Industrial Wireless Access Point Router

IAR-7002-WA / WA+ User's Manual



Version 1.0 May, 2008.



ORing Industrial Networking Corp.

4F, NO.3, Lane235, Baociao Rd. Sindian City, Taipei County 23145 Taiwan, R.O.C. Tel: + 886 2 2918 3036 Fax: + 886 2 2918 3084 Website: <u>www.oring-networking.com</u> E-mail: <u>support@oring-networking.com</u>

Tables of Content

Getting	g to Know your Wireless Router	1
1.1	Overview	1
1.2	Software Features	1
1.3	Hardware Features	2
Hardwa	are Installation	3
2.1	Installation Router on DIN-Rail	3
2.2	Wall Mounting Installation	4
Hardwa	are Overview	6
3.1	Front Panel	6
3.2	Front Panel LEDs	
3.3	Bottom Panel	
3.4	Rear Panel	9
Cables	s and Antenna	10
4.1	Ethernet Cables	
4.2	Wireless Antenna	11
Manag	ement Interface	12
5.1	First-time configuration	12
5.2	Configure the Wireless Router	
5.3	Main Interface	
5.3	B.1 Basic Setting	
١	WAN	
l	LAN	
I	DHCP	
١	Wireless	
5.3	3.2 Advanced Setting	
١	Wireless	
I	NAT Setting	
Ş	Security Setting	
١	VPN Setting	
I	Notification	
I	Miscellaneous (DDNS)	41
5.3	3.3 System Tools	41
[Date & Time	41

Login Setting	42
Router Restart	44
Firmware Upgrade	44
Save/Restore Config	45
Miscellaneous (Ping)	46
5.3.4 System Status	
System Info	46
System Log	47
Traffic Statistics	47
Wired/Wireless Clients	48
Technical Specifications	49
Appendix A How to configure openvpn and use openvpn in the Windows?	51



Getting to Know your Wireless AP Router

1.1 Overview

The ORing IAR-7002-WA / WA+ 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 IAR-7002-WA / WA+ wireless AP router is IEEE802.11g high-performance wireless equipment which is also compatible with IEEE802.11b equipment. It is capable of data transfer rates up to 54Mbps. It is easy for you to extend the reach and number of computers connected to your wireless network.

With the USB 3G WAN connection, the ORing IAR-7002-WA / WA+ wireless AP router can be mounted in harsh environment easily to provide internet access anytime and anywhere.



The ORing IAR-7002-WA / WA+ 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.
- USB connectivity providing Internet access via the USB to RS232 convertor + modem or 3G HSDPA module (HUAWEI E220) directly.
- 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 10/100Base-T(X) Ethernet ports for WAN / LAN connection individually.
- Fully Compliant with IEEE802.3af (Power Device at ETH2, WAN port, IAR-7002-WA+ only)
- Redundant Power Inputs: 12~48 VDC on terminal block
- Casing: IP-30
- Dimensions(W x D x H) : 52 mm(W)x 106 mm(D)x 144 mm(H)
- Operating Temperature: -10 to 55°C
- Storage Temperature: -20 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.

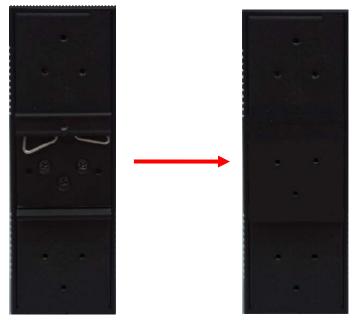




2.2 Wall Mounting Installation

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-7002-WA/WA+.



Step 3: Mount the combined AP router on the wall.





Hardware Overview

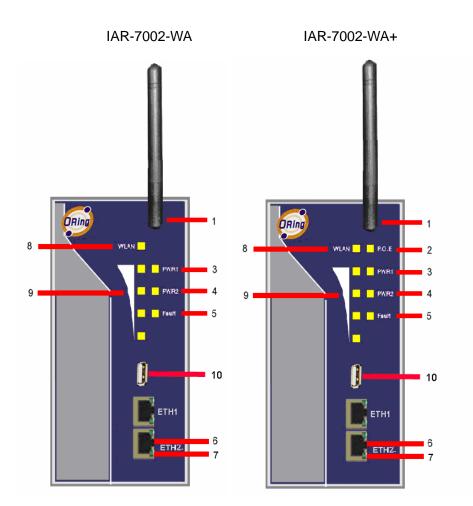
3.1 Front Panel

The following table describes the labels that stick on the IAR-7002-WA / WA+.

Port		Description
10/100 RJ-4	5 fast	2 10/100Base-T(X) RJ-45 fast Ethernet ports support
Ethernet ports	;	auto-negotiation. Default Setting : Speed: auto Duplex: auto
P.O.E. PD Por	:	ETH2 (WAN port) of IAR-7002-WA+ compliant with IEEE802.3af
		P.O.E. specifications and can be connected to P.O.E. switches.*
ANT.		Reversed SMA connector for external antenna.

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



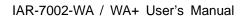


- 1. 2.4GHz antenna with typical 2.0dbi antenna.
- 2. LED for P.O.E. power and system status. When the P.O.E. power links, the green led will be light on.
- 3. LED for PWR1 and system status. When the PWR1 links, the green led will be light on.
- 4. LED for PWR2 and system status. When the PWR2 links, the green led will be light on.
- 5. LED for Fault indication. When the fault event occurs, the amber LED will be light on.
- 10/100Base-T(X) Ethernet ports. ETH1 for LAN port and ETH2 for WAN port. (IAR-7002-WA+ contains PD function of P.O.E. at ETH2)
- 7. LED for Ethernet ports status.
- 8. LED for WLAN link/act status.
- 9. LED for WLAN signal strength.
- 10. USB port for 3G USB modem connection.



3.2 Front Panel LEDs

LED	Color	Status	Description
System LED)		
		Green On	P.O.E. power connected.
	Green / Red	Green blinking	Device been located
P.O.E.			Indicates an IP conflict, or
		Red blinking	DHCP or BOOTP server did
			not respond properly
		Green On	DC power 1 activated.
		Green blinking	Device been located
PWR1	Green / Red		Indicates an IP conflict, or
		Red blinking	DHCP or BOOTP server did
			not respond properly
		Green On	DC power 2 activated.
		Green blinking	Device been located
PWR2	Green / Red		Indicates an IP conflict, or
		Red blinking	DHCP or BOOTP server did
			not respond properly
Fault	Amber	On	Fault relay. Power failure
raun	Amber		or Port link down.
WLAN	Green	On	WLAN activated.
	Oreen	Blinking	WLAN Data transmitted.
WLAN			WLAN signal strength.
Strength	Green	On	1<25%, 2<50%, 3<75%,
orengin			4<100%
10/100Base	-T(X) Fast Ethernet	ports	
10Mbps	Amber	On	Port link up at 10Mbps.
LNK/ACT	7411001	Blinking	Data transmitted.
100Mbps	Green	On	Port link up at 100Mbps.
LNK/ACT	Ciccii	Blinking	Data transmitted.

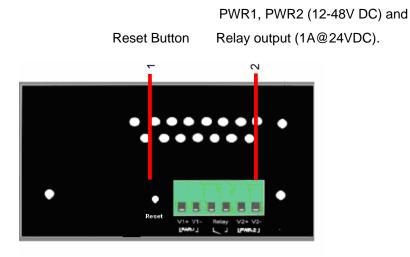




3.3 Bottom Panel

The bottom panel components of IAR-7002-WA / WA+ are shown as below:

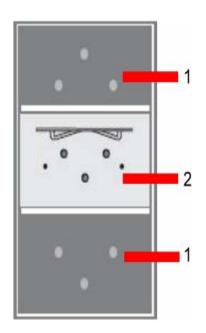
- 1. Terminal block includes: PWR1, PWR2 (12 ~ 48V DC) and Relay output (1A@24VDC).
- 2. Reset bottom. Push the bottom 3 seconds for reset; 5 seconds for factory default.



3.4 Rear Panel

The rear panel components of IAR-7002-WA / WA+ are shown as below:

- 1. Screw holes for wall mount kit.
- 2. DIN-Rail kit





Cables and Antenna

4.1 Ethernet Cables

The IAR-7002-WA / WA+ AP routers have standard Ethernet ports. According to the link type, the routers use 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 Types and Specifications

Cable	Туре	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45

100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

The IAR-7002-WA / WA+ routers support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and router. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.



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

MDI/MDI-X pins assignment

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

4.2 Wireless Antenna

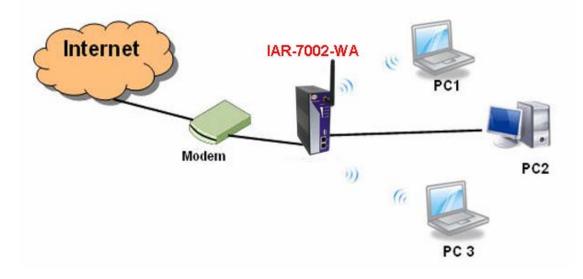
A 2.4GHz antenna is used for IAR-7002-WA / WA+ and connected with a reversed SMA connector. External antenna also can be applied with this connector.



Management Interface

5.1 First-time Installation

Before installing IAR-7002-WA / WA+ 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 IAR-7002-WA / WA+

Step 1: Select the Power Source

IAR-7002-WA / WA+ 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 IAR-7002-WA / WA+

Use either a straight-through Ethernet cable or cross-over cable to connect to ETH1 of IAR-7002-WA / WA+ 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 IAR-7002-WA / WA+

The default gateway IP of IAR-7002-WA / WA+ AP router is 192.168.10.1. Start the web browser of your computer and type <u>http://192.168.10.1</u> in the address box to access the webpage. A login window will popup, and then enter the default login name **admin**



and password admin.

Address 🙋 192.168.10.	1			💌 🄁 Go
	Connect to 192.1	68.10.1	? 🛛	
			G The	
	Login			
	<u>U</u> ser name:	2	₩	
	Password:			
		Remember my pa	assword	
		ОК	Cancel	

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, please plug in your USB to RS232 converter with modem or 3G USB modem directly (HUAWEI E220 is supported).

WAN settings.				
WAN Connection Type	: Dynamic/Static IF	v		
	ddress automatica			
		iiy		
O Use the follow IP Address:	192.168.0.94			
Subnet Mask:	255.255.255.0	-		
Default Gateway:	L			
Delault Gateway:	192.168.0.1			
	rver address autor ing DNS server ad			
O Use the follow Preferred DNS:				
O Use the follow	ing DNS server ad			
O Use the follow Preferred DNS:	ing DNS server ad			
O Use the follow Preferred DNS: Alternate DNS:	ing DNS server ad 192.168.0.1	dresses:		
O Use the follow Preferred DNS: Alternate DNS:	ing DNS server ad	dresses:		
O Use the follow Preferred DNS: Alternate DNS: Use Modem/3	ing DNS server ad 192.168.0.1	dresses:		
O Use the follow Preferred DNS: Alternate DNS: Use Modem/3/ Phone Number:	ing DNS server ad 192.168.0.1	dresses:		
O Use the follow Preferred DNS: Alternate DNS: Use Modem/3 Phone Number: User Name:	ing DNS server ad 192.168.0.1	dresses:		

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>		
These are the basic	wireless settings for the Storage Router.	
Wireless:	📀 Enabled 🔘 Disabled	
SSID:	RT61WRT00AB2C	
Channel:	6 🔽	
Security Options		
Security Type:	None	
	None	
	WEP	
	WPA-PSK/WPA2-PSK WPA/WPA2	

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.

Model:	I R-7002-WA			
Model Description:	escription: Industrial 802.11 a/b/g 3.5G VPN Router			
WAN:	Mode	Dynamic Setting		
	IP Address	192.168.0.94		
	Broadcast Address	192.168.0.255		
	Subnet Mask	255.255.255.0		
	Default Gateway	192.168.0.1		
	DNS(Primary)	192.168.0.1		
	DNS(Secondary)			
	MTU	1500		
	MAC Address	00:00:56:04:02:11		
LAN:	IP Address	192.168.10.1		
	Subnet Mask	255.255.255.0		
	MTU	1500		
	MAC Address	00:00:56:04:02:10		
	DHCP Server	Enabled		
Wireless:	Wireless	Enabled		
	SSID	RT61WRT00AB2C		
	Channel	6		
	Encryption Mode	None		
	MAC Address	00:19:DB:00:AB:2C		

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.

Address 🛃	192.168.10.	1				💌 🄁 Go
		Connect to 192.1	68.10.1	?		
		Login				
		<u>U</u> ser name:	2		~	
		<u>P</u> assword:				
			Remember my p	assword		
			ОК	Cancel		

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.

ORing	ndustrial 802.11 a/b/g 3.5G VPN	Router
open all Home Advanced Setting System Tools System Status	Firmware Ver: 1.5g Wan IP: 192.168.0.94 Uptime: 00:20:13 Home Welcome to Industrial 802.11 b/g 3.5G VPN Router configuration page.	www.oring-networking.com

Main Interface

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

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 IAR-7002-WA / WA+ AP router provide three types of WAN connection.

1. WAN Connection Type: Dynamic/Static IP

VAN settings.		
WAN Connection Typ	🖰 Dynamic/Static IP 💌	
Obtain an IP a	ddress automatically	
O Use the follow	ng IP address:	
IP Address:	192.168.0.94	
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.0.1	
O Use the follow	rver address automatically ng DNS server addresses:	
O Use the follow Preferred DNS:		
O Use the follow Preferred DNS: Alternate DNS:	ng DNS server addresses:	
O Use the follow Preferred DNS: Alternate DNS: ONS:	ng DNS server addresses:	
O Use the follow Preferred DNS: Alternate DNS: Ouse Modem/3 Phone Number:	ng DNS server addresses:	
O Use the follow Preferred DNS: Alternate DNS: Use Modem/3 Phone Number: User Name:	ng DNS server addresses:	
 O Use the follow Preferred DNS: Alternate DNS: 	ng DNS server addresses:	

Dynamic/Static IP

The following table describes the labels in this screen.

Label	Description
Obtain an IP address	Select this option if you would like to have an IP address assigned
automatically	automatically from the WAN port by DHCP server in your network.
Use the following IP	Select this option if you would like to assign an IP address to the
address	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	Obtain DNS server from DHCP server. If the above Obtain an
address	IP address automatically is selected, this option will be chosen
automatically	accordingly.
Use the following	Specify DNS server address manually.

ORing Industrial Networking Corp.



DNS server	
addresses	
Use Modem/3G as	Enable this option if you want to use Modem/3G as a backup
backup connection	connection when normal 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. Take www.google.com as an example.

2. WAN Connection Type: PPPoE

VAN Settings.				
VAN Connection Type:	PPP0E	~		
Jser Name:		2 2 2 2 2 2 2 2 2		
Password:	1997			
Service Name:			(optional)	
AC Name:	22		(optional)	
Connection Mode Auto Connect On De	emand			
Max Idle Time: O Manual	minutes (l) represents r	never bring down the link)	
Phone Number: User Name: Password: Ping Test Site:	3G as backup con	nection.		
Connect Dis	connect cted			

PPPoE Screen.



User Name /	Enter the username & password provided by your Internet
Password	Service Provider (ISP).
Service Name	Enter the service name provided by your ISP.
	Enter the name of the access concentrator as provided by your
AC Name	ISP.
Specify the IP & DNS	Enter static IP and DNS address which may required by some ISP
provided by ISP	
	Auto: Connect automatically when the router boots up.
	Connect on Demand: Select to disconnect the PPP session if
Connection Mode	the router has had no traffic for the specified amount of time.
Connection mode	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.
	Enable this option if you want to use Modem/3G as a backup
	connection when PPPoE connection is lost.
Use Modem/3G as	Phone Number, User Name and Password: Use these settings
backup connection	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

For using this type of connection, you need an USB to RS232 converter and a modem or 3G USB modem (HUAWEI E220 is supported) directly. Please connect the converter or 3G modem to the USB port before starting the WLAN AP router.

Basic Setting> WA	N
WAN Settings.	
WAN Connection Type:	Modem/3G
Phone Number:	
User Name:	
Password:	
PIN:	Enable PIN check before dialing PIN Code:
Auto Connect :	Enable
Device Status :	Modem is not present.
Operations :	Connect
Link Status :	Disconnected
Save Cancel	

Modem/3G Screen

The following table describes the labels in this screen.

Label	Description
Phone Number	Telephone number provided by your ISP.
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 .

LAN

These are the IP settings of the LAN interface for the IAR-7002-WA / WA+ WLAN AP router. The LAN IP address is privately for your internal network and can not be exposed on the Internet.



AN Side settings.							
P Address:	192.168.10.1						
ubnet Mask:	255.255.255.0						
		1.1.1					

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

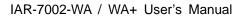
DHCP stands for Dynamic Host Control Protocol. The IAR-7002-WA / WA+ AP router with a built-in DHCP server. The internal DHCP server will assign an IP address to the computers (DHCP client) on the LAN automatically.

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.

1. DHCP Sever

	CP Server.			
DHCP S	Gerver:	💿 Enabled 🔘 Disabled		
Starting	g IP:	192.168.10.2		
Ending	IP:	192.168.10.254		
Lease ⁻	Time:	48 Hours		
Local D	omain Name:	(optio	onal)	
Current #	t DHCP Client Information	Mac	IP	Expires In

DHCP Server Screen





Label	Description
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.
Current DHCP Client	List of the computers on your network that are assigned an IP
Information	address by internal DHCP server.

The following table describes the labels in this screen.

2. IP Allocation

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 IAR-7002-WA / WA+ 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.

- Choose a	Client to Edit	Copy to	
	MAC Address	IP Address	
			Add Clear
tatic DHCP #	Client List: MAC Address	IP Address	Operations

IP Allocation Screen

Label	Description
Choose a Client to	The list shows the MAC addresses and IP addresses that are
Edit	already assigned by IAR-7002-WA / WA+. 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	The list shows the MAC address and IP address one-to-one
List	relationship.



Wireless

nese are the basic	wireless settings for the Storage Router.	
Wireless:	💿 Enabled 🔘 Disabled	
SSID:	RT61WRT00AB2C	
Channel:	6 🗸	
Security Options		
Security Type:	None	
	None	
	WEP	

Wireless Screen

The following table describes the labels in this screen.

Label	Description
	Service Set Identifier (SSID) is a unique name that identifies a
	network. All devices on the network must set the same SSID
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 6 is the default channel. All devices on the network
Channel	must share the same channel.*
Channel	*Note: The wireless devices will automatically scan and match the
	wireless setting of the AP router with the same SSID.
	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
Security options	communicating over the WLAN.
Security options	WPA-PSK/WPA2-PSK: WPA-PSK or WPA2-PSK with a
	pre-shared key, each authorized computer is given the same
	pass phrase.
	WPA/WPA2: Wi-Fi Protected Access (WPA) authentication in
	conjunction with a RADIUS server.

Security Type – None

No security protection for WLAN.



Security Type – WEP

Basic Setting> Wireless These are the basic wireless settings for the Storage Router.		
SSID:	RT61WRTD0AB2C	
Channel:	6 🗸	
Security Options		
Security Type:	WEP	
Auth Mode:	O Open O Shared O WEPAUTO	
WEP Encryption:	64 Bit 💌	
Кеу Туре:	ASCII (5 characters) 💌	
Default Key Index:	1 💌	
KEY1:		
KEY2:		
KEY3:		
KEY4:		
NET TI		

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-PSK/WPA2-PSK

hese are the basic w	ireless settings for the Storage Router.
Wireless:	⊙ Enabled ○ Disabled
SSID:	RT61WRT0DAB2C
Channel:	6 🗸
Security Options Security Type:	WPA-PSK/WPA2-PSK
Auth Mode: Encryption Type: Shared Key:	WPAPSK WPA2PSK WPAPSK/WPA2PSK mix TKIP AES TKIP/AES mix

Wireless Security Type-WPA-PSK/WPA2-PSK Screen



- 1. Security Type: Select WPA-PSK/WPA2-PSK.
- 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.

Basic Setting> Wireless		
These are the basic w	reless settings for the Storage Router.	
Wireless:	● Enabled ○ Disabled	
SSID:	RT61WRT00AB2C	
Channel:	6 🗸	
Security Options Security Type:	WPA/WPA2	
Auth Mode:	🔿 WPA 🔿 WPA2 🔿 WPA/WPA2 mix	
Encryption Type:	○ TKIP ○ AES ○ TKIP/AES mix	
Radius Server IP:	0.0.0.0	
Radius Port:	1812	
Shared Secret:	radius_key	

Security Type – WPA /WPA2

Wireless Security Type-WPA/WPA2 Screen

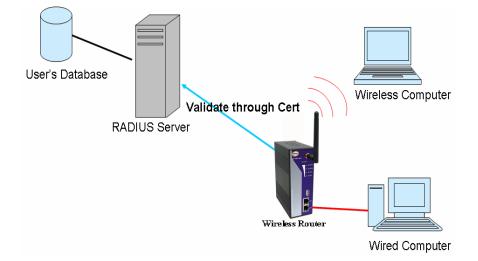
- 1. Security Type: Select **WPA/WPA2**
- 2. Auth Mode: Choose one of three Auth Modes: WPA, WPA2, WPA/WPA2 mix.
- 3. Encryption Type: Choose one of three Encryption Types: **TKIP**, **AES**, **TKIP/AES mix**.
- 4. Radius Server IP: Enter the IP address of the RADIUS Server.
- 5. Port: Enter the RADIUS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

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:



5.3.2 Advanced Setting

Wireless

1. Parameters

Advanced Setting> Wireless -> Parameters		
Advanced wireless paramet	ters settings.	
Beacon Interval:		
beacon incerval.	100 (msec, range:1~65525, default:100)	
DTIM Interval:	1 (range: 1~255, default:1)	
Fragmentation Threshold:	2346 (range: 256~2346, default:2346)	
RTS Threshold:	2347 (range: 1~2347, default:2347)	
Xmit Power:	100 % (range: 0~100, default:100)	
Wireless Mode:	💿 BG Mixed Mode 🔘 B Mode 🔘 G Mode	
Transmission Rate:	Auto 💌	
Preamble:	💿 Long 🔘 Short	
SSID Broadcast:	⊙ Enabled ○ Disabled	
Apply Cancel		

Parameters Screen

Label	Description
	The default value is 100. The Beacon Interval value indicates
Beacon Interval	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 connection.
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.
	This value should remain at its default setting of 2346. The
	range is 256-2346 bytes. It specifies the maximum size for a
F	packet before data is fragmented into multiple packets. If you
Fragmentation	experience a high packet error rate, you may slightly increase the
Threshold	Fragmentation Threshold. Setting the Fragmentation Threshold
	too low may result in poor network performance. Only minor
	modifications of this value are recommended.
	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 Threshold	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.
	This value ranges from 1 - 100 percent, default value is 100
	percent. A safe increase of up to 60 percent would be suitable
Xmit Power	for most users. Higher power settings are not recommended for
	users due to excess heat generated by the radio chipset, which
	can affect the life of the AP.
	If you have IEEE802.11g and IEEE802.11b devices in your
	network, then keep the default setting, BG Mixed mode . If you
Wireless Network	have only IEEE802.11g devices, select G Mode . If you would
Mode	
	like to limit your network to only IEEE802.11b devices, then
	select B Mode .
Transmission Rate	The default setting is Auto . The range is from 1 to 54Mbps.
	The rate of data transmission should be set depending on the



	speed of your wireless network. You can select from a range of
	transmission speeds, or keep the default setting, Auto, to have
	the AP automatically use the fastest possible data rate and
	enable the Auto-Fallback feature. Auto-Fallback will negotiate
	the best and possible connection speed between the AP and a
	wireless client.
	Values are Long and Short, default value is Long. If your
Preamble	wireless device supports the short preamble and you are having
Freample	trouble getting it to communicate with other IEEE802.11b
	devices, make sure that it is set to use the long preamble
	When wireless clients survey the local area for wireless networks
SSID Broadcast	to associate with, they will detect the SSID broadcast by the AP.
	To broadcast the AP SSID, keep the default setting, Enable. If
	you do not want to broadcast the AP SSID, then select Disable .

2. MAC Filter

Use **MAC Filter** to allow or deny wireless clients to associate with IAR-7002-WA / WA+ AP router. You can manually add a MAC address or select the MAC address from **Associated Clients** that are currently associated with IAR-7002-WA / WA+.

1AC Filter: C) Enabled 💿 Disabled	
Options Only allow MAC add	ress(es) listed below to connect to	р AP
O Only deny MAC add	ress(es) listed below to connect to) AP
ssociated Clients:	Choose an associated client	<u> </u>
1AC Address:		Add Clear
1AC Filter List:		Edit
NAC FIILER LISC:		Delete

MAC Filter 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					
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.				

The following table describes the labels in this screen.

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.

	ced Setting> N/	AT Setting ->	Virtual 9	Server				
Virtual :	server settings.							
Virtual !	Server:	💿 Enable 🤇) Disable					
Descrip	tion:							
Public I	P:	⊙ All ○ Sp	ecify					
Public P	Port:			1222				
Protoco	ol:	⊙ TCP ○ U	DP O Bo	oth				
Local IF	•:							
Local P	ort:							
Enable	Now:	💿 Yes 🔿 N	0					
		Add Can						
Virtual :	server list:							
#	Description	Public IP	Public Port	Protocol	Local IP	Local Port	Enabled	Ops
1	ftp	0/0	21	tcp	192.168.0.202	21	V	Edit De

Virtual Server

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 Port Trigger

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Trigger is used for some of the applications that can work with an NAT router.

Advanc	ed Setting> N	AT Setting -> Port Tri	gger				
Port Trig	ger settings.						
Port Trig	ger:	📀 Enable 🔿 Disable	•				
Descripti	ion:						
Trigger F	Port:						
Trigger F Incoming			oth				
Incoming Enable:	g Protocol:	 TCP ○ UDP ○ B Yes ○ No Add Cancel 	oth				
Port Trig	iger List:						
#	Description	Trigger Protocol	Trigger Port	Incoming Protocol	Incoming Port	Enable	Ops
1	pp	tcp	21	tcp	23,32,32,2222		Edit Del
10154							

Port Trigger Screen

Label	Description				
Port Trigger	Enable or disable Port Trigger.				
Description	This is the description for the entry.				
Trigger Port	This is the port used to trigger the application.				
Trigger Protocol	This is the protocol used to trigger the application.				
Incoming Port	This is the port number on the WAN side that will be used to				
	access the application.				
Enable	Enable the rule after adding the entry.				
Port Trigger List	Click Edit to edit the entry, click Del to delete the entry.				



3. 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.

Advanced Setting> NAT Setting -> DMZ								
DMZ settings.								
DMZ:	🔿 Enable 💿 Disable							
Description:								
DMZ Host IP:								
Apply Cancel								

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.

4. 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.

Auvanceu	Setting> NA	T Setting -> UP	nP			
UPnP settir	ngs.					
UPnP: UPnP List:		 Enabled Enable NAT-f 				
#	Application	Ext Port	Protocol	Int Port	IP Address	Status





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.						

Security 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 💿 Di	sable					
Description:			7				
Rule:	DROP M	Concellenter					
Direction:	LAN->WAN						
IP Address:	Source IP:						
	Destination IP:						
Protocol:	O All						
	O ICMP						
	O Specify proto	col number:					
	• TCP	Specify port	:				
	O UDP	Specify port					
Enable Now:	🖲 Yes 🔿 No						
	Add Cancel						
IP filter list:							
# Description R	ule Direction	Source IP	Destination IP	Protocol	Port	Enabled	Operations

IP Filter 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.	

The following table describes the labels in this screen.

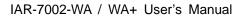
2. MAC Filter

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

MAC Filte	er settings.				
MAC Filte	er:	🔿 Enable 💿 Disable			
Descripti	on:				
Rule:		DROP V			
MAC Add	ress:	(e.x. 0)0:11:22:aa:bb:cc)		
Enable Now:		• Yes O No			
		Add Cancel			
IP filter li	st:				
#	Description	Rule	MAC Address	Enabled	Operations

MAC Filter 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.

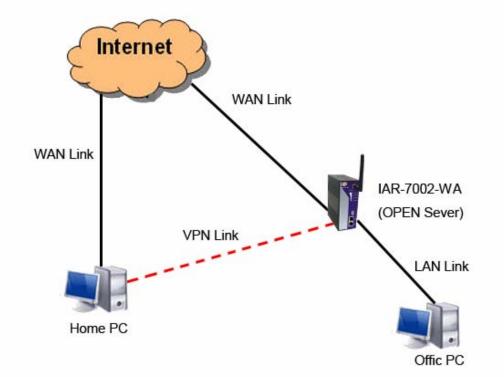
1. Open VPN

Open VPN is a full-functioned SSL VPN solution which can accommodates 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.

)penvpn settings.		
Server settings.		
Openvpn Server:	🔿 Enable 🔿 Disable	
Tunnel Protocol:		
Port:	1194	
LZO Compression:	💿 Enable 🔘 Disable	
Keys Setting:	Auto	
Client settings.		
Openvpn Client:	🔿 Enable 🔿 Disable	
Server IP :		
Tunnel Protocol:		
Port:	1194	
LZO Compression:	Enable Disable	
Keys Setting:	Auto 🔽	
	Apply	

Open VPN Screen





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

1: Open VPN Server



Before connecting to the Openvpn server of IAR-7002-WA / WA+ AP routuer, please install openvpn client software for your windows PC. It can be download from http://openvpn.net/download.html#stablel. The current version of Openvpn used in IAR-7002-WA / WA+ is version 2.0.9. The corresponding software for client should be installed.

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.



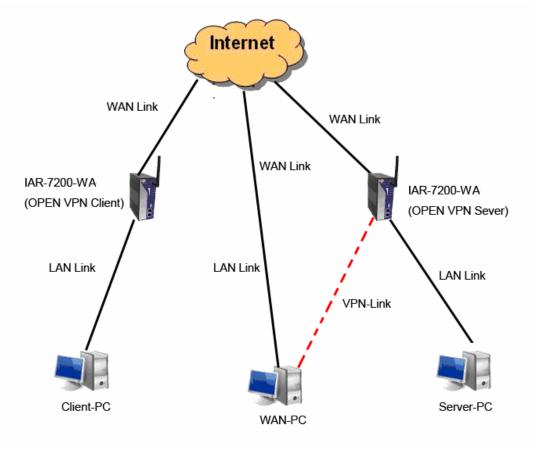
2: Open VPN Client

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

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.

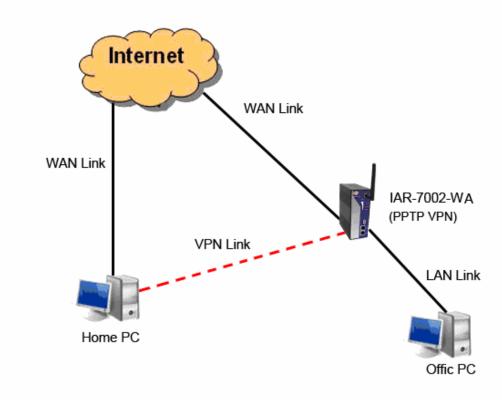
To create a PPTP connection to the router, you should create a PPTP network connection if you are using a window PC. The steps are: **Right click Network > property > create a new connection > connect to my work space (VPN) > use VPN to internet > enter the user name and password** which are set in the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



PPTP Server settir	ngs.				
PTP Server	🔿 Enable 🔿 Disable				
Server IP :	192.168.10.1				
Clients IP:	192.168.10.50-80				
CHAP-Secrets:	admin * admin *				
	~				

PPTP VPN Screen

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



Connection to PPTP VPN Server



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.

Notification

1. Email/SNMP/Syslog

Email Settings

SMTP Server:	(optional)
Server Port:	(O represents default)
E-mail Address 1:	
E-mail Address 2:	
E-mail Address 3:	
E-mail Address 4:	

Email Settings Screen

Label	Description
SMTP Server	Simple Message Transfer Protocol, enter the backup host to use if
	primary host is not available while sending mail by SMTP server.
Server Port	Specify the port where MTA can be contacted via SMTP server.
E-mail Address 1-4	Enter the mail addresses.



SNMP Settings

SNMP settings.	
SNMP Agent:	🔘 Enable 🔘 Disable
SNMP Trap Server 1:	
SNMP Trap Server 2:	
SNMP Trap Server 3:	
SNMP Trap Server 4:	
Community:	
SysLocation:	
SysContact:	

SNMP Settings

The following table describes the labels in this screen.

Label	Description
	SNMP (Simple Network Management Protocol) agent
	communicates with the SNMP manager. The agent provides
SNMP Agent	management information to the NMS by keeping track of various
	operational aspects of the system. Turn on to open this service
	and off to disable it.
SNMP Trap Server	Specify the IP address of trap server, which is the address to
1-4	which SNMP trap messages are sent.
	Community is essentially password to establish trust between
Community	managers and agents. Normally "public" is used for read-write
	community.
SysLocation	Specify sysLocation string.
SysContact	Specify sysContact string.

Syslog Server Settings

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

Syslog Server Screen

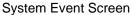


Label	Description
Syslog Server IP	Not only the Syslog keeps the logs locally, it can also log to
	remote server. Specify the IP of remote server. Leave it blank
	to disable logging remotely.
Syslog Server Port	Specify the port of remote logging. Default port is 514.

2. System Event

When specified event is triggered, the notification procedure will be performed according to the type of the event. Which notification would be performed depends on the selection of corresponding option in the **Advanced Setting > Notification > System Event** page.

Device Event Notifica	ation.					
Hardware Reset (Cold Start)		🔲 SMTP Mail	SNMP Trap		📃 Syslog	
Software Reset (Warm Start)		SMTP Mail	SNMP Trap		🔲 Syslog	
Login Failed		🔲 SMTP Mail	SNMP Trap		📃 Syslog	
IP Address Changed		🔲 SMTP Mail	SNMP Trap		📃 Syslog	
Password Changed		🔲 SMTP Mail	🔲 SNMP Trap	SNMP Trap		
Redundant Power Changed		🔲 SMTP Mail	SNMP Trap	SNMP Trap		
SNMP Access Failed		🔲 SMTP Mail	SNMP Trap		🔲 Syslog	
Wireless Client Associated		🔲 SMTP Mail	🔲 SNMP Trap		📃 Syslog	
Wireless Client Disassociated		SMTP Mail	SNMP Trap		🗌 Syslog	
Fault Event Notificat	ion and Fault LED/Rela	зу.				
Power 1 Fault	🔲 SMTP Mail	SNMP Trap	🔲 Syslog	🗌 Fa	ult LED/Relay	
Power 2 Fault	🔲 SMTP Mail	SNMP Trap	Syslog		🗌 Fault LED/Relay	
Eth1 Link Down	🔲 SMTP Mail	SNMP Trap	🔲 Syslog	🗌 Syslog 📃 Fau		
Eth2 Link Down	SMTP Mail	SNMP Trap	Syslog	🗌 Syslog 📃 Fa		



System events record the activities of the Wireless Router system. When the setting changes or action performs, the event will be sent to administrator by email. A trap will also be sent to SNMP trap server. The Syslog will record the event locally and may send the Syslog remotely to a Syslog server. If serious event occurred, such as the power failure or link down, the fault led will be switched on as warning indication.



Miscellaneous (DDNS)

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

DDNS Service:	www.3322.org			
User Name:	www.33222.org	(*)		
Password:	www.dyndns.org	(*)		
Domain:	www.tzo.org www.easydns.org	(*)		
Mail Server:	http://gnudip.cheapnet.net www.ods.org			
Use Wildcard:	www.justlinux.com			
Use Wildcard:	www.justlinux.com			

DDNS Screen

For example, Choose DDNS Service: <u>www.3322.org</u> 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.			
Mail Server	Enter the mail server if provided.			
Use Wildcard	Check the box the enable wildcard option.			

5.3.3 System Tools

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.



Date/Time settings. Local Date: 2008 Year 1 Month 1 Day Local Time: 2 Hour 12 Minute 18 Second Time Zone: GMT+08:00 ♥ Get Current Date & Time from Browser NTP: Enable NTP Server 1: pool.ntp.org NTP Server 2: time.nist.gov (optional) Synchronise: Every Day at 00 ♥ : 00 ♥	System Tools>)ate & Time	
Local Time: 2 Hour 12 Minute 18 Second Time Zone: GMT+08:00 V Get Current Date & Time from Browser NTP: Enable NTP Server 1: pool.ntp.org NTP Server 2: time.nist.gov (optional)	Date/Time settings.		
Image:	Local Date:	2008 Year 1 Month 1	Day
Get Current Date & Time from Browser NTP: Image: Enable NTP Server 1: pool.ntp.org NTP Server 2: time.nist.gov	Local Time:	2 Hour 12 Minute 18	Second
NTP: Enable NTP Server 1: pool.ntp.org NTP Server 2: time.nist.gov (optional)	Time Zone:		
NTP Server 1: pool.ntp.org NTP Server 2: time.nist.gov		Get Current Date & Time from B	rowser
NTP Server 1: pool.ntp.org NTP Server 2: time.nist.gov			
NTP Server 2: time.nist.gov (optional)	NTP:	🗹 Enable	
(optional)	NTP Server 1:	pool.ntp.org	
Synchronise: Every Day v at 00 v : 00 v	NTP Server 2:	time.nist.gov (c	optional)
	Synchronise:	Every Day 💙 at 00 💙 : 00 💙	

Date & Time 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 &	Click this button; you can set the time from your browser.					
Time from 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.					

Login Setting

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



.ogin settings.		
Old Login Name:	admin	
Old Password:	•••••	
New Login Name:	admin	
lew Password:		
Confirm New Password:		
Veb Protocol:	⊙ HTTP ○ HTTPS	
Port:	80	

Login Setting 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.

nable						
rt Every Day	📉 at 00 🚩 :	00 💌				
	nable rt Every Day					

Router Restart Screen

Firmware Upgrade

System Tools> Firmware Upgrade			
Do NOT power off the router while upgrading!			
Current Firmware Version: 1.5g			
	浏览		
Start 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

System Tools> Save/Restore Configurations						
Save/Restore Configurations.						
Save Current Configurations						
Save						
Restore previous saved configurations						
网版 Restore						
Restore factory default settings						
Restore Factory Default Settings						

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")

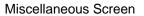


Label	Description					
Download	The current system settings can be saved as a file into your PC.					
configuration						
Upload configuration	The configuration can be restored to the router. To reload a					
	system settings file, click on Browse to browse your local hard					
	drive and locate the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



Miscellaneous (Ping)

System Tools> M	iscellaneous						
Miscellaneous utilities	•						
Ping Test:	Destination:		Ping				
Ping Test Result:							



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.

5.3.4 System Status

System Info

System Info.		
Model:	IAR-7002-WA	
Model Description:	Industrial 802.11 a/b/g 3.5	G VPN Router
WAN:	Mode	Dynamic Setting
AN: N:	IP Address	192.168.0.94
	Broadcast Address	192.168.0.255
	Subnet Mask	255.255.255.0
-AN:	Default Gateway	192.168.0.1
	DNS(Primary)	192.168.0.1
	DNS(Secondary)	
	MTU	1500
	MAC Address	00:00:56:04:02:11
LAN:	IP Address	192.168.10.1
	Subnet Mask	255.255.255.0
	MTU	1500
WAN:	MAC Address	00:00:56:04:02:10
	DHCP Server	Enabled
Wireless:	Wireless	Enabled
	SSID	RT61WRT00AB2C
	Channel	6
	Encryption Mode	None
	MAC Address	00:19:DB:00:AB:2C

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 Stati	us> S	ystem Log		
System log.				
Log Option:	 DHCP Server NTP Client PPPoE Client Wireless Client Firewall Select All 		Boot Message PPTP VPN OpenVpn UPNP Deselect All	Save Option
System Log:				Refresh Clear Logs
# Date Ti	ime	Item		Content
# Date Ti	ime	Item		Content
Apply C	ancel			



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

Interface	Send	Receive
Wired LAN	42108845 Bytes (200861 Packages)	41739910 Bytes (247076 Packages)
Wired WAN	45114425 Bytes (246303 Packages)	45465241 Bytes (242149 Packages)
/ireless LAN	3653 Packets	71415 Packets

Traffic Statistics Screen

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



Wired/Wireless Clients

Lease IP Address	Communication Type
192.168.10.84	Wired



This page of the list displays the **Mac Address** and **Lease IP Address** of the wired/wireless clients connected. **Communication Type** shows the physical connection type of the client.



Technical Specifications

LAN Interface	
RJ45 Ports	2 x 10/100Base-T(X), Auto MDI/MDI-X
Protection	Built-in1.5KV magnetic isolation
Protocols	ICMP, IP, TCP, UDP, DHCP, BOOTP, ARP/RARP,
	DNS, SNMP MIB II, HTTPS, SSH, SNMPV1/V2,
	Trap, Private MIB
P.O.E. PD	Present at ETH2 of IAR-7002-WA+
	Power Device (IEEE802.3af):
	IEEE 802.3af compliant input interface
	Power consumption: 8Watts max.
	Over load & short circuit protection
	Isolation Voltage: 1000 VDC min.
	Isolation Resistance: 10 ⁸ ohms min
WLAN Interface	
Antenna Connector	Reverse SMA
Radio Frequency Type	DSSS
Modulation	IEEE802.11a: OFDM with BPSK, QPSK, 16QAM,
	64QAM
	OFDM @ 54 Mbps, CCK @ 11/5.5
	Mbps, DQPSK @ 2 Mbps, DBSK @
	1 Mbps
	IEEE802.11b: CCK, DQPSK, DBPSK
	IEEE802.11g: OFDM with BPSK, QPSK, 16QAM,
	64QAM
Frequency Band	America / FCC: 2.412~2.462 GHz (11 channels)
	5.15 to 5.25 GHz (4 channels)
	Europe CE / ETSI: 2.412~2.472 Ghz (13 channels)
	5.15 to 5.25 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
Transmit Power	IEEE802.11a/b/g: 18dBm
Receiver Sensitivity	-81dBm@11Mbps, PER< 8%;
	-64dBm@54Mbps, PER< 10%
Encryption Security	WEP: (64-bit, 128-bit key supported)



	WPA:
	WPA2:802.11i (WEP and AES encryption)
	PSK (256-bit key pre-shared key supported)
	802.1X and Radius supported
	TKIP encryption
Wireless Security	
Wireless Security	SSID broadcast disable
LED Indicators	PWR 1(2) (P.O.E., IAR-7002-WA+) / Ready:
	1) Red On: Power is on and booting up.
	2) Green On: Power is on and functioning normally.
	ETH1 (2) Link / ACT:
	Orange ON/Blinking: 10 Mbps Ethernet
	Green ON/Blinking: 100 Mbps Ethernet
	WLAN Link/ACT: Green
	WLAN Strength:1<25%, 2<50%, 3<75%, 4<100%
	Fault: Power or LAN link down (Red)
Power Requirements	
Power Input Voltage	PWR1/2: 12 ~ 48VDC in 6-pin Terminal Block
Reverse Polarity Protection	Present
Power Consumption	6 Watts (USB device not included)
Environmental	
Operating Temperature	-10 to 55°C
Storage Temperature	-20 to 85°C
Operating Humidity	5% to 95%, non-condensing
Mechanical	
Dimensions(W x D x H)	52 mm(W)x 106 mm(D)x 144 mm(H)
Casing	IP-30 protection
Regulatory Approvals	
Regulatory Approvals	FCC Part 15, CISPER (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS),
	EN61000-4-4 (EFT), EN61000-4-5 (Surge),,
	EN61000-4-6 (CS)
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Waranty	3 years



Appendix A

How to configure openvpn and use openvpn in the Windows?

Step 1: Download openvpn-gui-1.0.3.exe and run the install program. If there is a pop-up box opened at the course of the install, please you click "Continue..." and finish the install. Default path is: "C:\Program Files\OpenVPN".

Step 2: Configure the OpenVPN Server.

 Modify the parts in "C:\Program Files\OpenVPN\easy-rsa\vars.bat.sample" as follows:

set KEY_COUNTRY=US set KEY_PROVINCE=CA set KEY_CITY=SanFrancisco set KEY_ORG=Oring set KEY_EMAIL=staff@oring-networking.com

 (2) Start > Run... > Input "cmd", and enter into Command Prompt. > Input "cd c:\Program Files\openvpn\easy-rsa"

Run **init-config.bat**: create the vars.bat and openssl Run **vars.bat**, **clean-all.bat**: create new empty index and serial files Run **build-ca.bat**: build a CA key Run **build-dh.bat**: build a DH file for server side Run **build-key-server.bat server**: build a private key/certificate for openvpn server Run **build-key.bat client**: build key files in PEM format for client machine

All inborn secret-keys are in "c:\Program Files\openvpn\easy-rsa\keys".

OpenVPN Server needs files: **ca.crt, dh1024.pem, server.crt, server.key,** and copy to "C:\Program Files\OPENVPN\Config".

OpenVPN Client needs files: ca.crt, client.crt, client.key, and copy to



"C:\Program Files\OPENVPN\Config".

(3) Edit the server.ovpn in the openvpn server and client.ovpn in the openvpn client.

server.ovpn:

Modify according to by the router web settings

#Tunnel options	would according t
mode server	# Set OpenVPN major mode

dev tap0	# TUN/TAP virtual network device
keepali∨e 15 60	# Simplify the expression ofping
#daemon	# Become a daemon after all initialization
verb 3	# Set output verbosity to n
comp-Izo	# Use fast LZO compression

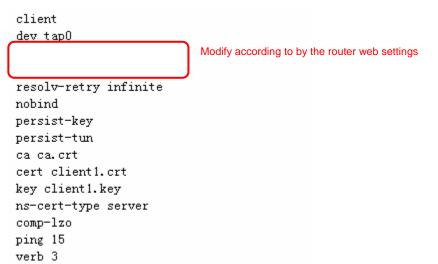
OpenVPN server mode options

client-to-client	# tells OpenVPN to internally route client-to-client traffic
duplicate-cn	# Allow multiple clients with the same common name

TLS Mode Options

tls-server	# Enable TLS and assume server role during TLS handshake
ca ca.crt	# Certificate authority (CA) file
dh dh1024.pem	# File containing Diffie Hellman parameters
cert server.crt	# Local peer's signed certificate
key server.key	# Local peer's private key

client.ovpn:





Step 3: Use the OpenVPN GUI.

- (1). Open Router web page and configure the Advanced Setting->VPN Setting->Open VPN.
- (2). In the OpenVPN Server, open "C:\Program Files\OpenVPN\config" and run server.ovpn. In the OpenVPN Client, open "C:\Program Files\OpenVPN\config" and run client.ovpn. The massage "Initialization Sequence Completed" indicates that the openvpn connection is established successfully.

<u>ex</u> [C:\Program Files\Ope	wWFW\config\client.ovpn] OpenWFW 2.0.9 F4:EXIT F1:USR1 F2:USR2 F3:HUP
		OpenVPN 2.0.9 Win32-MinGW ISSLI ILZOI built on Oct 1 2006
		IMPORTANT: OpenVPN's default port number is now 1194, based on an official port number assignment by IANA.
		rlier used 5000 as the default port.
		LZO compression initialized
		Control Channel MTU parms [L:1574 D:138 EF:38 EB:0 ET:0 EL:0]
		Data Channel MTU parms [L:1574 D:1450 EF:42 EB:135 ET:32 EL:0 AF:3/1]
		Local Options hash (UER=U4): 'd79ca330'
		Expected Remote Options hash (VER=V4): 'f?df56b8'
		UDPv4 link local: [undef]
		UDPv4 link remote: 192.168.0.59:1194
		TLS: Initial packet from 192.168.0.59:1194, sid=d821666a 3493d5fd
		UERIFY OK: depth=1,_/C=KG/ST=NA/L=BISHKEK/0=OpenUPN-TEST/0U=rd/CN=rich/emailAddress=me@myhost.mydomain
		UERIFY OK: nsCentType-SERVER
		UERIFY OK: depth=0, /C=KG/ST=NA/O=OpenUPN-TEST/OU=rd/CN=rich/emailAddress=me@myhost.mydomain
		Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
		Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
		Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
		Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
		Control Gnannel: 11501, cipner 11501/55103 DHE-HSH-HE2505-SHH, 1024 Dit KSH [rich] Peer Connection Initiated with 192.168.0.59:1194
		IPIENJ Feer Connection Initiated With 172.106.0.371174 SENT CONTROL (Fich): /PUSH_REQUEST/ <status=1)< td=""></status=1)<>
		Semi Control Inichi. Fost_negoesi Statusi. PUSH: Received control message: 'PUSH_REPUX,ping 15,ping-restart 60'
		1051 Necessa concrete message. 1051 Net 17, 119 17, 119 17, 119 18, 15, 119
		OF 11995 111996 - 11995 11997 - 11995 11997 - 11997 119
		The wind device the sector of
	Jan 04 13:35:00 2008	
		Successful ARP Flush on interface [5] (D6B3D213-32E2-45B2-651E-C7FE62B64456)
		IEST ROUTES: 0/0 succeeded len=1 ret=0 a=0 u/d=down
		Route: Waiting for IUN/IAP interface to come up
		TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
		Route: Waiting for TUN/TAP interface to come up
		TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
ri	Jan 04 13:35:03 2008	Route: Waiting for TUN/TAP interface to come up
ri .	Jan 04 13:35:07 2008	TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
		Route: Waiting for TUN/TAP interface to come up
		TEST ROUTES: 0/0 succeeded len=-1 ret=0 a=0 u/d=down
		Route: Waiting for TUN/TAP interface to come up
		TEST ROUTES: 0/0 succeeded len=-1 ret=1 a=0 u/d=up
Fri	Jan 04 13:35:09 2008	Initialization Sequence Completed