TDGAR/IGAR/IGR/IGMG Series

Official Firmware

User Manual

Version 1.1

July, 2025

www.oringnet.com

COPYRIGHT NOTICE

TRADEMARKS

is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.
3F., NO.542-2, Jhongjheng Rd., Sindian District, New Taipei City 231, Taiwan, R.O.C.
Tel: + 886 2 2218 1066 // Fax: + 886 2 2218 1014
Website: www.oringnet.com

Technical Support
E-mail: support@oringnet.com

Sales Contact
E-mail: sales@oringnet.com (Headquarters)
info@oring-china.com (China)

Tables of Content

Getting Started

1.1 Introduction

This guide is designed to help you navigate ORing router’s firmware function, configure, make deployment and jobs you may encounter while using ORing router. The all new ORing router’s web user interfaces are unified with Linux based distribution, user can easily understand how to configure devices by referring one single documentation.

1.2 Supported Series and Firmware Version

Below information in this guide is applicable to ORing product and firmware that use router operating system but the appearance, feature availability and setting may vary. For more information about which configuration are supported by each product series, please refer Supported Feature List.

Series	Models	Firmware Version
TDGAR Series	TDGAR-1083D+-D4GS-M12X-WV	V1.0 build 2024012217
	TDGAR-1083D+-D5GS-M12X-WV	V1.01 build 2024050310
	TDGAR-2083D+-D4G12S-M12X-WV	V1.0 build 2024021916
	TDGAR-1003-D5G-M12X	TBD
IGAR Series	IGAR-1004-D5G	TBD
IGR Series	IGR-40D	V1.0 build 2024091210
IGMG Series	IGMG-8224D-D5G	V1.0 build 2024091815
	IGMG-P832244GCC+-D4G	TBD

1.3 Supported Feature List

Depending on the product series and model, support of features varies, please refer to below table for checking which features are supported by different product series:

Section	Function	TDGAR Series	IGAR Series	IGR Series	IGMG Series
System Information	System Overview	Yes	Yes	Yes	Yes
	Cellular WAN Status	Yes	Yes	-	Yes
	Wireless LAN 1&2 Status	Yes*1	Yes*1	-	Yes
	Traffic Statistics	Yes	Yes	Yes	Yes

Interface Configuration	LAN Setting	Yes	Yes	Yes	Yes
	WAN Setting	Yes	Yes	Yes*2	Yes
	Port Setting	Yes	-	-	-
	Wireless LAN 1&2	Yes*1	Yes*1	-	Yes
Network Services	Routing Protocol: Routing Setting	Yes	Yes	Yes	Yes
	Routing Protocol: OSPF	Yes	Yes	Yes	Yes
	Routing Protocol: EIGRP	Yes	Yes	Yes	TBD
	Routing Protocol: BGP	Yes	Yes	Yes	TBD
	Routing Protocol: NHRP	Yes	Yes	Yes	TBD
	Routing Protocol: VRRP Setting	Yes	Yes	Yes	TBD
	DHCP	Yes	Yes	Yes	Yes
	Dynamic DNS	Yes	Yes	Yes	TBD
	Multicast DNS	Yes	Yes	Yes	TBD
	Date & Time / NTP	Yes	Yes	Yes	Yes
	SNMP Settings	Yes	Yes	Yes	Yes
	Wake On Lan	Yes	Yes	Yes	Yes
Firewall Setting	IP Filter	Yes	Yes	Yes	Yes
	MAC Filter	Yes	Yes	Yes	Yes
	Custom Rules	Yes	Yes	Yes	Yes
	DDoS Prevention	Yes	Yes	Yes	Yes
NAT Setting	Virtual Server	Yes	Yes	Yes	Yes
	DMZ	Yes	Yes	Yes	Yes
	UPnP	Yes	Yes	Yes	Yes
VLAN Setting	VLAN	Yes	Yes	Yes	Yes
VPN Setting	OpenVPN	Yes	Yes	Yes	Yes
	IPSec	Yes	Yes	Yes	Yes
	GRE Tunnel	Yes	Yes	Yes	Yes
Serial Settings	Serial Interface	-	-	-	Yes
	Port profile	-		-	Yes
	Service Mode-Virtual COM Mode	-	-	-	Yes
	Service Mode – TCP Server Mode	-		-	Yes
	Service Mode – TCP Client Mode	-	-	-	Yes
	Service Mode – UDP Mode	-		-	Yes
	Serial Master to TCP Slave Gateway	-	-	-	Yes
	TCP Master to Serial Slave	-		-	Yes

	Gateway				
QoS	QoS	Yes	Yes	Yes	TBD
GPS Setting	GPS	Yes*3	-	-	-
Event Setting	Digital I/O	Yes*3	-	-	Yes
	E-Mail	Yes	Yes	Yes	Yes
	SNMP Traps	Yes	Yes	Yes	Yes
	SMS	Yes	Yes	Yes	Yes
	Zabbix Traps	Yes	Yes	Yes	TBD
Administration	System Settings	Yes	Yes	Yes	Yes
	Zabbix Agent	Yes	Yes	Yes	TBD
	SSHFS	Yes	Yes	Yes	TBD
	Backup and Restore Configurations	Yes	Yes	Yes	Yes
	Firmware Upgrade	Yes	Yes	Yes	Yes
	Reboot	Yes	Yes	Yes	Yes
	Factory Default	Yes	Yes	Yes	Yes
	Save device configuration	Yes	Yes	Yes	Yes
Diagnostics	System Log	Yes	Yes	Yes	Yes
	Debug Tools	Yes	Yes	Yes	Yes

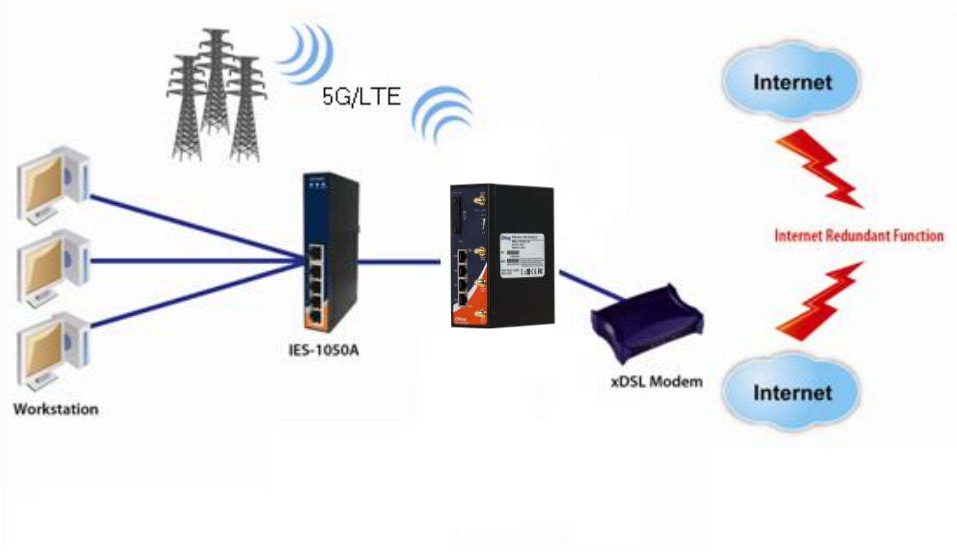
NOTICE:

1. TDGAR-1003-D5G-M12X and IGAR-1004-D5G do not support Wi-Fi function (pure Cellular/Ethernet WAN modem).
2. IGR-40D does not support Cellular WAN in WAN setting (Ethernet WAN only).
3. TDGAR-1003-D5G-M12X does not support GPS and Digital I/O function.

Management Interface

2.1 Installation

Before installing the router, you need to be able to access the router via a computer equipped with an Ethernet card. To simplify the connection, it is recommended to use an Ethernet card to connect to a LAN.

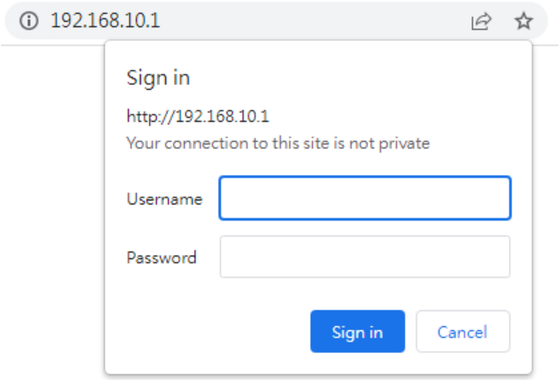


Follow the steps below to install and connect the router to PCs:

Step 1: Select power source. The router can be powered by DC power input.

Step 2: Connect a computer to the router. Use either a straight-through Ethernet cable or cross-over cable to connect the LAN port (IGAR/IGR/IGMG series: LAN1~3 or TDGAR series: G1~G2) of the router to a computer. Once the LED of the LAN port lights up, which indicates the connection is established, the computer will initiate a DHCP request to retrieve an IP address from the Router.

Step 3: Configure the router on a web-based management utility. Open a web browser on your computer and type http://192.168.10.1 (default gateway IP of the router) in the address box to access the webpage. A login window will pop up where you can enter the default login name admin and password admin. For security reasons, we strongly recommend you going to change the password. Click on **Administration** > **System Settings** after logging in to change the password.



192.168.10.1

Sign in

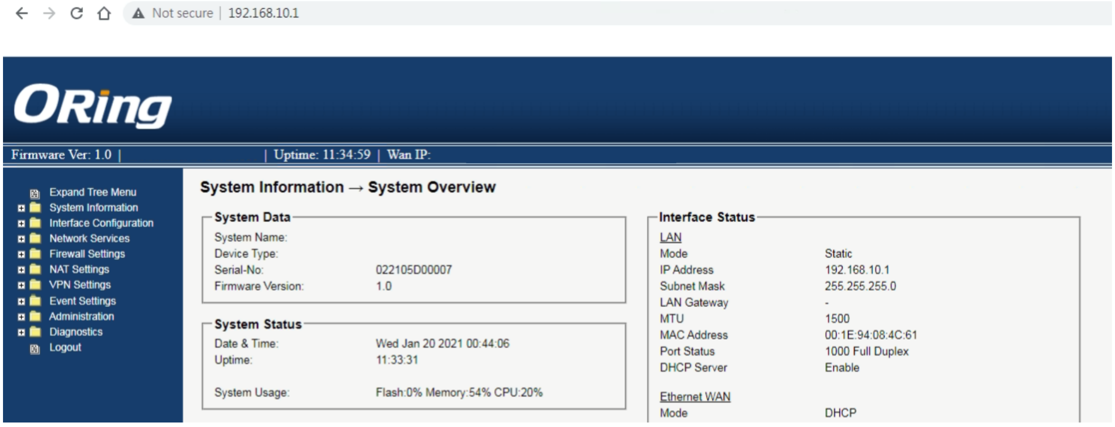
http://192.168.10.1

Your connection to this site is not private

Username

Password

After you log in successfully, a Web interface will appear, as shown below. On the left-hand side of the interface is a list of functions where you can configure the settings. The details of the configurations will be shown on the right screen.



Not secure | 192.168.10.1

Firmware Ver: 1.0 | | Uptime: 11:34:59 | Wan IP:

System Information → System Overview

System Data

System Name:	
Device Type:	
Serial-No:	022105D00007
Firmware Version:	1.0

System Status

Date & Time:	Wed Jan 20 2021 00:44:06
Uptime:	11:33:31
System Usage:	Flash:0% Memory:54% CPU:20%

Interface Status

LAN

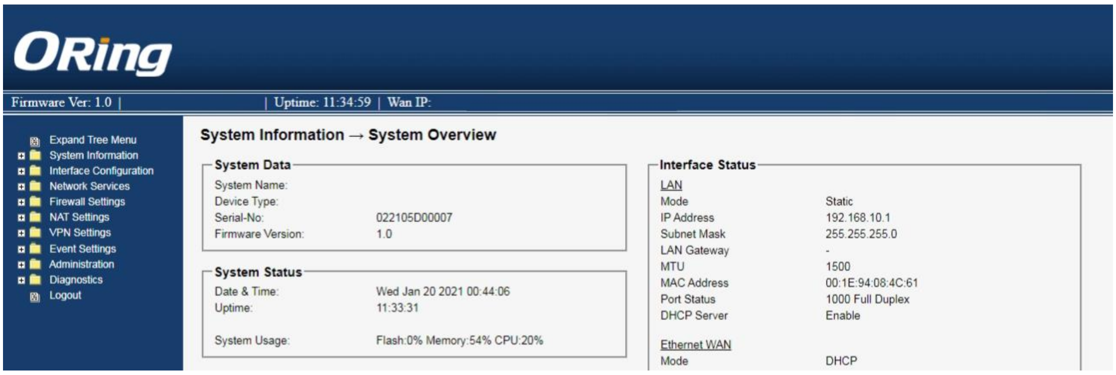
Mode	Static
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
LAN Gateway	-
MTU	1500
MAC Address	00:1E:94:08:4C:61
Port Status	1000 Full Duplex
DHCP Server	Enable

Ethernet WAN

Mode	DHCP

2.2 Configuration

On top of the screen shows information about the firmware version, uptime, and WAN IP address.



Firmware Ver: 1.0 | | Uptime: 11:34:59 | Wan IP:

System Information → System Overview

System Data
System Name:
Device Type:
Serial-No: 022105D00007
Firmware Version: 1.0

System Status
Date & Time: Wed Jan 20 2021 00:44:06
Uptime: 11:33:31
System Usage: Flash:0% Memory:54% CPU:20%

Interface Status
LAN
Mode: Static
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
LAN Gateway: -
MTU: 1500
MAC Address: 00:1E:94:08:4C:61
Port Status: 1000 Full Duplex
DHCP Server: Enable
Ethernet WAN
Mode: DHCP

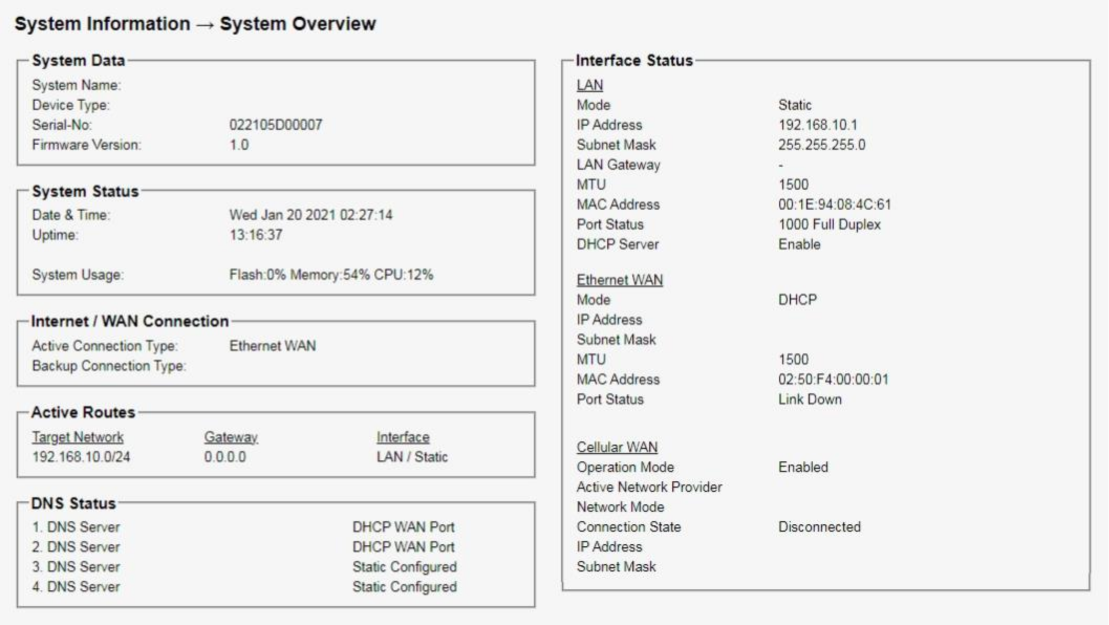
Label	Description
Firmware	Shows the current firmware version
Uptime	Shows the elapsed time since the Router is started
Wan IP	Shows WAN IP address

2.2.1 System Information

System information shows up all system information, Cellular WAN status, and Wired LAN/WAN traffic statistics.

System Overview

System basic information



System Information → System Overview

System Data
System Name:
Device Type:
Serial-No: 022105D00007
Firmware Version: 1.0

System Status
Date & Time: Wed Jan 20 2021 02:27:14
Uptime: 13:16:37
System Usage: Flash:0% Memory:54% CPU:12%

Internet / WAN Connection
Active Connection Type: Ethernet WAN
Backup Connection Type:

Active Routes

Target Network	Gateway	Interface
192.168.10.0/24	0.0.0.0	LAN / Static

DNS Status
1. DNS Server DHCP WAN Port
2. DNS Server DHCP WAN Port
3. DNS Server Static Configured
4. DNS Server Static Configured

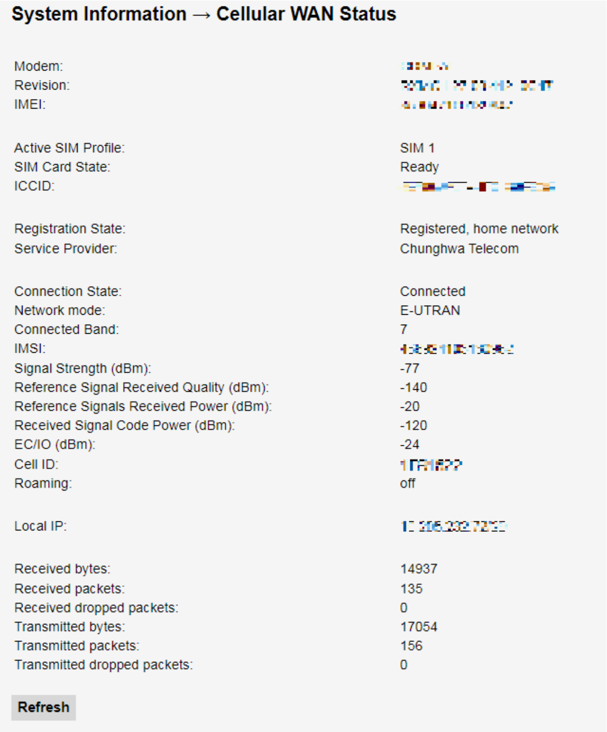
Interface Status
LAN
Mode: Static
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
LAN Gateway: -
MTU: 1500
MAC Address: 00:1E:94:08:4C:61
Port Status: 1000 Full Duplex
DHCP Server: Enable

Ethernet WAN
Mode: DHCP
IP Address:
Subnet Mask:
MTU: 1500
MAC Address: 02:50:F4:00:00:01
Port Status: Link Down

Cellular WAN
Operation Mode: Enabled
Active Network Provider:
Network Mode:
Connection State: Disconnected
IP Address:
Subnet Mask:

Cellular WAN Status

Include Cellular modem, SIM card and Base station information.

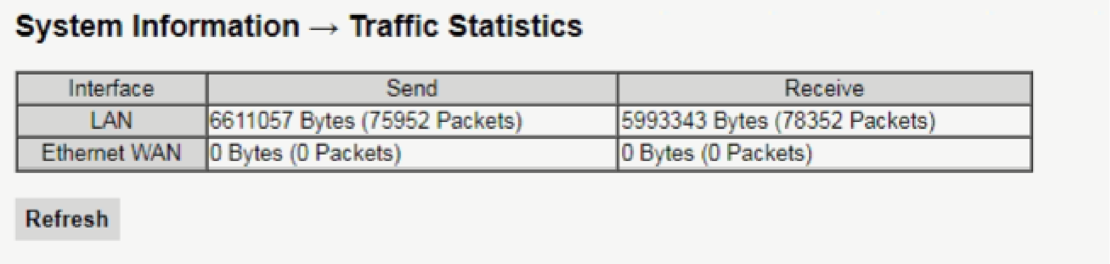


System Information → Cellular WAN Status

Modem:	[redacted]
Revision:	[redacted]
IMEI:	[redacted]
Active SIM Profile:	SIM 1
SIM Card State:	Ready
ICCID:	[redacted]
Registration State:	Registered, home network
Service Provider:	Chunghwa Telecom
Connection State:	Connected
Network mode:	E-UTRAN
Connected Band:	7
IMSI:	[redacted]
Signal Strength (dBm):	-77
Reference Signal Received Quality (dBm):	-140
Reference Signals Received Power (dBm):	-20
Received Signal Code Power (dBm):	-120
EC/IO (dBm):	-24
Cell ID:	[redacted]
Roaming:	off
Local IP:	[redacted]
Received bytes:	14937
Received packets:	135
Received dropped packets:	0
Transmitted bytes:	17054
Transmitted packets:	156
Transmitted dropped packets:	0

Traffic Statistics

Wire LAN/WAN traffic statistics.



System Information → Traffic Statistics

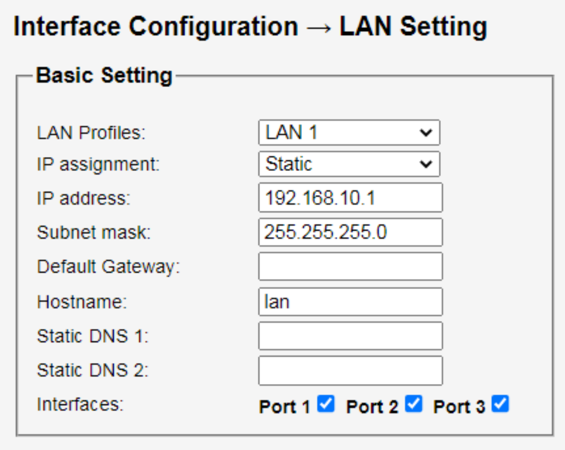
Interface	Send	Receive
LAN	6611057 Bytes (75952 Packets)	5993343 Bytes (78352 Packets)
Ethernet WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)

2.2.2 Interface Configuration

This section will guide you through the general settings for the router.

LAN Setting

This page allows you to configure the IP settings of the LAN for the router. The LAN IP address is private to your internal network and is not visible to Internet.



Interface Configuration → LAN Setting

Basic Setting

LAN Profiles:	LAN 1
IP assignment:	Static
IP address:	192.168.10.1
Subnet mask:	255.255.255.0
Default Gateway:	
Hostname:	lan
Static DNS 1:	
Static DNS 2:	
Interfaces:	Port 1 ☑ Port 2 ☑ Port 3 ☑

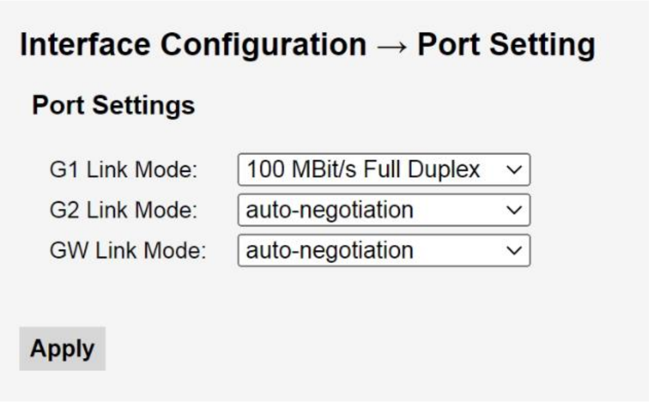
Label	Description
LAN Profiles	Assign profile (LAN1, LAN2 and LAN3) for group configuration
IP assignment	Assign IP address by static or DHCP
IP Address	The IP address of the LAN. The default value is **192.168.10.1**
Subnet Mask	The subnet mask of the LAN. The default value is **255.255.255.0**
Default Gateway	Assign default gateway address for router
Hostname	Assign hostname for router
Static DNS 1/2	Assign DNS address for router
Interfaces	Assign interface (Port 1, Port 2 and Port 3) for above configuration

WAN Setting

This page allows you to configure WAN settings. Different WAN connection types will have different settings.

Port Setting

This page allows user configuring port speed manually or auto-negotiation with G1, G2 and GW ports. This function may work when TDGAR is wire connected with legacy device without auto-negotiation function or non-qualified cable connection. We strongly recommend to use qualified cable/device for best compatibility.



Interface Configuration → Port Setting

Port Settings

G1 Link Mode: 100 MBit/s Full Duplex

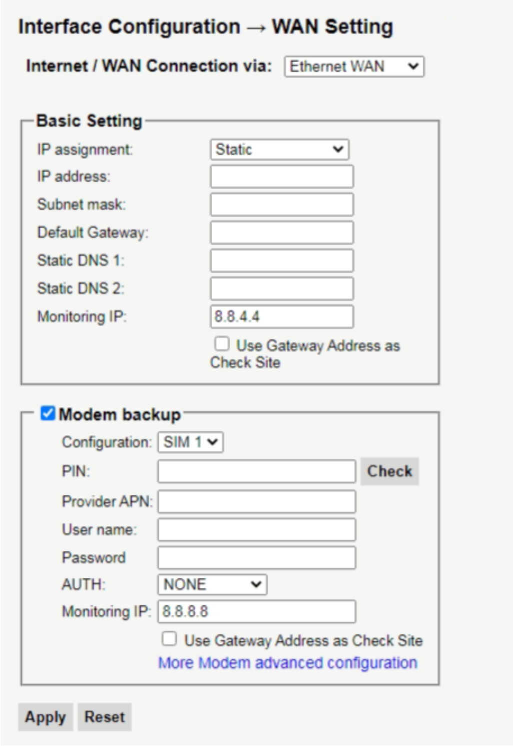
G2 Link Mode: auto-negotiation

GW Link Mode: auto-negotiation

Label	Description
auto-negotiation	Auto-detected with port speed. (Default)
1000 Mbit/s Full Duplex	Fix port speed at 1000 Mbit/s with full-duplex mode.
1000 Mbit/s Half Duplex	Fix port speed at 1000 Mbit/s with half-duplex mode.
100 Mbit/s Full Duplex	Fix port speed at 100 Mbit/s with full-duplex mode.
100 Mbit/s Half Duplex	Fix port speed at 100 Mbit/s with half-duplex mode.
10 Mbit/s Full Duplex	Fix port speed at 10 Mbit/s with full-duplex mode.
10 Mbit/s Half Duplex	Fix port speed at 10 Mbit/s with half-duplex mode.

Ethernet WAN

Connection Type as Static / DHCP / DHCP+Fallback:



Interface Configuration → WAN Setting

Internet / WAN Connection via: Ethernet WAN

Basic Setting

IP assignment: Static

IP address:

Subnet mask:

Default Gateway:

Static DNS 1:

Static DNS 2:

Monitoring IP: 8.8.4.4

□ Use Gateway Address as Check Site

☑ Modem backup

Configuration: SIM 1

PIN: Check

Provider APN:

User name:

Password

AUTH: NONE

Monitoring IP: 8.8.8.8

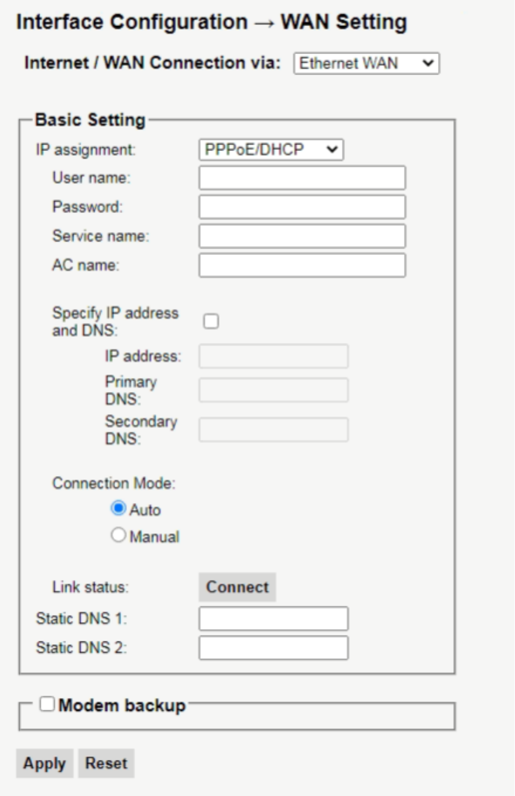
□ Use Gateway Address as Check Site

More Modem advanced configuration

Apply Reset

Label	Description
IP assignment	Select IP assignment Static, DHCP and when DHCP fail will back to static assigned address
IP address	In static mode, IP address must fill in manually
Subnet mask	In static mode, subnet mask must fill in manually
Default Gateway	Assign a default gateway IP address for router WAN interface
Static DNS 1/2	Specifies a DNS server address manually. You can enter two addresses as the primary and secondary options.
Monitoring IP (If "Modem backup" checkbox is checked)	Fill a host for monitoring WAN connection if available, it can use gateway address as well.
Use Gateway Address as Check Site	Checked if Monitoring IP address is the same as WAN interface's gateway IP address.
Modem backup	Enable this option if you want to use cellular Modem as a backup connection when main connection is lost. Enter your account username, password or AUTH method in the corresponding fields if needed.

Connection Type as PPPoE/DHCP:



Interface Configuration → WAN Setting

Internet / WAN Connection via: Ethernet WAN

Basic Setting

IP assignment: PPPoE/DHCP

User name:

Password:

Service name:

AC name:

Specify IP address and DNS: □

IP address:

Primary DNS:

Secondary DNS:

Connection Mode:

● Auto

○ Manual

Link status: Connect

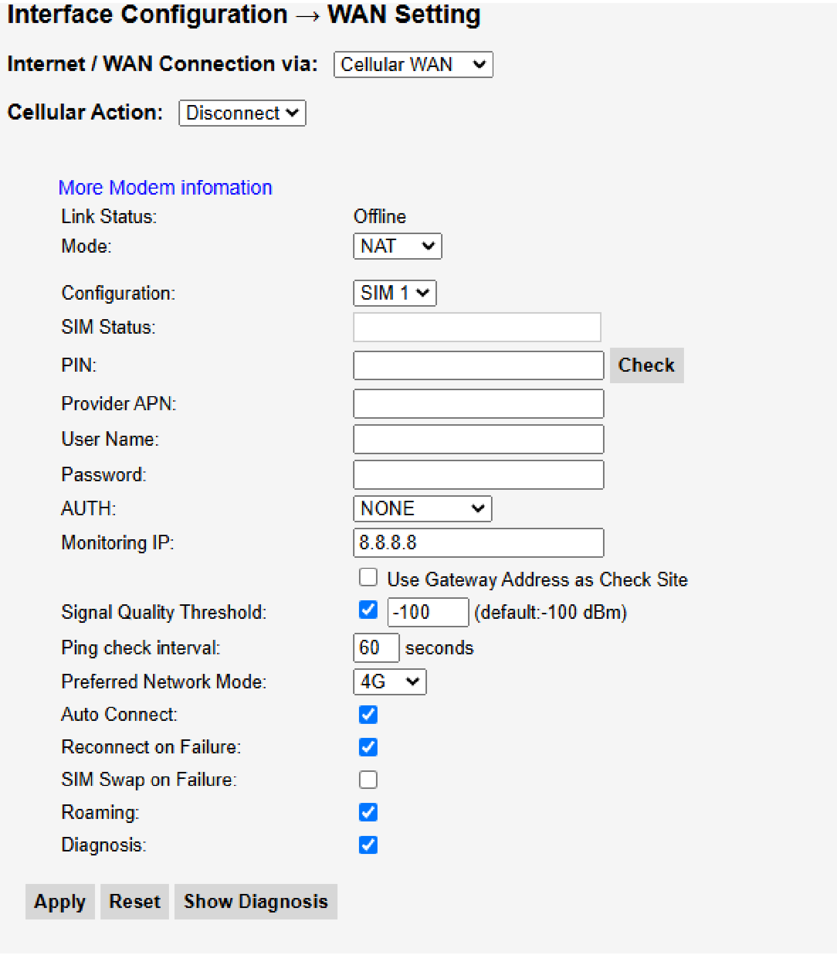
Static DNS 1:

Static DNS 2:

□ Modem backup

Label	Description
User Name / Password	Enter the username & password provided by your ISP.
AC Name	Enter the name of the access concentrator provided by your ISP
Service Name	Enter the service name provided by your ISP
Specify the IP & DNS provided by ISP	Enter a static IP and DNS address required by other ISPs.
Connection Mode	**Auto**: connect automatically when the router boots up **Connect on Demand**: disconnect the PPP session if the router has had no traffic for a specified amount of time. Fill a number in the Max Idle Time field. **Manual**: connects or disconnects manually via the Connect/Disconnect buttons at the end of the page
Modem backup	Enable this option if you want to use cellular modem as a backup connection when main connection is lost. Enter your account username and password in the corresponding fields.

Cellular WAN



Interface Configuration → WAN Setting

Internet / WAN Connection via: Cellular WAN

Cellular Action: Disconnect

More Modem infomation

Link Status:	Offline
Mode:	NAT
Configuration:	SIM 1
SIM Status:	
PIN:	Check
Provider APN:	
User Name:	
Password:	
AUTH:	NONE
Monitoring IP:	8.8.8.8
	☐ Use Gateway Address as Check Site
Signal Quality Threshold:	☑ -100 (default:-100 dBm)
Ping check interval:	60 seconds
Preferred Network Mode:	4G
Auto Connect:	☑
Reconnect on Failure:	☑
SIM Swap on Failure:	☐
Roaming:	☑
Diagnosis:	☑

Label	Description
Cellular Action	Active Cellular Connect or Disconnect
Link Status	Shows the status of connections
Mode	NAT mode: router with NAT function, Bridge mode: transparent and act as pure modem
Configuration	Select for SIM Card slot
SIM Status	Check SIM Card status
PIN	Enter a PIN code if you want to perform PIN check
Provider APN	Enter the APN value (optional)
User Name	Enter the username provided by your ISP
Password	Enter the password provided by your ISP
AUTH	Select connect auth method, support PAP/CHAP/MSCHAPv2
Monitoring IP	Type an IP address the field to use it to check if the connection

	alive or lost.
Use Gateway Address as Check Site	Checked if Monitoring IP address is the same as WAN interface's gateway IP address.
Signal Quality Threshold	The system will only be connected if it is better than the set value
Ping Check Interval	Enter the interval value for ping check (Monitoring IP) mechanism
Preferred Network Mode	Select Auto, 4G or 5G for preferred network
Auto Connect	Check to start connections when the router boots up
Reconnect on Failure	Checked to enable "Reconnect on Failure" mechanism
SIM Swap on Failure	Checked to enable SIM Card redundant function (SIM1 and SIM2)
Roaming	Check to enable roaming function if user requires data roaming between different ISP venders abroad.
Diagnosis	Check to enable diagnosis mode and press "Show Diagnosis" button to show results.

2.2.3 Networking Services

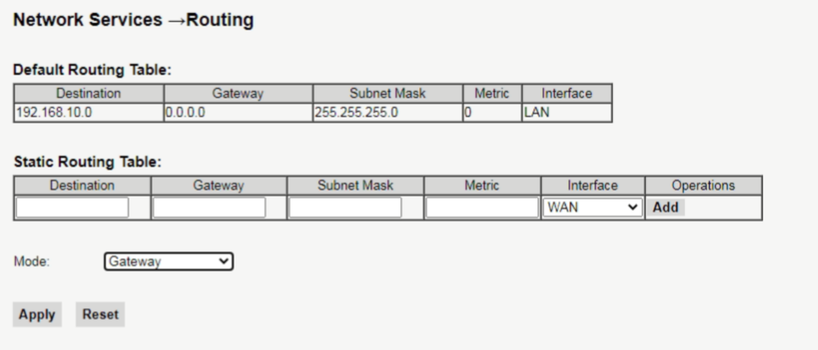
Routing Protocol

Routing Setting

This page shows the information of the routing table.

Static Routing

Router supported static routing mode, which means routers forward packets using route information from route table entries that you manually configure.



Network Services →Routing

Default Routing Table:

Destination	Gateway	Subnet Mask	Metric	Interface
192.168.10.0	0.0.0.0	255.255.255.0	0	LAN

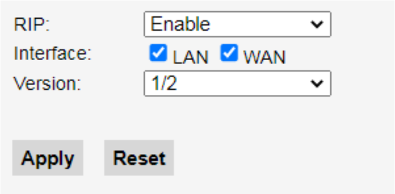
Static Routing Table:

Destination	Gateway	Subnet Mask	Metric	Interface	Operations
				WAN	Add

Mode: Gateway

Label	Description
Default Routing Table	Shows all routing information, including static and dynamic routing (if enabled)
Static Route Table	Fills in corresponding information to add new entries to the static routing tablet
Mode	Choose **Gateway Mode** if you want PCs in the LAN to visit external network, otherwise choose **Router Mode**

RIP



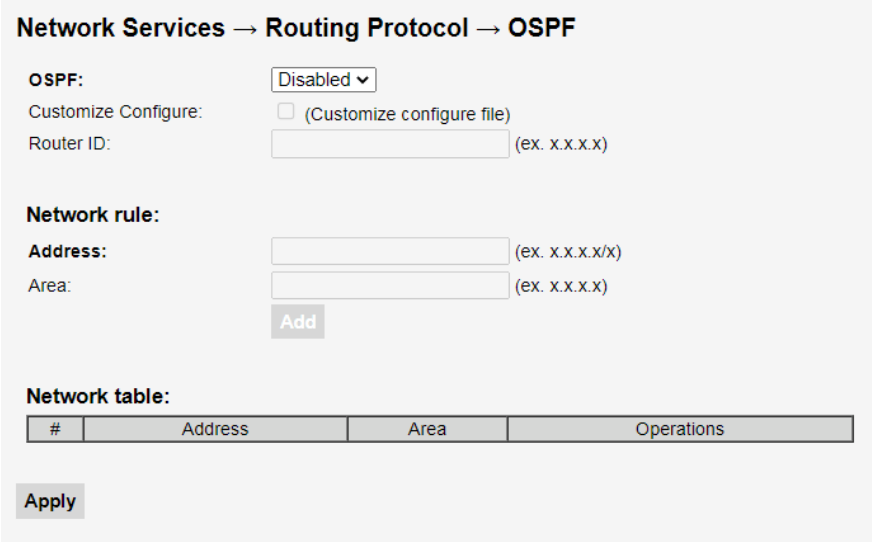
RIP: Enable

Interface: ☑ LAN ☑ WAN

Version: 1/2

Label	Description
RIP	Select to enable or disable RIP protocol
Interface	Check interface for RIP protocol
Version	1/2 for auto, 1 for version 1 or 2 for version 2

OSPF



Network Services → Routing Protocol → OSPF

OSPF: Disabled

Customize Configure: □ (Customize configure file)

Router ID: (ex. x.x.x.x)

Network rule:

Address: (ex. x.x.x.x/x)

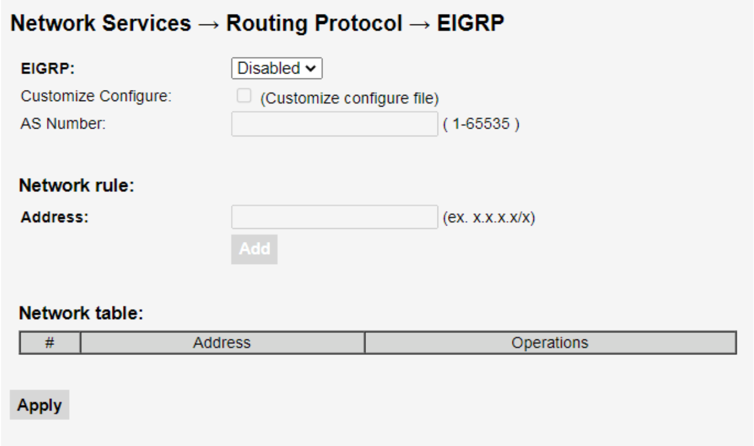
Area: (ex. x.x.x.x)

Network table:

#	Address	Area	Operations

Label	Description
OSPF	Select to enable or disable OSPF protocol
Customize Configure	Check and paste custom configuration as plain text
Router ID	Enter Router ID for OSPF protocol
Address	Enter Address for OSPF network rule
Area	Enter Area for OSPF network rule

EIGRP



Network Services → Routing Protocol → EIGRP

EIGRP: Disabled

Customize Configure: ☐ (Customize configure file)

AS Number: (1-65535)

Network rule:

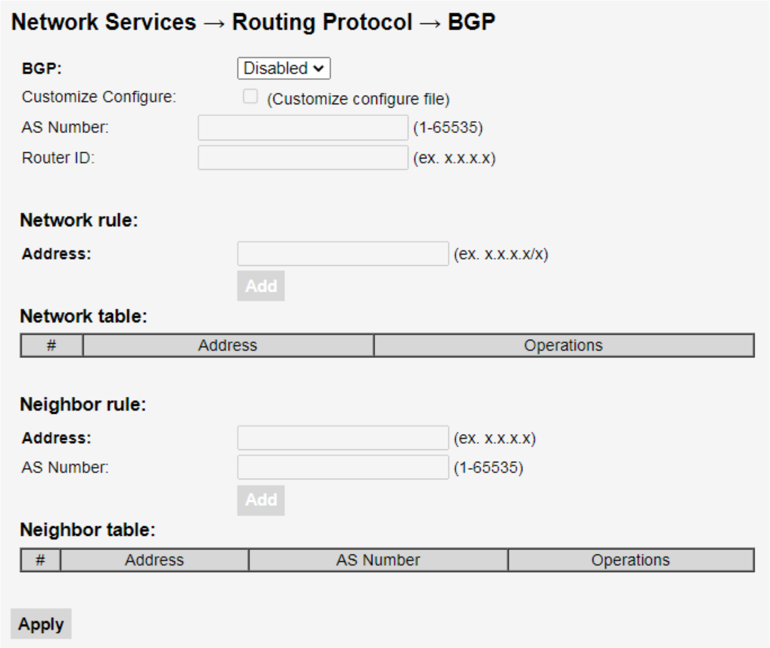
Address: (ex. x.x.x.x/x)

Network table:

#	Address	Operations

Label	Description
EIGRP	Select to enable or disable EIGRP protocol
Customize Configure	Check and paste custom configuration as plain text
AS Number	Enter AS Number for EIGRP protocol
Address	Enter Address for EIGRP network rule

BGP



Network Services → Routing Protocol → BGP

BGP: Disabled

Customize Configure: ☐ (Customize configure file)

AS Number: (1-65535)

Router ID: (ex. x.x.x.x)

Network rule:

Address: (ex. x.x.x.x/x)

Network table:

#	Address	Operations

Neighbor rule:

Address: (ex. x.x.x.x)

AS Number: (1-65535)

Neighbor table:

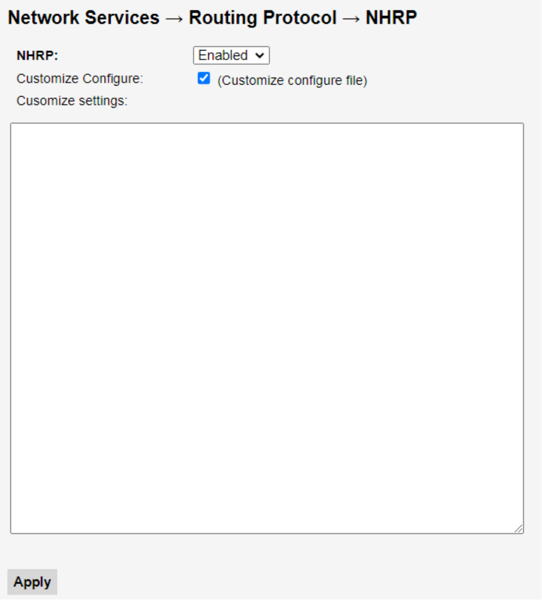
#	Address	AS Number	Operations

Label	Description
BGP	Select to enable or disable BGP protocol
Customize Configure	Check and paste custom configuration as plain text
AS Number	Enter AS Number for BGP protocol
Router ID	Enter Router ID for BGP protocol

Label	Description
Address	Enter Address for BGP network rule

Label	Description
Address	Enter Address for BGP neighbor rule
AS Number	Enter AS Number for BGP neighbor rule

NHRP



Network Services → Routing Protocol → NHRP

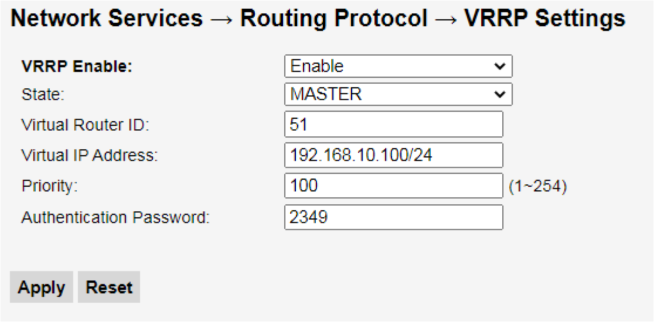
NHRP: Enabled

Customize Configure: ☑ (Customize configure file)

Cusomize settings:

Label	Description
OSPF	Select to enable or disable NHRP protocol
Customize Configure	Check and paste custom configuration as plain text

VRRP Setting



Network Services → Routing Protocol → VRRP Settings

VRRP Enable: Enable

State: MASTER

Virtual Router ID: 51

Virtual IP Address: 192.168.10.100/24

Priority: 100 (1~254)

Authentication Password: 2349

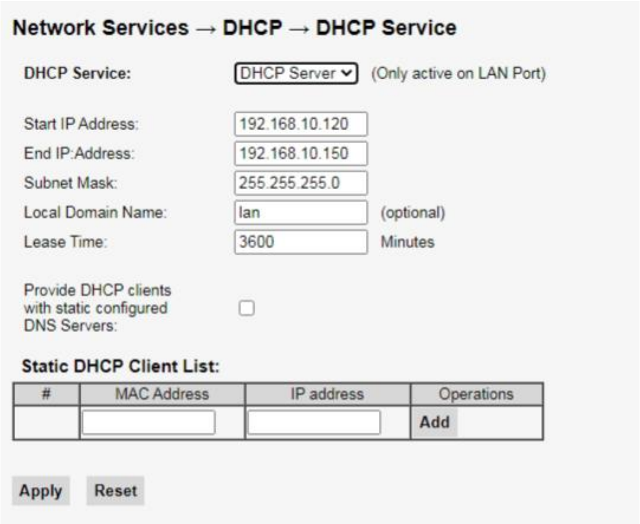
Label	Description
VRRP Setting	Select to enable or disable VRRP protocol
State	Select VRRP state (Master or Backup)
Virtual Router ID	Enter Virtual Router ID for VRRP protocol
Virtual IP Address	Enter Virtual IP Address for VRRP protocol
Priority	Enter Priority (1~254) for VRRP protocol
Authentication Password	Enter password for VRRP protocol

DHCP

DHCP is a network protocol designed to allow devices connected to a network to communicate with each other using an IP address. The connection works in a client-server model, in which DHCP clients request an IP address from a DHCP server. The router comes with a built-in DHCP (Dynamic Host Control Protocol) server which assigns an IP address to a computer (DHCP client) on the LAN automatically. The router can also serve as a relay agent which will forward DHCP requests from DHCP clients to a DHCP server on the Internet.

The IP allocation provides one-to-one mapping of MAC address to IP address. When a computer with a MAC address requesting an IP address from the router, it will be assigned with the IP address according to the mapping. You can choose one from the client list and add it to the mapping list.

DHCP Service



Network Services → DHCP → DHCP Service

DHCP Service: DHCP Server (Only active on LAN Port)

Start IP Address: 192.168.10.120

End IP:Address: 192.168.10.150

Subnet Mask: 255.255.255.0

Local Domain Name: lan (optional)

Lease Time: 3600 Minutes

Provide DHCP clients with static configured DNS Servers: □

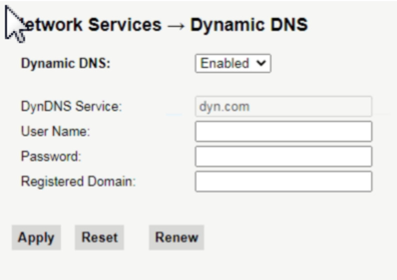
Static DHCP Client List:

#	MAC Address	IP address	Operations
			Add

Label	Description
DHCP Server	Enable or disable the DHCP server function. The default setting is **Enabled**.
Starting IP	The starting IP address of the IP range assigned by the DHCP server
Ending IP	The ending IP address of the IP range assigned by the DHCP server
Lease Time	The period of time for the IP address to be leased. During the lease time, the DHCP server cannot assign that IP address to any other clients. Enter a number in the field. The default setting is 48 hours.
Local Domain Name	Enter the local domain name of a private network (optional)
Provide DHCP clients with static configured DNS Servers	Provide static configured DNS server address (LAN Setting) to DHCP clients.
Static DHCP Client List	Add the one-to-one relationship of the MAC address and IP address.

Dynamic DNS

Dynamic Domain Name System (DDNS) allows you to configure a domain name for your IP address which is dynamically assigned by your ISP. Therefore, you can use a static domain name that always points to the current dynamic IP address.



Network Services → Dynamic DNS

Dynamic DNS: Enabled

DynDNS Service: dyn.com

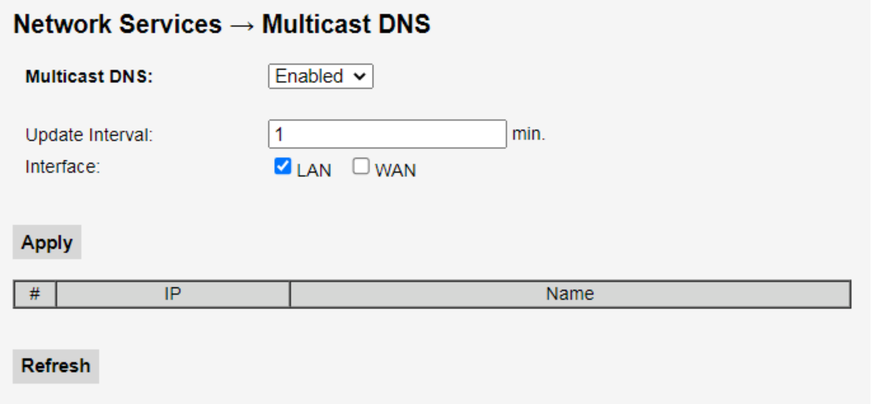
User Name:

Password:

Registered Domain:

Label	Description
DDNS Service	Choose a DDNS service provider from the list
User Name	Enter the username of your DDNS account
Password	Enter the password of your DDNS account
Registered Domain	Enter the domain name provided by your dynamic DNS service provider

Multicast DNS



Network Services → Multicast DNS

Multicast DNS: Enabled

Update Interval: 1 min.

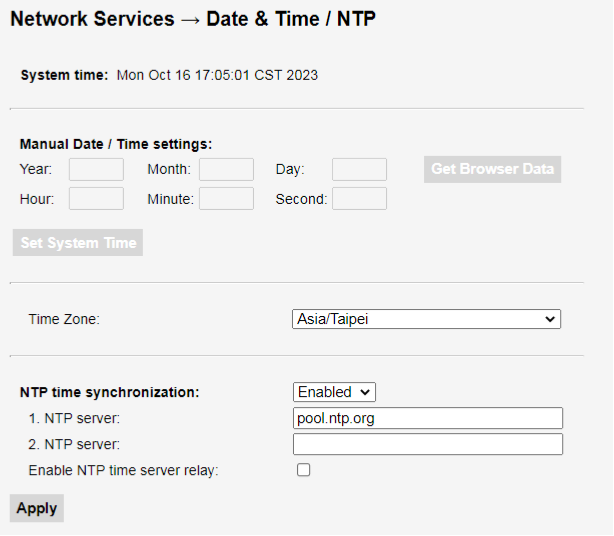
Interface: ☑ LAN ☐ WAN

#	IP	Name

Label	Description
Multicast DNS	Select to enable or disable Multicast DNS
Update Interval	Enter the update interval for Multicast DNS
Interface	Check the interface for Multicast DNS

Date & Time / NTP

In this page, you can set the date & time of the device. A correct date and time will help the system log events. You can set up a NTP (Network Time Protocol) client to synchronize date & time with a NTP server on the Internet.



Network Services → Date & Time / NTP

System time: Mon Oct 16 17:05:01 CST 2023

Manual Date / Time settings:

Year: Month: Day:

Hour: Minute: Second:

Time Zone: Asia/Taipei

NTP time synchronization: Enabled

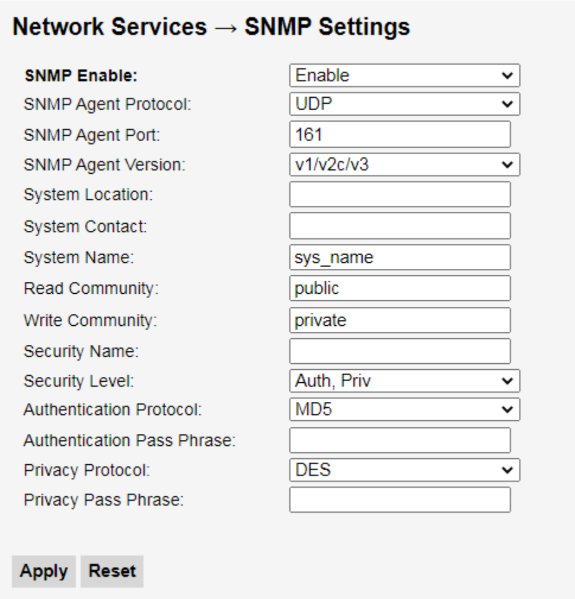
1. NTP server: pool.ntp.org

2. NTP server:

Enable NTP time server relay: □

Label	Description
Get Browser Date	Get Date and Time from Browser
Set System Time	Set the setting value to system
Time Zone	Assign Time Zone for system
NTP time synchronization	Enable or disable NTP function
Time Zone	Select the time zone you are located in
NTP Server	Set NTP server address for synchronization
Enable NTP time server relay	Check for NTP time server relay

SNMP Setting



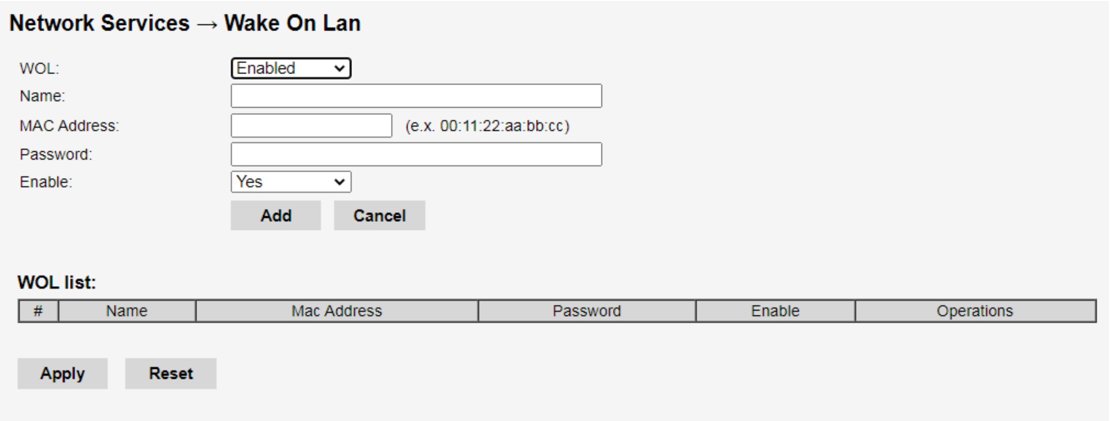
Network Services → SNMP Settings

SNMP Enable:	Enable
SNMP Agent Protocol:	UDP
SNMP Agent Port:	161
SNMP Agent Version:	v1/v2c/v3
System Location:	
System Contact:	
System Name:	sys_name
Read Community:	public
Write Community:	private
Security Name:	
Security Level:	Auth, Priv
Authentication Protocol:	MD5
Authentication Pass Phrase:	
Privacy Protocol:	DES
Privacy Pass Phrase:	

Label	Description
SNMP Enable	SNMP (Simple Network Management Protocol) Agent is a service program that runs on the router. The agent provides management information to the NMS by keeping track of various operational aspects of the system. Turn on to open this service and off to shutdown it.
SNMP Agent Protocol	Select packet type for SNMP protocol
SNMP Agent Port	Specify SNMP listening port
SNMP Agent Version	Specify SNMP protocol version
System Location	Specify System Location of SNMP Agent
System Contact	Specify System Contact of SNMP Agent
System Name	Specify System Name of SNMP Agent
Read Community	Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-only community.
Write Community	Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-write community.
Security Name:	Specify Security Name of SNMP Agent
Security Level	Specify Security Level (Authentication or Privacy) of SNMP Agent
Authentication Protocol	Select MD5 to authenticate using HMAC-MD5 algorithms Select SHA to authenticate using HMAC-SHA algorithms

Authentication Pass Phrase	Specify Authentication Pass Phrase of SNMP Agent
Privacy Protocol	Select DES to use DES-based data encryption Select AES to use AES-based data encryption
Privacy Pass Phrase	Specify Privacy Pass Phrase of SNMP Agent

Wake On LAN



Network Services → Wake On Lan

WOL: Enabled

Name:

MAC Address: (e.x. 00:11:22:aa:bb:cc)

Password:

Enable: Yes

WOL list:

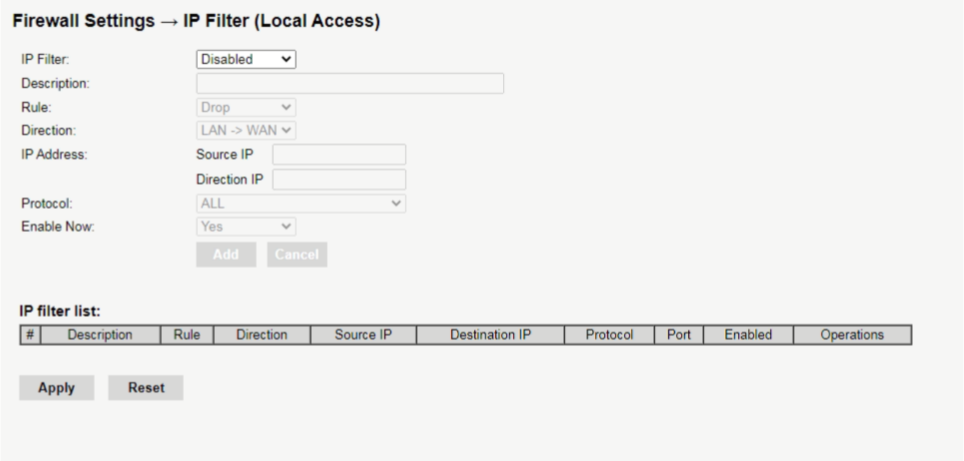
#	Name	Mac Address	Password	Enable	Operations

Label	Description
WOL	Select to enable or disable Wake On LAN
Name	Specify Name for Wake On LAN device
MAC Address	Specify MAC Address for Wake On LAN device
Password	Specify Password for Wake On LAN device
Enable	Select to enable or disable Wake On LAN item list

2.2.4 Firewall Setting

IP Filter

IP filters enable you to control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN. This control is implemented via IP filter rules which are defined to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN.



Firewall Settings → IP Filter (Local Access)

IP Filter: Disabled

Description:

Rule: Drop

Direction: LAN -> WAN

IP Address: Source IP

Direction IP

Protocol: ALL

Enable Now: Yes

Add Cancel

IP filter list:

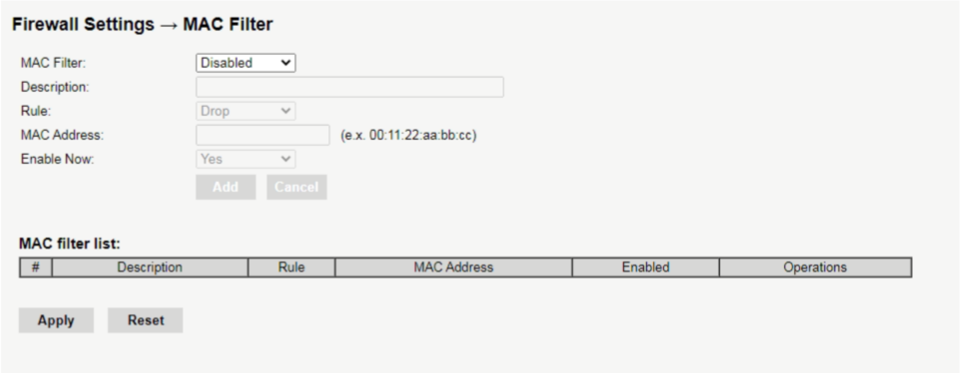
#	Description	Rule	Direction	Source IP	Destination IP	Protocol	Port	Enabled	Operations

Apply Reset

Label	Description
IP Filter	Enable or disable the IP Filter
Description	Enter description for the entry.
Rule	Configure the rules to be applied to the IP filter. Available options include **DROP**, **ACCEPT**, and **REJECT.**
Direction	Specify the direction of data flow to be filtered
IP Address	Enter the IP address of the source and destination computer
Protocol	Configures the protocol to be filtered
Enable Now	Click **Yes** to enable the entry after adding it
IP filter list	Shows the information of all IP filters. Click **Edit** to edit the entry or **Del** to delete the entry.

MAC Filter

This page enables you to deny or allow LAN computers to access the Internet based on their MAC addresses.



Firewall Settings → MAC Filter

MAC Filter: Disabled

Description:

Rule: Drop

MAC Address: (e.x. 00:11:22:aa:bb:cc)

Enable Now: Yes

Add Cancel

MAC filter list:

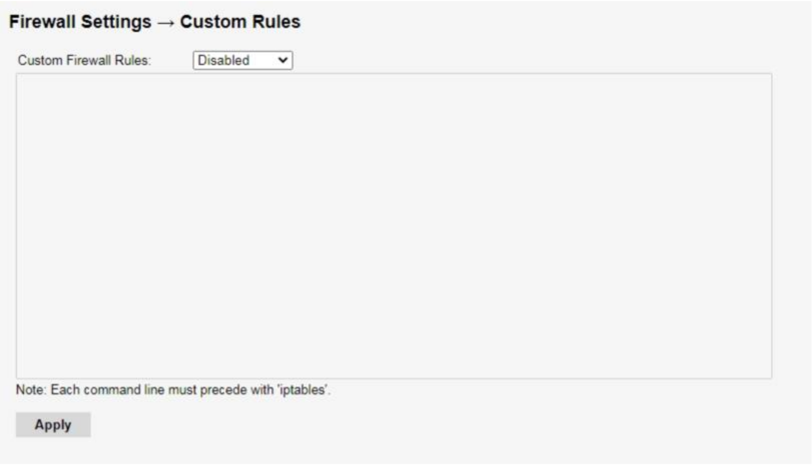
#	Description	Rule	MAC Address	Enabled	Operations

Apply Reset

Label	Description
MAC Filter	Enable or disable the MAC Filter
Description	Enter description for the entry
Rule	Configure the rules to be applied to the MAC filter. Available options include **DROP**, **ACCEPT**, and **REJECT.**
MAC Address	Enter the MAC address to be filtered
Enable Now	Click **Yes** to enable the entry after adding it
MAC filter list	Shows the information of all MAC filters. Click **Edit** to edit the entry or **Del** to delete the entry.

Custom Rules

Custom firewall rules provide more granular access control beyond LAN isolation. You can define a set of firewall rules that is evaluated for every request. Firewall rules are evaluated from top to bottom. The first rule that matches is applied, and subsequent rules are not evaluated. If no rules match, the default rule (allow all traffic) is applied.

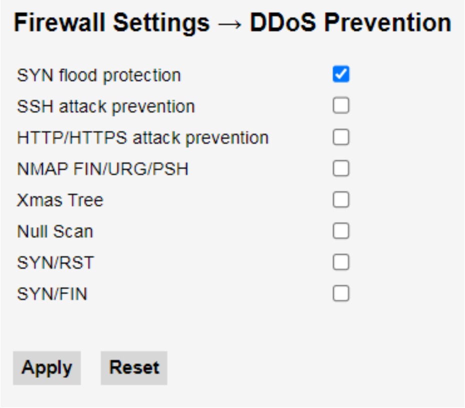


Firewall Settings → Custom Rules

Custom Firewall Rules: Disabled

Note: Each command line must precede with 'iptables'.

DDoS Prevention



Firewall Settings → DDoS Prevention

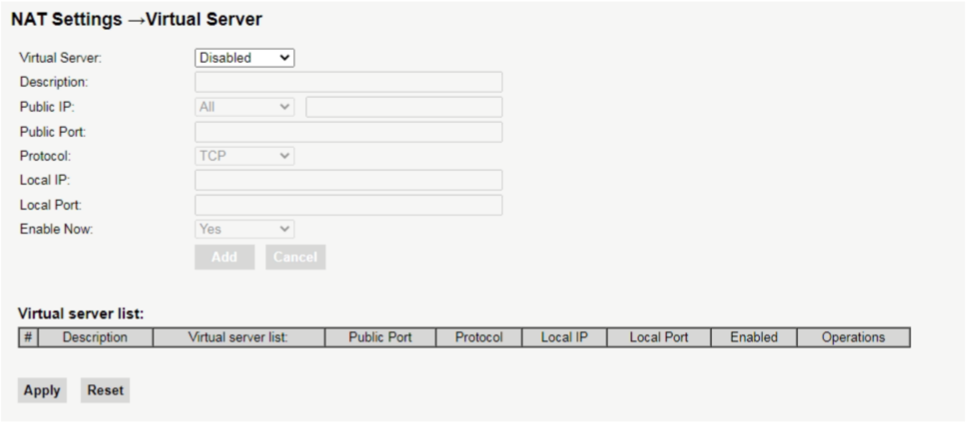
SYN flood protection ☑
SSH attack prevention □
HTTP/HTTPS attack prevention □
NMAP FIN/URG/PSH □
Xmas Tree □
Null Scan □
SYN/RST □
SYN/FIN □

Label	Description
SYN flood protection	Check to enable SYN flood protection
SSH attack prevention	Check to enable SSH attack prevention
HTTP/HTTPS attack prevention	Check to enable HTTP/HTTPS attack prevention
NMAP FIN/URG/PSH	Check to enable NMAP FIN/URG/PSH protection
Xmas Tree	Check to enable Xmas Tree protection
Null Scan	Check to enable Null Scan protection
SYN/RST	Check to enable SYN/RST protection
SYN/FIN	Check to enable SYN/FIN protection

2.2.5 NAT Setting

Virtual Server

This page allows you to set up virtual server setting. A virtual server allows Internet users to access services on your LAN. This is a useful function if you host services online such as FTP, Web or game servers. A public port must be defined for the virtual server on your router in order to redirect traffic to an internal LAN IP address and LAN port. Any PC used as a virtual server must have a static or reserved IP address.



NAT Settings →Virtual Server

Virtual Server: Disabled
Description:
Public IP: All
Public Port:
Protocol: TCP
Local IP:
Local Port:
Enable Now: Yes

Virtual server list:

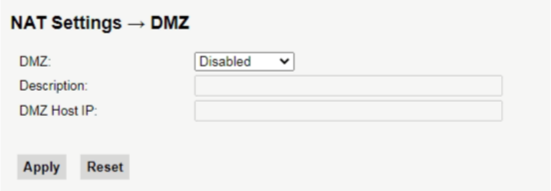
#	Description	Virtual server list	Public Port	Protocol	Local IP	Local Port	Enabled	Operations

Label	Description
Virtual Server	Select **Enabled** or **Disabled** to activate or deactivate virtual server
Description	Enter the description of the entry. Acceptable characters are 0-9, a-z, and A-Z. A null value is allowed.
Public IP	Enter a public IP allowed to access the virtual service. If not specified, choose **All**.
Public Port	The port number to be used to access the virtual service on the WAN (Wide Area Network)
Protocol	The protocol used for the virtual service
Local IP	The IP address of the computer that will provide virtual service
Local Port	The port number of the service used by the private IP computer
Enable Now	Enables the virtual server entry after adding it
Virtual server list	Click **Edit** to edit the virtual service entry and **Del** to delete the entry.

DMZ

DMZ (Demilitarized Zone) allows a computer to be exposed to the Internet without passing through the security settings and therefore is unsecured. This feature is useful for special purposes such as gaming.

To use this function, you need to set an internal computer as the DMZ host by entering its IP address. Adding a client to the DMZ may expose your local network to a variety of security risks, so use this function carefully.



NAT Settings → DMZ

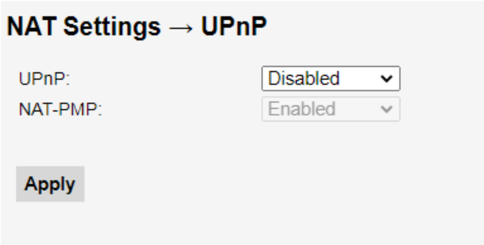
DMZ: Disabled

Description:

DMZ Host IP:

Label	Description
DMZ	Enable or disable DMZ
Description	Enter a description for the DMZ host entry
DMZ Host IP	Enter the IP address of the computer to act as the DMZ host

UPnP



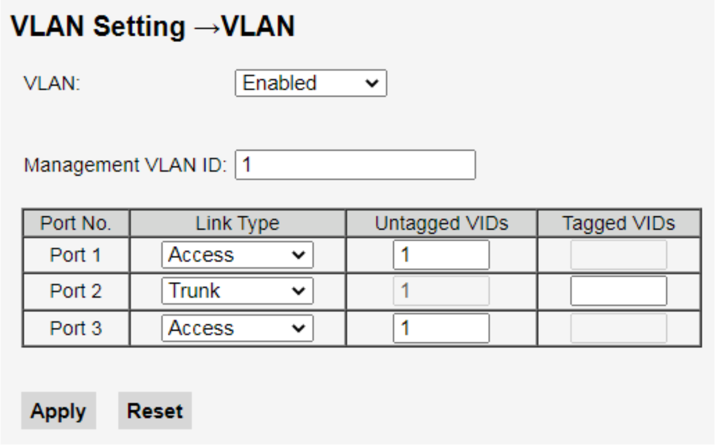
NAT Settings → UPnP

UPnP: Disabled

NAT-PMP: Enabled

Label	Description
UPnP	Enable or disable UPnP
NAT-PMP	Enable or disable NAT-PMP

2.2.6 VLAN



VLAN Setting →VLAN

VLAN: Enabled

Management VLAN ID: 1

Port No.	Link Type	Untagged VIDs	Tagged VIDs
Port 1	Access	1	
Port 2	Trunk	1	
Port 3	Access	1	

Label	**Description**
VLAN	Enable or disable VLAN
Management VLAN ID	Specify Management VLAN ID to allow access web interface
Link Type	Specify Link Type for each port
Untagged VIDs	Specify Untagged VIDs for each port
Tagged VIDs	Specify Tagged VIDs for each port

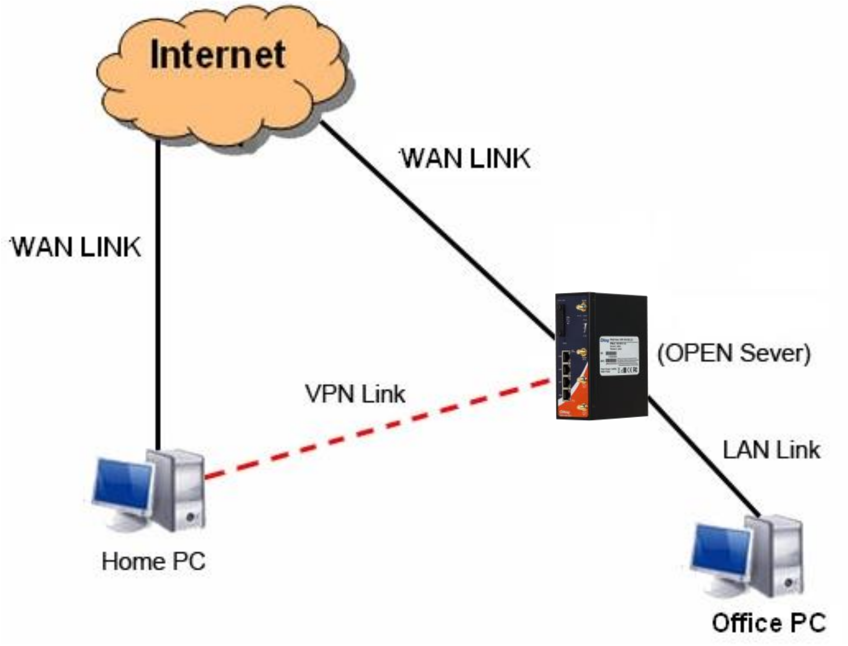
2.2.7 VPN Setting

OpenVPN

A VPN is a method of linking two locations as if they are on a local private network to facilitate data transmission and ensure data security. The links between the locations are known as tunnels. VPN can achieve confidentiality, authentication, and integrity of data by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

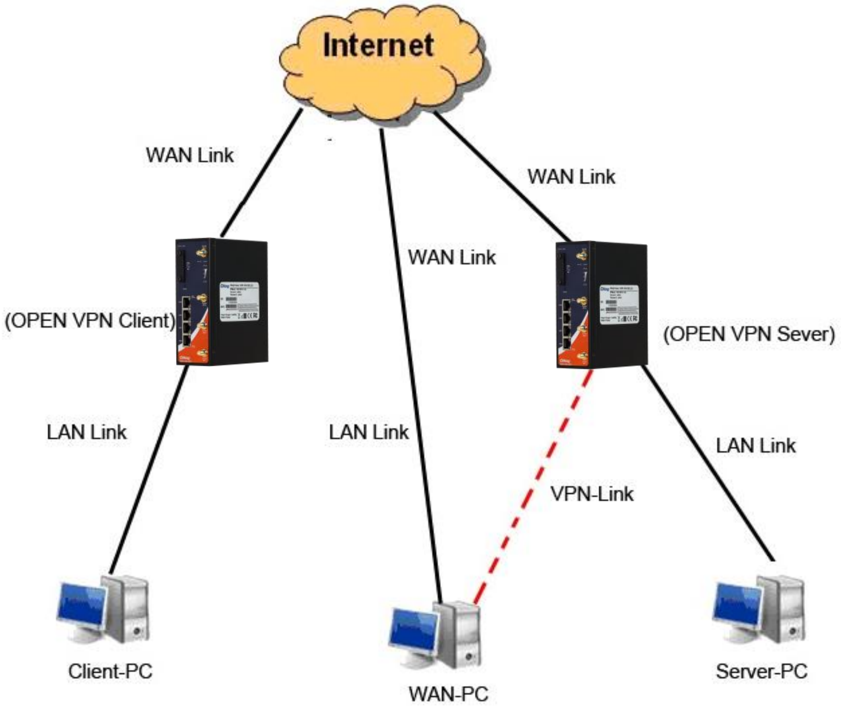
Open VPN enables you to easily set up a virtual private network over an encrypted connection. It is a full-function SSL VPN solution which accommodates a wide range of configurations including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-level remote access with load balancing, failover, and fine-grained access control features.

To set up your router as an Open VPN server, you need to install OpenVPN client software for your Windows-based PC. You can download it from http://openvpn.net/download.html#stablel. The software version must match the current version of OpenVPN used by the router which is version 2.0.9.

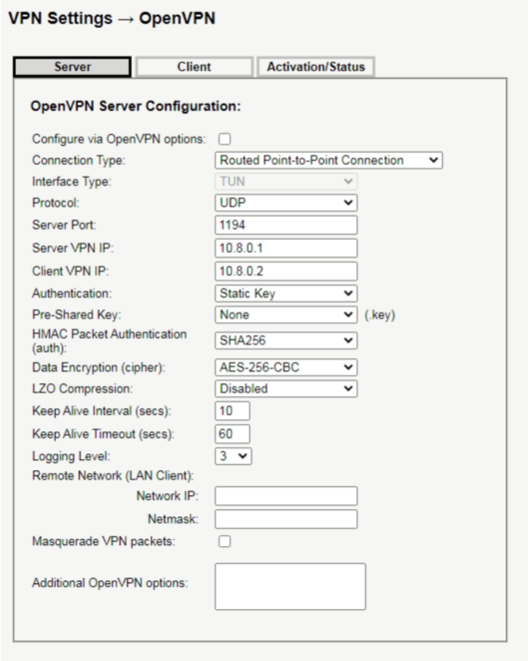


Connection to Open VPN Server

When you enable Open VPN Client, you need two routers to create site-to-site VPN connections. The server IP and client IP address should be within the same network domain.



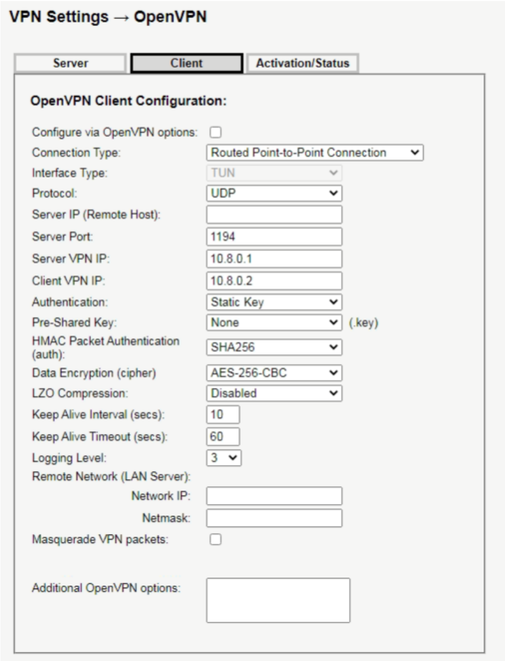
Open VPN Server and Client Connection



VPN Settings → OpenVPN

OpenVPN Server Configuration:

Configure via OpenVPN options: □
Connection Type: Routed Point-to-Point Connection
Interface Type: TUN
Protocol: UDP
Server Port: 1194
Server VPN IP: 10.8.0.1
Client VPN IP: 10.8.0.2
Authentication: Static Key
Pre-Shared Key: None (.key)
HMAC Packet Authentication (auth): SHA256
Data Encryption (cipher): AES-256-CBC
LZO Compression: Disabled
Keep Alive Interval (secs): 10
Keep Alive Timeout (secs): 60
Logging Level: 3
Remote Network (LAN Client):
Network IP:
Netmask:
Masquerade VPN packets: □
Additional OpenVPN options:



VPN Settings → OpenVPN

OpenVPN Client Configuration:

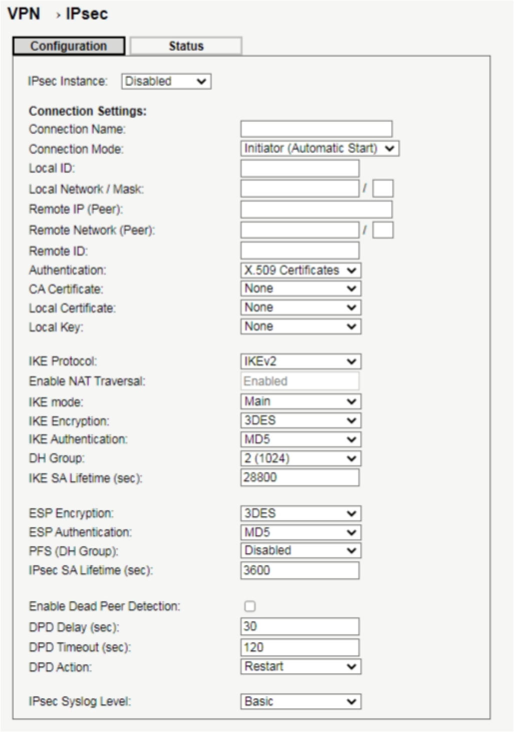
Configure via OpenVPN options: □
Connection Type: Routed Point-to-Point Connection
Interface Type: TUN
Protocol: UDP
Server IP (Remote Host):
Server Port: 1194
Server VPN IP: 10.8.0.1
Client VPN IP: 10.8.0.2
Authentication: Static Key
Pre-Shared Key: None (.key)
HMAC Packet Authentication (auth): SHA256
Data Encryption (cipher): AES-256-CBC
LZO Compression: Disabled
Keep Alive Interval (secs): 10
Keep Alive Timeout (secs): 60
Logging Level: 3
Remote Network (LAN Server):
Network IP:
Netmask:
Masquerade VPN packets: □
Additional OpenVPN options:

Label	**Description**
Connection Type	**Routed Point-to-Point / Multi-Client connection**: In a layer 3 network (Interface type - TUN), the clients can reach each other only by using IP addresses. The MAC address of the tun adapter is never revealed to the other VPN clients or even to the OpenVPN server itself. Because of this, a layer 3 network packet is slightly shorter than a layer 2 network packet. Under normal circumstances, the longer layer 2 network packets will not have a negative impact on performance. **Bridge Ethernet connection**: In a layer 2 network (Interface type - TAP), neighboring clients can reach each other by probing the address of a neighbor using ARP broadcasts. The ARP broadcasts allow the clients to discover the MAC address of the other clients. This allows the clients to reach each other over both IP and non-IP protocols.
Tunnel Protocol	Select **UDP** or **TCP** protocol depending on your needs. TCP is more reliable than UDP, but UDP performs better than TCP. It is recommended to use UDP if the distance between VPN server and client is short; otherwise, use TCP.
Port	The number of the port (default is **1194**).
LZO Compression	Enable or disable the function of LZO Compression

Keys Setting	Select **Auto** to use preset certificates or **Manual** to use your certificates. Please install OpenVPN client software to generate your certificates and paste them here. For more information, please visit OpenVPN website.

IPSec VPN

IPsec VPN provides secure IP communications by authenticating and encrypting each IP packet of a communication session. Setting up site-to-site IPSec VPN connection in general involves two phases. Phase 1 is called IKE or ISAKMP SA (Security Association) establishment and Phase 2 is called IPSec SA establishment. This page allows you to configure IPSec VPN settings.



IPsec Instance: Disabled

Connection Settings:
Connection Name:
Connection Mode: Initiator (Automatic Start)
Local ID:
Local Network / Mask: /
Remote IP (Peer):
Remote Network (Peer): /
Remote ID:
Authentication: X.509 Certificates
CA Certificate: None
Local Certificate: None
Local Key: None

IKE Protocol: IKEv2
Enable NAT Traversal: Enabled
IKE mode: Main
IKE Encryption: 3DES
IKE Authentication: MD5
DH Group: 2 (1024)
IKE SA Lifetime (sec): 28800

ESP Encryption: 3DES
ESP Authentication: MD5
PFS (DH Group): Disabled
IPsec SA Lifetime (sec): 3600

Enable Dead Peer Detection: □
DPD Delay (sec): 30
DPD Timeout (sec): 120
DPD Action: Restart

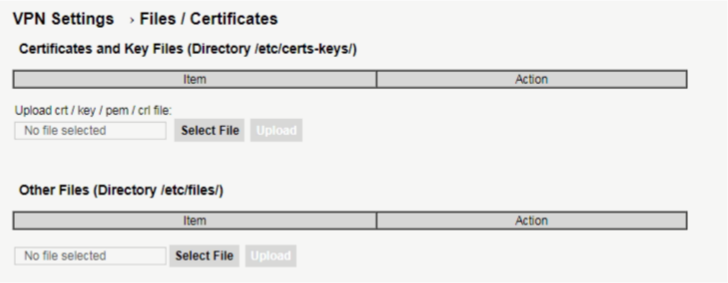
IPsec Syslog Level: Basic

Label	Description
Connection Mode	**Initiator:** it means that the VPN tunnel is initiated from this end **Responder:** it means that the peer initiated the VPN connection**.**
Authentication Type	You can choose to use X.509 digital certificates issued by a CA server to authenticate VPN tunnels between the routers or pre-shared key, a string consisting of alphabets, numbers, and characters that both sites agree to use. The key is then stored (and encrypted) within each VPN device configuration.

IKE Mode	**Main Mode** is more secure in providing identity protection for ISAKMP negotiating nodes, although it requires a static IP address on both IPSec security devices negotiating the VPN tunnel. **Aggressive Mode** is used when one IPSec security device has a dynamic WAN IP address. Aggressive Mode has more configuration requirements than Main Mode and may be difficult or impossible to achieve with some IPSec security device pairings.
IKE Encryption	You can choose to use **DES (Data Encryption Standard)**, **3DES (Triple Data Encryption Standard)**, or **AES (Advanced Encryption Standard)** encryption. AES offers the ultimate in IPSec VPN security and interoperability.
IKE Authentication	This specifies the authentication algorithm used in the ISAKMP negotiation. SHA1 is generally considered cryptographically stronger than MD5 but it requires more computing cycles to calculate so SHA1 is used in environments that require superior overall security.
DH Group	Specifies the DH (Diffie-Hellman) group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The lower the DH group no., the less CPU time it requires to execute. The higher the DH no., the greater the security.
IKE SA Lifetime	Specifies the SA lifetime. The default is 86,400 seconds. Remember, a shorter lifetime provides more secure ISAKMP negotiations (up to a point). However, with shorter lifetimes, the security appliance sets up future IPsec SAs more quickly.

Certificates

Certificate uploaded here for VPN using.



VPN Settings › Files / Certificates

Certificates and Key Files (Directory /etc/certs-keys/)

Item	Action

Upload crt / key / pem / crl file:

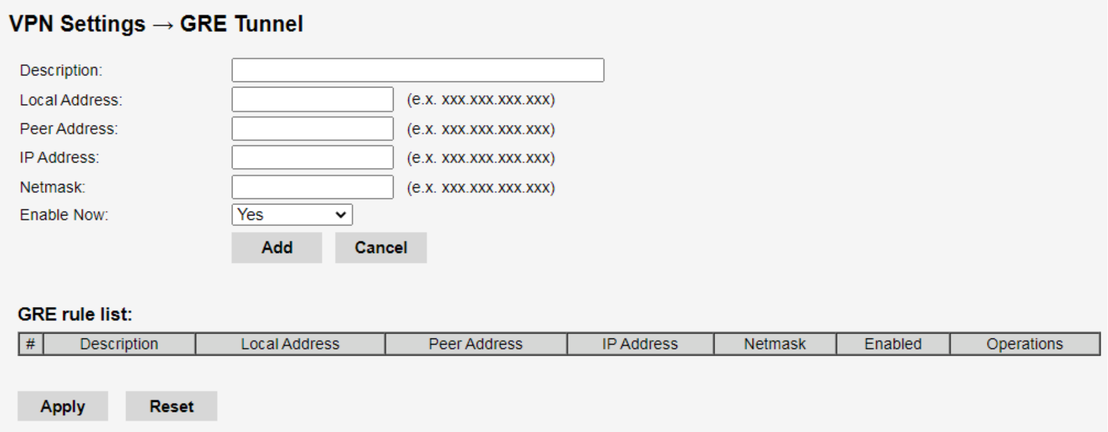
No file selected

Other Files (Directory /etc/files/)

Item	Action

No file selected

GRE Tunnel



VPN Settings → GRE Tunnel

Description:
Local Address: (e.x. xxx.xxx.xxx.xxx)
Peer Address: (e.x. xxx.xxx.xxx.xxx)
IP Address: (e.x. xxx.xxx.xxx.xxx)
Netmask: (e.x. xxx.xxx.xxx.xxx)
Enable Now: Yes

GRE rule list:

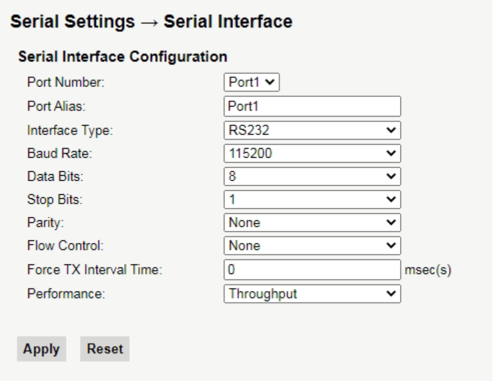
#	Description	Local Address	Peer Address	IP Address	Netmask	Enabled	Operations

Label	Description
Description	Specify Description for each GRE Tunnel
Local Address	Specify Local Address for each GRE Tunnel
Peer Address	Specify Peer Address for each GRE Tunnel
IP Address	Specify IP Address for each GRE Tunnel
Netmask	Specify Netmask for each GRE Tunnel
Enable Now	Select to enable or disable GRE Tunnel item list

2.2.8 Serial Settings

Serial Interface

This page allows you to configure serial port parameters.



Serial Settings → Serial Interface

Serial Interface Configuration

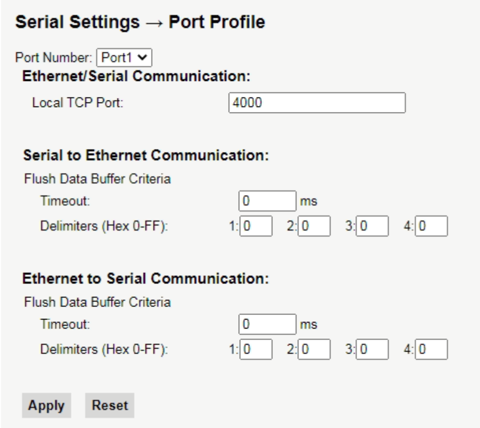
Port Number: Port1
Port Alias: Port1
Interface Type: RS232
Baud Rate: 115200
Data Bits: 8
Stop Bits: 1
Parity: None
Flow Control: None
Force TX Interval Time: 0 msec(s)
Performance: Throughput

Label	Description
Port Alias	Enter the COM port number that modem is connected to
Interface Type	Choose an interface for your serial device. Available interfaces include **RS-232, RS-422, RS-485(2-wires), and RS-485(4-wires),**
Baud Rate	Choose a baud rate in the range between 110 bps and 460800

	bps.
Data Bits	Choose the number of data bits to transmit. You can configure data bits to be 7, or 8. Data is transmitted as a series of five, six, seven, or eight bits (five and six bit data formats are used rarely for specialized communications equipment).
Stop Bits	Choose the number of bits used to indicate the end of a byte. You can configure stop bits to be 1 or 2(1.5). If Stop Bits is 1.5, the stop bit is transferred for 150% of the normal time used to transfer one bit. Both the computer and the peripheral device must be configured to transmit the same number of stop bits.
Parity	Chose the method of detecting errors in transmission. Parity control bit modes include None, Odd, Even, Mark, and Space. **None**: parity checking is not performed and the parity bit is not transmitted. **Odd**: the number of mark bits in the data is counted, and the parity bit is asserted or unasserted to obtain an odd number of mark bits. **Even**: the number of mark bits in the data is counted, and the parity bit is asserted or unasserted to obtain an even number of mark bits. **Mark**: the parity bit is always set to the mark signal condition (logical 1) **Space**: the last transmitted data bit will always be a logical 0
Flow Control	Serial communication consists of hardware flow control and software flow control, so called as the control is handled by software or hardware. **XOFF** and **OXN** is software flow control while **RTS/CTS or DTR/DSR** is hardware flow control. Choose **XOFF** to tell the computer to stop sending data; then the receiving side will send an XOFF character over its Tx line to tell the transmitting side to stop transmitting. Choose **XON** to tell the computer to begin sending data again; then the receiving side will send an XON character over its Tx line to tell the transmitting side to resume transmitting. In hardware flow control mode, when the device is ready to receive data, it sends a CTS (Clear To Send) signal to the device on the other end. When a device has something it wants to send, it will send a

	RTS (Ready To Send) signal and waits for a CTS signal to come back its way. These signals are sent apart from the data itself on separate wires.
ForceTX Interval Time	Force TX interval time is to specify the timeout when no data has been transmitted. When the timeout is reached or TX buffer is full (4K Bytes), the queued data will be sent. **0** means disable. Factory default value is **0**.
Performance	**Throughput**: This mode optimized for highest transmission speed. **Latency**: This mode optimized for shortest response time.

Port profile



Serial Settings → Port Profile

Port Number: Port1

Ethernet/Serial Communication:

Local TCP Port: 4000

Serial to Ethernet Communication:

Flush Data Buffer Criteria

Timeout: 0 ms

Delimiters (Hex 0-FF): 1: 0 2: 0 3: 0 4: 0

Ethernet to Serial Communication:

Flush Data Buffer Criteria

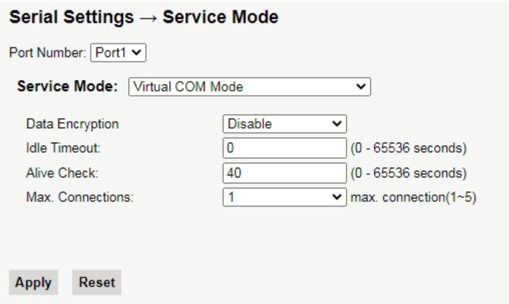
Timeout: 0 ms

Delimiters (Hex 0-FF): 1: 0 2: 0 3: 0 4: 0

Label	Description
Local TCP Port	The TCP port the device uses to listen to connections, and that other devices must use to contact the device. To avoid conflicts with well known TCP ports, the default is set to 4000.
Flush Data Buffer After	The received data will be queuing in the buffer until all the delimiters are matched. When the buffer is full (4K Bytes) or after "**flush S2E data buffer**" timeout the data will also be sent. You can set the time from 0 to 65535 seconds.
Delimiter	For advanced data packing options, you can specify delimiters for **Serial to Ethernet** and / or **Ethernet to Serial** communications. You can define max. 4 delimiters (00~FF, Hex) for each way. The data will be hold until the delimiters are received or the option **Flush Serial to Ethernet data buffer** times out. **0** means disable. Factory default is **0**.

Service Mode-Virtual COM Mode

In Virtual COM Mode, the driver establishes a transparent connection between the host and the serial device by mapping the port of the serial server to a local COM port on the host computer. Virtual COM Mode also supports up to 5 simultaneous connections, so that multiple hosts can send or receive data by the same serial device at the same time.



Serial Settings → Service Mode

Port Number: Port1

Service Mode: Virtual COM Mode

Data Encryption: Disable

Idle Timeout: 0 (0 - 65536 seconds)

Alive Check: 40 (0 - 65536 seconds)

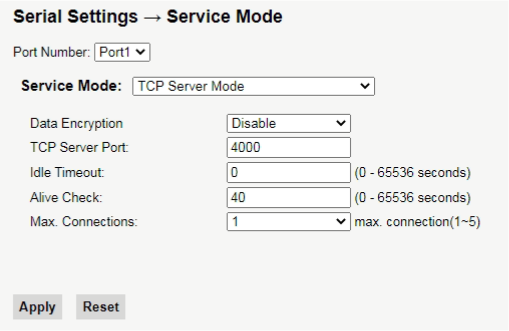
Max. Connections: 1 max. connection(1~5)

Label	Description
Data Encryption	Click on the radio button to enable or disable data encryption
Idle Timeout	When serial port stops data transmission for a defined period of time, the connection will be closed and the port will be freed and try to connect with other hosts. 0 indicate disable this function. Factory default value is **0**. If Multilink is configured, only the first host connection is effective for this setting.
Alive Check	The serial device will send TCP alive-check packages in each defined time interval to remote host to check the TCP connection. If the TCP connection is not alive, the connection will be closed and the port will be freed. **0** indicate disable this function. Factory default is **0**.
Max Connection	The number of Max connection can support simultaneous connections are **5**, default values is **1**.

*Not allowed to mapping Virtual COM from web

Service Mode – TCP Server Mode

In TCP Server Mode, DS is configured with a unique port combination on a TCP/IP network. In this case, DS waits passively to be contacted by the device. After the device establishes a connection with the serial device, it can then proceed with data transmission. TCP Server mode also supports up to 5 simultaneous connections, so that multiple device can receive data from the same serial device at the same time.



Serial Settings → Service Mode

Port Number: Port1

Service Mode: TCP Server Mode

Data Encryption: Disable

TCP Server Port: 4000

Idle Timeout: 0 (0 - 65536 seconds)

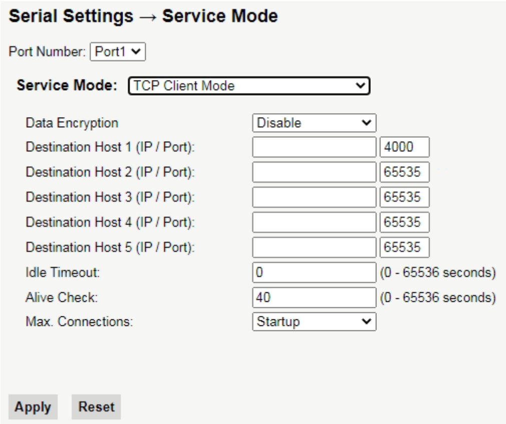
Alive Check: 40 (0 - 65536 seconds)

Max. Connections: 1 max. connection(1~5)

Label	Description
Data Encryption	Click on the radio button to enable or disable data encryption
TCP Server Port	Enter the TCP server port number
Idle Timeout	When serial port stops data transmission for a defined period of time, the connection will be closed and the port will be freed and try to connect with other hosts. 0 indicate disable this function. Factory default value is **0**. If Multilink is configured, only the first host connection is effective for this setting.
Alive Check	The serial device will send TCP alive-check package in each defined time interval (Alive Check) to remote host to check the TCP connection. If the TCP connection is not alive, the connection will be closed and the port will be freed. **0** indicate disable this function. Factory default is **0**.
Max Connection	The serial device will send TCP alive-check packages in each defined time interval to remote host to check the TCP connection. If the TCP connection is not alive, the connection will be closed and the port will be freed. 0 indicate disable this function. Factory default is 0.

Service Mode – TCP Client Mode

In TCP Client Mode, the device can establish a TCP connection with the server by the method you set (Startup or any character). After the data has been transferred, the device can disconnect automatically from the server by using the TCP alive check time or idle timeout settings.



Serial Settings → Service Mode

Port Number: Port1

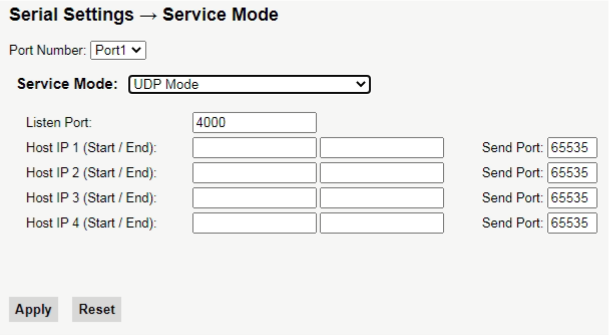
Service Mode: TCP Client Mode

Data Encryption	Disable	
Destination Host 1 (IP / Port):		4000
Destination Host 2 (IP / Port):		65535
Destination Host 3 (IP / Port):		65535
Destination Host 4 (IP / Port):		65535
Destination Host 5 (IP / Port):		65535
Idle Timeout:	0	(0 - 65536 seconds)
Alive Check:	40	(0 - 65536 seconds)
Max. Connections:	Startup	

Label	Description
Data Encryption	Click on the radio button to enable or disable data encryption
Destination Host	Set the IP address of host and the port number of data port.
Idle Timeout	When serial port stops data transmission for a defined period of time, the connection will be closed, and the port will be freed and try to connect with other hosts. 0 indicate disable this function. Factory default value is **0**. If Multilink is configured, only the first host connection is effective for this setting.
Alive Check	The serial device will send TCP alive-check packages in each defined time interval to remote host to check the TCP connection. If the TCP connection is not alive, the connection will be closed and the port will be freed. **0** indicate disable this function. Factory default is **0**.
Connect on Startup	The TCP Client will build TCP connection once the connected serial device is started.
Connect on Any Character	The TCP Client will build TCP connection once the connected serial device starts to send data.

Service Mode – UDP Mode

Compared to TCP communications, UDP is faster and more efficient. In UDP mode, you can uni-cast or multi-cast data from the serial device server to host computers, and the serial device can also receive data from one or multiple host.



Serial Settings → Service Mode

Port Number: Port1

Service Mode: UDP Mode

Listen Port: 4000

Host IP 1 (Start / End): Send Port: 65535

Host IP 2 (Start / End): Send Port: 65535

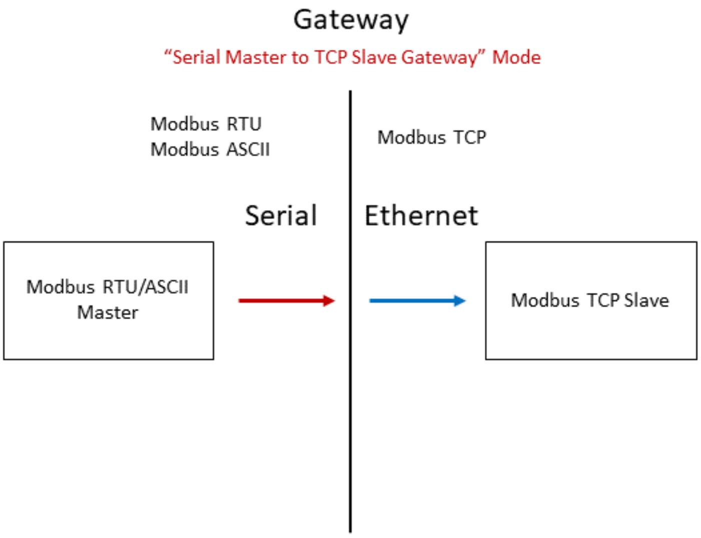
Host IP 3 (Start / End): Send Port: 65535

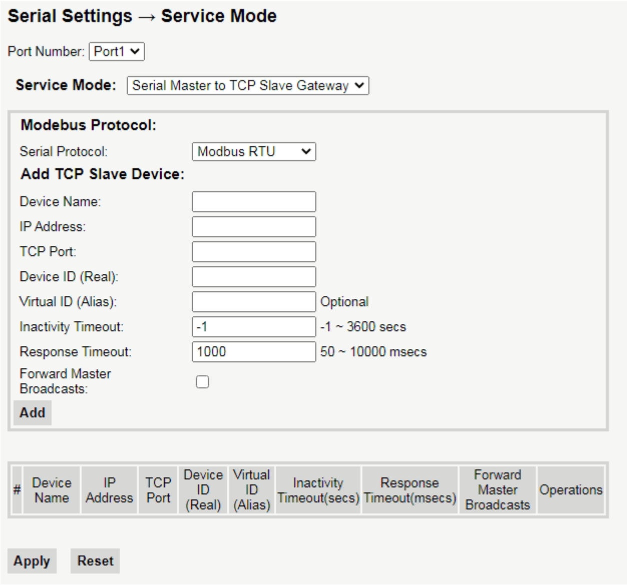
Host IP 4 (Start / End): Send Port: 65535

Label	Description
Listen Port	Allows the user to set a new TCP port number to listen on rather than the default value of the device
Host Start/End IP	If there are more than one destination hosts, specify the IP address range by inputting a value in **Host Start** / **End IP**. You can also auto scan the sending port number of the device
Send Port	Set the send port number.

Serial Master to TCP Slave Gateway

In Serial Master to TCP Slave mode, it can be used to integrate Modbus TCP Slaves into a serial Modbus application (RS232/RS422/RS485) with a Modbus RTU/ASCII Master, typical application as below drawing. The Modbus RTU/ASCII Master can access each defined Modbus TCP Slaves via Device ID just like Modbus RTU/ASCII Slaves, if Modbus RTU/ASCII Master starts a request to a Device ID defined to a Modbus TCP Slave, the gateway receives and converts the Modbus RTU/ASCII request into Modbus TCP protocol, also, the Modbus TCP packets will be forwarded to the Modbus TCP Slave. At last, the Modbus TCP Slave will handle the response for the request from Modbus RTU/ASCII Master. There are up to 16 TCP Slave connections can be configured.





Serial Settings → Service Mode

Port Number: Port1

Service Mode: Serial Master to TCP Slave Gateway

Modebus Protocol:

Serial Protocol: Modbus RTU

Add TCP Slave Device:

Device Name:

IP Address:

TCP Port:

Device ID (Real):

Virtual ID (Alias): Optional

Inactivity Timeout: -1 | -1 ~ 3600 secs

Response Timeout: 1000 | 50 ~ 10000 msecs

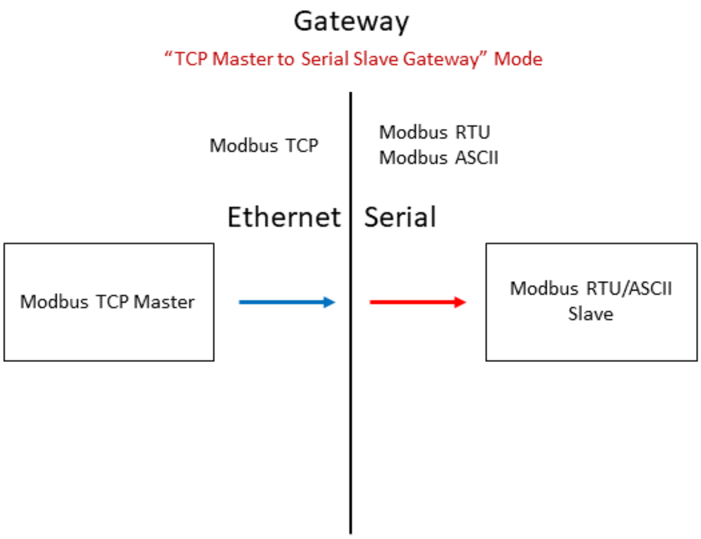
Forward Master Broadcasts: □

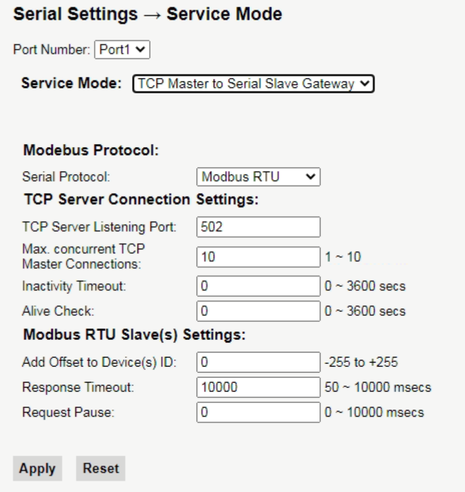
#	Device Name	IP Address	TCP Port	Device ID (Real)	Virtual ID (Alias)	Inactivity Timeout(secs)	Response Timeout(msecs)	Forward Master Broadcasts	Operations

Label	Description
Device Name	Remote Device name
IP Address	Set the IP address of host
TCP Port	the port number of data port
Inactivity Timeout	When serial port stops data transmission for a defined period of time, the connection will be closed and the port will be freed and try to connect with other hosts. **0** indicates disabling this function and is also the factory default value. If multilink is configured, only the first host connection is effective for this setting.
Response Timeout	The serial device will send TCP alive-check packages in each defined time interval to remote host to check the TCP connection. If the TCP connection is not alive, the connection will be closed and the port will be freed. **0** indicates disabling this function. Factory default is **0**.

TCP Master to Serial Slave Gateway

In TCP Master to Serial Slave Gateway mode, it can access serial Modbus RTU/ASCII Slaves from one or more Ethernet-based Mobus TCP Master(s). The Modbus TCP Master sends a request to a Mobus RTU/ASCII Slave, the gateway will receive Mobus TCP packets and convert to Modbus RTU/ASCII request based on Device ID, also, it will forward converted request to the serial interface, at last, the Modbus RTU/ASCII Slave will handle the request and make response. There are up to 10 TCP Master connections can be configured.





Serial Settings → Service Mode

Port Number: Port1

Service Mode: TCP Master to Serial Slave Gateway

Modebus Protocol:

Serial Protocol: Modbus RTU

TCP Server Connection Settings:

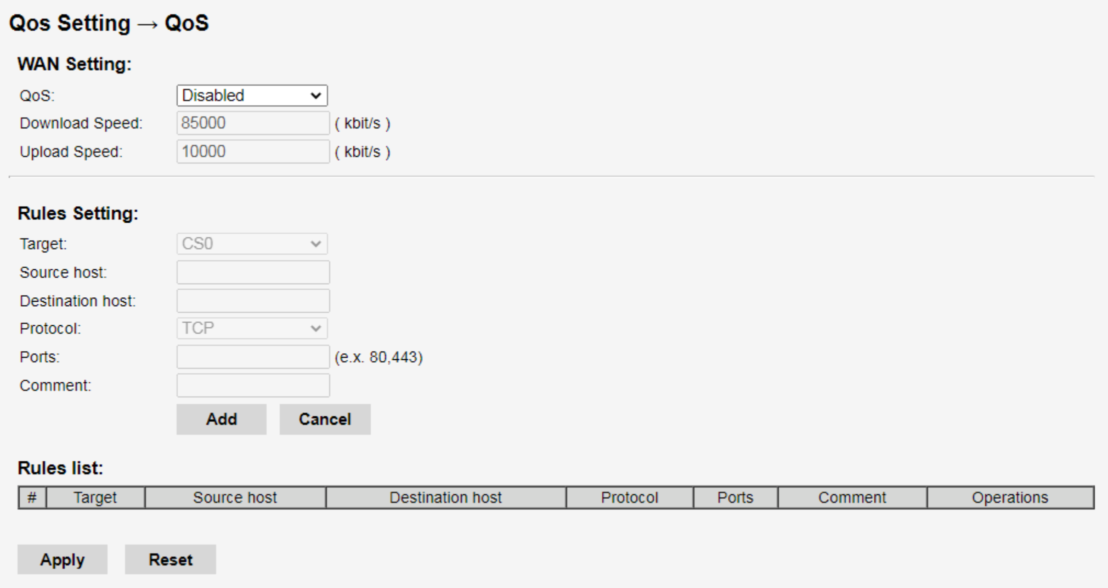
TCP Server Listening Port:	502	
Max. concurrent TCP Master Connections:	10	1 ~ 10
Inactivity Timeout:	0	0 ~ 3600 secs
Alive Check:	0	0 ~ 3600 secs

Modbus RTU Slave(s) Settings:

Add Offset to Device(s) ID:	0	-255 to +255
Response Timeout:	10000	50 ~ 10000 msecs
Request Pause:	0	0 ~ 10000 msecs

Label	Description
TCP Server Listening Port	Indicates the port used for the Modbus/TCP communication
Max TCP Master Connection	The total number of remote TCP/IP clients allowed to connect to this server.

2.2.9 QoS



Qos Setting → QoS

WAN Setting:

QoS:	Disabled	
Download Speed:	85000	(kbit/s)
Upload Speed:	10000	(kbit/s)

Rules Setting:

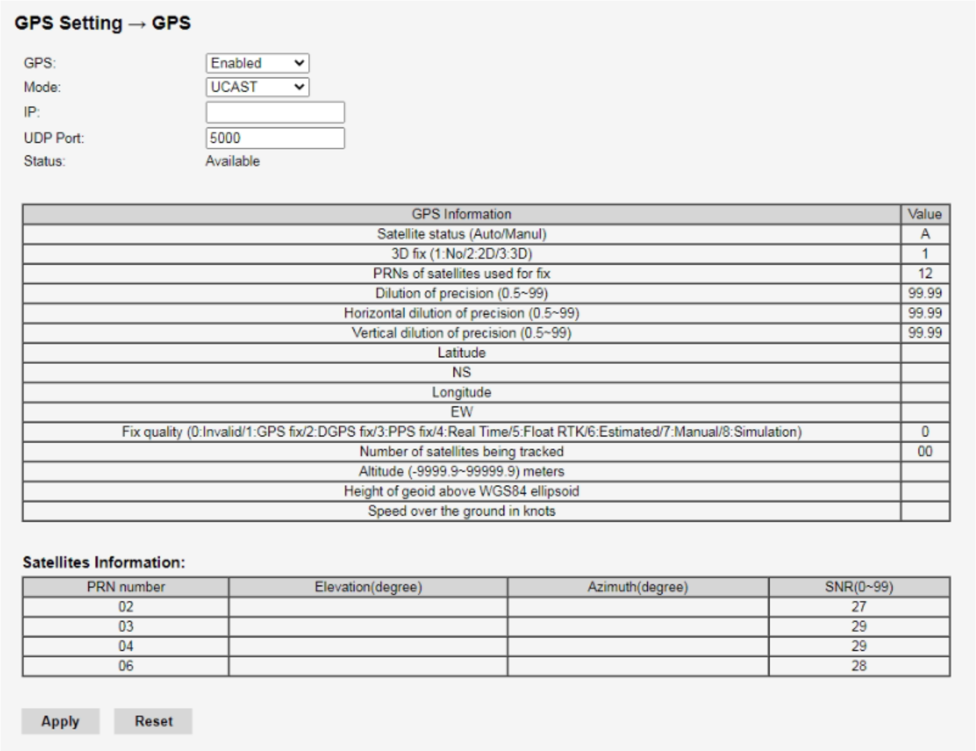
Target:	CS0	
Source host:		
Destination host:		
Protocol:	TCP	
Ports:		(e.x. 80,443)
Comment:		

Rules list:

#	Target	Source host	Destination host	Protocol	Ports	Comment	Operations

Label	Description
QoS	Select to enable or disable QoS
Download Speed	Specify Download Speed for WAN interface
Upload Speed	Specify Upload Speed for WAN interface
Target	Specify Target for QoS rule
Source host	Specify Source host for QoS rule
Destination host	Specify Destination host for QoS rule
Protocol	Specify Protocol for QoS rule
Ports	Specify Ports for QoS rule
Comment	Enter the comment for QoS rule

2.2.10 GPS Setting



GPS Setting → GPS

GPS: Enabled

Mode: UCAST

IP:

UDP Port: 5000

Status: Available

GPS Information	Value
Satellite status (Auto/Manul)	A
3D fix (1:No/2:2D/3:3D)	1
PRNs of satellites used for fix	12
Dilution of precision (0.5~99)	99.99
Horizontal dilution of precision (0.5~99)	99.99
Vertical dilution of precision (0.5~99)	99.99
Latitude	
NS	
Longitude	
EW	
Fix quality (0:Invalid/1:GPS fix/2:DGPS fix/3:PPS fix/4:Real Time/5:Float RTK/6:Estimated/7:Manual/8:Simulation)	0
Number of satellites being tracked	00
Altitude (-9999.9~99999.9) meters	
Height of geoid above WGS84 ellipsoid	
Speed over the ground in knots	

Satellites Information:

PRN number	Elevation(degree)	Azimuth(degree)	SNR(0~99)
02			27
03			29
04			29
06			28

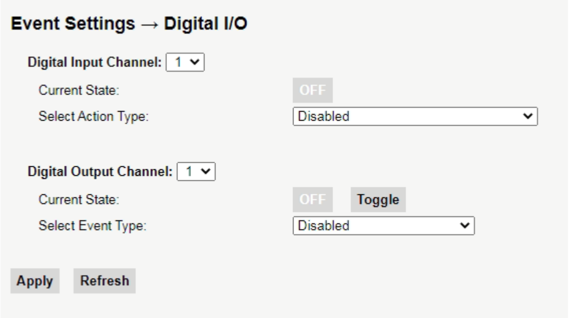
Send the GPS detail information to specify IP address

Label	Description
GPS	Enable/Disable GPS function
Mode	UCAST mode (unicast) / MCAST mode (multicast)
IP	Assign Specify IP address
UDP Port	Assign Specify UDP Port number
Status	Current GPS status

2.2.11 Event Setting

When an error occurs, the device will notify you through system log, and SNMP messages. You can configure the system to issue a notification when specific events occur by checking the box next to the event.

Digital I/O



Event Settings → Digital I/O

Digital Input Channel: 1

Current State: OFF

Select Action Type: Disabled

Digital Output Channel: 1

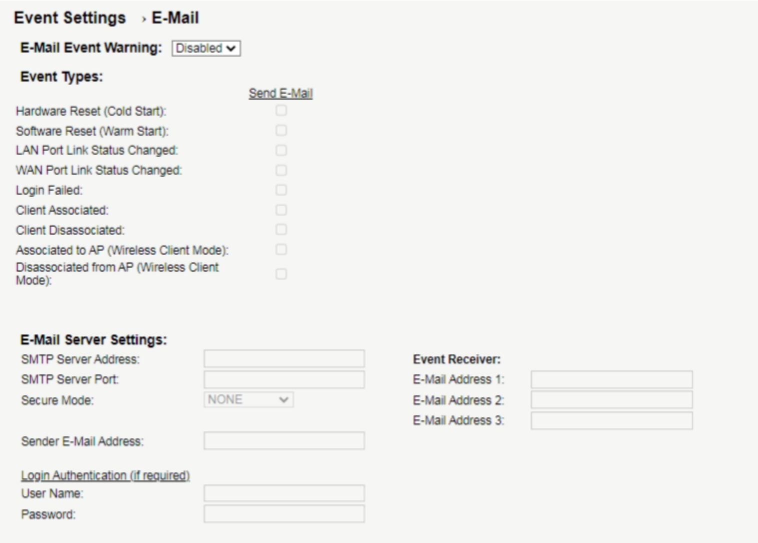
Current State: OFF

Select Event Type: Disabled

Label	Description
Digital Input	When Channel 1 and 2 State changed will action one of below **Start/Stop OpenVPN Server** or **Connect/Disconnect OpenVPN Client.**
Digital Output	manually or one of events below occur **OpenVPN Server status** or **OpenVPN Client status** will toggle channel 1 and 2 state

E-Mail

Send the event alart via Email.



Event Settings › E-Mail

E-Mail Event Warning: Disabled

Event Types:

	Send E-Mail
Hardware Reset (Cold Start):	□
Software Reset (Warm Start):	□
LAN Port Link Status Changed:	□
WAN Port Link Status Changed:	□
Login Failed:	□
Client Associated:	□
Client Disassociated:	□
Associated to AP (Wireless Client Mode):	□
Disassociated from AP (Wireless Client Mode):	□

E-Mail Server Settings:

SMTP Server Address:

SMTP Server Port:

Secure Mode: NONE

Sender E-Mail Address:

Login Authentication (if required)

User Name:

Password:

Event Receiver:

E-Mail Address 1:

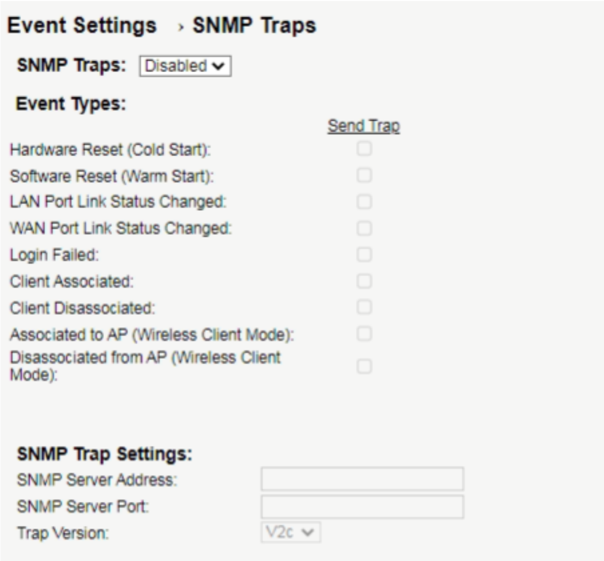
E-Mail Address 2:

E-Mail Address 3:

Label	Description
SMTP Server	Enter a backup host to be used when the primary host is unavailable.
Server Port	Specifies the port where MTA can be contacted via SMTP server
E-mail Address 1-3	Enter the mail address that will receive notifications

SNMP Traps

Send event alart via SNMP trap protocol.



Event Settings › SNMP Traps

SNMP Traps: Disabled

Event Types:

	Send Trap
Hardware Reset (Cold Start):	□
Software Reset (Warm Start):	□
LAN Port Link Status Changed:	□
WAN Port Link Status Changed:	□
Login Failed:	□
Client Associated:	□
Client Disassociated:	□
Associated to AP (Wireless Client Mode):	□
Disassociated from AP (Wireless Client Mode):	□

SNMP Trap Settings:

SNMP Server Address:

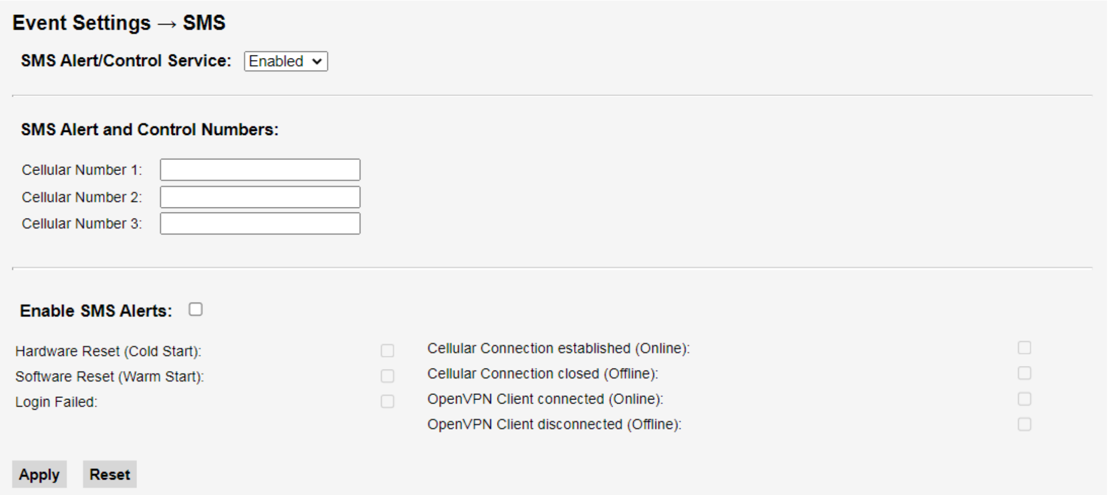
SNMP Server Port:

Trap Version: V2c

Label	Description
SNMP Server Address	Enter the IP address of the SNMP server which will send out traps generated by the AP.
SNMP Server Port	Enter Trap server using port
Trap Version	Support V2c

SMS

Send the event alert and control device via SMS



Event Settings → SMS

SMS Alert/Control Service: Enabled

SMS Alert and Control Numbers:

Cellular Number 1:

Cellular Number 2:

Cellular Number 3:

Enable SMS Alerts: □

Hardware Reset (Cold Start): □

Software Reset (Warm Start): □

Login Failed: □

Cellular Connection established (Online): □

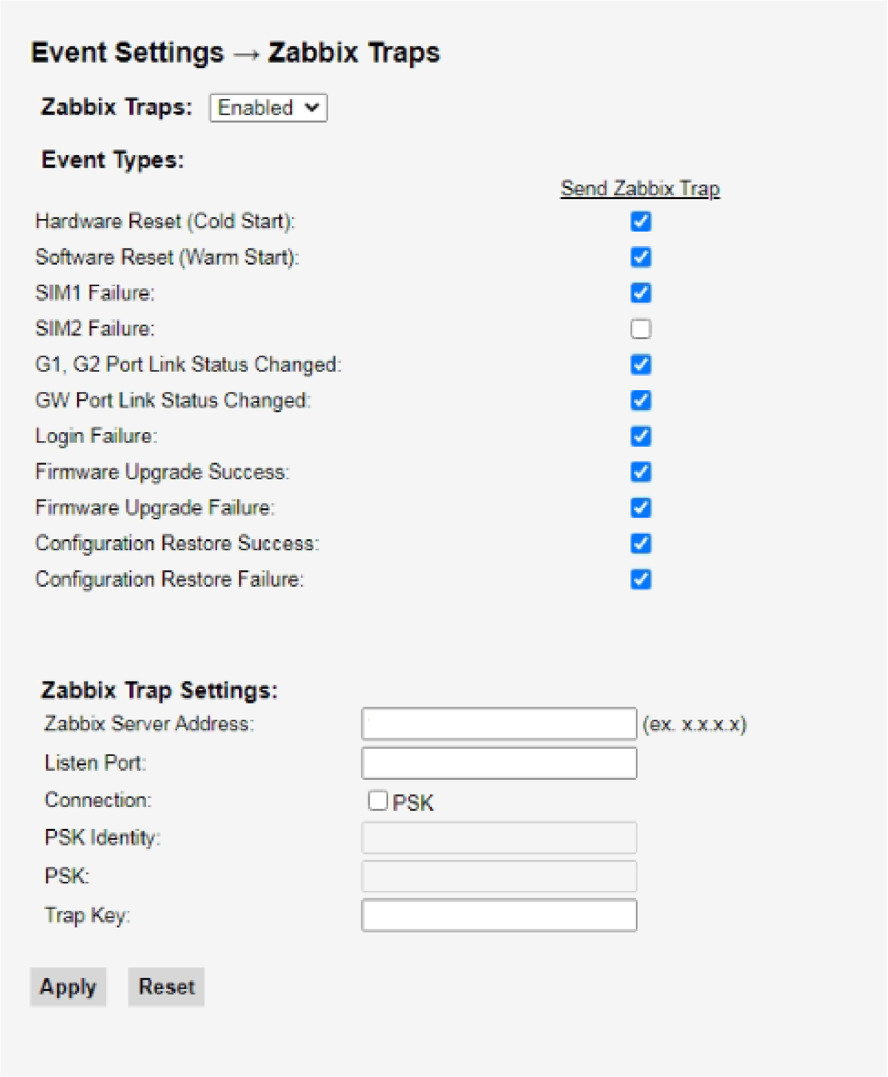
Cellular Connection closed (Offline): □

OpenVPN Client connected (Online): □

OpenVPN Client disconnected (Offline): □

Zabbix Trap

Send Event with Zabbix Traps



Event Settings → Zabbix Traps

Zabbix Traps: Enabled

Event Types:

	Send Zabbix Trap
Hardware Reset (Cold Start):	☑
Software Reset (Warm Start):	☑
SIM1 Failure:	☑
SIM2 Failure:	□
G1, G2 Port Link Status Changed:	☑
GW Port Link Status Changed:	☑
Login Failure:	☑
Firmware Upgrade Success:	☑
Firmware Upgrade Failure:	☑
Configuration Restore Success:	☑
Configuration Restore Failure:	☑

Zabbix Trap Settings:

Zabbix Server Address: (ex. x.x.x.x)

Listen Port:

Connection: □ PSK

PSK Identity:

PSK:

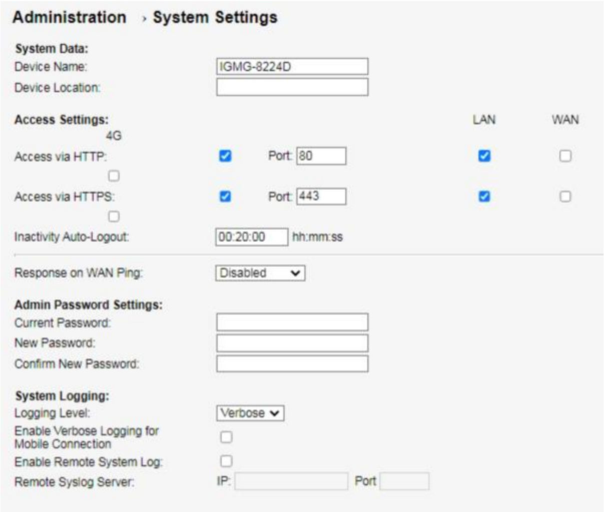
Trap Key:

Label	Description
Zabbix Server Address	Specify Server IP for Zabbix Trap
Listen Port	Specify Listening Port for Zabbix Trap
Connection	Check to enable encryption with Zabbix Trap
PSK Identity	Specify PSK Identity for Zabbix Trap
PSK	Specify PSK for Zabbix Trap
Trap Key	Specify Trap Key for Zabbix Trap

2.2.12 Administration

System Setting

System setting include web access setting, Web login name and password in page; default login name and password are both **admin** and system log server setting.



Administration › System Settings

System Data:
Device Name: IGMG-8224D
Device Location:

Access Settings: LAN WAN
4G
Access via HTTP: ☑ Port: 80 ☑ □
□
Access via HTTPS: ☑ Port: 443 ☑ □
□
Inactivity Auto-Logout: 00:20:00 hh:mm:ss

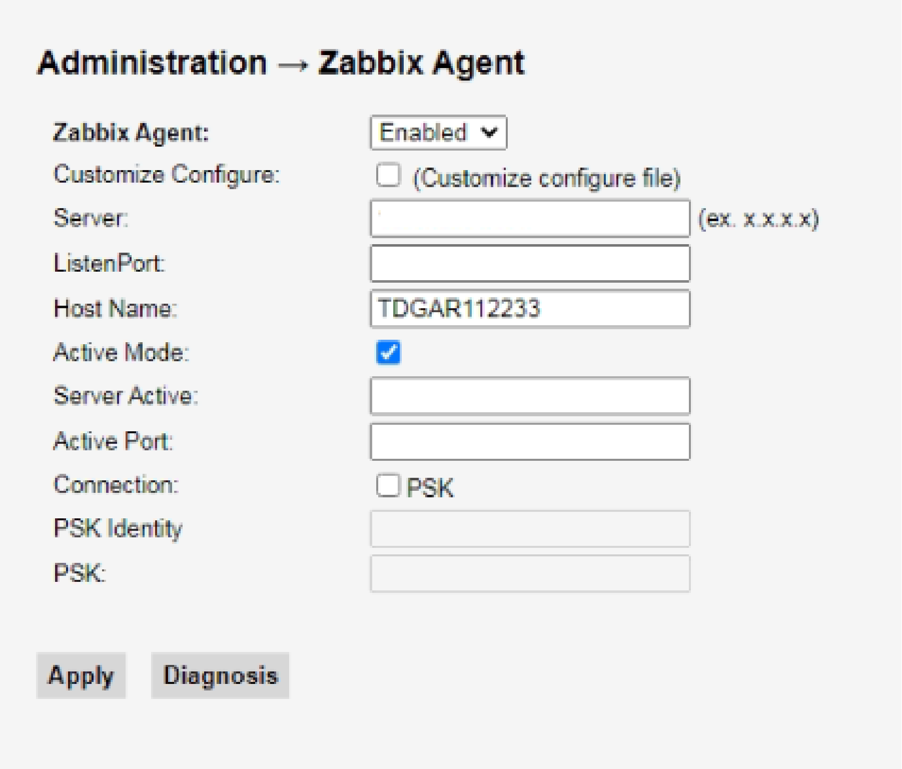
Response on WAN Ping: Disabled

Admin Password Settings:
Current Password:
New Password:
Confirm New Password:

System Logging:
Logging Level: Verbose
Enable Verbose Logging for Mobile Connection □
Enable Remote System Log: □
Remote Syslog Server: IP: Port

Label	**Description**
Device Name	Assign name for device
Device Location	Type in device location
Confirm New Password	Retype the new password to confirm it.
Access setting	Choose a web management page protocol from **HTTP** and **HTTPS**. HTTPS (HTTP over SSL) encrypts data sent and received over the Web. Choose HTTPS if you want a secure connection.
Port	Choose a web management page port number. For HTTP, default port is 80. For HTTPS, default port is 443.
Response on WAN Ping	Click Enable to allow system administrator to ping the router from WAN interface
Remote Syslog IP	Enter the IP address of a remote server if you want the logs to be stored remotely. Leave it blank will disable remote syslog.
Remote Syslog Port	Specifies the port to be logged remotely. Default port is 514.

Zabbix Agent

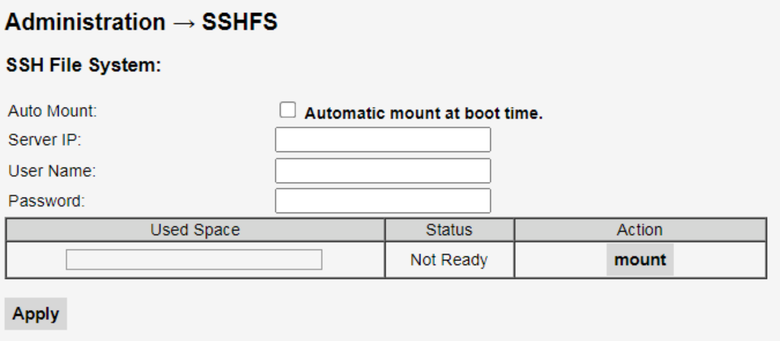


Administration → Zabbix Agent

Zabbix Agent:	Enabled
Customize Configure:	□ (Customize configure file)
Server:	(ex. x.x.x.x)
ListenPort:	
Host Name:	TDGAR112233
Active Mode:	☑
Server Active:	
Active Port:	
Connection:	□ PSK
PSK Identity	
PSK:	

Label	Description
Zabbix Agent	Select to enable or disable Zabbix Agent
Customize Configure	Check and copy-paste custom configuration as plain text
Server	Specify Server IP for Zabbix Agent
Listen Port	Specify Listening Port for Zabbix Agent
Host Name	Specify Host Name for Zabbix Agent
Active Mode	Check to enable active mode with Zabbix Agent
Server Active	Specify Server IP for Zabbix Agent (Active Mode)
Active Port	Specify Listening Port for Zabbix Agent (Active Mode)
Connection	Check to enable encryption with Zabbix Agent
PSK Identity	Specify PSK Identity for Zabbix Agent
PSK	Specify PSK for Zabbix Agent

SSHFS



Administration → SSHFS

SSH File System:

Auto Mount: □ Automatic mount at boot time.

Server IP:

User Name:

Password:

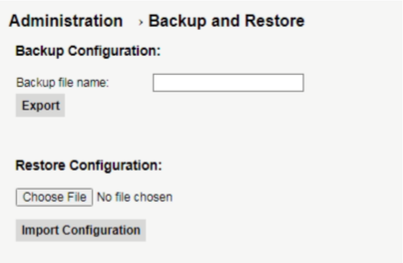
Used Space	Status	Action
	Not Ready	mount

Apply

Label	Description
Auto Mount	Check to enable auto mount disk at boot time
Server IP	Specify Server IP of remote server
User Name	Specify User Name of remote server
Password	Specify Password of remote server
mount	Click **mount** to mount disk from remote server

Backup and Restore Configurations

This page allows you to save configurations or return settings to previous status. You can download the configuration file from the Web. Note: users using old versions of Internet Explorer may have to click on the warning on top of the browser and choose Download File.



Administration › Backup and Restore

Backup Configuration:

Backup file name:

Export

Restore Configuration:

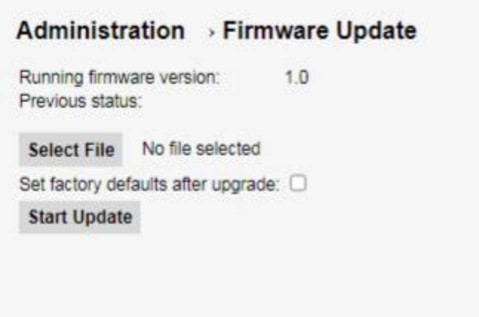
Choose File No file chosen

Import Configuration

Label	Description
Export	Click to Save existing configurations as a file for future usage.
Import	You can restore configurations to previous status by installing a previous configuration file.
Restore Factory Default Setting	Click to reset the router to the factory settings. The router will reboot to validate the default settings.

Firmware Upgrade

ORing launches new firmware constantly to enhance router performance and functions. To upgrade firmware, download new firmware from ORing's website to your PC and install it via Web upgrade. Make sure the firmware file matches the model of your router. It will take several minutes to upload and update the firmware. After upgrade completes successfully, reboot the router.



Administration › Firmware Update

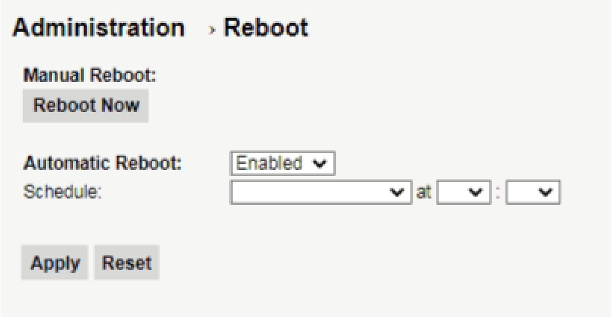
Running firmware version: 1.0
Previous status:

Set factory defaults after upgrade: □

During firmware upgrading, do not turn off the power of the router or press the reset button.

Reboot

This page allows you to configure restart settings for the router.



Administration › Reboot

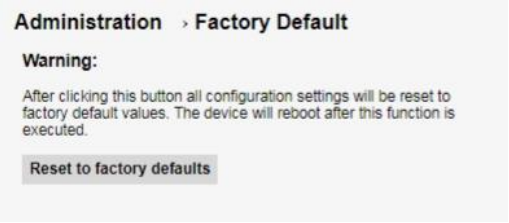
Manual Reboot:

Automatic Reboot: Enabled
Schedule: at :

Label	Description
Reboot Now	Click to restart the router via warm reset
Automatic Reboot	**Enable**: check to activate the setting Reboot at: specify the time for resetting the router. You can configure the action to be performed periodically.

Factory Default

Click to reset the router to the factory settings. The router will reboot to validate the default settings.



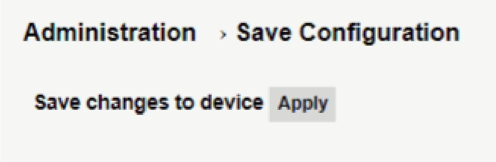
Administration › Factory Default

Warning:

After clicking this button all configuration settings will be reset to factory default values. The device will reboot after this function is executed.

Save device configuration

Click Apply to save all Changes to device.



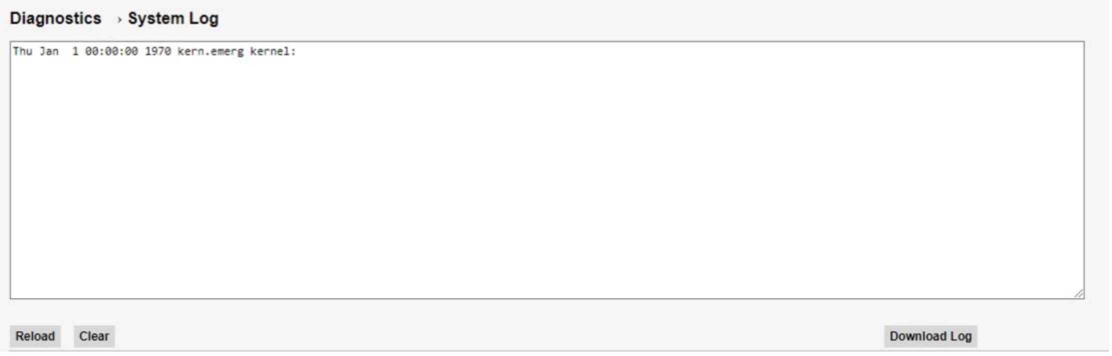
Administration › Save Configuration

Save changes to device

2.2.13 Diagnostics

System Log

The router will constantly log the events and provide the files for you to review. You can click **Reload** to renew the page, **Clear** to clear all or certain log entries and **Download** to save all logs to file.

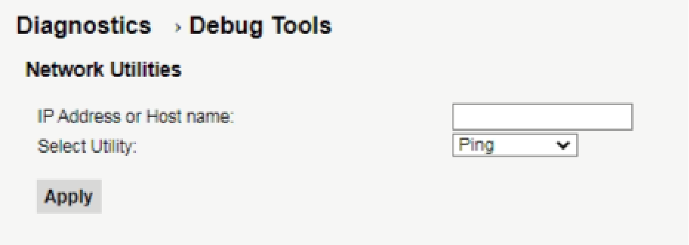


Diagnostics › System Log

```
Thu Jan  1 00:00:00 1970 kern.emerg kernel:
```

Debug Tools

Use utility Tool Ping, Trace Route and NSLookup to check any IP or Host.



Diagnostics › Debug Tools

Network Utilities

IP Address or Host name:

Select Utility: Ping