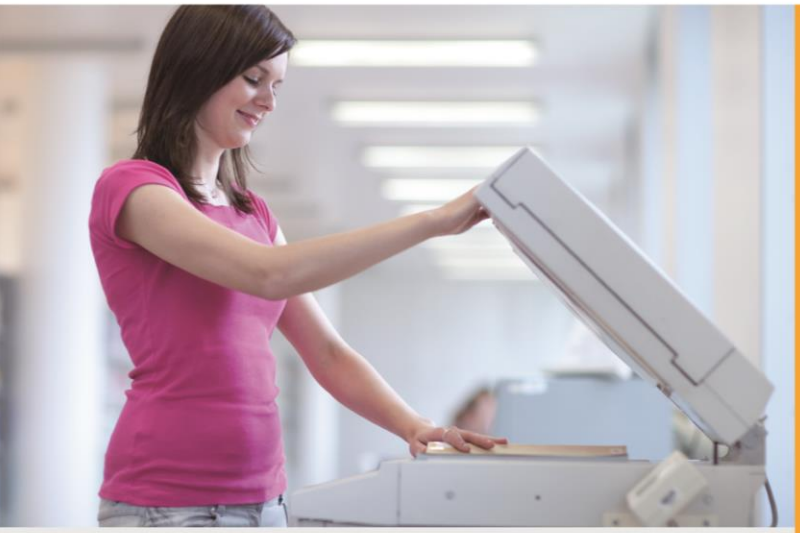
PLANET
Networking & Communication

User's Manual

Enterprise Dual 10G VPN Security Router

- XVR-800 Series
- ZT-800 Series
- CSG-800 Series



www.PLANET.com.tw

Copyright

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

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

EU Representative
PLANET Technology Europe B.V.
Address: Posthoornstraat 11, 3011 WD Rotterdam, NL
Email: eu_rep@planet.com.tw
URL: www.planet.com.tw

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.

Warning: 1) This device must be earthed. 2) For indoor use only!

CE mark Warning

This device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

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 Enterprise Dual 10G VPN Security Router

Model: XVR-800, XVR-800P, XVR-800BE, XVR-800BE-NR, ZT-800, ZT-800BE, CSG-800, CSG-800BE

Rev.: 1.1 (Aug., 2026)

Part No. EM-XVR-800_ZT-800_CSG-800_series_v1.1

Table of Contents

Chapter 1. Product Introduction

Thank you for purchasing PLANET VPN Router, XVR-800 / ZT-800 / CSG-800 series. The descriptions of these models are as follows:

XVR-800	Enterprise Dual 10G VPN Security Router with 4-Port 10/100/1000T
XVR-800P	Enterprise Dual 10G VPN Security Router with 4-Port 10/100/1000T 802.3at PoE+
XVR-800BE	Enterprise Wi-Fi 7 5100BE + Dual 10G VPN Security Router with 4-Port 10/100/1000T
XVR-800BE-NR	Enterprise 5G NR Cellular + Wi-Fi 7 5100BE + Dual 10G VPN Security Router with 4-Port 10/100/1000T
ZT-800	Dual 10G Zero Trust Security Gateway with 4-Port 10/100/1000T
ZT-800BE	Dual 10G Zero Trust Security Gateway with Wi-Fi 7 5100BE
CSG-800	Dual 10G Cybersecurity Gateway with 4-Port 10/100/1000T
CSG-800BE	Dual 10G Cybersecurity Gateway with Wi-Fi 7 5100BE

Model / Spec.	XVR-800 ZT-800 CSG-800	XVR-800BE ZT-800BE CSG-800BE	XVR-800P	XVR-800BE-NR
Wi-Fi	-	■	-	■
Fiber	■	■	■	■
PoE	-	-	■	--
5G NR Cellular	-	-	-	■

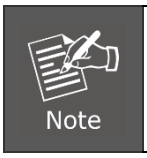
“VPN Router” mentioned in this Quick Installation Guide refers to the above models.

1.1 Package Contents

The package should contain the following:

- VPN Router x 1
- Quick Installation Guide (QR code) x 1
- Power Cord x 1
- Rubber Feet x 4
- Rack-mounting Kit x 1
- SFP Dust Cap x 1
- Other components as shown below:

Model Name	Dual band antenna	5G NR antenna
XVR-800	-	-
XVR-800P	-	-
XVR-800BE	3	-
XVR-800BE-NR	3	4
ZT-800	-	-
ZT-800BE	3	-
CSG-800	-	-
CSG-800BE	3	-



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

1.2 Overview

Dual 10G-Capable VPN Gateway with Comprehensive Multi-VPN and Post-Quantum Security Support

This VPN Gateway is designed for high-performance enterprise connectivity, featuring flexible 10G fiber and copper WAN/LAN interfaces and 4 Gigabit LAN ports for efficient network deployment. It supports multiple VPN protocols—including IPSec, SSL (OpenVPN), WireGuard, GRE, PPTP, and L2TP—to enable secure communication across distributed networks. With PQC TLS (Post-Quantum Cryptography TLS) readiness, the XVR-800 series enhances long-term security against emerging quantum computing threats. The gateway also delivers dual-WAN failover, load balancing, and advanced routing in a compact industrial-grade design.

The XVR-800 series serves as a central gateway connecting diverse IPv6-enabled IoT devices and network environments, as illustrated below.

Flexible 10Gbps WAN interface Enables Extension of Network Deployment

The XVR-800 is equipped with both copper and fiber WAN interfaces, featuring an SFP+ slot that supports a wide range of SFP+ transceivers for FTTx and long-distance extensions. Administrators can select SFP+ modules according to distance requirements:

- Multi-mode fiber: 550 m to 2 km
- Single-mode / WDM fiber: 10 km, 20 km, 30 km, 40 km, 50 km, 60 km, 70 km, up to 120 km

  This capability allows the device to efficiently uplink to backbone switches or monitoring centers over long distances.

Secure Boot for Trusted System Integrity

The XVR-800 series incorporates a Secure Boot mechanism to ensure that only authenticated and trusted firmware can be executed during system startup. This hardware-based protection prevents unauthorized or tampered firmware from being loaded, safeguarding the device against malicious attacks at the system level and ensuring a trusted foundation for network security.

Advanced Threat Protection with Built-in IDS/IPS and Layer 7 Deep Packet Inspection (CSG-800 series only)

The **CSG-800** integrates built-in **Intrusion Detection and Prevention (IDS/IPS)** with **Layer 7 Deep Packet Inspection (DPI)** to continuously inspect network traffic and identify malicious activities before they impact business operations. By analyzing application-layer traffic in real time, the gateway detects known threats, blocks suspicious connections, enhances application visibility, and helps organizations minimize cyber risks while maintaining stable, reliable, and high-performance network operations.

Continuous Security Monitoring with Security Log and Scheduled Signature Updates (CSG-800 series only)

The **CSG-800** provides comprehensive **security logs**, **event reports**, and **Scheduled Signature Updates** to simplify cybersecurity management and improve threat visibility. Administrators can efficiently monitor network activities, analyze security incidents, and quickly identify potential threats, while continuously updated threat signatures ensure protection against newly emerging cyber attacks without manual intervention, maintaining an up-to-date security posture with reduced management effort.

Zero Trust–Protected VPN Access with Passkey Authentication and MFA Enforcement (ZT-800 & CSG-800 series only)

The ZT-800 introduces a secure VPN Portal designed to strengthen identity verification before VPN connectivity is established. By supporting FIDO2 passkey authentication, multi-factor authentication (MFA), and optional external RADIUS integration, the portal ensures that only verified users can obtain authorized OpenVPN or WireGuard client configurations.

Unlike traditional VPN deployment models where credentials alone grant tunnel access, the ZT-800 enforces identity validation at the profile provisioning stage—reducing the risk of unauthorized VPN distribution and strengthening access control across remote users and distributed teams.

This identity-aware VPN onboarding mechanism enables organizations to implement Zero Trust principles for remote connectivity while maintaining compatibility with widely deployed VPN client infrastructures.

Automatic Failover between 5G NR and Dual WAN (For XVR-800FW-NR only)

Designed with 5G NR, dual WAN interfaces (fiber and copper), 1000X SFP and Gigabyte Ethernet, the XVR-800FW-NR ensures Internet connectivity by featuring failover functionality between 5G NR and dual WAN. It provides flexibilty to set priority for 5G NR or dual WAN connection. When the main WAN interface fails, the secondary WAN interface will automatically back up the connection to ensure always-on connectivity.

Ultra-Fast Speed 4G/5G Network (For XVR-800FW-NR only)

The XVR-800FW-NR supports 5G NR DL (downlink) speeds higher than 2.4 Gbps and 4G LTE DL speeds of up to 1 Gbps. The wide spectrum bandwidth accelerates internet speeds and reduces network latency for premium and time-sensitive connectivity services. It also supports multi-band connectivity including LTE FDD/TDD, WCDMA and GSM for a wide range of applications.

*The real 5G NR/4G LTE data rate is dependent on local service provider.

GPS Included (For XVR-800FW-NR only)

The XVR-800FW-NR is equipped with the global positioning system feature. It adopts the 5G NR technology for the multiple global navigation systems (GPS/GLONASS/BeiDou/Galileo/QZSS). It helps to position location of cellular gateway based on a network of satellites that continuously transmits necessary data. More signals transmitted from more satellites can triangulate its location on the ground, meaning any location can be easily tracked.

Wi-Fi 7 5100BE Delivers Ultra-High-Speed Wireless Performance (Wireless model only)

The XVR-800BE supports up to 160 MHz channel bandwidth, a key feature of Wi-Fi 7, doubling that of Wi-Fi 6E. Its peak transmission rate of 5100 Mbps is designed for commercial environments, delivering stable performance, higher efficiency, and reliable operation. With 4096-QAM encoding, the XVR-800BE transmits more data per signal, increasing throughput and making it ideal for high-bandwidth applications such as 4K/8K video streaming, AR/VR experiences, and real-time cloud services while maintaining a stable and efficient network connection. Designed for robust dual-band operation, the XVR-800BE ensures seamless connectivity across both 2.4 GHz and 5 GHz frequencies. This design guarantees consistent data transfer and stable connections even in interference-prone, high-density scenarios, delivering the reliability demanded by modern commercial applications.

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

The XVR-800 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 statuses, such as overload, low voltage, over voltage and high temperature. User can obtain detailed information about the real-time PoE working condition of the XVR-800 series directly.

PoE Schedule (PoE model only)

Under the trend of energy savings worldwide and contributing to environmental protection, the XVR-800 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 XVR-800 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 XVR-800 series can be configured to monitor connected PD status in real time via ping action. Once the PD stops working and responding, the XVR-800 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.

Integrated Wi-Fi Management for Secure and Easy Deployment

The XVR-800 integrates an AP Controller, Captive Portal, RADIUS authentication, and DHCP server to streamline Wi-Fi deployment for small and medium-sized businesses. These built-in services eliminate the need for external servers, enabling administrators to centrally manage APs, enforce access policies, and deliver secure employee and guest Wi-Fi networks with reduced setup complexity.

Centralized Remote Control of Managed APs

The XVR-800 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 XVR-800 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.

High-Availability VPN Security Router Designed for SMB Applications

The XVR-800 series ensures strong data privacy and secure remote access through its comprehensive VPN suite. It supports IPSec VPN with DES/3DES/AES encryption and MD5, SHA-1, SHA-256, SHA-384, and SHA-512 authentication, as well as GRE tunneling, SSL VPN, PPTP, L2TP, and WireGuard for modern, lightweight, high-speed encrypted connections. With this extensive VPN capability, the XVR-800 series provides secure, flexible, and resilient connectivity for branch sites, remote workers, and sensitive business operations.

Excellent Ability in Threat Defense

The XVR-800 series with built-in SPI (stateful packet inspection) firewall and DoS/DDoS attack mitigation functions provides 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.

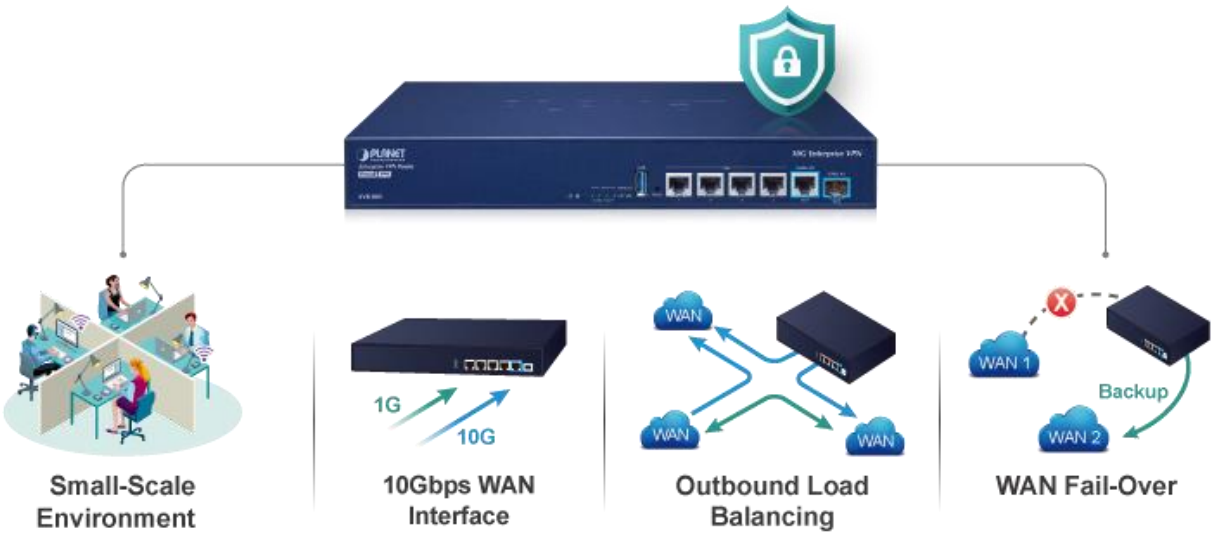
Cybersecurity Network Solution to Minimize Security Risks

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 XVR-800 series is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the XVR-800 series offers an easy-to-use, platform independent management and configuration facility. The XVR-800 series supports SNMP and it can be managed via any management software based on the standard SNMP protocol. With support for advanced security mechanisms such as Secure Boot and PQC TLS readiness, the XVR-800 series ensures long-term protection against evolving cyber threats, including quantum-era attacks.

1.3 Topology

High-Performance Network Reliability with Dual-WAN and Load Balancing

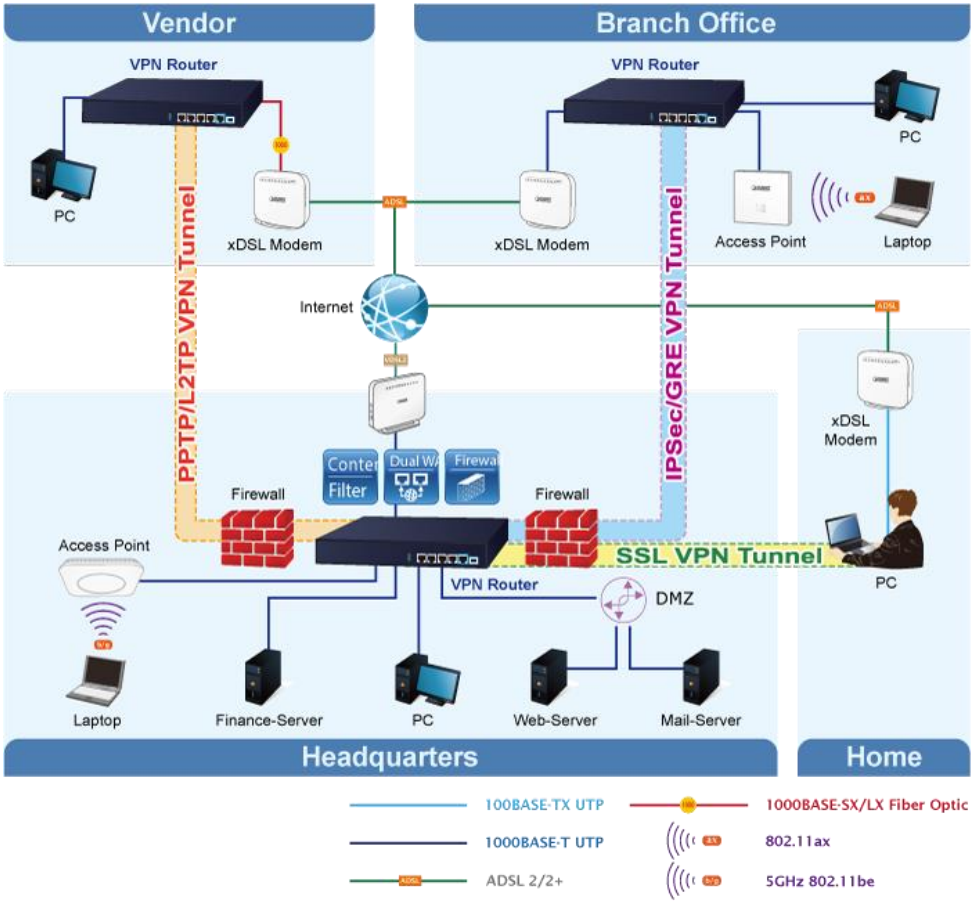
The XVR-800 series is ideal for small to medium-sized businesses that require stable and efficient network connectivity. With dual-WAN load balancing and automatic failover, it ensures continuous Internet access by intelligently distributing traffic and switching to a backup link when needed. Combined with high-speed Gigabit and 10G interfaces, QoS, and VPN capabilities, it supports critical applications such as VoIP, video conferencing, and cloud services, delivering reliable and optimized network performance for daily operations.



Furthermore, the XVR-800 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.

Centralized Network Management with Integrated Security Services

Designed for small to medium-sized businesses, the XVR-800 series integrates essential network services such as AP Controller, Captive Portal, RADIUS authentication, and DHCP server into a single platform. This allows administrators to easily deploy and manage secure wired and wireless networks without additional servers. Combined with SPI firewall, DoS/DDoS protection, content filtering, and QoS capabilities, the XVR-800 series delivers a unified solution that enhances network security, simplifies management, and ensures stable performance for daily business operations.

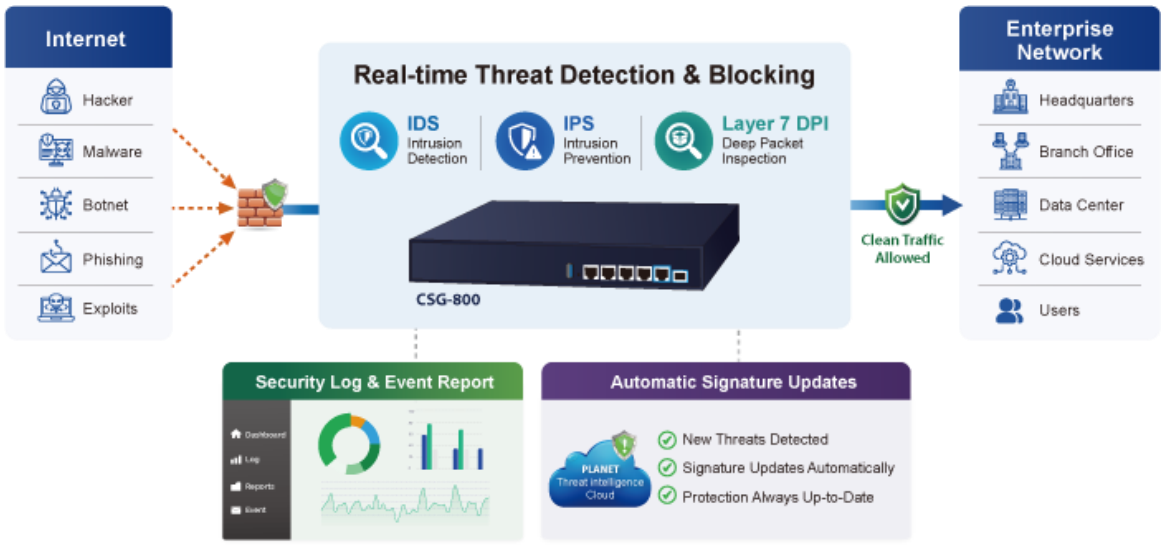


Zero Trust Access Control for Identity-Based Network Security

The ZT-800 series adopts a Zero Trust architecture to secure modern enterprise and hybrid work environments. By verifying every user, device, and connection through identity authentication, MFA, and policy enforcement, it prevents unauthorized access regardless of network location. With built-in RADIUS, Captive Portal, and VPN access control, administrators can enforce role-based policies across wired, wireless, and remote connections, effectively protecting sensitive resources and minimizing lateral movement within the network.

Intelligent Threat Detection for Enterprise Network Security

The **CSG-800** series provides comprehensive cybersecurity protection for enterprise headquarters, branch offices, and industrial networks by continuously inspecting inbound and outbound traffic with built-in **IDS/IPS** and **Layer 7 Deep Packet Inspection (DPI)**. It automatically detects malicious activities, blocks cyber threats, and provides application-level visibility, while **security logs**, **event reports**, and **Scheduled Signature Updates** enable administrators to monitor security events and respond quickly to newly emerging threats. This proactive security architecture helps organizations maintain continuous protection without interrupting normal network operations.



1.4 Features

➢ Highlights

- One 1G/2.5G/5G/10GBASE-T RJ45 Port for WAN/LAN interface
- One 1G/2.5G/10GBASE-X SFP+ slot for WAN/LAN interface
- Enterprise threat protection with built-in IDS/IPS, Layer 7 DPI, SPI firewall and content filtering (CSG-800 series only)
- Continuous security monitoring with security logs, event reports and Scheduled Signature Updates (CSG-800 series only)
- Zero Trust access control with FIDO2 Passkey, TOTP MFA and certificate-based authentication (ZT-800 & CSG-800 series only)
- Dual-WAN failover and dual-WAN load balancing
- SSL VPN and robust hybrid VPN (IPSec/PPTP/L2TP over IPSec/OpenVPN/WireGuard)
- Stateful Packet Inspection (SPI) firewall and content filtering
- Blocks DoS/DDOS attack, port range forwarding
- High Availability, AP Controller, Captive Portal and RADIUS
- IPv6, SNMP, PLANET DDNS and Universal Network Management System
- Planet NMS controller system and CloudNMS platform supported
- Supports up to 100 concurrent SSL VPN connections

➢ Hardware

- 4 10/100/1000BASE-T RJ45 ports
- 1 1G/2.5G/5G/10GBASE-T RJ45 Port for WAN/LAN interface
- 1 1G/2.5G/10GBASE-X SFP+ slot for WAN/LAN interface
- 1 USB port for system configuration backup and restoration
- Reset button
- Desktop installation or rack mounting

➢ Cellular Interface (XVR-800BE-NR only)

- Supports multi-band connectivity with 5G NR (NSA/SA), LTE-FDD, LTE-TDD, and WCDMA
- Built-in SIM and broadband backup for network redundancy
- Four detachable antennas for 5G NR connection
- LED indicators for signal strength and connection status
- Global Navigation Satellite System (GNSS)

➢ RF Interface Characteristics (Wireless model only)

- A state-of-the-art Wi-Fi 7 architecture with advanced MIMO technology

- Up to 5100 Mbps (approximately 689 Mbps at 2.4 GHz and 4324 Mbps at 5 GHz) with 4K-QAM (4096-QAM) encoding for boosted throughput

➢ 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

- Secure Boot to ensure trusted firmware integrity
- Hardware TRNG (True Random Number Generator) for high-entropy cryptographic key generation
- Stateful Packet Inspection (SPI) firewall
- Intrusion Detection and Prevention (IDS/IPS) (CSG-800 series only)
- Layer 7 Deep Packet Inspection (DPI) (CSG-800 series only)
- Blocks DoS/DDoS attack
- Content Filtering
- Application-level traffic visibility
- Zero Trust access control (ZT-800 & CSG-800 series only)
- Identity-based access policy
- MAC Filtering and IP Filtering
- NAT ALGs (Application Layer Gateway)
- Blocks SYN/ICMP Flooding

- Security log and event reporting
- Automatic threat signature updates
- Security design follows EU Cyber Resilience Act (CRA) principles

➢ VPN Features

- Zero Trust-protected VPN access (ZT-800 & CSG-800 series only)
- Identity-based VPN authentication
- IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (OpenVPN, compatible with VPN services such as Surfshark and NordVPN), WireGuard
- Encryption methods: DES, 3DES, AES, AES-128/192/256
- Authentication methods: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- PQC TLS (Post-Quantum Cryptography TLS) readiness for future-proof encryption

➢ Networking

- Outbound load balancing
- Failover for dual-WAN
- High Availability
- Captive Portal
- RADIUS Server/Client
- Static IP/PPPoE/DHCP client for WAN
- DHCP server/NTP client for LAN
- Protocols: TCP/IP, UDP, ARP, IPv4, IPv6
- Port forwarding, QoS, DMZ, IGMP, UPnP, SNMPv1,v2c, v3
- MAC address clone
- DDNS: PLANET DDNS, Easy DDNS, DynDNS and No-IP
- NAT disable support for pure routing mode deployment

➢ Others

- Setup wizard
- Dashboard for system and security monitoring
- Security log viewer (CSG-800 series only)
- Event reports
- Scheduled Signature Updates (CSG-800 series only)
- SFP-DDM (Digital Diagnostic Monitor)
- Supported access by HTTP or HTTPS
- Auto reboot
- PLANET NMS System and Smart Discovery Utility for deployment management
- PLANET CloudNMS app for real-time monitoring

1.5 Product Specifications

Standard

Model	XVR-800	ZT-800	CSG-800
Hardware Specifications			
Ethernet	4 10/100/1000BASE-T RJ45 Ethernet ports (Port 1 to 4) 1 1G/2.5G/5G/10GBASE-T RJ45 port (Port 5) Supports WAN port mode or LAN port mode over software configuration		
Fiber	One 1G/2.5G/10GBASE-X SFP+ port (Port 6) Supports WAN port mode or LAN port mode over software configuration		
USB Port	1 USB 2.0 port for system configuration backup and restoration		
Reset Button	Reset to factory default		
Thermal Fan	1		
LED Indicators	System: PWR, Internet, (Green) Ethernet Interfaces (Port 1-4): 10/100/1000 LNK/ACT (Green) Ethernet Interfaces (Port 5): 1G/2.5G/5G/10G LNK/ACT (Green) Fiber Interfaces (Port 6): 1G/2.5G/10G LNK/ACT (Green)		
Installation	Desktop installation or rack mounting		
Power Requirements	100~240V AC, 50/60Hz, auto-sensing		
Power Consumption / Dissipation	Max. 3.3 watts/10.92BTU (Power on without any connection) Max. 11 watts/37.53BTU (Full loading)		
Weight	1725g		
Dimensions (WxDxH)	330.2 x 200 x 43.1mm, 1U height		
Enclosure	Metal		
Security Service			
Firewall Security	Cybersecurity Secure Boot TRNG for Secure Cryptographic Key Generation Stateful Packet Inspection (SPI) Security Log and Event Reporting (CSG-800 series only) Automatic Threat Signature Updates (CSG-800 series only) Blocks DoS/DDoS Attacks Role-Based Access Policy Enforcement Multi-Factor Authentication via External Hardware Security Key Support		
ALG (Application Layer Gateway)	SIP, RTSP, FTP, H.323, TFTP		
NAT	Port forwarding DMZ Host UPnP NAT disable (supports routing mode)		
Content Filtering	MAC filtering IP filtering Web filtering		

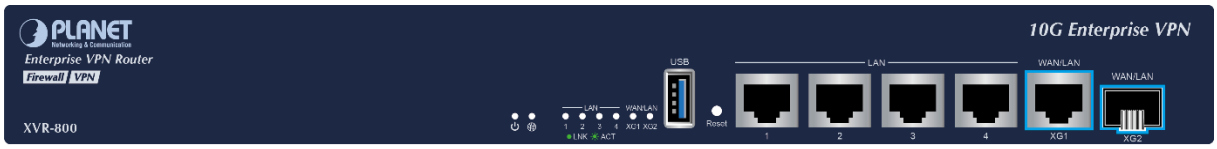
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)		
Intrusion Prevention System	-	-	Intrusion Detection and Prevention (IDS/IPS) Layer 7 Deep Packet Inspection (DPI) Application-level traffic visibility
Secure Boot	Establishes a **Chain of Trust (CoT)** across all boot stages via cryptographic image signature verification		
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. 9.4Gbps		
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 (Net-to-Net, Host-to-Net) IPSec Remote Server GRE PPTP Server L2TP Server SSL Server SSL Client (Open VPN, Surfshark, NordVPN, PureVPN) WireGuard VPN Server/Client		
VPN Tunnel Capacity by Protocol	IPSec：16 GRE：5 PPTP：100 SSL VPN：100		
VPN Throughput	L2TP (1Gbps): 145~463Mbps L2TP (10Gbps): 483~885Mbps L2TP/IPsec (1Gbps): 150~334Mbps L2TP/IPsec (10Gbps): 438~496Mbps IPsec/AES128 (1Gbps): 894~910Mbps IPsec/AES128 (10Gbps): 1,110~1,310Mbps IPsec/AES256 (1Gbps): 752~842Mbps IPsec/AES256 (10Gbps): 864~1,060Mbps WireGuard (1Gbps): 815~883Mbps WireGuard (10Gbps): 1,430~1,890Mbps		
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encryption		

	PQC TLS (Post-Quantum Cryptography TLS) ready Supports Hybrid Post-Quantum TLS key exchange using ML-KEM (Kyber)	
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm TLS_KYBER_RSA_WITH_AES_256_GCM_SHA384	
Zero Trust		
Zero Trust Authentication	-	CA Certificate, USB Key, Mobile QR code, Windows Hello
Access Control & Identity Security	-	Zero Trust access control Identity-based access policy Role-based access enforcement Multi-factor authentication (MFA) Hardware security key support (FIDO2)
Management		
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported PLANET NMS System/CloudNMS	
Secure Management Interfaces	SSHv2, TLSv1.3, SNMP v3	
System Log	System Event Log	
Others	Setup wizard Dashboard System status/service Statistics Connection 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)	

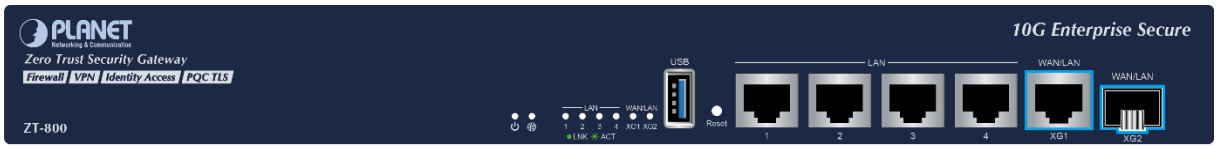
Chapter 2. Hardware Introduction

2.1 Physical Descriptions

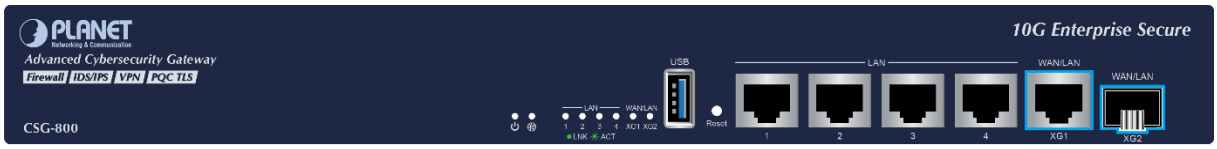
Front View



XVR-800



ZT-800



CSG-800

■ **System**

LED	Color	Function
PWR	**Green**	Lights up when the power is on.
Internet	**Green**	Lights up when the router connects to internet successfully.

■ **LAN Per 10/100/1000Mbps RJ45 Port (Ports 1 to 4)**

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

■ **WAN/LAN 100M/1G/2.5G/5G/10GBASE-T RJ45 Port (Port 5)**

LED	Color	Function	
LNK/ACT	**Green**	Lights	To indicate the port is running at 10Gbps or 5GMbps or 2.5GMbps or 1GMbps speed and successfully established
		Blink	To indicate that the router is actively sending or receiving data over that port.

■ **WAN/LAN 1G/2.5G/10GBASE-X SFP+ Port (Port 6)**

LED	Color	Function	
LNK/ACT	**Green**	Lights	To indicate the port is running at 10Gbps or 2.5GMbps or 1GMbps speed and successfully established
		Blink	To indicate that the router is actively sending or receiving data over that port.

Rear View

XVR-800 & ZT-800 & CSG-800

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

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 7/8/10/11, macOS 10.12 or later, Linux Kernel 2.6.18 or later, or other modern operating system are compatible with TCP/IP Protocols.

3. Recommended web browsers: Google Chrome, Microsoft Edge or Mozilla Firefox.

3.2 Setting TCP/IP on your PC

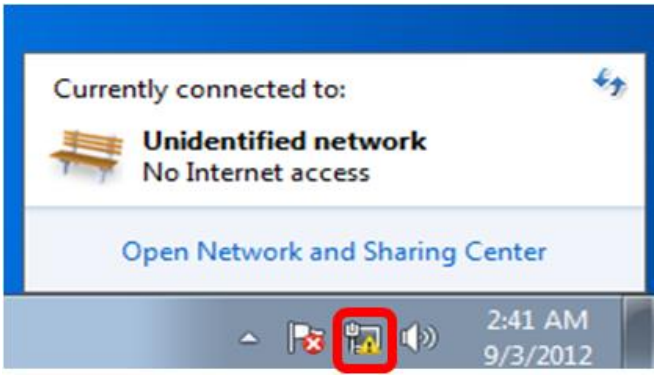
The default IP address of the VPN router is 192.168.1.1, and the DHCP Server is on. Please set the IP address of the connected PC as DHCP client, and the PC will get IP address automatically from the VPN router.

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

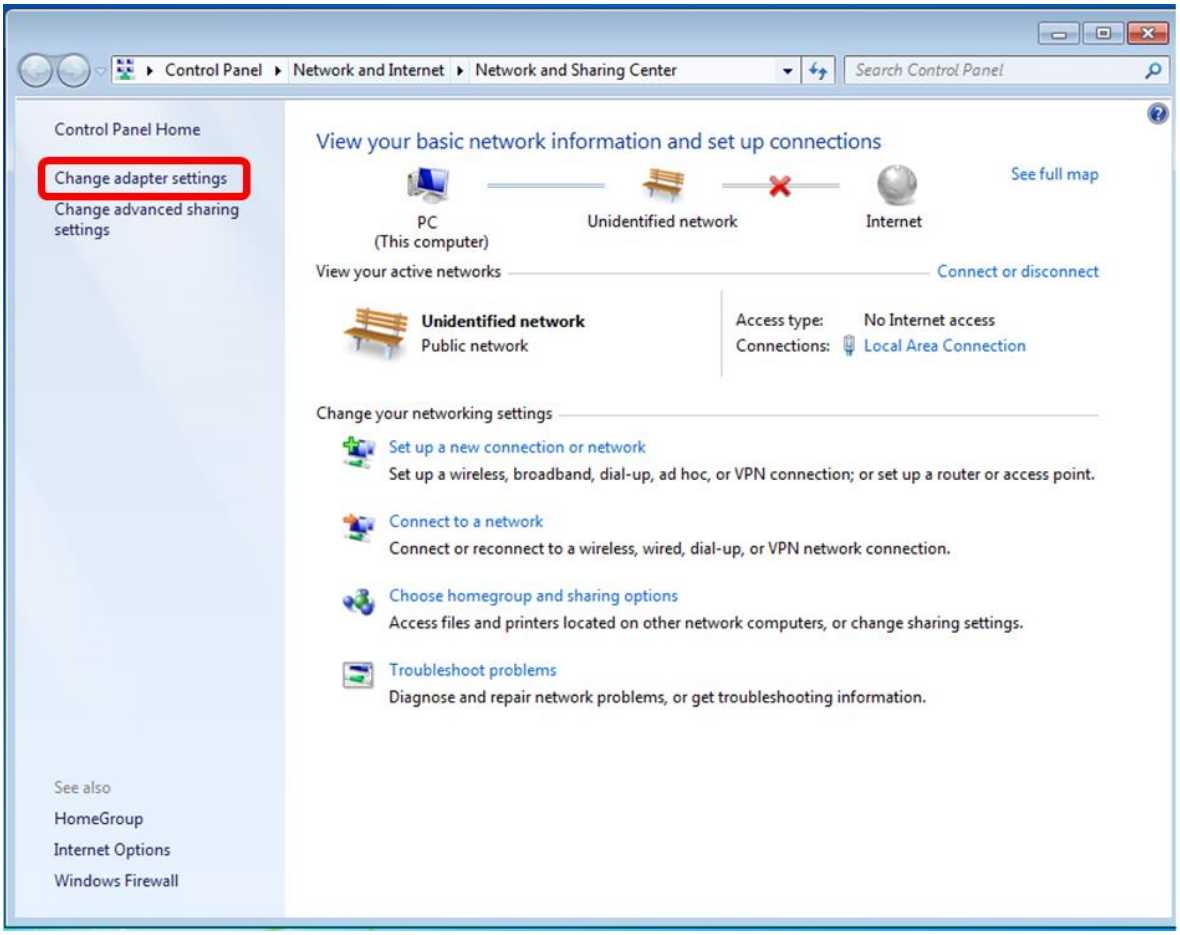
Windows 7/8

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

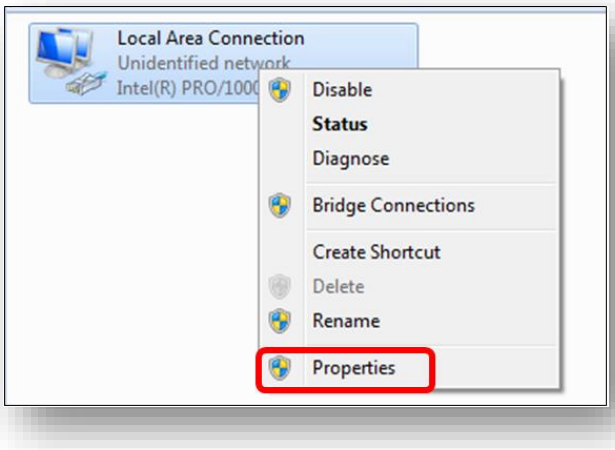
1. Click on the network icon from the right side of the taskbar and then click on “Open Network and Sharing Center”.



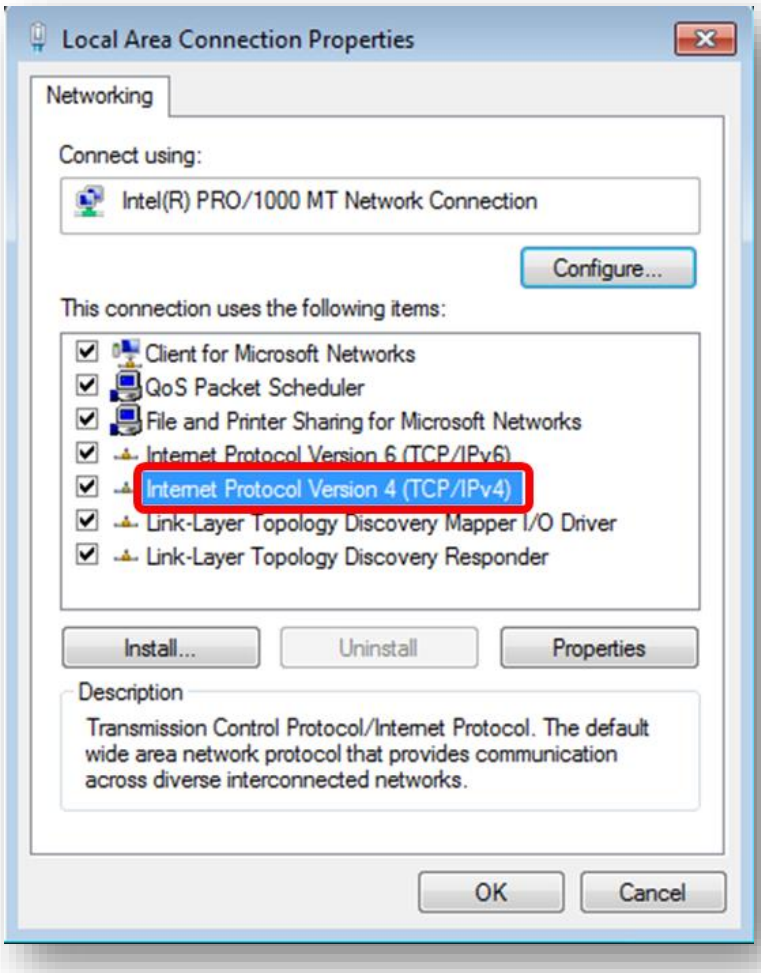
2. Click "**Change adapter settings**".



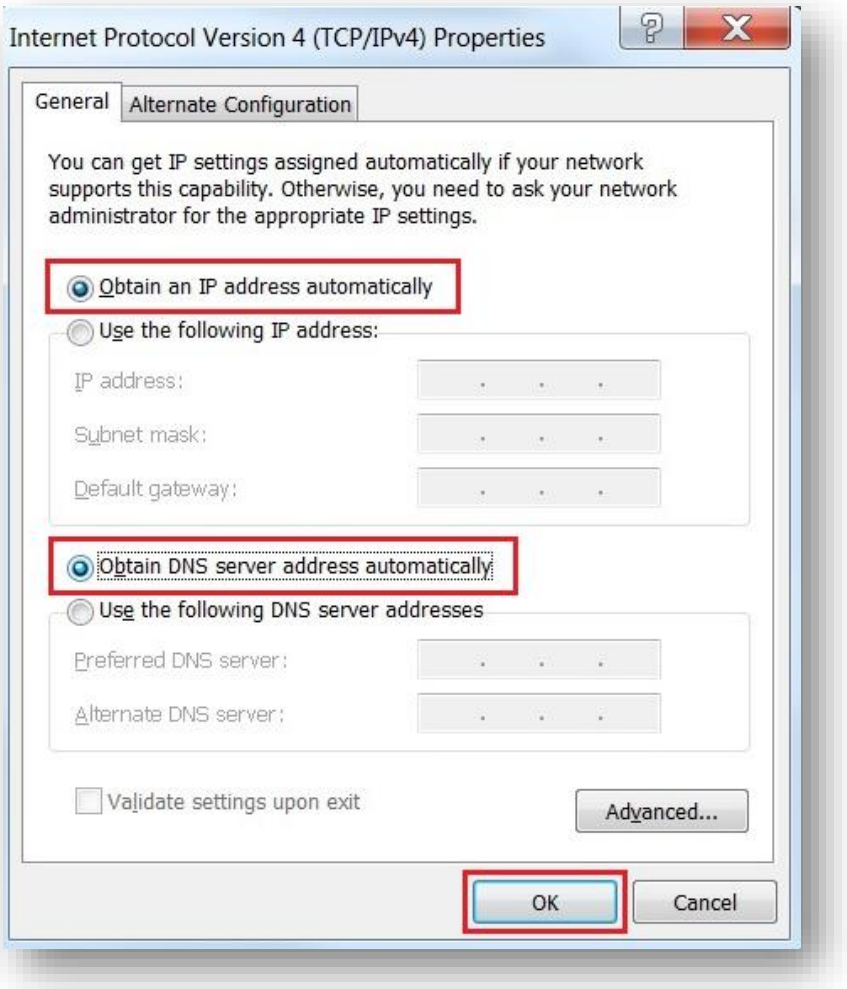
3. Right-click on the Local Area Connection and select Properties.



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



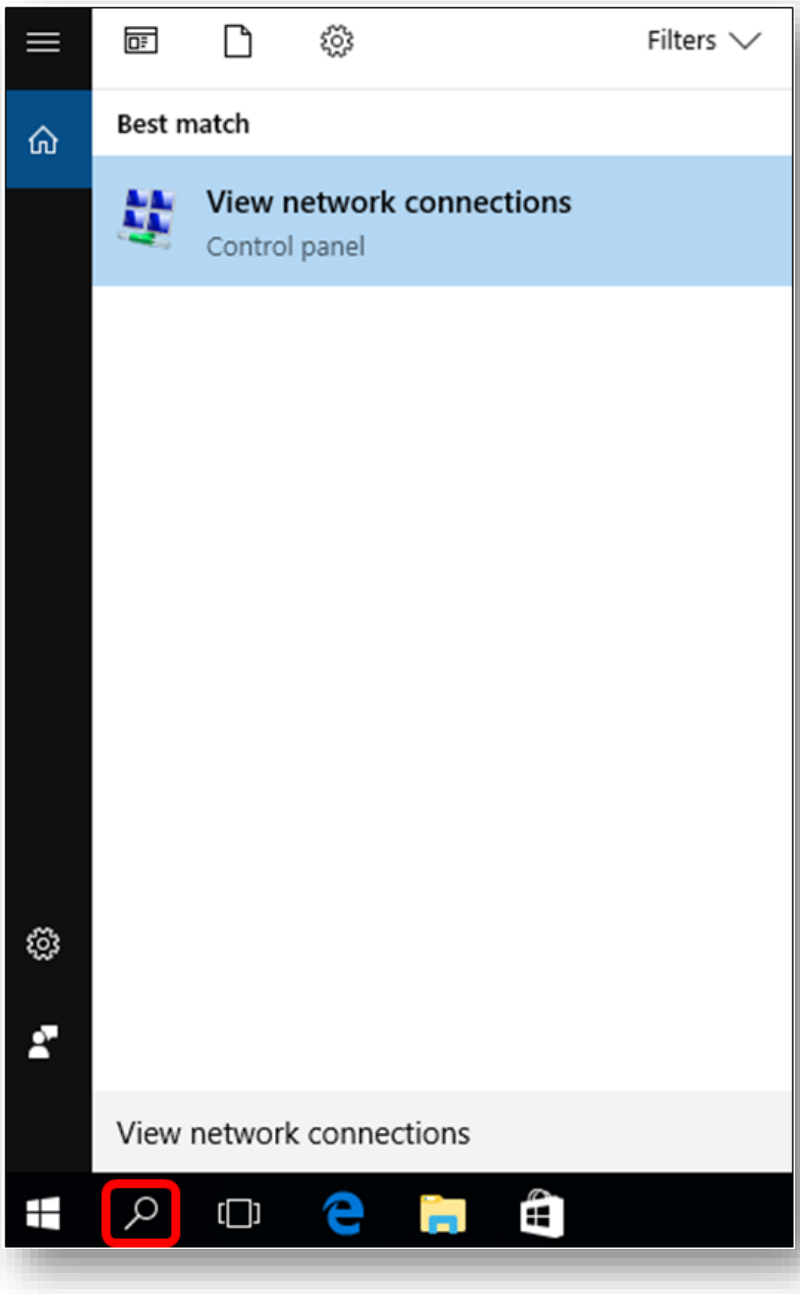
5. Select "**Use the following IP address**" and "**Obtain DNS server address automatically**", and then click the "**OK**" button.



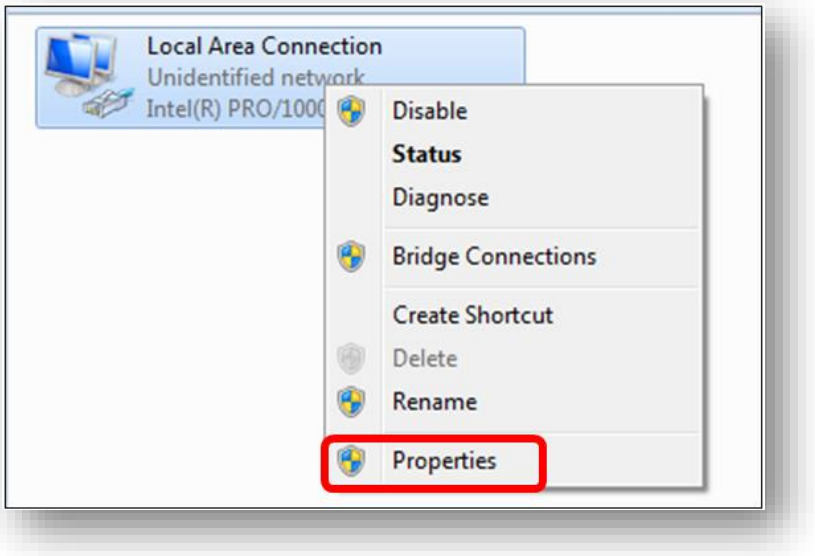
Windows 10/11

If you are using Windows 10/11, please refer to the following:

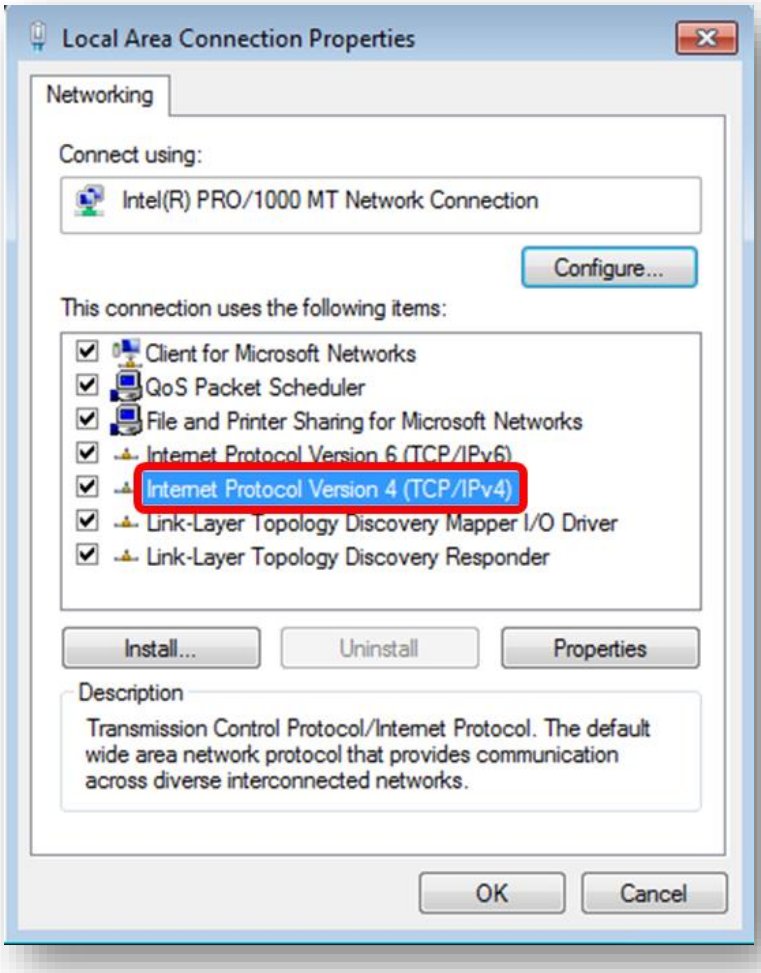
1. In the search box on the taskbar, type “View network connections”, and then select View network connections at the top of the list.



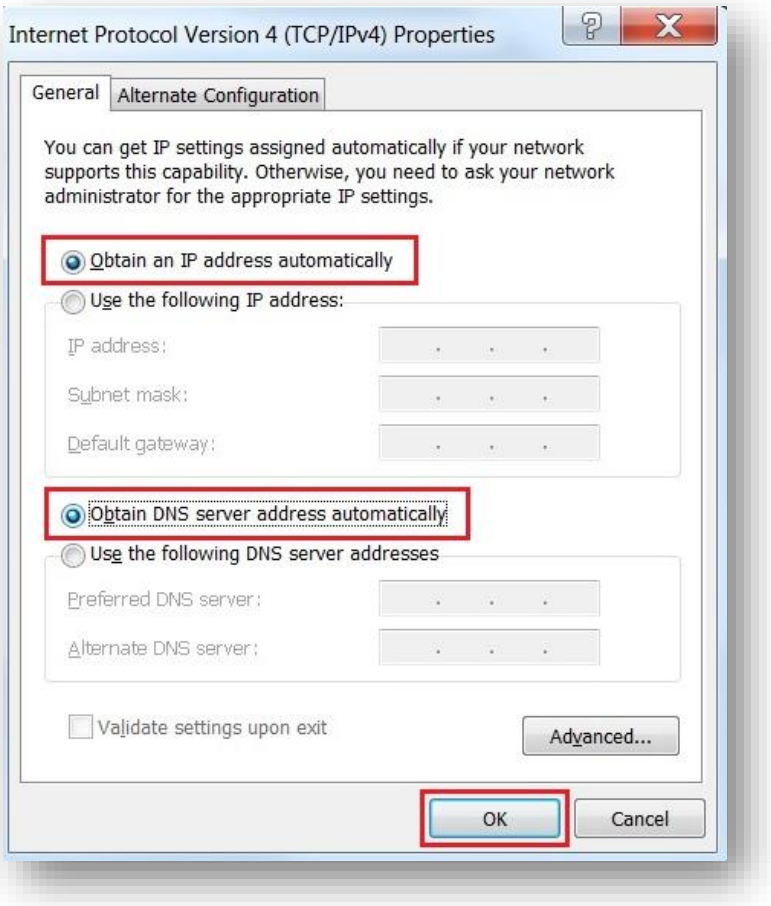
2. Right-click on the Local Area Connection and select Properties.



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



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



3.3 Planet Smart Discovery Utility

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

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

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

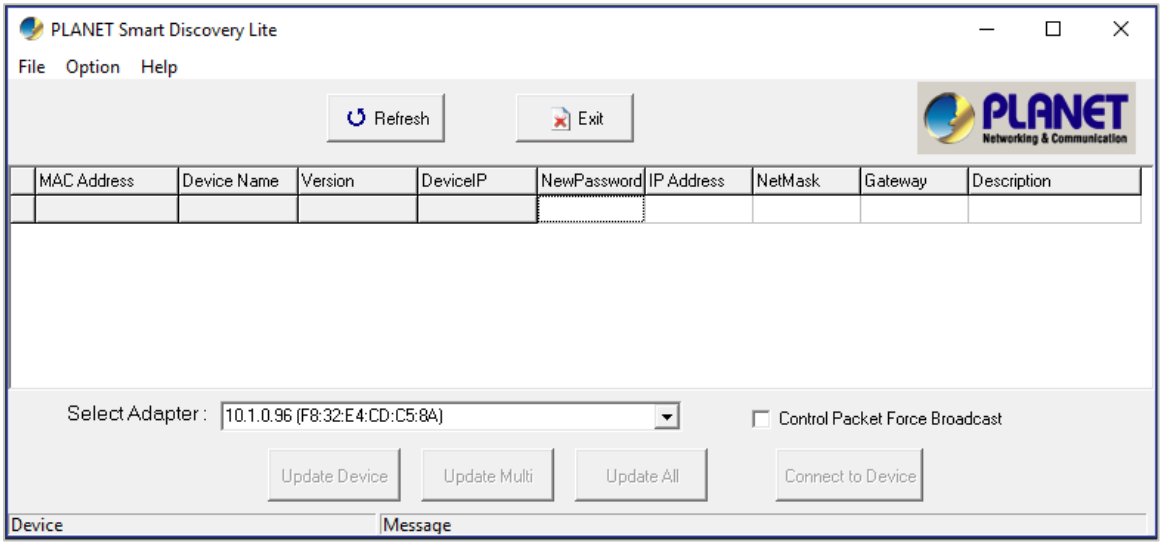


Figure 3-1-6: Planet Smart Discovery Utility Screen

Note

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

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

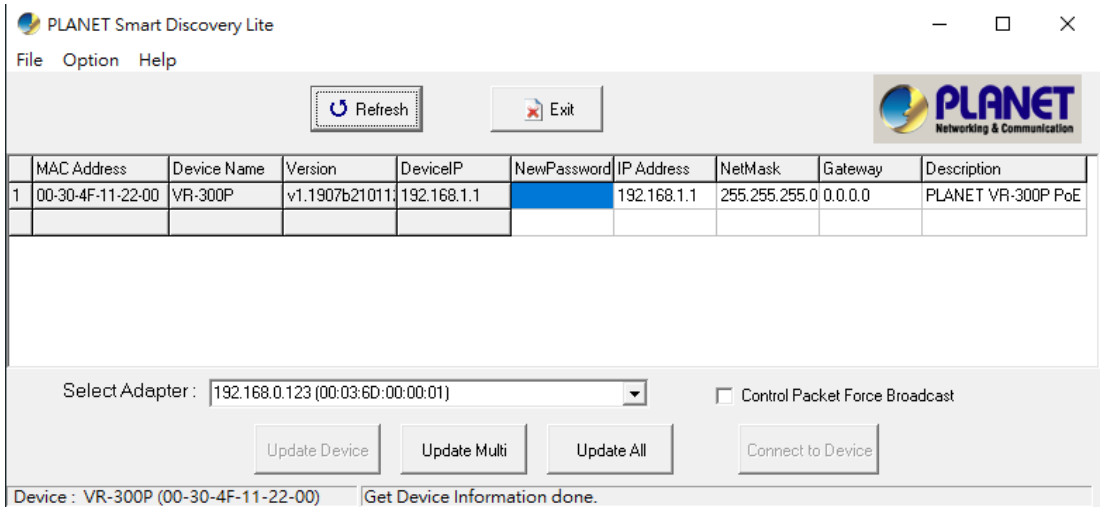


Figure 3-1-7: Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.

2. After setup is completed, press the "**Update Device**", "**Update Multi**" or "**Update All**" button to take effect. The functions of the 3 buttons above are shown below:
   - **Update Device**: use current setting on one single device.
   - **Update Multi:** use current setting on choose multi-devices.
   - **Update All:** use current setting on whole devices in the list.

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

3. To click the "**Control Packet Force Broadcast**" function, it allows you to assign a new setting value to the device under a different IP subnet address.

4. Press the "**Connect to Device**" button and the Web login screen appears.

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

Chapter 4. Web-based Management

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

4.1 Introduction

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

4.2 Logging in to the VPN Router

Refer to the steps below to configure the VPN router:

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

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

The following steps is based on the firmware version before **August of 2024**.

Default IP address: **192.168.1.1**
Default user name: **admin**
Default password: **admin**
Default SSID (2.4G): **PLANET_2.4G** (Wireless model only)
Default SSID (5G): **PLANET_5G** (Wireless model only)

Note

The SSIDs are designed for wireless models: XVR-800BE, ZT-800BE, CSG-800BE, XVR-800BE-NR

B. The browser prompts you for the login credentials.

Note

The following step is based on the firmware version of **August of 2024** or after.

Default IP address: 192.168.1.1
Default user name: admin
Default password: **cg + the last 6 characters of the MAC ID in lowercase**

When Login dialog box appears, please enter the default user name and password. Refer to Figure 4.2-1 to determine your initial login password. Default IP address is 192.168.1.1, default username is admin and default password is cg + the last 6 characters of the MAC ID in lowercase.
Find the MAC ID on your device label. The default password is "cg" followed by the last six lowercase characters of the MAC ID.

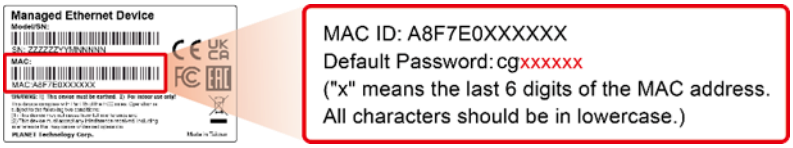


Figure 4-1: MAC ID Label

Note

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

4.3 Main Web Page

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

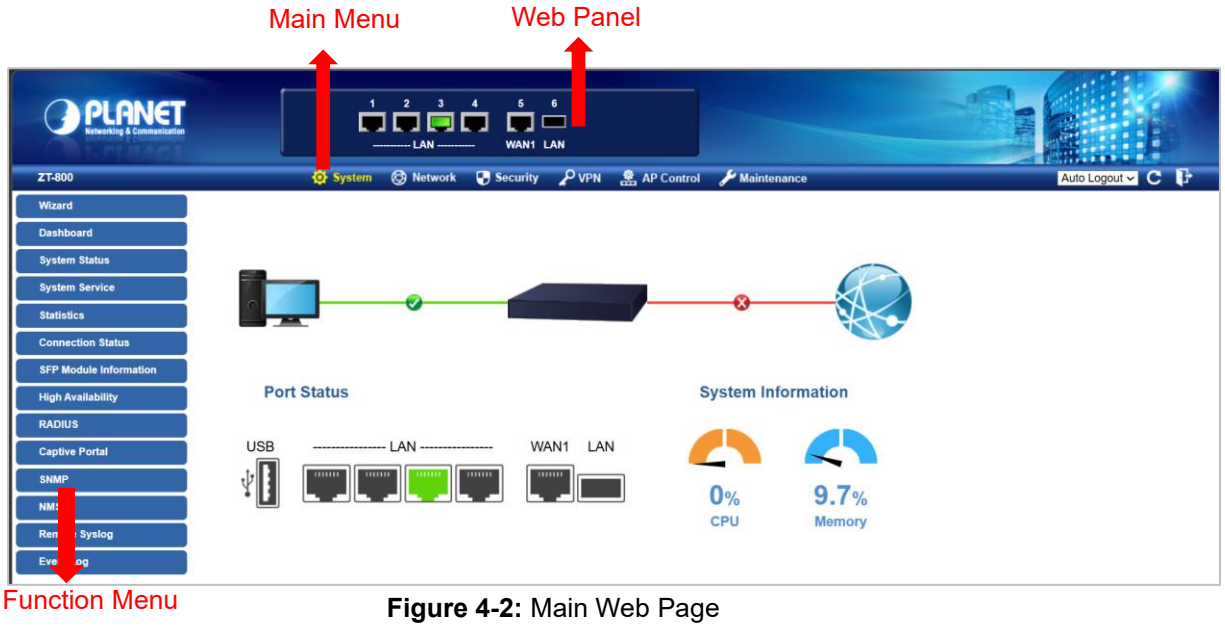


Figure 4-2: Main Web Page

■ Web Panel

The web panel displays an image of the device's ports as shown in Figure 4-3.

Figure 4-3: Web Panel

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

Main Menu

The main menu displays the product name, function menu, and main information in the center. Via the Web management, the administrator can set up the device by selecting the functions listed in the function menu and button as shown in Figures 4-4 and 4-5.

Figure 4-4: Function Menu

Object	Description
System	Provides system information of the router.
Network	Provides WAN, LAN and network configuration of the router.
Cellular	Provides cellular configuration of the router (XVR-800BE-NR Only).
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.
PoE	Provides PoE Management configuration of industrial wall-mount Gigabit router (XVR-800P only).
Wireless	Provides wireless configuration of the router.
Maintenance	Provides firmware upgrade and setting of the file restore/backup configuration of the router.

Figure 4-5: Function Button

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

4.4 System

Use the System menu items to display and configure basic administrative details of the router. The System menu shown in Figure 4-6 provides the following features to configure and monitor system.

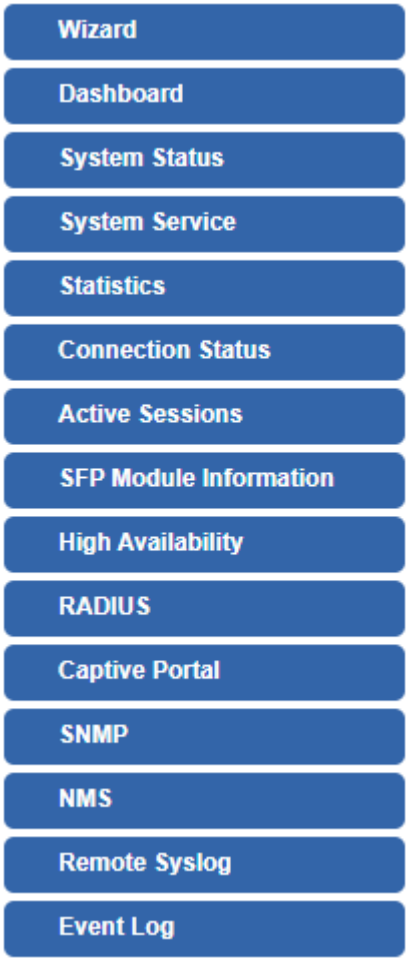


Figure 4-6: System Menu

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
Active Sessions	Display real-time active session trends and detailed session information, including protocol, source, destination, and traffic statistics.
SFP Module Information	Display the physical or operational status of an SFP module via the SFP Module Information page
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 4-7.

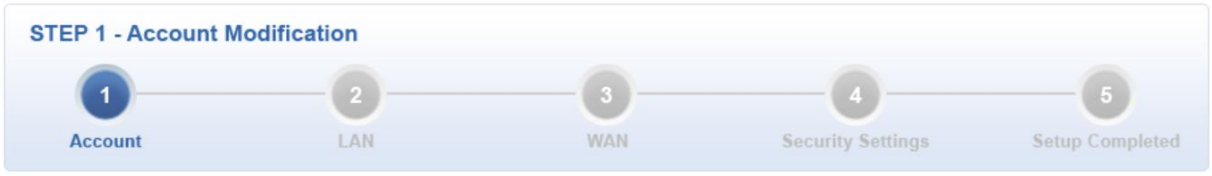
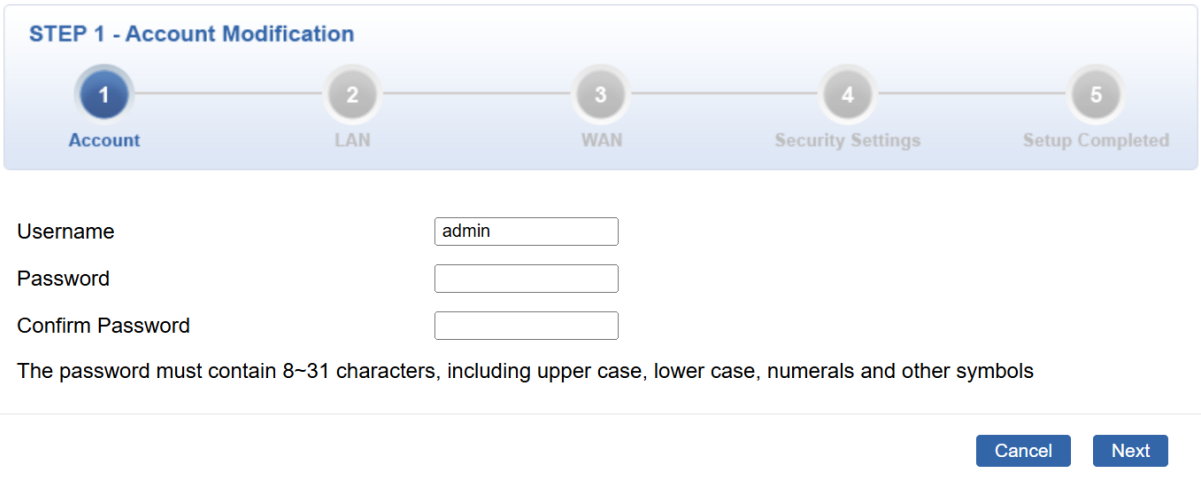


Figure 4-7: Setup Wizard

Step 1: Account Modification

Set up the Username and Password for the Account Modification



Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in Figure 4-8.

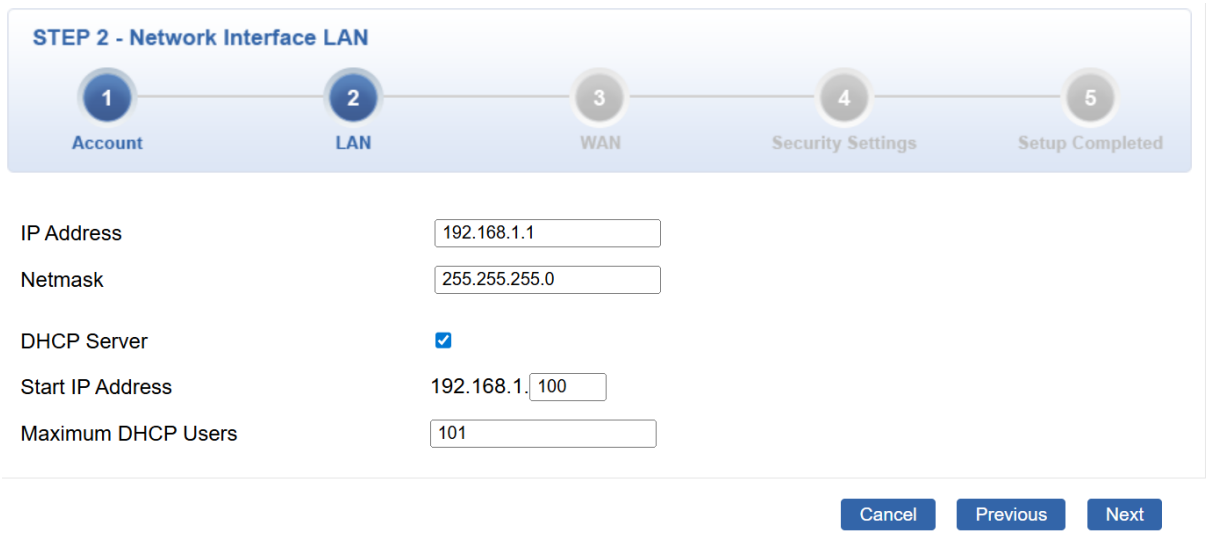


Figure 4-8: Setup Wizard – LAN Configuration

Object	Description
IP Address	Enter the IP address of your router. The default is 192.168.1.1.
Subnet Mask	An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
DHCP Server	By default, the DHCP Server is enabled. If user needs to disable the function, please uncheck the box.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the router.
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the router will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
Next	Press this button to the next step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Step 3: WAN Interface

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

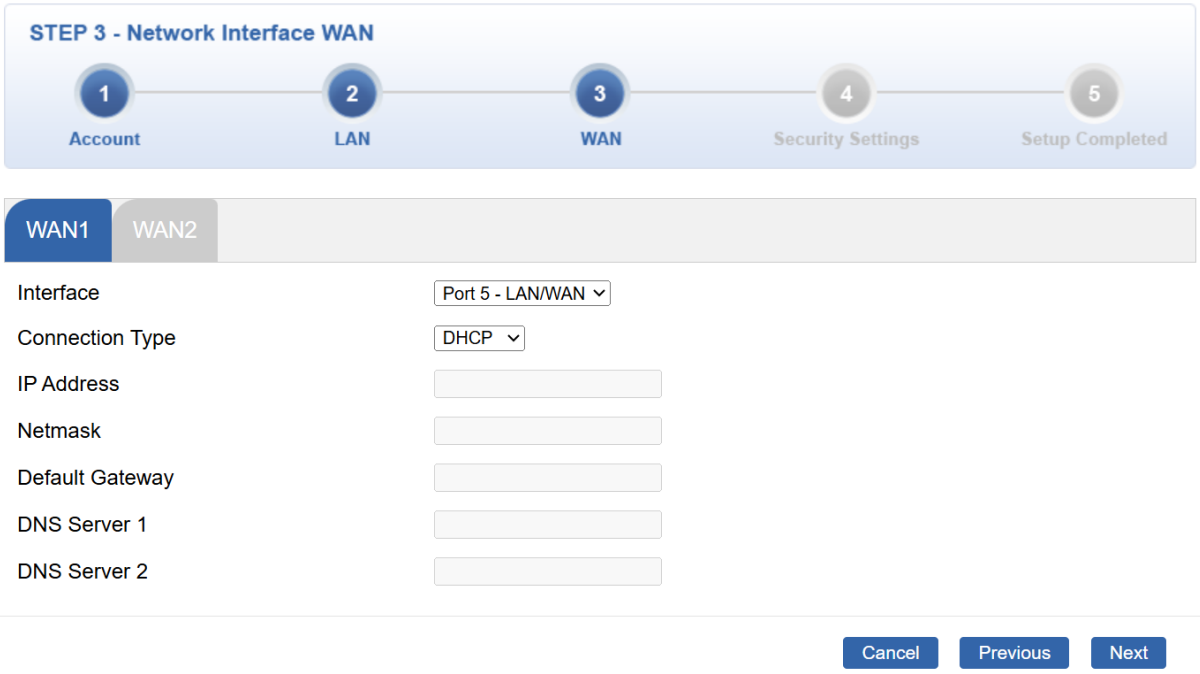


Figure 4-9: Setup Wizard – WAN 1 Configuration

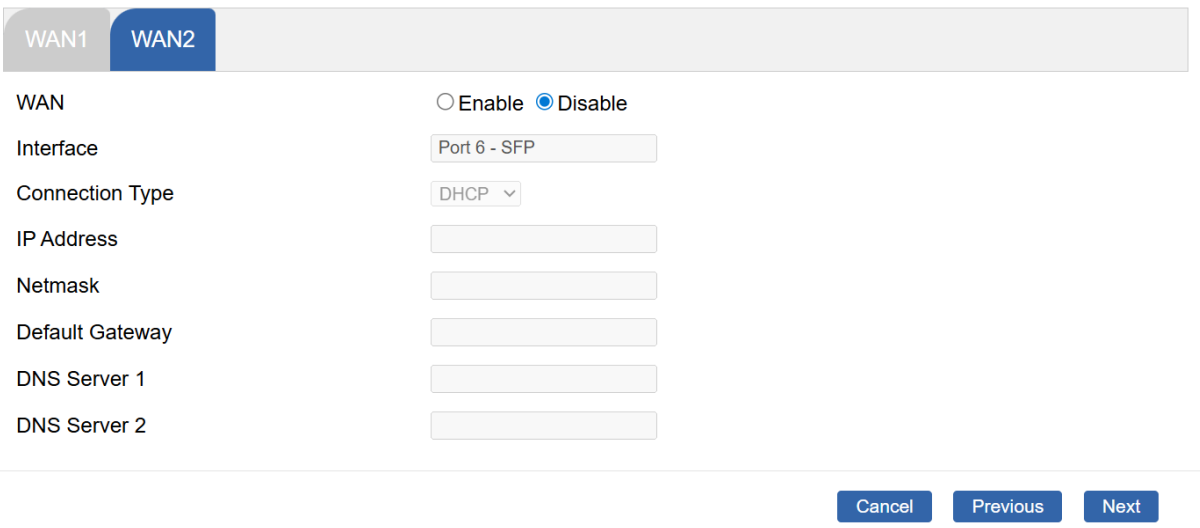


Figure 4-10: Setup Wizard – WAN 2 Configurations

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 4-11.

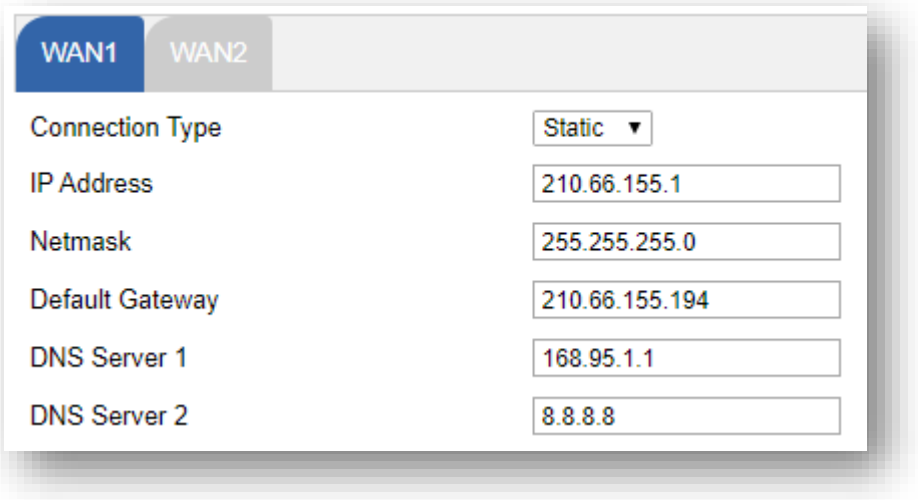


Figure 4-11: WAN Interface Setup – Static IP Setup

Object	Description
IP Address	Enter the IP address assigned by your ISP.
Netmask	Enter the Netmask assigned by your ISP.
Default Gateway	Enter the Gateway assigned by your ISP.
DNS Server	The DNS server information will be supplied by your ISP.
Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Mode 2 -- DHCP Client

Select DHCP Client to obtain IP Address information automatically from your ISP. The setup is shown in Figure 4-12.

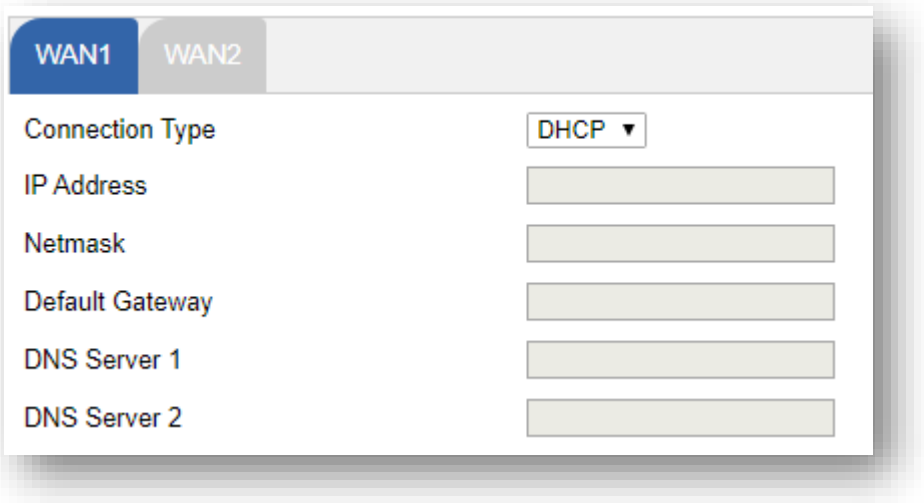


Figure 4-12: WAN Interface Setup – DHCP Setup

Step 4: Security Setting

Set up the Security Settings as shown in below..

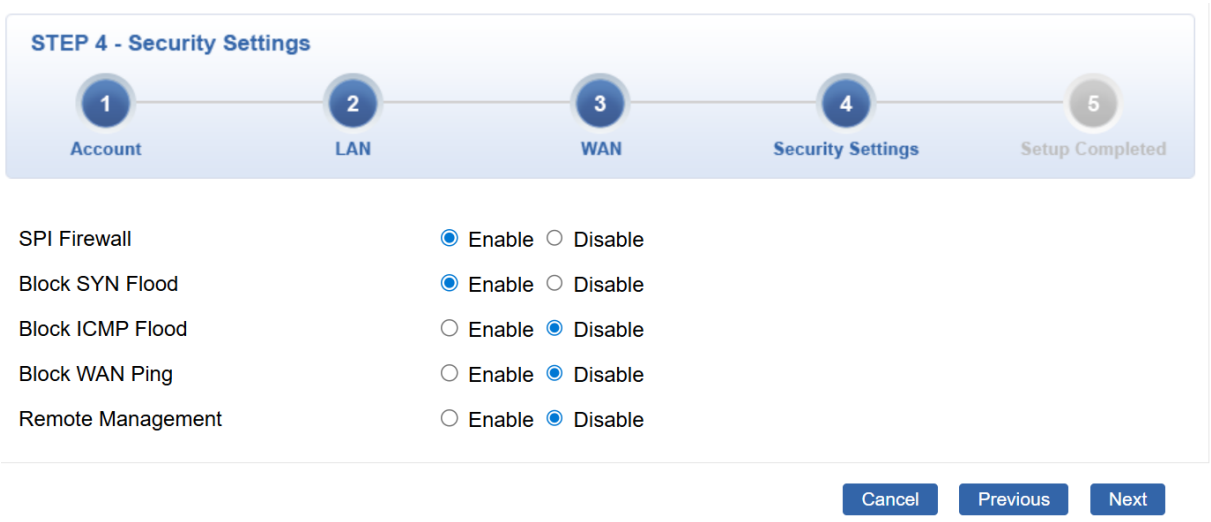


Figure 4-13: Setup Wizard – Security Setting

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. The default configuration is enabled.
Block SYN Flood	SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on. The default configuration is enabled.
Block ICMP Flood	ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack. The default configuration is disabled.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the cellular gateway from the Internet network. The default configuration is disabled.

Step 5: Setup Completed

The page will show the summary of LAN, WAN and Security settings as shown below.

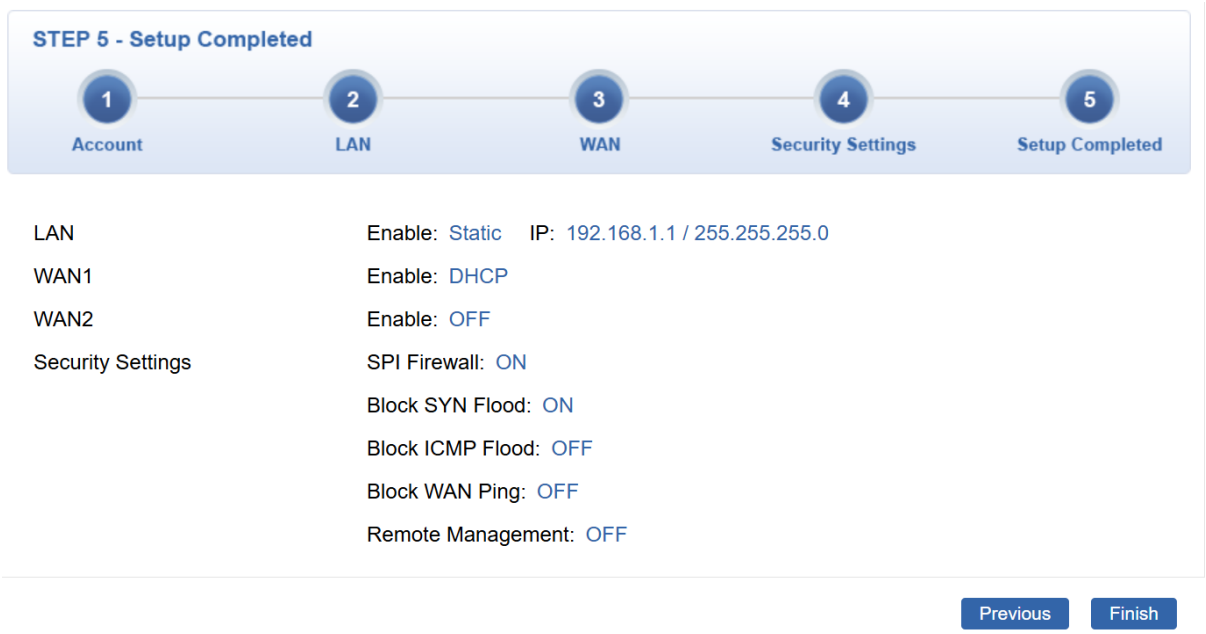


Figure 4-14: Setup Wizard – Setup Completed

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 4-15.

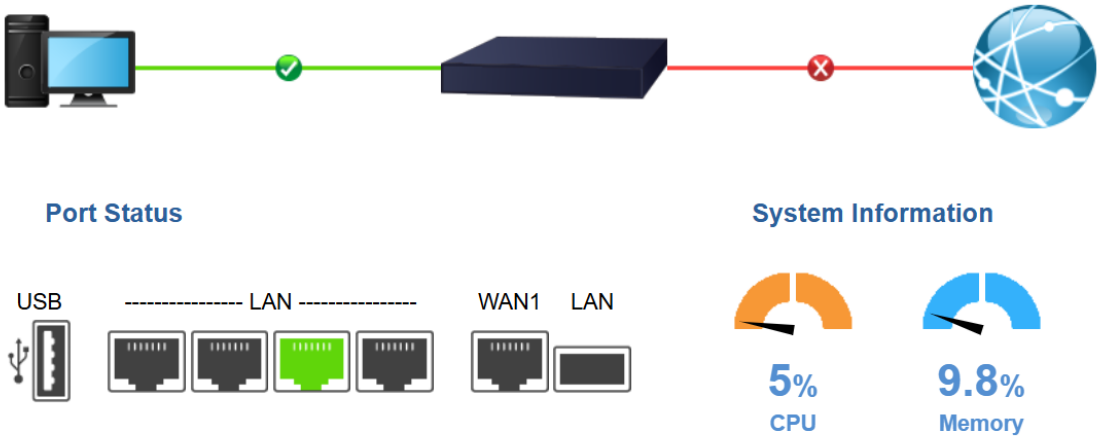


Figure 4-15: Dashboard

WAN/LAN Connection Status

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

Port Status

Object	Description
	Ethernet port is in use.
	Ethernet port is not in use.
	USB port is in use.
	USB port is not in use.
	SFP port is in use.
	SFP port is not in use.

System Information

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

4.4.3 System Status

This page displays system information as shown in Figure 4-16.

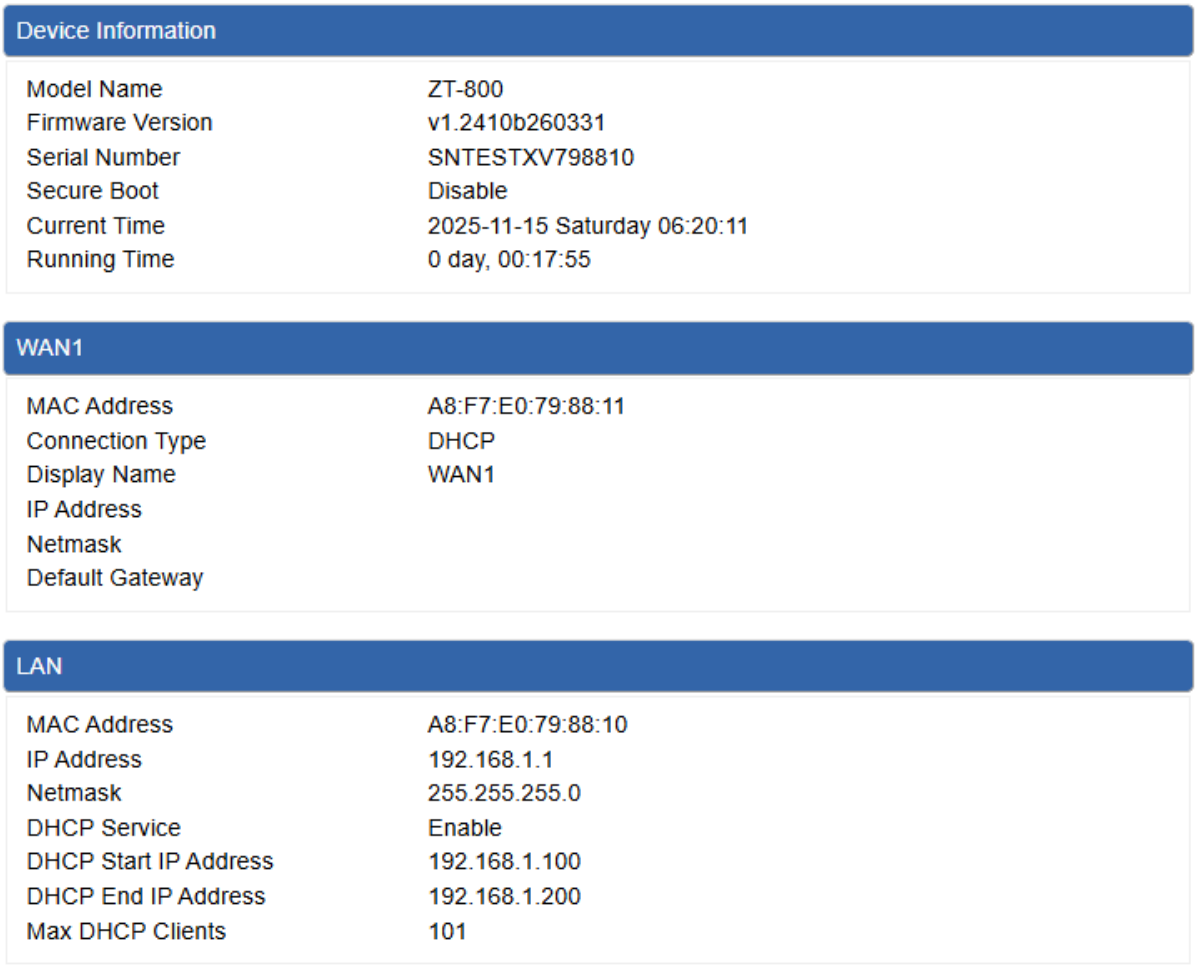


Figure 4-16: Status

4.4.4 System Service

This page displays system service information as shown below.

Service

#	State	Service	Detail
1	Enabled	DHCP Service	DHCP Table: 0
2	Disabled	DDNS Service	Not enabled
3	Disabled	SNMP Service	
4	Disabled	Quality of Service	
5	Disabled	High Availability	
6	Disabled	RADIUS Service	
7	Disabled	Captive Portal	

Secured Service

#	State	Service	Detail
1	Enabled	Cybersecurity	TLS 1.2, TLS 1.3
2	Enabled	NAT Function	NAT is enabled.
3	Enabled	SPI Firewall	
4	Disabled	MAC Filtering	(Active / Maximum Entries) 0 / 32
5	Disabled	IP Filtering	(Active / Maximum Entries) 0 / 32
6	Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32
7	Disabled	IPSec VPN Server	(Active / Maximum Tunnels) 0 / 16
8	Disabled	GRE	(Active / Maximum Tunnels) 0 / 5
9	Disabled	PPTP	(Active / Maximum Tunnels) 0 / 100
10	Disabled	SSL VPN	(Active / Maximum Tunnels) 0 / 100
11	Disabled	L2TP	(Active Tunnels) 0

Figure 4-17: System Service

4.4.5 Statistics

This page displays the number of packets that pass through the router on the WAN and LAN.

The statistics are shown in Figure 4-18.

Figure 4-18: Statistics

4.4.6 Connection Status

The page shows the DHCP Table and ARP Table. The status is shown in Figure 4-19.

DHCP Table

Name	IP Address	MAC Address	Expiration Time

ARP Table

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

Figure 4-19: Connection Status

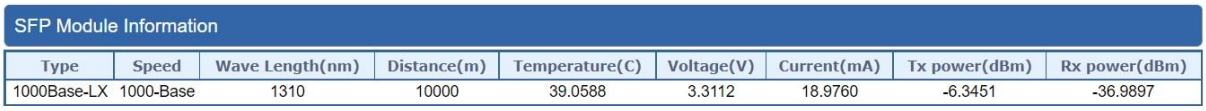
4.4.7 Active Sessions

The page displays the Session Trend and Session Table, providing real-time information about active TCP, UDP, and other network sessions. The status is shown in Figure 4-20.

Figure 4-20: Active Sessions

4.4.8 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 4-21.


SFP Module Information

Type	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 4-21: SFP Module Information

Object	Description
• **Type**	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)** **– SFP DDM Module Only**	Display the temperature of current SFP DDM module; the temperature value is gotten from the SFP DDM module.
• **Voltage (V)** **– SFP DDM Module Only**	Display the voltage of current SFP DDM module; the voltage value is gotten from the SFP DDM module.
• **Current (mA)** **– SFP DDM Module Only**	Display the ampere of current SFP DDM module; the ampere value is gotten from the SFP DDM module.
• **TX power (dBm)** **– SFP DDM Module Only**	Display the TX power of current SFP DDM module; the TX power value is gotten from the SFP DDM module.
• **RX power (dBm)** **– SFP DDM Module Only**	Display the RX power of current SFP DDM module; the RX power value is gotten from the SFP DDM module.

4.4.9 High Availability

High Availability (HA) is a system redundancy where two routers of XVR-800 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 shows the High Availability configuration. The High Availability page is shown in Figure 4-22.

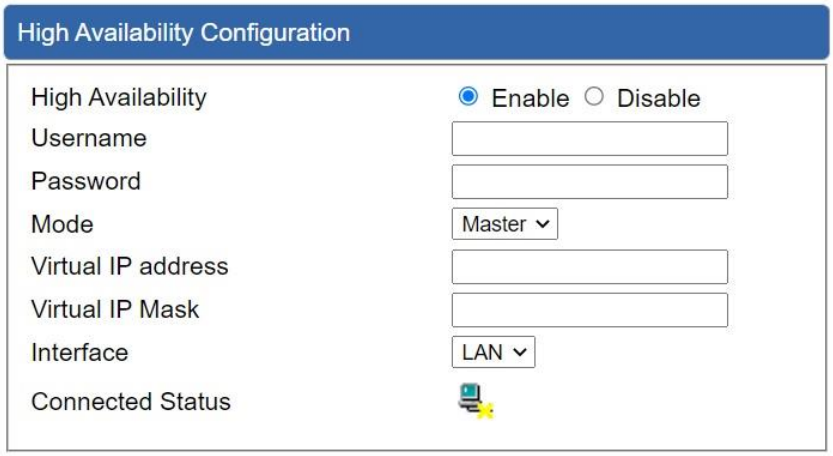


Figure 4-22: High Availability

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

4.4.10 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 4-23.

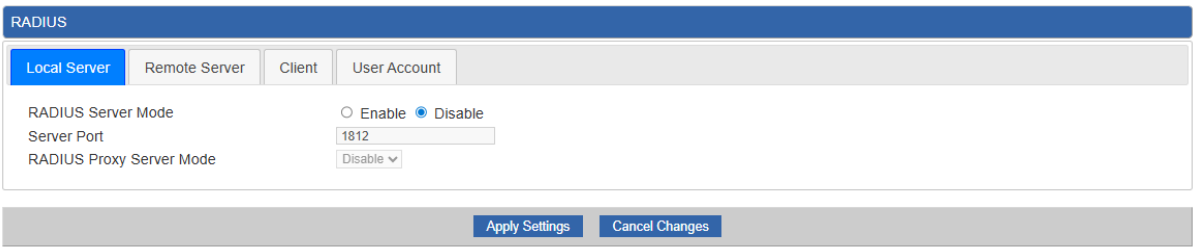


Figure 4-23: RADIUS Server

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

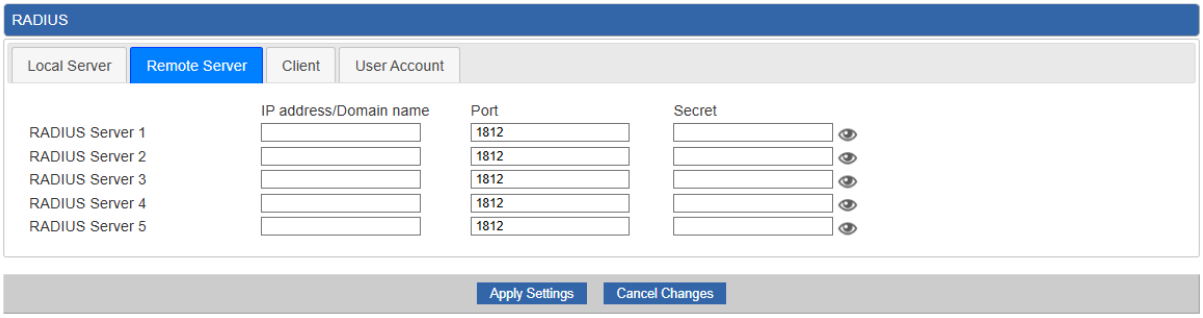


Figure 4-24: Remote Server

Object	Description
RADIUS Server 1–5	Configure up to five RADIUS servers by specifying the IP address/domain, port (default 1812), and shared secret for authentication redundancy and load distribution.
IP Address / Domain Name	Specify the destination RADIUS server IP address or domain name.
Server Port	UDP port number used for RADIUS authentication (default: 1812)
Secret	Shared secret key used for authentication between the device and the RADIUS server.

The RADIUS client page is shown in Figure 4-25.

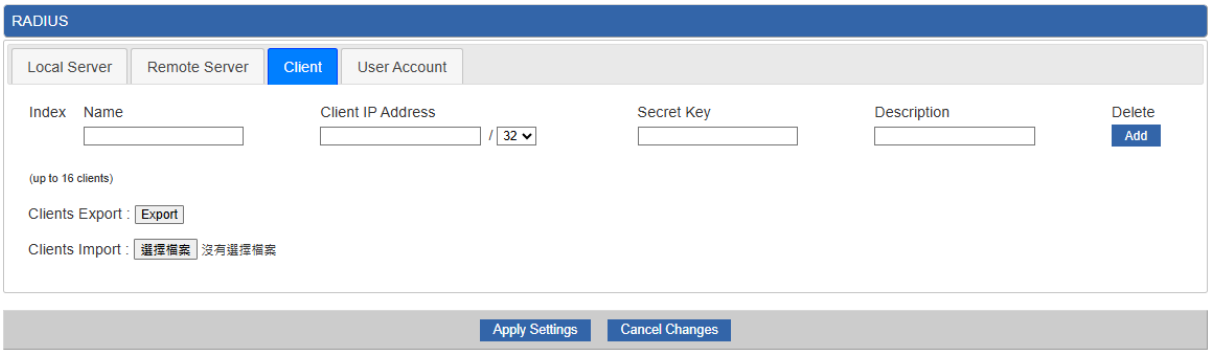


Figure 4-25: RADIUS Client

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

4.4.11 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 4-26.

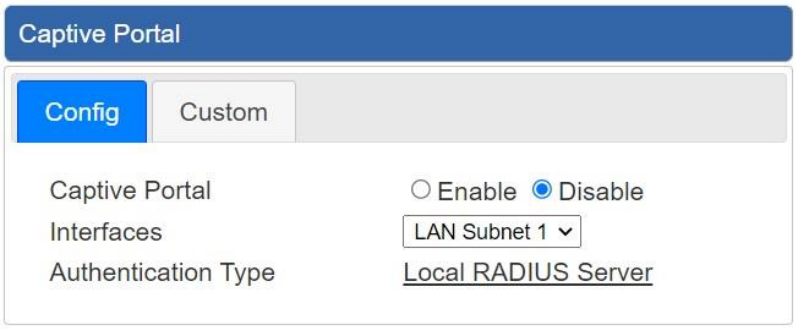


Figure 4-26: Captive portal

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

4.4.12 SNMP

This page provides SNMP setting of the router as shown in Figure 4-27.

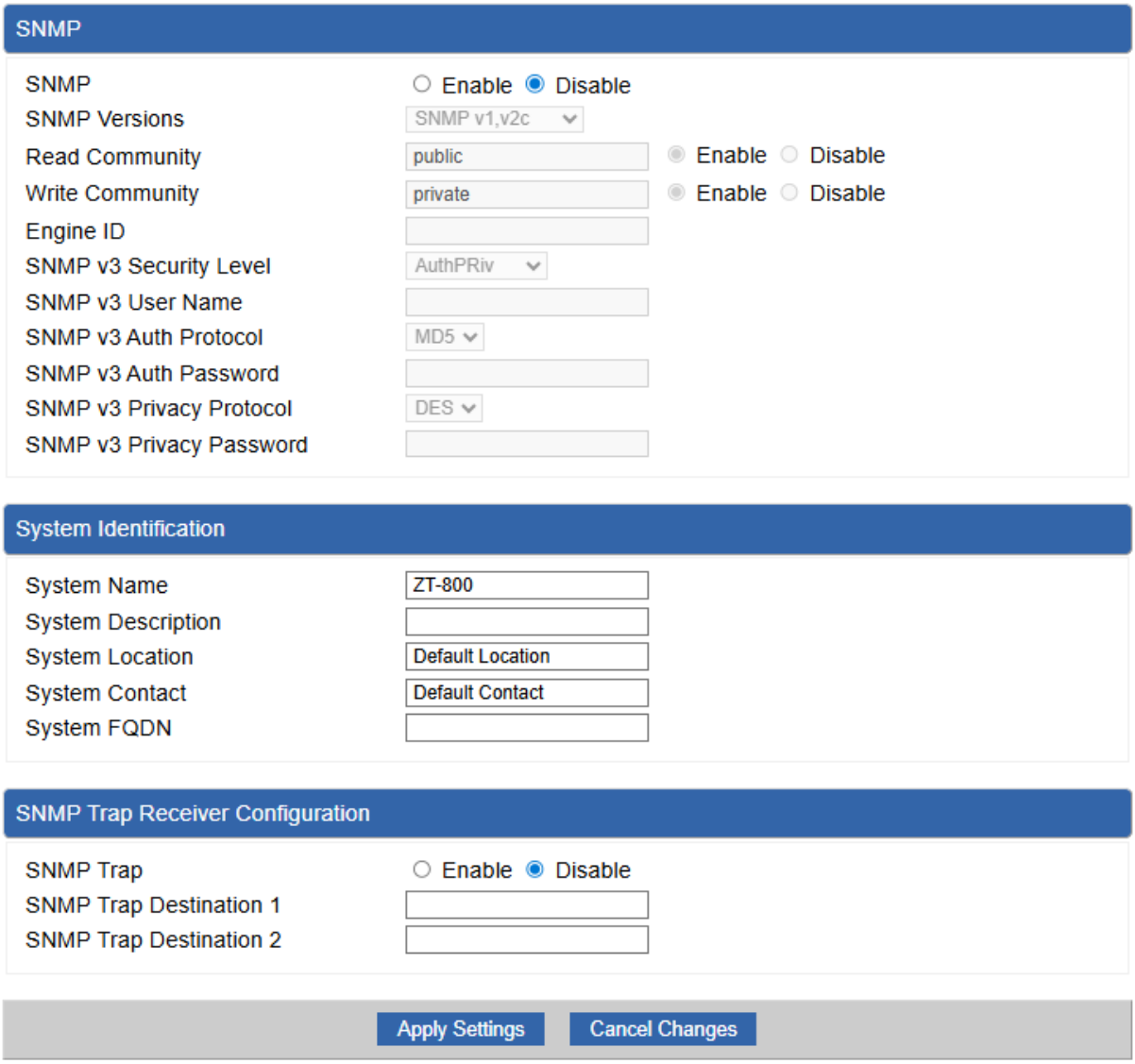


Figure 4-27: SNMP

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.

System FQDN	Specify the fully qualified domain name of the device.
SNMP Trap	Enable or disable SNMP trap notifications.
SNMP Trap Destination 1–2	Configure up to two trap receiver IP addresses for event notifications.
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.

4.4.13 NMS

The XVR-800 series can support both NMS controller and CloudNMS 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 CloudNMSis a free networking service just for PLANET products. This service provides simplified network monitoring and real-time network status. Working with PLANET CloudNMS app, user can easily check network status, device information, port and PoE status from Internet. Other services are not included.

NMS Configuration screen is shown in Figure 4-28.

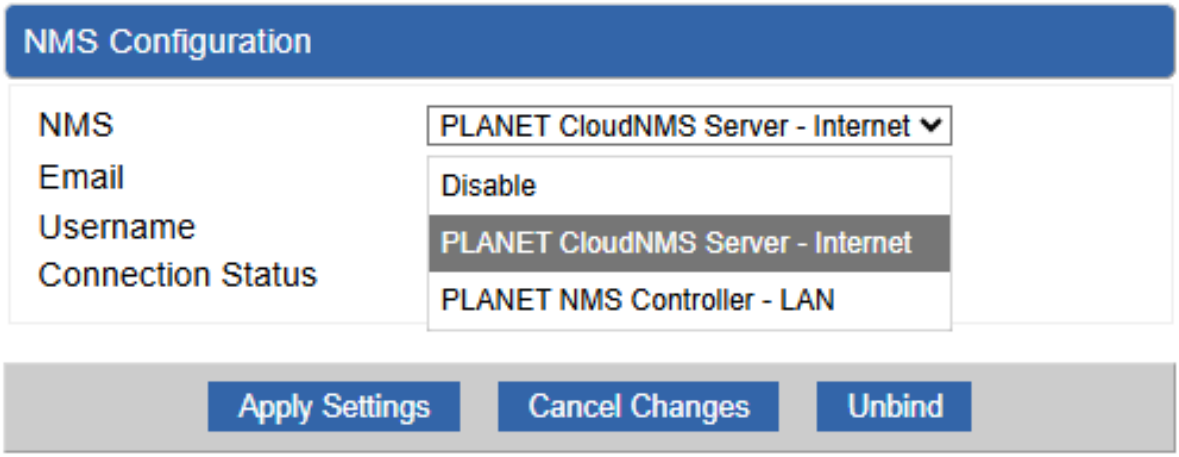


Figure 4-28 NMS Configuration Page

The NMS Controller – LAN Configuration screen is shown in Figure 4-29.

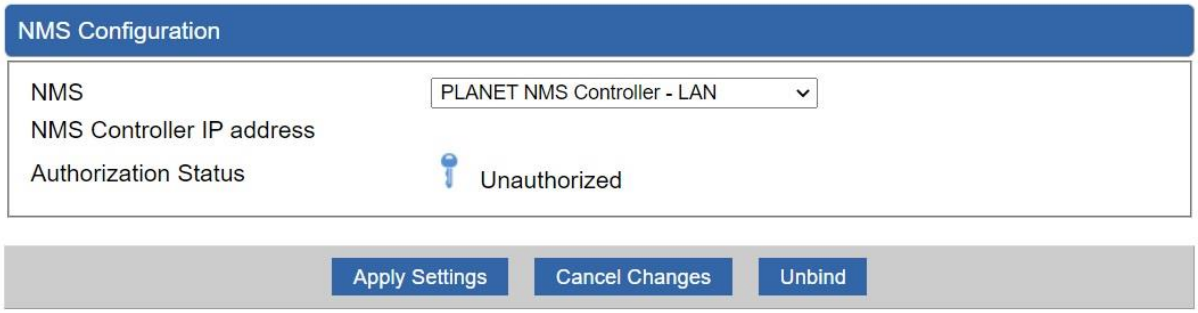


Figure 4-29 NMS Controller – LAN Configuration Page

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

The CloudNMS Server – Internet screens in Figure 4-30 appear.

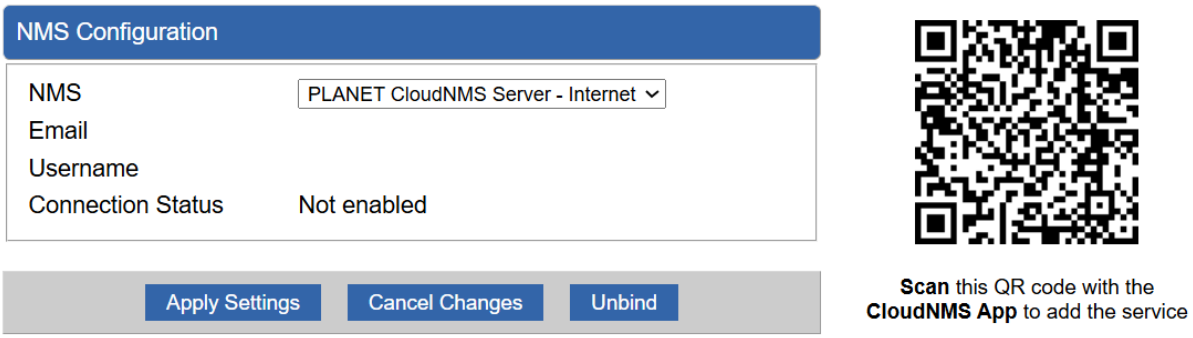


Figure 4-30 CloudNMS – Internet Configuration Page Screenshot

Object	Description
Remote NMS Enable	Enable NMS management
Email	The email registered on CloudNMS Server
Username	The username registered on CloudNMS Server
Connection Status	Indicate the status of connecting CloudNMS Server

4.4.14 Remote Syslog

This page provides remote syslog setting as shown below.

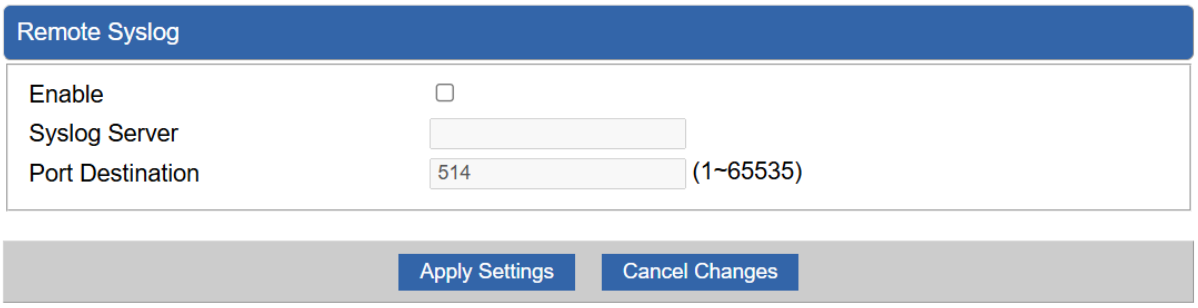


Figure 4-31: Connection Status

Object	Description
• **Enable**	Controls whether remote syslog is enabled
• **Syslog Server IP**	Indicates the IPv4 host address of syslog server
• **Port Destination**	Configure port for remote syslog

4.4.15 Event Log

This page provides Event Log as shown below.

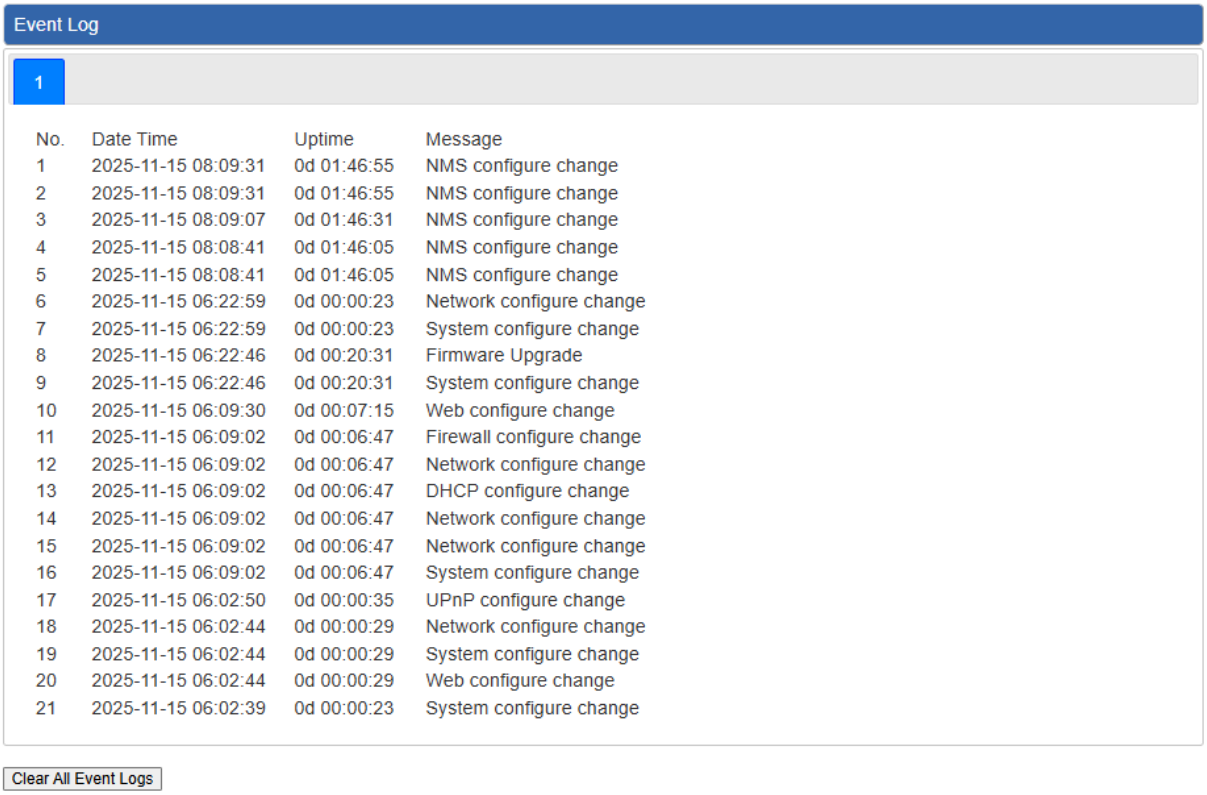


Figure 4-32: Event Log

4.5 Network

The Network function provides WAN, LAN and network configuration of the router as shown in Figure 4-33.

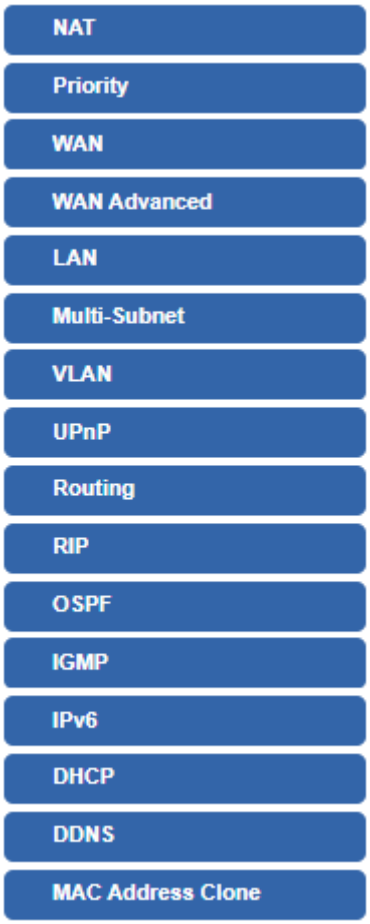


Figure 4-33: Network Menu

Object	Description
NAT	Allows setting NAT interface.
Priority	Allows setting WAN Priority interface.
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. 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 Clone	Allows setting WAN MAC Address Clone.

4.5.1 NAT

This page provides NAT setting as shown below.

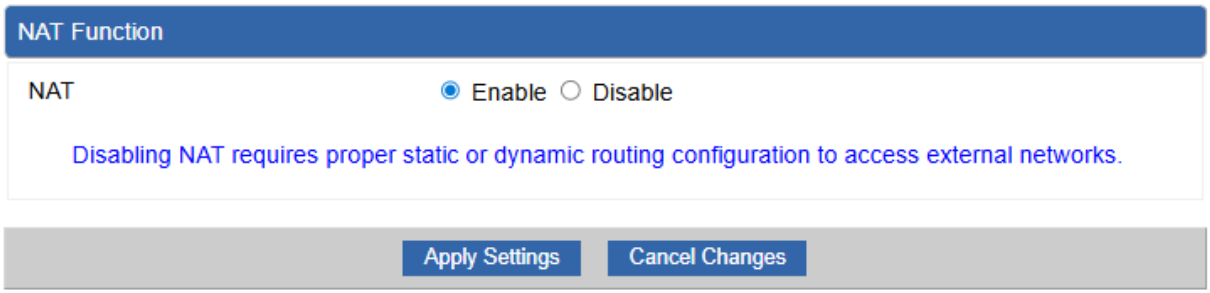


Figure 4-34: NAT

Object	Description
NAT	■ Enable or disable the Network Address Translation (NAT) function. Note: Disabling NAT requires proper static or dynamic routing configuration to ensure access to external networks.

4.5.2 Priority

This page provides WAN priority setting as shown below.

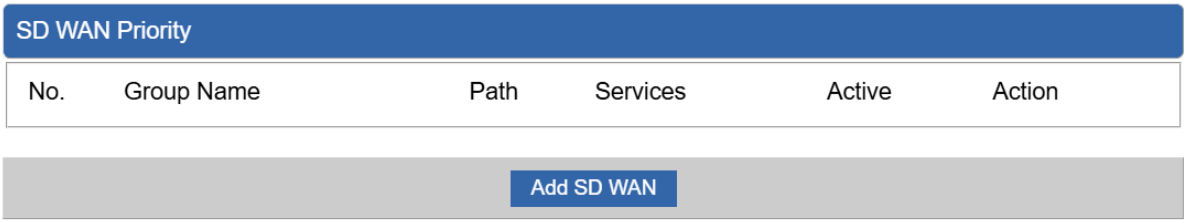


Figure 4-35: Priority

Object	Description
Active	■ Enable / Disable the Active
Group Name	■ Setting the Group Name.
Path	■ Setting the SD-WAN To / To SD-WAN
Service Port or Group	■ Setting the Service Port or Group Border Gateway Protocol

4.5.3 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 4-36. Here you may select the access method by clicking the item value of WAN access type.

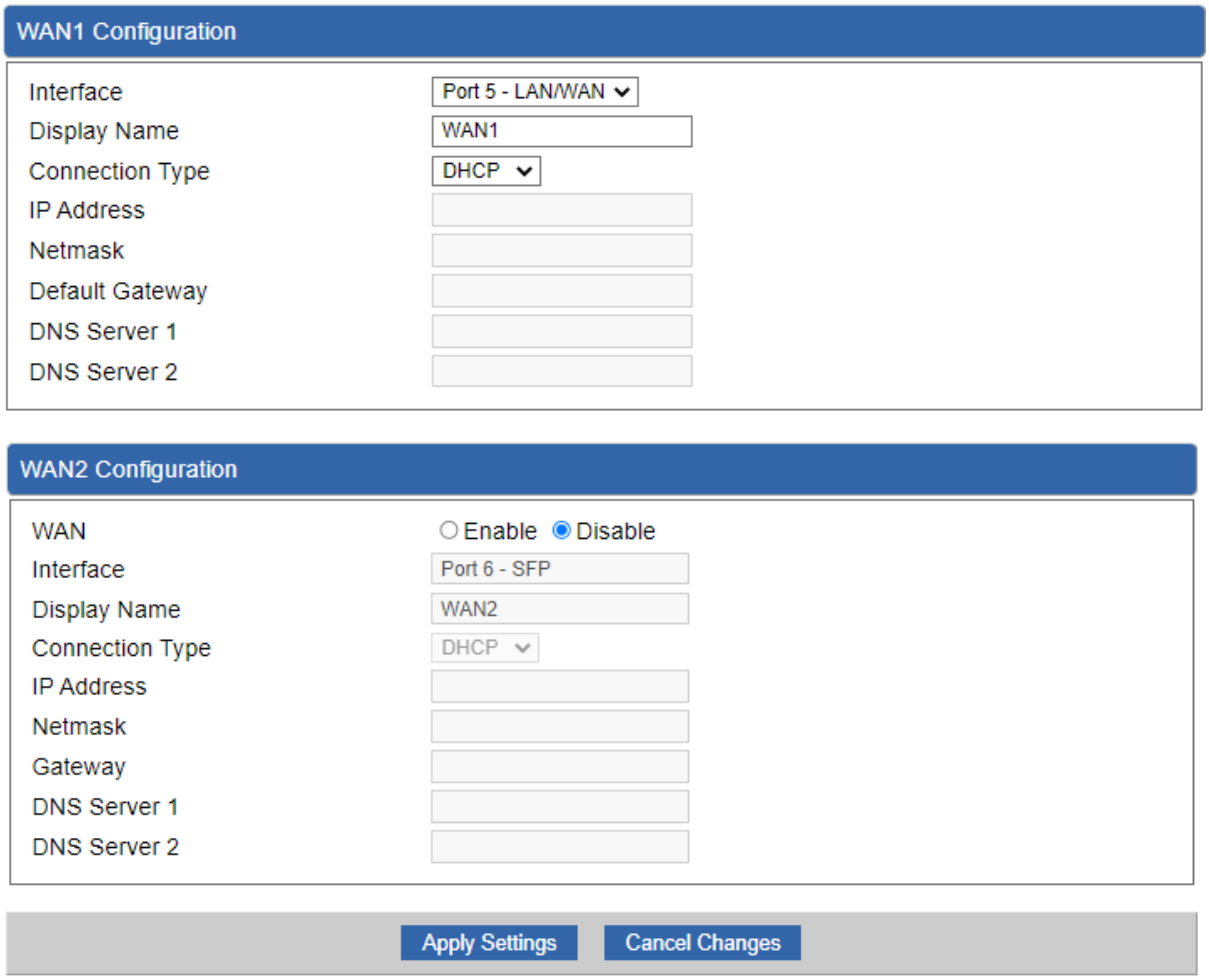


Figure 4-36: WAN

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

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

4.5.4 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 4-37. Here you may change the setting for Load Balance Weight, Detect Interval, Detect Link Up Threshold, etc.

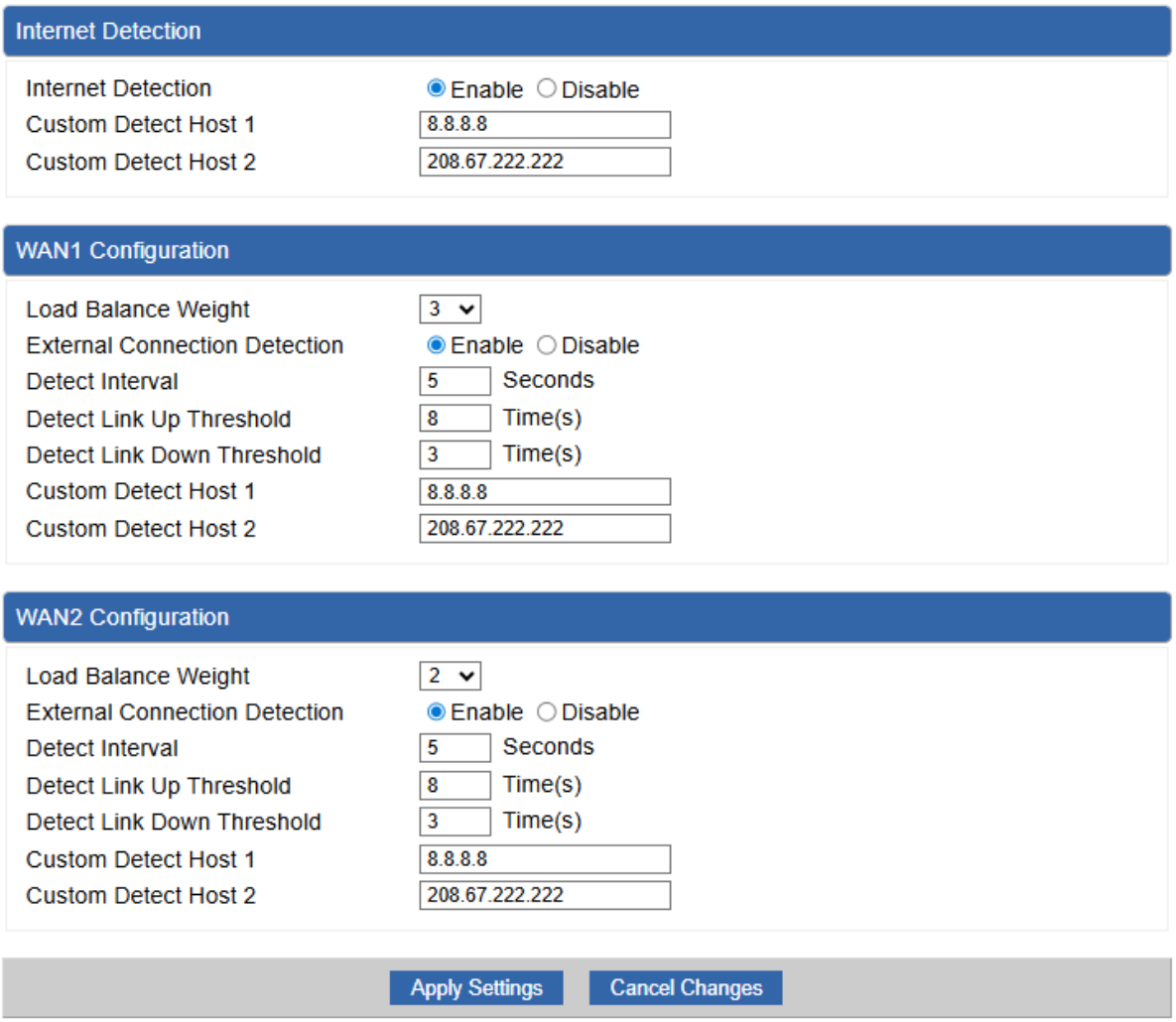


Figure 4-37: LAN Setup

Object	Description
Internet Detection	Enable or disable Internet connectivity detection.
Custom Detect Host 1–2	Specify IP addresses or domain names used to verify Internet connectivity.
Load Balance Weight	Load Balance Weight allows you to set a relative weight (from 1 - 10) for each WAN port.
External Connection Detection	Enable to detect the status of WAN connection.
Detect Interval	Set the detect interval as you need.

Object	Description
	The recommended value is 5 (default).
Detect Link Up Threshold	Set the times for detecting link up. The recommended value is 8 (default).
Detect Link Down Threshold	Set the times for detecting link down. The recommended value is 3 (default).
Custom Detect Host	The host is used to check whether the internet connection is alive or not.

4.5.5 LAN

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 4-38. Here you may change the settings for IP address, subnet mask, DHCP, etc.

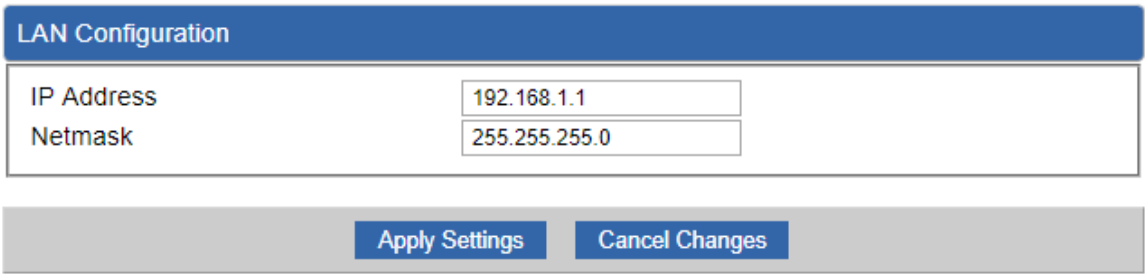


Figure 4-38: LAN Setup

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

4.5.6 Multi-Subnet

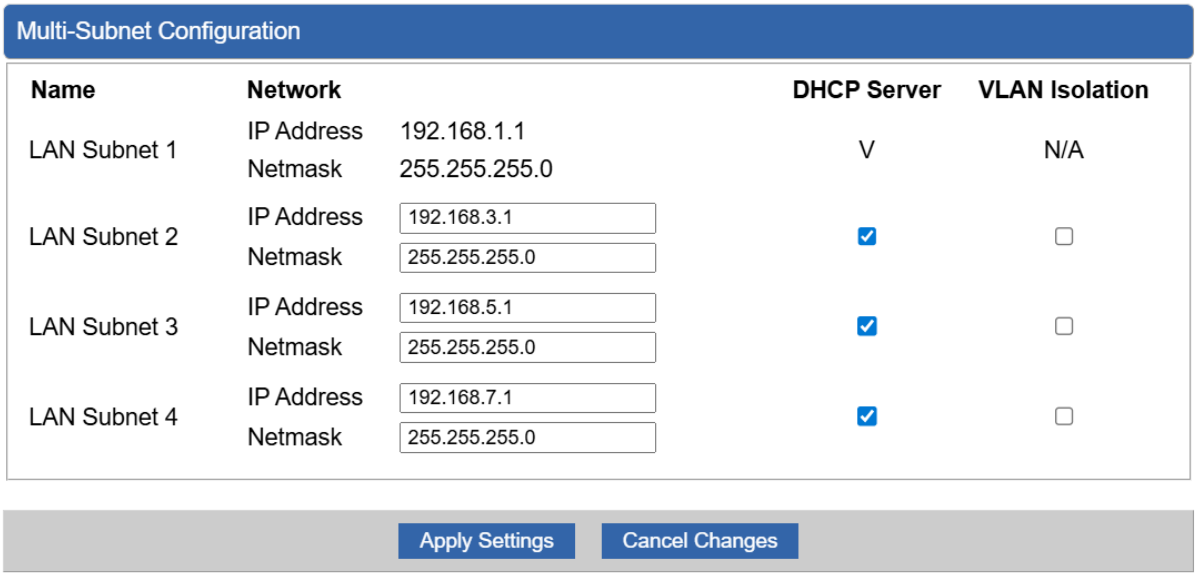


Figure 4-39: Multi-Subnet Configuration

Object	Description
LAN Subnet 1–4	Configure up to four LAN subnets with individual IP address and subnet mask settings.
IP Address	Specify the gateway IP address for each LAN subnet.
Netmask	Define the subnet mask for each LAN network segment.
DHCP Server	Enable or disable the DHCP server for each subnet to automatically assign IP addresses to clients.
VLAN Isolation	Enable or disable VLAN isolation to restrict communication between different subnets.

4.5.7 VLAN

Please refer to the following sections for the details as shown below.

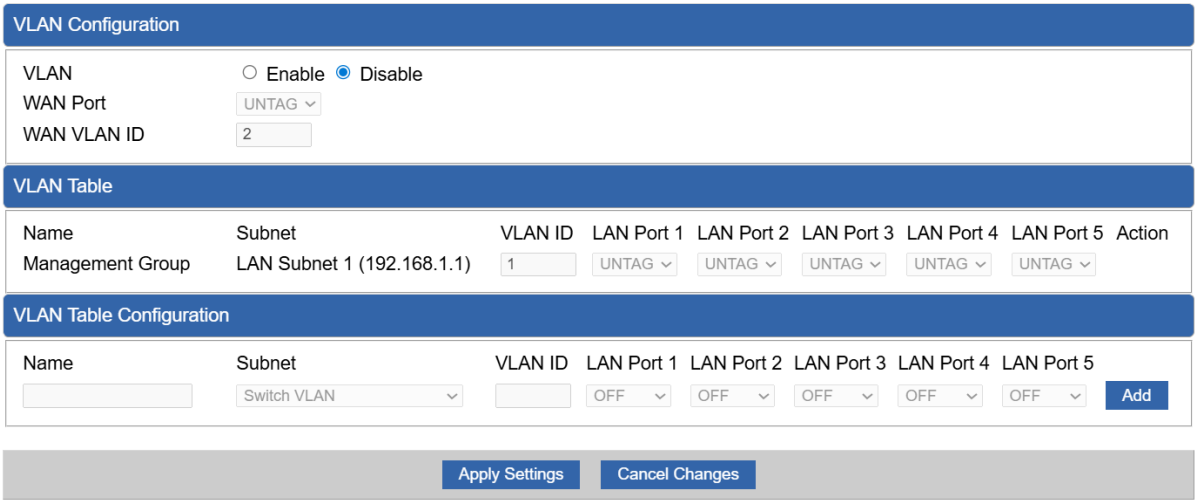


Figure ,4-40: VLAN Configuration

Object	Description
VLAN	Enable or disable VLAN functionality on the device.
WAN Port	Configure the VLAN mode of the WAN port (e.g., untagged/tagged).
WAN VLAN ID	Specify the VLAN ID used for the WAN interface.
VLAN Table	Display existing VLAN groups with associated subnet and port membership settings.
VLAN ID	Define the VLAN identifier for each VLAN group.
LAN Port 1–5	Configure each LAN port as tagged, untagged, or excluded (off) within the VLAN.
Management Group	Default VLAN group associated with the management subnet.
VLAN Table Configuration	Create or modify VLAN entries by assigning name, subnet type, VLAN ID, and port membership.
Name	Specify the name of the VLAN group.
Subnet	Select the subnet type (e.g., switch VLAN or associated LAN subnet).
Add	Add a new VLAN entry to the VLAN table.

4.5.8 UPnP

Please refer to the following sections for the details as shown below.

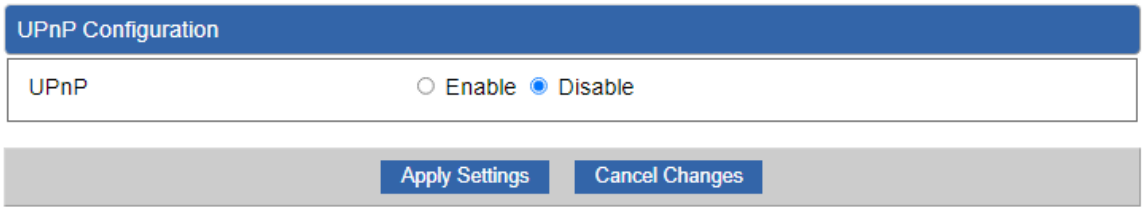


Figure 4-41: VLAN Configuration

Object	Description
UPnP	Enable or disable Universal Plug and Play (UPnP) to allow automatic port forwarding and network device discovery.

4.5.9 Routing

Please refer to the following sections for the details as shown in Figures 4-42 and 43.

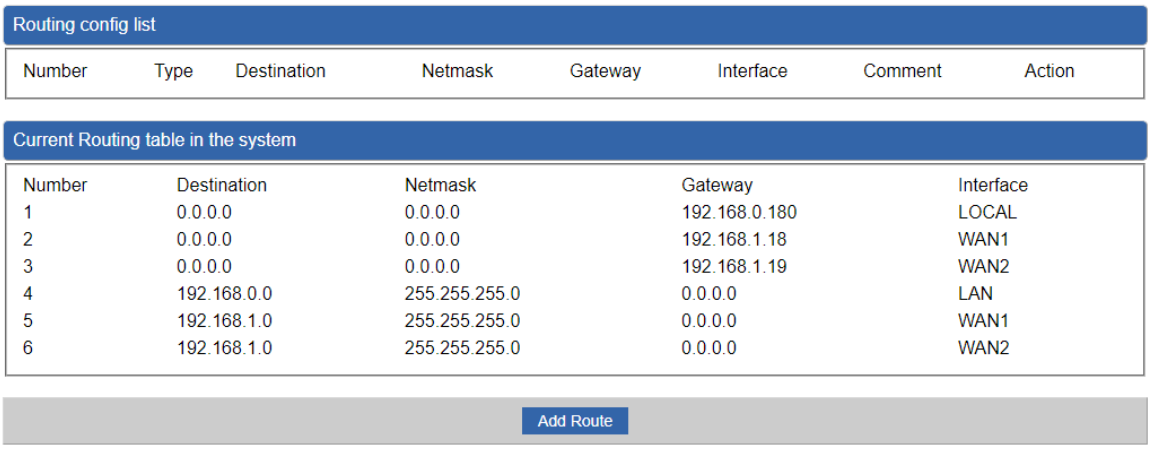


Figure 4-42: Routing table

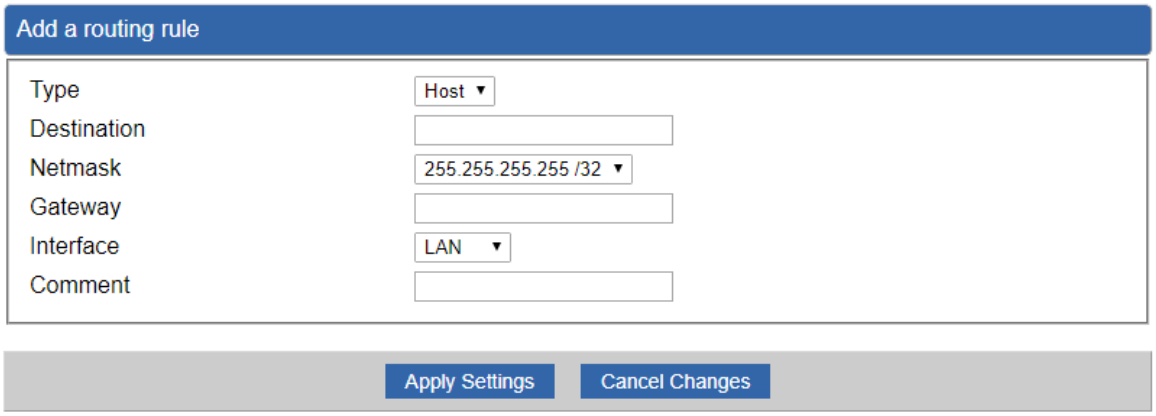


Figure 4-43: Routing setup

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 specify the destination IP address ranges that remote device will accept.

Object	Description
Type	There are two types: Host and Net. When the Net type is selected, user does not need to input the Gateway.
Destination	The network or host IP address desired to access.
Net Mask	The subnet mask of destination IP.
Gateway	The gateway is the router or host's IP address to which packet was sent. It must be the same network segment with

Object	Description
	the WAN or LAN port.
Interface	Select the interface that the IP packet must use to transmit out of the router when this route is used.
Comment	Enter any words for recognition.

4.5.10 RIP

Please refer to the following sections for the details as shown below.

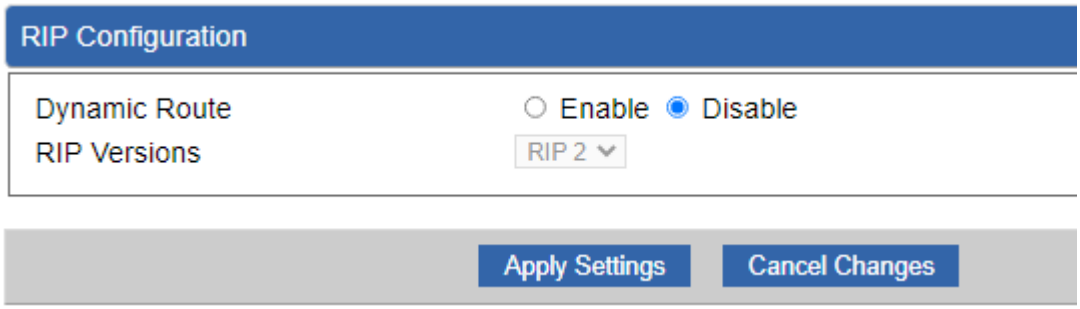


Figure ,4-44: OSPF Configuration table

Object	Description
Dynamic Route	Enable or disable dynamic routing using RIP protocol.
RIP Versions	Select the RIP version (e.g., RIP v1 or RIP v2) for route exchange.

4.5.11 OSPF

Please refer to the following sections for the details as shown below.

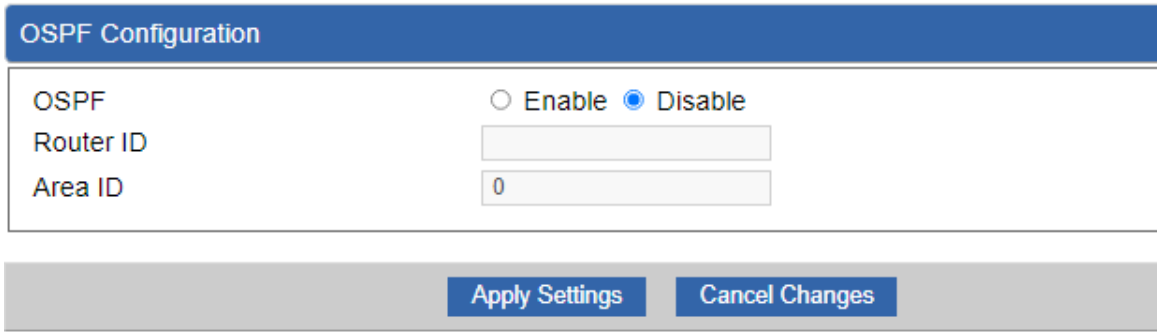


Figure 4-45: Routing table

Object	Description
OSPF	Enable or disable OSPF (Open Shortest Path First) dynamic routing protocol.
Router ID	Specify the unique router identifier used in the OSPF network.
Area ID	Define the OSPF area ID for routing domain segmentation (default: 0).

4.5.12 IGMP

Please refer to the following sections for the details as shown below.

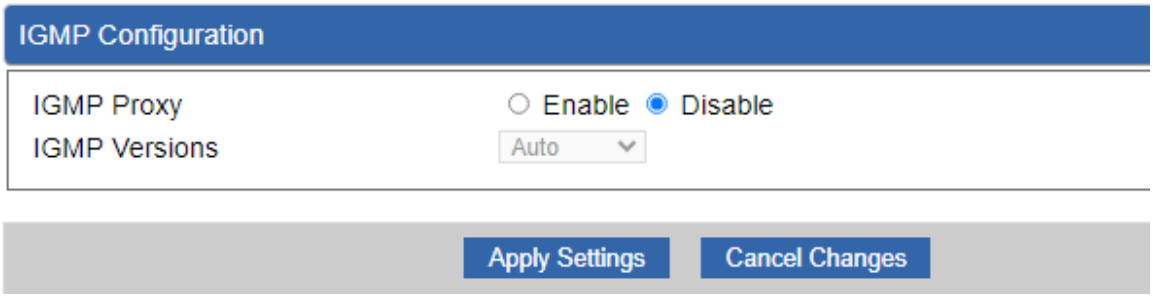


Figure 4-46: Routing table

Object	Description
IGMP Proxy	Enable or disable IGMP Proxy to forward multicast traffic between different network interfaces.
IGMP Versions	Select the IGMP version (e.g., v1, v2, v3 or Auto) for multicast group management.

4.5.13 IPv6

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the router as shown in Figure 4-47. 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.

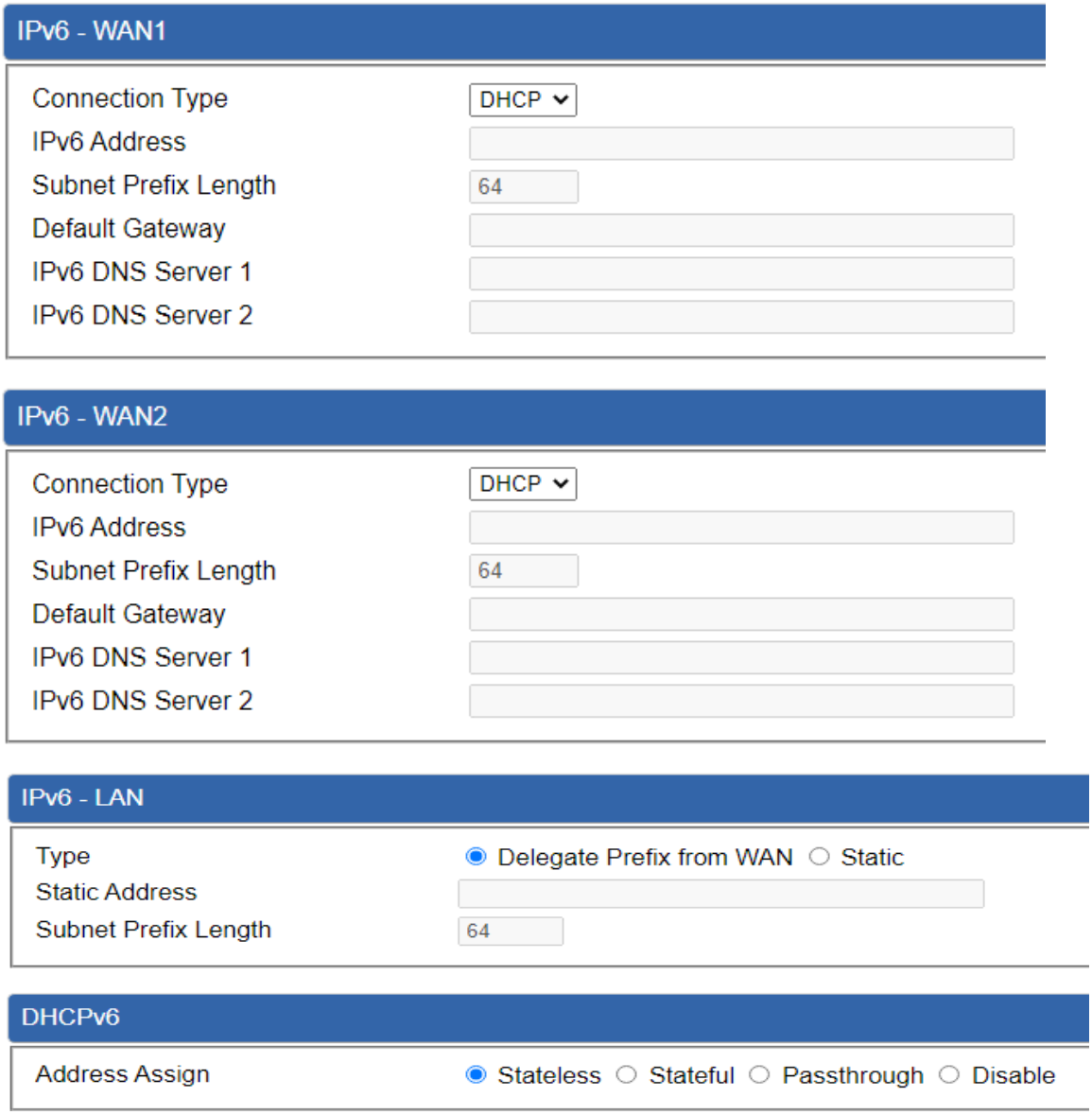


Figure 4-47: IPv6 WAN setup

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

4.5.14 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 4-48.

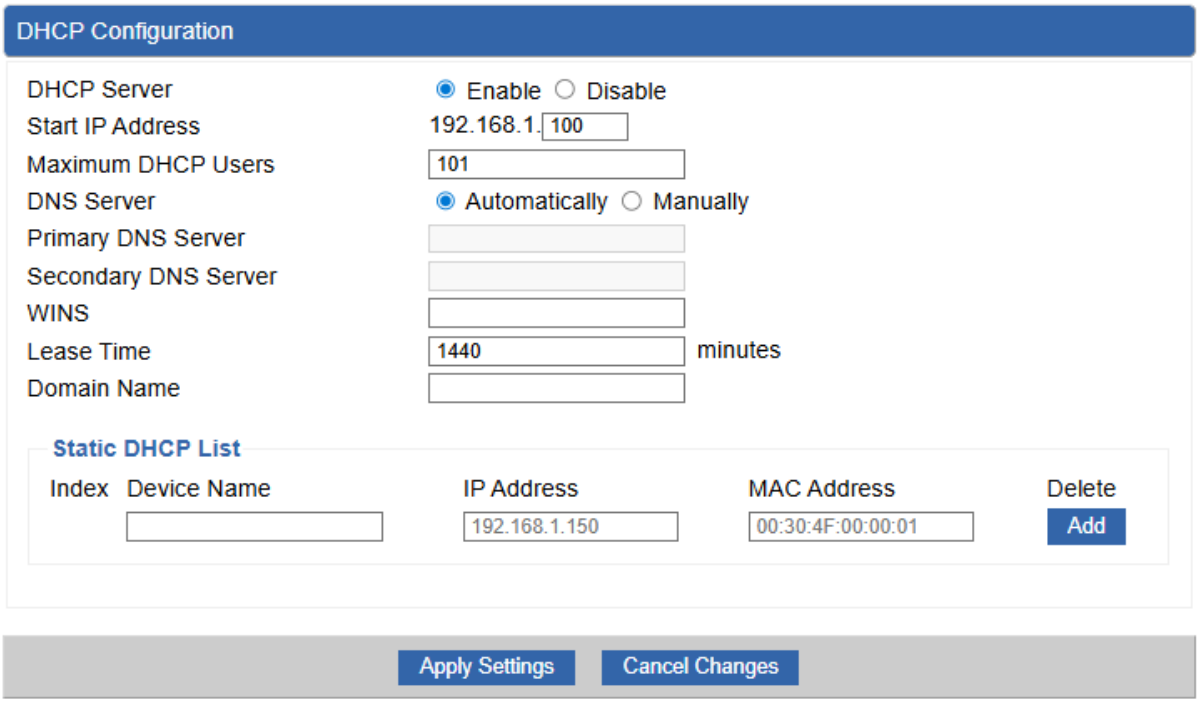


Figure 4-48: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the router will assign IP addresses to the DHCP clients automatically. If user needs to disable the function, please set it as disable.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the router.
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the router will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
Set DNS	By default, it is set as Automatically, and the DNS server

Object	Description
	is the router's LAN IP address. If user needs to use specific DNS server, please set it as Manually, and then input a specific DNS server.
Primary/Secondary DNS Server	Input a specific DNS server.
WINS	Input a WINS server if needed.
Lease Time	Set the time for using one assigned IP. After the lease time, the DHCP client will need to get new IP addresses from the router. Default is 1440 minutes.
Domain Name	Input a domain name for the router. Default is Planet.
Static DHCP List	Configure static IP bindings based on MAC address.
Device Name	Define the name of the client device for identification.
IP Address	Assign a fixed IP address to the specified device.
MAC Address	Specify the MAC address of the client device.
Add	Add a static DHCP entry to the list.

4.5.15 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 (**https://www.planetddns.com**)** and set up the domain name of your choice.

PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown in Figure 4-49.

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

PLANET Easy DDNS

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

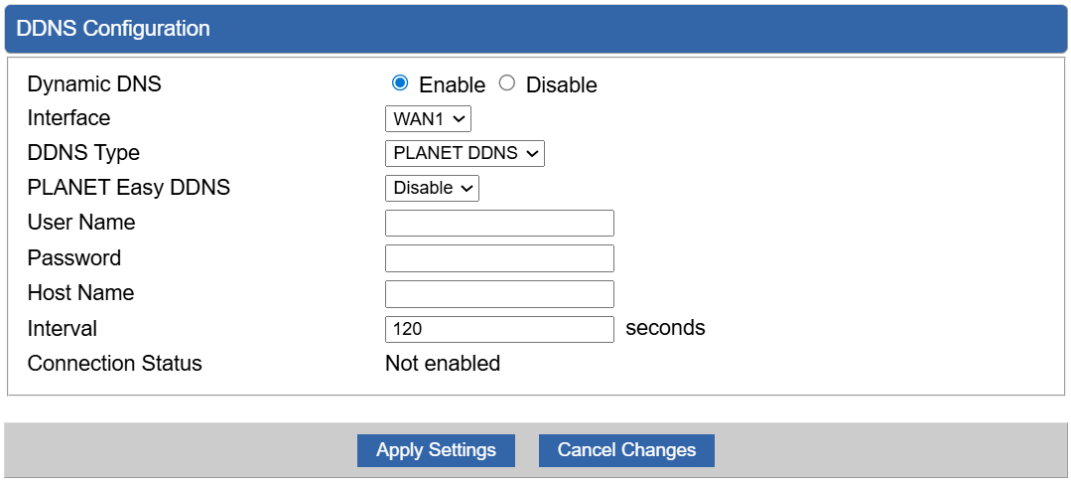


Figure 4-49: PLANET DDNS

Object	Description
DDNS Service	By default, the DDNS service is disabled. If user needs to enable the function, please set it as enable.
Interface	User is able to select the interface for DDNS service. By default, the interface is WAN 1.
DDNS Type	There are three options: 1. PLANET DDNS: Activate PLANET DDNS service. 2. DynDNS: Activate DynDNS service. 3. NOIP: Activate NOIP service. Note that please first register with the DDNS service and set up the domain name of your choice to begin using it.
Easy DDNS	When the PLANET DDNS service is activated, user is able to select to enable or disable Easy DDNS. When this function is enabled, DDNS hostname will appear automatically. User doesn't have to go to https://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 is registered with your DDNS provider.
Interval	Set the update interval of the DDNS function.
Update Status	Show the connection status of the DDNS function.

4.5.16 MAC Address Clone

Clone or change the MAC address of the WAN interface. The setup is shown in Figure 4-50.

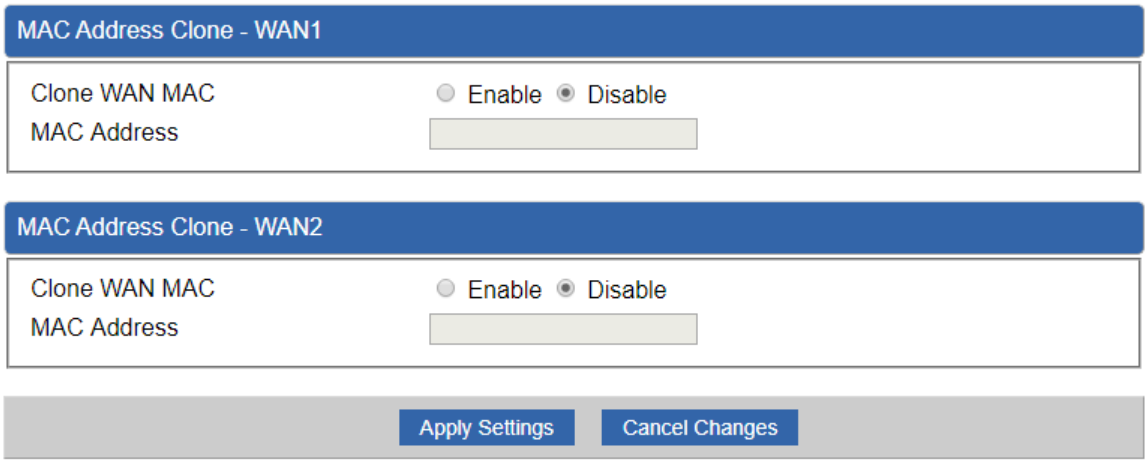


Figure 4-50: MAC Address Clone

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 Cellular

This chapter is for 5G NR cellular model only, ex. XVR-800BE-NR.

The Cellular menu provides LTE/NR related functions as shown in Figure 4-51. Please refer to the following sections for the details.

Figure 4-51: Cellular menu

Object	Description
LTE/NR Configuration	Allows setting LTE/NR configuration.
LTE/NR Advanced	Allows setting SIM configuration.
LTE/NR Status	Display the status of cellular.
LTE/NR Statistics	Display the statistics of cellular.
GPS	Display the location of cellular gateway.
SMS	Allows setting SMS configuration for alarm notification.

4.6.1 LTE/NR Configuration

This page provides LTE/NR configuration as shown in Figure 4-52.

Figure 4-52: LTE/NR configuration

Object	Description
LTE/NR Config	Indicates what kind of LTE will be used. Possible modes are: ■ **Auto**: Automatically connect the possible band. ■ **4G&5G Only**: Connect to 4G or 5G network only. ■ **5G Only**: Connect to 5G network only. ■ **4G Only**: Connect to 4G network only. ■ **3G Only**: Connect to 3G network only. ■ **2G Only**: Connect to 2G network only.
MTU	Maximum transfer unit; default is **1500**.

4.6.2 LTE/NR Advanced

This page provides LTE/NR advanced configuration as shown in Figure 4-53.

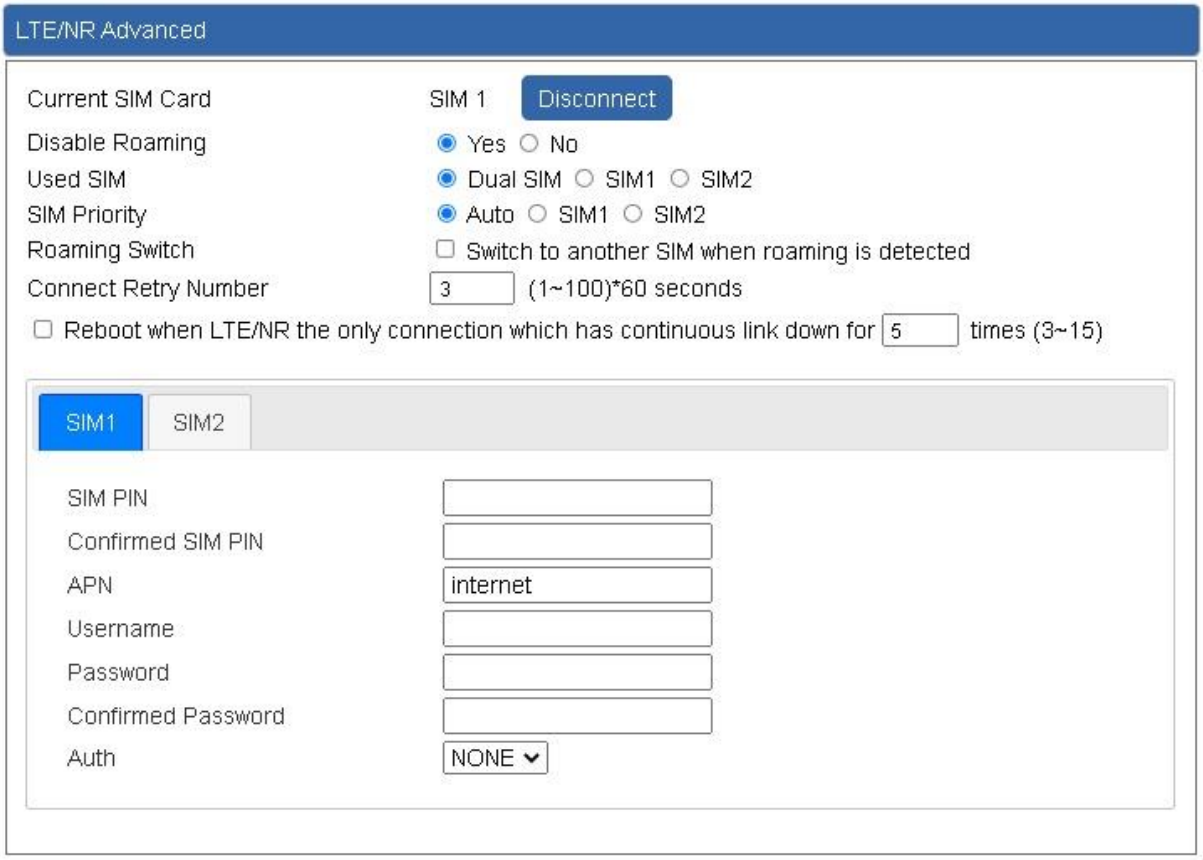


Figure 4-53: LTE/NR advanced

Object	Description
Current SIM Card	Display which SIM slot is using.
Disable Roaming	■ **Disable:** SIM gets connection even it is in roaming state. ■ **Enable:** SIM would not get connection when in roaming state.
Used SIM	Configure which SIM card or dual SIM cards is used.
SIM Priority	Configure priority of SIM card
Roaming Switch	Switch to another SIM when roaming is detected. System will switch to SIM slot when current SIM is in roaming state and the other SIM slot is in READY state.

Object	Description
SIM PIN	Configure PIN code to unlock SIM PIN.
Confirmed SIM PIN	Confirm PIN code.
APN	APN can be input by user or the system..
Username	The username can be input by user or the system.
Password	The password can be input by user or the system.
Confirm Password	Fill in your changed password.
Auth	Configure authentication ■ **None** ■ **PAP** ■ **CHAP**

4.6.3 LTE/NR Status

This page displays LTE/NR status as shown in Figure 4-54.

Figure 4-54: LTE/NR status

4.6.4 LTE/NR Statistics

This page displays LTE/NR status as shown in Figure 4-55.

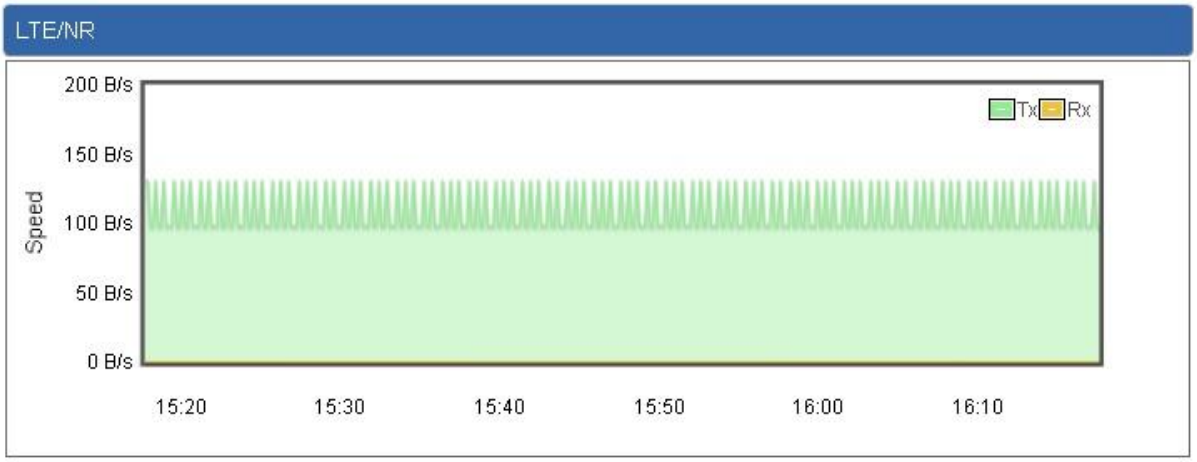


Figure 4-55: LTE/NR statistics

4.6.5 GPS

This page displays GPS status as shown in Figure 4-56.

Figure 4-56: GPS

4.6.6 SMS

This page provides SMS configuration as shown in Figure 4-57.

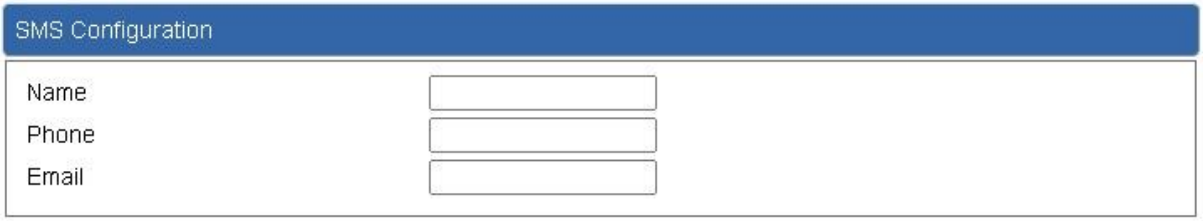


Figure 4-57: SMS

Object	Description
Name	Configure user's name
Phone	Configure user's phone number
Email	Configure user's email

4.7 Security

The Security menu provides Firewall, Access Filtering and other functions as shown in Figure 4-58. Please refer to the following sections for the details.

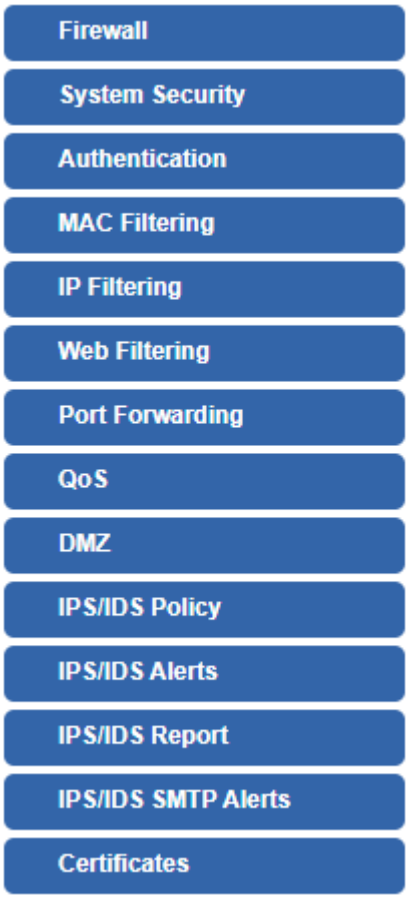


Figure 4-58: Security menu

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

IPS/IDS Policy	Allows configuring IPS/IDS policies and DPI engine settings.
IPS/IDS Alerts	Displays IPS/IDS alert information and event logs.
IPS/IDS Report	Allows generating and exporting IPS/IDS security reports.
IPS/IDS SMTP Alerts	Allows configuring email notifications for IPS/IDS alerts and reports.
Certificates	Allows managing web server and system CA certificates.

4.7.1 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 4-59.

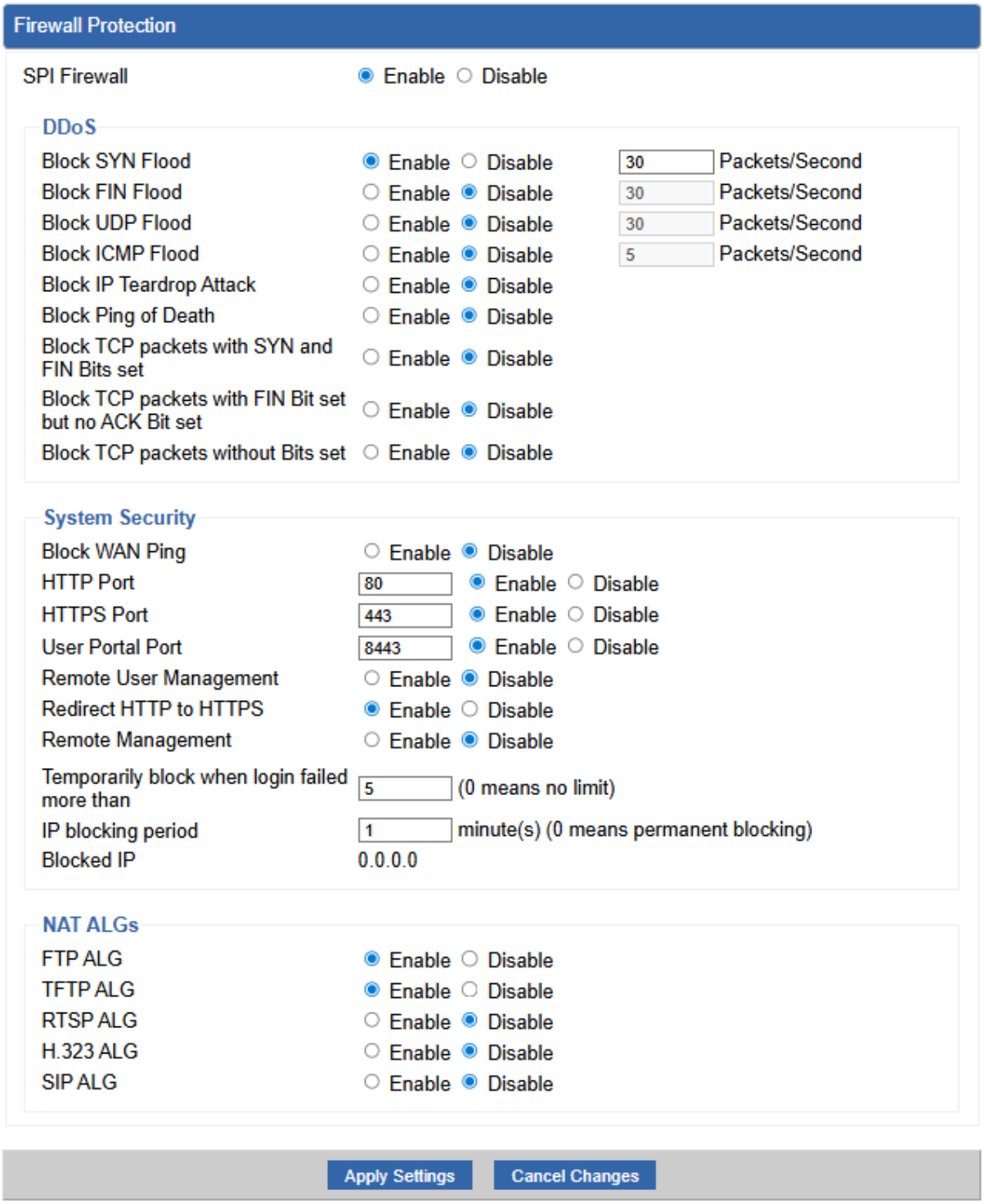


Figure 4-59: Firewall

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. The default configuration is enabled.
DDoS	
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.
Block ICMP Flood	ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack. The default configuration is disabled.
Block IP Teardrop Attack	If the function is enabled, the router will block malformed fragmented packets targeting IP reassembly vulnerabilities. The default configuration is disabled.
Block Ping of Death	If the function is enabled, the router will block oversized ICMP packets that may cause system crashes. The default configuration is disabled.
Block TCP SYN+FIN Packets	If the function is enabled, the router will block abnormal TCP packets with both SYN and FIN flags set. The default configuration is disabled.
Block TCP FIN without ACK	If the function is enabled, the router will block TCP packets with FIN flag but without ACK flag. The default configuration is disabled.
Block TCP without Flags	If the function is enabled, the router will block TCP packets with no flags set (null packets). The default configuration is disabled.

System Security	
Block WAN Ping	Enable the function to allow or block ping access from the Internet. The default configuration is disabled.
HTTP Port	Enable the function to allow HTTP access to the router and configure the port number. The default configuration is enabled (port 80).
HTTPS Port	Enable the function to allow HTTPS access to the router and configure the port number. The default configuration is enabled (port 443).
User Portal Port (ZT-800 series only)	Configure the portal access port for user login interface. The default configuration is enabled (port 8443).
Remote User Management	Enable the function to allow remote user access management. The default configuration is disabled.
Redirect HTTP to HTTPS	Enable the function to automatically redirect HTTP requests to HTTPS for secure access. The default configuration is enabled.
Remote Management	Enable the function to allow web management access from the Internet. The default configuration is disabled.
Login Failure Blocking	If enabled, the system will temporarily block access when login attempts exceed the specified number. The default configuration is enabled.
IP Blocking Period	Define the blocking duration for restricted IP addresses (0 means permanent blocking).
Blocked IP	Display the IP addresses currently blocked by the system.
NAT ALGs	
FTP ALG	Enable the function to support FTP protocol traversal through NAT. The default configuration is enabled.
TFTP ALG	Enable the function to support TFTP protocol traversal through NAT. The default configuration is enabled.
RTSP ALG	Enable the function to support RTSP streaming through NAT. The default configuration is disabled.

H.323 ALG	Enable the function to support H.323 protocol traversal. The default configuration is disabled.
SIP ALG	Enable the function to support SIP VoIP traffic through NAT. The default configuration is disabled.

4.7.2 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 4-60.

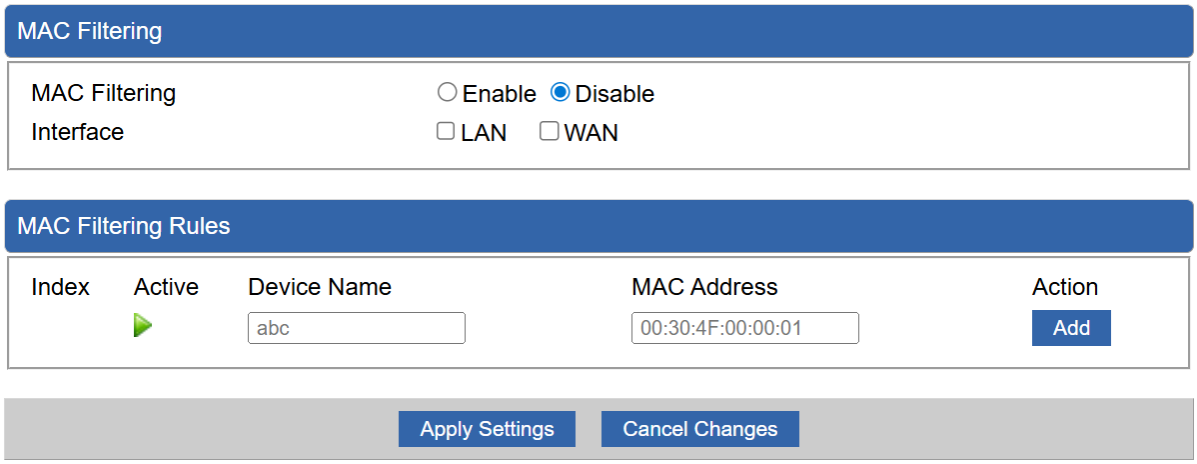


Figure 4-60: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. When the function is enabled, the router will block traffic of the MAC address on the list.
Interface	Select the function works on LAN, WAN or both. If you want to block a LAN device's MAC address, please select LAN, vice versa.
Active	Enable or disable an individual MAC filtering rule.
Device Name	Specify a name for the device for easier identification.
MAC Address	Input a MAC address you want to control, such as A8:F7:E0:00:06:62.
Add	When you input a MAC address, please click the "Add" button to add it into the list.

4.7.3 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown in Figure 4-61. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.

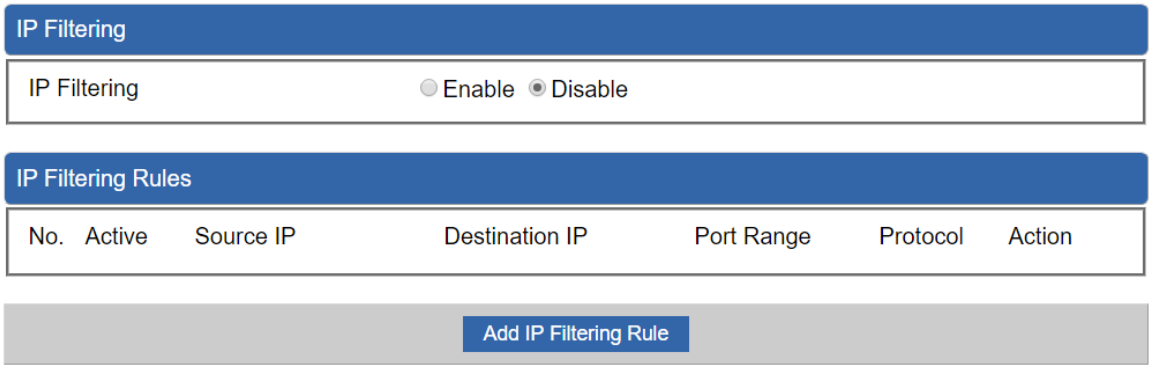


Figure 4-61: IP Filtering

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

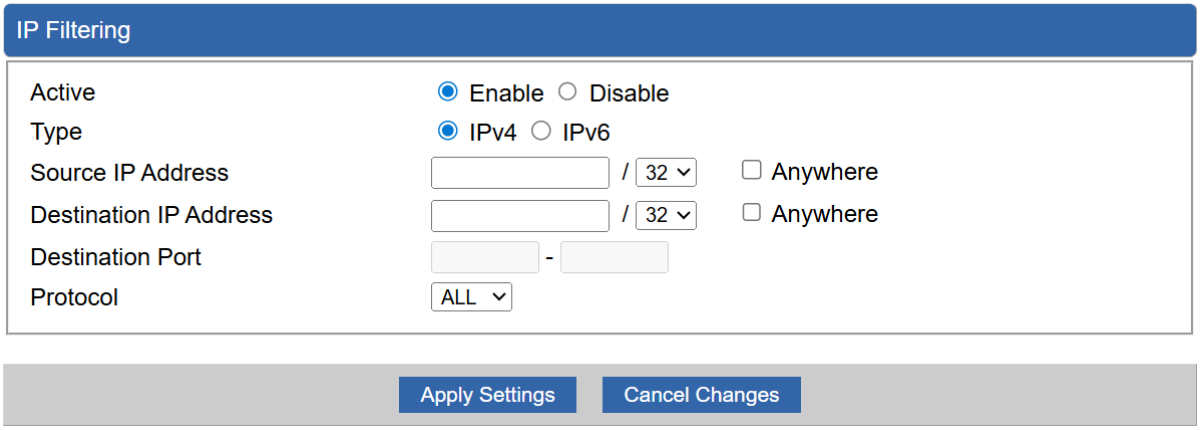


Figure 4-62: IP Filter Rule Setting

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

4.7.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in Figure 4-63. Block those URLs which contain keywords listed below.

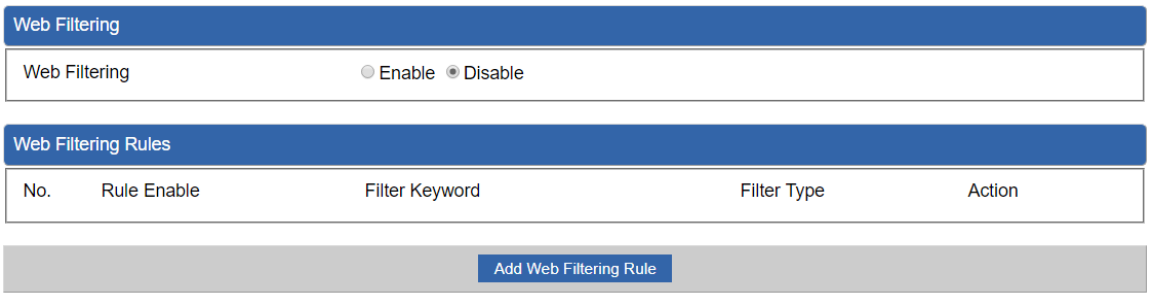


Figure 4-63: Web Filtering

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.

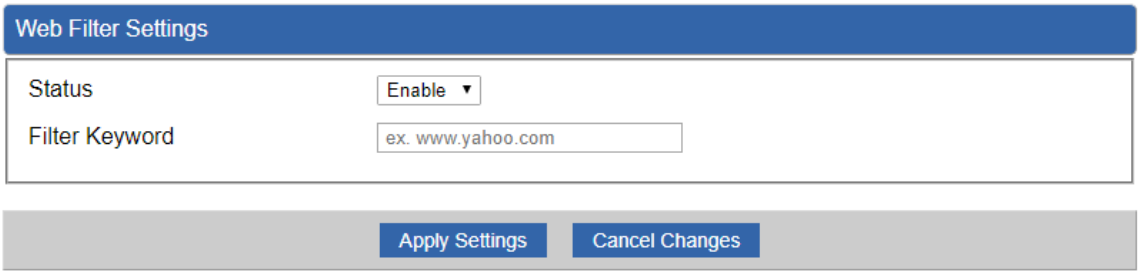


Figure 4-64: Web Filtering Rule Setting

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

4.7.5 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 4-65. 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.

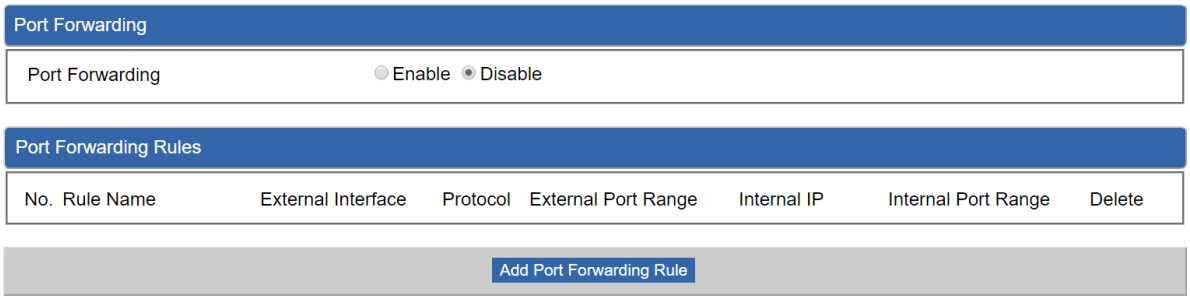


Figure 4-65: Port Forwarding

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

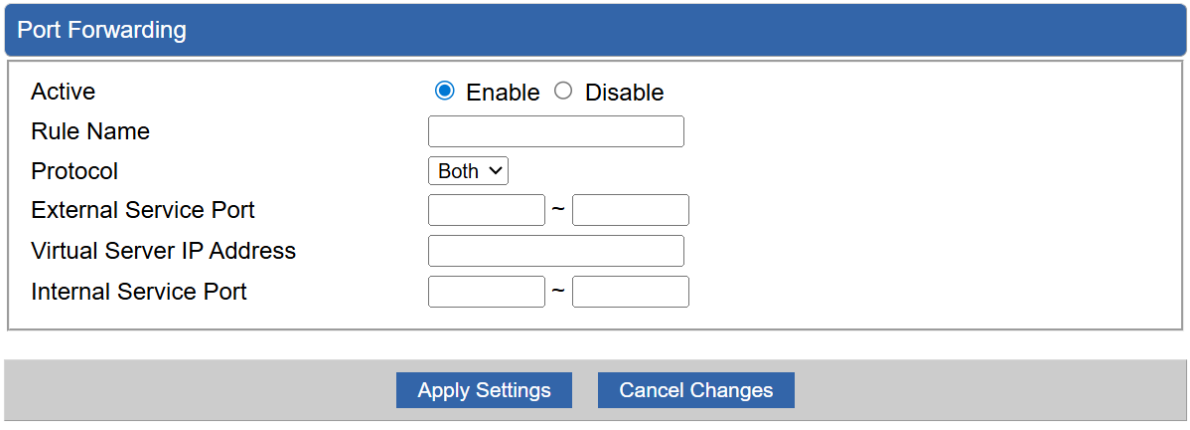
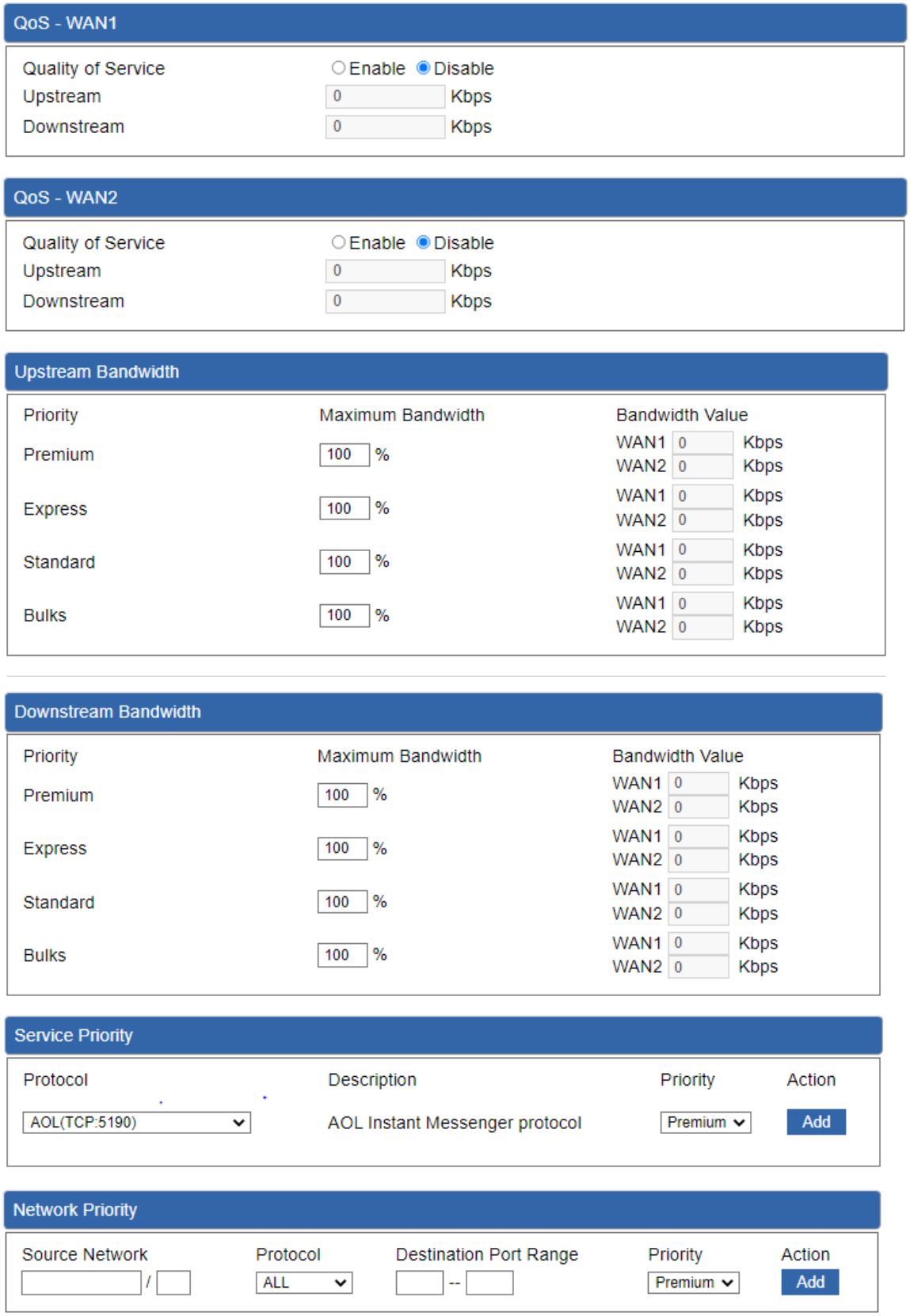


Figure 4-66: Port Forwarding Rule Setting

Object	Description
Rule Name	Enter any words for recognition.
Protocol	Select the protocol type (TCP, UDP or both). If you are unsure, please leave it to both the default 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.

4.7.6 QoS

Please refer to the following sections for the details as shown below.



4.7.7 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in Figure 4-67. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

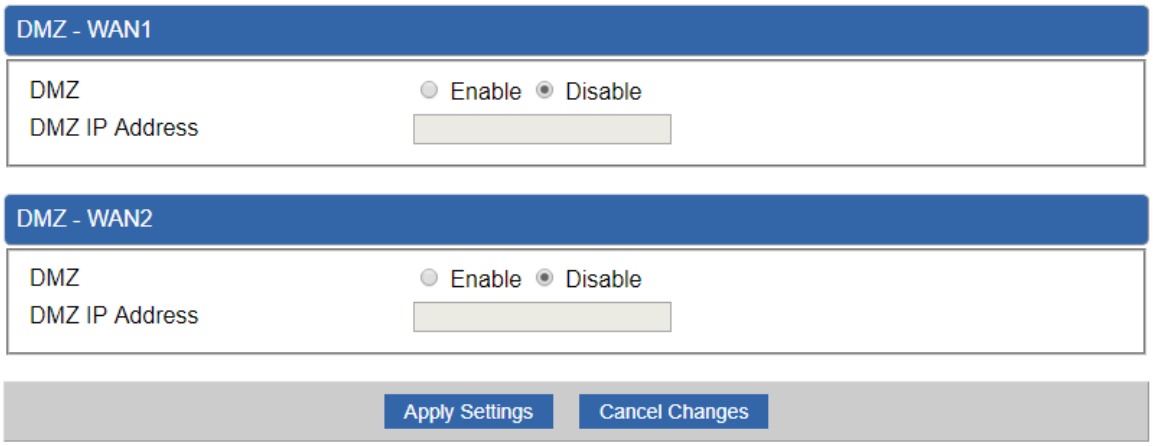


Figure 4-67: DMZ

Object	Description
DMZ	Set the function as enable or disable. If the DMZ function is enabled, it means that you set up DMZ at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/online game can have two way connections.
DMZ IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above.

4.7.8 IPS/IDS Policy (CSG-800 series Only)

The **IPS/IDS Policy** page is used to enable or disable the DPI Engine and configure IPS/IDS security policies. Users can create, modify, and apply security policies to detect and prevent network threats. The status is shown in Figure 4-68.

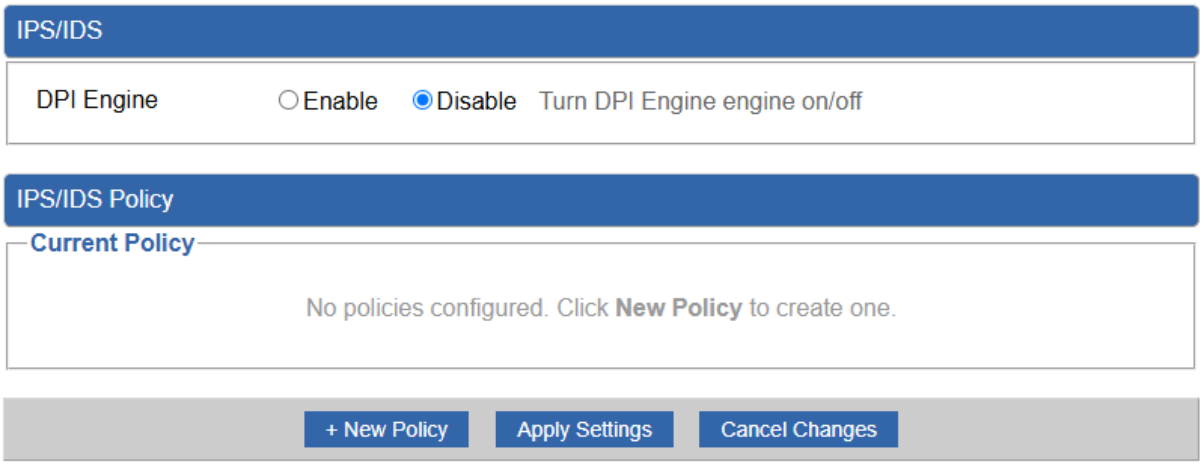


Figure 4-68: IPS/IDS Policy

Object	Description
DPI Engine	Enable or disable the DPI Engine. When enabled, the system inspects network traffic using the IPS/IDS engine to detect and prevent malicious activities.
Current Policy	Displays the configured IPS/IDS policies. If no policy has been created, the list will remain empty.
New Policy	Click to create a new IPS/IDS policy.
Apply Settings	Click to save and apply the current IPS/IDS configuration.
Cancel Changes	Click to discard any unsaved changes and restore the previous configuration.

4.7.8.1 Policy Wizard (CSG-800 series Only)

The **Policy Wizard** guides users through the process of creating an IPS/IDS policy. The wizard consists of five steps, including selecting a policy template, configuring protocols and threat types, specifying interfaces and exceptions, and reviewing the policy settings before applying them. The Policy Wizard is shown in Figure 4-69 through Figure 4-73

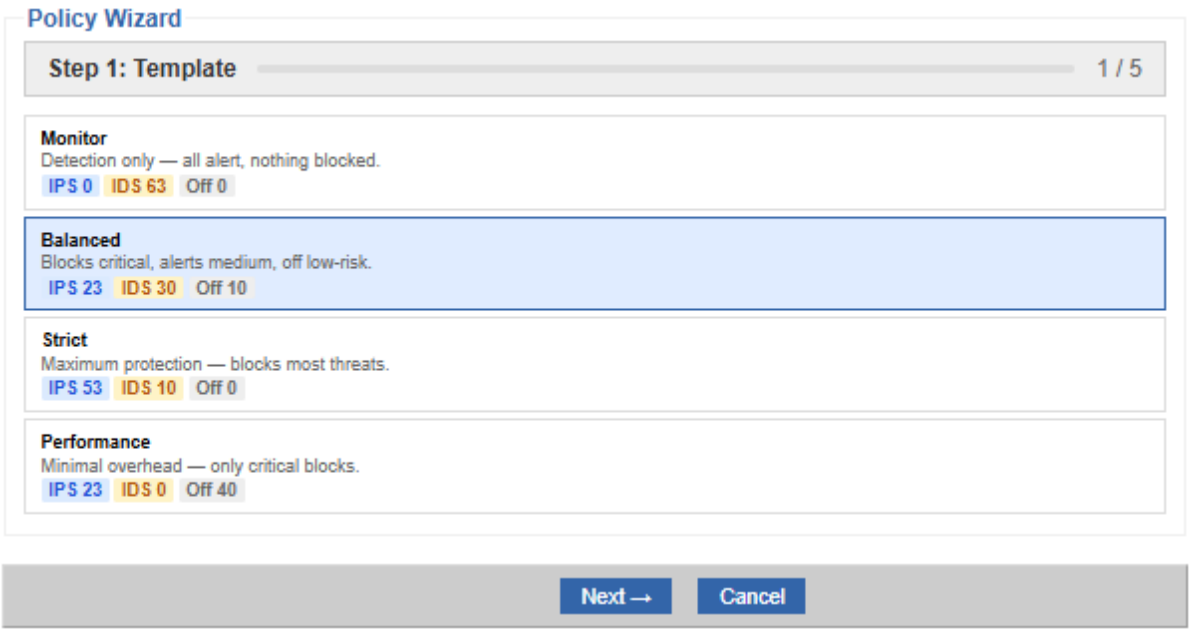


Figure 4-69: Policy Wizard Step 1: Template

Object	Description
Template	Select a predefined security policy template, including **Monitor**, **Balanced**, **Strict**, or **Performance**, according to the desired protection level.

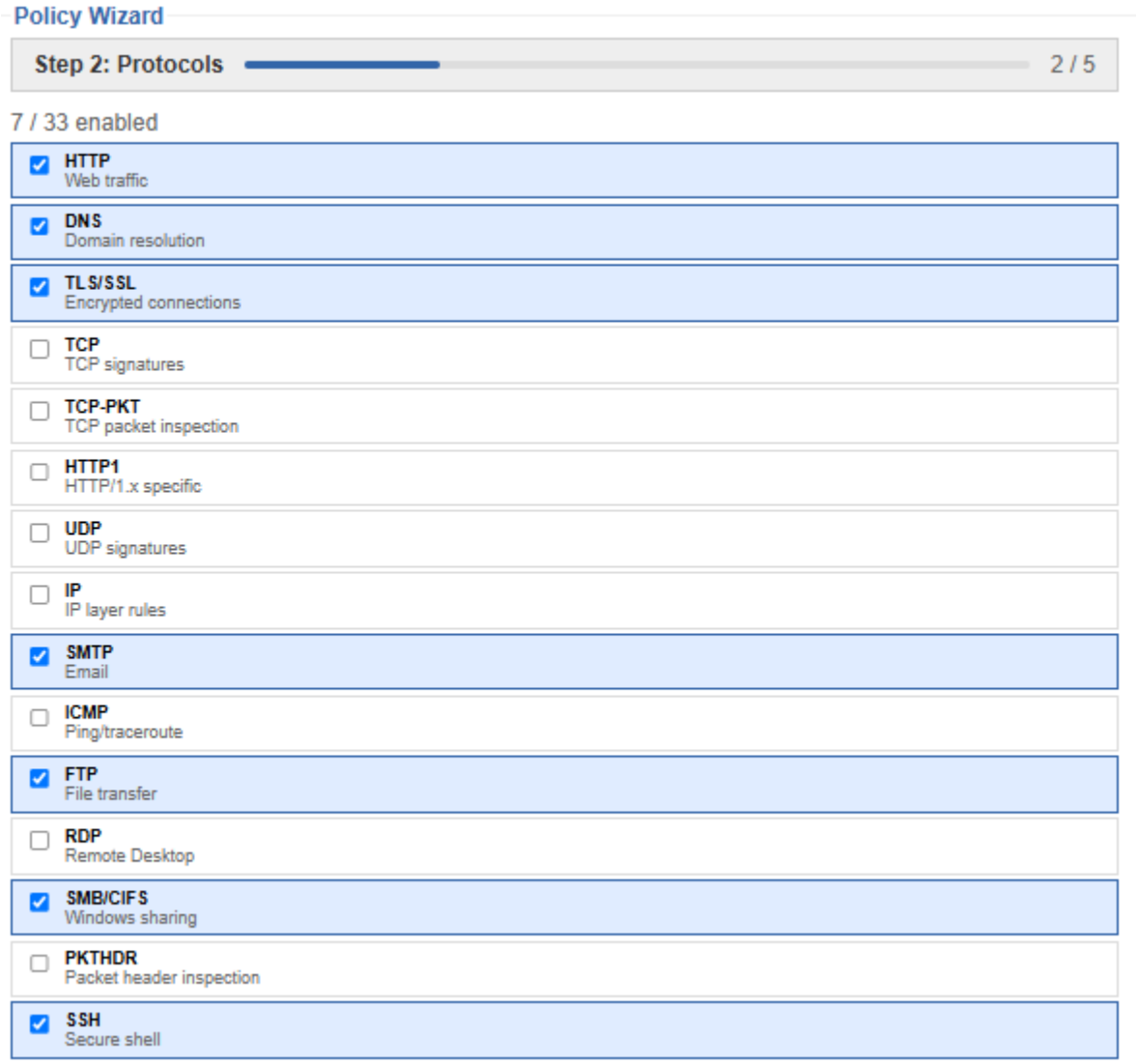


Figure 4-70: Policy Wizard Step 2: Protocols

Object	Description
Protocols	Select the network protocols to be inspected by the IPS/IDS engine.

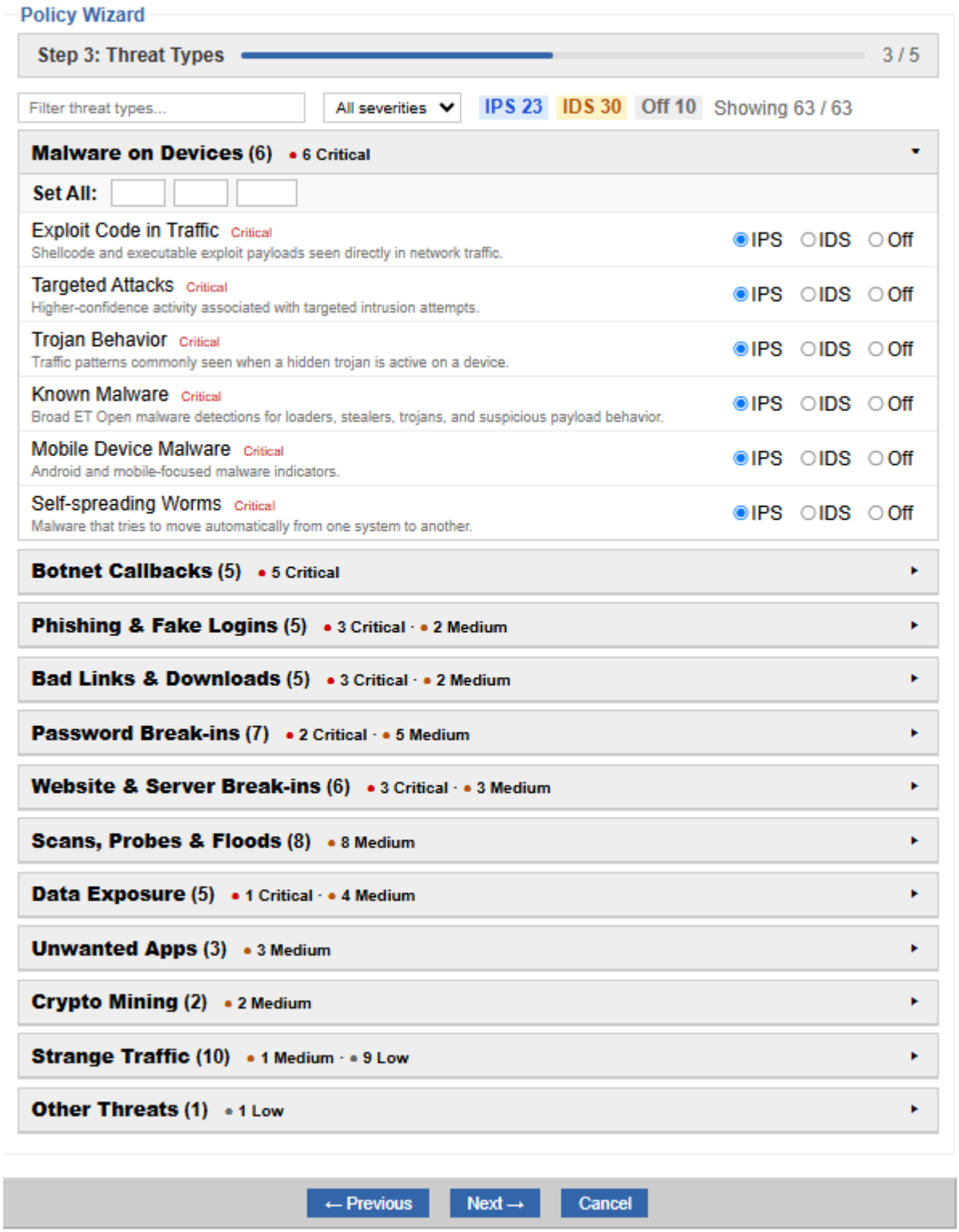


Figure 4-71: Policy Wizard Step 3: Threat Types

Object	Description
Threat Types	Displays the available threat categories for policy configuration. Expand a category to configure individual threat rules.

Object	Description
Severity Filter	Select a severity level to filter the displayed threat types.
Threat Statistics	Displays the number of rules currently configured as **IPS**, **IDS**, or **Off**.
Set All	Apply the selected action (**IPS**, **IDS**, or **Off**) to all threat rules in the current category.
Action	Select **IPS** to block threats, **IDS** to detect and log threats, or **Off** to disable the selected threat rule.

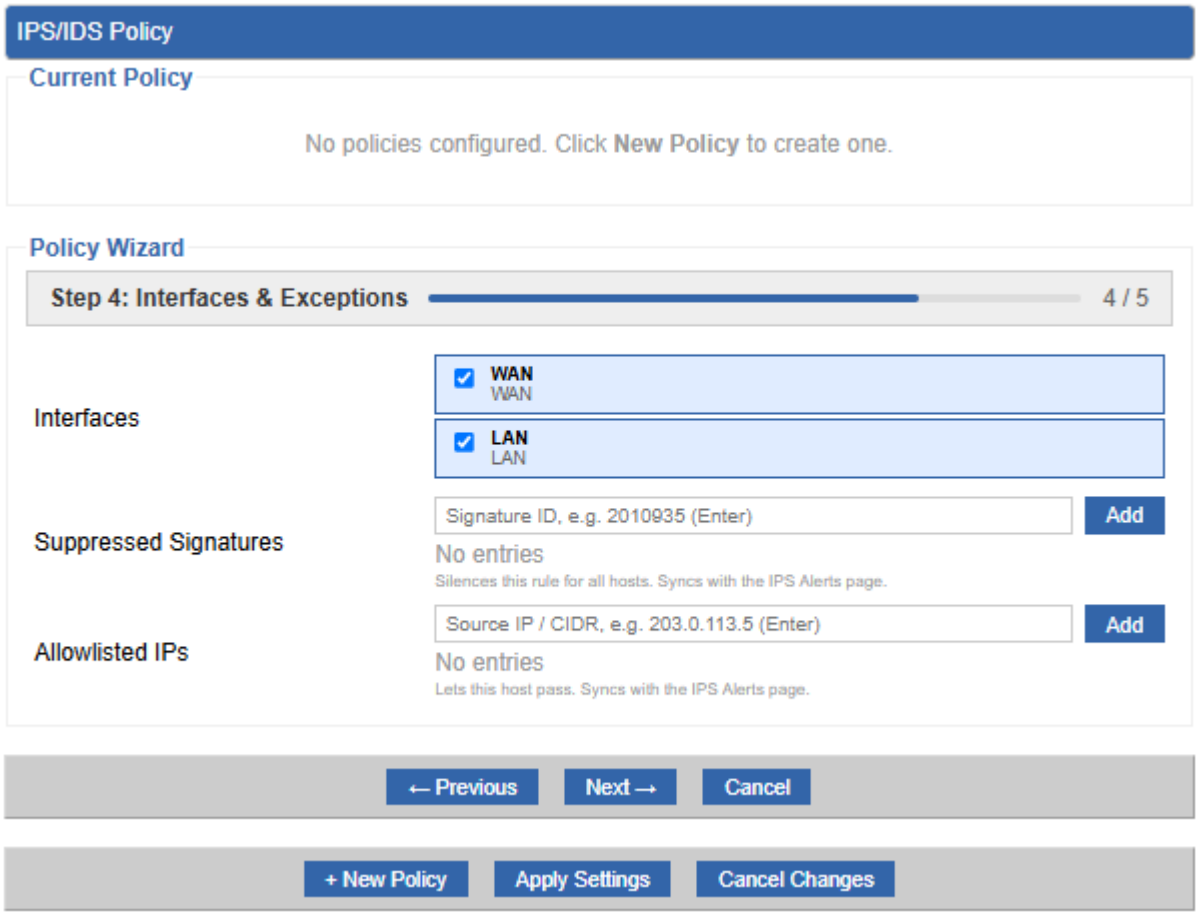


Figure 4-72: Policy Wizard Step 4: Interfaces & Exceptions

Object	Description
Interfaces	Select the network interfaces where the IPS/IDS policy will be applied.
Suppressed Signatures	Add signature IDs to suppress selected IPS/IDS signatures.
Allowlisted IPs	Specify trusted IP addresses or CIDR ranges that bypass IPS/IDS inspection.

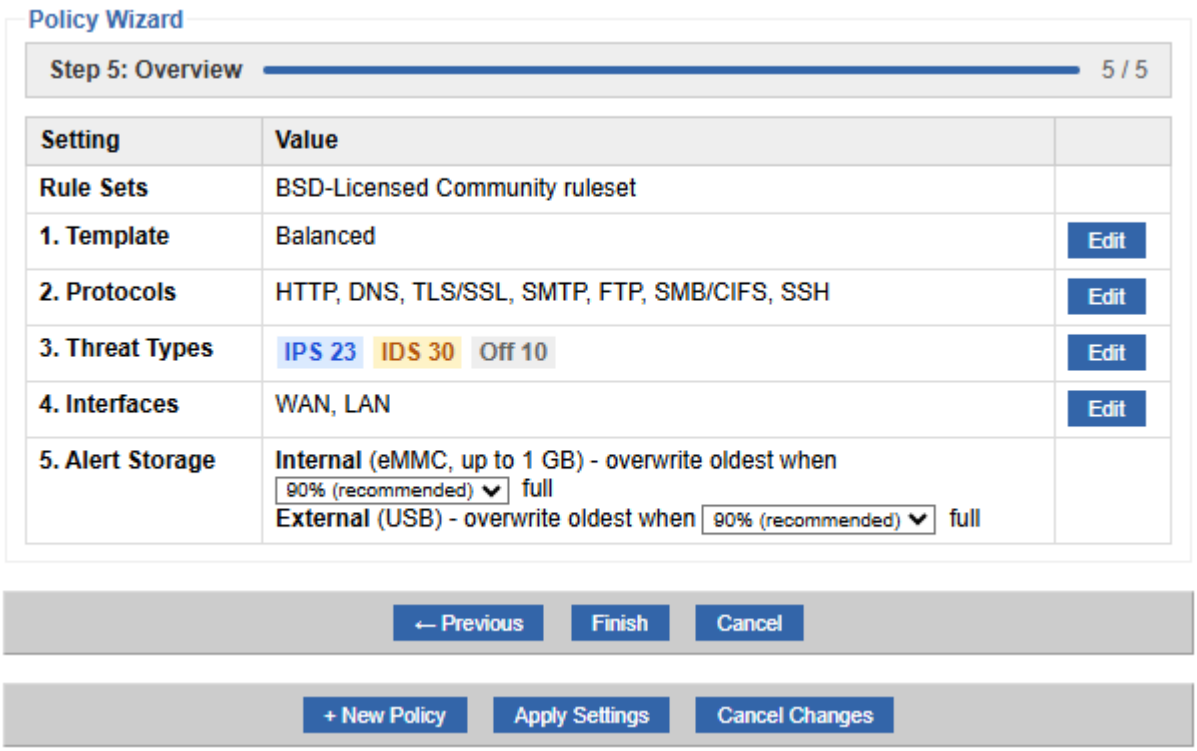


Figure 4-73: Policy Wizard Step 5: Overview

Object	Description
Overview	Displays a summary of the IPS/IDS policy configuration before saving.
Edit	Return to the selected step to modify the configuration.
Finish	Save and create the IPS/IDS policy.

4.7.9 IPS/IDS Alerts (CSG-800 series Only)

The **IPS/IDS Alerts** page displays real-time IPS/IDS detection events and security statistics. Users can search, filter, export, and manage alert records, as well as configure allowlist or suppression settings for individual alerts. The status is shown in Figure 4-74.

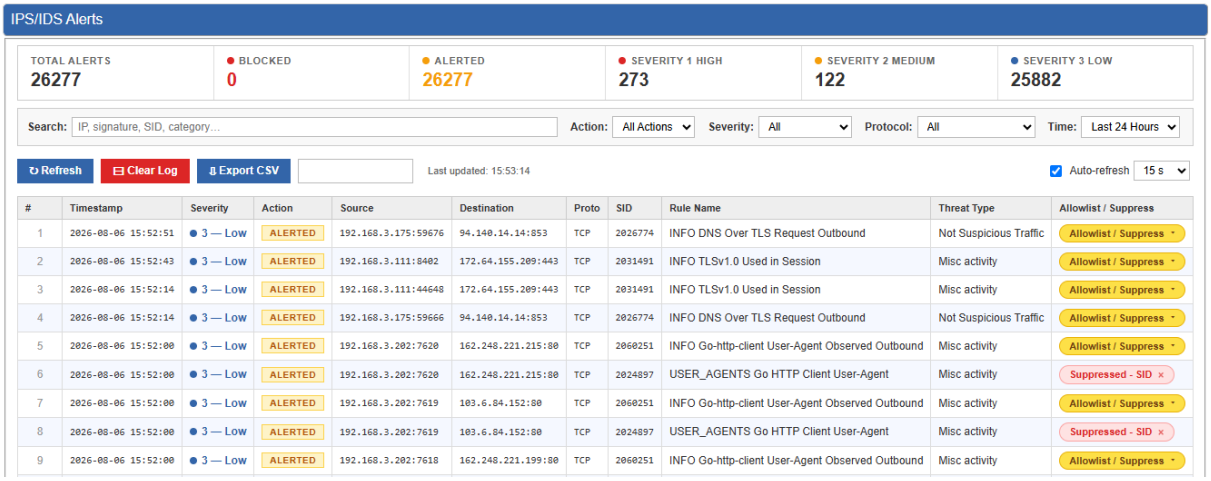


Figure 4-74: IPS/IDS Alerts

Object	Description
Alert Summary	Displays the total number of alerts, blocked events, alerted events, and the number of alerts by severity level.
Search	Search alert records by IP address, signature, SID, or threat category.
Action	Filter alert records by action type.
Severity	Filter alert records by severity level.
Protocol	Filter alert records by network protocol.
Time	Select the time range for displaying alert records.
Refresh	Refresh the current alert list.
Clear Log	Clear all IPS/IDS alert logs.
Export CSV	Export the current alert records in CSV format.
Auto-refresh	Automatically refresh the alert list at the selected interval.
Alert Log	Displays detailed information for each alert, including timestamp, severity, action, source, destination, protocol, SID, rule name, and threat type.
Allowlist / Suppress	Allowlist the selected source or suppress the selected signature to reduce repeated alerts.

4.7.10 IPS/IDS Report (CSG-800 series Only)

The **IPS/IDS Report** page is used to generate and export IPS/IDS security reports. Users can filter report data by report type, time range, severity, protocol, and keywords, then export the generated report in multiple formats. The status is shown in Figure 4-75.

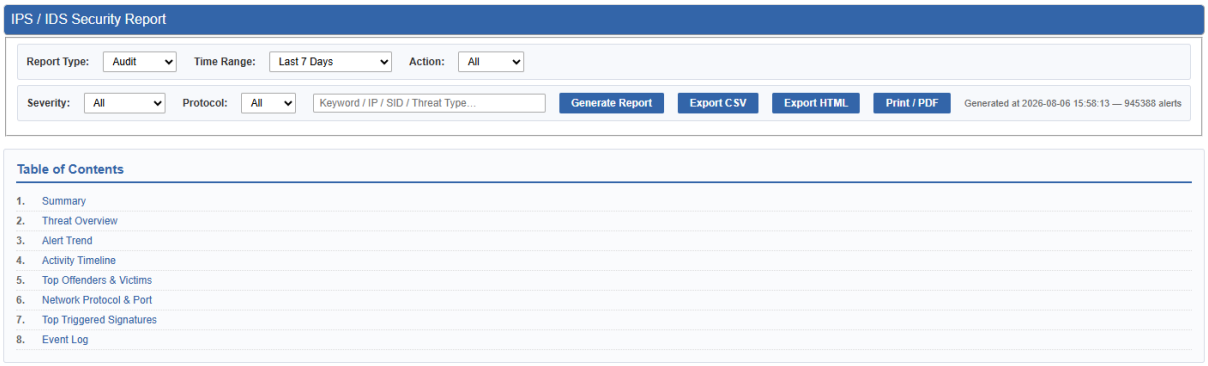


Figure 4-75: IPS/IDS Report

Object	Description
Report Type	Select the type of security report to generate.
Time Range	Select the time range for the report.
Action	Filter report data by action type.
Severity	Filter report data by severity level.
Protocol	Filter report data by network protocol.
Keyword	Search report data by keyword, IP address, SID, or threat type.
Generate Report	Generate the report based on the selected filter criteria.
Export CSV	Export the generated report in CSV format.
Export HTML	Export the generated report in HTML format.
Print / PDF	Print the report or save it as a PDF file.
Report Status	Displays the report generation status, including the generation time and the number of alerts included.
Table of Contents	Displays the sections included in the generated report, such as Summary, Threat Overview, Alert Trend, Activity Timeline, Top Offenders & Victims, Network Protocol & Port, Top Triggered Signatures, and Event Log.

4.7.10.1 IPS/IDS Security Report Table (CSG-800 series Only)

The **IPS/IDS Security Report** provides comprehensive security analysis based on the selected report criteria. The report includes statistical summaries, threat analysis, activity trends, network analysis, triggered signatures, and detailed event logs. The report sections are shown in Figure 4-76 through Figure 4-83.

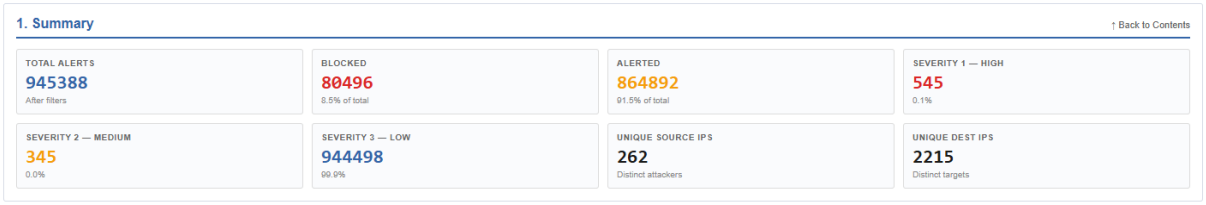


Figure 4-76: Summary

Object	Description
Summary	Displays an overview of IPS/IDS events, including total alerts, blocked and alerted events, severity distribution, and the number of unique source and destination IP addresses.

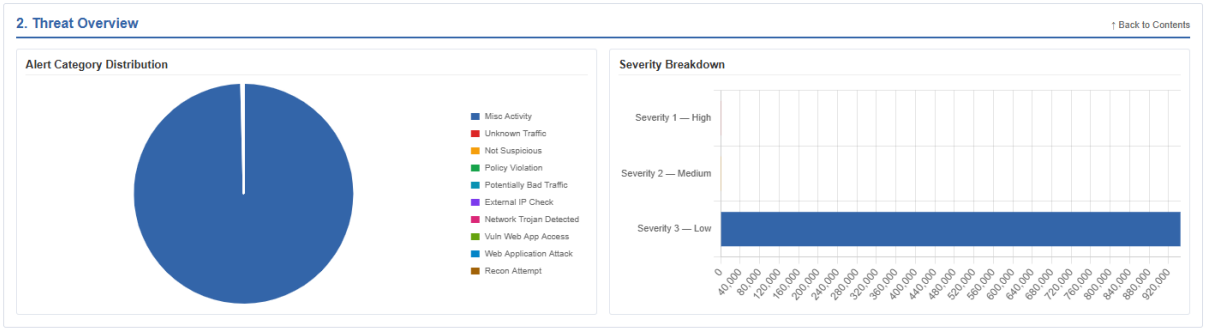


Figure 4-77: Threat Overview

Object	Description
Alert Category Distribution	Displays the distribution of detected threats by category.
Severity Breakdown	Displays the distribution of alerts by severity level.

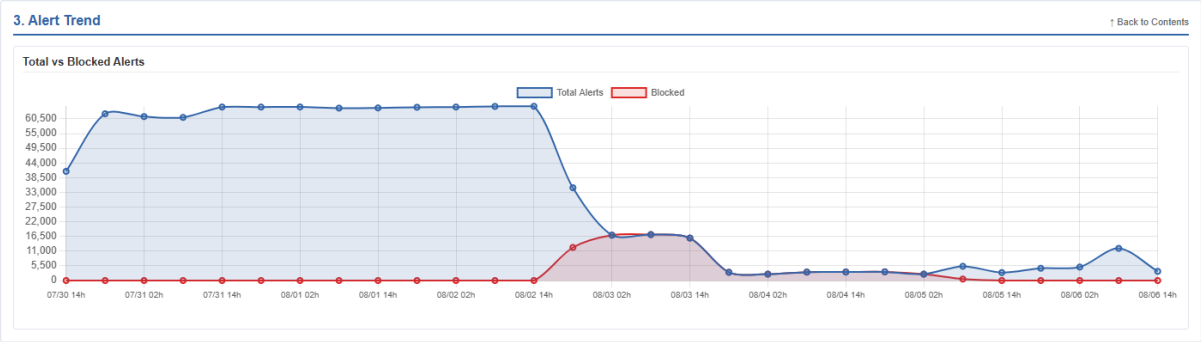


Figure 4-78: Alert Trend

Object	Description
Total vs Blocked Alerts	Displays the trend of total alerts and blocked events over the selected time period.

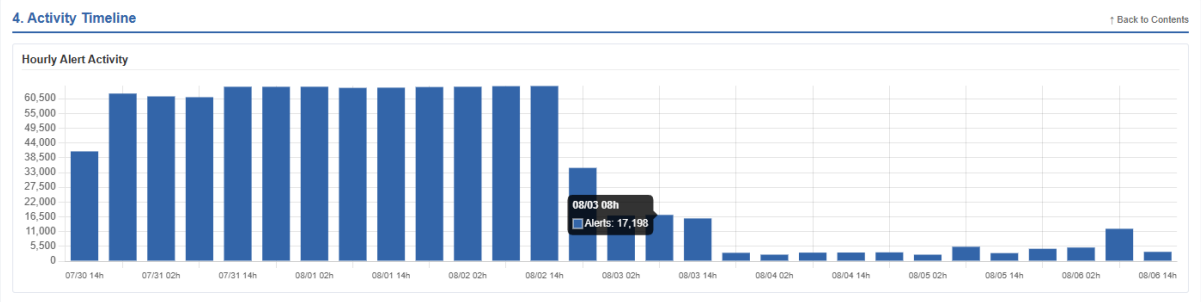


Figure 4-79: Activity Timeline

Object	Description
Hourly Alert Activity	Displays the number of alerts detected during each time interval.

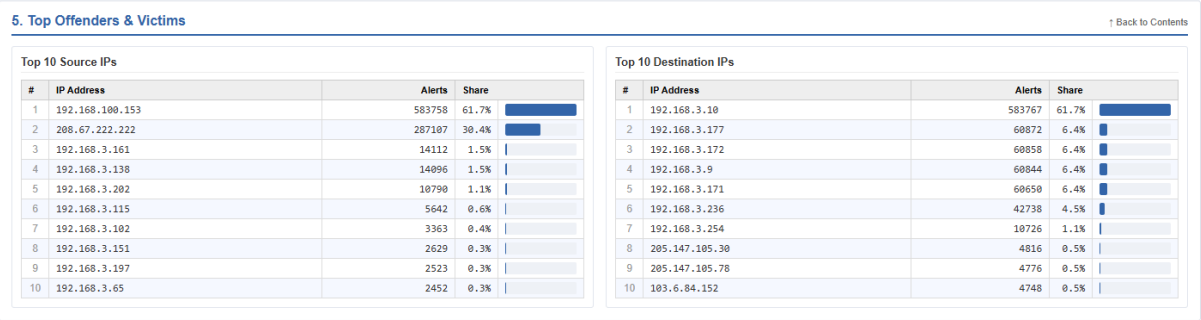


Figure 4-80: Top Offenders & Victims

Object	Description
Top 10 Source IPs	Displays the source IP addresses that generated the highest number of alerts.
Top 10 Destination IPs	Displays the destination IP addresses that received the highest number of alerts.

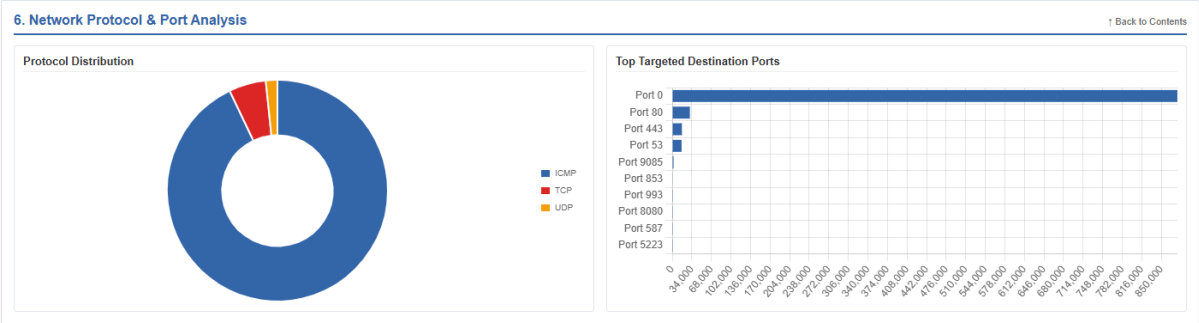
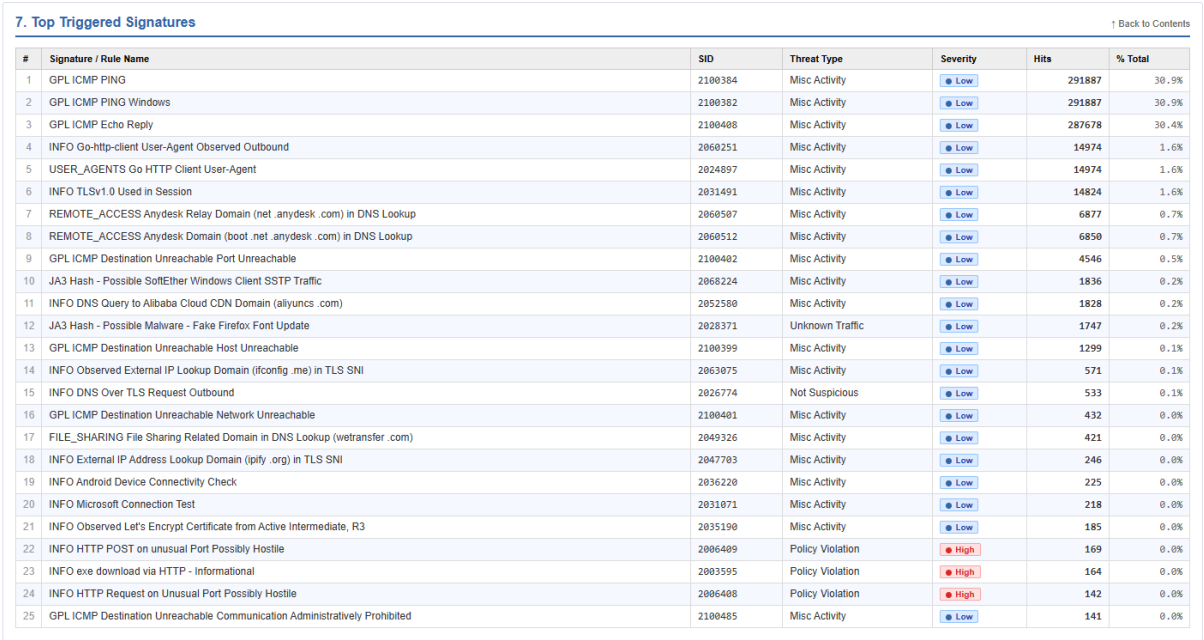


Figure 4-81: Network Protocol & Port Analysis

Object	Description
Protocol Distribution	Displays the distribution of alerts by network protocol.
Top Targeted Destination Ports	Displays the destination ports most frequently involved in detected threats.



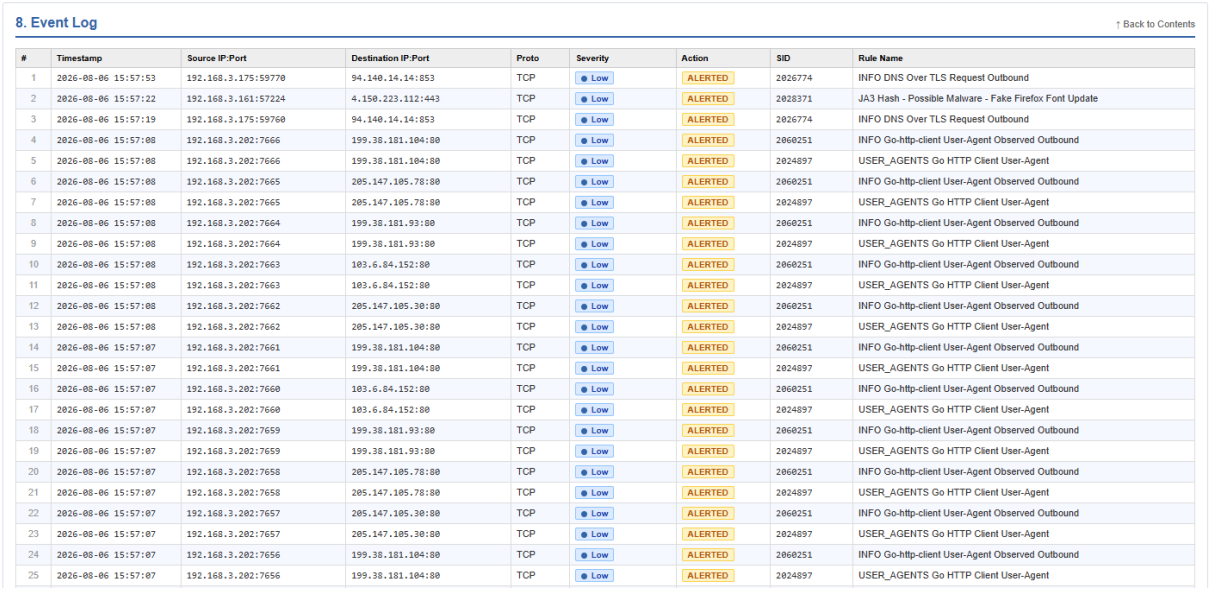
7. Top Triggered Signatures

↑ Back to Contents

#	Signature / Rule Name	SID	Threat Type	Severity	Hits	% Total
1	GPL ICMP PING	2100384	Misc Activity	Low	291887	30.9%
2	GPL ICMP PING Windows	2100382	Misc Activity	Low	291887	30.9%
3	GPL ICMP Echo Reply	2100408	Misc Activity	Low	287678	30.4%
4	INFO Go-http-client User-Agent Observed Outbound	2060251	Misc Activity	Low	14974	1.6%
5	USER_AGENTS Go HTTP Client User-Agent	2024897	Misc Activity	Low	14974	1.6%
6	INFO TLSv1.0 Used in Session	2031491	Misc Activity	Low	14824	1.6%
7	REMOTE_ACCESS Anydesk Relay Domain (net .anydesk .com) in DNS Lookup	2060507	Misc Activity	Low	6877	0.7%
8	REMOTE_ACCESS Anydesk Domain (boot .net .anydesk .com) in DNS Lookup	2060512	Misc Activity	Low	6850	0.7%
9	GPL ICMP Destination Unreachable Port Unreachable	2100402	Misc Activity	Low	4546	0.5%
10	JA3 Hash - Possible SoftEther Windows Client SSTP Traffic	2068224	Misc Activity	Low	1836	0.2%
11	INFO DNS Query to Alibaba Cloud CDN Domain (aliyuncs .com)	2052580	Misc Activity	Low	1828	0.2%
12	JA3 Hash - Possible Malware - Fake Firefox Font Update	2028371	Unknown Traffic	Low	1747	0.2%
13	GPL ICMP Destination Unreachable Host Unreachable	2100399	Misc Activity	Low	1299	0.1%
14	INFO Observed External IP Lookup Domain (ifconfig .me) in TLS SNI	2063075	Misc Activity	Low	571	0.1%
15	INFO DNS Over TLS Request Outbound	2026774	Not Suspicious	Low	533	0.1%
16	GPL ICMP Destination Unreachable Network Unreachable	2100401	Misc Activity	Low	432	0.0%
17	FILE_SHARING File Sharing Related Domain in DNS Lookup (wetransfer .com)	2049326	Misc Activity	Low	421	0.0%
18	INFO External IP Address Lookup Domain (ipify .org) in TLS SNI	2047703	Misc Activity	Low	246	0.0%
19	INFO Android Device Connectivity Check	2036220	Misc Activity	Low	225	0.0%
20	INFO Microsoft Connection Test	2031071	Misc Activity	Low	218	0.0%
21	INFO Observed Let's Encrypt Certificate from Active Intermediate, R3	2035190	Misc Activity	Low	185	0.0%
22	INFO HTTP POST on unusual Port Possibly Hostile	2006409	Policy Violation	High	169	0.0%
23	INFO exe download via HTTP - Informational	2003595	Policy Violation	High	164	0.0%
24	INFO HTTP Request on Unusual Port Possibly Hostile	2006408	Policy Violation	High	142	0.0%
25	GPL ICMP Destination Unreachable Communication Administratively Prohibited	2100485	Misc Activity	Low	141	0.0%

Figure 4-82: Top Triggered Signatures

Object	Description
Top Triggered Signatures	Displays the most frequently triggered IPS/IDS signatures, including SID, threat type, severity, and hit count.



8. Event Log

↑ Back to Contents

#	Timestamp	Source IP:Port	Destination IP:Port	Proto	Severity	Action	SID	Rule Name
1	2026-08-06 15:57:53	192.168.3.175:59770	94.140.14.14:853	TCP	Low	ALERTED	2026774	INFO DNS Over TLS Request Outbound
2	2026-08-06 15:57:22	192.168.3.161:57224	4.150.223.112:443	TCP	Low	ALERTED	2028371	JA3 Hash - Possible Malware - Fake Firefox Font Update
3	2026-08-06 15:57:19	192.168.3.175:59760	94.140.14.14:853	TCP	Low	ALERTED	2026774	INFO DNS Over TLS Request Outbound
4	2026-08-06 15:57:08	192.168.3.202:7666	199.38.181.104:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
5	2026-08-06 15:57:08	192.168.3.202:7666	199.38.181.104:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
6	2026-08-06 15:57:08	192.168.3.202:7665	205.147.105.78:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
7	2026-08-06 15:57:08	192.168.3.202:7665	205.147.105.78:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
8	2026-08-06 15:57:08	192.168.3.202:7664	199.38.181.93:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
9	2026-08-06 15:57:08	192.168.3.202:7664	199.38.181.93:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
10	2026-08-06 15:57:08	192.168.3.202:7663	103.6.84.152:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
11	2026-08-06 15:57:08	192.168.3.202:7663	103.6.84.152:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
12	2026-08-06 15:57:08	192.168.3.202:7662	205.147.105.30:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
13	2026-08-06 15:57:08	192.168.3.202:7662	205.147.105.30:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
14	2026-08-06 15:57:07	192.168.3.202:7661	199.38.181.104:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
15	2026-08-06 15:57:07	192.168.3.202:7661	199.38.181.104:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
16	2026-08-06 15:57:07	192.168.3.202:7660	103.6.84.152:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
17	2026-08-06 15:57:07	192.168.3.202:7660	103.6.84.152:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
18	2026-08-06 15:57:07	192.168.3.202:7659	199.38.181.93:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
19	2026-08-06 15:57:07	192.168.3.202:7659	199.38.181.93:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
20	2026-08-06 15:57:07	192.168.3.202:7658	205.147.105.78:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
21	2026-08-06 15:57:07	192.168.3.202:7658	205.147.105.78:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
22	2026-08-06 15:57:07	192.168.3.202:7657	205.147.105.30:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
23	2026-08-06 15:57:07	192.168.3.202:7657	205.147.105.30:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent
24	2026-08-06 15:57:07	192.168.3.202:7656	199.38.181.104:80	TCP	Low	ALERTED	2060251	INFO Go-http-client User-Agent Observed Outbound
25	2026-08-06 15:57:07	192.168.3.202:7656	199.38.181.104:80	TCP	Low	ALERTED	2024897	USER_AGENTS Go HTTP Client User-Agent

Figure 4-83: Event Log

Object	Description
Event Log	Displays detailed IPS/IDS event records, including timestamp, source and destination information, protocol, severity, action, SID, and rule name.

4.7.11 IPS/IDS SMTP Alerts (CSG-800 series Only)

The **IPS/IDS SMTP Alerts** page allows users to configure email notifications for IPS/IDS events and reports. Users can specify the notification schedule, severity threshold, SMTP server settings, and recipient information. The status is shown in Figure 4-84.

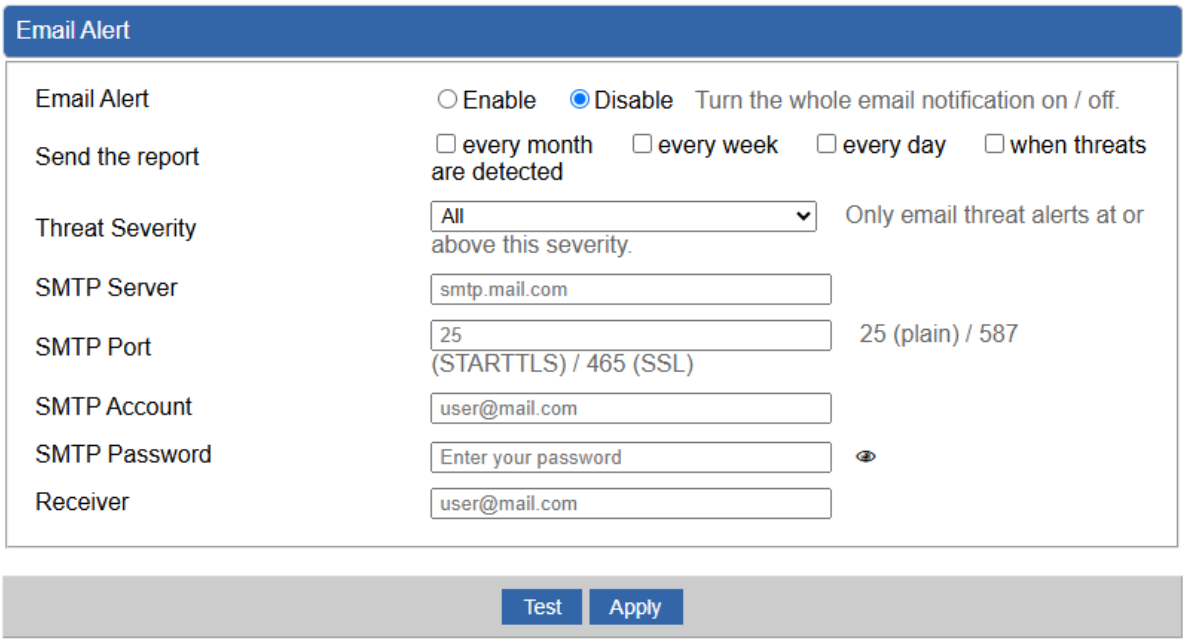


Figure 4-84: IPS/IDS SMTP Alerts

Object	Description
Email Alert	Enable or disable email notifications for IPS/IDS events and reports.
Send the Report	Select when email reports are sent, including **every month**, **every week**, **every day**, or **when threats are detected**.
Threat Severity	Select the minimum severity level required to trigger email notifications.
SMTP Server	Enter the hostname or IP address of the SMTP server.
SMTP Port	pecify the SMTP server port. Supported ports include **25 (Plain)**, **587 (STARTTLS)**, and **465 (SSL)**.
SMTP Account	Enter the SMTP account used for email authentication.
SMTP Password	Enter the password for the SMTP account.
Receiver	Specify the recipient email address for notifications.
Test	Send a test email using the current SMTP configuration.

4.7.12 Certificates

The **Certificates** page allows users to manage the web server certificate and download the system CA certificate. Users can regenerate the web server certificate when the device's IP address or hostname changes and download the CA certificate for HTTPS and VPN server authentication. The status is shown in Figure 4-85.

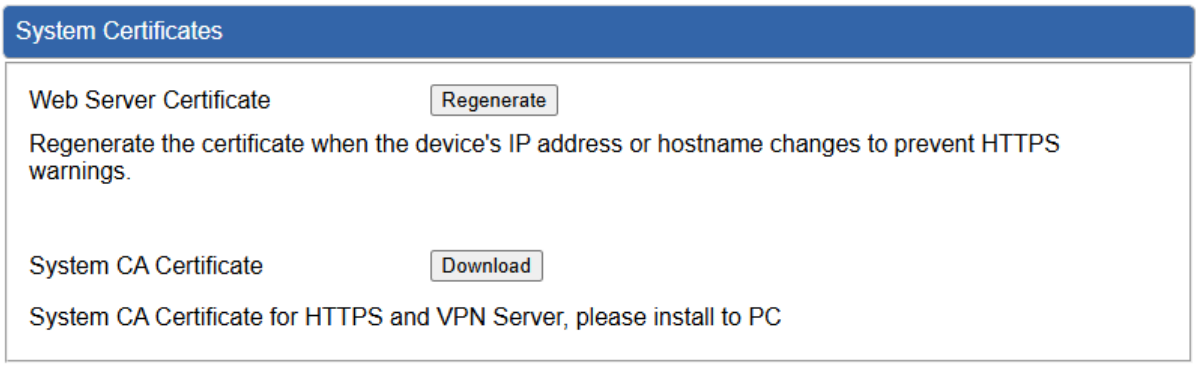


Figure 4-85: Certificates

Object	Description
Web Server Certificate	Displays the current web server certificate settings.
Regenerate	Generate a new web server certificate when the device's IP address or hostname changes to prevent HTTPS certificate warnings.
System CA Certificate	Displays the system CA certificate used for HTTPS and VPN server authentication.
Download	Download the system CA certificate for installation on client devices.

4.8 VPN

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

The Maintenance menu provides the following features for managing the system as Figure 4-86 is shown below:

Figure 4-86: VPN Menu

Object	Description
IPsec	Configure IPSec VPN for secure site-to-site or remote access connections.
IPsec Remote Server	Set up IPSec remote access server for client-to-site VPN connections.
GRE	Configure GRE tunnels for encapsulating network traffic between sites
PPTP	Configure PPTP VPN for legacy remote access connections.
L2TP	Configure L2TP VPN for secure remote access (often combined with IPSec).
SSL VPN Server	Configure SSL VPN server for secure remote user access via encrypted tunnels.
SSL VPN Client	Configure SSL VPN client settings to connect to remote VPN servers.
WireGuard VPN Server	Configure WireGuard VPN server for high-performance secure connections.
WireGuard VPN Client	Configure WireGuard VPN client for connecting to remote peers.
Zero Trust VPN	Configure Zero Trust Network Access (ZTNA) for identity-based secure connectivity.
VPN Connection	Monitor and manage active VPN connections and sessions.
SD WAN	Configure software-defined WAN for intelligent traffic routing and multi-WAN optimization.

4.8.1 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 with 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 allows you to modify the user name and passwords as shown in Figure 4-87.

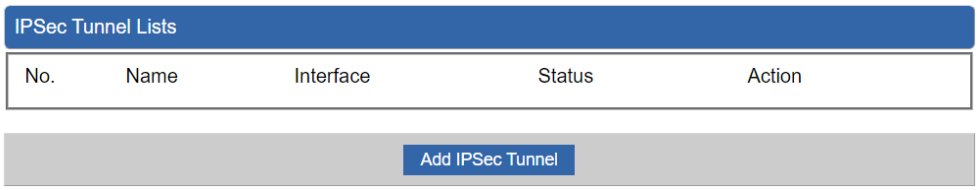


Figure 4-87: IPSec

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

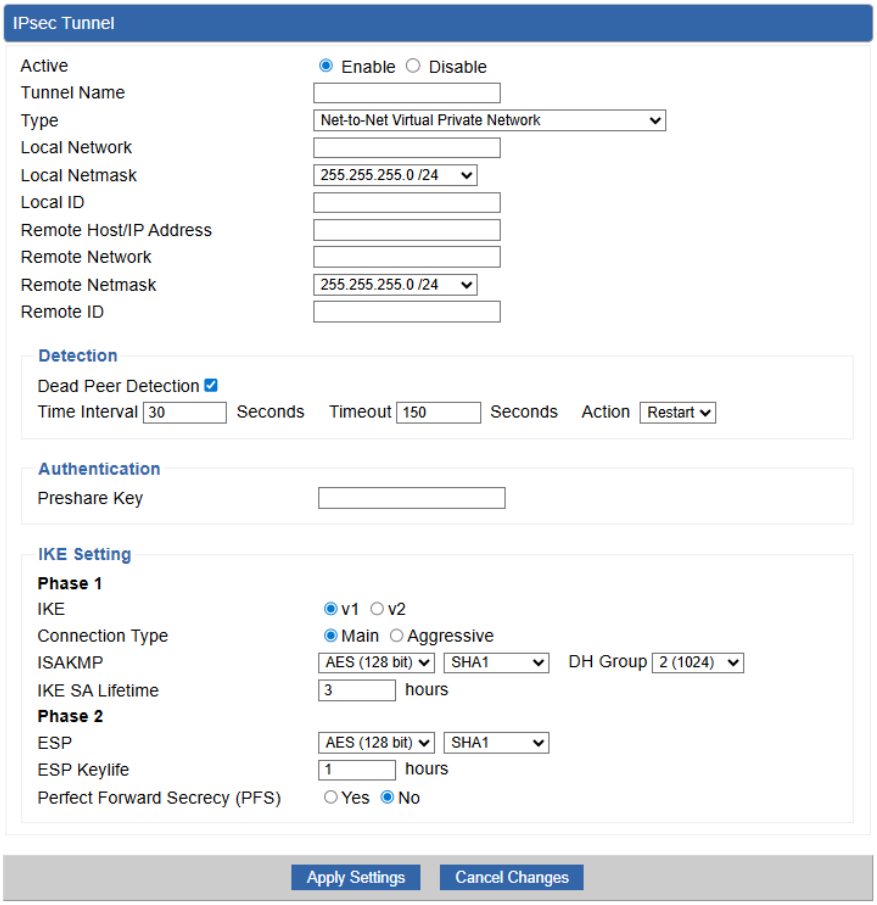


Figure 4-88: IPSec Tunnel

Object	Description
IPSec Tunnel Enable	Check the box to enable the function.
Tunnel Name	Enter any words for recognition.
Interface	This is only available for host-to-host connections and it specifies to which interface the host is connecting. 1. WAN 1. 2. WAN 2.
Local Network	The local subnet in CIDR notation. For instance, "192.168.1.0".
Local Netmask	The netmask of this router.
Remote IP Address	Input the IP address of the remote host. For instance, "210.66.1.10".
Remote Network	The remote subnet in CIDR notation. For instance, "210.66.1.0".
Remote Netmask	The netmask of the remote host.
Dead Peer Detection	Set up the detection time of **DPD** (Dead Peer Detection). By default, the DPD detection's gap is 30 seconds; if is over 150 seconds, the line is broken. When VPN detects an opposite party's reaction time, the function will take one of the actions: "Hold" means the system will retain IPSec SA. "Clear" means the tunnel is clear and waits for the new sessions. "Restart" will delete the IPSec SA and reset VPN tunnel.
Preshare Key	Enter a pass phrase to be used to authenticate the other side of the tunnel. Should be the same as the remote host.
IKE	Select the IKE (Internet Key Exchange) version.
Connection Type	1. Main. 2. Aggressive.
ISAKMP	It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways. 1. **AES**: if a 128-bit, 192-bit and 256-bit key is used, AES is a commonly seen and adopted nowadays.

	2. **3DES**: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. **SHA1**: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. **SHA2**: Either 256, 384 or 512 can be chosen 5. **MD5 Algorithm**: MD5 processes a variably long message into a fixed-length output of 128 bits. 6. **DH Group**: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen.
IKE SA Lifetime	You can specify how long IKE packets are valid.
ESP	It offers AES, 3 DES, SHA 1, SHA2, and MD5. 1. **AES**: If a 128-bit, 192-bit and 256-bit key is used, AES is a commonly seen and adopted nowadays. 2. **3DES**: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. **SHA1:** The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. **SHA2**: Either 256, 384 or 512 can be chosen. 5. **MD5 Algorithm**: MD5 processes a variably long message into a fixed-length output of 128 bits.
ESP Keylife	You can specify how long ESP packets are valid.
Perfect Forward Secrecy (PFS)	Set the function as enable or disable.

4.8.2 IPSec Remote Server

This section assists you in setting the GRE Tunnel as shown in Figure 4-89

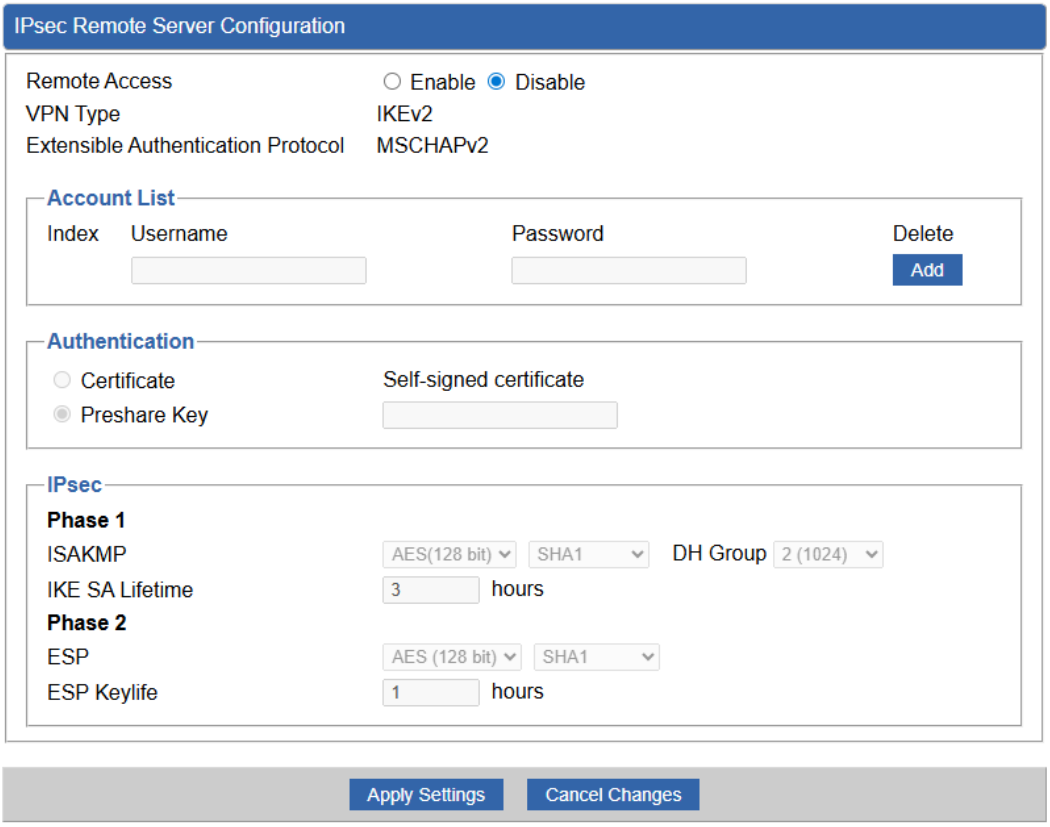


Figure 4-89: IPSec Remote Server

Object	Description
Remote Access	Enable or disable IPSec remote access server functionality.
Account List	Configure user accounts for IPSec remote access authentication.
Certificate	Use a certificate (e.g., self-signed certificate) for authentication.
Preshare Key	Configure a pre-shared key for VPN authentication.
ISAKMP	Select encryption and authentication algorithms (e.g., AES, SHA1).
DH Group	Define the Diffie-Hellman group used for key exchange.
IKE SA Lifetime	Specify the lifetime of the IKE security association (in hours).
ESP	Select encryption and authentication algorithms for data protection.
ESP Keylife	Define the lifetime of the ESP security association (in hours).

4.8.3 GRE

This section assists you in setting the GRE Tunnel as shown in Figure 4-90.

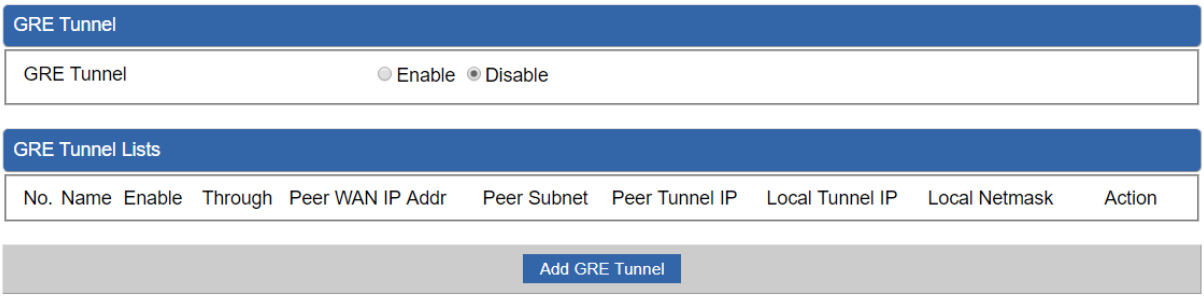


Figure 4-90: GRE

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.

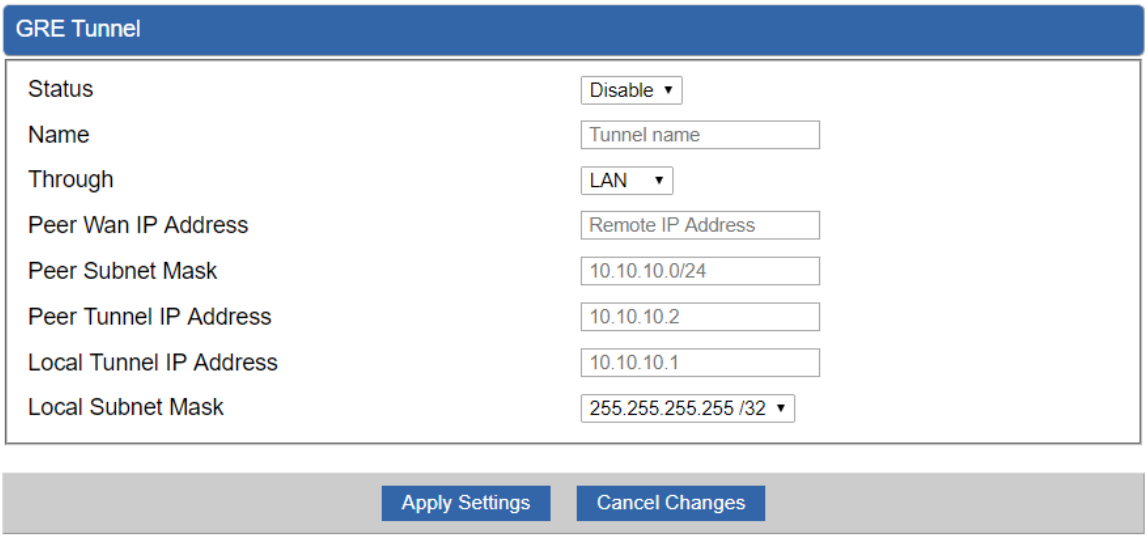


Figure 4-91: GRE Tunnel

Object	Description
Active	Check the box to enable the function.
Tunnel Name	Enter any words for recognition.
Through	This is only available for host-to-host connections and specifies to which interface the host is connecting. 1. LAN.

	2. WAN 1. 3. WAN 2.
Peer WAN IP Address	Input the IP address of the remote host. For instance, "210.66.1.10”.
Peer Netmask	The remote subnet in CIDR notation. For instance, "210.66.1.0/24”.
Peer Tunnel IP Address	Input the Tunnel IP address of remote host.
Local Tunnel IP Address	Input the Tunnel IP address of remote host.
Local Netmask	Input the Tunnel IP address of the router.

4.8.4 PPTP

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 4-92.

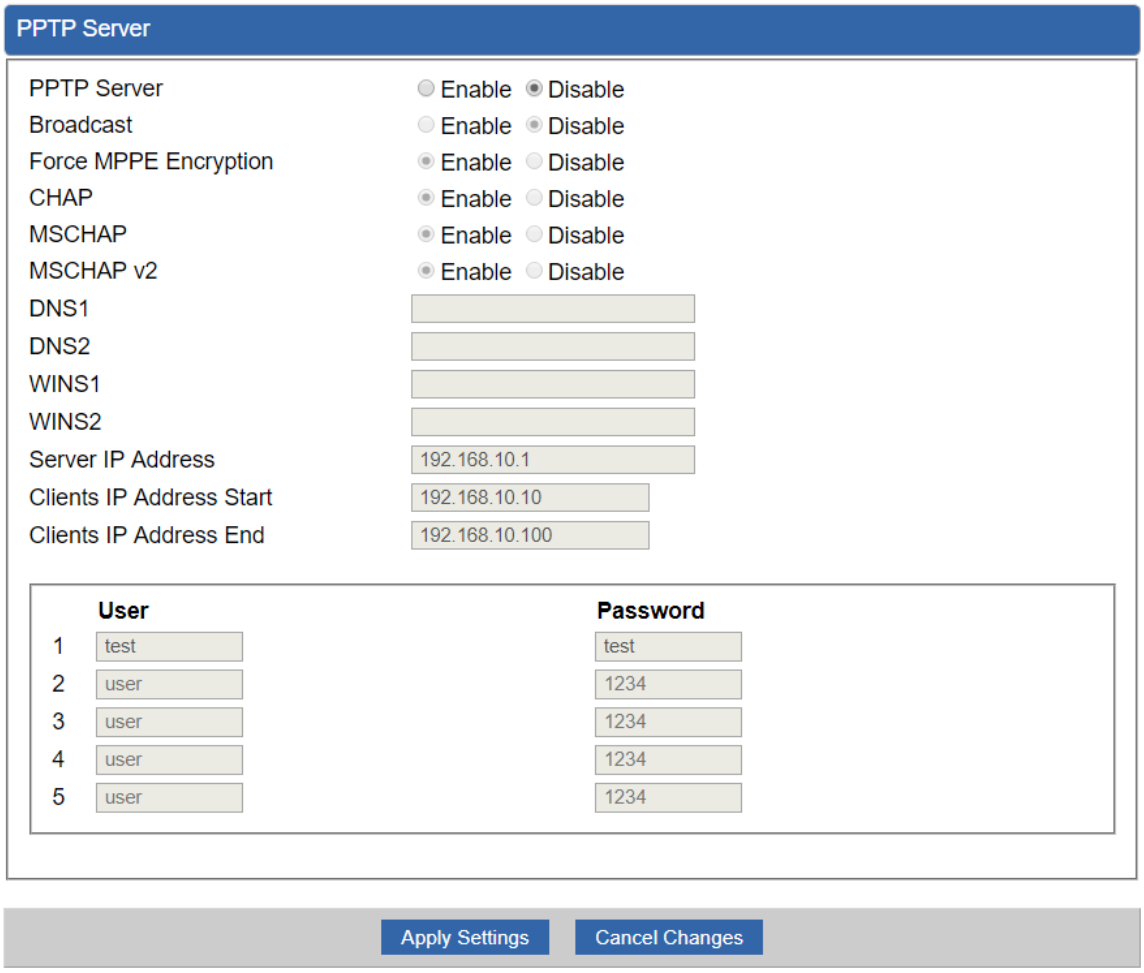


Figure 4-92: PPTP server

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

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

4.8.5 L2TP

This section assists you in setting the L2TP Server as shown in Figure 4-93.

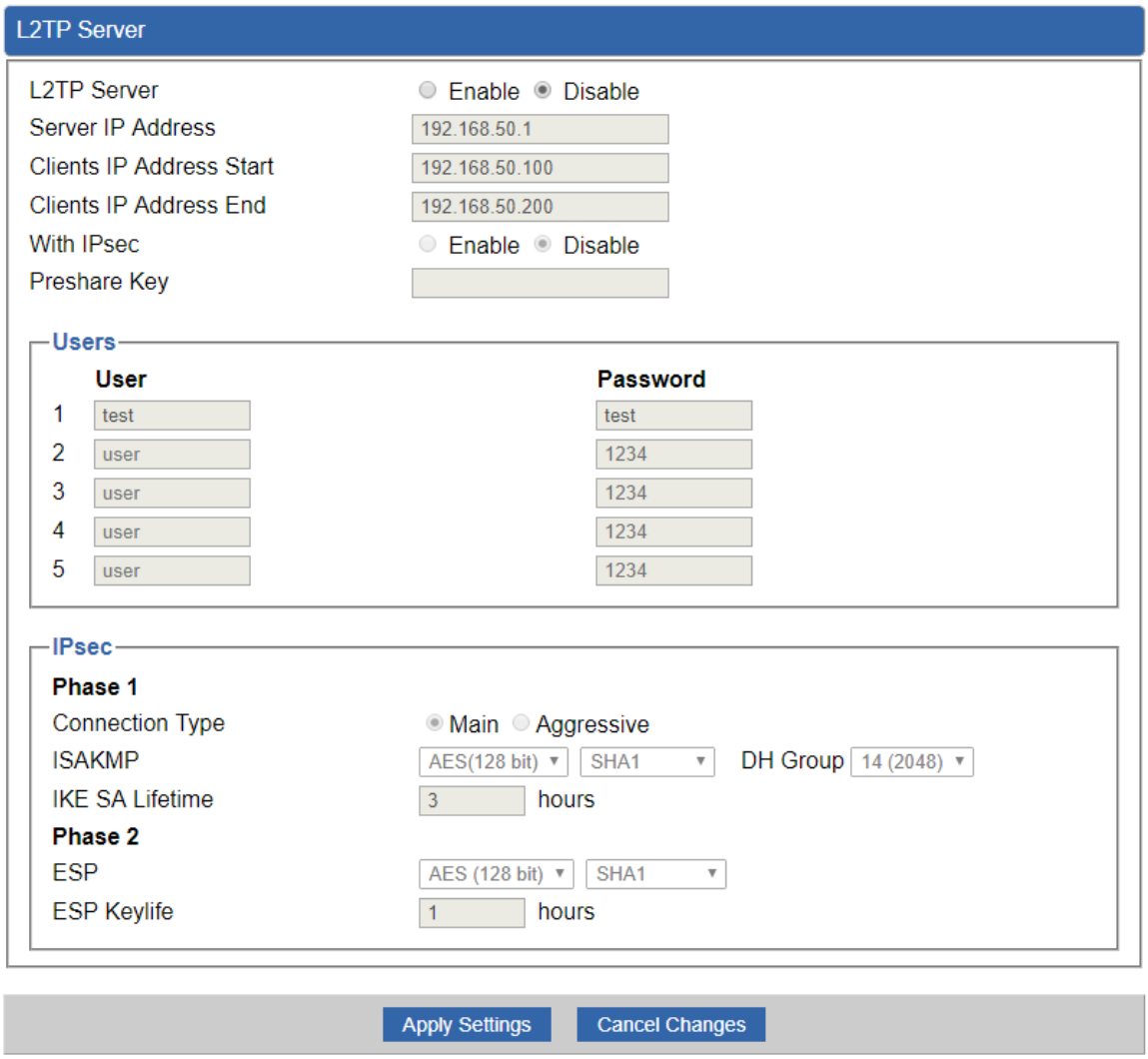


Figure 4-93: L2TP Server

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

Object	Description
	encryption.
Preshare Key	Enter a pass phrase.
User and Password	Create the username and password for the VPN client.
Connection Type	1. Main. 2. Aggressive.
ISAKMP	It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways. 1. AES: If a 128-bit, 192-bit and 256-bit key is used, AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen. 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits. 6. DH Group: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen.
IKE SA Lifetime	You can specify how long IKE packets are valid.
ESP	It offers AES, 3 DES, SHA 1, SHA2, and MD5. 1. AES: If a 128-bit, 192-bit and 256-bit key is used, AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen. 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits.
ESP Keylife	You can specify how long ESP packets are valid.

4.8.6 SSL VPN Server

This section assists you in setting the SSL VPN Server as shown in Figure 4-94.

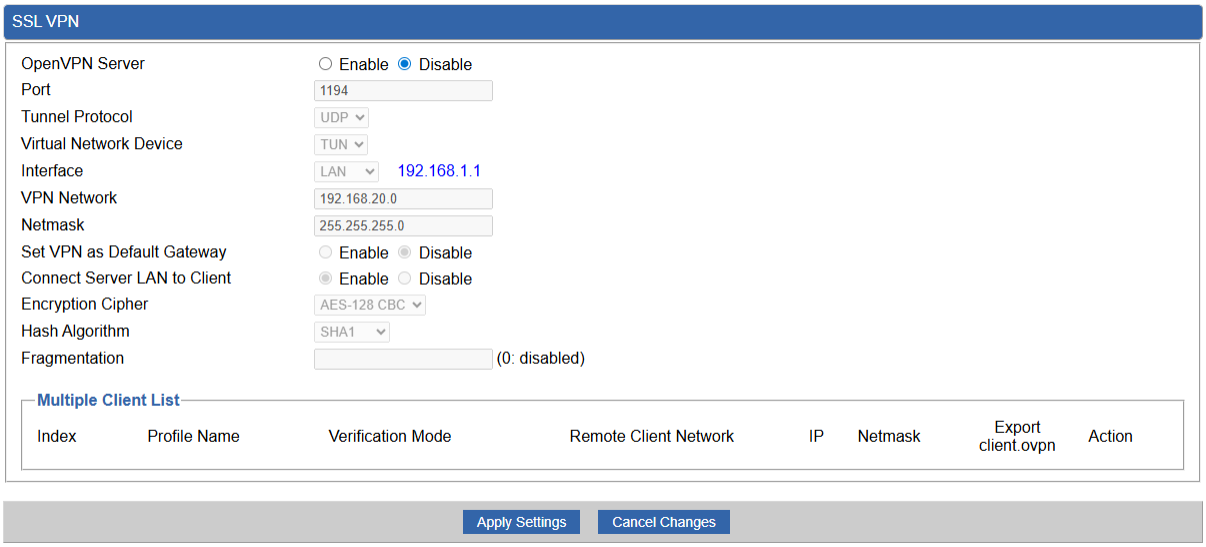


Figure 4-94: SSL VPN Server

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 usage.
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).

4.8.7 SSL VPN Client

This section assists you in setting the SSL VPN Client as shown in Figure 4-95.

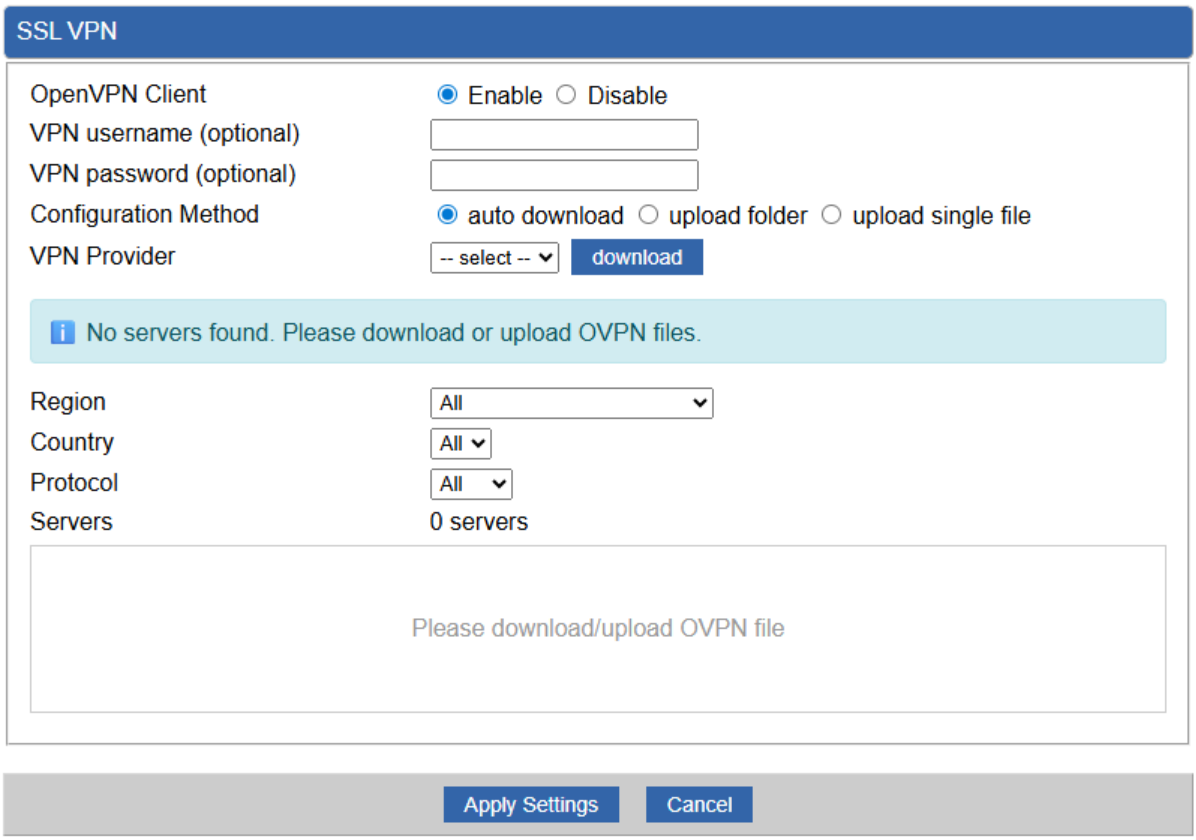


Figure 4-95: SSL VPN Client

Object	Description
OpenVPN Client	Set the function as enable or disable.
VPN Username (optional)	Enter the username for VPN authentication if required by the provider.
VPN Password (optional)	Enter the password for VPN authentication if required by the provider.
Configuration Method	Select the method to obtain VPN configuration (auto download, upload folder, or upload single file).
VPN Provider	Select a predefined VPN provider and download configuration files.
Region	Filter available VPN servers by region.
Country	Filter available VPN servers by country.
Protocol	Filter available VPN servers by protocol type.client (such as Open VPN software).

4.8.8 WireGuard VPN Server

This section assists you in setting the WireGuard VPN Server as shown in Figure 4-96.

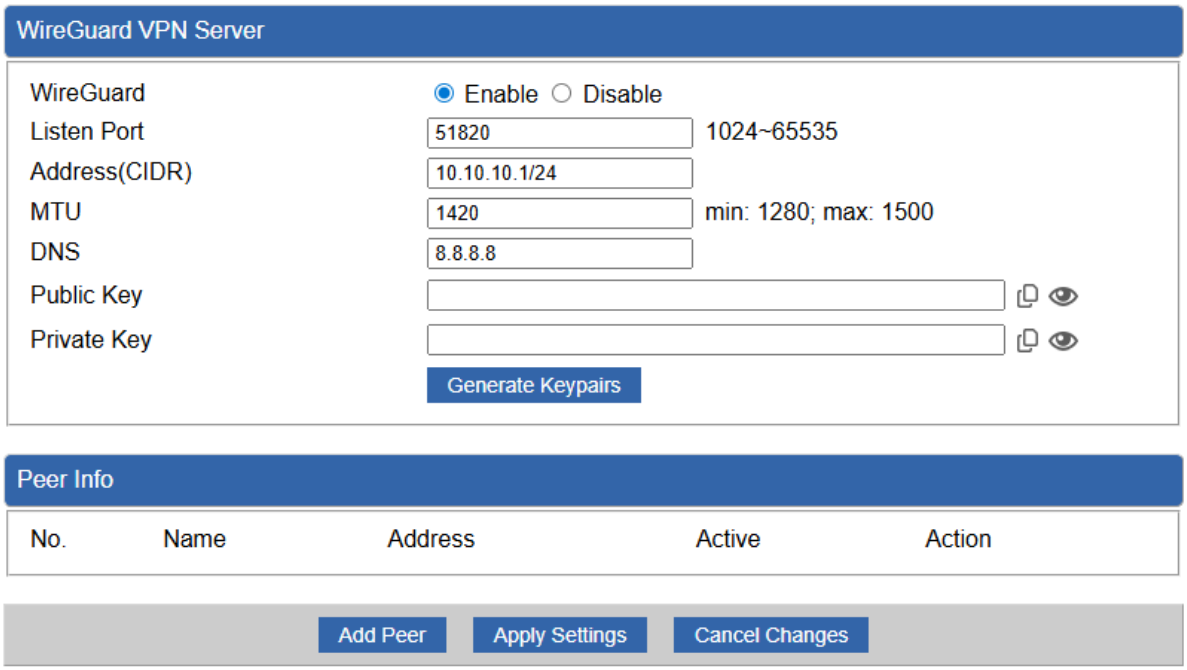


Figure 4-96: WireGuard VPN Server

Object	Description
WireGuard	Set the function as enable or disable.
Listen Port	Specify the UDP port used by the WireGuard server (range: 1024–65535).
Address (CIDR)	Define the VPN network address and subnet in CIDR notation.
MTU	Set the Maximum Transmission Unit for the tunnel (range: 1280–1500).
DNS	Specify the DNS server assigned to VPN clients.
Public Key	Display or enter the public key used for WireGuard communication.
Private Key	Display or enter the private key used for secure authentication.

4.8.9 WireGuard VPN Client

This section assists you in setting the WireGuard VPN Client as shown in Figure 4-97.

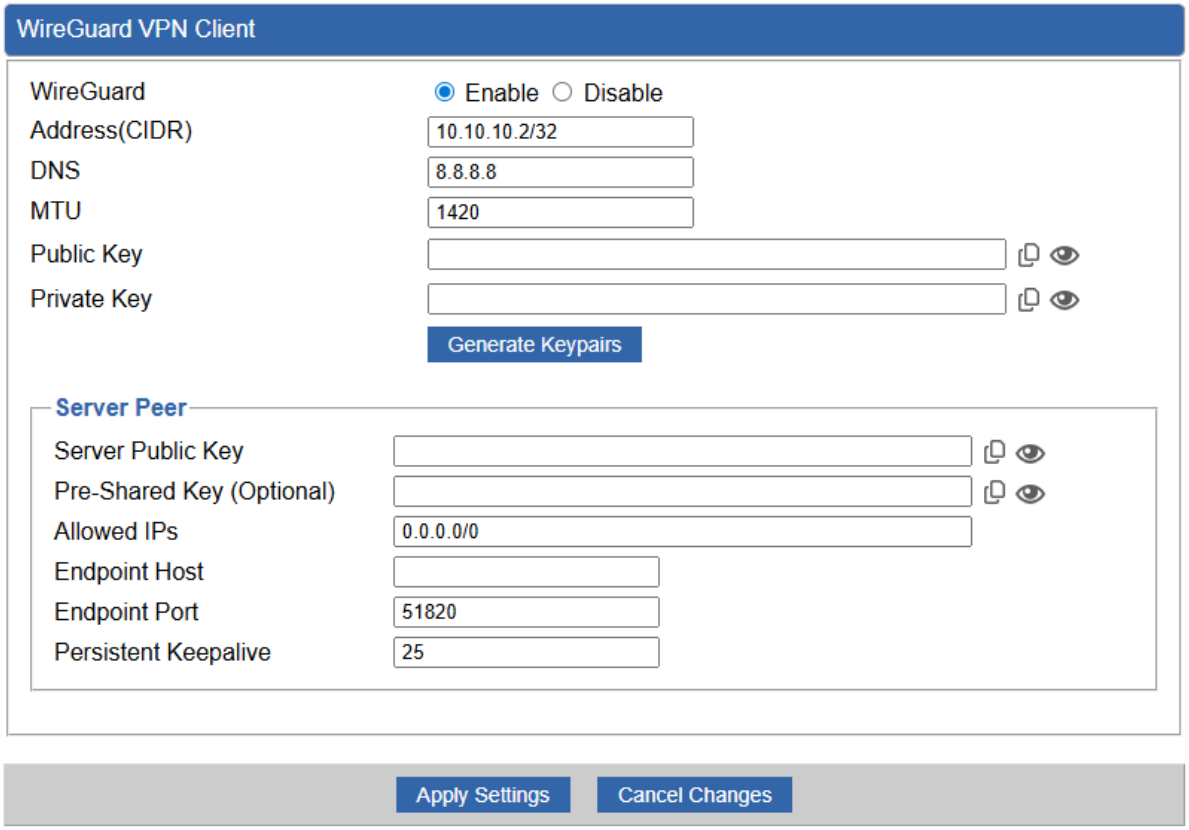


Figure 4-97: WireGuard VPN Client

Object	Description
WireGuard	Set the function as enable or disable.
Address (CIDR)	Define the client IP address and subnet in CIDR notation.
DNS	Specify the DNS server used by the VPN client.
MTU	Set the Maximum Transmission Unit for the VPN tunnel.
Public Key	Display or enter the client public key.
Private Key	Display or enter the client private key for authentication.
Server Public Key	Enter the public key of the WireGuard server.
Pre-Shared Key (Optional)	Configure an optional pre-shared key for additional security.
Allowed IPs	Define the IP ranges routed through the VPN tunnel (e.g., 0.0.0.0/0 for full tunnel).
Endpoint Host	Specify the domain name or IP address of the VPN server.
Endpoint Port	Specify the port used by the VPN server.
Persistent Keepalive	Set keepalive interval (in seconds) to maintain NAT traversal.

4.8.10 Zero Trust VPN (ZT-800 & CSG-800 series Only)

This section assists you in setting the Zero Trust VPN as shown in Figure 4-98.

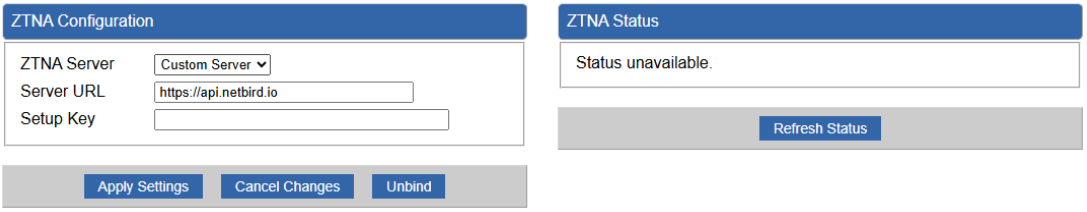


Figure 4-98: Zero Trust VPN

Object	Description
ZTNA Server	Select the ZTNA server type.
Server URL	Specify the URL of the ZTNA controller/server.
Setup Key	Enter the setup key used to register and authenticate the device with the ZTNA server.
Unbind	Remove the device binding from the ZTNA server.

4.8.11 VPN Connection

This page shows the VPN connection status as shown in Figure 4-99.

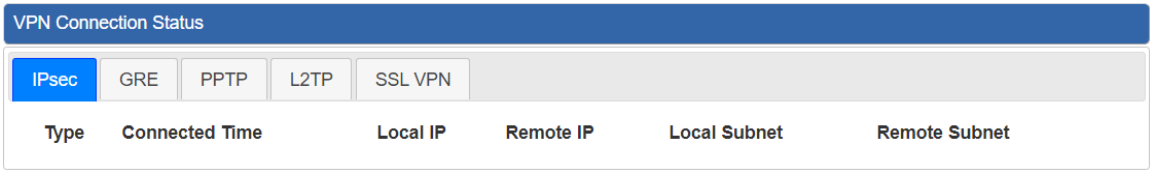


Figure 4-99: VPN Connection Status

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

4.8.12 SD WAN

This section assists you in setting the SD WAN as shown in Figure 4-100.

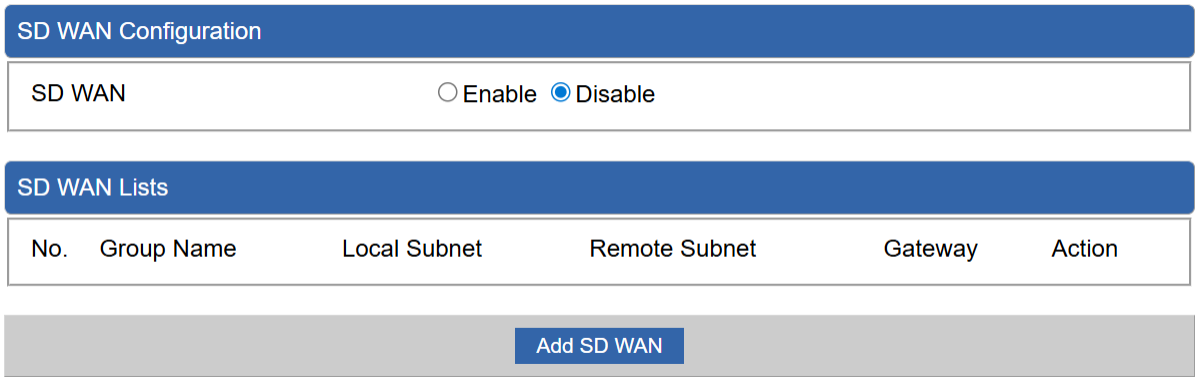


Figure 4-100: SD WAN

Object	Description
SD WAN	Set the function as enable or disable

4.9 AP Control

The AP Control menu provides the following features for managing the system as Figure 4-101 is shown below:

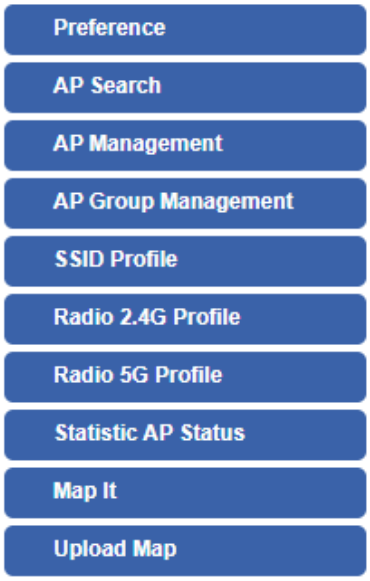


Figure 4-101: AP Control Menu

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

4.9.1 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.

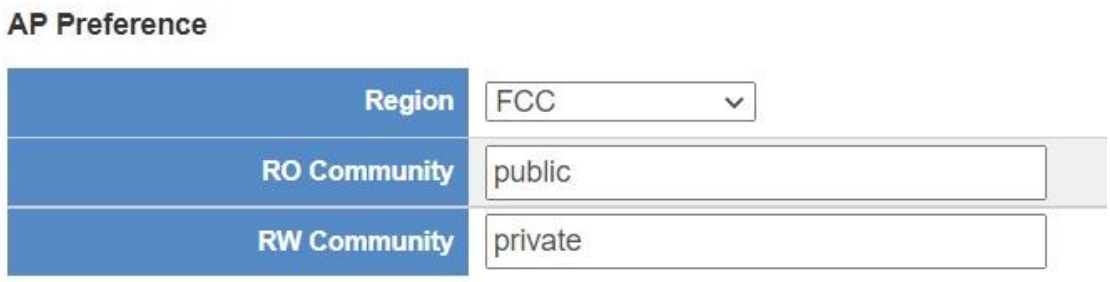


Figure 4-102: AP Preference

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

4.9.2 AP Search

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

Follow the steps:

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

Step 2. Wait for a while and the choose which AP you want to add to.

Step 3. Press the Apply button to finish addition.

Figure 4-103: AP Search

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

4.9.3 AP Management

On this page, you can manage your APs, including checking AP online status, configuring AP (IP address, Mask, SSID and Radio profile), rebooting AP, firmware update, and deleting AP in the AP Control system.

Status

Figure 4-104: AP Management

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

Action

Object	Description
	Setting: edit setting and allocate profile to AP
	Link: link to the AP's web page
	Firmware Update: Upgrade AP's firmware
	Reboot: Reboot the AP
	Delete: Delete the AP from the control list LED Control: Control the AP's LED.
	Mouse-click in a sequential order: LED blink-> LED off-> LED on

Note:

1. To configure multiple APs one at a 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 setting up of AP is done, you need to press the Apply button to complete the setup.

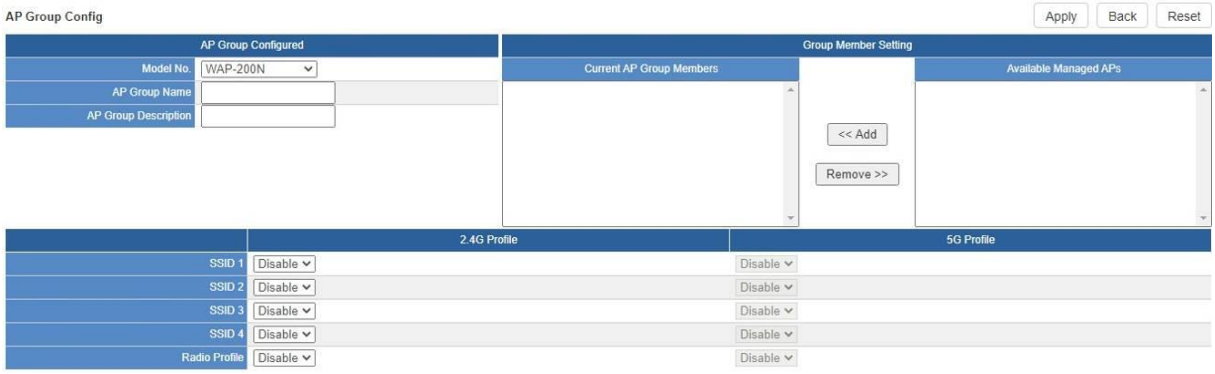
4.9.4 AP Group Management

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

Figure 4-105: AP Group Management

Action:

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



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 the Add button.
4. Select AP Group SSID profile and Radio Profile.
5. Press the Apply button to finish the job..

Note:

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

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

4.9.5 SSID Profile

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

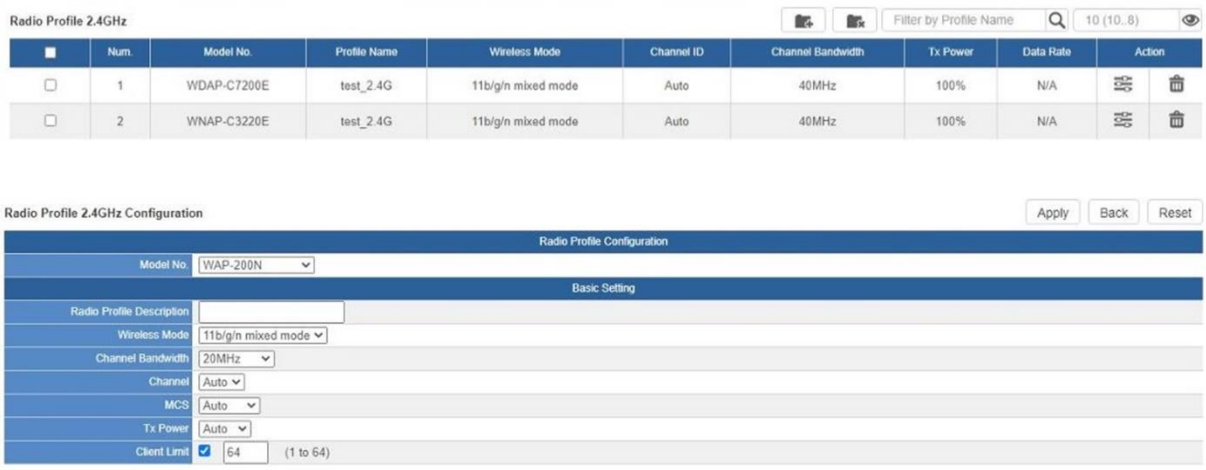


Figure 4-106: SSID Profile

Action:

Object	Description
	Add new profile: Click it to add a new profile.
	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
	Delete: Click it to delete the single profile.

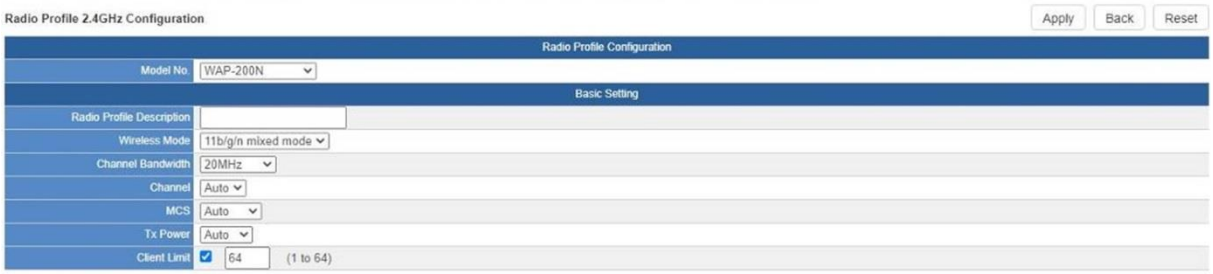
4.9.6 Radio 2.4G Profile

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

Figure 4-107: Radio 2.4G Profile

Action:

Object	Description
	Add new profile: Click it to add a new profile.
	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
	Delete: Click it to delete the single profile.



Note:

1. 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.

4.9.7 Radio 5G Profile

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

Figure 4-108: Radio 5G Profile

Action:

Object	Description
	Add new profile: Click it to add a new profile.
	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
	Delete: Click it to delete the single profile.

Note:

1. 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.

4.9.8 Statistics AP Status

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

Figure 4-109: Statistics AP Status

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.

4.9.9 Statistics Active Clients

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

Figure 4-110: Statistics Active Client

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.

4.9.10 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.

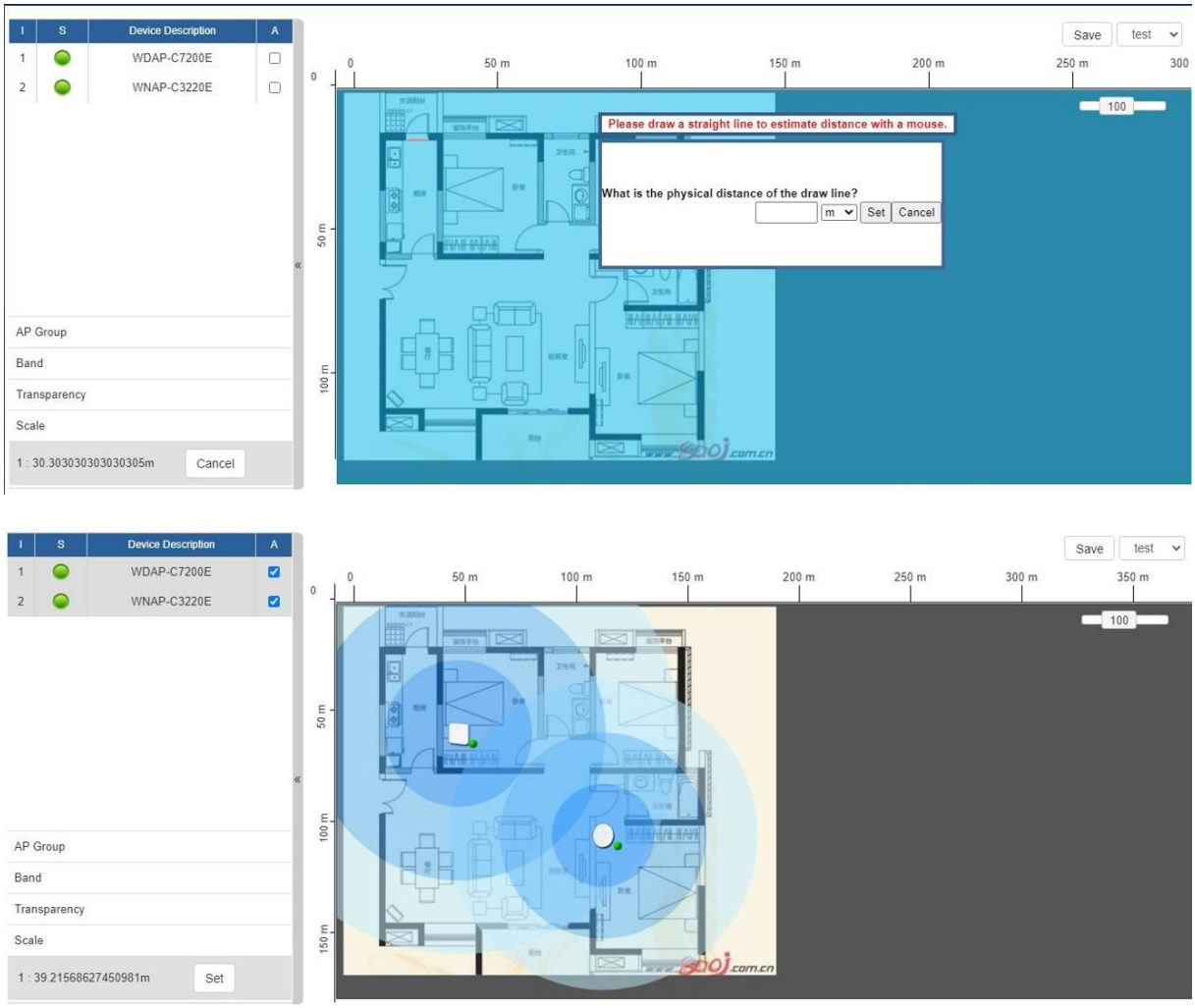


Figure 4-111: Map it

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 can be placed in their the actual position.

4.9.11 Upload Map

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

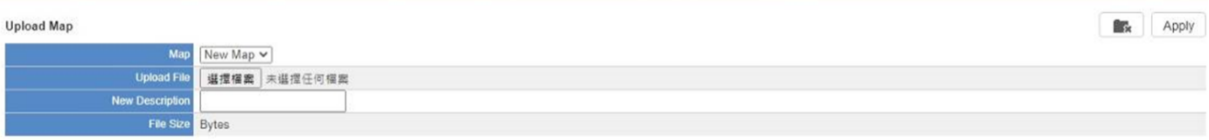


Figure 4-112: Upload Map

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

4.10 Power over Ethernet

This chapter is for PoE models only, ex. XVR-800P.

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

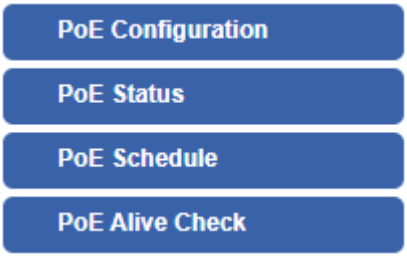


Figure 4-113: Power over ethernet Menu

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

4.10.1 PoE Configuration

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

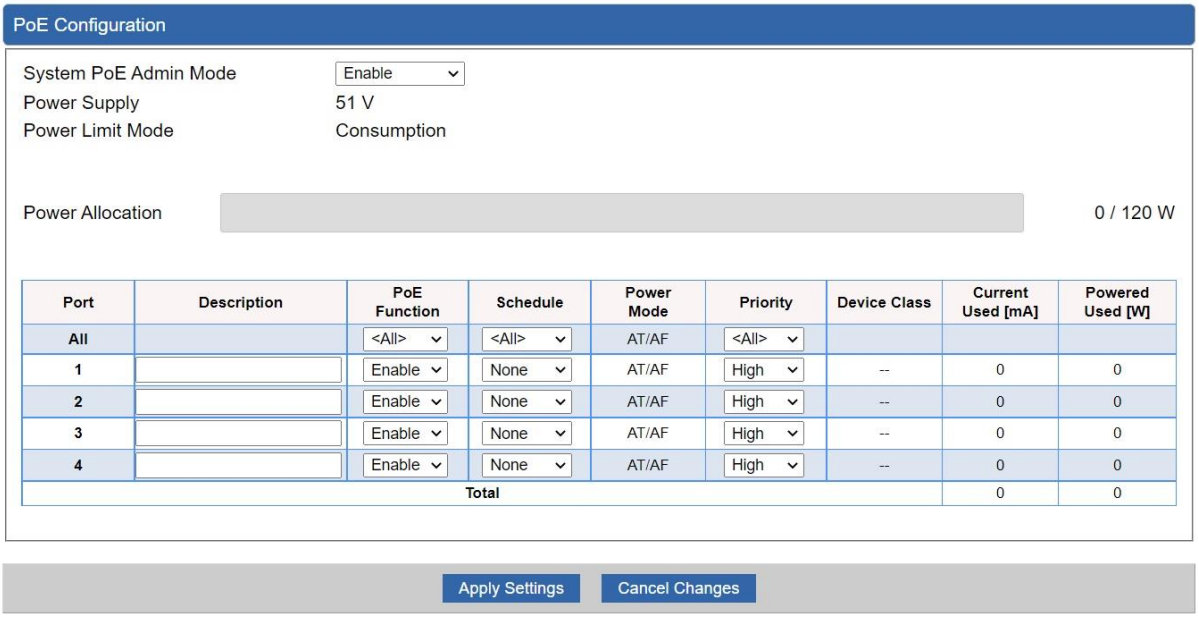


Figure 4-114: PoE Configuration

Object	Description
• **System PoE Admin Mode**	Allows user to enable or disable PoE function. It will cause all of PoE ports to supply or not to supply power.
• **PoE Function**	There are three modes for PoE mode. ■ **Enable**: enable PoE function.. ■ **Disable**: 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 **Power Used** shows how much current the PD currently is using.
• **Powered Used [W]**	The **Power Used** shows how much power the PD currently is using.

4.10.2 PoE Status

This section provides per port PoE status.

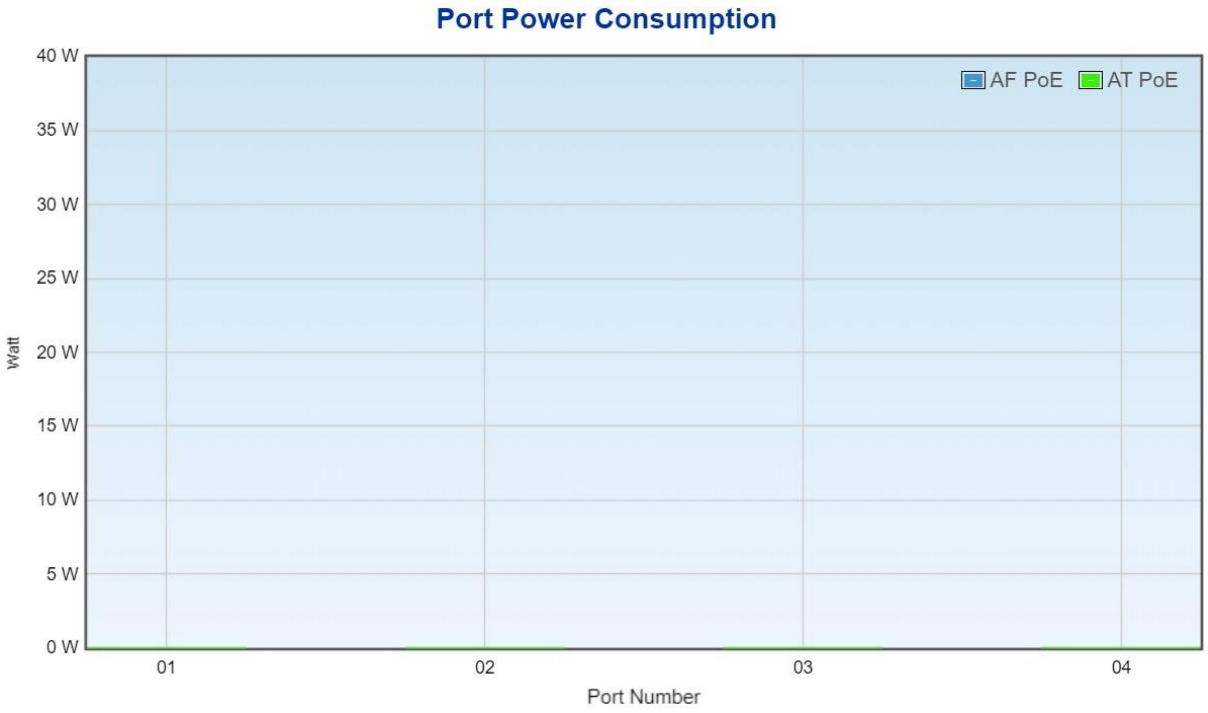


Figure 4-115: PoE Status

4.10.3 PoE Schedule

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

Please press the **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.

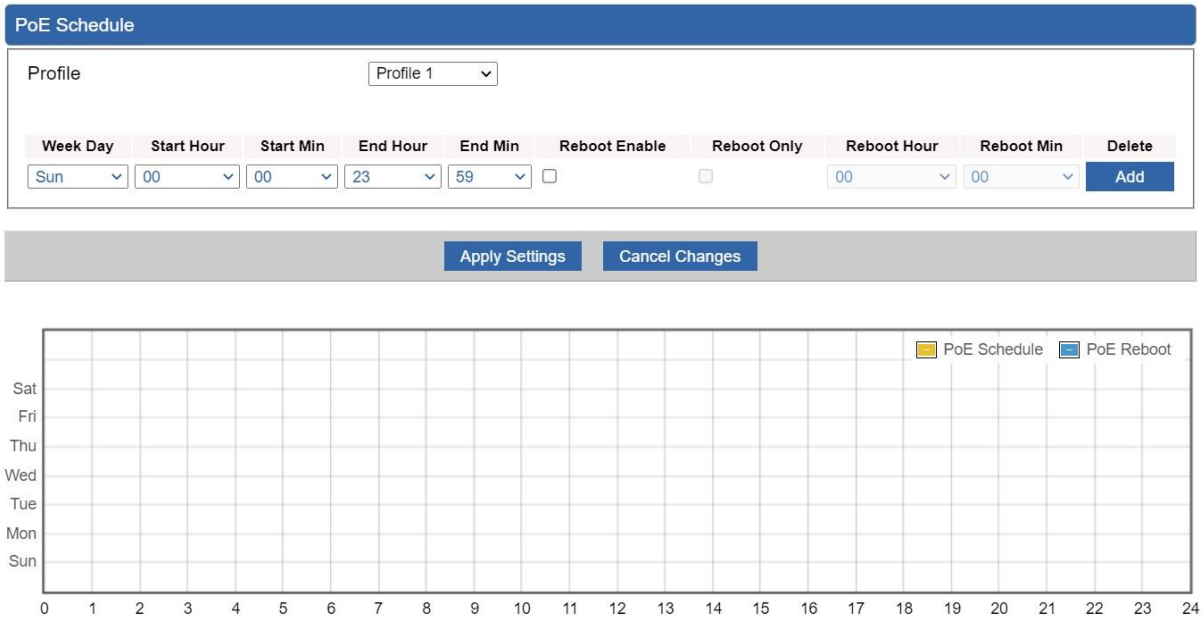


Figure 4-116: PoE Schedule

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 **Reboot Only** 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.

4.10.4 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.

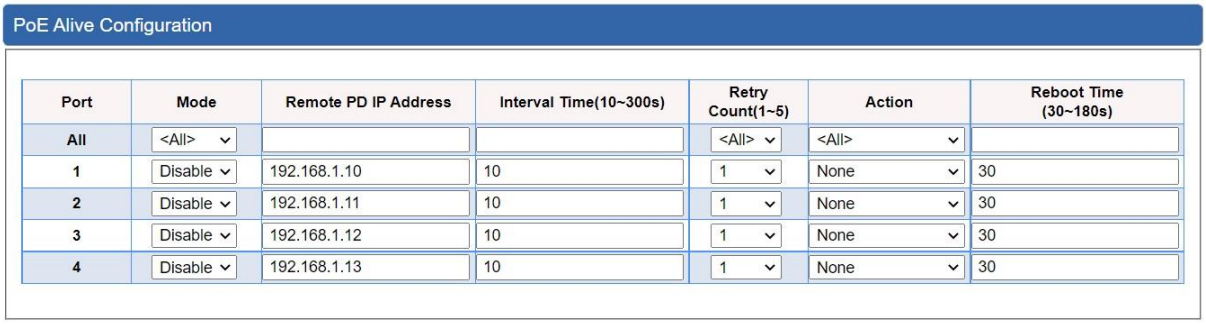


Figure 4-117: PD Alive Check

Object	Description
• **Mode**	Allows user to enable or disable per port PD Alive Check function. By default, all ports are disabled.
• **Remote PD IP Address**	This column allows user to set PoE device IP address for system 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 (10~300s)**	This column allows user to set how long system should issue a ping request to PD for detecting whether PD is alive or dead. Interval time range is from 10 seconds to 300 seconds.
• **Retry Count (1~5)**	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 (30~180s)**	This column allows user to set the PoE device rebooting time as 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.

4.11 Wireless

This chapter is for wireless models only, ex. XVR-800BE, XVR-800BE-NR and ZT-800BE.

The Wireless menu provides the following features for managing the system

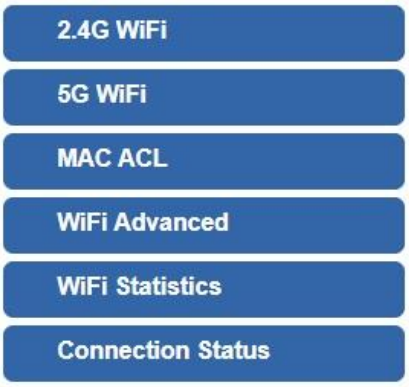


Figure 4-118: Wireless Menu

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

4.11.1 2.4G Wi-Fi

This page allows the user to define 2.4G Wi-Fi.

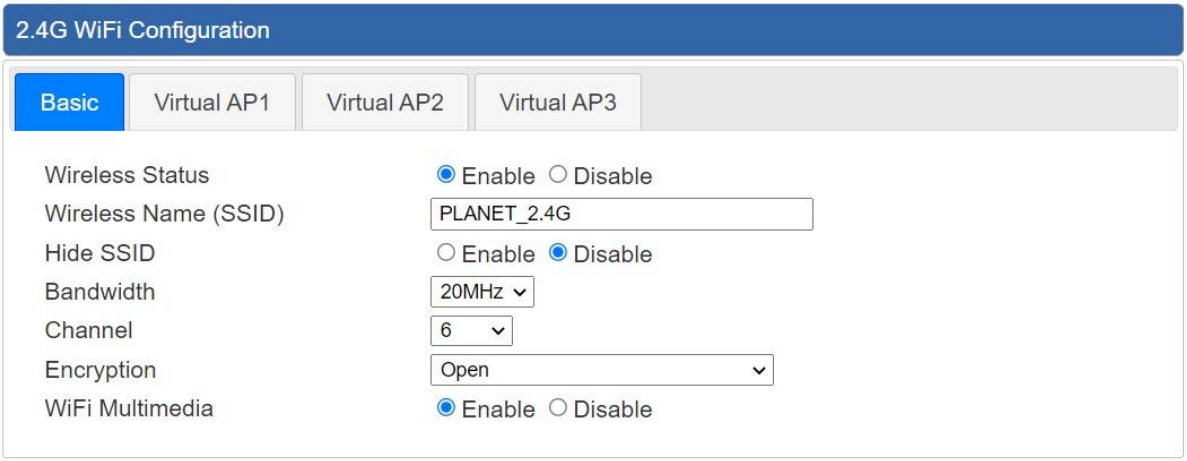


Figure 4-119: 2.4G Wifi Configuration

Object	Description
Wireless Status	Allows user to enable or disable 2.4G Wi-Fi
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 "**Open**"
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

4.11.2 5G Wi-Fi

This page allows the user to define 5G Wi-Fi.

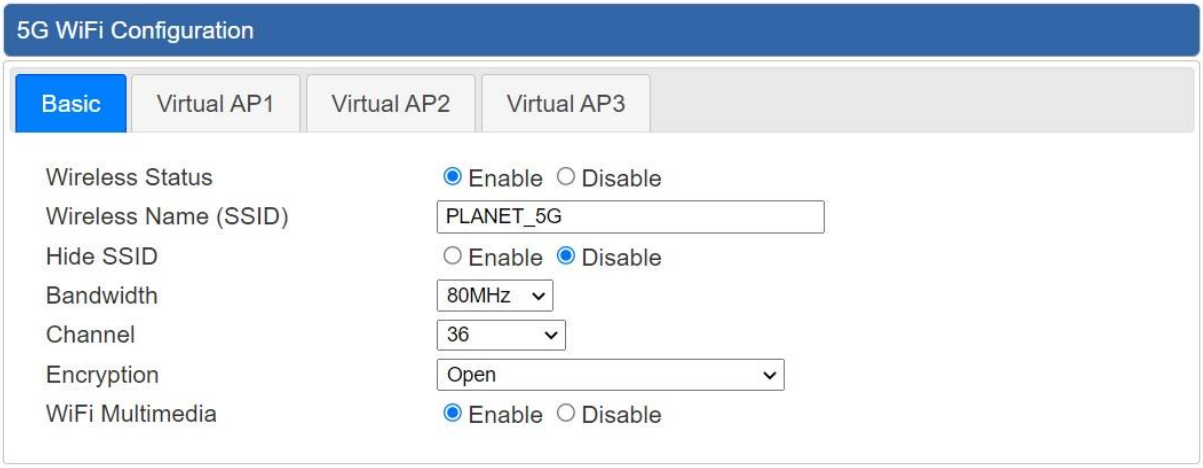


Figure 4-120: 5G Wifi Configuration

Object	Description
Wireless Status	Allows user to enable or disable 5G Wi-Fi
Wireless Name (SSID)	It is the wireless network name. The default 5G SSID is "PLANET_5G"
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, "**20MHz**" or "**40MHz**" or "**80MHz**"
Channel	It shows the channel of the CPE. Default 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is "**Open**"
WiFi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

4.11.3 MAC ACL

This page allows the user to define MAC ACL.

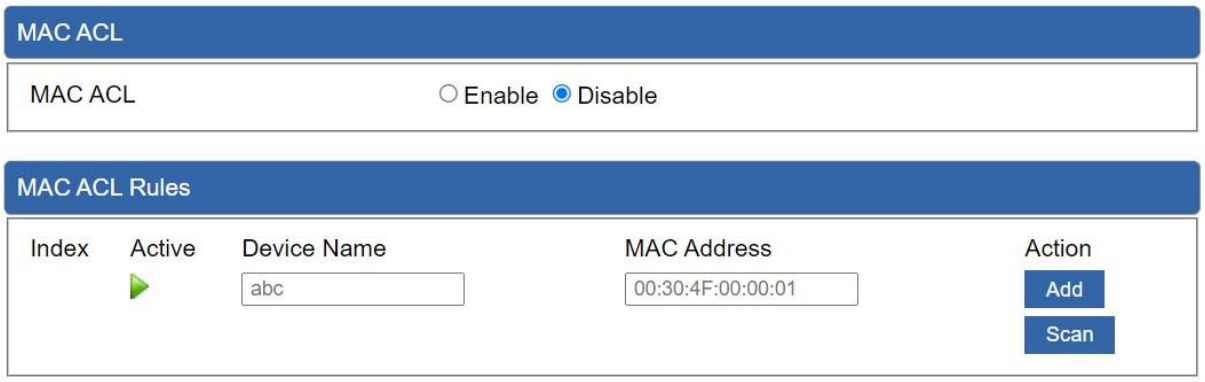


Figure 4-121: MAC ACL

Object	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 "**Add**" button to add end-device that is scanned from wireless network and mark them
Scan	Connect to client list

4.11.4 Wi-Fi Advanced

This page allows the user to define advanced setting of Wi-Fi.

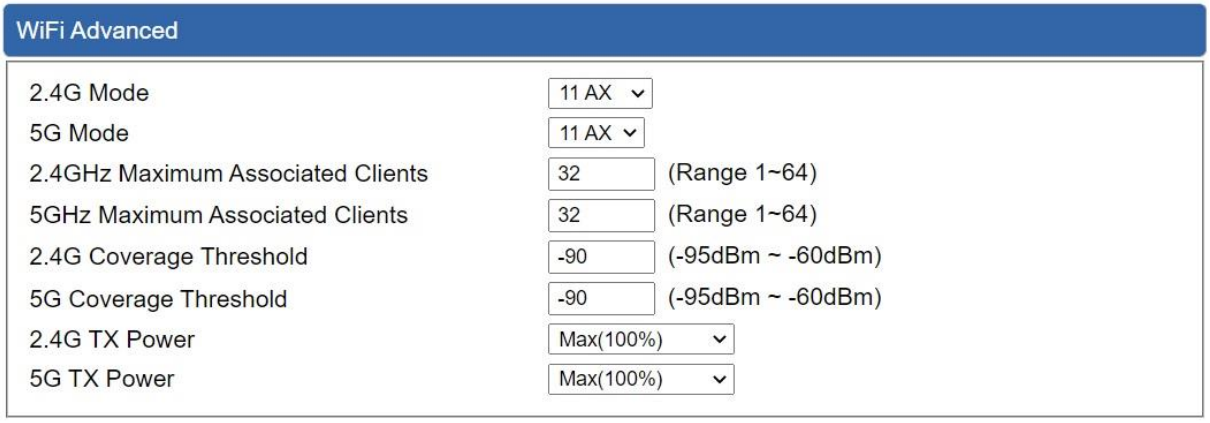


Figure 4-122: Wifi Advanced

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 Clients	The maximum users are 64
5GHz Maximum Associated Clients	The maximum users are 64
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 **Max (100%)**, **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 **Max (100%)**, **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

4.11.5 Wi-Fi Statistics

This page shows the statistics of Wi-Fi traffic.

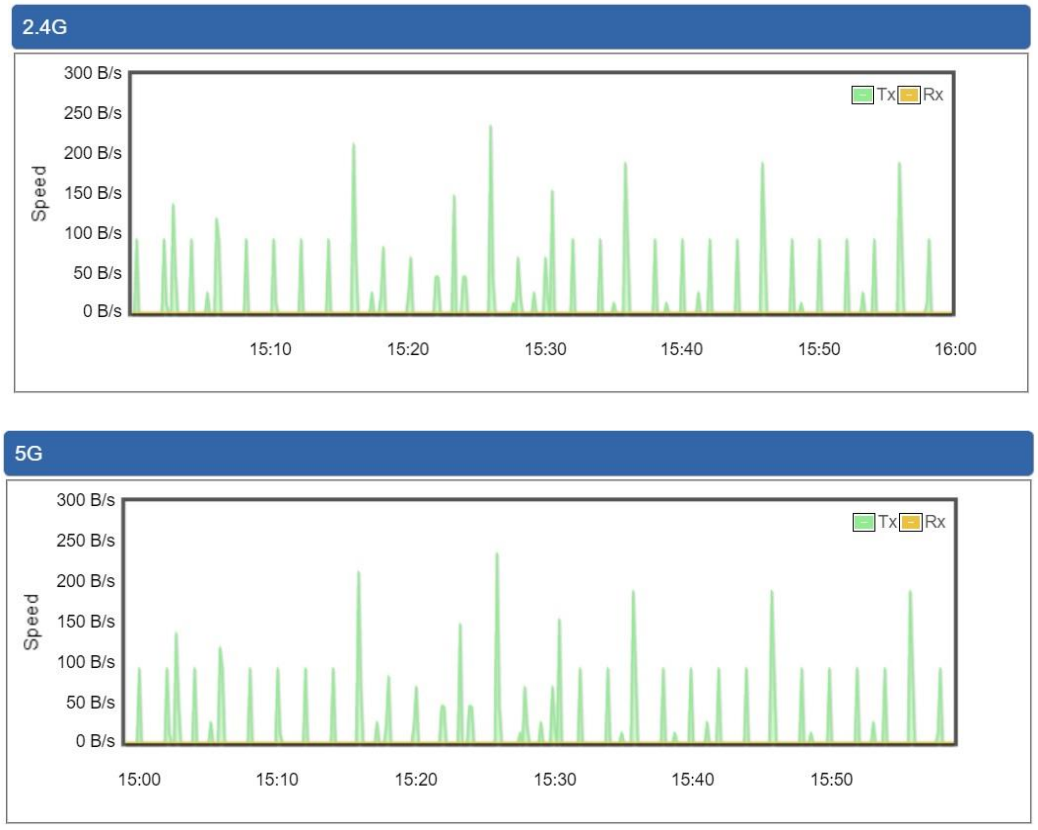


Figure 4-123: Wifi Statistics

4.11.6 Connection Status

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

Figure 4-124: Connection Status

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.

4.12 Maintenance

The Maintenance menu provides the following features for managing the system as Figure 4-125 is shown below:

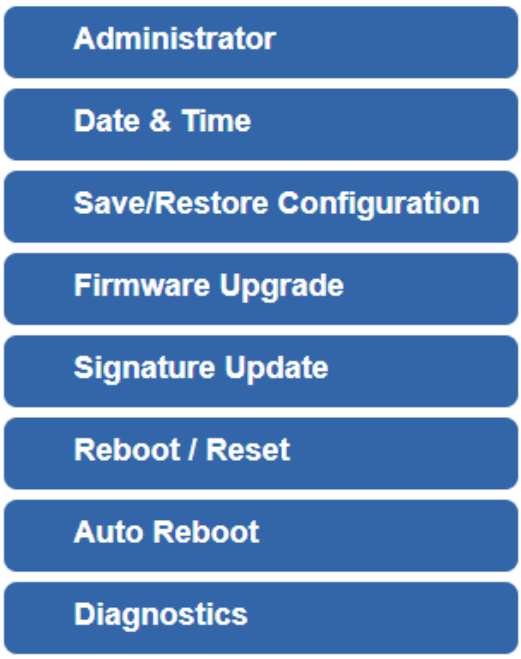


Figure 4-125: Maintenance Menu

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the router's configuration to local or USB sticker. Restore the router's configuration from local or USB sticker.
Firmware Upgrade	Upgrade the firmware from local or USB storage.
Signature Update	Allows configuring automatic IPS/IDS signature updates and update frequency.
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.

4.12.1 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.

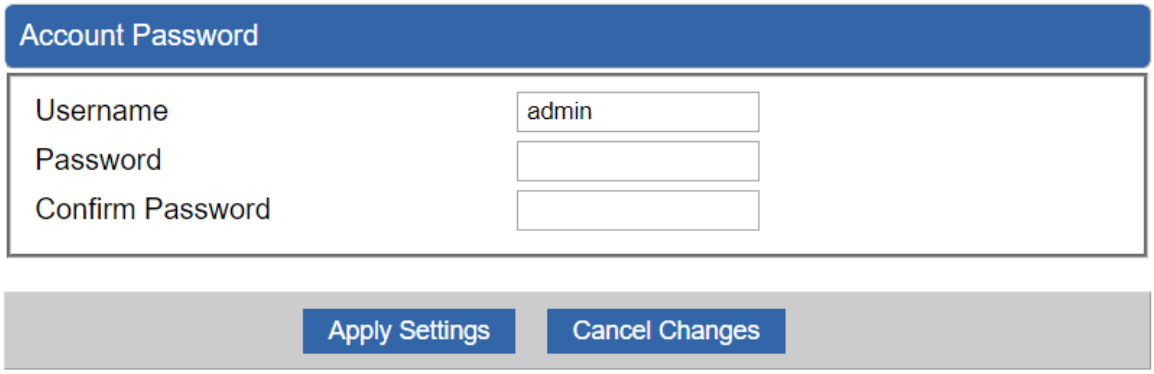


Figure 4-126: Account Settings (Standard Model – XVR-800)

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

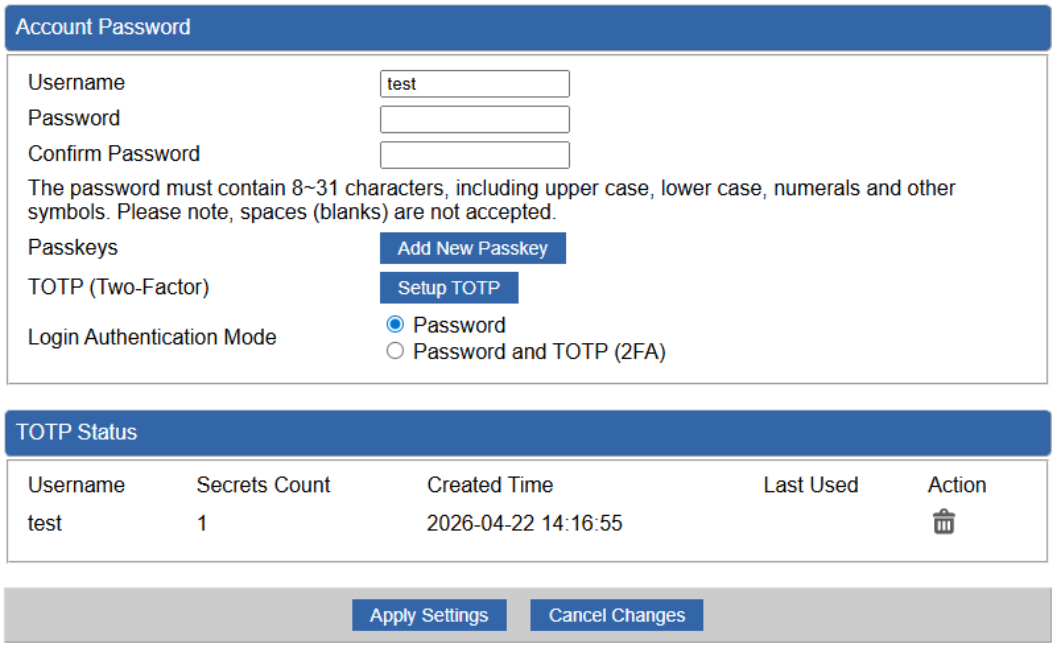


Figure 4-127: Account Settings (Zero Trust Model – ZT-800 & CSG-800 series)

Object	Description
Username	Input a new username.
Password	Input a new password.
Confirm Password	Input password again.
Passkeys	Add or manage passkey-based authentication for passwordless login.
TOTP (Two-Factor)	Configure time-based one-time password (TOTP) for multi-factor authentication.
Login Authentication Mode	Select the login method

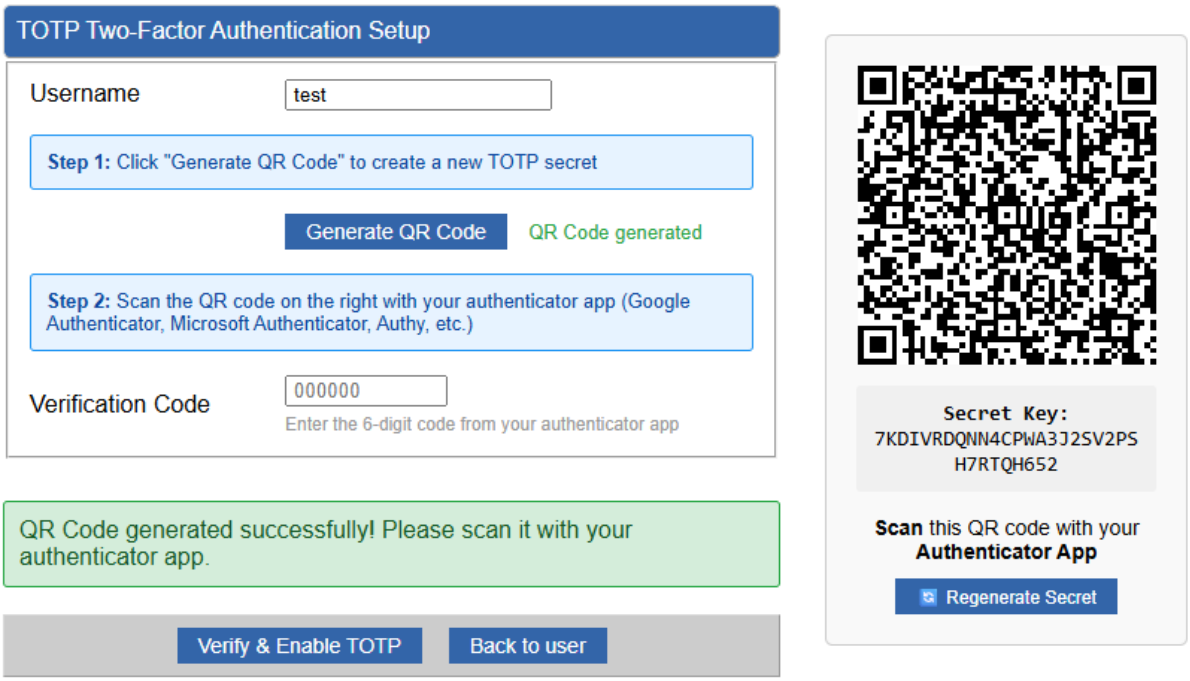


Figure 4-128: TOTP Setup (Zero Trust Model – ZT-800)

Object	Description
Username	Display the account username for TOTP setup.
Generate QR Code	Generate a QR code to create a new TOTP secret key.
Regenerate Secret	Generate a new TOTP secret key and QR code.
Verification Code	Enter the 6-digit code generated by the authenticator app for verification.

4.12.2 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 4-129.

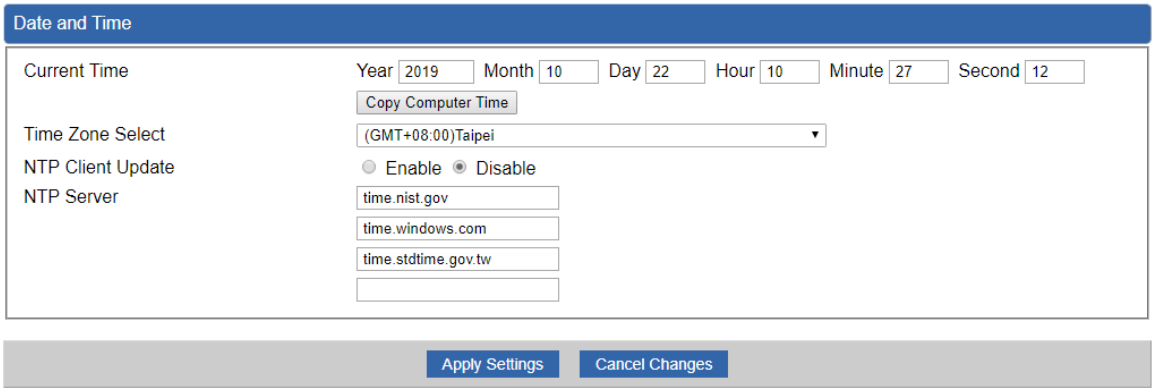


Figure 4-129: Date and Time

Object	Description
Current Time	Show the current time. User is able to set time and date manually.
Time Zone Select	Select the time zone of the country you are currently in. The router will set its time based on your selection.
NTP Client Update	Once this function is enabled, router will automatically update current time from NTP server.
NTP Server	User may use the default NTP sever or input NTP server manually.

4.12.3 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 4-130 is shown below:

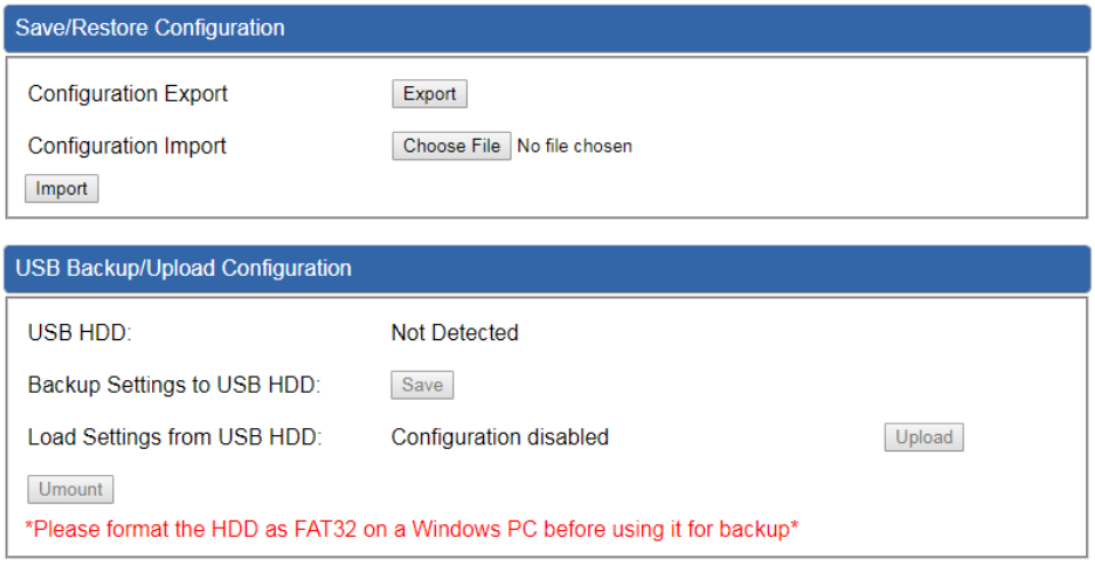


Figure 4-130: Save/Restoring Configuration

■ Save Setting to PC

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

■ Save Setting to USB Storage

Object	Description
USB Storage	The status of USB storage.
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.

4.12.4 Upgrading Firmware

This page provides the firmware upgrade of the route.

Figure 4-131: Upgrading Firmware

Object	Description
Choose File	Press the button to select the firmware.
Upgrade	Press the button to upgrade firmware to system.
USB Storage	Display the detection status of connected USB storage devices.
Load Firmware from USB Storage	Load firmware file from a connected USB storage device.
Unmount	Safely remove the mounted USB storage device.

4.12.5 Signature Update (CSG-800 series Only)

The **Signature Update** page allows users to configure automatic IPS/IDS signature updates. Users can enable automatic updates, select the update frequency, and view the last successful update time. The status is shown in Figure 4-132.

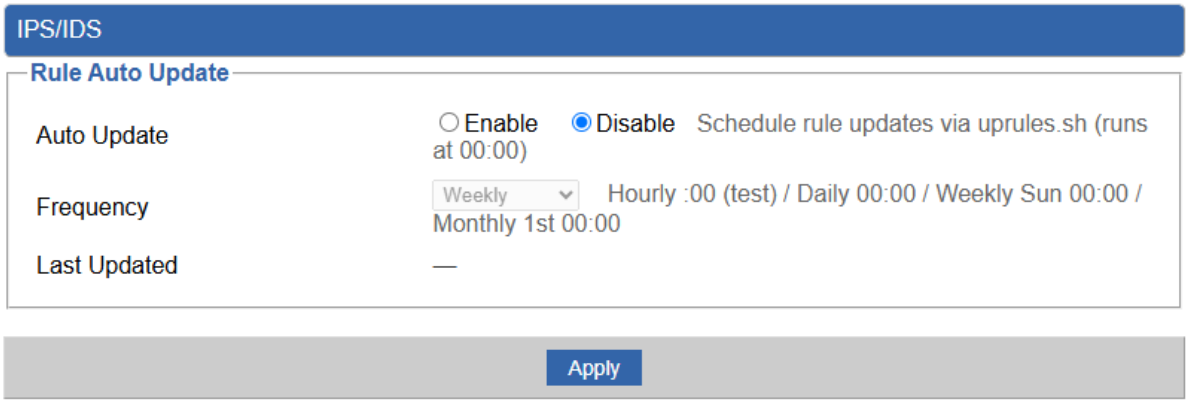


Figure 4-132: Signature Update

Object	Description
Auto Update	Enable or disable automatic IPS/IDS signature updates.
Frequency	Select the automatic update frequency, including **Hourly**, **Daily**, **Weekly**, or **Monthly**.
Last Updated	Displays the date and time of the last successful signature update.

4.12.6 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 4-133 is shown below:

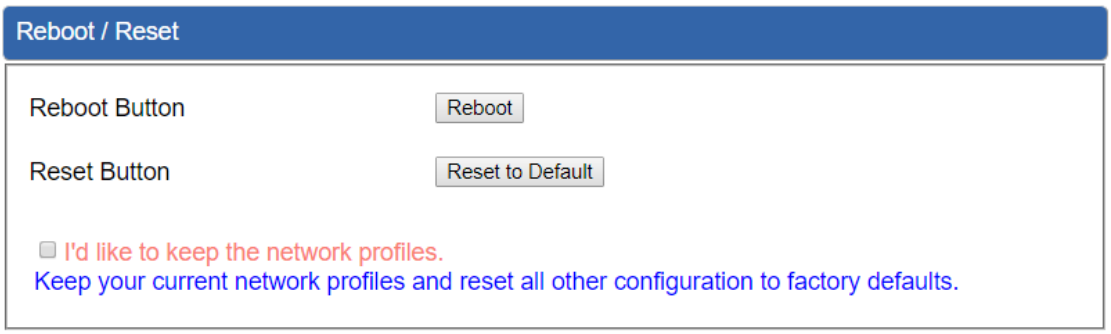


Figure 4-133: Reboot/Reset

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

4.12.7 Auto Reboot

This page provides the Auto Reboor of the route.

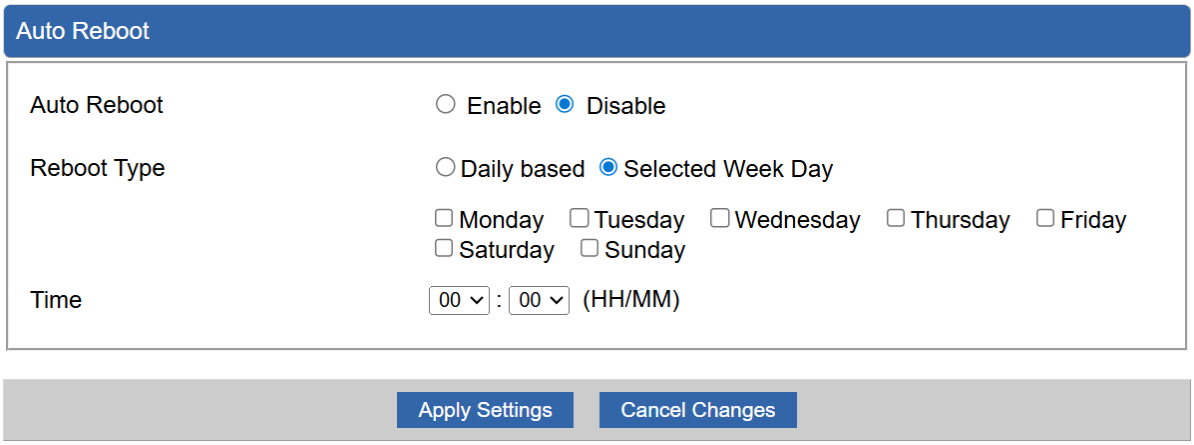


Figure 4-134: Auto Reboot

Object	Description
Auto Reboot	Enable or disable automatic system reboot scheduling.
Reboot Type	Select reboot schedule type (daily or specific weekdays).
Time	Set the reboot time in HH:MM format.

4.12.8 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.

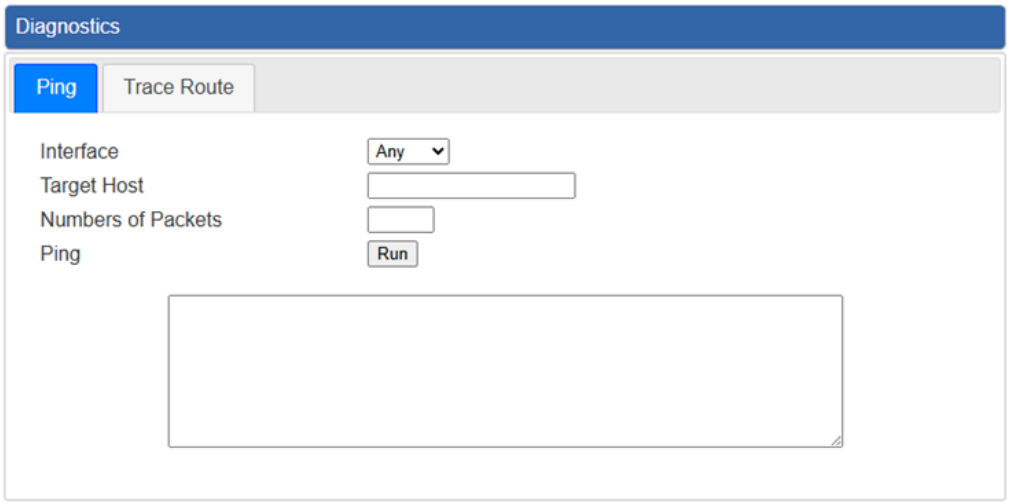


Figure 4-135: Ping

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

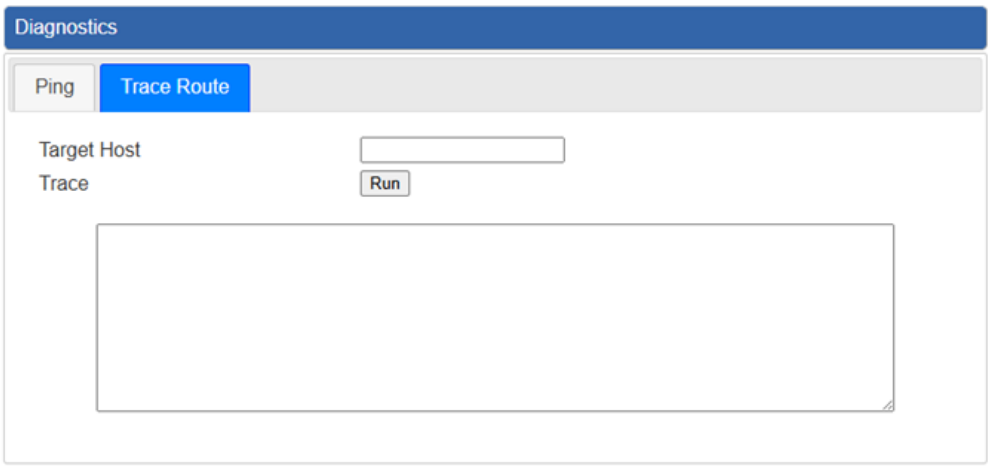


Figure 4-136: Trace Route

Object	Description
Target Host	The destination IP Address or domain.
Run	Execute the selected diagnostic test (ping or traceroute).

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 https://planetddns.com

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

Step 3: Input all DDNS settings.