IMG-W6121+-M12

Industrial Cellular M2M Gateway with IEEE802.11 a/b/g/n

User Manual

Version 1.1

January, 2015

www.oring-networking.com

ORing Industrial Networking Corp.

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 23148, Taiwan (R.O.C.)
Tel: +886-2-2218-1066 // Fax: +886-2-2218-1014
Website: www.oring-networking.com

Technical Support
E-mail: support@oring-networking.com

Sales Contact
E-mail: sales@oring-networking.com (Headquarters)
sales@oring-networking.com.cn (China)

Tables of Content

Getting Started..1
1.1 About the IMG-W6121+-3G/4G-M12 1
1.2 Software Features 1
1.3 Hardware Features..1

Hardware Overview 2
2.1 Bottom Panel 2
2.1.1 Ports and Connectors 2
2.1.2 Front Panel LEDs 2
2.2 Top Panel 3

Hardware Installation 4
3.1 Wall Mounting 5
3.2 Pole Mounting..7

Cables and Antenna 9
4.1 Ethernet Pin Definition 9
4.2 Serial Port Pin Definition 9
4.3 Wireless Antenna..10
4.4 Cellular Antenna 10

Management 11
5.1 Network Connection 11
5.2 Configuration...12
5.2.1 Basic Setting...12
WAN 12
LAN 15
DHCP...16
DHCP Client List..18
Wireless LAN 18
Serial Setting 23
Remote Management 23
Service Mode...25
TCP Server Mode 26
TCP Client Mode..27
UDP Client Mode 28
DDNS 29
Date & Time...30
5.2.2 Networking Setting..30
Wireless Setting...30
Advanced 30
MAC Filter..33

NAT Setting 34
Virtual Server 34
DMZ 35
NAT Setting – UPnP 35
Firewall Setting 36
IP Filter 36
MAC Filter 37
Custom Rules 37
Vpn Setting 38
Open Vpn 38
Routing Setting 41
PPTP VPN 42
PPTP Client 43
IPSec VPN 45
VRRP 45
Routing Protocol 47
Routing Topography 49
Load Balance Rule 50
5.2.3 System Tools 50
Login Setting 50
M2M Restart 51
Firmware Upgrade 52
Save/Restore Configurations 52
Miscellaneous 53
Event Warning 54
E-mail 55
SMS 57
5.2.4 System Status 58
System Info 58
System Log 59
Traffic Statistics 59
Wireless Link List 60
Technical Specifications 61
Compliance 63

Getting Started

1.1 About the IMG-W6121+-3G/4G-M12

The IMG-W6121+-3G/4G-M12 is an innovative IEEE802.11 a/b/g/n WLAN access point VPN gateway with two RS-232 serial ports and one 10/100/1000Base-T(X) port. The combination of two serial ports and one Ethernet port allows the device to connect to serial devices and networked devices at the same time. The device can be configured to connect to the Internet by dialing up the 3.5G/4G cellular modem. Therefore, it can be used in various applications through WLAN connections. With an IP-67 waterproof casing and PoE support, IMG-W6121+-3G-M12 can be deployed in harsh outdoor environments where power supply is difficult to come by. Furthermore, the device can also transfer SSL encryption data to five host PCs simultaneously for backup purposes.

1.2 Software Features

- High-speed air connectivity for up to 300Mbps
- High security with support for WEP/WPA/WPA-PSK(TKIP,AES)/ WPA2/WPA2-PSK(TKIP,AES)/802.1X/RADIUS authentication
- 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
- Event warning by Syslog, e-mail, and SNMP trap

1.3 Hardware Features

- 1 x 10/100 /1000Base–T(X) PoE port (P.D.)
- 3.5G HSUDPA or 4G LTE modem included
- 2 x RS-232 serial ports
- IP-67 grade waterproof casing
- Casing: IP-67
- Operating temperature: -25 to 70° C
- Storage temperature: -40 to 85° C
- Operating humidity: 5% to 95%, non-condensing
- Dimensions: 250 (W) x 220 (D) x 87 (H) mm (9.84 x 8.66 x 3.4 inch)

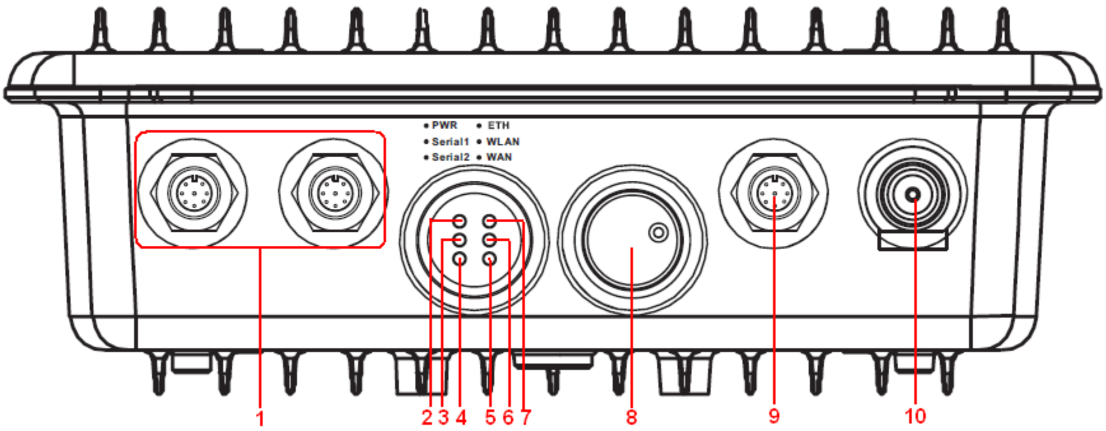
Hardware Overview

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
10/100/1000Base-T(X) Ethernet ports with M12 connectors	1 x 10/100/1000 Base-T(X) port supporting auto-negotiation.
SIM card slot	1 x SIM card slot
RS232 serial port	2 x serial port



1. Serial ports
2. Power LED
3. Serial port 1 status LED
4. Serial port 2 status LED
5. WAN status LED
6. WLAN status LED
7. Ethernet port status LED
8. SIM card
9. Ethernet port
10. 3G/4G antenna connector

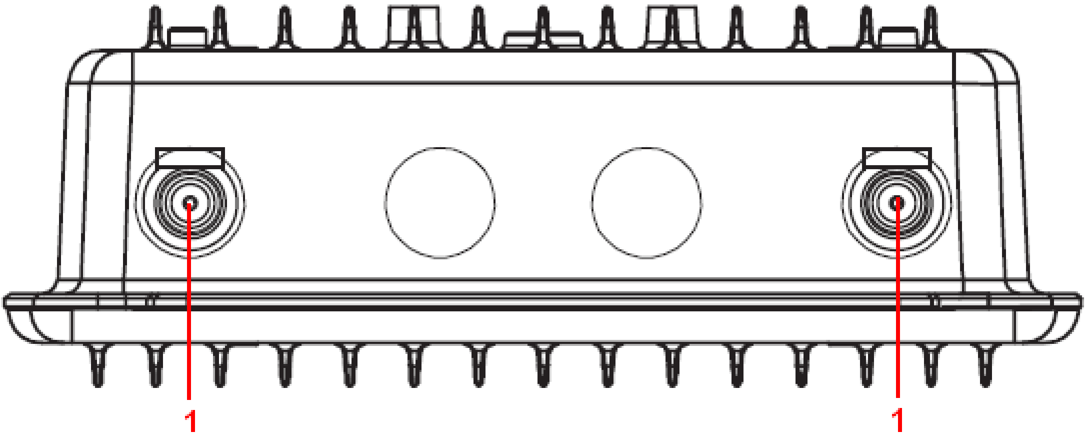
2.1.2 Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	Power is supplied over Ethernet
Serial 1/2	Green	Blinking	Transmitting data
ETH	Green	On	Port is linked

		Blinking	Transmitting data
WLAN	Green	On	WLAN is activated
		Blinking	Transmitting data
WAN	Green	On	Modem is connected

2.2 Top Panel

On the top panel sits a SIM card slot and a cellular antenna connector, as show as below.



1. Wi-Fi antenna connector

Hardware Installation

Before installing the device, make sure you have all of the package contents available and a PC with Microsoft Internet Explorer 6.0 or later, for using web-based system management tools.

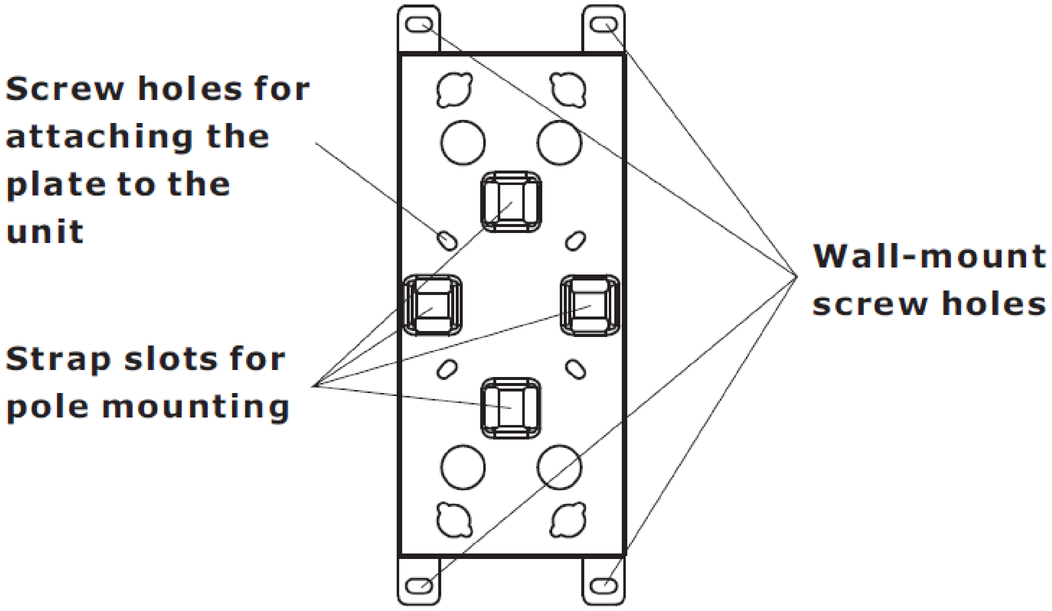
⚠ When installed outdoors, make sure the connectors on the panel are facing down to prevent water intrusion.

⚠ Do not remove the water-proof casing, and avoid touching or moving the device when the antennas are transmitting or receiving.

⚠ When installing the device, make sure to keep the radiating at a minimum distance of 20 cm (7.9 inches) from all persons to minimize the potential for human contact during normal operation.

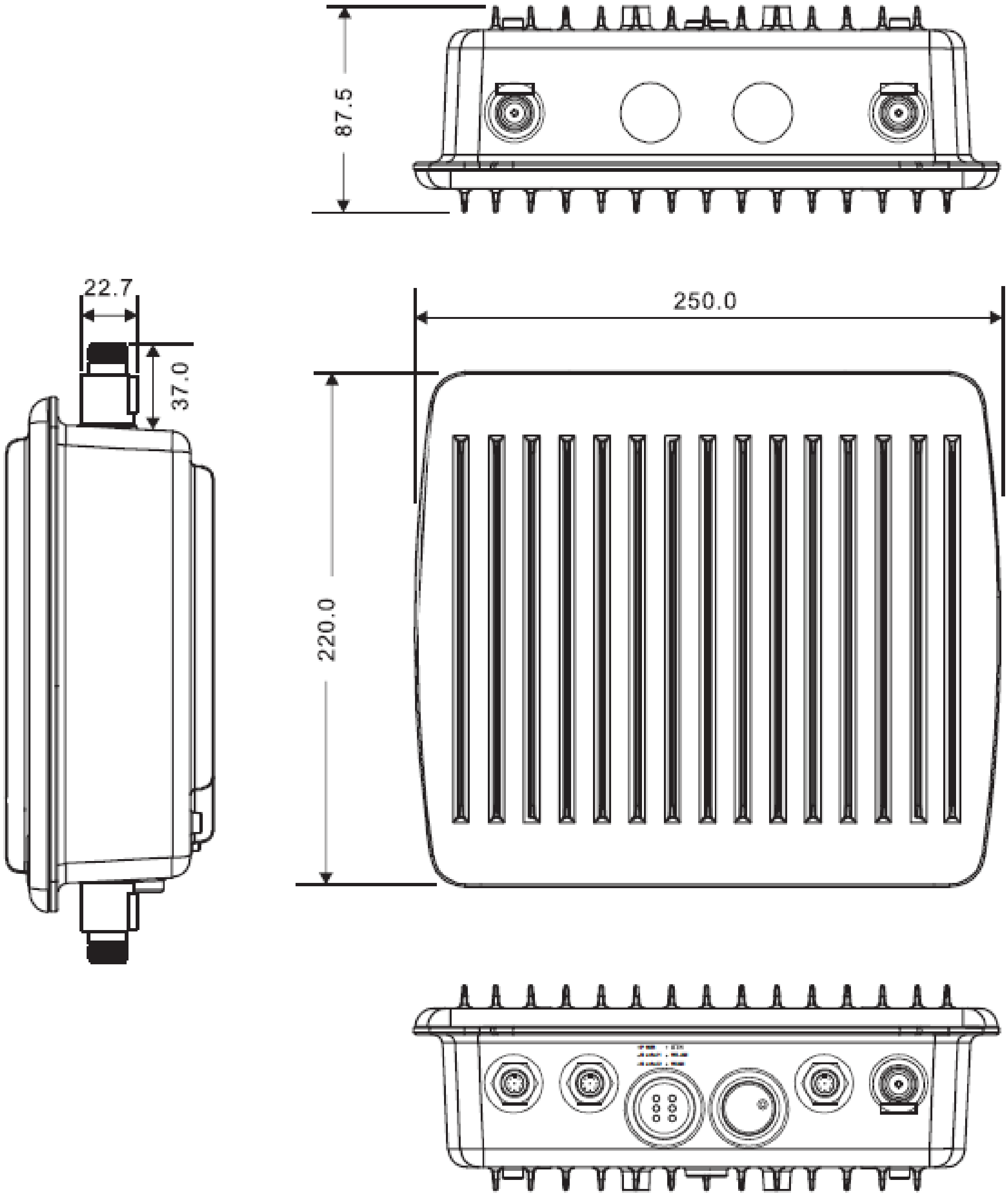
⚠ Do not operate the device near unshielded blasting caps or in an otherwise explosive environment unless the device has been modified for such use by qualified personnel.

The device can be fixed to a pole or the wall using the supplied mounting plate. Make sure the connectors on the bottom panel are facing down when installing to prevent water intrusion.


Screw holes for attaching the plate to the unit
Strap slots for pole mounting
Wall-mount screw holes

Mounting plate

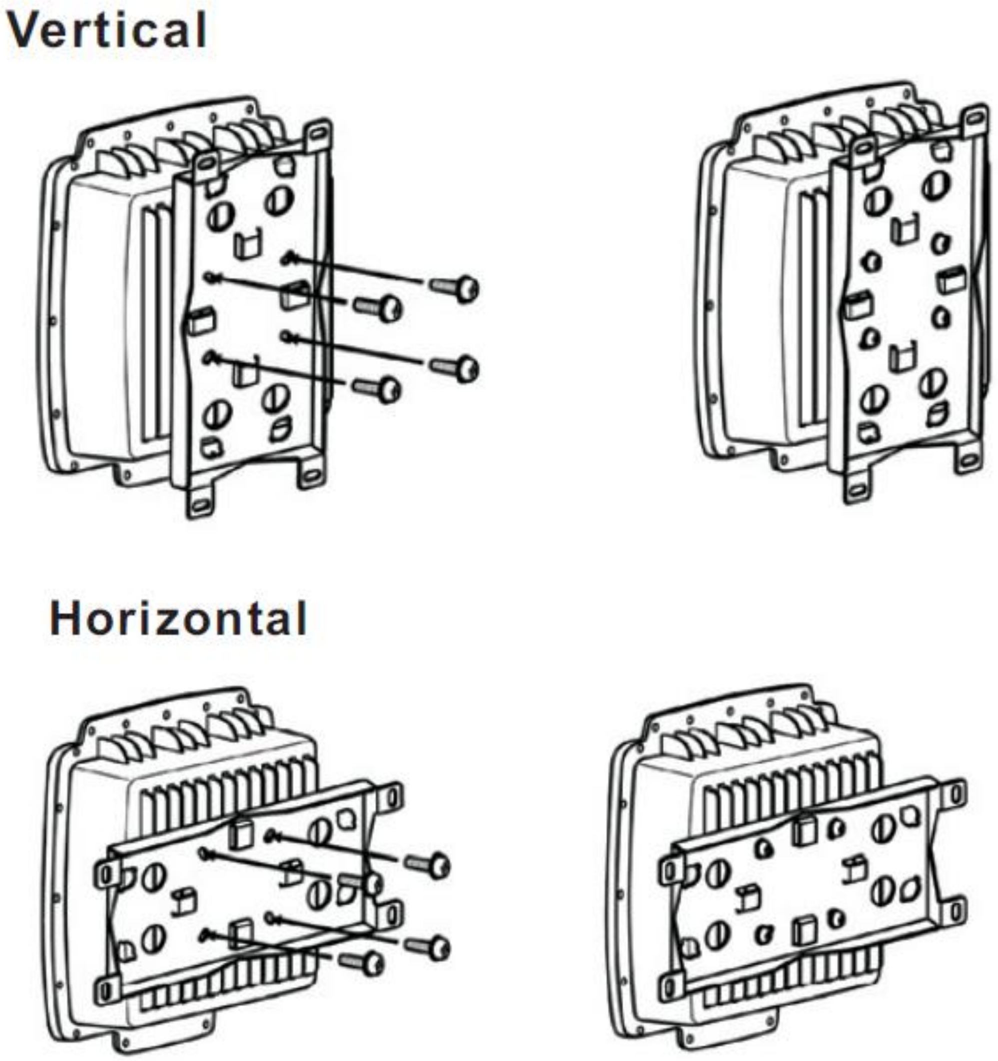
3.1 Wall Mounting



Wall-mount Measurements (Unit = mm)

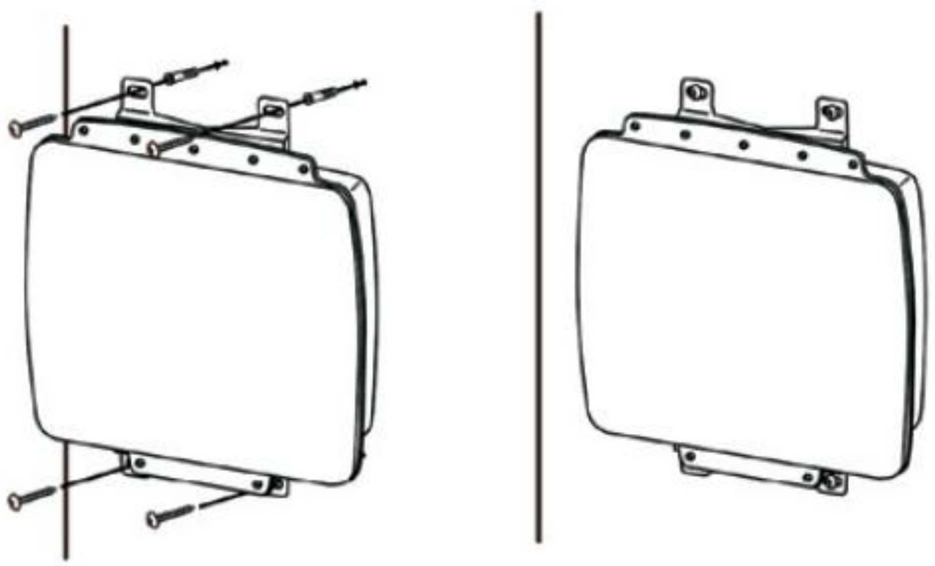
Follow the steps below to install the device to the wall.

Step 1: Attach the mounting plate to the back of the device using four screws. The plate can be attached vertically or horizontally to the device based on the space available.



Step 2: Hold the device upright against the wall

Step 3: Insert four screws through the large opening of the keyhole-shaped apertures at the top and bottom of the plate and fasten the screw to the wall with a screwdriver.

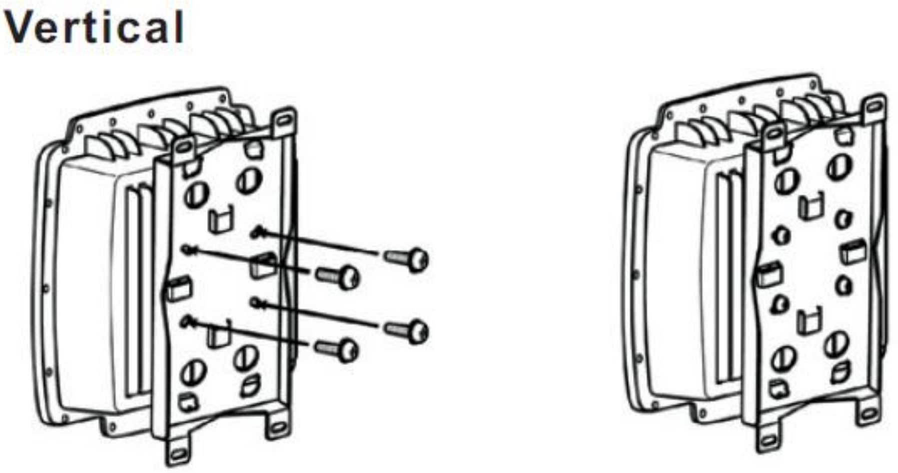


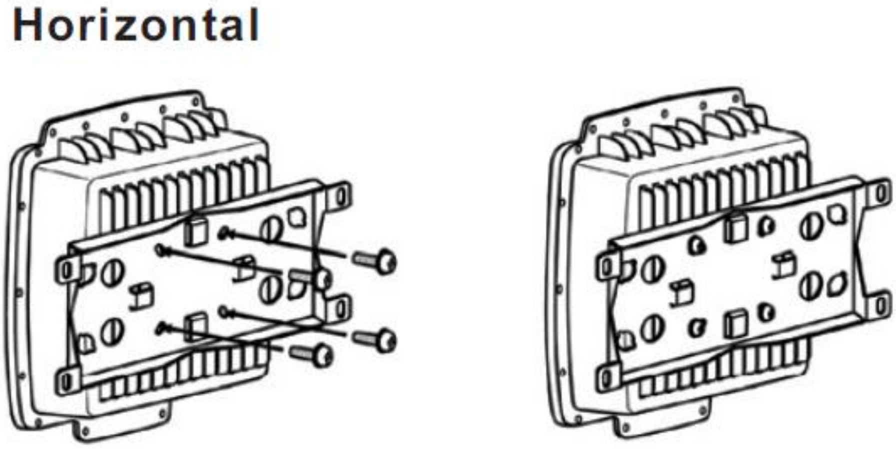
Instead of screwing the screws in all the way, it is advised to leave a space of about 2mm to allow room for sliding the device between the wall and the screws.

3.2 Pole Mounting

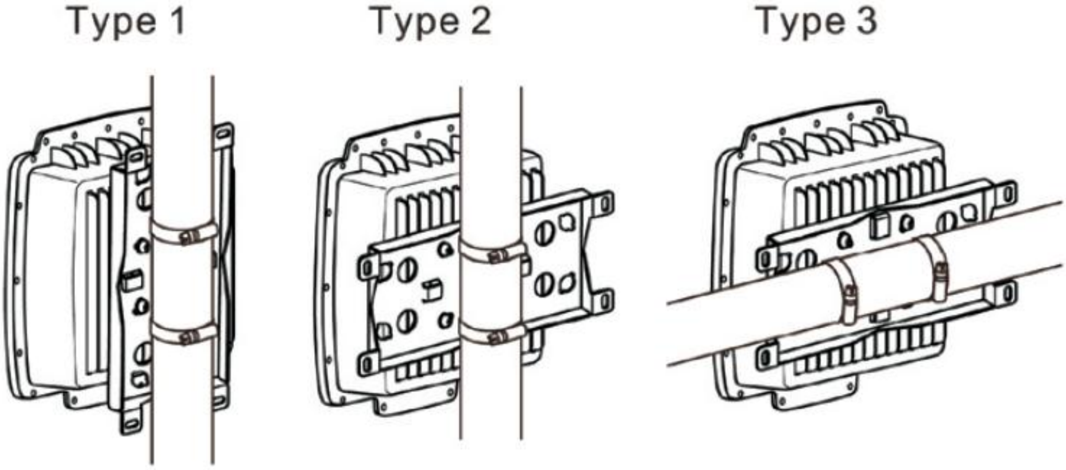
You can mount the device to a pole using adjustable steel band straps included in the kit. When installing the device to a pole:

Step 1: Attach the mounting plate to the back of the device using four screws. The plate can be attached vertically or horizontally to the device based on the space available.





Step 2: Thread the two supplied metal mounting straps through the large slots on the mounting plate and then put the straps around the pole.

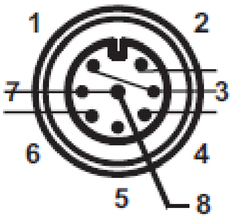


Cables and Antenna

4.1 Ethernet Pin Definition

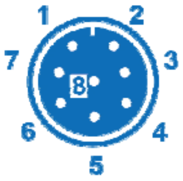
The device has one 10/100/1000 Base-T(X) Ethernet port. According to the link type, the device uses CAT 3, 4, 5, 5e, UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable	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,6	UTP 100 m (328 ft)	RJ45



PIN	Definition
1	BI_DC+
2	BI_DD+
3	BI_DD-
4	BI_DA-
5	BI_DB+
6	BI_DA+
7	BI_DC-
8	BI_DB-

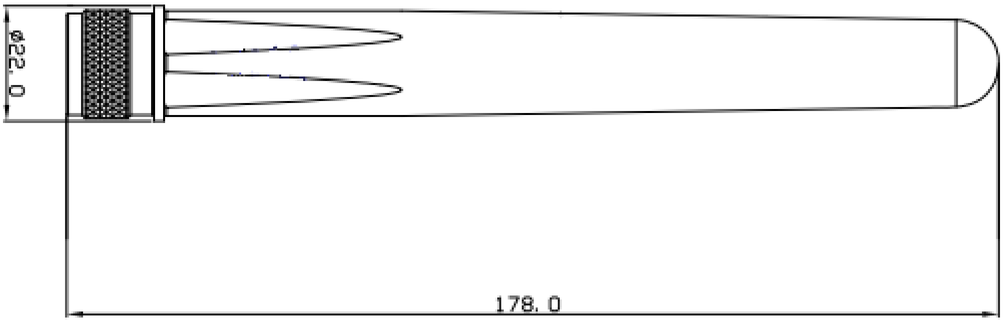
4.2 Serial Port Pin Definition



M12 Pin Definition	
Pin No.	Description
#1	RXD
#2	DCD
#3	RTS
#4	DSR
#5	GND
#6	DTR
#7	TXD
#8	CTS

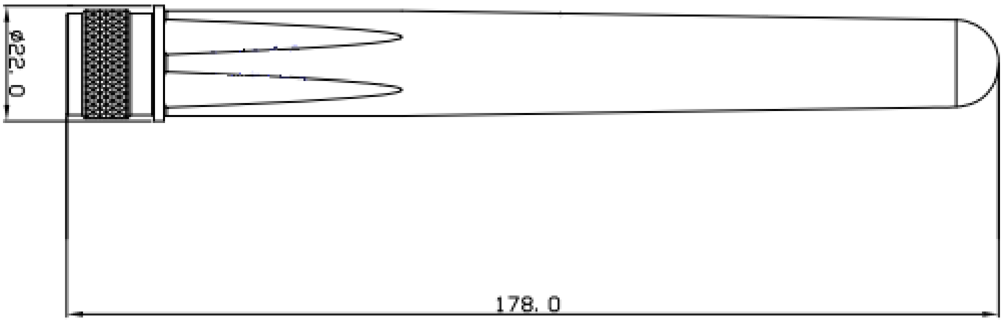
4.3 Wireless Antenna

The device provides two N-type female connectors for Wi-Fi antennas. You can also use external RF cables and antennas with the connectors.



4.4 Cellular Antenna

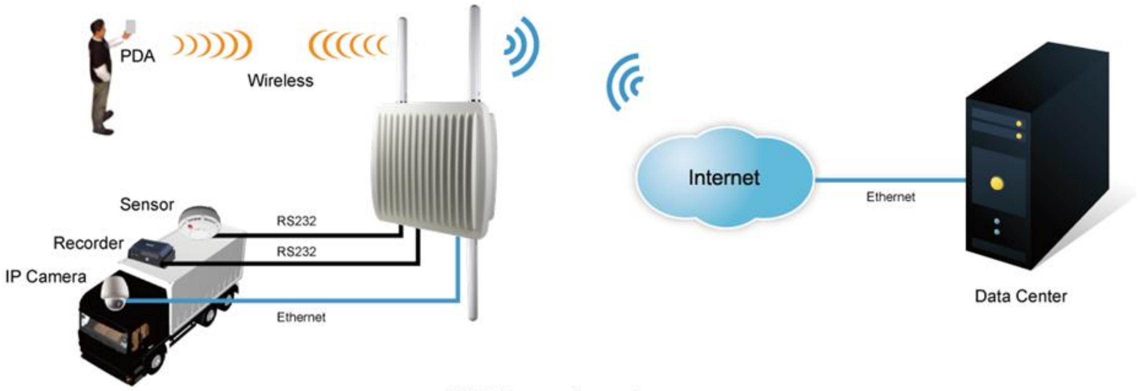
The device provides one cellular connector for 3G and 4G antennas. External RF cables and antennas can also be used with the connector.



Management

5.1 Network Connection

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



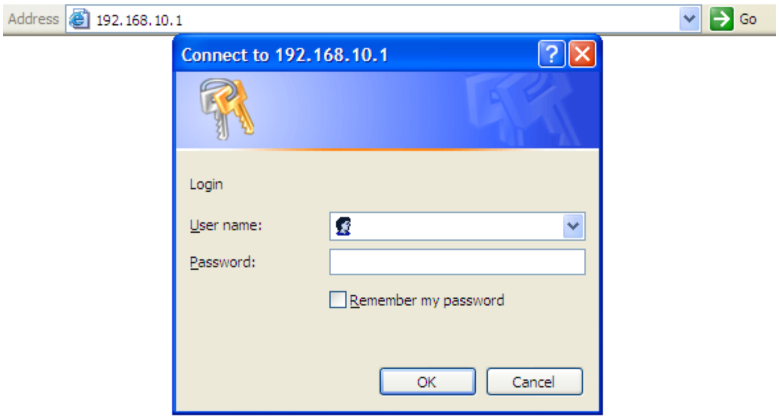
M2M Gateway Connection

Please Follow the steps below to install and connect the gateway to PCs:

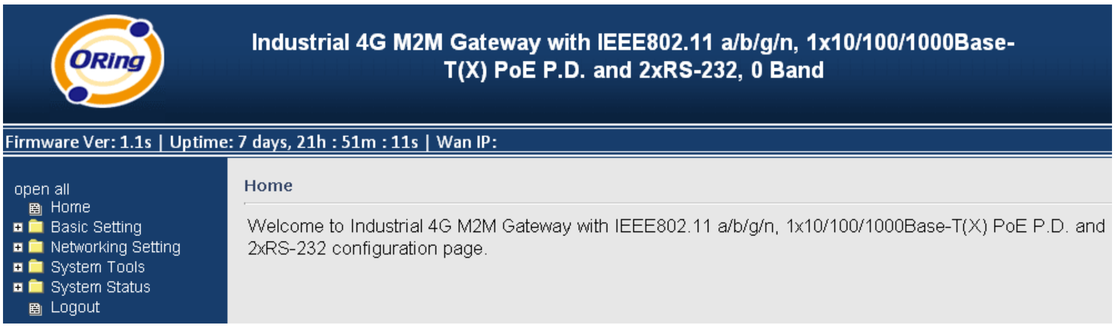
Step 1: Select a power source. The device is powered via the PoE (Power over Ethernet) port, so there is no need for additional power cords..

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 gateway 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 VPN 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 device) in the address box to access the web page. 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.



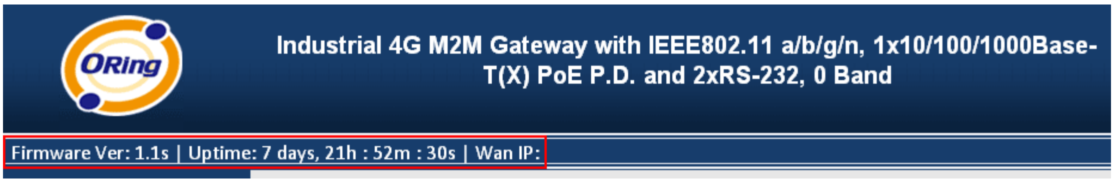
After you log in successfully, a Web interface will appear, as shown below. On the left hand side of the interface is a list of functions where you can configure the settings. The details of the configurations will be shown on the right screen.


ORing
Industrial 4G M2M Gateway with IEEE802.11 a/b/g/n, 1x10/100/1000Base-T(X) PoE P.D. and 2xRS-232, 0 Band
Firmware Ver: 1.1s | Uptime: 7 days, 21h : 51m : 11s | Wan IP:
open all
Home
Basic Setting
Networking Setting
System Tools
System Status
Logout
Home

Welcome to Industrial 4G M2M Gateway with IEEE802.11 a/b/g/n, 1x10/100/1000Base-T(X) PoE P.D. and 2xRS-232 configuration page.

5.2 Configuration

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


ORing
Industrial 4G M2M Gateway with IEEE802.11 a/b/g/n, 1x10/100/1000Base-T(X) PoE P.D. and 2xRS-232, 0 Band
Firmware Ver: 1.1s | Uptime: 7 days, 21h : 52m : 30s | Wan IP:

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

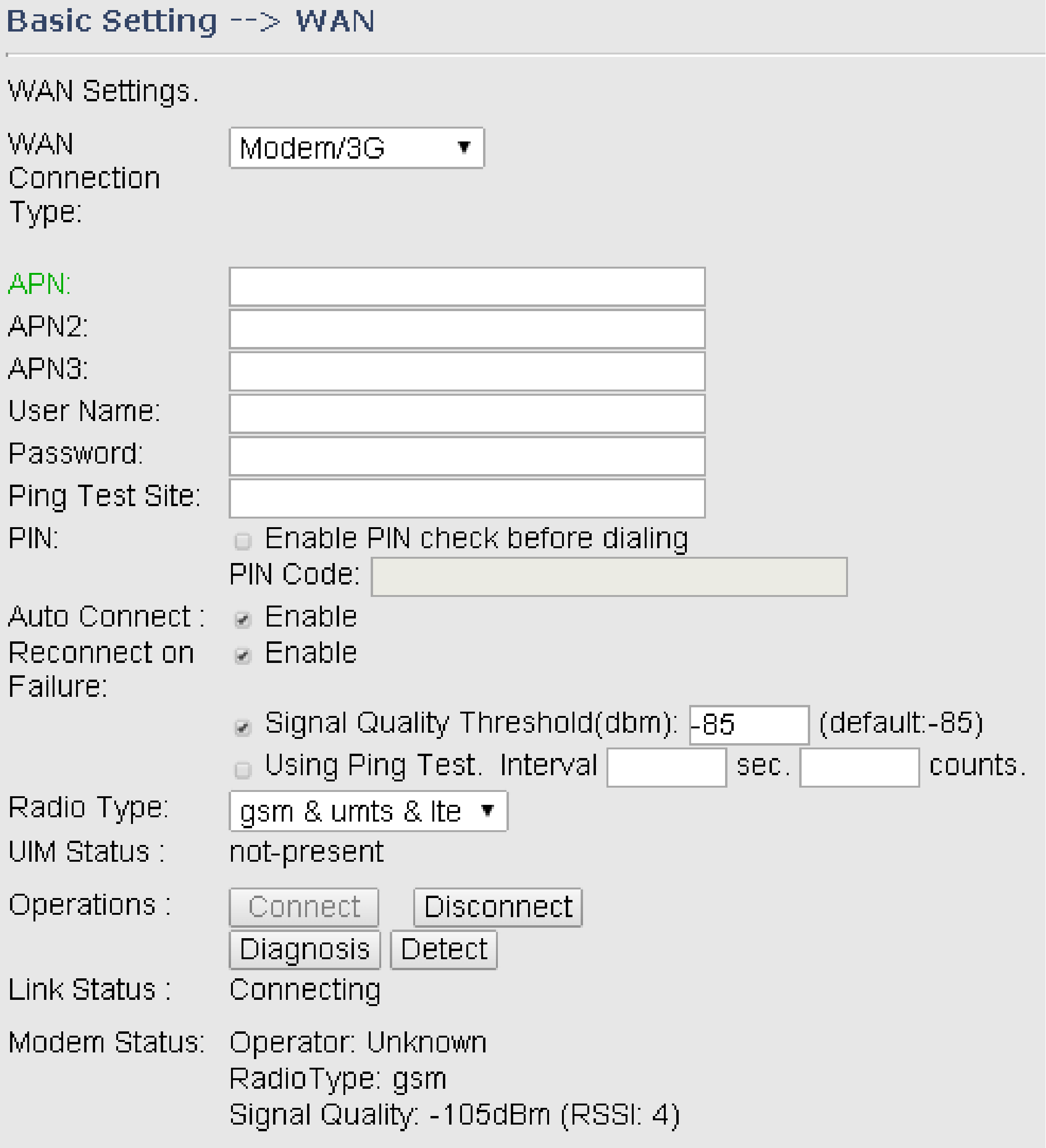
5.2.1 Basic Setting

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

WAN

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

WAN Connection Type as Modem/3G



Basic Setting --> WAN

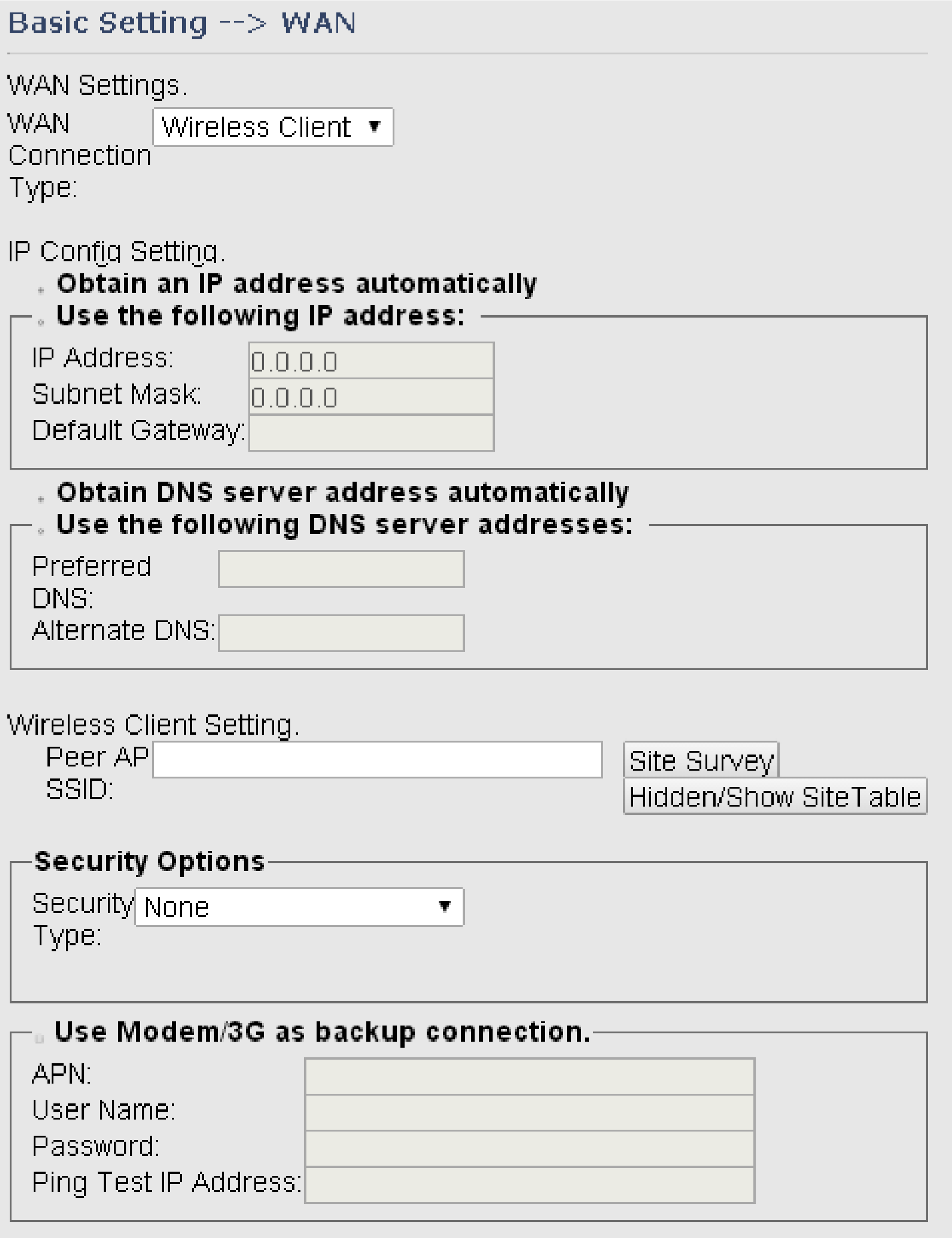
WAN Settings.

WAN Connection Type:	Modem/3G ▾
APN:	
APN2:	
APN3:	
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): -85 (default:-85) □ Using Ping Test. Interval sec. counts.
Radio Type:	gsm & umts & lte ▾
UIM Status :	not-present
Operations :	Connect Disconnect Diagnosis Detect
Link Status :	Connecting
Modem Status:	Operator: Unknown RadioType: gsm Signal Quality: -105dBm (RSSI: 4)

Label	Description
APN	Enter the APN value (optional)
User Name	Enter the user name provided by your ISP
Password	Enter the password provided by your ISP
Ping Test Site	Type a link in the field to test your Internet connection
PIN	Enter a PIN code if you want to perform PIN check
Auto Connect	Check to start connections when the gateway boots up
Reconnect on Failure	Check to allow for reconnection when links fail

Radio Type	Select a type of radio from the list which includes GSM, UMTS, and LTE
UIM Status	Shows the status of SIM card
Operations	Click **Connect** to start modem/3G connections or **Disconnect** to shut down connections
Link Status	Shows the status of connections
Modem Status	Shows information about the modem

WAN Connection Type as Wireless Client



Basic Setting --> WAN

WAN Settings.

WAN Connection Type: Wireless Client ▼

IP Config Setting.

○ Obtain an IP address automatically

○ Use the following IP address:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway:

○ Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS:

Alternate DNS:

Wireless Client Setting.

Peer AP SSID:

Security Options

Security Type: None ▼

□ Use Modem/3G as backup connection.

APN:

User Name:

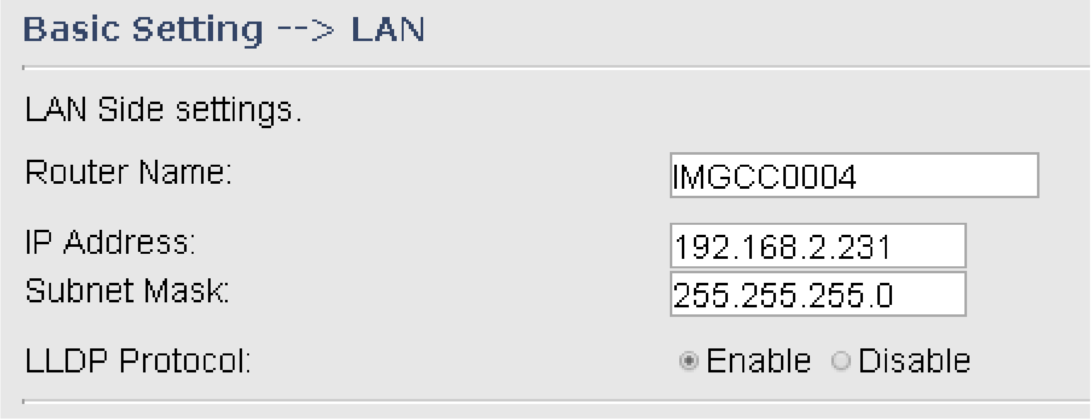
Password:

Ping Test IP Address:

Label	Description
Obtain an IP address automatically	Select this option if you want the IP address of the WAN port to be assigned automatically by the DHCP server in your network.
Use the following IP address	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.
Obtain DNS server address automatically	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.
Use the following DNS server addresses	Specifies a DNS server address manually. You can enter two addresses as the primary and secondary options.
Peer AP SSID	Enter the SSID of the AP you want to connect as a client
Site Survey	Click the button to browse available sites if you do not know the SSID. A list of available sites will be displayed.
Security Options	Select the security type used by the client you want to connect. You can choose WEP which will encrypt data transmitted on the WLAN or WPA-PSK/WPA2-PSK which uses a pre-shared key for authentication.
Use Modem/3G as backup connection	Enable this option if you want to use modem/3G as a backup connection when main connection is lost. Enter your account username and password in the corresponding fields. Type a website address such as www.google.com in Ping Test Site to use it to check if the connection is alive or lost.

LAN

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



Basic Setting --> LAN

LAN Side settings.

Router Name: IMGCC0004

IP Address: 192.168.2.231

Subnet Mask: 255.255.255.0

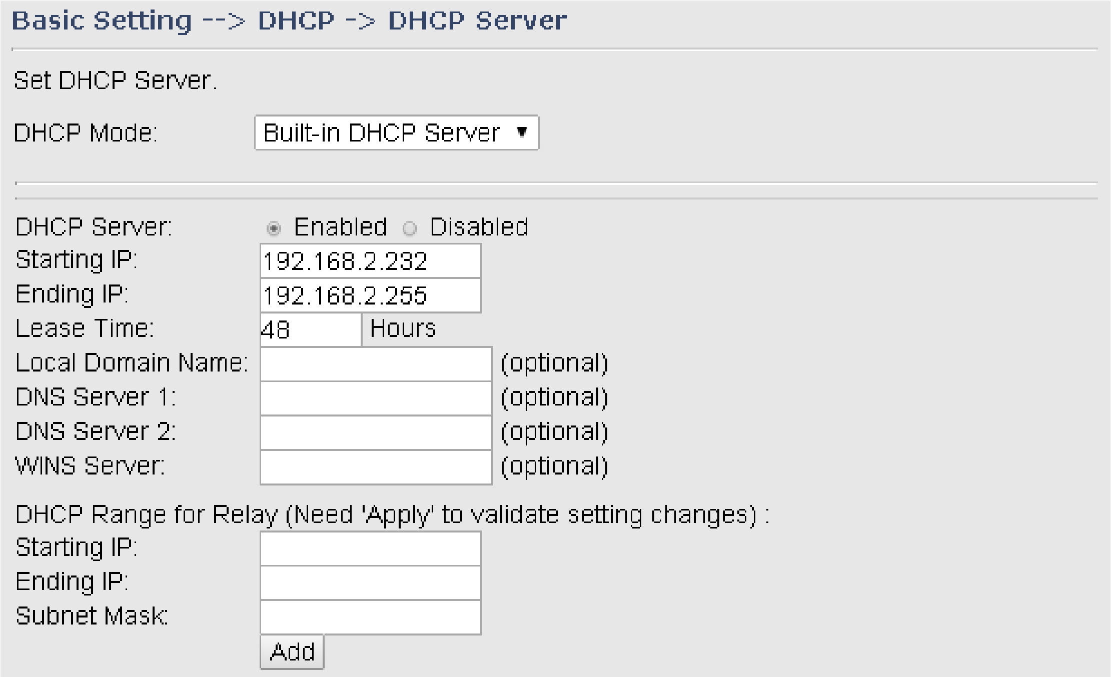
LLDP Protocol: ● Enable ○ Disable

Label	Description
Gateway Name	Enter the name of your gateway
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**
LLDP Protocol	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.

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 gateway 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 gateway 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 gateway, 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.



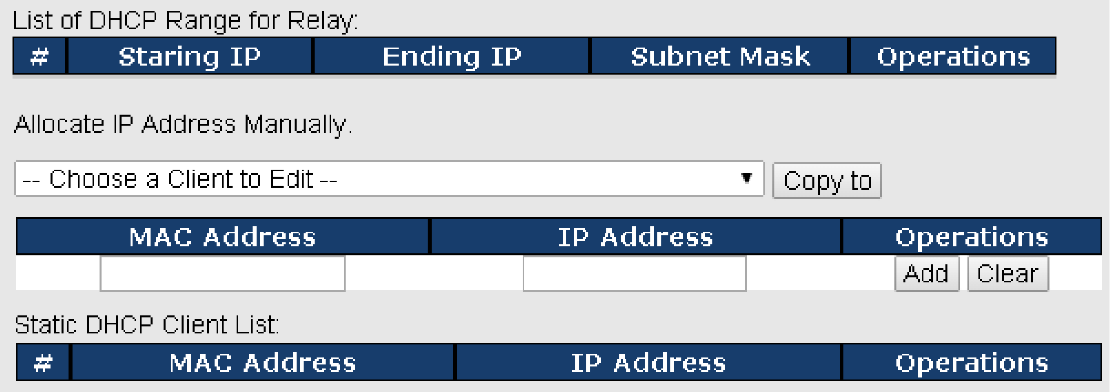
Basic Setting --> DHCP -> DHCP Server

Set DHCP Server.

DHCP Mode: Built-in DHCP Server ▼

DHCP Server: ● Enabled ○ Disabled
Starting IP: 192.168.2.232
Ending IP: 192.168.2.255
Lease Time: 48 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:

#	Staring IP	Ending IP	Subnet Mask	Operations

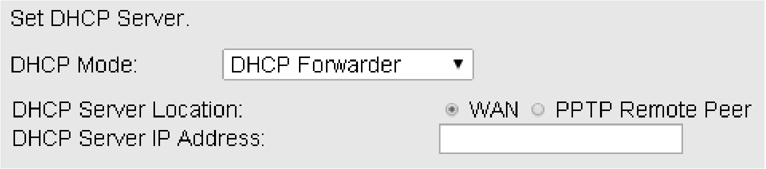
Allocate IP Address Manually:

-- Choose a Client to Edit -- ▾ Copy to

MAC Address	IP Address	Operations
		Add Clear

Static DHCP Client List:

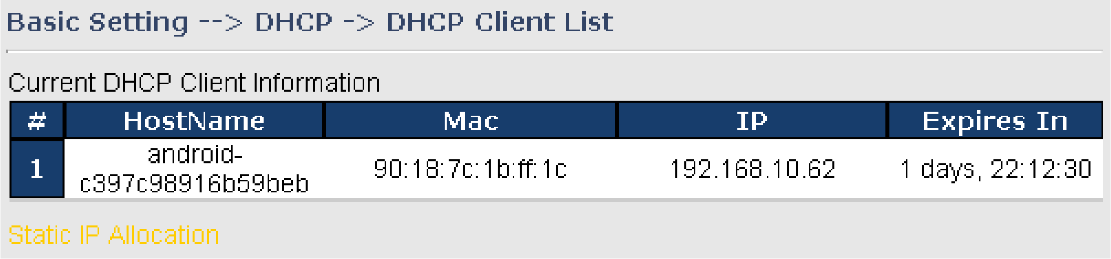
#	MAC Address	IP Address	Operations

Label	Description
DHCP Mode	Available options include **Built-in DHCP Server** and **DHCP Forwarder**. **Built-in DHCP Server** will enable the gateway to automatically assign an IP address to a computer on the LAN. **DHCP Forwarder** will forward DHCP messages to a server on the Internet to handle DHCP requests. If you choose **DHCP Forwarder**, enter a DHCP server IP address.  Set DHCP Server: DHCP Mode: DHCP Forwarder ▾ DHCP Server Location: ● WAN ○ PPTP Remote Peer DHCP Server IP Address:
DHCP Server	Enables or disables the DHCP server function. The default setting is **Enabled**. The Starting and Ending DHCP addresses should be in the same subnet as the LAN IP address of the VPN firewall.
Starting IP	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.
Ending IP	Specifies the last of the contiguous addresses in the IP address pool.
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). The DHCP will assign the entered domain to DHCP clients.
DNS Server 1&2	Enter the IP address for the DNS server (optional)

WINS Server	Specifies the IP address of a local Windows NetBios Server if one is present in your network. (optional)
DHCP Range for Relay	Configure the DHCP range for relay by inputting a starting and ending IP address and a subnet mask.
Starting IP	The starting IP for the DHCP relay range
Ending IP	The ending IP for the DHCP relay range
Subnet Mask	Enter a Subnet mask for the DHCP relay range
List of DHCP Range for Relay	Shows all IP addresses for the DHCP relay range
Allocate IP Address Manually	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 gateway and add it to Static DHCP Client List.
MAC Address	The MAC addresses of the computer.
IP Address	The IP address to be related to the MAC address.
Static DHCP Client List	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.



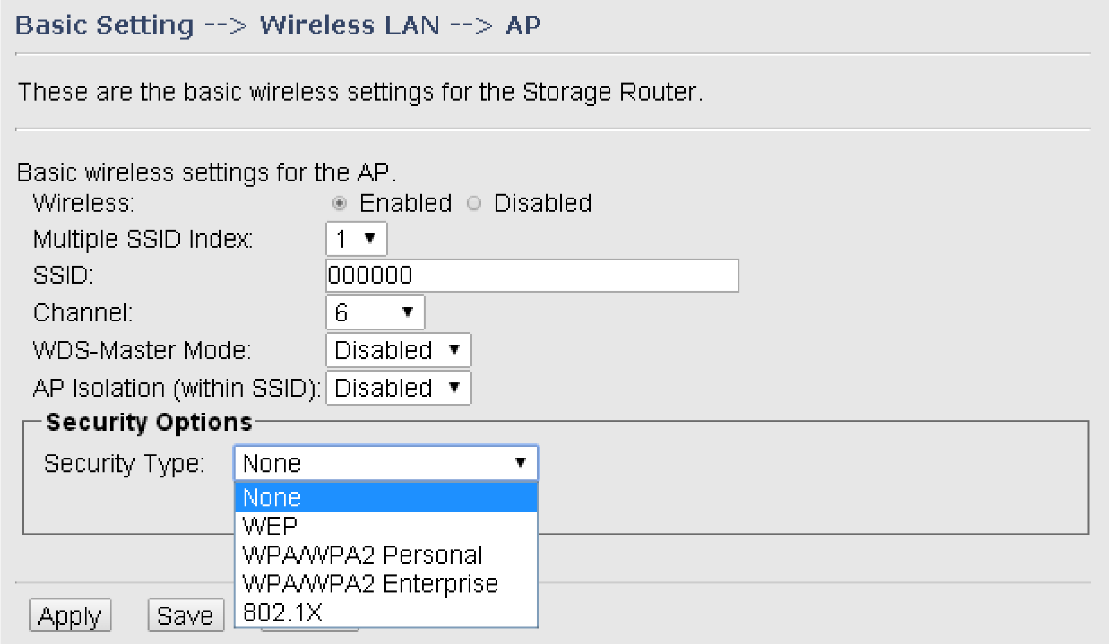
Basic Setting --> DHCP -> DHCP Client List

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

Wireless LAN

You can set the device to work in AP mode. This is the most common mode for all wireless APs. In this mode, the AP will act as a central connection point which other wireless clients can connect to.



Basic Setting --> Wireless LAN --> AP

These are the basic wireless settings for the Storage Router.

Basic wireless settings for the AP.

Wireless: ● Enabled ○ Disabled

Multiple SSID Index: 1

SSID: 000000

Channel: 6

WDS-Master Mode: Disabled

AP Isolation (within SSID): Disabled

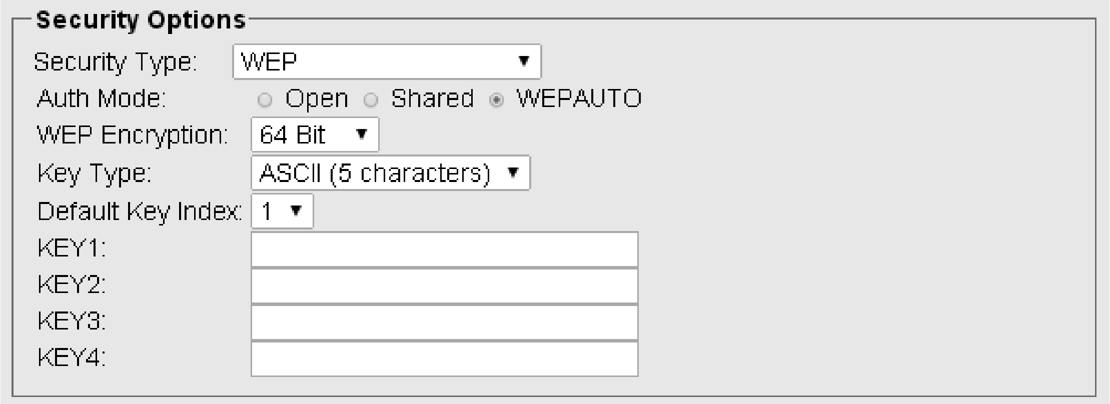
Security Options

Security Type: None

Label	Description
Multiple SSID index	The index of the SSID
SSID	SSID (Service Set Identifier) is a unique name that identifies a network. All devices on the network must be set with the same SSID in order to communicate with each other. Fill in a new SSID in this field if you do not want to use the default value.
Channel	Specify a channel to be used. **Channel 6** is the default channel. You can also select a new number from the dropdown list. All devices on the network must be set to use the same channel to communicate on the network.
WDS-Master Mode	A WDS master is the central control point for authenticating wireless clients, caching client key material, distributing MFP key material, reporting radio management information to an upstream network management station, and updating other APs participating in WDS. You can set the device as the WDS-master by selecting from the list.
AP Isolation (within SSID)	This function prevents devices connected to an AP from communicating directly with each other. This function is useful when many wireless clients request your network frequently.
Security options	You can choose the security type for your WLAN connection from the following options: **None**: no encryption

	WEP: WEP (Wired Equivalent Privacy) is a wireless security protocol for WLAN. WEP will encrypt data transmitted on the WLAN. **WPA/WPA2 Personal**: uses a pre-shared key for authentication. This pre-shared key is then dynamically sent between the AP and clients. Each authorized computer is given the same pass phrase. **WPA/WPA2 Enterprise**: this type includes all of the features of WPA/WPA2 Personal plus support for 802.1x RADIUS authentication. **802.1x**: authentication through a RADIUS server.

When you set security type as **WEP**, the following fields will appear to allow you to configure individual settings.



Security Options

Security Type: WEP

Auth Mode: ○ Open ○ Shared ● WEPAUTO

WEP Encryption: 64 Bit

Key Type: ASCII (5 characters)

Default Key Index: 1

KEY1:

KEY2:

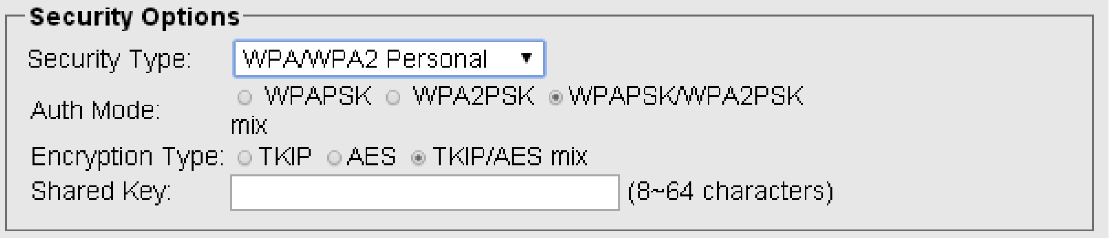
KEY3:

KEY4:

Label	Description
Auth Mode	Available values include **Open**, **Shared**, and **WEPAUTO**. When choosing **Open** or **Shared**, all of the clients must select the same authentication to associate this AP. If select **WEPAUTO**, the clients do not have to use the same **Open** or **Shared** authentication. They can choose any one to authenticate.
WEP Encryption	You can select **64 Bit** or **128 Bit**.
Key Type	Available values include **ASCII** and **Hex Key Type**. ASCII (American Standard Code for Information Interchange) is a code for representing English characters as numbers in the range from 0 to 127. Hex digits uses 0–9 to represent values zero to nine, and characters A-F to represent values ten to fifteen.

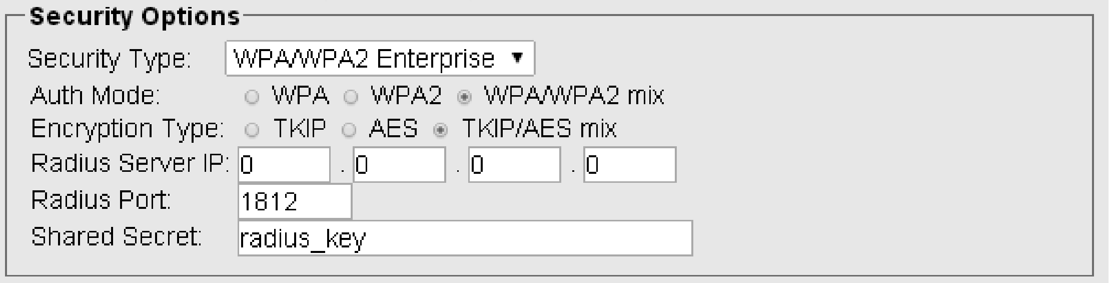
Default Key Index	Select one of the keys to be the active key
Key 1 to 4	You can input up to four encryption keys.

When you set security type as **WPA/WPA2-Personal**, the following fields will appear to allow you to configure individual settings.


Security Options
Security Type: WPA/WPA2 Personal ▼
Auth Mode: ○ WPAPSK ○ WPA2PSK ● WPAPSK/WPA2PSK mix
Encryption Type: ○ TKIP ○ AES ● TKIP/AES mix
Shared Key: (8~64 characters)

Label	Description
Auth Mode	Available values include **WPAPSK**, **WPA2PSK**, and **WPAPSK/WPA2PSK mix.** WPAPSK and WPA2PSK will encrypt the link without additional RADIUS server, only an access point and client station that supports WPA-PSK is required. For WPA/WPA2, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.
Encryption Type	Available values include **TKIP**, **AES**, and **TKIP/AES mix**. WPA-PSK uses TKIP encryption, and WPA2-PSK uses AES encryption. TKIP/AES provides the most reliable security, and is easiest to implement.
Shared Key	Enter a pass phrase in this field. The value must be within 8 to 64 characters

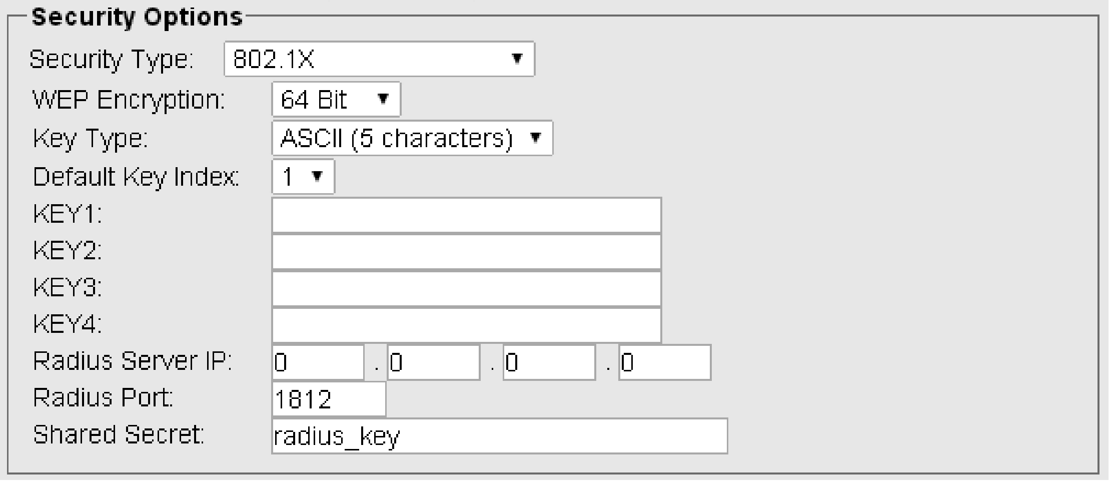
When you set security type as **WPA /WPA2 Enterprise**, the following screen will appear to allow you to configure individual settings.


Security Options
Security Type: WPA/WPA2 Enterprise ▼
Auth Mode: ○ WPA ○ WPA2 ● WPA/WPA2 mix
Encryption Type: ○ TKIP ○ AES ● TKIP/AES mix
Radius Server IP: 0 . 0 . 0 . 0
Radius Port: 1812
Shared Secret: radius_key

Label	Description
Auth Mode	Available values include **WPAPSK**, **WPA2PSK**, and

	WPAPSK/WPA2PSK mix. WPAPSK and WPA2PSK will encrypt the link without additional RADIUS server, only an access point and client station that supports WPA-PSK is required. For WPA/WPA2, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.
Encryption Type	Available values include **TKIP**, **AES**, and **TKIP/AES mix**. WPA-PSK uses TKIP encryption, and WPA2-PSK uses AES encryption. TKIP/AES provides the most reliable security, and is easiest to implement.
Radius Server IP	Enter the IP address of the RADIUS server
Radius Port	Enter the RADIUS port (default is 1812)
Shared Secret	Enter the RADIUS password or key.

When you set security type as **802.1x**, the following fields will appear to allow you to configure individual settings.



Security Options

Security Type: 802.1X

WEP Encryption: 64 Bit

Key Type: ASCII (5 characters)

Default Key Index: 1

KEY1:

KEY2:

KEY3:

KEY4:

Radius Server IP: 0 . 0 . 0 . 0

Radius Port: 1812

Shared Secret: radius_key

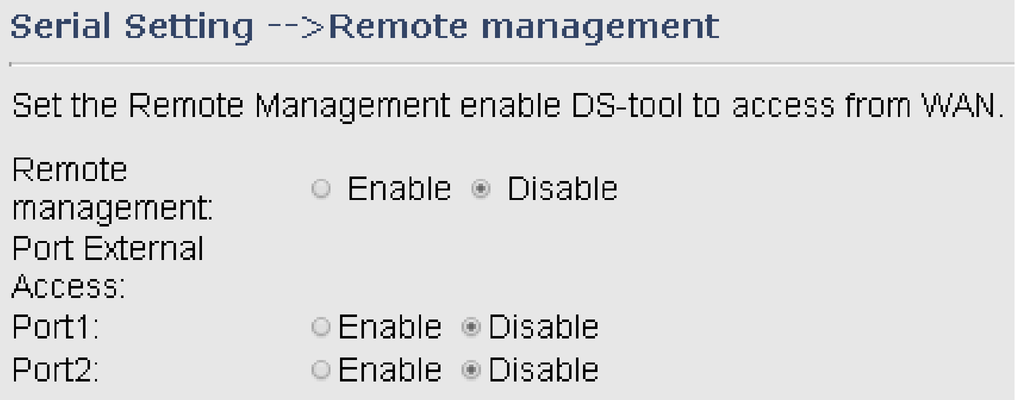
Label	Description
WEP Encryption	You can select **64 Bit** or **128 Bit**.
Key Type	Available values include **ASCII** and **Hex Key Type**. ASCII (American Standard Code for Information Interchange) is a code for representing English characters as numbers in the range from 0 to 127. Hex digits uses 0–9 to represent values zero to nine, and characters A-F to represent values ten to fifteen.
Default Key Index	Select one of the keys to be the active key
Key 1 to 4	Input up to four encryption keys
Radius Server IP	Enter the IP address of the RADIUS server

Radius Port	Enter the RADIUS port (default is **1812**)
Shared Secret	Enter the RADIUS password or key

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:

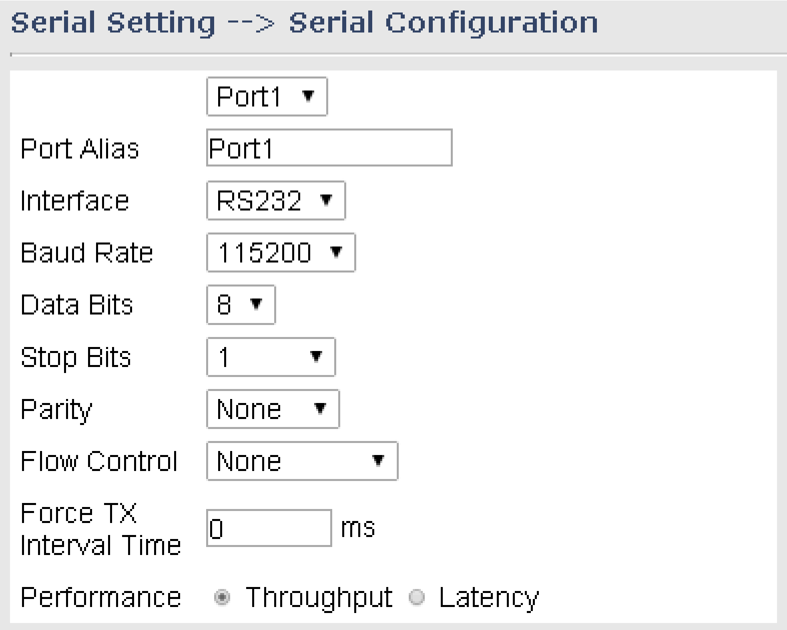
Port1: ○ Enable ● Disable

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: Port1

Interface: RS232 ▼

Baud Rate: 115200 ▼

Data Bits: 8 ▼

Stop Bits: 1 ▼

Parity: None ▼

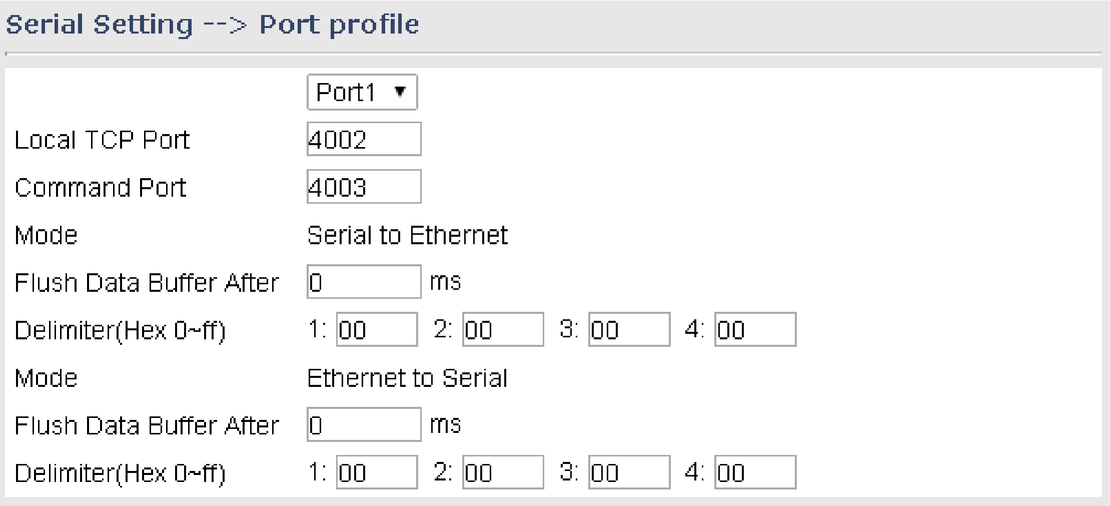
Flow Control: None ▼

Force TX Interval Time: 0 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 **RS-232**
Baud rate	Choose a baud rate in the range between 110 bps and 115200 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	Chose the method of detecting errors in transmission. Parity control bit modes include None, Odd, Even, Mark, and Space. **None** means parity checking is not performed and the parity bit is not transmitted. **Odd** 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. **Even** 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.
Flow Control	Choose **XOFF** to tell the computer to stop sending data or **XON** 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. **0** means disable. Factory default value is **0**.
Performance	**Throughput**: This mode is optimized for the highest transmission speed. **Latency**: This mode is optimized for the shortest response time.

Port Profile



Serial Setting --> Port profile

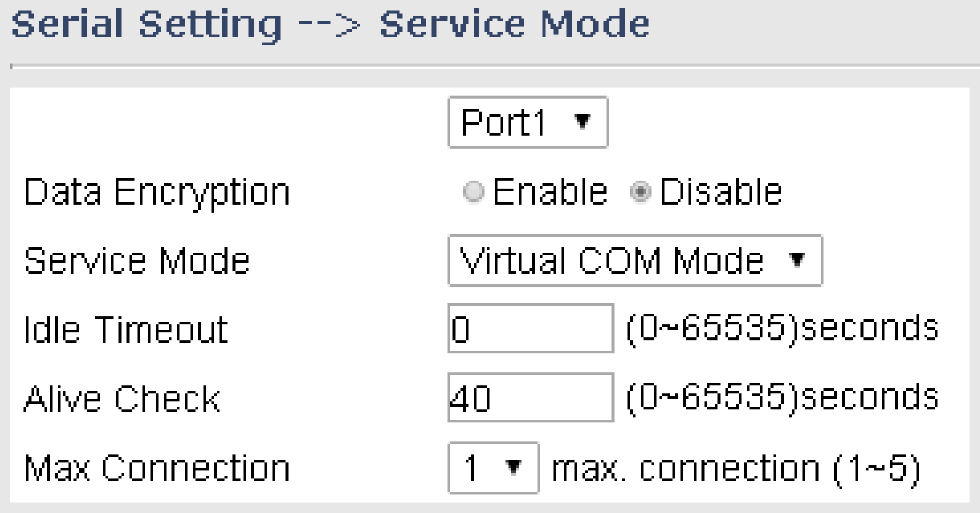
	Port1 ▼
Local TCP Port	4002
Command Port	4003
Mode	Serial to Ethernet
Flush Data Buffer After	0 ms
Delimiter(Hex 0~ff)	1: 00 2: 00 3: 00 4: 00
Mode	Ethernet to Serial
Flush Data Buffer After	0 ms
Delimiter(Hex 0~ff)	1: 00 2: 00 3: 00 4: 00

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 **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 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

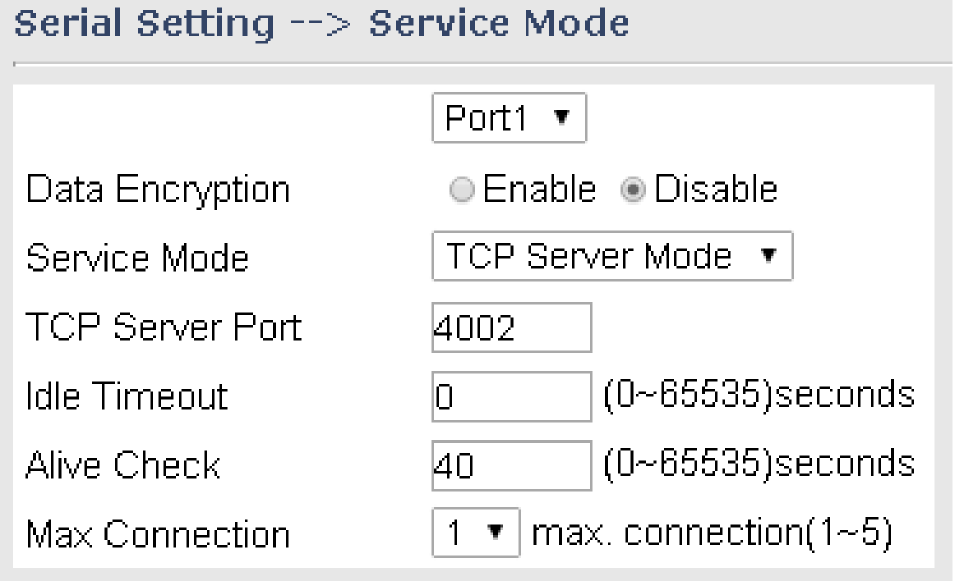
	Port1 ▼
Data Encryption	○ Enable ● Disable
Service Mode	Virtual COM Mode ▼
Idle Timeout	0 (0~65535)seconds
Alive Check	40 (0~65535)seconds
Max Connection	1 ▼ max. connection (1~5)

Label	Description
Data Encryption	Use SSL to encrypt data.
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. **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 number of maximum connections can be supported. The maximum value is **5**, default values is **1**.

*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

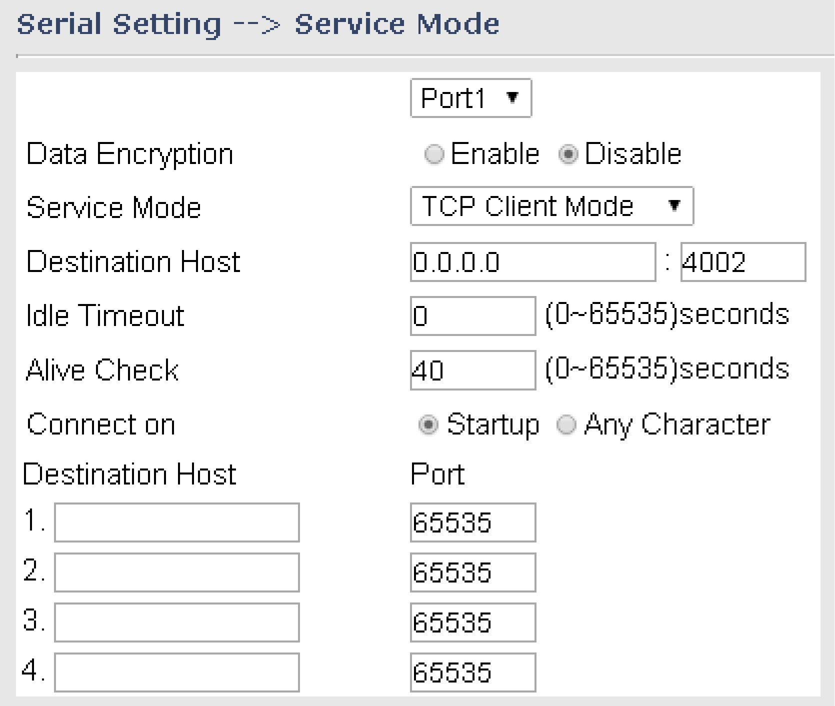
Alive Check: 40 (0~65535)seconds

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. **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 number of maximum connections can be supported. The maximum value is **5**, default values is **1**.

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.



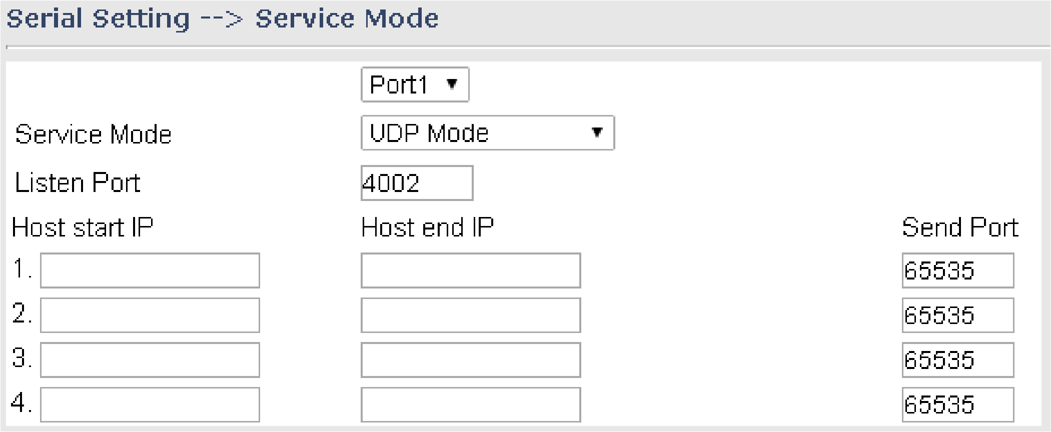
Serial Setting --> Service Mode

	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.	65535
2.	65535
3.	65535
4.	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. **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.**
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 Client 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

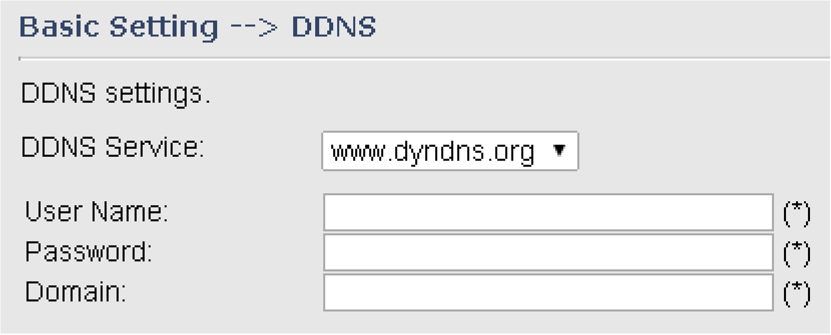
Listen Port: 4002

Host start IP	Host end IP	Send Port
1.		65535
2.		65535
3.		65535
4.		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 **Host Start** / **End IP**. You can also auto scan the sending port number of the device
Send Port	Set the send port number.

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: www.dyndns.org

User Name: (*)

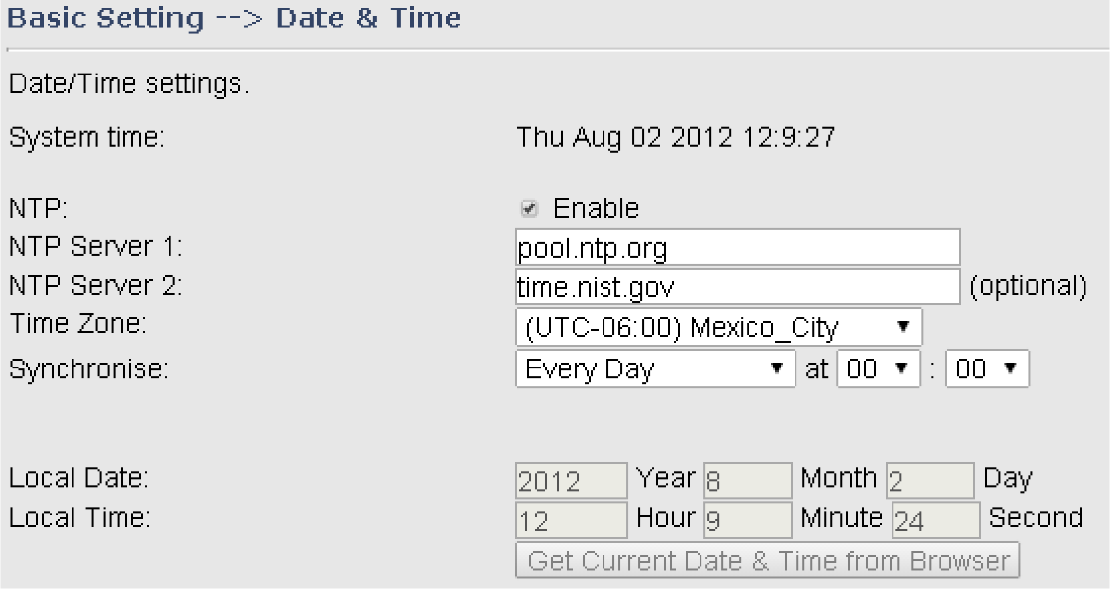
Password: (*)

Domain: (*)

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

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:	pool.ntp.org
NTP Server 2:	time.nist.gov (optional)
Time Zone:	(UTC-06:00) Mexico_City ▾
Synchronise:	Every Day ▾ at 00 ▾ : 00 ▾
Local Date:	2012 Year 8 Month 2 Day
Local Time:	12 Hour 9 Minute 24 Second

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

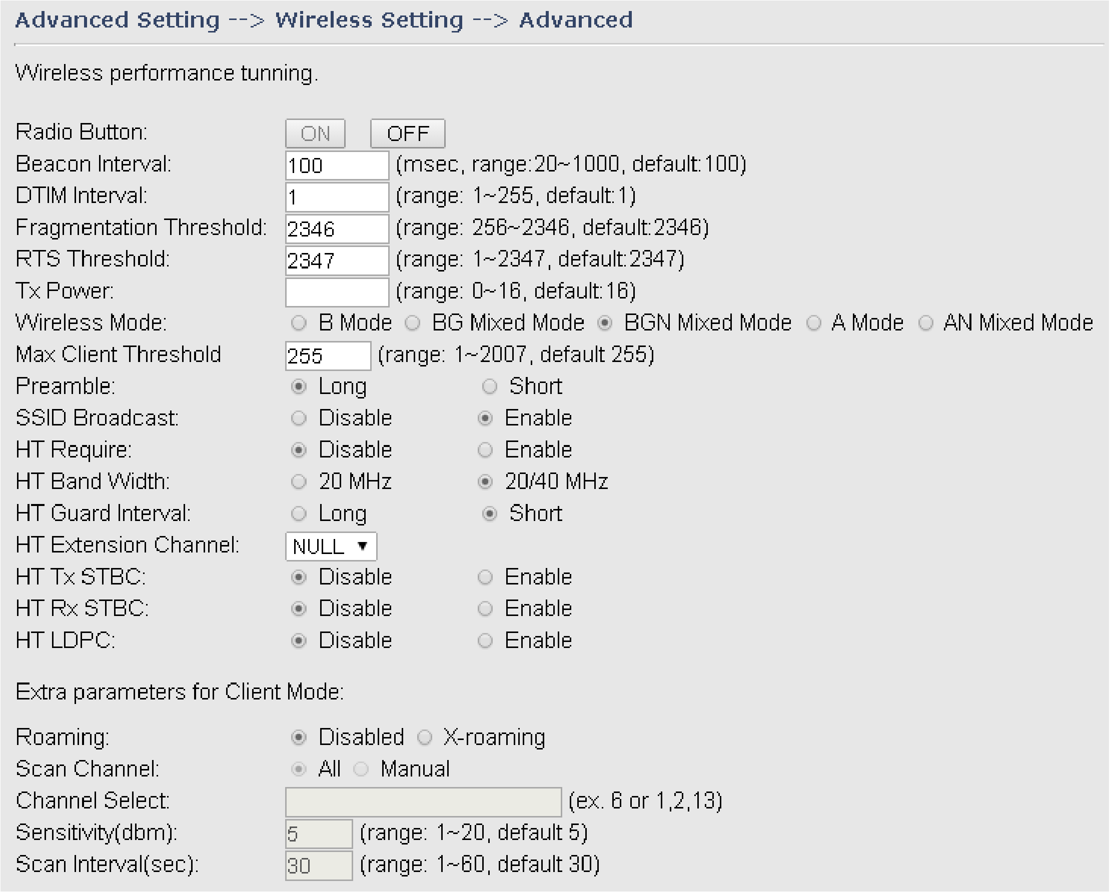
5.2.2 Networking Setting

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

Wireless Setting

Advanced

This page allows you to set up wireless configuration.



Advanced Setting --> Wireless Setting --> Advanced

Wireless performance tunning.

Radio Button: ON OFF

Beacon Interval: 100 (msec, range:20~1000, default:100)

DTIM Interval: 1 (range: 1~255, default:1)

Fragmentation Threshold: 2346 (range: 256~2346, default:2346)

RTS Threshold: 2347 (range: 1~2347, default:2347)

Tx Power: (range: 0~16, default:16)

Wireless Mode: ○ B Mode ○ BG Mixed Mode ● BGN Mixed Mode ○ A Mode ○ AN Mixed Mode

Max Client Threshold 255 (range: 1~2007, default 255)

Preamble: ● Long ○ Short

SSID Broadcast: ○ Disable ● Enable

HT Require: ● Disable ○ Enable

HT Band Width: ○ 20 MHz ● 20/40 MHz

HT Guard Interval: ○ Long ● Short

HT Extension Channel: NULL ▾

HT Tx STBC: ● Disable ○ Enable

HT Rx STBC: ● Disable ○ Enable

HT LDPC: ● Disable ○ Enable

Extra parameters for Client Mode:

Roaming: ● Disabled ○ X-roaming

Scan Channel: ● All ○ Manual

Channel Select: (ex. 6 or 1,2,13)

Sensitivity(dbm): 5 (range: 1~20, default 5)

Scan Interval(sec): 30 (range: 1~60, default 30)

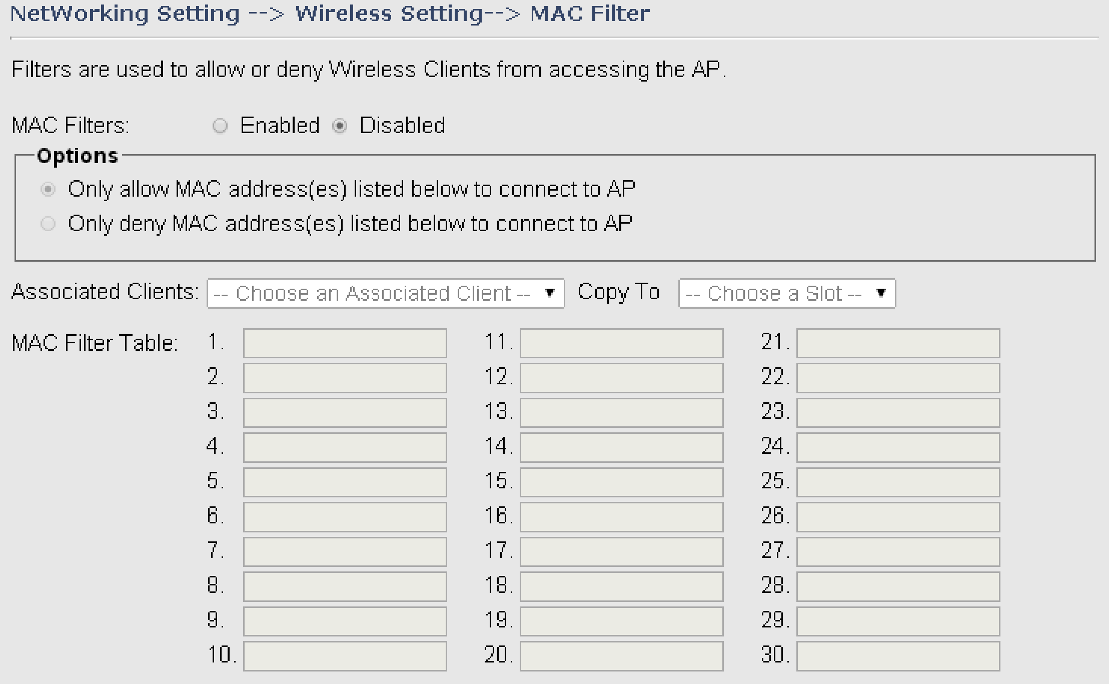
Label	**Description**
Radio Button	Enables or disables wireless function
Beacon Interval	A beacon is a packet sent by a wireless access point to synchronize wireless devices. The beacon interval value indicates the frequency interval of the beacon. Increasing the beacon interval reduces the number of beacons and the overhead associated with them. The default value is **100**, but **50** is recommended when reception is poor.
DTIM Interval	A DTIM interval determines how often a beacon frame includes a Delivery Traffic Indication message, a message that informs the clients about the presence of buffered multicast/broadcast data on the access point. The message is generated within the periodic beacon at a frequency specified by the DTIM Interval. When the AP sends a DTIM with a DTIM interval value, the client hearing the beacons will awake to receive the messages. The default value is **1**, and the value must be between 1 and 255

	milliseconds.
Fragmentation Threshold	The value specifies the maximum size for a packet before data is fragmented into multiple packets. The value should remain at the default **2346** (the range is 256 - 2346 bytes). If you experience a high packet error rate, you may slightly increase the value. Setting the value too low may result in poor network performance. Only minor modifications of this value are recommended.
RTS Threshold	The RTS (Request to Send) Threshold is the amount of time a wireless device, attempting to send, will wait for a recipient to acknowledge that it is ready. Normally, the AP sends a RTS frame to a station and negotiates the sending of data. After receiving the RTS, the station responds with a CTS (Clear to Send) frame to acknowledge the right to begin transmission. To ensure communication, the maximum value should be used, which is the default value 2347 (the range is 0-2347 bytes). If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled.
TX Power	This is the wireless device's transmission power and is typically measured in dBm. With greater Tx power, greater transmission distances can be achieved.
Wireless Mode	You can select 802.11 b, b/g, or b/g/n mode.
Max Client Threshold	This is the maximum number of clients for an AP. When the number of clients exceeds the value, the AP will reject the roaming connection. This value is only used on AP-mode equipment.
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.
SSID Broadcast	When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcasted by the AP. Click **Enable** if you want to broadcast the AP SSID, otherwise click **Disable** to inactivate the function.

Roaming	Select **Disabled** to disable X-Roaming protocol or select **X-roaming** to enable X-Roaming protocol
Scan Channel	Select **All** to scan all supported channels or **Manual** to scan only selected channels specified in Channel Select**.**
Channel Select	Assign the value roaming channels
Sensitivity	Configures signal sensitivity
Scan Interval	Configures scan interval

MAC Filter

This page allows you to set up MAC filters to allow or deny wireless clients to connect to the gateway. You can manually add a MAC address or select a MAC address from the Associated Clients list currently associated with the gateway.



NetWorking Setting --> Wireless Setting--> MAC Filter

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

MAC Filters: ○ Enabled ● Disabled

Options

● Only allow MAC address(es) listed below to connect to AP

○ Only deny MAC address(es) listed below to connect to AP

Associated Clients: -- Choose an Associated Client -- ▼ Copy To -- Choose a Slot -- ▼

MAC Filter Table:

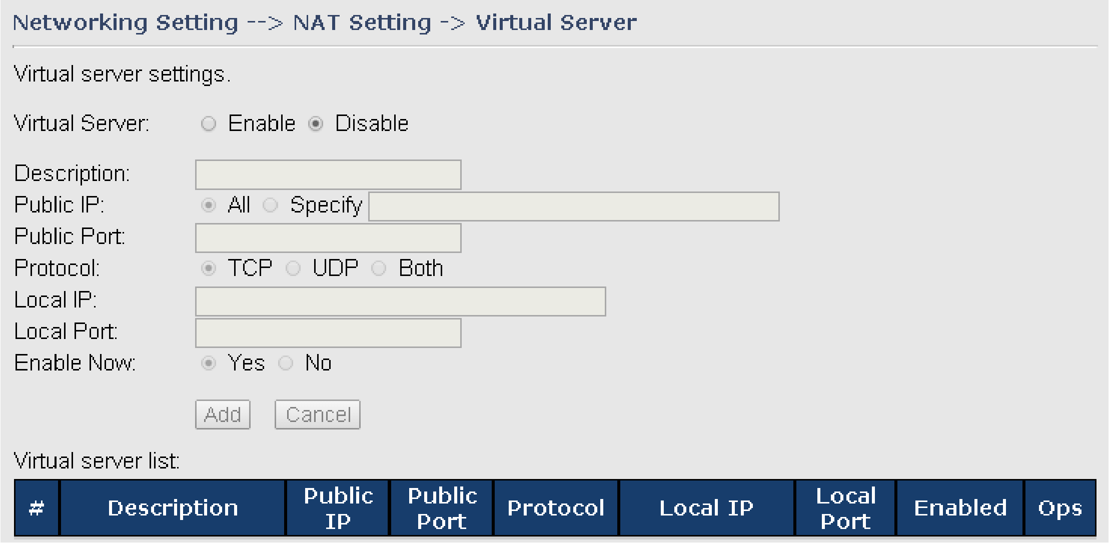
1.		11.		21.	
2.		12.		22.	
3.		13.		23.	
4.		14.		24.	
5.		15.		25.	
6.		16.		26.	
7.		17.		27.	
8.		18.		28.	
9.		19.		29.	
10.		20.		30.	

Label	**Description**
MAC Filter	Select **Enabled** or **Disabled** to activate or deactivate MAC filters
Options	Select one of the options to allow or deny the MAC address in the list
Associated Clients	Shows the wireless MAC addresses associated with the gateway
MAC Filter Table	You can edit up to MAC addresses in these fields

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 gateway 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

Add Cancel

Virtual server list:

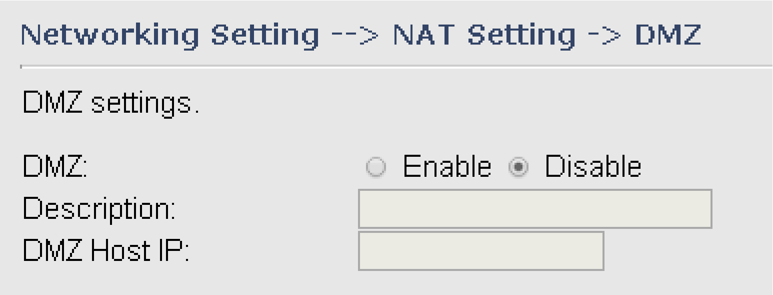
#	Description	Public IP	Public Port	Protocol	Local IP	Local Port	Enabled	Ops

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.



Networking Setting --> NAT Setting -> DMZ

DMZ settings.

DMZ: ○ Enable ● Disable

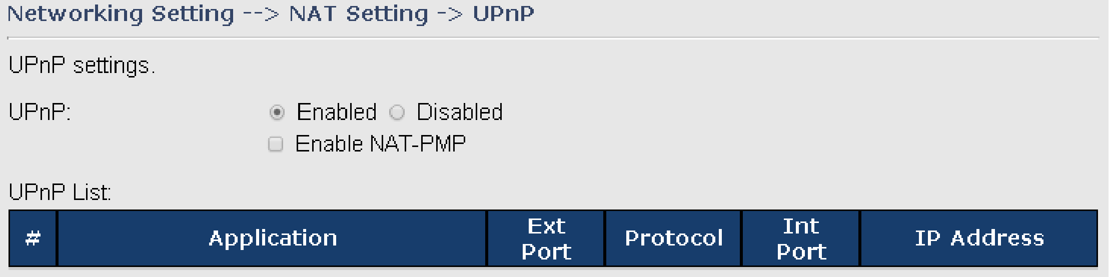
Description:

DMZ Host IP:

Label	Description
DMZ	Enables or disables 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

NAT Setting – 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

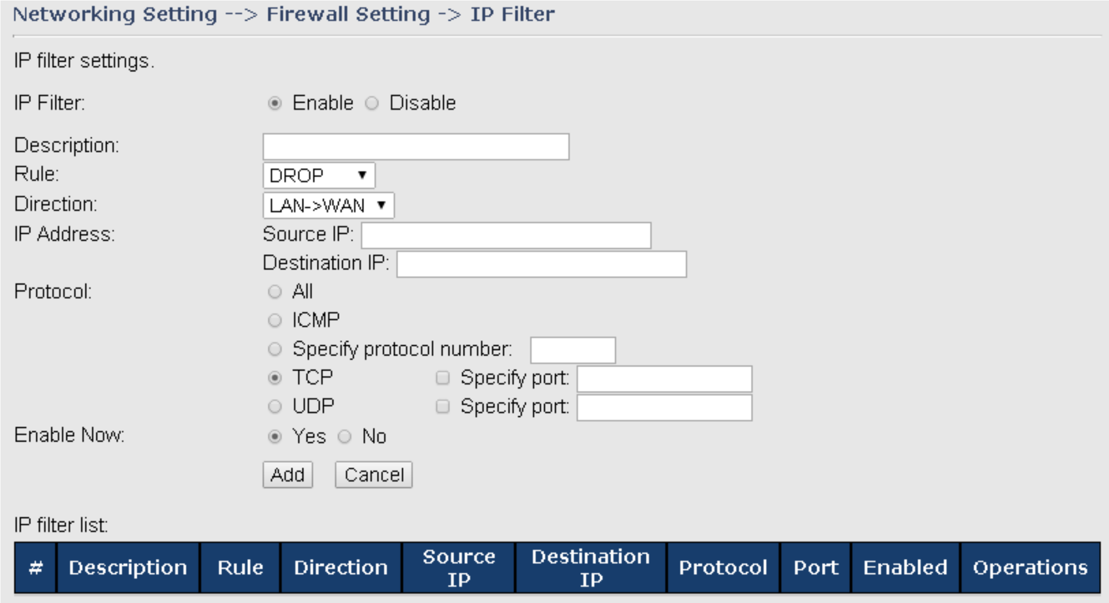
Label	Description
UPnP	Enable or disable UPnP.
Enable NAT-PMP	NAT-PMP allows a computer in a private network (behind a NAT router) to automatically configure the gateway to allow parties outside the private network to contact with each other. NAT-PMP operates with UDP. It essentially automates the process of port

	forwarding. Check the box to enable NAT-PMP.
UPnP List	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

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: DROP ▾

Direction: LAN->WAN ▾

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:

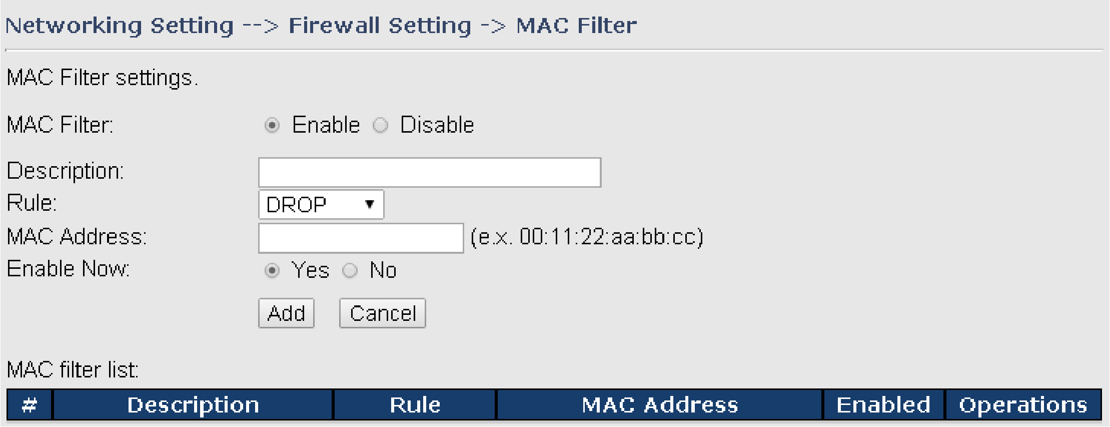
#	Description	Rule	Direction	Source IP	Destination IP	Protocol	Port	Enabled	Operations

Label	Description
IP Filter	Enables or disables the IP Filter
Description	Enter description for the entry.
Rule	Configures the rules to be applied to the IP filter. Available options include **DROP**, **ACCEPT**, and **REJECT.**
Direction	Specifies 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.



Networking Setting --> Firewall Setting -> MAC Filter

MAC Filter settings.

MAC Filter: ● Enable ○ Disable

Description:

Rule: DROP ▼

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

Enable Now: ● Yes ○ No

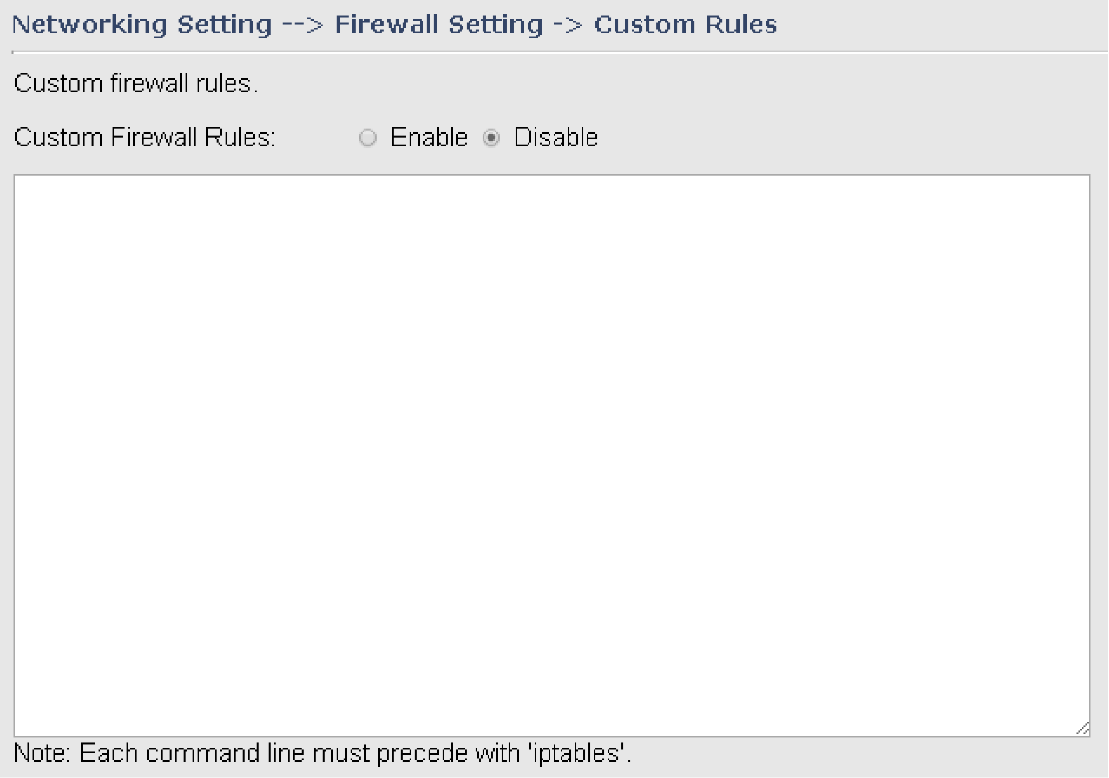
MAC filter list:

#	Description	Rule	MAC Address	Enabled	Operations

Label	Description
MAC Filter	Enables or disables the MAC Filter
Description	Enter description for the entry
Rule	Configures 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 sent by a wireless user associated to that SSID. 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.


Networking Setting --> Firewall Setting -> Custom Rules

Custom firewall rules.

Custom Firewall Rules: ○ Enable ● Disable

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

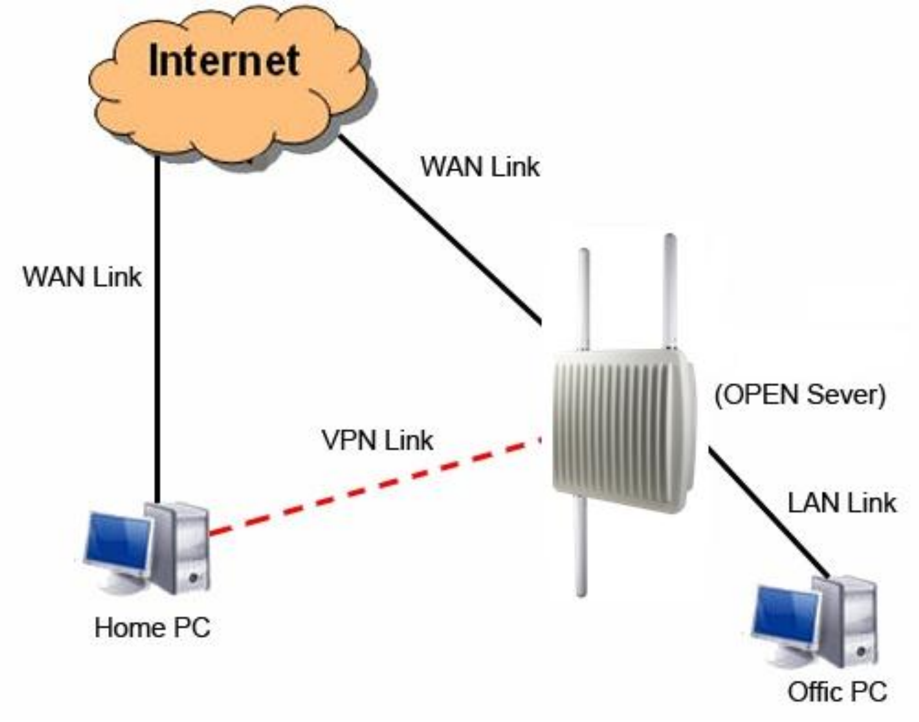
Vpn Setting

Open Vpn

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.

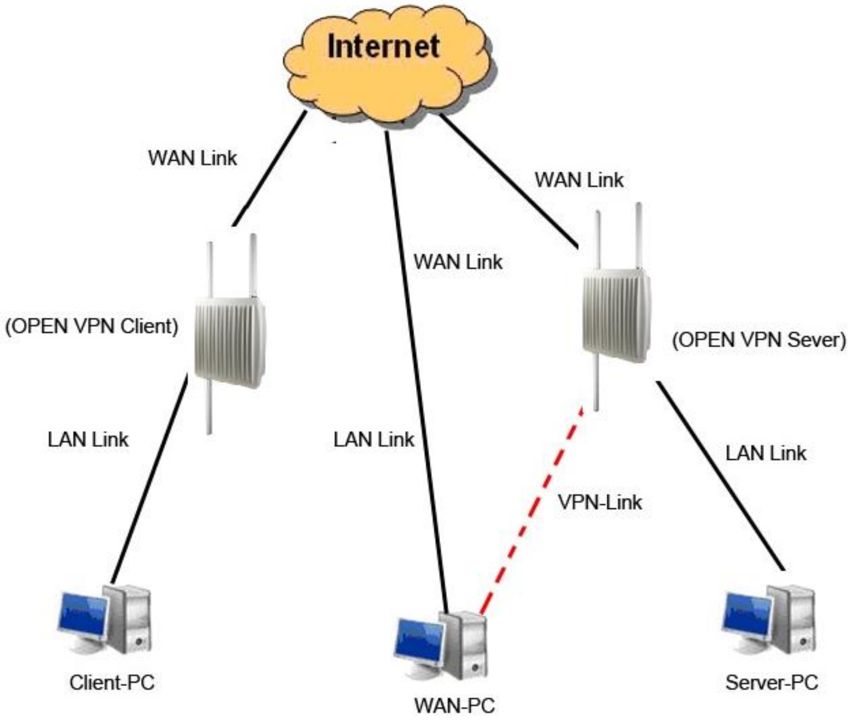
Open VPN enables you to easily set up a virtual private network over an encrypted connection. It is a full-function SSL VPN solution which accommodates a wide range of configurations including remote access, site-to-site VPNs, WiFi security, and enterprise-level remote access with load balancing, failover,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

To set up your gateway 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.

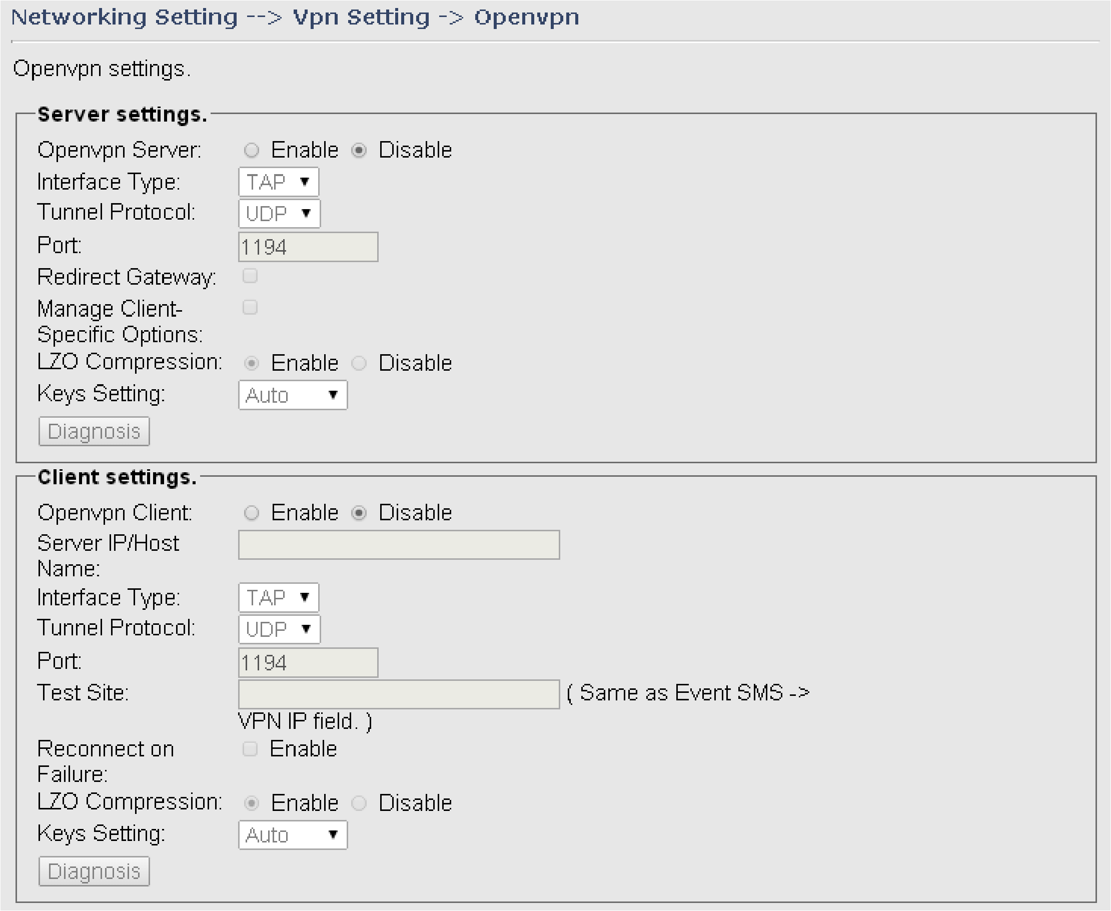


Connection to Open VPN Server

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

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

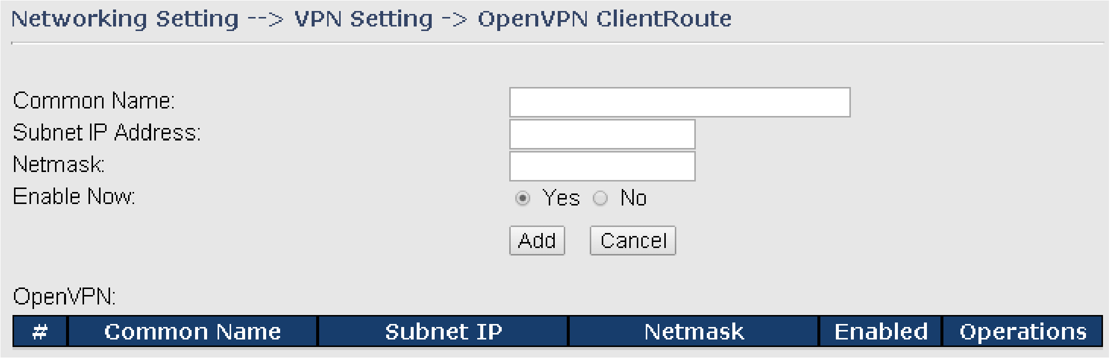
Keys Setting: Auto ▼

Diagnosis

Label	Description
Open VPN Server	Enables or disables the function of Open VPN server
Interface Type	Support TAP mode and TUN Mode
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**).
Redirect Gateway	Check this box will force all traffic to be routed through the VPN tunnel.
Manage Client-Specific Options	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.
LZO Compression	Enables or disables the LZO Compression. Check the box will enable compression over VPN.

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.
Open VPN Client	Enables or disables the function of Open VPN client.
Server IP/Host name	Enter the Open VPN server IP address
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**).
Test Site	Type a website address the field to use it to check if the connection is alive or lost.
Reconnection on Failure	Check the box to enable the device to reconnect when the link fails.
LZO Compression	Enables or disables the LZO Compression. Check the box will enable compression over VPN.
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.

Routing Setting



Networking Setting --> VPN Setting -> OpenVPN ClientRoute

Common Name:
Subnet IP Address:
Netmask:
Enable Now: ● Yes ○ No

OpenVPN:

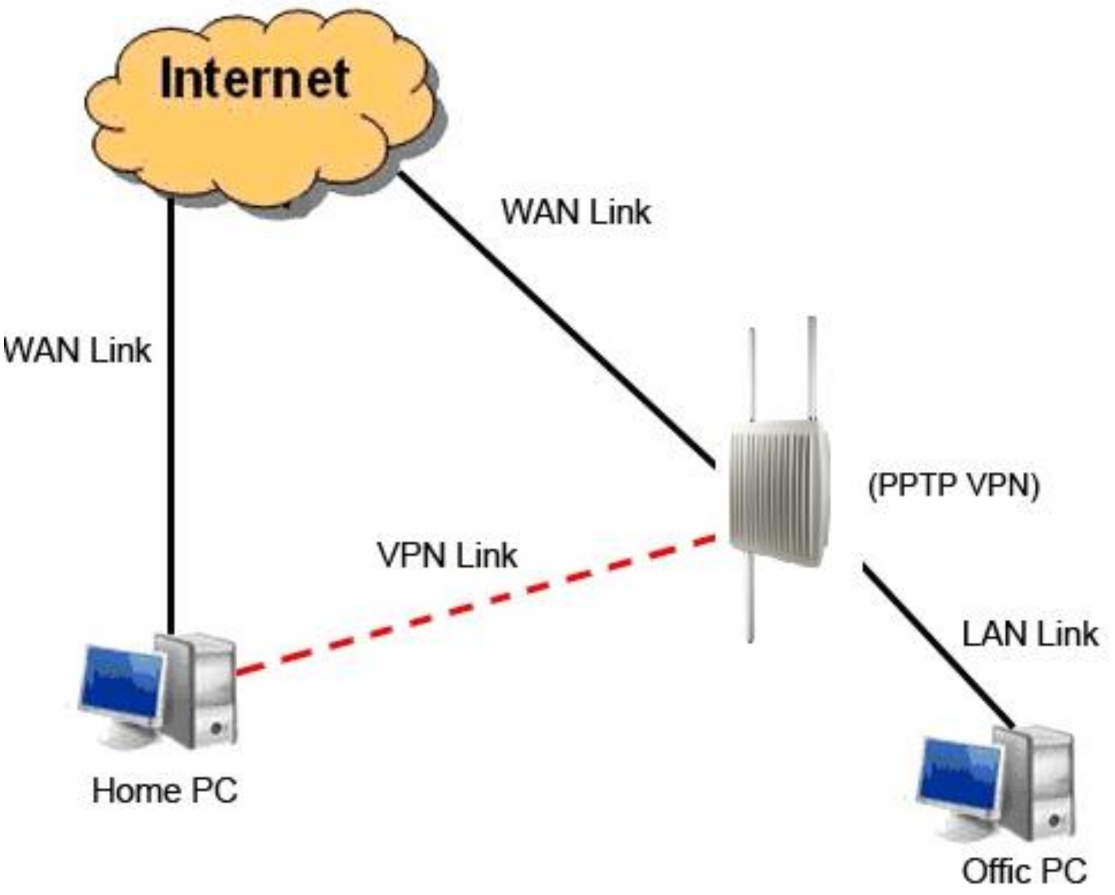
#	Common Name	Subnet IP	Netmask	Enabled	Operations

Label	Description
Common Name	Enter a common name for you to identify the VPN
Subnet IP Address	Enter the subnet IP address for the VPN.

Netmask	Enter the netmask IP address for the VPN.
Enable Now	Check to enable the function.

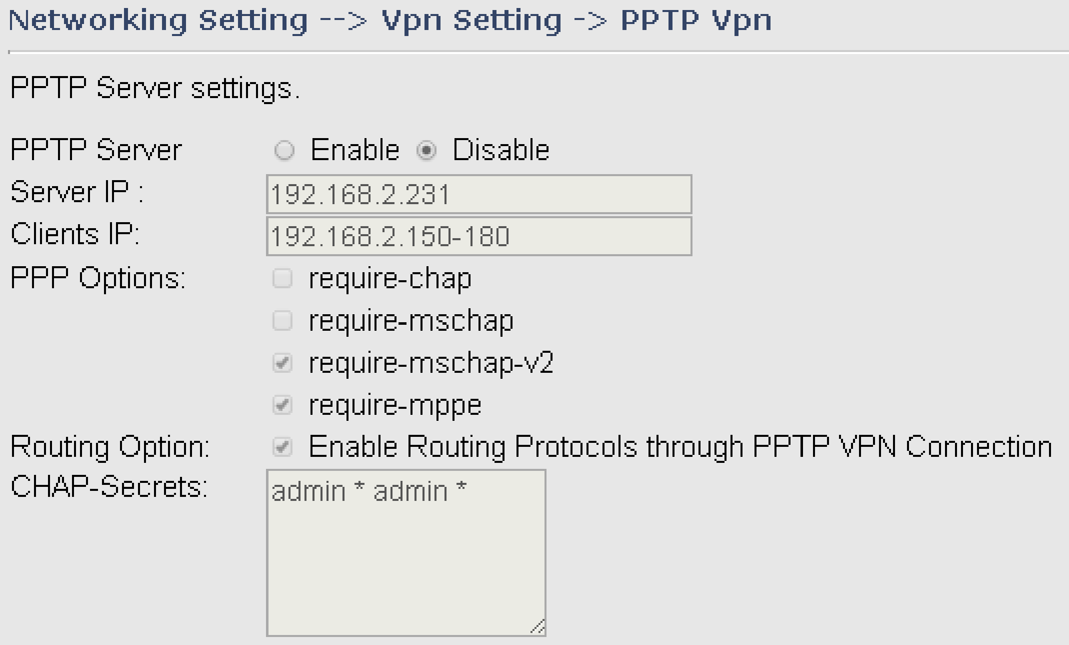
PPTP VPN

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 : 192.168.2.231

Clients IP: 192.168.2.150-180

PPP Options:

□ require-chap

□ require-mschap

☑ require-mschap-v2

☑ require-mppe

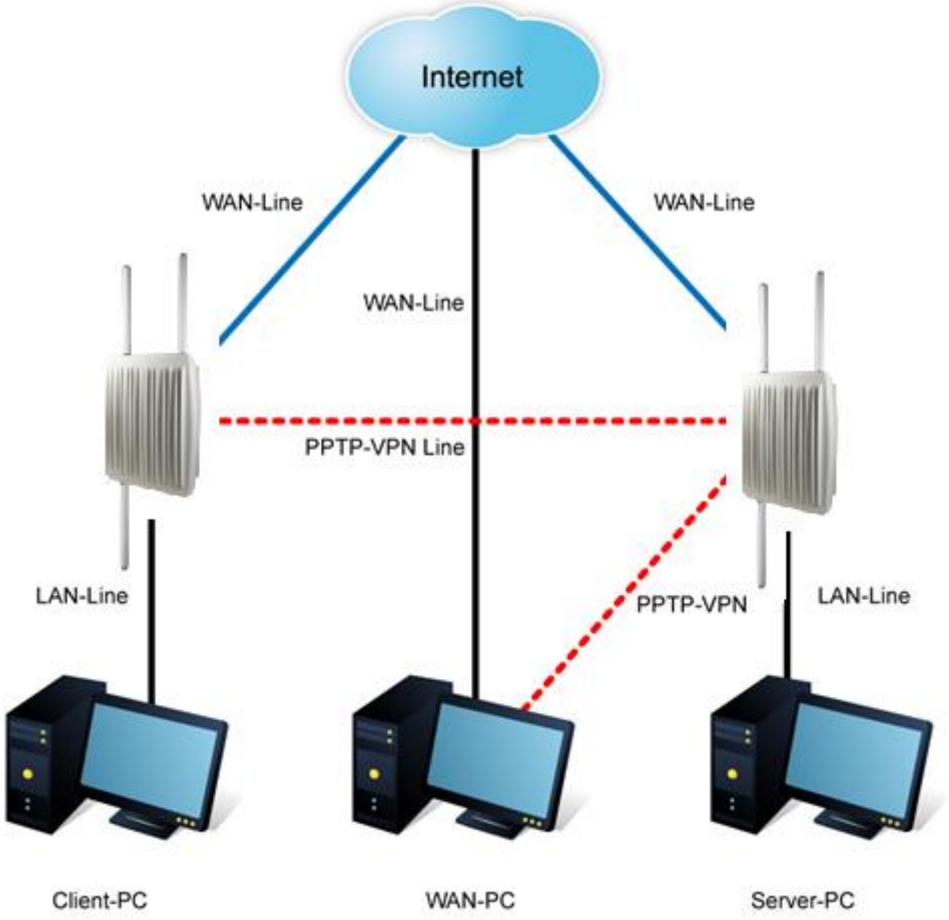
Routing Option: ☑ Enable Routing Protocols through PPTP VPN Connection

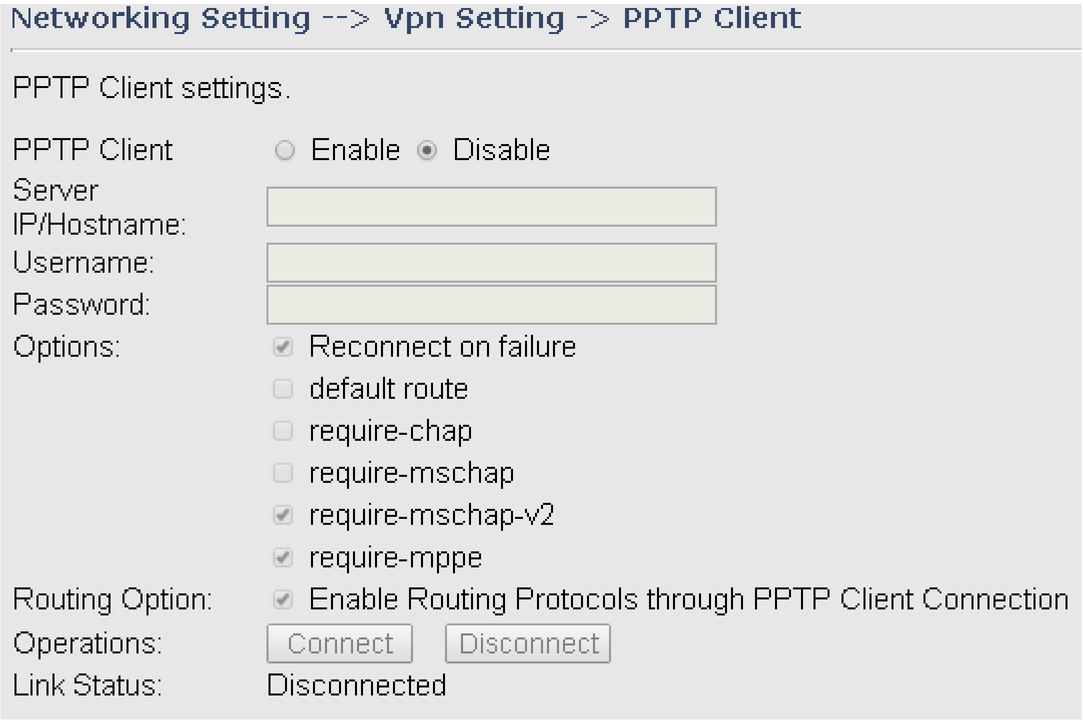
CHAP-Secrets: admin * admin *

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

PPTP Client

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





Networking Setting --> Vpn Setting -> PPTP Client

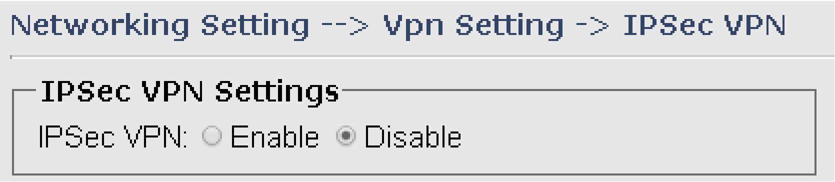
PPTP Client settings.

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:	Connect Disconnect
Link Status:	Disconnected

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



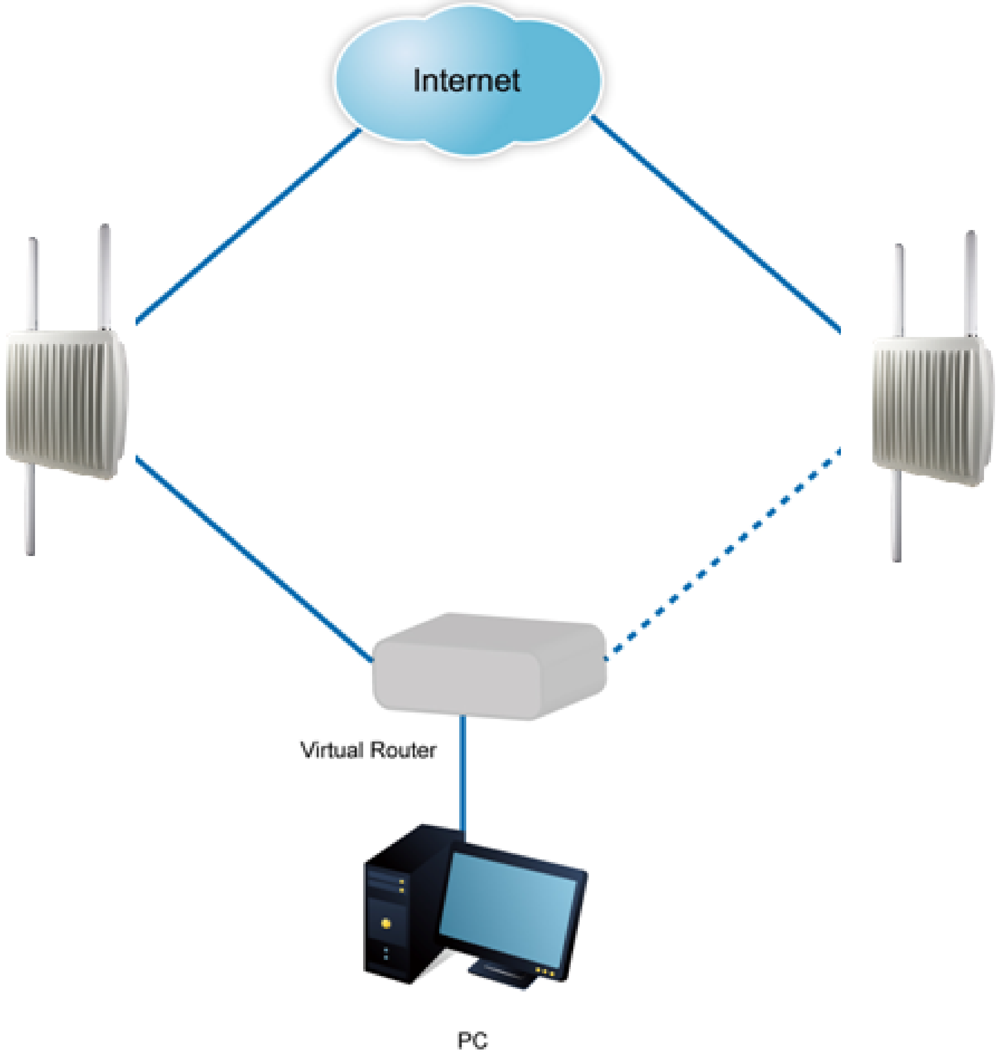
Networking Setting --> Vpn Setting -> IPSec VPN

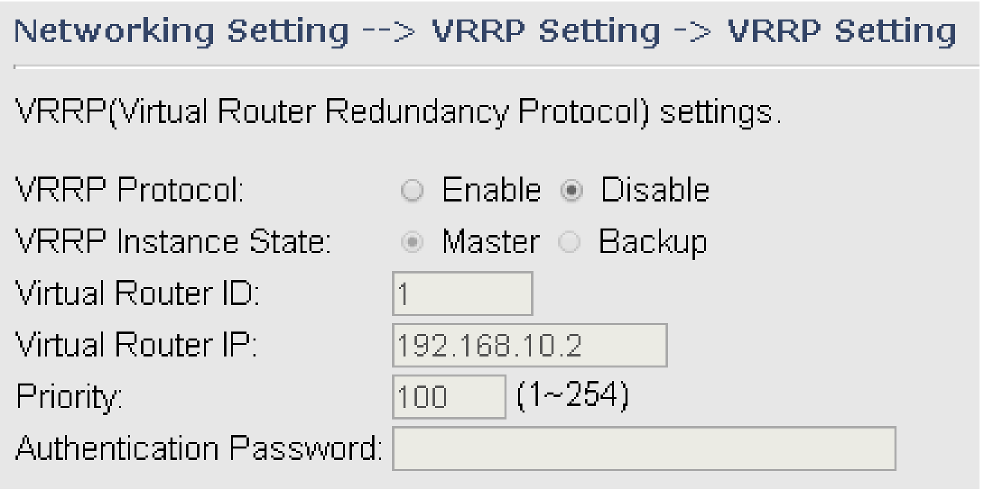
IPSec VPN Settings

IPSec VPN: ○ Enable ● Disable

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 --> VRRP Setting -> VRRP Setting

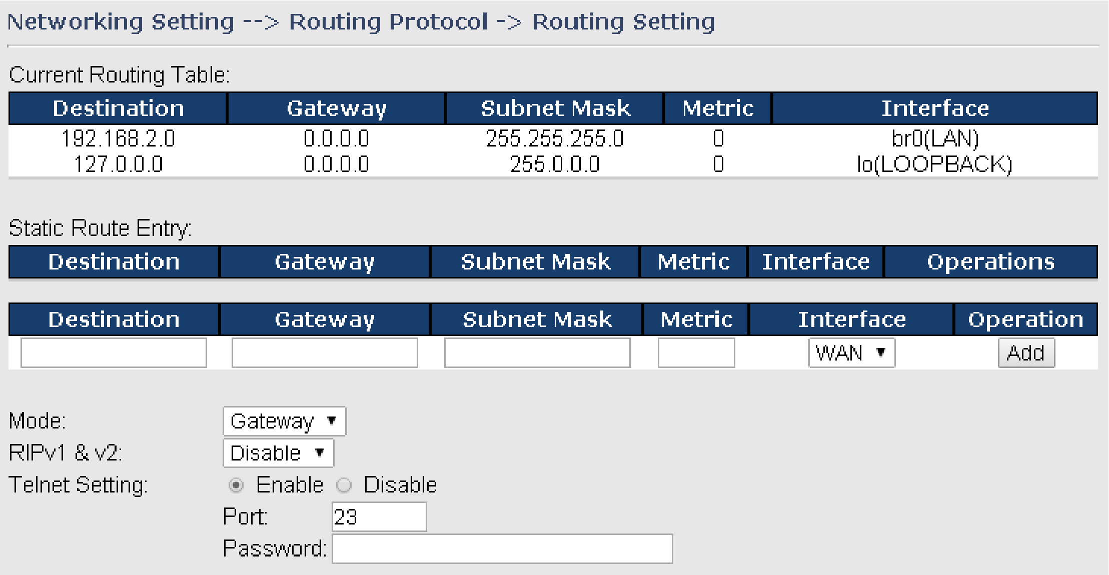
VRRP(Virtual Router Redundancy Protocol) settings.

VRRP Protocol:	○ Enable ● Disable
VRRP Instance State:	● Master ○ Backup
Virtual Router ID:	1
Virtual Router IP:	192.168.10.2
Priority:	100 (1~254)
Authentication Password:	

Label	Description
VRRP Protocol	Enables or disables VRRP function
VRRP Instance State	Specifies the gateway to act as the master or backup router
Virtual Router ID	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.
Virtual Router IP	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.
Priority	The priority value used by the VRRP router when selecting the master virtual router.
Authentication Password	Enter the password for authentication

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

Destination	Gateway	Subnet Mask	Metric	Interface	Operation
				WAN ▾	Add

Mode: Gateway ▾

RIPv1 & v2: Disable ▾

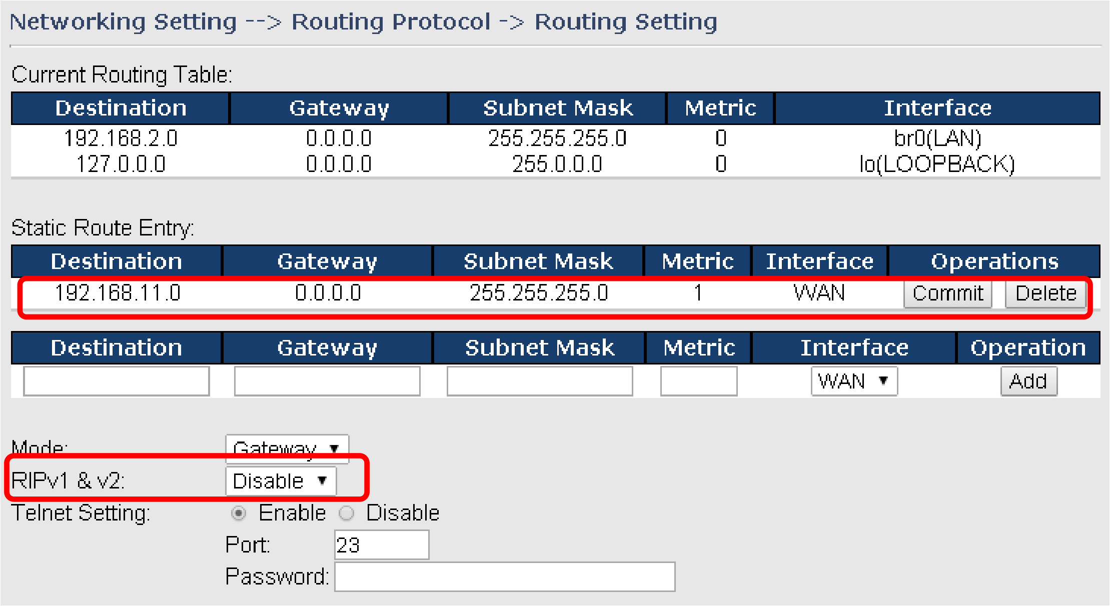
Telnet Setting: ● Enable ○ Disable

Port: 23

Password:

Static Routing

When RIPv1 & v2 is **Disabled**, the gateway will operate in static routing mode, which means gateways 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

Destination	Gateway	Subnet Mask	Metric	Interface	Operation
				WAN ▾	Add

Mode: Gateway ▾

RIPv1 & v2: Disable ▾

Telnet Setting: ● Enable ○ Disable

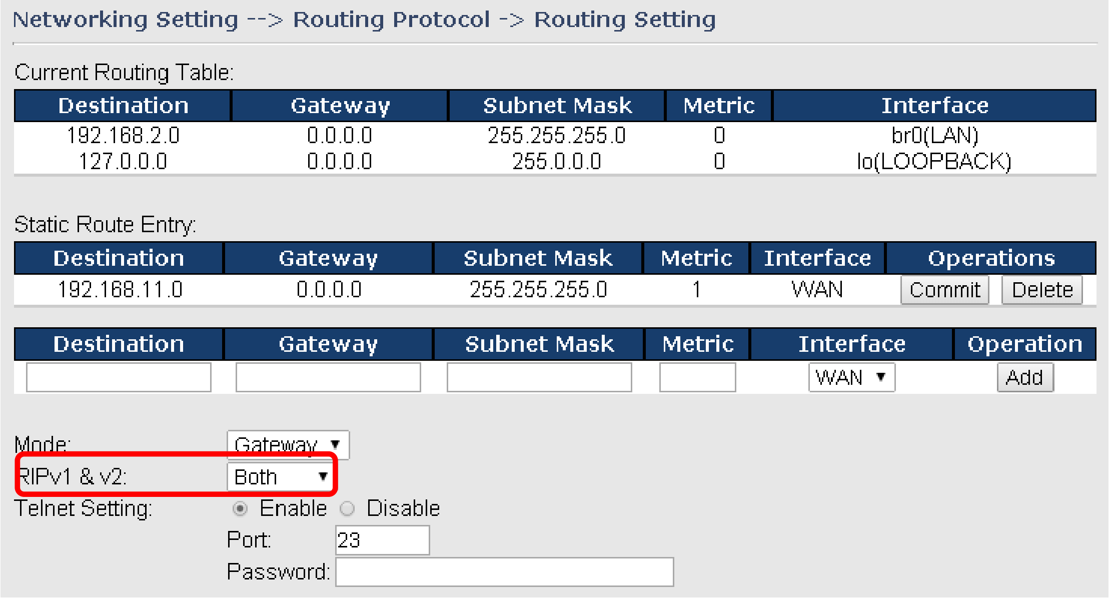
Port: 23

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	Commit Delete

Destination	Gateway	Subnet Mask	Metric	Interface	Operation
				WAN ▾	Add

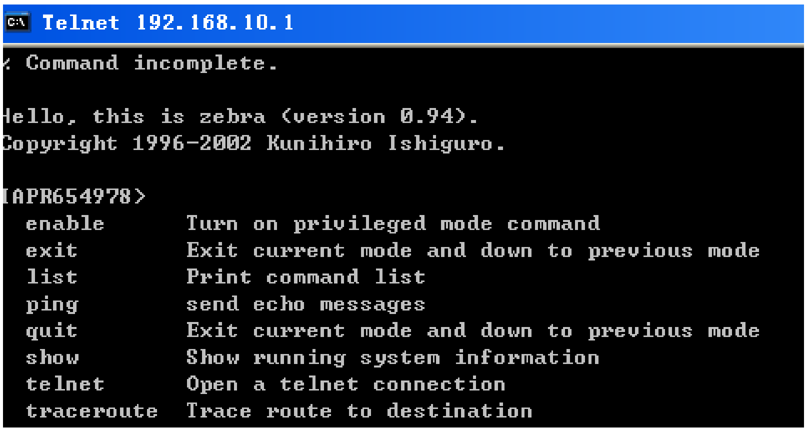
Mode: Gateway ▾

RIPv1 & v2: Both ▾

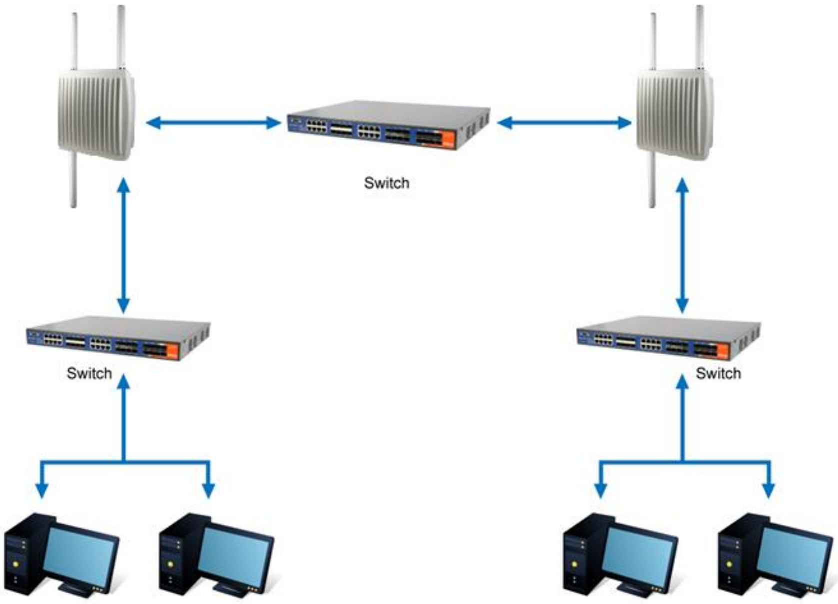
Telnet Setting: ● Enable ○ Disable

Port: 23

Password:

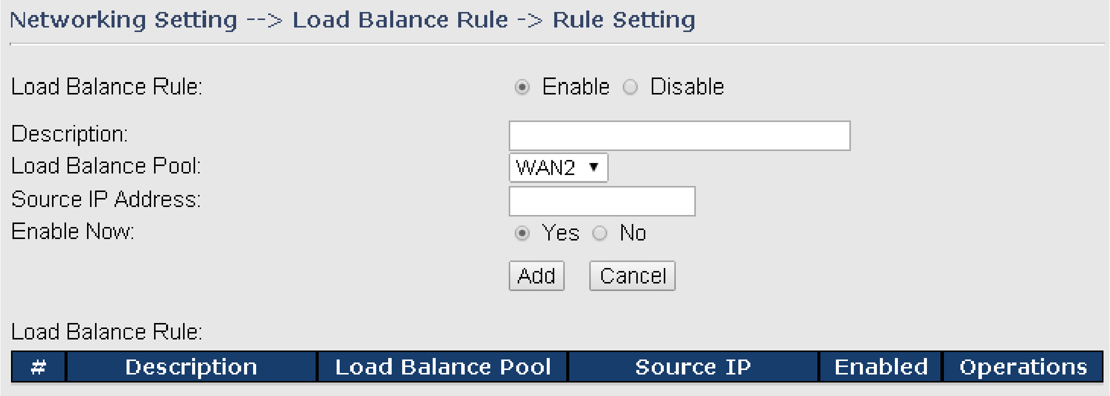
Label	Description
Current Routing Table	Shows all routing information, including static and dynamic routing (if enabled)
Static Route Entry	Fills in corresponding information to add new entries to the static routing tablet
Mode	Choose **Gateway Mode** if you want PCs in the LAN to visit external network,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

```
Telnet 192.168.10.1

% Command incomplete.

Hello, this is zebra (version 0.94).
Copyright 1996-2002 Kunihiro Ishiguro.

APR654978>
  enable       Turn on privileged mode command
  exit         Exit current mode and down to previous mode
  list         Print command list
  ping         send echo messages
  quit         Exit current mode and down to previous mode
  show         Show running system information
  telnet       Open a telnet connection
  traceroute   Trace route to destination
```



Routing Topography

Load Balance Rule



Networking Setting --> Load Balance Rule -> Rule Setting

Load Balance Rule: ● Enable ○ Disable

Description:

Load Balance Pool: WAN2

Source IP Address:

Enable Now: ● Yes ○ No

Load Balance Rule:

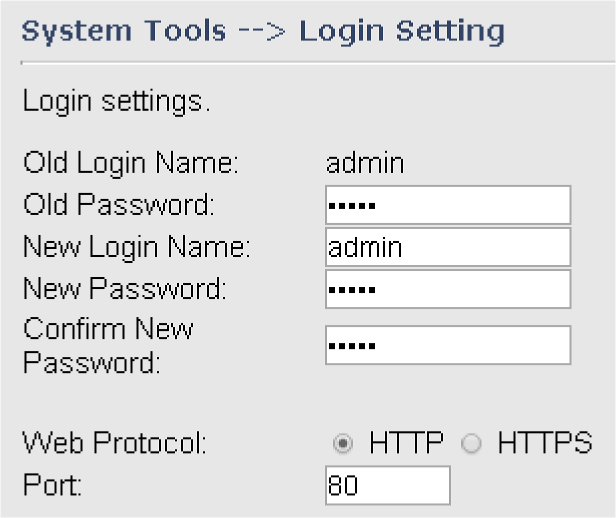
#	Description	Load Balance Pool	Source IP	Enabled	Operations

Label	Description
Load Balance Rule	Check to enable or disable the function.
Description	Type the description for the rule.
Load Balance Pool	Choose one of the profiles to be used by such rule.
Source IP Address	Type a WAN IP address here as the source IP address for such rule.
Enable Now	Check to activate the function immediately or at a later time.

5.2.3 System Tools

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: •••••

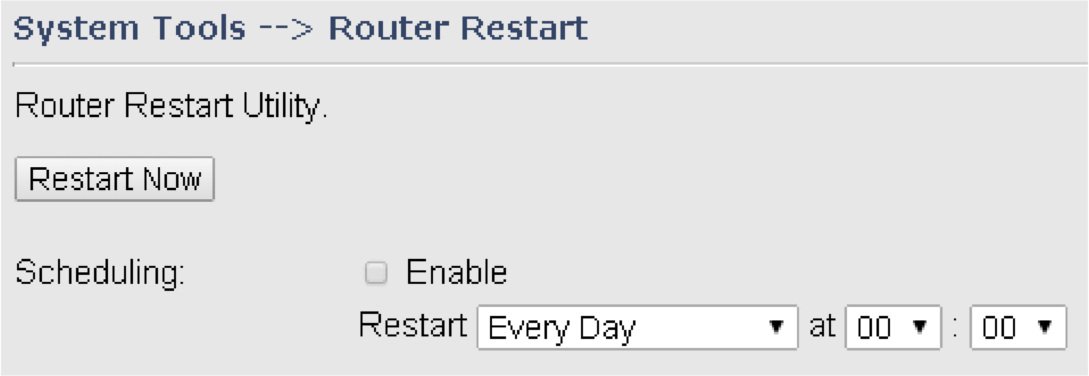
Web Protocol: ● HTTP ○ HTTPS

Port: 80

Label	**Description**
Old Name	Type in current login name
Old Password	Type in current password
New Name	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.
New Password	Enter a new login password. Acceptable characters contain '0-9', 'a-z', 'A-Z' and the length must be 0 to 15 characters.
Confirm New Password	Retype the new password to confirm it.
Web Protocol	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.

M2M Restart

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



System Tools --> Router Restart

Router Restart Utility.

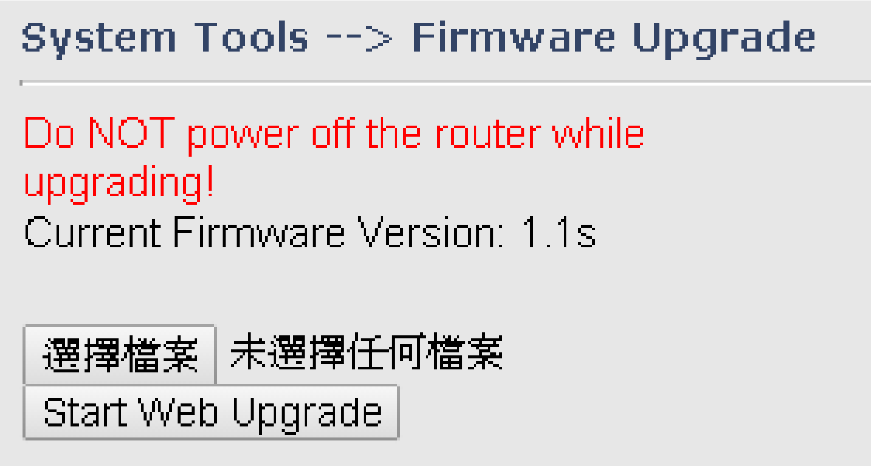
Scheduling: □ Enable

Restart Every Day ▼ at 00 ▼ : 00 ▼

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

Firmware Upgrade

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


System Tools --> Firmware Upgrade

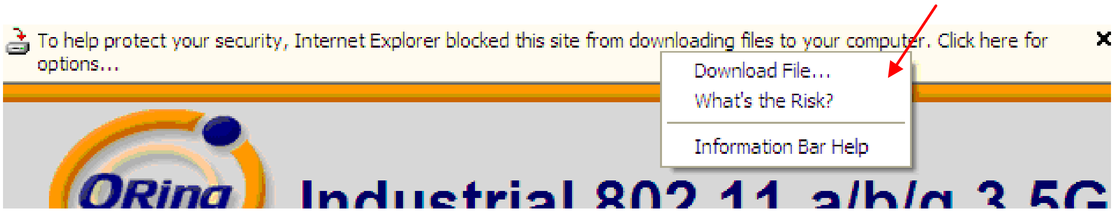
Do NOT power off the router while upgrading!

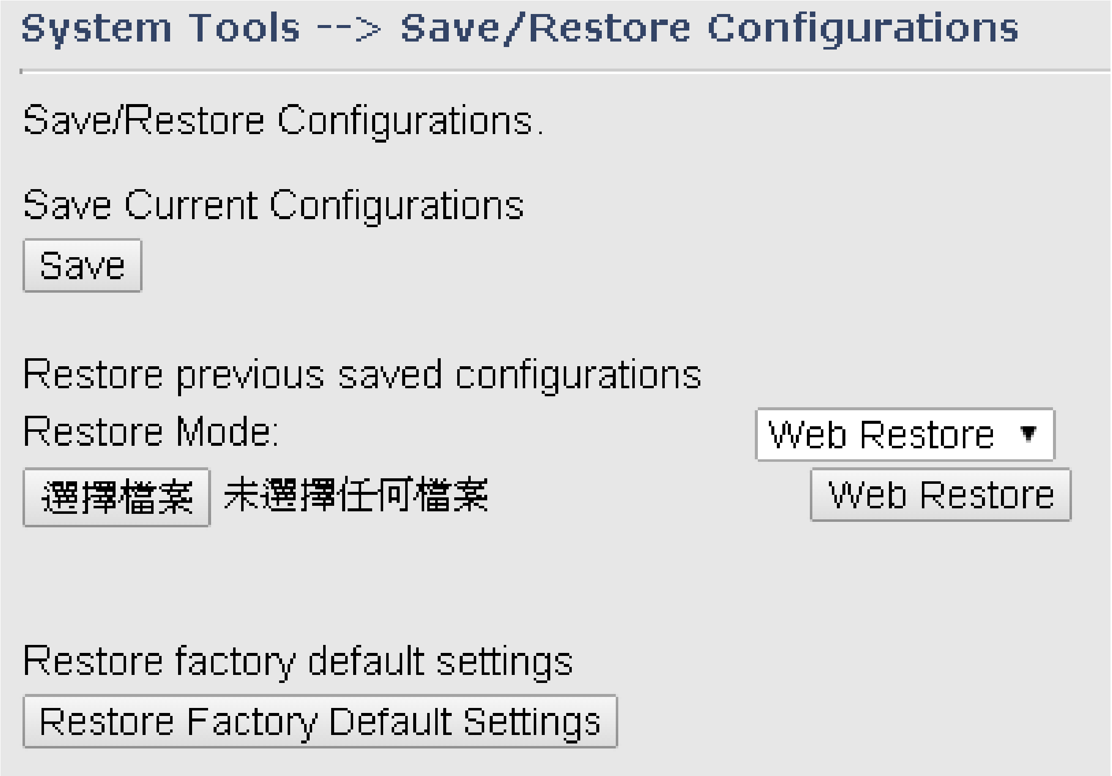
Current Firmware Version: 1.1s

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

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.


To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...



System Tools --> Save/Restore Configurations

Save/Restore Configurations.

Save Current Configurations

Save

Restore previous saved configurations

Restore Mode: Web Restore ▾

選擇檔案 未選擇任何檔案 Web Restore

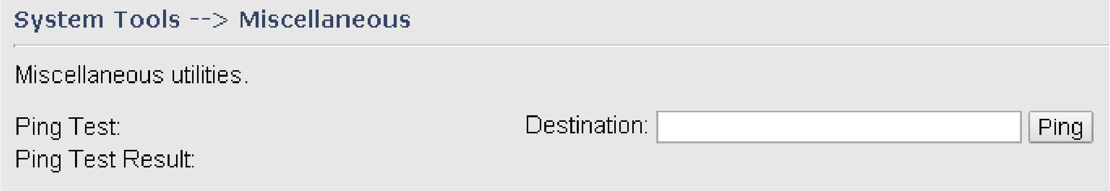
Restore factory default settings

Restore Factory Default Settings

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

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.

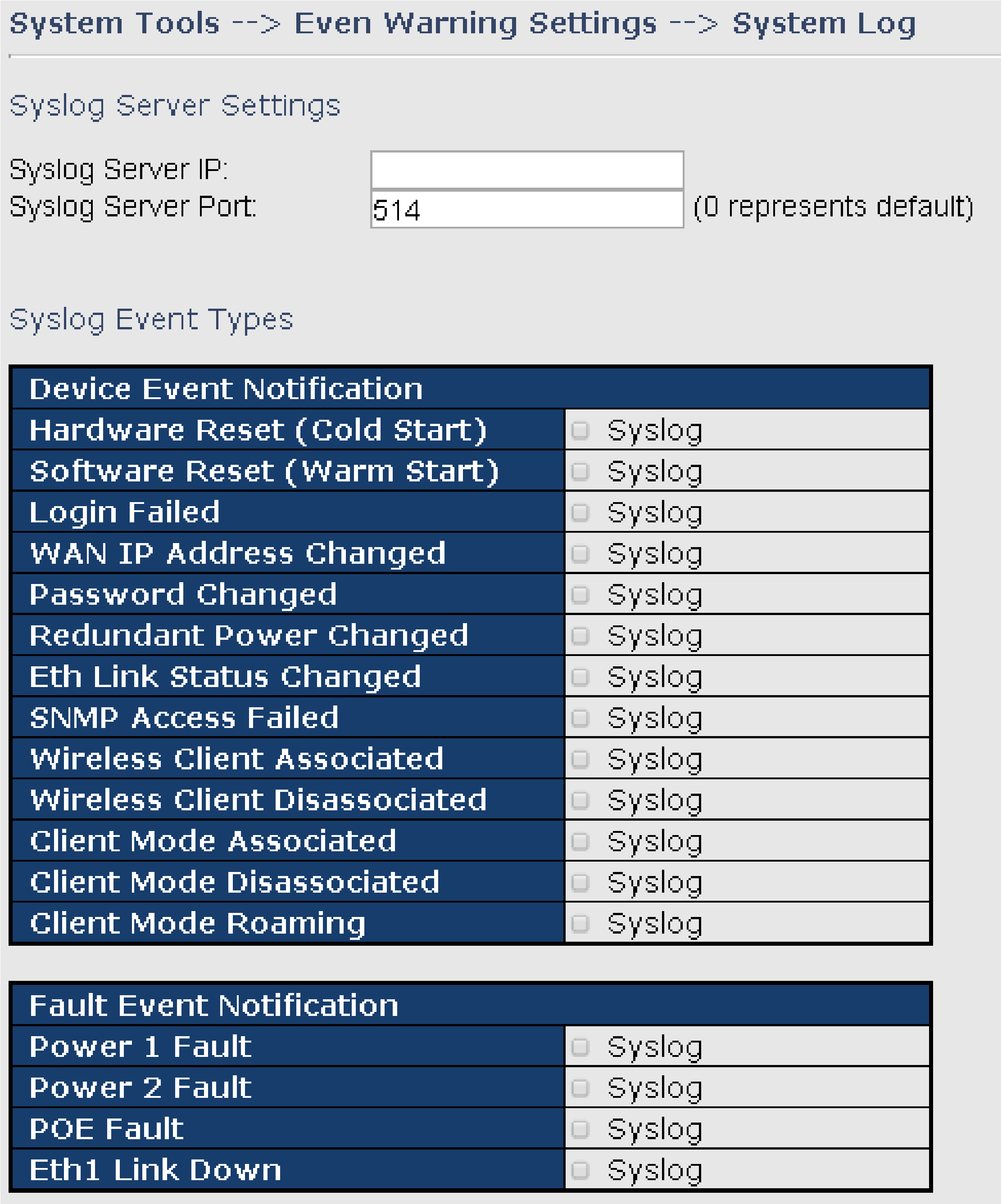
Ping Test: Destination: Ping

Ping Test Result:

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: 514 (0 represents default)

Syslog Event Types

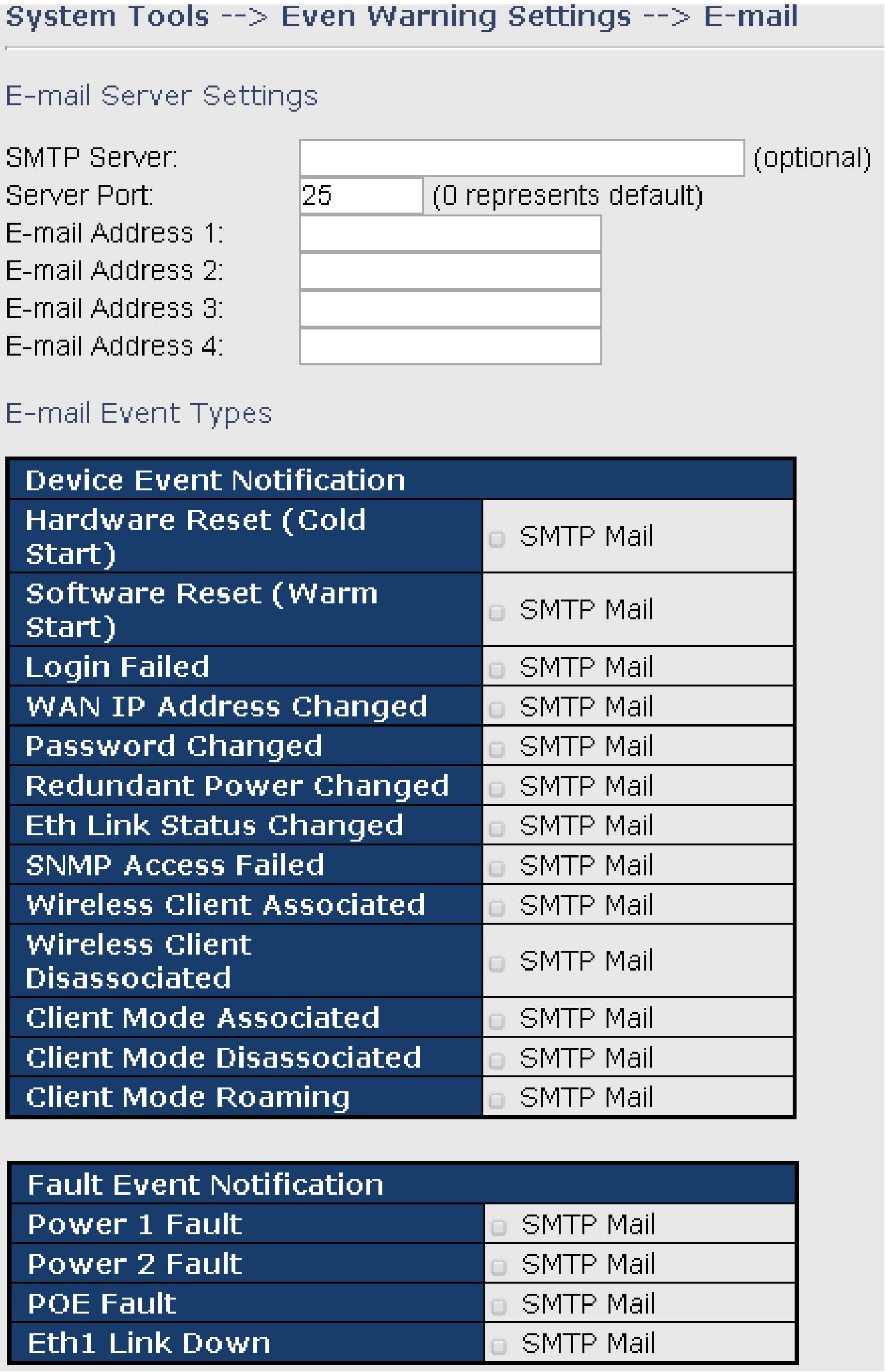
Device Event Notification	
Hardware Reset (Cold Start)	☐ Syslog
Software Reset (Warm Start)	☐ Syslog
Login Failed	☐ Syslog
WAN IP Address Changed	☐ Syslog
Password Changed	☐ Syslog
Redundant Power Changed	☐ Syslog
Eth Link Status Changed	☐ Syslog
SNMP Access Failed	☐ Syslog
Wireless Client Associated	☐ Syslog
Wireless Client Disassociated	☐ Syslog
Client Mode Associated	☐ Syslog
Client Mode Disassociated	☐ Syslog
Client Mode Roaming	☐ Syslog

Fault Event Notification	
Power 1 Fault	☐ Syslog
Power 2 Fault	☐ Syslog
POE Fault	☐ Syslog
Eth1 Link Down	☐ Syslog

Label	Description
Syslog Server 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.

Syslog Server Port	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:	25 (0 represents default)
E-mail Address 1:	
E-mail Address 2:	
E-mail Address 3:	
E-mail Address 4:	

E-mail Event Types

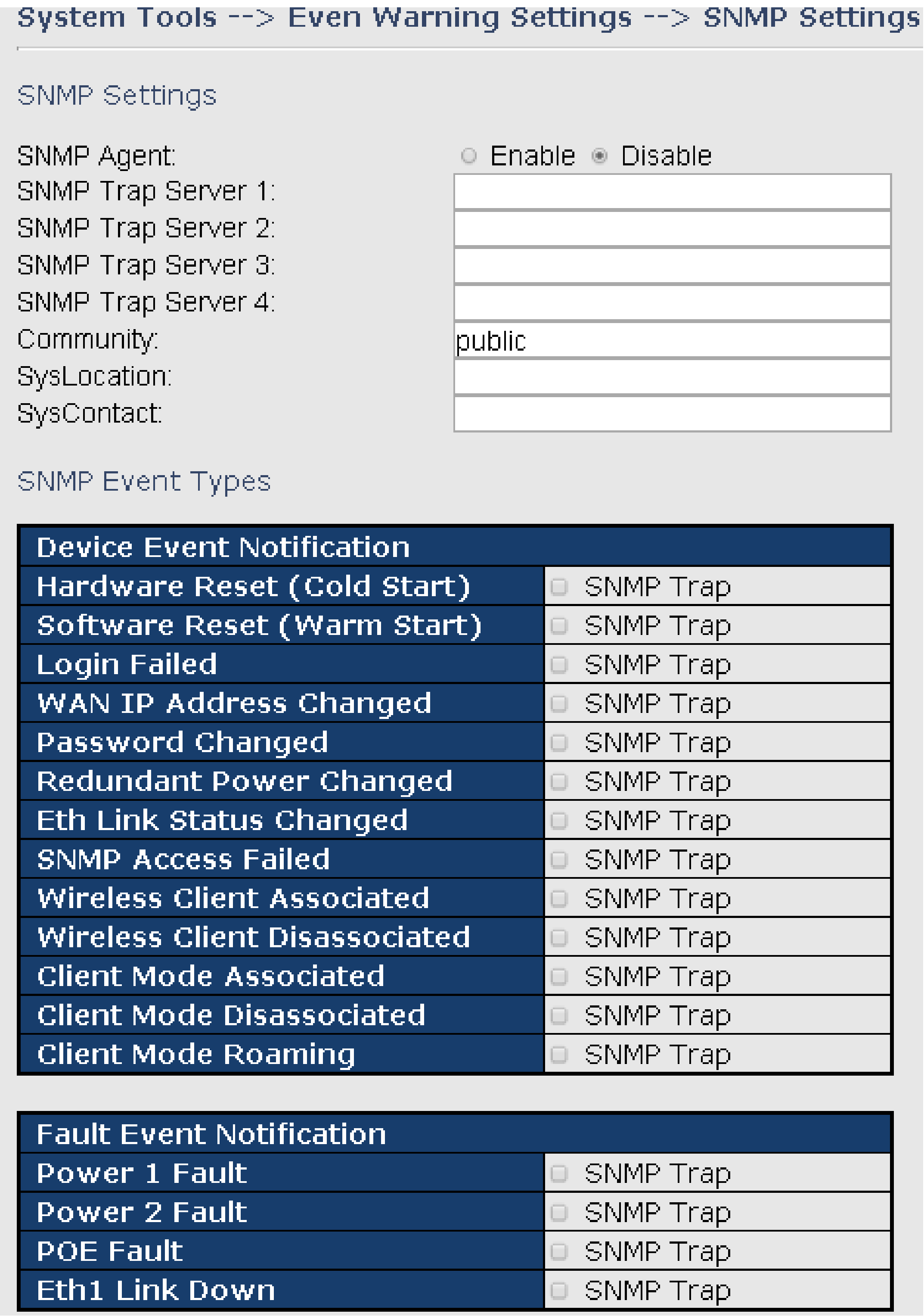
Device Event Notification	
Hardware Reset (Cold Start)	□ SMTP Mail
Software Reset (Warm Start)	□ SMTP Mail
Login Failed	□ SMTP Mail
WAN IP Address Changed	□ SMTP Mail
Password Changed	□ SMTP Mail
Redundant Power Changed	□ SMTP Mail
Eth Link Status Changed	□ SMTP Mail
SNMP Access Failed	□ SMTP Mail
Wireless Client Associated	□ SMTP Mail
Wireless Client Disassociated	□ SMTP Mail
Client Mode Associated	□ SMTP Mail
Client Mode Disassociated	□ SMTP Mail
Client Mode Roaming	□ SMTP Mail

Fault Event Notification	
Power 1 Fault	□ SMTP Mail
Power 2 Fault	□ SMTP Mail
POE Fault	□ SMTP Mail
Eth1 Link Down	□ SMTP Mail

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 1-4	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: public

SysLocation:

SysContact:

SNMP Event Types

Device Event Notification	
Hardware Reset (Cold Start)	□ SNMP Trap
Software Reset (Warm Start)	□ SNMP Trap
Login Failed	□ SNMP Trap
WAN IP Address Changed	□ SNMP Trap
Password Changed	□ SNMP Trap
Redundant Power Changed	□ SNMP Trap
Eth Link Status Changed	□ SNMP Trap
SNMP Access Failed	□ SNMP Trap
Wireless Client Associated	□ SNMP Trap
Wireless Client Disassociated	□ SNMP Trap
Client Mode Associated	□ SNMP Trap
Client Mode Disassociated	□ SNMP Trap
Client Mode Roaming	□ SNMP Trap

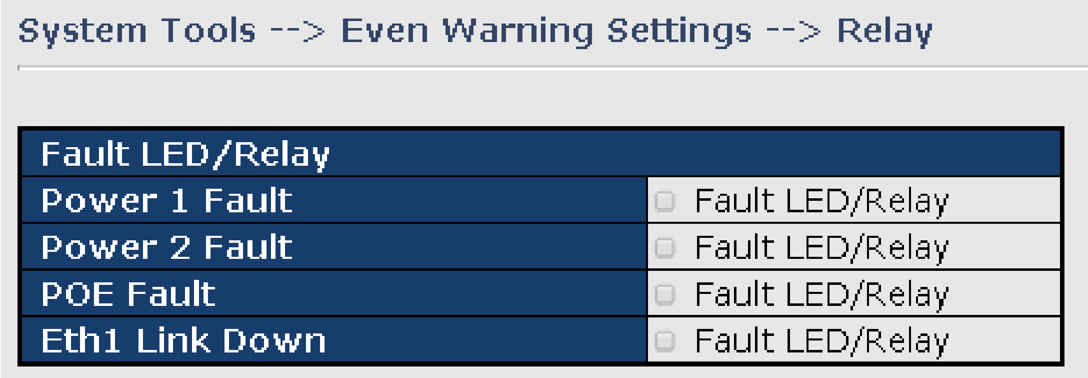
Fault Event Notification	
Power 1 Fault	□ SNMP Trap
Power 2 Fault	□ SNMP Trap
POE Fault	□ SNMP Trap
Eth1 Link Down	□ SNMP Trap

Label	Description
SNMP Agent	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.
SNMP Trap Server 1-4	Enter the IP address of the SNMP server which will send out traps generated by the AP.
Community	Community is a password to establish trust between managers and agents. Normally, **public** is used for read-write community.
SysLocation	Specifies sysLocation string
SysContact	Specifies sysContact string

Relay

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

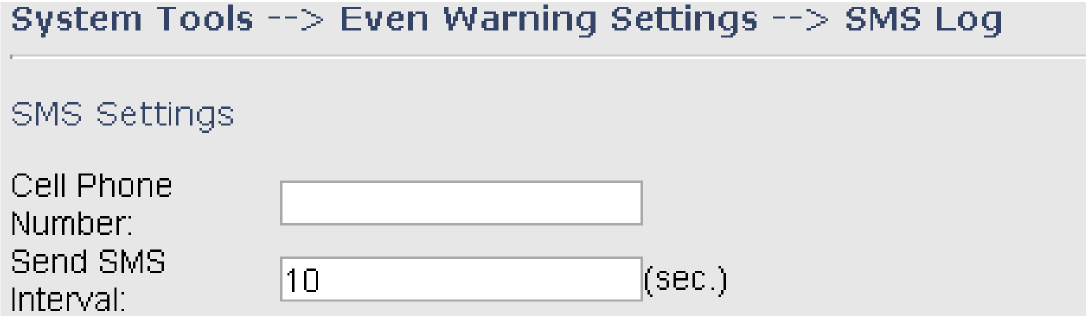


System Tools --> Even Warning Settings --> Relay

Fault LED/Relay	
Power 1 Fault	□ Fault LED/Relay
Power 2 Fault	□ Fault LED/Relay
POE Fault	□ Fault LED/Relay
Eth1 Link Down	□ Fault LED/Relay

SMS

You can configure the device to send notifications via SMS when the selected event occurs. You need to provide the phone number with which you want to receive the notifications and the time intervals between delivery attempts.

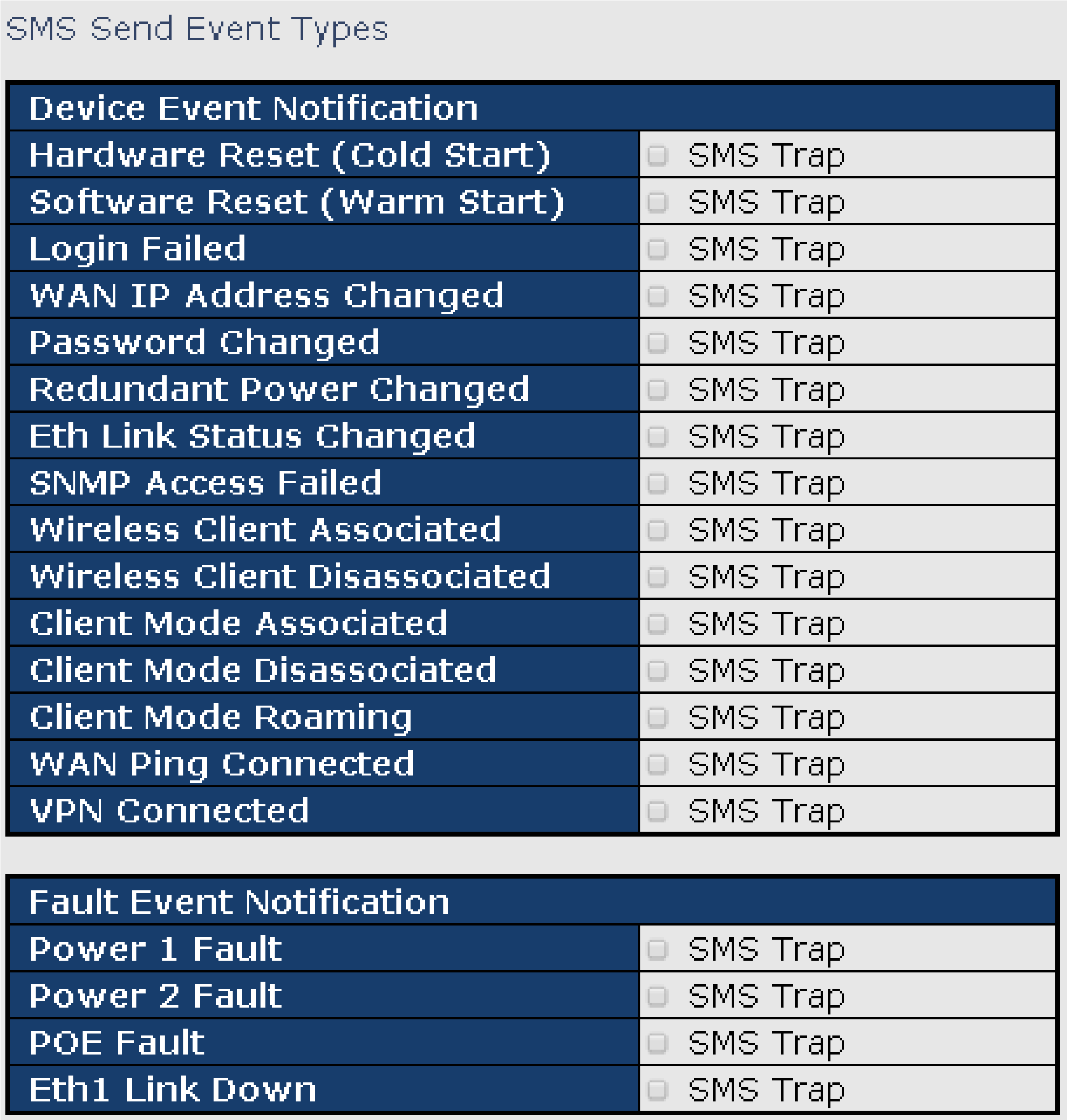


System Tools --> Even Warning Settings --> SMS Log

SMS Settings

Cell Phone Number:

Send SMS Interval: 10 (sec.)



SMS Send Event Types

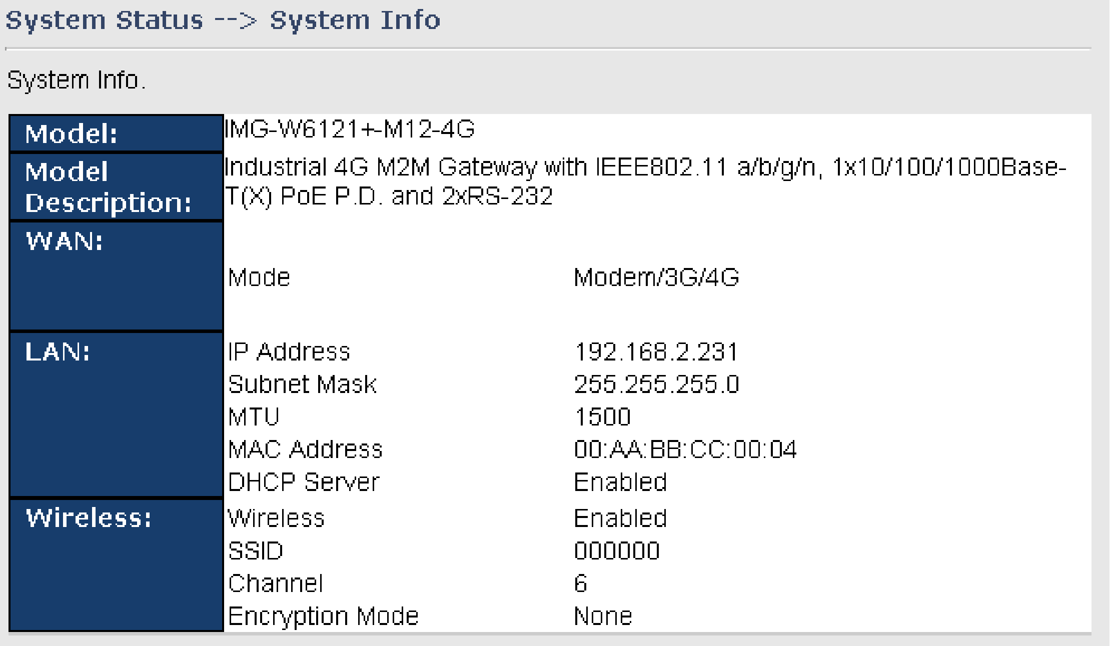
Device Event Notification	
Hardware Reset (Cold Start)	□ SMS Trap
Software Reset (Warm Start)	□ SMS Trap
Login Failed	□ SMS Trap
WAN IP Address Changed	□ SMS Trap
Password Changed	□ SMS Trap
Redundant Power Changed	□ SMS Trap
Eth Link Status Changed	□ SMS Trap
SNMP Access Failed	□ SMS Trap
Wireless Client Associated	□ SMS Trap
Wireless Client Disassociated	□ SMS Trap
Client Mode Associated	□ SMS Trap
Client Mode Disassociated	□ SMS Trap
Client Mode Roaming	□ SMS Trap
WAN Ping Connected	□ SMS Trap
VPN Connected	□ SMS Trap

Fault Event Notification	
Power 1 Fault	□ SMS Trap
Power 2 Fault	□ SMS Trap
POE Fault	□ SMS Trap
Eth1 Link Down	□ SMS Trap

5.2.4 System Status

System Info

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



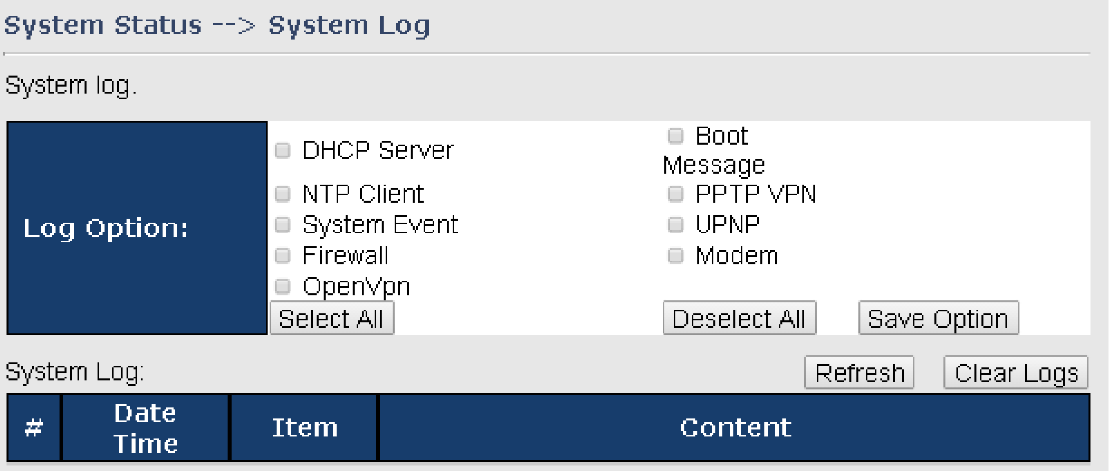
System Status --> System Info

System Info.

Model:	IMG-W6121+-M12-4G	
Model Description:	Industrial 4G M2M Gateway with IEEE802.11 a/b/g/n, 1x10/100/1000Base-T(X) PoE P.D. and 2xRS-232	
WAN:	Mode	Modem/3G/4G
LAN:	IP Address Subnet Mask MTU MAC Address DHCP Server	192.168.2.231 255.255.255.0 1500 00:AA:BB:CC:00:04 Enabled
Wireless:	Wireless SSID Channel Encryption Mode	Enabled 000000 6 None

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:

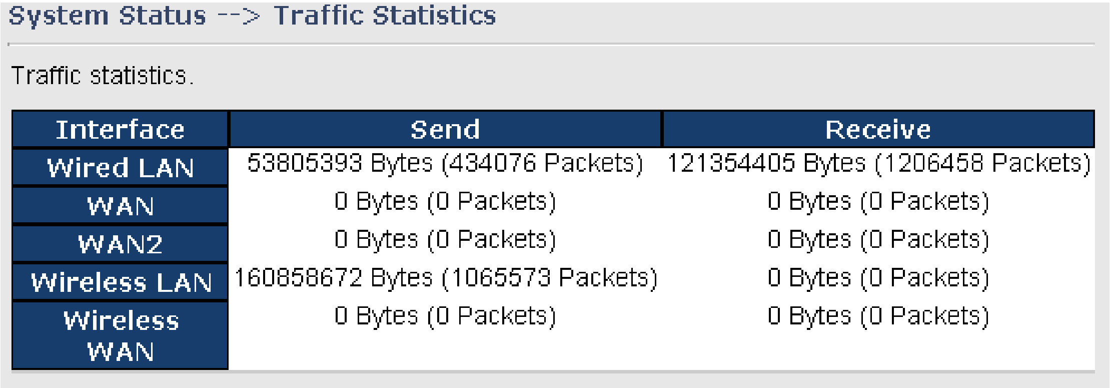
□ DHCP Server
□ NTP Client
□ System Event
□ Firewall
□ OpenVpn
□ Boot Message
□ PPTP VPN
□ UPNP
□ Modem

System Log:

#	Date Time	Item	Content

Traffic Statistics

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



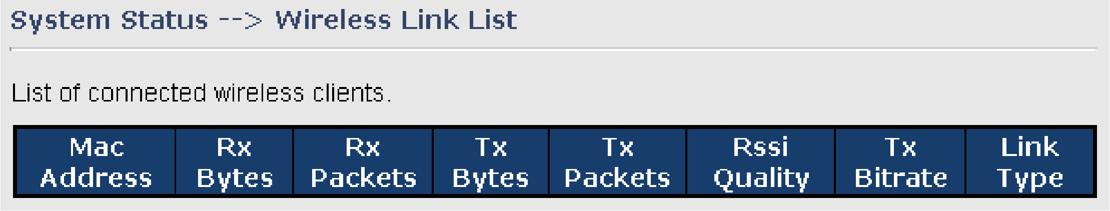
System Status --> Traffic Statistics

Traffic statistics.

Interface	Send	Receive
Wired LAN	53805393 Bytes (434076 Packets)	121354405 Bytes (1206458 Packets)
WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)
WAN2	0 Bytes (0 Packets)	0 Bytes (0 Packets)
Wireless LAN	160858672 Bytes (1065573 Packets)	0 Bytes (0 Packets)
Wireless WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)

Wireless Link List

This page displays the Mac address of all wireless clients connected.



System Status --> Wireless Link List

List of connected wireless clients.

Mac Address	Rx Bytes	Rx Packets	Tx Bytes	Tx Packets	Rssi Quality	Tx Bitrate	Link Type

Technical Specifications

ORing M2M Model	IMG-W6121+-3G-M12	IMG-W6121+-4G-M12
Physical Ports		
10/100/1000 Base-T(X) Ports in M12 Auto MDI/MDIX with PoE P.D.	**1 (8-pin M12 A-coding Female connector)**	
SIM card slot	**1**	
Cellular Interface		
Cellular Standard	GSM / GPRS / EGPRS / EDGE / WCDMA / HSDPA / HSUPA	GSM / GPRS / EGPRS / EDGE / WCDMA / HSDPA / HSUPA/LTE
Band options	**America(US)** UMTS/HSDPA/HSUPA/HSPA+/DC-HSPA+: 800/850/1900/2100 MHz GSM/GPRS/EDGE: 850/900/1800/1900 MHz **Europe(EU)** UMTS/HSDPA/HSUPA/HSPA+/DC-HSPA+: 900/2100 MHz GSM/GPRS/EDGE: 900/1800/1900 MHz	**America(US)** LTE: 700/1700/2100/ MHz UMTS/HSDPA/HSUPA/HSPA+/DC-HSPA+: 800/850/1900/2100 MHz GSM/GPRS/EDGE: 850/900/1800/1900 MHz **Europe(EU)** 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	N-type Female	
Antenna	GSM/DCS/UMT 3G antenna x1	GSM/DCS/UMT/LTE 4G antenna x1
WLAN Feature		
Antenna Connector	N-type Female	
Antenna	Wi-Fi ANT x2	
Radio Frequency Type	DSSS, OFDM	
Modulation	IEEE802.11a : OFDM with BPSK, QPSK, QAM, 64QAM IEEE802.11b: CCK, DQPSK, DBPSK IEEE802.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM IEEE802.11n : BPSK, QPSK, 16-QAM, 64-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	IEEE802.11b: 1 / 2 / 5.5 / 11 Mbps IEEE802.11a/g: 6 / 9 / 12 / 18 / 24 / 36 / 48 / 54 Mbps IEEE801.11n: up to 300Mbps	
Transmit Power	802.11a: 12dBm ± 1.5dBm 802.11b: 17dBm ± 1.5dBm 802.11g: 15dBm ± 1.5dBm 802.11gn HT20: 13dBm ± 1.5dBm@150Mbps 802.11gn HT40: 12dBm ± 1.5dBm@300Mbps 802.11an HT20: 12dBm ± 1.5dBm@150Mbps 802.11an HT40: 12dBm ± 1.5dBm@300Mbps	
Receiver Sensitivity	802.11a: -68dBm ± 2dBm@54Mbps 802.11b: -85dBm ± 2dBm@11Mbps 802.11g: -68dBm ± 2dBm@54Mbps 802.11gn HT20: -68dBm ± 2dBm@150Mbps 802.11gn HT40: -68dBm ± 2dBm@300Mbps	

	802.11an HT20: -68dBm ± 2dBm@150Mbps 802.11an HT40: -68dBm ± 2dBm@300Mbps
Encryption Security	WEP: (64-bit ,128-bit key supported) WPA/WPA2 : 802.11i(WEP and AES encryption) WPAPSK (256-bit key pre-shared key supported) 802.1X and Radius supported TKIP encryption
Wireless Security	SSID broadcast disable
Serial Ports	
Connector	2 (8-pin M12 A-coding Male connector)
Operation Mode	RS-232
Serial Baud Rate	110 bps to 115.2 Kbps
Data Bits	5, 6, 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, GND
LED Indicators	
Power indicator	Green On: Power is on and functioning Normally.
10/100/1000T M12 port indicator	Green for port Link/Act.
WLAN indicator	WLAN Link /ACT: Green: Link
Power	
Power Input	48VDC on PoE port compliant with IEEE802.3af standard
Power consumption (Typ.)	6.5 Watts
Overload current protection	Present
Physical Characteristic	
Enclosure	IP-67
Dimension (W x D x H)	250 (W) x 220 (D) x 87 (H) mm (9.84 x 8.66 x 3.4 inch)
Weight (g)	2653
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-25 to 70°C (-13 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	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	3 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 matérial 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 choisie que la puissance isotrope rayonnée équivalente (PIRE) est pas plus que celle premise 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.