



IGAR-1042/1062-3G series
IEEE 802.11 b/g/n Access Point Router
IEEE 802.11 a/b/g/n Access Point Router

User's Manual

Version 1.0

Mar, 2013

www.oring-networking.com

COPYRIGHT NOTICE

Copyright © 2012 ORing Industrial Networking Corp.

All rights reserved.

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

TRADEMARKS



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 to Know your Wireless AP Router | 1 |
| 1.1 Overview | 1 |
| 1.2 Software Features | 1 |
| 1.3 Hardware Features..... | 1 |
| Hardware Installation | 3 |
| 2.1 Installation Router on DIN-Rail | 3 |
| 2.2 Wall Mounting Installation | 4 |
| Hardware Overview | 6 |
| 3.1 Front Panel..... | 6 |
| 3.2 Front Panel LEDs | 8 |
| Cables and Antenna | 9 |
| 4.1 Ethernet Cables..... | 9 |
| 4.2 Wireless Antenna..... | 9 |
| 4.3 Cellular Antenna | 10 |
| Management Interface..... | 11 |
| 5.1 First-time Installation | 11 |
| 5.2 Configure the Wireless Router | 14 |
| 5.3 Main Interface | 14 |
| 5.3.1 Basic Setting..... | 15 |
| WAN | 15 |
| LAN..... | 20 |
| DHCP..... | 21 |
| Wireless..... | 22 |
| DDNS | 28 |
| Date&Time..... | 28 |
| 5.3.2 Networking Setting..... | 30 |
| Wireless setting..... | 30 |
| Extra parameters for Client Mode(X-Roaming) | 31 |
| NAT Setting..... | 33 |
| Firewall Setting | 35 |
| VPN Setting | 37 |
| VRRP..... | 44 |
| Routing Protocol (Routing Setting) | 44 |
| 5.3.3 System Tools | 48 |
| Login Setting..... | 48 |
| Router Restart..... | 49 |

| | |
|-----------------------------------|----|
| Firmware Upgrade | 49 |
| Save/Restore Configurations | 50 |
| Miscellaneous (Ping) | 51 |
| Even warning setting..... | 52 |
| DIDO | 57 |
| 5.3.4 System Status | 57 |
| System Info | 57 |
| System Log..... | 58 |
| Traffic Statistics..... | 58 |
| Wireless Link List..... | 58 |

Technical Specifications..... 59

Getting to Know your Wireless AP Router

1.1 Overview

The ORing IGAR-1042/1062-3G wireless AP router is designed to operate in industrial environment. The AP router provides a fast and effective ways of communicating to the internet over wired or wireless LAN. In addition, multiple types of WAN connection are provided for easily access to the internet.

The ORing IGAR-1042/1062-3G wireless AP router is IEEE802.11 b/g/n, a/b/g/n wireless equipment. It is easy for you to extend the reach and number of computers connected to your wireless network.

With the 3G WAN connection, the ORing IGAR-1042/1062-3G wireless AP router can be mounted in harsh environment easily to provide internet access anytime and anywhere.

The ORing IGAR-1042/1062-3G wireless AP router's VPN capability creates encrypted "Virtual Tunnels" through the internet, allowing remote or traveling users for secured connection with the network in your office.



1.2 Software Features

- Intuitive Web-based management user interface for simply and easily operation.
- Functions of firewall provides many security features such as blocking attacks from hacker, especially IP Spoofing, Ping flood, Ping of Death, DOS, DRDOS, Stealth Scan, ICMP flooding etc.
- Advanced firewall configuration to extend the capability and security, such as Virtual Server, Port Trigger, DMZ host, UPnP auto Forwarding, IP Filter and MAC filter.

1.3 Hardware Features

- Two 10/100/1000 Base-T(X) Ethernet ports for WAN / LAN connection individually.
- Fully Compliant with IEEE802.3af (Power Device at ETH2, WAN port, IGAR-1042+/1062+-3G only)
- Redundant Power Inputs: 12~48 VDC on terminal block



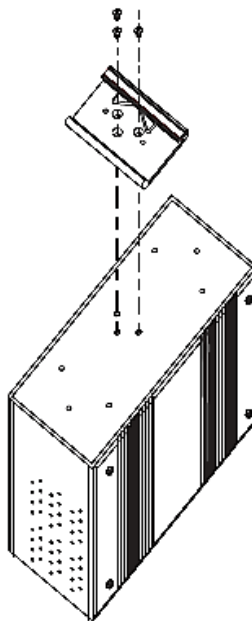
- Casing: IP-30
- Dimensions(W x D x H) : 74.3(W) x 109.2(D) x 153.6(H) mm
- Operating Temperature: -10 to 60°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing

Hardware Installation

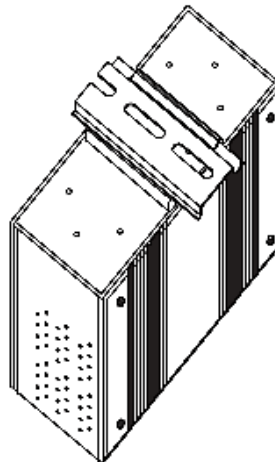
2.1 Installation Router on DIN-Rail

Each Wireless AP router has a DIN-Rail kit on rear panel. The DIN-Rail kit helps AP router to fix on the DIN-Rail.

Step 1: Slant the router and mount the metal spring to DIN-Rail.



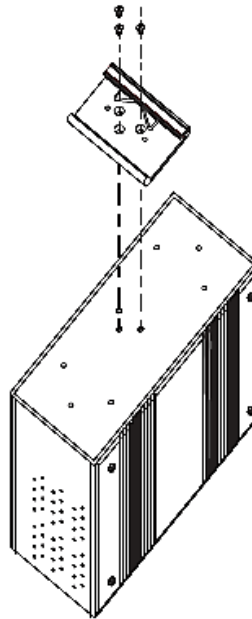
Step 2: Push the router toward the DIN-Rail until you heard a “click” sound.



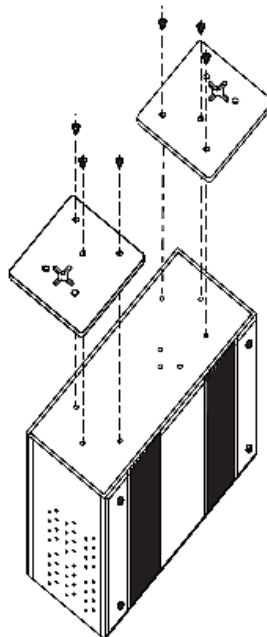
2.2 Wall Mounting Installation

Each AP router has another installation method to fix the AP router. A wall mount panel can be found in the package. The following steps show how to mount the AP router on the wall:

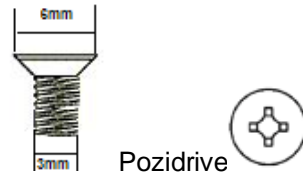
Step 1: Remove DIN-Rail kit.



Step 2: Use 6 screws that can be found in the package to combine the wall mount panel. Just like the picture shows below:



The screws specification shows in the following two pictures. In order to prevent the AP routers from any damage, the screws should not larger than the size that used in IAR-420/620.



Step 3: Mount the combined AR on the wall.

Hardware Overview

3.1 Front Panel

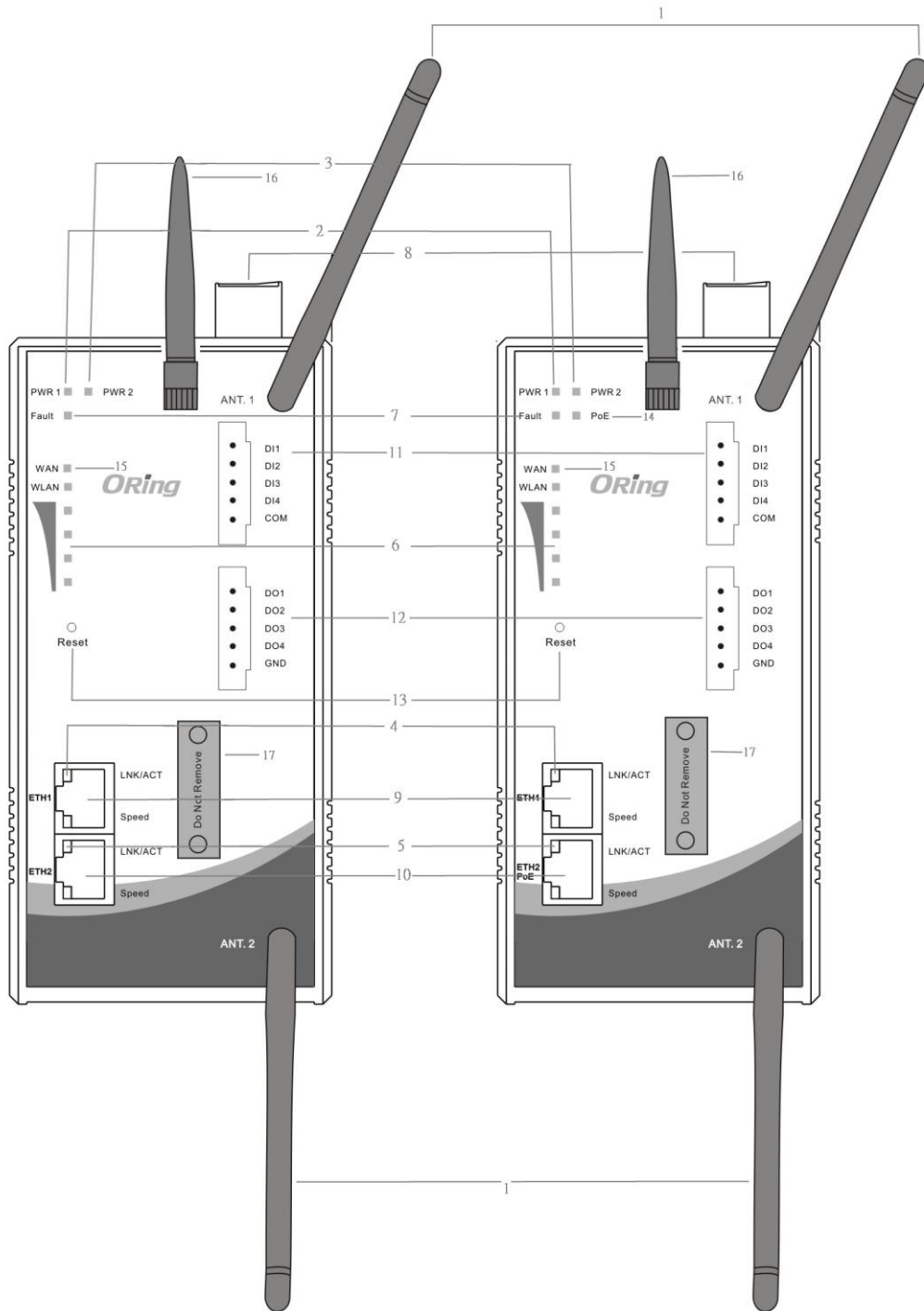
The following table describes the labels that stick on the IGAR-1042/1062-3G.

| Port | Description |
|---|--|
| 10/100 RJ-45 fast Ethernet ports | 2 10/100/1000Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto |
| PoE PD Port | ETH2 (WAN port) of IGAR-1042+/1062+-3G compliant with IEEE802.3af PoE specifications and can be connected to PoE switches.* |
| ANT. | Reversed SMA connector for external antenna. |

***Note:** Please refer to the products of **ORing IPS series** for P.O.E. Ethernet switch.

IGAR-1042/1062-3G

IGAR-1042+/1062+-3G





1. 2.4/5GHz antenna with typical 2 dBi antenna for 5GHz and 2.4GHz.
2. LED for PWR1 and system status. When the PWR1 links, the green LED will be light on.
3. LED for PWR2 and system status. When the PWR2 links, the green LED will be light on.
4. LED for Ethernet port1 status.
5. LED for Ethernet port2 status.
6. LED for WLAN link status.
7. LED for Fault Relay. When the fault occurs, the red LED will be light on.
8. Power Input port
9. Ethernet port1 connector
10. Ethernet port2 connector
11. Digital input
12. Digital output
13. Reset button
14. LED for P.O.E Status (IGAR-1042+/1062+-3G)
15. LED for Wan status
16. Modem antenna
17. SIM card slot

3.2 Front Panel LEDs

| LED | Color | Status | Description |
|--------------|-------------|----------|---|
| PWR1 | Green | Green On | DC power 1 activated. |
| PWR2 | Green | Green On | DC power 2 activated. |
| ETH1 | Green/Amber | On | Port link up at 10Mbps /1000Mbps. |
| | Green | On | Port link up at 100Mbps. |
| | | Blinking | Data transmitted. |
| ETH2 | Green/Amber | On | Port link up at 10Mbps/1000Mbps. |
| | Green | On | Port link up at 100Mbps. |
| | | Blinking | Data transmitted. |
| WLAN | Green | On | WLAN activated. |
| | | Blinking | WLAN Data transmitted. |
| WAN | Green | On | Modem Ready |
| Fault | Red | On | Fault relay. Power failure or Port down/fail. |

Cables and Antenna

4.1 Ethernet Cables

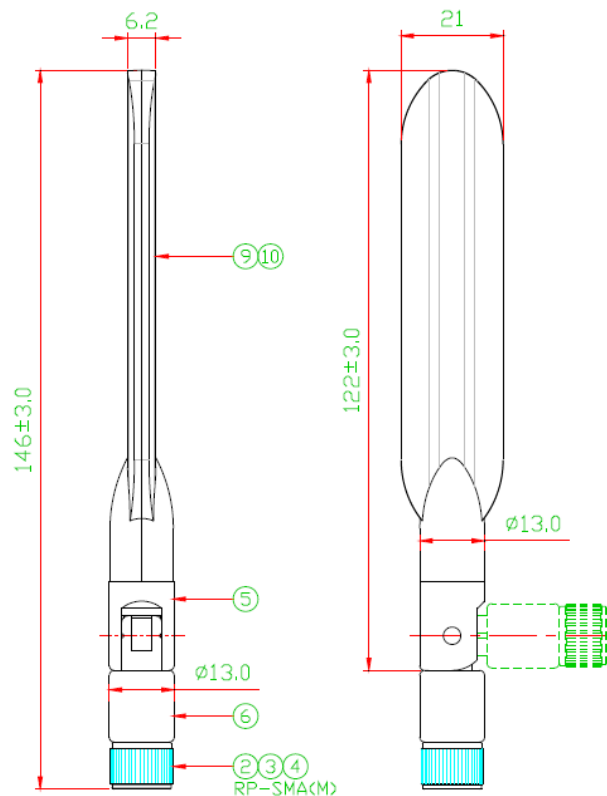
The IGAR-1042/1062-3G WLAN AP has two 10/100/1000 Base-T(X) Ethernet ports. According to the link type, the AP use CAT 3, 4, 5, 5e, 6 UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

| Cable | Type | Max. Length | Connector |
|---------------|----------------------|--------------------|-----------|
| 10Base-T | Cat. 3, 4, 5 100-ohm | UTP 100 m (328 ft) | RJ45 |
| 100Base-T(X) | Cat. 5 100-ohm UTP | UTP 100 m (328 ft) | RJ45 |
| 1000Base-T(X) | Cat 5e, 6 | UTP 100 m (328 ft) | RJ45 |

4.2 Wireless Antenna

2.4GHz/5GHz antenna is used for IGAR-1042/1062-3G and connected with a reversed SMA connector. External RF cable and antenna also can be applied with this connector.



4.3 Cellular Antenna

850/900/1800/2100MHz antenna is used for built-in modem. External RF cable and antenna also can be applied with this connector.

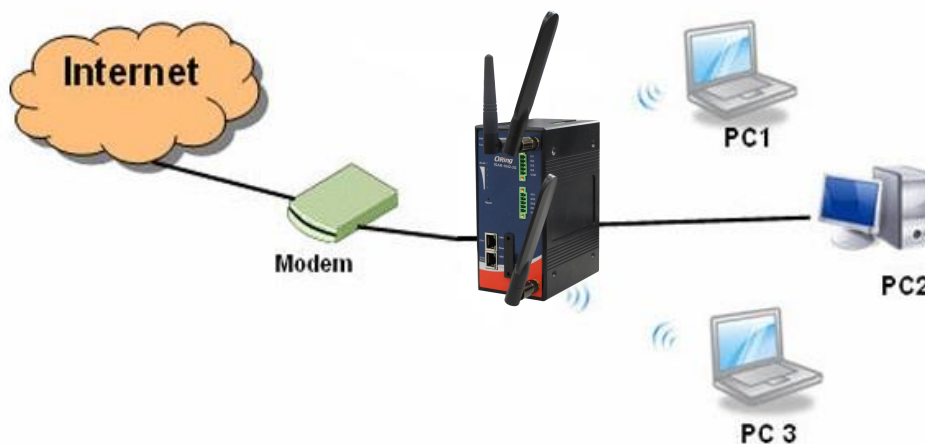


Cellular Antenna

Management Interface

5.1 First-time Installation

Before installing IGAR-1042/1062-3G WLAN AP router, you need to access the WLAN AP router by a computer equipped with an Ethernet card or wireless LAN interface. Using an Ethernet card to connect to LAN port is easier and recommended.



Basic connection for IGAR-1042/1062-3G

Step 1: Select the Power Source

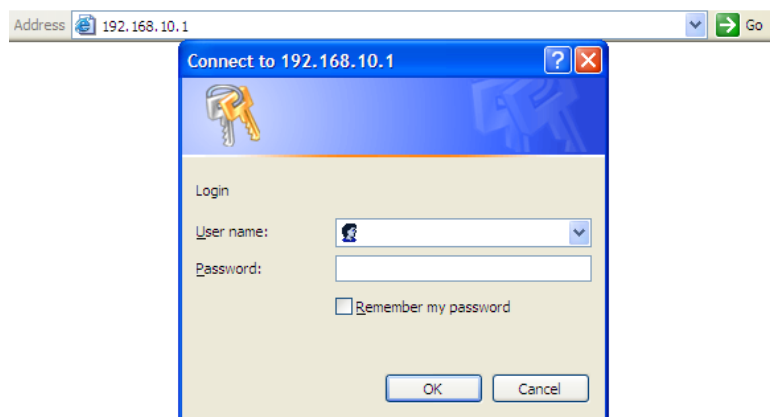
IGAR-1042/1062-3G AP router can be powered by +12~48V DC power input, or by P.O.E. (Power over Ethernet) PSE Ethernet switch.

Step 2: Connect a computer to IGAR-1042/1062-3G

Use either a straight-through Ethernet cable or cross-over cable to connect to ETH1 of IGAR-1042/1062-3G AP router to a computer. If the LED of the LAN port lights up, it indicates the connection is established. After that, the computer will initiate a DHCP request to get an IP address from the AP router.

Step 3: Use the web-based manager to configure IGAR-1042/1062-3G

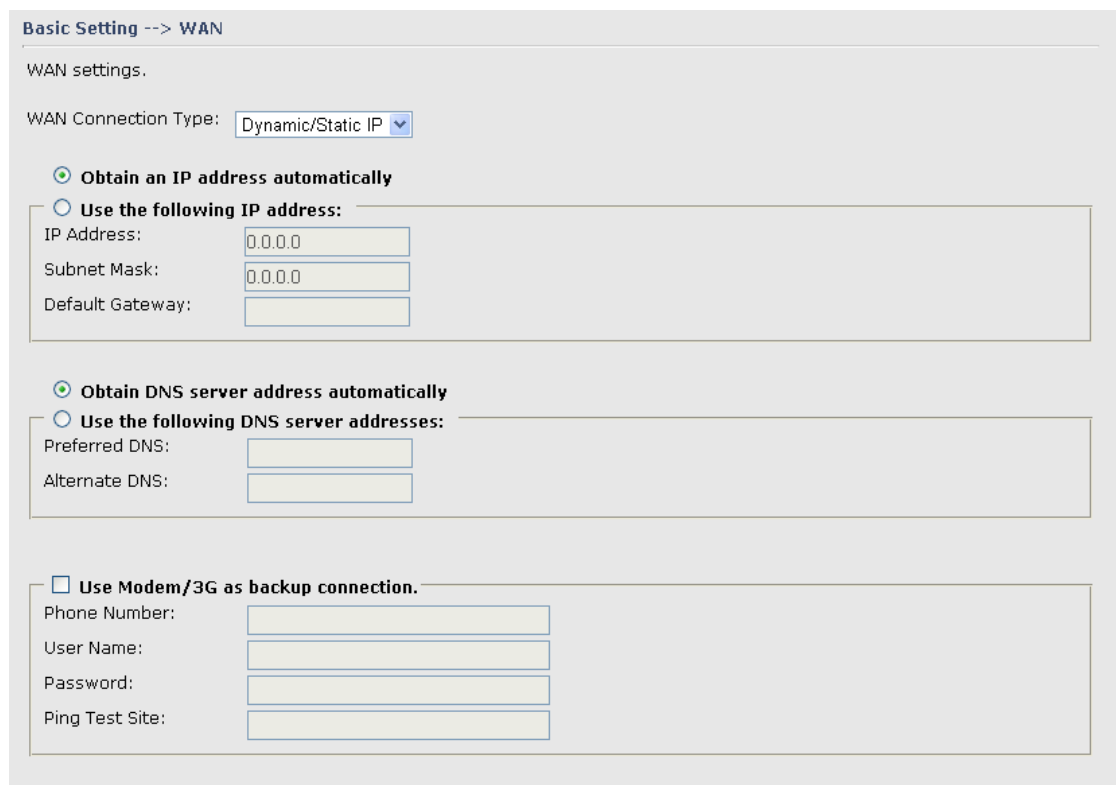
The default gateway IP of IGAR-1042/1062-3G AP router is 192.168.10.1. Start the web browser of your computer and type <http://192.168.10.1> in the address box to access the webpage. A login window will popup, and then enter the default login name **admin** and password **admin**.



Login screen

Step 4: Select WAN connection type

Click the **Basic Setting** in the top menu to enter the **WAN** configuration page, select the proper connection type according to the information of your ISP. If you use **modem/3G** as WAN connection



WAN connection type

Step 5: Protect the wireless access in encryption mode

Click the **Wireless** in **Basic Setting** menu, default encryption mode is **None**, choose WEP/WPA to enhance the security of wireless connection.

Basic Setting --> Wireless LAN

These are the basic wireless settings for the Storage Router.

Basic wireless settings for the AP.

Wireless: Enabled Disabled

SSID:

Channel:

Master Mode:

Security Options

Security Type:

- None
- WEP
- WPA/WPA2 Personal
- WPA/WPA2 Enterprise
- 802.1X

Wireless security option

Step 6: Review the router settings and check router status

Click the **System Status** in the top of the menu, the system info page will be shown. You can check all the configuration and status of the router.

System Status --> System Info

System Info.

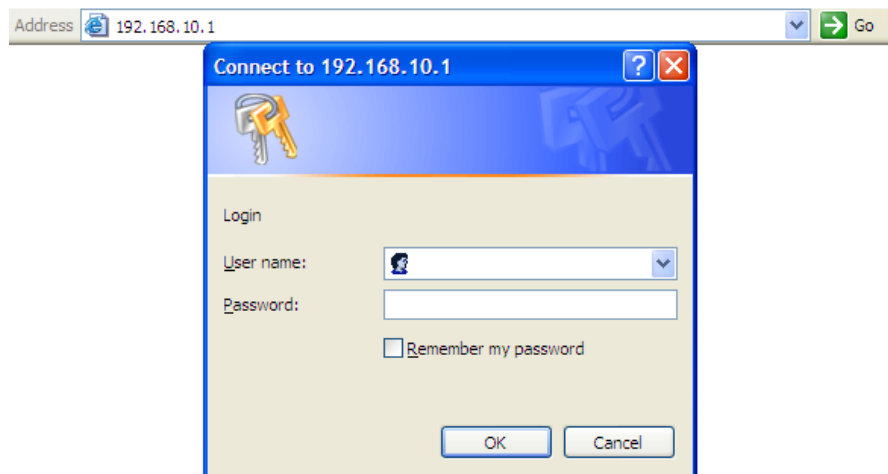
| | | |
|---------------------------|--|-------------------|
| Model: | IGAR-1042+-3G | |
| Model Description: | Industrial IEEE 802.11 b/g/n 3G Cellular 1000Base-T(X) with PoE VPN Router | |
| WAN: | Mode | Dynamic Setting |
| | IP Address | 192.168.2.173 |
| | Broadcast Address | 192.168.2.255 |
| | Subnet Mask | 255.255.255.0 |
| | Default Gateway | 192.168.2.1 |
| | DNS(Primary) | 192.168.2.6 |
| | DNS(Secondary) | 168.95.192.1 |
| | MTU | 1500 |
| | MAC Address | 00:1E:94:77:66:44 |
| LAN: | IP Address | 192.168.10.1 |
| | Subnet Mask | 255.255.255.0 |
| | MTU | 1500 |
| | MAC Address | 00:1E:94:99:55:67 |
| | DHCP Server | Enabled |
| Wireless: | Wireless | Enabled |
| | SSID | oring |
| | Channel | Auto |
| | Encryption Mode | None |

System status Screen

5.2 Configure the Wireless Router

In this section, the web management page will be explained in detail.

By default setting, you can type <http://192.168.10.1> in the address box of web browser to login the web management interface. A login window will be prompted, enter username **admin** & password **admin** to login.

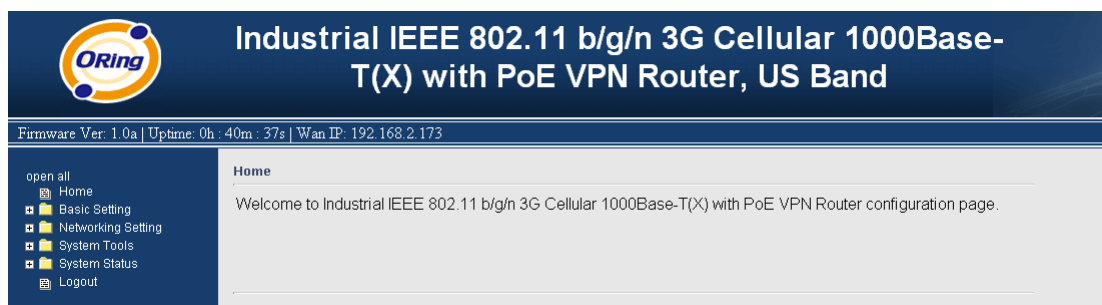


Login screen

For security reasons, we strongly recommend you to change the password. Click on **System Tools > Login Setting** and change the password.

5.3 Main Interface

The **Home** screen will be shown when login successfully.



Main Interface

In the page, you can check the Firmware version, the router running time and the WAN IP setting.

The following table describes the labels in this screen.

| Label | Description |
|----------|---|
| Firmware | Show the current firmware version. |
| Uptime | Show the elapsed time since the AP router is started. |
| Wan IP | Show the WAN IP address. |

5.3.1 Basic Setting

WAN

The IGAR-1042/1062-3G AP router provide four types of WAN connection.

1. WAN Connection Type: Dynamic/Static IP

Basic Setting --> WAN

WAN settings.

WAN Connection Type: Dynamic/Static IP

Obtain an IP address automatically

Use the following IP address:

IP Address:

Subnet Mask:

Default Gateway:

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS:

Alternate DNS:

Use Modem/3G as backup connection.

Phone Number:

User Name:

Password:

Ping Test Site:

Dynamic/Static IP

The following table describes the labels in this screen.

| Label | Description |
|------------------------------------|---|
| Obtain an IP address automatically | Select this option if you would like to have an IP address assigned automatically from the WAN port by DHCP server in your network. |
| Use the following IP address | Select this option if you would like to assign an IP address to the WAN port manually. You should set the IP Address, Subnet Mask and Default gateway appropriately so that they comply with IP |

| | |
|--|--|
| | rules. |
| Obtain DNS server address automatically | Obtain DNS server from DHCP server. If the above Obtain an IP address automatically is selected, this option will be chosen accordingly. |
| Use the following DNS server addresses | Specify DNS server address manually. |
| Use Modem/3G as backup connection | <p>Enable this option if you want to use Modem/3G as a backup connection when normal connection is lost.</p> <p>Phone Number, User Name and Password: Use these settings to dial up the Modem/3G connection.</p> <p>Ping Test Site: Use this site address to check if the connection is alive or lost. Take www.google.com as an example.</p> |

2. WAN Connection Type: PPPoE

Basic Setting --> WAN

WAN Settings.

WAN Connection Type:

User Name:

Password:

Service Name: (optional)

AC Name: (optional)

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

IP Address:

Preferred DNS:

Alternate DNS:

Connection Mode

Auto

Connect On Demand

Max Idle Time: minutes (0 represents never bring down the link)

Manual

Use Modem/3G as backup connection.

Phone Number:

User Name:

Password:

Ping Test Site:

PPPoE Screen.

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| User Name / Password | Enter the username & password provided by your Internet Service Provider (ISP). |
| Service Name | Enter the service name provided by your ISP. |
| AC Name | Enter the name of the access concentrator as provided by your ISP. |
| Specify the IP & DNS provided by ISP | Enter static IP and DNS address which may required by some ISP |
| Connection Mode | Auto: Connect automatically when the router boots up. Connect on Demand: Select to disconnect the PPP session if the router has had no traffic for the specified amount of time. Enter the Max Idle Time in minutes. Manual: Select this option to use only the Connect/Disconnect buttons to call up or close the connection. |
| Use Modem/3G as backup connection | Enable this option if you want to use Modem/3G as a backup connection when PPPoE connection is lost. Phone Number, User Name and Password: Use these settings to dial up the Modem/3G connection. Ping Test Site: Use this site address to check if the connection is alive or lost. Example is as www.google.com |

3. WAN Connection Type: Modem / 3G

Basic Setting --> WAN

WAN Settings.

WAN Connection Type:

Phone Number:

APN:

User Name:

Password:

Baud Rate:

PIN: Enable PIN check before dialing
PIN Code:

Auto Connect : Enable

Reconnect on Failure: Enable

Fast Mode: Enable

Two LAN Ports: Enable

Device Status : Modem not available.

Operations :

Link Status : Disconnected

Modem Status: Operator:
RadioType:
Signal Quality:

Modem/3G Screen

The following table describes the labels in this screen.

| Label | Description |
|----------------------|--|
| Phone Number | Telephone number provided by your ISP. |
| APN | Enter the APN value it is optional. |
| User Name | User name provided by your ISP. |
| Password | Password provided by your ISP. |
| PIN | Enter the PIN code if PIN check is required. |
| Auto Connect | If this option is enabled, the connection will be called up when router boots up. |
| Device Status | Show the status of Medem/3G device. |
| Operations | Click " Connect " to call up the Modem/3G. Click " Disconnect " to shut down the connection. |

Link Status

 Show the status of connection, **up**, **down** or **connecting**.

4. WAN Connection Type: Wireless client

Basic Setting --> WAN

WAN Settings.

WAN Connection Type:

IP Config Setting.

Obtain an IP address automatically

Use the following IP address:

IP Address:

Subnet Mask:

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: (Dropdown menu: None, WEP, WPA-PSK/WPA2-PSK)

Options:

Two LAN Ports: Enable

Use Modem/3G as backup connection.

Phone Number:

User Name:

Password:

Ping Test IP Address:

Wireless Client on WAN

| Label | Description |
|---|---|
| Obtain an IP address automatically | Select this option if you would like to have an IP address assigned automatically from the WAN port by DHCP server in your network. |
| Use the following IP address | Select this option if you would like to assign an IP address to the WAN port manually. You should set the IP Address, Subnet Mask |

| | |
|--|--|
| | and Default gateway appropriately so that they comply with IP rules. |
| Obtain DNS server address automatically | Obtain DNS server from DHCP server. If the above Obtain an IP address automatically is selected, this option will be chosen accordingly. |
| Use the following DNS server addresses | Specify DNS server address manually. |
| Peer AP SSID | Enter the other AP or AR SSID which you want to client |
| Site Scan | You can scan the SSIDs which used for AP mode in the certainty area |
| Security Type | Set the same security with the Client unit which you want to connect. |
| Use Modem/3G as backup connection | <p>Enable this option if you want to use Modem/3G as a backup connection when normal connection is lost.</p> <p>Phone Number, User Name and Password: Use these settings to dial up the Modem/3G connection.</p> <p>Ping Test Site: Use this site address to check if the connection is alive or lost. Take www.google.com as an example.</p> |

LAN

These are the IP settings of the LAN interface for the IGAR-1042/1062-3G WLAN AP router. The LAN IP address is privately for your internal network and can not be exposed on the Internet.

Basic Setting --> LAN

LAN Side settings.

Router Name:

IP Address:

Subnet Mask:

LLDP Protocol: Enable Disable

LAN Screen

The following table describes the labels in this screen.

| Label | Description |
|-------------------|---|
| IP Address | The IP address of the LAN interface, the default IP address is 192.168.10.1 |

| | |
|--------------------|--|
| Subnet Mask | The Subnet Mask of the LAN interface, the default Subnet mask is 255.255.255.0 |
|--------------------|--|

DHCP

DHCP stands for Dynamic Host Control Protocol. The IGAR-1042/1062-3G AP router with a built-in DHCP server. The internal DHCP server will assign an IP address to the computers (DHCP client) on the LAN automatically.

Set your computers to be DHCP clients by setting their TCP/IP settings to Obtain an IP Address Automatically. The DHCP server will allocate an unused IP address from the IP address pool to the requesting computer automatically.

The IP Allocation provides one-to-one mapping of MAC address to IP address. When a computer with the MAC address requesting an IP from the IGAR-1042/1062-3G AP router, it will be assigned with the IP address according to the mapping. You can choose one from the client lists and add it to the mapping relationship.

1. DHCP Sever

Basic Setting --> DHCP --> DHCP Server

Set DHCP Server.

DHCP Mode: Built-in DHCP Server

DHCP Server: Enabled Disabled

Starting IP:

Ending IP:

Lease Time: Hours

Local Domain Name: (optional)

DNS Server 1: (optional)

DNS Server 2: (optional)

WINS Server: (optional)

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

Starting IP:

Ending IP:

Subnet Mask:

List of DHCP Range for Relay:

| # | Starting IP | Ending IP | Subnet Mask | Operations |
|---|-------------|-----------|-------------|------------|
| | | | | |

Allocate IP Address Manually.

-- Choose a Client to Edit --

| MAC Address | IP Address | Operations |
|--|--|---|
| <input style="width: 100px;" type="text"/> | <input style="width: 100px;" type="text"/> | <input type="button" value="Add"/> <input type="button" value="Clear"/> |

Static DHCP Client List:

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

DHCP Server Screen

The following table describes the labels in this screen.

| Label | Description |
|-------------------------------------|---|
| DHCP Mode | Select built-in DHCP server or DHCP Forwarder |
| DHCP Server | Enable or Disable the DHCP Server. The default setting is Enable |
| Starting IP | The starting IP address of the IP range for the DHCP server |
| Ending IP | The ending IP address of the IP range for the DHCP server |
| Lease Time | The period of time for the IP to be leased. Enter the Lease time. The default setting is 48 hours. |
| Local Domain Name | Enter the local domain name of private network. It is optional. |
| DNS Server 1&2 | Enter the DNS Server. It is optional. |
| WINS Server | Enter the WINS Server. It is optional. |
| DHCP Relay start IP | Enter DHCP Relay starting IP |
| DHCP Relay end IP | Enter DHCP Relay Ending IP |
| Subnet Mask | Enter DHCP Relay IP Subnet mask |
| List of DHCP Range for relay | List DHCP Relay IP range |
| Choose a Client to Edit | The list shows the MAC addresses and IP addresses that are already assigned by IGAR-1042/1062-3G. Choose one from the list and click Copy to button for editing. |
| MAC Address | The MAC addresses of the computer. |
| IP Address | The IP address to be related to the MAC address. |
| Static DHCP Client List | The list shows the MAC address and IP address one-to-one relationship. |

Wireless

Basic Setting --> Wireless LAN

These are the basic wireless settings for the Storage Router.

Basic wireless settings for the AP:

Wireless: Enabled Disabled

SSID:

Channel:

Master Mode:

Security Options

Security Type:

Wireless Screen

The following table describes the labels in this screen.

| Label | Description |
|-------------------------|--|
| SSID | Service Set Identifier (SSID) is a unique name that identifies a network. All devices on the network must set the same SSID name in order to communicate on the network. If you change the SSID from the default setting, input your new SSID name in this field. |
| Channel | Channel 6 is the default channel. All devices on the network must share the same channel.* *Note: The wireless devices will automatically scan and match the wireless setting of the AP router with the same SSID. |
| Security options | Select the type of security for WLAN connection: None: NO encryption. WEP: Wired Equivalent Privacy (WEP) is a wireless security protocol for WLAN. WEP provides data encryption for communicating over the WLAN. WPA/WPA2 Personal: WPA-Personal or WPA2-Personal with a pre-shared key, each authorized computer is given the same pass phrase. WPA/WPA2 Enterprise: Wi-Fi Protected Access (WPA) authentication in conjunction with a RADIUS server. 802.1x: Authentication through RADIUS server |

Security Type – None

No security protection for WLAN.

Security Type – WEP

Basic Setting --> Wireless LAN

These are the basic wireless settings for the Storage Router.

Basic wireless settings for the AP:

Wireless: Enabled Disabled

SSID:

Channel:

Master Mode:

Security Options

Security Type:

Auth Mode: Open Shared WEPAUTO

WEP Encryption:

Key Type:

Default Key Index:

KEY1:

KEY2:

KEY3:

KEY4:

Wireless Security Type-WEP Screen

1. Choose one of three Auth Modes: **Open**, **Share** and **WEPAUTO**
2. WEP Encryption: Select 64 Bit or 128 Bit WEP encryption.
3. Key Type: Select **ASCII** or **Hex** key type.
4. Default Key Index: Select one of the keys to be the active key.
5. Key 1-4: Input up to four encryption keys.

ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. **Hex** digits consist of the numbers 0-9 and the letters A-F.

Security Type – WPA/WPA2-Personal

Basic Setting --> Wireless LAN

These are the basic wireless settings for the Storage Router.

Basic wireless settings for the AP.

Wireless: Enabled Disabled

SSID:

Channel:

Master Mode:

Security Options

Security Type:

Auth Mode: WPAPSK WPA2PSK WPAPSK/WPA2PSK mix

Encryption Type: TKIP AES TKIP/AES mix

Shared Key: (8~64 characters)

Wireless Security Type WPA/WPA2 Personal Screen

1. Security Type: Select **WPA/WPA2 Personal**.
2. Choose one of three Auth Modes: **WPAPSK**, **WPA2PSK**, **WPAPSK/WPA2PSK mix**
3. Encryption Type: Select **TKIP** or **AES** or **TKIP/AES mix**.
4. Share Key: Enter your pass phase. The pass phase should be between 8 and 64 characters.

Security Type – WPA /WPA2 Enterprise

Basic Setting --> Wireless LAN

These are the basic wireless settings for the Storage Router.

Basic wireless settings for the AP.

Wireless: Enabled Disabled

SSID:

Channel:

Master Mode:

Security Options

Security Type:

Auth Mode: WPA WPA2 WPA/WPA2 mix

Encryption Type: TKIP AES TKIP/AES mix

Radius Server IP: . . .

Radius Port:

Shared Secret:

Wireless Security Type-WPA/WPA2 Enterprise Screen

1. Security Type: Select **WPA/WPA2 Enterprise**
2. Auth Mode: Choose one of three Auth Modes: **WPA, WPA2, WPA/WPA2 mix**.
3. Encryption Type: Choose one of three Encryption Types: **TKIP, AES, TKIP/AES mix**.
4. Radius Server IP: Enter the IP address of the RADIUS Server.
5. Port: Enter the RADIUS port (1812 is default).
6. Shared Secret: Enter the RADIUS password or key.

Basic Setting --> Wireless LAN

These are the basic wireless settings for the Storage Router.

Basic wireless settings for the AP.

Wireless: Enabled Disabled

SSID:

Channel:

Master Mode:

Security Options

Security Type:

WEP Encryption:

Key Type:

Default Key Index:

KEY1:

KEY2:

KEY3:

KEY4:

Radius Server IP: . . .

Radius Port:

Shared Secret:

Security Type –802.1x

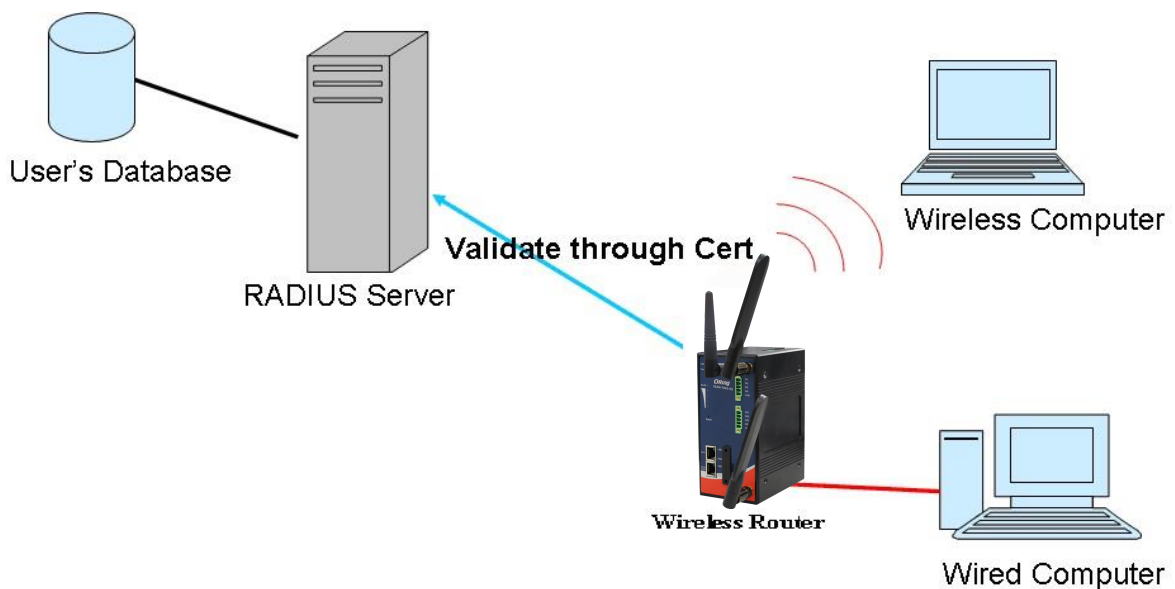
1. Security Type: Select **802.1X**
2. WEP Encryption: Select 64 Bit or 128 Bit WEP encryption.
3. Key Type: Select ASCII or Hex key type.
4. Default Key Index: Select one of the keys to be the active key.
5. Key 1-4: Input up to four encryption keys.
6. Radius Server IP: Enter the IP address of the RADIUS Server.
7. Port: Enter the RADIUS port (1812 is default).

8. Shared Secret: Enter the RADIUS password or key.

RADIUS, or Remote Authentication Dial-In User Service, is a widely deployed protocol that enables companies to authenticate, authorize and account for remote users who want access to a system or service from a central network server.

Radius server validates your proof, also carry on the authorization. So the Radius server received by ISA server responded (point out the customer carries proof to be not granted) and it means that the Radius server did not authorize you to carry. Even if the proof has already passed an identify verification, the ISA server may also refuse you to carry a claim according to the authorization strategy of the Radius server.

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



DDNS

Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP address.

Basic Setting --> DDNS

DDNS settings.

DDNS Service:

User Name: (*)

Password: (*)

Domain: (*)

DDNS Screen

For example, Choose DDNS Service: www.dyndns.org and configure the following instructions:

The following table describes the labels in this screen.

| Label | Description |
|------------------|---|
| User Name | Enter the user name for your DDNS account. |
| Password | Enter the password for your DDNS account. |
| Domain | Enter the domain names provided by your dynamic DNS service provider. |

Date&Time

In this page, you can set the date & time of the device. The correct date & time will be helpful for logging of system events. A NTP (Network Time Protocol) client can be used to synchronize date & time with NTP server through internet.

Basic Setting --> Date & Time

Date/Time settings.

System time: Wed Mar 20 2013 1:42:31

NTP: Enable

NTP Server 1:

NTP Server 2: (optional)

Time Zone: ▼

Synchronise: ▼ at ▼ : ▼

Local Date: Year Month Day

Local Time: Hour Minute Second

Date & Time Screen

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| Local Date | Set local date manually. |
| Local Time | Set local time manually. |
| Time Zone | Select the time zone manually |
| Get Current Date & Time from Browser | Click this button; you can set the time from your browser. |
| NTP | Enable or disable NTP function to synchronize time from the NTP server. |
| NTP Server 1 | The primary NTP Server. |
| NTP Server 2 | The secondary NTP Server. |
| Synchronize | This is the scheduled time when the NTP synchronization performed. |

5.3.2 Networking Setting

Wireless setting

1. Advanced

Wireless performance tuning.

Radio Button: ON OFF

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

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

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

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

Wireless Mode: B Mode BG Mixed Mode BGN Mixed Mode

Max Client Threshold (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:

HT Tx STBC: Disable Enable

HT Rx STBC: Disable Enable

Wireless options interface

The following table describes the labels in this screen.

| Label | Description |
|--------------------------------|--|
| Radio Button | Enable or Disable Wireless function |
| Beacon Interval | The default value is 100. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network. 50 is recommended in poor reception. |
| DTIM Interval | The default value is 1. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. |
| Fragmentation Threshold | This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a |

| | |
|------------------------------|---|
| | packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended. |
| RTS Threshold | This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The AP sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. |
| Wireless Network Mode | You can select 802.11 b/g/n wireless mode mix or single |
| Preamble | Values are Long and Short, default value is Long. If your wireless device supports the short preamble and you are having trouble getting it to communicate with other 802.11b devices, make sure that it is set to use the long preamble |

Extra parameters for Client Mode(X-Roaming)

Roaming: Disabled X-roaming

Scan Channel: All Manual

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

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

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

X-Roaming setting interface

The following table describes the labels in this screen

| Label | Description |
|---------------------|--|
| Roaming | Disable: Disable X-Roaming protocol. X-roaming: Enable X-Roaming protocol |
| Scan channel | All: scan all support channel Manual: only scan "channel select" value |

| | |
|-----------------------|----------------------------------|
| Channel Select | Assign the roaming channel value |
| Sensitivity | Set the signal sensitivity |
| Scan interval | Set the scan interval |

Wireless advance setting Screen

2. MAC Filter

Use **MAC Filter** to allow or deny wireless clients to associate with IGAR-1042/1062-3G AP router. You can manually add a MAC address or select the MAC address from **Associated Clients** that are currently associated with IGAR-1042/1062-3G.

Advanced Setting --> Wireless --> MAC filter

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

MAC Filter: 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: Copy to Slot

MAC Filter Table:

| | | |
|---|---|---|
| 1. <input style="width: 100%;" type="text"/> | 11. <input style="width: 100%;" type="text"/> | 21. <input style="width: 100%;" type="text"/> |
| 2. <input style="width: 100%;" type="text"/> | 12. <input style="width: 100%;" type="text"/> | 22. <input style="width: 100%;" type="text"/> |
| 3. <input style="width: 100%;" type="text"/> | 13. <input style="width: 100%;" type="text"/> | 23. <input style="width: 100%;" type="text"/> |
| 4. <input style="width: 100%;" type="text"/> | 14. <input style="width: 100%;" type="text"/> | 24. <input style="width: 100%;" type="text"/> |
| 5. <input style="width: 100%;" type="text"/> | 15. <input style="width: 100%;" type="text"/> | 25. <input style="width: 100%;" type="text"/> |
| 6. <input style="width: 100%;" type="text"/> | 16. <input style="width: 100%;" type="text"/> | 26. <input style="width: 100%;" type="text"/> |
| 7. <input style="width: 100%;" type="text"/> | 17. <input style="width: 100%;" type="text"/> | 27. <input style="width: 100%;" type="text"/> |
| 8. <input style="width: 100%;" type="text"/> | 18. <input style="width: 100%;" type="text"/> | 28. <input style="width: 100%;" type="text"/> |
| 9. <input style="width: 100%;" type="text"/> | 19. <input style="width: 100%;" type="text"/> | 29. <input style="width: 100%;" type="text"/> |
| 10. <input style="width: 100%;" type="text"/> | 20. <input style="width: 100%;" type="text"/> | 30. <input style="width: 100%;" type="text"/> |

MAC Filter Screen

The following table describes the labels in this screen.

| Label | Description |
|--------------------------|---|
| MAC Filter | Enable or disable the function of MAC filter. |
| MAC Filter List | This list shows the MAC addresses that are in the selected filter. |
| Connected Clients | This list shows the wireless MAC addresses that associated with AP. |
| MAC Address | MAC addresses for editing. |
| Apply | Click Apply to activate the configurations. |

NAT Setting

1. Virtual Server

Virtual Server is used for setting up public services on the LAN, such as DNS, FTP and Email. Virtual Server is defined as a Local Port to the LAN servers, and all requests from Internet to this Local port will be redirected to the computer specified by the Local IP. Any PC that was used for a virtual server must have static or reserved IP Address because its IP address may change when requesting IP by DHCP.

Advanced Setting --> NAT Setting -> Virtual Server

Virtual server settings.

Virtual Server: Enable Disable

Description:

Public IP: All Specify

Public Port:

Protocol: TCP UDP Both

Local IP:

Local Port:

Enable Now: Yes No

Virtual server list:

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

Virtual Server

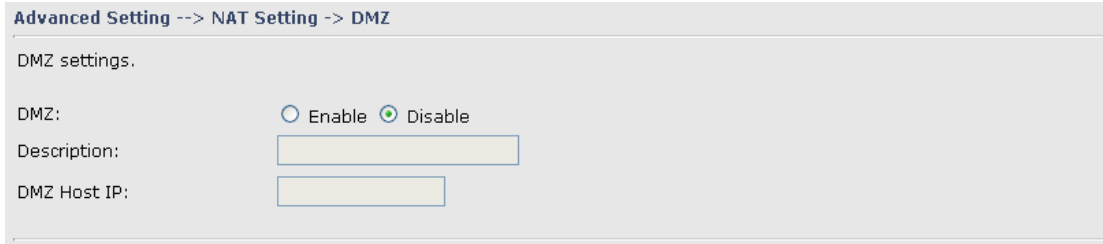
The following table describes the labels in this screen.

| Label | Description |
|----------------------------|--|
| Virtual Server | Enable or disable Virtual Server. |
| Description | Enter the description of the entry. Acceptable characters consist of '0-9', 'a-z', 'A-Z'. This field accepts null value. |
| Public IP | Enter the public IP that is allowed to access the virtual service, if not specified, choose All. |
| Public Port | The port number on the WAN (Wide Area Network) side that will be used to access the virtual service. |
| Protocol | The protocol used for the virtual service. |
| Local IP | The IP of the computer that will be providing the virtual service. |
| Local Port | The port number of the service used by the Private IP computer. |
| Enable Now | Enable the virtual server entry after adding it. |
| Virtual server list | Click Edit to edit the virtual service entry, Del to delete the entry. |

2. DMZ

It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes.

Enter the IP address of the internal computer that will be the DMZ host. Adding a client to the DMZ may expose your local network with variety of security risks, so only use this option carefully.



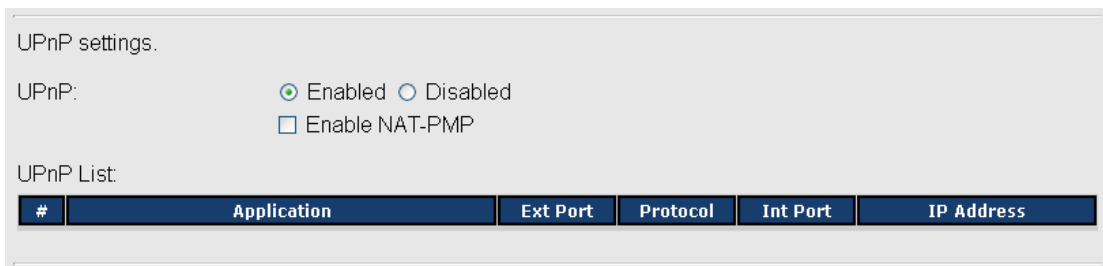
DMZ Screen

The following table describes the labels in this screen.

| Label | Description |
|--------------------|--|
| DMZ | Enable or disable the DMZ. |
| Description | Description for the DMZ host entry. |
| DMZ Host IP | Enter the IP address of the computer to be in the DMZ. |

3. UPnP

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



UPnP Screen

The following table describes the labels in this screen.

| 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 side. 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. Status: This status shows if the entry is valid or not. |

Firewall Setting

1. IP Filter

Filters are used to deny or allow LAN computers from accessing the internet. It also allow or deny WAN hosts to access LAN computers.

Advanced Setting --> Security Setting -> IP Filter

IP filter settings.

IP Filter: Enable Disable

Description:

Rule:

Direction:

IP Address: Source IP:
 Destination IP:

Protocol: All
 ICMP
 Specify protocol number:
 TCP Specify port:
 UDP Specify port:

Enable Now: Yes No

IP filter list:

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

IP Filter Screen

The following table describes the labels in this screen.

| Label | Description |
|-----------------------|--|
| IP Filter | Enable or disable the IP Filter. |
| Description | Enter description for the entry. |
| Rule | Select DROP , ACCEPT and REJECT rule for the entry. |
| Direction | Specify the direction of the data flow that is to be filtered. |
| IP Address | Enter the IP address of the source and destination computer. |
| Protocol | Choose which protocol to be filtered. |
| Enable Now | Enable the entry after adding it. |
| IP filter list | Click edit for editing the entry, click Del to delete the entry. |

2. MAC Filter

Filters are used to deny or allow LAN computers from accessing the internet, according to their MAC address.

Advanced Setting --> Security Setting --> MAC Filter

MAC Filter settings.

MAC Filter: Enable Disable

Description:

Rule:

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

Enable Now: Yes No

MAC filter list:

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

MAC Filter Screen

The following table describes the labels in this screen.

| Label | Description |
|-----------------------|--|
| MAC Filter | Enable or disable the MAC Filter. |
| Description | Enter the description for the entry. |
| Rule | Select DROP , ACCEPT and REJECT rule for the entry. |
| MAC Address | Enter the MAC address to be filtered. |
| Enable Now | Enable the entry after adding it. |
| IP filter list | Click Edit for editing the entry, click Del to delete the entry. |

VPN Setting

VPN Setting is settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin, authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

1. Open VPN

Open VPN is a full-functioned SSL VPN solution which can accommodate a wide range of configurations including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls.

Advanced Setting --> Vpn Setting -> Openvpn

Openvpn settings.

Server settings.

Openvpn Server: Enable Disable

Tunnel Protocol:

Port:

LZO Compression: Enable Disable

Keys Setting:

Client settings.

Openvpn Client: Enable Disable

Server IP/Host Name:

Tunnel Protocol:

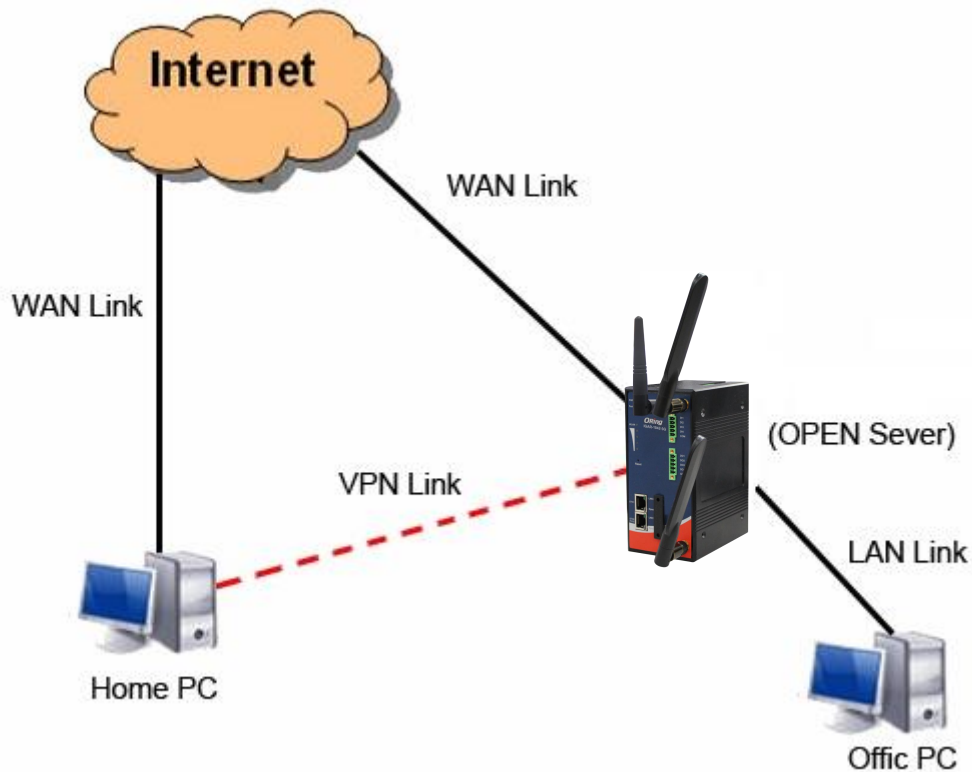
Port:

LZO Compression: Enable Disable

Keys Setting:

Open VPN Screen

The following topology shows the common use of VPN connection from WAN side.



1: Open VPN Server

Connection to Open VPN Server

Before connecting to the Openvpn server of IGAR-1042/1062-3G AP router, please install openvpn client software for your windows PC. It can be download from <http://openvpn.net/download.html#stable>. The current version of Openvpn used in IGAR-1042/1062-3G is version 2.0.9. The corresponding software for client should be installed.

The following table describes the labels in this screen.

| Label | Description |
|------------------------|---|
| Open VPN Server | Enable or disable the function of Open VPN Server. |
| Tunnel Protocol | Select UDP or TCP protocol. |
| Port | Input the number about the port, and the default is 1194. |
| LZO Compression | Enable or disable the function of LZO Compression. |
| Keys Setting | Select Auto to use the preset certificates, select Manual to paste your certificates. Please install openvpn client software to generate your certificates and paste them here. For more information, please visit openvpn website. |

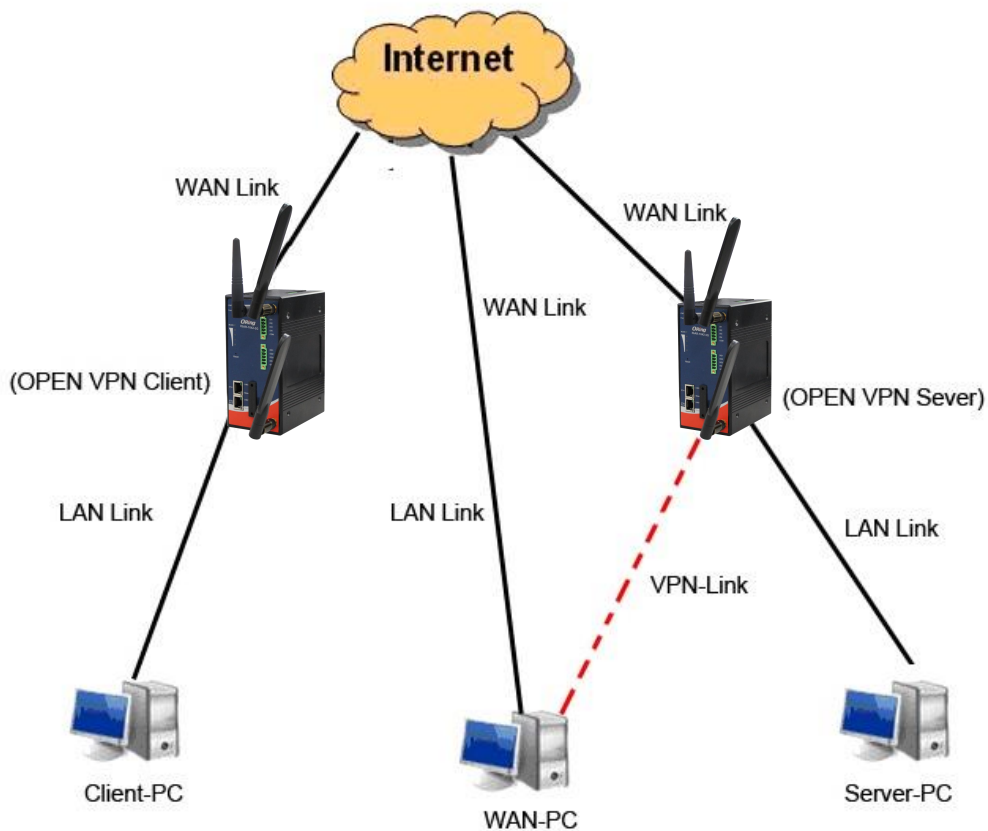
2: Open VPN Client

Two routers are needed for creating site-to-site VPN connection using this mode.

The following table describes the labels in this screen.

| Label | Description |
|------------------------|---|
| Open VPN Client | Enable or disable the function of Open VPN Client. You can allow or deny the Open VPN Client with this option. |
| Server IP | Enter the Open VPN Server IP address. |
| Tunnel Protocol | Select UDP or TCP protocol. |
| Port | Enter the port number, default is 1194. |
| LZO Compression | Enable or disable the LZO Compression. |
| Keys Setting | Select Auto to use the preset certificates, select Manual to paste your certificates. Please install software for openvpn client to generate your certificates and paste them here. For more information, please visit openvpn website. |

3: Open VPN Server VS Client



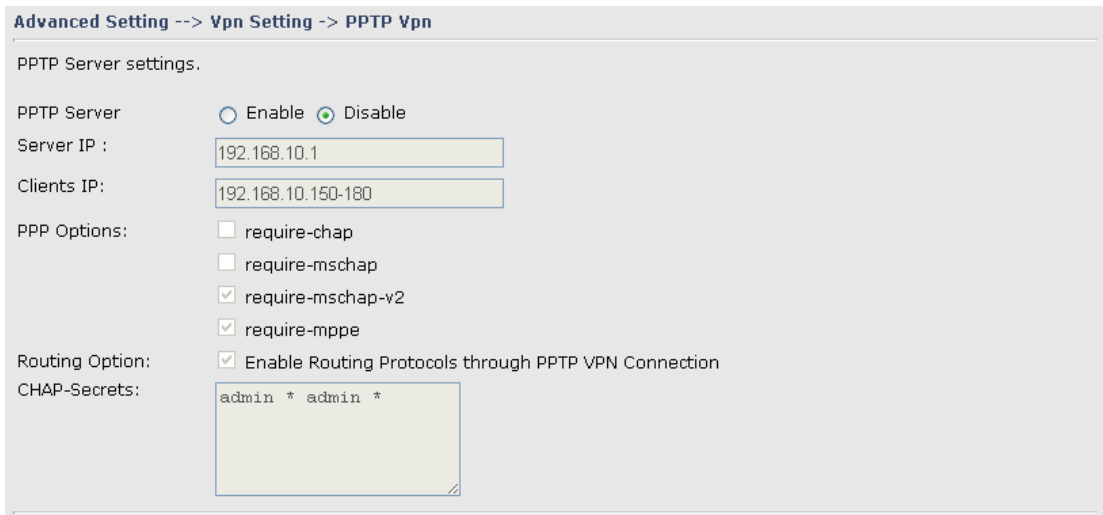
Client-PC and connect to Server-PC,WAN-PC

The chart above displays the connection of Open VPN Server and Client. The Server IP and Client IP address should configure with the same network domain.

2. PPTP VPN

The PPTP (Point to Point Tunneling Protocol) VPN feature allows PC connected to the router from WAN port, just like connecting in the LAN.

To create a PPTP connection to the router, you should create a PPTP network connection if you are using a window PC. The steps are: **Right click Network > property > create a new connection > connect to my work space (VPN) > use VPN to internet > enter the user name and password** which are set in the page.

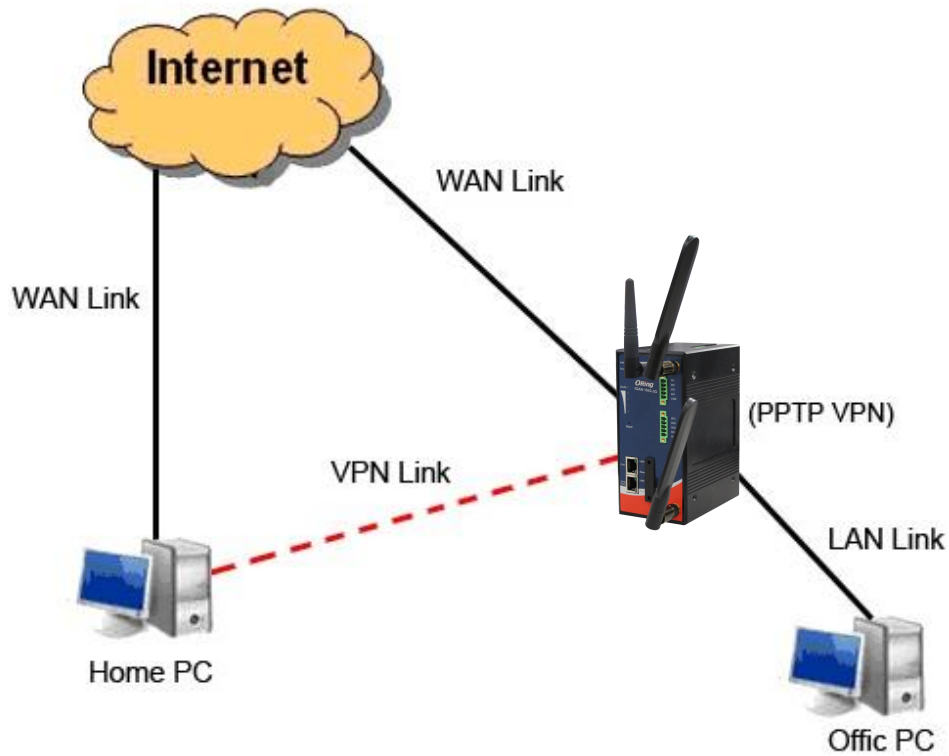


The screenshot shows the configuration page for PPTP VPN. The breadcrumb path is "Advanced Setting --> Vpn Setting -> PPTP Vpn". The page title is "PPTP Server settings." The configuration options are as follows:

- PPTP Server: Enable Disable
- Server IP:
- Clients IP:
- PPP Options:
 - require-chap
 - require-mschap
 - require-mschap-v2
 - require-mppe
- Routing Option: Enable Routing Protocols through PPTP VPN Connection
- CHAP-Secrets:

PPTP VPN Screen

The following topology shows the common use of PPTP connection from the internet.



Connection to PPTP VPN Server

The following table describes the labels in this screen.

| Label | Description |
|---------------------|---|
| PPTP Server | Enable or disable PPTP VPN Server. |
| Server IP | Enter the server side IP address, default is the LAN port IP. |
| Client IP | Enter the IP address range, format is as 192.168.10.xx-xx , connected client will be assigned the IP address. |
| CHAP-Secrets | Enter the username and password pairs, format is as user * pass *, multiple username password pairs are allowed. |

3. PPTP Client

If the router A want to link with the others which is not in the same network with the router A, the function of PPTP client should support in the router page.

Advanced Setting --> Vpn Setting -> PPTP Client

PPTP Client settings.

PPTP Client Enable Disable

Server IP/Hostname:

Username:

Password:

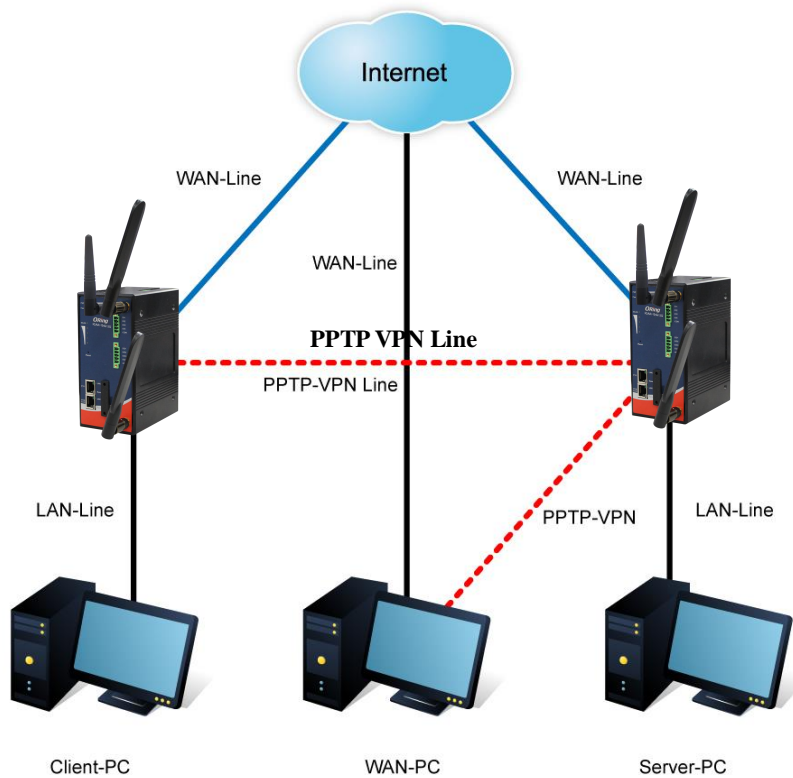
Options:

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

Routing Option: Enable Routing Protocols through PPTP Client Connection

Operations:

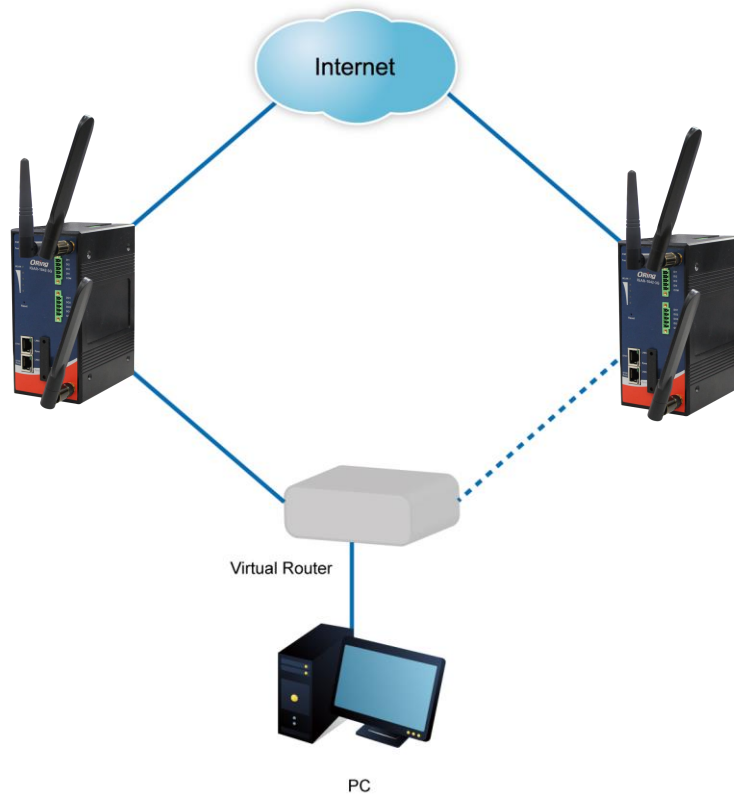
Link Status: Disconnected





| Label | Description |
|---------------------------|--|
| PPTP Client | Enable or disable PPTP Client. |
| Server IP/Hostname | Enter the server IP address or hostname. |
| Username/Password | Enter the username and password which is signed by PPTP server. |
| Option | <p>Reconnect on failure: Pitch on this option, it will be reconnect when the link is on failure.</p> <p>Require MPPE: Choose Enable Require MPPE (Microsoft Point-to-Point Encryption) to encrypt data across Point-to-Point Protocol (PPP) and Virtual Private Network links.</p> |
| Operations | Click "Connect" to link the server, if or not, you can click "Disconnect" to break off from the server. |
| Link Status | Show the status about the link. |

VRRP



VRRP(Virtual Router Redundancy Protocol) settings.

VRRP Protocol: Enable Disable

VRRP Instance State: Master Backup

Virtual Router ID:

Virtual Router IP:

Priority: (1~254)

Authentication Password:

Routing Protocol (Routing Setting)

This page shows the information of routing table. The initial state of the router connect to the WAN, it will be based on the outside networks to access the routing table automatically. You can refer the shows about the bellow page.

Current Routing Table:

| Destination | Gateway | Subnet Mask | Metric | Interface |
|--------------|-------------|---------------|--------|--------------|
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | 0 | eth1(WAN) |
| 192.168.10.0 | 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) |
| default | 192.168.2.1 | 0.0.0.0 | 0 | eth1(WAN) |

The table shows the normal routing table

1. Use Dynamic Routing

Use the dynamic routing, you should not choose “Disable” about the **RIPv1 & v2** in the routers.

Click “Apply”, and you can see the more information in the **Current Routing Table**, which shows the network segment of the other router.

Advanced 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 | eth1(WAN) |
| 192.168.10.0 | 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) |
| default | 192.168.2.1 | 0.0.0.0 | 0 | eth1(WAN) |

Static Route Entry:

| Destination | Gateway | Subnet Mask | Metric | Interface | Operations |
|----------------------|----------------------|----------------------|----------------------|-----------|------------------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | WAN | <input type="button" value="Add"/> |

Mode:

RIPv1 & v2:

Telnet Setting: Enable Disable

Port:

Password:

| Label | Description |
|------------------------------|---|
| Current Routing Table | Show the current the routing information. |
| Static Router Entry | Not RIP and enter the right value in the textbox will be showing. |
| Mode | If you want to the PC in the router can visit the outside network, only choose the Gateway Mode ; if or not, you choose the Router Mode . |
| RIPv1 & v2 | Choose “Disable” in the Static routing. |
| Telnet Setting | Only use in the Dynamic routing. |

Simultaneously, only use the Telnet function in the dynamic routing. You can telnet the LAN IP and there are many orders.

```

C:\ 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
  
```

2. Use Static Routing

Use the Static routing, you should choose “Disable” about the **RIPv1 & v2** in the routers.

Click “Apply”, and you can see the more information in the **Current Routing Table** and **Static Route Entry**, which shows the network segment of the other router.

Advanced 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 | eth1(WAN) |
| 192.168.11.0 | 0.0.0.0 | 255.255.255.0 | 0 | eth1(WAN) |
| 192.168.10.0 | 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) |
| default | 192.168.2.1 | 0.0.0.0 | 0 | eth1(WAN) |

Static Route Entry:

| Destination | Gateway | Subnet Mask | Metric | Interface | Operations |
|----------------------|----------------------|----------------------|----------------------|-----------|---|
| 192.168.11.0 | 0.0.0.0 | 255.255.255.0 | 0 | WAN | <input type="button" value="Commit"/> <input type="button" value="Delete"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | WAN | <input type="button" value="Add"/> |

Mode:

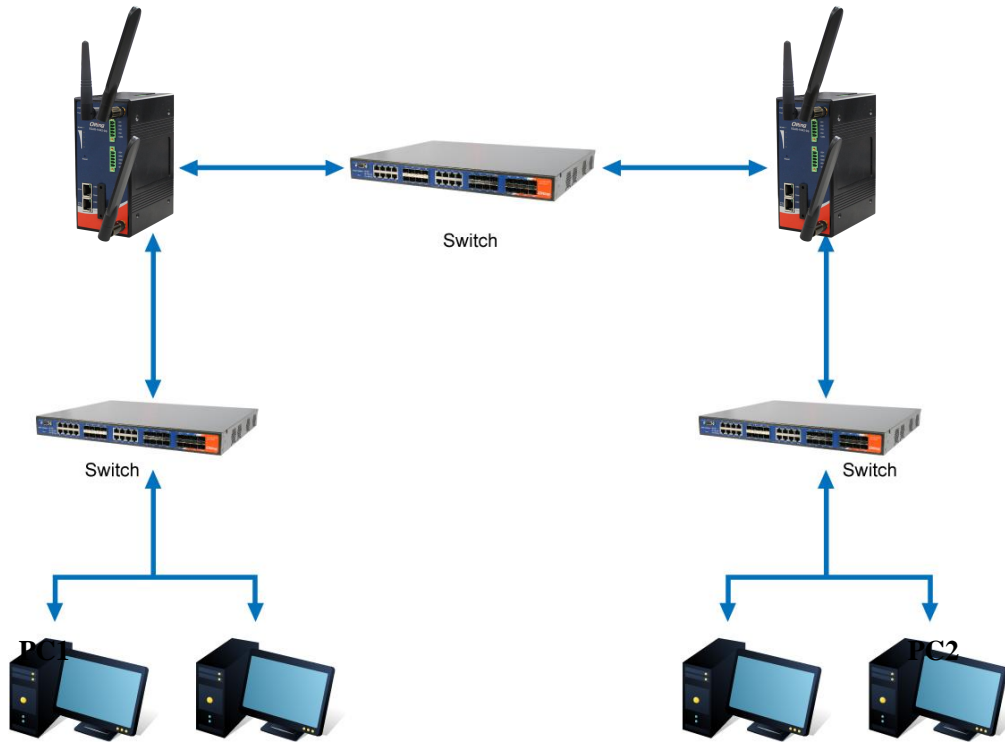
RIPv1 & v2:

Telnet Setting: Enable Disable

Port:

Password:

Use the dynamic routing; it will have many ways such as RIP, OSPF.BGP. In this router, we use the RIP Protocol to finish the dynamic routing table.



The Routing Topography

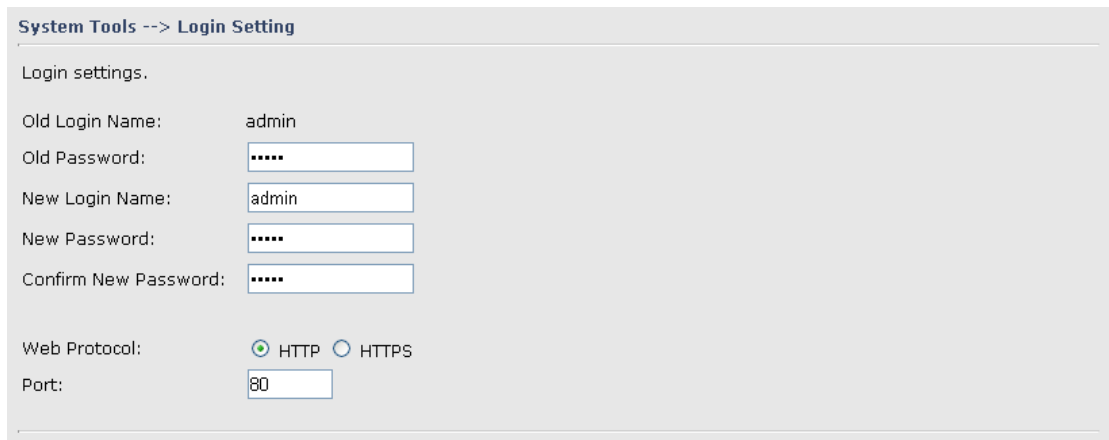
RIP, Routing Information Protocol, is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP) using the distance-vector routing algorithm.

After all settings, PC1 can visit PC2 which is different network segment of the PC1.

5.3.3 System Tools

Login Setting

At this page, the administrator can change the login name and password. The default name and password is **admin** and **admin**.



System Tools --> Login Setting

Login settings.

Old Login Name: admin

Old Password: [masked]

New Login Name: admin

New Password: [masked]

Confirm New Password: [masked]

Web Protocol: HTTP HTTPS

Port: 80

Login Setting Screen

The following table describes the labels in this screen.

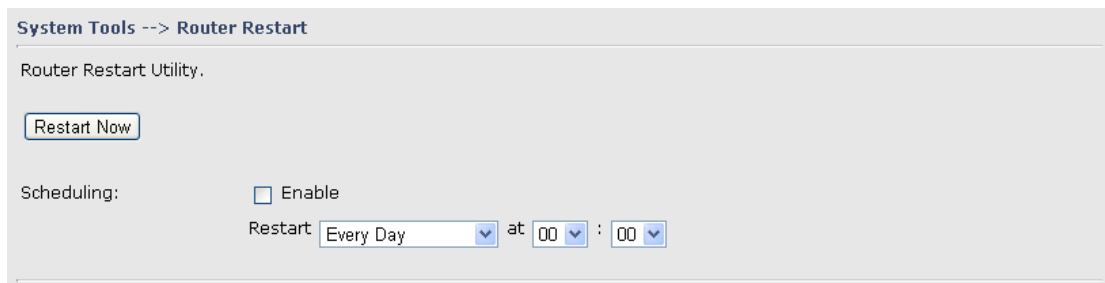
| Label | Description |
|-----------------------------|---|
| Old Name | This field shows the old login name. |
| Old Password | Before making a new setting, you should provide the old password for verification. Acceptable characters of this field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length. An empty password is also acceptable. |
| New Name | Enter a new login name. Acceptable characters of this field contains '0-9', 'a-z', 'A-Z' and must be between 1 to 15 characters in length. An empty name is not acceptable. |
| New Password | Enter a new login password. Acceptable characters of this field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length. |
| Confirm New Password | Retype the password to confirm it. Acceptable inputs of this field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length. |

| | |
|---------------------|---|
| Web Protocol | Choose the web management page protocol. HTTP and HTTPS are both supported. |
| Port | Choose the web management page port number. For HTTP, default port is 80; For HTTPS, default port is 443. |

HTTPS (HTTP over SSL) is a Web protocol which encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

Router Restart

If you want restart the router through the **Warm Reset**, click **Restart Now** to restart the Wireless Router. Also, you can set a **Scheduling** time to make the router restart.



System Tools --> Router Restart

Router Restart Utility.

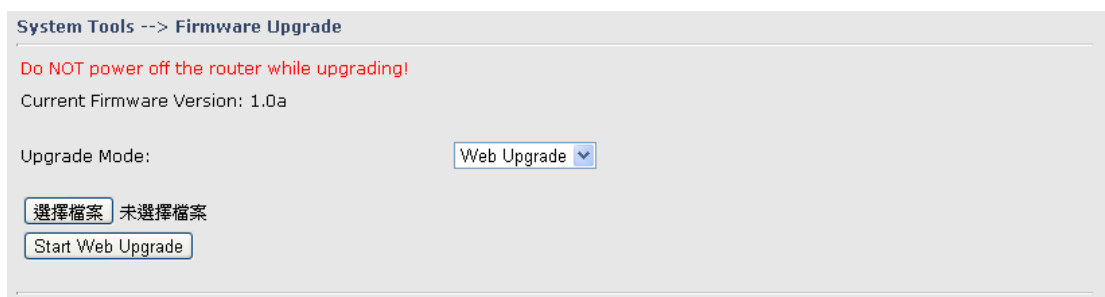
Restart Now

Scheduling: Enable

Restart: Every Day at 00 : 00

Router Restart Screen

Firmware Upgrade



System Tools --> Firmware Upgrade

Do NOT power off the router while upgrading!

Current Firmware Version: 1.0a

Upgrade Mode: Web Upgrade

選擇檔案 未選擇檔案

Start Web Upgrade

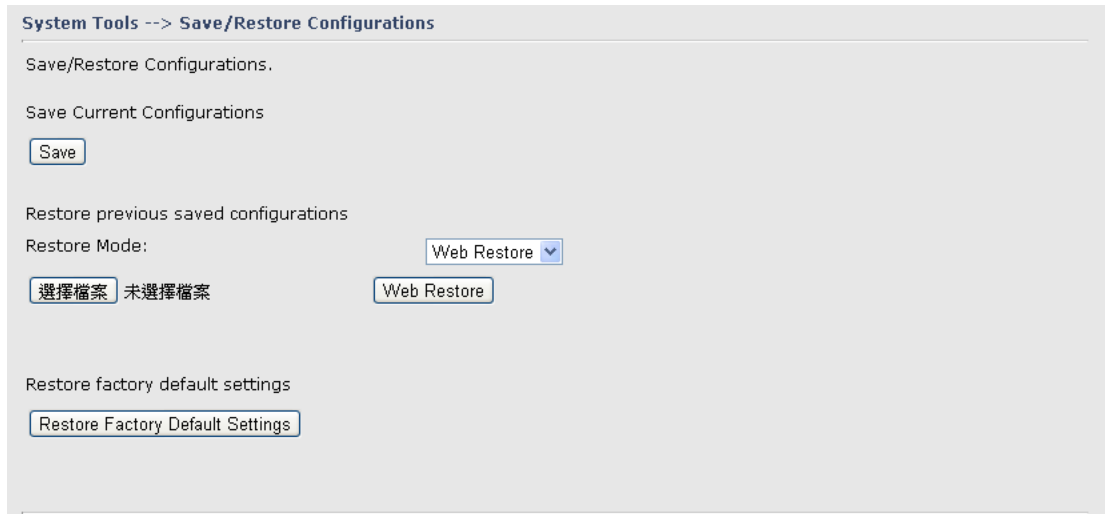
Firmware Upgrade Screen

Newer firmware may provide better performance or function extensions. To upgrade the new firmware, you need a firmware file which matches the model of this AP router. It will take several minutes to upload and update the firmware. After the upgrade is done successfully, reboot the router to utilized new firmware.

Important Notice: DO NOT POWER OFF THE ROUTER OR PRESS THE RESET

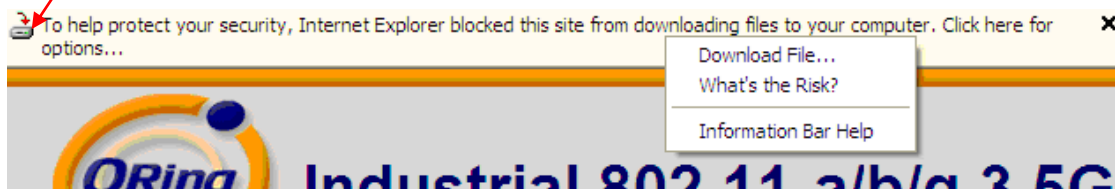
BUTTON WHILE THE FIRMWARE IS BEING UPGRADED.

Save/Restore Configurations



Save/Restore Configurations Screen

Save: The configuration file can be downloaded. (Internet Explorer user will need to click on the protection bar on top and click choose “download files”)



The following table describes the labels in this screen.

| Label | Description |
|---------------------------------|--|
| Download configuration | The current system settings can be saved as a file into your PC. |
| Upload configuration | The configuration can be restored to the router. To reload a system settings file, click on Browse to browse your local hard drive and locate the system settings file previously saved. Click Upload when you have selected the file. |
| Restore Default Settings | You may also reset the router to the factory settings by clicking on Restore Default Settings . The router will reboot to validate the default settings. |

Miscellaneous (Ping)

System Tools --> Miscellaneous

Miscellaneous utilities.

Ping Test: Destination:

Ping Test Result:

Miscellaneous Screen

The Ping Test is used to send Ping packets to test if a computer whether it is on the Internet or test if the WAN connection is OK. Enter a domain or IP in the destination box and click Ping to test.

Even warning setting

1. System Log

Syslog Server Settings

Syslog Server IP:

Syslog Server Port: (0 represents default)

Syslog Event Types

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

| Fault Event Notification | |
|--------------------------|---------------------------------|
| Power 1 Fault | <input type="checkbox"/> Syslog |
| Power 2 Fault | <input type="checkbox"/> Syslog |
| POE Fault | <input type="checkbox"/> Syslog |
| Eth1 Link Down | <input type="checkbox"/> Syslog |
| Eth2 Link Down | <input type="checkbox"/> Syslog |
| D11 ON->OFF | <input type="checkbox"/> Syslog |
| D12 ON->OFF | <input type="checkbox"/> Syslog |
| D13 ON->OFF | <input type="checkbox"/> Syslog |
| D14 ON->OFF | <input type="checkbox"/> Syslog |
| D11 OFF->ON | <input type="checkbox"/> Syslog |
| D12 OFF->ON | <input type="checkbox"/> Syslog |
| D13 OFF->ON | <input type="checkbox"/> Syslog |
| D14 OFF->ON | <input type="checkbox"/> Syslog |

System Log setting interface

The following table describes the labels in this screen.

| Label | Description |
|-------------------------|--|
| Syslog Server IP | Not only the syslog keeps the logs locally, it can also log to remote server. Specify the IP of remote server. Leave it blank to disable logging remotely. |

Syslog Server Port

Specify the port of remote logging. Default port is 514.

2. E-Mail

E-mail Server Settings

 SMTP Server: (optional)

 Server Port: (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) | <input type="checkbox"/> SMTP Mail |
| Software Reset (Warm Start) | <input type="checkbox"/> SMTP Mail |
| Login Failed | <input type="checkbox"/> SMTP Mail |
| WAN IP Address Changed | <input type="checkbox"/> SMTP Mail |
| Password Changed | <input type="checkbox"/> SMTP Mail |
| Redundant Power Changed | <input type="checkbox"/> SMTP Mail |
| Eth Link Status Changed | <input type="checkbox"/> SMTP Mail |
| SNMP Access Failed | <input type="checkbox"/> SMTP Mail |
| Wireless Client Associated | <input type="checkbox"/> SMTP Mail |
| Wireless Client Disassociated | <input type="checkbox"/> SMTP Mail |
| Client Mode Associated | <input type="checkbox"/> SMTP Mail |
| Client Mode Disassociated | <input type="checkbox"/> SMTP Mail |

| Fault Event Notification | |
|--------------------------|------------------------------------|
| Power 1 Fault | <input type="checkbox"/> SMTP Mail |
| Power 2 Fault | <input type="checkbox"/> SMTP Mail |
| POE Fault | <input type="checkbox"/> SMTP Mail |
| Eth1 Link Down | <input type="checkbox"/> SMTP Mail |
| Eth2 Link Down | <input type="checkbox"/> SMTP Mail |
| DI1 ON->OFF | <input type="checkbox"/> SMTP Mail |
| DI2 ON->OFF | <input type="checkbox"/> SMTP Mail |
| DI3 ON->OFF | <input type="checkbox"/> SMTP Mail |
| DI4 ON->OFF | <input type="checkbox"/> SMTP Mail |
| DI1 OFF->ON | <input type="checkbox"/> SMTP Mail |
| DI2 OFF->ON | <input type="checkbox"/> SMTP Mail |
| DI3 OFF->ON | <input type="checkbox"/> SMTP Mail |
| DI4 OFF->ON | <input type="checkbox"/> SMTP Mail |



E-Mail setting interface

The following table describes the labels in this screen.

| Label | Description |
|---------------------------|--|
| SMTP Server | Simple Message Transfer Protocol, enter the backup host to use if primary host is unavailable while sending mail by SMTP server. |
| Server Port | Specify the port where MTA can be contacted via SMTP server. |
| E-mail Address 1-4 | Inputs specify the destination mail address. |

3.SNMP

SNMP Settings

SNMP Agent: Enable Disable

SNMP Trap Server 1:

SNMP Trap Server 2:

SNMP Trap Server 3:

SNMP Trap Server 4:

Community:

SysLocation:

SysContact:

SNMP Event Types

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

| Fault Event Notification | |
|--------------------------|------------------------------------|
| Power 1 Fault | <input type="checkbox"/> SNMP Trap |
| Power 2 Fault | <input type="checkbox"/> SNMP Trap |
| POE Fault | <input type="checkbox"/> SNMP Trap |
| Eth1 Link Down | <input type="checkbox"/> SNMP Trap |
| Eth2 Link Down | <input type="checkbox"/> SNMP Trap |
| DI1 ON->OFF | <input type="checkbox"/> SNMP Trap |
| DI2 ON->OFF | <input type="checkbox"/> SNMP Trap |
| DI3 ON->OFF | <input type="checkbox"/> SNMP Trap |
| DI4 ON->OFF | <input type="checkbox"/> SNMP Trap |
| DI1 OFF->ON | <input type="checkbox"/> SNMP Trap |
| DI2 OFF->ON | <input type="checkbox"/> SNMP Trap |
| DI3 OFF->ON | <input type="checkbox"/> SNMP Trap |
| DI4 OFF->ON | <input type="checkbox"/> SNMP Trap |

SNMP setting interface

The following table describes the labels in this screen.

| 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. Turn on to open this service and off to shutdown it. |
| SNMP Trap Server 1-4 | Specify the IP of trap server, which is the address to which it will send traps AP generates. |
| Community | Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-write community. |
| SysLocation | Specify sysLocation string. |
| SysContact | Specify sysContact string. |

4.Relay

Even Warning Settings --> Relay

| Fault LED/Relay | |
|-----------------|--|
| Power 1 Fault | <input type="checkbox"/> Fault LED/Relay |
| Power 2 Fault | <input type="checkbox"/> Fault LED/Relay |
| POE Fault | <input type="checkbox"/> Fault LED/Relay |
| Eth1 Link Down | <input type="checkbox"/> Fault LED/Relay |
| Eth2 Link Down | <input type="checkbox"/> Fault LED/Relay |
| DI1 ON->OFF | <input type="checkbox"/> Fault LED/Relay |
| DI2 ON->OFF | <input type="checkbox"/> Fault LED/Relay |
| DI3 ON->OFF | <input type="checkbox"/> Fault LED/Relay |
| DI4 ON->OFF | <input type="checkbox"/> Fault LED/Relay |
| DI1 OFF->ON | <input type="checkbox"/> Fault LED/Relay |
| DI2 OFF->ON | <input type="checkbox"/> Fault LED/Relay |
| DI3 OFF->ON | <input type="checkbox"/> Fault LED/Relay |
| DI4 OFF->ON | <input type="checkbox"/> Fault LED/Relay |

Relay setting interface

DIDO

Basic Setting --> DIDO

| | | |
|------|-------------------------------------|--------------------------------------|
| DI | | |
| DI 1 | <input checked="" type="radio"/> On | <input type="radio"/> Off |
| DI 2 | <input checked="" type="radio"/> On | <input type="radio"/> Off |
| DI 3 | <input checked="" type="radio"/> On | <input type="radio"/> Off |
| DI 4 | <input checked="" type="radio"/> On | <input type="radio"/> Off |
| DO | | |
| DO 1 | <input type="radio"/> On | <input checked="" type="radio"/> Off |
| DO 2 | <input type="radio"/> On | <input checked="" type="radio"/> Off |
| DO 3 | <input type="radio"/> On | <input checked="" type="radio"/> Off |
| DO 4 | <input type="radio"/> On | <input checked="" type="radio"/> Off |

5.3.4 System Status

System Info

System Info.

| | | |
|---------------------------|--|-------------------|
| Model: | IGAR-1042+-3G | |
| Model Description: | Industrial IEEE 802.11 b/g/n 3G Cellular 1000Base-T(X) with PoE VPN Router | |
| WAN: | Mode | Dynamic Setting |
| | IP Address | 192.168.2.173 |
| | Broadcast Address | 192.168.2.255 |
| | Subnet Mask | 255.255.255.0 |
| | Default Gateway | 192.168.2.1 |
| | DNS(Primary) | 192.168.2.6 |
| | DNS(Secondary) | 168.95.192.1 |
| | MTU | 1500 |
| MAC Address | 00:1E:94:77:66:44 | |
| LAN: | IP Address | 192.168.10.1 |
| | Subnet Mask | 255.255.255.0 |
| | MTU | 1500 |
| | MAC Address | 00:1E:94:99:55:67 |
| | DHCP Server | Enabled |
| Wireless: | Wireless | Enabled |
| | SSID | oring |
| | Channel | Auto |
| | Encryption Mode | None |

System Info Screen

This page displays the details information for the AP router including model name, model description, firmware version, WAN, LAN and wireless settings.

System Log

System log.

Log Option:

DHCP Server
 NTP Client
 PPPoE Client
 System Event
 Firewall

Boot Message
 PPTP VPN
 OpenVpn
 UPNP
 Modem

System Log:

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

System Log Screen

The router keeps a running log of events and activities occurring on the router, several filters are provided for displaying related log entries.

Click the button '**Refresh**' to refresh the page.

Click the button '**Clear Logs**' to clear the log entries.

Traffic Statistics

Traffic statistics.

| Interface | Send | Receive |
|--------------|-------------------------------|-------------------------------|
| Wired LAN | 3788339 Bytes (11069 Packets) | 1203591 Bytes (9388 Packets) |
| Wired WAN | 6717 Bytes (126 Packets) | 7431150 Bytes (75383 Packets) |
| Wireless LAN | 0 Bytes (0 Packets) | 0 Bytes (0 Packets) |

Traffic Statistics Screen

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

Wireless Link List

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 |
|-------------|----------|------------|----------|------------|--------------|------------|-----------|
| | | | | | | | |
| | | | | | | | |

This page of the list displays the **Mac Address** of the wireless clients connected.



Technical Specifications

| LAN Interface | |
|---------------------------|---|
| Ethernet Ports | 2 x 10/100/1000Base-T(X), Auto MDI/MDI-X |
| Protocols | IP, TCP, UDP, DHCP, BOOTP, ARP/RARP, DNS, SNMP MIB II, HTTPS, SNMPV1/V2, Trap, Private MIB |
| Cellular Interface | |
| Cellular Standard | GSM / GPRS/ EGPRS/ EDGE / WCDMA / HSDPA / HSUPA |
| 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 |
| WLAN Interface | |
| Operating Mode | AP/ Client /Bridge/ AP-Client |
| Antenna and Connector | 2 antennas with 2dBi for 5GHz and 2.4GHz in reverse SMA connector |
| Radio Frequency Type | DSSS, OFDM |
| Modulation | IEEE802.11b: CCK/DQPSK/DBPSK IEEE802.11a/g: OFDM IEEE802.11n: BPSK, QPSK, 16-QAM, 64-QAM |
| Frequency Band | America/FCC: 2.412~2.462 GHz (11 channels) Europe CE/ETSI: 2.412~2.472 GHz (13 channels) |
| Transmission Rate | IEEE 802.11b: 11, 5.5, 2, 1 Mbps; IEEE 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps IEEE 802.11n: 20 MHz BW: 130, 117, 104, 78, 52, 39, 26, 13 40 MHz BW: 270, 243, 216, 162, 108, 81, 54, 27 |
| Transmit Power | IEEE 802.11b: 17dBm \pm 1.5dBm@11Mbps IEEE 802.11g: 16dBm \pm 1.5dBm@54Mbps IEEE 802.11gn HT20: 15dBm \pm 1.5dBm @MCS7 IEEE 802.11gn HT40: 14dBm \pm 1.5dBm @MCS7 |
| Receiver Sensitivity | IEEE 802.11b : -85dBm \pm 2dBm@11Mbps IEEE 802.11g : -76dBm \pm 2dBm@54Mbps IEEE 802.11gn HT20:-75dBm \pm 2dBm@MCS7 IEEE 802.11gn HT40:-72dBm \pm 2dBm@MCS7 |



| | |
|-----------------------------|--|
| Encryption Security | WEP: (64-bit, 128-bit key supported) WPA/WPA2:802.11i (WEP and AES encryption) WPA-PSK (256-bit key pre-shared key supported) TKIP encryption |
| Wireless Security | SSID broadcast disable |
| LED Indicators | 3 x LEDs, PWR1(2)(PoE) / Ready: 1) Red On: Power is on and booting up. 2) Green On: Power is on and functioning normally. ETH1(2) Link / ACT: Green for port Link/ Act at 1000Mbps Amber for port Link/ Act at 100Mbps. WLAN Link/ACT: Green for WLAN Fault indicator: Red On: Ethernet link down or power down |
| Power Requirements | |
| Power Input Voltage | Dual DC inputs. 12~48VDC on 6-pin terminal block |
| Reverse Polarity Protection | Present |
| Power Consumption | 8.3 Watts |
| Environmental | |
| Operating Temperature | -10 to 60°C |
| Storage Temperature | -40 to 85°C |
| Operating Humidity | 5% to 95%, non-condensing |
| Mechanical | |
| Dimensions(W x D x H) | 74.3(W) x 109.2(D) x 153.6(H) mm |
| Casing | IP-30 protection |
| 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 |
| Rail Traffic | EN60950-1 |



Compliance

FCC Statement

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

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

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

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

Industry Canada Statement

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

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

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

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



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

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

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

Afin de réduire les interférences radio potentielles pour les autres utilisateurs, le type d'antenne et son gain doivent être choisis de sorte que la puissance isotrope rayonnée équivalente (PIRE) est pas plus que celle permise 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 environnement incontrôlé. L'antenne (s) utilisée pour ce transmetteur ne doit pas être co-localisée ou fonctionner en conjonction avec toute autre antenne ou transmetteur.