Industrial

Wireless Access Point

IAP-6002-WA / WA+ User's Manual



Version 1.0 May, 2008.



Table of Content

Gettin	g to Know Your Access Point 1	I
1.1	About the ORing Access Point	1
1.2	Software Features	1
1.3	Hardware Features	1
Hardw	are Installation2	2
2.1	Installation AP on DIN-Rail	2
2.2	Wall Mounting Installation	3
Hardw	are Overview	;
3.1	Front Panel	5
3.2	Front Panel LEDs	7
3.3	Bottom Panel	3
3.4	Rear Panel	3
Cables	s and Antenna 9)
4.1	Ethernet Cables	9
4.2	100BASE-TX/10BASE-T Pin Assignments	9
4.3	Wireless Antenna 10)
Manag	jement Interface11	l
5.1	Explore IAP-6002-WA / WA+1	1
5.′	.1 AP-Tool software1	1
5.2	UPnP Equipment	2
5.3	Configuration by Web Browser13	3
5.4	About Web-based Management14	1
5.5	Main Interface14	1
5.5	5.1 Basic Setting	5
	Setting Operation Mode15	5
	Setting WDS (Bridge Mode) 16	3
	Setting Wireless)
	LAN Setting24	4

Setting DHCP Server
5.5.2 Advanced Setting
Wireless
MAC Filter
System Event
Email Settings
SNMP Settings
Syslog Server Settings 31
5.5.3 System Tools
Administrator
Date & Time
Configuration
Firmware Upgrade
Miscellaneous
5.5.4 System Status 37
System Info
System Log 37
Traffic Statistics
Wireless Clients
5.5.5 Online Help 39
Technical Specifications40





Getting to Know Your Access Point

1.1 About the ORing Access Point

IAP-6002-WA / WA+ are reliable IEEE802.11b/g WLAN with 2 ports LAN Access Point. It can be configured to operate in AP/Bridge/Repeater mode. You can configure IAP-6002-WA / WA+ by Window Utility or WEB interfaces via LAN port or WLAN interface. IAP-6002-WA / WA+ provide dual Ethernet ports in switch mode, so you can use Daisy Chain to reduce the usage of Ethernet switch ports. IAP-6002-WA+ also provides PD feature on ETH2 which is fully compliant with IEEE802.3af P.O.E. specification. Therefore, IAP-6002-WA / WA+ are one of the best communication solutions for wireless application.



1.2 Software Features

- High Speed Air Connectivity: WLAN interface support up to 54Mbps link speed connection
- Highly Security Capability: WEP/WPA/WPA2/Radius/TKIP supported
- Support AP/Bridge/Repeater Mode
- Switch Mode Supported: Daisy Chain support to reduce usage of switch ports
- Secured Management by HTTPS
- Event Warning by Syslog, Email, SNMP Trap, Relay and Beeper

1.3 Hardware Features

- Fully Compliant with IEEE802.3af (Power Device at ETH2, IAP-6002-WA+ only)
- Redundant Power Inputs: 12~48 VDC on terminal block
- 10/100Base-T(X) Ethernet port
- 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 AP on DIN-Rail

Each AP has a DIN-Rail kit on rear panel. The DIN-Rail kit helps AP to fix on the DIN-Rail. It is easy to install the AP on the DIN-Rail:

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



Step 2: Push the AP toward the DIN-Rail until you heard a "click" sound.





2.2 Wall Mounting Installation

Each AP has another installation method to fix the AP. A wall mount panel can be found in the package. The following steps show how to mount the AP 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 from any damage, the screws should not larger than the size that used in IAP-6002-WA / WA+.



Step 3: Mount the combined AP on the wall.





Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the IAP-6002-WA / WA+.

Port	Description	
10/100 RJ-45 fast	2 10/100Base-T(X) RJ-45 fast Ethernet ports support	
Ethernet ports	auto-negotiation.	
	Default Setting :	
	Speed: auto	
P.O.E. PD Port	ETH2 of IAP-6002-WA+ compliant with IEEE802.3af P.O.E.	
	specifications	
ANT.	Reversed SMA connector for external antenna.	





- 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.
- 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 Relay. When the fault occurs, the amber LED will be light on.
- 6. 10/100Base-T(X) Ethernet ports. (IAP-6002-WA+ contains PD function of P.O.E.)
- 7. LED for Ethernet ports status.
- 8. LED for WLAN link status.
- 9. LED for WLAN signal strength.



3.2 Front Panel LEDs

LED	Color	Status	Description	
	Green/Red	Green On	P.O.E. power connected.	
POF		Green blinking	Device been located	
F.U.E.		Red blinking	Indicates an IP conflict, or	
(141 -0002-1147)			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 or	
Taun			Port down/fail.	
	Green	On	WLAN activated.	
WEAN	Green	Blinking	WLAN Data transmitted.	
			WLAN signal strength.	
WLAN Strength	Green	On	1<25%, 2<50%, 3<75%,	
			4<100%	
10/100Base-T(X) Fast Ethernet ports				
10Mbps	Amber	On	Port link up at 10Mbps.	
LNK/ACT		Blinking	Data transmitted.	
100Mbps	Green	On	Port link up at 100Mbps.	
LNK/ACT		Blinking Data transmitted.		



3.3 Bottom Panel

The bottom panel components of IAP-6002-WA / WA+ are showed 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.



Bottom panel of IAP-6002-WA / WA+

3.4 Rear Panel

The rear panel components of IAP-6002-WA / WA+ are showed as below:

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



Rare panel of IAP-6002-WA / WA+



Cables and Antenna

4.1 Ethernet Cables

The IAP-6002-WA / WA+ WLAN AP have standard Ethernet ports. According to the link type, the AP 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

4.2 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.

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

RJ-45 Pin Assignments

The IAP-6002-WA / WA+ AP support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and AP. 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.

4.3 Wireless Antenna

A 2.4GHz antenna is used for IAP-6002-WA / WA+ and connected with a reversed SMA connector. External antenna also can be applied with this connector.



Management Interface

5.1 Explore IAP-6002-WA / WA+

5.1.1 AP-Tool software

Each model contains friendly software, AP-Tool, to explore IAP-6002-WA / WA+ on local area network.

Step 1: Open the AP tool and click "Refresh list", the AP devices will show on the list.

Step 2: Choose your access point, and it will show the AP attribute. Simultaneity, you can manual set the AP's IP address.

Firmware Version:	1.1b 802.11 a / b/g Industrial Access Point			
Description:				
Mac address:	c address: 00:12:77:55:42:aa address: 192.168.0.26 status: DHCP			
IP address:				
IP status:				
Protocol:	DHCP			
Protocol: IP address:	DHCP			
Protocol: IP address: Subnet mask:	DHCP ▼ 192 168 0 26 255 255 255 0			
Protocol: IP address: Subnet mask: Default gateway:	DHCP Image: Constraint of the second secon			
Protocol: IP address: Subnet mask: Default gateway: Primary dns:	DHCP Image: Constraint of the second secon			

User interface of AP-Tool

Step 3: Click "Access via web" button, it will go to web page.

Refresh list	Access via web	Apply	About	Quit



5.2 UPnP Equipment

Step 1: To check whether the UPnP UI of the computer is connected to the IAP-6002-WA / WA+, go to Control Panel > Add or Remove Programs > Windows Components Wizard > Networking Servers > UPnP User Interface and pitch on the UPnP User Interface.

Networking Services	5
To add or remove a component, click the check box. A shaded box of the component will be installed. To see what's included in a comp Subcomponents of Networking Services:	means that only part onent, click Details.
Internet Gateway Device Discovery and Control Client	0.0 MB
Peerto-Peer	0.0 MB
🔲 🛄 RIP Listener	0.0 MB
Simple TCP/IP Services	0.0 MB
🔄 🛄 UPnP User Interface	0.2 MB
	~
Description: Allows you to find and control Internet connection sha software that uses UPnP(TM).	aring hardware and
Total disk space required: 0.0 MB	Details
0	Dordila

UPnP configuration page

Step 2: At the right-below corner of the computer, you will find a sign of the UPnP equipment.





Step 3: Click the sign of the UPnP equipment, then you will find the UPnP equipment in the network neighborhood.



Step 4: Right click the UPnP equipment to choose "Properties", it will show as the following pictures:

Ě.	AP-6002-WA-546465
Manufacturer:	Oring
Model Name:	IAP-6002-WA
Model Number:	F/W Version 1.2h
Description:	Industrial 802.11 b/g Access Point
Device Address:	http://192.168.10.2/

Step 5: Right click the UPnP equipment or double click the UPnP equipment to transfer; it will go to the web page.

5.3 Configuration by Web Browser

This section introduces the configuration by Web browser.



5.4 About Web-based Management

An embedded HTML web site resides in flash memory in the system. It contains advanced management features and allows you to manage the AP from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

Through the front section's information, you will see as follows, enter your user name (admin) and your password (leave blank by default), then click OK to continue.

Connect to	? 🛛
IAP-6002-WG	
<u>U</u> ser name:	2
Password:	
	Remember my password
	OK Cancel

Login screen

For security reasons, we strongly suggest you change the password. Click on **System Tools > Administrator** and modify the password.

5.5 Main Interface

The **Home** screen will appear. Please click "Run Wizard" to go to the **Home > Setup Wizard** page to quick install the AP.



	ndustrial 802.11 a/b/g Access Point	
ipen all		www.oring-networking.co
Home Basic Setting	Home> Setup Wizard	
G Operation Mode Wireless WDS DHCP Server Advanced Setting System Tools System Status	Step 0/4	
	The wizard will guide you through these four steps. Begin by clicking on 'Next'.	
	Step 1: Set new administrator's password	
	Step 2: Set wireless SSID and channel	
) Online Help	Step 3: Set wireless encryption	
	Step 4: Save and revalidate AP	
	Back Next	

Main interface

5.5.1 Basic Setting Setting Operation Mode

AP	
This mode provi	les Access Point services for other wireless clients.
O AP-Client	
The AP-Client fu behind the AP ca	nction provides a 1-to-N MAC address mapping mechanism such that multiple stations an transparently connect to the other AP even they didn't support WDS.
O Bridge	
This mode provi supported throu	les Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is gh Wireless Distribution System(WDS).

Operation mode interface

Label	Description
Bridge	This mode provides Static LAN-to-LAN Bridging functionality.
	The static LAN-to-LAN bridging function is supported through
	Wireless Distribution System (WDS).
AP	This mode provides Access Point services for other wireless
	clients.
AP-Client	The AP-Client function provides a 1-to-N MAC address mapping
	mechanism such that multiple stations behind the AP can
	transparently connect to the other AP even they didn't support
	WDS.



In each mode, the IAP-6002-WA / WA+ forwards packet between its Ethernet interface and wireless interface for wired hosts on the Ethernet side, and wireless hosts on the wireless side.

Operation mode of the	AP should be set to "Brid	dge" mode before these settings changed.	
WDS Mode:	Disabled 💌		
Encryption Type:	None 💌		
WDS Key:	None		
Peer Mac Address 1:		Enabled	
Peer Mac Address 2:	ALS	Enabled	
Peer Mac Address 3:	6	Enabled	
Peer Mac Address 4:		Enabled	

Setting WDS (Bridge Mode)

WDS setting interface

This type of wireless link is established between two IEEE 802.11 access points. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.



Point-to-Multipoint WDS Link





Point-to-Point WDS Link

The following table describes the labels in this screen.

Label	Description
WDS Mode	This mode provides Static LAN-to-LAN Bridging functionality.
	The static LAN-to-LAN bridging function is supported through
	Wireless Distribution System (WDS).
Encryption Type	Select the type of security for your wireless network
WDS Key	Fill in the encryption key when Encryption Type is TKIP or AES.
Peer MAC Address	Set the Mac address(es) of other access point(s). Simultaneity,
	choose on "Enable".

First of all, if APs link with WDS mode, it should obey the following rules:

- 1. LAN IP Address should set different IP in the same network.
- 2. All AP's DHCP Server should set shutdown.
- 3. WDS should set Enable.
- Each AP should have the same setting except 'Peer Mac Address' set to the other's Mac address
- 5. WEP Key and Channel should be the same, and each AP's SSID should be broadcast to see in the other's computer.
- 6. AP's distance should limit to a certainty area.



WDS – Restricted Mode

Operation mode of the	IP should be set to "Bridge" mode before these settings changed.
WDS Mode:	Restricted Mode
Encryption Type:	None 💌
WDS Kev:	None
Peer Mac Address 1:	TKIP cc:dd:ee
Peer Mac Address 2:	Enabled
Peer Mac Address 3:	Enabled
Peer Mac Address 4:	Enabled

The peer WDS APs are according to the MAC address listed in "Peer Mac Address" fields.

WDS –Bridge Mode

WDS Mode:	Bridge Mode	
Encryption Type:	None 💌	
WDS Key:	None	
Peer Mac Address 1:	TKIP cc:dd:ee	✓ Enabled
Peer Mac Address 2:		Enabled
Peer Mac Address 3:		Enabled
Peer Mac Address 4:		Enabled

Same as Restrict mode in functionality and also one WDS link side can not set **Peer Mac** Address 1-4.



The working principle of Bridge Mode as follows:



In the figure, the AP behaves as a standard bridge that forwards traffic between WDS links (links that connect to other AP/wireless bridges) and an Ethernet port. As a standard bridge, the AP learns MAC addresses of up to 64 wireless or 128 total wired and wireless network devices, which are connected to their respective Ethernet ports to limit the amount of data to be forwarded. Only data destined for stations which are known to reside on the peer Ethernet link, multicast data or data with unknown destinations need to be forwarded to the peer AP via the WDS link.

WDS – Repeater Mode

Operation mode of the	AP should be set to "Bridge"	mode before these settings changed	d.
WDS Mode:	Repeater Mode 🗸		
Encryption Type:	None 💌		
WDS Key:	None		
Peer Mac Address 1:	TKIP cc:dd:ee	✓ Enabled	
Peer Mac Address 2:		Enabled	
Peer Mac Address 3:		Enabled	
Peer Mac Address 4:		Enabled	



Same as Restrict mode in functionality and also one WDS link side can not set **Peer Mac Address 1-4.**





In the figure, Repeater is used to extend the range of the wireless infrastructure by forwarding traffic between associated wireless stations and another repeater or AP connected to the wired LAN.

Setting Wireless

-	index on the second second second	
These are the basic	wireless settings for the AP.	
SSID:	masm_suzhou	
Channel:	Auto 🐱	
Peer AP SSID:		(Apply when 'AP-Client' mode selected)
Security Options		
Security Type:	None 🖌	
	None	
	WEP	
	WPA-PSK/WPA2-PSK WPA/WPA2	



The following table describes the labels in this screen.

Label	Description
	Service Set Identifier Default is the default setting. The SSID is
	a unique name that identifies a network. All devices on the
SSID	network must share 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 6 is the default channel, input a new number if you want
Channel	to change the default setting. All devices on the network must
	be set to the same channel to communicate on the network.
	Only Operation Mode selects AP-Client Mode, you should enter
reel af 331D	the peer AP SSID.
	Select the type of security for your wireless network at Security
	Туре:
	None: Select for no security.
Security options	WEP: Select for security.
county options	WPA-PSK/WPA2-PSK: Select for WPA-PSK or WPA2-PSK
	without a RADIUS server.
	WPA/WPA2: Select for WPA (Wi-Fi Protected Access) authentication in conjunction with a RADIUS server.

Security Type – None

No security protection on your wireless LAN access.



Security Type – WEP

nese are the basic wi	ireless settings for the AP.
SSID:	masm_suzhou
Channel:	Auto 👻
Peer AP SSID:	(Apply when 'AP-Client' mode selected)
Security Options	
Security Type:	WEP
Auth Mode:	○ Open ○ Shared ④ WEPAUTO
WEP Encryption:	128 Bit 💌
Key Type:	Hex (26 characters)
Default Key Index:	
KEY1:	111111111111111111111111
KEY2:	
KEY3:	
KEY4:	

- 1. Security Type: Select WEP
- 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

These are the basic w	vireless settings for the AP.	
SSID:	masm_suzhou	
Channel:	Auto 🛩	
Peer AP SSID:		(Apply when 'AP-Client' mode selected)
Security Options Security Type:	WPA-PSK/WPA2-PSK V	
Auth Mode:	○ WPAPSK ○ WPA2PSK ⊙ WP	APSK/WPA2PSK mix
Encryption Type:	○ TKIP	
Shared Key:	qwertyuiop	(8~64 characters)

- 1. Security Type: Select WPA-PSK/WPA2-PSK.
- 2. Encryption Type: Select **TKIP** or **AES** encryption.
- 3. Share Key: Enter your password. The password can be between 8 and 64 characters.

Security Type – WPA /WPA2

SSID:	masm_suzhou	
Channel:	Auto 💌	
Peer AP SSID:		(Apply when 'AP-Client' mode selected)
Security Options		
Security Type:	WPA/WPA2	
Auth Mode:	○ WPA ○ WPA2 ⊙ WPA/WPA2	mix
Encryption Type:	○ TKIP ④ AES ○ TKIP/AES mix	
Radius Server IP:	0.0.0.0	
Radius Port:	1812	
Shared Secret:	radius kev	

- 1. Security Type: Select WPA/WPA2
- 2. Radius Server IP: Enter the IP address of the RADIUS Server.
- 3. Port: Enter the RADIUS port (1812 is default).
- 4. Shared Secret: Enter the RADIUS password or key.



RADIUS (Remote Authentication Dial-in User Service) is the industrial standard agreement, and it is used to provide an identify verification. The Radius customer (is usually a dial-in server, VPN server or wireless point) send your proof and the conjunction parameter to the Radius server by Radius news. The Radius server validates the request of the Radius customer, and return Radius news to back.

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 shows in the following pictures:



LAN Setting

The **Basic Setting > LAN Setting** page is mainly set IP address for LAN interface. To access the AP normally, a valid IP address of your LAN should be specified to the LAN interface. The default IP setting is DHCP server (Obtain an IP address automatically).



AN settings of AP.										
Obtain an IP	addres	s automat	ically							
O Use the follo	wing IP	address								
IP Address:	192	. 168	. 0	. 12	1					
Subnet Mask:	255	255	255	0						
Default Gateway:	192	. 168		.1						
• Obtain DNS •	192 server a wing Di	ddress au	. 0	. 1 . 1						
Obtain DNS : Ottain DNS : Ottain DNS :	192 server a wing DI	ddress au NS server	. 0 . ddresse	. 1 . 1						
Obtain DNS s Obtain DNS s Ouse the follo Preferred DNS: Alternate DNS:	192 server a wing Di 192	. 168 address au NS server . 168	tomatical addresse	. 1 . 1 . 1						

Label	Description
Obtain an IP address	Select this option if you would like to have an IP address
automatically	automatically assigned to the IAP-6002-WA / WA+ by DHCP
	server in your network
Use the following IP	Select this option if you are manually assigning an IP address.
address	 IP Address: There is a default IP address in the AP, and you can input a new IP address. Subnet Mask: 255.255.255.0 is the default Subnet Mask. All devices on the network must have the same subnet mask to communicate on the network. Default Gateway: Enter the IP address of the router in your network.
Obtain DNS server	This option is selected by DHCP server.
address	
automatically	
Use the following	This option is selected by manually set
DNS server	
	Preferred DNS: There is a default DNS server, and you can input
addresses	Preferred DNS: There is a default DNS server, and you can input another new DNS server.
addresses	Preferred DNS: There is a default DNS server, and you can input another new DNS server.
addresses	 Preferred DNS: There is a default DNS server, and you can input another new DNS server. Alternate DNS: There is a default DNS server, and you can input



Setting DHCP Server

sasic setting> DHC	P Server		
The AP can be setup as a	DHCP server to distribute IP a	addresses to the WLAN network.	
DHCP Server Options Starting IP address: Maximum Number of IPs Lease Time:	 Enabled Disabled . <l< th=""><th></th><th></th></l<>		
DHCP Clients List:			

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. Enable – the AP
	will be the DHCP server on your local network
Start IP Address	The dynamic IP assign range. Low IP address is the beginning
	of the dynamic IP assigns range. For example: dynamic IP
	assign range is from 192.168.1.100 to 192.168.1.200.
	192.168.1.100 will be the Start IP address.
Maximum Number of	The dynamic IP assign range. High IP address is the end of the
IPs	dynamic IP assigns range. For example: dynamic IP assign
	range is from 192.168.1.100 to 192.168.1.200. 100 will be enter
	into textbox.
Lease Time (Hour)	It is the time period that system will reset the dynamic IP
	assignment to ensure the dynamic IP will not been occupied for a
	long time or the server doesn't know that the dynamic IP is idle.
DHCP Clients List	List the devices on your network that are receiving dynamic IP
	addresses from the IAP-6002-WA / WA+.



5.5.2 Advanced Setting

Wireless

Advanced Setting> Win	eless	
Wireless performance tunnin	g.	
Beacon Interval:	100	(msec, range:20~999, 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: 1~100, default:100)
Wireless Mode:	● BG I	— Mixed Mode 🔘 B Mode 🔘 G Mode
Transmission Rate:	Auto	v
Preamble:	💿 Lon	g 🔿 Short
SSID Broadcast:	💿 Ena	bled 🔿 Disabled
Apply Cancel		

Label	Description				
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	This value should remain at its default setting of 2346. The				
Threshold	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.
Xmit Power	This value ranges from 1 - 100 percent, default value is 100
	percent. A safe increase of up to 60 percent would be suitable
	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.
Wireless Network	If you have Wireless-G and 802.11b devices in your network, then
Mode	keep the default setting, BG Mixed mode. If you have only
	Wireless-G devices, select G Mode. If you would like to limit
	your network to only 802.11b 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
	possible connection speed between the AP and a wireless client.
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
SSID Broadcast	When wireless clients survey the local area for wireless networks
	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.



MAC Filter

Use **Advanced Setting > MAC Filters** to allow or deny wireless clients, by their MAC addresses, from accessing the IAP-6002-WA / WA+. You can manually add a MAC address or select the MAC address from **Connected Clients** that are currently connected to the AP.

Advanced Setting	J> MAC Filters
Filters are used to a	allow or deny Wireless Clients from accessing the AP.
MAC Filters:	O Enabled
Options Only allow MAC	Caddress(es) listed below to connect to AP
Only deny MAC	address(es) listed below to connect to AP
MAC Filter List:	Copyto
	Delete
Connected Clients:	Copyto
MAC Address:	
	Add Clear
Apply Cancel]

The following table describes the labels in this screen.

Label	Description
MAC Filter	Enable or disable the function of MAC filter. MAC address
	allowed or denied option is selected by you.
MAC Filter List	This list will display the MAC addresses that are in the selected
	filter.
Connected Clients	This list will display the wireless MAC addresses that linked with
	AP.
MAC Address	MAC addresses need to be added to or clear from MAC filter list.
Apply	Click Apply to set the configurations.

System Event

When the AP event 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 > System Event** page.



Advanced Setting	> System Event			
System Event Configu	iration.			
Device Event Notificat	tion			
Hardware Reset (Cold Start)		SMTP Mail	SNMP Trap	Syslog
Software Reset (War	Software Reset (Warm Start)		SNMP Trap	Syslog
Login Failed		SMTP Mail	SNMP Trap	Syslog
IP Address Changed		SMTP Mail	SNMP Trap	Syslog
Password Changed		SMTP Mail	SNMP Trap	Syslog
Redundant Power Ch	anged	SMTP Mail	SNMP Trap	Syslog
SNMP Access Failed		SMTP Mail	SNMP Trap	Syslog
Wireless Client Assoc	iated	SMTP Mail	SNMP Trap	Syslog
Wireless Client Disas	sociated	SMTP Mail	SNMP Trap	Syslog
	1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 -			
Fault Event Notificatio	on and Fault LED/Rela	У	1.101.001	10.997
Power 1 Fault	SMTP Mail	SNMP Trap	Syslog	Fault LED/Relay
Power 2 Fault	SMTP Mail	SNMP Trap	Syslog	Fault LED/Relay
Eth1 Link Down	SMTP Mail	SNMP Trap	Syslog	Fault LED/Relay
Eth2 Link Down	SMTP Mail	SNMP Trap	Syslog	E Fault LED/Relay
	Sector sector sector	a call a suspect and	and the sponse	and the state of the state of the

System events record the activities of the AP 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 server. The Syslog will record the event locally and may send the log 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.

Email Settings

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

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.

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:	

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	Specify the IP of trap server, which is the address to which it will							
1-4	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.							

Syslog Server Settings

Syslog Server settings		
Syslog Server IP:]
Syslog Server Port:	514	(0 represents default)



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.						

5.5.3 System Tools

Administrator

In this page, you can change the username and password. The new password must be typed twice to confirm (the default Name and Password is "**admin**" and "").

System Tools> Adminis	rator
Modify web administrator's na	me and password.
Old Name:	admin
Old Password:	
New Name:	admin
New Password:	
Confirm New Password:	
Web Protocol:	● HTTP ○ HTTPS
Port:	80
Web Access Control:	☑ Wired ☑ Wireless
UPnP:	💿 Enable 🔿 Disable
Apply Cancel	

Label	Description						
Old Name	This field displays the old login name. It's read only. The default						
	value of login name is "admin".						
Old Password	Before making a new setting, you should provide the old						
	password for a verify check. Acceptable inputs of this field						
	contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters						
	in length. The factory default value of login password is null.						
New Name	Enter a new login name. Acceptable inputs of this field contains						



	'0-9', 'a-z', 'A-Z' and must be between 1 to 15 characters in length.							
	This field can not accept null input.							
New Password	Enter a new login password. Acceptable inputs of this field							
	contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters							
	in length.							
Confirm New	Retype the password to confirm it. Acceptable inputs of this field							
Password	contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters							
	in length.							
Web Protocol	Choose on the protocol for web. The default value is HTTP, if							
	you want the web pages' security is better, choose the HTTPS							
	protocol.							
Port	Corresponding to the Web protocol, there is a default port (HTTP:							
	80, HTTPS: 443). And you can enter another number which							
	should be in range of 1-65535.							
Web Access Control	Choose the checkbox of the Wired and Wireless; you can visit the							
	web page through the mode you choose.							
UPnP	Pitch on "Enable", and the UPnP will display in the right-behind							
	corner.							

HTTPS (HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

Date & Time

In this page, 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.



System Tools> I	Date/Tim	e				
Date/Time settings.						
Local Date:	2008	Year	5	Month	13	Day
Local Time:	11	Hour	40	Minute	58	Second
Time Zone:	GMT+0	08:00 💌				
	Get Current Date & Time from Browser					
NTP:	Ena	able				
NTP Server 1:	time.ni:	st.gov				
NTP Server 2:	pool.ntp.org				(optional)	
Synchronise:	Every H	Hour	*	at 00 🗸	: 00) 🗸
	100					
Apply Cancel						

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 browser.					
Time from Browser						
NTP	Enable or disable NTP function to get the time from the NTP					
	server.					
NTP Server 1	The initial choice about NTP Server.					
NTP Server 2	The second choice about NTP Server.					
Synchronize	Set the time, and the AP's time synchronize with the NTP Server					
	at the time					



Configuration

System Tools> Configuration	
You can backup the configuration file to your computer, and restore a previously saved configuration.	
Save configuration to local	
Download	
Restore a previously saved configuration	
Browse	
Upload	
Use the button below to restore the default settings	
Restore Default Settings	

The following table describes the labels in this screen.

Label	Description
Download	The current system settings can be saved as a file onto the local
configuration	hard drive.
Upload configuration	The saved file or any other saved setting file can be uploaded
	back on the AP. To reload a system settings file, click on
	Browse to browse the local hard drive and locate the system file
	to be used. Click Upload when you have selected the file to be
	loaded back onto the AP.
Restore Default	You may also reset the IAP-6002-WA / WA+ back to factory
Settings	settings by clicking on Restore Default Settings . Make sure to
	save the unit's settings before clicking on this button. You will
	lose your current settings when you click this button.

Firmware Upgrade

System Tools> Firmware Upgrade							
Do NOT power off the AP while upgrading!							
	Brov	vse					
Start Upgrade							

New firmware may provide better performance, bug fixes or more functions. To upgrade, you need a firmware file correspond to this AP model. It will take several



minutes to upload and upgrade the firmware. After the upgrade is done successfully, the access point will reboot and get revalidated.

Notice: DO NOT POWER OFF THE AP OR PRESS THE RESET BUTTON WHILE THE FIRMWARE IS BEING UPGRADED.

Miscellaneous

If you want restart the access point through the **Warm Reset**, click **Restart Now** to restart the AP.

System Tools> Miscellaneous												
Miscellaneous settings.												
Click the button below to restart the AP.												
Restart Now												



5.5.4 System Status System Info

System Status> System Info					
System information details.					
Model					
Model Name:	IAP-6002-WA				
Model Description:	Industrial 802.11 a/b/g Access Point				
Firmware					
Version:	1.2f				
Ethernet					
MAC Address:	00:00:56:04:02:09				
IP Address:	192.168.0.12				
Subnet Mask:	255.255.255.0				
Default Gateway:	192.168.0.1				
DHCP Server:	Disabled				
Operation Mode					
Operation Mode:	AP				
Wireless					
MAC Address:	00:19:DB:00:AB:6C				
SSID:	masm_suzhou				
Encryption:	WPA-PSK/WPA2-PSK				
Channel:	Auto				
Device Time					
Current Time:	Tue, 13 May 2008 11:42:59 +0800				

This page displays the current information for the IAP-6002-WA / WA+. It will display model name, as well as firmware version, Ethernet, Wireless info and device time.

System Log

System Status> Syste	em Log													
System log details.														
Refresh Clear														
# Date Time					C	ont	ent							

The system log tracks the important events and setting changes of the AP. If the AP is rebooted, the logs are automatically cleared.

Click the button 'Refresh' to refresh the page; Click the button 'Clear' to clear log entries.



Traffic Statistics

terface	Send	Receive
Ethernet	516465 Bytes (1331 Packages)	1463797 Bytes (14474 Packages)
Wireless	0 Bytes (3085 Packages)	7824479 Bytes (64011 Packages)

This page displays the network traffic statistics for both received and transmitted packets through the Ethernet port and wireless connections associated with the AP. Simultaneity, the traffic counter will reset by the device rebooting.

Wireless Clients

ist of connected wireless clients.								
Mac Address	Send	Receive	Current TxRate					
00:20:b3:10:24:8d	2825 Bytes	4097 Bytes	54 Mbps					

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

Current TX Rate is corresponding to the Transmission Rate in the Advanced Setting

> Wireless pages.



5.5.5 Online Help

Click on any item in the **Online Help** screen for more information.

Index	Home -> Setup Wizard
Home	Setup Wizard
 Setup Wizard Basic Setting 	The Setup Wizard is a useful and easy utility to help setup the AP to quickly adapt it to your existing network with only a few steps required. It will guide you step by step to configure th settings of the AP. The Setup Wizard is a helpful guide for first time users to the AP.
Operation Mode WDS	For step 1, you can set a new login password if required, the default login name is 'admin', and default login password is null.
 Wireless 	For step 2, you can set the wireless SSID name and channel, a default SSID has been provided for you. By default the channel is set to 6.
 LAN Setting DHCP Server 	For step 3, set the wireless encryption to WEP will strengthen the security of the wireless network, or just leave encrytion disabled and anyone can connect to the AP.
Advanced Setting Wireless MAC Filter Email/SNMP/Syslog System Event	For setp 4, save the previous settings and revalidate the AP.
System Tools	
Administrator Date & Time Configuration Firmware Upgrade Miscellaneous	
System Status	
System Info	

- System Log
 Traffic Stats
 Wireless Clients



Technical Specifications

LAN Interface	
RJ45 Ports	2 x 10/100Base-T(X), Auto MDI/MDI-X
P.O.E. PD (Power Device)	Present at ETH2 of IAP-6002-WA+
	ETH2 act as 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
Protocols	ICMP, IP, TCP, UDP, DHCP, BOOTP, ARP/RARP,
	DNS, SNMP MIB II, HTTPS, SNMPV1/V2, Trap,
	Private MIB
WLAN Interface	
Operating Mode	AP/Bridge/Repeater
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
	FEE802 11b: CCK_DOPSK_DBPSK
	IEEE802 11g: OEDM with BPSK OPSK 160AM
	640AM
Frequency Band	America / FCC : 2 412~2 462 GHz (11 channels)
	5 15 to 5 25 GHz (4 channels)
	Europe CE / ETSI: $2.412 \sim 2.472$ Gbz (13 channels)
	5 15 to 5 25 GHz (4 channels)
Transmission Rate	IEEE802 11b: 1 / 2 / 5 5 / 11 Mbps
	IEEE802.11a/a: 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)
	TKIP encryption
Wireless Security	SSID broadcast disable
LED Indicators	PWR 1(2) (P.O.E., IAP-6002-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	Dual power inputs PWR1/2: 12 ~ 48VDC in 6-pin
	Terminal Block
Reverse Polarity Protection	Present
Power Consumption	6 Watts
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
Warranty	3 years