

# **User's Manual**



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

VR-300 Series



www.PLANET.com.tw



### Copyright

Copyright (C) 2021 PLANET Technology Corp. All rights reserved.

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

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

### Disclaimer

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

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

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

### **FCC Compliance Statement**

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:



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

### **CE mark Warning**

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

### WEEE



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out

wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

### Trademarks

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

### Revision

User's Manual of PLANET 5-Port 10/100/1000T VPN Security Router Model: VR-300, VR-300P, VR-300F, VR-300FP, VR-300W5, VR-300PW5, VR-300W6A, VR-300PW6A, VR-300W6, VR-300PW6 Rev.: 1.1 (October, 2021) Part No. EM-VR-300 series\_v1.2



# **Table of Contents**

Chapter	1. Produc	t Introduction	7
1.1	Package C	Contents	.8
1.2	Overview.		8
1.3	Topology		1
1.4	Features	1	3
1.5	Product Sp	pecifications1	6
Chapter	2. Hardwa	are Introduction4	0
2.1	Physical D	escriptions4	0
2.2	Hardware	Installation4	4
Chapter	3. Prepar	ation4	5
3.1	Requireme	ents4	5
3.2	Setting TC	P/IP on your PC4	6
3.3	Planet Sma	art Discovery Utility5	53
Chapter	4. Web-b	ased Management5	55
4.1	Introduction	n5	5
4.2	Logging in	to the VPN Router5	55
4.3	Main Web	Page5	6
4.4	System	5	8
	4.4.1	Setup Wizard6	60
	4.4.2	Dashboard6	6
	4.4.3	Status	57
	4.4.4	Statistics	8
	4.4.5	Connection Status	69
	4.4.6	SFP Module Information6	69
	4.4.7	High Availability7	'1
	4.4.8	RADIUS7	'2
	4.4.9	Captive Portal7	'3
	4.4.10	SNMP7	'4
	4.4.11	NMS	'5
4.5	Network	7	7
	4.5.1	WAN7	'9
	4.5.2	WAN Advanced8	80
	4.5.3	LAN Setup	31
	4.5.4	Multi-Subnet	32



			112000
	4.5.5	Routing	82
	4.5.6	WAN IPv6 Setting	84
	4.5.7	DHCP	84
	4.5.8	DDNS	86
	4.5.9	MAC Address Clone	88
4.6	Security		89
	4.6.1	Firewall	90
	4.6.2	MAC Filtering	92
	4.6.3	IP Filtering	93
	4.6.4	Web Filtering	94
	4.6.5	Port Forwarding	95
	4.6.6	DMZ	96
4.7	Virtual Priv	vate Network	97
	4.7.1	IPSec	98
	4.7.2	GRE	101
	4.7.3	PPTP Server	
	4.7.4	L2TP Server	105
	4.7.5	SSL VPN	107
	4.7.6	VPN Connection	108
4.8	AP Contro	DI	109
	4.8.1	Preference	110
	4.8.2	AP Search	110
	4.8.3	AP Management	111
	4.8.4	AP Group Management	112
	4.8.5	SSID Profile	113
	4.8.6	Radio 2.4G Profile	114
	4.8.7	Radio 5G Profile	115
	4.8.8	Statistics AP Status	116
	4.8.9	Statistics Active Clients	116
	4.8.10	Map It	117
	4.8.11	Upload Map	118
4.9	Power ove	er Ethernet	119
	4.9.1	PoE Configuration	119
	4.9.2	PoE Status	121
	4.9.3	PoE Schedule	121
	4.9.4	PD Alive Check	123
4.1	0 Wireless		125
	4.10.1	2.4G WiFi	125
	4.10.2	5G WiFi	126



4.10.3	MAC ACL	127
4.10.4	WiFi Advanced	128
4.10.5	WiFi Statistics	129
4.10.6	Connection Status	129
4.11 Maintenai	nce	130
4.11.1	Administrator	130
4.11.2	Date and Time	131
4.11.3	Saving/Restoring Configuration	132
4.11.4	Upgrading Firmware	133
4.11.5	Reboot / Reset	133
4.11.6	Diagnostics	134
Appendix A: DDNS	S Application	136



# **Chapter 1. Product Introduction**

Thank you for purchasing PLANET VPN Router, VR-300 Series. The descriptions of these models are as follows:

VR-300	Enterprise 5-Port 10/100/1000T VPN Security Router
VR-300P	Enterprise 4-Port 10/100/1000T 802.3at PoE + 1-Port 10/100/1000T VPN Security Router
VR-300F	Enterprise 4-Port 10/100/1000T + 1-Port 1000X SFP VPN Security Router
VR-300FP	Enterprise 4-Port 10/100/1000T 802.3at PoE + 1-Port 1000X SFP VPN Security Router
VR-300W5	Wi-Fi 5 AC1200 Dual Band VPN Security Router
VR-300PW5	Wi-Fi 5 AC1200 Dual Band VPN Security Router with 4-Port 802.3at PoE+
VR-300W6A	Wi-Fi 6 AX2400 2.4GHz/5GHz VPN Security Router
VR-300PW6A	Wi-Fi 6 AX2400 2.4GHz/5GHz VPN Security Router with 4-Port 802.3at PoE+
VR-300W6	Wi-Fi 6 AC1800 Dual Band VPN Security Router
VR-300PW6	Wi-Fi 6 AC1800 Dual Band VPN Security Router with 4-Port 802.3at PoE+

	VR-300	VR-300F	VR-300W5	VR-300W6	VR-300W6A
	VR-300P	VR-300FP	VR-300PW5	VR-300PW6	VR-300PW6A
Wi-Fi	-	-	11ac	11ax	11ax
Wi-Fi			up to 1.20 bpg	up to 1.8Gbps	up to 2.4Chpa
Performance	-	-	up to 1.2Gbps	up to 1.8Gbps	up to 2.4Gbps
Fiber	-		-	-	-
PoE	VR-300P	VR-300FP	VR-300PW5	VR-300PW6	VR-300PW6A

"VPN Router" mentioned in this Quick Installation Guide refers to the above models.



### **1.1 Package Contents**

The package should contain the following:

- VPN Router x 1
- Quick Installation Guide x 1
- Power Cord x 1
- Rubber Feet x 4
- Rack-mounting Kit x 1
- 2.4G Antenna x 2 (for VR-300W5 and VR-300PW5)
- 5G Antenna x 2 (for VR-300W5 and VR-300PW5)
- Dual Band Antenna x 4 (for VR-300W6A and VR-300PW6A)
- Dual Band Antenna x 2 (for VR-300W6 and VR-300PW6)



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

### 1.2 Overview

### **Powerful VPN Security Solution**

The innovation of the Internet has created tremendous worldwide opportunities for e-business and information sharing. It has become essential for businesses to focus more on network security issues. The demand for information security has become the primary concern for the enterprises. To fulfill this demand, PLANET has launched the VR-300 series VPN Security Router, an all-in-one appliance that carries several main categories across your network security deployments: Cyber security, SPI firewall security protection, policy auditing (Content Filtering, VPN Tunnel and MAC/IP Filtering), AP controller, captive portal, RADIUS and easy management (Setup Wizard, DHCP Server and Dashboard). Furthermore, its Dual-WAN Failover, Outbound Load Balance and High-Availability features can improve the network efficiency while the web-based interface provides friendly and consistent user experience.

### Wireless 11ac Brings Excellent Data Link Speed (Wireless mmodel only)

The VR-300 Series is designed with high power amplifier and 4 highly-sensitive antennas which provide stronger signal and excellent coverage even in the wide-ranging or bad environment. With adjustable transmit power option, the administrator can flexibly reduce or increase the output power for various environments, thus reducing interference to achieve maximum performance. To provide



extremely high-speed user experience, the VR-300W5 adopts IEEE 802.11ac technology to increase the speed from the 802.11n standard 40MHz to 80MHz and to implement the 256-QAM modulation where higher transmitting/receiving rates go up to 867Mbps in 5GHz less interference frequency band. In addition, the VR-300 Series is equipped with Gigabit LAN port to eliminate the restriction of 100Mbps Fast Ethernet wired connection to let users fully enjoy the high speed provided by wireless. The IEEE 802.11ac also optimizes MU-MIMO (Multi-User MIMO) mechanism to serve multiple devices simultaneously.

### Built-in Unique PoE Functions for Powered Devices Management (PoE model only)

The VR-300 series is capable of having a maximum of up to 120 watts of power output and can deliver up to 36W for each port. It also features the following special PoE management functions:

### • PoE Usage Monitoring (PoE model only)

With PoE usage monitoring, it can show the PoE loading of each port, total PoE power usage and system status, such as overload, low voltage, over voltage and high temperature. User can obtain detailed information about the real-time PoE working condition of the VR-300 series directly.

### • PoE Schedule (PoE model only)

Under the trend of energy saving worldwide and contributing to environmental protection, the VR-300 series can effectively control the power supply besides its capability of giving high watts power. The "PoE schedule" function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or enterprises save power and budget. It also increases security by powering off PDs that should not be in use during non-business hours.

### • Scheduled Power Recycling (PoE model only)

The VR-300 series allows each of the connected PoE IP cameras or PoE wireless access points to reboot at a specific time each week. Therefore, it will reduce the chance of IP camera or AP crash resulting from buffer overflow.

### • PD Alive Check (PoE model only)

The VR-300 series can be configured to monitor connected PD status in real time via ping action. Once the PD stops working and responding, the VR-300 series will resume the PoE port power and bring the PD back to work. It will greatly enhance the network reliability through the PoE port resetting the PD's power source and reducing administrator management burden.

### Wi-Fi Deployments and Authentication with Simplified Management

The VR-300 series also provides a built-in AP Controller, Captive Portal, RADIUS and a DHCP server to facilitate small and medium businesses to deploy secure employee and guest access services without any additional server. The VR-300 series can offer a secure Wi-Fi network with easy installation for your business.



### **Centralized Remote Control of Managed APs\***

The VR-300 series provides centralized management of PLANET Smart AP series via a user-friendly Web GUI. It's easy to configure AP for the wireless SSID, radio band and security settings. With a four-step configuration process, different purposes of wireless profiles can be simultaneously delivered to multiple APs or AP groups to minimize deployment time, effort and cost.

For example, to configure multiple Smart APs of the same model, the VR-300 series allows clustering them to a managed group for unified management. According to requirements, wireless APs can be flexibly expanded or removed from a wireless AP group at any time. The AP cluster benefits bulk provision and bulk firmware upgrade through single entry point instead of having to configure settings in each of them separately.

### Ideal High-Availability VPN Security Router Solution for SMBs

The VR-300 series provides complete data security and privacy for accessing and exchanging most sensitive data, built-in IPSec VPN function with DES/3DES/AES encryption and MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication, and GRE, SSL, PPTP and L2TP server mechanism. The full VPN capability in the VR-300 series makes the connection secure, more flexible, and more capable.

### **Excellent Ability in Threat Defense**

The VR-300's built-in SPI (stateful packet inspection) firewall and DoS/DDoS attack mitigation functions provide high efficiency and extensive protection for your network. Thus, virtual server and DMZ functions can let you set up servers in the Intranet and still provide services to the Internet users.

### **Cybersecurity Network Solution to Minimize Security Risks**

The cybersecurity feature included to protect the switch management in a mission-critical network virtually needs no effort and cost to install. For efficient management, the VR-300 is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the VR-300 series offers an easy-to-use, platform independent management and configuration facility. The VR-300 series supports SNMP and it can be managed via any management software based on the standard SNMP protocol.



### 1.3 Topology

### **Improving Network Efficiency**

It is applicable to the small-scale sector (from 60 to 100 people), using a 13-inch desktop design, with five Gigabit ports (WAN/LAN). It provides higher performance with all Gigabit Ethernet interfaces which offer faster speeds for your network applications. The Gigabit user-defined interfaces flexibly fulfill the network requirement nowadays, and the High-Availability and Dual-WAN interfaces enable the VR-300 series to support outbound load balancing and WAN fail-over features.



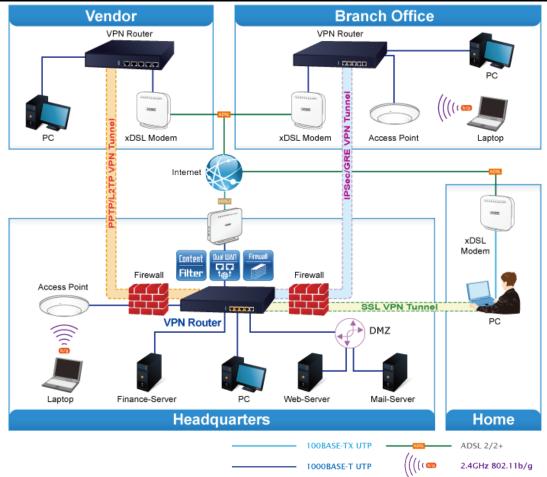
Furthermore, the VR-300 series can connect dual IPv4/v6 WANs with up to two different ISPs and supports many popular security features including Content Filtering to block specific URL feature that can automatically resolve the IP address corresponding to all. Users' network can be easily managed by just typing the URL of the websites like Facebook, YouTube and Yahoo.



The VR-300 series has link redundancy, MAC/IP filtering, outbound load balancing, QoS and many more functions to make the entire network system better. It creates a stable and qualified VPN security connection for many important applications such as VoIP, video conferencing and data transmission. The VR-300's economical price and complete network security management features make it an inevitable choice for the next-generation office network load balancer.



### Enterprise 5-Port 10/100/1000T VPN Security Router VR-300 series





### 1.4 Features

### Highlights

- Dual-WAN failover and Dual-WAN load balancing
- SSL VPN and robust hybrid VPN (IPSec/PPTP/L2TP over IPSec)
- Stateful Packet Inspection (SPI) firewall and content filtering
- Blocks DoS/DDOS attack, port range forwarding
- High Availability, AP Controller, Captive Portal and RADIUS
- Compliant with the IEEE 802.3at PoE+ with PD alive check and schedule management
- Planet Universal Network Management System and CloudViewer app supported

### Hardware

- 5 10/100/1000BASE-T RJ45 ports
- 4 10/100/1000BASE-T RJ45 ports + 1 1000BASE-X mini-GBIC/SFP slot (VR-300F and VR-300FP)
- 1 undefined Ethernet port (LAN/WAN) for Dual-WAN function
- 1 USB 3.0 port for system configuration backup and restoration
- Desktop installation or rack mounting

### RF Interface Characteristics

### VR-300W5 and VR-300PW5

- Features 2.4GHz (802.11b/g/n) and 5GHz (802.11a/n/ac) concurrent dual band for more efficiency of carrying high load of traffic
- 2T2R MIMO technology for enhanced throughput and coverage
- Provides multiple adjustable transmit power control
- High speed up to 1.2Gbps (300Mbps for 2.4GHz + 867Mbps for 5GHz) wireless data rate

### VR-300W6A and VR-300PW6A

- Features 2.4GHz (802.11b/g/n/ax) and 5GHz (802.11a/n/ac/ax) selectable dual band for carrying high load traffic
- 4T4R MIMO technology for enhanced throughput and coverage
- Provides multiple adjustable transmit power control
- High-speed wireless data rate of up to 2.4Gbps (600Mbps for 2.4GHz or 2400Mbps for 5GHz)

### VR-300W6 and VR-300PW6

- Features 2.4GHz (802.11b/g/n/ax) and 5GHz (802.11a/n/ac/ax) concurrent dual band for more efficiency of carrying high load of traffic
- 2T2R MIMO technology for enhanced throughput and coverage



- Provides multiple adjustable transmit power control
- High-speed wireless data rate of up to 18Gbps (600Mbps for 2.4GHz and 1200Mbps for 5GHz)

### Power over Ethernet (PoE model only)

- Complies with IEEE 802.3at Power over Ethernet Plus, end-span PSE
- Backward compatible with IEEE 802.3af Power over Ethernet
- Up to 4 ports of IEEE 802.3af / 802.3at devices powered
- Supports PoE power up to 36 watts for each PoE port
- Auto detects powered device (PD)
- Circuit protection prevents power interference between ports
- PoE management
  - Total PoE power budget control
  - Per port PoE function enable/disable
  - PoE port power feeding priority
  - Per PoE port power limitation
  - PD classification detection
  - PD alive check
  - PoE schedule

### > IP Routing Feature

- Static Route
- Dynamic Route
- OSPF

### Firewall Security

- Cybersecurity
- Stateful Packet Inspection (SPI) firewall
- Blocks DoS/DDoS attack
- Content Filtering
- MAC Filtering and IP Filtering
- NAT ALGs (Application Layer Gateway)
- Blocks SYN/ICMP Flooding

### > VPN Features

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



### > Networking

- Outbound load balancing
- Failover for dual-WAN
- Static IP/DHCP client for WAN
- Protocols: TCP/IP, UDP, ARP, IPv4, IPv6
- Port forwarding
- DMZ
- SNMP
- DHCP server/NTP client
- MAC address clone
- DDNS: PLANET DDNS, PLANET Easy DDNS, DynDNS and No-IP
- Cybersecurity

### > Others

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



## **1.5 Product Specifications**

### **VR-300**

Product	Enterprise 5-Port 10/100/1000T VPN Security Router
Hardware Specifications	
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)
USB Port	1 USB 3.0 port for system configuration backup and restoration
Reset Button	Reset to factory default
Thermal Fan	Fanless
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green)
Installation	Desktop installation or rack mounting
Power Requirements	100~240V AC, 50/60Hz, auto-sensing
Power Consumption	Max.13W
Weight	1.4kg
Dimensions (W x D x H)	330 x 155 x 43.5 mm
Enclosure	Metal
Security Service	
Firewall Security	Cybersecurity Stateful Packet Inspection (SPI) DoS/DDoS Attack Defense
ALG (Application Layer Gateway)	SIP, RTSP, FTP, H.323, TFTP
NAT	Port forwarding DMZ Host UPnP
Content Filtering	MAC filtering IP filtering Web filtering
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)
Networking	
Operation Mode	Routing mode
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF
VLAN	802.1q Tag-based, Port-based, Multi-VLAN
Multicast	IGMP Proxy
NAT Throughput	Max. 900Mbps
Outbound Load Balancing	Supported algorithms: Weight
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control SD-WAN* *Note: The feature will be available via firmware upgrade.
VPN VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server,



#### Enterprise 5-Port 10/100/1000T VPN Security Router VR-300 series

	L2TP Server, SSL Server/Client (Open VPN)	
VPN Tunnels	Max. 60	
VPN Throughput	Max. 60Mbps	
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting	
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm	
Management		
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported	
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3	
System Log	System Event Log	
Others	Setup wizard Dashboard System Status/Service Statistics Connections Status Auto reboot Diagnostics	
Standards Conformance		
Regulatory Compliance	CE, FCC	
Environment Specifications		
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	

### **VR-300P**

Product	Enterprise 4-Port 10/100/1000T 802.3at PoE + 1-Port 10/100/1000T VPN Security Router	
Hardware Specifications		
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)	
USB Port	1 USB 3.0 port for system configuration backup and restoration	
Reset Button	Reset to factory default	
Thermal Fan	1	
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green) PoE-in-Use LED (Amber)	
Installation	Desktop installation or rack mounting	
Power Requirements	100~240V AC, 50/60Hz, auto-sensing	
Power Consumption / Dissipation	Max.121 watts	
Weight	1.6kg	
Dimensions (W x D x H)	330 x 155 x 43.5 mm, 1U height	
Enclosure	Metal	
Power over Ethernet		
PoE Standard	IEEE 802.3af / 802.3at PoE+ PSE	
PoE Power Supply Type	End-span	
PoE Power Output	Per port 52V DC, 36 watts (max.)	



Power Pin Assignment	1/2 (+), 3/6 (-)
PoE Power Budget	120 watts (max.) @ 25 degrees C 100 watts (max.) @ 50 degrees C
Max. Number of Class 4 PDs	4
PoE Management	PD Alive Check Scheduled Power Recycling PoE Schedule PoE Usage Monitoring
Security Service	
Firewall Security	Cybersecurity Stateful Packet Inspection (SPI) Blocks DoS/DDoS attack
ALG (Application Layer Gateway	SIP, RTSP, FTP, H.323, TFTP
NAT	Port forwarding DMZ Host UPnP
Content Filtering	MAC filtering IP filtering Web filtering
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)
Networking	
Operation Mode	Routing mode
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF
VLAN	802.1q Tag-based, Port-based, Multi-VLAN
Multicast	IGMP Proxy
NAT Throughput	Max. 900Mbps
Outbound Load Balancing	Supported algorithms: Weight
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control SD-WAN* *Note: The feature will be available via firmware upgrade.
VPN	
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)
VPN Tunnels	Max. 60
VPN Throughput	Max. 60Mbps
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm
Management	
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3
System Log	System Event Log
Others	Setup wizard Dashboard System Status/Service Statistics Connections Status



	Auto reboot Diagnostics
Standards Conformance	
Regulatory Compliance	CE, FCC
Environment Specifications	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)



### **VR-300F**

Product	Enterprise 4-Port 10/100/1000T + 1-Port 1000X SFP VPN Security Router
Hardware Specifications	
Ethernet	4 10/100/1000BASE-T RJ45 Ethernet ports including 1 1000BASE-X mini-GBIC/SFP slot 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)
USB Port	1 USB 3.0 port for system configuration backup and restoration
Reset Button	Reset to factory default
Thermal Fan	Fanless
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green)
Installation	Desktop installation or rack mounting
Power Requirements	100-240V AC, 1A max.
Power Consumption	Max.3.7W
Weight	1.3kg
Dimensions (W x D x H)	330 x 155 x 43.5 mm
Enclosure	Metal
Security Service	
Firewall Security	Cybersecurity Stateful Packet Inspection (SPI) DoS/DDoS Attack Defense
ALG (Application Layer Gateway)	SIP, RTSP, FTP, H.323, TFTP
NAT	Port forwarding DMZ Host UPnP
Content Filtering	MAC filtering IP filtering Web filtering
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)
Networking	
Operation Mode	Routing mode
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF
VLAN	802.1q Tag-based, Port-based, Multi-VLAN
Multicast	IGMP Proxy
NAT Throughput	Max. 900Mbps
Outbound Load Balancing	Supported algorithms: Weight
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control SD-WAN* *Note: The feature will be available via firmware upgrade.
VPN	
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)



VPN Tunnels	Max. 60	
VPN Throughput	Max. 60Mbps	
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting	
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm	
Management		
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported	
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3	
System Log	System Event Log	
Others	Setup wizard Dashboard System Status/Service Statistics Connections Status Auto reboot Diagnostics	
Standards Conformance		
Regulatory Compliance	CE, FCC	
Environment Specifications		
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	

### VR-300FP

Product	Enterprise 4-Port 10/100/1000T 802.3at PoE + 1-Port 1000X SFP VPN Security Router		
Hardware Specifications			
Ethernet	4 10/100/1000BASE-T RJ45 Ethernet ports including 1 1000BASE-X mini-GBIC/SFP slot 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)		
USB Port	1 USB 3.0 port for system configuration backup and restoration		
Reset Button	Reset to factory default		
Thermal Fan	1		
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green) PoE-in-Use LED (Amber)		
Installation	Desktop installation or rack mounting		
Power Requirements	100~240V AC, 50/60Hz, auto-sensing		
Power Consumption / Dissipation	Max.132 watts		
Weight	1.5kg		
Dimensions (W x D x H)	330 x 155 x 43.5 mm, 1U height		
Enclosure	Metal		
Power over Ethernet			
PoE Standard	IEEE 802.3af / 802.3at PoE+ PSE		
PoE Power Supply Type	End-span		
PoE Power Output	Per port 52V DC, 36 watts (max.)		



Power Pin Assignment	1/2 (+), 3/6 (-)	
PoE Power Budget	120 watts (max.) @ 25 degrees C 100 watts (max.) @ 50 degrees C	
Max. Number of Class 4 PDs	4	
PoE Management	PD Alive Check Scheduled Power Recycling PoE Schedule PoE Usage Monitoring	
Security Service		
Firewall Security	Cybersecurity Stateful Packet Inspection (SPI) Blocks DoS/DDoS attack	
ALG (Application Layer Gateway	SIP, RTSP, FTP, H.323, TFTP	
NAT	Port forwarding DMZ Host UPnP	
Content Filtering	MAC filtering IP filtering Web filtering	
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)	
Networking		
Operation Mode	Routing mode	
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF	
VLAN	802.1q Tag-based, Port-based, Multi-VLAN	
Multicast	IGMP Proxy	
NAT Throughput	Max. 900Mbps	
Outbound Load Balancing	Supported algorithms: Weight	
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,	
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control SD-WAN* *Note: The feature will be available via firmware upgrade.	
VPN		
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)	
VPN Tunnels	Max. 60	
VPN Throughput	Max. 60Mbps	
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting	
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm	
Management	Web browser	
Basic Management Interfaces	SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported	
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3	
System Log	System Event Log	
Others	Setup wizard Dashboard System Status/Service Statistics Connections Status	



	Auto reboot Diagnostics	
Standards Conformance		
Regulatory Compliance	CE, FCC	
Environment Specifications		
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	



### VR-300W5

Product	Wi-Fi 5 AC1	1200 Dual Band VPN Security Router	
Hardware Specifications			
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)		
USB Port	1 USB 3.0 p	port for system configuration backup and restoration	
Reset Button	Reset to fac	ctory default	
Thermal Fan	Fanless		
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green) 2.4G (Green) 5G (Green)		
Installation	Desktop ins	stallation or rack mounting	
Power Requirements	100~240V A	AC, 50/60Hz, auto-sensing	
Power Consumption	Max. 24W		
Weight	1.6kg		
Dimensions (W x D x H)	330 x 155 x	: 43.5 mm	
Enclosure	Metal		
Wireless			
Standard	IEEE 802.11 b/g/n 2.4 GHz IEEE 802.11 a/n/ac 5 GHz		
Band Mode	2.4G / 5G c	oncurrent mode	
Frequency Range	2.4GHz	America FCC: 2.412~2.462GHz Europe ETSI: 2.412~2.484GHz	
	5GHz	America FCC: 5.180~5.240GHz, 5.725~5.850GHz Europe ETSI: 5.180~5.240GHz	
	2.4GHz	America FCC: 1~11 Europe ETSI: 1~13	
Operating Channels		America FCC: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140	
	5GHz	Europe ETSI: Non-DFS: 36, 40, 44, 48 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 5GHz channel list may vary in different countries according to their regulations.	
Channel Width	802.11ac: 20/40/80MHz 802.11n: 20/40MHz		
Data Transmission Rates	Transmit: 300 Mbps* for 2.4 GHz and 867 Mbps* for 5 GHz Receive: 300 Mbps* for 2.4 GHz and 867 Mbps* for 5 GHz		
	*The estim	ated transmission distance is based on the theory.	



	The actual distance may vary in different environments.	
	<=20dBm (2.4G frequency band: 2.400 – 2.4835 GHz)	
Transmission Power	<=20dBm (2.4G frequency band: 2.400 – 2.4055 GHz)	
	WEP (64/128-bit) encryption security	
Encryption Security	WPA / WPA2 (TKIP/AES)	
Encryption Security	WPA-PSK / WPA2-PSK (TKIP/AES)	
	802.1x Authenticator	
	Wi-Fi Multimedia (WMM)	
Wireless Advanced	Auto channel selection Wireless output power management	
	MAC address filtering	
Security Service		
	Cybersecurity	
Firewall Security	Stateful packet inspection (SPI)	
	DoS/DDoS attack defense	
ALG (Application Layer Gateway	SIP, RTSP, FTP, H.323, TFTP	
NAT	Port forwarding DMZ host	
	UPnP	
	MAC filtering	
Content Filtering	IP filtering	
	Web filtering	
	Outbound load balancing	
Bandwidth Management	Failover for dual-WAN	
Networking	QoS (Quality of Service)	
Operation Mode	Routing mode	
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF	
VLAN	802.1q Tag-based, Port-based, Multi-VLAN	
Multicast	IGMP Proxy	
NAT Throughput	Max. 900Mbps	
Outbound Load Balancing	Supported algorithms: Weight	
	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET	
Protocol	DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,	
	HA (High Availability)	
Key Features	Captive Portal	
	RADIUS Server/Client AP Control	
VPN		
	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server,	
VPN Function	L2TP Server, SSL Server/Client (Open VPN)	
VPN Tunnels	Max. 60	
VPN Throughput	Max. 60Mbps	
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting	
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm	
Management		
	Web browser	
<b>Basic Management Interfaces</b>	SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported	
	Planet CloudViewer APP	
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3	
System Log	System Event Log	
	Setup wizard	
Others	Dashboard	
	System status/service	



	Statistics Connections status Auto reboot Diagnostics	
Standards Conformance		
Regulatory Compliance	CE, FCC	
Environment Specifications		
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	

### VR-300PW5

	Wi Ei 5 AC4200 Duel Dand V/DN Coourity Douter with 4 Dart 802 Oct	
Product	Wi-Fi 5 AC1200 Dual Band VPN Security Router with 4-Port 802.3at PoE+	
Model	VR-300PW5	
Hardware Specifications		
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)	
USB Port	1 USB 3.0 port for system configuration backup and restoration	
Reset Button	Reset to factory default	
Thermal Fan	1	
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green) 2.4G (Green) 5G (Green) PoE-in-Use LED (Amber)	
Installation	Desktop installation or rack mounting	
Power Requirements	100~240V AC, 50/60Hz, auto-sensing	
Power Consumption	Max. 140W	
Weight	1.7kg	
Dimensions (W x D x H)	330 x 155 x 43.5 mm	
Enclosure	Metal	
Power over Ethernet		
PoE Standard	IEEE 802.3af / 802.3at PoE+ PSE	
PoE Power Supply Type	End-span	
PoE Power Output	Per port 52V DC, 36 watts (max.)	
Power Pin Assignment	1/2 (+), 3/6 (-)	
PoE Power Budget	120 watts (max.) @ 25 degrees C100 watts (max.) @ 50 degrees C	
Max. Number of Class 4 PDs	4	



PoE Management	PD alive check Scheduled power recycling PoE schedule PoE usage monitoring	
Wireless		
Standard	IEEE 802.11 b/g/n 2.4 GHz IEEE 802.11 a/n/ac 5 GHz	
Band Mode	2.4G / 5G c	oncurrent mode
Frequency Range	2.4GHz	America FCC: 2.412~2.462GHz Europe ETSI: 2.412~2.484GHz
	5GHz	America FCC: 5.180~5.240GHz, 5.725~5.850GHz Europe ETSI: 5.180~5.240GHz
	2.4GHz	America FCC: 1~11 Europe ETSI: 1~13
Operating Channels		America FCC: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140
	5GHz	Europe ETSI: Non-DFS: 36, 40, 44, 48 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 5GHz channel list will vary in different countries according to their regulations.
Channel Width	802.11ac: 2 802.11n: 20	0/40/80MHz
Data Transmission Rates	Transmit: 300 Mbps* for 2.4 GHz and 867 Mbps* for 5 GHz Receive: 300 Mbps* for 2.4 GHz and 867 Mbps* for 5 GHz *The estimated transmission distance is based on the theory. The actual distance may vary in different environments.	
Transmission Power	<pre>&lt;=20dBm (2.4G frequency band: 2.400 – 2.4835 GHz) &lt;=23dBm (5G frequency band: 5.150 – 5.350 GHz)</pre>	
Encryption Security	WEP (64/128-bit) encryption security WPA / WPA2 (TKIP/AES) WPA-PSK / WPA2-PSK (TKIP/AES) 802.1x Authenticator	
Wireless Advanced	Wi-Fi Multimedia (WMM) Auto channel selection Wireless output power management MAC address filtering	
Security Service		
Firewall Security	Cybersecurity Stateful Packet Inspection (SPI) DoS/DDoS Attack Defense	
ALG (Application Layer Gateway)	SIP, RTSP, FTP, H.323, TFTP	
NAT	Port forward DMZ Host UPnP	ding



Content Filtering	MAC filtering IP filtering Web filtering	
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)	
Networking		
Operation Mode	Routing mode	
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF	
VLAN	802.1q Tag-based, Port-based, Multi-VLAN	
Multicast	IGMP Proxy	
NAT Throughput	Max. 900Mbps	
Outbound Load Balancing	Supported algorithms: Weight	
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,	
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control	
VPN		
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)	
VPN Tunnels	Max. 60	
VPN Throughput	Max. 60Mbps	
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting	
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm	
Management		
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported Planet CloudViewer APP	
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3	
System Log	System Event Log	
Others	Setup wizard Dashboard System Status/Service Statistics Connections Status Auto reboot Diagnostics	
Standards Conformance		
Regulatory Compliance	CE, FCC	
Environment Specifications		
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	





### VR-300W6A

Product	Wi-Fi 6 AX2400 2.4GHz/5GHz VPN Security Router		
Model	VR-300W6A		
Hardware Specifications			
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)		
USB Port	1 USB 3.0 p	oort for system configuration backup and restoration	
Reset Button	Reset to fac	tory default	
Fanless	Yes		
Installation	Desktop ins	tallation or rack mounting	
Power Requirements		AC, 50/60Hz, auto-sensing	
Power Consumption	Max.26 wat	ts	
Weight	1.5kg		
Dimensions (W x D x H)	330 x 155 x	43.5 mm	
Enclosure	Metal		
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green) 2.4G (Green) 5G (Green)		
Wireless			
Standard	IEEE 802.11a/n/ac/ax 5GHz IEEE 802.11g/b/n/ax 2.4GHz		
Band Mode	2.4G / 5G s	electable mode	
From Dongo	2.4GHz	America FCC: 2.412~2.462GHz Europe ETSI: 2.412GHz~2.472GHz	
Frequency Range	5GHz	America FCC: 5.180~5.240GHz, 5.745~5.825GHz Europe ETSI: 5.180~5.700GHz	
	2.4GHz	America FCC: 1~11 Europe ETSI: 1~13	
		America FCC: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	
Operating Channels	5GHz	Europe ETSI: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	
		5GHz channel list may vary in different countries according to their regulations.	
Channel Width		/Hz, 80MHz, 80+80 MHz	
	Transmit: 600 Mbps* for 2.4 GHz or 2400 Mbps* for 5 GHz		
Data Transmission Rates	Receive: 600	0 Mbps* for 2.4 GHz or 2400 Mbps* for 5 GHz	
		ated transmission distance is based on the theory. distance may vary in different environments.	
		+/- 1.5dbm @11Mbps	
Transmission Power	11g: 20dbm+/- 1.5dbm @54Mbps 11g/n: 20dBm +/- 1.5dbm @MCS7, HT20		



Encryption Security	17dBm@MCS7,HT40 11a: 19.5dBm +/- 1.5dbm @54Mbps 11a/n: 19.5dBm+/- 1.5dbm @MCS7, HT20 17dBm@MCS7, HT40 11ac HT20: 20+/-1.5dBm @MCS8 11ac HT40: 17+/-1.5dBm @MCS9 11ac HT80: 14.5+/-1.5dBm @MCS9 11ax HT20: 20+/-1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9 11ax HT80: 14.5 +/- 1.5dBm @MCS9 11ax HT80 +/- 1.5dBm &/- 1.5dBm
Wireless Advanced	WPA-PSK / WPA2-PSK (TKIP/AES) / WPA3-PSK (TKIP/AES) 802.1x Authenticator Wi-Fi Multimedia (WMM) Auto channel selection Wireless output power management
	MAC address filtering
Security Service	
Firewall Security	Cybersecurity Stateful Packet Inspection (SPI) DoS/DDoS Attack Defense
ALG (Application Layer Gateway)	SIP, RTSP, FTP, H.323, TFTP
NAT	Port forwarding DMZ Host UPnP
Content Filtering	MAC filtering IP filtering Web filtering
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)
Networking	
Operation Mode	Routing mode
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF
VLAN	802.1q Tag-based, Port-based, Multi-VLAN
Multicast	IGMP Proxy
NAT Throughput	Max. 900Mbps
Outbound Load Balancing	Supported algorithms: Weight
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control
VPN	
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)
VPN Tunnels	Max. 60
VPN Throughput	Max. 60Mbps
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm
Management	
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported



	Planet CloudViewer APP	
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3	
System Log	System Event Log	
Others	Setup wizard Dashboard System Status/Service Statistics Connections Status Auto reboot Diagnostics	
Standards Conformance		
Regulatory Compliance	CE, FCC	
Environment Specifications		
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	

### **VR-300PW6A**

Product	Wi-Fi 6 AX2400 2.4GHz/5GHz VPN Security Router with 4-Port 802.3at PoE+	
Hardware Specifications		
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)	
USB Port	1 USB 3.0 port for system configuration backup and restoration	
Reset Button	Reset to factory default	
Thermal Fan	1	
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green) 2.4G (Green) 5G (Green) PoE-in-Use LED (Amber)	
Installation	Desktop installation or rack mounting	
Power Requirements	100~240V AC, 50/60Hz, auto-sensing	
Power Consumption	Max.145 watts	
Weight	1.7kg	
Dimensions (W x D x H)	330 x 155 x 43.5 mm	
Enclosure	Metal	
Power over Ethernet		
PoE Standard	IEEE 802.3af / 802.3at PoE+ PSE	
PoE Power Supply Type	End-span	
PoE Power Output	Per port 52V DC, 36 watts (max.)	
Power Pin Assignment	1/2 (+), 3/6 (-)	
PoE Power Budget	120 watts (max.) @ 25 degrees C 100 watts (max.) @ 50 degrees C	
Max. Number of Class 4 PDs	4	
PoE Management	PD alive check Scheduled power recycling PoE schedule PoE usage monitoring	



Γ

1

Wireless			
Standard	IEEE 802.11a/n/ac/ax 5GHz IEEE 802.11g/b/n/ax 2.4GHz		
Band Mode	2.4G / 5G selectable mode		
Frequency Range	2.4GHz 5GHz	America FCC: 2.412~2.462GHz Europe ETSI: 2.412GHz~2.472GHz America FCC: 5.180~5.240GHz, 5.745~5.825GHz	
	2.4GHz	Europe ETSI: 5.180~5.700GHz America FCC: 1~11 Europe ETSI: 1_42	
Operating Channels	5GHz	Europe ETSI: 1~13 America FCC: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 Europe ETSI: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 5GHz channel list may vary in different countries according to their regulations.	
Channel Width	20MHz, 40MHz,	80MHz, 80+80 MHz	
Data Transmission Rates	Transmit: 600 Mbps* for 2.4 GHz or 2400 Mbps* for 5 GHz Receive: 600 Mbps* for 2.4 GHz or 2400 Mbps* for 5 GHz *The estimated transmission distance is based on the theory. The actual distance may vary in different environments.		
Transmission Power	11b: 23dbm+/- 1.5dbm @11Mbps 11g: 20dbm+/- 1.5dbm @54Mbps 11g/n: 20dBm +/- 1.5dbm @MCS7, HT20 17dBm@MCS7,HT40 11a: 19.5dBm +/- 1.5dbm @54Mbps 11a/n: 19.5dBm+/- 1.5dbm @MCS7, HT20 17dBm@MCS7, HT40 11ac HT20: 20+/-1.5dBm @MCS8 11ac HT40: 17+/-1.5dBm @MCS9 11ac HT80: 14.5+/-1.5dBm @MCS9 11ax HT20: 20+/-1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9		
Encryption Security	11ax H180: 14.5 +/- 1.5dBm @MCS11WEP (64/128-bit) encryption securityWPA / WPA2 (TKIP/AES)WPA-PSK / WPA2-PSK (TKIP/AES) / WPA3-PSK (TKIP/AES)802.1x Authenticator		
Wireless Advanced	Wi-Fi Multimedia (WMM) Auto channel selection Wireless output power management MAC address filtering		
Security Service			
Firewall Security	Cybersecurity Stateful Packet Inspection (SPI) DoS/DDoS Attack Defense		
ALG (Application Layer Gateway)	SIP, RTSP, FTP, Port forwarding	H.323, TFTP	
	DMZ Host		



	UPnP		
Content Filtering	MAC filtering IP filtering Web filtering		
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)		
Networking			
Operation Mode	Routing mode		
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF		
VLAN	802.1q Tag-based, Port-based, Multi-VLAN		
Multicast	IGMP Proxy		
NAT Throughput	Max. 900Mbps		
Outbound Load Balancing	Supported algorithms: Weight		
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,		
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control		
VPN			
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)		
VPN Tunnels	Max. 60		
VPN Throughput	Max. 60Mbps		
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting		
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm		
Management			
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported Planet CloudViewer APP		
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3		
System Log	System Event Log		
Others	Setup wizard Dashboard System Status/Service Statistics Connections Status Auto reboot Diagnostics		
Standards Conformance			
Regulatory Compliance	CE, FCC		
Environment Specifications			
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)		
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)		



### VR-300W6

Hardware SpecificationsEthernet5 10/100/1000 3 LAN ports (F 1 LAN/WAN port 1 WAN port (F 1 WAN port (F 1 USB 3.0 portUSB Port1 USB 3.0 port Reset ButtonReset ButtonReset to factor FanlessThermal FanFanlessLED IndicatorsPWR (Green) Internet (Green) 5G (Green)InstallationDesktop install	hort-5) t for system configuration backup and restoration ry default n) een) lation or rack mounting , 50/60Hz, auto-sensing		
Ethernet3 LAN ports (F 1 LAN/WAN por 1 WAN port (P)USB Port1 USB 3.0 portReset ButtonReset to factorThermal FanFanlessLED IndicatorsPWR (Green) 1 nternet (Green) 5G (Green)InstallationDesktop install 100~240V AC, Power Consumption	Port-1 to Port-3) port (Port-4) (ort-5) t for system configuration backup and restoration ry default n) een) lation or rack mounting , 50/60Hz, auto-sensing		
Reset ButtonReset to factorThermal FanFanlessPWR (Green)Internet (Green)LED IndicatorsLAN/WAN (Green)InstallationDesktop instalPower Requirements100~240V AC,Power ConsumptionMax. 8W	ry default n) een) lation or rack mounting , 50/60Hz, auto-sensing		
Thermal FanFanlessLED IndicatorsPWR (Green) Internet (Green) 2.4G (Green) 5G (Green)InstallationDesktop install 100~240V AC, Power ConsumptionMax. 8W	n) een) lation or rack mounting , 50/60Hz, auto-sensing		
LED IndicatorsPWR (Green) Internet (Green) 2.4G (Green) 5G (Green)InstallationDesktop install 100~240V AC, Power ConsumptionMax. 8W	een) lation or rack mounting , 50/60Hz, auto-sensing		
LED IndicatorsInternet (Green LAN/WAN (Gr 2.4G (Green) 5G (Green)InstallationDesktop installPower Requirements100~240V AC Max. 8W	een) lation or rack mounting , 50/60Hz, auto-sensing		
Power Requirements100~240V ACPower ConsumptionMax. 8W	, 50/60Hz, auto-sensing		
Power Consumption Max. 8W			
·			
Weight 1.7kg			
<b>Dimensions (W x D x H)</b> 330 x 155 x 43	3.5 mm		
Enclosure Metal	Metal		
Wireless			
Standard IEEE 802.11g/	IEEE 802.11a/n/ac/ax 5GHz IEEE 802.11g/b/n/ax 2.4GHz		
Band Mode 2.4G / 5G cond	current mode		
Frequency Range	America FCC: 2.412~2.462GHz urope ETSI: 2.412GHz~2.472GHz 15GHz ~5.875GHz		
2.40HZ E	America FCC: 1~11 Europe ETSI: 1~13		
	America FCC: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140		
1	Europe ETSI: Non-DFS: 36, 40, 44, 48 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140		
	GHz channel list will vary in different countries coording to their regulations.		
Data Transmission Rates       Receive: 600 f         *The estimated	Transmit: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz Receive: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz *The estimated transmission distance is based on the theory. The actual distance will vary in different environments.		
	11b: 23dbm+/- 1.5dbm @11Mbps		



	VR-JUU Series	
	11g: 20dbm+/- 1.5dbm @54Mbps 11g/n: 20dBm +/- 1.5dbm @MCS7, HT20 17dBm@MCS7,HT40 11a: 19.5dBm +/- 1.5dbm @54Mbps 11a/n: 19.5dBm+/- 1.5dbm @MCS7, HT20 17dBm@MCS7, HT40 11ac HT20: 20+/-1.5dBm @MCS8 11ac HT40: 17+/-1.5dBm @MCS9 11ac HT80: 14.5+/-1.5dBm @MCS9 11ax HT20: 20+/-1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9 11ax HT80: 14.5 +/- 1.5dBm @MCS9	
Encryption Security	WEP (64/128-bit) encryption security WPA / WPA2 (TKIP/AES) WPA-PSK / WPA2-PSK (TKIP/AES) / WPA3-PSK (TKIP/AES) 802.1x Authenticator	
Wireless Advanced	Wi-Fi Multimedia (WMM) Auto channel selection Wireless output power management MAC address filtering	
Security Service		
Firewall Security	Cybersecurity Stateful packet inspection (SPI) DoS/DDoS attack defense	
ALG (Application Layer Gateway	SIP, RTSP, FTP, H.323, TFTP	
NAT	Port forwarding DMZ host UPnP	
Content Filtering	MAC filtering IP filtering Web filtering	
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)	
Networking		
Operation Mode	Routing mode	
Routing Protocol	Static Route, Dynamic Route (RIP), OSPF	
VLAN	802.1q Tag-based, Port-based, Multi-VLAN	
Multicast	IGMP Proxy	
NAT Throughput	Max. 900Mbps	
Outbound Load Balancing	Supported algorithms: Weight	
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,	
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control	
VPN		
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)	
VPN Tunnels	Max. 60	
VPN Throughput	Max. 60Mbps	
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting	
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm	
Management		
Basic Management Interfaces	Web browser	



	SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported Planet CloudViewer APP
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3
System Log	System Event Log
Others	Setup wizard Dashboard System status/service Statistics Connections status Auto reboot Diagnostics
Standards Conformance	
Regulatory Compliance	CE, FCC
Environment Specifications	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

#### **VR-300PW6**

Product	Wi-Fi 6 AC1800 Dual Band VPN Security Router with 4-Port 802.3at PoE+
Hardware Specifications	
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Port-1 to Port-3) 1 LAN/WAN port (Port-4) 1 WAN port (Port-5)
USB Port	1 USB 3.0 port for system configuration backup and restoration
Reset Button	Reset to factory default
Thermal Fan	1
LED Indicators	PWR (Green) Internet (Green) LAN/WAN (Green) 2.4G (Green) 5G (Green) PoE-in-Use LED (Amber)
Installation	Desktop installation or rack mounting
Power Requirements	100~240V AC, 50/60Hz, auto-sensing
Power Consumption	Max. 133W
Weight	1.7kg
Dimensions (W x D x H)	330 x 155 x 43.5 mm
Enclosure	Metal
Power over Ethernet	
PoE Standard	IEEE 802.3af / 802.3at PoE+ PSE
PoE Power Supply Type	End-span
PoE Power Output	Per port 52V DC, 36 watts (max.)
Power Pin Assignment	1/2 (+), 3/6 (-)
PoE Power Budget	120 watts (max.) @ 25 degrees C 100 watts (max.) @ 50 degrees C
Max. Number of Class 4 PDs	4
PoE Management	PD alive check Scheduled power recycling



	PoE schedu	le
	PoE usage i	monitoring
Wireless		
Standard		a/n/ac/ax 5GHz g/b/n/ax 2.4GHz
Band Mode	2.4G / 5G co	oncurrent mode
Frequency Range	2.4GHz	2.4GHz
Trequency Range	5GHz	5GHz
Operating Channels	2.4GHz	2.4GHz
	5GHz	5GHz
Channel Width	20MHz, 40N	
Data Transmission Rates	Receive: 60	0 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz 0 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz
	actual distar	ted transmission distance is based on the theory. The new will vary in different environments.
Transmission Power	11g: 20dbm 11g/n: 20dB 17dBm@M0 11a: 19.5dB 11a/n: 19.5dB 11a/n: 19.5dC 17dBm@M0 11ac HT20: 11ac HT40: 11ac HT80: 11ax HT20: 11ax HT40: 11ax HT80:	m +/- 1.5dbm @54Mbps IBm+/- 1.5dbm @MCS7, HT20 CS7, HT40 20+/-1.5dBm @MCS8 17+/-1.5dBm @MCS9 14.5+/-1.5dBm @MCS9 20+/-1.5dBm @MCS9 17 +/- 1.5dBm @MCS9 14.5 +/- 1.5dBm @MCS11
Encryption Security	WPA/WPA	8-bit) encryption security 2 (TKIP/AES) WPA2-PSK (TKIP/AES) / WPA3-PSK (TKIP/AES) enticator
Wireless Advanced	Auto channe	put power management
Security Service		
Firewall Security		ty ket Inspection (SPI) Attack Defense
ALG (Application Layer Gateway)	SIP, RTSP, I	FTP, H.323, TFTP
NAT	Port forward DMZ Host UPnP	ing
Content Filtering	MAC filtering IP filtering Web filtering	- 
Bandwidth Management	Failover for	ad balancing dual-WAN y of Service)
Networking		
Operation Mode	Routing mod	
Routing Protocol		, Dynamic Route (RIP), OSPF
VLAN		based, Port-based, Multi-VLAN
Multicast	IGMP Proxy	



NAT Throughput	Max. 900Mbps
Outbound Load Balancing	Supported algorithms: Weight
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, , PPPoE, SNMPv1/v2c/v3,
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control
VPN	
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)
VPN Tunnels	Max. 60
VPN Throughput	Max. 60Mbps
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm
Management	
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported Planet CloudViewer APP
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3
System Log	System Event Log
Others	Setup wizard Dashboard System Status/Service Statistics Connections Status Auto reboot Diagnostics
Standards Conformance	
Regulatory Compliance	CE, FCC
Environment Specifications	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 60 degrees C Relative Humidity: 5 ~ 95% (non-condensing)



# **Chapter 2. Hardware Introduction**

# 2.1 Physical Descriptions

**Front View** 

VR-300	Enterprise 5-Port 10/100/1000T VPN Security Router
VR-300F	Enterprise 4-Port 10/100/1000T + 1-Port 1000X SFP VPN Security Router
VR-300W5	Wi-Fi 5 AC1200 Dual Band VPN Security Router
VR-300W6A	Wi-Fi 6 AX2400 2.4GHz/5GHz VPN Security Router
VR-300W6	Wi-Fi 6 AX1800 Dual Band VPN Security Router

### ■ LAN Per 10/100/1000Mbps PoE port (Port-1 to Port-4)

LED	Color	Function	
LNK/ACT G		LIGHTS.	To indicate the port is running at 1000Mbps or 100Mbps or 10Mbps and successfully established
	Green	Blink:	To indicate that the router is actively sending or receiving data over that port.



#### ■ WAN Per 10/100/1000Mbps RJ45 port (Port and Port-5)

LED	Color	Function	
LNK/ACT	Green	Lights.	To indicate the port is running at 1000Mbps or 100Mbps or 10Mbps and successfully established
		Blink:	To indicate that the router is actively sending or receiving data over that port.

LED	Color	Function
PWR	Green	Lights up when the power is on.
Internet	Green	Lights up when the router connects to internet successfully.
2.4G	Green	Lights up when 2.4G Wi-Fi service is enabled
5G	Green	Lights up when 5G Wi-Fi service is enabled



	Enterprise 4-Port 10/100/1000T 802.3at PoE + 1-Port 1000X SFP VPN Security Router
VR-300FP	



Wi-Fi 5 AC1200 Dual Band VPN Security Router with 4		
VR-300PW5		
	VR-300PW5	





VR-300PW6



### ■ LAN Per 10/100/1000Mbps PoE port (Port-1 to Port-4)

LED	Color	Function		
LNK/ACT		Lights.	To indicate the port is running at 1000Mbps or 100Mbps or 10Mbps and successfully established	
LINK/ACT	Green Blink:	BIINK:	To indicate that the router is actively sending or receiving data over that port.	
PoE	0		Lights:	To indicate the port is providing 48V~56VDC in-line power
PoE Orange	Off:	To indicate the connected device is not a PoE powered device (PD)		

### ■ WAN Per 10/100/1000Mbps RJ45 port (Port-4 and Port-5)

LED	Color	Function	
	LNK/ACT Green	Lights.	To indicate the port is running at 1000Mbps or 100Mbps or 10Mbps and successfully established
LINK/ACT		Blink:	To indicate that the router is actively sending or receiving data over that port.

LED		
PWR	Green	Lights up when the power is on.
Internet	Green	Lights up when the router connects to internet successfully.
Ports 1-5	Green	"Steady on" indicates the port is connected to other network device. "Blink" to indicate there is traffic on the port.
PoE Ports 1-4	Amber	Lights up when the port is providing 48V~56VDC in-line power
2.4G	Green	Lights up when 2.4G WiFi service is enabled
5G	Green	Lights up when 5G WiFi service is enabled

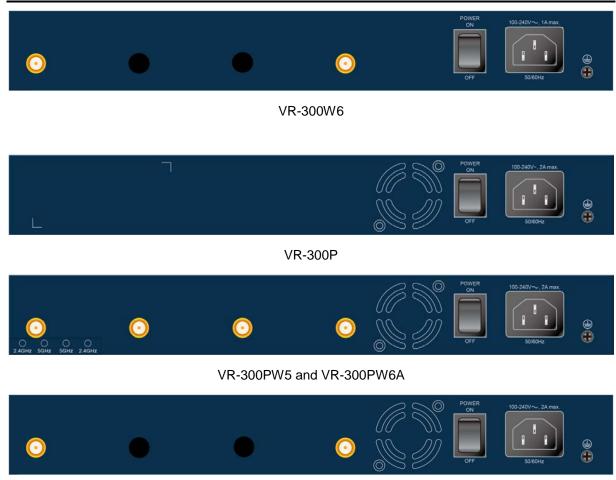
### **Rear View**



VR-300W5 and VR-300W6A



#### Enterprise 5-Port 10/100/1000T VPN Security Router VR-300 series



### VR-300PW6

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



# 2.2 Hardware Installation

To install the VR-300 Series on desktop, simply follow the following steps:

**Step 1**: For wireless models, fasten the 2.4G/5G antennas to the 2.4G/5G antenna connectors. And you can bend the antennas to fit your actual needs.



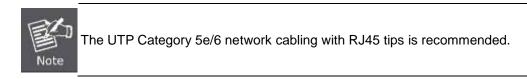
Step 2: Place the VPN Router on desktop.

Step 3: Keep enough ventilation space between the VPN Router and the surrounding objects.

When choosing a location, please keep in mind the environmental restrictions should be under the specifications of the VPN router.

Step 4: Connect your VPN Router to hub / switch.

- A. Connect one end of a standard network cable to the LAN port (port 1) on the front panel of the VPN router.
- B. Connect the other end of the cable to the hub / switch.



Step 5: Connect your VPN Router to internet.

- A. Connect one end of a standard network cable to the WAN port (port 5) on the front panel of the VPN router.
- B. Connect the other end of the cable to the ADSL router's LAN port or an upper layer port to outer network layer.



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 6: Connect the included power cord to an AC 100-240V wall outlet. When the VPN router receives power, the Power LED should remain solid Green.



# **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

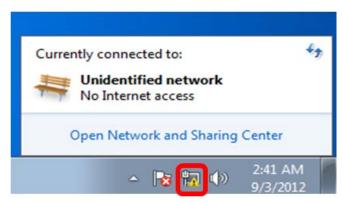
The default IP address of the VPN router is 192.168.1.1, and the DHCP Server is on. Please set the IP address of the connected PC as DHCP client, and the PC will get IP address automatically from the VPN router.

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

### Windows 7/8

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

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





2. Click "Change adapter settings".

Control Panel	<ul> <li>Network and Internet</li> <li>Network and Sharing Center</li> </ul>	r - 49 Search Control Panel
Control Panel Home	View your basic network information a	and set up connections
Change adapter settings Change advanced sharing settings	PC Unidentified (This computer) View your active networks	I network Internet Connect or disconnect
	Unidentified network Public network	Access type: No Internet access Connections: Uccal Area Connection
	Change your networking settings Set up a new connection or network Set up a wireless, broadband, dial-up, ad Connect to a network Connect or reconnect to a wireless, wired	l hoc, or VPN connection; or set up a router or access point. d, dial-up, or VPN network connection.
	Choose homegroup and sharing options Access files and printers located on othe Troubleshoot problems Diagnose and repair network problems, o	r network computers, or change sharing settings.
See also		
HomeGroup		
Internet Options Windows Firewall		

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

Intel(R) PRO/100	9	Disable
		Status
		Diagnose
	6	Bridge Connections
		Create Shortcut
	0	Delete
	0	Rename
	(	Properties



4. 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/1	1000 MT Network Connection
	Configure
This connection uses	
Client for Mic	
QoS Packet	
	ter Sharing for Microsoft Networks
	tocol Version 6 (TCP/IPv6)
	tocol Version 4 (TCP/IPv4) Topology Discovery Mapper I/O Driver
	Topology Discovery Responder
Install	Uninstall Properties
Description	
	rol Protocol/Internet Protocol. The default
wide area actuade	protocol that provides communication
	erconnected networks.



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

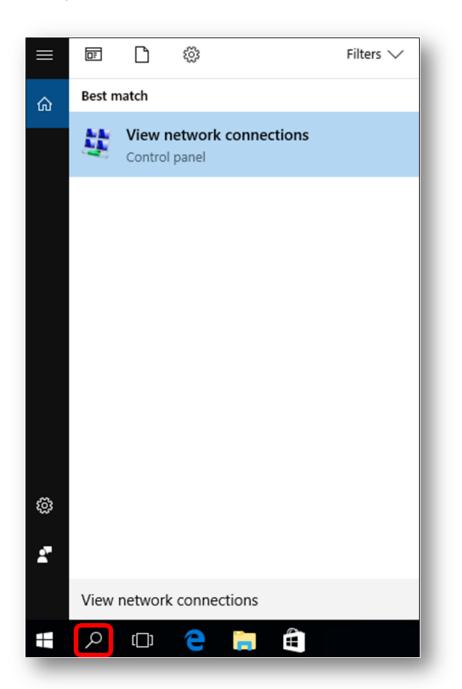
Alternate Configuration Du can get IP settings assigned autor				
ipports this capability. Otherwise, yo Iministrator for the appropriate IP se		o ask y	our netv	vork
Obtain an IP address automatica	lly			
Use the following IP address:				
IP address:				
S <u>u</u> bnet mask:				
<u>D</u> efault gateway:				
Obtain DNS server address autor	a ati ca lla	1		
Use the following DNS server address addres				
Preferred DNS server :				
<u>A</u> lternate DNS server:				
Validate settings upon exit			Ady	anced
	_			



### 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.

	Local Area Conne Unidentified netw		1
	Intel(R) PRO/1000	•	Disable
			Status
			Diagnose
		•	Bridge Connections
			Create Shortcut
			Delete
		0	Rename
		۲	Properties
_		۲	Properties

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

onnect using:		
Intel(R) PRO	/1000 MT Network Con	nection
		Configure
his connection use	es the following items:	
Client for M	Aicrosoft Networks	
🗹 📙 Qo S Pack	et Scheduler	
🗹 📙 File and Pr	inter Sharing for Microso	oft Networks
🖌 🛶 Internet Pr	otocol Version 6 (TCP/I	Pv6)
🗹 🔺 Internet Pr	otocol Version 4 (TCP/II	Pv4)
🗹 🛶 Link-Layer	Topology Discovery Ma	apper I/O Driver
<ul> <li>Link-Layer</li> </ul>	Topology Discovery Re	sponder
Install	Uninstall	Properties
Description		
Description		
Transmission Con	ntrol Protocol/Internet Pr	
Transmission Cor wide area netwo	ntrol Protocol/Internet Pr rk protocol that provides terconnected networks.	communication



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

u can get IP settings assigned aut pports this capability. Otherwise, ministrator for the appropriate IP	you ne	ed to			ork
Obtain an IP address automati	cally	í.			
OUse the following IP address:					
IP address:					
S <u>u</u> bnet mask:					
Default gateway:					
Obtain DNS server address aut					
0 _	address	ses	140		
Preferred DNS server:					
<u>A</u> lternate DNS server :					
Validate settings upon exit				Adva	anced



# 3.3 Planet Smart Discovery Utility

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

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

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

PLANET Smart D File Option Help								-		×
File Option Help		<b>U</b> Refre:	sh	🖹 Exit			9	PL	AN ng & Commu	ET
MAC Address	Device Name	Version	DevicelP	NewPassword	IP Address	NetMask	Gateway	Descrip	tion	
Select Adapt	ter: 10.1.0.96	(F8:32:E4:CD:C5	:8A)		•	Control Pac	ket Force Broa	dcast		
	U	odate Device	Update Multi	Upda	te All	Connect to	Device			
Device		Mes	sage							

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:

	- 🗆 X
File Option Help	
C Refresh Exit	PLANET Networking & Communication
MAC Address Device Name Version DeviceIP NewPassword IP Address NetMask Gateway	Description
1 00-30-4F-11-22-00 VR-300P v1.1907b21011 192.168.1.1 192.168.1.1 192.168.1.1 255.255.255.0 0.0.0.0	PLANET VR-300P PoE
Select Adapter : 192.168.0.123 (00:03:6D:00:00)	dcast



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

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

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

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

Press the "Exit" button to shut down the Planet Smart Discovery Utility.



# Chapter 4. Web-based Management

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

### 4.1 Introduction

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

## 4.2 Logging in to the VPN Router

Refer to the steps below to configure the VPN router:

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



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

Step 2. The browser prompts you for the login credentials. (Both are "admin" by default.)

Default IP address: **192.168.1.1** Default user name: **admin** Default password: **admin** Default SSID (2.4G): **PLANET\_2.4G** Default SSID (5G): **PLANET\_5G** 



The SSIDs are designed for wireless models: VR-300W5, VR-300PW5, VR-300W6A, VR-300PW6A, VR-300W6, VR-300PW6



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



# 4.3 Main Web Page

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



Figure 4-: Main Web Page

#### Web Panel

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

	1	2	3	4	5	
0 W						
		LAN		LAN/WAN	WAN	

Figure 4-2: Web Panel

		5
Object	lcon	Function
PoE Cosumption	0 W	To indicate the PoE consumption.
		To indicate the LAN with the RJ45 plug-in.
LAN		To indicate the PoE is in use. (VR-300P only)
		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.

🔅 System 🕲 Network 🕞 Security 🎤 VPN 🚆 AP Control 🕫 PoE 🎅 Wireless 🌽 Maintenance

Figure 4-3: Function Menu

Object Description	
System	Provides System information of the router.
Network	Provides WAN, LAN and network configuration of the router.
Security	Provides Firewall and security configuration of the router.
VPN	Provides VPN configuration of the router.
AP Control	Provides AP Control configuration of the router.
ΡοΕ	Provides PoE Management configuration of industrial wall-mount Gigabit router.
Wireless	Provides wireless configuration of the router.
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the router.



#### Figure 4-4: Function Button

Object	Description
C	Click the " <b>Refresh button</b> " to refresh the current web page.
F	Click the "Logout button" to log out the web UI of the router.



# 4.4 System

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



Figure 4-5: System Menu

Object	Description
Wizard	The Wizard will guide the user to configuring the router easily
	and quickly.
Dashboard	The overview of system information includes connection, port,
	and system status.
System Status	Display the status of the system, device information, LAN and
	WAN.
System Service	Display the status of the system, secured service and server
	service
Statistics	Display statistics information of network traffic of LAN and WAN.



Connection Status	Display the DHCP client table and the ARP table
SFP Module Information	Display the physical or operational status of an SFP module via
	the SFP Module Information page (VR-300F and VR-300FP
	only)
High Availability	Enable/Disable High Availability on routers
RADIUS	Enable/Disable RADIUS on routers
Captive Portal	Enable/Disable Captive Portal on routers
SNMP	Display SNMP system information
NMS	Enable/Disable NMS on routers
Remote Syslog	Enable Captive Portal on routers
Event Log	Display Event Log information



### 4.4.1 Setup Wizard

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

TEP 1 - Account N	ouncation			
1	2			5
Account	LAN	WAN	Security Settings	Setup Completed

Figure 4-6: Setup Wizard

### **Step 1: Account Modification**

Set up the Username and Password for the Account Modification

1	2	3	4	5
Account	LAN	WAN	Security Settings	Setup Completed
Jsername	admi	nenm		
Password				
Confirm Password				
The personal must cont	ain 9-21 characters incl	uding upper case. Jowe	r case, numerals and other sy	mbole

### Step 2: LAN Interface

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

3 WAN	Security Settings	5 Setup Completed
	Security Settings	Setup Completed
192.168.1.1		
255.255.255.0		
192.168.1. 100		
101		
	✓ 192.168.1.100	✓ 192.168.1.100



Figure 4-7: Setup Wizard -	LAN Configuration
----------------------------	-------------------

Object	Description
IP Address	Enter the IP address of your router. The default is 192.168.1.1.
Subnet Mask	An address code that determines the size of the network. Normally
	use 255.255.255.0 as the subnet mask.
	By default, the DHCP Server is enabled.
DHCP Server	If user needs to disable the function, please uncheck the box.
Start IP Address	By default, the start IP address is 192.168.1.100.
	Please do not set it to the same IP address of the router.
	By default, the maximum DHCP users are 101, which means the router
Maximum DHCP Users	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
Gancer	previously saved values.

### Step 3: WAN Interface

The router supports two access modes on the WAN side shown in Figure 4-8

STEP 3 - Network Inte	erface WAN			
1	2	3		5
Account	LAN	WAN	Security Settings	Setup Completed
WAN1 WAN2				
Connection Type	DHO	CP 🖌		
IP Address				
Netmask				
Default Gateway				
DNS Server 1				

Figure 4-8: Setup Wizard – WAN 1 Configuration



WAN1 WAN2	
WAN	Enable     Isable
Connection Type	DHCP v
IP Address	
Netmask	
Default Gateway	
DNS Server 1	
DNS Server 2	

Figure 4-9: Setup Wizard – WAN 2 Configurations

#### Mode 1 -- Static IP

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

Connection Type         Static            IP Address         210.66.155.1            Netmask         255.255.255.0            Default Gateway         210.66.155.194	WAN1 WAN2	
Netmask         255.255.255.0           Default Gateway         210.66.155.194	Connection Type	Static •
Default Gateway 210.66.155.194	P Address	210.66.155.1
-	letmask	255.255.255.0
DNS Server 1 460.05.1.1	)efault Gateway	210.66.155.194
DNS Server 1 108.95.1.1	ONS Server 1	168.95.1.1
DNS Server 2 8.8.8.8	NS 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		
Cancer	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.

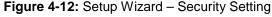
WAN1 WAN2	
Connection Type	DHCP V
IP Address	
Netmask	
Default Gateway	
DNS Server 1	
DNS Server 2	

Figure 4-11: WAN Interface Setup – DHCP Setup

### Step 4: Security Setting

Set up the Security Settings as shown in Figure 4-12.

LAN				
		WAN	Security Settings	Setup Completed
	Enable	○ Disable		
	Enable	O Disable		
	O Enable	Disable		
	O Enable	Disable		
	○ Enable	Disable		
			Cancel	Previous
		<ul> <li>Enable</li> <li>Enable</li> <li>Enable</li> <li>Enable</li> <li>Enable</li> </ul>	<ul> <li>Enable Oisable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> </ul>	<ul> <li>Enable O Disable</li> <li>Enable O Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> </ul>



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



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

### Step 5: Setup Completed

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



	2	3	4	- 5
Account	LAN	WAN	Security Settings	Setup Completed
LAN	Enable: Sta	tic IP: 192.168.1.1 /	255.255.255.0	
WAN1	Enable: DH	СР		
WAN2	Enable: OF	F		
Security Settings	SPI Firewall	ON		
	Block SYN F	lood: ON		
	Block ICMP	Flood: OFF		
	Block WAN	Ping: OFF		
	Remote Mar	nagement: OFF		

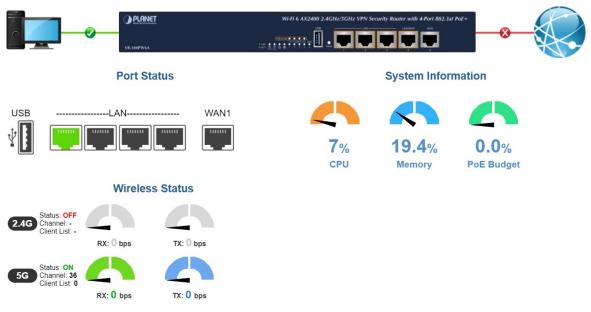
Figure 4-13: Setup Wizard – Setup Completed

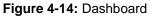
Object	Description
Finish	Press this button to save and apply changes.
Previous	Press this button for the previous step.



### 4.4.2 Dashboard

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





### **WAN/LAN Connection Status**

Object	Description
Also to have been a	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.

### Wireless Status

Obj	ect	Description
RX: 0 bps	TX: 0 bps	Wireless is in use.
RX: 0 bps	TX: 0 bps	Wireless is not in use.

### **System Information**

Object	Description
CPU	Display the CPU loading
Memory	Display the memory usage
PoE Budget	Display the PoE Budget usage (PoE model only)

### 4.4.3 Status

This page displays system information as shown in Figure 4-15.



Router Information	
Model Name	VR-100
Firmware Version	v1.1806b190904
Current Time	2019-01-30 Wed 20:21:45
Running Time	0d 00:00:57
WAN1	
MAC Address	A8:F7:E0:00:06:62
Connection Type	DHCP
IP Address	192.168.1.189
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
LAN	
MAC Address	A8:F7:E0:00:06:61
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Service	Enable
DHCP Start IP Address	192.168.1.100
DHCP End IP Address	192.168.1.200
Max DHCP Clients	101

Figure 4-15: Status

### 4.4.4 Statistics

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

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

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

Figure 4-16: Statistics



### 4.4.5 Connection Status

The page will show the DHCP Table and ARP Table. The status is shown in Figure 4-17.

DHCP Table				
Name IP Address	MAC Address	Expiration Time		
ARP Table				
	MAC Address			
IP Address 8.8.8.8	MAC Address 00:00:00:00:00:00	ARP Type 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		
	00:30:11:11:11:12	dynamic		

Figure 4-17: Connection Status

### 4.4.6 SFP Module Information

This page shows the operational status, such as the transceiver type, speed, wavelength, optical output power, optical input power, temperature, laser bias current and transceiver supply voltage in real time. The SFP Module Information page is shown in Figure 4-18.

SFP Module	e Informatio	on						
Туре	Speed	Wave Length(nm)	Distance(m)	Temperature(C)	Voltage(V)	Current(mA)	Tx power(dBm)	Rx power(dBm)
1000Base-LX	1000-Base	1310	10000	39.0588	3.3112	18.9760	-6.3451	-36.9897

Figure 4-18: SFP Module Information

Object	Description
• Туре	Display the type of current SFP module; the possible types are:
	■ 1000BASE-SX
	1000BASE-LX
Speed	Display the speed of current SFP module; the speed value or
	description is obtained from the SFP module. Different vendors SFP
	modules might show different speed information.
Wave Length(nm)	Display the wavelength of current SFP module; the wavelength
	value is obtained from the SFP module. Use this column to check if
	the wavelength values of two nodes match while the fiber connection



	fails.
Distance (m)	Display the support distance of current SFP module; the distance
	value is obtained from the SFP module.
• Temperature (C)	Display the temperature of current SFP DDM module; the
- SFP DDM Module	temperature value is gotten from the SFP DDM module.
Only	
Voltage (V)	Display the voltage of current SFP DDM module; the voltage value is
- SFP DDM Module	gotten from the SFP DDM module.
Only	
Current (mA)	Display the ampere of current SFP DDM module; the ampere value
– SFP DDM Module	is gotten from the SFP DDM module.
Only	
• TX power (dBm)	Display the TX power of current SFP DDM module; the TX power
- SFP DDM Module	value is gotten from the SFP DDM module.
Only	
RX power (dBm)	Display the RX power of current SFP DDM module; the RX power
- SFP DDM Module	value is gotten from the SFP DDM module.
Only	



### 4.4.7 High Availability

High Availability (HA) is a system redundancy where two routers of VR-300 series can be set up in a master/slave configuration. The master router provides the Internet connection but, in case hardware or WAN connectivity fails, the slave (backup) router automatically will take over Internet connection. It provides redundant hardware and software that make the system available despite failures. The page will show the High Availability configuration. The High Availability page is shown in Figure 4-19.

High Availability Configuration	
High Availability	Enable O Disable
Username	
Password	
Mode	Master 🗸
Virtual IP address	
Virtual IP Mask	
Interface	LAN V
Connected Status	<b>≞,</b> .

Figure 4-19: High Availability

Object	Description
High Availability	Disable or enable the High Availability function.
	The default configuration is disabled.
Username	Create the username for the HA.
Password	Create the password for the HA.
Mode	Choose Master or Slave role
Virtual IP address	Assign an IP address as a virtual IP.
Virtual mask	Assign a mask address as a virtual mask.
Interface	Use interface
Connection Status	Display the HA status



### **4.4.8 RADIUS**

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting. The RADIUS Server page is shown in Figure 4-20.

RADIUS		
Server	Client	User Account
RADIUS	Server Mod	de O Enable I Disable
Server Port		1812

Figure 4-20: RADIUS Server

Object	Description
RADIUS	Disable or enable the RADIUS function.
	The default configuration is disabled.
Server Port	UDP port number for authentication

The RADIUS client page is shown in Figure 4-21.

RADIUS							
Server	Client	User Account					
Index	Name		Client IP Address	/ 32 ~	Secret Key	Description	Delete Add
(up to 16 clients)							

### Figure 4-21: RADIUS Client

Object	Description		
Name	Describe client's name		
Client IP address	Describe client's IP address		
Secret Key	The RADIUS server and client share a secret key that is used to authenticate the messages sent between server and client.		
Description	Describe client's information		



# 4.4.9 Captive Portal

Captive portal service gives the ability to organize a public (or guest) Wi-Fi zone with user authorization. A captive portal is the authorization page that forcibly redirects users who connect to the public network before accessing the Internet. The Captive portal page is shown in Figure 4-22.

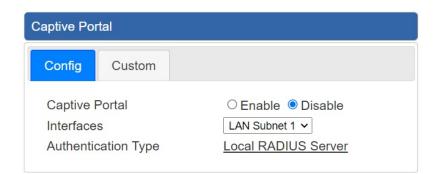


Figure 4-22: Captive portal

Object	Description
Captive portal	Disable or enable the Captive portal function.
	The default configuration is disabled.
Interface	Choose subnet interface
	LAN Subnet 1
	LAN Subnet 2
	LAN Subnet 3
	LAN Subnet 4
Authentication Type	Support local RADIUS server



### 4.4.10 SNMP

This page provides SNMP setting of the router as shown in Figure 4-23.

SNMP	
SNMP	● Enable ○ Disable
SNMP Versions	SNMP v1,v2c 🗸
Read Community	public
Write Community	private
Engine ID	
SNMP v3 Security Level	AuthPRiv 🗸
SNMP v3 User Name	
SNMP v3 Auth Protocol	MD5 🗸
SNMP v3 Auth Password	
SNMP v3 Privacy Protocol	DES ¥
SNMP v3 Privacy Password	
System Identification	
System Name	VR-300P
System Location	
System Contact	sales@planet.com.tw
	Apply Settings Cancel Changes

Figure 4-23: SNMP

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



### 4.4.11 NMS

The VR-300 series can support both NMS controller and CloudViewer Server for remote management. PLANET's NMS Controller is a Network Management System that can monitor all kinds of deployed network devices, such as managed switches, media converters, routers, smart APs, VoIP phones, IP cameras, etc., compliant with the SNMP Protocol, ONVIF Protocol and PLANET Smart Discovery utility. The CloudViewer is a free networking service just for PLANET products. This service provides simplified network monitoring and real-time network status. Working with PLANET CloudViewer app, user can easily check network status, device information, port and PoE status from Internet. Any other services are not included.

NMS Configuration screens in Figure 4-24 appear.

NMS Configuration		
NMS NMS Controller IP address Authorization Status	PLANET NMS Controller - LAN	

Figure 4-24 NMS Configuration Page

The NMS Controller – LAN Configuration screens in Figure 4-25 appear.

NMS Configuration	
NMS NMS Controller IP address Authorization Status	PLANET NMS Controller - LAN <ul> <li>Unauthorized</li> </ul>
	Apply Settings Cancel Changes Unbind

Figure 4-25 NMS Controller – LAN	Configuration Page
----------------------------------	--------------------

Object	Description
NMS Controller IP	The IP address of NMS Controller
address	
Authorization	Indicates the authorization status of the switch to NMS Controller
Status	



The CloudViewer Server – Internet screens in Figure 4-26 appear.

NMS Configuration	
NMS	PLANET CloudViewer Server - Internet V
Email	
Password	
Connection Status	Not enabled

#### Figure 4-26 CloudViewer Server – Internet Configuration Page

Object	Description
• Email	The email registered on CloudViewer Server
Password	The password of your CloudViewer account
Connection Status	Indicates the status of connecting CloudViewer Server



# 4.5 Network

The Network function provides WAN, LAN and network configuration of the router as shown in Figure 4-27.

WAN
WAN Advanced
LAN
Multi-Subnet
VLAN
UPnP
Routing
RIP
OSPF
IGMP
IPv6
DHCP
DDNS
MAC Address Clone

Figure 4-27: Network Menu

Object	Description
WAN	Allows setting WAN interface.
WAN Advanced	Allows setting WAN Advanced settings.
LAN	Allows setting LAN interface.
Multi-Subnet	Allows setting Multi-Subnet1 ~ Subnet4 interface.
VLAN	Disable or enable the VLAN function.
	The default configuration is disabled.
UPnP	Disable or enable the UPnP function.
	The default configuration is disabled.
Routing	Allows setting Route.
RIP	Disable or enable the RIP function.



	The default configuration is disabled.
OSPF	Disable or enable the OSPF function.
	The default configuration is disabled.
IGMP	Disable or enable the IGMP function.
IGMP	The default configuration is disabled.
IPv6	Allows setting IPv6 WAN interface.
DHCP	Allows setting DHCP Server.
DDNS	Allows setting DDNS and PLANET DDNS.
MAC Address	Allows setting WAN MAC Address Clone
Clone	Allows setting WAN MAC Address Clone.



### 4.5.1 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the router as shown in Figure 4-28. Here you may select the access method by clicking the item value of WAN access type.

WAN1	
Connection Type	DHCP V
IP Address	
Netmask	
Gateway	
DNS Server 1	
DNS Server 2	
WAN2	
WAN	Enable      Disable
Connection Type	DHCP V
IP Address	
Netmask	
Gateway	
DNS Server 1	
DNS Server 2	
	Apply Settings Cancel Changes

#### Figure 4-28: WAN

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



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

### 4.5.2 WAN Advanced

This page is used to configure the advanced parameters for Internet area network which connects to the WAN port of your router as shown in Figure 4-29. Here you may change the setting for Load Balance Weight, Detect Interval, Detect Link Up Threshold, etc...

WAN1	
Load Balance Weight External Connection Detection	3 ▼ ● Enable ○ Disable
Detect Interval Detect Link Up Threshold	5 Seconds 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 Oisable
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
	Apply Settings Cancel Changes

Figure 4-29: LAN Setup



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

#### 4.5.3 LAN Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your router as shown in Figure 4-30. Here you may change the settings for IP address, subnet mask, DHCP, etc.

IP Address	192.168.1.1	
Netmask	255.255.255.0	

Apply Settings	Cancel Changes

#### Figure 4-30: LAN Setup

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



# 4.5.4 Multi-Subnet

Multi-Subnet Configuration				
Name	Network	DHCP Server		
LAN Subnet 1	IP Address Netmask	192.168.1.1 V 255.255.255.0		
LAN Subnet 2	IP Address Netmask	192.168.3.1       255.255.255.0		
LAN Subnet 3	IP Address Netmask	192.168.5.1       255.255.255.0		
LAN Subnet 4	IP Address Netmask	192.168.7.1       255.255.255.0		
1		Apply Settings Cancel Changes		

# 4.5.5 Routing

Please refer to the following sections for the details as shown in Figures 4-31 and 32.

Number	Туре	Destination	Netmask	Gateway	Interface	Comment	Action
Current Routi	ing table in t	he system					
Number	Dest	ination	Netmask		Gateway	In	iterface
1	0.0.0	.0	0.0.0		192.168.0.180	L	OCAL
2	0.0.0	.0	0.0.0		192.168.1.18	W	/AN1
3	0.0.0	.0	0.0.0		192.168.1.19	W	/AN2
4	192.1	168.0.0	255.255.255.0		0.0.0.0	L	AN
5	192.1	168.1.0	255.255.255.0		0.0.0.0	V	/AN1
6	192.1	168.1.0	255.255.255.0		0.0.0.0	V	/AN2

Figure 4-31: Routing table



Add a routing rule	
Туре	Host 🔻
Destination	
Netmask	255.255.255.255 /32 🔻
Gateway	
Interface	LAN V
Comment	
	Apply Settings Cancel Changes

Figure 4-32: 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
	There are two types: Host and Net.
Туре	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.
	The gateway is the router or host's IP address to which packet was
Gateway	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
Interface	router when this route is used.
Comment	Enter any words for recognition.



### 4.5.6 WAN IPv6 Setting

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the router as shown in Figure 4-33. It allows you to enable IPv6 function and set up the parameters of the router's WAN. In this setting you may change WAN connection type and other settings.

WAN1 IPv6 Setting	
Connection Type IPv6 Address Subnet Prefix Length	DHCP • 64
Default Gateway WAN2 IPv6 Setting	
Connection Type	DHCP V
IPv6 Address	
Subnet Prefix Length	64
Default Gateway	

Apply Settings Cancel Changes



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.

### 4.5.7 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 4-34.



#### DHCP Server

DHCP Service	Enable Disable	
Start IP Address	192.168.1. 100	
Maximum DHCP Users	101	
Set DNS	Automatically O Ma	nually
Primary DNS Server		
Secondary DNS Server		
WINS		
Lease Time	1440	minutes
Domain Name	PLANET	
	-	

Apply Settings C

Cancel Changes

#### Figure 4-34: DHCP

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



### 4.5.8 DDNS

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as **PLANET DDNS (**<u>http://www.planetddns.com</u>) 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 4-35.

#### 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 (<u>http://www.planetddns.com</u>). Thus, you don't need to memorize the exact IP address but just the URL link: Mycam1.planetddns.com.

#### PLANET Easy DDNS

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

Dynamic Domain Name Service	
DDNS Servcie	Enable      Disable
Interface	WAN1 🔻
DDNS Type	PLANET DDNS V
Easy DDNS	Disable •
User Name	
Password	
Host Name	
Interval	120
Update Status	unknow status
	Apply Settings Cancel Changes



#### Figure 4-35: 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.	
Interface	By default, the interface is WAN 1.	
	There are three options:	
	1. PLANET DDNS: Activate PLANET DDNS service.	
	2. DynDNS: Activate DynDNS service.	
DDNS Type	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.	
	When the PLANET DDNS service is activated, user is able to select	
	to enable or disable Easy DDNS.	
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.	



# 4.5.9 MAC Address Clone

Clone or change the MAC address of the WAN interface. The setup is shown in Figure 4-36.

MAC Address Clone - WAN1	
Clone WAN MAC MAC Address	<ul> <li>Enable</li> <li>Disable</li> </ul>
MAC Address Clone - WAN2	2
Clone WAN MAC MAC Address	<ul> <li>Enable</li> <li>Disable</li> </ul>
	Apply Settings Cancel Changes

#### Figure 4-36: 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 4-37. Please refer to the following sections for the details.

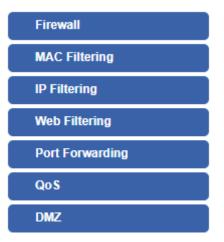


Figure 4-37: Security menu

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.
QoS	Allows setting Qos.
DMZ	Allows setting DMZ.



### 4.6.1 Firewall

A "Denial-of-Service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service. The router can prevent specific DoS attacks as shown in Figure 4-38.

irewall Protection		
SPI Firewall	Enable O Disable	
-DDos		
Block SYN Flood	Enable Oisable	30 Packets/Second
Block FIN Flood	Enable      Disable	30 Packets/Second
Block UDP Flood	Enable I Disable	30 Packets/Second
Block ICMP Flood	Enable I Disable	5 Packets/Second
IP TearDrop	Enable I Disable	
PingOfDeath	Enable      Disable	
- System Security		
Block WAN Ping	Enable Isable	
Remote Management	Enable      Disable	

Apply Settings Cancel Changes

#### Figure 4-38: Firewall

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



Block UDP Flood	If the function is enabled, when the number of the current
	UPD-FLOOD packets is beyond the set value, the router will start
	the blocking function immediately.
	The default configuration is disabled.
	ICMP is kind of a pack of TCP/IP; its important function is to transfer
Block ICMP Flood	simple signal on the Internet. There are two normal attack ways
BIOCK ICMIP FIOOD	which hackers like to use, Ping of Death and Smurf attack.
	The default configuration is disabled.
IP TearDrop	If the function is enabled, the router will block Teardrop attack that is
	targeting on TCP/IP fragmentation reassembly codes.
	If the function is enabled, the router will block Ping of Death attack
Ding Of Death	that aims to disrupt a targeted machine by sending a packet larger
Ping Of Death	than the maximum allowable size causing the target machine to
	freeze or crash.
	Enable the function to allow the Ping access from the Internet
Block WAN Ping	network.
	The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the router 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 router. Use of such filters can be helpful in securing or restricting your local network as shown in Figure 4-39.

Enable MAC Filtering nterface	<ul> <li>Enable</li> <li>LAN</li> <li>WAN</li> </ul>
	Index MAC Address
	MAC Address :
	Add Remove Remove All

Figure 4-39: MAC Filtering

Object	Description
	Set the function as enable or disable.
Enable MAC Filtering	When the function is enabled, the router will block traffic of the MAC
	address on the list.
Interface	Select the function works on LAN, WAN or both. If you want to block
Interface	a LAN device's MAC address, please select LAN, vice versa.
MAC Address	Input a MAC address you want to control, such as
MAC Address	A8:F7:E0:00:06:62.
٨٩٩	When you input a MAC address, please click the "Add" button to add
Add	it into the list.
Demove	If you want to remove a MAC address from the list, please click on
Remove	the MAC address, and then click the "Remove" button to remove it.
Demove All	If you want to remove all MAC addresses from the list, please click
Remove All	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 4-40. 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      Isable			
IP Filtering Rule	es				
No. Active	Source IP	Destination IP	Port Range	Protocol	Action
		Add IP Filtering Rule			

Figure 4-40: 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 4-41: IP Filter Rule Setting

Apply Settings Cancel Changes

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



Object	Description
Destination IP Address	Input the IP address of web site which you want to block.
Anywhere (of destination	Check the box if you want to control all web sites, meaning the LAN
IP Address)	user can't visit any web site.
Destination Bart	Input the port of destination IP Address which you want to block.
Destination Port	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 4-42. Block those URLs which contain keywords listed below.

Web Fil	tering			
Web F	iltering	Enable Isable		
Web Fil	tering Rules			
No.	Rule Enable	Filter Keyword	Filter Type	Action
		Add Web Filtering	Rule	

#### Figure 4-42: Web Filtering

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

Web Filter Settings	
Status Filter Keyword	Enable T ex. www.yahoo.com
	Apply Settings Cancel Changes



Object	Description
	Description



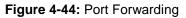
#### Enterprise 5-Port 10/100/1000T VPN Security Router VR-300 series

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 4-44. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Router's NAT firewall.

Port Forwarding						
Port Forwarding	⊖ Ena	ble 🖲 Disa	ble			
Port Forwarding Rules						
No. Rule Name	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range	Delete
		Ad	ld Port Forwarding Rule			



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 External Service Port Virtual Server IP Address	Both ▼
Internal Service Port	
	Apply Settings Cancel Changes

Figure 4-45: Port Forwarding Rule Setting

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



#### Enterprise 5-Port 10/100/1000T VPN Security Router VR-300 series

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

### 4.6.6 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in Figure 4-46.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 DMZ IP Address	Enable     Disable
DMZ - WAN2	
DMZ DMZ IP Address	Enable  Disable
	Apply Settings Cancel Changes



Object	Description
	Set the function as enable or disable. If the DMZ function is enabled,
DM7	it means that you set up DMZ at a particular computer to be exposed
DMZ	to the Internet so that some applications/software, especially
	Internet/online game can have two way connections.



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

# 4.7 Virtual Private Network

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

The Maintenance menu provides the following features for managing the system as Figure 4-47 is shown below:



Figure 4-47: VPN Menu

Object	Description
IPsec	Allows setting IPsec function.
IPsec Remote Server	Disable or enable the IPsec Remote Server function. The default configuration is disabled.
GRE	Allows setting GRE function.
РРТР	Allows setting PPTP function.



L2TP	Allows setting L2TP function.	
SSL VPN	Allows setting SSL VPN function.	
Certificates Download System CA Certificate		
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 4-48.

IPSec Tunnel Lists					
No.	Name	Interface	Status	Action	
Add IPSec Tunnel					
Figure 4-48: 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	
Detection	
Dead Peer Detection 🗹	
Time Interval 30 Seconds	Timeout 150 Seconds Action Restart •
A	
-Authentication	
Preshare Key	
- IKE Setting	
Phase 1	
IKE	● v1
Connection Type	Main      Aggressive
ISAKMP	AES (128 bit) ▼ SHA1 ▼ DH Group 2 (1024) ▼
IKE SA Lifetime	3 hours
Phase 2	
ESP FOR Koulife	AES (128 bit) V SHA1 V
ESP Keylife	1 hours
Perfect Forward Secrecy (PFS)	○ Yes ● No
I	L

Apply Settings Cancel Changes

Figure 4-49: IPSec Tunnel

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



	VIC OUD SETUS		
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.		
	Set up the detection time of <b>DPD</b> (Dead Peer Detection).		
	By default, the DPD detection's gap is 30 seconds, over 150 seconds		
	to think that is the broken line.		
Dead Peer Detection	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.		
	Enter a pass phrase to be used to authenticate the other side of the		
Preshare Key	tunnel. Should be the same as the remote host.		
IKE	Select the IKE (Internet Key Exchange) version.		
Connection Type	1. Main.		
	2. Aggressive.		
	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. <b>3DES</b> : Triple DES is a block cipher formed from the DES cipher		
ISAKMP	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. <b>SHA2</b> : Either 256, 384 or 512 can be chosen		
	5. <b>MD5 Algorithm</b> : MD5 processes a variably long message into a		
	fixed-length output of 128 bits.		
	6. <b>DH Group</b> : 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.		
	It offers AES, 3 DES, SHA 1, SHA2, and MD5.		
ESP	1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a		
_0.	commonly seen and adopted nowadays.		
	2. <b>3DES</b> : 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. <b>SHA2</b> : 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	Cat the function of each la or disable	
Secrecy (PFS)	Set the function as enable or disable.	

### 4.7.2 GRE

This section assists you in setting the GRE Tunnel as shown in Figure 4-50.

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
			Add GR	E Tunnel			

#### Figure 4-50: 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 🔻
Peer Wan IP Address Peer Subnet Mask Peer Tunnel IP Address Local Tunnel IP Address	Remote IP Address       10.10.10.0/24       10.10.10.2       10.10.10.1

Apply Settings

Cancel Changes

#### Figure 4-51: GRE Tunnel

Object	Description		
Active	Check the box to enable the function.		
Tunnel Name	Enter any words for recognition.		
Through	<ul><li>This is only available for host-to-host connections and specifies to which interface the host is connecting.</li><li>1. LAN.</li><li>2. WAN 1.</li><li>3. WAN 2.</li></ul>		
Peer WAN IP Address	Input the IP address of the remote host. For instance, "210.66.1.10".		
Peer Netmask	The remote subnet in CIDR notation. For instance, "210.66.1.0/24".		
Peer Tunnel IP Address	Input the Tunnel IP address of remote host.		
Local Tunnel IP Address	Input the Tunnel IP address of remote host.		
Local Netmask	Input the Tunnel IP address of the router.		



### 4.7.3 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 4-52.

PPTP Server			
PPTP Server	Enable      Disable		
Broadcast	Enable     Disable		
Force MPPE Encryption	Enable      Disable		
СНАР	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 4-52: PPTP server

Cancel Changes

Apply Settings

Object	Description	
PPTP Server	Set the function as enable or disable.	
Broadcast	Enter any words for recognition.	
Force MPPE	Set the encryption as enable or disable.	
Encryption		
СНАР	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	DNS server IP address to client.	
WINC	When the PPTP client connects to the PPTP server, it will assign the	
WINS WINS server IP address to client.		
Server IP Address	Input the IP address of the PPTP Server. For instance, "192.168.10.1".	
	When the VPN connection is established, the VPN client will get IP	
Clients IP Address	address from the VPN Server. Please set the range of IP Address. For	
(Start/End)	instance, the start IP address is "192.168.10.10", the end IP address is	
	"192.168.10.100".	
User and Password	Create the username and password for the VPN client.	



### 4.7.4 L2TP Server

This section assists you in setting the L2TP Server as shown in Figure 4-53.

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	
-	
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) V SHA1 V
ESP Keylife	1 hours
,	
	Apply Settings Cancel Changes

Figure 4-53: 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".			
	When the VPN connection is established, the VPN client will get IP			
<b>Clients IP Address</b>	address from the VPN Server. Please set the range of IP Address. For			
(Start/End)	instance, the start IP address is "192.168.50.100", the end IP address is			
	"192.168.50.200".			



Object	Description				
With IPsec	Set the function as enable to make the L2TP work with IPsec encryption.				
Preshare Key	Enter a pass phrase.				
User and Password	Create the username and password for the VPN client.				
Connection Type	1. Main.				
ISAKMP	<ol> <li>Aggressive.</li> <li>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.</li> <li>AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.</li> <li>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.</li> <li>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.</li> <li>SHA2: Either 256, 384 or 512 can be chosen.</li> <li>MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits.</li> <li>DH Group: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen.</li> </ol>				
IKE SA Lifetime	You can specify how long IKE packets are valid.				
ESP	<ul> <li>It offers AES, 3 DES, SHA 1, SHA2, and MD5.</li> <li>1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.</li> <li>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.</li> <li>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.</li> <li>4. SHA2: Either 256, 384 or 512 can be chosen.</li> <li>5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits.</li> </ul>				
ESP Keylife	You can specify how long ESP packets are valid.				



## 4.7.5 SSL VPN

This section assists you in setting the SSL Server as shown in Figure 4-54.

SSL Server	
SSL VPN Server	Enable      Disable
Port	1194
Tunnel Protocol	UDP T
Virtual Network Device	TUN 🔻
Interface	LAN <b>•</b> 192.168.1.1
VPN Network	192.168.20.0
Network Mask	255.255.255.0
Encryption Cipher	AES-128 CBC V
Hash Algorithm	SHA1 v
Export client.ovpn	Export

Apply Settings Cancel Changes

Figure 4-54: 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 4-55.

VPN Connection Status							
IPsec	GRE	PPTP	L2TP	SSL VPN			
Туре	Conne	cted Time		Local IP	Remote IP	Local Subnet	Remote Subnet

Figure 4-55:	VPN Connection Status
--------------	-----------------------

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



# 4.8 AP Control

The AP Control menu provides the following features for managing the system as Figure 4-56 is shown below:

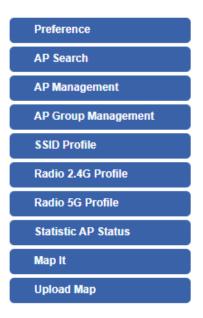


Figure 4-56: AP Control Menu

Object	Description
Preference	Edit region, RO community, RW community
AP Search	Search APs in the same domain
AP Management	Config APs IP Address, Subnet Mask, SSID and Radio Profiles
AP Group Management	Grouping same model AP
SSID Profile	Setup SSID Profile
Radio 2.4G Profile	Setup Radio 2.4G Profiles
Radio 5G Profile	Setup Radio 5G Profiles
Statistics AP Status	Show the status of managed APs
Statistics Active Clients	Show the status of active clients
Map It	Edit the map of AP location and coverage
Upload Map	Search APs in the same domain



### 4.8.1 Preference

On this page, you can choose the device region of FCC or ETSI. Then edit RO community and RW community for public or private use. Select Apply or Reset.

#### **AP Preference**

Region	FCC V
RO Community	public
RW Community	private

Noted: Device of FCC and device of ETIS cannot be shown at the same time.

#### 4.8.2 AP Search

On this page, you can add new APs in your AP Control System.

Step as follows :

Step 1. Press the Search button to discover PLANET devices.

Step 2. Waiting for few time, Choose which AP you want to add.

Step 3. Press the Apply button to finish addition.

P Search				Step1. Search	Apply Step3	P <b>Q</b> 10 (101024)	۲
Num.	MAC Address	Device Type	Model No.	Version	Devic	Device Description	-
1	a8:f7:e0:46:2e:38	Wireless	WDAP-C7200E	WDAP-C7200E-AP-FCC-V3.0-Build20200321122005	192.168.0.101	<b>O</b> ( <b>O</b> )	
2	a8:f7:e0:3c:5f:ab	Wireless	WNAP-C3220E	WNAP-C3220E-AP-FCC-V3.0-Build20200422115453	192.168.0.102		0

Note: When use AP Search, The APs IP Address must be same as WS-Series Switch IP domain



#### 4.8.3 AP Management

On this page, you can management your APs, Including check AP online status, config AP (IP address, Mask, SSID and Radio profile), reboot AP, firmware update, delete AP in the AP Control system.

#### Status

	inagemen	it Offline 🔘 Disa	ble				¢ 💼	Apply Filter by Co	ntext		Q	10 (10.	.64)	٢
	Status	AP Group	MAC Address	Device Type	Model No.	Version	IP Address	Device Description			Ac	tion		
0	•		a8:f7:e0:46:2e:38	Wireless	WDAP-C7200E	WDAP-C7200E-AP-FCC-V3.0- Build20200321122005	192.168.0.101		489	д		6	0	龠
0	•		a8:f7:e0:3c:5f.ab	Wireless	WNAP-C3220E	WNAP-C3220E-AP-FCC-V3.0- Build20200422115453	192.168.0.102		100	0		÷.	$\bigcirc$	龠

Object	Description
	Connection status: online, offline, Wi-Fi disabled
	In progress: action in progress
<b>v</b>	Finished/Successful: action finished and successful.
×	Failed: action failed.

#### Action

Object	Description
66	Setting: edit setting and allocate profile to AP
C	Link: link to the AP's web page
ĺ <b>↑</b> )	Firmware Update: Upgrade AP's firmware
Ċ,	Reboot: Reboot the AP
俞	Delete: Delete the AP from the control list LED Control: Control the
	AP's LED.
:ଡି: ଠିଡି	Mouse-click in a sequential order: LED blink-> LED off-> LED on



#### Notes:

- 1. To configure multiple APs at one time, select multiple APs and then choose one of the action icons on the top of the page. The "Link" action is not allowed for multiple APs.
- 2. When finish setup AP, you need to press Apply button to complete setup.

#### 4.8.4 AP Group Management

On the AP Group Management page, you can create AP group and control one or more AP groups.

Froup Mana	igement			14	i k	Apply	Filter by Context	Q	10 (1010)	0
	Num.	Group Name	Group Description				Action			
	1	GroupTest1	test	191	AID		6	Q	會	
0	2	GroupTest2	test	TOT	10		6	Q	畲	

#### Action:

Object	Description
4	Add new group: Click it to add an AP group
£:	Delete selected item: Click it to delete the selected AP group

A	P Group Configured	Group Member Setting						
Model No.	NAP-200N 🗸	Current AP Group Members		Available Managed APs				
AP Group Name		-						
AP Group Description			<< Add Remove >>					
	2.4G Pro	ofile		5G Profile				
	SSID 1 Disable 🗸	Disable 🛩						
	SSID 2 Disable V	Disable 🗸						
	SSID 3 Disable V	Disable 🗸						
	SSID 4 Disable V	Disable 🗸						
	Profile Disable V	Disable 🗸						

#### Create Group:

- 1. Select AP Model No. you want to Add
- 2. Type AP Group Name and AP Group Description.
- 3. Select AP you want to add in group member setting area and press Add button.
- 4. Select AP Group SSID profile and Radio Profile.
- 5. Press Apply button to finish create ap group.



Note:

To do profile provisioning to multiple AP groups at one time, select multiple AP groups, and then click the "Apply" button.

The "Link" action is not allowed for multiple APs or AP group.

### 4.8.5 SSID Profile

On the SSID profile configuration page, enter the value that you preferred and then click "Apply" to save the profile

Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Act	ion
1	WDAP-C7200E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	102	Ê
2	WNAP-C3220E	test 2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	1010	Ê

Radio Profile 2.4GHz Configuratio	n	Apply	Back	Reset
	Radio Profile Configuration			
Model No.	WAP-200N V			
	Basic Setting			
Radio Profile Description				
Wireless Mode	11b/g/n mixed mode 🗸			
Channel Bandwidth	20MHz 💙			
Channel	Auto 🗸			
MCS	Auto			
Tx Power	Auto 🗸			
Client Limit	✓ 64 (1 to 64)			

Action:

Object	Description
4	Add new profile: Click it to add a new profile.
<b>1</b> 5:	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
Ê	Delete: Click it to delete the single profile.



### 4.8.6 Radio 2.4G Profile

On the Radio profile configuration page, enter the value that you preferred and then click "Apply" to save the profile.

adio Profile	2.4GHz						Filter by Profile Nar	ne Q	10 (108)	٢
	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Activ	on
	1	WDAP-C7200E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	66	畲
	2	WNAP-C3220E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	1010	曲

Action:

Object	Description
4	Add new profile: Click it to add a new profile.
<b>1</b> 5:	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
â	Delete: Click it to delete the single profile.

Radio Profile 2.4GHz Configuration	Apply Back Reset
	Radio Profile Configuration
Model No.	WAP-200N V
	Basic Setting
Radio Profile Description	
Wreless Mode	11b/g/n mbxed mode 🗸
Channel Bandwidth	20MHz V
Channel	Auto V
MCS	Auto V
Tx Power	Auto V
Client Limit	84 (1 to 64)

Notes:

- Strongly suggest you to keep the values as default except the fields like Channel, Network Mode, Channel Bandwidth, Tx Power, IAPP, and Tx/Rx to prevent any unexpected error or impact on the performance.
- 2. WMM Capable is not allowed to be disabled.



### 4.8.7 Radio 5G Profile

On the Radio profile configuration page, enter the value that you preferred and then click "Apply" to save the profile.

o Profile	5GHz					ilts- ilts	Filter by Profile Na	me Q	10 (108)	0
	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Acti	on
	1	WDAP-C7200E	test_5G	11n/ac mixed mode	Auto	40MHz	100%	N/A	669	會

Action:

Object	Description
4	Add new profile: Click it to add a new profile.
<b>E</b> :	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
â	Delete: Click it to delete the single profile.

Radio Profile 5GHz Configuration		Apply	Back	Reset
	Radio Profile Configuration			
Model No.	WAP-500N V			
	Basic Setting			
Radio Profile Description				
Wireless Mode	11a/n mixed mode 🗸			
Channel Bandwidth	40MHz 💙			
Channel	Auto V			
Client Limit	2 64 (1 to 64)			

#### Notes:

- Strongly suggest you to keep the values as default except the fields like Channel, Network Mode, Channel Bandwidth, Tx Power, IAPP, and Tx/Rx to prevent any unexpected error or impact on the performance.
- 2. WMM Capable is not allowed to be disabled.



### 4.8.8 Statistics AP Status

On this page, you can observe the current configuration of all managed APs.

		aged APs Offline 🌑 Disable							Filter by Co	ntext Q	10 (1064)
Num.	Status	MAC Address	IP Address	Model No.	Name	firmware	AP Group	2.4GHz SSID Profile	5GHz SSID Profile	2.4GHz Radio Profile	5GHz Radio Prol
1	•	a8:f7:e0:46:2e:38	192.168.0.102	WDAP-C7200E		WDAP-C7200E-AP-FCC-V3.0- Build20200321122005					
2	•	a8:17:e0:3c:5f ab	192.168.0.101	WNAP-C3220E		WNAP-C3220E-AP-FCC-V3.0- Build20200422115453			N/A		N/A

Filter: You can filter the AP list by entering the keyword in the field next to the magnifier icon. The keyword should be in any context that belongs to the fields of this page.

#### **4.8.9 Statistics Active Clients**

On this page, you can observe the statuses of all associated clients including traffic statistics, transmission speed and RSSI signal strength.

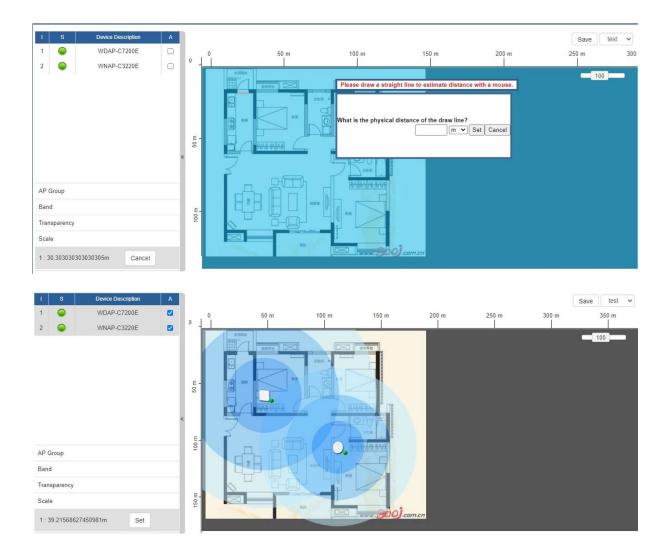
Statistic > A	Active Clients					Filter by N	IAC, IP, SSID, Band Q	10 (10256)	٢
Num.	Client MAC Address	AP MAC Address	AP SSID	Band	Tx (KB)	Rx (KB)	Speed (Mbps)	RSSI (dBm)	
1	00:00:00:00:00:00	a8:f7:e0:46:2e:38	SSIDtest_2.4G	2.4GHz	0	0	0	0	

Filter: You can filter the search result by entering the keywords in the field next to the magnifier icon. The keywords include MAC Address, IP Address, SSID and Band.



#### 4.8.10 Map It

On this page you can add managed APs to the actual position against the floor map. This is convenient to user to view and adjust the actual deployment by reference to its real transmission power and channel allocation.



- 1. Click "Scale" to start to reset the map scale.
- 2. Press the set button to draw a line on the map. Fill its physical distance in the blank and press Set or Cancel. For example, in the graph below, set the door width to 0.8 m

Note: You need to upload map image first before managed APs to the actual position.



# 4.8.11 Upload Map

On this page, the system allows you to upload your floor map to the system.

Upload Map	III Apply
Мар	New Map 💙
Upload File	> 編壇僅重,未編壇任何編興
New Description	
File Size	Bytes

Note: The system allows user to upload up to 10 floor maps.



# 4.9 **Power over Ethernet**

The PoE menu provides the following features for managing the system.

PoE Configuration
PoE Status
PoE Schedule
PoE Alive Check

Object	Description
PoE Configuration	Allows to centralize management PoE power for PDs.
PoE Status	Displays the current PoE usage.
PoE Schedule	Allows centralizing management PoE power for providing
	schedule.
PD Alive Check	Allows centralizing management PoE power for checking PDs
	alive.

### **4.9.1 PoE Configuration**

This section allows the user to inspect and configure the current PoE configuration setting.

ower Supply	•	Enable ~ 51 V						
Power Limit N	Mode	Consumption						
Power Alloca	tion							0 / 120 V
Port	Description	PoE Function	Schedule	Power Mode	Priority	Device Class	Current Used [mA]	Powered Used [W]
		<all> 🗸</all>	<all> 🗸</all>	AT/AF	<all> 🗸</all>			
All					[		0	0
All 1		Enable 🗸	None 🗸	AT/AF	High 🗸		0	
		Enable V Enable V	None V	AT/AF	High ✓		0	0
1								0
1 2		Enable V	None ~	AT/AF	High ~		0	

Cancel Changes

Apply Settings

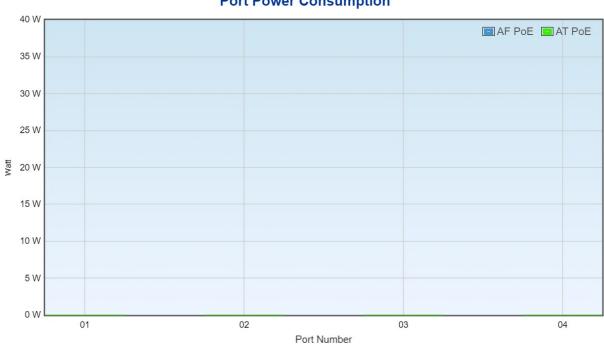


Object	Description
System PoE Admin	Allows user to enable or disable PoE function. It will cause all of PoE
Mode	ports to supply or not to supply power.
PoE Function	There are three modes for PoE mode.
	Enable : enable PoE function
	■ <b>Disable</b> : disable PoE function.
	Schedule: enable PoE function in schedule mode.
Schedule	Indicates the scheduled profile mode. Possible profiles are:
	■ Profile1
	■ Profile2
	■ Profile3
	■ Profile4
Priority	The Priority represents PoE ports priority. There are three levels of
	power priority named Low, High and Critical.
	The priority is used in case the total power consumption is over the
	total power budget. In this case, the port with the lowest priority will
	be turned off, and power for the port of higher priority will be offered.
Device Class	Displays the class of the PD attached to the port, as established by
	the classification process. Class 0 is the default for PDs. The PD is
	powered based on PoE Class level if the system is working in
	Classification mode. The PD will return to Class 0 to 4 in accordance
	with the maximum power
Current Used [mA]	The <b>Power Used</b> shows how much current the PD currently is
	using.
Powered Used [W]	The <b>Power Used</b> shows how much power the PD currently is using.



### 4.9.2 PoE Status

This section provide per port PoE status.



#### **Port Power Consumption**

#### 4.9.3 PoE Schedule

This page allows the user to define PoE schedule and scheduled power recycling.

Please press Add New Rule button to start setting PoE Schedule function. You have to set PoE schedule to profile and then go back to PoE Port Configuration, and select "Schedule" mode from per port "PoE Mode" option to enable you to indicate which schedule profile could be applied to the PoE port.



Profile	e						Profile	1	~												
Wee	k Day	Star	Hour	Star	t Min	En	d Hour	E	nd Min	R	eboot Ena	ble	Reboo	t Only	Reb	oot Hour	F	Reboot N	/lin	Delet	te
Sun	~	00	~	00	~	23	11	<ul><li>✓ 59</li></ul>	) ``	•					00		~ 00	)	~	Add	I
								A	pply Se	ettings	Ca	ncel Cha	anges								
_																			_		
																	PoE S	Schedule		PoE Rel	bo
																	PoE S	Schedule		PoE Rel	bod
																	PoE S	Schedule	-	PoE Rel	bo
																	PoE S	Schedule		PoE Rel	bod
																	PoE S	Schedule		PoE Rel	boo
																	PoE S	Schedule		PoE Rel	boo
																	PoE S	Schedule		PoE Rel	boc

Object	Description
Object	Description
Profile	Set the schedule profile mode. Possible profiles are:
	Profile1
	Profile2
	Profile3
	Profile4
Week Day	Allows user to set week day for defining PoE function by enabling it
	on the day.
Start Hour	Allows user to set what hour PoE function does by enabling it.
Start Min	Allows user to set what minute PoE function does by enabling it.
End Hour	Allows user to set what hour PoE function does by disabling it.
End Min	Allows user to set what minute PoE function does by disabling it.
Reboot Enable	Allows user to enable or disable the whole PoE port reboot by PoE
	reboot schedule. Please note that if you want PoE schedule and PoE
	reboot schedule to work at the same time, please use this function,
	and don't use <b>Reboot Only</b> function. This function offers
	administrator to reboot PoE device at an indicated time if
	administrator has this kind of requirement.
Reboot Only	Allows user to reboot PoE function by PoE reboot schedule. Please
	note that if administrator enables this function, PoE schedule will not
	set time to profile. This function is just for PoE port to reset at an



	indicated time.
Reboot Hour	Allows user to set what hour PoE reboots. This function is only for
	PoE reboot schedule.
Reboot Min	Allows user to set what minute PoE reboots. This function is only for
	PoE reboot schedule.

### 4.9.4 PD Alive Check

The VPN Router can be configured to monitor connected PD's status in real-time via ping action. Once the PD stops working and without response, the PoE Switch is going to restart PoE port power, and bring the PD back to work. It will greatly enhance the reliability and reduces administrator management burden.

Port	Mode	Remote PD IP Address	Interval Time(10~300s)	Retry Count(1~5)	Action	Reboot Time (30~180s)
All	<all> 🗸</all>			<all> 🗸</all>	<all> ~</all>	
1	Disable 🗸	192.168.1.10	10	1 ~	None 🗸	30
2	Disable 🗸	192.168.1.11	10	1 ~	None 🗸	30
3	Disable 🗸	192.168.1.12	10	1 ~	None 🗸	30
4	Disable V	192.168.1.13	10	1 -	None 🗸	30

Object	Description
• Mode	Allows user to enable or disable per port PD Alive Check function.
	By default, all ports are disabled.
Remote PD IP	This column allows user to set PoE device IP address for system
Address	making ping to the PoE device. Please note that the PD's IP address
	must be set to the same network segment with the PoE Switch.
Interval Time	This column allows user to set how long system should issue a ping
(10~300s)	request to PD for detecting whether PD is alive or dead.
	Interval time range is from 10 seconds to 300 seconds.
<ul> <li>Retry Count (1~5)</li> </ul>	This column allows user to set the number of times system retries
	ping to PD.
	For example, if we set count 2, it means that if system retries ping to
	the PD and the PD doesn't response continuously, the PoE port will
	be reset.
Action	Allows user to set which action will be applied if the PD is without any



	response. The PoE Switch Series offers the following 3 actions:
	PD Reboot: It means system will reset the PoE port that is
	connected to the PD.
	PD Reboot & Alarm: It means system will reset the PoE port
	and issue an alarm message via Syslog.
	Alarm: It means system will issue an alarm message via
	Syslog.
Reboot Time	This column allows user to set the PoE device rebooting time as
(30~180s)	there are so many kinds of PoE devices on the market and they have
	a different rebooting time.
	The PD Alive-check is not a defining standard, so the PoE device on
	the market doesn't report reboot done information to the PoE Switch.
	Thus, user has to make sure how long the PD will take to finish
	booting, and then set the time value to this column.
	System is going to check the PD again according to the reboot time.
	If you are not sure of the precise booting time, we suggest you set it
	longer.



# 4.10 Wireless

The Wireless menu provides the following features for managing the system

2.4G WiFi
5G WiFi
MAC ACL
WiFi Advanced
WiFi Statistics
Connection Status

Object	Description
2.4G WiFi	Allow to configure 2.4G WiFi.
5G WiFi	Allow to configure 5G WiFi.
MAC ACL	Allow configure MAC ACL.
WiFi Advanced	Allow to configure advanced setting of WiFi.
WiFi Statistics	Display the statistics of WiFi traffic.
Connection Status	Display the connection status.

### 4.10.1 2.4G WiFi

This page allows the user to define 2.4G WiFi.

2.4G WiFi	Configuration						
Basic	Virtual AP1	Virtual AP2	Virtual AP3				
Wireles	s Status	• E	Enable O Disable				
Wireles	s Name (SSID)	PLA	NET_2.4G				
Hide SS	SID	OE	Enable 💿 Disable				
Bandwie	dth	201	∕IHz ✓				
Channe	I	6	~				
Encrypt	ion	Ope	en	~			
WiFi Mu	ıltimedia	• E	Enable O Disable				



Object	Description
Wireless Status	Allows user to enable or disable 2.4G WiFi
Wireless Name (SSID)	It is the wireless network name. The default 2.4G SSID is
	"PLANET_2.4G"
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, "20MHz" or "40MHz"
Channel	It shows the channel of the CPE. Default 2.4GHz is channel 6.
Encryption	Select the wireless encryption. The default is " <b>Open</b> "
WiFi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia ) function

### 4.10.2 5G WiFi

This page allows the user to define 5G WiFi.

5G WiFi Configuration	
Basic Virtual AP1 Virtual	IAP2 Virtual AP3
Wireless Status Wireless Name (SSID) Hide SSID Bandwidth Channel Encryption WiFi Multimedia	<ul> <li>Enable O Disable</li> <li>PLANET_5G</li> <li>Enable O Disable</li> <li>80MHz </li> <li>36 </li> <li>Open </li> <li>Enable O Disable</li> </ul>
Object	Description
Object Wireless Status	Description Allows user to enable or disable 5G WiFi
Wireless Status	Allows user to enable or disable 5G WiFi
Wireless Status	Allows user to enable or disable 5G WiFi It is the wireless network name. The default 5G SSID is
Wireless Status Wireless Name (SSID)	Allows user to enable or disable 5G WiFi It is the wireless network name. The default 5G SSID is "PLANET_5G"
Wireless Status Wireless Name (SSID) Hide SSID	Allows user to enable or disable 5G WiFi It is the wireless network name. The default 5G SSID is "PLANET_5G" Allows user to enable or disable SSID
Wireless Status Wireless Name (SSID) Hide SSID	Allows user to enable or disable 5G WiFi It is the wireless network name. The default 5G SSID is "PLANET_5G" Allows user to enable or disable SSID Select the operating channel width, " <b>20MHz</b> " or " <b>40MHz</b> " or
Wireless Status Wireless Name (SSID) Hide SSID Bandwidth	Allows user to enable or disable 5G WiFi It is the wireless network name. The default 5G SSID is "PLANET_5G" Allows user to enable or disable SSID Select the operating channel width, " <b>20MHz</b> " or " <b>40MHz</b> " or " <b>80MHz</b> "



### 4.10.3 MAC ACL

This page allows the user to define MAC ACL.

MAC ACI	<u>L</u>			
MAC ACL			○ Enable	
	Rules			
Index	Active	Device Name	MAC Address Action       00:30:4F:00:00:01     Add       Scan	
Object		ct	Description	
Active			Allows the devices to pass in the rule	
Device Name			Set an allowed device name	
MAC Address			Set an allowed device MAC address	
Add			Press the " <b>Add</b> " button to add end-device that is scanned from wireless network and mark them	
Scan			Connect to client list	



### 4.10.4 WiFi Advanced

This page allows the user to define advanced setting of WiFi.

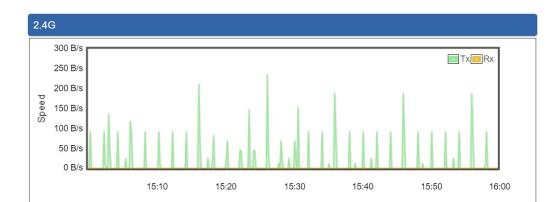
ViFi Advanced		
2.4G Mode	11 AX 🗸	
5G Mode	11 AX 🗸	
2.4GHz Maximum Associated Clients	32	(Range 1~64)
5GHz Maximum Associated Clients	32	(Range 1~64)
2.4G Coverage Threshold	-90	(-95dBm ~ -60dBm)
5G Coverage Threshold	-90	(-95dBm ~ -60dBm)
2.4G TX Power	Max(100%	) ~
5G TX Power	Max(100%	) <b>~</b>

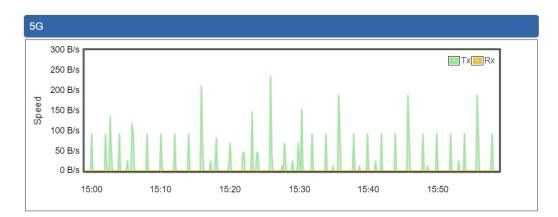
Object	Description
2.4G Mode	11AC: Select 802.11B/G or 802.11N/G
	11AX: Select 802.11B/G or 802.11N/G or 802.11AX
5G Mode	11AC: Select 802.11A or 802.11AN or 802.11AC
	11AX: Select 802.11A or 802.11AN or 802.11AC or 802.11AX
2.4GHz Maximum Associated	The maximum users are 64
Clients	
5GHz Maximum Associated	The maximum users are 64
Clients	
2.4G Coverage Threshold	The coverage threshold is to limit the weak signal of clients
	occupying session. The default is -90dBm
5G Coverage Threshold	The coverage threshold is to limit the weak signal of clients
	occupying session. The default is -90dBm
2.4G TX Power	The range of transmit power is <b>Max (100%)</b> , Efficient (75%),
	Enhanced (50%), Standard (25%) or Min (15%). In case of
	shortening the distance and the coverage of the wireless network,
	input a smaller value to reduce the radio transmission power
5G TX Power	The range of transmit power is <b>Max (100%)</b> , Efficient (75%),
	Enhanced (50%), Standard (25%) or Min (15%). In case of
	shortening the distance and the coverage of the wireless network,
	input a smaller value to reduce the radio transmission power



### 4.10.5 WiFi Statistics

This page shows the statistics of WiFi traffic.





# 4.10.6 Connection Status

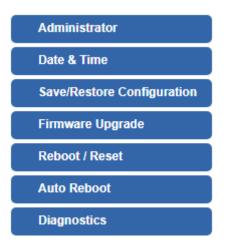
This page shows the host names and MAC address of all the clients in your network

Client List			
No. Name MAC Add	ress Signal Connected Time		
Object	Description		
Name	Display the host name of connected clients.		
MAC Address	Display the MAC address of connected clients.		
Signal	Display the connected signal of connected clients.		
Connected Time	Display the connected time of connected clients.		



# 4.11 Maintenance

The Maintenance menu provides the following features for managing the system



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

#### 4.11.1 Administrator

To ensure the router's security is secure, you will be asked for your password when you access the router's Web-based utility. The default user name and password are "**admin**". This page will allow you to modify the user name and passwords.



Account Password			
Username	admin		
Password			
Confirm Password			

Apply Settings

Cancel Changes

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

#### 4.11.2 Date and Time

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

Date and Time	
Current Time	Year         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 Isable
NTP Server	time.nist.gov
	time.windows.com
	time.stdtime.gov.tw
	Apply Settings Cancel Changes

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



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

### 4.11.3 Saving/Restoring Configuration

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

Save/Restore Configuration		
Configuration Export Configuration Import Import	Export Choose File No file chosen	
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*		

#### 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



Object	Description
USB Storage	The status of USB storage.
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 router, please press the Umount button first.

### 4.11.4 Upgrading Firmware

This page provides the firmware upgrade of the route.

Firmware Upgrade	
Select File	Choose File No file chosen
Upgrade	

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

### 4.11.5 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.	

Object	Description
Reboot	Press the button to reboot system.
Reset	Press the button to restore all settings to factory default settings.
	seungs.
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.

### 4.11.6 Diagnostics

The page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press "Ping", ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The Page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Ping Test	
Interface Target Host Numbers of Packet Ping	Any <b>v</b>
	/



#### Enterprise 5-Port 10/100/1000T VPN Security Router VR-300 series

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



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



# **Appendix A: DDNS Application**

#### Configuring PLANET DDNS steps:

- Step 1: Visit DDNS provider's web site and register an account if you do not have one yet. For example, register an account at <a href="http://planetddns.com">http://planetddns.com</a>
- Step 2: Enable DDNS option through accessing web page of the device.
- Step 3: Input all DDNS settings.

