Atop Technologies, Inc.

Getting started with PG59XX Protocol Gateway

Device Setup
Architectural overview
eNode Designer

User Manual

V1.4

December 19th, 2017

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 Chupei 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:	Matteo Tabarelli
Revision:	1.4
Revision History:	Software updates
Creation Date:	31 August 2016
Last Revision Date:	19 December 2017
Product Reference:	PG59XX Protocol Gateway Family
Document Status:	Released

Table of Contents

1 Introduction 8
1.1 Scope 8
1.2 Overview 8
1.2.1 List of Abbreviations 8
2 Getting Started 9
2.1 Packing List 9
2.2 How to order 10
2.3 First Time Installation 11
2.4 Factory Default Settings 11
3 Configuration and Setup 13
3.1 Configuration of Network Parameters through Device View 13
3.2 Configuration through Web Interface 15
3.3 LCM (Liquid Crystal Matrix) Configuration (PG5916 only) 16
3.4 Automatic IP Assignment configuration with DHCP 18
3.5 Web Overview 18
3.6 Network Configuration 19
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 IPsec Settings 24
3.9.1 IPsec Settings 27
3.9.2 Examples of IPsec Settings 32
3.10 System Setup 36
3.10.1 Time 36
3.10.2 Security 37
3.10.3 Restart 38
4 General Description 39
4.1 Protocol Gateway Overview 39
4.2 Device Client/Master 41
4.3 Device Server/Slave 41
4.4 Example – general settings 42
4.5 Example - Polling process 43
4.6 Example: Command process 45
4.7 eNode Designer Overview 47
5 eNode designer User Guide 48
5.1 Installation 48
5.2 Main Screen 49
5.3 Login 50
5.4 User Administration 51
5.4.1 Creating, modifying and removing users. 51
5.4.2 Defining User Groups 52
5.5 Importing eNode Modules 54
5.6 Creating a project 55
5.6.1 Project Information 55

5.6.2 Adding a Device (a.k.a. Target Platform or CFE) 55
5.6.3 Editing Ethernet Port Properties 56
5.6.4 Editing Communication Port Properties 57
5.6.5 Adding an ADH Application to a Communication Port 57
5.7 Data Points 59
5.8 Viewing the Database of Data Points 60
5.9 Generate and Send Configuration Files 61
5.9.1 Setting up the FTP Details 61
5.9.2 Send the Configuration 62
5.10 Diagnostics 63
5.11 Loading Projects from a Device 65
5.12 Organising a Project 67
5.13 Advanced – Tree Group Style Sheets 68
5.13.1 Editing the Style Sheets 68
5.13.2 Creating a Group with a Style Sheet 71
5.13.3 Changing and Existing Group's Style Sheet 73
5.14 Report Generation 74
5.14.1 Data Point Report Template 74
5.15 Settings 75
6 eNode designer Reference Guide 76
6.1 Menu Bar Options 76
6.1.1 File 76
6.1.2 Edit 76
6.1.3 View 76
6.1.4 Tools 77
6.1.5 Settings 77
6.1.6 Help 77
6.2 Tree Menu Options 77

Table of Figures

Figure 3-1 - List of Devices on Network in Device Management Utility 13
Figure 3-2 - Pull-down Menu of Configuration and Network 13
Figure 3-3 - Pop-up Window of Network Setting 14
Figure 3-4 - Authorization for Changes 14
Figure 3-5 - Overview web page of protocol gateway 15
Figure 3-6 – PG5900A/08A/16A menu structure 15
Figure 3-7 – Overview Page 18
Figure 3-8 – Network configuration Page, example on PG5900A/08A/16A 19
Figure 3-9 – Save completed Page 20
Figure 3-10 – Bonding settings 20
Figure 3-11 – Bonding status 21
Figure 3-12 – Virtual IP settings 21
Figure 3-13 – Redundancy settings 22
Figure 3-14 – IED conncetion statistics 23
Figure 3-15 – SNMP setting 23
Figure 3.16 An example of Host-to-Host Connection 24
Figure 3.17 Roadwarrior Application using Host-to-Subnet Connection 25
Figure 3.18 Gateway Application using Host-to-Subnet Connection 25
Figure 3.19 An example of network application using a subnet-to-subnet connection via the PG59XX and a peer device. 25
Figure 3.20 An example of host-network application via the subnet-to-subnet connection 26
Figure 3.21 An example of host-host application via the subnet-to-subnet connection 26

Figure 3.22 IPsec Tunnels Web Page under IPsec Setting Menu 27
Figure 3.23 IPsec VPN Tunnel with Host-to-Host Topology 32
Figure 3.24 General Settings for Host-to-Host with Static Peer 33
Figure 3.25 General Settings for Host-to-Host with Dynamic Peer 33
Figure 3.26 IPsec VPN Tunnel with Host-to-Network Topology 34
Figure 3.27 General Settings for Host-to-Network with Static Peer 34
Figure 3.28 General Settings for Host-to-Network with Dynamic Peer 35
Figure 3-29 – Time settings Page 37
Figure 3-30 – Admin settings Page 37
Figure 3-31 – Entering the User Name and the New Password 37
Figure 3-32 – Web mode settings 38
Figure 3-33 – Restart page 38
Figure 4-1 – Protocol Gateway Application Example 39
Figure 4-2 – Protocol Gateway Architectural overview 40
Figure 4-3 – Protocol Gateway Polling Process 43
Figure 4-4 – Protocol Gateway Command Process 45
Figure 4-5 - eNode Designer overview. 47
Figure 5-1 - eNode Designer Setup Installer 48
Figure 5-2 - eNode Designer setup wizard. 48
Figure 5-3 - eNode Designer main screen. 49
Figure 5-4 - Splash screen and login window. 50
Figure 5-5 - User administration principal. 51
Figure 5-6 - Access user administration. 51
Figure 5-7 - Adding a new user. 52
Figure 5-8 - Changing a user's user group. 52
Figure 5-9 - Adding a user group. 52
Figure 5-10 - User group added. 53
Figure 5-11 - Getting to the module management window. 54
Figure 5-12 - Import eNode Module example 54
Figure 5-13 - Project Information 55
Figure 5-14 - Adding a device to the project. 56
Figure 5-15 - Device added to project. 56
Figure 5-16 – Network properties modified. 56
Figure 5-17 - Editing communication port settings example. 57
Figure 5-18 - Add ADH Application to communication port example. 57
Figure 5-19 - Choosing client or server. 57
Figure 5-20 - ADH Application added to project. 58
Figure 5-21 - Adding data point references. 59
Figure 5-22 - Accessing the data points view. 60
Figure 5-23 - Data point view window. 60
Figure 5-24 - Access device settings to set FTP settings. 61
Figure 5-25 - Device settings window. 61
Figure 5-26 - Send configuration files window. 62
Figure 5-27 - Asked to reboot after sending configuration files. 63
Figure 5-28 - Starting diagnostics. 64
Figure 5-29 - Diagnostics screen explained. 64
Figure 5-30 - Browse project history of a device in the project. 65
Figure 5-31 – Browse project history of a device unknown to the project. 66
Figure 5-32 - Browse project history. 66
Figure 5-33 – Project tree organisation. 67
Figure 5-34 - Project tree group example. 68
Figure 5-35 - Style sheet interaction with groups. 68
Figure 5-36 - Accessing the style sheets. 69
Figure 5-37 - Edit style sheets window. 69
Figure 5-38 - Style sheet example one. 70
Figure 5-39 - Style sheet example two. 71
Figure 5-40 - Adding a group to the project. 72
Figure 5-41 - Group with style sheet has been added. 72
Figure 5-42 - Change the style sheet of existing group. 73

Figure 5-43 - Open report templates directory. 74
Figure 5-44 - Data point report template. 74
Figure 5-45 - Settings window. 75

List of Tables

Table 3.1 Description of Parameters in IPsec Tunnels Web Page 31
Table 6-1 - Tree context menu options. 77

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

AAP = Alarm Annunciator Panel
ADH = Application Data Hub
CFE = Communication Front End
EDM = eNode Designer Module
FTP = File Transfer Protocol
PDF = Portable Document Format
RAM = Random Access Memory

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 ● DIN-Rail Kit (x 1) or PG5908, PG5916, PG5900A, PG5908A, PG5916A Series ● Rack Mounting Type-L angles (x 2) ● Screws (x 6)
Terminal block		PG5904D and PG5904D-Sis ● 7-pin, 2ESDVM-07P (x 1) ● 5-pin, EC381VM-05P (x 4) for PG5904D-Sis-X only PG5901, PG5908, and PG5916 Series ● 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 is 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

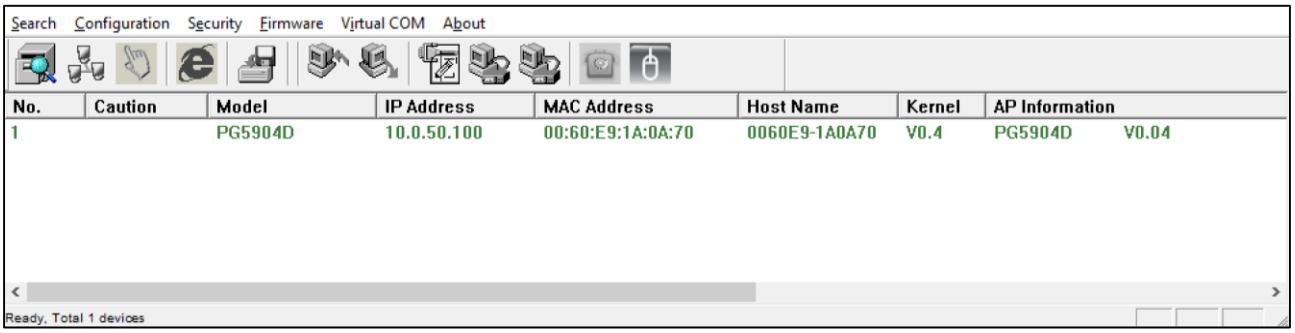


Figure 3-1 - List of Devices on Network in Device Management Utility

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.

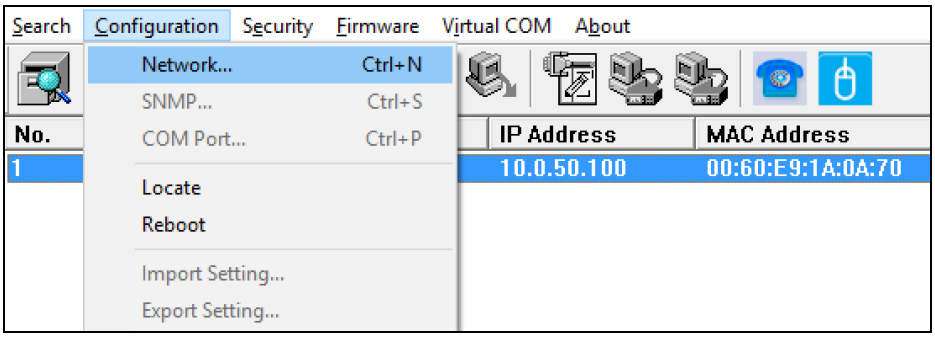


Figure 3-2 - Pull-down Menu of Configuration and Network

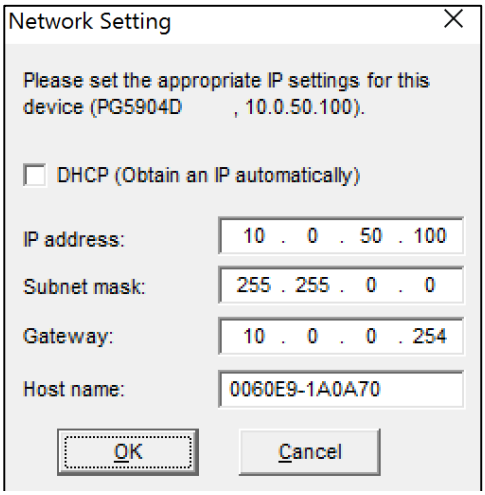


Figure 3-3 - Pop-up Window of Network Setting

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.

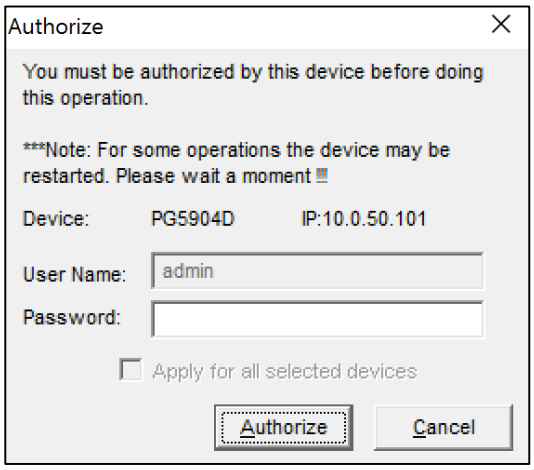


Figure 3-4 - Authorization for Changes

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.

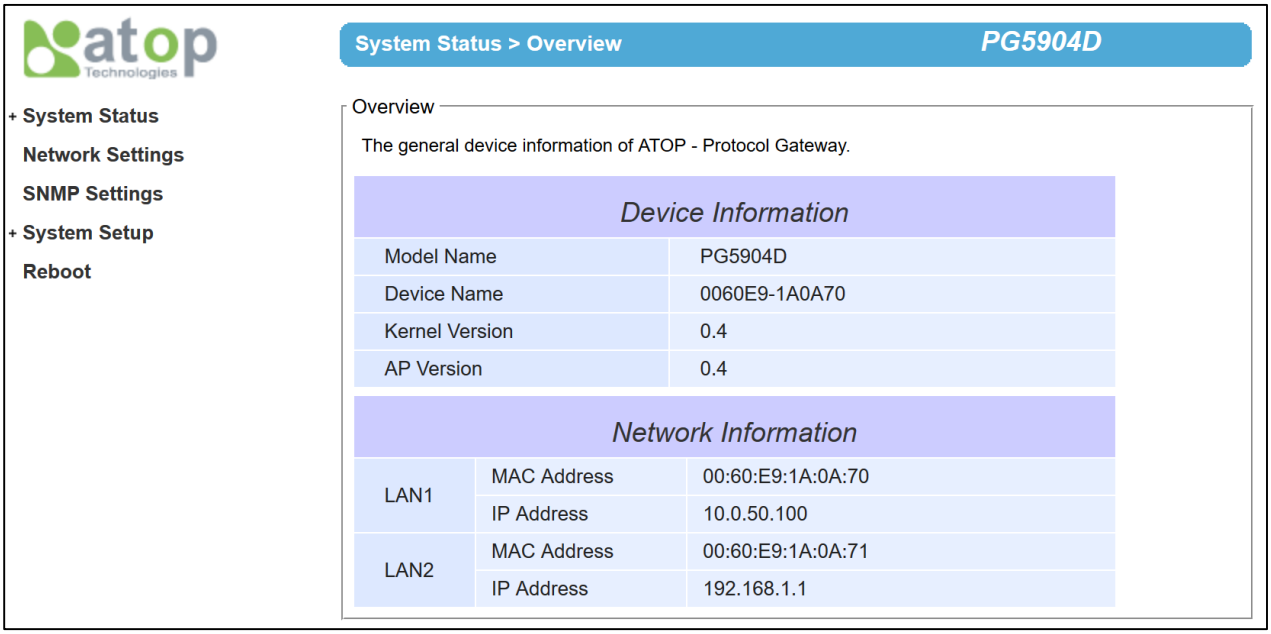


Figure 3-5 - Overview web page of protocol gateway

PG5900A/08A/16A, offer additional configuration options, such as redundancy, Virtual IP and Link Bond.

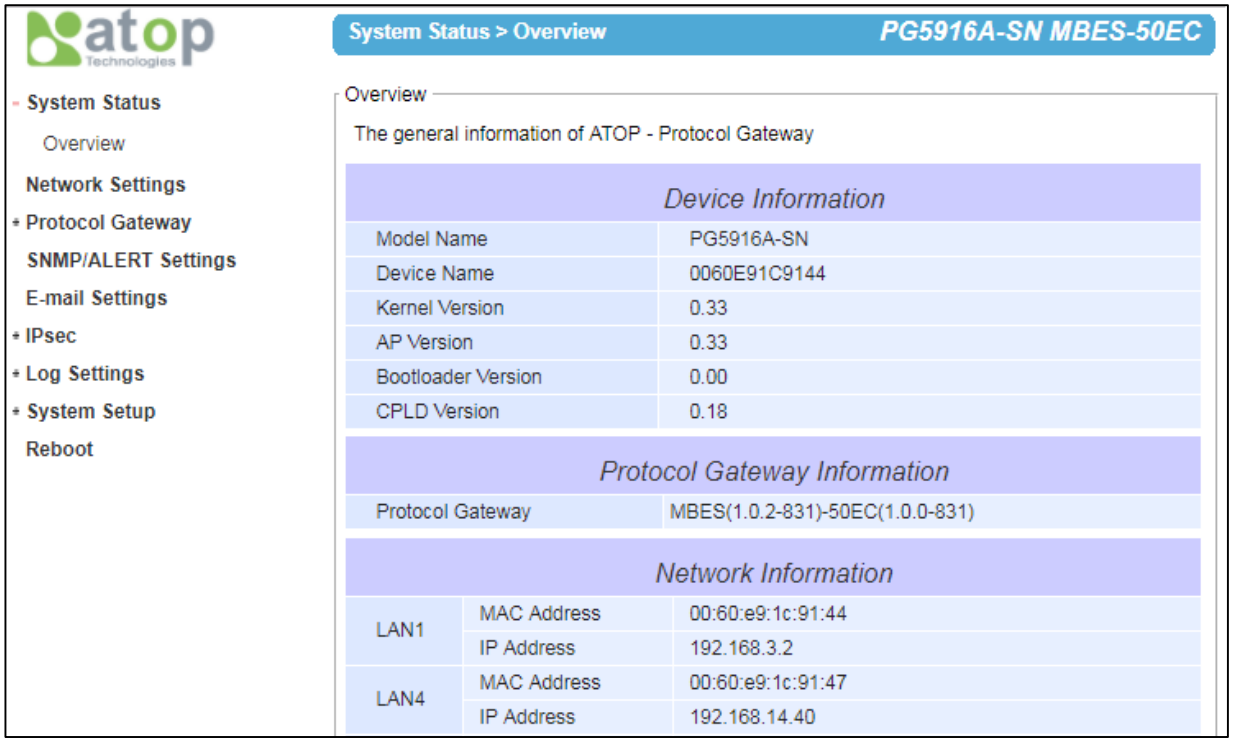


Figure 3-6 – PG5900A/08A/16A menu structure

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

1st layer	2nd layer	3rd layer	4th 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
	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.

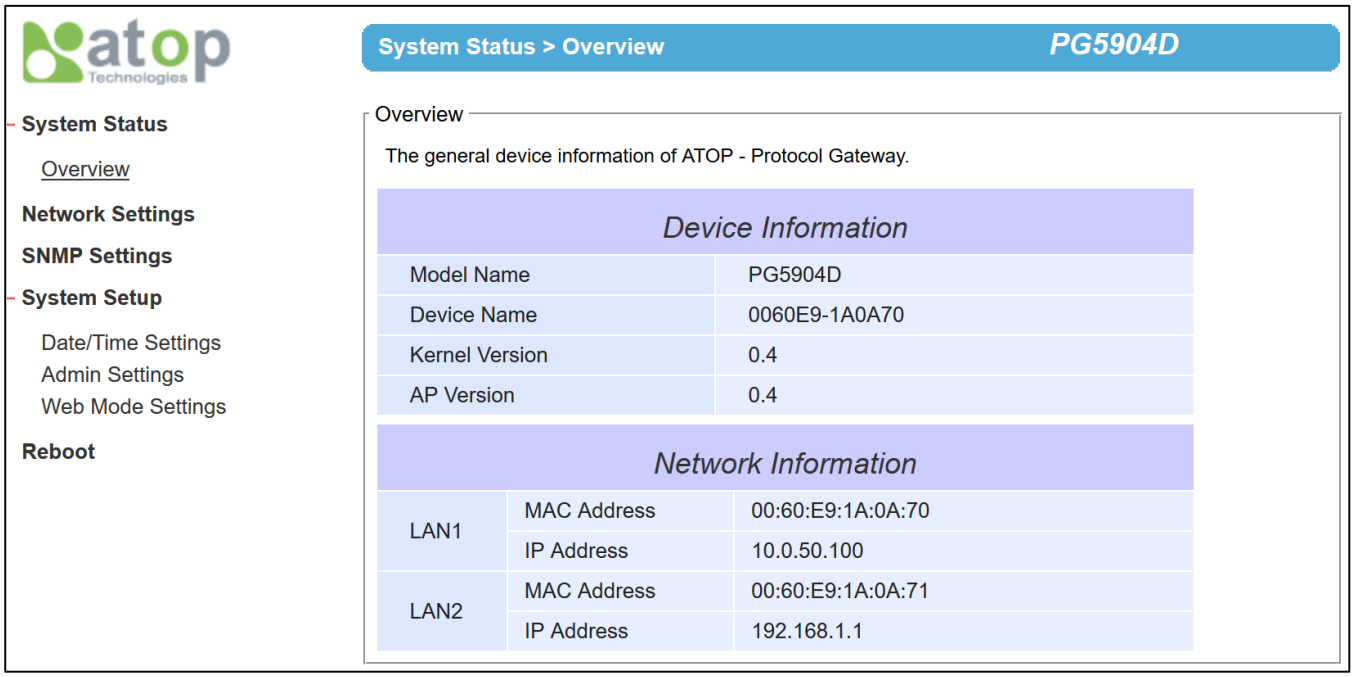


Figure 3-7 – Overview Page

In detail, the following information is given:

- **Model Name,** as its name implies, shows the device's model.
- **Device Information** displays information on the Kernel version as well as the AP version of the device.
- **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.

Note[1]: 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.
Note[2]: 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.

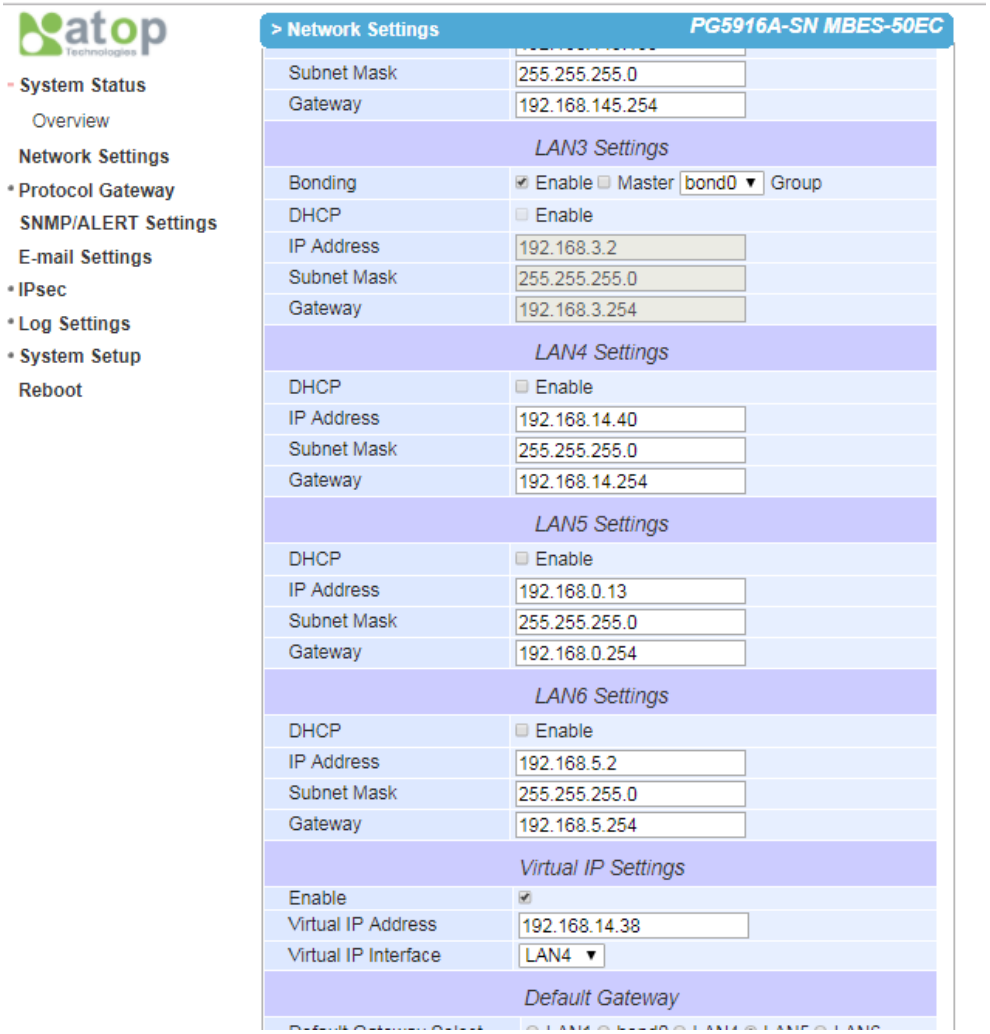


Figure 3-8 – Network configuration Page, example on PG5900A/08A/16A

At the lower section in Figure 3-8, 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.

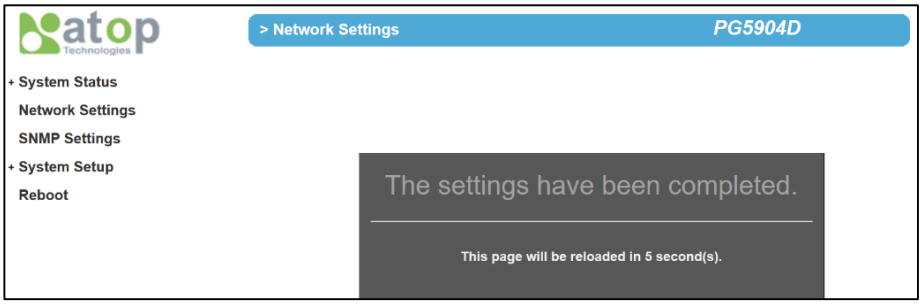


Figure 3-9 – Save completed Page

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 Figure 3-10.

- **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*

Please check the link aggregation status example in Figure 3-11.

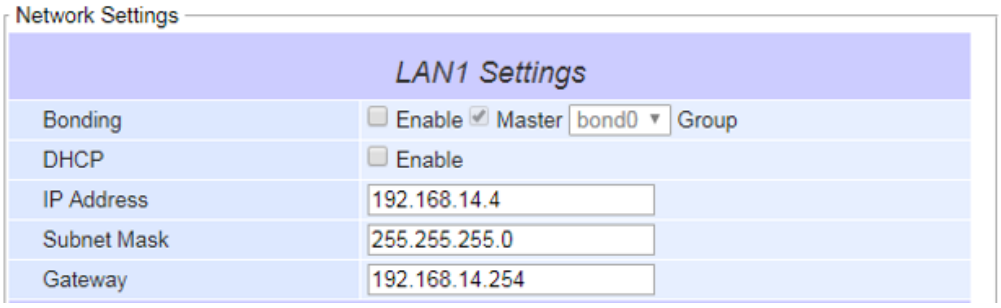


Figure 3-10 – Bonding settings

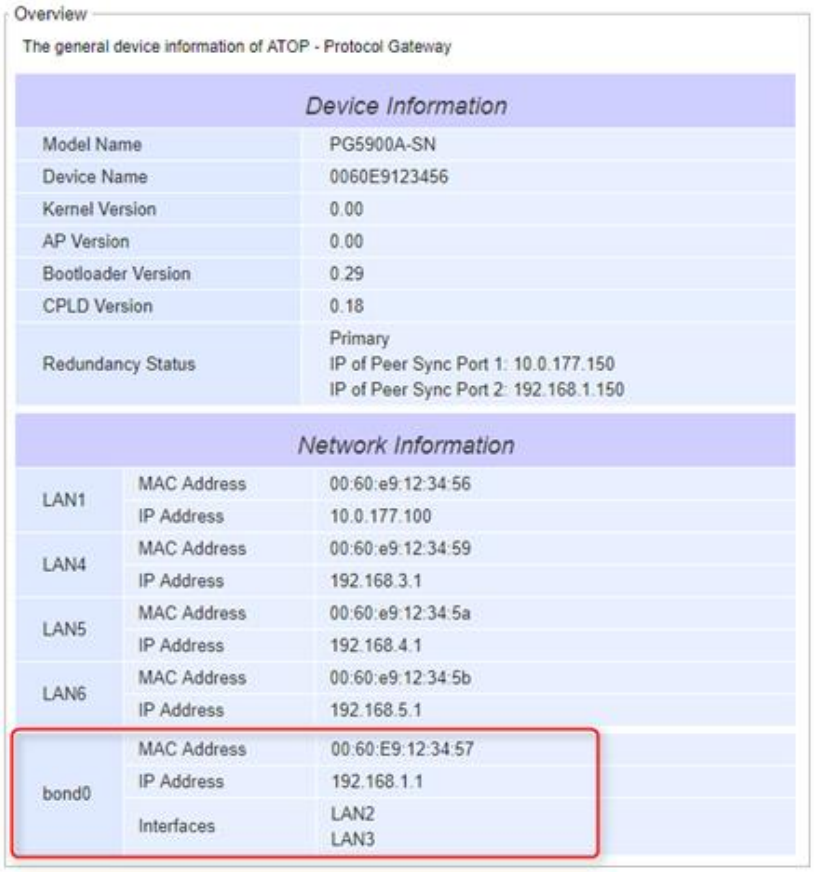


Figure 3-11 – Bonding status

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 3-12 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.

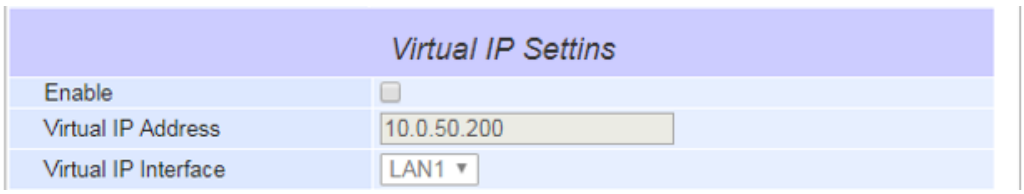


Figure 3-12 – Virtual IP settings

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 3-13 shows the configuration page, and below are explained the meaning of each field.

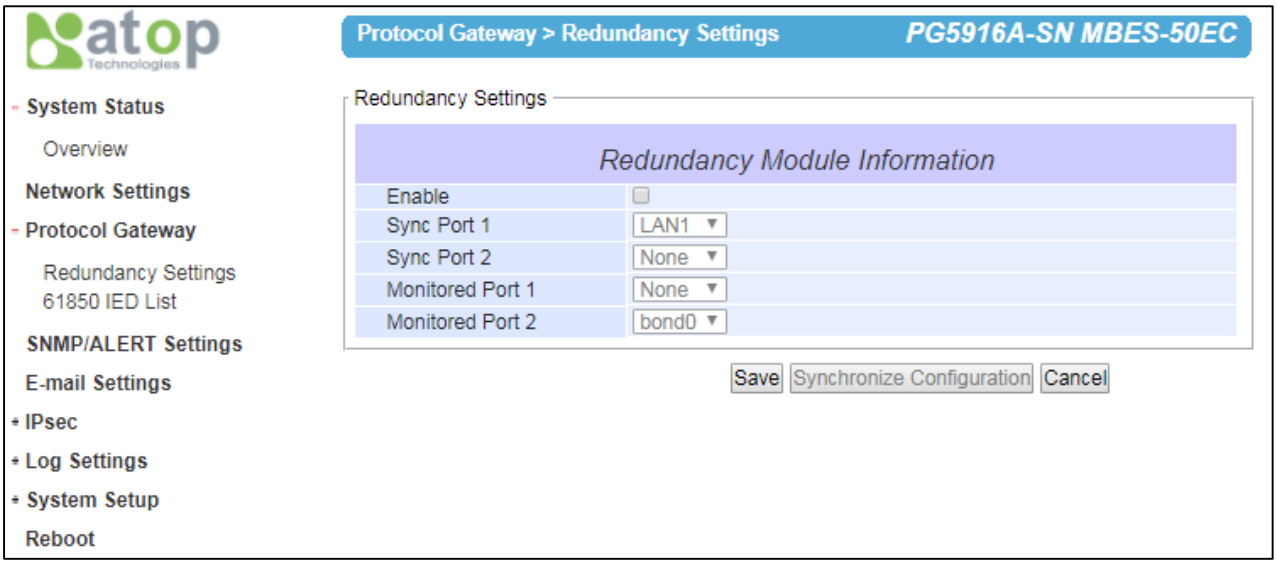


Figure 3-13 – Redundancy settings

- **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 the 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.

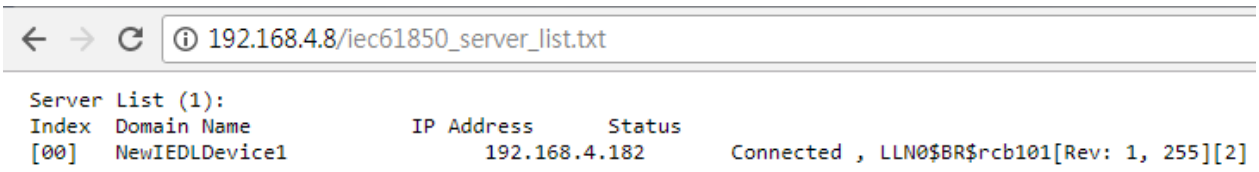


Figure 3-14 – IED conncetion statistics

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.

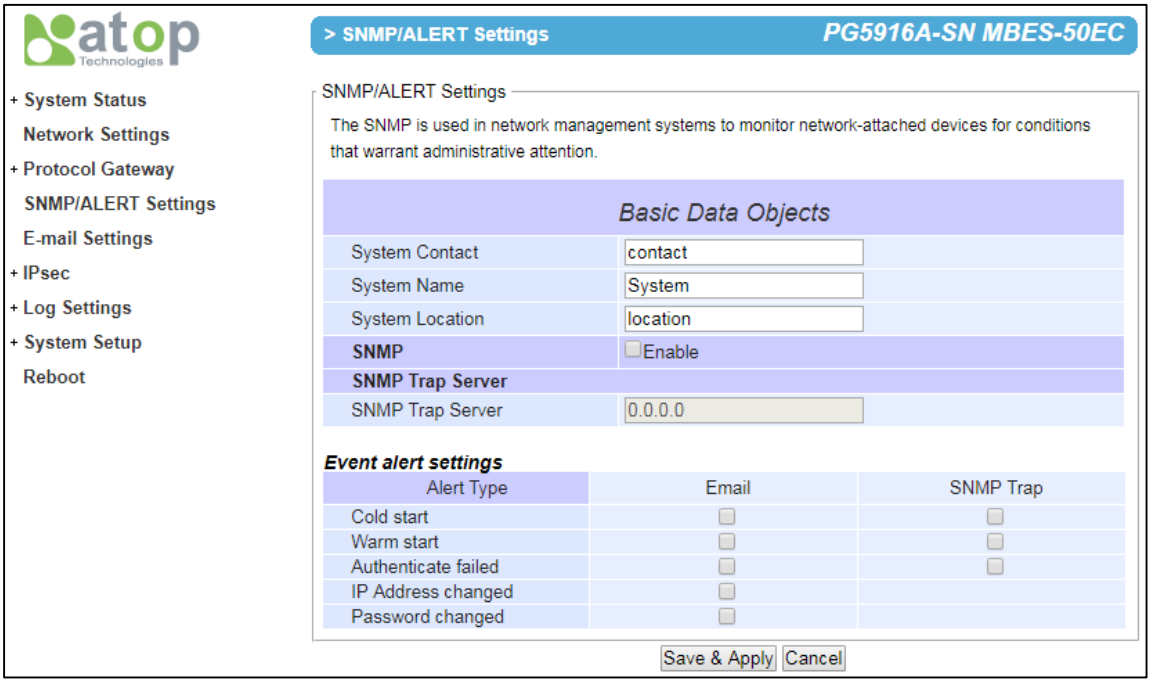


Figure 3-15 – SNMP setting

3.9 IPsec Settings

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

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, or an IED). Note that this type of connection cannot be use for accessing entire sub-network resources. Figure 3.16 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode.**

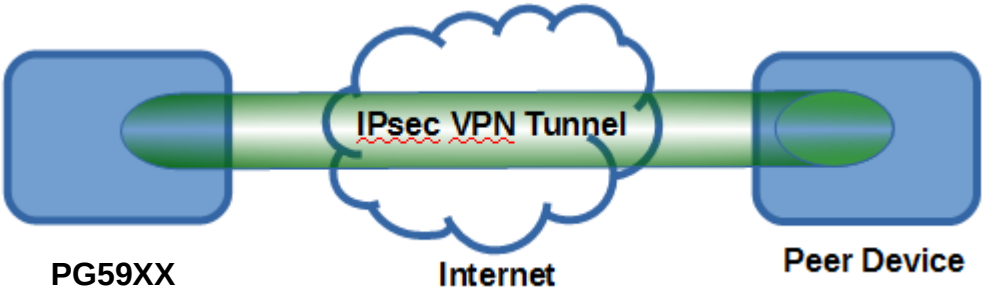


Figure 3.16 An example of Host-to-Host Connection

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 3.17 illustrates a road-warrior application in which PG59XX can access a

remote sub-network resource via a peer gateway. Figure 3.18 illustrates a gateway application in which PG59XX can passively accept connection requests from remote sides and provide access to PG59XX sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

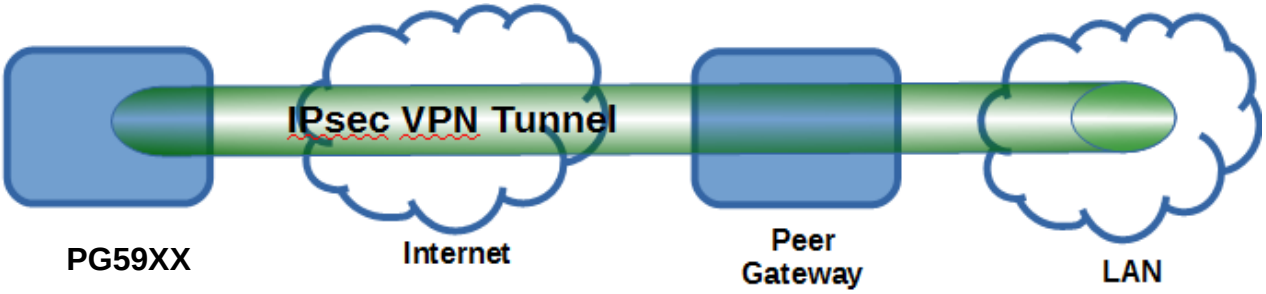


Figure 3.17 Roadwarrior Application using Host-to-Subnet Connection

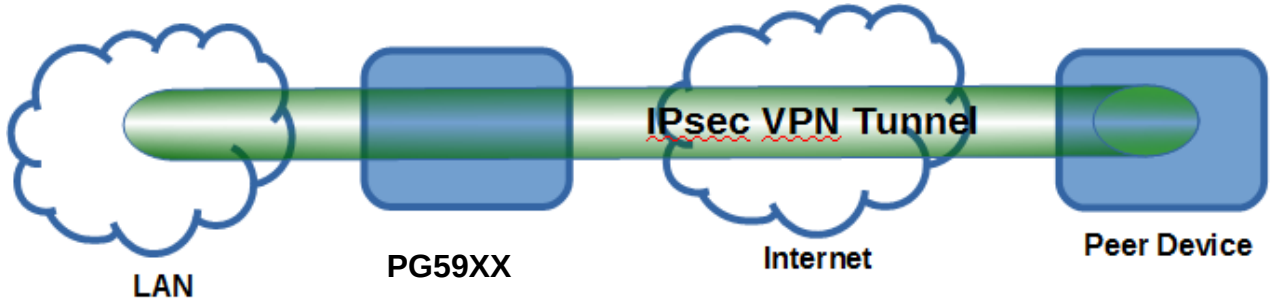


Figure 3.18 Gateway Application using Host-to-Subnet Connection

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 3.19 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 3.20. On the other hand, two different devices on two different subnets (host-host application) can be connected via a IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 3.21. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

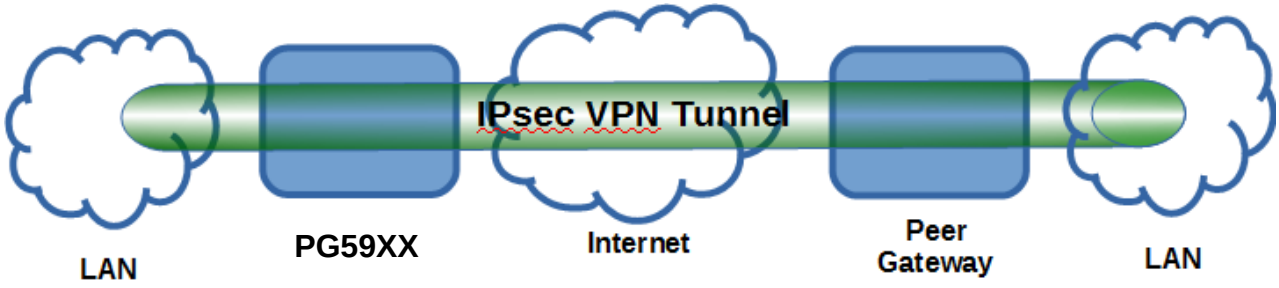


Figure 3.19 An example of network application using a subnet-to-subnet connection via the PG59XX and a peer device.

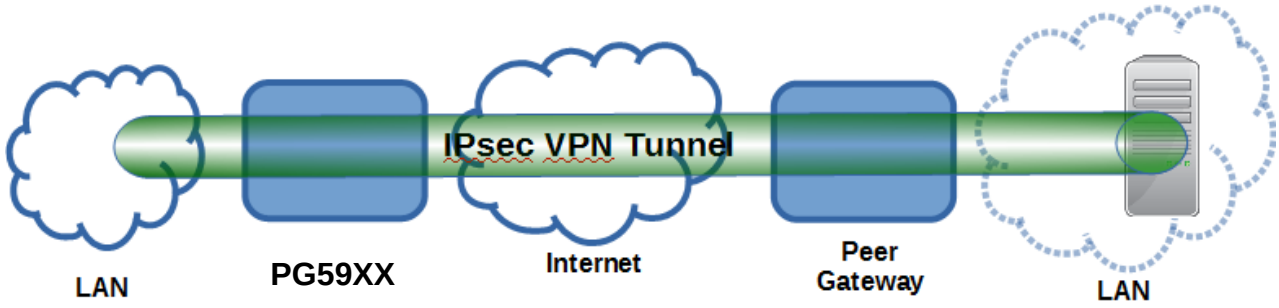


Figure 3.20 An example of host-network application via the subnet-to-subnet connection

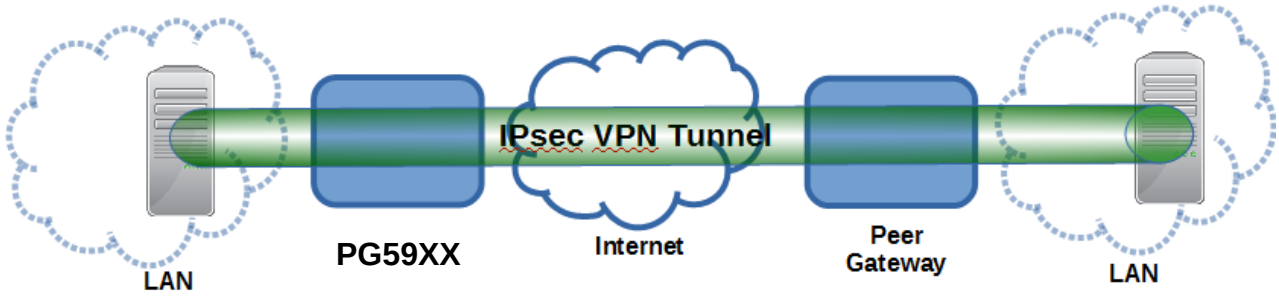


Figure 3.21 An example of host-host application via the subnet-to-subnet connection

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

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

PG59XX also has a feature called NAT traversal that allows the IPsec tunnel to pass through the NAT in its network.

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) is 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.

3.9.1 IPsec Settings

Figure 3.22 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**.

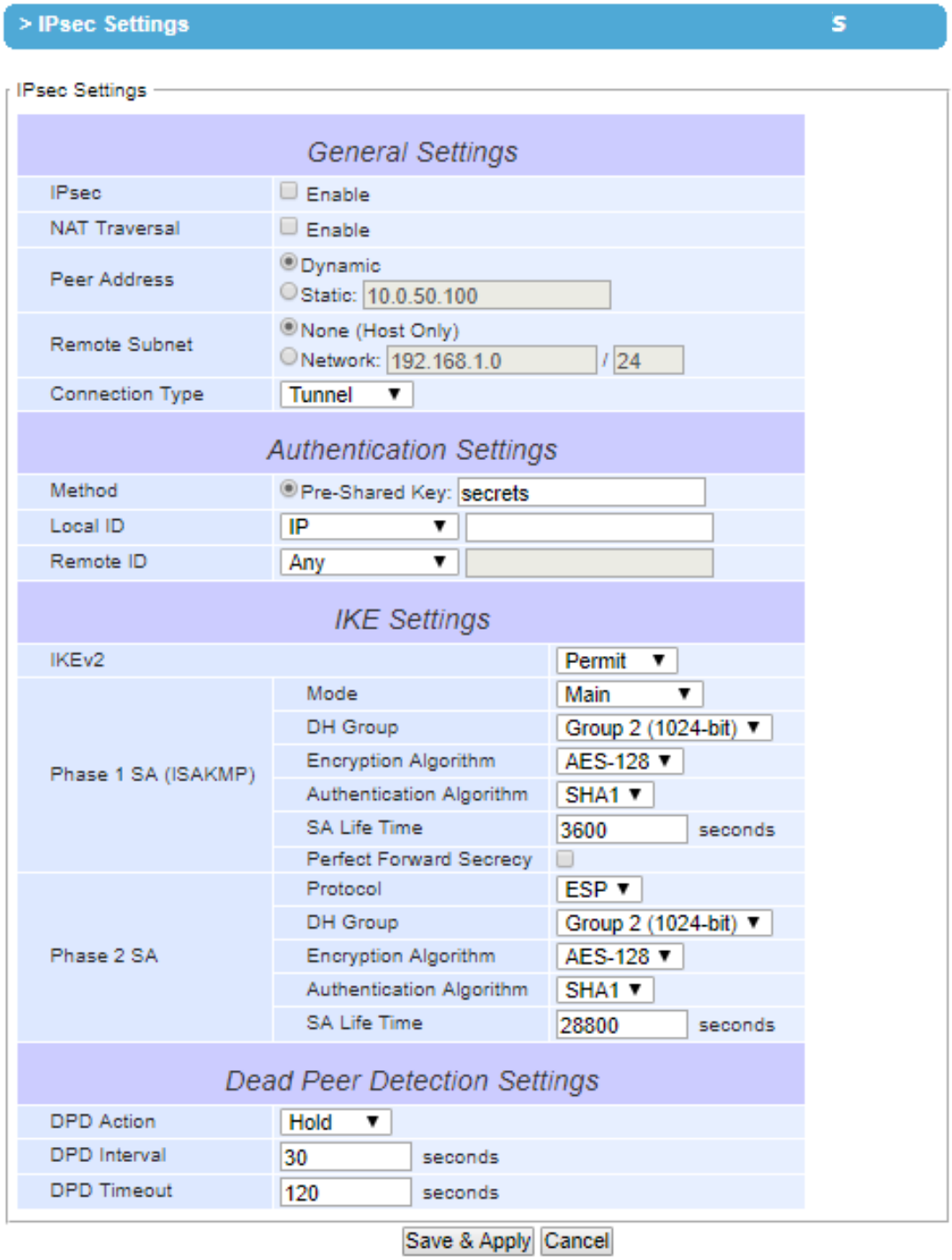


Figure 3.22 IPsec Tunnels Web Page under IPsec Setting Menu

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.

- **NAT Traversal**: If you are aware that there is a Network Address Translation (NAT) mechanism in between the two sides of the IPsec tunnel connection, please check this option. That is the host or the subnet is using address(es) in the private IP Address spaces. Some NAT routers will block IPsec packets if it does not support IPsec pass-through. If you connect to another NAT router which does not support IPsec pass-through at the WAN side, PG59XX will activate this option automatically and encapsulate the IPsec packets inside UDP port 4500 to be able to pass through the NAT router.
- **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 ratio 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 the VPN tunnel must use the same secret key or password. The pre-shared key can be 1 to 60 case-sensitive ASCII characters and special symbols.

The third part of **IPsec Settings** is the **IKE** (Internet Key Exchange) **Settings.** Internet Key Exchange (IKE) that 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 initiates 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 in to one exchange packet**. Aggressive Mode** makes the IKE negotiation quicker than **Main**

Mode. The difference between **Main Mode** and **Aggressive Mode** is that the "identity protection" is used in the **Main Mode**. The identity is transferred encrypted in the **Main Mode** but it is not encrypted in **Aggressive Mode**. Typically, the **Main Mode** is recommended.

- Second option is the selection of Diffie-Hellman's group (**DH Group**) of standardized global unique prime numbers and generators that will be used to provide secure asymmetric key exchange**.** The **DH Group** is used to encrypt this IKE communication. 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 or 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 disable, the protocol will use the same security key for different IPsec phases. If this option is enable 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 sent 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 of time for sending the hello message to the peer device or the interval that PG59XX will repeatly check the endpoint with keep-alive message**.** The **DPD interval** can be ranged from 1 to 65535 seconds. The default value for **DPD Interval** is 30 seconds**.** The **DPD Timeout** will be the time that 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 time 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 parameters 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
NAT Traversal		Enable the NAT Traversal mechanism	Enable
Peer Address		IP address of the remote device which can be dynamic (any address) or static (fixed address)	-
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

Field Name		Description	Default Value
	Authentication Algorithm	Section of hash algorithm to be used to authenticate packet data in the IPsec tunnel: either MD5 or SHA1	SHA1
	SA Life Time	Value that represents the lifetime of the IKE key which is dedicated in Phase 2 between both end host or network. The available setting ranges is from 180 to 86,400 seconds.	3600
Dead Peer Detection Settings			
DPD Action		Select either Hold or Restart the tunnel's security association for the peer**.** Note that Hold is suitable for a statistically defined tunnel**.**	Hold
DPD Interval		Duration of time for sending hello message to the peer device: value from 1 to 65535 seconds.	30 seconds
DPD Timeout		Duration of time to declare that the peer is dead: value from 1 to 65535 seconds.	120 seconds

After finishing the **IPsec settings** configuration, please click the **Save & 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.

3.9.2 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.

3.9.2.1 Host-to-Host Connections

Two scenarios can be configured for host-to-host connections: with static peer and with dynamic peer. A host-to-host topology for both scenarios is illustrated in Figure 3.23. Please follow the steps provided next for each scenario to set the **General Settings**.

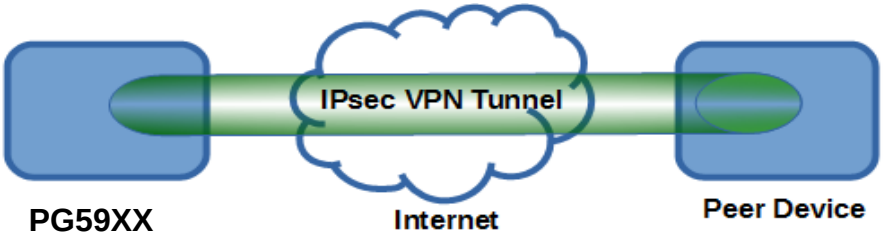


Figure 3.23 IPsec VPN Tunnel with Host-to-Host Topology

Scenario: host-to-host with static peer as shown in Figure 3.24

- Check the **Enable** box for **IPsec**.
- If you need to enable **NAT Traversal** option, check the **Enable** box for this option.
- 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, 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 raio 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**.

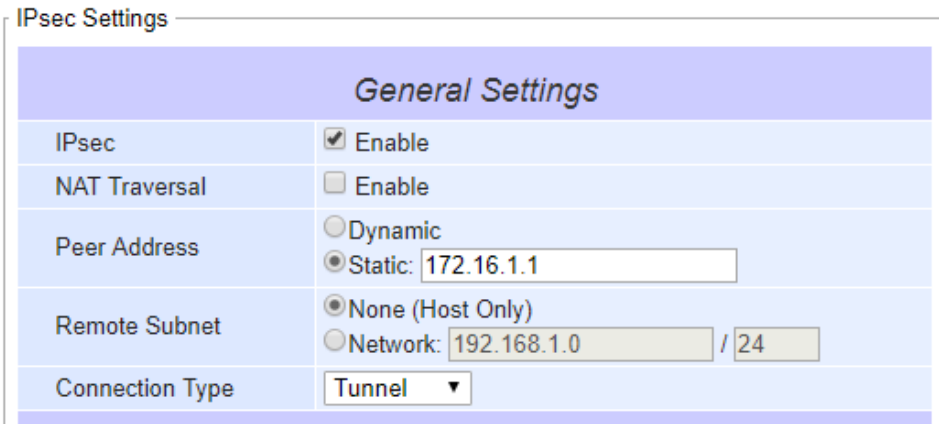


Figure 3.24 General Settings for Host-to-Host with Static Peer

Scenario: host-to-host with dynamic peer as shown in Figure 3.25

- Check the **Enable** box for **IPsec**.
- If you need to enable **NAT Traversal** option, check the **Enable** box for this option.
- In the **Peer Address** field, select the **Dynamic** option.
  Note: When VPN connects to a peer with dynamic IP address, 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.

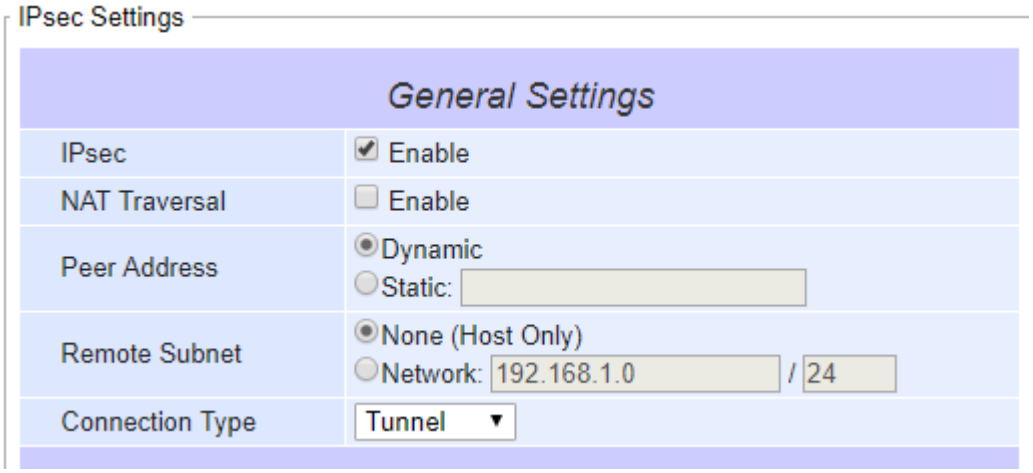


Figure 3.25 General Settings for Host-to-Host with Dynamic Peer

3.9.2.2 Host-to-Network Connections

Two scenarios can also be configured for host-to-network (or host-to-subnet or host-to-site) connections: with static peer and with dynamic peer. Note that PG59XX is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in Figure 3.26. Please follow the steps provided next for each scenario to set the **General Settings**.

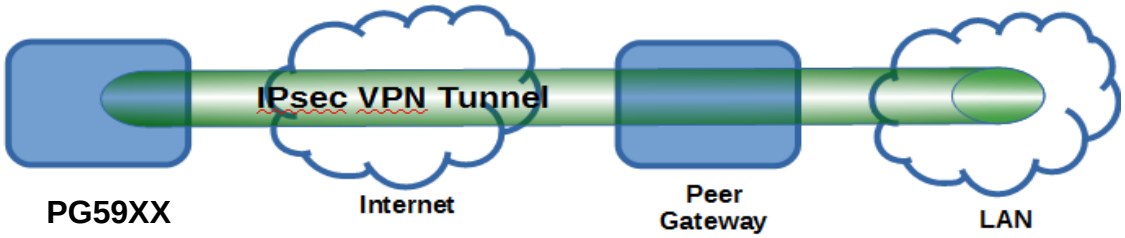


Figure 3.26 IPsec VPN Tunnel with Host-to-Network Topology

Scenario: host-to-network with static peer as shown in Figure 3.27

- Check the **Enable** box for **IPsec**.
- If you need to enable **NAT Traversal** option, check the **Enable** box for this option.
- 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, PG59XX is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. 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.

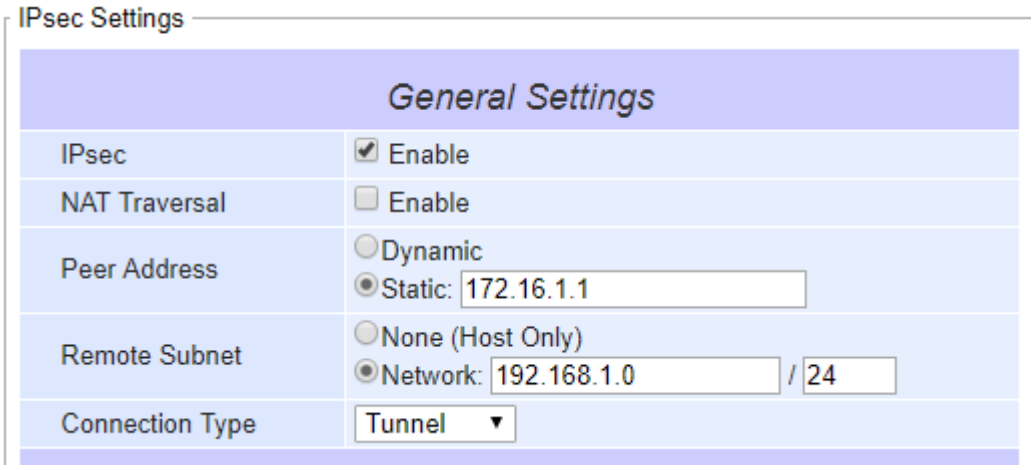


Figure 3.27 General Settings for Host-to-Network with Static Peer

Scenario: host-to-network with dynamic peer as shown in Figure 3.28

- Check the **Enable** box for **IPsec**.
- If you need to enable **NAT Traversal** option, check the **Enable** box for this option.
- In the **Peer Address** field, select the **Dynamic** option.
  Note: When VPN connection is set to a peer with dynamic IP address, 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.

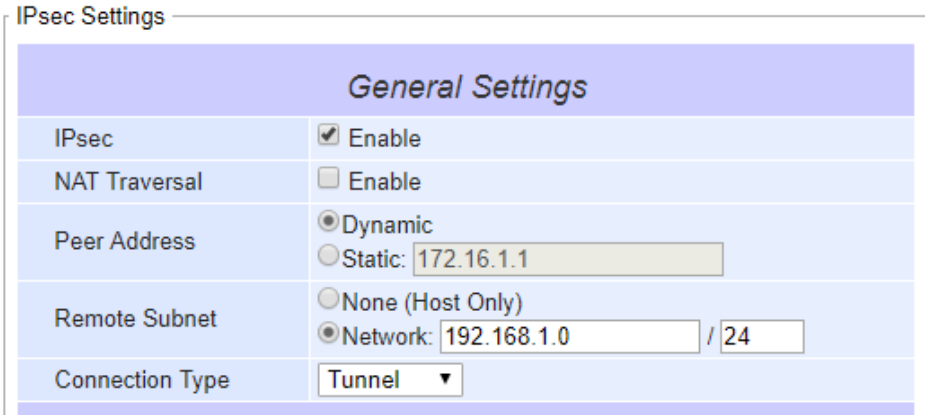


Figure 3.28 General Settings for Host-to-Network with Dynamic Peer

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 **N**etwork **T**ime **P**rotocol (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 hidden if the **NTP** option is selected.

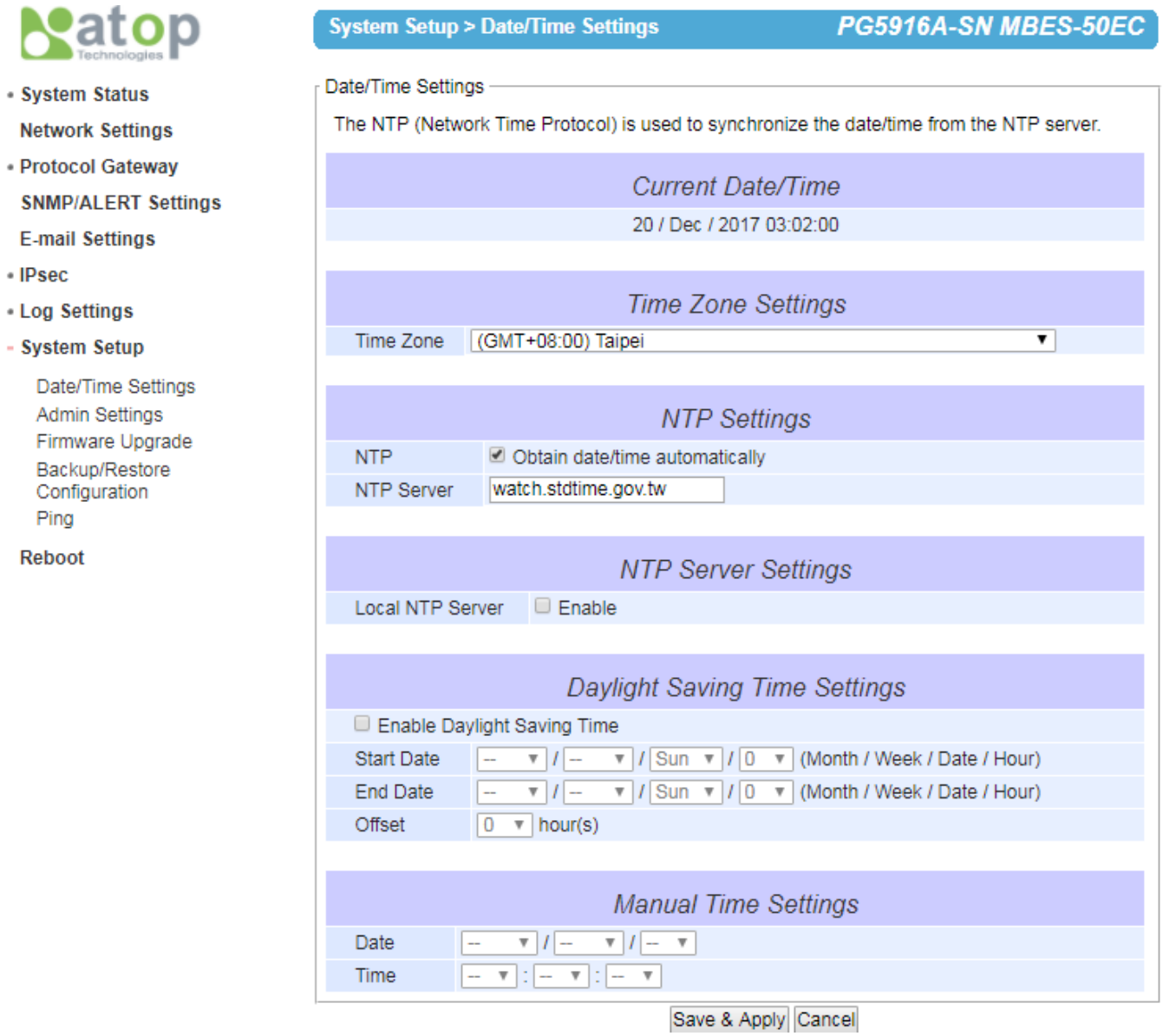


Figure 3-29 – Time settings Page

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.

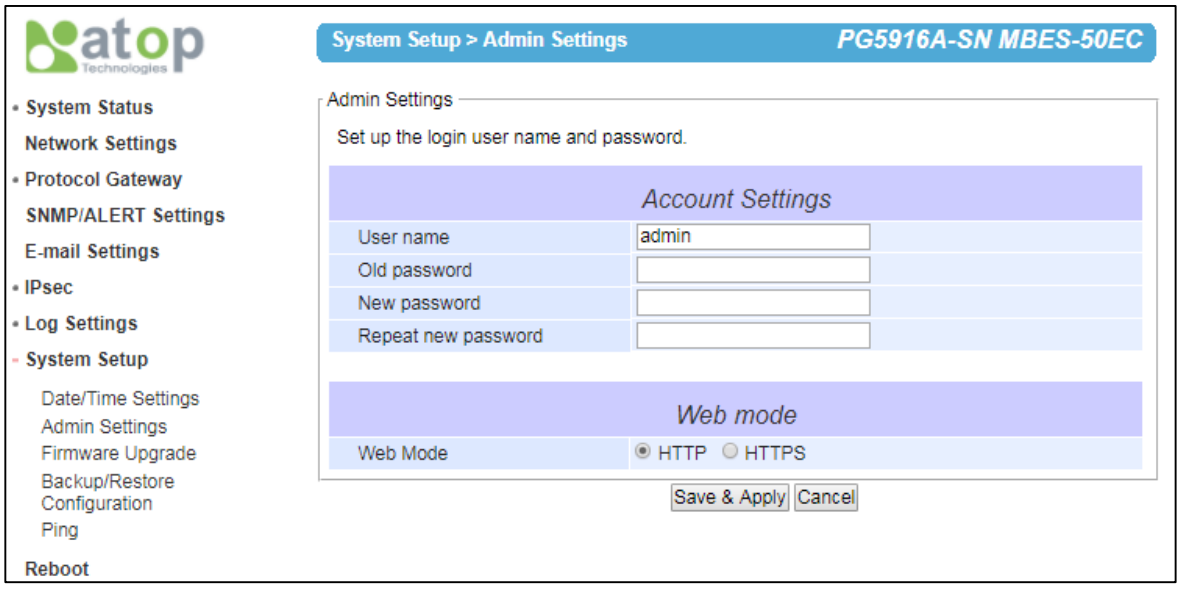


Figure 3-30 – Admin settings Page

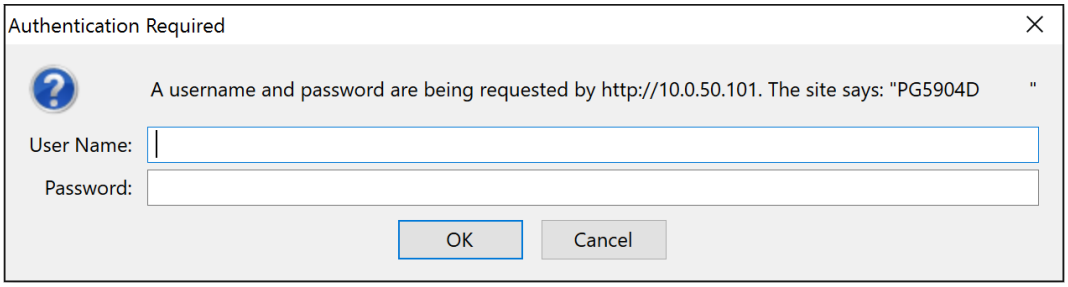


Figure 3-31 – Entering the User Name and the New Password

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.

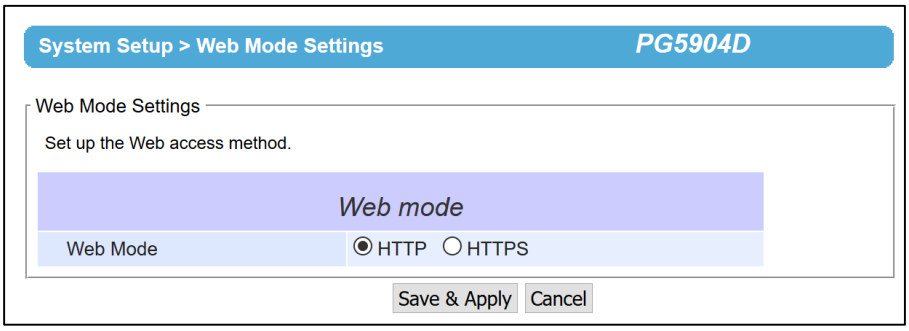


Figure 3-32 – Web mode settings

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.

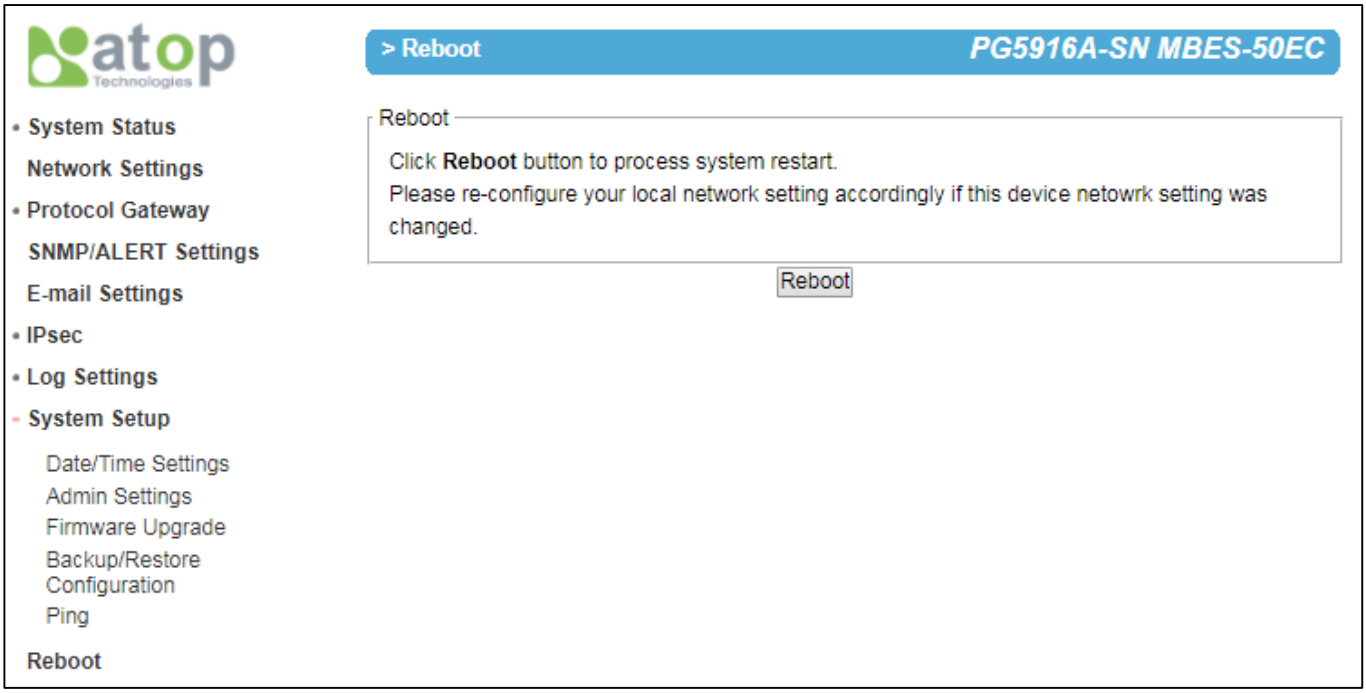


Figure 3-33 – Restart page

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

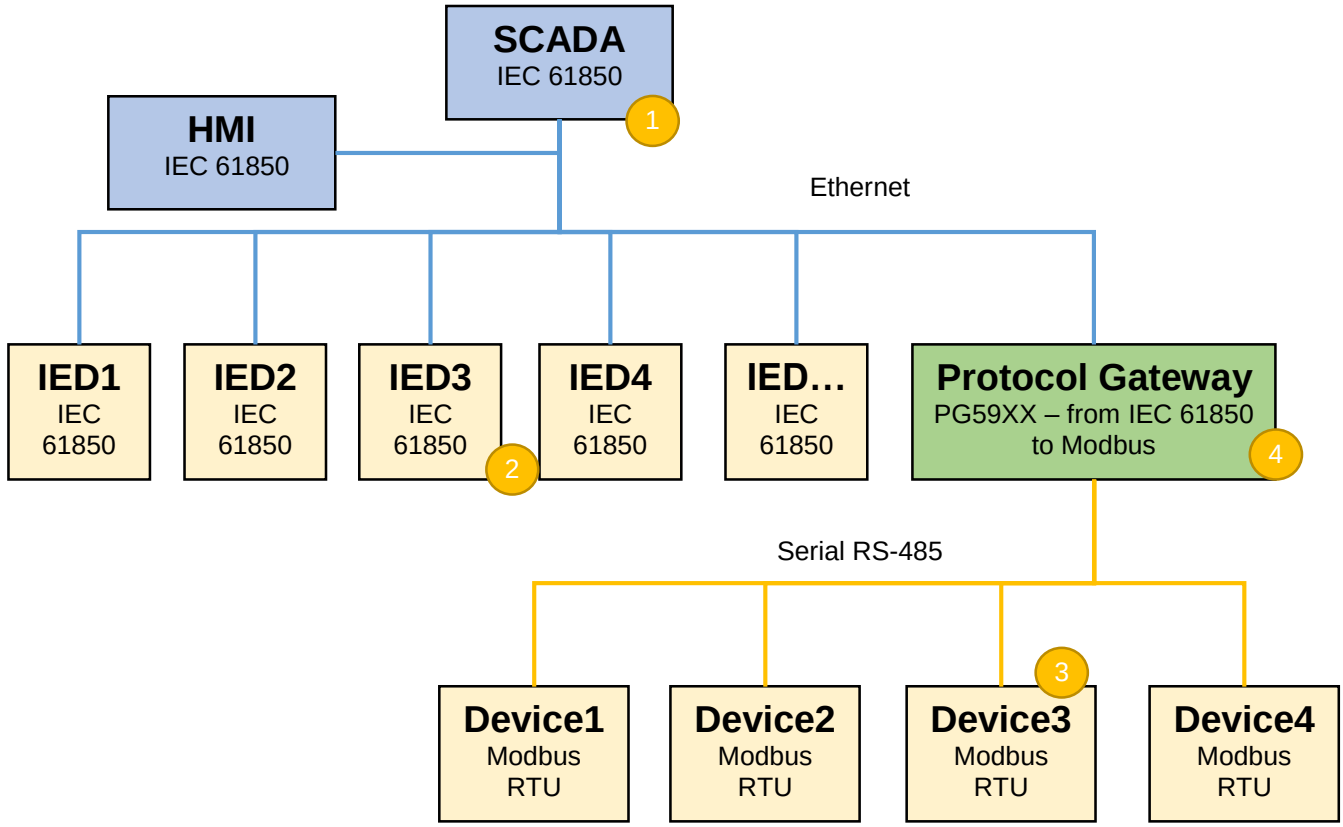


Figure 4-1 – Protocol Gateway Application Example

1 Represents the HOST side that is in control of the application issueing 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:

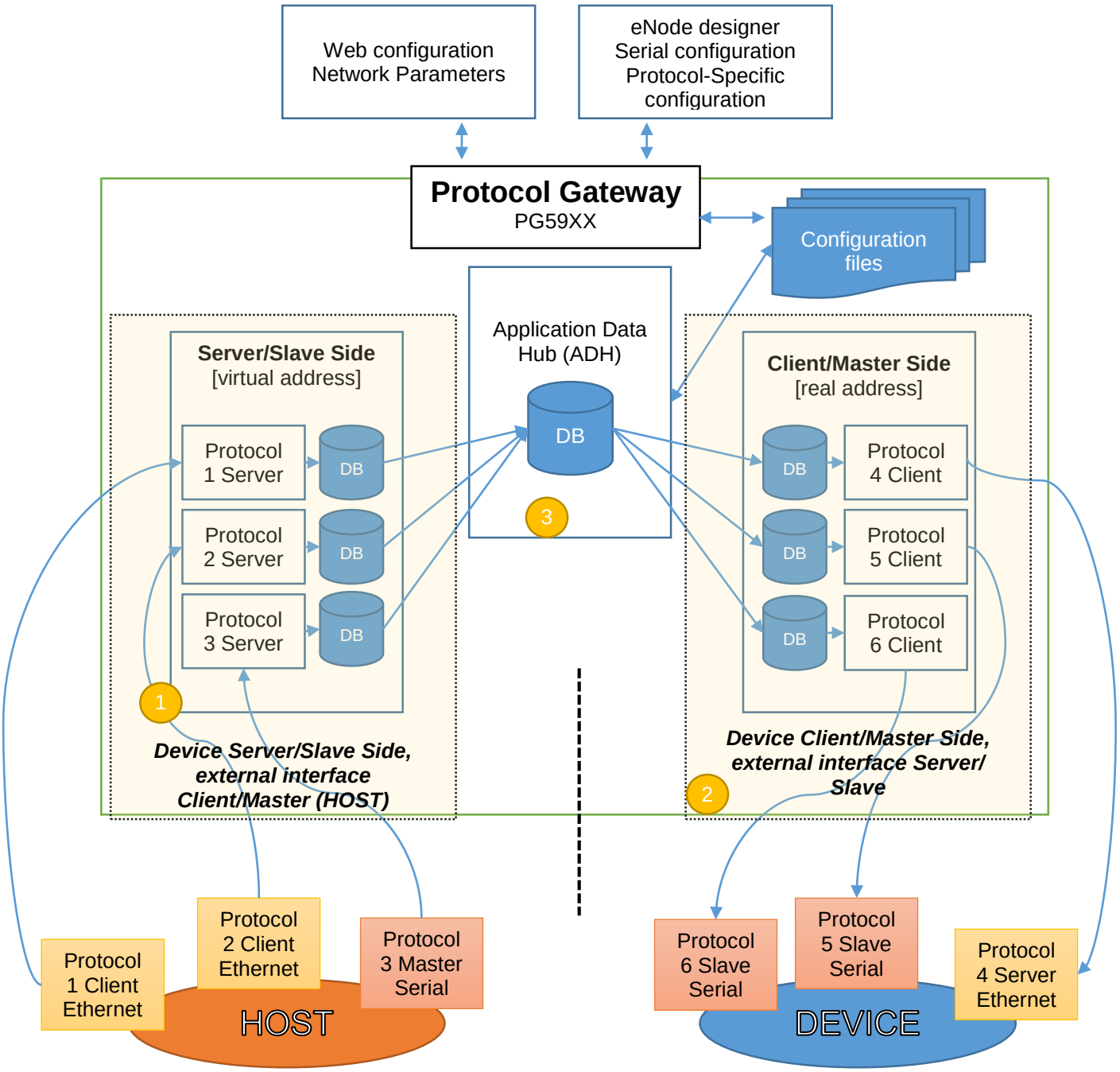


Figure 4-2 – Protocol Gateway Architectural overview

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 issueing 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 from 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 to be 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

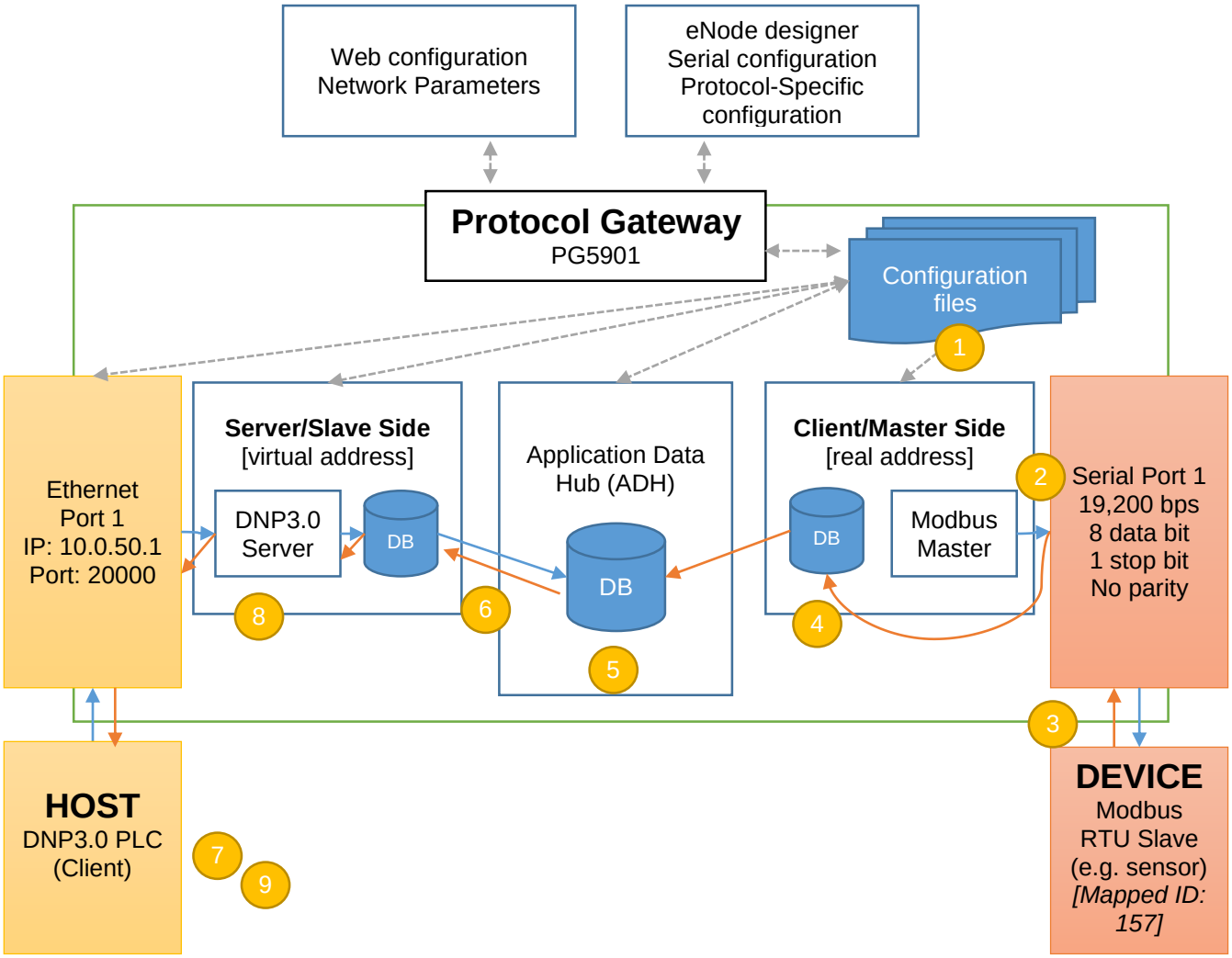


Figure 4-3 – Protocol Gateway Polling Process

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

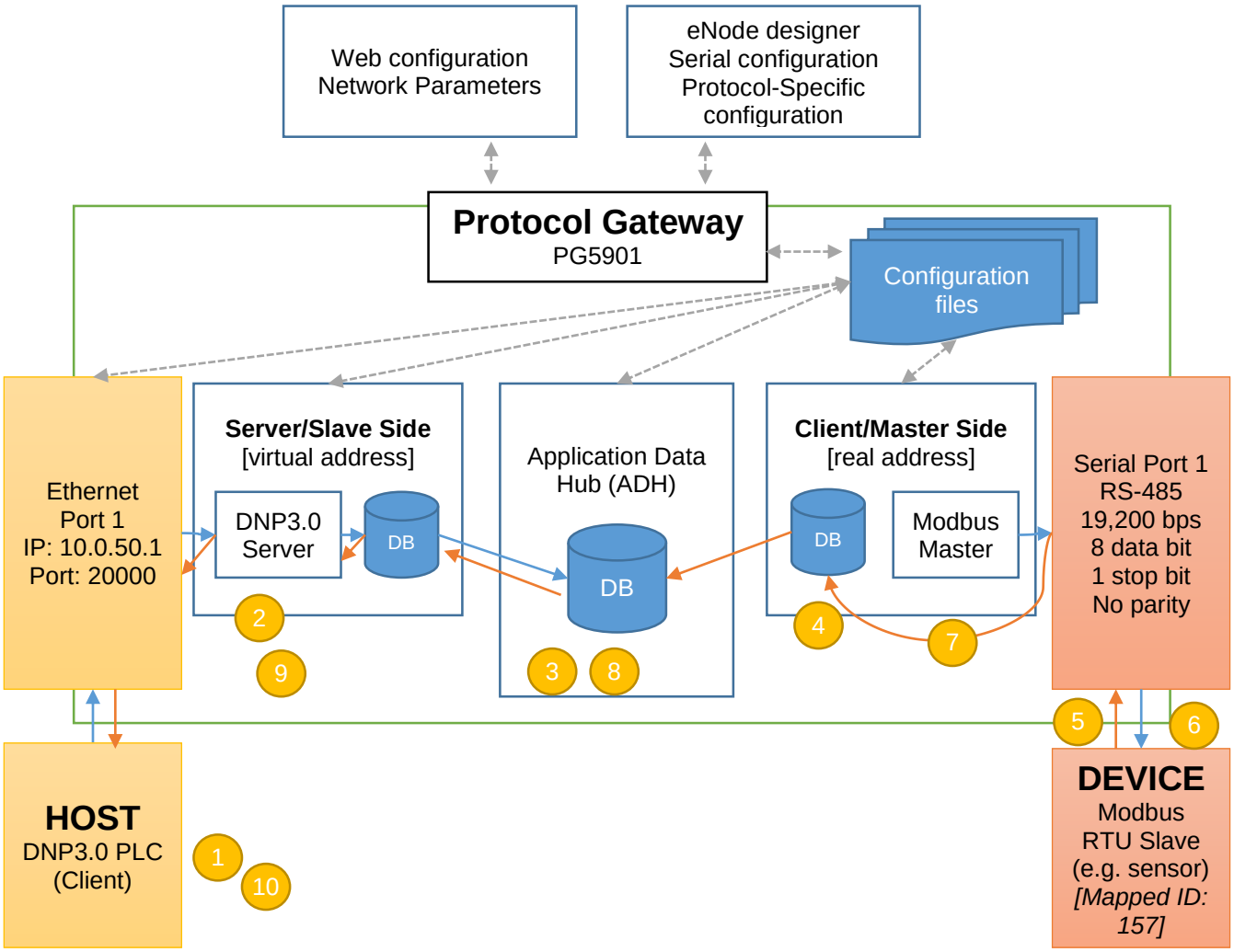


Figure 4-4 – Protocol Gateway Command Process

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 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.

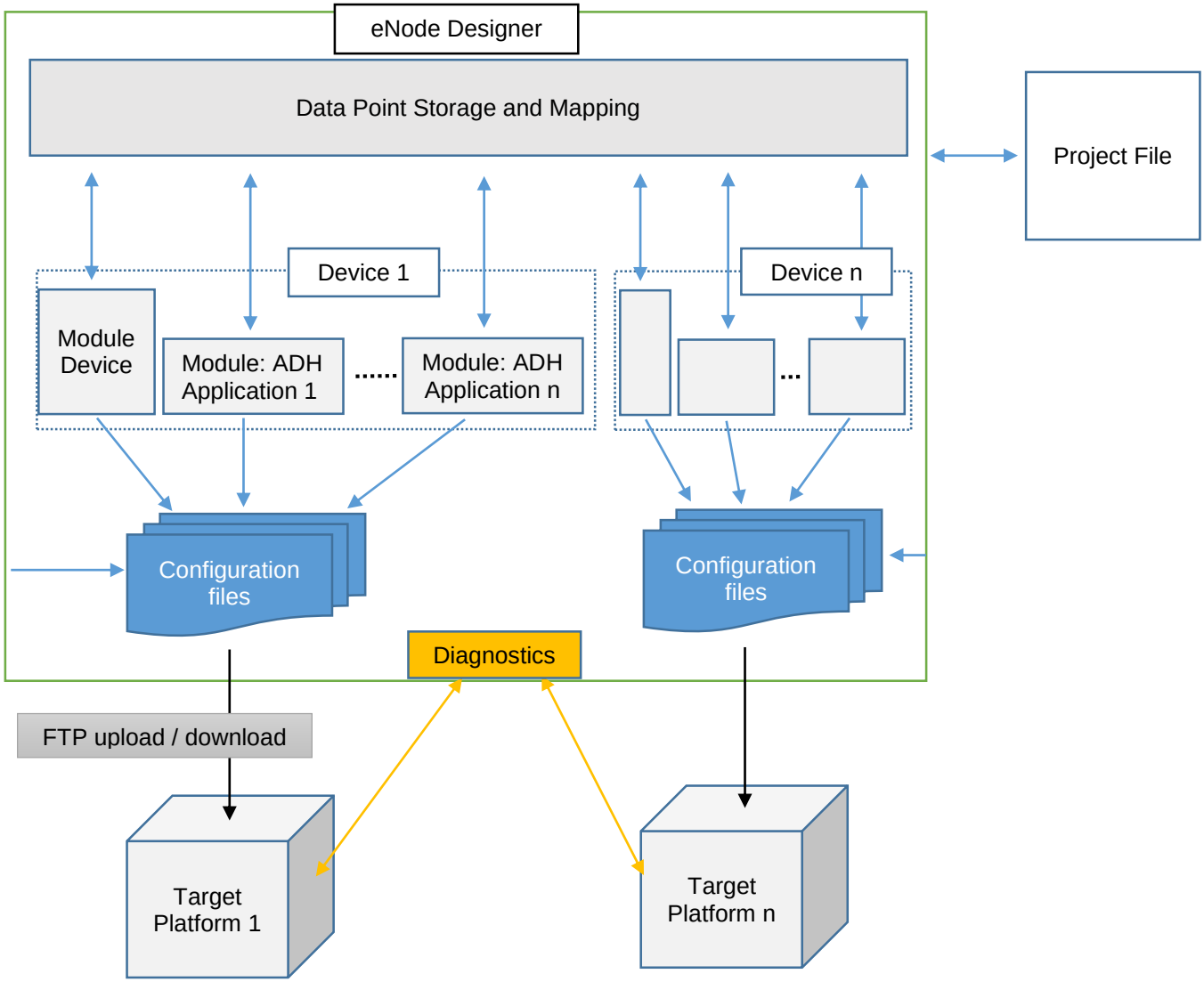


Figure 4-5 - eNode Designer overview.

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 recommend 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.

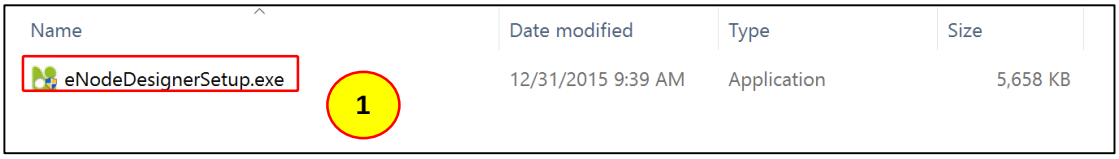
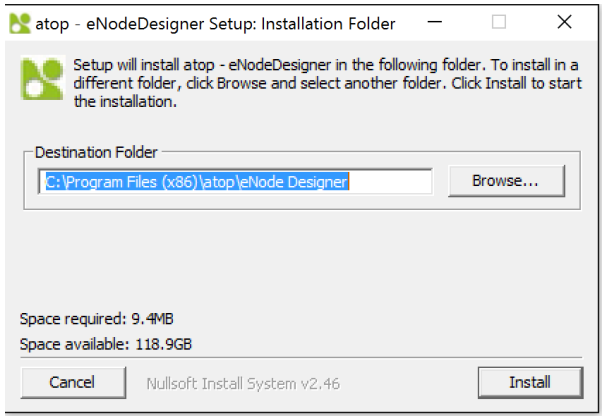


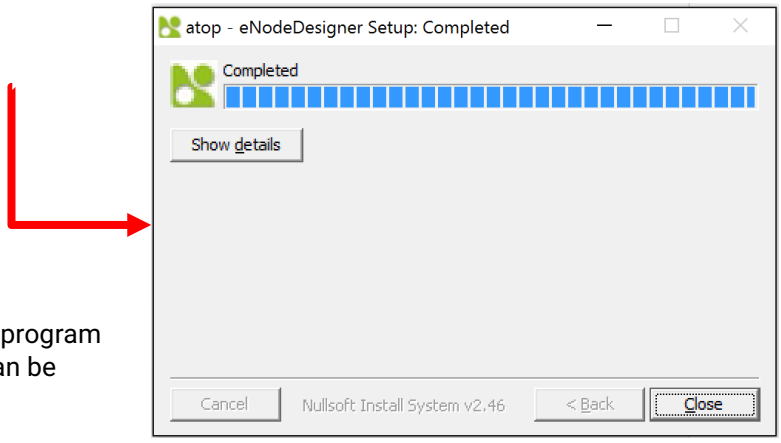
Figure 5-1 - eNode Designer Setup Installer

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

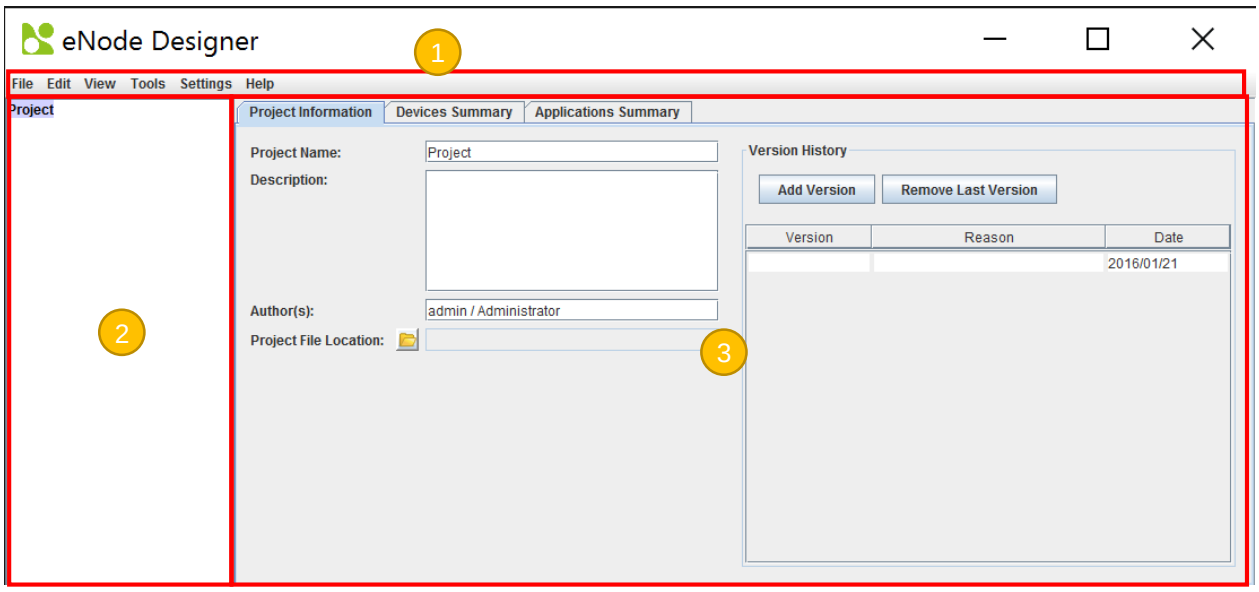


Figure 5-3 - eNode Designer main screen.

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 in to 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.

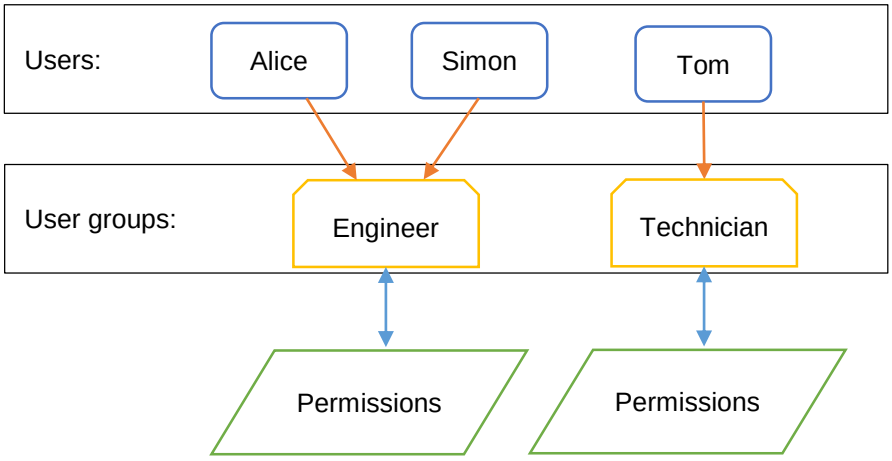


Figure 5-5 - User administration principal.

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

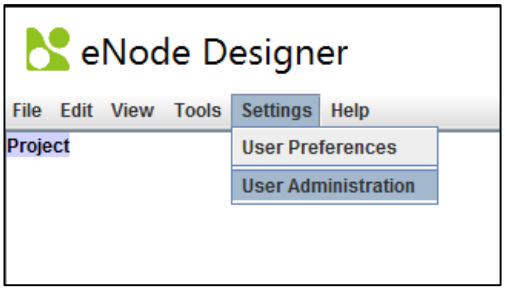


Figure 5-6 - Access user administration.

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.

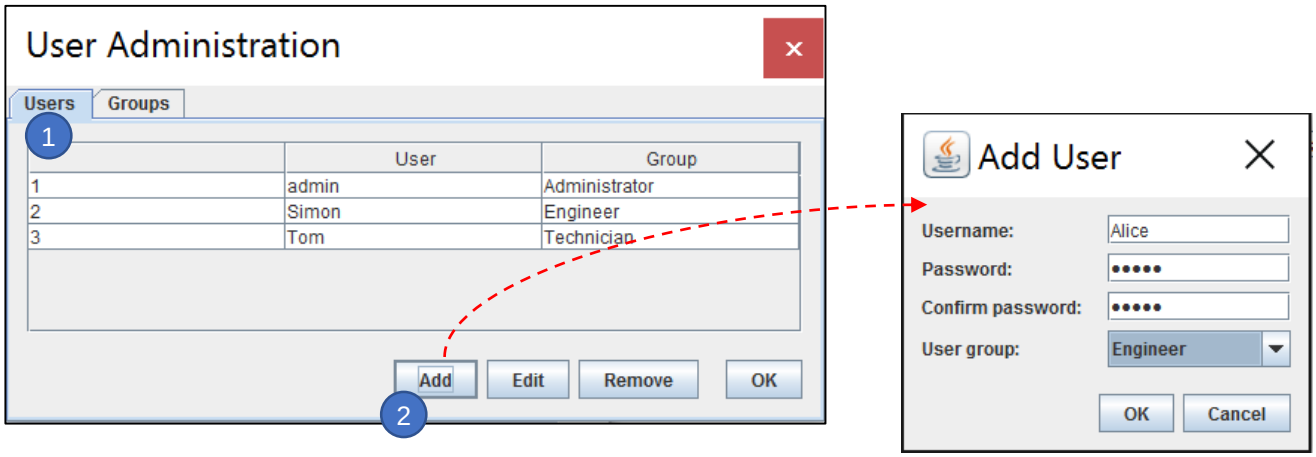


Figure 5-7 - Adding a new user.

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.

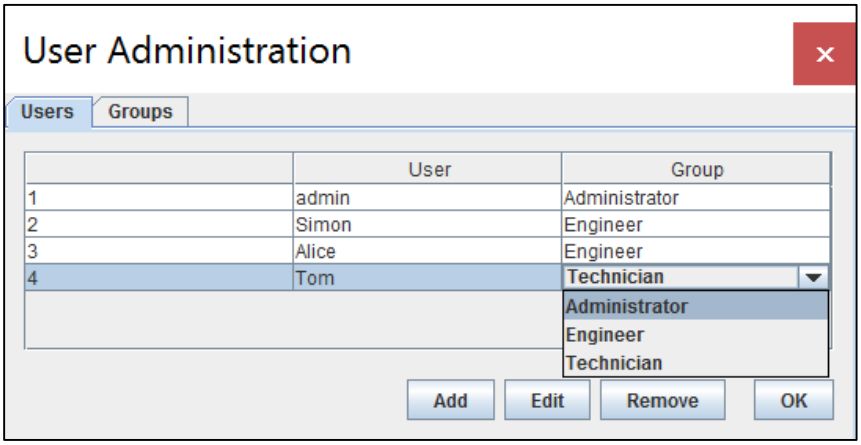


Figure 5-8 - Changing a user's user group.

5.4.2 Defining User Groups

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

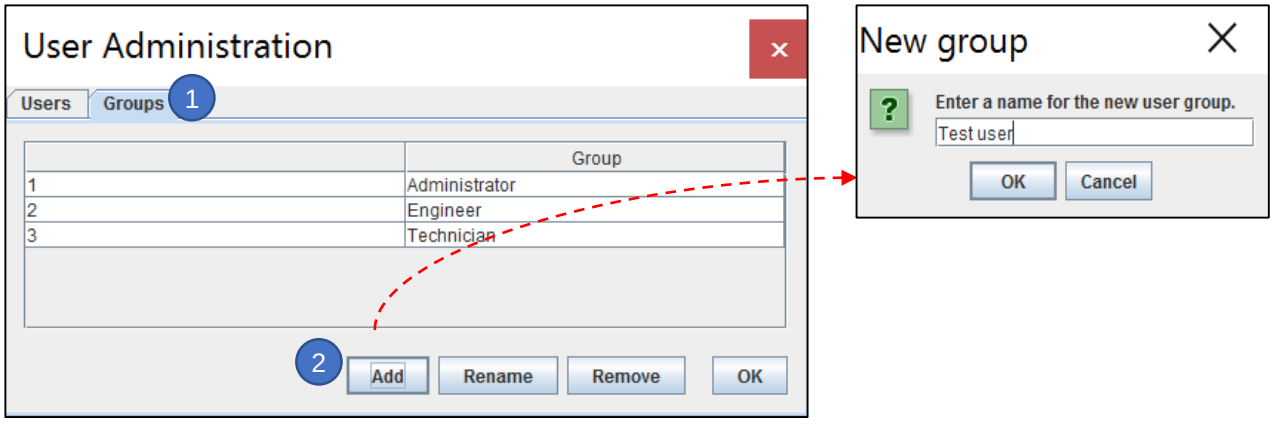


Figure 5-9 - Adding a user group.

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.

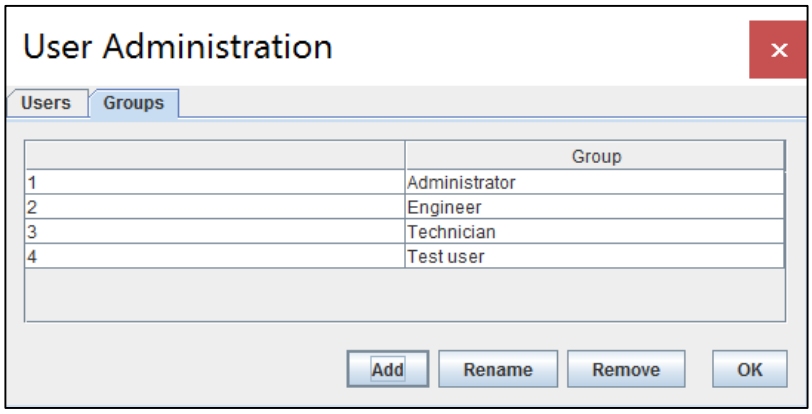


Figure 5-10 - User group added.

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 *Importing eNode Modules*

eNode Designer requires “eNode Modules” before it is particularly useful. Some eNode Modules may come bundled with the installation, but otherwise they need to be imported to eNode’s module library. Also if a new version of a module is released, it can be imported to replace the old version. This is achieved through the Module Management window, which can be reached from the Tools menu.

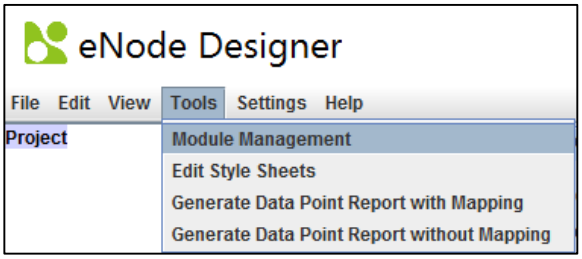
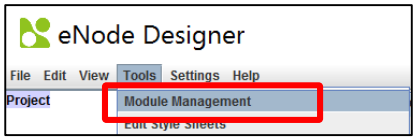
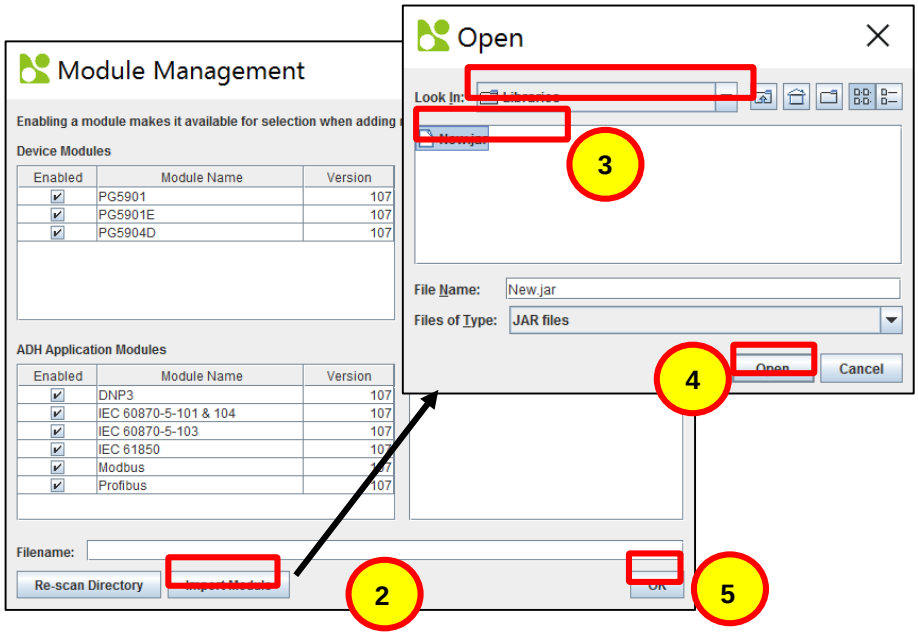


Figure 5-11 - Getting to the module management window.

This is an example that demonstrates importing a new module named the “New”.



1 Select **Module Management** under **Tools** in eNode Designer



2 Select **Import Module** and navigate to the subdirectory in which the New module is stored.

3 Select the **New.jar**

4 Click **Open** to import the New JAR

5

Click **OK** to finish

5.6 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.

5.6.1 Project Information

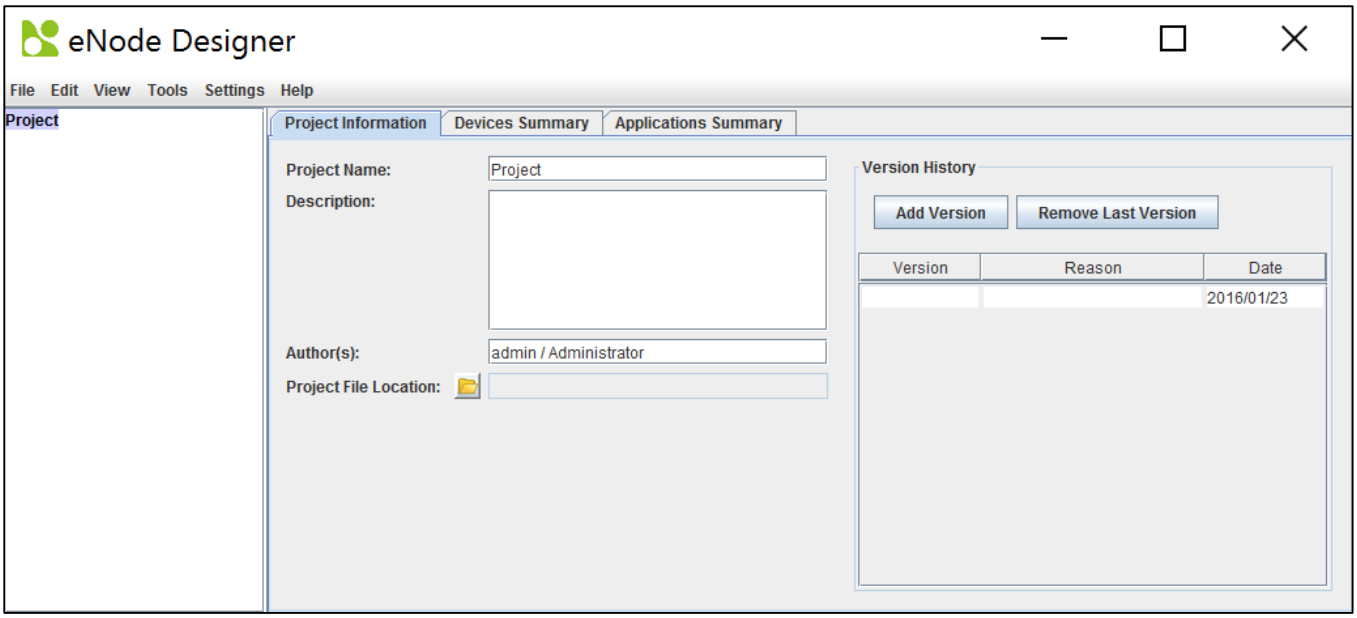


Figure 5-13 - Project Information

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.

5.6.2 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 5.5) they can be added to the project. Since ADH Applications have to 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.

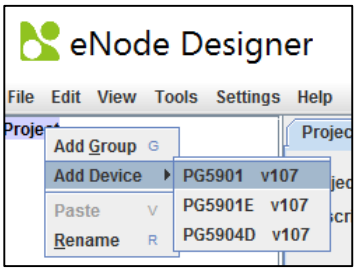


Figure 5-14 - Adding a device to the project.

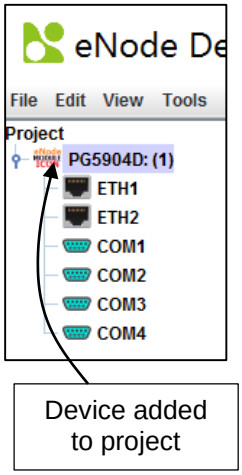


Figure 5-15 - Device added to project.

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.

5.6.3 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 network.

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.

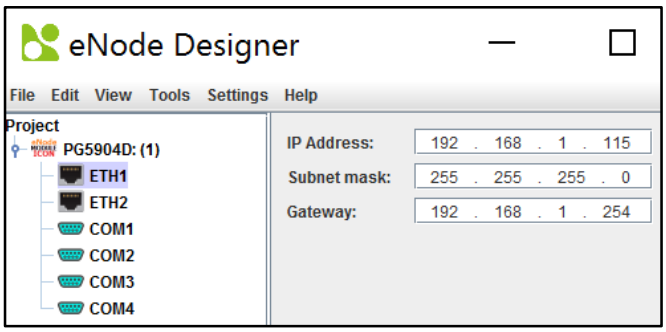


Figure 5-16 – Network properties modified.

5.6.4 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.

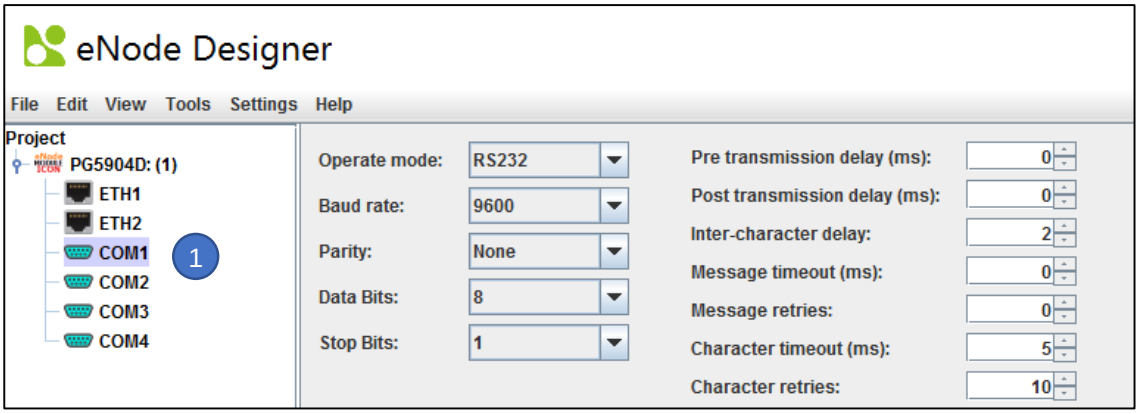


Figure 5-17 - Editing communication port settings example.

5.6.5 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 a 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.

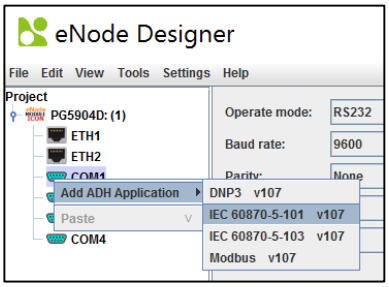


Figure 5-18 - Add ADH Application to communication port example.

When a Client/Server choice is possible for ADH Applications, such as IEC 60870-5-101, you will see a window like Figure 5-19.

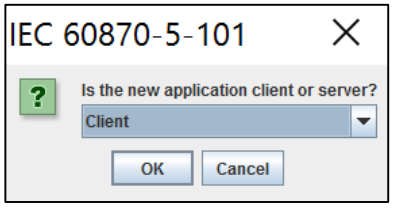


Figure 5-19 - Choosing client or server.

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.

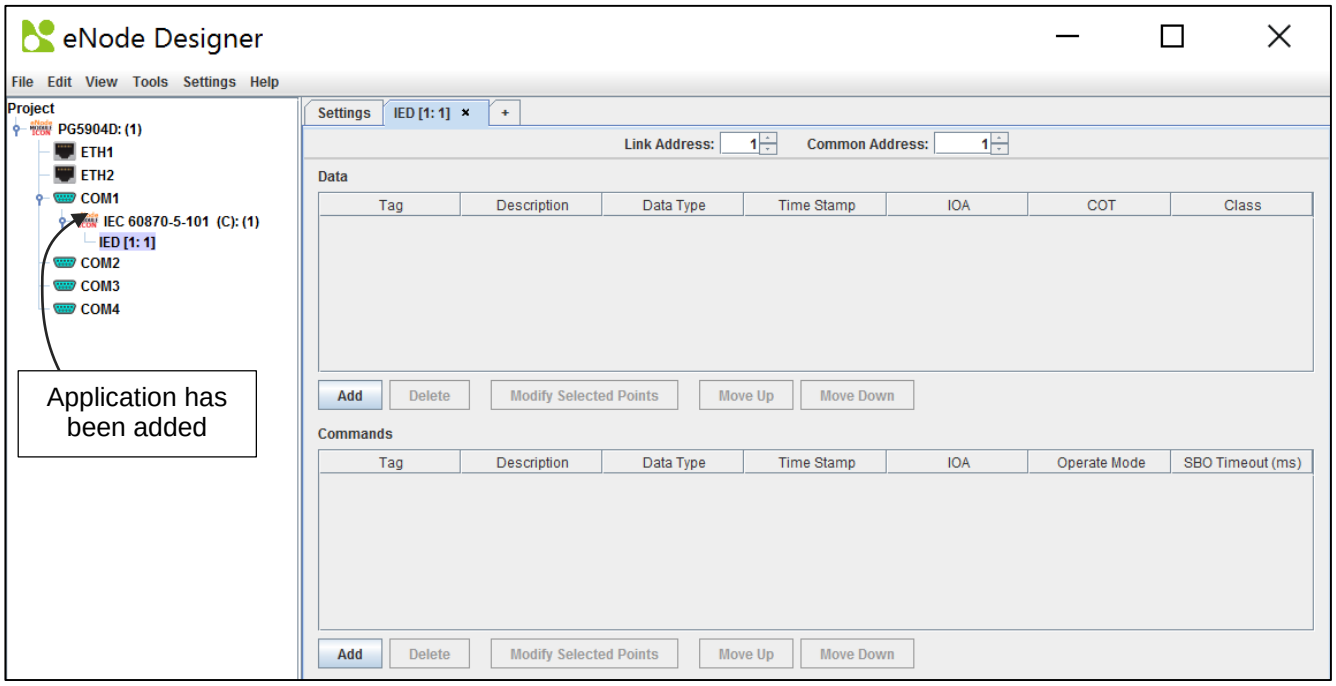


Figure 5-20 - ADH Application added to project.

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.

5.7 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.

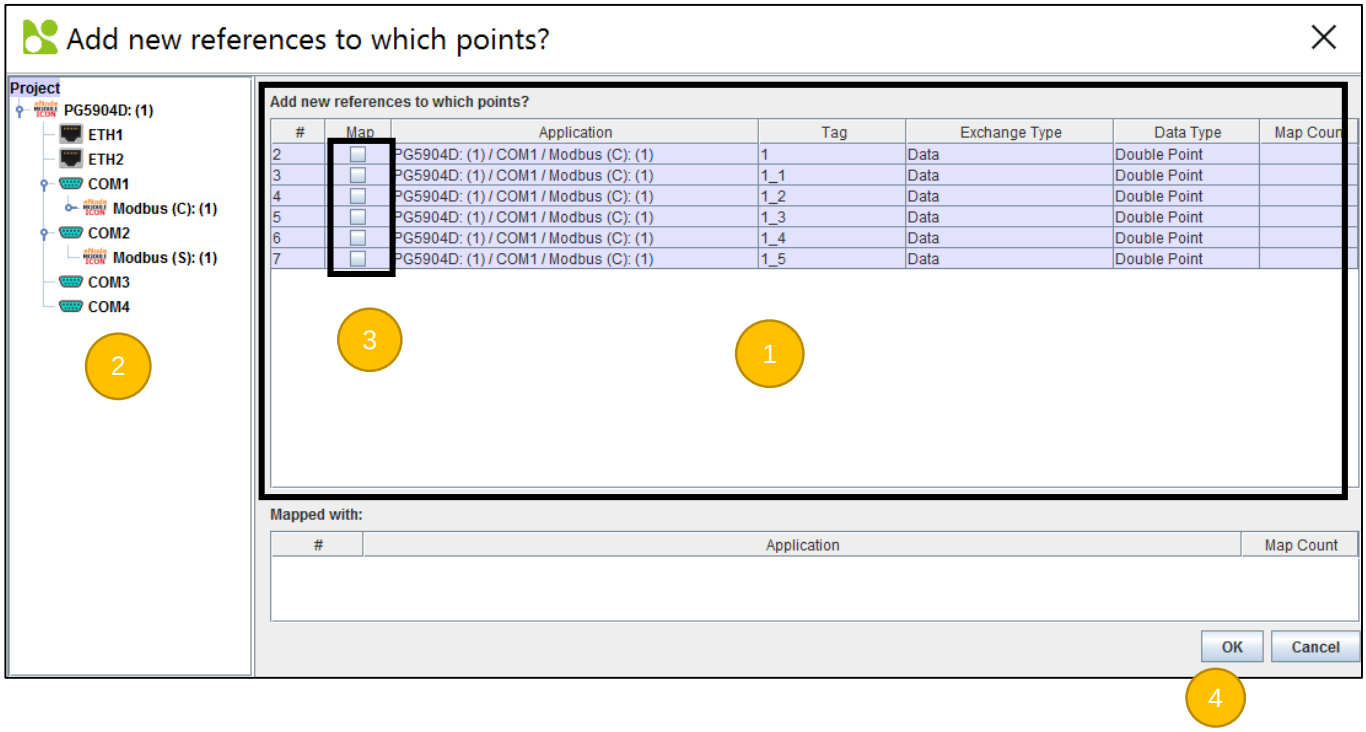


Figure 5-21 - Adding data point references.

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).

5.8 Viewing the Database of Data Points

To view the existing data points in the system use the “Data Point View” window accessed in the **View** menu.

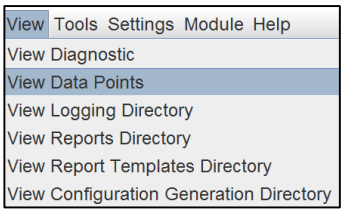


Figure 5-22 - Accessing the data points view.

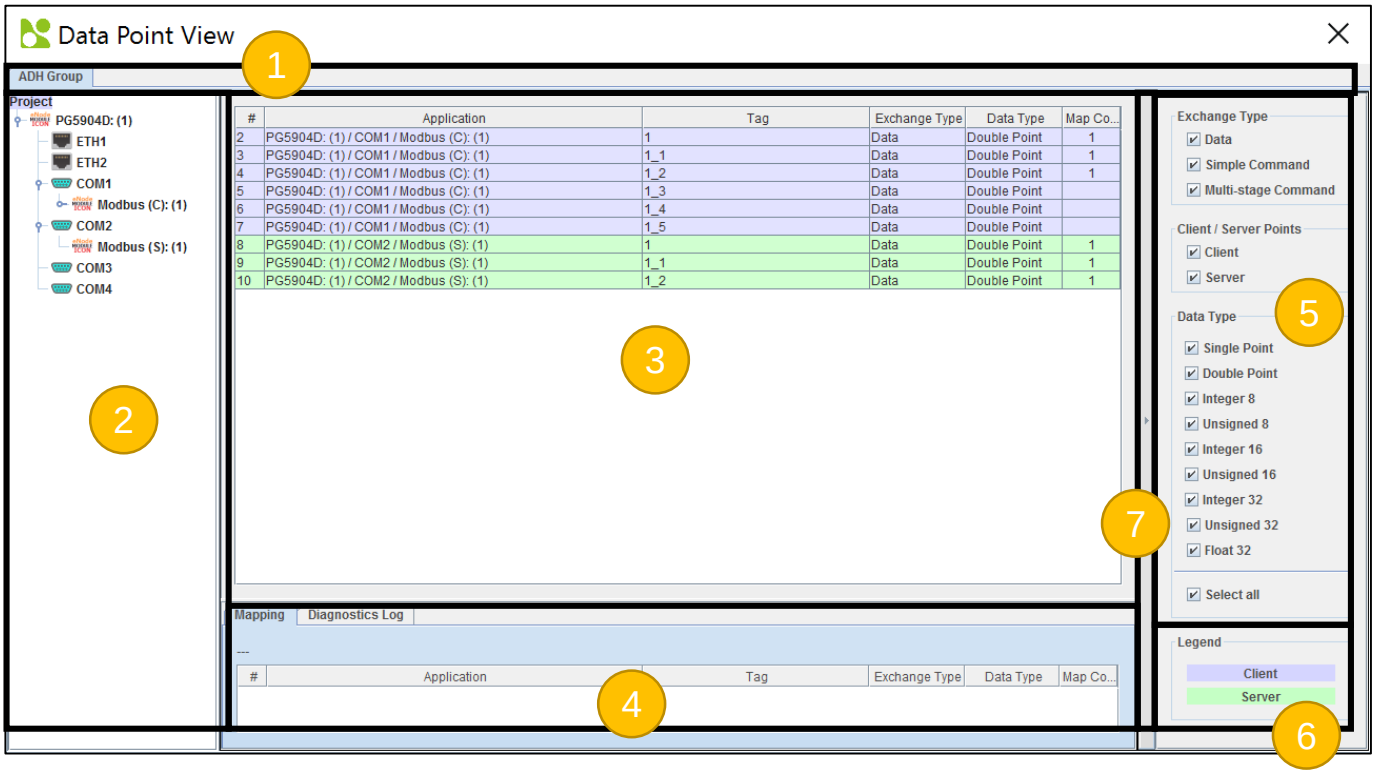


Figure 5-23 - Data point view window.

The data point view window is separated into many sections described below:

1. **ADH Group** – Select which ADH group to look at. Each ADH group is a network group in which only devices in that network can communicate. That is, a device in ADH Group 1 cannot communicate with a device in ADH Group 2. Most projects will only have one network group – in which all devices can communicate with each other.

2. **Project Tree** – The project tree display. The main point list will only show data points beneath the selected tree node.

3. **Data Points** – shows all the data points in the system subject to the filters of (2) and (5).

4. **Mapped Data Points** – shows where the selected data point in (3) is mapped.

5. **Filters** – Only show data points that match the given filters.

6. **Legend** – Describes the colour scheme of the tables.

7 **Show / Hide Filters** – Button to show and hide the right pane containing the filters and legend.

5.9 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.

5.9.1 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”.

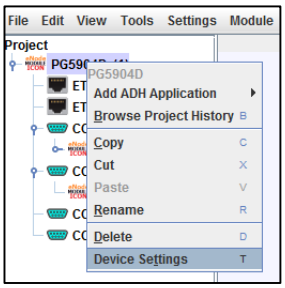


Figure 5-24 - Access device settings to set FTP settings.

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.

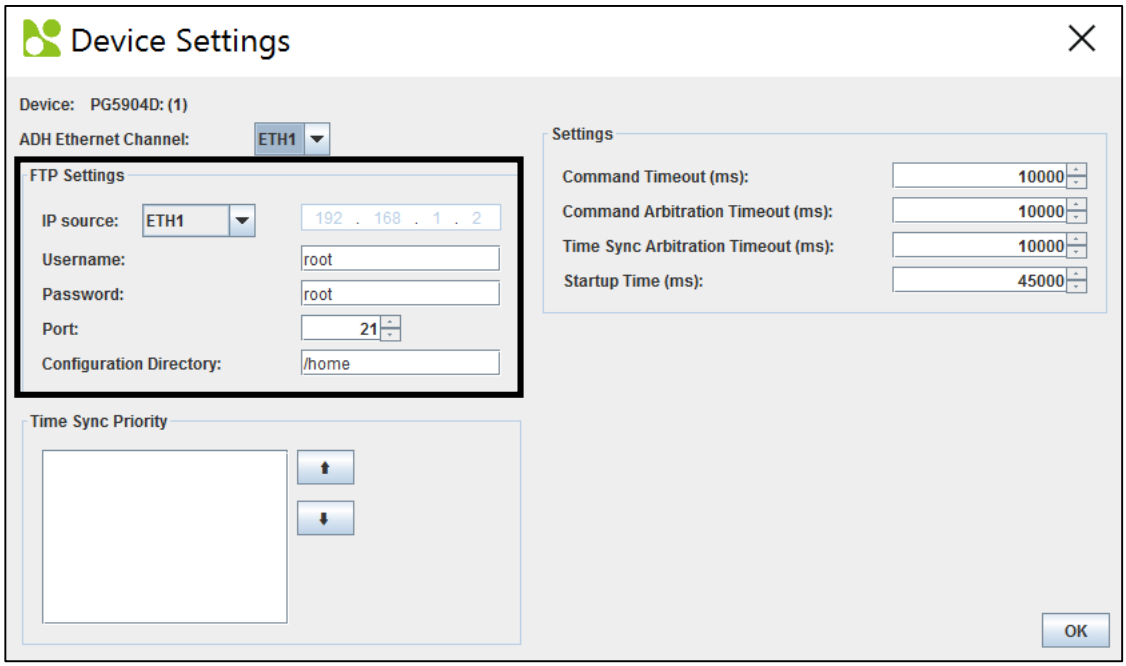


Figure 5-25 - Device settings window.

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.

5.9.2 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.

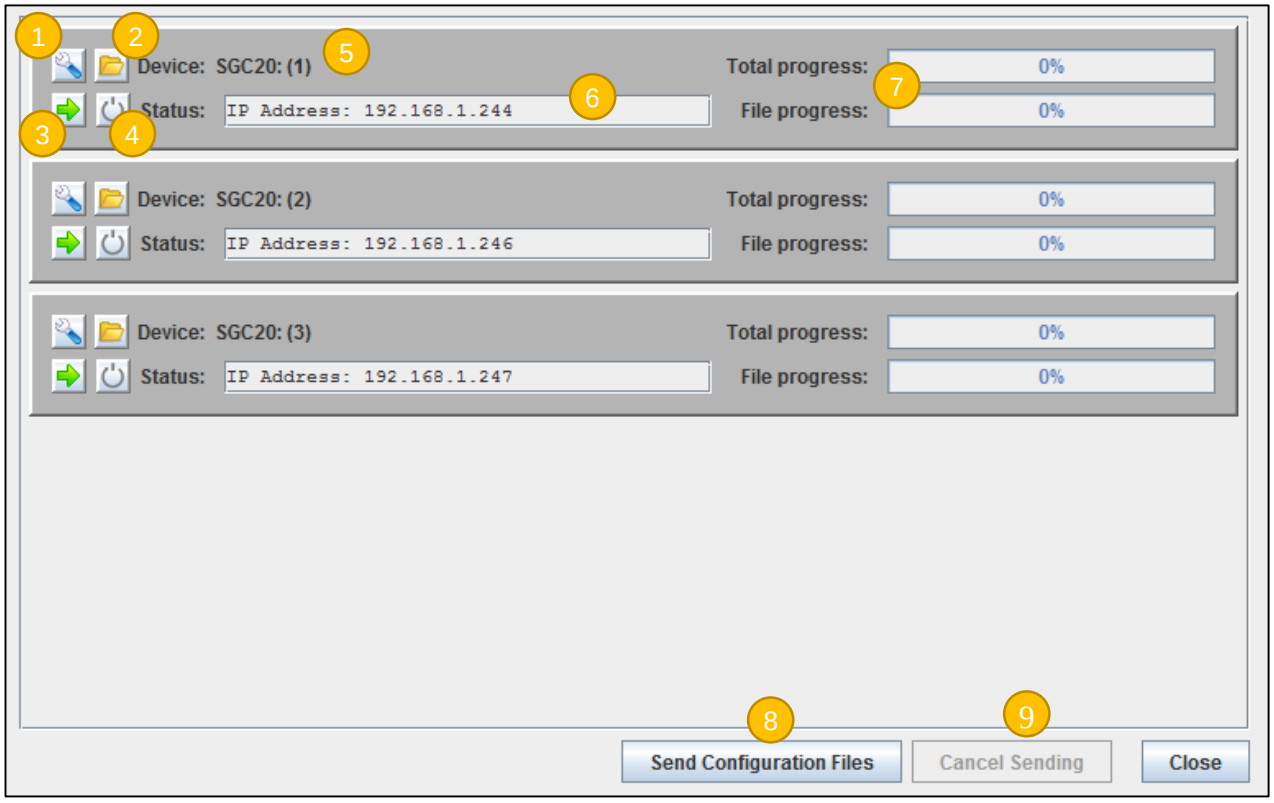


Figure 5-26 - Send configuration files window.

There are descriptions of the buttons and fields below.

1. **Open Device Settings** – Can be used to change FTP settings as in **Figure 5-25**.
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.

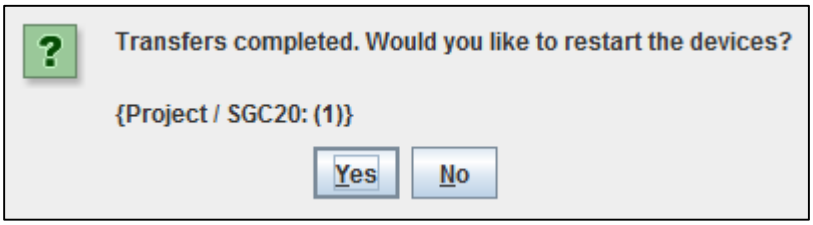


Figure 5-27 - Asked to reboot after sending configuration files.

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

5.10 Diagnostics

Diagnostics is used to examine the the execution of the ADH on target platforms while they are running.

Diagnostics features:

- View live values of all data points on each target platform.

Features that may be implemented in future:

- View communication port traffic – including transmitted and received data.
- Value substitution

The diagnostic information is transferred to eNode Designer by the Diagnostic ADH Application running on the device. As such, diagnostics is started per device, not per application. The diagnostic application is able to view the current data point values on the device.

The diagnostics window is the same as the Data Point View window as in **Section 0:**

Viewing the Database of Data Points. Access the window by the menu option **View => View Data Points**.

To start diagnostics on a device, right click the device (or any tree ancestor) and click “Start Diagnostics”.

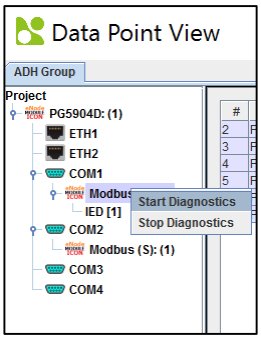


Figure 5-28 - Starting diagnostics.

Starting diagnostics will add a column to the table named “Live Value”, and automatically change the southern tab to the Diagnostics Log.

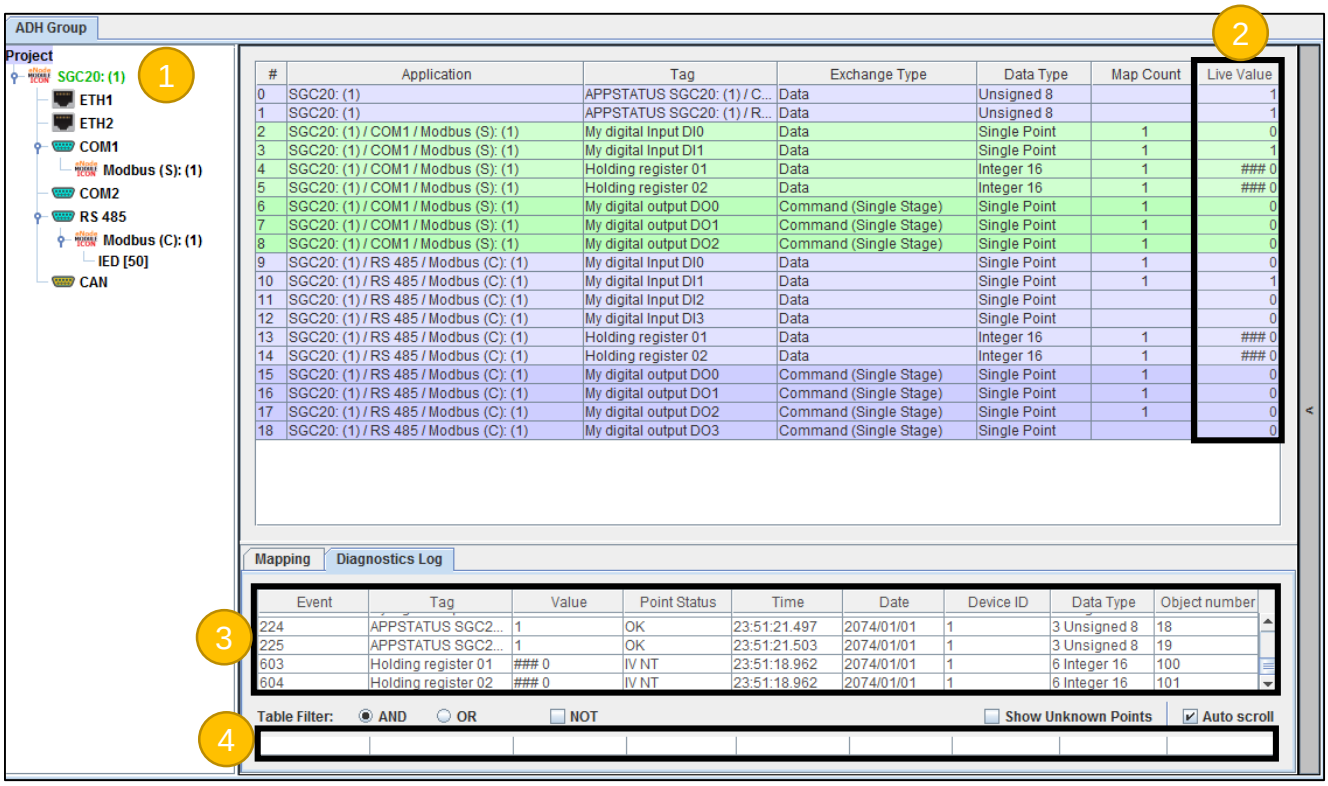
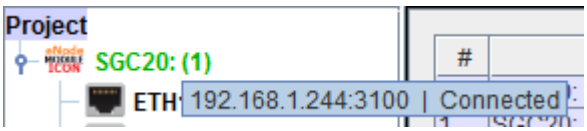


Figure 5-29 - Diagnostics screen explained.

Each major section is described below.

1. **Diagnostic Status** – the device tree node’s colour indicates its diagnostic status. Hovering over the device will give more information.



2 **Live Value** – shows the current value of the data point on the device. If the data point's quality status is not "OK", it will show with a "###" to indicate this.

3 **Diagnostic Log** – a log showing the data point update messages as they come in. This list is filtered by the selection in the project tree.

4 **Table Filter** – Filters the log by the specified values. The filter works with wildcards and the like by using "regular expressions" (regex). For example typing in "DI" in the "Tag" filter would filter the log to only contain points with a Tag containing "DI".

5.11 Loading Projects from a Device

In eNode Designer, every time configuration files are sent, a copy of the current project is also sent to the device. The project is also placed in a "Project History" directory on the device.

eNode Designer can recover any project that has been sent to the device, provided it hasn't been deleted. There are two ways to recover a project.

1. Right-click a device in the project and select "Browse Project History".

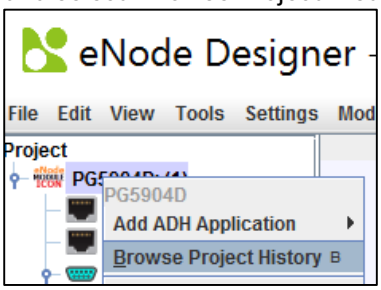


Figure 5-30 - Browse project history of a device in the project.

2. Use the option from the file menu. Using this option only the IP address and FTP details of the device are required, so can be accessed from an empty project.

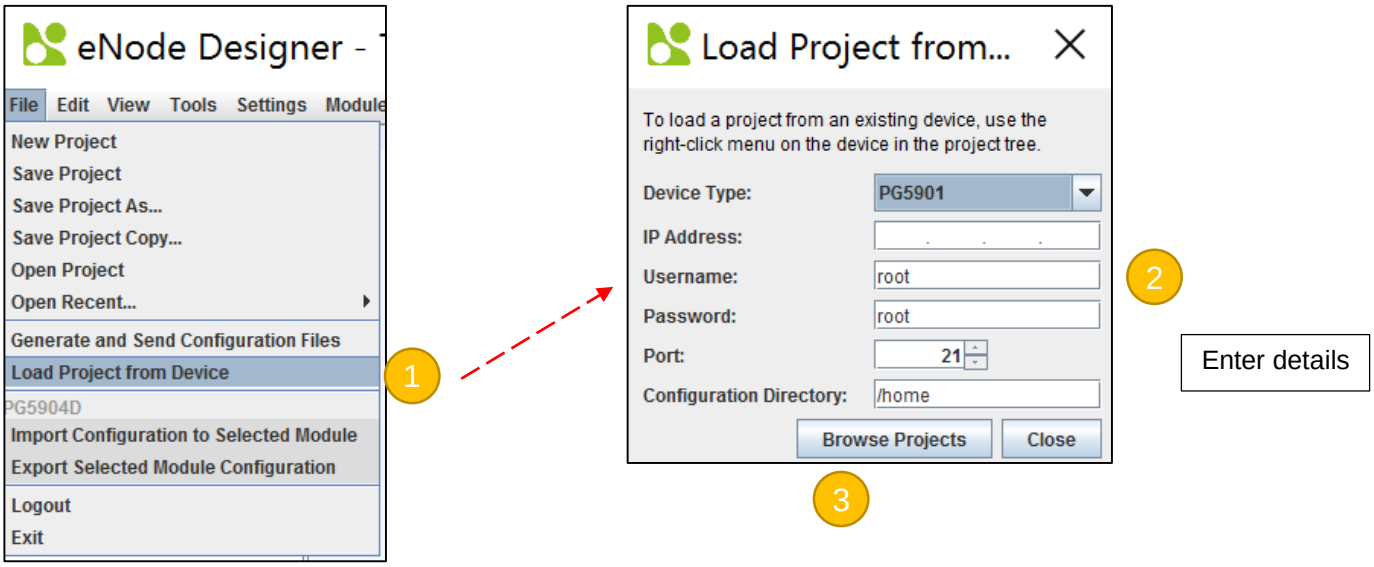


Figure 5-31 – Browse project history of a device unknown to the project.

Using either option, a "Browse Project History" window will open. This will connect to the specified FTP details (or the FTP details registered with the device in the project), and show the project history window.

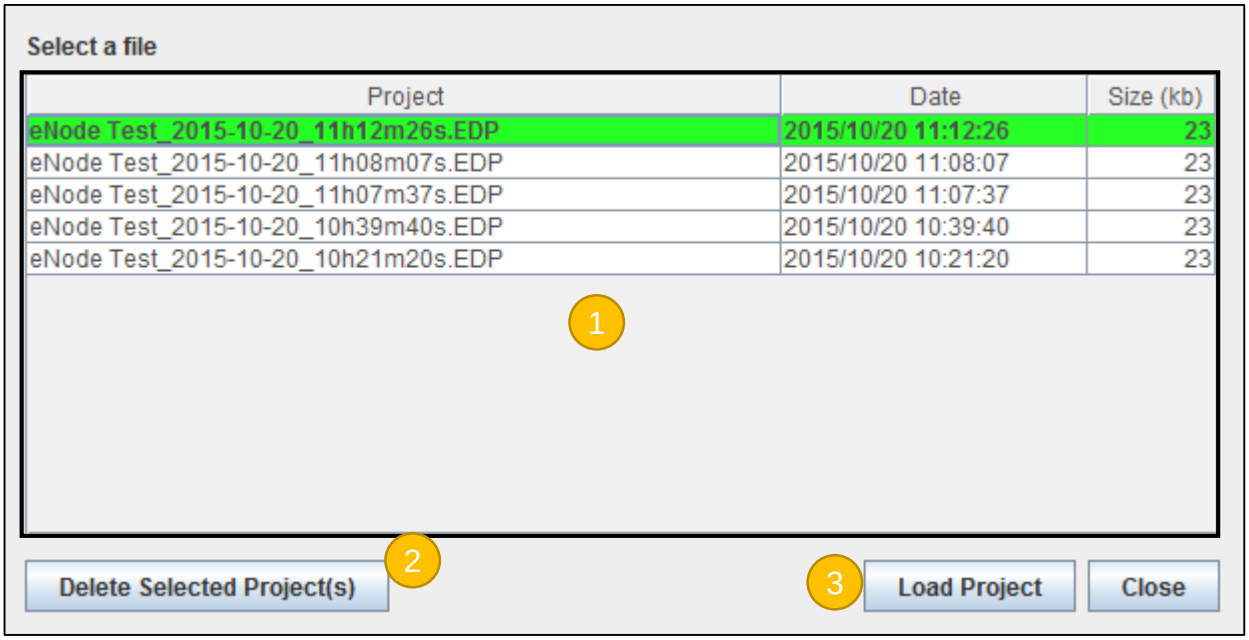


Figure 5-32 - Browse project history.

If the FTP connection and login are successful, the project history will be displayed in a list.

1. This area shows a list of projects which have been sent to the device. The currently active project is highlighted in green.
2. Use this button to delete projects from history. A confirmation message will appear. The currently active project cannot be deleted.
3. Retrieves the selected project from the device and loads it in eNode Designer.

5.12 Organising a Project

The eNode Designer tool allows managing a single product or a number of products to be configured and managed in one project.

►*Tip: It is always a good idea to use "Groups" in the project tree to define the location of a product if several units are being managed in one project file.*

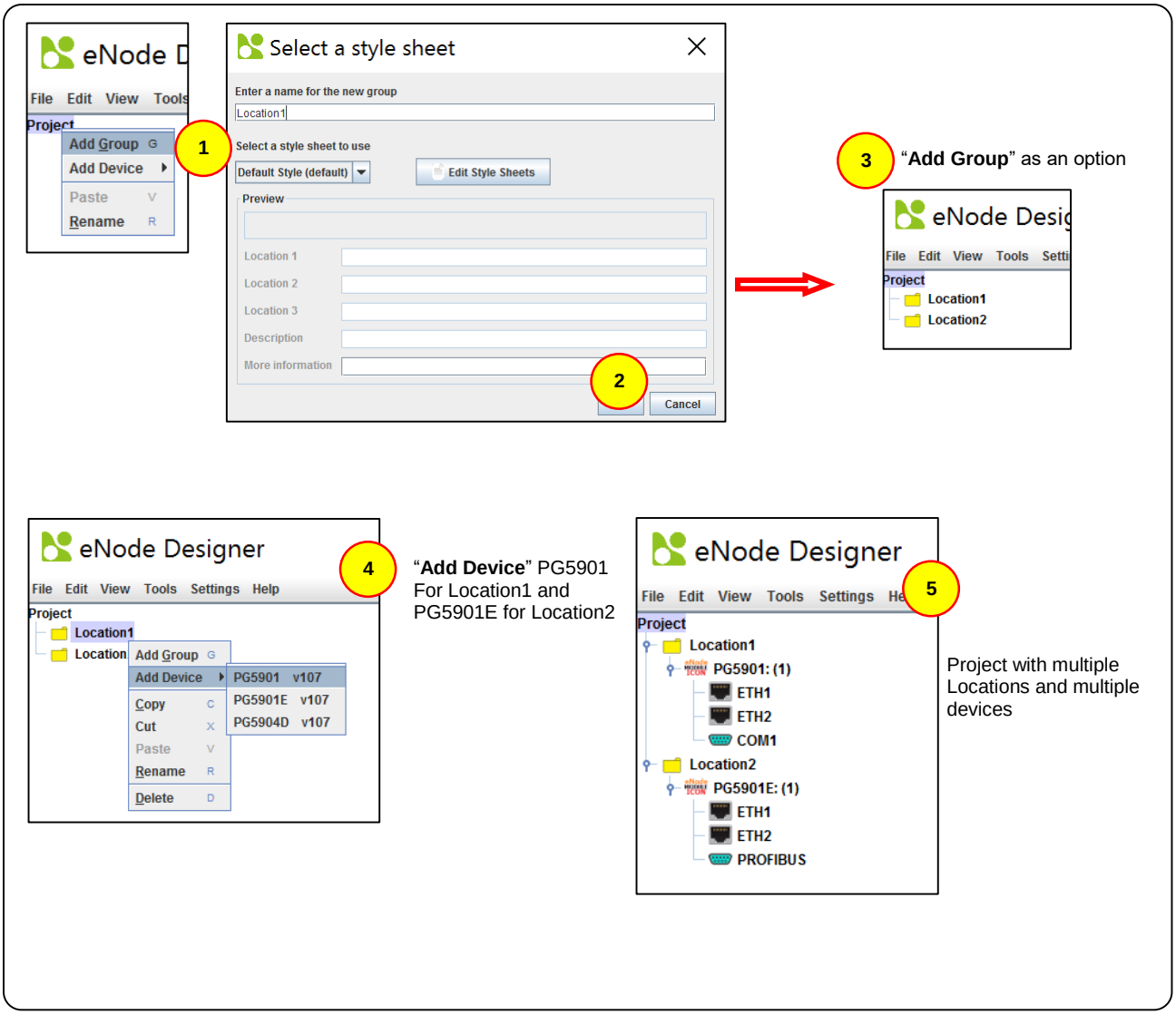


Figure 5-33 – Project tree organisation.

Groups can be added to the project root and inside other groups. For a detailed explanation about the options when adding groups, see **Section 5.13.2: Creating a Group with a Style Sheet**.

5.13 Advanced – Tree Group Style Sheets

Any project in eNode Designer can use logical groupings in the project tree to organise the project. For convenience, each of logical groups in the tree can contain customized information. There is an example in Figure 5-34.

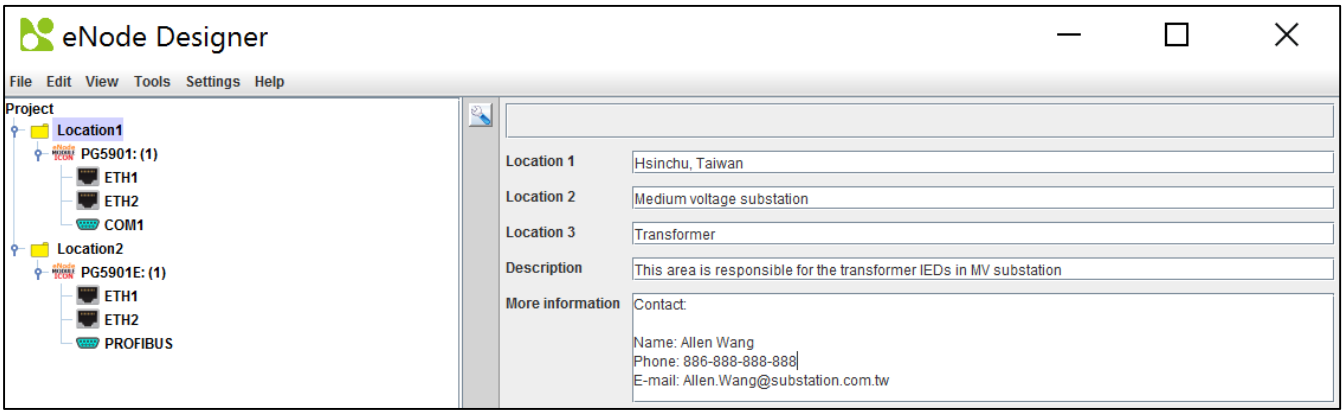


Figure 5-34 - Project tree group example.

In addition, exactly what labels and fields are available are customisable. This is achieved through “Style Sheets”. Each style sheet describes a set of fields, including their field types and labels. Every group is bound to a style sheet, and each style sheet can be used by many groups.

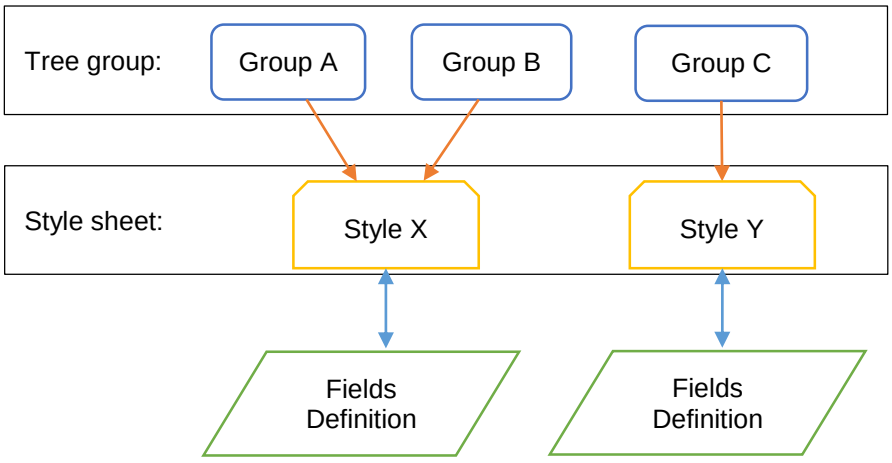


Figure 5-35 - Style sheet interaction with groups.

5.13.1 Editing the Style Sheets

The definition of a style sheet can be changed, and new style sheets can be added and removed. This is accessible through the **Tools** menu as shown below.

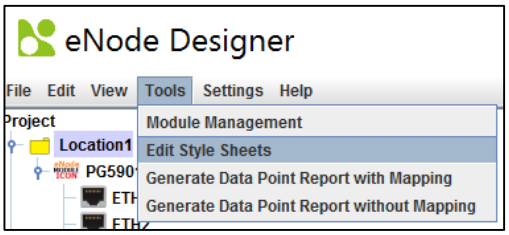


Figure 5-36 - Accessing the style sheets.

This will open the window to edit style sheets.

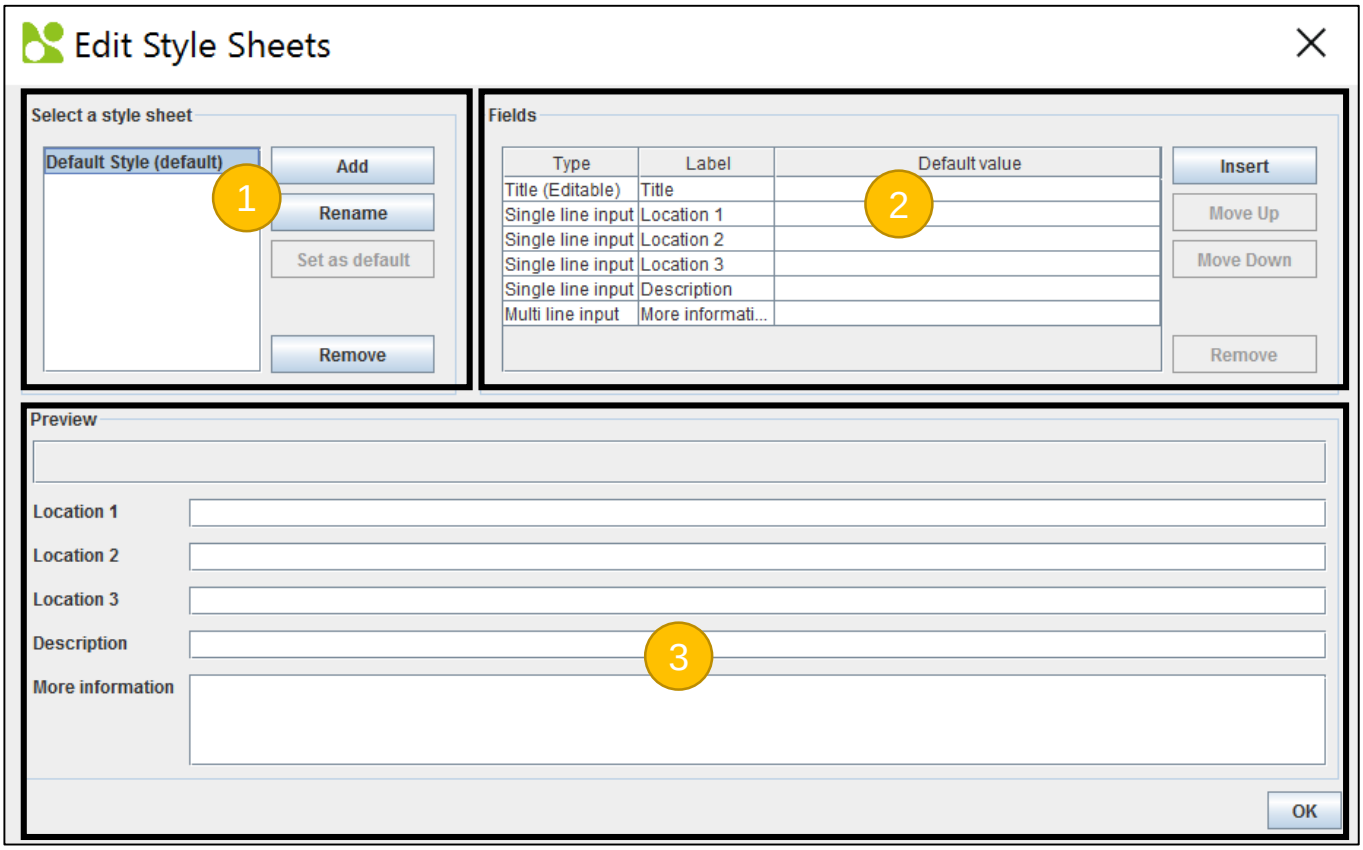


Figure 5-37 - Edit style sheets window.

There are three sections to the window:

1. **Style sheet selection** – Select which style sheet to investigate and edit.
2. **Fields** – The fields of the selected style sheet. This includes a type, label and default value.
3. **Preview** – The preview window of the style sheet, with default values. Editing the values in the preview will set the default values of the field.

The **fields** can be edited in the field table in area (2). The labels describe the static values which will appear before the text. The default value is the values which will appear in a new tree group when it is added to the project.

The field types available are:

- **Title (Constant)** – A title that is the same for all tree groups with this style.
- **Title (Editable)** – A title area in which each tree group can have its own value.

- **Single line input** – A single line input like “Location 1” in the above example.
- **Multi line input** – A multiple line input which takes up remaining space, as in “More Information” in the above example.

Examples:
You can change the labels and default values by editing the fields table. You can also type in the preview screen to modify the default value.

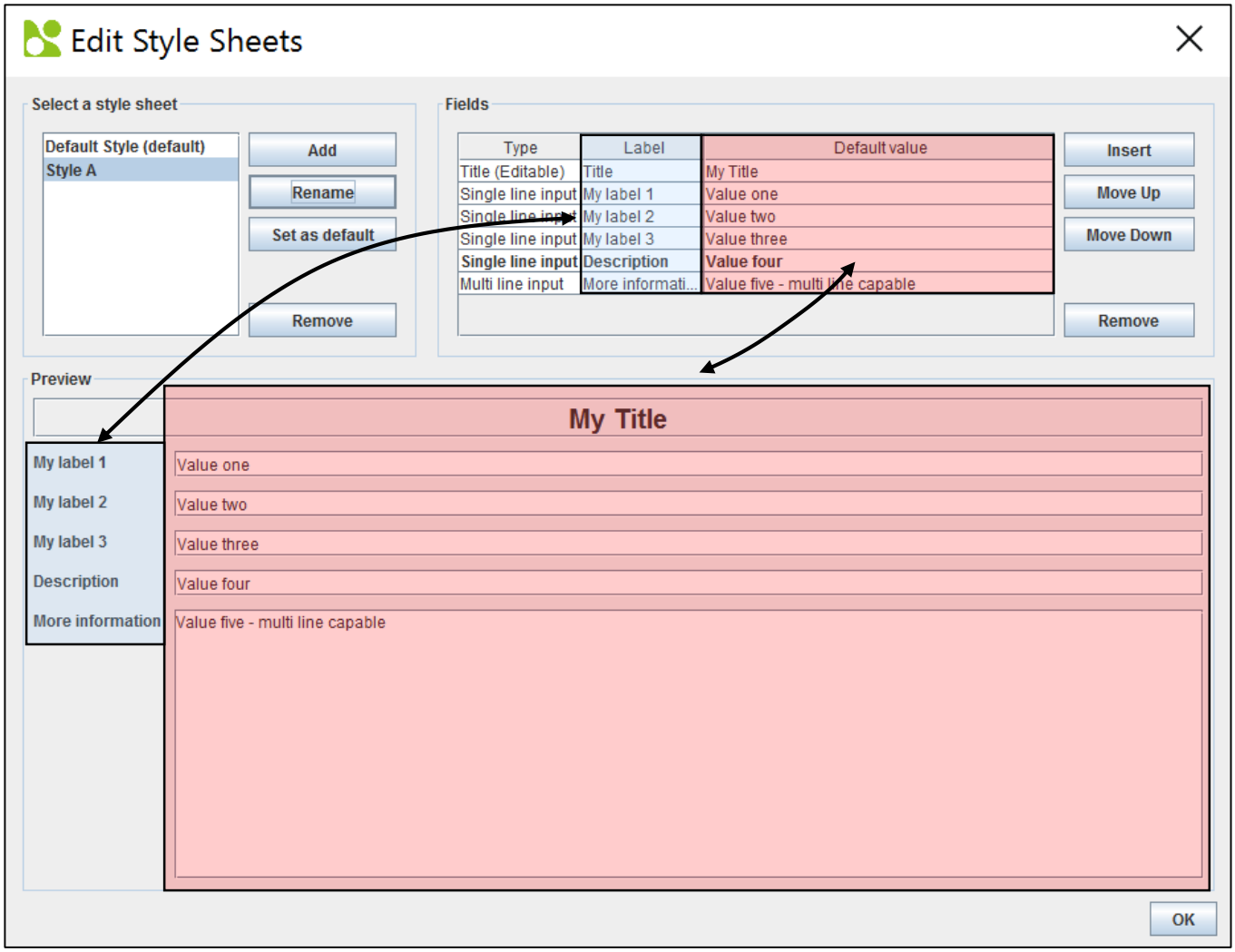


Figure 5-38 - Style sheet example one.

If we change the description to be a multi-line input, the remaining space will be evenly taken by both multi-line inputs.

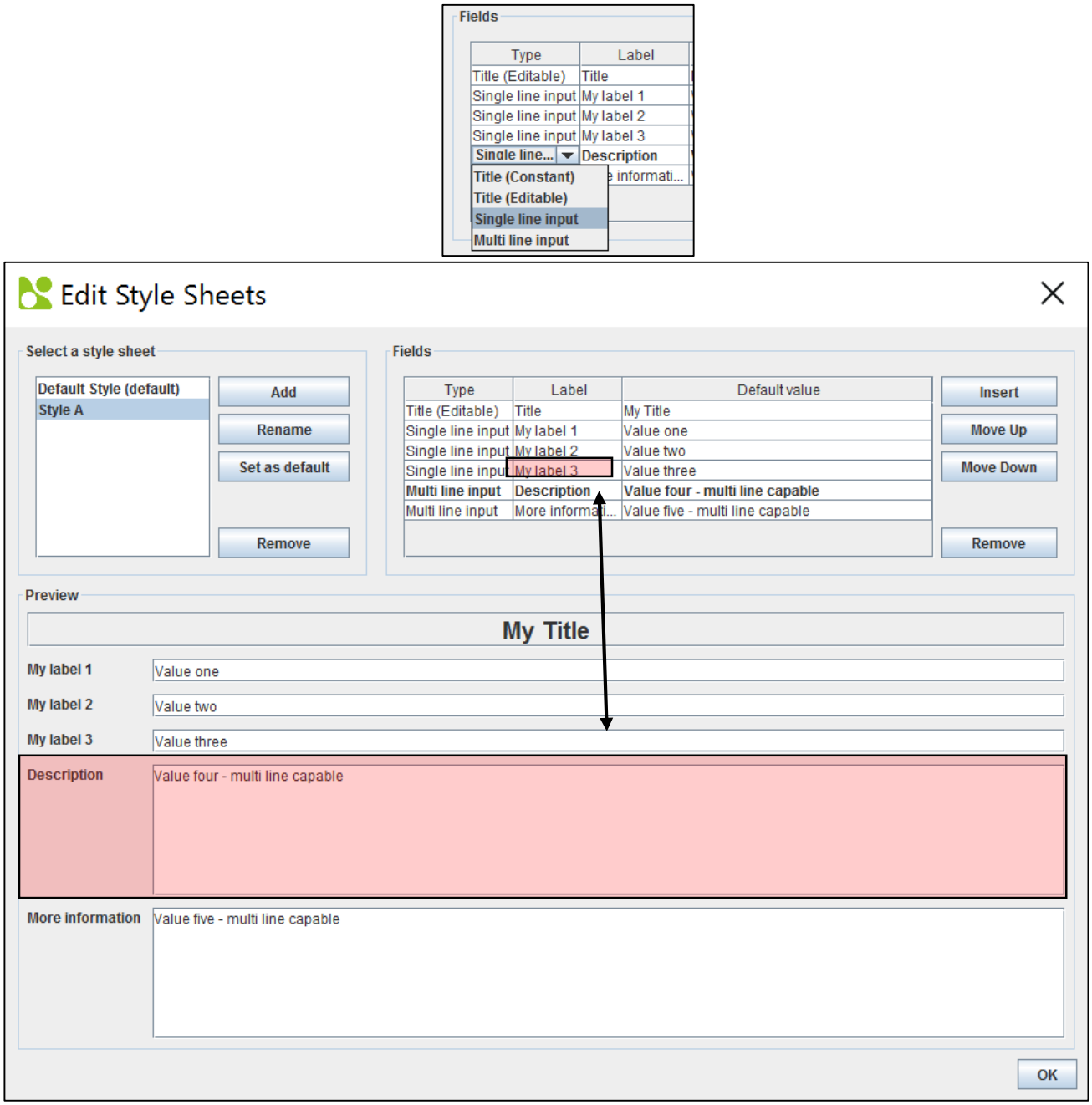


Figure 5-39 - Style sheet example two.

5.13.2 Creating a Group with a Style Sheet

When tree groups are added to the project, they need to bind to a style sheet. Select “Add Group” from the project tree menu. Groups can be added to the root project node and within other groups.

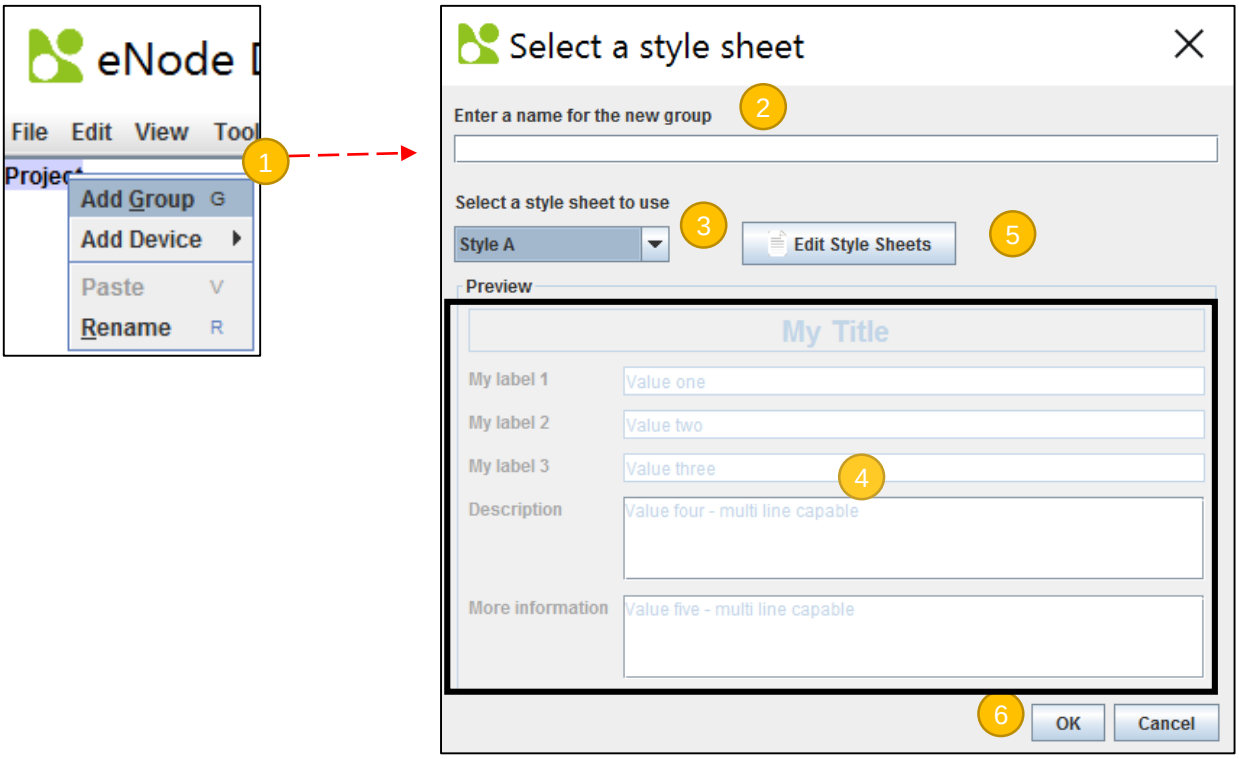


Figure 5-40 - Adding a group to the project.

1. Select “Add Group” from the right-click menu.
2. Enter the new name for the group. This is the name which will appear in the tree. It can be renamed later.
3. Select a style sheet to use. This shows a drop-down menu of all style sheets in the project.
4. A preview of the selected style sheet.
5. A convenience button to access the style sheet definitions.
6. Click **OK** when done.

A new group will be added to the project with the selected style sheet and default value.

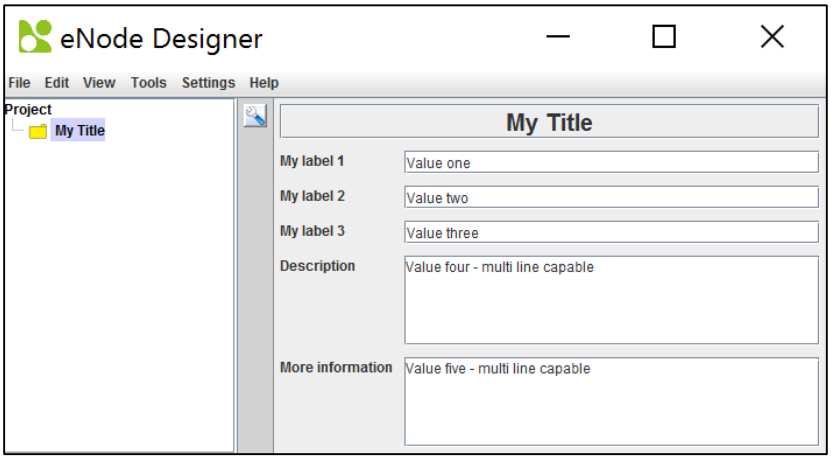


Figure 5-41 - Group with style sheet has been added.

5.13.3 Changing and Existing Group's Style Sheet

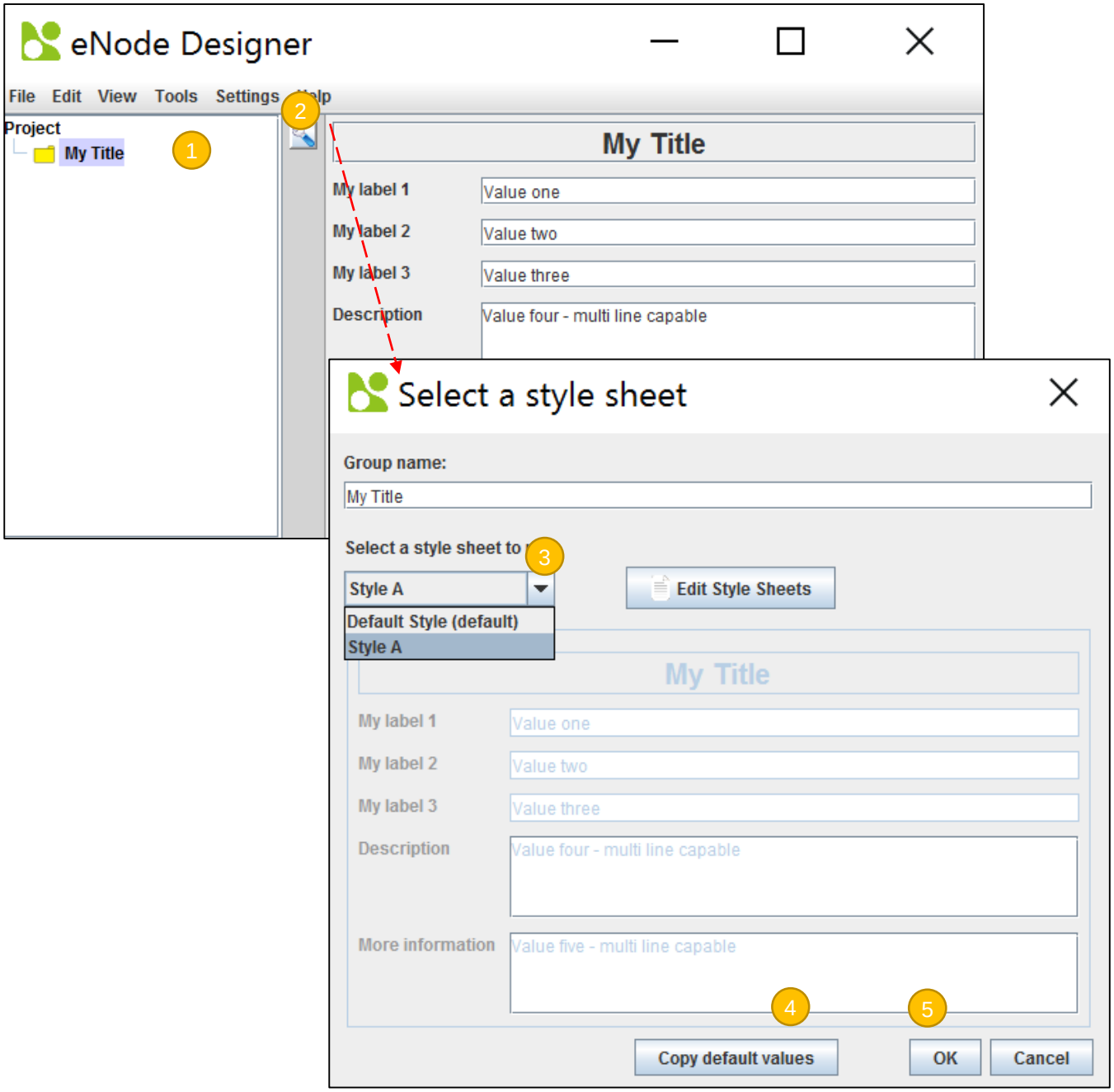


Figure 5-42 - Change the style sheet of existing group.

1. Select the group in the tree.
2. In the display pane of the group, there is a button. Clicking this will open a new window.
3. Select a new style sheet to use. This shows a drop-down menu of all style sheets in the project.
4. (Optional) Copies (resets) the values of the tree group to the defaults of the style sheet.
5. Click OK when done.

5.14 Report Generation

The following reports can be generated by eNode Designer.

- Data point report (with and without mapping). Access this by the **Tools** menu.

Generated reports are in the form of Microsoft Excel™ spreadsheets. They are based on editable user-editable Excel *templates*. To view and edit the template, use the **View => View Report Templates Directory** option in the eNode Designer menu bar.

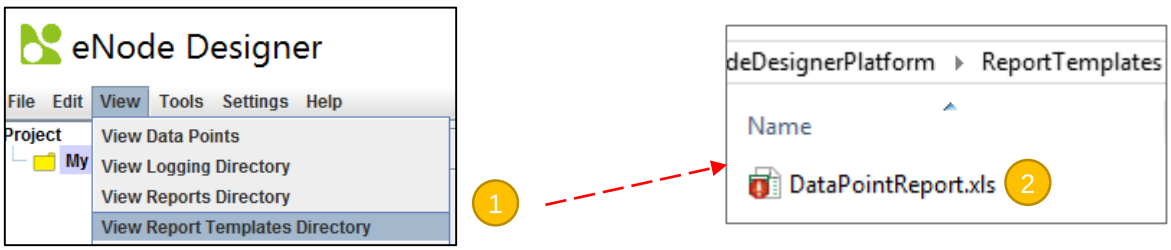
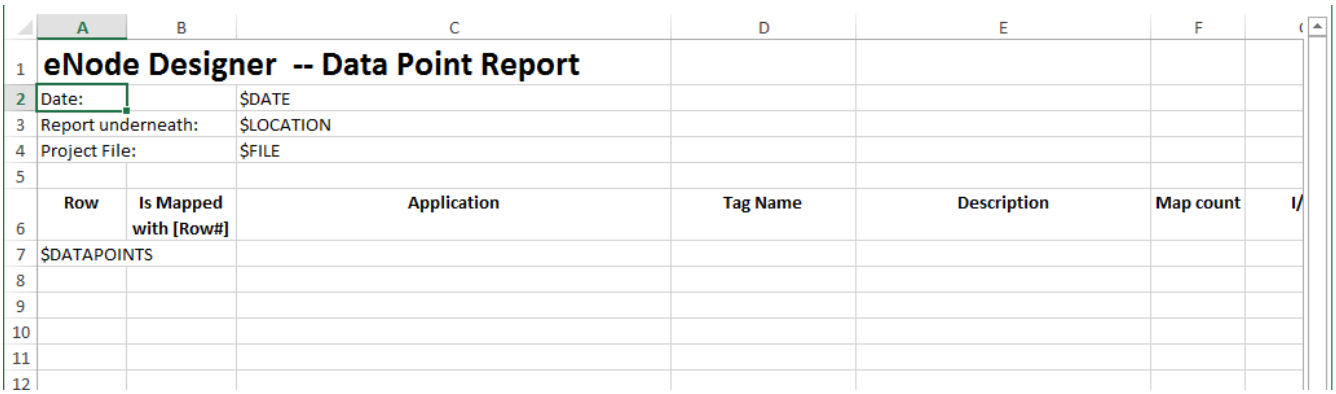


Figure 5-43 - Open report templates directory.

1. Clicking this will open the reports template directory in your operating system's file explorer.
2. Open the report template

5.14.1 Data Point Report Template

The data point report template generates a report on the data points beneath the specified location in the project tree. The default template looks like this.



	A	B	C	D	E	F
1	**eNode Designer -- Data Point Report**					
2	Date:		$DATE			
3	Report underneath:		$LOCATION			
4	Project File:		$FILE			
5						
6	**Row**	**Is Mapped with [Row#]**	**Application**	**Tag Name**	**Description**	**Map count**
7	$DATAPOINTS					
8						
9						
10						
11						
12						

Figure 5-44 - Data point report template.

All cell text, widths and heights are editable by the user. The generated report will start with a copy of the template and then just replace the *keywords*.

A cell must contain the *exact keyword* in order for it to be replaced. The keywords are as follows:

- $DATE – The date the report is generated.
- $LOCATION – The tree node location which is being reported on.
- $FILE – The filename of the eNode Designer project for which the report is generated.
- $DATAPOINTS – Data point information will replace this row and every row beneath this row, up to the number of rows required to generate the full report.

Replacing the values of data points *does not examine the title of the columns*. The columns output will always be in the same order.

5.15 Settings

The settings available in eNode Designer are available by using the Settings menu.

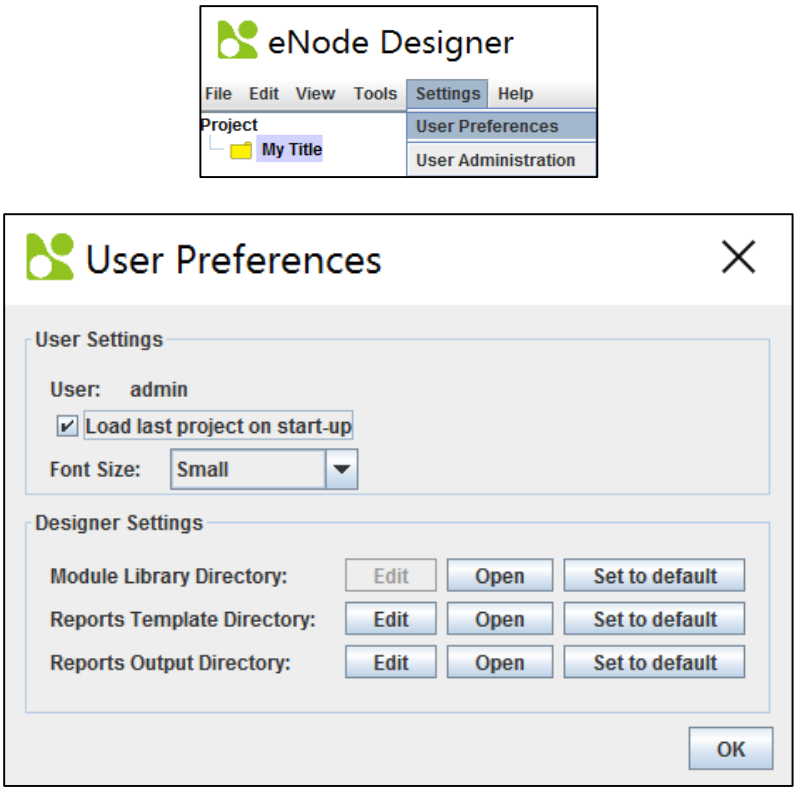


Figure 5-45 - Settings window.

Here the user's language and preferences can be set. The settings of eNode Designer can also be set in this window. Setting the language for eNode Designer will set it for all users that have "Use platform settings" set for their locale. An individual user can override the eNode Designer's language by specifying it as a particular language.

The locations of some directories of eNode Designer can also be set and opened in this window.

6 eNode designer Reference Guide

6.1 Menu Bar Options

6.1.1 File

Function	Description
New Project	Creates a new empty project.
Save Project	Saves the current project.
Save Project As…	Saves the current project as a new file.
Save Project Copy…	Copies current project to a new file. Editing continues on the original file
Open Project	Loads an eNode Designer project.
Open Recent	Shows recent project files for faster processing.
Generate and Send Configuration Files	Generates and sends the target platform settings and ADH application configuration files to the target platforms. See section Generate and Send Configuration Files 5.9 for details.
Load Project From Device	Loads the eNode Designer project stored on a target device. See section 5.11 for details.
Logout	Logs out of the current user.
Exit	Exits eNode Designer.

6.1.2 Edit

Function	Description
Copy	Copies the selected tree node (to be pasted).
Cut	Cuts the selected tree node (to be pasted).
Paste	Pastes the copied or cut tree node beneath the currently selected tree node.
Delete	Deletes the currently selected tree node.

6.1.3 View

Function	Description
View Data Point	Views the current data points in the system. Allows to access diagnostics.
View Logging Directory	Opens the directory containing log files.
View Reports Directory	Opens the directory containing reports, such as data point reports.
View Report Templates Directory	Opens the directory containing report templates
View Configuration Generation Directory	Opens the directory containing the files produced when sending configuration files to target platforms
Communication Overview	Opens a graphical display showing which devices are configured to communicating in the current project.

.

.

6.1.4 Tools

Function	Description
Module Management	Opens the module management window, responsible for importing, enabling and disabling eNode Modules.
Edit Style Sheets	Allows the user to define the tree group style sheets.
Generate Data Point Report with Mapping	Generates a data point report with mapping, using the report template.
Generate Data Point Report without Mapping	Generates a data point report without mapping, using the report template.

6.1.5 Settings

Function	Description
User Preferences	Opens the settings for the eNode Designer Platform and the current user.
User Administration	Opens the user administration window, allowing editing users and user groups.

6.1.6 Help

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

6.2 Tree Menu Options

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

Table 6-1 - Tree context menu options.

Atop Technologies, Inc.

www.atoponline.com
www.atop.com.tw

TAIWAN HEADQUARTER:

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.
Tel: +886-3-550-8137
Fax: +886-3-550-8131

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231

ATOP INDIA OFFICE:

Abhishek Srivastava
Head of India Sales
Atop Communication Solution(P) Ltd.
No. 22, Kensington Terrace,
Kensington Rd,
Bangalore, 560008, India
Tel: +91-80-4920-6363
E-mail: Abhishek.S@atop.in

ATOP INDONESIA BRANCH:

Jopson Li
Branch Director
Wisma Lampung Jl.
No. 40, Tomang Raya
Jakarta, Barat, 11430, Indonesia
Tel: +62-857-10595775
E-mail: jopsonli@atop.com.tw

ATOP EMEA OFFICE:

Bhaskar Kailas (BK)
Vice President (Business Development)
Atop Communication Solution(P) Ltd.
No. 22, Kensington Terrace,
Kensington Rd,
Bangalore, 560008, India
Tel: +91-988-0788-559
E-mail: Bhaskar.k@atop.in

ATOP AMERICAs OFFICE:

Venke Char
Sr. Vice President & Head of Business
11811 North Tatum Blvd, Suite 3031
Phoenix, AZ 85028,
United States
Tel: +1-602-953-7669
E-mail: venke@atop.in