Atop Technologies, Inc.

PG5201B Series

Low-Power Wide-Area LTE Protocol Gateway

User Manual
v1.0
April 10th, 2025

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.

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
sales@atop.com.tw
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 names referenced herein are registered trademarks of their respective companies.

Documentation Control

Author:	Simon Huang
Revision:	1.0
Revision History:	Initial version
Creation Date:	14th March 2025
Last Revision Date:	10th April 2025
Product Reference:	PG5201B Low-Power LTE Protocol Gateway User Manual
Document Status:	Significant updates

Table of Contents

Table of Figures

List of Tables

1 Preface

1.1 *Purpose of the Manual*

This manual supports user during the installation and configuring of the PG5201B Industrial Device Protocol Gateway. It explains the technical features available with the product. For example, it contains some advanced network management knowledge, instructions, examples, guidelines, and general theories to assist user's device management in both hardware and software. A background in general theory is necessary when reading it. Please refer to the Glossary for technical terms and abbreviations (if any).

1.2 *Who Should Use This User Manual*

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

1.3 *Supported Platform*

This manual is designed for PG5201B **Low-Power Protocol Gateway** only**.**

1.4 *Manufacturers' FCC Declaration of Conformity Statement*

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

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:
1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause an undesired operation.

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

2 Introduction

2.1 Overview

PG5201B is a Low-Power Wide-Area (LPWA) LTE Protocol Gateway, serving as a protocol converter. It provides seamless protocol conversion for devices in industrial network operations. With its rugged construction, PG5201B is designed to perform in the most demanding of industries – including power distribution, oil and gas, manufacturing, and agriculture. As a highly reliable and fault-tolerant Industrial Protocol Gateway, also features integrated 4G connectivity, making it ideal for any industry looking to implement devices at remote locations for smart grid operations.

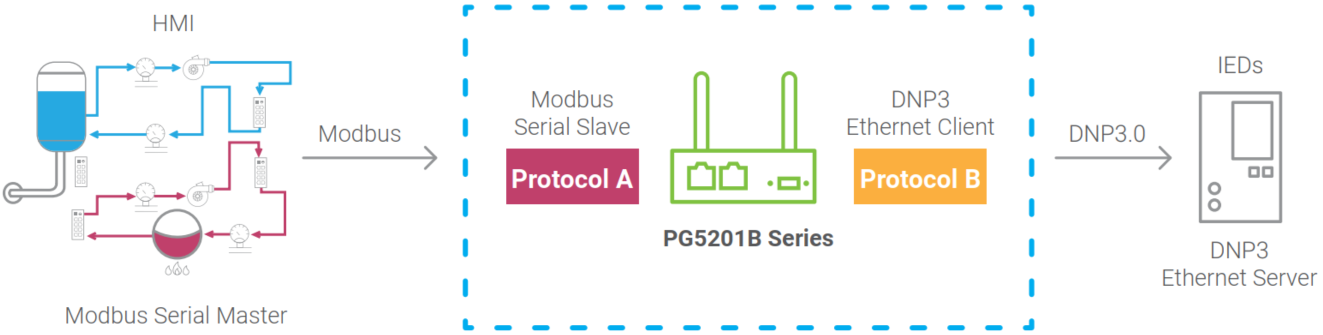


Figure 2-1 An Application of PG5201B with Modbus Serial HMI to DNP3

2.2 Features

The PG5201B Low-Power Protocol Gateway shares the same software platform on different available hardwares. It provides

- Flexible hardware platform, in different port variants based on your needs
- Configuration via Web Browser/Serial Console/Telnet Console/Atop's Windows Utility (Device Management Utility)
- Rugged metal housing with IP30 protection for wall or DIN-Rail mount
- Wide range power supply input between 9 - 48 VDC

Caution

Beginning from here, extreme caution must be exercised.

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

Warning: HOT!

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

3 Getting Started

3.1 *Packing List*

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

Table 3.1 Packing List

Item	PN	PG5201B-DB	PG5201B-TB	PG5201B-DB-GPS	PG5201B-TB-GPS	PG5201B-M1-DB	PG5201B-M1-TB
Terminal Block (7P)	TBD	1	1	1	1	1	1
Terminal Block (5P)	TBD	N/A	1	N/A	1	N/A	1
Terminal Block (3P)	TBD	N/A	N/A	N/A	N/A	N/A	N/A
LTE Antenna	TBD	2	2	2	2	N/A	N/A
LTE Antenna	TBD	N/A	N/A	N/A	N/A	1	1
GPS Antenna	TBD	N/A	N/A	1	1	N/A	N/A
Hardware Installation Guide (Warranty card is included)	TBD	1	1	1	1	1	1

Note:

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

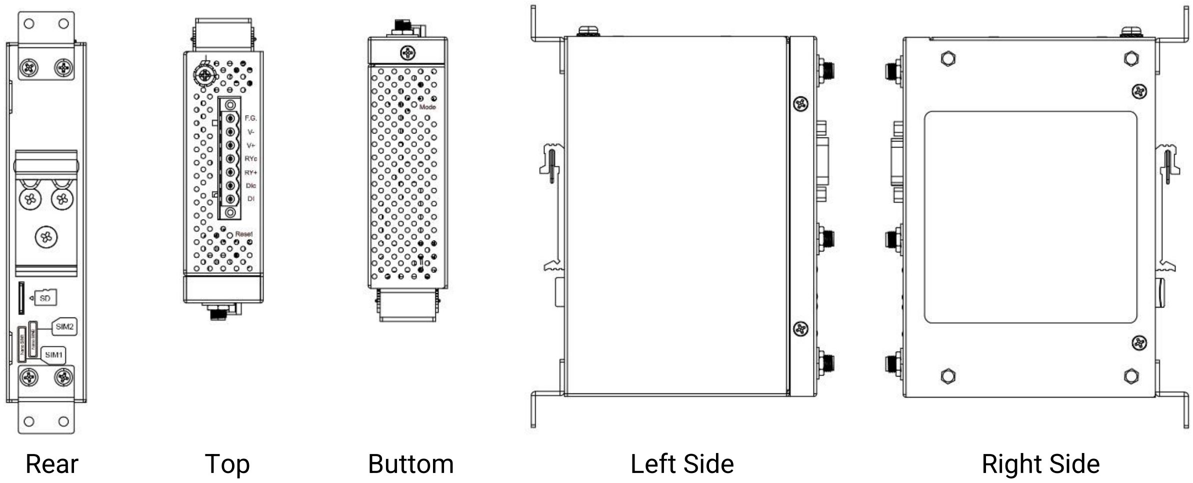
Table 3.2 Description of Optional Accessories

Optional Accessories		
Model Name	**Part Number**	**Description**
UN315-1212 US-Y	50500151120003G	Y-Type power adapter, 100~240VAC input, 1.25A @ 12VDC output, US plug, LV6
UNE315-1212 EU-Y	50500151120013G	Y-Type power adapter, 100~240VAC input, 1.25A @ 12VDC output, EU plug, LV6
ADP-DB9(F)-TB5	59906231G	Female DB9 to Female 3.81mm TB5 Converter
WMK-315-Black	70100000000050G	Black Aluminium Wall Mount Kit

3.2 *Appearance, Front and Rear Panels*

The following figures show PG5201B series device’s front and rear panels.

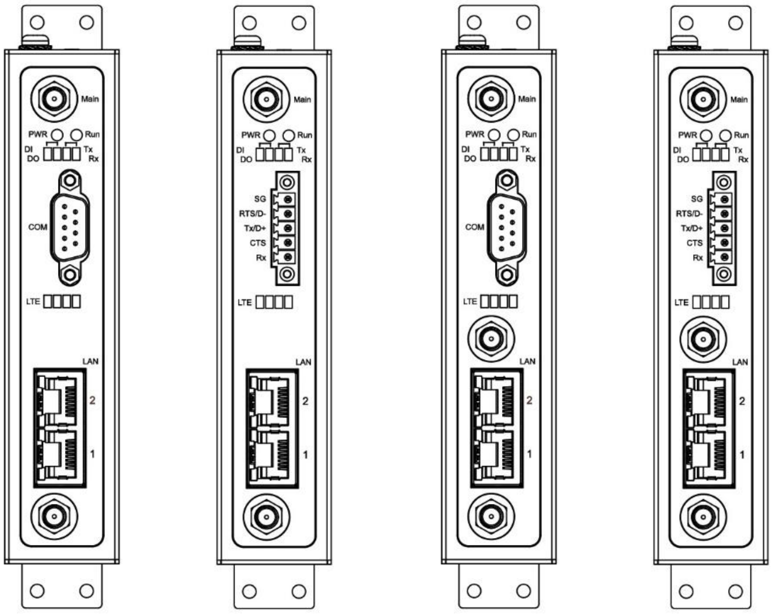
PG5201B All Series



Rear Top Buttom Left Side Right Side

Figure 3-1 PG5201B All Series Pannel except Front View

PG5201B All Series Front View



DB- TB DB-GPS TB-GPS

Figure 3-2 PG5201B All Series Front View

3.3 *First Time Installation*

Before installing the device, please follow strictly all safety procedures described in the hardware installation guide supplied inside the product. 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.

Note that some specific installation instructions are not provided here in this manual since they may differ considerably based on the purchased hardware.

3.4 *Factory Default Settings*

3.4.1 *Network Default Settings*

The PG5201B Low-Power Protocol Gateway is equipped with two LAN interfaces with one default IP address. Its default network parameters are listed in Table 3.3.

Table 3.3 Network Default Settings

Interface	Device IP	Subnet Mask	Gateway IP	DNS
LAN1	10.0.50.100	255.255.255.0	10.0.50.254	-

3.4.2 *Other Default Settings*

The PG5201B comes with the following default settings.

Table 3.4 Security, Serial, and SNMP Default Settings

Parameter	**Default Values**
Security	
User Name	admin
Password	default
Serial	
COM1	RS-232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control No Packet Delimiter timer
SNMP	
SysName of SNMP	System
SysLocation of SNMP	Location
SysContact of SNMP	Contact
SNMP	Disabled
Read Community	public
Write Community	private
SNMP Trap Server	0.0.0.0

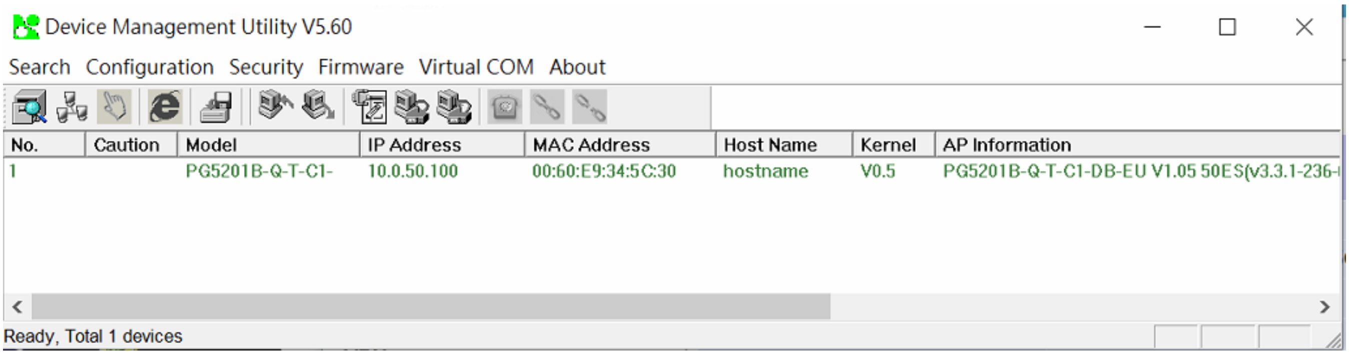
Note: Press the "**Reset**" button on the front panel for 5 seconds, to restore the PG5201B Series Low-Power Protocol Gateway to the factory default settings.

4 Configuration and Setup

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

4.1 *Configuration of Network Parameters through Device Management Utility*

Please install Atop's configuration utility program called **Device Management Utility®** that comes with the Product CD or can be downloaded from our websites (www.atop.com.tw or www.atoponline.com). For more information on how to install **Device Management Utility®**, please refer to the manual that comes in the Product CD. After you start **Device Management Utility®**, if the PG5201B Low-Power Protocol Gateway is already connected to the same subnet as your PC, the device can be accessed via broadcast packets. **Device Management Utility®** will automatically detect your PG5201B device and list it on **Device Management Utility®**'s window. Alternatively, if you did not see your PG5201B device on your network, press "**Rescan**" icon, a list of devices, including your PG5201B device currently connected to the network will be shown in the window of **Device Management Utility®** as shown in Figure 4-1.


Device Management Utility V5.60
Search Configuration Security Firmware Virtual COM About

No.	Caution	Model	IP Address	MAC Address	Host Name	Kernel	AP Information
1		PG5201B-Q-T-C1-	10.0.50.100	00:60:E9:34:5C:30	hostname	V0.5	PG5201B-Q-T-C1-DB-EU V1.05 50ES(v3.3.1-236-

Ready, Total 1 devices

Figure 4-1 List of Device in Device Management Utility

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

Sometime the PG5201B device might not be in the same subnet as your PC; therefore, you will have to use Atop's utility to locate it in your virtual environment. To configure each device, first click to select the desired PG5201B device (default IP: 10.0.50.100) in the list of **Device Management Utility©**, and then click "**Configuration → Network…**" (or Ctrl+N) menu on **Device Management Utility©** as shown in Figure 4-2 or click on the second icon called **Network** on the menu icon bar, and a pop-up window will appear as shown in Figure 4-3.

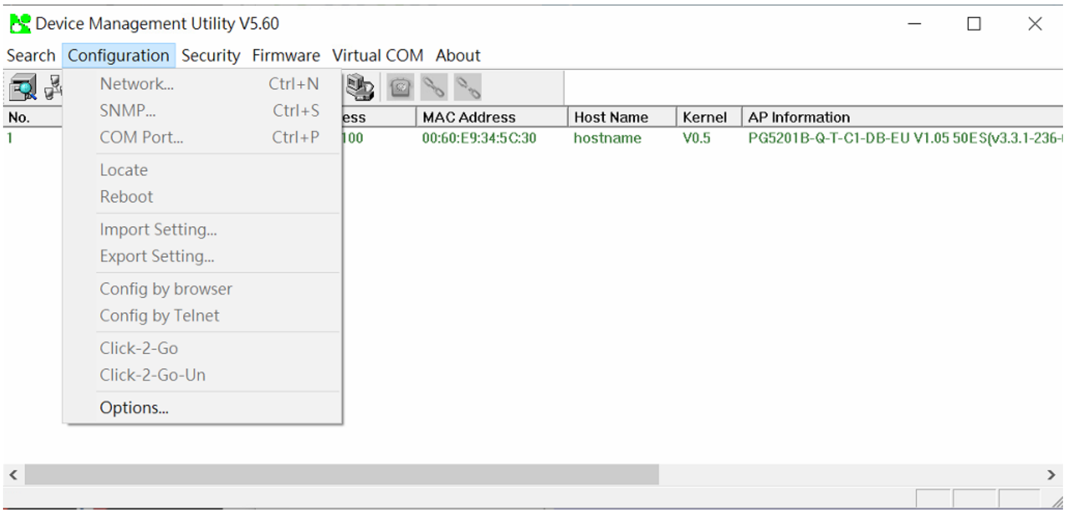
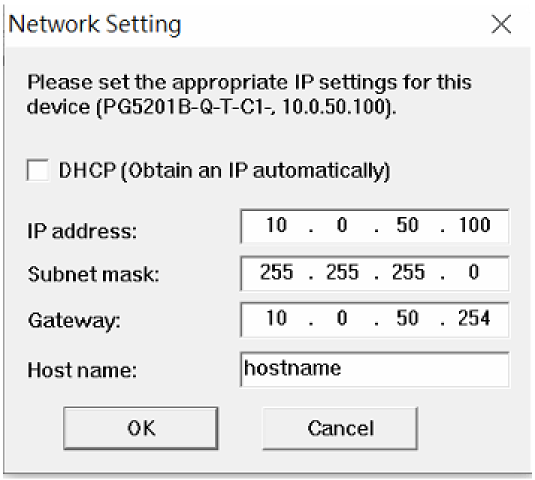


Figure 4-2 Pull-down Menu of Configuration and Network...



Network Setting

Please set the appropriate IP settings for this device (PG5201B-Q-T-C1-, 10.0.50.100).

□ DHCP (Obtain an IP automatically)

IP address: 10 . 0 . 50 . 100

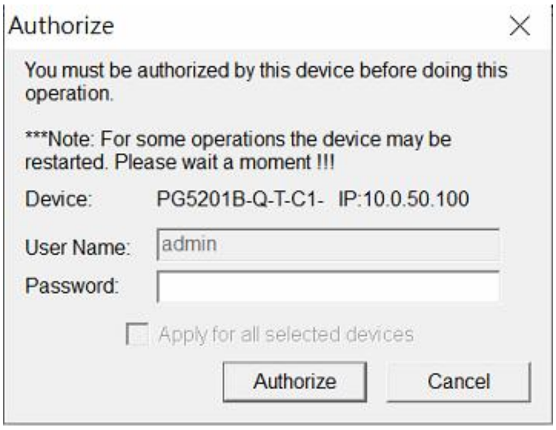
Subnet mask: 255 . 255 . 255 . 0

Gateway: 10 . 0 . 50 . 254

Host name: hostname

Figure 4-3 Pop-up Window of Network Setting

You may proceed then to change the IP address to avoid any IP address conflict with other hosts on your LAN or to connect the device to your existing LAN as shown in Figure 4-3. The system will prompt you for a credential to authorize the changes. It will ask you for the **Username** and the **Password** as shown in Figure 4-4. The default username is “**admin**”, while the default password is “**default**”. After clicking on the **Authorize** button, a notification window will pop-up as shown in Figure 4-5 and some device may be restarted. After the device is restarted (for some model), it will beep twice to indicate that the unit is running normally. Then, the PG5201B device can be found on a new IP address. It may be listed automatically by the **Device Management Utility©** or it can be found by clicking on the “**Rescan**” icon. Note that if you did not change the IP address but changed other parameter(s), you may encounter another notification window as shown in Figure 4-6.



Authorize

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

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

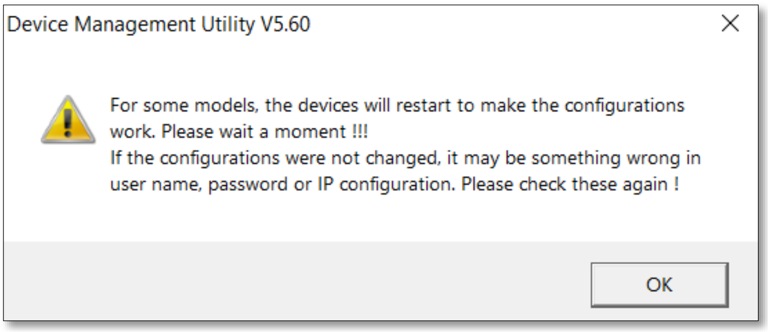
Device: PG5201B-Q-T-C1- IP:10.0.50.100

User Name: admin

Password:

□ Apply for all selected devices

Figure 4-4 Authorization for Change of Network Settings

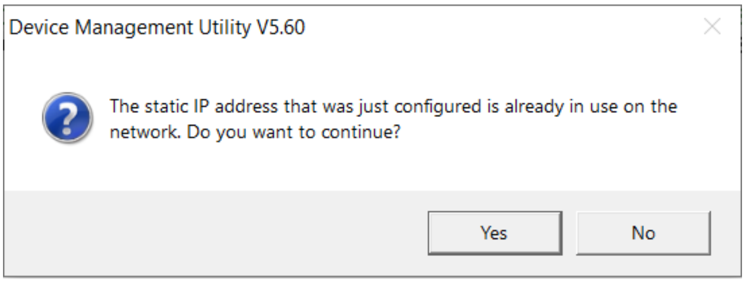


Device Management Utility V5.60

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

Figure 4-5 Pop-up Notification Window after Authorization

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



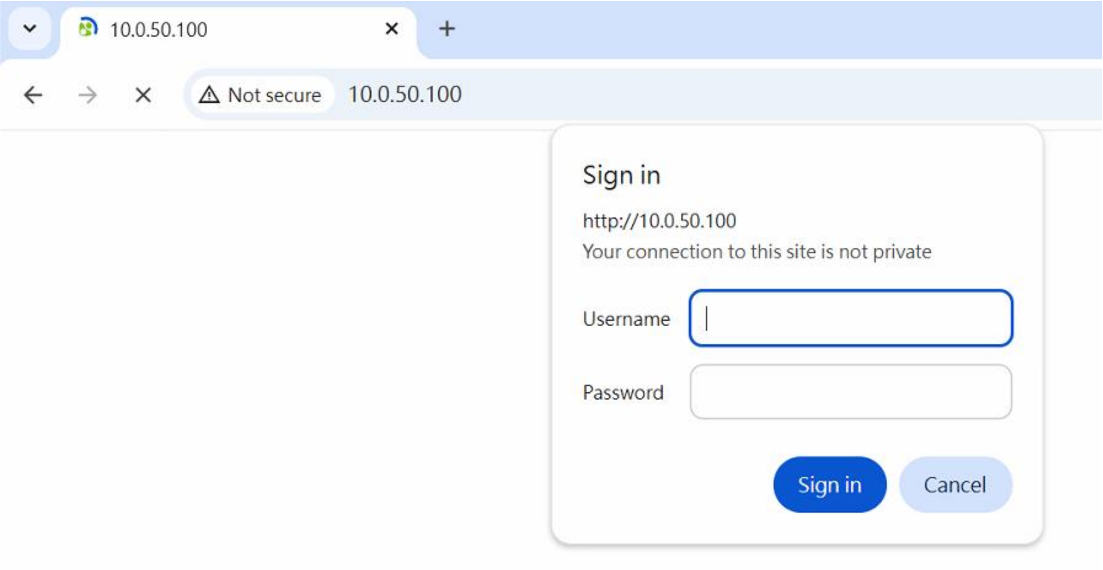
Device Management Utility V5.60

The static IP address that was just configured is already in use on the network. Do you want to continue?

Figure 4-6 Pop-up Notification Window when there is the same IP address in the network

4.2 *Configuring through Web*

Every PG5201B Low-Power Gateway is equipped with a built-in web server in the firmware. Therefore, the device can be accessed by using a web browser for configuring by entering the device's IP address (default value is 192.168.1.1) in the URL field of your web browser. As shown in Figure 4-7, an authentication will be required, and you will have to enter the username and password for accessing the web interface. The default value for username and password are "admin" and "default", respectively. The overview page of the web interface is illustrated as shown in Figure 4-8. Figure 4-9 lists all the menus and submenus for web configuration. Please see Section 3.4 for the default values.



Sign in

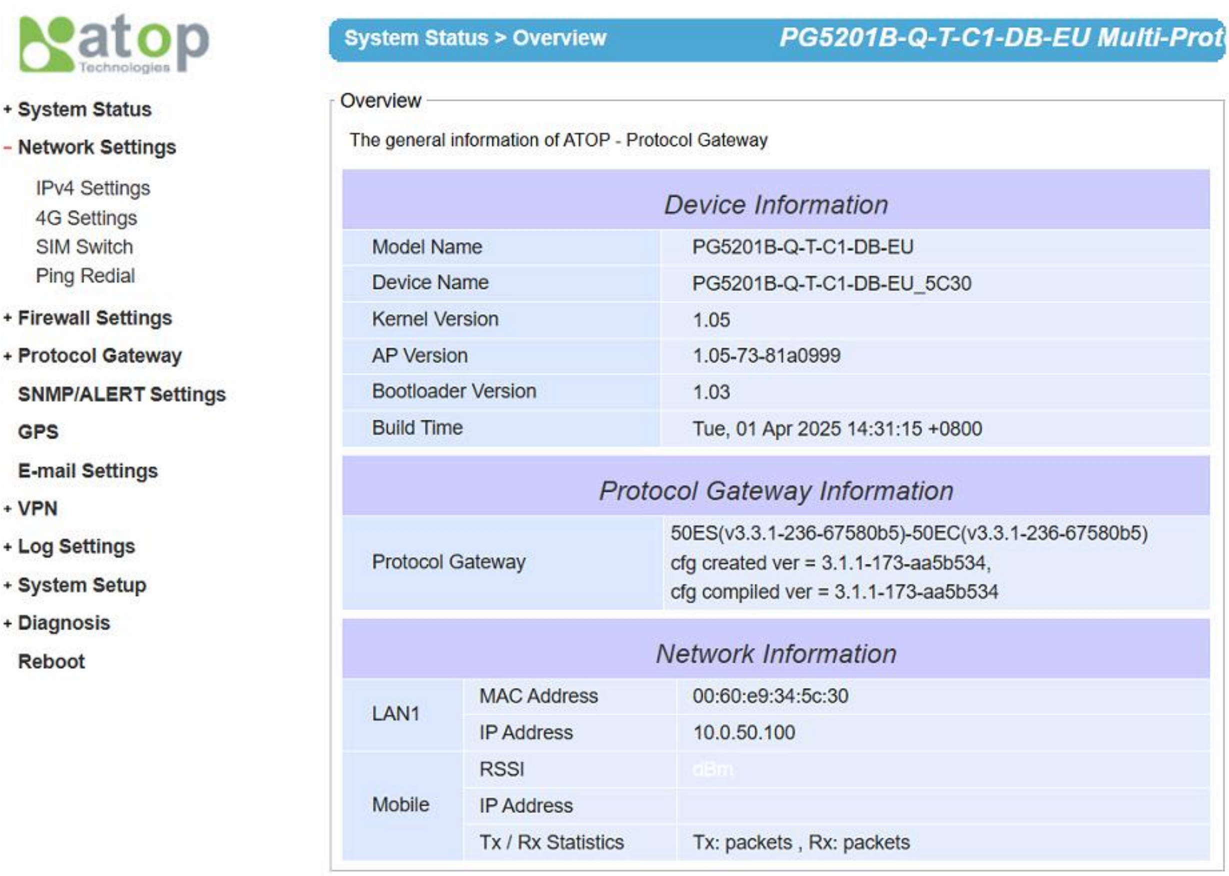
http://10.0.50.100

Your connection to this site is not private

Username

Password

Figure 4-7 Require Authentication for Accessing Web Interface



System Status > Overview PG5201B-Q-T-C1-DB-EU Multi-Prot

Overview

The general information of ATOP - Protocol Gateway

Device Information	
Model Name	PG5201B-Q-T-C1-DB-EU
Device Name	PG5201B-Q-T-C1-DB-EU_5C30
Kernel Version	1.05
AP Version	1.05-73-81a0999
Bootloader Version	1.03
Build Time	Tue, 01 Apr 2025 14:31:15 +0800

Protocol Gateway Information	
Protocol Gateway	50ES(v3.3.1-236-67580b5)-50EC(v3.3.1-236-67580b5) cfg created ver = 3.1.1-173-aa5b534, cfg compiled ver = 3.1.1-173-aa5b534

Network Information		
LAN1	MAC Address	00:60:e9:34:5c:30
	IP Address	10.0.50.100
Mobile	RSSI	dBm
	IP Address	
	Tx / Rx Statistics	Tx: packets , Rx: packets

Figure 4-8 Overview Webpage of PG5201B Low-Power Protocol Gateway

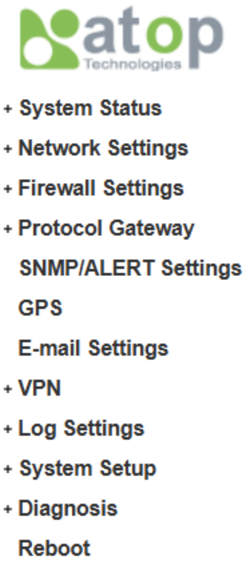
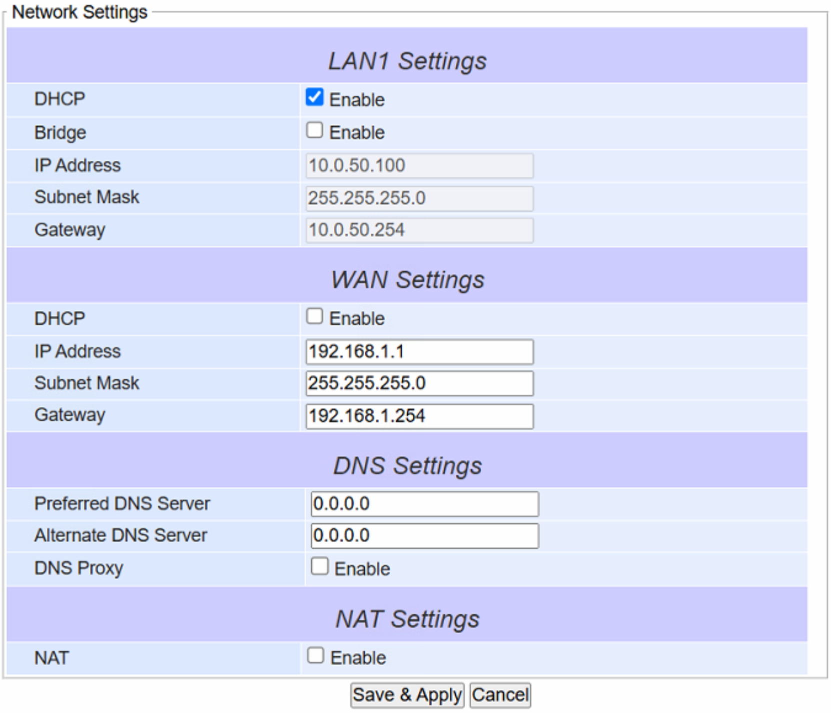


Figure 4-9 Memu of Configuring Web Page on PG5201B Low-Power Protocol Gateway

Typically, users are more familiar to use web interface for configuring the device. It is the most recommended and the most common method used for PG5201B Low-Power Gateway. Please go to its corresponding section for a detailed explanation.

4.3 *Configuring Automatic IP Assignment with DHCP*

A DHCP server can automatically assign IP addresses, Subnet Mask, and Network Gateway to LAN interface. You can simply check the **"DHCP (Obtain an IP Automatically)"** checkbox in the Network Setting dialog as shown in Figure 4-3 using Atop's **Device Management Utility©** and then restart the device. Once restarted, the IP address will be configured automatically.



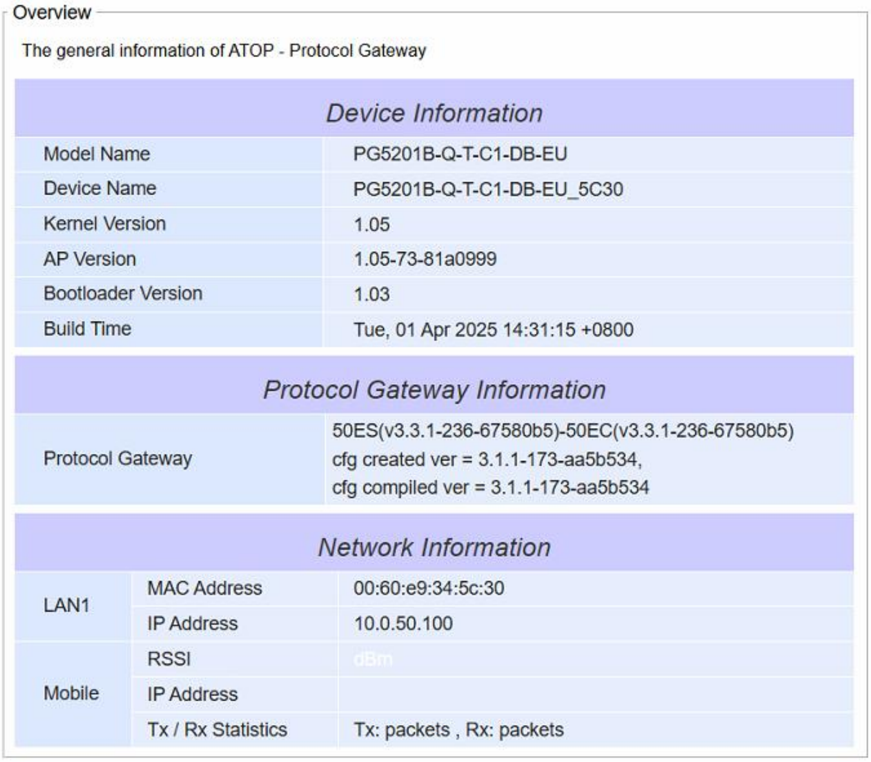
Network Settings

LAN1 Settings	
DHCP	☑ Enable
Bridge	□ Enable
IP Address	10.0.50.100
Subnet Mask	255.255.255.0
Gateway	10.0.50.254
WAN Settings	
DHCP	□ Enable
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS Settings	
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
DNS Proxy	□ Enable
NAT Settings	
NAT	□ Enable

Figure 4-10 Enable DHCP Option

4.4 *Web Overview*

In this section, current information on the device's status and settings will be displayed. An example of PG5201B's overview page is shown in Figure 4-11.



Overview

The general information of ATOP - Protocol Gateway

Device Information	
Model Name	PG5201B-Q-T-C1-DB-EU
Device Name	PG5201B-Q-T-C1-DB-EU_5C30
Kernel Version	1.05
AP Version	1.05-73-81a0999
Bootloader Version	1.03
Build Time	Tue, 01 Apr 2025 14:31:15 +0800

Protocol Gateway Information	
Protocol Gateway	50ES(v3.3.1-236-67580b5)-50EC(v3.3.1-236-67580b5) cfg created ver = 3.1.1-173-aa5b534, cfg compiled ver = 3.1.1-173-aa5b534

Network Information		
LAN1	MAC Address	00:60:e9:34:5c:30
	IP Address	10.0.50.100
Mobile	RSSI	dBm
	IP Address	
	Tx / Rx Statistics	Tx: packets , Rx: packets

Figure 4-11 Overview Web Page

In details, the following information is given and divided into 2 parts (Device Information and Network Information):

- Device Information
  - **Model Name**, as its name implies, shows the device's model.
  - **Device Name** shows a given name of the device in which the default value is the MAC address of the LAN interface.
  - **Kernel Version** is the value of the version of the kernel firmware of the device.
  - **AP Version** is the version of the application firmware of the device.
  - **Bootloader Version** is the version of the program that loads the operating system of the device.
  - **Build Time** is the time that the kernel based on its configuration is compiled.
- **Network Information** shows information about the wired and wireless network interfaces on the device.
  - **3G/4G:** The RSSI (Received Signal Strength Indicator) of the 3G/4G signal is shown, as well as its assigned IP address. The Tx/Rx statistics are also displayed here.
  - **LAN:** This will display the current **MAC Address**, and **IP Address** of the Ethernet interface.

4.5 *Network Settings*

In this section, both network interfaces and related network settings of the PG5201B device can be configured. The **Network Settings** menu has four submenus which are **IPv4 Settings**, **4G Settings**, and **SIM Switch**. Figure 4-12 shows the menu and its submenus.

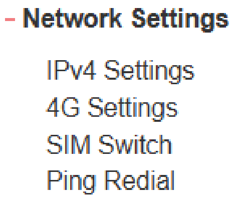
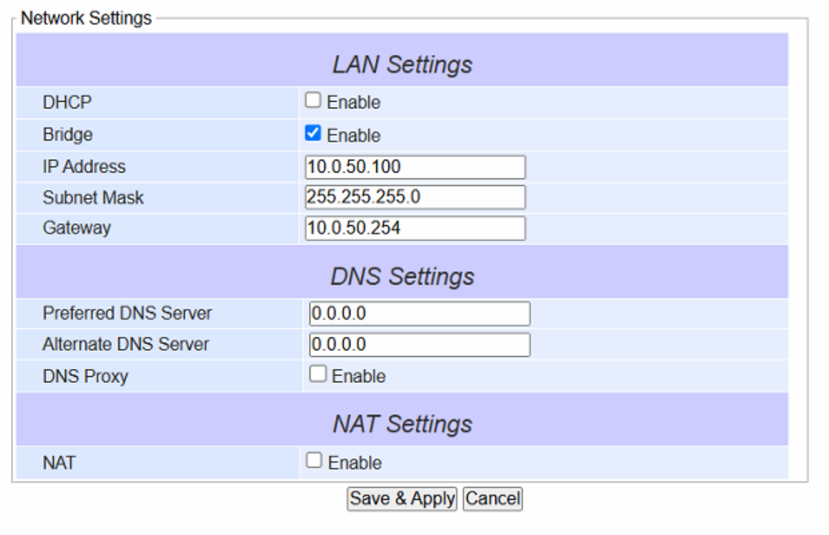


Figure 4-12 Three Submenus of the Network Settings Menu

4.5.1 *IPv4 Settings*

In the first submenu (**IPv4 Settings**), there are three sets of parameters which are **LAN Settings** and **DNS Settings** and **NAT settings** that the user can input information, as shown in Figure 4-14. More information on this parameter will be elaborated later. There are two Ethernet ports on PG5201B. Usually they are used for the LAN application. For the LAN application and the purpose of saving the cost of extra switch device, here the two Ethernet LAN ports are bridged by default. The user can un-bridge them by unchecking **Bridge** checkbox and get one Ethernet port for LAN application and the other Ethernet port for WAN application.

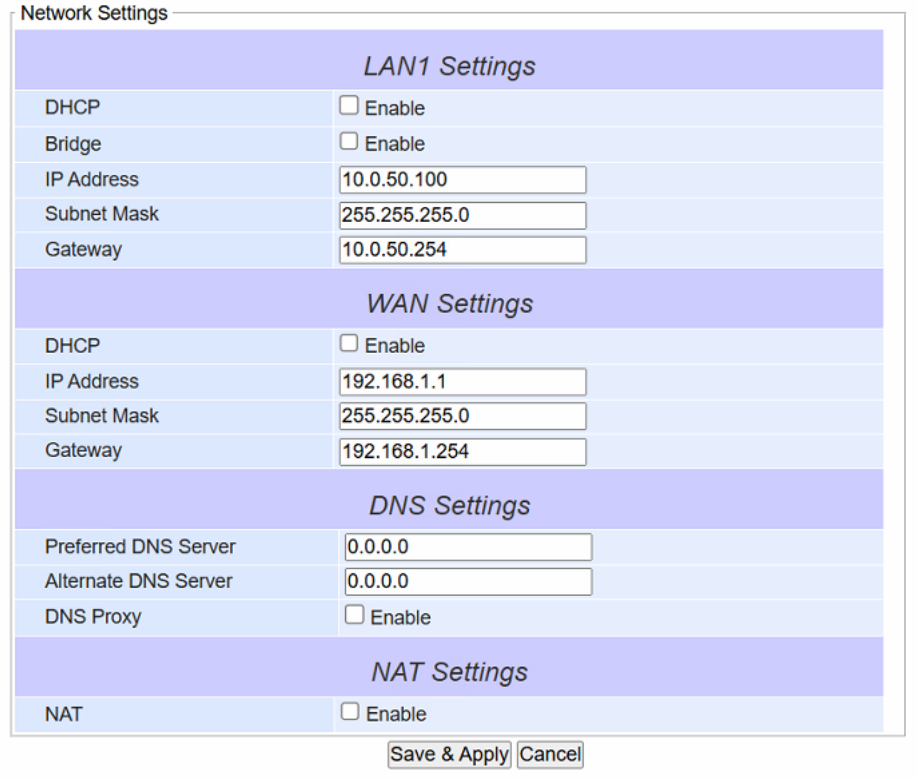
For the first set of parameters (**LAN Settings),** you can configure the **IP Address**, **Subnet Mask**, and **Default Gateway** for your wired LAN network. You can check the box behind **DHCP** option to obtain an IP address automatically. If you checked the box, the rest of the options for **LAN1 Settings** will be greyed out or disabled. For the Second parameter (**DNS Settings**), you can specify the IP Address of your **Preferred DNS Server** (Domain Name Server) and **Alternate DNS Server**. If the PG5201B device is connected to the Internet and should connect to other servers over the Internet to get some services such as Network Time Protocol (NTP) server, you will need to configure the DNS server to be able to resolve the host name of the NTP server. Please consult your network administrator or internet service provider (ISP) to obtain local DNS's IP addresses. PG5201B also provides **DNS Proxy** functionality that allows to improve the speed of DNS replies.



Network Settings

LAN Settings	
DHCP	□ Enable
Bridge	☑ Enable
IP Address	10.0.50.100
Subnet Mask	255.255.255.0
Gateway	10.0.50.254
DNS Settings	
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
DNS Proxy	□ Enable
NAT Settings	
NAT	□ Enable

Figure 4-13 Network Settings with Bridge enabled



Network Settings

LAN1 Settings	
DHCP	□ Enable
Bridge	□ Enable
IP Address	10.0.50.100
Subnet Mask	255.255.255.0
Gateway	10.0.50.254

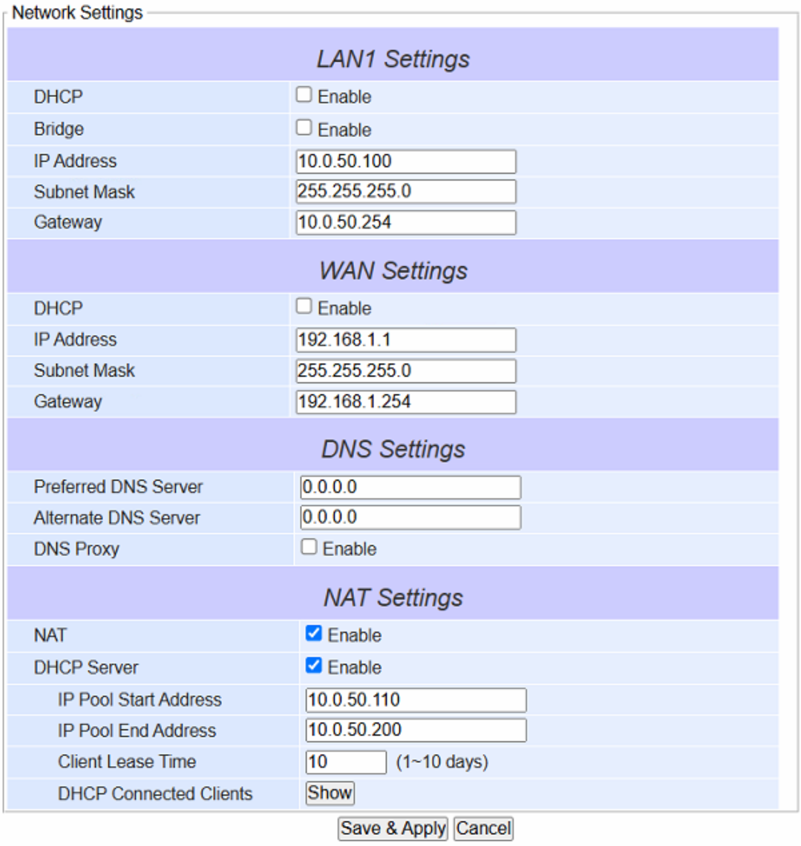
WAN Settings	
DHCP	□ Enable
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

DNS Settings	
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
DNS Proxy	□ Enable

NAT Settings	
NAT	□ Enable

Figure 4-14 Network Settings without Bridge enabled

As mentioned, there is **NAT Settings** for PG5201B only that can be configured at the end of the **IPv4 Settings** web page (under **Network Settings** menu) as shown in Figure 4-14 and Figure 4-15. NAT is referred to Network Address Translation which is a technique that allows PG5201B to create a local IP network or subnetwork with private IP addresses that can connect to the Internet through a public IP address via its Wide Area Network (WAN) port. The PG5201B will map the private IP address and port of a local device connected to its local interface to a public port on its public interface (WAN port). To enable **NAT** function on PG5201B, check on the **Enable** box behind **NAT** option under **NAT Settings** part as shown in Figure 4-15.

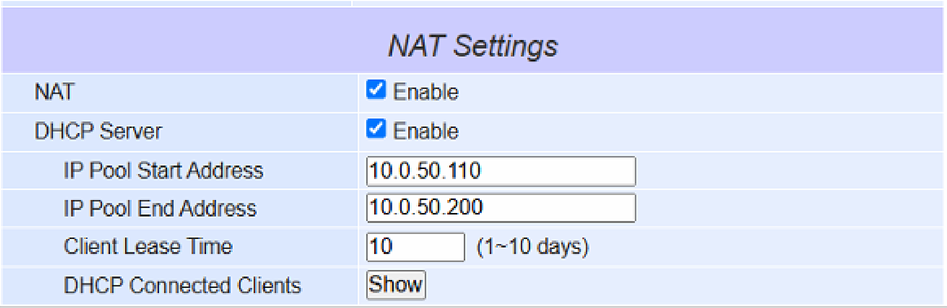


Network Settings

LAN1 Settings	
DHCP	☐ Enable
Bridge	☐ Enable
IP Address	10.0.50.100
Subnet Mask	255.255.255.0
Gateway	10.0.50.254
WAN Settings	
DHCP	☐ Enable
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS Settings	
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
DNS Proxy	☐ Enable
NAT Settings	
NAT	☑ Enable
DHCP Server	☑ Enable
IP Pool Start Address	10.0.50.110
IP Pool End Address	10.0.50.200
Client Lease Time	10 (1~10 days)
DHCP Connected Clients	Show

Figure 4-15 NAT Settings under IPv4 Settings Web Page for PG5201B

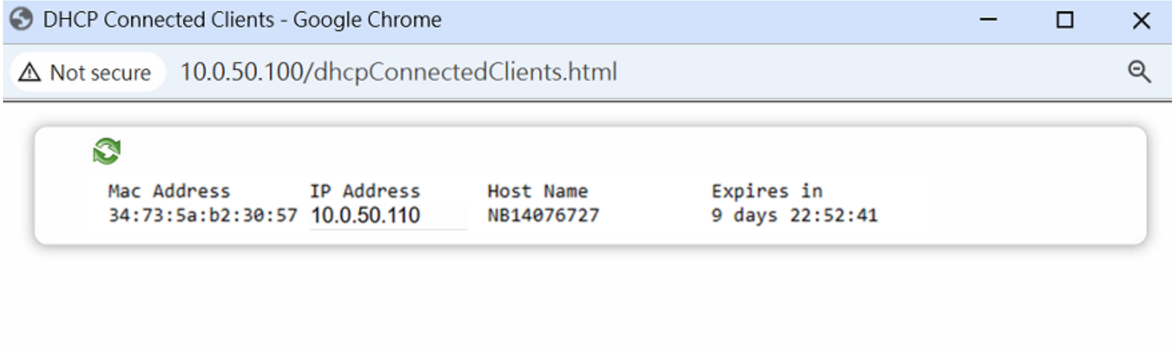
When **NAT** function is enabled on PG5201B, an additional set of parameters which is **DHCP Server** field will appear as shown in Figure 4-16. The **DHCP Server** or Dynamic Host Configuration Protocol Server is another function on PG5201B under the **NAT Settings**. This will allow PG5201B to automatically assign IP address for its local network. If the **DHCP Server** option is enabled (by checking the **Enable** box behind **DHCP Server** option), **IP Pool Start Address** and **IP Pool End Address** fields will appear under it. The IP Pool Addresses are the range of addresses that **DHCP Server** will be used to configure local IP addresses. The user can enter the starting and ending addresses inside these two fields**. The DHCP** Server function inside PG5201B can only support one LAN port and provide that port with IP address in the given range (from **IP Pool Start Address** to **IP Pool End Address**). Note that the range must be in NAT LAN port's network segment.



NAT Settings	
NAT	☑ Enable
DHCP Server	☑ Enable
IP Pool Start Address	10.0.50.110
IP Pool End Address	10.0.50.200
Client Lease Time	10 (1~10 days)
DHCP Connected Clients	Show

Figure 4-16 Enabling of NAT Settings with Additional Parameters for PG5201B

Finally, the last field is the **DHCP Connected Clients** which has a **Show** button that allows the user to see a list of currently connected DHCP Clients and their related IP addresses. When the **Show** button is clicked a pop-up window will show up with a table where each record contains Number, Client MAC Address, Client IP address, and Client name (if there is any). An example of one record is shown in Figure 4-17. Note that there is a green **Refresh** button that can be used to check the latest status of DHCP connected clients.



DHCP Connected Clients - Google Chrome

Not secure 10.0.50.100/dhcpConnectedClients.html

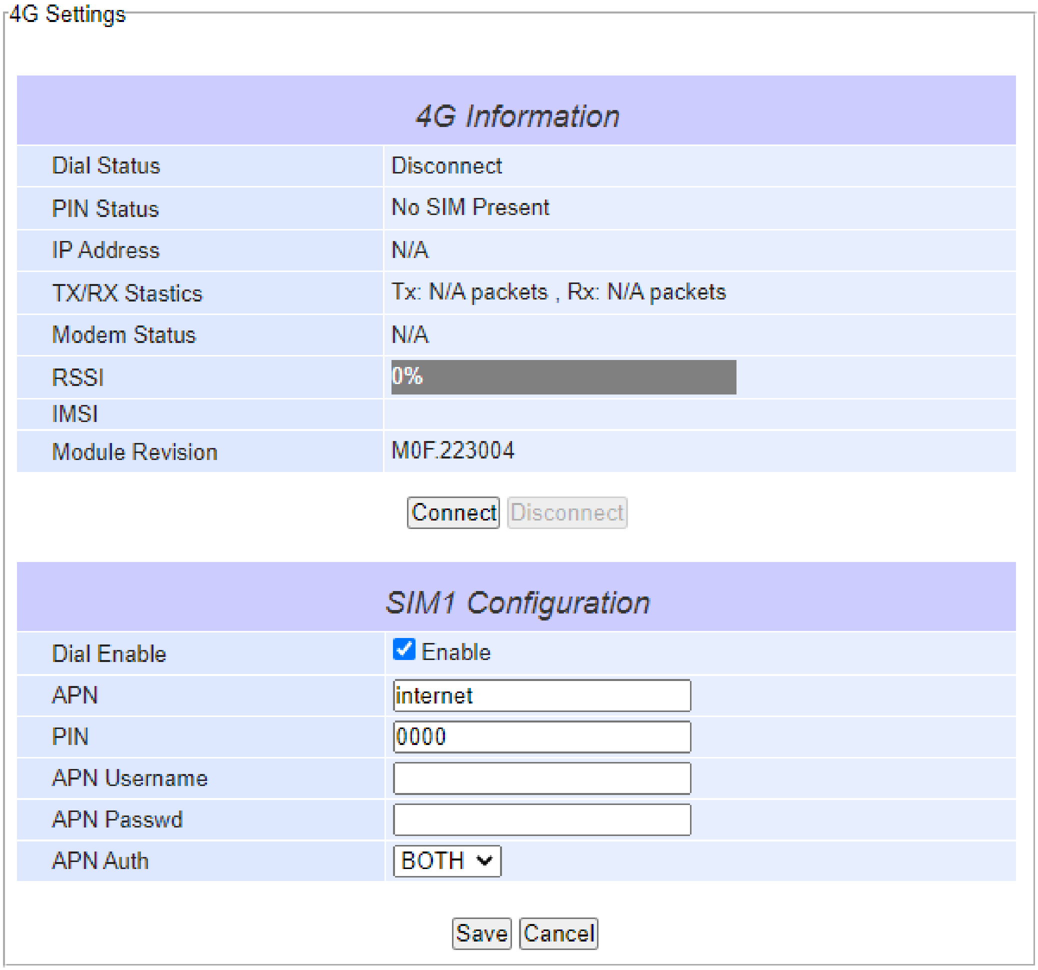
Mac Address	IP Address	Host Name	Expires in
34:73:5a:b2:30:57	10.0.50.110	NB14076727	9 days 22:52:41

Figure 4-17 A pop-up window shows an empty list of DHCP Connected Clients.

After finishing the network settings (or IPv4 settings) configuration, please click the **Save & Apply** button to save all changes that have been made. Finally, the web browser will be redirected to the **Overview** page as shown in Figure 4-11. If you would like to discard any setting, please click the **Cancel** button.

4.5.2 *4G Settings (Cellular Settings)*

Atop's PG5201B series provide the 4G settings page that allowed users to configure the cellular settings for AP (Access Point). Figure 4-18 illustrates the 4G Settings page. In the segment of 4G Information, users can manually connect/disconnect the 4G connection by clicking the **Connect/Disconnect** button.



4G Settings

4G Information	
Dial Status	Disconnect
PIN Status	No SIM Present
IP Address	N/A
TX/RX Stastics	Tx: N/A packets , Rx: N/A packets
Modem Status	N/A
RSSI	0%
IMSI	
Module Revision	M0F.223004

SIM1 Configuration	
Dial Enable	☑ Enable
APN	internet
PIN	0000
APN Username	
APN Passwd	
APN Auth	BOTH

Figure 4-18 4G Settings Web Page

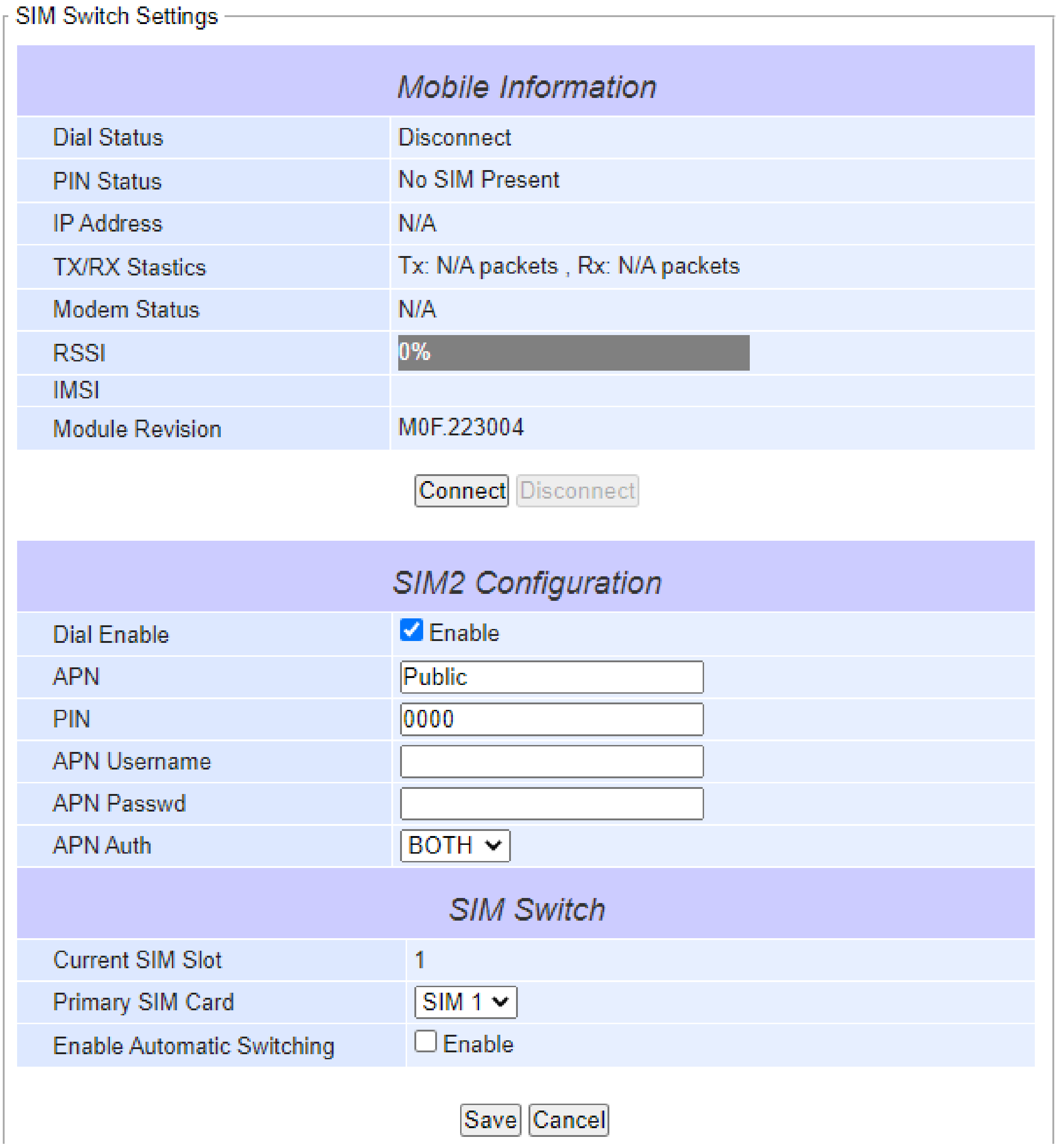
In the segment of SIM1 Configuration, users need to follow the requirements of cellular's AP (Access Point) to configure the settings. After finishing configurations, please click on the **Save** button to save all changes and enable your settings. Otherwise, click on the **Cancel** button to discard your settings. Table 4.1 summarizes the fields of 4G Settings web page.

Table 4.1 Descriptions of 4G Settings

Field Name	Description	Factory Default
Dial Enable	Check the **Enable** box to active the 4G dialing process when system start-up. Otherwise, the 4G connection will not be activated when system start-up.	Uncheck
APN	Access point name, this is determined by the carrier.	Public
PIN	PIN code used to unlock the SIM. This is required only when the SIM is locked.	0000
APN Username	The users name used to establish the connection during the dialing process. The requirement of this field is determined by the carrier.	NULL
APN Passwd	The password used to establish the connection during the dialing process. The requirement of this field is determined by the carrier.	NULL
APN Auth	Authentication method. The requirement of this field is determined by the carrier.	BOTH

4.5.3 *SIM Switch*

With a specific model, Atop's PG5201B might support two SIM card slots (SIM1 and SIM2) on the chassis of the device. Users can configure the parameters for SIM2 and enabling the switching of the SIMs on this SIM Switch web page. Figure 4-19 shows the **SIM Switch Settings** web page which consists of Mobile Information, SIM2 Configuration, and SIM switch sections. The first section called Mobile Information provides current information related to the device's mobile connectivity. The second section called SIM2 Configuration can be used to set the cellular's Access Point (AP) parameters for SIM card slot number 2. Note that the parameters are the same as described in Table 4.1. The third section called SIM Switch can be used to set which SIM card is the primary SIM card and enabling the automatically switching of primary SIM card.



SIM Switch Settings

Mobile Information

Dial Status	Disconnect
PIN Status	No SIM Present
IP Address	N/A
TX/RX Stastics	Tx: N/A packets , Rx: N/A packets
Modem Status	N/A
RSSI	0%
IMSI	
Module Revision	M0F.223004

SIM2 Configuration

Dial Enable	☑ Enable
APN	Public
PIN	0000
APN Username	
APN Passwd	
APN Auth	BOTH

SIM Switch

Current SIM Slot	1
Primary SIM Card	SIM 1
Enable Automatic Switching	□ Enable

Figure 4-19 SIM Switch Settings Web Page

Table 4.2 Description of SIM Switch's parameters

Field Name	Description	Factory Default
Current SIM Slot	Display the current SIM card slot that is the primary SIM	1
Primary SIM Card	Drop-down list of the available SIM slots: SIM1 and SIM2	SIM1
Enable Automatic Switching	This option allows the automatic switching of SIM card slot	Disable

The following procedures can be used to verify the cellular connection on the Atop's PG5201B.

1. Check the LED display.

- Check the LTE LEDs on the front panel.
- If the LTE LEDs are steady, it means that the PG5201B is connected to the 4G LTE network.
- If the LTE LEDs are off, it means that a SIM card is not installed or not detected, or the SIM card has not established a 4G data communication link.
- Check the LTE signal strength LEDs to see the current signal strength level. If the LTE signal strength LEDs are not on, this indicates that the PG5201B has not established a data service. Make sure that you enter the correct APN information in the web setting page described above.

2. Check the Overview page on the web.

- Log in to the web interface of PG5201B to display the Overview page. Check the Cellular RSSI, Cellular WAN IP address, and Cellular Mode fields to identify any connection problems.
- For Cellular RSSI (Received Signal Strength Indication), make sure that the value is above 60% to maintain a stable connection.
- If the Cellular WAN IP address is not available but the Cellular RSSI is more than 80%, make sure that the APN configuration is correct. The service provider might assign a private WAN IP address, which is not accessible externally.

3. Test the cellular network access on your computer.

Users with public SIM cards (instead of SIM cards with MDVPN service enabled) can test the connection to the Internet on your computer (assuming that your computer is connected to an Ethernet port on the PG5201B).

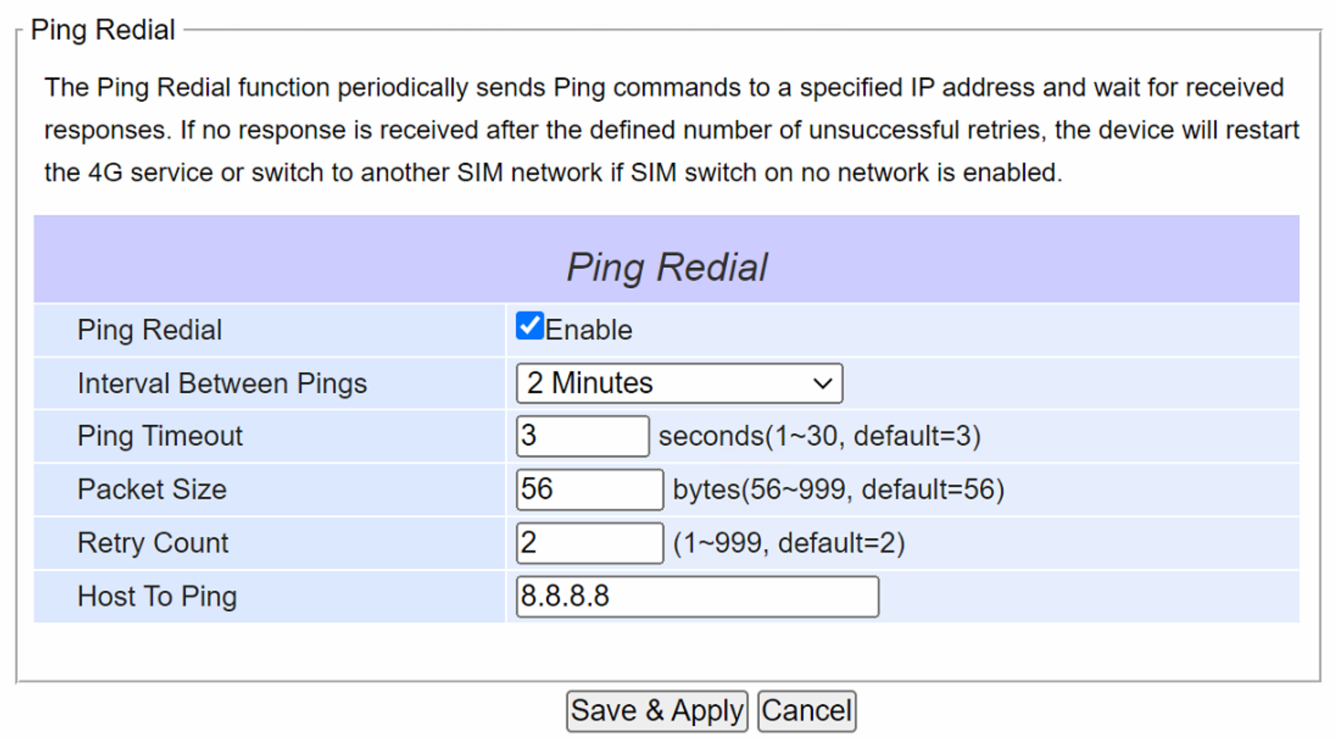
An example of the configuration settings on the computer is given below:

- Laptop IP Address: 192.168.1.4 (on the same subnet as the PG5201B Protocol Gateway)
- Laptop Subnet Mask: 255.255.255.0 (on the same subnet as the PG5201B Protocol Gateway)
- Laptop Default Gateway: 192.168.1.1 (the PG5201B gateway IP address)
- Laptop Primary DNS Server: 8.8.8.8 (test with Google's public DNS server)
- Laptop Primary DNS Server: 8.8.4.4 (test with Google's public DNS server)

After the configuration process is complete, your computer will be able to access the Internet.

4.5.4 *Ping Redial*

To guarantee the quality of LTE communication, the user could enable the **Ping Reboot** function under the **Network Settings** menu. The device will send packets periodically to specified destination (**Host To Ping**) via PING protocol. Once PG5901B detected that there was no response from the specified destination, it will initialize or reboot the 3G/4G module. Figure 4.5.4 shows the Ping Reboot web page and its parameters.



Ping Redial

The Ping Redial function periodically sends Ping commands to a specified IP address and wait for received responses. If no response is received after the defined number of unsuccessful retries, the device will restart the 4G service or switch to another SIM network if SIM switch on no network is enabled.

Ping Redial	
Ping Redial	☑Enable
Interval Between Pings	2 Minutes
Ping Timeout	3 seconds(1~30, default=3)
Packet Size	56 bytes(56~999, default=56)
Retry Count	2 (1~999, default=2)
Host To Ping	8.8.8.8

Figure 4-20 Ping Reboot Web Page under Network Settings

Table 4.3 Descriptions of Ping Reboot's Parameters

Field Name	Description	Factory Default
Ping Redial	Check the **Enable** box to active the **Ping Reboot** function. Input 0.0.0.0 or 127.0.0.1 in “Host to Ping” column can **disable** Ping Redial function too.	Enable
Interval Between Pings	The period that PG5201B will send out the Ping packet.	2 minutes
Ping Timeout	The timeout when there is no response from a destination host.	3 seconds
Packet size	The payload size of ICMP (Internet Control Message Protocol) used by Ping. You need to confirm that the destination host could accept the packet size that you defined.	56 Bytes
Retry Count	The number of retries if there is no response from a destination host.	2 times
Host to Ping	The specific IPv4 destination that PG5201B will send Ping packet to.	8.8.8.8

4.6 *Firewall Setting*

Atop’s PG5201B provides firewall features to improve security for your network. You can configure the firewall mechanisms under the Firewall Setting menu. Figure 4-21 shows the submenus of PG5201B under the Firewall Setting.

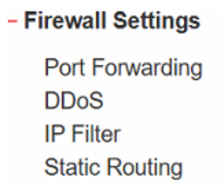


Figure 4-21 Firewall Setting Menu on PG5201B

4.6.1 *Port Forwarding*

Port forwarding is an application of Network Address Translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway. Figure 4-22 depicts an example of port forwarding through a PG5201B device (green pattern). In this example, a host or device behind the PG5201B (on the left of the figure) has a private IP address of 10.0.50.101 with port number 80. This is a http service that can be accessed through a public IP (on the PG5201B device) with IP address with port number 8080. This public IP address can be reached by a SCADA control center over the Internet. In other words, the SCADA system could access the IP address of PG5201B with specified port and the PG5201B will forward the packet from the SCADA system to the host on the LAN port of PG5201B with specified port.

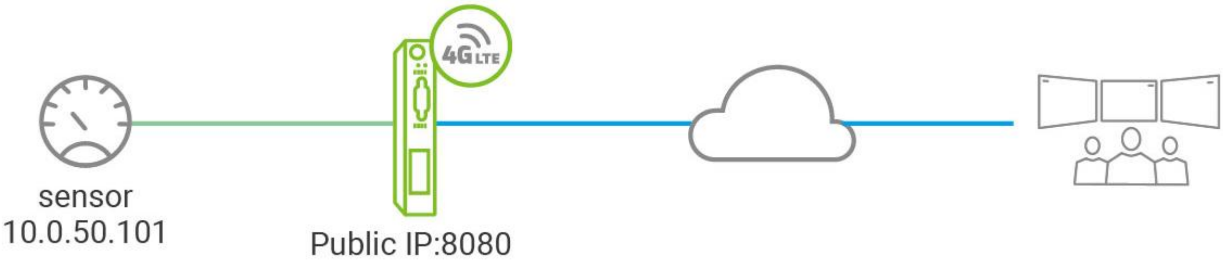
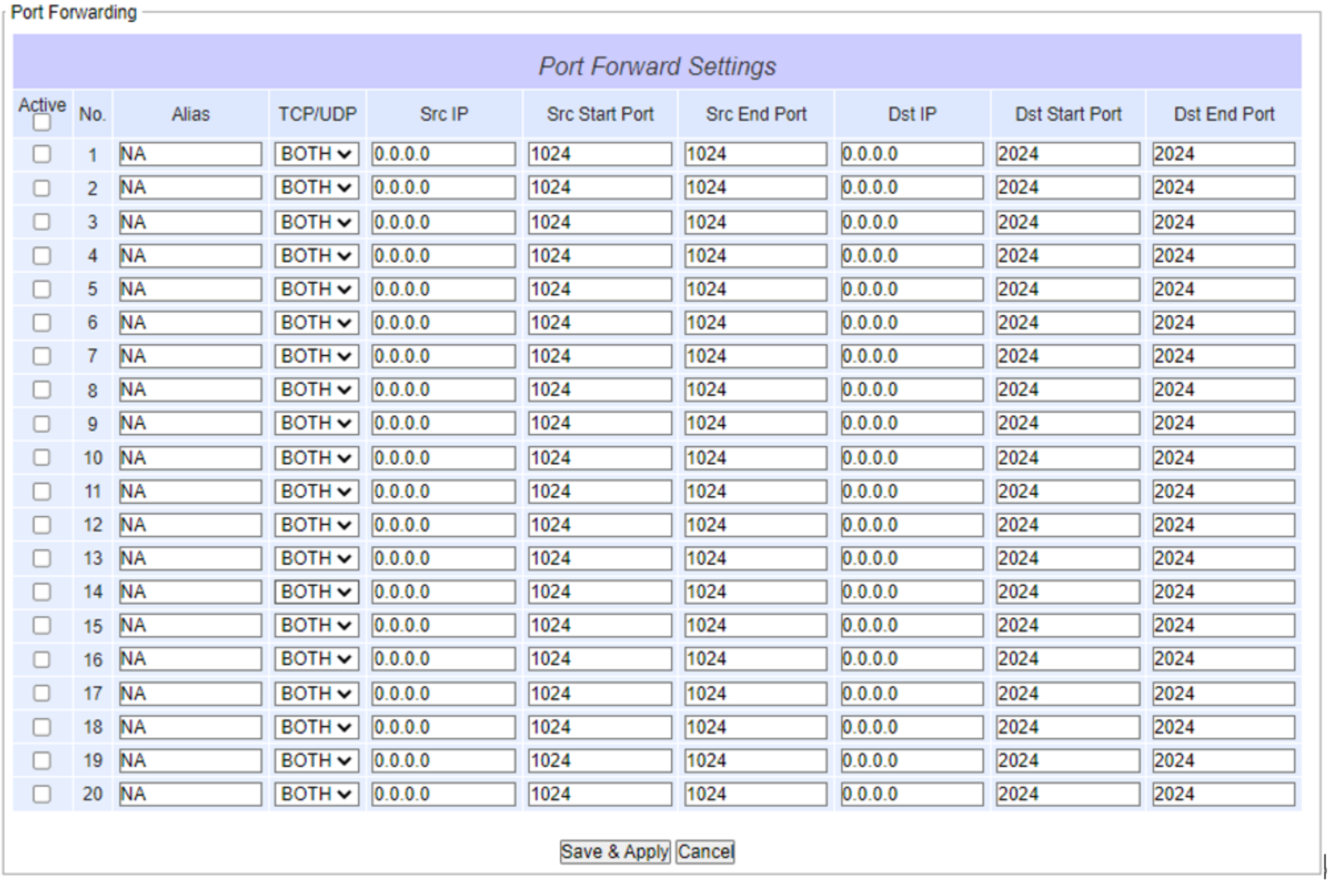


Figure 4-22 Example of Port Forwarding through PG5201B Low-Power Protocol Gateway

For PG5201B, when the user clicked on the **Port Forwarding** menu, the **Port Forwarding** web page will be displayed as shown in Figure 4-23. This port forwarding feature allows the user to configure port forwarding from WAN to LAN. This feature can redirect specific packets from a remote host on the WAN to a server on the LAN. It hides the IP address of a local server and prevents remote hosts from accessing the local server directly. This feature can also filter out unrecognized packets to protect your LAN network when computers connected to PG5201B are not visible to the WAN. Note that this feature is the result of **NAT Settings** described above. The user can configure port forwarding up to 20 entries. For each entry, the user can set an **Alias** (short name), allowable transport protocol(s) (**TCP/UDP**), source IP address (**Src IP**), source start port (**Src Start Port**), source end port (**Src End Port**), destination IP address (**Dst IP**), destination start port (**Dst Start Port**), and destination end port (**Dst End Port**). Table 4.4 describes each field (or column) in the Port Forwarding table.

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



Port Forwarding

Port Forward Settings

Active □	No.	Alias	TCP/UDP	Src IP	Src Start Port	Src End Port	Dst IP	Dst Start Port	Dst End Port
□	1	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	2	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	3	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	4	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	5	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	6	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	7	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	8	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	9	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	10	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	11	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	12	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	13	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	14	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	15	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	16	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	17	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	18	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	19	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024
□	20	NA	BOTH ▾	0.0.0.0	1024	1024	0.0.0.0	2024	2024

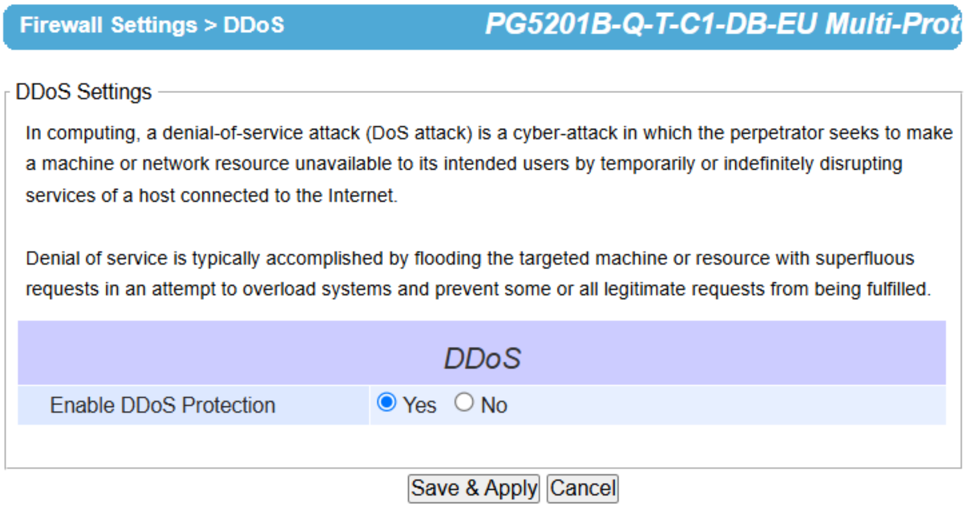
Figure 4-23 Port Forwarding Web Page of PG5201B series

Table 4.4 Description of Fields in Port Forwarding Table

Field Name	Description	Factory Default
Active	This radio button allows individually enabling or disabling each entry of the port forwarding configuration.	Disable
No.	This is the number of the row on the table which are from 1 up to 20.	-
Alias	This is a fillable textbox that allows to configure a short and easy-to-remember name for each port forwarding entry.	NA (Null)
TCP/UDP	This is the transport protocol that can be allowed on this port forwarding entry. The available options are TCP, UDP, or BOTH.	BOTH
Src IP	IPv4 address of the source (on WAN) which will be redirected through PG5201B.	0.0.0.0
Src Start Port	The starting port number of the source which can be between 0 to 65535.	1024
Src End Port	The ending port number of the source which can be between 0 to 65535.	1024
Dst IP	IPv4 address of the destination (on LAN) which is the translated destination IP address	0.0.0.0
Dst Start Port	The starting port number of the destination which can be between 0 to 65535.	2024
Dst End Port	The ending port number of the destination which can be between 0 to 65535.	2024

4.6.2 *DoS*

Atop’s PG5201B also has built-in distributed denial-of-service (DoS) protection mechanism. In network computing, a denial-of-service (DoS) attack is a cyber-attack that is accomplished by flooding the targeted machine such as PG5201B device with superfluous or fake requests in attempt to overload system and preventing some or all legitimate requests from being fulfilled. To enable this mechanism, users can choose the **DoS Setting** web page from the **DoS** submenu under the **Firewall Settings** menu. Figure 4-24 shows the option under the **DoS Settings** that can enable the DDoS Protection mechanism by selecting the **Yes** radio button.



DDoS Settings

In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

DDoS	
Enable DDoS Protection	● Yes ○ No

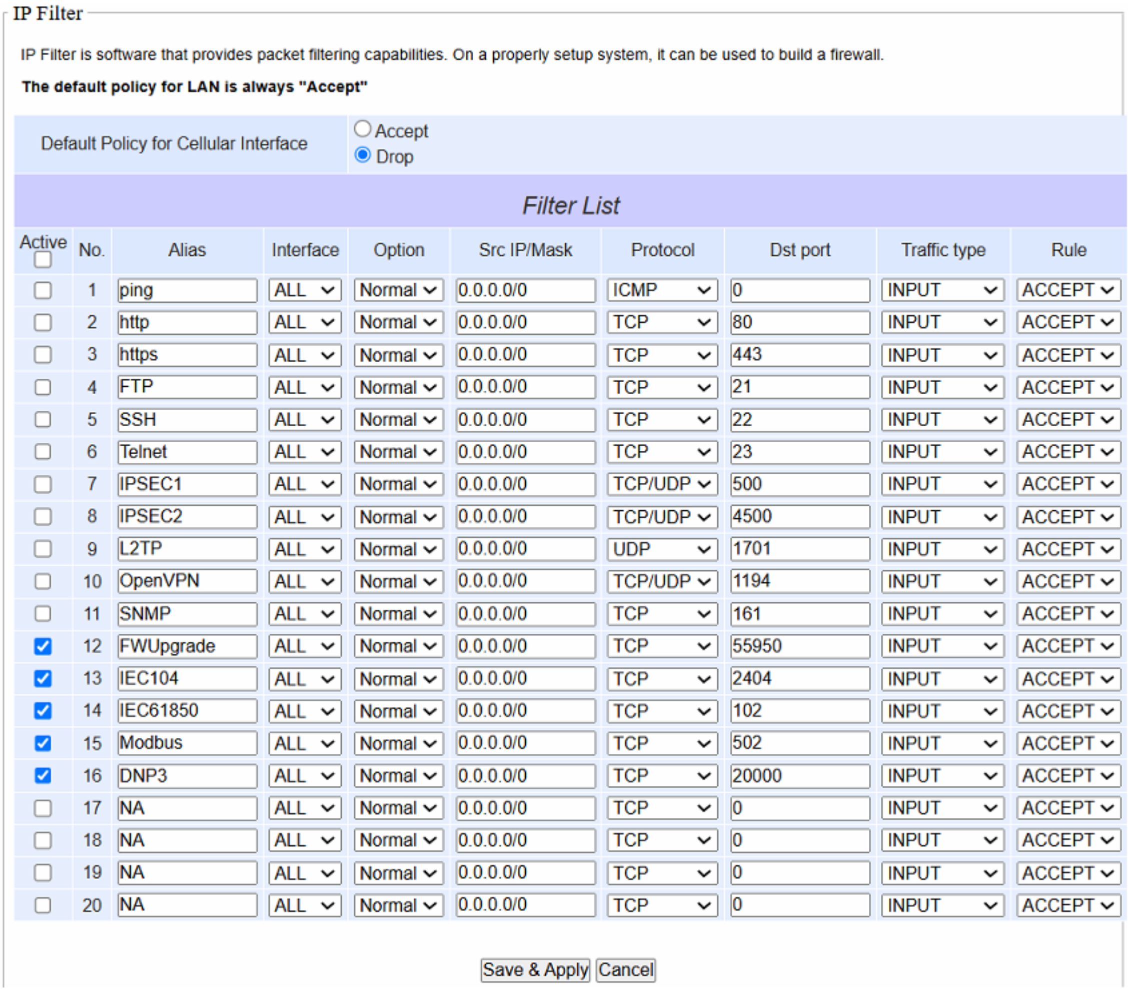
Figure 4-24 DoS Settings Web Page

4.6.3 *IP Filter*

One of the firewall features is to filter network traffic based on protocols, source addresses, and port numbers. Under the **IP Filter** web page shown in below Figure, you can configure the filtering for different network services. The first part of the **IP Filter** page is the **Default Policy** and the second part is the **Filter List**. By default, the policy is set in **Accept** mode in which all services on the device are accepted by the firewall. To deny a number of service types through the firewall, you can enable the filtering by selecting the **Drop** policy. Next, you can configure each denied service in the Filter List. Note that up to 30 entries can be set in the Filter List.

Under the **Filter List**, there are seven columns which are **Alias, Interface, Option, IP Addr/mask, Protocol**, **Port**, and **Rule**. The first three entries on the list are provided as examples for Ping, http, and https services. To enable each entry, you can check the box in front of that entry. Then, you can enter the short name or **Alias** for each entry to provide hint on the service that you allow. This name usually is the protocol service at the application layer. Next, you can select the transport protocol from the drop-down list under the **Interface** column. The choices for the interface are All, LAN1, and LAN2. The selection items depend on supported LAN interfaces on your device. The **Option** drop-down field allowed you to select the filtering rule is a normal or invert rule of **IP Addr/mask**. Next, you can enter the **IP Addr/mask, Protocol** and the **Port** number that will fit in the filtering rule. Then, you can determine the configured rule is Accept or Drop by the device from Rule drop-down list. Table below summarizes the description of each filed on the IP Filter web page.

After finishing configuring the **IP Filter**, please click on the **Save & Apply** button to save all changes and enable your setting. Otherwise, click on the **Cancel** button to discard your settings.



IP Filter

IP Filter is software that provides packet filtering capabilities. On a properly setup system, it can be used to build a firewall.

The default policy for LAN is always "Accept"

Default Policy for Cellular Interface ○ Accept ● Drop

Filter List

Active □	No.	Alias	Interface	Option	Src IP/Mask	Protocol	Dst port	Traffic type	Rule
□	1	ping	ALL	Normal	0.0.0.0/0	ICMP	0	INPUT	ACCEPT
□	2	http	ALL	Normal	0.0.0.0/0	TCP	80	INPUT	ACCEPT
□	3	https	ALL	Normal	0.0.0.0/0	TCP	443	INPUT	ACCEPT
□	4	FTP	ALL	Normal	0.0.0.0/0	TCP	21	INPUT	ACCEPT
□	5	SSH	ALL	Normal	0.0.0.0/0	TCP	22	INPUT	ACCEPT
□	6	Telnet	ALL	Normal	0.0.0.0/0	TCP	23	INPUT	ACCEPT
□	7	IPSEC1	ALL	Normal	0.0.0.0/0	TCP/UDP	500	INPUT	ACCEPT
□	8	IPSEC2	ALL	Normal	0.0.0.0/0	TCP/UDP	4500	INPUT	ACCEPT
□	9	L2TP	ALL	Normal	0.0.0.0/0	UDP	1701	INPUT	ACCEPT
□	10	OpenVPN	ALL	Normal	0.0.0.0/0	TCP/UDP	1194	INPUT	ACCEPT
□	11	SNMP	ALL	Normal	0.0.0.0/0	TCP	161	INPUT	ACCEPT
☑	12	FWUpgrade	ALL	Normal	0.0.0.0/0	TCP	55950	INPUT	ACCEPT
☑	13	IEC104	ALL	Normal	0.0.0.0/0	TCP	2404	INPUT	ACCEPT
☑	14	IEC61850	ALL	Normal	0.0.0.0/0	TCP	102	INPUT	ACCEPT
☑	15	Modbus	ALL	Normal	0.0.0.0/0	TCP	502	INPUT	ACCEPT
☑	16	DNP3	ALL	Normal	0.0.0.0/0	TCP	20000	INPUT	ACCEPT
□	17	NA	ALL	Normal	0.0.0.0/0	TCP	0	INPUT	ACCEPT
□	18	NA	ALL	Normal	0.0.0.0/0	TCP	0	INPUT	ACCEPT
□	19	NA	ALL	Normal	0.0.0.0/0	TCP	0	INPUT	ACCEPT
□	20	NA	ALL	Normal	0.0.0.0/0	TCP	0	INPUT	ACCEPT

Figure 4-25 IP Filter Settings Web page

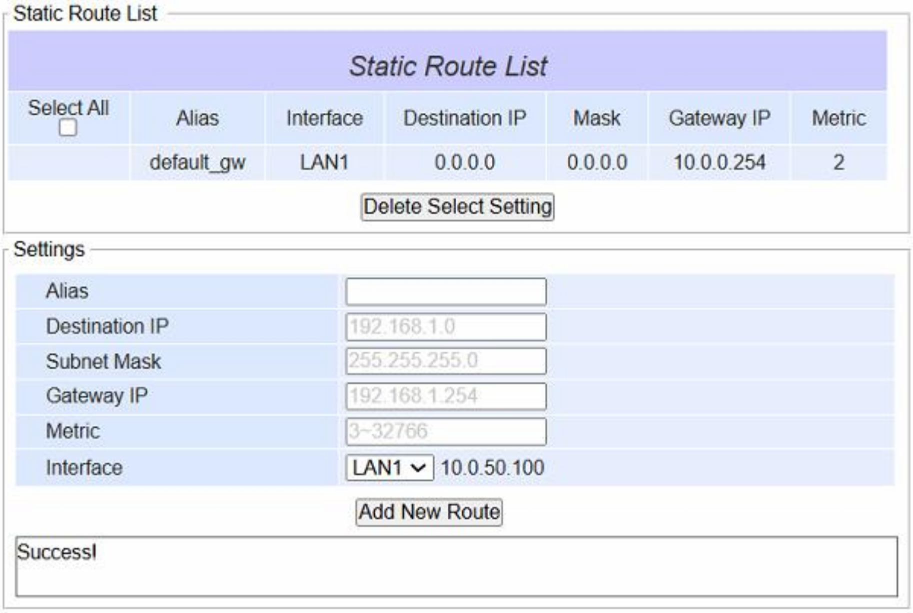
Table 4.5 Descriptions of Parameters for Services under IP Filter Setting

Field Name	Description	Factory Default
Default Policy	**Accept** all services or **Deny** specified services for the PG5201B.	Accept
Alias	Check the box in front of the entry and enter the alias name for the filtering rule.	Null
Interface	Select the interface that the filtering rule will activate on it. The interface depends on available network ports on your device.	All
Option	Select the option to determine this is a **Normal** or **Invert** rule of following settings.	Normal
IP Addr/mask	Enter the IP address that will be accepted or denied by the SE59XX service. Noted that you can enter one the followings: 1) IP address: only this unique IP address will match in the filtering rule. 2) IP with subnet mask: IP addresses within this subnet mask will match in the filtering rule.	0.0.0.0/0
Protocol	Select the protocol used by the service from the list: TCP, UDP, TCP/UDP, or ICMP	-
Port	Port number of TCP/UDP protocol	-

Rule	Select the rule to **Accept** or **Drop** to determine the filtering rule will be accepted or denied by the device.	Accept

4.6.4 *Static Routing*

PG5201B provides Static Routing functionality to allow network traffic to a specific destination network to be forwarded through a designated gateway. Users might use it for security or performance issues. It might also be helpful to route the network traffic to a network with only one path in and out, override a default route rule.



Static Route List

Static Route List

Select All ☐	Alias	Interface	Destination IP	Mask	Gateway IP	Metric
	default_gw	LAN1	0.0.0.0	0.0.0.0	10.0.0.254	2

Delete Select Setting

Settings

Alias	
Destination IP	192.168.1.0
Subnet Mask	255.255.255.0
Gateway IP	192.168.1.254
Metric	3~32766
Interface	LAN1 ⌄ 10.0.50.100

Add New Route

Success!

Figure 4-26 Static Route Settings Web page

Table 4.6 Descriptions of Parameters for Services under Static Routing

Field Name	Description	Factory Default
Alias	Alias name for the route rule.	Null
Destination IP	Target network or host IP address	Null
Subnet Mask	Netmask for the destination.	Null
Gateway IP	Next hop IP address.	Null
Metric	cost or priority of a route	Null
Interface	Interface used	LAN1

4.7 *Protocol Gateway*

Atop's PG5201B provides Protocol Gateway features that allow users to translate some multiple industrial protocols including Modbus, DNP3, I EC 61850, IEC 60870-5-101/3/4 to each others. Please find the detailed protocol user manuals on Atop official web site. Figure 4-21 shows the submenus of PG5201B under the Protocol Gateway.

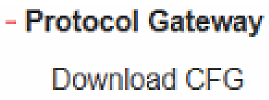
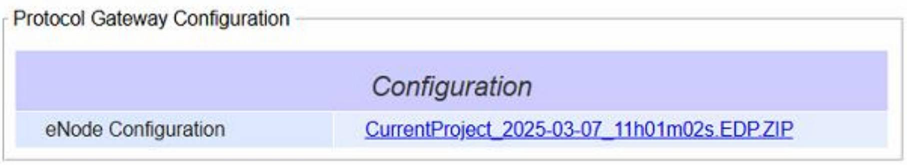


Figure 4-27 Protocol Gateway Menu on PG5201B

4.7.1 *Download CFG*

PG5201B Protocol Gateway configuration is configured by eNode Designer which is a Windows based utility and can be downloaded from Atop official web site. The users can download eNode Designer and its user manual from Atop official website web site.

After the users finish the protocol configuration and upload it to PG5201B by eNode Designer, the users can find and download the configuration from PG5901B by the Download CFG web page as the following for the review propose.



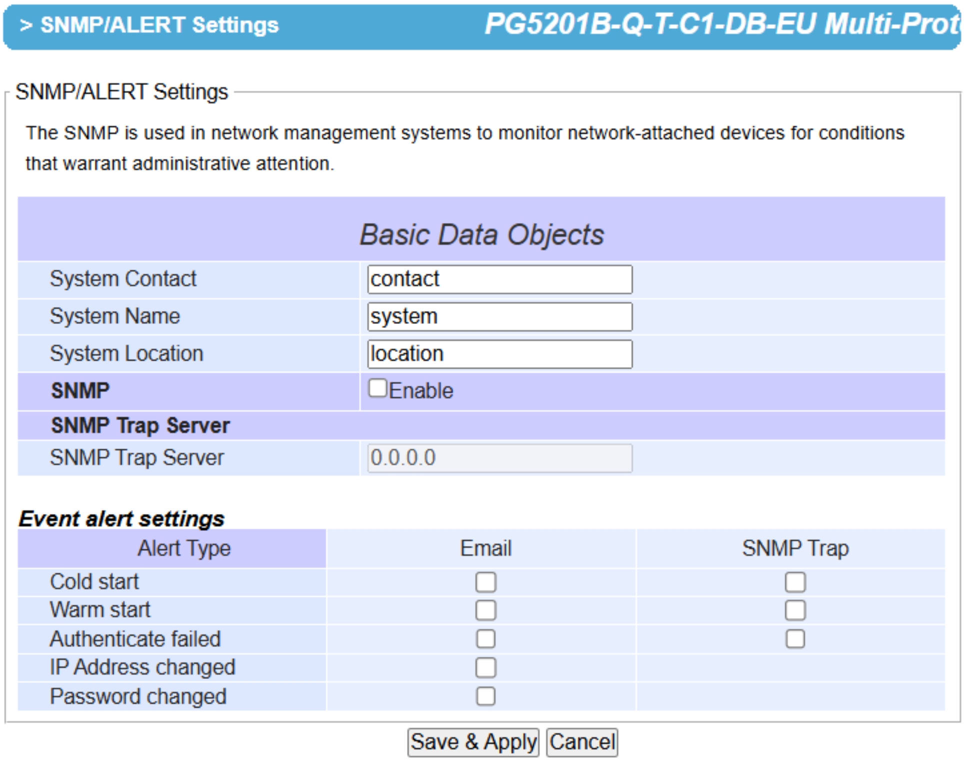
Protocol Gateway Configuration

Configuration	
eNode Configuration	CurrentProject_2025-03-07_11h01m02s.EDP.ZIP

Figure 4-28 Protocol Gateway Configuration

4.8 *SNMP/ALERT Settings*

The Simple Network Management Protocol (SNMP) is used by network management software to monitor devices in a network, to retrieve network status information of the devices, and to configure network parameters of the devices. The **SNMP/ALERT Settings** page showed in Figure 4-29 allows user to configure PG5201B device so that it can be viewed by third-party SNMP software, and allows PG5201B to send alert events to administrator and SNMP trap server.



> SNMP/ALERT Settings PG5201B-Q-T-C1-DB-EU Multi-Prot

SNMP/ALERT Settings

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

Basic Data Objects	
System Contact	contact
System Name	system
System Location	location
SNMP	□Enable
SNMP Trap Server	
SNMP Trap Server	0.0.0.0

Event alert settings

Alert Type	Email	SNMP Trap
Cold start	□	□
Warm start	□	□
Authenticate failed	□	□
IP Address changed	□	
Password changed	□	

Figure 4-29 SNMP/Alert Settings Web Page

PG5201B provides three basic SNMP fields under the **Basic Data Objects** part which are: "**System Contact**" usually used to specify the device's contact information in case of emergency (default value is "contact"), "**System Name**" usually used to identify this device (default value is "System"), and "**System Location**" usually used to specify the device location (default value is "location").

To make the device's information available for public viewing/editing, you can enable the **SNMP** function by checking the **Enable** box and fill in the two passphrases (or SNMP Community Strings) below it. Note that when the SNMP is unchecked, three setting option lines will not show up as depicted in Figure 4-29. By filling in the passphrase for the "**Read Community**", PG5201B device allows other network management software to read its information. By filling in the passphrase for the "**Write Community**", PG5201B device allows other network management software to read/modify its information. The default PG5201B's SNMP Community Strings (or passphrases) for **Read Community** and **Write Community** as shown in Figure 4-29 are "public" and "private", respectively.

Additionally, you can setup a **SNMP Trap Server** in the network to receive and collect all alert messages from PG5201B. To configure PG5201B to dispatch alert messages originated from any unexpected incidents, you can fill in the IP Address of the **SNMP Trap Server** in the field shown in Figure 4-29. Note that any changes in these settings will take effect after the PG5201B device is restarted.

Under the **SNMP Trap Server** part, there is a list of **Alert Type** under **Event alert settings** box in Figure 4-29. There can be up to two possible actions for each alert event: **Email** and **SNMP Trap**. You can enable the associated action(s) of each alert event by checking the box under the column of **Email** and/or **SNMP Trap**. When the **Email** box is checked and the corresponding event occurs, it will trigger an action for PG5201B to send an e-mail alert to designated addresses configured in the E-Mail Settings (described in the next section). When the **SNMP Trap** box is checked and the corresponding event occurs, it will trigger an action for PG5201B to send a trap alert to the designated SNMP Trap server (specified in the above paragraph). There are five events that will trigger the alarm from PG5201B as listed in Figure 4-29. However, some event can only be reported by e-mail. These alerts are useful for security control or security monitoring of the PG5201B device:

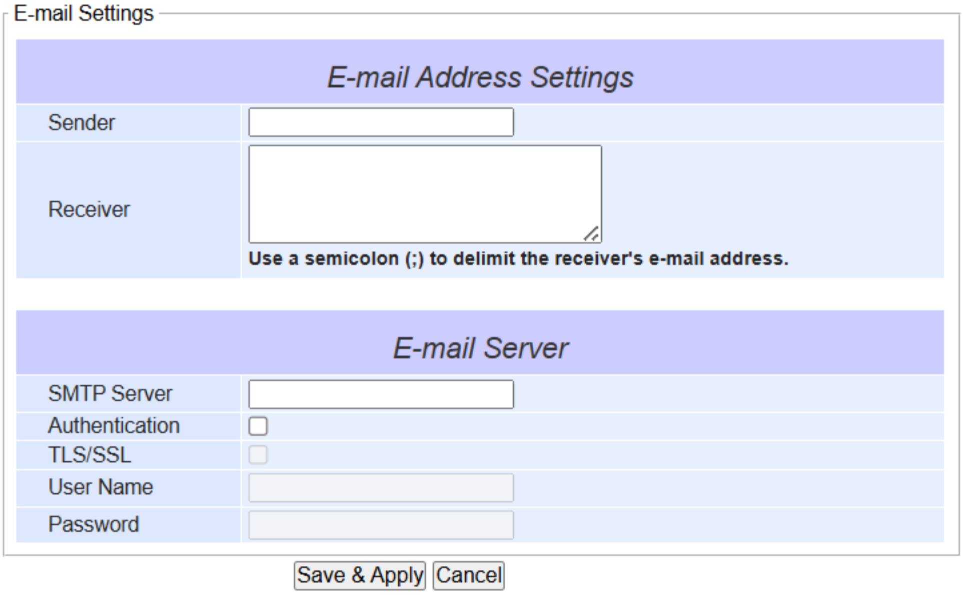
- **Warm Start**: This event occurs when the device resets.
- **Authentication Failure**: This event occurs when an incorrect username and/or password are entered which could indicate an unauthorized access to the PG5201B.
- **IP Address Changed**: This event occurs when the PG5201B device's IP address is changed.
- **Password Changed**: This event occurs when the administrator password is changed.

After finishing configuring the **SNMP/Alert Settings**, please click on **Save & Apply** button to keep the change that you have made and to apply your setting. When the saving and applying are finished, the web browser will remain on the **SNMP/Alert Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button.

Note: The options of "Cold Start" and "LAN Link Down-Relay" are only available for some specified models. For un-supported models, the "Cold Start" event option will not be shown on the page.

4.9 *E-Mail Settings*

When PG5201B device raises an alert and/or a warning message, it can send an e-mail to an administrator's mailbox. This **E-mail Settings** page allows you to set up the PG5201B to be able to send an e-mail. Figure 4-30 shows the **E-mail Settings** page in which there are two configurable parts: **E-mail Address Settings** and **E-mail Server**. First for the **E-mail Address Settings** part, a **Sender**'s e-mail address is required to be filled in the **Sender**'s text box which will be used in the **From** field of the e-mail. Note that the maximum length of sender email address is 48 characters. Then, for the **Receiver**'s text box you can enter multiple recipients which will be used in the **To** field of the e-mail. Note that to fill in multiple receiver e-mail addresses in the **Receiver**'s text box, please separate each e-mail address with semicolon (;).



E-mail Settings

E-mail Address Settings

Sender	
Receiver	Use a semicolon (;) to delimit the receiver's e-mail address.

E-mail Server

SMTP Server	
Authentication	□
TLS/SSL	□
User Name	
Password	

Figure 4-30 E-mail Setting Web Page

Second for the **E-mail Server** part, you must enter an **IP address** or **Host Name** of a **Mail Server** which is in your local network in the **SMTP Server**'s text box. Note that the maximum length of SMTP server address is 31 characters. If your Mail Server (or Simple Mail Transfer Protocol (SMTP) Server) requires a user authentication, you must check the "**SMTP server authentication required**" box in the **Authentication** option. Depending on your SMTP server, it may need to enable the TLS/SSL encryption method, too. After enabling the Authentication option, you can fill in the **Username** and the **Password** below. Please consult your local network administrator for the **IP address** of your **Mail Server** and the required **Username** and **Password**.

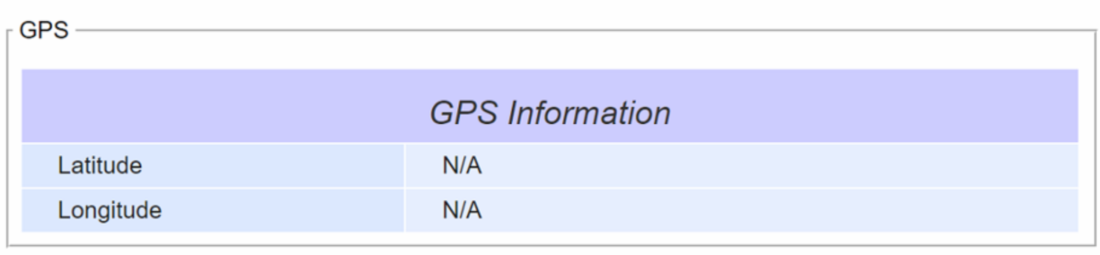
Attention

It is also important to setup Default Gateway and DNS Servers in the Network Settings properly so that PG5201B can lookup domain names and route the e-mails to the proper default gateway. Please see the Default Gateway and DNS Sever Settings in Section 4.5.1.

After finishing configuring the **E-mail Settings**, please click on **Save & Apply** button to keep the change that you have made and to apply your setting. When the saving and applying are finished, the web browser will remain on the **E-mail Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button.

4.10 *GPS (GPS model only)*

Atop's PG5201B-GPS series is equipped with GPS receiver to allows the device to acquire its current location. **The Global Positioning System (GPS)** is a space-based radio navigation system in which the GPS receiver requires signals from GPS's satellites orbiting the earth to calculate its location. Users do not need to activate the GPS module on the PG5201B since the GPS function is always enabled. However, please make sure that you plugged in the GPS antenna. When users selected the GPS menu, the device will provides the current location, including latitude and altitude information on the GPS web page as shown in Figure 4-31.



GPS

GPS Information	
Latitude	N/A
Longitude	N/A

Figure 4-31 GPS Web Page

4.11 *VPN*

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private networks, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. Figure 4-32 illustrates a VPN scenario of Atop's PG5201B device (green pattern) for your reference.

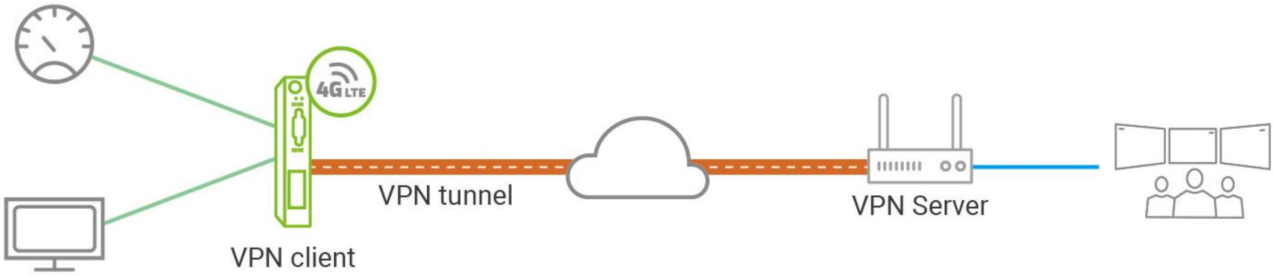


Figure 4-32 VPN Scenario of PG5201B Series

PG5201B Low-Power Gateway supports a number of VPN protocols which are IPsec (Internet Protocol Security), and OpenVPN. In order to configure VPN, please click on the related item in the dedicated VPN sub-menu on the left side of the screen, as shown in Figure 4-33 below. IPsec's basic will be discussed in Section 4.11.1 while IPsec related setting will be described in Section 4.11.2. Finally, OpenVPN Settings and Keys are described in Section 4.11.8 and Section 4.11.9, respectively.

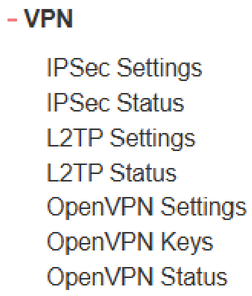


Figure 4-33 VPN Menu Structure

4.11.1 *IPsec*

IPsec (or Internet Protocol Security) which is a network protocol suit that can establish secure and reliable communications for different application scenarios. IPsec enables data confidentiality, data integrity, data origin authentication, and antireplay. For example, a corporate head quarter 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.

PG5201B 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 PG5201B 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 Host A (PG5201B) and a peer device Host B (such as another PG5201B). Note that this type of connection cannot be use for accessing entire sub-network resources. Figure 4-34 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode**.

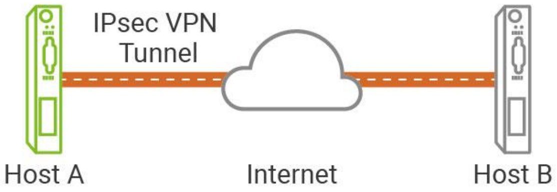


Figure 4-34 An Example of Host-to-Host Connection

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 4-35 illustrates a road-warrior application in which PG5201B can access a remote sub-network resource via a peer gateway. Figure 4-36 illustrates a gateway application in which Host A PG5201B can passively accept connection requests from remote sides Host B and provide access to the PG5201B sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

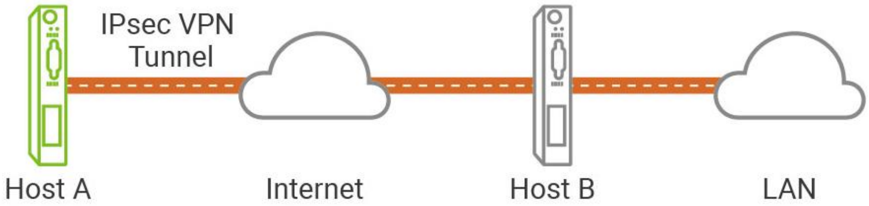


Figure 4-35 Roadwarrior Application using Host-to-Subnet Connection

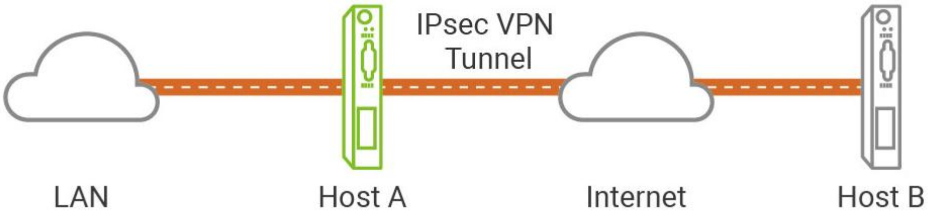


Figure 4-36 Gateway Application using Host-to-Subnet Connection

A **subnet-to-subnet** connection is mainly used to connect two subnets from different sides together. Typically, applications are corporate headquarters and branch offices that share internal network resources. A specific application can also be set up as one side's subnet to establish IPsec VPN tunnels for accessing a device in the other side's subnet or as a device in one's side subnet to establish IPsec VPN tunnels for accessing another device in the other side's subnet. Figure 4-37 illustrates an example of the subnet-to-subnet connection with a network application. A host inside the remote subnet can also connect to a local subnet (host-network application) based on this subnet-to-subnet connection as shown in Figure 4-38. On the other hand, two different devices on two different subnets (host-host application) can be connected via an IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 4-39. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

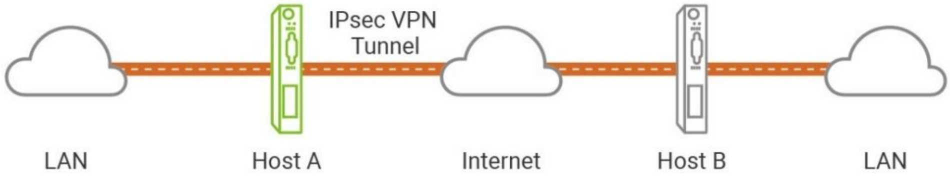


Figure 4-37 An example of network application using a subnet-to-subnet connection via the PG5201B and a peer device

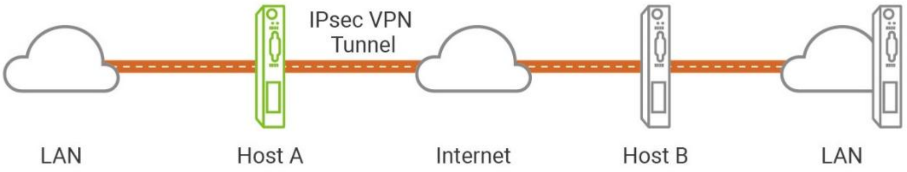


Figure 4-38 An example of host-network application via the subnet-to-subnet connection

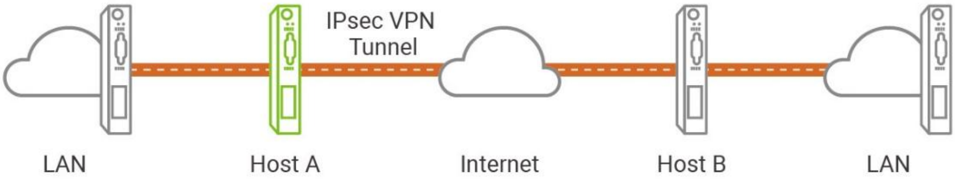


Figure 4-39 An example of host-host application via the subnet-to-subnet connection

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

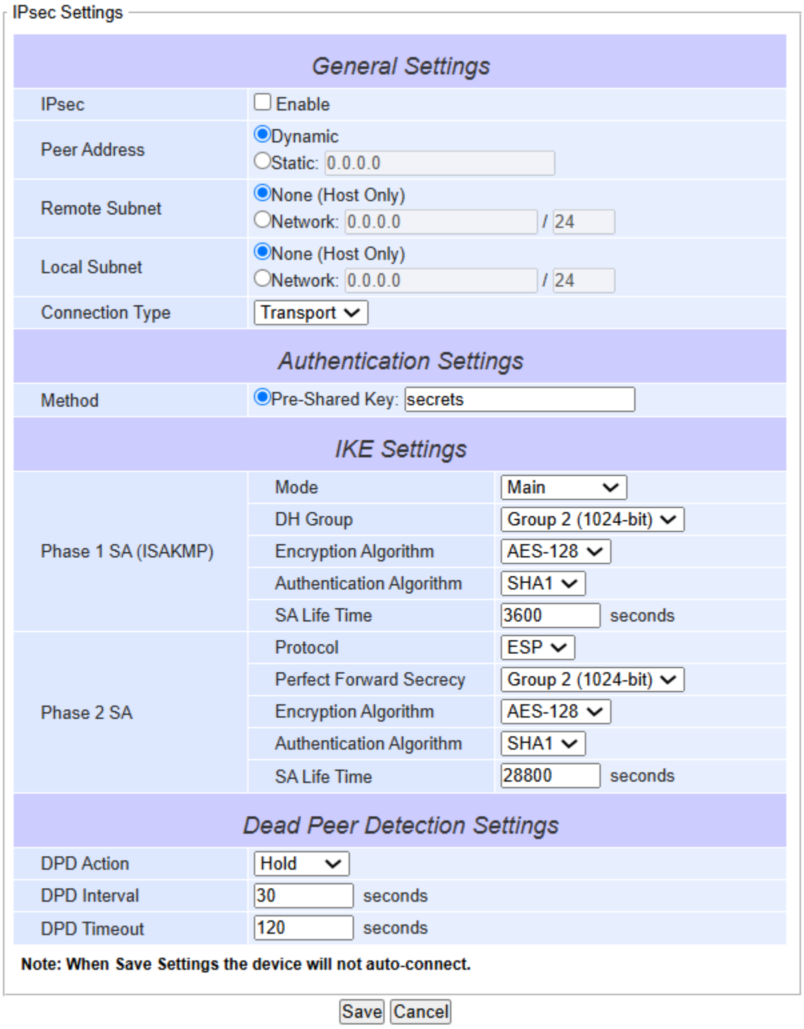
- Internet Key Exchange (IKE) protocol uses User Datagram Protocol (UDP) port number 500.
- Encapsulating Security Payload (ESP) uses IP protocol number 50.
- Authentication Header (AH) uses IP protocol number 51.
- IPsec NAT traversal uses UDP port number 4500 when NAT traversal is in use.

PG5201B also has a feature called NAT traversal (NAT-T) that allows the IPsec tunnel to pass through the NAT in its network. PG5201B will activate this option automatically and encapsulate the IPsec packets inside UDP port 4500 to be able to pass through a NAT router.

To provide security service for all types of tunnel connections and applications described above, PG5201B 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 association (SA) is divided into two phases. In phase one, IKE creates an authenticated secure channel between PG5201B and its peer device, which is called the IKE Security Association. The Diffie-Hellman (DH) key agreement is always performed in this phase to create a shared secret key or DH key. In phase two, IKE negotiates the IPsec security associations and generates the required key material for IPsec. This IPsec key which is a symmetrical key will be used for bulk data transfer inside the IPsec tunnel. A new Diffie-Hellman agreement can be done in phase two, or the keys can be derived from the phase one shared secret.

4.11.2 *IPsec Settings*

Figure 4-40 shows the IPsec Settings web page under the IPsec Settings menu. There are four sections on this page: **General Settings**, **Authentication Settings**, **IKE Settings**, and **Dead Peer Detection Settings**.



IPsec Settings

General Settings

IPsec	☐ Enable
Peer Address	● Dynamic ○ Static: 0.0.0.0
Remote Subnet	● None (Host Only) ○ Network: 0.0.0.0 / 24
Local Subnet	● None (Host Only) ○ Network: 0.0.0.0 / 24
Connection Type	Transport

Authentication Settings

Method	● Pre-Shared Key: secrets

IKE Settings

Phase 1 SA (ISAKMP)	Mode	Main
	DH Group	Group 2 (1024-bit)
	Encryption Algorithm	AES-128
	Authentication Algorithm	SHA1
	SA Life Time	3600 seconds
Phase 2 SA	Protocol	ESP
	Perfect Forward Secrecy	Group 2 (1024-bit)
	Encryption Algorithm	AES-128
	Authentication Algorithm	SHA1
	SA Life Time	28800 seconds

Dead Peer Detection Settings

DPD Action	Hold
DPD Interval	30 seconds
DPD Timeout	120 seconds

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

Figure 4-40 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 PG5201B.
- **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 PG5201B 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 PG5201B will be the initiator/responder.
- **Remote Subnet**: This option is to indicate whether you want to create an IPsec connection to the remote subnetwork. There are also two choices for **Remote Subnet** access:

  - **None (Host Only)**: This option is to specify that the remote subnet is not supported or no remote subnet and only host access is supported. That is the remote end of the IPsec tunnel is a host or peer device only.
  - **Network**: This option is to specify the **Remote Subnet** by entering the **Subnet IP Address** and the number of **Subnet Masking Bits** or associated routing prefix. This option supports the Classless Inter-Domain Routing (CIDR) notation. For example, Subnet IP Address is 192.168.11.0 and Subnet mask are 24 bits (from 255.255.255.0).

- **Local Subnet:** This option is to enable an IPsec connection to the local subnetwork. There are two choices for **Local Subnet** access:
  - **None (Host Only):** This option is to specify that the local subnet is not supported or no local subnet and only local host access is supported. That is the local end of the IPsec tunnel is a host or peer device only.
  - **Network:** This option is to specify the **Local Subnet** by entering the **Subnet IP Address** and the number of **Subnet Masking Bits** or associated routing prefix. This option supports the Classless Inter-Domain Routing (CIDR) notation. For example, Subnet IP Address is 192.168.11.0 and Subnet mask are 24 bits (from 255.255.255.0).
- **Connection Type**: This option is to specify the IPsec connection type which can be either **Tunnel** mode or **Transport** mode. Please select the corresponding connection type from the drop-down list. Note that the **Tunnel mode** can be applied to the **host-to-host**, the **host-to-subnet**, and the **subnet-to-subnet** communications. The **Transport mode** can only be applied in the **host-to-host** communication.

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

The third part of **IPsec Settings** is the **IKE** (Internet Key Exchange) **Settings.** Internet Key Exchange (IKE) that PG5201B supports is the IKE version 1 or **IKEv1.** Within the **Phase 1 SA (ISAKMP)**, there are five security options to be configured. In phase 1, the two VPN gateway exchange information about the encryption algorithms that they support and then establish a temporary secure connection to exchange authentication information.

- First option is the **Mode** of IKE session which defines how many steps or packets will be used or exchanged during the IKE SA negotiation. You can choose either **Main Mode** or **Aggressive Mode**. The **Main Mode** will send SA proposals, Diffie-Hellman public key, and ISAKMP session authentication in three exchange packets, while the **Aggressive Mode** will put all SA proposals, DH public key, and ISAKMP session authentication in to one exchange packet. **Aggressive Mode** makes the IKE negotiation quicker than **Main Mode**. The difference between **Main Mode** and **Aggressive Mode** is that the "identity protection" is used in the **Main Mode**. The identity is transferred encrypted in the **Main Mode** but it is not encrypted in **Aggressive Mode**. Typically, the **Main Mode** is recommended.
- Second option is the selection of Diffie-Hellman's group (**DH Group**) of standardized global unique prime numbers and generators that will be used to provide secure asymmetric key exchange. The **DH Group** is used to encrypt this IKE communication. PG5201B supports two **DH groups** which are **DH Group 2**, which is a 1024-bit modular exponentiation group (MODP), and **DH Group 5**, which is a 1536-bit MODP group.
- Third option is the selection of **Encryption Algorithm** which can be either **AES-128** or **3DES**. This option will select the key size and encryption algorithm to be used in the IKEv1 Phase 1. The default value is **AES-128**.
- Fourth option is the selection of **Authentication Algorithm** which can be either **SHA1** or **MD5**. This option will select which hash algorithm will be used to authenticate packet data in the IKEv1 Phase 1. The default value is **SHA1**.
- Fifth option is the **SA Life Time** which must be set in unit of seconds. This value represents the lifetime of the IKE key which is dedicated at Phase 1 between both end host or network. The default **SA Life Time** is 10800 seconds. The configurable range for **SA Life Time** is between 300 to 86400 seconds.

Within the **Phase 2 SA**, there are five security options to be configured. Similar to **Phase 1 SA**, PG5201B and its peer device will negotiate or exchange proposals to determine which security parameters will be used in this Phase 2 SA. A Phase 2 proposal also includes a security **Protocol** (first option), which you can choose either Encapsulating Security Payload (**ESP**) or Authentication Header (**AH**). The second option is the **Perfect Forward Secrecy** which is a property of key-agreement protocol to ensure that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. In Phase 2 SA, PG5201B also supports two **DH groups** which are **DH Group 2** (1024-bit) and **DH Group 5** (1536-bit).

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

The final part of the **IPsec Settings** is the **Dead Peer Detection Settings**. Dead peer detection (DPD) is a mechanism that PG5201B use to verify the existence of a remote Internet Key Exchange (IKE) gateway or the peer device of PG5201B. To detect the peer device, PG5201B will send encrypted IKE Phase 1 notification payloads (or hello message) to its peer device and wait for DPD acknowledgement from the peer device. If PG5201B does not receive an acknowledge message during a specific time interval (**DPD timeout**), it will consider that the peer device is dead. Then, PG5201B 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 PG5201B 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 PG5201B will repeatedly 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 PG5201B 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 PG5201B will take the PDP action. The **DPD Timeout** value range from 1 to 65535 seconds. The default value of **DPD Timeout** is 120 seconds. Description of each parameter in the IPsec Tunnels web page is summarized in Table 4.7.

Table 4.7 Description of Parameters in IPsec Tunnels Web Page

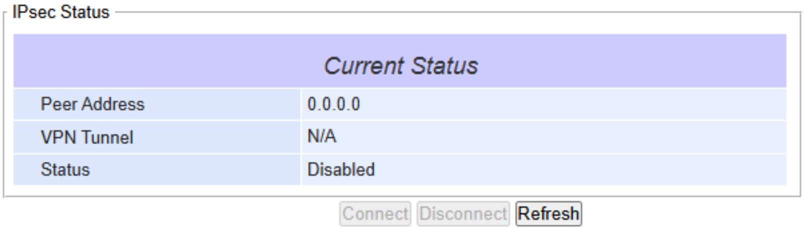
Field Name		Description	Default Value
General Settings			
IPsec		Enable the IPsec Tunnel	Disable
NAT Traversal		Enable the NAT Traversal mechanism	Enable
Peer Address		IP address of the remote device which can be dynamic (any address) or static (fixed address)	Dynamic
Remote Subnet		Remote subnet can be either None (Host only) or Network (IP and Netmask)	None (Host Only)
Local Subnet		Local subnet can be either None (Host Only) or Network (IP and Netmask)	None (Host Only)
Connection type		Tunnel mode or Transport mode	Tunnel
Authentication Settings			
Method		Pre-Shared Key	secrets
IKE Settings			
Phase 1 SA	**Mode**	Choose how IKE negotiation is performed between Main Mode and Aggressive Mode	Main Mode
	DH Group	Diffie-Hellman groups, determine the strength of the key used in the key exchange	Group 2 (1024-bit)

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

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

4.11.3 *IPsec Status*

On this web page, you can check the status of your IPsec connection between PG5201B and its peer device in different connection types and modes. The first information is the **Peer Address** which is the IP address of the other device that is connected to PG5201B. The second information is the **VPN Tunnel**'s status. The third information is the **Status** of the IPsec connection which can be **Disabled**, **Listening**, or **Connected**. Figure 4-41 shows the **IPsec Status** web page under the **IPsec Settings** menu. There are three buttons at the end of the web page which are **Connect**, **Disconnect**, and **Refresh**. The **Connect** and **Disconnect** buttons allow you to establish or tear down the IPsec connection. The **Refresh** button enable you to check the latest status of the connection.



IPsec Status

Current Status	
Peer Address	0.0.0.0
VPN Tunnel	N/A
Status	Disabled

Figure 4-41 IPsec Status Web Page

4.11.4 *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 now supported in new firmware of PG5201B.

4.11.5 *Host-to-Host Connections*

Two scenarios can be configured for host-to-host connections: with static peer and with dynamic peer. A host-to-host topology for both scenarios is illustrated in Figure 4-42

. Please follow the steps provided next for each scenario to set the **General Settings**.

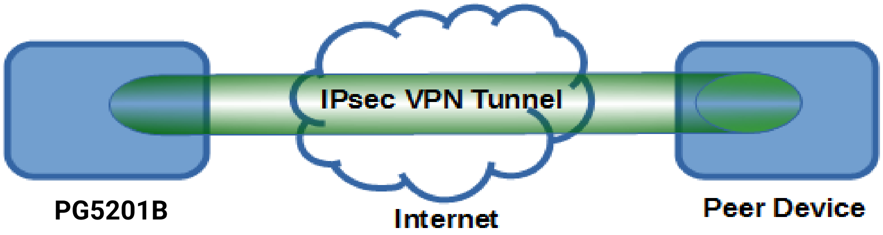
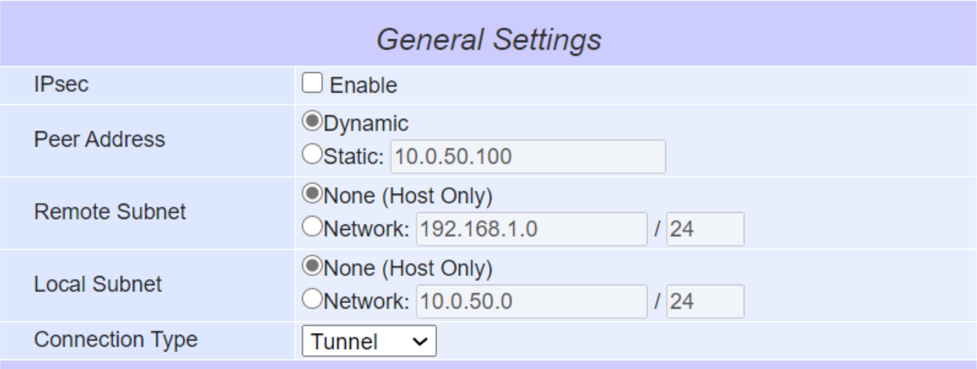


Figure 4-42 IPsec VPN Tunnel with Host-to-Host Topology

Scenario: host-to-host with static peer as shown in Figure 4-43

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  Note: When peer address is entered as the static address, the PG5201B acts as an **initiator** which takes the initiative and establishes a connection. The PG5201B also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Select the radio button for **None (Host Only)** in the **Remote Subnet** field.
- Since this VPN connection is established on two hosts, the **Connection Type** option can be either **Transport** or **Tunnel**.

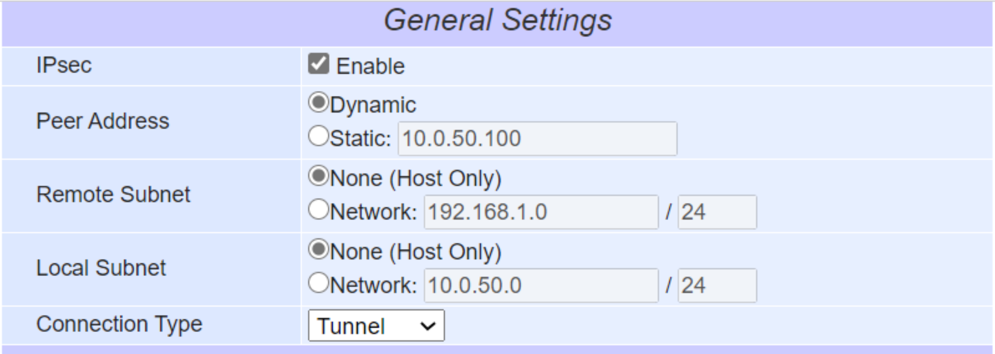


General Settings	
IPsec	☐ Enable
Peer Address	● Dynamic ○ Static: 10.0.50.100
Remote Subnet	● None (Host Only) ○ Network: 192.168.1.0 / 24
Local Subnet	● None (Host Only) ○ Network: 10.0.50.0 / 24
Connection Type	Tunnel

Figure 4-43 General Settings for Host-to-Host with Static Peer

Scenario: host-to-host with dynamic peer as shown in Figure 4-44

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  Note: When VPN connects to a peer with dynamic IP address, the PG5201B acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- The remaining settings are the same as the host-to-host with static peer scenario described above.



General Settings	
IPsec	☑ Enable
Peer Address	● Dynamic ○ Static: 10.0.50.100
Remote Subnet	● None (Host Only) ○ Network: 192.168.1.0 / 24
Local Subnet	● None (Host Only) ○ Network: 10.0.50.0 / 24
Connection Type	Tunnel

Figure 4-44 General Settings for Host-to-Host with Dynamic Peer

4.11.6 *Host-to-Network Connections*

Two scenarios can also be configured for host-to-network (or host-to-subnet or host-to-site) connections: with static peer and with dynamic peer. Note that the PG5201B is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in Figure 4-45. Please follow the steps provided next for each scenario to set the **General Settings**.

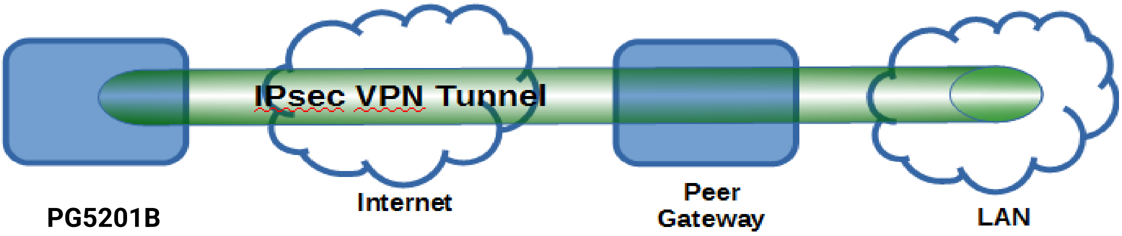
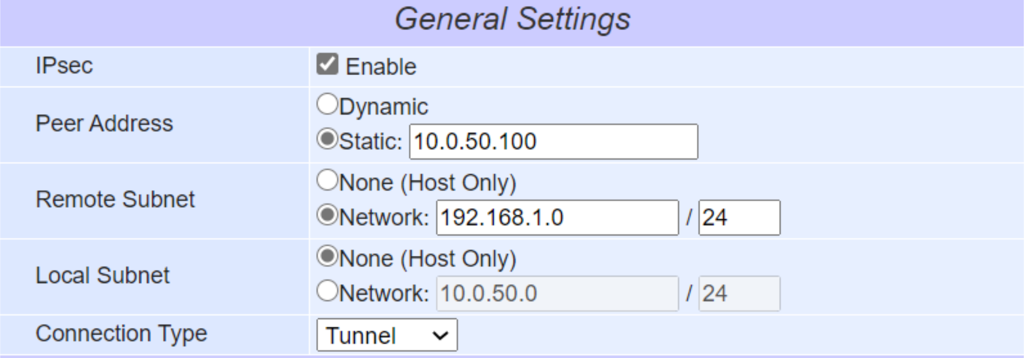


Figure 4-45 IPsec VPN Tunnel with Host-to-Network Topology

Scenario: host-to-network with static peer as shown in Figure 4-46

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  Note: When peer address is entered as a static address, the PG5201B is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. The PG5201B also acts as a **responder** and passively accepts the connection initiated by the remote gateway.

- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.

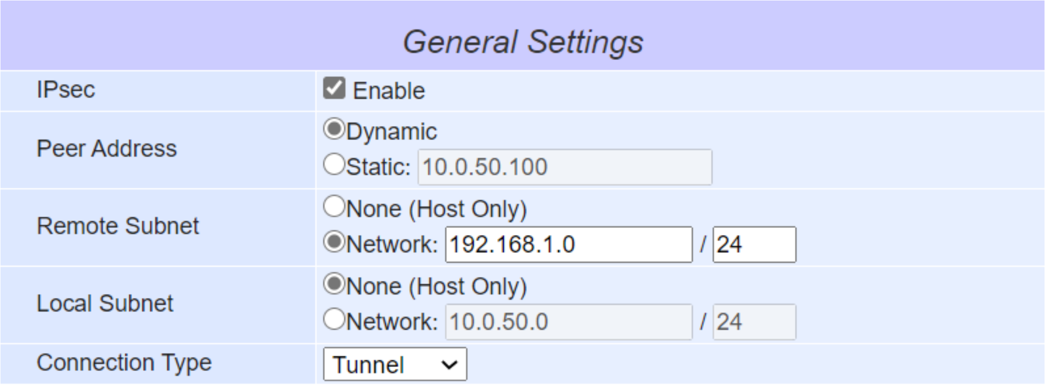


General Settings	
IPsec	☑ Enable
Peer Address	○Dynamic ●Static: 10.0.50.100
Remote Subnet	○None (Host Only) ●Network: 192.168.1.0 / 24
Local Subnet	●None (Host Only) ○Network: 10.0.50.0 / 24
Connection Type	Tunnel

Figure 4-46 General Settings for Host-to-Network with Static Peer

Scenario: host-to-network with dynamic peer as shown in Figure 4-47

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  <u>**Note:**</u> When VPN connection is set to a peer with dynamic IP address, the PG5201B will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.



General Settings	
IPsec	☑ Enable
Peer Address	●Dynamic ○Static: 10.0.50.100
Remote Subnet	○None (Host Only) ●Network: 192.168.1.0 / 24
Local Subnet	●None (Host Only) ○Network: 10.0.50.0 / 24
Connection Type	Tunnel

Figure 4-47 General Settings for Host-to-Network with Dynamic Peer

4.11.7 *Network-to-Network (Subnet-to-Subnet) Connections*

Two scenarios can also be configured for network-to-network (or subnet-to-subnet) connections: with static peer or with dynamic peer. A VPN tunnel will be created between two separate private sub-networks. Note that the PG5201B is the gateway to a local network in these scenarios. A network-to-network topology for both scenarios is illustrated in Figure 4-48. Please follow the steps provided next for each scenario to set the **General Settings**.

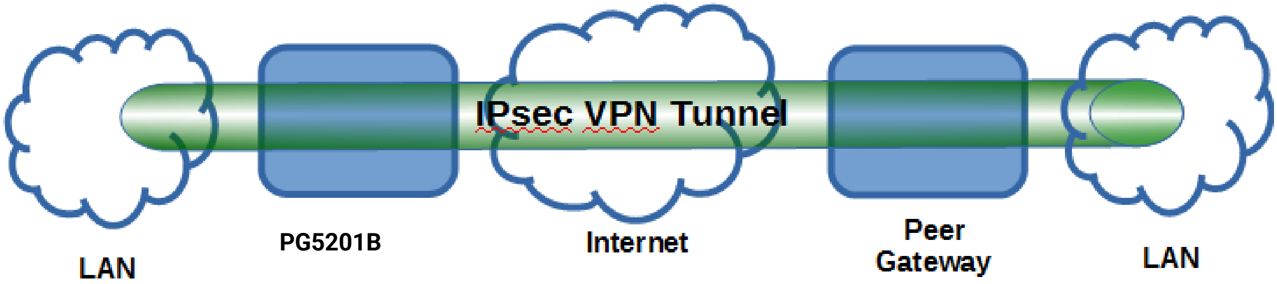
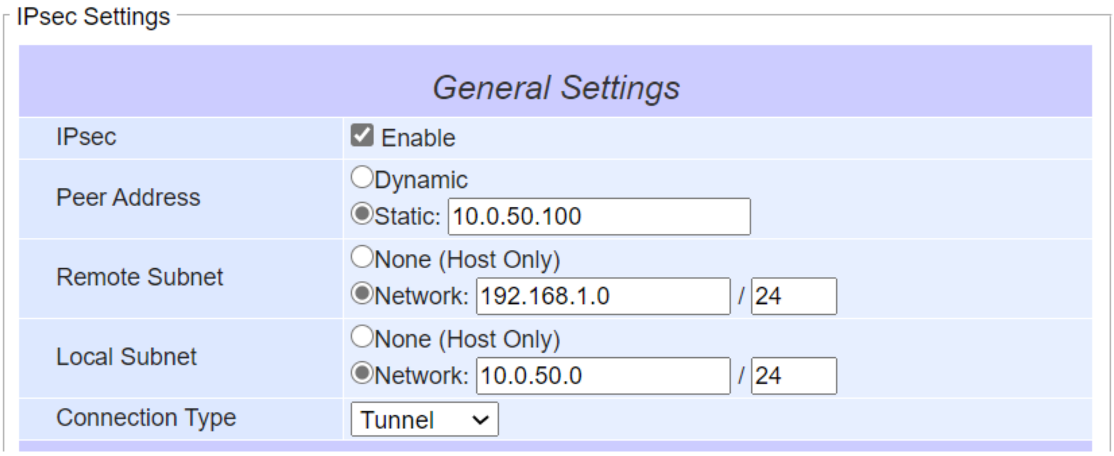


Figure 4-48 IPsec VPN Tunnel with Network-to-Network Topology

Scenario: network-to-network with static peer as shown in Figure 4-49

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  Note: When peer address is entered as a static address, the PG5201B is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. The PG5201B also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in "address prefix length" or behind the "/" symbol.
- Set the network IPv4 address in the **Local Subnet** with the number of bits for subnetmask in "address prefix length" or behind the "/" symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.



IPsec Settings

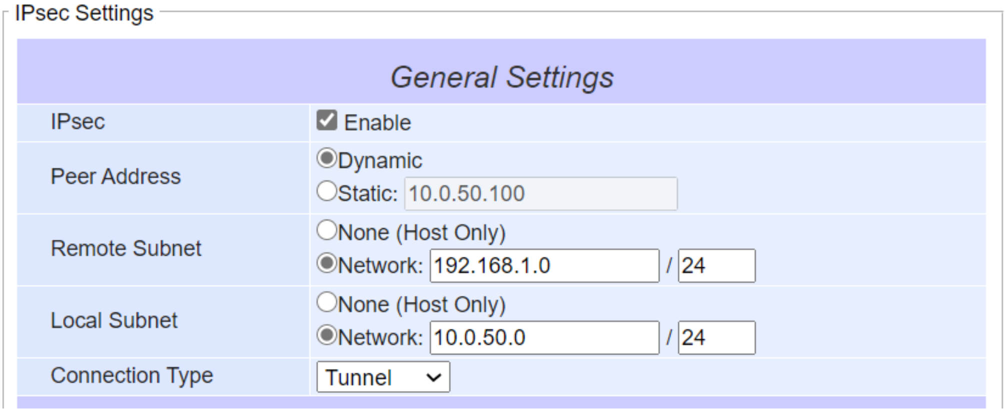
General Settings

IPsec	☑ Enable
Peer Address	○Dynamic ●Static: 10.0.50.100
Remote Subnet	○None (Host Only) ●Network: 192.168.1.0 / 24
Local Subnet	○None (Host Only) ●Network: 10.0.50.0 / 24
Connection Type	Tunnel

Figure 4-49 General Settings for Network-to-Network with Static Peer

Scenario: network-to-network with dynamic peer as shown in Figure 4-50

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  Note: When VPN connection is set to a peer with dynamic IP address, the PG5201B will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in "address prefix length" or behind the "/" symbol.
- Set the network IPv4 address in the **Local Subnet** with the number of bits for subnetmask in "address prefix length" or behind the "/" symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.



IPsec Settings

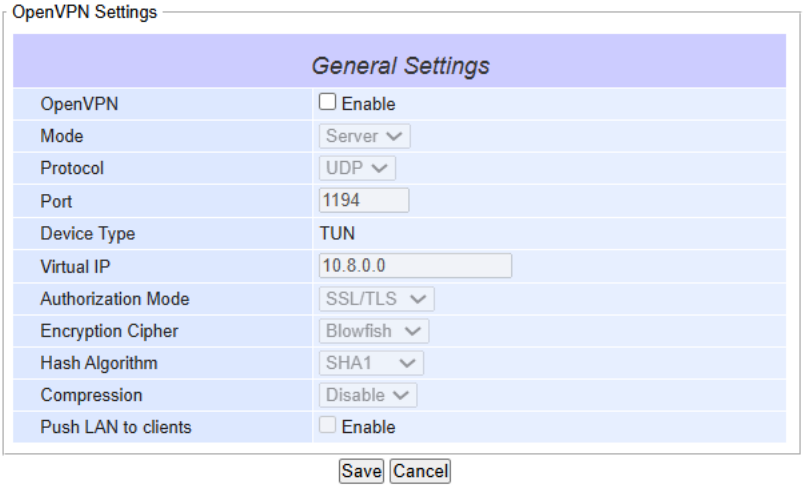
General Settings	
IPsec	☑ Enable
Peer Address	● Dynamic ○ Static: 10.0.50.100
Remote Subnet	○ None (Host Only) ● Network: 192.168.1.0 / 24
Local Subnet	○ None (Host Only) ● Network: 10.0.50.0 / 24
Connection Type	Tunnel

Figure 4-50 General Settings for Network-to-Network with Dynamic Peer

4.11.8 *OpenVPN Setting*

OpenVPN is an application that implements VPN for creating secure point-to-point or site-to-site connections in routed or burdged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificates. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and certificate authority.
There are two OpenVPN connection scenarios. They are the TAP and TUN scenario. The product can create ether a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, you have to specify which type of OpenPVN connection scenario is to be adopted. Currently PG5201B series only support TUN mode.

In order to configure OpenVPN, click on the VPN tab in the left side of the menu and then **OpenVPN Settings**. The user interface is shown in Figure 4-51.



OpenVPN Settings

General Settings	
OpenVPN	□ Enable
Mode	Server
Protocol	UDP
Port	1194
Device Type	TUN
Virtual IP	10.8.0.0
Authorization Mode	SSL/TLS
Encryption Cipher	Blowfish
Hash Algorithm	SHA1
Compression	Disable
Push LAN to clients	□ Enable

Figure 4-51 OpenVPN Setting

The OpenVPN parameters are described as following:

OpenVPN: Check this box to enable OpenVPN.

Mode: This parameter specifies what the role of this device will be which can be either **Server** or **Client**. When choosing server mode, the device will play as server role and will standby for client connection.

Protocol: The user can select the transport layer protocol that will be used for VPN (**TCP** or **UDP**).

Port: This parameter defines the port number for TCP/UDP connection.

Device Type: OpenVPN tunnel connection by TUN (Tunnel) mode or TAP mode. Currently PG5201B series only supports **TUN** (Tunnel) mode.

Virtual IP (only when "OpenVPN Server" mode is selected): This field specifies the server's virtual IP. Virtual IP will only be available when SSL/TLS is chosen as the Authentication Mode. The Server's virtual IP address will be 10.8.0.1/24 and client virtual IP address will be 10.8.0.x/24.

Local/Remote endpoint IP (only when "OpenVPN Client" mode is selected): This fields specifies the local and remote endpoint virtual IP address of this OpenPVN gateway. Local/Remote endpoint IP will be available when static key is chosen in Authentication Mode.

Authentication Mode: This parameter specifies the authorization mode of the OpenVPN server. There are two options available:

SSL/TLS and **SSL/TLS (TLS Auth)**: When OpenVPN uses TLS authorization mode, the CA Cert, Server Cert and DH PEM will be used. See the next Section for mode details.

Static Key: When OpenVPN uses static key authorization, the static key will be used. See the next Section for mode details.

Encryption Cipher: This parameter specifies the Encryption cipher. There are five options available: **Blowfish**, **AES 256**, **AES 192**, **AES 128** and **Disable**. When Disable option is selected, no encryption will be used.

Hash Algorithm: This parameter specifies the Hash algorithm. There are five options available: **SHA1**, **MD5**, **SHA 256**, **SHA 512** and **Disable**.When Disable option is selected, no Hash algorithm will be used.

Compression: This parameter specifies whether or not the tunnel packets will be compressed. There are three options available: **LZ4**, **LZO** and **Disable**. When Disable option is chosen, the packet will not be compressed.

Push LAN to clients (only when "OpenVPN Server" mode is selected): When this option is enabled, PG5201B will push the LAN port subnet to the OpenVPN remote client so that the remote client will add a route to the PG5201B local network. Only PG5201B supports this function.

4.11.9 *OpenVPN Keys*

OpenVPN requires encryption keys (unless Encryption Cipher is disabled). In order to key-in, import or generate encryption keys, please select "OpenVPN Keys" from the VPN menu on the left side of the user interface. The OpenVPN Keys web page is shown in Figure 4-52. The following terms are related to the OpenVPN keys:

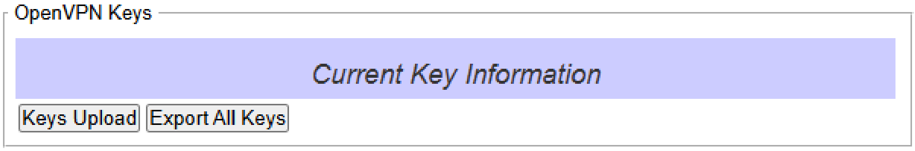


Figure 4-52 OpenVPN Keys web page

Certificate Authority: A certificate authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. A CA acts as a trusted third party, trusted both by the owner and by the party relying upon the certificate.

Server Certificate: It shows the information of server certificate. You can check the information if you use upload server certificate file.

Server Key: It shows the information of server key. You can check the information if you use upload server key file.

Diffie Hellman parameters: It shows the information of Diffie Hellman parameters.

When PG5201B acts as OpenVPN server, the user can import his/her own certification information by clicking on the **Key Upload** button. When clicking on the **Keys Upload** button, a pop-up window shown in Figure 4-53 will show up and will allow you to import the related server certificates. Note that for OpenVPN client, the pop-up window is slightly different as shown in Figure 4-54.

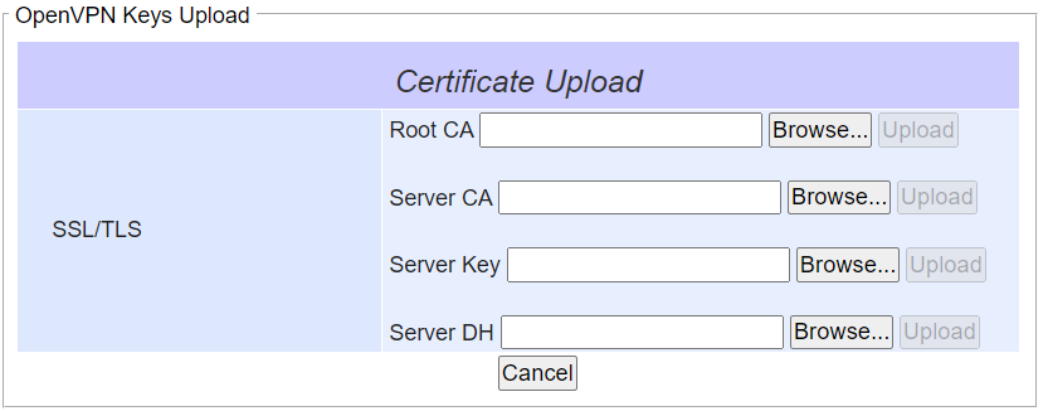


Figure 4-53 Certificate Upload for OpenVPN Server

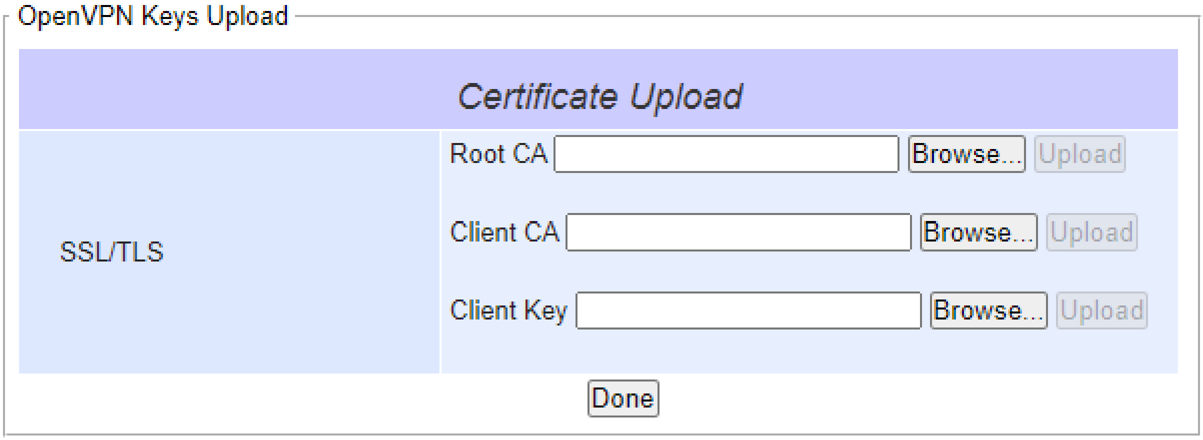
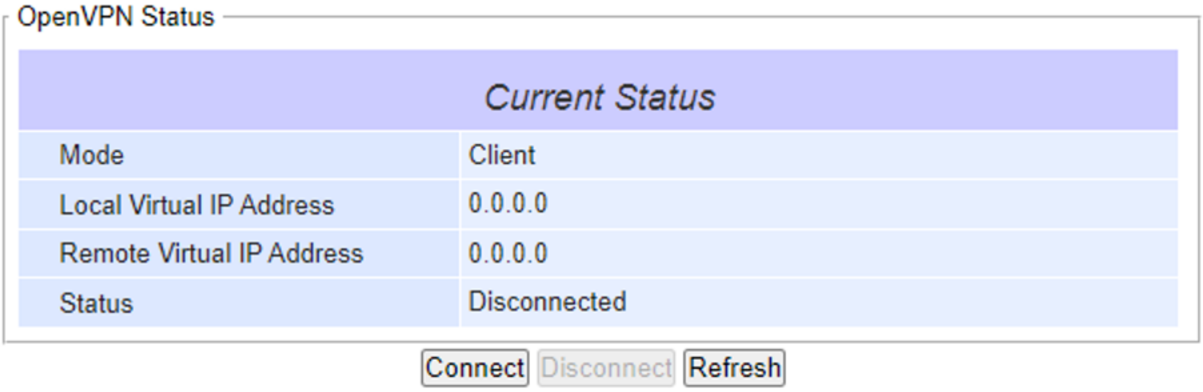


Figure 4-54 Certificate Upload for OpenVPN Client

Click the **Browse** button to select your own server or client certificate and click on the **Upload** button. When PG5201B acts as an OpenVPN server, use the **Export All Keys** button to download all the necessary certificates including CA.crt, CA.key and the certificate and key for client side.

4.11.10 *OpenVPN Status*

In order to check the current OpenVPN connection status, click "OpenVPN status" in the VPN menu on the left side of the screen. A web page similar to Figure 4-55 or Figure 4-56 will show up depending whether OpenVPN is set as a Client or a Server.



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

Figure 4-55 OpenVPN Client Status

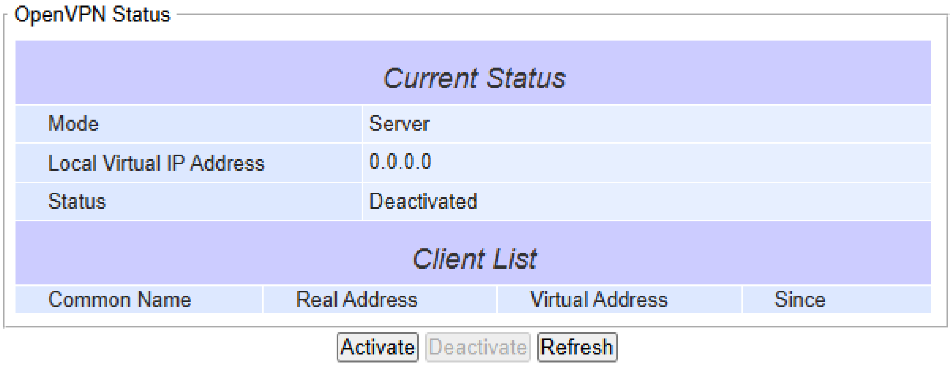
The description of each field under the Current Status of OpenVPN when it is in Client mode is as follows.

Mode: This indicates the OpenVPN mode that PG5201B is currently running as.

Local Virtual IP address: This field displays the Local virtual IP address.

Remote Virtual Status: This field displays the Remote virtual IP address.

Status: This field displays the current status of OpenVPN connection. It can be: Disconnected, Connecting or Connected.



OpenVPN Status

Current Status	
Mode	Server
Local Virtual IP Address	0.0.0.0
Status	Deactivated

Client List

Common Name	Real Address	Virtual Address	Since

Figure 4-56 OpenVPN Server Status

The description of each field under the Current Status of OpenVPN when it is in Server mode is as follows.

Mode: This indicates the OpenVPN mode that PG5201B is currently running as.

Local Virtual IP address: This field displays the Local virtual IP address.

Status: This filed displays the current status of OpenVPN connection. It can be: Deactivated, Activating, Disconnected, Connecting or Connected.

Client List: This table provide the list of clients and their information which are Common Name, Real Address, Virtual Address, and Since (the timestamp).

4.12 *Log Settings*

Under the **Log Settings** menu of web interface of PG5201B series Low-Power Gateway, you can configure various data logging for the device. Figure 4-57 lists the sub-menu under the **Log Settings**. It consists of **System Log Settings**, **COM Log Settings**, **System Log**, **COM log** and **Mobile Log.** Each of this sub-menu will be described in the following subsections.

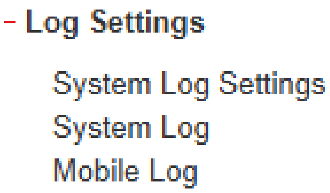
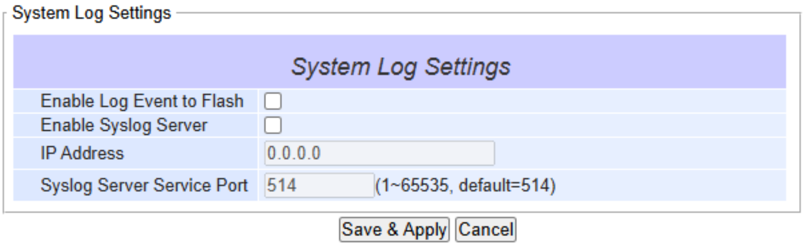


Figure 4-57 Log Setting Menu

4.12.1 *System Log Settings*

The Syslog function is turned on by default and cannot be turned off for PG5201B. It is used to keep log for system events and report to an external Syslog server if necessary. Figure 4-58 shows the **System Log Settings** page under the **Log Settings** menu. Description of each option is provided as follows.



System Log Settings

System Log Settings	
Enable Log Event to Flash	□
Enable Syslog Server	□
IP Address	0.0.0.0
Syslog Server Service Port	514 (1~65535, default=514)

Figure 4-58 Log Settings Web Page under Log Settings

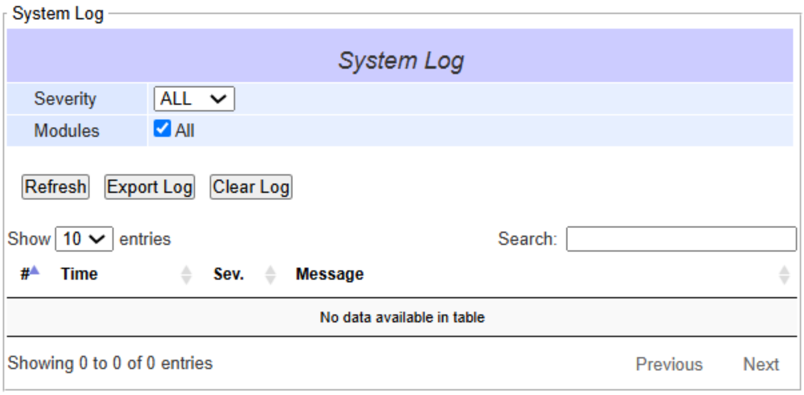
- **Enable Log Event to Flash**: When the check box is enabled, PG5201B will write log events to the local flash. Otherwise, the log events would be cleared when the device restarts because they are stored in the RAM by default.
- **Enable Syslog Server:** When the check box is enabled, it will allow PG5201B to send Syslog events to the remote Syslog server with the specified IP address (next option).
- **IP Address**: The user must specify the IP address of a remote Syslog Server in this field.
- **Syslog Server Service Port**: This option allows user to specify the remote Syslog Server Port number between 1 and 65535. Note that the default port number is 514.

After finishing configuring the **Log Settings**, please click on **Save & Apply** button to keep the change that you have made and to apply your setting. When the saving and applying are finished, the web browser will remain on the **Log Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button.

4.12.2 *System Log*

This page displays the current event log or system log stored in the PG5201B device. Figure 4-59 shows an example of logged event. In the **Severity** option, the user can choose the level of severity (i.e., All, Err, Warn, Info) to inspect from the drop-down box. The **Modules** option allows user to view only log from today or all available logs.

Each record of the **System Log** consists of **Time**, **Sev.** (short for Severity), and **Message** description.



System Log

System Log	
Severity	ALL
Modules	☑ All

#	Time	Sev.	Message
No data available in table			

Showing 0 to 0 of 0 entries

Figure 4-59 System Log Web Page under System Setup

At the end of the **System Log** page, there are two hyperlinks which can be used to navigate through all records. You can click on the "**Previous**" link to go to the last page of the log and click on the "**Next**" button to go to the next page. At the top of the **System Log** table, there are three buttons: **Refresh**, **Export Log**, and **Clear Log**. To display the latest event, you can click on **"Refresh"** button. When you click on the Export Log button, a log file will be saved on to your PC. By clicking on "**Clear Log**" button, you can clear all events stored in the device and the **System Log** will be empty. A message "No data available in table" will be displayed in the middle of the table. Moreover, you can choose from the drop-down list of 10 or 25 entries for the **Show entries**. Finally, you can search over the **System Log** by entering a keyword in the **Search** box.

4.12.3 *Mobile Log*

The Mobile Log menu provides log data related to the mobile interface on the PG5201B. The first line graph on this web page is the the Mobile Signal which plots the mobile Received Signal Strength Indication (RSSI) versus time as shown in Figure 4-60. The second line graph on this web page is the Mobile Temperature. This plots the temperature of the mobile module inside the PG5201B chasis versus the time as shown in Figure 4-61. Note that the mobile signal and the mobile temperature will be updated every 2 minutes and the system will record the data up to the maximum of 2 hours.

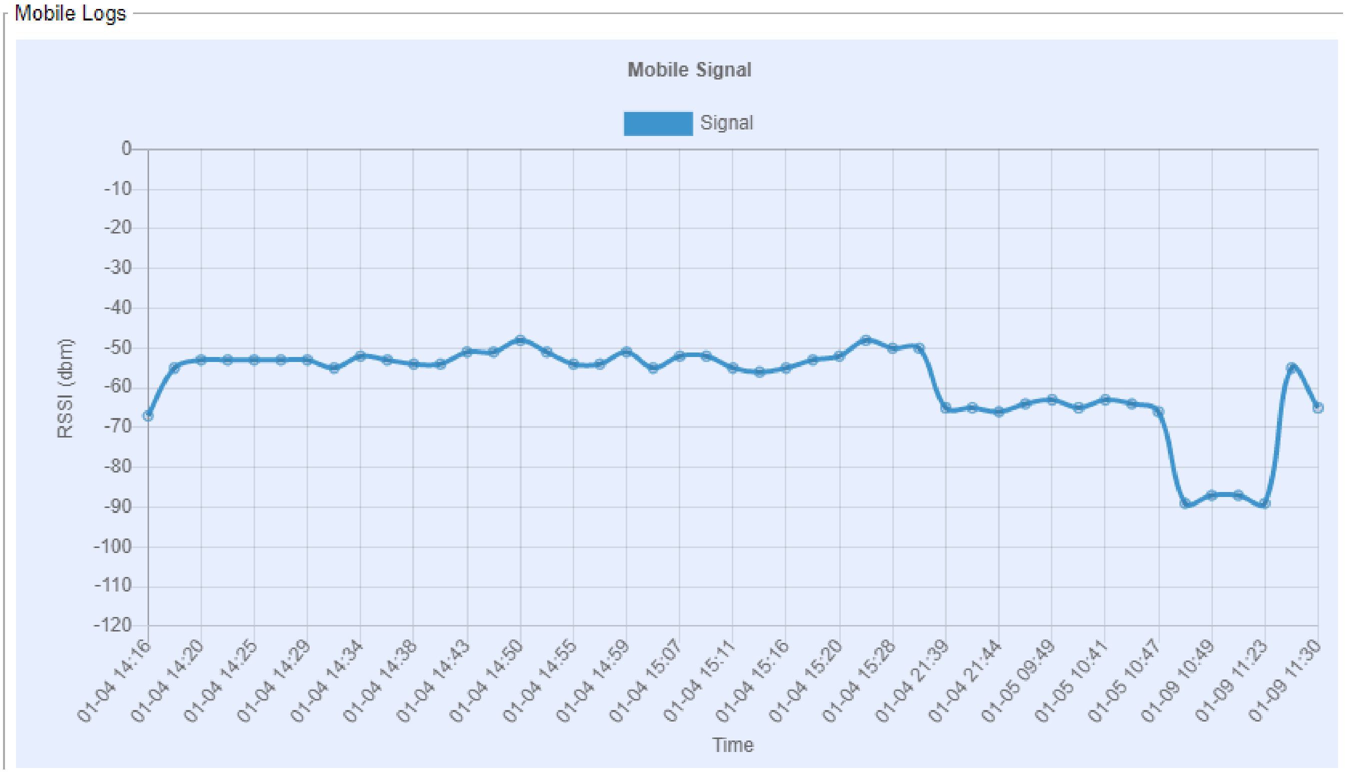


Figure 4-60 Mobile Log: Mobile Signal

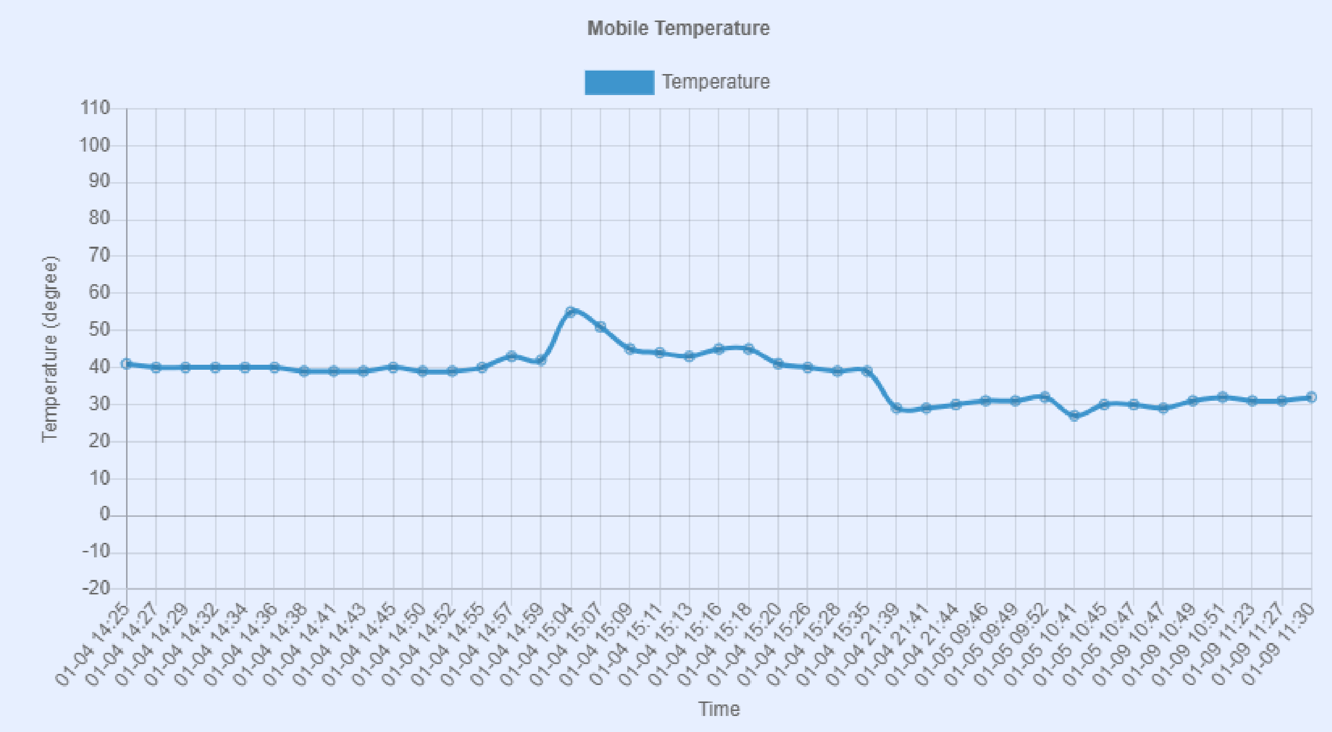


Figure 4-61 Mobile Log: Mobile Temperature

4.13 *System Setup*

Under the **System Setup** menu of web interface of PG5201B Low-Power Gateway, you can perform a number of administration tasks for the device. Figure 4-62 lists the sub-menu under the **System Setup**. It consists of **Date/Time Settings**, **Admin Settings**, **Firmware Upgrade**, **Backup/Restore Configuration**, **Power Management**, and **Ping**. Each of this sub-menu will be described in the following subsections.

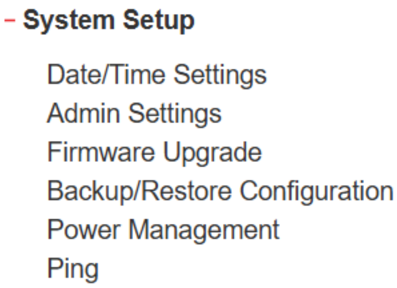
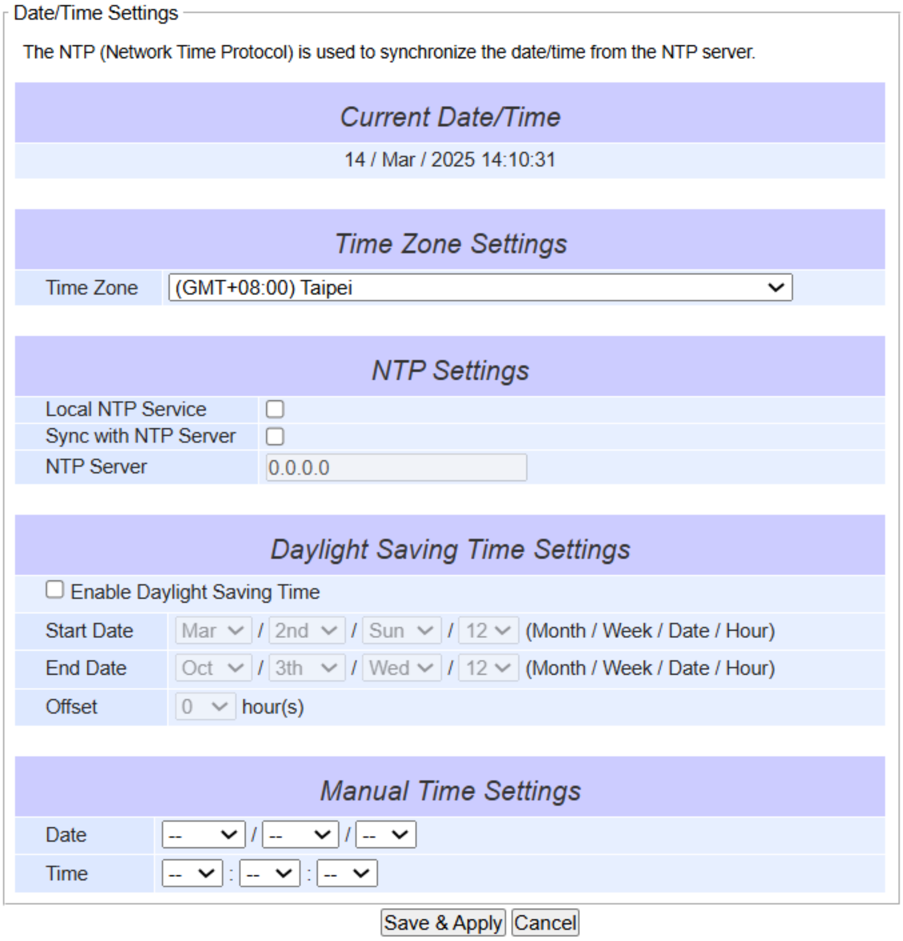


Figure 4-62 System Setup Menu

4.13.1 *Date/Time Settings*

Date and time can be set manually or using Network Time Protocol (NTP) to automatically synchronize date and time of PG5201B with a Time Server. Figure 4-63 shows the **Date/Time Settings** page. The first part of the page is the latest **Current Date/Time** which is in the format of **DD/Month/YYYY HH:MM:SS**. The second part of the page is the **Time Zone Settings**. You can select your local **Time Zone** from the drop-down list. The third part of the page is the **NTP Server Settings**. In this part, you can either enable the local NTP service inside PG5201B by checking the option **Local NTP Service** below **NTP Settings** part or automatically synchronize with a time server or NTP server. To enable automatic time synchronization, please check the box behind the **Sync with NTP Server** option. Then proceed to enter the **IP address** or **host name** for the **NTP Server**. Note that if a host name is entered, the DNS server must be configured properly (see detail in Section 4.5.1). The fourth part is the **Daylight Saving Time Settings** that can be enabled when **Enable Daylight Saving Time** box is checked. When it is enabled, the user can select the detailed setting of the daylight saving period, such as **Start Date** and **End Date** with **Offset**. Finally, the last part of the page is the **Manual Time Settings** where you can set **Date** and **Time** using corresponding drop-down lists in Figure 4-63.



Date/Time Settings

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

Current Date/Time

14 / Mar / 2025 14:10:31

Time Zone Settings

Time Zone	(GMT+08:00) Taipei

NTP Settings

Local NTP Service	□
Sync with NTP Server	□
NTP Server	0.0.0.0

Daylight Saving Time Settings

□ Enable Daylight Saving Time

Start Date	Mar / 2nd / Sun / 12 (Month / Week / Date / Hour)
End Date	Oct / 3th / Wed / 12 (Month / Week / Date / Hour)
Offset	0 hour(s)

Manual Time Settings

Date	-- / -- / --
Time	-- : -- : --

Figure 4-63 Date/Time Settings Web Page under System Setup

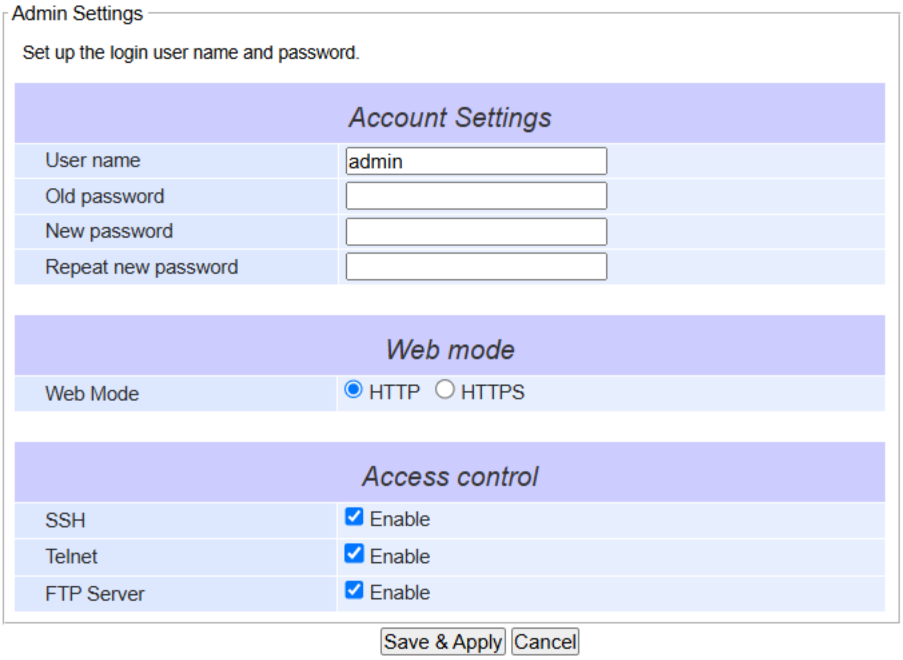
Attention

It is also important to setup Default Gateway and DNS Servers in the Network Settings properly (See Section 4.5.1), so PG5201B can lookup DNS names and point to the proper NTP server.

After finishing configuring the **Date/Time Settings**, please click on **Save & Apply** button to keep the change that you have made and to apply your setting. When the saving and applying are finished, the web browser will remain on the **Date/Time Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button.

4.13.2 *Admin Settings*

The PG5201B Series allows user and password management through this **Admin Settings** page under **System Setup** menu. By default, the User name is "**admin**" and the password is "**default**". To set or change their values, you can enter the information in the **User name**, the **Old password**, the **New password** and the **Repeat new password** fields under the **Account Settings** part as shown in Figure 4-64. The second part of the **Admin Settings** web page, there is the **Web mode** part which allow the user to select the radio button of normal **HTTP** or **HTTPS** for secure communication with the device's web user interface (Web UI). The thirt part of the web page allows the user to change the **Access Control** of three utilities: **SSH**, **Telnet**, and **FTP Server** by checking the corresponding **Enable** boxes.



Admin Settings

Set up the login user name and password.

Account Settings	
User name	admin
Old password	
New password	
Repeat new password	

Web mode	
Web Mode	● HTTP ○ HTTPS

Access control	
SSH	☑ Enable
Telnet	☑ Enable
FTP Server	☑ Enable

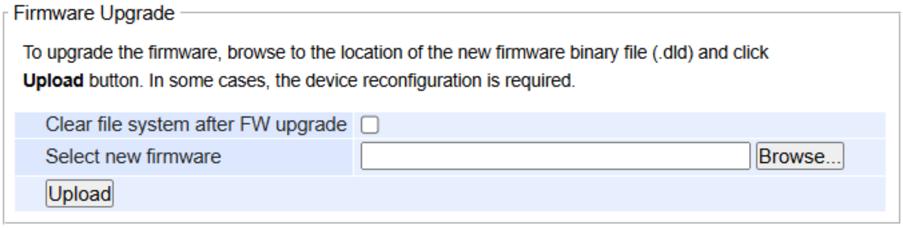
Figure 4-64 Admin Settings Web Page under System Setup

After finishing configuring the **Admin Settings**, please click on **Save & Apply** button to keep the change that you have made and to apply your setting. Another pop-up window will be displayed to re-authenticate the user to access the Web UI of PG5201B as shown in Figure 4-7. You must re-enter the username and the password to login to the PG5201B. When the saving, applying, and re-authentication are finished, the web browser will remain on the **Admin Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button.

4.13.3 *Firmware Upgrade*

Updated firmware for PG5201B is provided by Atop from time to time (for more information please visit Atop News & Events webpage) to fix bugs and optimize performance. It is very important that the device must **NOT be turned off or powered off during the firmware upgrading**, (**please be patient as this whole process might take up to 5 minutes**). Before upgrading the firmware, please make sure that the device has a reliable power source that will not be powered off or restarted during the firmware upgrading process.

To upgrade a new firmware to PG5201B, please downloaded the latest firmware for your PG5201B model from the download tab on the PG5201B product page or from the Download page under the Support link on Atop's main webpage. Then, copy the new firmware file to your local computer. Note that the firmware file is a binary file with ".dld" extension. Next, open the Web UI and select **Firmware Upgrade** page under the **System Setup** menu. Then, click "**Browse…**" button as shown in Figure 4-65 below to find and choose the new firmware file. Then, you can choose to tick the checkbox of "**Clear file system after FW upgrade**" if it's required to erase the user storage after firmware (FW) upgraded successfully, and click "**Upload**" button to start the firmware upgrade process. The program will show the upload status. Please wait until the uploading process is finished (the amount of time varies depending on the equipment used). Finally, the PG5201B device will then proceed to restart itself. In some cases, you might require to re-configure your PG5201B device. To restore your backup configuration from a file, please see the procedure in the next subsection.



Firmware Upgrade

To upgrade the firmware, browse to the location of the new firmware binary file (.dld) and click **Upload** button. In some cases, the device reconfiguration is required.

Clear file system after FW upgrade □

Select new firmware

Figure 4-65 Firmware Upgrade Web Page under System Setup

Note 1: If the checkbox of "**Clear file system after FW upgrade**" is enabled, the space of user storage will be erased after firmware upgraded successfully. The system would be restored to default settings, and the certifications will be re-generated after reboot.

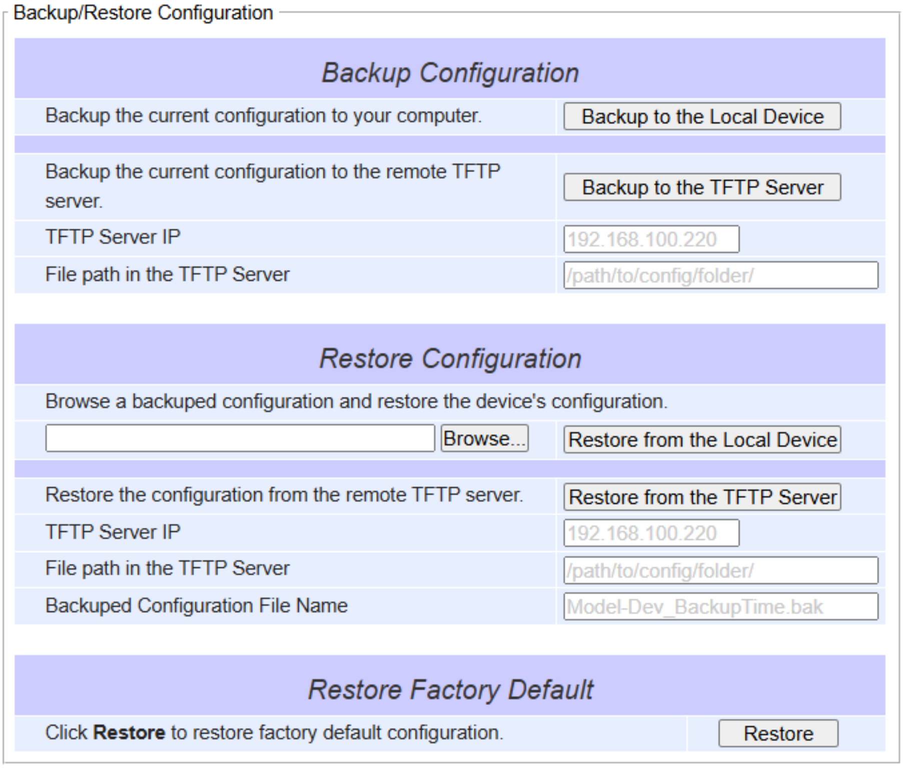
4.13.4 *Backup/Restore Configuration*

Once all the configurations are set and the device is working properly, the user should back up the current configuration of PG5201B. The backup configuration file can be used when the new firmware is uploaded and the device is reset to a factory default setting. This is done to prevent accidental loading of incompatible old settings. The backup configuration file could also be used to efficiently deploy multiple PG5201B Series devices of similar settings by uploading these settings to all devices.

To back up configuration, click "**Backup**" button under the **Backup Configuration** part as shown in Figure 4-66, and the backup file (ModelName-MACAddress.dat) will be automatically saved on your computer. It is important **NOT to manually modify the saved configuration file by any editor. Any modification to the file may corrupt the file and it may not be used for later restoration**. Please contact Atop's authorized distributors for more information on this subject.

To restore the backup configuration, click "**Browse**" button under the **Restore Configuration** part as shown in Figure 4-66 to locate the backup configuration file on user's computer. Then, click on "**Upload**" button to upload the backup configuration file to the device. Once the backup configuration file is successfully uploaded, the device will restart. Note that the time needed for this process may vary on the equipment used.

If you need to restore the PG5201B device to its factory default configuration, you can click on the **Restore** button under the **Restore Factory Default** section as shown in Figure 4-66.



Backup/Restore Configuration

Backup Configuration

Backup the current configuration to your computer.	Backup to the Local Device
Backup the current configuration to the remote TFTP server.	Backup to the TFTP Server
TFTP Server IP	192.168.100.220
File path in the TFTP Server	/path/to/config/folder/

Restore Configuration

Browse a backuped configuration and restore the device's configuration.

Browse...	Restore from the Local Device
Restore the configuration from the remote TFTP server.	Restore from the TFTP Server
TFTP Server IP	192.168.100.220
File path in the TFTP Server	/path/to/config/folder/
Backuped Configuration File Name	Model-Dev_BackupTime.bak

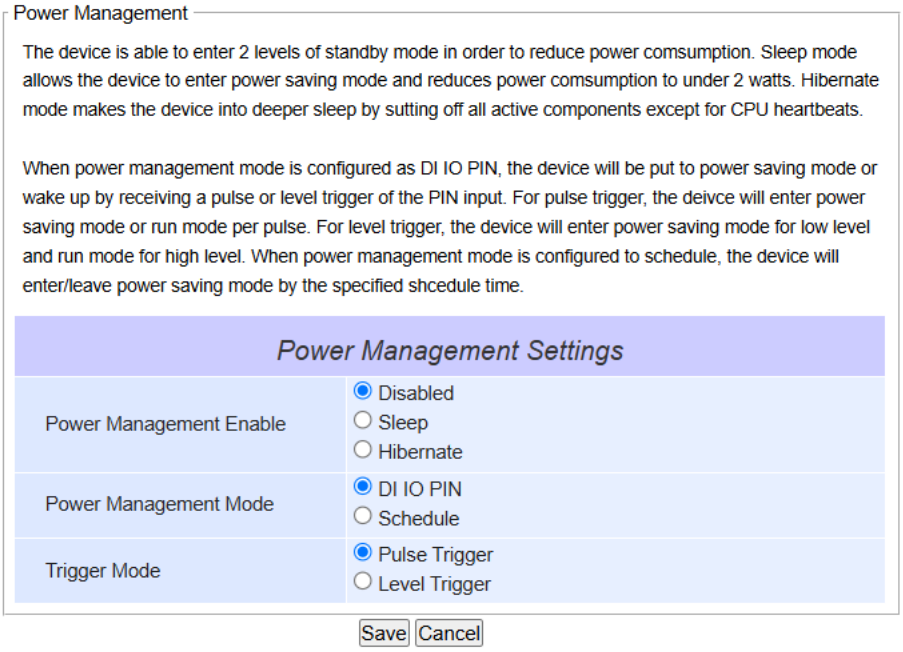
Restore Factory Default

Click **Restore** to restore factory default configuration.	Restore

Figure 4-66 Backup/Restore Settings Web Page under System Setup

4.13.5 *Power Management*

The PG5201B is able to enter two levels of standby mode to reduce power consumption when the PG5201B is idle. First, **Sleep** mode allows the PG5201B's CPU to enter power saving mode and effectively reduces the power consumption to less than 2 watts. While the cellular connection is still alive, the PG5201B can be woken up from sleep by DI control or by setting a regular schedule. Second, **Hibernate** mode puts the PG5201B into deeper sleep by shutting off all active components except for its CPU heartbeat. You can only wake the PG5201B from hibernation by using the schedule management function. shows the Power Management web page.



Power Management

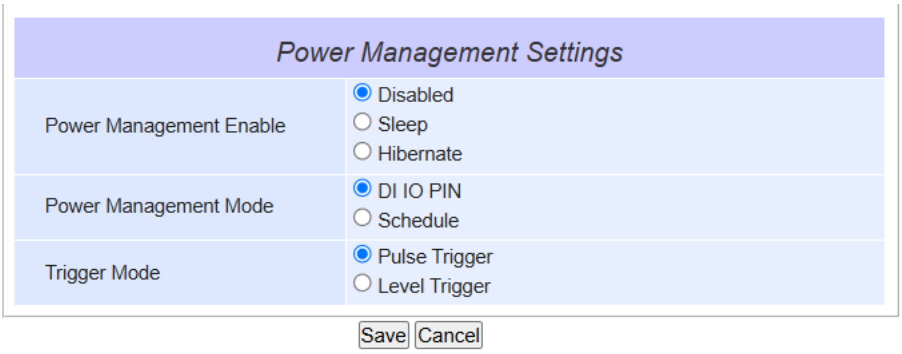
The device is able to enter 2 levels of standby mode in order to reduce power comsumption. Sleep mode allows the device to enter power saving mode and reduces power comsumption to under 2 watts. Hibernate mode makes the device into deeper sleep by sutting off all active components except for CPU heartbeats.

When power management mode is configured as DI IO PIN, the device will be put to power saving mode or wake up by receiving a pulse or level trigger of the PIN input. For pulse trigger, the deivce will enter power saving mode or run mode per pulse. For level trigger, the device will enter power saving mode for low level and run mode for high level. When power management mode is configured to schedule, the device will enter/leave power saving mode by the specified shcedule time.

Power Management Settings	
Power Management Enable	● Disabled ○ Sleep ○ Hibernate
Power Management Mode	● DI IO PIN ○ Schedule
Trigger Mode	● Pulse Trigger ○ Level Trigger

Figure 4-67 Power Management Web Page

When Power Management Mode option is configured as **DI IO PIN** (its radio button is selected), the device will be put to power saving mode or wake up by receiving a pulse or level trigger of the PIN input. When power management mode is configured to **Schedule** (its radio button is selected), the device will enter or leave power saving mode by specified schedule of day and time. When the Schedule option is selected, additional setting options are active as shown in Figure 4-68. Users can select the day of week and set the starting time (Enter Power Saving Mode Time) and stopping time (Leaving Power Saving Mode Time) with format of hours (HH) and minutes (MM).



Power Management Settings	
Power Management Enable	● Disabled ○ Sleep ○ Hibernate
Power Management Mode	● DI IO PIN ○ Schedule
Trigger Mode	● Pulse Trigger ○ Level Trigger

Figure 4-68 Options for Schedule Power Management Mode

There are two trigger modes that can be chosen by selecting corresponding radio button. For **Pulse trigger** mode, the device will enter power saving mode or run mode per pulse. For **Level trigger** mode, the device will enter power saving mode for low level and run mode for high level. Table 4.8 summarizes the description of each power management option.

Table 4.8 Description of Power Management Settings

Field Name	Description	Factory Default
Power Management Enable	**Disabled:** No power saving. **Sleep:** Power saving mode with power consumption under 2Watts. **Hibernate:** Deeper power saving mode with only CPU's heartbeat active.	Disabled
Power Management Mode	**DI IO PIN:** The power management mode is changed by triggering of signal through Digital Input/Output pin. **Schedule**: The power management mode is changed by the predefined schedule of day and time.	DI IO PIN
Trigger Mode	**Pulse Trigger:** The condition of signal that will change the power management mode is based on the pulse of signal. Need at least 100ms pulse from 4.3V to 36V. **Level Trigger:** The condition of signal that will change the power management mode is based on the level of signal. If the voltage of the signal is lower than 2.5V for at least 10 seconds, then PG5201B will enter the sleep or hibernate mode. If the voltage of the signal is higher than 4.3V for at least 3 seconds, then PG5201B will wake up.	Pulse Trigger

Example of Entering Hibernate Mode through DI pin in Pulse Trigger Mode

Figure 4-69 shows an example of how to create a trigger to entering the Hibernate mode. Users can wire DI and DIc pins to the two pins of the switch breaker as shown in the figure. While the device (PG5201B) is in ready state, users can switch the breaker to “I” first then to “O”. Alternatively, users can short circuit between the DI and the SG pins for at least 100ms then open circuit between the DI and the SG pins. This will cause the device to enter Hibernate mode. During the Hibernate mode, all of the LEDs in the front panel will turn off except the power LED as shonw in Figure 4-70.

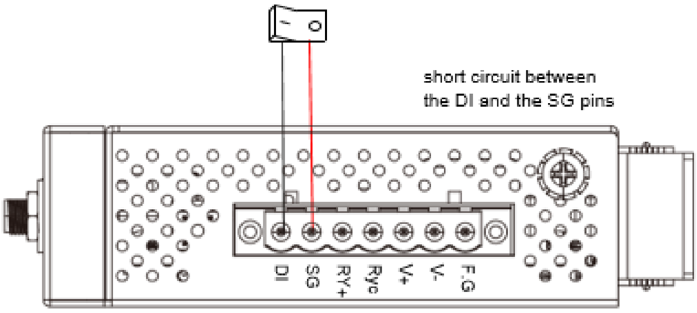


Figure 4-69 Example of Connecting a Switch Breaker between DI and DIc Pins on the PG5201B

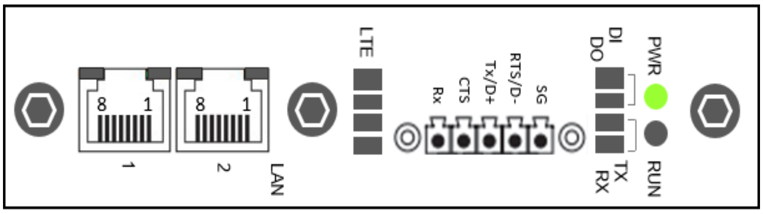


Figure 4-70 Example of LED status while device is in the Hibernate mode

Example of Leaving Hibernate Mode or Wake Up through DI pin in Pulse Trigger Mode

To wake up from Hibernate mode in pulse trigger mode with the same setup in Figure 4-69, users can switch the breaker to “I” then to “O” again. The device (PG5201B) will wake up as shown in Figure 4-71.

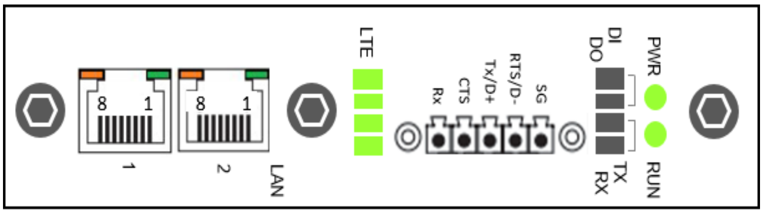


Figure 4-71 Example of Device in Wake Up State.

Example of Entering Hibernate Mode through Power Saving Button in Pulse Trigger Mode

The device (PG5201B) can be put into Hibernate mode by pressing the Power Saving Button on the side of the chasis. Figure 4-72 shows the location of the Power Saving or Hibernate button. By pressing this Power Saving or Hibernate button for at least 100 ms while the system is in ready state, the device will enter the Hibernate mode.

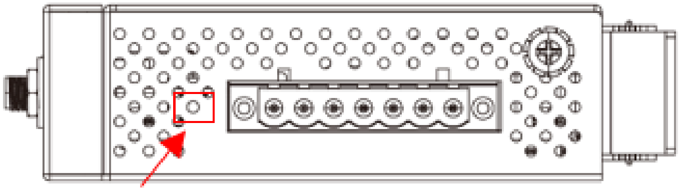


Figure 4-72 Location of the Hibernate button on the side of the chassis

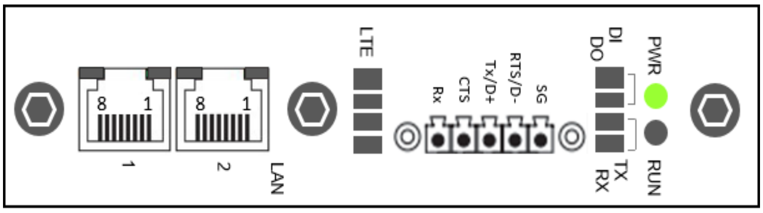


Figure 4-73 Example of LED status while device is in the Hibernate mode

Example of Leaving Hibernate Mode or Wake up through Power Saving Button in Pulse Trigger Mode

To leave the Hibernate mode or wake up, users can press the Power Saving/Hibernate button for at least 100ms while the device is in Hibernate mode. The device will wake up as shown in Figure 4-74.

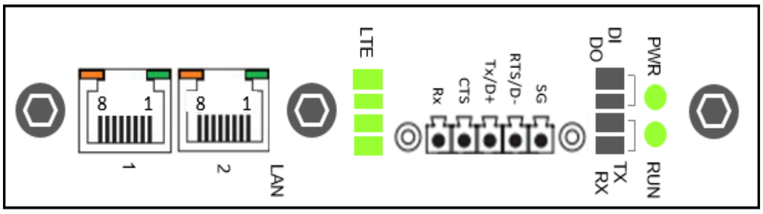
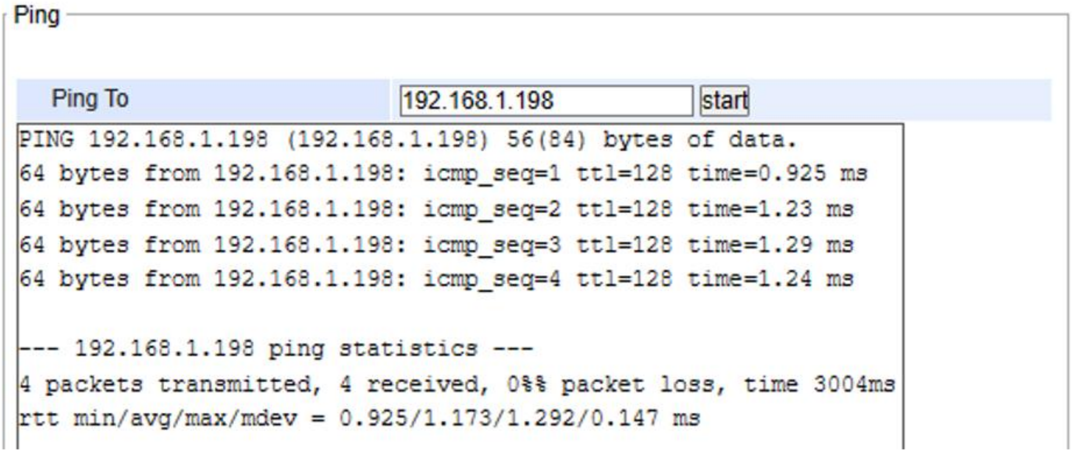


Figure 4-74 Example of Device in Wake Up State

4.13.6 *Ping*

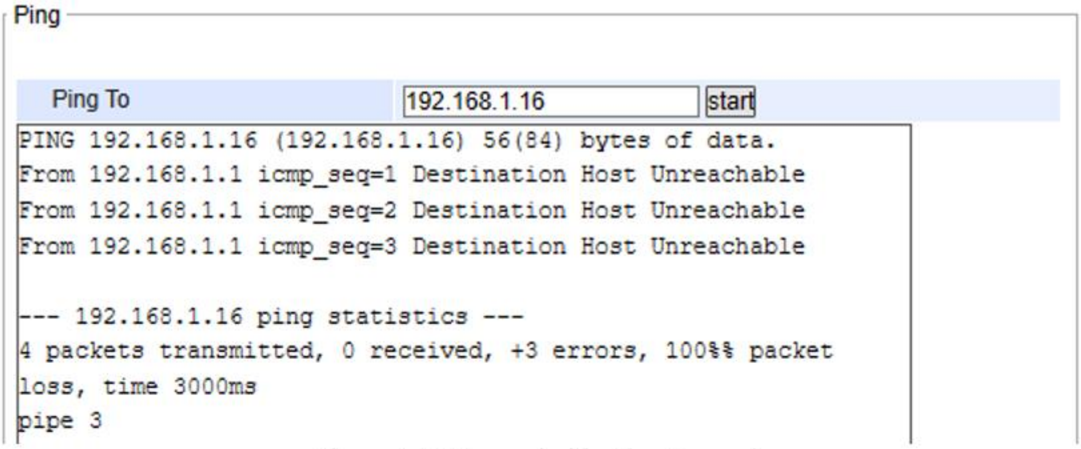
The Web UI of PG5201B has an interface to call **Ping** which is a network diagnostic utility for testing reachability. You can use the **Ping** function to determine whether PG5201B can reach the gateway or other devices in the network. To use the **Ping**, enter a destination IP address in the text box behind the **Ping To** and click **Start** button as shown in Figure 4-75. This process usually takes around 20 seconds. Figure 4-75 represents a successful ping without packet loss from PG5201B to the address 10.0.50.101 and back, while Figure 4-76 indicates that the connecting device at the address 10.0.50.202 is unreachable in which no packets have returned from the transmitted ping packets.



Ping To: 192.168.1.198

```
PING 192.168.1.198 (192.168.1.198) 56(84) bytes of data.
64 bytes from 192.168.1.198: icmp_seq=1 ttl=128 time=0.925 ms
64 bytes from 192.168.1.198: icmp_seq=2 ttl=128 time=1.23 ms
64 bytes from 192.168.1.198: icmp_seq=3 ttl=128 time=1.29 ms
64 bytes from 192.168.1.198: icmp_seq=4 ttl=128 time=1.24 ms

--- 192.168.1.198 ping statistics ---
4 packets transmitted, 4 received, 0%% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.925/1.173/1.292/0.147 ms
```

Figure 4-75 Ping Web Page under System Setup



Ping To: 192.168.1.16

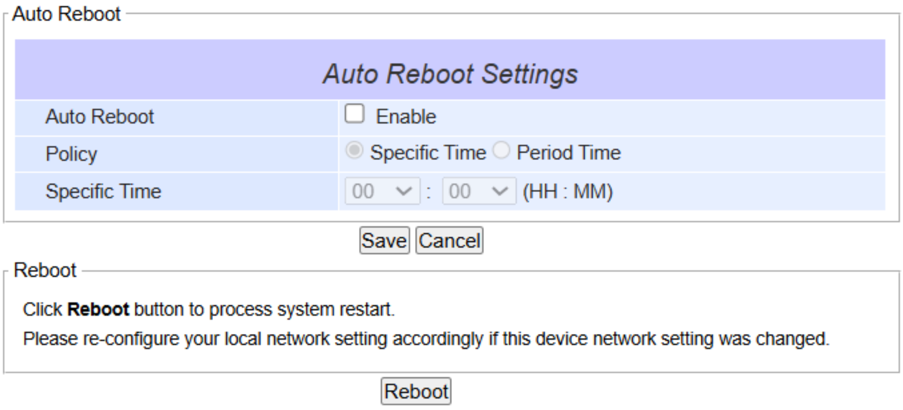
```
PING 192.168.1.16 (192.168.1.16) 56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable

--- 192.168.1.16 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100%% packet
loss, time 3000ms
pipe 3
```

Figure 4-76 Unreachable Ping Example

4.14 *Reboot*

4.14.1 *Auto Reboot*

PG5201B can be configured for automatic rebooting or **Auto Reboot** under the **Reboot** menu. To enable the **Auto Reboot** option, select the **Reboot** menu and under the **Auto Reboot Settings** check **Enable** box as shown in Figure 4-77. There are two auto reboot policies: **Specific Time** or **Period Time**. When **Specific Time Policy** is selected, the **Specific Time** option is active for setting the hour (**HH**) and minute (**MM**) that the device will be reboot. When **Period Time Policy** is selected, the device will be rebooted every period of hour(s) which can be selected from a drop-down list. After you finished setting, click on the **Save** button at the bottom of the **Auto Reboot** section or click **Cancel** button to discard any settings.



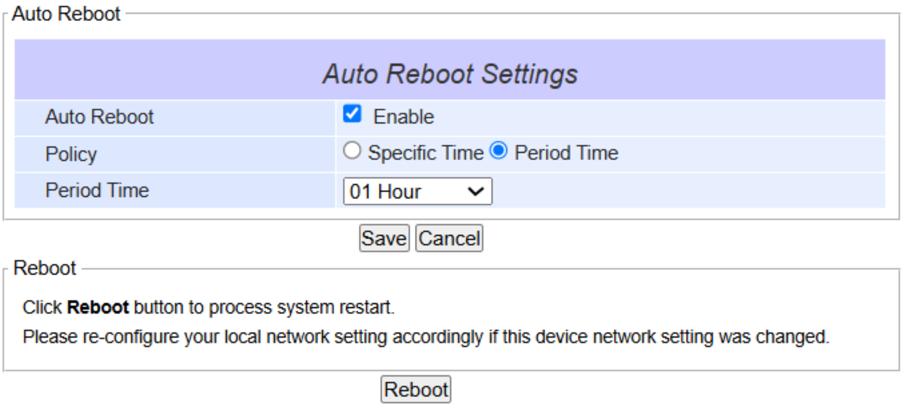
Auto Reboot

Auto Reboot Settings	
Auto Reboot	□ Enable
Policy	● Specific Time ○ Period Time
Specific Time	00 : 00 (HH : MM)

Reboot

Click **Reboot** button to process system restart.
Please re-configure your local network setting accordingly if this device network setting was changed.

Figure 4-77 Reboot Web Page with Specific Time Policy



Auto Reboot

Auto Reboot Settings	
Auto Reboot	☑ Enable
Policy	○ Specific Time ● Period Time
Period Time	01 Hour

Reboot

Click **Reboot** button to process system restart.
Please re-configure your local network setting accordingly if this device network setting was changed.

Figure 4-78 Reboot Web Page with Period Time Policy

4.14.2 *Manual Reboot*

To manually reboot the PG5201B device, click on the "**Reboot**" button at the end of the **Reboot** page as shown in Figure 4-77. The device will then restart. When the rebooting process is finished, you will hear the beep sound twice from the device and you might need to refresh your web browser to log into the web interface of the PG5201B again.

5 Specifications

5.1 *Hardware*

Table 5.1 Hardware Specification

System	
CPU	Nuvoton NUC980, Arm926EJ-S, 300MHz
Flash Memory	32MB
RAM	PG5201B DDR2 64MB
EEPROM	8 KB
Reset	Built-in Recessed Key (Restore to Factory Defaults)
Watchdog	Hardware built-in
Network	
Ethernet Interface	2x 10/100 BaseT(X) ports with RJ-45 connectors
Serial	
Serial Interface	RS-232/RS-485 Software Selectable (Default: RS-232)
Serial Connector	Connector Type • PG5201B – 1 Serial Port (TB-5 or DB-9)
Protection	PG5201B (1.5Kv isolation)
Serial Port Communication	Baud-rate: 1200 ~ 230400 bps Parity: None, Even, Odd, Mark, or Space Data Bits: 5, 6, 7, 8 Stop Bits: 1, 2 Software Selectable Flow Control: RTS/CTS (RS-232 only), XON/XOFF, None
LED Indicator	
LED indication	Power x 1 RUN x 1 LAN: 2x Orange/Yellow LED, 2x Green LED COM port: PG5201B-C1/PG5201B-M1: 1x TX- LED, 1x RX-LED
DIO	1x DI LED, 1x DO LED,
Power Requirement & EMC	
Input	DC Power: 9 ~ 48VDC (±10%)
Consumption	Max. < 8W (TBD, wait for HW update) Min. < 100mW (@12VDC)
Mechanical	
Dimensions (W x H x D, mm)	136 x 95 x 30
Enclosure	IP30 protection, metal housing
Environmental	
Temperature	Operations -30°C ~ +75°C Storage -40°C ~ +85°C
Relative Humidity	5 ~ 95%RH, (non-condensing)

5.2 *Serial port Pin Assignments*

5.2.1 *PG5201B Pin Assignments for Serial Interfaces*

DB9 to RS-232 /RS-485 connectors

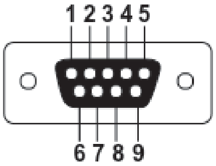


Figure 5-1 DB9 Pin Number

Table 5.2 PG5201B Pin Assignment for DB9 to RS-232 /RS-485 Connector

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

5-pin (Male Terminal Block) for RS-232/RS485 Connector

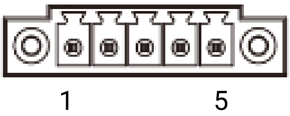


Figure 5-2 TB5 Pin Number

Table 5.3 PG5201B Pin Assignment for TB5 to RS-232/ RS-485 Connector

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

5.2.2 *PG5201B Pin Assignments for Terminal Block*

7-pin 45.72mm lockable Terminal Block

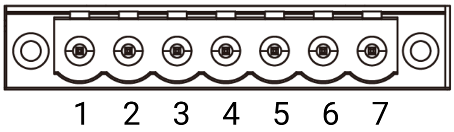


Figure 5-3 PG5201B Pin Assignments for Terminal Block

Table 5.4 PG5201B Power Connector& DIO

Pin#	Description
1	DI
2	COM
3	NC
4	NC
5	V+
6	V-
7	F.G.

5.3 *LED Indicators*

Table 5.6 Color Interpretation of LED Indicators of PG5201B

Name	Colour	Status	Message
PWR (Power)	🟢 Green	Steady/On	Power On and Power is being supplied
		Off	Power Off and
TX	🟢 Green	Blinking	COM port is transmitting data
		Off	COM port is not transmitting data
RX	🟢 Green	Blinking	COM port is receiving data
		Off	COM port is not receiving data
		Off	COM port is not receiving data
DIO	🟢 Green	On	Activated
		Off	Deactivated
RUN	🟢 Green	Blinking	AP Firmware is running normally
		On/Off	System is not ready or halt
LAN	🟠 Orange (Speed)	Solid: Link is established	Solid: Link is established Blink: Transmission (Tx/Rx events) is activated
		Off	Deactivated or no transmission data
	🟢 Green (Data)	On	Ethernet is transmitting at 100 Mbps
		Off	Ethernet is transmitting at 10 Mbps
LTE Signal Strength	🟢 Green	On	0-LED on (■■■■) No signal (RSSI <= -95dBm) 1-LED on (🟩■■■) Poor (-95dBm > RSSI <= -80dBm) 2-LED on (🟩🟩■■) Fair (-80dBm > RSSI <= -75dBm) 3-LED on (🟩🟩🟩■) Good (-75dBm > RSSI <= -65dBm) 4-LED on (🟩🟩🟩🟩) Excellent (RSSI > -65dBm)

5.4 *Software*

Table 5.7 Software Tools and Utilities

Software	
Configuration Tool	■ Web console ■ SSH console ■ Telnet console ■ **Network Management Utility©** ■ **eNode Designer©**

6 Warranty

Limited Warranty Conditions

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

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

RMA and Shipping Reimbursement

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

Limited Liability

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

Warranty

Atop Technologies Inc. provides a 5-year maximum warranty for Low-Power Gateway products.

Atop Technologies, Inc.

www.atoponline.com

Technical Support

www.atoponline.com/request-support

Contact Information

www.atoponline.com/contact-us/