



## **IGMG-P83244GC+-D4G**

### **Industrial Cellular M2M Gateway**

# **User Manual**

**Version 1.0**

**March, 2019**

#### **COPYRIGHT NOTICE**

[www.oringnet.com](http://www.oringnet.com)

Copyright © 2018 ORing Industrial Networking Corp.

All rights reserved.

No part of this publication may be reproduced in any form without the prior written consent of ORing Industrial Networking Corp.

## 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 23148, Taiwan (R.O.C.)

Tel: +886-2-2218-1066 // Fax: +886-2-2218-1014

Website: [www.oringnet.com](http://www.oringnet.com)

### **Technical Support**

E-mail: [support@oringnet.com](mailto:support@oringnet.com)

### **Sales Contact**

E-mail: [sales@oringnet.com](mailto:sales@oringnet.com) (Headquarters)

[sales@oring-networking.com.cn](mailto:sales@oring-networking.com.cn) (China)

## Tables of Content

<b>Getting Started.....</b>	<b>1</b>
1.1 About the IGMG-P83244GC+-D4G .....	1
1.2 Software Features .....	1
1.3 Hardware Features.....	1
 <b>Hardware Overview .....</b>	 <b>2</b>
2.1 Bottom Panel.....	2
2.1.1 Ports and Connectors .....	2
2.1.2 Front Panel LEDs .....	3
2.2 Top Panel.....	4
2.3 Rear Panel.....	4
 <b>Hardware Installation .....</b>	 <b>5</b>
3.1 DIN-Rail Mounting .....	5
3.2 Wall Mounting.....	5
3.3 Wiring .....	7
ATTENTION.....	7
3.3.1 Grounding .....	7
3.3.2 Fault Relay.....	7
3.3.3 Redundant Power Inputs .....	7
3.4 SIM Card Installation.....	8
 <b>Cables and Antenna .....</b>	 <b>9</b>
4.1 Ethernet Pin Definition .....	9
4.2 Serial Port Pin Definition.....	10
4.3 Cellular Antenna.....	11
 <b>Management .....</b>	 <b>12</b>
5.1 Network Connection .....	12
5.2 Configuration .....	13
5.2.1 Basic Setting .....	13
5.2.1.1 WAN.....	13
5.2.1.2 LAN .....	17
5.2.1.3 DHCP .....	18
5.2.1.6 DDNS.....	21
5.2.1.7 Date & Time .....	21
5.2.2 Serial Setting .....	22
5.2.3 Ignition Edge .....	32
5.2.4 Open Gateway-Inside .....	33
5.2.5 Networking Setting.....	33
5.2.2.1 NAT Setting.....	33
Virtual Server .....	33

5.2.2.2 Firewall Setting .....	35
5.2.2.3 VPN Setting .....	38
5.2.2.4 VRRP .....	46
5.2.2.5 Routing Protocol .....	47
5.2.6 System Tools.....	50
5.2.3.1 Login Setting.....	50
5.2.3.2 Router Restart.....	51
5.2.3.3 Firmware Upgrade .....	52
5.2.3.4 Save/Restore Configurations.....	52
5.2.3.5 Remote Management.....	53
5.2.3.6 Miscellaneous.....	54
5.2.3.7 Port Setting.....	54
5.2.3.8 Event Warning.....	55
5.2.3.9 Disk .....	59
5.2.7 System Status.....	60
5.2.4.1 System Info .....	60
5.2.4.2 System Log .....	60
5.2.4.3 Traffic Statistics.....	60
<b>Technical Specifications.....</b>	<b>62</b>
<b>Compliance.....</b>	<b>64</b>

# **Getting Started**

## **1.1 About the IGMG-P83244GC+-D4G**

IGMG-P83244GC+-D4G is a breakthrough innovation product which is a combines powerful hardware and software IoT gateway. It is using dual core ARMv7 Cortex-A9 CPU operating speed up to 2.0 GHz. It integrates 8 ports industrial Ethernet which 6 ports in switch mode for LAN and 2 ports in standalone for WAN, and 4 SFP fiber in combo ports and provides LTE 4G connectivity with AT&T<sup>®</sup> certification and dual SIM card support. It is also built in mSATA storage 64GB(up to 265GB) for huge IOT data collection. There are two serial ports RS232/422/485 and RS422/485 which both can support Modbus RTU serial protocol to connect with serial devices and providing all-in-one solutions to help user build up highly reliable and user-friendly SCADA and IOT system for variant industrial automation applications. IGMG-P83244GC+-D4G also supports VPN client/server including IPsec, OPENSLL VPN. It can provide remote access service through ORing-PaaS platform and NAT/firewall to protect networking security.

## **1.2 Software Features**

- Support Open VPN, PPTP VPN
- Versatile modes with redundant multiple host devices
- Supports 5 host devices: Virtual COM, TCP Server, TCP Client mode
- Supports 4 IP ranges: UDP
- Supports conversion between Modbus TCP and Modbus RTU
- Event warning by Syslog, e-mail, SNMP trap, and relay output

## **1.3 Hardware Features**

- 8 x 10/100 /1000Base-T(X) ports
- 4 x Gigabit SFP
- 1 x RS-232/422/485 serial port
- 1 x RS-422/485 serial port
- 3.5G HSUDPA or 4G LTE modem included
- 2 x SIM card slot
- Dual power inputs
- Casing: IP-30
- Operating temperature: -40 to 75°C
- Storage temperature: -40 to 85°C
- Operating humidity: 5% to 95%, non-condensing

- Dimensions: 116.4mm(W) x 170mm(D) x 154mm(H)

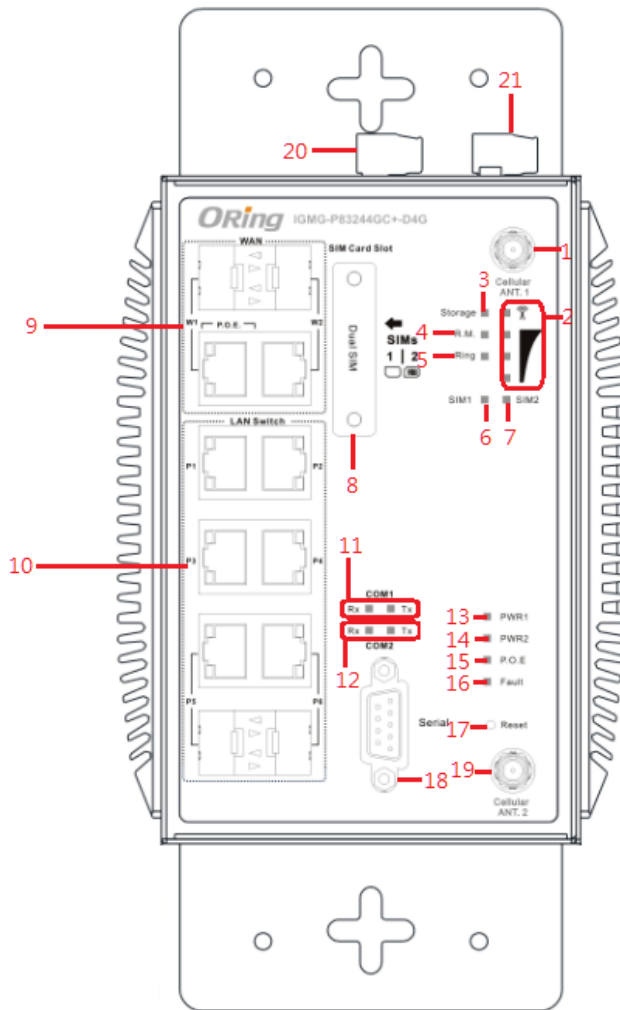
# Hardware Overview

## 2.1 Bottom Panel

### 2.1.1 Ports and Connectors

The series is equipped with the following ports and features on the front panel.

Port	Description
<b>10/100/1000Base-T(X) Ethernet ports</b>	4 x 10/100/1000 Base-T(X) ports supporting auto-negotiation.
<b>Gigabit Combo port with 10/100/1000Base-T(X) and 100/1000Base-X SFP ports</b>	4 x 10/100/1000Base-T(X) and 100/1000Base-X SFP ports
<b>SIM card slot</b>	2 x SIM card slot
<b>Serial port</b>	1 x RS-422/RS-485 serial port 1 x RS-232/RS-422/RS-485 serial port



1. Cellular 1 antenna connector
2. WiFi connection LED
3. Storage LED
4. Ring Master LED
5. Ring LED
6. SIM 1 card slot
7. SIM 2 card slot
8. SIM card slot
9. WAN port (P.o.E port)
10. Ethernet port
11. Serial port 1 TX / RX LED
12. Serial port 2 TX / RX LED
13. Power 1 LED
14. Power 2 LED
15. P.o.E LED
16. Fault LED
17. Reset button
18. Serial Port 2
19. Cellular 2 antenna connector
20. Serial port 1
21. Power 1 / 2 Connector

### 2.1.2 Front Panel LEDs

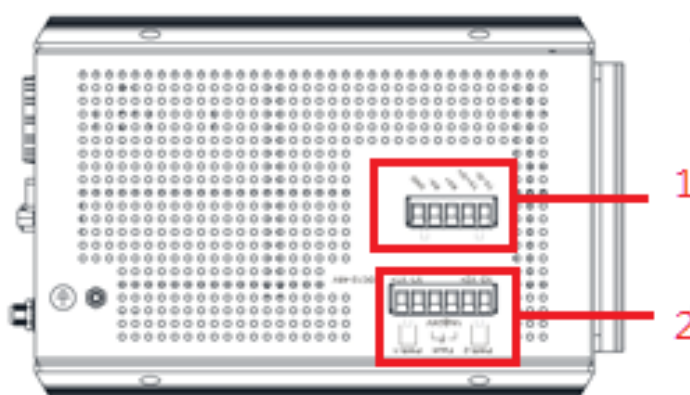
LED	Color	Status	Description
<b>PWR1/2</b>	Green	On	Power is on and function normally
<b>COM 1/2</b>	Green	On	Port is sending data
	Red	On	Port is receiving data
<b>10/100/1000Base-T(X) Ethernet ports</b>			
<b>LNK/ACT</b>	Green	On	Port is connected
		Blinking	Transmitting data
<b>Speed</b>	Green	On	Port running at 1000Mbps
	Amber	On	Port running at 100Mbps
	Green/Amber	Off	Port running at 10Mbps
<b>Fault</b>	Amber	On	Fault relay (power failure or port disconnected)

WLAN	Green	On	WLAN is activated (Strength: 1<25%, 2<50%, 3<75%, 4<100%)
		Blinking	Transmitting data

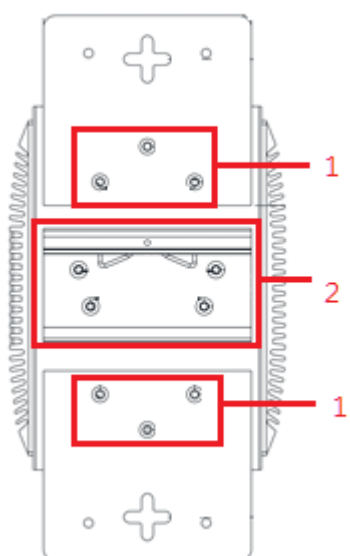
## 2.2 Top Panel

Below are the top panel components of the device:

1. Serial port 1: RS-422/RS-485(2W/4W),
2. Terminal Block, PWR1, PWR2, Relay.



## 2.3 Rear Panel

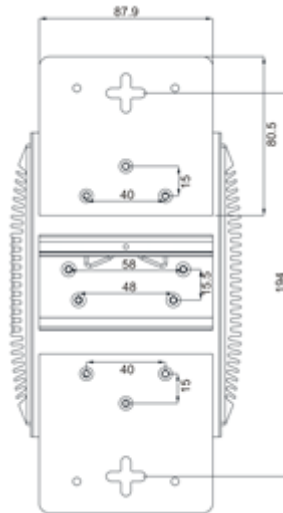


1. Wall-mount screw holes
2. DIN-rail screw holes

# Hardware Installation

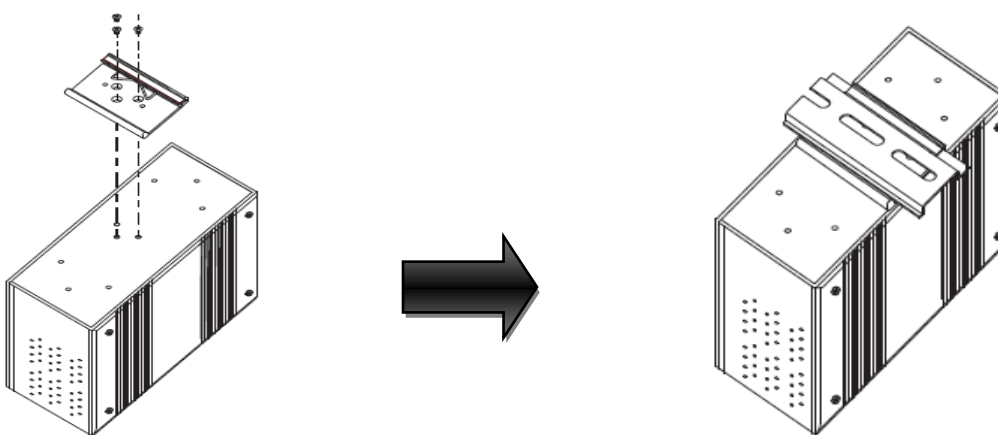
## 3.1 DIN-Rail Mounting

The device comes with a DIN-Rail kit in the package. The DIN-Rail kit allows you to fasten the device to a DIN-Rail.



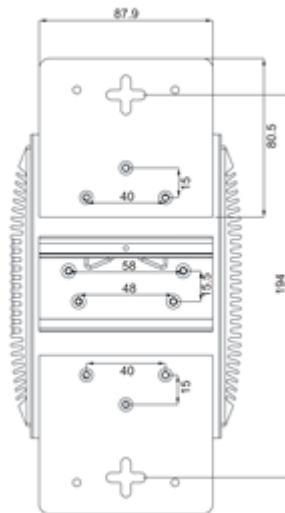
**DIN-rail Measurement (Unit = mm)**

Installing the device on the DIN-rail is easy. First, screw the Din-rail kit onto the back of the device, right in the middle of the back panel. Then slide the device onto a DIN-rail from the Din-rail kit and make sure the device clicks into the rail firmly.



## 3.2 Wall Mounting

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



**DIN-rail Measurement (Unit = mm)**

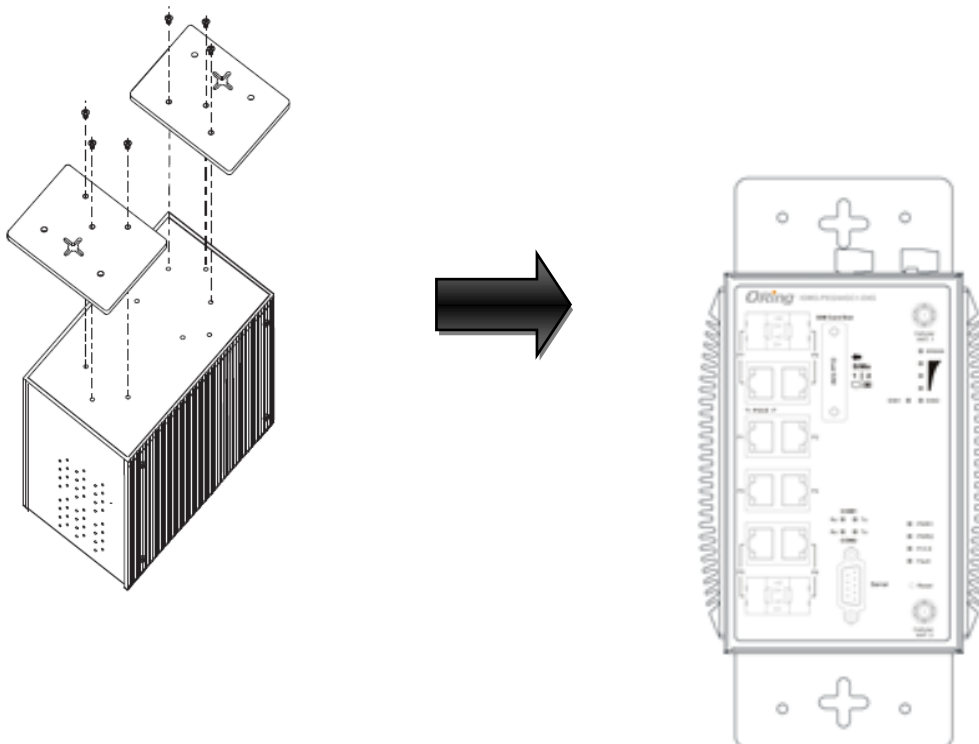
Follow the steps below to install the device to a rack.

**Step 1:** Screw the two pieces of wall-mount kits onto both ends of the rear panel of the switch.

A total of six screws are required, as shown below.

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

**Step 3:** Insert a screw through the cross-shaped aperture on the plate, and then slide the switch downwards. Tighten the screw for added stability.



## 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.

---



### ATTENTION

1. Be sure to disconnect the power cord before installing and/or wiring your devices.
  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.
- 

### 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 Fault Relay

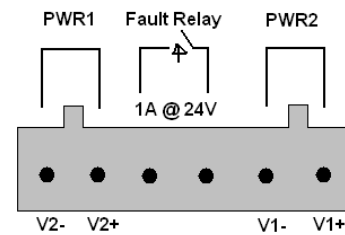
The two sets of relay contacts of the 6-pin terminal block connector are used to detect user-configured events. The two wires attached to the fault contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains closed.

### 3.3.3 Redundant Power Inputs

The device has two sets of power inputs, power input 1 and power input 2. The top two contacts and the bottom two contacts of the 6-pin terminal block connector on the device's top panel are used for the two digital inputs. Follow the steps below to wire redundant power inputs.

Step 1: insert the negative/positive 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.



### 3.4 SIM Card Installation

After disconnecting the power of the device:

1. Un-fasten the screws.
2. Remove the cover

**Note: only remove the cover for SIM card installation. DO NOT remove the cover in normal operation.**

3. Insert the SIM card into the slot.
4. Put the cover back
5. Fasten the screws.

**Note: Make sure the power is off before you install the SIM card.**

# Cables and Antenna

## 4.1 Ethernet Pin Definition

The device has standard Ethernet ports. According to the link type, the device uses CAT 3, 4, 5, 5e UTP cables to connect to any other network devices (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-TX	Cat 5e,6	UTP 100 m (328 ft)	RJ45

With 10/100Base-T(X) cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

**10/100Base-T(X) RJ-45 Port Pin Assignments:**

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
6	RD-

**1000Base-T RJ-45 Port Pin Assignments:**

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The device supports auto MDI/MDI-X operation. You can use a cable to connect the device to

a PC. The table below shows the 10/100Base-T(X) MDI and MDI-X port pin outs.

10/100Base-T(X) MDI/MDI-X Pin Assignments:

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

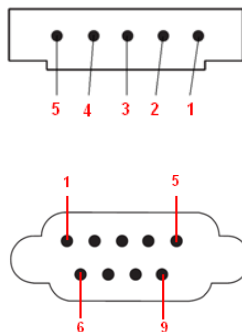
1000Base-T MDI/MDI-X Pin Assignments:

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

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

## 4.2 Serial Port Pin Definition

### Com 1 & Com 2

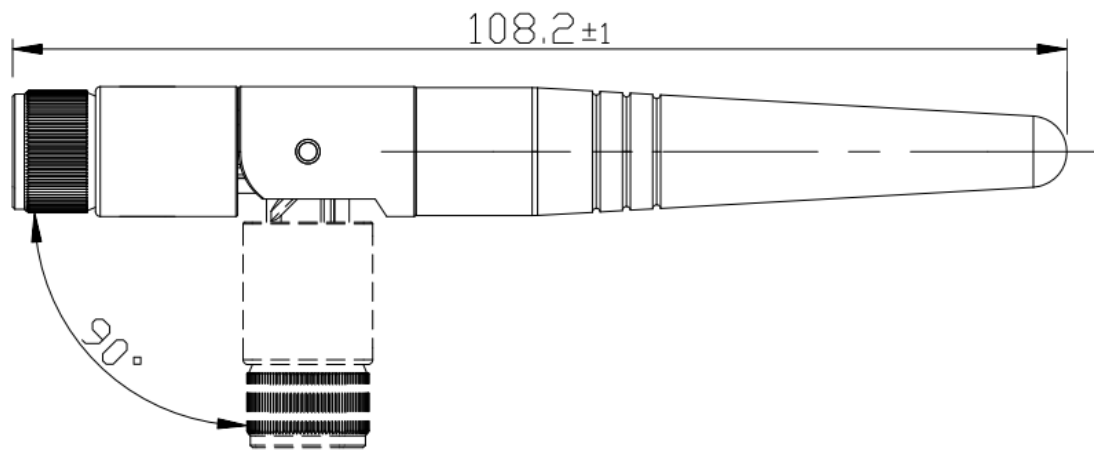


Pin #	RS-232	RS-422	RS-485 (4 wire )	RS-485 (2 wire )
1	DCD	TXD -	TXD -	DATA-
2	RXD	TXD +	TXD +	DATA+
3	TXD	RXD +	RXD +	
4	DTR	RXD -	RXD -	
5	GND	GND	GND	
6	DSR			

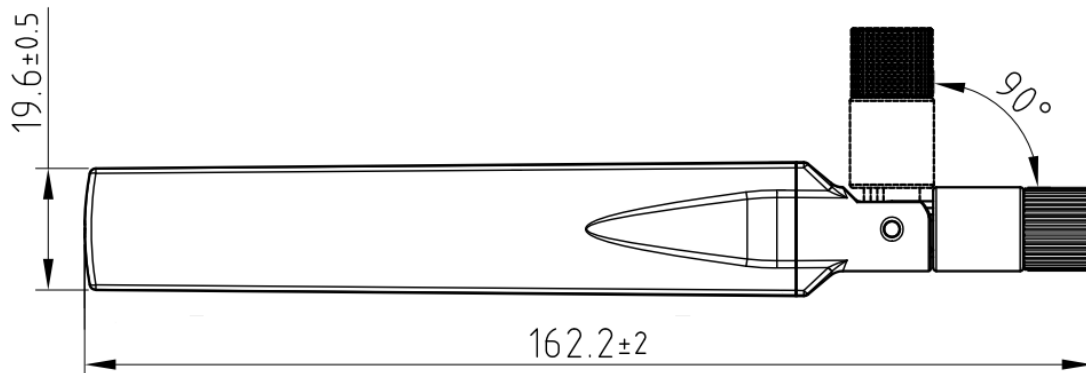
7	RTS			
8	CTS			
9	RI			
RS 232 mod act as DTE				

### 4.3 Cellular Antenna

The device provides one cellular connector for a 3G or 4G antenna. External RF cables and antennas can also be used with the connector.



**3G Cellular Antenna**



**4G LTE Antenna**

# Management

## 5.1 Network Connection

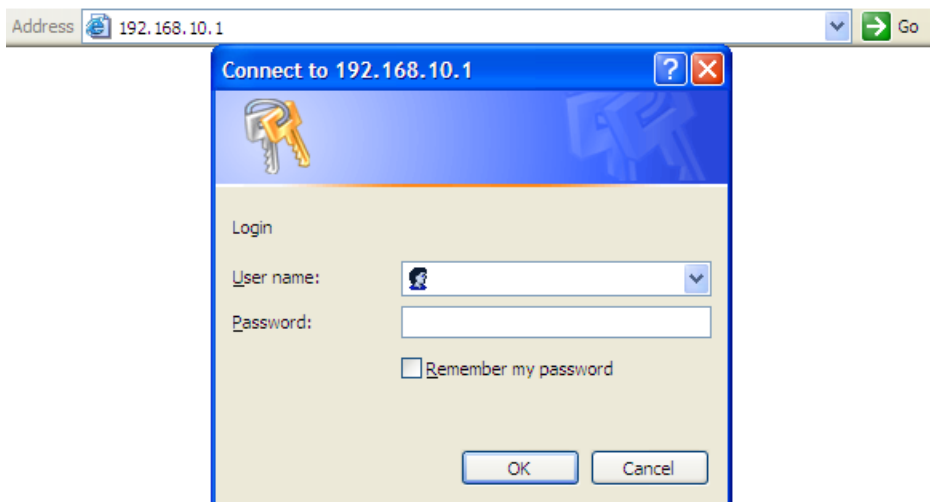
Before installing the Gateway, you need to be able to access the device via a computer equipped with an Ethernet card or LAN interface. To simplify the connection, it is recommended to use an Ethernet card to connect to a LAN.

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

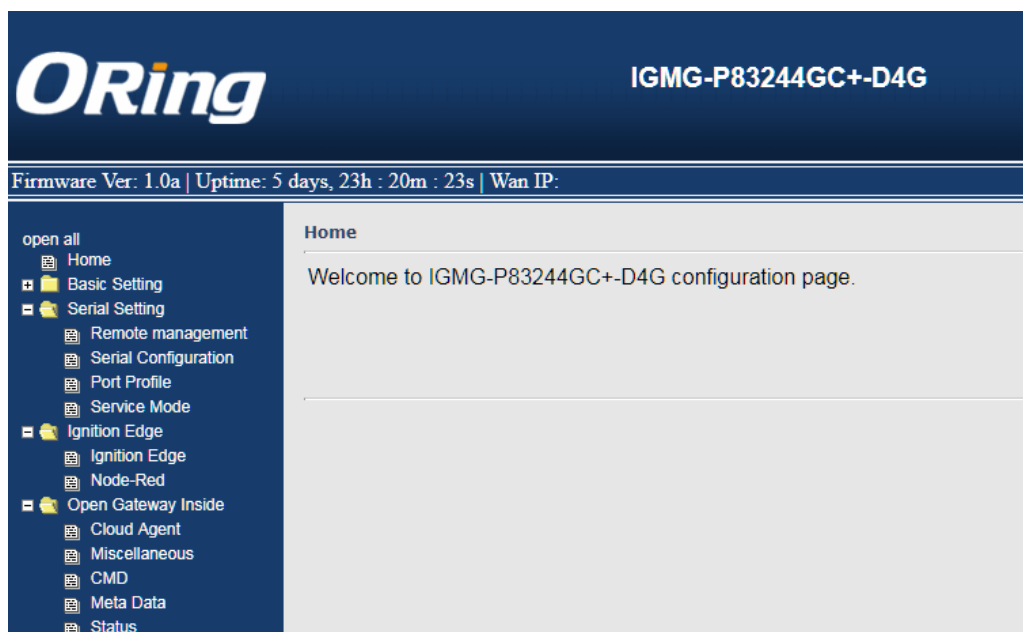
**Step 1:** Select a power source.

**Step 2:** Connect a computer to the device. Use either a straight-through Ethernet cable or cross-over cable to connect the ETH1 port 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 Gateway.

**Step 3:** Configure the device 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 Gateway) 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 to change the password. Click on **System Tools > Login Setting** after logging in to change the password.

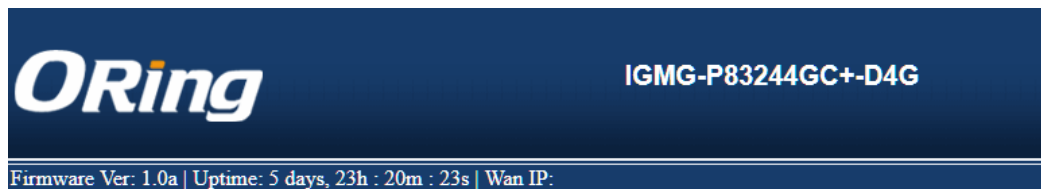


After you log in successfully, a Web interface will appear, as shown below. On the left hand side of the interface is a list of functions where you can configure the settings. The details of the configurations will be shown on the right screen.



## 5.2 Configuration

On top of the Home 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 AP router is started
Wan IP	Shows WAN IP address

### 5.2.1 Basic Setting

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

#### 5.2.1.1 WAN

This page allows you to configure WAN settings based on the type of connections you use. You can consult your ISP if you are unsure of your connection type. If you use the PPPoE option, make sure any PPPoE client software on your computers is removed or disabled.

#### WAN Connection Type as Dynamic/Static IP

Choose this option if your ISP provides you a fixed IP address or the ISP's servers assign the router's IP addressing upon establishing a connection. You have to manually input the IP information which is provided by your ISP.

**Basic Setting --> WAN**

WAN settings.

WAN Connection Type: Dynamic/Static IP ▾

**Obtain an IP address automatically**

**Use the following IP address:**

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway:

Ping Test Site:

**Obtain DNS server address automatically**

**Use the following DNS server addresses:**

Preferred DNS:

Alternate DNS:

**Use Modem/3G/4G as backup connection.**

APN:

User Name:

Password:

Ping Test Site:

Label	Description
<b>Obtain an IP address automatically</b>	Select this option if you want the IP address of the WAN port to be assigned automatically by the DHCP server in your network.
<b>Use the following IP address</b>	Select this option if you want to assign an IP address to the WAN port manually. You should set IP Address, Subnet Mask, and Default Gateway according to IP rules. You can also type a link in the Ping Test Site field to test your Internet connection
<b>Obtain DNS server address automatically</b>	Obtains a DNS server address from a DHCP server. If you have chosen to obtain an IP address automatically, this option will be

	selected accordingly.
<b>Use the following DNS server addresses</b>	Specifies a DNS server address manually. You can enter two addresses as the primary and secondary options.
<b>Use Modem/3G as backup connection</b>	<p>Enable this option if you want to use modem/3G as a backup connection when main connection is lost.</p> <p>Enter your account username and password in the corresponding fields.</p> <p>Type a website address such as <a href="http://www.google.com">www.google.com</a> in Ping Test Site to use it to check if the connection is alive or lost.</p>

### WAN Connection Type as PPPoE

Choose this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. This is a common option for DSL providers. You will need to enter a username and password

**Basic Setting --> WAN**

WAN Settings.

WAN Connection Type: PPPoE ▼

User Name:

Password:

Service Name:  (optional)

AC Name:  (optional)

Ping Test Site:

**Specify the IP & DNS provided by ISP ( If unknown, leave it unchecked )**

IP Address:

Preferred DNS:

Alternate DNS:

**Connection Mode**

Auto  
 Connect On Demand  
     Max Idle Time:  minutes (0 represents never bring down the link)  
 Manual

---

**Use Modem/3G/4G as backup connection.**

APN:   
 User Name:   
 Password:   
 Ping Test Site:

Link Status: Disconnected

### WAN Connection Type as Modem/3G

**Basic Setting --> WAN**

---

WAN Settings.

WAN Connection Type:

APN:   
 User Name:   
 Password:   
 Ping Test Site:

PIN:  Enable PIN check before dialing  
     PIN Code:

Auto Connect :  Enable  
 Reconnect on Failure:  Enable

Signal Quality Threshold(dbm):  (default:-85)  
 Using Ping Test. Interval  sec.  counts.

Two LAN Ports:  Enable

Radio Type:

UIM Status : not-present

Operations :

Link Status : Disconnected

Modem Status: Operator:  
 RadioType: lte  
 Signal Quality: -95dBm (RSSI: 9)  
 Network Type:

Label	Description
<b>APN</b>	Enter the APN value (optional)
<b>User Name</b>	Enter the user name provided by your ISP
<b>Password</b>	Enter the password provided by your ISP
<b>Ping Test Site</b>	Type a link in the field to test your Internet connection
<b>PIN</b>	Enter a PIN code if you want to perform PIN check
<b>Auto Connect</b>	Check to start connections when the device boots up
<b>Reconnect on Failure</b>	Check to allow for reconnection when links fail
<b>Two LAN ports</b>	Enable this option to use two LAN ports as WAN inputs.
<b>Radio Type</b>	Select a type of radio from the list which includes GSM, UMTS and both
<b>UIM Status</b>	Shows the status of SIM card
<b>Operations</b>	Click <b>Connect</b> to start modem/3G connections or <b>Disconnect</b> to shut down connections.
<b>Link Status</b>	Shows the status of connections
<b>Modem Status</b>	Shows information about the modem

### 5.2.1.2 LAN

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

**Basic Setting --> LAN**

>  
LAN Side settings.

Router Name:

LAN Profile:

Protocol:

IP Address:

Subnet Mask:

Gateway:

DNS:

Interface:  ETH1  Wireless1

Set the Function Of Physical Ports

ETH2 as WAN, ETH1 as LAN

ETH1 as WAN, ETH2 as LAN

LLDP Protocol:  Enable  Disable

SSH Server:  Enable  Disable

FTP Server:  Enable  Disable

Port

Samba Server:  Enable  Disable

Modbus TCP:  Enable  Disable

Port

Label	Description
<b>Router Name</b>	Enter the name of your device
<b>LAN Profile</b>	To choose IP setting for LAN0 and LAN1
<b>Protocol</b>	Static IP or DHCP Client
<b>IP Address</b>	The IP address of the LAN. The default value is <b>192.168.10.1</b>
<b>Subnet Mask</b>	The subnet mask of the LAN. The default value is <b>255.255.255.0</b>
<b>Gateway</b>	The Gateway address of the LAN. The default value is empty
<b>DNS</b>	The DNS address of the LAN. The default value is empty
<b>Interface</b>	To choose the interface to join this LAN profile
<b>LLDP Protocol</b>	LLDP is a vendor-neutral protocol used by network devices for advertising their identity, capabilities, and neighbors on a LAN. You can enable or disable LLDP protocol.
<b>Set the Function of Physical port</b>	ETH2 as WAN , ETH1 as LAN or ETH1 as WAN , ETH1 as WAN
<b>FTP Server</b>	Click to enable to disable network connectivity to a FTP server.
<b>Samba Server</b>	Click to enable to disable network connectivity to a Samba server.
<b>Modbus TCP</b>	Click to enable to disable network connectivity to Modbus TCP.

### 5.2.1.3 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 device 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 device can also serve as a relay agent which Sunday 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 device, 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.

**Basic Setting --> DHCP -> DHCP Server**

Set DHCP Server.

DHCP Mode:

---

DHCP Server:  Enabled  Disabled

Starting IP:

Ending IP:

Lease Time:  Hours

Local Domain Name:  (optional)

DNS Server 1:  (optional)

DNS Server 2:  (optional)

WINS Server:  (optional)

DHCP Range for Relay (Need 'Apply' to validate setting changes) :

Starting IP:

Ending IP:

Subnet Mask:

List of DHCP Range for Relay:

#	Starting IP	Ending IP	Subnet Mask	Operations
Allocate IP Address Manually.				
<input type="text" value="-- Choose a Client to Edit --"/>				<input type="button" value="Copy to"/>
MAC Address	IP Address		Operations	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>	<input type="button" value="Clear"/>

Static DHCP Client List:

#	MAC Address	IP Address	Operations
---	-------------	------------	------------

Label	Description
<b>DHCP Mode</b>	<p>Available options include <b>Built-in DHCP Server</b> and <b>DHCP Forwarder</b>. <b>Built-in DHCP Server</b> will enable the device to automatically assign an IP address to a computer on the LAN. <b>DHCP Forwarder</b> will forward DHCP messages to a server on the Internet to handle DHCP requests. If you choose <b>DHCP Forwarder</b>, enter a DHCP server IP address.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Set DHCP Server.</p> <p>DHCP Mode: <input type="text" value="DHCP Forwarder"/></p> <p>DHCP Server Location: <input checked="" type="radio"/> WAN <input type="radio"/> PPTP Remote Peer</p> <p>DHCP Server IP Address: <input type="text"/></p> </div>
<b>DHCP Server</b>	Enables or disables the DHCP server function. The default

	setting is <b>Enabled</b> . The Starting and Ending DHCP addresses should be in the same subnet as the LAN IP address of the VPN firewall.
<b>Starting IP</b>	Specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address.
<b>Ending IP</b>	Specifies the last of the contiguous addresses in the IP address pool.
<b>Lease Time</b>	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.
<b>Local Domain Name</b>	Enter the local domain name of a private network (optional). The DHCP will assign the entered domain to DHCP clients.
<b>DNS Server 1&amp;2</b>	Enter the IP address for the DNS server (optional)
<b>WINS Server</b>	Specifies the IP address of a local Windows NetBios Server if one is present in your network. (optional)
<b>DHCP Range for Relay</b>	Configure the DHCP range for relay by inputting a starting and ending IP address and a subnet mask.
<b>Starting IP</b>	The starting IP for the DHCP relay range
<b>Ending IP</b>	The ending IP for the DHCP relay range
<b>Subnet Mask</b>	Enter a Subnet mask for the DHCP relay range
<b>List of DHCP Range for Relay</b>	Shows all IP addresses for the DHCP relay range
<b>Allocate IP Address Manually</b>	By selecting an IP address from the drop-down list and click Copy to, you can edit the MAC addresses and IP addresses already assigned by the device and add it to the static DHCP client list.
<b>MAC Address</b>	The MAC addresses of the computer.
<b>IP Address</b>	The IP address to be related to the MAC address.
<b>Static DHCP Client List</b>	Shows the IP addresses locked to specific MAC addresses

## DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the

Host Name field will be blank.

Basic Setting --> DHCP -> DHCP Client List

Current DHCP Client Information

#	HostName	Mac	IP	Expires In
1	android-c397c98916b59beb	90:18:7c:1b:ff:1c	192.168.10.62	1 days, 22:12:30

Static IP Allocation

### 5.2.1.6 DDNS

DDNS (Dynamic Domain Name System) 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.

Basic Setting --> DDNS

DDNS settings.

DDNS Service:

User Name:  (\*)

Password:  (\*)

Domain:  (\*)

Label	Description
<b>DDNS Service</b>	Choose a DDNS service provider from the list
<b>User Name</b>	Enter the user name of your DDNS account
<b>Password</b>	Enter the password of your DDNS account
<b>Domain</b>	Enter the domain name provided by your dynamic DNS service provider

### 5.2.1.7 Date & Time

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.

**Basic Setting --> Date & Time**

Date/Time settings.

System time: Thu Aug 02 2012 12:9:27

NTP:  Enable

NTP Server 1:

NTP Server 2:  (optional)

Time Zone:  ▼

Synchronise:  ▼ at  ▼ :  ▼

Local Date:  Year  Month  Day

Local Time:  Hour  Minute  Second

Label	Description
<b>NTP</b>	Enables or disables NTP function
<b>NTP Server 1</b>	The primary NTP server
<b>NTP Server 2</b>	The secondary NTP server
<b>Time Zone</b>	Select the time zone you are located in
<b>Synchronize</b>	Specify the scheduled time for synchronization
<b>Local Date</b>	Set a local date manually
<b>Local Time</b>	Set a local time manually
<b>Get Current Date &amp; Time from Browser</b>	Click to set the time from your browser

## 5.2.2 Serial Setting

### Remote Management

The remote management setting allows you access the serial port from a WAN network.

**Serial Setting --> Remote management**

Set the Remote Management enable DS-tool to access from WAN.

Remote management:  Enable  Disable

Port External Access:

Port1:  Enable  Disable

Port2:  Enable  Disable

Label	Description
Remote Management	Enables or disables remote management function
Port External Access	Enable to allow using of serial data port and control port through WAN access.

## Serial Configuration

This page allows you to configure serial port parameters.

**Serial Setting --> Serial Configuration**

Port1 ▾

Port Alias

Interface  ▾

Baud Rate  ▾

Data Bits  ▾

Stop Bits  ▾

Parity  ▾

Flow Control  ▾

Force TX Interval Time  ms

Performance  Throughput  Latency

Label	Description
Port Alias	Enter the COM port number that modem is connected to
Interface	Choose an interface for your serial device. Available interfaces include <b>RS-232, RS-422, RS-485-2W, and RS-485-4W.</b>

Baud rate	Choose a baud rate in the range between 110 bps and 11520 bps
Data Bits	Choose the number of data bits to transmit. You can configure data bits to be 5, 6, 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 1.5(2). 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	<p>Choose the method of detecting errors in transmission. Parity control bit modes include None, Odd, Even, Mark, and Space.</p> <p><b>None</b> means parity checking is not performed and the parity bit is not transmitted.</p> <p><b>Odd</b> means 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.</p> <p><b>Even</b> means 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.</p>
Flow Control	Choose <b>XOFF</b> to tell the computer to stop sending data or <b>XON</b> to tell the computer to begin sending data again
Force TX 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. <b>0</b> means disable. Factory default value is <b>0</b> .
Performance	<p><b>Throughput:</b> This mode is optimized for the highest transmission speed.</p> <p><b>Latency:</b> This mode is optimized for the shortest response time.</p>

## Port Profile

This page allows you to set up parameters for individual ports.

**Serial Setting --> Port profile**

	Port1 ▼
Local TCP Port	4002
Command Port	4003
Mode	Serial to Ethernet
Flush Data Buffer After	0 ms
Delimiter(Hex 0~ff)	1: 00 2: 00 3: 00 4: 00
Mode	Ethernet to Serial
Flush Data Buffer After	0 ms
Delimiter(Hex 0~ff)	1: 00 2: 00 3: 00 4: 00

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.
Command Port	A listen TCP port for IP-Serial Lib commands from the host. In order to prevent a TCP port conflict with other applications, the user can set the Command port to another port if needed.
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 Data Buffer After" times out 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 <b>Flush Serial to Ethernet data buffer</b> times out. <b>0</b> means disabling the function. Factory default is <b>0</b> .

## Service mode

### Virtual COM Mode

In Virtual COM mode, the driver establishes a transparent connection between host and serial device by mapping the port of the serial server serial port to a local COM port on the host computer. The 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 Setting --> Service Mode**

	Port1 ▼
Data Encryption	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Service Mode	Virtual COM Mode ▼
Idle Timeout	<input type="text" value="0"/> (0~65535)seconds
Alive Check	<input type="text" value="40"/> (0~65535)seconds
Max Connection	<input type="text" value="1"/> max. connection (1~5)

Label	Description
Data Encryption	Use SSL to encrypt data.
Idle Timeout	When serial port stops data transmission for a defined period of time (Idle Timeout), the connection will be closed and the port will be freed and try to connect with other hosts. <b>0</b> indicates disabling this function. Factory default value is <b>0</b> . 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. <b>0</b> indicates disabling this function. Factory default is 0.
Max Connection	The number of maximum connections can be supported. The maximum value is <b>5</b> , default values is <b>1</b> .

\*Not allowed to mapping Virtual COM from web

### TCP Server mode

In TCP Server mode, IMG is configured with a unique port combination on a TCP/IP network. In this case, IMG 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. The 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 Setting --> Service Mode**

Port1 ▼

Data Encryption       Enable  Disable

Service Mode      TCP Server Mode ▼

TCP Server Port      4002

Idle Timeout      0 (0~65535)seconds

Alive Check      40 (0~65535)seconds

Max Connection      1 ▼ max. connection(1~5)

Label	Description
Data Encryption	Use SSL to encrypt data.
TCP Server Port	Set the port number for data transmission.
Idle Timeout	When serial port stops data transmission for a defined period of time (Idle Timeout), the connection will be closed and the port will be freed and try to connect with other hosts. <b>0</b> indicates disabling this function. Factory default value is <b>0</b> . 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. <b>0</b> indicates disabling this function. Factory default is <b>0</b> .
Max Connection	The number of maximum connections can be supported. The maximum value is <b>5</b> , default values is <b>1</b> .

**TCP Client Mode**

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

**Serial Setting --> Service Mode**

Port1 ▾

Data Encryption       Enable  Disable

Service Mode          TCP Client Mode ▾

Destination Host      0.0.0.0 : 4002

Idle Timeout          0 (0~65535)seconds

Alive Check          40 (0~65535)seconds

Connect on             Startup  Any Character

Destination Host	Port
1. <input type="text"/>	<input type="text" value="65535"/>
2. <input type="text"/>	<input type="text" value="65535"/>
3. <input type="text"/>	<input type="text" value="65535"/>
4. <input type="text"/>	<input type="text" value="65535"/>

Label	Description
Data Encryption	Use SSL to encrypt data.
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 (Idle Timeout), the connection will be closed and the port will be freed and try to connect with other hosts. <b>0</b> indicates disabling this function. Factory default value is <b>0</b> . 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. <b>0</b> indicates disabling this function. Factory default is <b>0</b> .
Connect on Startup	The TCP Client will build TCP connections once the connected serial device is started.
Connect on Any Character	The TCP Client will build TCP connections once the connected serial device starts to send data.

**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 Setting --> Service Mode**

Port1 ▾

Service Mode: UDP Mode ▾

Listen Port: 4002

Host start IP	Host end IP	Send Port
1. <input type="text"/>	<input type="text"/>	<input type="text" value="65535"/>
2. <input type="text"/>	<input type="text"/>	<input type="text" value="65535"/>
3. <input type="text"/>	<input type="text"/>	<input type="text" value="65535"/>
4. <input type="text"/>	<input type="text"/>	<input type="text" value="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 IP/end IP	If there are more than one destination hosts, specify the IP address range by inputting a value in <b>Host Start / End IP</b> . You can also auto scan the sending port number of the device
Send Port	Set the send port number.

### RTU/ASCII Slave Mode

Modbus RTU Slave mode allows communications between a host computer and a slave device. After a host computer sends a command, the slave device processes the command and returns a response to the host computer. This process is repeated, allowing the host computer to monitor and control controller operation. Modbus ASCII Slave mode works the same as Modbus/RTU Slave mode, except that the data format is Modbus/ASCII.

**Serial Setting --> Service Mode**

Port1 ▼

Service Mode: ASCII Slave Mode ▼

TCP Server Port: 502

Max Connection: 10 (1~128)Connection

Max Try Time: 5 (0~15)Try Times

Request Pause: 100 (1~10000) msec

Response Wait: 100 (1~10000) msec

Idle Timeout: 10 (1~10000)seconds

**Serial Setting --> Service Mode**

Port1 ▼

Service Mode: RTU Slave Mode ▼

TCP Server Port: 502

Max Connection: 10 (1~128)Connection

Max Try Time: 5 (0~15)Try Times

Request Pause: 100 (1~10000) msec

Response Wait: 100 (1~10000) msec

Idle Timeout: 10 (1~10000)seconds

Label	Description
<b>TCP Server Port</b>	Indicates the port used for the Modbus/TCP communication
<b>Max Connection</b>	The total number of remote TCP/IP clients allowed to connect to this server.
<b>Max Try Time</b>	The maximum number of request retries performed serially.
<b>Request Pause</b>	The delay between serial requests in milliseconds
<b>Response Wait</b>	The serial response timeout in milliseconds
<b>Idle Timeout</b>	Enter a TCP connection timeout in seconds. When no Modbus/TCP data is received within this timeout, the TCP connection will be dropped.

### RTU/ASCII Master Mode

The ModBus RTU Master mode is used to connect to the serial device which runs as RTU slave. Serial port server will connect to the remote TCP Server, which is also called Modbus TCP Slave.

#### Serial Setting --> Service Mode

	<input type="text" value="Port1"/>
Service Mode	<input type="text" value="RTU Master Mode"/>
Destination Host	<input type="text"/> : <input type="text" value="502"/>
Idle Timeout	<input type="text" value="0"/> (0~65535)seconds
Alive Check	<input type="text" value="0"/> (0~65535)seconds

#### Serial Setting --> Service Mode

	<input type="text" value="Port1"/>
Service Mode	<input type="text" value="ASCII Master Mode"/>
Destination Host	<input type="text"/> : <input type="text" value="502"/>
Idle Timeout	<input type="text" value="0"/> (0~65535)seconds
Alive Check	<input type="text" value="0"/> (0~65535)seconds

Label	Description
<b>Destination Host</b>	Set the IP address of host and the port number of data port. .
<b>Idle Timeout</b>	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. <b>0</b> 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.
<b>Alive Check</b>	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. <b>0</b> indicates disabling this function. Factory default is <b>0</b> .

### 5.2.3 Ignition Edge

User will need to Accept the agreement before activate the ignition edge.

#### Ignition-Edge

**Ignition Edge**

---

Ignition status: active successfully.

Launch Ignition WebBrowser:

Current Ignition: Edge version

Ignition Version: 7.9.10

Java Version: 1.8.0\_172

Available Disk Space: 783.7M / 64G

未選擇任何檔案

Label	Description
<b>Ignition-Edge</b>	Enabled./ Disabled the Ignition-Edge server.
<b>Launch Ignition-Edge Web</b>	Launch the Ignition Edge web in browser.
<b>Ignition-Edge Version</b>	Current Ignition-Edge version installed
<b>Java Version</b>	Current Java version installed
<b>Available Disk Space</b>	Free Disk Space remain
<b>Upgrade ignition files</b>	To upgrade the ignition –Edge module.

#### Node-Red

**Node Red**

---

Node Red:  Enabled  Disabled

Launch Node-Red:

Node-RED Version: v0.18.7

Node.js Version: v8.11.4

---

Label	Description
<b>Node Red</b>	Enabled./ Disabled the Node-Red
<b>Launch Node-Red</b>	Launch the Node-Red in browser.
<b>Node-Red Version</b>	To upgrade the Node-Red module.

## 5.2.4 Open Gateway-Inside

Please refer to Open Gateway User Manual for this feature.

## 5.2.5 Networking Setting

This section will guide you through various networking settings, including NAT, firewall, VPN, VRRP, and routing protocol.

### 5.2.2.1 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 device 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.

Networking Setting --> NAT Setting -> Virtual Server

Virtual server settings.

Virtual Server:  Enable  Disable

Description:

Public IP:  All  Specify

Public Port:

Protocol:  TCP  UDP  Both

Local IP:

Local Port:

Enable Now:  Yes  No

Virtual server list:

#	Description	Public IP	Public Port	Protocol	Local IP	Local Port	Enabled	Ops

Label	Description
<b>Virtual Server</b>	Select <b>Enabled</b> or <b>Disabled</b> to activate or deactivate virtual server
<b>Description</b>	Enter the description of the entry. Acceptable characters are 0-9,

	a-z, and A-Z. A null value is allowed.
<b>Public IP</b>	Enter a public IP allowed to access the virtual service. If not specified, choose <b>All</b> .
<b>Public Port</b>	The port number to be used to access the virtual service on the WAN (Wide Area Network)
<b>Protocol</b>	The protocol used for the virtual service
<b>Local IP</b>	The IP address of the computer that will provide virtual service
<b>Local Port</b>	The port number of the service used by the private IP computer
<b>Enable Now</b>	Enables the virtual server entry after adding it
<b>Virtual server list</b>	Click <b>Edit</b> to edit the virtual service entry and <b>Del</b> 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.

**Networking Setting --> NAT Setting -> DMZ**

DMZ settings.

DMZ:  Enable  Disable

Description:

DMZ Host IP:

Label	Description
<b>DMZ</b>	Enables or disables DMZ
<b>Description</b>	Enter a description for the DMZ host entry
<b>DMZ Host IP</b>	Enter the IP address of the computer to act as the DMZ host

## UPnP

The UPnP (Universal Plug and Play) feature allows Internet devices to access local host resources or devices as needed. UPnP-enabled devices can be automatically discovered by

the UPnP service application on the LAN.

Networking Setting --> NAT Setting -> UPnP

UPnP settings.

UPnP:  Enabled  Disabled  
 Enable NAT-PMP

UPnP List:

#	Application	Ext Port	Protocol	Int Port	IP Address
---	-------------	----------	----------	----------	------------

Label	Description
<b>UPnP</b>	Enable or disable UPnP.
<b>Enable NAT-PMP</b>	NAT-PMP allows a computer in a private network (behind a NAT router) to automatically configure the device to allow parties outside the private network to contact with each other. NAT-PMP operates with UDP. It essentially automates the process of port forwarding. Check the box to enable NAT-PMP.
<b>UPnP List</b>	This table lists the current auto port forwarding information. Application: The application that generates this port forwarding. Ext Port: The port opened on WAN Protocol: The protocol type Int Port: The port redirected to the local computer IP Address: The IP address of local computer to be redirected to

## 5.2.2.2 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.

Networking Setting --> Firewall Setting -> IP Filter

IP filter settings.

IP Filter:  Enable  Disable

Description:

Rule:

Direction:

IP Address: Source IP:  Destination IP:

Protocol:  All  ICMP  Specify protocol number:

TCP  Specify port:

UDP  Specify port:

Enable Now:  Yes  No

IP filter list:

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

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

Networking Setting --> Firewall Setting -> MAC Filter

MAC Filter settings.

MAC Filter:  Enable  Disable

Description:

Rule:

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

Enable Now:  Yes  No

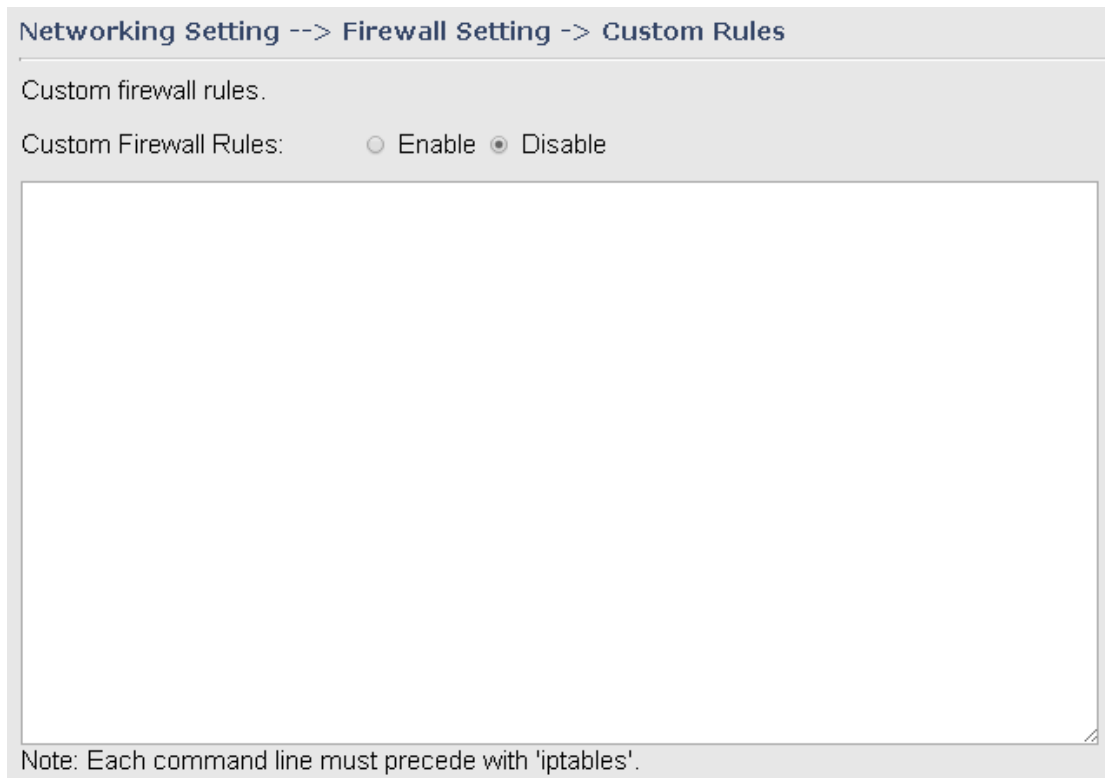
MAC filter list:

#	Description	Rule	MAC Address	Enabled	Operations
---	-------------	------	-------------	---------	------------

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

## Custom Rules

Custom firewall rules provide more granular access control beyond LAN isolation. 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.



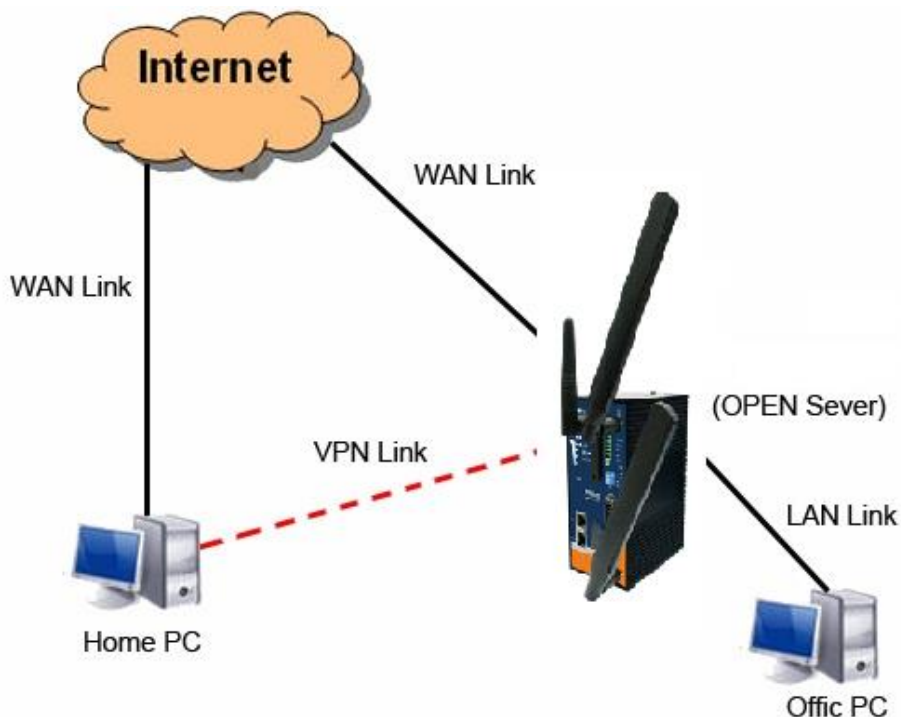
### 5.2.2.3 VPN Setting

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

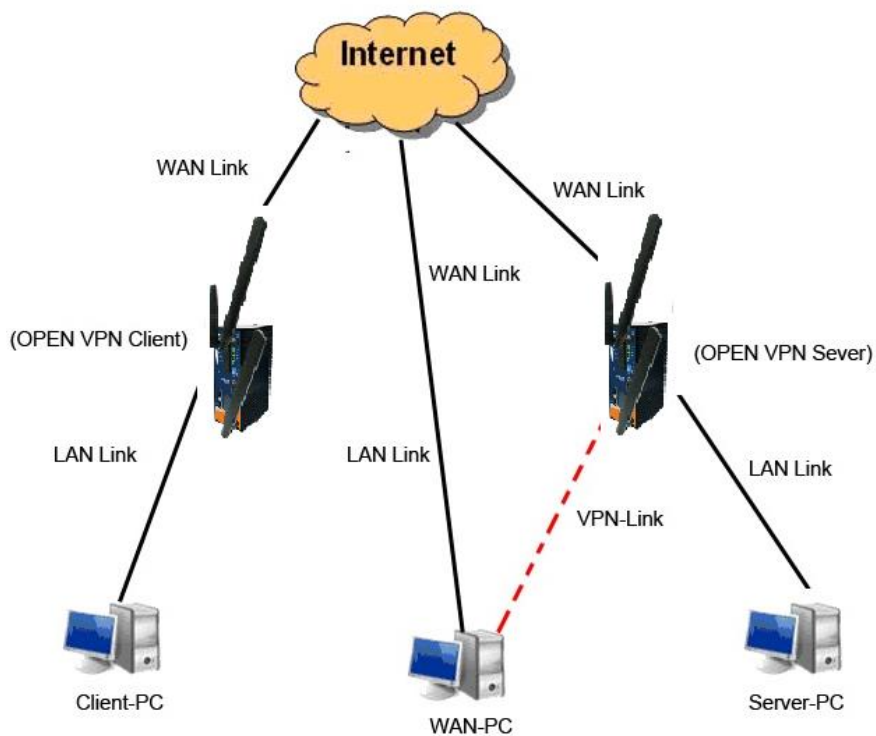
Open VPN enables you to easily set up a virtual private network over an encrypted connection. It is a full-function SSL VPN solution which accommodates a wide range of configurations including remote access, site-to-site VPNs, WiFi security, and enterprise-level remote access with load balancing, failover,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

To set up your device 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#stable>.



**Connection to Open VPN Server**

When you enable Open VPN Client, you need two Gateways 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**

Networking Setting --> Vpn Setting -> Openvpn

Openvpn settings.

**Server settings.**

Openvpn Server:  Enable  Disable

Interface Type: TAP ▼

Tunnel Protocol: UDP ▼

Port: 1194

Redirect Gateway:

Manage Client-Specific Options:

LZO Compression:  Enable  Disable

Cipher: BF-CBC ▼

Keys Setting: Auto ▼

Diagnosis

**Client settings.**

Openvpn Client:  Enable  Disable

Server IP/Host Name:

Interface Type: TAP ▼

Tunnel Protocol: UDP ▼

Port: 1194

Test Site:  ( Same as Event SMS -> VPN IP field. )

Reconnect on Failure:  Enable

LZO Compression:  Enable  Disable

Cipher: AUTO ▼

Keys Setting: Auto ▼

Diagnosis

Label	Description
<b>Open VPN Server</b>	Enables or disables the function of Open VPN server
<b>Interface Type</b>	Choose from the drop-down list to use <b>TAP</b> mode or <b>TUN</b> mode. TUN is for IP routing and TAP is for bridging. Choose TAP if you want to create a bridge tunnel between two locations using OpenVPN. If you want to route across your tunnel, then choose TUN.
<b>Tunnel Protocol</b>	Select <b>UDP</b> or <b>TCP</b> 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.
<b>Port</b>	The number of the port (default is <b>1194</b> ).
<b>Redirect Gateway</b>	Check this box will force all traffic to be routed through the VPN tunnel.

<b>Manage Client-Specific Options</b>	Check this box will allow VPN clients to access each other's shared resources. Otherwise, VPN clients can access the shared resources of only those computers directly connected to the local network of the device.
<b>LZO Compression</b>	Enables or disables the LZO Compression. Check the box will enable compression over VPN.
<b>Cipher</b>	Select a cryptographic cipher from the drop-down list. The client and server must use the same settings.
<b>Keys Setting</b>	Select <b>Auto</b> to use preset certificates or <b>Manual</b> to use your certificates. Please install openvpn client software to generate your certificates and paste them here. For more information, please visit openvpn website.
<b>Open VPN Client</b>	Enables or disables the function of Open VPN client.
<b>Server IP/Host name</b>	Enter the Open VPN server IP address.
<b>Tunnel Protocol</b>	Select <b>UDP</b> or <b>TCP</b> 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.
<b>Port</b>	The number of the port (default is <b>1194</b> ).
<b>Test Site</b>	Type a website address the field to use it to check if the connection is alive or lost.
<b>Reconnection on Failure</b>	Check the box to enable the device to reconnect when the link fails.
<b>LZO Compression</b>	Enables or disables the LZO Compression. Check the box will enable compression over VPN.
<b>Keys Setting</b>	Select <b>Auto</b> to use preset certificates or <b>Manual</b> to use your certificates. Please install openvpn client software to generate your certificates and paste them here. For more information, please visit openvpn website.

## Routing Setting

Networking Setting --> VPN Setting -> OpenVPN ClientRoute

Common Name:

Subnet IP Address:

Netmask:

Enable Now:  Yes  No

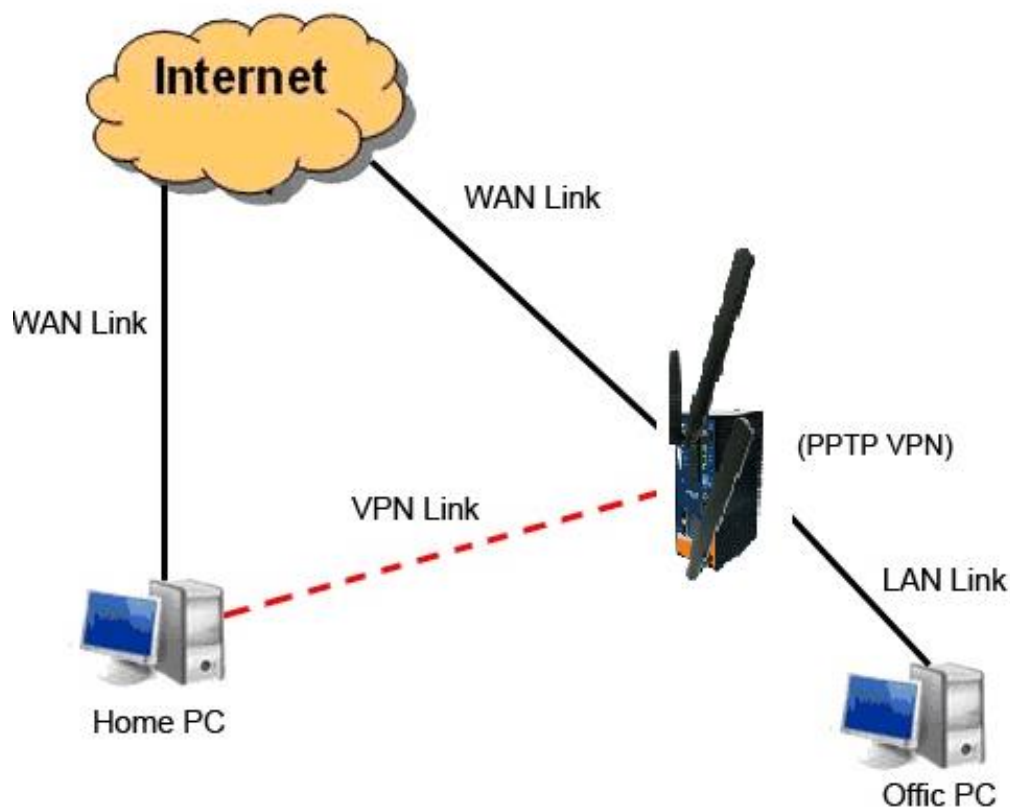
OpenVPN:

#	Common Name	Subnet IP	Netmask	Enabled	Operations
---	-------------	-----------	---------	---------	------------

Label	Description
<b>Common Name</b>	Enter a common name for you to identify the VPN
<b>Subnet IP Address</b>	Enter the subnet IP address for the VPN.
<b>Netmask</b>	Enter the netmask IP address for the VPN.
<b>Enable Now</b>	Check to enable the function.

## PPTP VPN

PPTP (Point to Point Tunneling Protocol) VPN allows PCs connected to the Gateway through WAN ports to act as PCs in the same LAN.



To create a PPTP connection to the Gateway, you must create a new network connection on your Windows PC by right clicking **Network > Property > Create a new connection > Connect to my work space (VPN) > Use VPN to Internet**, and then enter the user name and password set in the page.

After setting up a new connection, you can make configurations in the following page.

**Networking Setting --> Vpn Setting -> PPTP Vpn**

PPTP Server settings.

PPTP Server       Enable  Disable

Server IP :     

Clients IP:     

PPP Options:

require-chap

require-mschap

require-mschap-v2

require-mppe

Routing Option:  Enable Routing Protocols through PPTP VPN Connection

CHAP-Secrets:

Label	Description
<b>PPTP Server</b>	Enables or disables PPTP VPN server
<b>Server IP</b>	Enter the server IP address. The default value is the IP address of the connected LAN port.
<b>Client IP</b>	Enter the IP address range in the form of 192.168.10.xx-xx. The connected client will be assigned with an IP address.
<b>PPP Options</b>	<p><b>Require-chap:</b> check to use chap authentication on your PPTP server</p> <p><b>Require-mschap:</b> check to use mschap authentication on your PPTP server</p> <p><b>Require-mschap-v2:</b> check to use mschap-v2 authentication on your PPTP server.</p> <p><b>Require mppe:</b> check to use MPPE (Microsoft Point-to-Point Encryption) encryption on data transmitted through PPP (Point-to-Point Protocol) and VPN links.</p>
<b>Routing Option</b>	Check to enable routing protocols through PPTP VPN

	connections
<b>CHAP-Secrets</b>	Enter the username and password pairs in the form of <b>user *</b> <b>pass *</b> . Multiple username and password pairs are allowed.

**PPTP Client**

If a device wants to link to the devices in different networks, you should enable PPTP client in the following page.



Networking Setting --> Vpn Setting -> PPTP Client

PPTP Client settings.

PPTP Client  Enable  Disable

Server IP/Hostname:

Username:

Password:

Options:

- Reconnect on failure
- default route
- require-chap
- require-mschap
- require-mschap-v2
- require-mppe

Routing Option:  Enable Routing Protocols through PPTP Client Connection

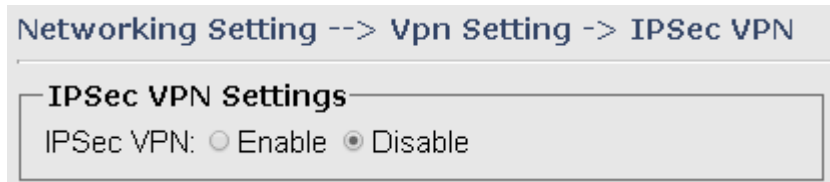
Operations:

Link Status: Disconnected

Label	Description
<b>PPTP Client</b>	Enables or disables PPTP client
<b>Server IP/Hostname</b>	Enter the server IP address or hostname
<b>Username/Password</b>	Enter the username and password assigned by PPTP server
<b>Options</b>	Choose the rules to be applied <b>Reconnect on failure:</b> prompts automatic reconnection when the link fails. <b>Require-chap:</b> check to use chap authentication on your PPTP server <b>Require-mschap:</b> check to use mschap authentication on your PPTP server <b>Require-mschap-v2:</b> check to use mschap-v2 authentication on your PPTP server <b>Require MPPE:</b> check to use MPPE (Microsoft Point-to-Point Encryption) encryption on data transmitted through PPP (Point-to-Point Protocol) and VPN links.
<b>Routing Option</b>	Click <b>Connect</b> to link to the server or <b>Disconnect</b> to disconnect from the server
<b>Operations</b>	Click <b>Connect</b> to link to the server or <b>Disconnect</b> to disconnect from the server
<b>Link Status</b>	Show the status of the link

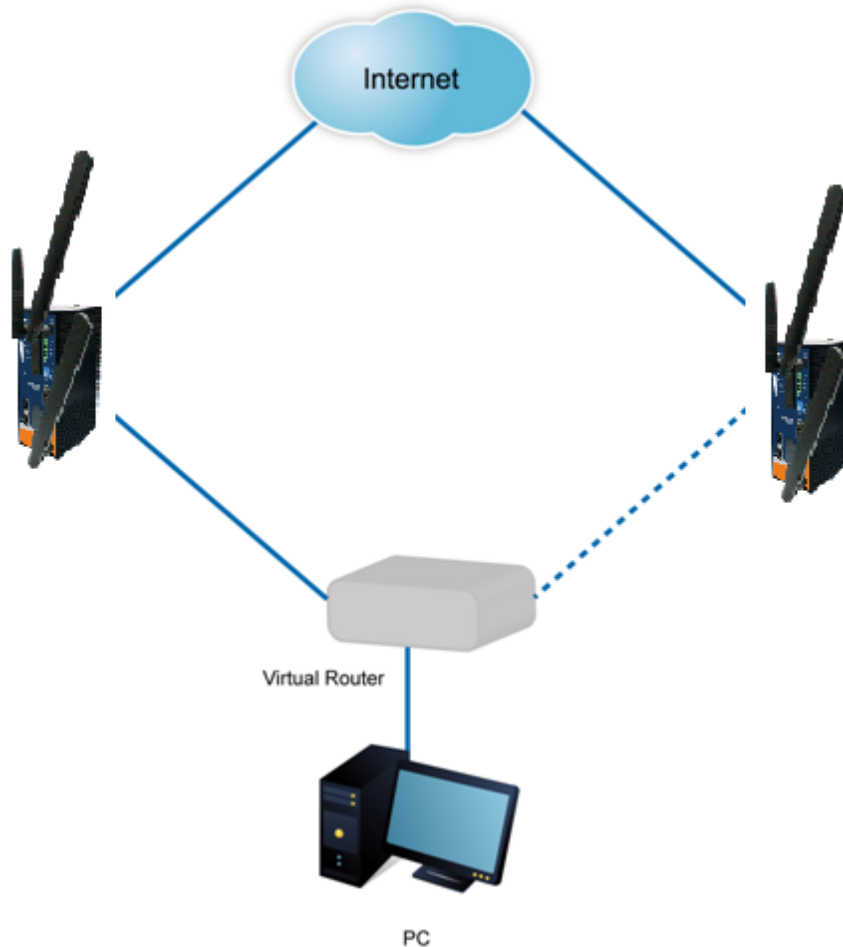
**IPSec VPN**

IPsec VPN provides secure IP communications by authenticating and encrypting each IP packet of a communication session. Check to box to enables or disables the function.



**5.2.2.4 VRRP**

A VRRP (Virtual Router Redundancy Protocol) is a computer networking protocol aimed to eliminate the single point of failure by automatically assigning available IP routers to participating hosts. Using a virtual router ID (VRID) address and virtual router IP (VRIP) address to represent itself, a virtual router consists of two or more physical routers, including one master router and one or more backup routers. All routers in the virtual router group share the same VRID and VRIP. The master router provides primary routing and the backup routers monitor the status of the master router and become active if the master router fails.



## Networking Setting --&gt; VRRP Setting -&gt; VRRP Setting

VRRP(Virtual Router Redundancy Protocol) settings.

VRRP Protocol:  Enable  Disable

VRRP Instance State:  Master  Backup

Virtual Router ID:

Virtual Router IP:

Priority:  (1~254)

Authentication Password:

Label	Description
<b>VRRP Protocol</b>	Enables or disables VRRP function
<b>VRRP Instance State</b>	Specifies the router to act as the master or backup router
<b>Virtual Router ID</b>	A VRID consists of one master router and one or more backup routers. The master router is the router that owns the IP address you associate with the VRID. Configure the VRID on the router that owns the default gateway interface. The other router in the VRID does not own the IP address associated with VRID but provides the backup path if the Master router becomes unavailable.
<b>Virtual Router IP</b>	An IP address associated with the VRID from which other hosts can obtain network service. The VRIP is managed by the VRRP instances belonging to a VRID.
<b>Priority</b>	The priority value used by the VRRP router when selecting the master virtual router.
<b>Authentication Password</b>	Enter the password for authentication

### 5.2.2.5 Routing Protocol

This page shows the information of the routing table. You can configure static and dynamic routing settings in this page.

Networking Setting --> Routing Protocol -> Routing Setting

Current Routing Table:

Destination	Gateway	Subnet Mask	Metric	Interface
192.168.2.0	0.0.0.0	255.255.255.0	0	br0(LAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)

Static Route Entry:

Destination	Gateway	Subnet Mask	Metric	Interface	Operations
				WAN	Add

Mode: Gateway

RIPv1 & v2: Disable

Telnet Setting:  Enable  Disable

Port: 23

Password:

### Static Routing

When RIPv1 & v2 is **Disabled**, the device will operate in static routing mode, which means devices forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.

Networking Setting --> Routing Protocol -> Routing Setting

Current Routing Table:

Destination	Gateway	Subnet Mask	Metric	Interface
192.168.2.0	0.0.0.0	255.255.255.0	0	br0(LAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)

Static Route Entry:

Destination	Gateway	Subnet Mask	Metric	Interface	Operations
192.168.11.0	0.0.0.0	255.255.255.0	1	WAN	Commit Delete
				WAN	Add

Mode: Gateway

RIPv1 & v2: Disable

Telnet Setting:  Enable  Disable

Port: 23

Password:

### Dynamic Routing

Dynamic routing lets routing tables in Gateways change as the routes change. If the best path to a destination cannot be used, dynamic routing protocols change routing tables when necessary to keep your network traffic moving. Dynamic routing protocols include RIP, OSPF, and BGP; however, the device only supports RIP (Routing Information Protocol).

Do not choose **Disable** in the RIPv1 & v2 list if you want to enable Dynamic Routing. After clicking **Apply**, more information will be displayed in Current Routing Table.

Networking Setting --> Routing Protocol -> Routing Setting

Current Routing Table:

Destination	Gateway	Subnet Mask	Metric	Interface
192.168.2.0	0.0.0.0	255.255.255.0	0	br0(LAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)

Static Route Entry:

Destination	Gateway	Subnet Mask	Metric	Interface	Operations
192.168.11.0	0.0.0.0	255.255.255.0	1	WAN	<input type="button" value="Commit"/> <input type="button" value="Delete"/>

Destination	Gateway	Subnet Mask	Metric	Interface	Operation
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	WAN ▾	<input type="button" value="Add"/>

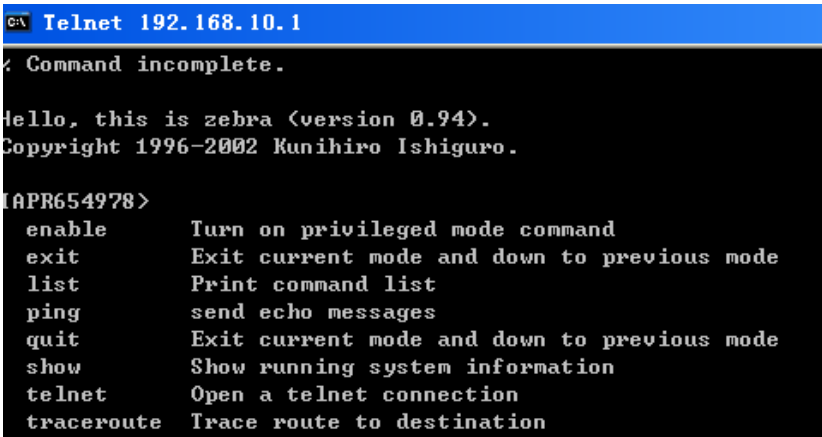
Mode:  ▾

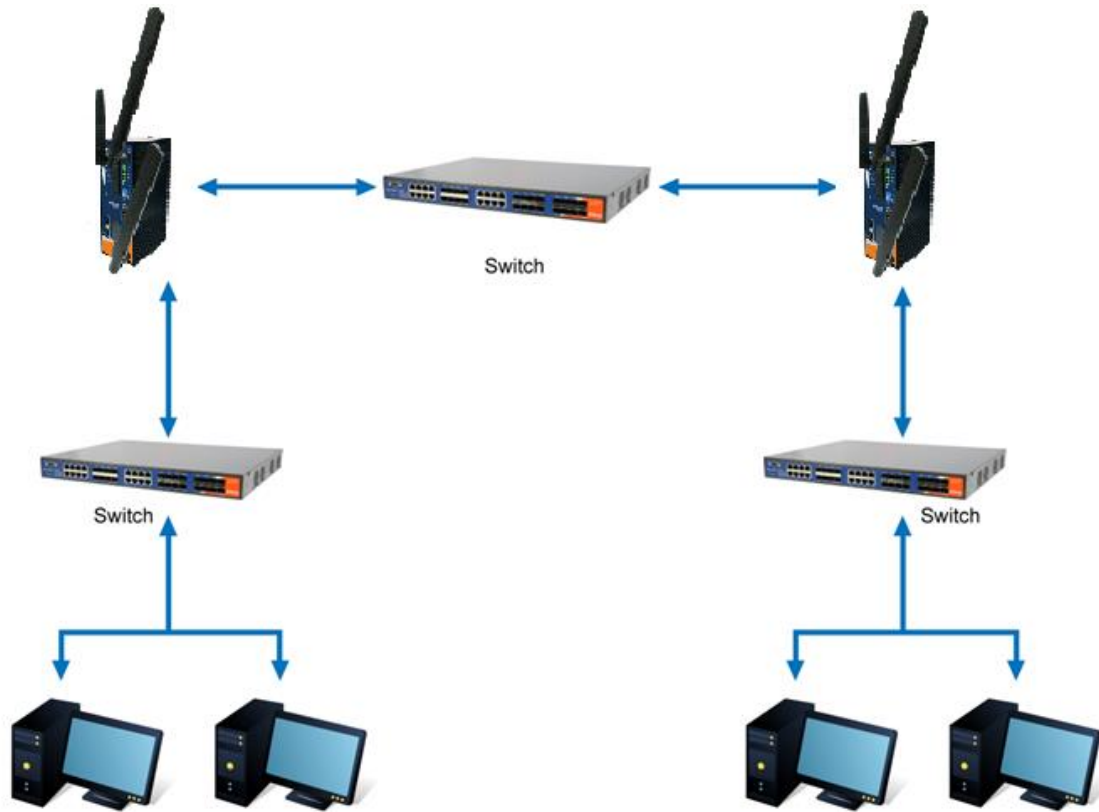
RIPv1 & v2:  ▾

Telnet Setting:  Enable  Disable

Port:

Password:

Label	Description
<b>Current Routing Table</b>	Shows all routing information, including static and dynamic routing (if enabled)
<b>Static Route Entry</b>	Fills in corresponding information to add new entries to the static routing tablet
<b>Mode</b>	Choose <b>Gateway Mode</b> if you want PCs in the LAN to visit external network, otherwise choose <b>Router Mode</b>
<b>RIPv1 &amp;v2</b>	Choose <b>Disable</b> to disable dynamic routing or other options to configure the interfaces for dynamic routing
<b>Telnet Setting</b>	This option is only available when dynamic routing is enabled. It allows you to make detailed configurations via simple comments.  



Routing Topography

## 5.2.6 System Tools

### 5.2.3.1 Login Setting

You can change login name and password in page. The default login name and password are both **admin**.

**System Tools --> Login Setting**

Login settings.

Old Login Name: admin

Old Password:

New Login Name: admin

New Password:

Confirm New Password:

Web Protocol:  HTTP  HTTPS

Port:

Label	Description
<b>Old Name</b>	Type in current login name
<b>Old Password</b>	Type in current password
<b>New Name</b>	Enter a new login name. Acceptable characters contain '0-9', 'a-z', 'A-Z' and the length must be 1 to 15 characters. An empty name is not acceptable.
<b>New Password</b>	Enter a new login password. Acceptable characters contain '0-9', 'a-z', 'A-Z' and the length must be 0 to 15 characters.
<b>Confirm New Password</b>	Retype the new password to confirm it.
<b>Web Protocol</b>	Choose a web management page protocol from <b>HTTP</b> and <b>HTTPS</b> . HTTPS (HTTP over SSL) encrypts data sent and received over the Web. Choose HTTPS if you want a secure connection.
<b>Port</b>	Choose a web management page port number. For HTTP, default port is <b>80</b> . For HTTPS, default port is <b>443</b> .

### 5.2.3.2 Router Restart

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

**System Tools --> Router Restart**

Router Restart Utility.

Scheduling:  Enable

Restart  at  :

Label	Description
<b>Restart Now</b>	Click to restart the device via warm reset
<b>Scheduling</b>	<b>Enable:</b> check to activate the setting Restart at: specify the time for resetting the device. You can configure the action to be performed periodically.

### 5.2.3.3 Firmware Upgrade

ORing launches new firmware constantly to enhance device 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 device. It will take several minutes to upload and update the firmware. After upgrade completes successfully, reboot the device.

**System Tools --> Firmware Upgrade**

Do NOT power off the router while upgrading!

Current Firmware Version: 1.2a

未選擇任何檔案

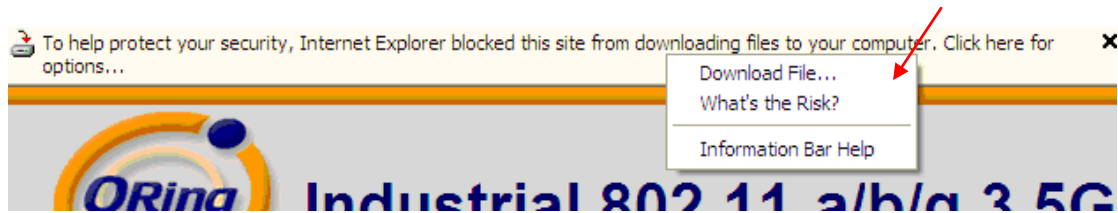


During firmware upgrading, do not turn off the power of the device or press the reset button.

### 5.2.3.4 Save/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
<b>Save</b>	Click to save existing configurations as a file for future usage.
<b>Select File</b>	You can restore configurations to previous status by installing a previous configuration file. To do this, choose <b>Web Restore</b> or <b>Tftp Restore</b> . If you choose <b>Web Restore</b> , you need to choose a file and click <b>Web Restore</b> . If you select <b>Tftp Restore</b> , fill in a Tftp server IP address and the file name before clicking <b>Tftp Restore</b> .
<b>Restore Factory Default Setting</b>	Click to reset the device to the factory settings. The device will reboot to validate the default settings.

### 5.2.3.5 Remote Management

The remote management setting allows you access the serial port from a WAN network.

**System Tools --> Remote Management**

Set the Remote Management to access the Router web pages from WAN side.

Remote Management:  Enable  Disable

Management Port:

Permission:  Any Host  
 Host with IP address:   
 Host within IP range:  -

Allow Ping from WAN:  Enable  Disable

Label	Description
<b>Remote Management</b>	Enables or disables remote management function
<b>Management Port</b>	Enter the port number that will be open to outside access. This port must be used when you establish a remote connection.
<b>Permission</b>	You can grant remote access to specific users by entering the IP address of their devices or assigning an IP range. Tick <b>Any Host</b> or enter a hostname or IP address if you only want a specific computer or device to be able to access the device.
<b>Allow Ping from WAN</b>	Click Enable to allow system administrator to ping the device from WAN interface

### 5.2.3.6 Miscellaneous

This page enables you to run ping test which will send out ping packets to test if a computer is on the Internet or if the WAN connection is OK. Enter a domain name or IP address in the destination box and click **Ping** to test.

**System Tools --> Miscellaneous**

Miscellaneous utilities.

Ping Test: Destination:

Ping Test Result:

### 5.2.3.7 Port Setting

You can choose port 1 or port 2 to act as WAN or LAN port in this page.

**Networking Setting --> Miscellaneous --> Port Setting**

Set the function of physical ports.

- Port2 as WAN, port1 as LAN
- Port1 as WAN, port2 as LAN

**5.2.3.8 Event Warning**

When an error occurs, the Gateway will notify you through system log, e-mail, SNMP, and relay.

**System Log**

**System Tools --> Even Warning Settings --> System Log**

## Syslog Server Settings

Syslog Server IP:   
 Syslog Server Port:  (0 represents default)

## Syslog Event Types

Device Event Notification	
Hardware Reset (Cold Start)	<input type="checkbox"/> Syslog
Software Reset (Warm Start)	<input type="checkbox"/> Syslog
Login Failed	<input type="checkbox"/> Syslog
WAN IP Address Changed	<input type="checkbox"/> Syslog
Password Changed	<input type="checkbox"/> Syslog
Redundant Power Changed	<input type="checkbox"/> Syslog
Eth Link Status Changed	<input type="checkbox"/> Syslog
SNMP Access Failed	<input type="checkbox"/> Syslog
Wireless Client Associated	<input type="checkbox"/> Syslog
Wireless Client Disassociated	<input type="checkbox"/> Syslog
Client Mode Associated	<input type="checkbox"/> Syslog
Client Mode Disassociated	<input type="checkbox"/> Syslog
Client Mode Roaming	<input type="checkbox"/> Syslog

Fault Event Notification	
Power 1 Fault	<input type="checkbox"/> Syslog
Power 2 Fault	<input type="checkbox"/> Syslog
Eth1 Link Down	<input type="checkbox"/> Syslog
Eth2 Link Down	<input type="checkbox"/> Syslog

Label	Description
<b>Syslog Server IP</b>	Enter the IP address of a remote server if you want the logs to be stored remotely. Leave it blank will disable remote syslog.
<b>Syslog Server Port</b>	Specifies the port to be logged remotely. Default port is 514.

**E-mail**

**System Tools --> Even Warning Settings --> E-mail**

---

E-mail Server Settings

SMTP Server:  (optional)

Server Port:  (0 represents default)

My Server requires authentication

User Name:

Password:

Sender Address:

E-mail Address 1:

E-mail Address 2:

E-mail Address 3:

E-mail Address 4:

E-mail Event Types

Device Event Notification	
Hardware Reset (Cold Start)	<input type="checkbox"/> SMTP Mail
Software Reset (Warm Start)	<input type="checkbox"/> SMTP Mail
Login Failed	<input type="checkbox"/> SMTP Mail
WAN IP Address Changed	<input type="checkbox"/> SMTP Mail
Password Changed	<input type="checkbox"/> SMTP Mail
Redundant Power Changed	<input type="checkbox"/> SMTP Mail
Eth Link Status Changed	<input type="checkbox"/> SMTP Mail
SNMP Access Failed	<input type="checkbox"/> SMTP Mail
Wireless Client Associated	<input type="checkbox"/> SMTP Mail
Wireless Client Disassociated	<input type="checkbox"/> SMTP Mail
Client Mode Associated	<input type="checkbox"/> SMTP Mail
Client Mode Disassociated	<input type="checkbox"/> SMTP Mail
Client Mode Roaming	<input type="checkbox"/> SMTP Mail

Fault Event Notification	
Power 1 Fault	<input type="checkbox"/> SMTP Mail
Power 2 Fault	<input type="checkbox"/> SMTP Mail
Eth1 Link Down	<input type="checkbox"/> SMTP Mail
Eth2 Link Down	<input type="checkbox"/> SMTP Mail

Label	Description
<b>SMTP Server</b>	Enter a backup host to be used when the primary host is unavailable.
<b>Server Port</b>	Specifies the port where MTA can be contacted via SMTP server
<b>E-mail Address 1-4</b>	Enter the mail address that will receive notifications

**SNMP**

**System Tools --> Even Warning Settings --> SNMP Settings**

SNMP Settings

SNMP Agent:  Enable  Disable

SNMP Trap Server 1:

SNMP Trap Server 2:

SNMP Trap Server 3:

SNMP Trap Server 4:

Community:

SysLocation:

SysContact:

SNMP Event Types

Device Event Notification	
Hardware Reset (Cold Start)	<input type="checkbox"/> SNMP Trap
Software Reset (Warm Start)	<input type="checkbox"/> SNMP Trap
Login Failed	<input type="checkbox"/> SNMP Trap
WAN IP Address Changed	<input type="checkbox"/> SNMP Trap
Password Changed	<input type="checkbox"/> SNMP Trap
Redundant Power Changed	<input type="checkbox"/> SNMP Trap
Eth Link Status Changed	<input type="checkbox"/> SNMP Trap
SNMP Access Failed	<input type="checkbox"/> SNMP Trap
Wireless Client Associated	<input type="checkbox"/> SNMP Trap
Wireless Client Disassociated	<input type="checkbox"/> SNMP Trap
Client Mode Associated	<input type="checkbox"/> SNMP Trap
Client Mode Disassociated	<input type="checkbox"/> SNMP Trap
Client Mode Roaming	<input type="checkbox"/> SNMP Trap

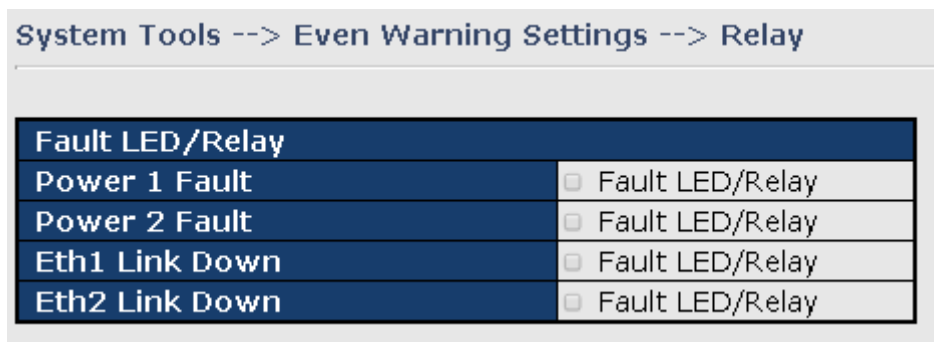
  

Fault Event Notification	
Power 1 Fault	<input type="checkbox"/> SNMP Trap
Power 2 Fault	<input type="checkbox"/> SNMP Trap
Eth1 Link Down	<input type="checkbox"/> SNMP Trap
Eth2 Link Down	<input type="checkbox"/> SNMP Trap

Label	Description
<b>SNMP Agent</b>	SNMP (Simple Network Management Protocol) Agent is a service program that runs on the access point. The agent provides management information to the NMS by keeping track of various operational aspects of the AP system. You can enable or disable the function.
<b>SNMP Trap Server 1-4</b>	Enter the IP address of the SNMP server which will send out traps generated by the AP.
<b>Community</b>	Community is a password to establish trust between managers and agents. Normally, <b>public</b> is used for read-write community.
<b>SysLocation</b>	Specifies sysLocation string
<b>SysContact</b>	Specifies sysContact string

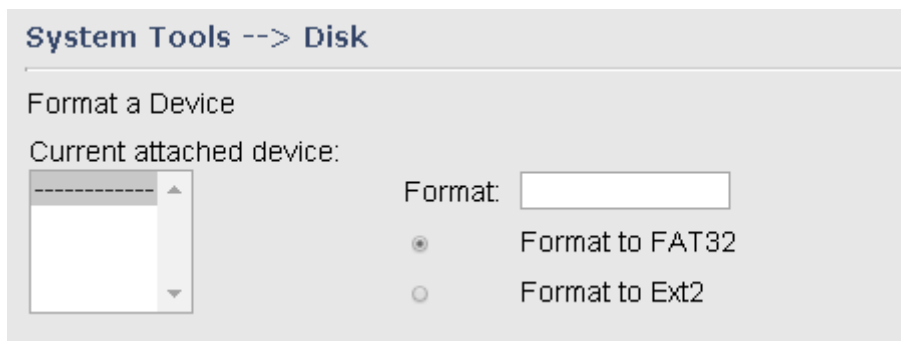
### Relay

You can select events to trigger relay action by checking the boxes in this section. Available events include power failure and Ethernet link disconnection.



### 5.2.3.9 Disk

This page allows you to format the disks in the device.



## 5.2.7 System Status

### 5.2.4.1 System Info

This page displays the detailed information of the device including model name, description, firmware version, WAN, LAN and settings.

System Status --> System Info

System Info.

<b>Model:</b>	IMG-6322GT	
<b>Model Description:</b>	IMG-6322GT (Sample Version)	
<b>WAN:</b>	Mode	Dynamic Setting
	Default Gateway	
	DNS(Primary)	
	DNS(Secondary)	
	MTU	1500
	MAC Address	00:1E:88:AA:BB:01
	IP Address	192.168.2.201
<b>LAN:</b>	Subnet Mask	255.255.255.0
	MTU	1500
	MAC Address	00:1E:88:AA:BB:00
	DHCP Server	Disabled

### 5.2.4.2 System Log

The Gateway will constantly log events and activities and provide the files for you to review. You can click **Refresh** to renew the page or **Clear Logs** to clear all or certain log entries.

System Status --> System Log

System log.

**Log Option:**

- DHCP Server
- Boot Message
- NTP Client
- PPTP VPN
- System Event
- UPNP
- Firewall
- Modem
- PPPoE Client
- OpenVpn

Select All
Deselect All
Save Option

System Log: Refresh Clear Logs

#	Date Time	Item	Content
---	-----------	------	---------

### 5.2.4.3 Traffic Statistics

This page displays network traffic statistics for packets both received and transmitted through Ethernet ports

**System Status --> Traffic Statistics**

Traffic statistics.

Interface	Send	Receive
Wired LAN	13095779 Bytes (70094 Packets)	75249239 Bytes (1364832 Packets)
Wired WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)
Wireless LAN	104332977 Bytes (1302176 Packets)	0 Bytes (0 Packets)
Wireless WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)

# Technical Specifications

ORing M2M Model	IGMG-P83244GC+-D4G
<b>Physical Ports</b>	
10/100/1000 Base-T(X) Ports in RJ45 Auto MDI/MDIX	8
10/100/1000Base-X SFP	4(combo)
SIM card slot	2
<b>Cellular interface</b>	
Cellular Standard	GSM / GPRS / EGPRS / EDGE / WCDMA / HSDPA / HSUPA/HSPA+/LTE
Band options	<b>America(US)</b> LTE: 700/1700/2100/ MHz UMTS/HSDPA/HSUPA/HSPA+/DC-HSPA+: 800/850/1900/2100 MHz GSM/GPRS/EDGE: 850/900/1800/1900 MHz <b>Europe(EU)</b> LTE: 800/900/1800/2100/2600 MHz UMTS/HSDPA/HSUPA/HSPA+/DC-HSPA+: 900/2100 MHz GSM/GPRS/EDGE: 900/1800/1900 MHz
Antenna Connector (Reverse SMA Female)	-
Antenna Connector (SMA Female)	1
<b>Serial Ports</b>	
Connector	Terminal Block x 1 (Port 1), DB9 male x 1 (Port 2)
Operation Mode	Port 1 : RS-422/RS-485(2W/4W), Which can be configured by utility Port 2 : RS-232/RS-422/RS-485(2W/4W). Which can be configured by utility
Serial Baud Rate	110 bps to 921.6 Kbps
Data Bits	7, 8
Parity	odd, even, none, mark, space
Stop Bits	1, 1.5, 2
Serial signals	RS-232 : TxD, RxD, DCD, RTS, CTS, DSR, DTR, RI, GND RS-422 : TX+, TX-, RX+, RX-, GND RS-485 (2W): D+, D- RS-485 (4W): TX+, TX-, RX+, RX-, GND
<b>LED Indicators</b>	
Power indicator	3 x LEDs, PWR 1, 2, PoE : Green On: Power is on
10/100/1000Base-T(X) RJ45 port indicator	2 x LEDs, LNK/ACT: Green for port LNK/ACT Speed: Amber for port Link at 100Mbps Off for port Link at 1000/10Mbps
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	Green On: in active
Fault	Power failure or port disconnected
Serial TX/RX LED	Red : Receiving data Green : Transmitting data
Power indicator	3 x LEDs, PWR 1, 2, PoE : Green On: Power is on
<b>Power</b>	
Power Input	Dual DC inputs. 12-48VDC on 6-pin terminal block
Power consumption (Typ.)	12 Watts
Overload current protection	Present
Reverse polarity protection	Present
<b>Physical Characteristic</b>	
Enclosure	IP-30
Dimension (W x D x H)	116.4mm W x 170mm D x 154mm H (4.6" W x 6.7" D x 6.1" H)
Weight (g)	2400 g
<b>Environmental</b>	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 70°C (-40 to 158°F)
Operating Humidity	5% to 95% Non-condensing
<b>Regulatory Approvals</b>	
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	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
<b>Warranty</b>	5 years

## Compliance

### FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

RF exposure warning: The equipment complies with RF exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment. This device should be operated with minimum distance 20cm between the device and all persons. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

### Industry Canada Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

*Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

Industry Canada - Class B This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

*Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie.*

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

*L'opération est soumise aux deux conditions suivantes: (1) cet appareil ne peut causer d'interférences, et (2) cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer fonctionnement du dispositif.*

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

*Afin de réduire les interférences radio potentielles pour les autres utilisateurs, le type d'antenne et son gain doivent être choisis que la puissance isotrope rayonnée équivalente (PIRE) est pas plus que celle promise pour une communication réussie*

RF exposure warning: The equipment complies with RF exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

*Avertissement d'exposition RF: L'équipement est conforme aux limites d'exposition aux RF établies pour un incontrôlés environnement. L'antenne (s) utilisée pour ce transmetteur ne doit pas être co-localisés ou fonctionner en conjonction avec toute autre antenne ou transmetteur.*