



Getting started with PG59XX Protocol Gateway

Device Setup
Architectural overview
eNode Designer

User Manual

V1.8

November 20th, 2024

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.

- [General Description](#)
- [User Guide](#)

Published by:

ATOP Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Zhubei City, Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137

Fax: +886-3-550-8131

www.atoponline.com

www.atop.com.tw

Important Announcement

The information contained in this document is the property of ATOP technologies, Inc., and is supplied for the sole purpose of operation and maintenance of ATOP Technologies, 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 ATOP Technologies, 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:	Simon Huang
Revision:	1.8
Revision History:	Software updates
Creation Date:	31 August 2016
Last Revision Date:	20 November 2024
Product Reference:	PG59XX Protocol Gateway Family
Document Status:	Released

Table of Contents

1	Introduction	7
1.1	Scope	7
1.2	Overview	7
1.2.1	List of Abbreviations	7
2	Getting Started	8
2.1	Packing List	8
2.2	How to order	9
2.3	First Time Installation	10
2.4	Factory Default Settings	10
3	Configuration and Setup	12
3.1	Configuration of Network Parameters through Device View	12
3.2	Configuration through Web Interface	14
3.3	LCM (Liquid Crystal Matrix) Configuration (PG5916 only)	14
3.4	Automatic IP Assignment configuration with DHCP	17
3.5	Web Overview	17
3.6	Network Configuration	18
3.6.1	Link Aggregation	20
3.6.2	Virtual IP settings	21
3.7	Protocol Gateway	22
3.7.1	Redundancy Settings	22
3.7.2	IEC 61850 IED List - connection statistic	23
3.8	Advanced Settings	23
3.8.1	SNMP Settings	23
3.9	VPN	24
3.9.1	PPTP	25
3.9.2	IPsec	26
3.9.3	Examples of IPsec Settings	34
3.9.4	Host-to-Host Connections	34
3.9.5	Host-to-Network Connections	35
3.9.6	OpenVPN	37
3.9.7	OpenVPN Setting	37
3.9.8	OpenVPN Keys	39
3.9.9	OpenVPN Status	40
3.10	System Setup	42
3.10.1	Time	42
3.10.2	Security	43
3.10.3	Restart	44
4	General Description	45
4.1	Protocol Gateway Overview	45
4.2	Device Client/Master	47
4.3	Device Server/Slave	47
4.4	Example – general settings	48
4.5	Example - Polling process	49
4.6	Example: Command process	51
4.7	eNode Designer Overview	53
5	eNode designer User Guide	54
5.1	Installation	54

5.2	Main Screen	55
5.3	Login.....	55
5.4	User Administration	57
5.4.1	Creating, modifying and removing users.....	57
5.4.2	Defining User Groups.....	58
5.5	Creating a project	60
5.5.1	Project Root.....	60
5.5.2	Adding a Device (a.k.a. Target Platform or CFE)	60
5.5.3	Editing Ethernet Port Properties.....	61
5.5.4	Editing Communication Port Properties	62
5.5.5	Adding an ADH Application to a Communication Port	62
5.6	Data Points.....	64
5.7	Generate and Send Configuration Files.....	65
5.7.1	Setting up the FTP Details	65
5.7.2	Send the Configuration	66
6	eNode designer Reference Guide	68
6.1	Menu Bar Options	68
6.1.1	File.....	68
6.1.2	Settings	68
6.1.3	Help	68
6.2	Tree Menu Options.....	68

Table of Figures

Figure 3-1 - List of Devices on Network in Device Management Utility	12
Figure 3-2 - Pull-down Menu of Configuration and Network	12
Figure 3-3 - Pop-up Window of Network Setting.....	13
Figure 3-4 - Authorization for Changes.....	13
Figure 3-5 - Overview web page of protocol gateway.....	14
Figure 3-6 – Overview Page	17
Figure 3-7 – Network configuration Page, example on PG5900A/08A/16A	19
Figure 3-8 – Save completed Page.....	20
Figure 3-9 – Bonding settings	21
Figure 3-10 – Bonding status	21
Figure 3-11 – Virtual IP settings.....	22
Figure 3-12 – Redundancy settings.....	22
Figure 3-13 – IED connction statistics.....	23
Figure 3-14 – SNMP settings.....	24
Figure 3-15 VPN Scenario of SE/PG/MB 5901B	25
Figure 3-16 PPTP configuration page.....	25
Figure 3-17 PPTP Link Status.....	26
Figure 3-18 An example of Host-to-Host Connection	27
Figure 3-19 Roadwarrior Application using Host-to-Subnet Connection	27
Figure 3-20 Gateway Application using Host-to-Subnet Connection.....	28
Figure 3-21 An example of network application using a subnet-to-subnet connection via the PG59XX and a peer device	28
Figure 3-22 An example of host-network application via the subnet-to-subnet connection	29
Figure 3-23 An example of host-host application via the subnet-to-subnet connection	29
Figure 3-24 IPsec Tunnels Web Page under IPsec Setting Menu	30
Figure 3-25 IPsec VPN Tunnel with Host-to-Host Topology.....	34
Figure 3-26 General Settings for Host-to-Host with Static Peer	35
Figure 3-27 General Settings for Host-to-Host with Dynamic Peer	35
Figure 3-28 IPsec VPN Tunnel with Host-to-Network Topology.....	36
Figure 3-29 General Settings for Host-to-Network with Static Peer	36

Figure 3-30 General Settings for Host-to-Network with Dynamic Peer 37

Figure 3-31 IPSec Link Status 37

Figure 3-32. OpenVPN Setting 38

Figure 3-33 OpenVPN Keys..... 39

Figure 3-34 Certification information 40

Figure 3-35 Certificate Upload 40

Figure 3-36 OpenVPN client status..... 41

Figure 3-37 OpenVPN server status 41

Figure 3-38 – Time settings Page 42

Figure 3-39 – Admin settings Page 43

Figure 3-40 – Entering the User Name and the New Password 44

Figure 3-41 – Web mode settings 44

Figure 3-42 – Restart page 44

Figure 4-1 – Protocol Gateway Application Example 45

Figure 4-2 – Protocol Gateway Architectural overview 46

Figure 4-3 – Protocol Gateway Polling Process 49

Figure 4-4 – Protocol Gateway Command Process 51

Figure 4-5 - eNode Designer overview. 53

Figure 5-1 - eNode Designer Setup Installer 54

Figure 5-2 - eNode Designer setup wizard. 54

Figure 5-3 - eNode Designer main screen..... 55

Figure 5-4 - Splash screen and login window. 56

Figure 5-5 - User administration principal. 57

Figure 5-6 - Access user administration..... 57

Figure 5-7 - Adding a new user. 58

Figure 5-8 - Changing a user's user group. 58

Figure 5-9 - Adding a user group. 58

Figure 5-10 - User group added..... 59

Figure 5-13 - Project Root..... 60

Figure 5-14 - Adding a device to the project. 61

Figure 5-15 - Device added to project..... 61

Figure 5-16 – Network properties modified. 62

Figure 5-17 - Editing communication port settings example. 62

Figure 5-18 - Add ADH Application to communication port example..... 63

Figure 5-19 - Choosing client or server..... 63

Figure 5-20 - ADH Application added to project. 63

Figure 5-21 - Adding data point references. 64

Figure 5-24 - Access device settings to set FTP settings..... 65

Figure 5-25 - Device settings window..... 65

Figure 5-26 - Send configuration files window. 66

Figure 5-27 - Asked to reboot after sending configuration files. 67

List of Tables

Table 3-1 Description of Parameters in IPsec Tunnels Web Page..... 33

Table 6-1 - Tree context menu options. 68

1 Introduction

Thank you for Buying ATOP's Protocol Gateway.

The product is bundled with the following three user manuals:

- 1) Hardware specific installation user manual, **not covered in this document**. It covers ATOP's hardware installation procedure, wiring, power connection etc.
- 2) Getting started with ATOP's Protocol Gateway: Basic Gateway configuration, Gateway architectural overview and eNode Designer general instructions– **this manual**. This manual covers the installation, network configuration, maintenance and using of the configuration tool software, including the procedure to be followed for uploading new configurations to ATOP's device.
- 3) Protocol specific user manual, **not covered in this document**. Such manual covers:
 - a. Step-by-step protocol set-up between Client/Master – Server/Slave of the Protocols in eNode Designer
 - b. Description of the protocol-specific software features (of both protocols), the device profile and the implementation table of supported functionalities.

1.1 Scope

This document is divided into four major sections:

- **Getting started**
- **Basic Network Settings with WebGUI**
- **General Description** : it explains the general Gateway architecture and the goals of eNode Designer and its working principals.
- **eNode designer** User Guide : it walks the user through all features of the eNode Designer, specifically explains how to add, delete, and edit projects and carry out device configurations.

1.2 Overview

1.2.1 *List of Abbreviations*

ADH = Application Data Hub
CFE = Communication Front End

2 Getting Started

2.1 Packing List

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

Table 2-1 Packing List

Item	Quantity	Description
PG59XX Series	1	Protocol Gateway
Mounting Kit	1	PG5901, PG5904D, PG5901B and PG5901E <ul style="list-style-type: none"> ● DIN-Rail Kit (x 1) or PG5908, PG5916, PG5900A, PG5908A, PG5916A Series <ul style="list-style-type: none"> ● Rack Mounting Type-L angles (x 2) ● Screws (x 6)
Terminal block		PG5904D and PG5904D-Sis <ul style="list-style-type: none"> ● 7-pin, 2ESDVM-07P (x 1) ● 5-pin, EC381VM-05P (x 4) for PG5904D-Sis-X only PG5901, PG5908, and PG5916 Series <ul style="list-style-type: none"> ● 3-pin, 2ESDV-03P (x 1)
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.

2.2 How to order

Please refer to the following product codes to place an order.

Table 2-2 Product Codes

Item	Description
PG5901-X	1-Port Serial-to-Ethernet Protocol Gateway, Dual LAN, RS-232/422/485 software selectable, DIN-Rail type
PG5901B-X	1-Port Cellular to Ethernet and Cellular to Serial Protocol Gateway, LAN, one RS-232/422/485 software selectable, DIN-Rail type
PG5901E-X	1-Port Serial-to-Ethernet Protocol Gateway with one Profibus port, Dual LAN, one RS-232/422/485 software selectable, DIN-Rail type
PG5904D-X	4-Port Serial-to-Ethernet Protocol Gateway, Dual LAN, RS-232/422/485 software selectable, DIN-Rail type
PG5908-X (US)	8-Port Serial-to-Ethernet Protocol Gateway with RJ45 connectors, AC 100-240V, US power plug
PG5908-X (EU)	8-Port Serial-to-Ethernet Protocol Gateway with RJ45 connectors, AC 100-240V, EU power plug
PG5916-X (US)	16-Port Serial-to-Ethernet Protocol Gateway with RJ45 connectors, AC 100-240V, US power plug
PG5916-X (EU)	16-Port Serial-to-Ethernet Protocol Gateway with RJ45 connectors, AC 100-240V, EU power plug
PG5900A-X	Ethernet-to-Ethernet Protocol Gateway, 6 RJ45 or SFP ports, IEC61850-3 certified hardware
PG5908A-X	8-Port Serial-to-Ethernet Protocol Gateway with DB9 or TB5 connectors, 6 RJ45 or SFP ports, IEC61850-3 certified hardware
PG5916A-X	16-Port Serial-to-Ethernet Protocol Gateway with DB9 or TB5 connectors, 6 RJ45 or SFP ports, IEC61850-3 certified hardware

2.3 First Time Installation

Before installing the device, please follow strictly all safety procedures described in the hardware installation guide that is available inside the box or on ATOP's website. ATOP 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 here. In such cases, please contact your dealer immediately.

When the device is running, connect it to computer to carry on network configuration. Connect LAN1 port to a network switch or to your LAN with a UTP cable and connect a host PC to your LAN with another UTP cable.

After network configuration is complete, it is possible to carry on protocol-specific settings. Protocol specific configuration is made through eNode-Designer utility that is available for download online.

For more information on how to install the device, please refer to the Hardware Installation Guide leaflet available in your package.

2.4 Factory Default Settings

Network Default Setting

The device comes with one IP address specifically for redundant Ethernet interfaces.

Table 2-3 Default Network Setting

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 3-4-5-6 (*)	192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.5	255.255.255.0	192.168.1.254

Remarks: Default DNS 1 setting is 192.168.1.254 and DNS 2 setting is 0.0.0.0. LAN 3-4-5-6 are available on PG59XXA family only

Other Default Settings

Other default settings are shown in the following table:

Table 2-4 Other Default Settings

Parameter	Default Values
Security	
User Name	admin
Password	default
SNMP	
SysName of SNMP	0060E9-XXXXXX
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 Sec. [3.9](#)), to restore the Protocol Gateway to the factory default settings.

3 Configuration and Setup

It is strongly recommended for the user to set the Network Parameters through **Device Management Utility**© first. The device-specific configuration can be carried out via ATOP’s user-friendly Web-Interface.

3.1 Configuration of Network Parameters through Device View

First, please install ATOP’s configuration utility program called **Device Management Utility** that can be downloaded from our websites (www.atop.com.tw or www.atoponline.com). After running **Device Management Utility**, the devices that are already connected to the same subnet of the PC in use will be shown automatically. **Device Management Utility** automatically detects the Protocol Gateway and lists it on **Device Management Utility**’s window.

Alternatively, the Protocol Gateway does not show up or is powered on after the software started, please press “Rescan” icon. The list of devices currently connected to the network will be refreshed as shown below

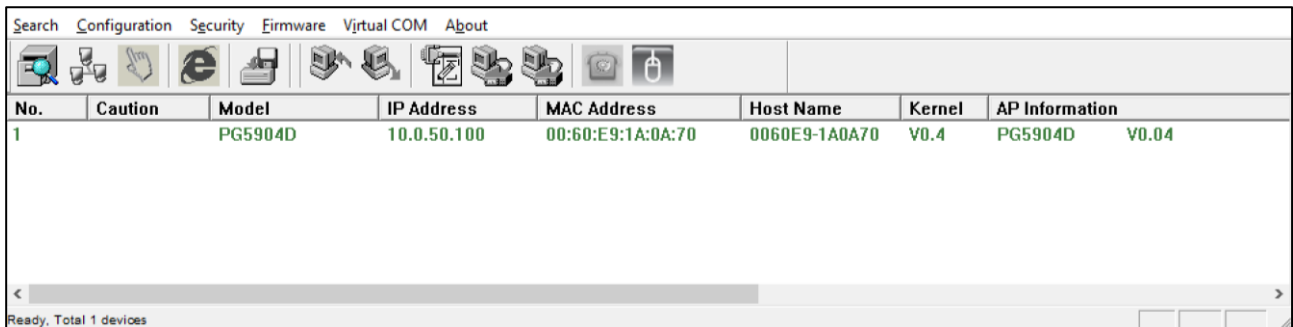


Figure 3-1 - List of Devices on Network in Device Management Utility

Note: This figure is for illustration purpose only. Actual values/settings may vary between devices.

In the event the Protocol Gateway device is not in the same subnet of the PC. Therefore, please use ATOP’s utility to locate it in your virtual environment. To configure each device, click the **selected device** (default IP: 10.0.50.100) in the list of **Device Management Utility**, and click “**Configuration Network...**” menu (or press Ctrl+N) or click on the second icon called **Network** on the menu bar, and a pop-up window will appear as shown below.

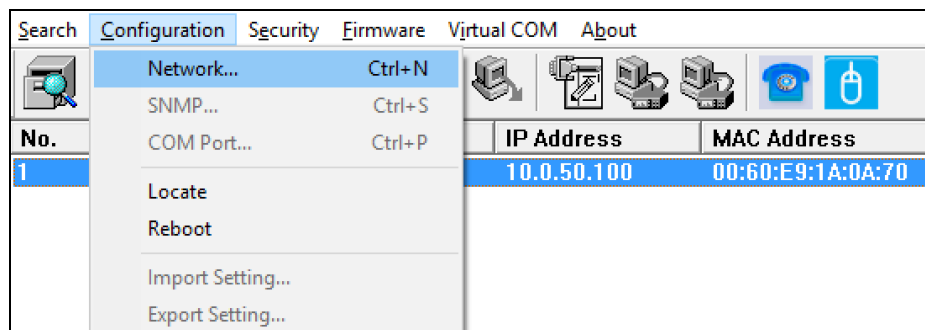


Figure 3-2 - Pull-down Menu of Configuration and Network

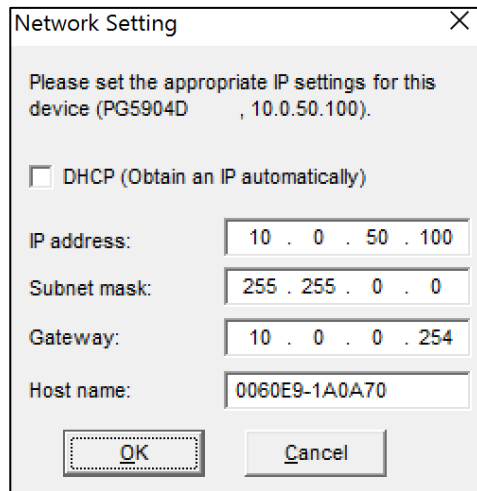


Figure 3-3 - Pop-up Window of Network Setting

Then, proceed then to change the IP address manually. The system will prompt for access credentials to authorize the changes. Please input the Username and Password. After confirmation, the device will be restarted with a beep. After restart, the device will beep twice indicating that the unit is running normally. At this moment the Protocol Gateway will be running on the new IP address. It will be listed automatically by **Device View** along with its old record or it can be found by clicking on the **Rescan** icon.

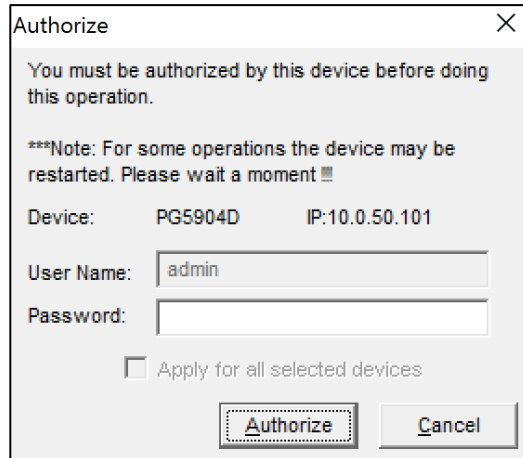


Figure 3-4 - Authorization for Changes

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.

3.2 Configuration through Web Interface

PG59XX Protocol Gateway device is equipped with a built-in web server feature. Thus, the device can be accessed with a web browser for configuration purposes simply by entering the device's IP address (default IP address is 10.0.50.100) in the URL field of your web browser. If the user needs to change the IP address in order to access the web-configuration, please go back to Sec. 3.1. The figure below illustrates the overview page of the web interface.

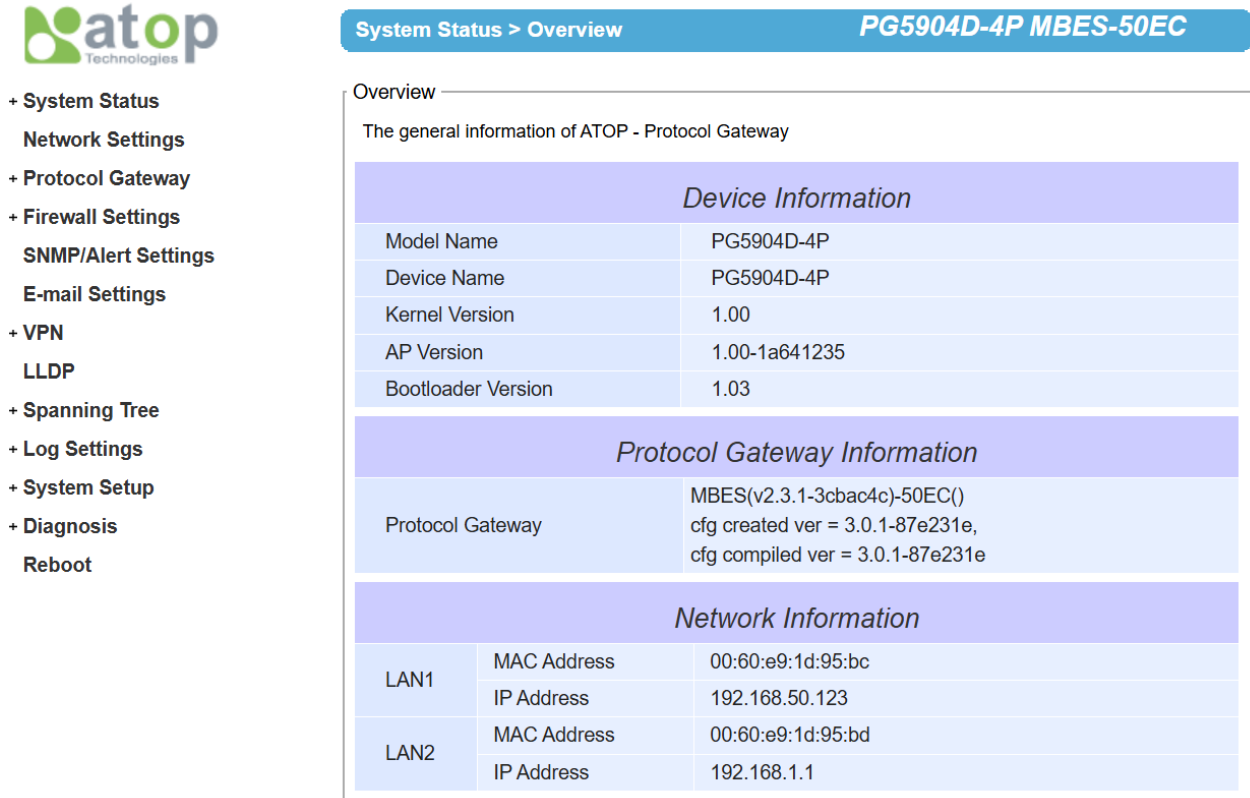


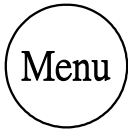
Figure 3-5 - web interface of protocol gateway




Configuring the device is user-friendly. Please go to its corresponding section for a detailed explanation.

3.3 LCM (Liquid Crystal Matrix) Configuration (PG5916 only)

The device also has the option of a configuration without using any software by using its interactive console. This method is however very easy and immediate. Buttons and their functions are described next.

Table 3-1 LCM Button's Description

Buttons		Button Description
	<Menu>	Open Main Menu or Return to the previous menu

	<Up>	Scroll up
	<Down>	Scroll down
	<SEL>	Select

Example

To change the device’s IP address, follow the instruction below.

- Press **<Menu>** to enter **Main Menu**
- Press **<Down>** to scroll down to **2. Network Set**
- Press **<SEL>** to enter Network setting and then **<Up>/<Down>** to scroll up or down to **LAN1**
- Press **<SEL>** to enter **LAN1** and then **<Down>** to scroll down to **1. IP Config**
- Press **<SEL>** to enter **LAN1 IP Config** and then press **<Down>** to scroll down to **1. Static**, finally press **<SEL>** to save the selection.
- Press **<SEL><Down>** to enter **2. IP Address**. Use **<Up>/<Down>** to increase or decrease the **Digits of IP Address**, press **<Menu>** to return to one level higher after completion.
- To enter: **3. Net mask**, use **<Up>/<Down>** to increase or decrease the digits of subnet mask and then **<Menu>** to return to one level higher after completion.
- To enter: **4. Gateway**, use **<Up>/<Down>** to increase the digits of default gateway and use **<Menu>** to return to one level higher after completion.
- Press **<SEL>** to the end of the menu to return to one level higher and the device shall display System message **“Save & Restart”**. Push **<SEL>** to **2. Yes**, and **<SEL>** again after completion. The device shall restart, and the new settings will appear.

The LCM command structure is summarized in Table 3-2.

Table 3-2 LCM Command Structure

1 st layer	2 nd layer	3rd layer	4 th layer	Description	
1.Overview	Model name			Display model name	
	Kernel ver.			Display kernel version	
	AP ver.			Display AP version	
	LAN 1		1.LAN status		Display status of LAN1
			2.MAC		Display MAC address of LAN1
	LAN 2		1.LAN status		Display status of LAN2
2.MAC				Display MAC address of LAN2	
2.Network set	1.LAN 1	1.IP config	1.Static IP	Display or change static IP	
			2.DHCP	Display dynamic IP or enable DHCP	
		2.IP address		Display or change LAN1 IP	
		3.Net mask		Display or change subnet mask	
	4.Gateway		Display or change the Gateway IP		
2.DNS server1			Display or change 1st DNS IP address		

1 st layer	2 nd layer	3rd layer	4 th layer	Description
	3.DNS server2			Display or change 2nd DNS IP address
3.Server state	1.Console	1.Web console	1.Disable	Disable web console
			2.Enable	Enable web console
		2.Telnet console	1.Disable	Disable telnet console
			2.Enable	Enable telnet console
	2.Password protection	1.LCM console	1.No	Disable LCM console password protection
			2.Yes	Enable and change the password
		2.Reset button	1.No	Disable the reset button password protection
			2.Yes	Enable and change the password on reset button
3.Ping	1.LAN 1		Use "ping" command to check specific IP address for LAN1	
	2.LAN 2		Use "ping" command to check specific IP address for LAN2	
4.Restart	1.No			Cancel restart command
	2.Yes			Restart immediately

3.4 Automatic IP Assignment configuration with DHCP

A DHCP server can automatically assign addresses, Subnet Mask and Network Gateway to LAN1 or LAN2. You can simply flag “**DHCP (Obtain an IP Automatically)**” checkbox in the Network Setting dialog using ATOP’s **Device View** utility and then restart it. Once restarted, the IP address(es) will be configured automatically.

3.5 Web Overview

In this section, current information on the device’s status and settings will be displayed. An example of PG5904D-X’s overview page is shown below. This page will look different on each device.

System Status > Overview		PG5904D-4P MBES-50EC
Overview		
The general information of ATOP - Protocol Gateway		
<i>Device Information</i>		
Model Name	PG5904D-4P	
Device Name	PG5904D-4P	
Kernel Version	1.00	
AP Version	1.00-1a641235	
Bootloader Version	1.03	
<i>Protocol Gateway Information</i>		
Protocol Gateway	MBES(v2.3.1-3cbac4c)-50EC() cfg created ver = 3.0.1-87e231e, cfg compiled ver = 3.0.1-87e231e	
<i>Network Information</i>		
LAN1	MAC Address	00:60:e9:1d:95:bc
	IP Address	192.168.50.123
LAN2	MAC Address	00:60:e9:1d:95:bd
	IP Address	192.168.1.1

Figure 3-6 – Overview Page

In detail, the following information is given:

- **Device Information** displays information about the device, such as model name, device name and the Kernel version as well as the AP version.
- **Protocol Gateway Information**, shows the Protocol Gateway model and utility version information for crating the configuration.
- **Network Information** shows the network properties of the two LAN ports

3.6 Network Configuration

In this section, IP address, Subnet Mask, Default (Network) Gateway, Domain Name System (DNS) and overall connectivity settings can be accessed as shown in Fig.3-8. If you flag the **DHCP** checkbox, then IP address, Subnet Mask, and Default (Network) Gateway will be assigned automatically.

Note¹: It is not necessary to connect both ports. The user can connect only one LAN port to the Protocol Gateway device and change the network settings.

Note²: the examples shown in the next pages refer to PG5900A/PG5908A/PG5916A. Other models do not support LAN bonding feature. These features are only available on LAN1,2,3 of PG5900A/08A/16A.

Network Settings	
LAN1 Settings	
Bonding	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	<input type="text" value="10.0.185.100"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Gateway	<input type="text" value="10.0.0.254"/>
LAN2 Settings	
Bonding	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.254"/>
LAN3 Settings	
Bonding	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	<input type="text" value="192.168.2.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.2.254"/>
LAN4 Settings	
DHCP	<input type="checkbox"/> Enable
IP Address	<input type="text" value="192.168.3.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.3.254"/>
LAN5 Settings	
DHCP	<input type="checkbox"/> Enable
IP Address	<input type="text" value="192.168.4.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.4.254"/>
LAN6 Settings	
DHCP	<input type="checkbox"/> Enable
IP Address	<input type="text" value="192.168.5.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.5.254"/>
Virtual IP Settings	
Enable	<input type="checkbox"/>
Virtual IP Address	<input type="text"/>
Virtual IP Interface	LAN1
Default Gateway	
Default Gateway Select	<input checked="" type="radio"/> LAN1 <input type="radio"/> LAN2 <input type="radio"/> LAN3 <input type="radio"/> LAN4 <input type="radio"/> LAN5 <input type="radio"/> LAN6
DNS Server	
Preferred DNS	<input type="text" value="0.0.0.0"/>
Alternate DNS	<input type="text" value="0.0.0.0"/>
<input type="button" value="Save & Apply"/> <input type="button" value="Cancel"/>	

Figure 3-7 – Network configuration Page, example on PG5900A/08A/16A

At the lower section in Figure 3-7, the DNS Servers can be set. This will allow the user to set the IP addresses of Domain Name Server 1 (DNS 1) and Domain Name Server 2 (DNS 2). If the device is connected to the Internet and should connect to other servers over the Internet (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. Please consult the network administrator or internet service provider (ISP) to obtain local DNS's IP addresses.

After finishing the network settings configuration, click **"Save & Apply"** button to save all changes that have been made. A **Save Successful** message will appear and after five seconds the web browser will be redirected to the Overview page7.

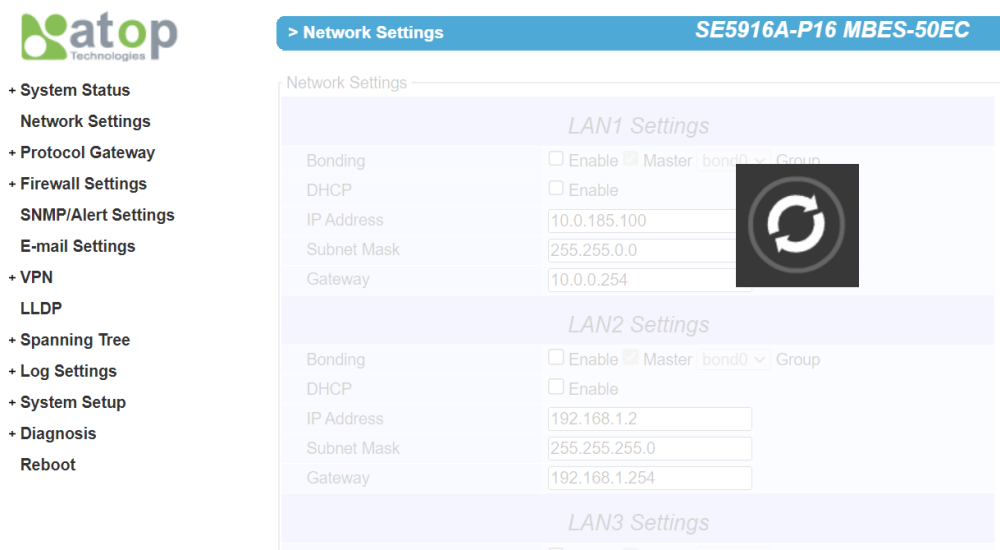


Figure 3-8 – Save completed Page

3.6.1 Link Aggregation

Note: This feature is only available on PG5900A/PG5908A/PG5916A and on LAN 1,2,3.

In the LAN settings, the Physical LAN port bonding is possible in order to allow link aggregation. When two LANs are configured to be in the same group, then only one port (Master) will be active, and the other one will be in standby mode. If the active port link is down, the standby ports will be activated.

The Link aggregation can be configured in the settings of each LAN port as per

Network Settings

LAN1 Settings	
Bonding	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	10.0.185.100
Subnet Mask	255.255.0.0
Gateway	10.0.0.254
LAN2 Settings	
Bonding	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
LAN3 Settings	
Bonding	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
LAN4 Settings	

Figure 3-9.

- **Enable:** Check this box to enable link bonding feature. *Default Unchecked*
- **Master:** Check this box to set this specific LAN port as Master. *Default Checked*

Overview

The general information of ATOP - Protocol Gateway

Device Information	
Model Name	SE5916A-P16
Device Name	SE5916A
Kernel Version	0.00
AP Version	0.00-b5c4f639-dirty
Bootloader Version	1.03
Protocol Gateway Information	
Protocol Gateway	MBES()-50EC()
Network Information	
LAN1	MAC Address 00:60:e9:1a:f4:50 IP Address 10.0.185.100
LAN4	MAC Address 00:60:e9:1a:f4:53 IP Address 192.168.3.1
LAN5	MAC Address 00:60:e9:1a:f4:54 IP Address 192.168.4.1
LAN6	MAC Address 00:60:e9:1a:f4:55 IP Address 192.168.5.1
bond0	MAC Address 66:AB:25:D7:43:EA IP Address 192.168.1.1 Interfaces LAN2 LAN3

Please check the link aggregation status example in Figure 3-10.

Network Settings	
LAN1 Settings	
Bonding	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	10.0.185.100
Subnet Mask	255.255.0.0
Gateway	10.0.0.254
LAN2 Settings	
Bonding	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
LAN3 Settings	
Bonding	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Master bond0 Group
DHCP	<input type="checkbox"/> Enable
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
LAN4 Settings	

Figure 3-9 – Bonding settings

Overview		
The general information of ATOP - Protocol Gateway		
Device Information		
Model Name	SE5916A-P16	
Device Name	SE5916A	
Kernel Version	0.00	
AP Version	0.00-b5c4f639-dirty	
Bootloader Version	1.03	
Protocol Gateway Information		
Protocol Gateway	MBES()-50EC()	
Network Information		
LAN1	MAC Address	00:60:e9:1a:f4:50
	IP Address	10.0.185.100
LAN4	MAC Address	00:60:e9:1a:f4:53
	IP Address	192.168.3.1
LAN5	MAC Address	00:60:e9:1a:f4:54
	IP Address	192.168.4.1
LAN6	MAC Address	00:60:e9:1a:f4:55
	IP Address	192.168.5.1
bond0	MAC Address	66:AB:25:D7:43:EA
	IP Address	192.168.1.1
	Interfaces	LAN2 LAN3

Figure 3-10 – Bonding status

3.6.2 Virtual IP settings

When Virtual IP settings are properly configured, multiple gateways on the same LAN will share the same IP address. The purpose of this feature is to provide failover redundancy, since DCS/SCADA is not aware the number of Gateways on the network if the intended IP address is the same.

When multiple gateways are set as Virtual IP hosts, internally one IP address owner (master host) will be auto-negotiated between them and this will take an active role. The other devices will act as backup hosts. The Master host will send keep-alive packets periodically and if the backup hosts don't receive this for three times, a new master host will be auto-negotiated, taking over the communication.

The meaning of the configuration fields shown in Figure 3-11 are:

- **Enable:** Enables Virtual IP address function. *Default is disabled.*
- **Virtual IP interface:** Setup which physical LAN port will be the virtual IP interface.
- **Virtual IP address:** Setup the Virtual IP address. The Virtual IP Address should be at the same subnet mask of the selected interface.

Virtual IP Settings	
Enable	<input type="checkbox"/>
Virtual IP Address	10.0.50.200
Virtual IP Interface	LAN1

Figure 3-11 – Virtual IP settings

3.7 Protocol Gateway

Use this section of the menu, to enable the redundancy gateways and check the IEDs connection diagnostics.

3.7.1 Redundancy Settings

Note: This feature is only available on PG5900A/PG5908A/PG5916A.

ATOP gateway provides data redundancy mechanism if two gateways are connected in pairs and share the same data point mapping configuration. One device plays the role as primary gateway and the other as secondary gateway. Only primary gateway will retrieve data from IEDs and synchronize data to secondary gateway via “sync port”. The redundancy roles *primary/secondary* will automatically change if there is a link failure. Figure 3-12 shows the configuration page, and below are explained the meaning of each field.

atop
Technologies

- + System Status
- Network Settings
- Protocol Gateway
 - Redundancy Settings
 - 61850 Client Status
 - Download CFG
 - Data Monitor
- + Firewall Settings
- SNMP/Alert Settings
- E-mail Settings
- + VPN
- LLDP
- + Spanning Tree
- + Log Settings
- + System Setup
- + Diagnosis
- Reboot

Protocol Gateway > Redundancy Settings
SE5916A-P16 MBES-50EC

Redundancy Settings

Enable	<input type="checkbox"/>
IEC61850 RCB Instance Num	1
Sync Port 1	LAN1
Sync Port 2	None
Monitored Port 1	None
Monitored Port 2	None

Figure 3-12 – Redundancy settings

- **Enable:** Check this checkbox to enable the gateway redundancy function. Default is disabled.
- **Sync Port1:** the active sync port

- **Sync Port2:** the backup sync port
- **Monitored Port1:** the link status of the physical port can be retrieved from Modbus memory address 65500.
- **Monitored Port2:** the link status of the physical port can be retrieved from Modbus memory address 65500.

If the physical link failure is detected, the gateway will change role to Secondary.

Note: when you create eNode configuration files for primary and secondary gateway, the sequence of data mapping creation should be the same in order to make sure both redundancy gateways get the same database for the data synchronization. When data mapping is deleted, added or moved, the sequence of steps should be the same.

In order to make sure the sequence is the same, it is recommended to follow below steps on both gateways:

1. **Create** eNode configuration template for the correct data mapping.
2. **Duplicate** the template as a new file and revise the IP and other proprietaries accordingly for the primary.
3. **Duplicate** the template as a new file and revise the IP and other proprietaries accordingly for the secondary.

Every time it is needed to revise an existing configuration adding new data mapping, it is recommended to repeat the above steps again in order to make sure the database to be Synchronized.

As far as IEC 61850 Report Control Block is concerned, for consistent data set for both redundancy gateways, it is strongly recommended to use the same CID file for both gateways.

3.7.2 IEC 61850 IED List - connection statistic

It is also possible to check the IED connection diagnostics via web page.

The screenshot shows the 'Protocol Gateway > 61850 Client Status' page for device 'PG5904D-4P MBES-50EC'. The page title is 'IEC61850 Client Status'. Below the title are 'Refresh' and 'Start Auto Refresh' buttons. A 'Show 10 entries' dropdown is present. The main table has columns for '#', 'IP', 'Name', 'Connectivity', and 'Report Status'. One entry is shown: #0, IP 10.0.177.3, Name S472D102BKR5LD0, Connectivity Connected. At the bottom, it says 'Showing 1 to 1 of 1 entries' with 'Previous', '1', and 'Next' navigation buttons.

Figure 3-13 – IED connection statistics

3.8 Advanced Settings

3.8.1 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 below shows the **SNMP Settings** page.

- **System Name**, which is by default, is the MAC address of the device.

- **System Location** is the device’s physical location.
- **System Contact** is the device administrator’s contact information.

In order to make the information available for public viewing by an SNMP Read Community string (a user ID or password), simply flag the “**Enable**” checkbox and fill in “**Public_viewers**” or your desired password string (the default string is “**public**”) in the **Read Community** field. In order to allow a group of people called “**Power_users**” to change the information, enter “**Power_users**” or your desired password string (the default string is “**private**”) in the **Write Community** field. After SNMP Settings configuration is finished, click the **Save & Apply** button to save all changes that have been made. That configuration will take effect after a few seconds and the web browser will be redirected to the Overview page.

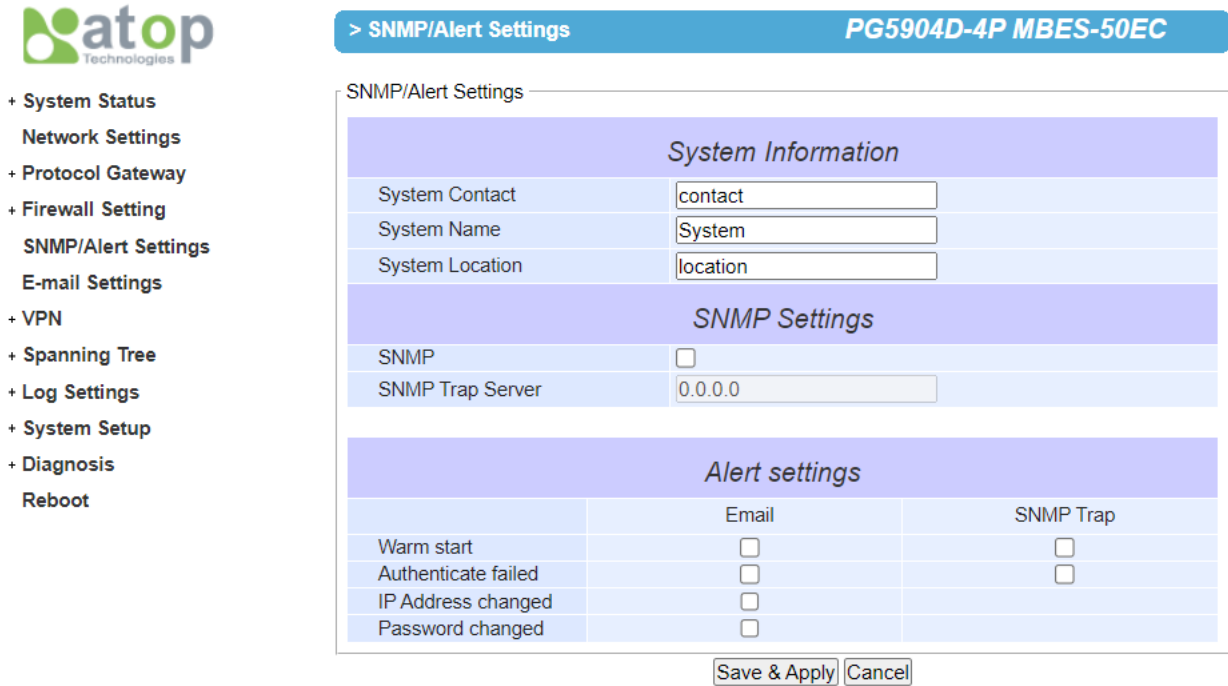


Figure 3-14 – SNMP settings

3.9 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/MB for your reference.

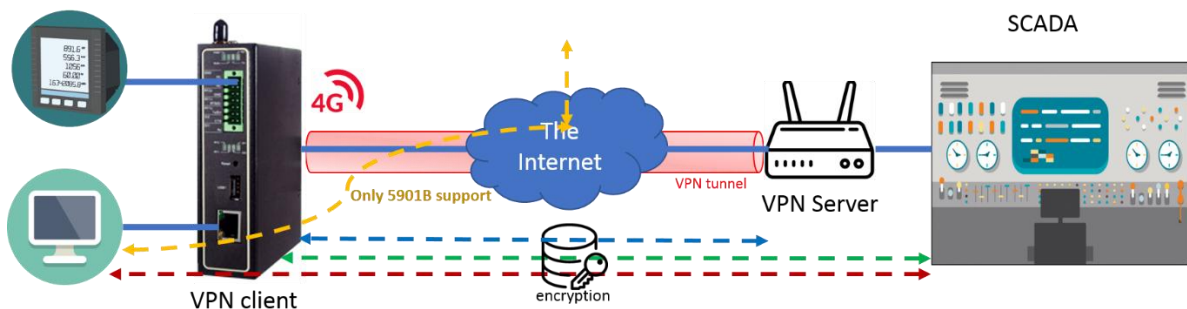


Figure 3-15 VPN Scenario of SE/PG/MB 5901B

3.9.1 PPTP

- 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 22 shows the PPTP configuration page under PPTP web setting. Currently PG59xx series only support PPTP client.

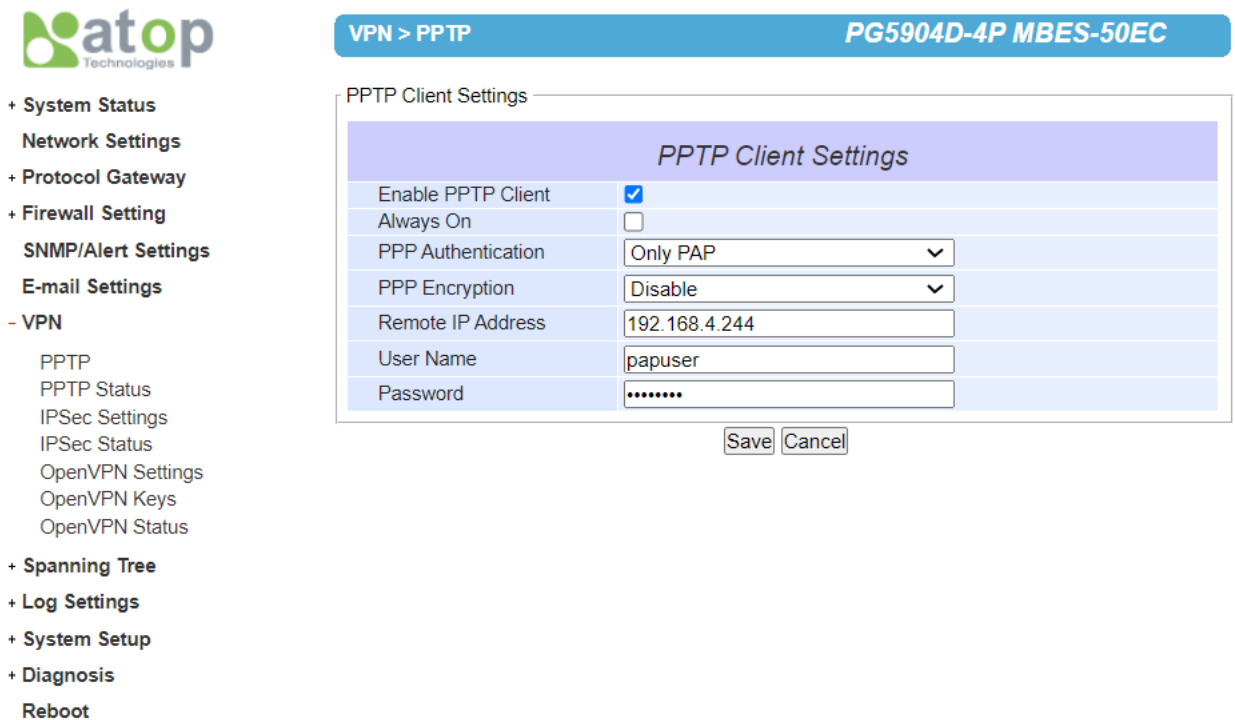


Figure 3-16 PPTP configuration page.

- PPTP client: By checking this to enable the PPTP client on PG59XX series.
- Always on: By checking this, PG59xx will reconnect if server disconnect the tunnel.
- PPP Authentication: Specify the authentication algorithm.
- PPP Encryption: Specify the encryption.
- Remote IP address: Specify the IP address of PPTP server.
- User Name: User name for authentication.
- Password: Password for authentication.

Figure 3-18 shows the PPTP Link status.

The screenshot shows the 'VPN > PPTP Status' page for device 'PG5904D-4P MBES-50EC'. On the left is a navigation menu with categories like System Status, Network Settings, Protocol Gateway, Firewall Setting, SNMP/Alert Settings, E-mail Settings, and VPN. The VPN section is expanded to show PPTP, PPTP Status, IPsec Settings, IPsec Status, OpenVPN Settings, OpenVPN Keys, and OpenVPN Status. The main content area displays the 'PPTP Link Status' table:

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

Below the table are three buttons: 'Connect', 'Disconnect', and 'Refresh'.

Figure 3-17 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: Click this button to refresh the PPTP tunnel status.*

3.9.2 IPsec

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.

PG59XX 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 PG59XX 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 (PG59XX) and a peer device (such as another PG59XX). Note that this type of connection cannot be use for accessing entire sub-network resources. Figure 3-18 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode**.

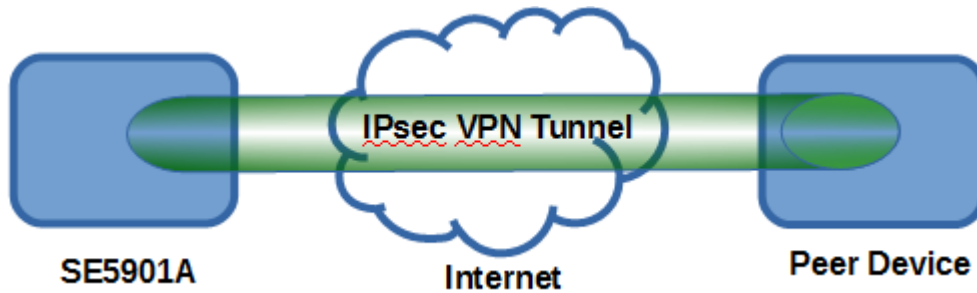


Figure 3-18 An example of Host-to-Host Connection

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 3-19 illustrates a road-warrior application in which PG59XX can access a remote sub-network resource via a peer gateway. Figure 3-20 illustrates a gateway application in which PG59XX can passively accept connection requests from remote sides and provide access to the PG59XX sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

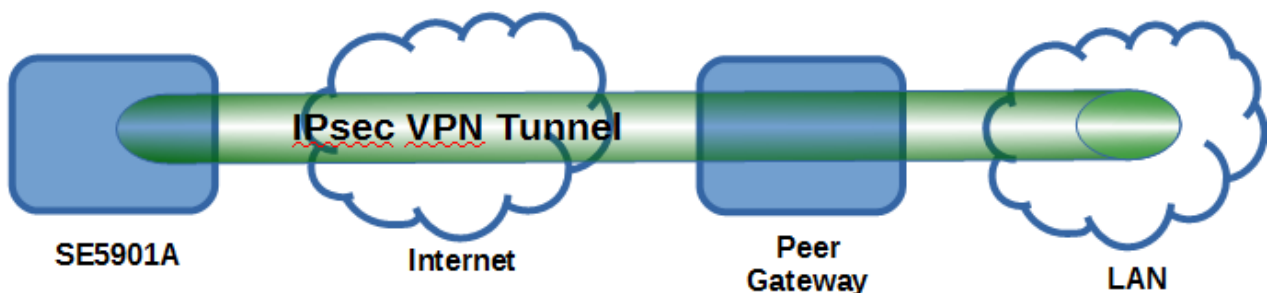


Figure 3-19 Roadwarrior Application using Host-to-Subnet Connection

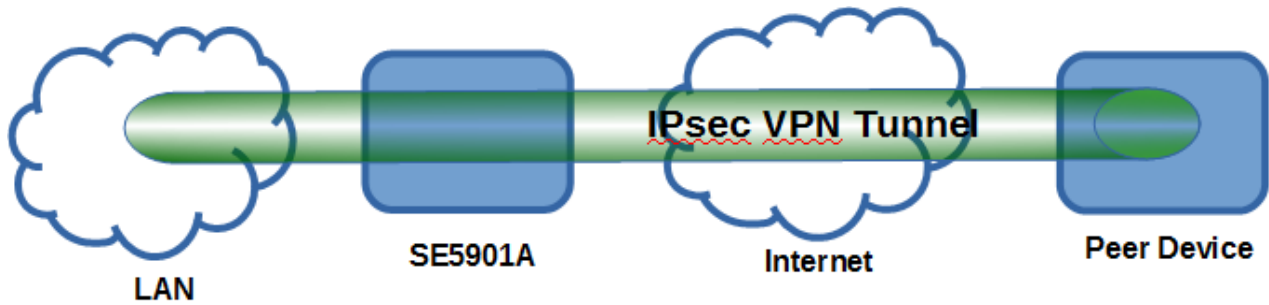


Figure 3-20 Gateway Application using Host-to-Subnet Connection

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 3-21 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 3-22. On the other hand, two different devices on two different subnets (host-host application) can be connected via an IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 3-23. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

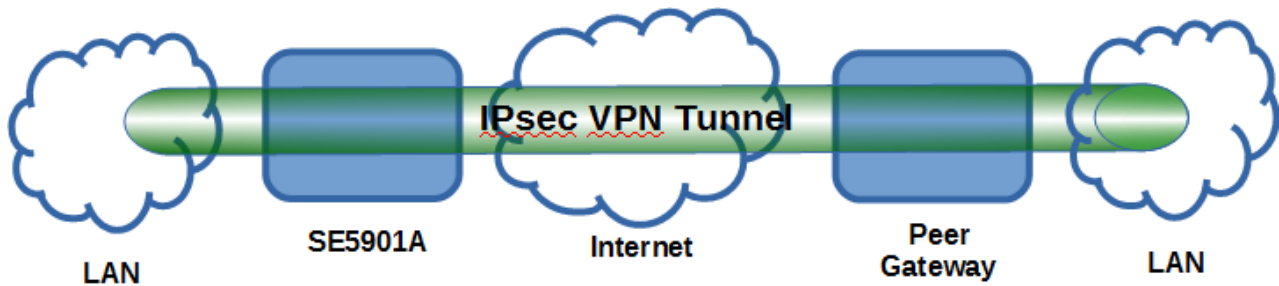


Figure 3-21 An example of network application using a subnet-to-subnet connection via the PG59XX and a peer device

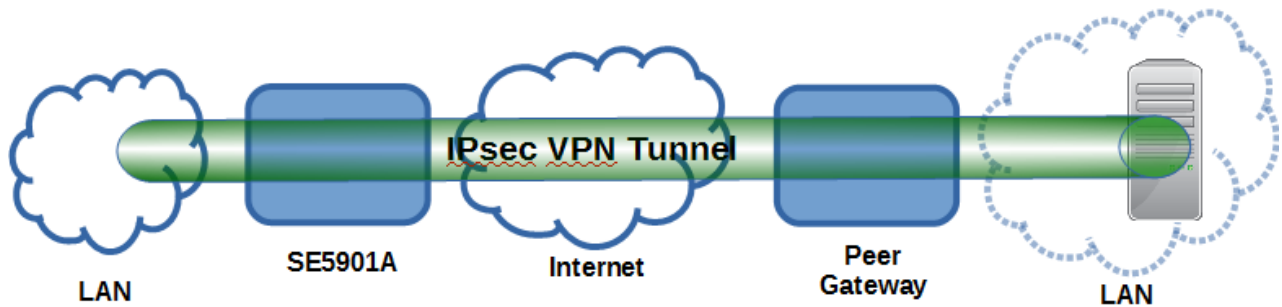


Figure 3-22 An example of host-network application via the subnet-to-subnet connection

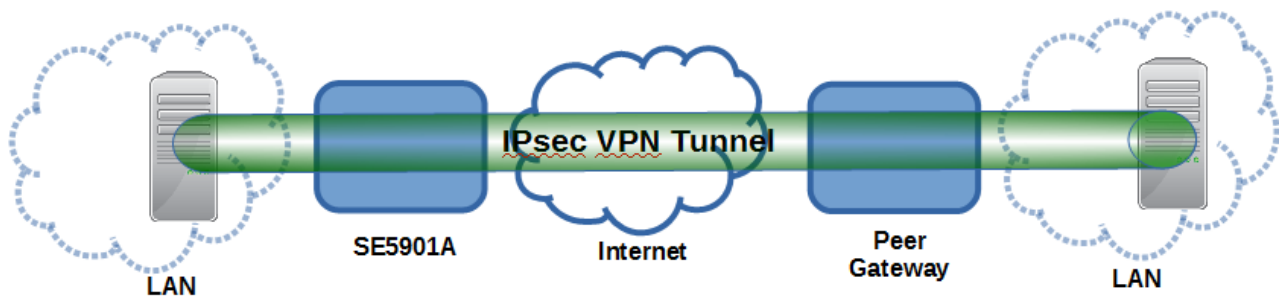


Figure 3-23 An example of host-host application via the subnet-to-subnet connection

In some network configurations, 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 communicate 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 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.

To provide security service for all types of tunnel connections and applications described above, PG59XX 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) are divided into two phases. In phase one, IKE creates an authenticated secure channel between PG59XX 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.

- *Figure 3-24 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**.*



- + System Status
- Network Settings
- + Protocol Gateway
- + Firewall Setting
- SNMP/Alert Settings
- E-mail Settings
- VPN
 - PPTP
 - PPTP Status
 - IPSec Settings
 - IPSec Status
 - OpenVPN Settings
 - OpenVPN Keys
 - OpenVPN Status
- + Spanning Tree
- + Log Settings
- + System Setup
- + Diagnosis
- Reboot

VPN > IPSec Settings PG5904D-4P MBES-50EC

IPsec Settings

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

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

Figure 3-24 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 PG59XX..
- 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 PG59XX 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 radio button for Static option and enter the IP address in the text box behind it. The PG59XX 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).
- **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 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 next option is the Remote ID. This is used to authenticate the remote certificate during Phase 1 IKE negotiation. To allow both sides of the tunnel to authenticate each other, you must select the local and remote identities and enter the **IDs** in the textboxes behind the **Local ID** and the **Remote ID**. Note that the available options for **Local ID** are **IP** address, **E-mail** address, or **Domain Name** while the available option for **Remote ID** are **Any**, **IP** address, **E-mail** address, or **Domain Name**. Note that if you select “**Any**” for Remote ID, you do not have to enter anything in the textbox and the remote ID will not be verified. If authentication IP is chosen for Remote ID but no IP address is configured in the field and the **Peer Address** is set to **Static Address** type (see above), then PG59XX will use the static IP as the authentication IP.

The third part of **IPsec Settings** is the **IKE** (Internet Key Exchange) **Settings**. Internet Key Exchange (IKE) that PG59XX supports is the IKE version 2 or **IKEv2**. In **IKE Settings**, there are four possible settings for **IKEv2** which are **Permit**, **Propose**, **Insist**, and **Never**. The default value is “**Permit**” which means that no **IKEv2** should be transmitted but will be accepted if the other ends initiate to PG59XX with **IKEv2**. If the **IKEv2** is set to “**propose**” then it means that **IKEv2** is permitted and it will be used as the default to initiate. If the **IKEv2** is set to “**Insist**” then it means that PG59XX will accept and receive **IKEv2** only and no **IKEv1** negotiation is allowed. If the **IKEv2** is set to “**Never**” then its means that no **IKEv2** negotiation should be transmitted or accepted.

Within the **Phase 1 SA (ISAKMP)**, there are six 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 into 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. PG59XX 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 and network. The default **SA Life Time** is 10800 seconds. The configurable range for **SA Life Time** is between 300 to 86400 seconds.
- The last 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. This option can be checked or unchecked. If this option is disabled, the protocol will use the same security key for different IPsec phases. If this option is enabled to enhance security, the protocol will select the different security key from either **DH Group 2** (1024-bit) or **DH Group 5** (1536-bit).

Within the **Phase 2 SA**, there are five security options to be configured. Similar to **Phase 1 SA**, PG59XX 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**), and selected encryption, and authentication algorithms. In Phase 2 SA, PG59XX also supports two **DH groups** which are **DH Group 2** and **DH Group 5**. 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 PG59XX use to verify the existence of a remote Internet Key Exchange (IKE) gateway or the peer device of PG59XX. To detect the peer device, PG59XX will send encrypted IKE Phase 1 notification payloads (or hello message) to its peer device and wait for DPD acknowledgement from the peer device. If PG59XX does not receive an acknowledge message during a specific time interval (**DPD timeout**), it will consider that the peer device is dead. Then, PG59XX 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 PG59XX 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 for sending the hello message to the peer device or the interval that PG59XX will repeat checking 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 PG59XX 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 period expires, the PG59XX 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 parameter in the IPsec Tunnels web page is summarized in

Table 3-1.

Table 3-1 Description of Parameters in IPsec Tunnels Web Page

Field Name		Description	Default Value
General Settings			
IPsec		Enable the IPsec Tunnel	Disable
Peer Address		IP address of the remote device which can be dynamic (any address) or static (fixed address)	-
Remote Subnet		Remote subnet can be either None (Host only) or Network (IP and Netmask)	-
Connection type		Tunnel mode or Transport mode	Tunnel
Authentication Settings			
Method		Pre-Shared Key	-
Local ID		How the local participant should be identified for authentication which can be IP, E-mail, or Domain Name	IP
Remote ID		How the remote participant should be identified for authentication which can be Any, IP, E-mail, or Domain Name	Any
IKE Settings			
IKEv2		Support of IKEv2	Permit
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)	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.	10,800
	Perfect Forward Secrecy	Whether Perfect Forward Secrecy of keys is desired on the connection's keying channel.	Unchecked
Phase 2 SA	Protocol	Choose how IP packet will be encrypted and verify: either Encapsulate Security Payload (ESP) or IP Authentication Header (AH)	ESP
	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	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 and network. The available setting ranges is from 180 to 86,400 seconds.	3600
Dead Peer Detection Settings			

Field Name	Description	Default Value
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 & Apply** button to save all changes that have been made. Finally, the web browser will return to the IPsec Tunnels web page. If you would like to discard any setting, please click the **Cancel** button.

3.9.3 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**. **Note** that the network-to-network (or subnet-to-subnet) connections are not supported in PG59XX.

3.9.4 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 3-25. Please follow the steps provided next for each scenario to set the **General Settings**.

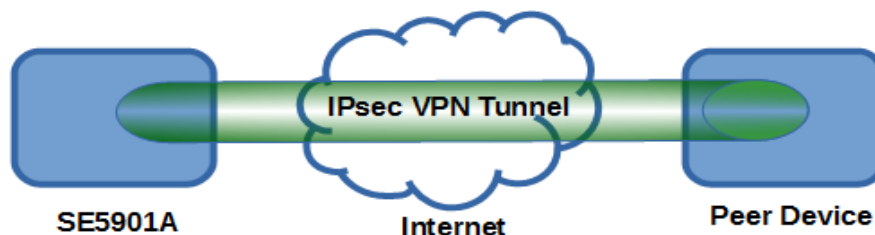


Figure 3-25 IPsec VPN Tunnel with Host-to-Host Topology

Scenario: host-to-host with static peer as shown in Figure 3-26

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
Note: When peer address is entered as the static address, the PG59XX acts as an **initiator** which takes the initiative and establishes a connection. The PG59XX 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	<input checked="" type="checkbox"/> Enable
Peer Address	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static: 172.16.1.1
Remote Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: 192.168.1.0 / 24
Local Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: 10.0.50.0 / 24
Connection Type	Tunnel

Figure 3-26 General Settings for Host-to-Host with Static Peer

Scenario: host-to-host with dynamic peer as shown in Figure 3-27

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
Note: When VPN connects to a peer with dynamic IP address, the PG59XX 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	<input checked="" type="checkbox"/> Enable
NAT Traversal	<input type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static:
Remote Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: 192.168.1.0 / 24
Connection Type	Tunnel

Figure 3-27 General Settings for Host-to-Host with Dynamic Peer

3.9.5 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 PG59XX is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in Figure 3-28. Please follow the steps provided next for each scenario to set the **General Settings**.

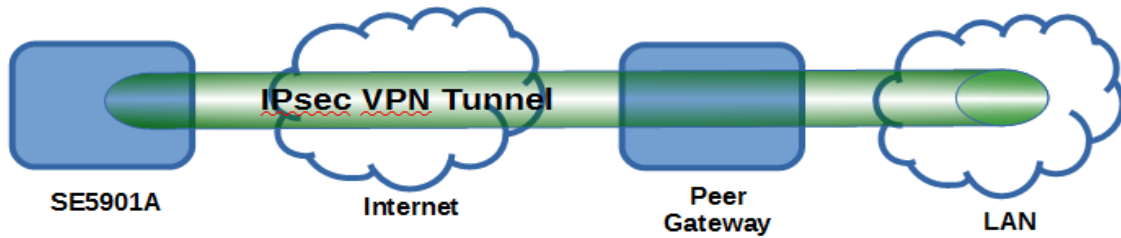


Figure 3-28 IPsec VPN Tunnel with Host-to-Network Topology

Scenario: host-to-network with static peer as shown in Figure 3-29

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
Note: When peer address is entered as a static address, the PG59XX is an **initiator** which takes the initiative and establish a connection or can be a **responder** waiting for connection. The PG59XX 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.

IPsec Settings	
General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
NAT Traversal	<input type="checkbox"/> Enable
Peer Address	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static: <input type="text" value="172.16.1.1"/>
Remote Subnet	<input type="radio"/> None (Host Only) <input checked="" type="radio"/> Network: <input type="text" value="192.168.1.0"/> / <input type="text" value="24"/>
Connection Type	<input type="text" value="Tunnel"/> ▼

Figure 3-29 General Settings for Host-to-Network with Static Peer

Scenario: host-to-network with dynamic peer as shown in Figure 3-30

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
Note: When VPN connection is set to a peer with dynamic IP address, the PG59XX 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.

IPsec Settings

General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static: <input type="text" value="10.0.50.100"/>
Remote Subnet	<input type="radio"/> None (Host Only) <input checked="" type="radio"/> Network: <input type="text" value="192.168.1.0"/> / <input type="text" value="24"/>
Local Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: <input type="text" value="10.0.50.0"/> / <input type="text" value="24"/>
Connection Type	<input type="text" value="Tunnel"/> ▼

Figure 3-30 General Settings for Host-to-Network with Dynamic Peer

Figure 3-32 shows the IPsec Link status.

IPsec Status

Current Status	
Peer Address	211.72.229.133
VPN Tunnel	10.0.159.14/32 === 10.0.62.0/24
Status	Connected

Figure 3-31 IPsec Link Status

- Peer Address: The peer IP address.
- VPN Tunnel: The local site and peer site IP address. The subnet “/32” means that it’s peer-to-site scenario.
- Status: It will show the Connected, Connecting and Disconnected.

3.9.6 OpenVPN

OpenVPN is an application that implements VPN for creating secure point-to-point or site-to-site connections in routed or bridged 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 either 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. Noted that currently PG59XX series only support TUN mode.

3.9.7 OpenVPN Setting

Go to VPN tab > OpenVPN Settings. You can find the general setting parameters for OpenVPN settings as below.

OpenVPN Settings

General Settings	
Profile	1 ▾
OpenVPN	<input type="checkbox"/> Enable
Mode	Server ▾
Protocol	UDP ▾
Port	1194
Device Type	TUN
Virtual IP	10.8.0.0
Authorization Mode	SSL/TLS ▾
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA1 ▾
Compression	Disable ▾
Push LAN to clients	<input type="checkbox"/> Enable

Save Cancel

Figure 3-32. OpenVPN Setting

- **OpenVPN:** By checking this to enable OpenVPN function.
- **Mode:** To specify 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:** Select the protocol to be used for VPN.
- **Port:** Define the port number for TCP/UDP connection.
- **Device Type:** Select OpenVPN tunnel connection by TUN mode or TAP mode. Currently PG59XX series only support TUN mode.
- **Virtual IP:** Specify the server virtual IP. Virtual IP only be available when SSL/TLS is chosen in Authentication Mode.
 Server 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: Specify the local and remote endpoint virtual IP address of this OpenVPN 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.
 SSL/TLS: The OpenVPN will use TLS authorization mode, and the following items CA cert, Server Cert and DH PEM will be use. See section 4.9.4.2 for server and client certificate.
 Static Key: the OpenVPN will use static key authorization, and the static key will be used. See section 4.9.4.2 for static key.
- **Encryption Cipher:** Specify the Encryption cipher. It could be Blowfish, AES256/192/128 and Disable. When choose Disable, no encryption will be used.
- **Hash Algorithm:** Specify the Hash algorithm. It could be SHA1, MD5, SHA256/512 and Disable. When choose Disable, none Hash algorithm will be used.
- **Compression:** Specify if the tunnel packets will be compressed. It could be LZ4, LZO and Disable. When choose Disable, the packet won't be compresses in tunnel.
- **Push Lan to clients:** This is the network that will be accessible from the remote endpoint. When enabled, PG59XX will push the LAN port subnet to the OpenVPN remote clients. So that remote client will add a route to the PG59XX local network.
 Noted that only SE5901B supports this function now.

3.9.8 OpenVPN Keys

Go to OpenVPN Keys for certificate authority and key.

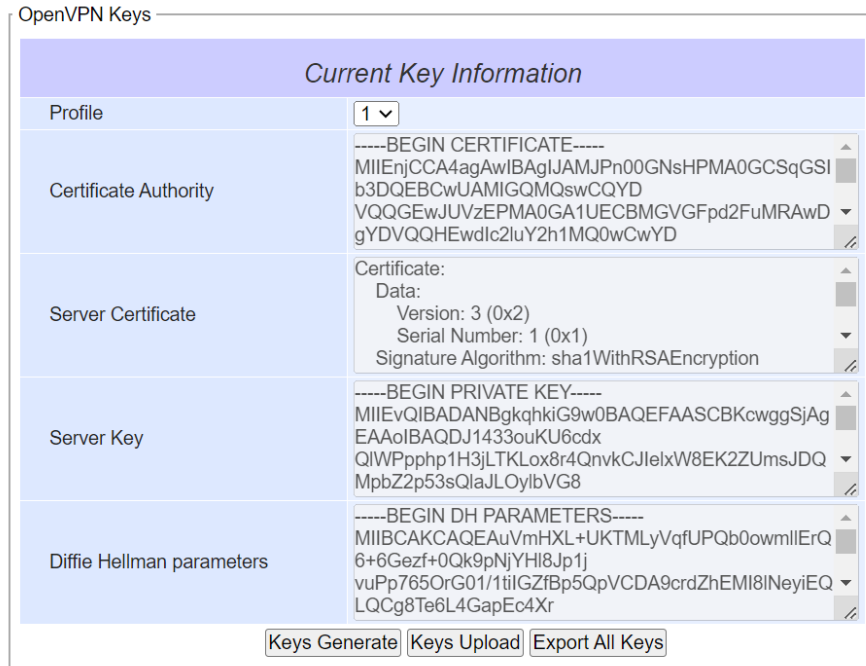


Figure 3-33 OpenVPN Keys

- **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 Certificate:** It shows the information of server certificate. You can check the information if you use upload server certificate file.
- **Server Key:** It shows the information of server key. You can check the information if you use upload server key file.
- **Diffie Hellman parameters:** It shows the information of Diffie Hellman parameters.

When PG59XX acts as OpenVPN server, user could define his own certification information by clicking Key generate.

OpenVPN Keys Generation

Certificate Information	
Profile	1
Country Code	TW
State	Taiwan
City	Hsinchu
Organization	Atop
Organizational Unit	Atop
Email Address	sales@atop.com.tw
Common Name (Read Only)	AtopPG
Expire time (Read Only)	10 (years)
<input type="button" value="Generation Keys & Apply"/>	

Figure 3-34 Certification information

- *Country Code: Enter the country.*
- *State: Enter the state*
- *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's name. (Read only)*
- *Expire time: The number of years the certificate is valid for. (Read only)*

Using Upload key function for uploading specified server or client certificate.

OpenVPN Keys Upload

Certificate Upload	
Profile	1
SSL/TLS	Root CA <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
	Server CA <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
	Server Key <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
	Server DH <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
<input type="button" value="Cancel"/>	

Figure 3-35 Certificate Upload

Click the Browse button to upload your own server or client certificate.

When PG59XX acts as OpenVPN server, using Export All Keys to download all the necessary certificates including CA.crt, CA. key and the certificate and key for client side.

3.9.9 OpenVPN Status

Go to tab OpenVPN status to check the current status of tunnel connection.

OpenVPN Status

Current Status	
Mode	Client
Local Virtual IP Address	0.0.0.0
Remote Virtual IP Address	0.0.0.0
Status	Disconnected

Connect Disconnect Refresh

Figure 3-36 OpenVPN client status

- *Mode: Display the mode PG59XX acts as.*
- *Local Virtual IP address: Display the Local virtual IP address.*
- *Remote Virtual Status: Display the Remote virtual IP address.*
- *Status: Display the current status of OpenVPN connection. It will include Disconnected, Connecting and Connected.*

OpenVPN Status

Current Status	
Mode	Server
Local Virtual IP Address	0.0.0.0
Status	Deactivated

Client List			
Common Name	Real Address	Virtual Address	Since

Activate Deactivate Refresh

Figure 3-37 OpenVPN server status

- *Mode: Display the mode PG59XX acts as.*
- *Local Virtual IP address: Display the Local virtual IP address.*
- *Status: Display the current status of OpenVPN connection. It will include Deactivated, Activating, Disconnected, Connecting and Connected.*

3.10 System Setup

Please use the sub-menus inside the System Setup menu in order to configure the system.

3.10.1 Time

Date and time can be set manually or through **Network Time Protocol (NTP)** to automatically synchronize date and time of the Protocol Gateway with a **Time Server**. The figure below 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, to enable automatic date/time update, flag the **Obtain date/time automatically** checkbox. If this is unchecked, please set the time manually in **“Manual time settings”** later explained.

If NTP is enabled, fill in the IP address or hostname of the preferred time server such as *pool.ntp.org* which is the default setting. If a hostname is entered, the DNS server should be configured properly following the procedure explained in [Sec.3.6](#). Other options will hide if the **NTP** option is selected.

System Setup > PG Date/Time Settings
PG5904D-4P MBES-50EC

PG Date/Time Settings

The NTP (Network Time Protocol) is used to synchronize the date/time from the NTP server.

Current Date/Time

21 / Nov / 2024 22:00:51

Time Zone Settings

Time Zone (GMT+08:00) Taipei ▼

Time Settings

Local NTP Service

Select Time Source NTP/SCADA ▼

NTP Server

Manual Time Settings

Date -- / -- / --

Time -- : -- : --

Sync Time from IEC61850 Object

Enable

IED Domain Name

Time 0 : 0 : 0

Daylight Saving Time Settings

Enable Daylight Saving Time

Start Date -- / -- / Sun / 0 (Month / Week / Date / Hour)

End Date -- / -- / Sun / 0 (Month / Week / Date / Hour)

Offset 0 hour(s)

Save & Apply
Cancel

Figure 3-38 – Time settings Page

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, flag 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 grayed-out area of Fig.3-42. After Time Setting is complete, click **Save Configuration** to save all changes that have been done. A **Save Successful** message will show, and the web browser will be redirected to the Overview page.

3.10.2 Security

The default security setting for the password is a standard password (default). To change security, 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.

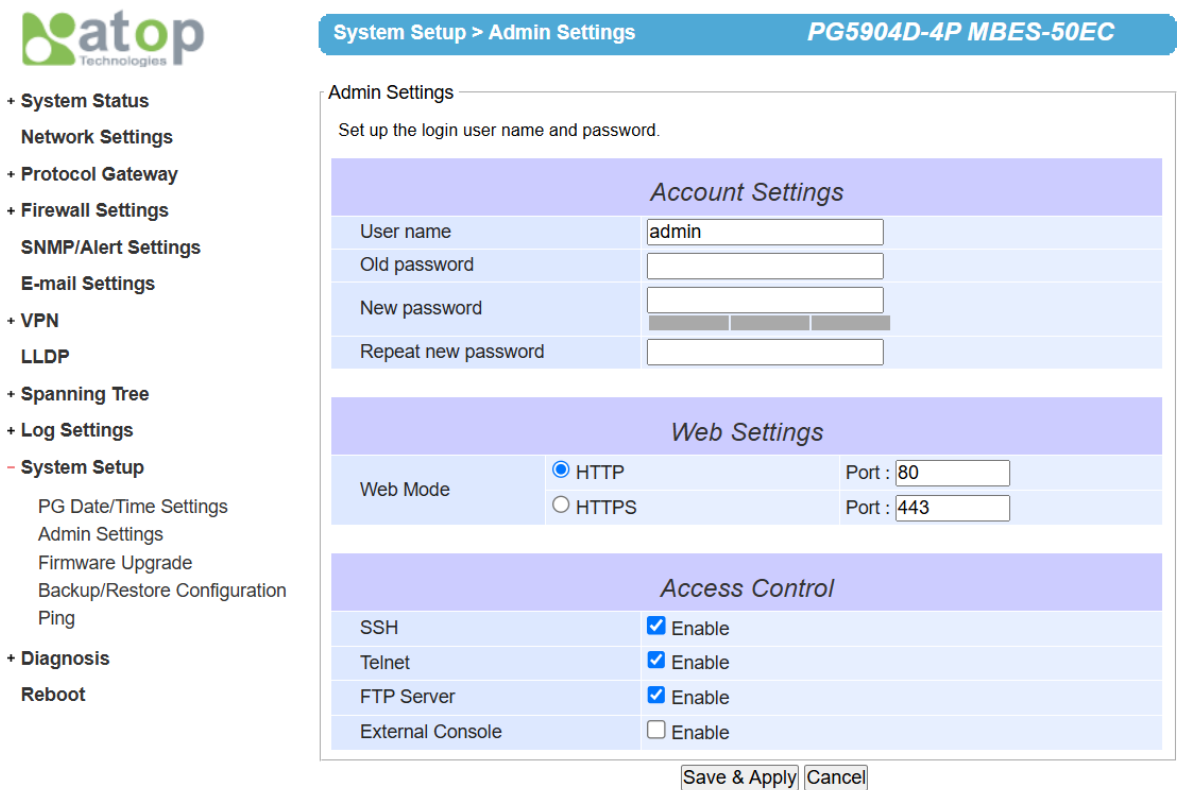


Figure 3-39 – Admin settings Page

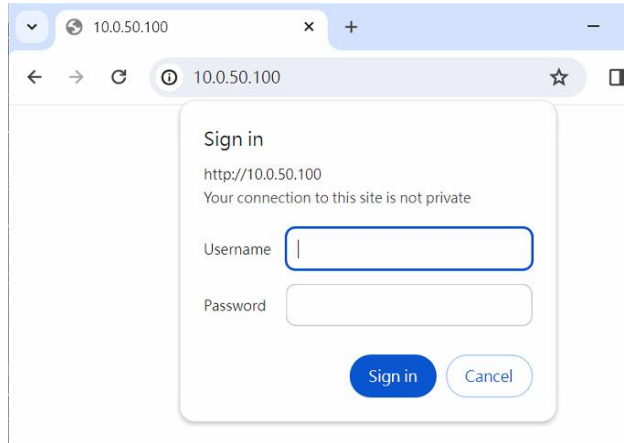


Figure 3-40 – Entering the User Name and the New Password

The user can define whether the web interface is encrypted (through HTTPS) or not (through HTTP). To carry on the selection, click on **“Web mode settings”** in the menu on the left-hand side and choose the desired setting as shown in the following figure. After the choice has been made, click **“Save & Apply”** A **Save Successful** message will appear with and the web browser will be redirected to the Overview page.

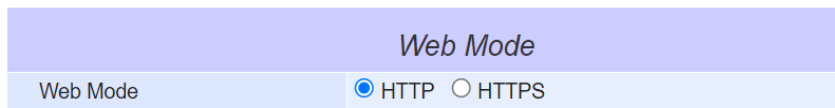


Figure 3-41 – Web mode settings

3.10.3 Restart

For some unexpected circumstances, the Protocol Gateway system may stop responding correctly. The user has the option to restart the device by clicking the **Restart** button as shown below. 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.

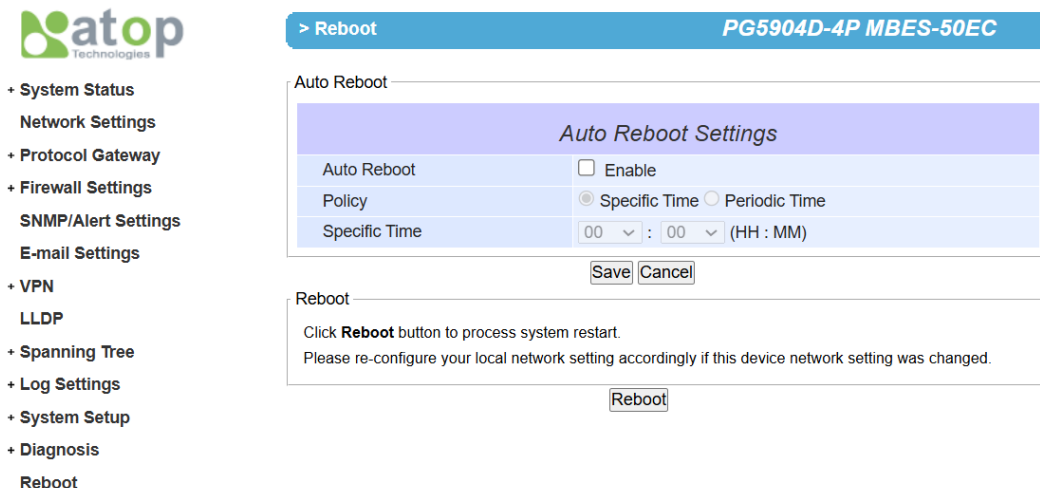


Figure 3-42 – Restart page

4 General Description

4.1 Protocol Gateway Overview

ATOP's Protocol Gateway "PG" family is a very powerful industrial protocol gateway platform. Based on your request, it is bundled with different protocol stacks that can run at the same time in the client/server – master/slave mode.

Shown in the below figure a typical application of ATOP's Protocol Gateway

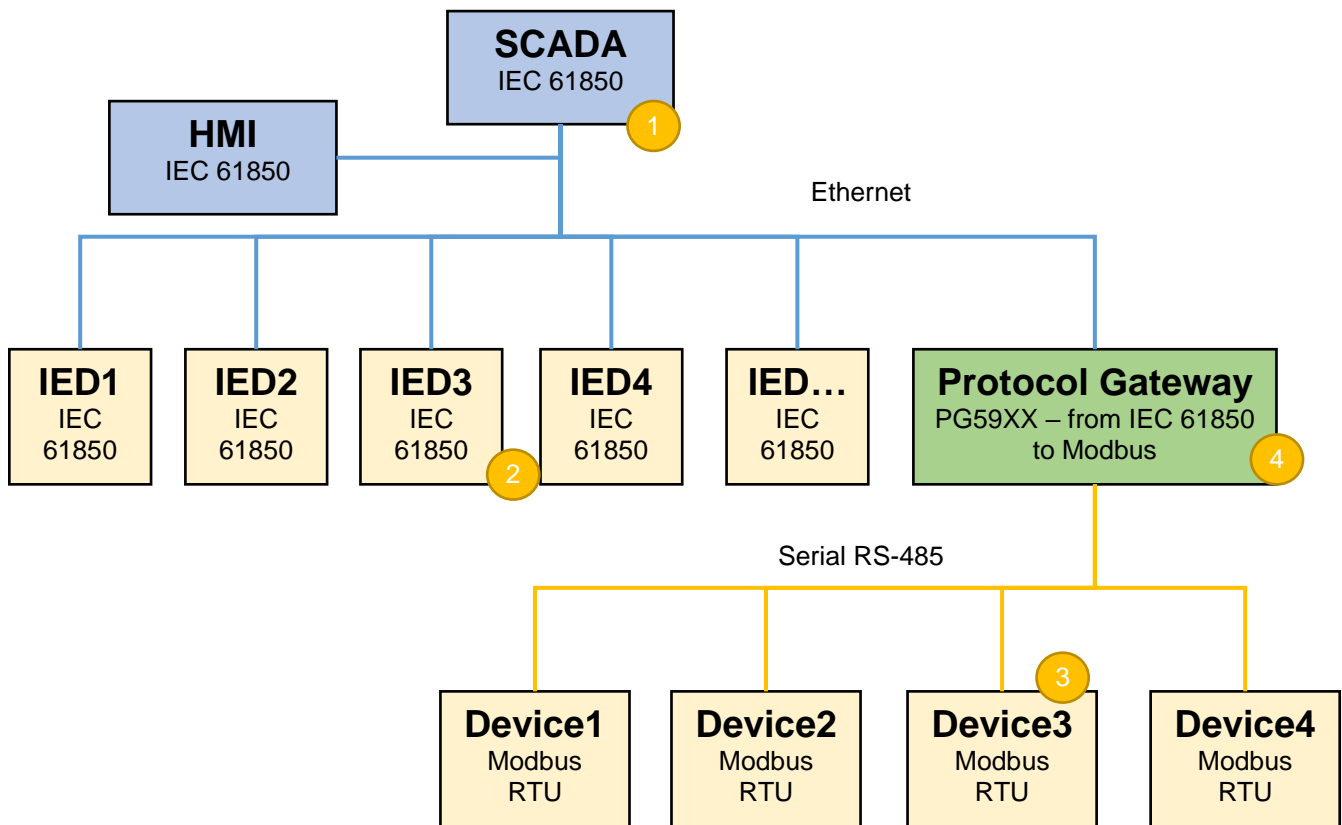


Figure 4-1 – Protocol Gateway Application Example

- 1 Represents the HOST side that is in control of the application issuing read and write commands and managing events. It can be a SCADA (Supervision Control and Data acquisition), an IPC, an HMI (Human / Machine Interface) etc... In this example, the HOST side works with IEC 61850. This is the Client/Master side.
- 2 Represents the Device side, connected to the HOST side that receives read/write commands and replies to the HOST. In this example, these devices are connected directly to the host because they run IEC 61850 protocol. This is the Server/Slave side. Only one server/slave per protocol is supported in ATOP protocol gateways
- 3 Represents the Device side. In this example these devices run Modbus RTU protocol on RS-485 and they will receive read/write commands from a Modbus RTU Host only. This is the Server/Slave side
- 4 Represents the Device side for the HOST (SCADA) and the HOST side for the Modbus RTU Devices.

The Protocol Gateway's job is to translate the information from IEC 61850 to Modbus RTU and to let the SCADA seamlessly connect to non-IEC-61850 devices. This is the Server/Slave side for SCADA and Client/Master side for the Modbus Devices.

Shown in the below figure the general software architecture of the device:

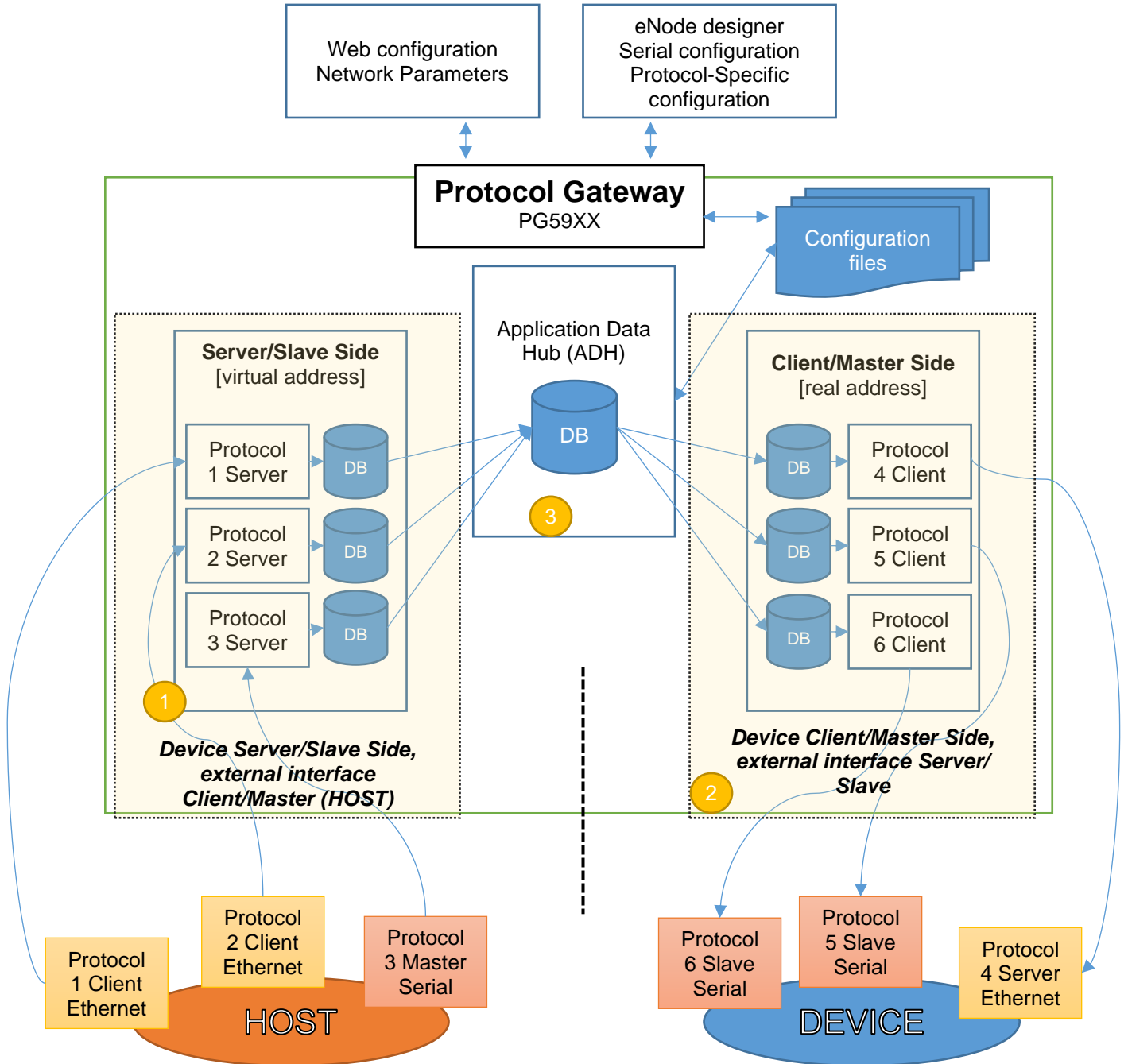


Figure 4-2 – Protocol Gateway Architectural overview

The protocol gateway main network settings can only be defined by Web interface.

The architecture is made of 3 different parts:

- 1 **Device Server/Slave interface** (that is listening to a Master/Client that is outside a device, a PLC for example). This means that ATOP's PG will behave towards an external master as a slave device, in the related protocol
- 2 **Device Client/Master interface** (that is actively polling or issuing commands to an external Slave/Server)
- 3 **ADH** the core of the unit that moves, translates and maps the data points/commands/events from the client side to the server side and vice-versa

In general, the device allows to map any protocol to any port (serial or Ethernet) based on the limitations and constrains from the protocol itself.

eNode Designer will allow the user to assign different protocols to different port, define the serial port settings and to the protocol-specific parameters.

Inside eNode Designer, the user will define for the Master/Client the real IDs of the devices need to get data/send commands from and will set for the Slave/Server the virtual addresses to be used by the client for data-point or command mapping to. The more information related to eNode Designer is available in chapter [5](#).

The core of the Gateway is the Application Data Hub, where the data/commands/events (if applicable) is stored and mapped to the other relevant protocol.

4.2 *Device Client/Master*

In eNode Designer, the user will have to assign a specific protocol to a serial or an Ethernet port. While Serial ports allow only one protocol to be assigned to each port, Ethernet ports may have more than one, since communication may use different TCP/UDP ports or layer. One Ethernet port can have an IP address only.

The user will have to specify which data points from which Slave/Server IDs should be polled, the data type/timeout if applicable and the polling frequency. After this is set and configuration is uploaded to the device, ATOP's Protocol Gateway will start to automatically poll the slaves based on that configuration.

The received data will be stored into the ADH internal database and then automatically synced with the server/slave protocol internal database.

Commands sent from the Device Server/Slave side instead, once properly mapped in eNode Designer will be executed only upon request and won't be routinely executed. The user will be able to customize timeout settings in eNode Designer.

In general, the gateway is as a client/master role and needs to read/write data from/to other devices which are as server/slave role, so:

- Step1. Assign a device with specific protocol to an interface (serial / Ethernet).
- Step2. Do the configuration for talking with the device including communication related parameters, protocol related parameters and data points for read/write.
- Step3. Goto the Step1 if there are more devices connected.

4.3 *Device Server/Slave*

As client/master, in eNode Designer, the user will have to assign a device to a serial or an Ethernet port by designating a specific protocol first. While Serial ports allow only one protocol to be assigned to each port, Ethernet

ports may have more than one, since communication may use different TCP/UDP ports or layer. One Ethernet port can have an IP address only.

The user will have to specify which data points/commands should be made available for the external client (e.g. a PLC) and may map such data points/commands with another Client/Master data point/command point.

Some protocols support unsolicited events triggered by the device. If this function is necessary, the user may set the threshold so that upon going over it an unsolicited event will automatically be triggered.

Aside unsolicited events, Server/Slave function is always in listening mode, waiting for read/write commands to be issued from the master. When a read command is received, the most updated data point available in the database will be returned with the related timestamp if defined in the server protocol specifications. When a write command is received, this will be relayed to the related Client/Master module and executed. If expected by the protocol spec, a confirmation message will be returned

In case of communication problems between Client/Master and the slave, exceptions will be returned.

In general, the gateway as a Server/Slave role needs to define virtual data points for the Hosts to read/write.

Step1. Create a virtual Sever/Slave with specific protocol to an interface (serial / Ethernet).

Step2. Do the configuration for this virtual Sever/Slave including communication related parameters, protocol related parameters and data points for read/write.

Step3. Go to Step1 if there are more virtual Severs/Slaves that the gateway plays.

4.4 Example – general settings

An example of a DNP3.0 Ethernet Server to Modbus Serial Master Gateway follows. Assuming the following configuration

- Protocol Gateway – Server/Slave settings:
 - Protocol: DNP3.0 Server (from eNode Designer)
 - Interface: LAN 1
 - IP (from WebUI): 10.0.50.1
 - TCP Port: 20000 (from eNode Designer)
 - Connected to: DNP3.0 Client PLC

- Protocol Gateway – Client/Master
 - Protocol: Modbus RTU (from eNode Designer)
 - Interface: RS-485, port 1
 - Baud rate: 19,200 bps
 - Data bits: 8
 - Stop bits: 1
 - Parity: none
 - Connected to: Modbus RTU sensor
 - Modbus RTU device ID: 157

- Client/Master Polling configuration (eNode Designer):
 - Device to be polled: Modbus ID 157
 - Function: 03 read status registers
 - Starting address: 10
 - Quantity: 2
 - Polling time: 200 ms
 - Timeout: 100 ms

- Server/Slave Data points (eNode Designer)
 - Number of points: 10

- Data Type: word
- Data points mapping (eNode Designer)
 - Modbus 0-1 >> DNP3.0 5-4

4.5 Example - Polling process

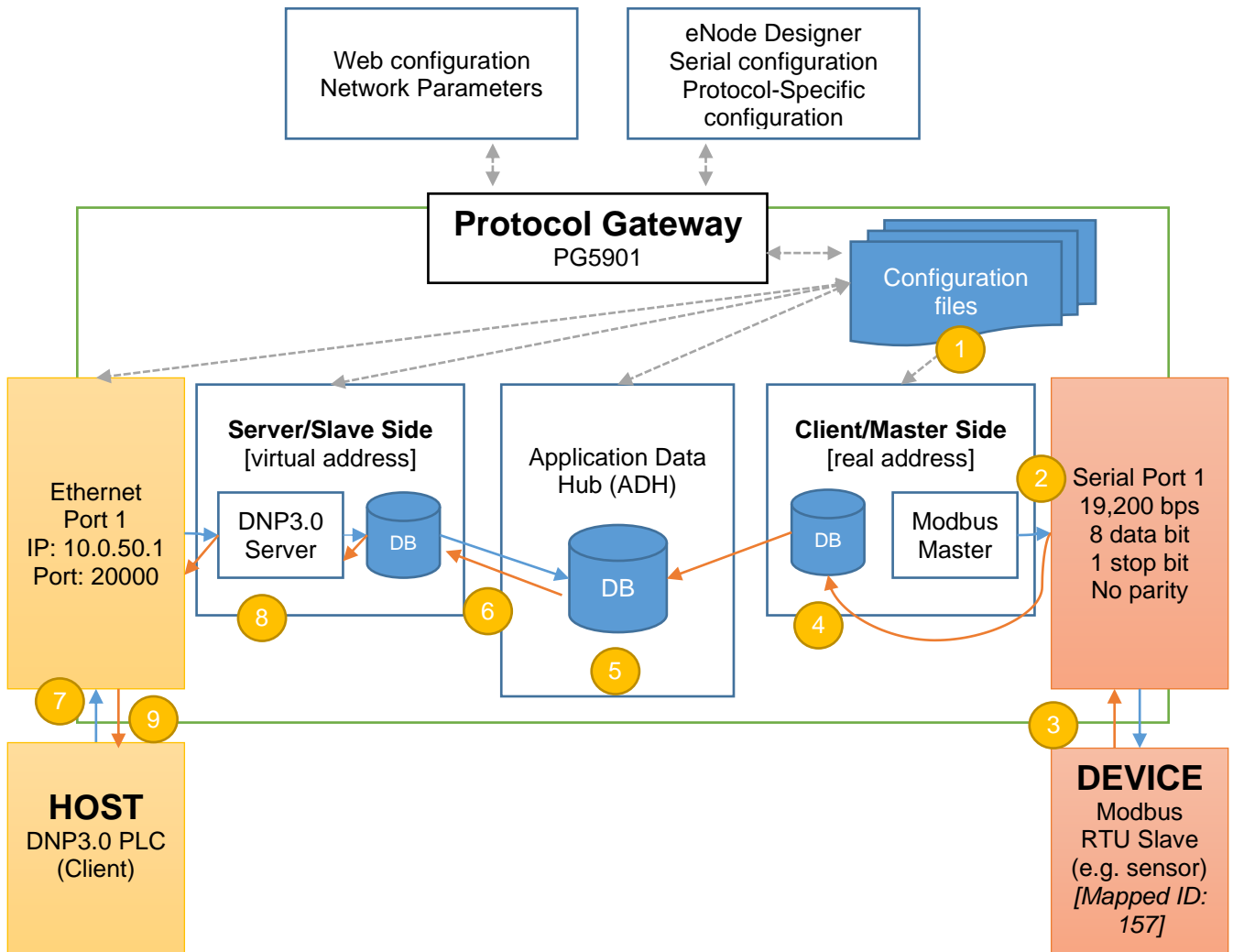


Figure 4-3 – Protocol Gateway Polling Process

- 1 The configuration file from eNode designer is successfully uploaded to ATOP’s Protocol Gateway
- 2 Following the configuration, Serial port 1 polls Modbus ID# 157, function 03, address 10 quantity 2. Serial port works with 19,200 bps, 8 data bits, 1 stop bit, no parity
- 3 Modbus device returns the data read for the 2 registers, the data is “FF” hexadecimal for register 0 and “06” hexadecimal for register 1
- 4 The data is stored into Modbus Client/Master database
- 5 The data is synced with the ADH database. The value “FF” hexadecimal is mapped automatically to DNP3.0 address 5 and the value “06” hexadecimal is mapped automatically to address 4 with the related timestamp.

- 6 The data is synced with the DNP3.0 Server/Slave database. The process from 2~6 is repeated automatically every 200 ms according to the configuration in eNode designer. In case of a communication error, an event may be issued (depending on the protocol)
- 7 The DNP3.0 client (e.g. a PLC) issues a read command to the DNP3.0 gateway with IP 10.0.50.1 on TCP port 20000, asking for addresses 4~5
- 8 ATOP's Gateway DNP3.0 server module returns to the DNP3.0 client "06" hexadecimal and "FF" hexadecimal (as respectively addresses 4 and 5)
- 9 DNP3.0 client receives the data.

4.6 Example: Command process

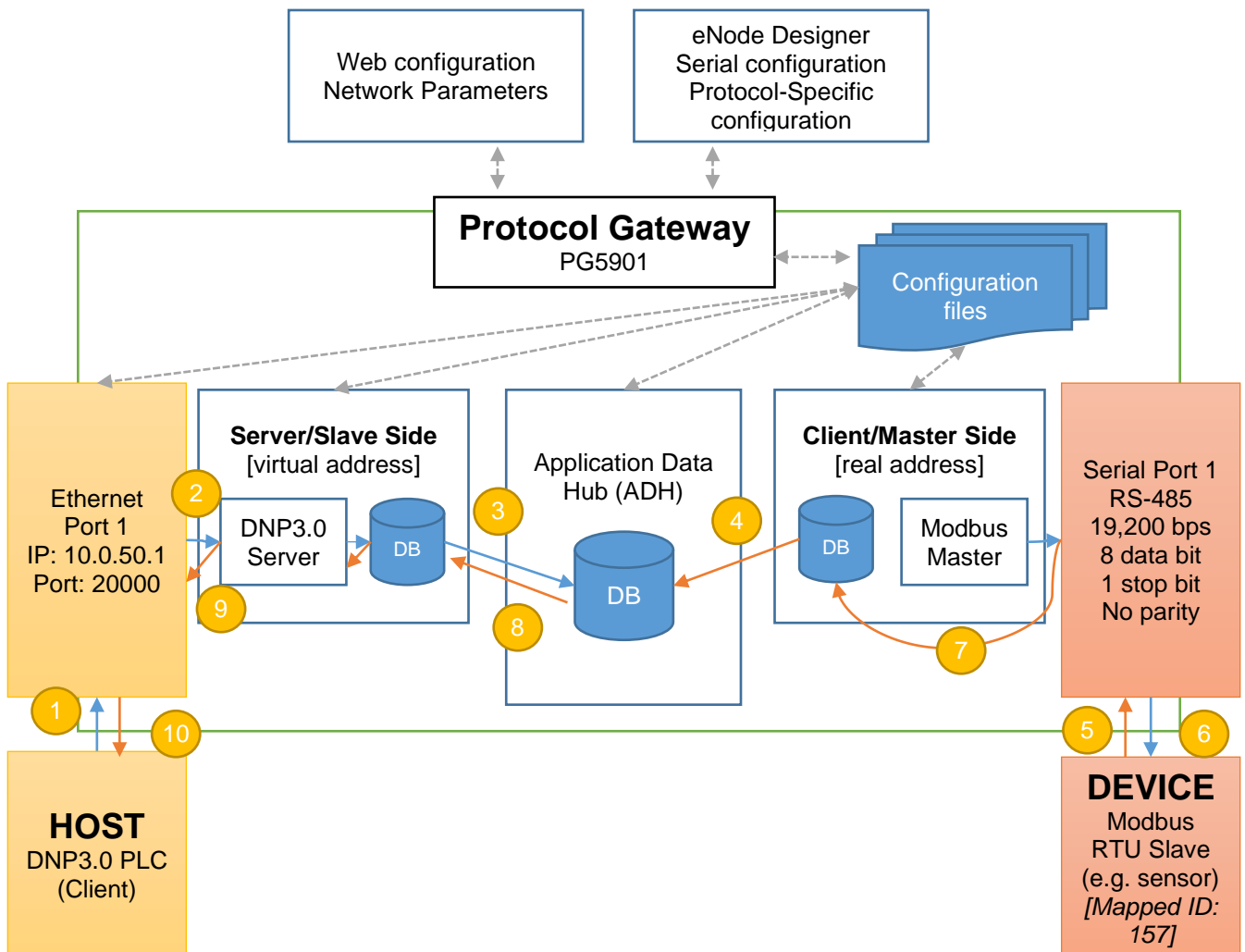


Figure 4-4 – Protocol Gateway Command Process

- 1 The DNP3.0 client issues a write command/ Select-Before-Operate command to ATOP's protocol gateway (IP 10.0.50.1; port 20000; connected to power 1)
- 2 The DNP3.0 server module on ATOP's protocol gateway receives the command and places it into the server command database
- 3 DNP3.0 Server command database is Synced with ADH database, where the command address/ write information is mapped to Modbus ID/ write command.
- 4 ADH database syncs with Modbus Client/Master.
- 5 Modbus Client/Master issues a Modbus command to the designated ID (157) with the Serial port parameters set in eNode designer (Baud rate: 19,200 bps, 8 data bits, 1 stop bit, no parity) and waits for Modbus device response within the timeout set.
- 6 The Modbus Slave responds to the command.
- 7 Modbus Client/Master receives the response and syncs with the Modbus module database.

- 8 The ADH database is synced and the information mapped back to DNP3.0 according to the settings made in eNode designer.
- 9 DNP3.0 server module syncs the information from ADH and issues the response to the DNP3.0 client.
- 10 DNP3.0 client receives the command execution confirmation or the exception.

4.7 eNode Designer Overview

The overall goal of eNode Designer is to configure target platforms, set device properties and ADH data point mapping. To do this, a project file representing the system should be created. This will include devices and the ADH applications running on them. The configuration is completely dependent on the “eNode Module” which represents that device or application – but may include things such as changing the communication port settings and defining where data point information enters and leaves the eNode Designer system.

Each target platform is represented by a “Device” eNode Module. This device may specify what communication ports it has, e.g. two Ethernet ports ETH1 and ETH2, and a serial port COM1.

Each ADH applications is represented by an “ADH Application” eNode Module. The module can be added to devices at an appropriate location. For example, a Modbus application can be linked to the COM1 port, while a PLC application can be added directly to the device itself (i.e. not bound to a communication port).

Each eNode module can add data points to eNode Designer that can then be mapped amongst the system.

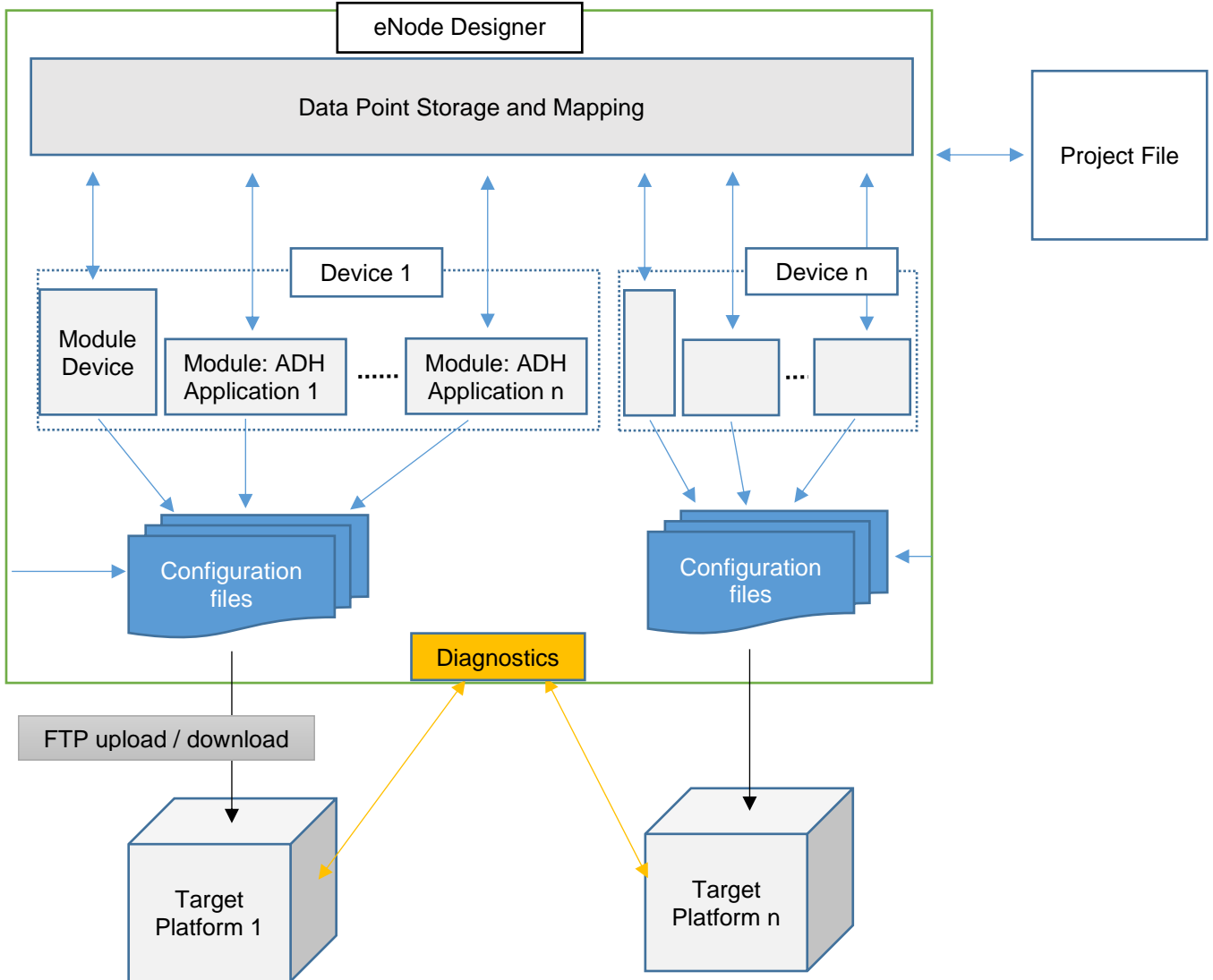


Figure 4-5 - eNode Designer overview.

eNode Designer also contains diagnostics capability – this includes reading the current values and health status of data points in the system and reporting back to the user.

5 eNode designer User Guide

5.1 Installation

The eNode Designer is being shipped with installer software for easy installation on a Windows™ based personal computer.

Minimum system requirements are:

- Windows 7 operating system or higher
- Java version 8 or higher installed on the computer
- One mouse device or mouse pad installed
- At least 1 GByte free hard disk space
- At least 500 Mbyte of free RAM
- Ethernet port for sending configuration files.

It is recommended to use at least a 17 Inch monitor when installing on a desktop type computer.

Installing the eNode Designer is easy. All files are self-extracting.


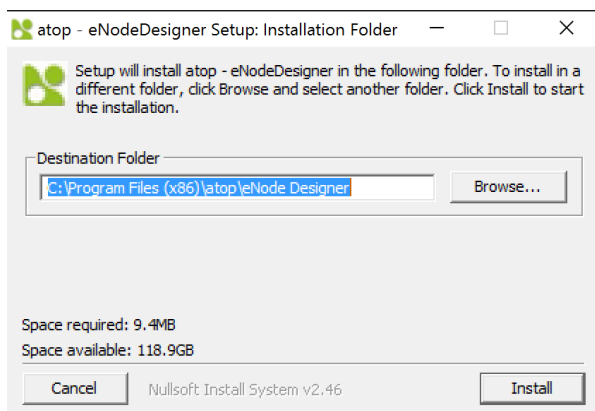
Name	Date modified	Type	Size
 eNodeDesignerSetup.exe	12/31/2015 9:39 AM	Application	5,658 KB

Figure 5-1 - eNode Designer Setup Installer

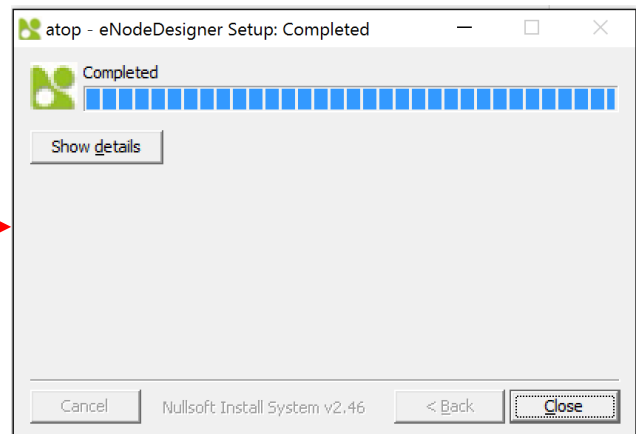
1

Run the **eNodeDesignerSetup.exe** program to install the eNode Designer.

The **User Account Control** window may appear asking to allow the application to make changes to the current computer settings. Click “Yes” to continue. Then the following window will appear.



Click **Install** to start installation



Click **Close** to complete installation. The program will show up in the Program menu and can be started from there

5.2 Main Screen

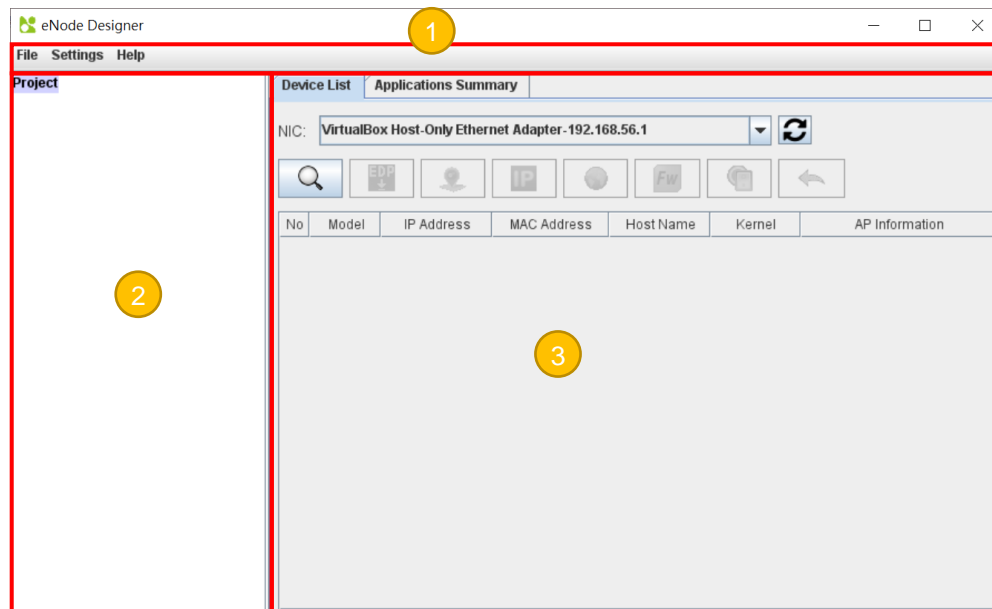


Figure 5-3 - eNode Designer main screen.

Throughout this document, all the screens and menus show what an eNode Designer user sees. There may be differences on the exact appearance, but the principals are the same. The three major parts of the eNode Designer screen are described below.

- 1 **Menu Bar** – contains various options available to the user, such as saving and loading projects.
- 2 **Project Tree** – shows the contents of the current project represented as a tree.
- 3 **Main Display Area** – displays according to what is selected in the project tree.

5.3 Login

In order to start using eNode Designer, you will first need to login. Type in your username and password, and press enter (or click Login) to login. If your details are correct, you will be brought into the main eNode Designer screen.

When eNode Designer is run for the first time, it will have one user:

Username: admin

Password: admin

It belongs to the "Administrator" user group, which by default has full permissions. After logging in for the first time it is recommended to change the username and password. See section 5.4 for details.



Figure 5-4 - Splash screen and login window.

5.4 User Administration

Each “User” login belongs to a “User Group” which defines the permissions of all users in that group.

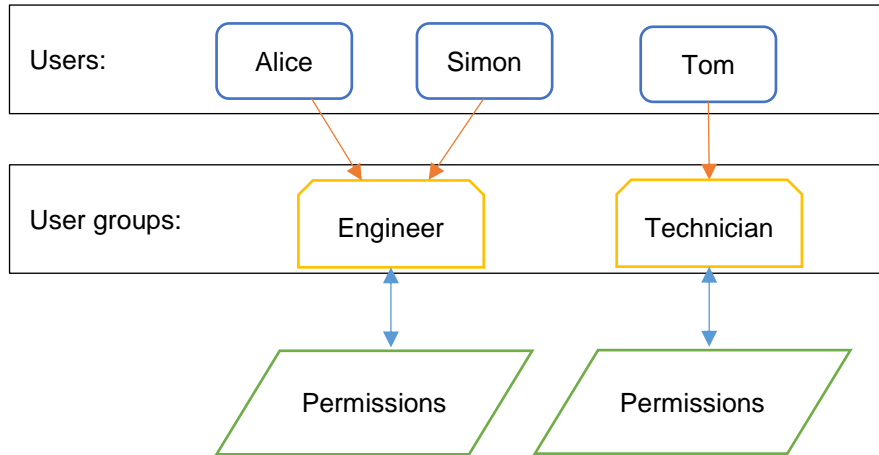


Figure 5-5 - User administration principal.

Adding, editing and removing users and user groups is achieved through the user administration menu.

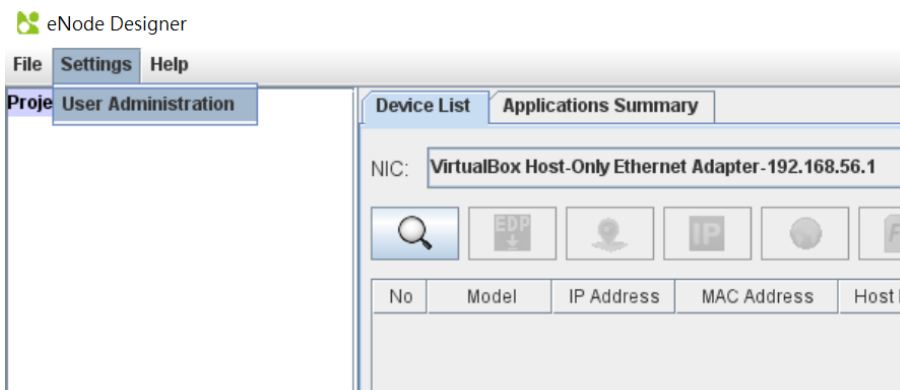


Figure 5-6 - Access user administration.

5.4.1 Creating, modifying and removing users.

To define users, use the “Users” tab of the user administration window. The three buttons are explained below:

- Add** This function adds a new user. The user will be prompted for the username, password and the user group the user will belong to.
- Edit** This function modifies the username and password of an existing user. The user should select the user in the table first.
- Remove** This function removes the selected user from the system. The user should select the user in the table first.

For example, to add the user “Alice” with user group “Engineer”, you can use the add button, set the information and click OK.

錯誤! 使用【常用】索引標籤
將 **Heading 1,Product
Manual** 套用到您想要在此
處顯示的文字。

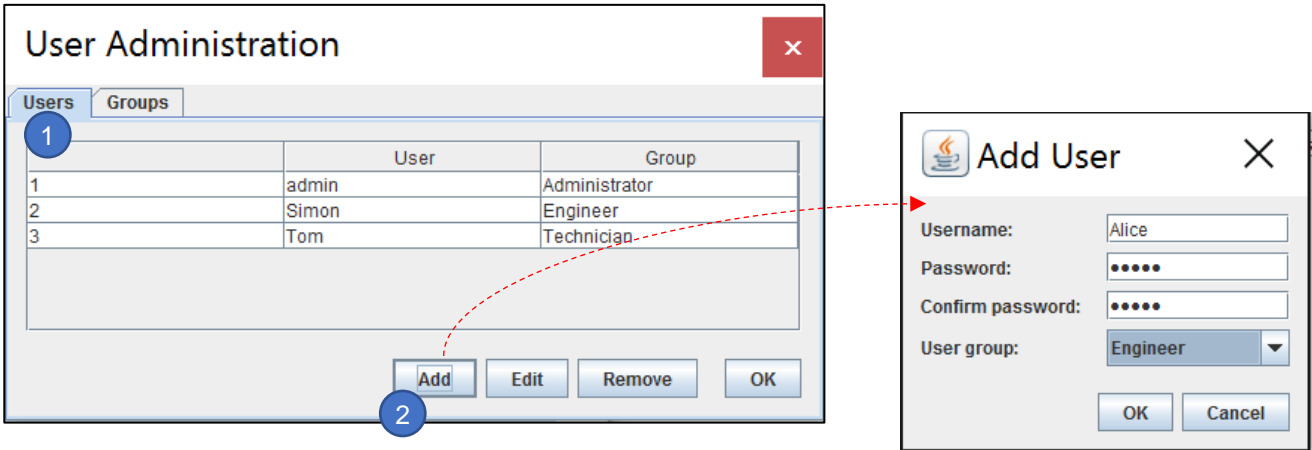


Figure 5-7 - Adding a new user.

This will add a new user who can login to eNode Designer with username “Alice” and the specified password. You can change the user group of a user by using the drop-down option in the user administration window.

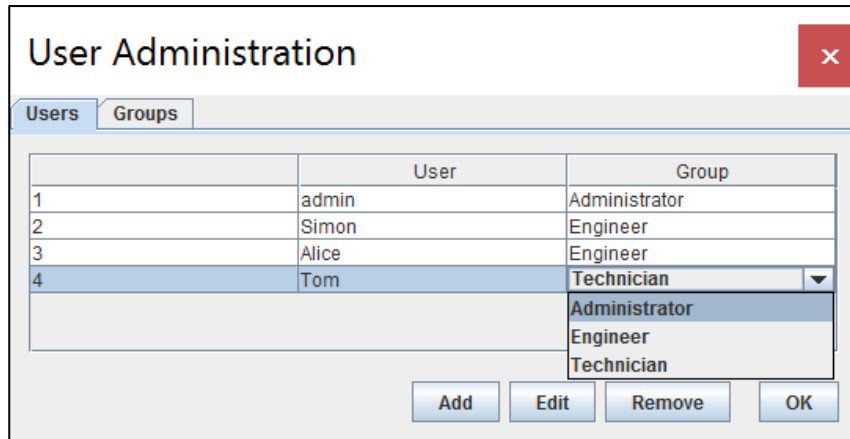


Figure 5-8 - Changing a user's user group.

5.4.2 Defining User Groups

To add a user group, move to the user groups tab and use the “Add” button.

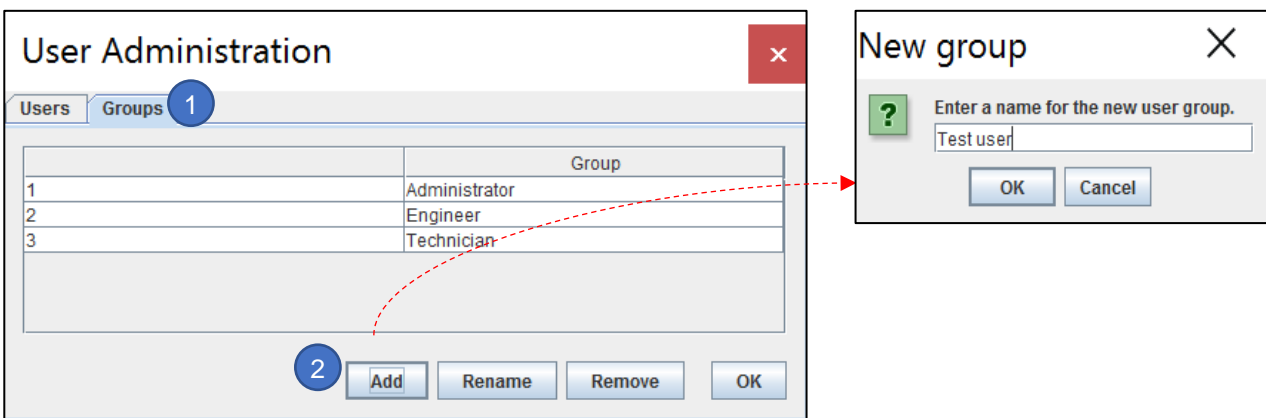


Figure 5-9 - Adding a user group.

You will be prompted to type a name for the user group, and then it will be added to the list. Users can then be added for that user group. All users with that user group will have the same permissions.

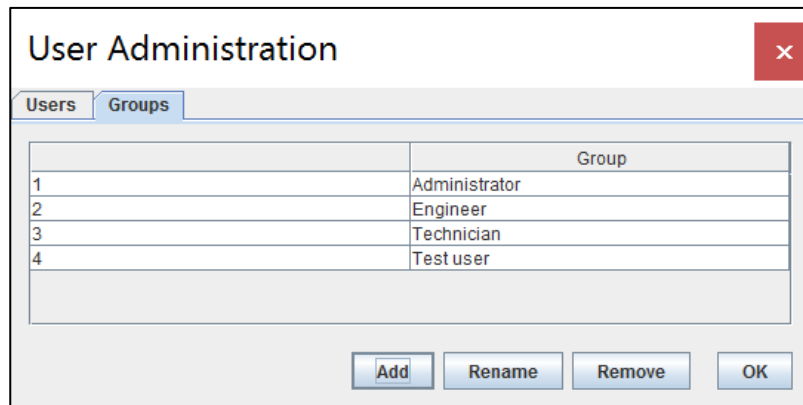


Figure 5-10 - User group added.

Other actions such as renaming the group and changing the permissions can be accessed by using the associated buttons after selecting which group you want to change.

Add **Adds** a new user group.

Rename **Renames** the selected user group.

Remove **Removes** the selected user group from the system.

5.5 Creating a project

By default, starting eNode Designer will load the last open project. The first time it runs it will start with a new project. The next time, it will open the last edited project.

Creating, changing and removing the contents of a project is achieved through the right-click menu on the project tree. The right click menus are context sensitive – right clicking the project node will have different options to when right clicking a device or ADH application.

5.5.1 Project Root

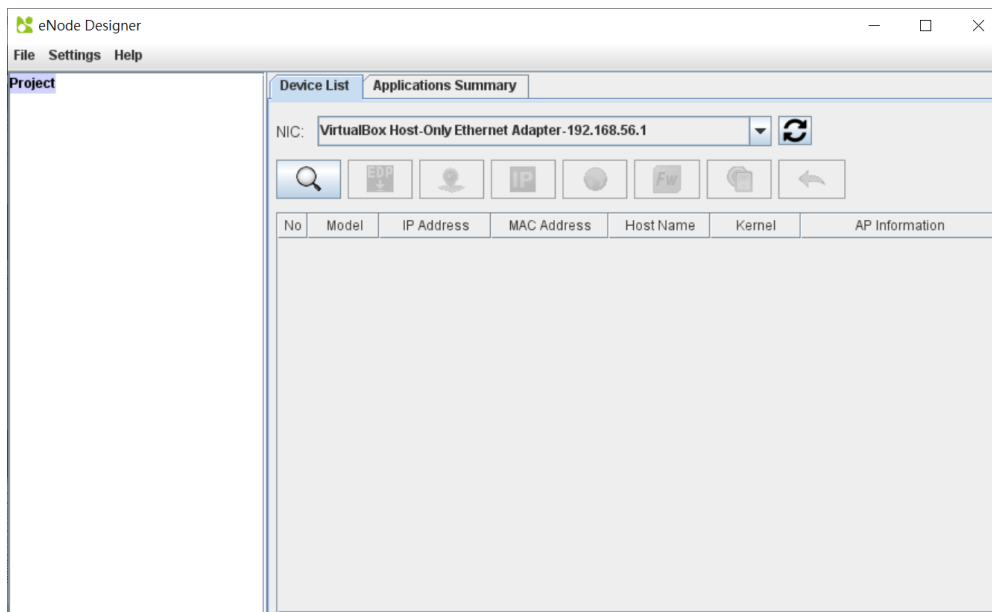


Figure 5-11 - Project Root

The project information pane is shown when the project root is selected in the project tree. Here the user can enter details about the project including a project name, description, author(s) and version history.

5.5.2 Adding a Device (a.k.a. Target Platform or CFE)

Once modules are known to eNode Designer (i.e. visible in the Module Management window, see section 錯誤! 找不到參照來源。) They can be added to the project. Since ADH Applications must have a platform to run on, the target platform must be added to the project first. This can be achieved through the right-click menu on the project tree root.

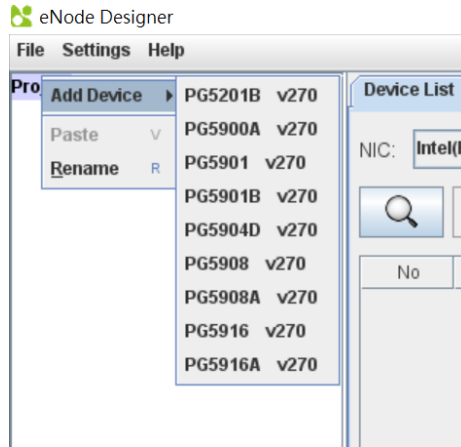


Figure 5-12 - Adding a device to the project.

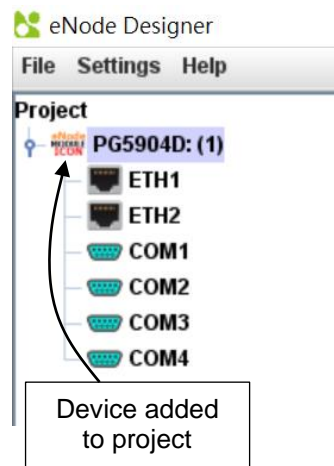


Figure 5-13 - Device added to project.

In this example, we have added a device with two Ethernet ports and four serial ports. More than one Device can be added to the project using the same process.

5.5.3 Editing Ethernet Port Properties

While the device-specific IP addresses can be set via Web interface (Refer to Chapter [Network Configuration](#)) or via Device View (Refer to Chapter [Configuration of Network Parameters through Device View](#)) eNode designer requires the user to specify the device’s properties in the project file too.

This is necessary in order to identify the device to which the configuration should be uploaded to uniquely among the networks.

In this example, the ETH1 port is set to IP address 192.168.1.115, Subnet mask to 255.255.255.0 and Default Gateway to 192.168.1.254.

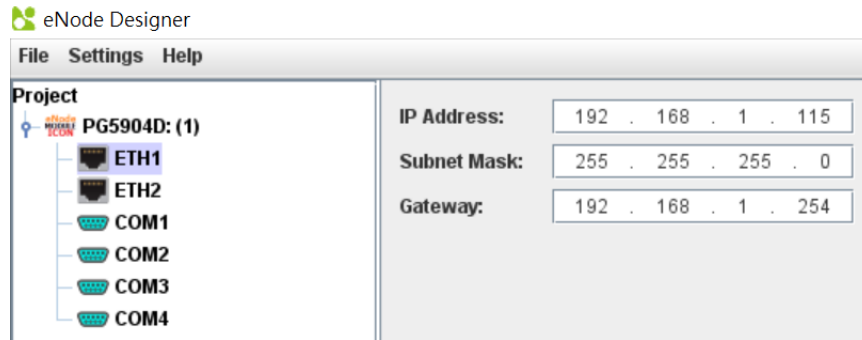


Figure 5-14 – Network properties modified.

5.5.4 Editing Communication Port Properties

It depends on the device module, but generally you can edit the properties of the communication ports by clicking the appropriate item in the project tree.

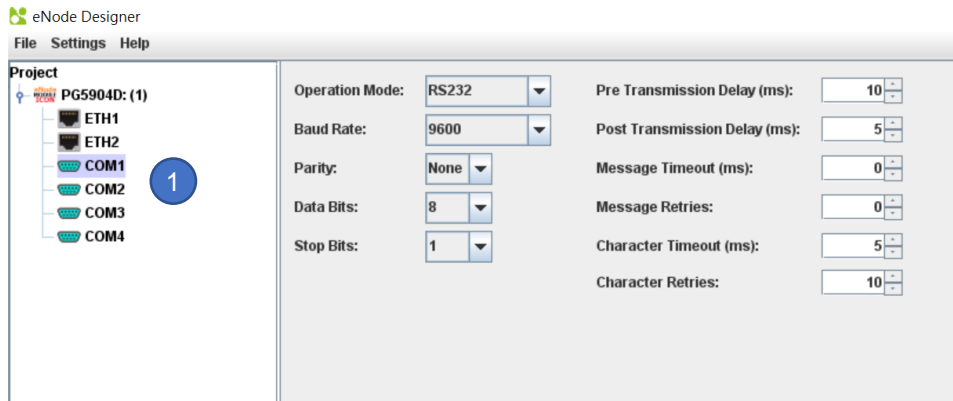


Figure 5-15 - Editing communication port settings example.

5.5.5 Adding an ADH Application to a Communication Port

ADH Applications can be added to the appropriate locations on the device via the right-click menus. Some eNode Designer Modules must be added on communication ports, while others may run on the device directly.

For example, an IEC 60870-5-101 application can run on serial ports only, so an IEC 60870-5-101 ADH Application could be added to the COM1, COM2, COM3, COM4 only. This IEC 60870-5-101 option will not show up for the Ethernet port since this protocol cannot run on Ethernet.

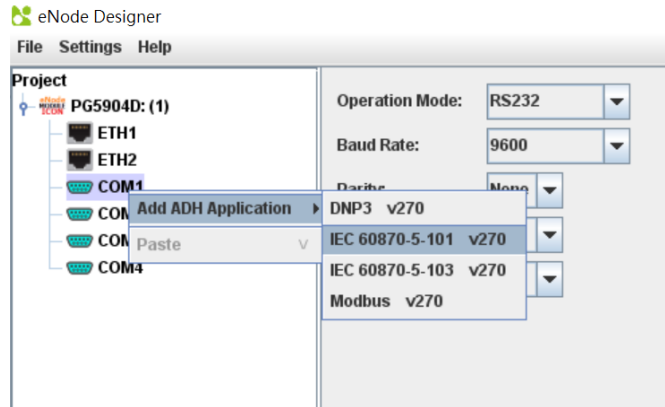


Figure 5-16 - Add ADH Application to communication port example.

When a Client/Server choice is possible for ADH Applications, such as IEC 60870-5-101, you will see a window like Figure 5-17.

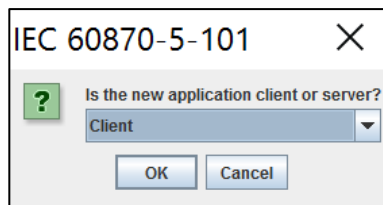


Figure 5-17 - Choosing client or server.

Use the dropdown menu to choose the client or server option, then click OK. ATOP protocol gateway supports one server application per protocol per device.

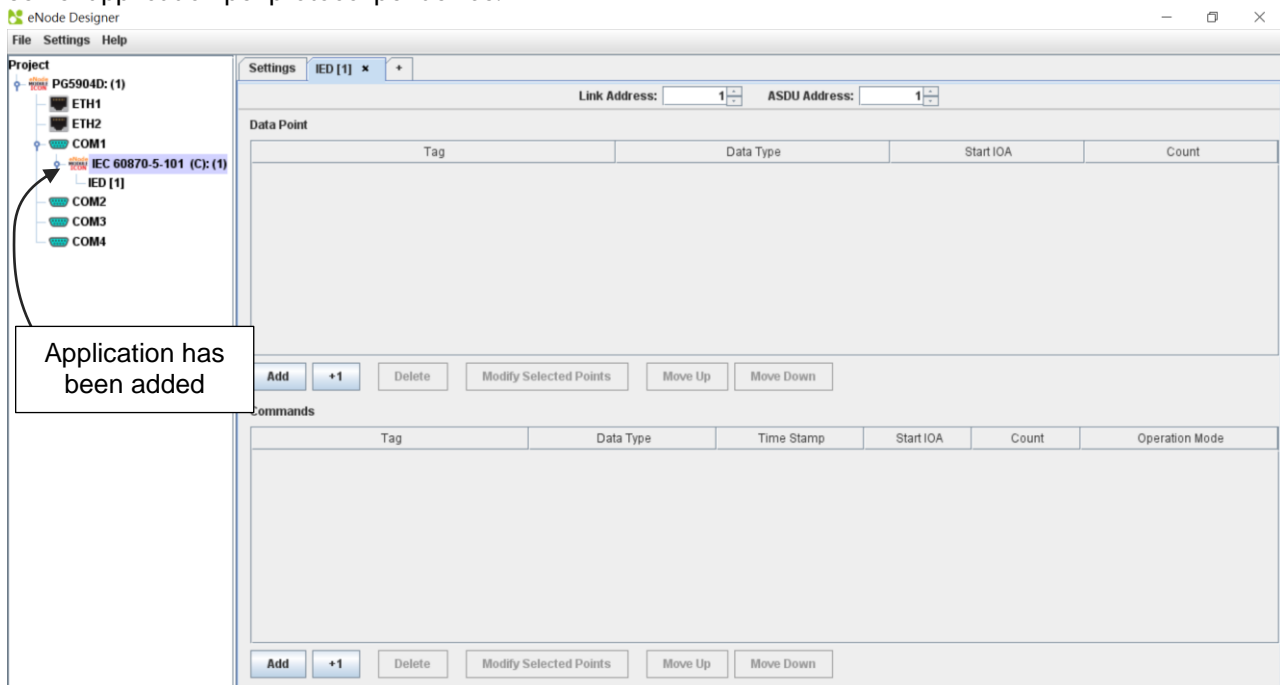


Figure 5-18 - ADH Application added to project.

Here the application has been added to the project, as a client. By default, new modules will be selected, and so their pane will be shown in the central area. How to configure an eNode Module is described in that module's user manual.

5.6 Data Points

Because creating data points is handled by the eNode Modules themselves, exactly how it looks is up to the respective module, so the screens cannot be described here. However, the general process is client applications produce data points, which are raised up to eNode Designer. These points can then be mapped to server applications. Most server applications will have a way to add references, which will bring up the following window.

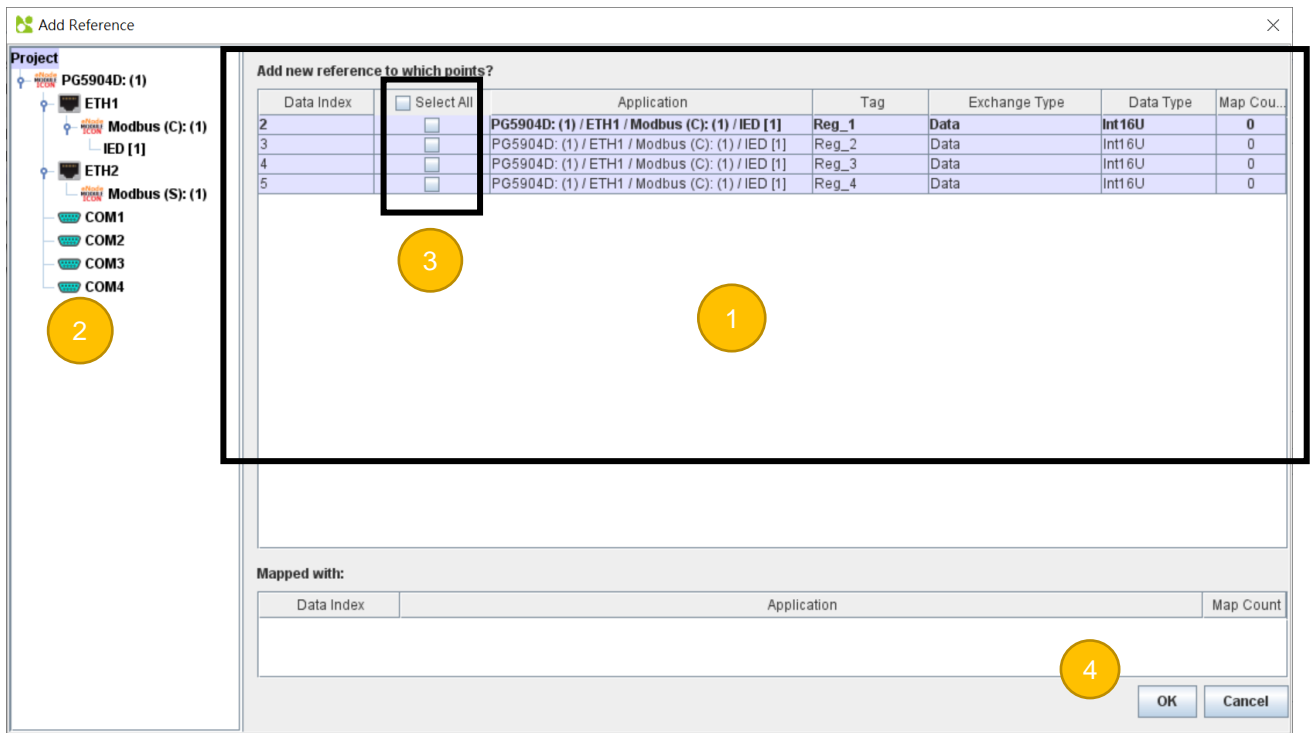


Figure 5-19 - Adding data point references.

- 1 **Point display area** – this shows the existing points in the system which can be mapped to the eNode Module which generated this window. Note that some modules may be restricted in what data types they may accept. For example, some may not have a 32-bit floating-point number type. So, 32-bit floats will not show in the list.
- 2 **Filter by Tree Selection** – the points display area shows only points beneath the selected tree node.
- 3 **Map Selection** – click the checkboxes to add a reference to that data point.
- 4 **Click OK** – to add the new reference(s).

5.7 Generate and Send Configuration Files

When all data points and mapping have been completed, you can generate and send the project configuration files to the target platforms.

5.7.1 Setting up the FTP Details

Sending the files works by FTP (File Transfer Protocol), so first the FTP settings must be set in eNode Designer. To do this, right click the device in the project tree and select “Device Settings”.

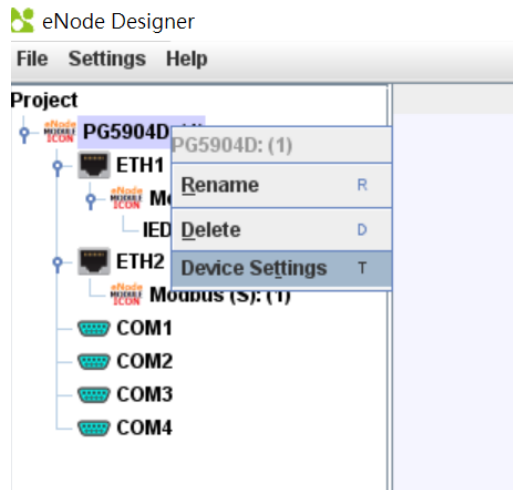


Figure 5-20 - Access device settings to set FTP settings.

This will bring up a new window in which you can set the FTP settings. This includes settings the Ethernet channel used for FTP, the username, password and port. On some devices, the configuration directory is also configurable.

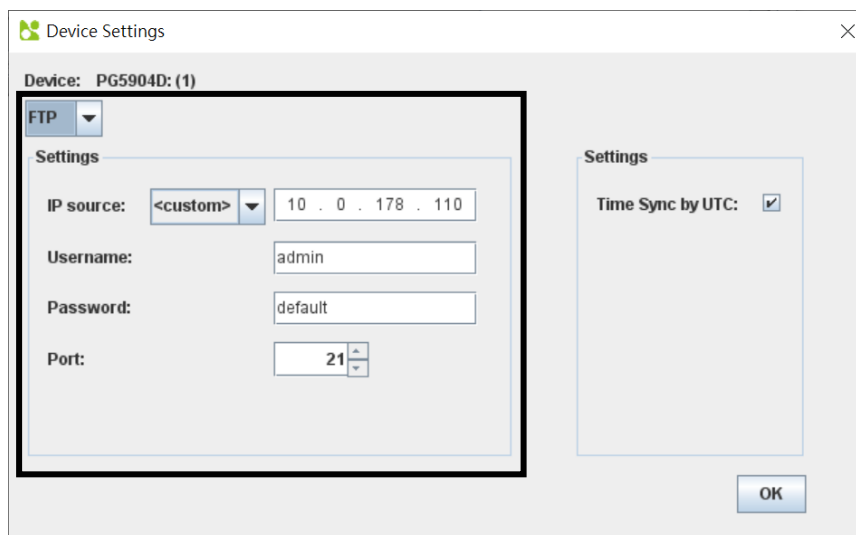


Figure 5-21 - Device settings window.

The IP address is extracted from the Ethernet’s properties configured in the project. If there are multiple Ethernet ports on the device, use the dropdown box to select which of the device’s Ethernet ports is to be connected to the PC running eNode Designer.

Note: If the device's Ethernet properties are going to be configured by the project, place the desired IP addresses in the project, and then use the FTP IP source as "Custom" and type in the current IP address of the device. This may be necessary when receiving a product from a manufacturer in which the IP address is pre-set and needs to be changed.

5.7.2 Send the Configuration

Once all the FTP settings of devices have been set, you can send the configuration files to them. Because sending configuration files is a significant event, you will first be prompted to add a new version to the version history.

The configuration files for all the devices and applications will be generated and stored on the local hard drive ready to be sent to the device. When completed, the send configuration files window will show.

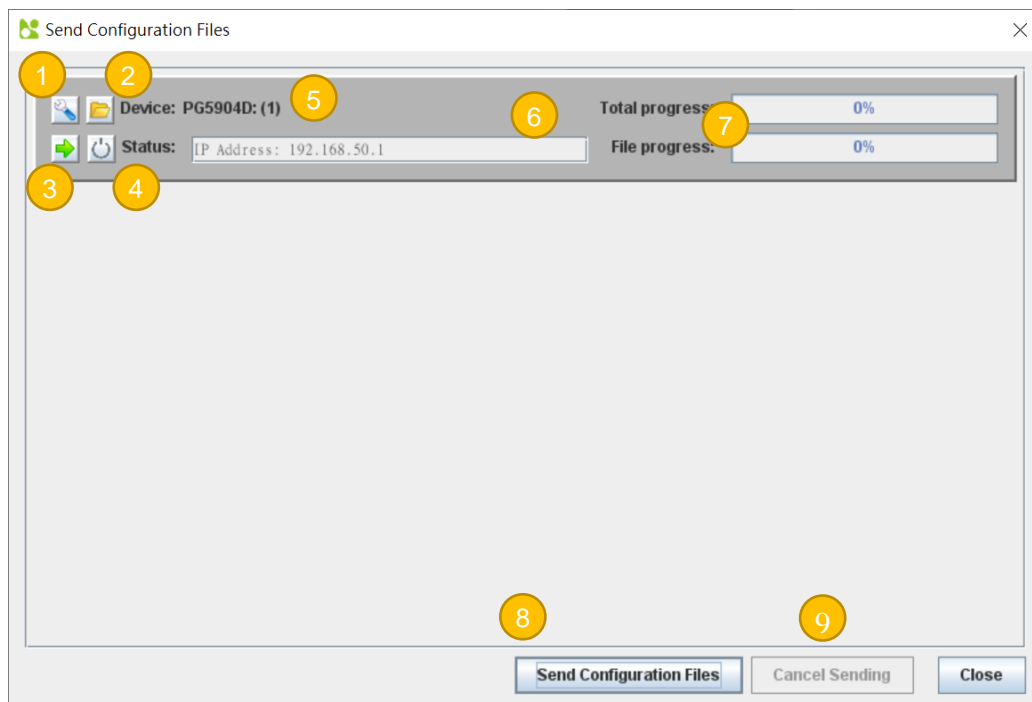
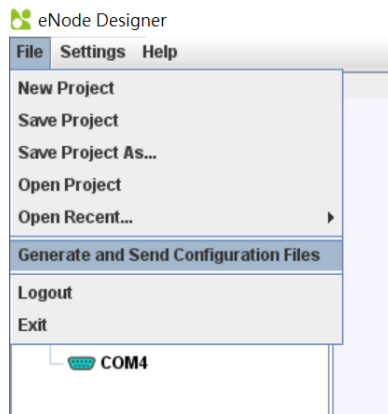


Figure 5-22 - Send configuration files window.

There are descriptions of the buttons and fields below.

- 1 **Open Device Settings** – Can be used to change FTP settings as in **Figure 5-21**.
- 2 **Open Configuration Directory** – Opens the local directory in which the configuration files were generated.
- 3 **Send to Device** – Sends the configuration files to the individual device by FTP.
- 4 **Reboot Device** – Sends a reboot command to the diagnostic application currently running on the device.
- 5 **Device Name** – Textual representation of the full path to the device in the project tree.
- 6 **Status** – The status of sending the files.
- 7 **Progress Indication** – Shows the progress of the file transfer
- 8 **Send All** – Sends the configuration files to all devices.
- 9 **Cancel Sending** – Cancels sending the configuration files.

After sending the files has completed, a dialog will show asking the user if they want to reboot the devices.

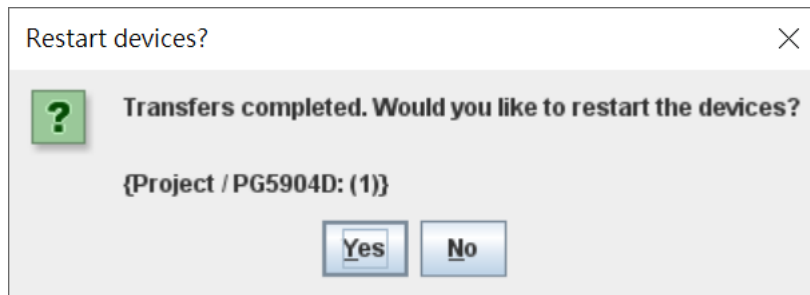


Figure 5-23 - Asked to reboot after sending configuration files.

The applications on the target platforms will require a restart to load the new configuration files.

6 eNode designer Reference Guide

6.1 Menu Bar Options

6.1.1 File

Function	Description
<i>New Project</i>	Creates a new empty project.
<i>Save Project</i>	Saves the current project.
<i>Save Project As...</i>	Saves the current project as a new file.
<i>Open Project</i>	Loads an eNode Designer project.
<i>Open Recent</i>	Shows recent project files for faster processing.
<i>Generate and Send Configuration Files</i>	Generates and sends the target platform settings and ADH application configuration files to the target platforms. See section Generate and Send Configuration Files 5.7 for details.
<i>Logout</i>	Logs out of the current user.
<i>Exit</i>	Exits eNode Designer.

6.1.2 Settings

Function	Description
<i>User Administration</i>	Opens the user administration window, allowing editing users and user groups.

6.1.3 Help

About Shows information about the eNode Designer version and copyright notice.

6.2 Tree Menu Options

Menu Item	Description	Availability
<i>Add Group</i>	Adds a new group to the project	Root, group
<i>Add Device</i>	Adds a new device to the project	Root, group
<i>Add ADH Application</i>	Adds a new ADH Application to the project	Device, valid communication port
<i>Copy</i>	Copies the tree node (for pasting)	All but communication port
<i>Cut</i>	Cuts the tree node (for pasting)	All but communication port
<i>Paste</i>	Pastes the copied or cut tree node	All
<i>Rename</i>	Rename the tree node	All
<i>Delete</i>	Removes the tree node (and descendants) from the project.	All but communication port
<i>Device Settings</i>	Opens the device settings window. Includes options to set ADH Ethernet channel and SFTP settings.	Device

Table 6-1 - Tree context menu options.



ATOP Technologies, Inc.

www.atoponline.com

www.atop.com.tw

TAIWAN HEADQUARTERS

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Zhubei City, Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137

E-mail: info@atop.com.tw

Fax: +886-3-550-8131

ATOP INDIA OFFICE & GLOBAL INQUIRIES

Prashant Mishra

No. 3M-217, East of NGEF Layout, Kasturi Nagar,
Bengaluru- 560043, Karnataka, India

Tel: +91-80-492-06308

E-mail: prashant.m@atop.com.tw

ATOP CHINA BRANCH

Sam Xia

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China

Tel: +86-21-64956231

E-mail: info@atop.com.tw

ATOP INDONESIA OFFICE

Anisah Ambarwati

Wisma Slipi, Kav. 12 Lt. 3 Unit 308
Jl. Let. Jend. S. Parman 11480 - Indonesia

Tel: +6221-5326171

E-mail: anisah@atop.com.tw

ATOP JAPAN OFFICE

易傑 Takashi Eki

東京都千代田区丸の内 1-1-3

日本生命丸の内ガーデンタワー3F

Tel: +81-3-4530-3390

E-mail: eki@atop.com.tw

ATOP COLOMBIA OFFICE

Brenda Solano Sarmiento

Calle 35 No. 19 - 41 - Oficina 315 Torre Norte,
Bucaramanga, Santander, Colombia

Tel: +57 322 848 9815

E-mail: brenda.solano@atop.com.tw

ATOP VIETNAM CONTACT

Jenny Duong

Tel: +84 93 275 18 52

E-mail: jenny.duong@atop.com.tw

ATOP NORTH AMERICA CONTACT

Sam Leong

Tel: +1 323 315 0484

E-mail: samleong@atop.com.tw

ATOP EUROPE CONTACT

Timur Dautov

Tel: +48 690 261 220

E-mail: timur@atop.com.tw