TCPlink

www.tcplink.com

TCPlink, Inc.

PS4000/8000/16000 Series
Industrial Device Server Series

User Manual

V1.0

November 6th, 2018

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:

TCPlink, Inc.

Important Announcement

Disclaimer

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

Documentation Control

Author:	Saowanee Saewong
Revision:	1.0
Revision History:	
Creation Date:	6 November 2018
Last Revision Date:	6 November 2018
Product Reference:	PS4000/8000/16000 Industrial Device Server Series User Manual
Document Status:	Initial Release

Table of Contents

Table of Figures

List of Tables

1 Preface

1.1 *Purpose of the Manual*

This manual supports the user during the installation and configuring of the PS4000/8000/16000 Industrial Device Server Series. It explains the technical features available with the mentioned product. As such, it contains some advanced network management knowledge, instructions, examples, guidelines and general theories designed to help users manage this device and its corresponding software. A background in general theory is necessary when reading it. Please refer to the Glossary for technical terms and abbreviations (if any).

1.2 *Who Should Use This User Manual*

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

1.3 *Supported Platform*

This manual is designed for **PS4000/8000/16000 Industrial Serial Device Server Series** and that series only**.**

1.4 *Manufacturers' FCC Declaration of Conformity Statement*

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

This device complies with Part 15 of the FCC Rules.

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

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

2 Introduction

2.1 Overview

The PS4000/8000/16000 is an industrial Ethernet serial device server which acts as a gateway for communications between Ethernet (TCP/UDP) port and RS-232/RS-422/RS-485 port. The information conveyed by the PS4000/8000/16000 model is transparent to both host computers (Ethernet) and serial devices (RS-232/RS-422/RS-485). Data coming from the Ethernet port is sent to the designated RS-232/RS-422/RS-485 port, and data received from RS-232/RS-422/RS-485 port is sent to the Ethernet port, allowing full-duplex and bi-directional communication. In the computer-aided manufacturing or industrial automation areas, field devices can directly connect to an Ethernet network via the PS4000/8000/16000 model. In normal PCs or laptops, a virtual COM port can be created using our vitual COM software to fetch serial data from PS4000/8000/16000 remotely over Ethernet.

With the PS4000/8000/16000 model, it is possible to communicate with a remote serial device over the LAN or even over the Internet, which dramatically increases reachability and scalability.

Figure 2.1 illustrates an example of multiple devices connected to the Industrial Serial Device Server. A PC connects to the Industrial Serial Device Server via Ethernet interface, and a monitored device reports to Industrial Serial Device Server via RS-232/RS-422/RS-485 interface. It is possible to have multiple PCs connected into the same Industrial Serial Device Server through TCP or UDP transport protocols, as well as multiple monitored devices connected via RS-232/RS-422/RS-485 to Industrial Serial Device Server.

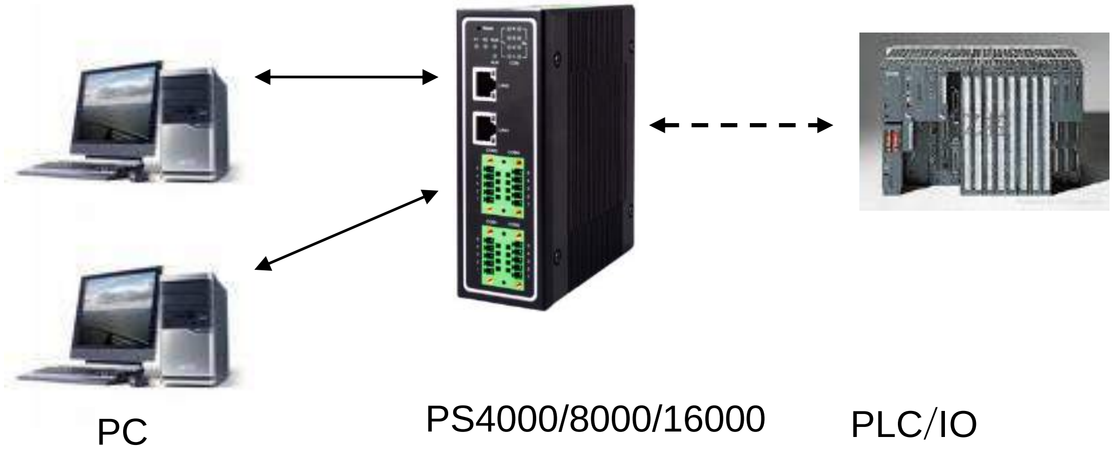


Figure 2.1 An Application of PS4000/8000/16000 Industrial Serial Device Server with Multiple Devices

2.2 Features

The PS4000/8000/16000 Industrial Serial Device Server Series share the same software platform on different available hardwares. It provides

- Flexible hardware platform, in different port variants based on Your needs
- TCP Server/Client, UDP, Virtual COM and Tunneling modes supported
- Remotely monitor, manage, and control industrial field devices
- Configuration via Web Browser/ Serial Console/ Telnet Console/ TCPlink'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 following items.

Table 3.1 Packing List

Item	Quantity	Description
PS4000/8000/16000	1	Industrial Serial Device Server
Mounting Kit	1	On PS8000 / PS16000 • Rack Mounting Type-L angles (x 2) • Screws (x 6) On PS4000 - DIN Rail Kit
Terminal Block		Power Supply/ Relay output: TB7 x1: 7-pin 5.08mm lockable Terminal Block (PS4000)
Documentation	1	Hardware Installation Guide (Warranty card is included)

Note:

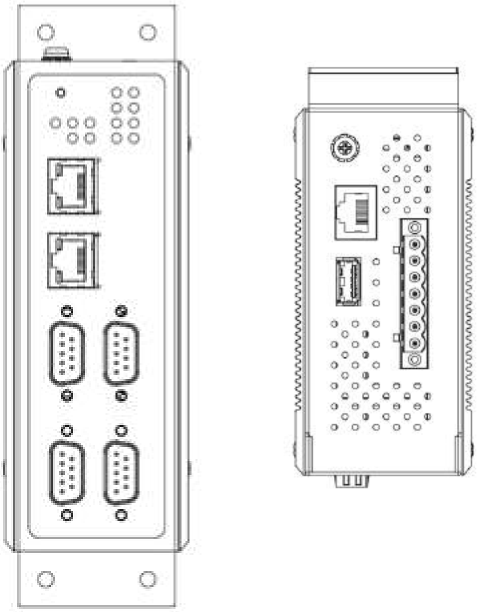
- Notify your sales representative immediately if any of the above items is missing or damaged upon delivery.
- TCPlink's utility software Device View© and Serial Manager© are obsolete and replaced by Device Management Utility® .

3.2 *Appearance, Front and Rear Panels*

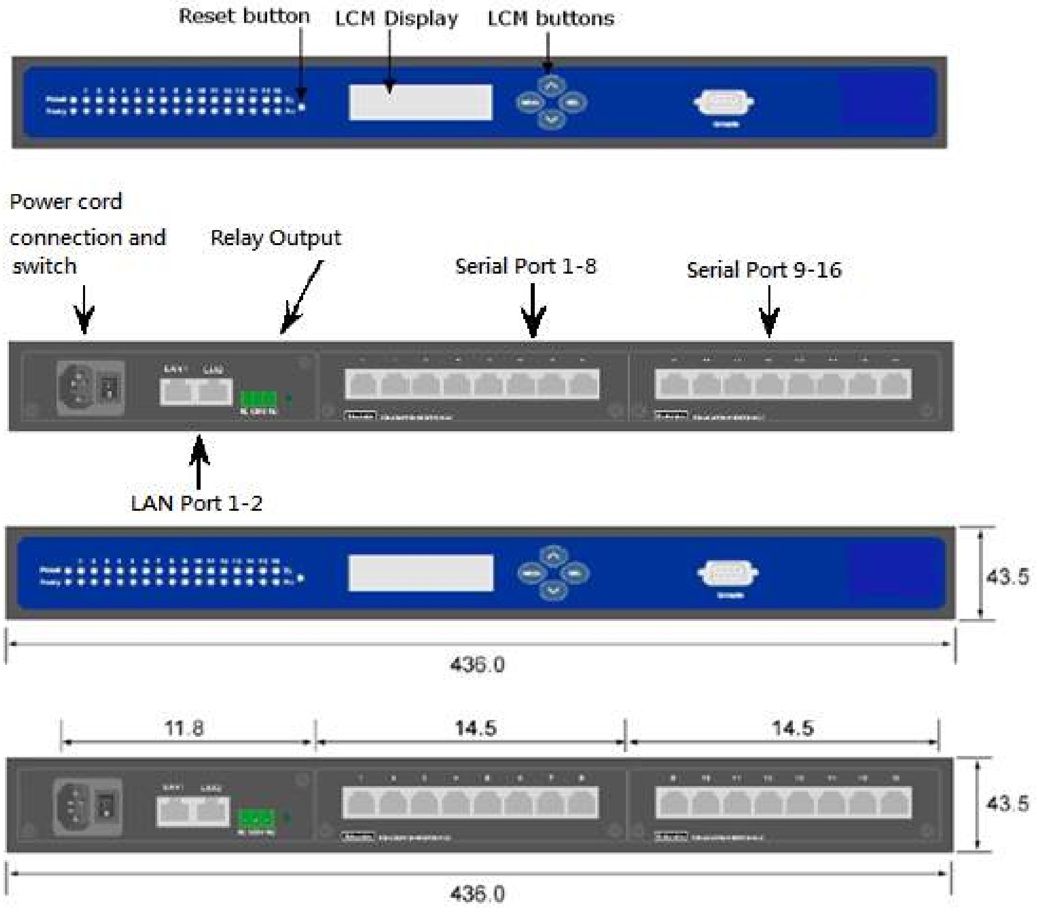
The following figures show particular PS4000/8000/16000 series device's front and rear panels.

PS4000

RJ45 DB9 Type



PS4000 / 16000



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. TCPlink will not be liable for any damages to property or personal injuries resulting from the installation or overall use of the device. Do not attempt to manipulate the product in any way if unsure of the steps described there. In such cases, please contact your dealer immediately.

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

3.4 *Factory Default Settings*

3.4.1 *Network Default Settings*

The PS4000/8000/16000 Industrial Serial Device Server is equipped with two LAN interfaces with two default IP addresses. Its default network parameters are listed in Table 3.2.

Table 3.2 Network Default Setting

Interface	Device IP	Subnet Mask	Gateway IP	DNS
LAN1	10.0.50.100	255.255.0.0	10.0.0.254	255.255.255.255
LAN2	192.168.1.1	255.255.255.0	192.168.1.254	

3.4.2 *Other Default Settings*

The PS4000/8000/16000 Industrial Serial Device Server comes with the following default settings.

Table 3.3 Security , Serial, and SNMP Default Settings

Parameter	Default Values
Security	
User Name	admin
Password	admin
Serial	
COM1	RS-232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM2	RS-232, 9600 bps, 8 data bits, No Parity bit, 1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM3	RS-232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM4	RS-232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
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

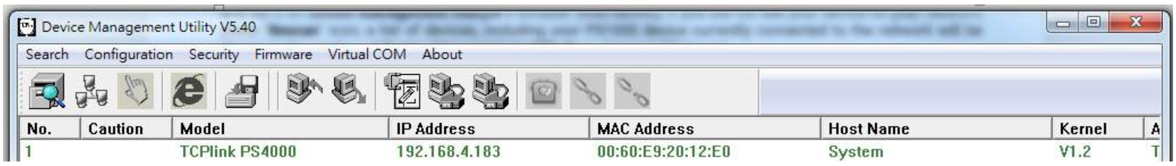
Note: Press the “Reset” button on the front panel for 5 seconds or follow the procedure in Section 4.16, to restore the PS4000/8000/16000 Series Industrial Serial Device Server to the factory default settings.

4 Configuration and Setup

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

4.1 *Configuration of Network Parameters through Device Management Utility*

Please install TCPlink's configuration utility program called **Device Management Utility®** that comes with the Product CD or can be downloaded from our websites (www.tcplink.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 PS4000/8000/16000 Industrial Serial Device Server 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 PS4000/8000/16000 device and list it on **Device Management Utility®**'s window. Alternatively, if you did not see your PS4000/8000/16000 device on your network, press "**Rescan**" icon, a list of devices, including your PS4000/8000/16000 device currently connected to the network will be shown in the window of **Device Management Utility®** as shown in Figure 4.1.

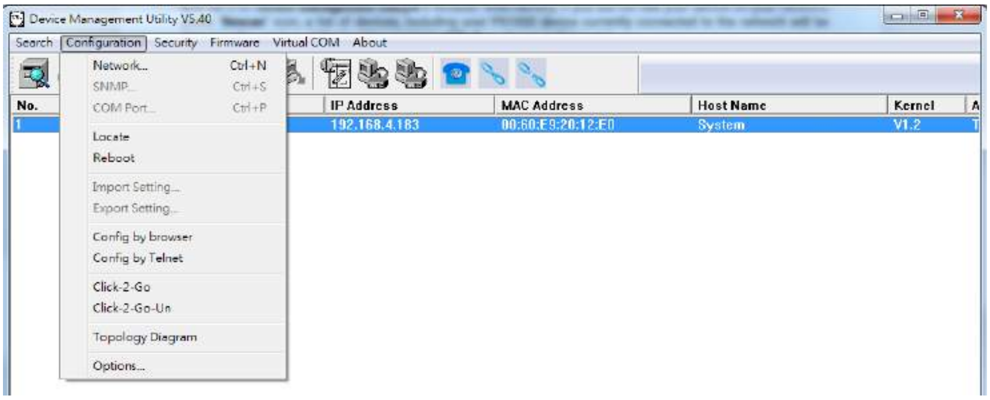


No.	Caution	Model	IP Address	MAC Address	Host Name	Kernel	A
1		TCPlink PS4000	192.168.4.183	00:60:E9:20:12:E0	System	V1.2	T

Figure 4.1 List of Device in Device Management Utility

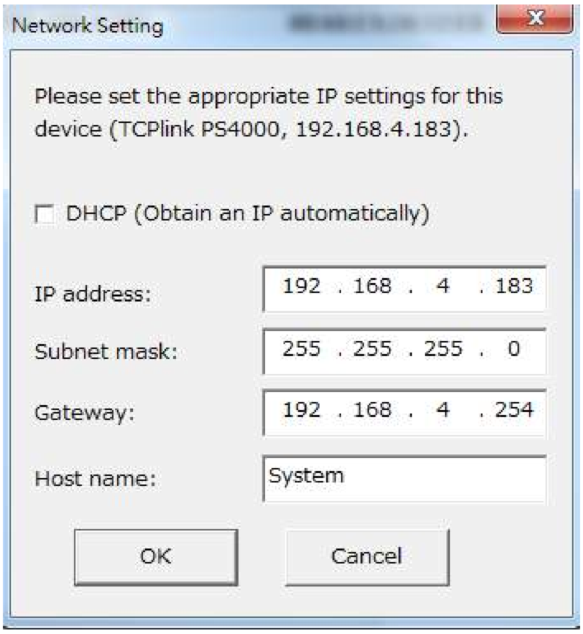
Note: This figure is for illustration purpose only. Actual values/settings may vary between devices.

Sometime the PS4000/8000/16000 device might not be in the same subnet as your PC; therefore, you will have to use TCPlink's utility to locate it in your virtual environment. To configure each device, first click to select the desired PS4000/8000/16000 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.



No.	IP Address	MAC Address	Host Name	Kernel	A
1	192.168.4.183	00:60:E9:20:12:E0	System	V1.2	T

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



Network Setting

Please set the appropriate IP settings for this device (TCPlink PS4000, 192.168.4.183).

□ DHCP (Obtain an IP automatically)

IP address: 192 . 168 . 4 . 183

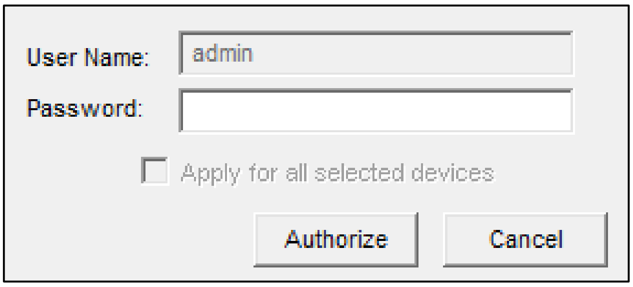
Subnet mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 4 . 254

Host name: System

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 “**admin**”. 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 PS4000/8000/16000 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, you may encounter another notification window as shown in Figure 4.6.

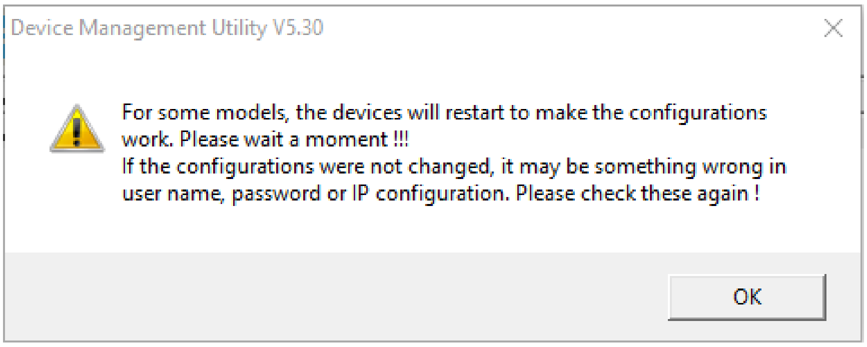


User Name: admin

Password:

□ Apply for all selected devices

Figure 4.4 Authorization for Change of Network Settings

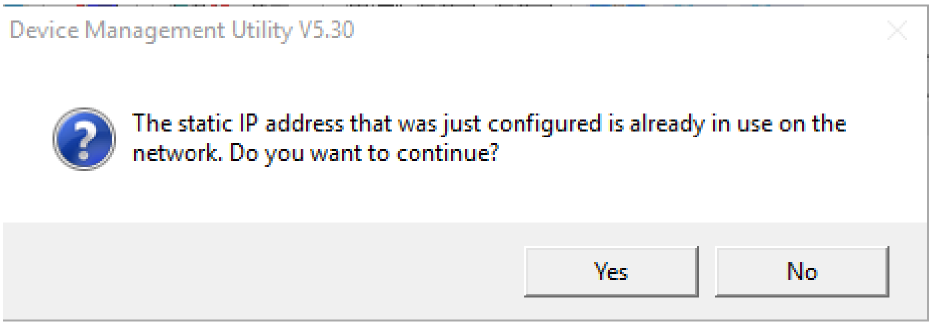


Device Management Utility V5.30

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.



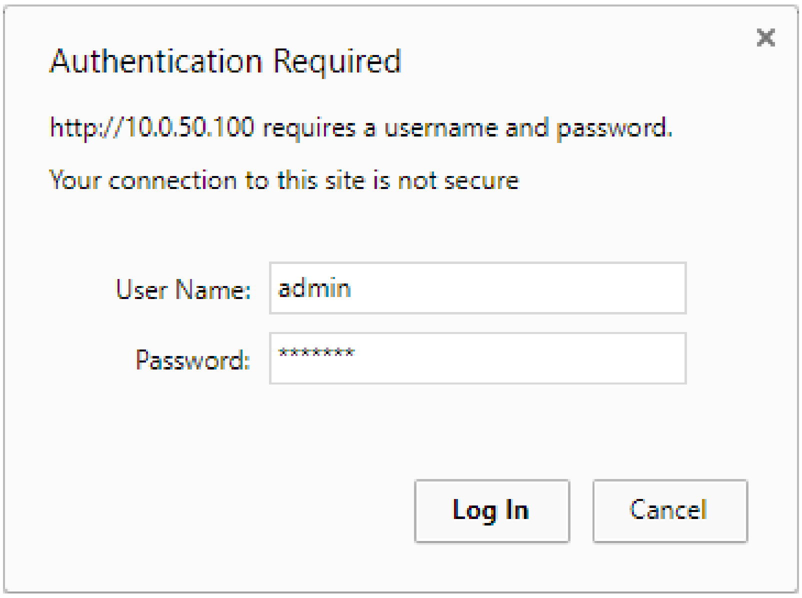
Device Management Utility V5.30

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/CLI Interface*

Every PS4000/8000/16000 Industrial Serial Device Server is equipped with a built-in web server in the firmware. Therefore, the device can be accessed by using a web browser for configuring by entering the device's IP address (default IP address is 10.0.50.100) in the URL field of your web browser. An authentication will be required and you will have to enter the username (Default value is "admin") and password (Default value is "admin") for accessing the web interface as shown in Figure 4.7. Note that you may encounter a warning pop-up window that urges you to change or reset your password to be different from the default value as shown in Figure 4.8. Figure 4.9 illustrates the overview page of the web interface. Figure 4.10 lists all the menus and submenus for web configuration. Please see Section 3.4 for default values. Note that the figures are captured from PS4000/8000/16000 series but the overview page for PS4000/8000/16000 series are the same.



Authentication Required

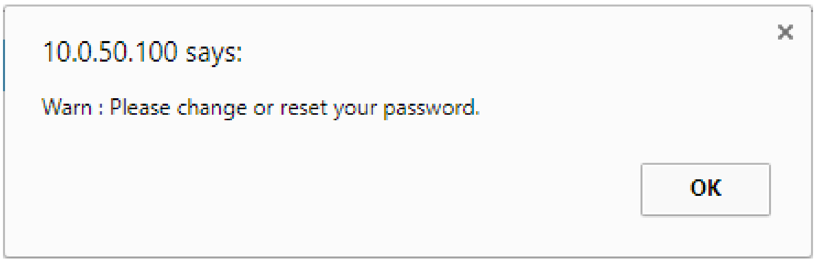
http://10.0.50.100 requires a username and password.

Your connection to this site is not secure

User Name: admin

Password: *******

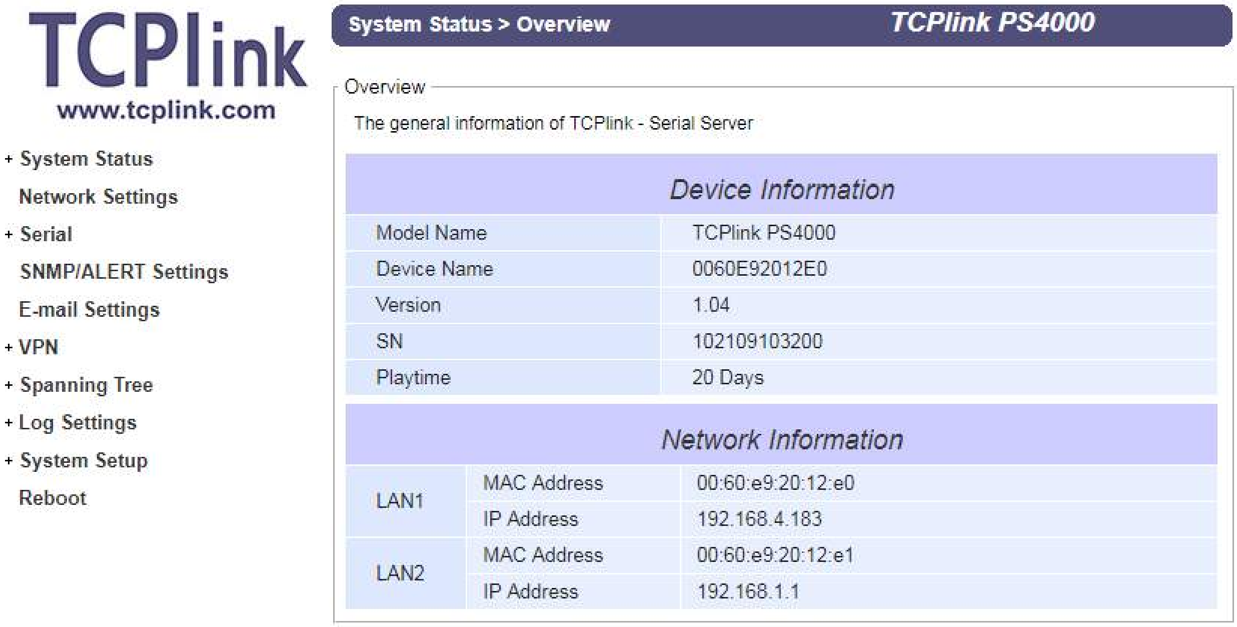
Figure 4.7 Authentication Required for Accessing Web Interface



10.0.50.100 says:

Warn : Please change or reset your password.

Figure 4.8 Warning Pop-up Window for Changing or Resetting Password from Default Value



Overview

The general information of TCPlink - Serial Server

Device Information	
Model Name	TCPlink PS4000
Device Name	0060E92012E0
Version	1.04
SN	102109103200
Playtime	20 Days

Network Information		
LAN1	MAC Address	00:60:e9:20:12:e0
	IP Address	192.168.4.183
LAN2	MAC Address	00:60:e9:20:12:e1
	IP Address	192.168.1.1

Figure 4.9 Overview Web Page (example on PS4000).

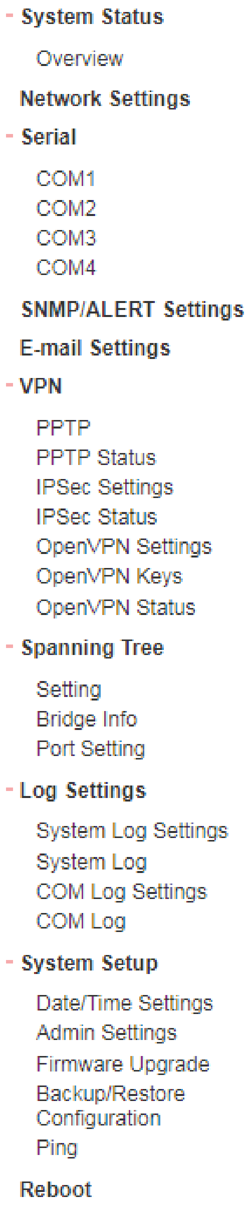
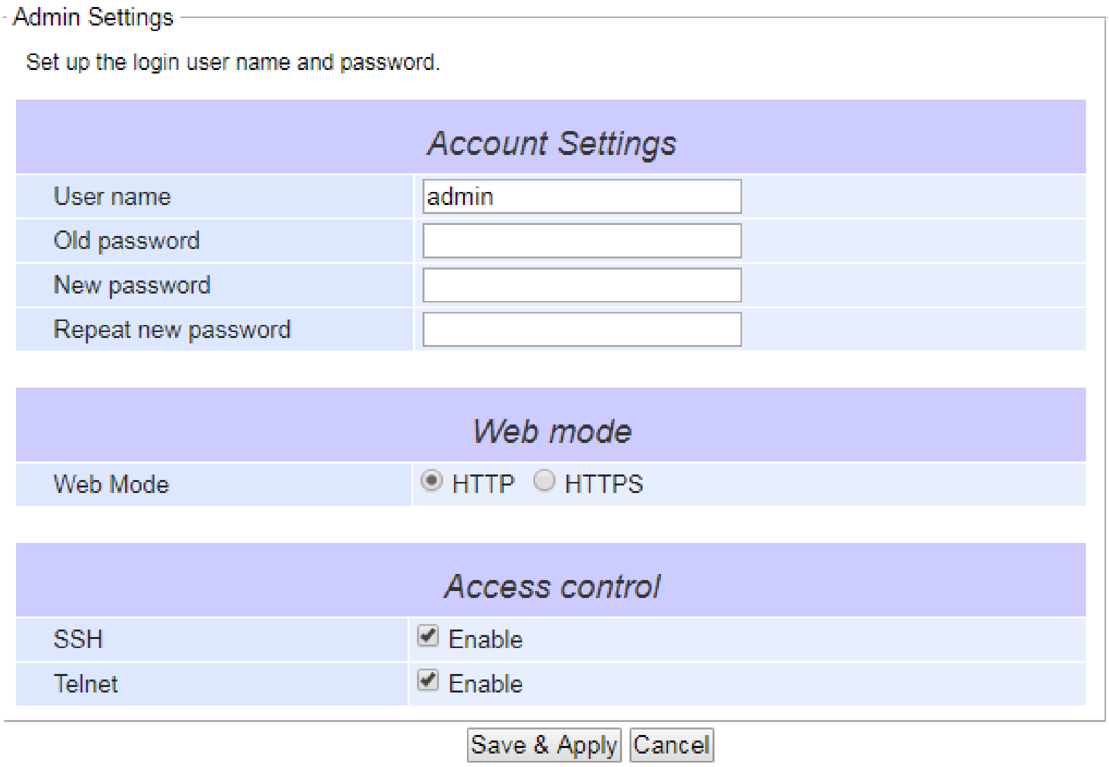


Figure 4.10 Map of Configuring Web Page (ex. on PS4000)

This approach (web interface) for configuring your device is the most user-friendly. It is the most recommended and the most common method used for PS4000/8000/16000 Industrial Serial Device Server Series. Please go to its corresponding section for a detailed explanation.

Furthermore, you can also use CLI interface through Consol port/Telnet/SSH to configure PS4000/8000/16000. Enable the Access Control (please refer to System Setup > Admin Settings), then you can use CLI interface.



Admin Settings

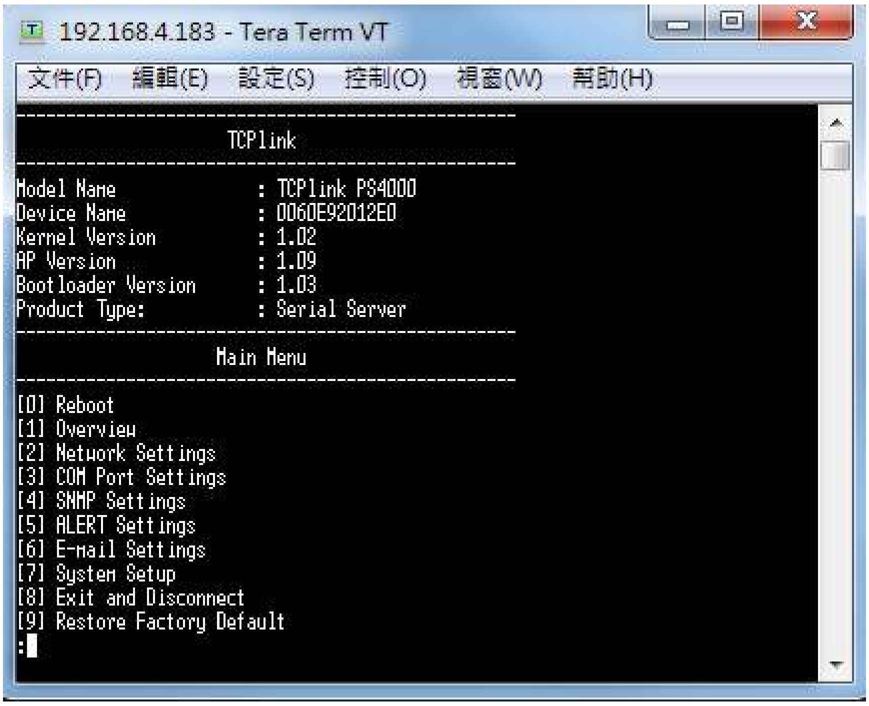
Set up the login user name and password.

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

Web mode	
Web Mode	● HTTP ○ HTTPS

Access control	
SSH	☑ Enable
Telnet	☑ Enable

Figure 4.11 Access control



192.168.4.183 - Tera Term VT
文件(F) 編輯(E) 設定(S) 控制(O) 視窗(W) 幫助(H)

```
--------------------------------------------------
                    TCPlink
--------------------------------------------------
Model Name               : TCPlink PS4000
Device Name              : 0060E92012E0
Kernel Version           : 1.02
AP Version               : 1.09
Bootloader Version       : 1.03
Product Type:            : Serial Server
--------------------------------------------------
                   Main Menu
--------------------------------------------------
[0] Reboot
[1] Overview
[2] Network Settings
[3] COM Port Settings
[4] SNMP Settings
[5] ALERT Settings
[6] E-mail Settings
[7] System Setup
[8] Exit and Disconnect
[9] Restore Factory Default
:
```

Figure 4.12 CLI interface

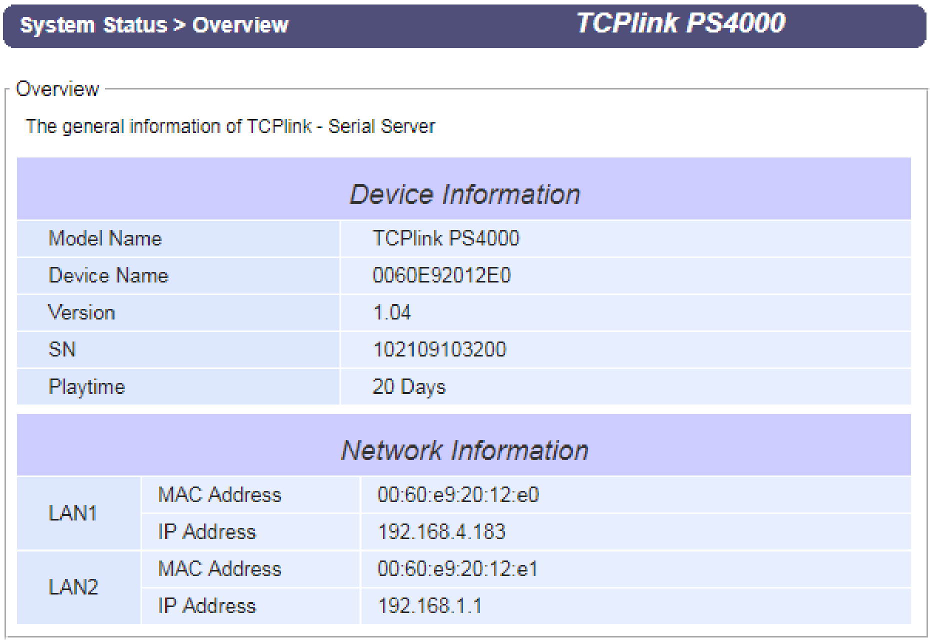
Please noted that change IP address need to restart PS4000/8000/16000.

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 TCPlink's **Device Management Utility©** and then restart the device. Once restarted, the IP address will be configured automatically.

4.4 *Web Overview*

In this section, current information on the device's status and settings will be displayed. An example of PS4000/8000/16000's overview page is shown in Figure 4.13. Note that the figures are captured from MB59XX series but the overview page for PS4000/8000/16000 series are the same.



System Status > Overview TCPlink PS4000

Overview

The general information of TCPlink - Serial Server

Device Information	
Model Name	TCPlink PS4000
Device Name	0060E92012E0
Version	1.04
SN	102109103200
Playtime	20 Days

Network Information		
LAN1	MAC Address	00:60:e9:20:12:e0
	IP Address	192.168.4.183
LAN2	MAC Address	00:60:e9:20:12:e1
	IP Address	192.168.1.1

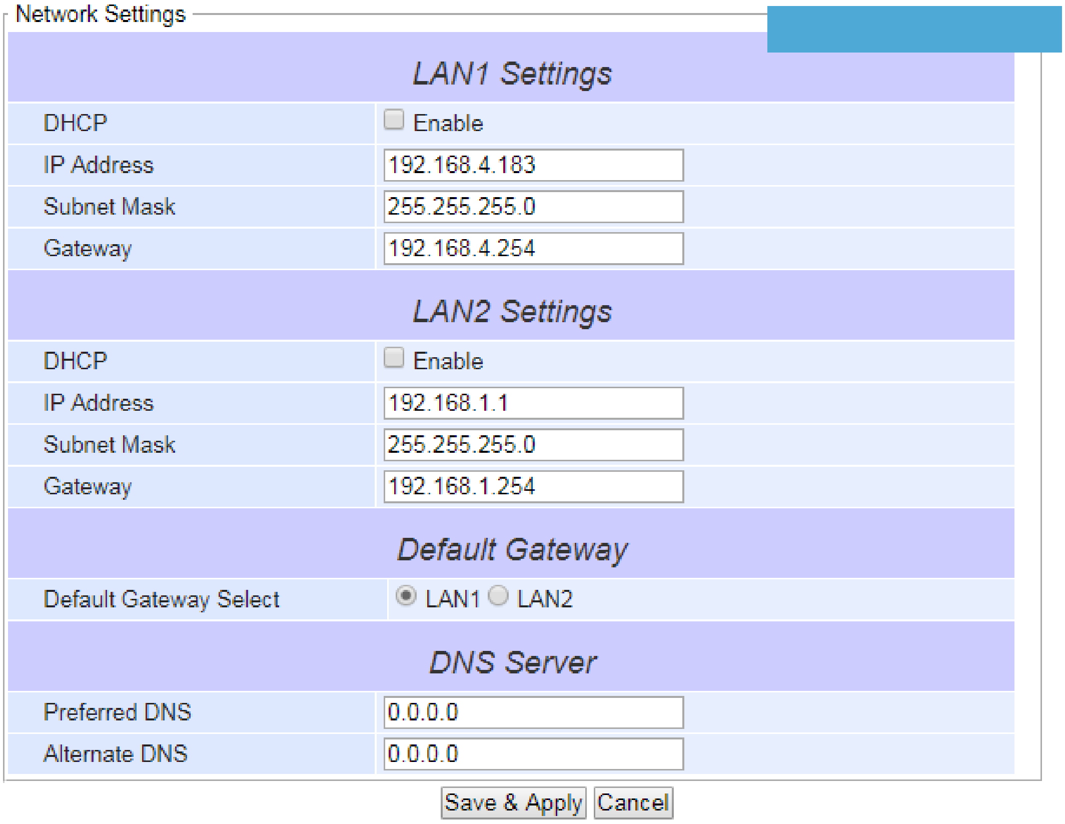
Figure 4.13 Overview Web Page (example on PS4000)

In detail, 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.
  - **Version** is the value of the version of the kernel firmware of the device.
  - **SN** is the serial number of the device.
  - **Playtime** is the elapsed time from the default settings is changed.
- **Network Information** shows information about the wired network interface on the device.
  - **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 PS4000/8000/16000 device can be configured. There are four sets of parameters which are **LAN1 Settings**, **LAN2 Settings**, **Default Gateway**, and **DNS Server** that can be entered as shown in Figure 4.14. First, **LAN1 Settings** part will allow you to configure the **IP Address**, **Subnet Mask**, and **Default Gateway** for your wired LAN1 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. Second, **LAN2 Settings** is the same as LAN1 Settings but for the second Ethernet interface. Third, **Default Gateway** part is where you can select the default gateway network for your serial device server. You can either select **LAN1** or **LAN2** by clicking on the corresponding radio button. Fourth, **DNS Server** part is where you can specify the IP Address of your **Preferred DNS** (Domain Name Server) and **Alternate DNS**. If the PS4000/8000/16000 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 in order to be able to resolve the host name of the NTP server. Please consult your network administrator or internet service provider (ISP) to obtain local DNS's IP addresses.



Network Settings

LAN1 Settings	
DHCP	□ Enable
IP Address	192.168.4.183
Subnet Mask	255.255.255.0
Gateway	192.168.4.254
LAN2 Settings	
DHCP	□ Enable
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Default Gateway	
Default Gateway Select	● LAN1 ○ LAN2
DNS Server	
Preferred DNS	0.0.0.0
Alternate DNS	0.0.0.0

Figure 4.14 Network Settings Web Page

4.6 *Serial*

Since PS4000/8000/16000 is an Industrial Serial Device Server, it supports serial communication with COM port(s). Note that PS4000/8000/16000 series can have up to four COM ports: **COM1**, **COM2**, **COM3**, and **COM4**, while typical PS4000 model will have only one COM port (**COM1**). Figure 4.15 shows the **Serial** menu on the left frame of the web interface of PS4000/8000/16000. The following subsections will describe how to configure these COM ports.

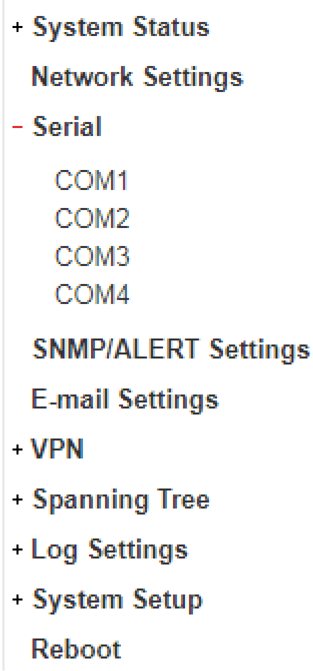
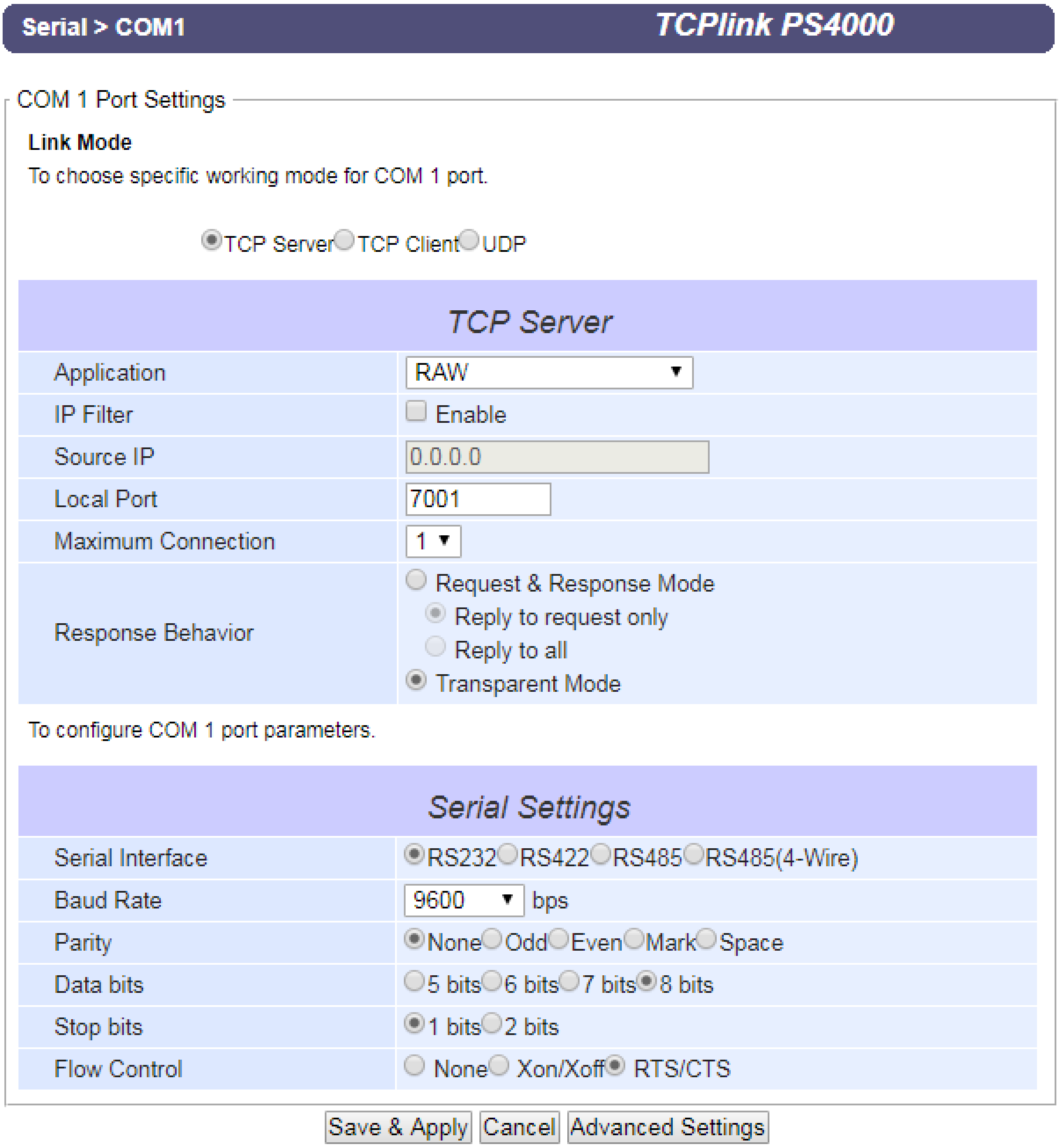


Figure 4.15 Serial Menu (example on PS4000)

4.6.1 *COM Port Overview*

Since details on **Link Mode** connectivity protocols and its settings of PS4000/8000/16000 series are given in Chapter 5 Link Modes and Applications, this section will only focus on the **Serial Settings** only**.** Figure 4.16 shows an example of the **COM 1 Port Settings** where the upper part is dedicated for **Link Mode** settings and the lower part is dedicated for **Serial Settings.** Note that similar settings web page is applicable for COM 2/COM 3/COM 4 Port Settings on PS4000/8000/16000 device**.**



Serial > COM1 TCPlink PS4000

COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

● TCP Server ○ TCP Client ○ UDP

TCP Server	
Application	RAW
IP Filter	□ Enable
Source IP	0.0.0.0
Local Port	7001
Maximum Connection	1
Response Behavior	○ Request & Response Mode ● Reply to request only ○ Reply to all ● Transparent Mode

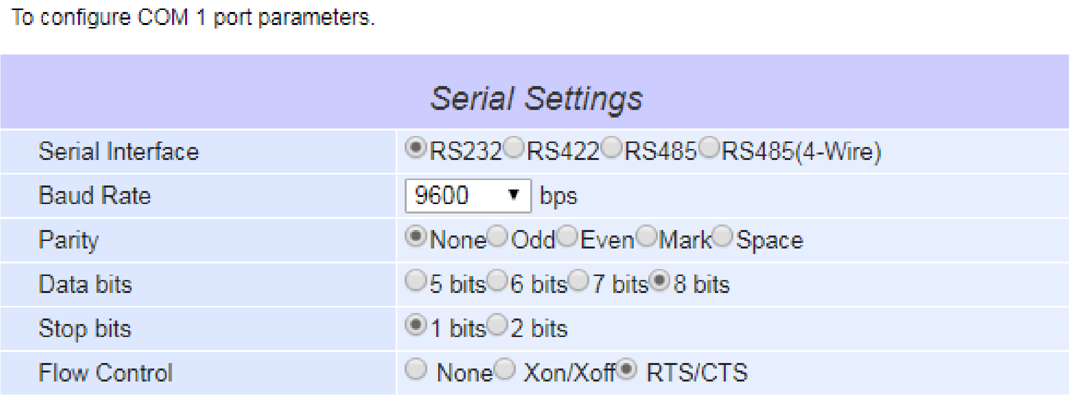
To configure COM 1 port parameters.

Serial Settings	
Serial Interface	● RS232 ○ RS422 ○ RS485 ○ RS485(4-Wire)
Baud Rate	9600 bps
Parity	● None ○ Odd ○ Even ○ Mark ○ Space
Data bits	○ 5 bits ○ 6 bits ○ 7 bits ● 8 bits
Stop bits	● 1 bits ○ 2 bits
Flow Control	○ None ○ Xon/Xoff ● RTS/CTS

Figure 4.16 COM 1 Port Settings Web Page

4.6.2 *COM Configuration*

Figure 4.17 excerpts the **Serial Settings** part of **COM** port settings of PS4000/8000/16000. Note that these settings need to match the parameters on the serial port of the serial device. Each option is described as follows.



To configure COM 1 port parameters.

Serial Settings	
Serial Interface	●RS232○RS422○RS485○RS485(4-Wire)
Baud Rate	9600 ▾ bps
Parity	●None○Odd○Even○Mark○Space
Data bits	○5 bits○6 bits○7 bits●8 bits
Stop bits	●1 bits○2 bits
Flow Control	○ None○ Xon/Xoff● RTS/CTS

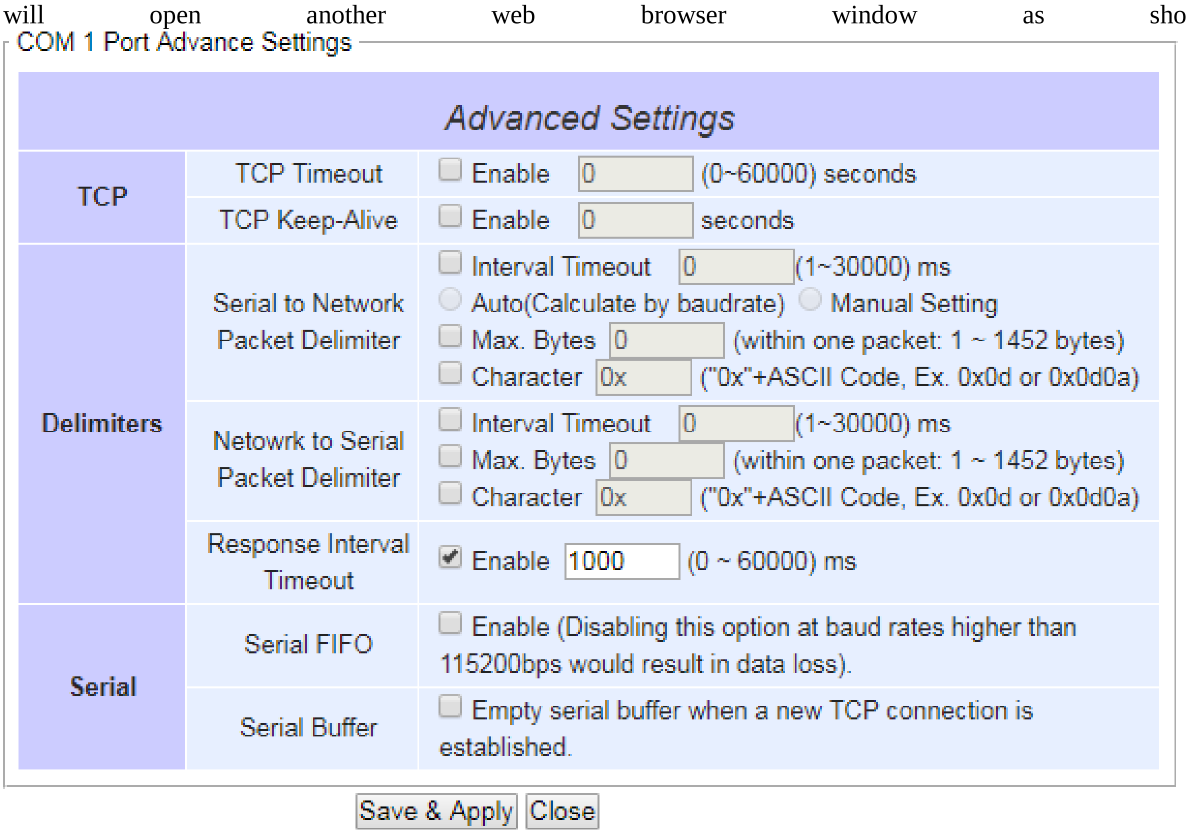
Figure 4.17 Serial Settings Part of COM 1 Port

- **Serial Interface**: This option allows selection between **RS-232**, **RS-422**, **RS-485**, and **RS-485 (4-Wire)** standards. <u>**Note:**</u>
  - RS-485 refers to 2-Wire RS-485 and RS-422 is compatible with 4-Wire RS-485.
- **Baud Rate**: The user can select one of the baud rates (from 1200 to 921600 bps) from the drop-down list.
- **Parity**: The available Parity options are **None**, **Odd**, **Even**, **Mark**, or **Space**.
- **Data Bits**: The setting for Data Bits can be **5 bits**, **6 bits**, **7 bits**, or **8 bits**.
- **Stop Bits**: The number of Stop Bits can be either **1 bit** or **2 bits**.
- **Flow Control**: The user can choose among **None** (No Flow Control), **RTS/CTS** (Hardware Flow Control), or **Xon/Xoff** (Software Flow Control). If Xon/Xoff is selected, the Xon and Xoff characters are changeable. Defaults are 0x11 for Xon and 0x13 for Xoff. Note that these are hexadecimal number of ASCII characters (i.e., 0x11 **=** ‘1’ and 0x13 **=** ‘3’).

After finish configuring the COM Port **Serial Settings**, please click on **Save & Apply** button to keep the change that you have made. Note that after click **Save & Apply**, the web browser will be refreshed and remain on the **Serial Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button. The **Advanced Settings** button will be described in the next subsection.

4.6.3 *COM Configuration: Advanced Settings*

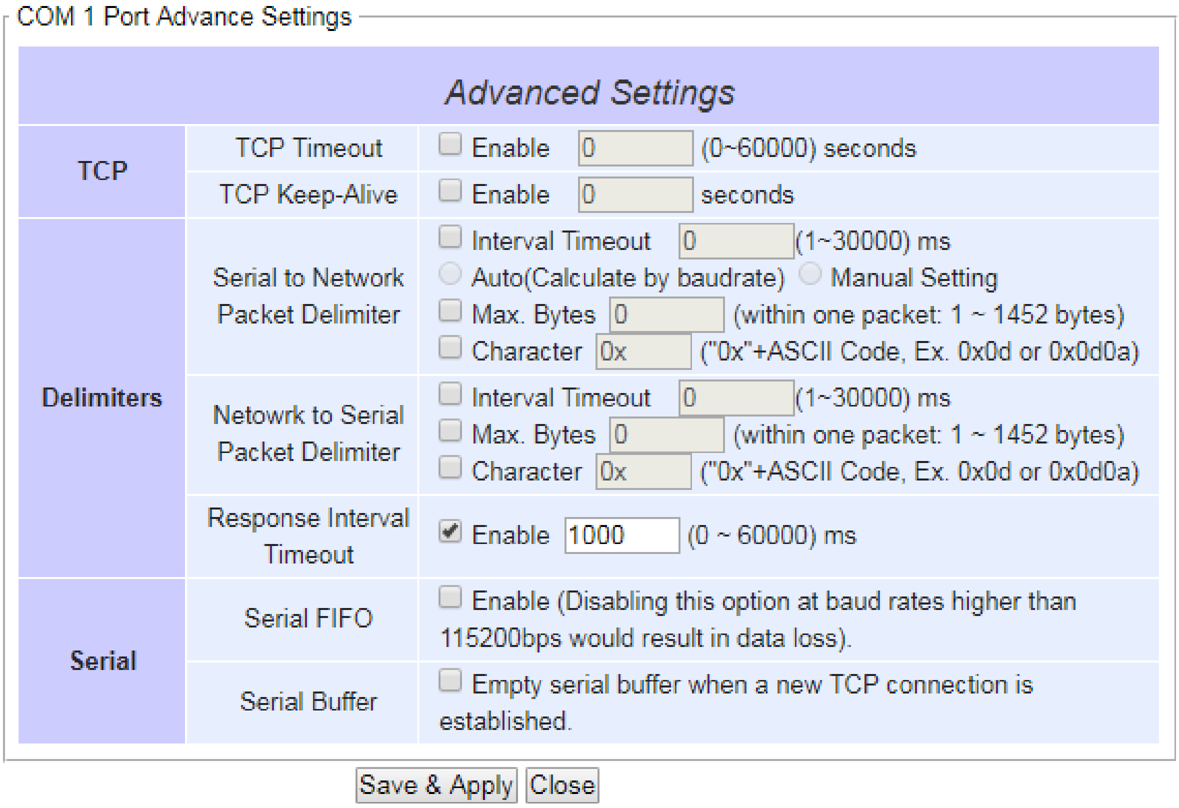
For advanced details of COM port setting, you can click on **Advanced Settings** button at the end of **Serial Settings** page which will open another web browser window as shown in Figure 4.18 below. Description of each option is explained as follows.



COM 1 Port Advance Settings

Advanced Settings

TCP	TCP Timeout	☐ Enable 0 (0~60000) seconds
	TCP Keep-Alive	☐ Enable 0 seconds
Delimiters	Serial to Network Packet Delimiter	☐ Interval Timeout 0 (1~30000) ms ○ Auto(Calculate by baudrate) ○ Manual Setting ☐ Max. Bytes 0 (within one packet: 1 ~ 1452 bytes) ☐ Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
	Netowrk to Serial Packet Delimiter	☐ Interval Timeout 0 (1~30000) ms ☐ Max. Bytes 0 (within one packet: 1 ~ 1452 bytes) ☐ Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
	Response Interval Timeout	☑ Enable 1000 (0 ~ 60000) ms
Serial	Serial FIFO	☐ Enable (Disabling this option at baud rates higher than 115200bps would result in data loss).
	Serial Buffer	☐ Empty serial buffer when a new TCP connection is established.



COM 1 Port Advance Settings

Advanced Settings

TCP	TCP Timeout	□ Enable 0 (0~60000) seconds
	TCP Keep-Alive	□ Enable 0 seconds
Delimiters	Serial to Network Packet Delimiter	□ Interval Timeout 0 (1~30000) ms ○ Auto(Calculate by baudrate) ○ Manual Setting □ Max. Bytes 0 (within one packet: 1 ~ 1452 bytes) □ Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
	Netowrk to Serial Packet Delimiter	□ Interval Timeout 0 (1~30000) ms □ Max. Bytes 0 (within one packet: 1 ~ 1452 bytes) □ Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
	Response Interval Timeout	☑ Enable 1000 (0 ~ 60000) ms
Serial	Serial FIFO	□ Enable (Disabling this option at baud rates higher than 115200bps would result in data loss).
	Serial Buffer	□ Empty serial buffer when a new TCP connection is established.

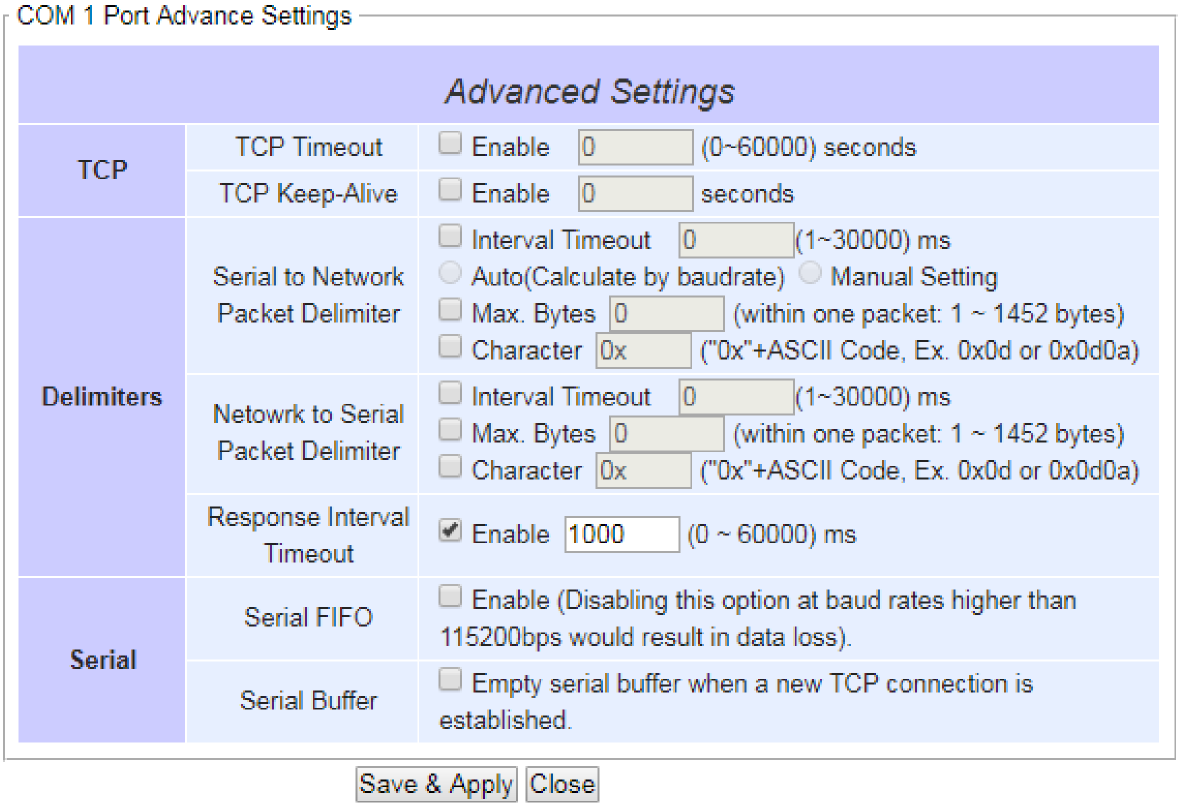
Figure 4.18 COM 1 Advanced Settings Web Page

TCP

- **TCP timeout:** By clicking the **Enable** box of **TCP Timeout** and input value in seconds between 0 and 60000,PS4000/8000/16000 will check if there's any data from serial port. If time expired, PS4000/8000/16000 will disconnect to its peer.
- **TCP Keep-alive:** By clicking the Ebable box of TCP Keep-alive and input value in seconds, PS4000/8000/16000 will check if its peer is still alive. Noted that it will retry 3 times and timeout is 5 seconds in default.

Delimiters

- **Serial to Network Packet Delimiter:** Packet delimiter is a way of packing data in the serial communication. It is designed to keep packets intact. PS4000/8000/16000 provides three types of delimiter: **Time Delimiter**, **Maximum Bytes** and **Character Delimiter**. Note that the following delimiters (Interval, Max Byte and Character) when they are selected are programmed in the OR logic. Meaning that if any of the three conditions were met, PS4000/8000/16000 would transmit the serial data in its buffer over the network.
  - **Interval timeout:** PS4000/8000/16000 will transmit the serial data in its buffer when the specified time interval has reached and no more serial data comes in. The default value is calculated automatically based on the baud rate which is the **Auto (calculate by baudrate)** option. If the automatic value results in chopped data, the timeout could be increased manually by switching to "**Manual setting**" (checking the radio button in



COM 1 Port Advance Settings

Advanced Settings		
TCP	TCP Timeout	□ Enable 0 (0~60000) seconds
	TCP Keep-Alive	□ Enable 0 seconds
Delimiters	Serial to Network Packet Delimiter	□ Interval Timeout 0 (1~30000) ms ○ Auto(Calculate by baudrate) ○ Manual Setting □ Max. Bytes 0 (within one packet: 1 ~ 1452 bytes) □ Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
	Netowrk to Serial Packet Delimiter	□ Interval Timeout 0 (1~30000) ms □ Max. Bytes 0 (within one packet: 1 ~ 1452 bytes) □ Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
	Response Interval Timeout	☑ Enable 1000 (0 ~ 60000) ms
Serial	Serial FIFO	□ Enable (Disabling this option at baud rates higher than 115200bps would result in data loss).
	Serial Buffer	□ Empty serial buffer when a new TCP connection is established.

- Figure 4.18) and specifying a larger value in the text box above. Note that the maximum interval is 30,000 milliseconds.

Attention

Manual Calculation of Interval Timeout

The optimal "Interval timeout" depends on the application, but it must be at least larger than one-character interval within the specified baud rate. For example, assuming that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits (included 1 start bit), and the time required to transfer one character is (10 (bits)/1200 (bits/s))*1000 (ms/s) = 8.3 ms. Therefore, you should set the "Interval timeout" to be larger than 8.3 ms. Rounding 8.3 ms to the next integer would give you 9 ms. Which can be set as your interval timeout.

- **Max Bytes:** PS4000/8000/16000 will transmit the serial data in its buffer when the specified length in the unit of bytes has reached. The range of maximum bytes is between 1 to 1452 bytes. Enabling this option by checking the box in front of **Max. Bytes**, if you would like PS4000/8000/16000 to queue the data until it reaches a specific length. This option is disabled by default.

- **Character:** PS4000/8000/16000 will transmit the serial data in its buffer when it sees the incoming data that includes the specified character (in hexadecimal (HEX) format). This field allows one or two characters. If character delimiter is set to 0x0d, PS4000/8000/16000 will push out its serial buffer when it sees 0x0d (carriage return) in the serial data. This option is disabled by default.

- **Network to Serial Packet Delimiter:** This group of options is the same as the delimiters described above, but they control data flow in the opposite direction. PS4000/8000/16000 will store data from the network interface in its queue. Until one of the delimiter conditions described above is met then PS4000/8000/16000 will send the data over to the serial interface.

- **Character Send Interval:** This option specifies the time gap between each character. When set to one second (1000ms), PS4000/8000/16000 would split the data in the queue and only transmit one character (a byte) every 1 second. The maximum value for this option is 1000 milliseconds or 1 second. This option is disabled by default.

- **Response Interval Timeout:** This option only affects the **Request & Response Mode** and has no effect on the **Transparent Mode**. Please see the discussion about **Request & Respond Mode** versus **Transparent Mode** in Chapter 5, Section 5.1.1. When TCP data is received (a request from network) and passed to serial device side, the PS4000/8000/16000 will wait for the set time before transferring another TCP data if the serial device side did not receive any data (no response from the serial device). The maximum value for this option is 60,000 milliseconds or 1 minute.

Serial

- **Serial FIFO:** By default, PS4000/8000/16000 has its First-In-First-Out (FIFO) function enabled to optimize its serial performance. In some applications (particularly when the flow control mechanism is enabled), it may deem necessary to disable the FIFO function to minimize the amount of data that is transmitted through the serial interface after a flow off event is triggered to reduce the possibility of overloading the buffer inside the serial device. Please note that disabling this option on baud rates higher than 115200bps would noticeably reduce the data integrity.

- **Serial Buffer:** By default, PS4000/8000/16000 will empty its serial buffer when a new TCP connection is established. This means that the TCP application will not receive buffered serial data during a TCP link breakage. To keep the serial data when there is no TCP connection and send out the buffered serial data immediately after a TCP connection is established, you can disable this option**.**

After finish configuring the COM Port**'**s **Advanced Settings**, please click on **Save & Apply** button to keep the change that you have made**.** Then, the **Advanced Settings** browser window can be closed by clicking on **Close** button and you will be returned to **COM 1 Port Setting** page**.**

4.7 *VPN*

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

PS4000/8000/16000 supports several VPN protocols: PPTP (Point-to-Point-Tunneling-Protocol), IPsec (Internet Protocol Security), and OpenVPN. In order to configure VPN, please click on the related item in the dedicated VPN sub-menu on the left-hand side of the screen, as shown in Figure 4.19 below.

A better description of PPTP is available in Chapter 0 아래.

A better description of OpenVPN is available in Chapter 4.9 아래.

A better description of IPsec related settings is available in Chapter 0 아래.

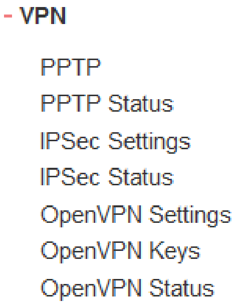
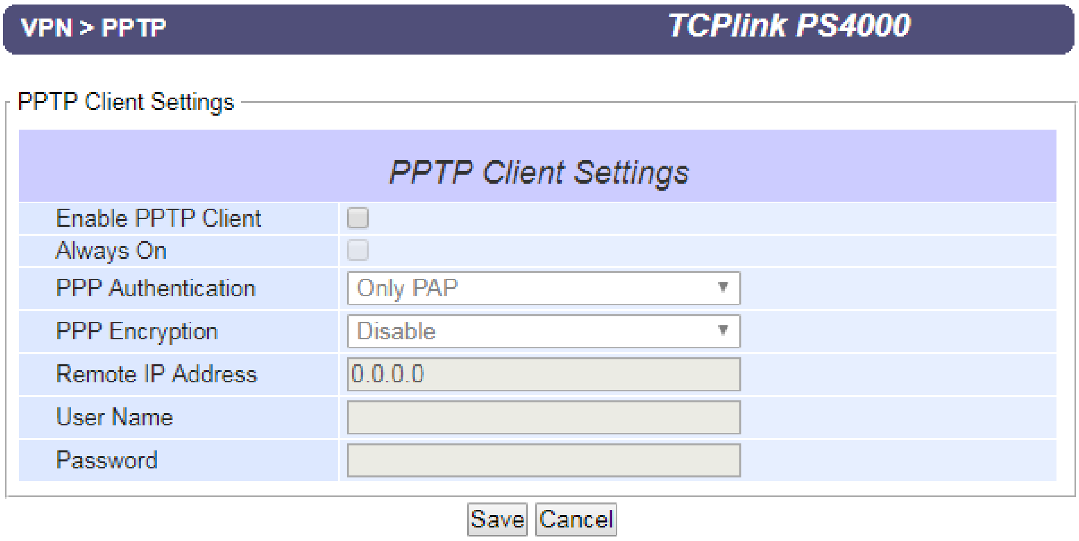


Figure 4.19 VPN menu structure

4.8 *PPTP Settings*

PPTP (Point-to-Point Tunneling Protocol) is a method for implementing virtual private networks. PPTP uses a TCP control channel and a GRE tunnel to encapsulate PPP packets. Select the PPTP item in the menu to configure a PPTP tunnel. Figure 4.20 shows the PPTP configuration page under PPTP web setting. Currently PS4000/8000/16000 series only supports PPTP client. After settings are completed, click “**Save**” to save the configuration.

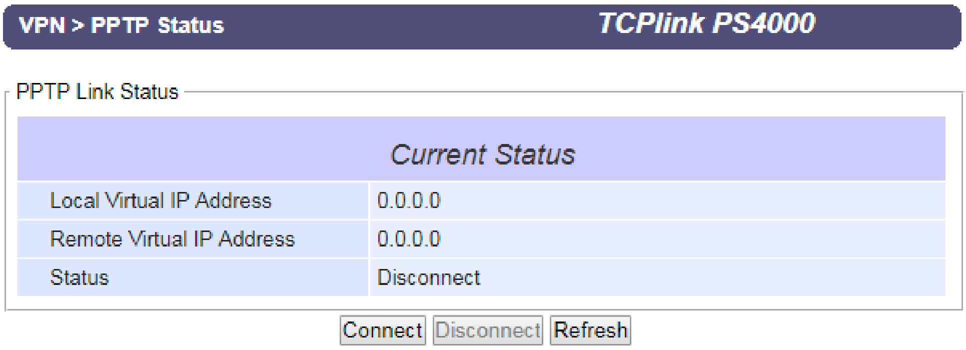


PPTP Client Settings	
Enable PPTP Client	☐
Always On	☐
PPP Authentication	Only PAP ▾
PPP Encryption	Disable ▾
Remote IP Address	0.0.0.0
User Name	
Password	

Figure 4.20 PPTP configuration page.

- Enable PPTP client: Check this to enable the PPTP client on PS4000/8000/16000 series.
- Always on: Check this to have PS4000/8000/16000 to automatically reconnect in event of disconnection.
- PPP Authentication: Specify the authentication algorithm – should be same as server
- PPP Encryption: Specify the encryption – should be same as server
- Remote IP address: Specify the IP address of PPTP server.
- User Name: Specify the User name for authentication.
- Password: Specify Password for authentication.

Figure 4.21 below shows the PPTP Link status.



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

Figure 4.21 PPTP Link Status

- Local Virtual IP Address: The virtual IP address assigned by PPTP server.
- Remote Virtual IP Address: The virtual IP address of PPTP server.
- Status: It shows the PPTP tunnel connection status. It will show Disconnect, Connect and Connecting.

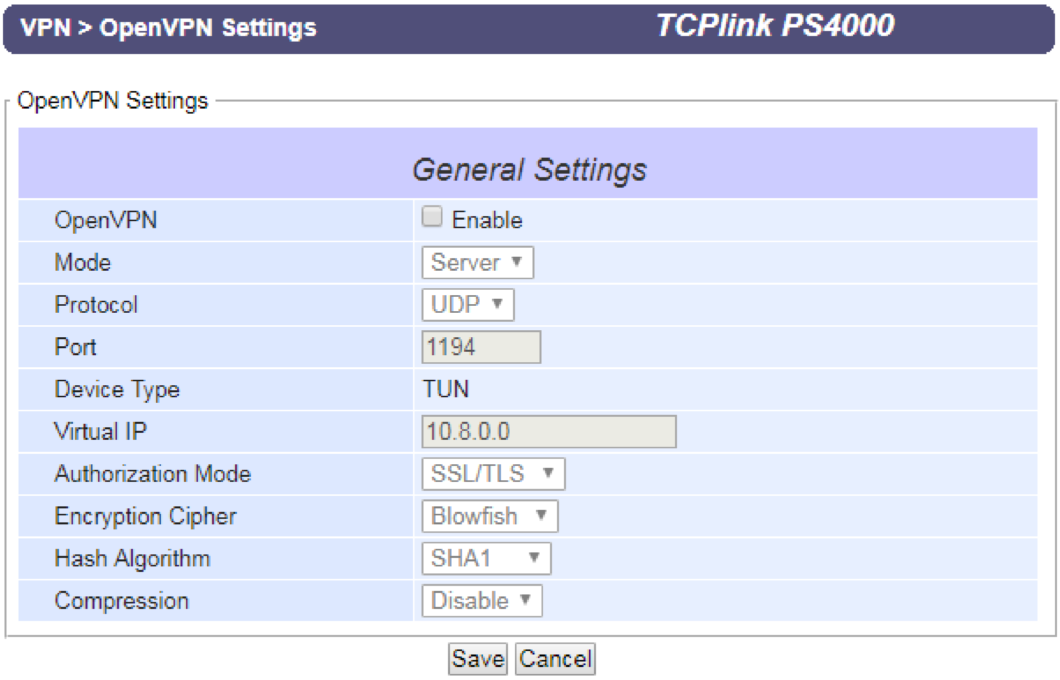
- Disconnect: No tunnel is established.
- Connect: PPTP Tunnel is established.
- Connecting: PPTP Tunnel is establishing.
- Connect: Click this button to connect to PPTP server.
- Disconnect: Click this button to disconnect PPTP tunnel.
- Refresh: Clieck this button to refresh the PPTP tunnel status.

4.9 *OpenVPN Settings*

OpenVPN is an application that implements VPN for creating secure point-to-point or site-to-site connections in routed or burdged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificates. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and certificate authority.
There are two OpenVPN connection scenarios. They are the TAP and TUN scenario. The product can create ether a layer-3 based IP tunnel(TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, you have to specify which type of OpenPVN connection scenario is to be adopted. Currently PS4000/8000/16000 series only support TUN mode.

4.9.1 *OpenVPN Setting*

In order to configure OpenVPN, click on the VPN tab in the left hand side of the menu and then **OpenVPN Settings**. The user interface is shown in below Figure 4.22.



VPN > OpenVPN Settings TCPlink PS4000

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

Figure 4.22 OpenVPN Setting

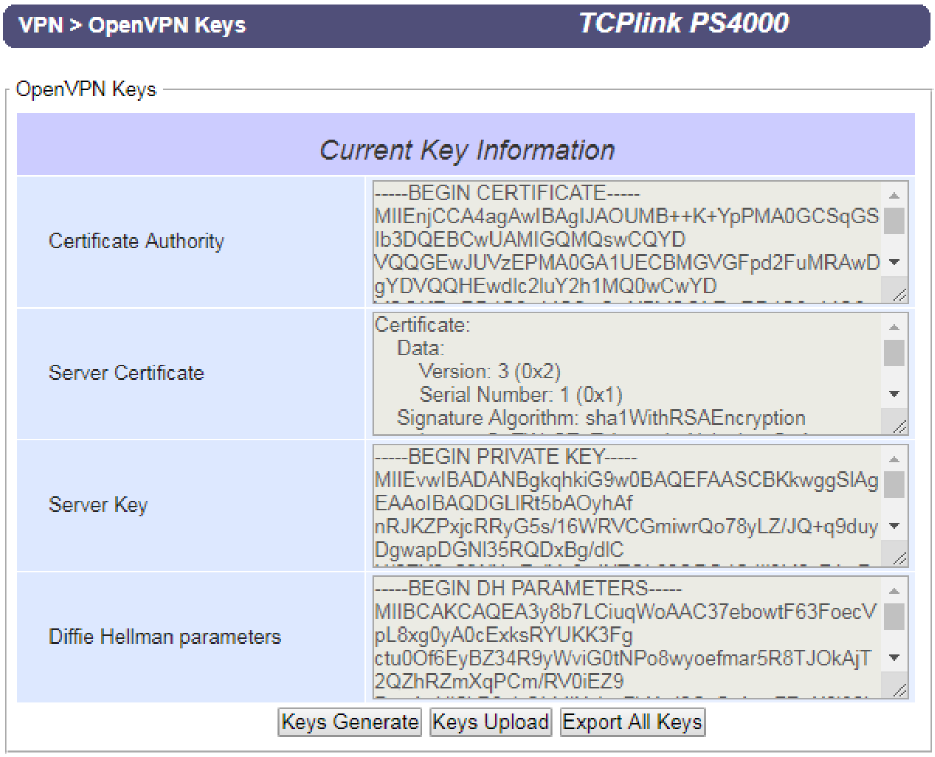
The OpenVPN parameters are described as below:

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

- **Port**: Defines the port number for TCP/UDP connection.
- **Device Type**: OpenVPN tunnel connection by TUN (Tunnel) mode or TAP mode. Currently PS4000/8000/16000 series only supports TUN (Tunnel) mode.
- **Virtual IP** (only when “OpenVPN Server” mode is selected): Specify the server’s virtual IP. Virtual IP will only be available when SSL/TLS is chosen as the Authentication Mode. The Server’s virtual IP address will be 10.8.0.1/24 and client virtual IP address will be 10.8.0.x/24.
- **Local/Remote endpoint IP** (only when “OpenVPN Client” mode is selected): Specifies the local and remote endpoint virtual IP address of this OpenPVN gateway. Local/Remote endpoint IP only be available when static key is chosen in Authentication Mode.
- **Authentication Mode**: Specify the authorization mode the OpenVPN server. There are 2 options available:
    - SSL/TLS: OpenVPN will use TLS authorization mode, and the following items CA cert, Server Cert and DH PEM will be used. See section 4.9.2 아래 for mode details.
    - Static Key: OpenVPN will use static key authorization, and the static key will be used. See section 4.9.2 아래 for mode details.
- **Encryption Cipher**: Specify the Encryption cipher. There are 5 options available: blowfish, AES 256, AES 192, AES 128 and Disable. When Disable is selected, no encryption will be used.
- **Hash Algorithm**: Specify the Hash algorithm. There are 5 options available: SHA1, MD5, SHA 256, SHA 512 and Disable.When Disable is selected, no Hash algorithm will be used.
- **Compression**: Specify whether or not the tunnel packets will be compressed. There are three options available: LZ4, LZO and Disable. When Disable is chosen, the packet won’t be compressed.
- **Push Lan to clients** (only when “OpenVPN Server” mode is selected): When enabled, PS4000/8000/16000 will push the LAN port subnet to the OpenVPN remote clients, so that the remote client will add a route to the PS4000/8000/16000 local network. Only PS4000B supports this function.

4.9.2 *OpenVPN Keys*

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

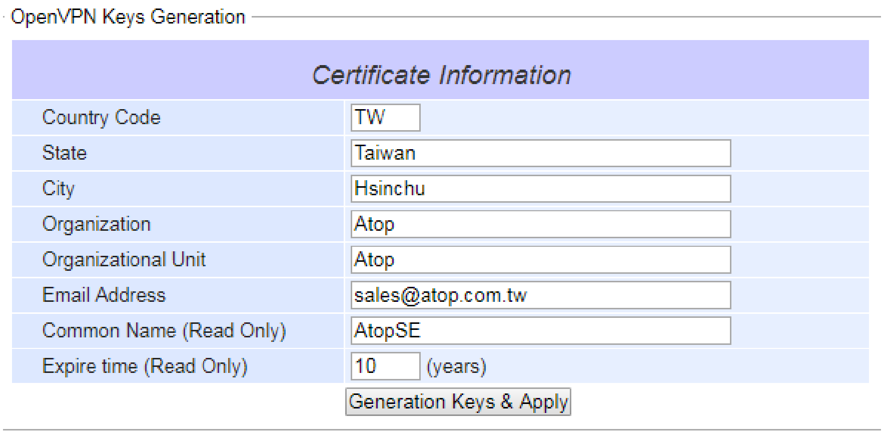


Current Key Information	
Certificate Authority	-----BEGIN CERTIFICATE----- MIIEnjCCA4agAwIBAgIJAOUMB++K+YpPMA0GCSqGS Ib3DQEBCwUAMIGQMQswCQYD VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAwD gYDVQQHEwdlc2luY2h1MQ0wCwYD
Server Certificate	Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) Signature Algorithm: sha1WithRSAEncryption
Server Key	-----BEGIN PRIVATE KEY----- MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAg EAAoIBAQDGLIRt5bAOyhAf nRJKZPxjcRRyG5s/16WRVCGmiwrQo78yLZ/JQ+q9duy DgwapDGNI35RQDxBg/dlC
Diffie Hellman parameters	-----BEGIN DH PARAMETERS----- MIIBCAKCAQEA3y8b7LCiuqWoAAC37ebowtF63FoecV pL8xg0yA0cExksRYUKK3Fg ctu0Of6EyBZ34R9yWviG0tNPo8wyoefmar5R8TJOkAjT 2QZhRZmXqPCm/RV0iEZ9

Figure 4.23 OpenVPN Keys

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

When PS4000/8000/16000 acts as OpenVPN server, the user could define his own certification information by clicking on the **Key generate** button. Otherwise, the certificate can be imported. When generating a new key, a Pop-up window will open. Fill in the parameters and click on "**Generation Keys & Apply**" button.



OpenVPN Keys Generation

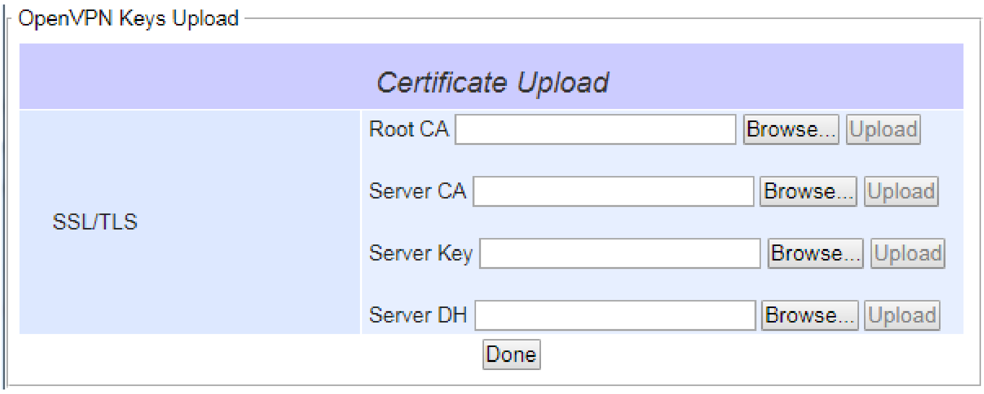
Certificate Information

Country Code	TW
State	Taiwan
City	Hsinchu
Organization	Atop
Organizational Unit	Atop
Email Address	sales@atop.com.tw
Common Name (Read Only)	AtopSE
Expire time (Read Only)	10 (years)

Figure 4.24 Certification information

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

When clicking on the **Keys Upload** button instead, a pop-up window shown in Figure 4.25 will show up and will allow you to import the related server or client certificates.



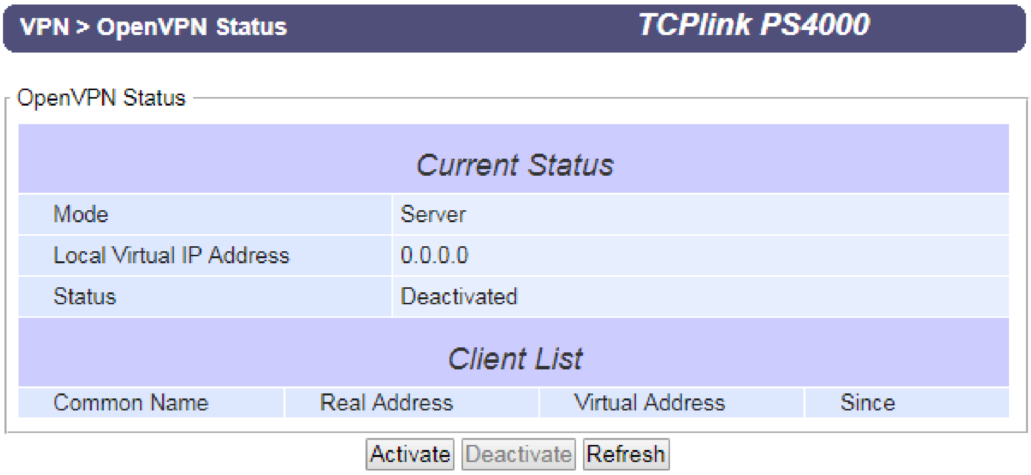
OpenVPN Keys Upload
Certificate Upload
SSL/TLS
Root CA Browse... Upload
Server CA Browse... Upload
Server Key Browse... Upload
Server DH Browse... Upload
Done

Figure 4.25 Certificate Upload

Click the **Browse** button to select your own server or client certificate and click on the **Upload** button. When PS4000/8000/16000 acts as an OpenVPN server, use **Export All Keys** button to download all the necessary certificates include CA.crt, CA.key and the certificate and key for client side.

4.9.3 *OpenVPN Status*

In order to check the current OpenVPN connection status, click "OpenVPN status" in the VPN menu on the left-hand side of the screen. A page like below Figure 4.26 or Figure 4.27 will show up depending whether OpenVPN is set as Client or Server.



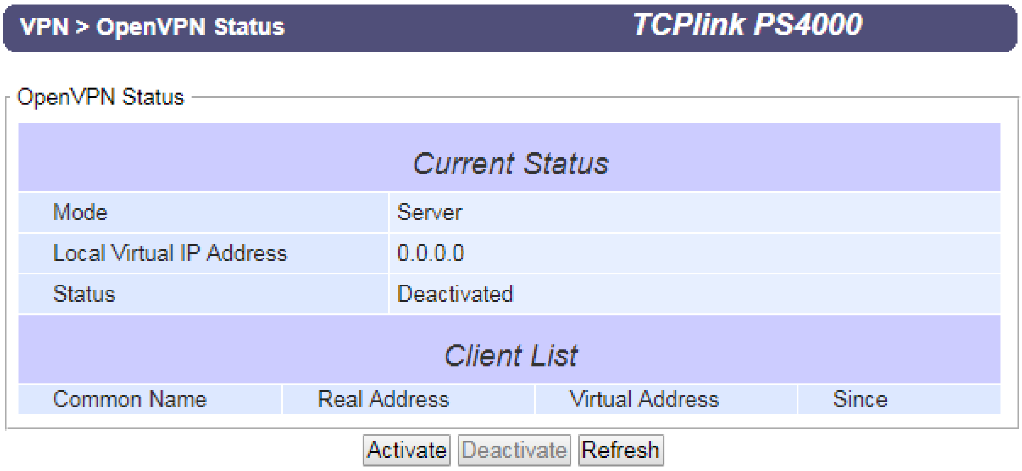
Current Status	
Mode	Server
Local Virtual IP Address	0.0.0.0
Status	Deactivated

Client List

Common Name	Real Address	Virtual Address	Since

Figure 4.26 OpenVPN client status

- **Mode**: Displays the OpenVPN mode PS4000/8000/16000 is currently running as.
- **Local Virtual IP address**: Displays the Local virtual IP address.
- **Remote Virtual Status**: Displays the Remote virtual IP address.
- **Status**: Displays the current status of OpvnVPN connection. It will include Disconnected, Connecting and Connected.



Current Status	
Mode	Server
Local Virtual IP Address	0.0.0.0
Status	Deactivated

Client List

Common Name	Real Address	Virtual Address	Since

Figure 4.27 OpenVPN server status

- **Mode**: Displays the OpenVPN mode PS4000/8000/16000 is currently running as.
- **Local Virtual IP address**: Displays the Local virtual IP address.
- **Status**: Displays the current status of OpvnVPN connection. It will be either be Deactivated, Activating, Disconnected, Connecting and Connected.

4.10 *IPsec Settings*

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

PS4000/8000/16000 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 PS4000/8000/16000 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 (PS4000/8000/16000) and a peer device (such as another PS4000/8000/16000). Note that this type of connection cannot be use for accessing entire sub-network resources. Figure 4.28 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode.**

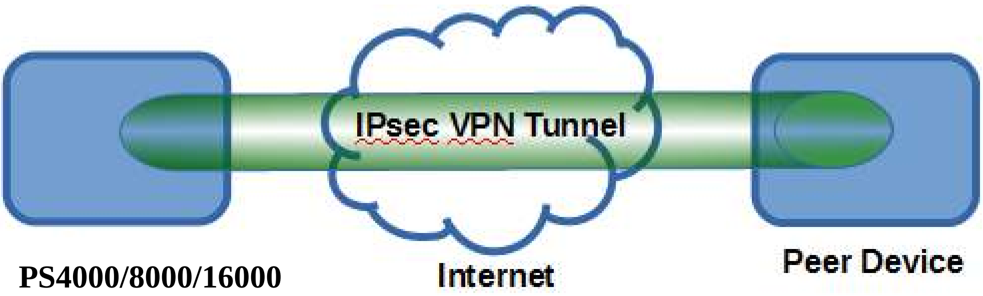


Figure 4.28 An example of Host-to-Host Connection

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 4.29 illustrates a road-warrior application in which PS4000/8000/16000 can access a remote sub-network resource via a peer gateway. Figure 4.30 illustrates a gateway application in which PS4000/8000/16000 can passively accept connection requests from remote sides and provide access to the PS4000/8000/16000 sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

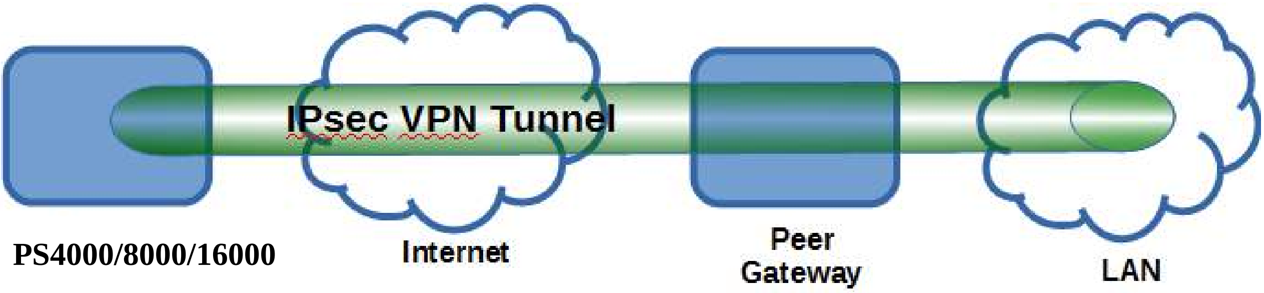


Figure 4.29 Roadwarrior Application using Host-to-Subnet Connection

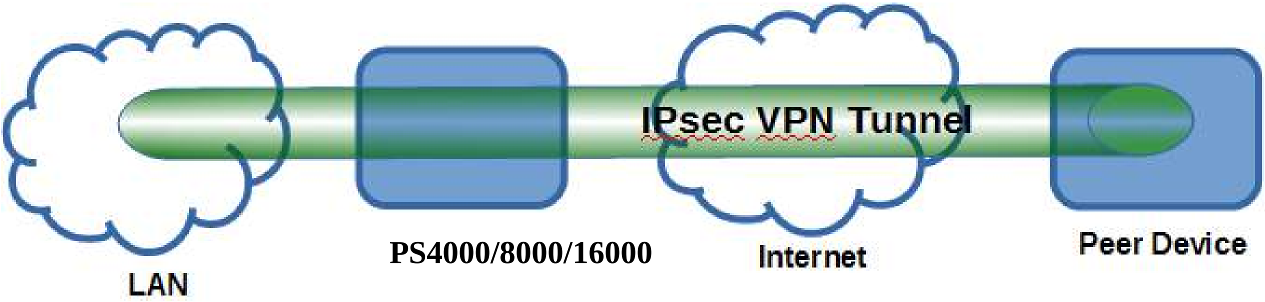


Figure 4.30 Gateway Application using Host-to-Subnet Connection

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. **오류! 참조 원본을 찾을 수 없습니다.** 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 4.31. On the other hand, two different devices on two different subnets (host-host application) can be connected via a IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 4.32. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

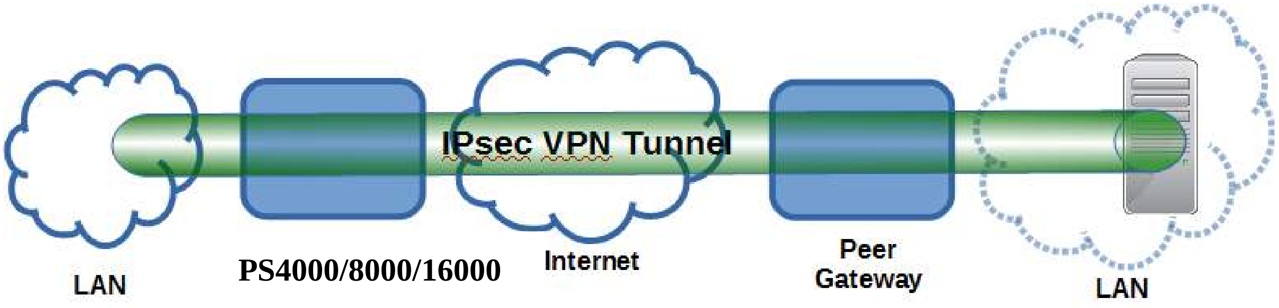


Figure 4.31 An example of host-network application via the subnet-to-subnet connection

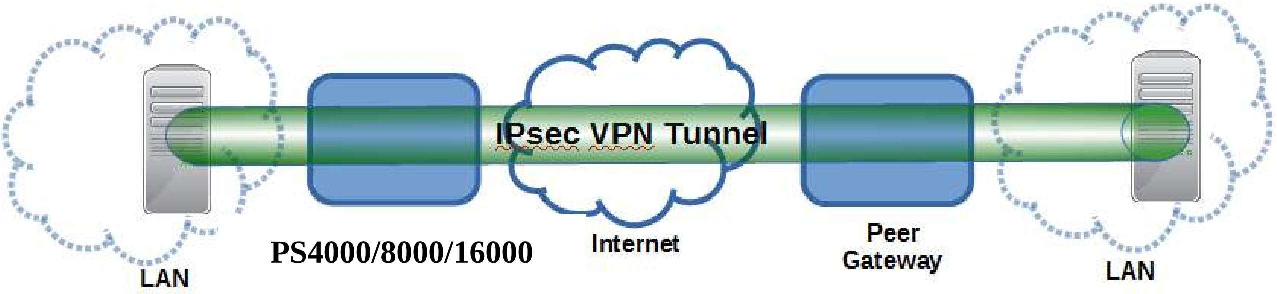


Figure 4.32 An example of host-host application via the subnet-to-subnet connection

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

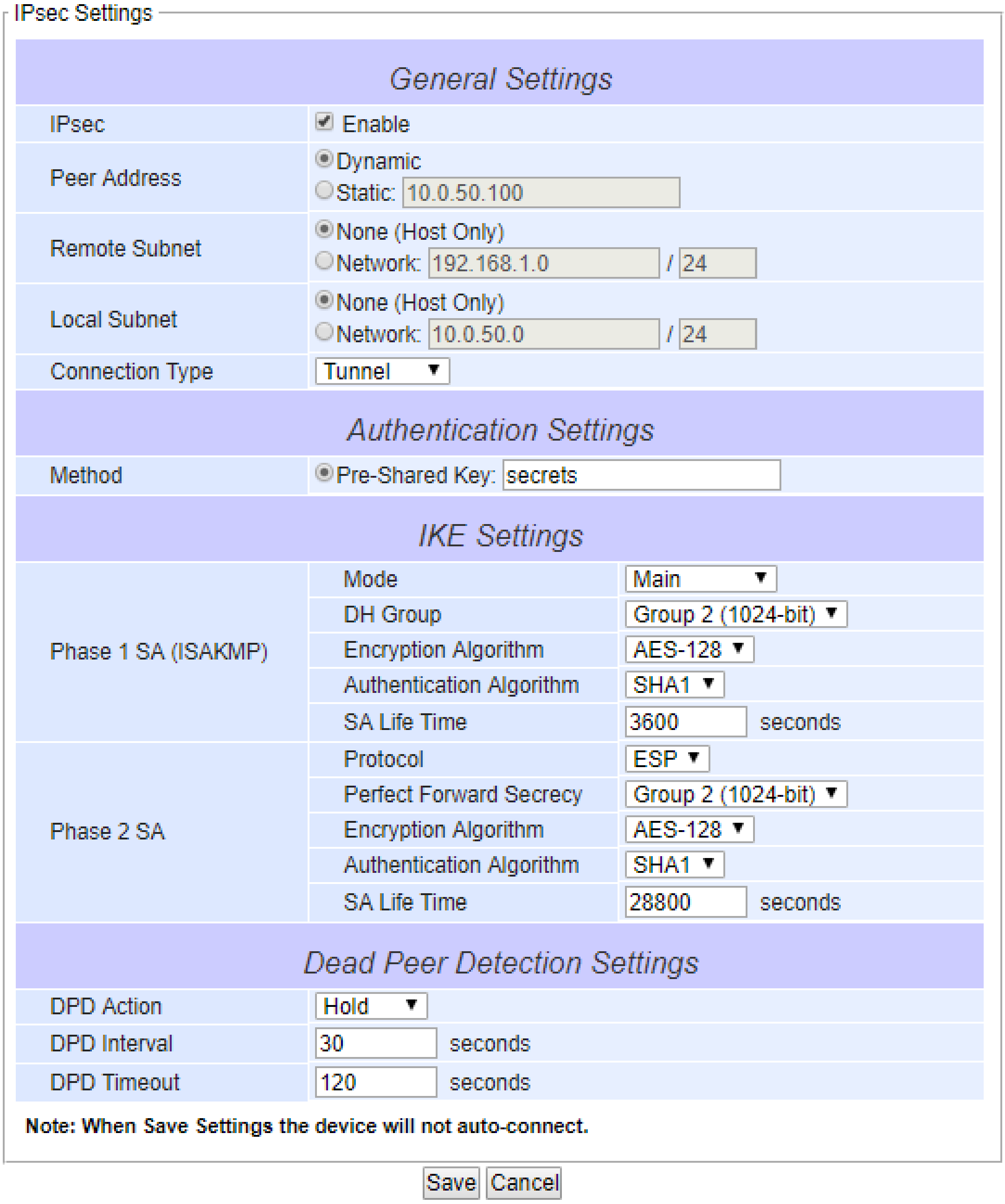
- Internet Key Exchange (IKE) protocol uses User Datagram Protocol (UDP) port number 500.
- Encapsulating Security Payload (ESP) uses IP protocol number 50.
- Authentication Header (AH) uses IP protocol number 51.
- IPsec NAT traversal uses UDP port number 4500 when NAT traversal is in use.

PS4000/8000/16000 also has a feature called NAT traversal (NAT-T) that allows the IPsec tunnel to pass through the NAT in its network. PS4000/8000/16000 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, PS4000/8000/16000 utilizes the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite. Note that IKE builds upon the Oakley protocol and ISAKMP (Internet Security Association and Key Management Protocol). IKE uses X.509 certificates for authentication either pre-shared or distributed using DNS (preferably with DNSSEC). IKE also uses a Diffie-Hellman key (DH) key exchange to set up a shared session secret from which cryptographic keys are derived. The IPsec security associations (SA) is divided into two phases. In phase one, IKE creates an authenticated secure channel between PS4000/8000/16000 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.

4.10.1 *IPsec Settings*

Figure 4.33 shows the **IPsec Settings** web page under the **IPsec Settings** menu**.** There are four sections on this page**: General Settings**, **Authentication Settings**, **IKE Settings**, and **Dead Peer Detection Settings.**



IPsec Settings

General Settings

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

Authentication Settings

Method	● Pre-Shared Key: secrets

IKE Settings

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

Dead Peer Detection Settings

DPD Action	Hold ▼
DPD Interval	30 seconds
DPD Timeout	120 seconds

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

Figure 4.33 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 PS4000/8000/16000.
- **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 PS4000/8000/16000 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 PS4000/8000/16000 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 PS4000/8000/16000 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. PS4000/8000/16000 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**, PS4000/8000/16000 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, PS4000/8000/16000 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 PS4000/8000/16000 use to verify the existence of a remote Internet Key Exchange (IKE) gateway or the peer device of PS4000/8000/16000**.** To detect the peer device, PS4000/8000/16000 will sent encrypted IKE Phase 1 notification payloads (or hello message) to its peer device and wait for DPD acknowledgement from the peer device**.** If PS4000/8000/16000 does not receive an acknowledge message during a specific time interval (**DPD timeout**), it will consider that the peer device is dead**.** Then, PS4000/8000/16000 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 PS4000/8000/16000 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 PS4000/8000/16000 will repeatly check the endpoint with keep-alive message**.** The **DPD interval** can be ranged from 1 to 65535 seconds. The default value for **DPD Interval** is 30 seconds**.** The **DPD Timeout** will be the time that PS4000/8000/16000 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 PS4000/8000/16000 will take the PDP action. The **DPD Timeout** value range from 1 to 65535 seconds. The default value of **DPD Timeout** is 120 seconds**.** Description of each parameters in the IPsec Tunnels web page is summarized in Table 4.1**.**

Table 4.1 Description of Parameters in IPsec Tunnels Web Page

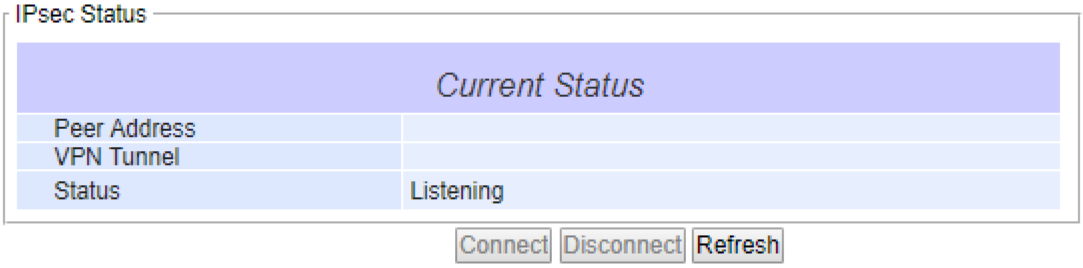
Field Name		**Description**	**Default Value**
General Settings			
IPsec		Enable the IPsec Tunnel	Disable
NAT Traversal		Enable the NAT Traversal mechanism	Enable
Peer Address		IP address of the remote device which can be dynamic (any address) or static (fixed address)	Dynamic
Remote Subnet		Remote subnet 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 process: DH Group 2 (1024-bit) or DH Group 5 (1536-bit)	Group 2 (1024-bit)
	Encryption Algorithm	Encryption algorithm used in the key exchange process: Either 3DES or AES	AES128
	Authentication Algorithm	Hash algorithm used to authenticate packet data in the key exchange process of IKEv1 phase 1: Either MD5 or SHA1	SHA1
	SA Life Time	How long a particular instance of a connection (a set of encryption/authentication keys for user	3600

Field Name		Description	Default Value
		packets) should last, from successful negotiation to expiry. The value can be from 300 to 86,400 seconds.	
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.

4.10.2 *IPsec Status*

On this web page, you can check the status of your IPsec connection between PS4000/8000/16000 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 PS4000/8000/16000. The second information is the **VPN Tunnel**'s status. The third information is the **Status** of the IPsec connection which can be **Disabled**, **Listening**, or **Connected.** shows the **IPsec Status** web page under the **IPsec Settings** menu. There are three buttons at the end of the web page which are **Connect**, **Disconnect**, and **Refresh.** The **Connect** and **Disconnect** buttons allow you to establish or tear down the IPsec connection. The **Refresh** button enable you to check the latest status of the connection.



IPsec Status

Current Status

Peer Address	
VPN Tunnel	
Status	Listening

Figure 4.34 IPsec Status Web Page

4.10.3 *Examples of IPsec Settings*

The following subsections provide examples of **IPsec settings**. However, each example will be focused only on the **General Settings** part. The other parts of the **IPsec Settings** can be configured according to the user's preference. Please consult previous section on the details of **Authentication Settings**, **IKE Settings**, and **Dead Peer Detection Settings**. <u>**Note**</u> that the network-to-network (or subnet-to-subnet) connections are now supported in new firmware of PS4000/8000/16000.

4.10.3.1 Host-to-Host Connections

Two scenarios can be configured for host-to-host connections: with static peer and with dynamic peer. A host-to-host topology for both scenarios is illustrated in Figure 4.35. Please follow the steps provided next for each scenario to set the **General Settings**.

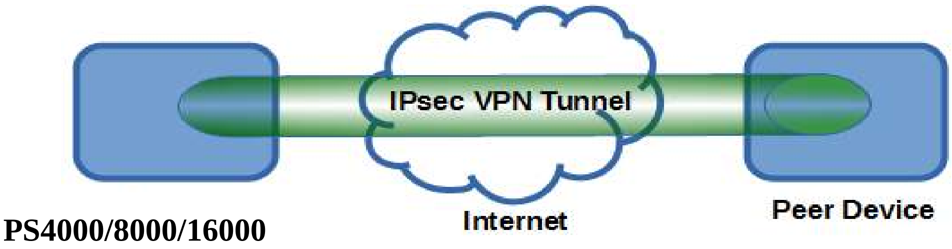
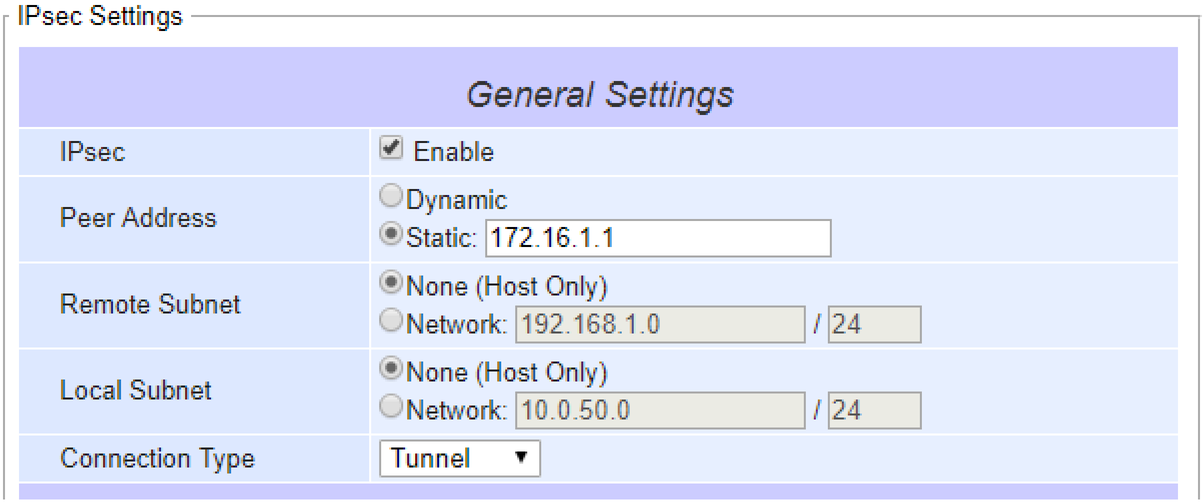


Figure 4.35 IPsec VPN Tunnel with Host-to-Host Topology

Scenario: host-to-host with static peer as shown in Figure 4.36

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  <u>**Note:**</u> When peer address is entered as the static address, the PS4000/8000/16000 acts as an **initiator** which takes the initiative and establishes a connection. The PS4000/8000/16000 also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Select the raio button for **None (Host Only)** in the **Remote Subnet** field.
- Since this VPN connection is established on two hosts, the **Connection Type** option can be either **Transport** or **Tunnel**.



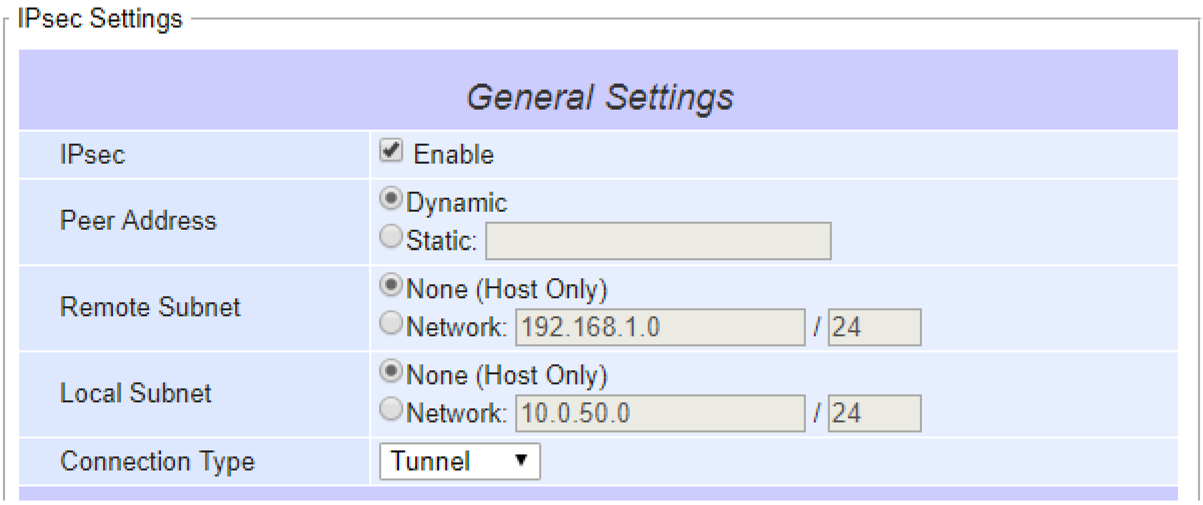
IPsec Settings

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

Figure 4.36 General Settings for Host-to-Host with Static Peer

Scenario: host-to-host with dynamic peer as shown in Figure 4.37

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  <u>**Note:**</u> When VPN connects to a peer with dynamic IP address, the PS4000/8000/16000 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.



IPsec Settings

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

Figure 4.37 General Settings for Host-to-Host with Dynamic Peer

4.10.3.2 Host-to-Network Connections

Two scenarios can also be configured for host-to-network (or host-to-subnet or host-to-site) connections: with static peer and with dynamic peer. Note that the PS4000/8000/16000 is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in Figure 4.38. Please follow the steps provided next for each scenario to set the **General Settings**.

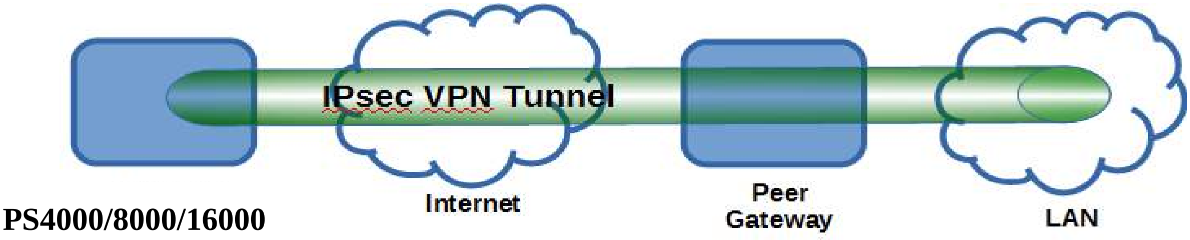
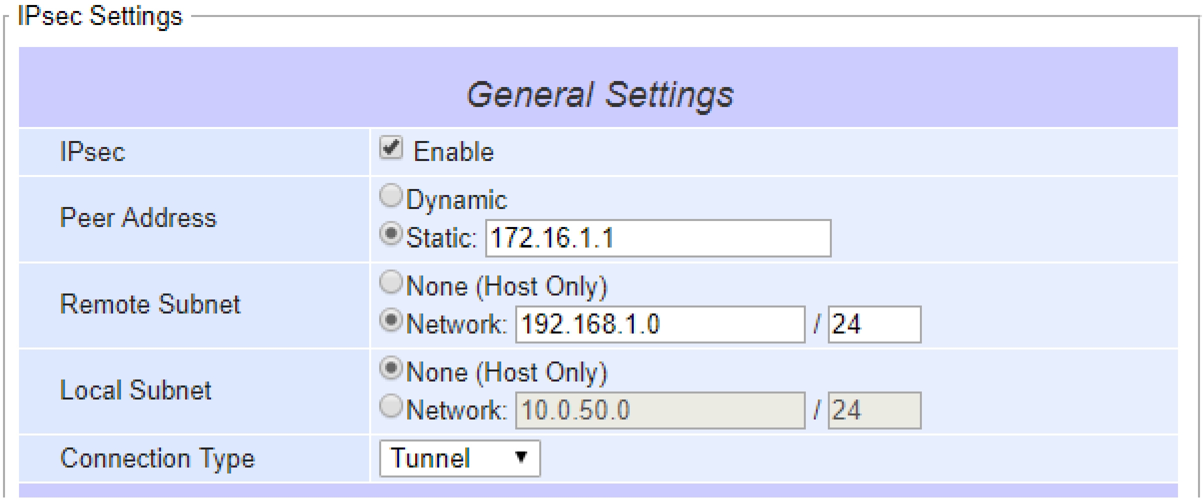


Figure 4.38 IPsec VPN Tunnel with Host-to-Network Topology

Scenario: host-to-network with static peer as shown in Figure 4.39

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  <u>**Note:**</u> When peer address is entered as a static address, the PS4000/8000/16000 is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. The PS4000/8000/16000 also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.



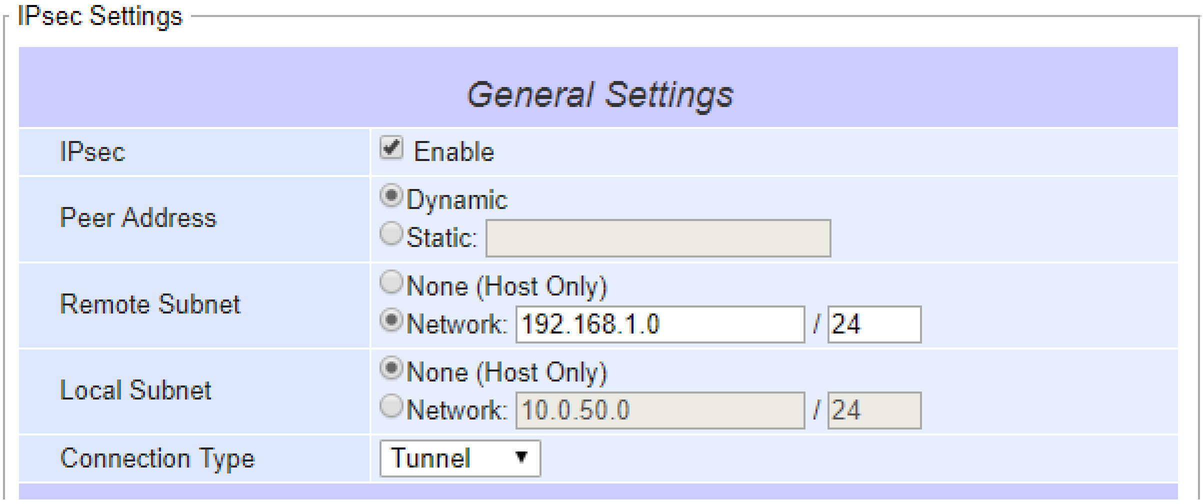
IPsec Settings

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

Figure 4.39 General Settings for Host-to-Network with Static Peer

Scenario: host-to-network with dynamic peer as shown in Figure 4.40

- 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 PS4000/8000/16000 will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in "address prefix length" or behind the "/" symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.



IPsec Settings

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

Figure 4.40 General Settings for Host-to-Network with Dynamic Peer

4.10.3.3 Network-to-Network (Subnet-to-Subnet) Connections

Two scenarios can also be configured for network-to-network (or subnet-to-subnet) connections: with static peer or with dynamic peer. A VPN tunnel will be created between two separate private sub-networks. Note that the PS4000/8000/16000 is the gateway to a local network in these scenarios. A network-to-network topology for both scenarios is illustrated in Figure 4.41. Please follow the steps provided next for each scenario to set the **General Settings**.

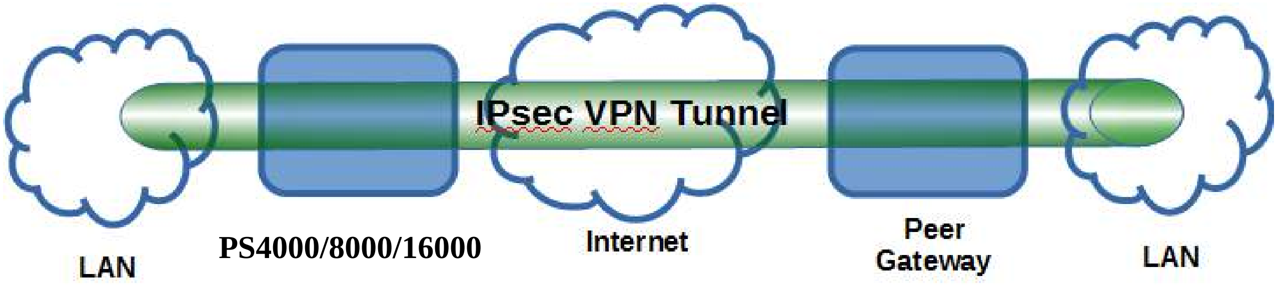
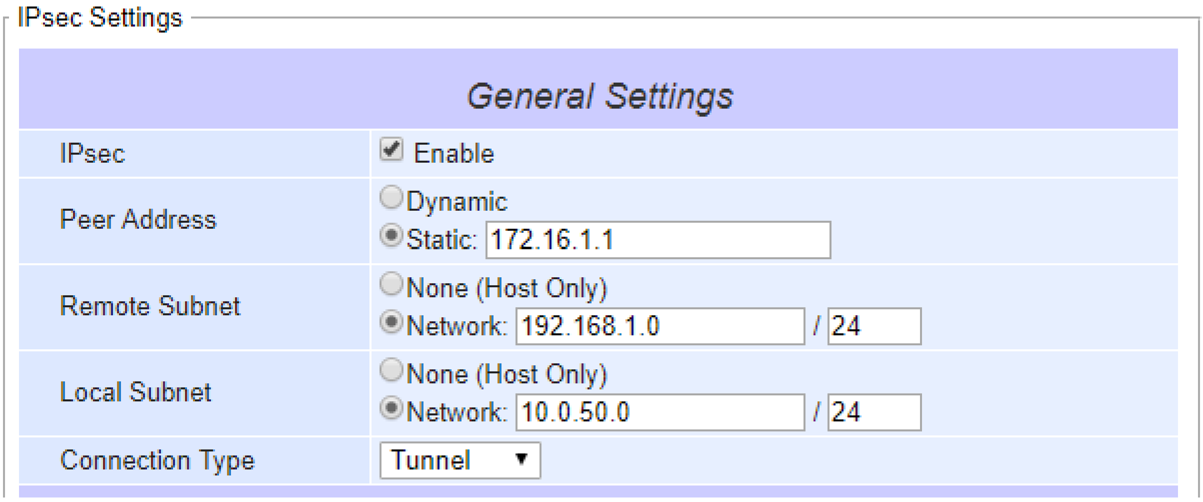


Figure 4.41 IPsec VPN Tunnel with Network-to-Network Topology

Scenario: network-to-network with static peer as shown in Figure 4.42

- 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 PS4000/8000/16000 is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. The PS4000/8000/16000 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

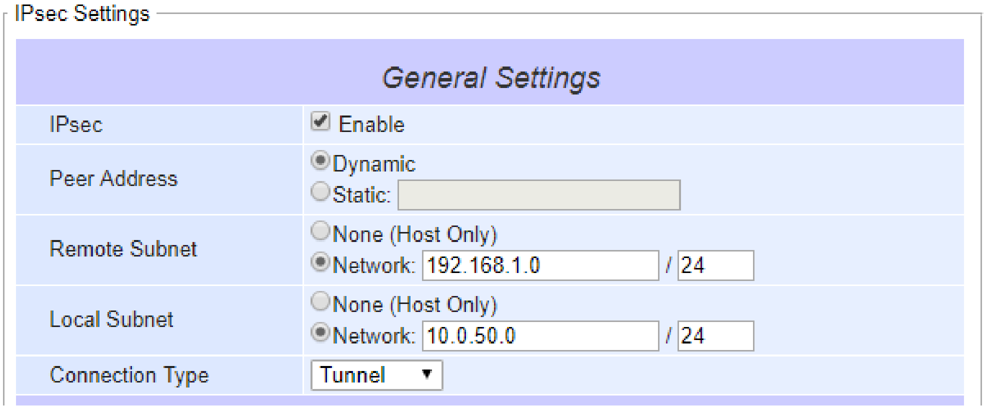
General Settings

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

Figure 4.42 General Settings for Network-to-Network with Static Peer

Scenario: network-to-network with dynamic peer as shown in Figure 4.43

- 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 PS4000/8000/16000 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:
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 Network-to-Network with Dynamic Peer

4.11 *Spanning Tree*

Spanning tree functionality is supported by TCPlink's PS4000/8000/16000 Industrial Device Server series. However, PS4000/8000/16000 is only an end device in a network; therefore, it only has the receiving function of spanning tree. Generally, the **S**panning **T**ree **P**rotocol (**STP**) provides a function to prevent switching loops and broadcast radiation at the OSI layer 2. A switching loop occurs in a network when there are multiple connections or redundant paths between two network switches or at least two ports are connected on both sides of the two network switches. The switching loop can create a broadcast radiation, which is the accumulation of broadcast and multicast traffics in a computer network. As broadcast and multicast messages are forwarded by bridges/switches to every port, the bridges/switches will repeatedly rebroadcast the broadcast messages, and this accumulation of traffic can flood the network. STP creates a spanning tree topology and disables those links of the network that are not part of the spanning tree, which leaves only a single active path between two nodes. This function can avoid flooding and increase network efficiency. Therefore, PS4000/8000/16000 deploys spanning tree as a tool when the users set up connection or port redundancy or fault-tolerance in their network.

RSTP (**R**apid **S**panning **T**ree **P**rotocol), IEEE 802.1W, is the only mode of spanning tree supported in PS4000/8000/16000. It is an evolution of the STP (IEEE 802.1D standard), but it is still backwards compatible with standard STP. RSTP has the advantage over the STP. When there is a topology change such as link failure in the network, the RSTP will converge significantly faster to a new spanning tree topology. RSTP improves convergence on point-to-point links by reducing the Max-Age time to 3 times Hello interval, removing the STP listening state, and exchanging a handshake between two switches to quickly transition the port to forwarding state.

The **Spanning Tree** menu and its sub-menus can be found on left frame of the web interface of PS4000/8000/16000. The list of **Spanning Tree** menu is shown in Figure 4.44. The sub-menus und the **Spanning Tree** are **Setting**, **Bridge Info**, and **Port Setting**. Each of this sub-menu will be described in the following subsections.

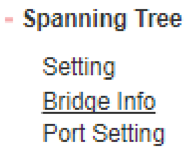
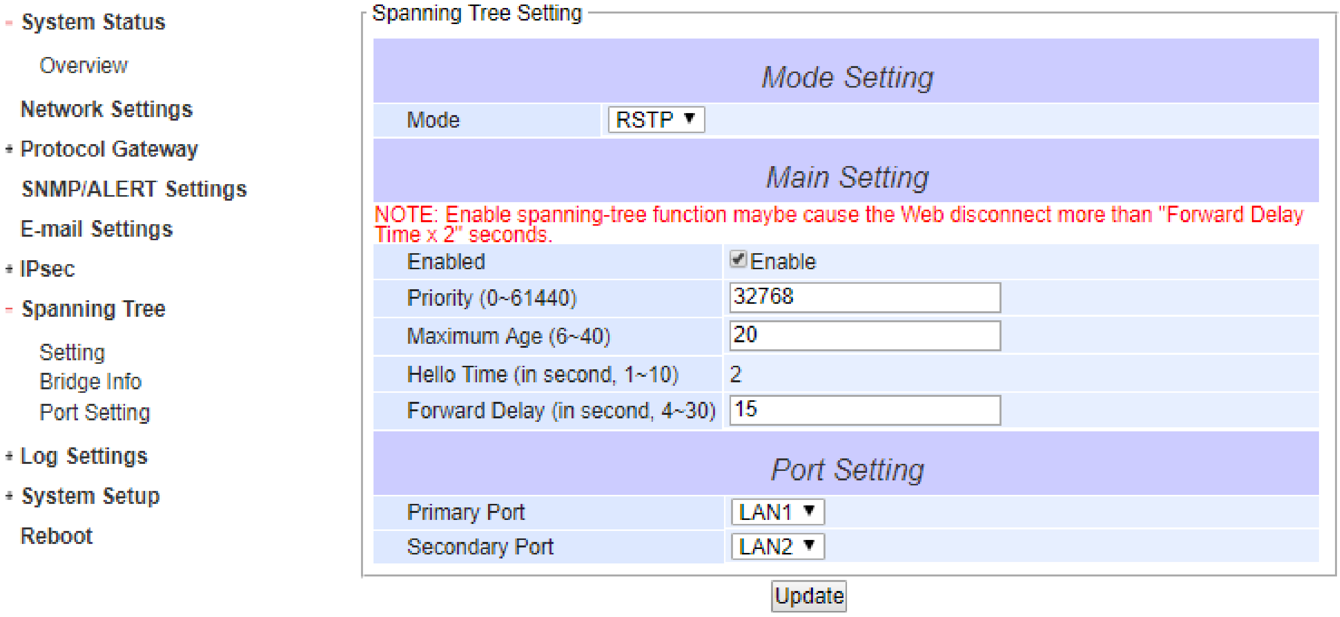


Figure 4.44 Spanning Tree Menu

4.11.1 *Spanning Tree's Setting*

Figure 4.45 shows an example of **Setting** web page of **Spanning Tree** menu. The **Spanning Tree Setting** page is divided into three parts which are **Mode Setting**, **Main Setting**, and **Port Setting**. For PS4000/8000/16000, the user can only select one spanning tree mode, which is the **RSTP** (Rapid Spanning Tree Protocol) under the **Mode Setting**. The user can enable or disable spanning tree protocol under the **Main Setting** by checking the box behind the **Enabled** option. Note that when Enabled option is checked, the rest of the fields will become active. Then, the user can configure the **Prioirty**, **Maximum Age**, **Hello**

Time, and **Forward Delay** or can leave the default setting values for each of these options. Under the **Port Setting** part, the user can select two different ports for **Primary Port** and **Secondary Port** options from the drop-down list. After configuring the spanning tree's parameters, please click **Update** button at the end of the page to allow the change to take effect. The description of each parameter is summarized in Table.



Spanning Tree Setting

Mode Setting

Mode: RSTP ▼

Main Setting

NOTE: Enable spanning-tree function maybe cause the Web disconnect more than "Forward Delay Time x 2" seconds.

Enabled	☑ Enable
Priority (0~61440)	32768
Maximum Age (6~40)	20
Hello Time (in second, 1~10)	2
Forward Delay (in second, 4~30)	15

Port Setting

Primary Port	LAN1 ▼
Secondary Port	LAN2 ▼

Figure 4.45 Setting Web Page of Spanning Tree

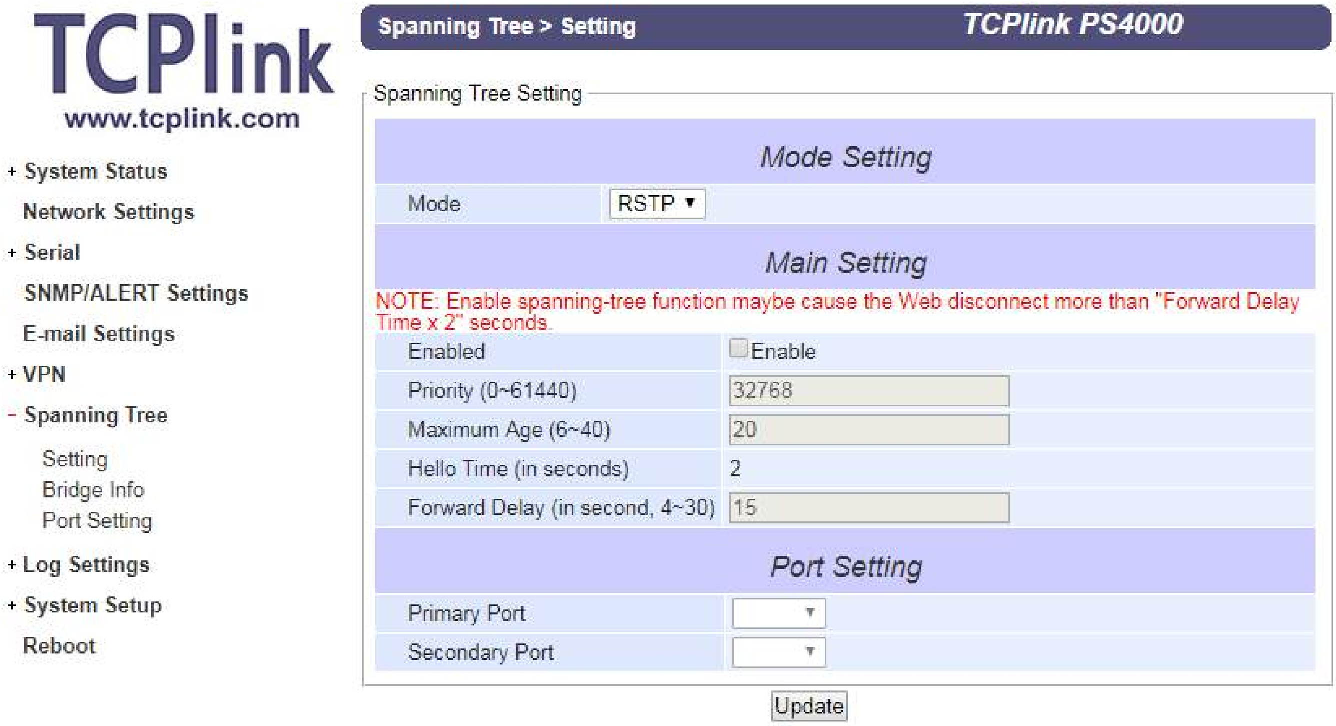
Table 4.2 Descriptions of Spanning Tree Parameters

Label	Description	Default Factory
Mode	Mode of Spanning Tree Protocol to be enabled on PS4000/8000/16000	RSTP
Enabled	Check the box to enable spanning tree functionality.	Disable
Priority	Enter a number to set the device priority**.** The value is in between 0 and 61440**.** The lower number gives higher priority**.**	32768
Maximum Age	Maximum expected arrival time for a hello message**.** It should be longer than Hello Time**.**	20
Hello Time	Hello time interval is given in seconds. The value is in between 1 to 10.	2
Forward Delay	Specify the time spent in the listening and learning states in seconds. The value is in between 4 to 30.	15
Primary Port	Spanning tree's primary port	LAN1
Secondary Port	Spanning tree's secondary port	LAN2

Note: To disable spanning tree function on PS4000/8000/16000, the user can uncheck the **Enable** option and then click **Update** butoon.

4.11.2 *Spanning Tree's Bridge Info*

Bridge Info (information) provides the current configured parameters of spanning tree protocol as shown in Figure 4.46. Note that this page will not display any data on all fields if the RSTP was not enabled in the Spanning Tree's **Setting** web page. The information is further divided into two parts: **Root Information** and **Topology Information**. To check the latest information, please click on the **Refresh** button at the end of the page. Table 4.3 and Table 4.4 summarize the descriptions of each entry in the root information table and topology information table, respectively.



Spanning Tree Setting

Mode Setting

Mode: RSTP ▾

Main Setting

NOTE: Enable spanning-tree function maybe cause the Web disconnect more than "Forward Delay Time x 2" seconds.

Enabled	□ Enable
Priority (0~61440)	32768
Maximum Age (6~40)	20
Hello Time (in seconds)	2
Forward Delay (in second, 4~30)	15

Port Setting

Primary Port: ▾

Secondary Port: ▾

Update

Figure 4.46 Bridge Info Web Page of Spanning Tree

Table 4.3 Bridge’s Root Information

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

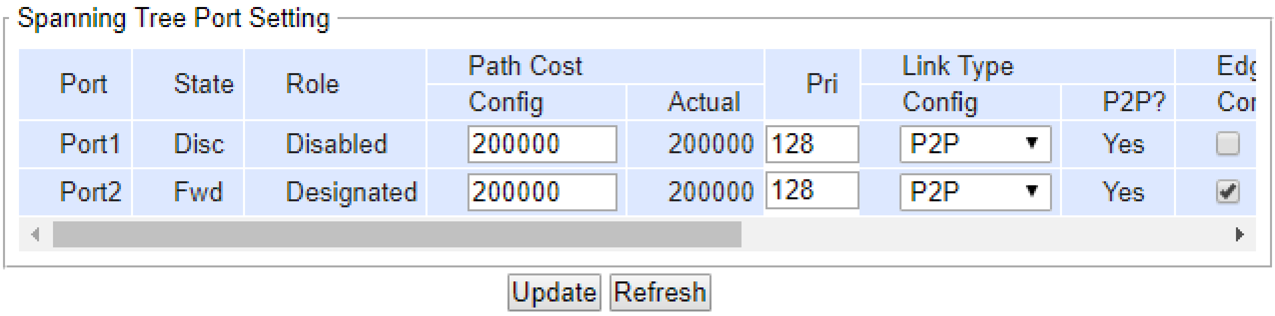
Table 4.4 Bridge's Topology Information

Label	Description	Factory Default
Root Port	A forwarding port that is the best port from non-root bridge/switch (PS4000/8000/16000) to root	-

	bridge/switch. Note that for a root switch there is no root port.	
Num. of Topology Change	The total number of spanning topology change over time.	0
Last TC time ago	The duration of time since last spanning topology change.	-

4.11.3 *Spanning Tree's Port Setting*

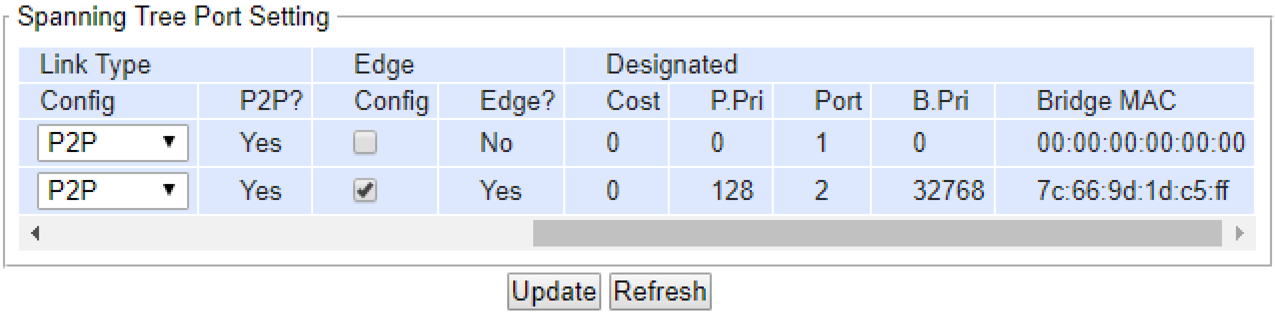
Spanning Tree's **Port Setting** shows the configured value of spanning tree protocol for each port, as shown in Figure 4.47 and Figure 4.48. The configured information for each port is **state**, **role**, **path cost**, **path priority**, **link type**, **edge**, **cost**, and **designated information**. To check the latest update on the statistics, please click on the **Refresh** button. Table 4.5 summarizes the descriptions of spanning three port setting. If **Spanning Tree** is enabled, the table of **Spanning Tree Port Stting** becomes editable and four parameters (**Path Cost** (**Config**), path priority (**Pri**), **Link Type** (**Config**) and **Edge** (**Config**)) can be adjusted on this page. The user can use the **Update** button to save the settings.



Spanning Tree Port Setting

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

Figure 4.47 Spanning Tree Port Setting (Part 1)



Spanning Tree Port Setting

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

Figure 4.48 Spanning Tree Port Setting (Part 2)

Table 4.5 Descriptions of Spanning Tree Port Setting

Label	**Description**	**Factory Default**
Port	The name of the PS4000/8000/16000's port	-
State	State of the port: **'Disc':** Discarding - No user data is sent over the port.	N/A

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

Note:

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

Table 4.6 Default Path Cost for RSTP

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

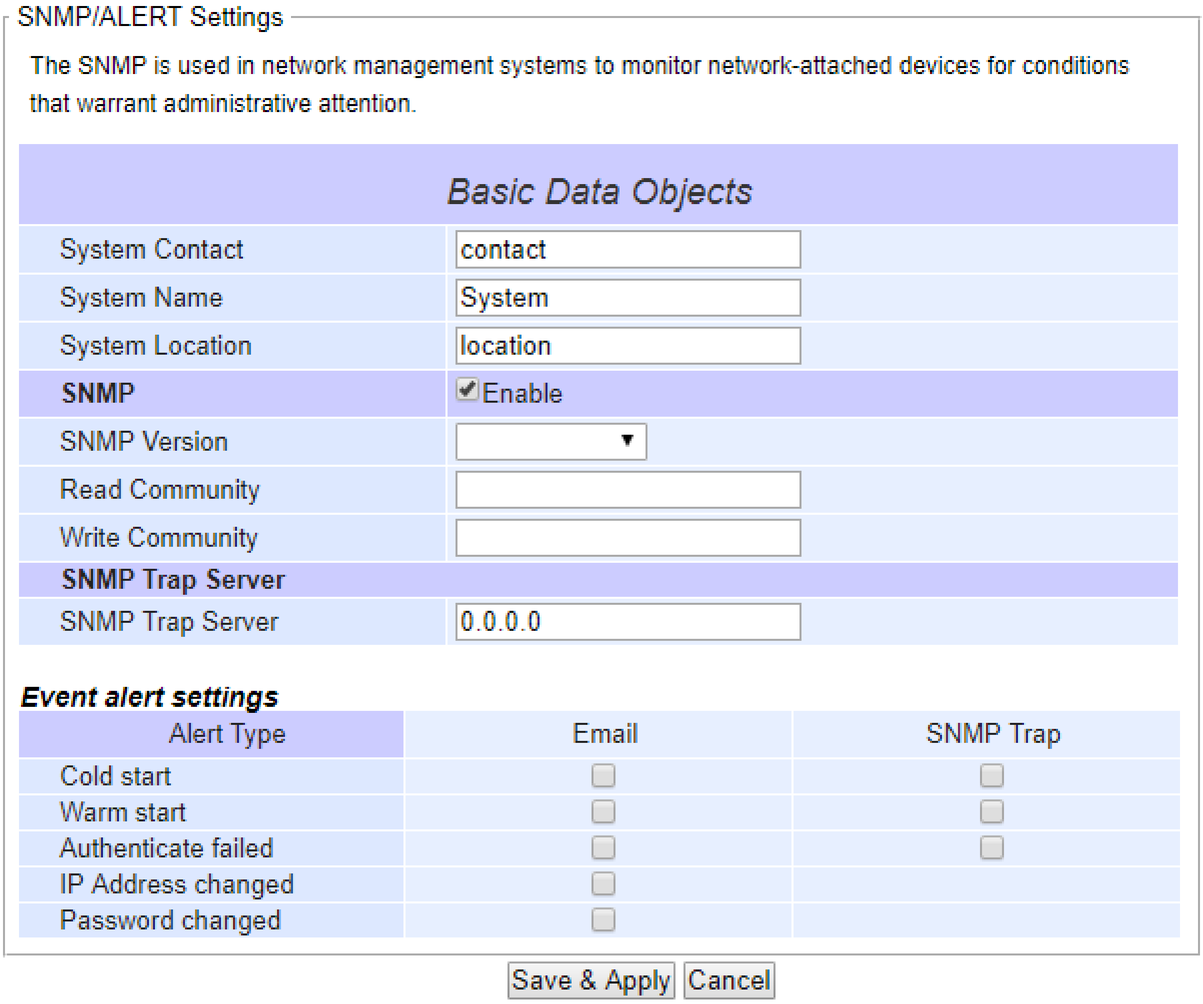
2. The sequence of events to determine the best received BPDU (which is the best path to the root).

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

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

4.12 *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 4.49 allows user to configure PS4000/8000/16000 device so that it can be viewed by third-party SNMP software, and allows PS4000/8000/16000 to send alert events to administrator and SNMP trap server.



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 Version	▼
Read Community	
Write Community	
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 4.49 SNMP/Alert Settings Web Page

PS4000/8000/16000 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 show up as depicted in Figure 4.49. By filling in the passphrase for the "**Read Community**", PS4000/8000/16000 device allows other network management software to read its information. By filling in the passphrase for the "**Write Community**", PS4000/8000/16000 device allows other network management software to read/modify its information. The default PS4000/8000/16000's SNMP Community Strings (or passphrases) for **Read Community** and **Write Community** as shown in Figure 4.49 are "public" and "private", respectively.

Additionally, you can setup a **SNMP Trap Server** in the network to receive and collect all alert messages from PS4000/8000/16000. To configure PS4000/8000/16000 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 4.49. Note that any changes in these settings will take effect after the PS4000/8000/16000 device is restarted.

Under the **SNMP Trap Server** part, there is a list of **Alert Type** under **Event alert settings** box in Figure 4.49. 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 PS4000/8000/16000 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 PS4000/8000/16000 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 PS4000/8000/16000 as listed in Figure 4.49. However, some event can only be reported by e-mail. These alerts are useful for security control or security monitoring of the PS4000/8000/16000 device:

- **Cold Start**: This event occurs when there is a power interruption.
- **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 PS4000/8000/16000.
- **IP Address Changed**: This event occurs when the PS4000/8000/16000 device's IP address is changed.
- **Password Changed**: This event occurs when the administrator password is changed.

After finish 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.

4.13 *E-Mail Settings*

When PS4000/8000/16000 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 PS4000/8000/16000 to be able to send an e-mail.

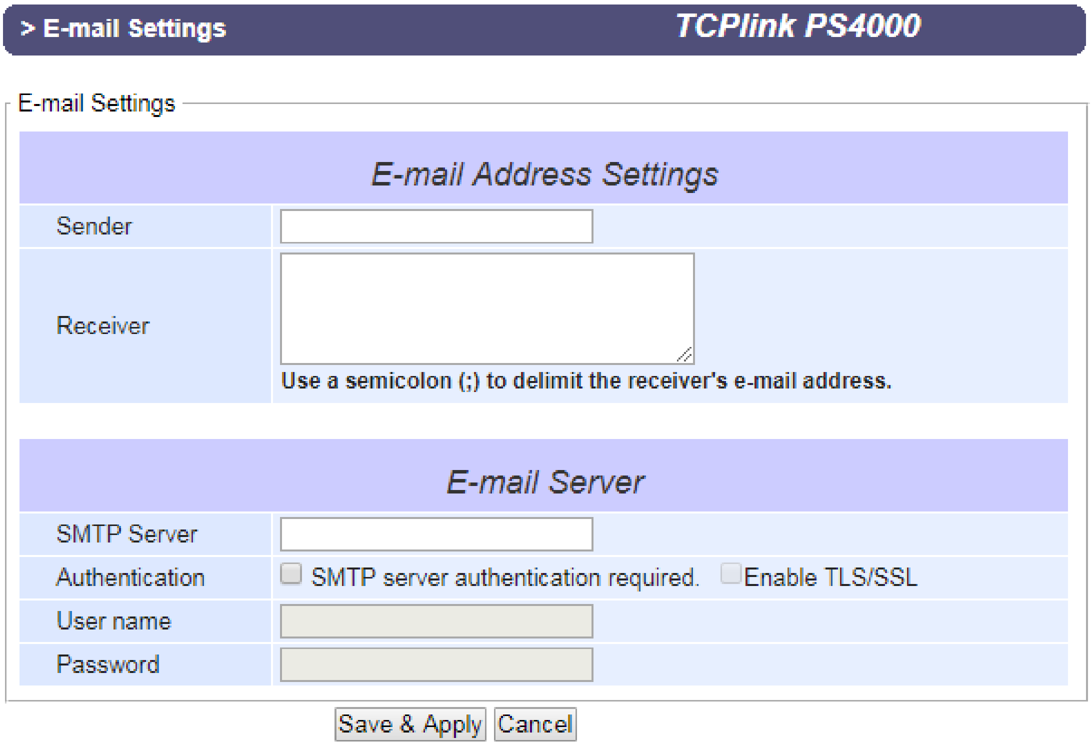
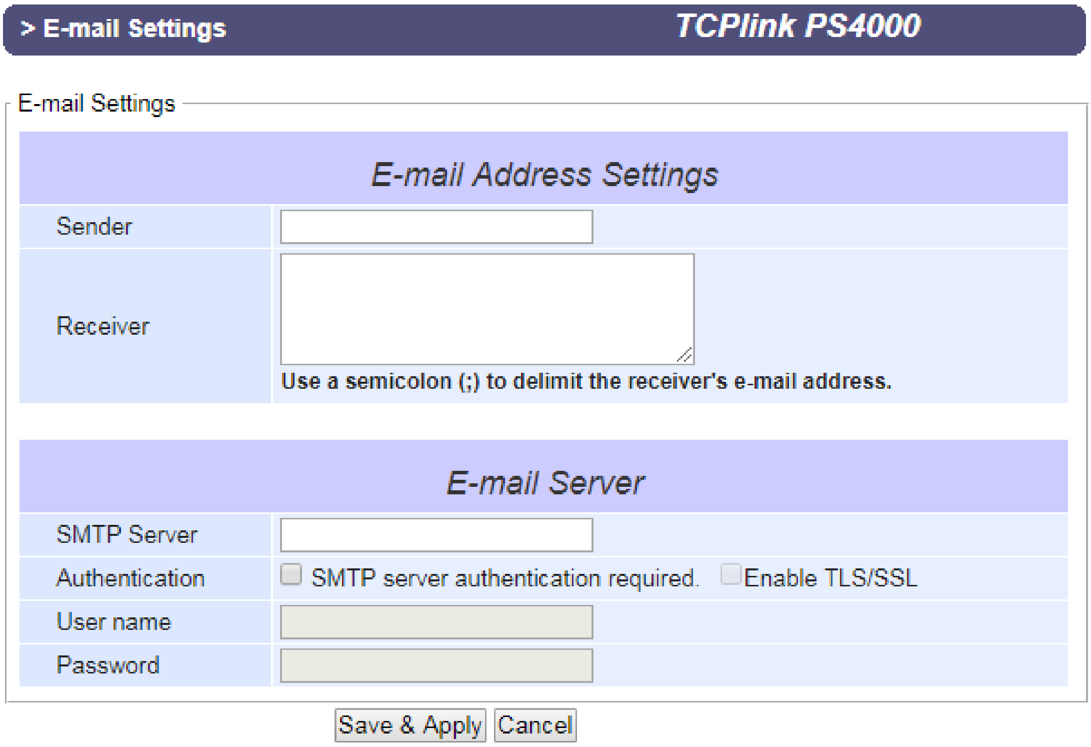


Figure 4.50 shows the **E-mail Settings** page in which there are two configurable parts: **E-mail Address Settings** and **E-mail Server**. First for the **E-mail Address Settings** part, a **Sender**'s e-mail address is required to be filled in the **Sender**'s text box which will be used in the **From** 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 TCPlink PS4000

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	□ SMTP server authentication required. □ Enable TLS/SSL
User name	
Password	

Figure 4.50 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. After enabling this 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 PS4000/8000/16000 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 o .

After finish 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.

4.14 *Log Settings*

Under the **Log Settings** menu of web interface of PS4000/8000/16000 series Industrial Serial Device Server, you can configure various data logging for the device. Figure 4.51 lists the sub-menu under the **Log Settings**. It consists of **System Log Settings**, **COM Log Settings**, **Event Log**, and **COM Datalog.** Each of this sub-menu will be described in the following subsections.

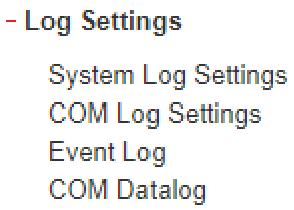
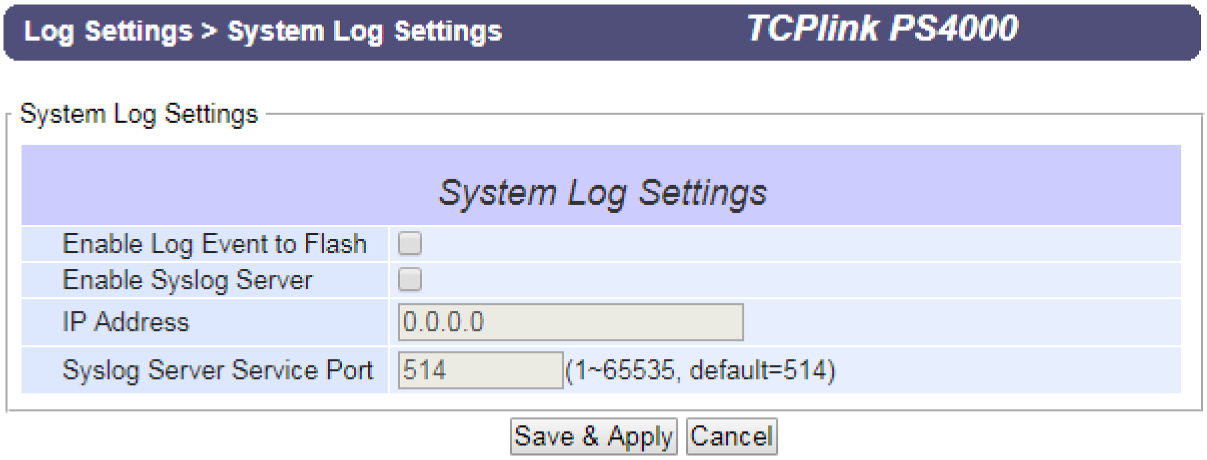


Figure 4.51 Log Settings Menu

4.14.1 *System Log Settings*

The Syslog function is turned on by default and cannot be turned off for PS4000/8000/16000. It is used to keep log for system events and report to an external Syslog server if necessary. Figure 4.52 shows the **System Log Settings** page under the **Log Settings** menu. Description of each option is provided as follows.


Log Settings > System Log Settings TCPlink PS4000

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)

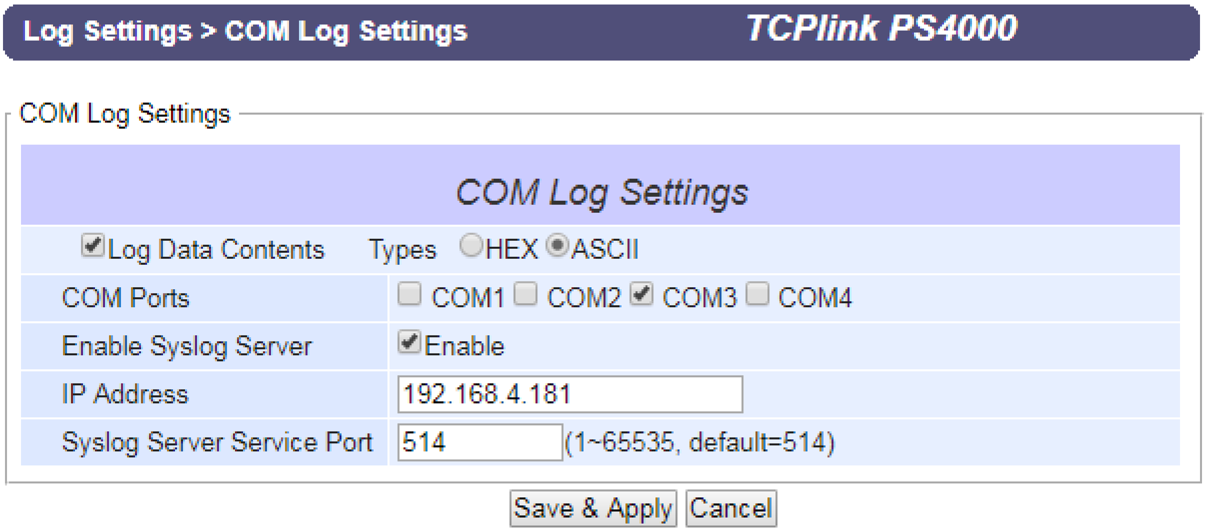
Figure 4.52 Log Settings Web Page under Log Settings

- **Enable Log Event to Flash**: When the check box is enabled, PS4000/8000/16000 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 PS4000/8000/16000 to send Syslog events to the remote Syslog server with the specified IP address (next option). All the data sent/received from serial interface will be logged and sent to Syslog Server.
- **Syslog Server IP**: 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 finish 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.

4.14.2 *COM Log Settings*

Transmitted data through COM port could be logged for recording or debugging purposes. Additionally, the logs could be reported to an external Syslog server as well. Figure 4.53 shows the **COM Log Settings** page under the **Log Settings** menu. Description of each option is explained as follows.



Log Settings > COM Log Settings TCPlink PS4000

COM Log Settings

COM Log Settings

☑Log Data Contents Types ○HEX ●ASCII

COM Ports	□ COM1 □ COM2 ☑ COM3 □ COM4
Enable Syslog Server	☑Enable
IP Address	192.168.4.181
Syslog Server Service Port	514 (1~65535, default=514)

Figure 4.53 COM Log Settings Web Page under System Setup

- **Log Data Contents**: if this option is enabled, the COM logging function will log the content's data that is being transmitted and received in raw bytes. If this option is disabled, COM logging function will only log the length of data to reduce system load.

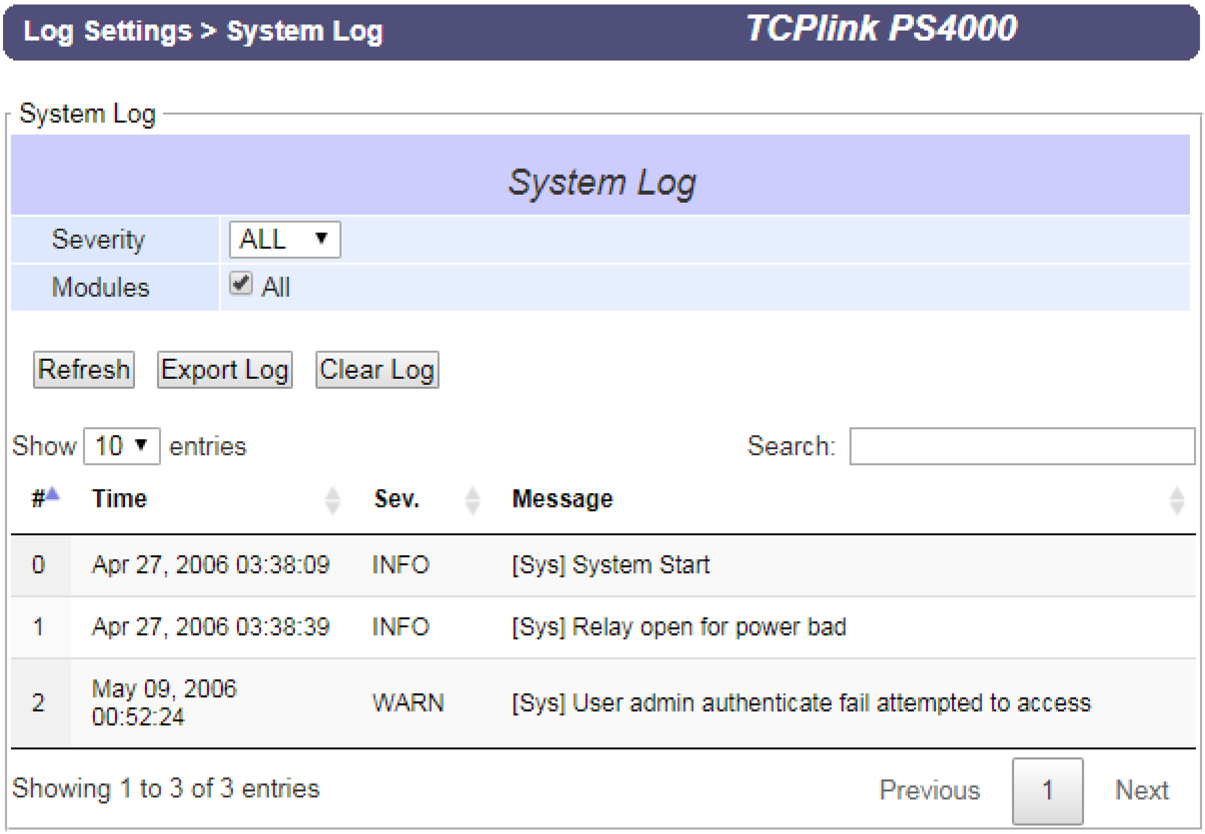
Note: PS4000/8000/16000 can store up to 100 KBytes internally. A request or a response will be in one line, and the data longer than 512 bytes will go into another line. You can retrieve logs by using a **FTP Client.** The FTP login is the same as the WebUI login. Logs are located in **/var/log/logcomxx** (xx is the port number). When the reserved space is full, new logs will replace old logs. We strongly recommend sending COM logs to a remote Syslog server.

- Data **Types**: There are two radio buttons which are hexadecimal (**HEX**) and **ASCII** for user to select the desired logged data's format.
- **COM Ports**: The user can select which port(s) will be logged by checking the corresponding boxes.
- **Enable Syslog Server**: Enabling this option would allow user to send COM logs to a remote Syslog server. It is possible to send COM logs to the same Syslog server used previously for event logging (See Section 4.14.1).
- **IP Address**: When the Syslog Server is enabled in the previous option, please specify the remote Syslog server's IP address 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 finish configuring the **COM 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 **COM Log Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button.

4.14.3 *Event Log*

This page displays the current event log or system log stored in the PS4000/8000/16000 device**.** Figure 4.54 shows an example of logged event**.** Each record of the **System Log** consists of **Time**, **Severity**, and **Message** description**.**



System Log

Severity: ALL ▾

Modules: ☑ All

Show 10 ▾ entries

Search:

#	Time	Sev.	Message
0	Apr 27, 2006 03:38:09	INFO	[Sys] System Start
1	Apr 27, 2006 03:38:39	INFO	[Sys] Relay open for power bad
2	May 09, 2006 00:52:24	WARN	[Sys] User admin authenticate fail attempted to access

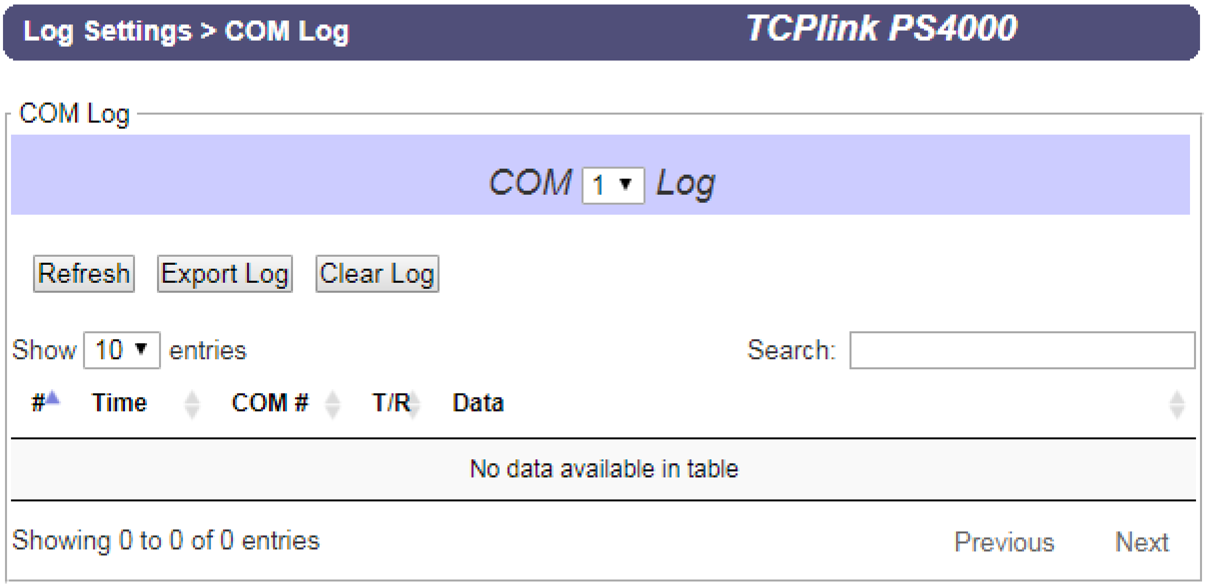
Showing 1 to 3 of 3 entries

Figure 4.54 System Log Web Page under System Setup

At the end of the **System Log** page, there are three 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 System Log**, and **Clear System Log**. To display the latest event, you can click on **"Refresh"** button. When you click on the Export System Log button, a log file will be save on to your PC. By clicking on "**Clear System 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.

4.14.4 *COM Datalog*

This page displays the current COM data log stored in the device. The desired **COM** port number can be selected from the **COM x Log** drop-down list in Figure 4.55, which allows it to display logs from different COM ports. An example of **COM 1 Log** is shown in Figure 4.55. Each record of the log consists of **Time**, **COM Index**, Direction (**T/R**) and **Data**.



#	Time	COM #	T/R	Data
No data available in table				

Showing 0 to 0 of 0 entries

Figure 4.55 COM Datalog Web Page under Log Settings

Under the COM x Log header, there are three buttons: **Refresh**, **Export Data Log**, and **Clear Data Log**. First, the **Refresh** button can be used to update the COM Log table below with the latest information. Second, the **Export Data Log** button will enable the user to save the log data onto their PC. The default file name of the exported data log will be “**DataLog.txt**”. Finally, the **Clear Data Log** button will clear all events stored in the device and the COM Datalog will be empty with a message “No data available in table”. At the end of the **COM Datalog** 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 previous page of the log and click on the **“Next”** link to go to the next page**.**

4.15 *System Setup*

Under the **System Setup** menu of web interface of PS4000/8000/16000 series Industrial Serial Device Server, you can perform a number of administration tasks for the device. Figure 4.56 lists the sub-menu under the **System Setup**. It consists of **Date/Time Settings**, **Admin Settings**, **Firmware Upgrade**, **Backup/Restore Setting**, and **Ping**. Each of this sub-menu will be described in the following subsections.

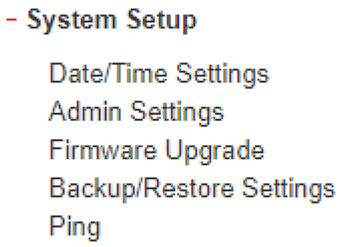
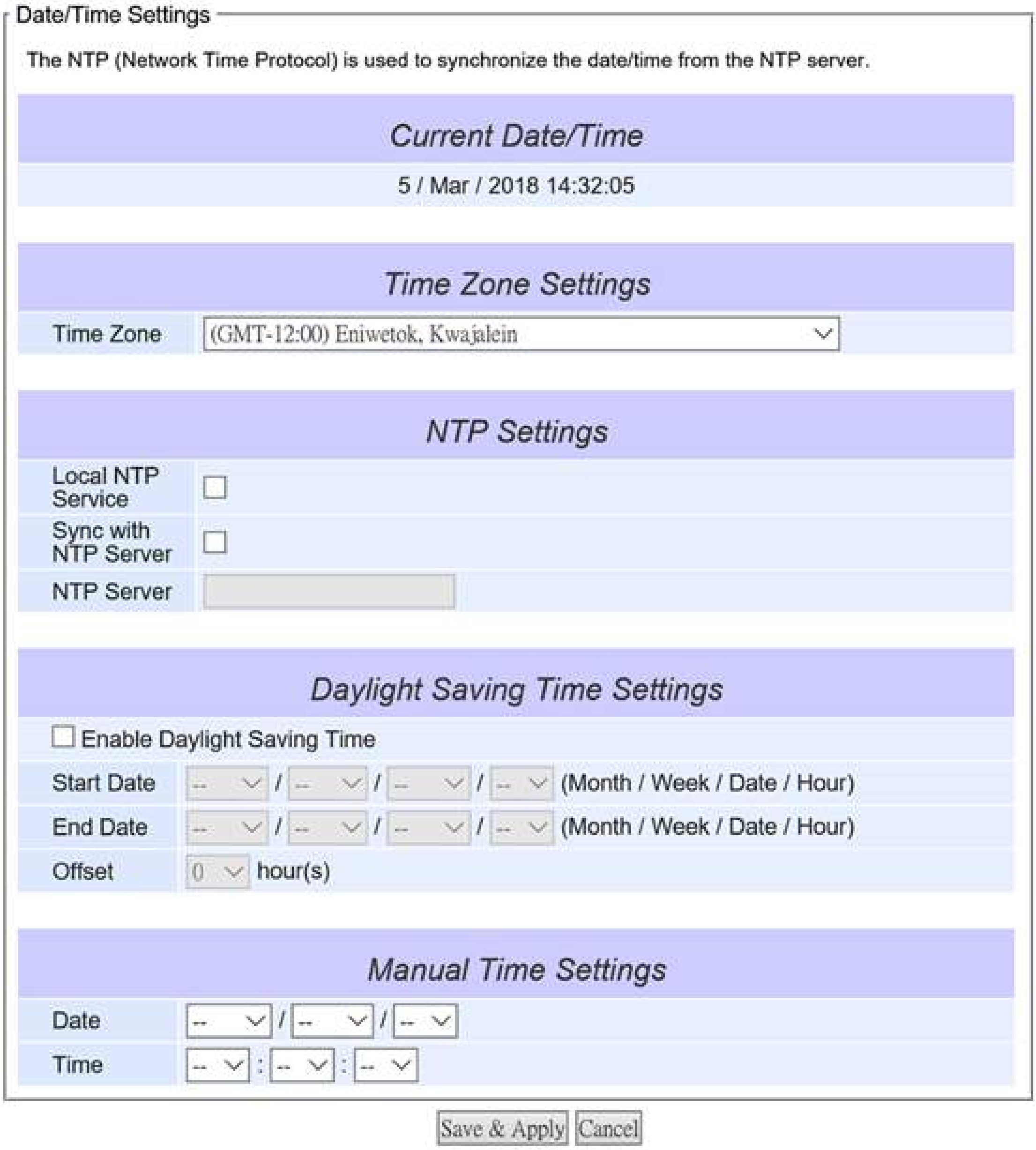


Figure 4.56 System Setup Menu

4.15.1 *Date/Time Settings*

Date and time can be set manually or using Network Time Protocol (NTP) to automatically synchronize date and time of PS4000/8000/16000 with a Time Server. Figure 4.57 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 Sttings**. In this part, you can either enable the local NTP service inside PS4000/8000/16000 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 o). 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 4.57.



Date/Time Settings

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

Current Date/Time

5 / Mar / 2018 14:32:05

Time Zone Settings

Time Zone: (GMT-12:00) Eniwetok, Kwajalein

NTP Settings

Local NTP Service: □

Sync with NTP Server: □

NTP Server:

Daylight Saving Time Settings

□ Enable Daylight Saving Time

Start Date: -- / -- / -- / -- (Month / Week / Date / Hour)

End Date: -- / -- / -- / -- (Month / Week / Date / Hour)

Offset: 0 hour(s)

Manual Time Settings

Date: -- / -- / --

Time: -- : -- : --

Figure 4.57 Date/Time Settings Web Page under System Setup

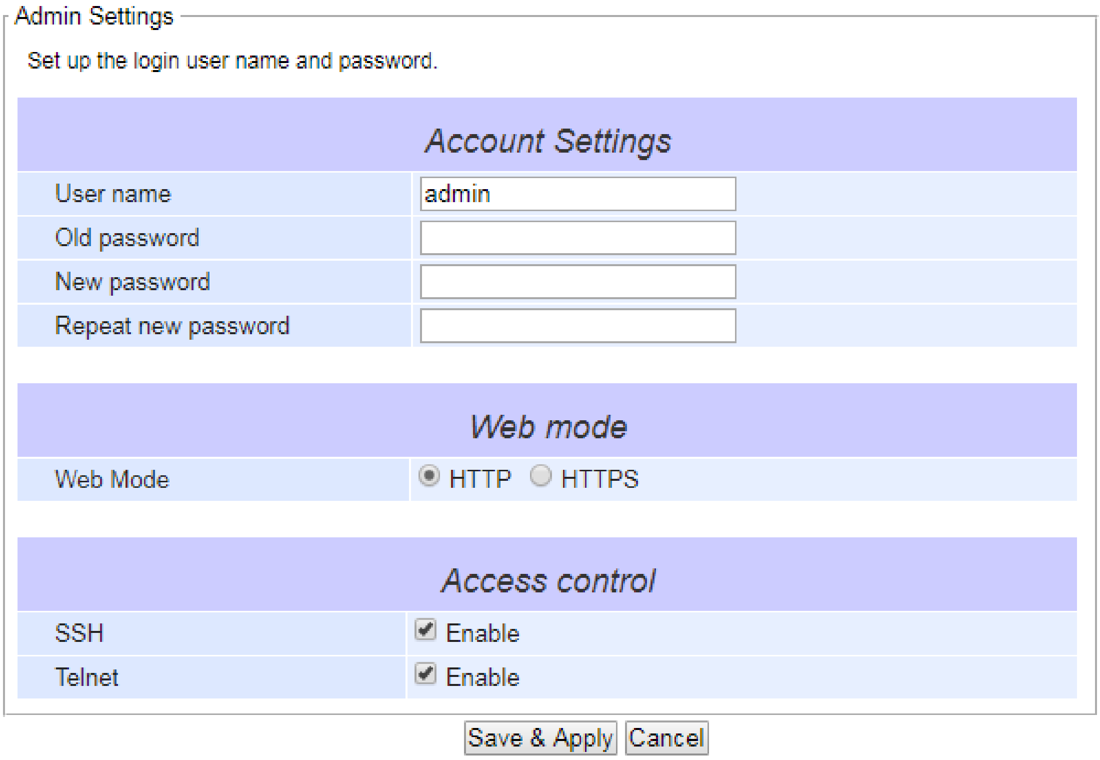
Attention

It is also important to setup Default Gateway and DNS Servers in the Network Settings properly (See Section o), so PS4000/8000/16000 can lookup DNS names and point to the proper NTP server.

After finish 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.

4.15.2 *Admin Settings*

The PS4000/8000/16000 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 4.58. At the end 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).



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

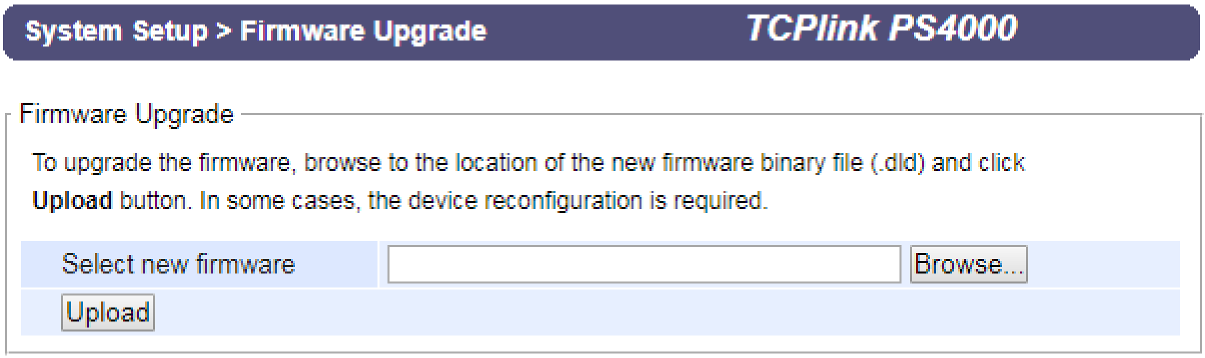
Figure 4.58 Admin Settings Web Page under System Setup

After finish 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 PS4000/8000/16000 as shown in Figure 4.7. You must re-enter the username and the password to login to the PS4000/8000/16000. 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.

4.15.3 *Firmware Upgrade*

Updated firmware for PS4000/8000/16000 is provided by TCPlink from time to time (for more information please visit TCPlink 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 PS4000/8000/16000, please downloaded the latest firmware for your PS4000/8000/16000 model from the download tab on the PS4000/8000/16000 product page or from the Download page under the Support link on TCPlink'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 4.59 below to find and choose the new firmware file. Then, 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 PS4000/8000/16000 device will then proceed to restart itself. In some cases, you might require to re-configure your PS4000/8000/16000 device. To restore your backup configuration from a file, please see the procedure in the next subsection.



System Setup > Firmware Upgrade
TCPlink PS4000

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.

Figure 4.59 Firmware Upgrade Web Page under System Setup

Note: if the firmware upgrade process fails and the device becomes unreachable, please follow the TFTP recovery procedure in Chapter 8 on Emergency System Recovery at the end of this manual.

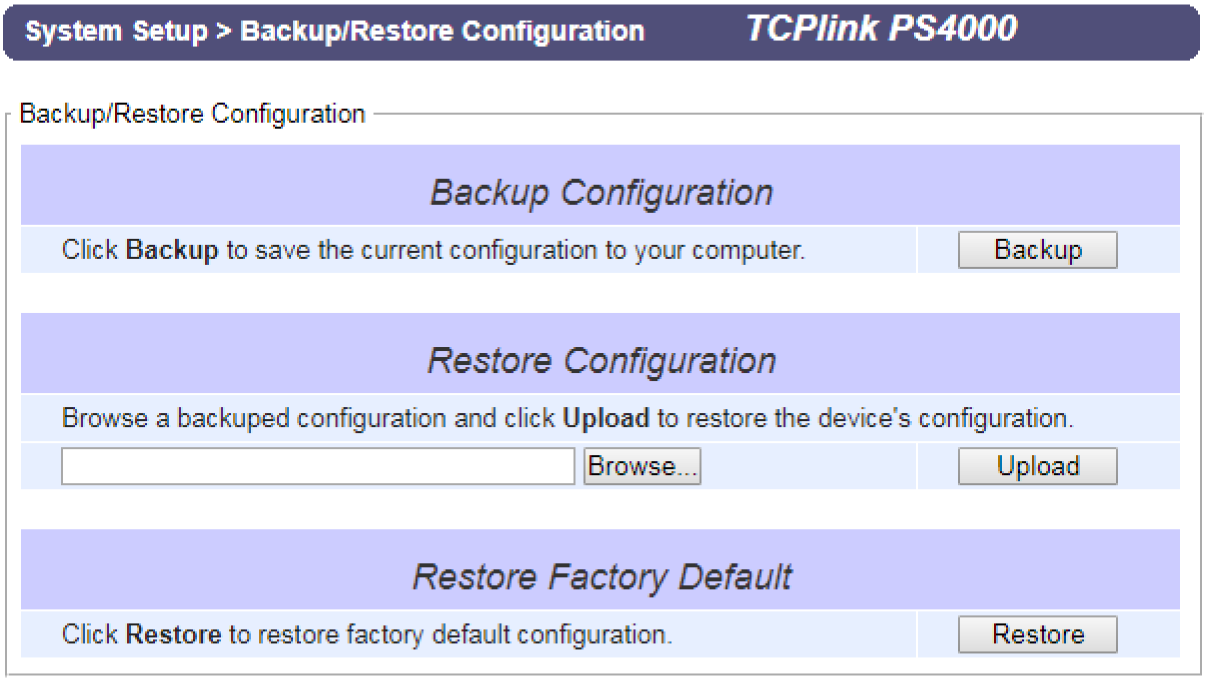
4.15.4 *Backup/Restore Settings*

Once all the configurations are set and the device is working properly, the user should back up the current configuration of PS4000/8000/16000. 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 PS4000/8000/16000 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 4.60, and a 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 TCPlink 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 4.60 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 PS4000/8000/16000 device to its factory default configuration, you can click on the **Restore** button under the **Restore Factory Default** section as shown in Figure 4.60.



System Setup > Backup/Restore Configuration TCPlink PS4000

Backup/Restore Configuration

Backup Configuration

Click **Backup** to save the current configuration to your computer.

Restore Configuration

Browse a backuped configuration and click **Upload** to restore the device's configuration.

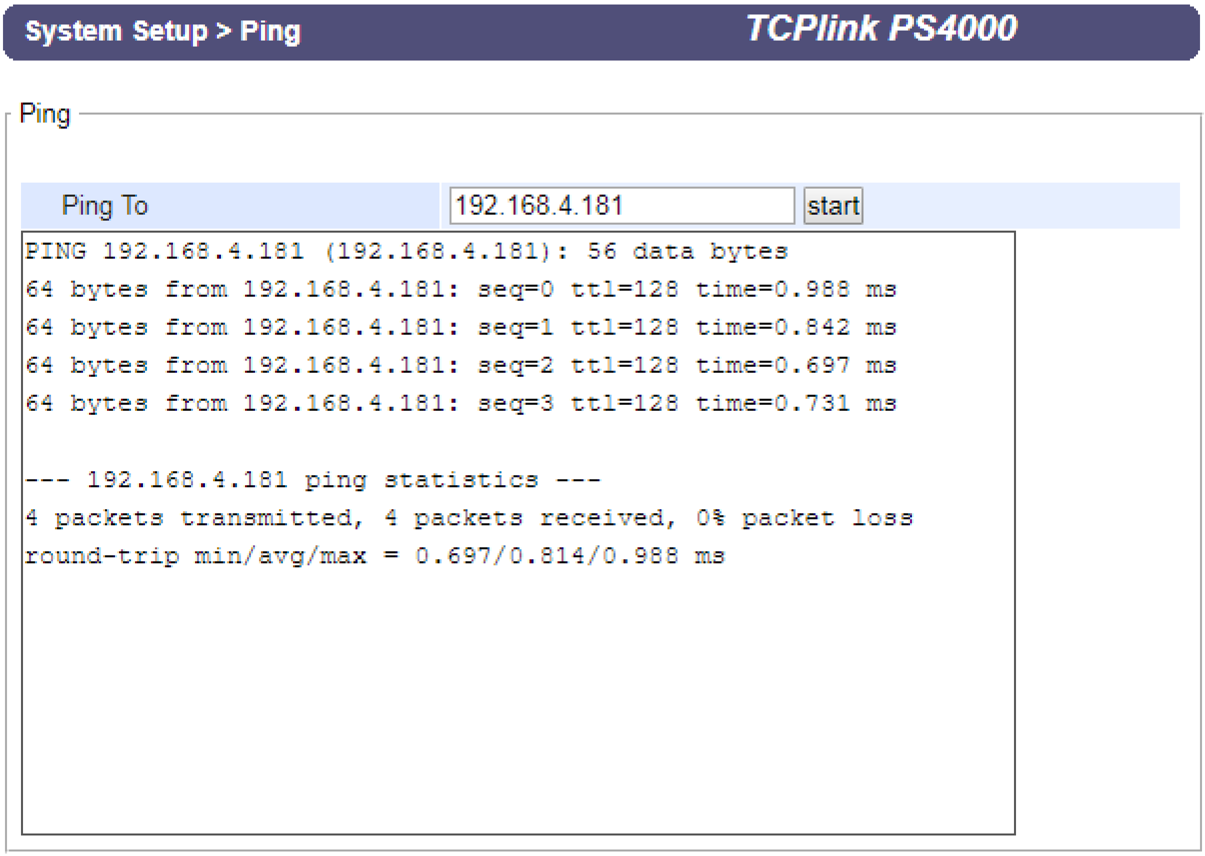
Restore Factory Default

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

Figure 4.60 Backup/Restore Settings Web Page under System Setup

4.15.5 *Ping*

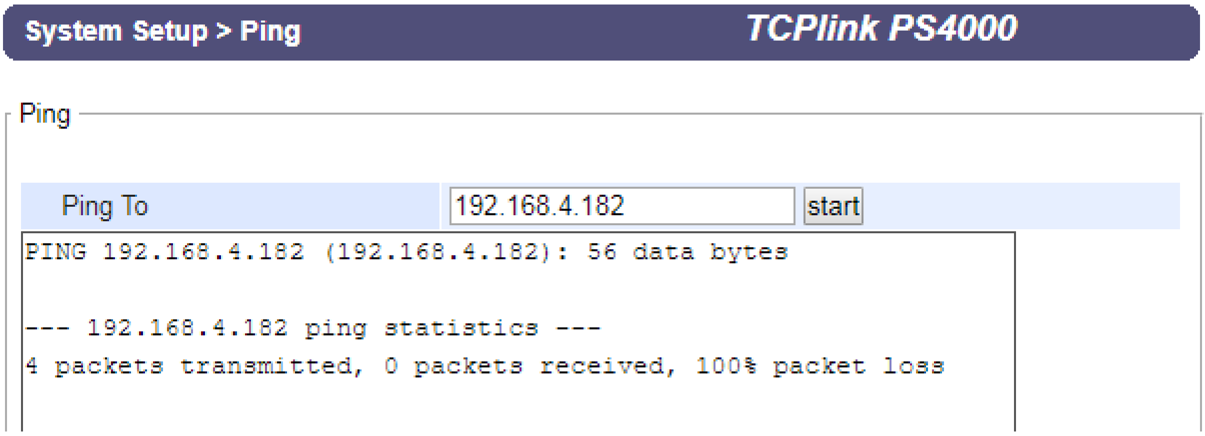
The Web UI of PS4000/8000/16000 has an interface to call **Ping** which is a network diagnostic utility for testing reachability. You can use the **Ping** function to determine whether PS4000/8000/16000 can reach the gateway or other devices in the network. To use the **Ping**, enter a destination IP address in the text box behind the **Ping To** and click **Start** button as shown in Figure 4.61. This process usually takes around 20 seconds. Figure 4.61 represents a successful ping without packet loss from PS4000/8000/16000 to the address 10.0.50.101 and back, while Figure 4.62 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 192.168.4.181

```
PING 192.168.4.181 (192.168.4.181): 56 data bytes
64 bytes from 192.168.4.181: seq=0 ttl=128 time=0.988 ms
64 bytes from 192.168.4.181: seq=1 ttl=128 time=0.842 ms
64 bytes from 192.168.4.181: seq=2 ttl=128 time=0.697 ms
64 bytes from 192.168.4.181: seq=3 ttl=128 time=0.731 ms

--- 192.168.4.181 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.814/0.988 ms
```

Figure 4.61 Ping Web Page under System Setup



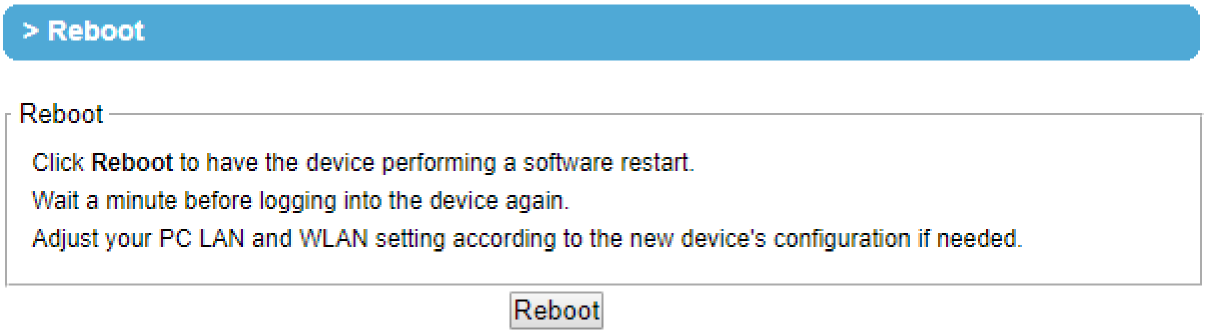
Ping To 192.168.4.182

```
PING 192.168.4.182 (192.168.4.182): 56 data bytes

--- 192.168.4.182 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

Figure 4.62 Unreachable Ping Example

4.16 *Reboot*

To manually reboot the PS4000/8000/16000 device, click on the **“Reboot**” button at the end of the **Reboot** page as shown in Figure 4.63. 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 PS4000/8000/16000 again



Click **Reboot** to have the device performing a software restart.

Wait a minute before logging into the device again.

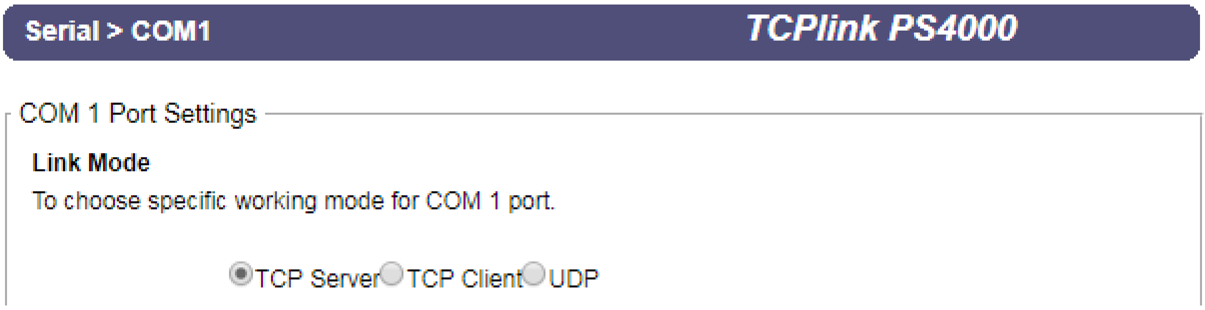
Adjust your PC LAN and WLAN setting according to the new device's configuration if needed.

Figure 4.63 Reboot Web Page

5 Link Modes and Applications

5.1 *Link Mode Configuration*

PS4000/8000/16000 series supports three different **Link Modes** which are **TCP Server**, **TCP Client**, and **UDP**. The **Link Mode** describes the role of PS4000/8000/16000 and the connection between PS4000/8000/16000 device and other remote devices in the network which would like to communicate with serial devices on PS4000/8000/16000's COM port(s). Under the three Link Modes, **TCP Server** mode can support **RAW**, **Virtual COM**, **Reverse Telnet** and **Pair Connection Master** applications, while **TCP Client** mode can only support **RAW**, **Virtual COM** and **Pair Connection Slave** applications. Note that **UDP** mode does not have the same supported applications as the previous two TCP modes. Discussion on how to setup different Link Modes properly will be presented in the following sections. Figure 5.1shows the **Link Mode** options for **COM 1** port which can be found on **COM1** page under **Serial** menu of Web UI (See details on Serial Settings in Section Figure 4.15). Note that on PS4000/8000/16000 model with IO interface will have two COM ports.



COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

● TCP Server ○ TCP Client ○ UDP

Figure 5.1 Link Mode Options for COM1 Port

5.1.1 *Link Mode: Configure PS4000/8000/16000 as a TCP Server*

PS4000/8000/16000 series can be configured as a Transport Control Protocol (TCP) server in a TCP/IP network to listen for an incoming TCP client connection to a serial device. Figure 5.2 depicts an example of a PLC (serial) device which is connected to PS4000/8000/16000 on a serial bus where a remote host computer is sending a request via Ethernet network. After the connection is established between the serial device server (PS4000/8000/16000) and the remote host computer (remote TCP client) in the figure, data can be transmitted in both directions. This also applies whenever the Virtual COM (VCOM) application is running on server mode. Please note that this is the PS4000/8000/16000 device's default link mode.

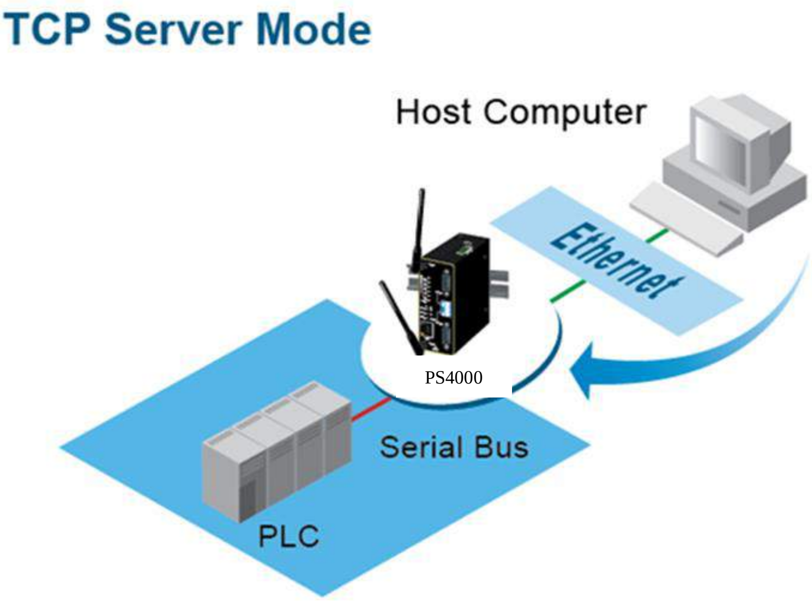
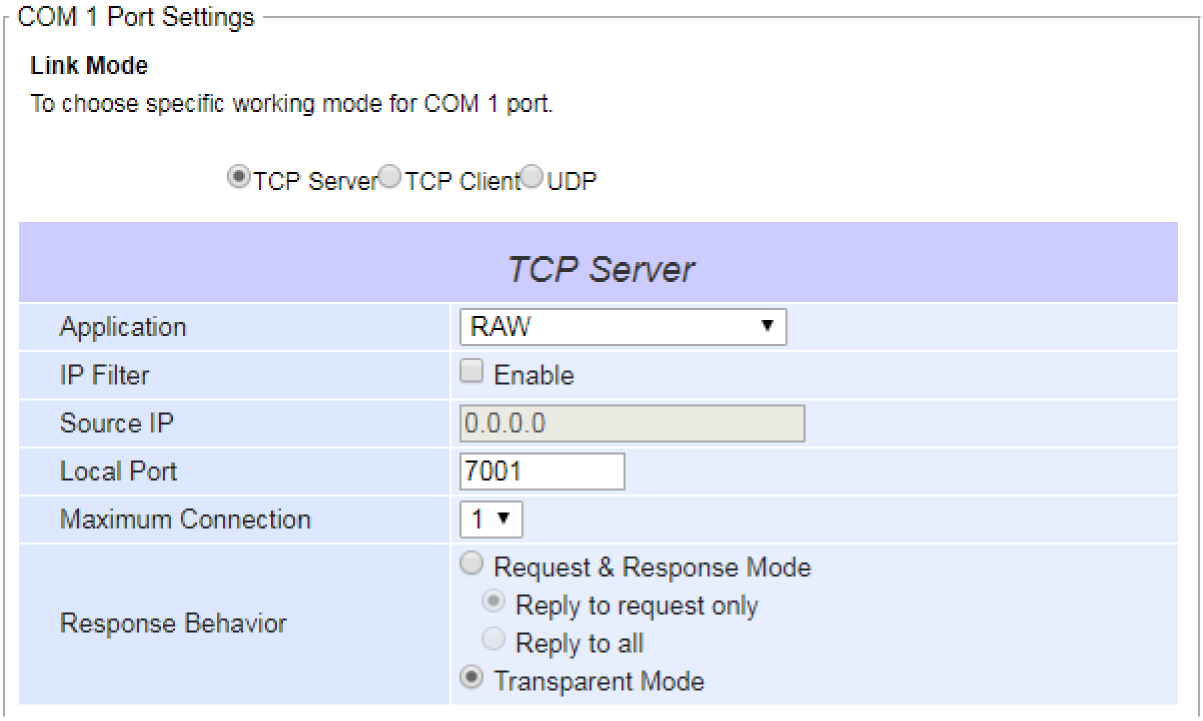


Figure 5.2 PS4000/8000/16000 is set as a TCP Server Link Mode

The default Link Mode of PS4000/8000/16000 is the **TCP Server** mode. Figure 5.3 shows an example of configuration setting for **TCP Server** Link Mode under the **COM 1** page. There are additional connection settings that can be configured as shown in Figure 5.3. By selecting the TCP Server Link Mode, a TCP client program on a remote host computer should be prepared to connect to PS4000/8000/16000. Please follow the following steps to configure connection settings of the Link Mode for each COM port.



COM 1 Port Settings

Link Mode

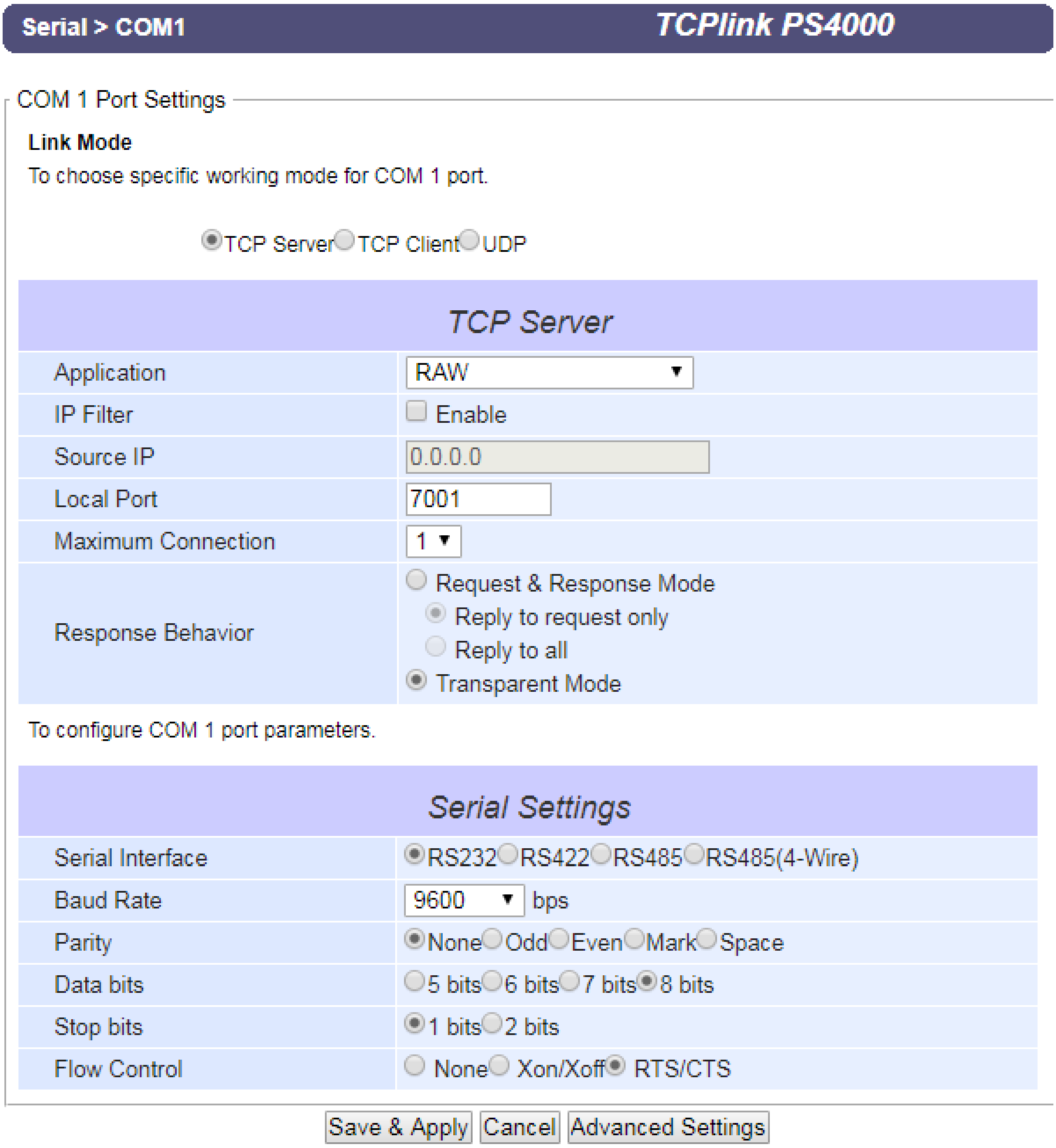
To choose specific working mode for COM 1 port.

● TCP Server ○ TCP Client ○ UDP

TCP Server	
Application	RAW ▼
IP Filter	□ Enable
Source IP	0.0.0.0
Local Port	7001
Maximum Connection	1 ▼
Response Behavior	○ Request & Response Mode ● Reply to request only ○ Reply to all ● Transparent Mode

Figure 5.3 Connection Settings for TCP Server Link Mode

- Click on the “**COM1**” link on the menu frame on the left side of Web UI to go to **COM 1** page as shown in Figure 5.4. Note that if you would like to configure **COM 2** (or any other COM port), please follow the same procedures.



Serial > COM1 TCPlink PS4000

COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

● TCP Server ○ TCP Client ○ UDP

TCP Server	
Application	RAW ▼
IP Filter	□ Enable
Source IP	0.0.0.0
Local Port	7001
Maximum Connection	1 ▼
Response Behavior	○ Request & Response Mode ● Reply to request only ○ Reply to all ● Transparent Mode

To configure COM 1 port parameters.

Serial Settings	
Serial Interface	● RS232 ○ RS422 ○ RS485 ○ RS485(4-Wire)
Baud Rate	9600 ▼ bps
Parity	● None ○ Odd ○ Even ○ Mark ○ Space
Data bits	○ 5 bits ○ 6 bits ○ 7 bits ● 8 bits
Stop bits	● 1 bits ○ 2 bits
Flow Control	○ None ○ Xon/Xoff ● RTS/CTS

Figure 5.4 TCP Server Link Mode Settings under COM 1 Page

- Select **TCP Server** radio button in the Link Mode options. Note that **TCP Server** is the default Link Mode for COM port of PS4000/8000/16000.
- Under the **TCP Server** section, you will find the following options.
  - **Application**: There are 3 different communication applications to choose from here:
    - **RAW**: There is no protocol on this mode which means that the data is passed transparently.
    - **Virtual COM**: The Virtual COM protocol is enabled on the serial device to communicate with a virtualized port from a remote client. It is possible to create a Virtual COM port on Windows/Linux in order to communicate with the serial device as a remote client.
    - **Reverse Telnet**: This application is used to connect the serial device and another serial device (usually a Terminal Server) with a Telnet program. Telnet programs in Windows/Linux usually require special handshaking to get the outputs and formatting to show properly. The PS4000/8000/16000 series will interact with those special commands (CR/LF commands) once Reverse Telnet application is enabled.

        - **Pair Connection Master**: This application is used when the user want to pair two serial devices over the Ethernet network.
    - **IP Filter**: This option will enable the **Source IP** option below. When this option is checked, PS4000/8000/16000 will block or filter out all other IP addresses from accessing the COM port except the one specified in the **Source IP**.
- **Source IP**: This option specifies the remote client's **Source IP** which will be transmitting data to our TCP Server (on PS4000/8000/16000). In other words, our TCP Server will only allow data from this IP address to flow (hence its own name implies Source IP). Note that only one source is allowed.
- **Local Port**: This option specifies the port number that the TCP server (on PS4000/8000/16000) should listen to. It is also used by the remote TCP client to connect to the TCP server. The default local port is 4660. You can enter different port number in this option.
- **Maximum Connection**: This option specifies the maximum number of remote devices/clients (with maximum of 4 clients) that can be connected to the serial device on this COM port.
- **Response Behavior**: This option specifies how PS4000/8000/16000 will proceed or behave when it receives requests from remote connected hosts in which we will have the following options:
    - **Request & Response Mode**: Under this mode, the COM port on PS4000/8000/16000 will hold requests from all other remote connected hosts until the serial device replies or the **Response Interval Timeout** takes into effect to discard it; however, unrequested data sent from the serial device would be forwarded to all connected hosts. Additionally, user can specify how a reply message from the serial device will be sent to the remote connected hosts with two possible options:
        - **Reply to requester only**: The COM port will reply to the remote connected host who has requested the data only.
        - **Reply to all**: A reply is sent to all remote connected hosts.
    - **Transparent mode**: The COM port on PS4000/8000/16000 will forward requests from all remote connected hosts to the serial device immediately and reply to all remote connected hosts once it receives data from the serial device.
- For other **Serial Settings** on the same configuration page, please go to Section 4.6.2 and for **Advanced Settings** please go to Section 4.6.3.
- After finish configuring the **Link Mode**, please scroll down to the bottom of the page and click on **"Save & Apply"** button to save all the changes that you have made.

Note: LINK1 is associated with COM1; LINK2 is associated with COM2, and so on.

5.1.2 *Link Mode: Configure PS4000/8000/16000 as a TCP Client*

PS4000/8000/16000 series can be configured as a TCP client in TCP/IP network to establish a connection to a TCP server on a remote host computer**.** Figure 5.5 depicts an example of two serial card readers connected to two different PS4000/8000/16000 devices where both PS4000/8000/16000 devices are on the same Ethernet network as the remote host computer**.** The arrow in Figure 5.5 indicates the connection request from the client side of TCP connection**.** After the connection is established, data can be transmitted between a serial device (connected to the COM port of each PS4000/8000/16000) and a remote host computer in both directions**.** This also applies to Virtual COM application running in the client mode**.**

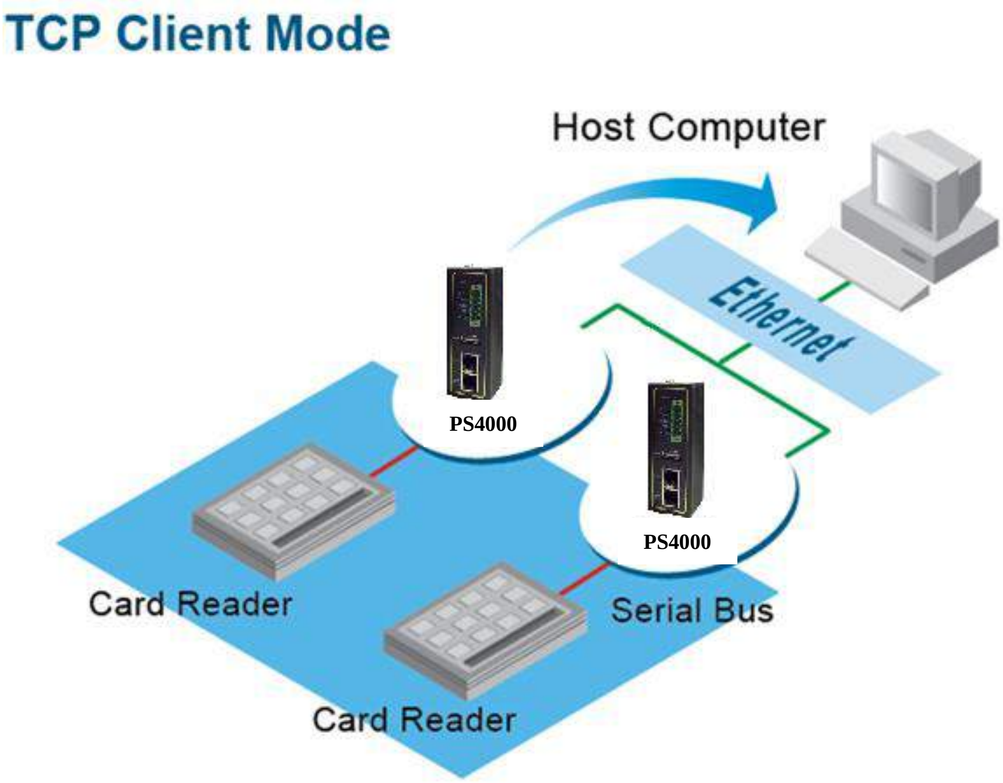
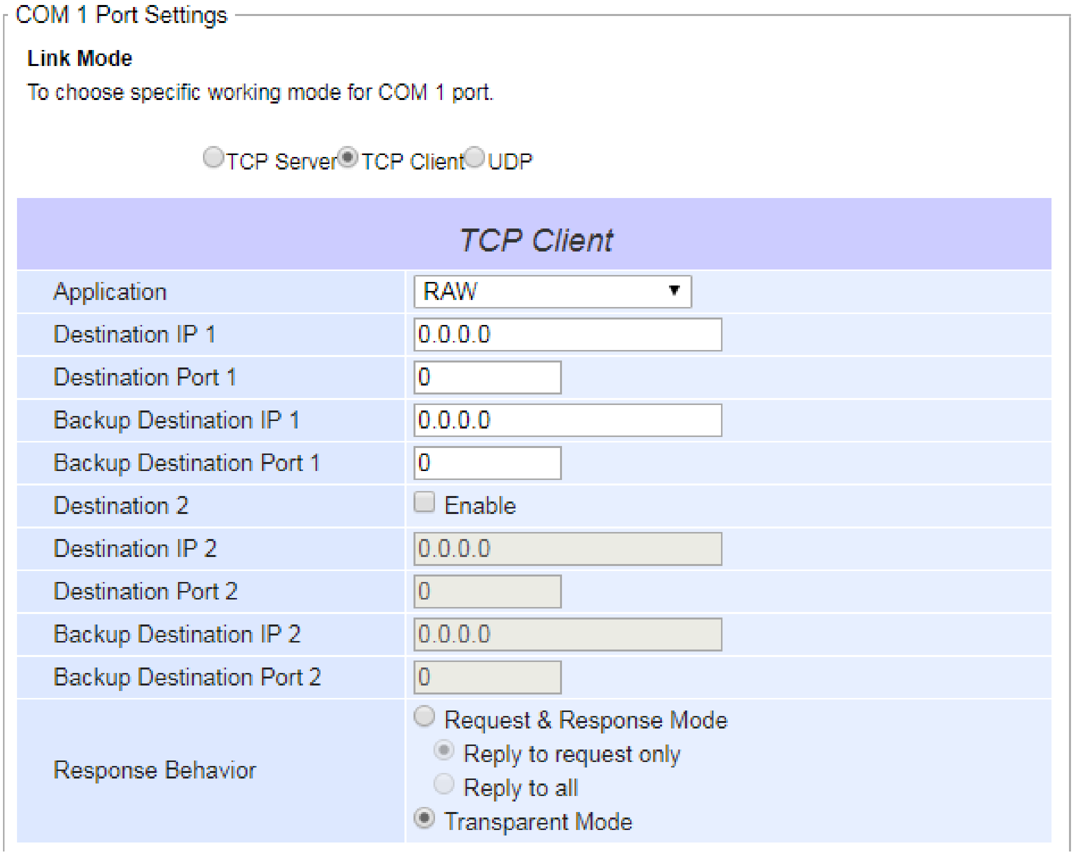


Figure 5.5 Example of PS4000/8000/16000 Configured as TCP Client Link Mode

Figure 5.6 shows an example of configuration setting for **TCP Client** Link Mode under the **COM 1** page. There are additional connection settings that can be configured as shown in Figure 5.7. By selecting the **TCP Client** Link Mode, a TCP server program on a remote host computer should be prepared to accept a connection request from PS4000/8000/16000. Please follow the following steps to configure connection settings of the Link Mode for each COM port.



COM 1 Port Settings

Link Mode

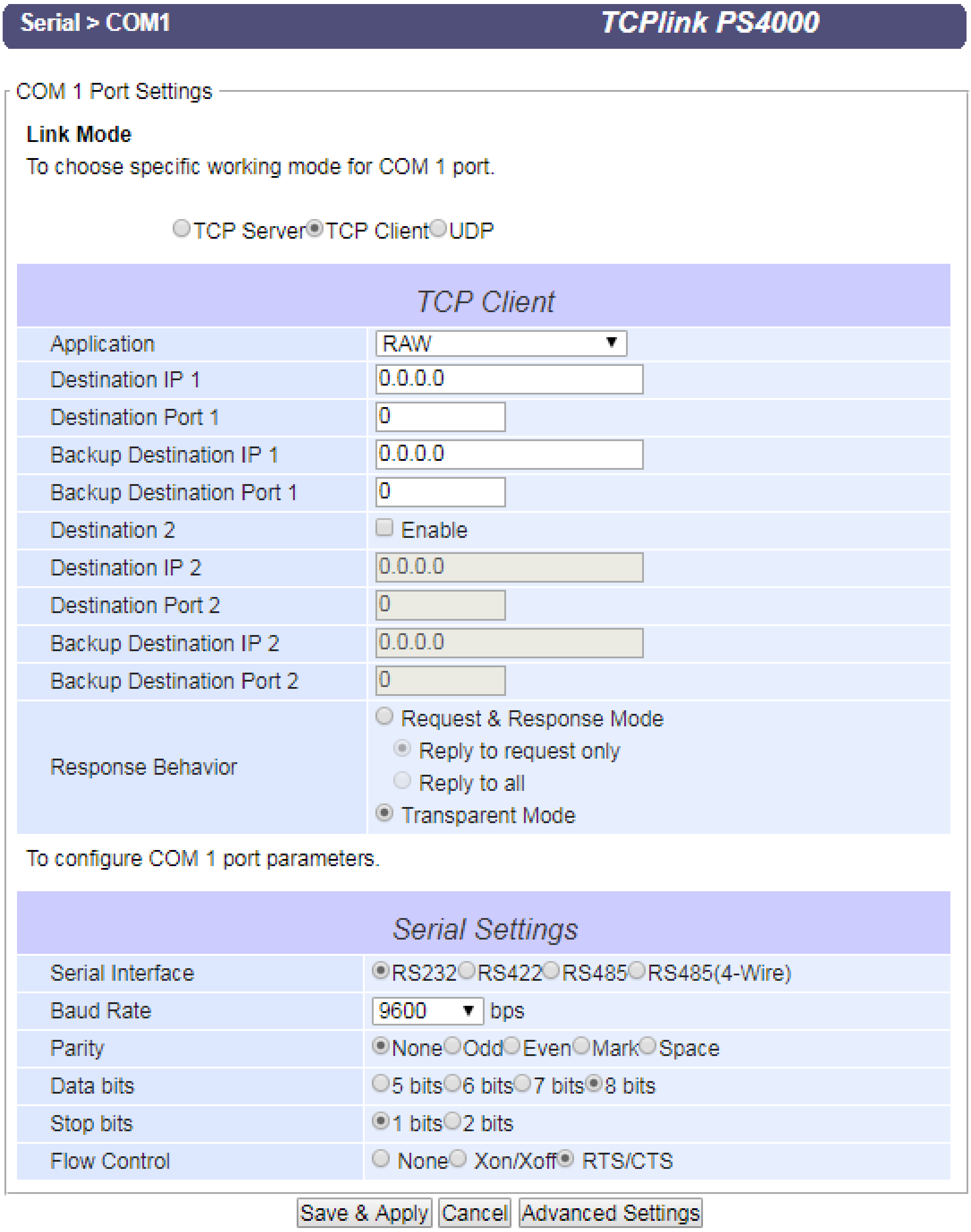
To choose specific working mode for COM 1 port.

○TCP Server ● TCP Client ○UDP

TCP Client	
Application	RAW ▾
Destination IP 1	0.0.0.0
Destination Port 1	0
Backup Destination IP 1	0.0.0.0
Backup Destination Port 1	0
Destination 2	□ Enable
Destination IP 2	0.0.0.0
Destination Port 2	0
Backup Destination IP 2	0.0.0.0
Backup Destination Port 2	0
Response Behavior	○ Request & Response Mode ● Reply to request only ○ Reply to all ● Transparent Mode

Figure 5.6 Connection Settings for TCP Client Link Mode

- Click on the "**COM1**" link on the menu frame on the left side of Web UI to go to **COM 1** page as shown in Figure 5.7. Note that if you would like to configure **COM 2** (or any other COM port), please follow the same procedures.



Serial > COM1 TCPlink PS4000

COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

○ TCP Server ● TCP Client ○ UDP

TCP Client

Application	RAW ▾
Destination IP 1	0.0.0.0
Destination Port 1	0
Backup Destination IP 1	0.0.0.0
Backup Destination Port 1	0
Destination 2	□ Enable
Destination IP 2	0.0.0.0
Destination Port 2	0
Backup Destination IP 2	0.0.0.0
Backup Destination Port 2	0
Response Behavior	○ Request & Response Mode ● Reply to request only ○ Reply to all ● Transparent Mode

To configure COM 1 port parameters.

Serial Settings

Serial Interface	● RS232 ○ RS422 ○ RS485 ○ RS485(4-Wire)
Baud Rate	9600 ▾ bps
Parity	● None ○ Odd ○ Even ○ Mark ○ Space
Data bits	○ 5 bits ○ 6 bits ○ 7 bits ● 8 bits
Stop bits	● 1 bits ○ 2 bits
Flow Control	○ None ○ Xon/Xoff ● RTS/CTS

Figure 5.7 Setting in TCP Client Link Mode

- Select **TCP Client** radio button in the **Link Mode** options.
- Under the TCP Client section, you will find the following options.
    - **Application**: Only three communication applications are available here: **RAW**, **Virtual COM** and **Pair Connection Slave** in which their definitions are the same as described above in Section 5.1.1.
    - **Destination IP 1**: Please specify the preferred **Destination IP** address of the TCP server program on the remote host in this field. This should match the IP settings of the TCP server program.
    - **Destination Port 1**: Please specify the preferred port number of the TCP server program on the remote host in this field. Once again, this should match the IP setting of the TCP server program.
    - **Backup Destination IP 1**: Please specify the preferred **Backup Destination IP** address of the TCP server program on the remote host in this field. Once the Destination IP 1 cannot be reachable, PS4000/8000/16000 will send the data to Backup Destination IP 1.

  - **Backup Destination Port 1**: Please specify the preferred port number of the TCP server program on the remote host in this field. Once again, this should match the IP setting of the TCP server program.
  - **Destination 2**: You can enable second remote destination for TCP connection if necessary by checking on the **Enable** box in this option. Two different TCP servers can be set for redundancy.
  - **Destination IP 2**: Please specify the preferred **Destination IP** address of the second TCP server program on the remote host in this field. This should match the IP settings of the second TCP server program.
  - **Destination Port 2**: Please specify the preferred port number of the second TCP server program on the remote host in this field. Once again, this should match the IP setting of the second TCP server program.
  - **Backup Destination IP 2**: Please specify the preferred **Backup Destination IP** address of the TCP server program on the remote host in this field. Once the Destination IP 2 cannot be reachable, PS4000/8000/16000 will send the data to Backup Destination IP 2.
  - **Backup Destination Port 2**: Please specify the preferred port number of the TCP server program on the remote host in this field. Once again, this should match the IP setting of the TCP server program.
  - **Response Behavior**: This option specifies how the device will proceed or behave when it receives request from remote connected hosts. The description of each option is the same as described in previous subsection (Section 5.1.1 Link Mode: Configure as a TCP Server) .
- For other **Serial Settings** on the same configuration page, please go to Section 4.6.2 and for **Advanced Settings** please go to Section 4.6.3 COM Configuration: Advanced Settings.
- After finish configuring the **Link Mode**, please scroll down to the bottom of the page and click on **"Save & Apply"** button to save all the changes that you have made.

5.1.3 *Link Mode: Configure PS4000/8000/16000 in UDP*

Since User Datagram Protocol (UDP) is a faster transport protocol than TCP but it is a connectionless transport protocol, it does not guarantee the delivery of network datagram**.** PS4000/8000/16000 also supports connectionless UDP protocol compared to the connection**-**oriented TCP protocol**.** The PS4000/8000/16000 series can be configured to transfer data using unicast or multicast UDP from the serial device to one or multiple host computers**.** The data can be transmitted between a serial device and a remote host computer in both directions**.**

There is no server or client concept on this protocol**.** All networked devices are called peers or nodes**.** Therefore, you only need to specify the **Local Port** that PS4000/8000/16000 should listen to and specify the **Destination IPs** of the remote UDP nodes**.** Figure 5.8 illustrates an example of UDP Link Mode in which a serial display device is connected on a serial bus and PS4000/8000/16000**.** Two remote host computers, which are on the same Ethernet network as PS4000/8000/16000, can both send UDP datagram or messages to the serial display device through PS4000/8000/16000**.**

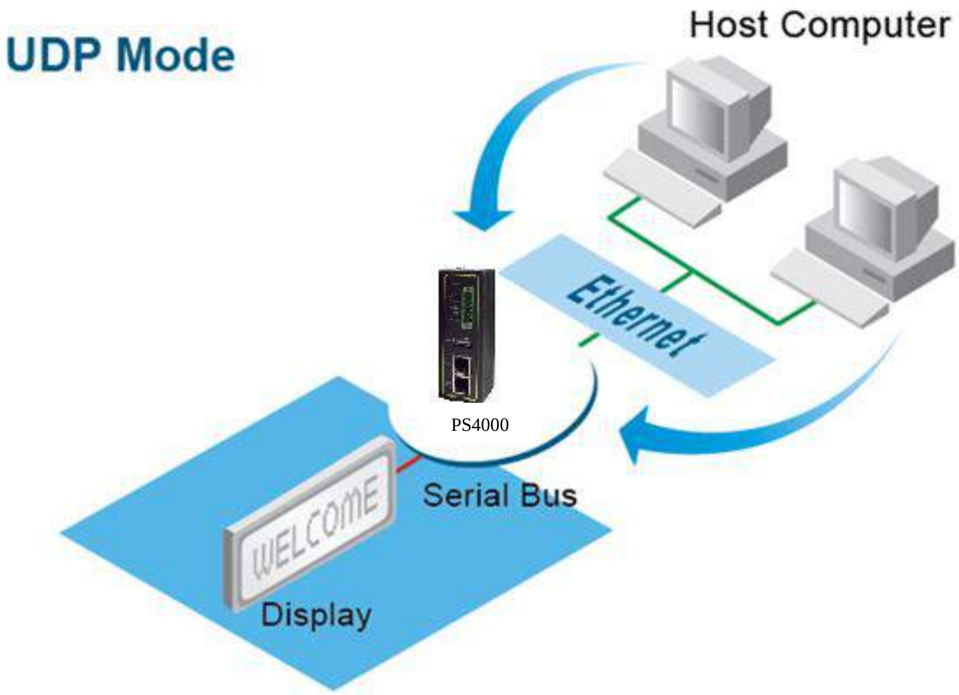
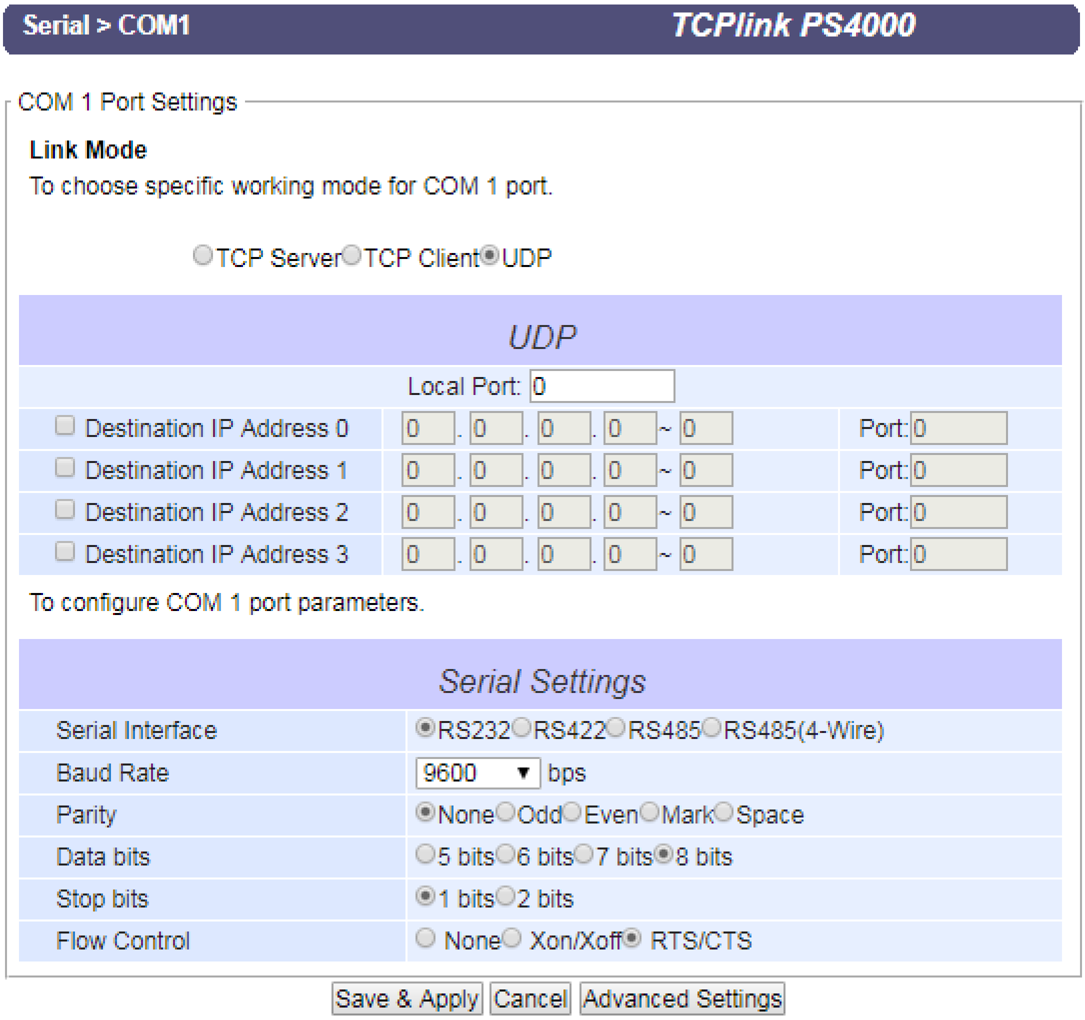


Figure 5.8 Example of PS4000/8000/16000 Configured in UDP Link Mode

Figure 5.9 shows an example of configuration setting for **UDP Link Mode** under the **COM 1** page. There are additional connection settings that can be configured as shown in Figure 5.10. Please beware that even though UDP provides better efficiency in terms of response time and resource usage, it does not guarantee data delivery. It is recommended to utilize UDP only with cyclic polling protocols where each request is repeated and independent, such as Modbus Protocol. Please follow the following steps to configure connection settings of the **Link Mode** for each **COM** port.



Serial > COM1 TCPlink PS4000

COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

○TCP Server ○TCP Client ●UDP

UDP

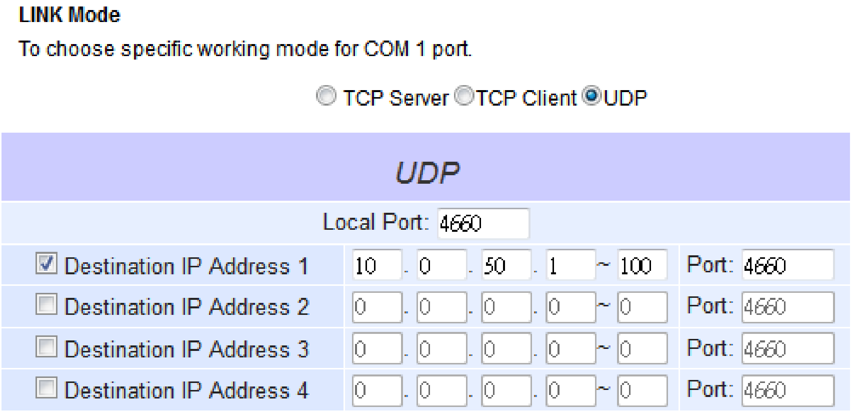
Local Port: 0

☐ Destination IP Address 0	0 . 0 . 0 . 0 ~ 0	Port: 0
☐ Destination IP Address 1	0 . 0 . 0 . 0 ~ 0	Port: 0
☐ Destination IP Address 2	0 . 0 . 0 . 0 ~ 0	Port: 0
☐ Destination IP Address 3	0 . 0 . 0 . 0 ~ 0	Port: 0

To configure COM 1 port parameters.

Serial Settings

Serial Interface	●RS232 ○RS422 ○RS485 ○RS485(4-Wire)
Baud Rate	9600 ▾ bps
Parity	●None ○Odd ○Even ○Mark ○Space
Data bits	○5 bits ○6 bits ○7 bits ●8 bits
Stop bits	●1 bits ○2 bits
Flow Control	○ None ○ Xon/Xoff ● RTS/CTS



LINK Mode

To choose specific working mode for COM 1 port.

○ TCP Server ○TCP Client ●UDP

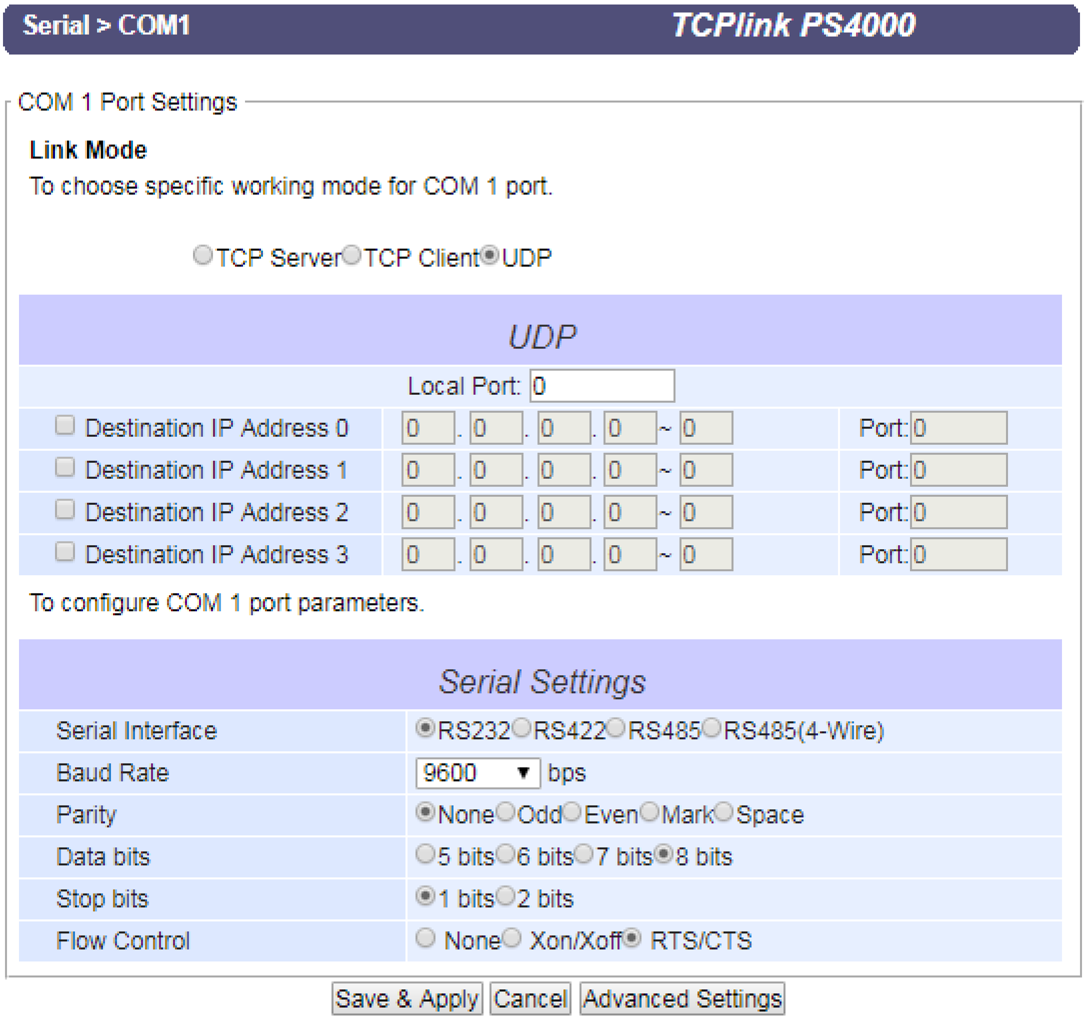
UDP

Local Port: 4660

☑ Destination IP Address 1	10 . 0 . 50 . 1 ~ 100	Port: 4660
☐ Destination IP Address 2	0 . 0 . 0 . 0 ~ 0	Port: 4660
☐ Destination IP Address 3	0 . 0 . 0 . 0 ~ 0	Port: 4660
☐ Destination IP Address 4	0 . 0 . 0 . 0 ~ 0	Port: 4660

Figure 5.9 Connection Setting in UDP Link Mode

- Click on the **"COM1"** link on the menu frame on the left side of Web UI to go to **COM 1** page as shown in Figure 4.10. Note that if you would like to configure **COM 2** (or any other COM port), please follow the same procedures.



Serial > COM1 TCPlink PS4000

COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

○ TCP Server ○ TCP Client ● UDP

UDP

Local Port: 0

□ Destination IP Address 0	0 . 0 . 0 . 0 ~ 0	Port: 0
□ Destination IP Address 1	0 . 0 . 0 . 0 ~ 0	Port: 0
□ Destination IP Address 2	0 . 0 . 0 . 0 ~ 0	Port: 0
□ Destination IP Address 3	0 . 0 . 0 . 0 ~ 0	Port: 0

To configure COM 1 port parameters.

Serial Settings

Serial Interface	● RS232 ○ RS422 ○ RS485 ○ RS485(4-Wire)
Baud Rate	9600 ▼ bps
Parity	● None ○ Odd ○ Even ○ Mark ○ Space
Data bits	○ 5 bits ○ 6 bits ○ 7 bits ● 8 bits
Stop bits	● 1 bits ○ 2 bits
Flow Control	○ None ○ Xon/Xoff ● RTS/CTS

Figure 5.10 UPD Link Mode Setting under COM 1 Page

- Select **UDP** radio button in the **Link Mode** options.
- Under the **UDP** section, you will find the following options.
  - **Local Port:** This field specifies the local port number for **UDP Link Mode** on PS4000/8000/16000 which it will be listening to and it can be any number between 1 and 65535. Note that typically the port number that is larger than 1024 is recommended to avoid conflicting with the well-known port numbers. You should match this setting with the remote UDP program. Note that this number is usually called destination port in the remote UDP program.
  - **Destination IP Address 1** to **4** and its **Port Numbers:** Each line of these options can specify the range of IP addresses and port number that will be communicating with PS4000/8000/16000. The user can define the **Begin** and **End IP Addresses** here. Four groups of ranges of IP addresses are allowed. Please check the box in front of that particular line to enable it. These are the IP Addresses of the remote UDP programs and the Port that they are listening to. Note that the maximum number of UDP nodes that PS4000/8000/16000 can handle would highly depend on the traffic load. We have tested that PS4000/8000/16000 can handle up to 200 UDP nodes (with baud rate of 9600 bps, request interval of 100ms, and data length of 30 bytes).
- For other Serial Settings on the same configuration page, please go to Section 4.6.2 and for Advanced Settings please go to Section 4.6.3.

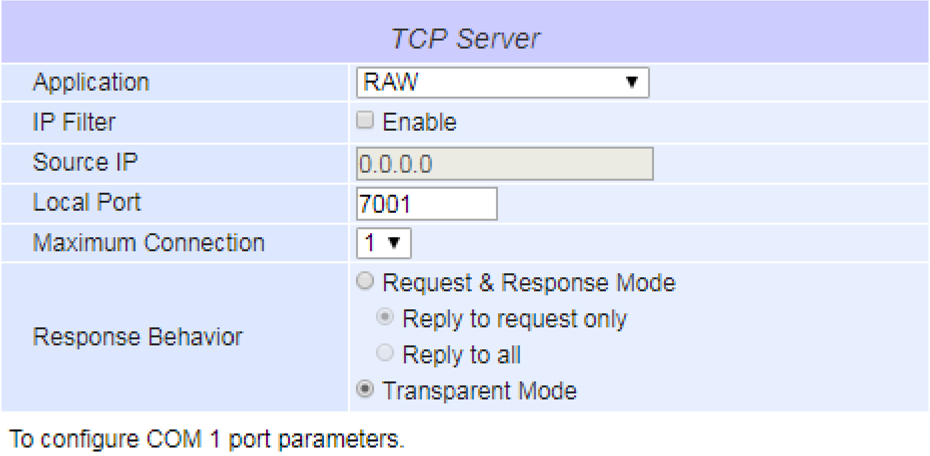
- After finish configuring the **Link Mode**, please scroll down to the bottom of the page and click on **"Save & Apply"** button to save all the changes that you have made**.**

5.2 *Link Mode Applications*

This section describes application options for the **TCP Server**, **TCP Client**, and **UDP Link Modes.** The application options will define how the serial data communication will be emulated over the network communication link**.** The user will have flexibility in choosing the suitable application that matches their need for serial data communication**.**

5.2.1 *TCP Server Application: Enable Virtual COM*

PS4000/8000/16000 will encapsulate control packets on top of the real data when **Virtual COM** is enabled**.** This will allow the Virtual COM port on the Windows/Linux operating system to access PS4000/8000/16000**'**s COM ports**.** The benefit of using Virtual COM is that rewriting an existing COM program to read IP packets is unnecessary**.** In other words, it is possible to use an ordinary or legacy serial (COM) program**.** The conversion/virtualization of IP to COM is all done in the system driver transparently**.** Figure 5.11 shows PS4000/8000/16000 in **TCP Server** mode with **Virtual COM** application enabled**.** Please follow the following steps to enable **Virtual COM** application in **TCP Server Link Mode.**



TCP Server

Application	RAW ▼
IP Filter	□ Enable
Source IP	0.0.0.0
Local Port	7001
Maximum Connection	1 ▼
Response Behavior	○ Request & Response Mode ● Reply to request only ○ Reply to all ● Transparent Mode

To configure COM 1 port parameters.

Figure 5.11 Virtual COM Application in TCP Server Link Mode

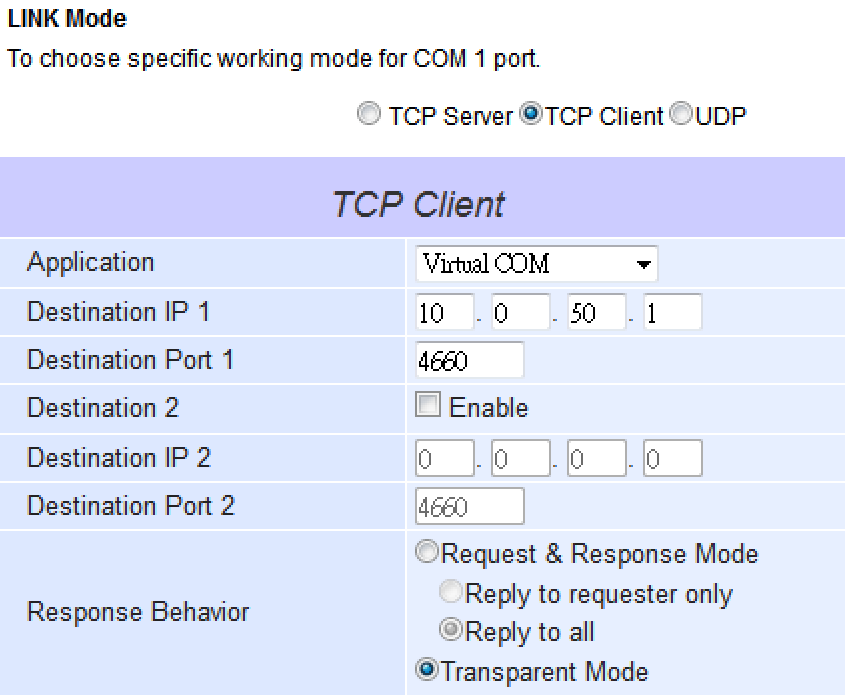
- Follow steps in Section 5.1.1 to configure PS4000/8000/16000 in **TCP Server Link Mode** properly.
- Click on the drop-down list of the **Application** option under **TCP Server** section and switch to "**Virtual COM**" to enabled Virtual COM application in PS4000/8000/16000.
- Scroll down to the bottom of the page and click on "**Save & Apply**" button to save the changes.
- Configure Virtual COM in the Operating System on the remote host computer. For Windows, please refer to Chapter 6 for necessary instructions. Please remember PS4000/8000/16000's IP address and the **Local Port** number configured on this page in order to enter the same information in Serial/IP Virtual COM's Control Panel later. Note that a Serial/IP Virtual COM Redirector software is provided as a utility software by TCPlink .

5.2.2 *TCP Server Application: Enable RFC 2217 through Virtual COM*

The underlying protocol of Virtual COM is based on RFC 2217 which is the Telnet COM Control Option**.** Therefore, it is possible to use RFC 2217 with PS4000/8000/16000 in the TCP Server mode**.** Note that the RFC 2217 allows a remote client, which can be any network device, to initiates a Telnet session to an access server (i**.**e**.** PS4000/8000/16000) to communicate with serial device on the access server's COM port**.** To do so, please refer to Section 5.2.1 (previous section) to enable Virtual COM so that PS4000/8000/16000 becomes aware of the command names and codes defined in RFC 2217**.** Note that there is no need to configure Virtual COM on the Operating System of the remote host computer because Virtual COM ports would not be used**.**

5.2.3 *TCP Client Application: Enable Virtual COM*

It is also possible to run Virtual COM in TCP Client Link Mode**.** shows a configuration of Virtual COM application in TCP Client Link Mode**.** It is usually easier to use Virtual COM in the TCP Client Link Mode if PS4000/8000/16000 uses dynamic IP (via DHCP) because setting a static IP address in Virtual COM's Control Panel in the Operating System is not possible**.** Please follow the following steps to enable Virtual COM application in TCP Client Link Mode**.**



LINK Mode

To choose specific working mode for COM 1 port.

○ TCP Server ● TCP Client ○ UDP

TCP Client	
Application	Virtual COM ▾
Destination IP 1	10 . 0 . 50 . 1
Destination Port 1	4660
Destination 2	□ Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	○ Request & Response Mode ○ Reply to requester only ● Reply to all ● Transparent Mode

Figure 5.12 Virtual COM Application in TCP Client Link Mode

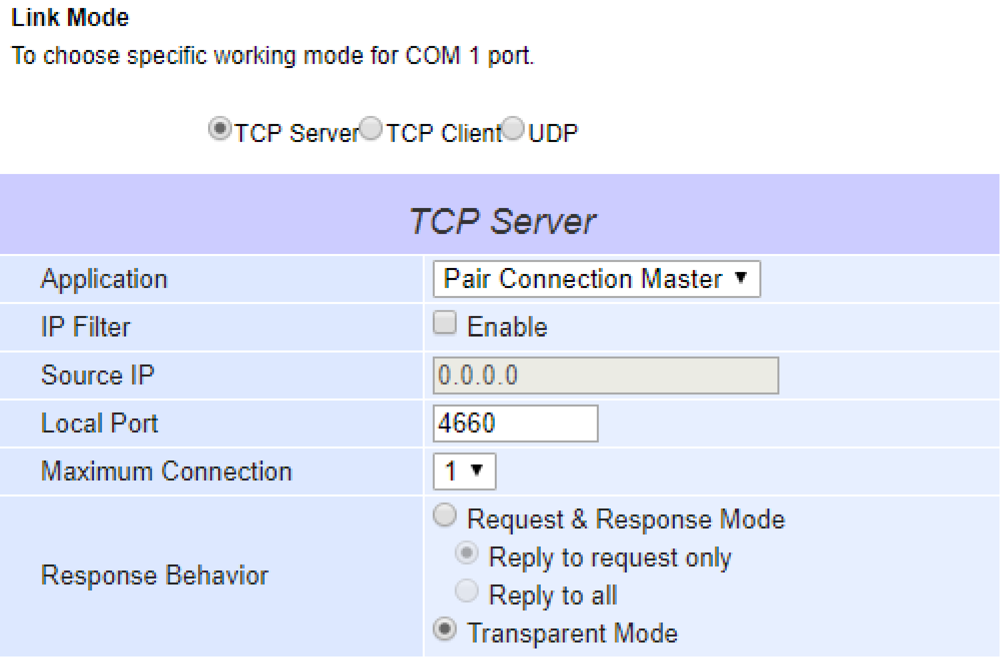
- Follow step in Section 5.1.2 to configure PS4000/8000/16000 in TCP Client Link Mode properly.
- Click on the drop-down list of the Application option under TCP Client section and switch to "Virtual COM" to enabled Virtual COM application in PS4000/8000/16000.
- Scroll down to the bottom of the page and click on "**Save & Apply**" button to save the changes.
- Configure Virtual COM in the Operating System on the remote host computer. For Windows, please refer to Chapter 6 for necessary instruction. Please remember the **Destination Port** number configured on this page in order to enter this information in Serial/IP Virtual COM's Control Panel later.

5.2.4 *TCP Client Application: Enable RFC 2217 through Virtual COM*

The underlying protocol of Virtual COM is based on RFC 2217 which is the Telnet COM Control Option**.** Therefore, it is possible to use RFC 2217 with PS4000/8000/16000 in the TCP Client mode**.** Note that the RFC 2217 allows a client, which is PS4000/8000/16000 in this case, to initiates a Telnet session to a remote host computer to communicate with serial device or serial (COM) program on the remote host computer**.** To do so, please refer to Section 5.2.3 (previous section) to enable Virtual COM so that PS4000/8000/16000 becomes aware of the command names and codes defined in RFC 2217**.** Note that there is no need to configure Virtual COM on the Operation System of the remote host computer because Virtual COM ports would not be used**.**

5.2.5 *TCP Server Application: Configure PS4000/8000/16000 as a Pair Connection Master*

A Pair Connection application is useful when pairing up two serial devices over the Ethernet or when it is impossible to install Virtual COM in the serial devices. However, the pair connection application does require two PS4000/8000/16000 to work in pair. One would be the Pair Connection Master and the other would be the Pair Connection Slave. Figure 5.13 shows a configuration of Pair Connection Master application in TCP Server Link Mode. Please follow the following steps to enable Pair Connection application and set the PS4000/8000/16000 as Master in TCP Server Link Mode.



Link Mode

To choose specific working mode for COM 1 port.

● TCP Server ○ TCP Client ○ UDP

TCP Server

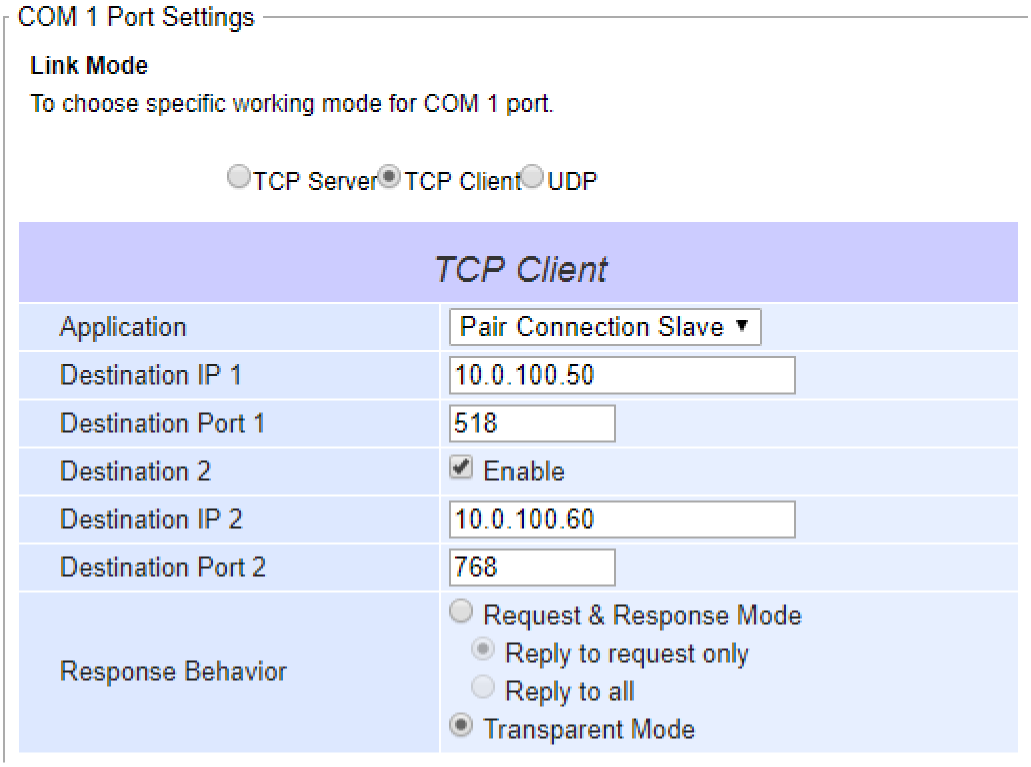
Application	Pair Connection Master ▼
IP Filter	□ Enable
Source IP	0.0.0.0
Local Port	4660
Maximum Connection	1 ▼
Response Behavior	○ Request & Response Mode ● Reply to request only ○ Reply to all ● Transparent Mode

Figure 5.13 Pair Connection Master Application in TCP Server Link Mode

- Follow steps in Section 5.1.1 to configure PS4000/8000/16000 in TCP Server Link Mode properly.
- Click on the drop-down list of the **Application** option under TCP Server section and switch to "**Pair Connection Master**" to enabled Pair Connection application in PS4000/8000/16000.
- Scroll down to the bottom of the page and click on "**Save & Apply**" button to save the changes.
- Please remember Pair Connection Master's IP address (i.e. PS4000/8000/16000's IP address on your desired network interface (either Ethernet or Wi-Fi)) and Local Port number here in order to enter these information in another PS4000/8000/16000 device with the Pair Connection Slave setting later.
- Proceed to the next section to configure a Pair Connection Slave to connect to this Master.

5.2.6 *TCP Client Application: Configure PS4000/8000/16000 as a Pair Connection Slave*

A Pair Connection Slave application is configured for PS4000/8000/16000 under TCP Client Link Mode as shown in Figure 5.14. It is necessary to pair up with a Pair Connection Master as described in previous section. Please setup a Pair Connection Master on another PS4000/8000/16000 device first before proceeding. Please follow the following steps to enable Pair Connection application and set this PS4000/8000/16000 device as Slave in TCP Client Link Mode.



COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

○ TCP Server ● TCP Client ○ UDP

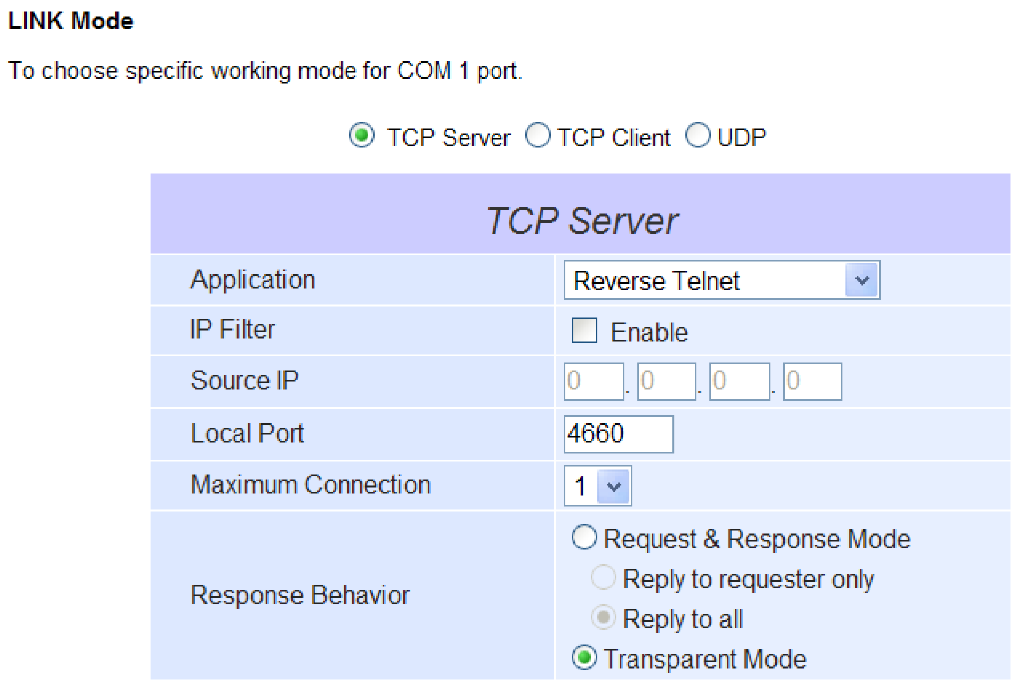
TCP Client	
Application	Pair Connection Slave ▼
Destination IP 1	10.0.100.50
Destination Port 1	518
Destination 2	☑ Enable
Destination IP 2	10.0.100.60
Destination Port 2	768
Response Behavior	○ Request & Response Mode ● Reply to request only ○ Reply to all ● Transparent Mode

Figure 5.14 Pair Connection Slave Application in TCP Client Link Mode

- Follow steps in Section 5.1.2 to configure PS4000/8000/16000 in TCP Client Link Mode properly.
- Click on the drop-down list of the **Application** option under TCP Client section and switch to "**Pair Connection Slave**" to enabled Pair Connection application in PS4000/8000/16000.
- Enter the **Destination IP** address and the **Destination Port** number (for Destination 1 and (optionally Destination 2)) that match to the settings of Pair Connection Master (another PS4000/8000/16000 device)'s IP and port number that were setup previously.
- Scroll down to the bottom of the page and click on "**Save & Apply**" button to save the changes.

5.2.7 *TCP Server Application: Enable Reverse Telnet*

Reverse Telnet application is useful if a Telnet program is used to connect to PS4000/8000/16000 and the serial interface of the PS4000/8000/16000 is connected to a Terminal Server**.** Telnet programs in Windows/Linux operating systems require special handshaking to get the outputs and the character formatting to show properly**.** PS4000/8000/16000 will interact with those special commands (such as CR/LF commands) if **Reverse Telnet** is enabled**.** Figure 5.15 shows a configuration of **Reverse Telnet** application in the **TCP Server Link Mode.** Note that the **Reverse Telnet** application is only available when PS4000/8000/16000 is configured as **TCP Server Link Mode.** Please follow the following steps to enable **Reverse Telnet** application under the **TCP Server Link Mode.**



LINK Mode

To choose specific working mode for COM 1 port.

● TCP Server ○ TCP Client ○ UDP

TCP Server	
Application	Reverse Telnet
IP Filter	□ Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1
Response Behavior	○ Request & Response Mode ○ Reply to requester only ● Reply to all ● Transparent Mode

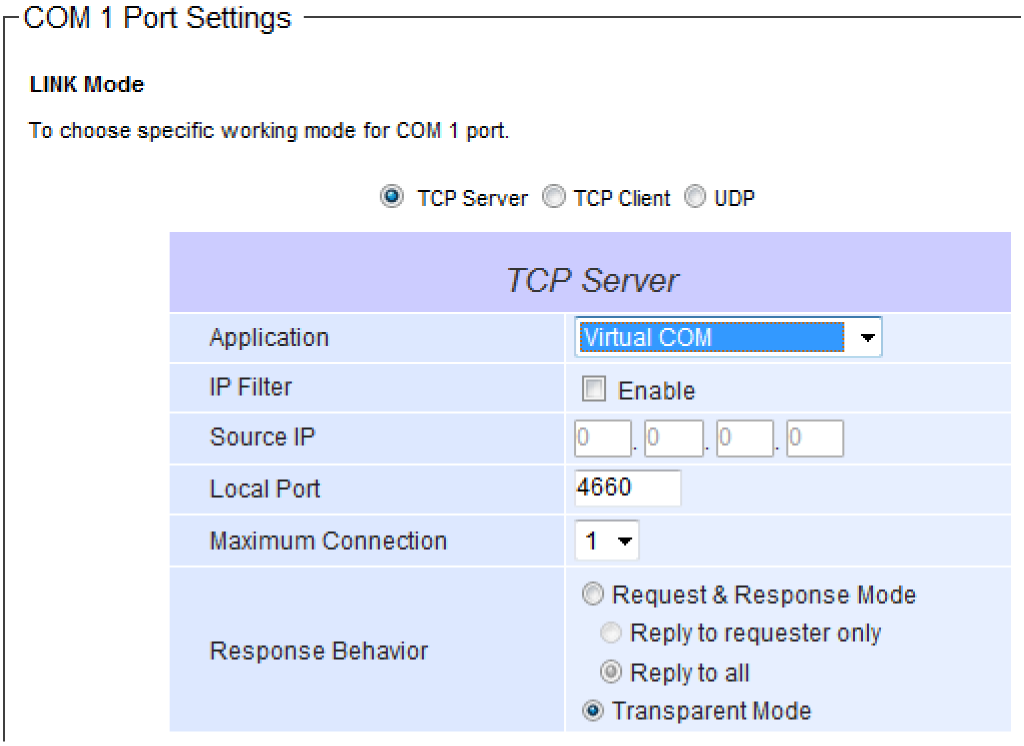
Figure 5.15 Reverse Telnet Application in TCP Server Link Mode

- Follow steps in Section 5.1.1 to configure PS4000/8000/16000 in **TCP Server Link Mode** properly.
- Click on the drop-down list of the **Application** option under **TCP Server** section and switch to **“Reverse Telnet**” to enabled reverse telnet application in PS4000/8000/16000.
- Scroll down to the bottom of the page and click on “**Save & Apply**” button to save the changes.

6 VCOM Installation & Troubleshooting

6.1 *Enabling VCOM*

PS4000/8000/16000 will encapsulate control packets on top of the actual serial data when **Virtual COM** (VCOM) **Application** is enabled**.** This will allow the Virtual COM port in the Windows/Linux system to access PS4000/8000/16000**'**s COM ports**.** Please note that **Virtual COM Application** can only be enabled in **TCP Server Link Mode** as shown in Figure 6.1 or **TCP Client Link Mode** as shown in Figure 6.2**.**



COM 1 Port Settings

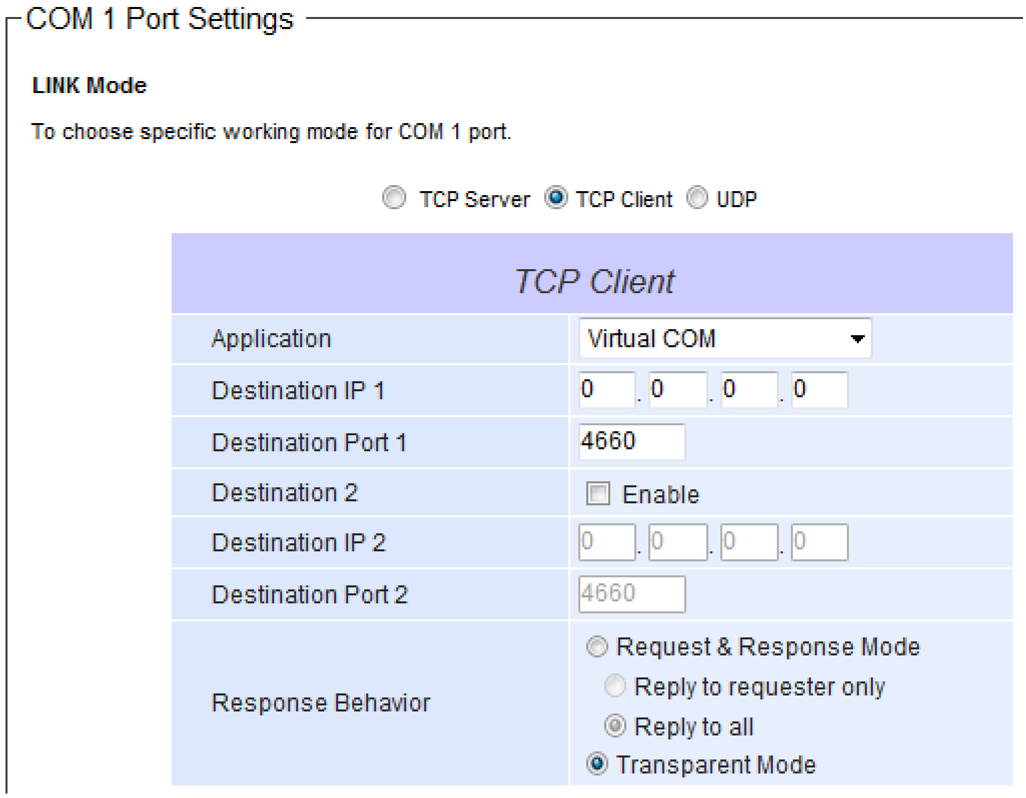
LINK Mode

To choose specific working mode for COM 1 port.

● TCP Server ○ TCP Client ○ UDP

TCP Server	
Application	Virtual COM
IP Filter	□ Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1
Response Behavior	○ Request & Response Mode ○ Reply to requester only ● Reply to all ● Transparent Mode

Figure 6.1 Enable a Virtual COM Application When Setting the Link Mode as the TCP Server



COM 1 Port Settings

LINK Mode

To choose specific working mode for COM 1 port.

○ TCP Server ● TCP Client ○ UDP

TCP Client	
Application	Virtual COM
Destination IP 1	0 . 0 . 0 . 0
Destination Port 1	4660
Destination 2	□ Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	○ Request & Response Mode ○ Reply to requester only ● Reply to all ● Transparent Mode

Figure 6.2 Enable a Virtual COM Application When Setting the Link Mode as the TCP Client

Virtual COM on host computer allows remote access of serial devices over TCP/IP networks through Serial/IP Virtual COM ports that work like local native COM ports. Figure 6.3 is an example of Virtual COM application diagram. In the diagram, multiple serial servers (i.e. PS4000/8000/16000 devices) in which each one connects to serial device are connected over an Ethernet hub. Their serial devices can be accessed through the TCP/IP network of the hub. Note that there are traditionally only two Physical COM ports (COM 1 and COM 2) on the personal computer (PC) while there can be several Virtual COM ports such as COM 3, 4, 5, and so on. In PS4000/8000/16000 case, the TCP/IP network can be wired network such as Ethernet.

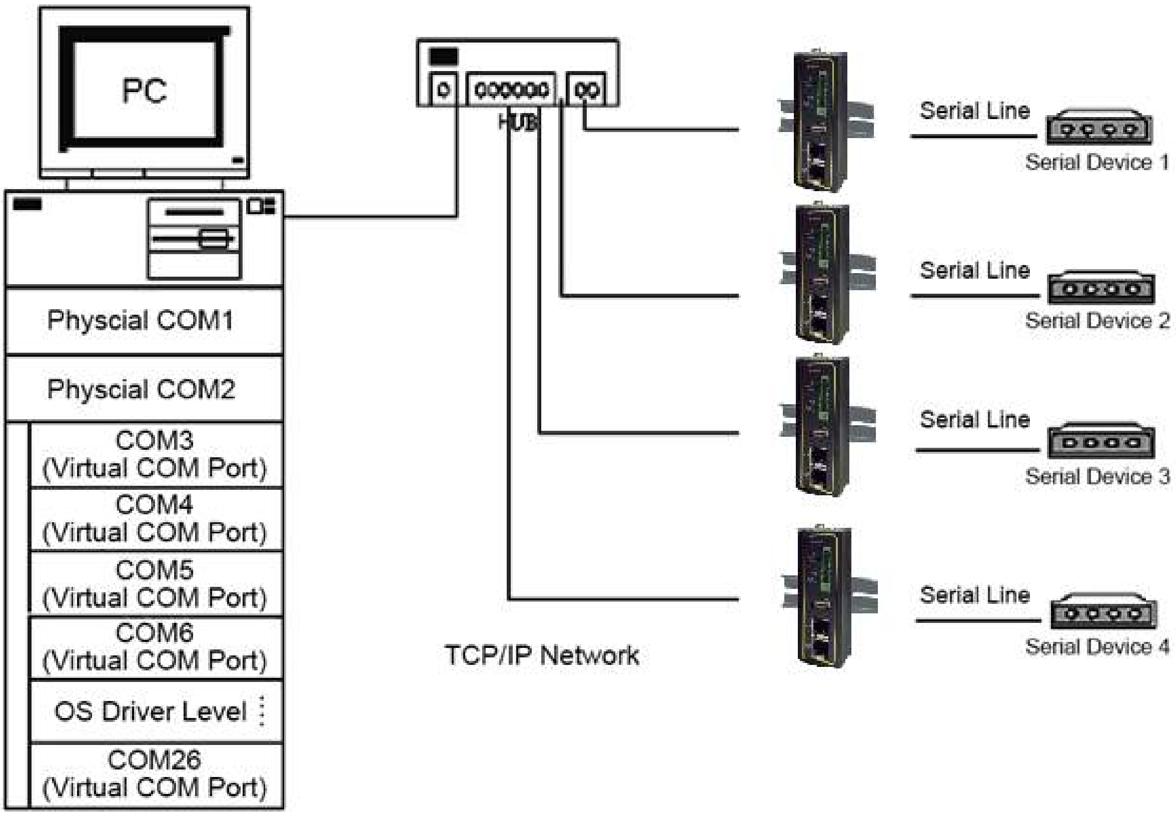


Figure 6.3 An Example Diagram of Virtual COM Application over TCP/IP Network

To enable Virtual COM on host computer, you will require a software utility or VCOM driver software to emulate the COM port. For Windows operating system, a software utility called **Serial/IP** is supported by TCPlink to be used for this purpose. Please see discussion about the VCOM driver utility in the following subsections.

6.1.1 *VCOM driver setup*

The supported VCOM driver or Serial/IP utility has the following requirements.

System Requirements

- Windows Operating System Supported Platform (32/64 bits)
  - Win10
  - Win8
  - Win7
  - Vista
  - XP
  - 2008
  - 2003 (also Microsoft 2003 Terminal Server)
  - 2000 (also Microsoft 2000 Terminal Server)
  - NT (also Microsoft NT Terminal Server)
  - 4.0
  - 9x
  - Citrix MetaFrame Access Suite

- Linux operating system also available, but first you might need to download a separate package called Virtual COM driver for Linux (TTYredirector) available for download on TCPlink website or in the product CD. The zipped package includes a binary file for installation and a manual for Linux systems.

6.1.2 *Limitation*

The Virtual COM driver allows up to 256 Virtual COM ports in a single PC. Selection of COM port number can be allowed in the range from COM1 to COM4096. Note that COM ports that are already occupied by the system or other devices will not be available.

6.1.3 *Installation*

Run the Virtual COM setup file included in the CD or download a copy from our website to install the Virtual COM driver for your operating system. Please turn off your anti-virus software and try again if the installation fails. At the end of the installation, please select at least one Virtual COM port from the Serial/IP Control Panel.

6.1.4 *Uninstallation*

- From Windows Start Menu select Control Panel then select Add/Remove Programs.
- Select Serial/IP Version x.x.x in the list of installed software.
- Click the Remove button to remove the program.

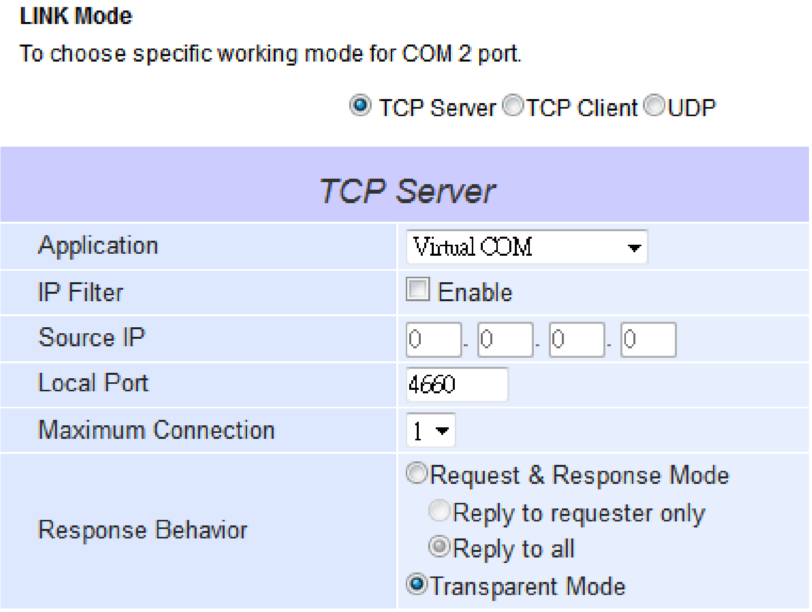
6.2 *Enable VCOM in Serial Device servers and Select VCOM in Windows*

This section will provide the procedure to enable Virtual COM (VCOM) on PS4000/8000/16000 and Windows based PC. Please follow the steps described here to configure your Virtual COM application.

6.2.1 *Enable VCOM in Serial Device servers*

Enable **Virtual COM** in our serial device servers (i.e. PS4000/8000/16000) by logging into the Web UI. It is located under **COM 1** or other **COM** configuration under **Serial** menu as described in Section 5.2.1.

Figure 6.4 shows how to enable **Virtual COM** in **TCP Server Link Mode** in PS4000/8000/16000. For a detail of **Link Mode** configuration with **Virtual COM**, please refer to the previous chapter starting from Section 5.1.



LINK Mode

To choose specific working mode for COM 2 port.

● TCP Server ○TCP Client ○UDP

TCP Server	
Application	Virtual COM ▾
IP Filter	□ Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1 ▾
Response Behavior	○Request & Response Mode ○Reply to requester only ●Reply to all ●Transparent Mode

Figure 6.4 Enable Virtual COM Application for COM 2 in TCP Server Link Mode

6.2.2 *Running Serial/IP Software Utility in Windows*

After installation of Virtual COM driver on Windows operating system as described in Section 6.1.3, you can open **Serial/IP Control Panel** by following any one of these methods:

1) Click on Windows' Start menu → Select All Programs → Select Serial/IP → Select Control Panel.
2) In the Windows' Control Panel, open the Serial/IP applet.
3) In the Windows notification area as shown in Figure 6.5, right click on the Serial/IP tray icon and click on Configure… menu to open the Serial/IP's Control Panel.

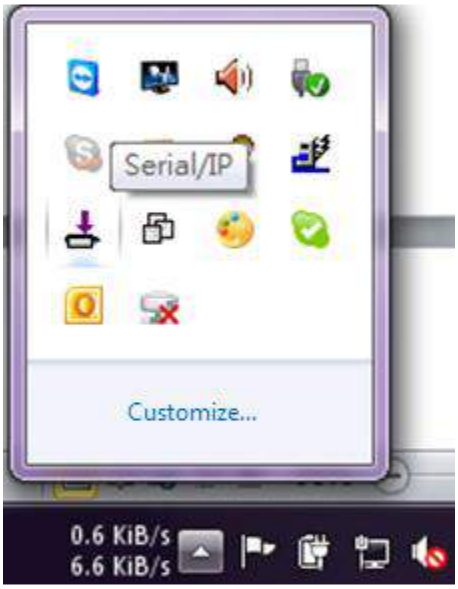
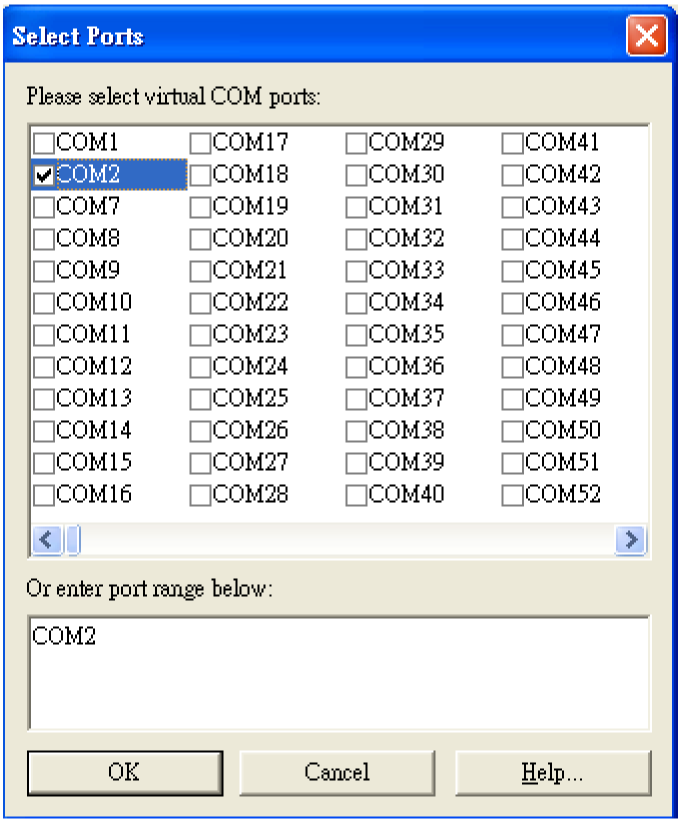


Figure 6.5 Serial/IP Tray Icon on Windows Notification Area

If no Virtual COM port is selected, a "**Select Ports**" dialog window will pop up and ask the user to select at least one COM port as the Virtual COM port before proceeding as shown in the pop-up window of Figure 6.6. You can select a COM port by checking the box in front of the list of virtual COM ports. Note that if a COM port number is not on the list, it may be used by other application or your operating system. The user may want to select a range of multiple COM ports to be used as Virtual COM ports by entering the range of COM port in the text box below the list. After selecting the virtual COM ports, please click OK button to proceed.



Please select virtual COM ports:

☐COM1
☑COM2
☐COM7
☐COM8
☐COM9
☐COM10
☐COM11
☐COM12
☐COM13
☐COM14
☐COM15
☐COM16
☐COM17
☐COM18
☐COM19
☐COM20
☐COM21
☐COM22
☐COM23
☐COM24
☐COM25
☐COM26
☐COM27
☐COM28
☐COM29
☐COM30
☐COM31
☐COM32
☐COM33
☐COM34
☐COM35
☐COM36
☐COM37
☐COM38
☐COM39
☐COM40
☐COM41
☐COM42
☐COM43
☐COM44
☐COM45
☐COM46
☐COM47
☐COM48
☐COM49
☐COM50
☐COM51
☐COM52

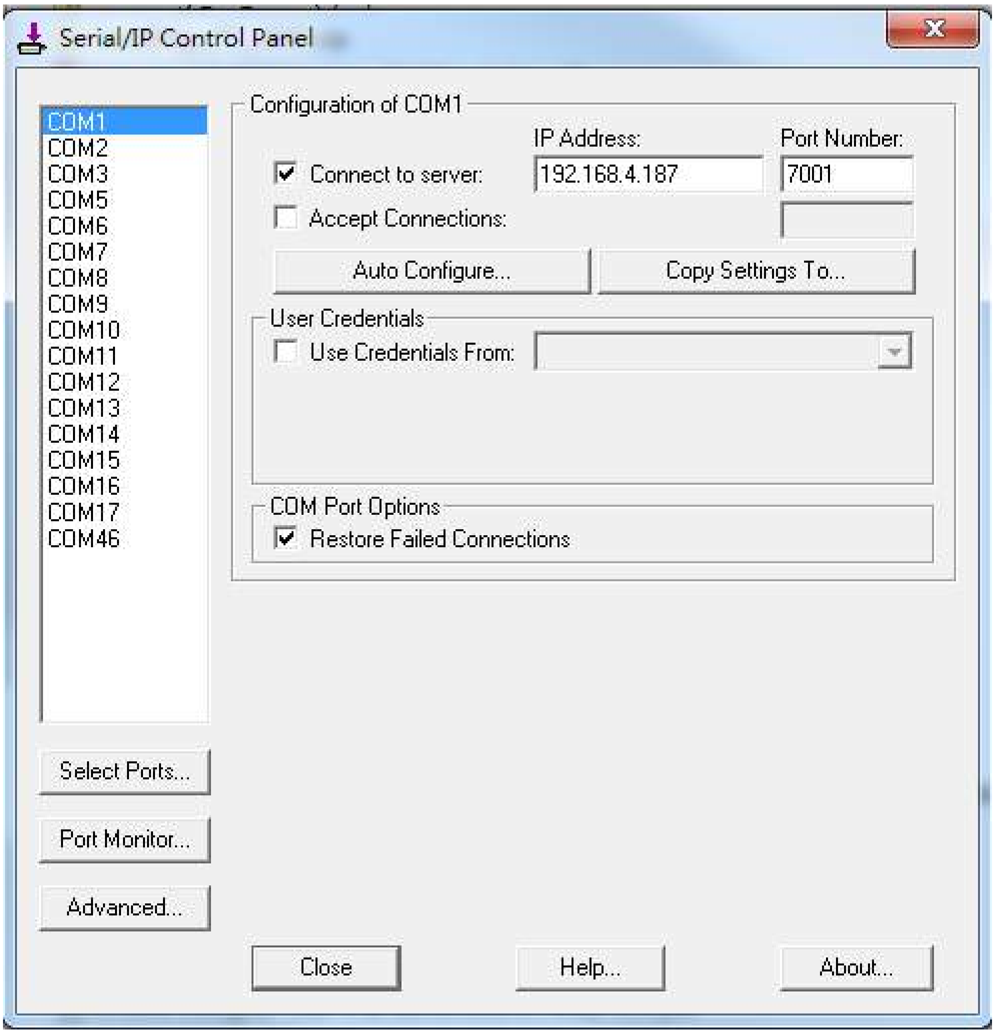
Or enter port range below:

COM2

Figure 6.6 A Pop-up Window for Selecting Virtual COM Ports

After at least one Virtual COM port is selected, the **Serial/IP Control Panel** window will show up as illustrated in Figure 6.7. The left side of the **Control Panel** window shows the list of selected Virtual COM ports. You can click on **Select Ports…** button below the list to add or remove Virtual COM ports from the list. The right side of the **Serial/IP Control Panel** window shows the configurations of the selected Virtual COM port marked in blue on the list. Each Virtual COM port can have its own settings. Details on how to configure the Virtual COM port will be described in the next subsection.

Note: The changes to Virtual COM ports apply immediately so there is no need to save the settings manually. However, if the Virtual COM port is already in use, it is necessary to close the Virtual COM port and open it after the TCP connection closes completely in order for the changes to take effect.



Serial/IP Control Panel

COM1
COM2
COM3
COM5
COM6
COM7
COM8
COM9
COM10
COM11
COM12
COM13
COM14
COM15
COM16
COM17
COM46

Configuration of COM1

☑ Connect to server: IP Address: 192.168.4.187 Port Number: 7001

☐ Accept Connections:

User Credentials

☐ Use Credentials From:

COM Port Options

☑ Restore Failed Connections

Figure 6.7 Serial/IP Control Panel Window

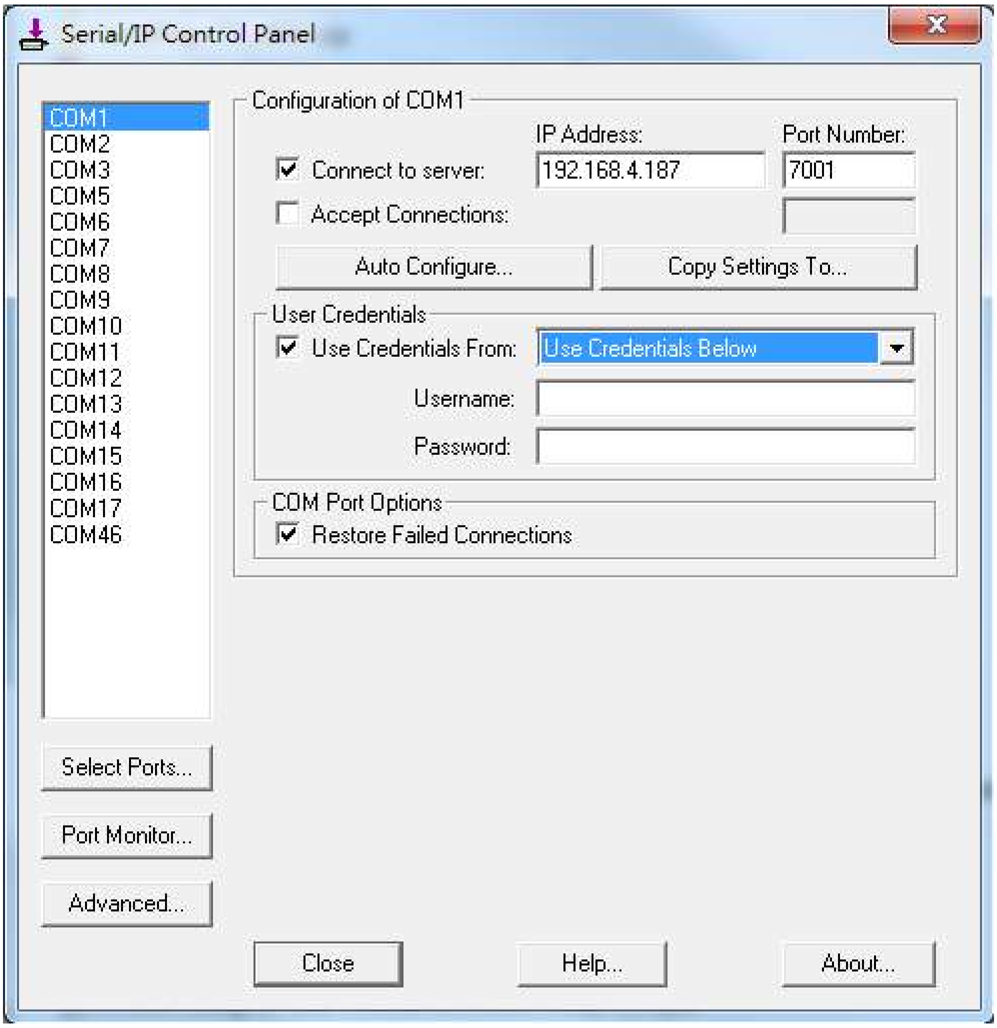
6.2.3 *Configuring VCOM Ports*

For each VCOM port selected on the listed on the left side of the **Serial/IP Control Panel**, you can use the following procedures to configure that VCOM port**.**

1. If the serial device server (i**.**e**.** PS4000/8000/16000) is running in **TCP Server Link Mode** (recommended), the **Serial/IP** utility on the host computer should be configured as the TCP client connecting to the serial device server**.** Enable **Connect to Server** option (by checking the box in front of it as shown in Figure 6.9) and enter the IP Address of the serial device server with the specified **Port Number.** The **Port Number** here is the **Local Listening Port** for the serial device server which is specified in the **Local Port** field of Figure 5.11**.**

2. If the serial device server **(**i**.**e**.** PS4000/8000/16000**)** is running in **TCP Client Link Mode**, the **Serial/IP** utility on the host computer should be configured as the TCP server waiting for a serial device server to connect to the host computer**.** Enable **Accept Connections option (**by checking the box in front of it**)** and enter the specified **Port Number.** This **Port Number** is the **Destination Port** of the serial device server**.** Do not enable **Connect to Server** option and **Accept Connections** option simultaneously**.**

3. Under **User Credentials** box, you can enable **Use Credentials From:** option by checking the box in front of it then select options from the drop**-**down list**.** The available sources of credentials are**: Prompt on COM Port Open**, **Prompt at Login**, and **Use Credentials Below** as shown in Figure 6.8. If you select **Use Credentials Below** option as shown in Figure 6.9, please specify the **Username** and the **Password** in their corresponding text boxes**.**



Serial/IP Control Panel

COM1
COM2
COM3
COM5
COM6
COM7
COM8
COM9
COM10
COM11
COM12
COM13
COM14
COM15
COM16
COM17
COM46

Configuration of COM1

☑ Connect to server: IP Address: 192.168.4.187 Port Number: 7001

□ Accept Connections:

User Credentials

☑ Use Credentials From: Use Credentials Below

Username:

Password:

COM Port Options

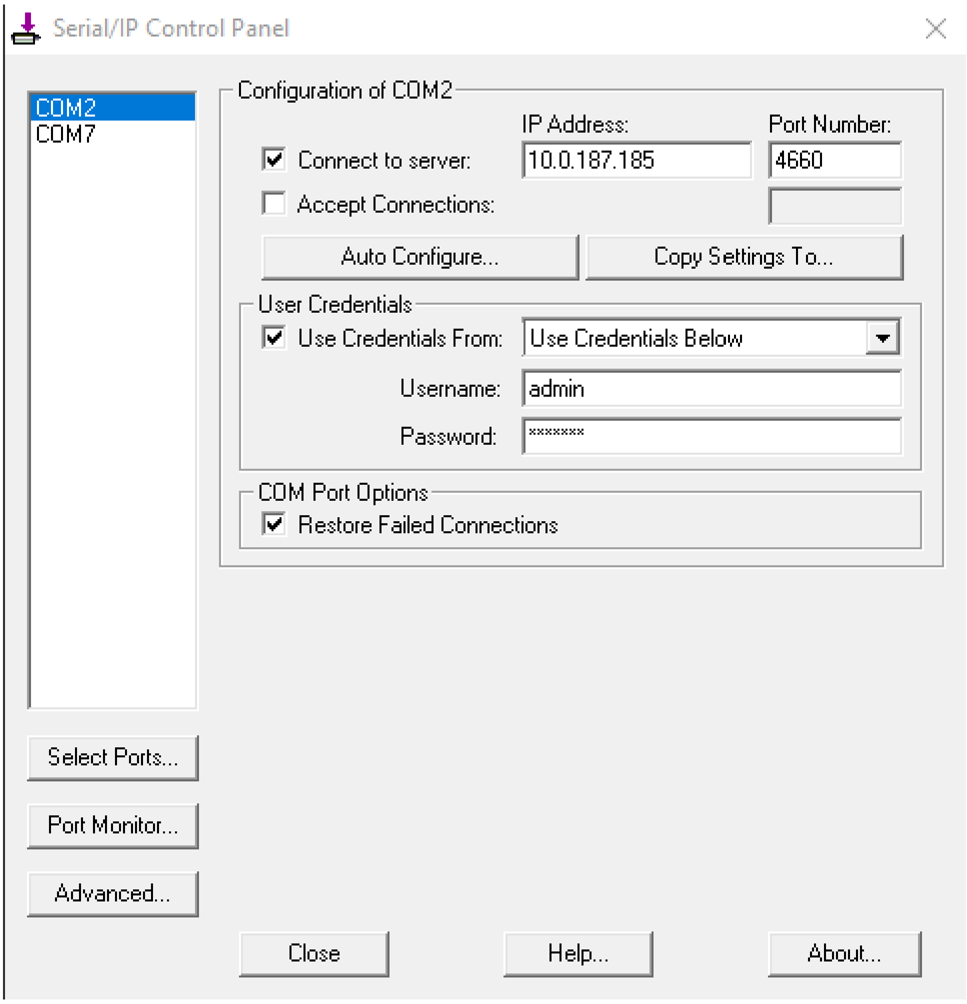
☑ Restore Failed Connections

Figure 6.8 Available Options for Use Credential From in Serial/IP Control Panel Version 4.9.10

4. Under **COM Port Options** box, you can enable **Restore Failed Connections** option by checking the box in front of it to force Virtual COM to automatically restore failed connections with the serial device server in case of unstable network connections.

5. To test the Virtual COM connection, you can click the **Auto Conigure…** button and then click the **Start** button in the pop up window as shown in Figure 6.10. If the test passes, all checks under the **Status** text box should be green. In this **Configuration Wizard** window, you can change the **IP Address** of Server, **Port Number**, **Username** (if **Use Credential** option is enabled), and **Password** (if **Use Credential** option is enabled). To apply the changes in the Configuration Wizard window to the Serial/IP Control Panel, please click on **Use Settings** button at the bottom of the window in Figure 6.10. You can also click on **Copy** button to copy the results to the PC system clipboard.

6. To transfer the settings between Virtual COM ports, click on the **Copy Settings To** button as shown in Figure 6.9.



Serial/IP Control Panel

COM2
COM7

Configuration of COM2

☑ Connect to server: IP Address: 10.0.187.185 Port Number: 4660

☐ Accept Connections:

User Credentials

☑ Use Credentials From: Use Credentials Below

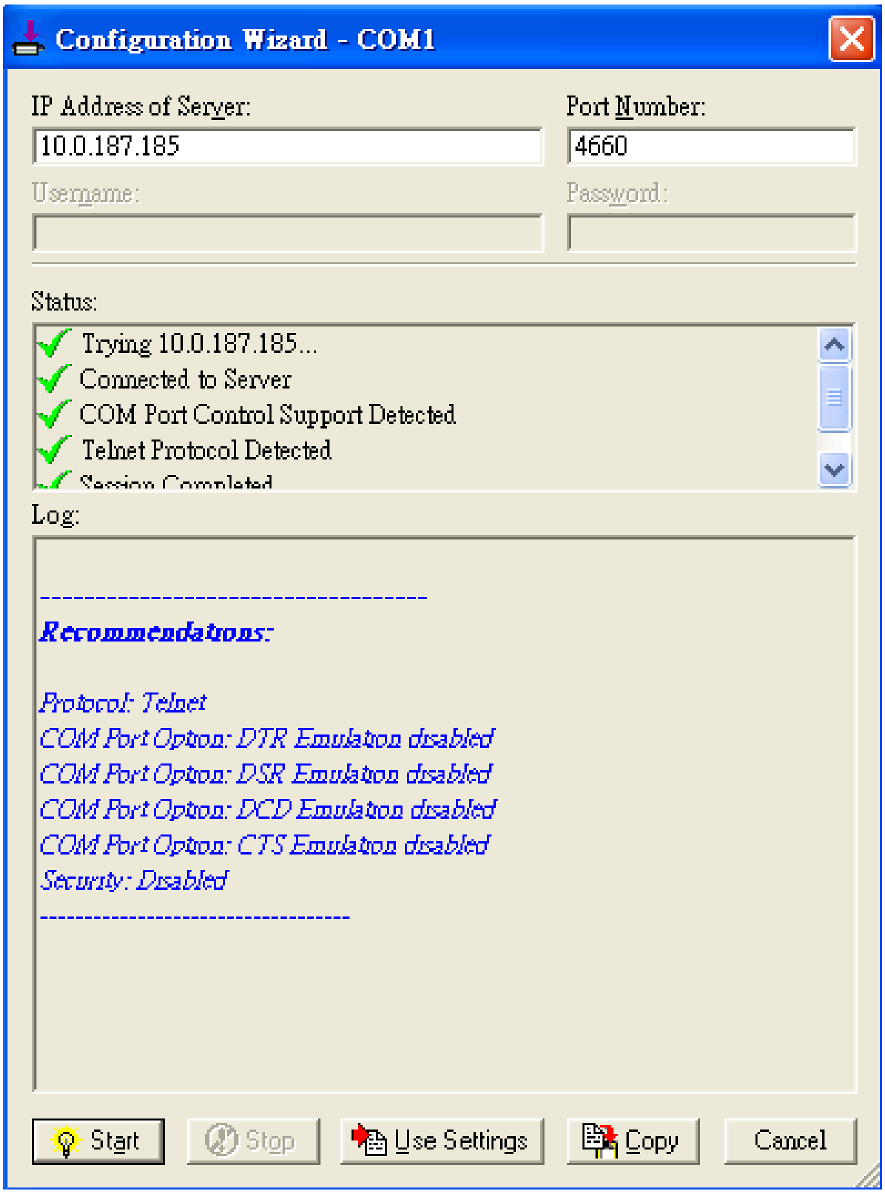
Username: admin

Password: *******

COM Port Options

☑ Restore Failed Connections

Figure 6.9 Configuring Virtual COM 2 Port as TCP Client



IP Address of Server: 10.0.187.185

Port Number: 4660

Username:

Password:

Status:

✓ Trying 10.0.187.185...
✓ Connected to Server
✓ COM Port Control Support Detected
✓ Telnet Protocol Detected
✓ Session Completed

Log:

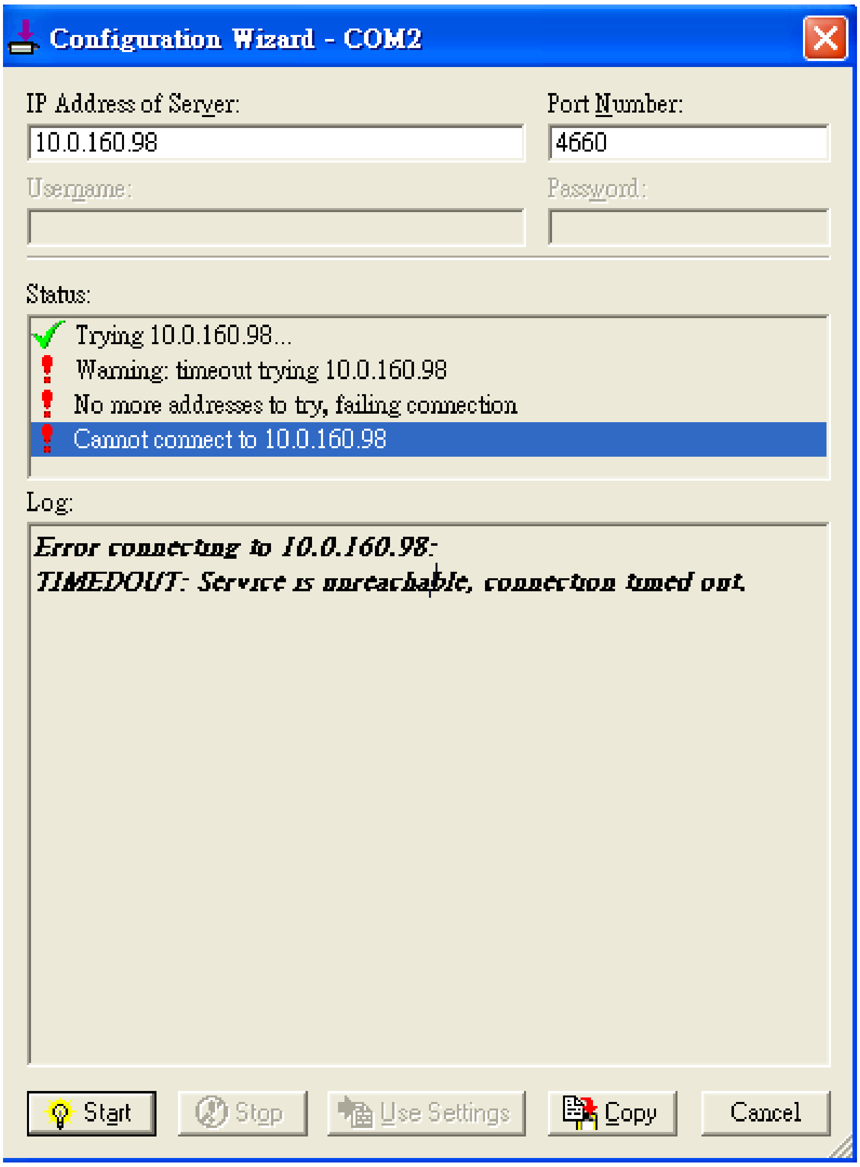
```
--------------------------------------
Recommendations:

Protocol: Telnet
COM Port Option: DTR Emulation disabled
COM Port Option: DSR Emulation disabled
COM Port Option: DCD Emulation disabled
COM Port Option: CTS Emulation disabled
Security: Disabled
-------------------------------
```

Figure 6.10 Auto Configure (formerly Configuration Wizard) Window for COM 1

6.3 *Exceptions*

This section lists possible exceptions which may occur when the user tested the VCOM connection through the **Auto Configure…** (formerly Configuring Wizard…) button**.** If there is a problem with the connection, there will be error(s) or warning(s) reported in the **Status and Log** text boxes**.** The possible correction or trouble shooting hint for each exception is given in each case**.**

- If the status reports with an exclamation mark with a message **"**Warning**:** timeout trying x**.**x**.**x**.**x**"** as shown in Figure 6.11, please recheck or correct the VCOM IP address and Port number configuration or the PC's network configuration**.**



Configuration Wizard - COM2

IP Address of Server: 10.0.160.98

Port Number: 4660

Username:

Password:

Status:

✓ Trying 10.0.160.98...

! Warning: timeout trying 10.0.160.98

! No more addresses to try, failing connection

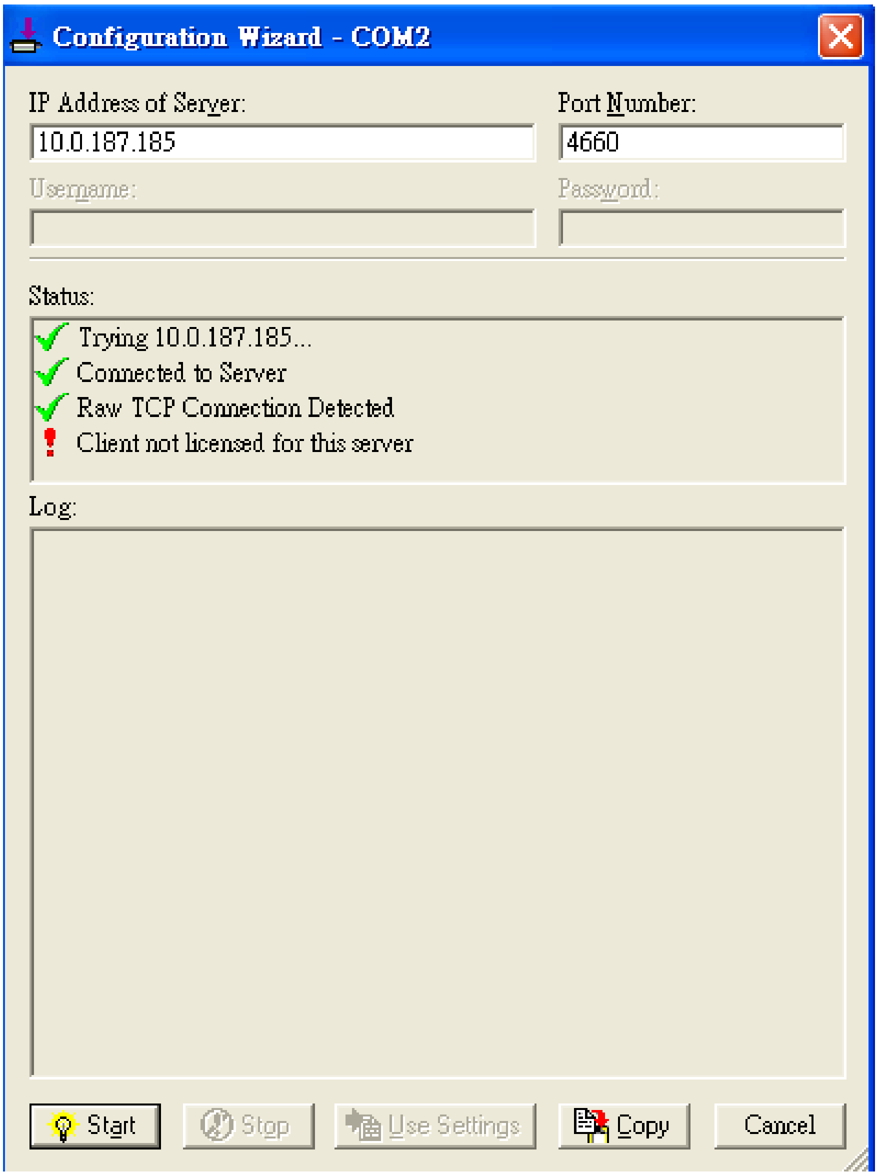
! Cannot connect to 10.0.160.98

Log:

```
Error connecting to 10.0.160.98:
TIMEDOUT: Service is unreachable, connection timed out.
```

Figure 6.11 Timeout Warning on VCOM Connection

- If the status reports with a check with a message **"Raw TCP Connection Detected"** and an exclamation mark with a message **"Client not licensed for this server"** as shown in Figure 6.12**.** Please enable the Virtual COM option in the serial Device server**.**



IP Address of Server: 10.0.187.185

Port Number: 4660

Username:

Password:

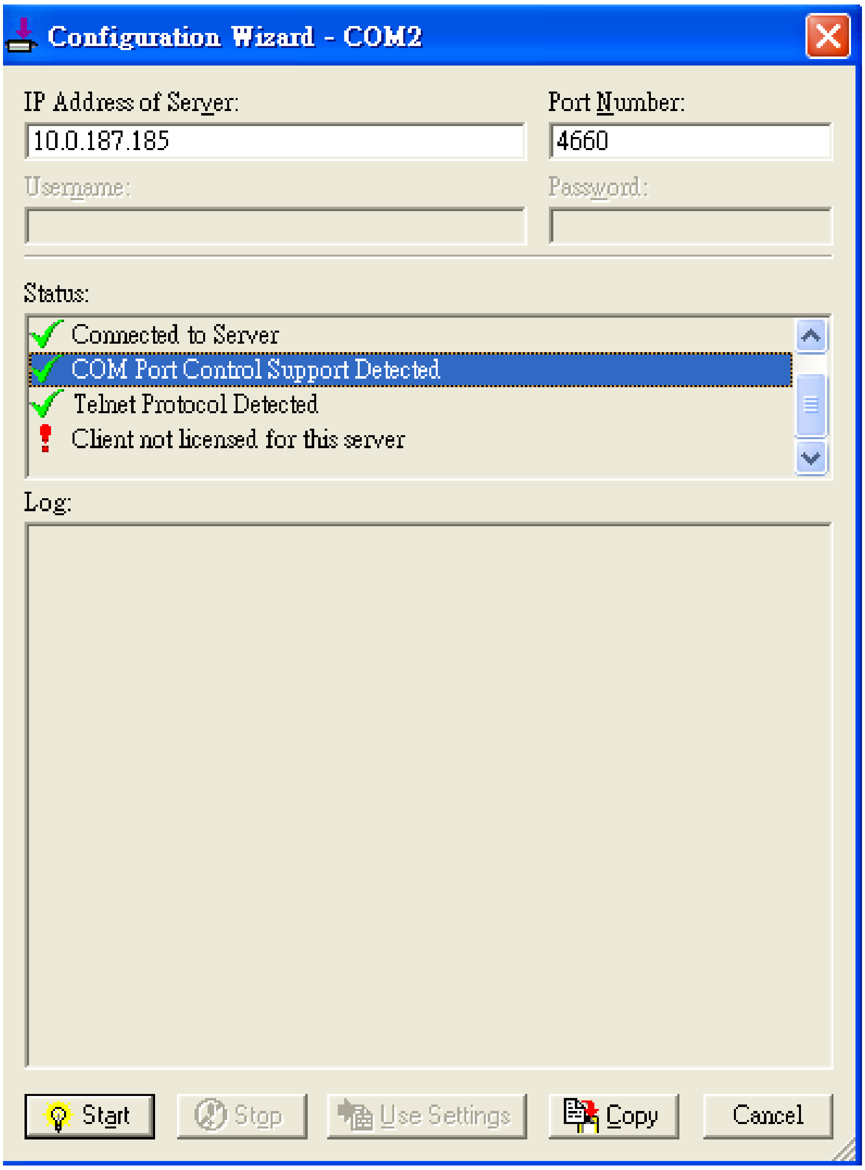
Status:

✓ Trying 10.0.187.185...
✓ Connected to Server
✓ Raw TCP Connection Detected
! Client not licensed for this server

Log:

Figure 6.12 Error of Client not licensed for this server

- If the status reports with a check with a message **“Telnet Protocol Detected”** and an exclamation mark with a message **“Client not licensed for this server”** as shown in Figure 6.13**.** This means that there is a licensing issue between the serial sateway (i**.**e**.** PS4000/8000/16000) and the Serial**/**IP Utility Software**.** Please contact TCPlink technical support to obtain the correct VCOM software**.**



Configuration Wizard - COM2

IP Address of Server: 10.0.187.185

Port Number: 4660

Username:

Password:

Status:

✓ Connected to Server

✓ COM Port Control Support Detected

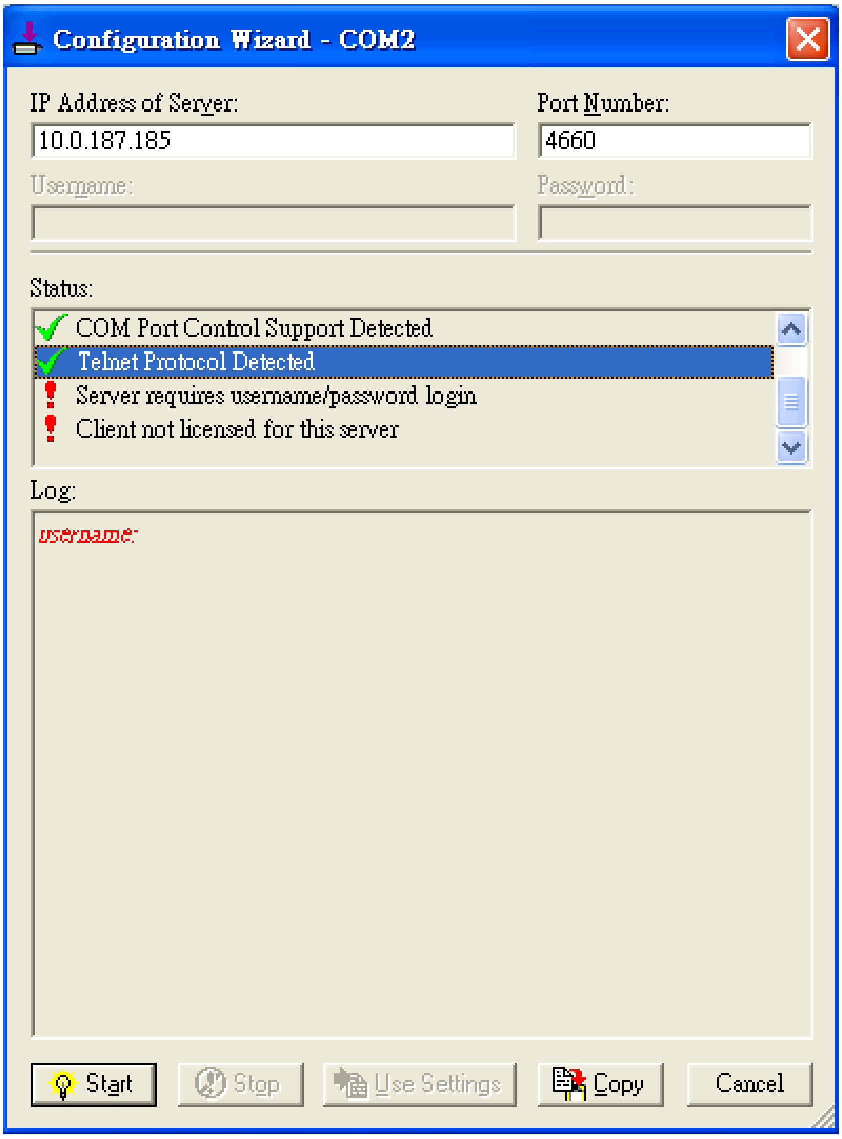
✓ Telnet Protocol Detected

! Client not licensed for this server

Log:

Figure 6.13 Licensing Issue of Serial/IP Utility Software

- If the status reports with an exclamation mark with a message **"Server requires username/password login"** as shown in Figure **6.14.** This means that the **VCOM Authentication** option in the serial device server (i**.**e**.** PS4000/8000/16000) is enabled but the **User Credentials** option in the **Serial/IP** utility software is not enabled**.** Please follow the steps in Section 4.15.2 for enabling the user credentials option and entering the username and the password**.**



IP Address of Server: 10.0.187.185

Port Number: 4660

Username:

Password:

Status:

✓ COM Port Control Support Detected

✓ Telnet Protocol Detected

! Server requires username/password login

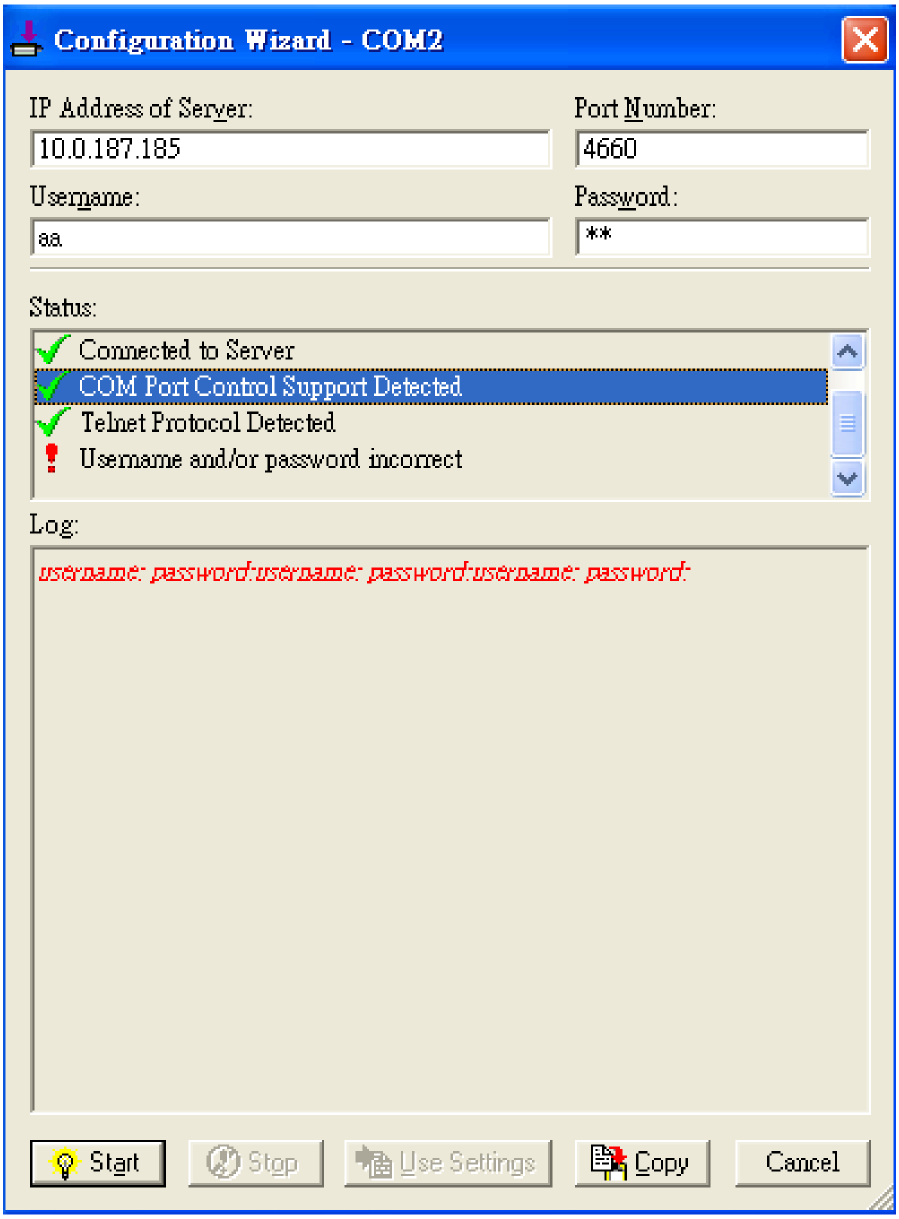
! Client not licensed for this server

Log:

```
username:
```

Figure 6.14 VCOM Authentication failed due to Missing Username/Password

- If the status reports with an exclamation mark with a message **"Username and/or password incorrect"** as shown in Figure 6.15. This means that the wrong username and/or password were entered and the authentication process failed.



IP Address of Server: 10.0.187.185

Port Number: 4660

Username: aa

Password: **

Status:

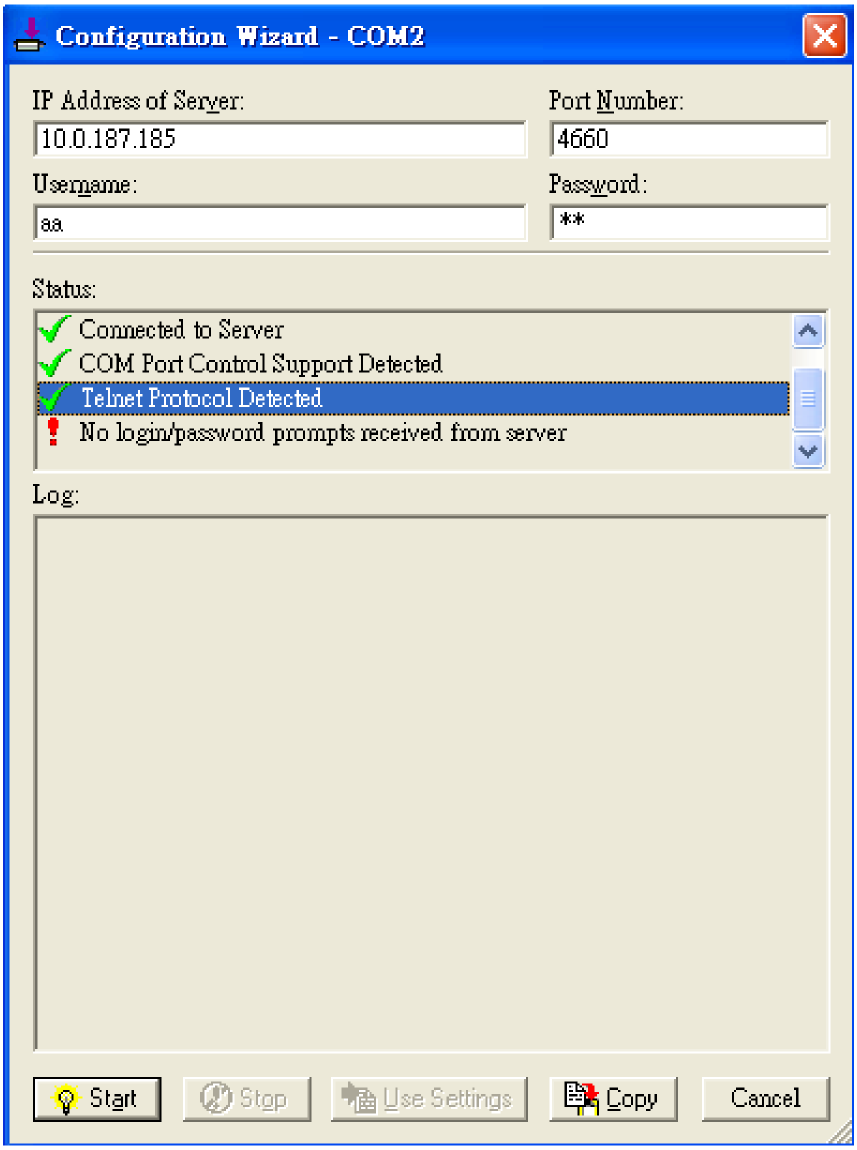
✓ Connected to Server
✓ COM Port Control Support Detected
✓ Telnet Protocol Detected
! Username and/or password incorrect

Log:

```
username: password:username: password:username: password:
```

Figure 6.15 VCOM Authentication failed due to incorrect Username and/or Password

- If the status reports with an exclamation mark with a message **"No login/password prompts received from server"** as shown in Figure 6.16. This means that the **User Credentials** option in the Serial/IP utility software is enabled but the VCOM Authentication option in the serial device server (i.e. PS4000/8000/16000) is not enabled. Please enable the **VCOM Authentication** option on the PS4000/8000/16000 by setting a new and non-blank administrator's Username and Password for PS4000/8000/16000 as described in Section 4.15.2. Note that the **Username** and the **Password** for VCOM authentication are the same username and password of PS4000/8000/16000 Web UI login. The default account, which has the username as "admin" and the password as "default", is considered as an unsecured account or no authentication option.



Configuration Wizard - COM2

IP Address of Server: 10.0.187.185

Port Number: 4660

Username: aa

Password: **

Status:

✓ Connected to Server

✓ COM Port Control Support Detected

✓ Telnet Protocol Detected

! No login/password prompts received from server

Log:

Figure 6.16 VCOM Authentication failed due to disabled VCOM Authentication on PS4000/8000/16000

6.4 *Using Serial/IP Port Monitor*

Serial/IP Port Monitor is another utility software provided for TCPlink's user. It allows user to monitor the activities or status of Virtual COM port and display the exchanged serial message which is called trace over the port.

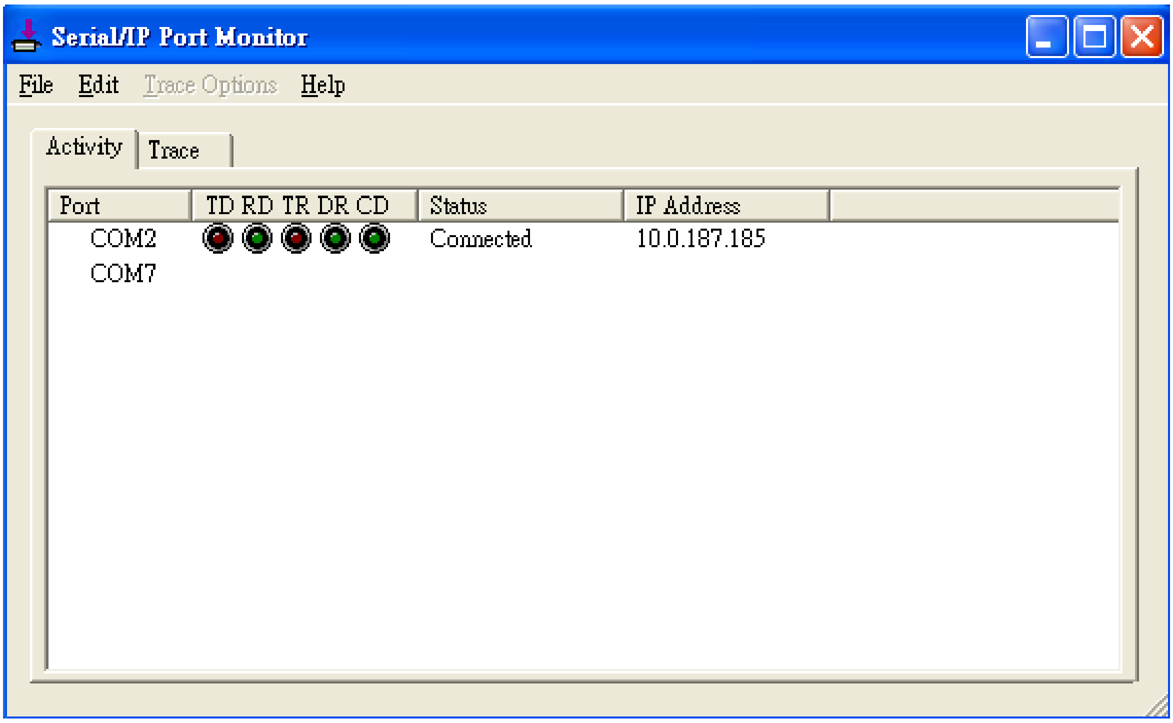
6.4.1 *Opening the Port Monitor*

The Serial/IP Port Monitor utility can be opened by one of the following methods:

- Click on Windows's Start menu → Select All Programs → Select Serial-IP → Select Port Monitor.
- Double click the Serial/IP tray icon in the Windows' notification area.
- In the Windows' notification area, right click on the Serial/IP tray icon and click on Port Monitor to open the Port Monitor.
- Click on the Port Monitor button in the Serial/IP Control Panel's window.

6.4.2 *The Activity Panel*

The **Activity** panel provides a real-time display of the status of all Serial/IP COM ports as shown in Figure 6.17. If the Virtual COM Port is opened and is properly configured to connect to a serial device server (i.e. PS4000/8000/16000), the status would be **Connected.** If Serial/IP utility software cannot find the specified serial device server, the status would be **Offline.**



Port	TD RD TR DR CD	Status	IP Address
COM2	● ● ● ● ●	Connected	10.0.187.185
COM7			

Figure 6.17 Activity Panel of Serial/IP Port Monitor

Each column in the **Activity Panel** is described as follows:

- **Port**: This is the virtual COM port number.
- **Line signal indicators**: Red color means no activity while green color indicates activity.
  - **TD** indicates data are being sent to the server.
  - **RD** indicates data are being received from the server.
  - **TR** (DTR) is the signal from the application to the server that the application has opened the virtual COM port. The most common use of DTR is to programmatically lower it to signal a modem to disconnect.

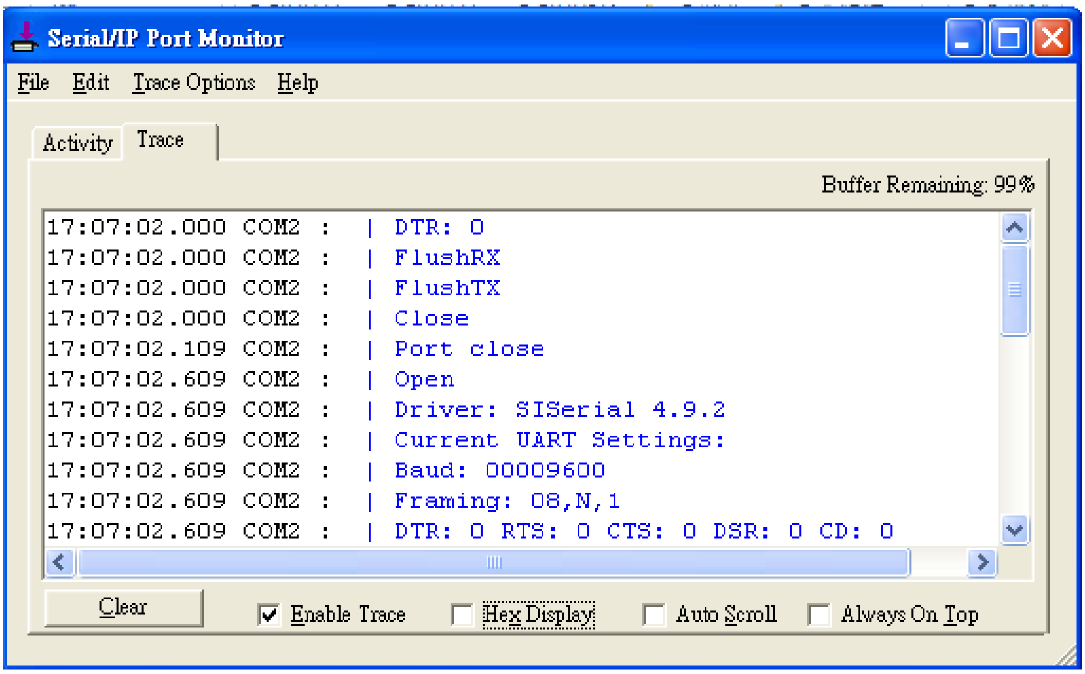
  - ○ **DR** (DSR) is the signal from the server to the application that a modem or serial device is connected to the server and ready to communicate.
  - ○ **CD** (DCD) is the signal from the server to the application that a modem has successfully negotiated a connection with another device.
- ■ **Status**: This indication the connection status of the software and serial device server which can be **connected** or **offline**.
- ■ **IP Address**: This is the IP address of the serial device server.

Notes:

- ■ The line signal indicators appear only when the virtual COM port is currently opened by an application.
- ■ The TR, DR, and CD indicators appear only if the COM Port Control protocol is being used or if the COM port options are enabled.

6.4.3 *The Trace Panel*

The **Trace** panel provides a detailed, time**-**stamped, real**-**time display of all Serial**/**IP COM ports operations as shown in Figure 6.18**.** Click on **Enable Trace** box to start logging Virtual COM communication**.** To stop logging, uncheck the **Enable Trace** box**.** The user can toggle the format of the display between ASCII text **(**more readable**)** and hexadecimal format **(**most detailed**)** by checking the **Hex Display** box**.** Click on **Auto Scroll** box will cause the display to show the most recent trace data continuously**.** To ensure that **Port Monitor'**s window is always on top of other application's windows, please check the **Always on Top** box**.** If you want to clear the displayed data in **Trace** panel, click on the **Clear** button**.**



```
17:07:02.000 COM2  :  | DTR: 0
17:07:02.000 COM2  :  | FlushRX
17:07:02.000 COM2  :  | FlushTX
17:07:02.000 COM2  :  | Close
17:07:02.109 COM2  :  | Port close
17:07:02.609 COM2  :  | Open
17:07:02.609 COM2  :  | Driver: SISerial 4.9.2
17:07:02.609 COM2  :  | Current UART Settings:
17:07:02.609 COM2  :  | Baud: 00009600
17:07:02.609 COM2  :  | Framing: 08,N,1
17:07:02.609 COM2  :  | DTR: 0 RTS: 0 CTS: 0 DSR: 0 CD: 0
```

☑ Enable Trace □ Hex Display □ Auto Scroll □ Always On Top

Figure 6.18 Trace Panel of Serial**/**IP Port Monitor

The pull-down menu of the **Port Monitor** windows allows the user to save the log and customize the capturing data of serial communication.

- ■ **File**: To save the log file which you can send the log to TCPlink for further analysis if problems occurs with the Virtual COM connection, please click on **File** menu then click **Save As**.
- ■ **Trace Options**:
  - ○ **Select Ports to Capture…:** This menu allows you to reduce the number of ports that are being traced to a subset of all configured Virtual COM ports. This feature can reduce the impact of tracing on memory and system performance for large applications.
  - ○ **Select Ports to Display…:** This menu allows you to reduce the number of ports that appear in the display to a subset of the ports being captured. For large applications, this feature provides a way to focus on ports of interest among all those being captured.

  - **Buffer Size:** This menu allows the change on the amount of RAM being used for tracing which can be normal or large.
  - **System Debug Output:** This menu allows user to enable the sending of trace data to the system debug channel and optionally put a label on them.

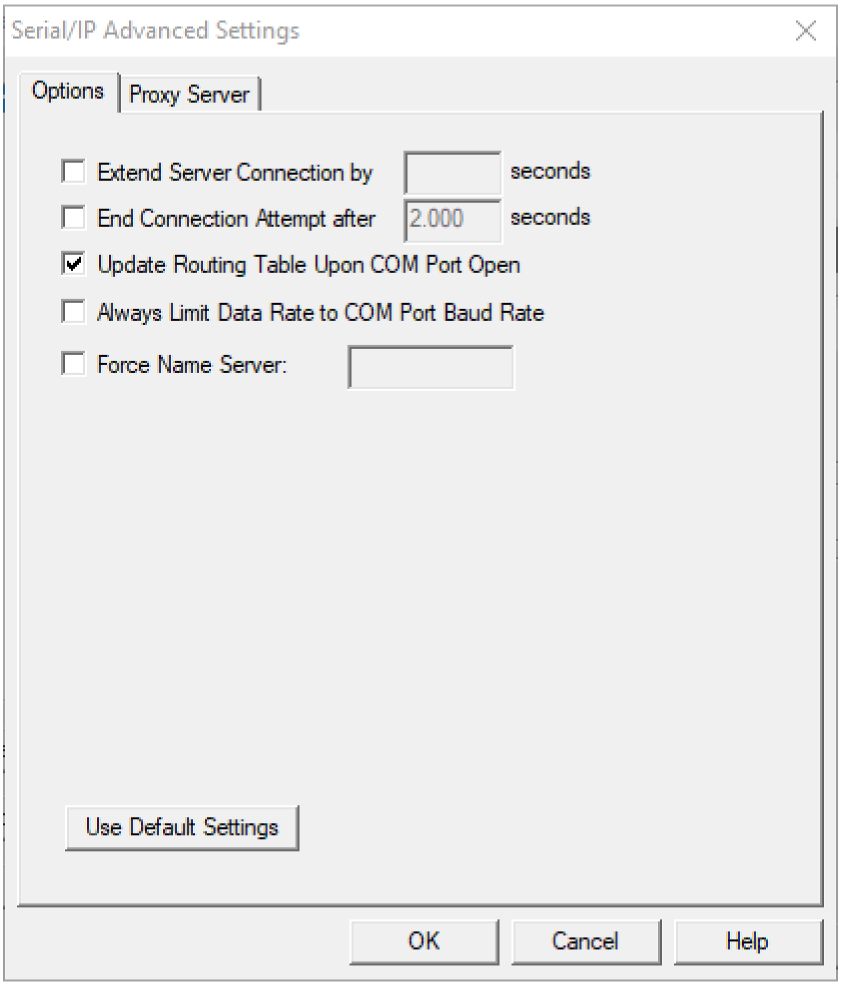
The **Trace** panel shows one serial event per line and in time order. Every event begins with a time tag. The transmit events will be shown in green and preceded by "»" while the receive event will be shown in red and preceded by "«". The control events will be shown in blue and preceded by “|”.

Notes:

- The **Trace** display covers up to 512k bytes of event data which is enough to cover a reasonably extensive tracing session. However, if the limit is reached, the trace clears and starts over.

6.5 *Serial/IP Advanced Settings*

In the **Serial/IP Control Panel**, you can click on the **Advanced…** button to open **Serial/IP Advanced Settings** window as shown in Figure 6.19**.** The **Serial/IP Advanced Settings** window contains two tabs**: Options** and **Proxy Server.** On the **Options** tab, you can click on **Use Default Settings** button to load the default settings**.** Detail description of each options and how to set a proxy server will be explained in the following subsections**.**



Serial/IP Advanced Settings

Options | Proxy Server

□ Extend Server Connection by [ ] seconds

□ End Connection Attempt after [2.000] seconds

☑ Update Routing Table Upon COM Port Open

□ Always Limit Data Rate to COM Port Baud Rate

□ Force Name Server: [ ]

Figure 6.19 Serial**/**IP Advanced Settings Window

6.5.1 *Advanced Setting Options*

Under the **Options** tab, you can enable a number of advanced settings and enter required parameters for Serial**/**IP software**.** Description of each option is provided as follows**.**

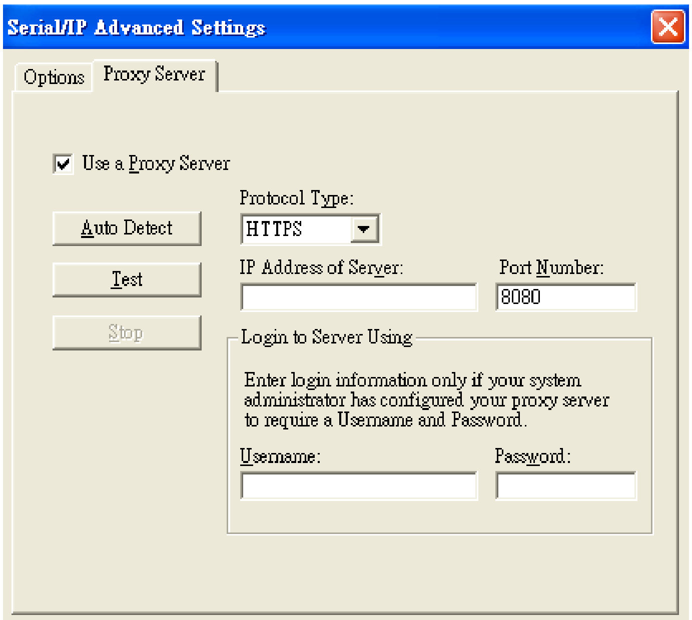
- **Extend Server Connection:** When enabled, this option maintains the TCP connection for specified amount of time after COM port is closed**.** The default time value is 8000 milliseconds**.**
- **End Connection Attempt after:** When enabled, this option terminates pending connection attempts if they do not succeed in the specified time**.** The default time value is 2000 milliseconds**.**
- **Update Routing Table Upon COM Port Open:** When enabled, this option maintains IP route to a server in a different subnet by modifying the IP routing table**.**
- **Always Limit Data Rate to COM Port Baud Rate:** When enabled, this option limits the data rate to the baud rate that is in effect for the virtual COM port**.**

- **Force Name Server:** This option allows the user to enter the desired Name Server IP address.

6.5.2 *Using Serial/IP with a Proxy Server*

The **Serial/IP Redirector** also supports TCP network connections made through a proxy server, which may be controlling access to external networks **(**such as the Internet**)** from a private network that lacks transparent IP**-**based routing, such as Network Address Translation **(**NAT**).** You can enable Serial**/**IP support of Virtual COM port through the proxy server using **Serial/IP Proxy Server settings.** You can find **Proxy Server** settings from the **Advanced Settings** windows and click on the **Proxy Server** tab as shown in

Figure 6.20**.** To enable the use of proxy server, check the box in front of **Use a Proxy Server** option**.** Then, select **the Protocol Type** which can be **HTTPS** or **Socks V4** or **Socks V5** from a drop**-**down list**.** Then, enter the IP address of the proxy server in the text box under **IP Address of Server** field and specify the **Port Number.** Note that the default port number for **HTTPS** is 8080, while for **Socks V4** and **V5** is 1080**.** Optionally, you can enter the **Username** and **Password** which may be required by your proxy server in the **Login to Server Using** box**.** Alternately, you can click on the **Auto Detect** button to have the software automatically detect the proxy server settings for you**.** Finally, you can test the proxy server settings by clicking on the **Test** button and stop the testing by clicking on **Stop** button**.**



☑ Use a Proxy Server

Protocol Type: HTTPS

IP Address of Server:

Port Number: 8080

Enter login information only if your system administrator has configured your proxy server to require a Username and Password.

Figure 6.20 Proxy Server Tab under Serial**/**IP Advanced Settings

7 Specifications

7.1 *Hardware*

Table 7.1 Hardware Specification

System	
CPU	32-bit ARM Based TI CPU AM3354 800MHz
Flash Memory	32MB
RAM	PS4000 DDR3 256MB PS8000/16000 DDR3 256MB
EEPROM	8 KB
Reset	Built-in Recessed Key (Restore to Factory Defaults)
Watchdog	Hardware built-in
Network	
Ethernet Interface	IEEE 802.3 10BaseT IEEE 802.3u 100BaseT(X) Auto-negotiation Auto MDI/MDI-X Connection: RJ45 x 2
Protocol	ICMP TCP UDP IPv4 HTTP Syslog DNS DHCP Client SNMPv1, v2c, v3 RADIUS SMTP NTP ARP Telnet RFC2217
Security	• VPN through IPsec tunnelling (max 64 tunnels) on LAN (software based)
Serial	
Serial Interface	RS-232/RS-422/RS-485 Software Selectable (Default: RS-232)
Serial Connector	Connector Type • PS16000 -16 Serial Ports (RJ45) • PS8000 - 8 Serial Ports (RJ45) • PS4000 – 4 Serial Ports (DB-9)
Serial Port Communication	Baud-rate: 1200 bps ~ 921600 bps Parity: None, Even, Odd, Mark, or Space Data Bits: 5, 6, 7, 8 Stop Bits: 1, 2 Software Selectable Flow Control: RTS/CTS (RS-232 only), XON/XOFF, None
LED Indicator	
LED indication	Power x 2 (PS4000 – PS8000 – PS16000 x 1) RUN x 1 ALARM x 1 LAN: • x 2 COM port: • x 16 (PS16000); • x 8 (PS8000); • x 4 (PS4000)
Power Requirement & EMC	

Input	PS8000 / 16000 : • Single 100~240 VAC (EU/US versions) • Single 24~48 VDC (DC version) PS4000 : Redundant 9~48 VDC	
Consumption	Max.17.5 W (PS8000/16000) Max. 7.8W(PS4000)	
EMI/EMC	FCC Part 15, Subpart B, Class A EN 55032, Class B, EN 61000-6-2, Class B EN 61000-3-2, EN 61000-3-3 EN 55024, EN 61000-6-4	
Mechanical		
Dimensions (W x H x D, mm)	PS4000: 55 mm x 145 mm x 113mm (2.17 x 5.17 x 4.45 in) PS8000: 436 mm x 43.5 mm x 200 mm (17.17 x 1.71 x 7.87 in) PS16000: 436 mm x 43.5 mm x 200 mm (17.17 x 1.71 x 7.87 in)	
Enclosure	IP30 protection, metal housing	
Environmental		
Temperature	Operations	-40℃ ~ 85℃ (-40℉ ~ 185℉) (PS8000/16000 -20℃ ~ 70℃)
	Storage	-40℃ ~ 85℃ (-40℉ ~ 185℉)
Relative Humidity	5% ~ 95%, 55℃ Non-condensing	

7.2 *Serial port Pin Assignments*

7.2.1 *PS4000 Pin Assignments*

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

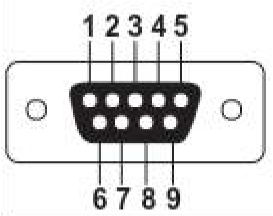


Figure 7.1 DB9 Pin Number

Table 7.2 PS4000 Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors

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

7.2.2 *PS8000/16000 Pin Assignments*

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

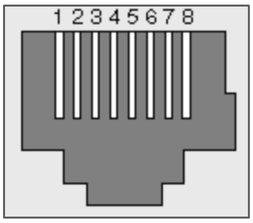


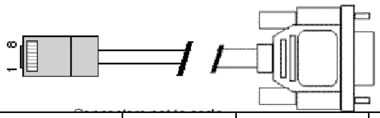
Figure 7.2 PS8000/16000 Serial port on RJ45 Pin Numbering

Table 7.3 PS8000/16000 Pin Assignment for RJ45 to RS-232/RS422/RS-485 Connectors

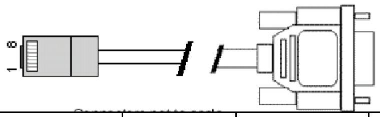
Pin#	RS-232	RS-422	RS-485
1	CTS	-	-
2	DSR	Rx -	Data -
3	RxD	Rx +	Data +
4	GND	GND	SG (Signal Ground)
5	DCD	-	-
6	TxD	Tx +	-
7	DTR	Tx -	-
8	RTS	-	-

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

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

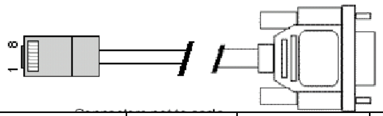
RJ45			Straight Through Female DB9	
				
RTS	Pin 1	⇔	Pin 7	RTS
DTR	Pin 2	⇔	Pin 4	DTR
TXD	Pin 3	⇔	Pin 3	TXD
SG	Pin 4	⇔	Pin 5	SG
SG	Pin 5	⇔		
RXD	Pin 6	⇔	Pin 2	RXD
DSR	Pin 7	⇔	Pin 6	DSR
CTS	Pin 8	⇔	Pin 8	CTS

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

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

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

50891781G - RJ45 TO DB9 CABLE-MALE(OLD)

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

50801561G- RJ-45 TO DB9 CABLE-MALE(2020/10/15~)

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

7.2.3 *PS4000/8000/16000 Pin Assignments for LAN Interface*

RJ45 connectors for 10/100/1000Base-T(X) Ethernet

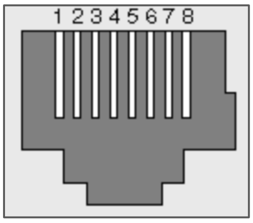


Figure 7.3 PS4000/8000/16000 Ethernet Port on RJ45 with Pin Numbering

Table 7.4 PS4000/8000/16000 Pin Assignment for RJ-45 Connector

10/100/1000Base-T(x)								
Pin#	1	2	3	4	5	6	7	8
Signal	Tx+	Tx-	Rx+	-	-	Rx-	-	-
1000Base-T								
Pin#	1	2	3	4	5	6	7	8
Signal	BI_DA+	BI_DA-	BI_DB+	BI_DC+	BI_DC-	BI_DB-	BI_DD+	BI_DD-

7.3 *LED Indicators*

Table 7.5 Color Interpretation of LED Indicators of PS4000/8000/16000

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
RUN	🟢 Green	Blinking	AP Firmware is running normally
		On/Off	System is not ready or halt
LAN	🟠 Orange (Speed)	On	Ethernet is transmitting at 1 Gbps
		Blinking slowly	Ethernet is transmitting at 100 Mbps
		Off	Ethernet is transmitting at 10 Mbps
	🟢 Green (Data)	Blinking	Ethernet data is transmitting
		Off	Ethernet has no data to transmit

7.4 *Software*

Table 7.6 Software Tools and Utilities

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

8 Emergency System Recovery

If the device becomes inaccessible and the management utility cannot find the device, please use the following procedure to recover the devices over Trivial File Transfer Protocol (TFTP).

8.1 *System Recovery Procedures*

System recovery is based on the TFTP Client embedded in the device. It can recover the device from a bad firmware or other unknown reasons corrupting the firmware image inside the flash memory. Please follow the procedures below to force PS4000/8000/16000 to download a valid firmware from the TFTP Server to recover its operating system.

Table 8.1 Default Settings for System Recovery Procedure

Default Settings	
TFTP Server	10.0.50.201
TFTP Server Subnet Mask	255.255.0.0
Name of firmware Image*	firmware.dld
*This firmware image can be obtained from TCPlink's website.	

- If the device is beeping continuously after power up, this means that the bootloader is damaged and there is no way to recover it. Please contact TCPlink directly to obtain RMA number for further solutions.
- Obtain and setup a TFTP server on your PC. Make sure that the PC's network settings are set properly according to the default setting in the above table.
- Rename the firmware image that you obtained from our website to "firmware.dld" and place it in the TFTP Server's root directory. For Solarwinds TFTP Server, it is usually C:\TFTP-Root.
- Make sure that the device is powered OFF and the Ethernet cable is plugged in.
- Press and hold the "**Reset**" button above the USB port then power ON the device. If the bootloader is still functioning, the user will hear one long beep followed by two shorter beeps.
- Release the reset pin after hearing seven consecutive short beeps. Then, the device will automatically request files from TFTP Server. Please wait until the device shows up on the Device Management Utility. This process could take up to five minutes or even more.

Important Note

Free TFTP Servers can be downloaded from the following locations:

Solarwinds TFTP Server	http://www.solarwinds.com/products/freetools/free_tftp_server.aspx
Note: for Solarwinds, please remember to Start the TFTP Server Service, the default state of the TFTP is Stop.	
TFTPD32 TFTP Server	http://tftpd32.jounin.net/tftpd32.html

9 Warranty

Limited Warranty Conditions

Products supplied by TCPlink, Inc. are covered in this warranty for undesired performance or defects resulting from shipping, or any other event deemed to be the result of TCPlink, 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

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

Warranty

TCPlink, Inc. provides a 5-year maximum warranty for Industrial Serial Device Server products.

TCPlink
www.tcplink.com

TCPlink, Inc.

www.tcplink.com

Korea HEADQUARTER:

1702ho, 288, Digital-ro
Guro-Gu, Seoul, South Korea, 08390
Tel: +82-2-711-2508
Fax: +82-2-711-2509