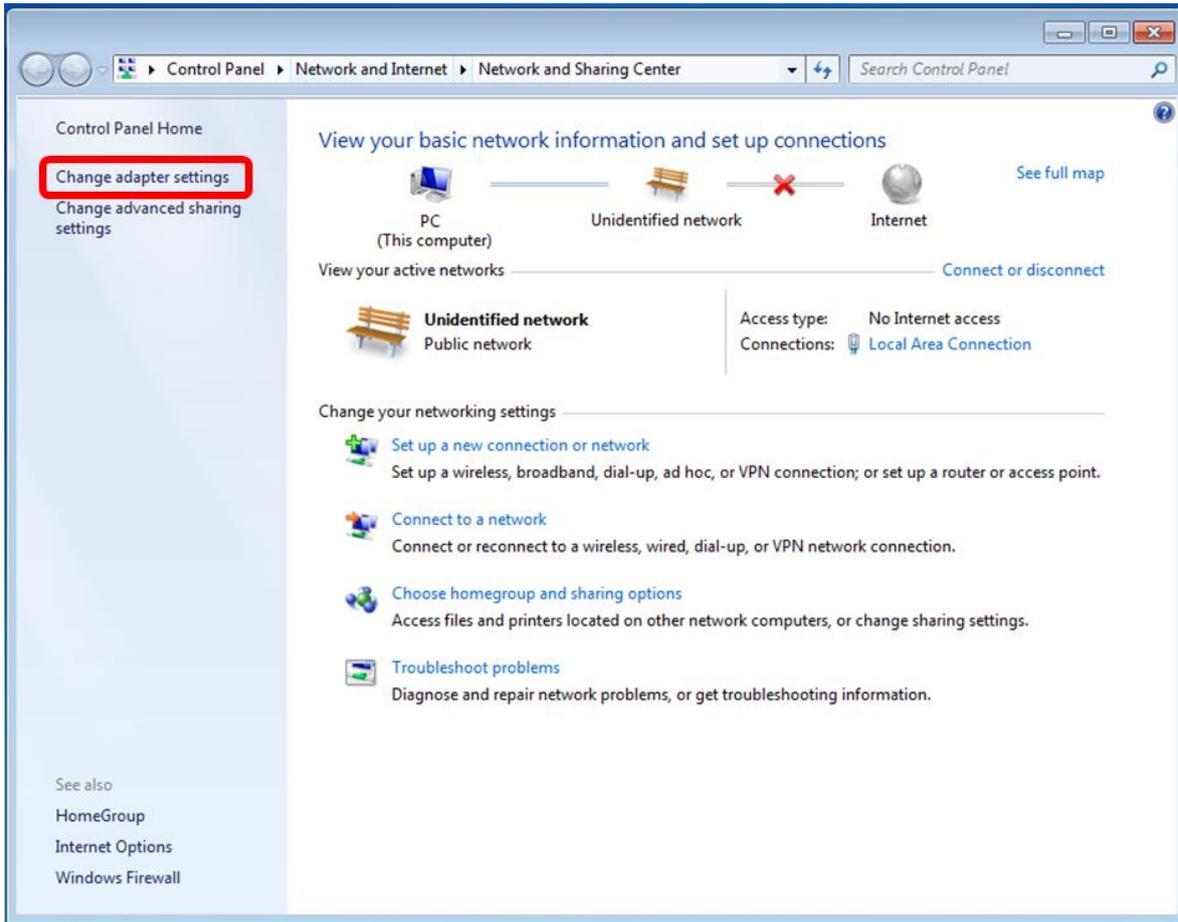
3.2.1 Windows 7/8

If you are using Windows 7/8, please refer to the following:

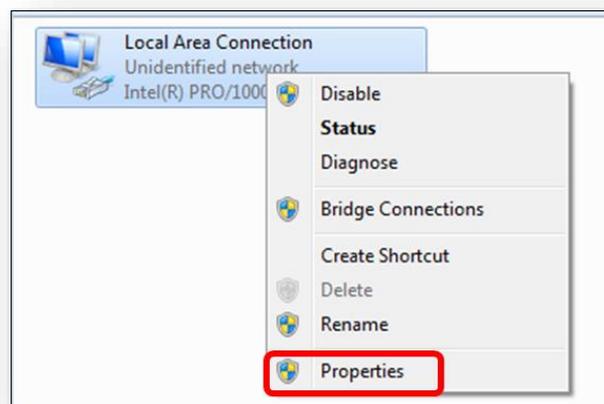
1. Click on the network icon from the right side of the taskbar and then click on “Open Network and Sharing Center”.



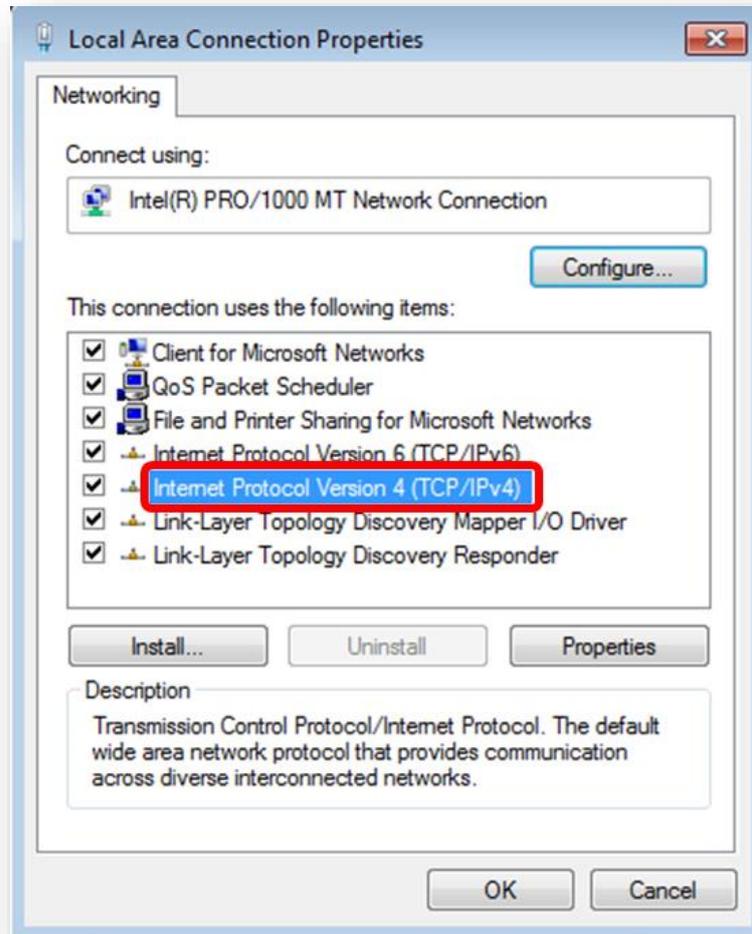
2. Click "Change adapter settings".



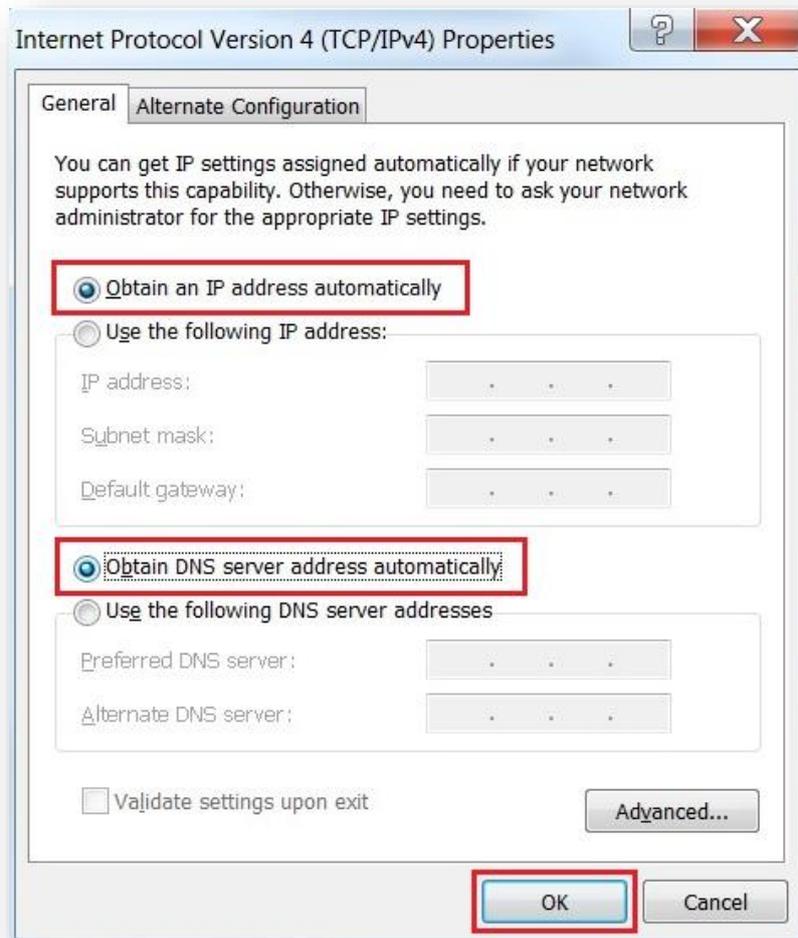
3. Right-click on the Local Area Connection and select Properties.



4. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).



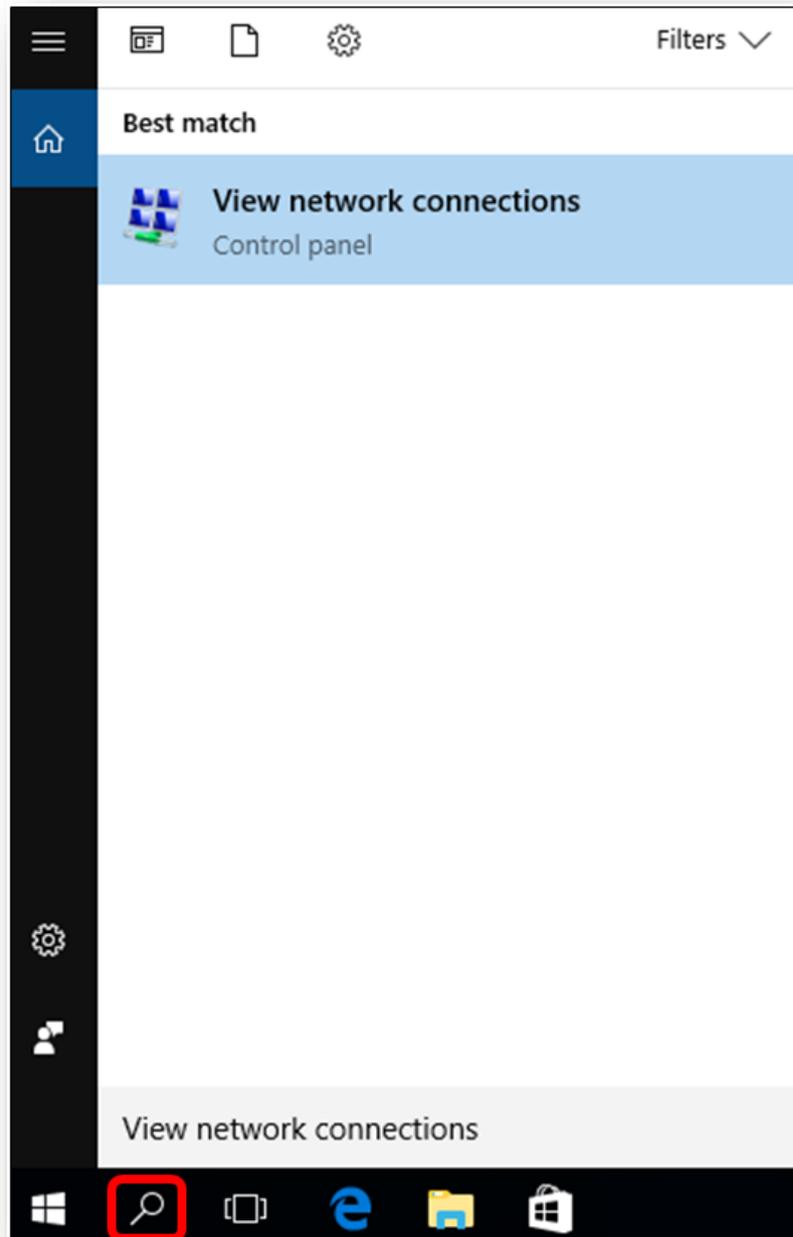
5. Select "Use the following IP address" and "Obtain DNS server address automatically", and then click the "OK" button.



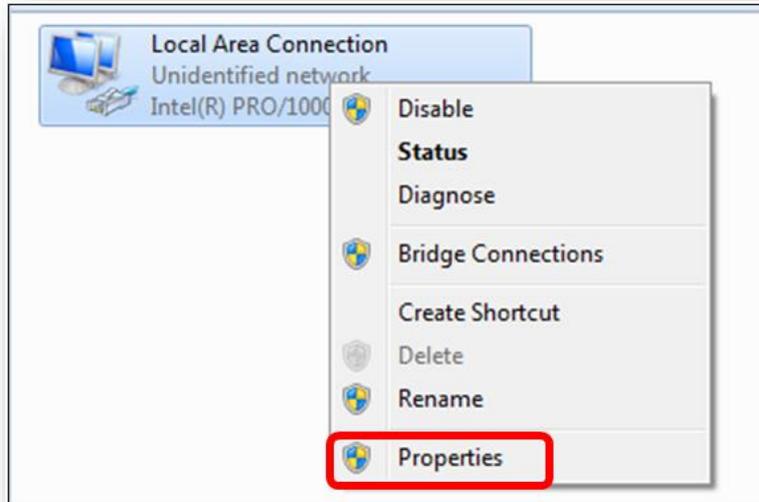
3.2.2 Windows 10

If you are using Windows 10, please refer to the following:

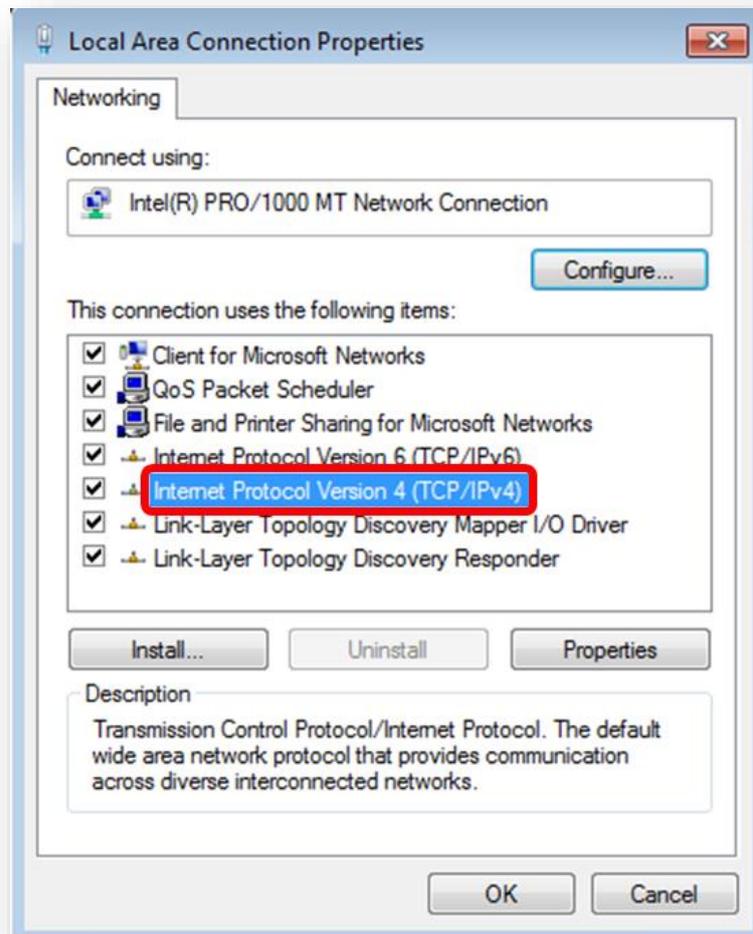
1. In the search box on the taskbar, type “View network connections”, and then select View network connections at the top of the list.



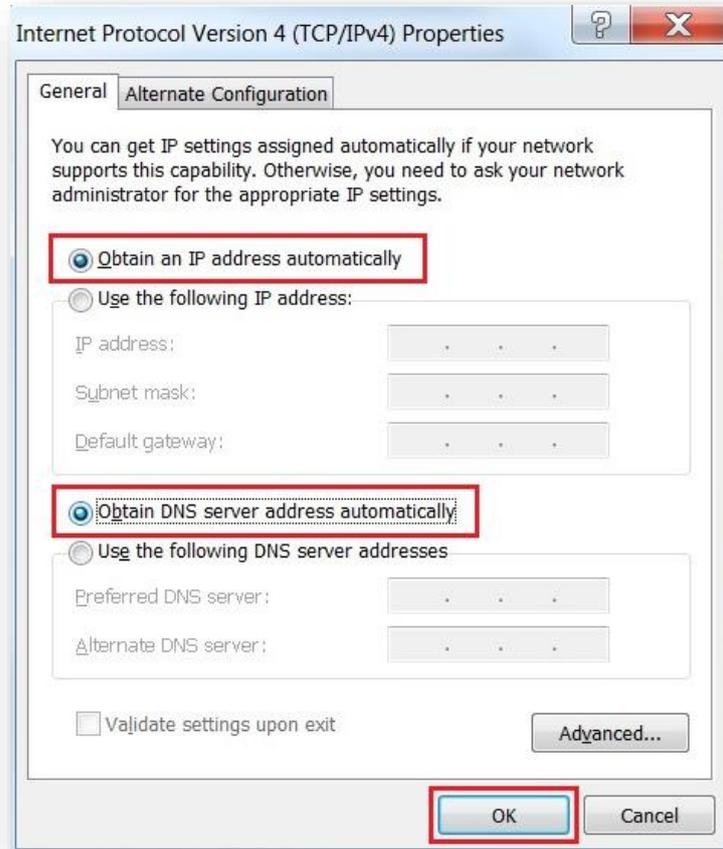
2. Right-click on the Local Area Connection and select Properties.



3. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).



4. Select "Use the following IP address" and "Obtain DNS server address automatically", and then click the "OK" button.



3.3 Planet Smart Discovery Utility

For easily listing the router in your Ethernet environment, the search tool -- Planet Smart Discovery Utility -- is an ideal solution.

The following installation instructions are to guide you to running the Planet Smart Discovery Utility.

1. Download the Planet Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

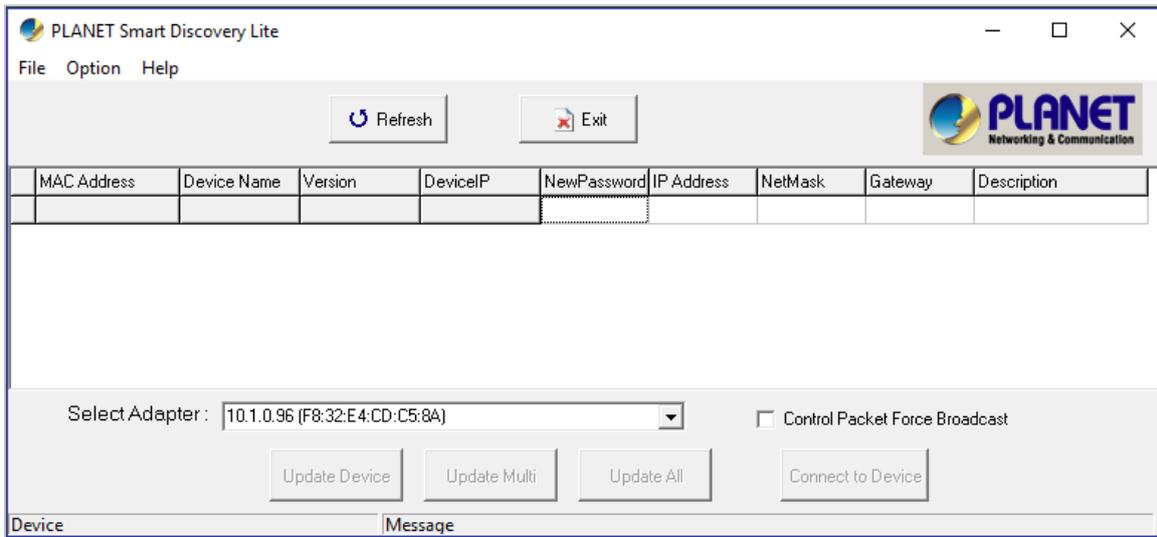


Figure 3-1-6: Planet Smart Discovery Utility Screen



If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the “**Select Adapter**” tool.

3. Press the “**Refresh**” button for the currently connected devices in the discovery list as the screen shows below:

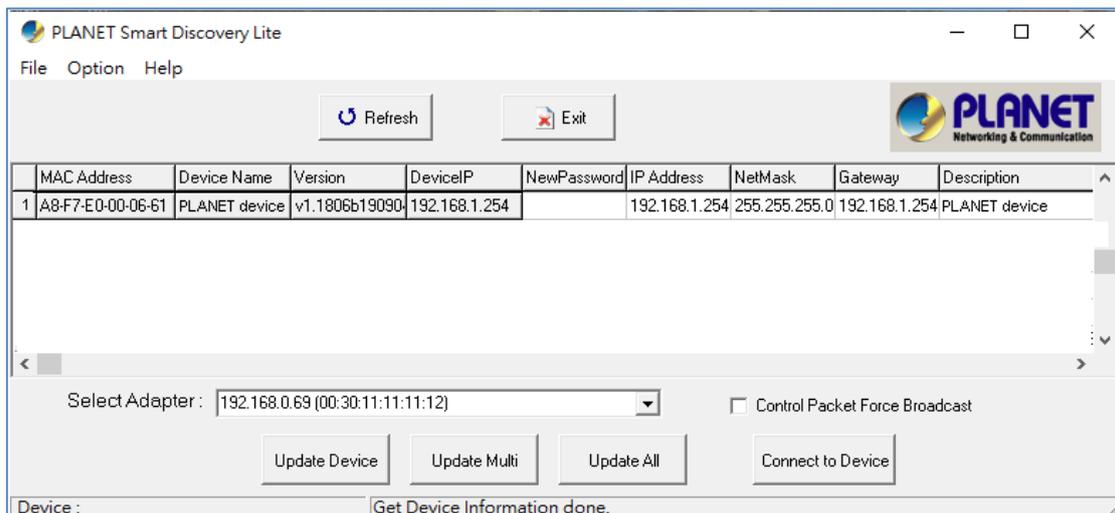


Figure 3-1-7: Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.
2. After setup is completed, press the “**Update Device**”, “**Update Multi**” or “**Update All**” button to take effect. The functions of the 3 buttons above are shown below:
 - **Update Device:** use current setting on one single device.
 - **Update Multi:** use current setting on choose multi-devices.
 - **Update All:** use current setting on whole devices in the list.

The same functions mentioned above also can be found in “**Option**” tools bar.

3. To click the “**Control Packet Force Broadcast**” function, it allows you to assign a new setting value to the device under a different IP subnet address.
4. Press the “**Connect to Device**” button and the Web login screen appears.

Press the “**Exit**” button to shut down the Planet Smart Discovery Utility.

Chapter 4. Web-based Management

This chapter provides setup details of the device's Web-based Interface.

4.1 Introduction

The device can be configured with your Web browser. Before configuring, please make sure your PC is under the same IP segment with the device.

4.2 Logging in to the VPN Router

Refer to the steps below to configure the VPN router:

- Step 1.** Connect the IT administrator's PC and VPN router's LAN port (port 1) to the same hub / switch, and then launch a browser to link the management interface address which is set to **http://192.168.1.1** by default.



The DHCP server of the VPN router is enabled. Therefore, the LAN PC will get IP from the VPN router. If user needs to set IP address of LAN PC manually, please set the IP address within the range between 192.168.1.2 and 192.168.1.254 inclusively, and assigned the subnet mask of 255.255.255.0.

- Step 2.** The browser prompts you for the login credentials. (Both are “**admin**” by default.)

Default IP address: **192.168.1.1**

Default user name: **admin**

Default password: **admin**



Administrators are strongly suggested to change the default admin and password to ensure system security.

4.3 Main Web Page

After a successful login, the main web page appears. The web main page displays the web panel, main menu, function menu, and the main information in the center.

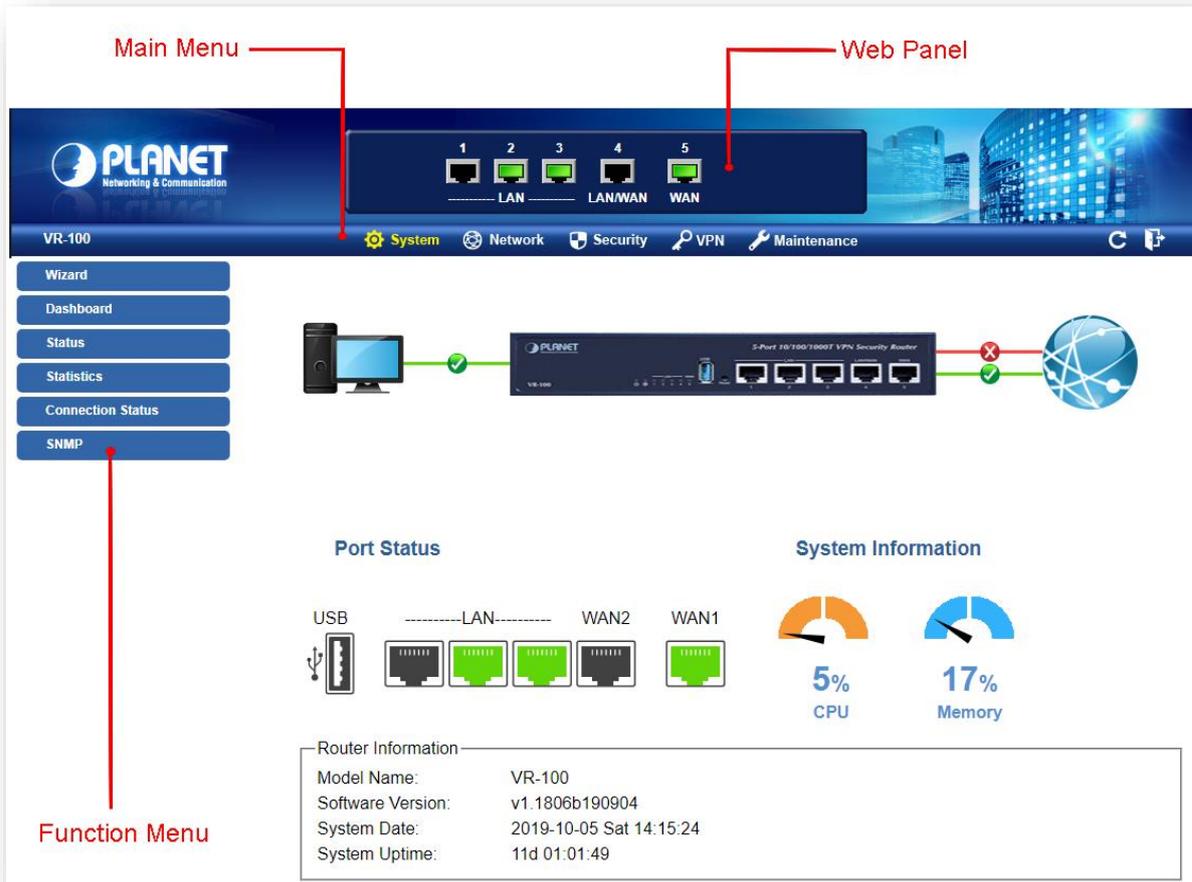


Figure 4-: Main Web Page

■ Web Panel

The web panel displays an image of the device's ports as shown in Figure 4-2.



Figure 4-2: Web Panel

Object	Icon	Function
LAN		To indicate the LAN with the RJ45 plug-in.
		To indicate network data is sending or receiving

■ **Main Menu**

The main menu displays the product name, function menu, and main information in the center. Via the Web management, the administrator can set up the device by selecting the functions those listed in the function menu and button as shown in [Figures 4-3 and 4-4](#).



Figure 4-3: Function Menu

Object	Description
System	Provides System information of the router.
Network	Provides WAN, LAN and network configuration of the router.
Security	Provides Firewall and security configuration of the router.
VPN	Provides VPN configuration of the router.
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the router.



Figure 4-4: Function Button

Object	Description
	Click the " Refresh button " to refresh the current web page.
	Click the " Logout button " to log out the web UI of the router.

4.4 System

Use the System menu items to display and configure basic administrative details of the router. The System menu shown in [Figure 4-5](#) provides the following features to configure and monitor system.

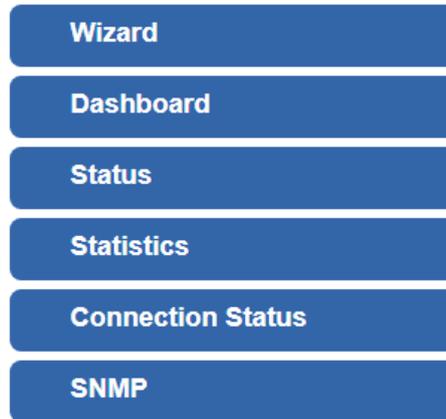


Figure 4-5: System Menu

Object	Description
Wizard	The Wizard will guide the user to configuring the router easily and quickly.
Dashboard	The overview of system information includes connection, port, and system status.
Status	Display the status of the system, LAN and WAN.
Statistics	Display statistics information of network traffic of LAN and WAN.
Connection Status	Display the DHCP client table and the ARP table.
SNMP	Display SNMP system information.

4.4.1 Setup Wizard

The Wizard will guide the user to configuring the router easily and quickly. There are different procedures in different operation modes. According to the operation mode you switch to, please follow the instructions below to configure the router via **Setup Wizard** as shown in [Figure 4-6](#).



Figure 4-6: Setup Wizard

Step 1: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in [Figure 4-7](#).

The screenshot shows the "STEP 1 - Network Interface LAN" configuration screen. At the top, there is a progress bar with four steps: 1 (LAN), 2 (WAN), 3 (Security Settings), and 4 (Setup Completed). Step 1 is active. Below the progress bar, there are several configuration fields:

- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- DHCP Server:
- Start IP Address: 192.168.1.100
- Maximum DHCP Users: 101

At the bottom right, there are "Cancel" and "Next" buttons.

Figure 4-7: Setup Wizard – LAN Configuration

Object	Description
IP Address	Enter the IP address of your router. The default is 192.168.1.1.
Subnet Mask	An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
DHCP Server	By default, the DHCP Server is enabled. If user needs to disable the function, please uncheck the box.

Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the router.
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the router will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
Next	Press this button to the next step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Step 2: WAN Interface

The router supports two access modes on the WAN side shown in [Figure 4-8](#)

STEP 2 - Network Interface WAN

1 LAN — 2 WAN — 3 Security Settings — 4 Setup Completed

WAN1 | WAN2

Connection Type: DHCP ▾

IP Address:

Netmask:

Default Gateway:

DNS Server 1:

DNS Server 2:

Cancel Previous Next

Figure 4-8: Setup Wizard – WAN 1 Configuration

WAN1 | **WAN2**

WAN Enable Disable

Connection Type: DHCP

IP Address: []

Netmask: []

Default Gateway: []

DNS Server 1: []

DNS Server 2: []

Figure 4-9: Setup Wizard – WAN 2 Configurations

Mode 1 -- Static IP

Select **Static IP Address** if all the Internet port's IP information is provided to you by your ISP. You will need to enter the **IP Address**, **Netmask**, **Default Gateway** and **DNS Server** provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format. The setup is shown in [Figure 4-10](#).

WAN1 | **WAN2**

Connection Type: Static

IP Address: 210.66.155.1

Netmask: 255.255.255.0

Default Gateway: 210.66.155.194

DNS Server 1: 168.95.1.1

DNS Server 2: 8.8.8.8

Figure 4-10: WAN Interface Setup – Static IP Setup

Object	Description
IP Address	Enter the IP address assigned by your ISP.
Netmask	Enter the Netmask assigned by your ISP.
Default Gateway	Enter the Gateway assigned by your ISP.
DNS Server	The DNS server information will be supplied by your ISP.

Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Mode 2 -- DHCP Client

Select DHCP Client to obtain IP Address information automatically from your ISP. The setup is shown in [Figure 4-11](#).

Figure 4-11: WAN Interface Setup – DHCP Setup

Step 3: Security Setting

Set up the Security Settings as shown in [Figure 4-12](#).

STEP 3 - Security Settings

1 LAN 2 WAN 3 Security Settings 4 Setup Completed

SPI Firewall Enable Disable

Block SYN Flood Enable Disable

Block ICMP Flood Enable Disable

Block WAN Ping Enable Disable

Remote Management Enable Disable

Cancel Previous Next

Figure 4-12: Setup Wizard –Security Setting

Object	Description
SPI Firewall	<p>The SPI Firewall prevents attack and improper access to network resources.</p> <p>The default configuration is enabled.</p>
Block SYN Flood	<p>SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on.</p> <p>The default configuration is enabled.</p>
Block ICMP Flood	<p>ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack.</p> <p>The default configuration is disabled.</p>
Block WAN Ping	<p>Enable the function to allow the Ping access from the Internet network.</p> <p>The default configuration is disabled.</p>
Remote Management	<p>Enable the function to allow the web server access of the router from the Internet network.</p> <p>The default configuration is disabled.</p>
Next	<p>Press this button for the next step.</p>
Previous	<p>Press this button for the previous step.</p>
Cancel	<p>Press this button to undo any changes made locally and revert to previously saved values.</p>

Step 4: Setup Completed

The page will show the summary of LAN, WAN and Security settings as shown in [Figure 4-13](#).

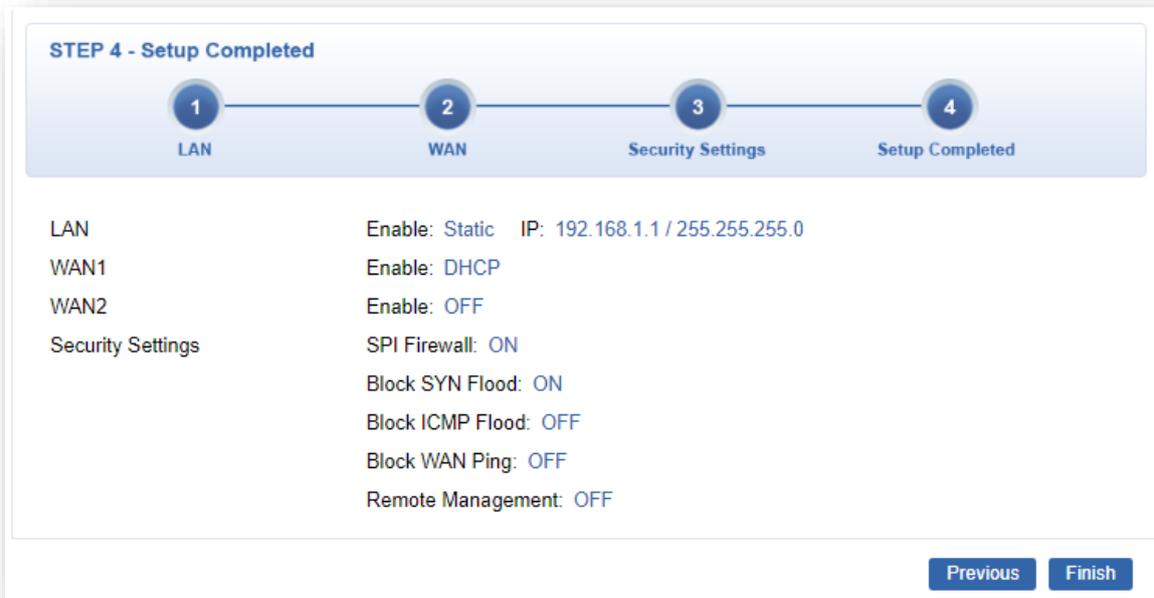


Figure 4-13: Setup Wizard –Setup Completed

Object	Description
Finish	Press this button to save and apply changes.
Previous	Press this button for the previous step.

4.4.2 Dashboard

The dashboard provides an overview of system information including connection, port, and system status as shown in Figure 4-14.

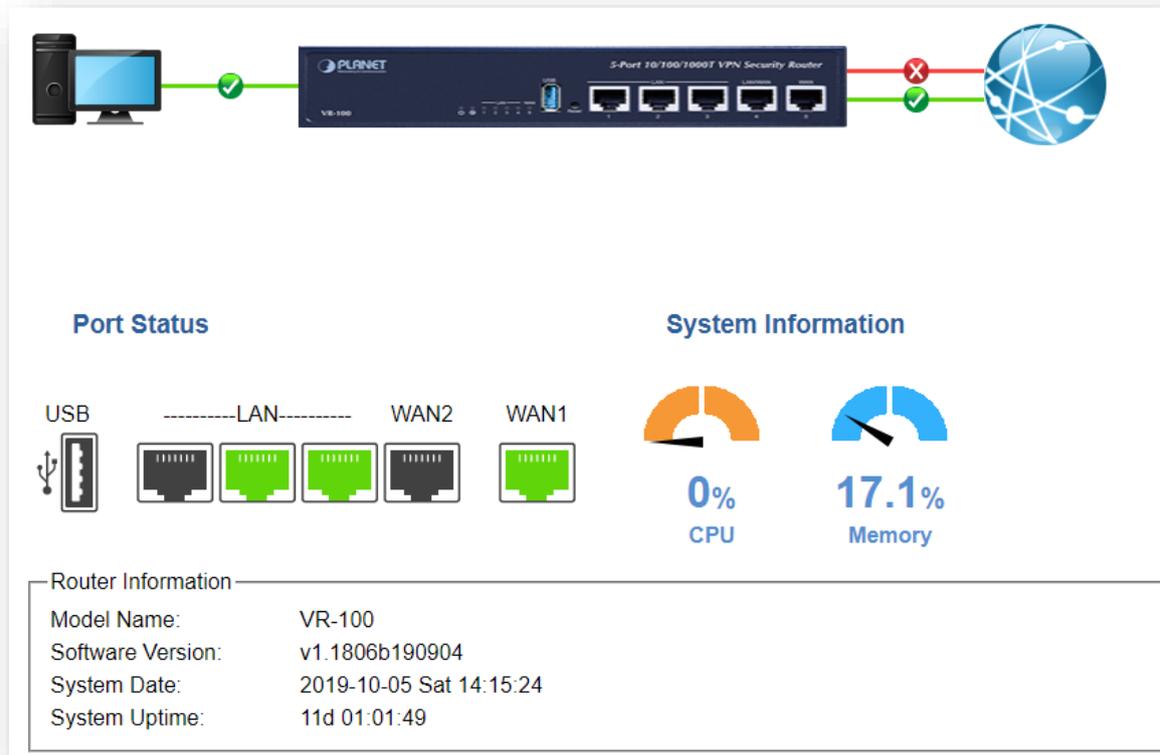


Figure 4-14: Dashboard

WAN/LAN Connection Status

Object	Description
	The status means WAN is connected to Internet and LAN is connected.
	The status means WAN is disconnected to Internet and LAN is connected.
	The status means WAN is connected to Internet and LAN is disconnected.

Port Status

Object	Description
	Ethernet port is in use.

	Ethernet port is not in use.
	USB port is in use.
	USB port is not in use.

System Information

Object	Description
CPU	Display the CPU loading
Memory	Display the memory usage

4.4.3 Status

This page displays system information as shown in [Figure 4-15](#).

Router Information	
Model Name	VR-100
Firmware Version	v1.1806b190904
Current Time	2019-01-30 Wed 20:21:45
Running Time	0d 00:00:57

WAN1	
MAC Address	A8:F7:E0:00:06:62
Connection Type	DHCP
IP Address	192.168.1.189
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

LAN	
MAC Address	A8:F7:E0:00:06:61
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Service	Enable
DHCP Start IP Address	192.168.1.100
DHCP End IP Address	192.168.1.200
Max DHCP Clients	101

Figure 4-15: Status

4.4.4 Statistics

This page displays the number of packets that pass through the router on the WAN and LAN. The statistics are shown in [Figure 4-16](#).

WAN1	
Sent Packets	223
Sent Bytes	198984
Received Packets	2008
Received Bytes	385555

LAN	
Sent Packets	7
Sent Bytes	746
Received Packets	221
Received Bytes	15363

Figure 4-16: Statistics

4.4.5 Connection Status

The page will show the DHCP Table and ARP Table. .

DHCP Table			
Name	IP Address	MAC Address	Expiration Time

ARP Table			
IP Address	MAC Address		ARP Type
8.8.8.8	00:00:00:00:00:00		unknow
208.67.222.222	00:00:00:00:00:00		unknow
8.8.8.8	00:00:00:00:00:00		unknow
208.67.222.222	00:00:00:00:00:00		unknow
192.168.1.18	00:00:00:00:00:00		unknow
192.168.1.69	00:30:11:11:11:12		dynamic
192.168.1.69	00:30:11:11:11:12		dynamic

Figure 4-17: Connection Status

4.4.6 SNMP

This page provides SNMP setting of the router as shown in [Figure 4-18](#).

SNMP

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Read Community	<input type="text" value="public"/>
Write Community	<input type="text" value="private"/>

System Identification

System Name	<input type="text" value="VR-100"/>
System Location	<input type="text"/>
System Contact	<input type="text" value="sales@planet.com.tw"/>

Figure 4-18: SNMP

Object	Description
Enable SNMP	Disable or enable the SNMP function. The default configuration is enabled.
Read/Write Community	Allows entering characters for SNMP Read/Write Community of the router.
System Name	Allows entering characters for system name of the router.
System Location	Allows entering characters for system location of the router.
System Contact	Allows entering characters for system contact of the router.
Apply Settings	Press this button to save and apply changes.
Cancel Changes	Press this button to undo any changes made locally and revert to previously saved values.

4.5 Network

The Network function provides WAN, LAN and network configuration of the router as shown in [Figure 4-19](#).

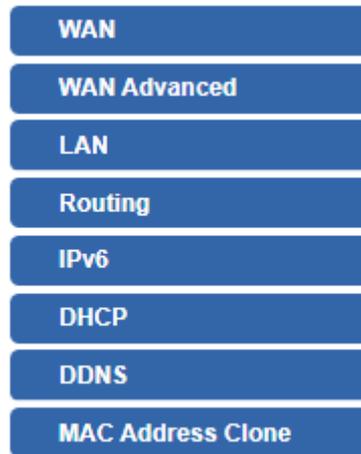


Figure 4-19: Network Menu

Object	Description
WAN Setup	Allows setting WAN interface.
WAN Advanced	Allows setting WAN Advanced settings.
LAN Setup	Allows setting LAN interface.
Routing	Allows setting Route.
IPv6	Allows setting IPv6 WAN interface.
DHCP	Allows setting DHCP Server.
DDNS	Allows setting DDNS and PLANET DDNS.
MAC Address Clone	Allows setting WAN MAC Address Clone.

4.5.1 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the router as shown in [Figure 4-20](#). Here you may select the access method by clicking the item value of WAN access type.

WAN1

Connection Type	<input type="text" value="DHCP"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

WAN2

WAN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection Type	<input type="text" value="DHCP"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

Figure 4-20: WAN

Object	Description
	Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.
WAN Access Type	<p>Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP.</p> <p>Static</p> <p>Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format.</p> <p>IP Address</p> <p>Enter the IP address assigned by your ISP.</p>

Object	Description
	<p>Netmask Enter the Subnet Mask assigned by your ISP.</p> <p>Gateway Enter the Gateway assigned by your ISP.</p> <p>DNS Server The DNS server information will be supplied by your ISP.</p>
DHCP	Select DHCP Client to obtain IP Address information automatically from your ISP.



WAN IP, whether obtained automatically or specified manually, should NOT be on the same IP net segment as the LAN IP; otherwise, the router will not work properly. In case of emergency, press the hardware-based "Reset" button.

4.5.2 WAN Advanced

This page is used to configure the advanced parameters for Internet area network which connects to the WAN port of your router as shown in [Figure 4-21](#). Here you may change the setting for Load Balance Weight, Detect Interval, Detect Link Up Threshold, etc...

WAN1

Load Balance Weight	<input type="text" value="3"/> ▾
External Connection Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Detect Interval	<input type="text" value="5"/> Seconds
Detect Link Up Threshold	<input type="text" value="8"/> Time(s)
Detect Link Down Threshold	<input type="text" value="3"/> Time(s)
Custom Detect Host 1	<input type="text" value="8.8.8.8"/>
Custom Detect Host 2	<input type="text" value="208.67.222.222"/>

WAN2

Load Balance Weight	<input type="text" value="2"/> ▾
External Connection Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Detect Interval	<input type="text" value="5"/> Seconds
Detect Link Up Threshold	<input type="text" value="8"/> Time(s)
Detect Link Down Threshold	<input type="text" value="3"/> Time(s)
Custom Detect Host 1	<input type="text" value="8.8.8.8"/>
Custom Detect Host 2	<input type="text" value="208.67.222.222"/>

Figure 4-21: LAN Setup

Object	Description
Load Balance Weight	Load Balance Weight allows you to set a relative weight (from 1 - 10) for each WAN port.
External Connection Detection	Enable to detect the status of WAN connection.
Detect Interval	Set the detect interval as you need. The recommended value is 5 (default).
Detect Link Up Threshold	Set the times for detecting link up. The recommended value is 8 (default).
Detect Link Down Threshold	Set the times for detecting link down. The recommended value is 3 (default).
Custom Detect Host	The host is used to check whether the internet connection is alive or not.

4.5.3 LAN Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your router as shown in [Figure 4-22](#). Here you may change the settings for IP address, subnet mask, DHCP, etc.

LAN Configuration

IP Address	<input style="width: 90%;" type="text" value="192.168.1.1"/>
Netmask	<input style="width: 90%;" type="text" value="255.255.255.0"/>

Apply Settings
Cancel Changes

Figure 4-22: LAN Setup

Object	Description
IP Address	The LAN IP address of the router and default is 192.168.1.1 .
Net Mask	Default is 255.255.255.0 .

4.5.4 Routing

Please refer to the following sections for the details as shown in [Figures 4-23 and 24](#).

Routing config list							
Number	Type	Destination	Netmask	Gateway	Interface	Comment	Action
Current Routing table in the system							
Number	Destination	Netmask	Gateway	Interface			
1	0.0.0.0	0.0.0.0	192.168.0.180	LOCAL			
2	0.0.0.0	0.0.0.0	192.168.1.18	WAN1			
3	0.0.0.0	0.0.0.0	192.168.1.19	WAN2			
4	192.168.0.0	255.255.255.0	0.0.0.0	LAN			
5	192.168.1.0	255.255.255.0	0.0.0.0	WAN1			
6	192.168.1.0	255.255.255.0	0.0.0.0	WAN2			

[Add Route](#)

Figure 4-23: Routing table

Add a routing rule	
Type	<input type="text" value="Host"/>
Destination	<input type="text"/>
Netmask	<input type="text" value="255.255.255.255 /32"/>
Gateway	<input type="text"/>
Interface	<input type="text" value="LAN"/>
Comment	<input type="text"/>

[Apply Settings](#) [Cancel Changes](#)

Figure 4-24: Routing setup

Routing tables contain a list of IP addresses. Each IP address identifies a remote router (or other network gateway) that the local router is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges that remote device will accept.

Object	Description
Type	There are two types: Host and Net. When the Net type is selected, user does not need to input the Gateway.
Destination	The network or host IP address desired to access.
Net Mask	The subnet mask of destination IP.

Object	Description
Gateway	The gateway is the router or host's IP address to which packet was sent. It must be the same network segment with the WAN or LAN port.
Interface	Select the interface that the IP packet must use to transmit out of the router when this route is used.
Comment	Enter any words for recognition.

4.5.5 WAN IPv6 Setting

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the router as shown in [Figure 4-25](#). It allows you to enable IPv6 function and set up the parameters of the router's WAN. In this setting you may change WAN connection type and other settings.

WAN1 IPv6 Setting

Connection Type	<input type="text" value="DHCP"/>
IPv6 Address	<input type="text"/>
Subnet Prefix Length	<input type="text" value="64"/>
Default Gateway	<input type="text"/>

WAN2 IPv6 Setting

Connection Type	<input type="text" value="DHCP"/>
IPv6 Address	<input type="text"/>
Subnet Prefix Length	<input type="text" value="64"/>
Default Gateway	<input type="text"/>

Figure 4-25: IPv6 WAN setup

Object	Description
Connection Type	Select IPv6 WAN type either by using DHCP or Static.
IPv6 Address	Enter the WAN IPv6 address.
Subnet Prefix Length	Enter the subnet prefix length.
Default Gateway	Enter the default gateway of the WAN port.

4.5.6 DHCP

The DHCP service allows you to control the IP address configuration of all your network devices. When a client (host or other device such as networked printer, etc.) joins your network it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP; this is something called "automatic network configuration" and is often the default setting. The setup is shown in [Figure 4-26](#).

DHCP Server

DHCP Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Start IP Address	192.168.1. <input style="width: 50px; border: 1px solid gray;" type="text" value="100"/>	
Maximum DHCP Users	<input style="width: 100px; border: 1px solid gray;" type="text" value="101"/>	
Set DNS	<input checked="" type="radio"/> Automatically <input type="radio"/> Manually	
Primary DNS Server	<input style="width: 100%; border: 1px solid gray;" type="text"/>	
Secondary DNS Server	<input style="width: 100%; border: 1px solid gray;" type="text"/>	
WINS	<input style="width: 100%; border: 1px solid gray;" type="text"/>	
Lease Time	<input style="width: 100px; border: 1px solid gray;" type="text" value="1440"/>	minutes
Domain Name	<input style="width: 100%; border: 1px solid gray;" type="text" value="PLANET"/>	

Apply Settings
Cancel Changes

Figure 4-26: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the router will assign IP addresses to the DHCP clients automatically. If user needs to disable the function, please set it as disable.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the router.
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the router will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
Set DNS	By default, it is set as Automatically, and the DNS server is the router's LAN IP address. If user needs to use specific DNS server, please set it as Manually, and then input a specific DNS server.
Primary/Secondary DNS Server	Input a specific DNS server.
WINS	Input a WINS server if needed.
Lease Time	Set the time for using one assigned IP. After the lease time, the DHCP client will need to get new IP addresses from the router. Default is 1440 minutes.
Domain Name	Input a domain name for the router. Default is Planet.

4.5.7 DDNS

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as **PLANET DDNS** (<http://www.planetddns.com>) and set up the domain name of your choice.

PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown in [Figure 4-27](#).

PLANET DDNS

For example, you've just installed a PLANET IP camera with dynamic IP like 210.66.155.93 in the network. You can name this device as "Mycam1" and register a domain as Mycam1.planetddns.com at PLANET DDNS (<http://www.planetddns.com>). Thus, you don't need to memorize the exact IP address but just the URL link: Mycam1.planetddns.com.

PLANET Easy DDNS

PLANET Easy DDNS is an easy way to help user to get your Domain Name with just one click. You can just log in to the Web Management Interface of your devices, say, your router, and check the DDNS menu and just enable it. You don't need to go to <http://www.planetddns.com> to apply for a new account. Once you enabled the Easy DDNS, your PLANET Network Device will use the format PLxxxxxx where xxxxxx is the last 6 characters of your MAC address that can be found on the Web page or bottom label of the device. (For example, if the router's MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)

Dynamic Domain Name Service	
DDNS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Interface	WAN1 ▼
DDNS Type	PLANET DDNS ▼
Easy DDNS	Disable ▼
User Name	<input type="text"/>
Password	<input type="text"/>
Host Name	<input type="text"/>
Interval	120
Update Status	unknow status

Figure 4-27: PLANET DDNS

Object	Description
DDNS Service	By default, the DDNS service is disabled. If user needs to enable the function, please set it as enable.
Interface	User is able to select the interface for DDNS service. By default, the interface is WAN 1.
DDNS Type	There are three options: <ol style="list-style-type: none"> 1. PLANET DDNS: Activate PLANET DDNS service. 2. DynDNS: Activate DynDNS service. 3. NOIP: Activate NOIP service. Note that please first register with the DDNS service and set up the domain name of your choice to begin using it.
Easy DDNS	When the PLANET DDNS service is activated, user is able to select to enable or disable Easy DDNS. When this function is enabled, DDNS hostname will appear automatically. User doesn't go to http://www.planetddns.com to apply for a new account.
User Name	The user name is used to log into DDNS service.
Password	The password is used to log into DDNS service.
Host Name	The host name as registered with your DDNS provider.
Interval	Set the update interval of the DDNS function.
Update Status	Show the connection status of the DDNS function.

4.5.8 MAC Address Clone

Clone or change the MAC address of the WAN interface. The setup is shown in [Figure 4-28](#).

The screenshot shows two identical configuration panels for WAN1 and WAN2. Each panel has a blue header with the interface name. Below the header, there is a 'Clone WAN MAC' label followed by two radio buttons: 'Enable' (unselected) and 'Disable' (selected). Underneath is a 'MAC Address' label followed by a light gray text input field. At the bottom of the entire configuration area, there are two blue buttons: 'Apply Settings' and 'Cancel Changes'.

Figure 4-28: MAC Address Clone

Object	Description
Clone WAN MAC	Set the function as enable or disable.
MAC Address	Input a MAC Address, such as A8:F7:E0:00:06:62.

4.6 Security

The Security menu provides Firewall, Access Filtering and other functions as shown in [Figure 4-29](#).

Please refer to the following sections for the details.

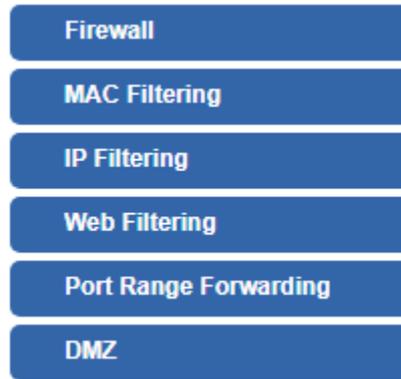


Figure 4-29: Security menu

Object	Description
Firewall	Allows setting DoS (Denial of Service) protection as enable.
MAC Filtering	Allows setting MAC Filtering.
IP Filtering	Allows setting IP Filtering.
Web Filtering	Allows setting Web Filtering.
Port Range Forwarding	Allows setting Port Forwarding.
DMZ	Allows setting DMZ.

4.6.1 Firewall

A "Denial-of-Service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service. The router can prevent specific DoS attacks as shown in [Figure 4-30](#).

Firewall Protection

SPI Firewall Enable Disable

DDos

Block SYN Flood Enable Disable Packets/Second

Block FIN Flood Enable Disable Packets/Second

Block UDP Flood Enable Disable Packets/Second

Block ICMP Flood Enable Disable Packets/Second

IP TearDrop Enable Disable

PingOfDeath Enable Disable

System Security

Block WAN Ping Enable Disable

Remote Management Enable Disable

Figure 4-30: Firewall

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. The default configuration is enabled.
Block SYN Flood	SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on. The default configuration is enabled.
Block FIN Flood	If the function is enabled, when the number of the current FIN packets is beyond the set value, the router will start the blocking function immediately. The default configuration is disabled.

<p>Block UDP Flood</p>	<p>If the function is enabled, when the number of the current UPD-FLOOD packets is beyond the set value, the router will start the blocking function immediately.</p> <p>The default configuration is disabled.</p>
<p>Block ICMP Flood</p>	<p>ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack.</p> <p>The default configuration is disabled.</p>
<p>IP TearDrop</p>	<p>If the function is enabled, the router will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes.</p>
<p>Ping Of Death</p>	<p>If the function is enabled, the router will block Ping of Death attack that aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size causing the target machine to freeze or crash.</p>
<p>Block WAN Ping</p>	<p>Enable the function to allow the Ping access from the Internet network.</p> <p>The default configuration is disabled.</p>
<p>Remote Management</p>	<p>Enable the function to allow the web server access of the router from the Internet network.</p> <p>The default configuration is disabled.</p>

4.6.2 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network or Internet through the router. Use of such filters can be helpful in securing or restricting your local network as shown in [Figure 4-31](#).

Figure 4-31: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. When the function is enabled, the router will block traffic of the MAC address on the list.
Interface	Select the function works on LAN, WAN or both. If you want to block a LAN device's MAC address, please select LAN, vice versa.
MAC Address	Input a MAC address you want to control, such as A8:F7:E0:00:06:62.
Add	When you input a MAC address, please click the "Add" button to add it into the list.
Remove	If you want to remove a MAC address from the list, please click on the MAC address, and then click the "Remove" button to remove it.
Remove All	If you want to remove all MAC addresses from the list, please click the "Remove All" button to remove all.

4.6.3 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown in [Figure 4-32](#). To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.

Figure 4-32: IP Filtering

Object	Description
IP Filtering	Set the function as enable or disable.
Add IP Filtering Rule	Go to the Add Filtering Rule page to add a new rule.

Figure 4-33: IP Filter Rule Setting

Object	Description
Enable	Set the rule as enable or disable.
Source IP Address	Input the IP address of LAN user (such as PC or laptop) which you want to control.
Anywhere (of source IP Address)	Check the box if you want to control all LAN users.

Object	Description
Destination IP Address	Input the IP address of web site which you want to block.
Anywhere (of destination IP Address)	Check the box if you want to control all web sites, meaning the LAN user can't visit any web site.
Destination Port	Input the port of destination IP Address which you want to block. Leave it as blank if you want to block all ports of the web site.
Protocol	Select the protocol type (TCP, UDP or all). If you are unsure, please leave it to the default all protocol.

4.6.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in [Figure 4-34](#). Block those URLs which contain keywords listed below.

Web Filtering

Web Filtering Enable Disable

Web Filtering Rules

No.	Rule Enable	Filter Keyword	Filter Type	Action
<div style="background-color: #4a7ebb; color: white; padding: 2px 10px; display: inline-block;">Add Web Filtering Rule</div>				

Figure 4-34: Web Filtering

Object	Description
Web Filtering	Set the function as enable or disable.
Add Web Filtering Rule	Go to the Add Web Filtering Rule page to add a new rule.

Web Filter Settings

Status

Filter Keyword

Apply Settings

Cancel Changes

Figure 4-35: Web Filtering Rule Setting

Object	Description
--------	-------------

Object	Description
Status	Set the rule as enable or disable.
Filter Keyword	Input the URL address that you want to filter, such as www.yahoo.com.

4.6.5 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall as shown in Figure 4-36. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Router's NAT firewall.

Port Forwarding

Port Forwarding Enable Disable

Port Forwarding Rules

No.	Rule Name	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range	Delete
<div style="background-color: #4a86e8; color: white; padding: 2px 10px; display: inline-block; margin: 0 auto;">Add Port Forwarding Rule</div>							

Figure 4-36: Port Forwarding

Object	Description
Port Forwarding	Set the function as enable or disable.
Add Port Forwarding Rule	Go to the Add Port Forwarding Rule page to add a new rule.

Port Forwarding

Rule Name	<input style="width: 90%;" type="text"/>
Protocol	<input type="text" value="Both"/> ▼
External Service Port	<input style="width: 40%;" type="text"/> ~ <input style="width: 40%;" type="text"/>
Virtual Server IP Address	<input style="width: 90%;" type="text"/>
Internal Service Port	<input style="width: 40%;" type="text"/> ~ <input style="width: 40%;" type="text"/>

Apply Settings

Cancel Changes

Figure 4-37: Port Forwarding Rule Setting

Object	Description
--------	-------------

Object	Description
Rule Name	Enter any words for recognition.
Protocol	Select the protocol type (TCP, UDP or both). If you are unsure, please leave it to the default both protocols.
External Service Port	Enter the external ports you want to control. For TCP and UDP services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.
Virtual Server IP Address	Enter the local IP address.
Internal Service Port	Enter local ports you want to control. For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

4.6.6 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in [Figure 4-38](#). Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ - WAN1

DMZ Enable Disable
DMZ IP Address

DMZ - WAN2

DMZ Enable Disable
DMZ IP Address

Figure 4-38: DMZ

Object	Description
DMZ	Set the function as enable or disable. If the DMZ function is enabled, it means that you set up DMZ at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/online game can have two way connections.

Object	Description
DMZ IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above.

4.7 VPN

To obtain a private and secure network link, the router is capable of establishing VPN connections. When used in combination with remote client authentication, it links the business' remote sites and users, conveniently providing the enterprise with an encrypted network communication method. By allowing the enterprise to utilize the Internet as a means of transferring data across the network, it forms one of the most effective and secure options for enterprises to adopt in comparison to other methods.

The Maintenance menu provides the following features for managing the system as [Figure 4-39](#) is shown below:



Figure 4-39: VPN Menu

Object	Description
IPsec	Allows setting IPsec function.
GRE	Allows setting GRE function.
PPTP	Allows setting PPTP function.
L2TP	Allows setting L2TP function.
SSL VPN	Allows setting SSL VPN function.
VPN Connection	Allows checking VPN Connection Status.

4.6.7 IPsec

IPsec (IP Security) is a generic standardized VPN solution. IPsec must be implemented in the IP stack which is part of the kernel. Since IPsec is a standardized protocol it is compatible to most vendors that implement IPsec. It allows users to have an encrypted network session by standard **IKE** (Internet Key Exchange). We strongly encourage you to use IPsec only if you need to because of interoperability purposes. When IPsec lifetime is specified, the device can randomly refresh and identify forged IKE's during the IPsec lifetime.

This page will allow you to modify the user name and passwords as shown in [Figure 4-40](#).



Figure 4-40: IPsec

Object	Description
Add IPsec Tunnel	Go to the Add IPsec Tunnel page to add a new tunnel.

IPSec Tunnel

IPSec Tunnel Enable

Tunnel Name

Interface WAN1 WAN2

Local Network

Local Netmask

Remote IP Address

Remote Network

Remote Netmask

Detection

Dead Peer Detection

Time Interval Seconds Timeout Seconds Action

Authentication

Preshare Key

IKE Setting

Phase 1

IKE v1 v2

Connection Type Main Aggressive

ISAKMP DH Group

IKE SA Lifetime hours

Phase 2

ESP

ESP Keylife hours

Perfect Forward Secrecy (PFS) Yes No

Figure 4-41: IPSec Tunnel

Object	Description
IPSec Tunnel Enable	Check the box to enable the function.
Tunnel Name	Enter any words for recognition.
Interface	This is only available for host-to-host connections and specifies to which interface the host is connecting. 1. WAN 1. 2. WAN 2.
Local Network	The local subnet in CIDR notation. For instance, "192.168.1.0".
Local Netmask	The netmask of this router.

Remote IP Address	Input the IP address of the remote host. For instance, "210.66.1.10".
Remote Network	The remote subnet in CIDR notation. For instance, "210.66.1.0".
Remote Netmask	The netmask of the remote host.
Dead Peer Detection	<p>Set up the detection time of DPD (Dead Peer Detection).</p> <p>By default, the DPD detection's gap is 30 seconds, over 150 seconds to think that is the broken line.</p> <p>When VPN detects opposite party reaction time, the function will take one of the actions: "Hold" stand for the system will retain IPSec SA, "Clear" stand for the tunnel will clean away and waits for the new sessions, "Restart" will delete the IPSec SA and reset VPN tunnel.</p>
Preshare Key	Enter a pass phrase to be used to authenticate the other side of the tunnel. Should be the same as the remote host.
IKE	Select the IKE (Internet Key Exchange) version.
Connection Type	<ol style="list-style-type: none"> 1. Main. 2. Aggressive.
ISAKMP	<p>It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits. 6. DH Group: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen.
IKE SA Lifetime	You can specify how long IKE packets are valid.
ESP	<p>It offers AES, 3 DES, SHA 1, SHA2, and MD5.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher

	<p>by using it three times. It can achieve an algorithm up to 168 bits.</p> <p>3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.</p> <p>4. SHA2: Either 256, 384 or 512 can be chosen.</p> <p>5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits.</p>
ESP Keylife	You can specify how long ESP packets are valid.
Perfect Forward Secrecy (PFS)	Set the function as enable or disable.

4.6.8 GRE

This section assists you in setting the GRE Tunnel as shown in [Figure 4-42](#).

GRE Tunnel

GRE Tunnel Enable Disable

GRE Tunnel Lists

No.	Name	Enable	Through	Peer WAN IP Addr	Peer Subnet	Peer Tunnel IP	Local Tunnel IP	Local Netmask	Action
<div style="background-color: #4a7ebb; color: white; padding: 2px 10px; display: inline-block; margin: 0 auto;">Add GRE Tunnel</div>									

Figure 4-42: GRE

Object	Description
GRE Tunnel	Set the function as enable or disable.
Add GRE Tunnel	Go to the Add GRE Tunnel page to add a new tunnel.

GRE Tunnel

Status	Disable ▼
Name	<input type="text" value="Tunnel name"/>
Through	LAN ▼
Peer Wan IP Address	<input type="text" value="Remote IP Address"/>
Peer Subnet Mask	<input type="text" value="10.10.10.0/24"/>
Peer Tunnel IP Address	<input type="text" value="10.10.10.2"/>
Local Tunnel IP Address	<input type="text" value="10.10.10.1"/>
Local Subnet Mask	<input type="text" value="255.255.255.255 /32 ▼"/>

Apply Settings
Cancel Changes

Figure 4-43: GRE Tunnel

Object	Description
Active	Check the box to enable the function.
Tunnel Name	Enter any words for recognition.
Through	<p>This is only available for host-to-host connections and specifies to which interface the host is connecting.</p> <ol style="list-style-type: none"> 1. LAN. 2. WAN 1. 3. WAN 2.
Peer WAN IP Address	Input the IP address of the remote host. For instance, "210.66.1.10".
Peer Netmask	The remote subnet in CIDR notation. For instance, "210.66.1.0/24".
Peer Tunnel IP Address	Input the Tunnel IP address of remote host.
Local Tunnel IP Address	Input the Tunnel IP address of remote host.
Local Netmask	Input the Tunnel IP address of the router.

4.6.9 PPTP Server

Use the IP address and the scope option needs to match the far end of the PPTP server; its goal is to use the PPTP channel technology, and establish Site-to-Site VPN where the channel can have equally good results from different methods with IPSec. The PPTP server is shown in [Figure 4-44](#).

PPTP Server

PPTP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Force MPPE Encryption	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
CHAP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MSCHAP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MSCHAP v2	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DNS1	<input type="text" value=""/>
DNS2	<input type="text" value=""/>
WINS1	<input type="text" value=""/>
WINS2	<input type="text" value=""/>
Server IP Address	<input type="text" value="192.168.10.1"/>
Clients IP Address Start	<input type="text" value="192.168.10.10"/>
Clients IP Address End	<input type="text" value="192.168.10.100"/>

	User	Password
1	<input type="text" value="test"/>	<input type="text" value="test"/>
2	<input type="text" value="user"/>	<input type="text" value="1234"/>
3	<input type="text" value="user"/>	<input type="text" value="1234"/>
4	<input type="text" value="user"/>	<input type="text" value="1234"/>
5	<input type="text" value="user"/>	<input type="text" value="1234"/>

Apply Settings
Cancel Changes

Figure 4-44: PPTP server

Object	Description
PPTP Server	Set the function as enable or disable.
Broadcast	Enter any words for recognition.
Force MPPE Encryption	Set the encryption as enable or disable.
CHAP	Set the authentication as enable or disable.
MSCHAP	Set the authentication as enable or disable.

MSCHAP v2	Set the authentication as enable or disable.
DNS	When the PPTP client connects to the PPTP server, it will assign the DNS server IP address to client.
WINS	When the PPTP client connects to the PPTP server, it will assign the WINS server IP address to client.
Server IP Address	Input the IP address of the PPTP Server. For instance, "192.168.10.1".
Clients IP Address (Start/End)	When the VPN connection is established, the VPN client will get IP address from the VPN Server. Please set the range of IP Address. For instance, the start IP address is "192.168.10.10", the end IP address is "192.168.10.100".
User and Password	Create the username and password for the VPN client.

4.6.10 L2TP Server

This section assists you in setting the L2TP Server as shown in [Figure 4-45](#).

L2TP Server

L2TP Server Enable Disable

Server IP Address

Clients IP Address Start

Clients IP Address End

With IPsec Enable Disable

Preshare Key

Users

	User	Password
1	<input type="text" value="test"/>	<input type="text" value="test"/>
2	<input type="text" value="user"/>	<input type="text" value="1234"/>
3	<input type="text" value="user"/>	<input type="text" value="1234"/>
4	<input type="text" value="user"/>	<input type="text" value="1234"/>
5	<input type="text" value="user"/>	<input type="text" value="1234"/>

IPsec

Phase 1

Connection Type Main Aggressive

ISAKMP DH Group

IKE SA Lifetime hours

Phase 2

ESP

ESP Keylife hours

Figure 4-45: L2TP Server

Object	Description
L2TP Server	Set the function as enable or disable.
Server IP Address	Input the IP address of the L2TP Server. For instance, "192.168.50.1".
Clients IP Address (Start/End)	When the VPN connection is established, the VPN client will get IP address from the VPN Server. Please set the range of IP Address. For instance, the start IP address is "192.168.50.100", the end IP address is "192.168.50.200".

Object	Description
With IPsec	Set the function as enable to make the L2TP work with IPsec encryption.
Preshare Key	Enter a pass phrase.
User and Password	Create the username and password for the VPN client.
Connection Type	<ol style="list-style-type: none"> 1. Main. 2. Aggressive.
ISAKMP	<p>It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen. 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits. 6. DH Group: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen.
IKE SA Lifetime	You can specify how long IKE packets are valid.
ESP	<p>It offers AES, 3 DES, SHA 1, SHA2, and MD5.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen. 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits.
ESP Keylife	You can specify how long ESP packets are valid.

4.6.11 SSL VPN

This section assists you in setting the SSL Server as shown in [Figure 4-46](#).

SSL Server

SSL VPN Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Port	<input type="text" value="1194"/>	
Tunnel Protocol	<input type="text" value="UDP"/>	
Virtual Network Device	<input type="text" value="TUN"/>	
Interface	<input type="text" value="LAN"/>	<input type="text" value="192.168.1.1"/>
VPN Network	<input type="text" value="192.168.20.0"/>	
Network Mask	<input type="text" value="255.255.255.0"/>	
Encryption Cipher	<input type="text" value="AES-128 CBC"/>	
Hash Algorithm	<input type="text" value="SHA1"/>	
Export client.ovpn	<input type="button" value="Export"/>	

Figure 4-46: SSL Server

Object	Description
SSL VPN Server	Set the function as enable or disable.
Port	Set a port for the SSL Service. Default port is 1194.
Tunnel Protocol	Set the protocol as TCP or UDP.
Virtual Network Device	Set the Virtual Network Device as TUN or TAP.
Interface	User is able to select the interface for SSL service using.
VPN Network	The VPN subnet in CIDR notation. For instance, "192.168.20.0".
Network Mask	The netmask of the VPN.
Encryption Cipher	There are four encryption types: None, AES-128 CBC, AES-192 CBC or AES-256 CBC.
Hash Algorithm	There are five types of Hash Algorithm: None, SHA1, SHA1, SHA512 or MD5.
Export client.ovpn	Export a configuration for the SSL client. User is able to upload it to VPN client (such as Open VPN software).

4.6.12 VPN Connection

This page shows the VPN connection status as shown in [Figure 4-47](#).

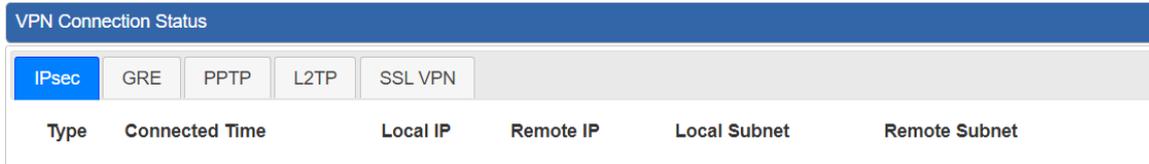


Figure 4-47: VPN Connection Status

Object	Description
VPN Connection Status	Click the IPSec/GRE/.../SSL VPN bookmark to check the current connection status.

4.7 Maintenance

The Maintenance menu provides the following features for managing the system as [Figure 4-48](#) is shown below:



Figure 4-48: Maintenance Menu

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the router's configuration to local or USB sticker. Restore the router's configuration from local or USB sticker.
Firmware Upgrade	Upgrade the firmware from local or USB storage.
Reboot / Reset	Reboot or reset the system.
Auto Reboot	Allows setting auto-reboot schedule.
Diagnostics	Allows you to issue ICMP PING packets to troubleshoot IP.

4.7.1 Administrator

To ensure the router's security is secure, you will be asked for your password when you access the router's Web-based utility. The default user name and password are "**admin**". This page will allow you to modify the user name and passwords as shown in [Figure 4-21](#).

Account Password

Username	<input type="text" value="admin"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Figure 4-48: Administrator

Object	Description
Username	Input a new username.
Password	Input a new password.
Confirm Password	Input password again.

4.7.2 Date and Time

This section assists you in setting the system time of the router. You are able to either select to set the time and date manually or automatically obtain the GMT time from Internet as shown in [Figure 4-49](#).

Date and Time

Current Time	Year <input type="text" value="2019"/> Month <input type="text" value="10"/> Day <input type="text" value="22"/> Hour <input type="text" value="10"/> Minute <input type="text" value="27"/> Second <input type="text" value="12"/>
	<input type="button" value="Copy Computer Time"/>
Time Zone Select	<input type="text" value="(GMT+08:00)Taipei"/>
NTP Client Update	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
NTP Server	<input type="text" value="time.nist.gov"/>
	<input type="text" value="time.windows.com"/>
	<input type="text" value="time.stdtime.gov.tw"/>
	<input type="text"/>

Figure 4-49: Date and Time

Object	Description
Current Time	Show the current time. User is able to set time and date manually.
Time Zone Select	Select the time zone of the country you are currently in. The router will

	set its time based on your selection.
NTP Client Update	Once this function is enabled, router will automatically update current time from NTP server.
NTP Server	User may use the default NTP sever or input NTP server manually.

4.7.3 Saving/Restoring Configuration

This page shows the status of the configuration. You may save the setting file to either USB storage or PC and load the setting file from USB storage or PC as [Figure 4-50](#) is shown below:

Save/Restore Configuration

Configuration Export

Configuration Import No file chosen

USB Backup/Upload Configuration

USB HDD: Not Detected

Backup Settings to USB HDD:

Load Settings from USB HDD: Configuration disabled

Please format the HDD as FAT32 on a Windows PC before using it for backup

Figure 4-50: Save/Restore Configuration

■ Save Setting to PC

Object	Description
Configuration Export	Press the <input type="button" value="Export"/> button to save setting file to PC.
Configuration Import	Press the <input type="button" value="Choose File"/> button to select the setting file, and then press the <input type="button" value="Import"/> button to upload setting file from PC.

■ Save Setting to USB Storage

Object	Description
--------	-------------

Object	Description
USB Storage	The status of USB storage.
Backup Settings to USB Storage	Press the <input type="button" value="Save"/> button to save setting file to USB storage.
Load Settings from USB Storage	Press the <input type="button" value="Upload"/> button to upload setting file from USB storage.
Unmount	Before removing the USB storage from the router, please press the <input type="button" value="Unmount"/> button first.

4.7.4 Upgrading Firmware

This page provides the firmware upgrade of the router as shown in [Figure 4-51](#).

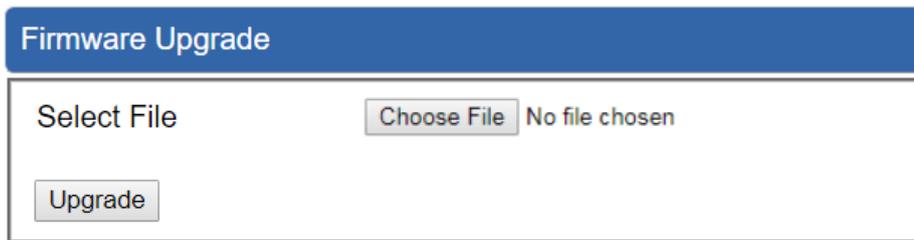


Figure 4-51: Firmware upgrade

Object	Description
Choose File	Press the button to select the firmware.
Upgrade	Press the button to upgrade firmware to system.

4.7.5 Reboot / Reset

This page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, users have to re-log in the Web interface as [Figure 4-52](#) is shown below:

Reboot / Reset

Reboot Button

Reset Button

I'd like to keep the network profiles.
Keep your current network profiles and reset all other configuration to factory defaults.

Figure 4-52: Reboot/Reset

Object	Description
Reboot	Press the button to reboot system.
Reset	Press the button to restore all settings to factory default settings.
I'd like to keep the network profiles.	Check the box and then press the <input type="button" value="Reset to Default"/> button to keep the current network profiles and reset all other configurations to factory defaults.

4.7.6 Diagnostics

The page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press "Ping", ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The Page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping is shown in [Figure 4-53](#).

Ping Test

Interface

Target Host

Numbers of Packets

Ping

Figure 4-53: Ping

Object	Description
Interface	Select an interface of the router.
Target Host	The destination IP Address or domain.
Number of Packets	Set the number of packets will be transmitted; the maximum is 100.
Ping	The time of ping.



Be sure the target IP address is within the same network subnet of the router, or you have to set up the correct gateway IP address.

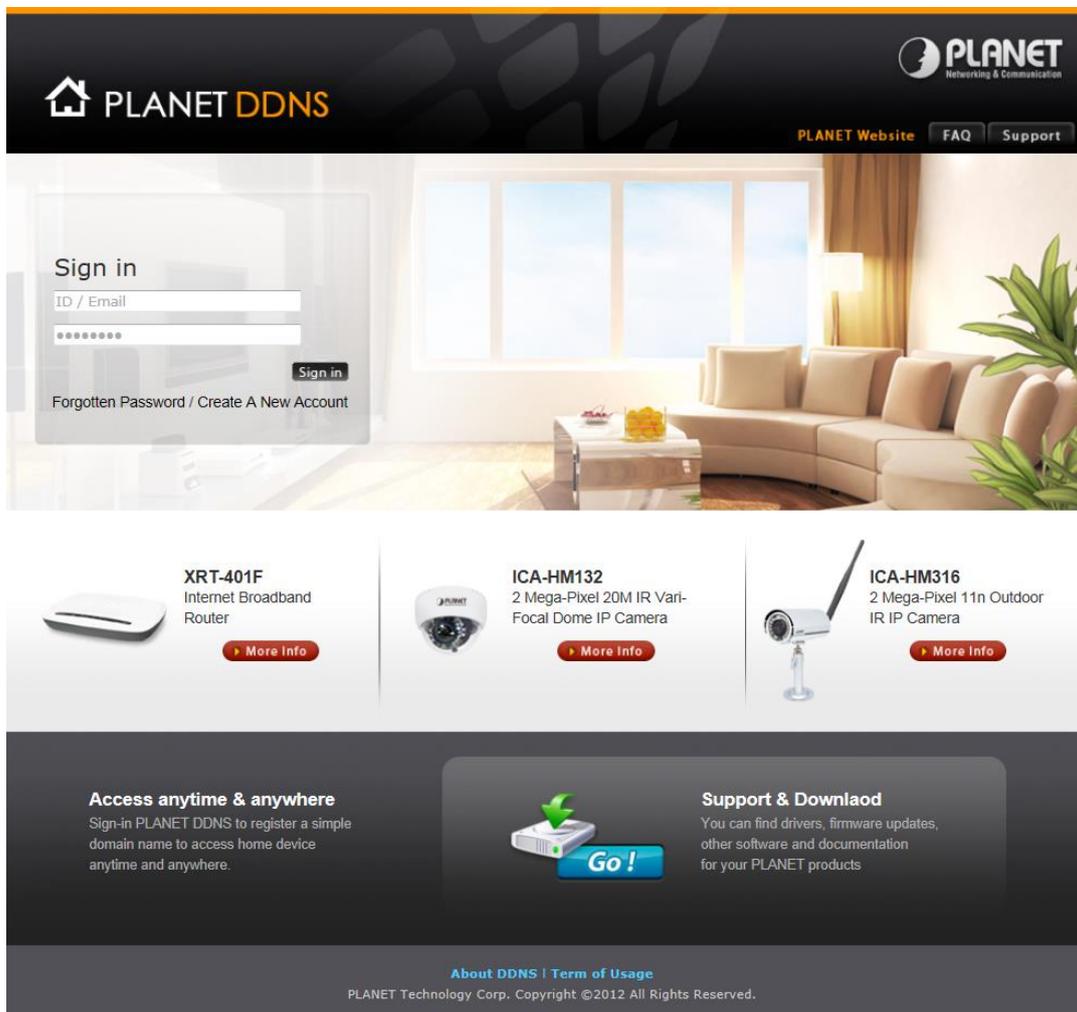
Appendix A: DDNS Application

Configuring PLANET DDNS steps:

Step 1: Visit DDNS provider's web site and register an account if you do not have one yet. For example, register an account at <http://planetddns.com>

Step 2: Enable DDNS option through accessing web page of the device.

Step 3: Input all DDNS settings.



The screenshot shows the PLANET DDNS website. At the top, there is a navigation bar with the PLANET logo and links for 'PLANET Website', 'FAQ', and 'Support'. The main content area features a 'Sign in' form with fields for 'ID / Email' and a password field, a 'Sign in' button, and links for 'Forgotten Password / Create A New Account'. Below the sign-in form, there are three product cards: 'XRT-401F Internet Broadband Router', 'ICA-HM132 2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera', and 'ICA-HM316 2 Mega-Pixel 11n Outdoor IR IP Camera'. Each card includes a 'More Info' button. At the bottom, there is a section for 'Access anytime & anywhere' and 'Support & Download', along with a 'Go!' button and a footer with 'About DDNS | Term of Usage' and 'PLANET Technology Corp. Copyright ©2012 All Rights Reserved.'