IGMG-8224D-D5G

Industrial WIFI5 and 5G Cellular Gateway/Router with Serial port and 4x10/100/1000Base-T(X)

User Manual

Version 1.0

January 2024

www.oringnet.com

COPYRIGHT NOTICE

TRADEMARKS

ORing 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 About the IGMG-8224D-D5G

IGMG-8224D-D5G is a reliable WIFI5 and 5G VPN router with 4 ports 10/100/1000Base-T(X) router where one port for WAN and three ports for LAN (LAN1~LAN3). WLAN interfaces support up to 867Mbps link speed with concurrent dual band operating. Also Provide 2 Digital Input and 2 Digital Output and provide full function RS232/422/485 with DB9 connector. It supports MAC filter for security control. It could be configured to operate in 5 modes function: Static, DHCP, DHCP/Fallback, PPPoE authentication, and Cellular WAN Modem dial up. In the mode of Cellular WAN Modem dial up, it supports 5G modem by internal cellular module. Therefore, IGMG-8224D-D5G is one of the best solutions for applications of cellular communication.

1.2 Software Features

- NAT support for enhanced LAN-to-WAN routing performance include
- Secure management by HTTPS
- Multiple WAN connection types supported: Dynamic/Static IP, PPPoE, Modem/Dial-up
- IP table to prevent access from unauthorized IP address.
- Supports NAT setting (virtual server, port trigger, DMZ, and UPnP)
- Versatile modes & event alarm by e-mail
- Event warning by Syslog, e-mail, SNMP trap and SMS

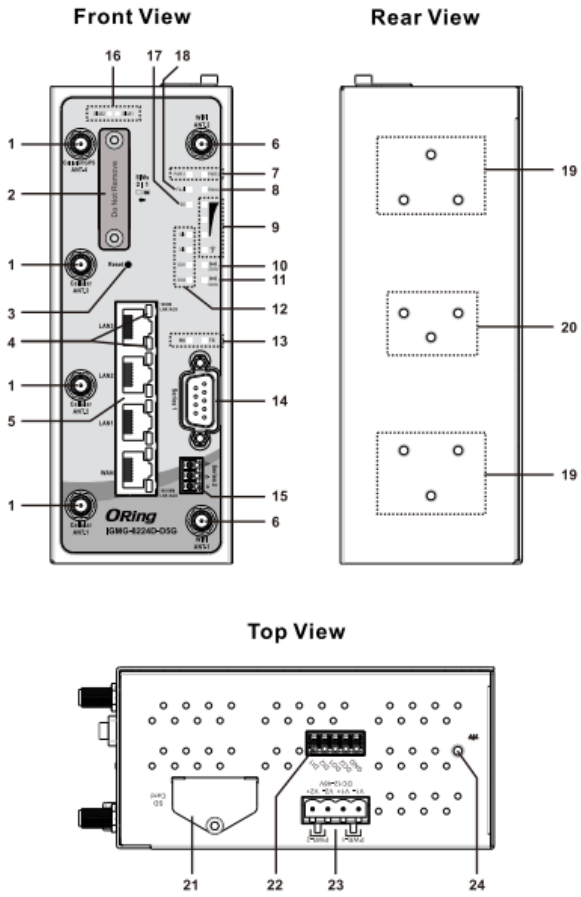
1.3 Hardware Features

- 4 x 10/100/1000 Base-T(X) Ethernet ports for WAN / LAN connection individually.
- Dual band WIFI5 up to 867Mbps link speed
- 2 x SIM card slot
- 5G dial-up modem included.
- 2 Digital Input and 2 Digital Output.
- Full function RS232/422/485 with DB9 connector
- Dual DC inputs
- Operating temperature: -30 to 70°C
- Storage temperature: -40 to 85°C
- Operating humidity: 5% to 95%, non-condensing
- DIN-Rail and Wall-mount.

- Casing: IP-30
- Dimensions: 60(W) x 125(D) x 158(H) mm

Hardware Overview

2.1 Panel Layouts



1. Cellular/GPS antenna connector
2. SIM card slot
   (Do not use adapter, only Mini SIM)
3. Reset button
4. Ethernet LED
5. Ethernet Port
6. WIFI antenna connector
7. LED for Power
8. LED for Status
9. Cellular Status
10. WIFI 2.4GHz On
11. WIFI 5GHz On
12. Digital High/Low
13. Serial signal Tx/Rx
14. Serial Port(DB-9)
15. Serial Port 2
16. SIM status
17. SD card status
18. Fault LED

19. Wall-mount screw holes
20. Din-rail screw holes

21. SD card slot
22. Digital Input/Output
23. Power Input
24. Grounding screw

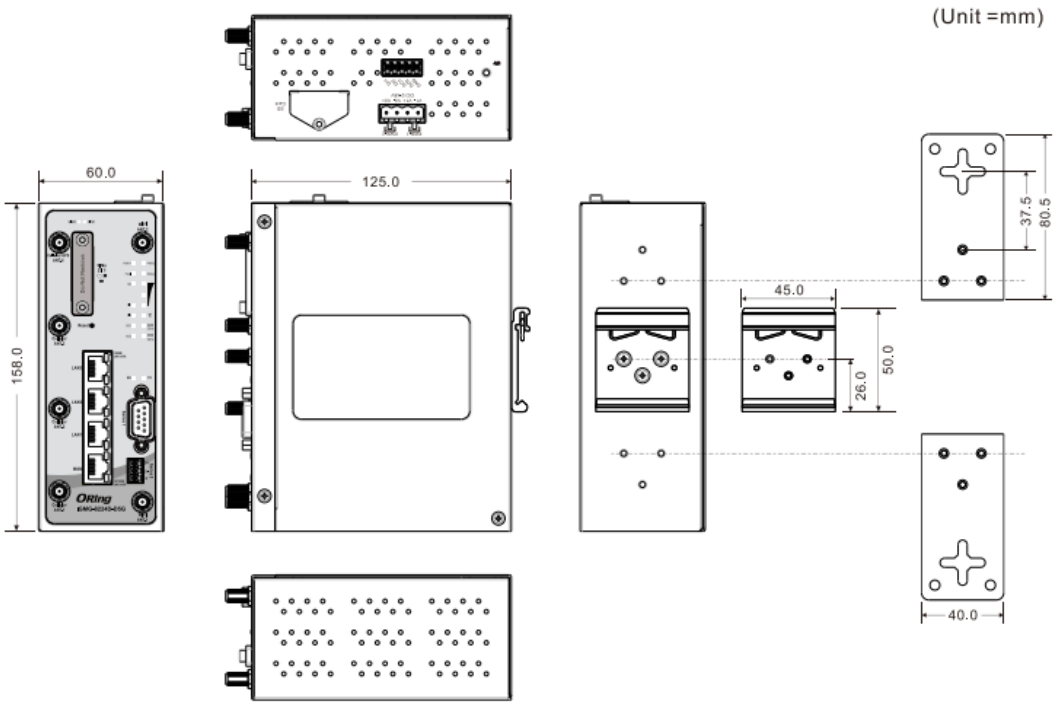
2.2 Front Panel LEDs

LED Indicators	
Power indicator	2 x LEDs, PWR1(2) / Ready: Green On: Power is on and functioning Normal
Ethernet Port Indicator	8 x LEDs, LNK: Green for port Link/AcT. SPD: Green On for 1000/100Base-T(X) link; Green Off for 10Base link
WWAN status	Green On : Power is on and functioning Normal
WWAN signal strength	3 x LEDs Green for Strength: 1<30%, 2 >30% <60%, 3>75%
SIM Indicator	2 x LEDs Green On: in active
DI/O LEDs	Green Solid On: High, Off:Low
2.4GHz LED	Green On : Working; Off:RF disable
5GHz LED	Green On : Working; Off:RF disable
Serial TX/RX LED	Red : Receiving data Green : Transmitting data
SD	Green:Working
Fault	1 x LED, Red for Ethernet link down or power down indicator

Hardware Installation

3.1 Wall Mounting

Besides Din-rail, the router can be fixed to the wall via a wall mount panel, which can be found in the package.



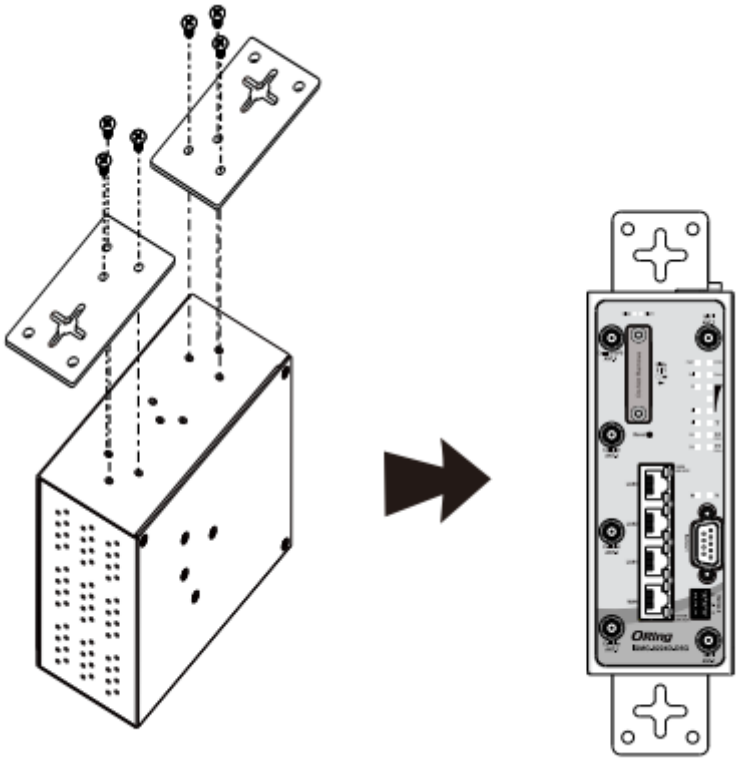
Wall-Mount Kit Measurement (Unit = mm)

To mount the router onto the wall, follow the steps:

Step 1: Screw the two pieces of wall-mount kits onto both ends of the rear panel of the router. A total of six screws are required, as shown below.

Step 2: Use the router, with wall mount plates attached, as a guide to mark the correct locations of the four screws.

Step 3: Insert a screw head through the large part of the keyhole-shaped aperture on the plate, and then slide the router downwards. Tighten the four screws for added stability.



The screws should be 6mm diameter head x 3mm diameter thread, as shown below. Note that the screws should not be larger than the size used in the series to prevent damaging the router.

3.3 Wiring

WARNING

Be sure to switch off the power and make sure the area is not hazardous before disconnecting modules or wires. The devices may only be connected to the supply voltage shown on the type plate.

3.3.1 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

3.3.2 Dual Power Inputs

IGMG-8224D-D5G has two sets of power inputs, power input 1 and power input 2, on a 4-pin terminal block on the router's top panel. Follow the steps below to wire redundant power

inputs.

Step 1: insert the negative/positive DC wires into the V-/V+ terminals, respectively.

Step 2: to keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

ATTENTION

1. Be sure to disconnect the power cord before installing and/or wiring your routers.
2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
3. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.
4. Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
5. Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
6. You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together
7. You should separate input wiring from output wiring
8. It is advised to label the wiring to all devices in the system

Cables and Antenna

4.1 Ethernet Cables

IGMG-8224D-D5G has four 10/100/1000Base-T(X) Ethernet ports. According to the link type, the device uses CAT 3, 4, 5, 5e, 6 UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft.)	RJ45
100BASE-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft.)	RJ45
1000BASE-T(X)	Cat. 5e 100-ohm UTP	UTP 100 m (328 ft.)	RJ45

4.2 RJ-45 Pin Assignment

10/100/1000 Base-T(X) RJ-45 Pin Assignements :

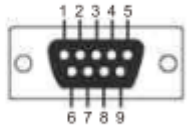
10/100 Base-T(X) RJ-45 port		1000 Base-T RJ-45 port	
Pin Number	**Assignment**	**Pin Number**	**Assignment**
1	TD+	1	BI_DA+
2	TD-	2	BI_DA-
3	RD+	3	BI_DB+
4	Not used	4	BI_DC+
5	Not used	5	BI_DC-
6	RD-	6	BI_DB-
7	Not used	7	BI_DD+
8	Not used	8	BI_DD-

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.3 Serial Pin Definition

DB9 connector Pin Assignment

Pin #	RS-232	RS-422	RS-485 (4 wire)	RS-485 (2 wire)
1	DCD	TX-	TX-	DATA-
2	RXD	TX+	TX+	DATA+
3	TXD	RX+	RX+	
4	DTR	RX-	RX-	
5	GND	GND	GND	GND
6	DSR			
7	RTS			
8	CTS			
9	RI			



DB9 connector

4.4 Cellular & WIFI Antenna

IGMG-8224D-D5G provides four SMA connectors for cellular antennas and two Reverse SMA Female for WIFI antennas. External RF cables and antennas can also be used with the connector. Please see below table for detail information of each antenna configuration:

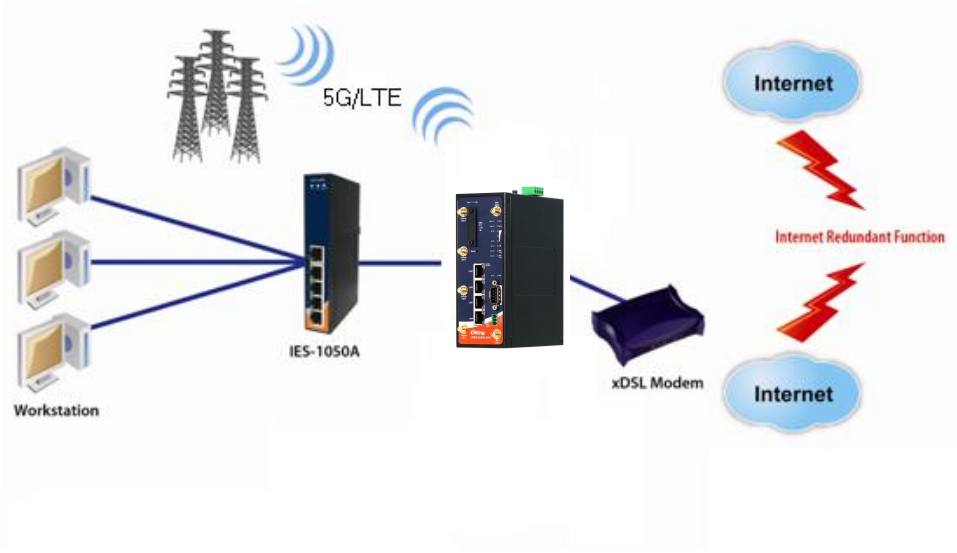
Antenna Connector	Function Description	Band Configuration (TX)	Band Configuration (RX)	Frequency Range (MHz)
Cellular ANT.1	Main TX / PRX	WCDMA: B1 LTE: B1/3/7/38/40/41/42/43 NR: n1/3/7/38/40/41/77/78	WCDMA: B1 LTE: B1/3/7/32/38/40/41/42/43 NR: n1/3/7/38/40/41/75/76/77/78	617-960 1427-2690 3300-4200
	Secondary TX /MIMO PRX	LTE: B5/20/28 NR: n5/20/28	LTE: B5/20/28 NR: n5/20/28	
Cellular ANT.2	DRX	-	WCDMA: B1/5/8 LTE: B1/3/5/7/8/28/32/38/40/41/42/43 NR: n1/3/5/7/8/20/28/38/40/41/75/76/77/78	617-960 1427-2690 3300-4200

Cellular ANT.3	MIMO DRX	-	LTE: B1/3/5/7/28/32/38/40/41/42/43 NR: n1/3/5/7/20/28/38/40/41/75/76/77/78	617-960 1427-2690 3300-4200
Cellular ANT.4	Main TX / PRX	WCDMA: B5/8 LTE: B5/8/20/28 NR: n5/8/20/28	WCDMA: B5/8 LTE: B5/8/20/28 NR: n5/8/20/28	617-960 1427-2690 3300-4200
	Secondary TX / MIMO PRX	LTE: B1/3/38/40/41 NR: n1/3/38/40/41/77/78	LTE: B1/3/B7/38/40/41/42/43 NR: n1/3/7/38/40/41/75/76/77/78	
Antenna Connector	**Frequency Band**			
WIFI ANT.1 & ANT.2	America / FCC: 2.412~2.462 GHz (11 channels) 5.180~5.240 GHz & 5.745~5.825 GHz (9 channels) Europe CE / ETSI: 2.412~2.472 GHz (13 channels) 5.180~5.240 GHz (4 channels)			

Management Interface

5.1 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.

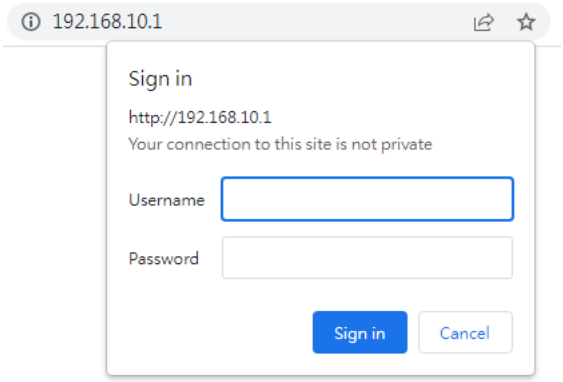


Follow the steps below to install and connect the router to PCs:

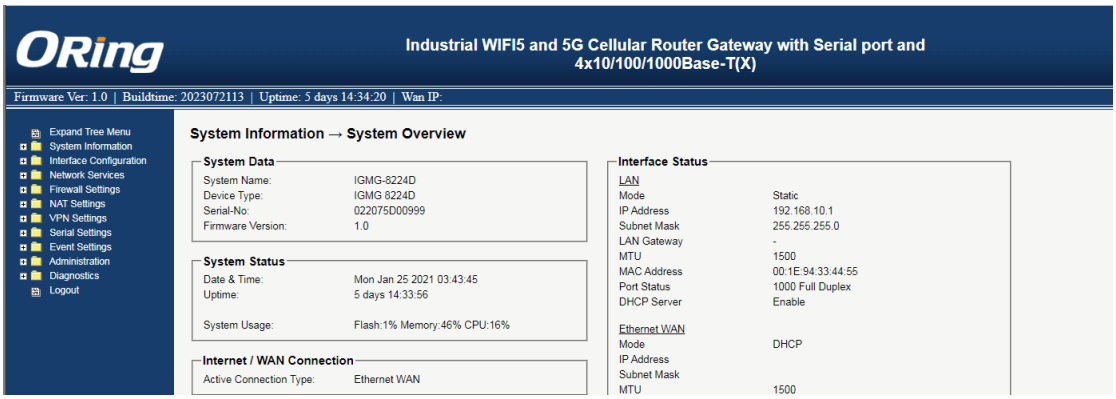
Step 1: Select power source. The router can be powered by +12~48V DC power input.

Step 2: Connect a computer to the router. Use either a straight-through Ethernet cable or cross-over cable to connect the LAN port (LAN1~LAN3) 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.

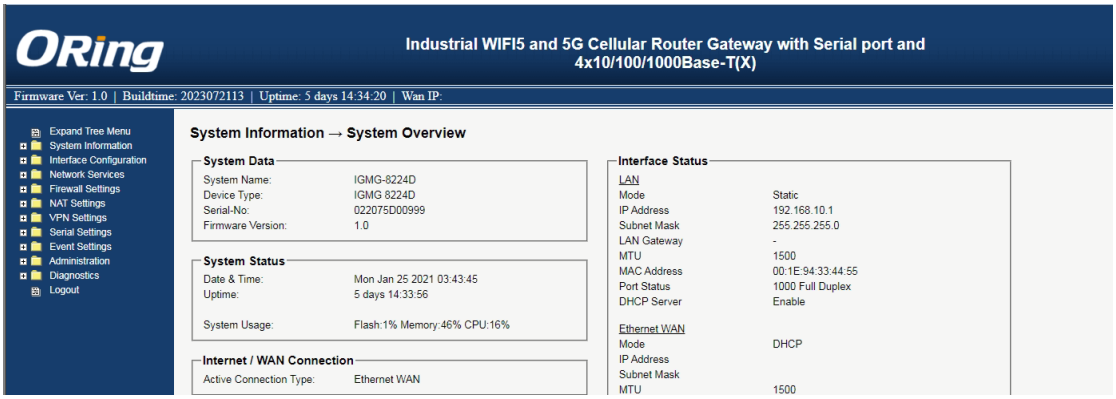


After you log in successfully, a Web interface will appear, as shown below. On the left-hand side of the interface is a list of functions where you can configure the settings. The details of the configurations will be shown on the right screen.



5.2 Configuration

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



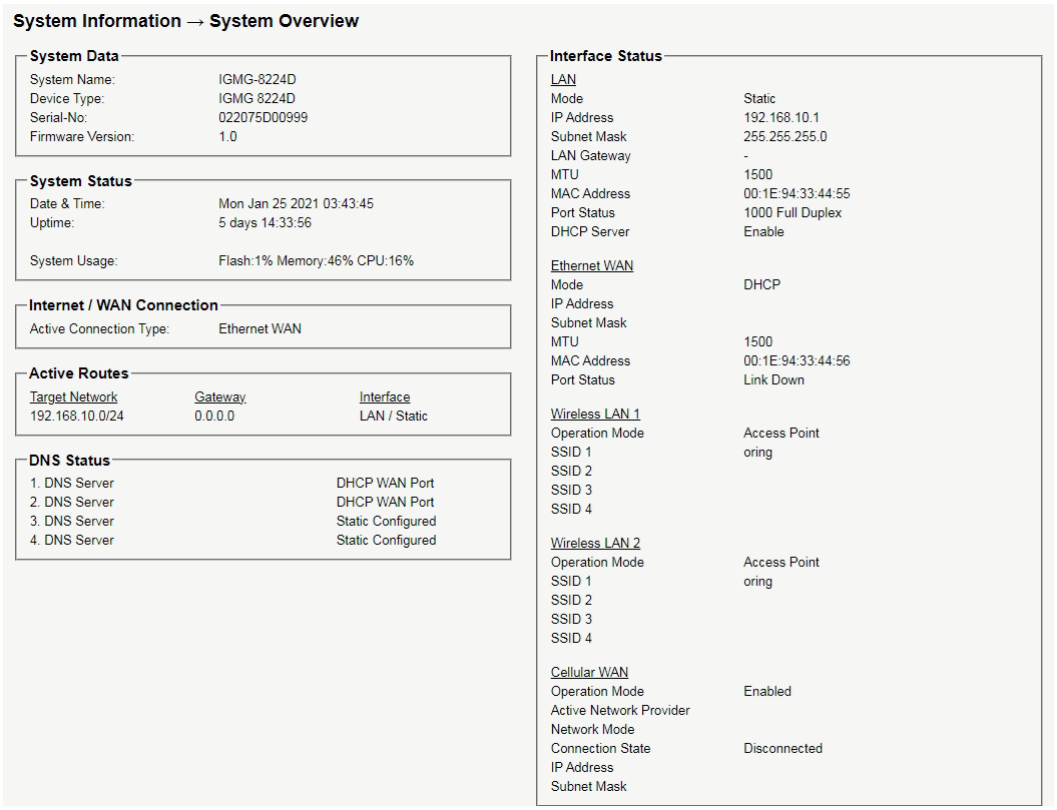
Label	Description
Firmware	Shows the current firmware version
Uptime	Shows the elapsed time since the Router is started
Wan IP	Shows WAN IP address

5.2.1 System Information

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

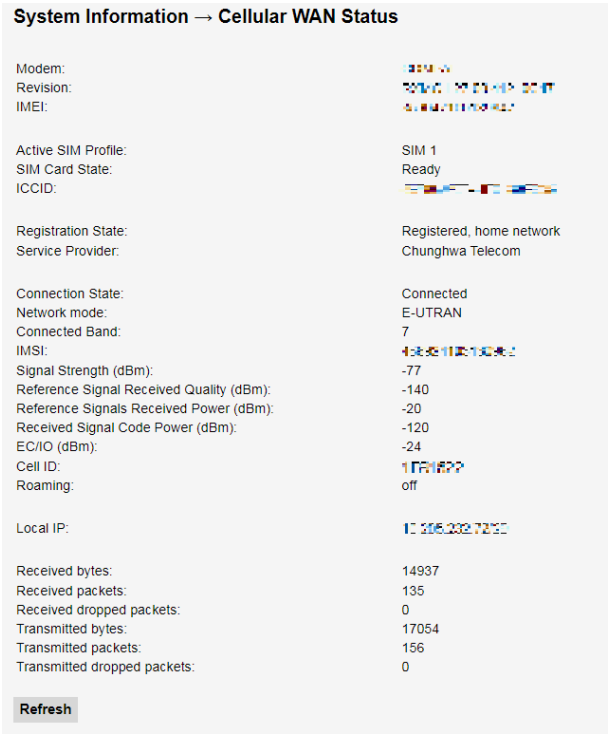
System Overview

System basic information



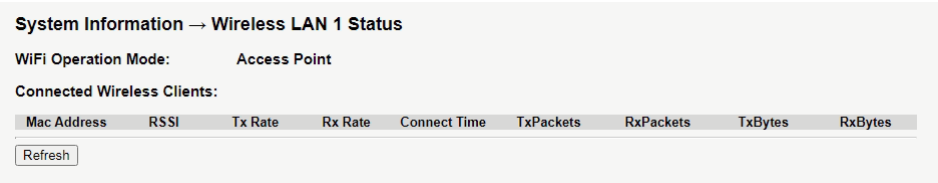
Cellular WAN Status

Include Cellular modem, SIM card and Base station information.



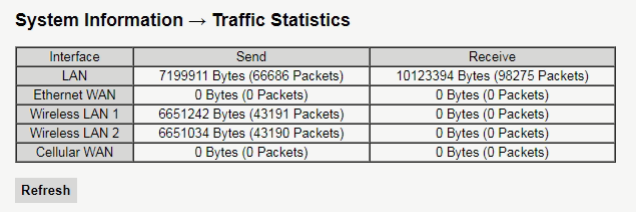
Wireless LAN 1&2 Status

Include Wireless Operation mode and connected client status.



Traffic Statistics

Wire LAN/WAN traffic statistics.

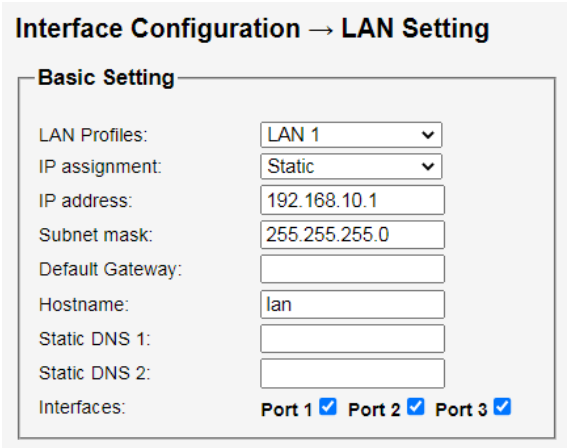


5.2.2 Interface Configuration

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.



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

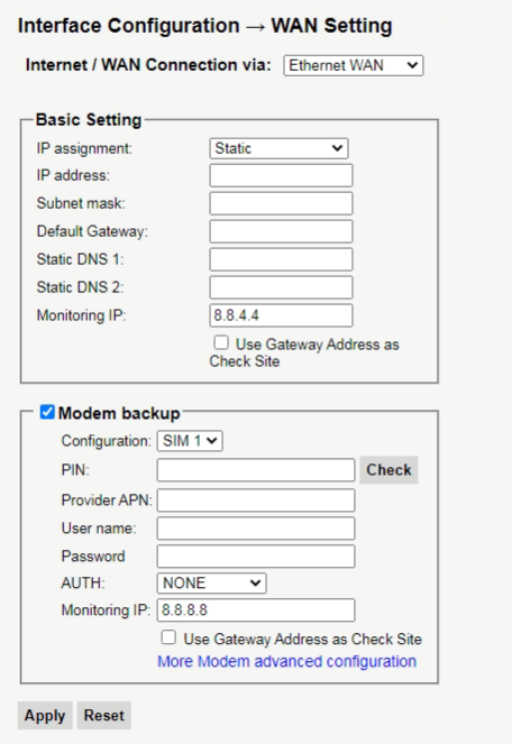
Hostname	Assign hostname for router
Static DNS 1/2	Assign DNS address for router
Interfaces	Assign interface (Port 1, Port 2 and Port 3) for above configuration

WAN Setting

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

Ethernet WAN

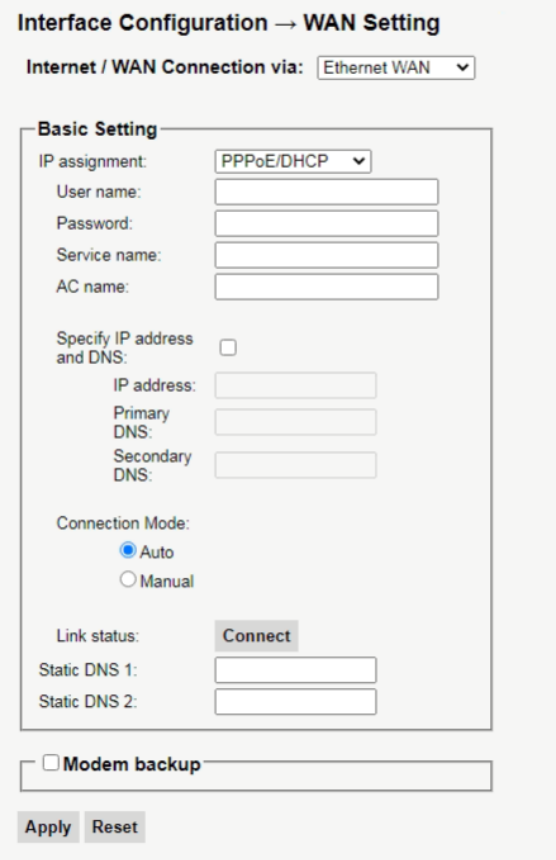
Connection Type as Static / DHCP / DHCP+Fallback:



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"	Fill a host for monitoring WAN connection if available, it can use gateway address as well.

checkbox is checked)	
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.

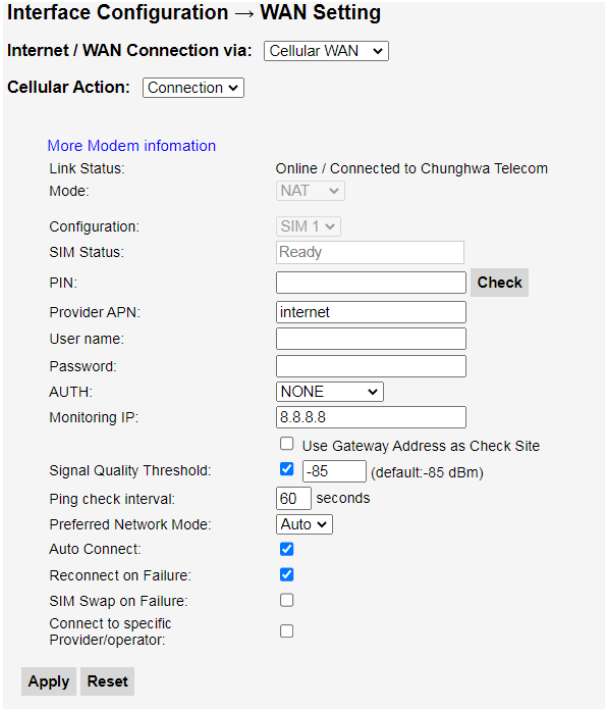
Connection Type as PPPoE/DHCP:



Label	Description
UserName / 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

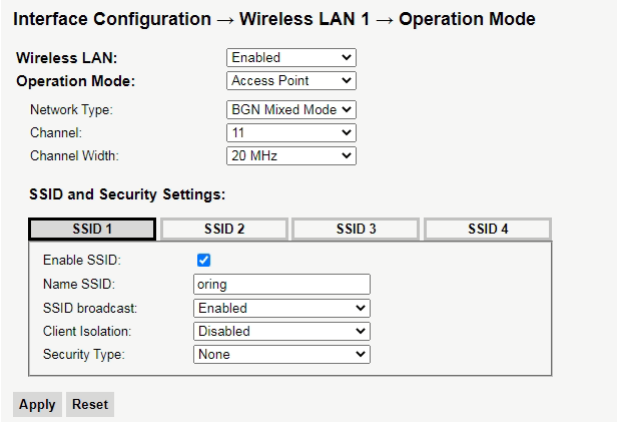


Label	Description
Cellular Action	Active Cellular Connect or Disconnect
Link Status	Shows the status of connections
Mode	NAT mode: router with NAT function, Bridge mode: transparent and act as pure modem
Configuration	Select for SIM Card slot
SIM Status	Check SIM Card status
PIN	Enter a PIN code if you want to perform PIN check
Provider APN	Enter the APN value (optional)

UserName	Enter the user name 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)
Connect to specific Provider/operator	Checked to connect specific provider/operator with Mobile Country Code (MCC) and Mobile Network Code (MNC)

Wireless LAN 1&2

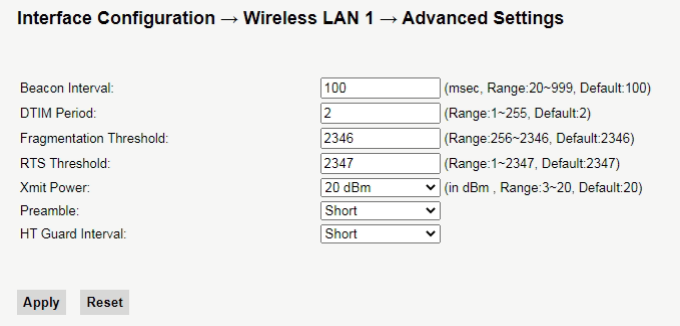
Operation mode



Label	Description
Wireless LAN	Enable/Disable interface
Operation Mode	Currently only support Access Point mode
Network Type	Wireless1 support WIFI 2.4G BG/BGN mode and Wireless 2 support WIFI 5G A/AN/AC mode

Channel	WIFI Channel setting
Channel Width	Wireless 1 support 20/40Mhz, Wireless 2 support 20/40/80MHz
SSID & Security Setting	Each Wireless interface support up to 4 individual SSID and Security setting

Advanced Settings

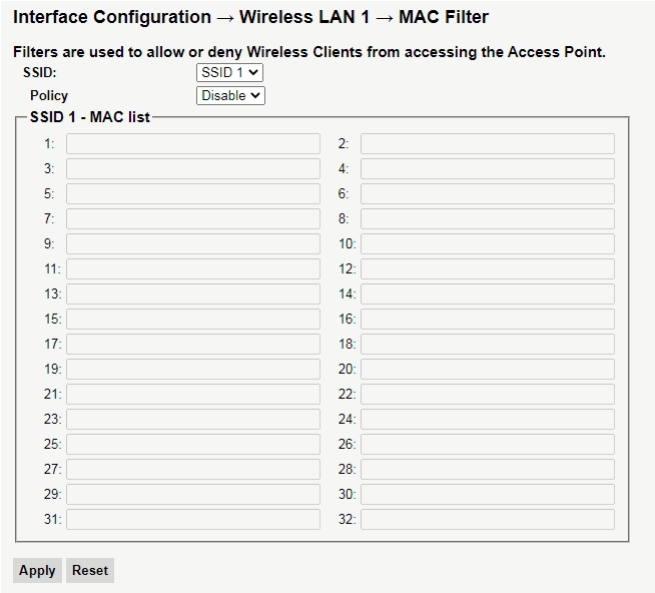


Label	Description
Beacon Interval	A beacon is a packet sent by a wireless access point to synchronize wireless devices. The beacon interval value indicates the frequency interval of the beacon. Increasing the beacon interval reduces the number of beacons and the overhead associated with them. The default value is 100, but 50 is recommended when reception is poor
DTIM Period	The value is an integer that ranges from 1 to 255, in Beacons. The DTIM interval specifies how many Beacon frames are sent before the Beacon frame that contains the DITM. A long DTIM interval lengthens the dormancy time of the STA and saves power, but degrades the transmission capability of the STA. A short interval helps transmitting data in a timely manner, but the STA is wakened up frequently, causing high power consumption
Fragmentation Threshold	Specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or “off”. Setting the Fragmentation Threshold too low may result in poor network performance. The use of fragmentation can increase the reliability of frame transmissions. Because smaller frames are sent, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result lower throughput as well. Little or no modification of the Fragmentation Threshold value is recommended as the default setting of 2346 is optimum for most wireless networks.

RTS Threshold	Determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or "off". The default value is 2347, which means that RTS is disabled. RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden AP25N01 User Manual 85terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately. System uses Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending an RTS frame first while data is sent only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provides clear media for the requesting station to send the data. CTS collision control management has time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.
Xmit Power	Transmit power of the radio. This is the total power supplied to the antennas of the radio
Preamble	Available values include **Long** and **Short**, with **Long** as the default value. If all clients and access points in your wireless network support short preamble, then enabling it can boost overall throughput. However, if any wireless device does not support short preamble, then it will not be able to communicate with your network. If you are not sure whether your radio supports the short RF preamble, you must disable this feature

MAC Filter

Filters are used to allow or deny Wireless Clients from accessing the Access Point.



Label	Description
SSID	Choose to apply SSID
Policy	Deny/Allow Policy
MAC list	Add Client MAC address to list table

5.2.3 Networking Services

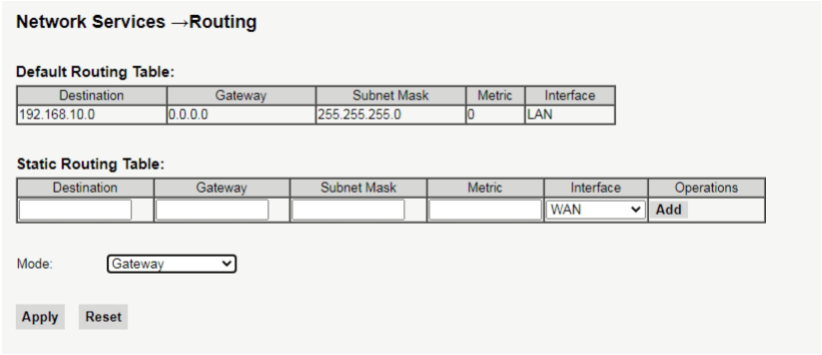
Routing Protocol

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.



Label	Description
Default Routing	Shows all routing information, including static and dynamic routing

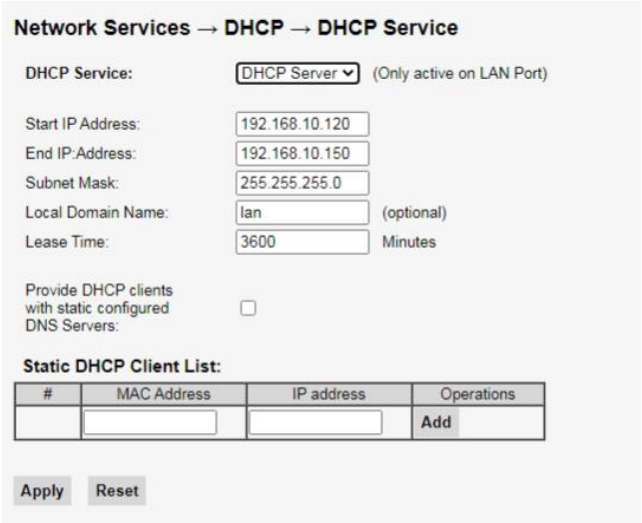
Table	(if enabled)
Static Route Table	Fills in corresponding information to add new entries to the static routing tablet
Mode	Choose **Gateway Mode** if you want PCs in the LAN to visit external network, otherwise choose **Router Mode**

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

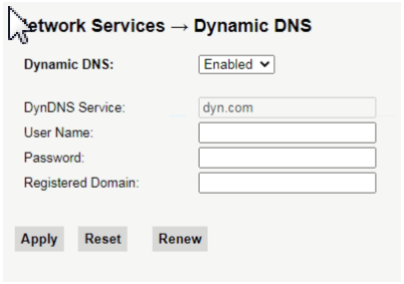


Label	Description
DHCP Server	Enable or disable the DHCP server function. The default setting is **Enabled**.
Starting IP	The starting IP address of the IP range assigned by the DHCP server
Ending IP	The ending IP address of the IP range assigned by the DHCP server
Lease Time	The period of time for the 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

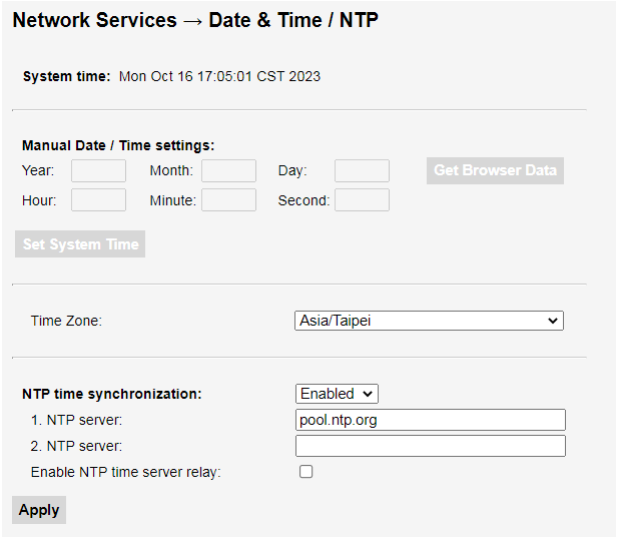
Dynamic Domain Name System (DDNS) allows you to configure a domain name for your IP address which is dynamically assigned by your ISP. Therefore, you can use a static domain name that always points to the current dynamic IP address.



Label	Description
DDNS Service	Choose a DDNS service provider from the list
Username	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

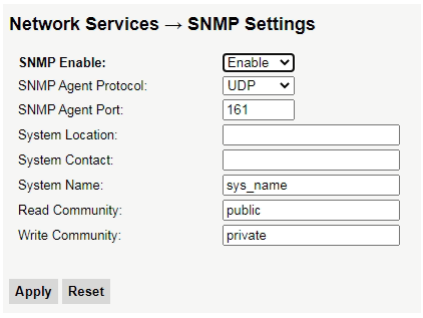
Date & Time / NTP

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.



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



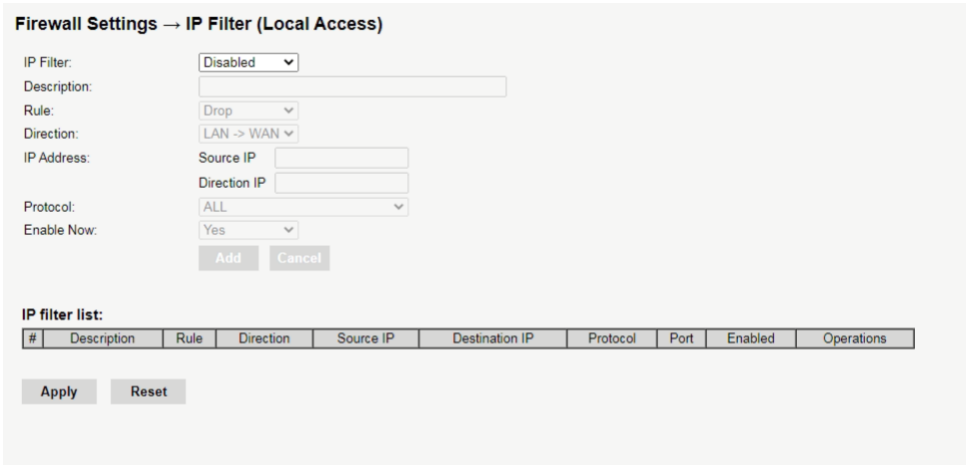
Label	Description
SNMP Enable	SNMP (Simple Network Management Protocol) Agent is a service program that runs on the router. The agent provides management information to the NMS by keeping track of various operational

	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
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.

5.2.4 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.

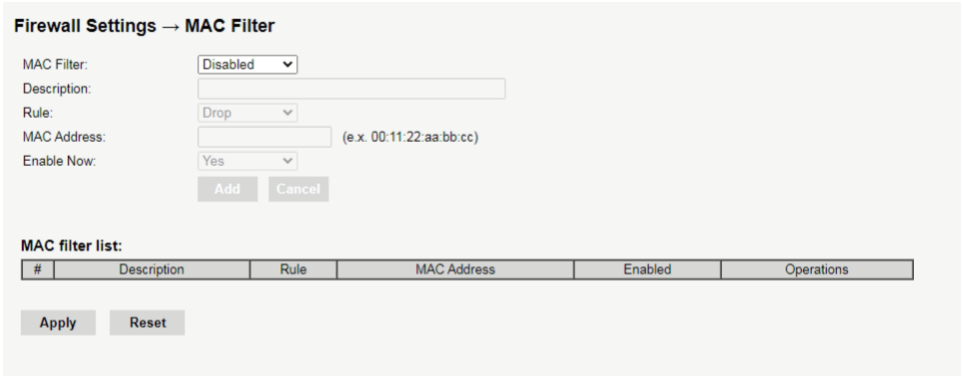


Label	Description
IP Filter	Enable or disable the IP Filter
Description	Enter description for the entry.
Rule	Configure the rules to be applied to the IP filter. Available options include **DROP**, **ACCEPT**, and **REJECT.**
Direction	Specify the direction of data flow to be filtered

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

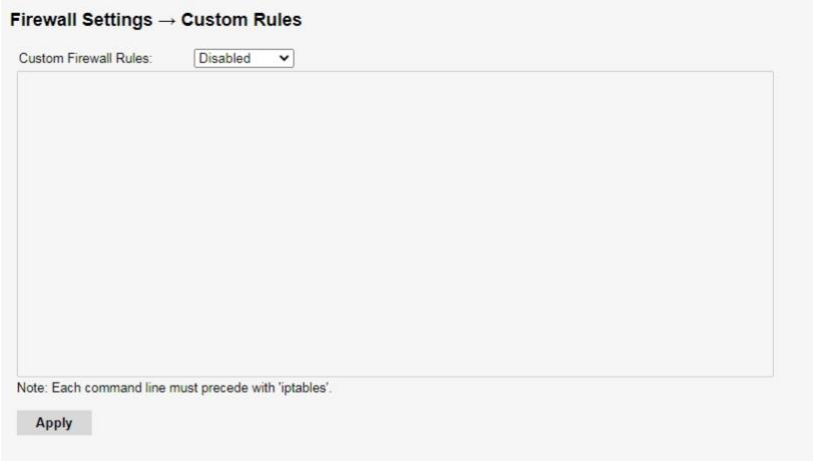
This page enables you to deny or allow LAN computers to access the Internet based on their MAC addresses.



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.



5.2.5 NAT Setting

Virtual Server

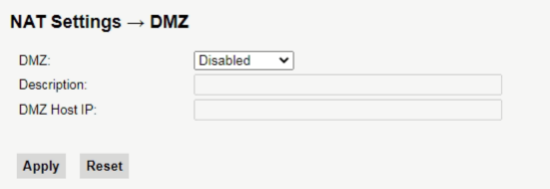
This page allows you to set up virtual server setting. A virtual server allows Internet users to access services on your LAN. This is a useful function if you host services online such as FTP, Web or game servers. A public port must be defined for the virtual server on your router in order to redirect 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.

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.



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

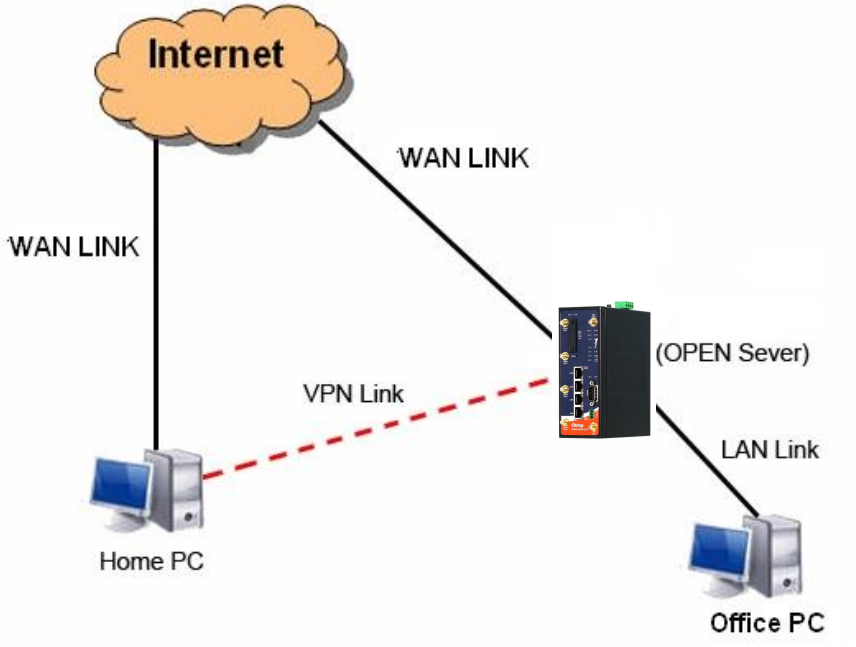
5.2.6 VPN Setting

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.

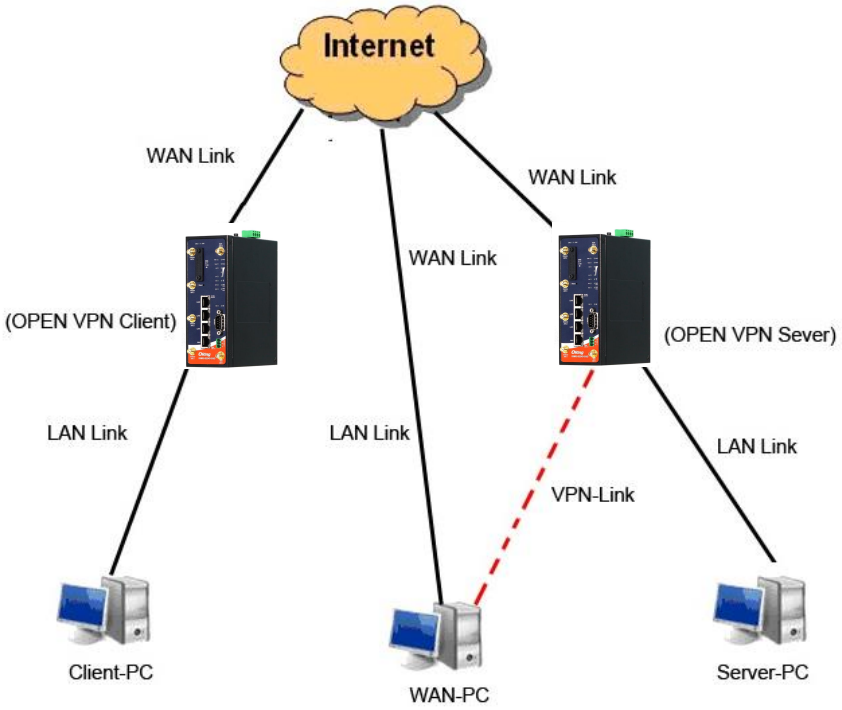
Open VPN enables you to easily set up a virtual private network over an encrypted connection. It is a full-function SSL VPN solution which accommodates a wide range of configurations including remote access, site-to-site VPNs, WiFi security, and enterprise-level remote access with load balancing, failover,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

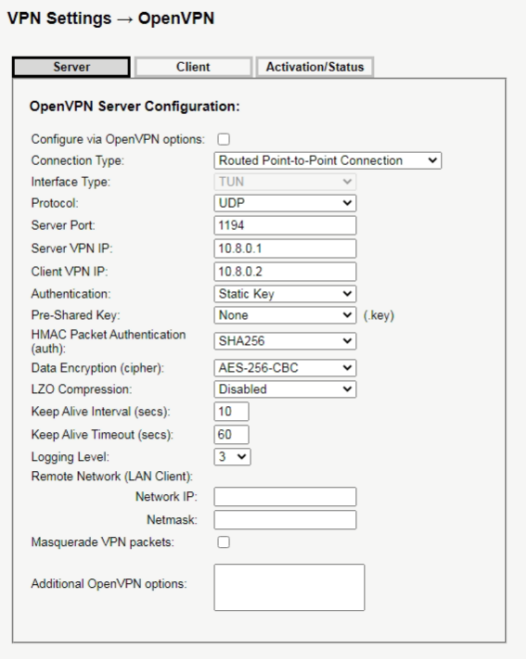


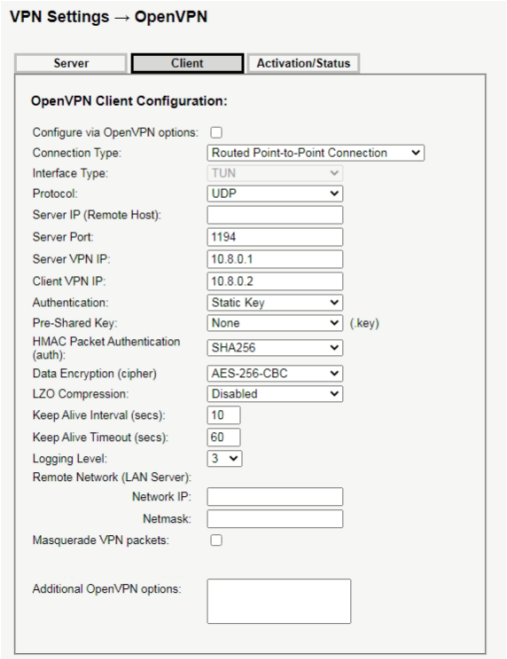
Connection to Open VPN Server

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



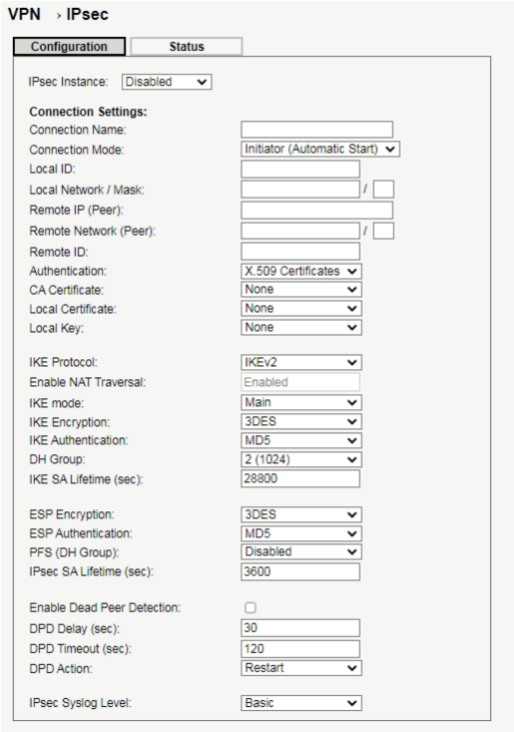


Label	Description
Connection Type	**Routed Point-to-Point / Multi-Client connection**: In a layer 3 network (Interface type - TUN), the clients can reach each other only by using IP addresses. The MAC address of the tun adapter is never revealed to the other VPN clients or even to the OpenVPN server 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.



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.

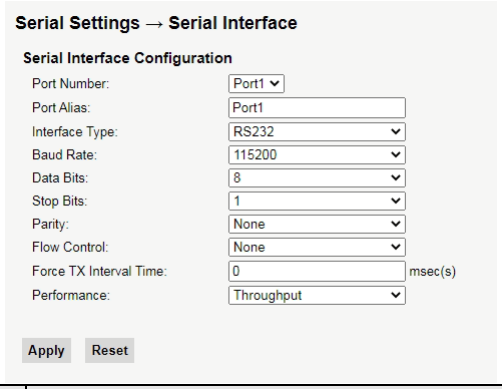
Certificates

Certificate uploaded here for VPN using.

5.2.7 Serial Settings

Serial Interface

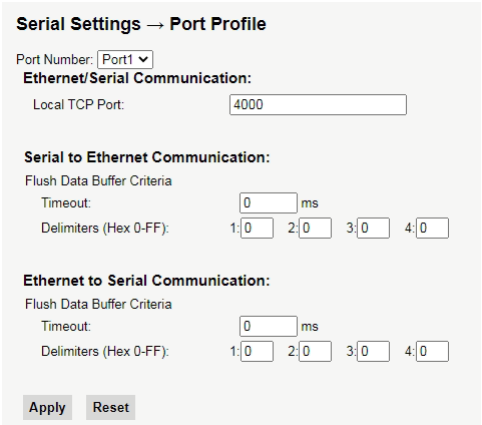
This page allows you to configure serial port parameters.



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.

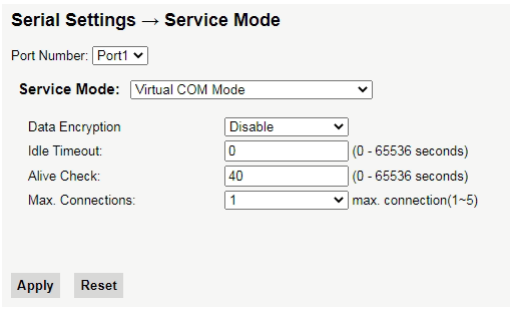
Port profile



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.

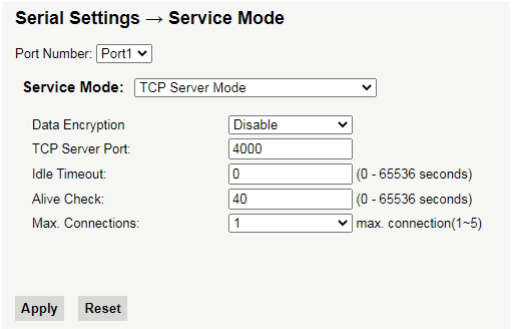


Label	Description
Data Encryption	Click on the radio button to enable or disable data encryption
Idle Timeout	When serial port stops data transmission for a defined period of time, the connection will be closed and the port will be freed and try to connect with other hosts. 0 indicate disable this function. 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.

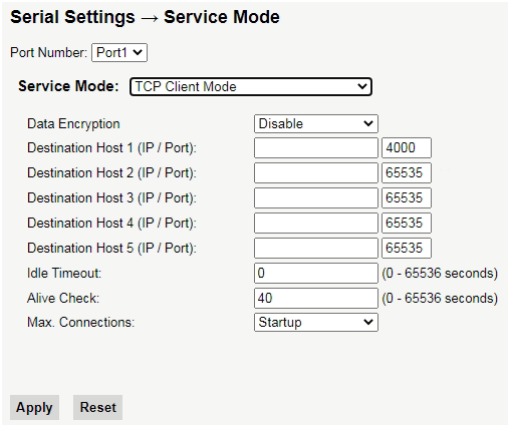


Label	Description
Data Encryption	Click on the radio button to enable or disable data encryption
TCP Server Port	Enter the TCP server port number
Idle Timeout	When serial port stops data transmission for a defined period of time, the connection will be closed and the port will be freed and try to connect 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.

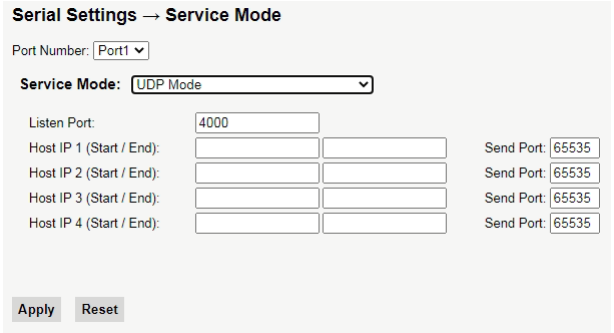


Label	Description
Data Encryption	Click on the radio button to enable or disable data encryption
Destination Host	Set the IP address of host and the port number of data port.
Idle Timeout	When serial port stops data transmission for a defined period of time, the connection will be closed, and the port 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

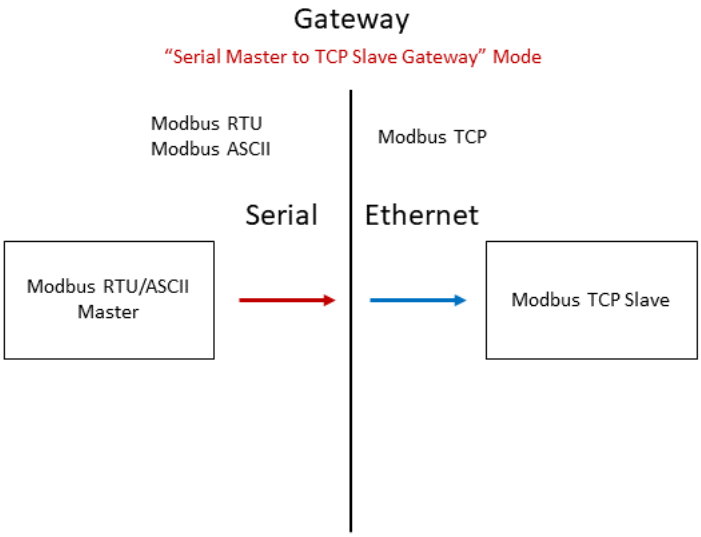
Compared to TCP communications, UDP is faster and more efficient. In UDP mode, you can uni-cast or multi-cast data from the serial device server to host computers, and the serial device can also receive data from one or multiple host.

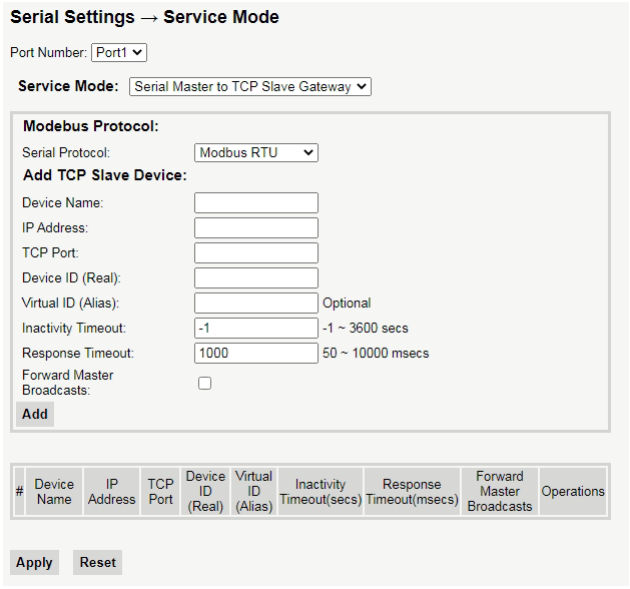


Label	Description
Listen Port	Allows the user to set a new TCP port number to listen on rather than the default value of the device
Host Start/End IP	If there are more than one destination hosts, specify the IP address range by inputting a value in **Host Start** / **End IP**. You can also auto scan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

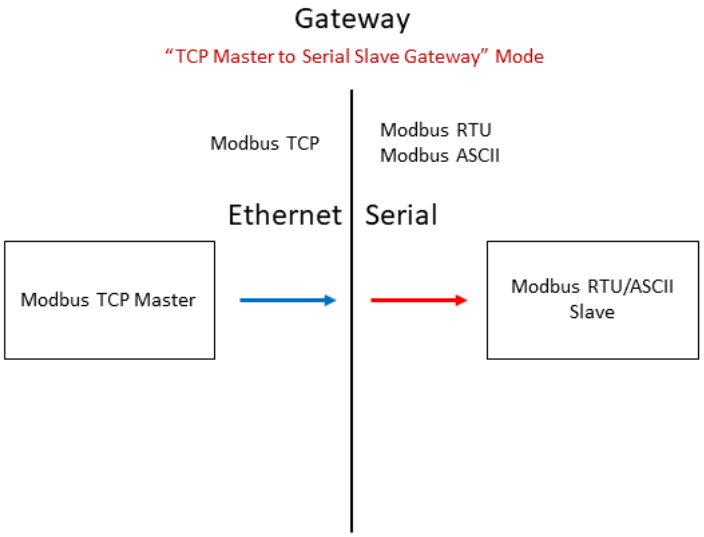


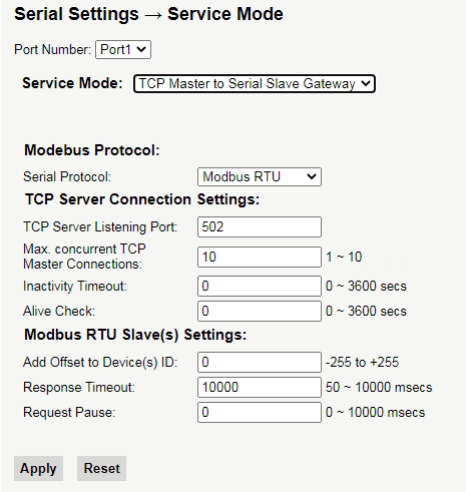


Label	Description
Device Name	Remote Device name
IP Address	Set the IP address of host
TCP Port	the port number of data port
Inactivity Timeout	When serial port stops data transmission for a defined period of time, the connection will be closed and the port will be freed and try to connect with other 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.



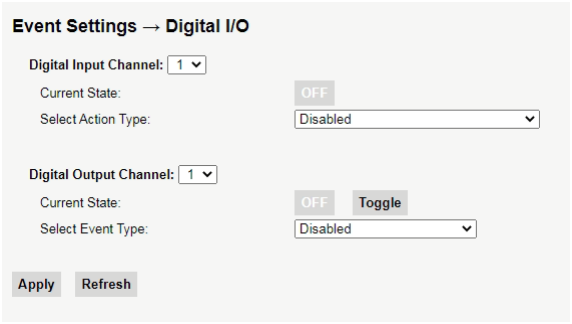


Label	Description
TCP Server Listening Port	Indicates the port used for the Modbus/TCP communication
Max TCP Master Connection	The total number of remote TCP/IP clients allowed to connect to this server.

5.2.8 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.

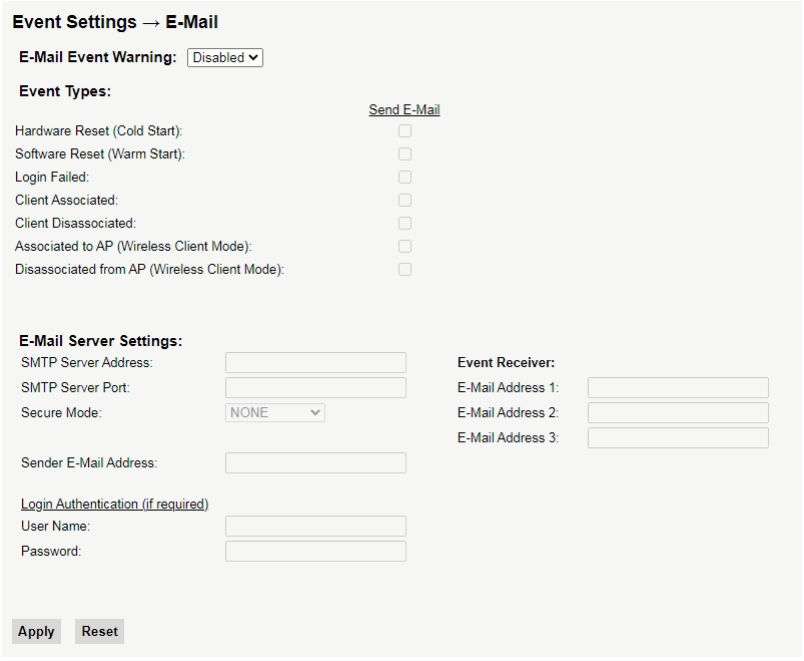
Digital I/O



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

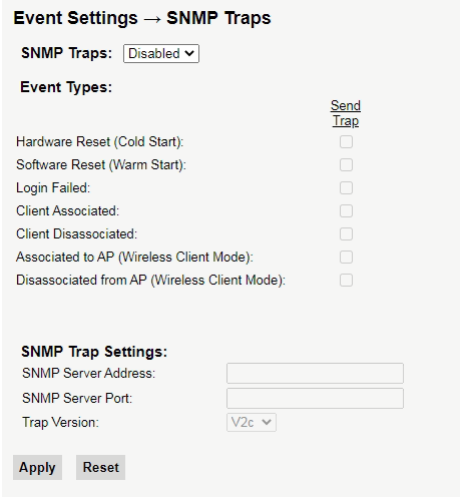
Send the event alert via Email.



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

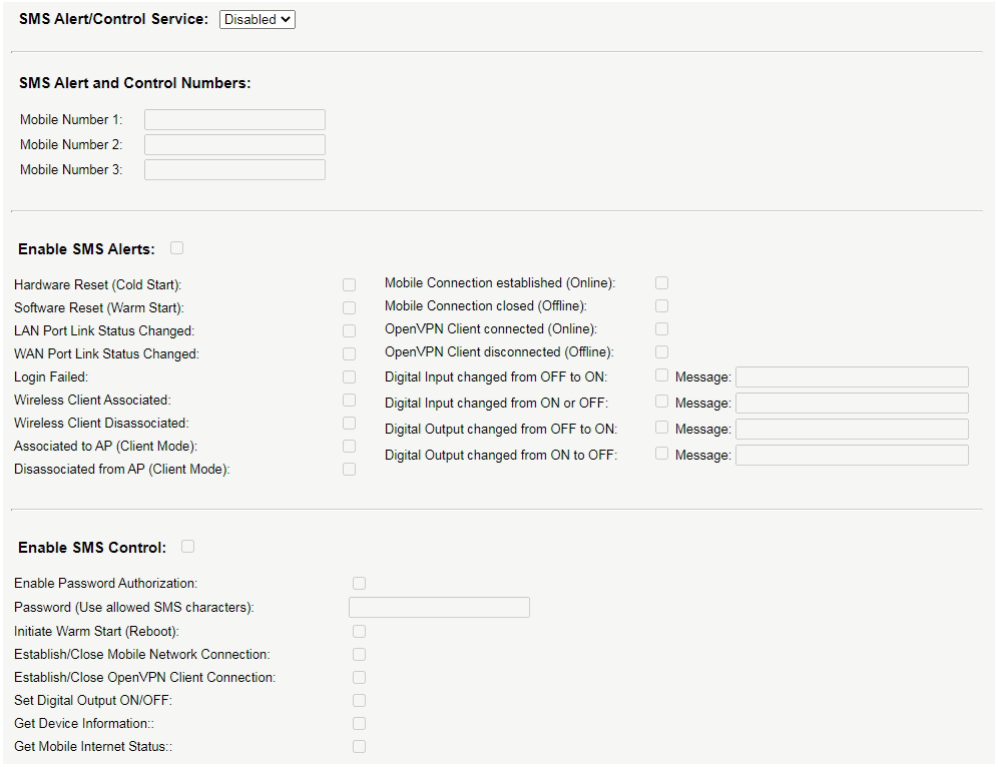
Send event alert via SNMP trap protocol.



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

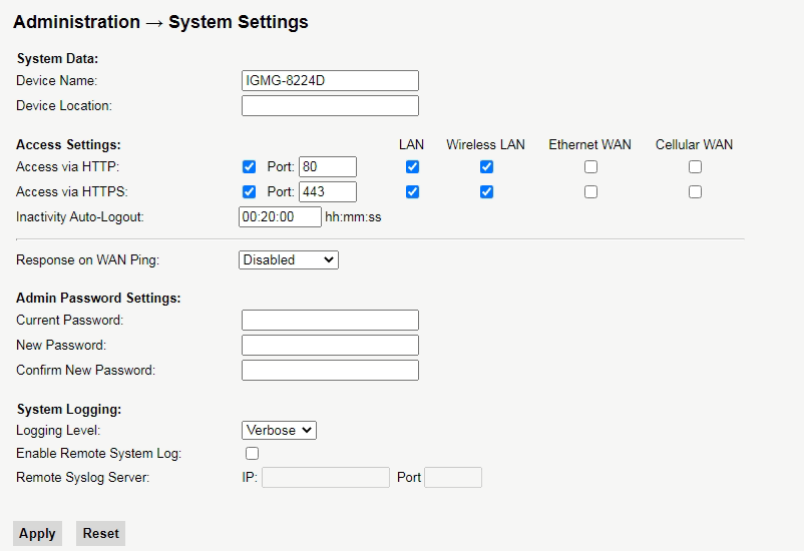
Send the event alert and control device via SMS



5.2.9 Administration

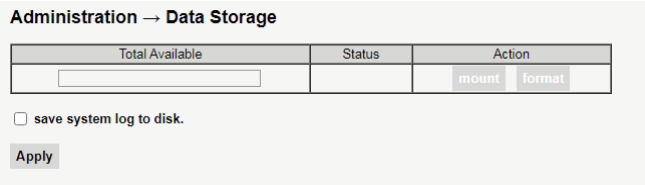
System Setting

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.



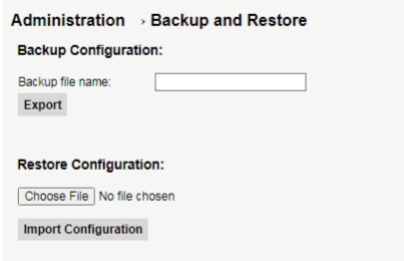
Label	Description
Device Name	Assign name for device
Device Location	Type in device location
Confirm New Password	Retype the new password to confirm it.
Access setting	Choose a web management page protocol from **HTTP** and **HTTPS**. HTTPS (HTTP over SSL) encrypts data sent and received over the Web. 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.

Data Storage



Backup and Restore Configurations

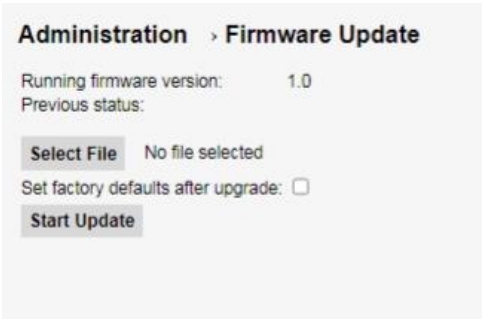
This page allows you to save configurations or return settings to previous status. You can download the configuration file from the Web. Note: users using old versions of Internet Explorer may have to click on the warning on top of the browser and choose Download File.



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

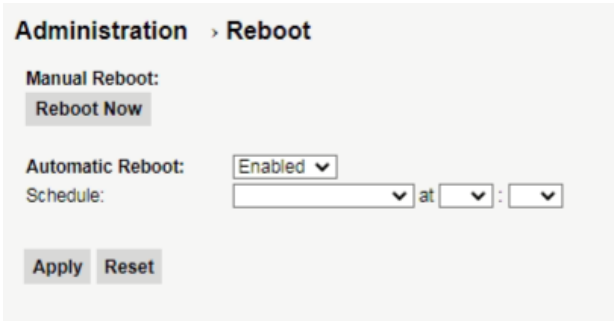
ORing launches new firmware constantly to enhance router performance and functions. To upgrade firmware, download new firmware from ORing's website to your PC and install it via Web upgrade. Make sure the firmware file matches the model of your router. It will take several minutes to upload and update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



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.



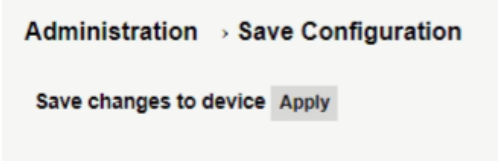
Label	Description
Reboot Now	Click to restart the router via warm reset
Automatic Reboot	**Enable**: check to activate the setting Reboot at: specify the time for resetting the router. You can configure the action to be performed periodically.

Factory Default

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

Save device configuration.

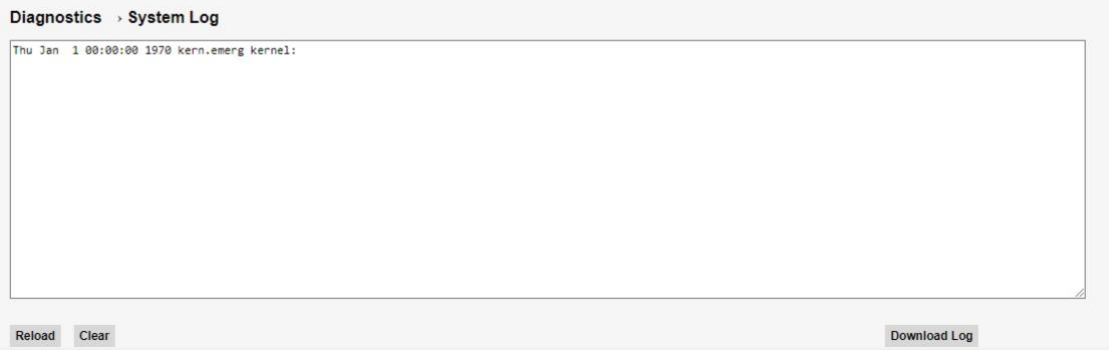
Click Apply to save all Changes to device.



5.2.10 Diagnostics

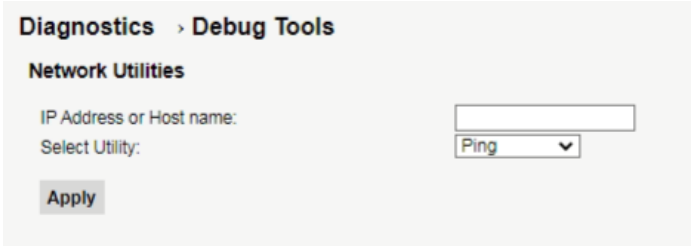
System Log

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.



Debug Tools

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



Technical Specifications

ORing Router Model	IGMG-8224D-D5G
Physical Ports	
10/100/1000 Base-T(X) Ports in RJ45	**1(WAN) + 3(LAN), Auto MDI/MDIX**
5-Pin Terminal Block	**DI x 2 and DO x 2 :** Dry Contact: On: short to GND, Off: open Wet Contact (DI to COM/GND): On: 0 to 3VDC, Off: 10 to 30VDC
RS-232 Serial port in DB9	**115200, 8 ,N ,1**
RS-485 Serial port in Termianl Block	**D+, D-, GND**
Sim Card Slot	**2**
SD Slot	**Standard SD**
Cellular Interface (Main)	
Antenna Connector	SMA Female x 4
SIM (Dual)	SIM (Micro SIM, 3FF)
Cellular Standard	HSDPA/ HSUPA / LTE/ LTE+/ 5G
Band Option	5G NR : n1,n2,n3,n5,n7,n8,n12,n20,n28,n41,n66,n71,n77,n78,n79 LTE : FDD : B1/B2/B3/B4/B5/B7/B8/B12/B13/B14/B17/B18/B19/B20/B25/B26/B28/B29/B30/B32/B66/B71 TDD : B34/B38/B39/B40/B41/B42/B46/B48 WCDMA : B1/B2/B3/B4/B5/B6/B8/B9/B19
WLAN Interfac	
Antenna Connector	2 x Reverse SMA Female
Modulation	802.11a: OFDM 802.11b: CCK, DQPSK, DBPSK 802.11g: OFDM 802.11n: BPSK, QPSK, 16-QAM, 64-QAM 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Frequency Band	America / FCC: 2.412~2.462 GHz (11 channels) 5.180~5.240 GHz & 5.745~5.825 GHz (9 channels) Europe CE / ETSI: 2.412~2.472 GHz (13 channels)

	5.180~5.240 GHz (4 channels)
Transmission Rate	802.11b: 1/2/5.5/11 Mbps 802.11a/g: 6/9/12/18/24/36/48/54 Mbps 802.11n: UP to 300 Mbps 802.11ac: up to 867Mbps
Transmit Power	IEEE 802.11a: 21dBm ± 2dBm@54Mbps IEEE 802.11b: 23dBm ± 2dBm@11Mbps IEEE 802.11g: 20dBm ± 2dBm@54Mbps IEEE 802.11gn HT20: 18dBm ± 2dBm @MCS7 IEEE 802.11gn HT40: 18dBm ± 2dBm @MCS7 IEEE 802.11an HT20: 20dBm ± 2dBm @MCS7 IEEE 802.11an HT40: 20dBm ± 2dBm @MCS7 IEEE 802.11ac VHT80: 20dBm ± 2dBm @MCS9
Receiver Sensitivity	IEEE 802.11a : -75dBm ± 2dBm@54Mbps IEEE 802.11b : -90dBm ± 2dBm@11Mbps IEEE 802.11g : -75dBm ± 2dBm@54Mbps IEEE 802.11gn HT20:-72dBm ± 2dBm@MCS7 IEEE 802.11gn HT40:-70dBm ± 2dBm@MCS7 IEEE 802.11an HT20:-72dBm ± 2dBm@MCS7 IEEE 802.11an HT40:-69dBm ± 2dBm@MCS7 IEEE 802.11ac VHT80:-60dBm ± 2dBm@MCS9
Encryption Security	WEP: (64-bit ,128-bit key supported) WPA/WPA2 :802.11i(WEP and AES encryption) WPA-PSK (256-bit key pre-shared key supported) 802.1X Authentication supported TKIP encryption
Wireless Security	SSID broadcast disable
LED indicators	
Power indicator	2 x LEDs, PWR1(2) / Ready: Green On: Power is on and functioning Normal
Ethernet Port Indicator	8 x LEDs, LNK: Green for port Link/AcT. SPD: Green On for 1000/100Base-T(X) link; Green Off for 10Base link
WWAN status	Green On : Power is on and functioning Normal
WWAN signal strength	3 x LEDs Green for Strength: 1<30%, 2 >30% <60%, 3>75%
SIM Indicator	2 x LEDs Green On: in active
DI/O LEDs	Green Solid On: High, Off:Low
2.4GHz LED	Green On : Working; Off:RF disable
5GHz LED	Green On : Working; Off:RF disable
Serial TX/RX LED	Red : Receiving data Green : Transmitting data
SD	Green:Working
Fault	1 x LED, Red for Ethernet link down or power down indicator
Power	
Redundant Input power	Dual DC inputs. 12-48VDC on 4-pin terminal block

Power consumption	13.9w
Overload current protection	Present
Reverse polarity protection	Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	60(W) x 125(D) x 158(H) mm
Weight (g)	1100g
Environmental	
Storage Temperature	-40 to 85oC (-40 to 185°F)
Operating Temperature	-30 to 70°C (-22 to 158°F)
Operating Humidity	5% to 95% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-31
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	5 years