



TAP-3120-M12
EN50155 IEEE 802.11 a/b/g and b/g Dual-RF
Wireless Access Point

User's Manual
Version 1.0
July, 2011

www.oring-networking.com



COPYRIGHT NOTICE

Copyright © 2011 ORing Industrial Networking Corp.

All rights reserved.

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

TRADEMARKS



is a registered trademark of ORing Industrial Networking Corp.

All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

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

WARRANTY

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

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

DISCLAIMER

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

CONTACT INFORMATION

ORing Industrial Networking Corp.

3F., No.542-2, Zhongzheng Rd., Xindian Dist., New Taipei City 23148, Taiwan (R.O.C.)

Tel: +886-2-2218-1066 // Fax: +886-2-2218-1014

Website: www.oring-networking.com

Technical Support

E-mail: support@oring-networking.com

Sales Contact

E-mail: sales@oring-networking.com (Headquarters)

sales@oring-networking.com.cn (China)



Table of Contents

Getting to Know Your Access Point	1
1.1 ABOUT THE ORING ACCESS POINT	1
1.2 SOFTWARE FEATURES.....	1
1.3 HARDWARE FEATURES	1
Hardware Installation.....	2
2.1 WALL MOUNTING INSTALLATION.....	2
Hardware Overview.....	3
3.1 FRONT PANEL.....	3
3.2 FRONT PANEL LEDs	5
Cables and Antenna.....	6
4.1 ETHERNET CABLES	6
4.2 100BASE-T(X)/10BASE-T PIN ASSIGNMENTS	6
4.3 WIRELESS ANTENNA	7
Management Interface	8
5.1 EXPLORE TAP-3120-M12	8
5.1.1 AP-Tool software	8
5.2 UPNP EQUIPMENT	9
5.3 CONFIGURATION BY WEB BROWSER	10
5.4 ABOUT WEB-BASED MANAGEMENT	10
5.5 MAIN INTERFACE.....	11
5.5.1 Basic Setting	12
Setting Operation Mode	12
Setting WDS (Bridge Mode).....	13
Setting Wireless.....	16
Client.....	21
LAN Setting	23
Setting DHCP Server	24
5.5.2 Advanced Setting	25
Wireless.....	25
MAC Filter	27



System Event	28
Email Settings.....	29
SNMP Settings	29
Syslog Server Settings.....	30
5.5.3 System Tools.....	30
Administrator	30
Date & Time.....	32
Configuration	33
Firmware Upgrade	34
Miscellaneous	34
5.5.4 System Status	35
System Info.....	35
System Log.....	36
Traffic Statistics.....	36
Wireless Clients	37
5.5.5 Online Help	37
Technical Specifications	38
Appendix A.....	40
How to configure SNMP MIB and use SNMP in the PCs?	40

Getting to Know Your Access Point

1.1 About the ORing Access Point

TAP-3120-M12 is reliable IEEE802.11a/b/g and 802.11b/g WLAN Access Point with 2 LAN ports. It can be configured to operate in Dual AP/Dual Client/Bridge/AP-Client mode. You can configure TAP-3120-M12 by Window Utility or WEB interfaces via LAN port or WLAN interface. TAP-3120-M12 provides dual Ethernet ports in switch mode, so you can use Daisy Chain to reduce the usage of Ethernet switch ports. Therefore TAP-3120-M12 is 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
- Supports AP/Client/Bridge 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

- Redundant Power Inputs: Dual 12~48 VDC on M23 connector
- 10/100Base-T(X) Ethernet port
- Casing: IP-40
- Dimensions(W x D x H): 125mm(W) x 65mm(D) x 196mm(H)
- Weight: 1015 g
- Operating Temperature: -20 to 70°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing

Hardware Installation

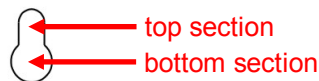
2.1 Wall Mounting Installation

If you wish to mount the TAP-3120-M12 on the wall, please do the following steps:

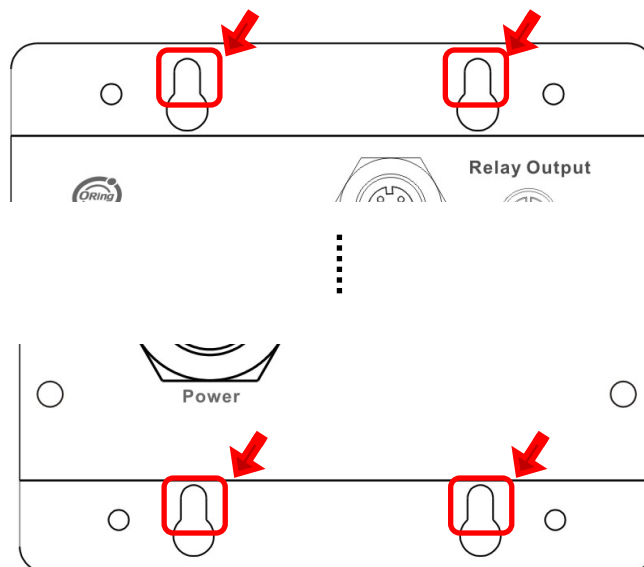
Step 1 Prepare 4 screws (not included in the package) similar to the ones shown below.



The screws should not be too long. The head of each screw should be larger than the width of the top section of the AP's screw hole. If you want absolutely the most secure wall-mount installation of the AP, the head of each screw should be larger than the bottom section of the AP's screw hole. If you wish to later un-mount the AP without loosening of the screws, the head of each screw should just *barely go pass by* the bottom section of the AP's screw hole.



Step 2 Secure the TAP-3120-M12 onto the wall by tightening the 4 screws all the way in so each screw firmly latches on the top section of its corresponding screw hole.



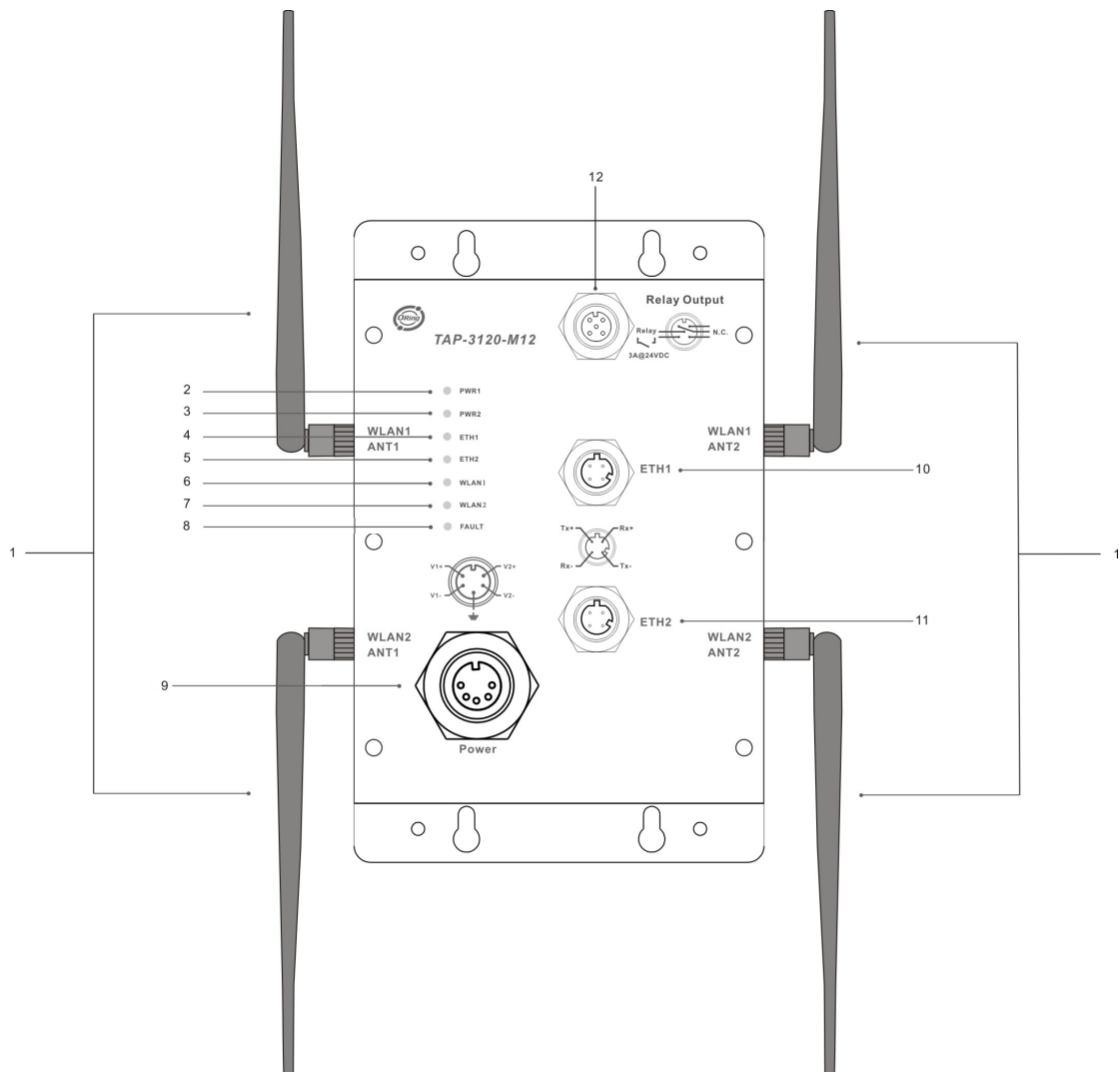
Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the TAP-3120-M12.

Port	Description
10/100 Base-T(X) fast Ethernet ports on M12 connector (D-coding)	2 10/100Base-T(X) fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto
Relay Output on M12 (A-coding) connector	Relay output to carry capacity of 3A at 24VDC
Redundant power inputs on M23 connector	Dual Power Inputs. 12~48 VDC on M23 connector (24 VDC Typ)

TAP-3120-M12



1. 2.4/5.8GHz antenna with typical 3.0 dBi antenna for IEEE 802.11a mode and 2 dBi for IEEE 802.11b/g mode.
2. LED for PWR1 and system status. When the PWR1 links, the green LED will light on.
3. LED for PWR2 and system status. When the PWR2 links, the green LED will light on.
4. LED for Ethernet port 1 (ETH1) status
5. LED for Ethernet port 2 (ETH2) status
6. LED for WLAN1 link status
7. LED for WLAN2 link status
8. LED for Fault Relay. When the fault occurs, the red LED will light on.
9. Power Input port on M23 connector
10. Ethernet port 1 (ETH1) on M12(D-coding) connector

11. Ethernet port 2 (ETH2) on M12(D-coding) connector
12. Relay output on M12(A-coding) connector

3.2 Front Panel LEDs

LED	Color	Status	Description
PWR1	Green/Red	Green On	DC power 1 activated.
		Green blinking	Device been located
		Red blinking	Indicates an IP conflict, or DHCP or BOOTP server did not respond properly
PWR2	Green/Red	Green On	DC power 2 activated.
		Green blinking	Device been located
		Red blinking	Indicates an IP conflict, or DHCP or BOOTP server did not respond properly
ETH1	Amber	On	Port link up at 10Mbps.
		Blinking	Data transmitted.
	Green	On	Port link up at 100Mbps.
		Blinking	Data transmitted.
ETH2	Amber	On	Port link up at 10Mbps.
		Blinking	Data transmitted.
	Green	On	Port link up at 100Mbps.
		Blinking	Data transmitted.
WLAN	Green	On	WLAN1 activated.
		Blinking	WLAN1 Data transmitted.
	Red	On	WLAN2 activated.
		Blinking	WLAN2 Data transmitted.
Fault	Red	On	Fault relay. Power failure or Port down/fail.

Cables and Antenna

4.1 Ethernet Cables

The TAP-3120-M12 WLAN AP has two 10/100Base-T(X) Ethernet ports. According to the link type, the AP uses CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10Base-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	M12(D-codng)
100Base-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	M12(D-coding)

4.2 100Base-T(X)/10Base-T Pin Assignments

With 100Base-T(X)/10Base-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

M12(4-pin, D-coding) Pin Assignments



Pin Number	Assignment
1	RD+
2	TD+
3	RD-
4	TD-

The TAP-3120-M12 supports 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-T(X) MDI and MDI-X port pin outs.

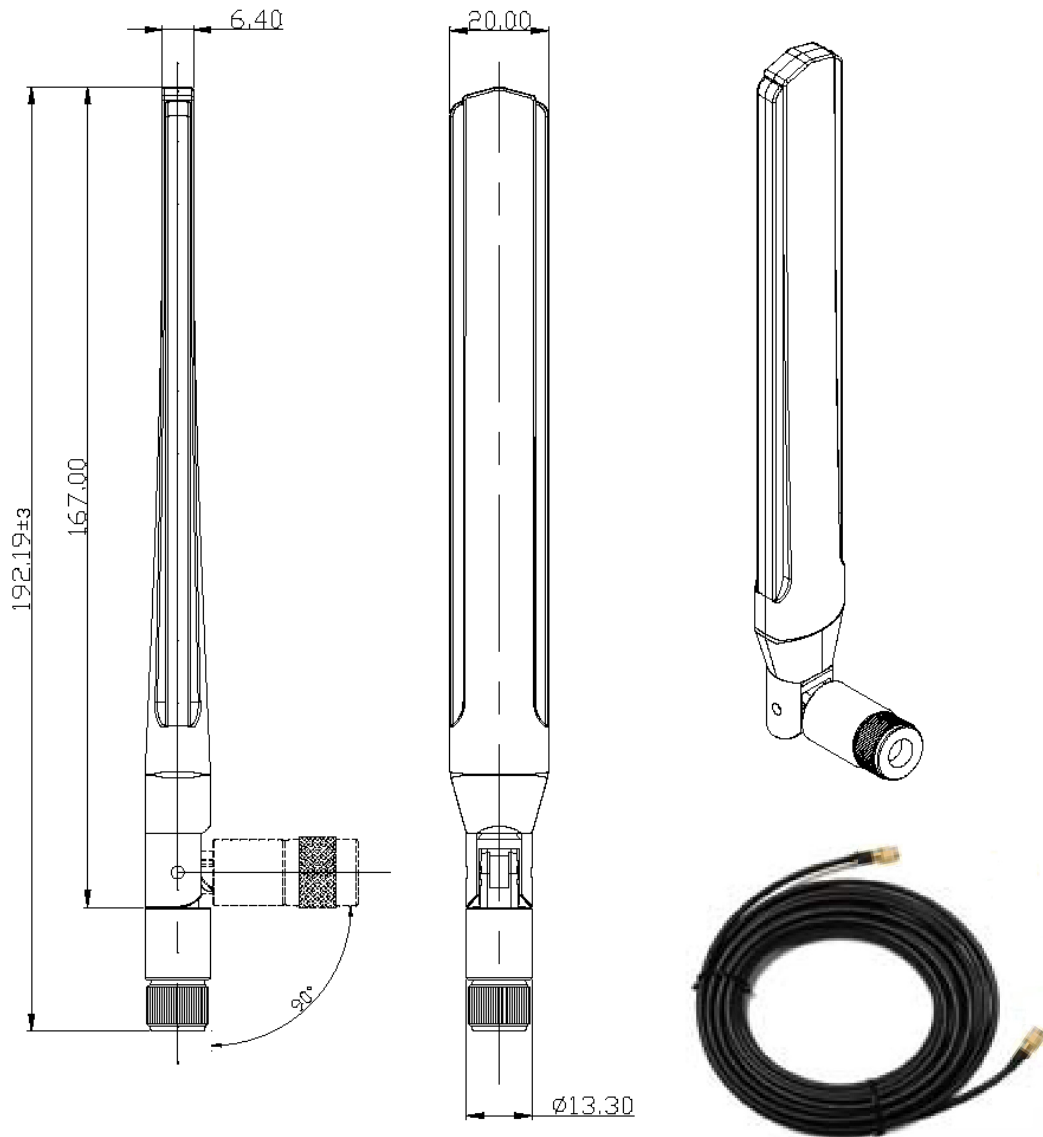
MDI/MDI-X pin assignment

Pin Number	MDI port	MDI-X port
1	RD+(receive)	TD+(transmit)
2	TD+(transmit)	RD+(receive)
3	RD-(receive)	TD-(transmit)
4	TD-(transmit)	RD-(receive)

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

4.3 Wireless Antenna

2.4GHz/5.8GHz antenna is used for TAP-3120-M12 and connected with a reversed SMA connector. External RF cable and antenna also can be applied with this connector.



Management Interface

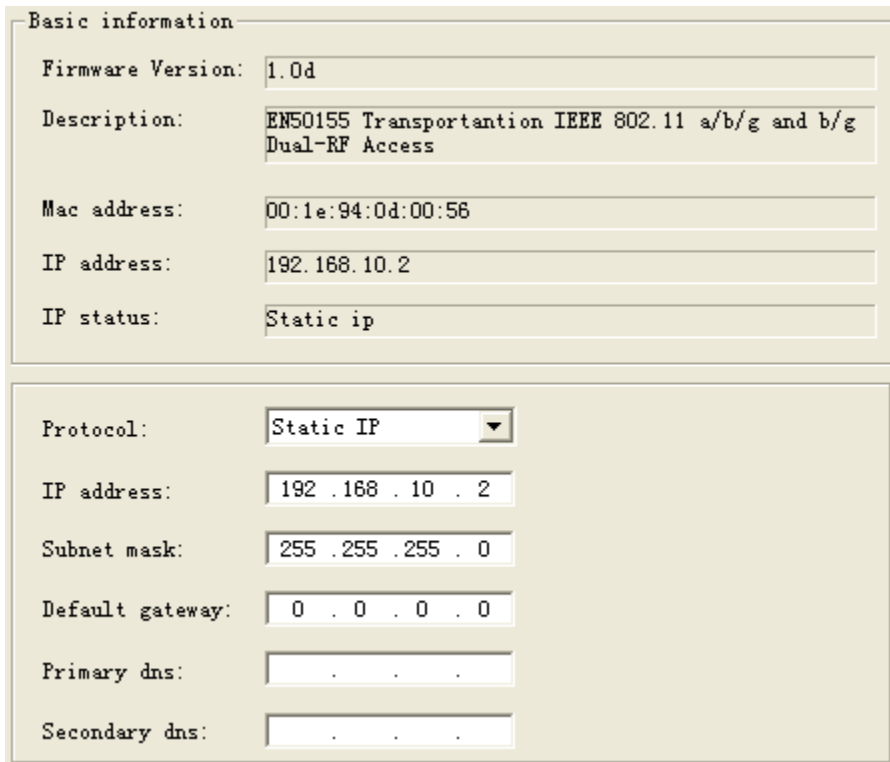
5.1 Explore TAP-3120-M12

5.1.1 AP-Tool software

Each model contains user-friendly software, AP-Tool, to explore TAP-3120-M12 on local area network.

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

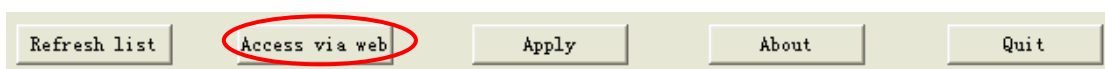
Step 2: Choose your access point, and it will show the AP attribute. Simultaneity, you can manually set the AP's IP address.



The screenshot displays the AP-Tool user interface, divided into two main sections. The top section, titled "Basic information", contains several fields: "Firmware Version" (1.0d), "Description" (EN50155 Transportantion IEEE 802.11 a/b/g and b/g Dual-RF Access), "Mac address" (00:1e:94:0d:00:56), "IP address" (192.168.10.2), and "IP status" (Static ip). The bottom section contains network configuration fields: "Protocol" (Static IP), "IP address" (192.168.10.2), "Subnet mask" (255.255.255.0), "Default gateway" (0.0.0.0), "Primary dns" (.), and "Secondary dns" (.).

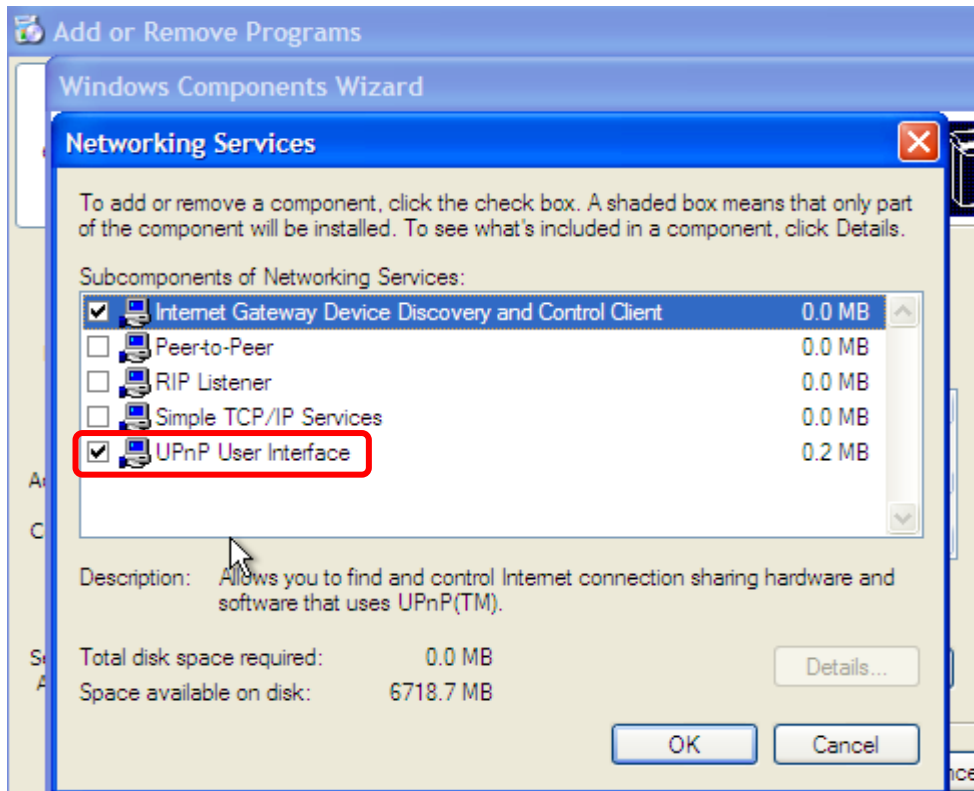
User interface of AP-Tool

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



5.2 UPnP Equipment

Step 1 To check whether the UPnP UI of the computer is connected to the TAP-3120-M12, go to **Control Panel > Add or Remove Programs > Windows Components Wizard > Networking Servers > UPnP User Interface** and enable the UPnP User Interface.

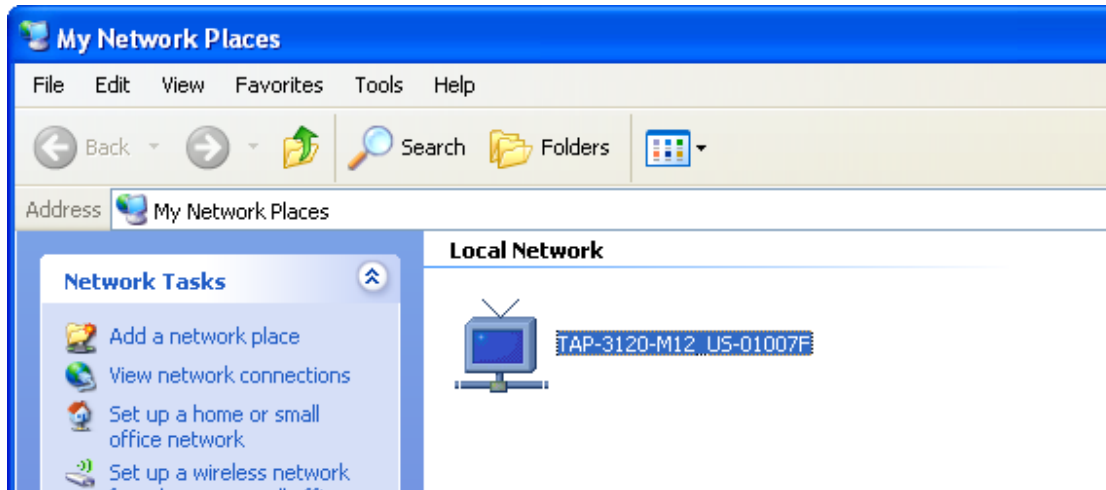


UPnP configuration page

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 To display information of the UPnP equipment, right-click the UPnP equipment and choose "Properties".

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.

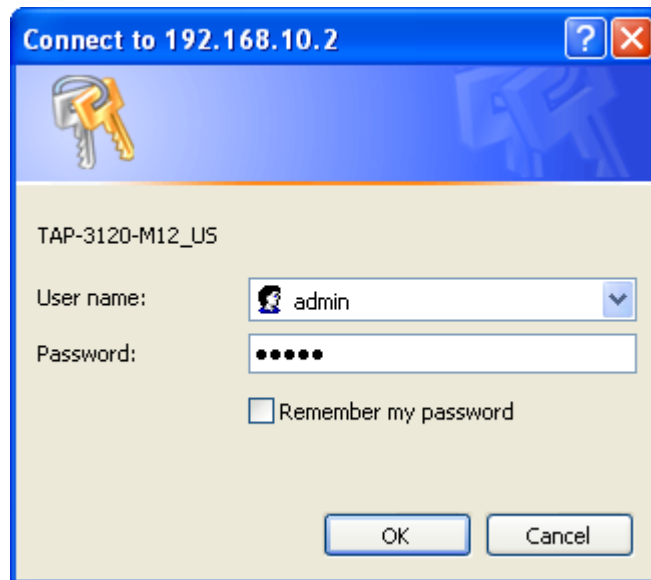
5.4 About Web-Based Management

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 the following dialog window. Enter your user name (**admin**) and your password (**admin**), and then click **OK** to continue.

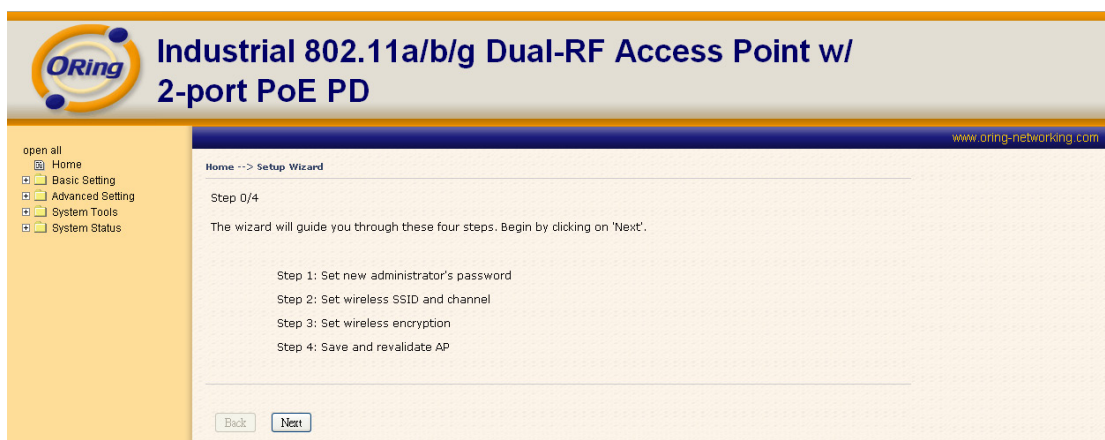


Login screen

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.



Main interface

5.5.1 Basic Setting

Setting Operation Mode

Basic Setting --> Operation Mode

Redundant AP
This mode provides redundant Access Point services for other redundant wireless clients.

Redundant Client
In this mode Dual RF redundant clients can join dual RF redundant APs.

AP-Client
In this mode one RF with AP function services for other wireless clients, and the other RF with client function can connect AP.

Client-AP
In this mode one RF with client function can connect the other AP, and the other with AP function provides Access Point services for other wireless clients.

Bridge
This mode provides Static dual LAN-to-LAN Bridging functionality. The static dual LAN-to-LAN bridging function is supported through Wireless Distribution System(WDS).

Operation mode interface

The following table describes the labels in this screen.

Label	Description
Redundant AP	This mode provides redundant Access Point services for other redundant wireless clients.
Redundant Client	In this mode Dual RF redundant clients can join dual RF redundant APs.
AP-Client	In this mode one RF with AP function services for other wireless clients, and the other RF with client function can connect AP.
Client-AP	In this mode one RF with client function can connect the other AP, and the other with AP function provides Access Point services for other wireless clients.
Bridge	This mode provides Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).

In each mode, the TAP-3120-M12 forwards packet between its Ethernet interface and wireless interface for wired hosts on the Ethernet side, and wireless hosts on the wireless side.

Setting WDS (Bridge Mode)

Basic Setting --> WLAN1 WDS

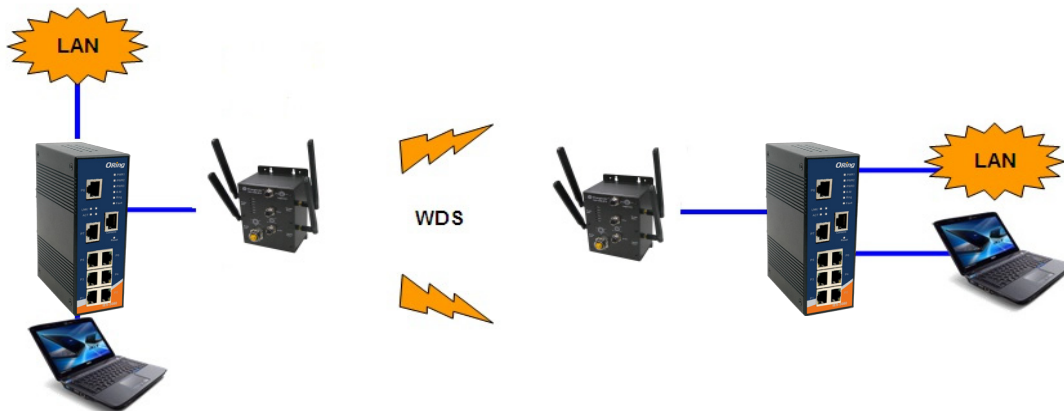
Operation mode of the AP should be set to "Bridge" mode before these settings changed.

WDS Mode:

Peer Mac Address: Enabled

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-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).
Peer MAC Address	Set the Mac address of other access point(s). Simultaneously, choose "Enabled".

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.
4. Each AP should have the same setting except 'Peer Mac Address' set to the other's Mac address
5. At wireless web setting Security and Channel should be the same,
6. AP's distance should be limited within a certainty area.

WDS – Restricted Mode

Basic Setting --> WLAN1 WDS

Operation mode of the AP should be set to "Bridge" mode before these settings changed.

WDS Mode:

Peer Mac Address: Enabled

Fill in the wireless MAC address of AP that you want to connect.

WDS –Bridge Mode

Basic Setting --> WLAN1 WDS

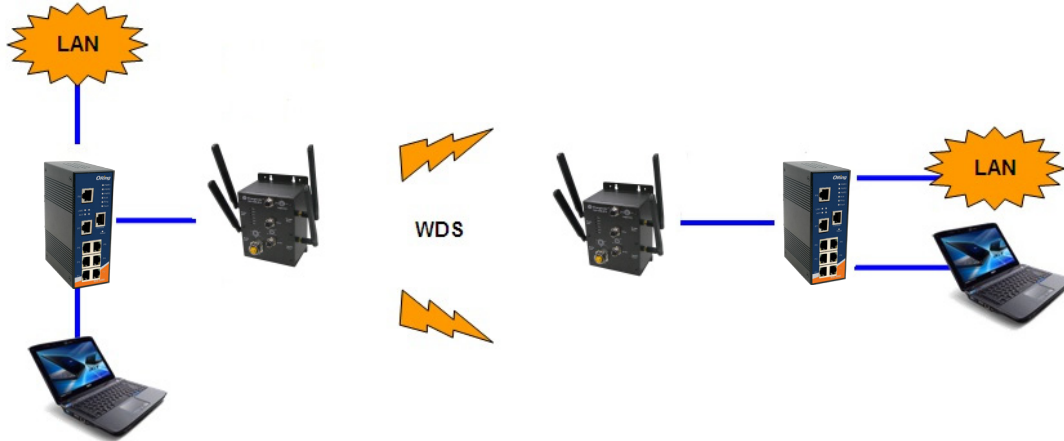
Operation mode of the AP should be set to "Bridge" mode before these settings changed.

WDS Mode:

Peer Mac Address: Enabled

Fill in the wireless MAC address of AP that you want to connect.

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

Basic Setting --> WLAN1 WDS

Operation mode of the AP should be set to "Bridge" mode before these settings changed.

WDS Mode: Repeater Mode ▾

Peer Mac Address: Enabled

Apply Cancel

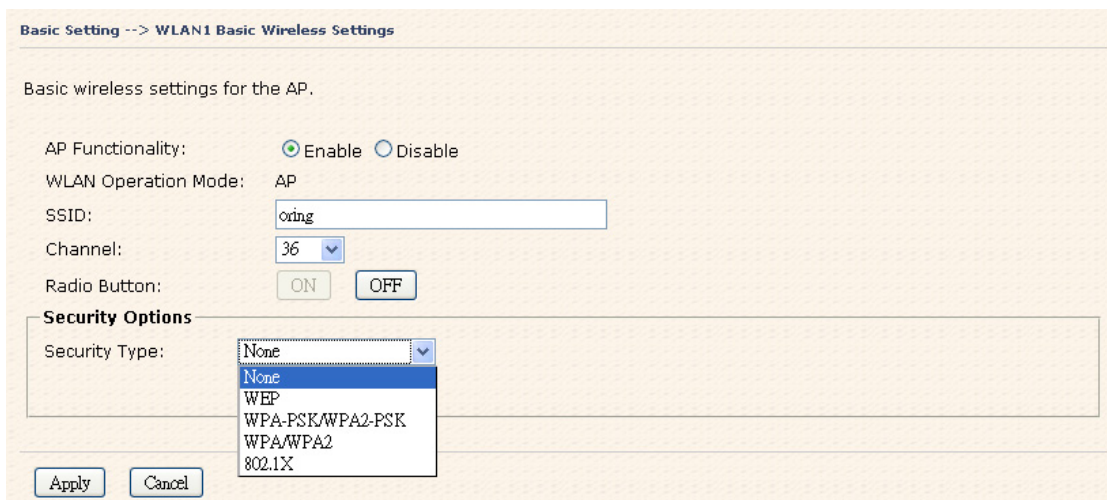
Fill in the wireless MAC address of AP that you want to connect.

The working principle of **Repeater Mode** as follows:



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



The following table describes the labels in this screen.

Label	Description
SSID	Service Set Identifier Default is the default setting. The SSID is a unique name that identifies a network. All devices on the 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	Channel 6 is the default channel, input a new number if you want

	to change the default setting. All devices on the network must be set to the same channel to communicate on the network.
Security options	<p>Select the type of security for your wireless network at Security Type:</p> <p>None: Select for no security.</p> <p>WEP: Select for security WEP.</p> <p>WPA-PSK/WPA2-PSK: Select for security WPA-PSK or WPA2-PSK without a RADIUS server.</p> <p>WPA/WPA2: Select for WPA or WPA2 (Wi-Fi Protected Access) authentication in conjunction with a RADIUS server.</p> <p>802.1x: Authentication through RADIUS server</p>

Security Type – None

No security protection on your wireless LAN access.

Security Type – WEP

Basic Setting --> WLAN1 Basic Wireless Settings

Basic wireless settings for the AP.

AP Functionality: Enable Disable

WLAN Operation Mode: AP

SSID:

Channel:

Radio Button:

Security Options

Security Type: WEP

Auth Mode: Open Shared WEPAUTO

WEP Encryption:

Key Type:

Default Key Index:

KEY1:

KEY2:

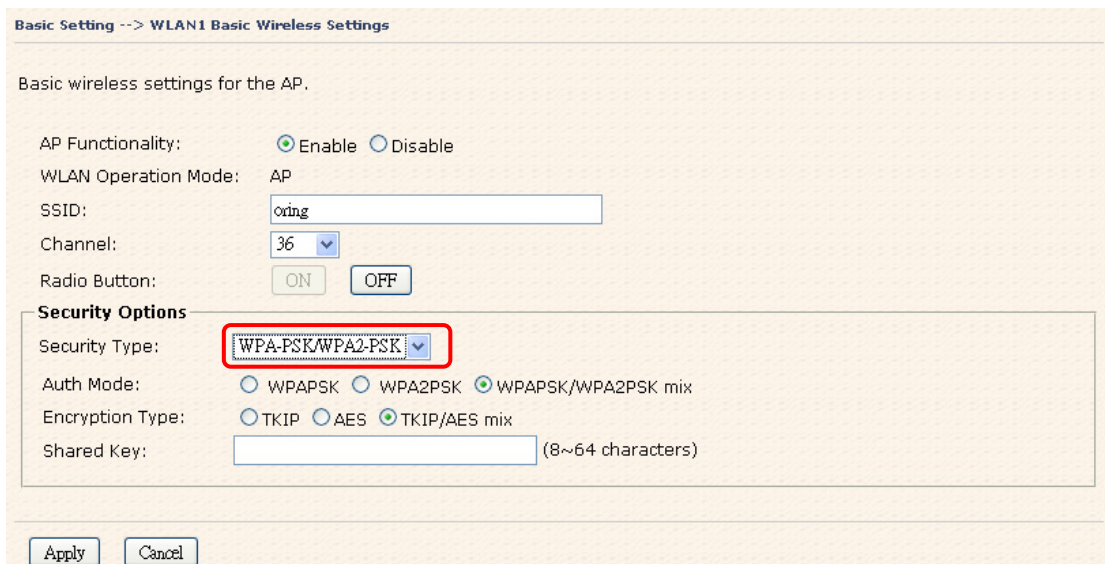
KEY3:

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



Basic Setting --> WLAN1 Basic Wireless Settings

Basic wireless settings for the AP.

AP Functionality: Enable Disable

WLAN Operation Mode: AP

SSID:

Channel:

Radio Button:

Security Options

Security Type:

Auth Mode: WPAPSK WPA2PSK WPAPSK/WPA2PSK mix

Encryption Type: TKIP AES TKIP/AES mix

Shared Key: (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

Basic Setting --> WLAN1 Basic Wireless Settings

Basic wireless settings for the AP.

AP Functionality: Enable Disable

WLAN Operation Mode: AP

SSID:

Channel:

Radio Button:

Security Options

Security Type:

Auth Mode: WPA WPA2 WPA/WPA2 mix

Encryption Type: TKIP AES TKIP/AES mix

Radius Server IP: . . .

Radius Port:

Shared Secret:

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.

Security Type – 802.1x

Basic Setting --> WLAN1 Basic Wireless Settings

Basic wireless settings for the AP.

AP Functionality: Enable Disable

WLAN Operation Mode: AP

SSID:

Channel:

Radio Button:

Security Options

Security Type:

WEP Encryption:

Key Type:

Default Key Index:

KEY1:

KEY2:

KEY3:

KEY4:

Radius Server IP: . . .

Radius Port:

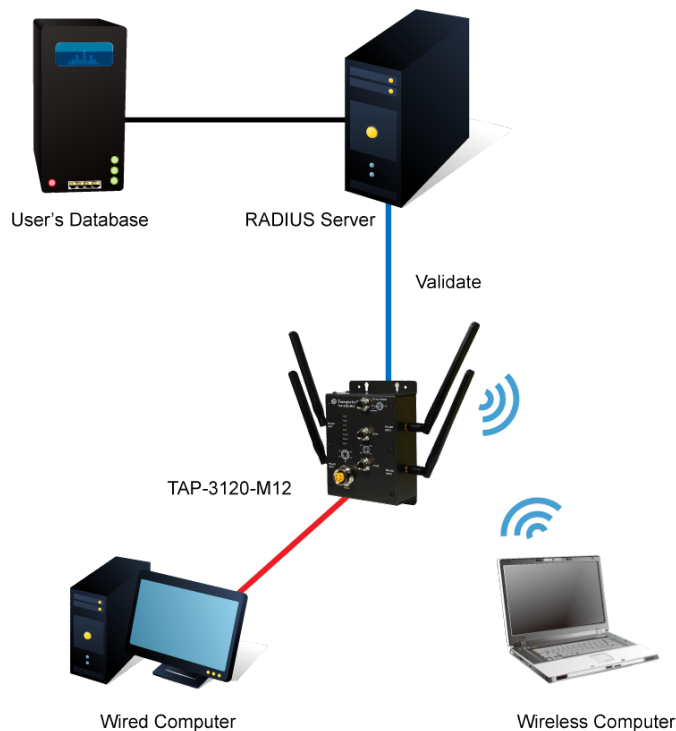
Shared Secret:

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

RADIUS (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.

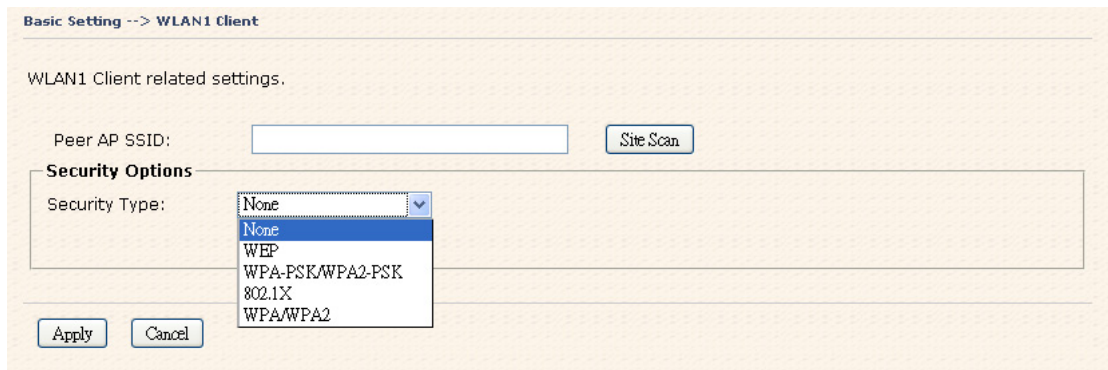
RADIUS server validates your proof and also carries on the authorization. For example, the RADIUS server receives ISA server's response, which points out that the customer carries unauthorized proof; then the RADIUS server would not grant you to carry. Even if the proof has already passed an identify 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 as below:

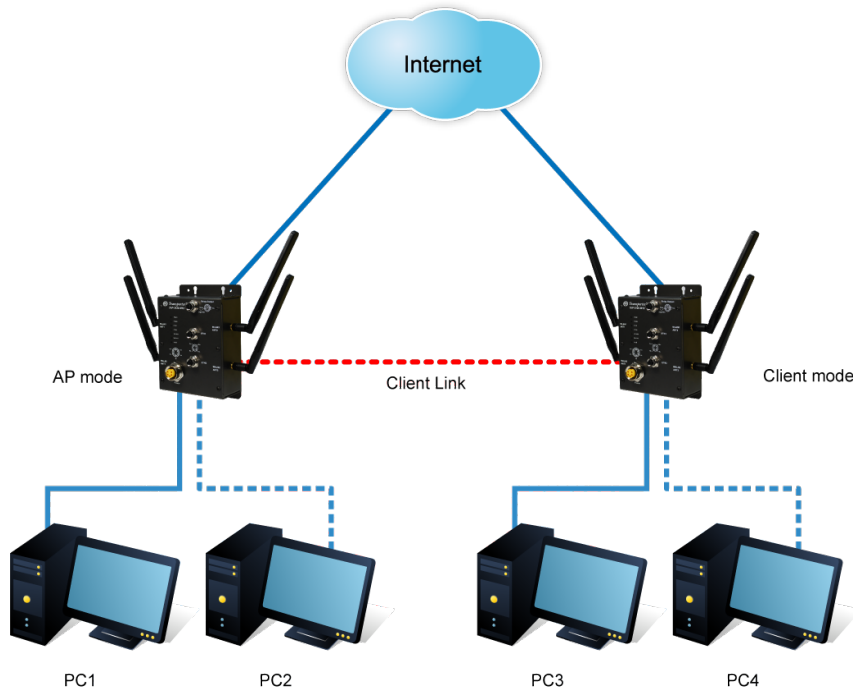


Client

The **Basic setting**—> **Client** page is mainly for setting the client's SSID and Security Options to connect to the other AP. In this mode, the Security Type should be the same with the AP Server.



The principle of the AP-Client/Client mode shows in the following pictures:



Result: ↵

1. PC1, PC2 can visit PC3, PC4 and AP Client
2. PC3, PC4 can visit PC1, PC2 and AP
3. AP Client can visit AP

The following table describes the labels in this screen.

Label	Description
Peer AP SSID	Enter the other AP which used for AP mode.
Site Scan	You can scan the APs which used for AP mode in the certainty area.
Security Type	Set the same security with the AP which you want to connect.

LAN Setting

The **Basic Setting > LAN Setting** page is mainly for setting IP address of 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).

Basic Setting --> LAN Setting

LAN settings of AP.

Obtain an IP address automatically
 Use the following IP address

IP Address: . . .
 Subnet Mask: . . .
 Default Gateway: . . .

Obtain DNS server address automatically
 Use the following DNS server addresses

Preferred DNS: . . .
 Alternate DNS: . . .

Device Name:

Ethernet Mode: Redundant Switch
 STP/RSTP: Enable Disable
 LLDP Protocol: Enable Disable

The following table describes the labels in this screen.

Label	Description
Obtain an IP address automatically	Select this option if you would like to obtain an IP address automatically assigned by DHCP server in your network
Use the following IP address	<p>Select this option if you are manually assigning an IP address.</p> <p>IP Address: There is a default IP address in the AP, and you can input a new IP address.</p> <p>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.</p> <p>Default Gateway: Enter the IP address of the router in your network.</p>
Obtain DNS server address automatically	This option is selected by DHCP server.

<p>Use the following DNS server addresses</p>	<p>This option is selected by manually set.</p> <p>Preferred DNS: There is a default DNS server, and you can input another new DNS server.</p> <p>Alternate DNS: There is a default DNS server, and you can input another new DNS server.</p>
--	---

Setting DHCP Server

Basic Setting --> DHCP Server

The AP can be setup as a DHCP server to distribute IP addresses to the WLAN network.

DHCP Server Enabled Disabled

Options

Starting IP address: . . .

Maximum Number of IPs:

Lease Time: hours

DHCP Clients List:

Hostname	Mac Address	IP Address	Expires In

The following table describes the labels in this screen.

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 IPs	The dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 100 will be entering 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 TAP-3120-M12.

5.5.2 Advanced Setting Wireless

Basic Setting --> WLAN1 Advanced Wireless Setting

Wireless performance tuning.

Beacon Interval: (msec, range:20~999, default:100)

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

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

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

Max Client Threshold: (range: 1~64, default 10)

Xmit Power: % (range: 1~100, default:100)

Wireless Mode: BG Mixed Mode B Mode A Mode G Mode

Transmission Rate: ▼

Preamble: Long Short

SSID Broadcast: Enabled Disabled

Extra parameters for Client Mode:

Fast Roaming: Disabled Standard Fixed Channel

Signal Threshold for Roaming dbm(range: 60~90, default 75)

The following table describes the labels in this screen.

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 Threshold	This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the



	Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The AP sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
Xmit Power	This value ranges from 1 - 100 percent, default value is 100 percent.
Wireless Network Mode	If you have Wireless-G and 802.11b devices in your network, then 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. If you would like to use 802.11a devices then select A only 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.
X-Roaming	Disable: Disable X-Roaming protocol. Standard: Roaming group does not require the same wireless channel, but slower to switch than the "fixed channel" mode

	Fixed channel: Roaming group must be required the same wireless channel, but faster to switch than the “Standard” mode
Signal Threshold for Roaming	Roaming signal threshold setting. When signal below this value AP will roaming to another client target which the same SSID, security option and signal strongest within the environment.(This value just effect on client-mode equipment)
Max Client Threshold	Max number of client equipment setting. When client number over this value AP will reject roaming equipment connection.(This value just effect on AP-mode equipment)

MAC Filter

Use **Advanced Setting > MAC Filters** to allow or deny wireless clients, by their MAC addresses, from accessing the TAP-3120-M12. You can manually add a MAC address or select the MAC address from **Connected Clients** that are currently connected to the AP.

Advanced Setting --> MAC Filters

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

MAC Filters: Enabled Disabled

Options

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

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

Associated Clients: Copy To

MAC Filter Table:

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

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 Configuration.

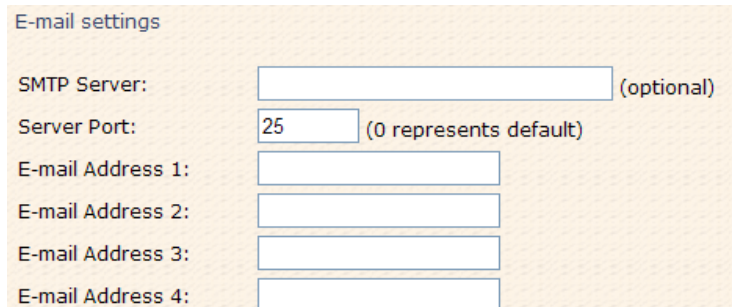
Device Event Notification				
Hardware Reset (Cold Start)	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Software Reset (Warm Start)	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Login Failed	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
IP Address Changed	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Password Changed	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Redundant Power Changed	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Eth Link Status Changed	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
SNMP Access Failed	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Wireless1 Client Associated	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Wireless2 Client Associated	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Wireless1 Client Disassociated	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Wireless2 Client Disassociated	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Client1 Mode Associated	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Client2 Mode Associated	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Client1 Mode Disassociated	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	
Client2 Mode Disassociated	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	

Fault Event Notification and Fault LED/Relay				
Power 1 Fault	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	<input type="checkbox"/> Fault LED/Relay
Power 2 Fault	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	<input type="checkbox"/> Fault LED/Relay
Eth1 Link Down	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	<input type="checkbox"/> Fault LED/Relay
Eth2 Link Down	<input type="checkbox"/> SMTP Mail	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog	<input type="checkbox"/> Fault LED/Relay

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: (0 represents default)

E-mail Address 1:

E-mail Address 2:

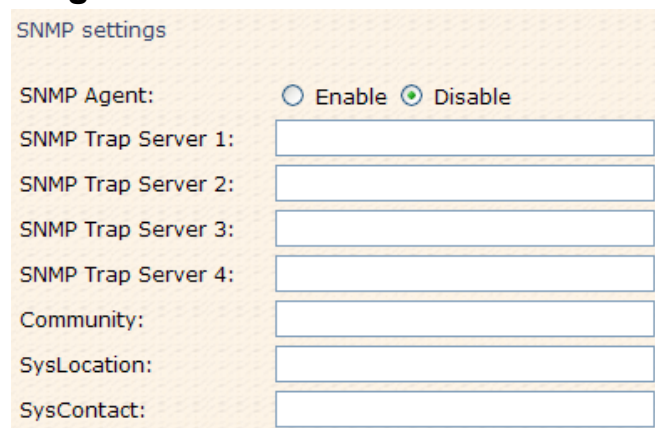
E-mail Address 3:

E-mail Address 4:

The following table describes the labels in this screen.

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

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 1-4	Specify the IP of trap server, which is the address to which it will send traps AP generates.
Community	Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-write community.
SysLocation	Specify sysLocation string.
SysContact	Specify sysContact string.

Syslog Server Settings

Syslog Server settings

Syslog Server IP:

Syslog Server Port: (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 --> Administrator

Modify web administrator's name and password.

Old Name:

Old Password:

New Name:

New Password:

Confirm New Password:

Web Protocol: HTTP HTTPS

Port:

Web Access Control: Wired Wireless

UPnP: Enable Disable

The following table describes the labels in this screen.

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 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 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 --> Date/Time

Date/Time settings.

Local Date: Year Month Day

Local Time: Hour Minute Second

Time Zone:

NTP: Enable

NTP Server 1:

NTP Server 2: (optional)

Synchronise: at :

The following table describes the labels in this screen.

Label	Description
Local Date	Set local date manually.
Local Time	Set local time manually.
Time Zone	Select the time zone manually
Get Current Date &	Click this button to 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

Restore a previously saved configuration

Use the button below to restore the default settings

The following table describes the labels in this screen.

Label	Description
Download configuration	The current system settings can be saved as a file onto the local 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 Settings	You may also reset the TAP-3120-M12 back to factory 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!

Current Firmware Version: 1.0b

瀏覽...

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 information details.

Model

Model Name: TAP-3120-M12
Model Description: Industrial 802.11a/b/g Dual-RF Access Point w/ 2-port PoE PD

Firmware

Version: 1.0b

Ethernet

MAC Address: 00:1E:94:0A:00:13
IP Address: 192.168.10.2
Subnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0
DHCP Server: Disabled

Operation Mode

Operation Mode: Redundant AP

Wireless 1

MAC Address: 00:0E:8E:28:7C:84
SSID: oring
Encryption: No encryption
Signal Strength: ----
Channel: 36
WDS MAC Address:
Peer AP SSID:
Client MAC Address:
Client Encryption: No encryption
Client Connection Info:

Wireless 2

MAC Address: 00:0E:8E:30:AD:1C
SSID: oring_1
Encryption: No encryption
Signal Strength: ----
Channel: 6
WDS MAC Address: 00:0E:8E:30:AD:1C
Peer AP SSID:
Client MAC Address:
Client Encryption: No encryption
Client Connection Info:

Device Time

Current Time: Thu, 01 Jan 2009 00:47:04 +0800

This page displays the current information for the TAP-3120-M12. It will display model name, as well as firmware version, Ethernet, Wireless info and device time.

System Log

System Status --> System Log

System log details.

#	Date Time	Content
---	-----------	---------

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

System Status --> Traffic/Port Status

Traffic status displays received and transmitted packets passing through the AP.

Interface	Send	Receive
Ethernet	542859 Bytes (2162 Packages)	82503 Bytes (651 Packages)
Wireless	80734 Bytes (1914 Packages)	56705 Bytes (682 Packages)

Port status displays the state of all ports in AP.

Port	State
Ethernet Port1	Link up, forwarding
Ethernet Port2	Link down, forwarding
Wireless1 AP Port	forwarding
Wireless2 AP Port	forwarding
Wireless1 Client Port	Not Set
Wireless2 Client Port	Not Set

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

System Status --> Wireless Clients

Wireless1: List of connected wireless clients.

Mac Address	Send	Receive	Current TxRate
-------------	------	---------	----------------

Wireless2: List of connected wireless clients.

Mac Address	Send	Receive	Current TxRate
-------------	------	---------	----------------

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
<p>Home</p> <ul style="list-style-type: none"> ■ Setup Wizard <hr/> <p>Basic Setting</p> <ul style="list-style-type: none"> ■ Operation Mode ■ WDS ■ Wireless ■ LAN Setting ■ DHCP Server <hr/> <p>Advanced Setting</p> <ul style="list-style-type: none"> ■ Wireless ■ MAC Filter ■ Email/SNMP/Syslog ■ System Event <hr/> <p>System Tools</p> <ul style="list-style-type: none"> ■ Administrator ■ Date & Time ■ Configuration ■ Firmware Upgrade ■ Miscellaneous <hr/> <p>System Status</p> <ul style="list-style-type: none"> ■ System Info ■ System Log ■ Traffic Stats ■ Wireless Clients 	<p>Setup Wizard</p> <p>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 the settings of the AP. The Setup Wizard is a helpful guide for first time users to the AP.</p> <p>For step 1, you can set a new login password if required, the default login name is 'admin', and default login password is null.</p> <p>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.</p> <p>For step 3, set the wireless encryption to WEP will strengthen the security of the wireless network, or just leave encryption disabled and anyone can connect to the AP.</p> <p>For step 4, save the previous settings and revalidate the AP.</p>

Technical Specifications

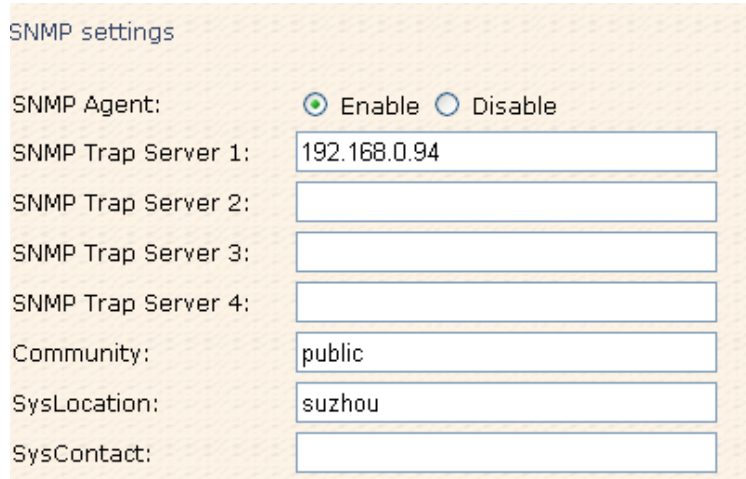
LAN Interface	
Ethernet Ports in M12 connector (4-pin, D-coding)	2 x 10/100Base-T(X), Auto MDI/MDI-X
Protocols	IP, TCP, UDP, DHCP, BOOTP, ARP/RARP, DNS, SNMP MIB II, HTTPS, SNMPV1/V2, Trap, Private MIB
WLAN Interface	
Operating Mode	Dual AP/Dual Client /Bridge/ AP-Client
Antenna and Connector	4 antennas with 3dBi for IEEE802.11a and 2dBi for IEEE802.1b/g in reverse SMA connector
Radio Frequency Type	DSSS, OFDM
Modulation	IEEE802.11a: OFDM with BPSK, QPSK, 16QAM, 64QAM 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 5.825 GHz (13 channels) Europe CE / ETSI: 2.412~2.472 GHz (13 channels) 5.15 to 5.724 GHz (19 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: 20dBm
Receiver Sensitivity	802.11a: -77dBm±2.0dB @ 54Mbps, PER< 10% 802.11b: -86dBm±1.5dB @ 11Mbps, PER< 8%; 802.11g: -78dBm±1.5dB @ 54Mbps, PER< 10%
Encryption Security	WEP: (64-bit, 128-bit key supported) WPA/WPA2:802.11i (WEP and AES encryption) WPA-PSK (256-bit key pre-shared key supported) TKIP encryption
Wireless Security	SSID broadcast disable
LED Indicators	PWR 1(2) / Ready: 1) Red Blinking: Indicates an IP conflict, or DHCP or BOOTP server did not respond properly.

	<p>2) Green On: Power is on and functioning normally.</p> <p>ETH1(2) Link / ACT:</p> <p>Orange ON/Blinking: 10 Mbps Ethernet</p> <p>Green ON/Blinking: 100 Mbps Ethernet</p> <p>WLAN Link/ACT: Green for WLAN 1 and Red for WLAN 2</p> <p>Fault indicator:</p> <p>Red On: Ethernet link down or power down</p>
Power Requirements	
Power Input Voltage	Dual power inputs PWR1/2: 12 ~ 48VDC in M23 connector
Reverse Polarity Protection	Present
Power Consumption	8.3 Watts
Environmental	
Operating Temperature	-20 to 70°C
Storage Temperature	-40 to 85°C
Operating Humidity	5% to 95%, non-condensing
Physical Characteristics	
Dimensions (W x D x H)	125mm(W) x 65mm(D) x 196mm(H)
Weight	1015 g
Casing	IP-40 protection
Regulatory Approvals	
EMI	FCC Part 15, CISPR (EN55022) class A, EN50155 (EN50121-3-2)
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27, EN61373
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6, EN61373
Rail Traffic	EN50155
Cooling	EN60068-2-1
Dry Heat	EN60068-2-2
Safety	EN60950-1

APPENDIX A

How to configure SNMP MIB and use SNMP in the PCs?

Step 1 Set Enable about the SNMP in the web of Advanced Setting→Email/SNMP/Syslog, and input the IP address of the PC used for SNMP trap server.

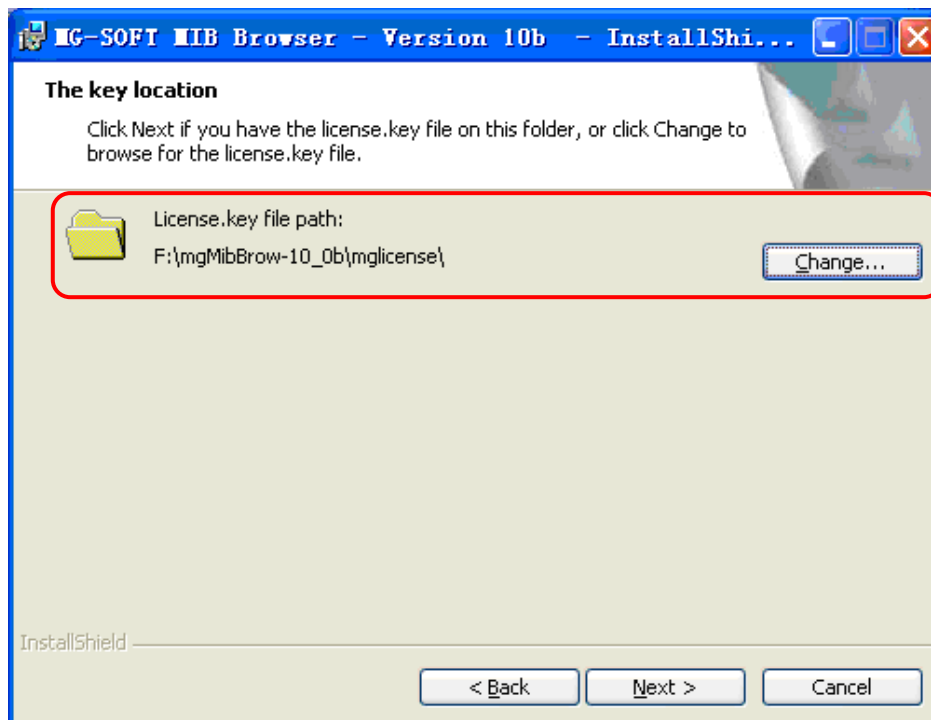


SNMP settings

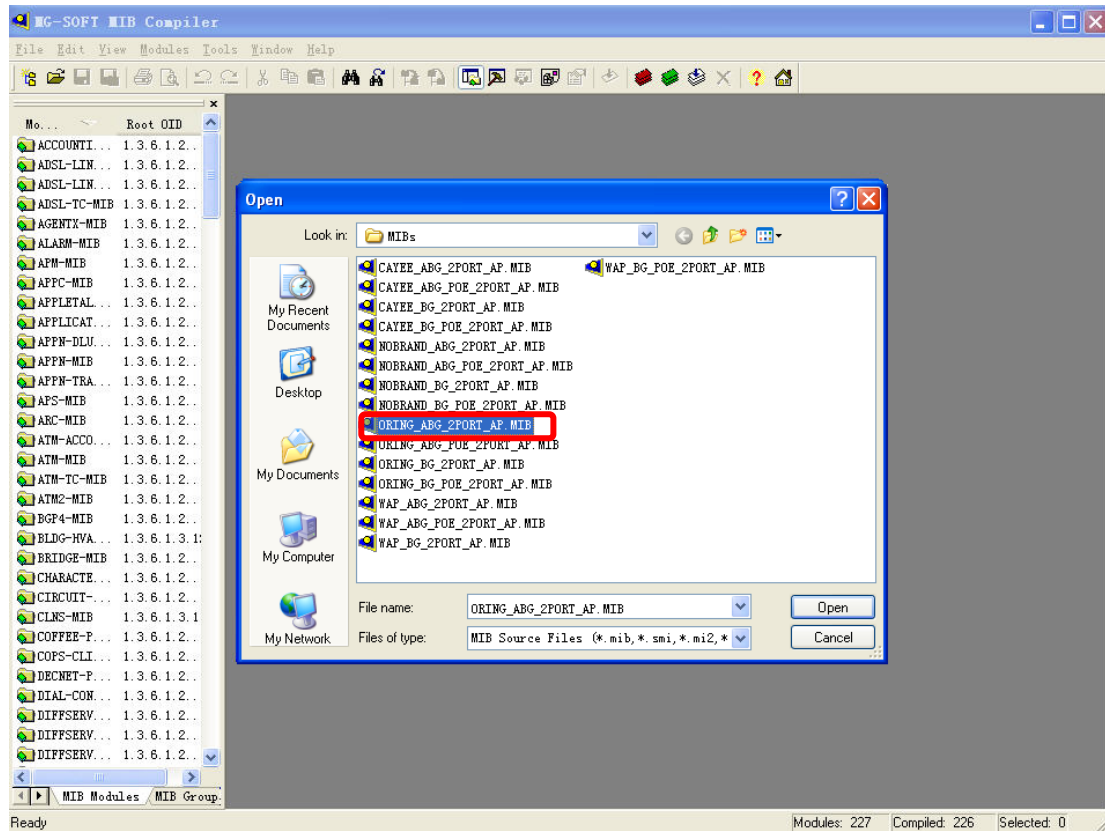
SNMP Agent:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SNMP Trap Server 1:	<input type="text" value="192.168.0.94"/>
SNMP Trap Server 2:	<input type="text"/>
SNMP Trap Server 3:	<input type="text"/>
SNMP Trap Server 4:	<input type="text"/>
Community:	<input type="text" value="public"/>
SysLocation:	<input type="text" value="suzhou"/>
SysContact:	<input type="text"/>

Step 2 In the PC, you should setup the SNMP trap server. Here we use MG-SOFT for example.

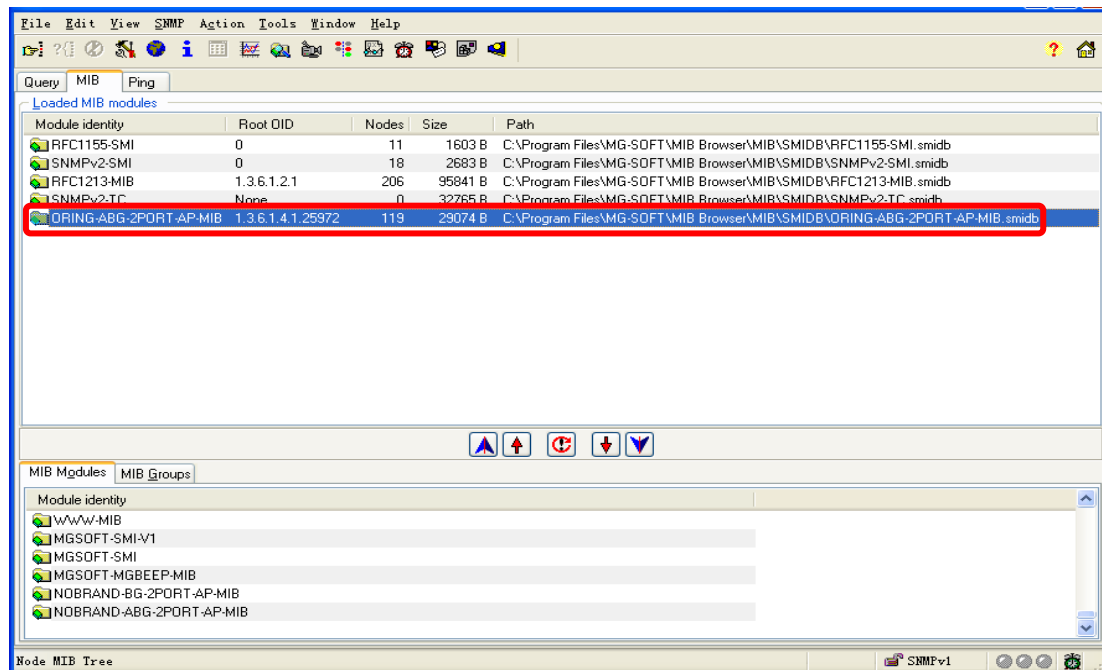
1. The location of the License should configure right during the process of the installation.



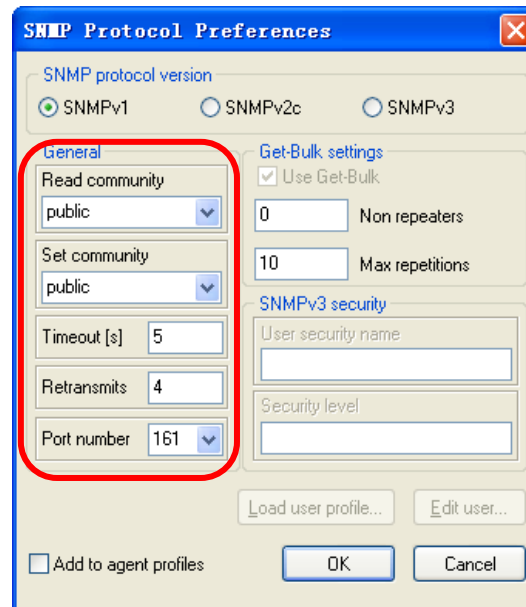
- After the installation, click into MIB Compile to add the MIB files (for example, the ORing 802.11a/b/g and no PoE FW), and save the configuration.



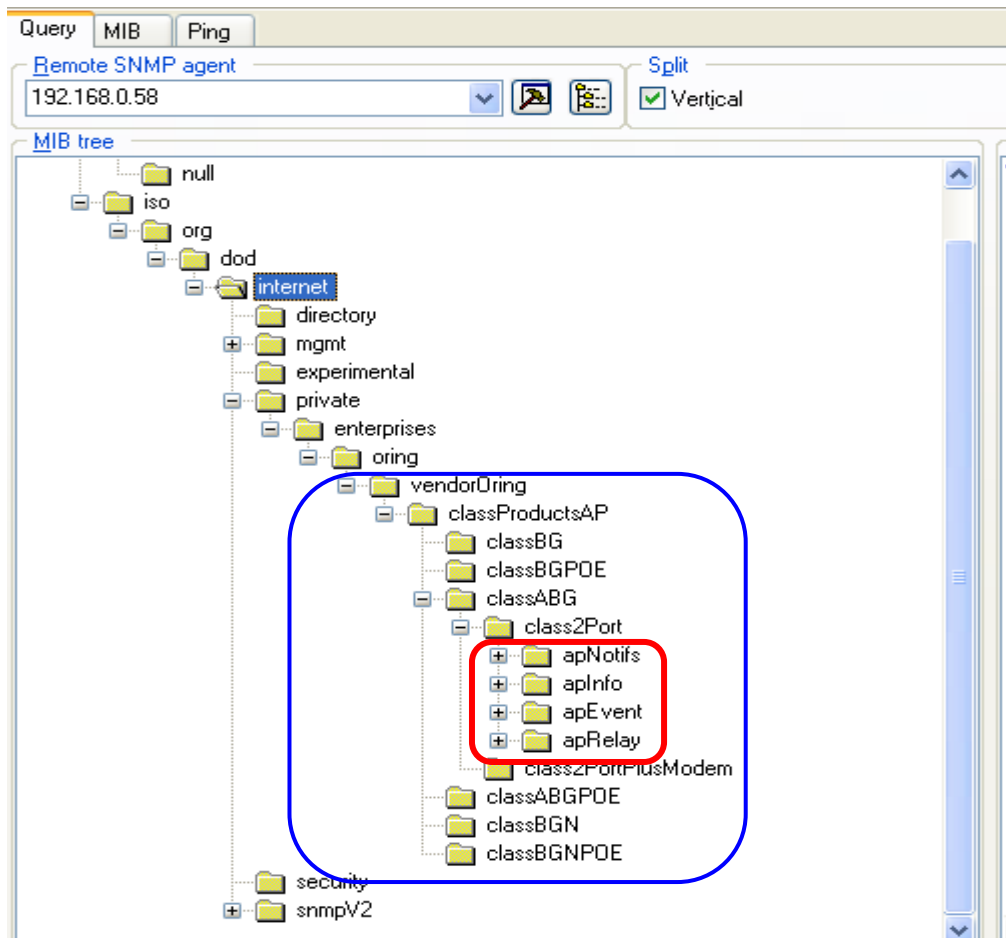
- Open MIB Brower and select the list of MIB; then select the **ORING-ABG-2PORT-AP-MIB** in the MIB Modules to add in the Loaded MIB modules.



- Click into Query list in the MIB Brower, and input the IP address of the AP in the Remote SNMP agent→ click “Apply”, there is an alarm box which let you enter the right community.

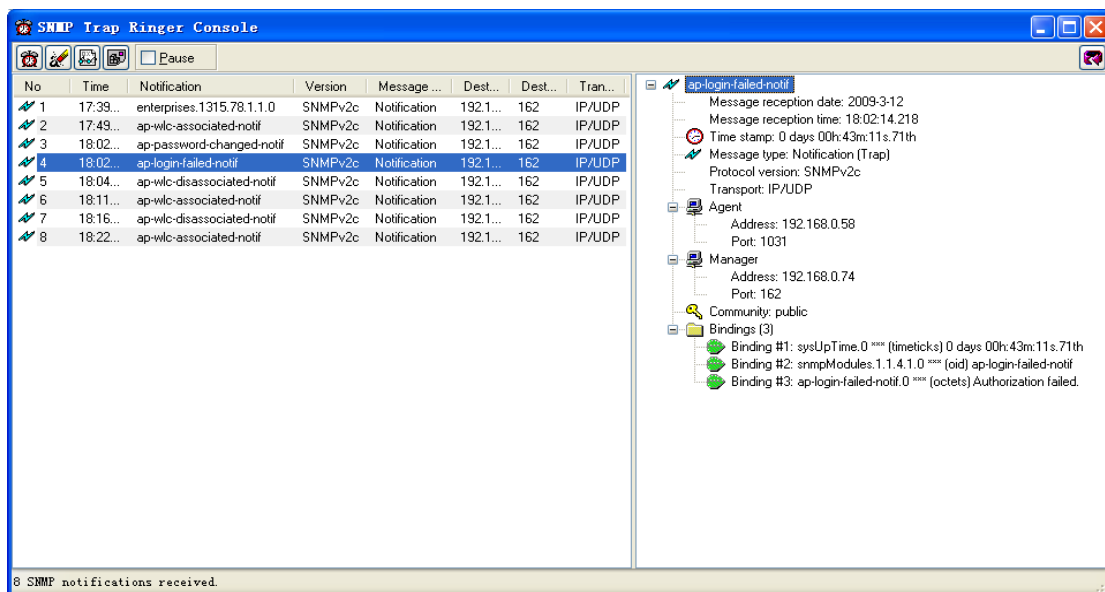


- After all the settings, you can see the information about the ORing AP in the MIB Tree.



Step 3 Be familiar with SNMP information

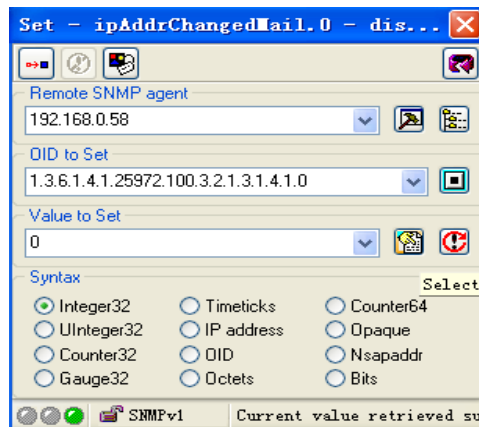
1. The **apNotifs** list will show the trap box. To modify password as an example → select the SNMP Trap option in the **Advanced Setting** → **System Event** page → modify the password in the page of Administrator → it will be have trap box in the SNMP.



- The **apInfo** shows the basic information of the AP. To *apSignalStrengthInfo* as an example, right-click and select "Get" on access to the Signal Strength information.

Shown in SNMP	Shown in the web page
Response binding: 1: apSignalStrengthInfo.0 (octet string) 100 [31.30.30 (hex)]	Signal Strength: 100%

- The **apEvent** shows the same content with the page of the System Event and you can also configure the options. For example: to *PAddrChangedMail* in the *ipAddrChanged* → now status is in 'selected' and the SNMP value is 1 → Set the SNMP value to 0, and then the web page will be not selected.



- To get relevant information, you can right-click "Properties" to view specific property features.