



IDS-1112

Industrial Wireless Device Server

User's Manual

Version 1.0 Apr, 2013

www.oring-networking.com

ORing Industrial Networking Corp.



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)

ORing Industrial Networking Corp.

Tables of Content

County	to Know your Wireless Media Gateway	1
1.1	Overview	1
1.2	Software Features	1
1.3	Hardware Features	2
Hardwa	are Installation	3
2.1	Installation Media Gateway on DIN-Rail	3
2.2	Wall Mounting Installation	4
Hardwa	are Overview	6
3.1	Front Panel	6
3.2	Front Panel LEDs	7
3.3	Bottom Panel	8
3.4	Rear Panel	8
Cables	and Antenna	9
4.1	Ethernet Cables	9
4.2	Wireless Antenna	10
Manage	ement Interface	11
5.1	First-time Installation	11
5.2		
	Configure the Wireless Media Gateway	•
5.3	Configure the Wireless Media Gateway	• 12
5.3 5.3.1	Configure the Wireless Media Gateway銷誤! 尚未定義書籤 Main Interface 1 Basic Setting	12 12
5.3 5.3.1 V	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface I Basic Setting VAN	12 12 12 12
5.3 5.3. ⁷ V	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface 1 Basic Setting VAN	12 12 12 12 13
5.3 5.3.1 V L	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface I Basic Setting VAN AN	12 12 12 13 14
5.3 5.3. V L E V	Configure the Wireless Media Gateway錯誤! 尚未定義書鎔 Main Interface Basic Setting VAN AN DHCP Vireless	12 12 12 13 14 16
5.3 5.3.1 V L E V 5.3.2	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface I Basic Setting VAN AN DHCP Vireless	12 12 12 13 14 16 21
5.3 5.3.1 V L E V 5.3.2 V	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface Basic Setting VAN VAN OHCP Vireless 2 Advanced Setting Vireless	 12 12 12 12 13 14 16 21 27
5.3 5.3.1 V L E V 5.3.2 V N	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface I Basic Setting VAN OHCP Vireless 2 Advanced Setting Vireless Vireless	 12 12 12 13 14 16 21 27 30
5.3 5.3.1 V L E V 5.3.2 V S.3.2 N S	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface I Basic Setting VAN AN OHCP Vireless 2 Advanced Setting Vireless Vireless Vireless	 12 12 12 12 13 14 16 21 27 30 34
5.3 5.3.1 L E V 5.3.2 V S.3.2 V S S V	Configure the Wireless Media Gateway	12 12 12 13 14 16 21 27 30 34 35
5.3 5.3.1 V L E V 5.3.2 V S S V R	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface	12 12 12 13 14 16 21 27 30 34 35 43
5.3 5.3.1 V L E V 5.3.2 V S S V R N	Configure the Wireless Media Gateway	12 12 12 13 14 16 21 27 30 34 35 43 44
5.3 5.3.1 V L E V 5.3.2 V S V R N N M	Configure the Wireless Media Gateway錯誤! 尚未定義書鎦 Main Interface	12 12 12 13 14 16 21 27 30 34 35 43 44 47



Date & Time	47
Login Setting	48
Media Gateway Restart	50
Firmware Upgrade	50
Save/Restore Configurations	51
Miscellaneous (Ping)	51
5.3.4 System Status	52
System Info	52
System Log	52
Traffic Statistics	53
Wired/Wireless Clients錯誤! 尙未	宅義書籤。
Technical Specifications	54



Getting to Know your Wireless Media Gateway

1.1 Overview

The ORing IMG-8042 is an innovative 4port RS232/422/485 Serial Wireless Gateway. You can conveniently manage the device by windows Tool The Media Gateway provides a fast and effective ways of communicating to the internet over wired or wireless LAN. In addition, multiple kinds of WAN connection are provided for easily access to the internet.



The ORing IMG-1321-D wireless Media Gateway is with IEEE 802.11a/b/g or IEEE

802.11b/g high-performance wireless equipment. It is capable of data transfer rates up to 54Mbps. It is easy for you to extend the reach and number of computers connected to your wireless network.

With build-in HSUPA WAN connection, the ORing IMG-1321-D wireless Media Gateway can be mounted in harsh environment easily to provide internet access anytime and anywhere.

The ORing IMG-1321-D wireless Media Gateway's VPN capability creates encrypted "Virtual Tunnels" through the internet, allowing remote or traveling users for secured connection with the network in your office.

1.2 Software Features

- Intuitive Web-based management user interface for simply and easily operation.
- USB connectivity providing Internet access via the USB to RS232 convertor + modem or 3G HSDPA module (HUAWEI E220) directly.
- Functions of firewall provides many security features such as blocking attacks from hacker, especially IP Spoofing, Ping flood, Ping of Death, DOS, DRDOS, Stealth Scan, ICMP flooding etc.
- Advanced firewall configuration to extend the capability and security, such as Virtual



Server, Port Trigger, DMZ host, UPnP auto Forwarding, IP Filter and MAC filter.

1.3 Hardware Features

- Two 10/100Base-T(X) Ethernet ports for WAN / LAN connection individually.
- Redundant Power Inputs: 12~48 VDC on terminal block
- 4 digital inputs/outputs on terminal block
- Casing: IP-40
- Dimensions(W x D x H) : 72(W)x29.4(D)x123.4(H) mm
- Operating Temperature: -10 to 60°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing



Hardware Installation

2.1 Installation Media Gateway on DIN-Rail

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

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



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





2.2 Wall Mounting Installation

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

Step 1: Remove DIN-Rail kit.



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





The screws specification shows in the following two pictures. In order to prevent the Media Gateways from any damage, the screws should not larger than the size that used in IMG-1312-D.



ORing Industrial Networking Corp......5



Hardware Overview

3.1 Front Panel



- 1. 850/900/1800/2100MHz antenna for internal HSUPA modem
- 2. HSUPA Cellular Modem with SIM card slot
- WLAN signal strength indicator, WLAN Strength: 1<25% , 2<50%, 3<75%, 4<100%
- 4. RS-232 serial port.
- 5. WLAN Antenna
- 6. WLAN LED indicator, light up after the wireless is enable.
- LED for PWR1 and system status. When the PWR1 links, the green LED will be light on.
- 8. LED for PWR2 and system status. When the PWR2 links, the green LED will be



light on

- 9. LED for fault indicator. When fault occurred, this red LED will be light on.
- 10. LED for HSUPA modem connection.
- 11. LED of serial port. Green for transmitting, red for receiving
- 12. 10/100Base-T(X) Ethernet port

3.2 Front Panel LEDs

The following table describes the labels that stick on the IMG-1312-D.

LED	Color	Status	Description
	Green	On	WLAN activated.
VULAIN	Green	Blinking	WLAN Data transmitted.
	Groop / Pod	Green On	DC power 1 activated.
	Gleen/ Keu	Green blinking	Device booting
	Groop / Rod	Green On	DC power 2 activated.
FVVKZ	Green / Keu	Green blinking	Device booting
\wedge	Amber	On	Fault relay. Power failure or
<u>/!</u> \			Port link down.
WLAN			WLAN signal strength.
Strength	Green	On	1<25%, 2<50%, 3<75%,
oliengin			4<100%
G	Green	On	Modem Ready
Coriol	Green	Blinking	Serial port is transmitting data
Serial	Red	Blinking	Serial port is receiving data
ETH 1/2	Green/Amber	Green On/Blinking	100Mbps LNK/ACT
LIII 1/2	Green/Amper	Amber On/Blinking	10Mbps LNK/ACT



3.3 Bottom Panel

The bottom panel components of IMG-1312-D are shown as below:



3.4 Rear Panel

The rear panel components of IMG-1312-D are shown as below:

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





Cables and Antenna

4.1 Ethernet Cables

The IMG-1312-D Media Gateways have standard Ethernet ports. According to the link type, the Media Gateways use CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, Media Gateways, 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)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45

Cable Types and Specifications

100BASE-TX/10BASE-T Pin Assignments

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

RJ-45 Pin Assignments

ORing Industrial Networking Corp......9



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

The IMG-1312-D Media Gateways support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and Media Gateway. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

MDI/MDI-X pins assignment

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

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

4.2 Wireless Antenna

A 2.4GHz antenna is used for IMG-1312-D and connected with a reversed SMA connector. External antenna also can be applied with this connector.



Management Interface

5.1 First-time Installation

Before installing IMG-1312-D WLAN Media Gateway, you need to access the WLAN Media Gateway by a computer equipped with an Ethernet card or wireless LAN interface. Using an Ethernet card to connect to LAN port is easier and recommended.

Step 1: Select the Power Source

IMG-1312-D Media Gateway can be powered by +12~48V DC power input, or by P.O.E. (Power over Ethernet) PSE Ethernet switch.

Step 2: Connect a computer to IMG-1312-D

Use either a straight-through Ethernet cable or cross-over cable to connect to ETH1 of IMG-1312-D Media Gateway to a computer. If the LED of the LAN port lights up, it indicates the connection is established. After that, the computer will initiate a DHCP request to get an IP address from the Media Gateway.

Step 3: Use the web-based manager to configure IMG-1312-D

The default gateway IP of IMG-1312-D Media Gateway is 192.168.10.1. Start the web browser of your computer and type <u>http://192.168.10.1</u> in the address box to access the webpage. A login window will popup, and then enter the default login name **admin** and password **admin**.

Address 🙆 192.168.10	.1			🖌 🄁 Co
	Connect to 192.1	68.10.1	? 🛛	
		E.		
	Login			
	<u>U</u> ser name:	2	*	
	<u>P</u> assword:			
		Remember my password		
		ОК Са	ncel	
		Login		



5.2 Main Interface

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

ORING	M2M 1 Port Serial Wireless Gateway	7928
open all B Home Basic Setting C C Setting C Setting C Setting C System Tools C System Status	Firmware Ver: 1.0a Wan IP: Uptime: 00:05:14 Home Welcome to M2M 1 Port Serial Wireless Gateway configuration page.	www.oring-networking.com



In the page, you can check the Firmware version, the Media Gateway up time and the WAN IP setting.

The following table describes the labels in this .

Label	Description
Firmware	Show the current firmware version.
Uptime	Show the elapsed time since the Media Gateway is started.
Wan IP	Show the WAN IP address.

5.3.1 Basic Setting WAN

The IMG-1312-D Media Gateway provide 3G WAN connection.



Basic Setting> WAN		
WAN Settings.		
Phone Number:		
APN:		
User Name:		
Password:		
Network Select Type:	Auto 💌	
Baud Rate:	460800 💌	
PIN:	Enable PIN check before dialing	
	PIN Code:	
Auto Connect :	✓ Enable	
Reconnect on Failure:	Enable	
Fast Mode:	Enable	
Device Status :	3G modem available.	
Operations :	Connect Disconnect	
Link Status :	Connecting	
Modem Status:	Operator:	
	RadioType:	
	Signal Quality:	
Auto recheck:	00h : 00m : 00s 🗌	
	Cancel	
Save Reifesh	Cancer	

Modem/3G

The following table describes the labels in this .

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

LAN

These are the IP settings of the LAN interface for the IMG-1312-D WLAN



Media Gateway. The LAN IP address is privately for your internal network and can not be exposed on the Internet.

Basic Setting> LAN		
LAN Side settings.		
Device Name:	IMG-1312-D-321131	
IP Address: Subnet Mask:	192.168.10.1 255.255.255.0	
Apply Cancel		

LAN

The following table describes the labels in this .

Label	Description		
Device Name	Enter a name for this device		
IP Address	The IP address of the LAN interface, the default IP address is		
	192.168.10.1		
Subnet Mask	The Subnet Mask of the LAN interface, the default Subnet mask		
	is 255.255.255.0		

DHCP

DHCP stands for Dynamic Host Control Protocol. The IMG-1312-D Media Gateway with a built-in DHCP server. The internal DHCP server will assign an IP address to the computers (DHCP client) on the LAN automatically.

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

1. DHCP Sever



ORing

Basic Setting> DHCP -> DHCP Server					
Set DHCP Server.					
DHCP Server:	💿 Ena	abled 🔿 Disa	abled		
Starting IP:	192.16	8.10.2			
Ending IP:	192.16	8.10.100			
Lease Time:	48	Hours			
Local Domain Name:			(optional)		
DNS Server 1:			(optional)		
DNS Server 2:			(optional)		
WINS Server:			(optional)		
Current DHCP Client Information					
# HostName			Мас	IP	Expires In
1 *		00:1e	:94:3c:02:84	192.168.1.20	Expired
Apply Cancel					

DHCP Server

The following table describes the labels in this .

Label	Description		
DHCP Server	Enable or Disable the DHCP Server. The default setting is		
	Enable		
Starting IP	The starting IP address of the IP range for the DHCP server		
Ending IP	The ending IP address of the IP range for the DHCP server		
Lease Time	The period of time for the IP to be leased. Enter the Lease time.		
	The default setting is 48 hours.		
Local Domain Name	Enter the local domain name of private network. It is optional.		
DNS Server 1&2	Enter the DNS Server. It is optional.		
WINS Server	Enter the WINS Server. It is optional.		
Current DHCP Client	List of the computers on your network that are assigned an IP		
Information	address by internal DHCP server.		

2. IP Allocation

The IP Allocation provides one-to-one mapping of MAC address to IP address. When a computer with the MAC address requesting an IP from the IMG-1312-D Media Gateway, it will be assigned with the IP address according to the mapping. You can choose one from the client lists and add it to the mapping relationship.



Basic Setting> DHCP -> IP Allocation		
Allocate IP Address Manually.		
Choose a Client to Edit 🔽 Copy to		
MAC Address	IP Address	
		Add Clear
Static DHCP Client List:		
# MAC Address	IP Address	Operations
Delete All		

IP Allocation

The following table describes the labels in this .

Label	Description	
Choose a Client to	The list shows the MAC addresses and IP addresses that are	
Edit	already assigned by IMG-1312-D. Choose one from the list and	
	click Copy to button for editing.	
MAC Address	The MAC addresses of the computer.	
IP Address	The IP address to be related to the MAC address.	
Static DHCP Client	The list shows the MAC address and IP address one-to-one	
List	relationship.	

Wireless

Basic Setting> Wireless		
These are the basic wirele	ess settings for the Storage Router.	
Wireless:	⊙ Enabled ○ Disabled	
SSID:	oring	
Channel:	6 💌	
Security Options		
Security Type:	None	
Apply Cancel		

Wireless

The following table describes the labels in this .

Label	Description
	Service Set Identifier (SSID) is a unique name that identifies a
SSID	network. All devices on the network must set the same SSID
	name in order to communicate on the network. If you change



	the SSID from the default setting, input your new SSID name in		
	this field.		
	Channel 6 is the default channel. All devices on the network		
Channel	must share the same channel.*		
Channel	*Note: The wireless devices will automatically scan and match the		
	wireless setting of the Media Gateway with the same SSID.		
	Select the type of security for WLAN connection:		
	None: disable encryption.		
	WEP: Wired Equivalent Privacy (WEP) is a wireless security		
	protocol for WLAN. WEP provides data encryption for		
0	communicating over the WLAN.		
Security options	WPA-PSK/WPA2-PSK: WPA-PSK or WPA2-PSK with a		
	pre-shared key, each authorized computer is given the same		
	pass phrase.		
	WPA/WPA2: Wi-Fi Protected Access (WPA) authentication in		
	conjunction with a RADIUS server.		

Security Type – None

No security protection for WLAN.

Security Type – WEP

Basic Setting> Wireless		
These are the basic wireless settings for the Storage Router.		
Wireless		
wireless:		
SSID:	oring	
Channel:	6 💌	
Security Options		
Security Type:	WEP	
Auth Mode:	○ Open ○ Shared ④ WEPAUTO	
WEP Encryption:	64 Bit 💌	
Кеу Туре:	ASCII (5 characters)	
Default Key Index:	1 💌	
KEY1:		
KEY2:		
KEY3:		
KEY4:		
(Annha) (Canach)		
Appiy Cancel		
	Wireless Security Type-WEP	



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

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

Security Type – WPA-PSK/WPA2-PSK

Basic Setting> Wireless		
These are the basic wireless settings for the Storage Router.		
Wireless:	● Enabled ○ Disabled	
SSID:	oring	
Channel:	6	
Security Options		
Security Type:	WPA-PSK/WPA2-PSK 💌	
Auth Mode:	○ WPAPSK ○ WPA2PSK ④ WPAPSK/WPA2PSK mix	
Encryption Type:	○ TKIP ○ AES ③ TKIP/AES mix	
Shared Key:		

Apply Cancel

Wireless Security Type-WPA-PSK/WPA2-PSK

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

Security Type – WPA /WPA2



Basic Setting> Wirel	ess
These are the basic wire	eless settings for the Storage Router.
Wireless:	● Enabled ○ Disabled
SSID:	oring
Channel:	6
Security Options	
Security Type:	WPA/WPA2
Auth Mode:	○ WPA ○ WPA2 ④ WPA/WPA2 mix
Encryption Type:	○ TKIP ○ AES ④ TKIP/AES mix
Radius Server IP:	0.0.0
Radius Port:	1812
Shared Secret:	radius_key
Apply Cancel	

Wireless Security Type-WPA/WPA2

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

Security Type – 802.1X



Basic Setting --> Wireless

These are the basic wireless settings for the Storage Router.

Wireless:	Enabled Disabled
SSID:	
Channel:	6 V
Security Options	
Security Type:	802.1X
WEP Encryption:	64 Bit 🗸
Key Type:	ASCII (5 characters)
Default Key Index:	
KEY1:	
KEY2:	
KEY3:	
KEY4:	
Radius Server IP:	
Radius Port:	1812
Shared Secret:	radius key
	Iddius_rey

Apply Cancel

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

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

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

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





5.3.2 Serial Setting

Wireless

1. Remote Management

Ser2net Setting>Remote management		
Set the Remote Management enable DS-tool to access from WAN.		
Remote management: Port External Access:	○ Enable ④ Disable	
Port1:	○Enable ⊙Disable	
Apply Cancel		

Label	Description
Remote Management	Enable to allow DS-tool to access M2M through WAN
Port External Access	Enable to allow the serial port to be access through WAN

2. Serial Configuration



Ser2net	Setting	>	Serial	Configuration
our znet	Setting		Denui	configuration

r	
	Port1 💌
Port Alias	Port1
Interface	RS232
Baud Rate	38400 🗸
Data Bits	8 💌
Stop Bits	1 💌
Parity	None 🗸
Flow Control	None
Force TX Interval Time	0 ms
Performance	Throughput O Latency
Apply Cancel	

Label	Description
Port Alias	Remark the port to hint the connected device.
Interface	RS232 / RS422 / RS485(2-wires) / RS485(4-wires)
Baud rate	110bps/300bps/1200bps/2400bps/4800bps/9600bps/19200bps/ 38400bps/57600bps/115200bps/230400bps
Data Bits	5, 6, 7, 8
Stop Bits	1, 2 (1.5)
Parity	No, Even, Odd, Mark, Space
Flow Control	No, XON/XOFF, RTS/CTS, DTR/DSR
Force TX Interval Time	Force TX interval time is to specify the timeout when no data has been transmitted. When the timeout is reached or TX buffer is full (4K Bytes), the queued data will be sent. 0 means disable. Factory default value is 0.
Performance	Throughput: This mode optimized for highest transmission speed. Latency: This mode optimized for shortest response time.
Apply	Activate settings on this page.



3. Port Profile

Ser2net Setting> Port Configuration		
	Port1 💌	
Local TCP Port	4000	
Command Port	4001	
Mode	Serial to Ethernet	
Flush Data Buffer After	0 ms	
Delimiter(Hex 0~ff)	1: 00 2: 00 3: 00 4: 00	
Mode	Ethernet to Serial	
Flush Data Buffer After	0 ms	
Delimiter(Hex 0~ff)	1: 00 2: 00 3: 00 4: 00	
Apply Cancel		

Label	Description
	Flush Data Buffer After:
	The received data will be queued in the buffer until all the delimiters are
	matched. When the buffer is full (4K Bytes) or after "flush S2E data buffer"
	timeout, the data will also be sent. You can set the time from 0 to 65535
Sorial to Ethornat	seconds.
Senar to Ethernet	
	Delimiter:
	You can define max. 4 delimiters (00~FF, Hex) for each way. The data will be
	hold until the delimiters are received or the option "Flush Serial to Ethernet
	data buffer" times out. 0 means disable. Factory default is 0
	Flush Data Buffer After:
	The received data will be queued in the buffer until all the delimiters are
	matched. When the buffer is full (4K Bytes) or after "flush E2S data buffer"
	timeout, the data will also be sent. You can set the time from 0 to 65535
Ethornot to sorial	seconds.
Ethemet to senal	
	Delimiter:
	You can define max. 4 delimiters (00~FF, Hex) for each way. The data will be
	hold until the delimiters are received or the option "Flush Ethernet to Serial
	data buffer" times out. 0 means disable. Factory default is 0

4. Service Mode --- Virtual COM Mode



In Virtual COM Mode, the driver establishes a transparent connection between host and serial device by mapping the Port of the serial server serial port to local COM port on the host computer. Virtual COM Mode also supports up to 5 simultaneous connections, so that multiple hosts can send or receive data by the same serial device at the same time.

Ser2net Setting> Service Mode	
	Port1 V
Data Encryption	© Enable ● Disable
Service Mode	Virtual COM Mode 💌
Idle Timeout	0 (0~65535)seconds
Alive Check	40 (0~65535)seconds
Max Connection	1 v max. connection (1~5)
Apply Cancel	

Label	Description
Data Encryption	Use SSL to encrypt data.
	When serial port stops data transmission for a defined period of time (Idle
	Timeout), the connection will be closed and the port will be freed and try to
Idle Timeout	connect with other hosts. 0 indicate disable this function. Factory default
	value is 0. If Multilink is configured, only the first host connection is effective for
	this setting.
	The serial device will send TCP alive-check package in each defined time
Alive Check	interval (Alive Check) to remote host to check the TCP connection. If the TCP
	connection is not alive, the connection will be closed and the port will be freed.
	0 indicate disable this function. Factory default is 0.
Max Connection	The number of Max connection can support simultaneous connections are 5,
	default values is 1.

*Not allowed to mapping Virtual COM from web

5. Service Mode – TCP Server mode



Ser2net Setting --> Service Mode

	Port1 V
Data Encryption	○ Enable
Service Mode	TCP Server Mode 💌
Telnet Negotiation	○ Enable ④ Disable
TCP Server Port	4000
Idle Timeout	0 (0~65535)seconds
Alive Check	40 (0~65535)seconds
Max Connection	1 v max. connection(1~5)

Apply Cancel

In TCP Server Mode, DS is configured with a unique Port combination on a TCP/IP network. In this case, DS waits passively to be contacted by the device. After the device establishes a connection with the serial device, it can then proceed with data transmission. TCP Server mode also supports up to 5 simultaneous connections, so that multiple device can receive data from the same serial device at the same time.

Label	Description
Data Encryption	Use SSL to encrypt data.
Telnet	Full Telnet command / symbol compatible
Negotiation	
TCP Server Port	Set the port number for data transmission.
	When serial port stops data transmission for a defined period of time (Idle
	Timeout), the connection will be closed and the port will be freed and try to
Idle Timeout	connect with other hosts. 0 indicate disable this function. Factory default
	value is 0. If Multilink is configured, only the first host connection is effective for
	this setting.
	The serial device will send TCP alive-check package in each defined time
Alive Check	interval (Alive Check) to remote host to check the TCP connection. If the TCP
Alive Check	connection is not alive, the connection will be closed and the port will be freed.
	0 indicate disable this function. Factory default is 0.
May Copposition	The number of Max connection can support simultaneous connections are 5,
IVIAX CONNECTION	default values is 1.

6. Service Mode – TCP Client Mode

In TCP Client Mode, device can establish a TCP connection with



server by the method you set (Startup or any character). After the data has been transferred, device can disconnect automatically from the server by using the TCP alive check time or Idle timeout settings.

Ser2net Setting> Service Mo	ode		
	Port1 💌		
Data Encryption	○ Enable		
Service Mode	TCP Client Mode		
Destination Host	0.0.0.0 : 4000		
Idle Timeout	0 (0~65535)seconds		
Alive Check	40 (0~65535)seconds		
Connect on	● Startup ○ Any Character		
Destination Host	Port		
1.	65535		
2.	65535		
3.	65535		
4.	65535		
Apply Cancel			

Label	Description	
Data Encryption	Use SSL to encrypt data.	
Destination Host	Set the IP address of host and the port number of data port.	
	When serial port stops data transmission for a defined period of time (Idle	
	Timeout), the connection will be closed and the port will be freed and try to	
Idle Timeout	connect with other hosts. 0 indicate disable this function. Factory default	
	value is 0. If Multilink is configured, only the first host connection is effective for	
	this setting.	
	The serial device will send TCP alive-check package in each defined time	
Alive Check	interval (Alive Check) to remote host to check the TCP connection. If the TCP	
Allve Check	connection is not alive, the connection will be closed and the port will be freed.	
	0 indicate disable this function. Factory default is 0.	
Connect on	The TCP Client will build TCP connection once the connected serial device is	
Startup	started.	
Connect on Any	The TCP Client will build TCP connection once the connected serial device	
Character starts to send data.		

7. Service Mode – UDP Mode

Compared to TCP communication, UDP is faster and more efficient.



In UDP mode, you can Uni-cast or Multi-cast data from the serial device server to host computers, and the serial device can also receive data from one or multiple host

Ser2net Setting> Service Mode					
	Port1 💌				
Service Mode	UDP Mode 🗸				
Listen Port	4000				
Host start IP	Host end IP	Send Port			
1.		65535			
2.		65535			
3.		65535			
4.		65535			
Apply Cancel					

5.3.3 Advanced Setting

Wireless

1. Parameters

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

Parameters

The following table describes the labels in this .

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 connection.					
	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					
D I IM Interval	multicast messages. When the AP has buffered broadcast or					
	multicast messages for associated clients, it sends the next DTIM					
	with a DTIM Interval value. Its clients hear the beacons and					
	awaken to receive the broadcast and multicast messages.					
	This value should remain at its default setting of 2346. The					
	range is 256-2346 bytes. It specifies the maximum size for a					
F	packet before data is fragmented into multiple packets. If you					
Fragmentation	experience a high packet error rate, you may slightly increase the					
Inresnoid	Fragmentation Threshold. Setting the Fragmentation Threshold					
	too low may result in poor network performance. Only minor					
	modifications of this value are recommended.					
	This value should remain at its default setting of 2347. The					
	range is 0-2347 bytes. Should you encounter inconsistent data					
	flow, only minor modifications are recommended. If a network					
	packet is smaller than the preset RTS threshold size, the					
RTS Threshold	RTS/CTS mechanism will not be enabled. The AP sends					
	Request to Send (RTS) frames to a particular receiving station					
	and negotiates the sending of a data frame. After receiving an					
	RTS, the wireless station responds with a Clear to Send (CTS)					
	frame to acknowledge the right to begin transmission.					
	This value ranges from 1 - 100 percent, default value is 100					
	percent. A safe increase of up to 60 percent would be suitable					
Xmit Power	for most users. Higher power settings are not recommended for					
	users due to excess heat generated by the radio chipset, which					
	can affect the life of the AP.					
	If you have IEEE802.11g and IEEE802.11b devices in your					
Wireless Network	network, then keep the default setting, BG Mixed mode . If you					
Mode	have only IEEE802.11g devices, select G Mode. If you would					
	like to limit your network to only IEEE802.11b devices, then					
	select B Mode .					



	The default setting is Auto. The range is from 1 to 54Mbps.				
Transmission Rate	The rate of data transmission should be set depending on the				
	speed of your wireless network. You can select from a range of				
	transmission speeds, or keep the default setting, Auto, to have				
	the AP automatically use the fastest possible data rate and				
	enable the Auto-Fallback feature. Auto-Fallback will negotiate				
	the best and possible connection speed between the AP and a				
	wireless client.				
	Values are Long and Short, default value is Long. If your				
Descentio	wireless device supports the short preamble and you are having				
Preamble	trouble getting it to communicate with other IEEE802.11b				
	devices, make sure that it is set to use the long preamble				
	When wireless clients survey the local area for wireless networks				
	to associate with, they will detect the SSID broadcast by the AP.				
SSID Broadcast	To broadcast the AP SSID, keep the default setting, Enable. If				
	you do not want to broadcast the AP SSID, then select Disable .				

2. MAC Filter

Use **MAC Filter** to allow or deny wireless clients to associate with IMG-1312-D Media Gateway. You can manually add a MAC address or select the MAC address from **Associated Clients** that are currently associated with IMG-1312-D.



Filters are used to a	llow or de	eny Wireless Clients users fr	om accessing the AP R	outer.
MAC Filter:	O Ena	abled 💿 Disabled		
Options Only allow MAG Only deny MAG	C address C address	s(es) listed below to connect s(es) listed below to connect	to AP to AP	
Associated Clients:	- Choo	ose an Associated Client – 💌	Copy to Slot Che	oose 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.

MAC Filter

The following table describes the labels in this .

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

NAT Setting

1. Virtual Server

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



Adva	nced Setting> NAT Set	ting -> Virtu	al Server					
Virtu	al server settings.							
Virtu	al Server: (🖲 Enable 🔿	Disable					
Desc	ription:							
Publi	c IP:	All 🔿 Spe	cify					
Publi	c Port:							
Proto	ocol:		DP 🔿 Both					
Loca	IP:							
Loca	Port:							
Enab	le Now: (Yes 🔿 No)					
	C	Add Car	icel					
Virtu	al server list:							
#	Description	Public IP	Public Port	Protocol	Local IP	Local Port	Enabled	Ops
1	Oring	All	21	ТСР	192.168.0.1	21	•	Edit Del

Virtual Server

The following table describes the labels in this .

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

2 Port Trigger

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





Advanced Setting>	NAT Setting ->	Port Trigger						
Port Trigger settings.								
Port Trigger:	Enal	Enable 🔿 Disable						
Description:								
Trigger Port:								
Trigger Protocol:	⊙ TCP	⊙ TCP ○ UDP ○ Both						
Incoming Port:								
Incoming Protocol:	⊙ TCP		th					
Enable:	Yes	⊙ Yes 🔿 No						
	Add	Cancel						
Port Trigger List:								
# Descript	tion	Trigger Protocol	Trigger Port	Incoming Protocol	Incoming Port	Enable	Ops	
1 Oring)	ТСР	100	ТСР	100-200	✓	Edit Del	

Port Trigger

The following table describes the labels in this .

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

3. DMZ

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

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



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

DMZ

The following table describes the labels in this .

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

4. UPnP

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

Advanced	Advanced Setting> NAT Setting -> UPnP					
UPnP setti	ngs.					
UPnP:	 Enabled O Disabled Enable NAT-PMP 					
UPnP List:						
#	Application	Ext Port	Protocol	Int Port	IP Address	
Apply	Cancel					

UPnP

The following table describes the labels in this .

Label	Description
UPnP	Enable or disable UPnP.



Enable NAT-PMP	NAT-PMP allows a computer in a private network (behind a NAT			
	Media Gateway) to automatically configure the Media Gateway to			
	allow parties outside the private network to contact with each			
	other. NAT-PMP operates with UDP. It essentially automates			
	the process of port forwarding. Check the box to enable			
	NAT-PMP.			
UPnP List	This table lists the current auto port forwarding information.			
	Application: The application that generates this port forwarding.			
	Ext Port: The port opened on WAN side.			
	Protocol: The protocol type.			
	Int Port: The port redirected to the local computer.			
	IP Address: The IP address of local computer to be redirected to.			
	Status: This status shows if the entry is valid or not.			

Security Setting

1. IP Filter

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

Adva	Advanced Setting> Security Setting -> IP Filter								
IP filt	er settings.								
IP Fil	ter:	C	○ Enable ④ Disable						
Desc	ription:]				
Rule:		[DROP 🔽						
Direc	tion:	l	AN->WAN 🔽						
IP Ad	ldress:	S	ource IP:						
		D	estination IP:						
Proto	ocol:		All						
			ICMP						
			Specify proto	ocol number:					
		C	ТСР	Specify port	:				
			UDP	Specify port	:				
Enab	le Now:	(Yes 🔿 No						
			Add Cance	el					
IP filt	er list:								
#	Description	Rule	Direction	Source IP	Destination IP	Protocol	Port	Enabled	Operations
				IP Filt	er				
-	The fellow:	na tabla	doooribood	ha lahala in th	:-				
	The followi	ng table	uescribes t	the labels in th	15.				

5	
Label	Description



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

2. MAC Filter

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

Advanced Setting> Security Setting -> MAC Filter						
MAC Filter sett	ings.					
MAC Filter:	0	○ Enable ④ Disable				
Description:						
Rule:	DF	DROP V				
MAC Address:		(e.x. 00:11:22:aa:bb:cc)				
Enable Now:	۲	◎ Yes ○ No				
	A	dd Cancel				
MAC filter list:						
#	Description	Rule	MAC Address	Enabled	Operations	



The following table describes the labels in this .

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

VPN Setting

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



protocols, encryption algorithms, and hashing algorithms.

1. Open VPN

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

Advanced Setting> Vp	n Setting -> Openvpn
Openvpn settings.	
Server settings.	
Openvpn Server:	○ Enable ④ Disable
Tunnel Protocol:	
Port:	1194
LZO Compression:	• Enable O Disable
Keys Setting:	Auto 💙
Diagnosis	
Client settings.	
Openvpn Client:	○ Enable ④ Disable
Server IP/Host Name:	
Tunnel Protocol:	
Port:	1194
LZO Compression:	• Enable
Keys Setting:	Auto 💟
Diagnosis	

Open VPN

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

1: Open VPN Server





Connection to Open VPN Server

Before connecting to the Openvpn server of IMG-1312-D AP routuer, please install openvpn client software for your windows PC. It can be downloading from http://openvpn.net/download.html#stablel. The current version of Openvpn used in IMG-1312-D is version 2.0.9. The corresponding software for client should be installed. The following table describes the labels in this .

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

2: Open VPN Client

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

The following table describes the labels in this .

Label	Description	
Open VPN Client	Enable or disable the function of Open VPN Client.	You can
	allow or deny the Open VPN Client with this option.	



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



3: Open VPN Server VS Client



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

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

2. PPTP VPN

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

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



Advanced Setting>	Vpn Setting -> PPTP Vpn
PPTP Server settings.	
PPTP Server	⊙ Enable ⊖ Disable
Server IP :	192.168.1.1
Clients IP:	192.168.1.150-180
PPP Options:	C require-chap
	🗌 require-mschap
	✓ require-mschap-v2
	✓ require-mppe
Routing Option:	$\hfill\square$ Enable Routing Protocols through PPTP VPN Connection
CHAP-Secrets:	admin * admin *
Apply Cancel	

PPTP VPN

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





The following table describes the labels in this .



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

3. PPTP Client

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

Advanced Setting> Vpn Setting -> PPTP Client		
PPTP Client settings.		
PPTP Client	O Enable 💿 Disable	
Server IP/Hostname:	118.165.230.208	
Username:	admin	
Password:	admin	
Options:	Reconnect on failure	
	default route	
	require-chap	
	require-mschap	
	require-mschap-v2	
	require-mppe	
Routing Option:	Enable Routing Protocols through PPTP	Client Connection
Operations:	Connect Disconnect	
Link Status:	Disconnected	
Save Cancel		





Result: Client-PC can connect to Server-PC, WAN-PC.

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



Routing Setting

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

Advanced Setting> Routing Protocol -> Routing Setting						
Current Routing Table:						
Destination	Gateway	Subnet Mask	Metric		Interface	
192.168.10.0	0.0.00	255.255.255.0	0		br0(LAN)	
127.0.0.0	0.0.00	255.0.0.0	0	le	O(LOOPBACK	()
Static Route Entry:						
Destination	Gateway	Subnet Mask	Metric	Interface	Oper	ations
Destination	Gateway	Subnet Mask	Metric	Inter	face	Operation
				WAI	V 💌	Add
Mode:	Router 💌					
RIPv1 & v2:	Disable 🔽					
Telnet Setting:	💿 Enable 🔘 Disable					
	Port: 23					
	Password:					
Apply Cancel						

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

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



🔤 Telnet 192	2. 168. 10. 1
: Command inc	complete.
Hello, this i Copyright 199	s zebra (version 0.94). 26-2002 Kunihiro Ishiguro.
[APR654978>	
enable	Turn on privileged mode command
exit	Exit current mode and down to previous mode
list	Print command list
ping	send echo messages
quit	Exit current mode and down to previous mode
show	Show running system information
telnet	Open a telnet connection
traceroute	Trace route to destination

Notification

1. Email/SNMP/Syslog

Email Settings

Advanced Setting --> Notification --> Email/SNMP/Syslog

Email settings.	
SMTP Server:	(optional)
Server Port:	25 (0 represents default)
	My Server requires authentication
User Name	
Password	
Sender Address:	
E-mail Address 1:	
E-mail Address 2:	
E-mail Address 3:	
E-mail Address 4:	

Email Settings

The following table describes the labels in this .

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



SNMP Settings

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

SNMP Settings

The following table describes the labels in this .

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

Syslog Server Settings

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

Syslog Server

The following table describes the labels in this .

Label	Description



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

2. System Event

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

System Event Configuration.			
Device Event Notification.			
Hardware Reset (Cold Start)	SMTP Mail	SNMP Trap	Syslog
Software Reset (Warm Start)	SMTP Mail	SNMP Trap	Syslog
Login Failed	SMTP Mail	SNMP Trap	Syslog
WAN IP changed	SMTP Mail	SNMP Trap	Syslog
Password Changed	SMTP Mail	SNMP Trap	Syslog
Redundant Power Changed	SMTP Mail	SNMP Trap	Syslog
Eth Link Status Changed	SMTP Mail	SNMP Trap	Syslog
SNMP Access Failed	SMTP Mail	SNMP Trap	Syslog
Wireless Client Associated	SMTP Mail	SNMP Trap	Syslog
Wireless Client Disassociated	SMTP Mail	SNMP Trap	Syslog
Fault Event Notification and Fault L	ED/Relay.		
Power 1 Fault SMTP Mail	SNMP Trap	Syslog	Fault LED/Relay
Power 2 Fault SMTP Mail	SNMP Trap	Syslog	Fault LED/Relay
Eth1 Link Down SMTP Mail	SNMP Trap	Syslog	Fault LED/Relay
Eth2 Link Down SMTP Mail	SNMP Trap	Syslog	Fault LED/Relay
Serial Port Event Notification.	_		
Serial Port Event Notification. DCD Changed	SMTP Mail	SNMP Trap	Syslog
Serial Port Event Notification. DCD Changed DSR Changed	SMTP Mail	SNMP Trap	Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed	SMTP Mail SMTP Mail	SNMP Trap	Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed	SMTP Mail SMTP Mail SMTP Mail	SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected	SMTP Mail SMTP Mail SMTP Mail SMTP Mail SMTP Mail	SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected	SMTP Mail	SNMP Trap	Syslog Syslog Syslog Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected	SMTP Mail SMTP Mail SMTP Mail SMTP Mail SMTP Mail SMTP Mail	 SNMP Trap 	Syslog Syslog Syslog Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected DIDO Event Notification.	SMTP Mail SMTP Mail SMTP Mail SMTP Mail SMTP Mail SMTP Mail	SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog Syslog Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected DIDO Event Notification. DI1 SMTP Mail	SMTP Mail SMTP Mail SMTP Mail SMTP Mail SMTP Mail SMTP Mail	SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog Syslog Syslog Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected DIDO Event Notification. DI1 SMTP Mail DI2 SMTP Mail DI3 SMTP Mail	SMTP Mail	SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected DIDO Event Notification. DI1 SMTP Mail DI2 SMTP Mail DI3 SMTP Mail DI4 SMTP Mail	SMTP Mail	SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected DIDO Event Notification. DI1 SMTP Mail DI2 SMTP Mail DI3 SMTP Mail DI4 SMTP Mail DO1 SMTP Mail	SMTP Mail SMTP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected DIDO Event Notification. DI1 SMTP Mail DI2 SMTP Mail DI3 SMTP Mail DI4 SMTP Mail DO1 SMTP Mail DO2 SMTP Mail	SMTP Mail SMTP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog Syslog
Serial Port Event Notification. DCD Changed DSR Changed RI changed CTS Changed Port Connected Port Disconnected DIDO Event Notification. DI1 SMTP Mail DI2 SMTP Mail DI3 SMTP Mail DI4 SMTP Mail DO1 SMTP Mail DO2 SMTP Mail DO3 SMTP Mail	SMTP Mail SMTP Trap SNMP Trap	SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap SNMP Trap	Syslog Syslog

System Event

System events record the activities of the Wireless Media Gateway system. When the setting changes or action performs, the event will be sent to administrator by email.



A trap will also be sent to SNMP trap server. The Syslog will record the event locally and may send the Syslog remotely to a Syslog server. If serious event occurred, such as the power failure or link down, the fault led will be switched on as warning indication.

Miscellaneous (DDNS)

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

Advanced Setting> Miscellaneous> DDNS		
DDNS settings.		
DDNS Service:	www.dyndns.org	
User Name:		(*)
Password:		(*)
Domain:		(*)
,		
Apply Cancel		

The following table describes the labels in this .

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

5.3.4 System Tools

Date & Time

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



System Tools> Date & Time		
Date/Time settings.		
Local Date:	2008 Year 01 Month 01 Day	
Local Time:	08 Hour 14 Minute 25 Second	
Time Zone:	GMT+08:00 💌	
	Get Current Date & Time from Browser	
NTP:	🕑 Enable	
NTP Server 1:	pool.ntp.org	
NTP Server 2:	time.nist.gov (optional)	
Synchronise:	Every Day 💙 at 00 💙 : 00 💙	
Apply Cancel		

Date & Time

The following table describes the labels in this .

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

Login Setting

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



System Tools> Login Setting		
Login settings.		
Old Login Name:	admin	
Old Password:	•••••	
New Login Name:	admin	
New Password:	••••	
Confirm New Password:	••••	
Web Protocol: Port:	 нттр О нттрз 80 	
Apply Cancel		

Login Setting

The following table describes the labels in this .

Label	Description
Old Name	This field shows the old login name.
Old Password	Before making a new setting, you should provide the old
	password for verification. Acceptable characters of this field
	contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15
	characters in length. An empty password is also acceptable.
New Name	Enter a new login name. Acceptable characters of this field
	contains '0-9', 'a-z', 'A-Z' and must be between 1 to 15
	characters in length. An empty name is not acceptable.
New Password	Enter a new login password. Acceptable characters of this
	field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15
	characters in length.
Confirm New Password	Retype the password to confirm it. Acceptable inputs of this
	field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15
	characters in length.
Web Protocol	Choose the web management page protocol. HTTP and
	HTTPS are both supported.
Port	Choose the web management page port number. For HTTP,
	default port is 80; For HTTPS, default port is 443.

HTTPS (HTTP over SSL) is a Web protocol which encrypts and decrypts user page



requests as well as the pages that are returned by the Web server.

Media Gateway Restart

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

System Tools> Router Restart		
Router Restart Utility.		
Restart Now		
Scheduling:	Enable	
	Restart Every Day at 00 💌 : 00 💌	
Apply Cancel		

Media Gateway Restart

Firmware Upgrade

System Tools> Firmware Upgrade	
Do NOT power off the router while upgrading! Current Firmware Version: 1.0a	
Upgrade Mode:	Web Upgrade 💌
選擇檔案 Start Web Upgrade	

Firmware Upgrade

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

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



Save/Restore Configurations



Save/Restore Configurations

The following table describes the labels in this .

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

Miscellaneous (Ping)

System Tools> Miscellaneous			
Miscellaneous utilities.			
Ping Test: Ping Test Result:	Destination:		Ping

Miscellaneous

The Ping Test is used to send Ping packets to test if a computer whether it is on the



Internet or test if the WAN connection is OK. Enter a domain or IP in the destination box and click Ping to test.

5.3.5 System Status

System Info

System Status> Syste	m Info		
System Info.			
Model:	IMG-1312-D		
Model Description:	M2M 1 Port Serial Wireless	M2M 1 Port Serial Wireless Gateway	
WAN:	Mode	Modem/3G	
LAN:	IP Address Subnet Mask MTU MAC Address DHCP Server	192.168.10.1 255.255.255.0 1500 00:13:21:32:11:31 Enabled	
Wireless:	Wireless SSID Channel Encryption Mode MAC Address	Enabled oring 6 None 00:0E:8E:61:D2:14	

System Info

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

System Log

System Status> System Log					
System log.					
Log Option:	 DHCP Server NTP Client System Event Firewall Select All 	OpenVpn PPTP VPN UPNP Modem Deselect All	Save	e Option	
System Log:				Refresh	Clear Logs
# Date Time	Item		Content		
Apply Cancel					

System Log

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



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

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

Traffic Statistics

System Status> Traffic Statistics		
Traffic statistics.		
Interface	Send	Receive
Wired LAN	152103 Bytes (330 Packets)	97653 Bytes (870 Packets)
WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)
Wireless LAN	130100 Bytes (1096 Packets)	0 Bytes (0 Packets)

Refresh

Traffic Statistics

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



Technical Specifications

ORing M2M Model	IMG-1312-D	
Physical Ports		
10/100 Base-T(X) Ports in RJ45 Auto MDI/MDIX	2	
SIM card slot	1	
Cellular interface		
Cellular Standard	GSM / GPRS / EGPRS / EDGE / WCDMA / HSDPA / HSUPA	
Band options	Dual band : HSUDPA 1900 / 2100 MHz Quad band : GSM / GPRS / EDGE 850 / 900 / 1800 / 1900 MHz / WCDMA / HSDPA 850 / 900 / 1900 / 2100MHz	
Antenna Connector	Reverse SMA connector x1	
Antenna	GSM/DCS/UMT 3G antenna x1	
WLAN Feature		
Antenna Connector	Reverse SMA connector x1	
Antenna	2.4GHz Wi-Fi ANT x1	
Radio Frequency Type	DSSS	
Modulation	IEEE802.11b: CCK, DQPSK, DBPSK	
modulation	IEEE802.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM	
Frequency Band	Europe CE/ETSI: 2.412~2.402 GHz (11 channels)	
Transmission Rate	IEEE802.11b: 1/ 2/ 5.5/ 11 Mbps	
II dhamaalon Kate	IEEE802.11g: 6/ 9/ 12/ 18/ 24/ 36/ 48/ 54 Mbps	
Transmit Power	IEEE802.11b/g: 18dBm	
Receiver Sensitivity	-81dBm @ 11Mbps, PER< 8%	
Encryption Security	WEP: (64-bit ,128-bit key supported) WPA: WPA2 : 802.11i(WEP and AES encryption) WPAPSK (256-bit key pre-shared key supported) 802.1X and Radius supported TKIP encryption	
Wireless Security	SSID broadcast disable	
Serial Ports		
Connector	DB9 male x 1	
Operation Mode	RS-232/RS-422/RS-485(2W/4W). Which can be configured by utility	
Serial Baud Rate	110 bps to 460.8 Kbps	
Data Bits	5, 6, 7, 8	
Parity	odd, even, none, mark, space	
Stop Bits	1, 1.5, 2	
Serial signals	RS-232 : TxD, RxD, DCD, RTS, CTS, DSR, DTR, RI, GND RS-422 : TX+, TX-, RX+, RX-, GND RS-485 (2W): D+, D-, GND RS-485 (4W): TX+, TX-, RX+, RX-, GND	



Digital Input / output	
Digital input	4 digital inputs on terminal block.
	Power input voltage: 5V TTL
Digital output	4 digital outputs on terminal block.
5	Power output voltage: 5V TTL
LED Indicators	
Power indicator	Green On: Power is on and functioning Normally.
10/100TX RJ45 port indicator	Green for port Link/Act.
WLAN indicator	WLAN Link /ACT: Green: Link
Power	
Power Input	Dual DC inputs. 12-48VDC on 6-pin terminal block
Power consumption (Typ.)	6.5 Watts
Overload current protection	Present
Reverse polarity protection	Present
Physical Characteristic	
Enclosure	IP-40
Dimension (W x D x H)	41 (W)x 114 (D)x153 (H) mm (1.61 x4.48 x6.02 inch.)
Weight (g)	602 g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-10 to 60°C (14 to 140°F)
Operating Humidity	5% to 95% Non-condensing
Regulatory Approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	3 years