



# TGAP-620(+)-/6620(+)-M12 Series IEEE 802.11 a/b/g/n Access Point with

# Single/Dual RF

# **User Manual**

Version 2.0 June, 2014

www.oring-networking.com

**ORing Industrial Networking Corp.** 



# **COPYRIGHT NOTICE**

Copyright © 2014 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

**ORing** is a registered trademark of ORing Industrial Networking Corp. All other trademarks belong to their respective owners.

## **REGULATORY COMPLIANCE STATEMENT**

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

# WARRANTY

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

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

# DISCLAIMER

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

## **CONTACT INFORMATION**

#### **ORing Industrial Networking Corp.**

3F., No.542-2, 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: <a href="mailto:support@oring-networking.com">support@oring-networking.com</a>

#### Sales Contact

E-mail: <u>sales@oring-networking.com</u> (Headquarters) <u>sales@oring-networking.com.cn</u> (China)



# **Table of Content**

Gettir	ng Started	4
1.1	About the TGAP-620(+)-/6620(+)-M12 Series	4
1.2	Software Features	4
1.3	Hardware Features	4
Hardy	ware Overview	5
2.1	Front Panel	5
2.1.1	1 Ports and Connectors	5
2.1.2	2 Front Panel LEDs	7
2.2	Side Panel	7
Hardy	ware Installation	8
3.1	Wall Mounting Installation	8
3.2	Wiring	9
3.2.1	1 Grounding	9
3.2.2	2 Power Port Pinouts	9
3.2.3	3 Relay Output Port Pinouts	
Cable	es and Antenna	11
4.1	Ethernet Pin Definition	11
4.2	Console Port Pin Definition	11
4.3	DI/DO	
4.4	Wireless Antenna	
Mana	agement	13
5.1	Network Connection	
5.2	Open-Vision Configuration	
5.3	UPnP Equipment	14
5.4	Web Browser Management	15
5.5	Configurations	16
	5.5.1 Overview	16
	5.5.2 Basic Setting	17
	5.5.3 Wireless Setting	21
	5.5.4 Advanced Setting	
	5.5.5 Event Warning Settings	
	5.5.6 System status	



5.5.7 Administrator	
Technical Specifications	41
Compliance	43



# **Getting Started**

# 1.1 About the TGAP-620(+)-/6620(+)-M12 Series

The TGAP-620(+)-/6620(+)-M12 series are reliable outdoor WLAN access points with one (TGAP-620(+)-M12) or dual (TGAP-6620(+)-M12) 802.11 a/b/g/n wireless modules alongside two Gigabit LAN ports in M12 connectors. The two Ethernet ports allow you to form Daisy



Chain structure to reduce the use of the ports. The series includes PoE models (TGAP-620+/6620+-M12) and non-PoE models (TGAP-620/6620-M12). With EN50155 compliance and M12 connectors to ensure tight and robust connections, the devices guarantee reliable operation against environmental disturbances, such as vibration and shock, and are ideal for rolling stock applications. The APs can be configured to operate in AP/Client/Bridge/AP-Client modes and support MAC filters for security control. The devices can be configured and managed via a Window utility or Web interface on LAN or WLAN networks.

# 1.2 Software Features

- High speed air connectivity with support up to 300Mbps
- Highly secure transmission with WEP/WPA/WPA2/Radius/TKIP supported
- Supports AP/Client/Bridge/AP-Client modes
- Supports Daisy Chain to reduce use of AP ports
- Secure management with HTTPS
- Event warning via Syslog, e-mail, SNMP traps, and relay

# **1.3 Hardware Features**

- 2 x 10/100/1000 Base-T(X) Ethernet ports
- Supports PoE (TGAP-620+/6620+-M12 only)
- Operating temperature: -25 to 70°C
- Storage temperature: -40 to 85°C
- Operating humidity: 5% to 95%, non-condensing
- Dimensions(W x D x H): 125.6(W) x 65(D) x 196.1(H) mm



# Hardware Overview

# 2.1 Front Panel

## 2.1.1 Ports and Connectors

The devices are equipped with the following ports and features on the front panel.

Port	Description	
10/100/1000 Base-T(X) Ethernet ports	2 x 10/100/1000 Base-T(X) ports supporting	
with M12 connectors (A-coding)	auto-negotiation.	
Relay output with M12 (A-coding)	1 x relay output to carry capacity of 1A at 24VDC	
connector		
M23 power connector with redundant	Dual power inputs for 12, 48 V/DC	
power inputs	Dual power inputs for 12~48 VDC	
DIDO with M12 connector (A-coding)	4 x digital input / 4 x digital output	
	Dry Contact:	
	On: short to GND, Off: open	
	Wet Contact (DI to COM/GND):	
	On: 0 to 3VDC, Off: 10 to 30VDC	



TGAP-620+-M12







- 1. LED for PWR1 status
- 2. LED for PWR2 status (with PoE indicator)
- 3. LED for Ethernet port 1 status
- 4. LED for Ethernet port 2 status
- 5. LED for fault relay
- 6. LED for WLAN connection

- 8. Console port
- 9. Ethernet port 1
- 10. Ethernet port 2 (with PoE)
- 11. Digital output
- 12. Digital input
- 13. Power connector
- 14. 2.4/5GHz antenna



LED	Color	Status	Description
PWR1	Green	On	DC power 1 activated
	Green	On	DC power 2 activated or PoE enabled (when
PWR2 (PoE)			device is not connected to power supply)
ETH1	Green	On	Port is linked link
2	Green	Blinking	Transmitting data
ETH2	Green	On	Port is linked link
	Green	Blinking	Transmitting data
	0	On	WLAN activated
WLAN (1/2)	Green	Blinking	Transmitting WLAN data
Fault	Red	On	Fault relay. Power failure or Port down/fail.

### 2.1.2 Front Panel LEDs

# 2.2 Side Panel



- 1. Antenna connector
- 2. Reset button

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



# Hardware Installation

Before installing the devices, make sure you have all of the package contents available and a

PC with Microsoft Internet Explorer 6.0 or later, for using web-based system management tools.



When installed outdoors, make sure the connectors on the panel are facing down to prevent water intrusion.



Do not remove the water-proof casing, and do not touch or move the device when the antennas are transmitting or receiving signals.



When installing the device, make sure to keep the radiating at a minimum distance of 20 cm (7.9 inches) from all persons to minimize the potential for human contact during normal operation.



Do not operate the device near unshielded blasting caps or in an otherwise explosive environment unless the device has been modified for such use by qualified personnel.

# 3.1 Wall Mounting Installation



**Wall-mount Measurements** 



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

Step 1: Hold the AP upright against the wall

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

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





Instead of screwing the screws in all the way, it is advised to leave a space of about 2mm to allow room for sliding the AP between the wall and the screws.

# 3.2 Wiring

For pin assignments of power, console and relay output ports, please refer to the following tables.

## 3.2.1 Grounding

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

## 3.2.2 Power Port Pinouts

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

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

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





### 3.2.3 Relay Output Port Pinouts

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





# Cables and Antenna

# 4.1 Ethernet Pin Definition

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

Cable	Туре	Max. Length	Connector
10Base-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	M12
100Base-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	M12
1000BASE-T	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	M12



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

# 4.2 Console Port Pin Definition





# 4.3 DI/DO



# 4.4 Wireless Antenna

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





# <u>Management</u>

# 5.1 Network Connection

Before installing the device, you need to be able to access the device via a computer equipped with an Ethernet card or wireless LAN interface. To simplify the connection, it is recommended to use an Ethernet card to connect to a LAN.



Follow the steps below to install and connect the device to PCs:

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

# 5.2 Open-Vision Configuration

The device can be configured using ORing's proprietary Windows utility Open-Vision. Follow the steps below to set up the device in Open-Vision.

Step 1: Open the commander and click Discover, a list of AP devices will be shown.

Step 2: Choose your access point. The functions of the AP will be shown in a tree structure.

Step 3: Type in the username and password to log in to setup the AP.



Commander .	
Task Settings Help	
Q         Q         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A	Seitesh ClearState Refresh All Group IP Wizard Group Firmware Wizard Group O-Ring Wizard About
Sort Devices By: Model	Image: Sparse Strength of the strenge strength of the strength of the strength

## 5.3 UPnP Equipment

The device supports UPnP; therefore, when you connect the device to the PC, it will discover the presence of the device automatically. To check the connection of the device to you PC, follow the steps below.

Step 1: Go to Control Panel > Add or Remove Programs > Windows Components Wizard > Networking Servers > UPnP User Interface and pitch on the UPnP User Interface.

6	Add or Remove Programs		
Γ	Windows Components Wizard		
	Networking Services	X	F
L	To add or remove a component, click the check box. A shaded box me of the component will be installed. To see what's included in a component		L
	Subcomponents of Networking Services:		L
	Internet Gateway Device Discovery and Control Client	0.0 MB 🔥	L
	🗆 📮 Peerto-Peer	0.0 MB	L
	🗆 📮 RIP Listener	0.0 MB	
	Simple TCP/IP Services	0.0 MB	
A	🗹 📇 UPnP User Interface	0.2 MB	
C		~	
	Description: Allows you to find and control Internet connection sharin software that uses UPnP(TM).	g hardware and	2
S	Total disk space required: 0.0 MB	Details	
4	Space available on disk: 6718.7 MB		ľ
	ОК	Cancel	
	UK		ice



**Step 2**: At the right-below corner of the computer, you will find an UPnP icon of the device.



Step 3: Click on the icon and you will find the UPnP device in My Network Places.



**Step 4**: Right click the UPnP device and choose **Properties**, the following picture will be shown.

Step 5: Double click the device icon will lead you to the management web page.

#### 5.4 Web Browser Management

An embedded HTML web site resides in the flash memory of the device. It contains advanced management features which you can manage from anywhere on the network through a standard web browser such as Microsoft Internet Explorer (Internet Explorer 5.0 or later versions). It is based on Java Applets which can reduce network bandwidth consumption, enhance access speed, and provide user-friendly viewing windows.

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

Open a web browser on your computer and type <u>http://192.168.10.2</u> (default gateway IP of the device) in the address box to access the webpage. A login window will pop up where you can enter the default login name admin and password **admin**. For security reasons, we strongly recommend you to change the password. Click on **Administrator > Password** after



logging in to change the password.

Pleas	e enter your user ID and password	
	ID	
	Password	
	Apply Cancel	

# 5.5 Configurations

The **Home** screen will appear with a short description of the device. You can lick **Run Wizard** on the page for quick configurations of a new password, wireless SSID and channel, and encryption.

ORing	Industrial EN50155 IEEE 802.11 a/b/g/n Wireless Access Point with 2x10/100/1000Base-T(X), M12 connector, EU Band	
Firmware Ver: 1.1h   Uptime: 0h	: 56m : 21s	www.oring-networking.com
open all B. Home C. Overview Basic Selfings D. Wireless Selfings D. Wireless Selfings D. Advanced Selfings D. Konning Selfings D. System Status D. Advinistator B. Logout	Home Welcome to Industrial EN50155 IEEE 802.11 a/b/g/n Wireless Access Point with 2x10/100/1000Base-T(X), M12 connector web configuration page. The setup wizard will guide you to configure the Access Point. Please follow the wizard step by step to configure the Access Point. Run Wizard	

#### 5.5.1 Overview

This setting will show the general information with regard to the device, including system information, LAN network information, and wireless network information.

#### System Info

Overview> System Info			
System information details.			
Model			
Model Name:	TGAP-620-M12		
Device Name:	TGAP-620-M12-558877		
Device Location:			
Device Description:			
System Up Time:	00:56:49		
FW Version:	1.1h		
Region:	EU		



#### LAN Info

00:1E:94:55:88:77	
192.168.10.2	
255.255.255.0	
0.0.0.0	
	192.168.10.2 255.255.255.0

#### Wireless Info

Overvies> Wireless Info		
System information details.		
Wireless		
MAC Address:	00:0E:8E:47:45:10	
SSID:	oring	
Peer AP SSID:		
Encryption Type:	No encryption	
Channel:	6	
Operation Mode:	AP	
RF Type:	BGN Mixed Mode	

### 5.5.2 Basic Setting

This section will allow you to configure the general settings for the device.

### System Info Setting

Basic Settings> System Info Setting	
Device Name:	TGAP-620-M12-55887
Device Location:	
Device Description:	
Apply Cancel	

Label	Description
Device Name	Define the name of the device
Device Location	Enter the location of the device
Device Description	Enter a description for the device



#### LAN Setting

This page allows you to configure the IP settings of the LAN port for the device.

Basic Settings> LAN Setting
LAN settings of AP.
<ul> <li>Obtain an IP address automatically</li> </ul>
C  O Use the following IP address
IP Address: 192 . 168 . 10 . 2
Subnet Mask: 255 , 255 , 255 , 0
Default Gateway:
<ul> <li>Obtain DNS server address automatically</li> </ul>
O Use the following DNS server addresses
Primary DNS:
Secondary DNS:
Web Protocol:  OHTTP OHTTPS
Port 80
Web Access Control: Wired Wireless
The AP can be setup as a DHCP server to distribute IP addresses to the WLAN network.
DHCP Server
Options
Starting IP address:
Maximum Number of IPs:
Lease Time: 48 hours
Apply Cancel

Label	Description
Obtain an IP address	Select this option if you want the IP address to be assigned
automatically	automatically by the DHCP server in your network.
Use the following IP address	Select this option if you want to assign an IP address to the device manually. You should set up IP address, subnet mask, and default gateway for the device. <b>IP Address:</b> The device comes with default IP address, but you can also input a new IP address. <b>Subnet Mask: 255.255.255.0</b> is the default value. All devices on the network must have the same subnet mask to communicate on the network.



Default Gateway: Enter the IP address of the device in your
network.
Obtains a DNS server address from a DHCP server. If you have
chosen to obtain an IP address automatically, this option will be
selected accordingly.
Specifice a DNS conver address manually. You can enter two
Specifies a DNS server address manually. You can enter two
addresses as the primary and secondary options.
Choose a Web protocol for the device. The default value is
HTTP. For higher security, choose HTTPS.
Each Web protocol has a default port (HTTP is 80 and HTTPS is
443). You can also enter a value from 1 to 65535.
You can choose to access the web page via wired or wireless
connections.
Enables or disables the DHCP server function. When enabled,
the device will become the DHCP server on your local network.
The starting IP address of the IP range assigned by the DHCP
server. The start IP address is usually the lowest figures. For
example, in a dynamic IP range from 192.168.1.100 to
192.168.1.200, 192.168.1.100 will be the start IP address.
You can specify the number of IPs allowed to access the device.
For example, if the dynamic IP range is from 192.168.1.100 to
192.168.1.200, you should enter <b>100</b> in this box.
The period of time for an IP address to be leased. During the
lease time, the DHCP server cannot assign that IP address to
any other clients. Once the lease time ends, the system will
reassign the IP address.

#### **Time Setting**

In this page, you can set the date & time of the device. A correct date and time will help the system log events. You can set up a NTP (Network Time Protocol) client to synchronize date & time to a NTP server on the Internet.



Basic Settings> Time Setting	
Date/Time settings	3.
System time:	Wed Jul 25 2012 14:31:12
NTP:	✓ Enable
NTP Server 1:	time.nist.gov
NTP Server 2:	pool.ntp.org (optional)
Time Zone:	(UTC+08:00) Taipei 🛛 🗸
Synchronise:	Every Hour 💽 at 00 💟 : 00 💟
Local Date:	2012 Year 7 Month 25 Day
Local Time:	14 Hour 31 Minute 9 Second
	Get Current Date & Time from Browser
Apply Cancel	

Label	Description
NTP	Enables or disables NTP function
NTP Server 1	The primary NTP server
NTP Server 2	The secondary NTP server
Time Zone	Select the time zone you are located in
Synchronize	Specify the scheduled time for synchronization
Local Date	Set a local date manually
Local Time	Set a local time manually
Get Current Date &	Click to set the time from your browser
Time from Browser	

#### DIDO

This page allows you to set up digital input/output for the device. Simply click on the radio button to activate or deactivate the function.

Basic Setting> DIDO			
DI			
DI 1	⊖ On	⊙ Off	
DI 2	⊖ On	⊙ Off	
DI 3	⊖ On	⊙ Off	
DI 4	⊖ On	⊙ Off	
DO			
DO 1	⊙ On	● Off	
DO 2	● On	● Off	
DO 3	● On	● Off	
DO 4	● On	● Off	
Apply Cancel			



## 5.5.3 Wireless Setting

This section allows you to configure the wireless settings of the device when operating in different modes.

Wireless Settings> Wireless Settings
AP  AP AP-Client Client
Bridge
Basic wireless settings for the AP.
Multiple SSID Index:
SSID: oring
Channel: 6 💌
WDS-Master Mode: Disabled 💌
AP Isolation: Disabled 💌
Security Options
Security Type: None 💌
Apply Save Cancel

#### AP Mode

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





Label	Description
Multiple SSID index	The index of the SSID
	SSID (Service Set Identifier) is a unique name that identifies a
COID	network. All devices on the network must be set with the same
SSID	SSID in order to communicate with each other. Fill in a new SSID
	in this field if you do not want to use the default value.
	Specify a channel to be used. Channel 6 is the default channel.
Channel	You can also select a new number from the dropdown list. All
Channel	devices on the network must be set to use the same channel to
	communicate on the network.
	A WDS master is the central control point for authenticating
	wireless clients, caching client key material, distributing MFP key
WDS-Master Mode	material, reporting radio management information to an upstream
WDS-Master Mode	network management station, and updating other APs
	participating in WDS. You can set the device as the WDS-master
	by selecting from the list.
	This function prevents devices connected to an AP from
AP Isolation	communicating directly with each other. This function is useful
	when many wireless clients request your network frequently.
	You can choose the security type for your WLAN connection from
	the following options:
	None: no encryption
	WEP: WEP (Wired Equivalent Privacy) is a wireless security
	protocol for WLAN. WEP will encrypt data transmitted on the
	WLAN.
Security options	WPA/WPA2 Personal: uses a pre-shared key for authentication.
Security options	This pre-shared key is then dynamically sent between the AP and
	clients. Each authorized computer is given the same pass phrase.
	WPA/WPA2 Enterprise: this type includes all of the features of
	WPA/WPA2 Personal plus support for 802.1x RADIUS
	authentication.
	802.1x: authentication through a RADIUS server

When you set security type as **WEP**, the following fields will appear to allow you to configure individual settings.



Security Options	
Security Type:	WEP 💌
Auth Mode:	Open ● Shared ● WEPAUTO
WEP Encryption:	64 Bit 🔽
Key Type:	ASCII (5 characters) 💌
Default Key Index:	1 🗸
KEY1:	
KEY2:	
KEY3:	
KEY4:	

Label	Description		
	Available values include Open, Shared, and WEPAUTO. When		
	choosing Open or Shared, all of the clients must select the		
Auth Mode	same authentication to associate this AP. If select WEPAUTO,		
	the clients do not have to use the same Open or Shared		
	authentication. They can choose any one to authenticate.		
WEP Encryption	You can select <b>64 Bit</b> or <b>128 Bit</b> .		
	Available values include <b>ASCII</b> and <b>Hex Key Type</b> . ASCII		
	(American Standard Code for Information Interchange) is a		
	code for representing English characters as numbers in the		
Кеу Туре	range from 0 to 127. Hex digits uses 0-9 to represent values		
	zero to nine, and characters A-F to represent values ten to		
	fifteen.		
Default Key Index	Select one of the keys to be the active key		
Key 1 to 4	You can input up to four encryption keys.		

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

<ul> <li>Security Options</li> </ul>	
Security Type:	WPA/WPA2 Personal
Auth Mode:	○ WPAPSK ○ WPA2PSK ○ WPAPSK/WPA2PSK mix
Encryption Type:	● TKIP ● AES ● TKIP/AES mix
Shared Key:	(8~64 characters)

Label	Description	
Auth Made	Available values include WPAPSK, WPA2PSK, and	
Auth Mode	WPAPSK/WPA2PSK mix. WPAPSK and WPA2PSK will	



	encrypt the link without additional RADIUS server, only an	
	access point and client station that supports WPA-PSK is	
	required. For WPA/WPA2, authentication is achieved via WPA	
	RADIUS Server. You need a RADIUS or other authentication	
	server on the network.	
	Available values include <b>TKIP</b> , <b>AES</b> , and <b>TKIP/AES mix</b> .	
Enonymtion Type	WPA-PSK uses TKIP encryption, and WPA2-PSK uses AES	
Encryption Type	encryption. TKIP/AES provides the most reliable security, and is	
	easiest to implement.	
Sharad Kay	Enter a pass phrase in this field. The value must be within 8 to	
Shared Key	64 characters	

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

C Security Options	
Security Type:	WPA/WPA2 Enterprise 🔽
Auth Mode:	● WPA ● WPA2 ● WPA/WPA2 mix
Encryption Type:	○ TKIP ● AES ● TKIP/AES mix
Radius Server IP:	0 . 0 . 0
Radius Port:	1812
Shared Secret:	radius_key

Label	Description		
	Available values include WPAPSK, WPA2PSK, and		
	WPAPSK/WPA2PSK mix. WPAPSK and WPA2PSK will		
	encrypt the link without additional RADIUS server, only an		
Auth Mode	access point and client station that supports WPA-PSK is		
	required. For WPA/WPA2, authentication is achieved via WPA		
	RADIUS Server. You need a RADIUS or other authentication		
	server on the network.		
	Available values include TKIP, AES, and TKIP/AES mix.		
Enonymtion Type	WPA-PSK uses TKIP encryption, and WPA2-PSK uses AES		
Encryption Type	encryption. TKIP/AES provides the most reliable security, and is		
	easiest to implement.		
Radius Server IP	Enter the IP address of the RADIUS server		
Radius Port	Enter the RADIUS port (default is 1812)		
Shared Secret	Enter the RADIUS password or key		



When you set security type as **802.1x**, the following fields will appear to allow you to configure individual settings.



Label	Description	
WEP Encryption	You can select 64 Bit or 128 Bit.	
	Available values include ASCII and Hex Key Type. ASCII	
	(American Standard Code for Information Interchange) is a	
	code for representing English characters as numbers in the	
Кеу Туре	range from 0 to 127. Hex digits uses 0–9 to represent values	
	zero to nine, and characters A-F to represent values ten to	
	fifteen.	
Default Key Index	Select one of the keys to be the active key	
Key 1 to 4	Input up to four encryption keys	
Radius Server IP	Enter the IP address of the RADIUS server	
Radius Port	Enter the RADIUS port (default is <b>1812</b> )	
Shared Secret	Enter the RADIUS password or key	

RADIUS (Remote Authentication Dial-In User Service) is a widely deployed protocol that enables companies to authenticate and authorize remote users' access to a system or service from a central network server.

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







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

#### **AP-Client Mode**

This mode provides a 1-to-N MAC address mapping mechanism such that multiple stations behind the AP can transparently connect to the other AP even if they don't support WDS.

Note: When the device	in AP-Client mode, wireless channel must be the same with the other device in group.
Basic wireless settings	for the AP.
Multiple SSID Index:	1 💌
SSID:	oring
Channel:	6 💌
WDS-Master Mode:	Disabled 🔽
AP Isolation:	Disabled 🔽
<ul> <li>Security Options</li> </ul>	
Security Type:	None
AP-Client related settin	ıgs.
AP-Client related settin Peer AP SSID:	Igs. Site Survey Hidden/Show SiteTable
AP-Client related settin Peer AP SSID: Peer AP BSSID:	ıgs.
AP-Client related settin Peer AP SSID: Peer AP BSSID:	ngs. Site Survey Hidden/Show SiteTable Enabled
AP-Client related settin Peer AP SSID: Peer AP BSSID: Slave Mode: Di	Igs. Site Survey Hidden/Show SiteTable Enabled sabled V

Label	Description	
	SSID (Service Set Identifier) is a unique name that identifies a	
SSID	network. All devices on the network must be set with the same SSID	
3310	in order to communicate with each other. Fill in a new SSID in this	
	field if you do not want to use the default value.	
Channel	Specify a channel to be used. Channel 6 is the default channel. You	
Channer	can also select a new number from the dropdown list. All devices on	



	the network must be set to the same channel to communicate on the		
	network. (Wireless channel must be the same as the other device		
	in the group)		
	A WDS master is the central control point for authenticating wireless		
	clients, caching client key material, distributing MFP key material,		
WDS-Master Mode	reporting radio management information to an upstream network		
	management station, and updating other APs participating in WDS.		
	You can set the device as the WDS-master by selecting from the list.		
	You can choose the security type for your WLAN connection from the		
	following options:		
	None: no encryption		
	WEP: WEP (Wired Equivalent Privacy) is a wireless security protocol		
Security options	for WLAN. WEP will encrypt data transmitted on the WLAN.		
	WPA/WPA2 Personal: uses a pre-shared key for authentication.		
	This pre-shared key is then dynamically sent between the AP and		
	clients. Each authorized computer is given the same pass phrase.		
Peer AP SSID	Enter the SSID of the AP you want to connect as a client		
Peer AP BSSID	Enter the BSSID (Wireless MAC address) to limit client target		
Slave Mode	Enables or disables slave mode		
Site Scan	You can scan APs on the network using this mode.		
Security Type	Select the security type used by the client you want to connect		

#### **Client Mode**

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

Wireless Settings	Wireless Settings> Wireless Settings				
Client 💌					
	functions as a wireless client wirlesss port. This mode prov				
Client related setting	js.				
Peer AP SSID:		Sit	e Survey	Hidden/Show SiteTable	
Peer AP BSSID:		🗆 E	Inabled		
Slave Mode:	Disabled 💌				
Security Options					
Security Type:	None	~			
Apply Cancel					



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

#### **Bridge Mode**

Select this option if the device is connected to a local network downstream from another router. In this mode, the device functions as a bridge between the network on its WAN port and the devices on its LAN port and those connected to it wirelessly.

Wireless Settings> Wireless Settings		
Bridge  This mode provides Static LAN supported through Wireless Di	-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is stribution System(WDS).	
Note: When the device in Bridg	e mode, wireless channel must be the same with the other device in group.	
WDS Mode:     Bridge I       Peer MAC Address 1:     Bridge I       Peer MAC Address 2:     Repeat       Peer MAC Address 3:     Peer MAC Address 4:       Please input the wireless MAC Format example :     Peer MAC Address 4:	Aode Enabled	
SSID: oring Security Options Security Type: None	Channel: 6 💌	
Apply Cancel		

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.





Label	Description	
WDS Mode	This mode provides static LAN-to-LAN bridging functionality, which is	
	supported through WDS. WDS enables access points or routers to	
	be wirelessly connected to one another. This function is usually used	
	in large, open areas such as warehouses where wiring is restricted or	
	costly, and in some larger home environments.	
Peer MAC Address	Enter the Mac address of other access point(s) and check the	
	Enable box.	
	SSID (Service Set Identifier) is a unique name that identifies a	
SSID (only Repeater	network. All devices on the network must be set with the same SSID	
mode support)	in order to communicate with each other. Fill in a new SSID in this	
	field if you do not want to use the default value.	
	Specify a channel to be used. Channel 6 is the default channel. Yo	
	can also select a new number from the dropdown list. All devices on	
Channel	the network must be set to the same channel to communicate on the	
	network. (Wireless channel must be the same as the other device	
	in the group)	
	You can choose the security type for your WLAN connection from the	
	following options:	
	None: no encryption	
	<b>WEP</b> : WEP (Wired Equivalent Privacy) is a wireless security protocol	
Security options	for WLAN. WEP will encrypt data transmitted on the WLAN.	
	WPA/WPA2 Personal: uses a pre-shared key for authentication.	
	This pre-shared key is then dynamically sent between the AP and	
	clients. Each authorized computer is given the same pass phrase.	

#### Set WDS as Bridge Mode

In the mode, the AP acts as a standard bridge that forwards traffic between WDS links (links connected 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 wired and wireless network devices, which are connected to their respective Ethernet ports to limit the amount of forwarded data. 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. The peer WDS APs are based on the MAC addresses listed in **Peer Mac Address**.





Bear in mind the following principles when setting the WDS mode to bridge mode:

- 1. LAN IP address should use a different IP in the same network.
- 2. Shut down all DHCP server functions of the AP.
- 3. Enable WDS.
- 4. Each AP should have the same setting, except **Peer Mac Address** should be set to the other's Mac address.
- 5. The settings of security and channel must be the same.
- 6. The distance of the AP should be limited within a certainty area.

#### Set WDS as Repeater Mode

In this mode, 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. The peer WDS APs are based on the MAC addresses listed in **Peer Mac Address**.





# **Wireless Options**

Wireless Settings> Wireless Options		
Wireless performance tunning.		
Radio Button:	ON OFF	
Beacon Interval:	100 (msec,	range:20~1000, 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)
Wireless Mode:		G Mixed Mode 💿 BGN Mixed Mode 🔿 A Mode 💿 AN Mixed
	Mode	
Max Client Threshold	255 (range: 1	~2007, default 255)
Preamble:	<ul> <li>Long</li> </ul>	<ul> <li>Short</li> </ul>
SSID Broadcast:	<ul> <li>Disable</li> </ul>	• Enable
HT Require:	<ul> <li>Disable</li> </ul>	Enable
HT Band Width:	O 20 MHz	• 20/40 MHz
HT Guard Interval:	<ul> <li>Long</li> </ul>	Short
HT Extension Channel:	10 💌	
HT Tx STBC:	<ul> <li>Disable</li> </ul>	Enable
HT Rx STBC:	<ul> <li>Disable</li> </ul>	Enable
HT LDPC:	<ul> <li>Disable</li> </ul>	• Enable

Label	Description
Radio	Enables or disables wireless functions
Button	
Beacon	A beacon is a packet sent by a wireless access point to synchronize
Interval	wireless devices. The beacon interval value indicates the frequency interval
	of the beacon. Increasing the beacon interval reduces the number of
	beacons and the overhead associated with them. The default value is 100,
	but <b>50</b> is recommended when reception is poor.
DTIM	The value specifies the maximum size for a packet before data is
Interval	fragmented into multiple packets. The value should remain at the default
	2346 (the range is 256 - 2346 bytes). If you experience a high packet error
	rate, you may slightly increase the value. Setting the value too low may
	result in poor network performance. Only minor modifications of this value
	are recommended.
Fragmentati	The RTS (Request to Send) Threshold is the amount of time a wireless
on	device, attempting to send, will wait for a recipient to acknowledge that it is
Threshold	ready. Normally, the AP sends a RTS frame to a station and negotiates the
	sending of data. After receiving the RTS, the station responds with a CTS
	(Clear to Send) frame to acknowledge the right to begin transmission. To
	ensure communication, the maximum value should be used, which is the



	default value <b>2347</b> (the range is 0-2347 bytes). If a network packet is
	smaller than the preset RTS threshold size, the RTS/CTS mechanism will
	not be enabled.
RTS	You can called 202 11 b. b/g. or b/g/g mode
Threshold	You can select 802.11 b, b/g, or b/g/n mode.
Wireless	Available values include Long and Short, with Long as the default value. If
Network	all clients and access points in your wireless network support short
Mode	preamble, then enabling it can boost overall throughput. However, if any
	wireless device does not support short preamble, then it will not be able to
	communicate with your network. If you are not sure whether your radio
	supports the short RF preamble, you must disable this feature.
Preamble	The value specifies the maximum size for a packet before data is
	fragmented into multiple packets. The value should remain at the default
	2346 (the range is 256 - 2346 bytes). If you experience a high packet error
	rate, you may slightly increase the value. Setting the value too low may
	result in poor network performance. Only minor modifications of this value
	are recommended.

Extra parameters for Client Mode:	
Roaming:	• Disabled • X-roaming
Scan Channel:	⊙ All ⊖ Manual
Channel Select:	(ex. 6 or 1,2,13)
Sensitivity(dbm):	5 (range: 1~20, default 5)
Scan Interval(sec):	30 (range: 0~60, default 30 , 0: Trigger immediate scan)

Label	Description	
Roaming	Select Disabled to disable X-Roaming protocol or select	
	X-roaming to enable X-Roaming protocol	
Scan channel	Select All to scan all supported channels or Manual to scan only	
	selected channels specified in Channel Select.	
Channel Select	Assign the value roaming channels	
Sensitivity	Configures signal sensitivity	
Scan interval	Configures scan interval	

# 5.5.4 Advanced Setting

### Filters

This page allows you to set up MAC filters to allow or deny wireless clients to connect to the AP. You can manually add a MAC address or select a MAC address from the Associated



#### Clients list currently associated with the AP.

Advanced Settings> 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:	Choose an Associated Cl	ient 🕑 Copy To Choose	e a Slot - 💌
MAC Filter Table:	1.	11.	21.
	2.	12.	22.
	3.	13.	23.
	4.	14.	24.
	5.	15.	25.
	6.	16.	26.
	7.	17.	27.
	8.	18.	28.
	9.	19.	29.
	10.	20.	30.
Apply Cancel	J		

Label	Description	
MAC Filter	Select Enabled or Disabled to activate or deactivate MAC filters	
Options	Select one of the options to allow or deny the MAC address in the	
	list	
Associated Clients	Shows the wireless MAC addresses associated with the device	
MAC Filter Table	You can edit up to MAC addresses in these fields	
Apply	Click to activate the configurations	

# Misc. Settings

Advanced Settings> Misc. Settings		
UPnP:	<ul> <li>Enable</li> </ul>	<ul> <li>Disable</li> </ul>
LLDP Protocol:	<ul> <li>Enable</li> </ul>	<ul> <li>Disable</li> </ul>
Spanning Tree Protocol:	<ul> <li>Enable</li> </ul>	<ul> <li>Disable</li> </ul>
Apply Cancel		

Label	Description
UPnP	Enables or disables UPnP function



LLDP Protocol	Enables or disables LLDP protocol
Spanning Tree Protocol	Enables or disables STP function

# 5.5.5 Event Warning Settings

When an error occurs, the device will notify you through system log, e-mail, SNMP, and relay. You can choose the system to issue a notification when specific events occur by checking the box next to the event.

# System Log

Even Warning Settings> System Log		
Syslog Server Settings		
Syslog Server IP:	_	
Syslog Server Port: 514	(0 represents default)	
Systeg Cervert off. 514		
Surles Fuert Tures		
Syslog Event Types		
Device Event Notification		
Hardware Reset (Cold Start)	Syslog	
Software Reset (Warm Start)	Syslog	
Login Failed	Syslog	
IP Address Changed	Syslog	
Password Changed	Syslog	
Redundant Power Changed	Syslog	
Eth Link Status Changed	Syslog	
SNMP Access Failed	Syslog	
Wireless Client Associated	🗌 Syslog	
Wireless Client Disassociated	🗌 Syslog	
Client Mode Associated	🗆 Syslog	
Client Mode Disassociated	🗆 Syslog	
Client Mode Roaming	Syslog	
Fault Event Notification		
Power 1 Fault Power 2 Fault	Syslog	
Eth1 Link Down		
Eth2 Link Down	Syslog	
DI1 ON->OFF		
DI2 ON->OFF		
DI3 ON->OFF		
DI4 ON->OFF	Syslog	
DI1 OFF->ON	Syslog	
DI2 OFF->ON	🔲 Syslog	
DI3 OFF->ON	Syslog	
DI4 OFF->ON	Syslog	

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



## E-Mail

Even Warning Settings> E-mail	
E-mail Server Settings	
SMTP Server:	(optional)
Server Port: 25 (0 represent	
E-mail Address 1:	, 
E-mail Address 2:	
E-mail Address 3:	
E-mail Address 4:	-
E-mail Event Types	
Device Event Notification	
Hardware Reset (Cold Start)	SMTP Mail
Software Reset (Warm Start)	SMTP Mail
Login Failed	SMTP Mail
IP Address Changed	SMTP Mail
Password Changed	SMTP Mail
Redundant Power Changed	SMTP Mail
Eth Link Status Changed	SMTP Mail
SNMP Access Failed	SMTP Mail
Wireless Client Associated	SMTP Mail
Wireless Client Disassociated	SMTP Mail
Client Mode Associated	SMTP Mail
Client Mode Disassociated	SMTP Mail
Client Mode Roaming	SMTP Mail
Fault Event Notification	
Power 1 Fault	SMTP Mail
Power 2 Fault	SMTP Mail
Eth1 Link Down	SMTP Mail
Eth2 Link Down	SMTP Mail
DI1 ON->OFF	🗌 SMTP Mail
DI2 ON->OFF	🗌 SMTP Mail
DI3 ON->OFF	🗌 SMTP Mail
DI4 ON->OFF	🔲 SMTP Mail
DI1 OFF->ON	🗖 SMTP Mail
DI2 OFF->ON	SMTP Mail
DI3 OFF->ON	SMTP Mail
DI4 OFF->ON	🗌 SMTP Mail

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



# SNMP

Even Warning Settings> SNMP Set	ttings	
SNMP Settings		
SNMP Agent: • Ena SNMP Trap Server 1: SNMP Trap Server 2: SNMP Trap Server 3: SNMP Trap Server 4: Community: public SysLocation: 0: SysContact: 0: SNMP Event Types	ible • Disable	
Device Event Notification		
Hardware Reset (Cold Start)		SNMP Trap
Software Reset (Warm Start)		SNMP Trap
Login Failed		SNMP Trap
IP Address Changed	_	SNMP Trap
Password Changed		SNMP Trap
Redundant Power Changed		SNMP Trap
Eth Link Status Changed		SNMP Trap
SNMP Access Failed		SNMP Trap
Wireless Client Associated		SNMP Trap
Wireless Client Disassociated		SNMP Trap
Client Mode Associated		SNMP Trap
Client Mode Disassociated		SNMP Trap
Client Mode Roaming		SNMP Trap
Fault Event Notification		
Power 1 Fault		
Power 2 Fault		SNMP Trap
Eth1 Link Down		SNMP Trap SNMP Trap
Eth2 Link Down	_	SNMP Trap
DI1 ON->OFF		
DI2 ON->OFF		SNMP Tran
	_	SNMP Trap
DI3 ON->OFF		SNMP Trap
DI3 ON->OFF DI4 ON->OFF		SNMP Trap SNMP Trap
		SNMP Trap SNMP Trap SNMP Trap
DI4 ON->OFF		SNMP Trap SNMP Trap SNMP Trap SNMP Trap
DI4 ON->OFF DI1 OFF->ON		SNMP Trap SNMP Trap SNMP Trap

Label	Description
SNMP Agent	SNMP (Simple Network Management Protocol) Agent is a service
	program that runs on the access point. The agent provides
	management information to the NMS by keeping track of various



	operational aspects of the AP system. You can enable or disable
	the function.
SNMP Trap Server	Enter the IP address of the SNMP server which will send out traps
1-4	generated by the AP.
Community	Community is a password to establish trust between managers
	and agents. Normally, <b>public</b> is used for read-write community.
SysLocation	Specifies sysLocation string
SysContact	Specifies sysContact string

#### Relay

This page allows you to enable faulty relay function for the device by check the individual boxes.

Even Warning Settings> Relay				
Fault LED/Relay				
Power 1 Fault	🔲 Fault LED/Relay			
Power 2 Fault	Fault LED/Relay			
Eth1 Link Down	Fault LED/Relay			
Eth2 Link Down	Fault LED/Relay			
DI1 ON->OFF	Fault LED/Relay			
DI2 ON->OFF	Fault LED/Relay			
DI3 ON->OFF	Fault LED/Relay			
DI4 ON->OFF	Fault LED/Relay			
DI1 OFF->ON	Fault LED/Relay			
DI2 OFF->ON	Fault LED/Relay			
DI3 OFF->ON	Fault LED/Relay			
DI4 OFF->ON	Fault LED/Relay			

# 5.5.6 System status Wireless Link List

This page displays the information of the wireless clients connected to the device, including their MAC address, data rate, and link types.





## **DHCP Clients List**

This page lists the devices on your network that are receiving dynamic IP addresses from the

device.					
System Status> DHCP Client Lis	System Status> DHCP Client List				
DHCP Clients List:					
Hostname	Mac Address	IP Address	Expires In		

### **Traffic/Port Status**

This page displays the network traffic statistics for both received and transmitted packets through the Ethernet port and wireless connections associated with the AP. Note that the traffic counter will reset when the device is rebooted.

Send	Receive	
554373 Bytes (789 Packages)	52386 Bytes (488 Packages)	
79219 Bytes (362 Packages)	0 Bytes (0 Packages)	
lin	State	
Lin	k up, forwarding	
	k down, disabled	
	forwarding	
	Not Set	
Not Set		
	554373 Bytes (789 Packages) 79219 Bytes (362 Packages) e state of all ports in AP.	

# System Log

Refresh

The device will constantly log events and activities in System Log and provide the file for you

to review. You can click **Refresh** to renew the page or **Clear** to clear all or certain log entries.

system status> system i	
System log details.	
Refresh Clear	
# Date Time	Content

## 5.5.7 Administrator Setting Password



This page allows you to change the username and password. You must type in the new password twice to confirm (the default username and password are **admin**).

Administrator> Password			
Modify web administrator's na	me and password.		
Old Name:	admin		
Old Password:			
New Name:	admin		
New Password:			
Confirm New Password:			
Apply Cancel			

Label	Description
Old Name	Type in current login name
Old Password	Type in current password
New Name	Enter a new login name. Acceptable characters contain '0-9', 'a-z',
	'A-Z' and the length must be 1 to 15 characters. An empty name is
	not acceptable.
New Password	Enter a new login password. Acceptable characters contain '0-9',
	'a-z', 'A-Z' and the length must be 0 to 15 characters.
Confirm New	Retype the new password to confirm it.
Password	

## **Saving Configurations**

This page allows you to save existing configurations as a backup file or return the device to previous settings.

Iministrator> Configuration		
You can backup the configuration file to your computer, and restore a previously saved configuration.		
ave configuration to local		
Download		
estore a previously saved configuration		
瀏覽… 未選擇檔案。		
Upload		

Label	Description	
Download	Click to save the current system settings as a file stored in the	
	local hard drive.	
Upload	You can restore configurations to previous status by installing a	



previous configuration file. To do this, click on Browse to locat	
	the file you want to upload in the local hard drive and click
	Upload.
Restore Default	Click to reset the device to the factory settings. The device will
Settings	reboot to validate the default settings.

#### **Firmware Upgrade**

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





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

## Load Factory Default

You can use this page to restore the device to factory default settings. Make sure to save the device settings before clicking on this button. All current settings will be lost after you click this button.



#### Restart

Click the button in this page to restart the device through warm reset.





# **Technical Specifications**

ORing WLAN Access Point Model	TGAP-6620(+)-M12	TGAP-620(+)-M12
Physical Ports		
10/100/1000Base-T(X) Ports in M12		2
Auto MDI/MDIX (8-pin A-coding)	(Present at ETH2 Fully compliant with IEEE 802.3af PoE P.D)	
	2(DI x 4	and DO x 4)
	D	ry Contact:
DI/DO port in M12 (5-pin A-coding)	On: short to GND, Off: open	
	Wet Contact (DI to COM/GND):	
	On: 0 to 3VD	C, Off: 10 to 30VDC
RS-232 Console port in M12 (5-pin A-coding)	115200, 8 ,N ,1	
Relay port in M12 (5-pin A-coding)	14	@24VDC
WLAN interface		
Operating Mode	Dual AP/Dual Client /Bridge /AP-Client Mode	AP/Bridge/Client/AP-Client
Antenna Connector	4 x External reverse SMA antenna connector	2 x External reverse SMA antenna connector
Radio Frequency Type	DSSS, OFDM	
	IEEE802.11a : OFDM with BPSK, OPSK, QAM, 64Q	AM
	IEEE802.11b: CCK, DQPSK, DBPSK	
Modulation	IEEE802.11g: OFDM with BPSK, QPSK, 16QAM, 64	QAM
	IEEE802.11n : BPSK, QPSK, 16-QAM, 64-QAM	
	America / FCC: 2.412~2.462 GHz (11 channels)	
Frequency Band	5.180~5.240 GHz & 5.745~5.825 GHz ( 9 channels )	
Trequency bana	Europe CE / ETSI : 2.412~2.472 Ghz (13 channels)	
	5.180~5.240 GHz (4 channels)	
	IEEE802.11b: 1 / 2 / 5.5 / 11 Mbps	
Transmission Rate	IEEE802.11a/g: 6 / 9 / 12 / 18 / 24 / 36 / 48 / 54 Mbps	
	IEEE801.11n: up to 300Mbps 802.11a: 12dBm ± 1.5dBm	
	802.11b: 18dBm ± 1.5dBm	
	802.11g: 15dBm ± 1.5dBm	
Transmit Power	802.11gn HT20: 13dBm ± 1.5dBm@150Mbps	
	802.11gn HT40: 12dBm ± 1.5dBm@300Mbps	
	802.11an HT20: 12dBm ± 1.5dBm@150Mbps	
	802.11an HT40: 12dBm ± 1.5dBm@300Mbps	
	802.11a: -68dBm ±2dBm@54Mbps	
	802.11b: -85dBm ±2dBm@11Mbps	
Passiver Constitute	802.11g: -68dBm ±2dBm@54Mbps	
Receiver Sensitivity	802.11gn HT20: -68dBm ±2dBm@150Mbps	
	802.11gn HT40: -68dBm ±2dBm@300Mbps 802.11an HT20: -68dBm ±2dBm@150Mbps	
	802.11an H120: -68dBm ±2dBm@150Mbps 802.11an HT40: -68dBm ±2dBm@300Mbps	
	WEP: (64-bit ,128-bit key supported)	
	WPA/WPA2 :802.11i(WEP and AES encryption)	
Encryption Security	WPAPSK (256-bit key pre-shared key supported)	
	802.1X Authentication supported	
	TKIP encryption	
Wireless Security	SSID broadcast disable and enable	
Protocol Support		
Protocol	ARP,BOOTP, DHCP, DNS, HTTP, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, STP, RSTP,	
LED indicators		
	2 x LEDs,	
Power indicator	PW1:Green for DC Power on	
	PW2:Green for DC Power on or power by PoE	



10/100/1000Base-T(X) indicator	2 x LEDs, Green for port Link/Act	
WLAN LED	2 x LEDs, Green for WLAN Link /Act	1 x LED, Green for WLAN Link/Act
Fault	1 x LED, Red for Ethernet link down or power down indicator	
Fault contact		
Relay	Relay output to carry capacity of 1A at 24VDC(5-pin M12 A-coding)	
Power		
Input power	Dual Power Inputs. 12~48 VDC	
Power consumption (Typ.)	11Watts	8W
Physical Characteristic		
Enclosure	IP-40	
Dimension (W x D x H)	125.6(W) x 65(D) x 196.1(H) mm (4.94 x 2.55 x 7.72 inch.)	
Weight (g)	965g	955g
Environmental		
Storage Temperature	-40 to 85°C (-40 to 185°F)	
Operating Temperature	-25 to 70°C (-13 to 158°F)	
Operating Humidity	5 to 95% Non-condensing	
Regulatory approvals		
EMI	FCC Part 15, CISPR (EN55022) class A, EN50155 (EN50121-3-2, EN55011, EN50121-4)	
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	IEC60068-2-31	
Vibration	IEC60068-2-6	
Safety	EN60950-1	
Warranty	5 years	



### Compliance

#### **FCC Statement**

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

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

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

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

#### **Industry Canada Statement**

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

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

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

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



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

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

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

Afin de réduire les interférences radio potentielles pour les autres utilisateurs, le type d'antenne et son gain doivent être choisie que la puissance isotrope rayonnée équivalente (PIRE) est pas plus que celle premise pour une communication réussie

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

Avertissement d'exposition RF: L'équipement est conforme aux limites d'exposition aux RF établies pour un incontrôlés environnement. L'antenne (s) utilisée pour ce transmetteur ne doit pas être co-localisés ou fonctionner en conjonction avec toute autre antenne ou transmetteur.