



## STE-6104C-T-V2

**4-Port Industrial Serial RS232/422/485 to Ethernet Device Server, with  
Dual LAN; EOT: -40°C to 85°C; Version 2 Hardware**



## User Manual

Version 1.0  
(March 2021)



## **Important Announcement**

The information contained in this document is the property of Antaira Technologies, LLC and is supplied for the sole purpose of operation and maintenance of products of Antaira Technologies, LLC. No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, store in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of Antaira Technologies, LLC.

### **Published by**

Antaira Technologies, LLC

Toll-Free: 1-844-268-2472

E-mail: [info@antaira.com](mailto:info@antaira.com)

Website: [www.antaira.com](http://www.antaira.com)

Copyright 2021 Antaira Technologies, LLC. All rights reserved.

All other product names referenced herein are registered trademarks of their respective companies.

Thank you for purchasing the STE-6104C Serial Device Server Series product. This document intends to provide customers with brief descriptions about the product and to assist customers to get started. For detailed information and operations of the product, please refer to the product user manual in the product CD.

## **FCC Warning**

### **Class A for Serial Device Server**

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 radiates radio frequency energy and if not installed and used in accordance with the instructions 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 their own expenses.

*Antaira Technologies - Industrial Serial Device Server*  
**STE-6104C-T-V2 - User Manual - v1.0**

---

A shielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord can be used.

Use only shielded cables to connect other devices to this equipment by RS232 or RS485 ports.

Be cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

# Table of Contents

<b>1 Introduction</b>	<b>1</b>
1.1 Overview	1
1.2 Features	2
<b>2 Getting Started</b>	<b>3</b>
2.1 Packing List	3
2.2 Appearance, Front Panel and Top Views	4
2.3 First Time Installation	5
2.4 Factory Default Settings	5
2.4.1 Network Default Settings	5
2.4.2 Other Default Settings	6
<b>3 Configuration and Setup</b>	<b>7</b>
3.1 Configuration of Network Parameters Through Device Management Utility	7
3.2 Configuration through Web/CLI Interface	10
3.3 Configuring Automatic IP Assignment with DHCP	13
3.4 Web Overview	14
3.5 Wizard	15
3.6 Network Settings	21
3.7 Firewall Setting	22
3.7.1 IP Filter	23
3.8 Serial	25
3.8.1 COM Port Overview	26
3.8.2 COM Configuration	27
3.8.3 COM Configuration: Advanced Settings	28
3.9 VPN	31
3.10 PPTP Settings	32
3.11 OpenVPN Settings	33
3.11.1 OpenVPN Settings	34
3.11.2 OpenVPN Keys	36
3.11.3 OpenVPN Status	38
3.12 IPsec Settings	39
3.12.1 IPsec Settings	43
3.12.2 IPsec Status	49
3.12.3 Examples of IPsec Settings	50
3.12.3.1 Host-to-Host Connections	50

3.12.3.2 Host-to-Network Connections	52
3.12.3.3 Network-to-Network (Subnet-to-Subnet) Connections	54
3.13 Spanning Tree	56
3.13.1 Spanning Tree's Setting	57
3.13.2 Spanning Tree's Bridge Info	59
3.13.3 Spanning Tree's Port Settings	60
3.14 SNMP/ALERT Settings	63
3.15 Email Settings	65
3.16 Log Settings	67
3.16.1 System Log Settings	67
3.16.2 System Log	68
3.16.3 COM Log Settings	69
3.16.4 COM Log	71
3.17 System Setup	72
3.17.1 Date/Time Settings	72
3.17.2 Admin Settings	74
3.17.3 Firmware Upgrade	75
3.17.4 Backup/Restore Settings	76
3.17.5 Ping	77
3.18 Reboot	78
<b>4 Link Modes and Applications</b>	<b>80</b>
4.1 Link Mode Configuration	80
4.1.1 Link Mode: Configure STE-6104C as a TCP Server	80
4.1.2 Link Mode: Configure STE-6104C as a TCP Client	85
4.1.3 Link Mode: Configure STE-6104C in UDP	90
4.2 Link Mode Applications	94
4.2.1 TCP Server Application: Enable Virtual COM	94
4.2.2 TCP Server Application: Enable RFC 2217 through Virtual COM	95
4.2.3 TCP Client Application: Enable Virtual COM	96
4.2.4 TCP Client Application: Enable RFC 2217 through Virtual COM	97
4.2.5 TCP Server Application: Configure STE-6104C as a Pair Connection Master	97
4.2.6 TCP Client Application: Configure STE-6104C as a Pair Connection Slave	98
4.2.7 TCP Server Application: Enable Reverse Telnet	99
<b>5 VCOM Installation &amp; Troubleshooting</b>	<b>101</b>
5.1 Enabling VCOM	101
5.1.1 VCOM Driver Setup	103
5.1.2 Limitation	104

5.1.3 Installation	104
5.1.4 Uninstallation	104
5.2 Enable VCOM in Serial Device Servers and Select VCOM in Windows	105
5.2.1 Enable VCOM in Serial Device Servers	105
5.2.2 Running Serial/IP Software Utility in Windows	106
5.2.3 Configuring VCOM Ports	108
5.3 Exceptions	112
5.4 Using Serial/IP Port Monitor	118
5.4.1 Opening the Port Monitor	118
5.4.2 The Activity Panel	119
5.4.3 The Trace Panel	120
5.5 Serial/IP Advanced Settings	122
5.5.1 Advanced Setting Options	123
5.5.2 Using Serial/IP with a Proxy Server	124
<b>6 Specifications</b>	<b>126</b>
6.1 Hardware	126
6.2 Serial Port Pin Assignments	127
6.2.1 Pin Assignments	127
6.3 LED Indicators	128
6.4 Software	129
<b>7 Emergency System Recovery</b>	<b>130</b>
7.1 System Recovery Procedures	130

# 1 Introduction

## 1.1 Overview

The STE-6104C model is an industrial Ethernet serial device server which acts as a gateway for communication between an Ethernet (TCP/UDP) port and an RS-232/RS-422/RS-485 port. The information conveyed by the STE-6104C 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 the 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 STE-6104C model. In normal PCs or laptops, a virtual COM port can be created using our virtual COM software to fetch serial data from the STE-6104C remotely over Ethernet.

With the STE-6104C 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 1.1 illustrates an example of multiple devices connected to the industrial serial device server. A PC connects to the industrial serial device server via an Ethernet interface, and a monitored device reports to the industrial serial server via an RS232/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 RS232/RS-422/RS-485 to an industrial serial device server.

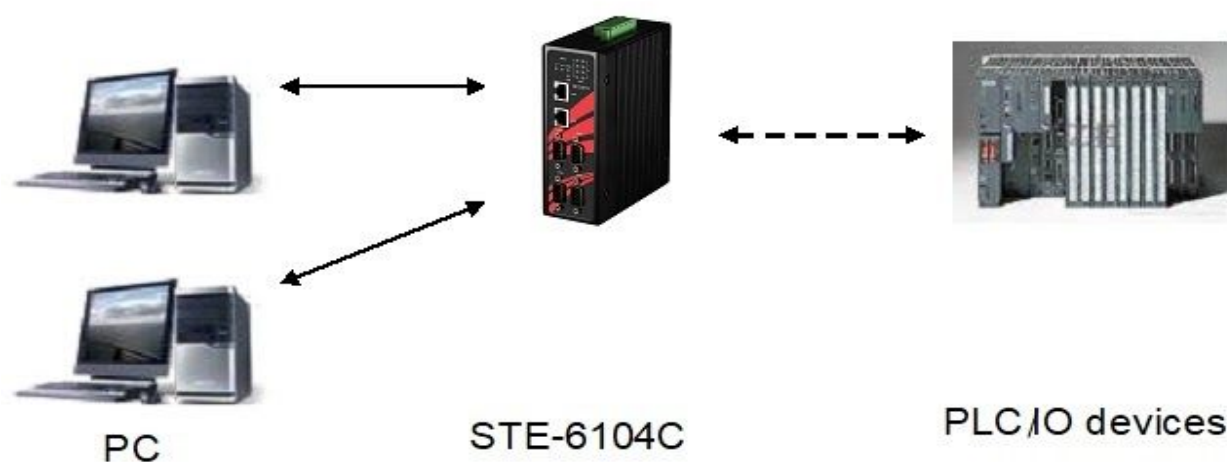


Figure 1.1 - An Application of STE-6104C Industrial Serial Device Server with Multiple Devices

## 1.2 Features

The STE-6104C Industrial Serial Device Server Series has the below features:

- 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/ Windows Utility (Device Management Utility)
- Rugged metal housing with IP30 protection for wall or DIN-Rail mount
- Wide range power supply input between 12 to 48 VDC

---

### Caution

Starting 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 the unit to cool for 5 minutes before touching.



## 2 Getting Started

### 2.1 Packing List

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

Item	Quantity	Description
STE-6104C-T-V2	1	Industrial Serial Device Server
Mounting Kit	1	DIN Rail Kit (Already mounted to the device)
Terminal Block	1	7-pin 5.08mm lockable terminal block
Documentation	1	Hardware Installation Guide

*Table 2.1 - Packing List*

**\*Note:**

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

## 2.2 Appearance, Front Panel and Top Views

The following figures show the STE-6104C model series' front panel and top view.

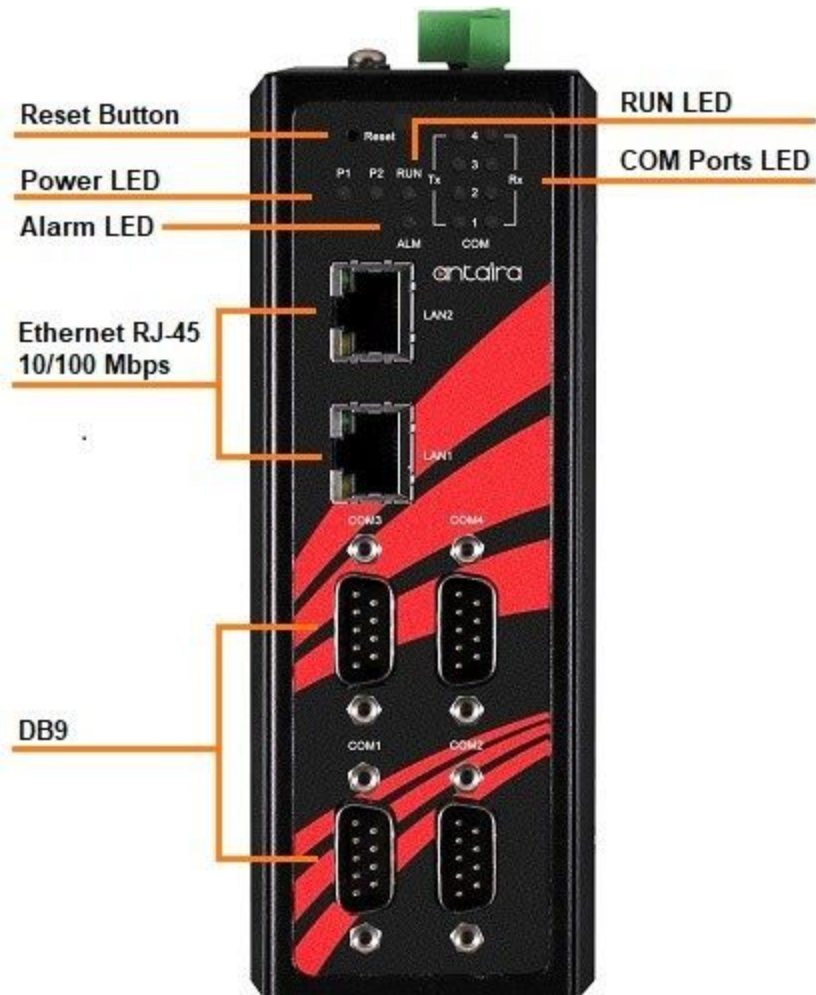
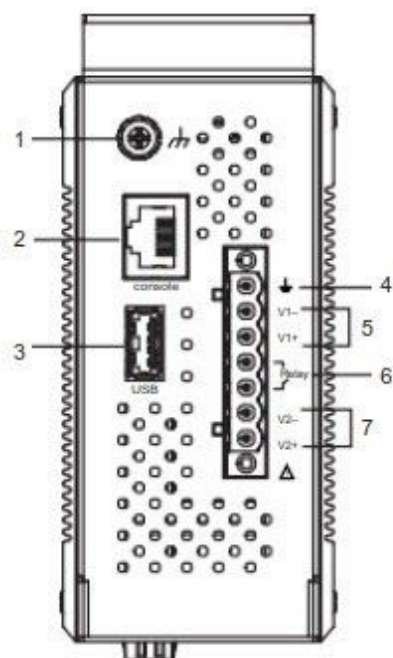


Figure 2.1 - Front Panel and LED Indicators



1. Grounding Screw
2. Console
3. Type A USB for storage
4. Frame Ground
5. Terminal for Power1
6. Relay Output with current carrying capacity of 1A@30 VDC (Normal Open)
7. Terminal for Power2

Figure 2.2 - Top View

## 2.3 First Time Installation

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

## 2.4 Factory Default Settings

### 2.4.1 Network Default Settings

The STE-6104C industrial serial device server model is equipped with two LAN interfaces with two default IP addresses. Its default network parameters are listed in *Table 2.2*.

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	

Table 2.2 - Network Default Setting

## 2.4.2 Other Default Settings

The STE-6104C industrial serial device server comes with the following default settings.

Parameter	Default Values
<b>Security</b>	
User Name	admin
Password	default
<b>Serial</b>	
COM1	RS232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM2	RS232, 9600 bps, 8 data bits, No Parity bit, 1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM3	RS232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM4	RS232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
<b>SNMP</b>	
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

*Table 2.3 - Security, Serial, and SNMP Default Settings*

**\*Note:** Press the “Reset” button on the front panel for 5 seconds to restore the STE-6104C series industrial serial device server to the factory default settings.

## 3 Configuration and Setup

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

### 3.1 Configuration of Network Parameters Through Device Management Utility

Please install Antaira's configuration utility program called **Device Management Utility®** that comes with the product on a CD or it can be downloaded from our website ([www.antaira.com](http://www.antaira.com)). For more information on how to install **Device Management Utility®**, please refer to the manual that comes on the product CD. After you start **Device Management Utility®**, if the STE-6104C 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 STE-6104C device and list it on the **Device Management Utility®**'s window. Alternatively, if you did not see your STE-6104C device on your network, press "Rescan" icon, a list of devices, including your STE-6104C device currently connected to the network will be shown in the window of **Device Management Utility®** as shown in Figure 3.1.

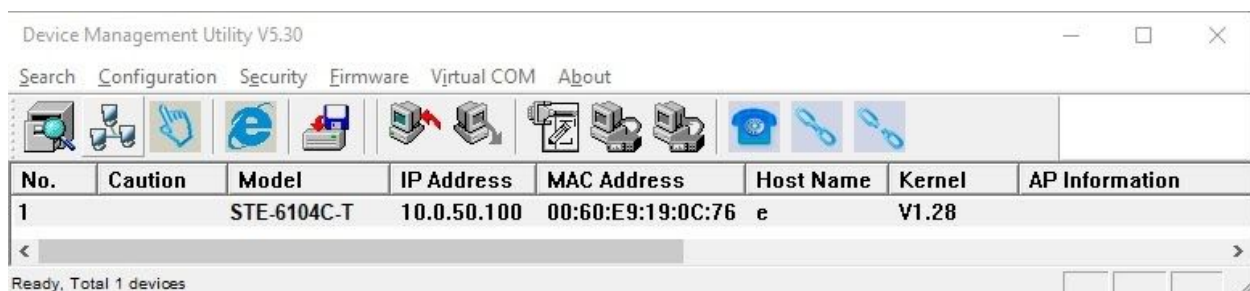


Figure 3.1 - List of Device in Device Management Utility

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

Sometimes the STE-6104C device might not be in the same subnet as your PC; therefore, you will have to use Antaira's utility to locate it in your virtual environment. To configure each device, first click to select the desired STE-6104C device (default IP: 10.0.50.100) in the list of **Device Management Utility®**, and then click "Configuration à Network..." (or Ctrl+N) menu on **Device Management Utility®** as shown in

Figure 3.2 or click on the second icon called **Network** on the menu icon bar, and a pop-up window will appear as shown in Figure 3.3.

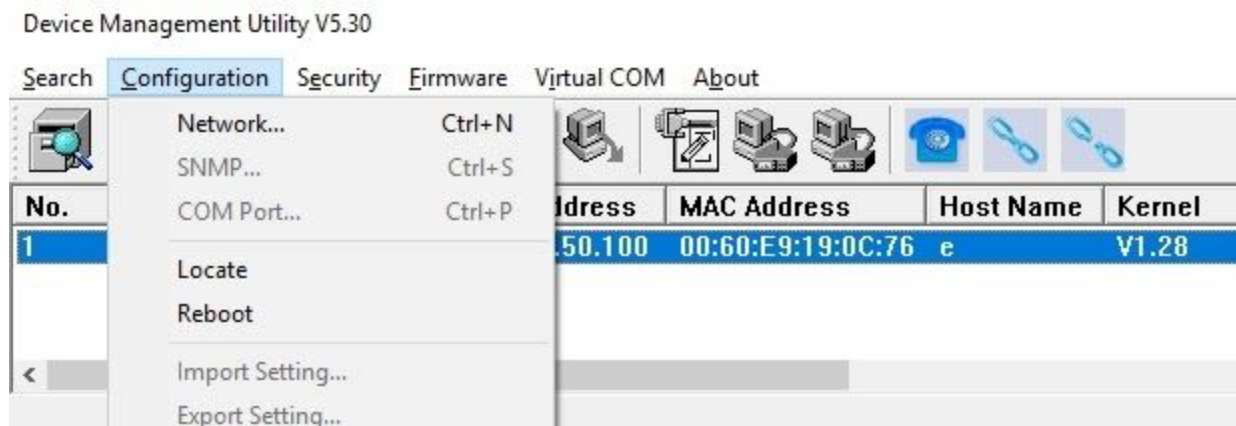


Figure 3.2 - Pull-down Menu of Configuration and Network

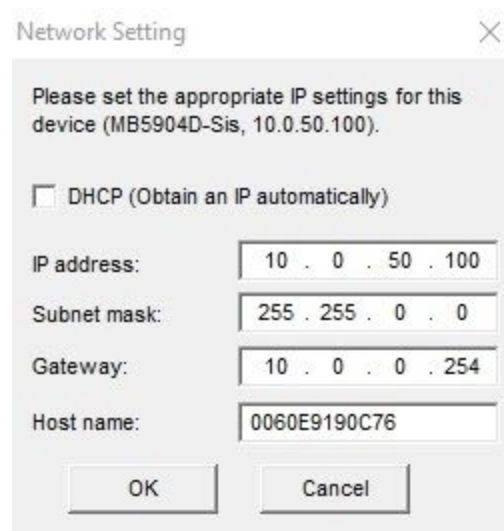


Figure 3.3 - Pop-up Window of Network Setting

You may proceed 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 3.3. 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 3.4. The default username is "**admin**", while the default password is "**default**". After clicking on the **Authorize** button, a notification window will pop-up as shown in Figure 3.5 and some devices may need to be restarted. After the device is restarted (for some models), it will beep twice to indicate that the unit is running normally. Then, the STE-6104C 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:** If you did not change the IP address but changed another parameter, you may encounter another notification window as shown in *Figure 3.6*.



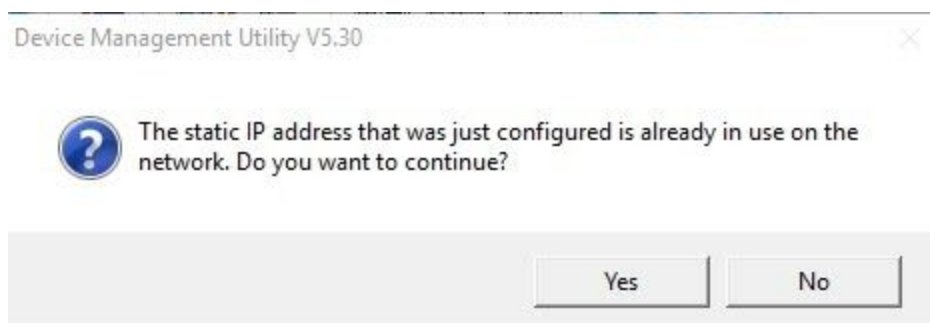
A dialog box for authorization. It contains two text input fields: 'User Name:' with 'admin' entered, and 'Password:' which is empty. Below these fields is a checkbox labeled 'Apply for all selected devices' which is unchecked. At the bottom right are two buttons: 'Authorize' and 'Cancel'.

*Figure 3.4 - Authorization for Change of Network Setting*



*Figure 3.5 - Pop-up Notification Window after Authorization*

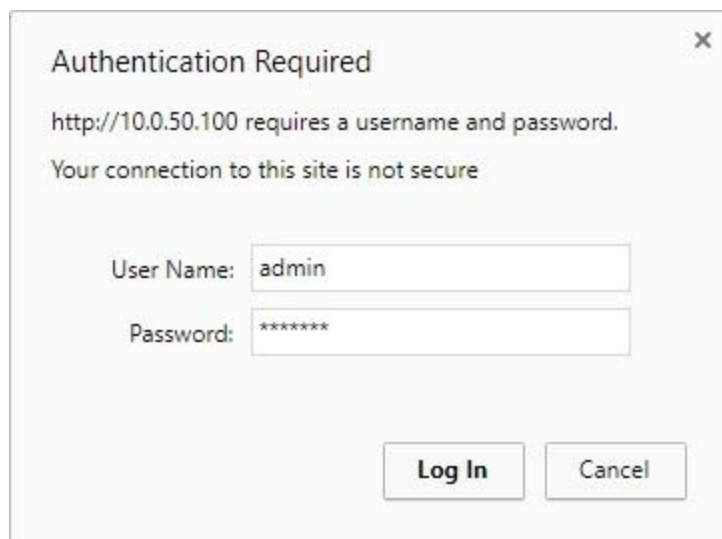
Please consult your system administrator if you do not know your network's subnet mask and gateway address.



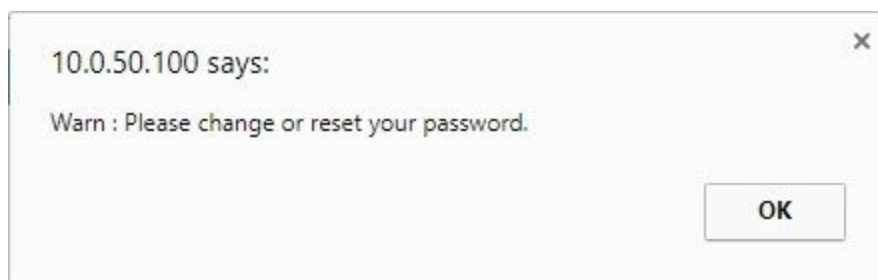
*Figure 3.6 - Pop-up Notification Window when there is the Same IP address in the Network*

## 3.2 Configuration through Web/CLI Interface

Every STE-6104C 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 "default") for accessing the web interface as shown in *Figure 3.7*. 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 3.8*. *Figure 3.9* illustrates the overview page of the web interface. *Figure 3.10* lists all the menus and submenus for web configuration. Please see Section 2.4 for default values.

A dialog box titled "Authentication Required" with a close button (X) in the top right corner. The text inside reads: "http://10.0.50.100 requires a username and password." followed by "Your connection to this site is not secure" in a smaller, lighter font. Below this, there are two input fields: "User Name:" with the text "admin" entered, and "Password:" with "\*\*\*\*\*" entered. At the bottom right, there are two buttons: "Log In" and "Cancel".

*Figure 3.7 - Authentication Required for Accessing Web Interface*

A warning pop-up window with a close button (X) in the top right corner. The text inside reads: "10.0.50.100 says:" followed by "Warn : Please change or reset your password." in a smaller, lighter font. At the bottom right, there is a single button labeled "OK".

*Figure 3.8 - Warning Pop-up Window for Changing or Resetting Password from Default Value*



The screenshot displays the Antaira web interface. On the left is a sidebar menu with the following items: + System Status, Wizard, Network Settings, + Firewall Setting, + Serial, SNMP/ALERT Settings, E-mail Settings, + VPN, + Spanning Tree, + Log Settings, + System Setup, and Reboot. The main content area has a header bar with 'System Status > Overview' and 'STE-6104C-T-V2'. Below this, the 'Overview' section is titled 'The general information of Antaira - Serial Server'. It contains two tables: 'Device Information' and 'Network Information'.

Device Information		
Model Name	STE-6104C-T-V2	
Device Name	7CCB0D0640A8	
Kernel Version	1.01	
AP Version	1.03	
Bootloader Version	1.01	

Network Information		
LAN1	MAC Address	7c:cb:0d:06:40:a8
	IP Address	10.0.50.100
LAN2	MAC Address	7c:cb:0d:06:40:a9
	IP Address	192.168.1.1

Figure 3.9 - Overview Web Page of STE-6104C Industrial Serial Device Server

- System Status
  - Overview
- Wizard
- Network Settings
- Firewall Setting
  - IP Filter
- Serial
  - COM1
  - COM2
  - COM3
  - COM4
- SNMP/ALERT Settings
- E-mail Settings
- + VPN
- Spanning Tree
  - Setting
  - Bridge Info
  - Port Setting
- + Log Settings
- + System Setup
  - Reboot

*Figure 3.10 - Map of Configuring Web Page on STE-6104C Industrial Serial Device Server*

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 the STE-6104C Industrial Serial Device Server Series. Please go to its corresponding section for a detailed explanation.

Furthermore, you can also use the CLI interface through Console port/Telnet/SSH to configure STE-6104C. 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	<input type="text" value="admin"/>
Old password	<input type="password"/>
New password	<input type="password"/>
Repeat new password	<input type="password"/>

Web mode	
Web Mode	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS

Access control	
SSH	<input checked="" type="checkbox"/> Enable
Telnet	<input checked="" type="checkbox"/> Enable

Figure 3.11 - Access Control

```
-----
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 3.12 - CLI Interface

Please note that if you change the IP address, you will need to restart the STE-6104C.

## 3.3 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 3.3* using Antaira's **Device Management Utility**® and then restart the device. Once restarted, the IP address will be configured automatically.

## 3.4 Web Overview

In this section, current information on the device's status and settings will be displayed.

System Status > Overview

STE-6104C-T-V2

Overview

The general information of Antaira - Serial Server

Device Information		
Model Name	STE-6104C-T-V2	
Device Name	7CCB0D0640A8	
Kernel Version	1.01	
AP Version	1.03	
Bootloader Version	1.01	

Network Information		
LAN1	MAC Address	7c:cb:0d:06:40:a8
	IP Address	10.0.50.100
LAN2	MAC Address	7c:cb:0d:06:40:a9
	IP Address	192.168.1.1

*Figure 3.13 - Overview Web Page*

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

### Device Information

- **Model Name**, as its name implies, shows the device's model.
- **Device Name** shows a given name of the device in which the default value is the MAC address of the LAN interface.
- **Kernel Version** is the value of the version of the kernel firmware of the device.
- **AP Version** is the value of the version of the application firmware of the device.
- **Bootloader Version** is the version of the program that loads the operating system of the device.

- **CPLD Version** is the version of the Complex Programmable Logic Device (logic device) of the device.

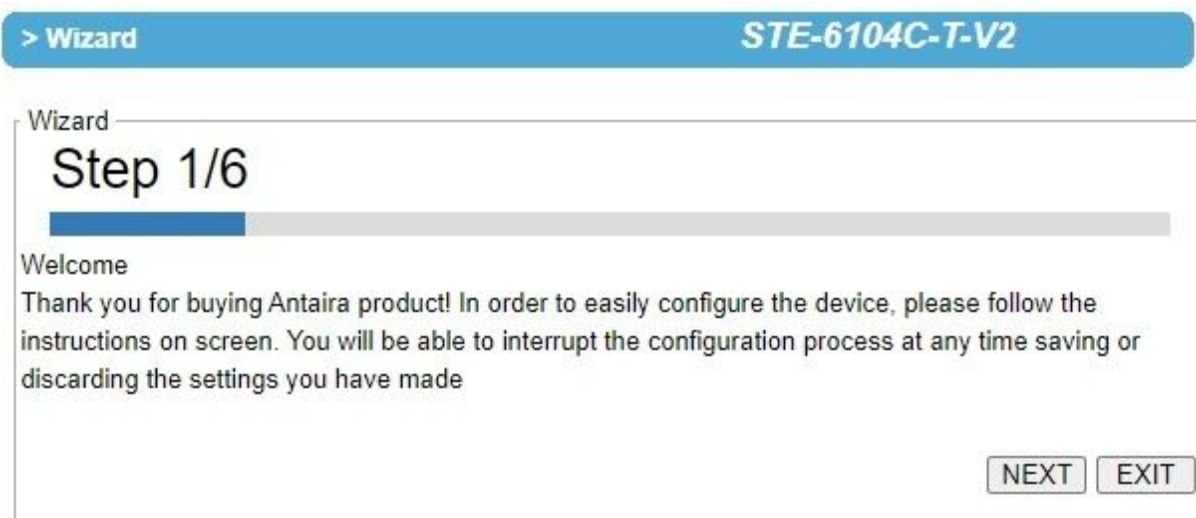
Network Information shows information about the wired network interface on the device.

- **LAN:** This will display the current **MAC Address**, and **IP Address** of the Ethernet interface.

## 3.5 Wizard

In this section, we describe how users can easily configure the device for the first-time using Wizard. The wizard will allow the user to simply set up a password, Date/Time, LAN, and COM port. However, if the user wants to set something more advanced, the user can manually put in setting values in other menus. Or if the user wants to monitor the activities or status of Virtual COM port, the user can instead use the "Serial/IP Port monitor software program".

There are a total of six steps/windows in the wizard which include: **Welcome, Administration, DATE/Time, Network, COM**, and **Final**. In Step 1/6, the **Welcome** window as shown in *Figure 3.14* will introduce the user how to use the wizard. Click the "Next" button to forward to Step 2/6, or "EXIT" to see



other menus.

*Figure 3.14 - Step 1/6 - A Welcome Web Page to the Configuration Wizard*

In Step 2/6, the **Administration** window as shown in *Figure 3.15* will let the user set a new password of the login device to increase security. The user has to re-input the password in "Repeat New Password" to set the new password. We recommend you to use a mix of upper- and lower-case letters, as well as, numbers

and symbols to make it more secure. If you want to go back to Step 1/6, click the “Prev” button. Click the “Next” button to move on to the Date/Time window in Step 3/6. Otherwise, if you want to leave the wizard anytime, click the “EXIT” button. If the “EXIT” button is clicked, a pop-up window will be generated. The

The screenshot shows a web-based wizard interface for the STE-6104C-T-V2 device. The top header bar is blue with a white arrow pointing right, the word "Wizard", and the device model "STE-6104C-T-V2". Below the header, the main content area has a title "Wizard" and "Step 2/6". A progress bar shows the current step is highlighted in blue. The section is titled "Administration" and contains a paragraph of instructions: "Antaira recommends you to change the device password for increased security. Please input the password in the 'new password' field below and repeat it in the 'Repeat new password' field. Use of upper and lower case letters, numbers and symbols is recommended." Below this text is a light blue box with the title "Administration" in italics. Inside this box are two input fields: "New Password" and "Repeat New Password". At the bottom right of the form are three buttons: "PREV", "NEXT", and "EXIT".

user will have a choice to either save or discard the settings which were made until that moment.

*Figure 3.15 - Step 2/6 - An Administration Web Page to Set Password*

In Step 3/6, the **Date/Time** window as shown in *Figure 3.16* will let the user set a Date/Time for the device. The user can select a proper Time Zone from the dropdown box. If the device is connected to the internet or to a local NTP server, the Date/time can be set automatically by selecting the option for “Synchronize the time automatically from an NTP server”. It is selected by default. If you do not want to automatically sync from the NTP server, you can manually set it. For more advanced options such as Daylight-Saving time, you can set it in the “Date/Time settings” page. If this option is chosen, the default value “time.nist.gov” should be shown in the NTP server field. If the STE-6104C device is connected to the Internet, it should connect to other servers over the Internet to get the NTP server, you will need to configure the DNS server in Step 4/6 in order to be able to resolve the host name of the NTP server. Click “PREV” to go back to Step 2/6 to re-enter the new password. Click “NEXT” to move on to the **Network** window, or “EXIT” to discard or save the settings until that moment.

> Wizard

STE-6104C-T-V2

Wizard

Step 3/6

Date/Time

This device, if connected to the internet or to a local NTP server can set its system time automatically. Otherwise, you can set the system time manually. You can configure more advanced options such as Daylight Saving time in the 'Date/Time settings' page. Note: if you're using an internet address, please make sure that 'default gateway' and DNS server fields are filled in in the next page of this wizard.

Date/Time

Time Zone

(GMT-12:00) Eniwetok, Kwajalein

NTP

☒ Synchronize the time automatically from an NTP server

☐ Set up the time manually

NTP Server

time.nist.gov

PREV

NEXT

EXIT

Figure 3.16 - Step 3/6 - A Date/Time Web Page of the Configuration Wizard

In Step 4/6, the **Network** window as shown in Figure 3.17 will let users set the network on more than one port. In the Network window, it will display "This device has x Ethernet ports". You are now setting up LAN1. The user has a choice to either set it manually or obtain it automatically from a DHCP server. If you selected "Obtain IP address automatically from a DHCP server", the rest of the options for LAN1 settings will be greyed out or disabled. If the option "Set up the network settings manually" is selected, the user can input an IP address with a subnet mask and gateway, and the DNS of the device. The user can select Default Internet Gateway to your serial device server. DNS (Domain Name Server) is where you can specify the IP Address of your preferred DNS and alternate DNS, which is why there are two DNS IPs to input here. Please consult your network administrator or internet service provider (ISP) to obtain local DNS's IP addresses. If the user has only one LAN connected, you have an option to move to Step 4/6 by selecting option "I'm done with LAN port configuration". Otherwise, you can select the option "I need to configure LANx". A new window with LANx settings will be shown and the user can continue with its setting, the same way you input in LANx Settings.



> Wizard
STE-6104C-T-V2

Wizard

## Step 4/6

**Network**

This device has 2 Ethernet ports, You are now setting up LAN1. The network settings can be obtained automatically from a DHCP server or set up manually. The changes will become effective upon completion of the Configuration Wizard

Lan 1	
Manual/DHCP	<input checked="" type="radio"/> Set up the network settings manually <input type="radio"/> Obtain IP address automatically from a DHCP server
IP	<input type="text" value="10.0.50.100"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Gateway	<input type="text" value="10.0.0.254"/>
Default Internet Gateway	<input checked="" type="radio"/>
DNS 1	<input type="text" value="0.0.0.0"/>
DNS 2	<input type="text" value="0.0.0.0"/>
Action	<input checked="" type="radio"/> I need to configure LAN2 <input type="radio"/> I'm done with LAN port configuration

Figure 3.17 - Step 4/6 - Network Web Page to Set LAN's IP Address

In Step 5/6, the **COM** window as shown in Figure 3.18 will let the user set the COM port of the device. If the device has more than one port (network or COM), there will be one page for each COM within Step 5/6. The STE-6104C series supports three different **Link Modes** which are **TCP Server**, **TCP Client**, and **UDP**. The **Link Mode** describes the role of the STE-6104C and the connection between the STE-6104C device and other remote devices in the network which would like to communicate with serial devices on the STE-6104C's COM port(s). Please select the one suitable to your end-application. There is no radio checked for the default. If the user wants to set-up more advanced settings, you can click on the COMx link on the left-hand side menu to configure.



In this Wizard, **TCP Server** and **TCP Client** mode can support **RAW** and **Virtual COM**, while **UDP** mode does not have the same supported applications as the previous two TCP modes.

If the user selects **TCP Server**, the Serial Server application related to COMx will be waiting for one or more connections to be established on a specific port, and will transfer the data transparently to the end-application (in case that **RAW** radio button is chosen in application submenu) or the data is transferred to a virtualCOM driver installed on your Linux or Microsoft Windows-based computer (in case that **VirtualCOM** is selected in application submenu). In both cases, the default local port is set to 4660.

When the **VirtualCOM** in the application submenu is chosen, the serial device server will be seen as an extension of the COM peripherals on your computer. The user can click to download ANTAIRA Device management Utility and install Serial/IP utility from the provided link.

If a user selects the **TCP Client**, the Serial Server application which is related to COMx will connect to one or more server's IP addresses/ports. Once a connection is established, the data will be transferred to the server transparently (RAW radio button) or via VirtualCOM. In both cases, the destination IP is set to Server IP address by default, and the destination port is set to 518 by default.

If a user selects **UDP**, the Serial Server application related to COMx will transfer the data via UDP to the destination IP and port. Note here that the device can support up to 4 UDP destinations. There are various UDP fields in the "Serial Setting" 's drop-down menus: Mode, Baud rate, Data bit, Parity, and Stop bit. The user can select the value that is appropriate to an equipment connected to your device. The Serial Port settings will be effective upon completion of the Wizard.

The screenshot shows a web-based configuration wizard for the STE-6104C-T-V2 device. The title bar at the top indicates the device model and the current step is 'Step 5/6'. The main heading is 'COM', with a sub-heading 'COM 1'. The text explains that the device has 1 COM port and the user is setting up COM1. It lists three communication modes: TCP Server, TCP Client, and UDP. The 'Link Mode' section has three radio buttons: 'TCP Server' (selected), 'TCP Client', and 'UDP'. The 'Application' section has two radio buttons: 'RAW' (selected) and 'VirtualCOM'. The 'Local Port' is set to 4660. Below this is the 'Serial Settings' section with dropdown menus for Mode (RS232), Baud Rate (1200), Data Bit (5 bits), Parity (None), and Stop Bit (1 bit). At the bottom right are 'PREV', 'NEXT', and 'EXIT' buttons.

COM 1	
Link Mode	<input checked="" type="radio"/> TCP Server: The Serial Server application related to COMx will be waiting for one or more connections to be established on a specific port, and will transfer the data transparently or via VirtualCOM. <input type="radio"/> TCP Client: The Serial Server application related to COMx will connect to one or more servers destination IP addresses/ports. Once connection is established, will transfer the data to the server transparently or via VirtualCOM <input type="radio"/> UDP: The Serial Server application related to COMx will transfer the data via UDP to the destination IP and port. The device supports up to 4 UDP destinations.
Application	<input checked="" type="radio"/> RAW: the data is transferred transparently to the end-application <input type="radio"/> VirtualCOM: the data is transferred to a virtualCOM driver installed on your Linux or Microsoft Windows-based computer. The serial device server will be seen as an extension of the COM peripherals on your computer. Click <a href="#">here</a> to download Device management Utility and install Serial/IP utility
Local Port	4660

Serial Settings	
Mode	RS232 ▼
Baud Rate	1200 ▼
Data Bit	5 bits ▼
Parity	None ▼
Stop Bit	1 bits ▼

PREV NEXT EXIT

Figure 3.18 - Step 5/6 - COM Web Page to Set COM Port

In Step 6/6, the **Final** window as shown in Figure 3.19 will notify the user to download a link for the Device Management Utility and Serial/IP utility as well as necessary information for any user who uses VirtualCOM.

[CLICK HERE](#) to download Antaira Device management Utility via our website.



*Figure 3.19 - Step 6/6 - Final Web Page to Introduce Serial/IP Utility*

[CLICK HERE](#) to download Antaira Device management Utility via our website.

## 3.6 Network Settings

In this section, both network interfaces and related network settings of the STE-6104C 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 3.20. 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 the **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, the **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 STE-6104C 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

Network Settings

LAN1 Settings

DHCP	<input type="checkbox"/> Obtain an IP Address Automatically
IP Address	<input type="text" value="10.0.50.100"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Gateway	<input type="text" value="10.0.0.254"/>

LAN2 Settings

DHCP	<input type="checkbox"/> Obtain an IP Address Automatically
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.254"/>

Default Gateway

Default Gateway Select	<input checked="" type="radio"/> LAN1 <input type="radio"/> LAN2
------------------------	--

DNS Server

Preferred DNS	<input type="text" value="168.95.1.1"/>
Alternate DNS	<input type="text" value="8.8.8.8"/>

Figure 3.20 - Network Settings Web Page

## 3.7 Firewall Setting

Antaira's Industrial Device Server provides firewall features to improve security for your network. You can configure the firewall mechanisms under the Firewall Setting menu.

### - Firewall Setting

IP Filter

Figure 3.21 Firewall Setting Menu

### 3.7.1 IP Filter

One of the firewall features is to filter network traffic based on protocols, source addresses, and port numbers. Under the IP Filter web page shown in *Figure 3.21*, you can configure the filtering for different network services. The first part of the IP Filter page is the Default Policy and the second part is the Filter List. By default, the policy is set in Accept mode in which all services on the device are accepted by the firewall. To deny a number of service types through the firewall, you can enable the filtering by selecting the Drop policy. Next, you can configure each denied service in the Filter List. Note that up to 30 entries can be set in the Filter List.

Under the Filter List, there are seven columns which are Alias, Interface, Option, IP Addr/mask, Protocol, Port, and Rule. The first three entries on the list are provided as examples for Ping, http, and https services. To enable each entry, you can check the box in front of that entry. Then, you can enter the short name or Alias for each entry to provide hints on the service that you allow. This name usually is the protocol service at the application layer. Next, you can select the transport protocol from the drop-down list under the Interface column. The choices for the interface are All, LAN1, and LAN2. The selection items depend on supported LAN interfaces on your device. The Option drop-down field allows you to select the filtering rule is a normal or invert rule of IP Addr/mask. Next, you can enter the IP Addr/mask, Protocol and the Port number that will fit in the filtering rule. Then, you can determine the configured rule is Accept or Drop by the device from the Rule drop-down list. *Figure 3.22* summarizes the description of each field on the IP Filter web page.

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

Firewall Setting > IP Filter
STE-6104C-T-V2

**Filtering**

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

Default Policy

☒ Accept
 ☐ Drop

Filter List						
Alias	Interface	Option	IP Addr/mask	Protocol	Port	Rule
<input type="checkbox"/> allow-ping	ALL ▼	Normal ▼		ICMP ▼		ACCEPT ▼
<input type="checkbox"/> http	ALL ▼	Normal ▼		TCP ▼	80	ACCEPT ▼
<input type="checkbox"/> https	ALL ▼	Normal ▼		TCP ▼	443	ACCEPT ▼
<input type="checkbox"/>	ALL ▼	Normal ▼		TCP ▼		ACCEPT ▼
<input type="checkbox"/>	ALL ▼	Normal ▼		TCP ▼		ACCEPT ▼
<input type="checkbox"/>	ALL ▼	Normal ▼		TCP ▼		ACCEPT ▼
<input type="checkbox"/>	ALL ▼	Normal ▼		TCP ▼		ACCEPT ▼
<input type="checkbox"/>	ALL ▼	Normal ▼		TCP ▼		ACCEPT ▼
<input type="checkbox"/>	ALL ▼	Normal ▼		TCP ▼		ACCEPT ▼
<input type="checkbox"/>	ALL ▼	Normal ▼		TCP ▼		ACCEPT ▼
<input type="checkbox"/>	ALL ▼	Normal ▼		TCP ▼		ACCEPT ▼

◀ Previous   Next ▶
Page 1/3

Save & Apply
Cancel

Figure 3.22 - IP Filter Page under Firewall Setting Menu

Field Name	Description	Factory Default
<b>Default Policy</b>	<b>Accept</b> all services or <b>Deny</b> specified services for the STE-6104C.	Accept
<b>Alias</b>	Check the box in front of the entry and enter the alias name for the filtering rule.	Null
<b>Interface</b>	Select the interface that the filtering rule will activate on it. The interface depends on available network ports on your device.	
<b>Option</b>	Select the option to determine this is a <b>Normal</b> or <b>Invert</b> rule of following settings.	
<b>IP Addr/Mask</b>	Enter the IP address that will be accepted or denied by the STE-6104C service. Noted that you can enter one the followings: 1) IP address: only this unique IP address will match in the filtering rule.	

	2) IP with subnet mask: IP addresses within this subnet mask will match in the filtering rule.	
<b>Protocol</b>	Select the protocol used by the service from the list: TCP, UDP, TCP/UDP, or ICMP	TCP
<b>Port</b>	Port number of TCP/UDP protocol	Null
<b>Rule</b>	Select the rule to <b>Accept</b> or <b>Drop</b> to determine the filtering rule will be accepted or denied by the device.	

Table 3.1 - Descriptions of Parameters for Services under Firewall Setting

## 3.8 Serial

Since the STE-6104C is an Industrial Serial Device Server, it supports serial communication with COM port(s). Note that the STE-6104C series can have up to four COM ports: **COM1**, **COM2**, **COM3**, and **COM4**.

Figure 3.23 shows the **Serial** menu on the left frame of the web interface of the STE-6104C. The following subsections will describe how to configure these COM ports.



Figure 3.23 - Serial Menu



### 3.8.1 COM Port Overview

Since details on **Link Mode** connectivity protocols and its settings of the STE-6104C series are given in Chapter 4 Link Modes and Applications, this section will only focus on the **Serial Settings** only. Figure 3.24 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 for the web page is applicable for COM 2/COM 3/COM 4 Port Settings on the STE-6104C device.

Serial > COM1

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	<input type="checkbox"/> Enable
Source IP	0.0.0.0
Local Port	4660
Maximum Connection	1 ▼
Response Behavior	<input type="radio"/> Request & Response Mode <input checked="" type="radio"/> Reply to request only <input type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

To configure COM 1 port parameters.

**Serial Settings**

Serial Interface	<input type="radio"/> RS232 <input checked="" type="radio"/> RS422 <input type="radio"/> RS485 <input type="radio"/> RS485(4-Wire)
Baud Rate	19200 ▼ bps
Parity	<input checked="" type="radio"/> None <input type="radio"/> Odd <input type="radio"/> Even <input type="radio"/> Mark <input type="radio"/> Space
Data bits	<input type="radio"/> 5 bits <input type="radio"/> 6 bits <input type="radio"/> 7 bits <input checked="" type="radio"/> 8 bits
Stop bits	<input checked="" type="radio"/> 1 bits <input type="radio"/> 2 bits
Flow Control	<input checked="" type="radio"/> None <input type="radio"/> Xon/Xoff <input type="radio"/> RTS/CTS

Save & Apply Cancel Advanced Settings

Figure 3.24 - COM 1 Port Settings Web Page



### 3.8.2 COM Configuration

Figure 3.25 shows the **Serial Settings** of the **COM** port settings for the STE-6104C. These settings need to match the parameters on the serial port of the serial device. Each option is described below.

To configure COM 1 port parameters.

Serial Settings	
Serial Interface	<input type="radio"/> RS232 <input checked="" type="radio"/> RS422 <input type="radio"/> RS485 <input type="radio"/> RS485(4-Wire)
Baud Rate	19200 ▼ bps
Parity	<input checked="" type="radio"/> None <input type="radio"/> Odd <input type="radio"/> Even <input type="radio"/> Mark <input type="radio"/> Space
Data bits	<input type="radio"/> 5 bits <input type="radio"/> 6 bits <input type="radio"/> 7 bits <input checked="" type="radio"/> 8 bits
Stop bits	<input checked="" type="radio"/> 1 bits <input type="radio"/> 2 bits
Flow Control	<input checked="" type="radio"/> None <input type="radio"/> Xon/Xoff <input type="radio"/> RTS/CTS

Figure 3.25 - Serial Settings Part of COM 1 Port

- **Serial Interface:** This option allows the selection between **RS-232**, **RS-422**, **RS-485**, and **RS-485 (4-Wire)** standards.
  - **Note:**
    - 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 numbers of ASCII characters (i.e., 0x11 = '1' and 0x13 = '3').

After you finish configuring the COM Port **Serial Settings**, please click on the **Save & Apply** button to keep the changes that you have made. Note that after you click the **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.

Serial Settings	
Serial Interface	<input checked="" type="radio"/> RS232 <input type="radio"/> RS422 <input type="radio"/> RS485 <input type="radio"/> RS485(4-Wire)
Baud Rate	1200 <input type="button" value="v"/> bps
Parity	<input checked="" type="radio"/> None <input type="radio"/> Odd <input type="radio"/> Even <input type="radio"/> Mark <input type="radio"/> Space
Data bits	<input checked="" type="radio"/> 5 bits <input type="radio"/> 6 bits <input type="radio"/> 7 bits <input type="radio"/> 8 bits
Stop bits	<input checked="" type="radio"/> 1 bits <input type="radio"/> 2 bits
Flow Control	<input checked="" type="radio"/> None <input type="radio"/> Xon/Xoff <input type="radio"/> RTS/CTS
Sync DTR signal with TCP connection	<input type="radio"/> YES <input checked="" type="radio"/> NO
Sync RTS signal with TCP connection	<input type="radio"/> YES <input checked="" type="radio"/> NO

Figure 3.26 - Serial Settings for COM 1

### 3.8.3 COM Configuration: Advanced Settings

For advanced details of the COM port settings, you can click on the Advanced Settings button at the end of the Serial Settings page which will open another web browser window as shown in *Figure 3.27* below. A description of each option is explained as follows.

COM 1 Port Advance Settings

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

Figure 3.27 - COM 1 Advanced Settings Web Page

## TCP

- **TCP Timeout:** By clicking the **Enable** box of **TCP Timeout** and inputting a value in seconds between 0 and 60000, STE-6104C will check if there is any data from the serial port. If time expires, the STE-6104C will disconnect from its peer.
- **TCP Keep-alive:** By clicking the **Enable** box of **TCP Keep-alive** and inputting a value in seconds, the STE-6104C will check if its peer is still alive. Note that it will retry 3 times and timeout is 5 seconds in default mode.

## Delimiters

- **Serial to Network Packet Delimiter:** Packet delimiter is a way of packing data for serial communication. It is designed to keep packets intacting. The STE-6104C 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, the STE-6104C would transmit the serial data in its buffer over the network.

- **Interval Timeout:** The STE-6104C will transmit the serial data in its buffer when the specified time interval has been 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 Figure 3.27) 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 a 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  $(10 \text{ (bits)} / 1200 \text{ (bits/s)}) * 1000 \text{ (ms/s)} = 8.3 \text{ ms}$ . 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:** The STE-6104C will transmit the serial data in its buffer when the specified length in the unit of bytes has been 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 the STE-6104C to queue the data until it reaches a specific length. This option is disabled by default.
- **Character:** The STE-6104C 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 the character delimiter is set to 0x0d, the STE-6104C 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. The STE-6104C will store data from the network interface in its queue. Until one of the delimiter conditions described above is met then the STE-6104C 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), the STE-6104C 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 & Response Mode** versus **Transparent Mode** in Chapter 4, Section 4.1.1. When TCP data is received (a request from the network) and passed to the serial device side, the STE-6104C 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, the STE-6104C 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 seem necessary to disable the FIFO function to minimize the amount of data that is transmitted through the serial interface after a flow of events 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, the STE-6104C 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 finishing the configuration, the COM Port's **Advanced Settings**, please click on the **Save & Apply** button to keep the change that you have made. Then, the **Advanced Settings** browser window can be closed by clicking on the **Close** button and you will be returned to the **COM 1 Port Setting** page.

## 3.9 VPN

The STE-6104C 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 3.28* below.

- VPN
  - PPTP
  - PPTP Status
  - IPSec Settings
  - IPSec Status
  - OpenVPN Settings
  - OpenVPN Keys
  - OpenVPN Status

Figure 3.28 - VPN Menu Structure

## 3.10 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 3.29 shows the PPTP configuration page under PPTP web setting. Currently, the STE-6104C series only supports the PPTP client. After the settings are completed, click the **"Save"** to save the configuration.

VPN > PPTP STE-6104C-T-V2

PPTP Client Settings

**PPTP Client Settings**

Enable PPTP Client	<input type="checkbox"/>
Always On	<input type="checkbox"/>
PPP Authentication	Only PAP ▼
PPP Encryption	Disable ▼
Remote IP Address	0.0.0.0
User Name	
Password	

Save Cancel

Figure 3.29 - PPTP Configuration Page

- Enable PPTP Client: Check this to enable the PPTP client on the STE-6104C series.
- Always on: Check this to have the STE-6104C 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 3.30 below shows the PPTP Link status.



Figure 3.30 - PPTP Link Status

- Local Virtual IP Address: The virtual IP address assigned by the PPTP server.
- Remote Virtual IP Address: The virtual IP address of the 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 established.
- Connect: Click this button to connect to PPTP server.
- Disconnect: Click this button to disconnect PPTP tunnel.
- Refresh: Click this button to refresh the PPTP tunnel status.

## 3.11 OpenVPN Settings

OpenVPN is an application that implements VPN for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificates. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and certificate authority.

There are two OpenVPN connection scenarios. They are the TAP and TUN scenario. The product can create either a layer-3 based IP tunnel(TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, you have to specify which type of OpenVPN connection scenario is to be adopted. Currently, the STE-6104C series only supports the TUN mode.

### 3.11.1 OpenVPN Settings

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 3.31*.

The screenshot displays the 'OpenVPN Settings' window for the 'STE-6104C-T-V2' device. The window has a blue header bar with the text 'VPN > OpenVPN Settings' on the left and 'STE-6104C-T-V2' on the right. Below the header, the 'OpenVPN Settings' title is followed by a 'General Settings' section. This section contains a table of configuration options:

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

At the bottom of the settings table, there are two buttons: 'Save' and 'Cancel'.

Figure 3.31 - Open VPN Setting



The OpenVPN parameters are described as below:

- **OpenVPN:** Check this to enable the OpenVPN.
- **Mode:** Specifies the scenario of this device, server or client. When choosing server mode, the device will play as server role and will standby for client connection.
- **Protocol:** Select the 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, the STE-6104C series only supports TUN (Tunnel) mode.
- **Virtual IP** (only when “OpenVPN Server” mode is selected): Specifies the server’s virtual IP. Virtual IP will only be available when SSL/TLS is chosen as the Authentication Mode. The Server’s virtual IP address will be 10.8.0.1/24 and client virtual IP address will be 10.8.0.x/24.
- **Local/Remote endpoint IP** (only when “OpenVPN Client” mode is selected): Specifies the local and remote endpoint virtual IP address of this OpenVPN gateway. Local/Remote endpoint IP is only available when a static key is chosen in Authentication Mode.
- **Authentication Mode:** Specifies the authorization mode of 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 3.11.2* for mode details.
  - Static Key: OpenVPN will use static key authorization, and the static key will be used. See section 3.11.2 below for mode details.
- **Encryption Cipher:** Specify the Encryption cipher. There are 5 options available: Blowfish, AES 256, AES 192, AES 128 and Disable. When Disable is selected, no encryption will be used.
- **Hash Algorithm:** Specifies 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:** Specifies 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, the STE-6104C will push the LAN port subnet to the OpenVPN remote clients, so that the remote client will add a route to the STE-6104C local network.

### 3.11.2 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.

VPN > OpenVPN Keys

STE-6104C-T-V2

OpenVPN Keys

Current Key Information

Profile	1 ▾
Certificate Authority	<div>-----BEGIN CERTIFICATE----- MIIExzCCA6+gAwIBAgIJAlxVHh6qLBDwMA0GCSqGSI b3DQEBCwUAMIGdMQswCQYD VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcn5pY TENMAsgA1UEBxMEQnJlYTEQMA4G</div>
Server Certificate	<div>Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) Signature Algorithm: sha1WithRSAEncryption</div>
Server Key	<div>-----BEGIN PRIVATE KEY----- MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBAkwggSIAg EAAoIBAQCwSvBfudJHABE5 Hnx61t+ozxhhXiiNJT8jx+Bz1dsO4TedUT7cjRZihCymtLv Rlx+y622aImH+/8MI</div>
Diffie Hellman parameters	<div>-----BEGIN DH PARAMETERS----- MIIBCAKCAQEAiT/vfb6h2oBfV4DwXjLUNzkP0HWt1gD vgzzLuPSKUDgaGMPgbsxx QqGMcdMtXSwgEWpPNjFPTbMtnkcWuydq7rRWzmU/v BfaJiP3cD3Hg5N0buQtKTcL</div>

Keys Generate

Keys Upload

Export All Keys

Figure 3.32 - 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 the server certificate. You can check the information if you uploaded a server certificate file.

- **Server Key:** It shows the information of the server key. You can check the information if you uploaded a server key file.
- **Diffie Hellman Parameters:** It shows the information of Diffie Hellman parameters.

When the STE-6104C acts as an OpenVPN server, the user can define its 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 the “**Generation Keys & Apply**” button.

OpenVPN Keys Generation

Certificate Information	
Country Code	TW
State	Taiwan
City	Taipei
Organization	Antaira
Organizational Unit	Antaira
Email Address	sales@antaira.com
Common Name (Read Only)	AntairaSE
Expire time (Read Only)	10 (years)
Generation Keys & Apply	

Figure 3.33 - 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 3.34 will show up and will allow you to import the related server or client certificates.



The screenshot shows a web interface titled "OpenVPN Keys Upload". On the left is a sidebar with "SSL/TLS" selected. The main area has a purple header "Certificate Upload". Below it are four rows, each with a label, a text input field, a "Browse..." button, and an "Upload" button. The labels are "Root CA", "Server CA", "Server Key", and "Server DH". At the bottom center is a "Done" button.

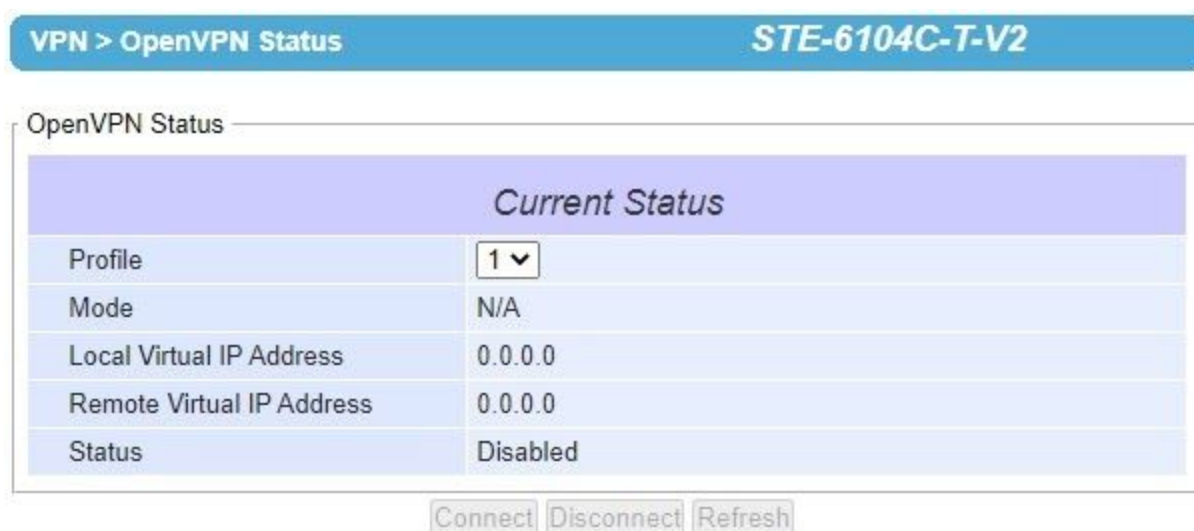
Certificate Upload	
Root CA	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Server CA	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Server Key	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Server DH	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
<input type="button" value="Done"/>	

Figure 3.34 - Certificate Upload

Click the **Browse** button to select your own server or client certificate and click on the **Upload** button. When the STE-6104C acts as an OpenVPN server, use the **Export All Keys** button to download all the necessary certificates including CA.crt, CA.key and the certificate and key for client side.

### 3.11.3 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 3.35* or *Figure 3.36* will show up depending whether the OpenVPN is set as a Client or Server.



The screenshot shows a web interface titled "VPN > OpenVPN Status" with "STE-6104C-T-V2" on the right. Below is a section titled "OpenVPN Status" containing a table with the heading "Current Status". The table has two columns: the first column lists status attributes, and the second column shows their values. At the bottom are three buttons: "Connect", "Disconnect", and "Refresh".

Current Status	
Profile	1 ▾
Mode	N/A
Local Virtual IP Address	0.0.0.0
Remote Virtual IP Address	0.0.0.0
Status	Disabled

Figure 3.35 - OpenVPN Client Status

- **Mode:** Displays the OpenVPN mode and that the STE-6104C 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 OpenVPN connection. It will include Disconnected, Connecting and Connected.

OpenVPN Status

Current Status			
Mode	Server		
Local Virtual IP Address	0.0.0.0		
Status	Deactivated		
Client List			
Common Name	Real Address	Virtual Address	Since

Activate

Deactivate

Refresh

Figure 3.36 - OpenVPN Server Status

- **Mode:** Displays the OpenVPN mode that the STE-6104C is currently running as.
- **Local Virtual IP Address:** Displays the Local virtual IP address.
- **Status:** Displays the current status of the OpenVPN connection. It will either be Deactivated, Activating, Disconnected, Connecting or Connected.

## 3.12 IPsec Settings

IPsec (or Internet Protocol Security) which is a network protocol suite that can establish secure and reliable communications for different application scenarios. IPsec enables data confidentiality, data integrity, data origin authentication, and anti-replay. 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 share a 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.

The STE-6104C 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 secure communication. There are two types of IPsec connection modes or types supported by STE-6104C 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
--------------------	--------------	--------------------	------------------------

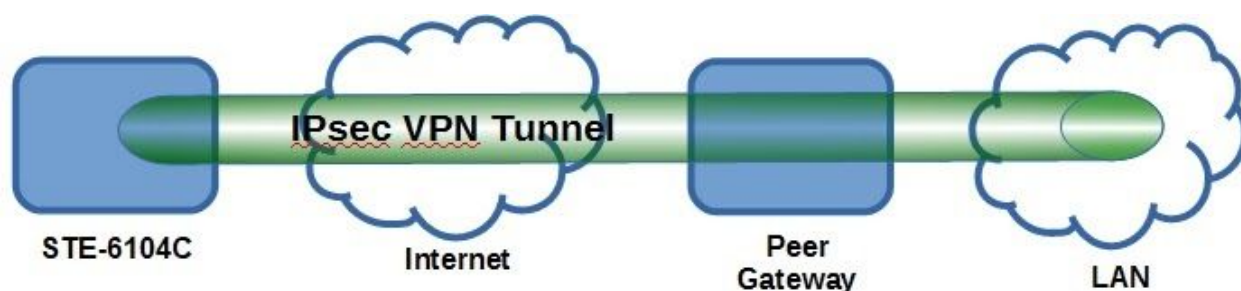
A **host-to-host** connection is typically used in a simple point-to-point communication. It is useful for direct communication with a server or between the device (STE-6104C) and a peer device (such as another STE-6104C). Note that this type of connection cannot be used for accessing entire sub-network resources. Figure 3.37 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode**.



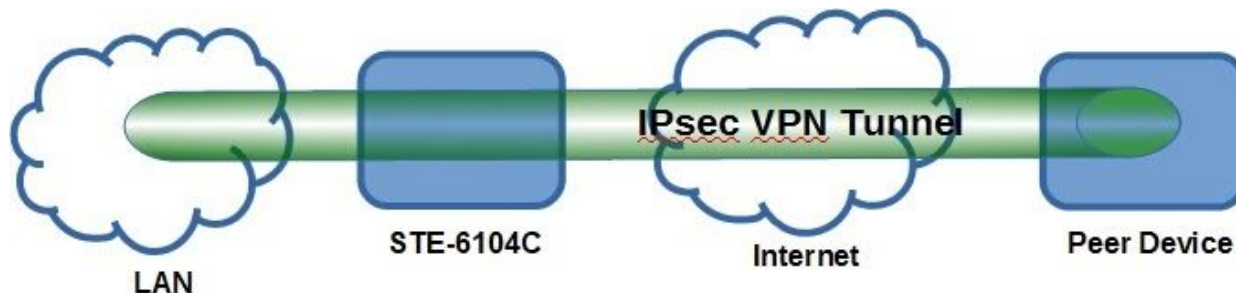
Figure 3.37 - An Example of a Host-to-Host Connection



A **host-to-subnet** (or host-to-network) connection is mainly applied when one endpoint needs to access the other side's sub-networks. A typical application is when employees are travelling on business and would like to connect back to their corporate headquarters via mobile devices. They can establish IPsec connections to access the internal corporate network resources. *Figure 3.38* illustrates a road-warrior application in which STE-6104C can access a remote sub-network resource via a peer gateway. *Figure 3.39* illustrates a gateway application in which the STE-6104C can passively accept connection requests from remote sides and provide access to the STE-6104C sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.



*Figure 3.38 - Roadwarrior Application Using a Host-to-Subnet Connection*

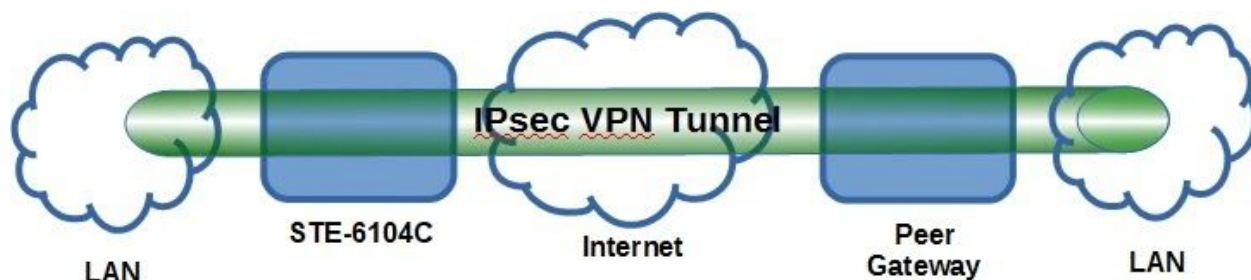


*Figure 3.39 - Gateway Application using Host-to-Subnet Connection*

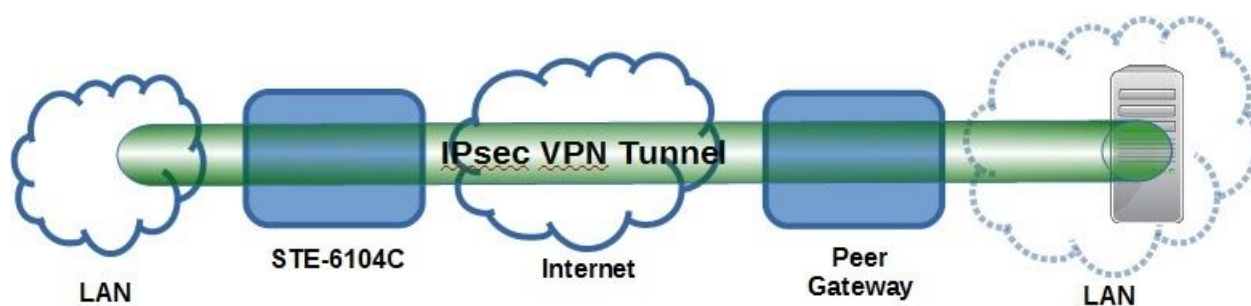
A **subnet-to-subnet** connection is mainly used to connect two subnets from different sides together. Typically, applications are corporate headquarters and branch offices that share internal network resources. A specific application can also be set up as one side's subnet to establish IPsec VPN tunnels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

*Figure 3.40* illustrates an example of the subnet-to-subnet connection with a network application. A host inside the remote subnet can also connect to a local subnet (host-network application) based on this subnet-to-subnet connection as shown in *Figure 3.41*. On the other hand, two different devices on two different subnets (host-host application) can be connected via a IPsec VPN tunnel based on this

subnet-to-subnet connection as shown in *Figure 3.42*. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.



*Figure 3.40 - An Example of a Network Application Using a Subnet-to-Subnet Connection via the STE-6104C and a Peer Device*



*Figure 3.41 - An example of host-network application via the subnet-to-subnet connection*



*Figure 3.42 - An Example of a Host-to-Host Application via the Subnet-to-Subnet Connection*

In some network configurations, there is an implementation of Network Address Translation (NAT) on its gateway/routers. NAT is typically used to allow private IP addresses on private networks behind gateways/routers with a single public IP address connecting to the public Internet. The internal network devices can communicate with hosts on the external network by changing the source address of outgoing requests to that of the NAT device (gateway/router) and relaying replies back to the originating device. IPsec 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.

The STE-6104C also has a feature called NAT traversal (NAT-T) that allows the IPsec tunnel to pass through the NAT in its network. Antaira's STE-6104C 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, the STE-6104C utilizes the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite. Note that IKE builds upon the Oakley protocol and ISAKMP (Internet Security Association and Key Management Protocol). IKE uses X.509 certificates for authentication either pre-shared or distributed using DNS (preferably with DNSSEC). IKE also uses a Diffie-Hellman key (DH) key exchange to set up a shared session secret from which cryptographic keys are derived. The IPsec Security Association (SA) is divided into two phases. In phase one, IKE creates an authenticated secure channel between the STE-6104C and its peer device, which is called the IKE Security Association. The Diffie-Hellman (DH) key agreement is always performed in this phase to create a shared secret key or DH key. In phase two, IKE negotiates the IPsec security associations and generates the required key material for IPsec. This IPsec key which is a symmetrical key will be used for bulk data transfer inside the IPsec tunnel. A new Diffie-Hellman agreement can be done in phase two, or the keys can be derived from the phase one shared secret.

### **3.12.1 IPsec Settings**

Figure 3.43 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	<input checked="" type="checkbox"/> Enable	
Peer Address	<input type="radio"/> Dynamic <input type="radio"/> Static: 10.0.50.100	
Remote Subnet	<input type="radio"/> None (Host Only) <input type="radio"/> Network: 192.168.1.0 / 24	
Local Subnet	<input type="radio"/> None (Host Only) <input type="radio"/> Network: 10.0.50.0 / 24	
Connection Type	Tunnel ▼	
Authentication Settings		
Method	<input type="radio"/> 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.		
Save Cancel		

Figure 3.43 - 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 the STE-6104C.

- **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 select **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 STE-6104C can accept remote connection requests or will be the responder.
  - **Static:** On the other hand, if you know the IP address of the remote device, you can choose the radio button for **Static** option and enter the IP address in the text box behind it. The STE-6104C 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 is already selected as the **Pre-Shared Key**. Then, you must enter in a secret key or a pass-phrase in the textbox behind it. Both ends of the VPN tunnel must use the same secret key or password. The pre-shared key can be 1 to 60 case-sensitive ASCII characters and special symbols.

The third part of **IPsec Settings** is the **IKE** (Internet Key Exchange) **Settings**. Internet Key Exchange (IKE) that the STE-6104C 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.

- The first option is the **Mode** of IKE session which defines how many steps or packets will be used or exchanged during the IKE SA negotiation. You can choose either **Main Mode** or **Aggressive Mode**. The **Main Mode** will send SA proposals, Diffie-Hellman public key, and ISAKMP session authentication in three exchange packets, while the **Aggressive Mode** will put all SA proposals, DH public key, and ISAKMP session authentication into one exchange packet. **Aggressive Mode** makes the IKE negotiation quicker than **Main Mode**. The difference between **Main Mode** and **Aggressive Mode** is that the "identity protection" is used in the **Main Mode**. The identity is transferred encrypted in the **Main Mode** but it is not encrypted in **Aggressive Mode**. Typically, the **Main Mode** is recommended.
- The 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. STE-6104C 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.
- The 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**.
- The fourth option is the selection of an **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**.
- The fifth option is the **SA Life Time** which must be set in units 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**, the STE-6104C 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, STE-6104C also supports two **DH groups** which are **DH Group 2** (1024-bit) and **DH Group 5** (1536-bit).

Then you can proceed to select the encryption and authentication algorithms. The third option is to select the **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 a 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 the STE-6104C uses to verify the existence of a remote Internet Key Exchange (IKE) gateway or the peer device of STE-6104C. To detect the peer device, the STE-6104C will be sent encrypted IKE Phase 1 notification payloads (or hello message) to its peer device and wait for DPD acknowledgement from the peer device. If the STE-6104C does not receive an acknowledge message during a specific time interval (**DPD timeout**), it will consider that the peer device is dead. Then, the STE-6104C 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 STE-6104C will perform if it finds 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 the STE-6104C will repeatedly check at the endpoint with the 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 STE-6104C 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 STE-6104C will take the PDP action. The **DPD Timeout** value ranges from 1 to 65535 seconds. The default value of **DPD Timeout** is 120 seconds. The description of each parameter in the IPsec Tunnels web page is summarized in *Table 3.1*.

Field Name		Description	Default Value
<b>General Settings</b>			
<b>IPsec</b>		Enable the IPsec Tunnel	Disable
<b>NAT Traversal</b>		Enable the NAT Traversal mechanism	Enable
<b>Peer Address</b>		IP address of the remote device which can be dynamic (any address) or static (fixed address)	Dynamic
<b>Remote Subnet</b>		Remote subnet can be either None (Host only) or Network (IP and Netmask)	None (Host Only)
<b>Local Subnet</b>		Local subnet can be either None (Host Only) or Network (IP and Netmask)	None (Host Only)
<b>Connection Type</b>		Tunnel mode or Transport mode	Tunnel
<b>Authentication Settings</b>			
<b>Method</b>		Pre-Shared Key	Secrets
<b>IKE Settings</b>			
<b>Phase 1 SA</b>	<b>Mode</b>	Choose how IKE negotiation is performed between Main Mode and Aggressive Mode	Main Mode
	<b>DH Group</b>	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)
	<b>Encryption Algorithm</b>	Encryption algorithm used in the key exchange process: Either 3DES or AES	AES128
	<b>Authentication Algorithm</b>	Hash algorithm used to authenticate packet data in the key exchange process of IKEv1 phase 1: Either MD5 or SHA1	SHA1
	<b>SA Life Time</b>	How long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry. The value can be from 300 to 86,400 seconds.	3600
<b>Phase 2 SA</b>	<b>Protocol</b>	Choose how the IP packet will be encrypted and verify: either Encapsulate Security Payload (ESP) or IP Authentication Header (AH)	ESP
	<b>Perfect Forward Secrecy</b>	Diffie-Hellman groups for Perfect Forward Secrecy of keys, determine the strength of the key used in the key exchange process: DH Group	Group 2 (1024-bit)

		2 (1024-bit) or DH Group 5 (1536-bit)	
	<b>Encryption Algorithm</b>	Select which key size and encryption algorithm will be used in IPsec tunnel: either 3DES or AES128	AES128
	<b>Authentication Algorithm</b>	Section of hash algorithm to be used to authenticate packet data in the IPsec tunnel: either MD5 or SHA1	SHA1
	<b>SA Life Time</b>	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 from 180 to 86,400 seconds.	28800
<b>Dead Peer Detection Settings</b>			
<b>DPD Action</b>	Select either Hold or Restart the tunnel's security association for the peer. Note that Hold is suitable for a statistically defined tunnel.		Hold
<b>DPD Interval</b>	Duration of time for sending a hello message to the peer device: value from 1 to 65535 seconds.		30 seconds
<b>DPD Timeout</b>	Duration of time to declare that the peer is dead: value from 1 to 65535 seconds.		120 seconds

*Table 3.1 - Description of Parameters in IPsec Tunnels Web Page*

### 3.12.2 IPsec Status

On this web page, you can check the status of your IPsec connection between the STE-6104C 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 the STE-6104C. 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 enables you to check the latest status of the connection.



Figure 3.44 - IPsec Status Web Page

### 3.12.3 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 the previous section on the details of **Authentication Settings**, **IKE Settings**, and **Dead Peer Detection Settings**. **\*Note** that the network-to-network (or subnet-to-subnet) connections are now supported in the new firmware of the STE-6104C.

#### 3.12.3.1 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 3.45*. Please follow the steps provided next for each scenario to set the **General Settings**.



Figure 3.45 - IPsec VPN Tunnel with Host-to-Host Topology

**Scenario: Host-to-host with static peer as shown in *Figure 3.46***

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



**\*Note:** When a peer address is entered as the static address, the STE-6104C acts as an **initiator** which takes the initiative and establishes a connection. The STE-6104C also acts as a **responder** and passively accepts the connection initiated by the remote gateway.

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

The screenshot shows the 'IPsec Settings' window with the 'General Settings' tab selected. The settings are as follows:

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

Figure 3.46 - General Settings for Host-to-Host with Static Peer

**Scenario: Host-to-host with dynamic peer as shown in Figure 3.47**

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.

**\*Note:** When the VPN connects to a peer with dynamic IP address, the STE-6104C 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	<input checked="" type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static: <input type="text"/>
Remote Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: <input type="text" value="192.168.1.0"/> / <input type="text" value="24"/>
Local Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: <input type="text" value="10.0.50.0"/> / <input type="text" value="24"/>
Connection Type	Tunnel ▼

Figure 3.47 - General Settings for Host-to-Host with Dynamic Peer

### 3.12.3.2 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 STE-6104C is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in *Figure 3.48*. Please follow the steps provided next for each scenario to set the **General Settings**.

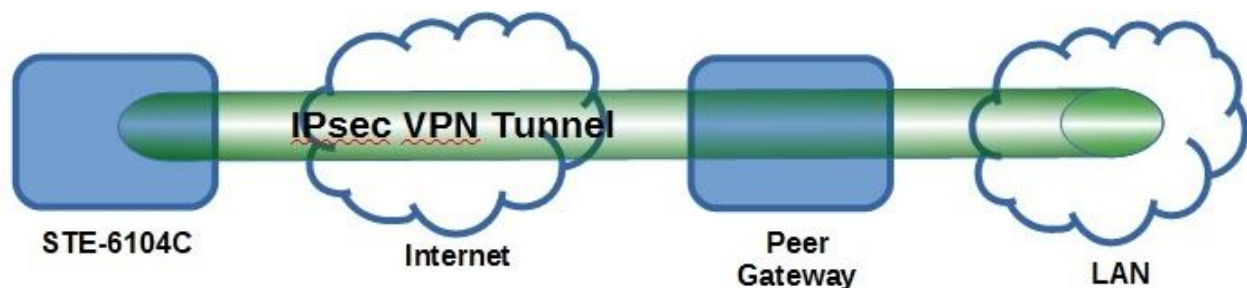


Figure 3.48 - IPsec VPN Tunnel with Host-to-Network Topology

**Scenario: Host-to-network with static peer as shown in *Figure 3.49***

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

**\*Note:** When a peer address is entered as a static address, the STE-6104C is an **initiator** which takes the initiative and establishes a connection, or can be a **responder** waiting for connection.

The STE-6104C 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 the subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.



General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static: 172.16.1.1
Remote Subnet	<input type="radio"/> None (Host Only) <input checked="" type="radio"/> Network: 192.168.1.0 / 24
Local Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 3.49 - General Settings for Host-to-Network with Static Peer

**Scenario: Host-to-network with dynamic peer as shown in Figure 3.50**

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.

**\*Note:** When the VPN connection is set to a peer with dynamic IP address, the STE-6104C 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 the subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.

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

Figure 3.50 - General Settings for Host-to-Network with Dynamic Peer

### 3.12.3.3 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 STE-6104C is the gateway to a local network in these scenarios. A network-to-network topology for both scenarios is illustrated in Figure 3.51. Please follow the steps provided next for each scenario to set the **General Settings**.



Figure 3.51 - IPsec VPN Tunnel with Network-to-Network Topology

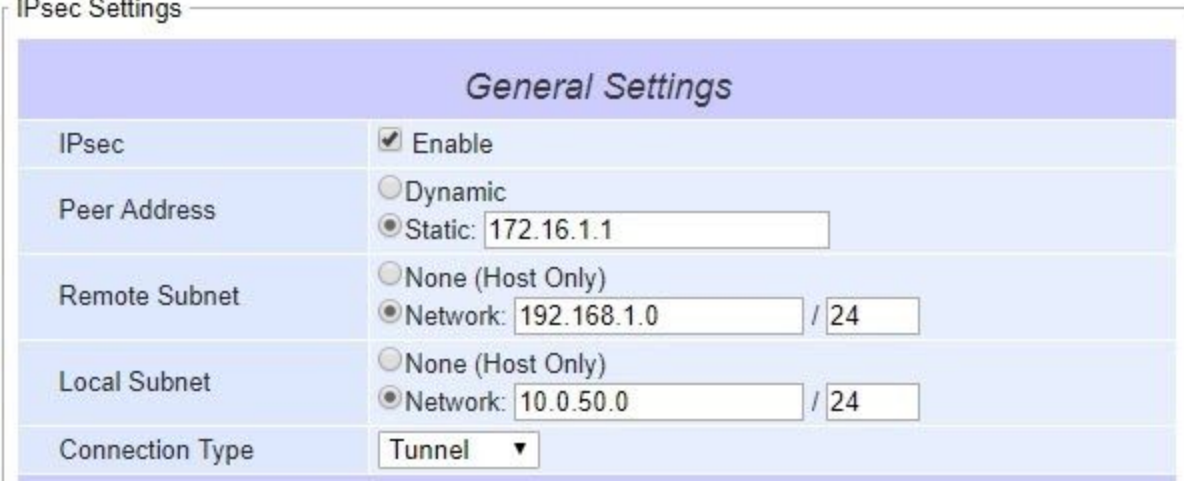
**Scenario: Network-to-network with static peer as shown in Figure 3.52**

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

**\*Note:** When a peer address is entered as a static address, the STE-6104C is an **initiator** which takes the initiative and establishes a connection, or can be a **responder** waiting for connection.

The STE-6104C 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 the 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 the subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.



General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static: 172.16.1.1
Remote Subnet	<input type="radio"/> None (Host Only) <input checked="" type="radio"/> Network: 192.168.1.0 / 24
Local Subnet	<input type="radio"/> None (Host Only) <input checked="" type="radio"/> Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 3.52 - General Settings for Network-to-Network with Static Peer

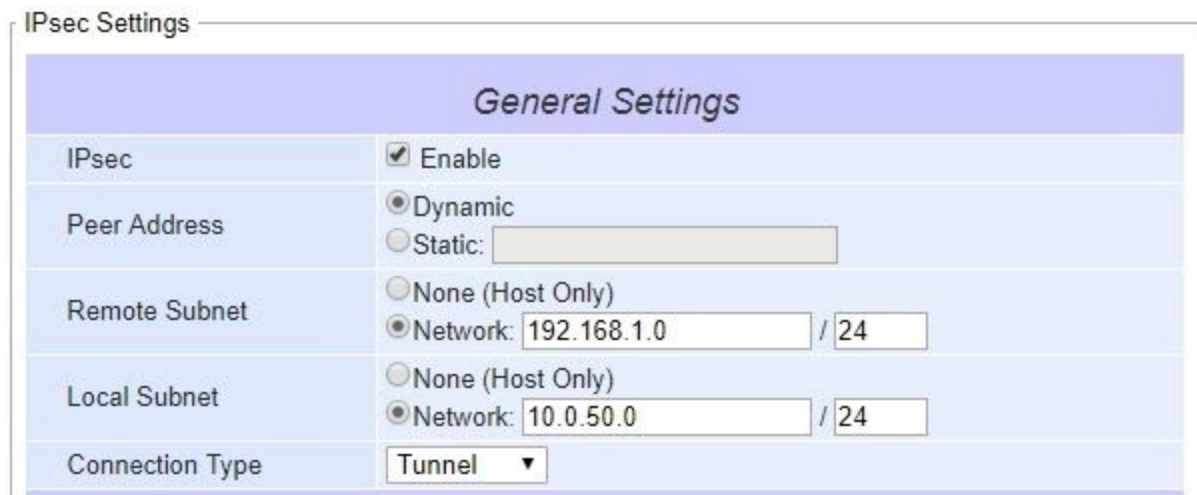
**Scenario: Network-to-network with dynamic peer as shown in Figure 3.53**

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.

**\*Note:** When a VPN connection is set to a peer with dynamic IP address, the STE-6104C 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 the 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 the subnet mask 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.



The screenshot shows the 'IPsec Settings' window with a 'General Settings' tab. The settings are as follows:

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

Figure 3.53 - General Settings for Network-to-Network with Dynamic Peer

## 3.13 Spanning Tree

Spanning tree functionality is supported by Antaira's STE-6104C Industrial Device Server series. However, the STE-6104C is only an end device in a network; therefore, it only has the receiving function of spanning tree. Generally, the **Spanning Tree Protocol (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, the STE-6104C deploys spanning tree as a tool when the users set up connection or port redundancy or fault-tolerance in their network.

**RSTP (Rapid Spanning Tree Protocol)**, IEEE 802.1W, is the only mode of spanning tree supported with the STE-6104C. 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 the left frame of the web interface of the STE-6104C. The list of **Spanning Tree** menu is shown in *Figure 3.54*. The sub-menus under the **Spanning Tree** are **Setting**, **Bridge Info**, and **Port Setting**. Each of this sub-menu will be described in the following subsections.



*Figure 3.54 - Spanning Tree Menu*

### 3.13.1 Spanning Tree's Setting

*Figure 3.55* shows an example of the **Setting** web page of the **Spanning Tree** menu. The **Spanning Tree Setting** page is divided into three parts which are **Mode Setting**, **Main Setting**, and **Port Setting**. For the STE-6104C, 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 the Enabled option is checked, the rest of the fields will become active. Then, the user can configure the **Priority**, **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 the **Update** button at the end of the page to allow the change to take effect. The description of each parameter is summarized below in *Table 3.2*.



- + System Status
- Wizard
- Network Settings
- + Firewall Setting
- + Serial
- SNMP/ALERT Settings
- E-mail Settings
- + VPN
- Spanning Tree
  - Setting
  - Bridge Info
  - Port Setting
- + Log Settings
- + System Setup
- Reboot

Spanning Tree > Setting
STE-6104C-T-V2

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 3.55 - Setting Web Page of Spanning Tree

Label	Description	Default Factory
<b>Mode</b>	Mode of Spanning Tree Protocol to be enabled on the STE-6104C	RSTP
<b>Enabled</b>	Check the box to enable spanning tree functionality.	Disable
<b>Priority</b>	Enter a number to set the device priority. The value is in between 0 and 61440. The lower number gives higher priority.	32768
<b>Maximum Age</b>	Maximum expected arrival time for a hello message. It should be longer than Hello Time.	20
<b>Hello Time</b>	Hello time interval is given in seconds. The value is in between 1 to 10.	2
<b>Forward Delay</b>	Specify the time spent in the listening and learning states in seconds. The value is in between 4 to 30.	15
<b>Primary Port</b>	Spanning tree's primary port	LAN1
<b>Secondary Port</b>	Spanning tree's secondary port	LAN2

Table 3.2 - Descriptions of Spanning Tree Parameters



**Note:** To disable the spanning tree function on the STE-6104C, the user can uncheck the **Enable** option and then click the **Update** button.

### 3.13.2 Spanning Tree's Bridge Info

**Bridge Info** (information) provides the current configured parameters of spanning tree protocol as shown in *Figure 3.56*. Note that this page will not display any data on any of the fields if the RSTP is not enabled on 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 3.3* and *Table 3.4* summarize the descriptions of each entry in the root information table and topology information table, respectively.

- + System Status
- Wizard
- Network Settings
- + Firewall Setting
- + Serial
- SNMP/ALERT Settings
- E-mail Settings
- + VPN
- Spanning Tree
  - Setting
  - Bridge Info
  - Port Setting
- + Log Settings
- + System Setup
  - Reboot

Spanning Tree > Bridge Info
STE-6104C-T-V2

Bridge Information

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

Root Information	
Root MAC Address	87:f0:96:7c:20:66
Root Priority	46842
Root Path Cost	3201131992
Root Maximum Age	139
Root Hello Time	139
Root Forward Delay	139

Topology Information	
Root Port	Port140
Num. of Topology Change	3201131992
Last TC time ago	3201131992

Figure 3.56 - Bridge Info Web Page of Spanning Tree

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

<b>Root Maximum Age</b>	Root's maximum age is the maximum amount of time that the device will maintain protocol information received on a link.	0
<b>Root Hello Time</b>	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
<b>Root Forward Delay</b>	Root's forward delay is the duration that the switch will be in learning and listening states before a link begins forwarding.	0

Table 3.3 - Bridge's Root Information

Label	Description	Factory Default
<b>Root Port</b>	A forwarding port is the best port from non-root bridge/switch (STE-6104C) to root bridge/switch. Note that for a root switch there is no root port.	-
<b>Num. of Topology Change</b>	The total number of spanning topologies change over time.	0
<b>Last TC time ago</b>	The duration of time since last spanning topology change.	-

Table 3.4 - Bridge's Topology Information

### 3.13.3 Spanning Tree's Port Settings

Spanning Tree's **Port Setting** shows the configured value of spanning tree protocol for each port, as shown in *Figure 3.57* and *Figure 3.58*. 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 3.5* summarizes the descriptions of the spanning three port settings. If **Spanning Tree** is enabled, the table of **Spanning Tree Port Setting** 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		Edge Cost
			Config	Actual		Config	P2P?	
Port1	Disc	Disabled	<input type="text" value="200000"/>	200000	128	<input type="text" value="P2P"/>	Yes	<input type="checkbox"/>
Port2	Fwd	Designated	<input type="text" value="200000"/>	200000	128	<input type="text" value="P2P"/>	Yes	<input checked="" type="checkbox"/>

Figure 3.57 - 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	<input type="checkbox"/>	No	0	0	1	0	00:00:00:00:00:00
P2P ▼	Yes	<input checked="" type="checkbox"/>	Yes	0	128	2	32768	7c:66:9d:1d:c5:ff

Update Refresh

Figure 3.58 - Spanning Tree Port Setting (Part 2)

Label		Description	Factory Default
<b>Port</b>		The name of the STE-6104C's port	-
<b>State</b>		State of the Port: <b>'Disc'</b> : Discarding - No user data is sent over the port. <b>'Lrn'</b> : Learning - The port is not forwarding frames yet, but it is populating its MAC Address Table. <b>'Fwd'</b> : Forwarding - The port is fully operational.	N/A
<b>Role</b>		Non-STP or STP RSTP bridge port roles: <b>'Root'</b> - A forwarding port that is the best port from non-root bridge to root bridge. <b>'Designated'</b> - A forwarding port for every LAN segment. <b>'Alternate'</b> - An alternate path to the root bridge. This path is different from using the root port. <b>'Backup'</b> - A backup/redundant path to a segment whose another bridge port already connects. <b>'Disabled'</b> - Note strictly part of STP, a network administrator can manually disable a port.	Non-STP
<b>Path Cost</b>		Setting the path cost for each switch port	
	<b>Config</b>	Setting path cost (default: 0, meaning that using the system default value (depending on link speed))	0
	<b>Actual</b>	The actual value path cost (For RSTP, please see Note 1 below and table.)	0
<b>Pri</b>		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
<b>Link Type</b>		The connection between two or more switches (for RSTP)	

	<b>Config</b>	Setting of the Link Type <b>P2P:</b> A port that operates in full-duplex mode is assumed to be point-to-point link. <b>Non-P2P:</b> A half-duplex port (through a hub) <b>Auto:</b> Detect link type automatically	Auto
	<b>P2P?</b>	<b>Yes:</b> This port is a Point-to-Point (P2P). <b>No:</b> This port is not Point-to-Point (Non-P2P).	No
<b>Edge</b>		Edge port is a port which no other STP/RSTP switch connects to (for RSTP). An edge port can be set to forwarding state directly.	
	<b>Config</b>	Edge functional is set: <b>Yes</b> or <b>No</b>	No
	<b>Edge?</b>	<b>Yes:</b> This port is an edge port. <b>No:</b> This port is not an edge port.	No
<b>Designated</b>		This shows some information of the best BPDU packet through this port.	
	<b>Cost</b>	Root path cost	0
	<b>P. Pri. (Port Priority)</b>	Port priority (high 4 bits of the Port ID), Value = 16 x N, (N: 0~15)	128
	<b>Port</b>	Interface number (lower 12 bits of the Port ID)	-
	<b>Bri. Pri. (Bridge Priority)</b>	Bridge priority, (value = 4096 x N), (N: 0~15)	32768
	<b>Bridge MAC</b>	The MAC address of the switch which sent this BPDU	-

Table 3.5 - Descriptions of Spanning Tree Port Setting

**Note:**

1. In general, the path cost is dependent on the link speed. Table 3.6 lists the default values of 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

Table 3.6 - Default Path Cost for RSTP

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 tiebreaker 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.

## 3.14 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 shown in *Figure 3.59* allows users to configure the STE-6104C device so that it can be viewed by third-party SNMP software, and allows the STE-6104C to send alert events to administrator and SNMP trap server.

> SNMP/ALERT Settings

STE-6104C-T-V2

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	<input type="text" value="contact"/>
System Name	<input type="text" value="System"/>
System Location	<input type="text" value="location"/>
SNMP	<input type="checkbox"/> Enable
SNMP Trap Server	
SNMP Trap Server	<input type="text" value="0.0.0.0"/>

Event alert settings

Alert Type	Email	SNMP Trap
Warm start	<input type="checkbox"/>	<input type="checkbox"/>
Authenticate failed	<input type="checkbox"/>	<input type="checkbox"/>
IP Address changed	<input type="checkbox"/>	
Password changed	<input type="checkbox"/>	

Save & Apply

Cancel

Figure 3.59 - SNMP/Alert Settings Web Page

The STE-6104C 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 filling 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 3.59*. By filling in the passphrase for the “**Read Community**”, the STE-6104C device allows other network management software to read its information. By filling in the passphrase for the “**Write Community**”, STE-6104C device allows other network management software to read/modify its information. The default STE-6104C’s SNMP Community Strings (or passphrases) for **Read Community** and **Write Community** as shown in *Figure 3.59* are “public” and “private”, respectively.

Additionally, you can set up a **SNMP Trap Server** in the network to receive and collect all alert messages from the STE-6104C. To configure the STE-6104C 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 3.59*. **Note** that any changes in these settings will take effect after the STE-6104C device is restarted.

Under the **SNMP Trap Server** part, there is a list of **Alert Type** under **Event alert settings** box in *Figure 3.59*. 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 the STE-6104C 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 the STE-6104C 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 the STE-6104C as listed in *Figure 3.59*. However, some events can only be reported by e-mail. These alerts are useful for security control or security monitoring of the STE-6104C 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 STE-6104C.
- **IP Address Changed:** This event occurs when the STE-6104C device's IP address is changed.
- **Password Changed:** This event occurs when the administrator password is changed.

After finishing the configuration for the **SNMP/Alert Settings**, please click on the **Save & Apply** button to keep the changes 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.

## 3.15 Email Settings

When the STE-6104C 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 STE-6104C to be able to send an e-mail. *Figure 3.60* 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 the 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, separate each e-mail address with a semicolon (;).

> E-mail Settings

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.

User name

Password

Save & Apply Cancel

Figure 3.60 - 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 a 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 set up a Default Gateway and DNS Servers in the Network Settings properly so that the STE-6104C can lookup domain names and route the e-mails to the proper default gateway. Please see the Default Gateway and DNS Server Settings in Section o .



After finishing the configuration of the **Email Settings**, please click on the **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 **Email Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button.

## 3.16 Log Settings

Under the **Log Settings** menu of the web interface of the STE-6104C series Industrial Serial Device Server, you can configure various data logging for the device. *Figure 3.61* lists the sub-menu under the **Log Settings**. It consists of **System Log Settings**, **System Log**, **COM Log Setting**, and **COM Log**. Each of these sub-menus will be described in the following subsections.



*Figure 3.61 - Log Settings Menu*

### 3.16.1 System Log Settings

The Syslog function is turned on by default and cannot be turned off for the STE-6104C. It is used to keep as a log for system events and report to an external Syslog server if necessary. *Figure 3.62* shows the **System Log Settings** page under the **Log Settings** menu. The description of each option is provided as follows.

System Log Settings	
Enable Log Event to Flash	<input type="checkbox"/>
Enable Syslog Server	<input type="checkbox"/>
IP Address	80.61.49.57
Syslog Server Service Port	11826 (1~65535, default=514)

Save & Apply Cancel

Figure 3.62 - Log Settings Web Page under Log Settings

- **Enable Log Event to Flash:** When the checkbox is enabled, the STE-6104C 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 checkbox is enabled, it will allow the STE-6104C to send Syslog events to the remote Syslog server with the specified IP address (next option). All the data sent/received from the 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 users to specify the remote Syslog Server Port number between 1 and 65535. Note that the default port number is 514.

After finishing the configuration of the **Log Settings**, please click on the **Save & Apply** button to keep the changes that you have made and to apply your settings. When the save and apply 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.

### 3.16.2 System Log

This page displays the current event log or system log stored in the STE-6104C device. *Figure 3.63* shows an example of a logged event. Each record of the **System Log** consists of **Time**, **Severity**, and **Message** description.

Log Settings > System Log STE-6104C-T-V2

System Log

System Log

Severity ALL ▾

Modules ☒ All

Refresh Export Log Clear Log

Show 10 ▾ entries Search:

#	Time	Sev.	Message
0	Jan 01, 1970 01:00:33	INFO	[Sys] System Start
1	Jan 01, 1970 01:01:03	INFO	[Sys] Relay open for power bad

Showing 1 to 2 of 2 entries Previous 1 Next

Figure 3.63 - 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 the “**Refresh**” button. When you click on the Export System Log button, a log file will be saved on to your PC. By clicking on the “**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.

### 3.16.3 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 3.64* shows the **COM Log Settings** page under the **Log Settings** menu. Description of each option is explained as follows.

Log Settings > COM Log Settings

COM Log Settings

☒ Log Data Contents    Types    ☐ HEX ☒ ASCII

COM Ports    ☒ COM1 ☒ COM2 ☒ COM3 ☐ COM4

Enable Syslog Server    ☒ Enable

IP Address    111.109.0.0

Syslog Server Service Port    0 (1~65535, default=514)

Save & Apply    Cancel

Figure 3.64 - COM Log Settings Web Page under 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:** The STE-6104C 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 the 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 users to send COM logs to a remote Syslog server.
- **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 users to specify the remote Syslog Server Port number between 1 and 65535. Note that the default port number is 514.

After finishing the configuration of the **COM Log Settings**, please click on the **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.

### 3.16.4 COM Log

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 3.65*, which allows it to display logs from different COM ports. An example of **COM 1 Log** is shown in *Figure 3.75*. Each record of the log consists of **Time**, **COM Index**, Direction (**T/R**) and **Data**.

Log Settings > COM Log STE-6104C-T-V2

COM Log

COM 1 Log

Refresh Export Log Clear Log

Show 10 entries Search:

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

Showing 0 to 0 of 0 entries Previous Next

*Figure 3.65 - 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.

## 3.17 System Setup

Under the **System Setup** menu of the web interface of the STE-6104C series Industrial Serial Device Server, you can perform a number of administration tasks for the device. *Figure 3.66* lists the sub-menu under the **System Setup**. It consists of **Date/Time Settings**, **Admin Settings**, **Firmware Upgrade**, **Backup/Restore Setting**, and **Ping**. Each sub-menu will be described in the following subsections.



*Figure 3.66 - System Setup Menu*

### 3.17.1 Date/Time Settings

Date and time can be set manually or using Network Time Protocol (NTP) to automatically synchronize the date and time of the STE-6104C with a Time Server. *Figure 3.67* shows the **Date/Time Settings** page. The first part of the page is the latest **Current Date/Time** which is in the format of **DD/Month/YYYY HH:MM:SS**. The second part of the page is the **Time Zone Settings**. You can select your local **Time Zone** from the drop-down list. The third part of the page is the **NTP Server Settings**. In this part, you can either enable the local NTP service inside the STE-6104C 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 3.67*.

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

End Date

Offset

Manual Time Settings

Date

Time

Save & Apply

Cancel

Figure 3.67 - Date/Time Settings Web Page under System Setup



**\*Attention:**

It is also important to set up the Default Gateway and DNS Servers in the Network Settings properly (See Section o), so the STE-6104C can lookup DNS names and point to the proper NTP server.

After finishing the configuration of the **Date/Time Settings**, please click on the **Save & Apply** button to keep the changes 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.

### 3.17.2 Admin Settings

The STE-6104C 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 3.68*. At the end of the **Admin Settings** web page, there is the **Web mode** part which allows 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	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS

Access control	
SSH	<input checked="" type="checkbox"/> Enable
Telnet	<input checked="" type="checkbox"/> Enable

Save & Apply Cancel

Figure 3.68 - Admin Settings Web Page under System Setup

After finishing the configuration of the **Admin Settings**, please click on the **Save & Apply** button to keep the changes 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 the STE-6104C as shown in *Figure 3.7*. You must re-enter



the username and the password to login to the STE-6104C. When the saving, applying, and re-authenticating 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.

### 3.17.3 Firmware Upgrade

Updated firmware for the STE-6104C is provided by Antaira from time-to-time (for more information please visit Antaira's website) 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 new firmware onto the STE-6104C, please download the latest firmware for your STE-6104C model from the download tab on the STE-6104C product page of Antaira's website. 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 the **"Browse..."** button as shown in *Figure 3.69* below to find and choose the new firmware file. Then, click the **"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 STE-6104C device will then proceed to restart itself. In some cases, you might require to re-configure your STE-6104C device. To restore your backup configuration from a file, please see the procedure in the next subsection.

The screenshot shows a web interface for the STE-6104C-T-V2 device. At the top, there is a blue header bar with the text "System Setup > Firmware Upgrade" on the left and "STE-6104C-T-V2" on the right. Below the header, the main content area is titled "Firmware Upgrade". It contains a paragraph of instructions: "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." Below this text, there is a light blue form area. It contains a checkbox labeled "Clear the flash after firmware upgrade" which is currently unchecked. Below the checkbox is a text input field labeled "Select new firmware" with a "Browse..." button to its right. At the bottom of the form area is an "Upload" button.

Figure 3.69 - 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 7 on Emergency System Recovery at the end of this manual.

### **3.17.4 Backup/Restore Settings**

Once all the configurations are set and the device is working properly, the user should back up the current configuration of the STE-6104C. 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 STE-6104C devices of similar settings by uploading these settings to all devices.

To back up configuration, click the **"Backup"** button under the **Backup Configuration** part as shown in *Figure 3.70*, and the backup file (ModelName-MACAddress.dat) will be automatically saved on your computer. It is important **NOT to manually modify the saved configuration file by any editor. Any modification to the file may corrupt the file and it may not be used for later restoration.** Please contact an Antaira authorized distributor for more information on this subject.

To restore the backup configuration, click the **"Browse"** button under the **Restore Configuration** part as shown in *Figure 3.70* to locate the backup configuration file on the user's computer. Then, click on the **"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 STE-6104C device to its factory default configuration, you can click on the **Restore** button under the **Restore Factory Default** section as shown in *Figure 3.70*.

**System Setup > Backup/Restore Settings**

**Backup & Restore Configuration**  
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.

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

Backup

**Restore Configuration**  
Browse a backup configuration file and click Upload button to restore the device's configuration.

Browse... Upload

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

Restore

Figure 3.70 - Backup/Restore Settings Web Page under System Setup

### 3.17.5 Ping

The Web UI of the STE-6104C has an interface option called **Ping** which is a network diagnostic utility for testing reachability. You can use the **Ping** function to determine whether the STE-6104C 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 3.71. This process usually takes around 20 seconds. Figure 3.71 represents a successful ping without packet loss from the STE-6104C to the address 10.0.50.101 and back, while Figure 3.72 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.

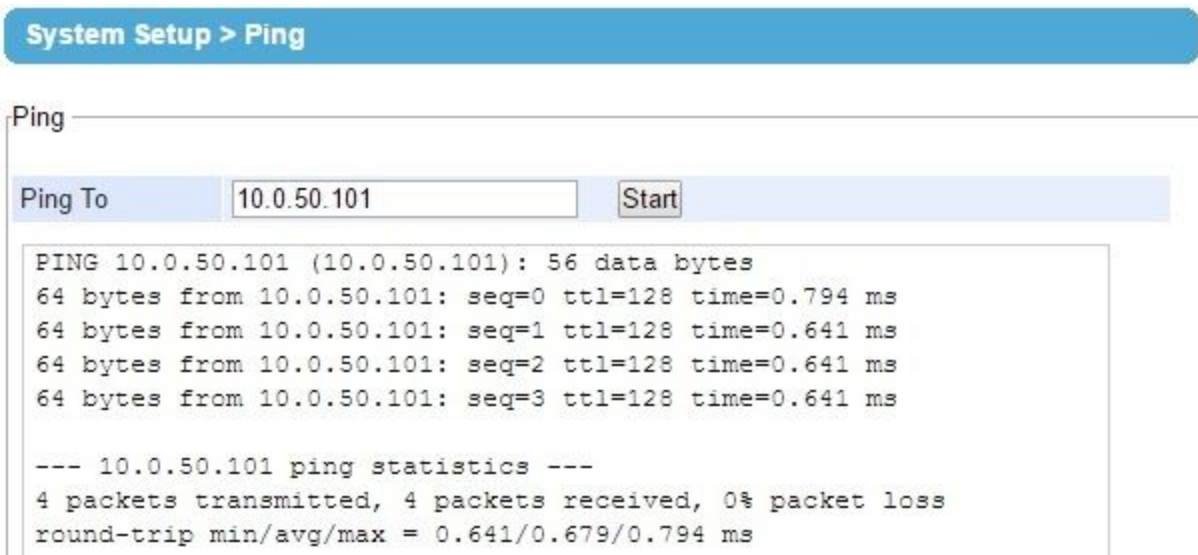


Figure 3.71 - Ping Web Page under System Setup

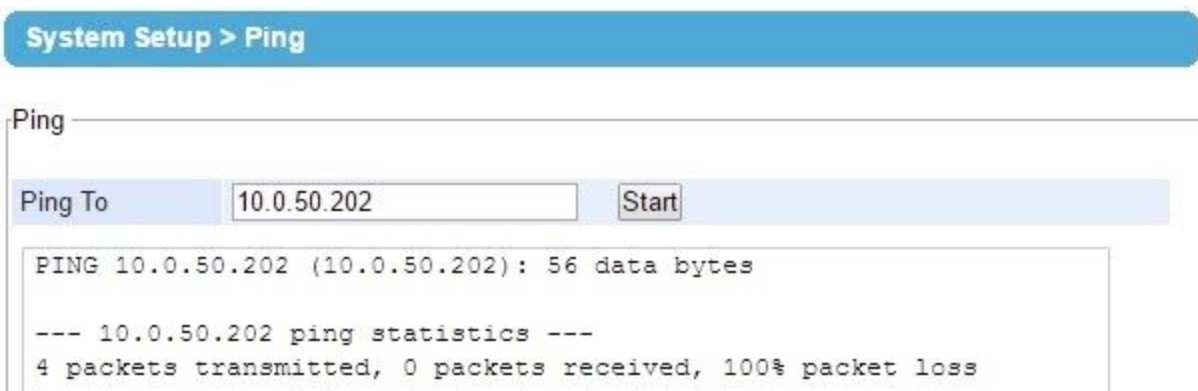


Figure 3.72 - Unreachable Ping Example

## 3.18 Reboot

To manually reboot the STE-6104C device, click on the “Reboot” button at the end of the Reboot page as shown in *Figure 3.73*. 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 STE-6104C again.



Figure 3.73 - Reboot Web Page

## 4 Link Modes and Applications

### 4.1 Link Mode Configuration

The STE-6104C series supports three different **Link Modes** which are **TCP Server**, **TCP Client**, and **UDP**. The **Link Mode** describes the role of the STE-6104C and the connection between the STE-6104C device and other remote devices in the network which would like to communicate with serial devices on the STE-6104C'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 the **UDP** mode does not have the same supported applications as the previous two TCP modes. Discussion on how to set up different Link Modes properly will be presented in the following sections. *Figure 4.1* shows the **Link Mode** options for **COM 1** port which can be found on the **COM1** page under the **Serial** menu of the Web UI (See details on Serial Settings in *Section 3.8*).



*Figure 4.1 - Link Mode Options for COM1 Port*

#### 4.1.1 Link Mode: Configure STE-6104C as a TCP Server

The STE-6104C 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 4.2* depicts an example of a PLC (serial) device which is connected to the STE-6104C 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 (STE-6104C) 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 STE-6104C device's default link mode.

## TCP Server Mode

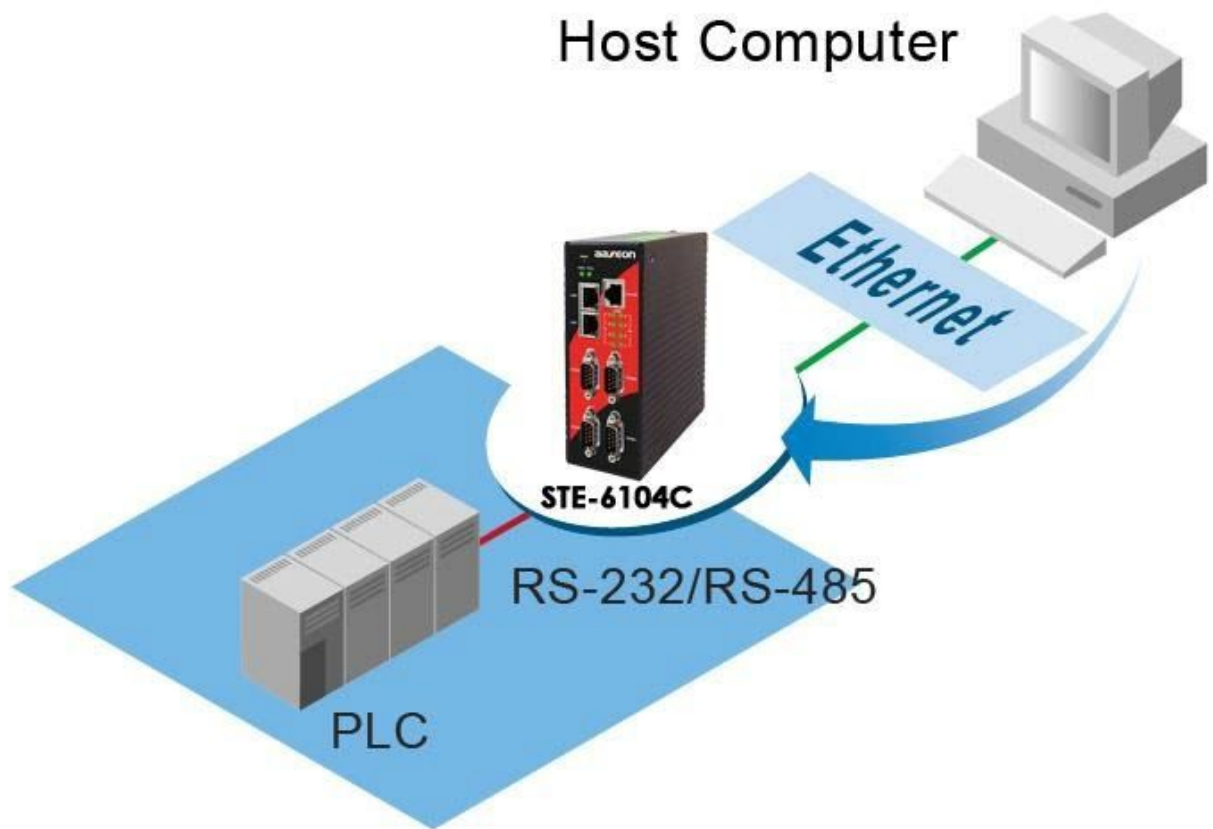


Figure 4.2 - STE-6104C is Set as a TCP Server Link Mode

The default Link Mode of the STE-6104C is the **TCP Server** mode. Figure 4.3 shows an example of the configuration settings for **TCP Server** Link Mode under the **COM 1** page. There are additional connection settings that can be configured as shown in Figure 4.3. By selecting the TCP Server Link Mode, a TCP client program on a remote host computer should be prepared to connect to the STE-6104C. Please follow the following steps to configure connection settings of the Link Mode for each COM port.

**LINK Mode**  
To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	RAW ▼
IP Filter	<input type="checkbox"/> Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1 ▼
Response Behavior	<input type="radio"/> Request & Response Mode <input type="radio"/> Reply to requester only <input type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

Figure 4.3 - 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 4.4. Note that if you would like to configure **COM 2** (or any other COM port), please follow the same procedures.



Serial > COM1

**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	<input type="checkbox"/> Enable
Source IP	0.0.0.0
Local Port	4660
Maximum Connection	1 ▼
Response Behavior	<input type="radio"/> Request & Response Mode <input checked="" type="radio"/> Reply to request only <input type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

To configure COM 1 port parameters.

Serial Settings

Serial Interface	<input type="radio"/> RS232 <input checked="" type="radio"/> RS422 <input type="radio"/> RS485 <input type="radio"/> RS485(4-Wire)
Baud Rate	19200 ▼ bps
Parity	<input checked="" type="radio"/> None <input type="radio"/> Odd <input type="radio"/> Even <input type="radio"/> Mark <input type="radio"/> Space
Data bits	<input type="radio"/> 5 bits <input type="radio"/> 6 bits <input type="radio"/> 7 bits <input checked="" type="radio"/> 8 bits
Stop bits	<input checked="" type="radio"/> 1 bits <input type="radio"/> 2 bits
Flow Control	<input checked="" type="radio"/> None <input type="radio"/> Xon/Xoff <input type="radio"/> RTS/CTS

Figure 4.4 - TCP Server Mode Settings under COM 1 Page

- Select the **TCP Server** radio button in the Link Mode options. Note that **TCP Server** is the default Link Mode for COM port of the STE-6104C.
- Under the **TCP Server** section, you will find the following options.
  - **Application:** There are 4 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 STE-6104C series will interact with those special commands (CR/LF commands) once the Reverse Telnet application is enabled.
- **Pair Connection Master:** This application is used when the user wants 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, the STE-6104C 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 STE-6104C). 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 STE-6104C) 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 numbers 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 the STE-6104C 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 the STE-6104C 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, a 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 the STE-6104C 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 3.8.2* and for **Advanced Settings** please go to *Section 3.8.3*.
- After finishing the configuration of the **Link Mode**, please scroll down to the bottom of the page and click on the "**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.

### 4.1.2 Link Mode: Configure STE-6104C as a TCP Client

The STE-6104C 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 4.5* depicts an example of two serial card readers connected to two different STE-6104C devices where both STE-6104C devices are on the same Ethernet network as the remote host computer. The arrow in *Figure 4.5* 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 STE-6104C) and a remote host computer in both directions. This also applies to Virtual COM applications running in the client mode.

## TCP Client Mode

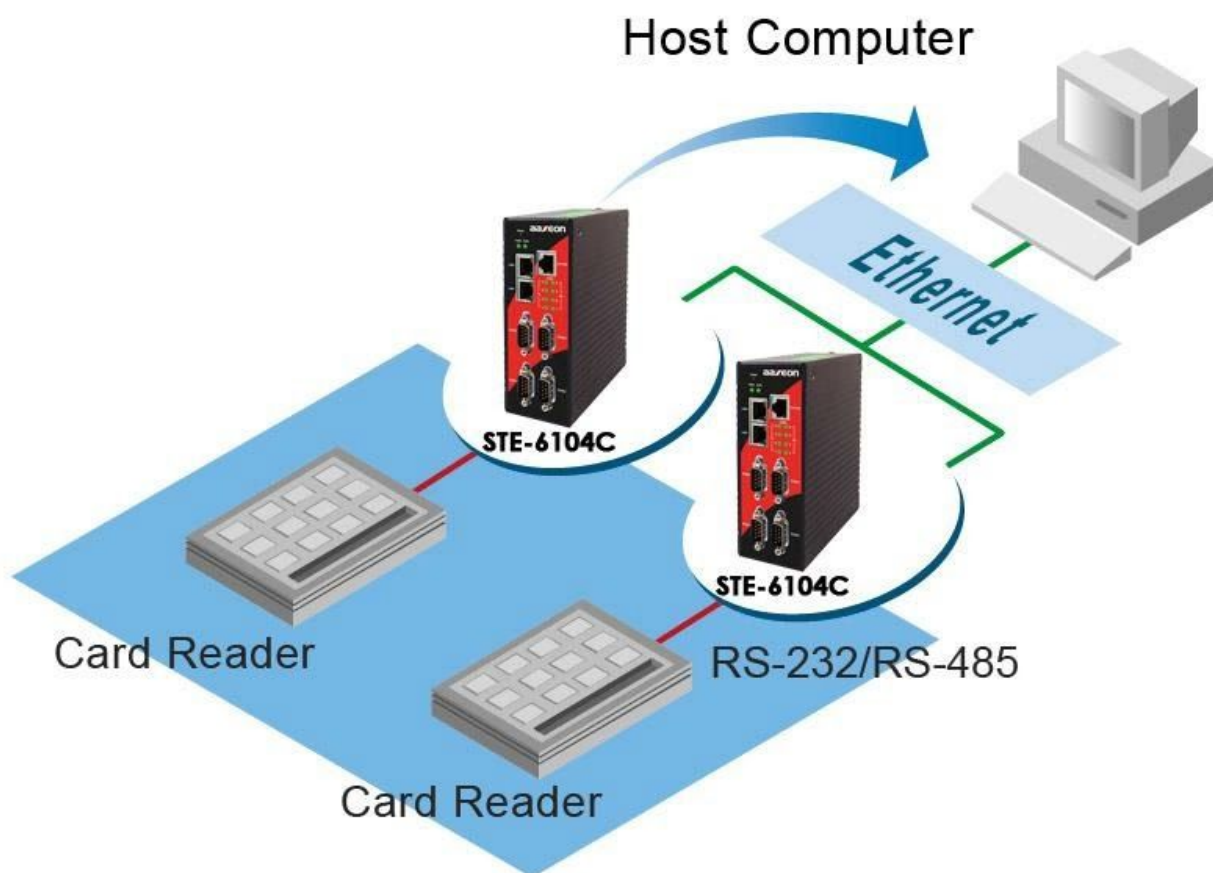


Figure 4.5 - Example of STE-6104C Configured as TCP Client Link Mode

Figure 4.6 shows an example of the 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 4.7. 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 the STE-6104C. Please follow the following steps to configure connection settings of the Link Mode for each COM port.

☐ TCP Server ☒ TCP Client ☐ UDP

TCP Client	
Application	RAW
Destination IP 1	10 . 0 . 50 . 1
Destination Port 1	4660
Destination 2	<input type="checkbox"/> Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	<input type="radio"/> Request & Response Mode <input type="radio"/> Reply to requester only <input checked="" type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

Figure 4.6 - 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 4.7. Note that if you would like to configure **COM 2** (or any other COM port), please follow the same procedures.

Serial > COM1

**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	10.0.50.200
Destination Port 1	518
Destination 2	<input checked="" type="checkbox"/> Enable
Destination IP 2	10.0.50.300
Destination Port 2	768
Response Behavior	<input type="radio"/> Request & Response Mode <input type="radio"/> Reply to request only <input type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

To configure COM 1 port parameters.

Serial Settings

Serial Interface	<input checked="" type="radio"/> RS232 <input type="radio"/> RS422 <input type="radio"/> RS485 <input type="radio"/> RS485(4-Wire)
Baud Rate	19200 ▼ bps
Parity	<input checked="" type="radio"/> None <input type="radio"/> Odd <input type="radio"/> Even <input type="radio"/> Mark <input type="radio"/> Space
Data bits	<input type="radio"/> 5 bits <input type="radio"/> 6 bits <input type="radio"/> 7 bits <input checked="" type="radio"/> 8 bits
Stop bits	<input checked="" type="radio"/> 1 bits <input type="radio"/> 2 bits
Flow Control	<input checked="" type="radio"/> None <input type="radio"/> Xon/Xoff <input type="radio"/> RTS/CTS

Figure 4.7 - Setting in TCP Client Link Mode

- Select the **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 4.1.1*.

- **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, the STE-6104C 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 a 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, the STE-6104C 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 a request from remote connected hosts. The description of each option is the same as described in the previous subsection (*Section 4.1.1 Link Mode: Configure as a TCP Server*).
- For other **Serial Settings** on the same configuration page, please go to *Section 3.8.2* and for **Advanced Settings** please go to *Section 3.8.3 COM Configuration: Advanced Settings*.

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

### 4.1.3 Link Mode: Configure STE-6104C 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. The STE-6104C also supports connectionless UDP protocol compared to the connection-oriented TCP protocol. The STE-6104C 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 the STE-6104C should listen to and specify the **Destination IPs** of the remote UDP nodes. *Figure 4.8* illustrates an example of UDP Link Mode in which a serial display device is connected on a serial bus and the STE-6104C. Two remote host computers, which are on the same Ethernet network as the STE-6104C, can both send UDP datagram or messages to the serial display device through the STE-6104C.



## UDP Mode

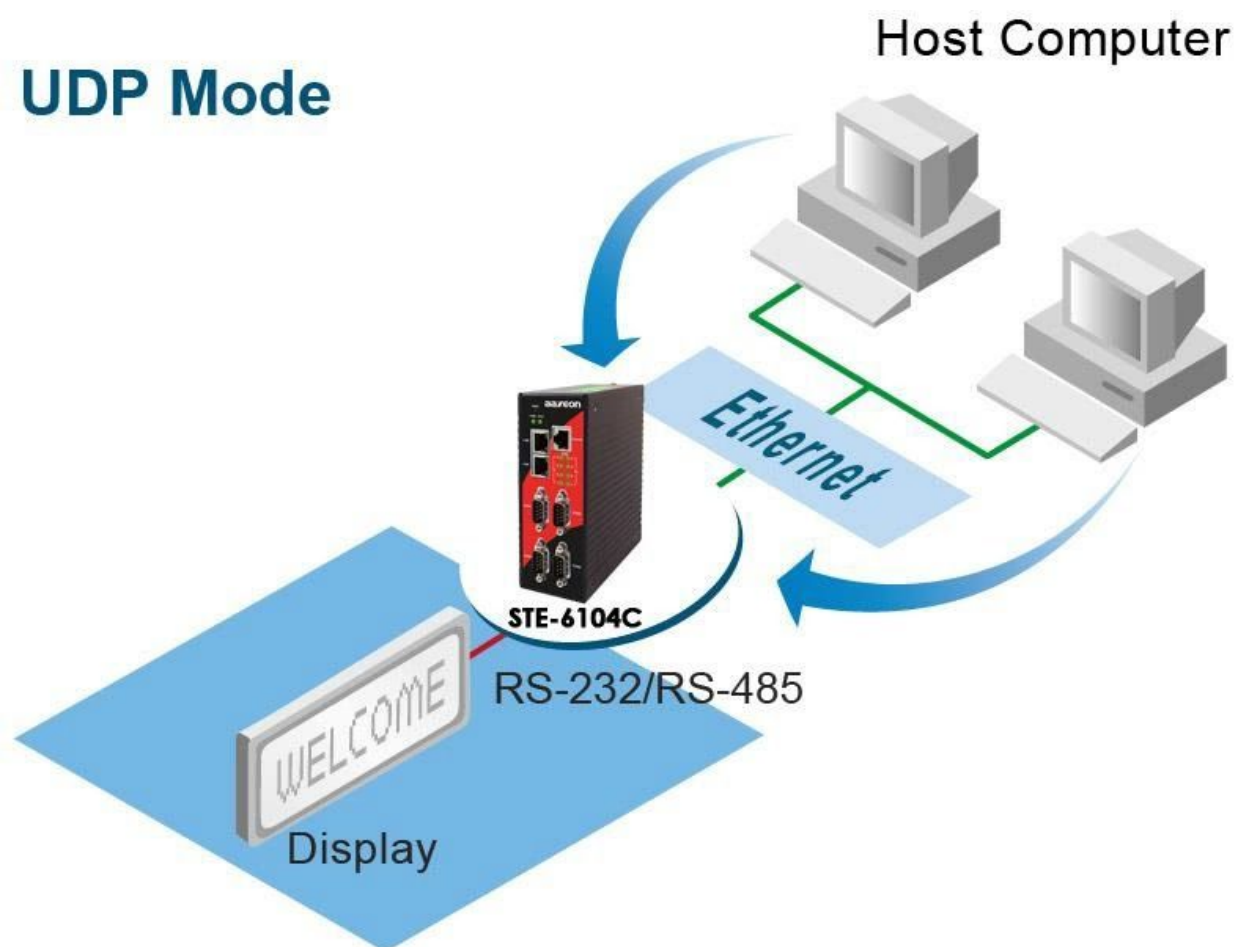


Figure 4.8 - Example of STE-6104C Configured in UDP Link Mode

Figure 4.9 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 4.10. Please be aware 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.

**LINK Mode**  
To choose specific working mode for COM 1 port.

☐ TCP Server ☐ TCP Client ☒ UDP

UDP					
Local Port: 4660					
<input checked="" type="checkbox"/> Destination IP Address 1	10	0	50	1 ~ 100	Port: 4660
<input type="checkbox"/> Destination IP Address 2	0	0	0	0 ~ 0	Port: 4660
<input type="checkbox"/> Destination IP Address 3	0	0	0	0 ~ 0	Port: 4660
<input type="checkbox"/> Destination IP Address 4	0	0	0	0 ~ 0	Port: 4660

Figure 4.9 - 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

**COM 1 Port Settings**

**Link Mode**  
 To choose specific working mode for COM 1 port.

☐ TCP Server
 ☐ TCP Client
 ☒ **UDP**

**UDP**

Local Port:

<input checked="" type="checkbox"/> Destination IP Address 0	10	0	50	101 ~ 102	Port: <input style="width: 50px;" type="text" value="511"/>
<input checked="" type="checkbox"/> Destination IP Address 1	10	0	100	100 ~ 150	Port: <input style="width: 50px;" type="text" value="252"/>
<input checked="" type="checkbox"/> Destination IP Address 2	10	0	201	200 ~ 250	Port: <input style="width: 50px;" type="text" value="65535"/>
<input checked="" type="checkbox"/> Destination IP Address 3	10	0	55	100 ~ 100	Port: <input style="width: 50px;" type="text" value="65535"/>

To configure COM 1 port parameters.

**Serial Settings**

Serial Interface	<input checked="" type="radio"/> RS232 <input type="radio"/> RS422 <input type="radio"/> RS485 <input type="radio"/> RS485(4-Wire)
Baud Rate	<input style="width: 50px;" type="text" value="19200"/> ▼ bps
Parity	<input checked="" type="radio"/> None <input type="radio"/> Odd <input type="radio"/> Even <input type="radio"/> Mark <input type="radio"/> Space
Data bits	<input type="radio"/> 5 bits <input type="radio"/> 6 bits <input type="radio"/> 7 bits <input checked="" type="radio"/> 8 bits
Stop bits	<input checked="" type="radio"/> 1 bits <input type="radio"/> 2 bits
Flow Control	<input checked="" type="radio"/> None <input type="radio"/> Xon/Xoff <input type="radio"/> RTS/CTS

Figure 4.10 - UDP Link Mode Setting under COM 1 Page

- Select the **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 the STE-6104C 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 from these options can specify the range of IP addresses and port numbers that will be communicating with the STE-6104C. 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 the STE-6104C can handle would highly depend on the traffic load. We have tested that the STE-6104C 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 3.8.2* and for Advanced Settings please go to *Section 3.8.3*.
- After finishing the configuration of the **Link Mode**, please scroll down to the bottom of the page and click on the "**Save & Apply**" button to save all the changes that you have made.

## 4.2 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.

### 4.2.1 TCP Server Application: Enable Virtual COM

The STE-6104C 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 the STE-6104C'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 4.11* shows the STE-6104C in the **TCP Server** mode with the **Virtual COM** application enabled. Please follow the following steps to enable the **Virtual COM** application in **TCP Server Link Mode**.

## LINK Mode

To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Virtual COM <span>▼</span>
IP Filter	<input type="checkbox"/> Enable
Source IP	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Local Port	<input type="text" value="4660"/>
Maximum Connection	<input type="text" value="1"/> <span>▼</span>
Response Behavior	<p><input type="radio"/> Request &amp; Response Mode</p> <p><input type="radio"/> Reply to requester only</p> <p><input checked="" type="radio"/> Reply to all</p> <p><input checked="" type="radio"/> Transparent Mode</p>

Figure 4.11 - Virtual COM Application in TCP Server Link Mode

- Follow steps in Section 4.1.1 to configure the STE-6104C in **TCP Server Link Mode** properly.
- Click on the drop-down list of the **Application** option under the **TCP Server** section and switch to **"Virtual COM"** to enable the Virtual COM application for the STE-6104C.
- Scroll down to the bottom of the page and click the **"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 5 for necessary instructions. Please remember the STE-6104C'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 Antaira Technologies.

### 4.2.2 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 the STE-6104C in TCP Server mode. Note that the RFC 2217 allows a remote client, which can be any network device, to initiate a Telnet session to an access server

(i.e. STE-6104C) to communicate with serial devices on the access server's COM port. To do so, please refer to *Section 4.2.1* (previous section) to enable the Virtual COM so that the STE-6104C 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.

### 4.2.3 TCP Client Application: Enable Virtual COM

It is also possible to run Virtual COM in TCP Client Link Mode. *Figure 4.12* shows a configuration of the Virtual COM application in TCP Client Link Mode. It is usually easier to use Virtual COM in the TCP Client Link Mode if the STE-6104C 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 below steps to enable the Virtual COM application in the 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	<input type="checkbox"/> Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	<input type="radio"/> Request & Response Mode <input type="radio"/> Reply to requester only <input checked="" type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

*Figure 4.12 - Virtual COM Application in TCP Client Link Mode*

- Follow the steps in *Section 4.1.2* to properly configure the STE-6104C in TCP Client Link Mode.
- Click on the drop-down list of the Application option under TCP Client section and switch to "Virtual COM" to enable the Virtual COM application for the STE-6104C.
- Scroll down to the bottom of the page and click the **"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 5 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.

#### **4.2.4 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 the STE-6104C in the TCP Client mode. Note that the RFC 2217 allows a client, which is the STE-6104C in this case, to initiate a Telnet session to a remote host computer to communicate with a serial device or serial (COM) program on the remote host computer. To do so, please refer to *Section 4.2.3* (previous section) to enable Virtual COM so that the STE-6104C 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.

#### **4.2.5 TCP Server Application: Configure STE-6104C as a Pair Connection Master**

A Pair Connection application is useful when pairing up two serial devices over Ethernet or when it is impossible to install Virtual COM in the serial devices. However, the pair connection application does require two STE-6104C devices to work as a pair. One would be the Pair Connection Master and the other would be the Pair Connection Slave. *Figure 4.13* shows a configuration of Pair Connection Master application in TCP Server Link Mode. Please follow the below steps to enable the Pair Connection application and set the STE-6104C as the 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	<input type="checkbox"/> Enable
Source IP	0.0.0.0
Local Port	4660
Maximum Connection	1 ▼
Response Behavior	<input type="radio"/> Request & Response Mode <input checked="" type="radio"/> Reply to request only <input type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

Figure 4.13 - Pair Connection Master Application in TCP Server Link Mode

- Follow steps in Section 4.1.1 to properly configure the STE-6104C in TCP Server Link Mode.
- Click on the drop-down list of the **Application** option under TCP Server section and switch to “**Pair Connection Master**” to enable the Pair Connection application for the STE-6104C.
- Scroll down to the bottom of the page and click the “**Save & Apply**” button to save the changes.
- Please remember Pair Connection Master’s IP address (i.e. STE-6104C’s IP address on your desired network interface (either Ethernet or Wi-Fi)) and Local Port number here in order to enter this information in another STE-6104C device with the Pair Connection Slave setting later.
- Proceed to the next section to configure a Pair Connection Slave to connect to this Master.

### 4.2.6 TCP Client Application: Configure STE-6104C as a Pair Connection Slave

A Pair Connection Slave application is configured for the STE-6104C under TCP Client Link Mode as shown in Figure 4.14. It is necessary to pair up with a Pair Connection Master as described in the previous section. Please set up a Pair Connection Master on another STE-6104C device first before proceeding. Please follow the below steps to enable the Pair Connection application and set this STE-6104C 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	<input checked="" type="checkbox"/> Enable
Destination IP 2	10.0.100.60
Destination Port 2	768
Response Behavior	<input type="radio"/> Request & Response Mode <input checked="" type="radio"/> Reply to request only <input type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

Figure 4.14 - Pair Connection Slave Application in TCP Client Link Mode

- Follow steps in Section 4.1.2 to properly configure the STE-6104C in TCP Client Link Mode.
- Click on the drop-down list of the **Application** option under TCP Client section and switch to “**Pair Connection Slave**” to enable Pair Connection application in the STE-6104C.
- Enter the **Destination IP** address and the **Destination Port** number (for Destination 1 and (optionally Destination 2) that match the settings of Pair Connection Master (another STE-6104C device)’s IP and port number that were setup previously.
- Scroll down to the bottom of the page and click the “**Save & Apply**” button to save the changes.

#### 4.2.7 TCP Server Application: Enable Reverse Telnet

The **Reverse Telnet** application is useful if a Telnet program is used to connect the STE-6104C and the serial interface of the STE-6104C 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. The STE-6104C will interact with those special commands (such as CR/LF commands) if **Reverse Telnet** is enabled. Figure 4.15 shows a configuration of **Reverse Telnet** application in the **TCP Server Link Mode**. Note that the **Reverse Telnet** application is only available when the STE-6104C is

configured as **TCP Server Link Mode**. Please follow the below steps to enable the **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 <span>▼</span>
IP Filter	<input type="checkbox"/> Enable
Source IP	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Local Port	<input type="text" value="4660"/>
Maximum Connection	<input type="text" value="1"/> <span>▼</span>
Response Behavior	<div><input type="radio"/> Request &amp; Response Mode <input type="radio"/> Reply to requester only <input checked="" type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode</div>

Figure 4.15 - Reverse Telnet Application in TCP Server Link Mode

- Follow steps in Section 4.1.1 to properly configure the STE-6104C in **TCP Server Link Mode**.
- Click on the drop-down list of the **Application** option under **TCP Server** section and switch to **"Reverse Telnet"** to enable the reverse telnet application in the STE-6104C.
- Scroll down to the bottom of the page and click the **"Save & Apply"** button to save the changes.

## 5 VCOM Installation & Troubleshooting

### 5.1 Enabling VCOM

The STE-6104C 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 the STE-6104C's COM ports. Please note that **Virtual COM Application** can only be enabled in **TCP Server Link Mode** as shown in *Figure 5.1* or **TCP Client Link Mode** as shown in *Figure 5.2*.

The screenshot shows the 'COM 1 Port Settings' window. Under the 'LINK Mode' section, 'TCP Server' is selected. Below this, a table lists various settings for the 'TCP Server' mode.

TCP Server	
Application	Virtual COM
IP Filter	<input type="checkbox"/> Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1
Response Behavior	<input type="radio"/> Request & Response Mode <input type="radio"/> Reply to requester only <input checked="" type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

Figure 5.1 - 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	<input type="checkbox"/> Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	<input type="radio"/> Request & Response Mode <input type="radio"/> Reply to requester only <input checked="" type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

Figure 5.2 - Enable a Virtual COM Application When Setting the Link Mode as the TCP Client

Virtual COM on host computers allow remote access of serial devices over TCP/IP networks through Serial/IP Virtual COM ports that work like local native COM ports. Figure 5.3 is an example of the Virtual COM application diagram. In the diagram, multiple serial servers (i.e. STE-6104C devices) in which each one connects to a serial device are connected over an Ethernet hub. The 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 the STE-6104C case, the TCP/IP network can be a wired network such as Ethernet.

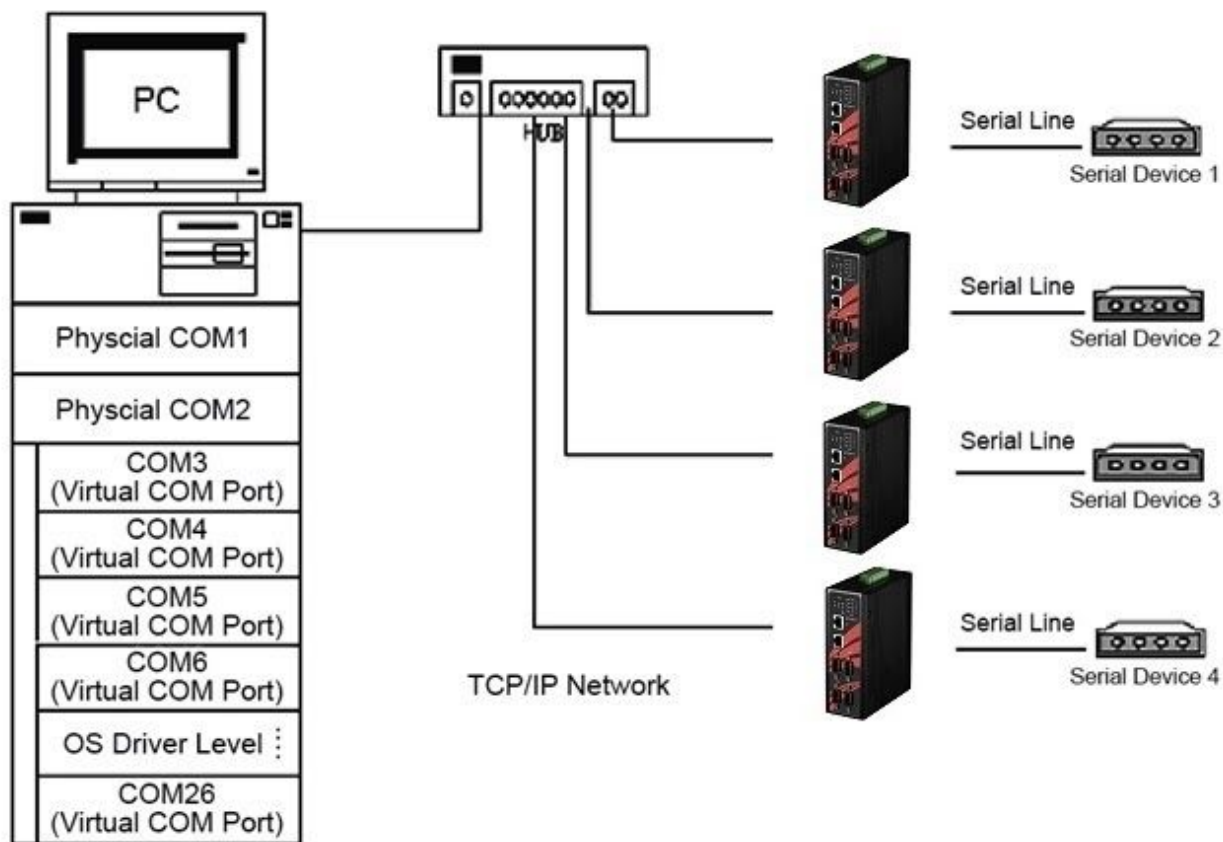


Figure 5.3 - An Example Diagram of Virtual COM Application over TCP/IP Network

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

### 5.1.1 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
- 
- The Linux operating system is also available, but first you might need to download a separate package called Virtual COM driver for Linux (TTYredirector) available for download on Antaira's website or in the product CD. The zipped package includes a binary file for installation and a manual for Linux systems.

### **5.1.2 Limitation**

The Virtual COM driver allows up to 256 Virtual COM ports in a single PC. Selection of COM port numbers 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.

### **5.1.3 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.

### **5.1.4 Uninstallation**

- From the 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.

## 5.2 Enable VCOM in Serial Device Servers and Select VCOM in Windows

This section will provide the steps to enable Virtual COM (VCOM) on the STE-6104C and a Windows based PC. Please follow the steps described here to configure your Virtual COM application.

### 5.2.1 Enable VCOM in Serial Device Servers

Enable **Virtual COM** in our serial device servers (i.e. STE-6104C) by logging into the Web UI. It is located under **COM 1** or other **COM** configuration under the **Serial** menu.

Figure 5.4 shows how to enable **Virtual COM** in **TCP Server Link Mode** in the STE-6104C. For more detail on the **Link Mode** configuration with **Virtual COM**, please refer to the previous chapter starting from Section 4.1.

**LINK Mode**  
To choose specific working mode for COM 2 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Virtual COM
IP Filter	<input type="checkbox"/> Enable
Source IP	0 . 0 . 0 . 0
Local Port	4660
Maximum Connection	1
Response Behavior	<input type="radio"/> Request & Response Mode <input type="radio"/> Reply to requester only <input checked="" type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

Figure 5.4 - Enable Virtual COM Application for COM 2 in TCP Server Link Mode

## 5.2.2 Running Serial/IP Software Utility in Windows

After installation of the Virtual COM driver on a Windows operating system as described in *Section 4.1.3*, you can open the **Serial/IP Control Panel** by following any one of the below 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 5.5, right click on the Serial/IP tray icon and click on Configure... menu to open the Serial/IP's Control Panel.



Figure 5.5 - 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 5.6*. 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 another 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 the COM ports in the text box below the list. After selecting the virtual COM ports, please click the OK button to proceed.



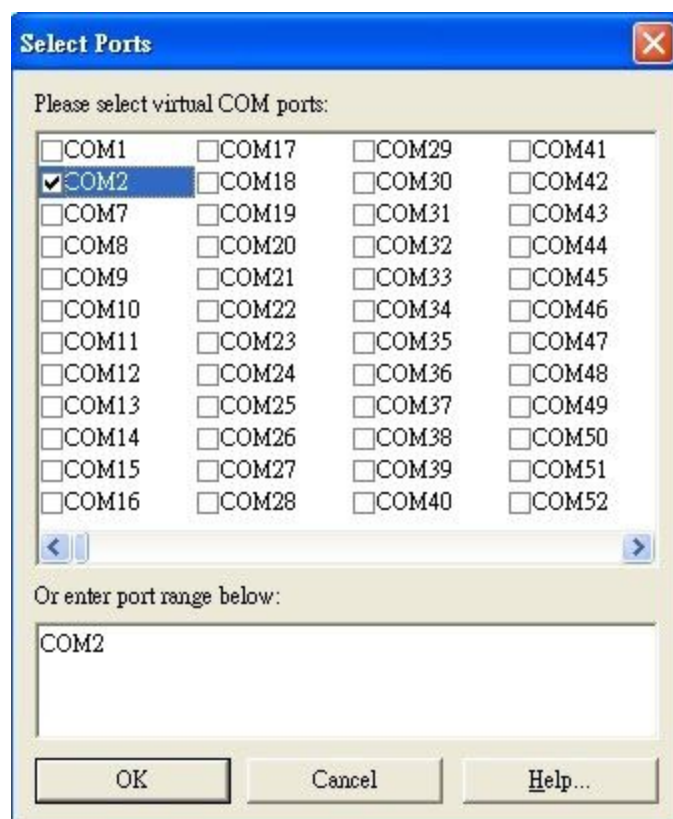


Figure 5.6 - A Pop-up Window for Selecting Virtual COM Ports

After at least one Virtual COM port is selected, the **Serial/IP Control Panel** window will show up as illustrated in Figure 5.7. The left side of the **Control Panel** window shows the list of selected Virtual COM ports. You can click on the **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.

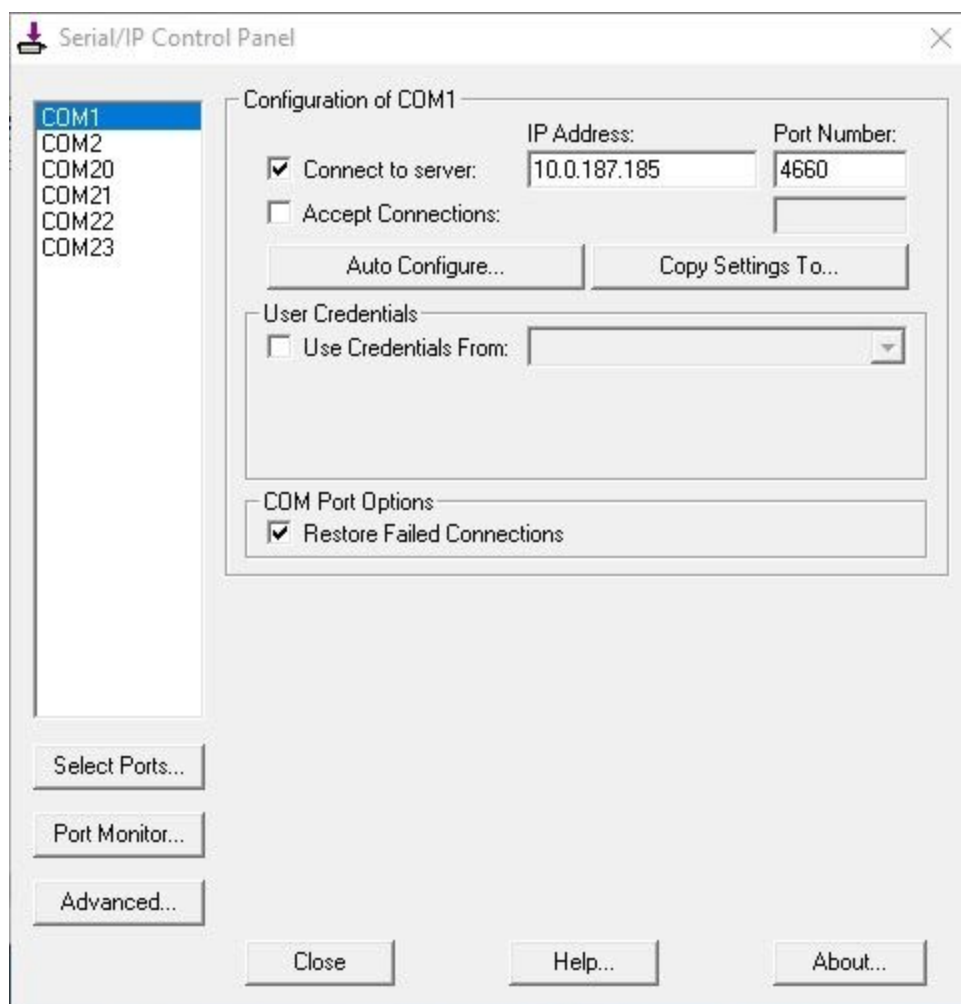


Figure 5.7 - Serial/IP Control Panel Window

### 5.2.3 Configuring VCOM Ports

For each VCOM port selected on the list off to 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. STE-6104C) 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 5.9) 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 4.11.

2. If the serial device server (i.e. STE-6104C) 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 the **Connect to Server** option and **Accept Connections** option simultaneously.
3. Under the **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 5.8. If you select **Use Credentials Below** option as shown in Figure 5.9, please specify the **Username** and the **Password** in their corresponding text boxes.

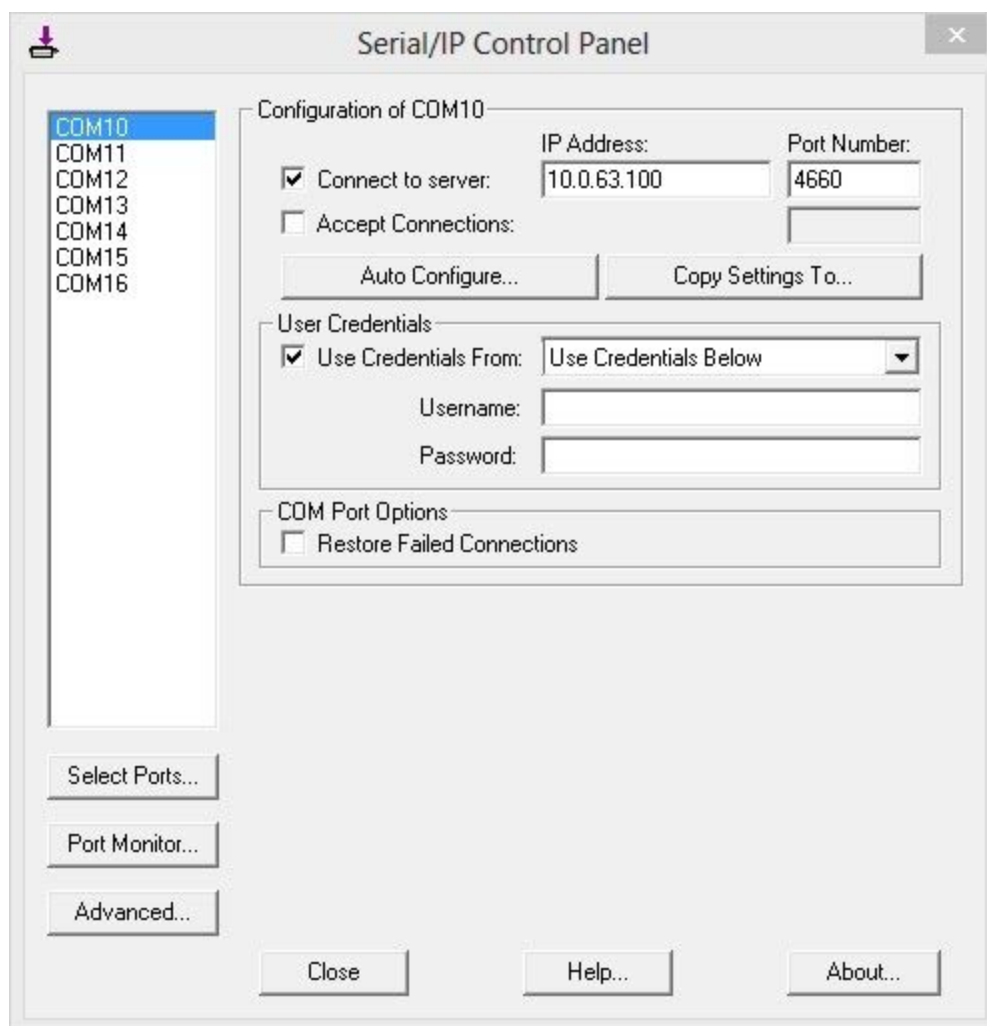


Figure 5.8 - Available Options for Use Credential Form in Serial/IP Control Panel Version 4.9.10

1. Under the **COM Port Options** box, you can enable the **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.
2. To test the Virtual COM connection, you can click the **Auto Configure...** button and then click the **Start** button in the pop up window as shown in *Figure 5.10*. 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 5.10*. You can also click on the **Copy** button to copy the results to the PC system clipboard.
3. To transfer the settings between Virtual COM ports, click on the **Copy Settings To** button as shown in *Figure 5.9*.

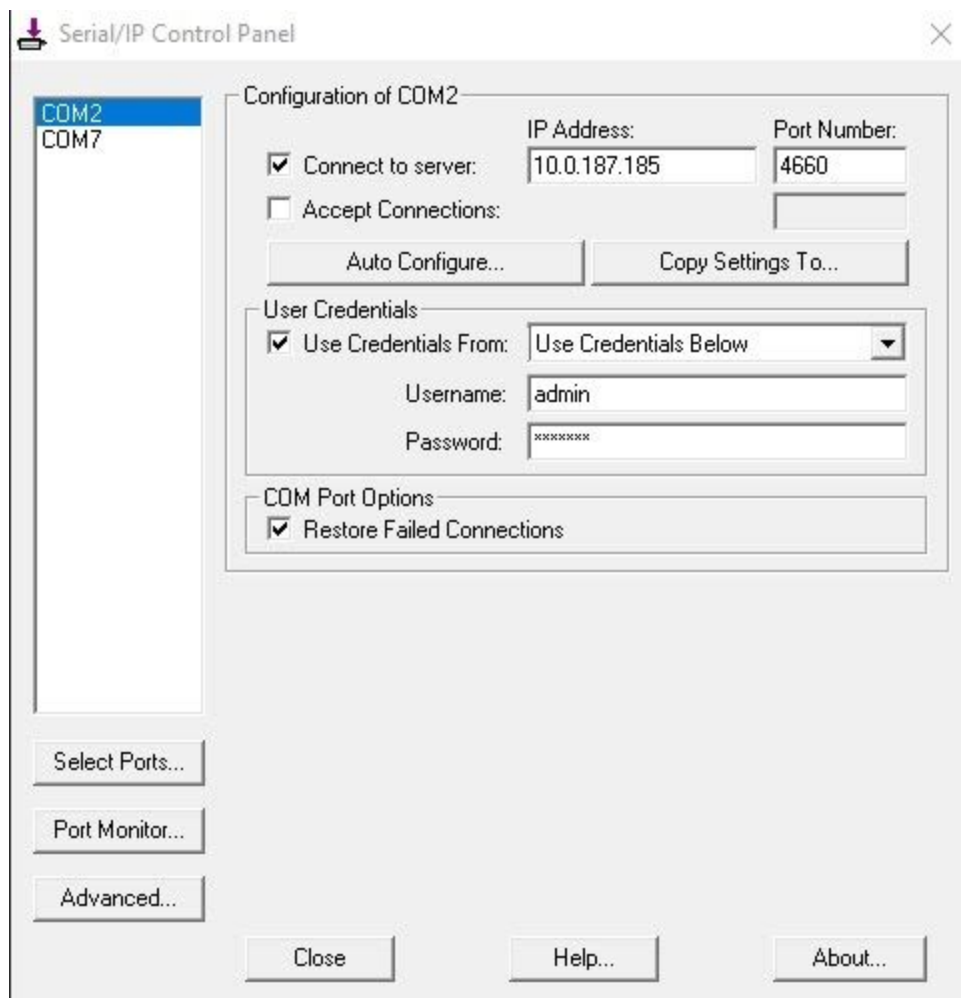


Figure 5.9 - Configuring Virtual COM 2 Port as TCP Client

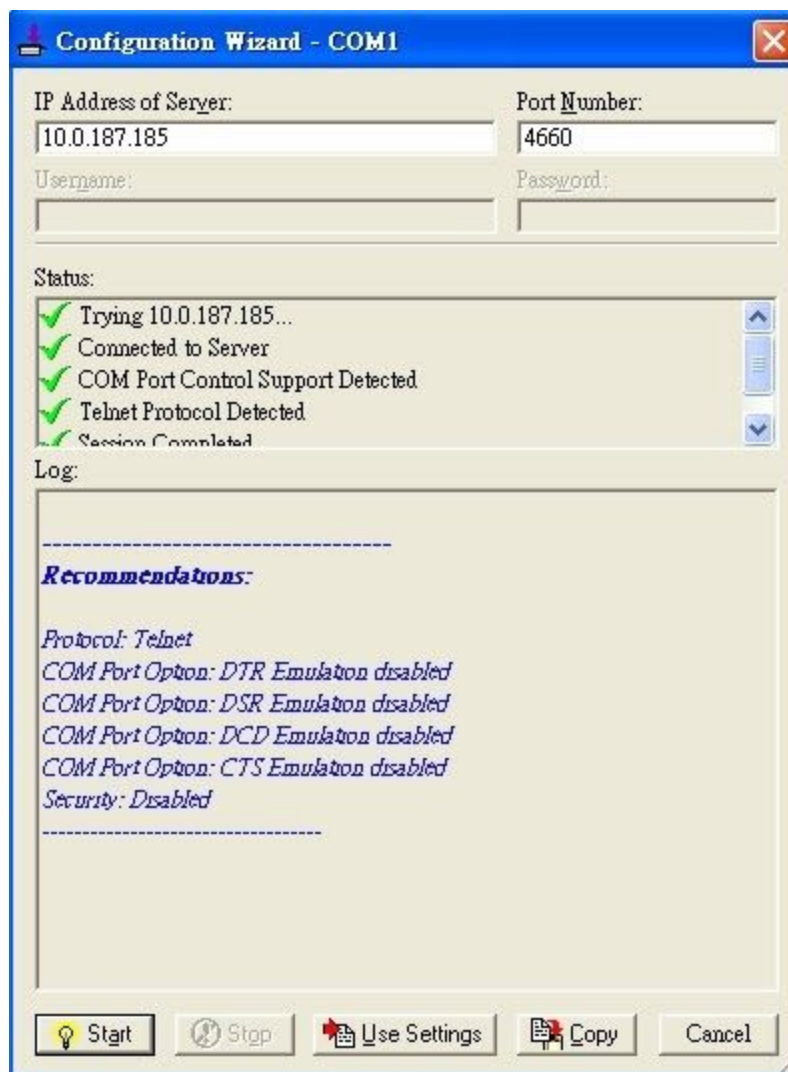


Figure 5.10 - Auto Configure (Formerly Configuration Wizard) Window for COM 1

## 5.3 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 an 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 5.11, please recheck or correct the VCOM IP address and Port number configuration or the PC’s network configuration.

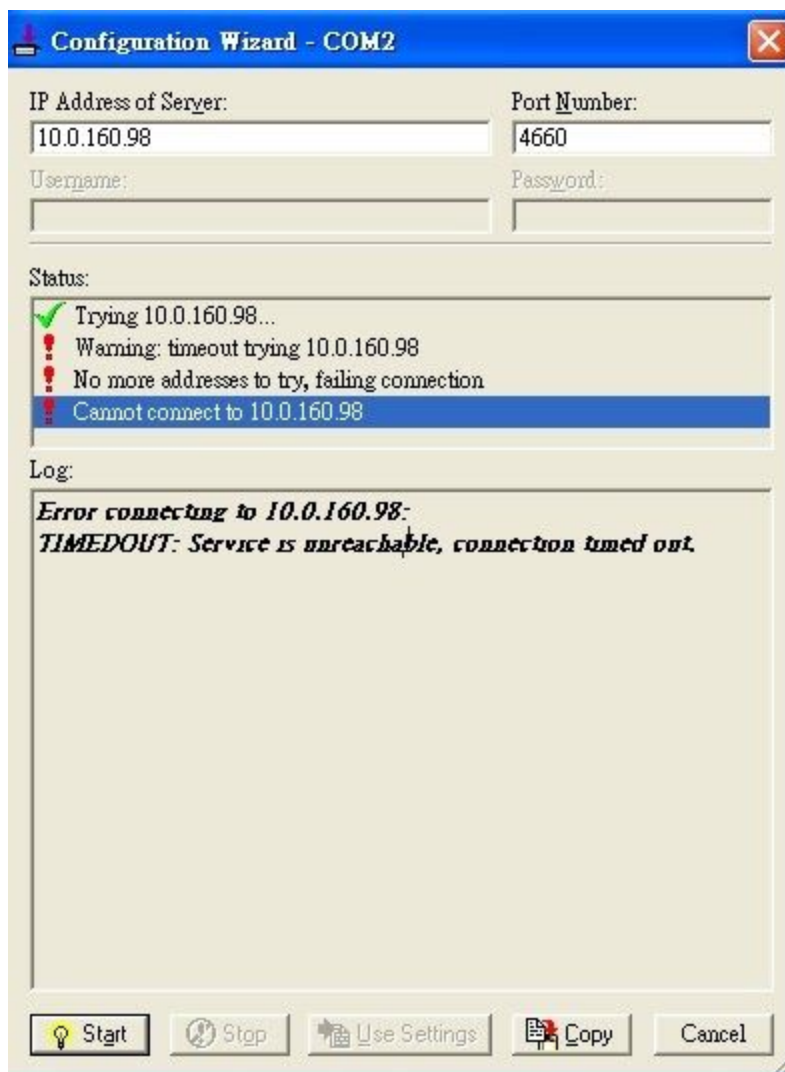


Figure 5.11 - Timeout Warning on VCOM Connection

- 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 5.12. Please enable the Virtual COM option in the serial Device server.

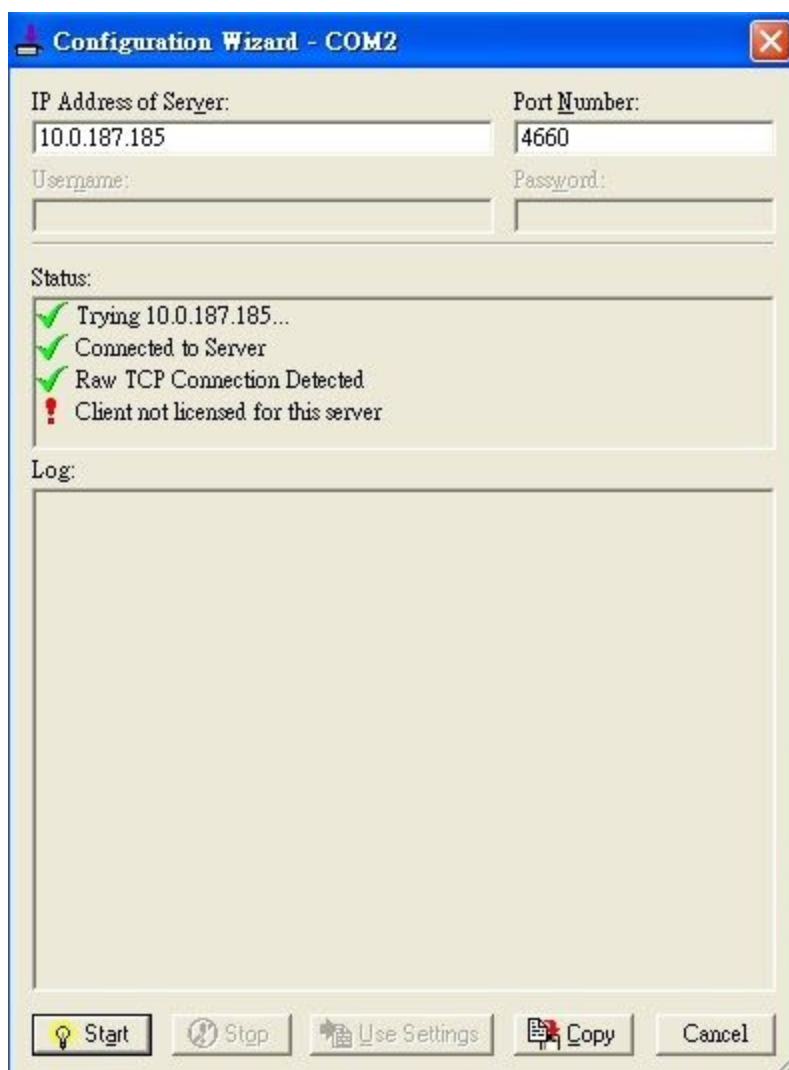


Figure 5.12 - Error of Client Not Licensed for this Server

- 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 5.13. This means that there is a licensing issue between the serial gateway (i.e. STE-6104C) and the Serial/IP Utility Software. Please contact Antaira’s technical support to obtain the correct VCOM software.



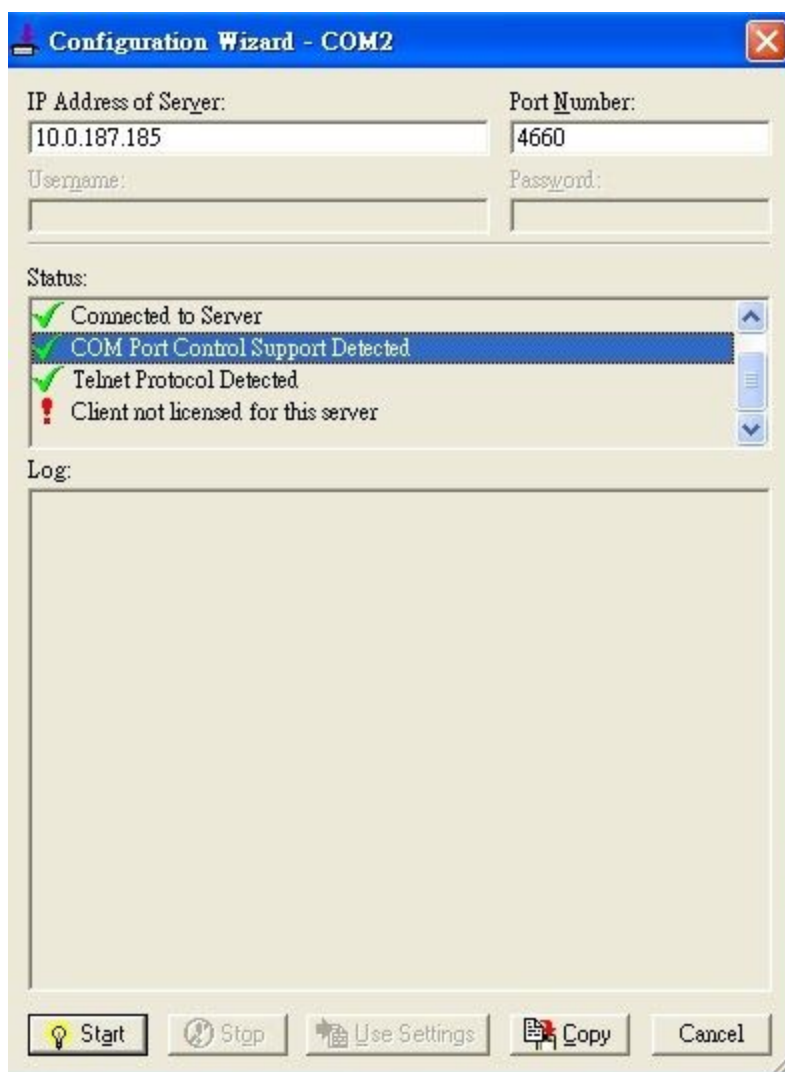


Figure 5.13 - Licensing Issue of Serial/IP Utility Software

- If the status reports with an exclamation mark with a message **"Server requires username/password login"** as shown in Figure 5.14. This means that the **VCOM Authentication** option in the serial device server (i.e. STE-6104C) is enabled but the **User Credentials** option in the **Serial/IP** utility software is not enabled. Please follow the steps in Section 3.16.2 for enabling the user credentials option and entering the username and the password.

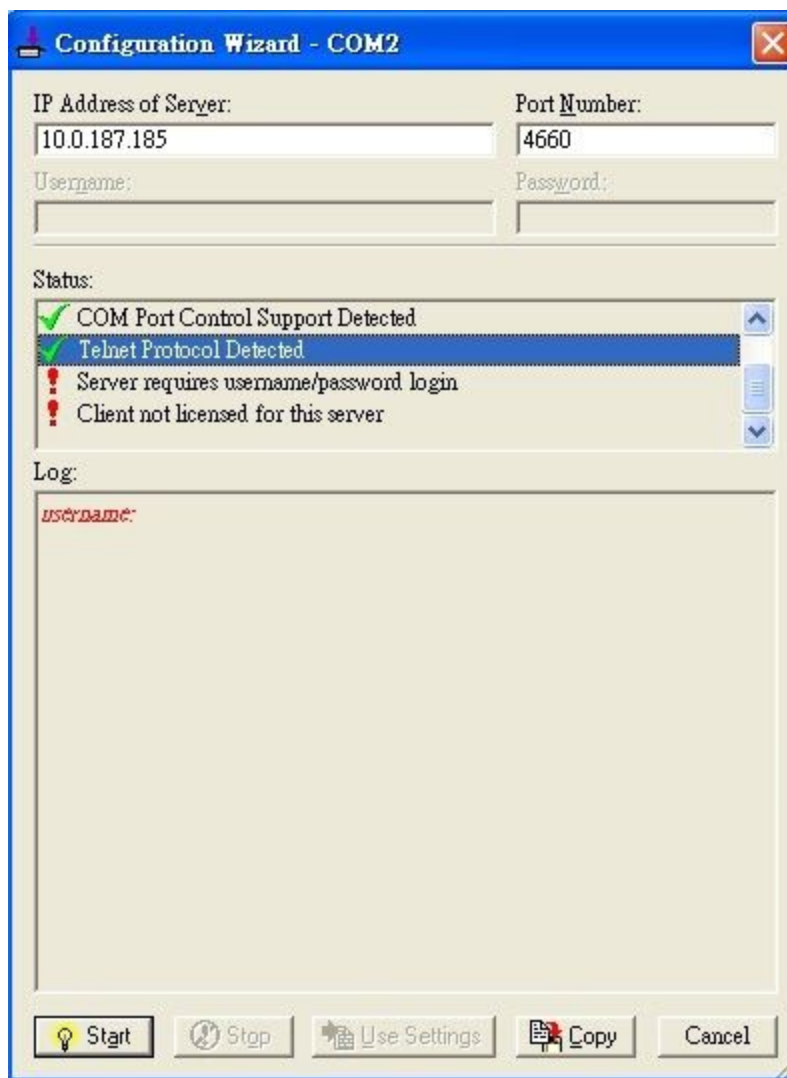


Figure 5.14 - VCOM Authentication Failed Due to Missing Username/Password

- If the status reports with an exclamation mark with a message **"Username and/or password incorrect"** as shown in Figure 5.15. This means that the wrong username and/or password were entered and the authentication process failed.

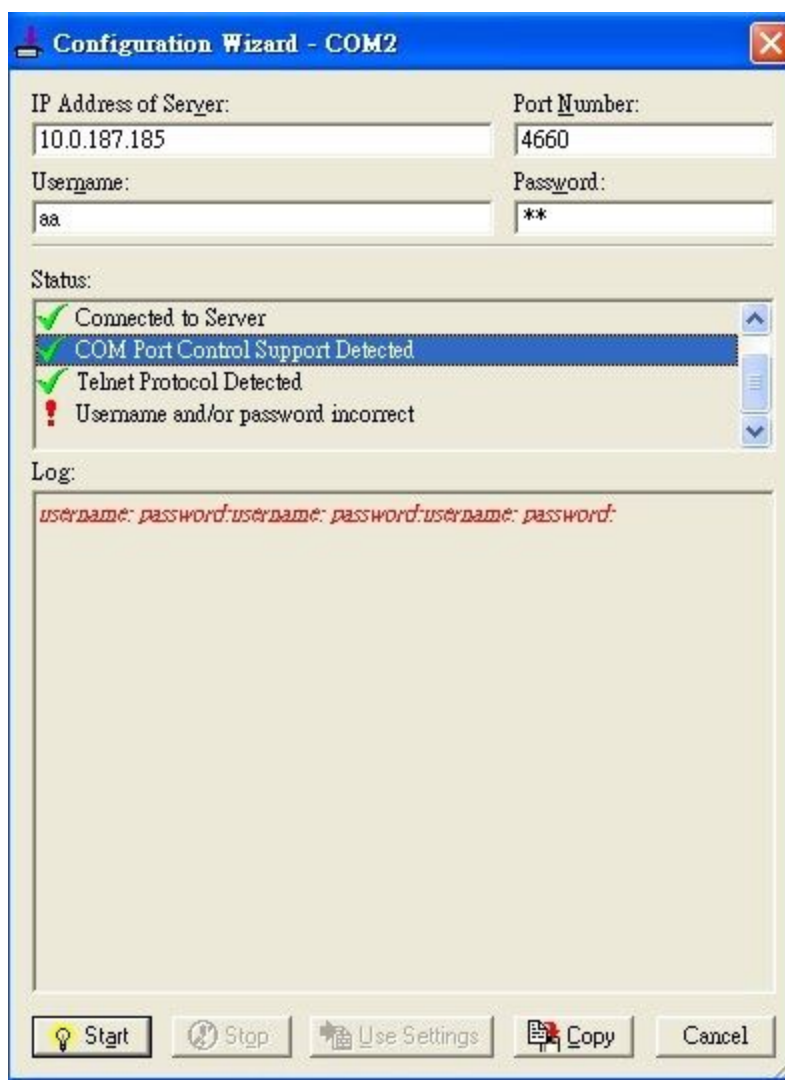


Figure 5.15 - VCOM Authentication Failed Due to Incorrect Username and/or Password

- If the status reports with an exclamation mark with a message **“No login/password prompts received from server”** as shown in Figure 5.16. 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. STE-6104C) is not enabled. Please enable the **VCOM Authentication** option on the STE-6104C by setting a new and non-blank administrator’s Username and Password for the STE-6104C as described in Section 3.16.2. Note that the **Username** and the **Password** for VCOM authentication are the same username and password of the STE-6104C 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.

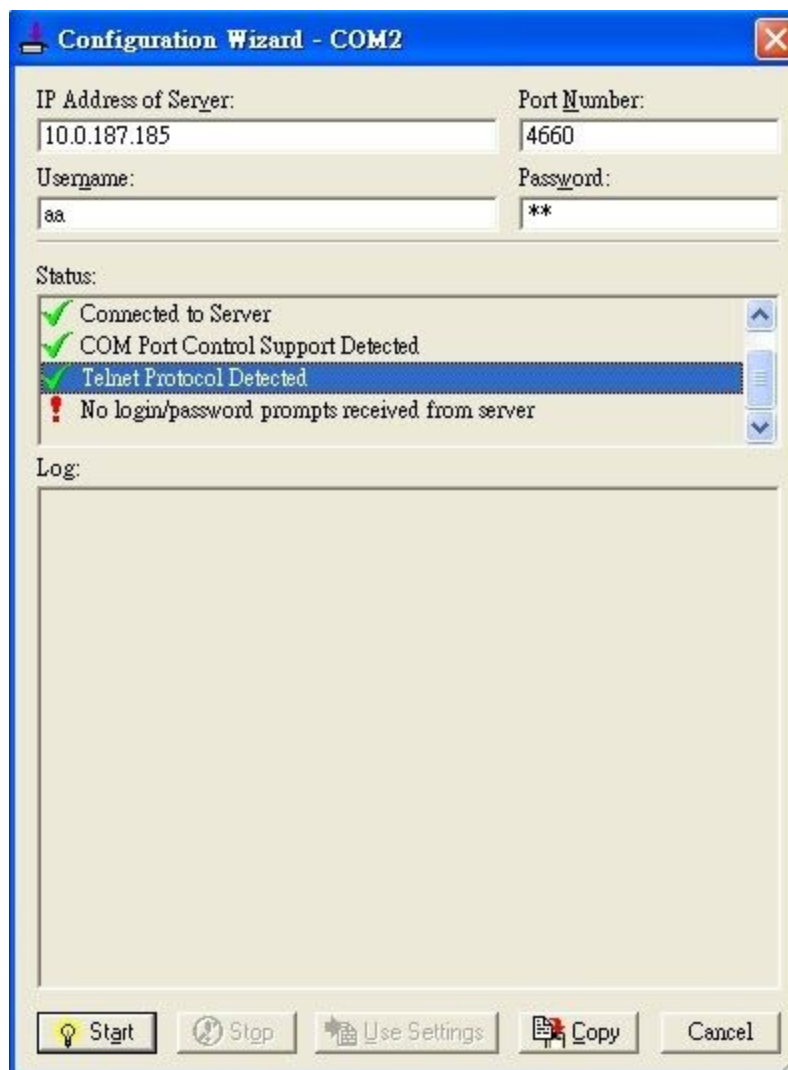


Figure 5.16 - VCOM Authentication Failed Due to Disabled VCOM Authentication on the STE-6104C

## 5.4 Using Serial/IP Port Monitor

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

### 5.4.1 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.

## 5.4.2 The Activity Panel

The **Activity** panel provides a real-time display of the status of all Serial/IP COM ports as shown in *Figure 5.17*. If the Virtual COM Port is opened and is properly configured to connect to a serial device server (i.e. STE-6104C), the status would be **Connected**. If Serial/IP utility software cannot find the specified serial device server, the status would be **Offline**.

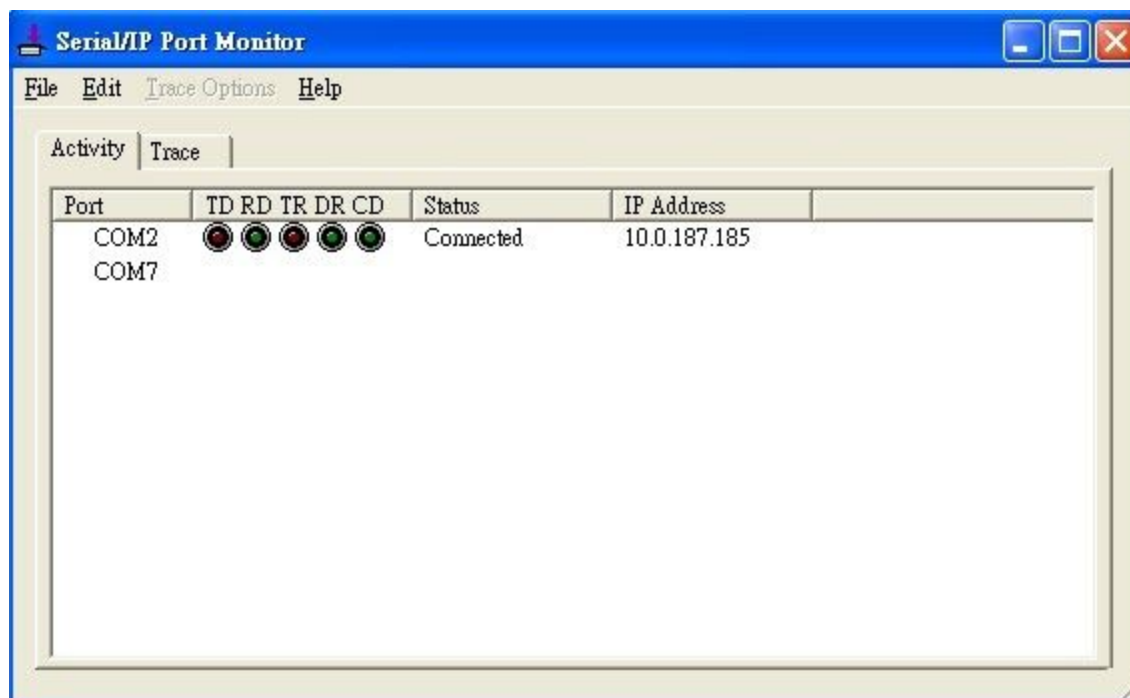


Figure 5.17 - Activity Panel of Serial/IP Port Monitor

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 indicates 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.

### 5.4.3 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 5.18*. Click on the **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 the **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 the **Trace** panel, click on the **Clear** button.

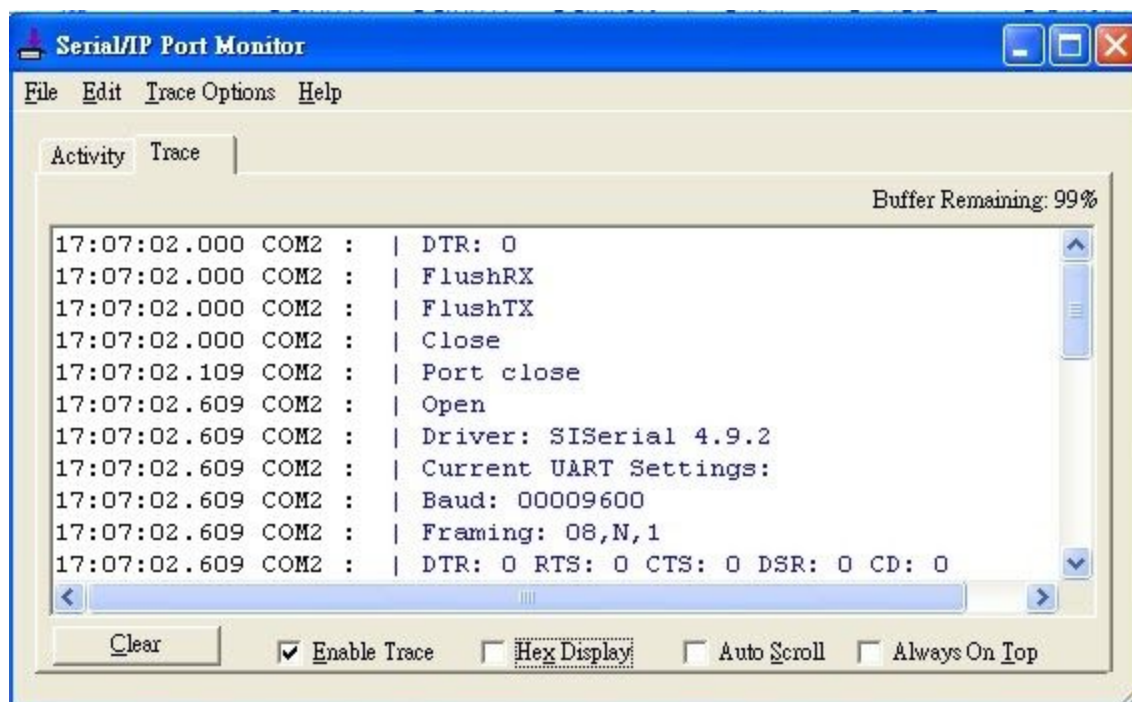


Figure 5.18 - Trace Panel of Serial/IP Port Monitor

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 Antaira for further analysis if problems occur with the Virtual COM connection, please click on the **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 users 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 "I".

**\*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.

## **5.5 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 5.19*. 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. A detailed description of each option and how to set a proxy server will be explained in the following subsections.



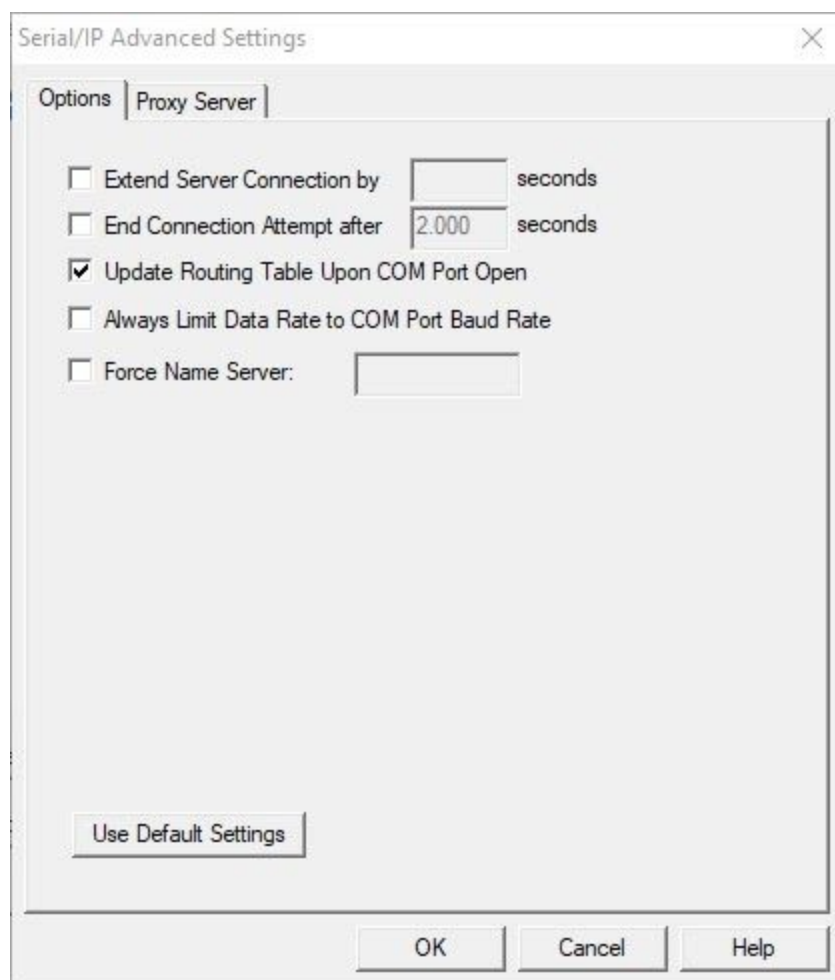


Figure 5.19 - Serial/IP Advanced Settings Window

### 5.5.1 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 a specified amount of time after the 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.

### 5.5.2 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 5.20*. To enable the use of a 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 the **Stop** button.

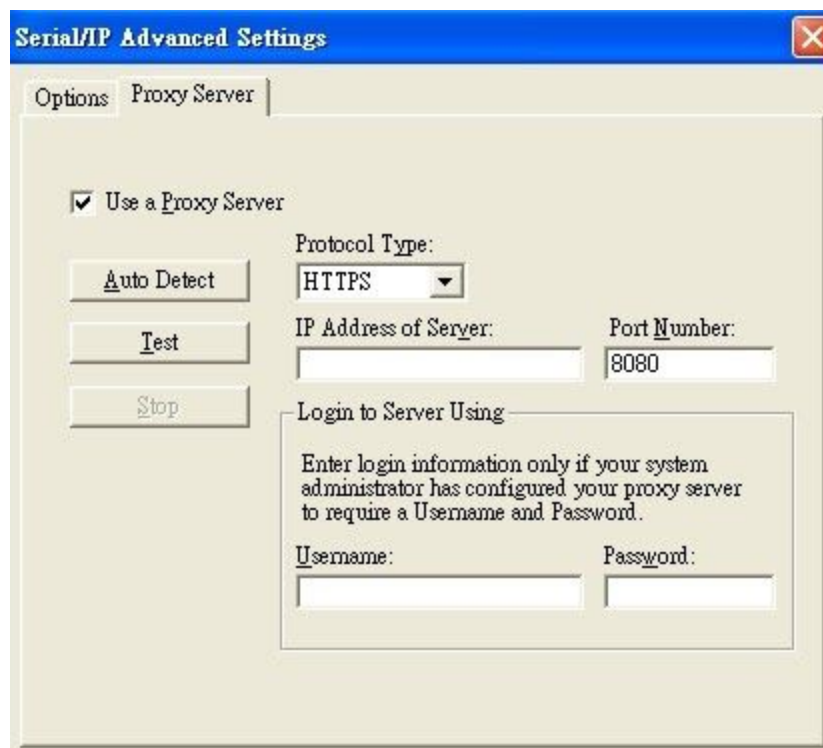


Figure 5.20 - Proxy Server Tab under Serial/IP Advanced Settings

## 6 Specifications

### 6.1 Hardware

System	
CPU	32-bit ARM Based TI CPU AM3354 800MHz
Flash Memory	32MB
RAM	DDR3 256MB
EEPROM	8KB
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)
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	RS232/RS422/RS485 Software Selectable (Default: RS232)
Serial Connector	Connector Type - 4 Serial DB-9 Ports
Protection	16A (optional 3V)
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 (RS232 only), XON/XOFF, None
LED Indicators	

LED Indication	Power x2 RUN x1 ALARM x1 LAN: x2 COM port: x4
<b>Power Requirement &amp; EMC</b>	
Input	Dual 12~48VDC
Consumption	Max. 8W
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
<b>Mechanical</b>	
Dimensions (W x H x D, mm)	55 x 145 x 113 mm (2.17 x 5.17 x 4.45 in)
Enclosure	IP30 protection, metal housing
<b>Environmental</b>	
Temperature	Operations: -40°C ~ 85°C (-40°F ~ 185°F) Storage: -40°C ~ 85°C (-40°F ~ 185°F)
Relative Humidity	5% ~ 95%, non-condensing

Table 6.1 - Hardware Specifications

## 6.2 Serial Port Pin Assignments

### 6.2.1 Pin Assignments

DB9 to RS232/RS485/RS422 Connectors

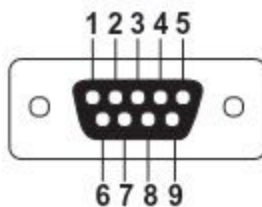


Figure 6.1 - DB9 Pin Number

Pin #	RS232 Full Duplex	RS422 Full Duplex	RS485 Half Duplex
1	DCD	-	-
2	RxD	TxD+	Data+
3	TxD	RxD+	-
4	DTR	-	-
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)
6	DSR	-	-
7	RTS	RxD-	-
8	CTS	TxD-	Data-
9	RI	-	-

Table 6.2 - Pin Assignment for DB9 to RS232/RS422/RS485 Connectors

## 6.3 LED Indicators

Name	Color	Status	Message
PWR (Power)	Green	Steady/On	Power On and Power is being supplied
		Off	Power Off
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 1Gbps
		Blinking slowly	Ethernet is transmitting at 100Mbps
		Off	Ethernet is transmitting at 10Mbps

	Green (Data)	Blinking	Ethernet data is transmitting
		Off	Ethernet has no data to transmit

*Table 6.3 - Color Interpretation of LED Indicators*

## 6.4 Software

Software	
Utility	Windows Virtual COM Driver and Linux TTY Driver: Linux 2.4.x, Linux 2.6.x, 3.x
Configuration Tool	<ul style="list-style-type: none"><li>- Web console</li><li>- Serial console</li><li>- SSH console</li><li>- Telnet console</li><li>- <b>Device Management Utility</b> ©</li></ul>

*Table 6.4 - Software Tools and Utilities*

## 7 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).

### 7.1 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 the STE-6104C to download a valid firmware from the TFTP Server to recover its operating system.

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 Antaira's website on the product page.	

*Table 7.1 - Default Settings for System Recovery Procedure*

- 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 Antaira directly to obtain an RMA number for further solutions.
- Obtain and set up 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.



## *Antaira Technologies - Industrial Serial Device Server*

### **STE-6104C-T-V2 - User Manual - v1.0**

---

- 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:

<b>Solarwinds TFTP Server</b>
<a href="http://www.solarwinds.com/products/freetools/free_tftp_server.aspx">http://www.solarwinds.com/products/freetools/free_tftp_server.aspx</a>
<b>**Note:</b> For solarwinds, please remember to Start the TFTP Server Service, the default state of the TFTP is Stop.
<b>TFTPD32 TFTP Server</b>
<a href="http://tftpd32.jounin.net/tftpd32.html">http://tftpd32.jounin.net/tftpd32.html</a>

#### **Antaira Customer Service and Support**

(Antaira US Headquarter) + 844-268-2472

(Antaira Europe Office) +48-22-862-88-81

(Antaira Asia Office) +886-2-2218-9733

#### **Please report any problems to Antaira:**

[www.antaira.com](http://www.antaira.com) / [support@antaira.com](mailto:support@antaira.com)

[www.antaira.eu](http://www.antaira.eu) / [info@antaira.eu](mailto:info@antaira.eu)

[www.antaira.com.tw](http://www.antaira.com.tw) / [info@antaira.com.tw](mailto:info@antaira.com.tw)

**Any changes to this material will be announced on the Antaira website.**