TGAR-1062/2062/1662 Series

IEEE 802.11 a/b/g/n Access Point Router

User Manual

Version 1.1

July, 2014

www.oring-networking.com

COPYRIGHT NOTICE

TRADEMARKS

ORing is a registered trademark of ORing Industrial Networking Corp.

All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

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

WARRANTY

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

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

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

CONTACT INFORMATION

ORing Industrial Networking Corp.
3F., No.542-2, JhongJheng Rd., Sindian District, New Taipei City 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 TGAR-1062/2062/1662 Series 1
1.2 Software Features 1
1.3 Hardware Features 2
2.1 Front Panel 3
2.1.1 Ports and Connectors 3
2.1.2 Front Panel LEDs 5
2.2 Side Panel 5
2.2 Top Panel 6
2.3 Bottom Panel 7

Hardware Installation 8
3.1 Wall Mounting Installation 8
3.2 Wiring 11
3.2.1 Grounding 11
3.2.2 Fault Relay 11
3.2.3 Redundant Power Inputs 12

Cables and Antenna 13
4.1 Ethernet Pin Definition 13
4.2 Console Port Pin Definition 13
4.3 DI/DO 14
4.4 Wireless Antenna 14
4.5 Cellular Antenna 15

Management 16
5.1 Network Connection 16
5.2 Configuration 17
5.2.1 Basic Setting 17
WAN 18
LAN 22
DHCP 22
Wireless AP 24
DDNS 30
Date & Time 30
5.2.2 Networking Setting 31
Wireless Setting – Advanced Setting 31
Wireless Setting – MAC Filter 33
NAT Setting - Virtual Server 34
NAT Setting – DMZ 35
NAT Setting – UPnP 35

Firewall Setting – IP Filter 36
Firewall Setting – MAC Filter 37
Vpn Setting – Open Vpn 38
Vpn Setting – PPTP VPN 40
Vpn Setting – PPTP Client 42
VRRP 43
Routing Protocol – Routing Setting 45
5.2.3 System Tools 48
Login Setting 48
Router Restart 48
Firmware Upgrade 49
Save/Restore Configurations 49
Miscellaneous 50
GPS 51
Event Warning 52
E-mail 53
DIDO 56
5.2.4 System Status 57
System Info 57
System Log 57
Traffic Statistics 57
Wireless Link List 58

Technical Specifications 59

Compliance 64

Getting Started

1.1 About TGAR-1062/2062/1662 Series

Designed for industrial and rolling stock wireless applications with two LAN ports in M12 connectors and EN50155 compliance, the ORing TGAR-1062/2062/1662 series are IEEE802.11 a/b/g/n routers capable of providing a fast and effective way to communicate with the Internet over wired or wireless LANs. Consisting of 3G and 4G models, the series of devices can be configured to operate in 3 modes of routing function: dynamic/static IP route, PPPoE authentication, and cellular modem dial up. Users can set up WLAN environment to fulfill demands of various applications rapidly by dialing up cellular modem. With dual Ethernet ports in switch mode, you can use Daisy Chain to reduce the usage of Ethernet switch ports. The router also provides VPN capabilities which create encrypted virtual tunnels on the Internet, allowing remote or mobile users to connect to the network of your office.

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 authentication
- Secure management by HTTPs
- Various kinds of WAN connections supported, including dynamic/static IP, PPPoE, and modem dial up
- Configurable IP tables to prevent unauthorized access
- Supports VPN for secure network connection (Open VPN , PPTP VPN)
- Supports NAT setting (virtual server , port trigger , DMZ , UPnP)
- Supports DHCP forwarding through PPTP
- 3.5G HSDPA modem dial up (3G models)
- 4G LTE modem dial up (4G models)
- Supports redundant mode (Recovery time < 10ms) and switch mode in M12 connector (A-coding)
- Wireless connection status monitoring
- Event warning by Syslog, e-mail, SNMP trap, and relay output

1.3 Hardware Features

- 2 x 10/100/1000 Base-T(X) Ethernet ports in M12 connectors
- 2 x WLAN antenna connectors (TGAR-1062/2062 series) or 4 x WLAN antenna connectors (TGAR-1662 series)
- 1 x cellular antenna connectors (TGAR-1062/1662 series) or 2 x cellular antenna connectors (TGAR-2062 series)
- EN50155 compliance
- Fully Compliant with IEEE802.3af (Power Device at ETH2, WAN port,TGAR-1062+、TGAR2062+、TGAR-1662+ supported)
- Redundant power inputs: 12~48 VDC
- Casing: IP-40
- Dimensions: 125.6mm (W) x 65mm (D) x 196.1mm (H) (4.94 x 2.55 x 7.72 inch)
- Operating temperature: -25 to 70°C
- Storage temperature: -40 to 85°C
- Operating humidity: 5% to 95%, non-condensing
- Wall mounting enabled

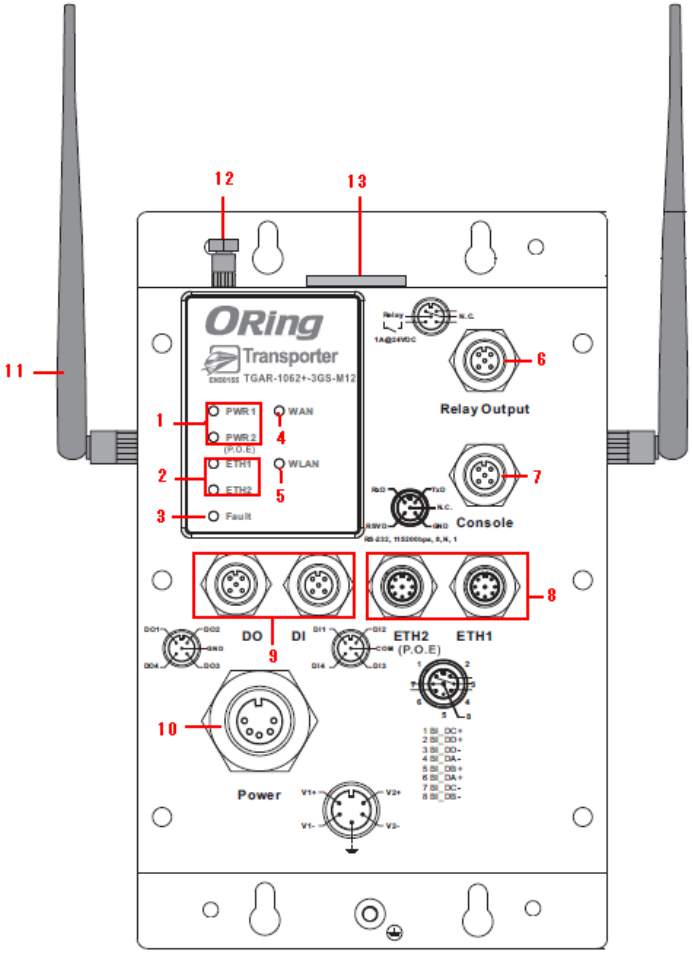
Hardware Overview

2.1 Front Panel

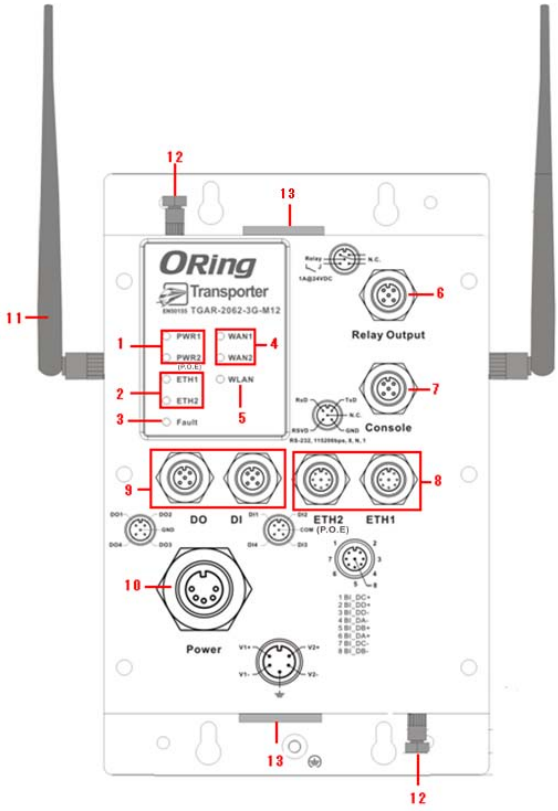
2.1.1 Ports and Connectors

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

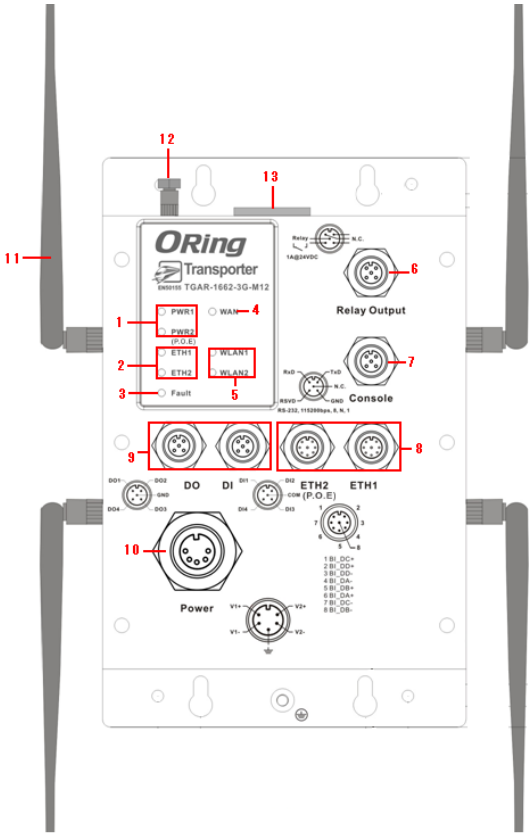
Port	Description
10/100/1000 Base-T(X) Ethernet ports with M12 connectors (D-coding)	2 x 10/100/1000 Base-T(X) ports supporting auto-negotiation.
Relay output with M12 (A-coding) connector	1 x relay output to carry capacity of 1A at 24VDC
M23 power connector with redundant power inputs	Dual power inputs for 12~48 VDC
DIDO with M12 connector (D-coding)	4 x digital input / 4 x digital output



TGAR-1062 Series



TGAR-2062 Series



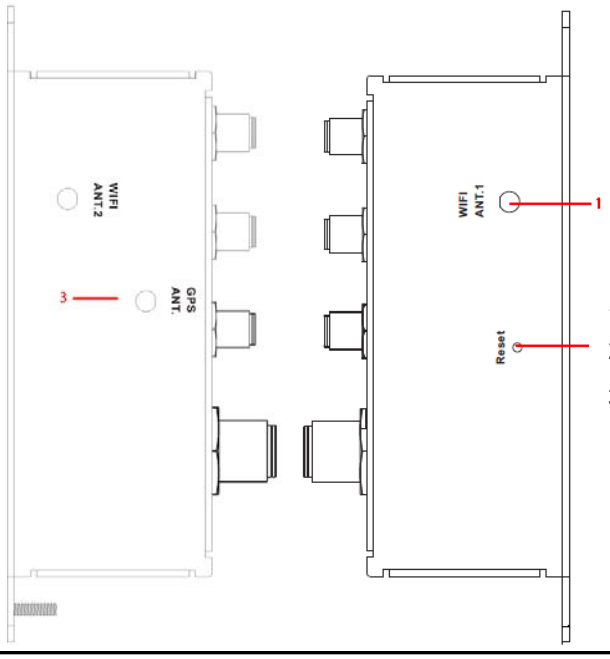
TGAR-1662 Series

1. Power status LED
2. LAN port status LED
3. Fault status LED
4. WAN status LED
5. WLAN status LED
6. Relay output port
7. Console & Backup unit port
8. Ethernet LAN ports
9. DI/DO ports
10. Power connector
11. 2.4/5GHz antenna
12. Cellular antenna connector
13. SIM card slot

2.1.2 Front Panel LEDs

LED	Color	Status	Description
PWR1	Green	On	DC power 1 activated.
PWR2	Green	On	DC power 2 activated.
ETH1	Green	On	Port is linked
		Blinking	Data transmitted.
ETH2	Green	On	Port is linked
	Green	Blinking	Transmitting data
		On	Port is linked
WLAN 1 (2)	Green	On	WLAN is activated
		Blinking	Transmitting data
WAN1 (2)	Green	On	Modem is connected
Fault	Red	On	Error occurs (power fails or port disconnected)

2.2 Side Panel

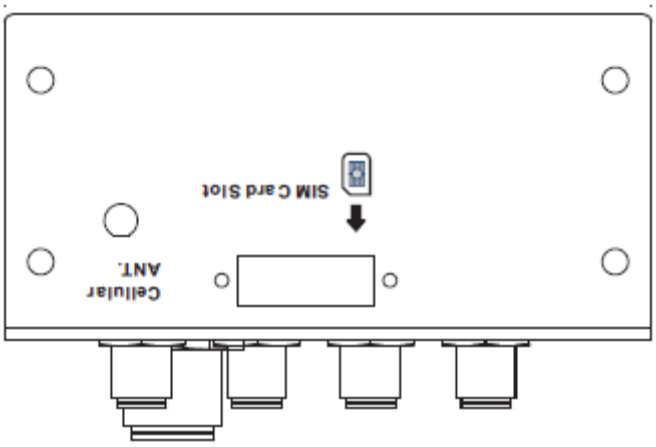


1. Antenna connector
2. Reset button
3. GPS Antenna(3GS/4GS Series)

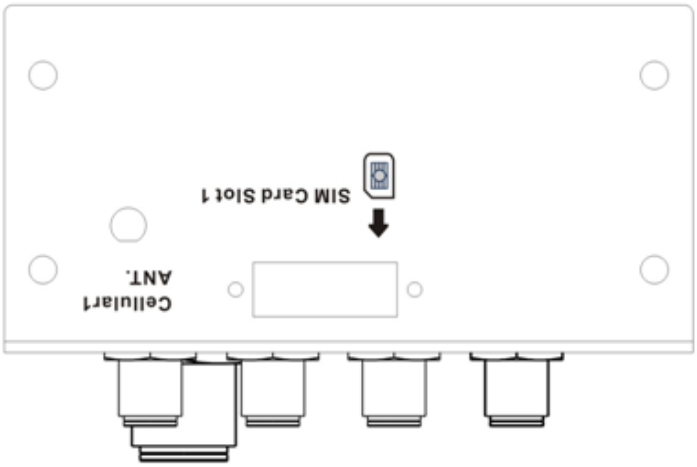
Note: to restore the device configurations back to the factory defaults, press the Reset button for a few seconds. Once the power indicator starts to flash, release the button. The device will then reboot and return to factory defaults.

2.2 Top Panel

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

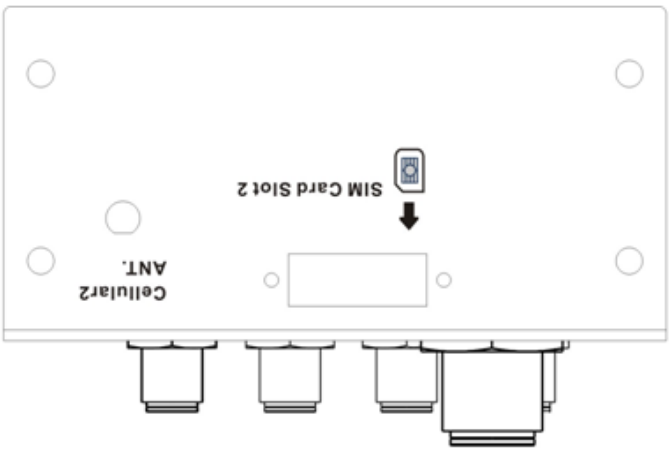


TGAR-1062/1662 Series



TGAR-2062 Series

2.3 Bottom Panel



TGAR-2062 Series

Hardware Installation

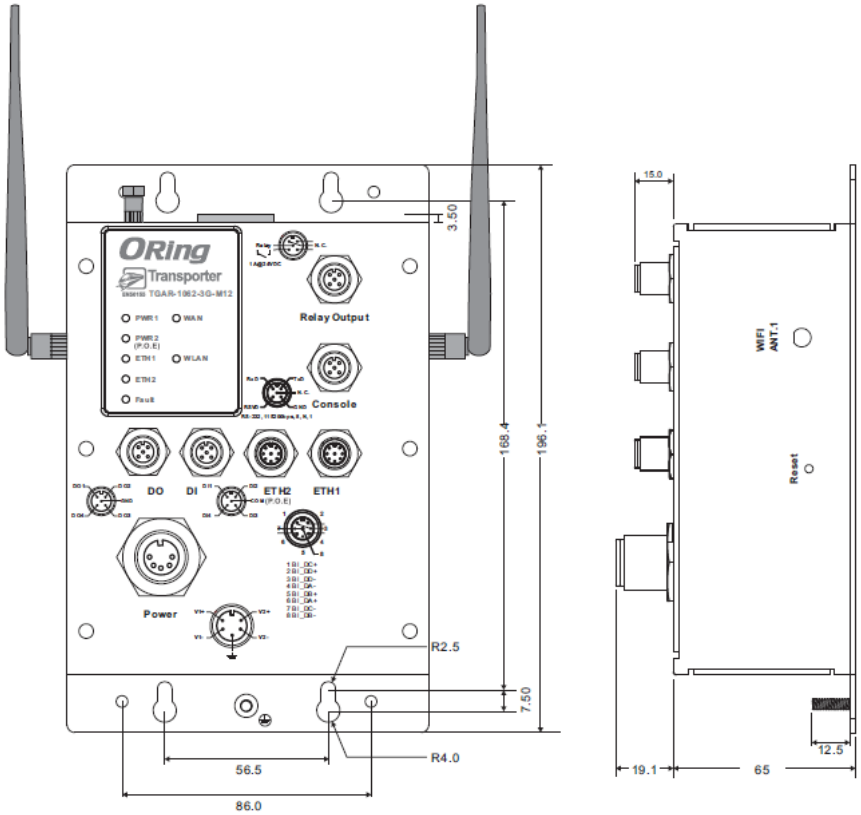
Elevated Operating Ambient: If installed in a closed environment, make sure the operating ambient temperature is compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Reduced Air Flow: Make sure the amount of air flow required for safe operation of the equipment is not compromised during installation.

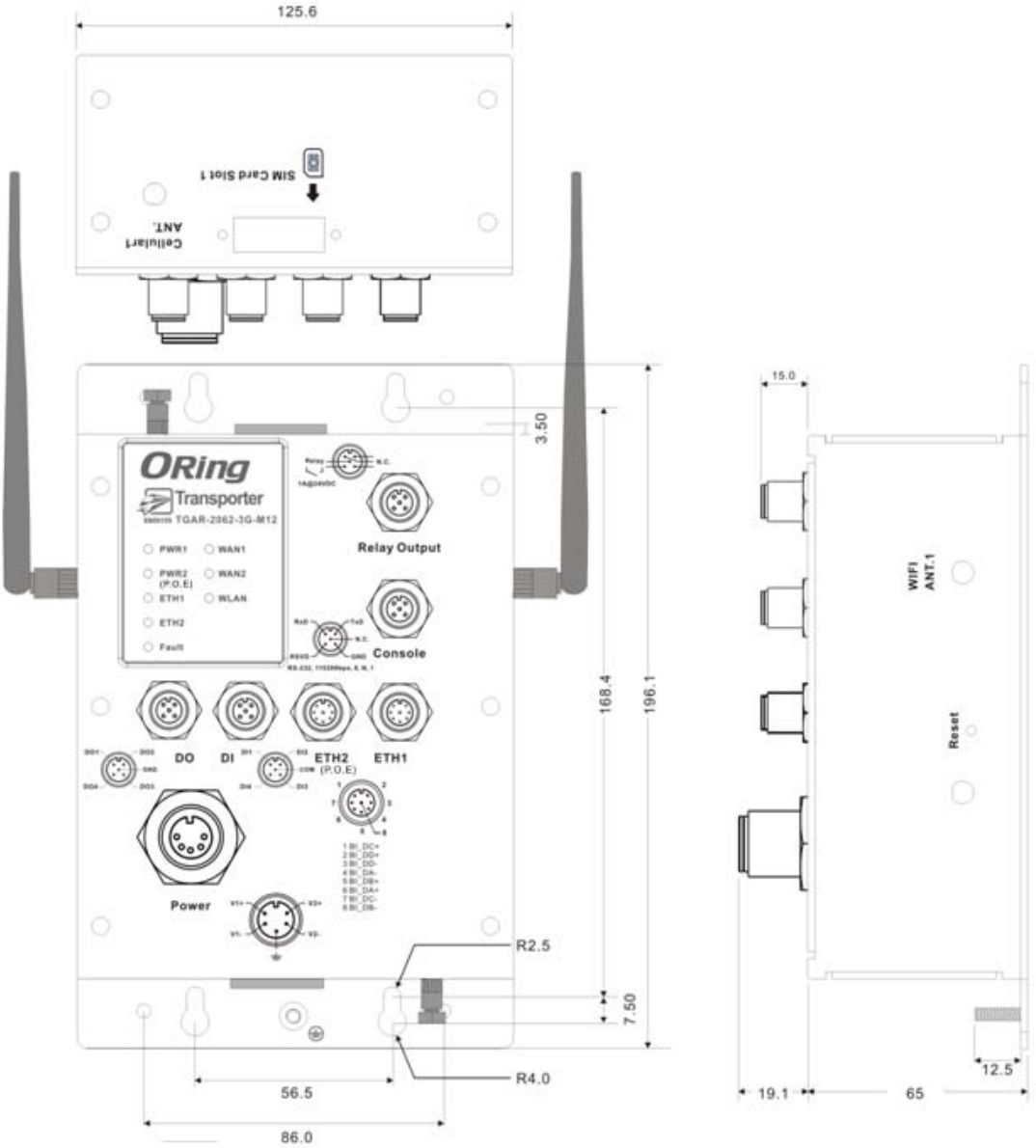
Mechanical Loading: Make sure the mounting of the equipment is not in a hazardous condition due to uneven mechanical loading.

Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

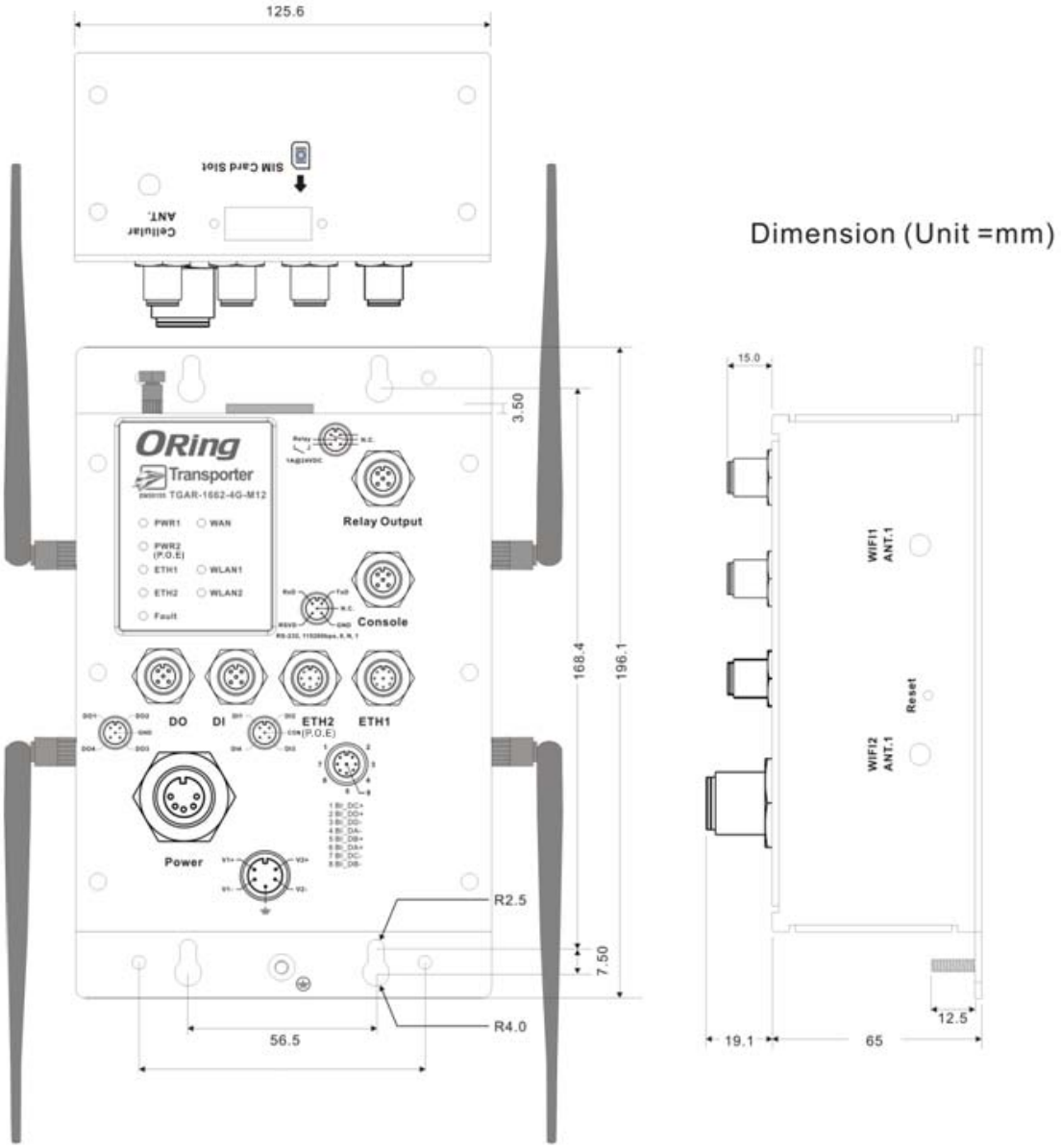
3.1 Wall Mounting Installation



TGAR-1062 Series Wall-mount Kit Measurement



TGAR-2062 Series Wall-mount Kit Measurement



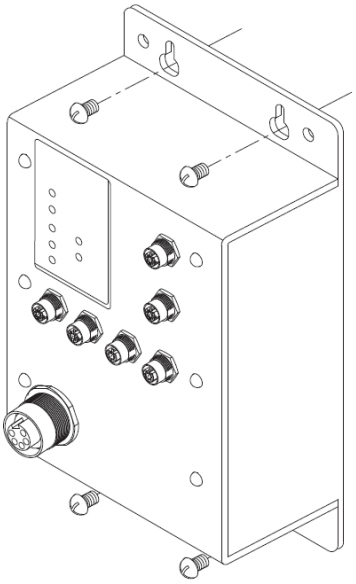
TGAR-1662 Series Wall-mount Kit Measurement

The device can be fixed to the wall. Follow the steps below to install the device on the wall.

Step 1: Hold the router upright against the wall

Step 2: Insert four screws through the large opening of the keyhole-shaped apertures at the top and bottom of the unit and fasten the screw to the wall with a screwdriver.

Step 3: Slide the router downwards and tighten the four screws for added stability.



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 switch between the wall and the screws.

3.2 Wiring

WARNING

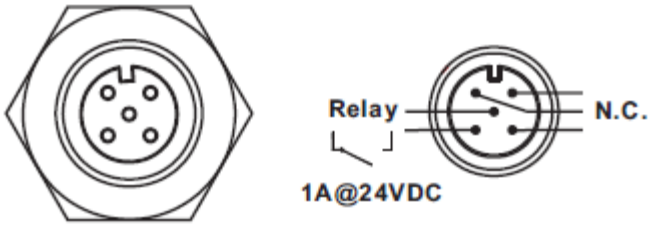
Be sure to switch off the power and make sure the area is not hazardous before disconnecting modules or wires. The devices may only be connected to the supply voltage shown on the type plate.

3.2.1 Grounding

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

3.2.2 Fault Relay

The router uses a M12 A-coded 5-pin male connector on the front panel for relay output. Use a power cord with an M12 A-coded 5-pin female connector to connect the relay. The relay contacts will detect user-configured events and form an open circuit when an event is triggered.

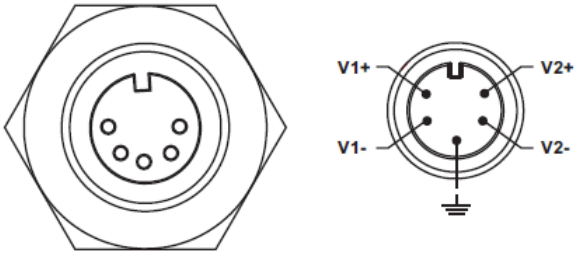


3.2.3 Redundant Power Inputs

The device supports two sets of power supplies and uses the M23 5-pin female connector on the front panel for the dual power inputs.

Step 1: Insert a power cable to the power connector on the device.

Step 2: Rotate the outer ring of the cable connector until a snug fit is achieved. Make sure the connection is tight



ATTENTION

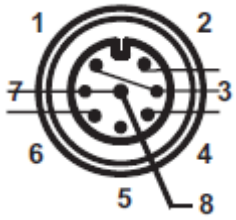
1. Be sure to disconnect the power cord before installing and/or wiring your routers.
2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
3. If the current goes above the maximum ratings,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

Cables and Antenna

4.1 Ethernet Pin Definition

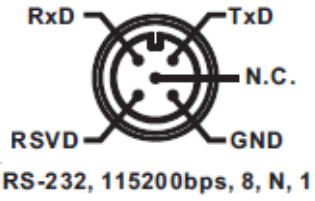
The routers have two 10/100/1000 Base-T(X) Ethernet ports. According to the link type, the AP uses CAT 3, 4, 5, 5e, UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

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

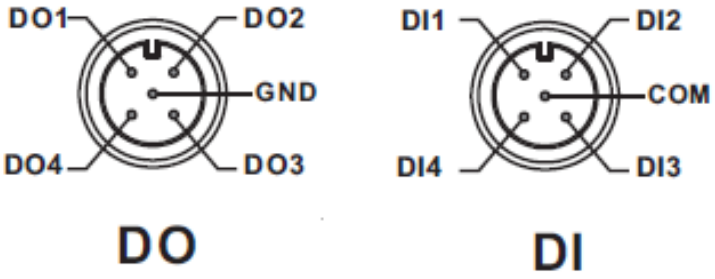


PIN	Definition
1	BI_DC+
2	BI_DD+
3	BI_DD-
4	BI_DA-
5	BI_DB+
6	BI_DA+
7	BI_DC-
8	BI_DB-

4.2 Console Port Pin Definition

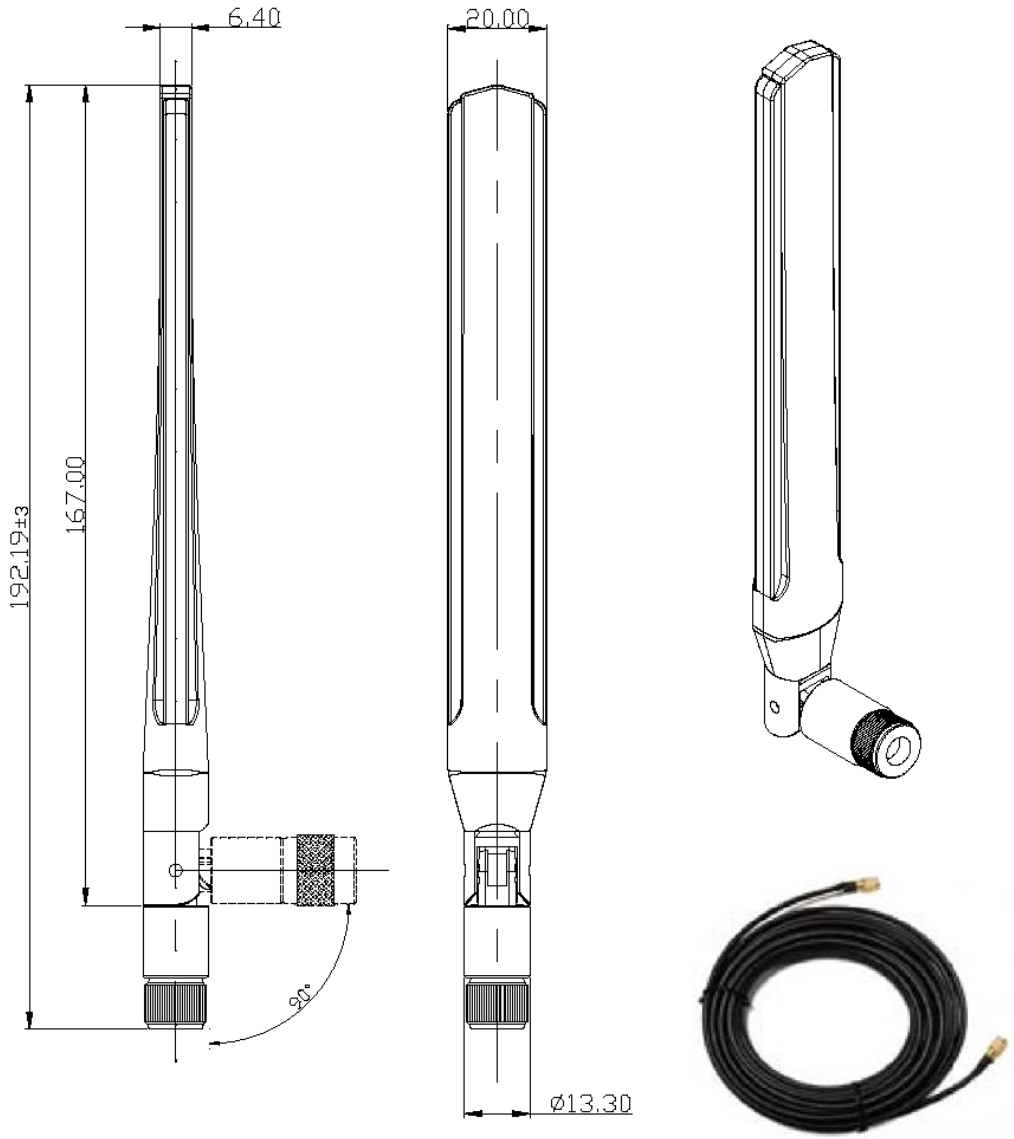


4.3 DI/DO



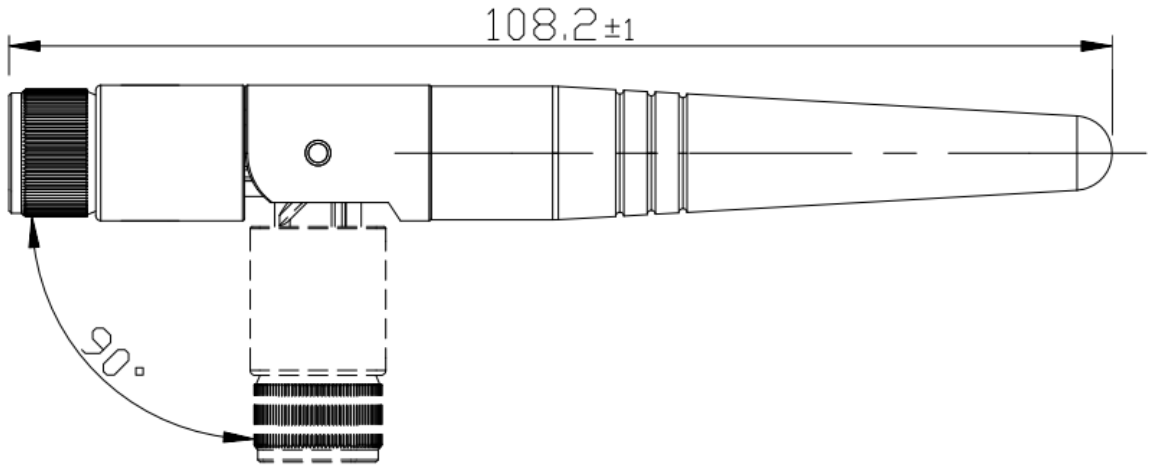
4.4 Wireless Antenna

The series uses 2.4GHz/5GHz antennas with reversed SMA connectors. You can also use external RF cables and antennas with the connectors.

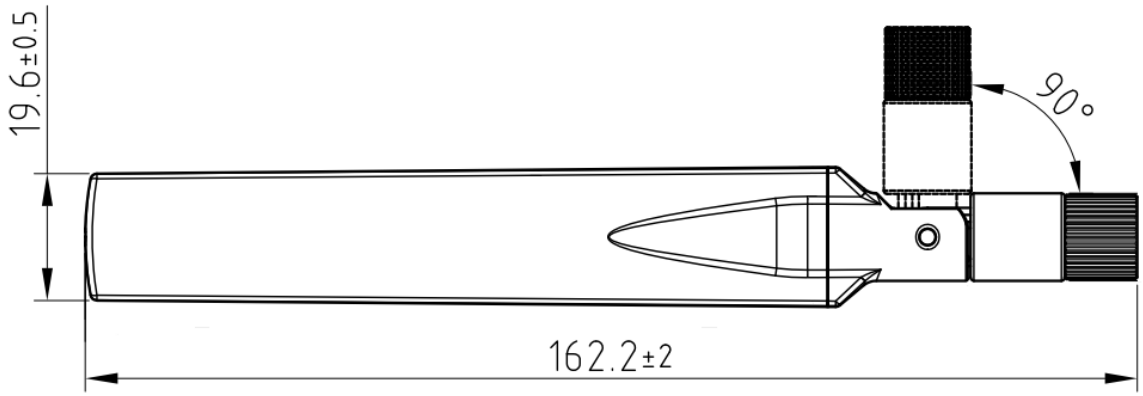


4.5 Cellular Antenna

The series are packed with one or two 3G and 4G antennas. External RF cables and antennas can also be used with the connector.



3G Cellular Antenna

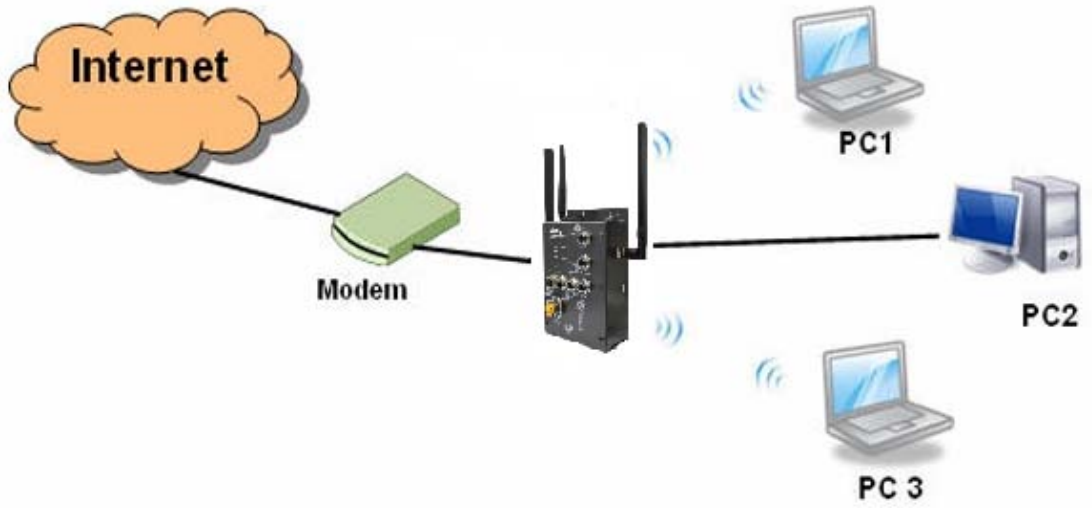


4G LTE Antenna

Management

5.1 Network Connection

Before installing the router, you need to be able to access the router 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.



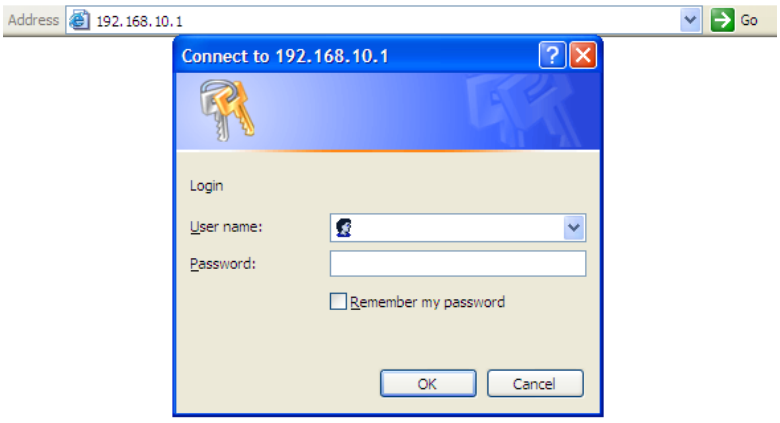
Network Connection of the Router

Before installing the router, you need 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. Follow the steps below to install and connect the router to PCs:

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

Step 2: Connect a computer to the router. Use either a straight-through Ethernet cable or cross-over cable to connect the ETH1 port of the router to a computer. Once the LED of the LAN port lights up, which indicates the connection is established, the computer will initiate a DHCP request to retrieve an IP address from the AP router.

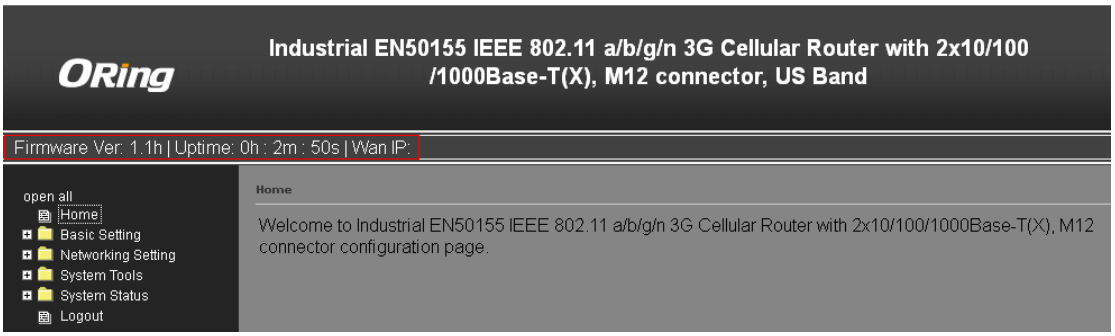
Step 3: Configure the router on a web-based management utility. Open a web browser on your computer and type http://192.168.10.1 (default gateway IP of the router) in the address box to access the webpage. A login window will pop up where you can enter the default login name **admin** and password **admin**.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



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

5.2 Configuration

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



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

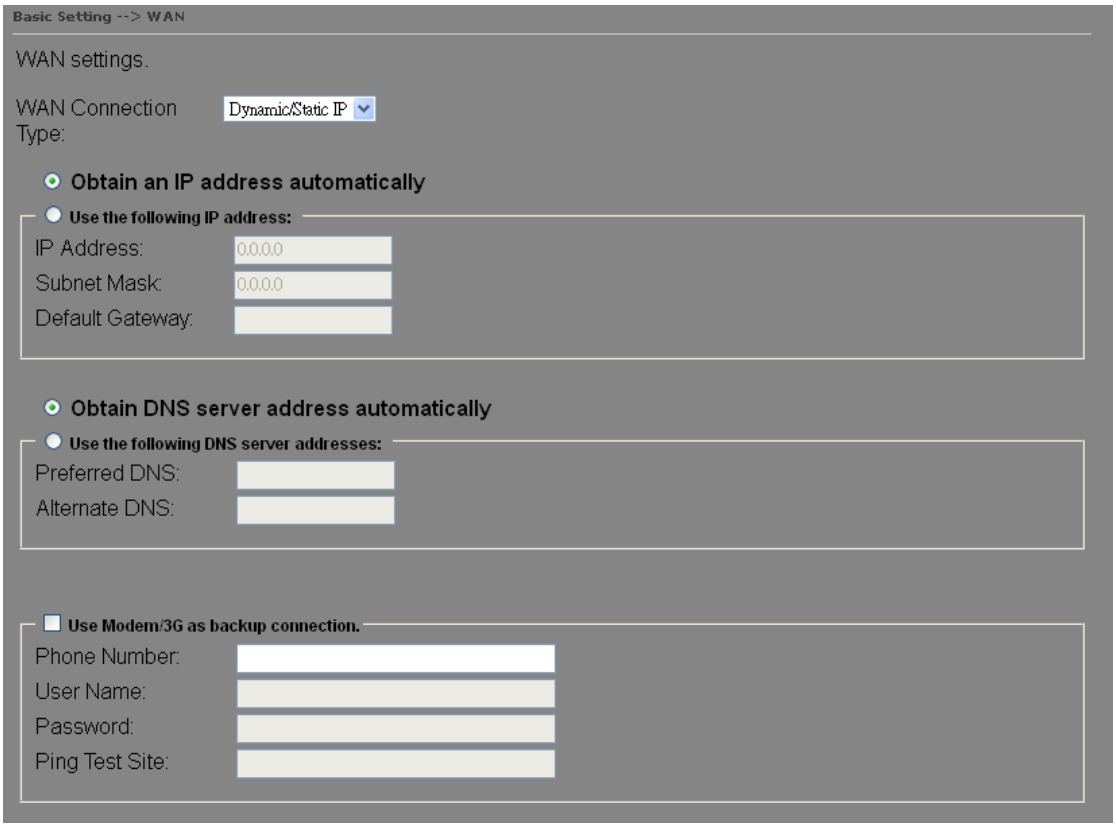
5.2.1 Basic Setting

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

WAN

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

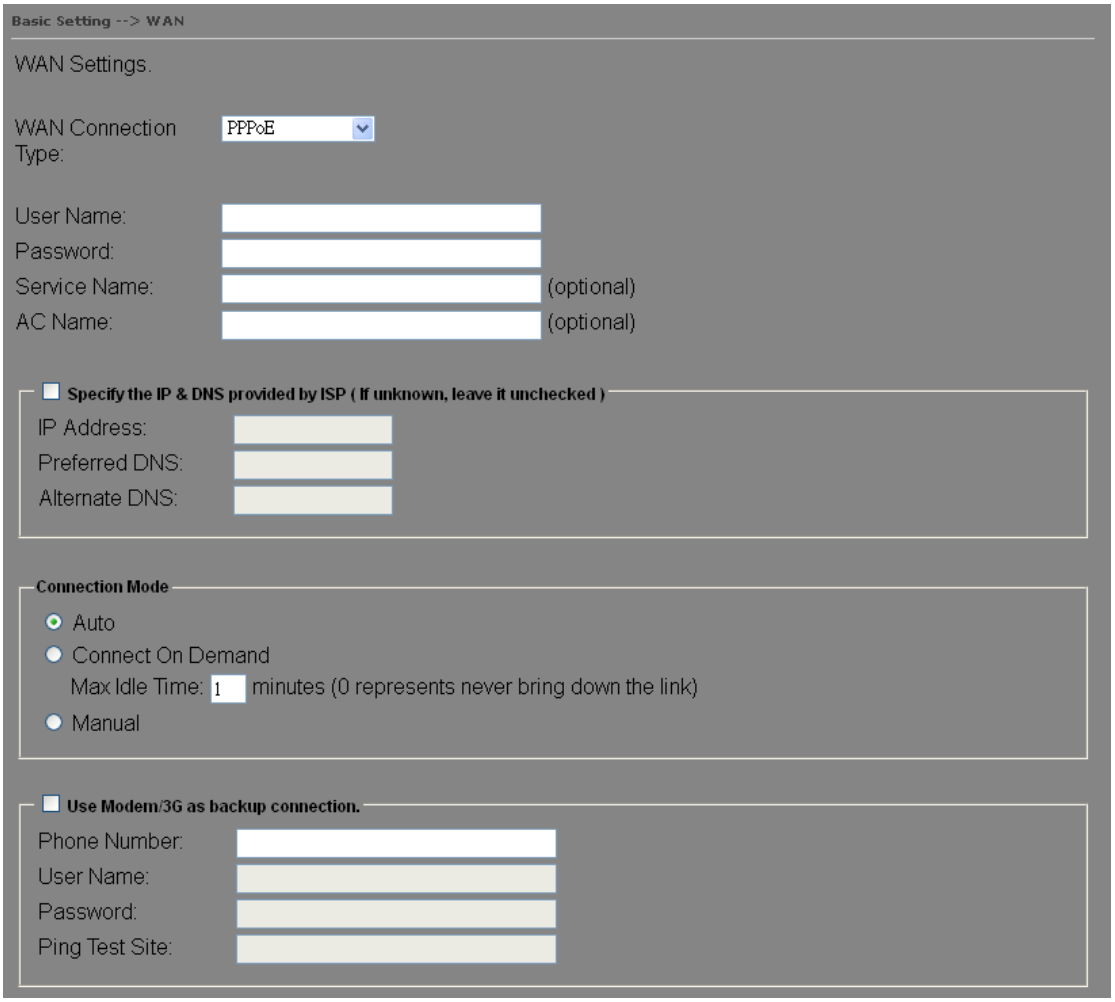
WAN Connection Type as Dynamic/Static IP:



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.
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.

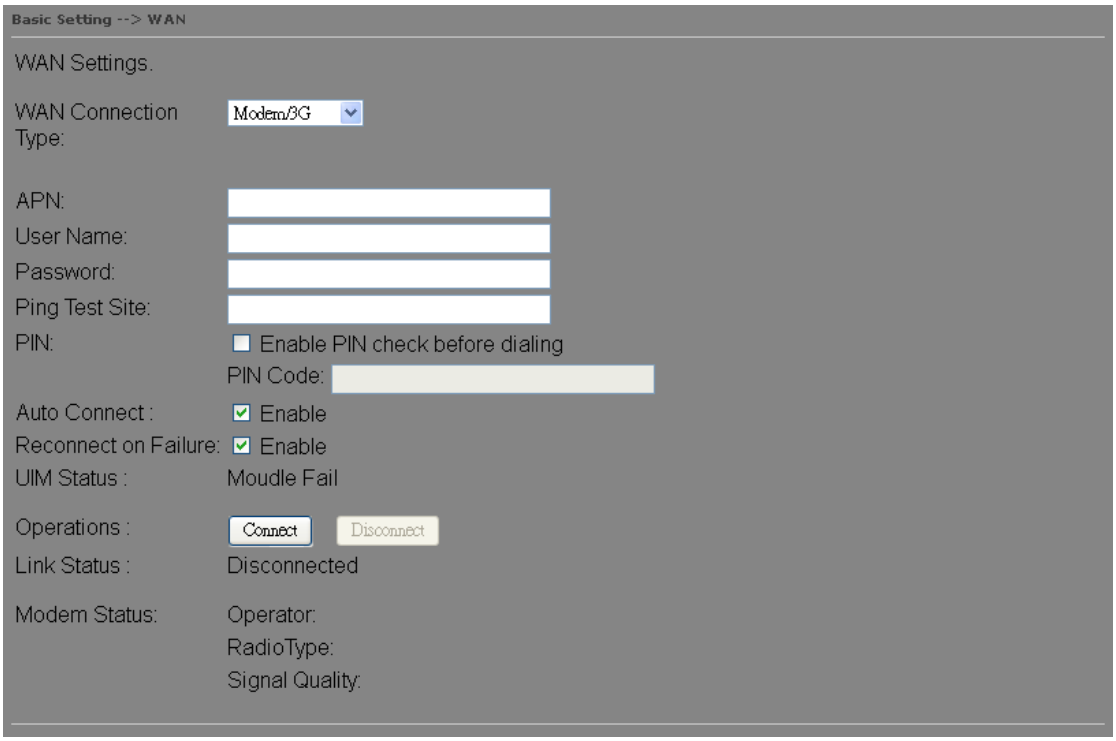
WAN Connection Type as PPPoE:



Label	Description
User Name / Password	Enter the username & password provided by your ISP.
Service Name	Enter the service name provided by your ISP
AC Name	Enter the name of the access concentrator provided by your ISP
Specify the IP & DNS provided by ISP	Enter a static IP and DNS address required by other ISPs
Connection Mode	**Auto**: connect automatically when the router boots up **Connect on Demand**: disconnect the PPP session if the router

	has had no traffic for a specified amount of time. Fill a number in the Max Idle Time field. **Manual**: connects or disconnects manually via the Connect/Disconnect buttons at the end of the page
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.

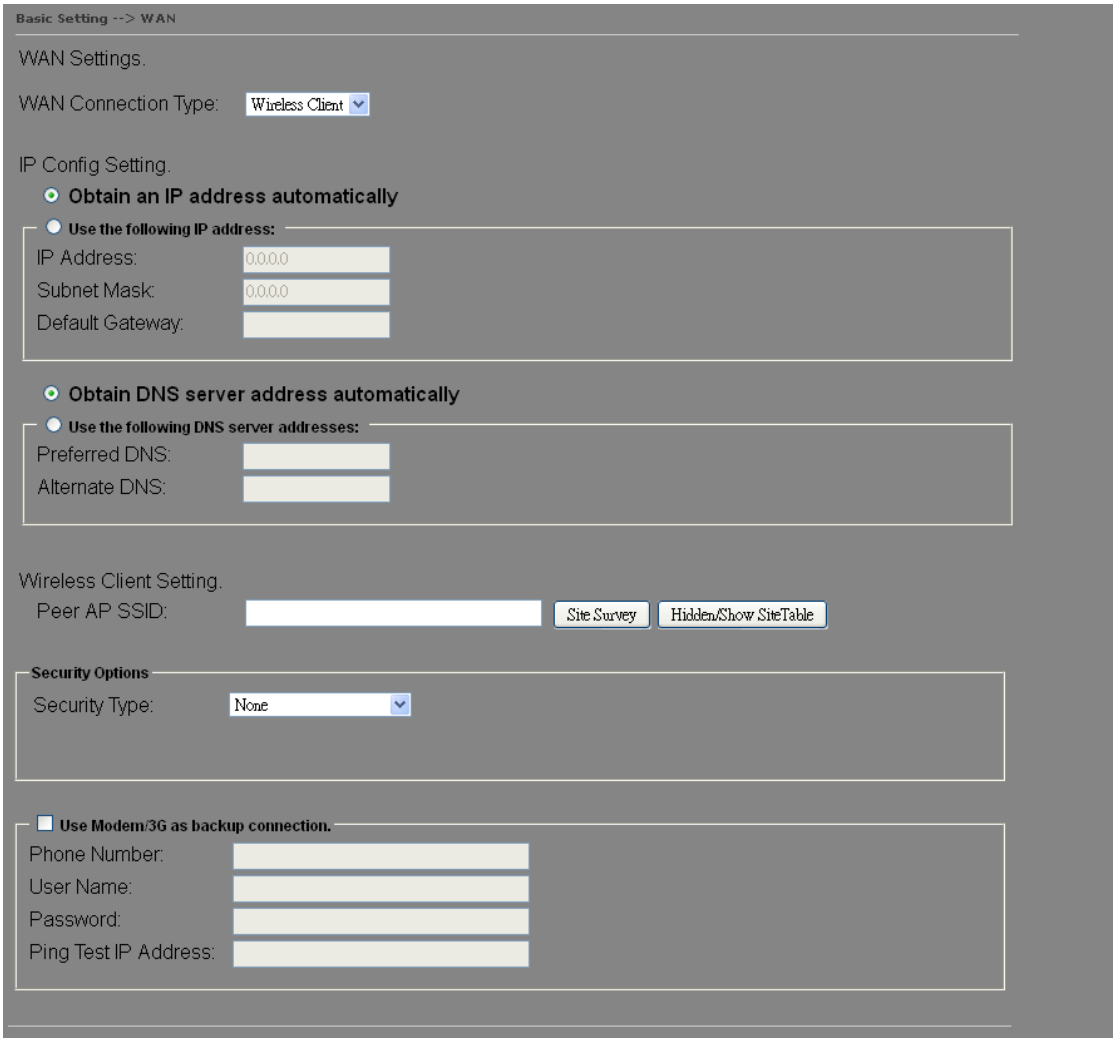
WAN Connection Type as Modem/3G/4G



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
PIN	Enter a PIN code if you want to perform PIN check
Auto Connect	Check to start connections when the router boots up
Reconnect on Failure	Check to allow for reconnection when links fail
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



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	Obtains a DNS server address from a DHCP server. If you have

address automatically	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 Type	Select the security type used by the client you want to connect
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 router. The LAN IP address is private to your internal network and is not visible to Internet.

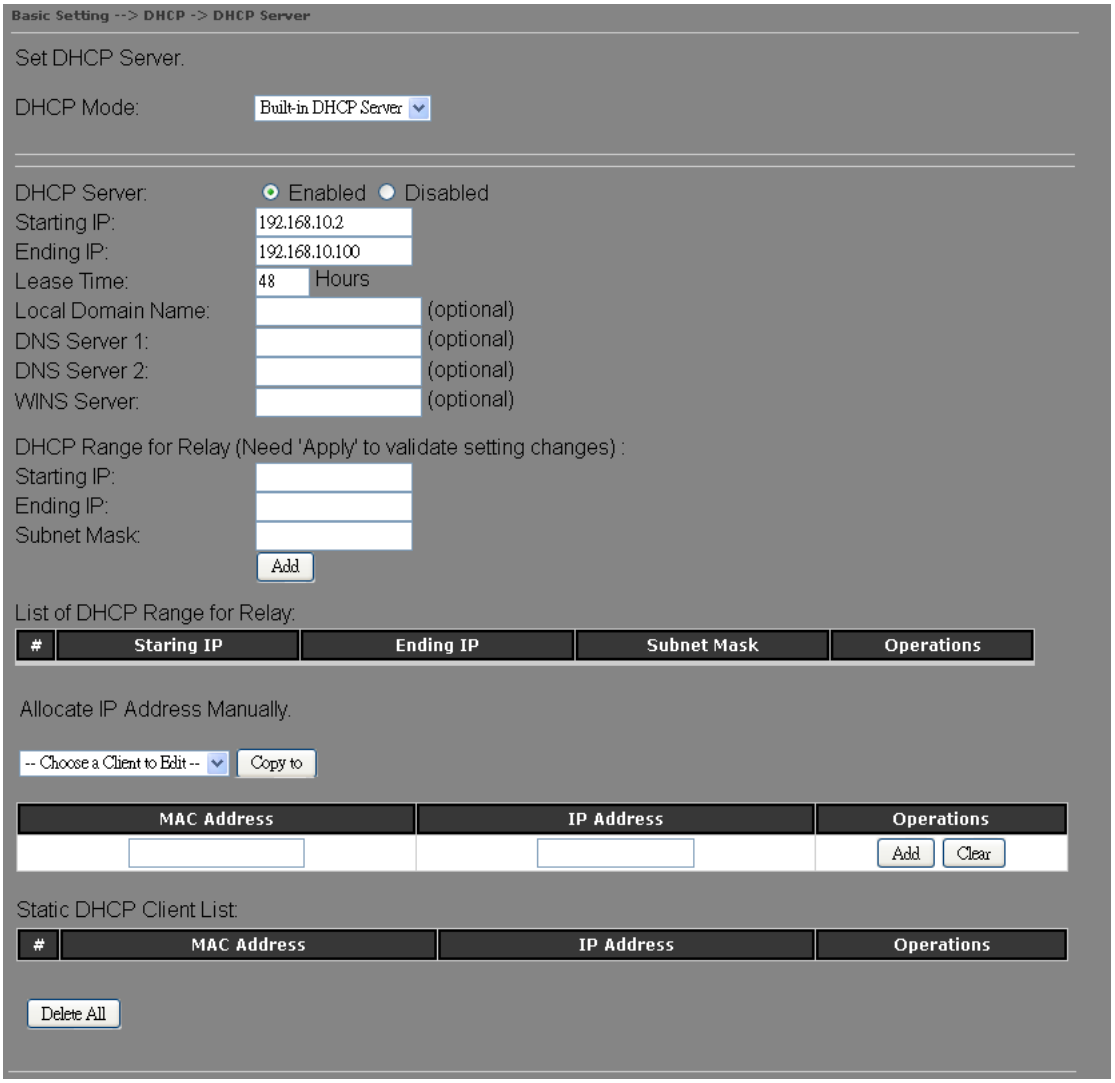
Label	Description
Router Name	Enter the name of your router
IP Address	The IP address of the LAN. The default value is **192.168.10.1**
Subnet Mask	The subnet mask of the LAN. The default value is **255.255.255.0**
LLDP Protocol	LLDP is a vendor-neutral protocol used by network devices for advertising 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 router comes with a built-in DHCP (Dynamic Host Control Protocol) server which assigns an IP address to a computer (DHCP client) on the LAN automatically. The router can also serve as a relay agent which will forward DHCP requests from DHCP clients to a DHCP server on the Internet.

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

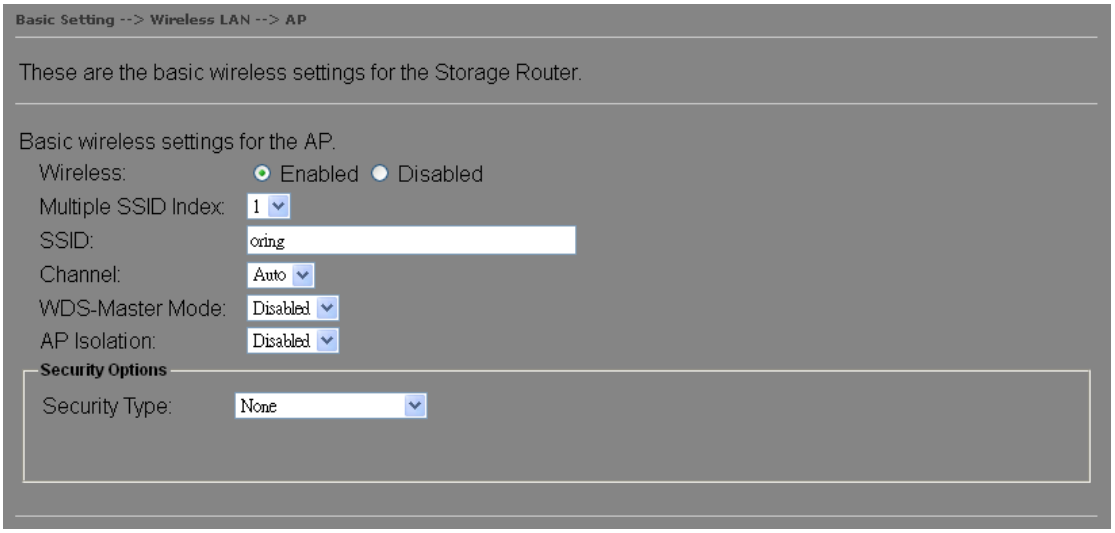


Label	Description
DHCP Mode	Available options include **Built-in DHCP Server** and **DHCP Forwarder**. **Built-in DHCP Server** will enable the router to automatically assign an IP address to a computer on the LAN.

	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.
DHCP Server	Enables or disables the DHCP server function. The default setting is **Enabled**.
Starting IP	The starting IP address of the IP range assigned by the DHCP server
Ending IP	The ending IP address of the IP range assigned by the DHCP server
Lease Time	The period of time for the IP address to be leased. During the lease time, the DHCP server cannot assign that IP address to any other clients. Enter a number in the field. The default setting is 48 hours.
Local Domain Name	Enter the local domain name of a private network (optional)
DNS Server 1&2	Enter the IP address for the DNS server (optional)
WINS Server	Enter the WINS server (optional)
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 router 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

Wireless AP

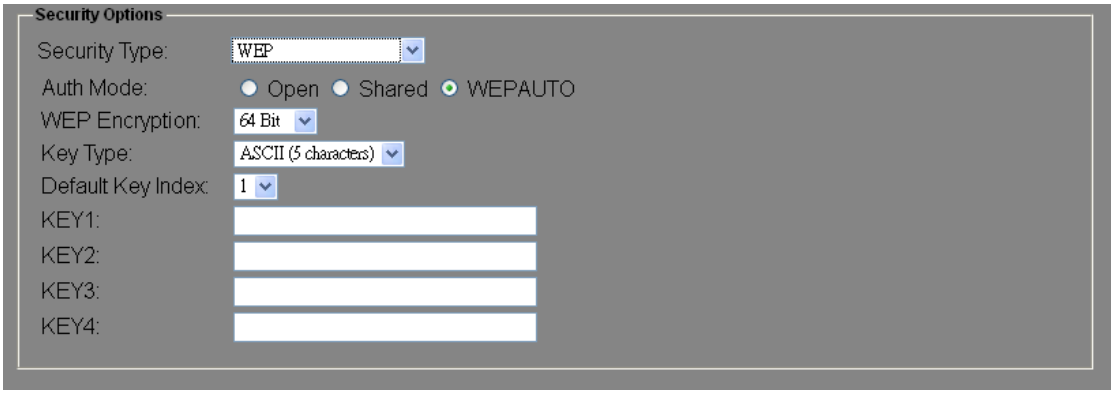
You can set the device to work in AP mode. This is the most common mode for all wireless APs. In this mode, the AP will act as a central connection point which other wireless clients can connect to.



Label	Description
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	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.

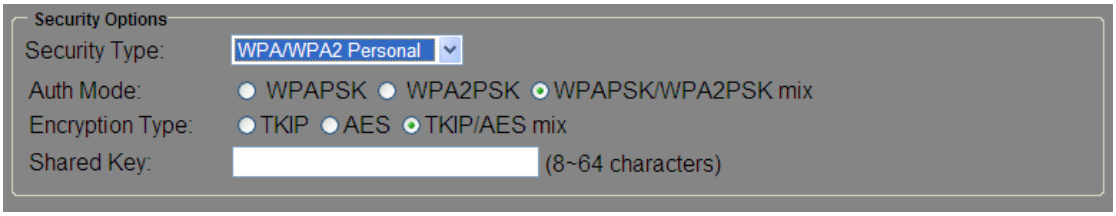
	WPA/WPA2 Personal: uses a pre-shared key for authentication. This pre-shared key is then dynamically sent between the AP and clients. Each authorized computer is given the same pass phrase. **WPA/WPA2 Enterprise**: this type includes all of the features of WPA/WPA2 Personal plus support for 802.1x RADIUS 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.



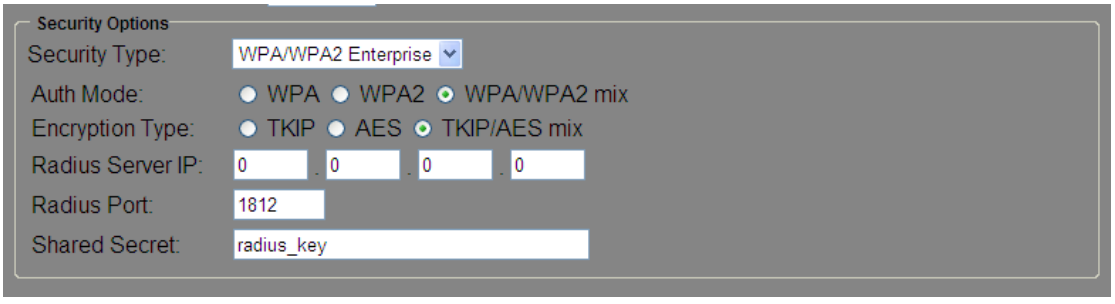
Label	Description
Auth Mode	Available values include **Open**, **Shared**, and **WEPAUTO**. When choosing **Open** or **Shared**, all of the clients must select the same authentication to associate this AP. If select **WEPAUTO**, the clients do not have to use the same **Open** or **Shared** authentication. 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.



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

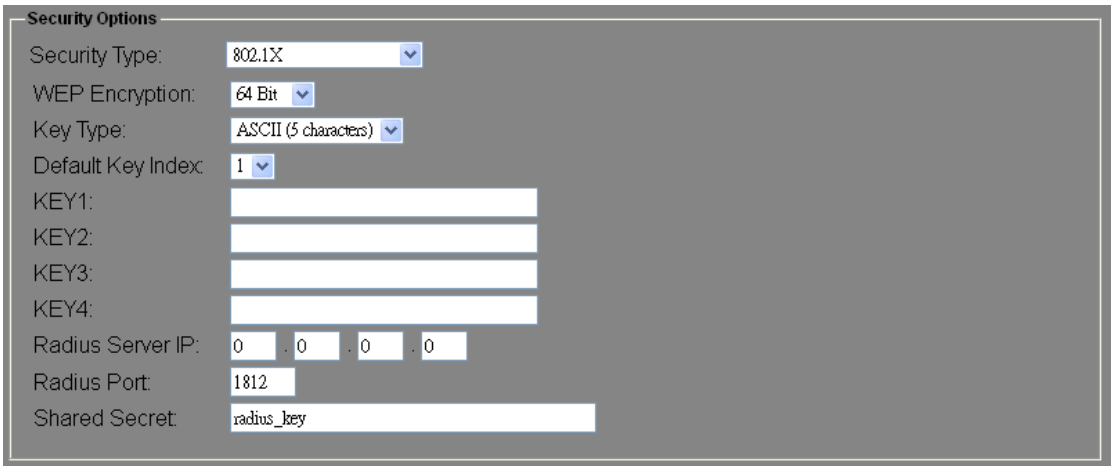
When you set security type as **WPA /WPA2 Enterprise**, the following screen will appear to allow you to configure individual settings.



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.



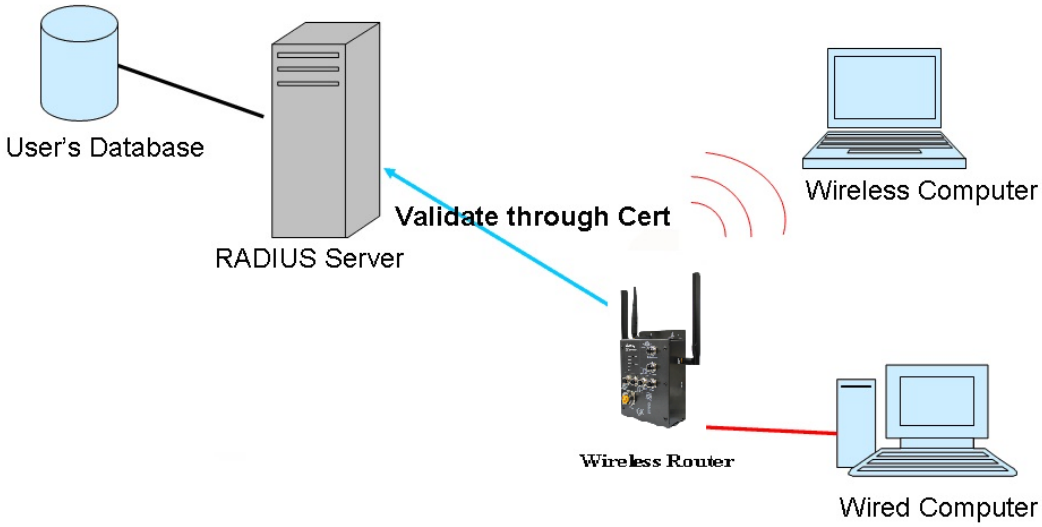
Label	Description
WEP Encryption	You can select **64 Bit** or **128 Bit**.
Key Type	Available values include **ASCII** and **Hex Key Type**. ASCII (American Standard Code for Information Interchange) is a code for representing English characters as numbers in the range from 0 to 127. Hex digits uses 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

RADIUS (Remote Authentication Dial-In User Service) is a widely deployed protocol that

enables companies to authenticate and authorize remote users' access to a system or service from a central network server.

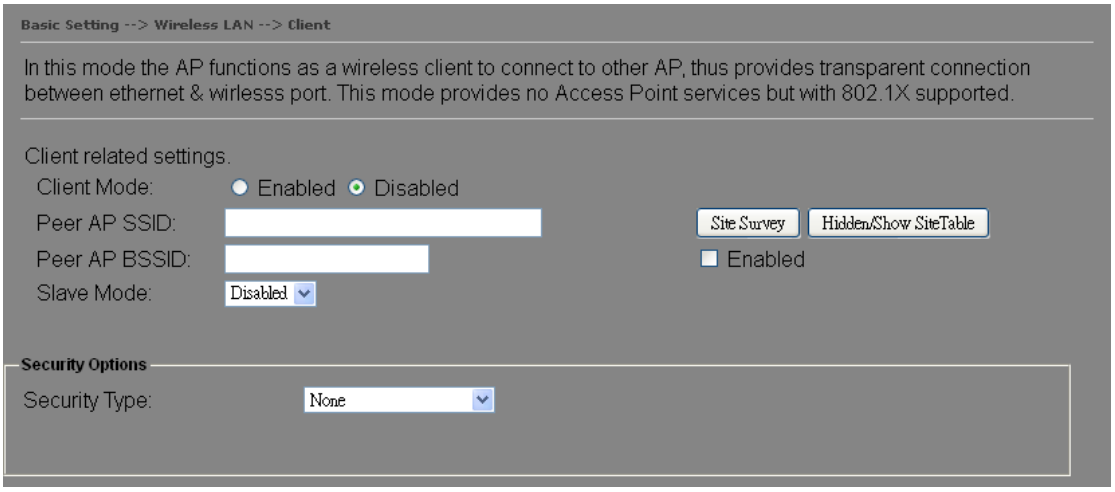
When you configure the remote access server for RADIUS authentication, the credentials of the connection request are passed to the RADIUS server for authentication and authorization. If the request is both authenticated and authorized, the RADIUS server sends an accept message back to the remote access server and the connection attempt is accepted. If the request is either not authenticated or not authorized, the RADIUS server sends a reject message back to the remote access server and the connection attempt is rejected.

The principle of the Radius server is shown in the following pictures:



Client Mode

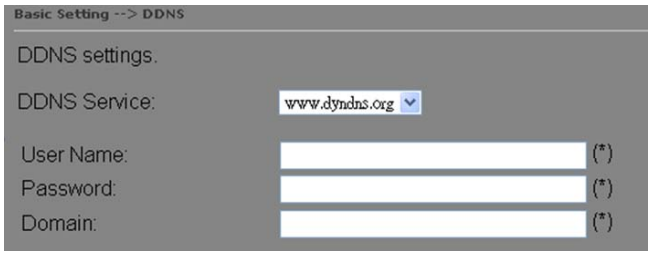
In this mode, the router functions as a wireless client to connect your wired devices to a wireless network. This mode provides no access point services but supports 802.1X.



Label	Description
Peer AP SSID	Enter the SSID of the AP you want to connect as a client
Peer AP BSSID	Enter the BSSID (Wireless MAC address) to limit client target
Site Survey	You can scan APs on the network using this mode.
Slave Mode	Enables or disables slave mode
Security Type	Select the security type used by the client you want to connect

DDNS

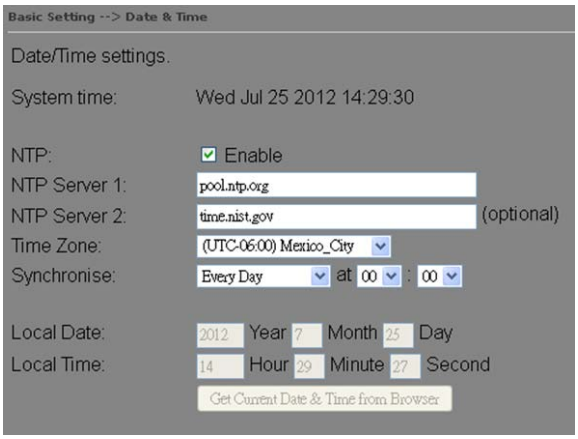
DDNS (Dynamic Domain Name System) allows you to configure a domain name for your IP address which is dynamically assigned by your ISP. Therefore, you can use a static domain name that always points to the current dynamic IP address.



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.



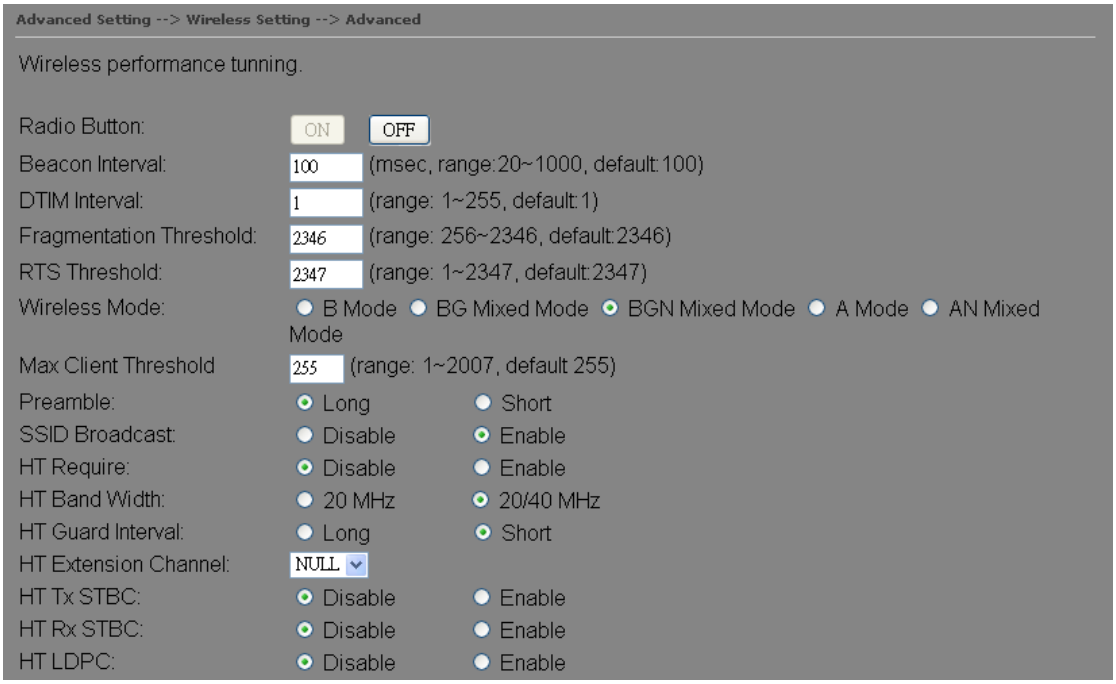
Label	Description
NTP	Enables or disables NTP function
NTP Server 1	The primary NTP server
NTP Server 2	The secondary NTP server
Time Zone	Select the time zone you are located in
Synchronize	Specify the scheduled time for synchronization
Local Date	Set a local date manually
Local Time	Set a local time 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.

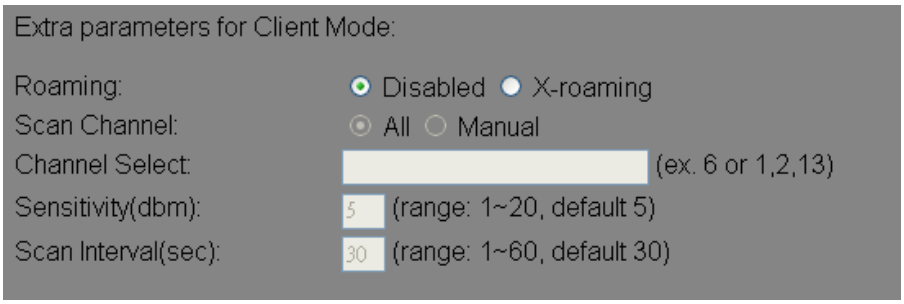
Wireless Setting – Advanced Setting

This page allows you to set up wireless configuration.



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

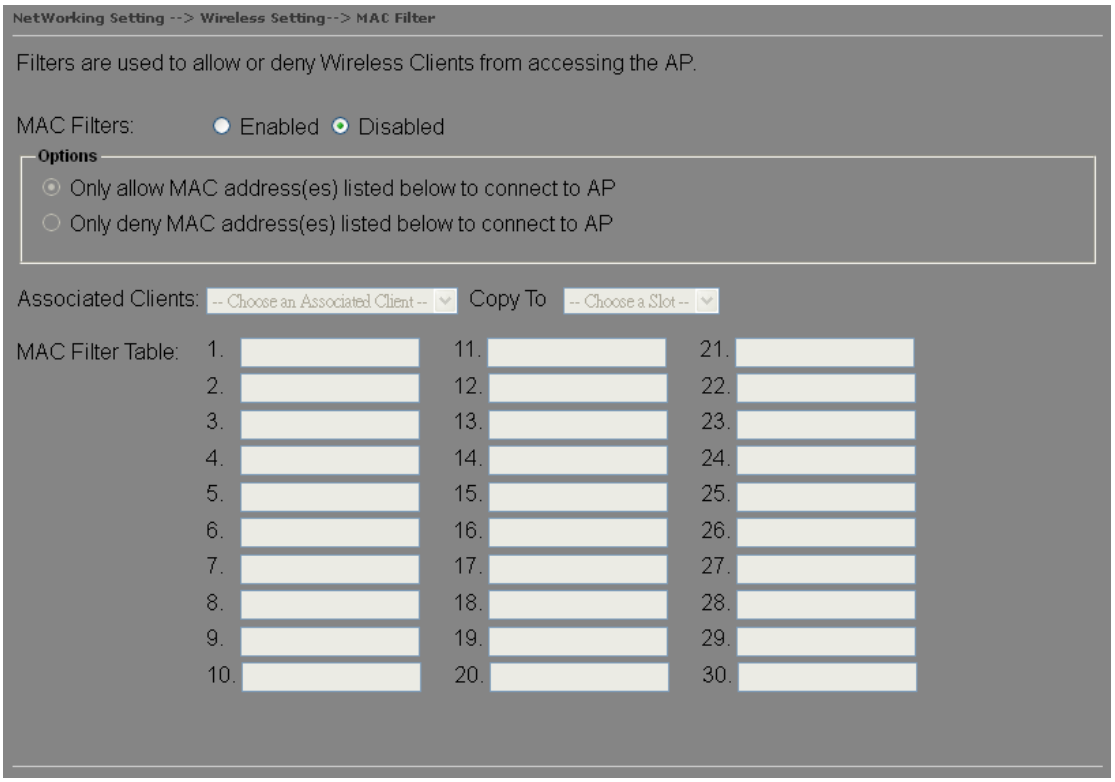
	the frequency interval of the beacon. Increasing the beacon interval reduces the number of beacons and the overhead associated with them. The default value is **100**, but **50** is recommended when reception is poor.
DTIM Interval	A DTIM interval determines how often a beacon frame includes a Delivery 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.
Wireless Mode	You can select 802.11 b, b/g, or b/g/n mode.
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.



Label	Description
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

Wireless Setting – MAC Filter

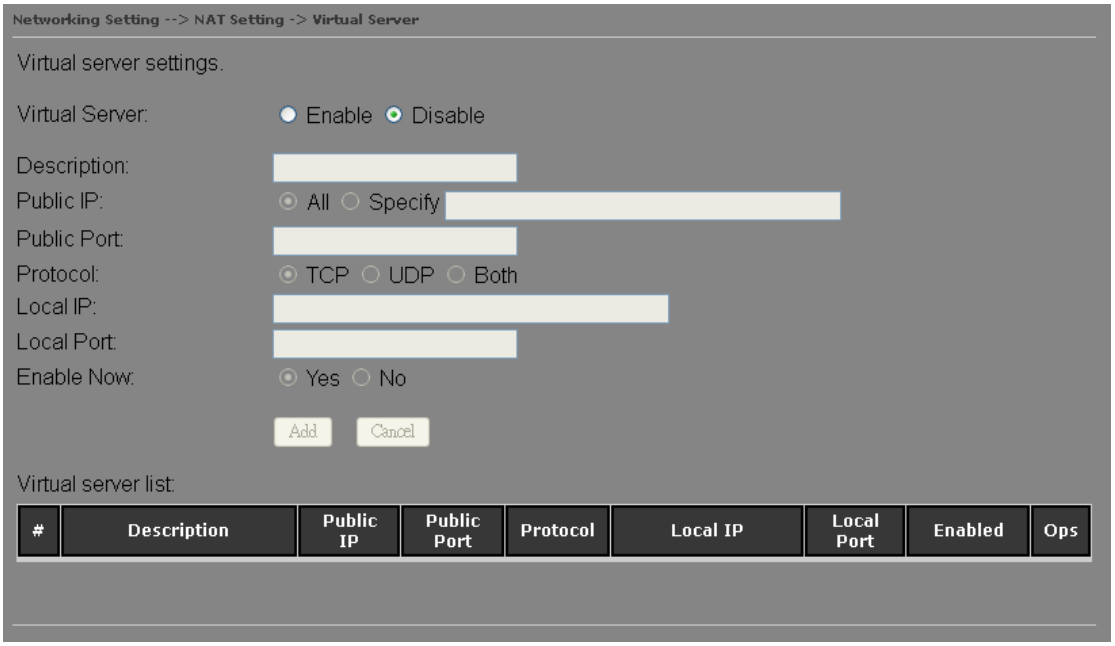
This page allows you to set up MAC filters to allow or deny wireless clients to connect to the router. You can manually add a MAC address or select a MAC address from the Associated Clients list currently associated with the router.



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 router
MAC Filter Table	You can edit up to MAC addresses in these fields
Apply	Click to activate the configurations

NAT Setting - Virtual Server

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



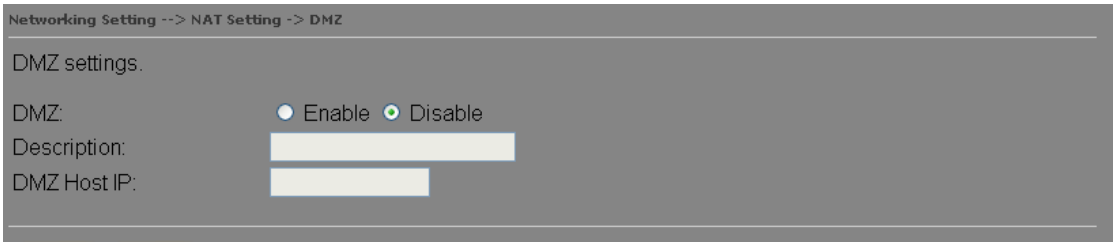
Label	Description
Virtual Server	Select **Enabled** or **Disabled** to activate or deactivate virtual server
Description	Enter the description of the entry. Acceptable characters are 0-9, a-z, and A-Z. A null value is allowed.
Public IP	Enter a public IP allowed to access the virtual service. If not specified, choose **All**.
Public Port	The port number to be used to access the virtual service on the

	WAN (Wide Area Network)
Protocol	The protocol used for the virtual service
Local IP	The IP address of the computer that will provide virtual service
Local Port	The port number of the service used by the private IP computer
Enable Now	Enables the virtual server entry after adding it
Virtual server list	Click **Edit** to edit the virtual service entry and **Del** to delete the entry.

NAT Setting – DMZ

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

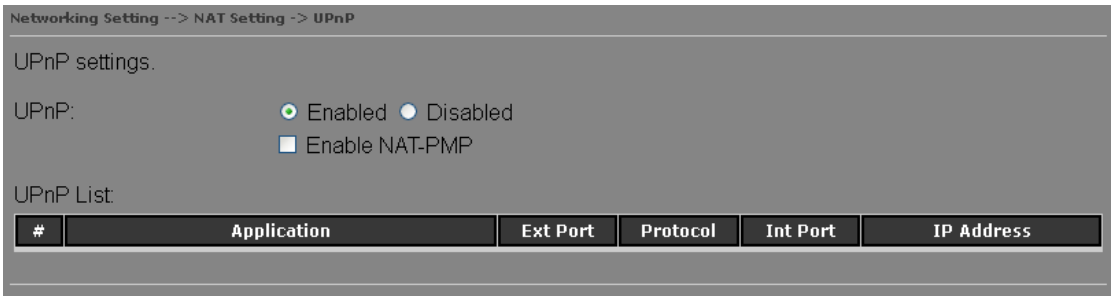
To use this function, you need to set an internal computer as the DMZ host by entering its IP address. Adding a client to the DMZ may expose your local network to a variety of security risks, so use this function carefully.



Label	Description
DMZ	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

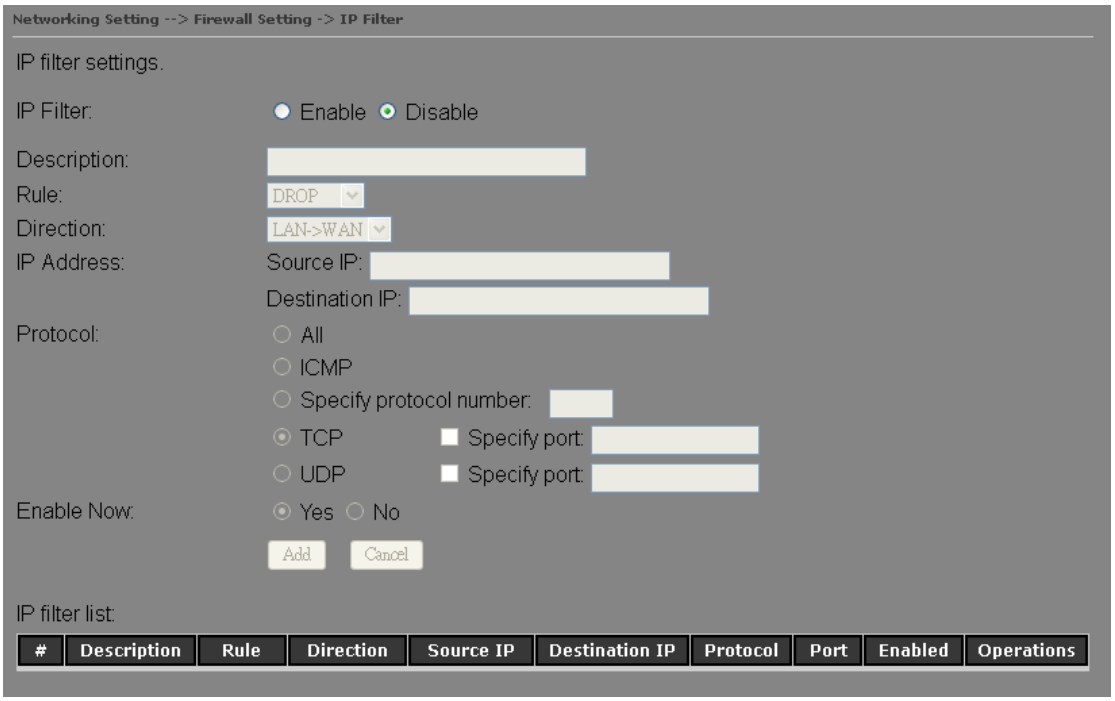
The UPnP (Universal Plug and Play) feature allows Internet devices to access local host resources or devices as needed. UPnP-enabled devices can be automatically discovered by the UPnP service application on the LAN.



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 router 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

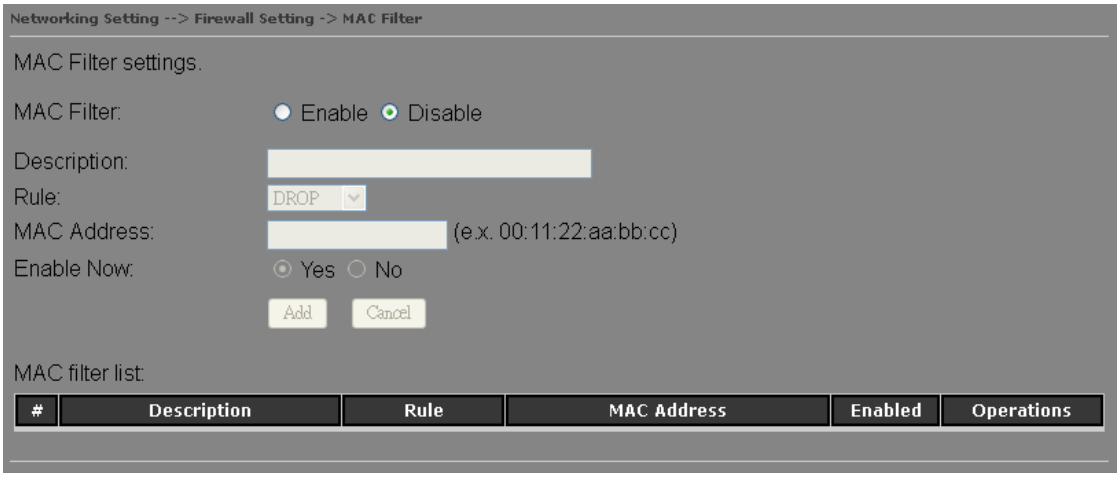
IP filters enable you to control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN. This control is implemented via IP filter rules which are defined to block attempts by certain computers on your LAN to access certain types of data or Internet locations.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



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.

Firewall Setting – MAC Filter

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



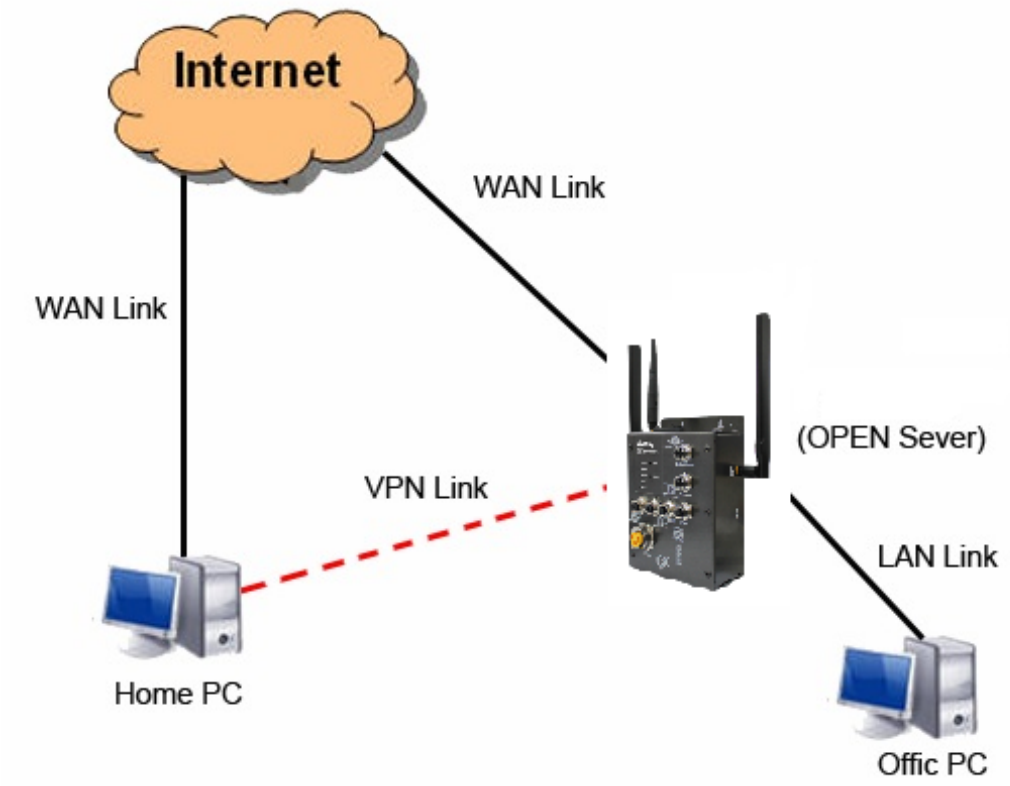
Label	Description
MAC Filter	Enables or disables the MAC Filter
Description	Enter description for the entry
Rule	Configures the rules to be applied to the MAC filter. Available options include **DROP**, **ACCEPT**, and **REJECT.**
MAC Address	Enter the MAC address to be filtered
Enable Now	Click **Yes**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

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.

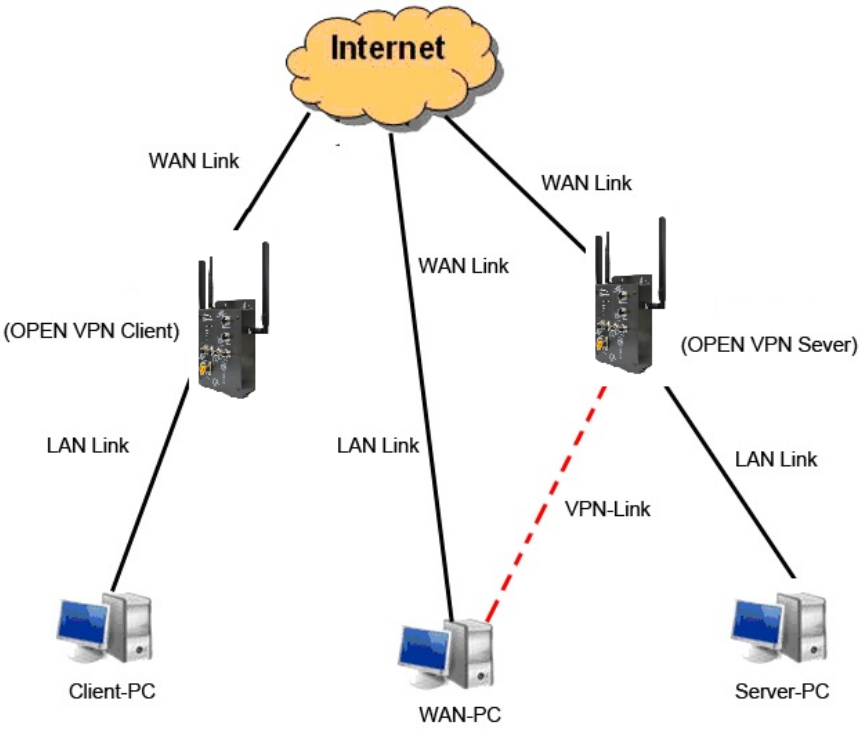
Open VPN enables you to easily set up a virtual private network over an encrypted connection. It is a full-function SSL VPN solution which accommodates a wide range of configurations including remote access, site-to-site VPNs, WiFi security, and enterprise-level remote access with load balancing, failover,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

To set up your router as an Open VPN server, you need to install openvpn client software for your Windows-based PC. You can download it from http://openvpn.net/download.html#stablel. The software version must match the current version of Openvpn used by IGAR-2062+-3G/4G which is version 2.0.9.

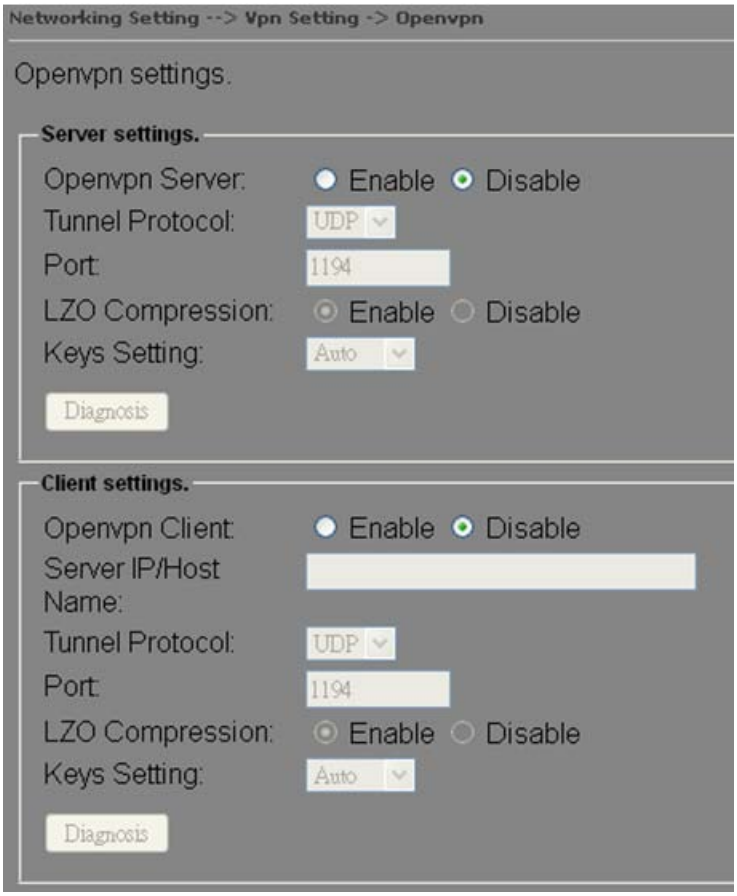


Connection to Open VPN Server

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



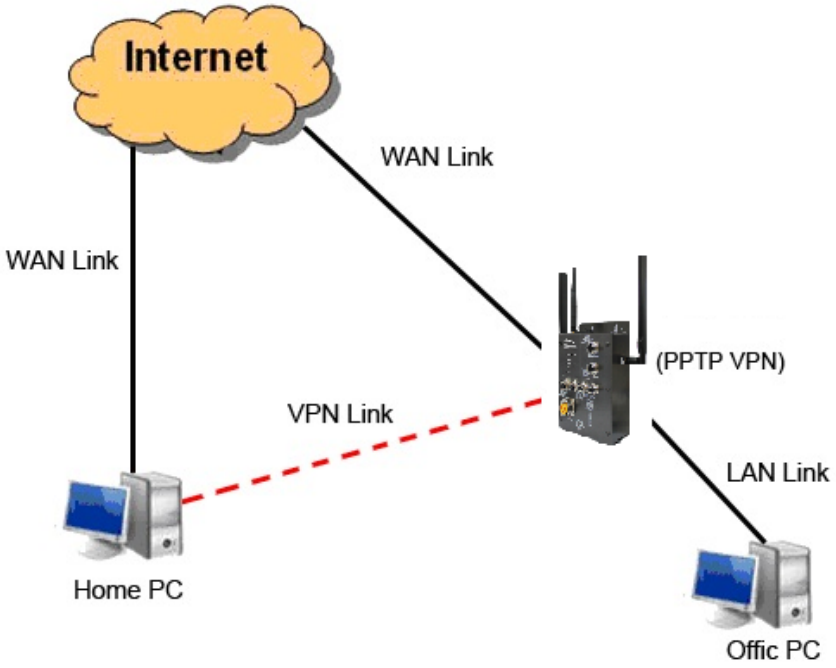
Open VPN Server and Client Connection



Label	Description
Open VPN Server	Enables or disables the function of Open VPN server
Tunnel Protocol	Select **UDP** or **TCP** protocol depending on your needs. TCP is more reliable than UDP, but UDP performs better than TCP. It is recommended to use UDP if the distance between VPN server and client is short; otherwise, use TCP.
Port	The number of the port (default is **1194**).
LZO Compression	Enables or disables the function of LZO Compression
Keys Setting	Select **Auto** to use preset certificates or **Manual** to use your certificates. Please install openvpn client software to generate your certificates and paste them here. For more information, please visit openvpn website.
Open VPN Client	Enables or disables the function of Open VPN client.
Server IP	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**).
LZO Compression	Enables or disables the LZO Compression
Keys Setting	Select **Auto** to use preset certificates or **Manual** to use your certificates. Please install openvpn client software to generate your certificates and paste them here. For more information, please visit openvpn website.

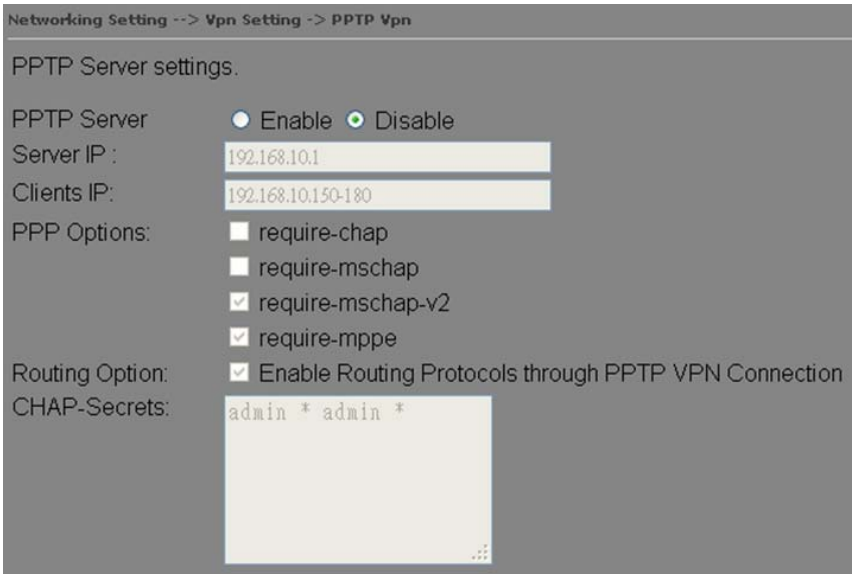
Vpn Setting – PPTP VPN

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



To create a PPTP connection to the router, 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.

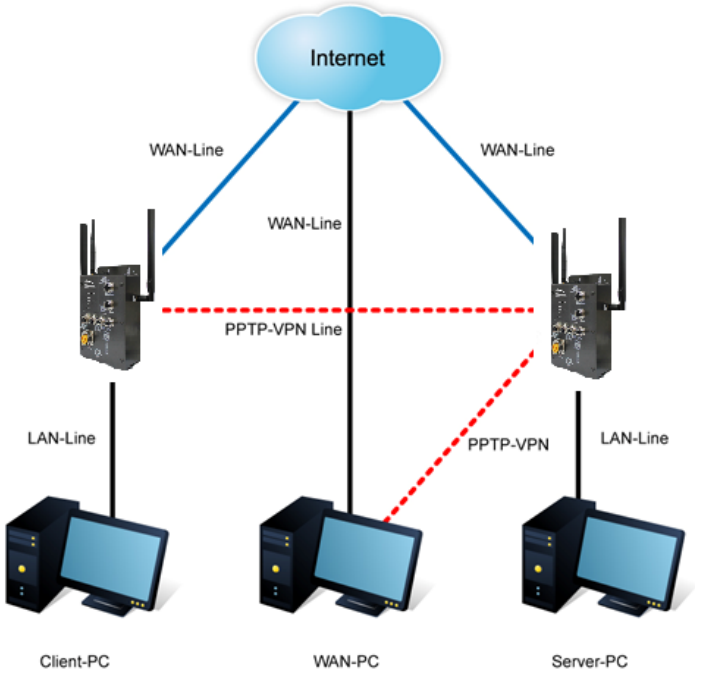


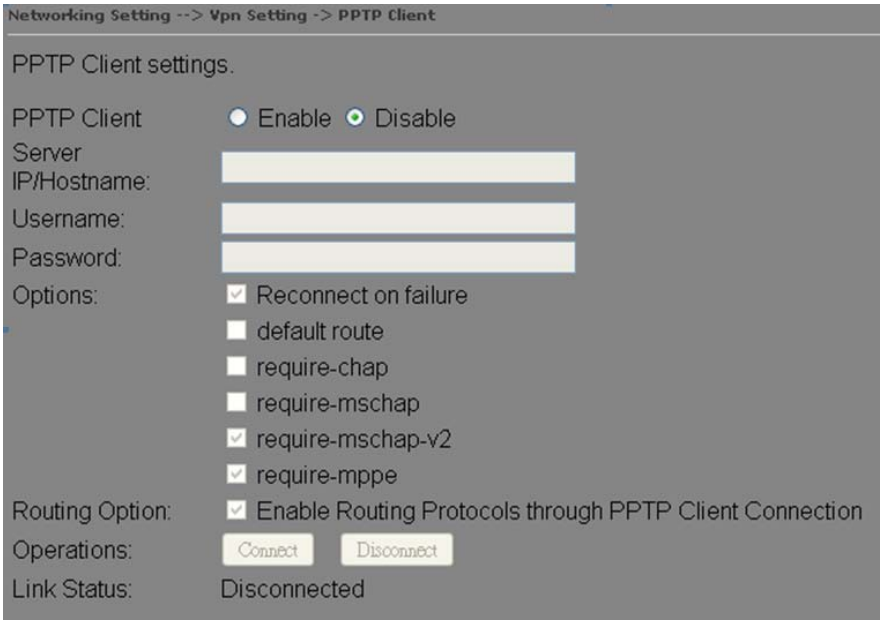
Label	Description
PPTP Server	Enables or disables PPTP VPN server
Server IP	Enter the server IP address. The default value is the IP address of the connected LAN port.

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.
CHAP-Secrets	Enter the username and password pairs in the form of **user * pass ***. Multiple username and password pairs are allowed.

Vpn Setting – PPTP Client

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

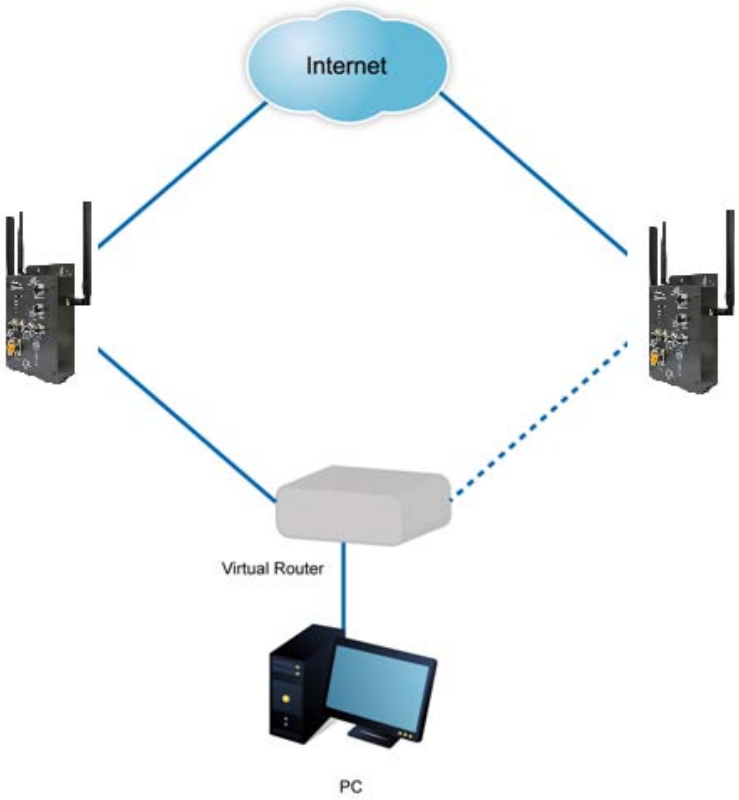


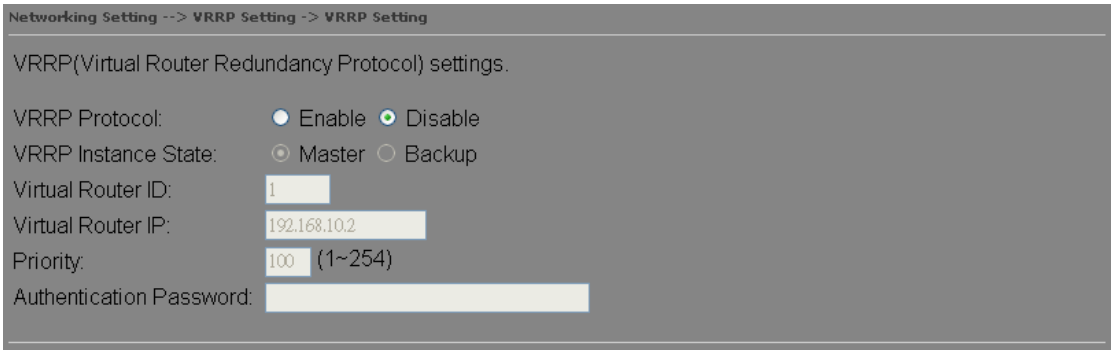


Label	Description
PPTP Client	Enables or disables PPTP client
Server IP/Hostname	Enter the server IP address or hostname
Username/Password	Enter the username and password assigned by PPTP server
Options	Choose the rules to be applied **Reconnect on failure**: prompts automatic reconnection when the link 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.
Operations	Click **Connect** to link to the server or **Disconnect** to disconnect from the server
Link Status	Show the status of the link

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.



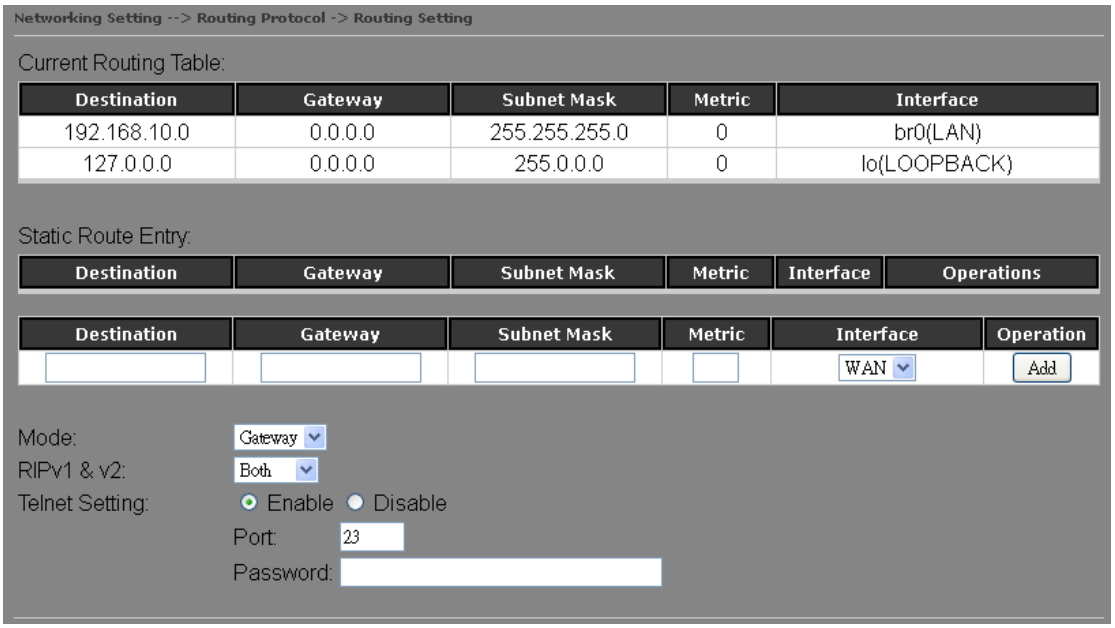


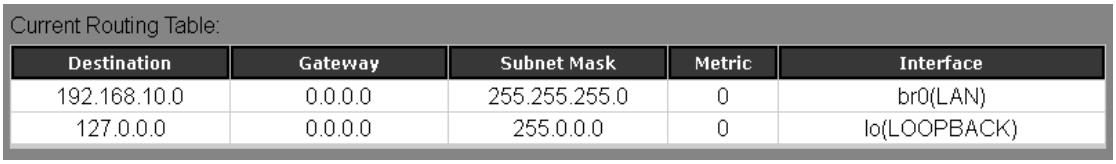
Label	Description
VRRP Protocol	Enables or disables VRRP function
VRRP Instance State	Specifies the router to act as the master or backup router
Virtual Router ID	A VRID consists of one master router and one or more backup routers. The master router is the router that owns the IP address you associate 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 – Routing Setting

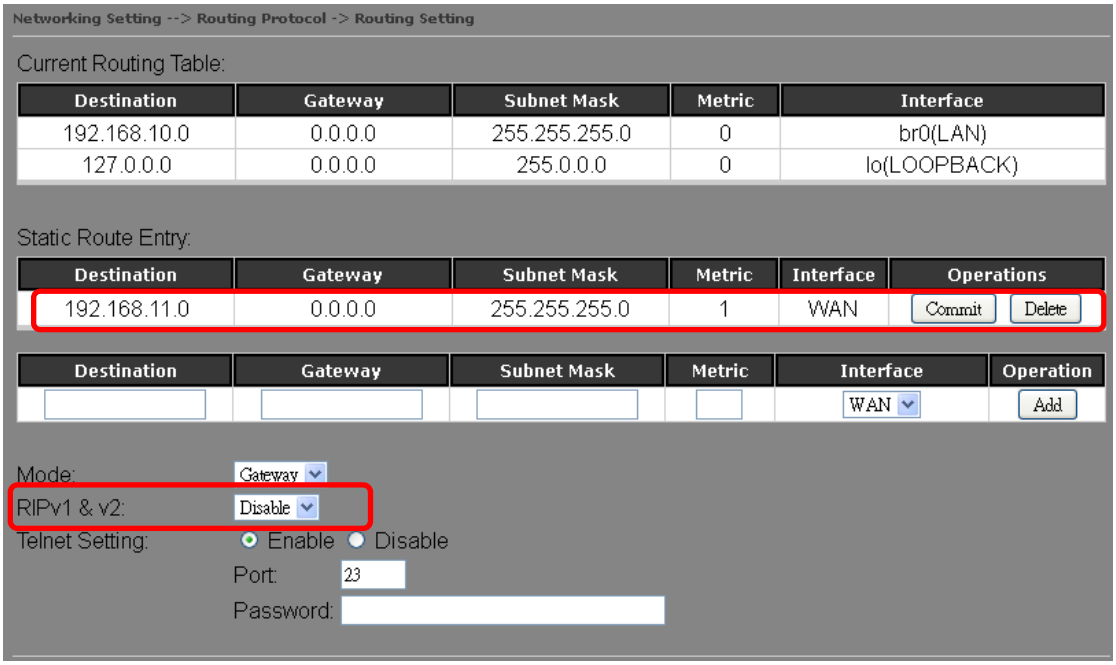
This page shows the information of the routing table. You can configure static and dynamic routing settings in this page.





Static Routing

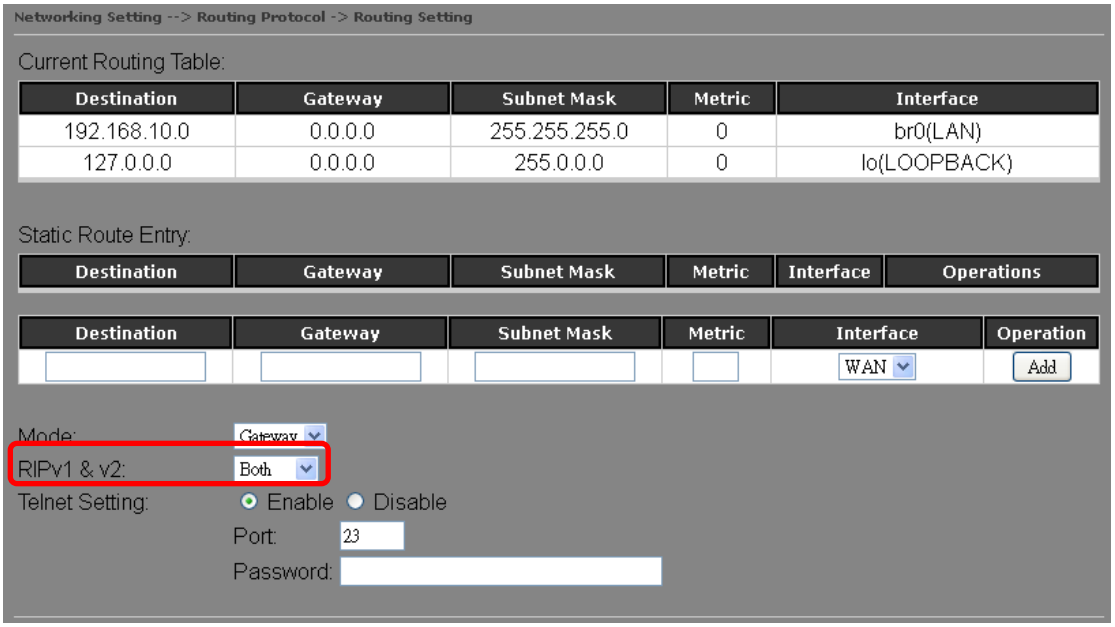
When RIPv1 & v2 is **Disabled**, the router will operate in static routing mode, which means routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.



Dynamic Routing

Dynamic routing lets routing tables in routers 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 IGAR-2062 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.

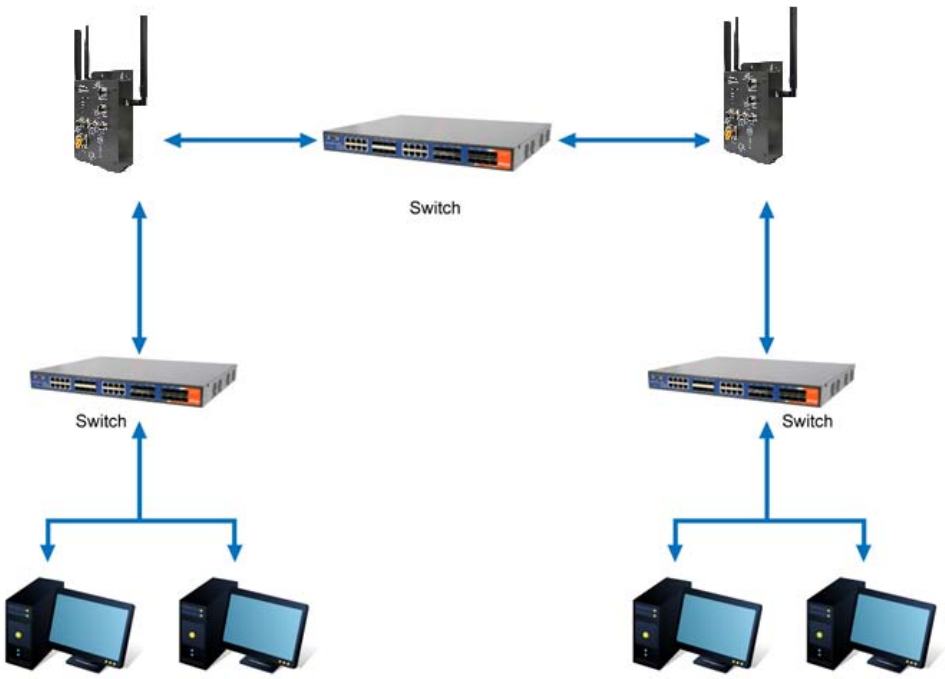


Label	Description
Current Routing Table	Shows all routing information, including static and dynamic routing (if enabled)
Static Route Entry	Fills in corresponding information to add new entries to the static routing tablet
Mode	Choose **Gateway Mode** if you want PCs in the LAN to visit external network,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

IAPR654978>
  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
```

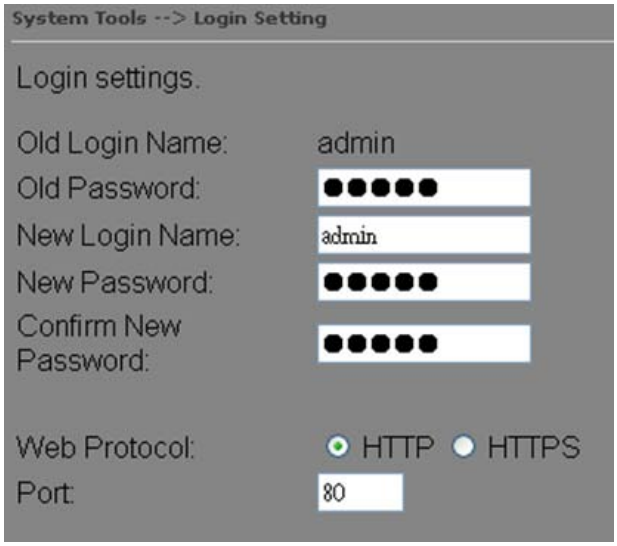


Routing Topography

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**.



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.

Router Restart

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

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

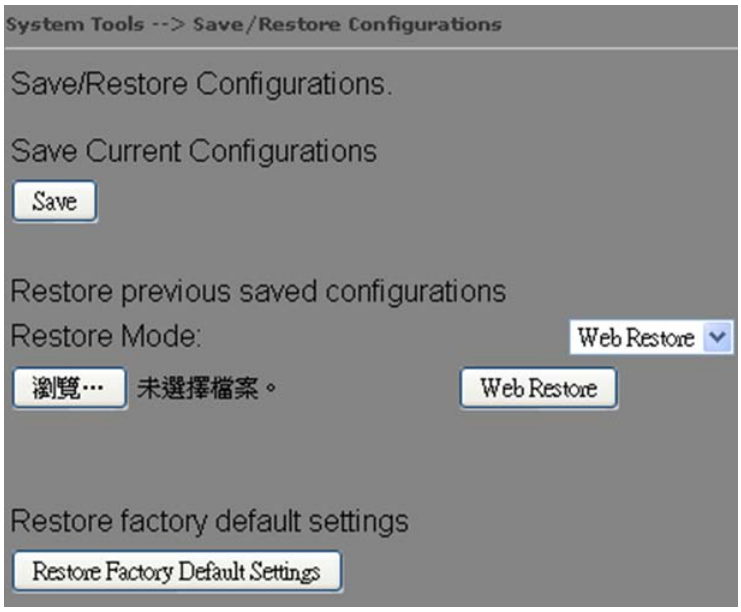
Firmware Upgrade

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

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

Save/Restore Configurations

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



Label	Description
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 router to the factory settings. The router 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.

GPS

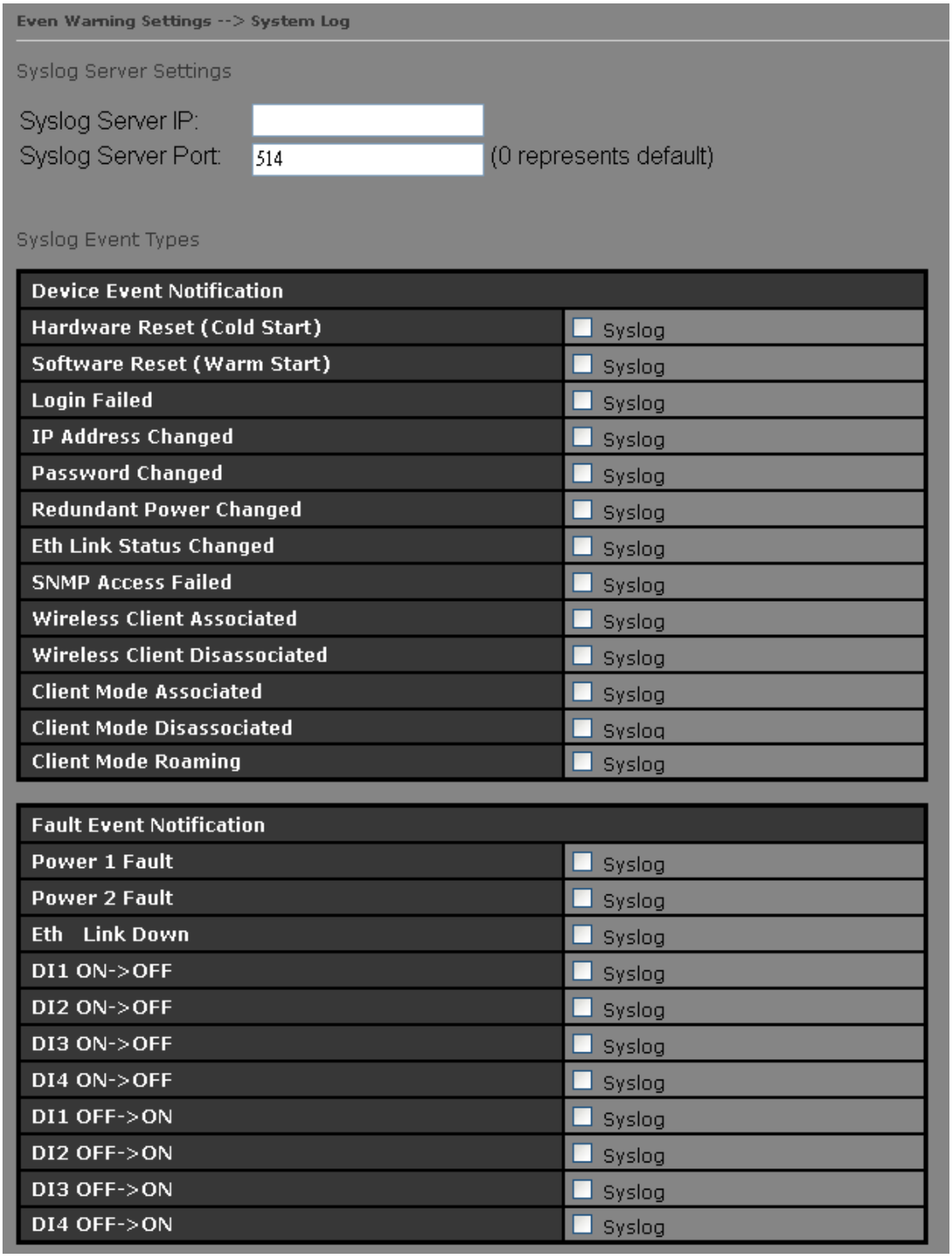
Enable GPS feature in this page, sent GPS information to specific host server with unicast or multicast packet

Label	Description
GPS	Enable or disable GPS feature
Mode	Unicast or Multlcast packet select
IP	Assign receive host IP
UDP Port	Assign UDP port (only allow in MCAST mode)
Interval	Packet sent interval

Event Warning

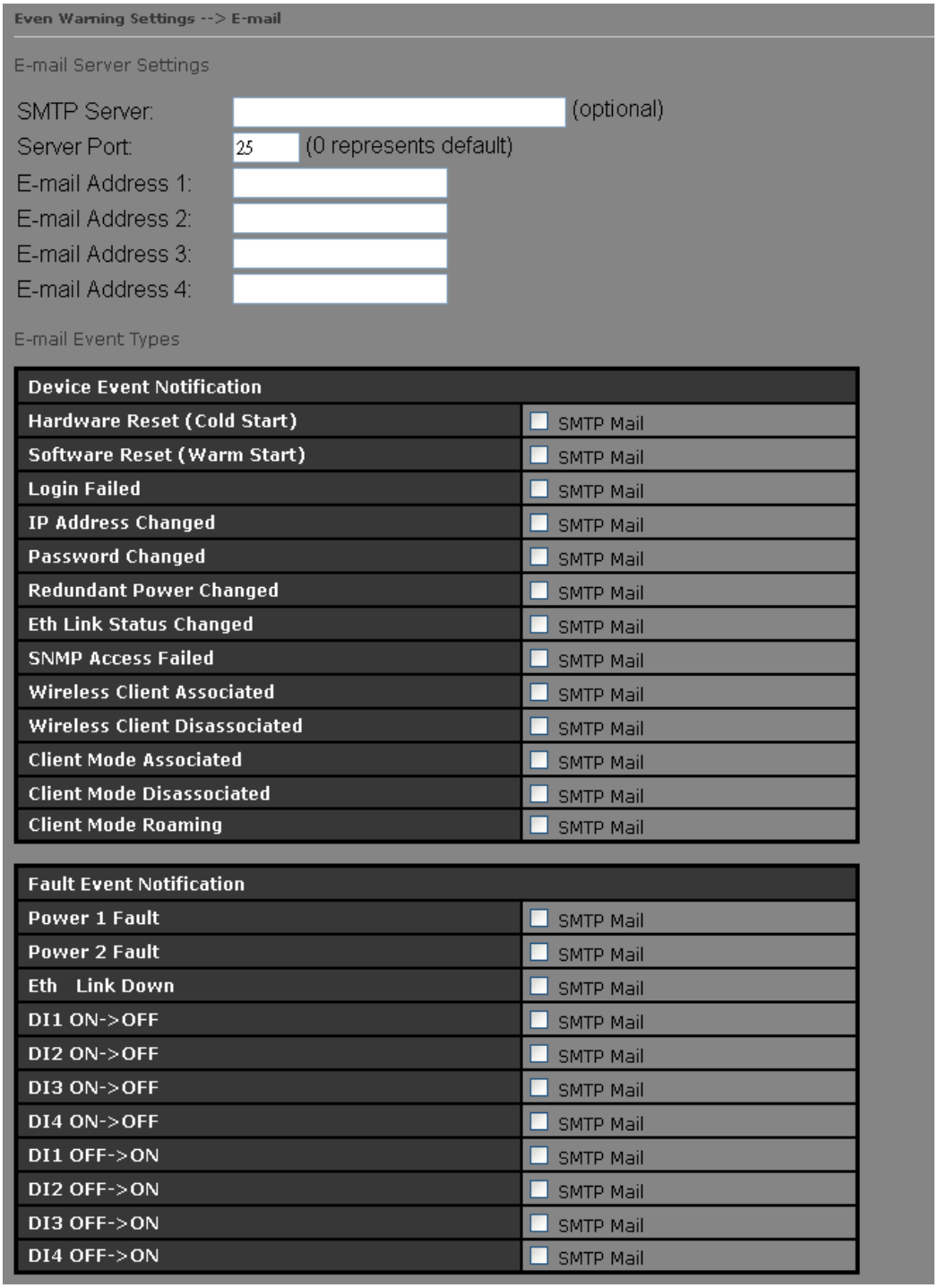
When an error occurs, the router will notify you through system log, e-mail, SNMP, and relay.

System Log



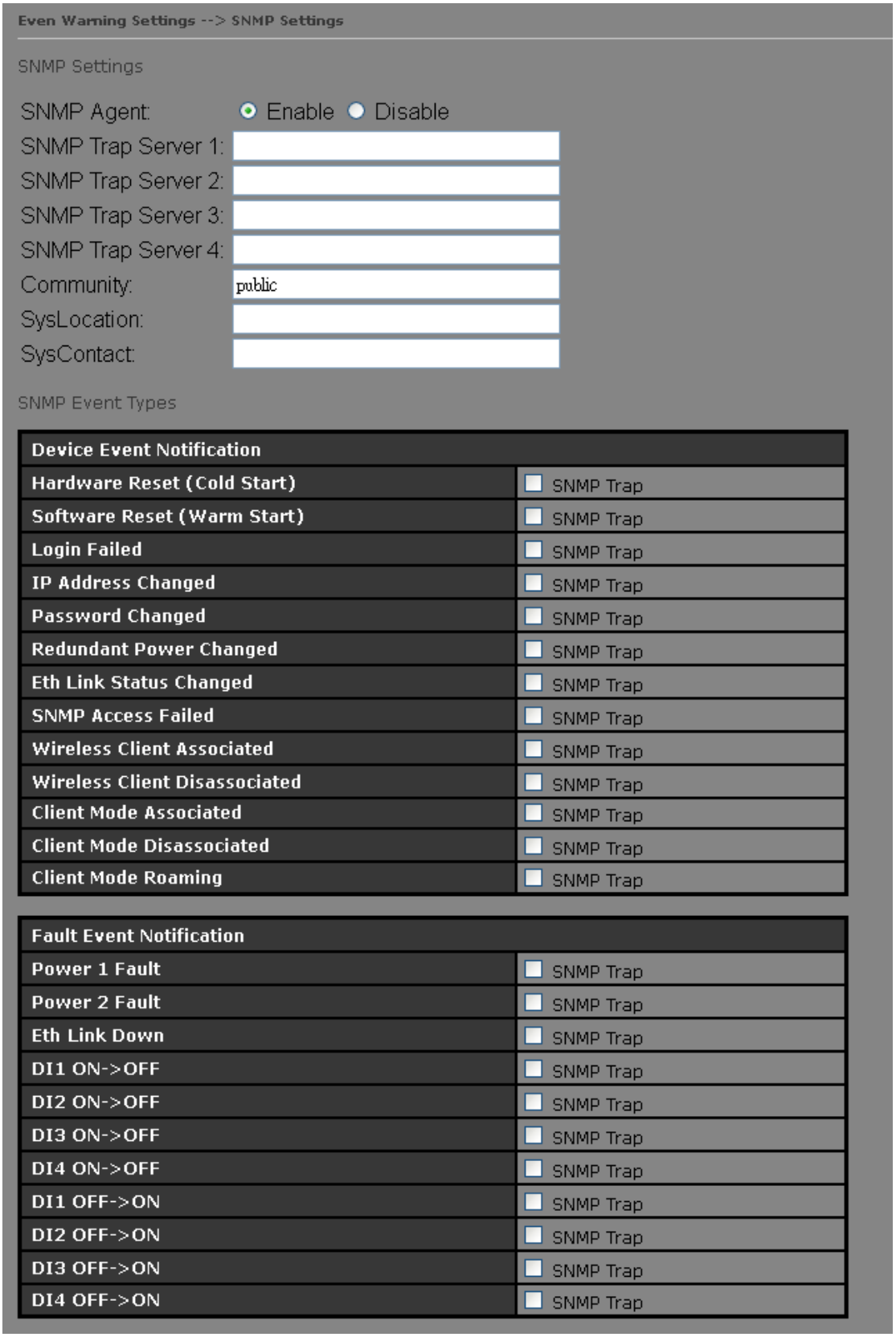
Label	Description
Syslog Server IP	Enter the IP address of a remote server if you want the logs to be stored remotely. Leave it blank will disable remote syslog.
Syslog Server Port	Specifies the port to be logged remotely. Default port is 514.

E-mail



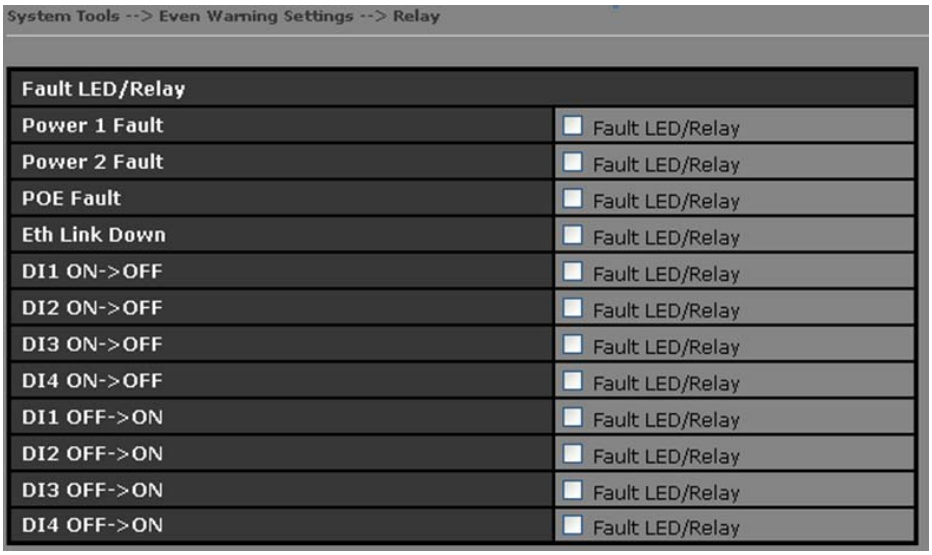
Label	Description
SMTP Server	Enter a backup host to be used when the primary host is unavailable.
Server Port	Specifies the port where MTA can be contacted via SMTP server
E-mail Address 1-4	Enter the mail address that will receive notifications

SNMP

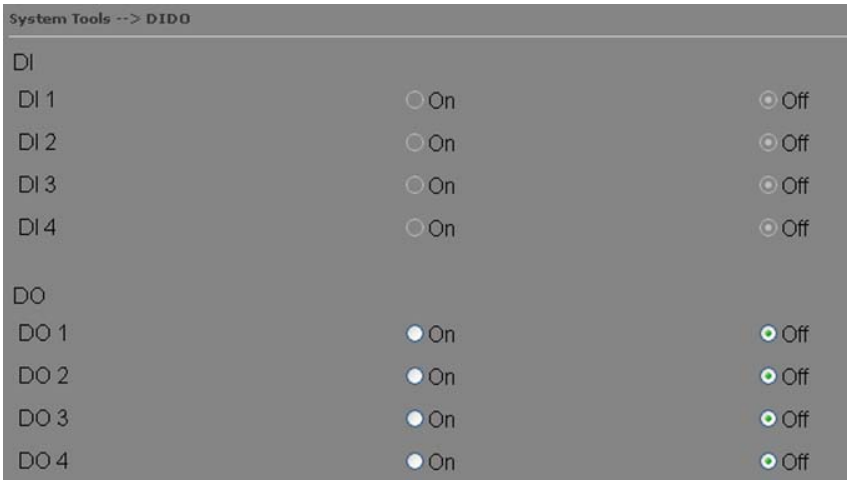

Even Warning Settings --> SNMP Settings
SNMP Settings
SNMP Agent: Enable Disable
SNMP Trap Server 1:
SNMP Trap Server 2:
SNMP Trap Server 3:
SNMP Trap Server 4:
Community: public
SysLocation:
SysContact:
SNMP Event Types
Device Event Notification
Hardware Reset (Cold Start) SNMP Trap
Software Reset (Warm Start) SNMP Trap
Login Failed SNMP Trap
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
Eth Link Down SNMP Trap
DI1 ON->OFF SNMP Trap
DI2 ON->OFF SNMP Trap
DI3 ON->OFF SNMP Trap
DI4 ON->OFF SNMP Trap
DI1 OFF->ON SNMP Trap
DI2 OFF->ON SNMP Trap
DI3 OFF->ON SNMP Trap
DI4 OFF->ON 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



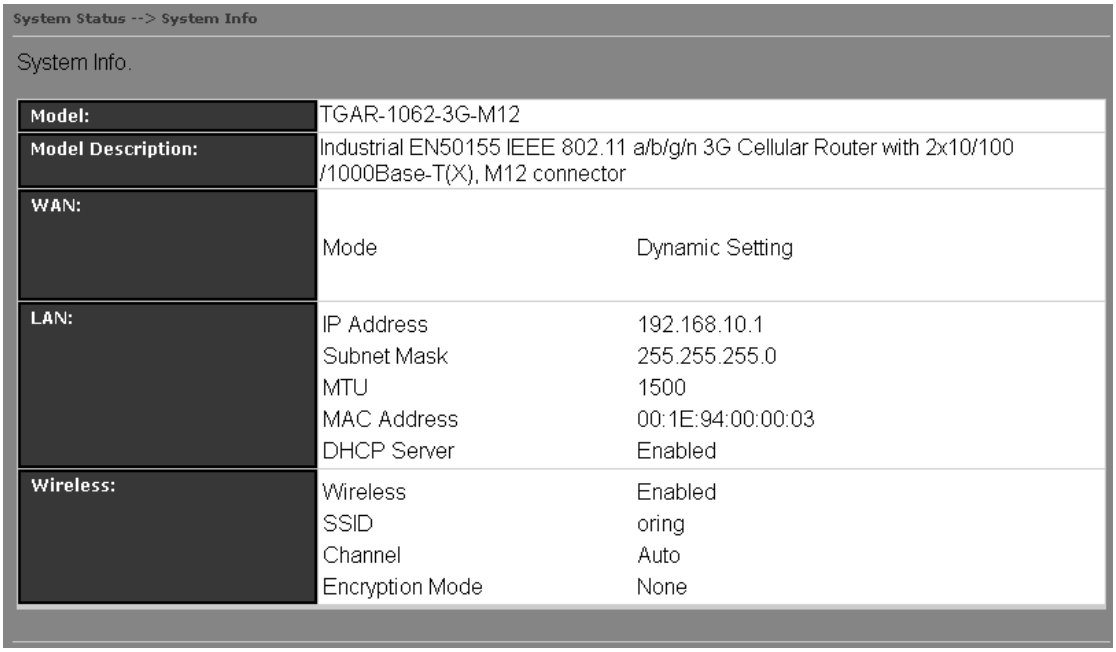
DIDO



5.2.4 System Status

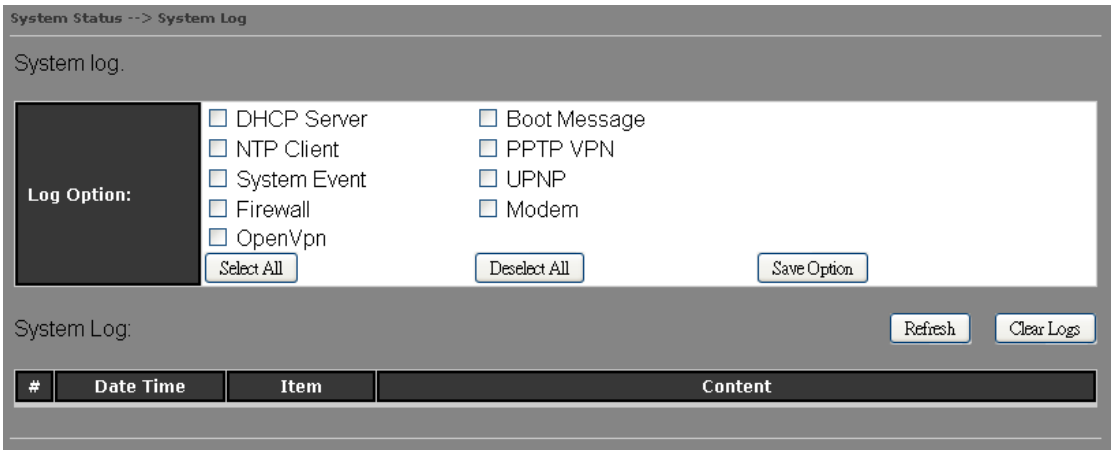
System Info

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



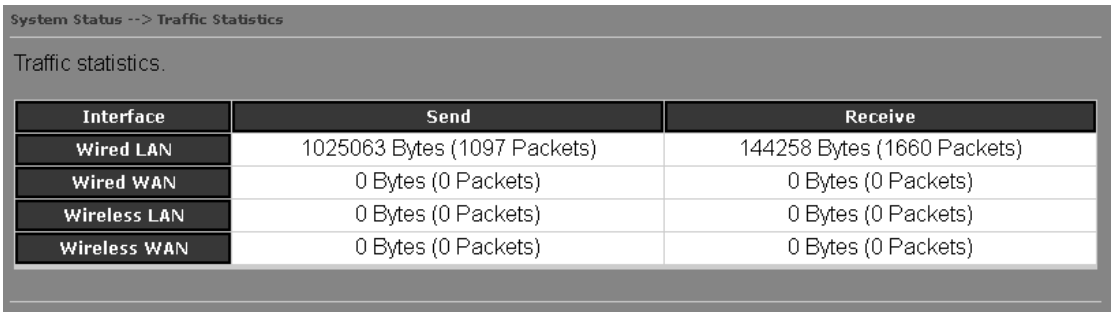
System Log

The router 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.



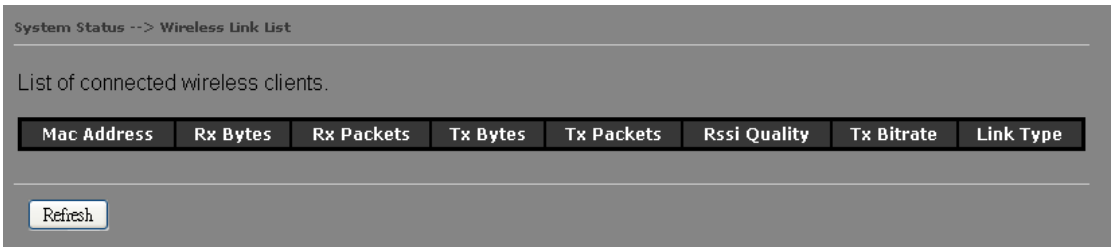
Traffic Statistics

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



Wireless Link List

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



Technical Specifications

ORing WLAN Access Point Model	TGAR-1062-M12-3G	TGAR-1062-M12-4G	TGAR-2062-M12-3G	TGAR-2062-M12-3G
Physical Ports				
10/100/1000Base-T(X) Ports in M12 Auto MDI/MDIX (8-pin A-coding)	**2**			
DIDO port in M12 (5-pin A-coding)	**2 (DI x 4 and DO x 4)**			
RS-232 Console port in M12 (5-pin A-coding)	**115200, 8 ,N ,1**			
Relay port in M12 (5-pin A-coding)	**1A@24VDC**			
SIM Card Slot	**1**	**1**	**2**	**2**
WLAN interface				
Antenna Connector	2 x reverse SMA-type antenna connector			
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: 18dBm ± 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 Authentication supported TKIP encryption			
Wireless Security	SSID broadcast disable			
Cellular Interface				
Cellular Standard	GSM / GPRS/ EGPRS/ EDGE / WCDMA / HSDPA / HSUPA	GSM / GPRS/ EGPRS/ EDGE / WCDMA / HSDPA / HSUPA /HSPA+ /LTE	GSM / GPRS/ EGPRS/ EDGE / WCDMA / HSDPA / HSUPA	GSM / GPRS/ EGPRS/ EDGE / WCDMA / HSDPA / HSUPA /HSPA+ /LTE
Antenna Connector	1 x RP-SMA Female	1 x SMA Female	2 x RP-SMA Female	2 x SMA Female

Band Option	Dual-band : HSUPA 1900/2100 MHz Quad-band : GSM/GPRS/EDGE 850/900/1800/1900 MHz WCDMA/HSDPA 850/900/1900/2100 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	Dual-band : HSUPA 1900/2100 MHz Quad-band : GSM/GPRS/EDGE 850/900/1800/1900 MHz WCDMA/HSDPA 850/900/1900/2100 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
Protocol Support				
Protocol	ARP,BOOTP, DHCP, DNS, HTTP, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, PPPoE, STP (IEEE 802.1D)			
LED indicators				
Power Indicator	2 x LEDs, Green for Power on			
10/100/1000Base-T(X) Indicator	2 x LEDs, Green for port Link/Act			
WLAN LED	1 x LED, Green for WLAN Link/Act			
WAN LED	1 x LED, Green for Cellular modem Link/ Act		2 x LEDs, Green for functioning normal	
Fault Indicator	1 x LED, Red for Ethernet link down or power down indicator			
Fault contact				
Relay	Relay output to carry capacity of 3A at 24VDC		Relay output to carry capacity of 1A at 24VDC	
Power				
Redundant Input Power	Dual Power Inputs. 12~48 VDC on M23 connector (24 VDC Typ.)			
Power Consumption (Typ.)	9 Watts	9.5 Watts	13 Watts	15 Watts
Overload Current Protection	Present			
Reverse Polarity Protection	Present			
Physical Characteristic				
Enclosure	IP-40			
Dimension (W x D x H)	125.6(W) x 65(D) x 196.1(H) mm (4.94 x 2.55 x 7.72 inch.)			
Weight (g)	985g	968g	1030g	1030g
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, EN50155 (EN50121-3-2)			
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, EN61373
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6, EN61373
Rail Traffic	EN50155
Cooling	EN60068-2-1
Dry Heat	EN60068-2-2
Safety	EN60950-1
Warranty	5 years

ORing WLAN Access Point Model	TGAR-1662-M12-3G	TGAR-1662-M12-4G
Physical Ports		
10/100/1000Base-T(X) Ports in M12 Auto MDI/MDIX (8-pin A-coding)	**2**	
DIDO port in M12 (5-pin A-coding)	**2 (DI x 4 and DO x 4)**	
RS-232 Console port in M12 (5-pin A-coding)	**115200, 8 ,N ,1**	
Relay port in M12 (5-pin A-coding)	**1A@24VDC**	
SIM Card Slot	**1**	
WLAN interface		
Antenna Connector	4 x reverse SMA-type antenna connector	
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: 18dBm ± 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 Authentication supported TKIP encryption	
Wireless Security	SSID broadcast disable	

Cellular Interface		
Cellular Standard	GSM / GPRS/ EGPRS/ EDGE / WCDMA / HSDPA / HSUPA	GSM / GPRS/ EGPRS/ EDGE / WCDMA / HSDPA / HSUPA /HSPA+ /LTE
Antenna Connector	1 x Reverse SMA Female	1 x SMA Female
Band Option	Dual-band : HSUPA 1900/2100 MHz Quad-band : GSM/GPRS/EDGE 850/900/1800/1900 MHz WCDMA/HSDPA 850/900/1900/2100 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
Protocol Support		
Protocol	ARP,BOOTP, DHCP, DNS, HTTP, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, PPPoE, STP (IEEE 802.1D)	
LED indicators		
Power Indicator	2 x LEDs, Green for Power on	
10/100/1000Base-T(X) Indicator	2 x LEDs, Green for port Link/Act	
WLAN LED	2 x LED, Green for WLAN Link/Act	
WAN LED	1 x LED, Green for Cellular modem Link/ Act	
Fault Indicator	1 x LED, Red for Ethernet link down or power down indicator	
Fault contact		
Relay	Relay output to carry capacity of 1A at 24VDC	
Power		
Redundant Input Power	Dual Power Inputs. 12~48 VDC on M23 connector (24 VDC Typ.)	
Power Consumption (Typ.)	13 Watts	14 Watts
Overload Current Protection	Present	
Reverse Polarity Protection	Present	
Physical Characteristic		
Enclosure	IP-40	
Dimension (W x D x H)	125.6(W) x 65(D) x 196.1(H) mm (4.94 x 2.55 x 7.72 inch.)	
Weight (g)	1030g	
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, EN50155 (EN50121-3-2)	
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, EN61373	
Free Fall	IEC60068-2-32	
Vibration	IEC60068-2-6, EN61373	
Rail Traffic	EN50155	
Cooling	EN60068-2-1	

Dry Heat	EN60068-2-2
Safety	EN60950-1
Warranty	5 years

Compliance

FCC Statement

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

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

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

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

Industry Canada Statement

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

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

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

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le 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.