IMG-111

Industrial M2M Gateway

User's Manual

Version 1.0

January, 2013

www.oring-networking.com

ORing Industrial Networking Corp.

COPYRIGHT NOTICE

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: support@oring-networking.com

Sales Contact

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

Tables of Contents

Getting to Know your M2M Gateway

1.1 Overview

The ORing IMG-111 M2M Gateway is designed to operate in industrial environment. The M2M Gateway provides a fast and effective ways of communicating to the internet over wired LAN. And also include a RS-232 interface which allow user to get the RS-232 data through 3G.connection.

With built-in HSUPA WAN connection the ORing IMG-111 M2M Gateway can be mounted in harsh environment easily to provide internet access anytime and anywhere.

The ORing IMG-111 M2M 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

- Secured Management by HTTPS
- Intuitive Web-based management user interface for simply and easily operation.
- 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, 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.
- Event Warning by Syslog and Relay
- Serial Data Encryption with SSL for Security data transfer.
- Redundant multiple host devices: 5 simultaneous in Virtual COM, TCP Server, TCP Client mode, UDP
- Versatile Modes: Virtual Com, Serial Tunnel, TCP Server, TCP Client, UDP
- Various Windows O.S. supported: Windows NT/2000/ XP/ 2003/VISTA / Server 2008 / Windows 7 and Windows 8

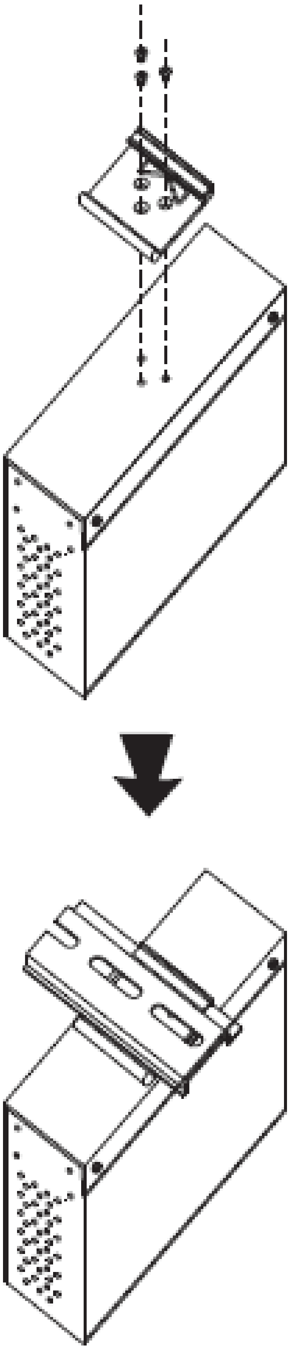
1.3 Hardware Features

- Built-in HSUPA Cellular Modem with SIM card slot included for WAN connection (IR-710)
- USB port for installing user-selectable 3G USB modem for WAN connection (IR-711UB)
- 10/100Base-T(X) Ethernet ports for LAN connection individually.
- 1 RS-232 Interface
- Power Inputs: 12~48 VDC
- Casing: IP-30
- Operating Temperature: -10 to 60 ^{o}C
- Storage Temperature: -40 to 85^{o}C
- Operating Humidity: 5% to 95%, non-condensing

Hardware Installation

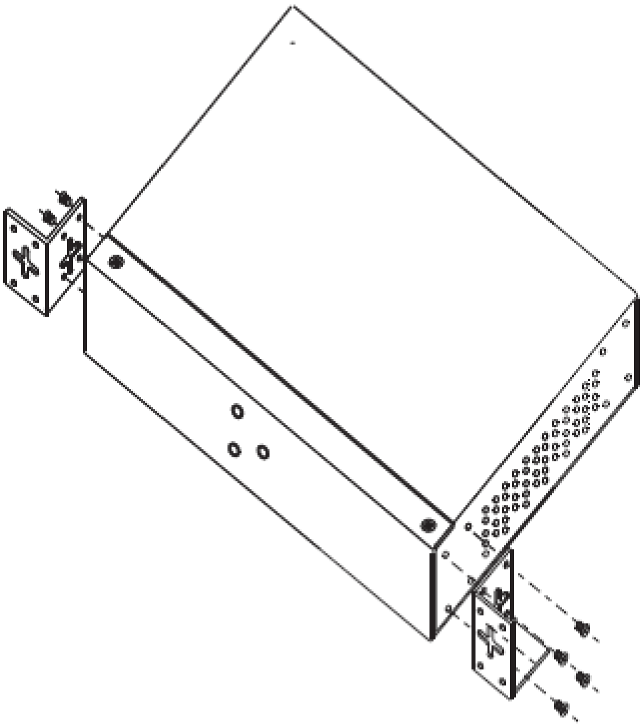
2.1 DIN-Rail Installation

IMG-111 has DIN-Rail Kit on rear panel. The DIN-Rail kit helps IMG-111 to fix on the DIN-Rail. It is easy to install the M2M Gateway on the DIN-Rail.



2.2 Wall-Mounted Installation

IMG-111 has another installation method to secure the M2M Gateway. A wall mount panel can be found in the package.

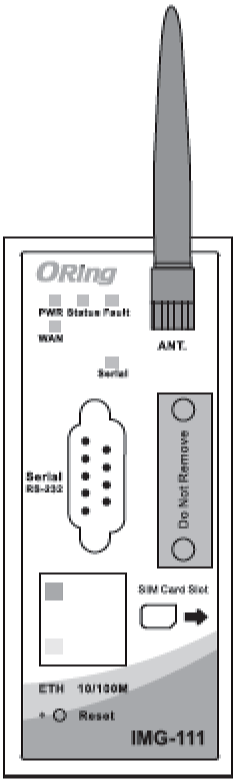


2.3 SIM Card Installation

With IR-710 POWERED DOWN :

1. Un-fasten the screws.
2. Remove the cover.
   (NOTE : The cover removal is only for SIM card installation. DO NOT remove the cover in normal operation.)
3. Install SIM card into its slot.
4. Replace the cover.
5. Fasten the screws.

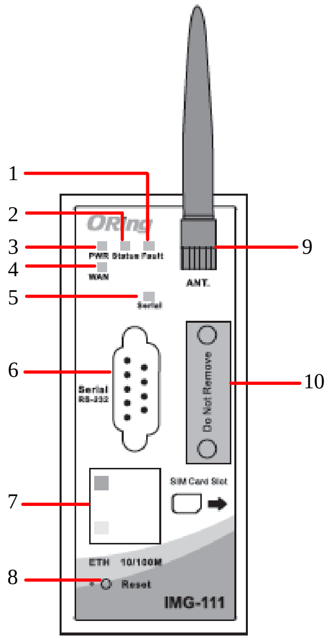
Important Notice: POWER DOWN THE IMG-111 BEFORE INSTALLING SIM CARD.



Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the IMG-111



1. Fault LED. .
2. Status LED
3. Power LED
4. WAN LED
5. Serial Transmition LED
6. RS-232 Serial port.
7. 10/100Base-T(X) RJ45 fast Ethernet port
8. Reset button
9. 850/900/1800/2100MHz antenna for internal HSUPA modem
10. SIM card slot

3.2 Front Panel

LED	Color	Status	Description
PWR	Green	Green On	Power On.
Status	Green	Green On	Device Ready
		Green Blinking	Booting up
Fault	Amber	Amber On	WAN connection fail (enable event through web)
WAN	Green	Green On	Modem Ready
		Green Blinking	Checking Modem status
ETH	Amber	Amber On	Port speed to 10Base-T
	Green	Green On	Port speed to 100Base-TX

Cables and Antenna

4.1 Ethernet Cables

The IMG-111 M2M Gateway has one 10/100Base-T(X) Ethernet ports. According to the link type, use CAT 3, 4, 5,5e UTP cables to connect to any other network device (PCs, servers, switches, M2M Gateways, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10Base-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ45
100Base-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ45

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

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

RJ45 Pin Assignments

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

The IMG-111 M2M Gateways supports auto MDI/MDI-X operation. You can use a straight-through cable to connect PC.The following table below shows the 10Base-T/ 100Base-T(X) 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.

4.3 Wireless Antenna

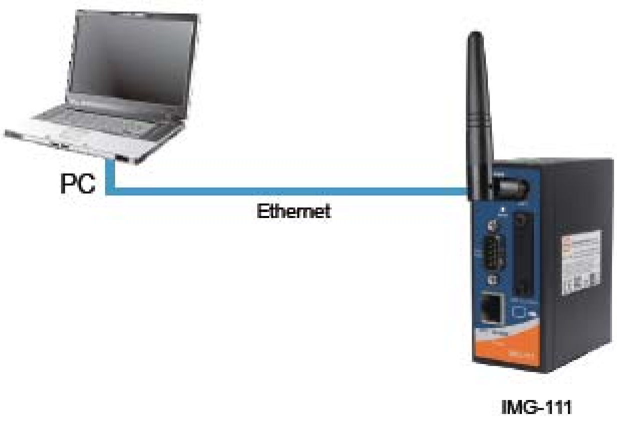
850/900/1800/2100MHz antenna is used for built-in HSUPA modem. External RF cable and antenna also can be applied with this connector.

Cellular Antenna

Management Interface

5.1 First-time Installation

Before installing IMG-111 M2M Gateway, you need to access the M2M Gateway by a computer equipped with an Ethernet card. Using an Ethernet card to connect to LAN port is easier and is recommended.



Step 1: Select the Power Source

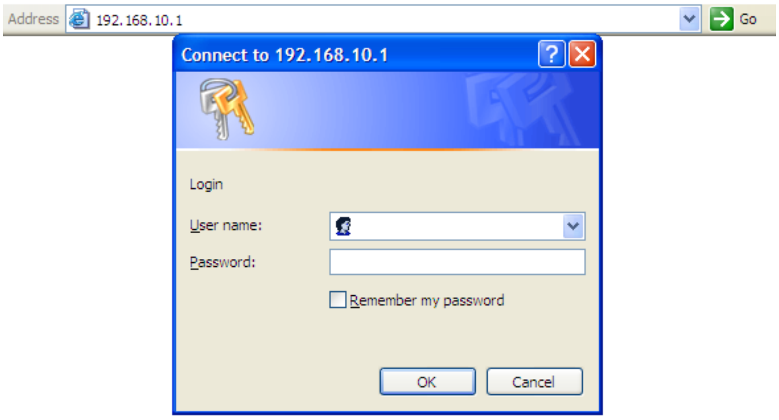
IMG-111 M2M Gateway can be powered by +12~48V DC power input.

Step 2: Connect a computer to IMG-111

Use either an Ethernet cable to connect to ETH of IMG-111 M2M 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 M2M Gateway.

Step 3: Use the web-based manager to configure IMG-111

The default gateway IP of IMG-111 M2M Gateway is 192.168.10.1. Start the web browser of your computer and type http://192.168.10.1 in the address box to access the webpage. A login window will popup, and then enter the default login name **admin** and password **admin.**

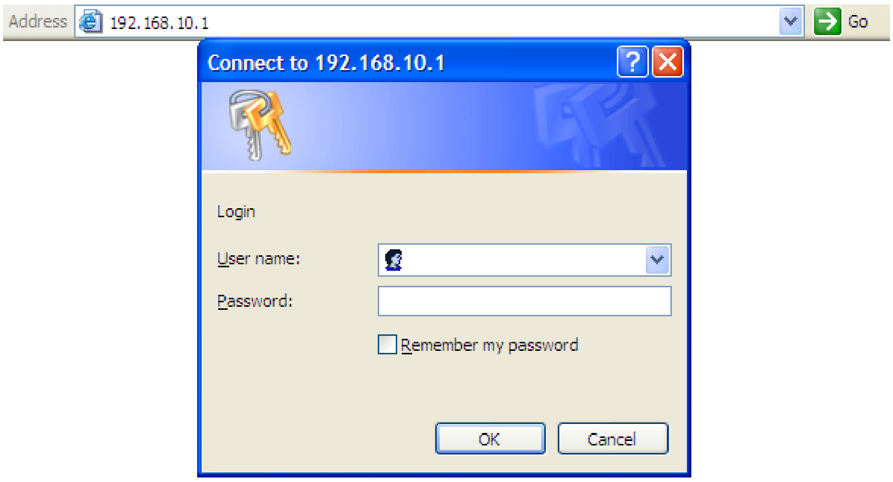


Login screen

5.2 M2M Gateway Configuration

In this section, the web management page will be explained in detail.

With default setting, you can type http://192.168.10.1 in the address box of web browser to login the web management interface. A login window will be prompted, enter username **admin** & password **admin** to login.

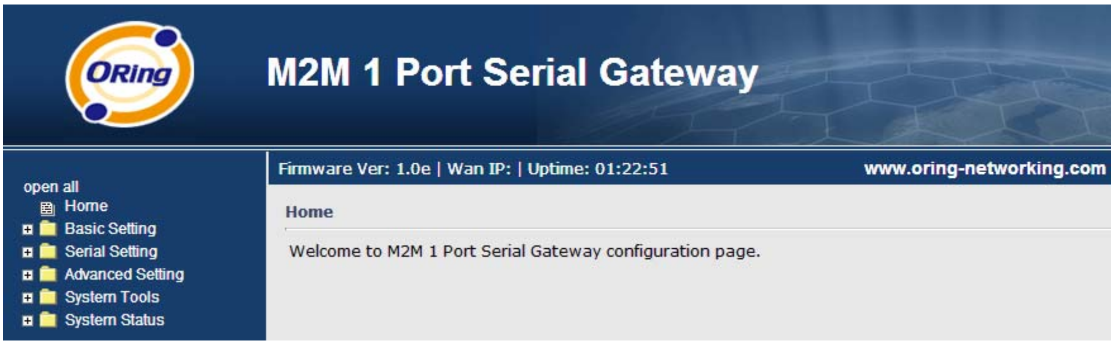


Login screen

For security reasons, we strongly recommend you to change the password. Click on **System Tools > Login Setting** and change the password.

5.3 Main Interface

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



Firmware Ver: 1.0e | Wan IP: | Uptime: 01:22:51

Home

Welcome to M2M 1 Port Serial Gateway configuration page.

Main page

In the main page, you can check the Firmware version, the M2M Gateway running time and the WAN IP setting.

The following table describes the labels in this screen.

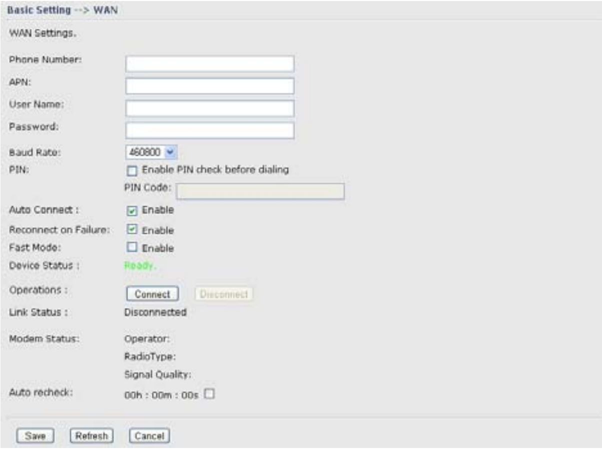
Label	Description
Firmware	Show the current firmware version.
Uptime	Show the elapsed time since the AP M2M Gateway is started.
Wan IP	Show the WAN IP address.

5.3.1 Basic Setting

WAN

The IMG-111 M2M Gateway provides Modem/3G connection.

WAN Connection Type: Modem / 3G



Basic Setting --> WAN

WAN Settings.

Phone Number:

APN:

User Name:

Password:

Baud Rate: 460800

PIN: □ Enable PIN check before dialing

PIN Code:

Auto Connect : ☑ Enable

Reconnect on Failure: ☑ Enable

Fast Mode: □ Enable

Device Status : Ready.

Operations : Connect Disconnect

Link Status : Disconnected

Modem Status: Operator:

RadioType:

Signal Quality:

Auto recheck: 00h : 00m : 00s □

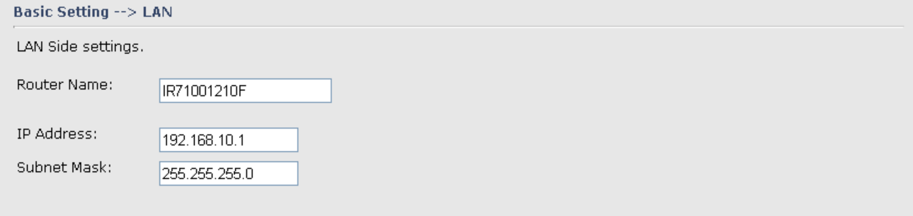
Modem/3G Screen

The following table describes the labels in this screen.

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 M2M Gateway boots up.
Device Status	Show the status of built-in HSUPA modem device.
Operations	Click “**Connect**” to call up the built-in HSUPA modem. Click "**Disconnect**" to shut down the connection.
Link Status	Show the status of connection, **up**, **down** or **connecting**.
Auto recheck	Enable auto refresh modem status per 28 sec

LAN

These are the IP settings of the LAN interface for the IMG-111 M2M Gateway. The LAN IP address is privately for your internal network and cannot be exposed on the Internet.



Basic Setting --> LAN

LAN Side settings.

Router Name: IR71001210F

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

LAN Screen

The following table describes the labels in this screen.

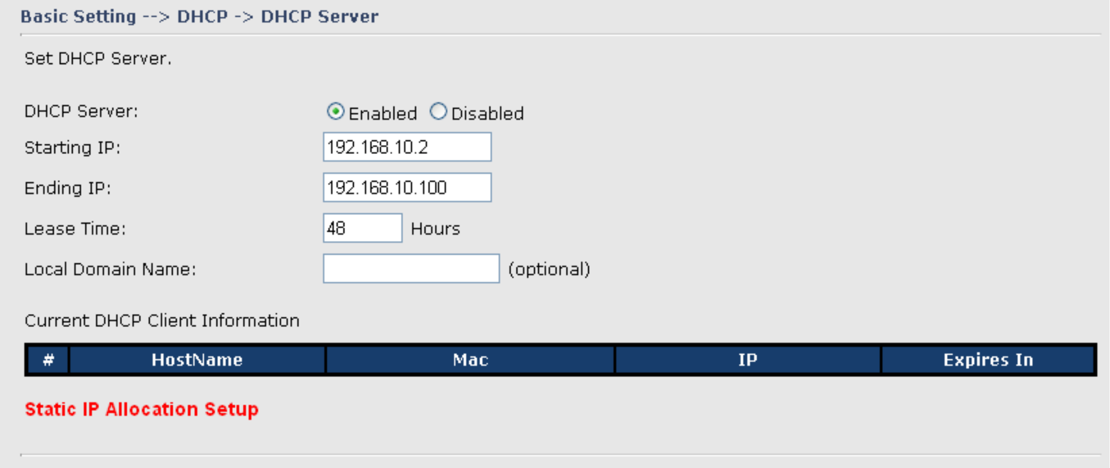
Label	**Description**
IP Address	The IP address of the LAN interface, the default IP address is 192.168.10.1
Subnet Mask	The Subnet Mask of the LAN interface, the default Subnet mask is 255.255.255.0

DHCP

DHCP stanIMG for Dynamic Host Control Protocol. The IMG-111 was 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



Basic Setting --> DHCP -> DHCP Server

Set DHCP Server.

DHCP Server: ● Enabled ○ Disabled

Starting IP: 192.168.10.2

Ending IP: 192.168.10.100

Lease Time: 48 Hours

Local Domain Name: (optional)

Current DHCP Client Information

#	HostName	Mac	IP	Expires In

Static IP Allocation Setup

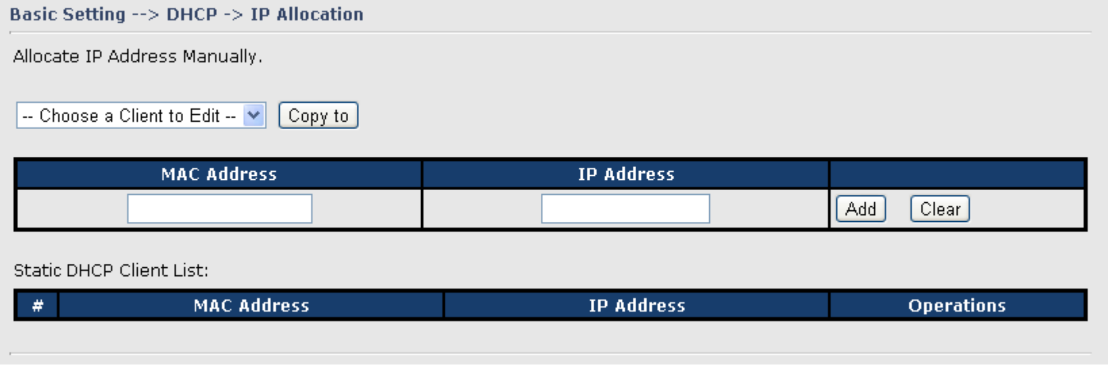
DHCP Server Screen

The following table describes the labels in this screen.

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

2. IP Allocation

The IP Allocation provides one-to-one mapping of MAC address to IP address. When computers with the MAC address requesting an IP from the IMG-111 M2M 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.

MAC Address	IP Address	
		Add Clear

Static DHCP Client List:

#	MAC Address	IP Address	Operations

IP Allocation Screen

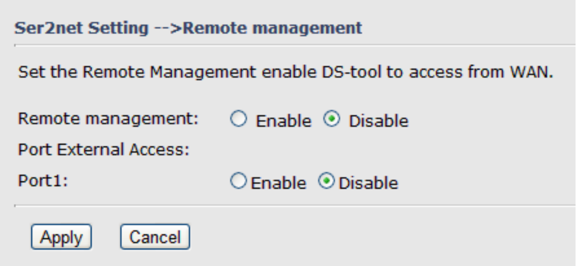
The following table describes the labels in this screen.

Label	Description
Choose a Client to Edit	The list shows the MAC addresses and IP addresses that are already assigned by IMG-111. 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 List	The list shows the MAC address and IP address one-to-one relationship.

5.3.2 Serial Setting.

Remote management

The Remote management setting allow user to enable the WAN access of the DS-tool management and Serial port access



Ser2net Setting -->Remote management

Set the Remote Management enable DS-tool to access from WAN.

Remote management: ○ Enable ● Disable

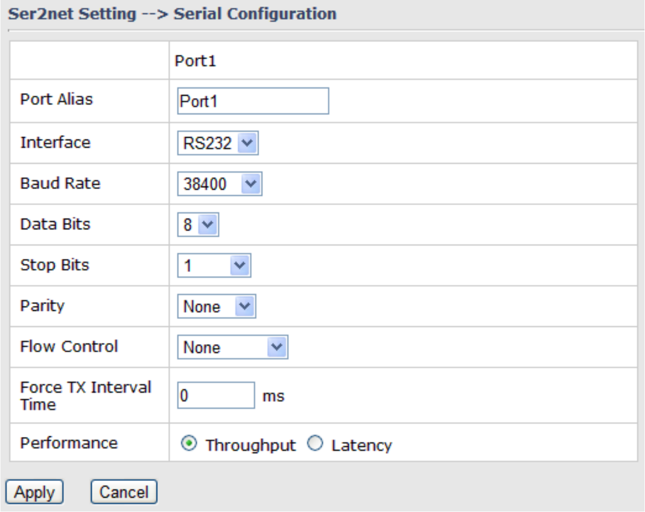
Port External Access:

Port1: ○Enable ●Disable

The following table describes the labels in this screen.

Label	Description
Remote Management	Enable to managed IMG-111 by DS-tool through WAN access
Port External Access	Enable to allow using of serial data port and control port through WAN access l

Serial Configuration



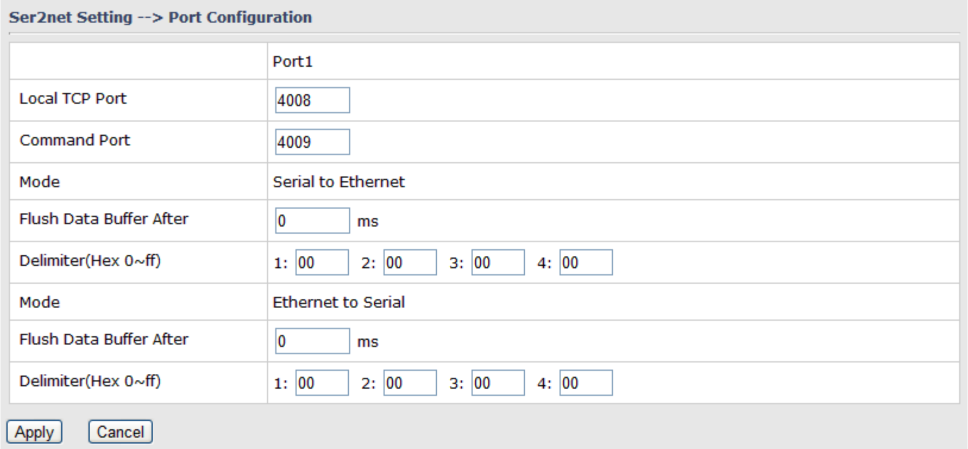
Ser2net Setting --> Serial Configuration

	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 ○ Latency

The following table describes the labels in this screen.

Label	Description
Port Alias	Remark the port to hint the connected device.
Interface	RS422 / RS485(2-wires) / RS485(4-wires)
Baud rate	110bps/300bps/1200bps/2400bps/4800bps/9600bps/19200bps/ 38400bps/57600bps/115200bps
Data Bits	5, 6, 7, 8
Stop Bits	1, 2 (1.5)
Parity	No, Even, Odd, Mark, Space
Flow Control	No, XON/XOFF
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.

Port Profile



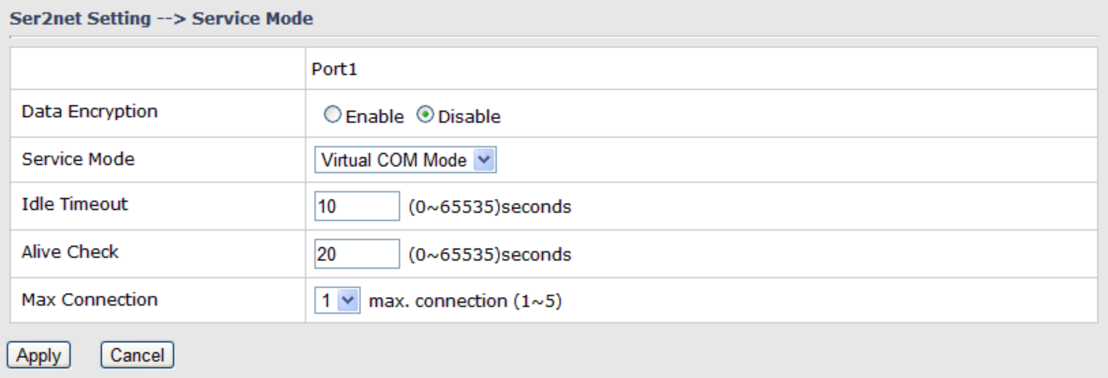
Ser2net Setting --> Port Configuration

	Port1
Local TCP Port	4008
Command Port	4009
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

Label	Description
Serial to Ethernet	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 seconIMG. 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
Ethernet to serial	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 seconIMG. 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

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
Data Encryption	○ Enable ● Disable
Service Mode	Virtual COM Mode
Idle Timeout	10 (0~65535)seconds
Alive Check	20 (0~65535)seconds
Max Connection	1 max. connection (1~5)

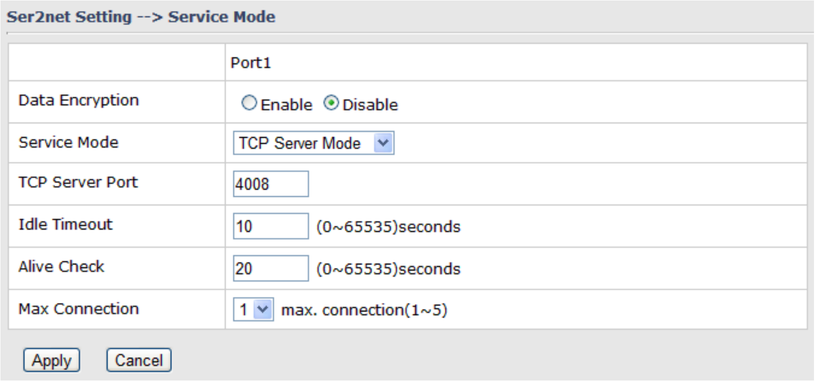
The following table describes the labels in this screen.

Label	Description
Data Encryption	Use SSL to encrypt data.
Idle Timeout	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 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.
Alive Check	The serial device will send TCP alive-check package in each defined time 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

Service Mode – TCP Server Mode

In TCP Server Mode, IMG is configured with a unique Port combination on a TCP/IP network. In this case, IMG 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.



Ser2net Setting --> Service Mode

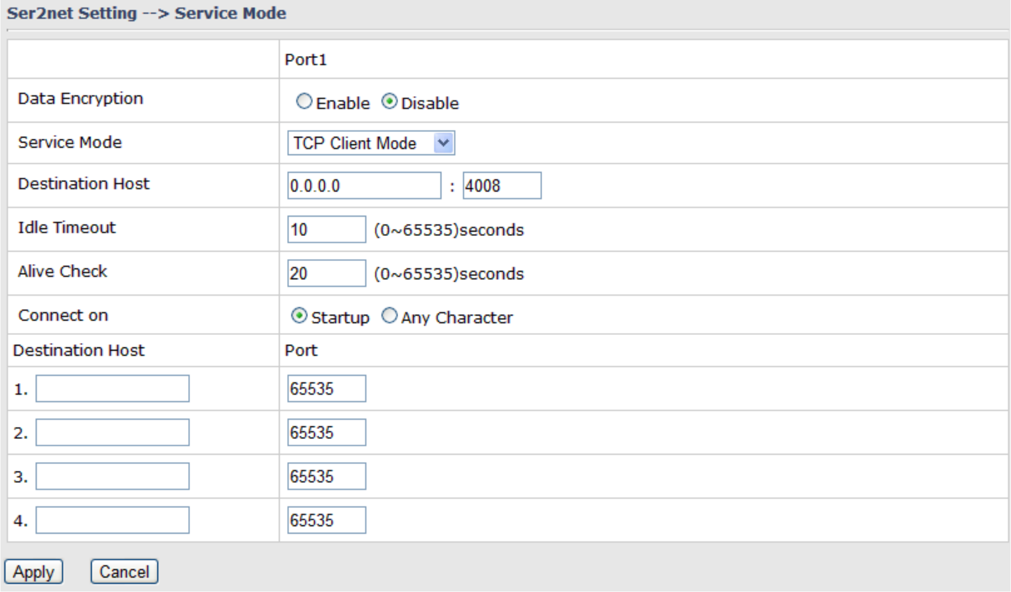
	Port1
Data Encryption	○ Enable ● Disable
Service Mode	TCP Server Mode
TCP Server Port	4008
Idle Timeout	10 (0~65535)seconds
Alive Check	20 (0~65535)seconds
Max Connection	1 max. connection(1~5)

The following table describes the labels in this screen.

Label	Description
Data Encryption	Use SSL to encrypt data.
TCP Server Port	Set the port number for data transmission.
Idle Timeout	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 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.
Alive Check	The serial device will send TCP alive-check package in each defined time 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.

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 Mode

	Port1
Data Encryption	○ Enable ● Disable
Service Mode	TCP Client Mode
Destination Host	0.0.0.0 : 4008
Idle Timeout	10 (0~65535)seconds
Alive Check	20 (0~65535)seconds
Connect on	● Startup ○ Any Character
Destination Host	Port
1.	65535
2.	65535
3.	65535
4.	65535

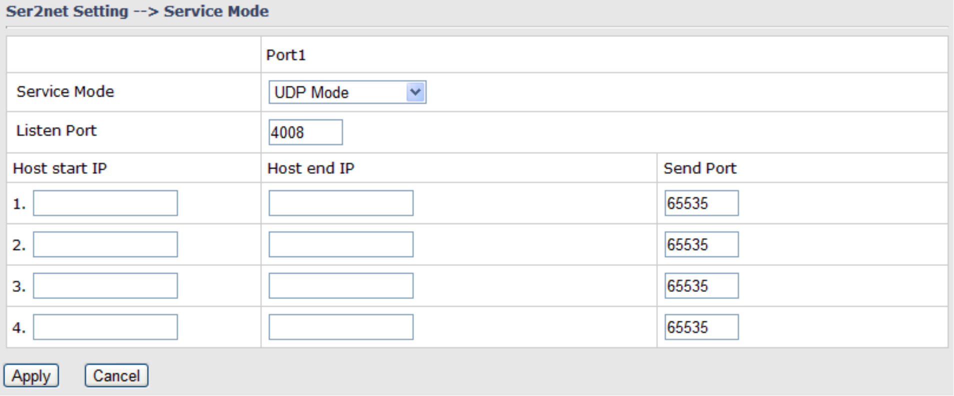
Apply Cancel

The following table describes the labels in this screen.

Label	Description
Data Encryption	Use SSL to encrypt data.
Destination Host	Set the IP address of host and the port number of data port. .
Idle Timeout	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 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.
Alive Check	The serial device will send TCP alive-check package in each defined time 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.
Connect on Startup	The TCP Client will build TCP connection once the connected serial device is started.
Connect on Any Character	The TCP Client will build TCP connection once the connected serial device starts to send data.

Service Mode – UDP Client 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	4008	
Host start IP	Host end IP	Send Port
1.		65535
2.		65535
3.		65535
4.		65535

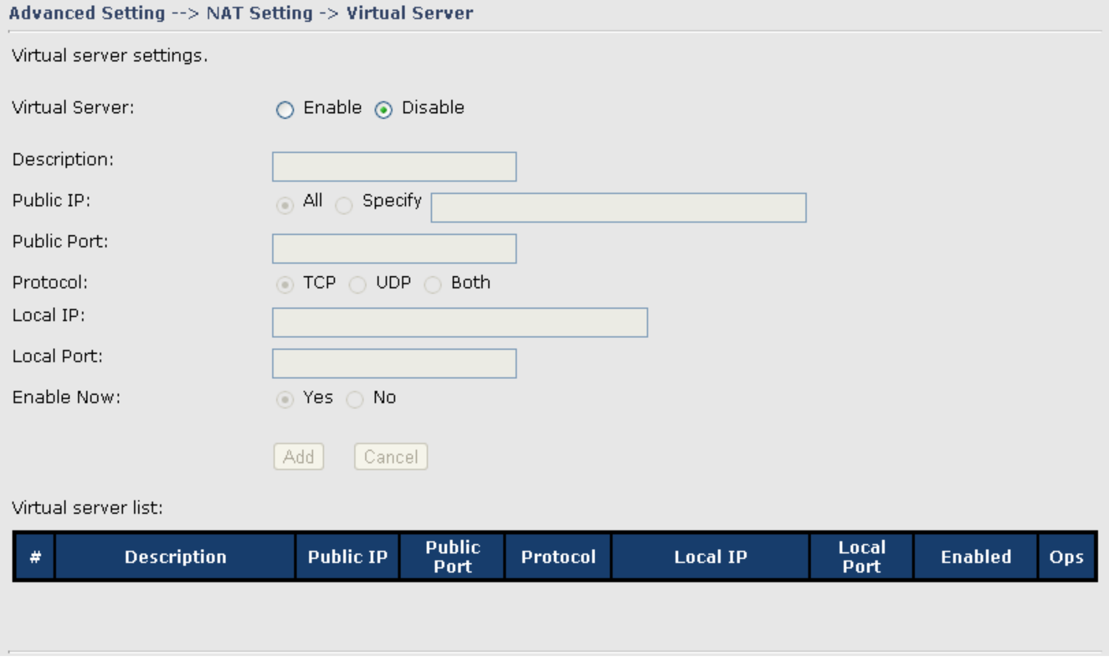
Apply Cancel

5.3.3 Advanced Settings

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.



Advanced Setting --> NAT Setting -> Virtual Server

Virtual server settings.

Virtual Server: ○ Enable ● Disable

Description:

Public IP: ● All ○ Specify

Public Port:

Protocol: ● TCP ○ UDP ○ Both

Local IP:

Local Port:

Enable Now: ● Yes ○ No

Add Cancel

Virtual server list:

#	Description	Public IP	Public Port	Protocol	Local IP	Local Port	Enabled	Ops

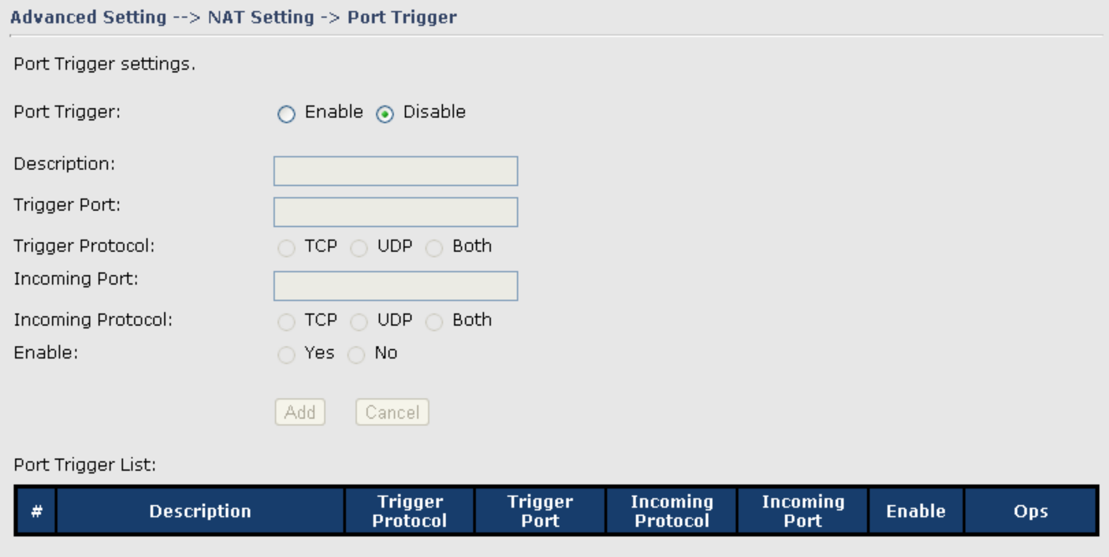
Virtual Server

The following table describes the labels in this screen.

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 M2M Gateway. Port Trigger is used for some of the applications that can work with an NAT M2M Gateway.



Advanced Setting --> NAT Setting -> Port Trigger

Port Trigger settings.

Port Trigger: ○ Enable ● Disable

Description:

Trigger Port:

Trigger Protocol: ○ TCP ○ UDP ○ Both

Incoming Port:

Incoming Protocol: ○ TCP ○ UDP ○ Both

Enable: ○ Yes ○ No

Port Trigger List:

#	Description	Trigger Protocol	Trigger Port	Incoming Protocol	Incoming Port	Enable	Ops

Port Trigger Screen

The following table describes the labels in this screen.

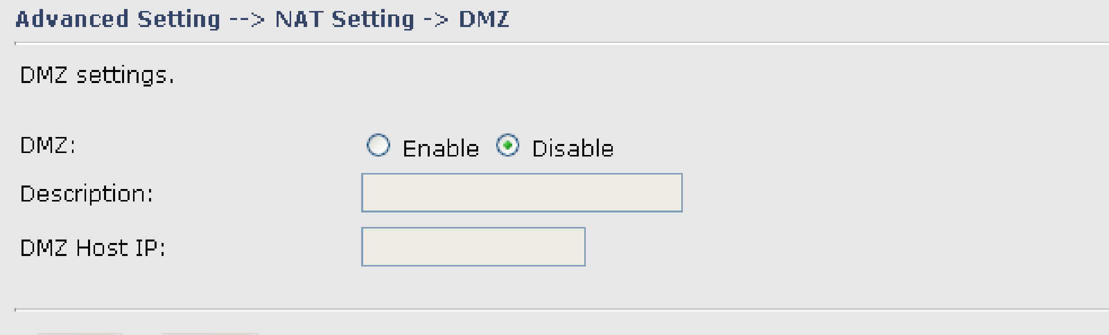
Label	Description
Port Trigger	Enable or disable Port Trigger.
Description	This is the description for the entry.

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

3. DMZ

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

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



Advanced Setting --> NAT Setting -> DMZ

DMZ settings.

DMZ: ○ Enable ● Disable

Description:

DMZ Host IP:

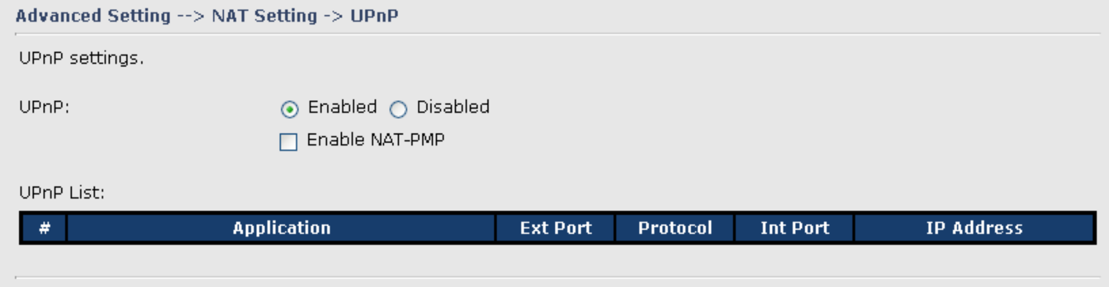
DMZ Screen

The following table describes the labels in this screen.

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

4. UPnP

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



Advanced Setting --> NAT Setting -> UPnP

UPnP settings.

UPnP: ● Enabled ○ Disabled

□ Enable NAT-PMP

UPnP List:

#	Application	Ext Port	Protocol	Int Port	IP Address

UPnP Screen

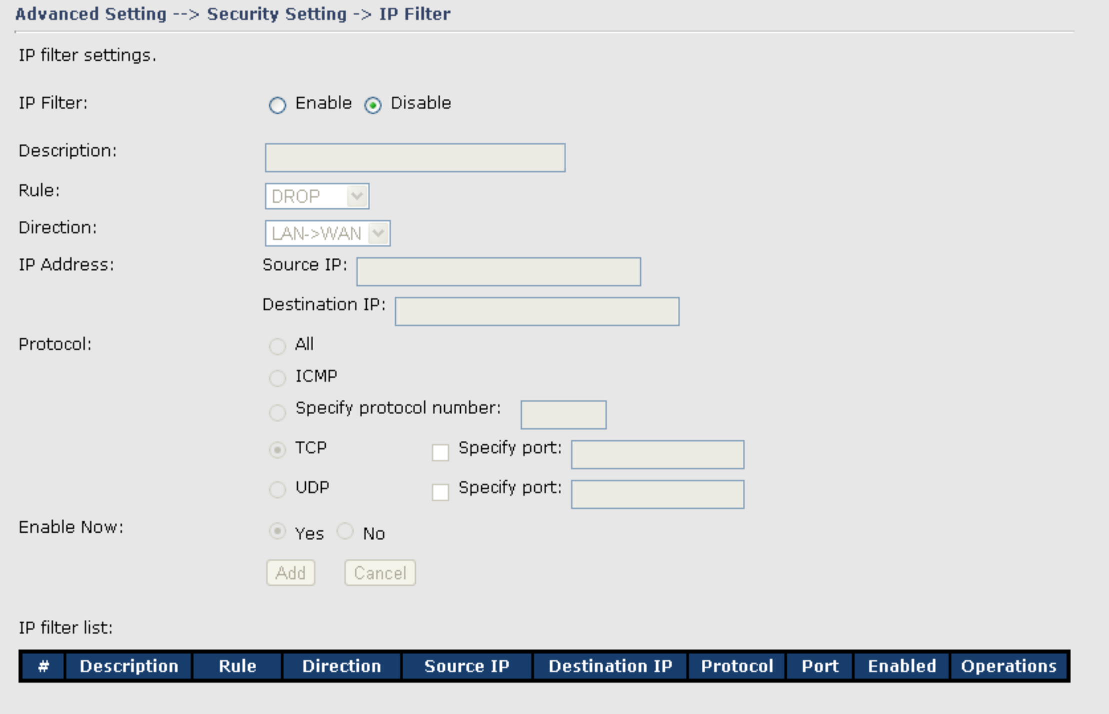
The following table describes the labels in this screen.

Label	Description
UPnP	Enable or disable UPnP.
Enable NAT-PMP	NAT-PMP allows a computer in a private network (behind a NAT M2M Gateway) to automatically configure the M2M 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 allows or denies WAN hosts to access LAN computers.



Advanced Setting --> Security Setting -> IP Filter

IP filter settings.

IP Filter: ○ Enable ● Disable

Description:

Rule: DROP

Direction: LAN->WAN

IP Address: Source IP:

Destination IP:

Protocol:
○ All
○ ICMP
○ Specify protocol number:
● TCP □ Specify port:
○ UDP □ Specify port:

Enable Now: ● Yes ○ No

IP filter list:

#	Description	Rule	Direction	Source IP	Destination IP	Protocol	Port	Enabled	Operations

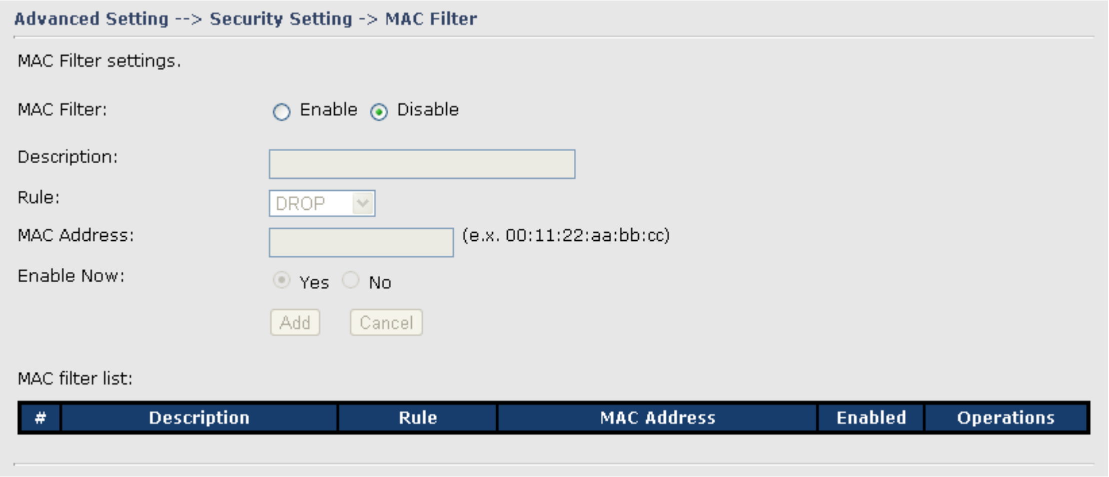
IP Filter Screen

The following table describes the labels in this screen.

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

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 settings.

MAC Filter: ○ Enable ● Disable

Description:

Rule: DROP

MAC Address: (e.x. 00:11:22:aa:bb:cc)

Enable Now: ● Yes ○ No

MAC filter list:

#	Description	Rule	MAC Address	Enabled	Operations

MAC Filter Screen

The following table describes the labels in this screen.

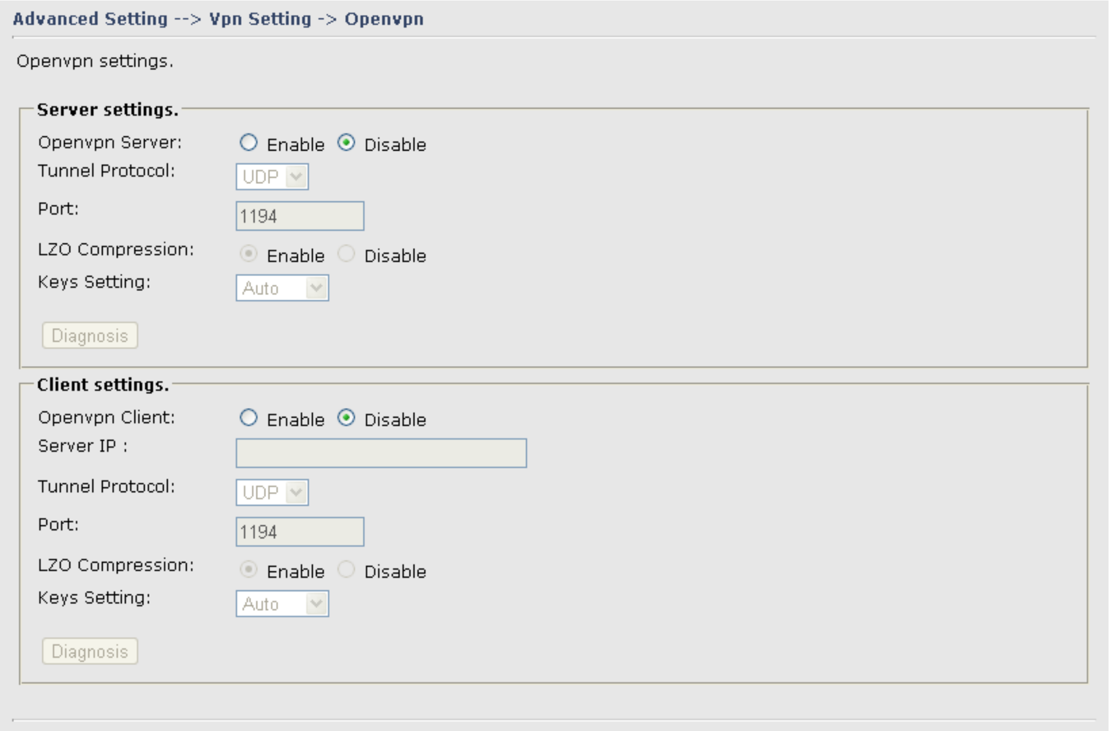
Label	Description
MAC Filter	Enable or disable the MAC Filter.
Description	Enter the description for the entry.
Rule	Select DROP, ACCEPT and REJECT rule for the entry.
MAC Address	Enter the MAC address to be filtered.
Enable Now	Enable the entry after adding it.
IP filter list	Click Edit for editing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

VPN Setting

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

1. Open VPN

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



Advanced Setting --> Vpn Setting -> Openvpn

Openvpn settings.

Server settings.

Openvpn Server: ○ Enable ● Disable

Tunnel Protocol: UDP

Port: 1194

LZO Compression: ● Enable ○ Disable

Keys Setting: Auto

Diagnosis

Client settings.

Openvpn Client: ○ Enable ● Disable

Server IP :

Tunnel Protocol: UDP

Port: 1194

LZO Compression: ● Enable ○ Disable

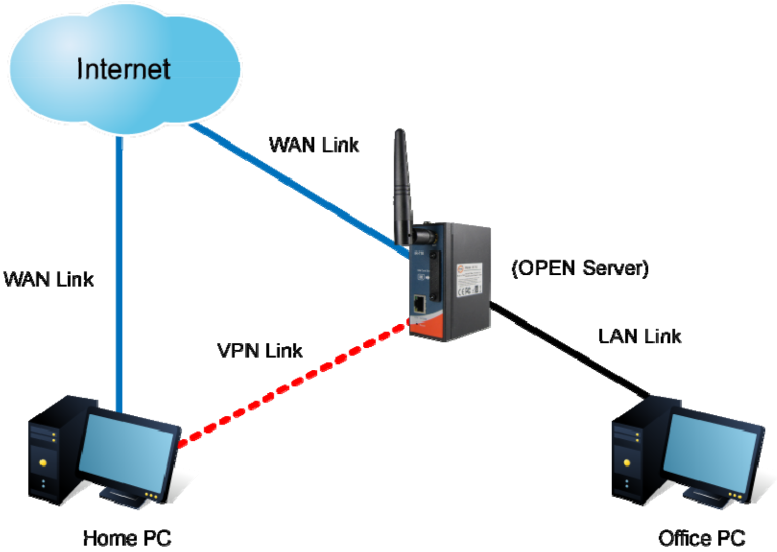
Keys Setting: Auto

Diagnosis

Open VPN Screen

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 Open VPN server of IMG-111 M2M Gateway, please install Open VPN client software for your windows PC. It can be downloading from [http://Open VPN.net/download.html#stablel](http://OpenVPN.net/download.html#stablel). The current version of Open VPN used in IMG-111 is version 2.0.9. The corresponding software for client should be installed.

The following table describes the labels in this screen.

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 Open VPN client software to generate your certificates and paste them here. For more information, please visit Open VPN website.

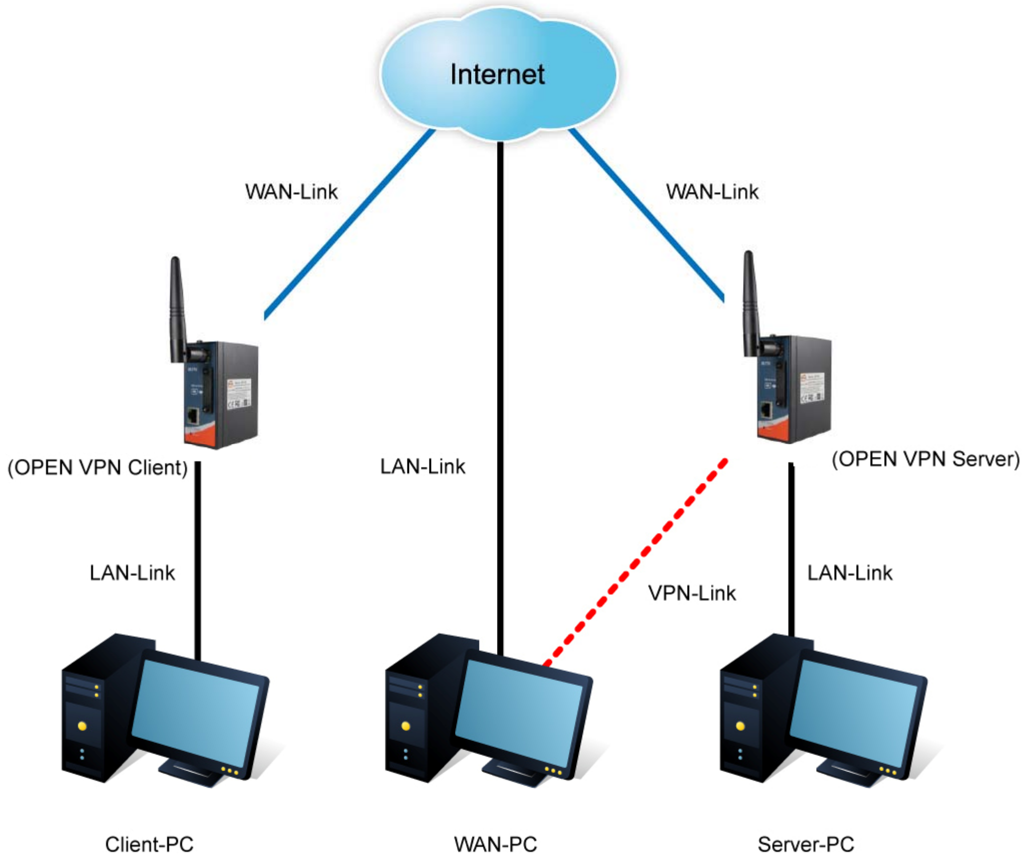
2: Open VPN Client

Two M2M Gateways are needed for creating site-to-site VPN connection using this mode.

The following table describes the labels in this screen.

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 Open VPN client to generate your certificates and paste them here. For more information, please visit Open VPN website.

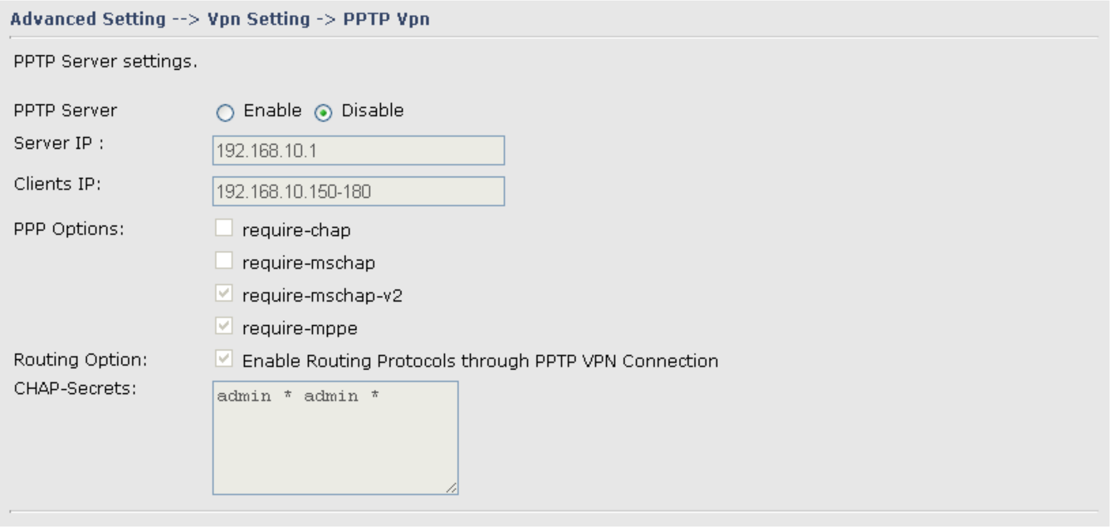
3: Open VPN Server VS Client



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 M2M Gateway from WAN port, just like connecting in the LAN. To create a PPTP connection to the M2M 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 : 192.168.10.1

Clients IP: 192.168.10.150-180

PPP Options: □ require-chap

□ require-mschap

☑ require-mschap-v2

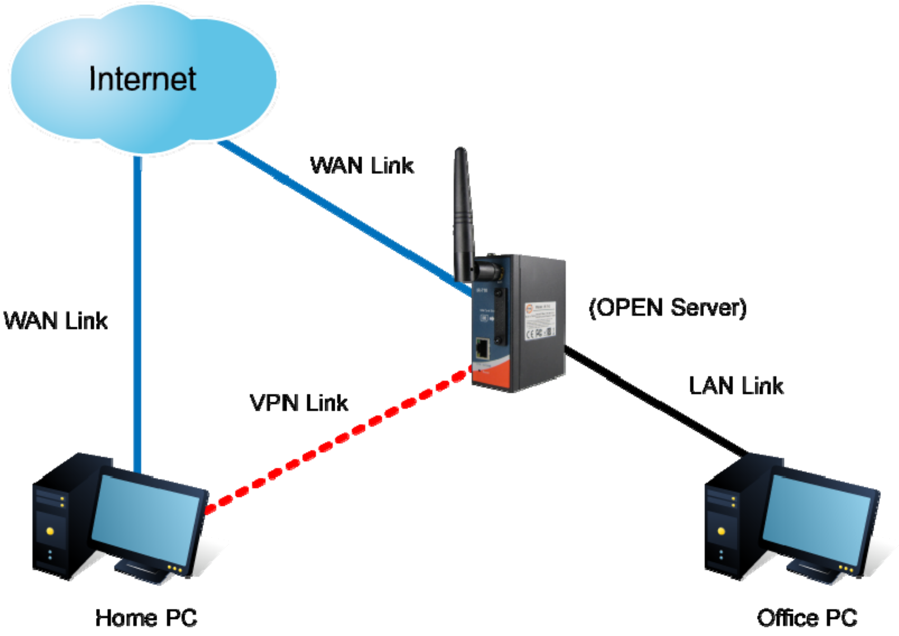
☑ require-mppe

Routing Option: ☑ Enable Routing Protocols through PPTP VPN Connection

CHAP-Secrets: admin * admin *

PPTP VPN Screen

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



Connection to PPTP VPN Server

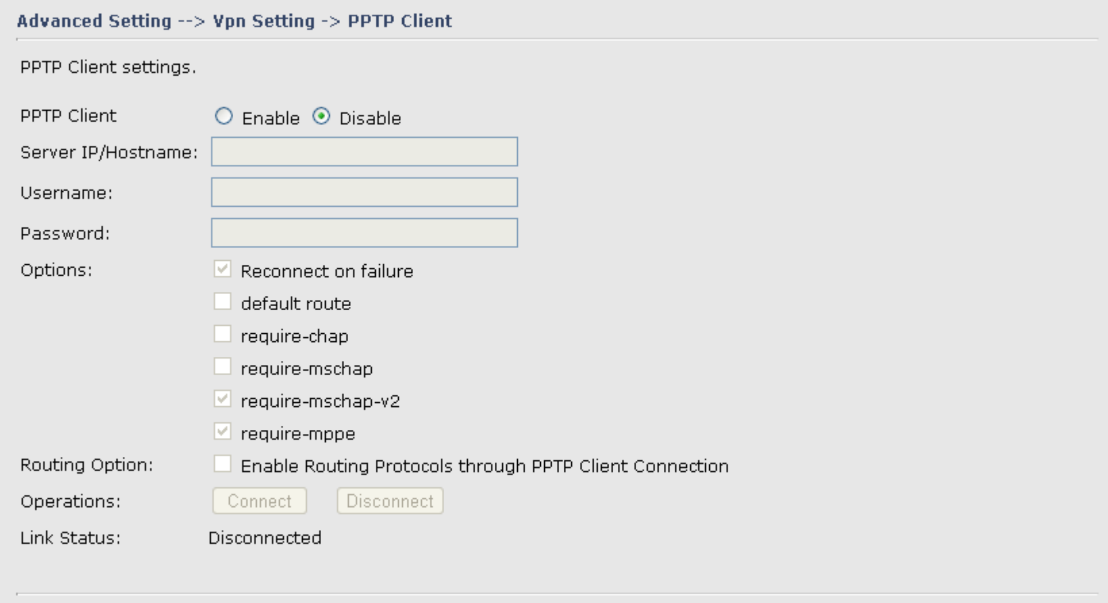
The following table describes the labels in this screen.

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 M2M Gateway A want to link with the others which is not in the same network with the M2M Gateway A, the function of PPTP client should support in the M2M Gateway page.



Advanced Setting --> Vpn Setting -> PPTP Client

PPTP Client settings.

PPTP Client ○ Enable ● Disable

Server IP/Hostname:

Username:

Password:

Options: ☑ Reconnect on failure

□ default route

□ require-chap

□ require-mschap

☑ require-mschap-v2

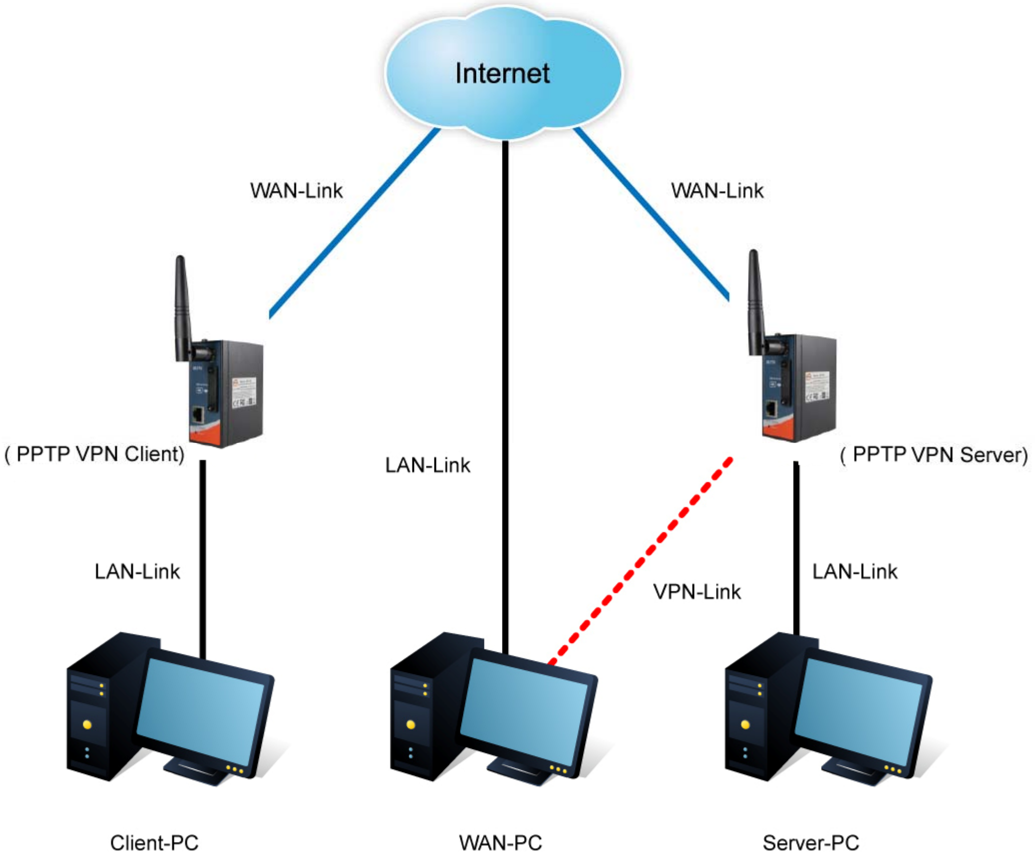
☑ require-mppe

Routing Option: □ Enable Routing Protocols through PPTP Client Connection

Operations: Connect Disconnect

Link Status: Disconnected

PPTP client settings screen

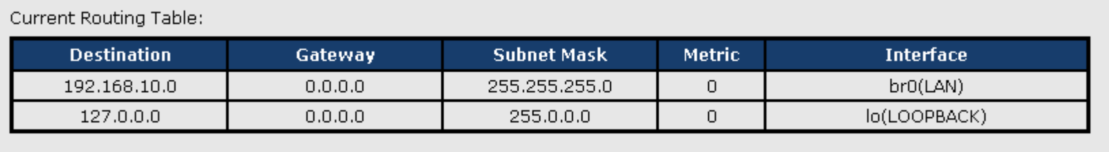


The following table describes the labels in this screen.

Label	Description
PPTP Client	Enable or disable PPTP Client.
Server IP/Hostname	Enter the server IP address or hostname.
Username/Password	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 Protocol (Routing Setting)

This page shows the information of routing table. The initial state of the M2M 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.



Current Routing Table:

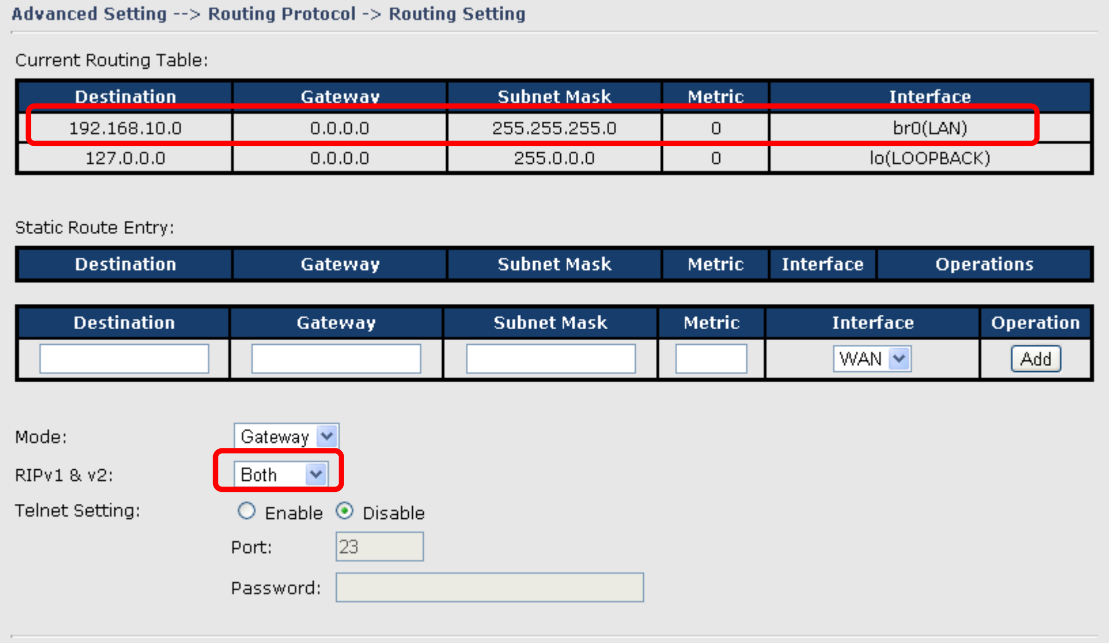
Destination	Gateway	Subnet Mask	Metric	Interface
192.168.10.0	0.0.0.0	255.255.255.0	0	br0(LAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)

The table shows the normal routing table

1. Use Dynamic Routing

Use the dynamic routing, you should not choose "Disable" about the **RIPv1 & v2** in the M2M Gateways.

Click "Apply", and you can see the more information in the **Current Routing Table**, which shows the network segment of the other M2M Gateway.



Advanced Setting --> Routing Protocol -> Routing Setting

Current Routing Table:

Destination	Gateway	Subnet Mask	Metric	Interface
192.168.10.0	0.0.0.0	255.255.255.0	0	br0(LAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)

Static Route Entry:

Destination	Gateway	Subnet Mask	Metric	Interface	Operations

Destination	Gateway	Subnet Mask	Metric	Interface	Operation
				WAN	Add

Mode: Gateway

RIPv1 & v2: Both

Telnet Setting: ○ Enable ● Disable

Port: 23

Password:

Routing setting screen

The following table describes the labels in this screen.

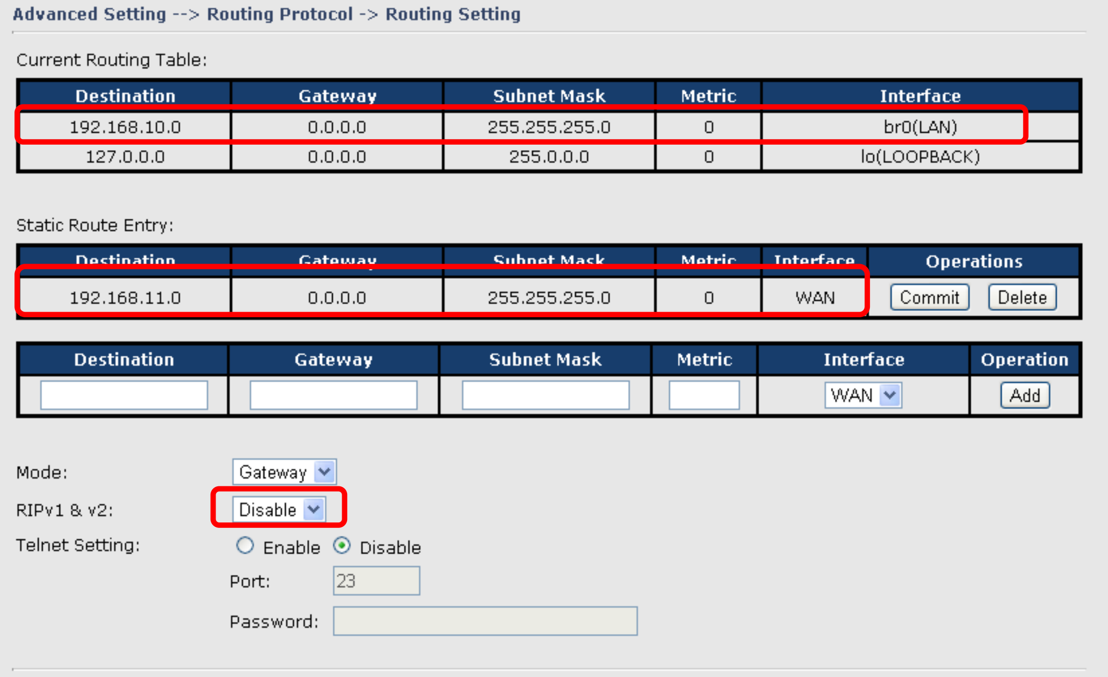
Label	Description
Current Routing Table	Show the current the routing information.
Static Route Entry	Not RIP and enter the right value in the textbox will be showing.

Mode	If you want to the PC in the M2M Gateway can visit the outside network, only choose the Gateway Mode; if or not, you choose the M2M Gateway Mode.
RIPv1 &v2	Choose "Disable" in the Static routing.
Telnet Setting	Only use in the Dynamic routing.

2. Use Static Routing

Use the Static routing, you should choose "Disable" about the **RIPv1 & v2** in the M2M Gateways.

Click "Apply", and you can see the more information in the **Current Routing Table** and **Static Route Entry**, which shows the network segment of the other M2M Gateway.



Advanced Setting --> Routing Protocol -> Routing Setting

Current Routing Table:

Destination	Gateway	Subnet Mask	Metric	Interface
192.168.10.0	0.0.0.0	255.255.255.0	0	br0(LAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)

Static Route Entry:

Destination	Gateway	Subnet Mask	Metric	Interface	Operations
192.168.11.0	0.0.0.0	255.255.255.0	0	WAN	Commit Delete

Destination	Gateway	Subnet Mask	Metric	Interface	Operation
				WAN	Add

Mode: Gateway

RIPv1 & v2: Disable

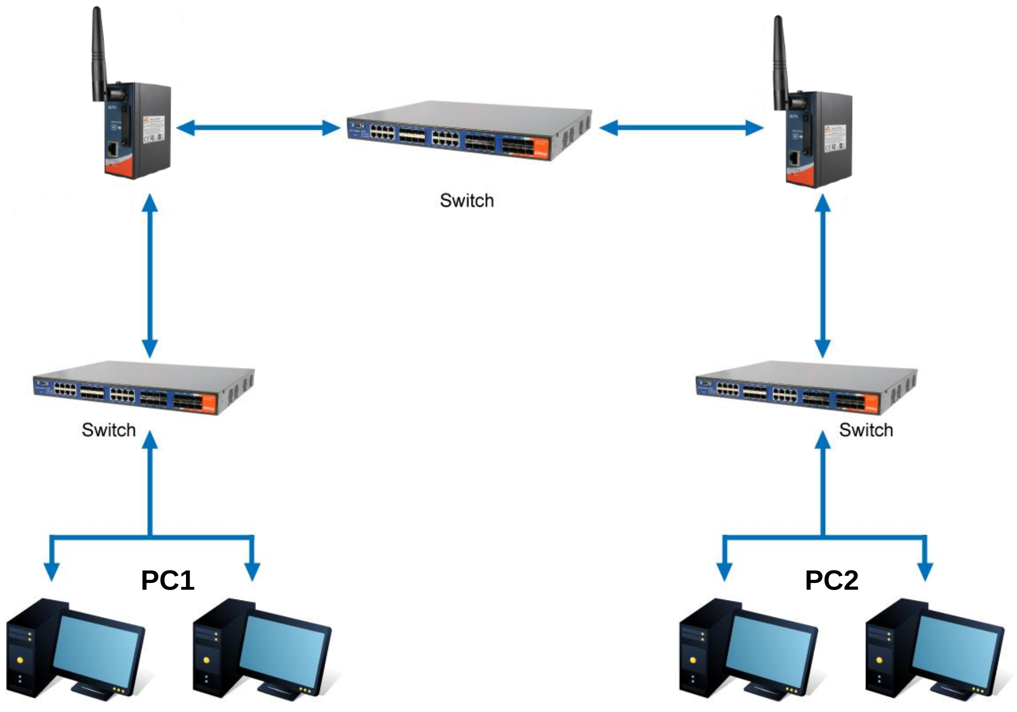
Telnet Setting: ○ Enable ● Disable

Port: 23

Password:

Static route setting screen

Use the dynamic routing; it will have many ways such as RIP, OSPF.BGP. In this M2M Gateway, we use the RIP Protocol to finish the dynamic routing table.



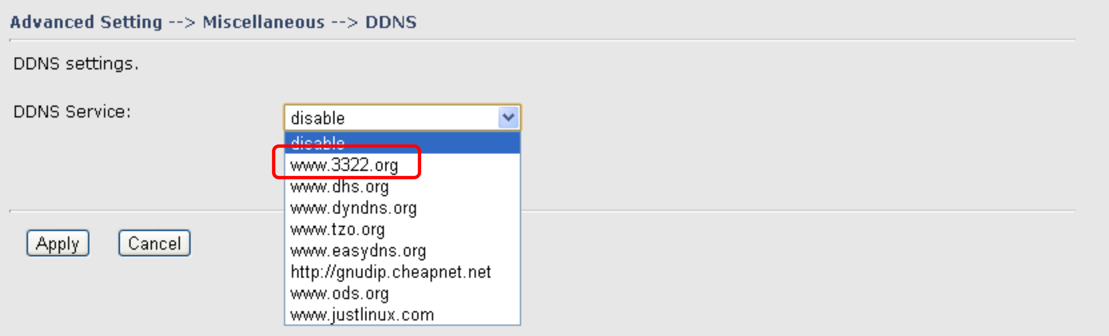
The Routing Topography

RIP, Routing Information Protocol, is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP) using the distance-vector routing algorithm.

After all settings, PC1 can visit PC2 which is different network segment of the PC1.

Miscellaneous DDNS

Dynamic Domain Name Server is to keep a domain name linked to a dynamic IP address.



Advanced Setting --> Miscellaneous --> DDNS

DDNS settings.

DDNS Service: disable

DDNS Screen

For example, Choose DDNS Service: www.3322.org and configure the following instructions:

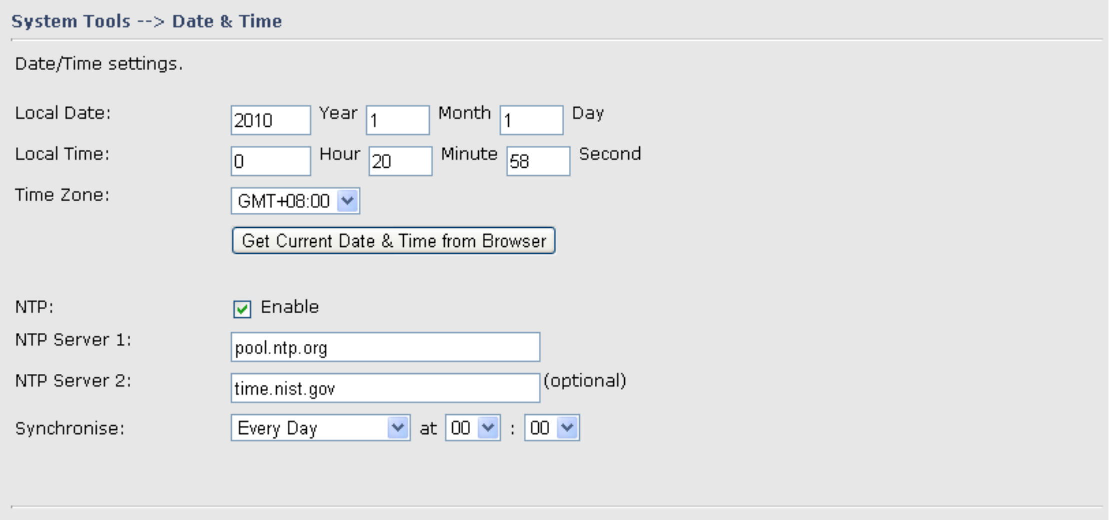
The following table describes the labels in this screen.

Label	Description
User Name	Enter the user name for your DDNS account.
Password	Enter the password for your DDNS account.
Domain	Enter the domain names provided by your dynamic DNS service provider.
Mail Server	Enter the mail server if provided.
Use Wildcard	Check the box the enable wildcard option.

5.3.4 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: 2010 Year 1 Month 1 Day

Local Time: 0 Hour 20 Minute 58 Second

Time Zone: GMT+08:00

NTP: ☑ Enable

NTP Server 1: pool.ntp.org

NTP Server 2: time.nist.gov (optional)

Synchronise: Every Day at 00 : 00

Date & Time Screen

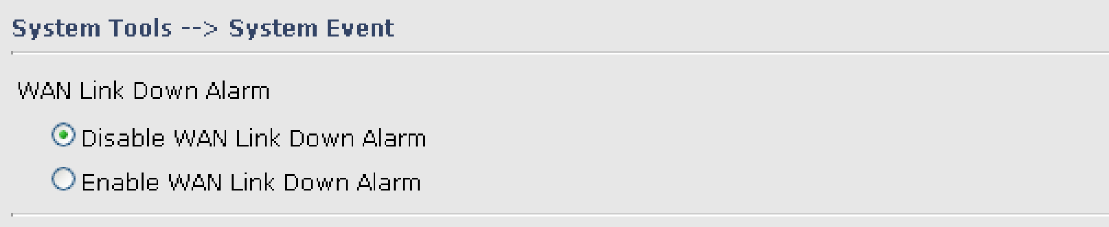
The following table describes the labels in this screen.

Label	Description
Local Date	Set local date manually.
Local Time	Set local time manually.
Time Zone	Select the time zone manually

Get Current Date & Time from Browser	Click this button; you can set the time from your 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.

System Event

When the WAN Link Down is triggered, the notification procedure will be performed



System Tools --> System Event

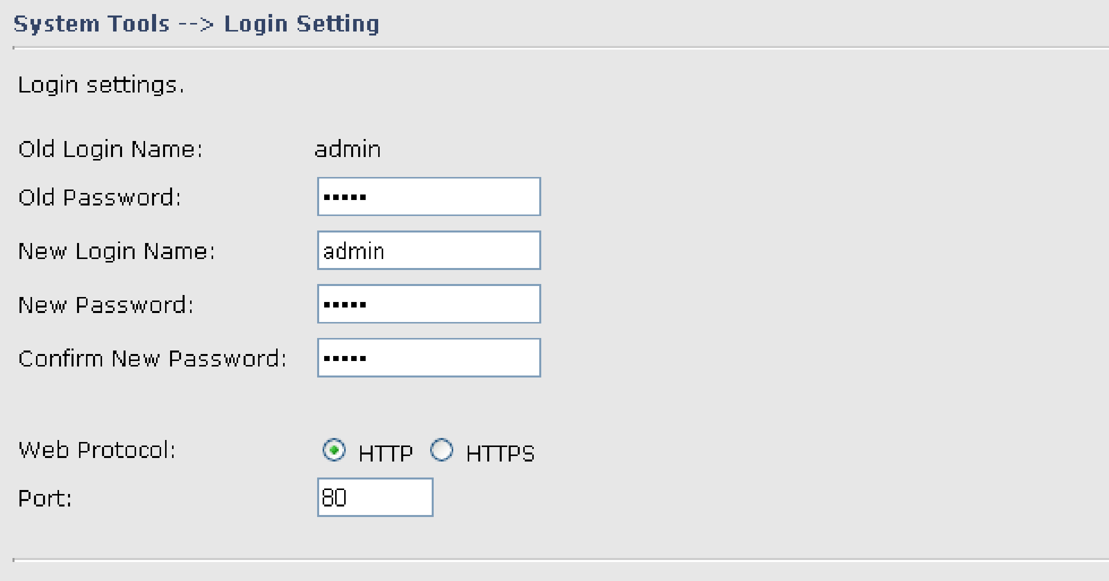
WAN Link Down Alarm

● Disable WAN Link Down Alarm

○ Enable WAN Link Down Alarm

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:	● HTTP ○ HTTPS
Port:	80

Login Setting Screen

The following table describes the labels in this screen.

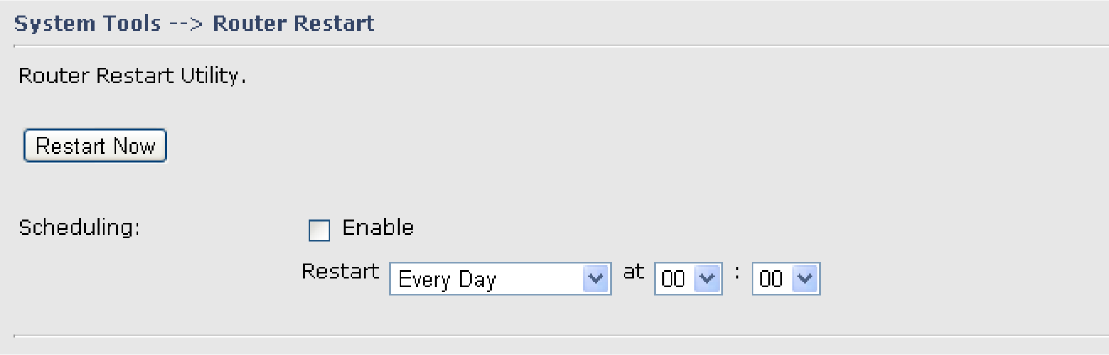
Label	Description
Old Name	This field shows the old login name.

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

HTTPS (HTTP over SSL) is a Web protocol which encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

M2M Gateway Restart

If you want restart the M2M Gateway through the **Warm Reset**, click **Restart Now** to restart the Wireless M2M Gateway. Also, you can set a **Scheduling** time to make the M2M Gateway restart.



System Tools --> Router Restart

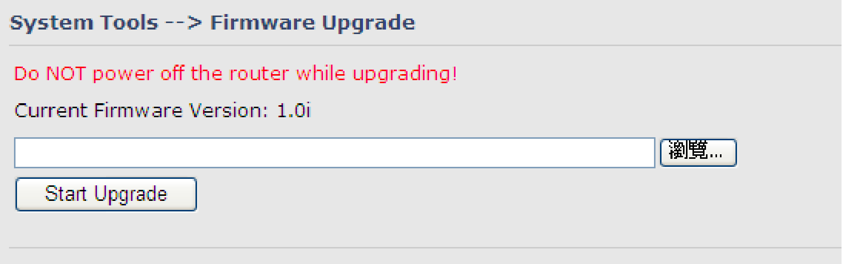
Router Restart Utility.

Scheduling: □ Enable

Restart Every Day at 00 : 00

M2M Gateway Restart Screen

Firmware Upgrade



System Tools --> Firmware Upgrade

Do NOT power off the router while upgrading!

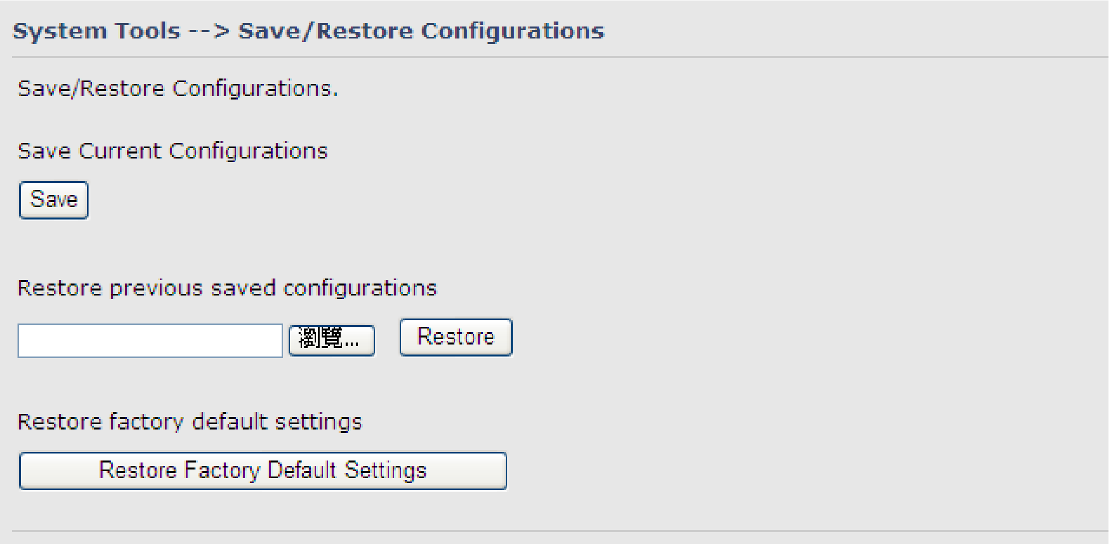
Current Firmware Version: 1.0i

Firmware Upgrade Screen

Newer firmware may provide better performance or function extensions. To upgrade the new firmware, you need a firmware file which matches the model of this AP M2M Gateway. It will take several minutes to upload and update the firmware. After the upgrade is done successfully, reboot the M2M Gateway to utilized new firmware.

Important Notice: DO NOT POWER OFF THE M2M GATEWAY OR PRESS THE RESET BUTTON WHILE THE FIRMWARE IS BEING UPGRADED.

Save/Restore Configurations



System Tools --> Save/Restore Configurations

Save/Restore Configurations.

Save Current Configurations

Restore previous saved configurations

Restore factory default settings

Save/Restore Configurations Screen

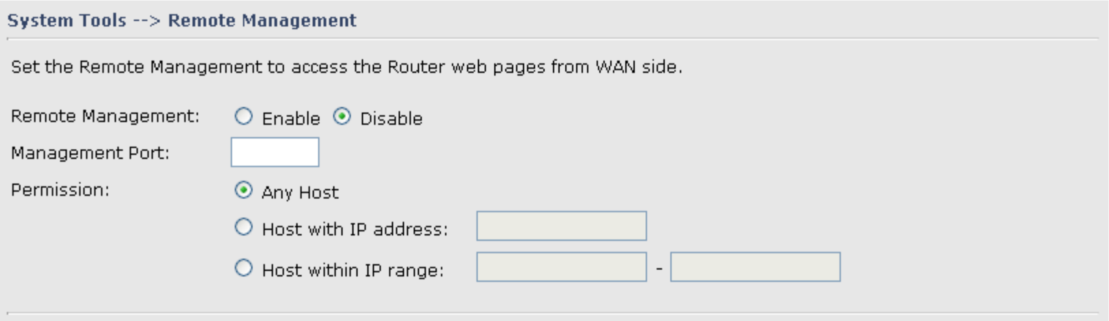
Save: The configuration file can be downloaded. (Internet Explorer user will need to click on the protection bar on top and click choose "download files")

The following table describes the labels in this screen.

Label	Description
Download configuration	The current system settings can be saved as a file into your PC.
Upload configuration	The configuration can be restored to the M2M 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 Settings	You may also reset the M2M Gateway to the factory settings by clicking on Restore Default Settings. The M2M Gateway will reboot to validate the default settings.

Remote management

Set the Remote Management to access the M2M Gateway web pages from WAN side.



System Tools --> Remote Management

Set the Remote Management to access the Router web pages from WAN side.

Remote Management: ○ Enable ● Disable

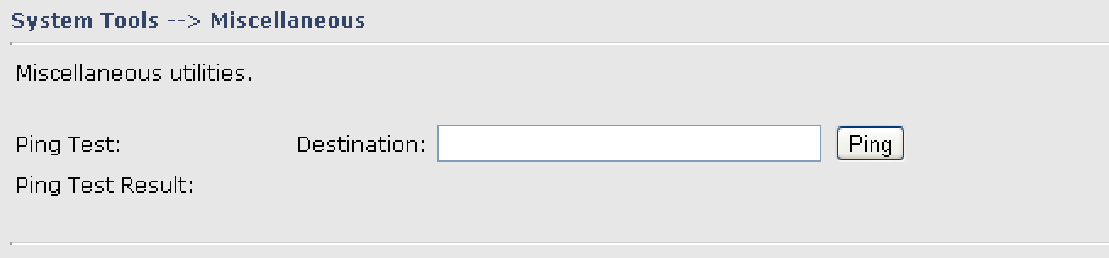
Management Port:

Permission: ● Any Host

○ Host with IP address:

○ Host within IP range: -

Miscellaneous (Ping)



System Tools --> Miscellaneous

Miscellaneous utilities.

Ping Test: Destination:

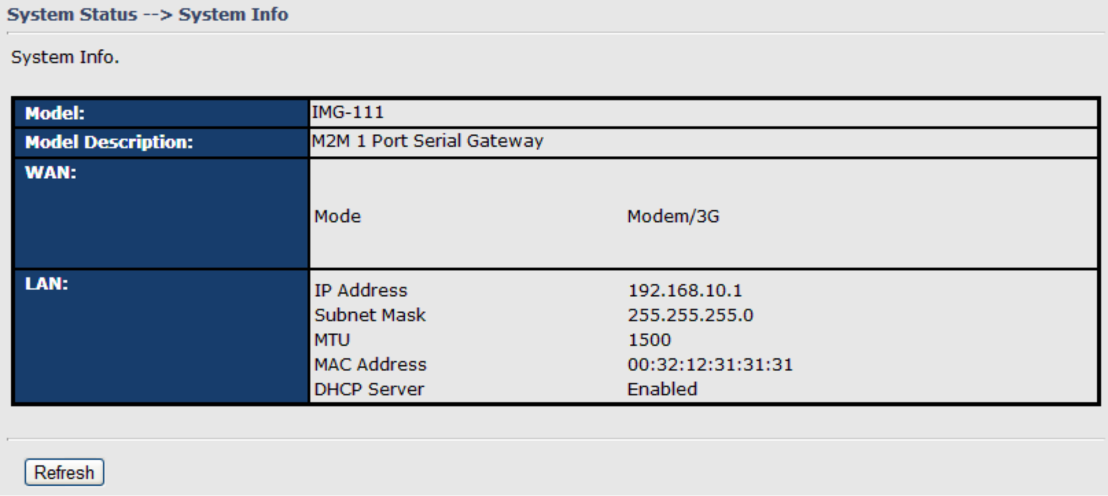
Ping Test Result:

Miscellaneous Screen

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 --> System Info

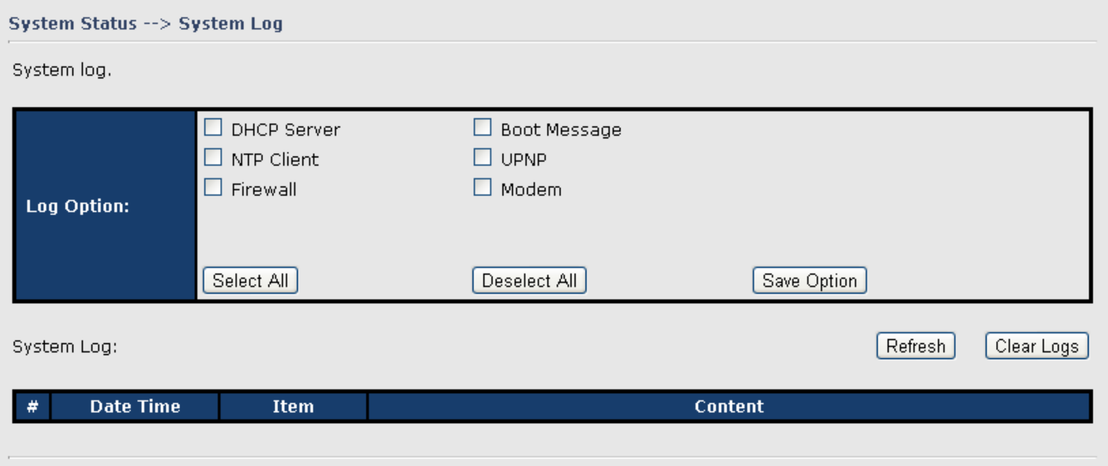
System Info.

Model:	IMG-111
Model Description:	M2M 1 Port Serial Gateway
WAN:	Mode Modem/3G
LAN:	IP Address 192.168.10.1 Subnet Mask 255.255.255.0 MTU 1500 MAC Address 00:32:12:31:31:31 DHCP Server Enabled

System Info Screen

This page displays the details information for the M2M Gateway including model name, model description, firmware version, WAN, LAN settings.

System Log



System Status --> System Log

System log.

Log Option:

□ DHCP Server □ Boot Message
□ NTP Client □ UPNP
□ Firewall □ Modem

System Log:

#	Date Time	Item	Content

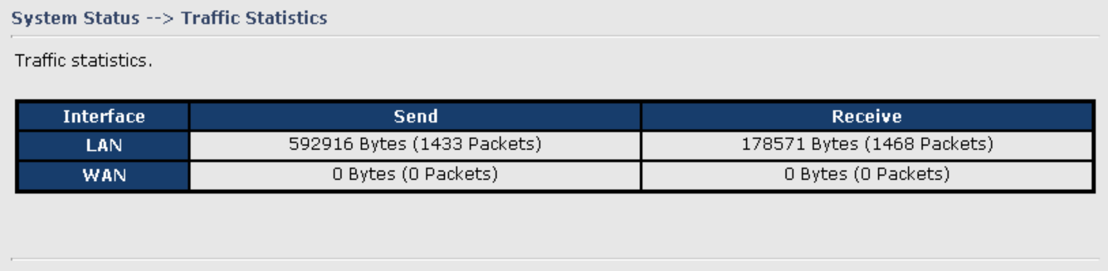
System Log Screen

The M2M Gateway keeps a running log of events and activities occurring on the M2M 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
LAN	592916 Bytes (1433 Packets)	178571 Bytes (1468 Packets)
WAN	0 Bytes (0 Packets)	0 Bytes (0 Packets)

Traffic Statistics Screen

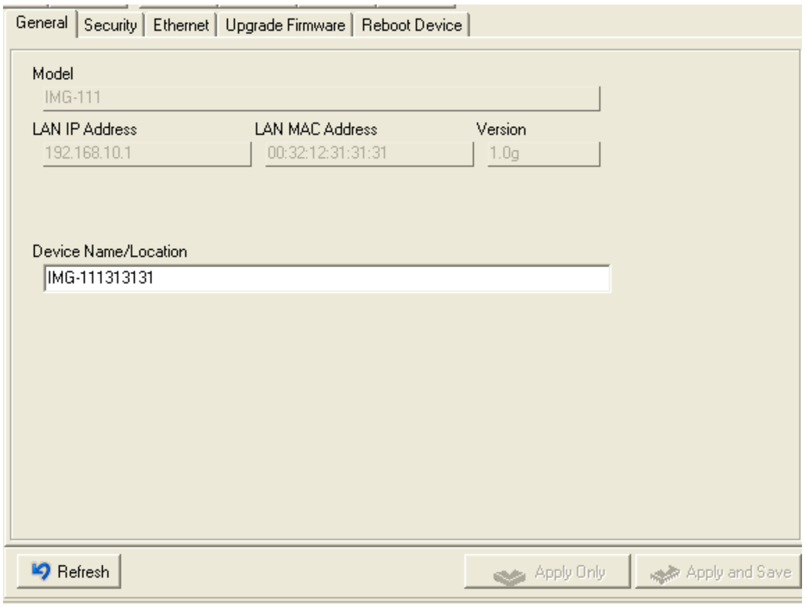
This page displays the network traffic statistics for both received and transmitted packets through the Ethernet port and wireless connections.

5.4 DS-tool

The IMG basic information and some serial port related function can be configure by using DS-tool, including the VCOM Mapping

General settings

This page display some basic information of the device and also includes the setting of device name.



Model: IMG-111

LAN IP Address: 192.168.10.1

LAN MAC Address: 00:32:12:31:31:31

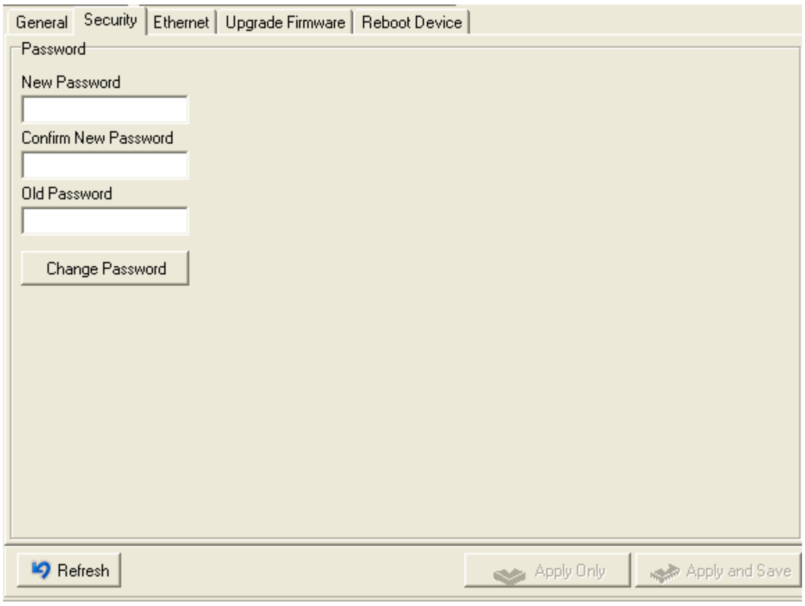
Version: 1.0g

Device Name/Location: IMG-111313131

The following table describes the labels in this screen.

Label	Description
Device Name/location	set the device name

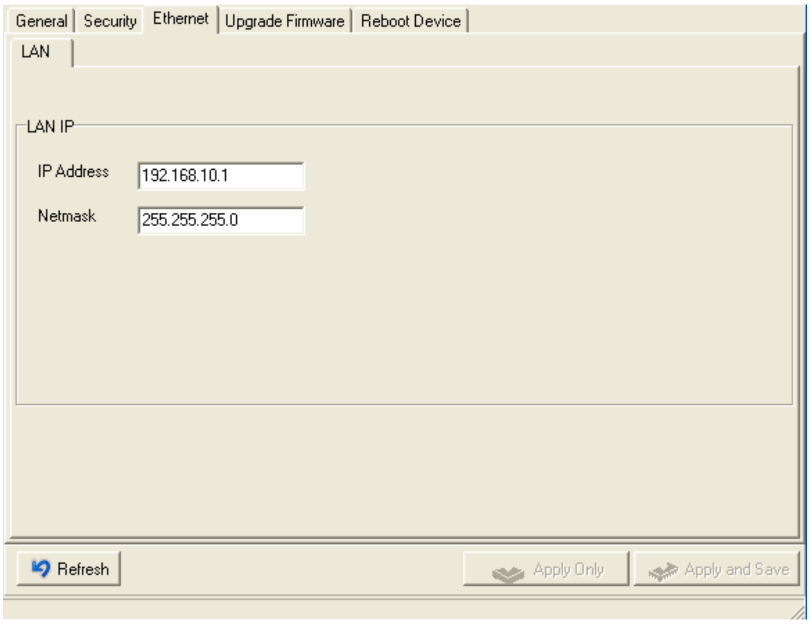
Security



The following table describes the labels in this screen.

Label	Description
Password setting	Changing new password

Network Setting



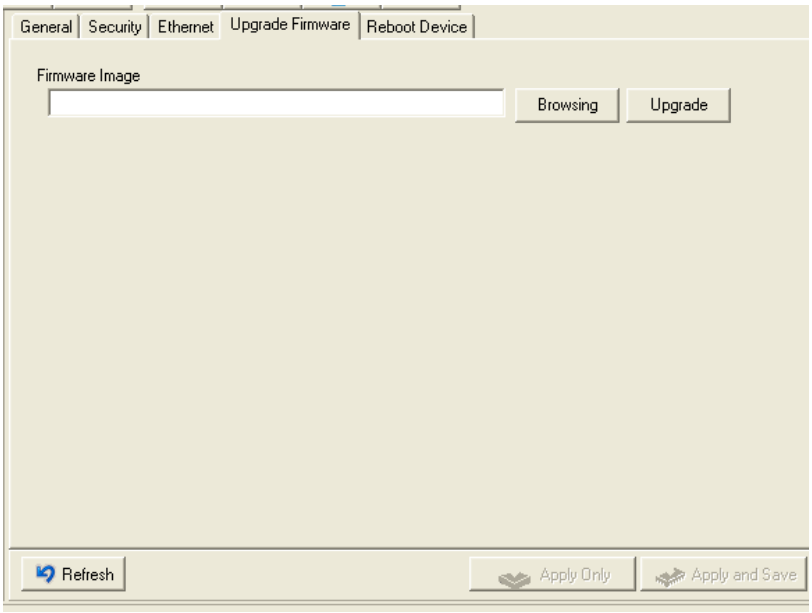
IP Address 192.168.10.1

Netmask 255.255.255.0

The following table describes the labels in this screen.

Label	Description
LAN IP	Assigning an IP address.
Subnet Mask	All devices on the network must have the same subnet mask to communicate on the network.

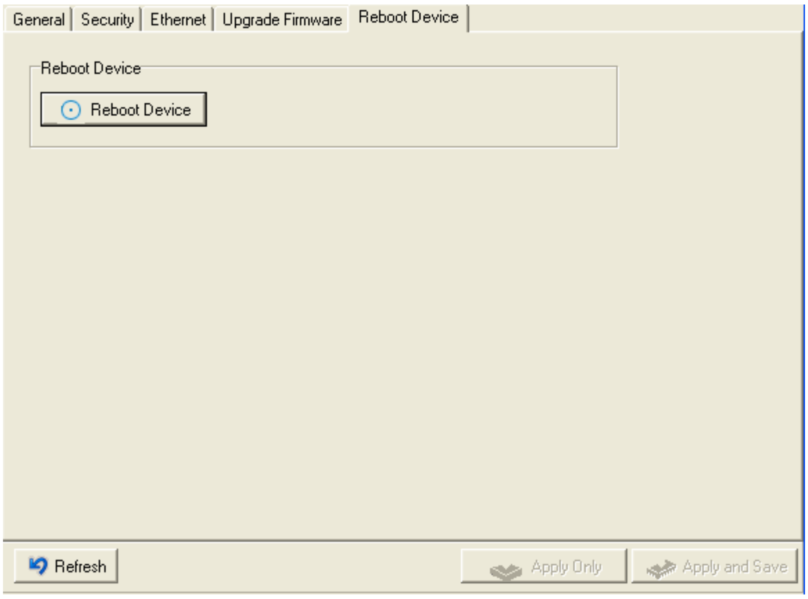
Upgrade Firmware



The following table describes the labels in this screen.

Label	Description
Upgrade	Enable the firmware upgrade.

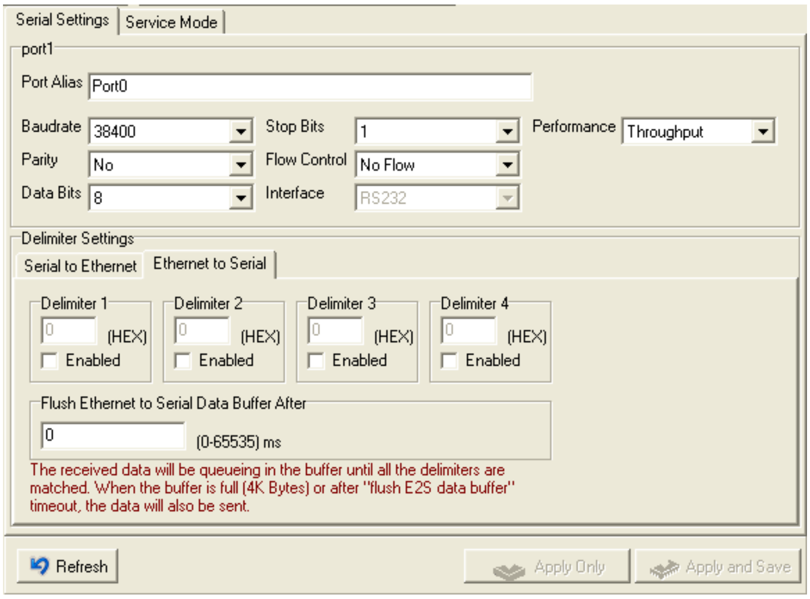
Save/Load



The following table describes the labels in this screen.

Label	Description
Reboot Device	Reboot the IMG-111 (warm start).

Serial Settings



Port Alias: Port0

Baudrate: 38400

Parity: No

Data Bits: 8

Stop Bits: 1

Flow Control: No Flow

Interface: RS232

Performance: Throughput

Delimiter 1: 0 (HEX) □ Enabled

Delimiter 2: 0 (HEX) □ Enabled

Delimiter 3: 0 (HEX) □ Enabled

Delimiter 4: 0 (HEX) □ Enabled

Flush Ethernet to Serial Data Buffer After: 0 (0-65535) ms

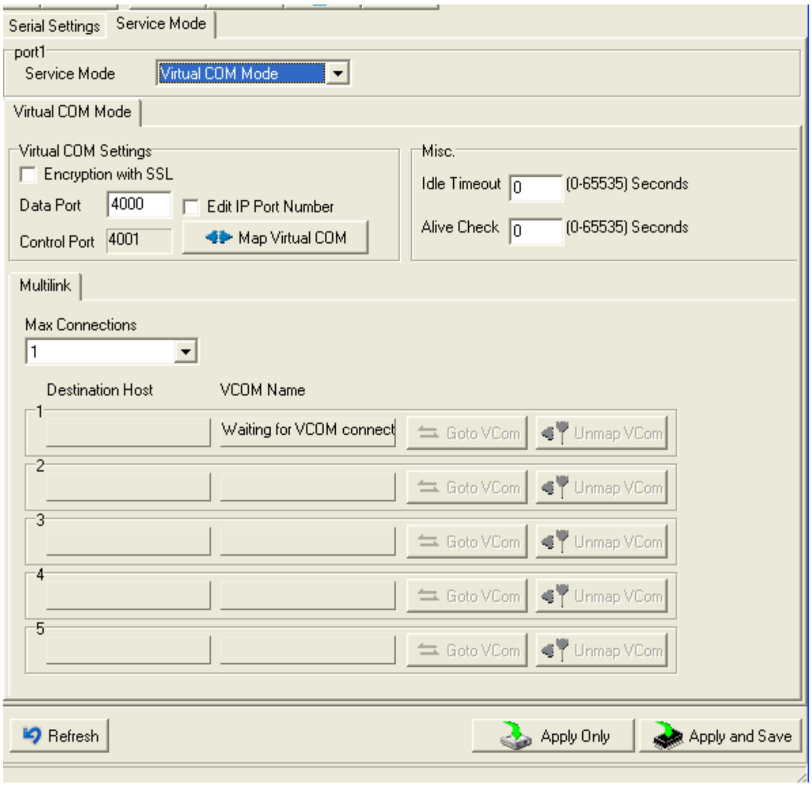
The received data will be queueing in the buffer until all the delimiters are matched. When the buffer is full (4K Bytes) or after "flush E2S data buffer" timeout, the data will also be sent.

The following table describes the labels in this screen.

Label	Description
Port Alias	Remark the port to hint the connected device.
Interface	RS232
Baud rate	110bps/300bps/1200bps/2400bps/4800bps/9600bps/19200bps/ 38400bps/57600bps/115200bps
Data Bits	5, 6, 7, 8
Stop Bits	1, 2 (1.5)
Parity	No, Even, Odd, Mark, Space
Flow Control	No, XON/XOFF
Performance	Throughput: This mode optimized for highest transmission speed. Latency: This mode optimized for shortest response time.
Serial 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 queuing 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 seconIMG.
Ethernet to Serial	**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. **Flush Data Buffer After:** The received data will be queuing in the buffer until all the delimiters are matched. When the buffer is full (4K Bytes) or after "**flushE2S data buffer**" timeout the data will also be sent. You can set the time from 0 to 65535 seconIMG.
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.

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.



port1

Service Mode: Virtual COM Mode

Virtual COM Settings

□ Encryption with SSL

Data Port: 4000

Control Port: 4001

□ Edit IP Port Number

Misc.

Idle Timeout: 0 (0-65535) Seconds

Alive Check: 0 (0-65535) Seconds

Multilink

Max Connections: 1

	Destination Host	VCOM Name
1		Waiting for VCOM connect
2		
3		
4		
5		

The following table describes the labels in this screen.

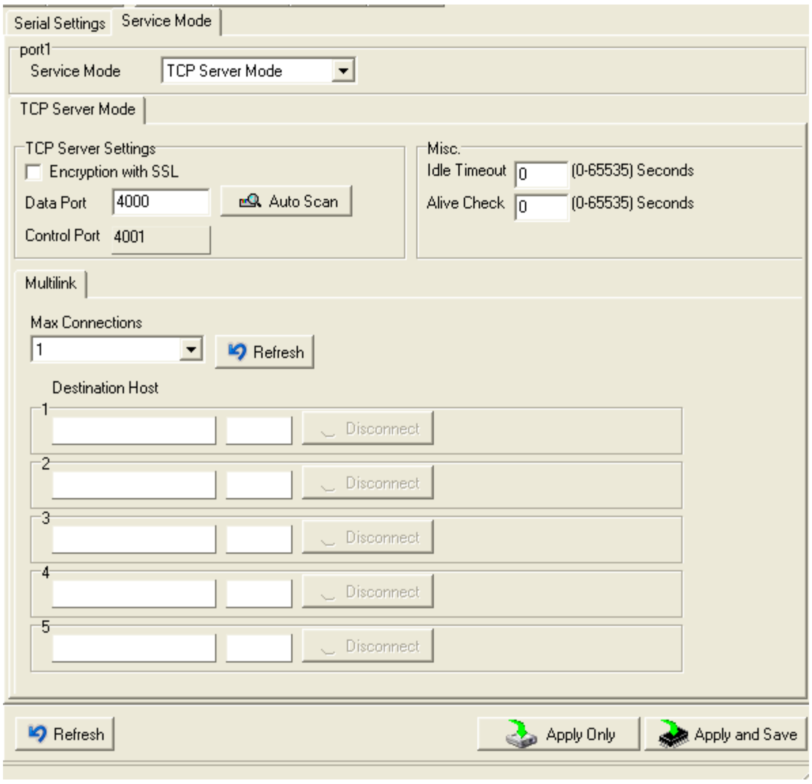
Label	Description
Encryption with SSL	Use SSL to encrypt data.
Map Virtual COM	Select a Virtual COM Name to map on.
Max Connection	The number of Max connection can support simultaneous connections are 5, default values is 1.
Idle Timeout	When serial port stops data transmission for a defined period of time (Idle Timeout), the connection will be closed and the port will be freed and try to 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.
Alive Check	The serial device will send TCP alive-check package in each defined time 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.

*Not allowed to mapping Virtual COM from web

Service Mode – TCP Server Mode

In TCP Server Mode, IMG is configured with a unique Port combination on a TCP/IP network. In this case, IMG waits passively to be contacted by the device. After a connection is established, 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.



port1

Service Mode: TCP Server Mode

TCP Server Settings

□ Encryption with SSL

Data Port: 4000

Control Port: 4001

Misc.

Idle Timeout: 0 (0-65535) Seconds

Alive Check: 0 (0-65535) Seconds

Max Connections: 1

Destination Host

Figure 5-16 TCP Server mode

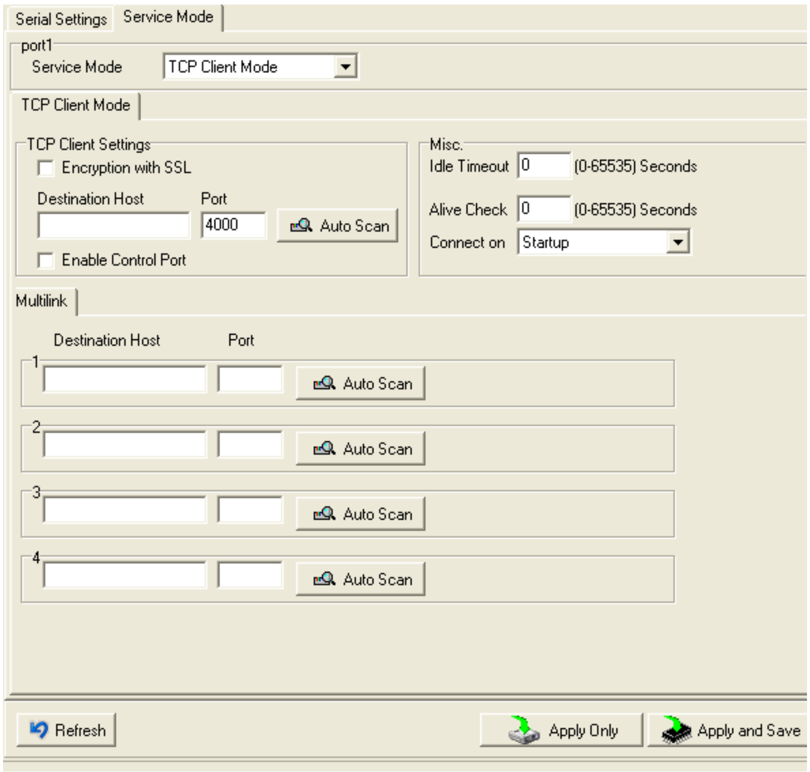
The following table describes the labels in this screen.

Label	Description
Encryption with SSL	Use SSL to encrypt data.
Data Port	Set the port number for data transmission.
Auto Scan	Scan the data port automatically.
Idle Timeout	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 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.
Alive Check	The serial device will send TCP alive-check package in each defined time 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.

Table 5-11 TCP Server mode

Service Mode – TCP Client Mode

In TCP Client Mode, device can establish a TCP connection with server by the method you have settled (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 time settings.



Service Mode: TCP Client Mode

□ Encryption with SSL

Destination Host:

Port: 4000

□ Enable Control Port

Idle Timeout: 0 (0-65535) Seconds

Alive Check: 0 (0-65535) Seconds

Connect on: Startup

Figure 5-17 TCP Client Mode

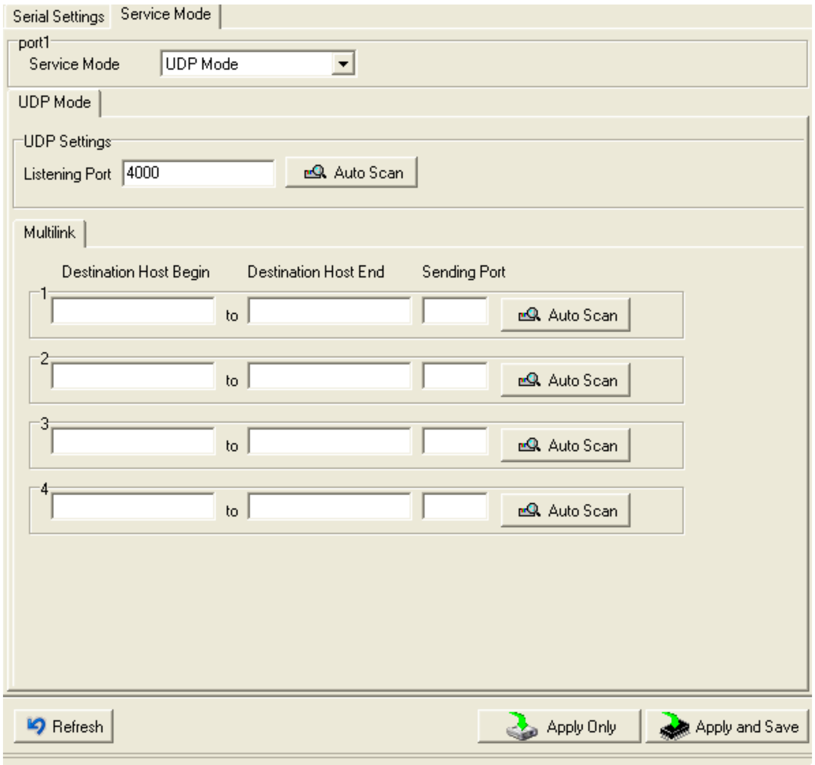
The following table describes the labels in this screen.

Label	Description
Encryption with SSL	Use SSL to encrypt data.
Destination Host	Set the IP address of host.
Port	Set the port number of data port.
Idle Timeout	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 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.
Alive Check	The serial device will send TCP alive-check package in each defined time 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.
Connect on Startup	The TCP Client will build TCP connection once the connected serial device is started.
Connect on Any Character	The TCP Client will build TCP connection once the connected serial device starts to send data.

Table 5-12TCP Client mode

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



Service Mode: UDP Mode

Listening Port: 4000

Technical Specifications

ORing M2M Model	IMG-111
Physical Ports	
10/100 Base-T(X) Ports in RJ45 Auto MDI/MDIX	**1**
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
Antenna	GSM/DCS/UMT 3G antenna x1
Serial Ports	
Connector	DB9 Male x 1
Operation Mode	RS-232
Serial Baud Rate	110 bps to 115.2 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, GND
LED Indicators	
Power indicator	Green On: Power is on and functioning Normally.
Status indicator	Green : System status indicator
Fault indicator	Amber on : WAN connection link down
WAN	Green on : 3.5G dial up Green blinking : 3.5G disconnect
Serial TX/RX LED	Red : Receiving data Green : Transmitting data
10/100TX RJ45 port indicator	Green for port Link/Act.
Fault Contac	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Power input	12-48VDC power input on terminal block
Power consumption	4.5 Watts
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	41 (W) x 70 (D) x 95 (H) mm (1.61 x 2.76 x 3.74 inch)
Weight (g)	360 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