



SE59XX Series

Industrial Device Server Series

User Manual

v1.5

July 19th, 2019

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the [Table of Contents](#) to go to that page.

Published by:

Atop Technologies, Inc.

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

Tel: +886-3-550-8137
Fax: +886-3-550-8131
sales@atop.com.tw
www.atoponline.com
www.atop.com.tw

Important Announcement

The information contained in this document is the property of Atop technologies, Inc., and is supplied for the sole purpose of operation and maintenance of Atop Technologies, Inc., products.

No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of Atop Technologies, Inc.,
Offenders will be held liable for damages and prosecution.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.

Suggestions for improvement are welcome.

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

Documentation Control

Author:	Saowanee Saewong
Revision:	1.5
Revision History:	Add Firewall, DMZ, ICMP
Creation Date:	25 September 2017
Last Revision Date:	19 July 2019
Product Reference:	SE59XX Industrial Device Server Series User Manual
Document Status:	Update

Table of Contents

1	Preface	10
1.1	Purpose of the Manual	10
1.2	Who Should Use This User Manual	10
1.3	Supported Platform	10
1.4	Manufacturers' FCC Declaration of Conformity Statement	10
2	Introduction	11
2.1	Overview	11
2.2	Features	11
3	Getting Started	13
3.1	Packing List	13
3.2	Appearance, Front and Rear Panels	14
3.3	First Time Installation	16
3.4	Factory Default Settings	17
3.4.1	Network Default Settings	17
3.4.2	Other Default Settings	17
4	Configuration and Setup	18
4.1	Configuration of Network Parameters through Device Management Utility	18
4.2	Configuring through Web/CLI Interface	21
4.3	Configuring Automatic IP Assignment with DHCP	24
4.4	Web Overview	24
4.5	Network Settings	25
4.5.1	Ping Reboot	28
4.5.2	Dynamic DNS	28
4.6	Firewall Setting	30
4.6.1	Services	30
4.6.2	Port Forwarding	32
4.6.3	DMZ	34
4.7	Serial	35
4.7.1	COM Port Overview	36
4.7.2	COM Configuration	37
4.7.3	COM Configuration: Advanced Settings	39
4.8	VPN	41
4.9	PPTP Settings	42
4.10	OpenVPN Settings	43
4.10.1	OpenVPN Setting	43
4.10.2	OpenVPN Keys	44
4.10.3	OpenVPN Status	46
4.11	IPsec Settings	47
4.11.1	IPsec Settings	50
4.11.2	IPsec Status	54
4.11.3	Examples of IPsec Settings	54
4.11.3.1	Host-to-Host Connections	54
4.11.3.2	Host-to-Network Connections	56
4.11.3.3	Network-to-Network (Subnet-to-Subnet) Connections	57
4.12	Spanning Tree	59
4.12.1	Spanning Tree's Setting	60
4.12.2	Spanning Tree's Bridge Info	61
4.12.3	Spanning Tree's Port Setting	62

4.13	SNMP/ALERT Settings	65
4.14	SMS	67
4.14.1	Basic Settings	67
4.14.2	Phone Settings	68
4.14.3	Manual Send	70
4.14.4	Remote Control Command List	71
4.14.5	Alert Type List	72
4.15	E-Mail Settings	74
4.16	Log Settings	75
4.16.1	System Log Settings	75
4.16.2	COM Log Settings	76
4.16.3	Event Log	77
4.16.4	COM Datalog	77
4.17	System Setup	78
4.17.1	Date/Time Settings	78
4.17.2	Admin Settings	80
4.17.3	Firmware Upgrade	81
4.17.4	Backup/Restore Settings	81
4.17.5	Ping	82
4.17.6	Special Settings	84
4.17.6.1	Examples of SE5901B DO & DI Command Set	86
4.18	Reboot	87
5	Link Modes and Applications	88
5.1	Link Mode Configuration	88
5.1.1	Link Mode: Configure SE59XX as a TCP Server	88
5.1.2	Link Mode: Configure SE59XX as a TCP Client	91
5.1.3	Link Mode: Configure SE59XX in UDP	94
5.2	Link Mode Applications	97
5.2.1	TCP Server Application: Enable Virtual COM	97
5.2.2	TCP Server Application: Enable RFC 2217 through Virtual COM	98
5.2.3	TCP Client Application: Enable Virtual COM	98
5.2.4	TCP Client Application: Enable RFC 2217 through Virtual COM	98
5.2.5	TCP Server Application: Configure SE59XX as a Pair Connection Master	99
5.2.6	TCP Client Application: Configure SE59XX as a Pair Connection Slave	99
5.2.7	TCP Server Application: Enable Reverse Telnet	101
6	VCOM Installation & Troubleshooting	102
6.1	Enabling VCOM	102
6.1.1	VCOM driver setup	104
6.1.2	Limitation	105
6.1.3	Installation	105
6.1.4	Uninstallation	105
6.2	Enable VCOM in Serial Device servers and Select VCOM in Windows	105
6.2.1	Enable VCOM in Serial Device servers	105
6.2.2	Running Serial/IP Software Utility in Windows	106
6.2.3	Configuring VCOM Ports	108
6.3	Exceptions	112
6.4	Using Serial/IP Port Monitor	118
6.4.1	Opening the Port Monitor	118
6.4.2	The Activity Panel	118
6.4.3	The Trace Panel	119
6.5	Serial/IP Advanced Settings	121
6.5.1	Advanced Setting Options	121

6.5.2	Using Serial/IP with a Proxy Server	122
7	Specifications	123
7.1	Hardware.....	123
7.2	Serial port Pin Assignments	125
7.2.1	SE5901 Pin Assignments for Serial Interfaces.....	125
7.2.2	SE5904D Pin Assignments	126
7.2.3	SE5901B Pin Assignments	127
7.2.4	SE5908A/ SE5916A Pin Assignments	128
7.2.5	SE5908/ SE5916 Pin Assignments	130
7.2.6	SE59XX Pin Assignments for LAN Interface	131
7.3	LED Indicators	132
7.4	Software.....	132
8	Emergency System Recovery	133
8.1	System Recovery Procedures.....	133
9	Warranty	134

Table of Figures

Figure 2.1	An Application of SE59XX Industrial Serial Device Server with Multiple Devices	11
Figure 4.1	List of Device in Device Management Utility.....	18
Figure 4.2	Pull-down Menu of Configuration and Network.....	18
Figure 4.3	Pop-up Window of Network Setting	19
Figure 4.4	Authorization for Change of Network Settings.....	19
Figure 4.5	Pop-up Notification Window after Authorization	19
Figure 4.6	Pop-up Notification Window when there is the same IP address in the network.....	20
Figure 4.7	Authentication Required for Accessing Web Interface	21
Figure 4.8	Warning Pop-up Window for Changing or Resetting Password from Default Value	21
Figure 4.9	Overview Web Page of SE59XX Industrial Serial Device Server (example on SE5901B).	22
Figure 4.10	Map of Configuring Web Page on SE59XX Industrial Serial Device Server (ex. on SE5901B)	22
Figure 4.11	Access control	23
Figure 4.12	CLI interface.....	23
Figure 4.13	Overview Web Page (example on SE5901B)	24
Figure 4.14	Network Settings Web Page	25
Figure 4.15	Network Settings Menu of SE5901B series	26
Figure 4.16	NAT Settings under IPv4 Settings Web Page for SE5901B	26
Figure 4.17	Enabling of NAT Settings with Additional Parameters for SE5901B.....	27
Figure 4.18	A pop-up window shows an empty list of DHCP Connected Clients.....	27
Figure 4.19	Ping Reboot Web Page under Network Settings	28
Figure 4.20	Example of Dynamic DNS Server Operations	29
Figure 4.21	Dynamic DNS Web Page	29
Figure 4.22	Firewall Setting Menu of SE5901B	30
Figure 4.23	Services Page under Firewall Setting Menu	31
Figure 4.24	Example of Port Forwarding through SE5901B Industrial Device Server.....	32
Figure 4.25	Port Forwarding Web Page of SE5901B series	33
Figure 4.26	DMZ Page under Firewall Setting Menu.....	34
Figure 4.27	Serial Menu (example on SE5904D).....	35
Figure 4.28	COM 1 Port Settings Web Page.....	36

Figure 4.29 Serial Settings Part of COM 1 Port	37
Figure 4.30 Serial Settings for COM 1 of SE5901B (Note that it supports only RS-232 and RS-485)	38
Figure 4.31 COM 1 Advanced Settings Web Page	39
Figure 4.32 VPN Scenario of SE/PG/MB59XX	41
Figure 4.33 VPN menu structure	41
Figure 4.34 PPTP configuration page.	42
Figure 4.35 PPTP Link Status	42
Figure 4.36 OpenVPN Setting	43
Figure 4.37 OpenVPN Keys	44
Figure 4.38 Certification information	45
Figure 4.39 Certificate Upload	45
Figure 4.40 OpenVPN client status	46
Figure 4.41 OpenVPN server status	46
Figure 4.42 An example of Host-to-Host Connection	47
Figure 4.43 Roadwarrior Application using Host-to-Subnet Connection	48
Figure 4.44 Gateway Application using Host-to-Subnet Connection	48
Figure 4.45 An example of network application using a subnet-to-subnet connection via the SE59XX and a peer device	48
Figure 4.46 An example of host-network application via the subnet-to-subnet connection	49
Figure 4.47 An example of host-host application via the subnet-to-subnet connection	49
Figure 4.48 IPsec Tunnels Web Page under IPsec Setting Menu	50
Figure 4.49 IPsec Status Web Page	54
Figure 4.50 IPsec VPN Tunnel with Host-to-Host Topology	55
Figure 4.51 General Settings for Host-to-Host with Static Peer	55
Figure 4.52 General Settings for Host-to-Host with Dynamic Peer	56
Figure 4.53 IPsec VPN Tunnel with Host-to-Network Topology	56
Figure 4.54 General Settings for Host-to-Network with Static Peer	57
Figure 4.55 General Settings for Host-to-Network with Dynamic Peer	57
Figure 4.56 IPsec VPN Tunnel with Network-to-Network Topology	58
Figure 4.57 General Settings for Network-to-Network with Static Peer	58
Figure 4.58 General Settings for Network-to-Network with Dynamic Peer	59
Figure 4.59 Spanning Tree Menu	59
Figure 4.60 Setting Web Page of Spanning Tree	60
Figure 4.61 Bridge Info Web Page of Spanning Tree	61
Figure 4.62 Spanning Tree Port Setting (Part 1)	62
Figure 4.63 Spanning Tree Port Setting (Part 2)	62
Figure 4.64 SNMP/Alert Settings Web Page	65
Figure 4.65 Basic Settings Web page for SMS	67
Figure 4.66 Phone Settings Web Page for SMS	69
Figure 4.67 Manual Send Web Page under SMS	70
Figure 4.68 E-mail Setting Web Page	74
Figure 4.69 Log Settings Menu	75
Figure 4.70 Log Settings Web Page under Log Settings	75
Figure 4.71 COM Log Settings Web Page under System Setup	76
Figure 4.72 System Log Web Page under System Setup	77
Figure 4.73 COM Datalog Web Page under Log Settings	78
Figure 4.74 System Setup Menu	78
Figure 4.75 Date/Time Settings Web Page under System Setup	79
Figure 4.76 Admin Settings Web Page under System Setup	80
Figure 4.77 Firmware Upgrade Web Page under System Setup	81
Figure 4.78 Backup/Restore Settings Web Page under System Setup	82
Figure 4.79 Ping Web Page under System Setup	83
Figure 4.80 Unreachable Ping Example	83
Figure 4.81 Special Setting Web Page under System Setup for SE5901B with IO version only	84
Figure 4.82 Reboot Web Page	87

Figure 5.1 Link Mode Options for COM1 Port	88
Figure 5.2 SE59XX is set as a TCP Server Link Mode.....	89
Figure 5.3 Connection Settings for TCP Server Link Mode	89
Figure 5.4 TCP Server Link Mode Settings under COM 1 Page.....	90
Figure 5.5 Example of SE59XX Configured as TCP Client Link Mode	92
Figure 5.6 Connection Settings for TCP Client Link Mode	92
Figure 5.7 Setting in TCP Client Link Mode	93
Figure 5.8 Example of SE59XX Configured in UDP Link Mode.....	95
Figure 5.9 Connection Setting in UDP Link Mode	95
Figure 5.10 UDP Link Mode Setting under COM 1 Page	96
Figure 5.11 Virtual COM Application in TCP Server Link Mode.....	97
Figure 5.12 Virtual COM Application in TCP Client Link Mode.....	98
Figure 5.13 Pair Connection Master Application in TCP Server Link Mode	99
Figure 5.14 Pair Connection Slave Application in TCP Client Link Mode	100
Figure 5.15 Reverse Telnet Application in TCP Server Link Mode	101
Figure 6.1 Enable a Virtual COM Application When Setting the Link Mode as the TCP Server.....	102
Figure 6.2 Enable a Virtual COM Application When Setting the Link Mode as the TCP Client.....	103
Figure 6.3 An Example Diagram of Virtual COM Application over TCP/IP Network	104
Figure 6.4 Enable Virtual COM Application for COM 2 in TCP Server Link Mode	105
Figure 6.5 Serial/IP Tray Icon on Windows Notification Area	106
Figure 6.6 A Pop-up Window for Selecting Virtual COM Ports	107
Figure 6.7 Serial/IP Control Panel Window.....	108
Figure 6.8 Available Options for Use Credential From in Serial/IP Control Panel Version 4.9.10	109
Figure 6.9 Configuring Virtual COM 2 Port as TCP Client.....	110
Figure 6.10 Auto Configure (formerly Configuration Wizard) Window for COM 1	111
Figure 6.11 Timeout Warning on VCOM Connection	112
Figure 6.12 Error of Client not licensed for this server	113
Figure 6.13 Licensing Issue of Serial/IP Utility Software.....	114
Figure 6.14 VCOM Authentication failed due to Missing Username/Password	115
Figure 6.15 VCOM Authentication failed due to incorrect Username and/or Password	116
Figure 6.16 VCOM Authentication failed due to disabled VCOM Authentication on SE59XX.....	117
Figure 6.17 Activity Panel of Serial/IP Port Monitor	118
Figure 6.18 Trace Panel of Serial/IP Port Monitor	119
Figure 6.19 Serial/IP Advanced Settings Window	121
Figure 6.20 Proxy Server Tab under Serial/IP Advanced Settings	122
Figure 7.1 DB9 Pin Number	125
Figure 7.2 TB5 Pin Number.....	125
Figure 7.3 DB9 Pin Number	126
Figure 7.4 Terminal Block (TB-5) Pin Number.....	127
Figure 7.5 DB9 Pin Number	127
Figure 7.6 2 x 7-pin Male Terminal Block.....	128
Figure 7.7 DB9 Pin Number	128
Figure 7.8 Terminal Block (TB-5) Pin Number.....	129
Figure 7.9 MB5908/MB5916 Serial port on RJ45 Pin Numbering	130
Figure 7.10 SE59XX Ethernet Port on RJ45 with Pin Numbering.....	131

List of Tables

Table 3.1 Packing List.....	13
Table 3.2 Description of Optional Accessories	13
Table 3.3 Network Default Setting	17
Table 3.4 Security , Serial, and SNMP Default Settings	17
Table 4.1 Descriptions of Ping Reboot's Parameters	28
Table 4.2 Descriptions of Dynamic DNS Web Page's parameters	30
Table 4.3 Descriptions of Parameters for Services under Firewall Setting	31
Table 4.4 Description of Fields in Port Forwarding Table.....	33
Table 4.5 Description of DMZ's Options	34
Table 4.6 Description of Parameters in IPsec Tunnels Web Page.....	52
Table 4.7 Descriptions of Spanning Tree Parameters	60
Table 4.8 Bridge's Root Information	61
Table 4.9 Bridge's Topology Information.....	62
Table 4.10 Descriptions of Spanning Tree Port Setting.....	63
Table 4.11 Default Path Cost for RSTP.....	64
Table 4.12 Description of Options under the Basic Settings of SMS.....	68
Table 4.13 Description of Options under the Phone Settings of SMS	70
Table 4.14 Description of Options in the Manual Send Web Page.....	70
Table 4.15 List of All Supported Remote Control Commands	71
Table 4.16 List of All SMS Alert Types.....	72
Table 7.1 Hardware Specification	123
Table 7.2 SE59XX Pin Assignment for DB9 to RS-232/RS-422/RS-485 Connector	125
Table 7.3 SE59XX Pin Assignment for TB5 to RS-232/RS-422/RS-485 Connector	125
Table 7.4 MB5904D Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors.....	126
Table 7.5 MB5904D Pin Assignment for 5-Pin Terminal Block to RS-232/RS-422/RS-485 Connectors	127
Table 7.6 MB5901B Pin Assignment for DB9 to RS-232/RS-485 Connector	127
Table 7.7 SE5901B 2 x 7-pin Male TB for RS-232/485(COM 1),RS-232(COM 2) Relay and DI pin-assignment	128
Table 7.8 MB5908A/16A Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors.....	128
Table 7.9 MB5908A/16A Pin Assignment for 5-Pin Terminal Block to RS-232/RS-422/RS-485 Connectors	129
Table 7.10 MB5908/16 Pin Assignment for RJ45 to RS-232/RS422/RS-485 Connectors.....	130
Table 7.11 SE59XX Pin Assignment for RJ-45 Connector	131
Table 7.12 Color Interpretation of LED Indicators of SE59XX	132
Table 7.13 Software Tools and Utilities	132
Table 8.1 Default Settings for System Recovery Procedure.....	133

1 Preface

1.1 *Purpose of the Manual*

This manual supports the user during the installation and configuring of the SE59XX Industrial Device Server Series. It explains the technical features available with the mentioned product. As such, it contains some advanced network management knowledge, instructions, examples, guidelines and general theories designed to help users manage this device and its corresponding software. A background in general theory is necessary when reading it. Please refer to the Glossary for technical terms and abbreviations (if any).

1.2 *Who Should Use This User Manual*

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

1.3 *Supported Platform*

This manual is designed for **SE59XX Industrial Serial Device Server Series** and that series only.

1.4 *Manufacturers' FCC Declaration of Conformity Statement*

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

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause an undesired operation.

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

2 Introduction

2.1 Overview

The SE59XX is an industrial Ethernet serial device server which acts as a gateway for communications between Ethernet (TCP/UDP) port and RS-232/RS-422/RS-485 port. The information conveyed by the SE59XX model is transparent to both host computers (Ethernet) and serial devices (RS-232/RS-422/RS-485). Data coming from the Ethernet port is sent to the designated RS-232/RS-422/RS-485 port, and data received from RS-232/RS-422/RS-485 port is sent to the Ethernet port, allowing full-duplex and bi-directional communication. In the computer-aided manufacturing or industrial automation areas, field devices can directly connect to an Ethernet network via the SE59XX model. In normal PCs or laptops, a virtual COM port can be created using our virtual COM software to fetch serial data from SE59XX remotely over Ethernet. Note that SE5901B model does not support RS-422 and 4-wired RS-485.

With the SE59XX model, it is possible to communicate with a remote serial device over the LAN or even over the Internet, which dramatically increases reachability and scalability.

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



Figure 2.1 An Application of SE59XX Industrial Serial Device Server with Multiple Devices

2.2 Features

The SE59XX Industrial Serial Device Server Series share the same software platform on different available hardwares. It provides

- Flexible hardware platform, in different port variants based on Your needs
- TCP Server/Client, UDP, Virtual COM and Tunneling modes supported
- Remotely monitor, manage, and control industrial field devices

- Configuration via Web Browser/ Serial Console/ Telnet Console/ Atop's Windows Utility (Device Management Utility)
- Rugged metal housing with IP30 protection for wall or DIN-Rail mount
- Wide range power supply input between 9 – 48 VDC

Caution

Beginning from here, extreme caution must be exercised.



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



Warning: HOT!

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

3 Getting Started

3.1 Packing List

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

Table 3.1 Packing List

Item	Quantity	Description
SE59XX	1	Industrial Serial Device Server
Mounting Kit	1	On SE5908 / SE5916 / SE5908A / SE5916A <ul style="list-style-type: none">• Rack Mounting Type-L angles (x 2)• Screws (x 6) On SE5901 / SE5904D / SE5901B - DIN Rail Kit
Terminal Block		Power Supply/ Relay output: <ul style="list-style-type: none">• TB3 x 1: 3-pin 5.08mm lockable Terminal Block (SE5901, SE5901B)• TB3 x 2: 3-pin 5.08mm lockable Terminal Block (SE5908-DC, SE5916-DC)• TB7 x 1: 7-pin 5.08mm lockable Terminal Block (SE5904D only) Serial ports: Terminal block is included only on TB model <ul style="list-style-type: none">• TB5 x 1: 5-pin 5.08mm lockable Terminal Block (SE5901)• TB5 x 4: 5-pin 5.08mm lockable Terminal Block (SE5904D)• TB5 x 8: 5-pin 5.08mm lockable Terminal Block (SE5908A)• TB5 x 16: 5-pin 5.08mm lockable Terminal Block (SE5916A)
Documentation	1	Hardware Installation Guide (Warranty card is included)

Note:

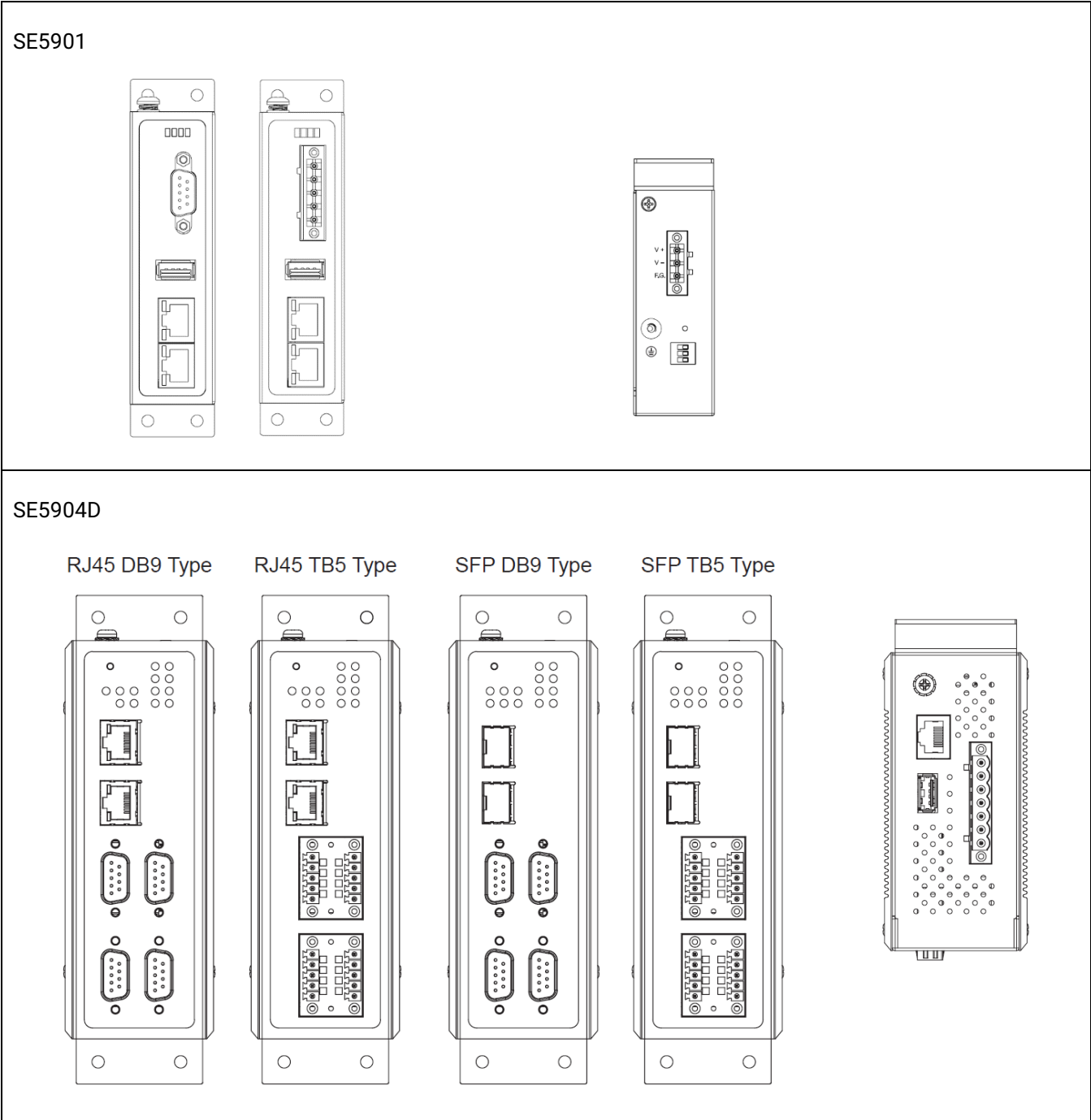
- Notify your sales representative immediately if any of the above items is missing or damaged upon delivery.
- Atop's utility software Device View® and Serial Manager® are obsolete and replaced by Device Management Utility®.

Table 3.2 Description of Optional Accessories

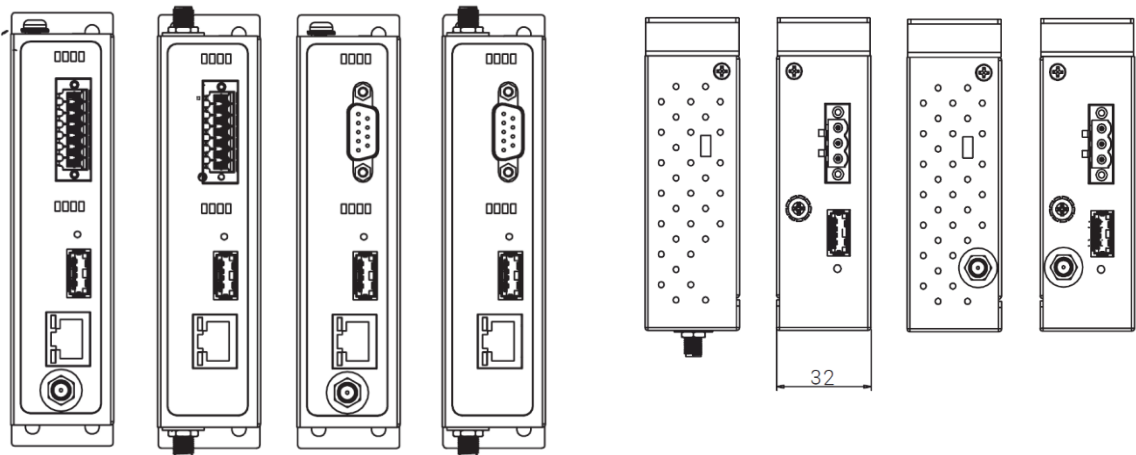
Optional Accessories		
Model Name	Part Number	Description
Wall Mount Kit	70100000000050G	Black aluminum wall mount kit
ADP-DB9(F)-TB5	59906231G	Female DB9 to Female 3.81mm, a TB5 Converter
SDR-75-24	50500752240001G	75W/3.2A DIN-Rail 24VDC power supply 88~264VAC/124-370VDC in
UN315-1212(US-Y)	50500151120003G	Y-Type power adaptor, 100~240VAC input, 1.25A @ 12VDC output, US plug, LV6
UNE315-1212(EU-Y)	50500151120013G	Y-Type power adaptor, 100~240VAC in, 1.25A @ 12VDC out, EU plug, LV6
LM28-C3S-TI-N	50708031G	SFP Transceiver, 1250Mbps, 850nm VCSEL, Multi-mode, 550m, -20~85C
LM38-C3S-TI-N	50709411G	SFP Transceiver, 1250Mbps, 1310nm FP, Multi-mode, 2km, -40~85C
LS38-C3S-TI-N	50709391G	SFP Transceiver, 1250Mbps, 1310nm FP, Single-mode, 10km, -40~85C
LS38-C3L-TI-N	50709441G	SFP Transceiver, 1250Mbps, 1310nm DFB, Single-mode, 30km, -40~85C
LM38-A3S-TI-N	50708051G	SFP Transceiver, 155Mbps, 1310nm LED, Multi-mode, 2km, -40~85C
LS38-A3S-TI-N	50709431G	SFP Transceiver, 155Mbps, 1310nm FP, Single-mode, 30km, -40~85C

3.2 Appearance, Front and Rear Panels

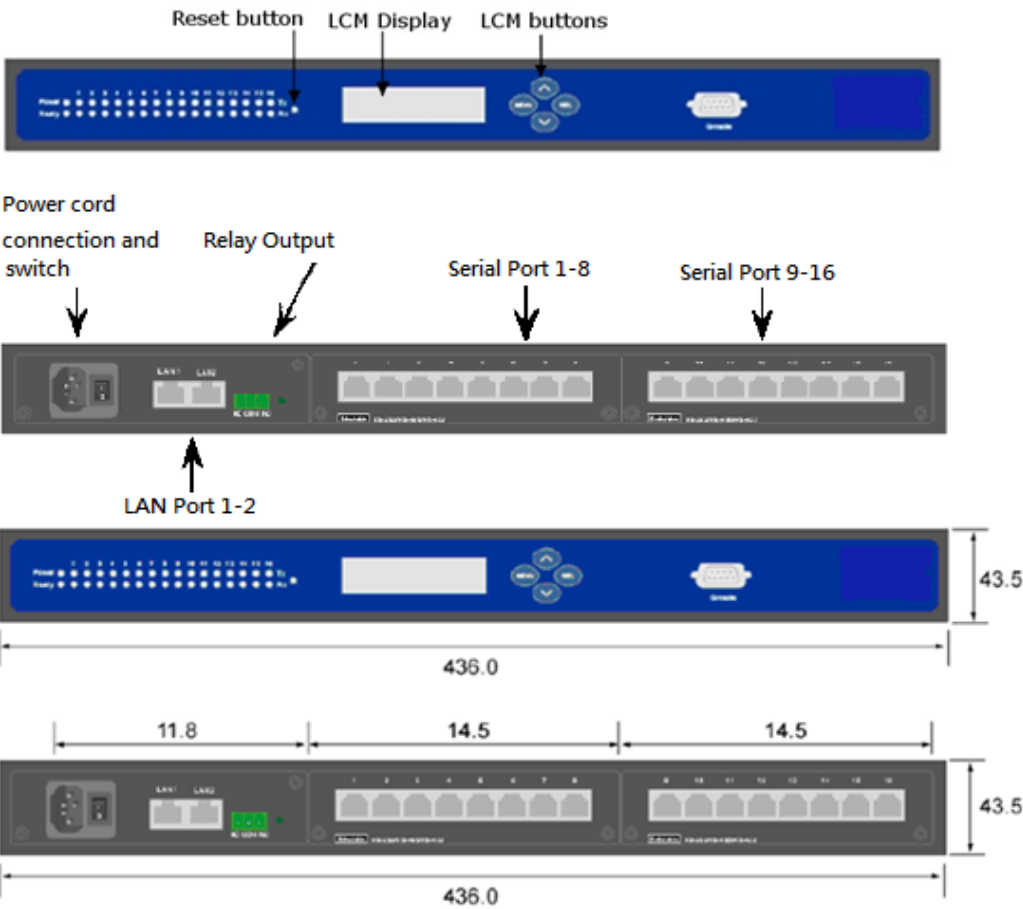
The following figures show particular SE59XX series device’s front and rear panels.



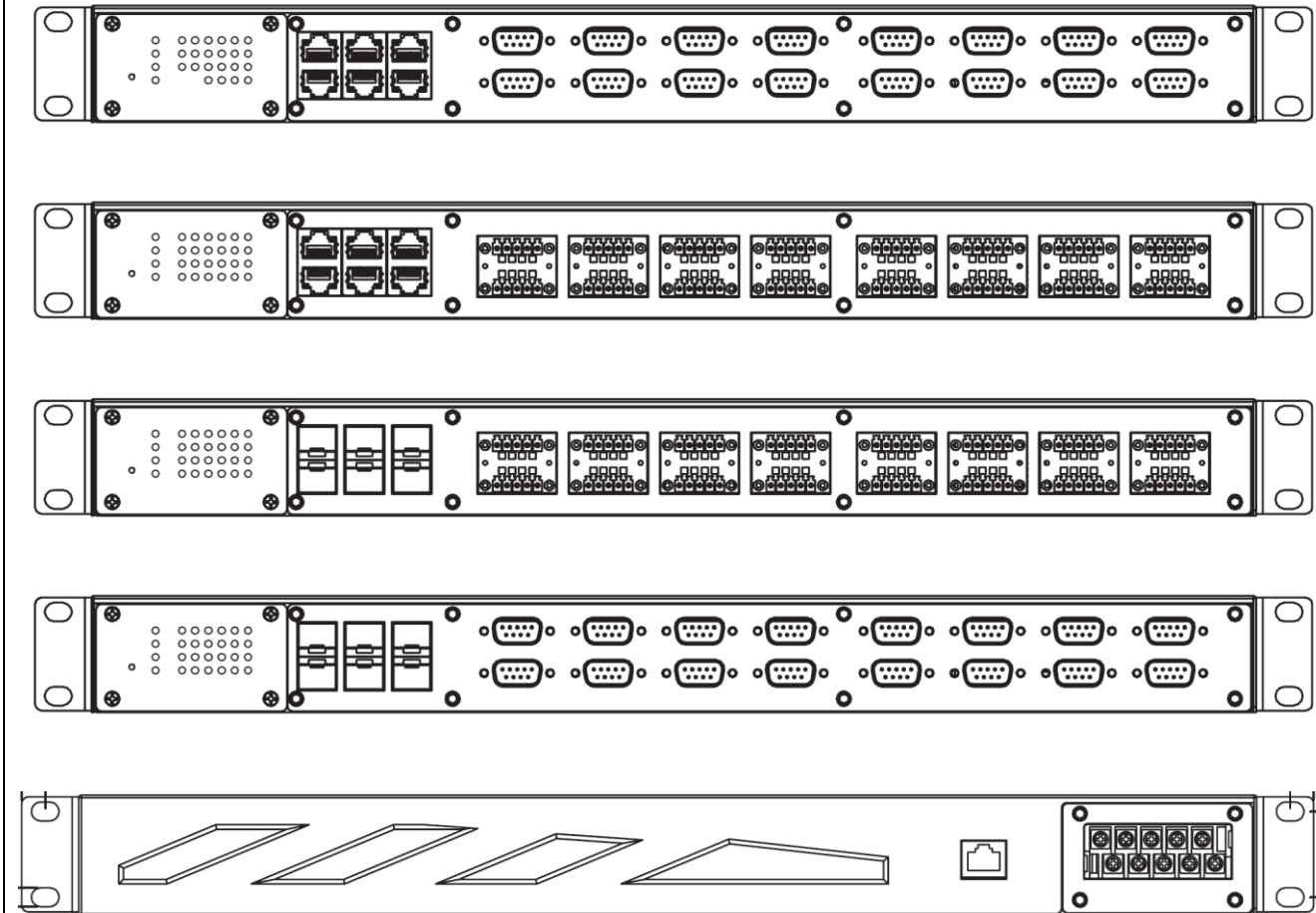
SE5901B



SE5908/16



SE5908A/16A



3.3 First Time Installation

Before installing the device, please follow strictly all safety procedures described in the Hardware installation guide supplied inside the product. Atop will not be liable for any damages to property or personal injuries resulting from the installation or overall use of the device. Do not attempt to manipulate the product in any way if unsure of the steps described there. In such cases, please contact your dealer immediately.

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

3.4 Factory Default Settings

3.4.1 Network Default Settings

The SE59XX Industrial Serial Device Server is equipped with two LAN interfaces with two default IP addresses. Its default network parameters are listed in Table 3.3.

Table 3.3 Network Default Setting

Interface	Device IP	Subnet Mask	Gateway IP	DNS
LAN1	10.0.50.100	255.255.0.0	10.0.0.254	255.255.255.255
LAN2	192.168.1.1	255.255.255.0	192.168.1.254	
LAN 3~6 SE5908A and SE5916A only	192.168.2.1~5.1	255.255.255.0	192.168.1.254	

3.4.2 Other Default Settings

The SE59XX Industrial Serial Device Server comes with the following default settings.

Table 3.4 Security , Serial, and SNMP Default Settings

Parameter	Default Values
Security	
User Name	admin
Password	default
Serial	
COM1	RS-232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM2	RS-232, 9600 bps, 8 data bits, No Parity bit, 1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM3	RS-232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
COM4	RS-232, 9600 bps, 8 data bits, No Parity bit,1 stop bit, No Flow Control Packet Delimiter timer: Auto
SNMP	
SysName of SNMP	System
SysLocation of SNMP	Location
SysContact of SNMP	Contact
SNMP	Disabled
Read Community	public
Write Community	private
SNMP Trap Server	0.0.0.0

Note: Press the “Reset” button on the front panel for 5 seconds or follow the procedure in Section 0, to restore the SE59XX Series Industrial Serial Device Server to the factory default settings.

4 Configuration and Setup

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

4.1 Configuration of Network Parameters through Device Management Utility

Please install Atop's configuration utility program called **Device Management Utility**® that comes with the Product CD or can be downloaded from our websites (www.atop.com.tw or www.atoponline.com). For more information on how to install **Device Management Utility**®, please refer to the manual that comes in the Product CD. After you start **Device Management Utility**®, if the SE59XX 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 SE59XX device and list it on **Device Management Utility**®'s window. Alternatively, if you did not see your SE59XX device on your network, press "Rescan" icon, a list of devices, including your SE59XX device currently connected to the network will be shown in the window of **Device Management Utility**® as shown in Figure 4.1.

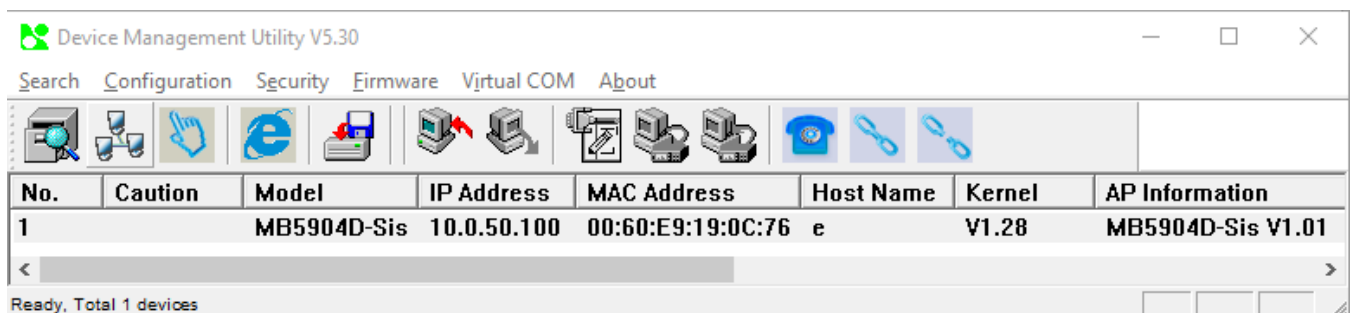


Figure 4.1 List of Device in Device Management Utility

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

Sometime the SE59XX device might not be in the same subnet as your PC; therefore, you will have to use Atop's utility to locate it in your virtual environment. To configure each device, first click to select the desired SE59XX device (default IP: 10.0.50.100) in the list of **Device Management Utility**®, and then click "Configuration → Network..." (or Ctrl+N) menu on **Device Management Utility**® as shown in Figure 4.2 or click on the second icon called **Network** on the menu icon bar, and a pop-up window will appear as shown in Figure 4.3.

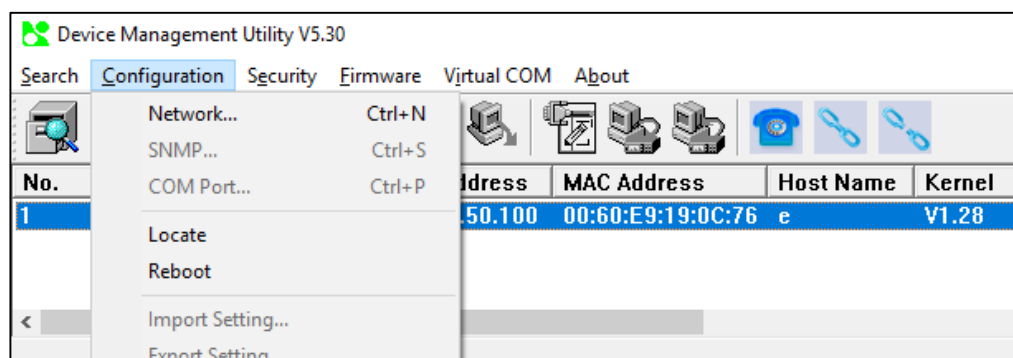
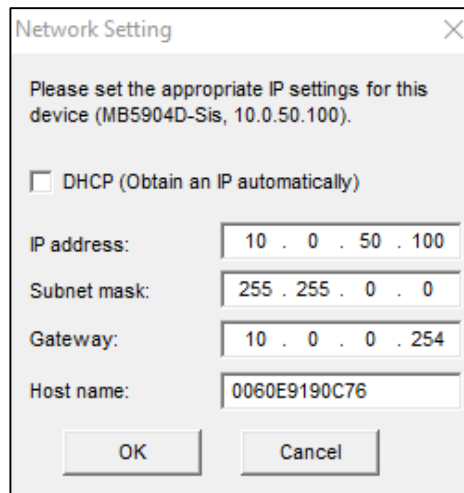


Figure 4.2 Pull-down Menu of Configuration and Network...



Network Setting

Please set the appropriate IP settings for this device (MB5904D-Sis, 10.0.50.100).

☐ DHCP (Obtain an IP automatically)

IP address: 10 . 0 . 50 . 100

Subnet mask: 255 . 255 . 0 . 0

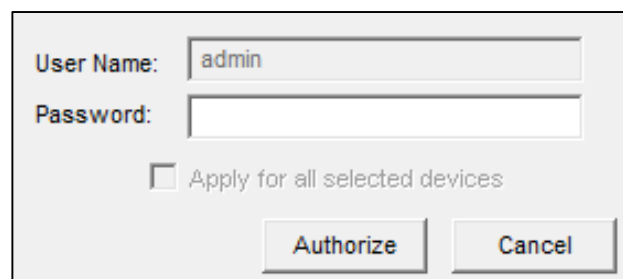
Gateway: 10 . 0 . 0 . 254

Host name: 0060E9190C76

OK Cancel

Figure 4.3 Pop-up Window of Network Setting

You may proceed then to change the IP address to avoid any IP address conflict with other hosts on your LAN or to connect the device to your existing LAN as shown in Figure 4.3. The system will prompt you for a credential to authorize the changes. It will ask you for the **Username** and the **Password** as shown in Figure 4.4. The default username is “**admin**”, while the default password is “**default**”. After clicking on the **Authorize** button, a notification window will pop-up as shown in Figure 4.5 and some device may be restarted. After the device is restarted (for some model), it will beep twice to indicate that the unit is running normally. Then, the SE59XX device can be found on a new IP address. It may be listed automatically by the **Device Management Utility**® or it can be found by clicking on the “**Rescan**” icon. Note that if you did not change the IP address but changed other parameter, you may encounter another notification window as shown in Figure 4.6.



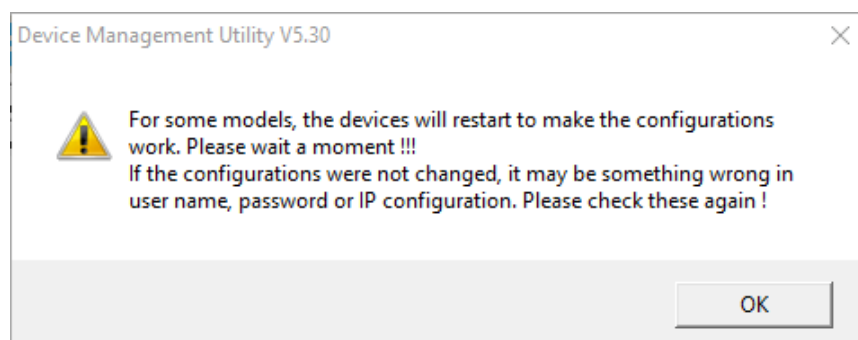
User Name: admin

Password:


☐ Apply for all selected devices

Authorize Cancel

Figure 4.4 Authorization for Change of Network Settings



Device Management Utility V5.30

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

OK

Figure 4.5 Pop-up Notification Window after Authorization

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

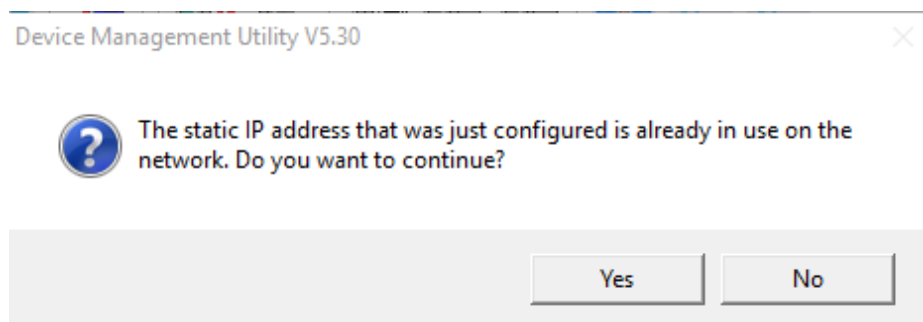
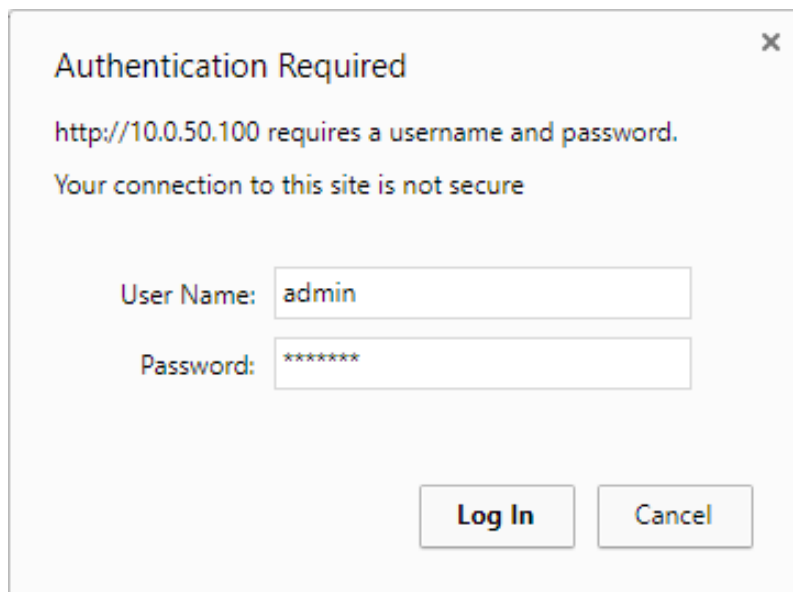


Figure 4.6 Pop-up Notification Window when there is the same IP address in the network

4.2 Configuring through Web/CLI Interface

Every SE59XX 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 4.7. Note that you may encounter a warning pop-up window that urges you to change or reset your password to be different from the default value as shown in Figure 4.8. Figure 4.9 illustrates the overview page of the web interface. Figure 4.10 lists all the menus and submenus for web configuration. Please see Section 3.4 for default values. Note that the figures are captured from SE59XX series but the overview page for SE59XX series are the same.

A screenshot of a web browser's authentication dialog box. The title bar says "Authentication Required" with a close button (X) in the top right corner. The main text reads: "http://10.0.50.100 requires a username and password." followed by "Your connection to this site is not secure". 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".

Authentication Required

http://10.0.50.100 requires a username and password.

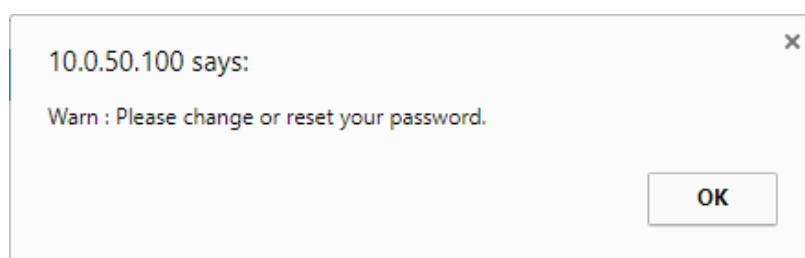
Your connection to this site is not secure

User Name: admin

Password: *****

Log In Cancel

Figure 4.7 Authentication Required for Accessing Web Interface

A screenshot of a warning pop-up window. The title bar says "10.0.50.100 says:" with a close button (X) in the top right corner. The main text reads: "Warn : Please change or reset your password." At the bottom right, there is an "OK" button.

10.0.50.100 says:

Warn : Please change or reset your password.

OK

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

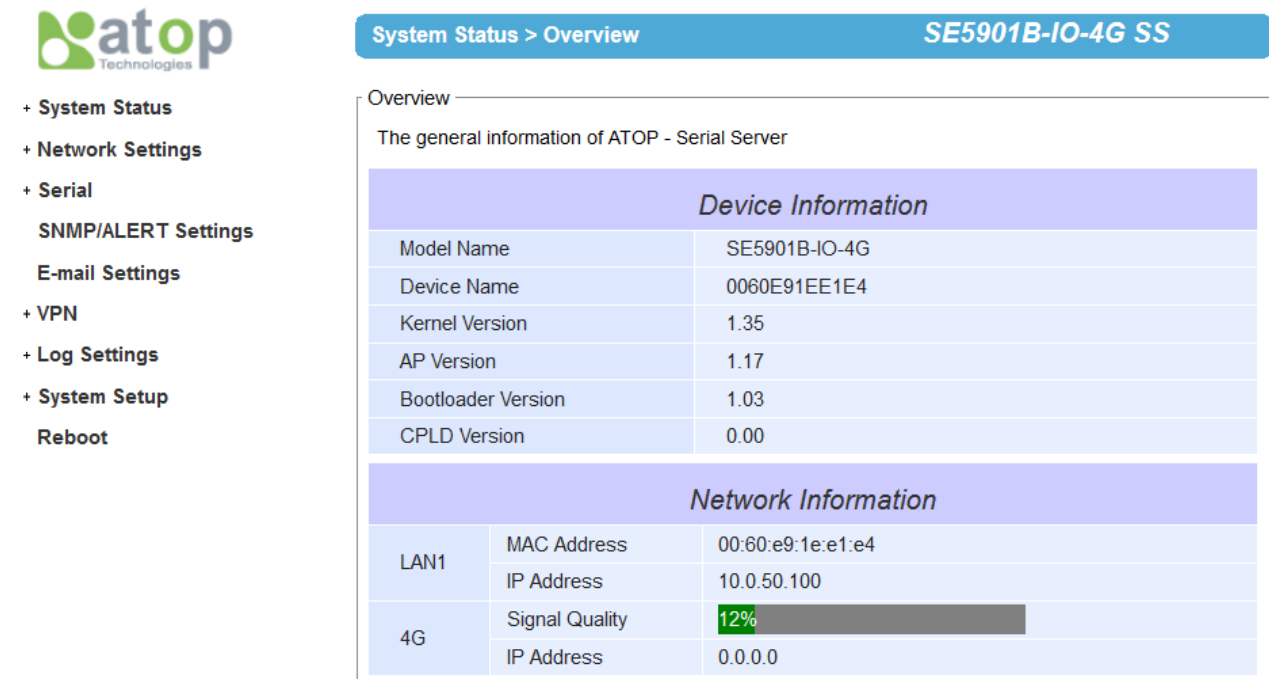


Figure 4.9 Overview Web Page of SE59XX Industrial Serial Device Server (example on SE5901B).

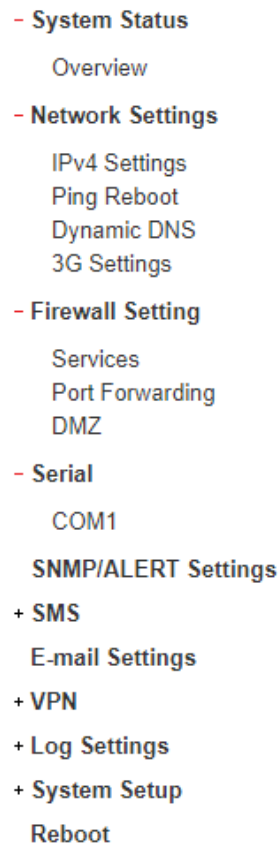


Figure 4.10 Map of Configuring Web Page on SE59XX Industrial Serial Device Server (ex. on SE5901B)

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 SE59XX Industrial Serial Device Server Series. Please go to its corresponding section for a detailed explanation.

Furthermore, you can also use CLI interface through Consol port/Telnet/SSH to configure SE59XX. Enable the Access Control (please refer to System Setup > Admin Settings), then you can use CLI interface.

Admin Settings

Set up the login user name and password.

Account Settings

User name	admin
Old password	
New password	
Repeat new password	

Web mode

Web Mode	<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 4.11 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 4.12 CLI interface

Please noted that change IP address need to restart SE59XX.

4.3 Configuring Automatic IP Assignment with DHCP

A DHCP server can automatically assign IP addresses, Subnet Mask and Network Gateway to LAN interface. You can simply check the “**DHCP (Obtain an IP Automatically)**” checkbox in the Network Setting dialog as shown in Figure 4.3 using Atop’s **Device Management Utility**® and then restart the device. Once restarted, the IP address will be configured automatically.

4.4 Web Overview

In this section, current information on the device’s status and settings will be displayed. An example of SE59XX’s overview page is shown in Figure 4.13. Note that the figures are captured from MB59XX series but the overview page for SE59XX series are the same.

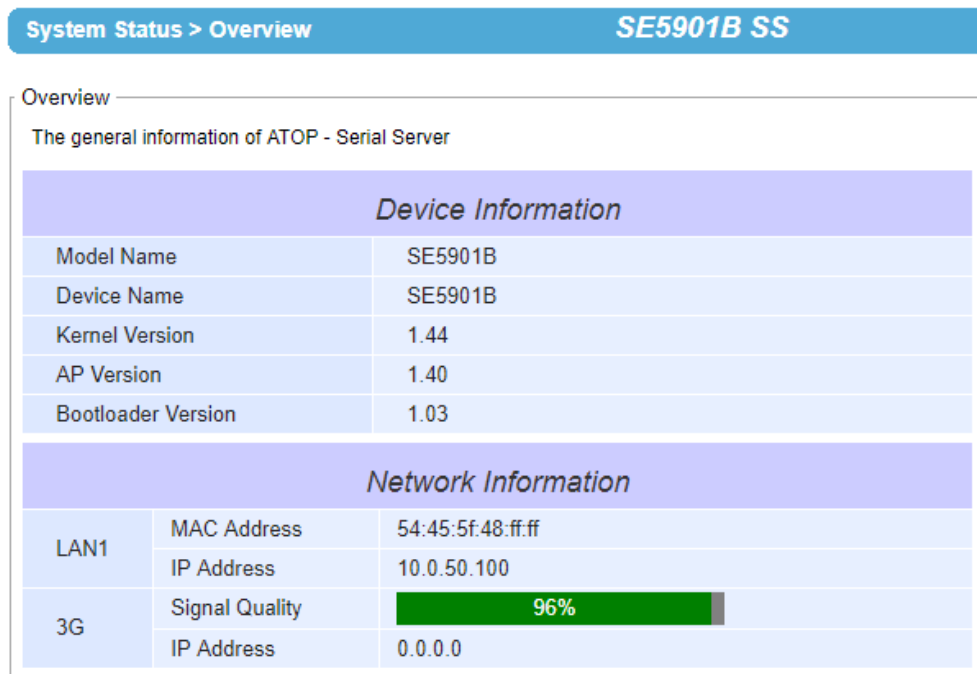


Figure 4.13 Overview Web Page (example on SE5901B)

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

- **Device Information**
 - **Model Name**, as its name implies, shows the device’s model
 - **Device Name** shows a given name of the device in which the default value is the MAC address of the LAN interface.
 - **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.

4.5 Network Settings

In this section, both network interfaces and related network settings of the SE59XX device can be configured. There are four sets of parameters which are **LAN1 Settings**, **LAN2 Settings**, **Default Gateway**, and **DNS Server** that can be entered as shown in Figure 4.14. First, **LAN1 Settings** part will allow you to configure the **IP Address**, **Subnet Mask**, and **Default Gateway** for your wired LAN1 network. You can check the box behind **DHCP** option to obtain an IP address automatically. If you checked the box, the rest of the options for **LAN1 Settings** will be greyed out or disabled. Second, **LAN2 Settings** is the same as LAN1 Settings but for the second Ethernet interface. Third, **Default Gateway** part is where you can select the default gateway network for your serial device server. You can either select **LAN1** or **LAN2** by clicking on the corresponding radio button. Fourth, **DNS Server** part is where you can specify the IP Address of your **Preferred DNS** (Domain Name Server) and **Alternate DNS**. If the SE59XX 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="0.0.0.0"/>
Alternate DNS	<input type="text" value="0.0.0.0"/>

Figure 4.14 Network Settings Web Page

For SE5901B, the **Network Settings** menu has four submenus which are **IPv4 Settings**, **Ping Reboot**, **Port Forwarding**, and **3G/4G Settings**. Figure 4.15 shows the menu and its submenus. Note that the **IPv4 Settings** web page for SE5901B is the same as the **Network Settings** web page described above.

- Network Settings

IPv4 Settings

Ping Reboot

Dynamic DNS

3G Settings

Figure 4.15 Network Settings Menu of SE5901B series

For SE5901B only, there is another set of parameters for **NAT Settings** that can be configured at the end of the **IPv4 Settings** Webpage (under **Network Settings** menu) as shown in Figure 4.16 and Figure 4.17. NAT is referred to Network Address Translation which is a technique that allows SE5901B to create a local IP network or subnetwork with private IP addresses that can connect to the Internet through a public IP address via its Wide Area Network (WAN) port. The SE5901B will map the private IP address and port of a local device connected to its local interface to a public port on its public interface (WAN port). To enable **NAT** function on SE5901B, check on the **Enable** box behind **NAT** option under **NAT Settings** part as shown in Figure 4.16.

Network Settings > IPv4 Settings **SE5901B SS**

Network Settings

LAN1 Settings

DHCP	<input type="checkbox"/> Enable
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"/>

DNS Server

Preferred DNS	<input type="text" value="0.0.0.0"/>
Alternate DNS	<input type="text" value="0.0.0.0"/>

NAT Settings

NAT	<input type="checkbox"/> Enable
-----	---------------------------------

Figure 4.16 NAT Settings under IPv4 Settings Web Page for SE5901B

When **NAT** function is enabled on SE5901B, additional set of parameters which is **DHCP Server** field will appear as shown in Figure 4.17. The **DHCP Server** or Dynamic Host Configuration Protocol Server is another function on SE5901B under the **NAT Settings**. This will allow SE5901B to automatically assign IP address for its local network. If the **DHCP Server** option is enabled (by checking the **Enable** box behind **DHCP Server** option), **IP Pool Start Address** and **IP Pool End Address** fields will appear under it. The IP Pool Addresses are the range of addresses that **DHCP Server** will be used to configure local IP addresses. The user can enter the starting and ending addresses inside these two fields. The **DHCP** Server function inside SE5901B can only support one LAN port and provide that port with IP address in the given range (from **IP Pool Start Address** to **IP Pool End Address**). Note that the range must be in NAT LAN port's network segment.

DNS Server	
Preferred DNS	<input type="text" value="0.0.0.0"/>
Alternate DNS	<input type="text" value="0.0.0.0"/>
NAT Settings	
NAT	<input checked="" type="checkbox"/> Enable
DHCP Server	<input checked="" type="checkbox"/> Enable
IP Pool Start Address	<input type="text"/>
IP Pool End Address	<input type="text"/>
DHCP Connected Clients	<input type="button" value="Show"/>

Figure 4.17 Enabling of NAT Settings with Additional Parameters for SE5901B

Finally, the last field in Figure 4.17 is the **DHCP Connected Clients** which has a **Show** button that allows the user to see a list of currently connected DHCP Clients and their related IP addresses. When the **Show** button is clicked a pop-up window will show up with a table where each record contains Number, Client MAC Address, Client IP address, and Client name (if there is any). An example of empty record is shown in Figure 4.18. Note that at the two green arrows that form a circle is a **Refresh** button that can check the latest list of DHCP connected clients when the user clicked on the arrows.

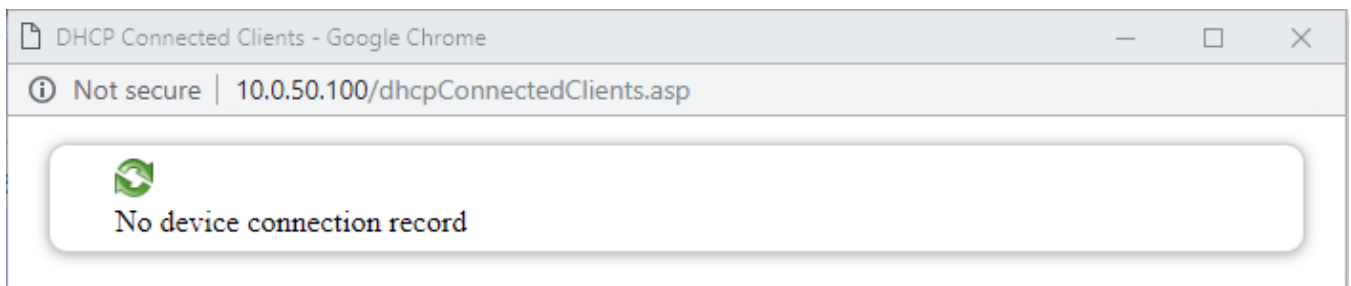


Figure 4.18 A pop-up window shows an empty list of DHCP Connected Clients.

After finishing the network settings (or IPv4 settings) configuration, please click the **Save & Apply** button to save all changes that have been made. Finally, the web browser will be redirected to the **Overview** page as shown in Figure 4.13. If you would like to discard any setting, please click the **Cancel** button.

4.5.1 Ping Reboot

To guarantee the quality of 3G/4G communication, the user could enable the **Ping Reboot** function under the **Network Settings** menu. The device will send packets periodically to specified destination (**Host To Ping**) via PING protocol. Once SE5901B detected that there was no response from the specified destination, it will initialize or reboot the 3G/4G module. Figure 4.19 shows the Ping Reboot web page and its parameters.

Network Settings > Ping Reboot SE5901B SS

Ping Reboot

The Ping Reboot function periodically sends Ping commands to a specified IP address and wait for received responses. If no response is received after the defined number of unsuccessful retries, the device will restart the 4G service.

Ping Reboot	
Ping Reboot	<input type="checkbox"/> Enable
Interval Between Pings	3 Minute
Ping Timeout	5 seconds(1~999, default=5)
Packet Size	56 bytes(1~999, default=56)
Retry Count	2 (1~999, default=2)
Host To Ping	

Figure 4.19 Ping Reboot Web Page under Network Settings

Table 4.1 Descriptions of Ping Reboot's Parameters

Field Name	Description	Factory Default
Ping Reboot	Check the Enable box to active the Ping Reboot function.	Uncheck
Interval Between Pings	The period that SE59XX will send out the Ping packet.	3 minutes
Ping Timeout	The timeout when ther is no response from a destination host.	5 seconds
Packet size	The payload size of ICMP (Internet Control Message Protocol) used by Ping. You need to confirm that the destination host could accept the packet size that you defined.	56 Bytes
Retry Count	The number of retries if there is no response from a destination host.	2 times
Host to Ping	The specific destination that SE59XX will send Ping packet to.	NULL

4.5.2 Dynamic DNS

Atop's SE5901B series support eight well-known Dynamic Domain Name System (DDNS) servers such as noip.com and mydns. Please refer to official DDNS provider's website of your choice to register the domain name. Figure 4.20 illustrates the operations of Dynamic DNS Server in which two hosts (203.0.113.6 and 203.0.113.2) registered or informed their IP addresses with a Dynamic DNS provider (DDNS server). Other clients that would like connect to the two hosts with fixed host (domain) names can inquire the DDNS server for the actual IP addresses. This service is useful when the two hosts do not have fixed IP addresses. This is usually the case when the host is using a dial-up service or 3G/4G interface which is often given different IP address when it is reconnected with the network.

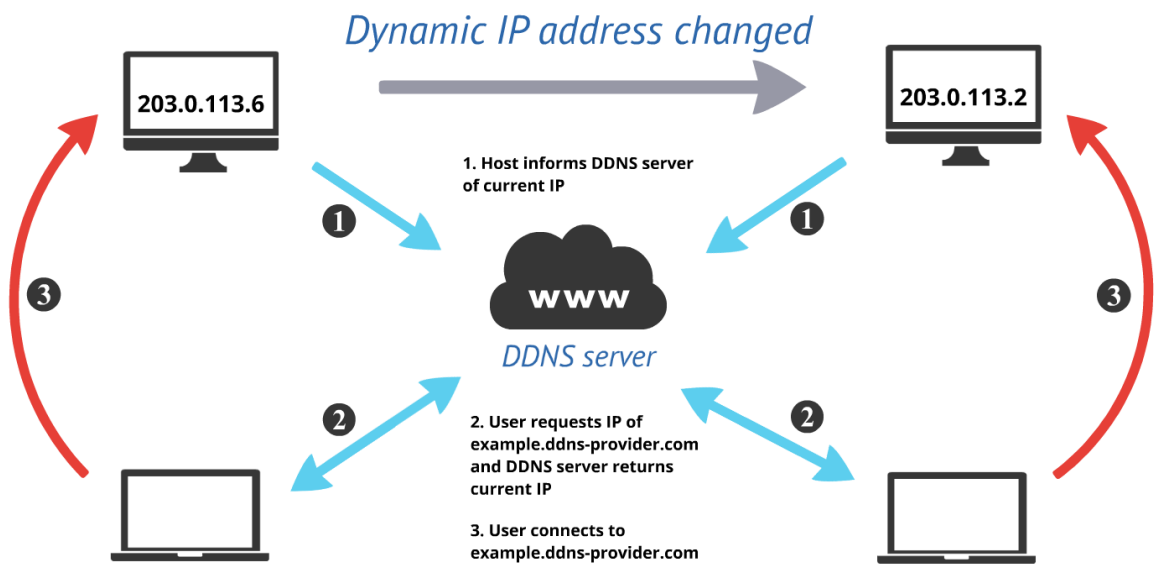


Figure 4.20 Example of Dynamic DNS Server Operations

To configure the Dynamic DNS on the SE5901B, first click on the **Dynamic DNS** submenu under the **Network Settings**. Then, check the **Enable** box behind the **DDNS** option. Next, select a DDNS provider from the pull-down list of **Service** option. Then, fill in the **Hostname**, **Username**, and **Password** that you already registered with the DDNS service provider. Next choose a mode of **IP Source** from the pull-down list which can be one of the followings: **Public**, **Private**, or **Custom**. Finally, you can specify the **IP Renew Interval (min)** and **Force IP Renew Interval (min)**. Table 4.2 summarizes the descriptions of Dynamic DNS's parameters and options.

Network Settings > Dynamic DNSSE5901B SS

Dynamic DNS Settings

Dynamic DNS allows you to reach your device using a fixed hostname while having a dynamically changing IP address.

Dynamic DNS	
DDNS	<input checked="" type="checkbox"/> Enable
Status	N/A
Service	noip.com
Hostname	
Username	
Password	
IP Source	Public
IP Renew Interval (min)	10 (5~600000, default=10)
Force IP Renew Interval (min)	472 (5~600000, default=472)

Save & ApplyCancel

Figure 4.21 Dynamic DNS Web Page

Table 4.2 Descriptions of Dynamic DNS Web Page's parameters

Field Name	Description	Factory Default
DDNS	Check the Enable box to active the DDNS function	Uncheck
Status	Show the DDNS update status.	N/A
Service	Select a DDNS server provider from the pull-down list.	No-IP.com
Hostname	Enter the domain name that you already registered with the specific DDNS server provider.	NULL
Username	Enter the user account that you already registered with the DDNS server provider.	NULL
Password	Enter the password that you already registered with the DDNS server provider.	NULL
IP Source	Select which IP address (Public, Private or customized) from the pull-down list to be register to DDNS server.	Public IP
Network Interface	When choosing the custom mode in IP source, you can choose which network interface that you want to use for DDNS.	4G
IP Renew Interval (min)	The interval that SE59XX will check whether the IP source is changed or not. If IP address is changed, SE59XX will update it to the specific DDNS server.	10 mins
Force IP renew Interval	The interval that SE59XX will update the IP address to the specific DDNS server. The is performed no matter that the IP address is changed or not.	472 mins

4.6 Firewall Setting

Atop's SE5901B Industrial Device Server provides firewall features to improve security for your network. You can configure the firewall mechanisms under the Firewall Setting menu. Figure 4.22 shows the submenus under the Firewall Setting which are Services, Port Forwarding, and Demilitarized Zone (DMZ).

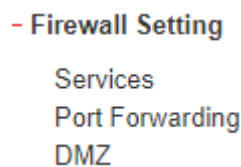


Figure 4.22 Firewall Setting Menu of SE5901B

4.6.1 Services

One of the firewall features is to filter network traffic based on protocols, source addresses, and port numbers. Under the **Services** web page shown in Figure 4.23, you can configure the filtering for different network services. The first part of the **Services** page is the **Services Mode** and the second part is the **Service List**. By default, the SE5901B is set in **Deny** service mode in which all services on the device are blocked by the firewall. To allow a number of service types through the firewall, you can enable the filtering by selecting the **Allow** service mode. Next, you can configure each allowed service in the Service List. Note that up to 16 entries can be set in the Service List.

Under the **Service List**, there are four columns which are **Alias**, **Protocol**, **Source Address**, and **Port**. The first three entries on the list are provided as examples for Ping, http, and https services. To enable each entry, you can check the box in front of that entry. Then, you can enter the short name or **Alias** for each entry to provide hint on the

service that you allow. This name usually is the protocol service at the application layer. Next, you can select the transport protocol from the drop-down list under the **Protocol** column. The choices for the transport protocols are TCP, UDP, TCP/UDP, and ICMP. Then, you can enter the IP address and the **Port** number of the Source or the host that will send the traffic to this SE5901B. Table 4.3 summarizes the description of each field on the Services web page.

After finish configuring the **Service List**, please click on the **Save & Apply** button to save all changes and enable your setting. Otherwise, click on the **Cancel** button to discard your setting.

Firewall Setting > Services

SE5901B SS

Service Type Filtering

This is a list of TCP and UDP port numbers used by protocols of the application layer of the Internet protocol suite for the establishment of client-to-host connectivity.

Services Mode

☒ Deny all services on the device

☐ Allow following services on the device

Services List

Alias	Protocol	Source Address	Port
<input type="checkbox"/> allow-ping	ICMP		
<input type="checkbox"/> http	TCP		80
<input type="checkbox"/> https	TCP		443
<input type="checkbox"/>	TCP		
<input type="checkbox"/>	TCP		
<input type="checkbox"/>	TCP		
<input type="checkbox"/>	TCP		
<input type="checkbox"/>	TCP		
<input type="checkbox"/>	TCP		
<input type="checkbox"/>	TCP		

◀ Previous

Next ▶

Page 1/2

Save & Apply

Cancel

Figure 4.23 Services Page under Firewall Setting Menu

Table 4.3 Descriptions of Parameters for Services under Firewall Setting

Field Name	Description	Factory Default
Service Mode	Deny all services or Allow specified services for the SE59XX.	Deny
Alias	Check the box in front of the entry and enter the alias name for the filtering rule.	Null
Protocol	Select the protocol used by the service from the list: TCP, UDP, TCP/UDP, or ICMP	TCP

Source Address	Enter the IP address to allow it to access the SE59XX service. Noted that you can enter one the followings: 1) IP address: only this unique IP address can access SE59XX's service. 2) IP with subnet mask: only this subnet mask can access SE59XX's service. 3) Leave the field empty: all IP addresses could access SE59XX's service.	Null
Port	Port number of TCP/UDP protocol	Null

4.6.2 Port Forwarding

Port forwarding is an application of Network Address Translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway. Figure 4.24 depicts an example of port forwarding through a SE5901B device. In this example, a host or device behind the SE5901B (on the left of the figure) has a private IP address of 192.168.5.1 with port number 80. This is a http service that can be accessed through a public IP (on the SE59XX device) with IP address of 220.120.49.91 with port number 8080. This public IP address can be reached by a SCADA control center over the Internet. In other words, the SCADA system could access the IP address of SE5901B with specified port and the SE5901B will forward the packet from the SCADA system to the host on the LAN port of SE5901B with specified port.

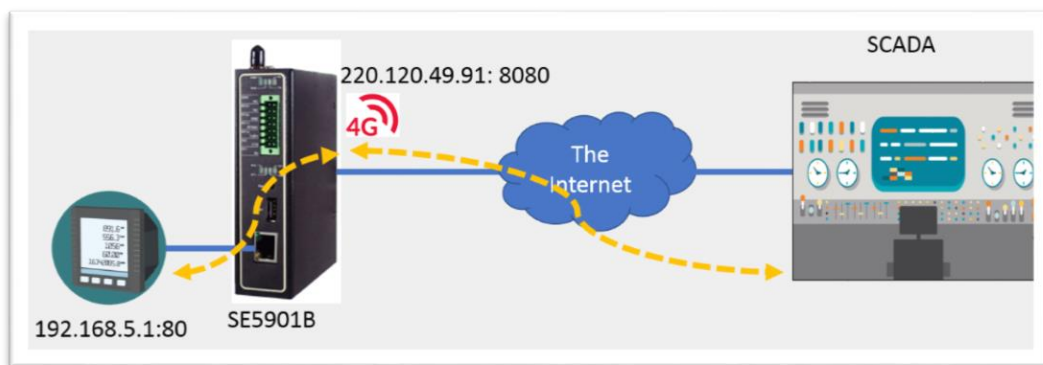


Figure 4.24 Example of Port Forwarding through SE5901B Industrial Device Server

For SE5901B only, when the user clicked on the **Port Forwarding** menu, the **Port Forwarding** web page will be displayed as shown in Figure 4.25. This port forwarding feature allows the user to configure port forwarding from WAN to LAN. This feature can redirect specific packets from a remote host on the WAN to a server on the LAN. It hides the IP address of a local server and prevents remote hosts from accessing the local server directly. This feature can also filter out unrecognized packets to protect your LAN network when computers connected to SE5901B are not visible to the WAN. Note that this feature is the result of **NAT Settings** described above. The user can configure port forwarding up to 32 entries. For each entry, the user can set an **Alias** (short name), allowable transport protocol(s) (**TCP/UDP**), source IP address (**Src IP**), source start port (**Src Start Port**), source end port (**Src End Port**), destination IP address (**Dst IP**), destination start port (**Dst Start Port**), and destination end port (**Dst End Port**). Describes each field in the Port Forwarding table. Table 4.4 Description of Fields in Port Forwarding Table

Table 4.4 summarizes the description of each column of the Port Forwarding table.

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

Network Settings > Port Forwarding

SE5901B SS

Port Forwarding

Device Information									
Active	No.	Alias	TCP/UDP	Src IP	Src Start Port	Src End Port	Dst IP	Dst Start Port	Dst End Port
<input type="checkbox"/>	1	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	2	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	3	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	4	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	5	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	6	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	7	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	8	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	9	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	10	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	11	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	12	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	13	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	14	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	15	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	16	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	17	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	18	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	19	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	20	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	21	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	22	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	23	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	24	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	25	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	26	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	27	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	28	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	29	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	30	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	31	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024
<input type="checkbox"/>	32	na	BOTH ▼	0.0.0.0	1024	1024	0.0.0.0	2024	2024

Save & Apply Cancel

Figure 4.25 Port Forwarding Web Page of SE5901B series

Table 4.4 Description of Fields in Port Forwarding Table

Field Name	Description	Factory Default
Active	This radio button allows individually enabling or disabling each entry of the port forwarding configuration.	Disable
No.	This is the number of the row on the table which are from 1 up to 32.	-
Alias	This is a fillable textbox that allows to configure a short and easy-to-remember name for each port forwarding entry.	na (Null)
TCP/UDP	This is the transport protocol that can be allowed on this port forwarding entry. The available options are TCP, UDP, or BOTH.	BOTH
Src IP	IPv4 address of the source (on WAN) which will be redirected through SE59XX.	0.0.0.0

Field Name	Description	Factory Default
Src Start Port	The starting port number of the source which can be between 0 to 65535.	1024
Src End Port	The ending port number of source which can be between 0 to 65535.	1024
Dst IP	IPv4 address of the destination (on LAN) which is the translated destination IP address	0.0.0.0
Dst Start Port	The starting port number of the destination which can be between 0 to 65535.	2024
Dst End Port	The ending port number of the destination which can be between 0 to 65535.	2024

4.6.3 DMZ

DMZ or demilitarized zone is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks, usually the Internet. External-facing servers, resources, and services are often placed in the DMZ. So that, they are accessible from the internet, but the rest of the internal LAN remains unreachable and safe. This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the Internet.

Atop's SE5901B provides the **DMZ** configuration under the **Firewall Setting** as shown in Figure 4.26. By default, the DMZ feature is disabled. You can enable the DMZ by selecting the **Yes** radio button. Then, you can enter the IP Address of the Exposed Station in the following field. This is the translated destination IP address which will be mapped or the public IP address on the 3G/4G interface. Table 4.5 summarizes the options under the DMZ web page.

Note: Be caution when using the DMZ function. Once you enabled this function, all the packet will be forwarded to the translated destination IP addresss (which is the host on the LAN port). That means you can no longer access the SE5901B via 4G interface over the Internet.

Firewall Setting > DMZ

SE5901B SS

DMZ Settings

In computer security, a DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.

DMZ

Enable DMZ

☐ Yes ☒ No

IP Address of Exposed Station

Save & Apply

Cancel

Figure 4.26 DMZ Page under Firewall Setting Menu

Table 4.5 Description of DMZ's Options

Field Name	Description	Factory Default
Enable DMZ	Enable or disable DMZ feature	Disable (No)
IP Address of Exposed Station	The translated destination IP address	Null

4.7 *Serial*

Since SE59XX is an Industrial Serial Device Server, it supports serial communication with COM port(s). Note that SE59XX series can have up to four COM ports: **COM1**, **COM2**, **COM3**, and **COM4**, while typical SE5901 model will have only one COM port (**COM1**).

Figure 4.27 shows the **Serial** menu on the left frame of the web interface of SE59XX. The following subsections will describe how to configure these COM ports.

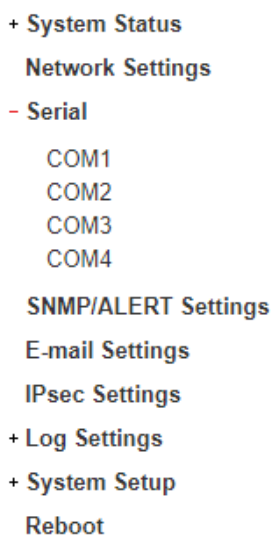


Figure 4.27 Serial Menu (example on SE5904D)

4.7.1 COM Port Overview

Since details on **Link Mode** connectivity protocols and its settings of SE59XX series are given in Chapter 5 Link Modes and Applications, this section will only focus on the **Serial Settings** only. Figure 4.28 shows an example of the **COM 1 Port Settings** where the upper part is dedicated for **Link Mode** settings and the lower part is dedicated for **Serial Settings**. Note that similar settings web page is applicable for COM 2/COM 3/COM 4 Port Settings on SE59XX 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 4.28 COM 1 Port Settings Web Page

4.7.2 COM Configuration

Figure 4.29 excerpts the **Serial Settings** part of **COM** port settings of SE59XX. Note that these settings need to match the parameters on the serial port of the serial device. Each option is described as follows.

To configure COM 1 port parameters.

Serial Settings	
Serial Interface	<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 4.29 Serial Settings Part of COM 1 Port

- **Serial Interface:** This option allows selection between **RS-232**, **RS-422**, **RS-485**, and **RS-485 (4-Wire)** standards. **Note:**
 - RS-485 refers to 2-Wire RS-485 and RS-422 is compatible with 4-Wire RS-485.
 - SE5901B and MB5901B models do not support RS-422 and RS-485 (4-Wire). Figure 4.30 illustrates an example of Serial Settings of COM 1 port for SE5901B model that only support RS-232 and RS-485.
- **Baud Rate:** The user can select one of the baud rates (from 1200 to 921600 bps) from the drop-down list.
- **Parity:** The available Parity options are **None**, **Odd**, **Even**, **Mark**, or **Space**.
- **Data Bits:** The setting for Data Bits can be **5 bits**, **6 bits**, **7 bits**, or **8 bits**.
- **Stop Bits:** The number of Stop Bits can be either **1 bit** or **2 bits**.
- **Flow Control:** The user can choose among **None** (No Flow Control), **RTS/CTS** (Hardware Flow Control), or **Xon/Xoff** (Software Flow Control). If Xon/Xoff is selected, the Xon and Xoff characters are changeable. Defaults are 0x11 for Xon and 0x13 for Xoff. Note that these are hexadecimal number of ASCII characters (i.e., 0x11 = '1' and 0x13 = '3').

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

Serial > COM1

SE5901B

COM 1 Port Settings

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

To configure COM 1 port parameters.

Serial Settings

Serial Interface	<input checked="" type="radio"/> RS232 <input type="radio"/> RS485
Baud Rate	115200 ▾ 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 4.30 Serial Settings for COM 1 of SE5901B (Note that it supports only RS-232 and RS-485)

4.7.3 COM Configuration: Advanced Settings

For advanced details of COM port setting, you can click on **Advanced Settings** button at the end of **Serial Settings** page which will open another web browser window as shown in Figure 4.31 below. 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
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 4.31 COM 1 Advanced Settings Web Page

TCP

- **TCP timeout:** By clicking the **Enable** box of **TCP Timeout** and input value in seconds between 0 and 60000, SE59XX will check if there's any data from serial port. If time expired, SE59XX will disconnect to its peer.
- **TCP Keep-alive:** By clicking the **Enable** box of **TCP Keep-alive** and input value in seconds, SE59XX will check if its peer is still alive. Noted that it will retry 3 times and timeout is 5 seconds in default.

Delimiters

- **Serial to Network Packet Delimiter:** Packet delimiter is a way of packing data in the serial communication. It is designed to keep packets intact. SE59XX 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, SE59XX would transmit the serial data in its buffer over the network.
 - ◆ **Interval timeout:** SE59XX will transmit the serial data in its buffer when the specified time interval has reached and no more serial data comes in. The default value is calculated automatically based on the baud rate which is the **Auto (calculate by baudrate)** option. If the automatic value results in chopped data, the timeout could be increased manually by switching to "**Manual setting**" (checking the radio button in Figure 4.31) and specifying a larger value in the text box above. Note that the maximum interval is 30,000 milliseconds.

**Attention****Manual Calculation of Interval Timeout**

The optimal “Interval timeout” depends on the application, but it must be at least larger than one-character interval within the specified baud rate. For example, assuming that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits (included 1 start bit), and the time required to transfer one character is $(10 \text{ (bits)}/1200 \text{ (bits/s)}) \times 1000 \text{ (ms/s)} = 8.3 \text{ ms}$. 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:** SE59XX will transmit the serial data in its buffer when the specified length in the unit of bytes has reached. The range of maximum bytes is between 1 to 1452 bytes. Enabling this option by checking the box in front of **Max. Bytes**, if you would like SE59XX to queue the data until it reaches a specific length. This option is disabled by default.
- ◆ **Character:** SE59XX will transmit the serial data in its buffer when it sees the incoming data that includes the specified character (in hexadecimal (HEX) format). This field allows one or two characters. If character delimiter is set to 0x0d, SE59XX 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. SE59XX will store data from the network interface in its queue. Until one of the delimiter conditions described above is met then SE59XX 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), SE59XX would split the data in the queue and only transmit one character (a byte) every 1 second. The maximum value for this option is 1000 milliseconds or 1 second. This option is disabled by default.
- **Response Interval Timeout:** This option only affects the **Request & Response Mode** and has no effect on the **Transparent Mode**. Please see the discussion about **Request & Respond Mode** versus **Transparent Mode** in Chapter 5, Section 5.1.1. When TCP data is received (a request from network) and passed to serial device side, the SE59XX 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, SE59XX has its First-In-First-Out (FIFO) function enabled to optimize its serial performance. In some applications (particularly when the flow control mechanism is enabled), it may deem necessary to disable the FIFO function to minimize the amount of data that is transmitted through the serial interface after a flow off event is triggered to reduce the possibility of overloading the buffer inside the serial device. Please note that disabling this option on baud rates higher than 115200bps would noticeably reduce the data integrity.
- **Serial Buffer:** By default, SE59XX will empty its serial buffer when a new TCP connection is established. This means that the TCP application will not receive buffered serial data during a TCP link breakage. To keep the serial data when there is no TCP connection and send out the buffered serial data immediately after a TCP connection is established, you can disable this option.

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

4.8 VPN

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

See below VPN scenario of SE/PG/MB59XX for your reference.

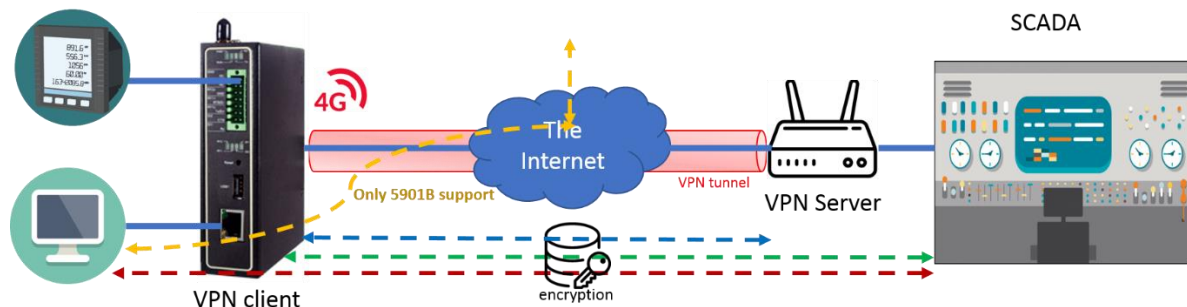


Figure 4.32 VPN Scenario of SE/PG/MB59XX

SE59XX supports several VPN protocols: PPTP (Point-to-Point-Tunneling-Protocol), IPsec (Internet Protocol Security), and OpenVPN. In order to configure VPN, please click on the related item in the dedicated VPN sub-menu on the left-hand side of the screen, as shown in Figure 4.33 below.

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

A better description of OpenVPN is available in Chapter 4.10 below.

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

- VPN

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

Figure 4.33 VPN menu structure

4.9 PPTP Settings

PPTP (Point-to-Point Tunneling Protocol) is a method for implementing virtual private networks. PPTP uses a TCP control channel and a GRE tunnel to encapsulate PPP packets. Select the PPTP item in the menu to configure a PPTP tunnel. Figure 4.34 shows the PPTP configuration page under PPTP web setting. Currently SE59xx series only supports PPTP client. After settings are completed, click “**Save**” to save the configuration.

PPTP Client Settings	
Enable PPTP Client	<input checked="" type="checkbox"/>
Always On	<input type="checkbox"/>
PPP Authentication	Only PAP
PPP Encryption	Disable
Remote IP Address	192.168.4.244
User Name	papuser
Password	*****

Save Cancel

Figure 4.34 PPTP configuration page.

- Enable PPTP client: Check this to enable the PPTP client on SE59XX series.
- Always on: Check this to have SE59xx to automatically reconnect in event of disconnection.
- PPP Authentication: Specify the authentication algorithm – should be same as server
- PPP Encryption: Specify the encryption – should be same as server
- Remote IP address: Specify the IP address of PPTP server.
- User Name: Specify the User name for authentication.
- Password: Specify Password for authentication.

Figure 4.35 below shows the PPTP Link status.

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

Connect Disconnect Refresh

Figure 4.35 PPTP Link Status

- Local Virtual IP Address: The virtual IP address assigned by PPTP server.
- Remote Virtual IP Address: The virtual IP address of PPTP server.
- Status: It shows the PPTP tunnel connection status. It will show Disconnect, Connect and Connecting.
- Disconnect: No tunnel is established.
- Connect: PPTP Tunnel is established.

- Connecting: PPTP Tunnel is establishing.
- Connect: Click this button to connect to PPTP server.
- Disconnect: Click this button to disconnect PPTP tunnel.
- Refresh: Click this button to refresh the PPTP tunnel status.

4.10 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 SE59xx series only support TUN mode.

4.10.1 OpenVPN Setting

In order to configure OpenVPN, click on the VPN tab in the left hand side of the menu and then **OpenVPN Settings**. The user interface is shown in below Figure 4.36.

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

Save Cancel

Figure 4.36 OpenVPN Setting

The OpenVPN parameters are described as below:

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

- **Device Type:** OpenVPN tunnel connection by TUN (Tunnel) mode or TAP mode. Currently SE59xx series only supports TUN (Tunnel) mode.
- **Virtual IP** (only when “OpenVPN Server” mode is selected): Specify the server’s virtual IP. Virtual IP will only be available when SSL/TLS is chosen as the Authentication Mode. The Server’s virtual IP address will be 10.8.0.1/24 and client virtual IP address will be 10.8.0.x/24.
- **Local/Remote endpoint IP** (only when “OpenVPN Client” mode is selected): Specifies the local and remote endpoint virtual IP address of this OpenVPN gateway. Local/Remote endpoint IP only be available when static key is chosen in Authentication Mode.
- **Authentication Mode:** Specify the authorization mode the OpenVPN server. There are 2 options available:
 - SSL/TLS: OpenVPN will use TLS authorization mode, and the following items CA cert, Server Cert and DH PEM will be used. See section 4.10.2 below for mode details.
 - Static Key: OpenVPN will use static key authorization, and the static key will be used. See section 4.10.2 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:** Specify the Hash algorithm. There are 5 options available: SHA1, MD5, SHA 256, SHA 512 and Disable. When Disable is selected, no Hash algorithm will be used.
- **Compression:** Specify whether or not the tunnel packets will be compressed. There are three options available: LZ4, LZ0 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, SE59xx will push the LAN port subnet to the OpenVPN remote clients, so that the remote client will add a route to the SE59XX local network. Only SE5901B supports this function.

4.10.2 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 KeysSE5901B SS

Current Key Information

Certificate Authority	<pre>-----BEGIN CERTIFICATE----- MIIEEnjCCA4agAwIwAgJAIq9J0+6i1d+MA0GCSqGSIb3 DQEBEwUAMIGQMqswCQYD VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAdD gYDVQQHEwdlc2luY2h1MQ0wCwYD -----</pre>
Server Certificate	<pre>7VawGz8gJOyJSDaWg34 WP/vPfbXHjJRRORibUvmkNgxAC/oU2uEAxsH2fGCQO p84ThP -----END CERTIFICATE-----</pre>
Server Key	<pre>-----BEGIN PRIVATE KEY----- MIIEwAIBADANBgkqhkiG9w0BAQEFAASCBAKowggSm AgEAAoIBAQPcuHrDjtiH1lz OZ44oS4BiichNGzM6NC9Cri1YzRxesVSXq46xeR+kMH jJAUloM4rABSnp2bsw/EI -----</pre>
Diffie Hellman parameters	<pre>-----BEGIN DH PARAMETERS----- MIIBCAKCAQEA0eaxNXkcjHOfCXp/tVAIkQTPHeDDv+ GPd+Lg9KNjUgG3orfcIPBX QAe0KAfPR31oyO5mADmHdL3P+mPZLyFV9TpFoDp FDmPg0TTzGVr3Sze/mQ0TijLV -----</pre>

Keys Generate Keys Upload Export All Keys

Figure 4.37 OpenVPN Keys

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

When SE59XX acts as OpenVPN server, the user could define his own certification information by clicking on the **Key generate** button. Otherwise, the certificate can be imported. When generating a new key, a Pop-up window will open. Fill in the parameters and click on “**Generation Keys & Apply**” button.

OpenVPN Keys Generation

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

Figure 4.38 Certification information

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

When clicking on the **Keys Upload** button instead, a pop-up window shown in Figure 4.39 will show up and will allow you to import the related server or client certificates.

OpenVPN Keys Upload

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

Figure 4.39 Certificate Upload

Click the **Browse** button to select your own server or client certificate and click on the **Upload** button. When SE59xx acts as an OpenVPN server, use **Export All Keys** button to download all the necessary certificates include CA.crt, CA.key and the certificate and key for client side.

4.10.3 OpenVPN Status

In order to check the current OpenVPN connection status, click "OpenVPN status" in the VPN menu on the left-hand side of the screen. A page like below Figure 4.40 or Figure 4.41 will show up depending whether OpenVPN is set as Client or Server.

VPN > OpenVPN Status		SE5901B SS
OpenVPN Status		
Current Status		
Mode	Client	
Local Virtual IP Address	0.0.0.0	
Remote Virtual IP Address	0.0.0.0	
Status	Disconnected	
		Connect Disconnect Refresh

Figure 4.40 OpenVPN client status

- **Mode:** Displays the OpenVPN mode SE59xx is currently running as.
- **Local Virtual IP address:** Displays the Local virtual IP address.
- **Remote Virtual Status:** Displays the Remote virtual IP address.
- **Status:** Displays the current status of OpvnVPN connection. It will include Disconnected, Connecting and Connected.

VPN > OpenVPN Status

SE5901B SS

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
<div><div>Activate</div><div>Deactivate</div><div>Refresh</div></div>			

Figure 4.41 OpenVPN server status

- **Mode:** Displays the OpenVPN mode SE59xx is currently running as.
- **Local Virtual IP address:** Displays the Local virtual IP address.
- **Status:** Displays the current status of OpvnVPN connection. It will be either be Deactivated, Activating, Disconnected, Connecting and Connected.

4.11 IPsec Settings

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

SE59XX has an IPsec connection function to establish a secure communication link between **host-to-host**, **host-to-subnet** (or host-to-network), and **subnet-to-subnet** (or network-to-network). Note that at the other endpoint of the Internet, a router or gateway with full IPsec capability is required to successfully establish the secure communication. There are two types of IPsec connection modes or types supported by SE59XX which are **Tunnel mode** and **Transport mode**.

- In **Tunnel mode**, the entire IP packet is encrypted and authenticated. The IP packet is then encapsulated into a new IP packet with a new IP header. The **Tunnel mode** which is used to create Virtual Private Network (VPN) can be applied to the **host-to-host**, the **host-to-subnet**, and the **subnet-to-subnet** communications. The packet (datagram) format for **Tunnel mode** is as follow:

New IP Header	IPsec Header	Original IP Packet	Optional IPsec Trailer
---------------	--------------	--------------------	------------------------

- In **Transport mode**, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact because the IP header is not modified and not encrypted. However, when the authentication header is used, the IP addresses cannot be modified by Network Address Translation (NAT). The **Transport mode** can only be applied in the **host-to-host** communication. The packet (datagram) format for **Transport mode** is as follow:

Original IP Header	IPsec Header	Original IP Packet	Optional IPsec Trailer
--------------------	--------------	--------------------	------------------------

A **host-to-host** connection is typically used in a simple point-to-point communication. It is useful for a direct communication with a server or between the device (SE59XX) and a peer device (such as another SE59XX). Note that this type of connection cannot be use for accessing entire sub-network resources. Figure 4.42 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode**.

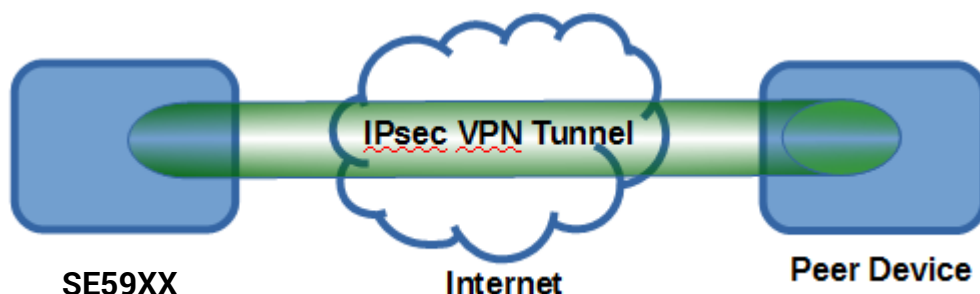


Figure 4.42 An example of Host-to-Host Connection

A **host-to-subnet** (or host-to-network) connection is mainly applied when one endpoint needs to access the other side's sub-networks. Typical applications are employees who are travelling on business and would like to connect back to their corporate headquarters via mobile devices. They can establish IPsec connections to access the internal corporate network resources. Figure 4.43 illustrates a road-warrior application in which SE59XX can access

a remote sub-network resource via a peer gateway. Figure 4.44 illustrates a gateway application in which SE59XX can passively accept connection requests from remote sides and provide access to the SE59XX sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

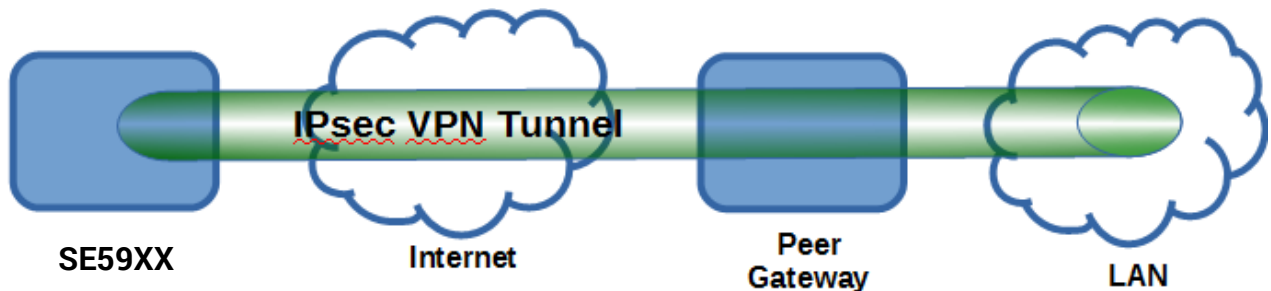


Figure 4.43 Roadwarrior Application using Host-to-Subnet Connection

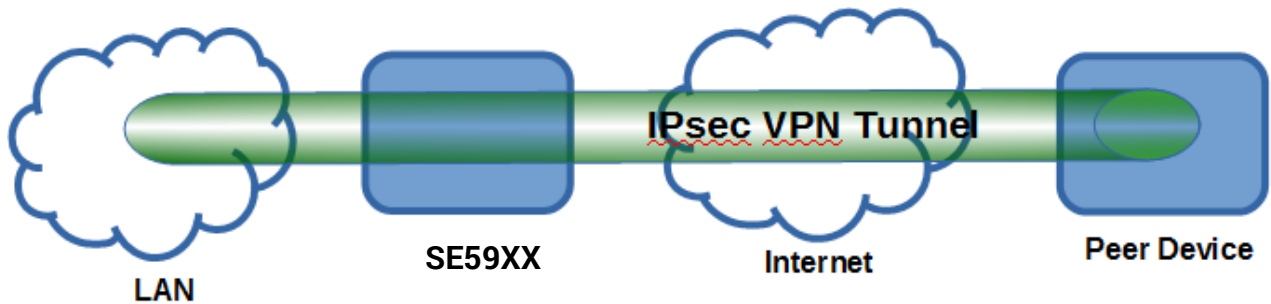


Figure 4.44 Gateway Application using Host-to-Subnet Connection

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

Figure 4.45 illustrates an example of the subnet-to-subnet connection with a network application. A host inside the remote subnet can also connect to a local subnet (host-network application) based on this subnet-to-subnet connection as shown in Figure 4.46. On the other hand, two different devices on two different subnets (host-host application) can be connected via a IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 4.47. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

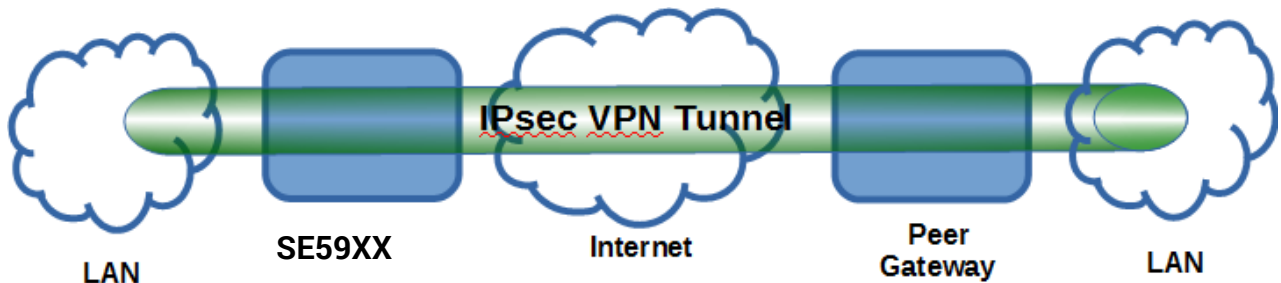


Figure 4.45 An example of network application using a subnet-to-subnet connection via the SE59XX and a peer device

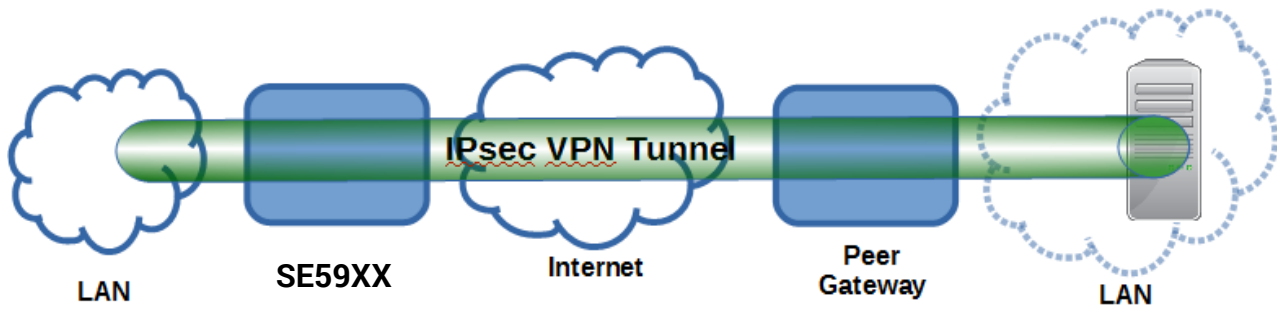


Figure 4.46 An example of host-network application via the subnet-to-subnet connection

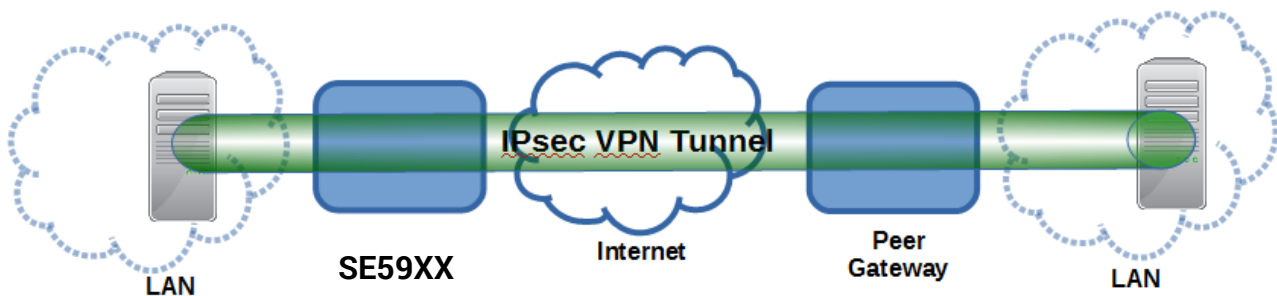


Figure 4.47 An example of host-host application via the subnet-to-subnet connection

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

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

SE59XX also has a feature called NAT traversal (NAT-T) that allows the IPsec tunnel to pass through the NAT in its network. SE59XX 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, SE59XX utilizes the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite. Note that IKE builds upon the Oakley protocol and ISAKMP (Internet Security Association and Key Management Protocol). IKE uses X.509 certificates for authentication either pre-shared or distributed using DNS (preferably with DNSSEC). IKE also uses a Diffie-Hellman key (DH) key exchange to set up a shared session secret from which cryptographic keys are derived. The IPsec security associations (SA) is divided into two phases. In phase one, IKE creates an authenticated secure channel between SE59XX and its peer device, which is called the IKE Security Association. The Diffie-Hellman (DH) key agreement is always performed in this phase to create a shared secret key or DH key. In phase two, IKE negotiates the IPsec security associations and generates the required key material for IPsec. This IPsec key which is a symmetrical key will be used for bulk data transfer inside the IPsec tunnel. A new Diffie-Hellman agreement can be done in phase two, or the keys can be derived from the phase one shared secret.

4.11.1 IPsec Settings

Figure 4.48 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: <input type="text" value="10.0.50.100"/>
Remote Subnet	<input 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 type="radio"/> None (Host Only) <input type="radio"/> Network: <input type="text" value="10.0.50.0"/> / <input type="text" value="24"/>
Connection Type	<input type="text" value="Tunnel"/>

Authentication Settings	
Method	<input type="radio"/> Pre-Shared Key: <input type="text" value="secrets"/>

IKE Settings		
Phase 1 SA (ISAKMP)	Mode	<input type="text" value="Main"/>
	DH Group	<input type="text" value="Group 2 (1024-bit)"/>
	Encryption Algorithm	<input type="text" value="AES-128"/>
	Authentication Algorithm	<input type="text" value="SHA1"/>
	SA Life Time	<input type="text" value="3600"/> seconds
Phase 2 SA	Protocol	<input type="text" value="ESP"/>
	Perfect Forward Secrecy	<input type="text" value="Group 2 (1024-bit)"/>
	Encryption Algorithm	<input type="text" value="AES-128"/>
	Authentication Algorithm	<input type="text" value="SHA1"/>
	SA Life Time	<input type="text" value="28800"/> seconds

Dead Peer Detection Settings	
DPD Action	<input type="text" value="Hold"/>
DPD Interval	<input type="text" value="30"/> seconds
DPD Timeout	<input type="text" value="120"/> seconds

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

Figure 4.48 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 SE59XX.
- **Peer Address:** This option is to specify the IP address of a remote host or peer host or remote gateway. There are two choices for the **Peer Address** which are **Dynamic** and **Statics**.

- **Dynamic:** When you selected the **Dynamic** by choosing the **Dynamic** radio button, the **Peer Address** or the remote device IP address is not fixed or unknown. Note that when **Peer Address** is set to dynamic mode, the SE59XX can accept remote connection request or will be the responder.
- **Static:** On the other hand, if you know the IP address of the remote device, you can choose the radio button for **Static** option and enter the IP address in the text box behind it. The SE59XX will be the initiator/responder.
- **Remote Subnet:** This option is to indicate whether you want to create an IPsec connection to the remote subnetwork. There are also two choices for **Remote Subnet** access:
 - **None (Host Only):** This option is to specify that the remote subnet is not supported or no remote subnet and only host access is supported. That is the remote end of the IPsec tunnel is a host or peer device only.
 - **Network:** This option is to specify the **Remote Subnet** by entering the **Subnet IP Address** and the number of **Subnet Masking Bits** or associated routing prefix. This option supports the Classless Inter-Domain Routing (CIDR) notation. For example, Subnet IP Address is 192.168.11.0 and Subnet mask are 24 bits (from 255.255.255.0).
- **Local Subnet:** This option is to enable an IPsec connection to the local subnetwork. There are two choices for **Local Subnet** access:
 - **None (Host Only):** This option is to specify that the local subnet is not supported or no local subnet and only local host access is supported. That is the local end of the IPsec tunnel is a host or peer device only.
 - **Network:** This option is to specify the **Local Subnet** by entering the **Subnet IP Address** and the number of **Subnet Masking Bits** or associated routing prefix. This option supports the Classless Inter-Domain Routing (CIDR) notation. For example, Subnet IP Address is 192.168.11.0 and Subnet mask are 24 bits (from 255.255.255.0).
- **Connection Type:** This option is to specify the IPsec connection type which can be either **Tunnel** mode or **Transport** mode. Please select the corresponding connection type from the drop-down list. Note that the **Tunnel mode** can be applied to the **host-to-host**, the **host-to-subnet**, and the **subnet-to-subnet** communications. The **Transport mode** can only be applied in the **host-to-host** communication.

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

The third part of **IPsec Settings** is the **IKE** (Internet Key Exchange) **Settings**. Internet Key Exchange (IKE) that SE59XX supports is the IKE version 1 or **IKEv1**. Within the **Phase 1 SA (ISAKMP)**, there are five security options to be configured. In phase 1, the two VPN gateway exchange information about the encryption algorithms that they support and then establish a temporary secure connection to exchange authentication information.

- First option is the **Mode** of IKE session which defines how many steps or packets will be used or exchanged during the IKE SA negotiation. You can choose either **Main Mode** or **Aggressive Mode**. The **Main Mode** will send SA proposals, Diffie-Hellman public key, and ISAKMP session authentication in three exchange packets, while the **Aggressive Mode** will put all SA proposals, DH public key, and ISAKMP session authentication in to one exchange packet. **Aggressive Mode** makes the IKE negotiation quicker than **Main Mode**. The difference between **Main Mode** and **Aggressive Mode** is that the "identity protection" is used in the **Main Mode**. The identity is transferred encrypted in the **Main Mode** but it is not encrypted in **Aggressive Mode**. Typically, the **Main Mode** is recommended.
- Second option is the selection of Diffie-Hellman's group (**DH Group**) of standardized global unique prime numbers and generators that will be used to provide secure asymmetric key exchange. The **DH Group** is

used to encrypt this IKE communication. SE59XX supports two **DH groups** which are **DH Group 2**, which is a 1024-bit modular exponentiation group (MODP), and **DH Group 5**, which is a 1536-bit MODP group.

- Third option is the selection of **Encryption Algorithm** which can be either **AES-128** or **3DES**. This option will select the key size and encryption algorithm to be used in the IKEv1 Phase 1. The default value is **AES-128**.
- Fourth option is the selection of **Authentication Algorithm** which can be either **SHA1** or **MD5**. This option will select which hash algorithm will be used to authenticate packet data in the IKEv1 Phase 1. The default value is **SHA1**.
- Fifth option is the **SA Life Time** which must be set in unit of seconds. This value represents the lifetime of the IKE key which is dedicated at Phase 1 between both end host or network. The default **SA Life Time** is 10800 seconds. The configurable range for **SA Life Time** is between 300 to 86400 seconds.

Within the **Phase 2 SA**, there are five security options to be configured. Similar to **Phase 1 SA**, SE59XX 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, SE59XX also supports two **DH groups** which are **DH Group 2** (1024-bit) and **DH Group 5** (1536-bit).

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

The final part of the **IPsec Settings** is the **Dead Peer Detection Settings**. Dead peer detection (DPD) is a mechanism that SE59XX use to verify the existence of a remote Internet Key Exchange (IKE) gateway or the peer device of SE59XX. To detect the peer device, SE59XX will sent encrypted IKE Phase 1 notification payloads (or hello message) to its peer device and wait for DPD acknowledgement from the peer device. If SE59XX does not receive an acknowledge message during a specific time interval (**DPD timeout**), it will consider that the peer device is dead. Then, SE59XX 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 SE59XX will perform if it found that the peer device is dead. You can choose either **Hold** to still hold the security association for the peer device and wait for the peer device to return or **Restart** to restart the security association process again. The **DPD Interval** is the period of time for sending the hello message to the peer device or the interval that SE59XX will repeatedly check the endpoint with keep-alive message. The **DPD interval** can be ranged from 1 to 65535 seconds. The default value for **DPD Interval** is 30 seconds. The **DPD Timeout** will be the time that SE59XX 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 SE59XX will take the PDP action. The **DPD Timeout** value range from 1 to 65535 seconds. The default value of **DPD Timeout** is 120 seconds. Description of each parameters in the IPsec Tunnels web page is summarized in Table 4.6.

Table 4.6 Description of Parameters in IPsec Tunnels Web Page

Field Name	Description	Default Value
General Settings		
IPsec	Enable the IPsec Tunnel	Disable
NAT Traversal	Enable the NAT Traversal mechanism	Enable

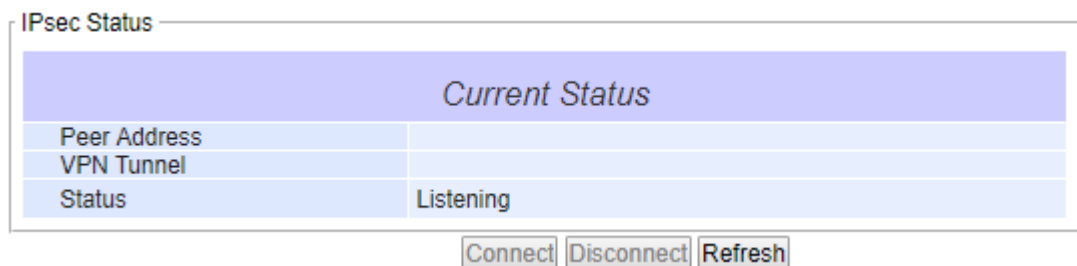
Field Name		Description	Default Value
Peer Address		IP address of the remote device which can be dynamic (any address) or static (fixed address)	Dynamic
Remote Subnet		Remote subnet can be either None (Host only) or Network (IP and Netmask)	None (Host Only)
Local Subnet		Local subnet can be either None (Host Only) or Network (IP and Netmask)	None (Host Only)
Connection type		Tunnel mode or Transport mode	Tunnel
Authentication Settings			
Method		Pre-Shared Key	secrets
IKE Settings			
Phase 1 SA	Mode	Choose how IKE negotiation is performed between Main Mode and Aggressive Mode	Main Mode
	DH Group	Diffie-Hellman groups, determine the strength of the key used in the key exchange process: DH Group 2 (1024-bit) or DH Group 5 (1536-bit)	Group 2 (1024-bit)
	Encryption Algorithm	Encryption algorithm used in the key exchange process: Either 3DES or AES	AES128
	Authentication Algorithm	Hash algorithm used to authenticate packet data in the key exchange process of IKEv1 phase 1: Either MD5 or SHA1	SHA1
	SA Life Time	How long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry. The value can be from 300 to 86,400 seconds.	3600
Phase 2 SA	Protocol	Choose how IP packet will be encrypted and verify: either Encapsulate Security Payload (ESP) or IP Authentication Header (AH)	ESP
	Perfect Forward Secrecy	Diffie-Hellman groups for Perfect Forward Secrecy of keys, determine the strength of the key used in the key exchange process: DH Group 2 (1024-bit) or DH Group 5 (1536-bit)	Group 2 (1024-bit)
	Encryption Algorithm	Select which key size and encryption algorithm will be used in IPsec tunnel: either 3DES or AES128	AES128
	Authentication Algorithm	Section of hash algorithm to be used to authenticate packet data in the IPsec tunnel: either MD5 or SHA1	SHA1
	SA Life Time	Value that represents the lifetime of the IKE key which is dedicated in Phase 2 between both end host or network. The available setting ranges is from 180 to 86,400 seconds.	28800
Dead Peer Detection Settings			
DPD Action		Select either Hold or Restart the tunnel's security association for the peer. Note that Hold is suitable for a statistically defined tunnel.	Hold
DPD Interval		Duration of time for sending hello message to the peer device: value from 1 to 65535 seconds.	30 seconds

Field Name	Description	Default Value
DPD Timeout	Duration of time to declare that the peer is dead: value from 1 to 65535 seconds.	120 seconds

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

4.11.2 IPsec Status

On this web page, you can check the status of your IPsec connection between SE59XX 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 SE59XX. The second information is the **VPN Tunnel**'s status. The third information is the **Status** of the IPsec connection which can be **Disabled**, **Listening**, or **Connected**. shows the **IPsec Status** web page under the **IPsec Settings** menu. There are three buttons at the end of the web page which are **Connect**, **Disconnect**, and **Refresh**. The **Connect** and **Disconnect** buttons allow you to establish or tear down the IPsec connection. The **Refresh** button enable you to check the latest status of the connection.



Current Status	
Peer Address	
VPN Tunnel	
Status	Listening

Figure 4.49 IPsec Status Web Page

4.11.3 Examples of IPsec Settings

The following subsections provide examples of **IPsec settings**. However, each example will be focused only on the **General Settings** part. The other parts of the **IPsec Settings** can be configured according to the user's preference. Please consult previous section on the details of **Authentication Settings**, **IKE Settings**, and **Dead Peer Detection Settings**. **Note** that the network-to-network (or subnet-to-subnet) connections are now supported in new firmware of SE59XX.

4.11.3.1 Host-to-Host Connections

Two scenarios can be configured for host-to-host connections: with static peer and with dynamic peer. A host-to-host topology for both scenarios is illustrated in Figure 4.50. Please follow the steps provided next for each scenario to set the **General Settings**.

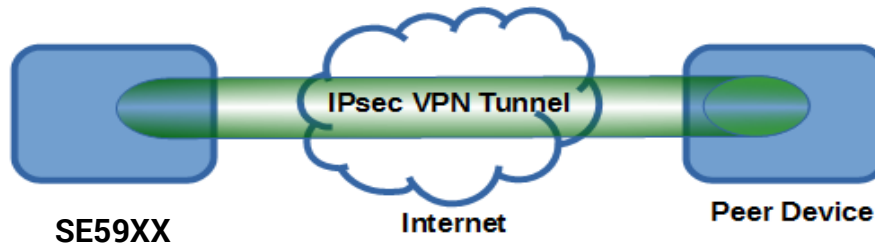


Figure 4.50 IPsec VPN Tunnel with Host-to-Host Topology

Scenario: host-to-host with static peer as shown in Figure 4.51

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
Note: When peer address is entered as the static address, the SE59XX acts as an **initiator** which takes the initiative and establishes a connection. The SE59XX 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**.

IPsec Settings

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

Figure 4.51 General Settings for Host-to-Host with Static Peer

Scenario: host-to-host with dynamic peer as shown in Figure 4.52

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
Note: When VPN connects to a peer with dynamic IP address, the SE59XX 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"/> / <input type="text"/>
Local Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: <input type="text"/> / <input type="text"/>
Connection Type	<input type="text" value="Tunnel"/>

Figure 4.52 General Settings for Host-to-Host with Dynamic Peer

4.11.3.2 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 SE59XX is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in Figure 4.53. Please follow the steps provided next for each scenario to set the **General Settings**.

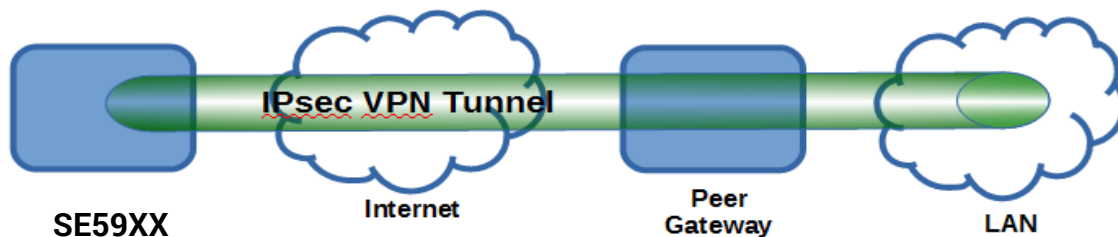


Figure 4.53 IPsec VPN Tunnel with Host-to-Network Topology

Scenario: host-to-network with static peer as shown in Figure 4.54

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
Note: When peer address is entered as a static address, the SE59XX is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. The SE59XX also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.

IPsec Settings

General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
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 4.54 General Settings for Host-to-Network with Static Peer

Scenario: host-to-network with dynamic peer as shown in Figure 4.55

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
Note: When VPN connection is set to a peer with dynamic IP address, the SE59XX will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.

IPsec Settings

General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static:
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 4.55 General Settings for Host-to-Network with Dynamic Peer

4.11.3.3 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 SE59XX is the gateway to a local network in these scenarios. A network-to-network topology for both scenarios is illustrated in Figure 4.56. Please follow the steps provided next for each scenario to set the **General Settings**.

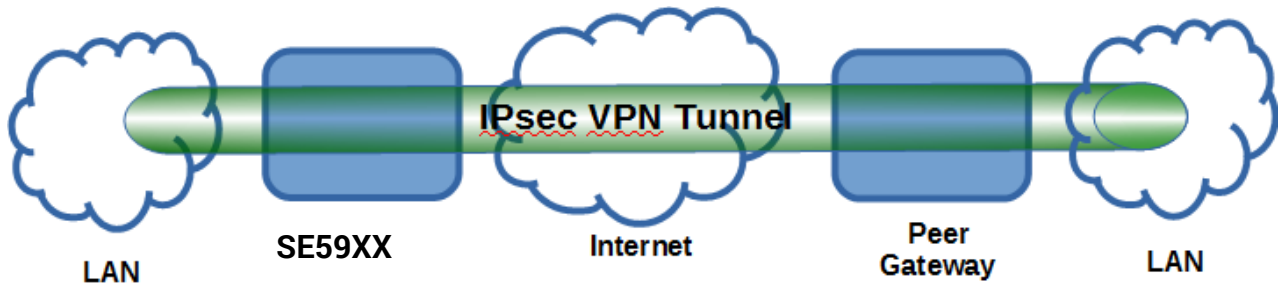


Figure 4.56 IPsec VPN Tunnel with Network-to-Network Topology

Scenario: network-to-network with static peer as shown in Figure 4.57

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
Note: When peer address is entered as a static address, the SE59XX is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. The SE59XX also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Set the network IPv4 address in the **Local Subnet** with the number of bits for subnetmask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.

IPsec Settings

General Settings	
IPsec	<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 4.57 General Settings for Network-to-Network with Static Peer

Scenario: network-to-network with dynamic peer as shown in Figure 4.58

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
Note: When VPN connection is set to a peer with dynamic IP address, the SE59XX will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Set the network IPv4 address in the **Local Subnet** with the number of bits for subnetmask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.

IPsec Settings

General Settings	
IPsec	<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 4.58 General Settings for Network-to-Network with Dynamic Peer

4.12 Spanning Tree

Spanning tree functionality is supported by Atop's SE59XX Industrial Device Server series. However, SE59XX 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, SE59XX 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 in SE59XX. It is an evolution of the STP (IEEE 802.1D standard), but it is still backwards compatible with standard STP. RSTP has the advantage over the STP. When there is a topology change such as link failure in the network, the RSTP will converge significantly faster to a new spanning tree topology. RSTP improves convergence on point-to-point links by reducing the Max-Age time to 3 times Hello interval, removing the STP listening state, and exchanging a handshake between two switches to quickly transition the port to forwarding state.

The **Spanning Tree** menu and its sub-menus can be found on left frame of the web interface of SE59XX. The list of **Spanning Tree** menu is shown in Figure 4.59. 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.

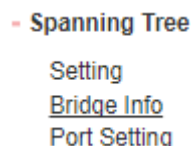


Figure 4.59 Spanning Tree Menu

4.12.1 Spanning Tree's Setting

Figure 4.60 shows an example of **Setting** web page of **Spanning Tree** menu. The **Spanning Tree Setting** page is divided into three parts which are **Mode Setting**, **Main Setting**, and **Port Setting**. For SE59XX, the user can only select one spanning tree mode, which is the **RSTP** (Rapid Spanning Tree Protocol) under the **Mode Setting**. The user can enable or disable spanning tree protocol under the **Main Setting** by checking the box behind the **Enabled** option. Note that when Enabled option is checked, the rest of the fields will become active. Then, the user can configure the **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 **Update** button at the end of the page to allow the change to take effect. The description of each parameter is summarized in Table.

Spanning Tree Setting

Mode Setting

Mode: RSTP

Main Setting

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

Enabled: ☒ Enable

Priority (0~61440): 32768

Maximum Age (6~40): 20

Hello Time (in second, 1~10): 2

Forward Delay (in second, 4~30): 15

Port Setting

Primary Port: LAN1

Secondary Port: LAN2

Update

Figure 4.60 Setting Web Page of Spanning Tree

Table 4.7 Descriptions of Spanning Tree Parameters

Label	Description	Default Factory
Mode	Mode of Spanning Tree Protocol to be enabled on SE59XX	RSTP
Enabled	Check the box to enable spanning tree functionality.	Disable
Priority	Enter a number to set the device priority. The value is in between 0 and 61440. The lower number gives higher priority.	32768
Maximum Age	Maximum expected arrival time for a hello message. It should be longer than Hello Time.	20
Hello Time	Hello time interval is given in seconds. The value is in between 1 to 10.	2
Forward Delay	Specify the time spent in the listening and learning states in seconds. The value is in between 4 to 30.	15
Primary Port	Spanning tree's primary port	LAN1
Secondary Port	Spanning tree's secondary port	LAN2

Note: To disable spanning tree function on SE59XX, the user can uncheck the **Enable** option and then click **Update** button.

4.12.2 Spanning Tree's Bridge Info

Bridge Info (information) provides the current configured parameters of spanning tree protocol as shown in Figure 4.61. Note that this page will not display any data on all fields if the RSTP was not enabled in the Spanning Tree's **Setting** web page. The information is further divided into two parts: **Root Information** and **Topology Information**. To check the latest information, please click on the **Refresh** button at the end of the page. Table 4.8 and Table 4.9 summarize the descriptions of each entry in the root information table and topology information table, respectively.

- System Status
- Network Settings
- Protocol Gateway
- SNMP/ALERT Settings
- E-mail Settings
- IPsec
- Spanning Tree
 - Setting
 - Bridge Info
 - Port Setting
- Log Settings
- + System Setup
- Reboot

Bridge Information

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

Root Information	
Root MAC Address	7c:66:9d:1d:c5:ff
Root Priority	32768
Root Path Cost	0
Root Maximum Age	20
Root Hello Time	2
Root Forward Delay	15

Topology Information	
Root Port	N/A
Num. of Topology Change	0
Last TC time ago	0

Refresh

Figure 4.61 Bridge Info Web Page of Spanning Tree

Table 4.8 Bridge's Root Information

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

Table 4.9 Bridge's Topology Information

Label	Description	Factory Default
Root Port	A forwarding port that is the best port from non-root bridge/switch (SE59XX) to root bridge/switch. Note that for a root switch there is no root port.	-
Num. of Topology Change	The total number of spanning topology change over time.	0
Last TC time ago	The duration of time since last spanning topology change.	-

4.12.3 Spanning Tree's Port Setting

Spanning Tree's **Port Setting** shows the configured value of spanning tree protocol for each port, as shown in Figure 4.62 and Figure 4.63. The configured information for each port is **state**, **role**, **path cost**, **path priority**, **link type**, **edge**, **cost**, and **designated information**. To check the latest update on the statistics, please click on the **Refresh** button. Table 4.10 summarizes the descriptions of spanning three port setting. If **Spanning Tree** is enabled, the table of **Spanning Tree Port Stting** becomes editable and four parameters (**Path Cost (Config)**, path priority (**Pri**), **Link Type (Config)** and **Edge (Config)**) can be adjusted on this page. The user can use the **Update** button to save the settings.

Spanning Tree Port Setting

Port	State	Role	Path Cost		Pri	Link Type		Edge
			Config	Actual		Config	P2P?	
Port1	Disc	Disabled	<input type="text" value="200000"/>	200000	<input type="text" value="128"/>	<input type="text" value="P2P"/>	<input type="text" value="Yes"/>	<input type="checkbox"/>
Port2	Fwd	Designated	<input type="text" value="200000"/>	200000	<input type="text" value="128"/>	<input type="text" value="P2P"/>	<input type="text" value="Yes"/>	<input checked="" type="checkbox"/>

Figure 4.62 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
<input type="text" value="P2P"/>	<input type="text" value="Yes"/>	<input type="checkbox"/>	<input type="text" value="No"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="P2P"/>	<input type="text" value="Yes"/>	<input checked="" type="checkbox"/>	<input type="text" value="Yes"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="2"/>	<input type="text" value="32768"/>	<input type="text" value="7c:66:9d:1d:c5:ff"/>

Figure 4.63 Spanning Tree Port Setting (Part 2)

Table 4.10 Descriptions of Spanning Tree Port Setting

Label		Description	Factory Default
Port		The name of the SE59XX's port	-
State		State of the port: 'Disc': Discarding - No user data is sent over the port. 'Lrn': Learning - The port is not forwarding frames yet, but it is populating its MAC Address Table. 'Fwd': Forwarding - The port is fully operational.	N/A
Role		Non-STP or STP RSTP bridge port roles: 'Root' - A forwarding port that is the best port from non-root bridge to root bridge. 'Designated' - A forwarding port for every LAN segment. 'Alternate' - An alternate path to the root bridge. This path is different from using the root port. 'Backup' - A backup/redundant path to a segment whose another bridge port already connects. 'Disabled' - Note strictly part of STP, a network administrator can manually disable a port.	Non-STP
Path Cost		Setting the path cost for each switch port	
	Config	Setting path cost (default: 0, meaning that using the system default value (depending on link speed))	0
	Actual	The actual value path cost (For RSTP, please see Note 1 below and table.)	0
Pri		Setting the port priority, used in the Port ID field of BPDU packet, value = 16 x N, (N:0~15) See Note 2 below.	128
Link Type		The connection between two or more switches (for RSTP)	
	Config	Setting of the Link Type P2P : A port that operates in full-duplex mode is assumed to be point-to-point link. Non-P2P : A half-duplex port (through a hub) Auto : Detect link type automatically	Auto
	P2P?	Yes : This port is a Point-to-Point (P2P). No : This port is not Point-to-Point (Non-P2P).	No
Edge		Edge port is a port which no other STP/RSTP switch connect to (for RSTP). An edge port can be set to forwarding state directly.	
	Config	Edge functional is set: Yes or No	No
	Edge?	Yes : This port is an edge port. No : This port is not an edge port.	No
Designated		This shows some information of the best BPDU packet through this port.	
	Cost	Root path cost	0
	P. Pri. (Port Priority)	Port priority (high 4 bits of the Port ID), Value = 16 x N, (N: 0~15)	128
	Port	Interface number (lower 12 bits of the Port ID)	-
	Bri. Pri. (Bridge Priority)	Bridge priority, (value = 4096 x N, (N: 0~15)	32768
	Bridge MAC	The MAC address of the switch which sent this BPDU	-

Note:

1. In general, the path cost is dependent on the link speed. Table 4.11 lists the default values of path cost for RSTP.

Table 4.11 Default Path Cost for RSTP

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

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

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

Bridge ID = priority (4 bits) + locally assigned system ID extension (12 bits) + ID [MAC Address] 48 bits

The default bridge priority is 32768.

Port ID = priority (4 bits) + ID (Interface number) (12 bits)

The default port priority is 128.

4.13 SNMP/ALERT Settings

The Simple Network Management Protocol (SNMP) is used by network management software to monitor devices in a network, to retrieve network status information of the devices, and to configure network parameters of the devices. The **SNMP/ALERT Settings** page showed in Figure 4.64 allows user to configure SE59XX device so that it can be viewed by third-party SNMP software, and allows SE59XX to send alert events to administrator and SNMP trap server.

SNMP/ALERT Settings

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

Basic Data Objects	
System Contact	<input type="text" value="contact"/>
System Name	<input type="text" value="System"/>
System Location	<input type="text" value="location"/>
SNMP	<input checked="" type="checkbox"/> Enable
SNMP Version	<input type="text" value="v2"/>
Read Community	<input type="text"/>
Write Community	<input type="text"/>
SNMP Trap Server	
SNMP Trap Server	<input type="text" value="0.0.0.0"/>

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

Figure 4.64 SNMP/Alert Settings Web Page

SE59XX provides three basic SNMP fields under the **Basic Data Objects** part which are: “**System Contact**” usually used to specify the device’s contact information in case of emergency (default value is “contact”), “**System Name**” usually used to identify this device (default value is “System”), and “**System Location**” usually used to specify the device location (default value is “location”).

To make the device’s information available for public viewing/editing, you can enable the **SNMP** function by checking the **Enable** box and fill in the two passphrases (or SNMP Community Strings) below it. Note that when the SNMP is unchecked, three setting option lines will show up as depicted in Figure 4.64. By filling in the passphrase for the “**Read Community**”, SE59XX device allows other network management software to read its information. By filling in the passphrase for the “**Write Community**”, SE59XX device allows other network management software to read/modify its information. The default SE59XX’s SNMP Community Strings (or

passphrases) for **Read Community** and **Write Community** as shown in Figure 4.64 are “public” and “private”, respectively.

Additionally, you can setup a **SNMP Trap Server** in the network to receive and collect all alert messages from SE59XX. To configure SE59XX to dispatch alert messages originated from any unexpected incidents, you can fill in the IP Address of the **SNMP Trap Server** in the field shown in Figure 4.64. Note that any changes in these settings will take effect after the SE59XX device is restarted.

Under the **SNMP Trap Server** part, there is a list of **Alert Type** under **Event alert settings** box in Figure 4.64. 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 SE59XX 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 SE59XX 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 SE59XX as listed in Figure 4.64. However, some event can only be reported by e-mail. These alerts are useful for security control or security monitoring of the SE59XX 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 SE59XX.
- **IP Address Changed:** This event occurs when the SE59XX device's IP address is changed.
- **Password Changed:** This event occurs when the administrator password is changed.

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

4.14 SMS

The Short-Message-Service (SMS) feature is supported in some SE59XX Industrial Device Server models such as SE5901B-IO-4G which has 3G/4G cellular network interface equipped within the device. The main purpose of this function is to enable the network administrator to remotely control the device. This feature will be useful when the device is installed in a hard-to-reach location or in the location where wired network cable is not available. The SMS service allows the device to accept specific commands or to send specific alerts related to the device status. This menu has three submenus (web pages) which are **Basic Settings**, **Phone Settings**, and **Manual Send**. Each submenu will be explained as follows.

4.14.1 Basic Settings

An example of **Basic Settings** web page is shown in Figure 4.65. It provides the list of basic options for configuring the SMS's operation. You can configure the **Mode** of operation, the **Password**, whether the device will response to an SMS command (**Reply to command**), how the device will reply when it encounters an **Unrecognized command**, and adding additional **Alert delay time** to different types of alert messages. Description of each option under the Basic Settings is summarized in Table 4.12.



- + System Status
- + Network Settings
- + Serial
- SNMP/ALERT Settings
- SMS
 - Basic Settings
 - Phone Settings
 - Manual Send
- E-mail Settings
- + VPN
- + Log Settings
- + System Setup
- Reboot

SMS > Basic SettingsSE5901B-IO-4G SS

Basic Settings

Mode	<input type="radio"/> Disable commands by SMS <input checked="" type="radio"/> Allow commands from all phone numbers <input type="radio"/> Allow commands from restricted list only
Password	<input type="password"/> <input type="checkbox"/> Show Password
Reply to command	<input type="radio"/> No <input checked="" type="radio"/> Yes
Unrecognized command	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">Command not recognized, please try again!</div>
Alert delay time	<div style="display: flex; flex-direction: column; gap: 5px;"><div>Lan link down <input type="text" value="5"/></div><div>Lan link up <input type="text" value="10"/></div><div>DI1 status changed <input type="text" value="10"/></div><div>DI2 status changed <input type="text" value="10"/></div><div>DI1 status to 1 <input type="text" value="10"/></div><div>DI1 status to 0 <input type="text" value="10"/></div><div>DI2 status to 1 <input type="text" value="10"/></div><div>DI2 status to 0 <input type="text" value="3"/></div><div>IPsec disconnected <input type="text" value="10"/></div><div>OpenVPN disconnected <input type="text" value="10"/></div><div>PPTP disconnected <input type="text" value="1"/></div></div>

Figure 4.65 Basic Settings Web page for SMS

Table 4.12 Description of Options under the Basic Settings of SMS

Field Name	Description	Limit	Default Value
Mode	There are 3 modes that can be selected via the radio buttons for SMS operation: 1. "Disable command by SMS" means that command sent by SMS function is disabled, but it still can read by SMS. 2. "Allow commands from all phone numbers" means that the device will accept a valid SMS command from any phone number. 3. "Allow command from restricted list only" , means that the device will only accept a valid SMS command from phone numbers in the list (defined in the Phone Settings web page).	-	Disable
Password	This option allows the user to set a private password as SMS command validation rule.	Max. 16 characters Min. 4 characters	-
Reply to command	This option set the action of the device when the device receives an SMS command. The user can decide whether the device need to reply to an SMS message.	-	Yes
Unrecognized command	If the device receives a wrong or unsupported command via SMS, it will reply with specific content entered in the textbox.	Max. 160 characters	Command not recognized, please try again!
Alert delay time	To prevent too frequent alert SMS, you can set delay time for alerts in the list below and no alert will be generated with the delay between two alerts as entered in the box of each alert. List of alerts: <ul style="list-style-type: none">• LAN link down• LAN link up• DI1 status changed• DI2 status changed• DI1 status to 1• DI1 status to 0• DI2 status to 1• DI2 status to 0• IPsec disconnected• OpenVPN disconnected• PPTP disconnected	Max. 30 seconds Min. 0 seconds	10 seconds

After you finished updating or changing the setting on this page, please click on the **Save** button. Otherwise, click on the **Cancel** button to discard any changes.

4.14.2 Phone Settings

Under the **Phone Settings** web page of **SMS** menu, you can configure the options related to each phone number such as **Alias**, **Phone Number**, and related **Permission Settings** which are **Remote Control** or **Device Alert**. Figure 4.66 shows an example of **Phone Settings** web page. The upper part is a box called **Phone Settings**. This box allows you to enter information and permission of each phone number individually. The lower box called **Phone**

List is a table that lists all configured phones that can send remote control's SMS message or can receive device alerts via SMS message.

atop
Technologies

- + System Status
- + Network Settings
- + Serial
- SNMP/ALERT Settings
- SMS
 - Basic Settings
 - Phone Settings
 - Manual Send
- E-mail Settings
- + VPN
- + Log Settings
- + System Setup
- Reboot

SMS > Phone Settings **SE5901B-IO-4G SS**

Phone Settings

General Settings

Alias	<input type="text"/>
Phone Number	<input type="text"/>

Permission Settings

Remote Control	<input type="checkbox"/> Enable
Device Alert	<input type="checkbox"/> Enable

Phone List

Delete	Alias	Phone Number	Remote Control	Device Alert
<input type="checkbox"/>	Tes1	0911111111	Disabled	Cold start Authenticate fail Authenticate success IP Address changed Password changed Reset to default Restore config Lan link down Lan link up DI1 status changed DI2 status changed
<input type="checkbox"/>	Test2	0922222222	Enabled	
<input type="checkbox"/>	Test3	0933333333	Enabled	DI1 status to 0 DI2 status to 0 IPsec connected IPsec disconnected OpenVPN connected OpenVPN disconnected PPTP connected PPTP disconnected Unable to connect to Network Unknown command

Figure 4.66 Phone Settings Web Page for SMS

To add a new phone to the **Phone List**, first you must enter a name for that phone in the **Alias**'s text box. Second, you can enter the phone number in the **Phone Number**'s text box. Third, you can check or uncheck the **Enable** boxes behind the **Remote Control** and **Device Alert** options. If you check the box for **Remote Control**, the corresponding phone will be able to send SMS command to the SE59XX device. If you check the box for **Device Alert**, the corresponding phone will be able to receive SMS alerts from the SE59XX device. After you finished configuring the **Phone Settings** box, you must click the **Add** button to add that particular phone to the **Phone List**. Note that the maximum number of the phone in the list is 5 phone numbers.

To remove any phone from the **Phone List**, you can simply check the box under the **Delete** column of the **Phone List** and then click on the **Delete** button.

Table 4.13 summarizes the description of the options under the **Phone Settings** web page.

Table 4.13 Description of Options under the Phone Settings of SMS

Field Name	Description	Limit	Default Value
Alias	The alias is the nickname of the phone number for easy identifying.	Max. 10 characters	-
Phone Number	The phone number that will be sending SMS commands or receiving SMS alerts.	Max. 12 digits (numeric only)	-
Remote Control	This option enables or disables the permission for the phone that it can remotely control the SE59XX device.	-	Disabled
Device Alert	This option enables or disables the permission for the phone that it can receive alert form the SE59XX device. Note that the alert type list will show up in the table of Phone List when the device alert permission is enabled.	-	Disabled

4.14.3 Manual Send

The web page called **Manual Send** under the **SMS** menu allows you to test sending an SMS message to a phone number. Figure 4.67 shows the **Manual Send** web page. To perform a manual sending of SMS message, you must enter a phone number and fill in your SMS content. Then, you must click on the **Send** button to have the SE59XX device send the specified SMS content to the destination phone number directly.

The screenshot shows the 'Manual Send' web page. On the left is a navigation menu with the 'atop Technologies' logo at the top. The menu items are: + System Status, + Network Settings, + Serial, SNMP/ALERT Settings, - SMS (expanded), Basic Settings, Phone Settings, Manual Send (highlighted with a green box), E-mail Settings, + VPN, + Log Settings, + System Setup, and Reboot. The main content area has a blue header bar with 'SMS > Manual Send' and 'SE5901B-IO-4G SS'. Below the header, there's a section titled 'Manual send SMS message' with a sub-header 'Manual Send'. It contains two input fields: 'Phone Number' with the value '0912345678' and 'SMS content' with the text 'This is a test message.'. A 'Send' button is located at the bottom right of the form.

Figure 4.67 Manual Send Web Page under SMS

Table 4.14 Description of Options in the Manual Send Web Page

Field Name	Description	Limit	Default Value
Phone Number	The phone number that will be receiving SMS message.	Max. 12 digits (numeric only)	-

Field Name	Description	Limit	Default Value
SMS content	The content of SMS message is entered in the text box.	Max. 160 characters	-

4.14.4 Remote Control Command List

To control the SE59XX industrial device server remotely, you need to configure the SE59XX as described in Section 4.14.1 and 4.14.2 first. This section explains how to format a remote control command that can be sent via SMS message and can be recognized by the SE59XX. When a remote control command is received at SE59XX, the device will decide whether to reply with a message based on the configuration defined in **SMS's Basic Settings**. All the remote control commands are case insensitive and each command must follow the format shown below.

#password# command [**variable**]

Note that the **red (bold) variable** are necessary while the *green (italic) password* is optional. Note that the password should match the one defined in Section 4.14.1. Table 4.15 summarizes the list of all supported commands, their message formats, and their corresponding reply messages.

Table 4.15 List of All Supported Remote Control Commands

Command	Description	Format
		Reply Message
Reboot	Rebooting the device	<i>#password#</i> reboot
		"rebooting DeviceName..."
Operate relay	Trigger relay, number=1 or 2, status = 1(open), 0(closed)	<i>#password#</i> set Relay number,status
		"Relay number is now open/closed"
Connect IPsec	Start the IPsec, connect to peer device	<i>#password#</i> connect IPsec
		"IPsec is now connected" or "Could not connect to IPsec"
Disconnect IPsec	Stop the IPsec, disconnect to peer device	<i>#password#</i> disconnect IPsec
		IPsec is now disconnected
Connect OpenVPN	Start the OpenVPN, connect to peer device	<i>#password#</i> connect OpenVPN
		"OpenVPN is now connected" or "Could not connect to OpenVPN"
Disconnect OpenVPN	Stop the OpenVPN, disconnect to peer device	<i>#password#</i> disconnect OpenVPN
		"OpenVPN is now disconnected"
Connect PPTP	Start the PPTP, connect to peer device	<i>#password#</i> connect PPTP
		"PPTP is now connected" or "Could not connect to PPTP"
Disconnect PPTP	Stop the PPTP, disconnect to peer device	<i>#password#</i> disconnect PPTP
		"PPTP is now disconnected"
Alive	Check the device if it is still running normally	<i>#password#</i> alive
		Yes, here I am!

Command	Description	Format
		Reply Message
GPS coordinates	Get GPS coordinates of the device	<i>#password#</i> position
		"DeviceName is at XXX.XXXXXX N/S, YYYYY.YYYYY E/W" or "Could not locate DeviceName"
IP address	Get 3G/4G IP address of the device	<i>#password#</i> get IP
		"DeviceName address is xxx.xxx.xxx.xxx" or "DeviceName has no IP address"
Signal strength	Get 3G/4G signal strength of the device	<i>#password#</i> get signal strength
		"DeviceName NetworkName signal strength is XXX%"
Activate cellular data	Activate the 3G/4G cellular data	<i>#password#</i> go online
		"Cellular data has been enabled" or "Cellular data was already enabled"
Deactivate cellular data	Deactivate the 3G/4G cellular data	<i>#password#</i> go offline
		"Cellular data has been disabled" or "Cellular data was already disabled"

4.14.5 Alert Type List

This section provides the list of all available alerts that can be sent out by the SE59XX to the user via SMS message. While SE59XX device is running, there can be a number of events to be notified as list in Table 4.16. The user can define which alert types are needed to be notified or reported via SMS message.

Table 4.16 List of All SMS Alert Types

Alert Type	Description
Cold start	Device reboot alert. It is triggered with or without power off.
Authenticate fail	This alert is sent out when a web login failed.
Authenticate success	Web login success alert. This alert may happen many times while web browser is loading.
IP Address changed	This alert is sent out when IP address was changed.
Password changed	This alert is sent out when Password was changed.
Reset to default	This alert is sent out when the system was restored to the factory default setting.
Restore config	This alert is sent out when valid configurations was restored to the system.
Lan link down	This alert is sent out when a LAN's physical link was unplugged.
Lan link up	This alert is sent out when a LAN's physical link was plugged.
DI1 status changed	This alert is triggered when DI1 status was changed.
DI2 status changed	This alert is triggered when DI2 status was changed.
DI1 status to 1	This alert is triggered only when DI1 status was changed from 0 to 1.

Alert Type	Description
DI1 status to 0	This alert is triggered only when DI1 status was changed from 1 to 0.
DI2 status to 1	This alert is triggered only when DI2 status was changed from 0 to 1.
DI2 status to 0	This alert is triggered only when DI2 status was changed from 1 to 0.
IPsec connected	This alert is triggered when IPsec was started.
IPsec disconnected	This alert is triggered when IPsec was stopped.
OpenVPN connected	This alert is triggered when OpenVPN was started.
OpenVPN disconnected	This alert is triggered when OpenVPN was stopped.
PPTP connected	This alert is triggered when PPTP was started.
PPTP disconnected	This alert is triggered when PPTP was stopped.
Unable to connect to Network	If there is no signal or bad signal for communication, it is triggered when device could not connect to network.
Unknown command	This alert is triggered if device receives wrong or unsupported command from SMS.

4.15 E-Mail Settings

When SE59XX 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 SE59XX to be able to send an e-mail. Figure 4.68 shows the **E-mail Settings** page in which there are two configurable parts: **E-mail Address Settings** and **E-mail Server**. First for the **E-mail Address Settings** part, a **Sender's** e-mail address is required to be filled in the **Sender's** text box which will be used in the **From** field of the e-mail. Note that the maximum length of sender email address is 48 characters. Then, for the **Receiver's** text box you can enter multiple recipients which will be used in the **To** field of the e-mail. Note that to fill in multiple receiver e-mail addresses in the **Receiver's** text box, please separate each e-mail address with semicolon (;).

> E-mail Settings

E-mail 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 4.68 E-mail Setting Web Page

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



Attention

It is also important to setup Default Gateway and DNS Servers in the Network Settings properly so that SE59XX can lookup domain names and route the e-mails to the proper default gateway. Please see the Default Gateway and DNS Sever Settings in Section o .

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

4.16 Log Settings

Under the **Log Settings** menu of web interface of SE59XX series Industrial Serial Device Server, you can configure various data logging for the device. Figure 4.69 lists the sub-menu under the **Log Settings**. It consists of **System Log Settings**, **COM Log Settings**, **Event Log**, and **COM Datalog**. Each of this sub-menu will be described in the following subsections.

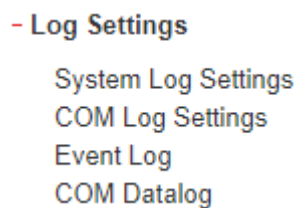


Figure 4.69 Log Settings Menu

4.16.1 System Log Settings

The Syslog function is turned on by default and cannot be turned off for SE59XX. It is used to keep log for system events and report to an external Syslog server if necessary. Figure 4.70 shows the **System Log Settings** page under the **Log Settings** menu. Description of each option is provided as follows.

The image shows a web page titled "Log Settings > System Log Settings". Below the title is a section titled "System Log Settings" with a light blue header. The settings are 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)

At the bottom of the form are two buttons: "Save & Apply" and "Cancel".

Figure 4.70 Log Settings Web Page under Log Settings

- **Enable Log Event to Flash:** When the check box is enabled, SE59XX will write log events to the local flash. Otherwise the log events would be cleared when the device restarts because they are stored in the RAM by default.
- **Enable Syslog Server:** When the check box is enabled, it will allow SE59XX to send Syslog events to the remote Syslog server with the specified IP address (next option). All the data sent/received from serial interface will be logged and sent to Syslog Server.
- **Syslog Server IP:** The user must specify the IP address of a remote Syslog Server in this field.

- **Syslog Server Service Port:** This option allows user to specify the remote Syslog Server Port number between 1 and 65535. Note that the default port number is 514.

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

4.16.2 COM Log Settings

Transmitted data through COM port could be logged for recording or debugging purposes. Additionally, the logs could be reported to an external Syslog server as well. Figure 4.71 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

Syslog Server Service Port

(1~65535, default=514)

Save & Apply

Cancel

Figure 4.71 COM Log Settings Web Page under System Setup

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

Note: SE59XX can store up to 100 KBytes internally. A request or a response will be in one line, and the data longer than 512 bytes will go into another line. You can retrieve logs by using a **FTP Client**. The FTP login is the same as the WebUI login. Logs are located in `/var/log/logcomxx` (xx is the port number). When the reserved space is full, new logs will replace old logs. We strongly recommend sending COM logs to a remote Syslog server.

- **Data Types:** There are two radio buttons which are hexadecimal (**HEX**) and **ASCII** for user to select the desired logged data's format.
- **COM Ports:** The user can select which port(s) will be logged by checking the corresponding boxes.
- **Enable Syslog Server:** Enabling this option would allow user to send COM logs to a remote Syslog server. It is possible to send COM logs to the same Syslog server used previously for event logging (See Section 4.16.1).
- **IP Address:** When the Syslog Server is enabled in the previous option, please specify the remote Syslog server's IP address in this field.
- **Syslog Server Service Port:** This option allows user to specify the remote Syslog Server Port number between 1 and 65535. Note that the default port number is 514.

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

4.16.3 Event Log

This page displays the current event log or system log stored in the SE59XX device. Figure 4.72 shows an example of logged event. Each record of the **System Log** consists of **Time**, **Severity**, and **Message** description.

Log Settings > Event Log

System Log

System Log ALL ▾

Refresh Export System Log Clear System Log

Show 10 ▾ entries Search:

Time	Severity	Message
May 24 00:02:32	INFO	System Start.
May 24 16:14:27	WARN	User admin authenticate fail attempted to access

Showing 1 to 2 of 2 entries

Previous 1 Next

Figure 4.72 System Log Web Page under System Setup

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

4.16.4 COM Datalog

This page displays the current COM data log stored in the device. The desired **COM** port number can be selected from the **COM x Log** drop-down list in Figure 4.73, which allows it to display logs from different COM ports. An example of **COM 1 Log** is shown in Figure 4.73. Each record of the log consists of **Time**, **COM Index**, Direction (**T/R**) and **Data**.

Log Settings > COM Datalog

COM Log

COM 1 Log

Refresh Export Data Log Clear Data Log

Show 10 entries Search:

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

Showing 0 to 0 of 0 entries

Previous Next

Figure 4.73 COM Datalog Web Page under Log Settings

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

4.17 System Setup

Under the **System Setup** menu of web interface of SE59XX series Industrial Serial Device Server, you can perform a number of administration tasks for the device. Figure 4.74 lists the sub-menu under the **System Setup**. It consists of **Date/Time Settings**, **Admin Settings**, **Firmware Upgrade**, **Backup/Restore Setting**, and **Ping**. Each of this sub-menu will be described in the following subsections.

- System Setup
 - Date/Time Settings
 - Admin Settings
 - Firmware Upgrade
 - Backup/Restore Settings
 - Ping

Figure 4.74 System Setup Menu

4.17.1 Date/Time Settings

Date and time can be set manually or using Network Time Protocol (NTP) to automatically synchronize date and time of SE59XX with a Time Server. Figure 4.75 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 SE59XX by checking the option **Local NTP Service** below **NTP Settings** part or automatically synchronize with a time server or NTP server. To enable automatic time synchronization, please check the box behind the **Sync with NTP Server** option. Then proceed to enter the **IP address** or **host name** for the **NTP Server**. Note that if a host name is entered, the DNS server must be configured properly (see detail in Section o). The fourth part is the **Daylight Saving Time Settings** that can be enabled when **Enable Daylight Saving Time** box is checked. When it is enabled, the user can select the detailed setting of the daylight saving period, such as **Start Date** and **End Date** with **Offset**. Finally, the last part of the page is the **Manual Time Settings** where you can set **Date** and **Time** using corresponding drop-down lists in Figure 4.75.

Date/Time Settings

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

Current Date/Time

5 / Mar / 2018 14:32:05

Time Zone Settings

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

NTP Settings

Local NTP Service

Sync with NTP Server

NTP Server

Daylight Saving Time Settings

Enable Daylight Saving Time

Start Date

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

End Date

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

Offset

0 hour(s)

Manual Time Settings

Date

-- / -- / --

Time

-- : -- : --

Save & Apply

Cancel

Figure 4.75 Date/Time Settings Web Page under System Setup

**Attention**

It is also important to setup Default Gateway and DNS Servers in the Network Settings properly (See Section o), so SE59XX can lookup DNS names and point to the proper NTP server.

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

4.17.2 Admin Settings

The SE59XX Series allows user and password management through this **Admin Settings** page under **System Setup** menu. By default, the user name is “**admin**” and the password is “**default**”. To set or change their values, you can enter the information in the **User name**, the **Old password**, the **New password** and the **Repeat new password** fields under the **Account Settings** part as shown in Figure 4.76. At the end of the **Admin Settings** web page, there is the **Web mode** part which allow the user to select the radio button of normal **HTTP** or **HTTPS** for secure communication with the device’s web user interface (Web UI).

Admin Settings

Set up the login user name and password.

Account Settings	
User name	<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 4.76 Admin Settings Web Page under System Setup

After finish configuring the **Admin Settings**, please click on **Save & Apply** button to keep the change that you have made and to apply your setting. Another pop-up window will be displayed to re-authenticate the user to access the Web UI of SE59XX as shown in Figure 4.7. You must re-enter the username and the password to login to the SE59XX. When the saving, applying, and re-authentication are finished, the web browser will remain on the **Admin Settings** page. If you want to cancel the change and reset all changes back to their original values, just click the **Cancel** button.

4.17.3 Firmware Upgrade

Updated firmware for SE59XX is provided by Atop from time to time (for more information please visit Atop News & Events webpage) to fix bugs and optimize performance. It is very important that the device must **NOT be turned off or powered off during the firmware upgrading, (please be patient as this whole process might take up to 5 minutes)**. Before upgrading the firmware, please make sure that the device has a reliable power source that will not be powered off or restarted during the firmware upgrading process.

To upgrade a new firmware to SE59XX, please download the latest firmware for your SE59XX model from the download tab on the SE59XX product page or from the Download page under the Support link on Atop's main webpage. Then, copy the new firmware file to your local computer. Note that the firmware file is a binary file with ".dld" extension. Next, open the Web UI and select **Firmware Upgrade** page under the **System Setup** menu. Then, click "**Browse...**" button as shown in Figure 4.77 below to find and choose the new firmware file. Then, click "**Upload**" button to start the firmware upgrade process. The program will show the upload status. Please wait until the uploading process is finished (the amount of time varies depending on the equipment used). Finally, the SE59XX device will then proceed to restart itself. In some cases, you might require to re-configure your SE59XX device. To restore your backup configuration from a file, please see the procedure in the next subsection.

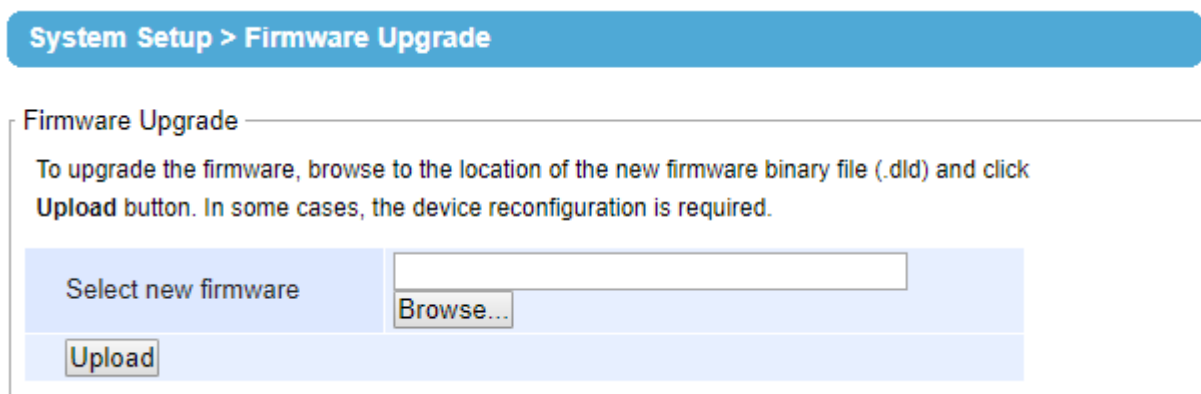


Figure 4.77 Firmware Upgrade Web Page under System Setup

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

4.17.4 Backup/Restore Settings

Once all the configurations are set and the device is working properly, the user should back up the current configuration of SE59XX. 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 SE59XX Series devices of similar settings by uploading these settings to all devices.

To back up configuration, click "**Backup**" button under the **Backup Configuration** part as shown in Figure 4.78, and a the backup file (ModelName-MACAddress.dat) will be automatically saved on your computer. It is important **NOT to manually modify the saved configuration file by any editor. Any modification to the file may corrupt the file and it may not be used for later restoration.** Please contact Atop authorized distributors for more information on this subject.

To restore the backup configuration, click "**Browse**" button under the **Restore Configuration** part as shown in Figure 4.78 to locate the backup configuration file on user's computer. Then, click on "**Upload**" button to upload the backup configuration file to the device. Once the backup configuration file is successfully uploaded, the device will restart. Note that the time needed for this process may vary on the equipment used.

If you need to restore the SE59XX device to its factory default configuration, you can click on the **Restore** button under the **Restore Factory Default** section as shown in Figure 4.78.

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 4.78 Backup/Restore Settings Web Page under System Setup

4.17.5 Ping

The Web UI of SE59XX has an interface to call **Ping** which is a network diagnostic utility for testing reachability. You can use the **Ping** function to determine whether SE59XX can reach the gateway or other devices in the network. To use the **Ping**, enter a destination IP address in the text box behind the **Ping To** and click **Start** button as shown in Figure 4.79. This process usually takes around 20 seconds. Figure 4.79 represents a successful ping without packet loss from SE59XX to the address 10.0.50.101 and back, while Figure 4.80 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.

System Setup > Ping

Ping

Ping To

10.0.50.101

Start

```
PING 10.0.50.101 (10.0.50.101): 56 data bytes
64 bytes from 10.0.50.101: seq=0 ttl=128 time=0.794 ms
64 bytes from 10.0.50.101: seq=1 ttl=128 time=0.641 ms
64 bytes from 10.0.50.101: seq=2 ttl=128 time=0.641 ms
64 bytes from 10.0.50.101: seq=3 ttl=128 time=0.641 ms

--- 10.0.50.101 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.641/0.679/0.794 ms
```

Figure 4.79 Ping Web Page under System Setup

System Setup > Ping

Ping

Ping To

10.0.50.202

Start

```
PING 10.0.50.202 (10.0.50.202): 56 data bytes

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

Figure 4.80 Unreachable Ping Example

4.17.6 Special Settings

Note that this **Special Settings** page will be available on SE5901B with IO version only. Under the **Special Settings** page, you can configure a number of special hardware and software utilities for SE5901B. Figure 4.81 displays the **Special Settings** page for SE5901B with IO version. Under this menu, user can set **DO Control**, **Current DI/DO Status**, **Ping Function**, **Auto Reboot**, **3G Rx Timeout**, **Internal Battery**, and **Actively report device information**. Description of each special setting is briefly explained as followings. Note that for non-IO version of SE5901B, there will be no DO Control and Current DI/DO Status options.

System Setup > Special Settings

SE5901B-3G-IO

Special Settings

DO Control	
From Network	<input type="checkbox"/> Enable
Check DO Reset Function	<input type="checkbox"/> Enable
Current DI/DO Status	
DI 1	Off
DI 2	Off
DO 1	<input type="radio"/> On <input checked="" type="radio"/> Off
DO 2	<input type="radio"/> On <input checked="" type="radio"/> Off
Ping Function	
<input type="checkbox"/> Enable	
Destination IP	<input type="text"/>
Interval	<input type="text" value="30"/> (10~180 sec) seconds
Auto Reboot	
<input type="checkbox"/> Enable	
<input checked="" type="radio"/> Specific time <input type="radio"/> Periodic time	
<input type="text" value="00"/> : <input type="text" value="00"/> (HH : MM)	
4G Rx Timeout	
<input type="checkbox"/> Enable <input type="text" value="0"/> (1~1440) mins	
Internal Battery	
Power Failure Message	<input type="text"/>
Actively report device information	
<input type="checkbox"/> Enable	

Save & Apply

Cancel

Figure 4.81 Special Setting Web Page under System Setup for SE5901B with IO version only

- **DO Control** (Only for SE5901B with IO version): The user can initialize and send a Digital Input (DI) command to SE5901B using special sequence of characters. Then, SE5901B will trigger its Digital Output (DO) which is connected to an external device such as sound alarm or light alarm. Note that DO 1 pin is referred to Relay 1 pin and DO 2 pin is referred to Relay 2 pin as depicted and summarized in Figure 7.6 and Table 7.7, respectively.

Typically, the user has to re-code or rewrite their own program to initialize the Digital Input (DI) command. Note that examples of SE5901B DO & DO command set are given in the Section 4.17.6.1.

- **From Network:** When this option is enabled, it will allow SE5901B to accept Digital IO control commands which is sent by the network.
- **Check DO Reset Function:** When this option is enabled, it will provide a test action for the DO 1 (Relay 1) pin that is connected to an external device Reset pin. After the test action, SE5901B will set the DO 1 (Relay 1) pin to "ON" state and after a period of 1 second the DO 1 (Relay 1) pin will be set to "OFF" state.
- **Current DI/DO Status** (Only for SE5901B with IO version): This part allows the user to instantly display and control the DI/DO status.
 - **DI 1:** The status of Digital Input 1 can be either "Off" or "On".
 - **DI 2:** The status of Digital Input 2 can be either "Off" or "On".
 - **DO 1 (Relay 1):** There are two radio buttons for the user to select between "On" and "Off".
 - **DO 2 (Relay 2):** There are two radio buttons for the user to select between "On" and "Off".
- **Ping Function:** This function is used for the controller inside the SE5901B to ensure that 3G/4G connection is checked for its status periodically. You can enable this function by checking the **Enable** box. The SE5901B will periodically ping the "**Destination IP**" with the specified **Interval**. When there are two consecutive unreachable responses by the ping command or ping failures, the controller will automatically disconnect the 3G/4G connection. In addition, if the 3G/4G connection and the **Reconnect on Dial Failure** option under the **3G/4G Configuration** part under **3G/4G Settings** web page are enabled the SE5901B will re-dial to re-establish its 3G/4G connection.
 - **Enable:** Check the box to enable the **Ping Function**.
 - **Destination IP:** This field is to enter the IP address of the device which will be pinged.
 - **Interval:** This field indicates the interval of ping which can be between 10 and 180 seconds.
- **Auto Reboot:** When this option is enabled, the SE5901B can automatically reboot itself either on a specific time of day or every specific period of time.
 - **Enable:** Check the box to enable the **Auto Reboot**.
 - **Specific Time or Periodic Time:** Choose the corresponding radio button for your selection.
 - **(HH : MM):** Enter the hour and minute for the time based on the selection of previous option.
- **3G/4G Rx Timeout:** This setting is used to automatically disconnect the cellular connection when the 3G/4G interface did not receive any packet in a certain period of time specified in this option.
 - **Enable:** Check the box to enable the 3G/4G Rx Timeout.
 - **Time:** Timeout period between 1 and 1440 minutes.
- **Internal Battery** (Only for SE5901B with Internal Battery version): In the built-in battery version, if the main power supply of SE5901B is off or interrupted, the SE5901B will transmit the specified **Power Failure Message** by SNMP trap or E-mail or Alert method to a network computer.
 - **Power Failure Message:** The message filled in this textbox will be transmitted.
- **Actively report device information:** When this option is enabled, the SE5901B will actively broadcast its information periodically. The information includes all the content for **Device Management Utility** (or formerly **Serial Manager**) software's columns, e.g. Model, IP Address, MAC Address, Host Name, Kernel version, and AP Information. Note that the purpose of this option is that the user can check the status of a number of SE5901Bs on the network (e.g. when there are more than 20 units) without using ping, browsing SE5901B's web page or even clicking the Rescan button on the Device Management Utility software.
 - **Enable:** Check the box to enable this option.

4.17.6.1 Examples of SE5901B DO & DI Command Set

The following transmitted (TX) or received (RX) hexadecimal sequences are examples of SE5901B DO (Digital Input) and DI (Digital Output) Command Set. The users need to write their own program to generate or interpret the hexadecimal sequences. The command set can be divided into READ operation and WRITE operation.

- Examples of READ Operation
 - For Digital Output (DO), an operation to read a status from a coil connected to SE5901B's DO may consist of the following TX and RX sequences:
 - TX: 00 13 00 00 00 06 01 01 00 00 00 02
 - RX: 00 13 00 00 00 04 01 01 01 00
 - The last two hexadecimal numbers of the RX sequence are the status of the coil.
 - Coil Status: 00
 - The following table is the map of the Bit 0 to Bit 7 which represent DO_0 to DO_7 pin, respectively.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	0
DO_7	DO_6	DO_5	DO_4	DO_3	DO_2	DO_1	DO_0

- For Digital Input (DI), an operation to read discrete inputs connected to SE5901B's DI may consist of the following TX and RX sequences:
 - TX: 00 7C 00 00 00 06 01 02 00 00 00 02
 - RX: 00 7C 00 00 00 04 01 02 01 00
- The last two hexadecimal numbers of the RX sequence are the status of the inputs.
 - Input Status: 00
- The following table is the map of the Bit 0 to Bit 7 which represent DI_0 to DI_7 pins, respectively.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	0
DI_7	DI_6	DI_5	DI_4	DI_3	DI_2	DI_1	DI_0

- Examples of WRITE Operation
 - For Digital Output (DO), an operation to write to a single coil connected to SE5901B's DO may consist of the following TX and RX sequences:
 - TX: 00 00 00 00 00 06 0F 05 00 01 FF 00
 - RX: 00 00 00 00 00 06 0F 05 00 01 FF 00
 - The RX result indicate that the DO_1 is in an "On" state.
 - For Digital Output (DO), an operation to write to multiple coils connected to SE5901B's DO may consist of the following TX and RX sequences:
 - TX: 00 FF 00 00 00 08 01 0F 00 00 00 02 01 03
 - RX: 00 FF 00 00 00 06 01 0F 00 00 00 02
 - The RX result indicate that the DO_0 and DO_1 are in "On" state.

4.18 Reboot

To manually reboot the SE59XX device, click on the “**Reboot**” button at the end of the **Reboot** page as shown in Figure 4.82. 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 SE59XX again

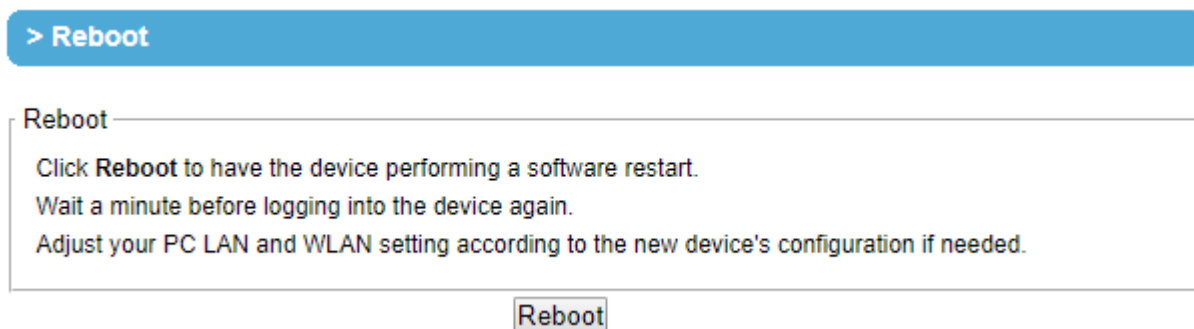


Figure 4.82 Reboot Web Page

5 Link Modes and Applications

5.1 Link Mode Configuration

SE59XX series supports three different **Link Modes** which are **TCP Server**, **TCP Client**, and **UDP**. The **Link Mode** describes the role of SE59XX and the connection between SE59XX device and other remote devices in the network which would like to communicate with serial devices on SE59XX's COM port(s). Under the three Link Modes, **TCP Server** mode can support **RAW**, **Virtual COM**, **Reverse Telnet** and **Pair Connection Master** applications, while **TCP Client** mode can only support **RAW**, **Virtual COM** and **Pair Connection Slave** applications. Note that **UDP** mode does not have the same supported applications as the previous two TCP modes. Discussion on how to setup different Link Modes properly will be presented in the following sections. Figure 5.1 shows the **Link Mode** options for **COM 1** port which can be found on **COM1** page under **Serial** menu of Web UI (See details on Serial Settings in Section

Figure 4.27). Note that on SE59XX model with IO interface will have two COM ports.

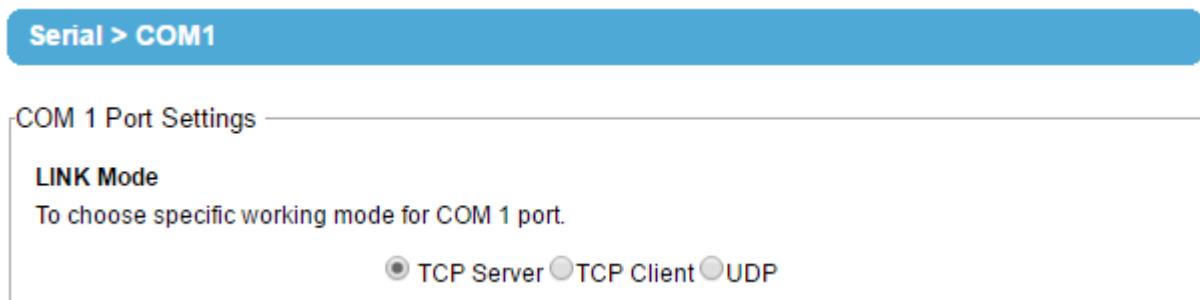


Figure 5.1 Link Mode Options for COM1 Port

5.1.1 Link Mode: Configure SE59XX as a TCP Server

SE59XX series can be configured as a Transport Control Protocol (TCP) server in a TCP/IP network to listen for an incoming TCP client connection to a serial device. Figure 5.2 depicts an example of a PLC (serial) device which is connected to SE59XX 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 (SE59XX) 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 SE59XX device's default link mode.

TCP Server Mode

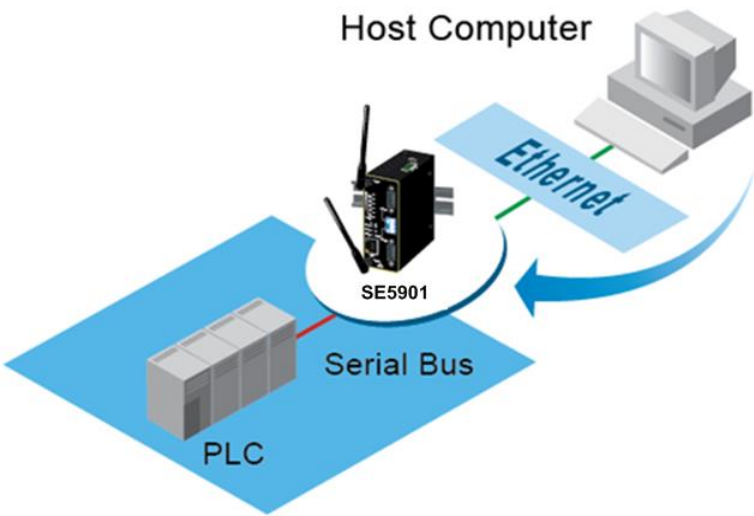


Figure 5.2 SE59XX is set as a TCP Server Link Mode

The default Link Mode of SE59XX is the **TCP Server** mode. Figure 5.3 shows an example of configuration setting for **TCP Server** Link Mode under the **COM 1** page. There are additional connection settings that can be configured as shown in Figure 5.3. By selecting the TCP Server Link Mode, a TCP client program on a remote host computer should be prepared to connect to SE59XX. 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 checked="" type="radio"/> Reply to all <input checked="" type="radio"/> Transparent Mode

Figure 5.3 Connection Settings for TCP Server Link Mode

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

Serial > COM1

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

Save & Apply Cancel Advanced Settings

Figure 5.4 TCP Server Link Mode Settings under COM 1 Page

- Select **TCP Server** radio button in the Link Mode options. Note that **TCP Server** is the default Link Mode for COM port of SE59XX.
- Under the **TCP Server** section, you will find the following options.
 - **Application:** There are 3 different communication applications to choose from here:
 - **RAW:** There is no protocol on this mode which means that the data is passed transparently.
 - **Virtual COM:** The Virtual COM protocol is enabled on the serial device to communicate with a virtualized port from a remote client. It is possible to create a Virtual COM port on Windows/Linux in order to communicate with the serial device as a remote client.
 - **Reverse Telnet:** This application is used to connect the serial device and another serial device (usually a Terminal Server) with a Telnet program. Telnet programs in

Windows/Linux usually require special handshaking to get the outputs and formatting to show properly. The SE59XX series will interact with those special commands (CR/LF commands) once Reverse Telnet application is enabled.

- **Pair Connection Master:** This application is used when the user want to pair two serial devices over the Ethernet network.
- **IP Filter:** This option will enable the **Source IP** option below. When this option is checked, SE59XX 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 SE59XX). 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 SE59XX) should listen to. It is also used by the remote TCP client to connect to the TCP server. The default local port is 4660. You can enter different port number in this option.
- **Maximum Connection:** This option specifies the maximum number of remote devices/clients (with maximum of 4 clients) that can be connected to the serial device on this COM port.
- **Response Behavior:** This option specifies how SE59XX 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 SE59XX will hold requests from all other remote connected hosts until the serial device replies or the **Response Interval Timeout** takes into effect to discard it; however, unrequested data sent from the serial device would be forwarded to all connected hosts. Additionally, user can specify how a reply message from the serial device will be sent to the remote connected hosts with two possible options:
 - **Reply to requester only:** The COM port will reply to the remote connected host who has requested the data only.
 - **Reply to all:** A reply is sent to all remote connected hosts.
 - **Transparent mode:** The COM port on SE59XX will forward requests from all remote connected hosts to the serial device immediately and reply to all remote connected hosts once it receives data from the serial device.
- For other **Serial Settings** on the same configuration page, please go to Section 4.7.2 and for **Advanced Settings** please go to Section 4.7.3.
- After finish configuring the **Link Mode**, please scroll down to the bottom of the page and click on "**Save & Apply**" button to save all the changes that you have made.

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

5.1.2 *Link Mode: Configure SE59XX as a TCP Client*

SE59XX series can be configured as a TCP client in TCP/IP network to establish a connection to a TCP server on a remote host computer. Figure 5.5 depicts an example of two serial card readers connected to two different SE59XX devices where both SE59XX devices are on the same Ethernet network as the remote host computer. The arrow in Figure 5.5 indicates the connection request from the client side of TCP connection. After the connection is established, data can be transmitted between a serial device (connected to the COM port of each SE59XX) and a remote host computer in both directions. This also applies to Virtual COM application running in the client mode.

TCP Client Mode

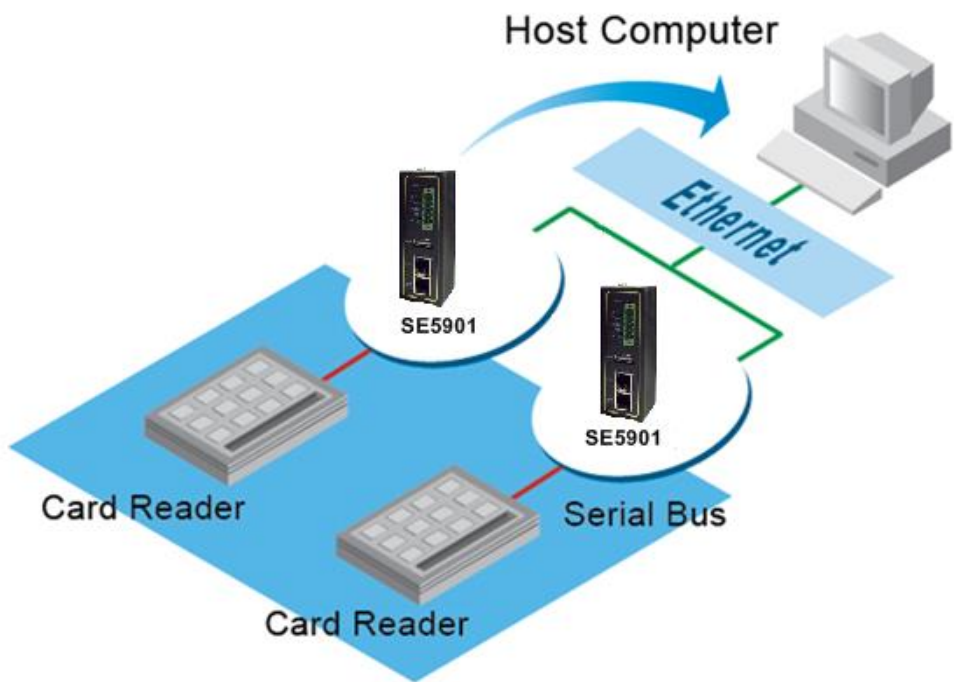


Figure 5.5 Example of SE59XX Configured as TCP Client Link Mode

Figure 5.6 shows an example of configuration setting for **TCP Client** Link Mode under the **COM 1** page. There are additional connection settings that can be configured as shown in Figure 5.7. By selecting the **TCP Client** Link Mode, a TCP server program on a remote host computer should be prepared to accept a connection request from SE59XX. 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 5.6 Connection Settings for TCP Client Link Mode

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

Serial > COM1

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

Save & Apply Cancel Advanced Settings

Figure 5.7 Setting in TCP Client Link Mode

- Select **TCP Client** radio button in the **Link Mode** options.
- Under the TCP Client section, you will find the following options.
 - **Application**: Only three communication applications are available here: **RAW**, **Virtual COM** and **Pair Connection Slave** in which their definitions are the same as described above in Section 5.1.1.
 - **Destination IP 1**: Please specify the preferred **Destination IP** address of the TCP server program on the remote host in this field. This should match the IP settings of the TCP server program.
 - **Destination Port 1**: Please specify the preferred port number of the TCP server program on the remote host in this field. Once again, this should match the IP setting of the TCP server program.
 - **Backup Destination IP 1**: Please specify the preferred **Backup Destination IP** address of the TCP server program on the remote host in this field. Once the Destination IP 1 cannot be reachable, SE59XX will send the data to Backup Destination IP 1.
 - **Backup Destination Port 1**: Please specify the preferred port number of the TCP server program on the remote host in this field. Once again, this should match the IP setting of the TCP server program.

- **Destination 2:** You can enable second remote destination for TCP connection if necessary by checking on the **Enable** box in this option. Two different TCP servers can be set for redundancy.
- **Destination IP 2:** Please specify the preferred **Destination IP** address of the second TCP server program on the remote host in this field. This should match the IP settings of the second TCP server program.
- **Destination Port 2:** Please specify the preferred port number of the second TCP server program on the remote host in this field. Once again, this should match the IP setting of the second TCP server program.
- **Backup Destination IP 2:** Please specify the preferred **Backup Destination IP** address of the TCP server program on the remote host in this field. Once the Destination IP 2 cannot be reachable, SE59XX will send the data to Backup Destination IP 2.
- **Backup Destination Port 2:** Please specify the preferred port number of the TCP server program on the remote host in this field. Once again, this should match the IP setting of the TCP server program.
- **Response Behavior:** This option specifies how the device will proceed or behave when it receives request from remote connected hosts. The description of each option is the same as described in previous subsection (Section 5.1.1 Link Mode: Configure as a TCP Server) .
- For other **Serial Settings** on the same configuration page, please go to Section 4.7.2 and for **Advanced Settings** please go to Section 4.7.3 COM Configuration: Advanced Settings.
- After finish configuring the **Link Mode**, please scroll down to the bottom of the page and click on "**Save & Apply**" button to save all the changes that you have made.

5.1.3 *Link Mode: Configure SE59XX 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. SE59XX also supports connectionless UDP protocol compared to the connection-oriented TCP protocol. The SE59XX 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 SE59XX should listen to and specify the **Destination IPs** of the remote UDP nodes. Figure 5.8 illustrates an example of UDP Link Mode in which a serial display device is connected on a serial bus and SE59XX. Two remote host computers, which are on the same Ethernet network as SE59XX, can both send UDP datagram or messages to the serial display device through SE59XX.

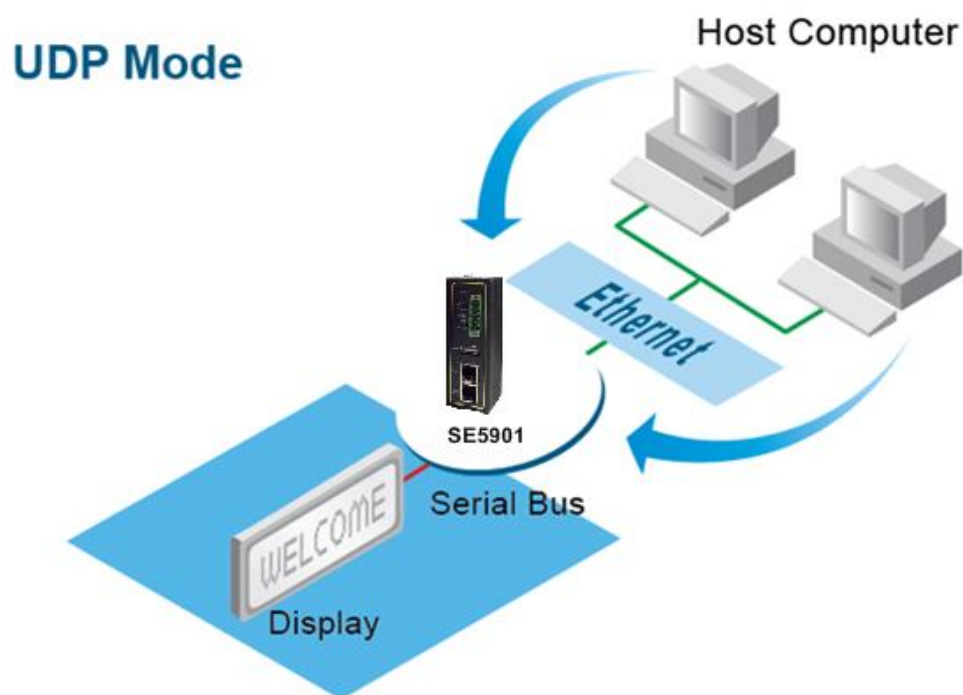


Figure 5.8 Example of SE59XX Configured in UDP Link Mode

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

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 5.9 Connection Setting in UDP Link Mode

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

Serial > COM1 M

COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

☐ TCP Server ☐ TCP Client ☒ UDP

UDP

Local Port: 65535

<input checked="" type="checkbox"/> Destination IP Address 0	10	0	50	101 ~ 102	Port: 511
<input checked="" type="checkbox"/> Destination IP Address 1	10	0	100	100 ~ 150	Port: 252
<input checked="" type="checkbox"/> Destination IP Address 2	10	0	201	200 ~ 250	Port: 65535
<input checked="" type="checkbox"/> Destination IP Address 3	10	0	55	100 ~ 100	Port: 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	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 5.10 UPD Link Mode Setting under COM 1 Page

- Select **UDP** radio button in the **Link Mode** options.
- Under the **UDP** section, you will find the following options.
 - **Local Port:** This field specifies the local port number for **UDP Link Mode** on SE59XX which it will be listening to and it can be any number between 1 and 65535. Note that typically the port number that is larger than 1024 is recommended to avoid conflicting with the well-known port numbers. You should match this setting with the remote UDP program. Note that this number is usually called destination port in the remote UDP program.
 - **Destination IP Address 1 to 4 and its Port Numbers:** Each line of these options can specify the range of IP addresses and port number that will be communicating with SE59XX. 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 SE59XX can handle would highly depend on the traffic load. We have tested that SE59XX can handle up to 200 UDP nodes (with baud rate of 9600 bps, request interval of 100ms, and data length of 30 bytes).
- For other Serial Settings on the same configuration page, please go to Section 4.7.2 and for Advanced Settings please go to Section 4.7.3.
- After finish configuring the **Link Mode**, please scroll down to the bottom of the page and click on "**Save & Apply**" button to save all the changes that you have made.

5.2 Link Mode Applications

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

5.2.1 TCP Server Application: Enable Virtual COM

SE59XX 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 SE59XX's COM ports. The benefit of using Virtual COM is that rewriting an existing COM program to read IP packets is unnecessary. In other words, it is possible to use an ordinary or legacy serial (COM) program. The conversion/virtualization of IP to COM is all done in the system driver transparently. Figure 5.11 shows SE59XX in **TCP Server** mode with **Virtual COM** application enabled. Please follow the following steps to enable **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
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 5.11 Virtual COM Application in TCP Server Link Mode

- Follow steps in Section 5.1.1 to configure SE59XX in **TCP Server Link Mode** properly.
- Click on the drop-down list of the **Application** option under **TCP Server** section and switch to "**Virtual COM**" to enabled Virtual COM application in SE59XX.
- Scroll down to the bottom of the page and click on "**Save & Apply**" button to save the changes.
- Configure Virtual COM in the Operating System on the remote host computer. For Windows, please refer to Chapter 6 for necessary instructions. Please remember SE59XX'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 Atop Technologies.

5.2.2 TCP Server Application: Enable RFC 2217 through Virtual COM

The underlying protocol of Virtual COM is based on RFC 2217 which is the Telnet COM Control Option. Therefore, it is possible to use RFC 2217 with SE59XX in the 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. SE59XX) to communicate with serial device on the access server's COM port. To do so, please refer to Section 5.2.1 (previous section) to enable Virtual COM so that SE59XX becomes aware of the command names and codes defined in RFC 2217. Note that there is no need to configure Virtual COM on the Operating System of the remote host computer because Virtual COM ports would not be used.

5.2.3 TCP Client Application: Enable Virtual COM

It is also possible to run Virtual COM in TCP Client Link Mode. shows a configuration of Virtual COM application in TCP Client Link Mode. It is usually easier to use Virtual COM in the TCP Client Link Mode if SE59XX uses dynamic IP (via DHCP) because setting a static IP address in Virtual COM's Control Panel in the Operating System is not possible. Please follow the following steps to enable Virtual COM application in TCP Client Link Mode.

LINK Mode

To choose specific working mode for COM 1 port.

☐ TCP Server ☒ TCP Client ☐ UDP

TCP Client	
Application	Virtual COM
Destination IP 1	10 . 0 . 50 . 1
Destination Port 1	4660
Destination 2	<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 5.12 Virtual COM Application in TCP Client Link Mode

- Follow step in Section 5.1.2 to configure SE59XX in TCP Client Link Mode properly.
- Click on the drop-down list of the Application option under TCP Client section and switch to "Virtual COM" to enable Virtual COM application in SE59XX.
- Scroll down to the bottom of the page and click on "Save & Apply" button to save the changes.
- Configure Virtual COM in the Operating System on the remote host computer. For Windows, please refer to Chapter 6 for necessary instruction. Please remember the **Destination Port** number configured on this page in order to enter this information in Serial/IP Virtual COM's Control Panel later.

5.2.4 TCP Client Application: Enable RFC 2217 through Virtual COM

The underlying protocol of Virtual COM is based on RFC 2217 which is the Telnet COM Control Option. Therefore, it is possible to use RFC 2217 with SE59XX in the TCP Client mode. Note that the RFC 2217 allows a client, which is SE59XX in this case, to initiate a Telnet session to a remote host computer to communicate with serial device or serial (COM) program on the remote host computer. To do so, please refer to Section 5.2.3 (previous section) to

enable Virtual COM so that SE59XX becomes aware of the command names and codes defined in RFC 2217. Note that there is no need to configure Virtual COM on the Operation System of the remote host computer because Virtual COM ports would not be used.

5.2.5 TCP Server Application: Configure SE59XX as a Pair Connection Master

A Pair Connection application is useful when pairing up two serial devices over the Ethernet or when it is impossible to install Virtual COM in the serial devices. However, the pair connection application does require two SE59XX to work in pair. One would be the Pair Connection Master and the other would be the Pair Connection Slave. Figure 5.13 shows a configuration of Pair Connection Master application in TCP Server Link Mode. Please follow the following steps to enable Pair Connection application and set the SE59XX as Master in TCP Server Link Mode.

Link Mode

To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Pair Connection Master ▼
IP Filter	<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 5.13 Pair Connection Master Application in TCP Server Link Mode

- Follow steps in Section 5.1.1 to configure SE59XX in TCP Server Link Mode properly.
- Click on the drop-down list of the **Application** option under TCP Server section and switch to “**Pair Connection Master**” to enabled Pair Connection application in SE59XX.
- Scroll down to the bottom of the page and click on “**Save & Apply**” button to save the changes.
- Please remember Pair Connection Master’s IP address (i.e. SE59XX’s IP address on your desired network interface (either Ethernet or Wi-Fi)) and Local Port number here in order to enter these information in another SE59XX device with the Pair Connection Slave setting later.
- Proceed to the next section to configure a Pair Connection Slave to connect to this Master.

5.2.6 TCP Client Application: Configure SE59XX as a Pair Connection Slave

A Pair Connection Slave application is configured for SE59XX under TCP Client Link Mode as shown in Figure 5.14. It is necessary to pair up with a Pair Connection Master as described in previous section. Please setup a Pair Connection Master on another SE59XX device first before proceeding. Please follow the following steps to enable Pair Connection application and set this SE59XX 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 5.14 Pair Connection Slave Application in TCP Client Link Mode

- Follow steps in Section 5.1.2 to configure SE59XX in TCP Client Link Mode properly.
- Click on the drop-down list of the **Application** option under TCP Client section and switch to “**Pair Connection Slave**” to enabled Pair Connection application in SE59XX.
- Enter the **Destination IP** address and the **Destination Port** number (for Destination 1 and (optionally Destination 2)) that match to the settings of Pair Connection Master (another SE59XX device)’s IP and port number that were setup previously.
- Scroll down to the bottom of the page and click on “**Save & Apply**” button to save the changes.

5.2.7 TCP Server Application: Enable Reverse Telnet

Reverse Telnet application is useful if a Telnet program is used to connect to SE59XX and the serial interface of the SE59XX 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. SE59XX will interact with those special commands (such as CR/LF commands) if **Reverse Telnet** is enabled. Figure 5.15 shows a configuration of **Reverse Telnet** application in the **TCP Server Link Mode**. Note that the **Reverse Telnet** application is only available when SE59XX is configured as **TCP Server Link Mode**. Please follow the following steps to enable **Reverse Telnet** application under the **TCP Server Link Mode**.

LINK Mode

To choose specific working mode for COM 1 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Reverse Telnet
IP Filter	<input type="checkbox"/> Enable
Source IP	0.0.0.0
Local Port	4660
Maximum Connection	1
Response Behavior	<div><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</div>

Figure 5.15 Reverse Telnet Application in TCP Server Link Mode

- Follow steps in Section 5.1.1 to configure SE59XX in **TCP Server Link Mode** properly.
- Click on the drop-down list of the **Application** option under **TCP Server** section and switch to “**Reverse Telnet**” to enabled reverse telnet application in SE59XX.
- Scroll down to the bottom of the page and click on “**Save & Apply**” button to save the changes.

6 VCOM Installation & Troubleshooting

6.1 Enabling VCOM

SE59XX 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 SE59XX’s COM ports. Please note that **Virtual COM Application** can only be enabled in **TCP Server Link Mode** as shown in Figure 6.1 or **TCP Client Link Mode** as shown in Figure 6.2.

COM 1 Port Settings

LINK Mode

To choose specific working mode for COM 1 port.

☒ TCP Server

☐ TCP Client

☐ UDP

TCP Server

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

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

COM 1 Port Settings

LINK Mode

To choose specific working mode for COM 1 port.

☐ TCP Server

☒ TCP Client

☐ UDP

TCP Client

Application	Virtual COM
Destination IP 1	0 . 0 . 0 . 0
Destination Port 1	4660
Destination 2	<input type="checkbox"/> Enable
Destination IP 2	0 . 0 . 0 . 0
Destination Port 2	4660
Response Behavior	<div><div><input type="radio"/> Request & Response Mode</div><div><input type="radio"/> Reply to requester only</div><div><input type="radio"/> Reply to all</div><div><input checked="" type="radio"/> Transparent Mode</div></div>

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

Virtual COM on host computer allows remote access of serial devices over TCP/IP networks through Serial/IP Virtual COM ports that work like local native COM ports. Figure 6.3 is an example of Virtual COM application diagram. In the diagram, multiple serial servers (i.e. SE59XX devices) in which each one connects to serial device are connected over an Ethernet hub. Their serial devices can be accessed through the TCP/IP network of the hub. Note that there are traditionally only two Physical COM ports (COM 1 and COM 2) on the personal computer (PC) while there can be several Virtual COM ports such as COM 3, 4, 5, and so on. In SE59XX case, the TCP/IP network can be wired network such as Ethernet.

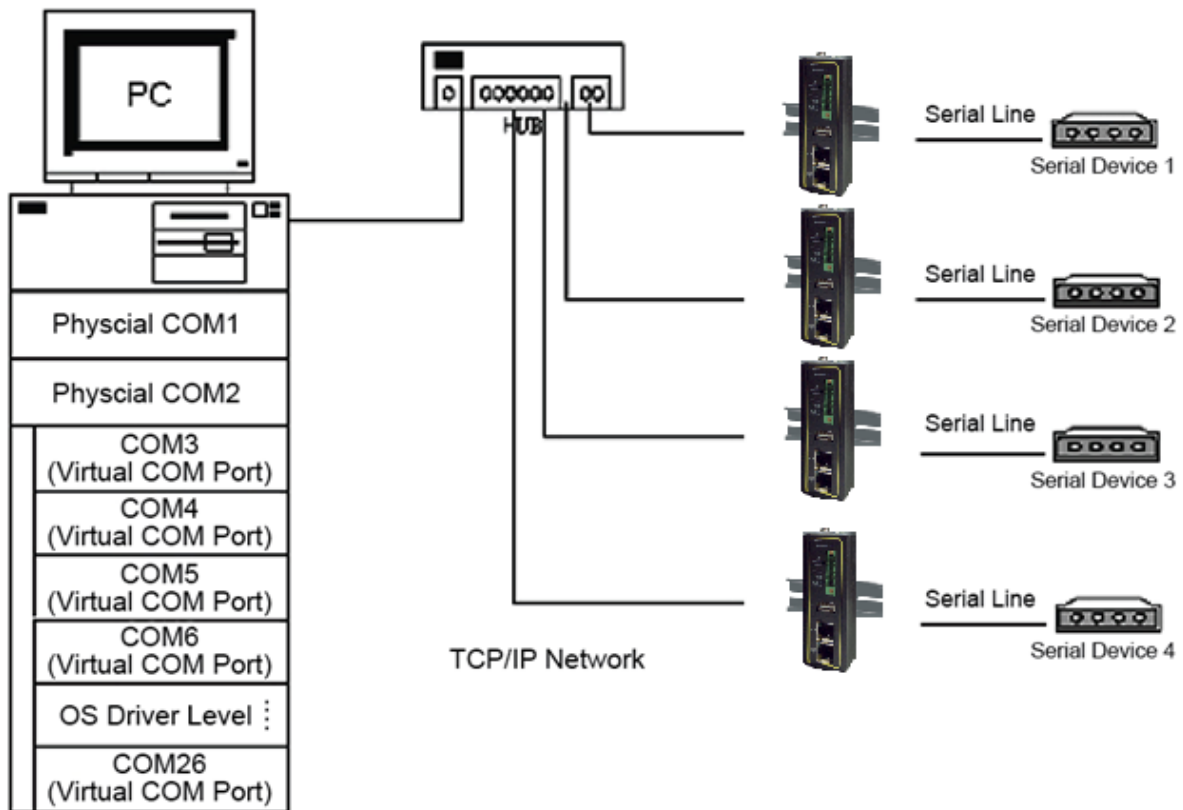


Figure 6.3 An Example Diagram of Virtual COM Application over TCP/IP Network

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

6.1.1 VCOM driver setup

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

System Requirements

- Windows Operating System Supported Platform (32/64 bits)
 - Win10
 - Win8
 - Win7
 - Vista
 - XP
 - 2008
 - 2003 (also Microsoft 2003 Terminal Server)
 - 2000 (also Microsoft 2000 Terminal Server)
 - NT (also Microsoft NT Terminal Server)
 - 4.0
 - 9x
 - Citrix MetaFrame Access Suite
- Linux operating system also available, but first you might need to download a separate package called Virtual COM driver for Linux (TTYredirector) available for download on Atop website or in the product CD. The zipped package includes a binary file for installation and a manual for Linux systems.

6.1.2 Limitation

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

6.1.3 Installation

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

6.1.4 Uninstallation

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

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

This section will provide the procedure to enable Virtual COM (VCOM) on SE59XX and Windows based PC. Please follow the steps described here to configure your Virtual COM application.

6.2.1 Enable VCOM in Serial Device servers

Enable **Virtual COM** in our serial device servers (i.e. SE59XX) by logging into the Web UI. It is located under **COM 1** or other **COM** configuration under **Serial** menu as described in Section 5.2.1.

Figure 6.4 shows how to enable **Virtual COM** in **TCP Server Link Mode** in SE59XX. For a detail of **Link Mode** configuration with **Virtual COM**, please refer to the previous chapter starting from Section 5.1.

LINK Mode

To choose specific working mode for COM 2 port.

☒ TCP Server ☐ TCP Client ☐ UDP

TCP Server	
Application	Virtual COM
IP Filter	<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 6.4 Enable Virtual COM Application for COM 2 in TCP Server Link Mode

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

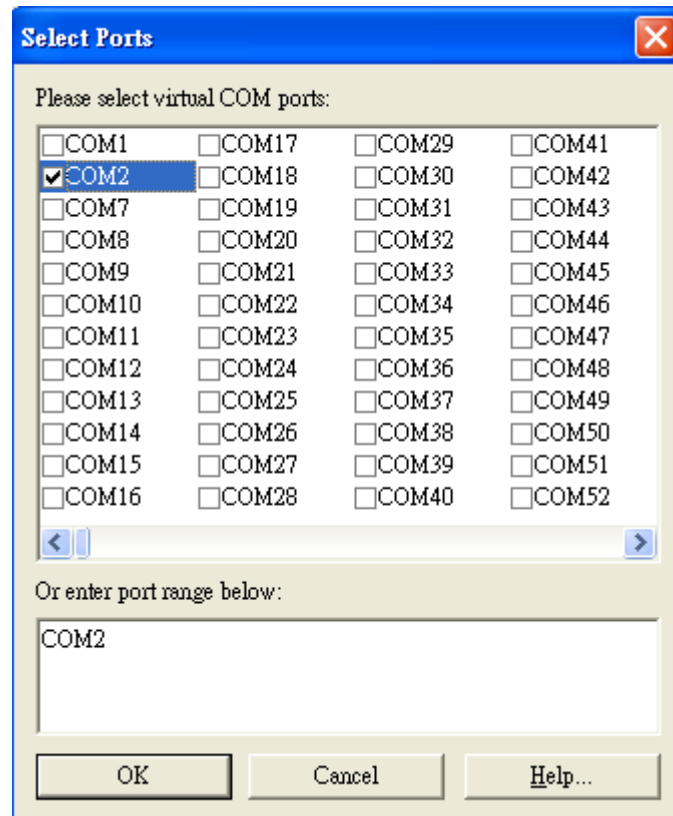


Figure 6.6 A Pop-up Window for Selecting Virtual COM Ports

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

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

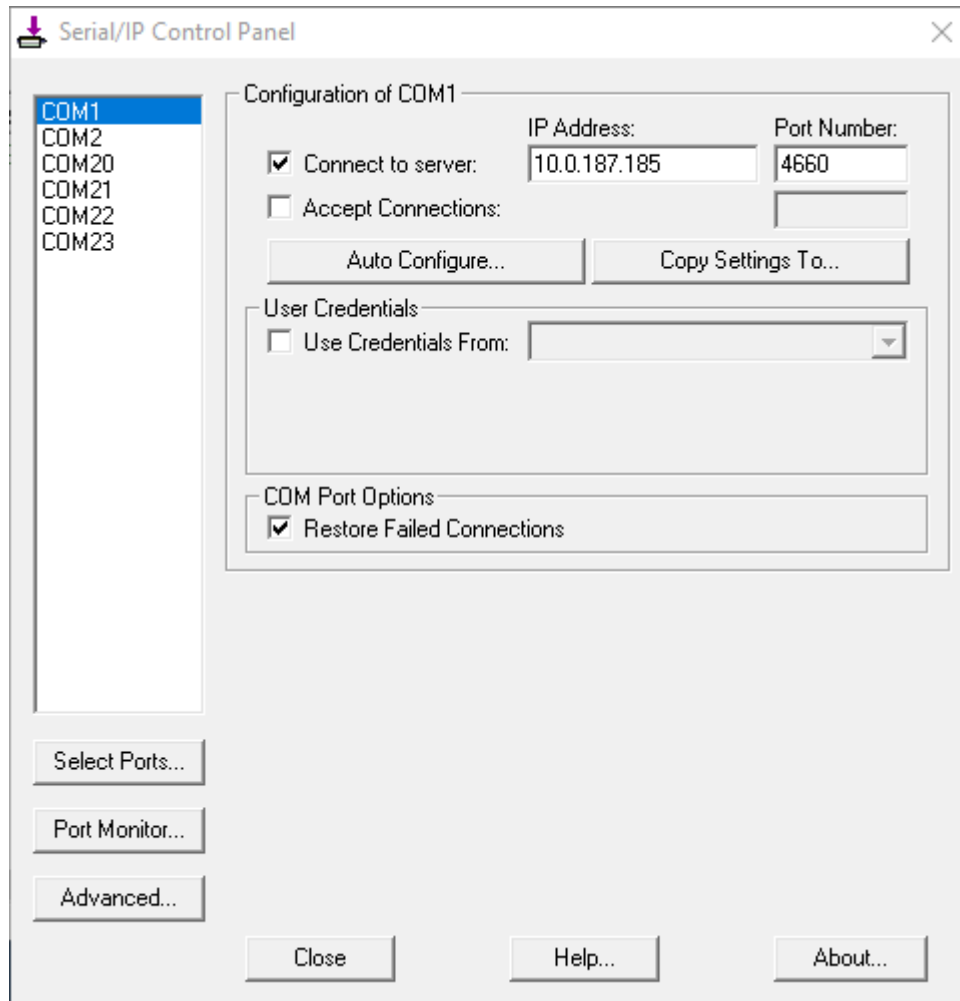


Figure 6.7 Serial/IP Control Panel Window

6.2.3 Configuring VCOM Ports

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

1. If the serial device server (i.e. SE59XX) is running in **TCP Server Link Mode** (recommended), the **Serial/IP** utility on the host computer should be configured as the TCP client connecting to the serial device server. Enable **Connect to Server** option (by checking the box in front of it as shown in Figure 6.9) and enter the IP Address of the serial device server with the specified **Port Number**. The **Port Number** here is the **Local Listening Port** for the serial device server which is specified in the **Local Port** field of Figure 5.11.
2. If the serial device server (i.e. SE59XX) is running in **TCP Client Link Mode**, the **Serial/IP** utility on the host computer should be configured as the TCP server waiting for a serial device server to connect to the host computer. Enable **Accept Connections** option (by checking the box in front of it) and enter the specified **Port Number**. This **Port Number** is the **Destination Port** of the serial device server. Do not enable **Connect to Server** option and **Accept Connections** option simultaneously.
3. Under **User Credentials** box, you can enable **Use Credentials From:** option by checking the box in front of it then select options from the drop-down list. The available sources of credentials are: **Prompt on COM Port Open**, **Prompt at Login**, and **Use Credentials Below** as shown in Figure 6.8. If you select **Use Credentials Below** option as shown in Figure 6.9, please specify the **Username** and the **Password** in their corresponding text boxes.

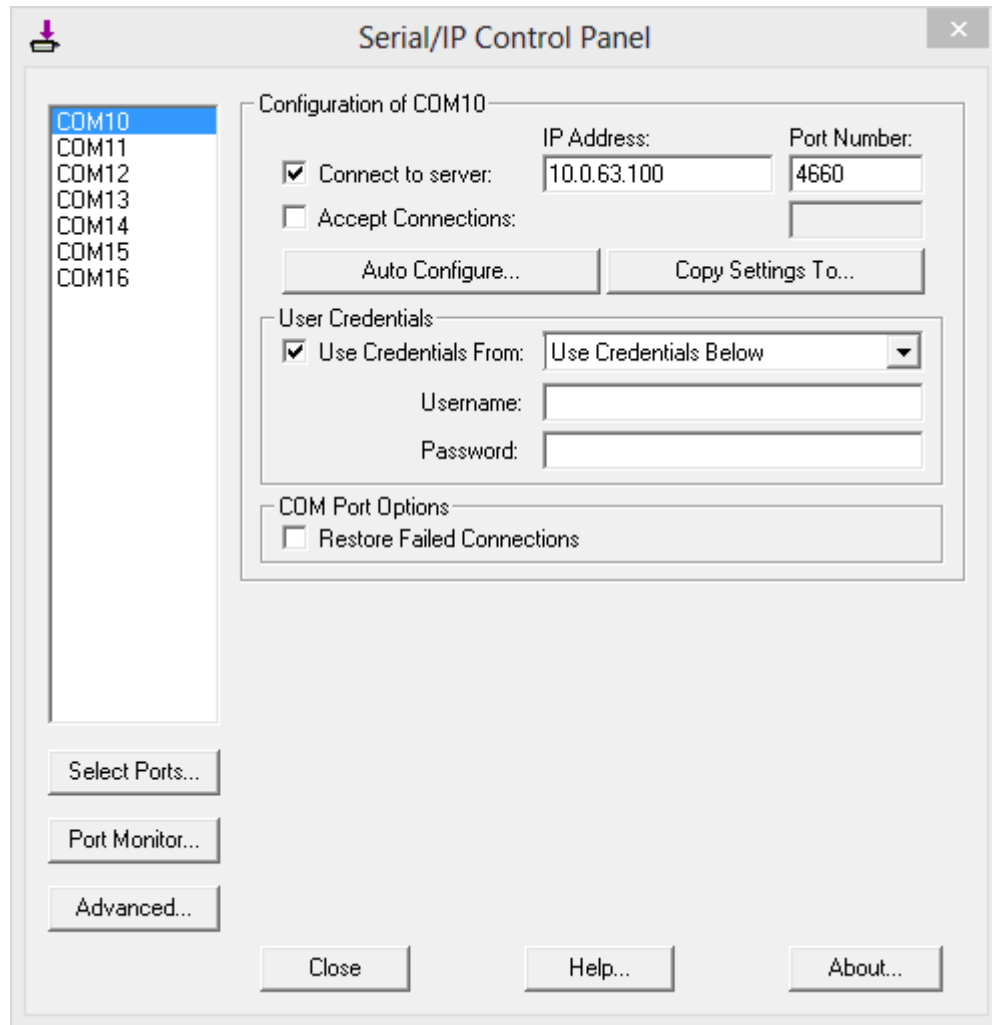


Figure 6.8 Available Options for Use Credential From in Serial/IP Control Panel Version 4.9.10

4. Under **COM Port Options** box, you can enable **Restore Failed Connections** option by checking the box in front of it to force Virtual COM to automatically restore failed connections with the serial device server in case of unstable network connections.
5. To test the Virtual COM connection, you can click the **Auto Configure...** button and then click the **Start** button in the pop up window as shown in Figure 6.10. If the test passes, all checks under the **Status** text box should be green. In this **Configuration Wizard** window, you can change the **IP Address** of Server, **Port Number**, **Username** (if **Use Credential** option is enabled), and **Password** (if **Use Credential** option is enabled). To apply the changes in the Configuration Wizard window to the Serial/IP Control Panel, please click on **Use Settings** button at the bottom of the window in Figure 6.10. You can also click on **Copy** button to copy the results to the PC system clipboard.
6. To transfer the settings between Virtual COM ports, click on the **Copy Settings To** button as shown in Figure 6.9.

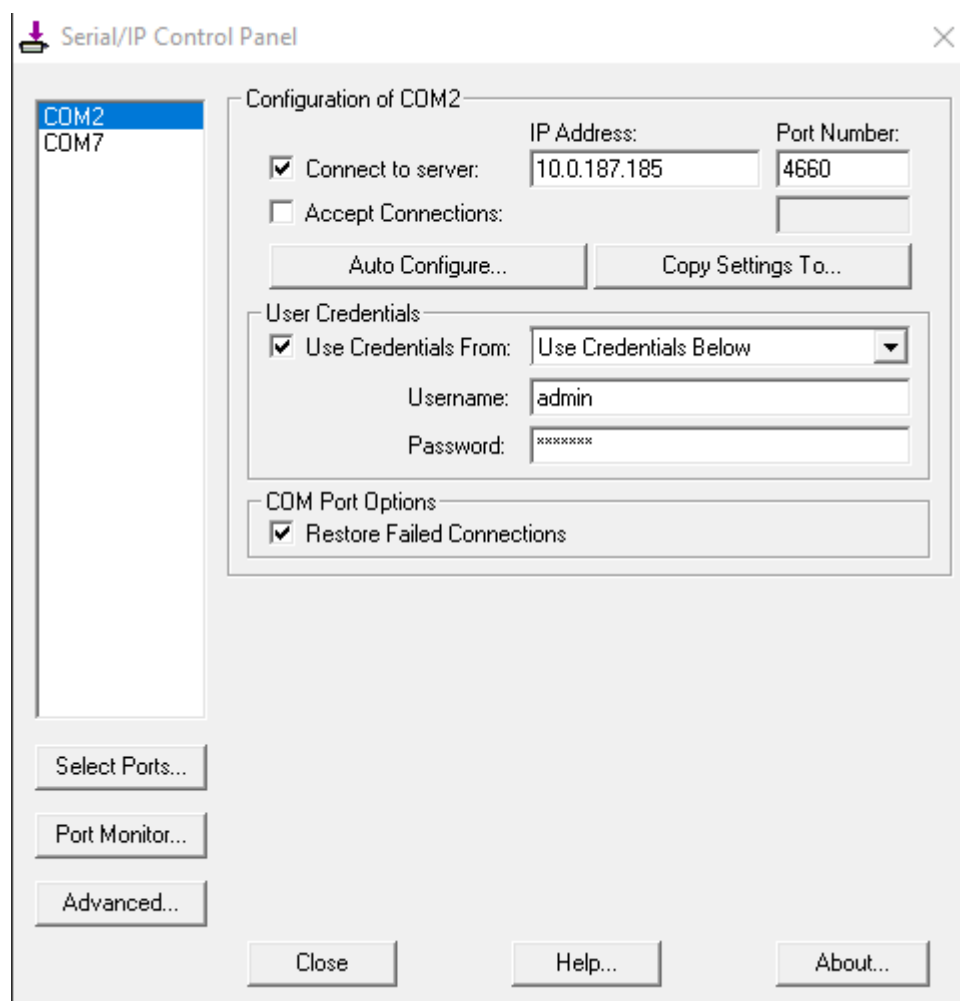


Figure 6.9 Configuring Virtual COM 2 Port as TCP Client

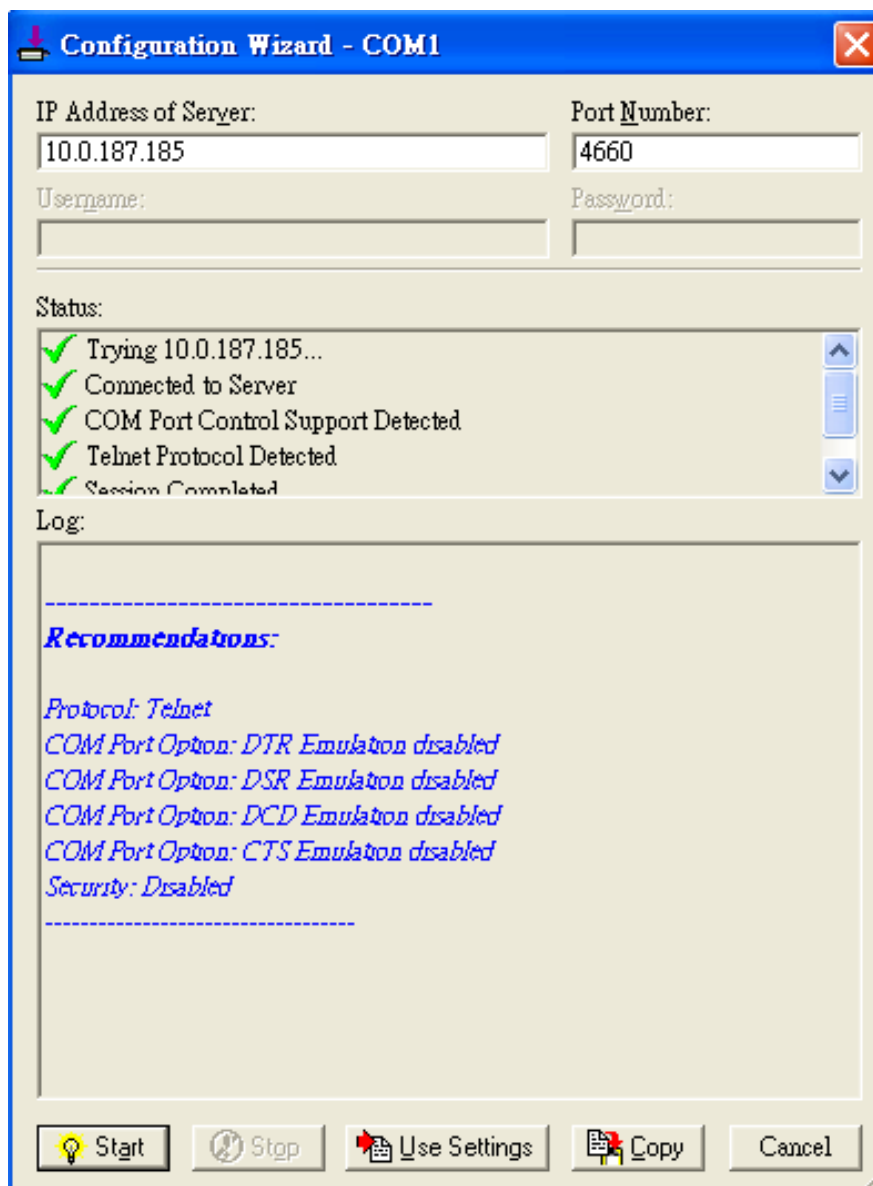


Figure 6.10 Auto Configure (formerly Configuration Wizard) Window for COM 1

6.3 Exceptions

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

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

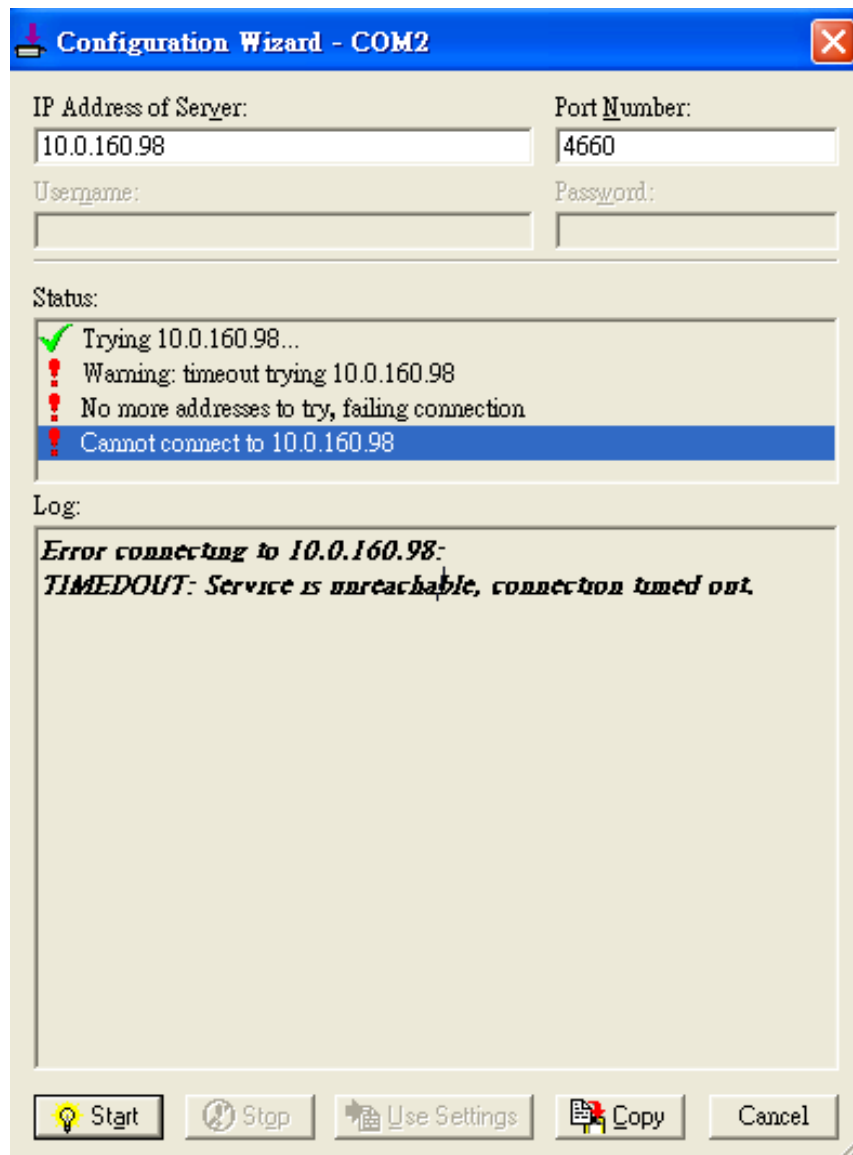


Figure 6.11 Timeout Warning on VCOM Connection

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

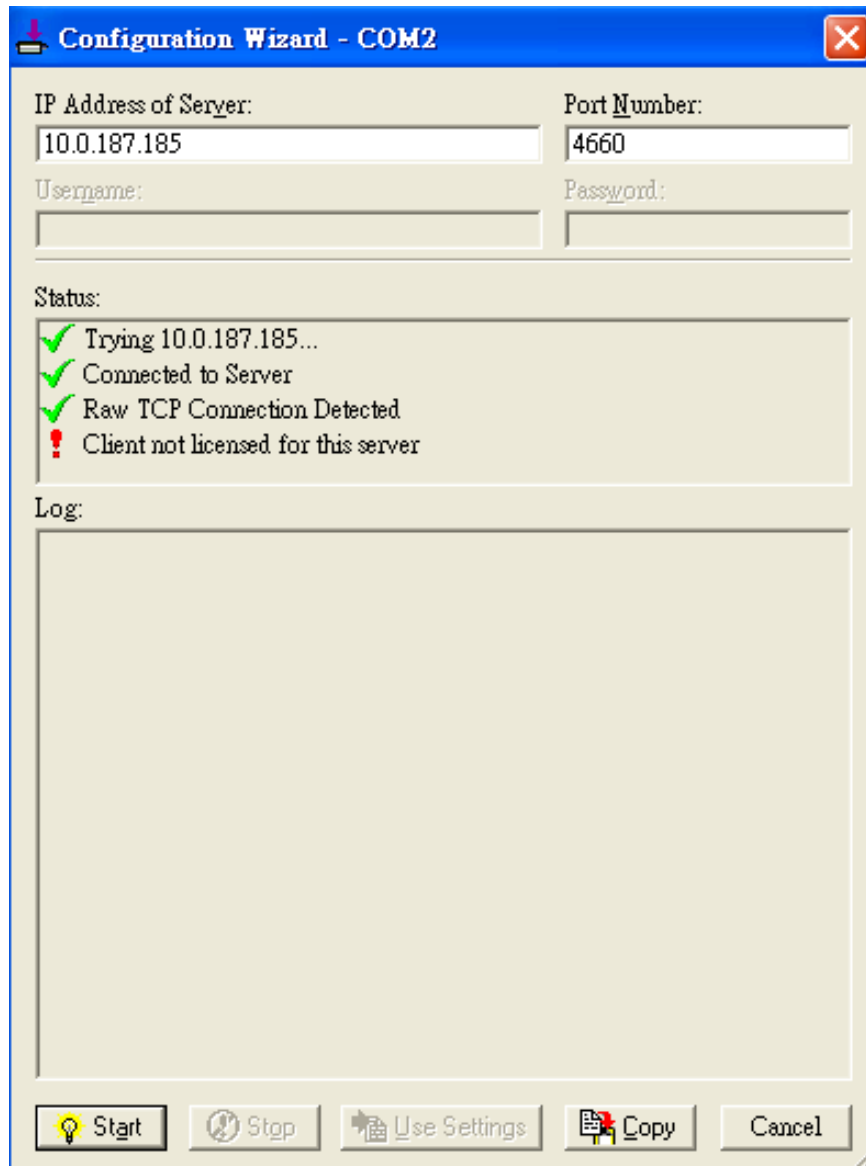


Figure 6.12 Error of Client not licensed for this server

- If the status reports with a check with a message **“Telnet Protocol Detected”** and an exclamation mark with a message **“Client not licensed for this server”** as shown in Figure 6.13. This means that there is a licensing issue between the serial gateway (i.e. SE59XX) and the Serial/IP Utility Software. Please contact Atop technical support to obtain the correct VCOM software.

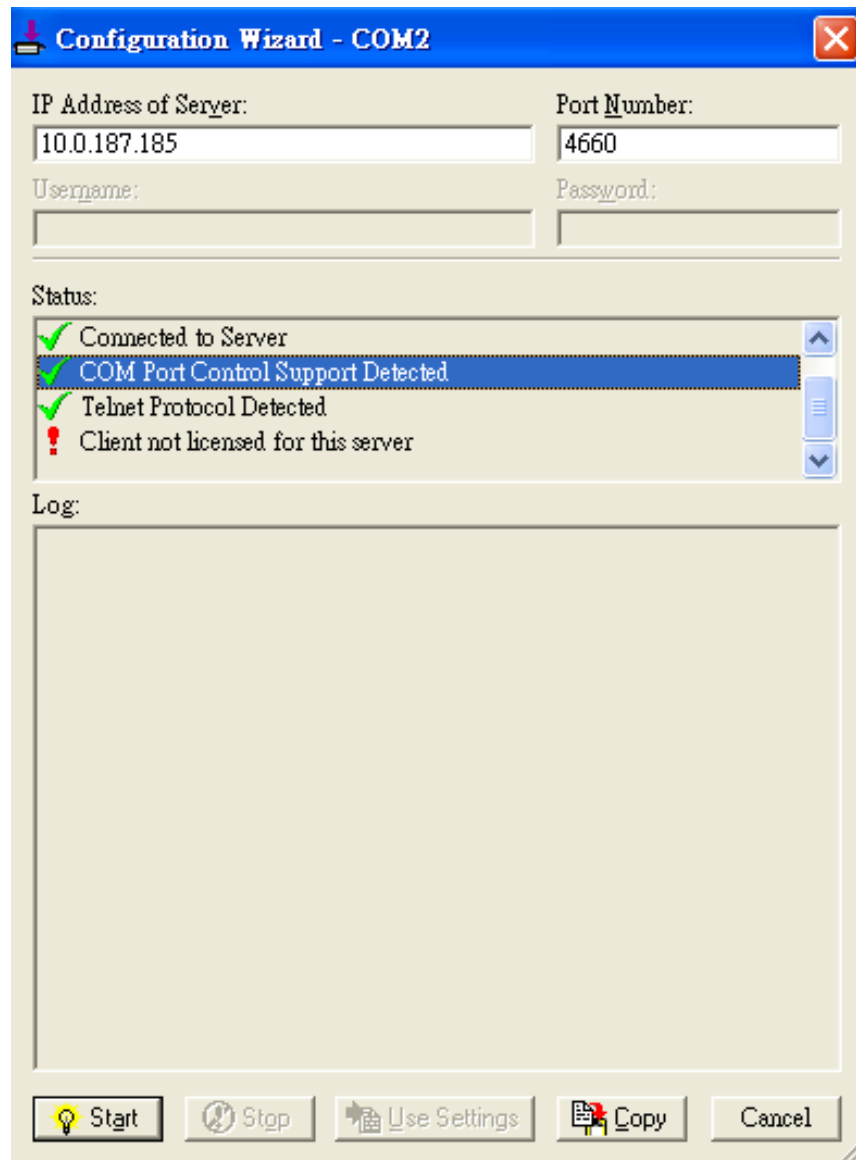


Figure 6.13 Licensing Issue of Serial/IP Utility Software

- If the status reports with an exclamation mark with a message “**Server requires username/password login**” as shown in Figure 6.14. This means that the **VCOM Authentication** option in the serial device server (i.e. SE59XX) is enabled but the **User Credentials** option in the **Serial/IP** utility software is not enabled. Please follow the steps in Section 4.17.2 for enabling the user credentials option and entering the username and the password.

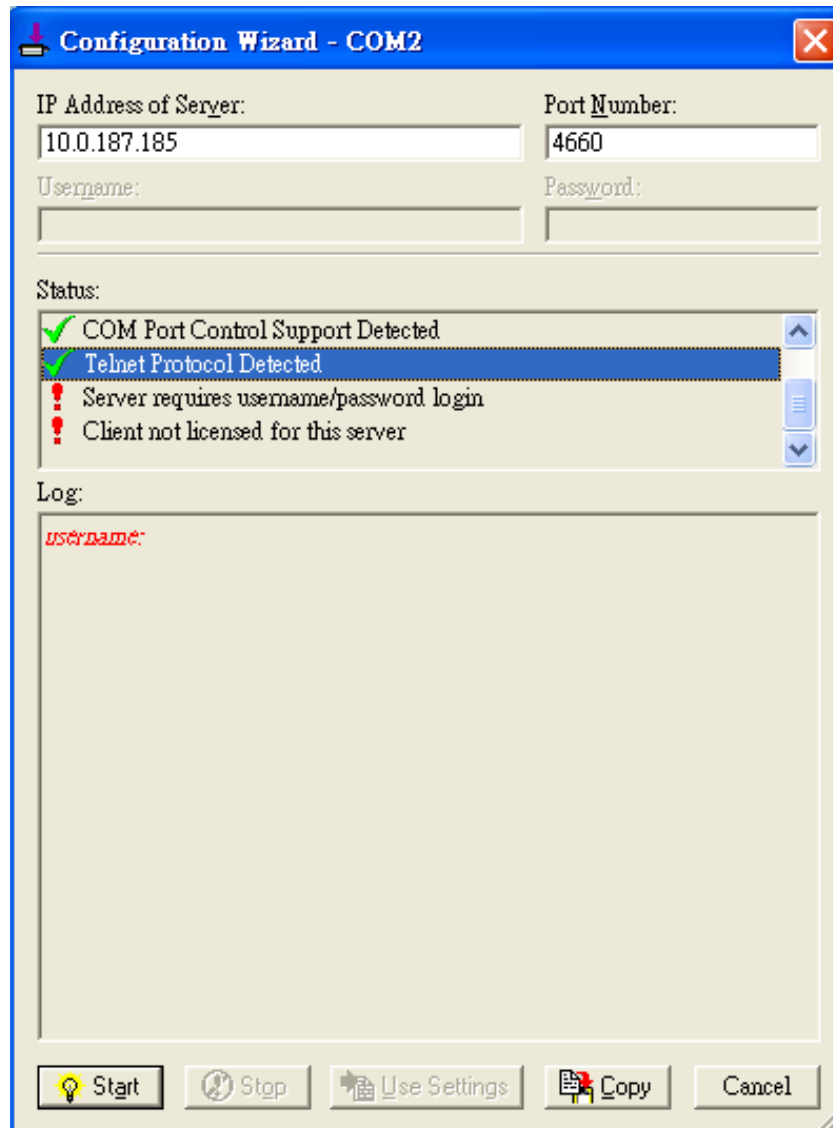


Figure 6.14 VCOM Authentication failed due to Missing Username/Password

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

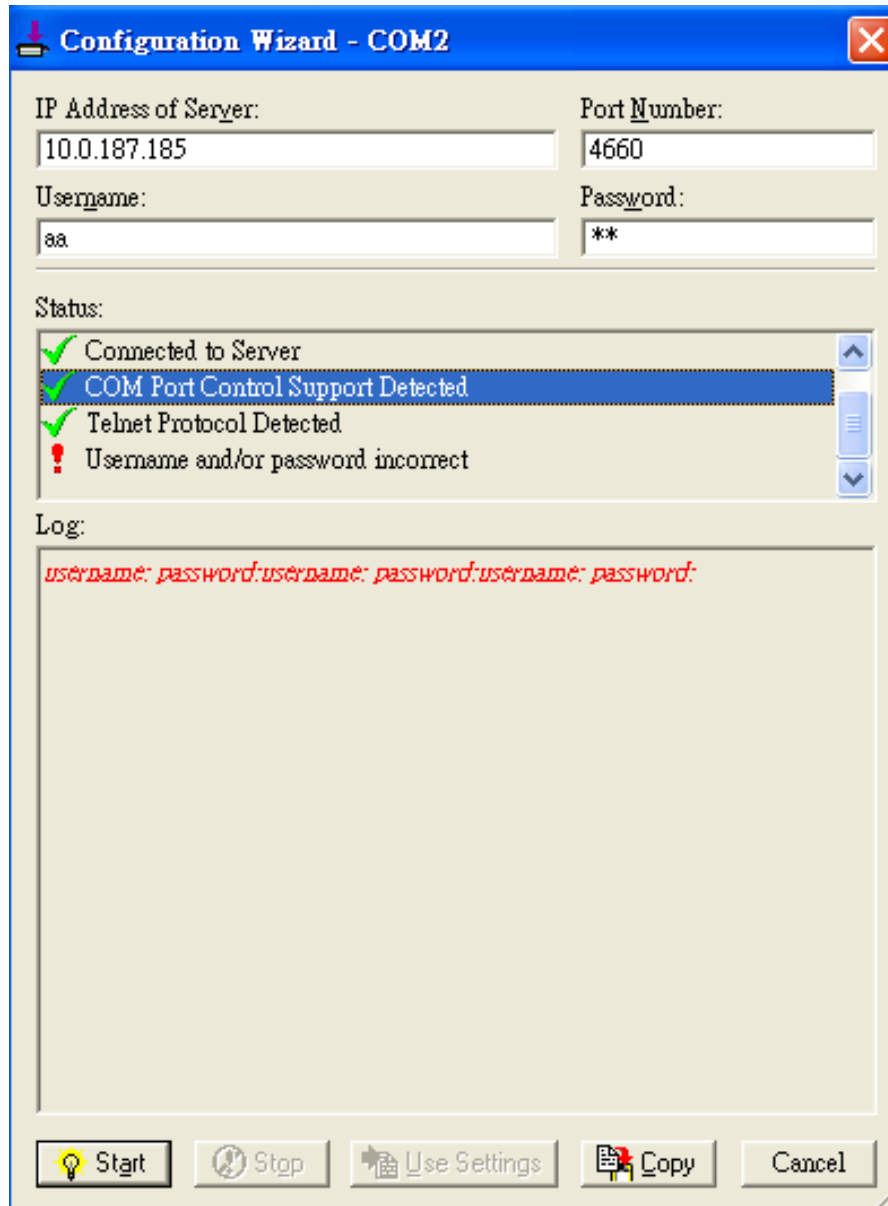


Figure 6.15 VCOM Authentication failed due to incorrect Username and/or Password

- If the status reports with an exclamation mark with a message “**No login/password prompts received from server**” as shown in Figure 6.16. This means that the **User Credentials** option in the Serial/IP utility software is enabled but the VCOM Authentication option in the serial device server (i.e. SE59XX) is not enabled. Please enable the **VCOM Authentication** option on the SE59XX by setting a new and non-blank administrator’s Username and Password for SE59XX as described in Section 4.17.2. Note that the **Username** and the **Password** for VCOM authentication are the same username and password of SE59XX 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.

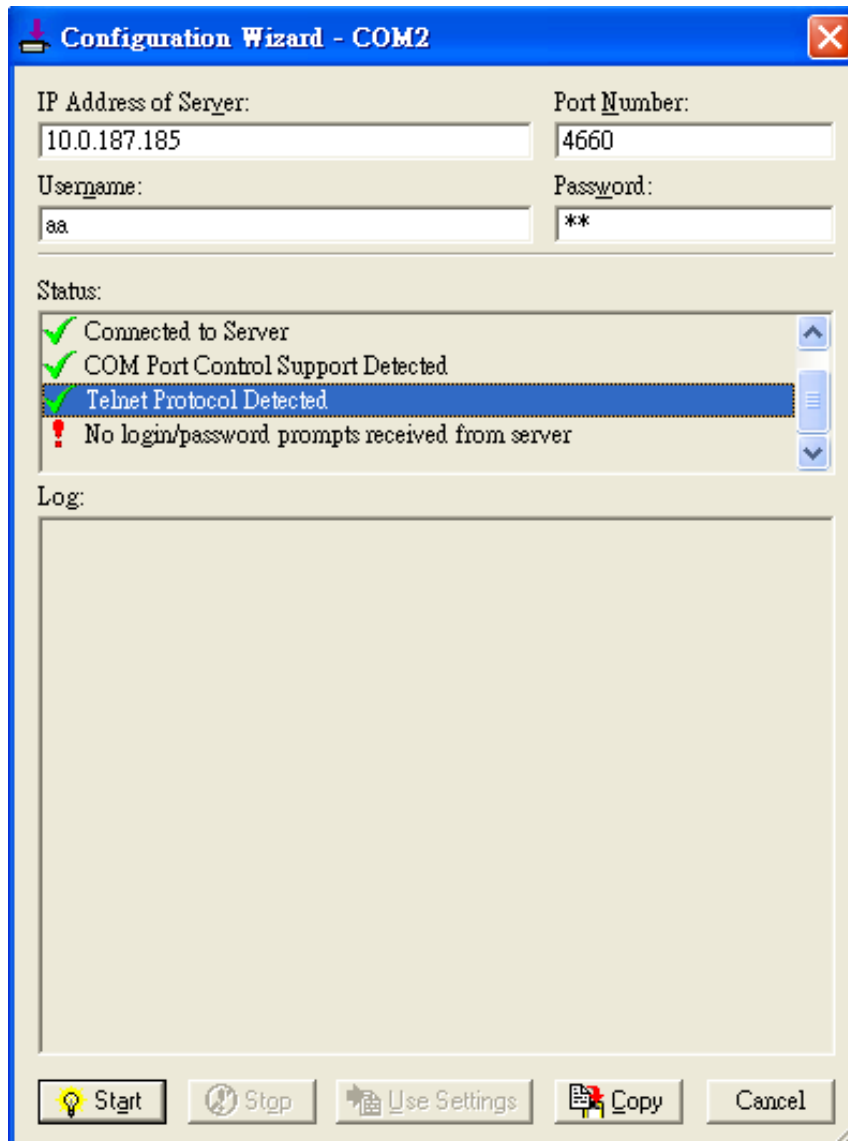


Figure 6.16 VCOM Authentication failed due to disabled VCOM Authentication on SE59XX

6.4 Using Serial/IP Port Monitor

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

6.4.1 Opening the Port Monitor

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

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

6.4.2 The Activity Panel

The **Activity** panel provides a real-time display of the status of all Serial/IP COM ports as shown in Figure 6.17. If the Virtual COM Port is opened and is properly configured to connect to a serial device server (i.e. SE59XX), the status would be **Connected**. If Serial/IP utility software cannot find the specified serial device server, the status would be **Offline**.

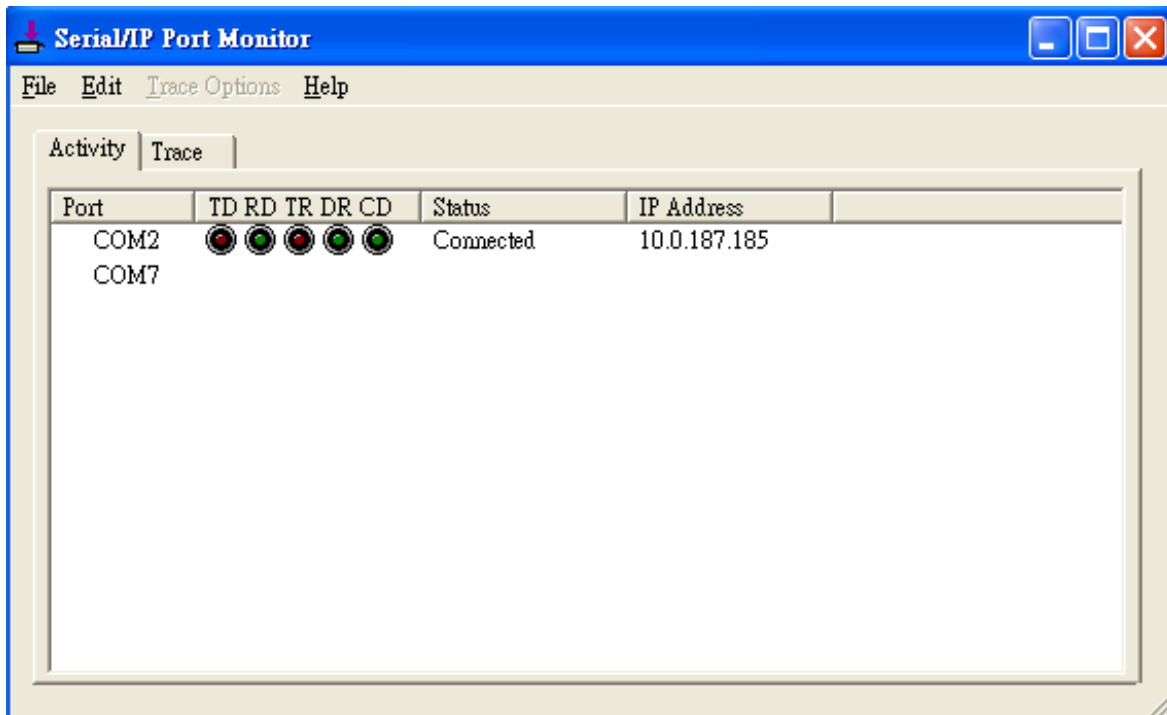


Figure 6.17 Activity Panel of Serial/IP Port Monitor

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

- **Port:** This is the virtual COM port number.
- **Line signal indicators:** Red color means no activity while green color indicates activity.
 - **TD** indicates data are being sent to the server.

- **RD** indicates data are being received from the server.
- **TR** (DTR) is the signal from the application to the server that the application has opened the virtual COM port. The most common use of DTR is to programmatically lower it to signal a modem to disconnect.
- **DR** (DSR) is the signal from the server to the application that a modem or serial device is connected to the server and ready to communicate.
- **CD** (DCD) is the signal from the server to the application that a modem has successfully negotiated a connection with another device.

■ **Status:** This indication the connection status of the software and serial device server which can be **connected** or **offline**.

■ **IP Address:** This is the IP address of the serial device server.

Notes:

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

6.4.3 The Trace Panel

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

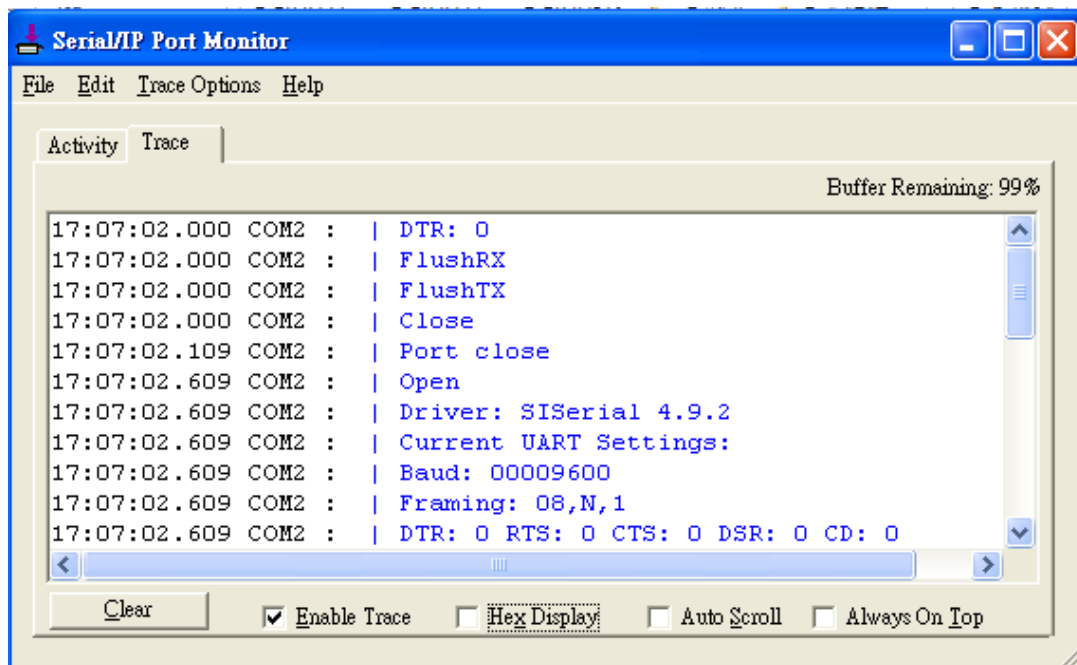


Figure 6.18 Trace Panel of Serial/IP Port Monitor

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

- **File:** To save the log file which you can send the log to Atop for further analysis if problems occurs with the Virtual COM connection, please click on **File** menu then click **Save As**.
- **Trace Options:**
 - **Select Ports to Capture...:** This menu allows you to reduce the number of ports that are being traced to a subset of all configured Virtual COM ports. This feature can reduce the impact of tracing on memory and system performance for large applications.
 - **Select Ports to Display...:** This menu allows you to reduce the number of ports that appear in the display to a subset of the ports being captured. For large applications, this feature provides a way to focus on ports of interest among all those being captured.
 - **Buffer Size:** This menu allows the change on the amount of RAM being used for tracing which can be normal or large.
 - **System Debug Output:** This menu allows user to enable the sending of trace data to the system debug channel and optionally put a label on them.

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

6.5 Serial/IP Advanced Settings

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

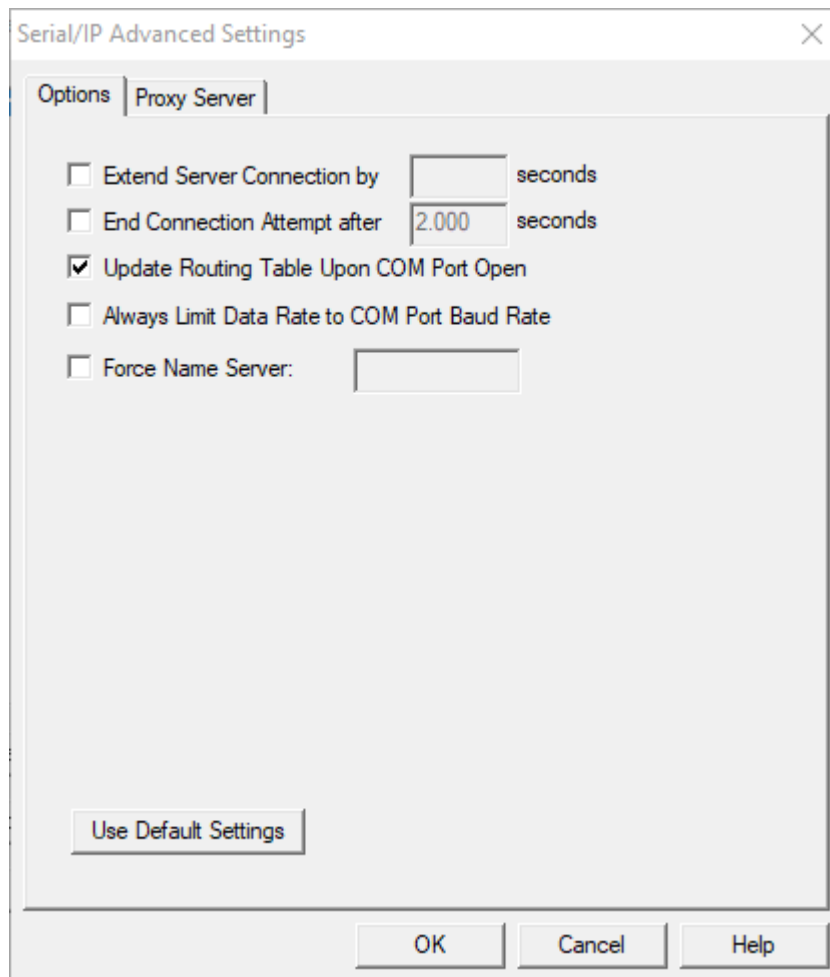


Figure 6.19 Serial/IP Advanced Settings Window

6.5.1 Advanced Setting Options

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

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

- **Always Limit Data Rate to COM Port Baud Rate:** When enabled, this option limits the data rate to the baud rate that is in effect for the virtual COM port.
- **Force Name Server:** This option allows the user to enter the desired Name Server IP address.

6.5.2 Using Serial/IP with a Proxy Server

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

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

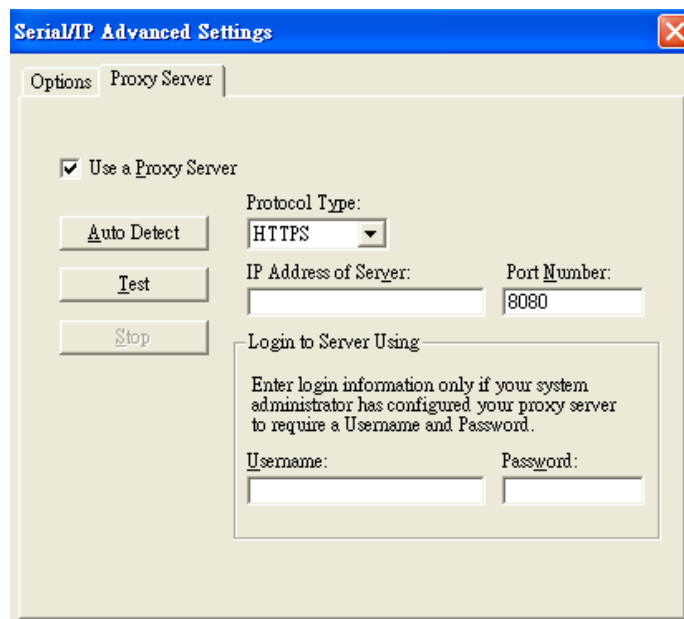


Figure 6.20 Proxy Server Tab under Serial/IP Advanced Settings

7 Specifications

7.1 Hardware

Table 7.1 Hardware Specification

System			
CPU	32-bit ARM Based TI CPU AM3354 800MHz (except SE5908A/SE5916A use AM3352 1GHz)		
Flash Memory	32MB		
RAM	SE5901 DDR2 128MB SE5901B DDR2 256MB SE5904D DDR3 256MB SE5908A/16A/MB5908/16 DDR3 256MB		
EEPROM	8 KB		
Reset	Built-in Recessed Key (Restore to Factory Defaults)		
Watchdog	Hardware built-in		
Network			
Ethernet Interface	IEEE 802.3 10BaseT IEEE 802.3u 100BaseT(X) IEEE 802.3ac 1000BaseT(X) – SFP version of SE5904D only IEEE 802.3af (PoE PD) –selected SE5901 and SE5904D versions can be powered through PoE Connection: SFP or RJ45		
Protocol	ICMP TCP UDP IPv4 HTTP Syslog	DNS DHCP Client SNMPv1, v2c, v3 RADIUS	SMTP NTP ARP Telnet RFC2217
Security	<ul style="list-style-type: none">VPN through IPsec tunnelling (max 64 tunnels) on LAN (software based)		
Serial			
Serial Interface	RS-232/RS-422/RS-485 Software Selectable (Default: RS-232) <ul style="list-style-type: none">The first port available on SE5901B is RS-232/RS-485The second port available on SE5901B-IO-X is only RS-232The isolation version (-SiS) on SE5908/SE5916/SE5908A/SE5916A supports only RS-422/ RS-485		
Serial Connector	Connector Type <ul style="list-style-type: none">SE5916 -16 Serial Ports (RJ45)SE5908 - 8 Serial Ports (RJ45)SE5916A – 16 Serial Ports (TB-5 or DB-9)SE5908A – 8 Serial Ports (TB-5 or DB-9)SE5904 – 4 Serial Ports (TB-5 or DB-9)SE5901 – 1 Serial Port (TB-5 or DB-9)SE5901B – 1 Serial Port (TB-14 or DB-9) – includes I/O		
Protection	SE5901/SE5901B no isolation SE5904D/ SE5908A/16A (optional 3V) SE5908/16 (optional 2.5kV)		

Serial Port Communication	Baud-rate: 1200 bps ~ 921600 bps Parity: None, Even, Odd, Mark, or Space Data Bits: 5, 6, 7, 8 Stop Bits: 1, 2 Software Selectable Flow Control: RTS/CTS (RS-232 only), XON/XOFF, None
LED Indicator	
LED indication	Power x 2 (SE5901- SE5901B – SE5908 – SE5916 x 1) RUN x 1 ALARM x 1 LAN: <ul style="list-style-type: none">x 2 (all versions except SE5908A and SE5916A)x 6 (SE5908A and SE5916A only) COM port: <ul style="list-style-type: none">x 16 (SE5916 and SE5916A);x 8 (SE5908 and SE5908A);x 4 (SE5904D);x 1 (SE5901 and SE5901B)
Power Requirement & EMC	
Input	SE5908/ SE5916 : <ul style="list-style-type: none">Single 100~240 VAC (EU/US versions)Single 24~48 VDC (DC version) SE5908A/ SE5916A <ul style="list-style-type: none">Redundant 100~240 VAC or 100~370 VDC (TB)– HV vers.Redundant 24~48 VDC- DC version SE5901/SE5901B : Single 9~48 VDC SE5904D : Redundant 9~48 VDC
Consumption	Max.17.5 W (SE5908 /SE5916) Max. 6W (SE5901) Max. 7.8W(SE5904D) Max. 17.5W(SE5908A/SE5916A) Max. 7.2W(SE5901B)
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 IEC 61850-3 / IEEE 1613 (SE5908A and SE5916A only)
Mechanical	
Dimensions (W x H x D, mm)	SE5901: 32 mm x 110 mm x 90 mm (1.26 x 4.33 x 3.54 in) SE5901B: 32 mm x 122mm x 92 mm (1.26 x 4.8 x 3.62 in) SE5904D: 55 mm x 145 mm x 113mm (2.17 x 5.17 x 4.45 in) SE5908: 436 mm x 43.5 mm x 200 mm (17.17 x 1.71 x 7.87 in) SE5916: 436 mm x 43.5 mm x 200 mm (17.17 x 1.71 x 7.87 in) SE5908A: 440.6mm x 44 mm x 309 mm (17.35 x 1.73 x 12.17 in) SE5916A: 440.6mm x 44 mm x 309 mm (17.35 x 1.73 x 12.17 in)
Enclosure	IP30 protection, metal housing
Environmental	
Temperature	Operations -40°C ~ 85°C (-40°F ~ 185°F) (except SE5901B -40°C ~ 70°C and SE5908/SE5916 -20°C ~ 70°C)
	Storage -40°C ~ 85°C (-40°F ~ 185°F)
Relative Humidity	5% ~ 95%, 55°C Non-condensing

7.2 Serial port Pin Assignments

7.2.1 SE5901 Pin Assignments for Serial Interfaces

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

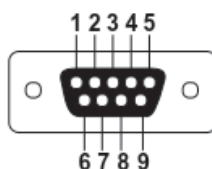


Figure 7.1 DB9 Pin Number

Table 7.2 SE59XX Pin Assignment for DB9 to RS-232/RS-422/RS-485 Connector

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

1 x 5-pin (Male Terminal Block) for RS-232/RS-422/RS485 Connector

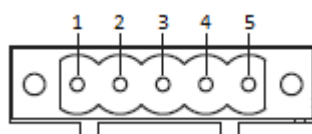


Figure 7.2 TB5 Pin Number

Table 7.3 SE59XX Pin Assignment for TB5 to RS-232/RS-422/RS-485 Connector

Pin#	RS-232 Full Duplex	RS-422/4-Wire RS-485 Full Duplex	2-Wire RS-485 Half Duplex
1	RxD	T+	NC
2	CTS	T-	NC
3	TxD	R+	Data+
4	RTS	R-	Data-
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)

7.2.2 SE5904D Pin Assignments

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

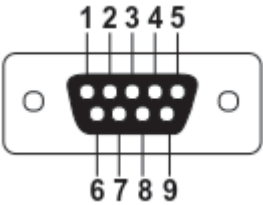


Figure 7.3 DB9 Pin Number

Table 7.4 MB5904D Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors

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

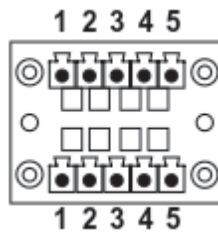
5-Pin Terminal Block to RS-485/RS-422 connectors

Figure 7.4 Terminal Block (TB-5) Pin Number

Table 7.5 MB5904D Pin Assignment for 5-Pin Terminal Block to RS-232/RS-422/RS-485 Connectors

Pin#	RS-232	RS-422 4-Wire RS-485	2-W RS-485
1	RxD	TxD+	Data+
2	CTS	TxD-	Data-
3	TxD	RxD+	N/A
4	RTS	RxD-	N/A
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)

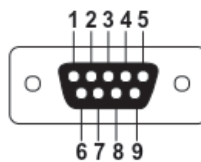
7.2.3 SE5901B Pin Assignments**DB9 to RS-232/RS-485/RS-422 connectors**

Figure 7.5 DB9 Pin Number

Table 7.6 MB5901B Pin Assignment for DB9 to RS-232/RS-485 Connector

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

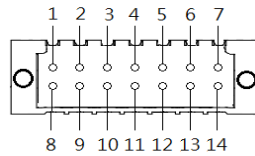
2 x 7-pin Male Terminal Block for RS-232/485(COM 1),RS-232(COM 2) Relay and DI

Figure 7.6 2 x 7-pin Male Terminal Block

Table 7.7 SE5901B 2 x 7-pin Male TB for RS-232/485(COM 1),RS-232(COM 2) Relay and DI pin-assignment

Pin#	DI and Relay	COM1 (RS-232)	COM1 (RS-485)	COM2 (RS-232)
1	DI1	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>
2	DI2	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>
3	Relay 1 -	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>
4	Relay 1+	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>
5	Relay 2 -	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>
6	Relay 2+	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>	<i>Dedicated for DI/DO</i>
7	<i>Dedicated for COM</i>	SG (Signal Ground)	SG (Signal Ground)	-
8	<i>Dedicated for COM</i>	Rx	-	-
9	<i>Dedicated for COM</i>	CTS	-	-
10	<i>Dedicated for COM</i>	Tx	Data +	-
11	<i>Dedicated for COM</i>	RTS	Data -	-
12	<i>Dedicated for COM</i>	-	-	SG (Signal Ground)
13	<i>Dedicated for COM</i>	-	-	Rx
14	<i>Dedicated for COM</i>	-	-	Tx

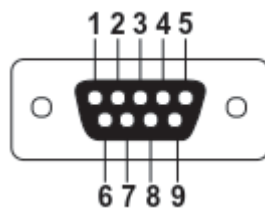
7.2.4 SE5908A/ SE5916A Pin Assignments**DB9 to RS-232/RS-485/RS-422 connectors**

Figure 7.7 DB9 Pin Number

Table 7.8 MB5908A/16A Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors

Pin#	RS-232	RS-422	RS-485
1	-	-	-
2	RxD	TxD+	Data+
3	TxD	RxD+	-
4	-	-	-
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)
6	-	-	-

7	RTS	RxD-	-
8	CTS	TxD-	Data-
9	-	-	-

5-Pin Terminal Block to RS-232/RS-485/RS-422 connectors

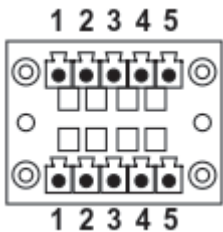


Figure 7.8 Terminal Block (TB-5) Pin Number

Table 7.9 MB5908A/16A Pin Assignment for 5-Pin Terminal Block to RS-232/RS-422/RS-485 Connectors

Pin#	RS-232	RS-422 4-Wire RS-485	2-W RS-485
1	RxD	TxD+	Data +
2	CTS	TxD-	Data -
3	TxD	RxD+	-
4	RTS	RxD-	-
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)

7.2.5 SE5908/ SE5916 Pin Assignments

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

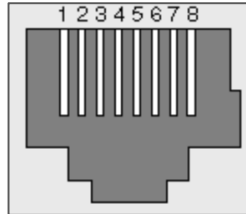


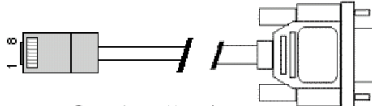
Figure 7.9 MB5908/MB5916 Serial port on RJ45 Pin Numbering

Table 7.10 MB5908/16 Pin Assignment for RJ45 to RS-232/RS422/RS-485 Connectors


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

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

- 50891791G - RJ45 TO DB9 CABLE-FEMALE:

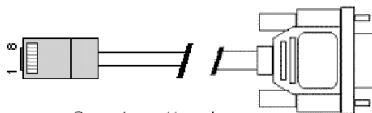
RJ45		Straight Through Female DB9		
				
RTS	Pin 1	↔	Pin 7	RTS
DTR	Pin 2	↔	Pin 4	DTR
TXD	Pin 3	↔	Pin 3	TXD
SG	Pin 4	↔	Pin 5	SG
SG	Pin 5	↔		
RXD	Pin 6	↔	Pin 2	RXD
DSR	Pin 7	↔	Pin 6	DSR
CTS	Pin 8	↔	Pin 8	CTS

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

RJ45		Cross Over Female DB9		
				
RTS	Pin 1	↕	Pin 8	CTS
DTR	Pin 2	↕	Pin 6	DSR

TXD	Pin 3	↔	Pin 2	RXD
SG	Pin 4	↔	Pin 5	GND
SG	Pin 5	↔		
RXD	Pin 6	↔	Pin 3	TXD
DSR	Pin 7	↔	Pin 4	DTR
CTS	Pin 8	↔	Pin 7	RTS

50891781G - RJ45 TO DB9 CABLE-MALE:

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

7.2.6 SE59XX Pin Assignments for LAN Interface

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

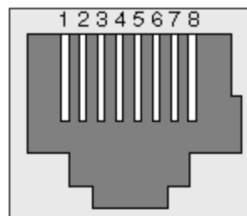








Figure 7.10 SE59XX Ethernet Port on RJ45 with Pin Numbering

Table 7.11 SE59XX Pin Assignment for RJ-45 Connector

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

7.3 LED Indicators

Table 7.12 Color Interpretation of LED Indicators of SE59XX

Name	Colour	Status	Message
PWR (Power)	 Green	Steady/On	Power On and Power is being supplied
		Off	Power Off and
TX	 Green	Blinking	COM port is transmitting data
		Off	COM port is not transmitting data
RX	 Green	Blinking	COM port is receiving data
		Off	COM port is not receiving data
RUN	 Green	Blinking	AP Firmware is running normally
		On/Off	System is not ready or halt
LAN	 Orange (Speed)	On	Ethernet is transmitting at 1 Gbps
		Blinking slowly	Ethernet is transmitting at 100 Mbps
		Off	Ethernet is transmitting at 10 Mbps
	 Green (Data)	Blinking	Ethernet data is transmitting
		Off	Ethernet has no data to transmit

7.4 Software

Table 7.13 Software Tools and Utilities

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

8 Emergency System Recovery

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

8.1 System Recovery Procedures

System recovery is based on the TFTP Client embedded in the device. It can recover the device from a bad firmware or other unknown reasons corrupting the firmware image inside the flash memory. Please follow the procedures below to force SE59XX to download a valid firmware from the TFTP Server to recover its operating system.

Table 8.1 Default Settings for System Recovery Procedure

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

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

Important Note

Free TFTP Servers can be downloaded from the following locations:

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

9 Warranty

Limited Warranty Conditions

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

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

RMA and Shipping Reimbursement

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

Limited Liability

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

Warranty

Atop Technologies Inc. provides a 5-year maximum warranty for Industrial Serial Device Server products.



Atop Technologies, Inc.

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

TAIWAN HEADQUARTER:

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

ATOP CHINA BRANCH:

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

ATOP INDIA OFFICE:

Abhishek Srivastava
Head of India Sales
Atop Communication Solution(P) Ltd.
No. 311, 6th Main Rd, Indiranagar,
Bangalore, 560038, India
Tel: +91-80-4920-6363
E-mail: Abhishek.S@atop.in

ATOP INDONESIA BRANCH:

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

ATOP EMEA OFFICE:

Prashant Mishra
Business Development (EMEA)
Atop Communication Solution(P) Ltd.
No. 311, 6th Main Rd, Indiranagar,
Bangalore, 560038, India
Tel: +91-738-702-0003
E-mail: prashant.m@atop.in

ATOP AMERICAs OFFICE:

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