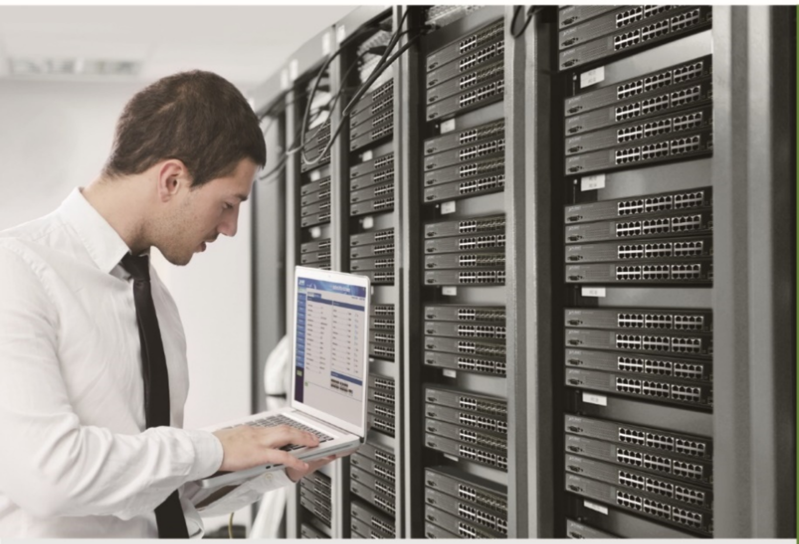
Networking & Communication

User’s Manual

Industrial 5-Port 10/100/1000T VPN Security Gateway

► IVR-100



www.PLANET.com.tw

Copyright

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 Industrial 5-Port 10/100/1000T VPN Security Gateway
Model: IVR-100
Rev.: 1.0 (December, 2020)
Part No. EM-IVR-100_v1.0

Table of Contents

Chapter 1. Product Introduction..6
1.1 Package Contents..6
1.2 Overview..6
1.3 Topology..11
1.4 Features..12
1.5 Product Specifications..14

Chapter 2. Hardware Introduction..17
2.1 Physical Descriptions..17
2.1.1 Front View..17
2.1.2 Top View..18
2.1.3 Wiring the Power Inputs..18
2.1.4 Wiring the Fault Alarm Contact..19
2.1.5 Dimensions..21
2.2 Hardware Installation..22
2.2.1 DIN-rail Mounting..22
2.2.2 Wall Mount Plate Mounting..23
2.2.4 Side Wall Mount Plate Mounting..25

Chapter 3. Preparation..26
3.1 Requirements..26
3.2 Setting TCP/IP on your PC..26
3.2.1 Windows 7/8..26
3.2.2 Windows 10..30
3.3 Planet Smart Discovery Utility..33

Chapter 4. Web-based Management..35
4.1 Introduction..35
4.2 Logging in to the VPN Gateway..35
4.3 Main Web Page..36
4.4 System..38
4.4.1 Setup Wizard..39
4.4.2 Dashboard..45
4.4.3 Status..46
4.4.4 Statistics..47
4.4.5 Connection Status..47
4.4.6 SNMP..48

4.5 Network 49
4.5.1 WAN 50
4.5.2 WAN Advanced 51
4.5.3 LAN Setup 52
4.5.4 Routing 53
4.5.5 WAN IPv6 Setting 54
4.5.6 DHCP 55
4.5.7 DDNS 57
4.5.8 MAC Address Clone 59
4.6 Security 60
4.6.1 Firewall 61
4.6.2 MAC Filtering 63
4.6.3 IP Filtering 64
4.6.4 Web Filtering 65
4.6.5 Port Forwarding 66
4.6.6 DMZ 67
4.7 VPN 68
4.7.1 IPSec 69
4.7.2 GRE 74
4.7.3 PPTP Server 76
4.7.4 L2TP Server 80
4.7.5 SSL VPN 85
4.7.6 VPN Connection 86
4.8 Maintenance 87
4.8.1 Administrator 87
4.8.2 Date and Time 88
4.8.3 Saving/Restoring Configuration 89
4.8.4 Upgrading Firmware 90
4.8.5 Reboot / Reset 90
4.8.6 Diagnostics 91

Appendix A: DDNS Application 93

Chapter 1. Product Introduction

1.1 Package Contents

The package should contain the following:

- VPN Gateway x 1
- Quick Installation Guide x 1
- Wall-mount Kit x 1
- Dust Cap x 5

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

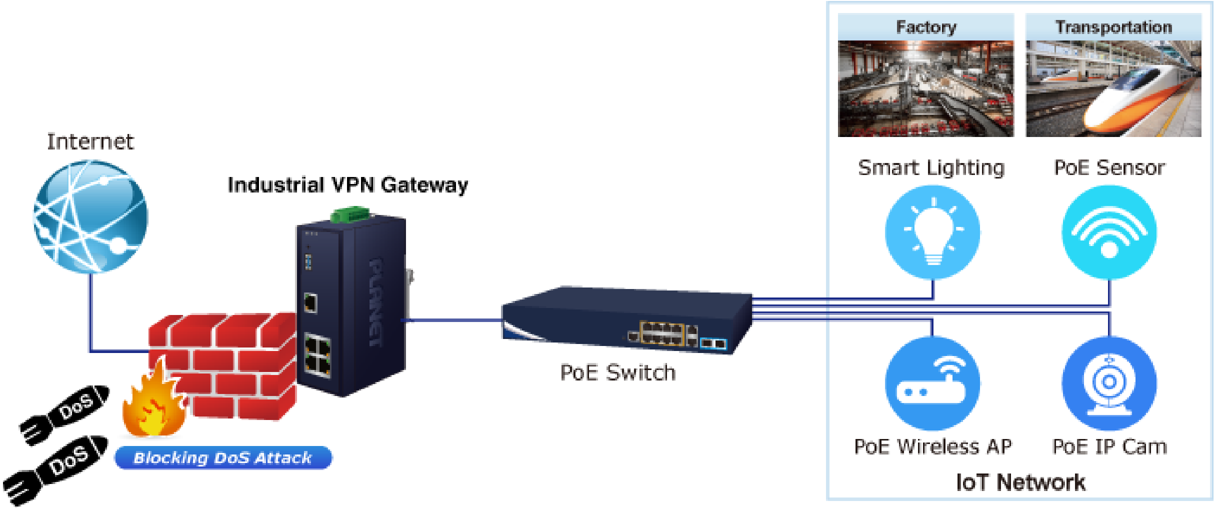
1.2 Overview

Powerful Industrial 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 IVR-100 Industrial VPN Security Gateway, an all-in-one appliance that carries several main categories across your industrial network security deployments: Cyber security, SPI firewall security protection, policy auditing (Content Filtering, VPN Tunnel and VLAN), and easy management (Setup Wizard, QoS and Dashboard). Furthermore, its Dual-WAN Failover and Outbound Load Balancing features can improve the network efficiency while the web-based interface provides friendly and consistent user experience. For the harsh environment, the IVR-100 can not only operate stably under temperature range from -40 to 75 degrees C, but also is equipped with a compact IP30 metal case that allows either DIN-rail or wall mounting for efficient use of cabinet space.

Excellent Ability in Threat Defense

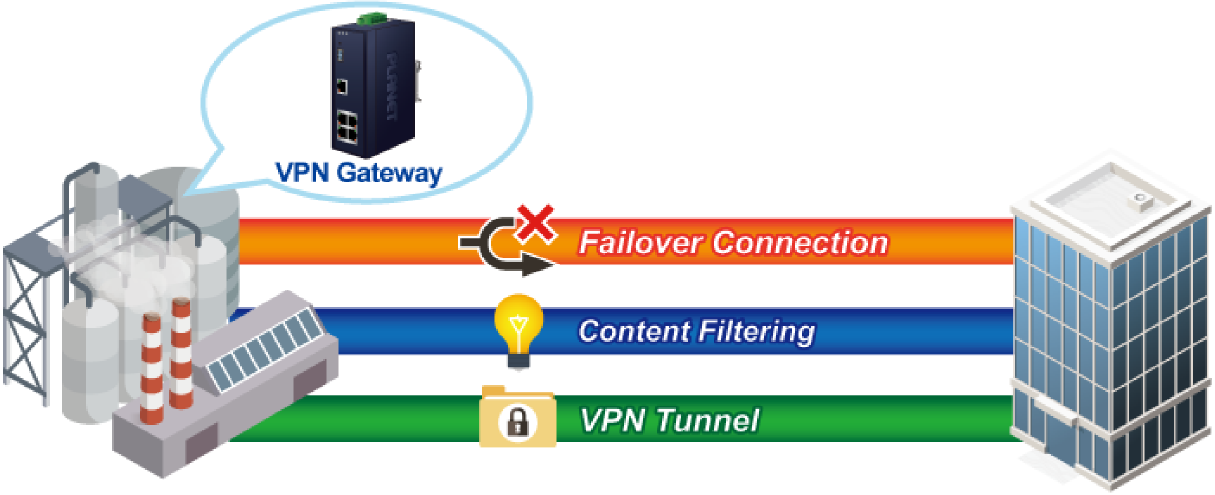
The IVR-100 built-in SPI (stateful packet inspection) firewall and anti DoS/DDoS attack functions provide high efficiency and extensive protection for your network. Virtual server and DMZ functions can let you set up servers in the Intranet and still provide services to the Internet users.



Ideal VPN Security Gateway Solution for SMBs

The IVR-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 IVR-100 makes the connection solidly secure, more flexible, and more capable.

The IVR-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 requirements, and the dual-WAN interfaces enable the IVR-100 to support outbound load balancing and WAN fail-over features.



Cybersecurity Network Solution to Minimize Security Risks

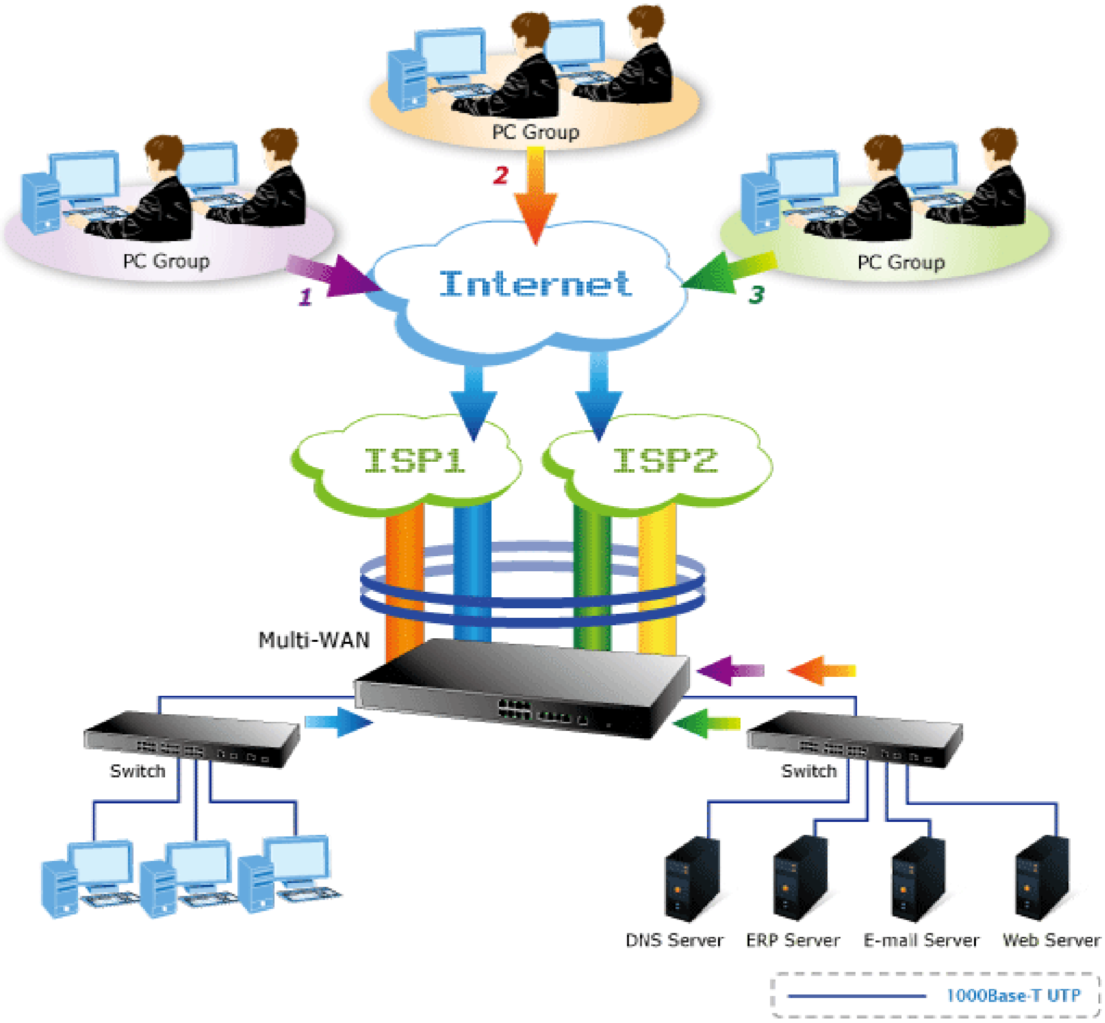
The cybersecurity feature included to protect the switch management in a mission-critical network virtually needs no effort and cost to install. For efficient management, the IVR-100 is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the IVR-100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

Improving Network Efficiency

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

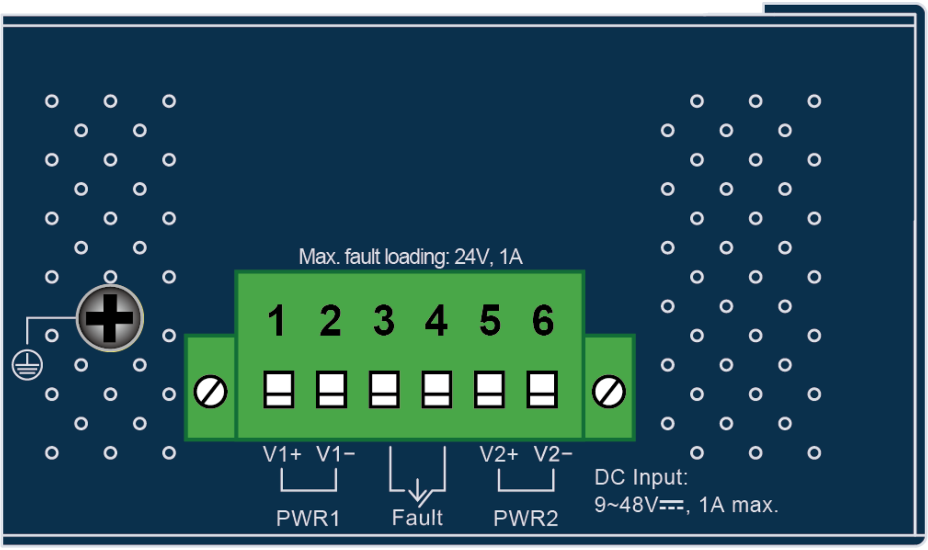
The IVR-100's built-in content filtering feature can automatically resolve the IP address corresponding to all. Users' network can be easily managed by just typing the URL of the websites like Facebook, YouTube and Yahoo.

The IVR-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.



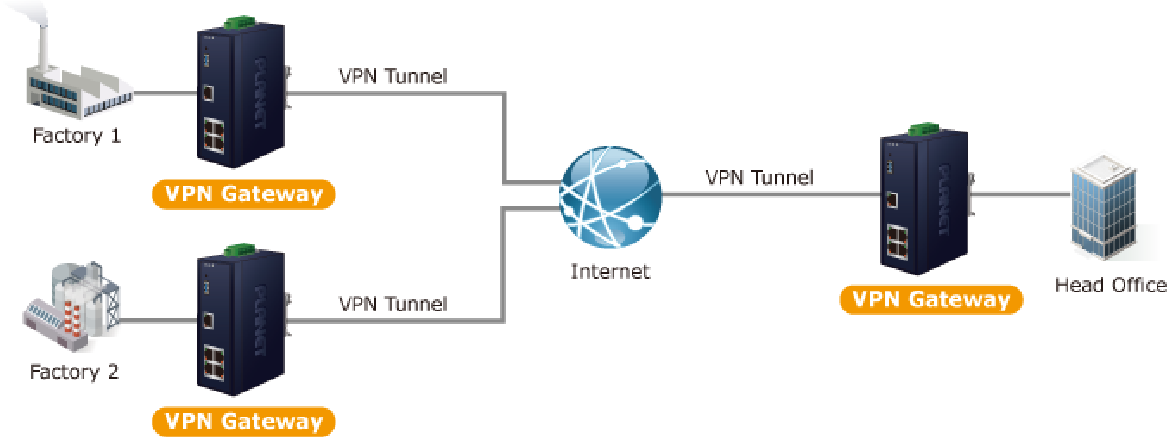
Convenient and Reliable Power System

To facilitate transportation and industrial-level applications, the IVR-100 provides an integrated power solution with a wide range of voltages (9~48V DC) for worldwide operability. It also provides dual-redundant, reversible polarity 9~48V DC power supply inputs for high availability applications.



Stable Operating Performance under Difficult Environments

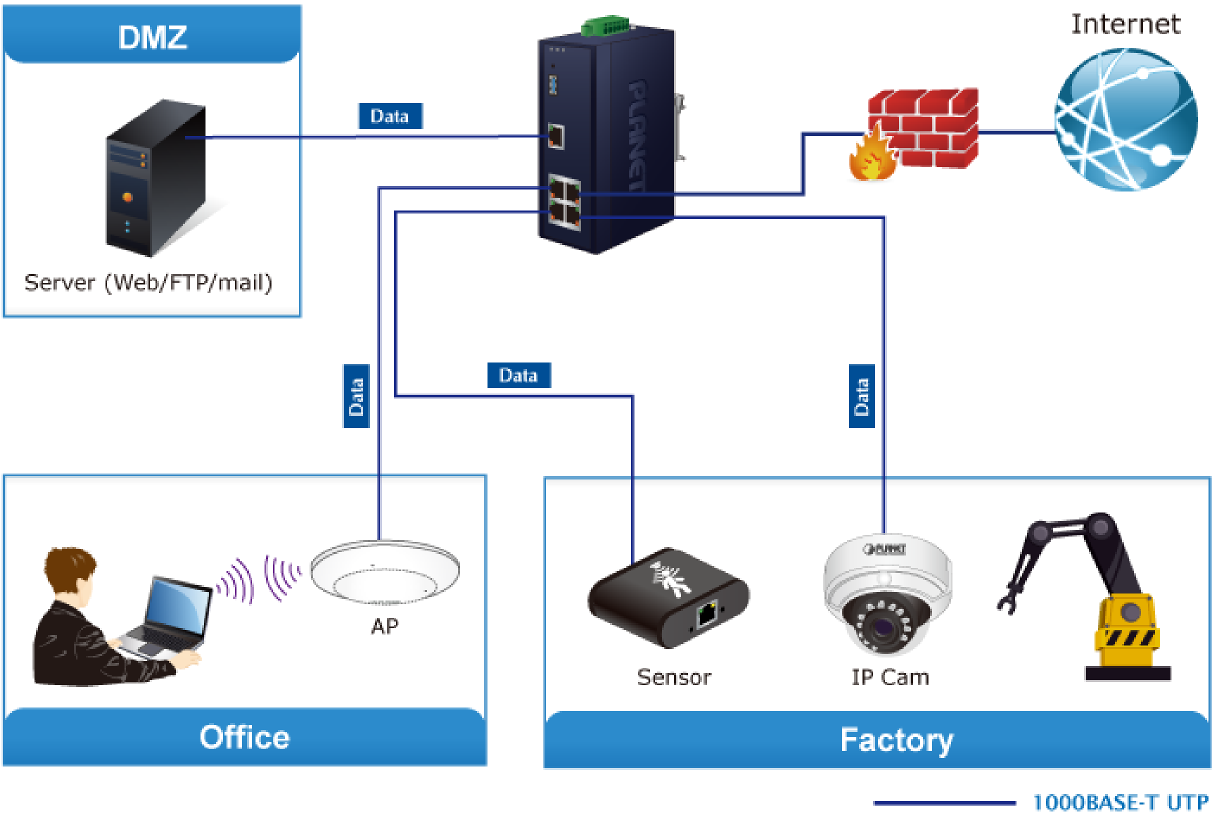
Today, the VPN demand expands from commercial applications to many critical networks in the harsh environment. The IVR-100 will be one of the ideal solutions that provide a high level of immunity against electromagnetic interference and heavy electrical surges typical of environments found on plant floors or in curb-side traffic control cabinets. The IVR-100 can operate stably under temperature range from -40 to 75 degrees C which enables the users to conveniently apply the device in almost any location of the network. The IVR-100 is also equipped with a compact IP30 standard metal case that allows either DIN-rail or wall mounting for efficient use of cabinet space.



1.3 Topology

PLANET IVR-100 can work as a VPN security gateway in an industrial application for a company that has a factory and many different divisions. With IPSec/GRE/PPTP/L2TP/SSL VPN solutions, the IVR-100 provides secured data communication for branches, vendors, and mobile workers with a flexible way to connect back to the headquarters.

The IVR-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 firmware upgrade
- Reset button

➢ Industrial Case and Installation

- IP30 metal case
- Solid DIN-rail, wall-mount or side wall-mount design
- Supports 6KV DC Ethernet ESD protection
- Fault alarm for power input failure
- DC redundant power with reverse polarity protection
- -40 to 75 degrees C operating temperature

➢ IP Routing Feature

- Static Route
- Dynamic Route (RIPv1/v2)

➢ 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
- QoS
- DMZ
- VLAN
- IGMP Proxy
- SNMP(v1/v2C/v3)
- 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
- Configuration backup and restoration via remote/USB port
- Firmware upgrade via remote/USB port
- Event message logging to remote syslog server
- PLANET Smart Discovery utility/UNI-NMS supported

1.5 Product Specifications

Product	VPN security gateway
Model	IVR-100
Hardware	
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including ■ 3 LAN ports ■ 1WAN port ■ 1 LAN/WAN port
USB Port	1 USB 3.0 port for system configuration backup and firmware upgrade
Reset Button	< 5 sec: System reboot > 5 sec: Factory default
Enclosure	IP30 metal case
LED Indicators	Power1/Power2 (Green) Fault (Red)
Installation	DIN-rail, wall-mount or side wall-mount design
Connector	Removable 6-pin terminal block Pin 1/2 for Power 1 Pin 3/4 for power fault alarm Pin 5/6 for Power 2
Alarm	One relay output for power failure. Alarm relay current carry ability: 1A @ 24V AC
Power Requirements	9-48V AC, 1A max.
Power Consumption	9W max.
Weight	0.53kg
Dimensions (W x D x H)	135 x 87.8 x 50 mm
ESD Protection	6KV DC
Software	
Management	Web browser
Operation Mode	Routing mode
Routing Protocol	Static route: 32 Dynamic route (RIPv1/v2): 4096
NAT Throughput	Max. 900Mbps
Firewall Security	Stateful packet inspection (SPI) Blocks DoS/DDoS attack
Outbound Load Balancing	Supported algorithms: Weight

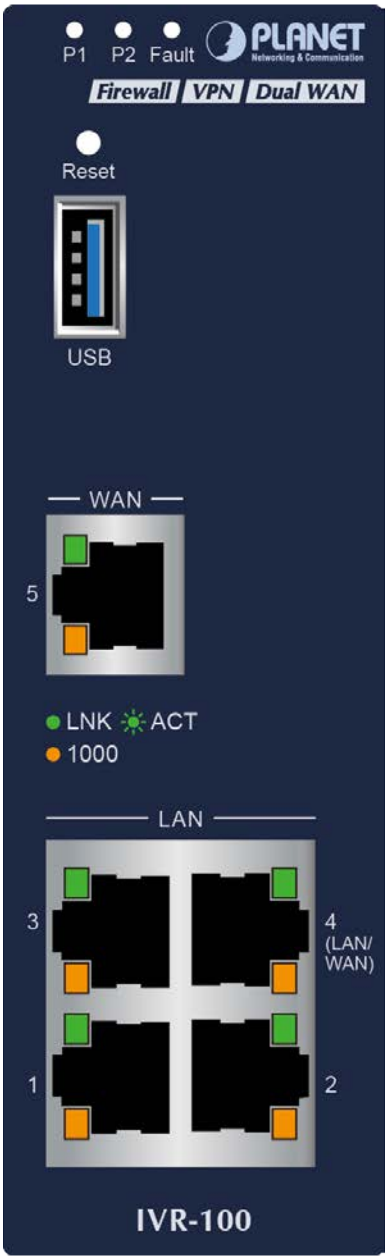
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, SNMP(v1/v2C/v3), PPPoE, SNMP, QoS, VLAN, IGMP Proxy
Content Filtering	MAC filtering IP filtering Web filtering
Log	System operation log Event message logging to remote syslog server
Others	Outbound load balancing Failover for dual-WAN Port forwarding DMZ Cybersecurity Dashboard Setup wizard Auto reboot PLANET Smart Discovery utility/UNI-NMS supported
VPN	
VPN Function	IPSec (Host to Host)/GRE/PPTP server/L2TP/SSL (Open VPN)
VPN Tunnels	Max. 60
VPN Throughput	Max. 100Mbps
VPN concurrent users	Max. 60
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
Stability Testing	IEC60068-2-32 (free fall) IEC60068-2-27 (shock) IEC60068-2-6 (vibration)
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3ab Gigabit 1000T IEEE 802.1Q VLAN tagging RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP

Environment Specifications	
Operating	Temperature: -40 ~ 75 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -40 ~ 85 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Standard Accessories	
Packet Contents	IVR-100 x 1 Quick Installation Guide x 1 Wall-mount Kit x 1 Dust Cap x 5

Chapter 2. Hardware Introduction

2.1 Physical Descriptions

2.1.1 Front View

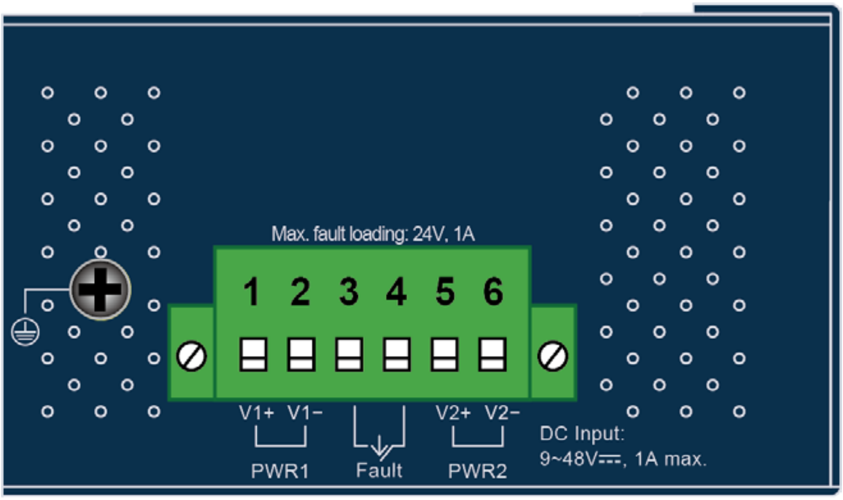


LED		
P1 P2	Green	Lights up when the power is on.
Fault	Red	Lights to indicate that power input has failed.
LNK / ACT	Green	"Steady on" to indicate the port is connected to other network device successfully. "Blink" to indicate there is traffic on the port.
1000	Amber	"Steady on" to indicate that the port is successfully connecting to the network at 1000Mbps. "Off" to indicate that the port is successfully connecting to the network at 10Mbps or 100Mbps.

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 less than 5 seconds to reboot it or over 5 seconds to restore it to factory default settings.
Gigabit Port 1-3	It is a LAN port for connecting to a switch.
Gigabit Port 4	Default is LAN port. It can be defined as LAN port or WAN port.
Gigabit Port 5	It is a WAN port for connecting to a perimeter gateway.

2.1.2 Top View

The upper panel of the Industrial Gateway consists of one terminal block connector within two DC power inputs.

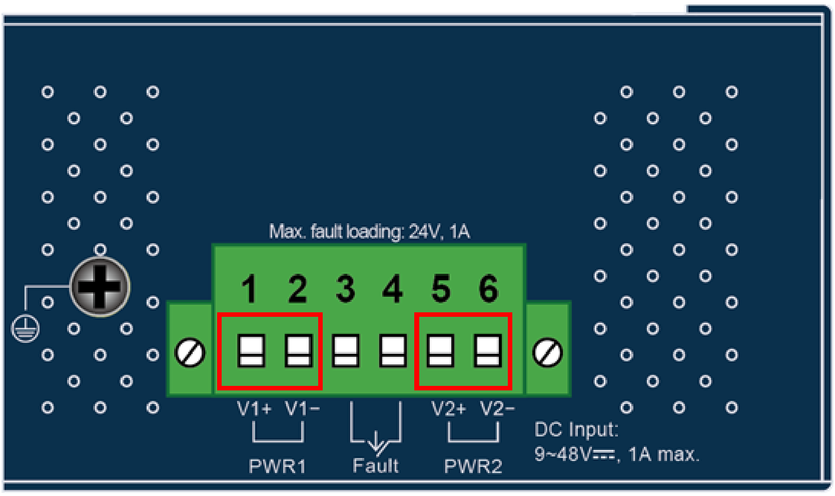


2.1.3 Wiring the Power Inputs

The 6-contact terminal block connector on the top panel of Industrial Gateway is used for two DC redundant power inputs. Please follow the steps below to insert the power wire.

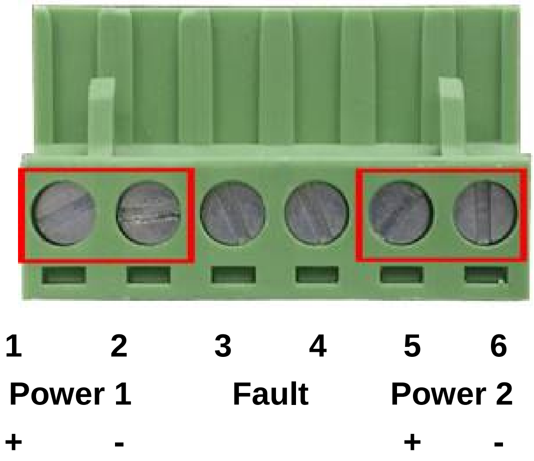
When performing any of the procedures like inserting the wires or tightening the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

1. Insert positive and negative DC power wires into contacts 1 and 2 for POWER 1, or 5 and 6 for POWER 2.



To avoid damage, please use the Industrial Gateway under its specification.

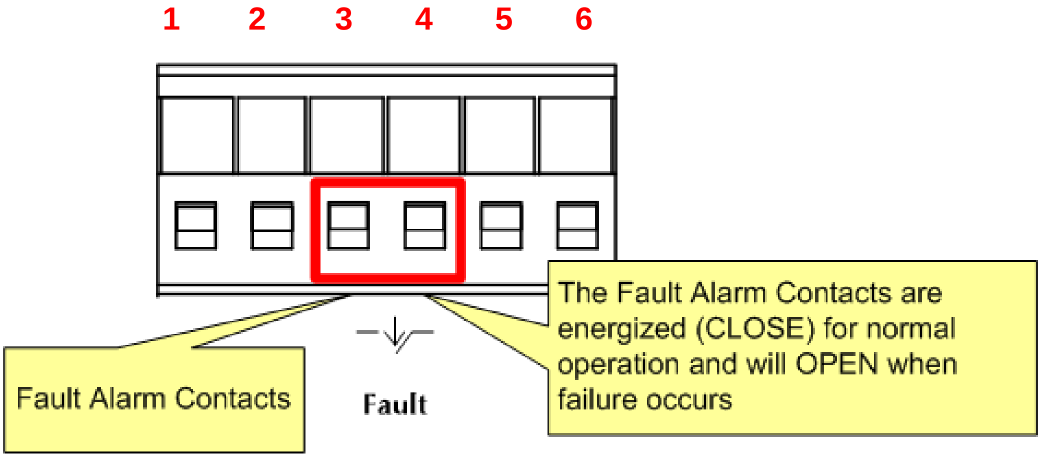
2. Tighten the wire-clamp screws for preventing the wires from loosening.



The wire gauge for the terminal block should be in the range from **12** to **24** AWG.

2.1.4 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the Industrial Gateway will detect the fault status of the power failure and then forms an open circuit. The following illustration shows an application example for wiring the fault alarm contacts.

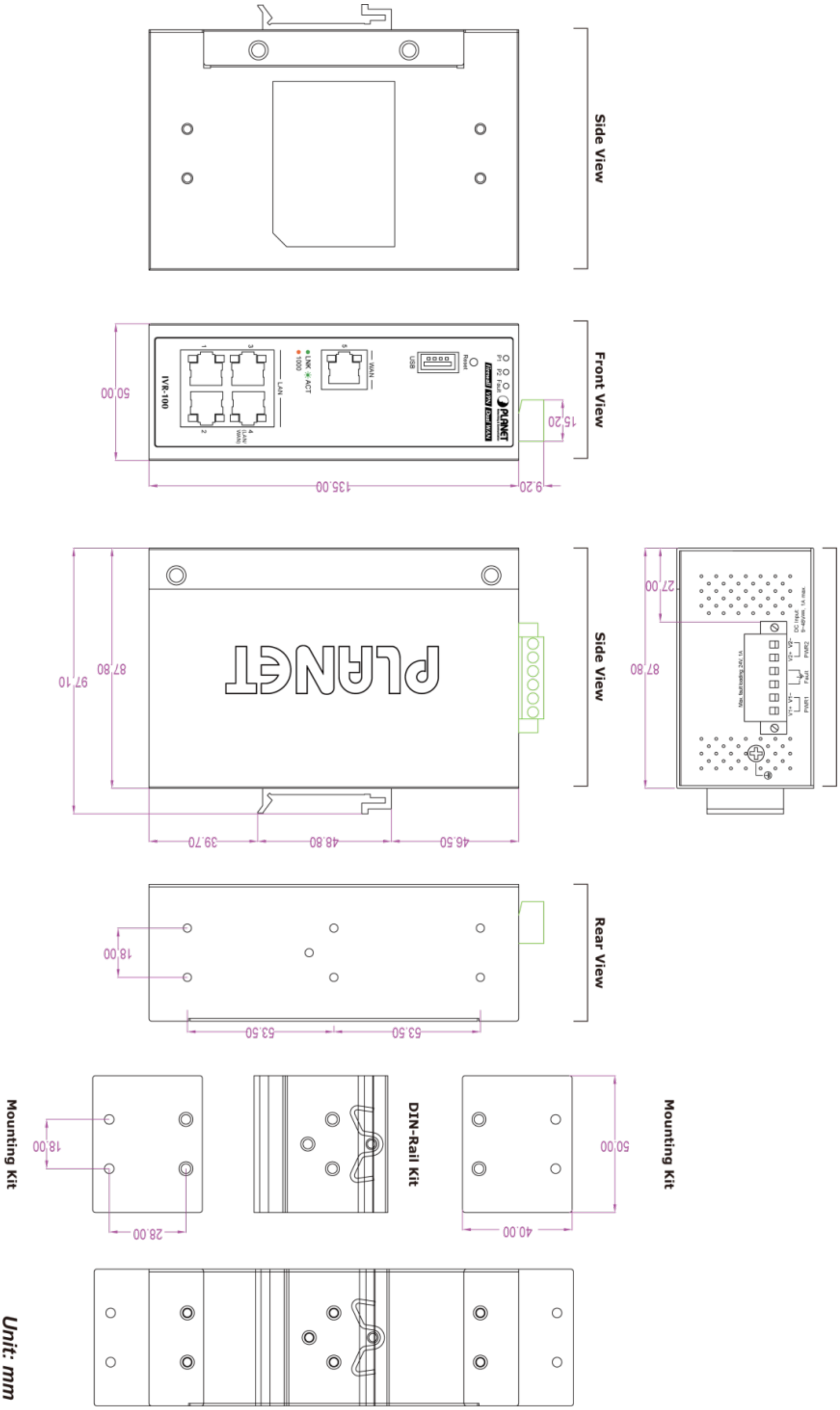

1
2
3
4
5
6
Fault Alarm Contacts
Fault
The Fault Alarm Contacts are energized (CLOSE) for normal operation and will OPEN when failure occurs

Insert the wires into the fault alarm contacts

Note

1. The wire gauge for the terminal block should be in the range between 12 and 24 AWG.
2. Alarm relay circuit accepts up to 24V, max. 1A currents.

2.1.5 Dimensions



2.2 Hardware Installation

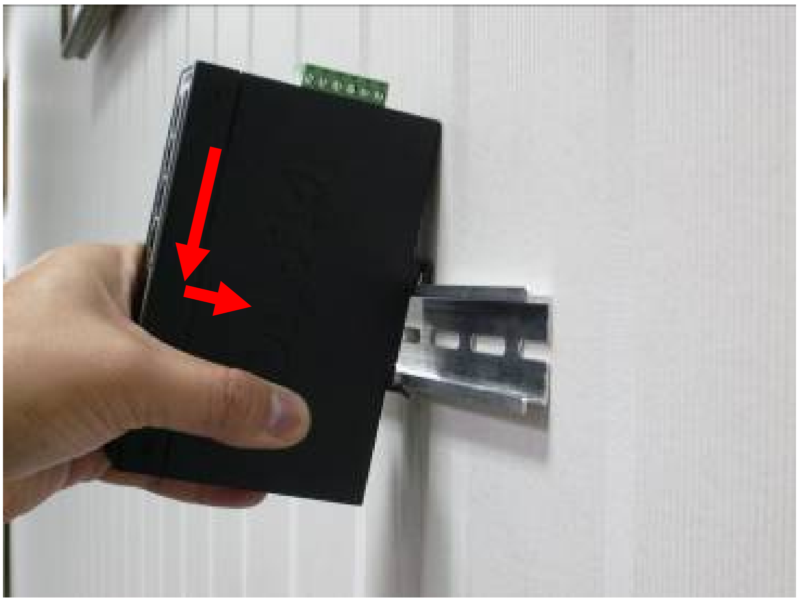
This section describes how to install the Industrial Gateway. There are three methods to install the Industrial Gateway -- DIN-rail mounting, wall mounting and side wall mounting. Basic knowledge of networking is assumed.

Please read the following sections and perform the procedures in the order being presented.

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

2.2.1 DIN-rail Mounting

Step 1: Lightly slide the DIN-rail into the track.



Step 2: Check whether the DIN-rail is tightly on the track.

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.

Note

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).

Note

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).

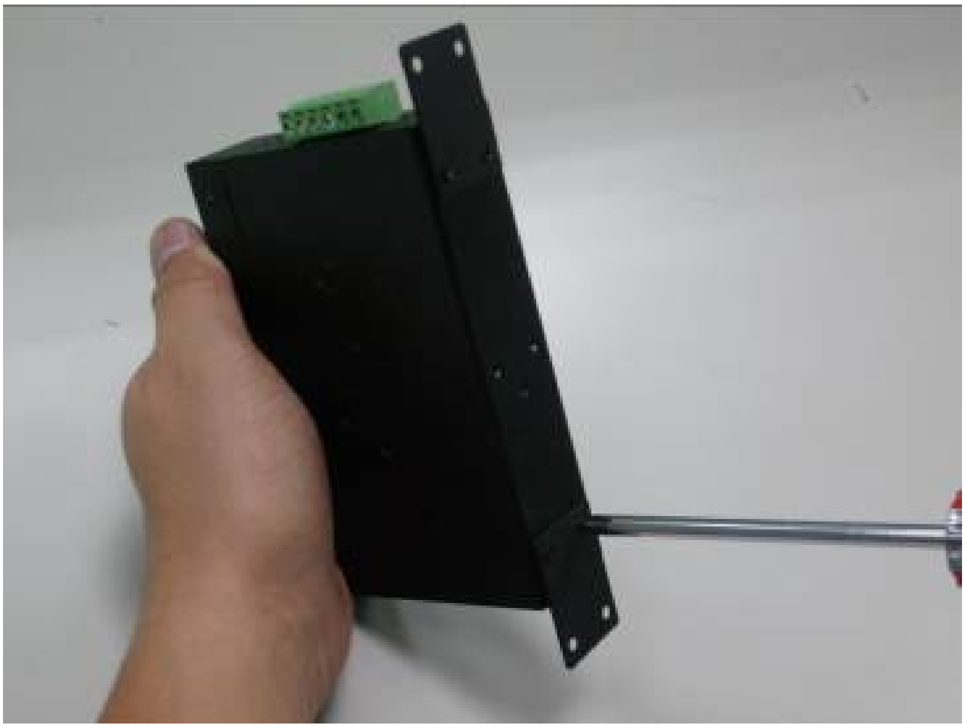
Step 5: Power on the device. When the device receives power, the Power LED should remain solid Green.

2.2.2 Wall Mount Plate Mounting

To install the Industrial Gateway on the wall, please follow the instructions below.

Step 1: Remove the DIN-rail from the Industrial Gateway. Use the screwdriver to loosen the screws to remove the DIN-rail.

Step 2: Place the wall-mount plate on the rear panel and use the screwdriver to screw the wall mount plate tightly on the Industrial Gateway.



Step 3: Use the hook holes at the corners of the wall mount plate to hang the Industrial Gateway on the wall.

Step 4: To remove the wall mount plate, reverse the steps above.

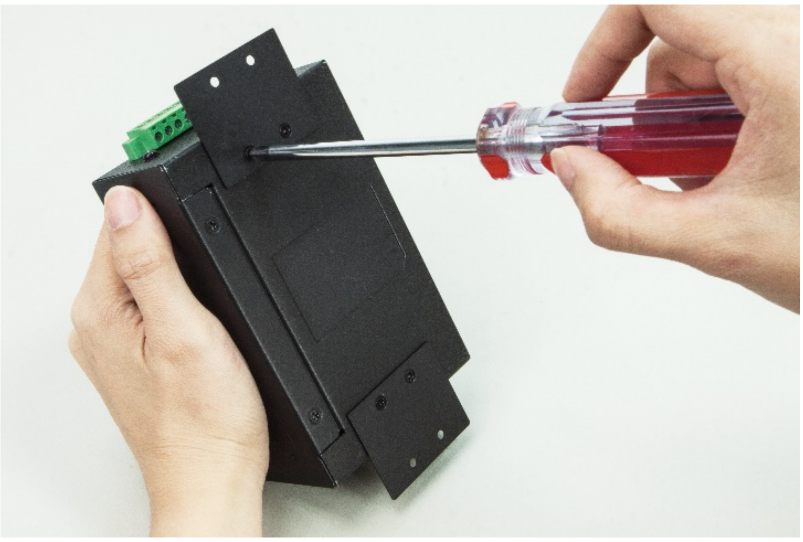
Step 5: Proceed with Steps 3, 4 and 5 in Section 2.2.1 DIN-rail Mounting to connect the network cabling and power on the device.

2.2.4 Side Wall Mount Plate Mounting

To install the Industrial Gateway on the wall, please follow the instructions below.

Step 1: Remove the DIN-rail from the Industrial Gateway. Use the screwdriver to loosen the screws to remove the DIN-rail.

Step 2: Place the wall-mount plate on the side panel and use the screwdriver to screw the wall mount plate tightly on the Industrial Gateway.



Step 3: Use the hook holes at the corners of the wall mount plate to hang the Industrial Gateway on the wall.

Step 4: To remove the wall mount plate, reverse the steps above.

Step 5: Proceed with Steps 3, 4 and 5 in Section 2.2.1 DIN-rail Mounting 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.

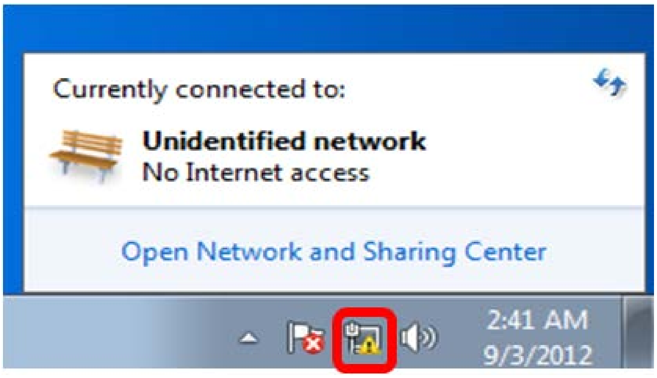
3.2 Setting TCP/IP on your PC

The default IP address of the VPN Gateway 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 VPN Gateway.
Please refer to the following to set the IP address of the connected PC.

3.2.1 Windows 7/8

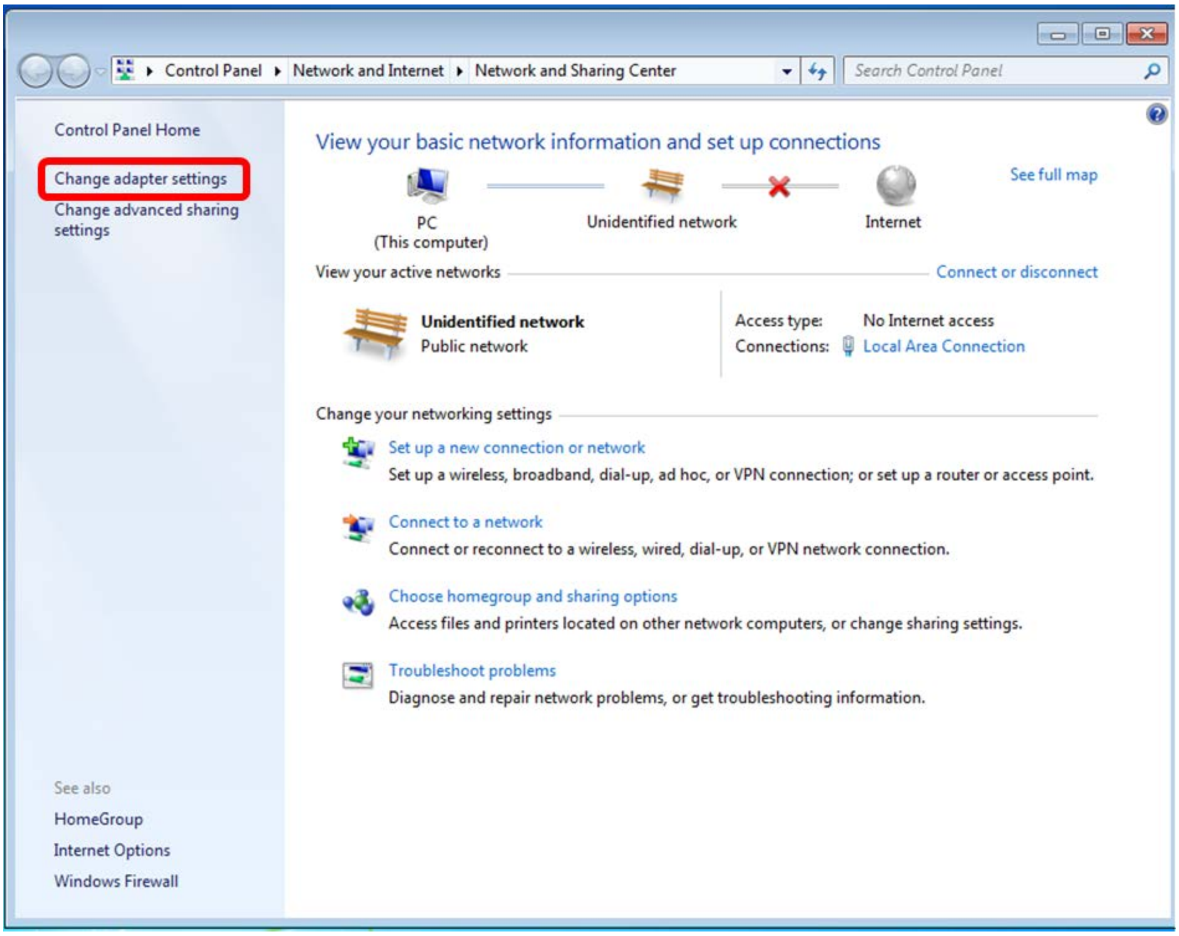
If you are using Windows 7/8, please refer to the following:

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



Currently connected to:
Unidentified network
No Internet access

2. Click "**Change adapter settings**".



View your basic network information and set up connections

View your active networks

Unidentified network Public network	Access type: No Internet access Connections: Local Area Connection

Change your networking settings

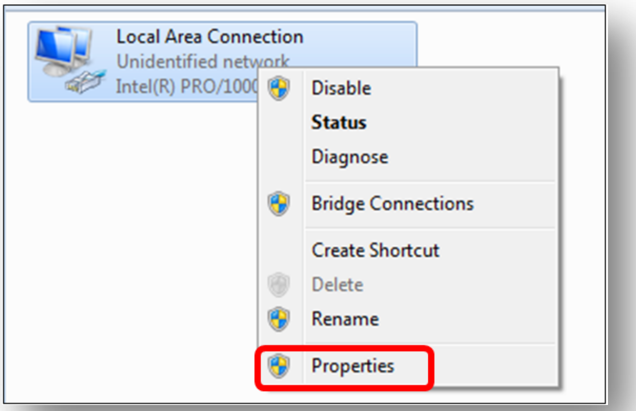
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

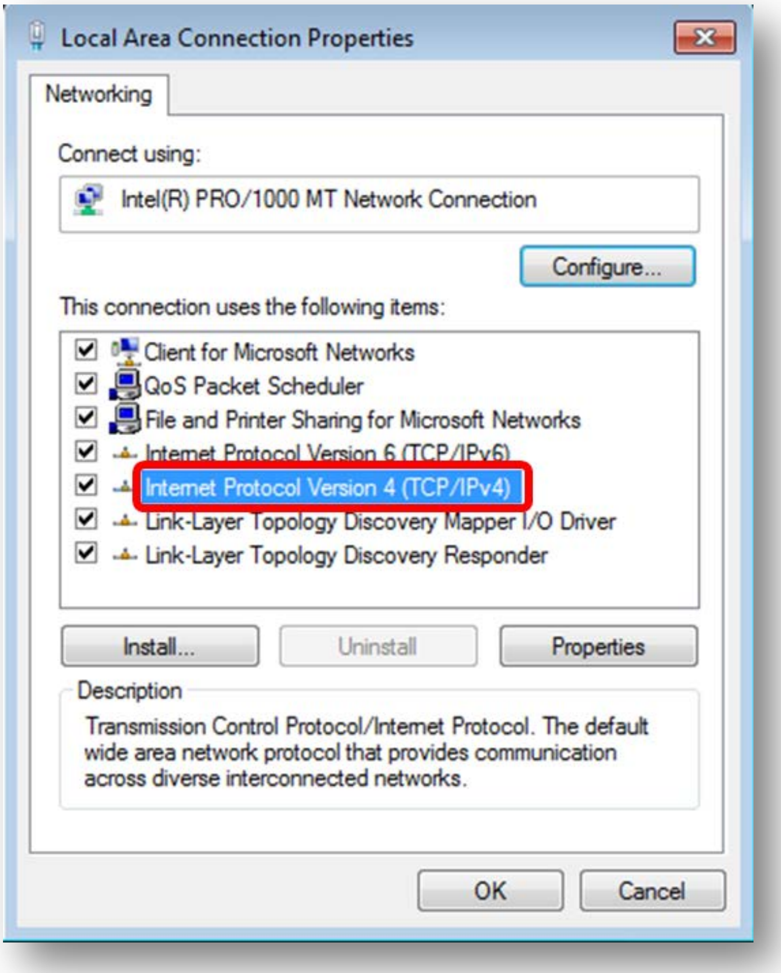
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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

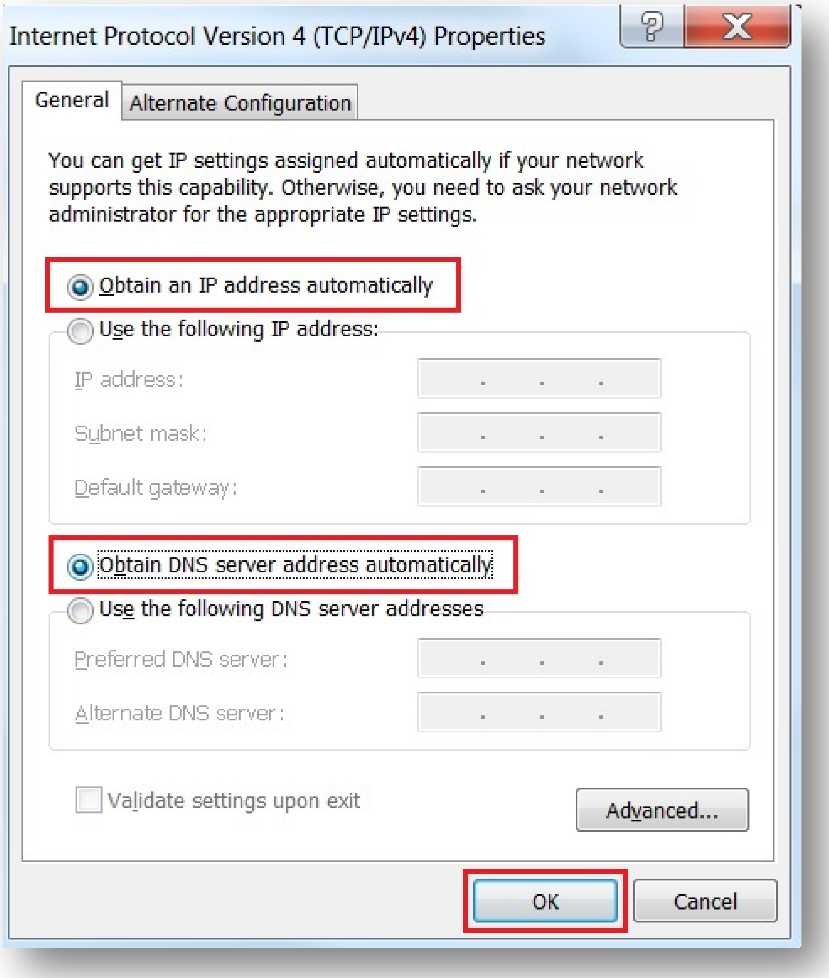


4. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).


Local Area Connection Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Network Connection
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
OK
Cancel

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses

Preferred DNS server: . . .

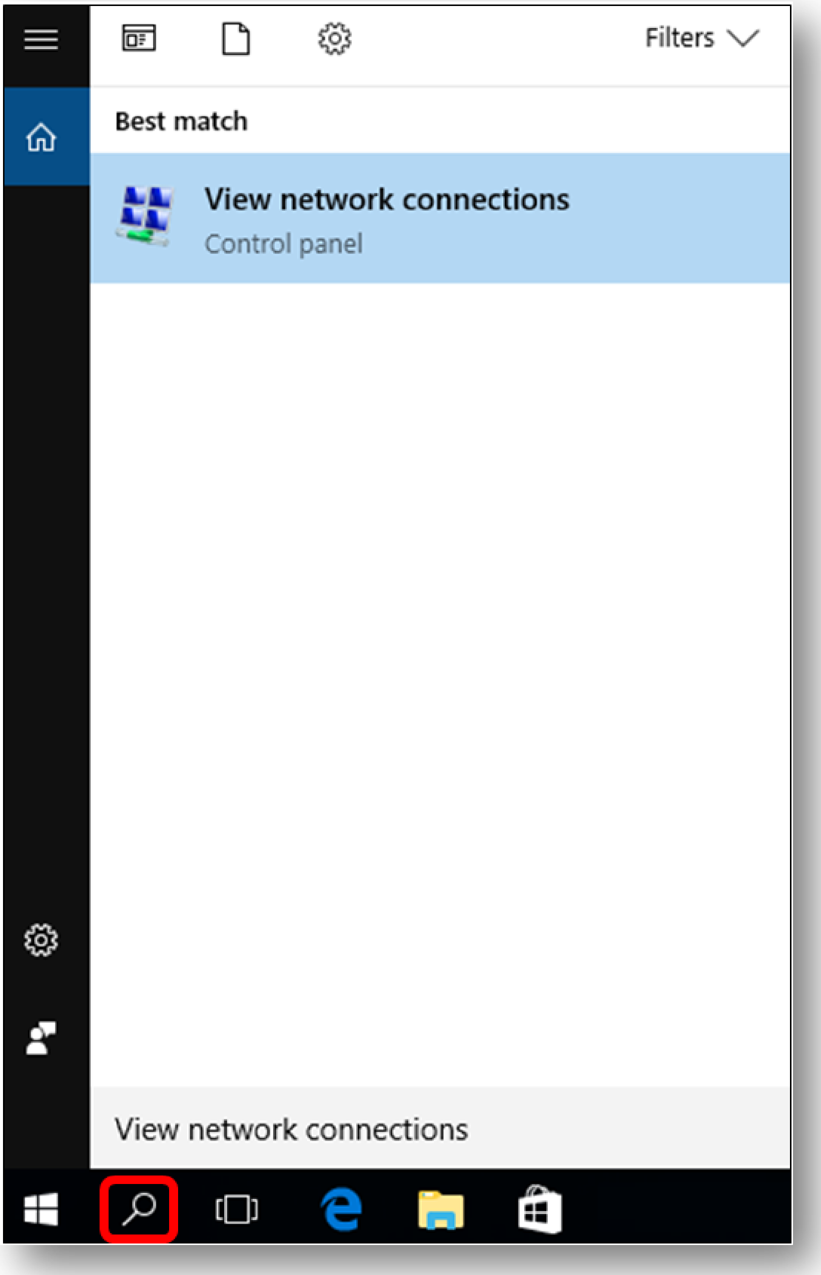
Alternate DNS server: . . .

□ Validate settings upon exit

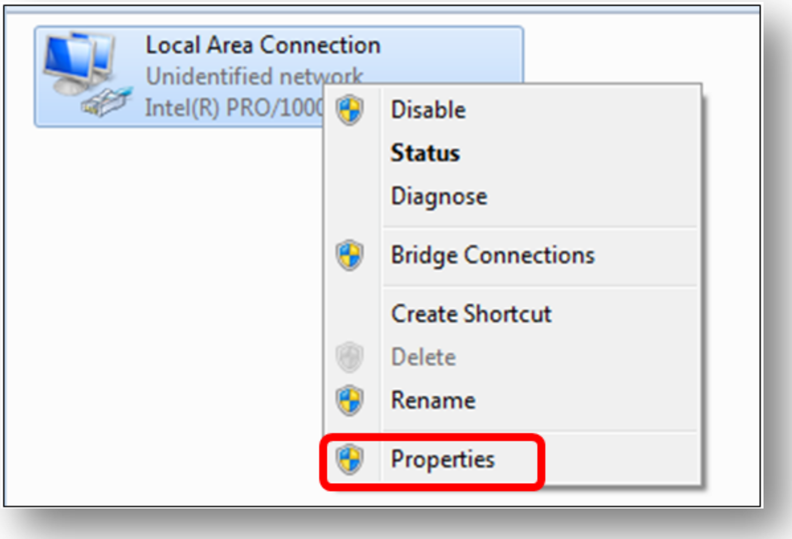
3.2.2 Windows 10

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

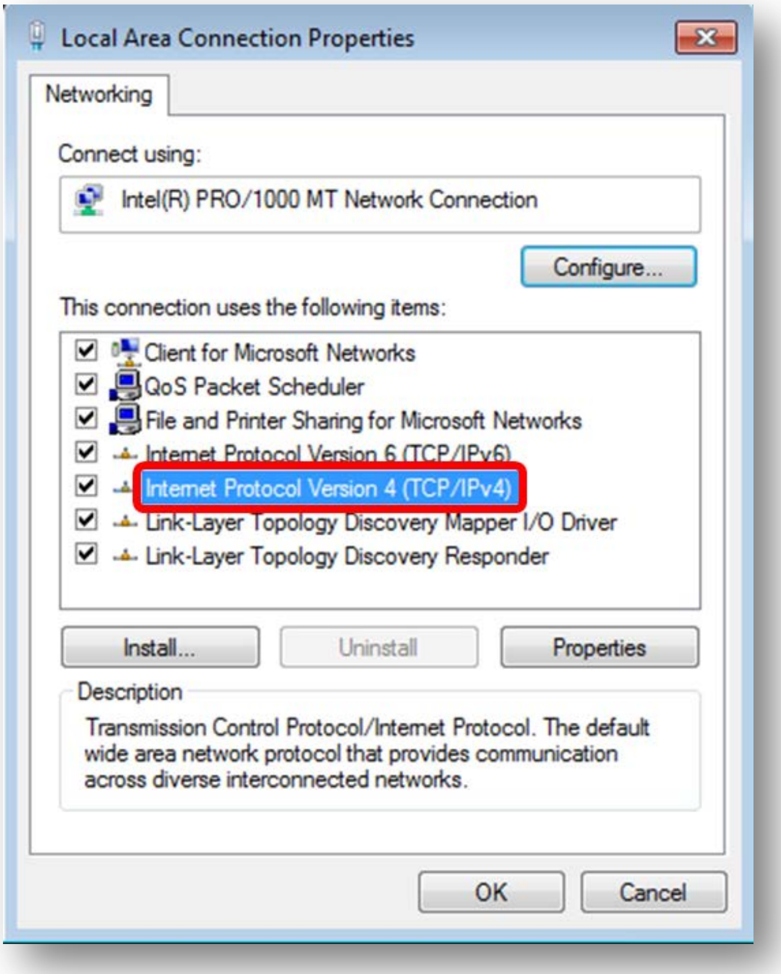
1. In the search box on the taskbar, type "View network connections", and then select View network connections at the top of the list.



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).



Connect using:

Intel(R) PRO/1000 MT Network Connection

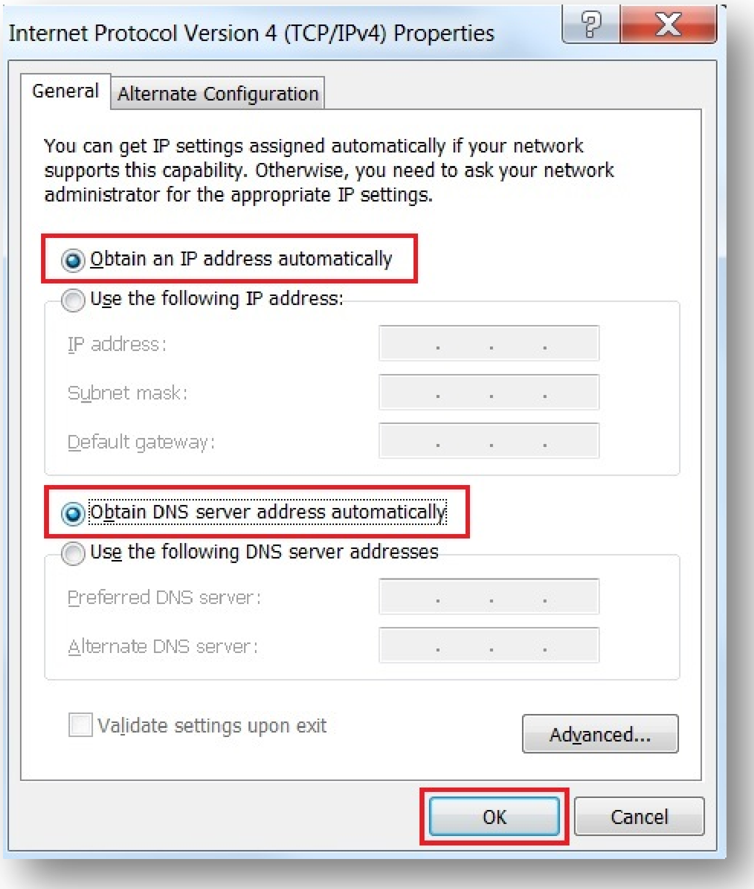
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses

Preferred DNS server: . . .
Alternate DNS server: . . .

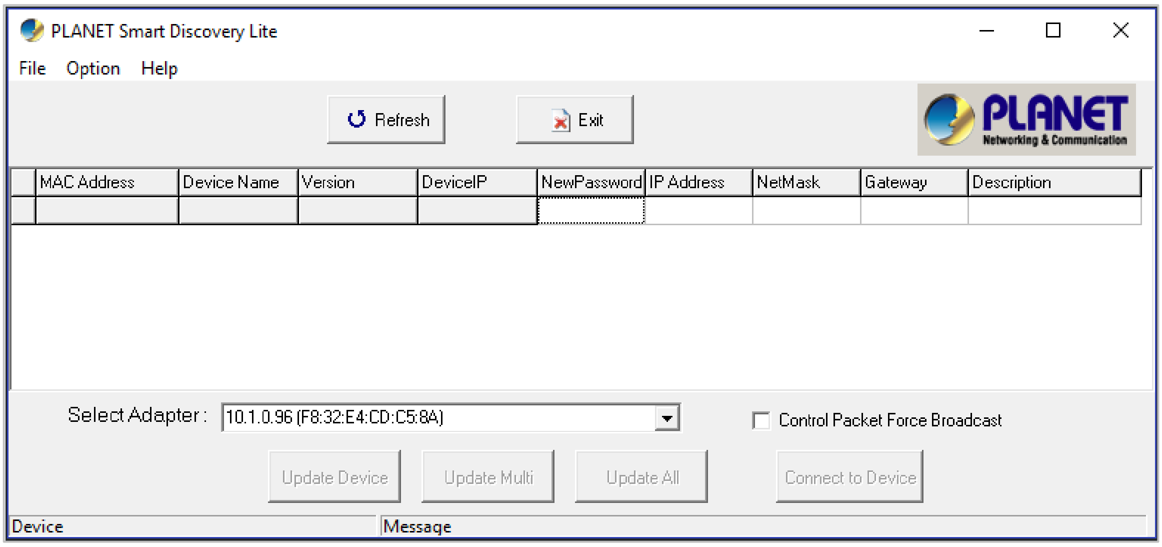
□ Validate settings upon exit

3.3 Planet Smart Discovery Utility

For easily listing the Gateway 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.



	MAC Address	Device Name	Version	DeviceIP	NewPassword	IP Address	NetMask	Gateway	Description

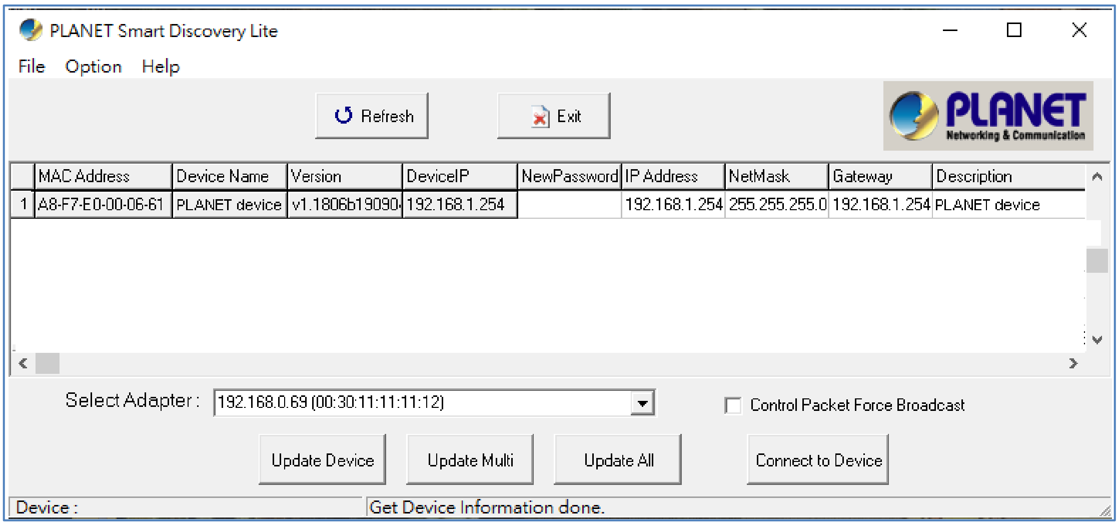
Select Adapter : 10.1.0.96 (F8:32:E4:CD:C5:8A)

□ Control Packet Force Broadcast

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:



	MAC Address	Device Name	Version	DeviceIP	NewPassword	IP Address	NetMask	Gateway	Description
1	A8-F7-E0-00-06-61	PLANET device	v1.1806b19090	192.168.1.254		192.168.1.254	255.255.255.0	192.168.1.254	PLANET device

Select Adapter : 192.168.0.69 (00:30:11:11:11:12)

□ Control Packet Force Broadcast

Device :

Get Device Information done.

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 Gateway

Refer to the steps below to configure the VPN Gateway:

Step 1. Connect the IT administrator's PC and VPN Gateway'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.

Note

The DHCP server of the VPN Gateway is enabled. Therefore, the LAN PC will get IP from the VPN Gateway. 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**

Note

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.

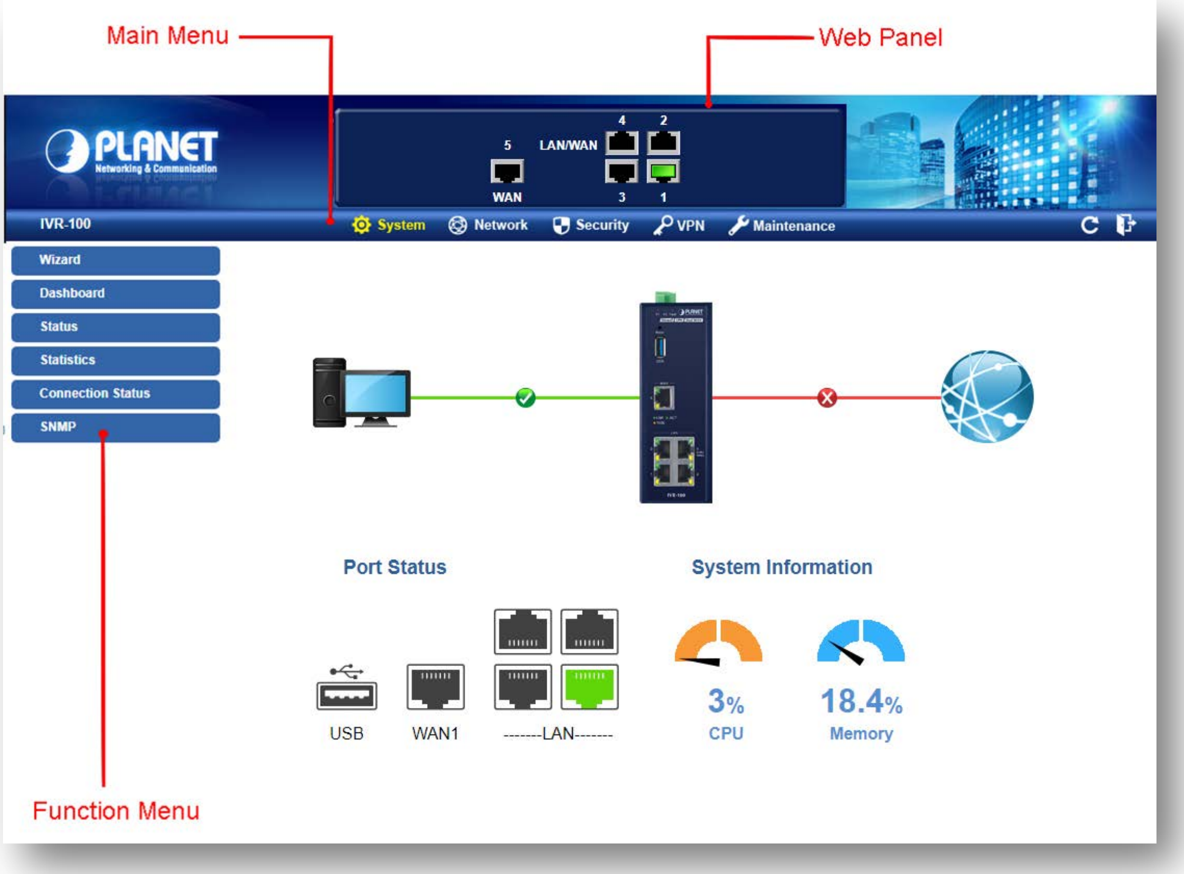


Figure 4-1: Main Web Page

■ Web Panel

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

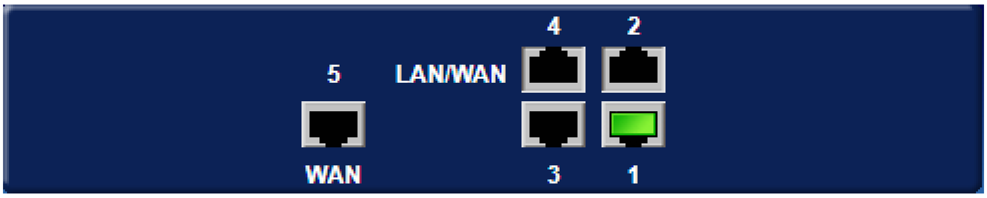


Figure 4-2: Web Panel

Object	Icon	Function
Ethernet port	⬛	To indicate the port without 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.

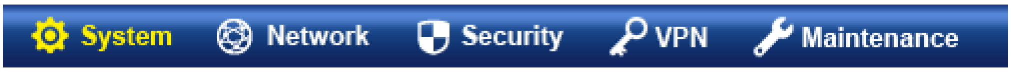


Figure 4-3: Function Menu

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

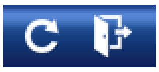


Figure 4-4: Function Button

Object	Description
↻	Click the "**Refresh button**" to refresh the current web page.
⇥	Click the "**Logout button**" to log out the web UI of the Gateway.

4.4 System

Use the System menu items to display and configure basic administrative details of the Gateway. The System menu shown in Figure 4-5 provides the following features to configure and monitor system.

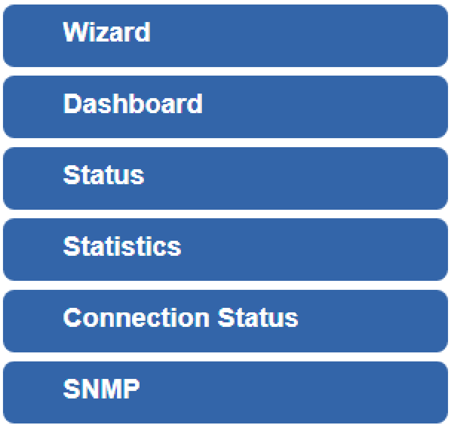


Figure 4-5: System Menu

Object	Description
Wizard	The Wizard will guide the user to configuring the Gateway 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 Gateway 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 Gateway via **Setup Wizard** as shown in Figure 4-6.

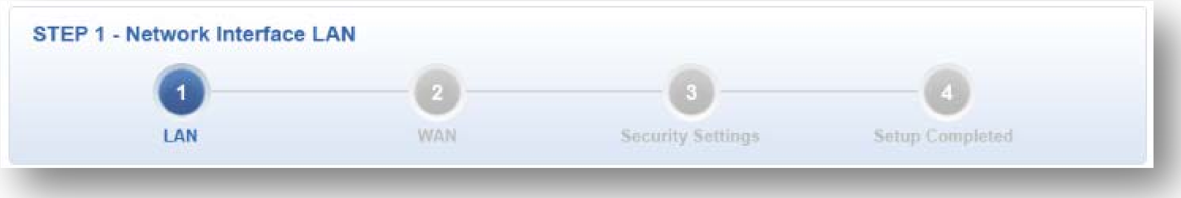
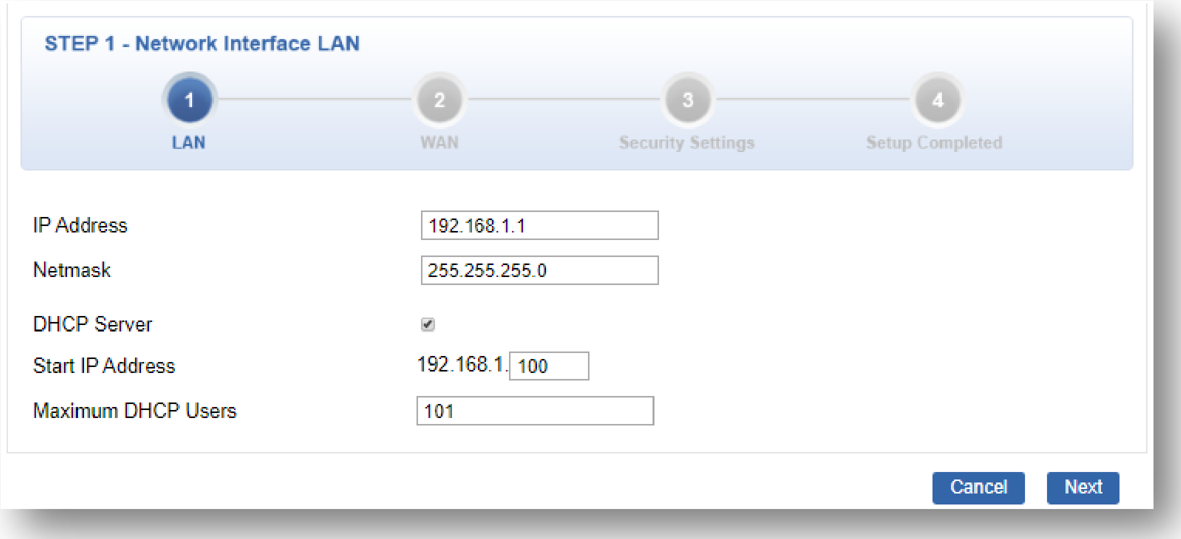


Figure 4-6: Setup Wizard

Step 1: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in Figure 4-7.



IP Address 192.168.1.1

Netmask 255.255.255.0

DHCP Server ☑

Start IP Address 192.168.1. 100

Maximum DHCP Users 101

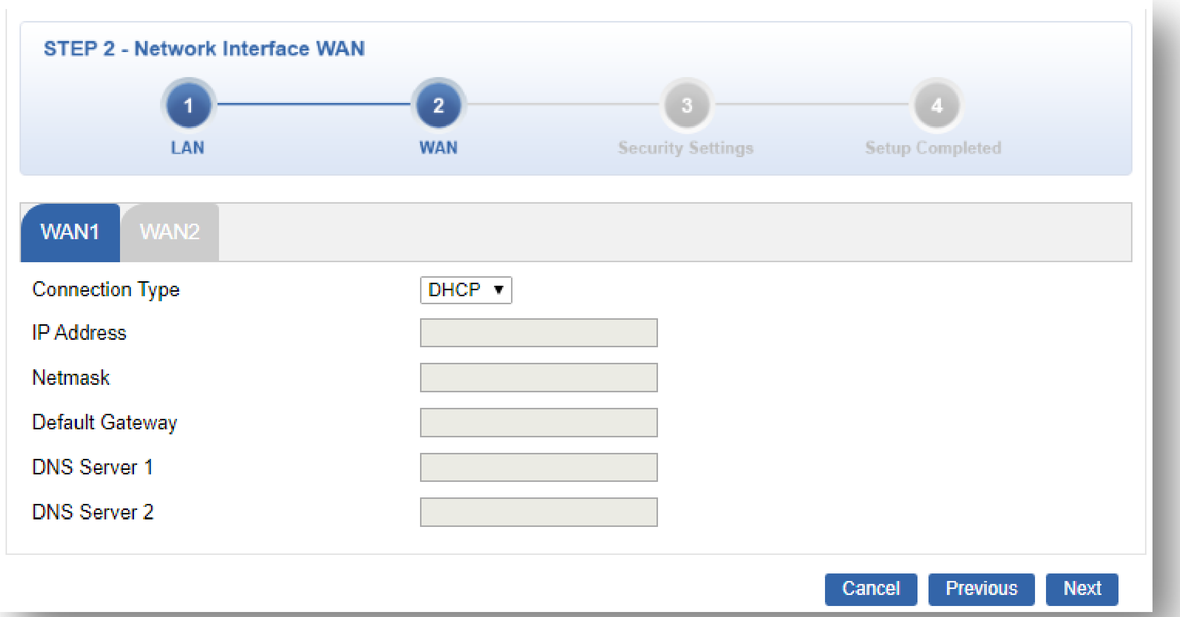
Figure 4-7: Setup Wizard – LAN Configuration

Object	Description
IP Address	Enter the IP address of your Gateway. 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 Gateway.
Maximum DHCP Users	By default, the maximum DHCP users are 101, which mean the Gateway 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 Gateway supports two access modes on the WAN side shown in Figure 4-8



Connection Type DHCP ▾

IP Address

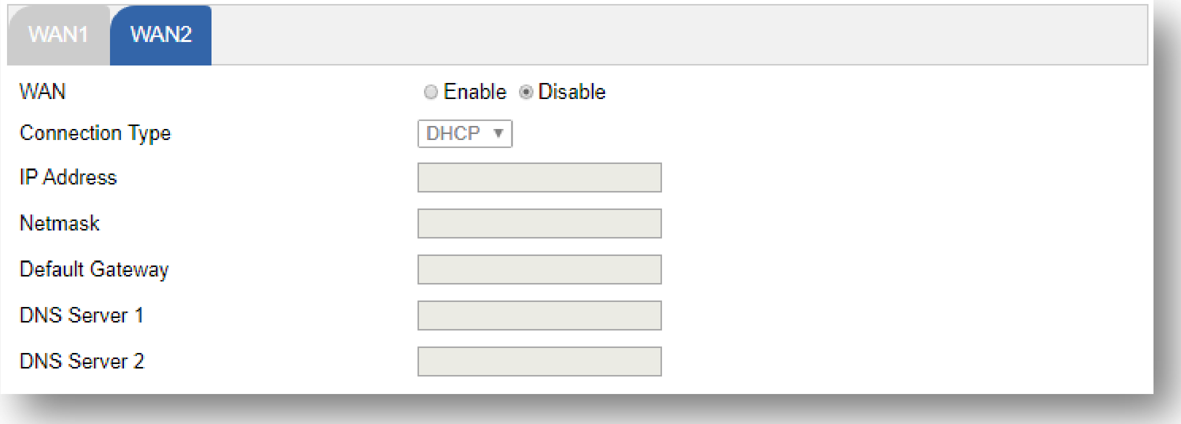
Netmask

Default Gateway

DNS Server 1

DNS Server 2

Figure 4-8: Setup Wizard – WAN 1 Configuration

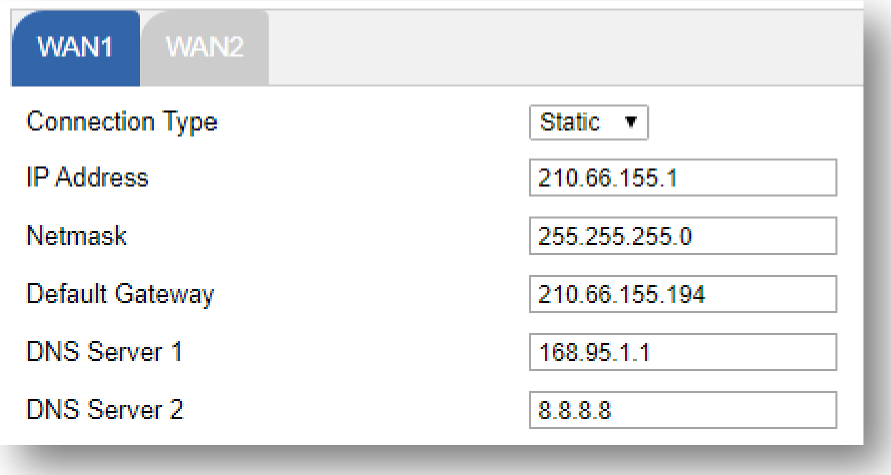


WAN ○ Enable ● Disable
Connection Type DHCP
IP Address
Netmask
Default Gateway
DNS Server 1
DNS Server 2

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 Gateway will not accept the IP address if it is not in this format. The setup is shown in Figure 4-10.



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

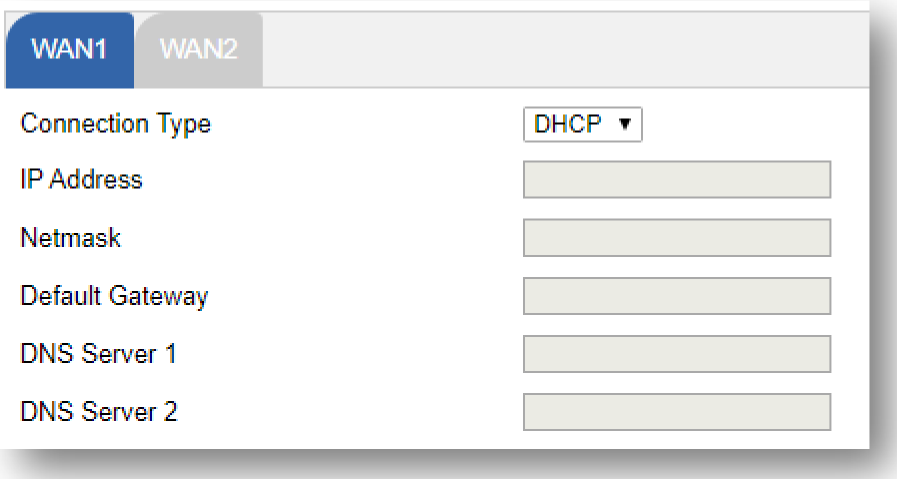
Figure 4-10: WAN Interface Setup – Static IP Setup

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.

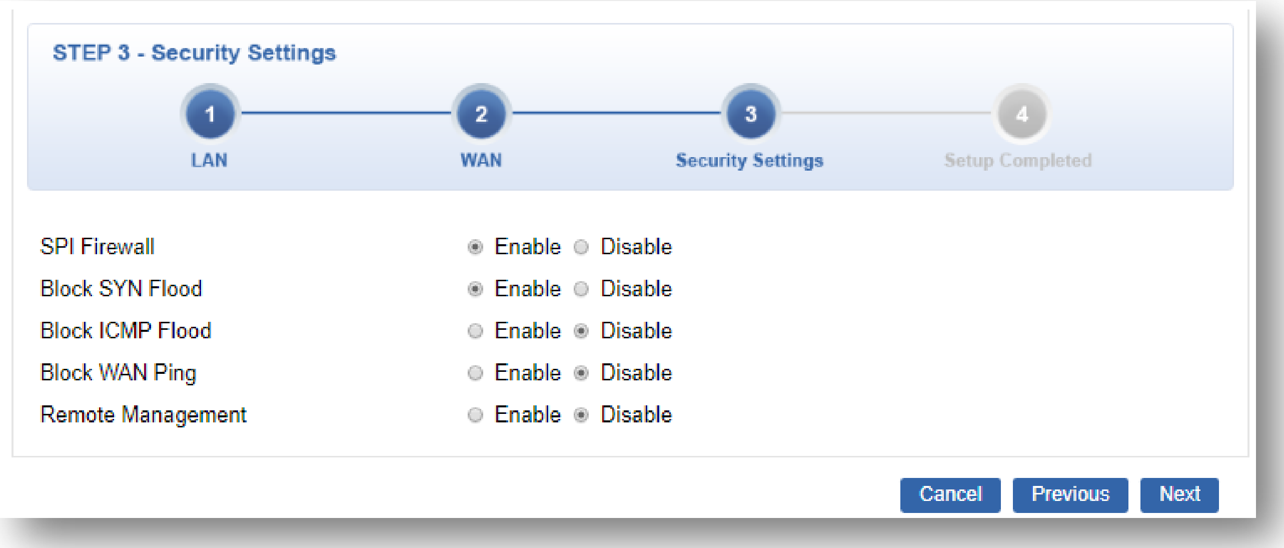


Connection Type	DHCP ▼
IP Address	
Netmask	
Default Gateway	
DNS Server 1	
DNS Server 2	

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

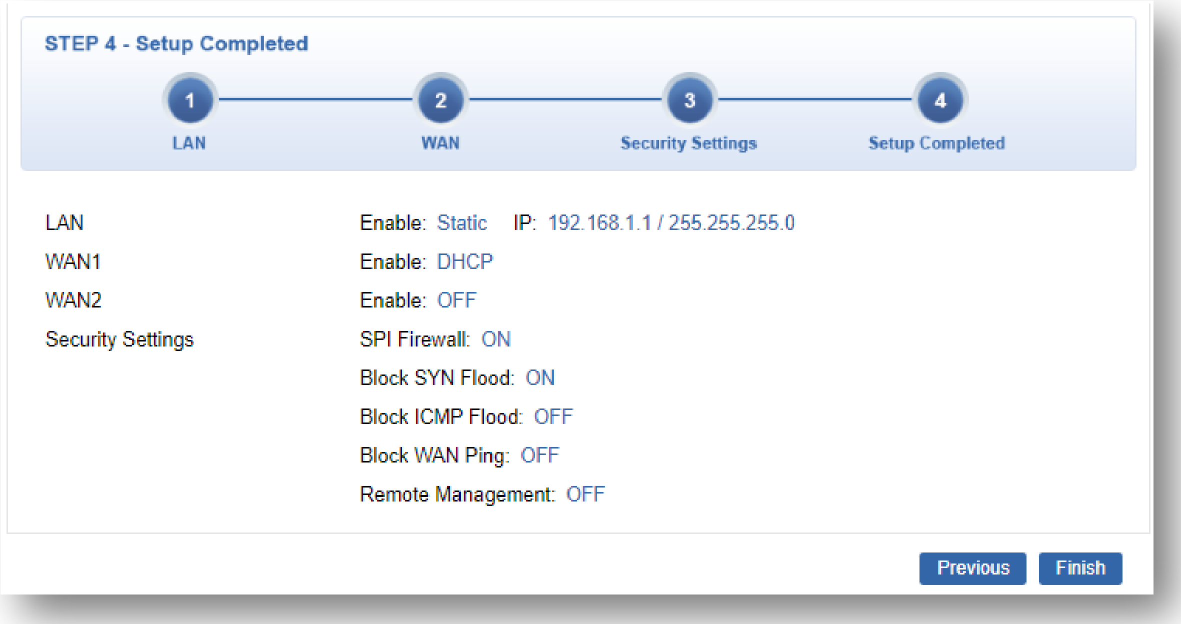
SPI Firewall	● Enable ○ Disable
Block SYN Flood	● Enable ○ Disable
Block ICMP Flood	○ Enable ● Disable
Block WAN Ping	○ Enable ● Disable
Remote Management	○ Enable ● Disable

Figure 4-12: Setup Wizard –Security Setting

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 ICMP Flood	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. The default configuration is disabled.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the Gateway from the Internet network. The default configuration is disabled.
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.

Step 4: Setup Completed

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



LAN Enable: Static IP: 192.168.1.1 / 255.255.255.0

WAN1 Enable: DHCP

WAN2 Enable: OFF

Security Settings SPI Firewall: ON

Block SYN Flood: ON

Block ICMP Flood: OFF

Block WAN Ping: OFF

Remote Management: OFF

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.

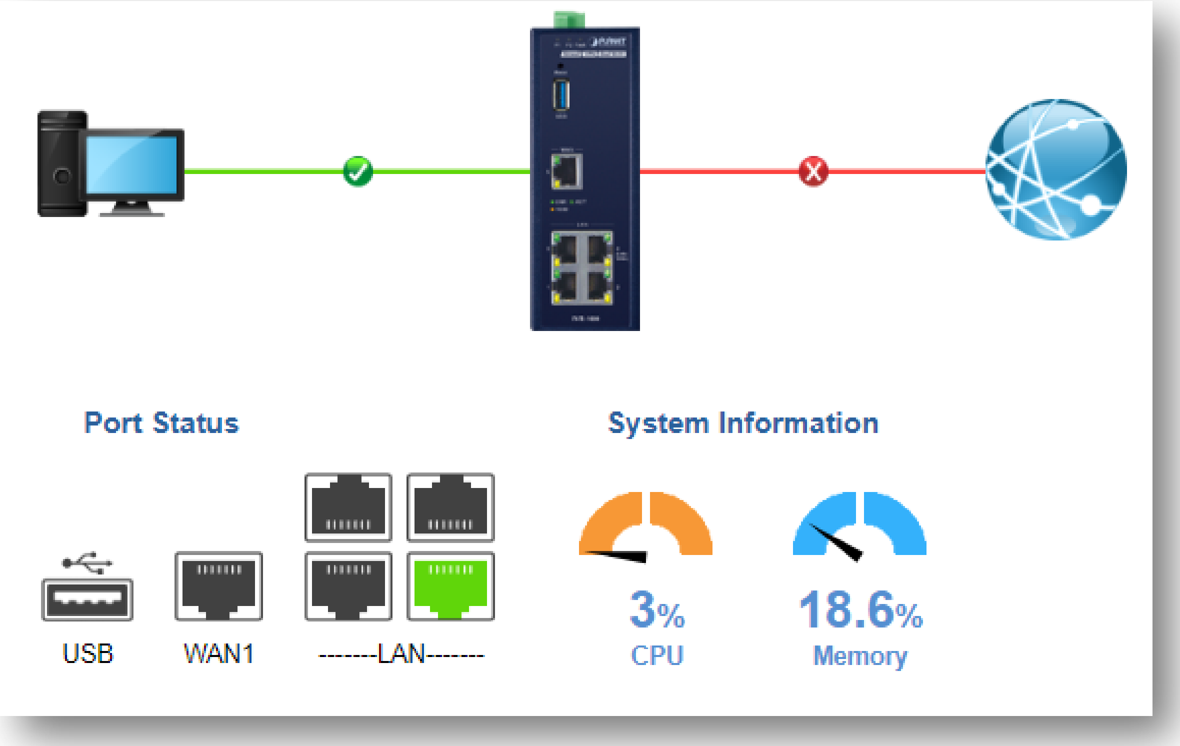
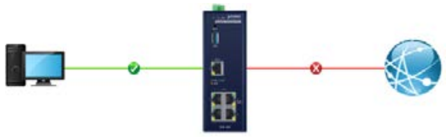
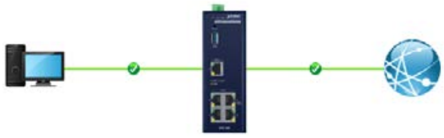
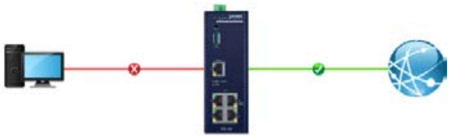


Figure 4-14: Dashboard

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

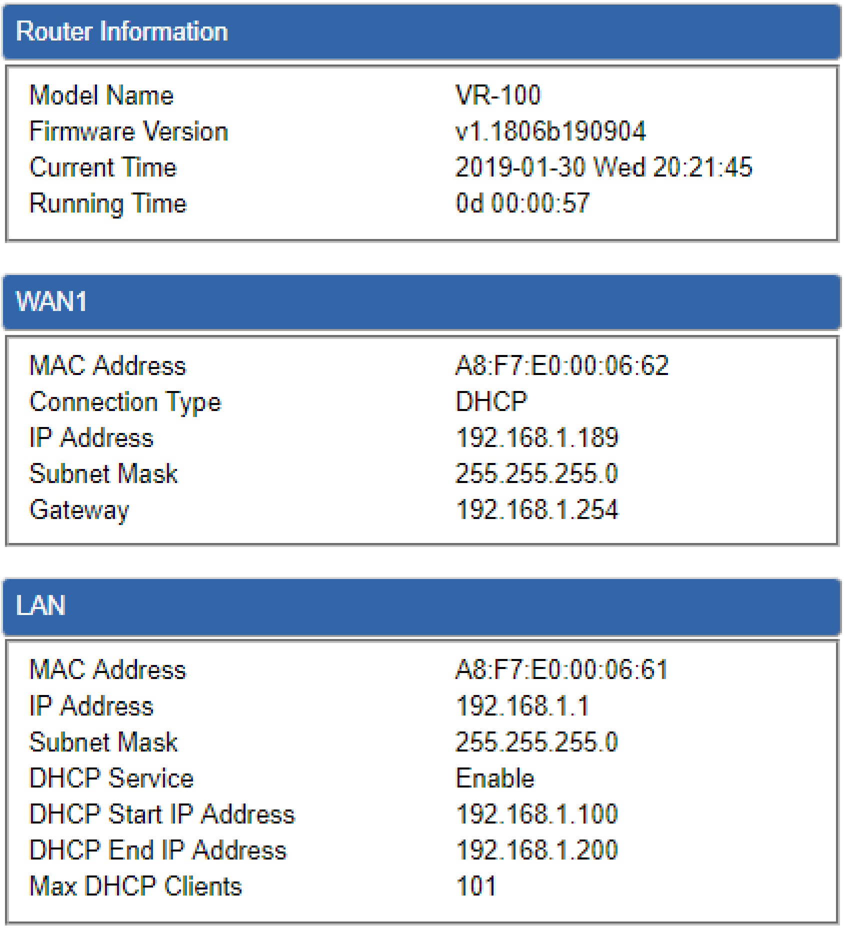
Object	Description
🟩	Ethernet port is in use.
⬛	Ethernet port is not in use.
🟩	USB port is in use.
⬛	USB port is not in use.

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 Gateway on the WAN and LAN. The statistics are shown in Figure 4-16.

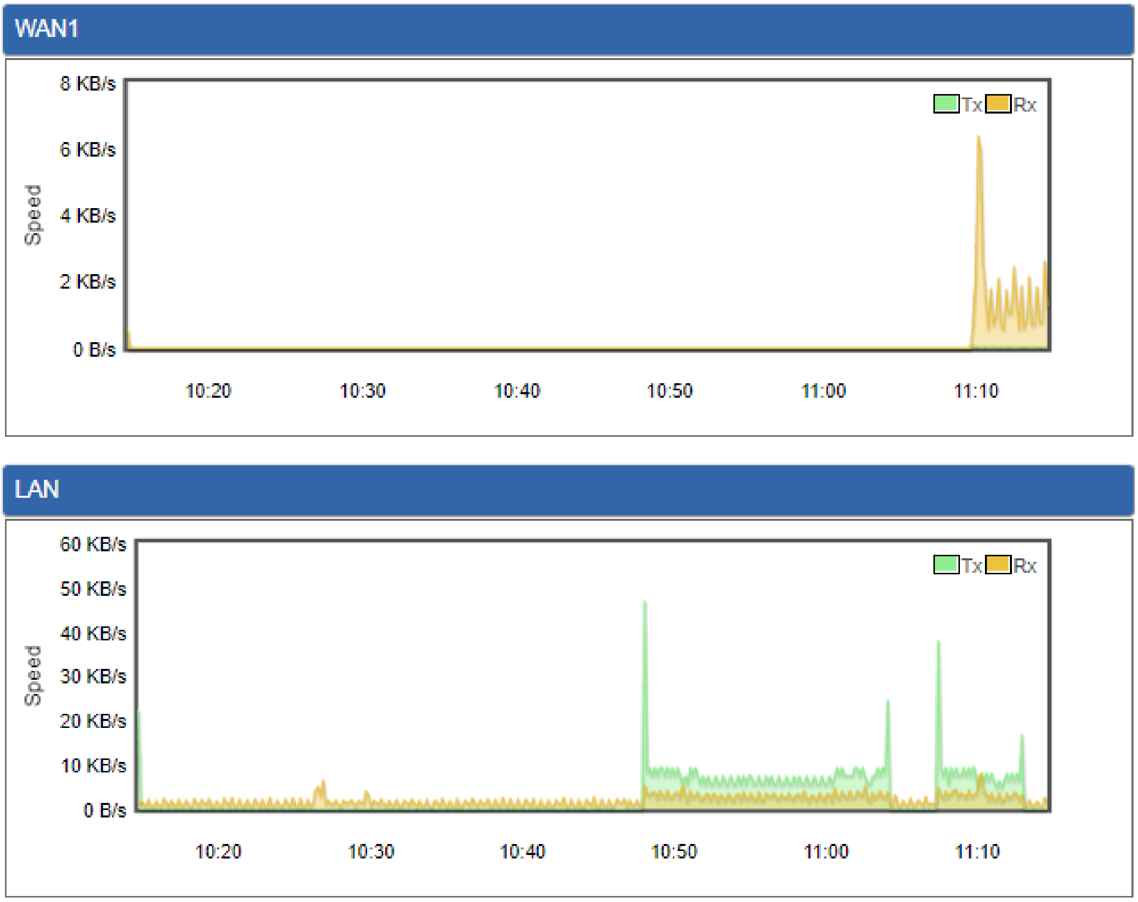
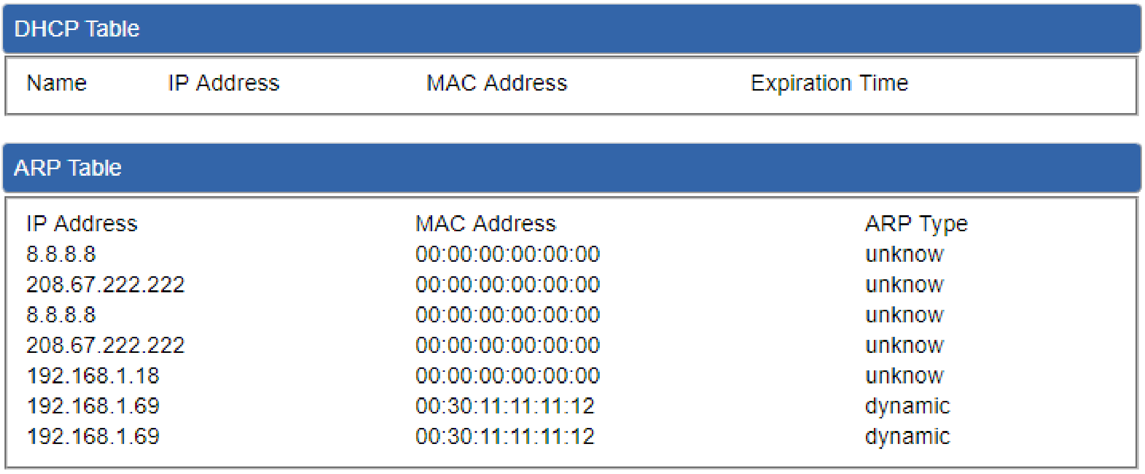


Figure 4-16: Statistics

4.4.5 Connection Status

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



DHCP Table

Name	IP Address	MAC Address	Expiration Time

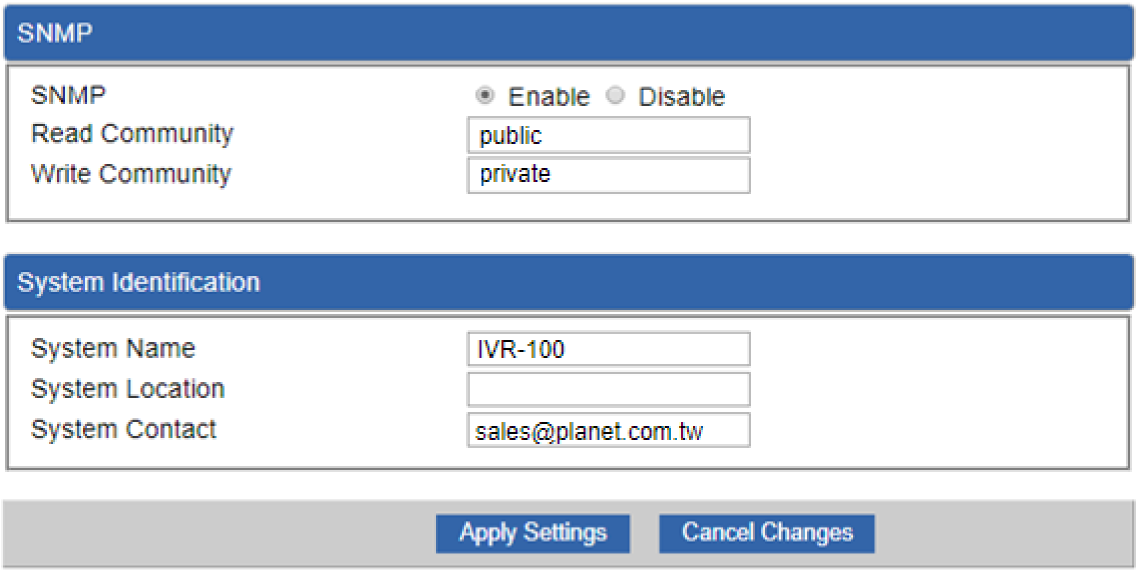
ARP Table

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 Gateway as shown in Figure 4-18.



SNMP

SNMP ● Enable ○ Disable

Read Community: public

Write Community: private

System Identification

System Name: IVR-100

System Location:

System Contact: 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 Gateway.
System Name	Allows entering characters for system name of the Gateway.
System Location	Allows entering characters for system location of the Gateway.
System Contact	Allows entering characters for system contact of the Gateway.
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 Gateway as shown in Figure 4-19.

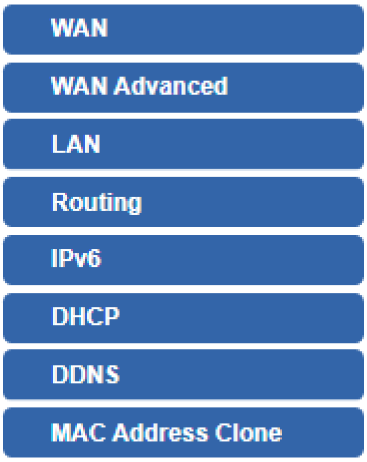
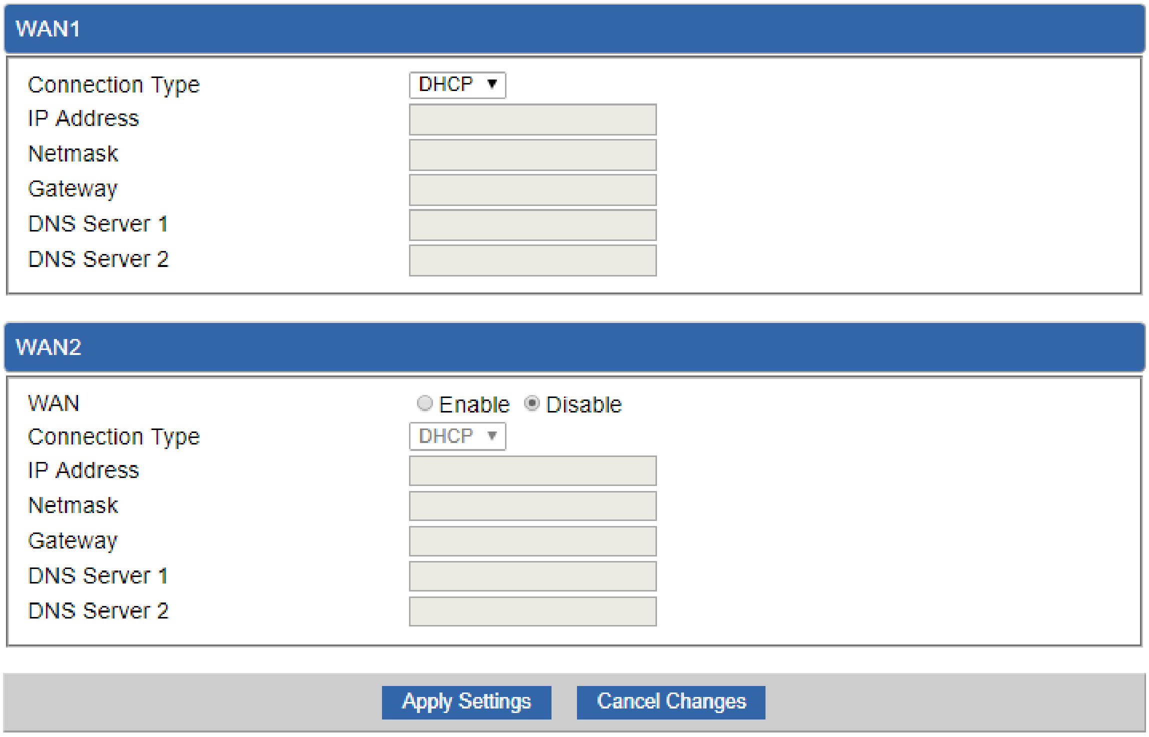


Figure 4-19: Network Menu

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 Gateway 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	DHCP ▾
IP Address	
Netmask	
Gateway	
DNS Server 1	
DNS Server 2	

WAN2

WAN	○ Enable ● Disable
Connection Type	DHCP ▾
IP Address	
Netmask	
Gateway	
DNS Server 1	
DNS Server 2	

Figure 4-20: WAN

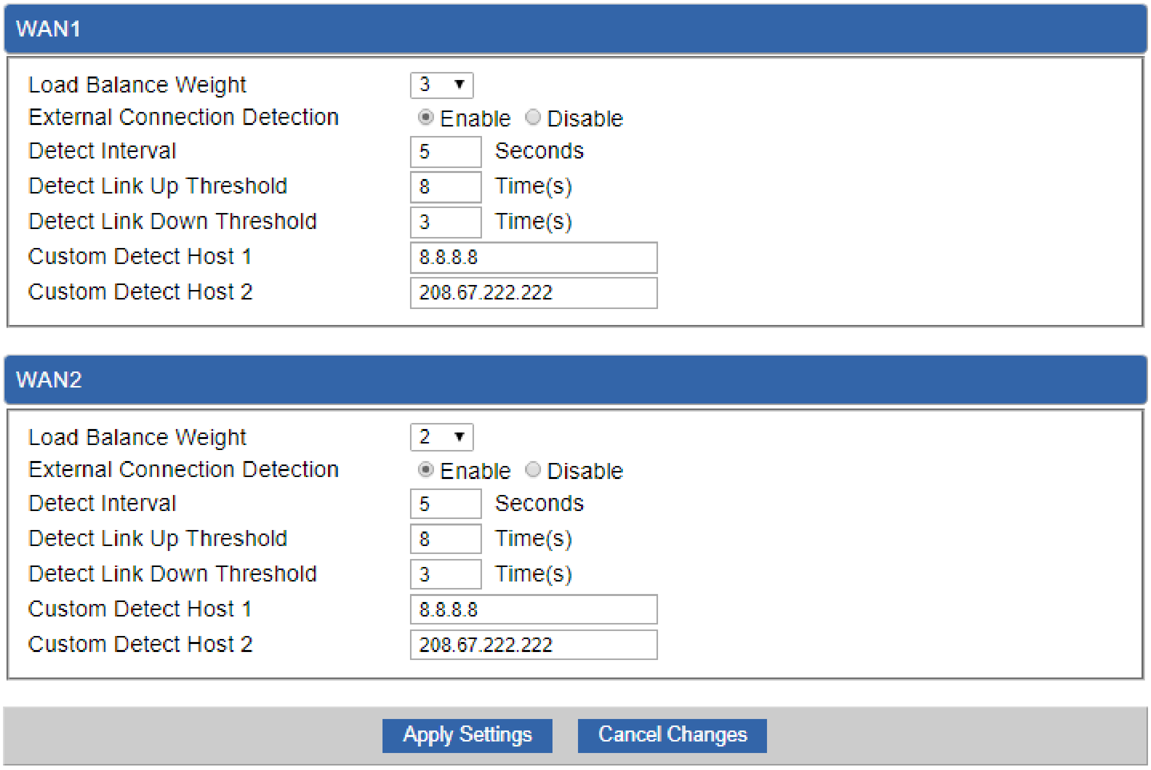
Object	Description	
WAN Access Type	Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.	
	Static	Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP. 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 Gateway will not accept the IP address if it is not in this format. **IP Address** Enter the IP address assigned by your ISP.

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

Note: WAN IP, whether obtained automatically or specified manually, should NOT be on the same IP net segment as the LAN IP; otherwise, the Gateway 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 Gateway 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	3 ▼	
External Connection Detection	● Enable ○ Disable	
Detect Interval	5	Seconds
Detect Link Up Threshold	8	Time(s)
Detect Link Down Threshold	3	Time(s)
Custom Detect Host 1	8.8.8.8	
Custom Detect Host 2	208.67.222.222	

WAN2

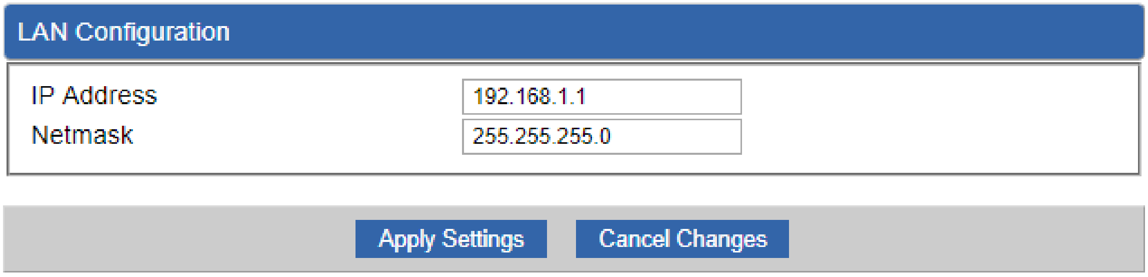
Load Balance Weight	2 ▼	
External Connection Detection	● Enable ○ Disable	
Detect Interval	5	Seconds
Detect Link Up Threshold	8	Time(s)
Detect Link Down Threshold	3	Time(s)
Custom Detect Host 1	8.8.8.8	
Custom Detect Host 2	208.67.222.222	

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 Gateway as shown in Figure 4-22. Here you may change the settings for IP address, subnet mask, DHCP, etc.



LAN Configuration

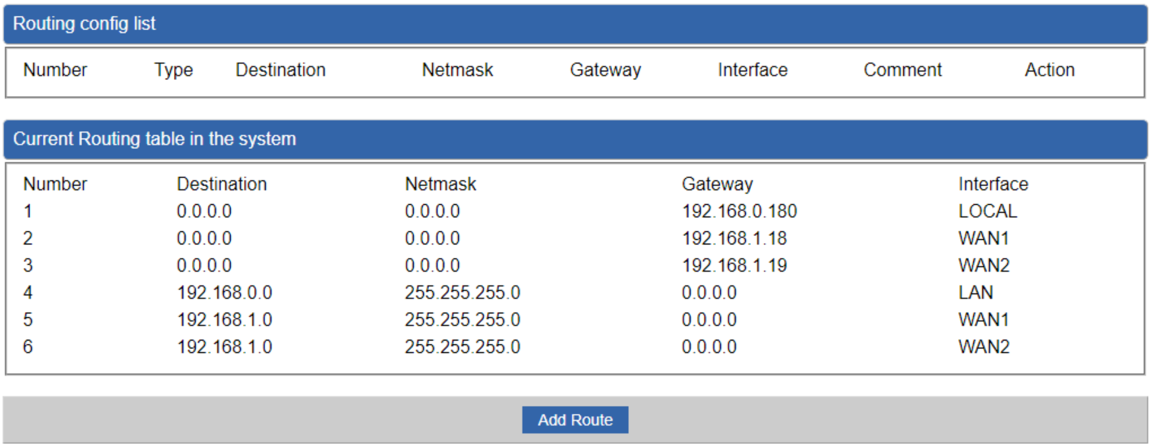
IP Address 192.168.1.1
Netmask 255.255.255.0

Figure 4-22: LAN Setup

Object	Description
IP Address	The LAN IP address of the Gateway 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.



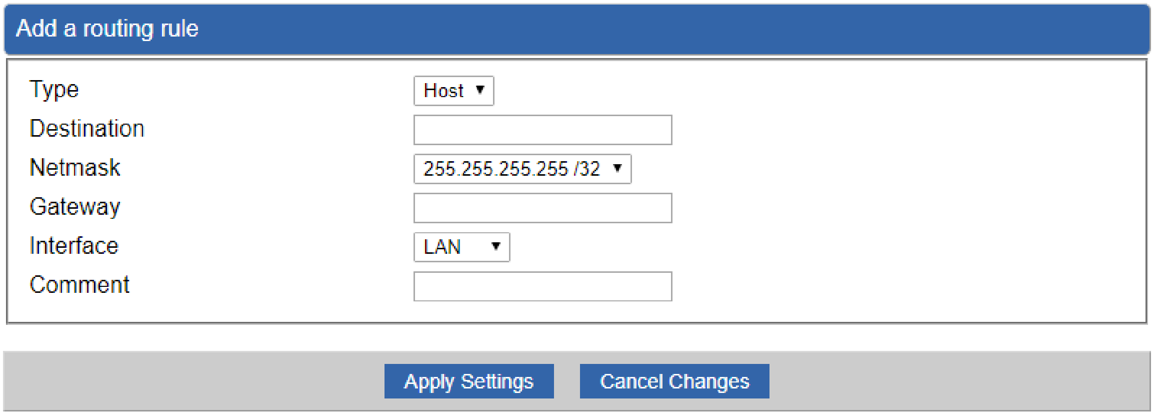
Routing config list

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

Figure 4-23: Routing table



Add a routing rule

Type	Host ▼
Destination	
Netmask	255.255.255.255 /32 ▼
Gateway	
Interface	LAN ▼
Comment	

Figure 4-24: Routing setup

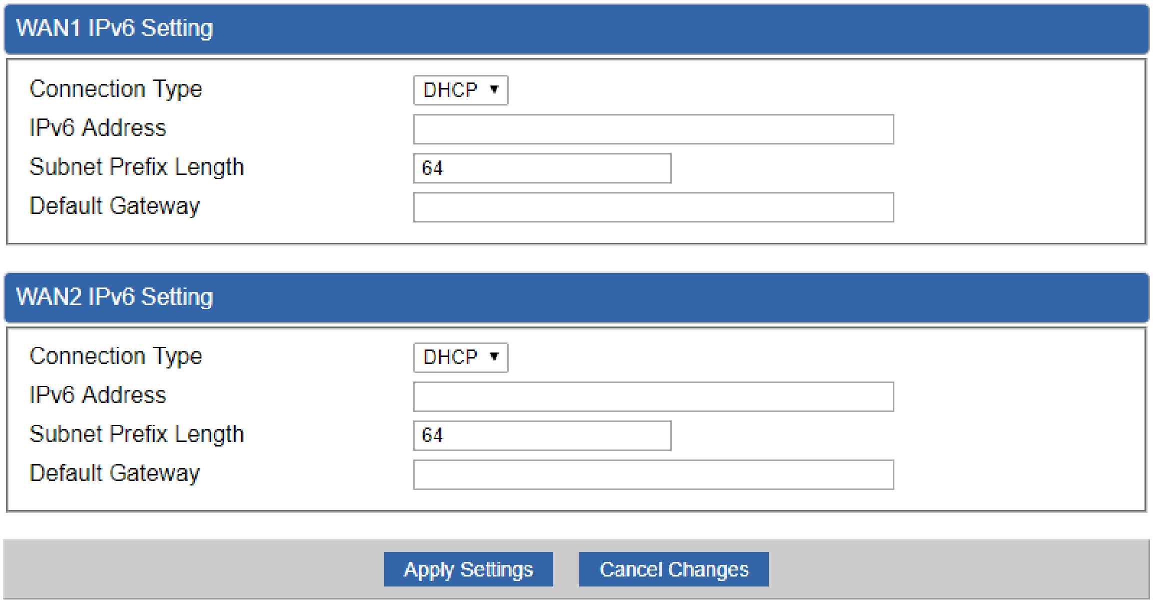
Routing tables contain a list of IP addresses. Each IP address identifies a remote router (or other network gateway) that the local router is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges 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 Gateway as shown in Figure 4-25. It allows you to enable IPv6 function and set up the parameters of the Gateway’s WAN. In this setting you may change WAN connection type and other settings.


WAN1 IPv6 Setting

Connection Type	DHCP ▼
IPv6 Address	
Subnet Prefix Length	64
Default Gateway	

WAN2 IPv6 Setting

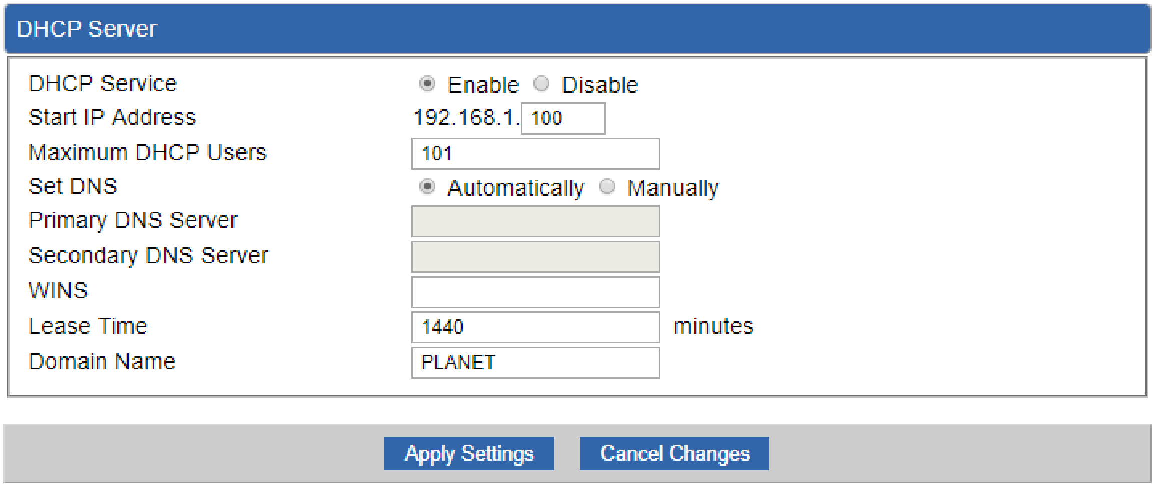
Connection Type	DHCP ▼
IPv6 Address	
Subnet Prefix Length	64
Default Gateway	

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	● Enable ○ Disable
Start IP Address	192.168.1. 100
Maximum DHCP Users	101
Set DNS	● Automatically ○ Manually
Primary DNS Server	
Secondary DNS Server	
WINS	
Lease Time	1440 minutes
Domain Name	PLANET

Figure 4-26: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the Gateway 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 Gateway.
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the Gateway 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 Gateway’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.

Object	Description
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 Gateway. Default is 1440 minutes.
Domain Name	Input a domain name for the Gateway. Default is Planet.

4.5.7 DDNS

The Gateway 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.

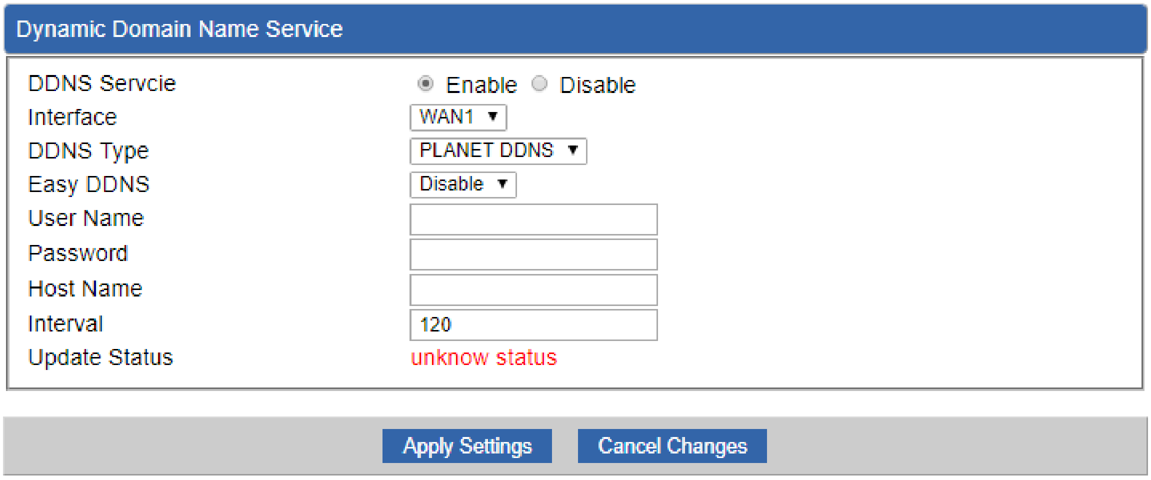
PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. 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 Gateway, 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 Gateway’s MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)



Dynamic Domain Name Service

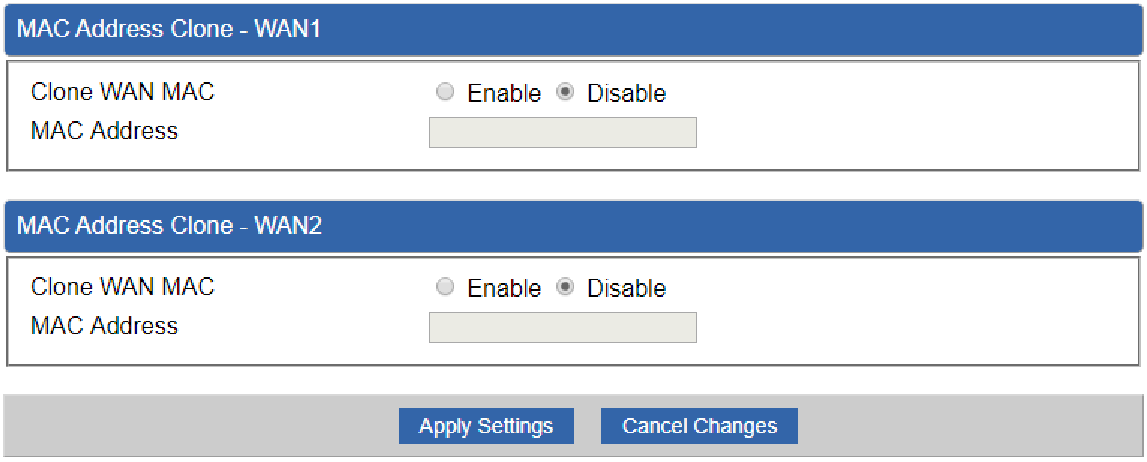
DDNS Servcie	● Enable ○ Disable
Interface	WAN1 ▼
DDNS Type	PLANET DDNS ▼
Easy DDNS	Disable ▼
User Name	
Password	
Host Name	
Interval	120
Update Status	unknow status

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: 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.



MAC Address Clone - WAN1

Clone WAN MAC ○ Enable ● Disable

MAC Address

MAC Address Clone - WAN2

Clone WAN MAC ○ Enable ● Disable

MAC Address

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.

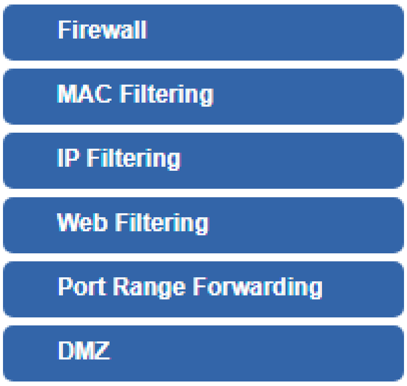
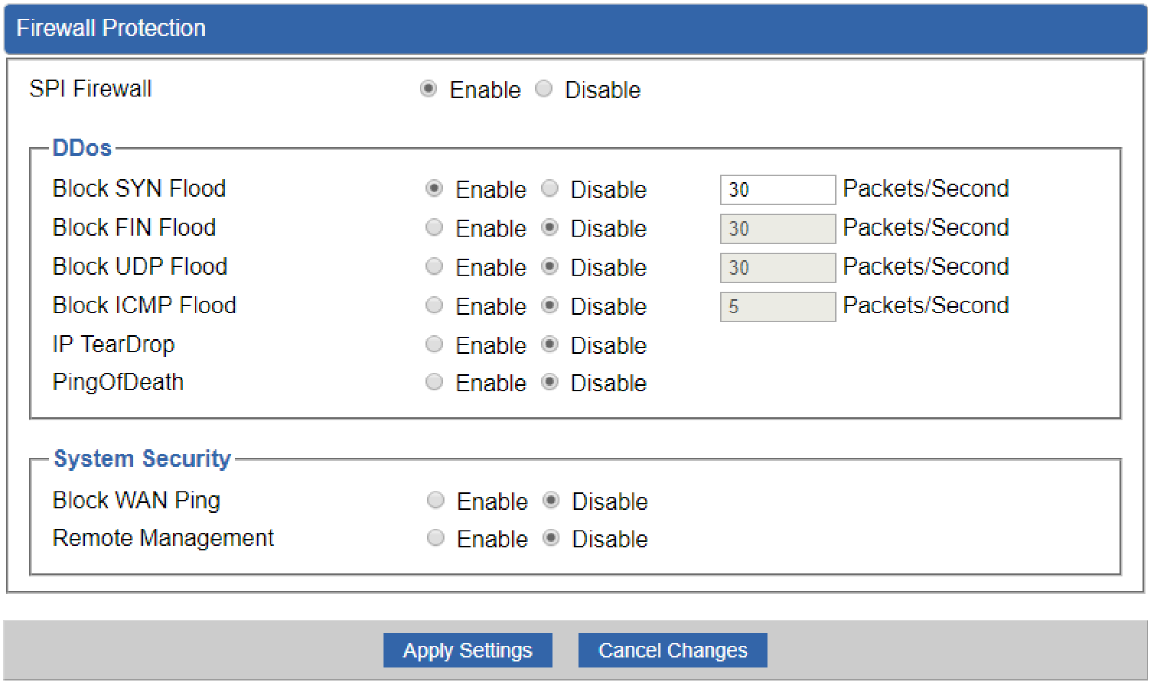


Figure 4-29: Security menu

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 Gateway can prevent specific DoS attacks as shown in Figure 4-30.



Firewall Protection

SPI Firewall ● Enable ○ Disable

DDos

Block SYN Flood	● Enable ○ Disable	30	Packets/Second
Block FIN Flood	○ Enable ● Disable	30	Packets/Second
Block UDP Flood	○ Enable ● Disable	30	Packets/Second
Block ICMP Flood	○ Enable ● Disable	5	Packets/Second
IP TearDrop	○ Enable ● Disable		
PingOfDeath	○ Enable ● Disable		

System Security

Block WAN Ping	○ Enable ● Disable
Remote Management	○ Enable ● Disable

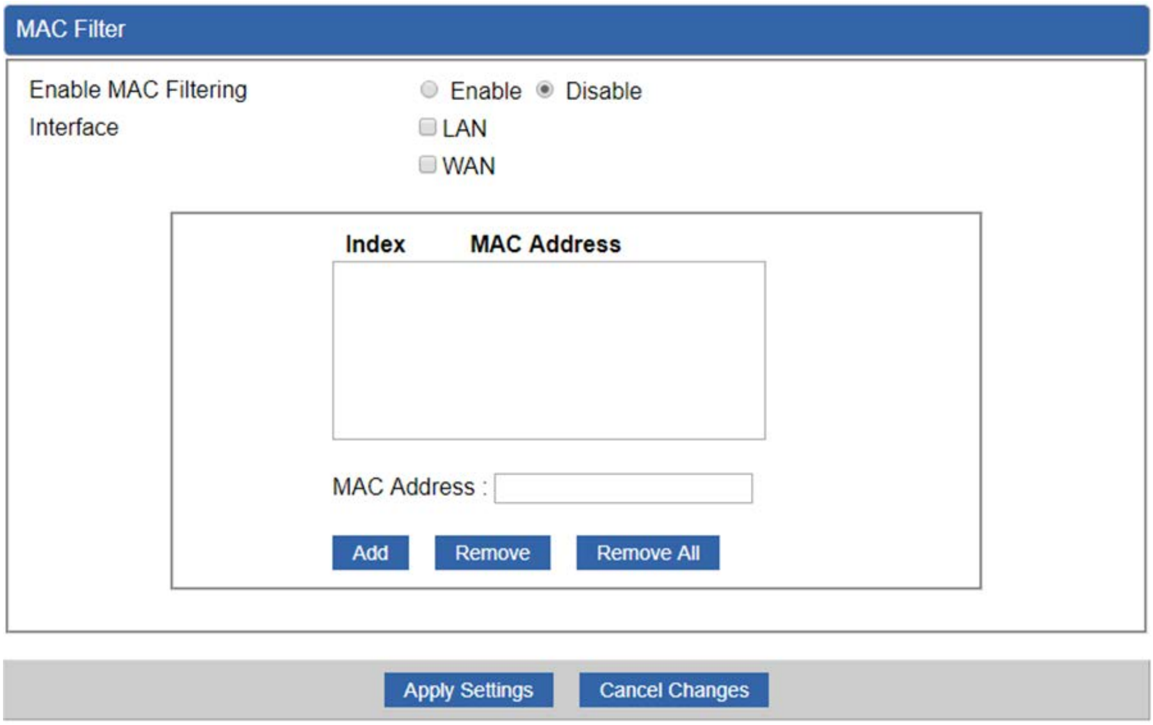
Figure 4-30: Firewall

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 Gateway will start the blocking function immediately. The default configuration is disabled.

Block UDP Flood	If the function is enabled, when the number of the current UPD-FLOOD packets is beyond the set value, the Gateway will start the blocking function immediately. The default configuration is disabled.
Block ICMP Flood	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. The default configuration is disabled.
IP TearDrop	If the function is enabled, the Gateway will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes.
Ping Of Death	If the function is enabled, the Gateway 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.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the Gateway from the Internet network. The default configuration is disabled.

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 Gateway. Use of such filters can be helpful in securing or restricting your local network as shown in Figure 4-31.



MAC Filter

Enable MAC Filtering ○ Enable ● Disable

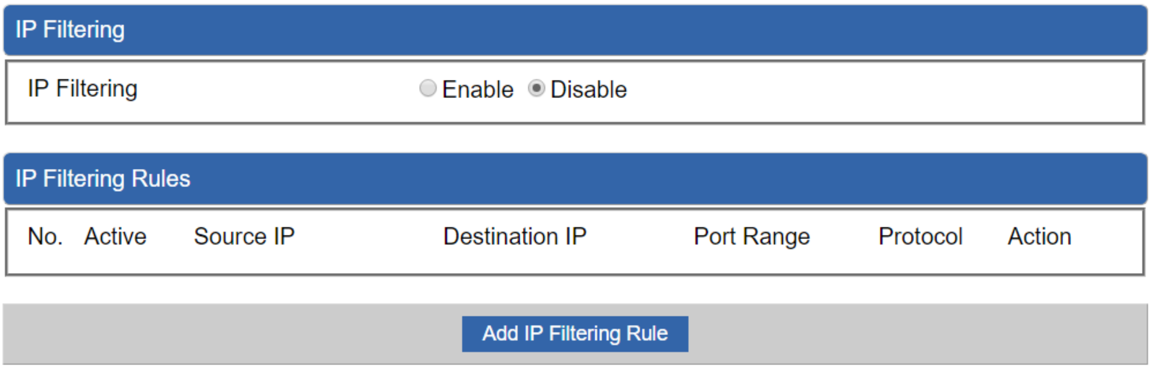
Interface □ LAN □ WAN

Figure 4-31: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. When the function is enabled, the Gateway 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.



IP Filtering

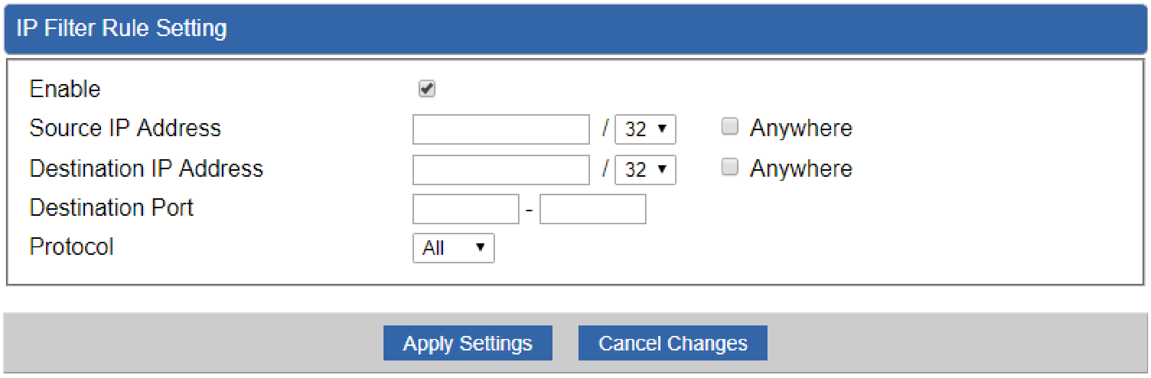
IP Filtering ○ Enable ● Disable

IP Filtering Rules

No.	Active	Source IP	Destination IP	Port Range	Protocol	Action

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.



IP Filter Rule Setting

Enable ☑
Source IP Address [ ] / 32 ☐ Anywhere
Destination IP Address [ ] / 32 ☐ Anywhere
Destination Port [ ] - [ ]
Protocol All

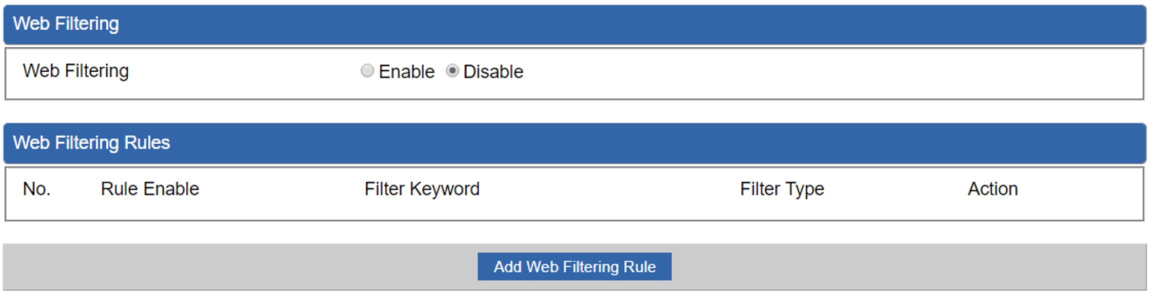
Figure 4-33: IP Filter Rule Setting

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.
Destination IP Address	Input the IP address of web site which you want to block.

Object	Description
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

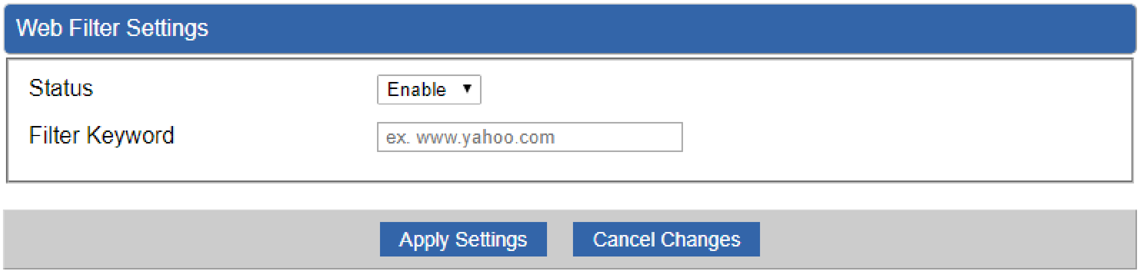
Web Filtering ○ Enable ● Disable

Web Filtering Rules

No.	Rule Enable	Filter Keyword	Filter Type	Action

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: Enable ▼

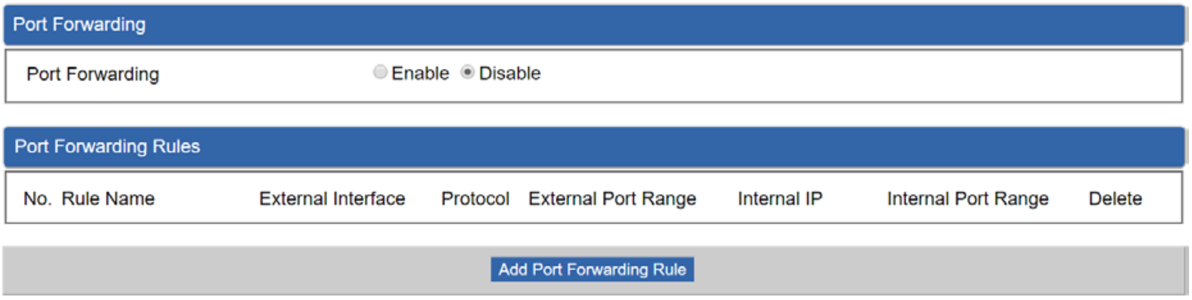
Filter Keyword: ex. www.yahoo.com

Figure 4-35: Web Filtering Rule Setting

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 Gateway's NAT firewall.



Port Forwarding

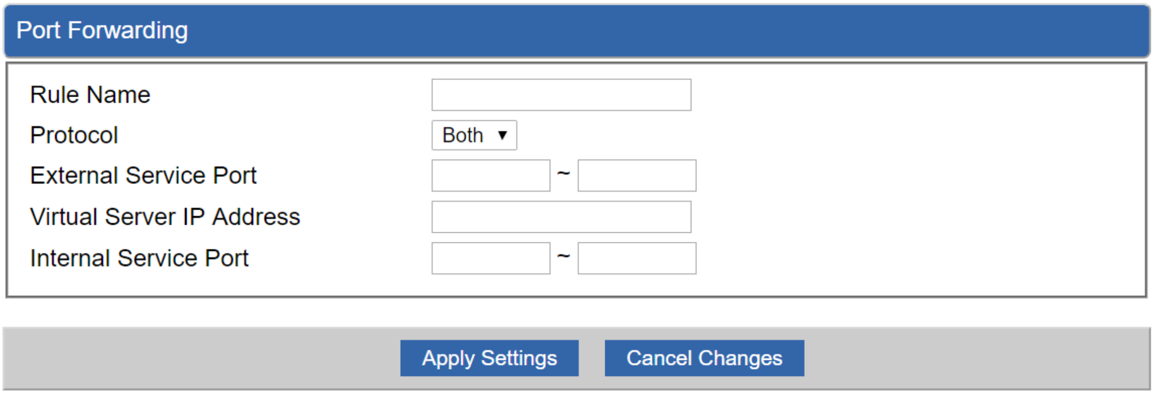
Port Forwarding ○ Enable ● Disable

Port Forwarding Rules

No.	Rule Name	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range	Delete

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
Protocol: Both ▼
External Service Port ~
Virtual Server IP Address
Internal Service Port ~

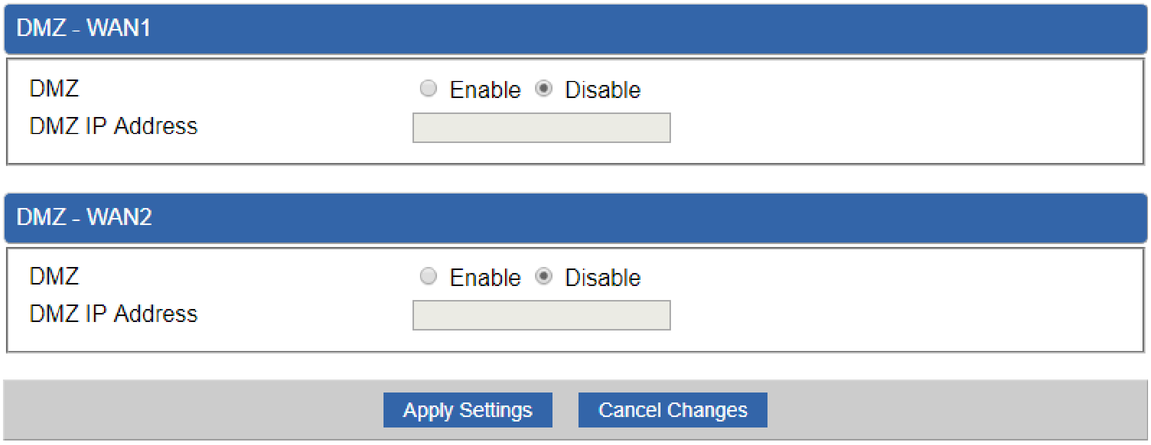
Figure 4-37: Port Forwarding Rule Setting

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.

Object	Description
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.
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 Gateway 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:

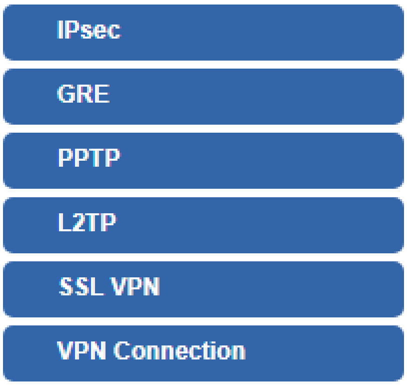


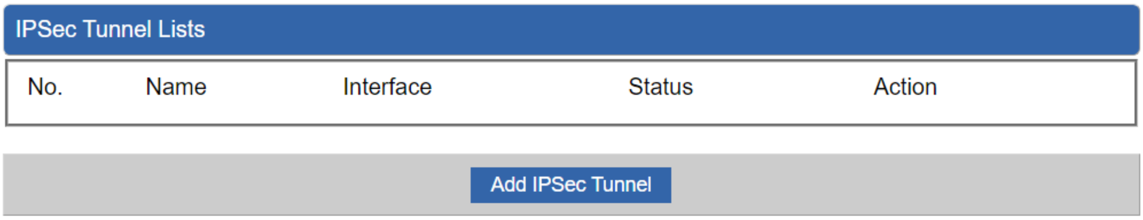
Figure 4-39: VPN Menu

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.

4.7.1 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.

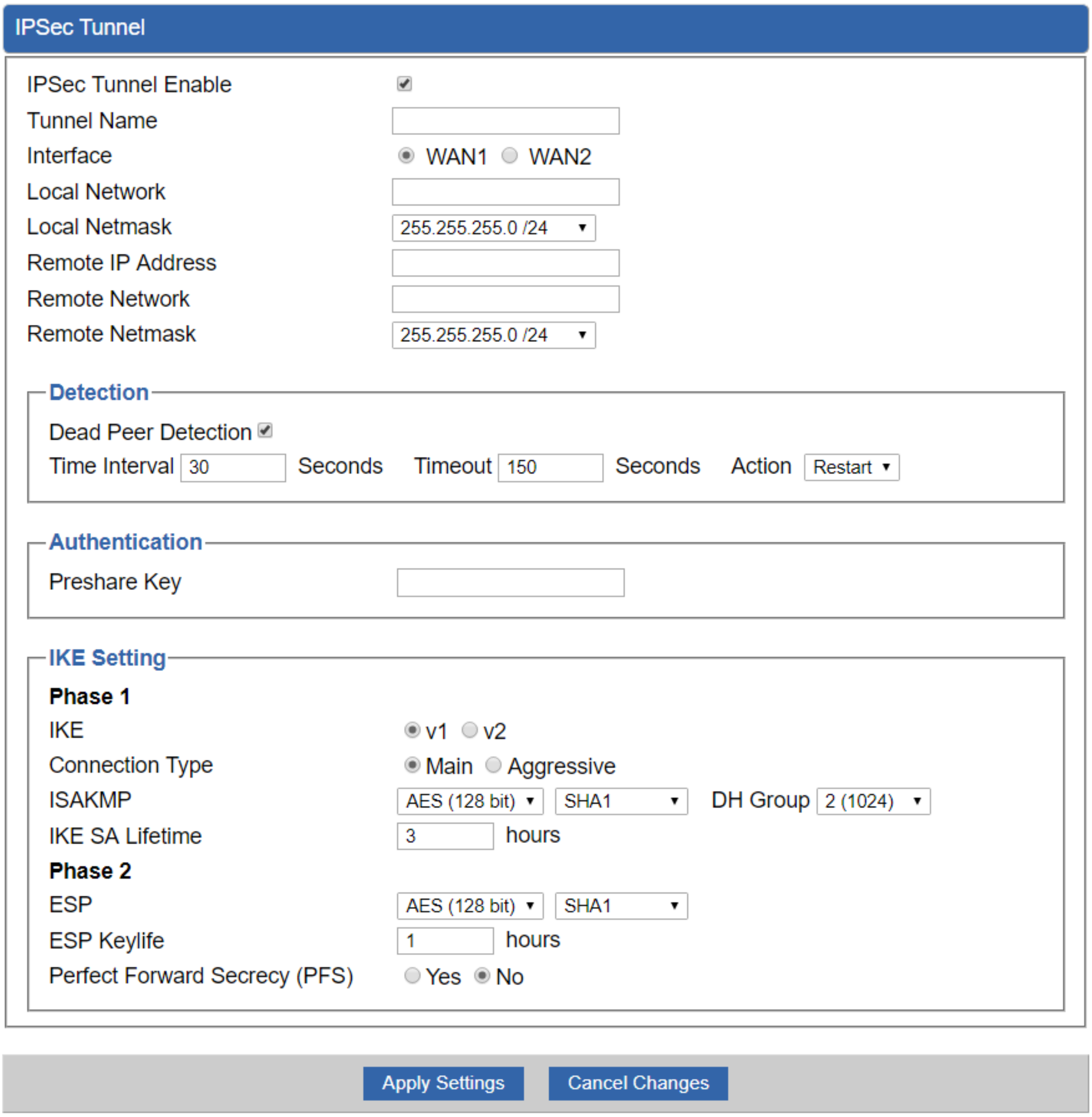


IPSec Tunnel Lists

No.	Name	Interface	Status	Action

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	255.255.255.0 /24
Remote IP Address	
Remote Network	
Remote Netmask	255.255.255.0 /24

Detection

Dead Peer Detection ☑

Time Interval 30 Seconds Timeout 150 Seconds Action Restart

Authentication

Preshare Key

IKE Setting

Phase 1

IKE	● v1 ○ v2
Connection Type	● Main ○ Aggressive
ISAKMP	AES (128 bit) SHA1 DH Group 2 (1024)
IKE SA Lifetime	3 hours

Phase 2

ESP	AES (128 bit) SHA1
ESP Keylife	1 hours
Perfect Forward Secrecy (PFS)	○ Yes ● No

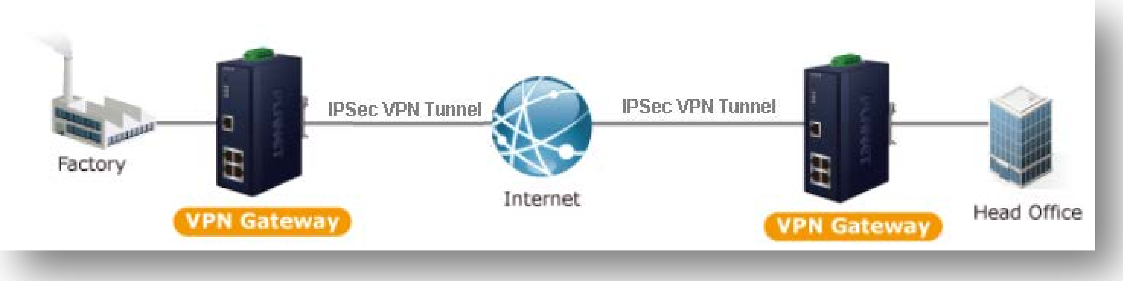
Figure 4-41: IPSec Tunnel

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 Gateway.

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	Set up the detection time of **DPD** (Dead Peer Detection). By default, the DPD detection’s gap is 30 seconds, over 150 seconds to think that is the broken line. 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.
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	1. Main. 2. Aggressive.
ISAKMP	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. 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	It offers AES, 3 DES, SHA 1, SHA2, and MD5. 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

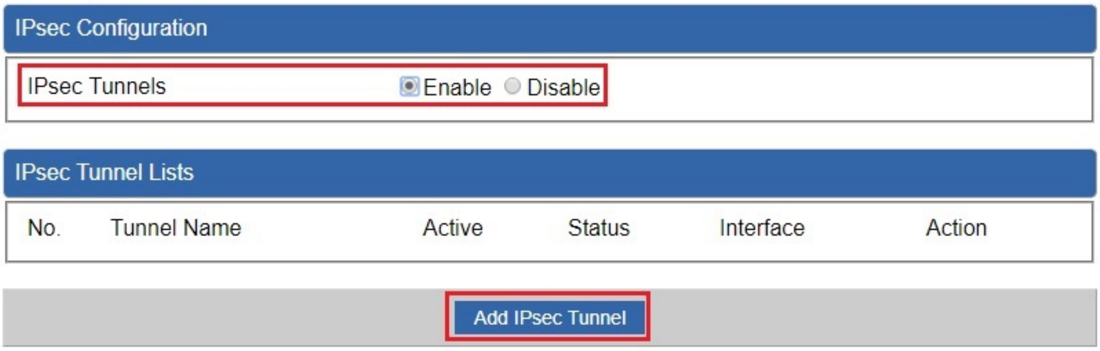
	by using it three times. It can achieve an algorithm up to 168 bits. 3. **SHA1:** The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. **SHA2**: Either 256, 384 or 512 can be chosen. 5. **MD5 Algorithm**: 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.
Perfect Forward Secrecy (PFS)	Set the function as enable or disable.

- **[Example]** Establishing the IPSec VPN connection between two VPN Gateways.



Follow the steps below for setting up the Gateways:

1. Go to the **VPN** -> **IPsec** page.



IPsec Configuration

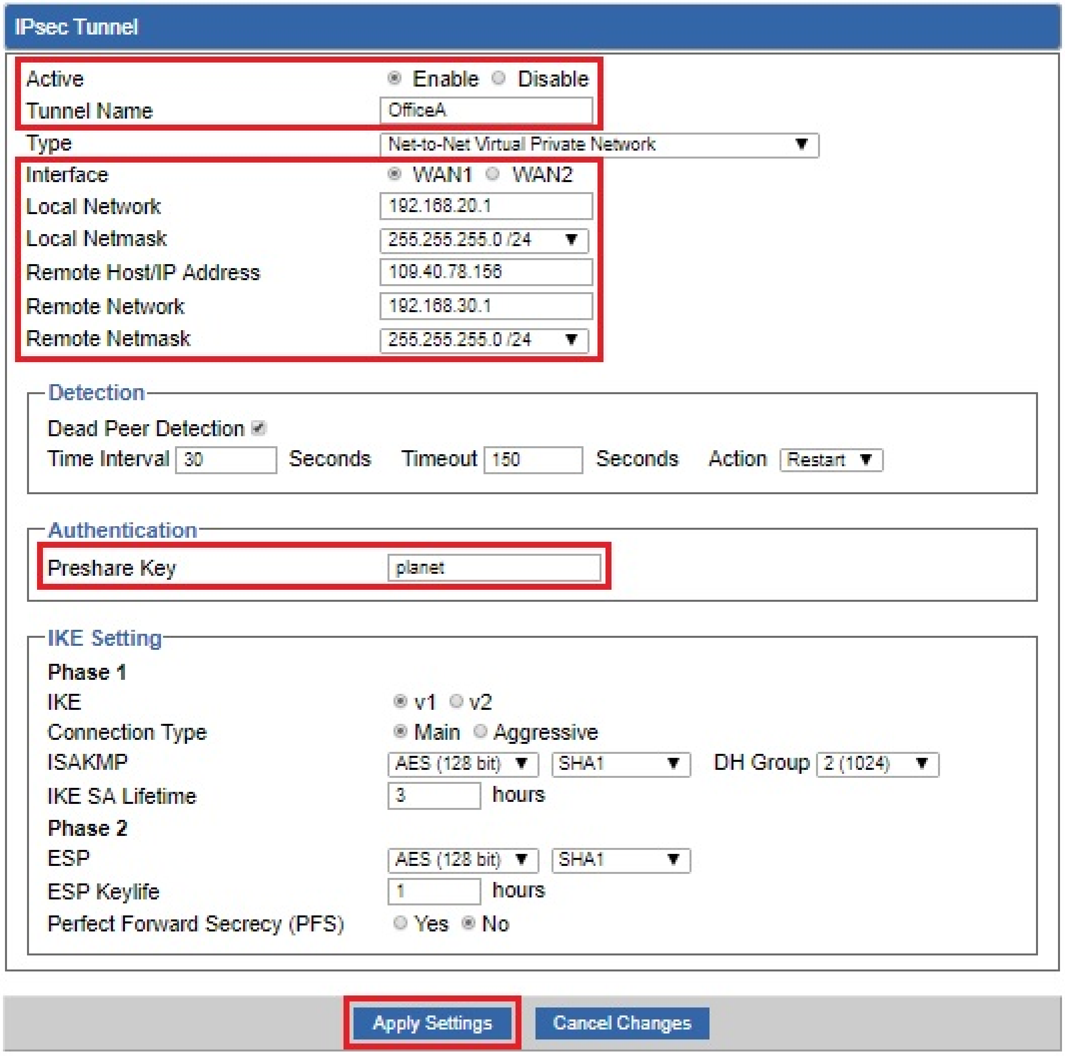
IPsec Tunnels ● Enable ○ Disable

IPsec Tunnel Lists

No.	Tunnel Name	Active	Status	Interface	Action

2. Set the **IPsec Tunnels** as enable.

3. Click **Add IPsec Tunnel** button.



IPsec Tunnel

Active	● Enable ○ Disable
Tunnel Name	OfficeA
Type	Net-to-Net Virtual Private Network ▼
Interface	● WAN1 ○ WAN2
Local Network	192.168.20.1
Local Netmask	255.255.255.0 /24 ▼
Remote Host/IP Address	109.40.78.156
Remote Network	192.168.30.1
Remote Netmask	255.255.255.0 /24 ▼

Detection

Dead Peer Detection ☑

Time Interval 30 Seconds Timeout 150 Seconds Action Restart ▼

Authentication

Preshare Key planet

IKE Setting

Phase 1	
IKE	● v1 ○ v2
Connection Type	● Main ○ Aggressive
ISAKMP	AES (128 bit) ▼ SHA1 ▼ DH Group 2 (1024) ▼
IKE SA Lifetime	3 hours
Phase 2	
ESP	AES (128 bit) ▼ SHA1 ▼
ESP Keylife	1 hours
Perfect Forward Secrecy (PFS)	○ Yes ● No

4. Set the **Active** as enable.

5. Input the **Tunnel Name** and select **Interface.**

6. Input the **Local Network** and **Netmask** as the Gateway's LAN IP address.

7. Input the **Remote Host/IP Address** as another Gateway's public WAN IP address.

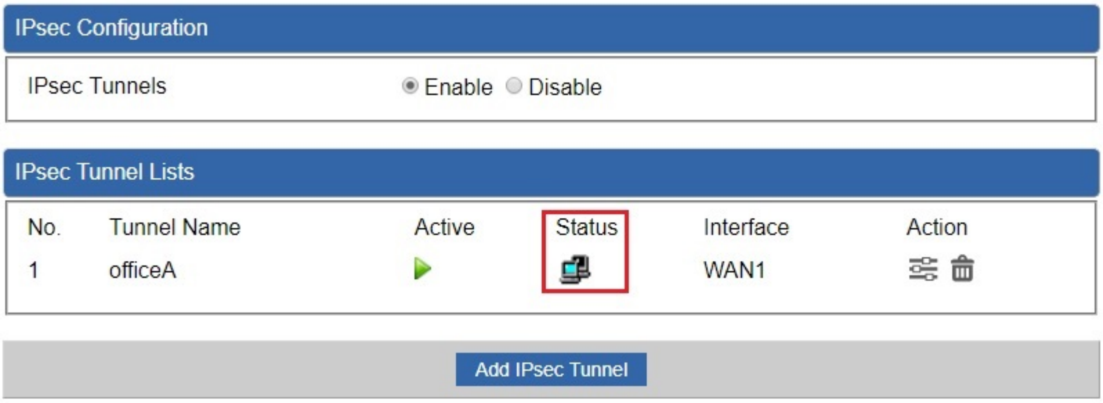
8. Input the **Remote Network and Netmask** as another Gateway's LAN IP address.

9. Input the **Preshare Key** as the same as the one set on both Gateways.

10. Set the **IKE Setting. It should be** the same as the other Gateway.

11. Click **Apply Settings** button to save changes.

12. Go back to the **VPN** -> **IPsec** page. The status shows Connected.



IPsec Configuration

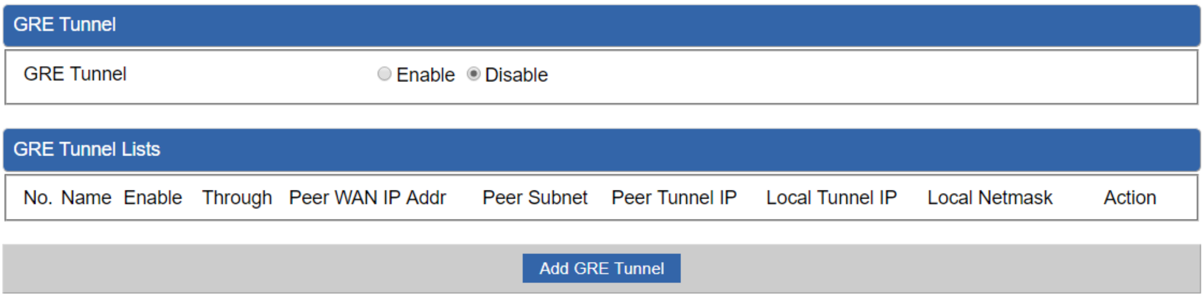
IPsec Tunnels ● Enable ○ Disable

IPsec Tunnel Lists

No.	Tunnel Name	Active	Status	Interface	Action
1	officeA	▶		WAN1	

4.7.2 GRE

This section assists you in setting the GRE Tunnel as shown in Figure 4-42.



GRE Tunnel

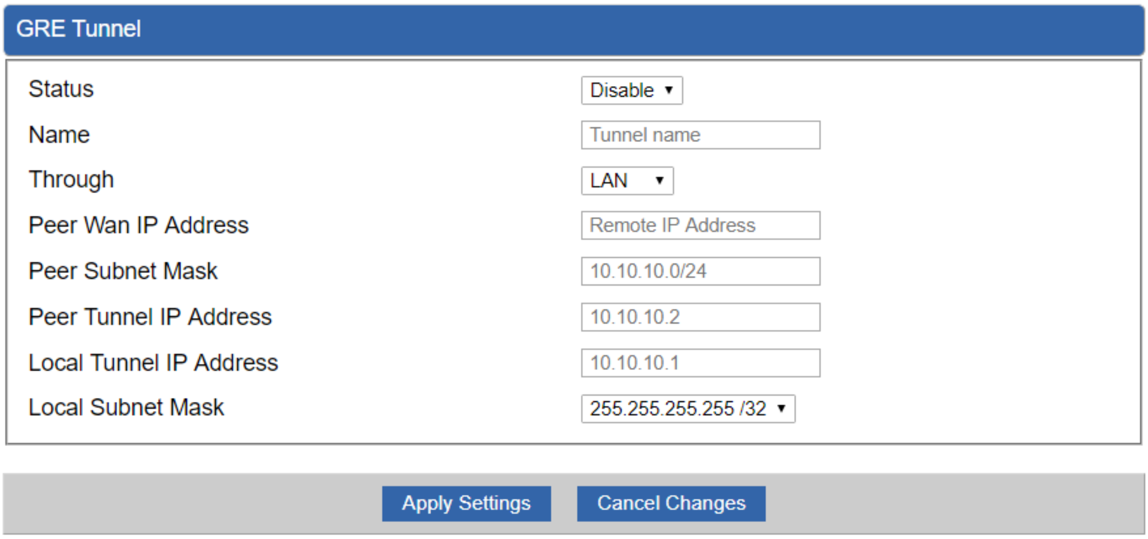
GRE Tunnel ○ Enable ● Disable

GRE Tunnel Lists

No.	Name	Enable	Through	Peer WAN IP Addr	Peer Subnet	Peer Tunnel IP	Local Tunnel IP	Local Netmask	Action

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

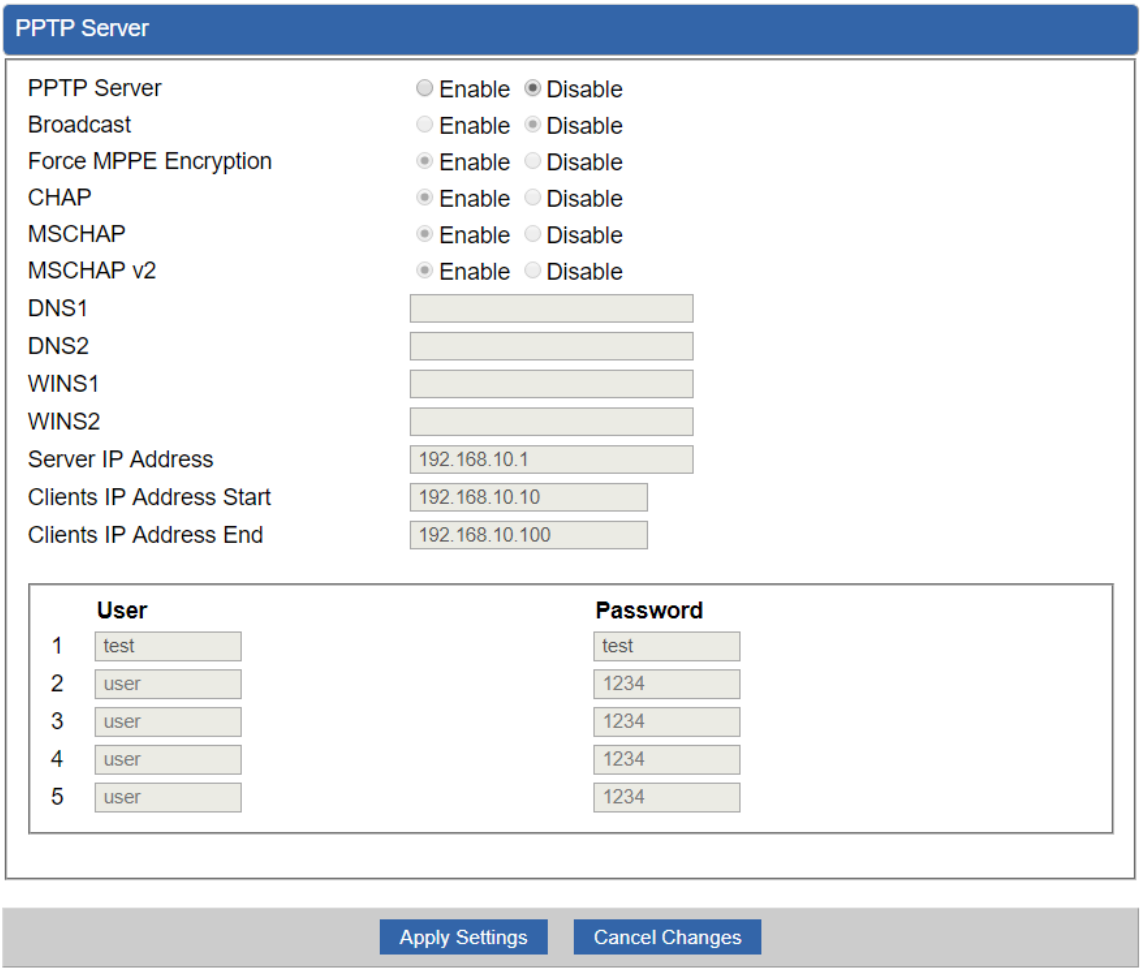
Status	Disable ▾
Name	Tunnel name
Through	LAN ▾
Peer Wan IP Address	Remote IP Address
Peer Subnet Mask	10.10.10.0/24
Peer Tunnel IP Address	10.10.10.2
Local Tunnel IP Address	10.10.10.1
Local Subnet Mask	255.255.255.255 /32 ▾

Figure 4-43: GRE Tunnel

Object	Description
Active	Check the box to enable the function.
Tunnel Name	Enter any words for recognition.
Through	This is only available for host-to-host connections and specifies to which interface the host is connecting. 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 Gateway.

4.7.3 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	○ Enable ● Disable
Broadcast	○ Enable ● Disable
Force MPPE Encryption	● Enable ○ Disable
CHAP	● Enable ○ Disable
MSCHAP	● Enable ○ Disable
MSCHAP v2	● Enable ○ Disable
DNS1	
DNS2	
WINS1	
WINS2	
Server IP Address	192.168.10.1
Clients IP Address Start	192.168.10.10
Clients IP Address End	192.168.10.100

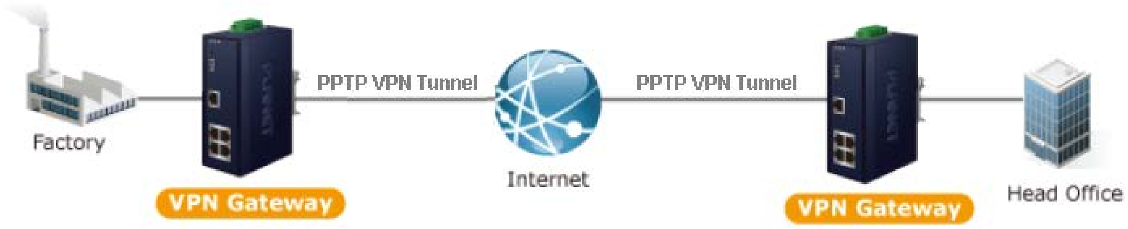
	User	Password
1	test	test
2	user	1234
3	user	1234
4	user	1234
5	user	1234

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.

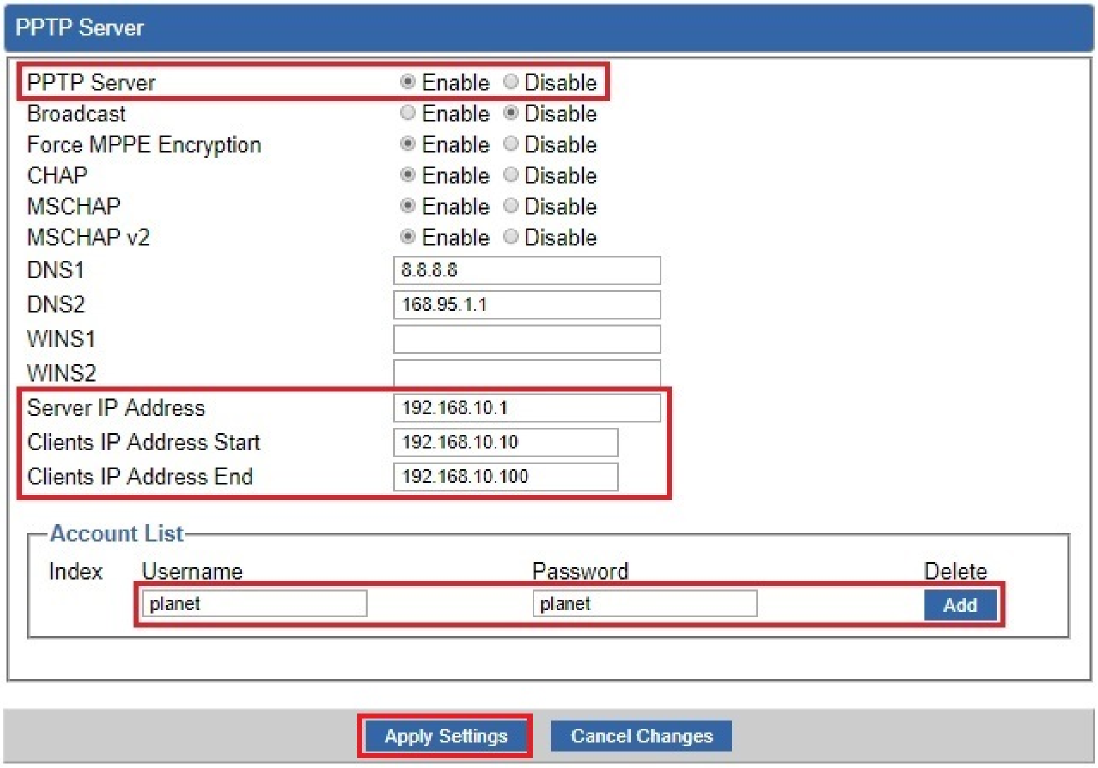
MSCHAP v2	Set the authentication as enable or disable.
DNS	When the PPTP client connects to the PPTP server, it will assign the DNS server IP address to client.
WINS	When the PPTP client connects to the PPTP server, it will assign the WINS server IP address to client.
Server IP Address	Input the IP address 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.

- **[Example]** Establishing the PPTP VPN connection between two VPN Gateways.



Follow the steps below for setting up the **PPTP VPN server**:

1. Go to the **VPN** -> **PPTP** page of PPTP VPN server.



PPTP Server

PPTP Server	● Enable ○ Disable
Broadcast	○ Enable ● Disable
Force MPPE Encryption	● Enable ○ Disable
CHAP	● Enable ○ Disable
MSCHAP	● Enable ○ Disable
MSCHAP v2	● Enable ○ Disable
DNS1	8.8.8.8
DNS2	168.95.1.1
WINS1	
WINS2	
Server IP Address	192.168.10.1
Clients IP Address Start	192.168.10.10
Clients IP Address End	192.168.10.100

Account List

Index	Username	Password	Delete
	planet	planet	Add

2. Set the **PPTP Server** as enable.

3. Input the **Server IP Address** as the Gateway's another subnet address.

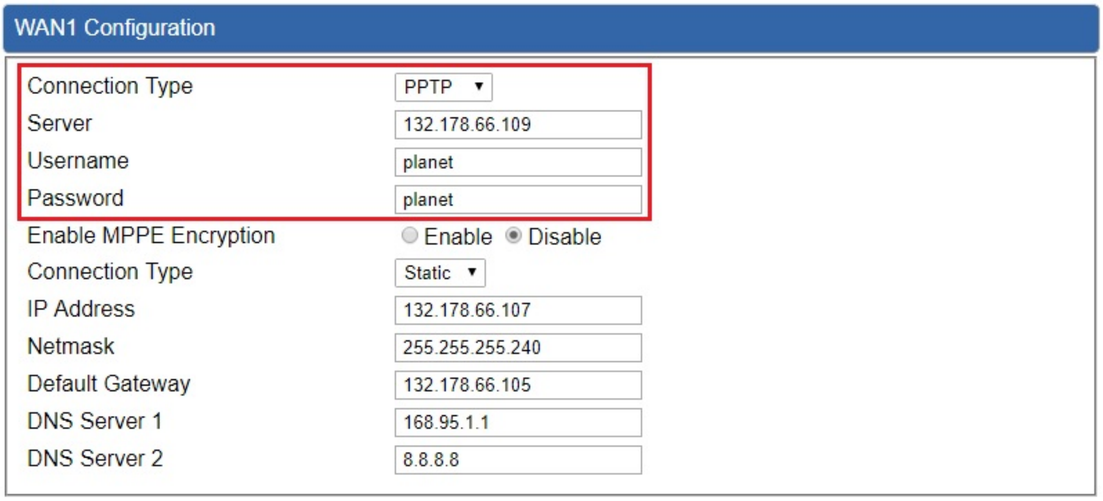
4. Input **Clients IP Address Start** and **Clients IP Address End**.

5. Create an account. Enter **Username** and **Password**.

6. Click **Apply Settings** button to save changes.

Follow the following steps for setting up **PPTP VPN client**:

1. Go to the **Network** -> **WAN** page.



WAN1 Configuration

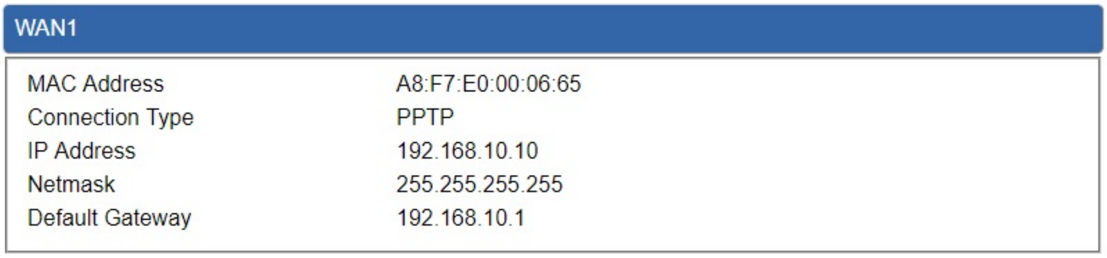
Connection Type	PPTP ▾
Server	132.178.66.109
Username	planet
Password	planet
Enable MPPE Encryption	○ Enable ● Disable
Connection Type	Static ▾
IP Address	132.178.66.107
Netmask	255.255.255.240
Default Gateway	132.178.66.105
DNS Server 1	168.95.1.1
DNS Server 2	8.8.8.8

2. Select Connection Type as **PPTP**.

3. Input the **Server** as the VPN Server Gateway's public WAN IP address.

4. Input the same **Username** and **Password** as the one set on the VPN Server Gateway.

5. Go to the **System** -> **Status** page to check the Connection Type and IP Address. Make sure the VPN client Gateway gets the VPN Server's subnet IP address.

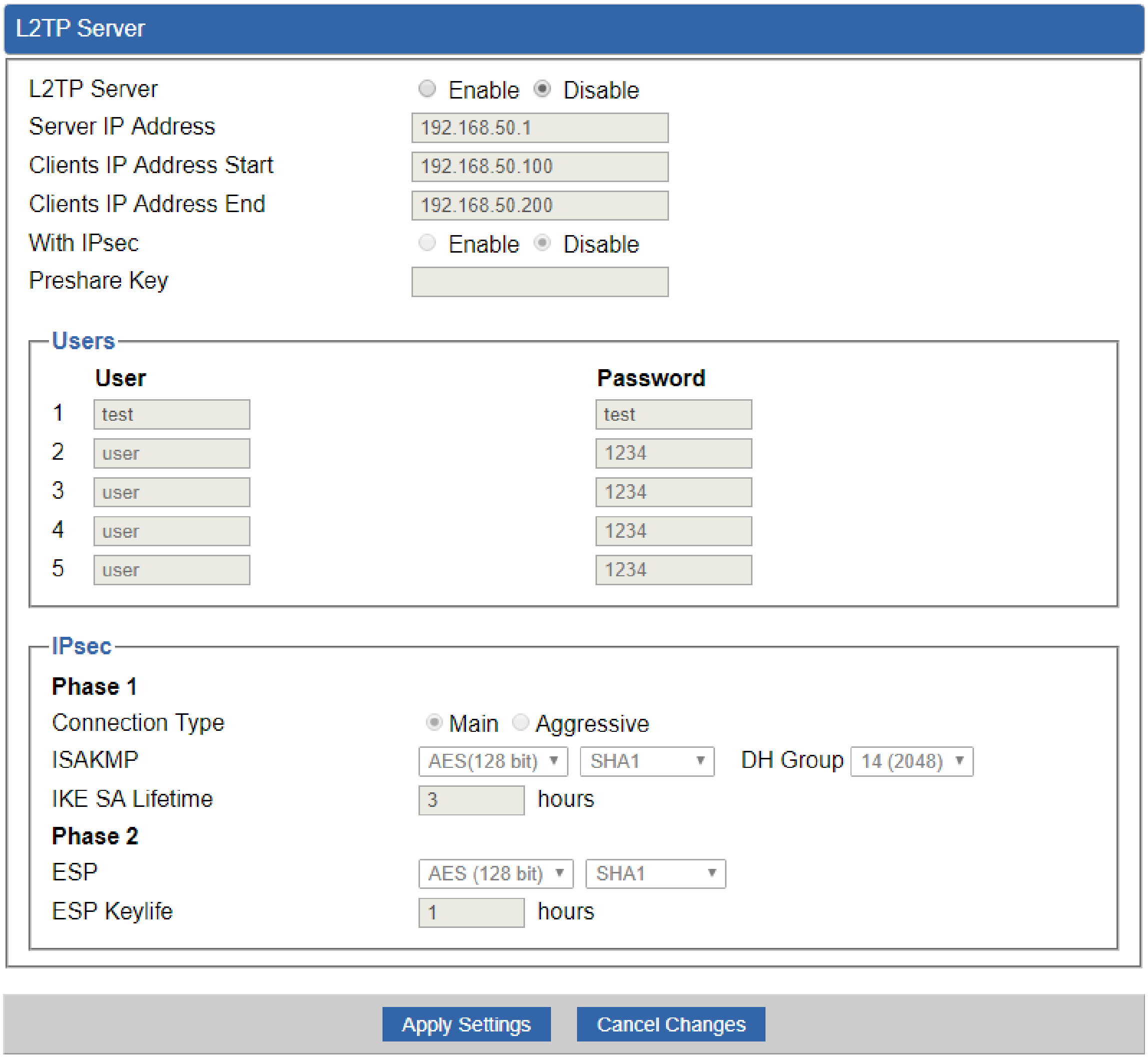


WAN1

MAC Address	A8:F7:E0:00:06:65
Connection Type	PPTP
IP Address	192.168.10.10
Netmask	255.255.255.255
Default Gateway	192.168.10.1

4.7.4 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 192.168.50.1
Clients IP Address Start 192.168.50.100
Clients IP Address End 192.168.50.200
With IPsec ○ Enable ● Disable
Preshare Key

Users

	User	Password
1	test	test
2	user	1234
3	user	1234
4	user	1234
5	user	1234

IPsec

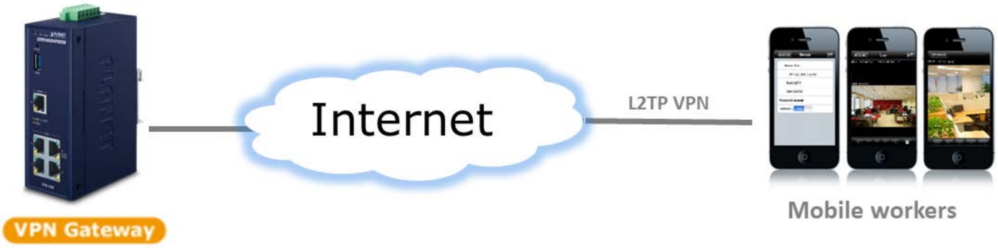
Phase 1
Connection Type ● Main ○ Aggressive
ISAKMP AES(128 bit) ▼ SHA1 ▼ DH Group 14 (2048) ▼
IKE SA Lifetime 3 hours
Phase 2
ESP AES (128 bit) ▼ SHA1 ▼
ESP Keylife 1 hours

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".
With IPsec	Set the function as enable to make the L2TP work with IPsec encryption.

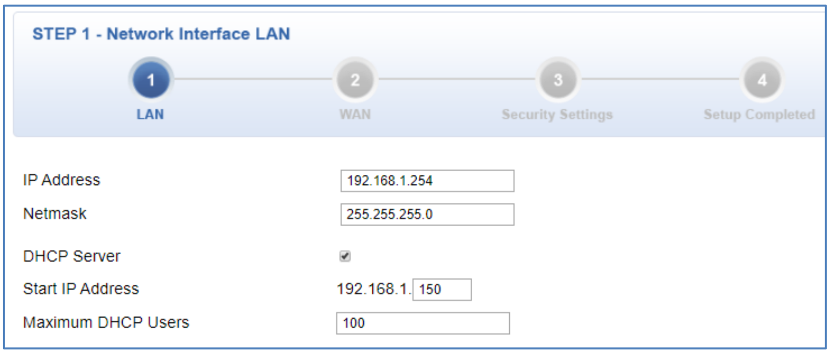
Object	Description
Preshare Key	Enter a pass phrase.
User and Password	Create the username and password for the VPN client.
Connection Type	1. Main. 2. Aggressive.
ISAKMP	It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways. 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	It offers AES, 3 DES, SHA 1, SHA2, and MD5. 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.

- **[Example]** Establishing the L2TP VPN connection between the VPN Gateway and mobile phone.



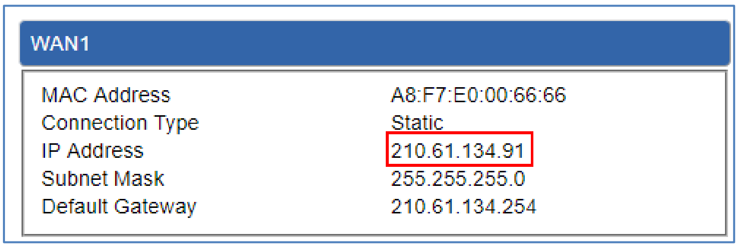
Please refer the steps to configure the VPN settings of the VPN Gateway:

1. Connect the VPN Gateway to internet by the Wizard.



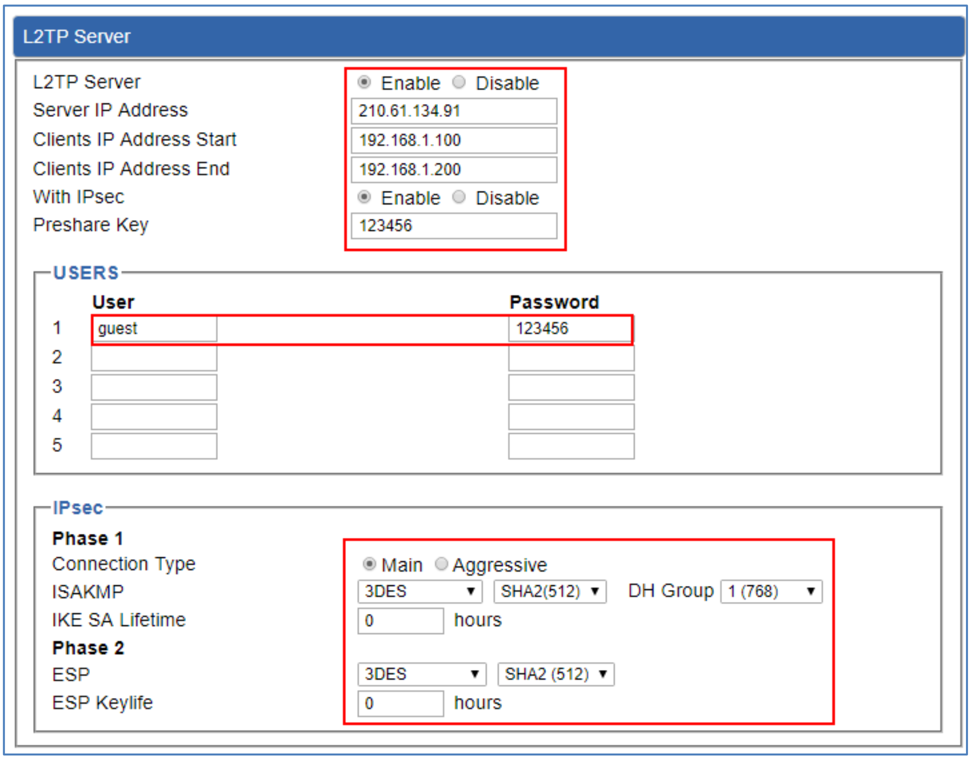
IP Address	192.168.1.254
Netmask	255.255.255.0
DHCP Server	☑
Start IP Address	192.168.1. 150
Maximum DHCP Users	100

2. Go to the **System** -> **Status** page to check the WAN IP address. Make sure the VPN Gateway gets public IP address successfully.


WAN1

MAC Address	A8:F7:E0:00:66:66
Connection Type	Static
IP Address	210.61.134.91
Subnet Mask	255.255.255.0
Default Gateway	210.61.134.254

3. Go to the **VPN** -> **L2TP** page. Set the L2TP Server as enable, input the Server IP Address as the VPN Gateway's public WAN IP address and other necessary information.



L2TP Server

L2TP Server	● Enable ○ Disable
Server IP Address	210.61.134.91
Clients IP Address Start	192.168.1.100
Clients IP Address End	192.168.1.200
With IPsec	● Enable ○ Disable
Preshare Key	123456

USERS

	User	Password
1	guest	123456
2		
3		
4		
5		

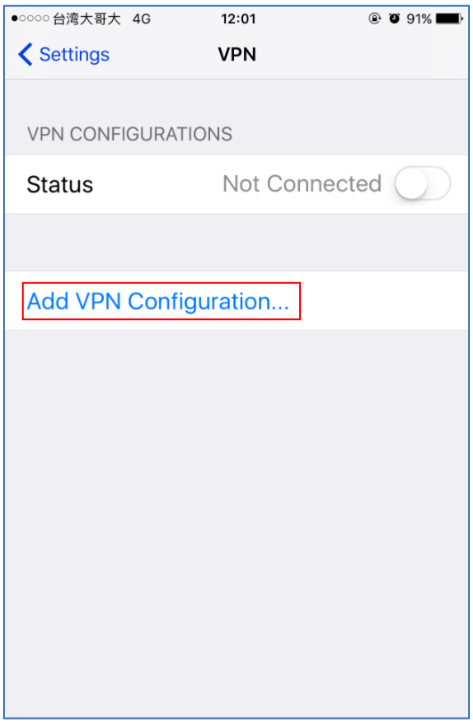
IPsec

Phase 1	
Connection Type	● Main ○ Aggressive
ISAKMP	3DES ▼ SHA2(512) ▼ DH Group 1 (768) ▼
IKE SA Lifetime	0 hours
Phase 2	
ESP	3DES ▼ SHA2 (512) ▼
ESP Keylife	0 hours

The VPN settings of VPN Gateway are done.

4. Please configure the VPN settings of your mobile phone.

   Here we use iPhone as the example: please go to the **Settings** -> **VPN** page, click the “Add VPN Configuration…”.



VPN CONFIGURATIONS

Status Not Connected

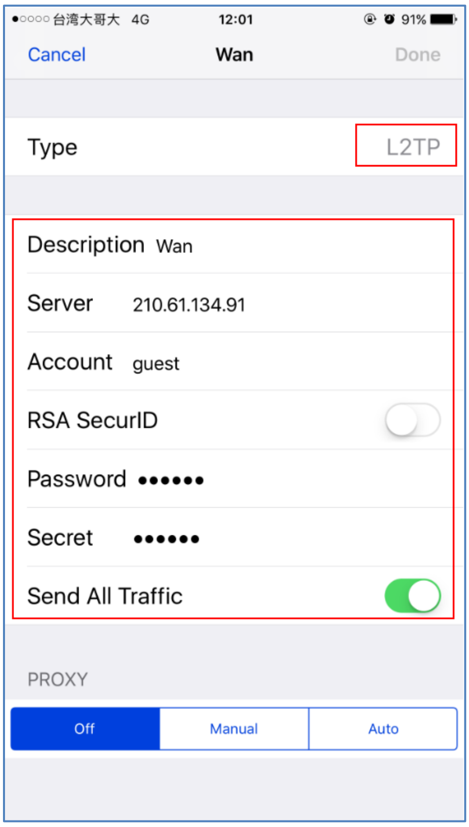
Add VPN Configuration...

Note that the VPN settings might be different from each OS of mobile phone, if you do not know how to configure it, please contact with the dealer of mobile phone.

5. Input the necessary information.

The all information should be the same as VPN Gateway.

For example, the Type should be L2TP, the Server should be the WAN IP of VPN Gateway, the account should be the L2TP User of VPN Gateway, the Password should be the L2TP Password of VPN Gateway, and the Secret should be the L2TP Preshare Key of VPN Gateway.



Type L2TP

Description Wan

Server 210.61.134.91

Account guest

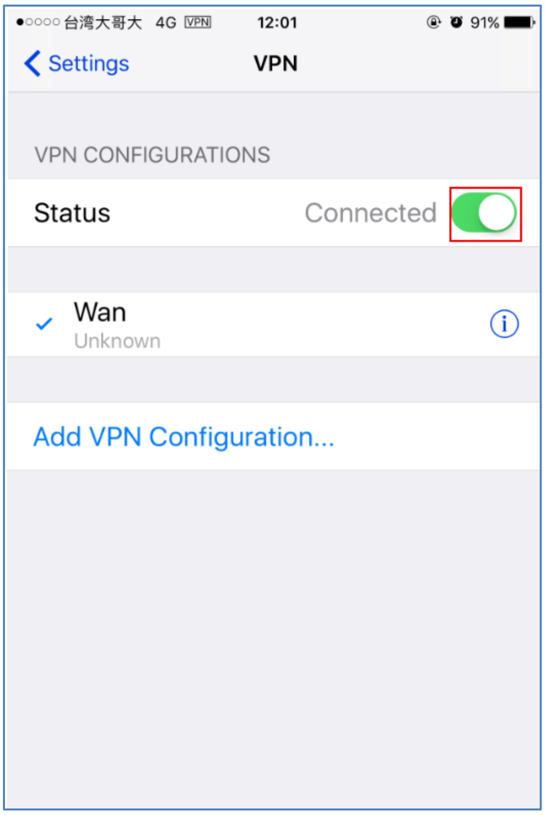
RSA SecurID

Password ●●●●●●

Secret ●●●●●●

Send All Traffic

6. Slide the **Status** slider to “Connecting”, it will start to connect to the VPN server. When the VPN connection is established, the Status will show “Connected”.



●○○○○ 台湾大哥大 4G VPN 12:01 91%

Settings VPN

VPN CONFIGURATIONS

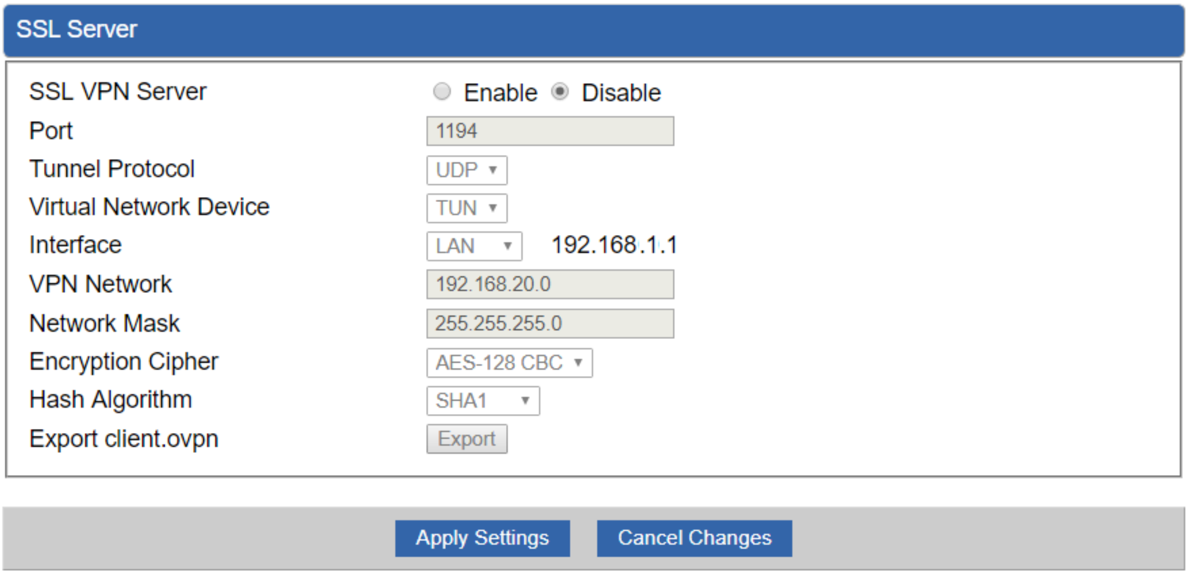
Status Connected

✓ Wan
Unknown

Add VPN Configuration...

4.7.5 SSL VPN

This section assists you in setting the SSL Server as shown in Figure 4-46.



SSL Server

SSL VPN Server	○ Enable ● Disable
Port	1194
Tunnel Protocol	UDP
Virtual Network Device	TUN
Interface	LAN 192.168.1.1
VPN Network	192.168.20.0
Network Mask	255.255.255.0
Encryption Cipher	AES-128 CBC
Hash Algorithm	SHA1
Export client.ovpn	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).

4.7.6 VPN Connection

This page shows the VPN connection status as shown in Figure 4-47.

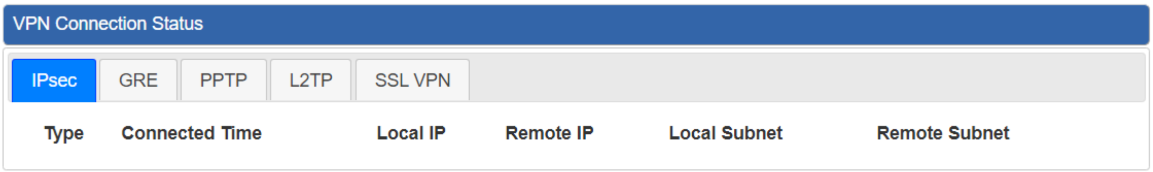


Figure 4-47: VPN Connection Status

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

4.8 Maintenance

The Maintenance menu provides the following features for managing the system as Figure 4-48 is shown below:

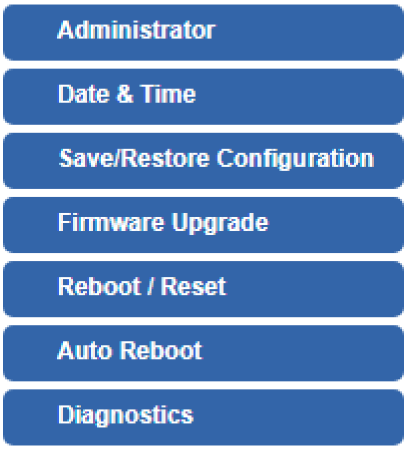
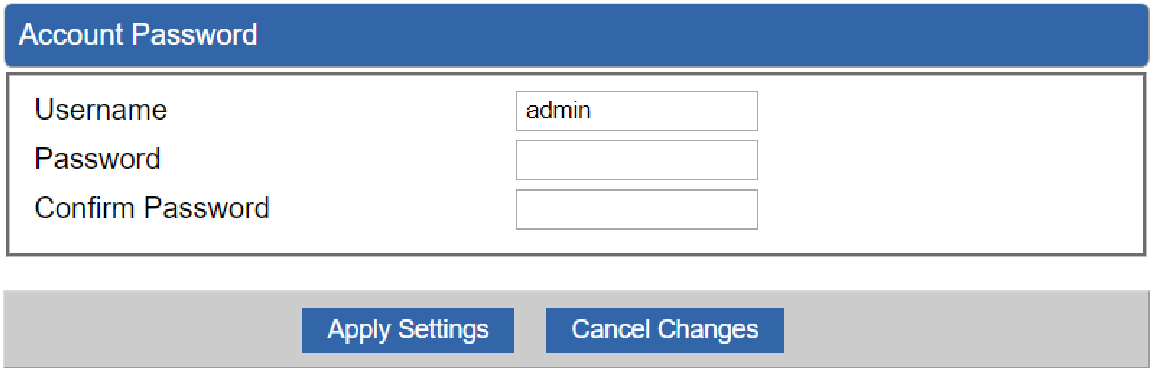


Figure 4-48: Maintenance Menu

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the Gateway’s configuration to local or USB sticker. Restore the Gateway’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.

4.8.1 Administrator

To ensure the Gateway's security is secure, you will be asked for your password when you access the Gateway'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

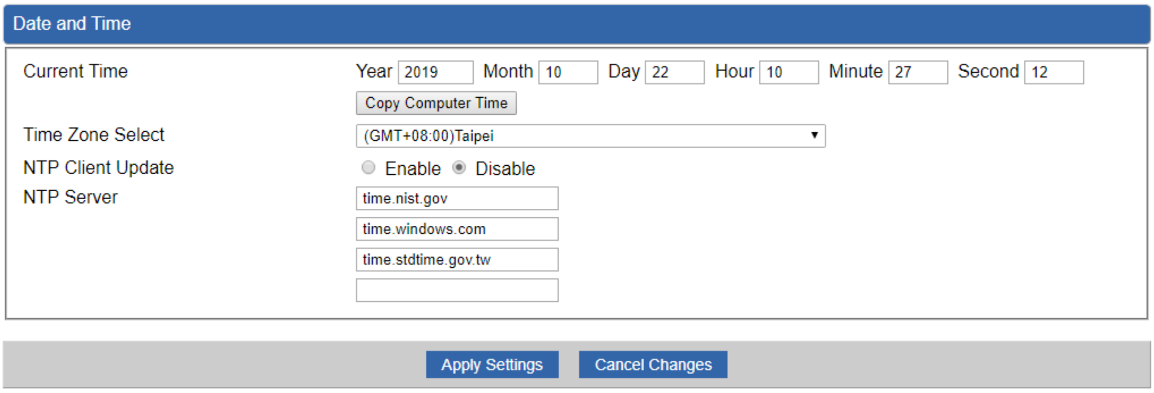
Username	admin
Password	
Confirm Password	

Figure 4-48: Administrator

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

4.8.2 Date and Time

This section assists you in setting the system time of the Gateway. 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 2019 Month 10 Day 22 Hour 10 Minute 27 Second 12 Copy Computer Time
Time Zone Select	(GMT+08:00)Taipei
NTP Client Update	○ Enable ● Disable
NTP Server	time.nist.gov time.windows.com time.stdtime.gov.tw

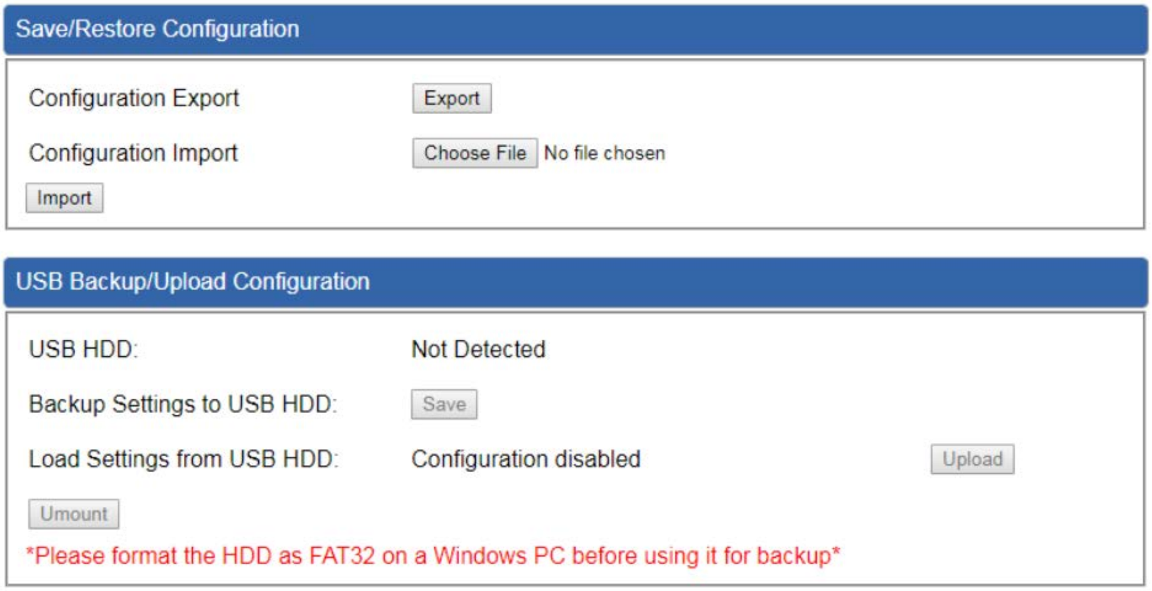
Figure 4-49: Date and Time

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 Gateway will set its time based on your selection.

NTP Client Update	Once this function is enabled, Gateway will automatically update current time from NTP server.
NTP Server	User may use the default NTP sever or input NTP server manually.

4.8.3 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 Export

Configuration Import Choose File No file chosen

Import

USB Backup/Upload Configuration

USB HDD: Not Detected

Backup Settings to USB HDD: Save

Load Settings from USB HDD: Configuration disabled Upload

Umount

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 Export button to save setting file to PC.
Configuration Import	Press the Choose File button to select the setting file, and then press the Import button to upload setting file from PC.

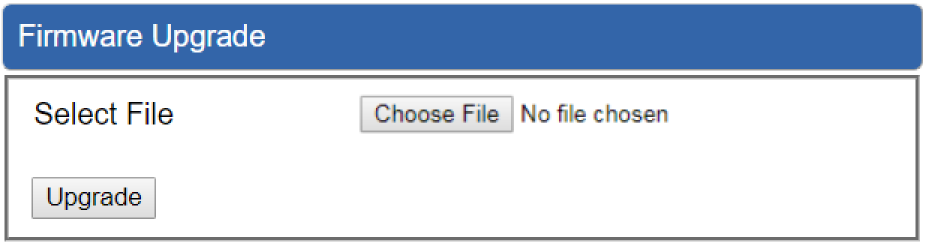
■ **Save Setting to USB Storage**

Object	Description
USB Storage	The status of USB storage.

Object	Description
Backup Settings to USB Storage	Press the Save button to save setting file to USB storage.
Load Settings from USB Storage	Press the Upload button to upload setting file from USB storage.
Unmount	Before removing the USB storage from the Gateway, please press the Umount button first.

4.8.4 Upgrading Firmware

This page provides the firmware upgrade of the Gateway as shown in Figure 4-51.



Firmware Upgrade

Select File

Choose File No file chosen

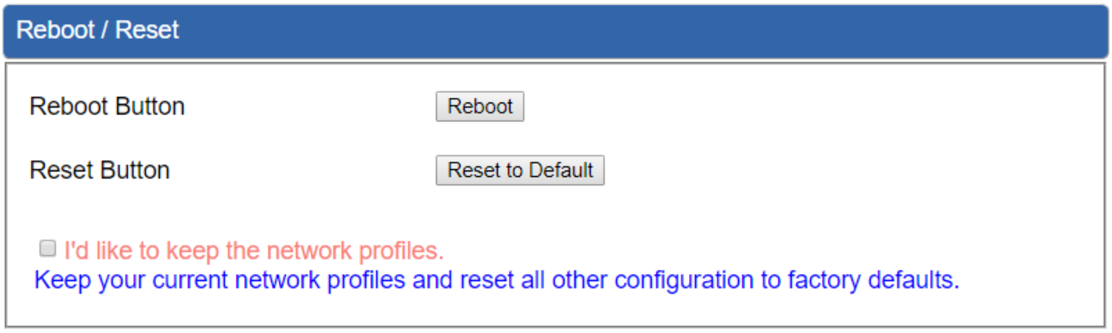
Upgrade

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.

4.8.5 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 [Reboot]

Reset Button [Reset to Default]

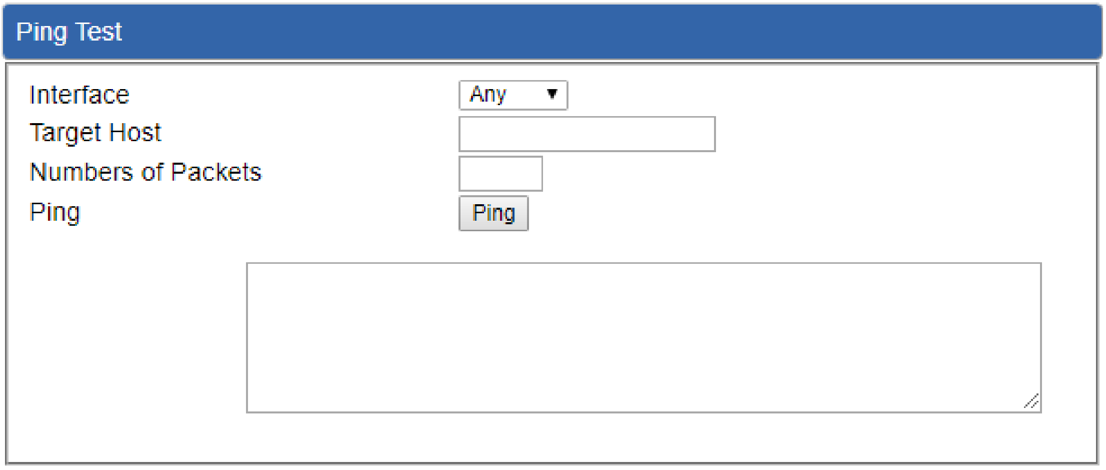
□ I'd like to keep the network profiles.
Keep your current network profiles and reset all other configuration to factory defaults.

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 [Reset to Default] button to keep the current network profiles and reset all other configurations to factory defaults.

4.8.6 Diagnostics

The page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you have pressed “Ping”, ICMP packets will be transmitted, and the sequence number and roundtrip time will be 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: Any ▼
Target Host:
Numbers of Packets:
Ping: [Ping]

Figure 4-53: Ping

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

Note

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

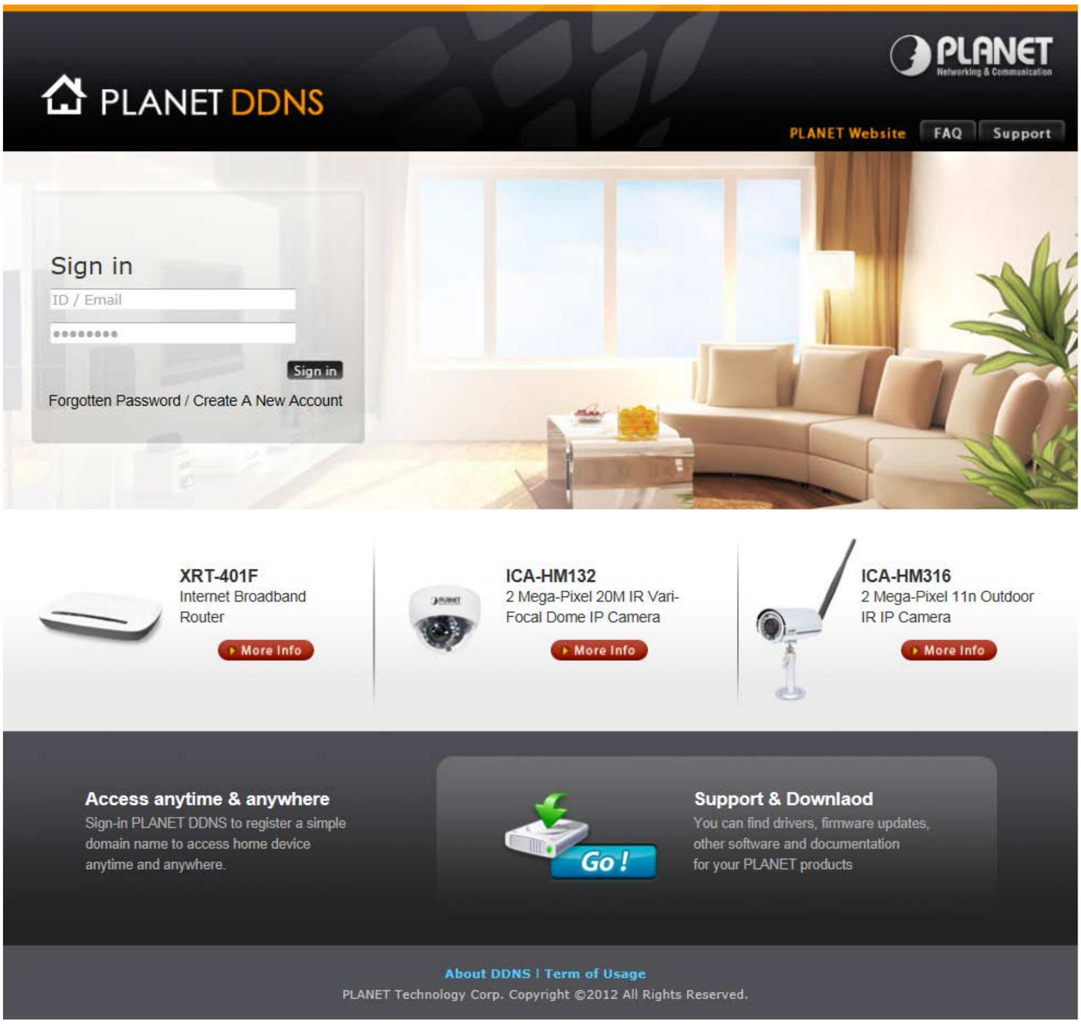
Appendix A: DDNS Application

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.


PLANET DDNS
PLANET Networking & Communication
PLANET Website
FAQ
Support
Sign in
ID / Email
••••••••
Sign in
Forgotten Password / Create A New Account
XRT-401F
Internet Broadband Router
More Info
ICA-HM132
2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera
More Info
ICA-HM316
2 Mega-Pixel 11n Outdoor IR IP Camera
More Info
Go !
About DDNS | Term of Usage

Access anytime & anywhere
Sign-in PLANET DDNS to register a simple domain name to access home device anytime and anywhere.

Support & Downlaod
You can find drivers, firmware updates, other software and documentation for your PLANET products

PLANET Technology Corp. Copyright ©2012 All Rights Reserved.