RELIABLE SECURE CONNECTIVITY

XMT59XX Series
Modbus Gateway and
Data Concentrator

User Manual

V1.5

August 8th, 2023

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the **Table of Contents** to go to that page.

Important Announcement

The information contained in this document is the property of Agatel, Inc., and is supplied for the sole purpose of operation and maintenance of Agatel, Inc., products.
No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of Agatel, Inc.,
Offenders will be held liable for damages and prosecution.
All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.
Suggestions for improvement are welcome.
All other product’s names referenced herein are registered trademarks of their respective companies.

Documentation Control

Author:	Nonswitch Team
Revision:	1.5
Revision History:	Add Chapter 4.8 Data Concentrator
Creation Date:	24 March 2017
Last Revision Date:	8 August 2023
Product Reference:	XMT59XX Series Modbus Gateway and Concentrator User Manual
Document Status:	Update

Table of Contents

Table of Figures

List of Tables

1 Preface

1.1 *Purpose of the Manual*

This manual supports the user during the installation and configuring of the XMT59XX Series Modbus Gateway. It explains the technical features available with the mentioned product. As such, it contains some advanced network management knowledge, instructions, examples, guidelines and general theories designed to help users manage this device and its corresponding software. A background in general theory is necessary when reading it. Please refer to the Glossary for technical terms and abbreviations (if any).

1.2 *Who Should Use This User Manual*

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations. It might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first time users. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.Agatel.co.uk

1.3 *Supported Platform*

This manual is designed for **XMT59XX Series Modbus Gateway** and that series only**.**

1.4 *Manufacturers' FCC Declaration of Conformity Statement*

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause an undesired operation.

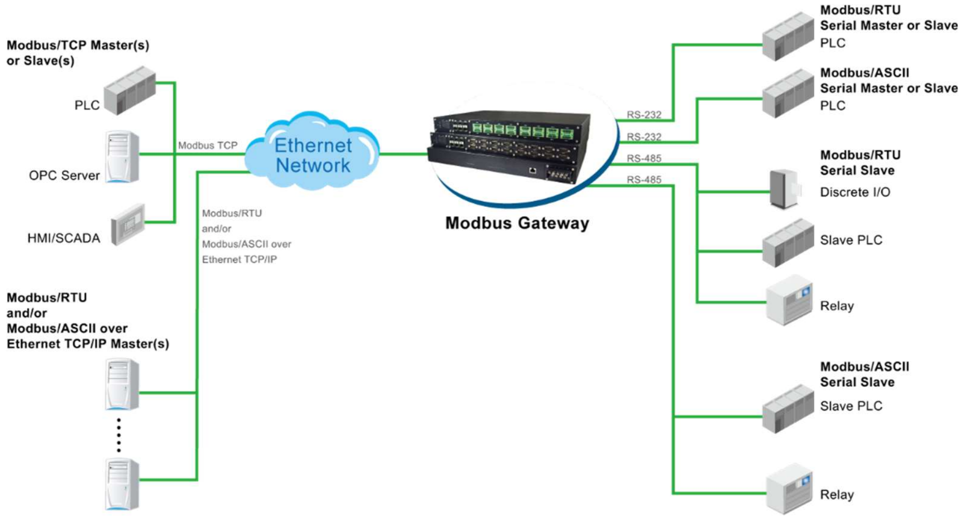
Note: all the figures herein are intended for illustration purposes only. This software and certain features work only on certain Agatel's devices.

2 Introduction

2.1 Overview

The XMT59XX Modbus Gateway is an industrial network device in between Modbus over Serieal Line devices and computer hosts running Modbus/TCP on Ethernet network. Figure 2.1 illustrates a possible network configuration of the XMT59XX Series Modbus Gateway. Fully compliant with Modbus/TCP protocol, the Modbus gateway offers a convenient solution to connect existing devices or controllers running Modbus serial protocol (Modbus/ASCII or Modbus/RTU) to an Ethernet network. The XMT59XX Series are standard Modbus gateways that convert packets between Modbus TCP and Modbus RTU/ASCII protocols.

The XMT59XX Series supports 64 simultaneous TCP masters. Overall, 247 Servers are supported (TCP, COM and VCOM). Each RS-232/422/485 serial port can be individually configured for Modbus/RTU or Modbus/ASCII operation with different baud rate, allowing both types of networks to be fully integrated with Modbus/TCP within one package.


Modbus/TCP Master(s) or Slave(s)
PLC
OPC Server
HMI/SCADA
Modbus TCP
Ethernet Network
Modbus/RTU and/or Modbus/ASCII over Ethernet TCP/IP
Modbus/RTU and/or Modbus/ASCII over Ethernet TCP/IP Master(s)
Modbus Gateway
RS-232
RS-232
RS-485
RS-485
Modbus/RTU Serial Master or Slave
PLC
Modbus/ASCII Serial Master or Slave
PLC
Modbus/RTU Serial Slave
Discrete I/O
Slave PLC
Relay
Modbus/ASCII Serial Slave
Slave PLC
Relay

Note:
A total of up to 254 slave devices can be supported.

Figure 2.1 Possible Network Configuration of XMT59XX Series Modbus Gateway

Figure 2.2 shows three different use cases of the XMT59XX Series Modbus Gateway:

1) the interface between Modbus RTU/ASCII serial host to Modbus RTU/ASCII serial devices
2) the interface between Modbus/TCP over Ethernet network to Modbus RTU/ASCII serial devices
3) the interface between Modbus RTU/ASCII host connected through Serial IP over Ethernet (virtual communication port (VCOM)) to Modbus RTU/ASCII serial devices.

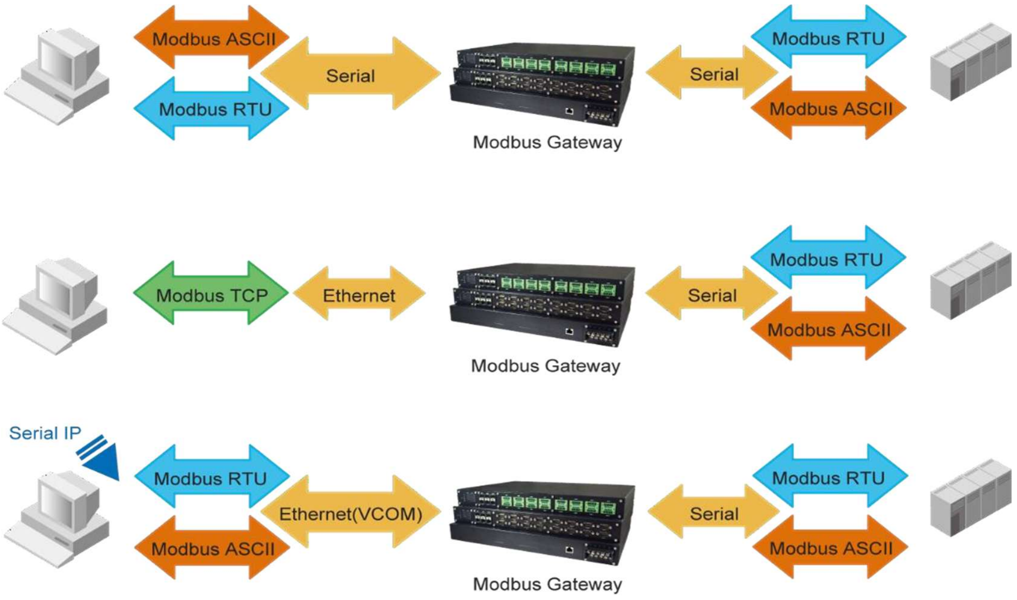


Figure 2.2 Use Cases of the XMT59XX Series Modbus Gateway

Caution

Beginning from here, extreme caution must be exercised.

Never install or work with electricity or cabling during periods of lightning activity. Never connect or disconnect power when hazardous gases are present.

Warning: HOT!

WARNING: Disconnect the power and allow unit to cool for 5 minutes before touching.

3 Getting Started

3.1 *Packing List*

Inside the purchased package, you will find the following items.

Table 3.1 Packing List

Item	Quantity	Description
XMT59XX/ XMT59XX-CT	1	Industrial Serial Device Server
Mounting Kit	1	On XMT5908 / XMT5916 / XMT5908A / XMT5916A • Rack Mounting Type-L angles (x 2) • Screws (x 6) On XMT5901(XMT59XX Only) / XMT5904D / XMT5901B (XMT59XX Only) - DIN Rail Kit
Terminal Block		Power Supply/ Relay output: • TB3 x 1: 3-pin 5.08mm lockable Terminal Block (XMT5901, XMT5901B) • TB3 x 2: 3-pin 5.08mm lockable Terminal Block (XMT5908-DC,XMT5916- DC) TB7 x1: 7-pin 5.08mm lockable Terminal Block (XMT5904D only) Serial ports: Terminal block is included only on TB model • TB5 x 1: 5-pin 5.08mm lockable Terminal Block (XMT5901) • TB5 x 4: 5-pin 5.08mm lockable Terminal Block (XMT5904D) • TB5 x 8: 5-pin 5.08mm lockable Terminal Block (XMT5908A) • TB5 x 16: 5-pin 5.08mm lockable Terminal Block (XMT5916A)
Documentation	1	Hardware Installation Guide (Warranty card is included)

Note:

- Notify your sales representative immediately if any of the above items is missing or damaged upon delivery.
- Agatel's utility software Device View© and Serial Manager© are obsolete and replaced by Device Management Utility®.

Table 3.2 Optional Accessories

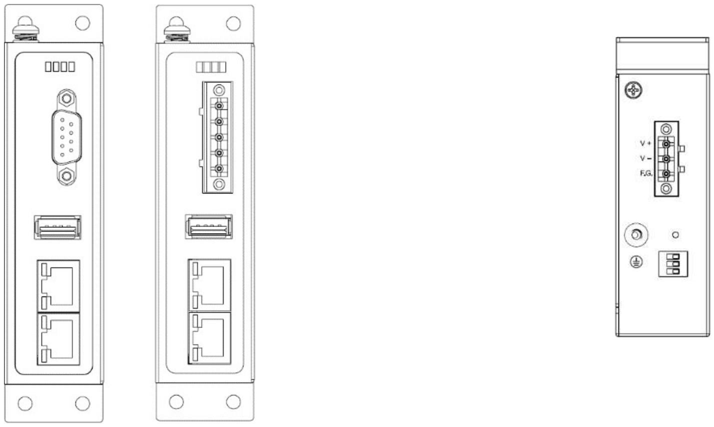
XMT5901, XMT5901B		
Model Name	**Part Number**	**Description**
UN315-1212(US-Y)	50500151120003G	Y-Type power adaptor, 100~240VAC input, 1.25A @ 12VDC output, US plug, LV6
UNE315-1212(EU-Y)	50500151120013G	Y-Type power adaptor, 100~240VAC input, 1.25A @ 12VDC output, EU plug, LV6
WMK-315-Black	70100000000050G	Black Aluminum Wall Mount Kit
ADP-DB9(F)-TB5	59906231G	Female DB9 to Female 3.81mm, a TB5 Converter
XMT5908, XMT5916		
Model Name	**Part Number**	**Description**
AD17-24D (EU-Y)	50500151240012G	Y-Type power adaptor,100-240VAC input, 0.6A @ 24VDC output, EU plug

AD17-24C (US-Y)	50500151240002G	Y-Type power adaptor,100-240VAC input, 0.6A @ 24VDC output, US plug
RMK-718-Black	70100000000040G	Rack Mount Mounting-Kit, Black (XMT5908, XMT5916 only)
Power Cable (US)	50801041G	6 feet Power Cable, US (XMT5908, XMT5916 only)
Power Cable (EU)	50801051G	6 feet Power Cable, EU (XMT5908, XMT5916 only)
Fuse	50709441G	Fuse (XMT5908, XMT5916 only)
CBL-RJ45(8P)-DB9(M)-90	50891781G	RJ45 to DB9 Male Cable, 90cm (XMT5908, XMT5916 only)
CBL-RJ45(8P)-DB9(M)-200	50891951G	RJ45 to DB9 Male Cable, 200cm (XMT5908, XMT5916 only)
CBL-RJ45(8P)-DB9(F)-90	50891791G	RJ45 to DB9 Female Cable, 90cm (XMT5908, XMT5916 only)
CBL-RJ45(8)-DB9(F)-200-C	50891961G	RJ45 to DB9 Female Cross Over Cable, 200cm (XMT5908, XMT5916 only)
CBL-RJ45(8P)-DB9(F)-90-C	50891971G	8-pin RJ45-DB9 debug cable, 90cm (XMT5904D, XMT5908, XMT5916 only)
SDR-75-24	50500752240001G	75W/3.2A DIN-Rail 24VDC power supply 88~264VAC / 124-370VDC input (XMT5904D, XMT5908, XMT5916 only)
GDC-120	59906861G	120mm copper woven grounding cable
XMT5908A, XMT5916A		
Model Name	**Part Number**	**Description**
SDR-75-24	50500752240001G	75W/3.2A DIN-Rail 24VDC power supply 88~264VAC / 124-370VDC input (XMT5904D, XMT5908, XMT5916 only)
GDC-120	59906861G	120mm copper woven grounding cable
ADP-DB9(F)-TB5	59906231G	Female DB9 to Female 3.81 TB5 Converter
AXFD-1314-0523	522AXFD1314011G	SFP Transceiver;155Mbps, Multi-mode;1310nm;2km;-40~85, DDMI
AXFD-1314-0553	522AXFD1314011G	SFP Transceiver;155Mbps, Single-mode;1310nm;30km;-40~85, DDMI
XMT5904D		
Model Name	**Part Number**	**Description**
WMK-450-Black	70100000000052G	Aluminum wall mount kit
LM28-C3S-TI-N	50708031G	SFP Transceiver, 1250Mbps, 850nmVCSEL, Multi-mode, 550m, 3.3V, -20~85°C
LM38-C3S-TI-N	50709411G	SFP Transceiver, 1250Mbps, 1310nmFP, Multi-mode, 2km, 3.3V, -40~85°C
LS38-C3S-TI-N	50709391G	SFP Transceiver, 1250Mbps, 1310nmFP, Single-mode, 10km, 3.3V, -40~85°C
LS38-C3L-TI-N	50709441G	SFP Transceiver, 1250Mbps, 1310nmDFB, Single-mode, 30km, 3.3V, -40~85°C
ADP-DB9(F)-TB5	59906231G	Female DB9 to Female 3.81mm, a TB5 Converter
CBL-RJ45(8P)-DB9(F)-90-C	50891971G	8-pin RJ45-DB9 debug cable, 90cm (XMT5904D, XMT5908, XMT5916 only)
SDR-75-24	50500752240001G	75W/3.2A DIN-Rail 24VDC power supply 88~264VAC / 124-370VDC input (XMT5904D, XMT5908, XMT5916 only)
GDC-120	59906861G	120mm copper woven grounding cable

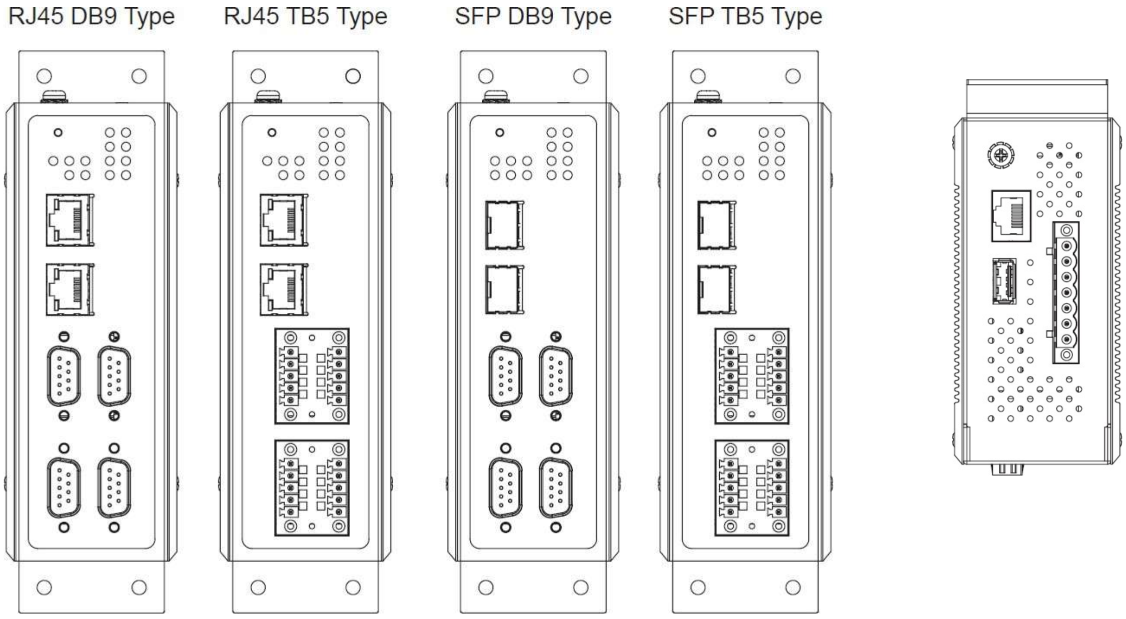
3.2 *Appearance, Front and Rear Panels*

The following figures show particular XMT59XX series device’s front and rear panels.

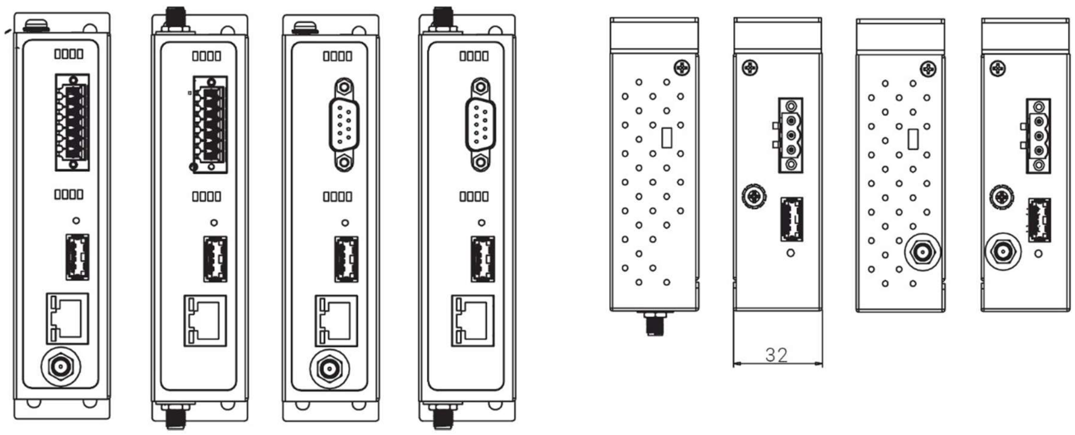
XMT5901



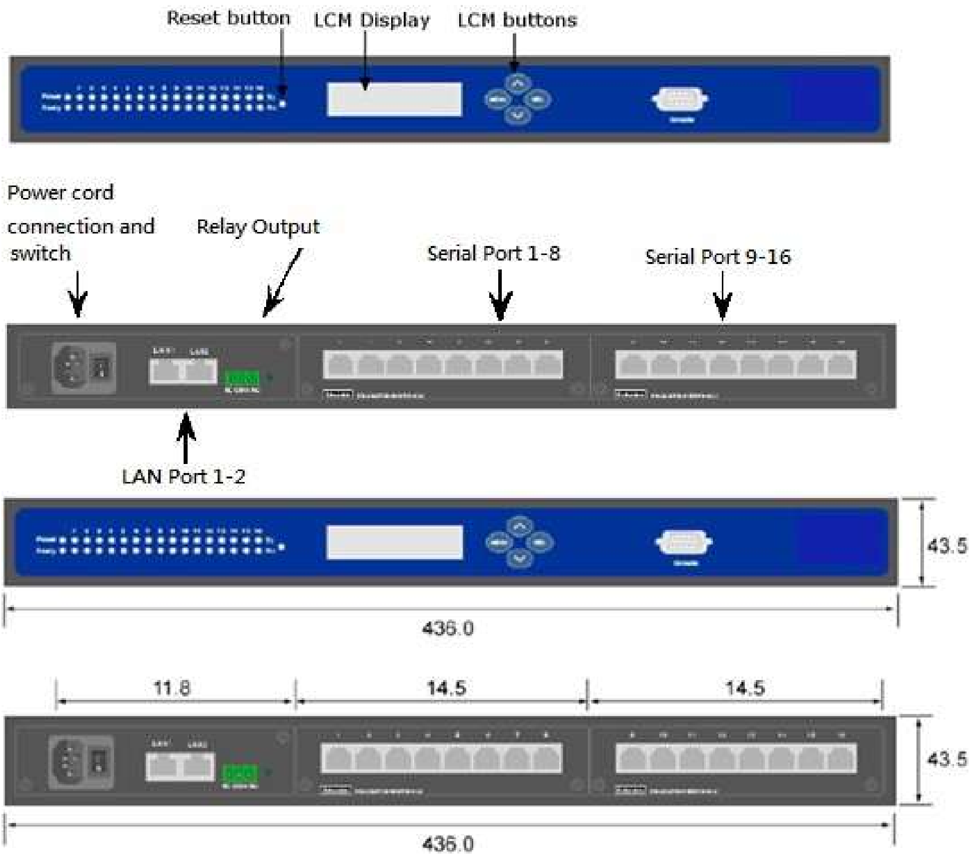
XMT5904D



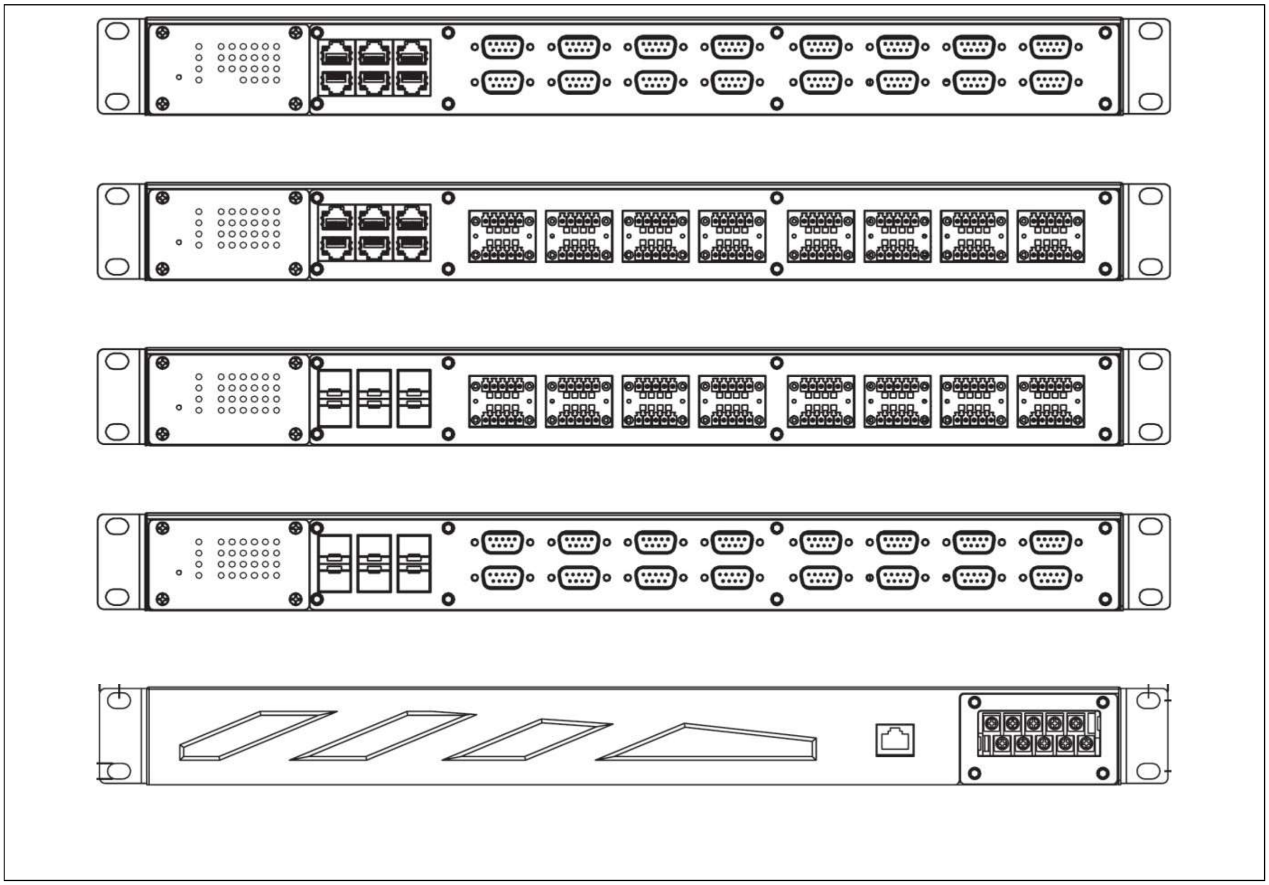
XMT5901B



XMT5908/16



XMT5908A/16A



3.3 *First Time Installation*

Before installing the device, please follow strictly all safety procedures described in the Hardware installation guide supplied inside the product. Agatel will not be liable for any damages to property or personal injuries resulting from the installation or overall use of the device. Do not attempt to manipulate the product in any way if unsure of the steps described there. In such cases, please contact your dealer immediately.

Specific installation instructions are not provided in this manual since they may differ considerably based on the hardware purchased.

3.4 *Factory Default Settings*

3.4.1 *Network Default Settings*

The XMT59XX Modbus Gateway comes with one IP address specifically for redundant Ethernet interfaces.

Interface	Device IP	Subnet Mask	Gateway IP
LAN 1	10.0.50.100	255.255.0.0	10.0.0.254
LAN 2	192.168.1.1	255.255.255.0	192.168.1.254
LAN 3~6 (XMT5908A and XMT5916A only)	192.168.2.1~5.1	255.255.255.0	192.168.1.254

Remarks: Default DNS 1 setting is 168.95.1.1 and DNS 2 setting is 0.0.0.0.

3.4.2 *Modbus Default Settings*

The XMT59XX Modbus Gateway comes with the following default Modbus settings.

Table 3.3 Modbus Default Settings

Parameter	**Default Values**
Modbus Master	
TCP Settings	TCP Master Mode: TCP Master Port: 502
Modbus Slave	
• XMT5901 • XMT5904 • XMT5908 • XMT5916 • XMT5908A • XMT5916A	Mode: RTU Slave Serial Configuration: RS-232, 9600 bps, 8 data bits, No parity bit, 1 stop bit, No Flow Control, Buffer Disable

Other default settings are shown in the following table.

Table 3.4 Other Default Settings

Parameter	**Default Values**
Security	
User Name	admin
Password	default
SNMP	
SysName of SNMP	Agatel
SysLocation of SNMP	Location
SysContact of SNMP	Contact
SNMP	Disable (Unchecked)
Read Community	Public
Write Community	Private
SNMP Trap Server	0.0.0.0

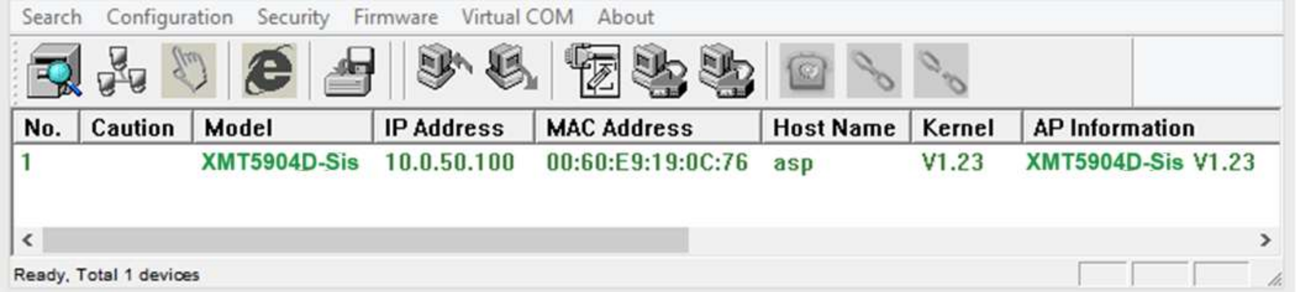
Note: Press the “Reset” button on the front panel for 5 seconds (see Section 4.16.8 and Section 4.17), to restore the XMT59XX Series Modbus Gateway to the factory default settings.

4 Configuration and Setup

It is strongly recommended for the user to set the Network Parameters through **Device Management Utility©** first. Other device-specific configurations can later be carried out via Agatel's user-friendly Web-Interface.

4.1 *Configuration of Network Parameters through Device Management Utility*

First, please install Agatel's configuration utility program called **Device Management Utility®** that comes with the Product CD For more information on how to install **Device Management Utility®**, please refer to the manual that comes in the Product CD. After you start **Device Management Utility®**, if the Modbus Gateway is already connected to the same subnet as your PC, the device can be accessed via broadcast packets. **Device Management Utility®** will automatically detect your Modbus Gateway and list it on **Device Management Utility®**'s window. Alternatively, if you did not see your Modbus Gateway on your network, press "**Rescan**" icon, a list of devices, including your Modbus Gateway device currently connected to the network will be shown in the window of **Device Management Utility®** as shown in Figure 4.1.

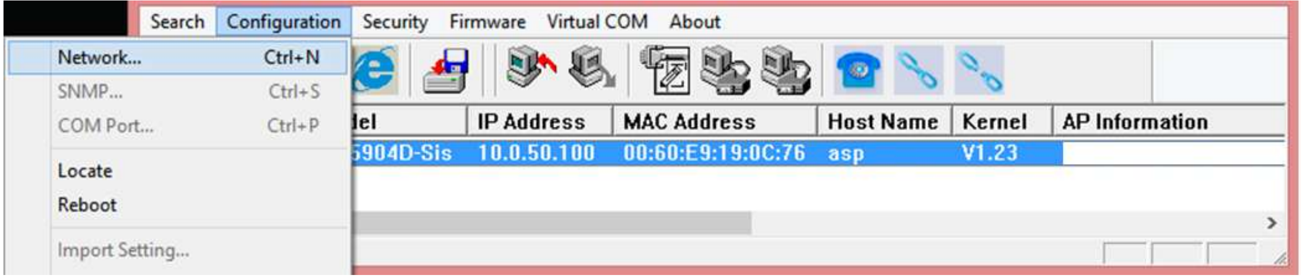


No.	Caution	Model	IP Address	MAC Address	Host Name	Kernel	AP Information
1		XMT5904D-Sis	10.0.50.100	00:60:E9:19:0C:76	asp	V1.23	XMT5904D-Sis V1.23

Ready, Total 1 devices

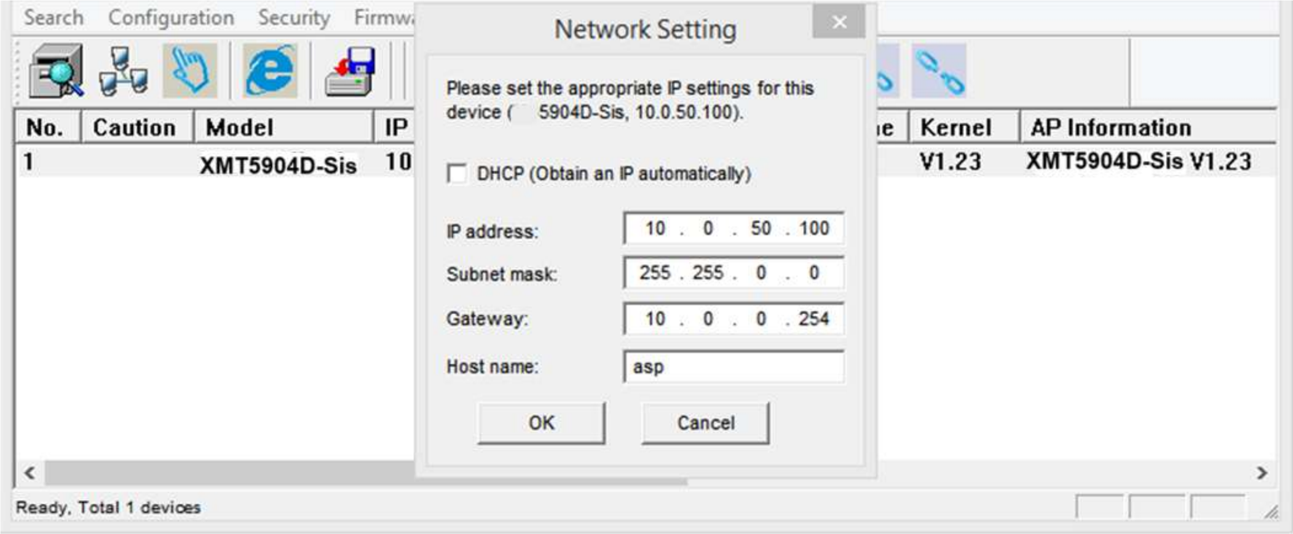
Figure 4.1 List of Device in Device Management Utility

Note: This figure is for illustration purpose only. Actual values/settings may vary between devices.
Sometime the Modbus Gateway device might not be in the same subnet as your PC; therefore, you will have to use Agatel's utility to locate it in your virtual environment. To configure each device, first click to select the desired Modbus Gateway device (default IP: 10.0.50.100) in the list of **Device Management Utility©**, and then click "**Configuration →**□ **Network**…" (or Ctrl+N) menu on **Device Management Utility©** as shown in Figure 4.2 or click on the second icon called **Network** on the menu icon bar, and a pop-up window will appear as shown in Figure 4.3.



lel	IP Address	MAC Address	Host Name	Kernel	AP Information
5904D-Sis	10.0.50.100	00:60:E9:19:0C:76	asp	V1.23	

Figure 4.2 Pull-down Menu of Configuration and Network**...**



Network Setting

No.	Caution	Model	IP	…	Kernel	AP Information
1		XMT5904D-Sis	10		V1.23	XMT5904D-Sis V1.23

Please set the appropriate IP settings for this device (5904D-Sis, 10.0.50.100).

□ DHCP (Obtain an IP automatically)

IP address: 10 . 0 . 50 . 100

Subnet mask: 255 . 255 . 0 . 0

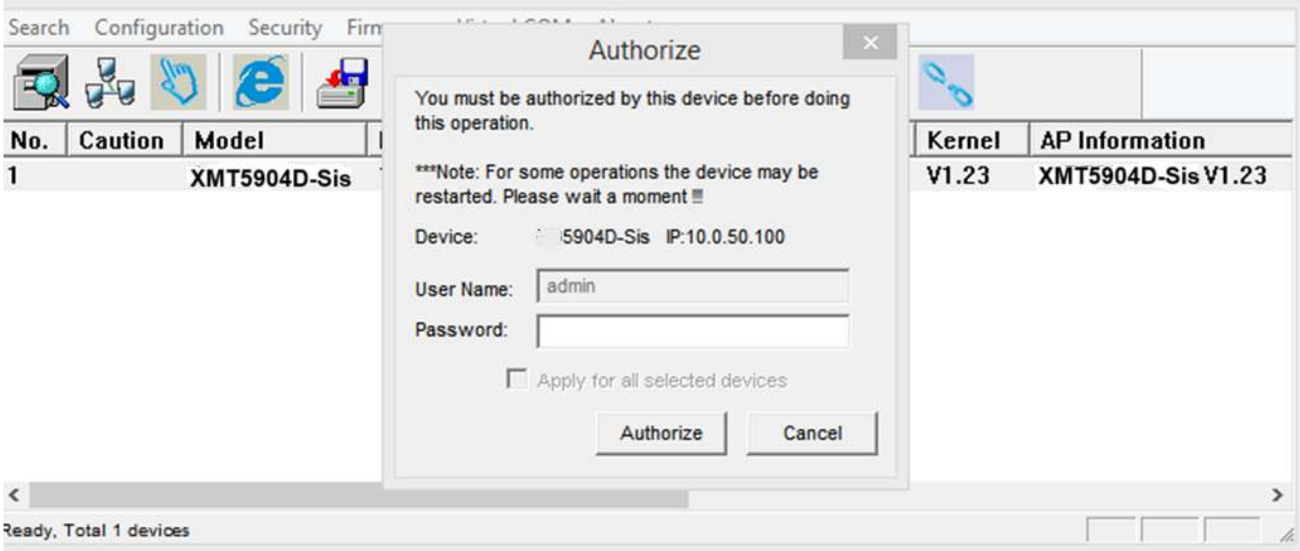
Gateway: 10 . 0 . 0 . 254

Host name: asp

Ready, Total 1 devices

Figure 4.3 Pop-up Window of Network Setting

You may proceed then to change the IP address to avoid any IP address conflict with other hosts on your LAN or to connect the device to your existing LAN as shown in Figure 4.3. The system will prompt you for a credential to authorize the changes. It will ask you for the **Username** and the **Password** as shown in Figure 4.4. The default username is “**admin**”, while the default password “**agatel**”. After clicking on the **Authorize** button, a notification window will pop-up as shown in Figure 4.5 and some device may be restarted. After the device is restarted (for some model), it will beep twice to indicate that the unit is running normally. Then, the Modbus Gateway can be found on a new IP address. It may be listed automatically by the **Device Management Utility©** or it can be found by clicking on the “**Rescan”** icon.



Authorize

No.	Caution	Model	…	Kernel	AP Information
1		XMT5904D-Sis		V1.23	XMT5904D-Sis V1.23

You must be authorized by this device before doing this operation.

***Note: For some operations the device may be restarted. Please wait a moment !!

Device: 5904D-Sis IP:10.0.50.100

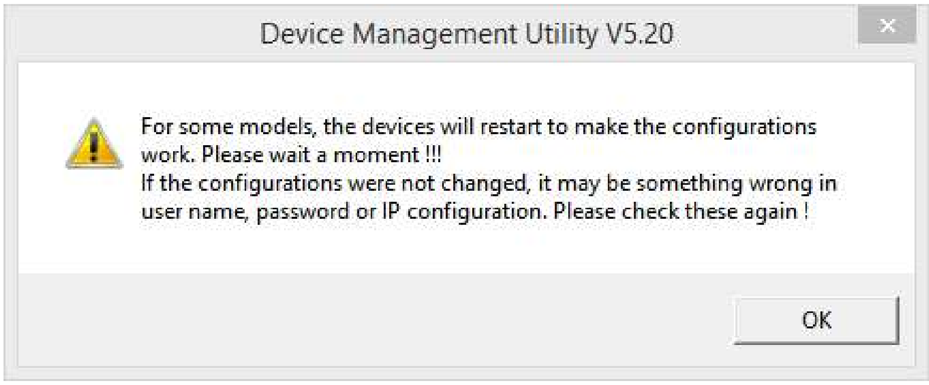
User Name: admin

Password:

□ Apply for all selected devices

Ready, Total 1 devices

Figure 4.4 Authorization for Changes of Network Setting



Device Management Utility V5.20

For some models, the devices will restart to make the configurations work. Please wait a moment !!!
If the configurations were not changed, it may be something wrong in user name, password or IP configuration. Please check these again !

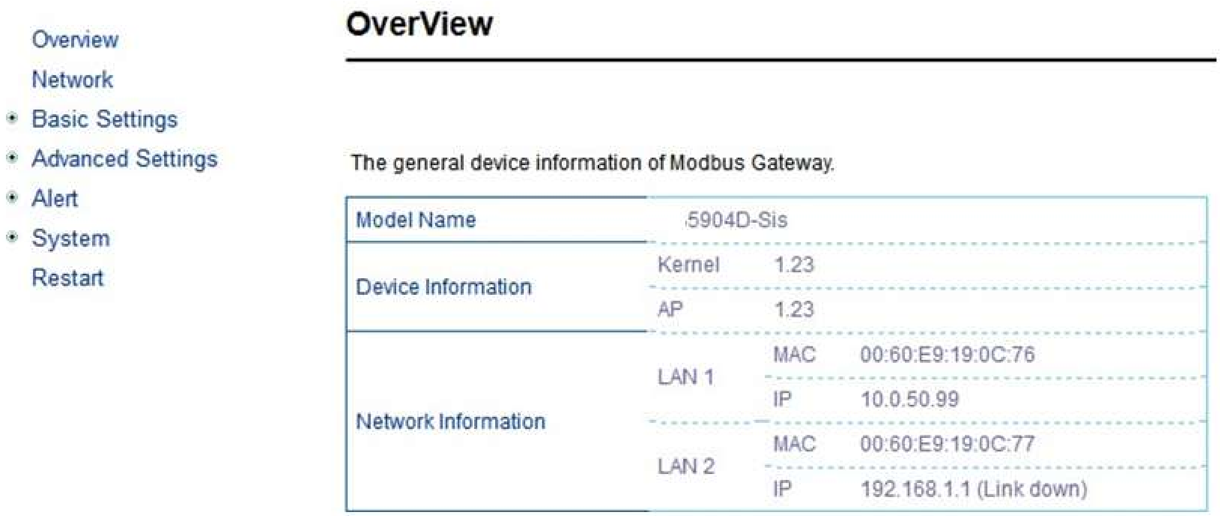
Figure 4.5 Pop-up Notification Window after Authorization

Please consult your system administrator if you do not know your network's subnet mask and gateway address.

Note: If your LAN address begins with 192.168.X.X, please use the LAN2 interface for configuration.

4.2 *Configuring through Web Interface*

Every XMT59XX Modbus Gateway device is equipped with a built-in web server in the firmware. Therefore, the device can be accessed by using a web browser for configuring by entering the device’s IP address (default IP address is 10.0.50.100) in the URL field of your web browser. Figure 4.6 illustrates the overview page of the web interface. Please see Section 0 for default values.



OverView

The general device information of Modbus Gateway.

Model Name	5904D-Sis		
Device Information	Kernel	1.23	
	AP	1.23	
Network Information	LAN 1	MAC	00:60:E9:19:0C:76
		IP	10.0.50.99
	LAN 2	MAC	00:60:E9:19:0C:77
		IP	192.168.1.1 (Link down)

Figure 4.6 Overview Web Page of Modbus Gateway

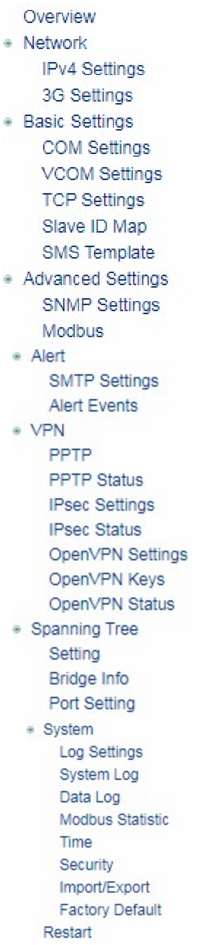


Figure 4.7 Map of Configuring Web Page on Modbus Gateway

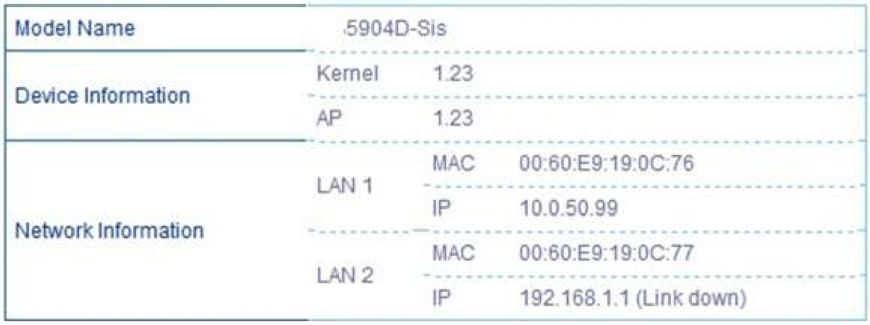
This approach for configuring your device is the most user-friendly. It is the most recommended and the most common method used for XMT59XX Series Modbus Gateway. Please go to its corresponding section for a detailed explanation.

4.3 *Configuring Automatic IP Assignment with DHCP*

A DHCP server can automatically assign IP addresses, Subnet Mask and Network Gateway to LAN1 or LAN2 interface. You can simply check the **"DHCP (Obtain an IP Automatically)"** checkbox in the Network Setting dialog as shown in Figure 4.3 using Agatel's **Device Management Utility©** and then restart the device. Once restarted, the IP address(es) will be configured automatically.

4.4 *Web Overview*

- In this section, current information on the device's status and settings will be displayed. An example of XMT5904D-Sis's overview page is shown in Figure 4.8. An example on XMT5901B (with 3G/4G is provided in the figure below

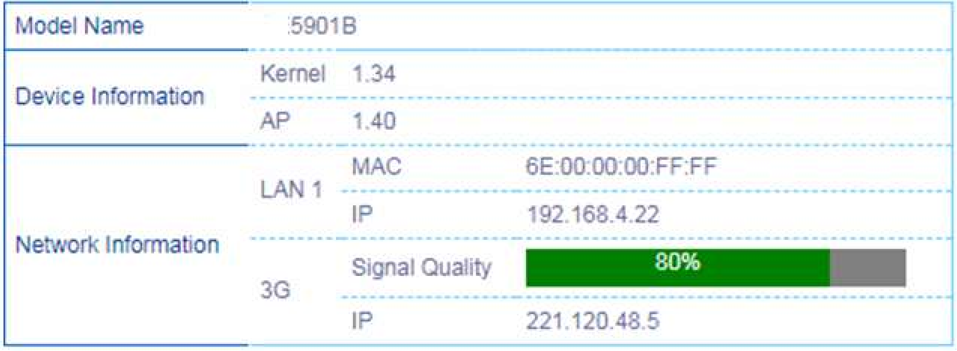


Model Name	5904D-Sis		
Device Information	Kernel	1.23	
	AP	1.23	
Network Information	LAN 1	MAC	00:60:E9:19:0C:76
		IP	10.0.50.99
	LAN 2	MAC	00:60:E9:19:0C:77
		IP	192.168.1.1 (Link down)

Figure 4.8 Overview Web Page

In detail, the following information is given:

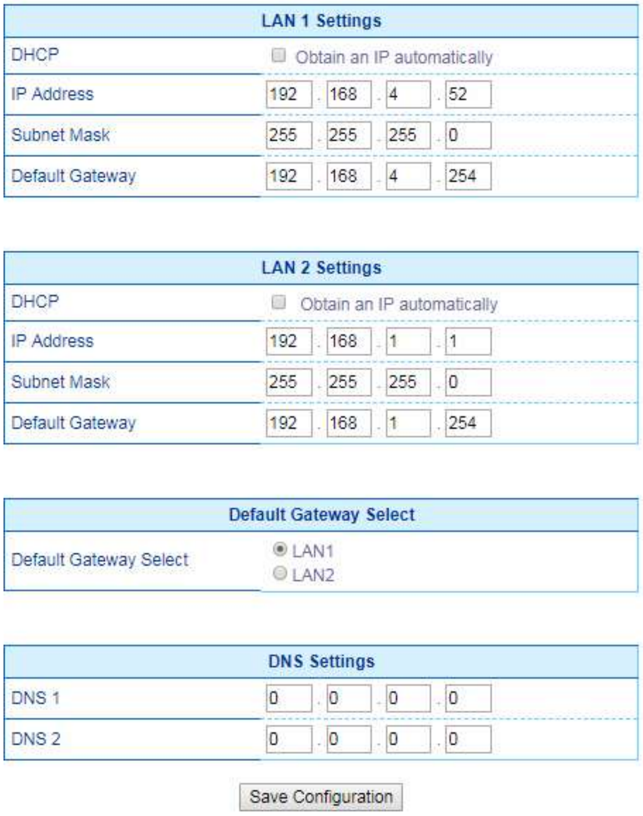
- **Model Name**, as its name implies, shows the device's model
- **Device Information** displays information on the Kernel version as well as the AP version of your Modbus Gateway device.
- **Network Information** shows the Mode in which the Modbus Gateway device is currently operating on (Dual Subnet Mode or Redundancy Mode), and one of the used LAN for Redundancy Mode as shown in Figure 4.8 or both LANs corresponding MAC and IP addresses for Dual Subnet mode.
  - **Dual Subnet Mode:** Two or six Ethernet ports have separate IP addresses and subnets.
  - **Redundancy Mode:** The system will use only one port for data transfer. If the port is disconnected, the whole system will change to another port automatically.



Model Name	5901B		
Device Information	Kernel	1.34	
	AP	1.40	
Network Information	LAN 1	MAC	6E:00:00:00:FF:FF
		IP	192.168.4.22
	3G	Signal Quality	80%
		IP	221.120.48.5

4.5 *Network Configuration*

In this section, **IP address**, **Subnet Mask**, **Default (Network) Gateway**, **Domain Name System** (**DNS**) and overall connectivity settings of Modbus Gateway device can be accessed as shown in Figure 4.9. For any LAN Interface Settings (i.e. LAN1 or LAN2), you can check the corresponding **DHCP** box to obtain an **IP address**, **Subnet Mask**, and **Default (Network) Gateway** automatically. The **Default Gateway Select** box is the next option after the LAN Interface Settings. In this box, you will have option to select (either one of the two radio buttons) which LAN interface (LAN1 or LAN2 in Figure 4.9) will be the default interface in the **Default Gateway Select** box.



LAN 1 Settings	
DHCP	□ Obtain an IP automatically
IP Address	192 . 168 . 4 . 52
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 4 . 254

LAN 2 Settings	
DHCP	□ Obtain an IP automatically
IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 1 . 254

Default Gateway Select	
Default Gateway Select	● LAN1 ○ LAN2

DNS Settings	
DNS 1	0 . 0 . 0 . 0
DNS 2	0 . 0 . 0 . 0

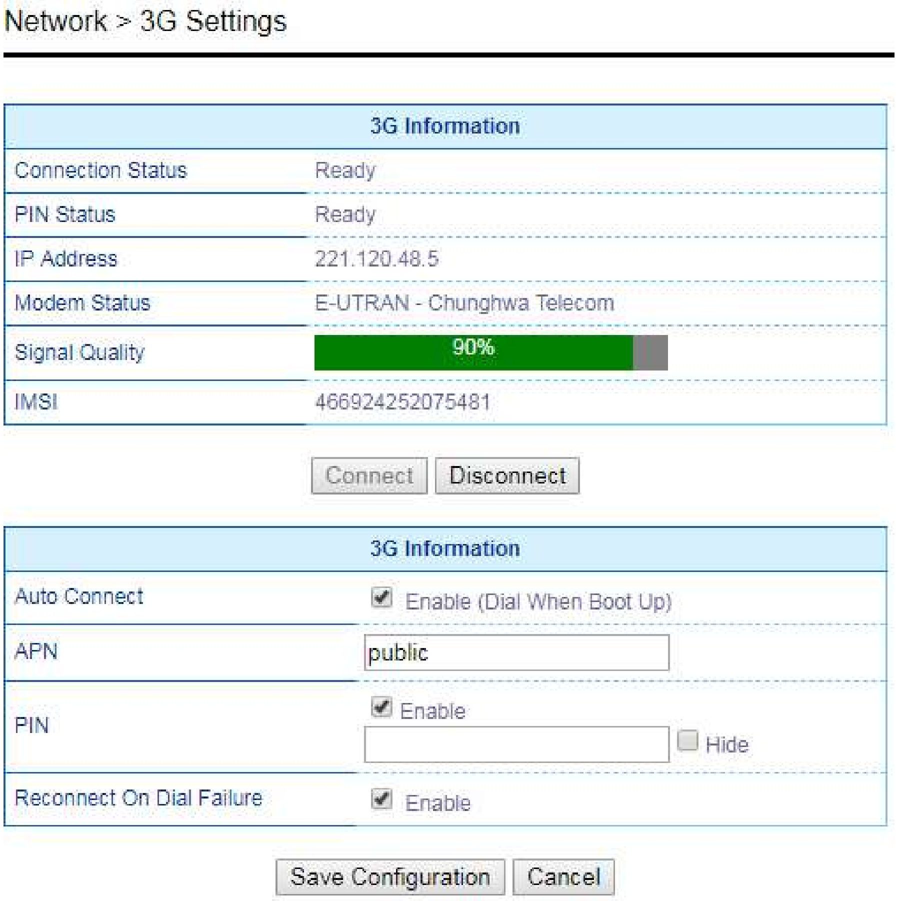
Figure 4.9 Network Web Page

At the lowest box in Figure 4.9, you will have the **DNS Settings** box which allows you to set the **IP addresses** of Domain Name Server 1 (**DNS 1**) and Domain Name Server 2 (**DNS 2**) for redundancy. If the device is connected to the Internet and should connect to other servers over the Internet to get some services such as Network Time Protocol (NTP) server, the user will need to configure the DNS server in order to be able to resolve the host name of the NTP server. Please consult your network administrator or internet service provider (ISP) to obtain local DNS's IP addresses.

4.6 *3G Settings or 4G Settings*

XMT5901B has a built-in 3G or 4G cellular network interface depending on your purchased model. On this web page, you can check the status of your cellular connection, set parameters for your cellular (3G or 4G) network configuration, and set three phone numbers that can reboot the XMT5901B. Figure 4.10 shows an example of **3G Settings** web page which is divided into three parts: **3G Information**, **3G Configuration**, and **Phone Number Settings**.

Note: The user is required to insert a valid SIM card of your local cellular network operator (3G or 4G) into the SIM card socket inside the chassis of XMT5901B.



Network > 3G Settings

3G Information	
Connection Status	Ready
PIN Status	Ready
IP Address	221.120.48.5
Modem Status	E-UTRAN - Chunghwa Telecom
Signal Quality	90%
IMSI	466924252075481

3G Information	
Auto Connect	☑ Enable (Dial When Boot Up)
APN	public
PIN	☑ Enable □ Hide
Reconnect On Dial Failure	☑ Enable

Figure 4.10 3G Settings Web Page

Under the **3G Information** part, you can inspect the following information of your cellular network interface: **Connection Status**, **PIN Status**, **IP Address**, **Modem Status**, and **Signal Quality**. Table 4.1 describes each field under the 3G Information part. Under the 3G Information part, there are **Connect** button and **Disconnect** button that allow you to control the cellular connection.

Table 4.1 Description of 3G Information

Field Name	Description	Possible Values
Connection Status	Reports the status of cellular data connection	No Sim Card Inserted, Disable Disconnect, Connect, Dialling
PIN Status	Reports the status of the PIN	READY or some wrong!

Field Name	Description	Possible Values
IP Address	IP address assigned by the cellular operator	-
Modem Status	Reports the status of cellular modem	3G-UTRAN, E-UTRAN,…,Unknown Status
Signal Quality	Indicates the cellular network signal strength in percentage and bar graph.	0% up to 100%
IMSI	The International Mobile Subscriber Identity or IMSI is used to identify the user of a cellular network and is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network	64-bit number

Under the **3G Configuration** part, you can configure how the cellular connection is established. First option is the **Auto Connect**. You can check the box in front of **Enable (Dial When Boot Up)** to let the XMT5901B automatically dials 3G Modem when the device finished booting up. Next, the **APN** option which is the Access Point Name used for establishing the cellular connection. This name is depended on your local cellular network operator's recommendation. The default value is "internet". Next, the **PIN** or Personal Identification Number option is the 4-digit code used to unlock the SIM of the 3G Modem on the XMT5901B. You can enable this PIN security by checking the **Enable** box. After enabling the **PIN** option, you will be able to enter the **PIN Code** in the textbox. Note that the default display of the textbox is to hide the code. You have an option to uncheck the box in front of **Hide** to see the PIN Code. Finally, the last option is to enable the **Reconnect on Dial Failure** option by checking the **Enable** box. The default for this option is disable.

After finishing the network settings configuration, please click the **Save Configuration** button to save all changes that have been made. A pop-up window will show up with **"Please wait for a while…"** message. Then, the web browser will return to the **3G Settings/4G Settings** web page again.

4.7 *Spanning Tree*

Spanning tree functionality is supported by Agatel's XMT59XX Industrial Device Server series. However, XMT59XX is only an end device in a network; therefore, it only has the receiving function of spanning tree. Generally, the **S**panning **T**ree **P**rotocol (**STP**) provides a function to prevent switching loops and broadcast radiation at the OSI layer 2. A switching loop occurs in a network when there are multiple connections or redundant paths between two network switches or at least two ports are connected on both sides of the two network switches. The switching loop can create a broadcast radiation, which is the accumulation of broadcast and multicast traffics in a computer network. As broadcast and multicast messages are forwarded by bridges/switches to every port, the bridges/switches will repeatedly rebroadcast the broadcast messages, and this accumulation of traffic can flood the network. STP creates a spanning tree topology and disables those links of the network that are not part of the spanning tree, which leaves only a single active path between two nodes. This function can avoid flooding and increase network efficiency. Therefore, XMT59XX deploys spanning tree as a tool when the users set up connection or port redundancy or fault-tolerance in their network.

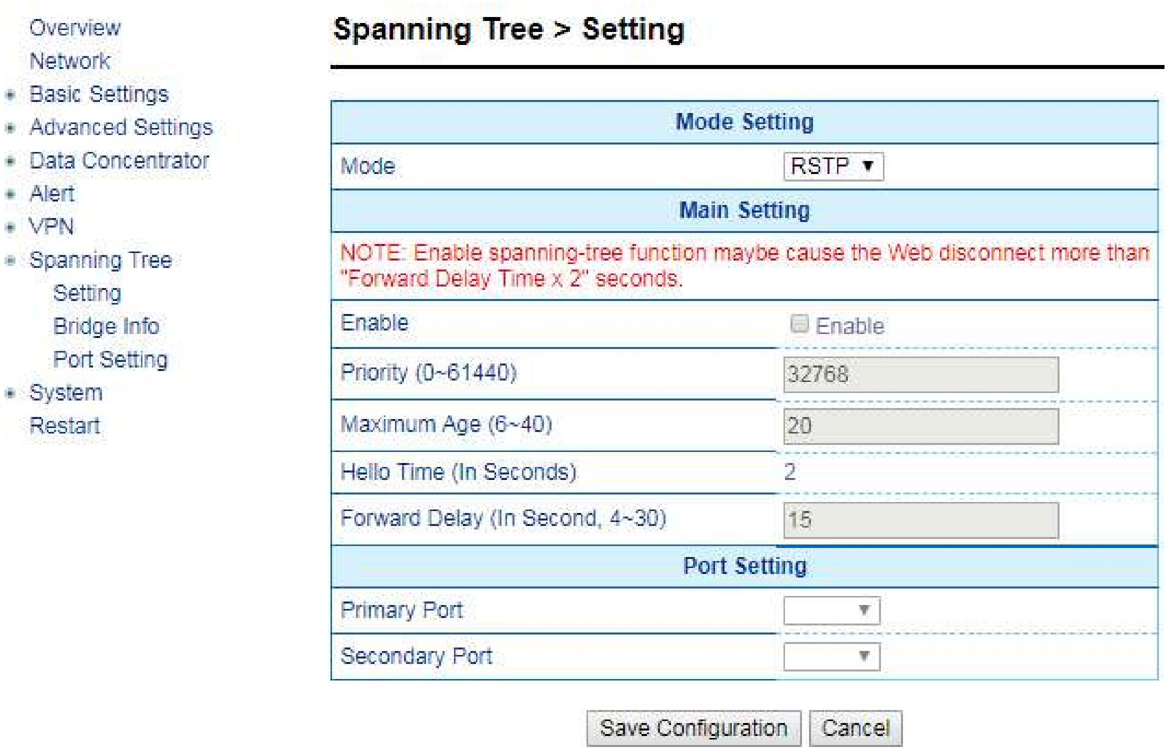
RSTP (**R**apid **S**panning **T**ree **P**rotocol), IEEE 802.1W, is the only mode of spanning tree supported in XMT59XX. It is an evolution of the STP (IEEE 802.1D standard), but it is still backwards compatible with standard STP. RSTP has the advantage over the STP. When there is a topology change such as link failure in the network, the RSTP will converge significantly faster to a new spanning tree topology. RSTP improves convergence on point-to-point links by reducing the Max-Age time to 3 times Hello interval, removing the STP listening state, and exchanging a handshake between two switches to quickly transition the port to forwarding state.

The **Spanning Tree** menu and its sub-menus can be found on left frame of the web interface of XMT59XX. The list of **Spanning Tree** menu is shown in Figure 4.11. The sub-menus und the **Spanning Tree** are **Setting**, **Bridge Info**, and **Port Setting**. Each of this sub-menu will be described in the following subsections.

Figure 4.11 Spanning Tree Menu

4.7.1 *Spanning Tree's Setting*

Figure 4.12 shows an example of **Setting** web page of **Spanning Tree** menu. The **Spanning Tree Setting** page is divided into three parts which are **Mode Setting**, **Main Setting**, and **Port Setting**. For XMT59XX, the user can only select one spanning tree mode, which is the **RSTP** (Rapid Spanning Tree Protocol) under the **Mode Setting**. The user can enable or disable spanning tree protocol under the **Main Setting** by checking the box behind the **Enabled** option. Note that when Enabled option is checked, the rest of the fields will become active. Then, the user can configure the **Prioirty**, **Maximum Age**, **Hello Time**, and **Forward Delay** or can leave the default setting values for each of these options. Under the **Port Setting** part, the user can select two different ports for **Primary Port** and **Secondary Port** options from the drop-down list. After configuring the spanning tree's parameters, please click **Update** button at the end of the page to allow the change to take effect. The description of each parameter is summarized in Table.



Spanning Tree > Setting

Mode Setting	
Mode	RSTP ▼
Main Setting	
NOTE: Enable spanning-tree function maybe cause the Web disconnect more than "Forward Delay Time x 2" seconds.	
Enable	□ Enable
Priority (0~61440)	32768
Maximum Age (6~40)	20
Hello Time (In Seconds)	2
Forward Delay (In Second, 4~30)	15
Port Setting	
Primary Port	▼
Secondary Port	▼

Figure 4.12 Setting Web Page of Spanning Tree

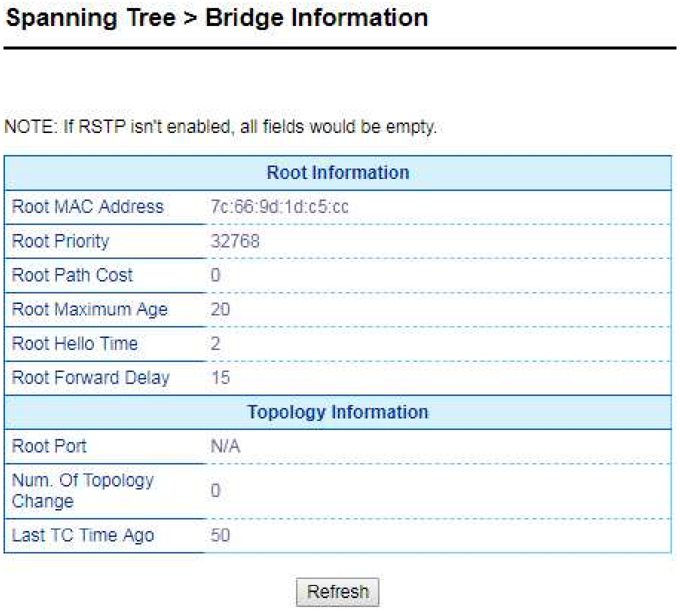
Table 4.2 Descriptions of Spanning Tree Parameters

Label	Description	Default Factory
Mode	Mode of Spanning Tree Protocol to be enabled on XMT59XX	RSTP
Enabled	Check the box to enable spanning tree functionality.	Disable
Priority	Enter a number to set the device priority**.** The value is in between 0 and 61440**.** The lower number gives higher priority**.**	32768
Maximum Age	Maximum expected arrival time for a hello message**.** It should be longer than Hello Time**.**	20
Hello Time	Hello time interval is given in seconds. The value is in between 1 to 10.	2
Forward Delay	Specify the time spent in the listening and learning states in seconds. The value is in between 4 to 30.	15
Primary Port	Spanning tree’s primary port	LAN1
Secondary Port	Spanning tree’s secondary port	LAN2

Note: To disable spanning tree function on XMT59XX, the user can uncheck the **Enable** option and then click **Update** butoon.

4.7.2 *Spanning Tree’s Bridge Info*

Bridge Info (information) provides the current configured parameters of spanning tree protocol as shown in Figure 4.13. Note that this page will not display any data on all fields if the RSTP was not enabled in the Spanning Tree’s **Setting** web page. The information is further divided into two parts: **Root Information** and **Topology Information**. To check the latest information, please click on the **Refresh** button at the end of the page. Table 4.3 and Table 4.4 summarize the descriptions of each entry in the root information table and topology information table, respectively.



Spanning Tree > Bridge Information

NOTE: If RSTP isn't enabled, all fields would be empty.

Root Information	
Root MAC Address	7c:66:9d:1d:c5:cc
Root Priority	32768
Root Path Cost	0
Root Maximum Age	20
Root Hello Time	2
Root Forward Delay	15
Topology Information	
Root Port	N/A
Num. Of Topology Change	0
Last TC Time Ago	50

Figure 4.13 Bridge Info Web Page of Spanning Tree

Table 4.3 Bridge's Root Information

Label	Description	Factory Default
Root MAC Address	MAC address of the root of the spanning tree	-
Root Priority	Root's priority value: The device with highest priority has the lowest priority value and it will be elected as the root of the spanning tree.	0
Root Path Cost	Root's path cost is calculated from the data rate of the device's port.	0
Root Maximum Age	Root's maximum age is the maximum amount of time that the device will maintain protocol information received on a link.	0
Root Hello Time	Root's hello time which is the time interval for RSTP to send out a hello message to the neighboring nodes to detect any change in the topology.	0
Root Forward Delay	Root's forward delay is the duration that the switch will be in learning and listening states before a link begins forwarding .	0

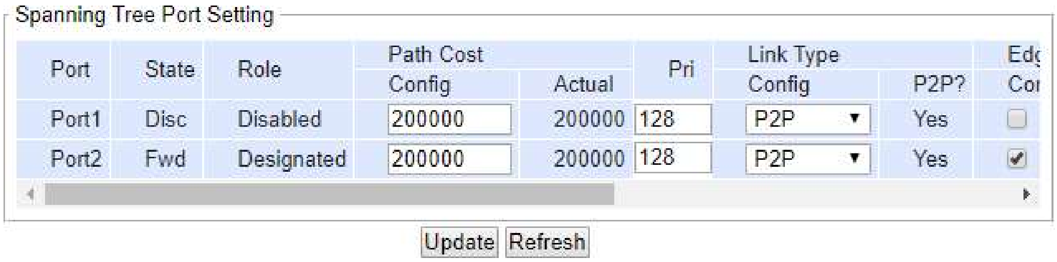
Table 4.4 Bridge's Topology Information

Label	Description	Factory Default

Root Port	A forwarding port that is the best port from non-root bridge/switch (XMT59XX) to root bridge/switch. Note that for a root switch there is no root port.	-
Num. of Topology Change	The total number of spanning topology change over time.	0
Last TC time ago	The duration of time since last spanning topology change.	-

4.7.3 *Spanning Tree's Port Setting*

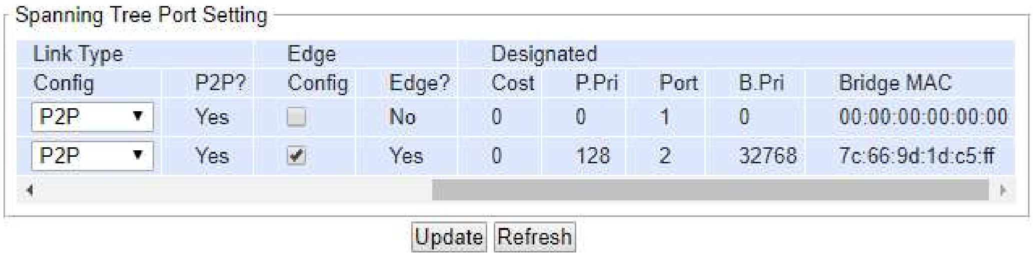
Spanning Tree's **Port Setting** shows the configured value of spanning tree protocol for each port, as shown in Figure 4.14 and Figure 4.15. The configured information for each port is **state**, **role**, **path cost**, **path priority**, **link type**, **edge**, **cost**, and **designated information**. To check the latest update on the statistics, please click on the **Refresh** button. Table 4.5 summarizes the descriptions of spanning three port setting. If **Spanning Tree** is enabled, the table of **Spanning Tree Port Stting** becomes editable and four parameters (**Path Cost** (**Config**), path priority (**Pri**), **Link Type** (**Config**) and **Edge** (**Config**)) can be adjusted on this page. The user can use the **Update** button to save the settings.



Spanning Tree Port Setting

Port	State	Role	Path Cost		Pri	Link Type		Edg
			Config	Actual		Config	P2P?	Cor
Port1	Disc	Disabled	200000	200000	128	P2P ▼	Yes	□
Port2	Fwd	Designated	200000	200000	128	P2P ▼	Yes	☑

Figure 4.14 Spanning Tree Port Setting (Part 1)



Spanning Tree Port Setting

Link Type		Edge		Designated				
Config	P2P?	Config	Edge?	Cost	P.Pri	Port	B.Pri	Bridge MAC
P2P ▼	Yes	□	No	0	0	1	0	00:00:00:00:00:00
P2P ▼	Yes	☑	Yes	0	128	2	32768	7c:66:9d:1d:c5:ff

Figure 4.15 Spanning Tree Port Setting (Part 2)

Table 4.5 Descriptions of Spanning Tree Port Setting

Label	**Description**	**Factory Default**
Port	The name of the XMT59XX's port	-
State	State of the port: **'Disc':** Discarding - No user data is sent over the port. **'Lrn':** Learning - The port is not forwarding frames yet, but it is populating its MAC Address Table. **'Fwd':** Forwarding - The port is fully operational.	N/A
Role	Non-STP or STP RSTP bridge port roles:	Non-STP

		‘Root’ - A forwarding port that is the best port from non-root bridge to root bridge. **‘Designated’** - A forwarding port for every LAN segment. **‘Alternate’** - An alternate path to the root bridge. This path is different from using the root port. **‘Backup’** - A backup/redundant path to a segment whose another bridge port already connects. **‘Disabled’** - Note strictly part of STP, a network administrator can manually disable a port.	
Path Cost		Setting the path cost for each switch port	
	Config	Setting path cost (default: 0, meaning that using the system default value (depending on link speed))	0
	Actual	The actual value path cost (For RSTP, please see Note 1 below and table.)	0
Pri		Setting the port priority, used in the Port ID field of BPDU packet, value = 16 x N, (N:0~15) See Note 2 below.	128
Link Type		The connection between two or more switches (for RSTP)	
	Config	Setting of the Link Type **P2P:** A port that operates in full-duplex mode is assumed to be point-to-pint link. **Non-P2P:** A half-duplex port (through a hub) **Auto:** Detect link type automatically	Auto
	P2P?	**Yes:** This port is a Point-to-Point (P2P). **No:** This port is not Point-to-Point (Non-P2P).	No
Edge		Edge port is a port which no other STP/RSTP switch connect to (for RSTP). An edge port can be set to forwarding state directly.	
	Config	Edge functional is set: **Yes** or **No**	No
	Edge?	**Yes:** This port is an edge port. **No:** This port is not an edge port.	No
Designated		This shows some information of the best BPDU packet through this port.	
	Cost	Root path cost	0
	P. Pri. (Port Priority)	Port priority (high 4 bits of the Port ID), Value = 16 x N, (N: 0~15)	128
	Port	Interface number (lower 12 bits of the Port ID)	-
	Bri. Pri. (Bridge Priority)	Bridge priority, (value = 4096 x N, (N: 0~15)	32768
	Bridge MAC	The MAC address of the switch which sent this BPDU	-

Note: In general, the path cost is dependent on the link speed.
Table 4.6 lists the default values of path cost for RSTP.

Table 4.6 Default Path Cost for RSTP

Data Rate	RSTP Cost (802.1W-2004)
4 Mbits/s	5,000,000
10 Mbits/s	2,000,000
16 Mbits/s	1,250,000
100 Mbits/s	200,000
1 Gbits/s	20,000
2 Gbits/s	10,000
10 Gbits/s	2,000

2. The sequence of events to determine the best received BPDU (which is the best path to the root).

- Lowest root bridge ID determines the root bridge.
- Lowest cost to the root bridge favors the upstream switch with the least cost to root.
- Lowest sender bridge ID serves as a tie breaker if multiple upstream switches have equal cost to root.
- Lowest sender port ID serves as a tie breaker if a switch has multiple (non-Ether channel) links to a single upstream switch.

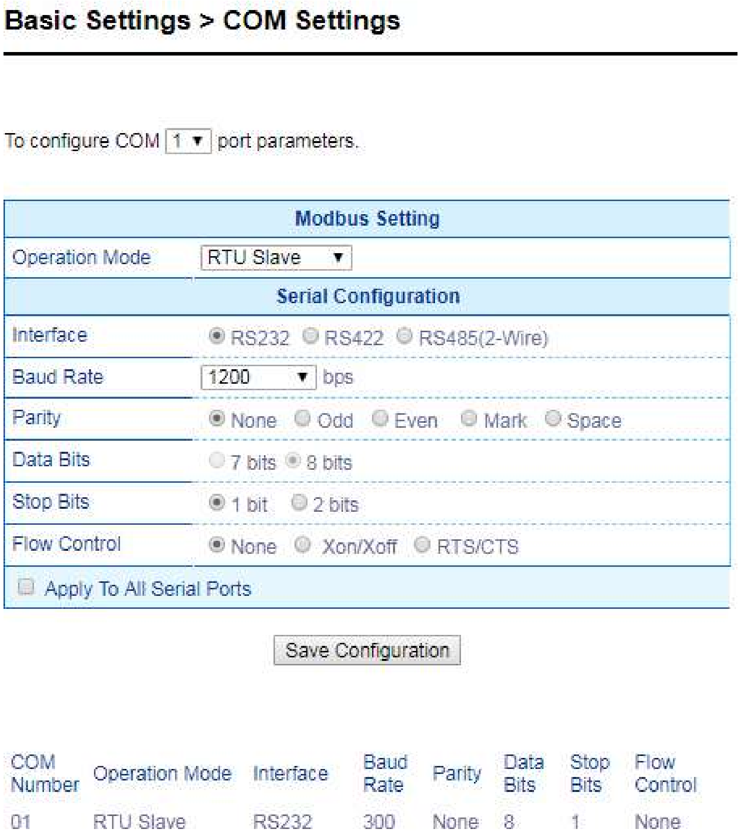
Bridge ID = priority (4 bits) + locally assigned system ID extension (12 bits) + ID [MAC Address] 48 bits
The default bridge priority is 32768.
Port ID = priority (4 bits) + ID (Interface number) (12 bits)
The default port priority is 128.

4.8 *Basic Settings*

In this section, the term **"Modbus Gateway device"** will be used to refer to the **XMT59XX series** and the term **"serial device"** to refer to any Modbus device that connect to Modbus Gateway via COM, VCOM, or TCP connections. In any Modbus network, there are two types of Modbus devices: Modbus Master and Modbus Slave. The Modbus Master will send a request message to a Modbus Slave. Then, the Modbus Slave will respond to the Modbus Master's request. A Modbus device (serial device) that is connected to the XMT59XX series Modbus Gateway device will either assume a role of Modbus Master or Modbus Slave. The basic settings in this section will address how to configure the role of the serial device in your Modbus Gateway device and its serial communication parameters. The term **"Operation Mode"** will be used to refer to the combination of role (Master or Slave) and the message or data transfer types (RTU/ASCII/TCP) of the Modbus protocol used by the serial device.

4.8.1 *COM Settings*

This section shows how to set up the physical ports of the Modbus Gateway device (COM ports or serial ports that serial devices are connected to). The available number of COM ports may vary according to the chosen Modbus Gateway model. Figure 4.16 shows the COM Settings web page in which COM1 port is shown with its **Operation Mode** under **Modbus Setting** and **Serial Configuration** settings. These settings will configure the role of the serial device through the **Operation Mode** and the serial communication parameters of that serial device through the **Serial Configuration** settings.



Basic Settings > COM Settings

To configure COM 1 ▾ port parameters.

Modbus Setting	
Operation Mode	RTU Slave ▾
Serial Configuration	
Interface	● RS232 ○ RS422 ○ RS485(2-Wire)
Baud Rate	1200 ▾ bps
Parity	● None ○ Odd ○ Even ○ Mark ○ Space
Data Bits	○ 7 bits ● 8 bits
Stop Bits	● 1 bit ○ 2 bits
Flow Control	● None ○ Xon/Xoff ○ RTS/CTS
☐ Apply To All Serial Ports	

COM Number	Operation Mode	Interface	Baud Rate	Parity	Data Bits	Stop Bits	Flow Control
01	RTU Slave	RS232	300	None	8	1	None

Figure 4.16 COM Settings Web Page

4.8.2 *Operation Mode*

To set the **Operation Mode** of the serial device that is connected to the Modbus Gateway through a COM port, use the pull-down menu to select among the following modes under **Modbus Setting**.

- **RTU Slave:** The serial device is working as a Modbus Slave node: the serial device will wait, accept request from, and response to its Modbus Master node. Data transfer is done in RTU format.
- **RTU Master:** The serial device is working as a Modbus Master node: the serial device will issue commands to or query Modbus slave nodes. Data transfer is done in RTU format.
- **ASCII Slave:** The serial device is working as a Modbus Slave node: the serial device will wait, accept request from, and response to its Modbus Master node. Data transfer is done in ASCII format.
- **ASCII Master:** The serial device is working as a Modbus Master node: the serial device will issue commands to or query Modbus Slave nodes. Data transfer is done in ASCII format.

4.8.3 *Serial Settings*

This section summarizes the options of serial communication parameters used between the serial device and the Modbus Gateway device over the selected COM port.

- RS-232/RS-422/RS-485 (2-wire) Software Selectable
- Baud-rate: 110 bps ~ 921600 bps Software Selectable
- Parity: None, Odd, Even, Mark, or Space
- Data Bits: 5, 6,7 or 8
- Stop Bits: 1 or 2 Software Selectable
- Flow Control: None, Software Xon/Xoff, Hardware RTS/CTS
- Receiver Resistor: On or Off
- Pull Resistor: 1K Ω or 100K Ω

Apply to all Serial Ports (check box**):** The settings can be chosen to apply to all serial ports if needed by checking the last checkbox on the options.

After finish the **COM Settings** configuration, click the **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up as shown in Figure 4.17 and after a short period of time the web browser will be redirected back to **COM Settings** page (Figure 4.16).

Figure 4.17 Save Successfully Message

Save Successfully

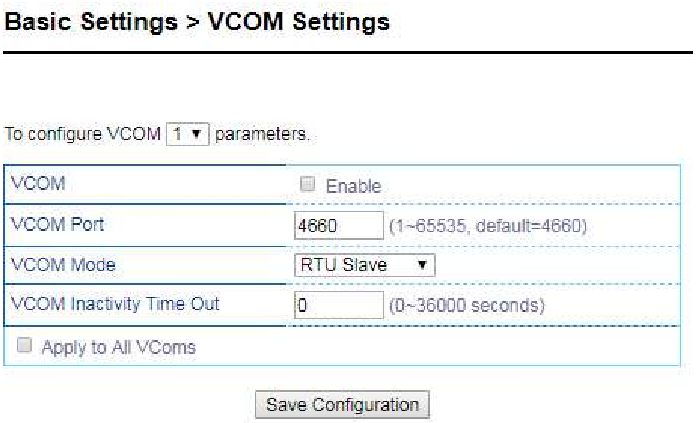
4.8.4 *VCOM Settings*

These settings will generate a virtual Serial (VCOM) port within the Modbus Gateway device based on a TCP network connection. VCOM is a **TCP connection** which is encoded in an Agatel' exclusive private protocol. XMT59XX series Modbus Gateway can only run as a TCP server which will be waiting for a connection request from a TCP client (a serial device).

Figure 4.18 shows the page of VCOM Settings in which the VCOM number 1 is set as an RTU Slave. This means that a device that is connected to this VCOM port on the Modbus Gateway will be a Modbus Slave node and communicate with a Modbus Master node using Modbus/RTU protocol. It is an interface concept that allows Modbus Slave devices to be connected via TCP connection by using VCOM from a PC (for example). If a VCOM setting is needed, proceed to select **Basic Settings** → **VCOM Settings** and check the VCOM's **"Enable"** box to allow configuration on the selected TCP's port of the Modbus Gateway device.

- **VCOM Port:** Using a TCP connection, the Modbus Gateway device (TCP server) listens to any TCP Clients (VCOM Clients) connecting (using Serial-IP) to its ports. The VCOM Port or the port of the TCP connection can be configured as a number between 1 and 65535. The default VCOM Port number is 4660.

Note: For Windows operating system, a Serial/IP software is required to use this feature. A restrictive **Serial/IP Redirector** software is installed along with Agatel's **Device Management Utility®**. The user can access the Serial/IP software through **Virtual COM → Serial/IP Tools** menu.



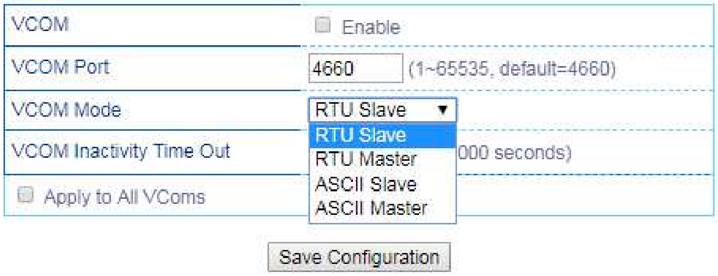
Basic Settings > VCOM Settings

To configure VCOM 1 ▼ parameters.

VCOM	□ Enable
VCOM Port	4660 (1~65535, default=4660)
VCOM Mode	RTU Slave ▼
VCOM Inactivity Time Out	0 (0~36000 seconds)
□ Apply to All VComs	

Figure 4.18 VCOM Settings Web Page

- **VCOM Mode:** This setting is a pull-down menu in which the user can select the **Operation Mode** of the devices connected through this VCOM port as shown in Figure 4.19. Its definition is the same to the one given in Section 4.8.2. Here the user can choose whether device conforms to a RTU or an ASCII message format and can select whether the device is either Modbus Slave node or Modbus Master Node. Figure 4.18 depicts the **RTU Slave** mode. So, the devices connected through VCOM 1 port will assume Modbus Slave role and communicate using Modbus/RTU protocol. If a Master mode (either RTU or ASCII) is selected, the options for the Master mode will be the same as the Slave mode. The only difference is the device's function.

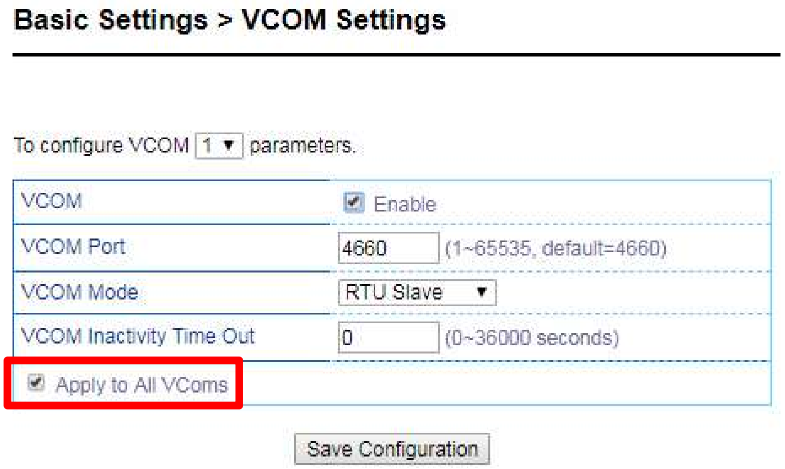


VCOM	□ Enable
VCOM Port	4660 (1~65535, default=4660)
VCOM Mode	RTU Slave ▼
VCOM Inactivity Time Out	000 seconds)
□ Apply to All VComs	

Figure 4.19 Pull-down Menu of VCOM Mode

- **VCOM inactivity Time Out:** This is a period of time allowed between actions. This setting can be set with a maximum of 600 minutes (36000 seconds) or 10 hours. If there is no activity within this period, the VCOM connection (TCP connection) will be automatically closed by the Modbus Gateway.

These settings can be applied to All VCOMs if needed by checking the last checkbox on the options. Figure 4.20 highlights the checkbox for applying the settings to all VCOMs.



Basic Settings > VCOM Settings

To configure VCOM 1 ▼ parameters.

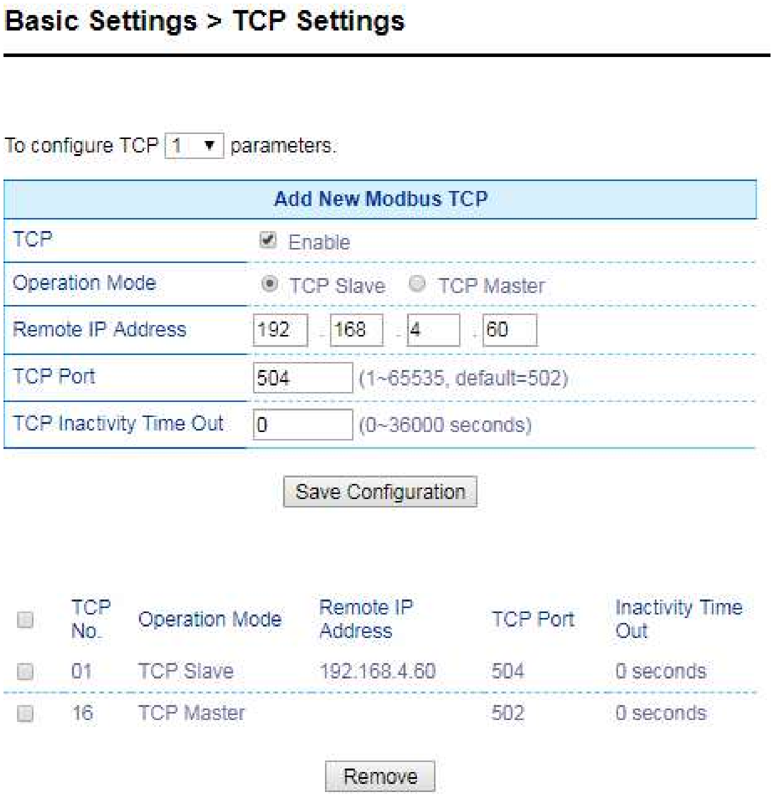
VCOM	☑ Enable
VCOM Port	4660 (1~65535, default=4660)
VCOM Mode	RTU Slave ▼
VCOM Inactivity Time Out	0 (0~36000 seconds)
☑ Apply to All VComs	

Figure 4.20 Check Box for Applying the Settings to All VCOMSs

After finishing configuring the **VCOM Settings**, click on **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, then the web browser will be redirected back to the **VCOM Settings** page**.**

4.8.5 *TCP Settings*

A device using Modbus/TCP connection, which communicates over the internet, can be set in this section. If a Modbus/TCP connection is needed, navigate to **Basic Settings → TCP Settings**, then choose whether or not to enable TCP by checking on the "**Enable**" check box. Figure 4.21 shows the Modbus TCP Settings page in which a device connected to this Modbus Gateway device is chosen to be run in **TCP Slave Operation Mode**. The device will take the Modbus Slave role and communicate using Modbus/TCP protocol.



Basic Settings > TCP Settings

To configure TCP 1 ▼ parameters.

Add New Modbus TCP	
TCP	☑ Enable
Operation Mode	● TCP Slave ○ TCP Master
Remote IP Address	192 . 168 . 4 . 60
TCP Port	504 (1~65535, default=502)
TCP Inactivity Time Out	0 (0~36000 seconds)

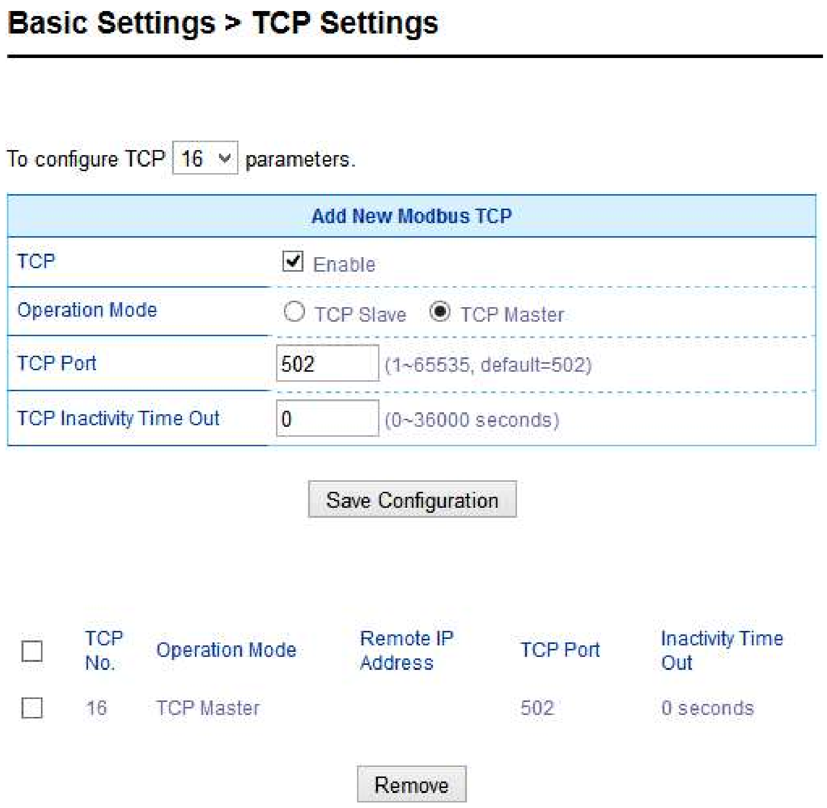
□	TCP No.	Operation Mode	Remote IP Address	TCP Port	Inactivity Time Out
□	01	TCP Slave	192.168.4.60	504	0 seconds
□	16	TCP Master		502	0 seconds

Figure 4.21 Modbus TCP Settings Web Page with TCP Slave Mode

- **Operation Mode:** There are two radio buttons in this setting: TCP Slave and TCP Master. When running on TCP Slave mode (the TCP Slave radio button is checked) as shown in Figure 4.21, the device will wait to receive Modbus requests from a Modbus Master. The data transmission is done under a Modbus/TCP protocol format. This means that the device will operate as a TCP Server that opens its TCP port to accept connections. The TCP Master option will be described at the end of this section.
- **Remote IP Address:** This setting shows the IP address of the device which is a Modbus slave node. This address refers to the IP address that belongs to the device that is going to be controlled from the XMT59XX Series Modbus Gateway device. This device can also be considered as a TCP server of whom it is needed to know its IP address. This option will disappear when the operation mode as TCP Master is selected, because in that mode the device will be running as a TCP Client which does not require to publish its IP address.
- **TCP Port:** This setting shows the TCP port number of the device (or Modbus Slave node in Figure 4.21) which can be a number in between 1 and 65535. The default port number is 502.
- **TCP inactivity Time Out:** A time out period, which is the maximum period of time allowed between actions, can be set as well. This setting has a maximum duration of 600 minutes (36000 seconds) or 10 hours. If no activity has occurred within this period, the Modbus/TCP connection will be automatically terminated by the Modbus Gateway.

At the end of the **TCP Settings** page shown in Figure 4.21, a list of all configured Modbus/TCP connections with TCP No., Operation Mode, Remote IP Address, TCP Port and TCP Inactivity Time Out information will appear. The user will have the ability to remove any Modbus/TCP connection settings by checking on box in front of the record of the desired TCP settings and clicking on the **Remove** button. To remove all TCP connections, simply check the box on the header row of the list to select all items and click remove.

Alternatively, the Modbus/TCP connection can be configured to run in **TCP Master Operation Mode**. This means that the device will be a Modbus Master node and communicate using Modbus/TCP protocol. Figure 4.22 shows the TCP Master Settings. When **TCP Master Operation Mode** is selected, the **Remote IP address** setting will disappear because the device will be running as a TCP Client. Next, the **TCP Port** is the port through which the signal is going to be relayed upon by the Modbus Gateway. Once again, there is a **TCP Inactivity Time Out** with the same maximum value of 10 hours as stated in the previous mode.



Basic Settings > TCP Settings

To configure TCP 16 parameters.

Add New Modbus TCP	
TCP	☑ Enable
Operation Mode	○ TCP Slave ● TCP Master
TCP Port	502 (1~65535, default=502)
TCP Inactivity Time Out	0 (0~36000 seconds)

□	TCP No.	Operation Mode	Remote IP Address	TCP Port	Inactivity Time Out
□	16	TCP Master		502	0 seconds

Figure 4.22 Modbus TCP Setting Page with TCP Master Operation Mode Selection

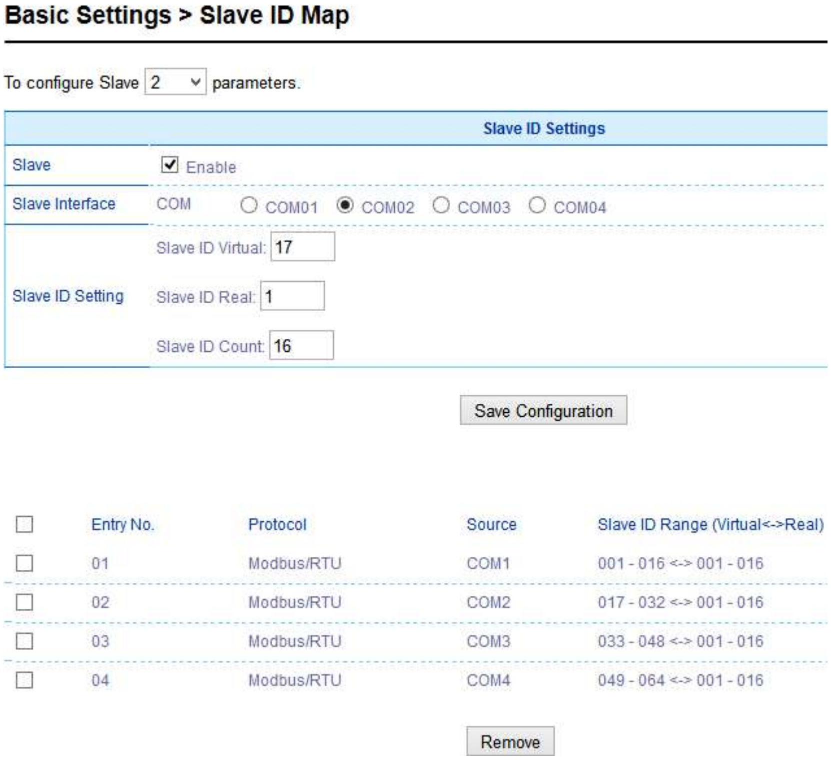
After **TCP Settings** configuration is finished, click on **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, and the web browser will be redirected back to the **TCP Settings** page**.**

4.8.6 *Slave ID Map*

The system uses the Modbus ID to route Modbus' request commands from a Modbus master node to the related Modbus Slave node. It is important to define ID mapping for each Modbus Slave node. For every Modbus Slave node, there should be a correct Virtual ID (Alias ID) and Real ID defined in the mapping. Figure 4.23 shows the Slave ID Map settings. To configure Slave 2's parameters, check the **Enable** box to enable Slave. Then, select the corresponding Slave interface.

- **Slave Interface:** When a port is set to Modbus slave mode, a slave interface will be created. Select a radio button of a port number behind the **Slave Interface,** which can be any one of the listed **COM/VCOM/TCP ports**.
- **Slave ID Setting Mode**: Next, select the mapping between real slave ID and Virtual ID to modify the slave ID setting as needed.

    - **Slave ID Virtual** maps a virtual ID to a real ID by the **Slave ID Count**. Figure 4.23 depicts Slave ID settings of COM02 to have real slave ID from 1 to 16 mapped from virtual ID 17 to 32.
        - **Slave ID Virtual** refers to a Virtual ID for the reading Master node.
        - **Slave ID Real** is the starting real ID within this interface (COM02 in Figure 4.23).
        - **Slave ID Count** is the number of slave devices in this interface that are mapped**.**



Basic Settings > Slave ID Map

To configure Slave 2 parameters.

	Slave ID Settings
Slave	☑ Enable
Slave Interface	COM ○ COM01 ● COM02 ○ COM03 ○ COM04
Slave ID Setting	Slave ID Virtual: 17 Slave ID Real: 1 Slave ID Count: 16

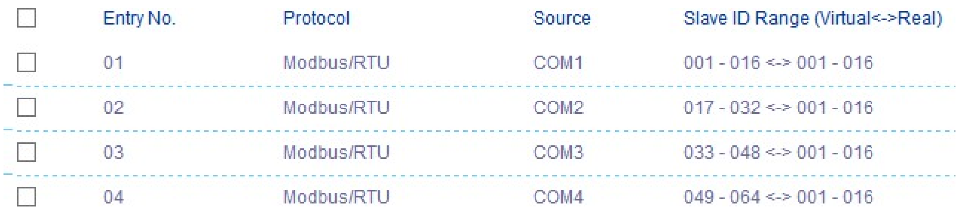
□	Entry No.	Protocol	Source	Slave ID Range (Virtual<->Real)
□	01	Modbus/RTU	COM1	001 - 016 <-> 001 - 016
□	02	Modbus/RTU	COM2	017 - 032 <-> 001 - 016
□	03	Modbus/RTU	COM3	033 - 048 <-> 001 - 016
□	04	Modbus/RTU	COM4	049 - 064 <-> 001 - 016

Figure 4.23 Slave ID Map Page with Slave ID Setting in Alias Mode

Note: Master and Slave IDs can be set on COM, VCOM, and TCP. However, COM works only with serial ports while TCP and VCOM operate via Ethernet ports.

After finishing configuring the **Slave ID Settings**, click the **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, then the web browser will be redirected back to the **Slave ID Settings** page**.**

Below the **Slave ID Settings** box, there is a list of mapping entries as shown in Figure 4.24 in which each line will summarize an **Entry No.**, a Modbus **Protocol**, a **Source**, a Slave ID Setting **Mode**, and the **Slave ID Range (Virtual <-**
> Real). Check the box in front of each entry to select that entry. Then, click **Remove** button to remove that particular entry from the **Slave ID Map**. To remove all entries, check on the box in front of the header line and click **Remove** button.



□	Entry No.	Protocol	Source	Slave ID Range (Virtual<->Real)
□	01	Modbus/RTU	COM1	001 - 016 <-> 001 - 016
□	02	Modbus/RTU	COM2	017 - 032 <-> 001 - 016
□	03	Modbus/RTU	COM3	033 - 048 <-> 001 - 016
□	04	Modbus/RTU	COM4	049 - 064 <-> 001 - 016

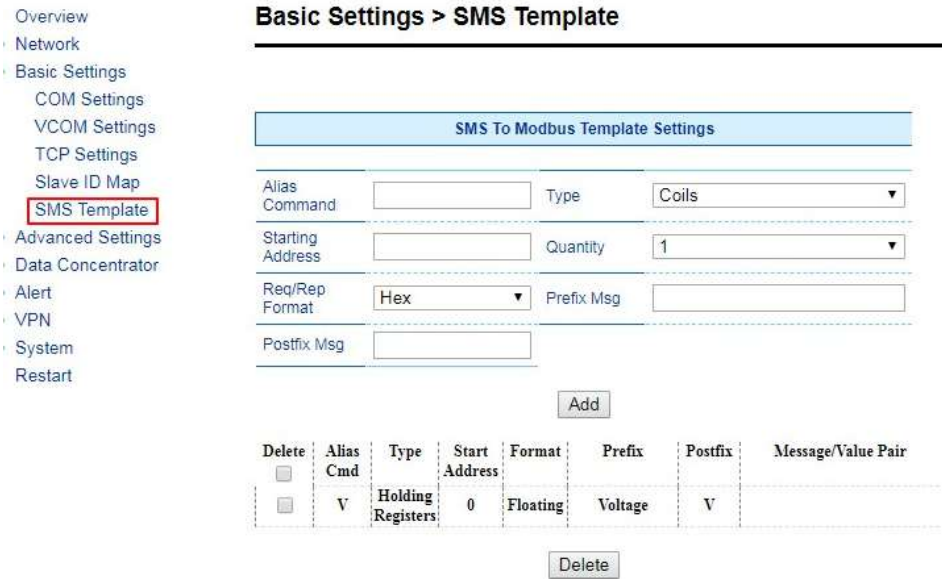
Figure 4.24 Slave ID Map Web Page with Slave ID Setting in in Offset Mode

4.8.7 *SMS Template*

XMT5901B allows the device to get data from a Modbus slave connected to the device. Setting up SMS function is easy and straightforward. Since this function requires cellular connectivity, it is available on XMT5901B only. Settings require the following steps to be carried out:

1) Define the alias command that the device will recognize as a specific command coming from SMS (NB- all other SMS commands will be ignored)
2) Associate to such command the Modbus Starting address, the quantity and the formatting method of the data that will be returned to the same number. Figure 4.25 below shows a configuration example.

Figure 4.25 SMS Template – configuration interface – Hex, Decimal or Floating reporting format



Basic Settings > SMS Template

SMS To Modbus Template Settings

Alias Command		Type	Coils ▼
Starting Address		Quantity	1 ▼
Req/Rep Format	Hex ▼	Prefix Msg	
Postfix Msg			

Delete □	Alias Cmd	Type	Start Address	Format	Prefix	Postfix	Message/Value Pair
□	V	Holding Registers	0	Floating	Voltage	V	

In the example shown in above Figure 4.25 and already configured, the alias command "V" is associated to the reading of 2 Holding Registers starting from Address 0 and returned in a floating format, with Prefix "Voltage" and Postfix "V". If the voltage measured is 6.45VDC, and 6 is stored in address 0 and 45 is stored in Address 1, the behavior of the device will be the following:

- Receive the SMS containing “V” from any cell phone number
- Retrieve the data and format it in the proper format
- Reply to the SMS with the following text: “Voltage 6.45 V”

Table 4.7 below explains the meaning of the configuration fields, if “Hex, Dec, Floating” is selected.

Note: if “string” is selected as an output format, then it’s necessary to associate a register value to a string. This is possible. For a more detailed explanation, please refer to Table 4.8 and Figure 4.26.

Table 4.7 SMS Template - Settings

Item	Description	Value setting
Alias command	The alias command makes it possible to execute Modbus command by entering a pre-set string (i.e., sequence of characters).	*Blank* Max. 6 characters (case sensitive)
Type	Modbus function code.	**01-** Read Coil
Starting Address	The starting of memory address.	*Blank* (Numeric 0-65535)
Quantity	The quantity of this command.	*1* (Numeric 1~2)
Req/Rep Format	The data type of request and response.	*Hex* (Hex, Dec, String, Floating) (Hex will be raw data) (Dec will be a signed integer) (Floating will be XX.YY format)
Prefix Msg	The prefix string of response message.	*Blank* - Max. 16 characters
Postfix Msg	The postfix string of response message.	*Blank* - Max. 6 characters

If “String” is selected as an output format, then it’s necessary to associate a register value to an output string. The fields shown in Figure 4.26 and explained in Table 4.8 will Pop-up.

Table 4.8 SMS Template settings - Message/Value Pair

Item	Description	Default setting
Message 1/ Message2	The SMS message represented by the corresponding value 1 and value 2	*Blank* Max. 6 characters (case sensitive)
Value 1/ Value2	The corresponding value of the SMS message 1 and message 2.	*Blank*

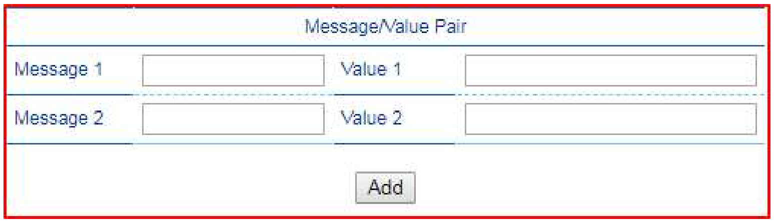


Figure 4.26 SMS Template – configuration interface – String reporting format

When the configuration of one command is done, click on the **Add** button to add the related SMS command in the list.

4.8.8 *SMS Settings*

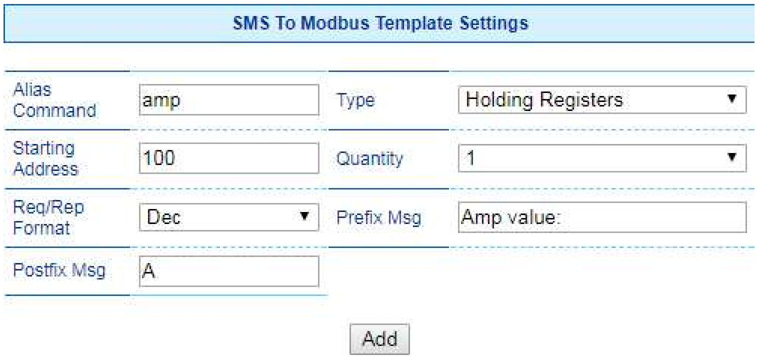
The SMS message format is defined as follows:

Alias command, *Modbus virtual ID*, *value (for write command)*

Example 1:

You’d like to see the current value of the IED with Modbus ID “10” by sending “amp, 10” by SMS to XMT5901B. You’d like to receive value from SMS in the format “Amp value: XXX (*signed integer*) A”

The settings should be completed as below:



SMS To Modbus Template Settings

Alias Command	amp	Type	Holding Registers ▾
Starting Address	100	Quantity	1 ▾
Req/Rep Format	Dec ▾	Prefix Msg	Amp value:
Postfix Msg	A		

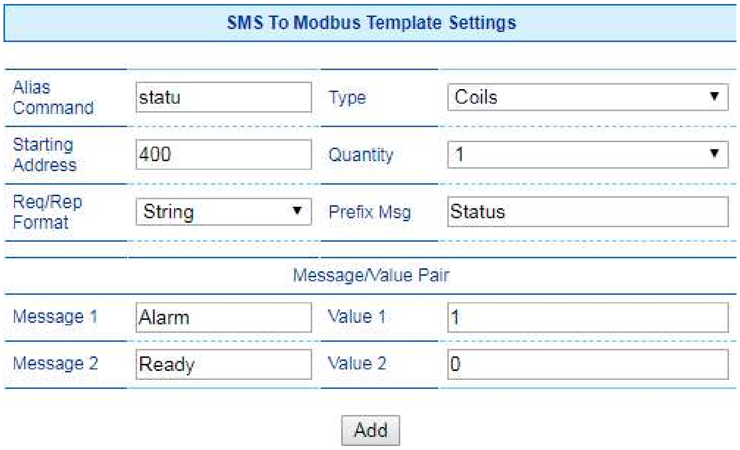
Figure 4.27 SMS Settings – Example 1

Please note that starting address “100” is an example. The address depends on the actual IED data mapping that is being used and may be slave-specific

Example 2:

You’d like to see the current value of the IED Customer request value of voltage of IED with Modbus ID “30” by sending “status, 30” and would like to receive value from SMS in a format of “Status: Alarm” or “Status: Ready”.

The settings should be completed as below:



SMS To Modbus Template Settings

Alias Command	statu	Type	Coils ▾
Starting Address	400	Quantity	1 ▾
Req/Rep Format	String ▾	Prefix Msg	Status

Message/Value Pair

Message 1	Alarm	Value 1	1
Message 2	Ready	Value 2	0

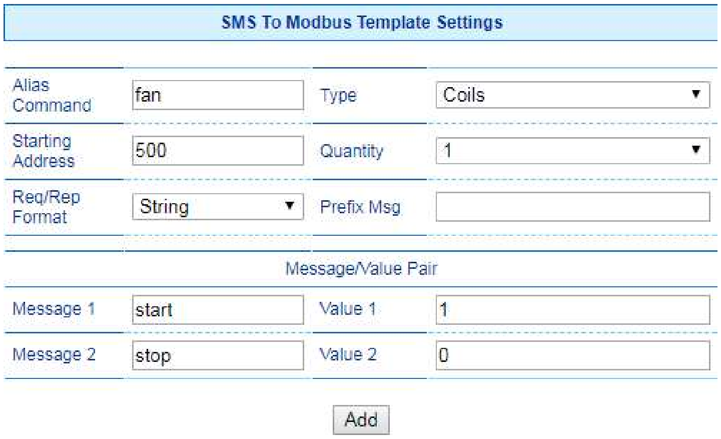
Figure 4.28 SMS Settings – Example 2

Please note that starting address “400” is an example. The address depends on the actual IED data mapping that is being used and may be slave-specific

Example 3:

You’d like to send value to the IED with Modbus ID “40” to start/stop a fan by sending “fan, start” or “fan, stop” and would like to receive value from SMS in a format of “Success” or “Error message”

The settings should be completed as below:



SMS To Modbus Template Settings

Alias Command	fan	Type	Coils ▼
Starting Address	500	Quantity	1 ▼
Req/Rep Format	String ▼	Prefix Msg	

Message/Value Pair

Message 1	start	Value 1	1
Message 2	stop	Value 2	0

Figure 4.29 SMS Settings – Example 3

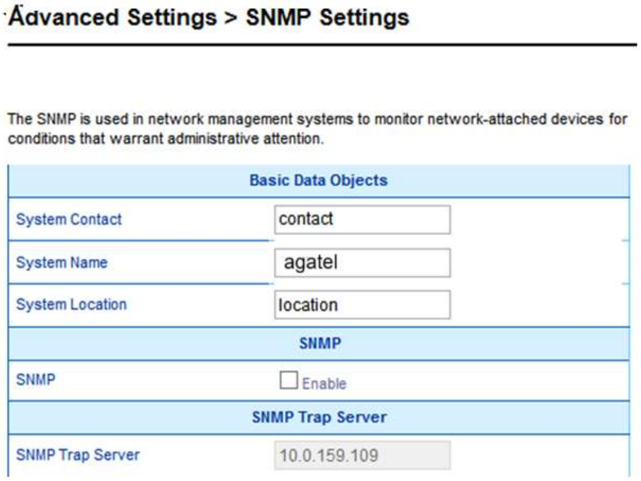
Please note that starting address “500” is an example. The address depends on the actual IED data mapping that is being used and may be slave-specific

4.9 *Advanced Settings*

4.9.1 *SNMP Settings*

SNMP (Simple Network Management Protocol) Settings determine whether the device settings can be viewed with a standard SNMP software. By default, it is disabled.
Figure 4.31 shows the **SNMP Settings** page with SNMP disabled. The first group of options on this web page is called **Basic Data Objects**:

- **System Contact** is the device administrator's contact information. The default value is "contact".
- **System Name,** which is by default, is the MAC address of the Modbus Gateway. The default value is "Agatel".
- **System Location** is the device's physical location. The default value is "location".



Advanced Settings > SNMP Settings

The SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

Basic Data Objects	
System Contact	contact
System Name	agatel
System Location	location
SNMP	
SNMP	□ Enable
SNMP Trap Server	
SNMP Trap Server	10.0.159.109

Figure 4.30 SNMP Settings Web Page with SNMP disabled

The second group of options is called **SNMP:**

- **SNMP** is followed by a "**Enable**" check box in which to enable the SNMP feature on the Modbus Gateway. If this box is not checked, it means that SNMP is disabled. Then, the rest of the options will be disappeared as shown in Figure 4.30. If the SNMP option is enabled, there can be three different views for SNMP options as shown in
- Figure 4.31, Figure 4.32, and Figure 4.33.
- **SNMP Version** is a drop-down box which allows the user to choose version of supported SNMP protocol. This can be **v1/v2c** or **v1/v2c/v3** or **Only v3**. Note that if this option is set as v1/v2c/v3, the SNMP options will be shown as in
- Figure 4.31.

    - SNMP v1 and v2c support simple community string based authentication protocol for their security mechanism. If this option is selected as v1/v2c, the SNMP options will be shown as in Figure 4.32.
    - SNMP v3 is improved with additional authentication and cryptography security. If this option is selected as Only v3, the SNMP options will be shown as in Figure 4.33.

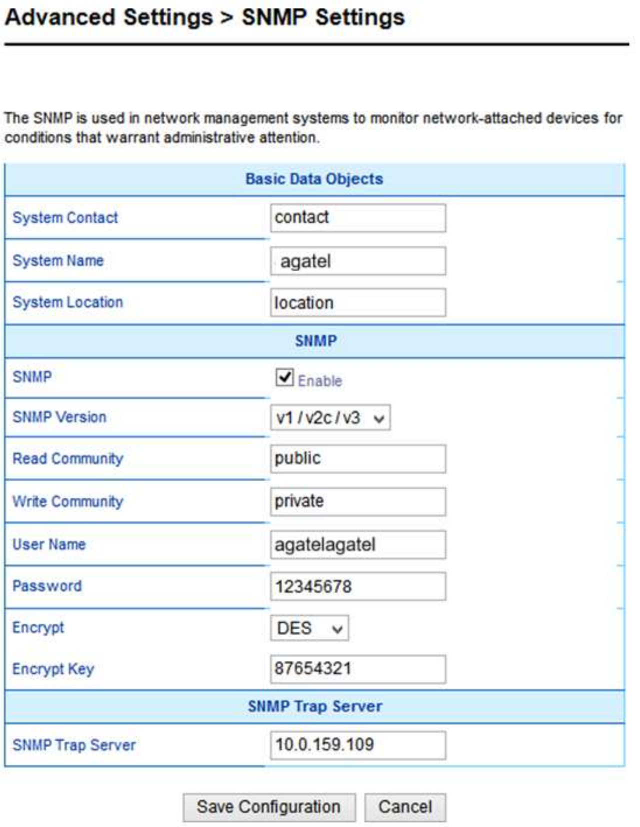
- **Read Community** is the field that you can specify the **SNMP Read Community String** which is a user ID or plaintext password string for simple authentication in SNMP v1 and v2c. In order to make the SNMP information available for public viewing, simply flag the **"Enable SNMP"** checkbox and fill in your desired password string (the default string is **"public"**) in the **Read Community** field.
- **Write Community** is the field that you can specify the **SNMP Write Community String** which is a user ID or

plaintext password string for simple authentication in SNMP v1 and v2c. In order to allow a group of people to change the SNMP information, enter your desired password string (the default string is **“private”**) in the **Write Community** field**.**

- **User Name** is the user name for SNMP account for SNMP v3.
- **Password** is the password for SNMP account for SNMP v3.
- **Encrypt** is a drop-down box which allows the user to choose the encryption scheme for SNMP v3. The available options are None, DES, or AES. The default is “None”.
- **Encrypt Key** is where you can specify the encryption key for the SNMP v3 access.

The last group of option is **SNMP Trap Server**. In order to allow a trap server to collect device information, fill in **SNMP Trap Server** with its corresponding IP address (a trap server is designed to collect all alarm information from the Modbus Gateway). An example in
Figure 4.31 is 10.0.159.109.

After **SNMP Settings** configuration is finished, click the **Save Configuration** button to save all changes that have been made or click **Cancel** button to discard your changes.

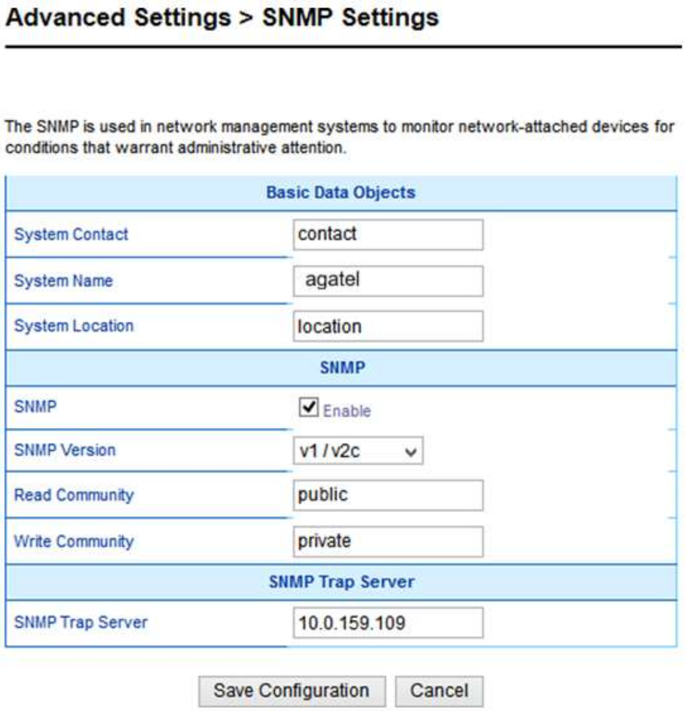


Advanced Settings > SNMP Settings

The SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

Basic Data Objects	
System Contact	contact
System Name	agatel
System Location	location
SNMP	
SNMP	☑ Enable
SNMP Version	v1 / v2c / v3
Read Community	public
Write Community	private
User Name	agatelagatel
Password	12345678
Encrypt	DES
Encrypt Key	87654321
SNMP Trap Server	
SNMP Trap Server	10.0.159.109

Figure 4.31 SNMP Settings Web Page with SNMP Enabled and Version v1/v2c/v3

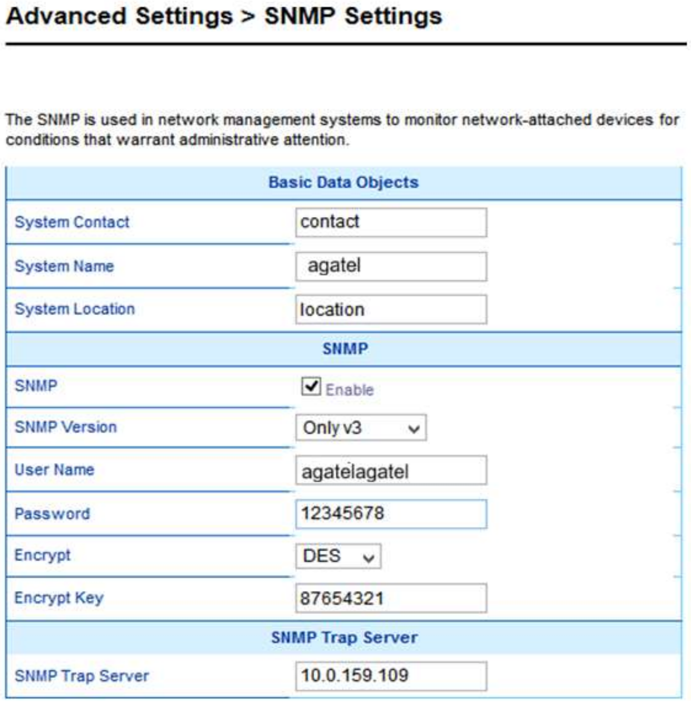


Advanced Settings > SNMP Settings

The SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

Basic Data Objects	
System Contact	contact
System Name	agatel
System Location	location
SNMP	
SNMP	☑ Enable
SNMP Version	v1 / v2c
Read Community	public
Write Community	private
SNMP Trap Server	
SNMP Trap Server	10.0.159.109

Figure 4.32 SNMP Settings Web Page with SNMP Enabled and Version v1/v2c



Advanced Settings > SNMP Settings

The SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

Basic Data Objects	
System Contact	contact
System Name	agatel
System Location	location
SNMP	
SNMP	☑ Enable
SNMP Version	Only v3
User Name	agatelagatel
Password	12345678
Encrypt	DES
Encrypt Key	87654321
SNMP Trap Server	
SNMP Trap Server	10.0.159.109

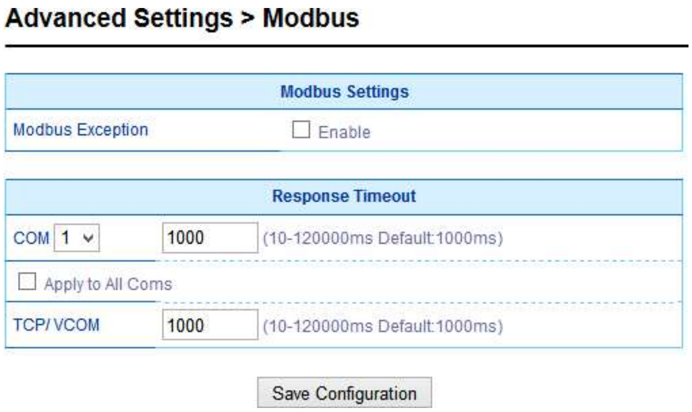
Figure 4.33 SNMP Settings Web Page with SNMP Enabled and Version Only v3

4.9.2 *Modbus*

In **Modbus** settings, it is possible select whether to enable **Modbus Exception** by flagging the **Enable** checkbox as shown in
Figure 4.34. If the Modbus slave returns no response and timeout occurs, it may then be necessary for the gateway to return an exception. To set **Response Timeout** for COM and TCP/VCOM, fill in the timeout periods in the fields as shown in
Figure 4.34. Note that the timeout setting can be applied to all COM ports by checking the **Apply to All Coms** box.

- Configure timeout for each COM port between 10ms to 120000ms with a default value of 1000ms.
- Configure timeout for TCP/VCOM port between 10ms to 120000ms with a default value of 1000ms.

After finishing the Advanced Modbus Settings configuration, click on the **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, and the web browser will be redirected back to the **Modbus** page**.**



Advanced Settings > Modbus

Modbus Settings	
Modbus Exception	□ Enable

Response Timeout		
COM 1	1000	(10-120000ms Default:1000ms)
□ Apply to All Coms		
TCP/ VCOM	1000	(10-120000ms Default:1000ms)

Save Configuration

Figure 4.34 Advanced Modbus Settings of Response Timeout for Modbus Exception

4.10 *Data Concentrator (XMT59XX-CT Only)*

Before starting this section, some basic concept of Modbus data Concentrator will be briefly introduced. Please note, this section only applies to XMT59XX-CT series products.

4.10.1 *Concentrator Concept*

The Concentrator acts as a gateway to collect data from Modbus Slaves devices independently from the Master enquiry. The data is saved to main memory (or database), and the requests from Modbus Master will be executed directly from the memory to increase the performance. The memory mapping can save the time necessary for the Gateway to relay the query to the device via serial line (that is usually slow). Thus, a better response time is obtained. The baud rate of the serial line is mostly used in range of 9600 to 115200 bps. With a 9600-bps setting, 1 byte can be transferred per millisecond (0.001 s). Querying 100 IEDs (Intelligent Electronic Device) with 10 registers each (one register is 2 bytes), will require 100*10*2/1000=2 seconds. The Ethernet network performance is normally 100Mbps and transferring the same information is much faster. So, if the device is queried only upon Master request, the Modbus Master will always be in waiting state. In Figure 4.35, it shows the concept of the Modbus Concentrator. There are 6 IEDs via a serial line connecting to the Concentrator which is abbreviated as GW (Gateway). The Gateway maps all 6 IEDs into a memory map in different address. The register of IED-1 is mapped in 0x1000 address of the GW while the registers of IED-3 is mapped in 0x3000. The Modbus Master can use the same Modbus commands but different slave ID (see in Figure 4.35, we set the GW as 248) and a different address to get the data for all IEDs. A Modbus command (″id=248, func=3, start=0x1000, quan=20″) reads the data of the registers in IED-1. And a Modbus command (″id=248, func=3, start=0x3000, quan=10″) reads the data of the registers in IED-3.

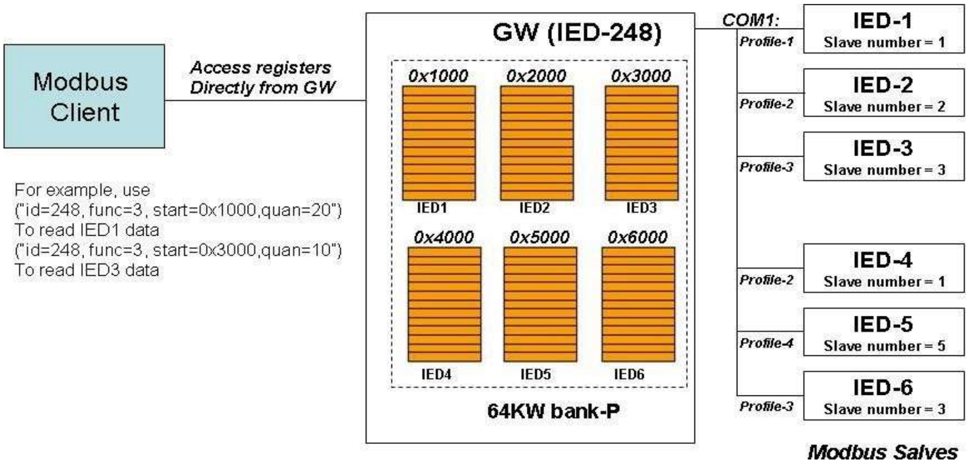


Figure 4.35 Concentrator Concept

● *Gateway Configuration in Slave Map*

A Modbus slave can have 64K words address mapping. The Gateway will have a lot of serial lines supported. The first thing to be done is to map all the IEDs into the address area of GW. A Slave Map will describe the way every IED is mapped to each address in the 64K address memory. The steps include:

- **Setup a mapping for each IEDs connected**: Some IEDs will have the same default slave number, for example slave number = 1. But in each serial line, there should not exist any IED sharing the same slave number. The term "device ID" is used internally and uniquely to identify all IEDs. Thus, each IED will have a unique "device ID", which can be set from 1 to 247. The GW is also defined a device ID, such as 248 in Figure 4.35. This virtual device ID can be used for a Modbus Master. If a Modbus Master needs to update a certain register in an IED, it can use this device ID to tell the GW where it needs to update.

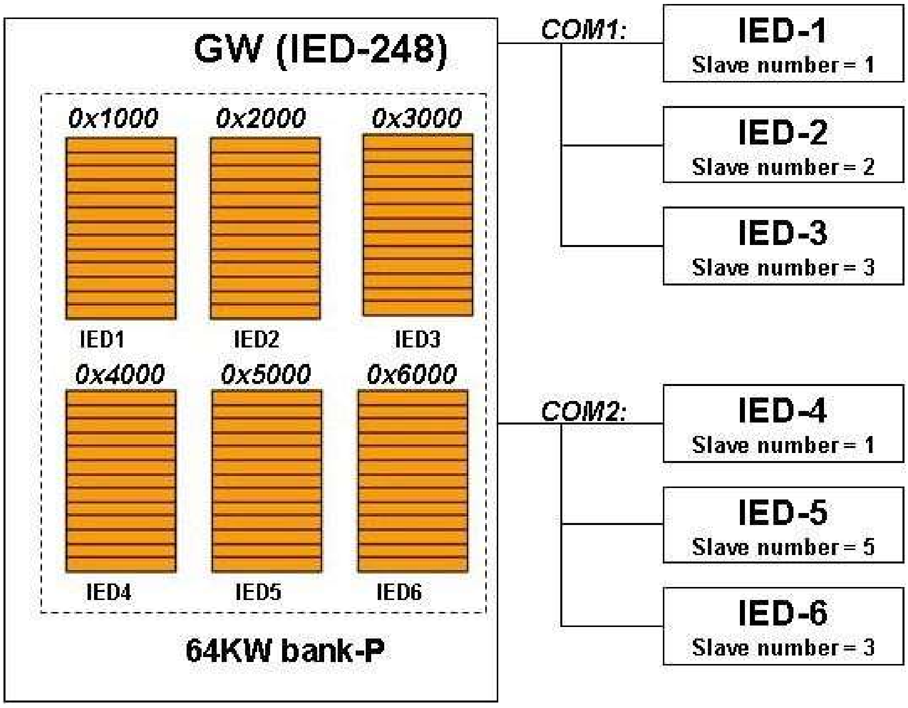


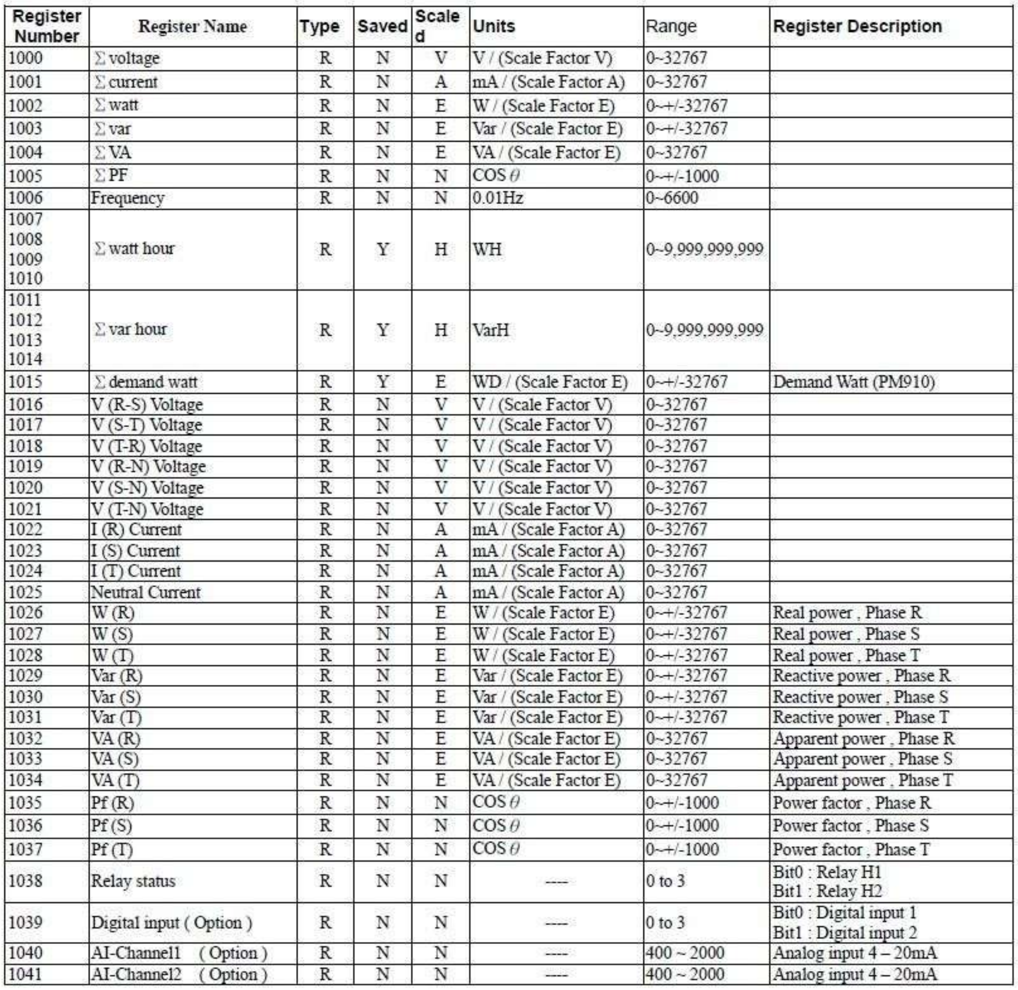
Figure 4.36 An example for Slave Mapping

For the example in Figure 4.36, there are 2 serial ports connected to the GW. In COM1 port, there are 3 IEDs with Slave number 1, 2, and 3. And in COM2 port, there are 3 IEDs with Slave number 1, 5, and 3. To identify Slave number 1 of COM2 and Slave 1 of COM1, the virtual Slave ID can be used as IED-1, IED-2, IED-3 for COM1 port, and IED-4, IED-5 and IED-6 for COM2 port. The number from 1 to 6 becomes a logical ID mapping to the physical Slave number. It is used for both GW and the Modbus Maters connected to GW.

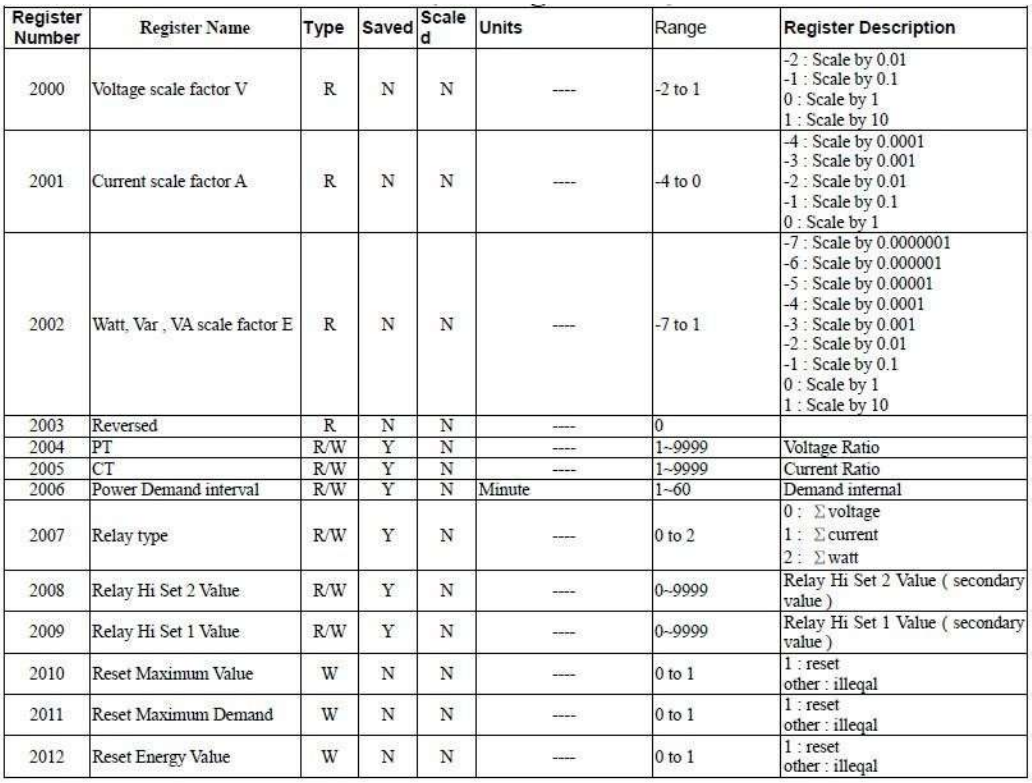
- **Setup an address area from IEDs to GW**: After a slave mapping activity is carried out, the next step is to configure the address mapping in the GW. A Modbus Master can then use this memory mapping to get all the registers of IEDs. As the same example in Figure 4.36, the registers of IED-1 are mapped into the address 0x1000 of GW, IED-2 is mapped to the address 0x2000, and IED-3 is mapped to the address 0x3000. A Modbus Master command (“id=248, func=3, start=0x1000, quan=20”) will query the registers in IED-1, and a
  Modbus command (“id=248, func=3, start=0x3000, quan=10”) will query the registers in IED3. These addresses 0x1000, 0x2000, 0x3000, 0x4000, 0x5000 and 0x6000 are called **"relative address to GW"** for IEDs.

- *Address Mapping inside an IED*

A Modbus Slave can have a range of registers to be accessed, which means users can use more than one Modbus command to retrieve data. These addresses are defined from the specification of IEDs. It is possible to use the same type of IEDs within the same GW. For example, a power meter can be used for measuring the current or the voltage in different locations. The following two tables are the example.



Register Number	Register Name	Type	Saved	Scaled	Units	Range	Register Description
1000	Σ voltage	R	N	V	V / (Scale Factor V)	0~32767	
1001	Σ current	R	N	A	mA / (Scale Factor A)	0~32767	
1002	Σ watt	R	N	E	W / (Scale Factor E)	0~+/-32767	
1003	Σ var	R	N	E	Var / (Scale Factor E)	0~+/-32767	
1004	Σ VA	R	N	E	VA / (Scale Factor E)	0~32767	
1005	Σ PF	R	N	N	COS θ	0~+/-1000	
1006	Frequency	R	N	N	0.01Hz	0~6600	
1007 1008 1009 1010	Σ watt hour	R	Y	H	WH	0~9,999,999,999	
1011 1012 1013 1014	Σ var hour	R	Y	H	VarH	0~9,999,999,999	
1015	Σ demand watt	R	Y	E	WD / (Scale Factor E)	0~+/-32767	Demand Watt (PM910)
1016	V (R-S) Voltage	R	N	V	V / (Scale Factor V)	0~32767	
1017	V (S-T) Voltage	R	N	V	V / (Scale Factor V)	0~32767	
1018	V (T-R) Voltage	R	N	V	V / (Scale Factor V)	0~32767	
1019	V (R-N) Voltage	R	N	V	V / (Scale Factor V)	0~32767	
1020	V (S-N) Voltage	R	N	V	V / (Scale Factor V)	0~32767	
1021	V (T-N) Voltage	R	N	V	V / (Scale Factor V)	0~32767	
1022	I (R) Current	R	N	A	mA / (Scale Factor A)	0~32767	
1023	I (S) Current	R	N	A	mA / (Scale Factor A)	0~32767	
1024	I (T) Current	R	N	A	mA / (Scale Factor A)	0~32767	
1025	Neutral Current	R	N	A	mA / (Scale Factor A)	0~32767	
1026	W (R)	R	N	E	W / (Scale Factor E)	0~+/-32767	Real power , Phase R
1027	W (S)	R	N	E	W / (Scale Factor E)	0~+/-32767	Real power , Phase S
1028	W (T)	R	N	E	W / (Scale Factor E)	0~+/-32767	Real power , Phase T
1029	Var (R)	R	N	E	Var / (Scale Factor E)	0~+/-32767	Reactive power , Phase R
1030	Var (S)	R	N	E	Var / (Scale Factor E)	0~+/-32767	Reactive power , Phase S
1031	Var (T)	R	N	E	Var / (Scale Factor E)	0~+/-32767	Reactive power , Phase T
1032	VA (R)	R	N	E	VA / (Scale Factor E)	0~32767	Apparent power , Phase R
1033	VA (S)	R	N	E	VA / (Scale Factor E)	0~32767	Apparent power , Phase S
1034	VA (T)	R	N	E	VA / (Scale Factor E)	0~32767	Apparent power , Phase T
1035	Pf (R)	R	N	N	COS θ	0~+/-1000	Power factor , Phase R
1036	Pf (S)	R	N	N	COS θ	0~+/-1000	Power factor , Phase S
1037	Pf (T)	R	N	N	COS θ	0~+/-1000	Power factor , Phase T
1038	Relay status	R	N	N	----	0 to 3	Bit0 : Relay H1 Bit1 : Relay H2
1039	Digital input (Option)	R	N	N	----	0 to 3	Bit0 : Digital input 1 Bit1 : Digital input 2
1040	AI-Channel1 (Option)	R	N	N	----	400 ~ 2000	Analog input 4 – 20mA
1041	AI-Channel2 (Option)	R	N	N	----	400 ~ 2000	Analog input 4 – 20mA



Register Number	Register Name	Type	Saved	Scaled	Units	Range	Register Description
2000	Voltage scale factor V	R	N	N	----	-2 to 1	-2 : Scale by 0.01 -1 : Scale by 0.1 0 : Scale by 1 1 : Scale by 10
2001	Current scale factor A	R	N	N	----	-4 to 0	-4 : Scale by 0.0001 -3 : Scale by 0.001 -2 : Scale by 0.01 -1 : Scale by 0.1 0 : Scale by 1
2002	Watt, Var , VA scale factor E	R	N	N	----	-7 to 1	-7 : Scale by 0.0000001 -6 : Scale by 0.000001 -5 : Scale by 0.00001 -4 : Scale by 0.0001 -3 : Scale by 0.001 -2 : Scale by 0.01 -1 : Scale by 0.1 0 : Scale by 1 1 : Scale by 10
2003	Reversed	R	N	N	----	0	
2004	PT	R/W	Y	N	----	1~9999	Voltage Ratio
2005	CT	R/W	Y	N	----	1~9999	Current Ratio
2006	Power Demand interval	R/W	Y	N	Minute	1~60	Demand internal
2007	Relay type	R/W	Y	N	----	0 to 2	0 : Σvoltage 1 : Σcurrent 2 : Σwatt
2008	Relay Hi Set 2 Value	R/W	Y	N	----	0~9999	Relay Hi Set 2 Value (secondary value)
2009	Relay Hi Set 1 Value	R/W	Y	N	----	0~9999	Relay Hi Set 1 Value (secondary value)
2010	Reset Maximum Value	W	N	N	----	0 to 1	1 : reset other : illeqal
2011	Reset Maximum Demand	W	N	N	----	0 to 1	1 : reset other : illeqal
2012	Reset Energy Value	W	N	N	----	0 to 1	1 : reset other : illeqal

Users need at least 2 Modbus commands to retrieve these register data. It can be a Modbus command (“id=1, func=3, start=1000, quan=42”) for the first, or a Modbus command (“id=1, func=3, start=2000, quan=13”) for the second. If other IEDs with the same type exist on the network, they will share the same method to retrieve the registers. In Agatel’s concentrator product, it is possible to define a profile (such as these 2 Modbus commands) so that other IEDs can be configured to get the data easily. The only variable becomes the Slave number. The steps are:

- **Setup a profile (uniquely identified with an ID number or name):** This profile will include one or more than one Modbus commands. This is defined for any physical IED to use. Only the commands, the starting address and the quantity are required at this stage.
- **Setup a relative address for each Modbus command:** Each Modbus command of the profile will require a relative address to IED. For example, the final mapping of IED-3 to GW is at the address 0x3000. If the IED-3 is the type of power meter in the above table, the address range is 1000~2012. Before this IED is mapped to 0x3000, these two Modbus commands: ("func=3, start=1000, quan=42”), and (“func=3, start=2000, quan=13”) will require a mapping to a relative address with respect to the starting address. For example, if it is necessary to keep Modbus 64K words more efficient, then the mapping 1000 ~1041 to the starting address is needed, meaning that "0", and 2000 ~ 2012 to "42". Then it looks like the following Figure 4.37.

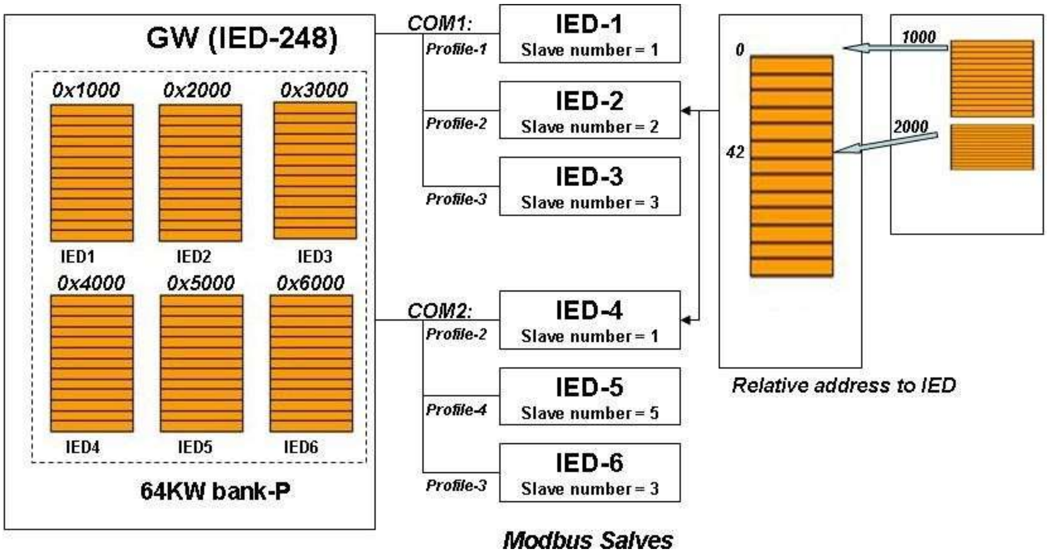


Figure 4.37 The concept of profile and relative address of IED The

right side of the Figure shows the Modbus commands and the mapping to the relative address of the Profile-2. IED-2 and IED-4 are the same power meter, and they use the same profile-2. So, the address 0x2000 of GW and 0x4000 of GW represent the same kind of value "∑voltage" in different IEDs. The address 0x2006 & 0x4006 represent "Frequency" register.

- Modbus Client Mapping

The Modbus Master can read or poll registers from the memory map in the device ID =248 (GW). Since a Modbus command can only read less than 147 registers at a time, considering that data is not arranged by the specific requirement of the Master all the time, it may be useful for the users to define a new memory mapping for a certain Modbus Client by specifying the IP address. Refer to Figure 4.38.

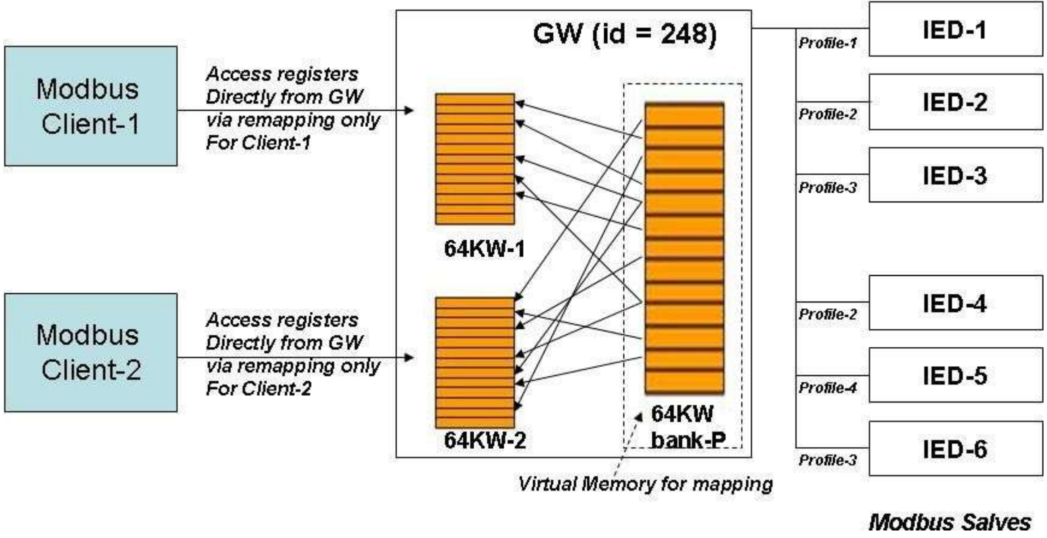


Figure 4.38 A New mapping from Modbus client to GW

Users can regard the Gateway as a device which ID is 248 in the same way of a new Modbus device with a 64KW address mapping. Modbus Client-1 and Modbus Client-2 can define their Modbus devices by changing the

mapping of the GW memory. The GW might be a "big" Modbus device which can transfer many registers from different slaves to a continuous storage so that these registers can be retrieved easily within few commands. It becomes more efficient to use as less Modbus commands as possible to retrieve what it need.
These new Modbus commands will build different virtual Modbus slave devices. Sometimes, it might also need to group a certain of information from Modbus slaves. In the example above, there is a Modbus meter which can measure voltage, current and power. Users can group all these values in continuous memory addresses to retrieve them easier. If, instead, the relay is set with a certain threshold of voltage, it would be better to keep voltage and relay together for querying. Voltage values can be copied in more than one location as Figure 4.39 shown.

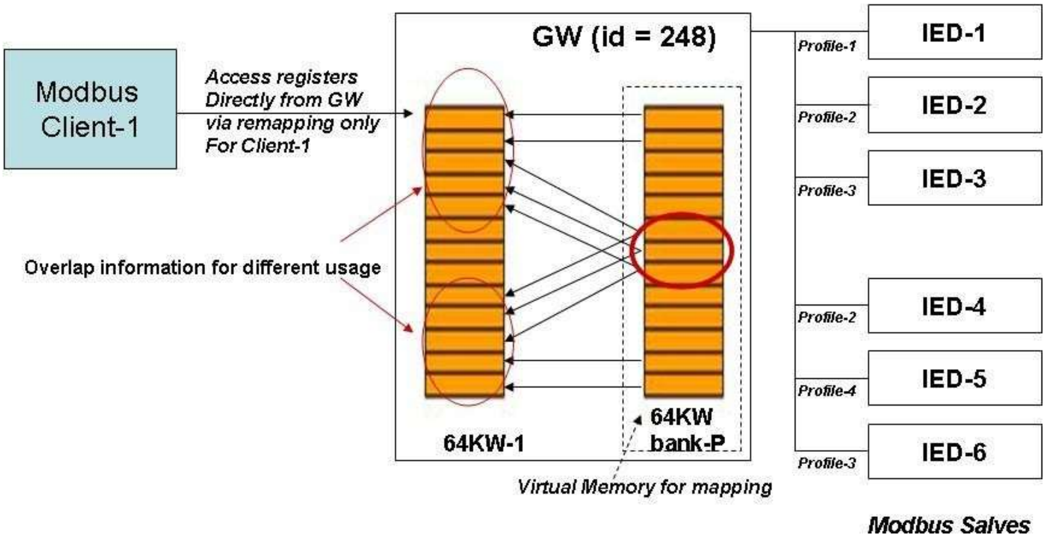
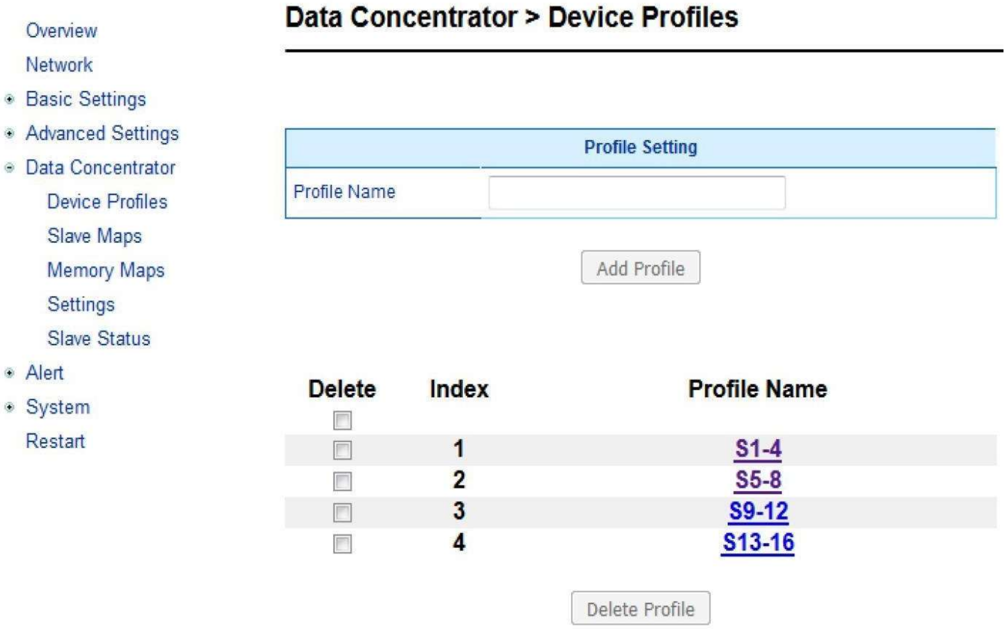


Figure 4.39 Mapping to Multiple locations for Modbus client to GW

4.10.2 *Device Profile*

As explained in section 4.10.1, "Profile" is a description of the IED device type. The same device type will use the same Modbus commands to retrieve data. This section explains how to create profiles for certain types of Modbus Slaves. For example, it shows how to create number 4 profiles. There is maximum 32 profiles allowed to be established. In Figure 4.40, 4 profiles are created. A column “Profile Name” is used to remember it easier (in the example, "S1-4" is a device name). For each profile, there are a maximum of 32 Modbus commands allowed to be set. In Figure 4.41, the Modbus command is set to a read coil function with the start address 0x0, and quantity 2000. To make sure the required performance is achieved, the user can setup how often this data should be polled in the "interval" item. During the creation process of Modbus commands for a profile, users can enable/disable this command by using the "Enable" button.
In figure 4.40 below, there are 4 demo Profiles which are S1-4, S5-8, S9-12, and S13-16 at the page of "Data Concentrator > Device Profiles". For the demo setting of the polling function, the S1-4 is selected as the example to show you the configuration.

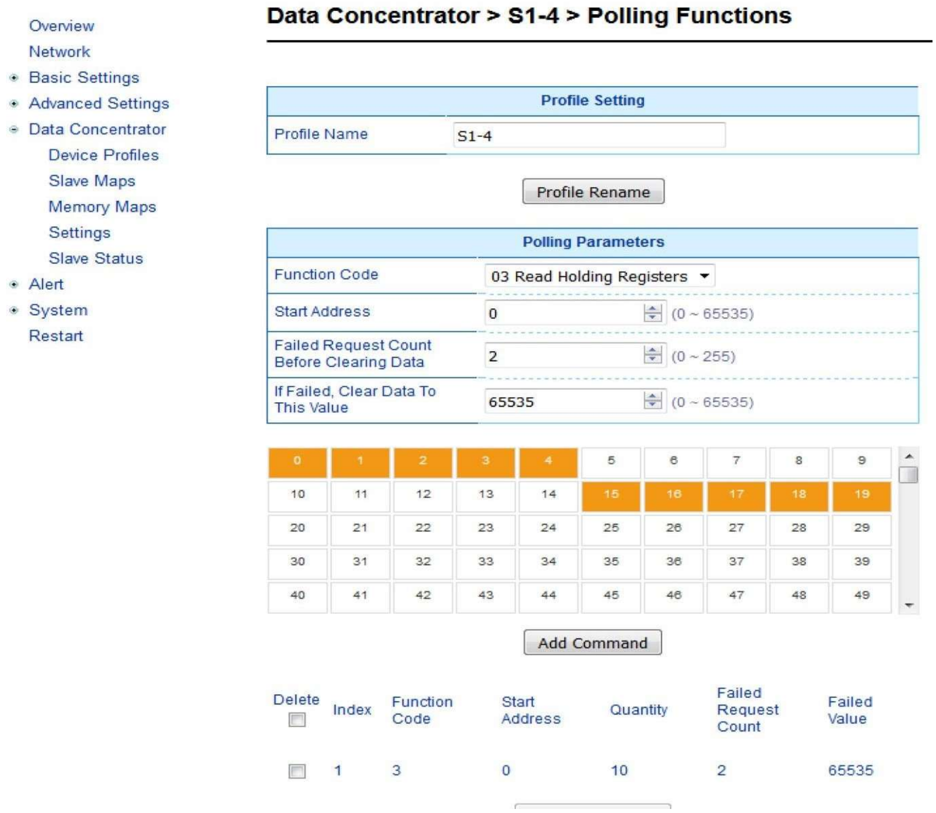


Profile Name	

Delete	Index	Profile Name
□		
□	1	S1-4
□	2	S5-8
□	3	S9-12
□	4	S13-16

Figure 4.40 Setup profile in "Device Profile" Function

Figure 4.41 shows how users can modify this Profile by clicking “**Profile name**”. You can input the starting address of the slave device. The selection can be made using the left mouse button on the table that shows up. Click the register you would like to poll together with “**CTRL**” or “**SHIFT**” buttons to select single or multiple registers. They will be highlighted in orange colour. Once finished, click “**Add**” button to add this new command. In the example shown in Figure 4.41 below, the Modbus command entered is “read holding register” (Function ID: 3) for starting address 0x0, quantity 10.
The field “Failed Request Count Before Clearing Date” defines the number of unsuccessful attempts to be made before clearing the data in the memory. A maximum of 255 attempts is allowed. The field “If Failed, Clearing Data To This Value”, defines the value that the memory should be set to after the number of failed attempts above defined. The value can range from 0 to 65535. For each Device Profile, there are a maximum of 32 Modbus commands allowed. User can enable checkbox and click “Delete Command” Button to delete the selected command.



Data Concentrator > S1-4 > Polling Functions

Profile Setting	
Profile Name	S1-4

Polling Parameters		
Function Code	03 Read Holding Registers	
Start Address	0	(0 ~ 65535)
Failed Request Count Before Clearing Data	2	(0 ~ 255)
If Failed, Clear Data To This Value	65535	(0 ~ 65535)

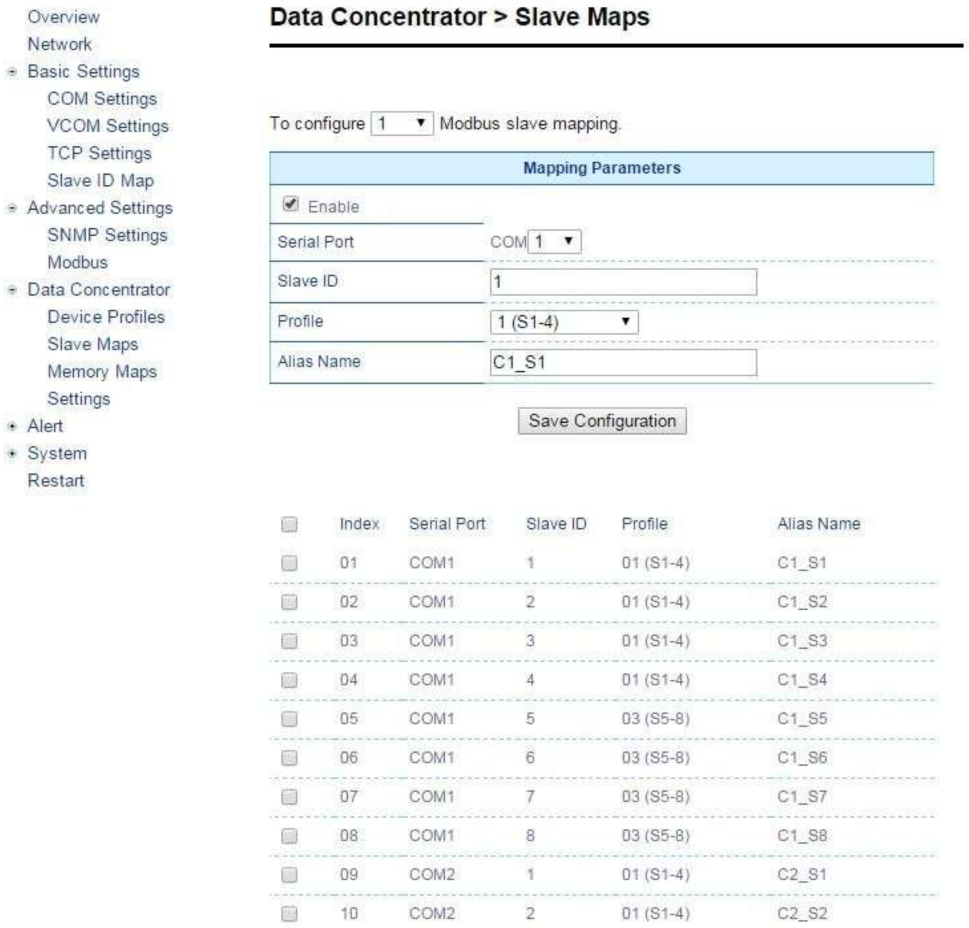
0	**1**	**2**	**3**	**4**	5	6	7	8	9
10	11	12	13	14	**15**	**16**	**17**	**18**	**19**
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49

Delete ☐	Index	Function Code	Start Address	Quantity	Failed Request Count	Failed Value
☐	1	3	0	10	2	65535

Figure 4.41 Setup Modbus commands for type name "S1-4"

4.10.3 *Slave Maps*

This section is used to map real Modbus slave devices with the predefined profile so that it will be easy to enable the concentrator function. As explained in the overview section, there won't be too many types of devices. Thus, it is faster for the user to establish profiles first, then map the Modbus slaves created in section 3.7 to them. In Figure 4.42, Modbus slave devices with ID 1~4 from port COM1, ID 1~2 of COM2, are assigned to profile "S1-4". Once enabled, the Modbus gateway will follow the settings of profile S1-4 to issue polling commands and store the response into the device's memory. The query from the Master for the data related to these slaves will be released very quickly to ensure the performance. To remove the setting, follow the steps shown on Figure 4.43. The alias name on Figure 4.42 is used to remember the real Modbus slave even with the same profile or type.



Data Concentrator > Slave Maps

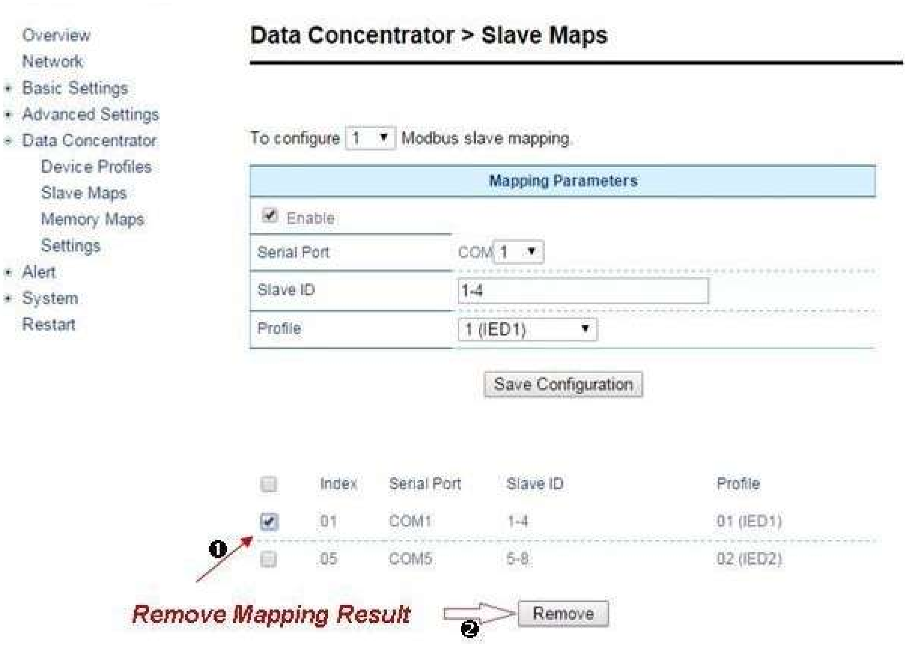
To configure 1 ▼ Modbus slave mapping.

Mapping Parameters	
☑ Enable	
Serial Port	COM 1 ▼
Slave ID	1
Profile	1 (S1-4) ▼
Alias Name	C1_S1

□	Index	Serial Port	Slave ID	Profile	Alias Name
□	01	COM1	1	01 (S1-4)	C1_S1
□	02	COM1	2	01 (S1-4)	C1_S2
□	03	COM1	3	01 (S1-4)	C1_S3
□	04	COM1	4	01 (S1-4)	C1_S4
□	05	COM1	5	03 (S5-8)	C1_S5
□	06	COM1	6	03 (S5-8)	C1_S6
□	07	COM1	7	03 (S5-8)	C1_S7
□	08	COM1	8	03 (S5-8)	C1_S8
□	09	COM2	1	01 (S1-4)	C2_S1
□	10	COM2	2	01 (S1-4)	C2_S2

Figure 4.42 Map Modbus device

Figure 4.43 Remove the Map to profile.



Data Concentrator > Slave Maps

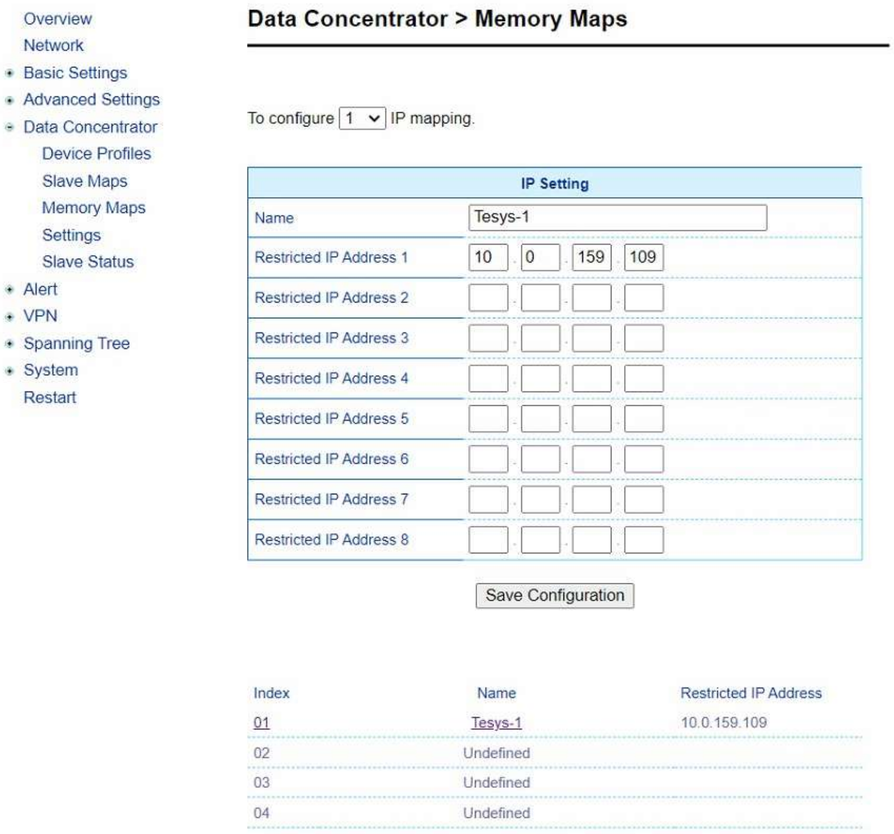
To configure 1 ▾ Modbus slave mapping

Mapping Parameters	
☑ Enable	
Serial Port	COM 1 ▾
Slave ID	1-4
Profile	1 (IED1) ▾

□	Index	Serial Port	Slave ID	Profile
☑	01	COM1	1-4	01 (IED1)
□	05	COM5	5-8	02 (IED2)

4.10.4 *Memory Mapping*

This section explains how to map the addresses of the Modbus slaves into a new address space that will be restricted access by a certain Modbus Master. As "Modbus Client Mapping" in section 4.10.1, configuring a continuous address space, so that a single Modbus command can retrieve data from more than one Modbus slave device, which is more efficient. As Figure 4.44 shows, there are maximum 16 kinds of memory mapping inside. For each entry of the memory mapping, the user can configure a new memory address mapping and select only what is required. Figure 4.44 shows a mapping example for "Tesys-T". This “Tesys-T” profile allows the Modbus master at IP 10.0.50.159 to have access.



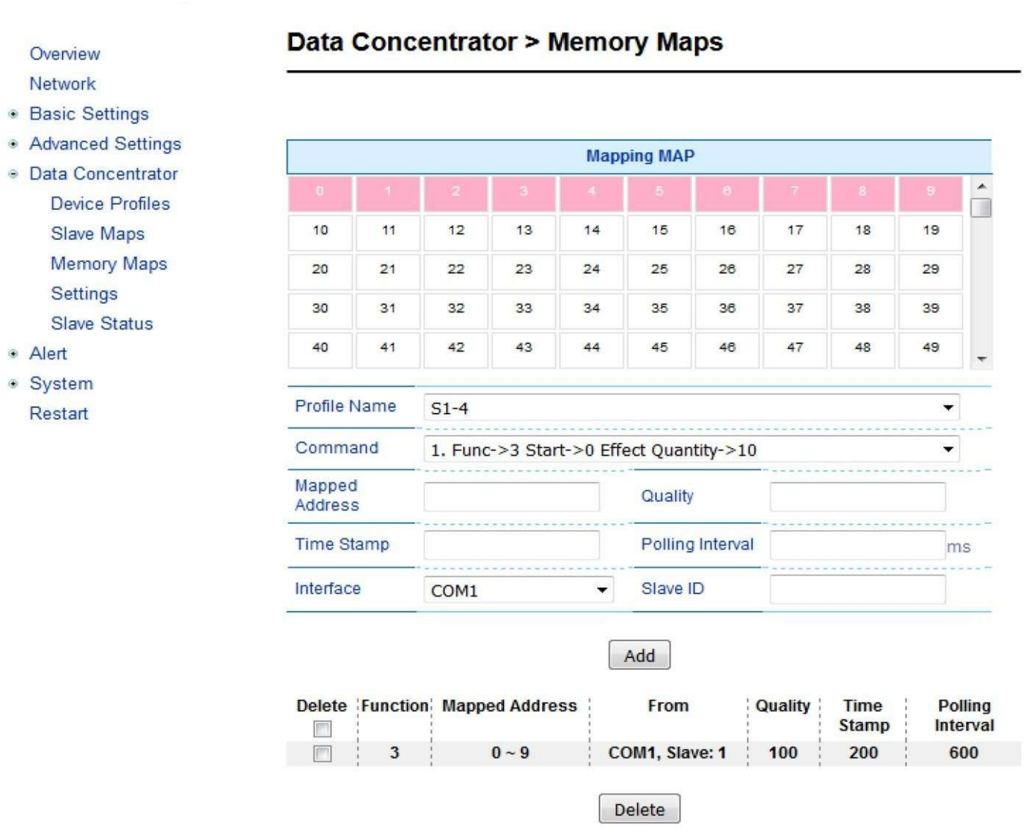
Data Concentrator > Memory Maps

To configure 1 IP mapping.

IP Setting	
Name	Tesys-1
Restricted IP Address 1	10 . 0 . 159 . 109
Restricted IP Address 2	. . .
Restricted IP Address 3	. . .
Restricted IP Address 4	. . .
Restricted IP Address 5	. . .
Restricted IP Address 6	. . .
Restricted IP Address 7	. . .
Restricted IP Address 8	. . .

Index	Name	Restricted IP Address
01	Tesys-1	10.0.159.109
02	Undefined	
03	Undefined	
04	Undefined	

The figure below shows the configured command set in the profile and maps each profile to the memory address starting from 0.



Data Concentrator > Memory Maps

Mapping MAP

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49

Profile Name	S1-4		
Command	1. Func->3 Start->0 Effect Quantity->10		
Mapped Address		Quality	
Time Stamp		Polling Interval	ms
Interface	COM1	Slave ID	

Delete ☐	Function	Mapped Address	From	Quality	Time Stamp	Polling Interval
☐	3	0 ~ 9	COM1, Slave: 1	100	200	600

Figure 4.44 Memory Maps

To make sure the required performance is achieved, the user can setup here how often this data should be polled/refreshed in the "Polling interval" item.
The first 10 registers are mapped from “S1-4” profile. These registers are mapped as address 0~9 from the viewpoint of 10.0.159.109. Figure 4.44 highlights this when the memory mapping line is left-clicked.
The upper section of the table shows the overall current situation of the 64K memory: the occupied memory will be shows pink colour. This function allows the user to know how much memory is available.
The user can put all or only the application-relevant registers of the devices sharing the same profile together, so that a single command can retrieve all the information required.
Column “Quality” and “Time Stamp” fields can provide to the master additional information about aging of data and status of the communication line. Such fields compensate the fact that Modbus protocol does not to carry any time stamp information.
When this field set, there will be 1 word (registers) and 4 words (registers) available for each mapped register or coil.
The format is:

- Data Quality (1 word):
  MSB (Bit 7): station role. Value = 1: primary; Value 0 – Secondary
  Bit 0~6 area all 0: valid
  Bit 0~6 is 0x7F (Hex): invalid.

Bit 0~6 is 0x01 (Hex): access failed from secondary unit
Bit 0~6 is 0x02 (Hex): access failed from primary unit. Bit
0~6 is 0x01 (Hex): access failed from secondary unit. Bit
0~6 is 0x04 (Hex): synchronization link failed.

Data Time Stamp (4 words):

	MSB byte	**LSB byte**
1st word		YEAR
2nd word	MONTH	DAY-OF-MONTH
3rd word	HOUR	MINUTE
4th word	MILLISECOND	

YEAR: from 0~99; this value shall be added 2000 to become real year value

MONTH: from 1~12

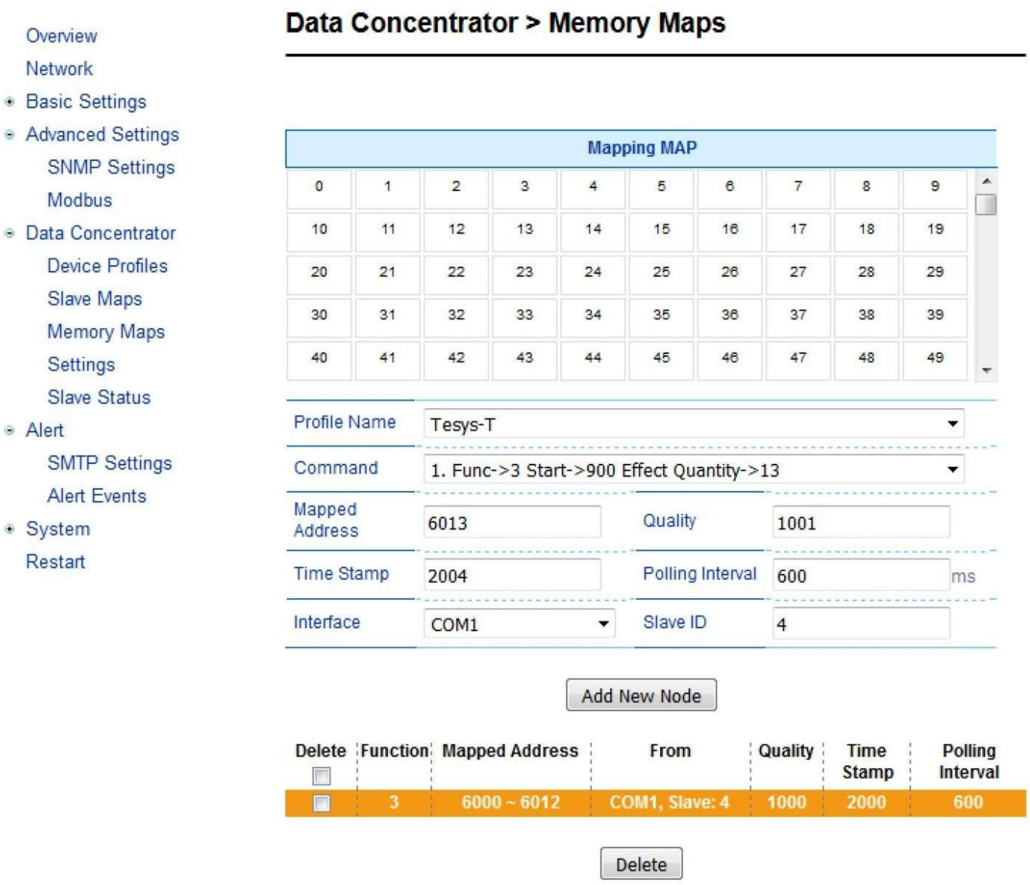
DAY-OF-MONTH: from 1~31

HOUR: from 0~23

MINUTE: from 0~59

MILLISECOND: from 0~59999

To speed up configuration for the user, once the first mapping addresses for data, quality and timestamp are set, the system will automatically suggest the next available memory address to avoid memory address overlapping errors as per below example in Figure 4.45.



Data Concentrator > Memory Maps

Mapping MAP									
0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49

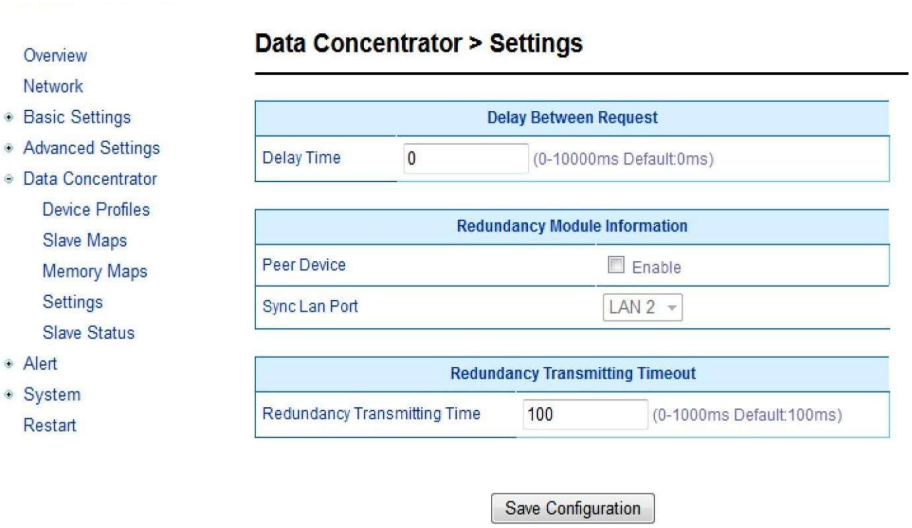
Profile Name	Tesys-T		
Command	1. Func->3 Start->900 Effect Quantity->13		
Mapped Address	6013	Quality	1001
Time Stamp	2004	Polling Interval	600 ms
Interface	COM1	Slave ID	4

Delete □	Function	Mapped Address	From	Quality	Time Stamp	Polling Interval
□	3	6000 ~ 6012	COM1, Slave: 4	1000	2000	600

Figure 4.45 Data Address-Quality address- Time stamp address auto-increment feature

4.10.5 *Concentrator settings*

This final setting of Concentrator is the time interval between each request. It is shown in the Figure 4.46. This feature is used to identify the time between Modbus commands and to configure the redundancy function.



Data Concentrator > Settings

Delay Between Request		
Delay Time	0	(0-10000ms Default:0ms)

Redundancy Module Information	
Peer Device	□ Enable
Sync Lan Port	LAN 2

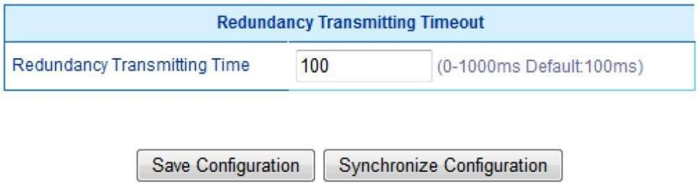
Redundancy Transmitting Timeout		
Redundancy Transmitting Time	100	(0-1000ms Default:100ms)

Figure 4.46 Time interval setting between Modbus commands

For activating the redundancy function, the user is required to:

1. Enable the Redundancy function by flagging the “Peer Device” check box.
2. Select the “Sync Lan port” that is connected directly to the peer device.

After enabling the “Peer Device” check box, the button “Synchronize Configuration” shown in Figure 4.47 will show up. If the data concentrator is already fully configured, the user can click “**Synchronize Configuration**” to make the devices sync configuration. In this way, the user can ensure both are set in the same way. And the parameter “Redundancy Transmitting Timeout” defines how often the two devices will sync with each other in a normal situation. If users would like to obtain the most efficient real-time data gathering, set the value to 0.



Redundancy Transmitting Timeout		
Redundancy Transmitting Time	100	(0-1000ms Default:100ms)

Figure 4.47 Synchronize configuration button.

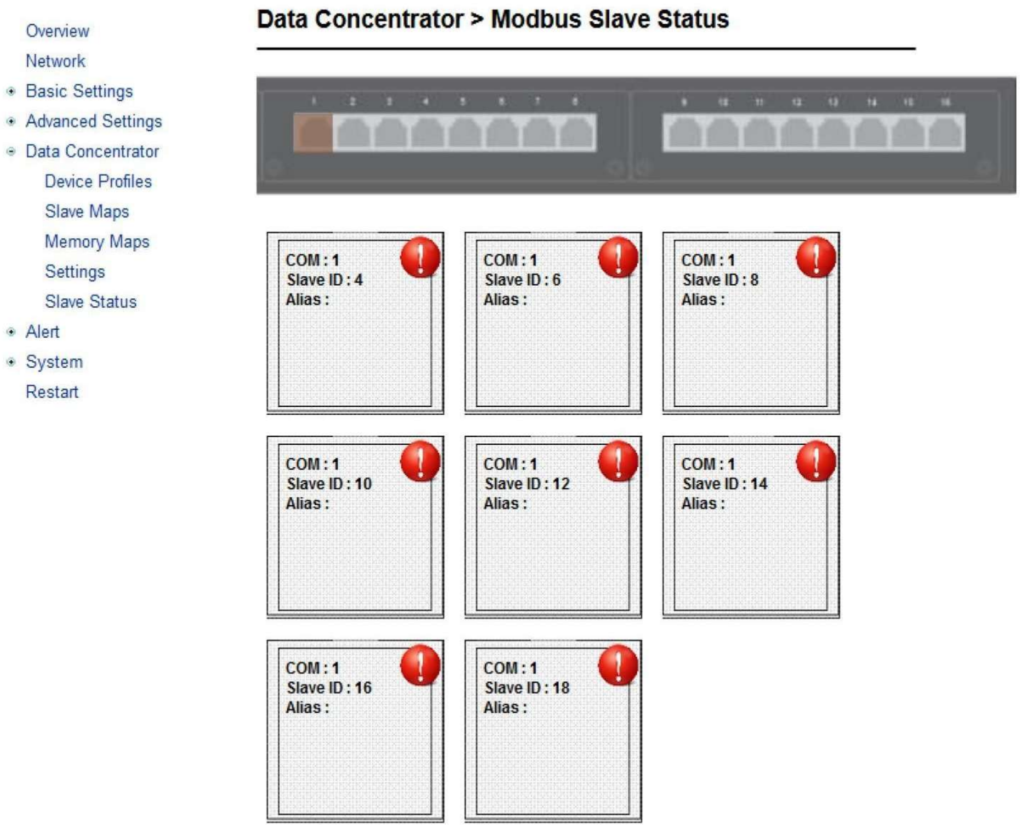
4.10.6 *Modbus Slave Status - Status Registers*

To avoid the miscommunication from the Concentrator to the device, the Concentrator will always return a value to the host, which can be the last available value (that may be outdated) or a value set by the user as specified in Section 4.10.2.

To allow users to get the device online/offline status, in XMT59XX-CT, 16 status registers are defined specifically. The range is from number 65501 to 65516. 65501 refers to COM1 and 65516 to COM 16. Each register includes 16 bits/1 word. Each bit from LSB to MSB indicates the status of mapped slave id.

The page “Status Registers”, also accessible from the Web UI, reports this information also.

Registers shown in the Fig. 4.48 refer to all slave device status under 16 COMs. The host Modbus Master can read these data to retrieve the status anytime and realize if the data is not updated and if the devices -or the communication line- have something wrong.



Data Concentrator > Modbus Slave Status

COM : 1
Slave ID : 4
Alias :

COM : 1
Slave ID : 6
Alias :

COM : 1
Slave ID : 8
Alias :

COM : 1
Slave ID : 10
Alias :

COM : 1
Slave ID : 12
Alias :

COM : 1
Slave ID : 14
Alias :

COM : 1
Slave ID : 16
Alias :

COM : 1
Slave ID : 18
Alias :

Figure 4.48 Status registers

4.10.7 *Concentrator role Status Registers*

To identify the concentrator role, status register number 65500 has been defined. By accessing this register (1 word, 2 bytes) the concentrator will return the information related to primary/secondary role of the concentrator.

Role register (1 word, 2 bytes)

Bit 2: Sync link bit – 1: sync link alive; 0: sync link broken.
Bit 7: Role bit – 1: Primary; 0: Secondary
Bit 8: Redundancy bit – 1: Redundancy module is enabled; 0: Redundancy module is disabled

Example:

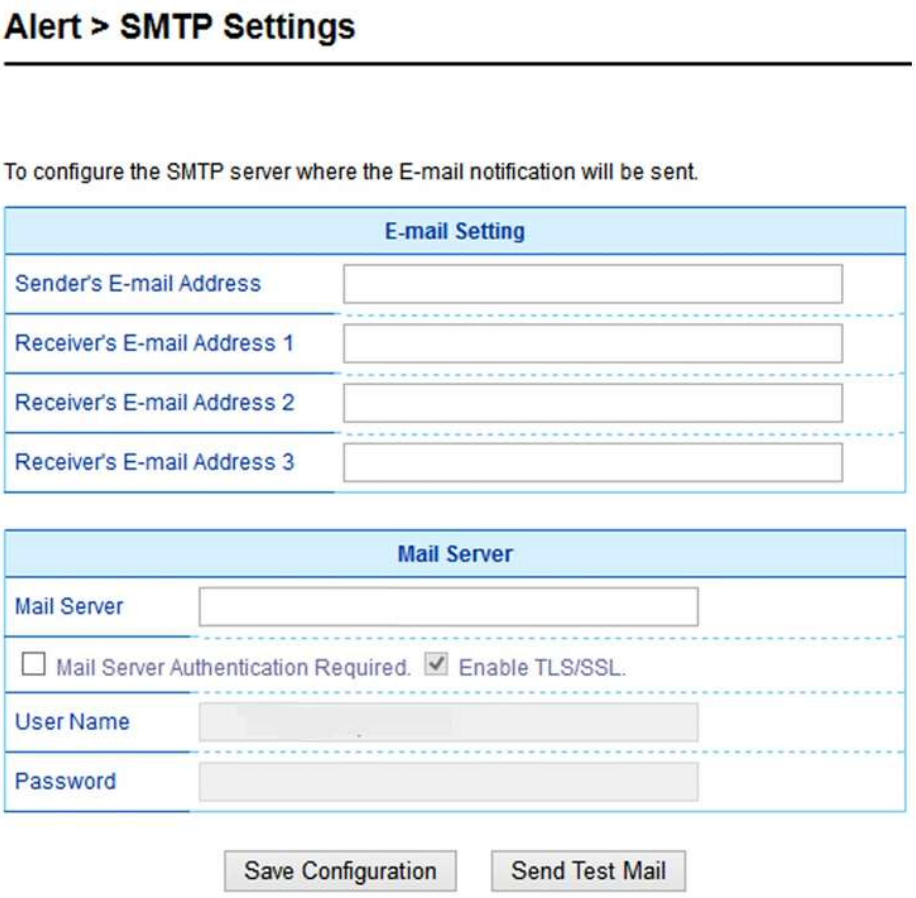
0x180: Redundancy enabled; Primary; Sync link OK.
0x100: Redundancy enabled; Secondary; Sync link OK.
0x184: Redundancy enabled; Primary; Sync link Fail.
0x104: Redundancy enabled; Secondary; Sync link Fail.

4.11 *Alert*

4.11.1 *Settings*

When enabled, an E-mail alert will be sent to the designated E-mail addresses in the **SMTP** (Simple Mail Transfer Protocol) **Settings.** To setup an email alert function, the user needs to configure the **sender's E-mail address**, the **receiver's E-mail addresses** (up to three receivers), and the mail server configuration as shown in Figure 4.49. Under **Mail Server** settings, fill in the IP address or host name of a **Mail Server**. Make sure that the Modbus Gateway device is able to resolve the host name properly. This require the DNS server to be configured first as explained in Section o. If a mail server authentication is required, check on the **Mail Server Authentication Required** box and fill in the **User Name** and the **Password** fields.

After configuration of the SMTP Settings is complete, click **Save Configuration** to save all changes that have been made. A **Save Successfully** message will show up, and the web browser will be redirected back to the **SMTP Settings** page**.** The user can also send a test E-mail from the Modbus Gateway by clicking on the **Send Test Mail** button. A pop-up window will notify the user of the result of test mail. If there is a problem, please re-check the information of **Mail Server**, **User Name** and **Password** or check the network connection to the **Mail Server**.



Alert > SMTP Settings

To configure the SMTP server where the E-mail notification will be sent.

E-mail Setting	
Sender's E-mail Address	
Receiver's E-mail Address 1	
Receiver's E-mail Address 2	
Receiver's E-mail Address 3	

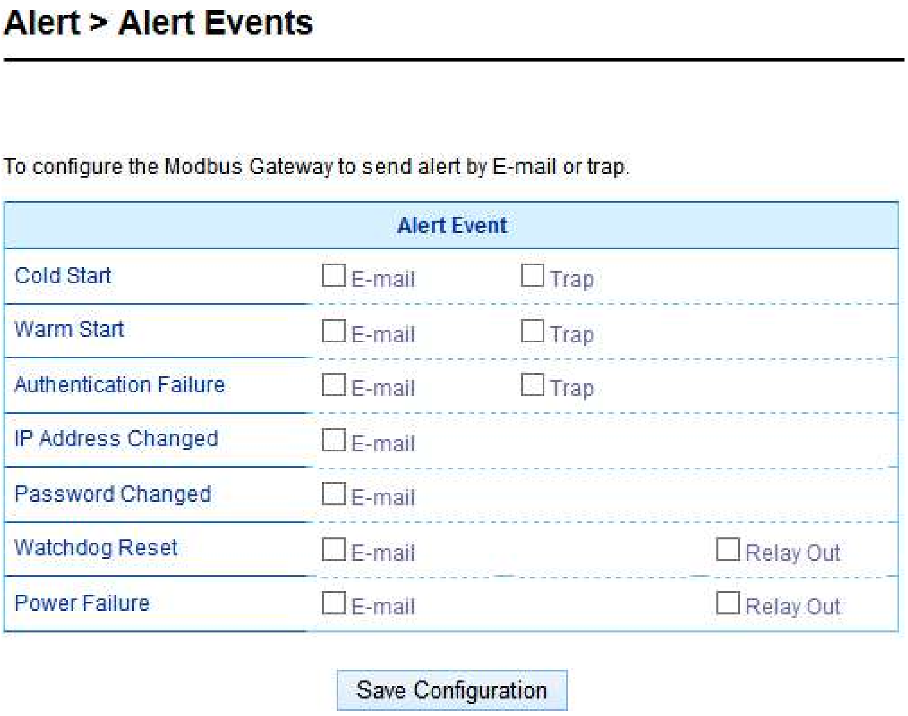
Mail Server	
Mail Server	
□ Mail Server Authentication Required. ☑ Enable TLS/SSL.	
User Name	
Password	

Figure 4.49 SMTP Settings Web Page

4.11.2 *Alert Events*

In **Alert Events** settings**,** the user can configure options to have the Modbus Gateway sending out device information to alert users, administrators, or responsible personnel as shown in Figure 4.50. They can be sent out automatically. There are seven anomalies defined on this page that can trigger alert functions (by checking the corresponding **E-mail** boxes), which are:

- **Cold Start** is an event when power supply is interrupted,
- **Warm Start** is an event when the device Restart function is used either by pressing a button or by its interface,
- **Authentication Fail** is an event when incorrect username and password are entered,
- **IP address change** is an event when the device's IP address is changed,
- **Password Changed** is an event when the authentication password is changed,
- **Watchdog Reset** is an event when the system reboots because of a hardware failure or a software crash,
- **Power Failure** : devices equipped with redundant (dual) power input are set as they expect to have power available from both sources at the same time. In the event one of the two power inputs is missing, the Relay output is triggered.



Alert > Alert Events

To configure the Modbus Gateway to send alert by E-mail or trap.

Alert Event			
Cold Start	□ E-mail	□ Trap	
Warm Start	□ E-mail	□ Trap	
Authentication Failure	□ E-mail	□ Trap	
IP Address Changed	□ E-mail		
Password Changed	□ E-mail		
Watchdog Reset	□ E-mail		□ Relay Out
Power Failure	□ E-mail		□ Relay Out

Figure 4.50 Alert Events Web Page

The user can also set an SNMP trap by checking the **Trap** checkbox for each of the first three anomalies above. This will send out alerts to an SNMP Trap Server. Note that to configure **SNMP Trap Server** please see Section 4.9.

The user can enable **Watchdog Reset** and **Power Failure** events to trigger the Relay Output alarm digital output. In order to do so, check the corresponding checkbox in front of the "**Relay Out**".

After the **Alert Events** setting is complete, click on **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, and the web browser will be redirected back to the **Alert Events** page**.**

4.12 *VPN*

A virtual private network(VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private networks, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.
See below VPN scenario of SE/PG/XMT59XX for your reference.

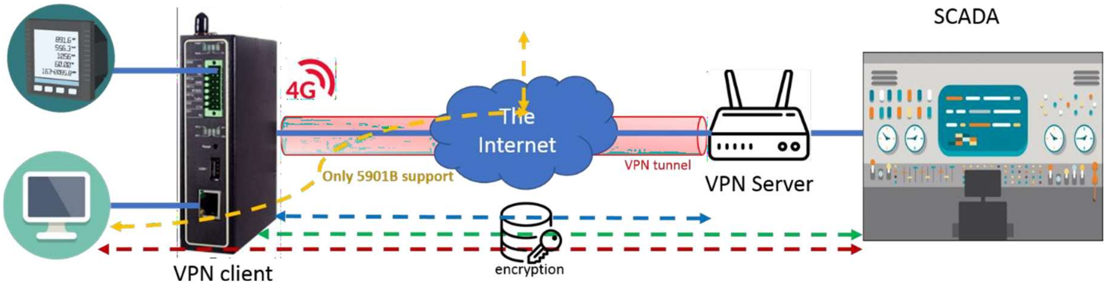


Figure 4.51 VPN Scenario of XSE/XGP/XMT59XX

XMT59XX supports several VPN protocols: PPTP (Point-to-Point-Tunneling-Protocol), IPsec (Internet Protocol Security), and OpenVPN. In order to configure VPN, please click on the related item in the dedicated VPN sub-menu on the left-hand side of the screen, as shown in Figure 4.52 below.

A better description of PPTP is available in Chapter 4.13 below
A better description of OpenVPN is available in Chapter 4.14 below.
A better description of IPsec related settings is available in Chapter 4.15 below.

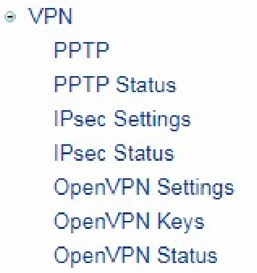
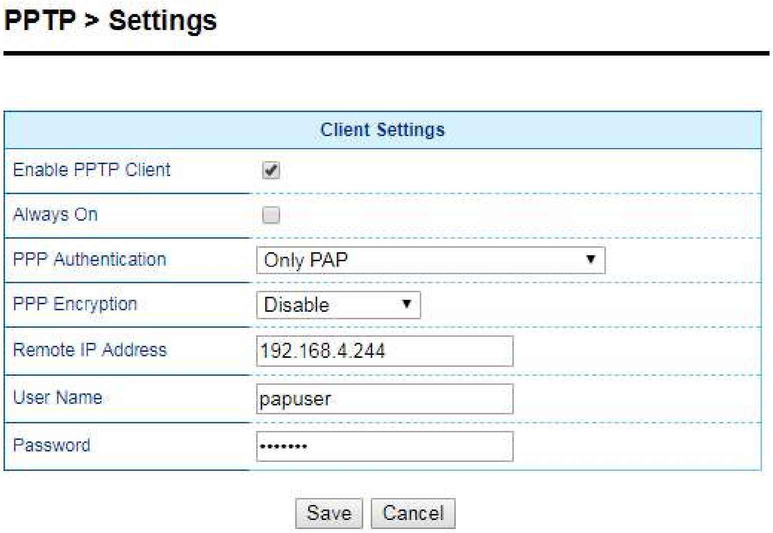


Figure 4.52 VPN menu structure

4.13 *PPTP Settings*

PPTP (Point-to-Point Tunneling Protocol) is a method for implementing virtual private networks. PPTP uses a TCP control channel and a GRE tunnel to encapsulate PPP packets. Select the PPTP item in the menu to configure a PPTP tunnel. Figure 4.53 shows the PPTP configuration page under PPTP web setting. Currently XMT59xx series only supports PPTP client. After settings are completed, click "**Save**" to save the configuration.



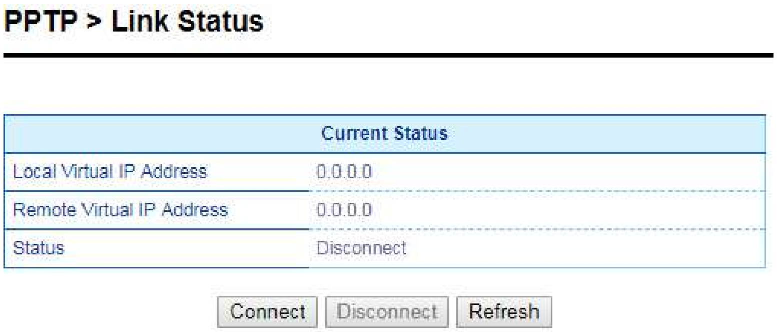
PPTP > Settings

Client Settings	
Enable PPTP Client	☑
Always On	□
PPP Authentication	Only PAP ▼
PPP Encryption	Disable ▼
Remote IP Address	192.168.4.244
User Name	papuser
Password	•••••••

Figure 4.53 PPTP configuration page.

- Enable PPTP client: Check this to enable the PPTP client on XMT59XX series.
- Always on: Check this to have XMT59xx to automatically reconnect in event of disconnection.
- PPP Authentication: Specify here the authentication algorithm – should be same as server
- PPP Encryption: Specify here the encryption – should be same as server
- Remote IP address: Specify here the IP address of PPTP server.
- User Name: Specify here the User name for authentication.
- Password: Specify herePassword for authentication.

Figure 4.54 below shows the PPTP Link status.



PPTP > Link Status

Current Status	
Local Virtual IP Address	0.0.0.0
Remote Virtual IP Address	0.0.0.0
Status	Disconnect

Figure 4.54 PPTP Link Status

- Local Virtual IP Address: The virtual IP address assigned by PPTP server.
- Remote Virtual IP Address: The virtual IP address of PPTP server.
- Status: It shows the PPTP tunnel connection status. It will show Disconnect, Connect and Connecting.
- Disconnect: No tunnel is established.

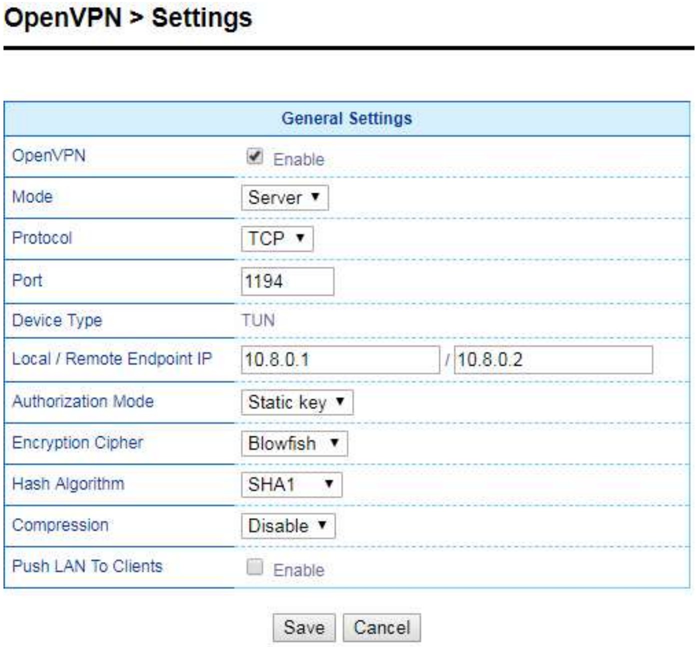
- Connect: PPTP Tunnel is established.
- Connecting: PPTP Tunnel is establishing.
- Connect: Click this button to connect to PPTP server.
- Disconnect: Click this button to disconnect PPTP tunnel.
- Refresh: Clieck this button to refresh the PPTP tunnel status.

4.14 *OpenVPN Settings*

OpenVPN is an application that implements VPN for creating secure point-to-point or site-to-site connections in routed or burdged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.
OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificates. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and certificate authority.
There are two OpenVPN connection scenarios. They are the TAP and TUN scenario. The product can create ether a layer-3 based IP tunnel(TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, you have to specify which type of OpenPVN connection scenario is to be adopted. Currently XMT59xx series only support TUN mode.

4.14.1 *OpenVPN Setting*

In order to configure OpenVPN, click on the VPN tab in the left hand side of the menu and then **OpenVPN Settings**. The user interface is shown in below Figure 4.55.



OpenVPN > Settings

General Settings	
OpenVPN	☑ Enable
Mode	Server ▼
Protocol	TCP ▼
Port	1194
Device Type	TUN
Local / Remote Endpoint IP	10.8.0.1 / 10.8.0.2
Authorization Mode	Static key ▼
Encryption Cipher	Blowfish ▼
Hash Algorithm	SHA1 ▼
Compression	Disable ▼
Push LAN To Clients	□ Enable

Figure 4.55 OpenVPN

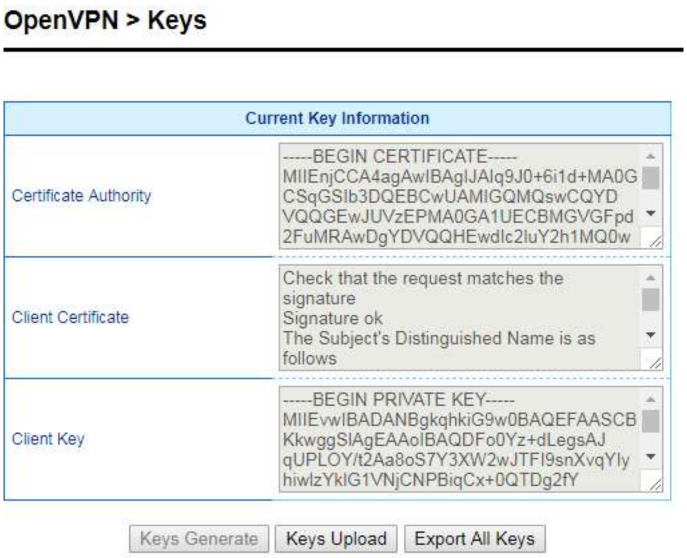
Setting The OpenVPN parameters are described as below:

- **OpenVPN**: Check this to enable OpenVPN.
- **Mode**: Specifies what the scenario of this device, server or client. When choosing server mode, the device will play as server role and will standby for client connection.
- **Protocol**: Selects the transport layer protocol to be used for VPN (TCP or UDP).

- **Port**: Defines the port number for TCP/UDP connection.
- **Device Type**: OpenVPN tunnel connection by TUN (Tunnel) mode or TAP mode. Currently XMT59xx series only supports TUN (Tunnel) mode.
- **Virtual IP** (only when "OpenVPN Server" mode is selected): Specify the server's virtual IP. Virtual IP will only be available when SSL/TLS is chosen as the Authentication Mode. The Server's virtual IP address will be 10.8.0.1/24 and client virtual IP address will be 10.8.0.x/24.
- **Local/Remote endpoint IP** (only when "OpenVPN Client" mode is selected): Specifies the local and remote endpoint virtual IP address of this OpenPVN gateway. Local/Remote endpoint IP only be available when static key is chosen in Authentication Mode.
- **Authentication Mode**: Specify the authorization mode the OpenVPN server. There are 2 options available:
  - SSL/TLS: OpenVPN will use TLS authorization mode, and the following items CA cert, Server Cert and DH PEM will be used. See section 4.14.2 below for mode details.
  - Static Key: OpenVPN will use static key authorization, and the static key will be used. See section 4.14.2 below for mode details.
- **Encryption Cipher**: Specify the Encryption cipher. There are 5 options available: blowfish, AES 256, AES 192, AES 128 and Disable. When Disable is selected, no encryption will be used.
- **Hash Algorithm**: Specify the Hash algorithm. There are 5 options available: SHA1, MD5, SHA 256, SHA 512 and Disable.When Disable is selected, no Hash algorithm will be used.
- **Compression**: Specify whether or not the tunnel packets will be compressed. There are three options available: LZ4, LZO and Disable. When Disable is chosen, the packet won't be compressed.
- **Push Lan to clients** (only when "OpenVPN Server" mode is selected): When enabled, XMT59xx will push the LAN port subnet to the OpenVPN remote clients, so that the remote client will add a route to the XMT59XX local network. Only XMT5901B supports this function.

4.14.2 *OpenVPN Keys*

OpenVPN requires encryption keys (unless Encryption Cipher is disabled). In order to key-in, import or generate encryption keys, please select "OpenVPN Keys" from the VPN menu on the left-hand side of the user interface.



OpenVPN > Keys

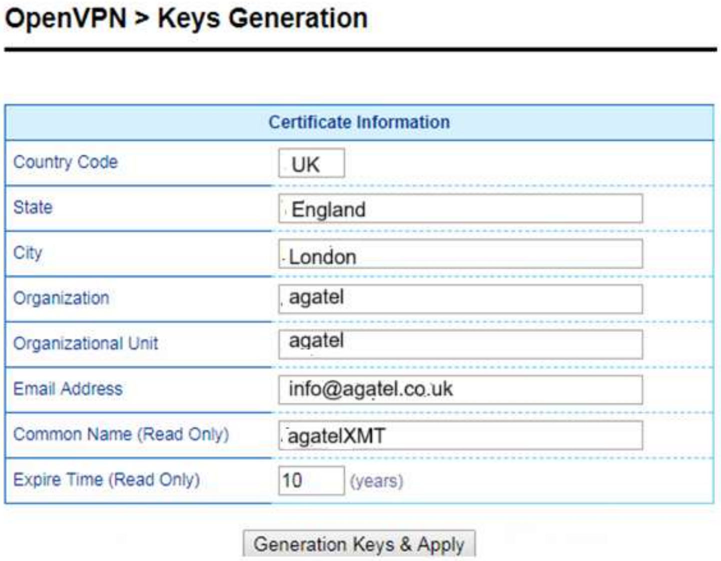
Current Key Information	
Certificate Authority	-----BEGIN CERTIFICATE----- MIIEnjCCA4agAwIBAgIJAIq9J0+6i1d+MA0G CSqGSIb3DQEBCwUAMIGQMQswCQYD VQQGEwJUVzEPMA0GA1UECBMGVGFpd 2FuMRAwDgYDVQQHEwdlc2luY2h1MQ0w
Client Certificate	Check that the request matches the signature Signature ok The Subject's Distinguished Name is as follows
Client Key	-----BEGIN PRIVATE KEY----- MIIEvwIBADANBgkqhkiG9w0BAQEFAASCB KkwggSlAgEAAoIBAQDFo0Yz+dLegsAJ qUPLOY/t2Aa8oS7Y3XW2wJTFI9snXvqYly hiwlzYkIG1VNjCNPBiqCx+0QTDg2fY

Figure 4.56 OpenVPN Keys

- **Certificate Authority**: A certificate authority(CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. A CA acts as a trusted third party, trusted both by the owner and by the party relying upon the certificate.
- **Server/Client Certificate**: It shows the information of server certificate. You can check the information if you use upload server certificate file.
- **Server/Client Key**: It shows the information of server key. You can check the information if you use upload server key file.

- **Diffie Hellman parameters (Server only)**: It shows the information of Diffie Hellman paramaters.

When XMT59XX acts as OpenVPN server, the user could define his own certification information by clicking on the **Secret generate** button. Otherwise, the certificate can be imported. When generating a new key, a Pop-up window will open. Fill in the parameters and click on "**Generation Keys & Apply**" button.



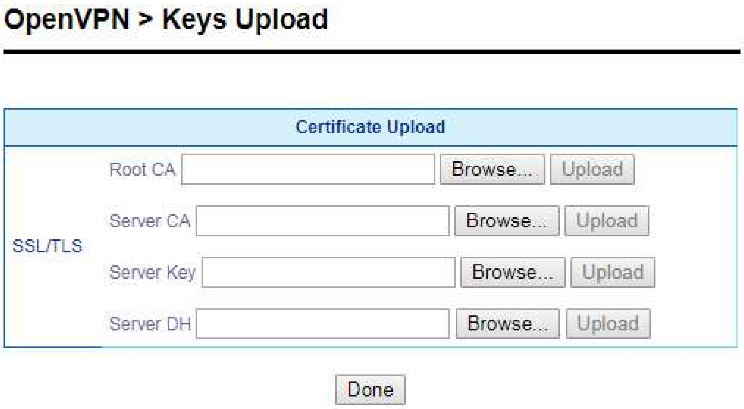
OpenVPN > Keys Generation

Certificate Information	
Country Code	UK
State	England
City	London
Organization	agatel
Organizational Unit	agatel
Email Address	info@agatel.co.uk
Common Name (Read Only)	agatelXMT
Expire Time (Read Only)	10 (years)

Figure 4.57 Certification information

- **Country Code**: Enter the country ISO code.
- **State**: Enter the state (if applicable)
- **City**: Enter the city
- **Organization**: Enter the name of organization.
- **Organization Unit**: Enter the unit or section in the organization.
- **Email Address**: Enter an email address.
- **Common Name**: The server name. (Read only)
- **Expire time**: The number of years the certificate is valid for. (Read only)

When clicking on the **Keys Upload** button instead, a pop-up window shown in Figure 4.58 will show up and will allow you to import the related server or client certificates.



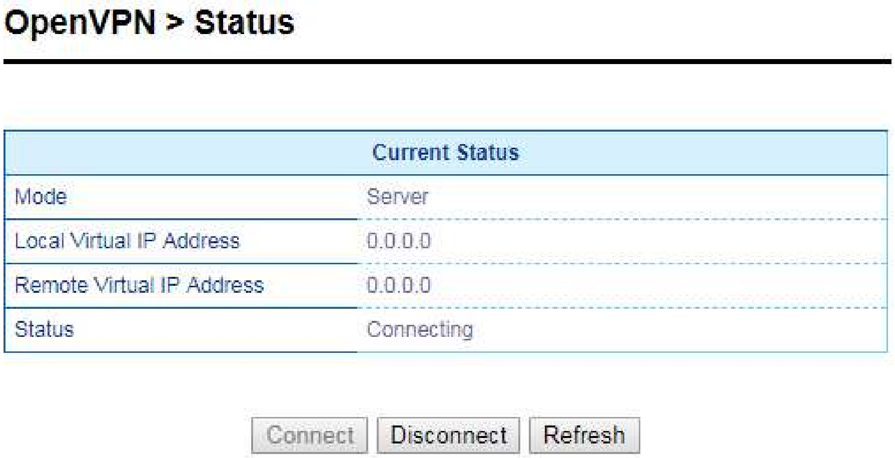
OpenVPN > Keys Upload

Figure 4.58 Certificate Upload

Click the **Browse** button to select your own server or client certificate and click on the **Upload** button. When XMT59xx acts as an OpenVPN server, use **Export All Keys** button to download all the necessary certificates include CA.crt, CA.key and the certificate and key for client side.

4.14.3 *OpenVPN Status*

In order to check the current OpenVPN connection status, click “OpenVPN status” in the VPN menu on the left-hand side of the screen. A page like below Figure 4.59 will show up when OpenVPN is in Server mode. It will look similar when set in Client mode.



OpenVPN > Status

Current Status	
Mode	Server
Local Virtual IP Address	0.0.0.0
Remote Virtual IP Address	0.0.0.0
Status	Connecting

Figure 4.59 OpenVPN server status

Client Mode Description:

- **Mode**: Displays the OpenVPN mode XMT59xx is currently running as.
- **Local Virtual IP address**: Displays the Local virtual IP address.
- **Remote Virtual Status**: Displays the Remote virtual IP address.
- **Status**: Displays the current status of OpvnVPN connection. It will include Disconnected, Connecting and Connected.

Server Mode Description:

- **Mode**: Displays the OpenVPN mode XMT59xx is currently running as.
- **Local Virtual IP address**: Displays the Local virtual IP address.
- **Status**: Displays the current status of OpvnVPN connection. It will be either be Deactivated, Activating, Disconnected, Connecting and Connected.

4.15 *IPsec Settings*

IPsec (or Internet Protocol Security) which is a network protocol suit that can establish secure and reliable communications for different application scenarios. IPsec enables data confidentiality, data integrity, data origin authentication, and antireplay. For example, a corporate headquarter and its branch offices in the fields do not need to apply for dedicated communication lines for sharing their network resources securely. To securely communicate and shared company's resources over the Internet, IPsec connections can be employed to secure all applications at the IP layer. In another case, when employees are on a business trip, they can establish IPsec connections with their company over their mobile devices or the public network to access the internal network resources in their company.

XMT59XX has an IPsec connection function to establish a secure communication link between **host-to-host**, **host-to-subnet** (or host-to-network), and **subnet-to-subnet** (or network-to-network). Note that at the other endpoint of the Internet, a router or gateway with full IPsec capability is required to successfully establish the secure communication. There are two types of IPsec connection modes or types supported by XMT59XX which are **Tunnel mode** and **Transport mode.**

- In **Tunnel mode**, the entire IP packet is encrypted and authenticated. The IP packet is then encapsulated into a new IP packet with a new IP header. The **Tunnel mode** which is used to create Virtual Private Network (VPN) can be applied to the **host-to-host**, the **host-to-subnet**, and the **subnet-to-subnet** communications. The packet (datagram) format for **Tunnel mode** is as follow:

New IP Header	IPsec Header	Original IP Packet	Optional IPsec Trailer

- In **Transport mode**, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact because the IP header is not modified and not encrypted. However, when the authentication header is used, the IP addresses cannot be modified by Network Address Translation (NAT). The **Transport mode** can only be applied in the **host-to-host** communication. The packet (datagram) format for **Transport mode** is as follow:

Original IP Header	IPsec Header	Original IP Packet	Optional IPsec Trailer

A **host-to-host** connection is typically used in a simple point-to-point communication. It is useful for a direct communication with a server or between the device (XMT59XX) and a peer device (such as another XMT59XX). Note that this type of connection cannot be use for accessing entire sub-network resources. Figure 4.60 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode.**

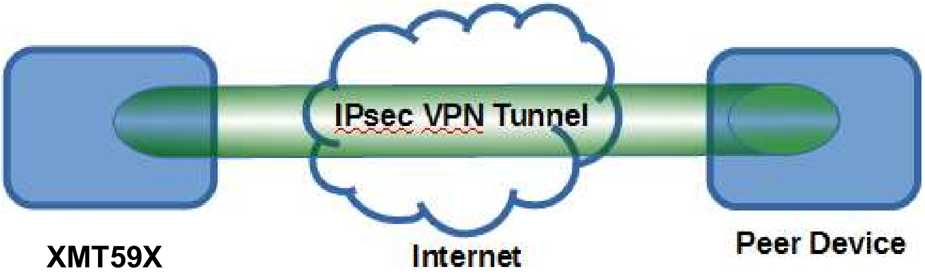


Figure 4.60 An example of Host-to-Host Connection on XMT59XX.

A **host-to-subnet** (or host-to-network) connection is mainly applied when one endpoint needs to access the other side's sub-networks. Typical applications are employees who are travelling on business and would like to connect back to their corporate headquarters via mobile devices. They can establish IPsec connections to access the internal corporate network resources. Figure 4.61 illustrates a road-warrior application in which XMT59XX can access a remote sub-network resource via a peer gateway. Figure 4.62 illustrates a gateway application in which

XMT59XX can passively accept connection requests from remote sides and provide access to the XMT59XX sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

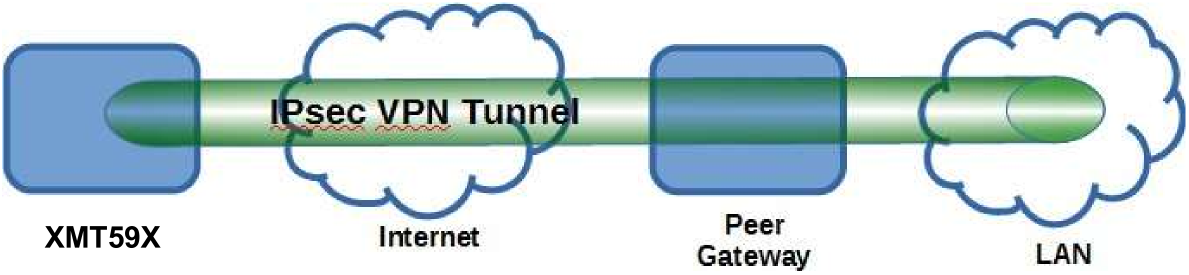


Figure 4.61 Roadwarrior Application using Host-to-Subnet Connection

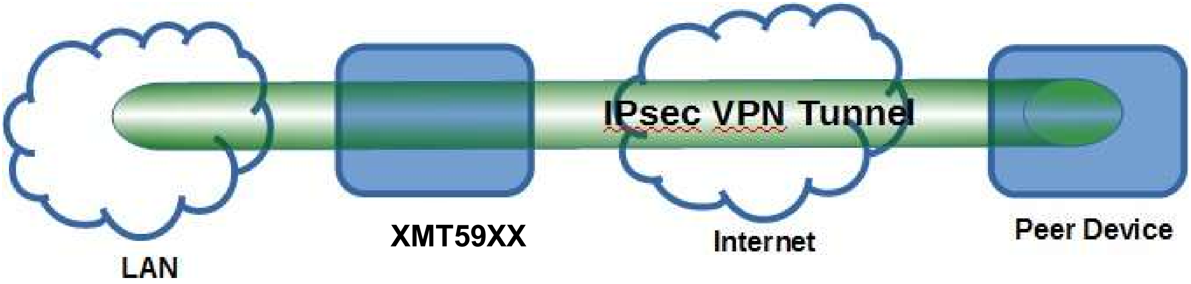


Figure 4.62 Gateway Application using Host-to-Subnet Connection

A **subnet-to-subnet** connection is mainly used to connect two subnets from different sides together. Typically, applications are corporate headquarters and branch offices that share internal network resources. A specific application can also be set up as one side's subnet to establish IPsec VPN tunnels for accessing a device in the other side's subnet or as a device in one's side subnet to establish IPsec VPN tunnels for accessing another device in the other side's subnet.

Figure 4.63 illustrates an example of the subnet-to-subnet connection with a network application. A host inside the remote subnet can also connect to a local subnet (host-network application) based on this subnet-to-subnet connection as shown in Figure 4.64. On the other hand, two different devices on two different subnets (host-host application) can be connected via a IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 4.65. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

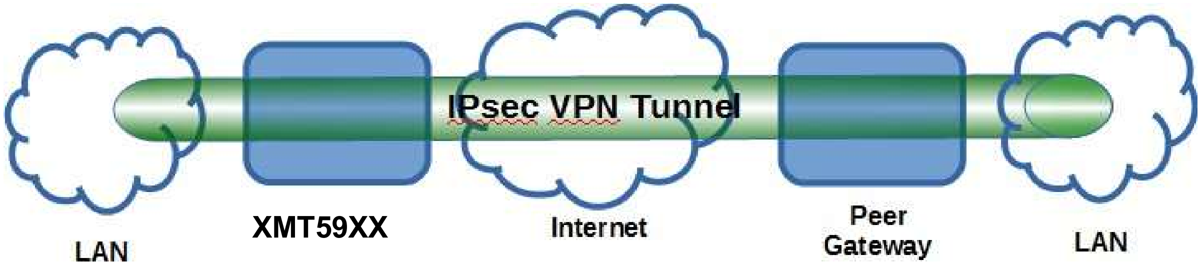


Figure 4.63 Example of network application using subnet-2-subnet connection via XMT59XX and a peer device

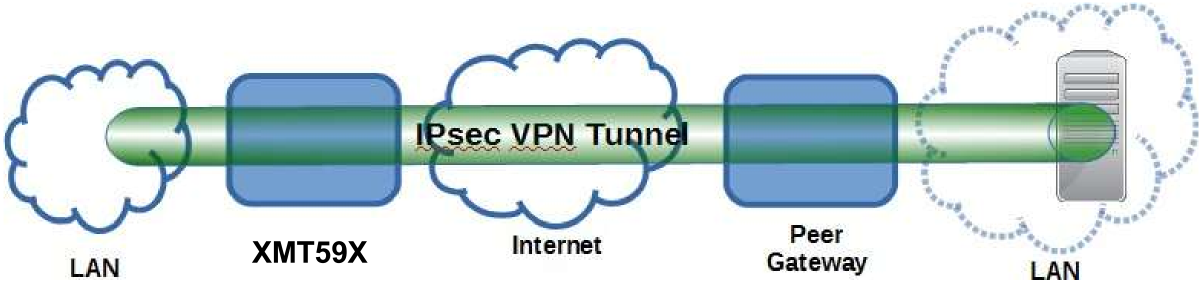


Figure 4.64 An example of host-network application via the subnet-to-subnet connection

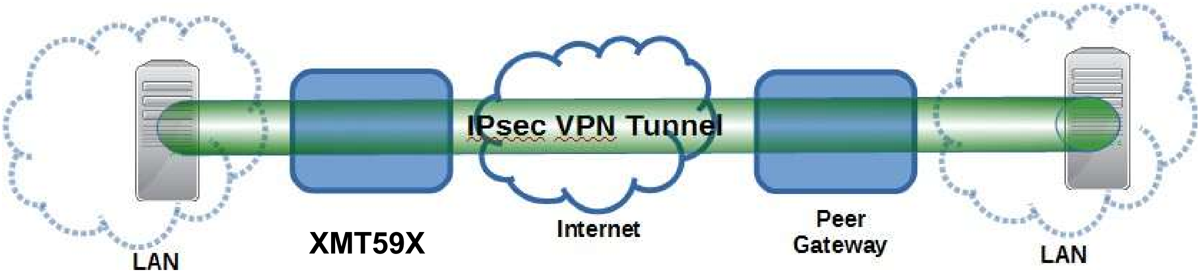


Figure 4.65 An example of host-host application via the subnet-to-subnet connection

In some network configuration, there is an implementation of network address translation (NAT) on its gateway/routers. NAT is typically used to allow private IP addresses on private networks behind gateways/routers with a single public IP address connecting to the public Internet. The internal network devices can communication with hosts on the external network by changing the source address of outgoing requests to that of the NAT device (gateway/router) and relaying replies back to the originating device. IPsec virtual private network (VPN) clients use network address translation (NAT) traversal in order to have Encapsulating Security Payload (ESP) packets traverse NAT. IPsec uses several protocols in its operation, which must be enabled to traverse firewalls and network address translators (NATs), such as

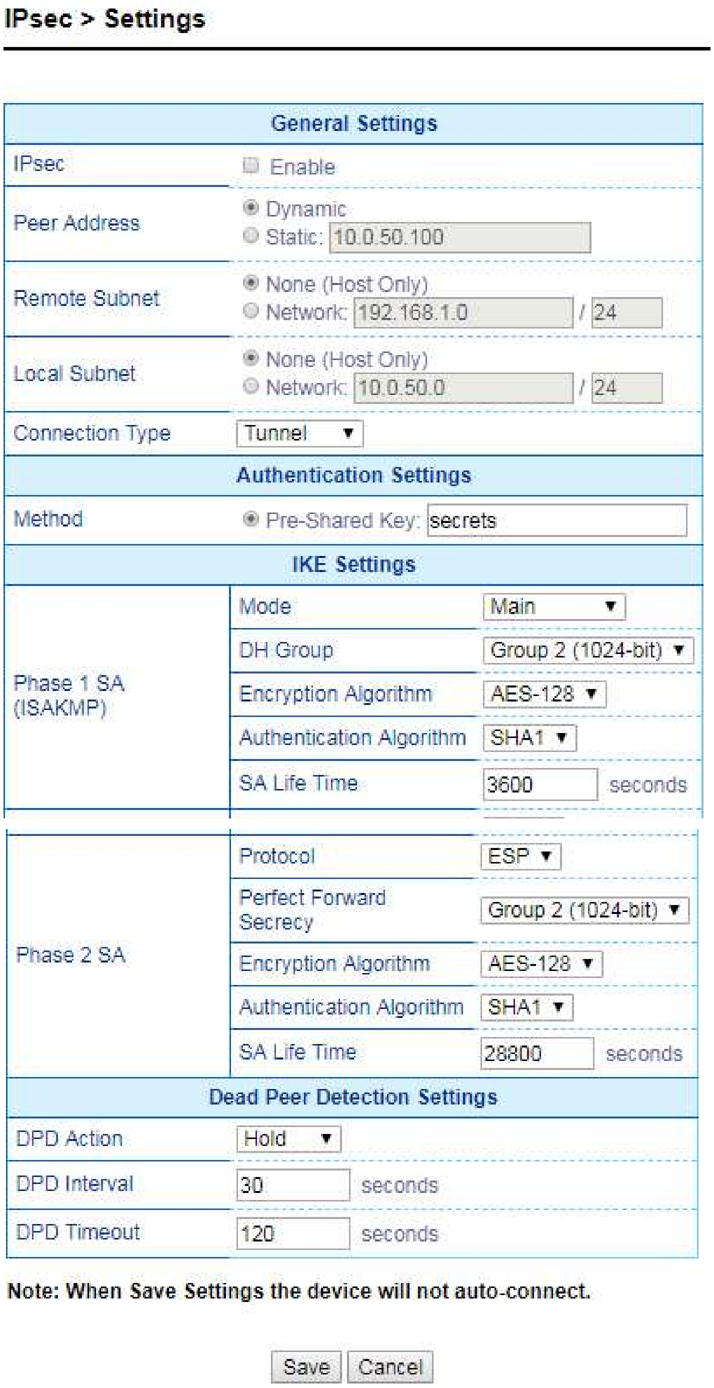
- Internet Key Exchange (IKE) protocol uses User Datagram Protocol (UDP) port number 500.
- Encapsulating Security Payload (ESP) uses IP protocol number 50.
- Authentication Header (AH) uses IP protocol number 51.
- IPsec NAT traversal uses UDP port number 4500 when NAT traversal is in use.

XMT59XX also has a feature called NAT traversal (NAT-T) that allows the IPsec tunnel to pass through the NAT in its network. XMT59XX will activate this option automatically and encapsulate the IPsec packets inside UDP port 4500 to be able to pass through a NAT router.

To provide security service for all types of tunnel connections and applications described above, XMT59XX utilizes the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite. Note that IKE builds upon the Oakley protocol and ISAKMP (Internet Security Association and Key Management Protocol). IKE uses X.509 certificates for authentication either pre-shared or distributed using DNS (preferably with DNSSEC). IKE also uses a Diffie-Hellman key (DH) key exchange to set up a shared session secret from which cryptographic keys are derived. The IPsec security associations (SA) is divided into two phases. In phase one, IKE creates an authenticated secure channel between XMT59XX and its peer device, which is called the IKE Security Association. The Diffie-Hellman (DH) key agreement is always performed in this phase to create a shared secret key or DH key. In phase two, IKE negotiates the IPsec security associations and generates the required key material for IPsec. This IPsec key which is a symmetrical key will be used for bulk data transfer inside the IPsec tunnel. A new Diffie-Hellman agreement can be done in phase two, or the keys can be derived from the phase one shared secret.

4.15.1 *IPsec Settings*

Figure 4.66 shows the **IPsec Settings** web page under the **IPsec Settings** menu**.** There are four sections on this page**: General Settings**, **Authentication Settings**, **IKE Settings**, and **Dead Peer Detection Settings.**



IPsec > Settings

General Settings		
IPsec	☐ Enable	
Peer Address	● Dynamic ○ Static: 10.0.50.100	
Remote Subnet	● None (Host Only) ○ Network: 192.168.1.0 / 24	
Local Subnet	● None (Host Only) ○ Network: 10.0.50.0 / 24	
Connection Type	Tunnel ▼	
Authentication Settings		
Method	● Pre-Shared Key: secrets	
IKE Settings		
Phase 1 SA (ISAKMP)	Mode	Main ▼
	DH Group	Group 2 (1024-bit) ▼
	Encryption Algorithm	AES-128 ▼
	Authentication Algorithm	SHA1 ▼
	SA Life Time	3600 seconds
Phase 2 SA	Protocol	ESP ▼
	Perfect Forward Secrecy	Group 2 (1024-bit) ▼
	Encryption Algorithm	AES-128 ▼
	Authentication Algorithm	SHA1 ▼
	SA Life Time	28800 seconds
Dead Peer Detection Settings		
DPD Action	Hold ▼	
DPD Interval	30 seconds	
DPD Timeout	120 seconds	

Note: When Save Settings the device will not auto-connect.

Figure 4.66 IPsec Tunnels Web Page under IPsec Setting Menu

To configure **IPsec Settings**, first you need to configure the **General Settings** section under the **IPsec Settings** menu**.** Under the **General Settings**, there are five parameters that need to be set as follows:

- **IPsec**: By checking the box for this option, you enable the IPsec feature for XMT59XX.

- **Peer Address:** This option is to specify the IP address of a remote host or peer host or remote gateway. There are two choices for the **Peer Address** which are **Dynamic** and **Statics.**
    - **Dynamic:** When you selected the **Dynamic** by choosing the **Dynamic** radio button, the **Peer Address** or the remote device IP address is not fixed or unknown**.** Note that when **Peer Address** is set to dynamic mode, the XMT59XX can accept remote connection request or will be the responder**.**
    - **Static:** On the other hand, if you know the IP address of the remote device, you can choose the ratio button for **Static** option and enter the IP address in the text box behind it**.** The XMT59XX will be the initiator/responder.
- **Remote Subnet:** This option is to indicate whether you want to create an IPsec connection to the remote subnetwork**.** There are also two choices for **Remote Subnet** access**:**
    - **None (Host Only):** This option is to specify that the remote subnet is not supported or no remote subnet and only host access is supported**.** That is the remote end of the IPsec tunnel is a host or peer device only**.**
    - **Network:** This option is to specify the **Remote Subnet** by entering the **Subnet IP Address** and the number of **Subnet Masking Bits** or associated routing prefix**.** This option supports the Classless Inter-Domain Routing (CIDR) notation**.** For example, Subnet IP Address is 192**.**168**.**11**.**0 and Subnet mask are 24 bits (from 255.255.255.0)**.**
- **Local Subnet:** This option is to enable an IPsec connection to the local subnetwork. There are two choices for **Local Subnet** access:
    - **None (Host Only):** This option is to specify that the local subnet is not supported or no local subnet and only local host access is supported. That is the local end of the IPsec tunnel is a host or peer device only.
    - **Network:** This option is to specify the **Local Subnet** by entering the **Subnet IP Address** and the number of **Subnet Masking Bits** or associated routing prefix. This option supports the Classless Inter-Domain Routing (CIDR) notation**.** For example, Subnet IP Address is 192**.**168**.**11**.**0 and Subnet mask are 24 bits (from 255.255.255.0)**.**
- **Connection Type:** This option is to specify the IPsec connection type which can be either **Tunnel** mode or **Transport** mode**.** Please select the corresponding connection type from the drop**-**down list**.** Note that the **Tunnel mode** can be applied to the **host-to-host**, the **host-to-subnet**, and the **subnet-to-subnet** communications**.** The **Transport mode** can only be applied in the **host-to-host** communication**.**

The second part of **IPsec Settings** is the **Authentication Settings.** Here you have an authentication**'**s **Method** which already selected as the **Pre-Shared Key.** Then, you must enter in a secret key or a pass**-**phrase in the textbox behind it**.** Both ends of the the VPN tunnel must use the same secret key or password. The pre-shared key can be 1 to 60 case-sensitive ASCII characters and special symbols.

The third part of **IPsec Settings** is the **IKE** (Internet Key Exchange) **Settings.** Internet Key Exchange (IKE) that XMT59XX supports is the IKE version 1 or **IKEv1.** Within the **Phase 1 SA (ISAKMP)**, there are five security options to be configured**.** In phase 1, the two VPN gateway exchange information about the encryption algorithms that they support and then establish a temporary secure connection to exchange authentication information.

- First option is the **Mode** of IKE session which defines how many steps or packets will be used or exchanged during the IKE SA negotiation**.** You can choose either **Main Mode** or **Aggressive Mode.** The **Main Mode** will send SA proposals, Diffie-Hellman public key, and ISAKMP session authentication in three exchange packets, while the **Aggressive Mode** will put all SA proposals, DH public key, and ISAKMP session authentication in to one exchange packet**. Aggressive Mode** makes the IKE negotiation quicker than **Main Mode.** The difference between **Main Mode** and **Aggressive Mode** is that the "identity protection" is used in the **Main Mode**. The identity is transferred encrypted in the **Main Mode** but it is not encrypted in **Aggressive Mode**. Typically, the **Main Mode** is recommended.
- Second option is the selection of Diffie**-**Hellman**'**s group (**DH Group**) of standardized global unique prime numbers and generators that will be used to provide secure asymmetric key exchange**.** The **DH Group** is

used to encrypt this IKE communication. XMT59XX supports two **DH groups** which are **DH Group 2**, which is a 1024-bit modular exponentiation group (MODP), and **DH Group 5**, which is a 1536-bit MODP group.

- Third option is the selection of **Encryption Algorithm** which can be either **AES-128** or **3DES.** This option will select the key size and encryption algorithm to be used in the IKEv1 Phase 1. The default value is **AES-128**.
- Fourth option is the selection of **Authentication Algorithm** which can be either **SHA1** or **MD5.** This option will select which hash algorithm will be used to authenticate packet data in the IKEv1 Phase 1. The default value is **SHA1**.
- Fifth option is the **SA Life Time** which must be set in unit of seconds. This value represents the lifetime of the IKE key which is dedicated at Phase 1 between both end host or network. The default **SA Life Time** is 10800 seconds. The configurable range for **SA Life Time** is between 300 to 86400 seconds.

Within the **Phase 2 SA**, there are five security options to be configured. Similar to **Phase 1 SA**, XMT59XX and its peer device will negotiate or exchange proposals to determine which security parameters will be used in this Phase 2 SA. A Phase 2 proposal also includes a security **Protocol** (first option), which you can choose either Encapsulating Security Payload (**ESP**) or Authentication Header (**AH**). The second option is the **Perfect Forward Secrecy** which is a property of key-agreement protocol to ensure that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. In Phase 2 SA, XMT59XX also supports two **DH groups** which are **DH Group 2** (1024-bit) and **DH Group 5** (1536-bit).

Then you can proceed to select encryption and authentication algorithms. Third option is the selection of **Encryption Algorithm** which can be either **AES-128** or **3DES.** This encryption algorithm will be used in the IPsec tunnel. The default setting is the **AES128**. Fourth option is the selection of **Authentication Algorithm** which can be either **SHA1** or **MD5.** This is the hash algorithm that will be used to authenticate packet data in the IPsec tunnel. The default selection is the **SHA1**. Finally, the last option is the **SA Life Time** for phase 2 which must be set in unit of seconds. The range of this setting can be from 180 to 86400 seconds. The default **SA Life Time** is 3,600 seconds.

The final part of the **IPsec Settings** is the **Dead Peer Detection Settings.** Dead peer detection (DPD) is a mechanism that XMT59XX use to verify the existence of a remote Internet Key Exchange (IKE) gateway or the peer device of XMT59XX. To detect the peer device, XMT59XX will sent encrypted IKE Phase 1 notification payloads (or hello message) to its peer device and wait for DPD acknowledgement from the peer device. If XMT59XX does not receive an acknowledge message during a specific time interval (**DPD timeout**), it will consider that the peer device is dead. Then, XMT59XX will remove the Phase 1 Security Association and all Phase 2 Security Association of that dead peer device. Under the **Dead Peer Detection Settings**, you will have to choose the **DPD Action** that the XMT59XX will perform if it found that the peer device is dead. You can choose either **Hold** to still hold the security association for the peer device and wait for the peer device to return or **Restart** to restart the security association process again. The **DPD Interval** is the period of time for sending the hello message to the peer device or the interval that XMT59XX will repeatly check the endpoint with keep-alive message. The **DPD interval** can be ranged from 1 to 65535 seconds. The default value for **DPD Interval** is 30 seconds. The **DPD Timeout** will be the time that XMT59XX declares the peer device dead if it did not receive any reply or traffic from the peer device. If the keep-alive check fails before this time period expires, the XMT59XX will take the PDP action. The **DPD Timeout** value range from 1 to 65535 seconds. The default value of **DPD Timeout** is 120 seconds. Description of each parameters in the IPsec Tunnels web page is summarized in Table 4.9

Table 4.9 Description of Parameters in IPsec Tunnels Web Page

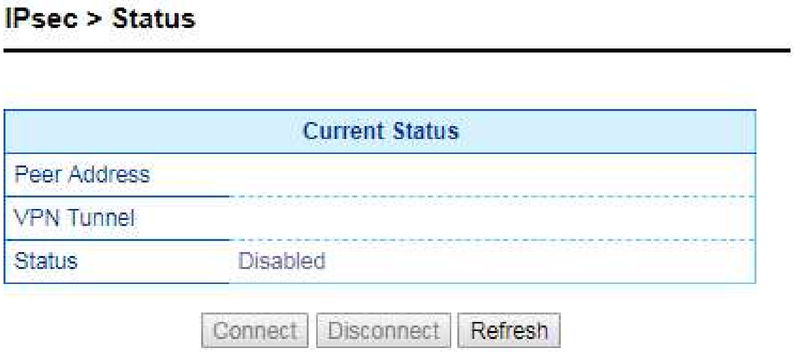
Field Name	Description	Default Value
General Settings		
IPsec	Enable the IPsec Tunnel	Disable
NAT Traversal	Enable the NAT Traversal mechanism	Enable
Peer Address	IP address of the remote device which can be dynamic (any address) or static (fixed address)	Dynamic
Remote Subnet	Remote subnet can be either None (Host only) or Network (IP and Netmask)	None (Host Only)
Local Subnet	Local subnet can be either None (Host Only) or Network (IP and Netmask)	None (Host Only)
Connection type	Tunnel mode or Transport mode	Tunnel

Field Name		Description	Default Value
Authentication Settings			
Method		Pre-Shared Key	secrets
IKE Settings			
Phase 1 SA	**Mode**	Choose how IKE negotiation is performed between Main Mode and Aggressive Mode	Main Mode
	DH Group	Diffie-Hellman groups, determine the strength of the key used in the key exchange process: DH Group 2 (1024-bit) or DH Group 5 (1536-bit)	Group 2 (1024-bit)
	Encryption Algorithm	Encryption algorithm used in the key exchange process: Either 3DES or AES	AES128
	Authentication Algorithm	Hash algorithm used to authenticate packet data in the key exchange process of IKEv1 phase 1: Either MD5 or SHA1	SHA1
	SA Life Time	How long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry. The value can be from 300 to 86,400 seconds.	3600
Phase 2 SA	**Protocol**	Choose how IP packet will be encrypted and verify: either Encapsulate Security Payload (ESP) or IP Authentication Header (AH)	ESP
	Perfect Forward Secrecy	Diffie-Hellman groups for Perfect Forward Secrecy of keys, determine the strength of the key used in the key exchange process: DH Group 2 (1024-bit) or DH Group 5 (1536-bit)	Group 2 (1024-bit)
	Encryption Algorithm	Select which key size and encryption algorithm will be used in IPsec tunnel: either 3DES or AES128	AES128
	Authentication Algorithm	Section of hash algorithm to be used to authenticate packet data in the IPsec tunnel: either MD5 or SHA1	SHA1
	SA Life Time	Value that represents the lifetime of the IKE key which is dedicated in Phase 2 between both end host or network. The available setting ranges is from 180 to 86,400 seconds.	28800
Dead Peer Detection Settings			
DPD Action		Select either Hold or Restart the tunnel's security association for the peer. Note that Hold is suitable for a statistically defined tunnel.	Hold
DPD Interval		Duration of time for sending hello message to the peer device: value from 1 to 65535 seconds.	30 seconds
DPD Timeout		Duration of time to declare that the peer is dead: value from 1 to 65535 seconds.	120 seconds

After finishing the **IPsec settings** configuration, please click the **Save** button to save all changes that have been made. If you would like to discard any setting, please click the **Cancel** button.

4.15.2 *IPsec Status*

On this web page, you can check the status of your IPsec connection between XMT59XX and its peer device in different connection types and modes**.** The first information is the **Peer Address** which is the IP address of the other device that is connected to XMT59XX**.** The second information is the **VPN Tunnel**'s status. The third information is the **Status** of the IPsec connection which can be **Disabled**, **Listening**, or **Connected.** shows the **IPsec Status** web page under the **IPsec Settings** menu. There are three buttons at the end of the web page which are **Connect**, **Disconnect**, and **Refresh.** The **Connect** and **Disconnect** buttons allow you to establish or tear down the IPsec connection**.** The **Refresh** button enable you to check the latest status of the connection**.**



IPsec > Status

Current Status	
Peer Address	
VPN Tunnel	
Status	Disabled

Figure 4.67 IPsec Status Web Page

4.15.3 *Examples of IPsec Settings*

The following subsections provide examples of **IPsec settings**. However, each example will be focused only on the **General Settings** part. The other parts of the **IPsec Settings** can be configured according to the user's preference. Please consult previous section on the details of **Authentication Settings**, **IKE Settings**, and **Dead Peer Detection Settings**. <u>**Note**</u> that the network-to-network (or subnet-to-subnet) connections are now supported in new firmware of XMT59XX.

4.15.3.1 Host-to-Host Connections

Two scenarios can be configured for host-to-host connections: with static peer and with dynamic peer. A host-to- host topology for both scenarios is illustrated in Figure 4.68. Please follow the steps provided next for each scenario to set the **General Settings**.

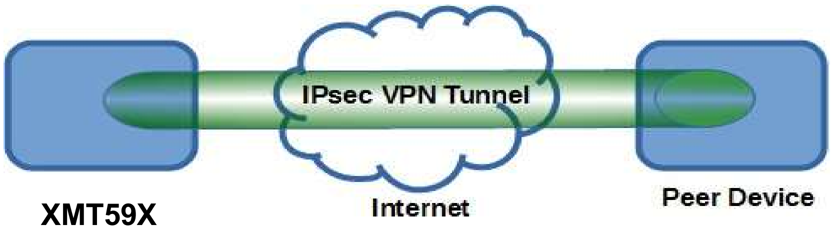


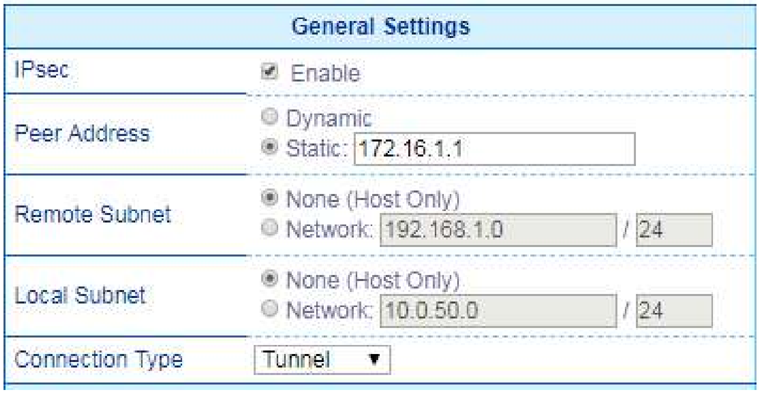
Figure 4.68 IPsec VPN Tunnel with Host-to-Host Topology

Scenario: host-to-host with static peer as shown in Figure 4.69

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.

<u>Note:</u> When peer address is entered as the static address, the XMT59XX acts as an **initiator** which takes the initiative and establishes a connection. XMT59XX also acts as a **responder** and passively accepts the connection initiated by the remote gateway.

- Select the radio button for **None (Host Only)** in the **Remote Subnet** field.
- Since this VPN connection is established on two hosts, the **Connection Type** option can be either **Transport** or **Tunnel**.



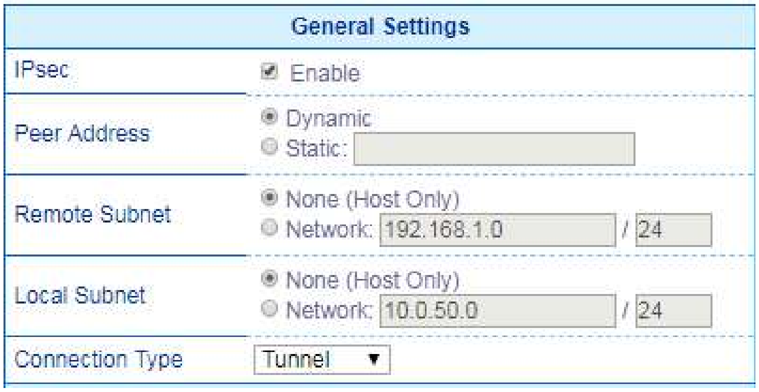
General Settings

IPsec	☑ Enable
Peer Address	○ Dynamic ● Static: 172.16.1.1
Remote Subnet	● None (Host Only) ○ Network: 192.168.1.0 / 24
Local Subnet	● None (Host Only) ○ Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 4.69 General Settings for Host-to-Host with Static Peer

Scenario: host-to-host with dynamic peer as shown in Figure 4.70

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  <u>Note:</u> When VPN connects to a peer with dynamic IP address, the XMT59XX acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- The remaining settings are the same as the host-to-host with static peer scenario described above.



General Settings

IPsec	☑ Enable
Peer Address	● Dynamic ○ Static:
Remote Subnet	● None (Host Only) ○ Network: 192.168.1.0 / 24
Local Subnet	● None (Host Only) ○ Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 4.70 General Settings for Host-to-Host with Dynamic Peer

4.15.3.2 Host-to-Network Connections

Two scenarios can also be configured for host-to-network (or host-to-subnet or host-to-site) connections: with static peer and with dynamic peer. Note that the XMT59XX is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in Figure 4.71. Please follow the steps provided next for each scenario to set the **General Settings**.

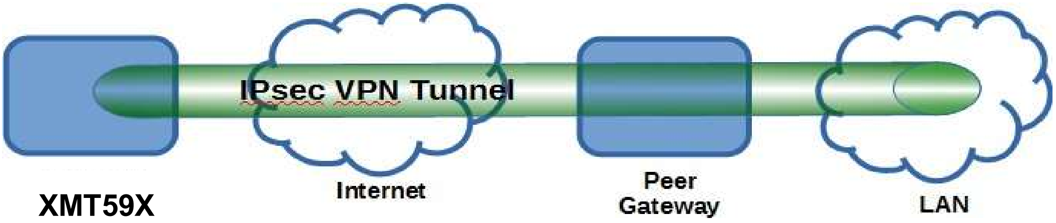
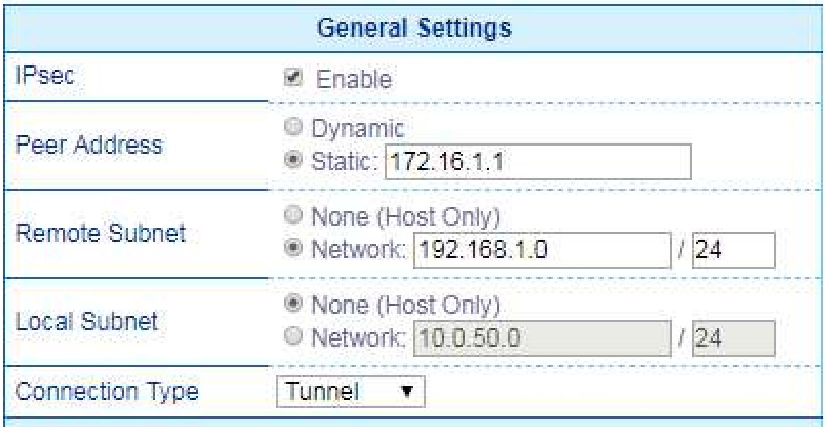


Figure 4.71 IPsec VPN Tunnel with Host-to-Network Topology

Scenario: host-to-network with static peer as shown in Figure 4.72

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  <u>**Note:**</u> When peer address is entered as a static address, XMT59XX is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. XMT59XX also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.



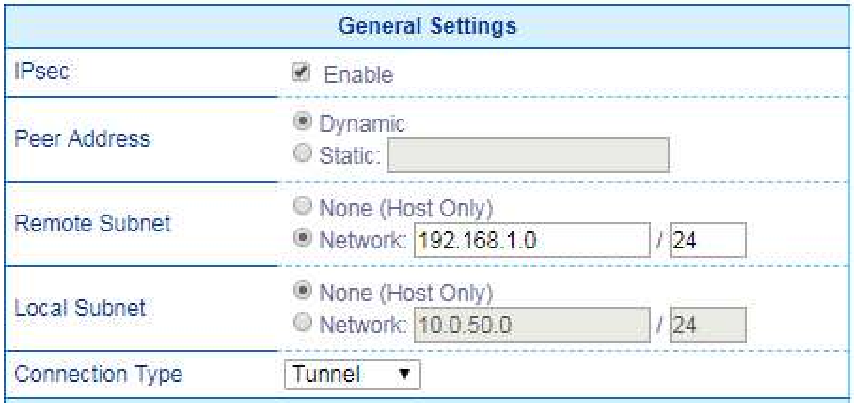
General Settings

IPsec	☑ Enable
Peer Address	○ Dynamic ● Static: 172.16.1.1
Remote Subnet	○ None (Host Only) ● Network: 192.168.1.0 / 24
Local Subnet	● None (Host Only) ○ Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 4.72 General Settings for Host-to-Network with Static Peer

Scenario: host-to-network with dynamic peer as shown in Figure 4.73

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  <u>**Note:**</u> When VPN connection is set to a peer with dynamic IP address, XMT59XX will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.



General Settings	
IPsec	☑ Enable
Peer Address	● Dynamic ○ Static:
Remote Subnet	○ None (Host Only) ● Network: 192.168.1.0 / 24
Local Subnet	● None (Host Only) ○ Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 4.73 General Settings for Host-to-Network with Dynamic Peer

4.15.3.3 Network-to-Network (Subnet-to-Subnet) Connections

Two scenarios can also be configured for network-to-network (or subnet-to-subnet) connections: with static peer or with dynamic peer. A VPN tunnel will be created between two separate private sub-networks. Note that the XMT59XX is the gateway to a local network in these scenarios. A network-to-network topology for both scenarios is illustrated in Figure 4.74. Please follow the steps provided next for each scenario to set the **General Settings**.

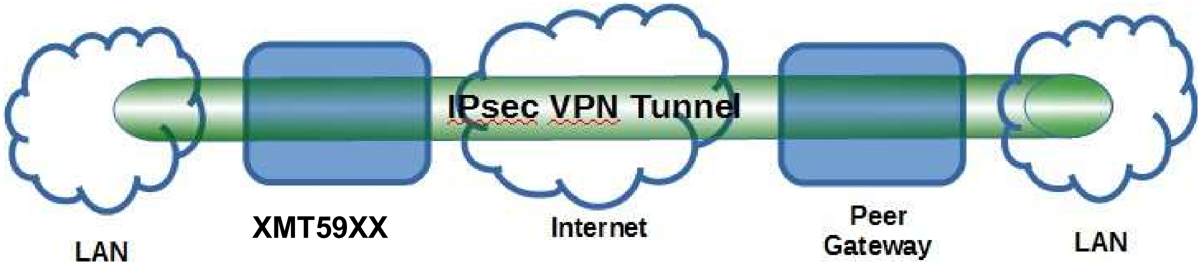
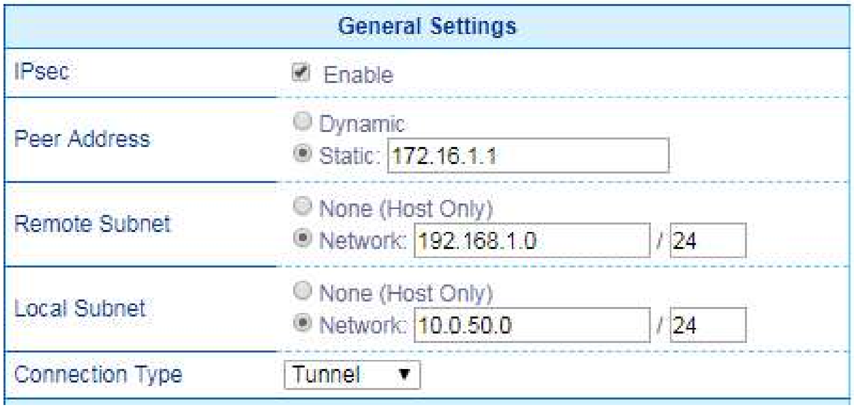


Figure 4.74 IPsec VPN Tunnel with Network-to-Network Topology

Scenario: network-to-network with static peer as shown in Figure 4.75

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  <u>**Note:**</u> When peer address is entered as a static address, XMT59XX is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. XMT59XX also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in "address prefix length" or behind the "/" symbol.
- Set the network IPv4 address in the **Local Subnet** with the number of bits for subnetmask in "address prefix length" or behind the "/" symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.



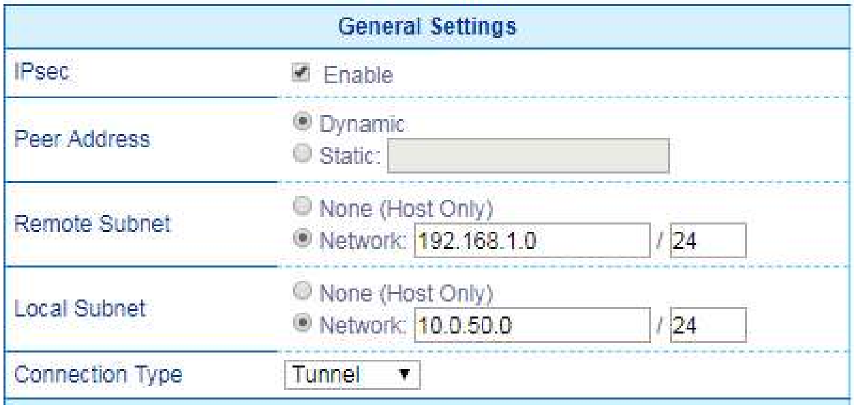
General Settings

IPsec	☑ Enable
Peer Address	○ Dynamic ● Static: 172.16.1.1
Remote Subnet	○ None (Host Only) ● Network: 192.168.1.0 / 24
Local Subnet	○ None (Host Only) ● Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 4.75 General Settings for Network-to-Network with Static Peer

Scenario: network-to-network with dynamic peer as shown in Figure 4.76

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  <u>Note:</u> When VPN connection is set to a peer with dynamic IP address, XMT59XX will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Set the network IPv4 address in the **Local Subnet** with the number of bits for subnetmask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.



General Settings

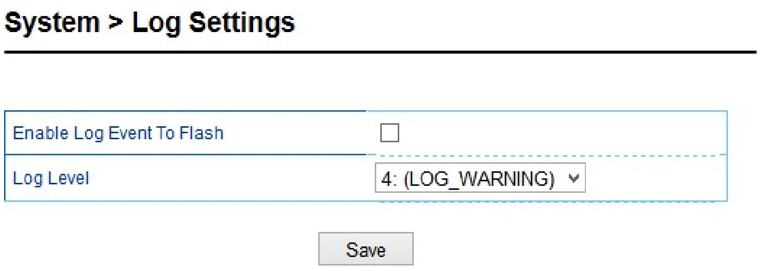
IPsec	☑ Enable
Peer Address	● Dynamic ○ Static:
Remote Subnet	○ None (Host Only) ● Network: 192.168.1.0 / 24
Local Subnet	○ None (Host Only) ● Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 4.76 General Settings for Network-to-Network with Dynamic Peer

4.16 *System*

4.16.1 *Log Settings*

This section allows the user to change the way to report the Log. The user can save his Log Event to the flash memory of the Modbus Gateway by checking the **Enable Log Event to Flash** box. To specify the contents of the Log, select different **Log Level** by changing the pull-down menu of the **Log Level**. There are two log levels available on the menu: **Level 3: (LOG_ERR)** and **Level 4: (LOG_WARNING)**. Figure 4.77 shows a selection of **Log Level 4** which will keep **LOG_WARNING**.



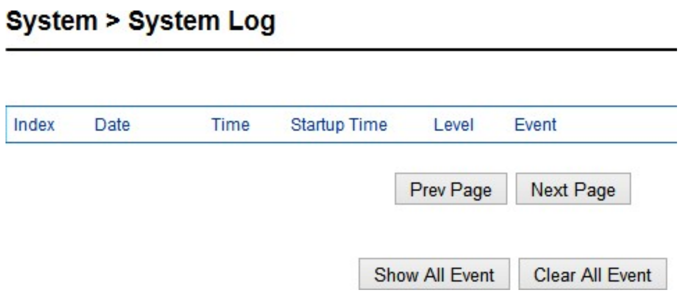
System > Log Settings

Enable Log Event To Flash	□
Log Level	4: (LOG_WARNING)

Figure 4.77 Log Settings Web Page

4.16.2 *System Log*

This section lists current system events aside its properties (**Date, Time, Startup Time, Level, and Event**). Figure 4.78 shows an empty **System Log** page. The user can navigate through the system log by using **Last Page** or **Next Page** buttons. The user will have the option to show all events by clicking the **Show All Event** button and the option to clear them all by clicking on **Clear All Event** button.



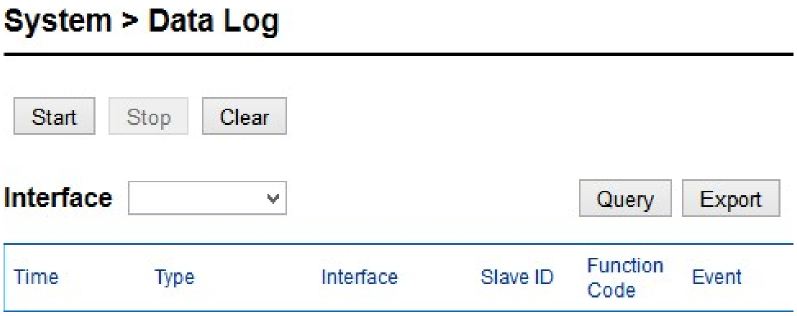
System > System Log

Index	Date	Time	Startup Time	Level	Event

Figure 4.78 System Log Web Page

4.16.3 *Data Log*

The log of Modbus's exchanged messages will be shown in the **Data Log** section and listed in Figure 4.79. This can be very useful for debugging and testing. The user can filter the data based on the **Interface** by using the drop-down box. All available interfaces will be listed in the box such as COM1, COM2, COM3, COM4, and TCP_Link*XX*. Then click on the **Query** button to list the data log based on the chosen interface. Traffic analysis in the system can be done here as well. Click the **Start** button to enable continuous data log collection or click **Stop** to end it. All data log can be cleared by clicking the **Clear** button. The user will be able to browse through the list of message by clicking on the **Last Page** or the **Next Page** buttons at the bottom of the log table. Finally, if the user would like to save the data log to a file on the local PC, please click on the **Export** button.



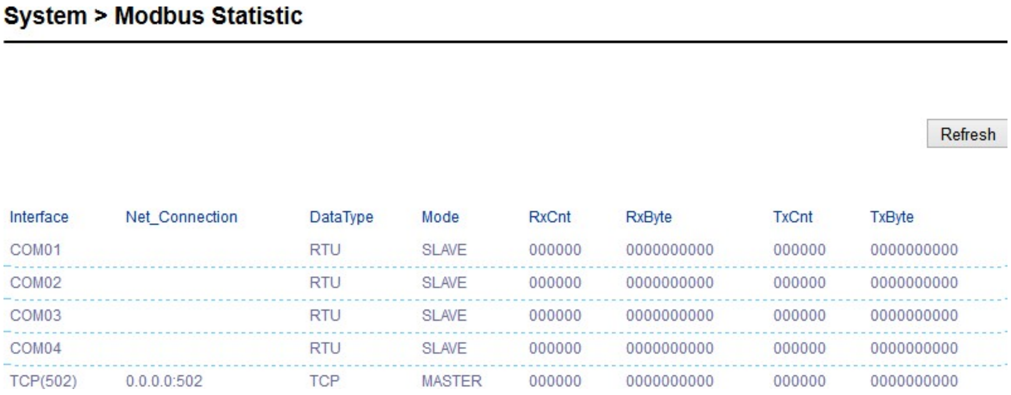
System > Data Log

Time	Type	Interface	Slave ID	Function Code	Event

Figure 4.79 Data Log Web Page

4.16.4 *Modbus Statistic*

Modbus's interface statistics are reported in this section as shown in Figure 4.80. For each interface, there is a **Net_Connection** or socket which is an IP address bundled with its port number (only for TCP and VCOM interfaces), a **DataType** of the interface (**ASCII**, **RTU**, or **TCP**), a **Mode** of the Interface (either **MASTER** or **SLAVE**), the count of received messages (**RxCnt**), the received bytes (**RxByte**), the count of transmitted message (**TxCnt**), and the transmitted bytes (**TxByte**). Click on the **Refresh** button to obtain the latest statistics of the Modbus's interfaces.



System > Modbus Statistic

Interface	Net_Connection	DataType	Mode	RxCnt	RxByte	TxCnt	TxByte
COM01		RTU	SLAVE	000000	0000000000	000000	0000000000
COM02		RTU	SLAVE	000000	0000000000	000000	0000000000
COM03		RTU	SLAVE	000000	0000000000	000000	0000000000
COM04		RTU	SLAVE	000000	0000000000	000000	0000000000
TCP(502)	0.0.0.0:502	TCP	MASTER	000000	0000000000	000000	0000000000

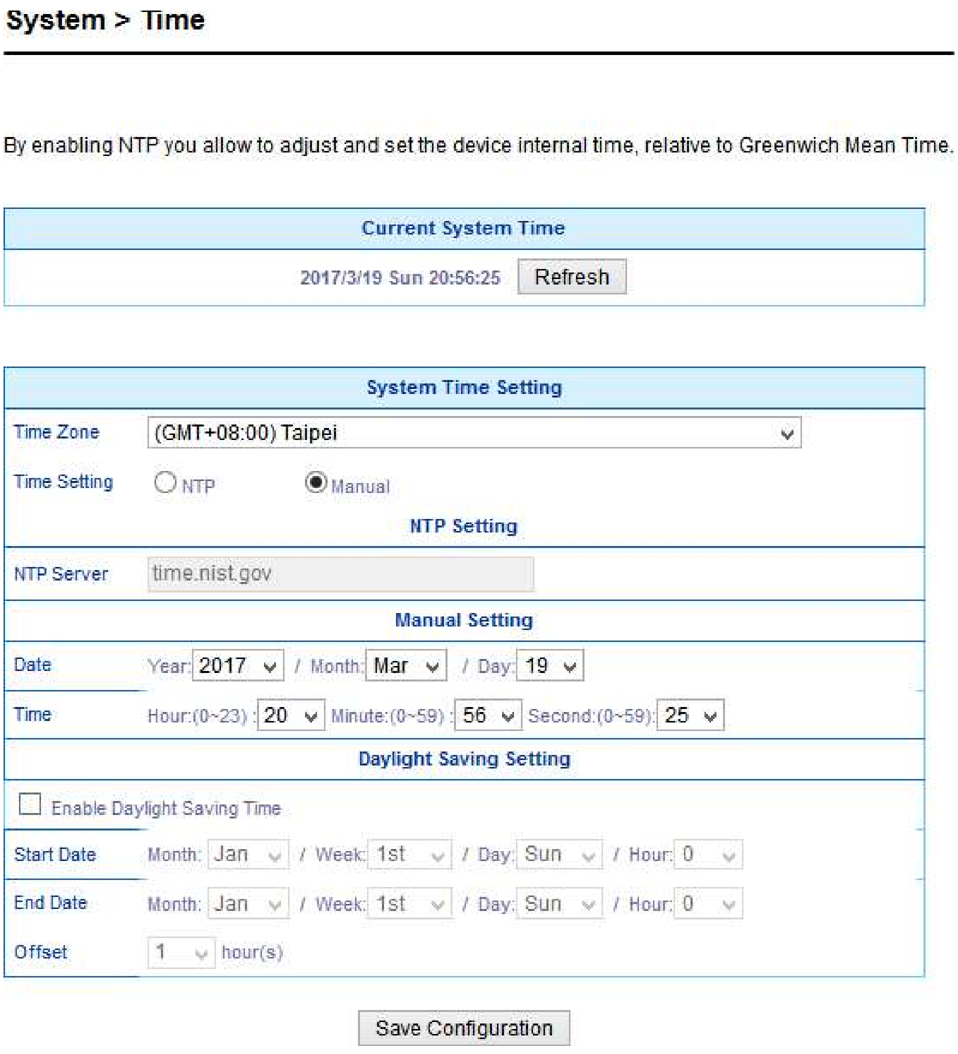
Figure 4.80 Modbus Statistics Web Page

4.16.5 *Time*

Date and time can be set manually or through **N**etwork **T**ime **P**rotocol (NTP) to automatically synchronize date and time of the Modbus Gateway with a **Time Server.** Figure 4.81 shows the **Time** setting page. The user can obtain the **Current System Time** by clicking on the **Refresh** button. Under the **System Time Setting** box, the user can set the **Time Zone** by selecting the proper time zone from the pull-down menu. Then, in order to choose the options of time setting, select either **NTP** or **Manual**. For auto-synchronization, check the radio button in front of **NTP** option. Then, proceed to fill in the IP address or hostname of the preferred time server such as time.nist.gov which is the default setting. If a hostname is entered, the DNS server should be configured properly following the procedure explained in Section o. Other options will be disabled if the **NTP** option is selected.

If the **Manual** option is selected, select the current **Date (Year, Month, Day)** and **Time (Hour, Minute, and Second)** from their corresponding pull-down menus under the **Manual Setting** box. In certain region, the daylight time saving is practiced. In order to enable it, check the **Enable Daylight Saving Time** checkbox and specify the **Start Date**, **End Date**, and **Offset** in the fields under **Daylight Save Setting** box as shown in the greyed out area of Figure 4.81.

After Time Setting is complete, click **Save Configuration** to save all changes that have been done. A **Save Successful** message will show up with a hyperlink to **restart** the device as shown in **錯誤! 找不到參照來源。** Click the **restart** hyperlink to apply the changes**.** Then, a message indicating **System Restarting** status with a counting down number will show up as shown in Figure 4.88**.** After a successful device**'**s restart, the web browser will be redirected to the Overview page as shown in Figure 4.8**.**



System > Time

By enabling NTP you allow to adjust and set the device internal time, relative to Greenwich Mean Time.

Current System Time

2017/3/19 Sun 20:56:25 Refresh

System Time Setting

Time Zone: (GMT+08:00) Taipei

Time Setting: ○ NTP ● Manual

NTP Setting

NTP Server: time.nist.gov

Manual Setting

Date: Year: 2017 / Month: Mar / Day: 19

Time: Hour:(0~23) : 20 Minute:(0~59) : 56 Second:(0~59): 25

Daylight Saving Setting

□ Enable Daylight Saving Time

Start Date: Month: Jan / Week: 1st / Day: Sun / Hour: 0

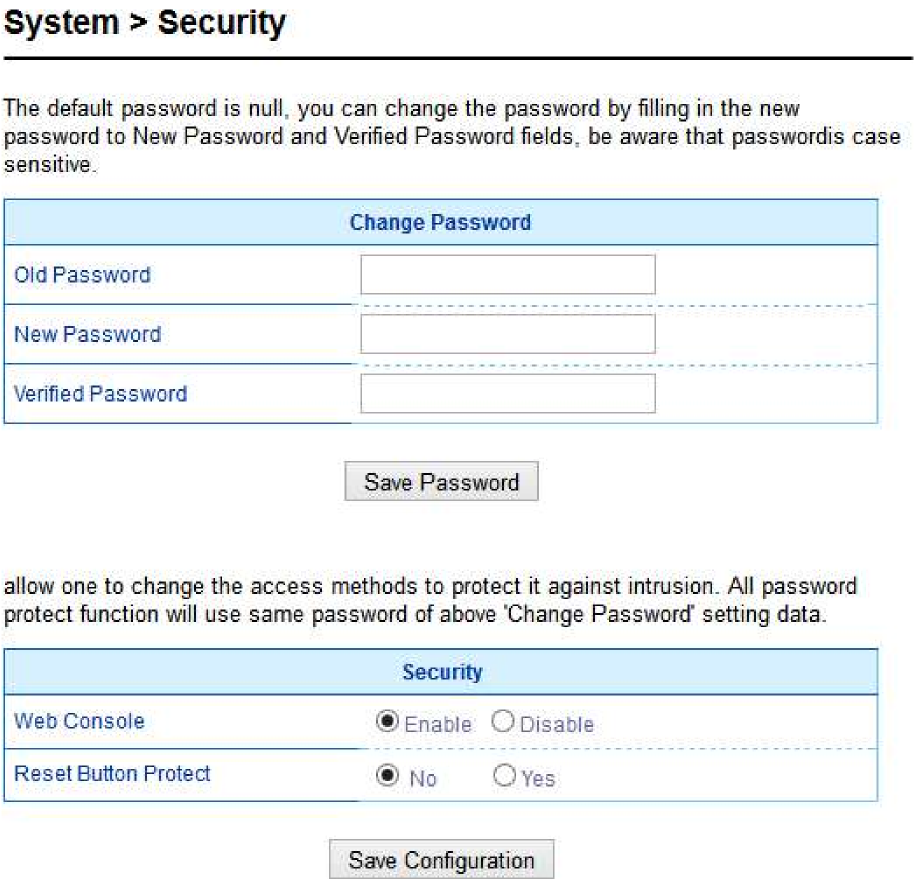
End Date: Month: Jan / Week: 1st / Day: Sun / Hour: 0

Offset: 1 hour(s)

Figure 4.81 Time Web Page

4.16.6 *Security*

The default security setting for the password is a standard password (default). To change security, enter the Security web page as shown in Figure 4.82, enter a password in the **Change Password** box. The user should enter the **Old Password** (enter nothing in case of a null password), the **New Password**, and the **Verified Password** (same as the New Password). The password is case sensitive and limited to a maximum of 8 characters. After entering all required fields, click **Save Password** button to save the change. After the **Save Successfully** message showed up, the user will be prompted with a pop-up window to enter the **User name** and the **New Password** again for verification, as shown in Figure 4.83.



System > Security

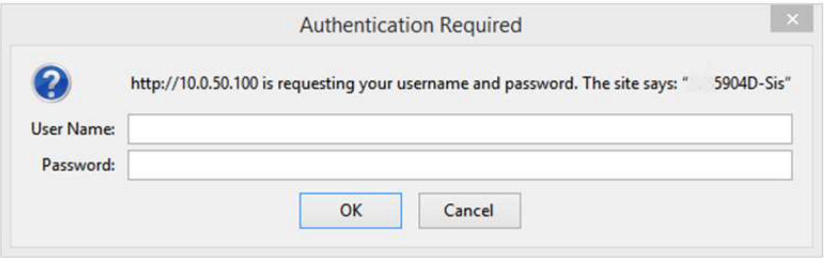
The default password is null, you can change the password by filling in the new password to New Password and Verified Password fields, be aware that passwordis case sensitive.

Change Password	
Old Password	
New Password	
Verified Password	

allow one to change the access methods to protect it against intrusion. All password protect function will use same password of above 'Change Password' setting data.

Security	
Web Console	● Enable ○ Disable
Reset Button Protect	● No ○ Yes

Figure 4.82 Security Web Page



Authentication Required

http://10.0.50.100 is requesting your username and password. The site says: " 5904D-Sis"

User Name:

Password:

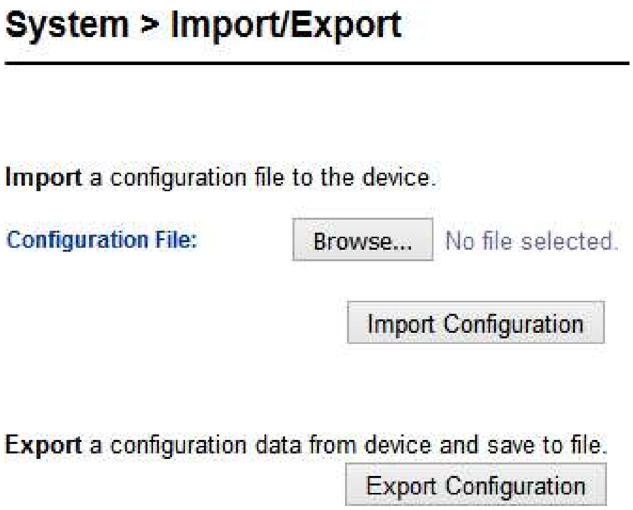
Figure 4.83 Authentication Required after a Password Change

The user can limit how the Modbus Gateway is accessed and controlled by changing the settings under the **Security** box in Figure 4.82. All password-protected features will use the same password whose setting is described in the previous paragraph. The user can enable or disable **Web Console** by clicking on the corresponding radio button. Additionally, the user can protect how the user accesses the device with a **Reset Button Protect** option by checking on either **No** or **Yes** radio buttons.

After Security Settings are set, click **Save Configuration** to save all changes that have been made. A **Save Successful** message will appear with a hyperlink asking to **restart** the device as shown inFigure 4.17**.** Please click the **restart** hyperlink to apply the changes**.** Then, a message indicating **System Restarting** status with a countdown will show up**.** After a successful restart, the web browser will be redirected to the Overview page as shown in Figure 4.6**.**

4.16.7 *Import/Export*

Once all configurations are set and the device is working properly, the user may want to backup **(Export)** the configuration to a file. A backup configuration file can be used when a new firmware is uploaded and the device is reset to a factory default settings, or simply to prevent accidental loading of incompatible old settings. The backup file could also be used to efficiently deploy multiple Modbus Gateways of similar settings by restoring the settings to the devices by **importing** the corresponding file. Figure 4.84 depicts the Import/Export web page.



System > Import/Export

Import a configuration file to the device.

Configuration File: No file selected.

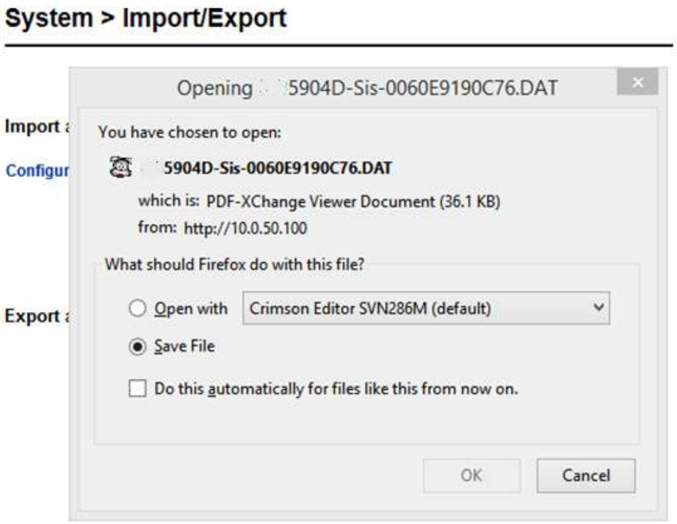
Export a configuration data from device and save to file.

Figure 4.84 Import/Export Web Page

To import a configuration file from the computer, click on the **Browse…** button. Then, a pop-up window will ask the user to choose a configuration file (with .DAT extension). After selection, click **Open button** as shown in Fig.3-46. Then, click on the **Import Configuration** button to start the importing process.

After importing is complete, the system will show a **Save Successful** message with a hyperlink to **restart** the device**.** Click the **restart** hyperlink to apply the changes**.** Then, a message indicating **System Restarting** status with a countdown will show up**.** After a successful device**'**s restart, the web browser will be redirected to the Overview page as shown in Figure 4.8**.**

In order to export the current configuration of the Modbus Gateway to a file for backup purposes, click the **Export Configuration** button as shown in Figure 4.84. Then, a pop-up window will ask to either **Open** the configuration file for viewing with a default application such as Notepad or to simply **Save** the configuration file to the preferred name and destination path as shown in Figure 4.86.



System > Import/Export

Import a

Configur

Export a

Opening 5904D-Sis-0060E9190C76.DAT

You have chosen to open:

5904D-Sis-0060E9190C76.DAT

which is: PDF-XChange Viewer Document (36.1 KB)

from: http://10.0.50.100

What should Firefox do with this file?

○ Open with Crimson Editor SVN286M (default)

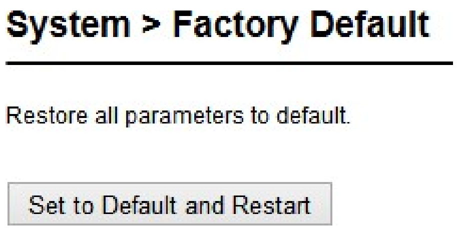
● Save File

□ Do this automatically for files like this from now on.

Figure 4.86 Export Configuration File from Modbus Gateway

4.16.8 *Factory Default*

A return to **Factory Default** function is available in Agatel's XMT59XX Series. To restore all parameters of the Modbus Gateway to the original factory default setting, click **Set to Default and Restart** button as shown in Figure 4.87. After a short moment, a message indicating **System Restarting** status with a countdown number will show up**.** After a successful device**'**s restart, the web browser will be redirected to the Overview page as shown in Figure 4.8**.**



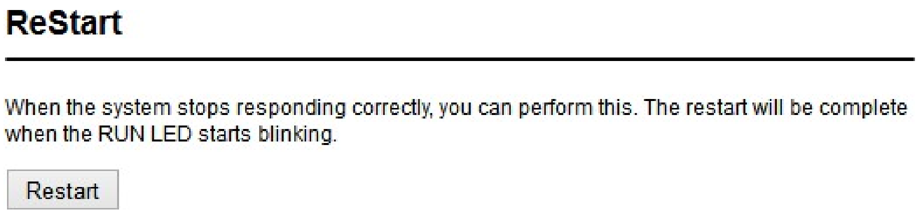
System > Factory Default

Restore all parameters to default.

Figure 4.87 Factory Default Web Page

4.17 *Restart*

For some unexpected circumstances, the Modbus Gateway system may stop responding correctly**.** The user has the option to restart the device by clicking the **Restart** button as shown in Figure 4.88. The device's RUN LED will start blinking when the restart process is completed. Then, a message indicating **System Restarting** status with a countdown will show up**.** After a successful device**'**s restart, the web browser will be redirected to the Overview page as shown in Figure 4.8**.**



ReStart

When the system stops responding correctly, you can perform this. The restart will be complete when the RUN LED starts blinking.

Figure 4.88 Restart Web Page

5 Applications and Examples

On the device two different Slave ID mapping definitions are available, which represent the alias mode and the offset mode. Both Modbus ID definitions can be used to route the request command (from the Master) to the Slave node. Please see details of Slave ID setting mode in Section 4.8.6.

5.1 *Using ID offset range mapping*

If the Slave ID is continuous as shown in Figure 5.1, it is recommended to use the Offset mode in your configuration setting of ID mapping as shown in Figure 5.2.

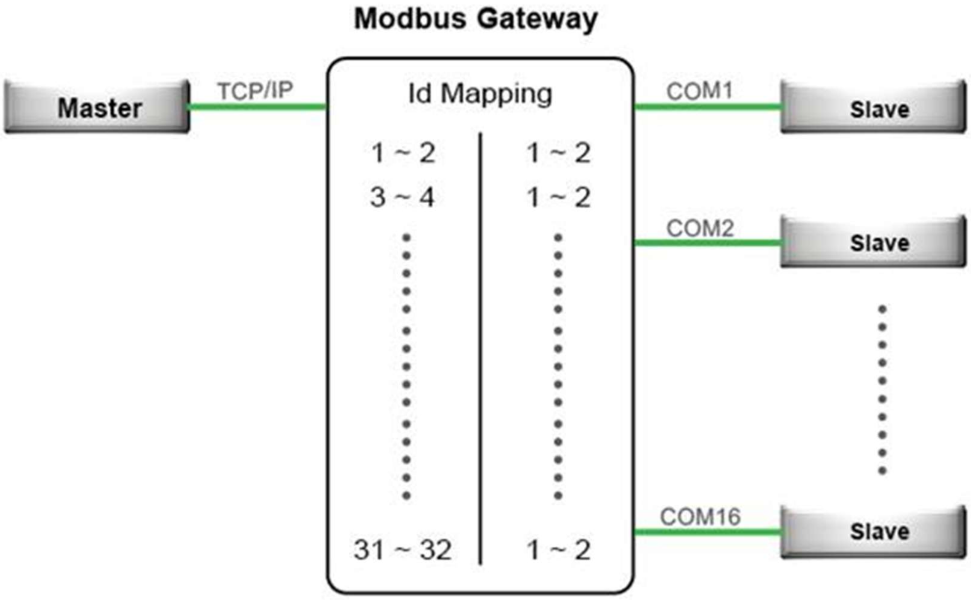
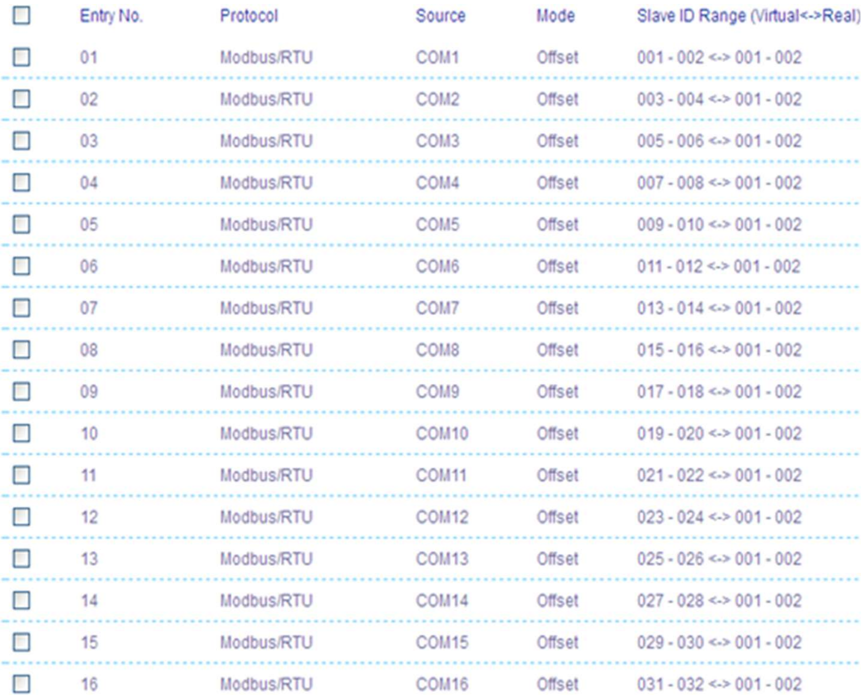


Figure 5.1 Continuous Slave ID Mapping Example



□	Entry No.	Protocol	Source	Mode	Slave ID Range (Virtual<->Real)
□	01	Modbus/RTU	COM1	Offset	001 - 002 <-> 001 - 002
□	02	Modbus/RTU	COM2	Offset	003 - 004 <-> 001 - 002
□	03	Modbus/RTU	COM3	Offset	005 - 006 <-> 001 - 002
□	04	Modbus/RTU	COM4	Offset	007 - 008 <-> 001 - 002
□	05	Modbus/RTU	COM5	Offset	009 - 010 <-> 001 - 002
□	06	Modbus/RTU	COM6	Offset	011 - 012 <-> 001 - 002
□	07	Modbus/RTU	COM7	Offset	013 - 014 <-> 001 - 002
□	08	Modbus/RTU	COM8	Offset	015 - 016 <-> 001 - 002
□	09	Modbus/RTU	COM9	Offset	017 - 018 <-> 001 - 002
□	10	Modbus/RTU	COM10	Offset	019 - 020 <-> 001 - 002
□	11	Modbus/RTU	COM11	Offset	021 - 022 <-> 001 - 002
□	12	Modbus/RTU	COM12	Offset	023 - 024 <-> 001 - 002
□	13	Modbus/RTU	COM13	Offset	025 - 026 <-> 001 - 002
□	14	Modbus/RTU	COM14	Offset	027 - 028 <-> 001 - 002
□	15	Modbus/RTU	COM15	Offset	029 - 030 <-> 001 - 002
□	16	Modbus/RTU	COM16	Offset	031 - 032 <-> 001 - 002

Figure 5.2 Entries of Slave ID Mapping in Offset Mode

6 Specifications

6.1 *Hardware*

Table 6.1 Hardware Specification

System	
CPU	32-bit ARM Based TI CPU AM3354 800MHz (except XMT5908A/XMT5916A use AM3352 1GHz)
Flash Memory	32MB
RAM	XMT5901 DDR2 128MB XMT5901B DDR2 256MB XMT5904D DDR3 256MB XMT5908A/16A/XMT5908/16 DDR3 256MB
EEPROM	8 KB
Reset	Built-in Recessed Key (Restore to Factory Defaults)
Watchdog	Hardware built-in
Network	
Ethernet Interface	IEEE 802.3 10BaseT IEEE 802.3u 100BaseT(X) IEEE 802.3ac 1000BaseT(X) – SFP version of XMT5904D only IEEE 802.3af (PoE PD) –selected XMT5901 and XMT5904D versions can be powered through PoE Connection: SFP or RJ45
Protocol	ICMP TCP UDP IPv4 HTTP Syslog DNS DHCP Client SNMPv1,v2c,v3 Modbus TCP/ASCII/RT U SMTP NTP ARP Telnet RFC221 7
Serial	
Serial Interface	RS-232/RS-422/RS-485 Software Selectable (Default: RS-232) • The first port available on XMT5901B is RS-232/RS-485 • The second port available on XMT5901B-IO-X is only RS-232 The isolation version (-SiS) on XMT5908/XMT5916/XMT5908A/ XMT5916A supports only RS-422/ RS-485
Serial Connector	Connector Type • XMT5916 -16 Serial Ports (RJ45) • XMT5908 - 8 Serial Ports (RJ45) • XMT5916A – 16 Serial Ports (TB-5 or DB-9) • XMT5908A – 8 Serial Ports (TB-5 or DB-9) • XMT5904 – 4 Serial Ports (TB-5 or DB-9) • XMT5901 – 1 Serial Port (TB-5 or DB-9) • XMT5901B – 1 Serial Port (TB-14 or DB-9) – includes I/O
Protection	XMT5901/XMT5901B no isolation XMT5904D/ XMT5908A/16A (optional 3V) XMT5908/16 (optional 2.5kV)
Serial Port Communication	Baud-rate: 1200 bps ~ 921600 bps Parity: None, Even, Odd, Mark, or Space Data Bits: 5, 6, 7, 8

	Stop Bits: 1, 2 Software Selectable Flow Control: RTS/CTS (RS-232 only), XON/XOFF, None
LED Indicator	
LED indication	Power x 2 (XMT5901- XMT5901B – XMT5908 – XMT5916 x 1) RUN x 1 ALARM x 1 LAN: • x 2 (all versions except XMT5908A and XMT5916A) • x 6 (XMT5908A and XMT5916A only) COM port: • x 16 (XMT5916 and XMT5916A); • x 8 (XMT5908 and XMT5908A); • x 4 (XMT5904D); • x 1 (XMT5901 and XMT5901B)
Power Requirement & EMC	
Input	XMT5908/ XMT5916 : • Single 100~240 VAC (EU/US versions) • Single 24~48 VDC (DC version) XMT5908A/ XMT5916A • Redundant 100~240 VAC or 100~370 VDC (TB)– HV vers. • Redundant 24~48 VDC- DC version XMT5901/XMT5901B : Single 9~48 VDC XMT5904D : Redundant 9~48 VDC
Consumption	Max.17.5 W (XMT5908 /XMT5916) Max. 6W (XMT5901) Max. 7.8W(XMT5904D) Max. 17.5W(XMT5908A/XMT5916A) Max. 7.2W(XMT5901B)
EMC	FCC Part 15, Subpart B, Class A EN 55032, Class B, EN 61000-6-2, Class B EN 61000-3-2, EN 61000-3-3 EN 55024, EN 61000-6-4 IEC 61850-3 / IEEE 1613 (XMT5908A and XMT5916A only)
Mechanical	
Dimensions (W x H x D, mm)	XMT5901: 32 mm x 110 mm x 90 mm (1.26 x 4.33 x 3.54 in) XMT5901B: 32 mm x 122mm x 92 mm (1.26 x 4.8 x 3.62 in) XMT5904D: 55 mm x 145 mm x 113mm (2.17 x 5.17 x 4.45 in) XMT5908: 436 mm x 43.5 mm x 200 mm (17.17 x 1.71 x 7.87 in) XMT5916: 436 mm x 43.5 mm x 200 mm (17.17 x 1.71 x 7.87 in) XMT5908A: 440.6mm x 44 mm x 309 mm (17.35 x 1.73 x 12.17 in) XMT5916A: 440.6mm x 44 mm x 309 mm (17.35 x 1.73 x 12.17 in)
Enclosure	IP30 protection, metal housing
Environmental	
Temperature	Operations -40°C ~ 85°C (-40°F ~ 185°F) (except XMT5901B -40°C ~ 70°C and XMT5908/XMT5916 -20°C ~ 70°C)
	Storage -40°C ~ 85°C (-40°F ~ 185°F)
Humidity	5% ~ 95%, 55°C Non-condensing

6.2 *Serial port Pin Assignments*

6.2.1 *XMT5901 Pin Assignments*

DB9 to RS-232/RS-485/RS-422 connectors

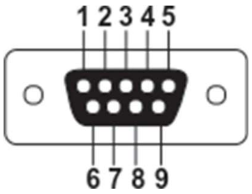


Figure 6.1 DB9 Pin Number

Table 6.2 XMT5901 Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors

Pin#	RS-232 Full Duplex	RS-422 Full Duplex	RS-485 Half Duplex
1	DCD	N/A	N/A
2	RxD	TxD+	N/A
3	TxD	RxD+	Data+
4	DTR	N/A	N/A
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)
6	DSR	N/A	N/A
7	RTS	RxD-	Data-
8	CTS	TxD-	N/A
9	RI	N/A	N/A

5-Pin Terminal Block to RS-485/RS-422 connectors

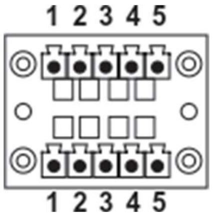


Figure 6.2 Terminal Block (TB-5) Pin Number

Table 6.3 XMT5901 Pin Assignment for 5-Pin Terminal Block to RS-232/RS-422/RS-485 Connectors

Pin#	RS-232	RS-422 4-Wire RS-485	2-W RS-485
1	RxD	TxD+	N/A
2	CTS	TxD-	N/A
3	TxD	RxD+	Data+
4	RTS	RxD-	Data-
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)

6.2.2 *XMT5904D Pin Assignments*

DB9 to RS-232/RS-485/RS-422 connectors

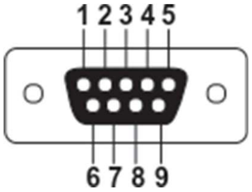


Figure 6.3 DB9 Pin Number

Table 6.4 XMT5904D Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors

Pin#	RS-232 Full Duplex	RS-422 Full Duplex	RS-485 Half Duplex
1	DCD	N/A	N/A
2	RxD	TxD+	Data+
3	TxD	RxD+	N/A
4	DTR	N/A	N/A
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)
6	DSR	N/A	N/A
7	RTS	RxD-	N/A
8	CTS	TxD-	Data-
9	RI	N/A	N/A

5-Pin Terminal Block to RS-485/RS-422 connectors

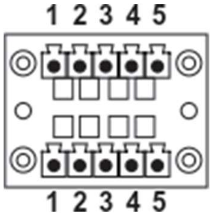


Figure 6.4 Terminal Block (TB-5) Pin Number

Table 6.5 XMT5904D Pin Assignment for 5-Pin Terminal Block to RS-232/RS-422/RS-485 Connectors

Pin#	RS-232	RS-422 4-Wire RS-485	2-W RS-485
1	RxD	TxD+	Data+
2	CTS	TxD-	Data-
3	TxD	RxD+	N/A
4	RTS	RxD-	N/A
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)

6.2.3 *XMT5901B Pin Assignments*

DB9 to RS-232/RS-485/RS-422 connectors

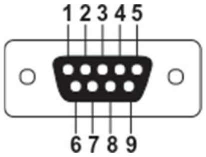


Figure 6.5 DB9 Pin Number

Table 6.6 XMT5901B Pin Assignment for DB9 to RS-232/RS-485 Connector

Pin#	RS-232 Full Duplex	RS-485 Half Duplex
1	DCD	N/A
2	RxD	N/A
3	TxD	Data+
4	DTR	N/A
5	SG (Signal Ground)	SG (Signal Ground)
6	DSR	N/A
7	RTS	Data-
8	CTS	N/A
9	RI	N/A

2 x 7-pin Male Terminal Block for RS-232/485(COM 1),RS-232(COM 2) Relay and DI

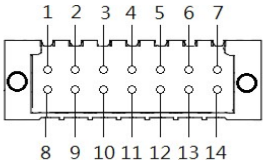


Figure 6.6 2 x 7-pin Male Terminal Block

Table 6.7 XMT5901B 2 x 7-pin Male TB for RS-232/485(COM 1),RS-232(COM 2) Relay and DI pin-assignment

Pin#	DI and Relay	COM1 (RS-232)	COM1 (RS-485)	COM2 (RS-232)
1	DI1	*Dedicated for DI/DO*	*Dedicated for DI/DO*	*Dedicated for DI/DO*
2	DI2	*Dedicated for DI/DO*	*Dedicated for DI/DO*	*Dedicated for DI/DO*
3	Relay 1 -	*Dedicated for DI/DO*	*Dedicated for DI/DO*	*Dedicated for DI/DO*
4	Relay 1+	*Dedicated for DI/DO*	*Dedicated for DI/DO*	*Dedicated for DI/DO*
5	Relay 2 -	*Dedicated for DI/DO*	*Dedicated for DI/DO*	*Dedicated for DI/DO*
6	Relay 2+	*Dedicated for DI/DO*	*Dedicated for DI/DO*	*Dedicated for DI/DO*
7	*Dedicated for COM*	SG (Signal Ground)	SG (Signal Ground)	-
8	*Dedicated for COM*	Rx	-	-
9	*Dedicated for COM*	CTS	-	-
10	*Dedicated for COM*	Tx	Data +	-
11	*Dedicated for COM*	RTS	Data -	-
12	*Dedicated for COM*	-	-	SG (Signal Ground)
13	*Dedicated for COM*	-	-	Rx
14	*Dedicated for COM*	-	-	Tx

6.2.4 *XMT5908A/XMT5916A Pin Assignments*

DB9 to RS-232/RS-485/RS-422 connectors

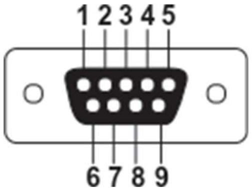


Figure 6.7 DB9 Pin Number

Table 6.8 XMT5908A/16A Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors

Pin#	RS-232	RS-422	RS-485
1	-	-	-
2	RxD	TxD+	Data+
3	TxD	RxD+	-
4	-	-	-
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)
6	-	-	-
7	RTS	RxD-	-
8	CTS	TxD-	Data-
9	-	-	-

5-Pin Terminal Block to RS-232/RS-485/RS-422 connectors

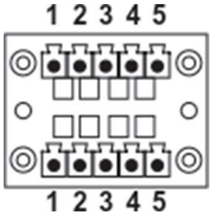


Figure 6.8 Terminal Block (TB-5) Pin Number

Table 6.9 XMT5908A/16A Pin Assignment for 5-Pin Terminal Block to RS-232/RS-422/RS-485 Connectors

Pin#	RS-232	RS-422 4-Wire RS-485	2-W RS-485
1	RxD	TxD+	Data +
2	CTS	TxD-	Data -
3	TxD	RxD+	-
4	RTS	RxD-	-
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)

6.2.5 *XMT5908/XMT5916 Pin Assignments*

RJ45 to RS-232/RS-485/RS-422 connectors

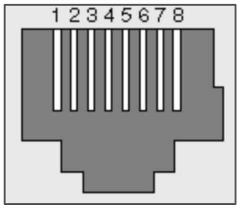


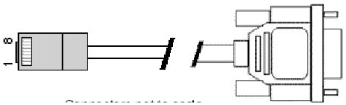
Figure 6.9 XMT5908/XMT5916 Serial port on RJ45 Pin Numbering

Table 6.10 XMT5908/16 Pin Assignment for RJ45 to RS-232/RS422/RS-485 Connectors

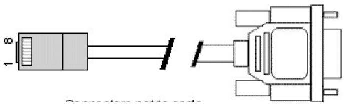
Pin#	RS-232	RS-422	RS-485
1	RTS	-	-
2	DTR	Tx -	-
3	TxD	Tx +	-
4	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)
6	RxD	Rx +	Data +
7	DSR	Rx -	Data -
8	CTS	-	-

RJ45 to RS-232/RS-485/RS-422 accessories provided by AGATEL

- **50891791G - RJ45 TO DB9 CABLE-FEMALE:**

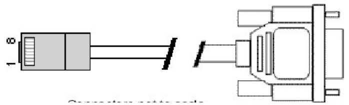
RJ45			Straight Through Fe male DB9	
				
RTS	Pin 1	⇔	Pin 7	RTS
DTR	Pin 2	⇔	Pin 4	DTR
TXD	Pin 3	⇔	Pin 3	TXD
SG	Pin 4	⇔	Pin 5	SG
SG	Pin 5	⇔		
RXD	Pin 6	⇔	Pin 2	RXD
DSR	Pin 7	⇔	Pin 6	DSR
CTS	Pin 8	⇔	Pin 8	CTS

- **50891971G - RJ45 TO DB9 CROSS OVER CABLE-FEMALE:**

RJ45			Cross Over Female DB9	
				
RTS	Pin 1	⇔	Pin 8	CTS
DTR	Pin 2	⇔	Pin 6	DSR
TXD	Pin 3	⇔	Pin 2	RXD
SG	Pin 4	⇔	Pin 5	GND
SG	Pin 5	⇔		

RXD	Pin 6	⇔	Pin 3	TXD
DSR	Pin 7	⇔	Pin 4	DTR
CTS	Pin 8	⇔	Pin 7	RTS

50891781G - RJ45 TO DB9 CABLE-MALE:

RJ45			Straight Through Male DB9	
				
RTS	Pin 1	⇔	Pin 7	RTS
DTR	Pin 2	⇔	Pin 4	DTR
TXD	Pin 3	⇔	Pin 3	TXD
SG	Pin 4	⇔	Pin 5	SG
SG	Pin 5	⇔		
RXD	Pin 6	⇔	Pin 2	RXD
DSR	Pin 7	⇔	Pin 6	DSR
CTS	Pin 8	⇔	Pin 8	CTS

6.3 *LED Indicators*

Table 6.11 Color Interpretation of LED Indicators

Name	Color	Message
PWR (Power)	🟢 (Steady Green)	Power ON
RUN (Ready)	🟢 (Steady On/Off Green)	System is not ready or halt
	✹ (Blinking Green)	AP firmware is running normally
ALM (Alarm)	🔴 (Steady Red)	Alarm is triggered by user defined events
	⚫ (Light Off)	Alarm is not triggered by user defined events
COM	✹ (Blinking Green)	COM port is transmitting data
	⚫ (Light Off)	COM port is not transmitting data
LAN	🟡 (Steady Amber)	Data is transmitting at 10Mbps
	⚫ (Light Off Green)	Ethernet is disconnected
	✹ (Blinking Green)	Data is transmitting at 100Mbps
LAN (On LED Panel)	🟢 (Steady Green)	Ethernet is connected
	⚫ (Light Off Green)	Ethernet is disconnected
	✹ (Blinking Green)	Data is transmitting on this port
SFP (On LED Panel)	🟢 (Steady Green)	SFP port is connected
	⚫ (Light Off Green)	SFP port is disconnected
	✹ (Blinking Green)	Data is transmitting on this port

6.4 *Software*

Table 6.12 Software Tools and Utilities

Software	
Utility	Windows Virtual COM Driver and Linux TTY Driver: Linux 2.4.x, Linux 2.6.x, 3.x
Configuration Tool	■ Web console ■ Serial console ■ SSH console ■ Telnet console ■ **Device Management Utility©**

7 Warranty

Limited Warranty Conditions

Products supplied by Agatel Inc. are covered in this warranty for undesired performance or defects resulting from shipping, or any other event deemed to be the result of Agatel Inc. mishandling. The warranty doesn't cover; however, equipment which has been damaged due to accident, misuse, abuse, such as:

- Use of incorrect power supply, connectors, or maintenance procedures
- Use of accessories not sanctioned by us
- Improper or insufficient ventilation
- Improper or unauthorized repair
- Replacement with unauthorized parts
- Failure to follow our operating Instructions
- Fire, flood, "Act of God", or any other contingencies beyond our control.

RMA and Shipping Reimbursement

- Customers must always obtain an authorized **"RMA" number** from us before shipping the goods to be repaired.
- When in normal use, a sold product shall be replaced with a new one within 3 months upon purchase. The shipping cost from the customer to us will be reimbursed.
- After 3 months and still within the warranty period, it is up to us whether to replace the unit with a new one; normally, as long as a product is under warranty, all parts and labor are free-of-charge to the customers.
- After the warranty period, the customer shall cover the cost for parts and labor.
- Three months after purchase, the shipping cost from the customer to us will not be reimbursed, but the shipping costs from us to the customer will be paid by us.

Limited Liability

Agatel Inc. shall not be held responsible for any consequential losses from using our products.

Warranty

Agatel Inc. provides a 5-year maximum warranty for Modbus Gateway produ