

USER MANUAL

LES920 SERIES

INDUSTRIAL DEVICE SERVER SERIES



BLACK BOX®

This page intentionally left blank.

Important Announcement

The information contained in this document is the property of Black Box Corporation, and it is supplied for the sole purpose of operation and maintenance of Black Box Corporation's 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 from Black Box Corporation. 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.

Table of Contents

1	Preface	7
1.1	Purpose of the Manual	7
1.2	Who Should Use This User Manual	7
1.3	Supported Platform	7
1.4	FCC and IC Statements	7
2	Introduction	9
2.1	Overview	9
2.2	Features	10
3	Getting Started	11
3.1	Packing List	11
3.2	Appearance, Front and Rear Panels	12
3.3	First Time Installation	13
3.4	Factory Default Settings	13
3.4.1	Network Default Settings	13
3.4.2	Other Default Settings	14
4	Configuration and Setup	15
4.1	Configuration of Network Parameters through Device Management Utility	15
4.2	UI Configuration	18
4.3	CLI Configuration	21
4.3.1	Connect to CLI	21
4.3.2	General Information of CLI	23
4.3.3	Network Configuration	24
4.3.4	LAN Setting	25
4.3.5	DNS Settings	26
4.3.6	Default Gateway Settings	26
4.3.7	Firewall Settings	27
4.3.8	IP Filter Setting	28
4.3.9	COM Port Settings	29
4.3.10	Link Mode Settings	30
4.3.11	Application of the Link Mode	32
4.3.12	SNMP Settings	33
4.3.13	Alert Settings	34
4.3.14	E-mail Settings	35
4.3.15	Spanning Tree	36
4.3.16	System Setup	37
4.3.17	Exit and Disconnect	39
4.3.18	Restore to the Factory Default	40
4.4	Configuring Automatic IP Assignment with DHCP	41
4.5	Web Overview	41
4.6	Wizard	42
4.7	Network Settings	48
4.8	Serial	50
4.8.1	COM Port Overview	50
4.8.2	COM Configuration	52
4.8.3	COM Configuration: Advanced Settings	53
4.9	SNMP/ALERT Settings	56

4.10	E-Mail Settings.....	58
4.11	VPN	59
4.11.1	PPPTP Settings.....	60
4.11.2	PPPTP Status.....	61
4.11.3	IPsec.....	62
4.11.4	IPsec Settings.....	66
4.11.5	IPsec Status.....	71
4.11.6	Examples of IPsec Settings	72
4.11.7	Host-to-Host Connections	72
4.11.8	Host-to-Network Connections	73
4.11.9	Network-to-Network (Subnet-to-Subnet) Connections	75
4.11.10	OpenVPN Setting	77
4.11.11	OpenVPN Keys	79
4.11.12	OpenVPN Status	81
4.12	Log Settings.....	83
4.12.1	System Log Settings	83
4.12.2	System Log	84
4.12.3	COM Log Settings.....	85
4.12.4	COM log	87
4.13	System Setup.....	87
4.13.1	Date/Time Settings	88
4.13.2	Admin Settings	90
4.13.3	Firmware Upgrade.....	90
4.13.4	Backup/Restore Settings	91
4.13.5	Ping	92
4.14	Reboot.....	94
4.14.1	Auto Reboot	94
4.14.2	Manual Reboot	94
5	Link Modes and Applications.....	95
5.1	Link Mode Configuration.....	95
5.1.1	Link Mode: Configure LES920 series as a TCP Server	95
5.1.2	Link Mode: Configure LES920 series as a TCP Client.....	99
5.1.3	Link Mode: Configure LES920 series in UDP	102
5.2	Link Mode Applications.....	106
5.2.1	TCP Server Application: Enable Virtual COM.....	106
5.2.2	TCP Server Application: Enable RFC 2217 through Virtual COM.....	107
5.2.3	TCP Client Application: Enable Virtual COM.....	107
5.2.4	TCP Client Application: Enable RFC 2217 through Virtual COM.....	108
5.2.5	TCP Server Application: Configure LES920 Series as a Pair Connection Master	109
5.2.6	TCP Client Application: Configure LES920 Series as a Pair Connection Slave	110
5.2.7	TCP Server Application: Enable Reverse Telnet	111
6	VCOM Installation & Troubleshooting.....	113
6.1	Enabling VCOM.....	113
6.1.1	VCOM driver setup	115
6.1.2	Limitation	116
6.1.3	Installation	116
6.1.4	Uninstallation.....	116
6.2	Enable VCOM in Serial Device servers and Select VCOM in Windows	116
6.2.1	Enable VCOM in Serial Device servers	116
6.2.2	Running Serial/IP Software Utility in Windows®.....	117
6.2.3	Configuring VCOM Ports.....	120
6.3	Exceptions	124
6.4	Using Serial/IP Port Monitor	130

6.4.1	Opening the Port Monitor.....	130
6.4.2	The Activity Panel.....	130
6.4.3	The Trace Panel.....	131
6.5	Serial/IP Advanced Settings	133
6.5.1	Advanced Setting Options	133
6.5.2	Using Serial/IP with a Proxy Server	134
7	Specifications.....	135
7.1	Hardware.....	135
7.1.1	Pin Assignments	137
7.1.2	Pin Assignments for LAN Interface.....	138
7.2	LED Indicators	139
7.3	Software.....	139
8	Warranty.....	140
9	Tech Support/Contact Information	141

1 Preface

1.1 Purpose of the Manual

This manual supports the user during the installation and configuration of the LES920 Industrial Device Server Series. It explains the product's technical features. As such, it contains some advanced network management knowledge. Instructions, examples, guidelines, and general theories are designed to help users manage this device and its corresponding software.

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 information for first time users. For any related problems, contact Black Box technical support.

1.3 Supported Platform

This manual is designed exclusively for the **LES920 Industrial Serial Device Server series**.

1.4 FCC and IC Statements

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference- to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission- from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

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

2 Introduction

2.1 Overview

The LES920 Series is an industrial Ethernet serial device server which acts as a gateway for communications between an Ethernet (TCP/UDP) port and a RS-232/RS-422/RS-485 port. The information conveyed by the LES920 model is transparent to both host computers (Ethernet) and serial devices (RS-232/RS-422/RS-485). Data originating 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 LES920 model. In normal PCs or laptops, a virtual COM port can be created using our virtual COM software to fetch serial data from the LES920 series remotely over Ethernet.

With the LES920 series, it is possible to communicate with a remote serial device over the LAN or 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 an Ethernet interface, and a monitored device reports to the Industrial Serial Device Server via a RS-232/RS-422/RS-485 interface. It is possible to have multiple PCs connected to 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 an Industrial Serial Device Server.

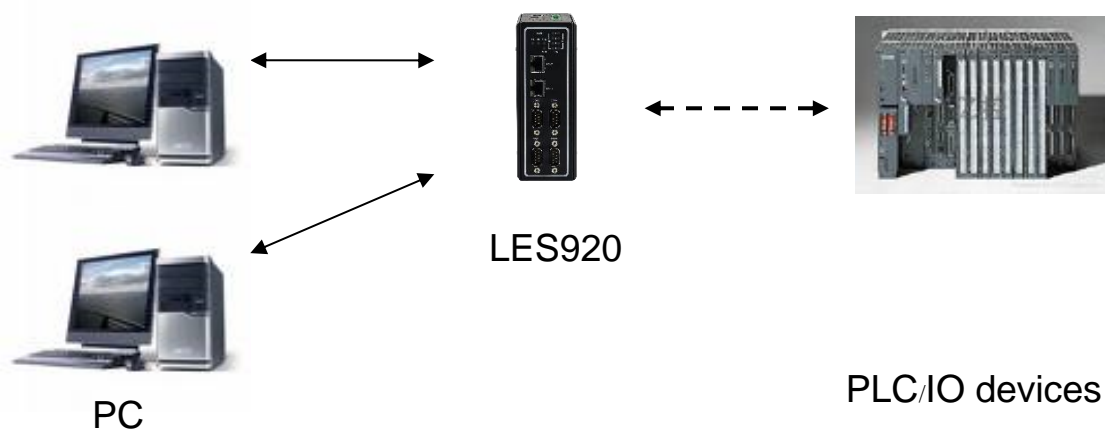


Figure 2.1 An Application of LES920 Industrial Serial Device Server with Multiple Devices

2.2 Features

The LES920 Industrial Serial Device Server series comes with a software platform. It provides:

- Flexible hardware platform with 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/Black Box 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

Table 3.1 Packing List

Item	Quantity	Description
LES920	1	Industrial Serial Device Server
Mounting Kit	1	LES920 Series - DIN Rail Kit
Terminal Block		Power Supply/Relay output: <ul style="list-style-type: none">• TB7 x1: 7-pin 5.08mm lockable Terminal Block Serial ports: Terminal block is included only on TB model <ul style="list-style-type: none">• TB5 x 4: 5-pin 5.08mm lockable Terminal Block
Documentation	1	Product insert card

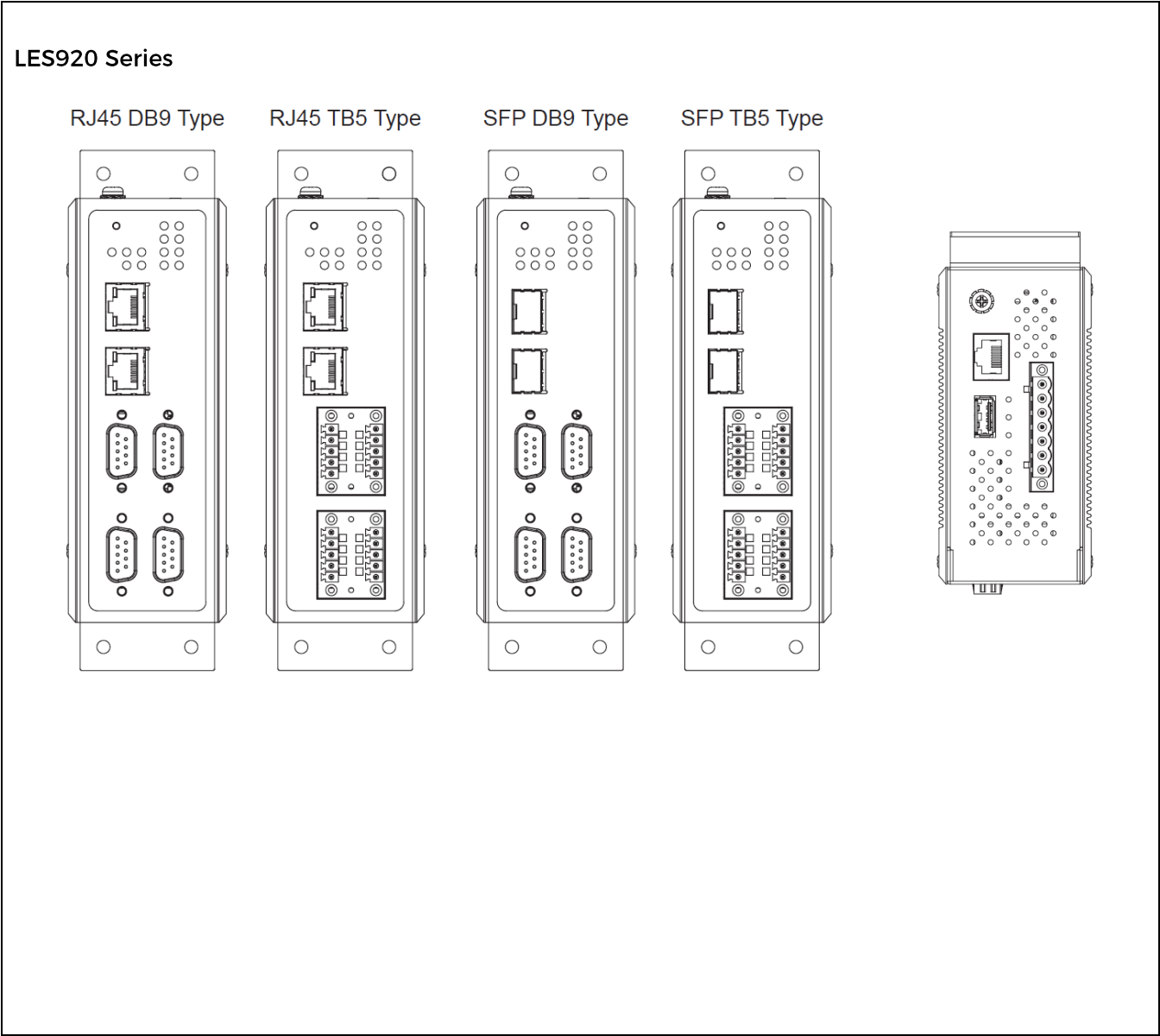
Note:

- Upon delivery, notify your sales representative immediately if any of the above items are missing or damaged.

3.2 Appearance, Front and Rear Panels

The following figure shows the LES920 series device's front and rear panels.

Table 3.2 Front and Rear Panels



3.3 First Time Installation

Before installing the device, strictly follow all safety procedures described in this manual. Black Box Corporation 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 you do not understand the steps described in the manual. In such case, contact Black Box technical support immediately.

3.4 Factory Default Settings

3.4.1 Network Default Settings

The LES920 Industrial Serial Device Server is equipped with two LAN interfaces with two default IP addresses. Its default network parameters are listed in Table 3.2.

Table 3.2 Network Default Settings

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

3.4.2 Other Default Settings

The LES920 Industrial Serial Device Server comes with the default settings listed in Table 3.4.

Table 3.3 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 4.13.4, to restore the LES920 Series Industrial Serial Device Server to factory default settings.

4 Configuration and Setup

We strongly recommend that you set the Network Parameters through the **Device Management Utility**® before using the product. Other device-specific configurations can later be carried out via the user-friendly Web Interface.

4.1 Configuration of Network Parameters through Device Management Utility

Install the configuration utility program called **Device Management Utility** that can be downloaded from www.blackbox.com. After you start the **Device Management Utility**, if the LES920 Industrial Serial Device Server is already connected to the same subnet as your PC, the device can be accessed via broadcast packets. The **Device Management Utility** will automatically detect your LES920 device and list it in the **Device Management Utility**'s window. Alternatively, if you did not see your LES920 device on your network, click on the “Rescan” icon. A list of devices, including your LES920 device currently connected to the network, will be shown in the **Device Management Utility**'s window, as shown in Figure 4.1.

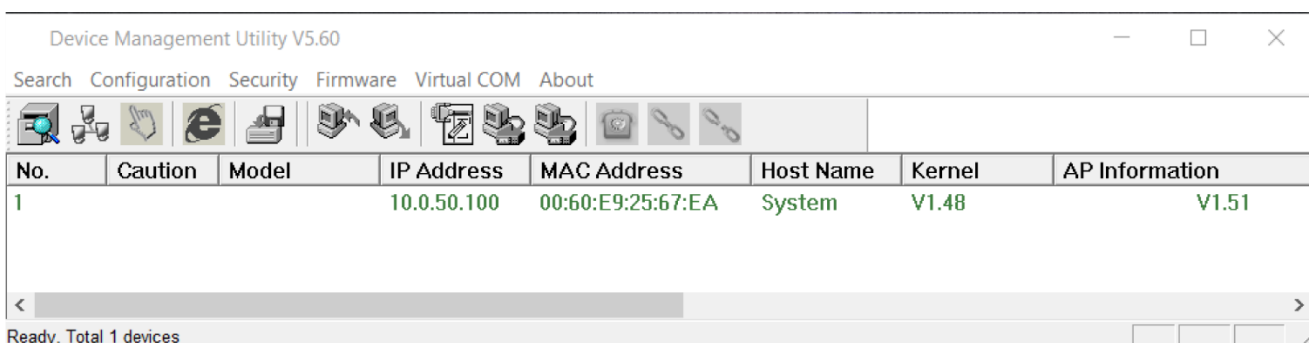


Figure 4.1 List of Devices in Device Management Utility

Note: As with all figures contained in this manual, this figure is generic, and it is intended for illustration purposes only. The information displayed when you use the product/software may differ, and it could differ depending upon the device(s) used.

The LES920 device might not be in the same subnet as your PC; therefore, you will have to use the utility to locate it in your virtual environment. To configure each device, first click to select the desired LES920 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.

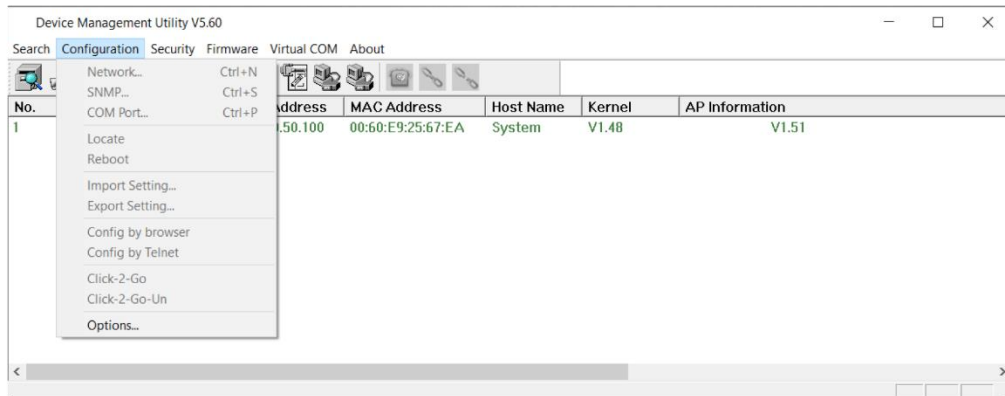


Figure 4.2 Pull-down Menu of Configuration and Network

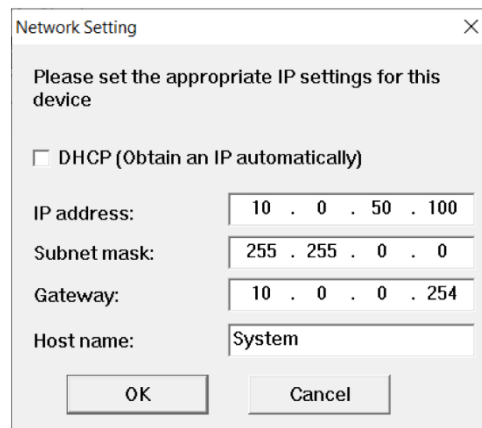


Figure 4.3 Pop-up Window of Network Setting

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 the device may be restarted. After the device is restarted (for some models), it will beep twice to indicate that the unit is running normally. Then, the LES920 device can be found on a new IP address. It may be listed automatically by the **Device Management Utility®**, or it can be found by clicking on the **Rescan** icon. Note that if you did not change the IP address but changed other parameter(s), you may encounter another notification window, as shown in Figure 4.6.

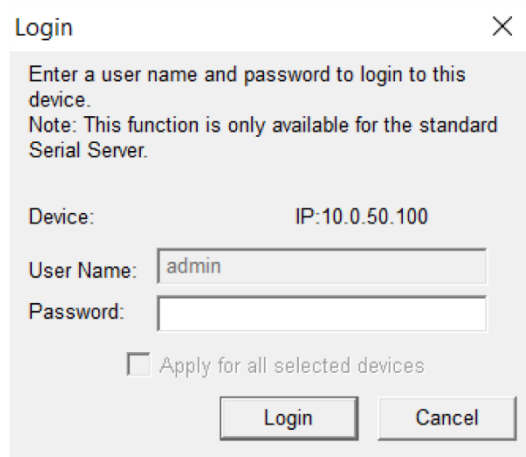


Figure 4.4 Authorization for Change of Network Settings

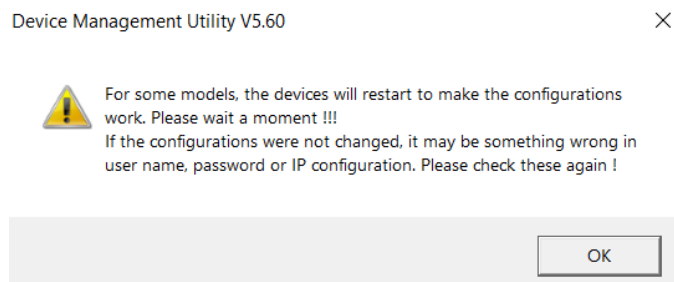


Figure 4.5 Pop-up Notification Window after Authorization

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

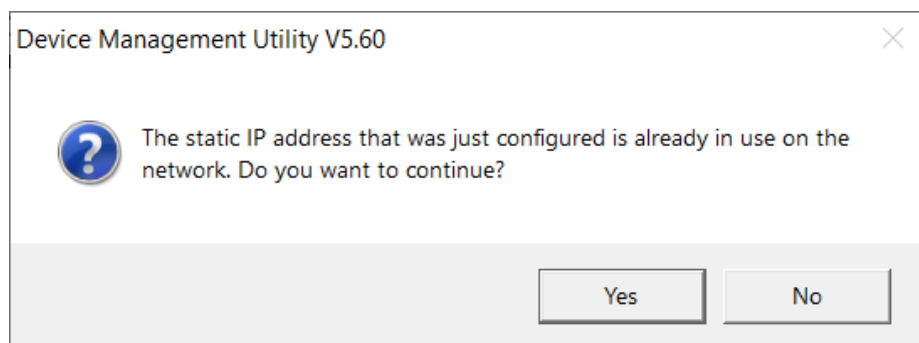
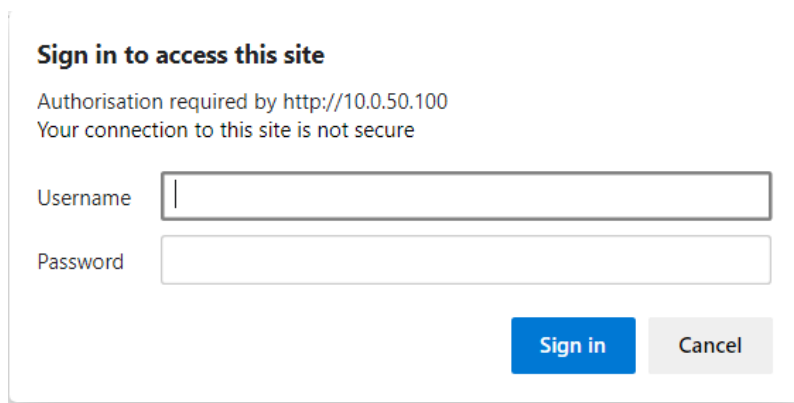


Figure 4.6 Pop-up Notification Window When There is the Same IP Address in the Network

4.2 UI Configuration

Every LES920 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 configuration by entering the device's IP address in the URL field of your web browser. (The default IP address is 10.0.50.100) An authentication will be required, and you will need to enter the username (Default value is "admin") and password (Default value is "default") to access the web interface as shown in Figure 4.7. Note that you may encounter a warning pop-up window, as shown in Figure 4.8, that urges you to change or reset your password to be different from the default value. Figure 4.9 illustrates the overview page of the web interface. Figure 4.10 lists all the menus and submenus for web configuration. See Section 3.4 for default values.



The image shows a web browser authentication dialog box. At the top, it says "Sign in to access this site". Below that, it states "Authorisation required by http://10.0.50.100" and "Your connection to this site is not secure". There are two input fields: "Username" and "Password". At the bottom right, there are two buttons: "Sign in" (blue) and "Cancel" (grey).

Figure 4.7 Authentication Required for Accessing Web Interface

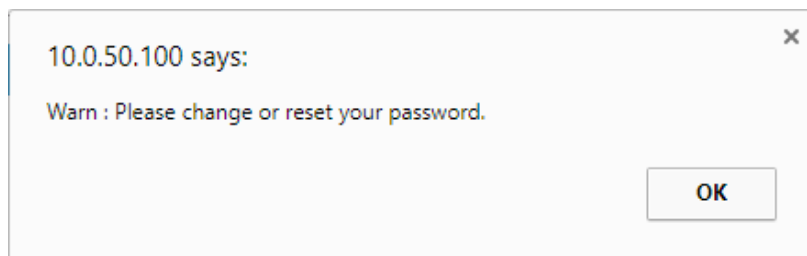


Figure 4.8 Warning Pop-up Window for Changing or Resetting Password from Default Value

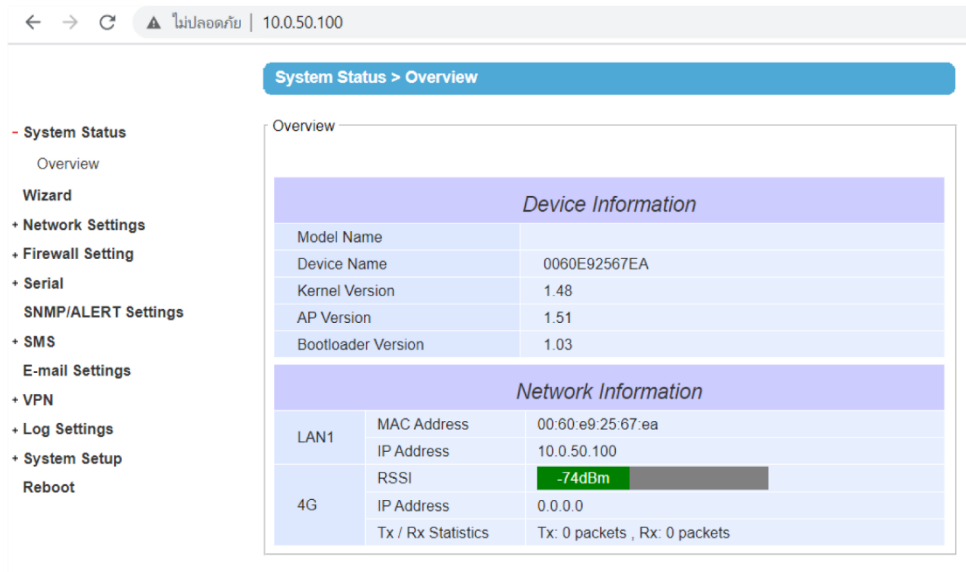


Figure 4.9 Overview Web Page of LES920 Industrial Serial Device Server

System Status

Overview

Wizard**Network Settings**

IPv4 Settings

Ping Reboot

Dynamic DNS

4G Settings

Firewall Setting

Services

Port Forwarding

DMZ

Serial

COM1

SNMP/ALERT Settings**SMS****E-mail Settings****VPN****Log Settings****System Setup****Reboot**

Figure 4.10 Map of Configuring Web Page on LES920 Industrial Serial Device Server

This approach (web interface) for configuring your device is the most user-friendly. It is the most recommended and the most common method used for the LES920 Industrial Serial Device Server Series. Refer to the menu's corresponding section for a detailed explanation.

System Setup > Admin Settings

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 4.11 Access control

4.3 CLI Configuration

4.3.1 Connect to CLI

You can also configure the setting throughout CLI via the terminal emulators, such as PUTTY or Teraterm.

- Open the terminal emulator; enter the IP Address; and choose Telnet connection.

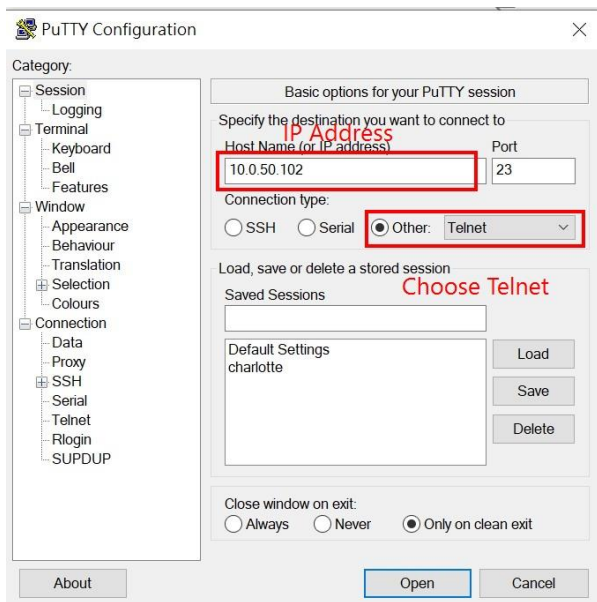


Figure 4-12 Connect the device with Telnet

■ **Log in with the account (same as the web one).**

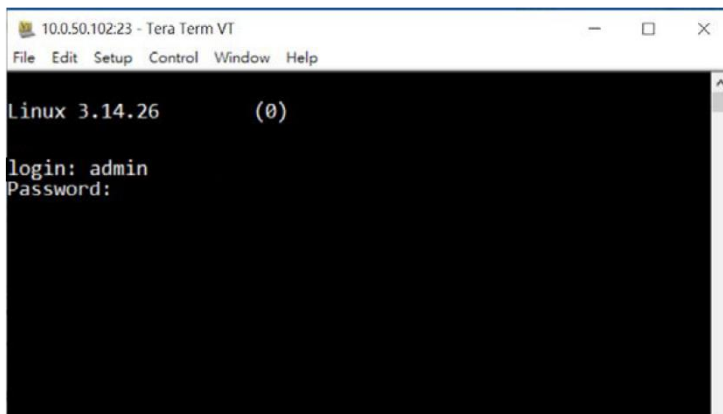


Figure 4-13 Log into the account

After you access the CLI, you will see the Main Menu page.

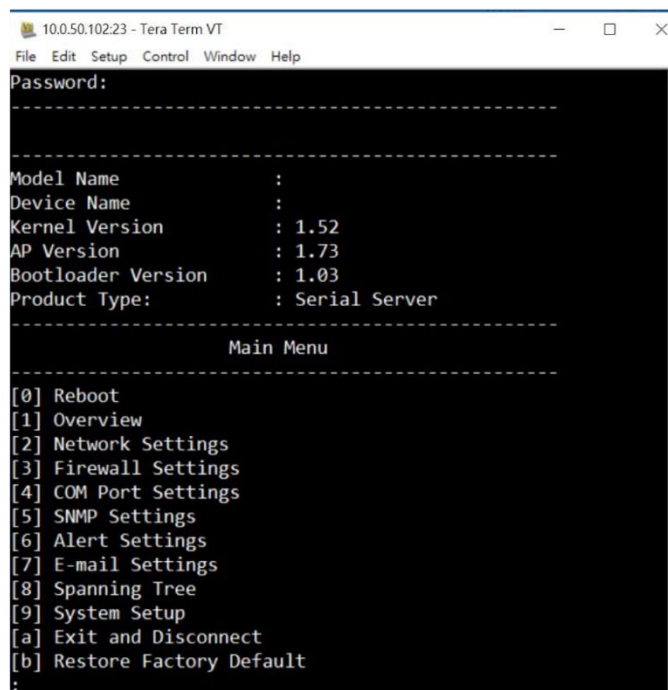


Figure 4-14 Main Menu page on CLI

4.3.2 General Information of CLI

Once entering a number from the menu, the terminal will go to the corresponding function setting. General information about the CLI follows:

Operation: Main → [1] Overview

This system overview window gives the general information on Ethernet, MAC address, kernel, and AP version.

```
-----
Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 1
-----
Overview
-----
[0] Exit
[*] LAN 1 MAC -----> 00:60:e9:1e:6c:56
[*] LAN 1 IP -----> 10.0.50.102
[*] LAN 2 MAC -----> ff:ff:ff:ff:ff:ff
[*] LAN 2 IP -----> 0.0.0.0
:
```

Figure 4-15 Overview Information by Telnet

4.3.3 Network Configuration

Operation: Main → [2] Networking

This section allows for changes in **Lan Setting**, **DNS Setting**, and **Default Gateway** information. Note that setting changes will not take effect until the device is restarted.

```
-----  
Main Menu  
-----  
[0] Reboot  
[1] Overview  
[2] Network Settings  
[3] Firewall Settings  
[4] COM Port Settings  
[5] SNMP Settings  
[6] Alert Settings  
[7] E-mail Settings  
[8] Spanning Tree  
[9] System Setup  
[a] Exit and Disconnect  
[b] Restore Factory Default  
: 2  
-----  
Networking  
-----  
[0] Exit  
[1] Lan Settings  
[2] DNS Settings  
[3] Default Gateway ----> LAN 1  
:  
:
```

Figure 4-16 Network Settings by Telnet

4.3.4 LAN Setting

Operation: Main → [2] Networking → [1] Lan Settings

For SE products, there might be multiple LAN ports on a DUT, and each of the LAN ports contains the exact same setting. Therefore, we use only the LAN 1 Setting as an example.

The “[1] **LAN settings**” option enables you to view information about **MAC address, IP address, Netmask, Gateway, and IP mode (static/DHCP)** of LAN 1.

Operation: Main → [2] Networking → [1] Lan Settings → [1] LAN 1 Setting

```
-----
Networking
-----
[0] Exit
[1] Lan Settings
[2] DNS Settings
[3] Default Gateway ----> LAN 1
: 1
-----
LAN Settings
-----
[0] Exit
[1] LAN 1 Setting
[2] LAN 2 Setting
: 1
-----
LAN 1 Settings
-----
[0] Exit
[*] MAC -----> 00:60:e9:1e:6c:56
[1] IP -----> 10.0.50.102
[2] Netmask -----> 255.255.0.0
[3] Gateway -----> 10.0.0.254
[4] IP Mode -----> Static
:
```

Figure 4-17 LAN 1 Settings by Telnet

4.3.5 DNS Settings

Operation: Main → [2] Networking → [2] DNS Setting

The Serial Server can configure the Preferred DNS and Alternate DNS Server manually.

```
-----  
Networking  
-----  
[0] Exit  
[1] Lan Settings  
[2] DNS Settings  
[3] Default Gateway ----> LAN 1  
: 2  
-----  
DNS Settings  
-----  
[0] Exit  
[1] Preferred DNS -----> 0.0.0.0  
[2] Alternate DNS -----> 0.0.0.0  
:  
:
```

Figure 4-18 DNS Settings by Telnet

4.3.6 Default Gateway Settings

Operation: Main → [2] Networking → [3] Default Gateway

The default gateway setting allows you to change the default gateway of LAN1 and other Lan interfaces.

```
-----  
Networking  
-----  
[0] Exit  
[1] Lan Settings  
[2] DNS Settings  
[3] Default Gateway ----> LAN 1  
: 3  
-----  
Default Gateway Settings  
-----  
[0] LAN 1  
[1] LAN 2  
:  
:
```

Figure 4-19 Default Gateway Setting by Telnet

4.3.7 Firewall Settings

Operation: Main → [3] Firewall Settings

This section allows you to set up the **IP Filter** and **DDoS Protection** functions. Note that setting changes will not take effect until the device is restarted.

```
-----
                          Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 3
-----
                          Firewall Settings
-----
[0] Exit
[1] IP Filter
[2] DDoS Protection ----> Enable
:
```

Figure 4-20 Firewall Setting by Telnet

4.3.8 IP Filter Setting

This menu contains IP Filter and DDoS Protection function.

Operation: Main → [3] Firewall Settings → [1] IP Filter → [1] Default Policy

The default policy of IP Filter refers to the default policy on the 4G interface. The default value is Accept.

```
-----
                        IP Filter
-----
[0] Exit
[1] Default Policy -----> Drop
[2] Filter List
: 1
-----
                        Default Policy
-----
[0] Accept
[1] Drop
:
```

Figure 4-21 Default policy of IP Filter by Telnet

Operation: Main → [3] Firewall Settings → [1] IP Filter → [2] Filter List

In this IP filter list, a total of 30 fields are available for configuration. The default parameters in this list are consistent with the web page, and all the settings are set to accept by default.

```
-----
                        Firewall Settings
-----
[0] Exit
[1] IP Filter
[2] DDoS Protection -----> Enable
: 1
-----
                        IP Filter
-----
[0] Exit
[1] Default Policy -----> Drop
[2] Filter List
: 2
-----
                        Filter Item
-----
[0] Exit
[1] ping
[2] http
[3] https
[4] IPSEC_1
[5] IPSEC_2
[6] SerialIP
[7] DeviceManager
```

Figure 4-22 Filter List of IP Filter by Telnet

4.3.9 COM Port Settings

Operation: Main → [4] COM Port Setting

For SE products, the number of COM ports can be one, two, four, eight, and sixteen. Each setting of the COM number contains exact same setting. Therefore, we use only the COM 1 setting as an example.

The setting inside the “**COM 1 settings**” includes **Serial Interface, Baud Rate, Parity, Data bit, and Stop bit**.

```
-----
Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 4
-----
COM Port Settings
-----
[0] Exit
[1] COM 1 Setting
:
```

Figure 4-23 COM Port Settings by Telnet

Operation: Main → [4] COM Port Setting → [1] COM 1 Setting

```
-----
COM 1 Settings
-----
[0] Exit
[1] Link Mode -----> TCP Server
[2] Com Setting -----> RS232,9600,8,None,1
: 2
-----
Com Setting (COM 1)
-----
[0] Exit
[1] Serial interface ---> RS232
[2] Baud rate -----> 9600
[3] Parity -----> None
[4] Data bits -----> 8
[5] Stop bits -----> 1
[6] Flow control -----> None
:
```

Figure 4-24 COM 1 Setting by Telnet

4.3.10 Link Mode Settings

In the Link Mode Settings, there are three different categories: TCP Server, TCP Client, and UDP.

Operation: Main → [4] COM Port Setting → [1] COM 1 Setting → [1] TCP Server

In the TCP Server mode, you can change the setting of **Application**, **Max Connection**, **IP Filter**, **port**, and **Response Behavior**.

```
-----
COM 1 Settings
-----
[0] Exit
[1] Link Mode -----> TCP Server
[2] Com Setting -----> RS232,9600,8,None,1
: 1
-----

Link Mode (COM 1)
-----
[0] Exit
[1] TCP Server
[2] TCP Client
[3] UDP
: 1
-----

TCP Server (COM 1)
-----
[0] Exit
[1] Application -----> RAW
[2] Max Connection -----> 1
[3] IP Filter -----> Disable
[4] Port -----> 4660
[5] Response Behavior --> Transparent Mode
: 
```

Figure 4-25 TCP Server link mode setting by Telnet

Operation: Main → [4] COM Port Setting → [1] COM 1 Setting → [2] TCP Client

In the TCP Server mode, you can change the setting of **Application, Destination, Backup Destination, and Response Behavior**.

```
-----
Link Mode (COM 1)
-----
[0] Exit
[1] TCP Server
[2] TCP Client
[3] UDP
: 2
-----
TCP Client (COM 1)
-----
[0] Exit
[1] Application -----> RAW
[2] Destination IP 1 ---> 0.0.0.0
[3] Destination Port 1 -> 0
[4] Destination 2 -----> Disable
[5] Response Behavior --> Transparent Mode
:
```

Figure 4-26 TCP Client link mode setting by Telnet

Operation: Main → [4] COM Port Setting → [1] COM 1 Setting → [3] UDP

In the TCP Server mode, you can change the settings for **Local Port, and Destination IPs**.

```
-----
Link Mode (COM 1)
-----
[0] Exit
[1] TCP Server
[2] TCP Client
[3] UDP
: 3
-----
UDP (COM 1)
-----
[0] Exit
[1] Local Port -----> 0
[2] Destination 1 -----> Disable
[3] Destination 2 -----> Disable
[4] Destination 3 -----> Disable
[5] Destination 4 -----> Disable
:
```

Figure 4-27 UDP link mode setting by Telnet

4.3.11 Application of the Link Mode

Operation: Main → [4] COM Port Setting → [1] COM 1 Setting → [1] TCP Server → [1] Application
The Application setting of the Link Mode in TCP Server contains RAW, VCOM, Reverse Telnet, and Pair connection.

```
-----
TCP Server (COM 1)
-----
[0] Exit
[1] Application -----> RAW
[2] Max Connection -----> 1
[3] IP Filter -----> Disable
[4] Port -----> 4660
[5] Response Behavior --> Transparent Mode
: 1
-----

[0] RAW
[1] VCOM
[2] Reverse Telnet
[3] Pair Connection Slave
:
```

Figure 4-28 Application Setting of TCP Server by Telnet

Operation: Main → [4] COM Port Setting → [1] COM 1 Setting → [1] TCP Server → [1] Application
The Application Setting of the Link Mode in TCP Client contains RAW, VCOM, and Pair connection.

```
-----
Link Mode (COM 1)
-----
[0] Exit
[1] TCP Server
[2] TCP Client
[3] UDP
: 2
-----

TCP Client (COM 1)
-----
[0] Exit
[1] Application -----> RAW
[2] Destination IP 1 ---> 0.0.0.0
[3] Destination Port 1 -> 0
[4] Destination 2 -----> Disable
[5] Response Behavior --> Transparent Mode
: 1
-----

[0] RAW
[1] VCOM
[2] Pair Connection Slave
:
```

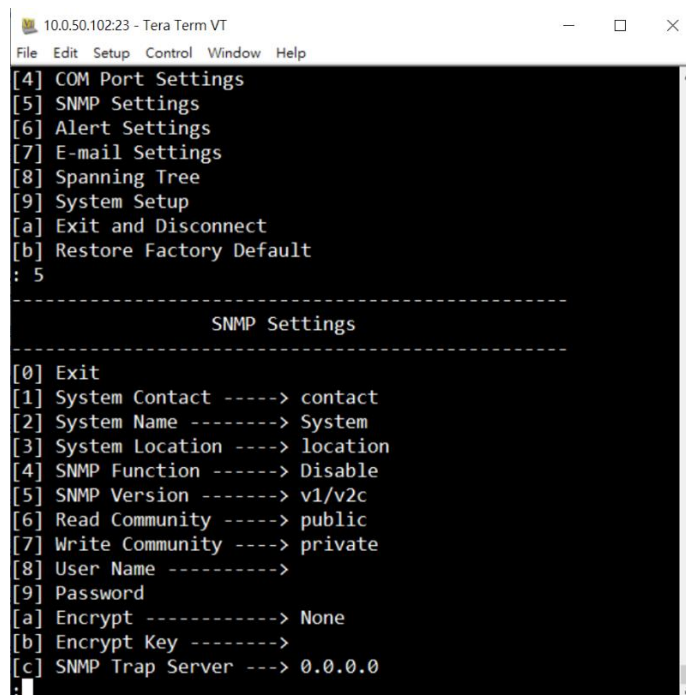
Figure 4-29 Application Setting of TCP Client by Telnet

4.3.12 SNMP Settings

Serial Server allows you to Enable or Disable the SNMP function by choosing the “[5] **SNMP: Disable**” option and selecting “**Enable**” to enable the **SNMP** operation. The changes will be effective immediately.

Serial Server supports basic SNMP function for system MIB (Management Information Base). It can definite the SNMP Trap server, Read/Write Community, SysName (System Name), SysLocation (System Location), and SysContact (System Contact) via Telnet console.

Operation: Main → [5] SNMP Settings



```
10.0.50.102:23 - Tera Term VT
File Edit Setup Control Window Help
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 5

-----
                SNMP Settings
-----

[0] Exit
[1] System Contact ----> contact
[2] System Name -----> System
[3] System Location ----> location
[4] SNMP Function ----> Disable
[5] SNMP Version ----> v1/v2c
[6] Read Community ----> public
[7] Write Community ----> private
[8] User Name ----->
[9] Password
[a] Encrypt -----> None
[b] Encrypt Key ----->
[c] SNMP Trap Server ---> 0.0.0.0
:
```

Figure 4-30 SNMP Settings by Telnet

4.3.13 Alert Settings

Operation: Main → [6] Alert Settings

Two subsystem settings include E-mail and Alert Event.

```
-----
Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 6
-----
Alert Settings
-----
[0] Exit
[1] Warm Start -----> Email:Disable, Trap:Disable
[2] Cold Start -----> Email:Disable, Trap:Disable
[3] Auth Failed -----> Email:Disable, Trap:Disable
[4] IP Changed -----> Email:Disable
[5] Password Changed ---> Email:Disable
:
```

Figure 4-31 Alert Settings by Telnet

4.3.14 E-mail Settings

The settings inside the E-mail Settings includes **Sender, Receiver, SMTP Server, and Authentication.**

Operation: Main → [7] E-mail Settings

```
-----
Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 7
-----
E-mail Settings
-----
[0] Exit
[1] Sender ----->
[2] Receiver
[3] SMTP Server ----->
[4] Authentication -----> Disable
:
```

Figure 4-32 E-mail Settings by Telnet

4.3.15 Spanning Tree

This menu includes the Spanning Tree settings and status values.

Operation: Main → [8] Spanning Tree

```
-----
Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 8
-----
Spanning Tree
-----
[0] Exit
[1] Spanning Tree Settings
[2] Port Settings Info
[3] Bridge Info
: 1
```

Figure 4-33 Set up Spanning Tree by Telnet

4.3.16 System Setup

This menu contains system-related settings, such as system time, web access password, web mode, Telnet/SSH/FTP, ping, and firmware update function.

Operation: Main → [9] System Setup

```
-----
Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 9
-----
System Settings
-----
[0] Exit
[1] Date/Time Settings
[2] Admin Settings
[3] Ping
[4] Firmware upgrade
:
```

Figure 4-34 System Setup by Telnet

Operation: Main → [9] System Setup → [1] Date/Time Settings

The settings inside Date/Time Settings are **NTP**, **Manual**, **Daylight Saving Time**, and **Local NTP Service**.

```
-----
System Settings
-----
[0] Exit
[1] Date/Time Settings
[2] Admin Settings
[3] Ping
[4] Firmware upgrade
: 1
-----
Date/Time Settings
-----
[0] Exit
[1] NTP -----> Disable
[2] Manual -----> 12 / Feb / 2015 02:25:35
[3] Daylight Saving Time
[4] Local NTP Service --> Disable
:
```

Figure 4-35 Date/Time Settings by Telnet

Operation: Main → [9] System Setup → [2] Admin Settings

The settings in the Admin Settings option are: **Change Password, Web Settings, Telnet, SSH, and FTP.**

```
-----
System Settings
-----
[0] Exit
[1] Date/Time Settings
[2] Admin Settings
[3] Ping
[4] Firmware upgrade
: 2
-----
Admin Settings
-----
[0] Exit
[1] Change Password
[2] Web Settings
[3] Telnet -----> Enable
[4] SSH -----> Enable
[5] FTP -----> Enable
:
```

Figure 4-36 Admin Settings by Telenet

Operation: Main → [9] System Setup → [3] Ping

Enter the IP address; the system will execute the command.

```
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: 9
-----
System Settings
-----
[0] Exit
[1] Date/Time Settings
[2] Admin Settings
[3] Ping
[4] Firmware upgrade
: 3
: 10.0.50.101
PING 10.0.50.101 (10.0.50.101): 56 data bytes
64 bytes from 10.0.50.101: seq=0 ttl=128 time=2.010 ms
64 bytes from 10.0.50.101: seq=1 ttl=128 time=1.816 ms
```

Figure 4-37 Ping IP address by Telnet

Operation: Main → [9] System Setup → [4] Firmware Upgrade

The Firmware Upgrade setting allows you to change the firmware through Telnet.

```
-----
                        System Settings
-----
[0] Exit
[1] Date/Time Settings
[2] Admin Settings
[3] Ping
[4] Firmware upgrade
: 4
-----
                        Firmware upgrade
-----
[0] Exit
[1] Firmware Location --> TFTP server
[2] File name ----->
[3] TFTP server IP -----> 0.0.0.0
[4] Upgrade
:
```

Figure 4-38 Firmware Upgrade by Telnet

4.3.17 Exit and Disconnect

Please select this menu to exit and disconnect from the CLI.

Operation: Main → [a] Exit and Disconnect

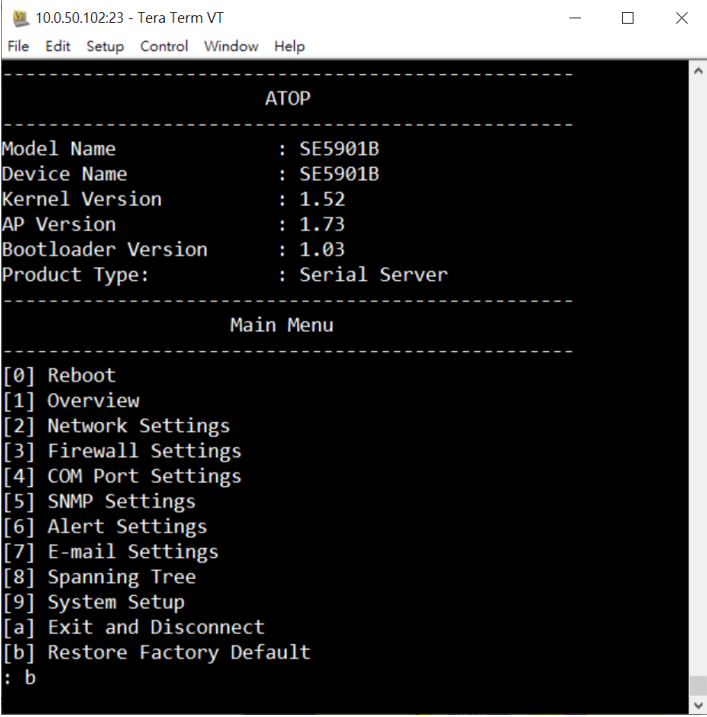
```
10.0.50.102:23 - Tera Term VT
File Edit Setup Control Window Help
-----
                        ATOP
-----
Model Name       : SE5901B
Device Name      : SE5901B
Kernel Version   : 1.52
AP Version       : 1.73
Bootloader Version : 1.03
Product Type:    : Serial Server
-----
                        Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
```

Figure 4-39 Exit and Disconnect CLI by Telnet

4.3.18 Restore to the Factory Default

Select this menu to restore Serial Server's settings to Factory Default Settings. After completing [b] Restore Factory Default, next, choose Step [0] Reboot to restore to factory default settings.

Operation: Main → [b] Restore Factory Default



```
10.0.50.102:23 - Tera Term VT
File Edit Setup Control Window Help
-----
ATOP
-----
Model Name       : SE5901B
Device Name      : SE5901B
Kernel Version   : 1.52
AP Version       : 1.73
Bootloader Version : 1.03
Product Type:    : Serial Server
-----
Main Menu
-----
[0] Reboot
[1] Overview
[2] Network Settings
[3] Firewall Settings
[4] COM Port Settings
[5] SNMP Settings
[6] Alert Settings
[7] E-mail Settings
[8] Spanning Tree
[9] System Setup
[a] Exit and Disconnect
[b] Restore Factory Default
: b
```

Figure 4-40 Restore to the Default by Telnet

4.4 Configuring Automatic IP Assignment with DHCP

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

4.5 Web Overview

In this section, current information on the device’s status and settings will be displayed. An example of the overview page is shown in Figure 4-41.

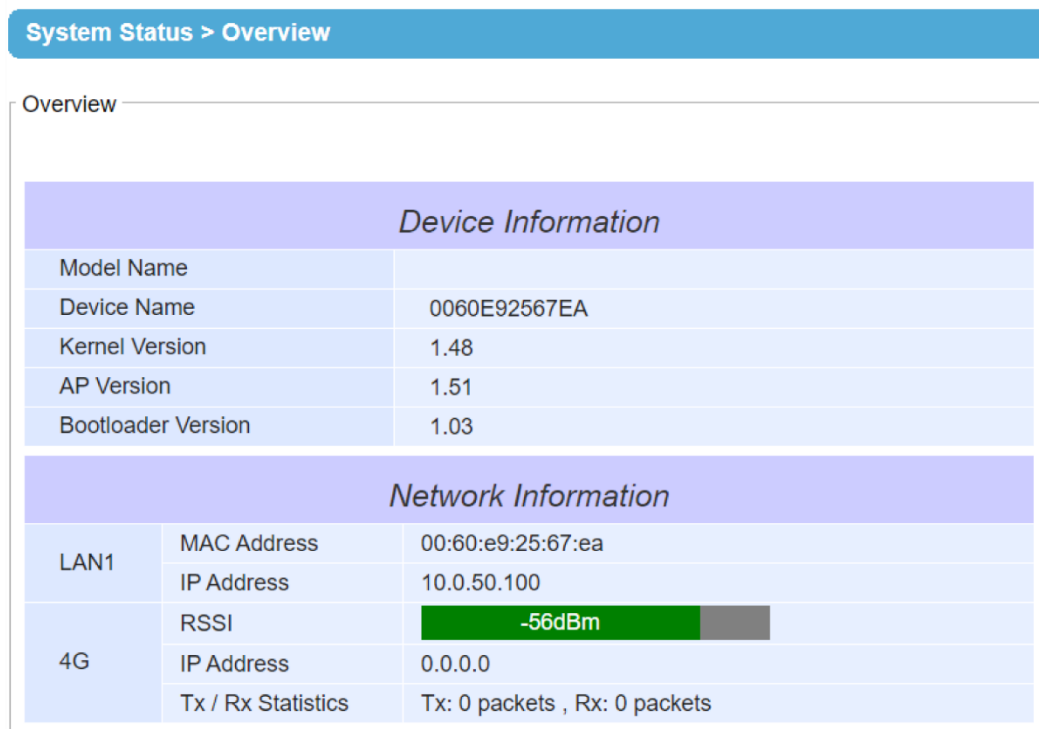


Figure 4.41 Overview Web Page

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

■ **Device Information**

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

■ **Network Information** shows information about the device's wired and wireless network interfaces.

- **LAN1**: This will display the current **MAC Address** and **IP Address** of the Ethernet interface.
- **3G/4G**: The RSSI (Received Signal Strength Indicator) of the 3G/4G signal is shown, as well as its assigned IP address. The Tx/Rx statistics are also displayed.

4.6 Wizard

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

There are the total of six steps/windows in the wizard, which include Welcome, Administration, DATE/Time, Network, COM, and Final. In Step 1/6, the Welcome window, as shown in Figure 4-42, will introduce you how to use the wizard. Click on the "Next" button to advance to Step 2/6, or "EXIT" to see other menus.

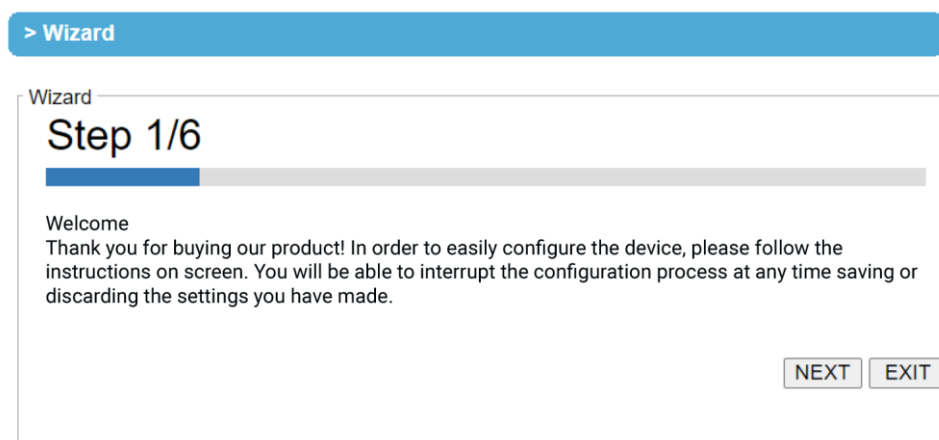


Figure 4.42 Step 1/6 – A Welcome Web Page to the Configuration Wizard

In Step 2/6, the **Administration** window, as shown in Figure 4-43, will let you set a new password for the login device to increase security. You have to re-input the password in “Repeat New Password” to set the new password. We recommend that you to use a mix of upper- and lower-case letters, as well as numbers and symbols to make the password more secure. If you want to go back to Step 1/6, click on the “Prev” button. Click on the “Next” button to move on to the Date/Time window in Step 3/6. If you want to leave the wizard, click on the “EXIT” button. If the “EXIT” button is clicked, a pop-up window will appear. You will have a choice to either save or discard the settings which were selected through the wizard.

The screenshot shows a web-based wizard interface. At the top, a blue header bar contains the text "> Wizard". Below this, the main content area is titled "Wizard" and "Step 2/6". A progress bar is visible, with the first segment highlighted in blue. The section is titled "Administration" and contains the following text: "We recommend that you change the device password for increased security. Please input the password in the 'new password' field below and repeat it in the 'Repeat new password' field. Use of upper and lower case letters, numbers and symbols is recommended." Below the text are two input fields: "New Password" and "Repeat New Password". At the bottom right of the form are three buttons: "PREV", "NEXT", and "EXIT".

Figure 4.43 Step 2/6 – An Administration Web Page to Set Password

In Step 3/6, the **Date/Time** window, as shown in Figure 4.44, will let you set the device's Date/Time. You can select the correct time zone from the dropdown box. If device is connected to the internet or to a local NTP server, the Date/time can be set automatically by selecting the option “Synchronize the time automatically from an NTP server.” This option is selected by default. If you do not want to automatically sync from the NTP server, you can manually set it. You can set more advanced options, such as Daylight-Saving time, on the “Date/Time settings” page. If this option is chosen, the default value “time.nist.gov” should be shown in the NTP server field. If the LES920 device is connected to the Internet and should connect to other servers over the Internet to get the NTP server, you will need to configure the DNS server in Step 4/6 in order to be able to resolve the host name of the NTP server. Click “PREV” to go back to Step 2/6 to re-enter new password, “NEXT” to move on to **Network** window, or “EXIT” to discard or save the settings that were selected through the wizard.

The screenshot shows a web-based configuration wizard. At the top, a blue bar contains a back arrow and the word 'Wizard'. Below this, the title 'Step 3/6' is displayed in a large font. A progress bar is shown with the first three steps completed. The main heading is 'Date/Time'. Below the heading is a paragraph of text: 'This device, if connected to the internet or to a local NTP server can set its system time automatically. Otherwise, you can set the system time manually. You can configure more advanced options such as Daylight Saving time in the 'Date/Time settings' page. Note: if you're using an internet address, please make sure that 'default gateway' and DNS server fields are filled in in the next page of this wizard.' Below the text is a form with a light blue background. The form has a title 'Date/Time' in a purple header. It contains three rows: 'Time Zone' with a dropdown menu showing '(GMT-12:00) Eniwetok, Kwajalein'; 'NTP' with two radio buttons, 'Synchronize the time automatically from an NTP server' (selected) and 'Set up the time manually'; and 'NTP Server' with a text input field containing 'time.nist.gov'. At the bottom right of the form are three buttons: 'PREV', 'NEXT', and 'EXIT'.

> Wizard

Wizard

Step 3/6

Date/Time

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

Date/Time	
Time Zone	(GMT-12:00) Eniwetok, Kwajalein
NTP	<input checked="" type="radio"/> Synchronize the time automatically from an NTP server <input type="radio"/> Set up the time manually
NTP Server	time.nist.gov

PREV NEXT EXIT

Figure 4.44 Step 3/6 – A Date/Time Web Page of the Configuration Wizard

In Step 4/6, the **Network** window, as shown in Figure 4-45, will let you set network information for more than one port. The Network window will display “This device has x Ethernet ports. You are now setting up LAN1.” You have a choice to either set it up manually or obtain information automatically from a DHCP server. If you selected “Obtain IP address automatically from a DHCP server,” the rest of the options for LAN1 settings will be greyed out or disabled. If the option “Set up the network settings manually” is selected, you can input an IP address with subnet mask and gateway, and the device’s DNS. You can select Default Internet Gateway, if applicable. DNS (Domain Name Server) is where you can specify the IP Address of your preferred DNS and alternate DNS, which is why there are two DNS IPs to enter on the screen. Consult with your network administrator or internet service provider (ISP) to obtain the local DNS IP addresses. If you have only one LAN connected, you have an option to move to Step 4/6 by selecting the option “I’m done with LAN port configuration.” Otherwise, you can select the option “I need to configure LANx”. A new window with LANx settings will be shown, and you can continue with its configuration, the same way you entered LANx Settings.

[> Wizard](#)

Wizard

Step 4/6

Network

This device has 1 Ethernet ports, You are now setting up LAN1. The network settings can be obtained automatically from a DHCP server or set up manually. The changes will become effective upon completion of the Configuration Wizard

<i>Lan 1</i>	
Manual/DHCP	<input checked="" type="radio"/> Set up the network settings manually <input type="radio"/> Obtain IP address automatically from a DHCP server
IP	<input type="text" value="10.0.50.100"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Gateway	<input type="text" value="10.0.0.254"/>
Default Internet Gateway	<input checked="" type="radio"/>
DNS 1	<input type="text" value="0.0.0.0"/>
DNS 2	<input type="text" value="0.0.0.0"/>

Figure 4.45 Step 4/6 – Network Web Page to Set LAN's IP address

In Step 5/6, the **COM** window, as shown in 46, will let you set the device's COM port. If the device has more than one port (network or COM), there will be one page for each COM within Step 5/6. The LES920 series supports three different **Link Modes**: **TCP Server**, **TCP Client**, and **UDP**. The **Link Mode** describes the role of the LES920 and the connection between the LES920 device and other remote devices in the network which would like to communicate with serial devices on the LES920's COM port(s). Select the one suitable to your end-application. **There is no radio** is checked for the default. If you want to set up more additional advanced settings, click on the COMx link on the left-hand side menu to configure additional options.

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

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

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

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

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

> Wizard

Wizard

Step 5/6

COM

This device has 1 COM ports, You are now setting up COM1. This Serial device Server supports different communication modes. Please select the one suitable to your end-application. If you'd like to set-up additional advanced settings, please click on the COM1 link on the left-hand side menu to configure

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

Serial Settings	
Mode	<input type="text" value="RS232"/>
Baud Rate	<input type="text" value="1200"/>
Data Bit	<input type="text" value="5 bits"/>
Parity	<input type="text" value="None"/>
Stop Bit	<input type="text" value="1 bits"/>

Figure 4.46 Step 5/6 – COM Web Page to Set COM Port

In Step 6/6, the **Final** window, as shown in Figure 4-47, will provide the download link for the Device Management Utility and Serial/IP utility as well as necessary information for the user who uses VirtualCOM.

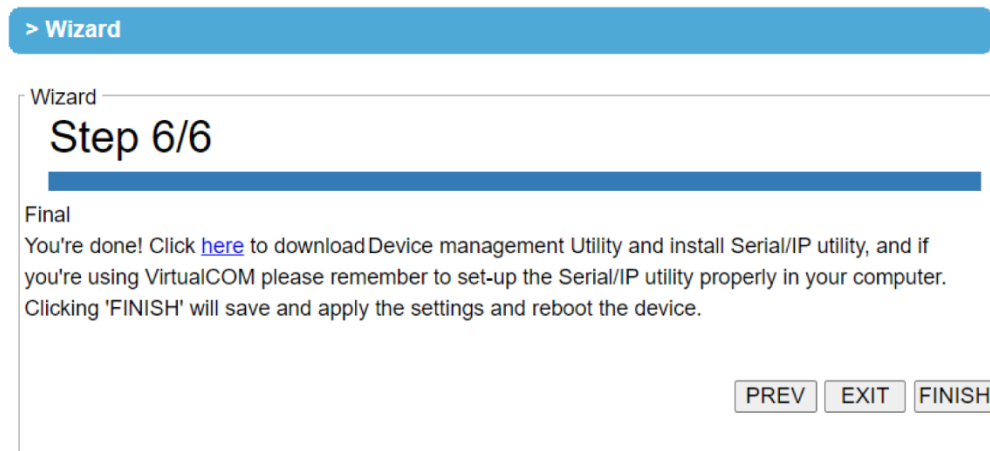


Figure 4.47 Step 6/6 – Final Web Page to introduce Serial/IP utility

4.7 Network Settings

In this section, both network interfaces and related network settings of the LES920 device can be configured. The **Network Settings** menu has four submenus: **IPv4 Settings**, **Ping Reboot**, **Dynamic DNS**, and **4G Settings**. Figure 4-48 shows the menu and its submenus.

- Network Settings

- IPv4 Settings
- Ping Reboot
- Dynamic DNS
- 4G Settings

Figure 4.48 Submenus of the Network Settings Menu

In the first submenu (**IPv4 Settings**), there are two sets of parameters, which are **LAN1 Settings** and **DNS Server**, where you can enter information, as shown in Figure 4-49. More information on this parameter will be provided later. For the first parameter (**LAN1 Settings**), you can configure the **IP Address**, **Subnet Mask**, and **Default Gateway** for your wired LAN1 network. You can check the box behind the **DHCP** option to obtain an IP address automatically. If you checked the box, the rest of the options for **LAN1 Settings** will be greyed out or disabled. For the Second parameter (**DNS Server**), you can specify the IP Address of your **Preferred DNS** (Domain Name Server) and **Alternate DNS**. If the LES920 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. Contact your network administrator or internet service provider (ISP) to obtain local DNS IP addresses.

The screenshot shows a web interface for configuring IPv4 settings. At the top is a blue header bar with the text "Network Settings > IPv4 Settings". Below this is a form titled "Network Settings" with a light blue border. The form is divided into three main sections, each with a light purple header bar:

- LAN1 Settings**: Contains four rows. The first row has "DHCP" and an unchecked checkbox labeled "Enable". The second row has "IP Address" and a text box containing "10.0.50.100". The third row has "Subnet Mask" and a text box containing "255.255.0.0". The fourth row has "Gateway" and a text box containing "10.0.0.254".
- DNS Server**: Contains two rows. The first row has "Preferred DNS" and a text box containing "0.0.0.0". The second row has "Alternate DNS" and a text box containing "0.0.0.0".
- NAT Settings**: Contains one row with "NAT" and an unchecked checkbox labeled "Enable".

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

Figure 4.49 IPv4 Setting within the Network Settings Menu

After finishing the network settings (or IPv4 settings) configuration, click on the **Save & Apply** button to save all changes that have been made. The web browser will be redirected to the **Overview** page as shown in Figure 4-41. If you would like to discard any setting, click on the **Cancel** button.

4.8 Serial

Since the LES920 is an Industrial Serial Device Server, it supports serial communication with COM port(s). Note that the LES920 series can have up to four COM ports: **COM1**, **COM2**, **COM3**, and **COM4**. Figure 4-50 shows the **Serial** menu on the left frame of the web interface of the LES920. The following subsections will describe how to configure these COM ports.

- System Status
 - Overview
- Wizard
- Network Settings
 - IPv4 Settings
 - Ping Reboot
 - Dynamic DNS
 - 4G Settings
- Firewall Setting
 - Services
 - Port Forwarding
 - DMZ
- Serial
 - COM1
- SNMP/ALERT Settings
- + SMS
- E-mail Settings
- + VPN
- + Log Settings
- + System Setup
- Reboot

Figure 4.50 Serial Menu

4.8.1 COM Port Overview

Since details on Link Mode connectivity protocols and its settings of the LES920 series are given in Chapter 5 Link Modes and Applications, this section will only focus on the Serial Settings. Figure 4-51 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 web page settings are applicable for COM 2/COM 3/COM 4 Port Settings on other LES920 devices.

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	<div><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</div>

To configure COM 1 port parameters.

Serial Settings

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

Save & Apply

Cancel

Advanced Settings

Figure 4.51 COM 1 Port Settings Web Page

4.8.2 COM Configuration

Figure 4-52 shows an excerpt of the **Serial Settings** part of **COM** port settings for the LES920. Note that these settings need to match the parameters on the serial port of the serial device. Each option is described below:

To configure COM 1 port parameters.

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

Save & Apply Cancel Advanced Settings

Figure 4.52 Serial Setting 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.
- **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').
- **Sync DTR signal with TCP connection:** The user can synchronize the DTR (Data Terminal Ready) control signal of the serial interface with the status of TCP connection. When the TCP connection is established or disconnected, the DTR signal will be turn on or off accordingly. Select the **YES** radio button to enable this function. Otherwise, select the **NO** radio button to disable this function.
- **Sync RTS signal with TCP connection:** The user can synchronize the RTS (Ready To Send) control signal of the serial interface with the status of TCP connection. When the TCP connection is established or disconnected, the DTR signal will be turned on or off accordingly. Select the **YES** radio button to enable this function. Otherwise, select **NO** radio button to disable this function.
- **Receiver Resistor:** The setting of Pull Resistor can be either OFF or ON.
- **Pull Resistor:** The setting of Pull Resistor can be either 1KΩ or 100KΩ.

Note: The “Receiver Resistor” and “Pull Resistor” options are only available for some specified models. For unsupported models, the “Cold Start” event option will not be displayed on the page.

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

4.8.3 COM Configuration: Advanced Settings

For advanced details of COM port settings, click on the **Advanced Settings** button at the end of the **Serial Settings** page. Another web browser window will open, as shown in Figure 4-53 below. A description of each option follows:

COM 1 Port Advance Settings

Advanced Settings		
TCP	TCP Timeout	<input type="checkbox"/> Enable 0 (0~60000) seconds
	TCP Keep-Alive	<input checked="" type="checkbox"/> Enable 65535 seconds
Delimiters	Serial to Network Packet Delimiter	<input checked="" type="checkbox"/> Interval Timeout 16 (1~30000) ms
		<input checked="" type="radio"/> Auto(Calculate by baudrate) <input type="radio"/> Manual Setting
		<input type="checkbox"/> Max. Bytes 0 (within one packet: 1 ~ 1452 bytes)
	Network to Serial Packet Delimiter	<input type="checkbox"/> Character 0x ("0x"+ASCII Code, Ex. 0x0d or 0x0d0a)
<input type="checkbox"/> Interval Timeout 0 (1~30000) ms		
<input type="checkbox"/> Max. Bytes 0 (within one packet: 1 ~ 1452 bytes)		
Serial	Serial FIFO	<input checked="" 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 4.53 COM 1 Advanced Settings Web Page

TCP

- **TCP timeout:** By clicking in the **Enable** box of **TCP Timeout** and entering a value in seconds between 0 and 60000, the LES920 series will check if there is any data from the serial port. If time expired, the LES920 series will disconnect from its peer.
- **TCP Keep-alive:** By clicking in the **Enable** box of **TCP Keep-alive** and entering a value in seconds, the LES920 series will check if its peer is still active. Note that it will retry three times, and the timeout is five seconds by 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. The LES920 series provides three types of delimiters: **Time Delimiter**, **Maximum Bytes**, and **Character Delimiter**. Note that the following delimiters (**Interval**, **Max Byte** and **Character**), when selected, are programmed in the OR logic. Therefore, if any of the three conditions were met, the LES920 series will transmit the serial data in its buffer over the network.
- ◆ **Interval timeout:** The LES920 series will transmit the serial data in its buffer when the specified time interval has reached and no more serial data is received. The default value is calculated automatically based on the baud rate, which is the **Auto (calculate by baud rate)** option. If the automatic value results in chopped data, the timeout could be increased manually by switching to **“Manual setting”** (activating the radio button in Figure 4.) and specifying a larger value in the corresponding text box. Note that the maximum interval is 30,000 milliseconds.



Attention

Manual Calculation of Interval Timeout

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

- ◆ **Max Bytes:** The LES920 series 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 and 1452 bytes. Enable this option by checking the box in front of **Max. Bytes** if you would like the LES920 series to queue the data until it reaches a specific length. This option is disabled by default.
- ◆ **Character:** The LES920 series will transmit the serial data in its buffer when it sees the incoming data that includes the specified character (in hexadecimal (HEX) format). This field allows one or two characters. If the character delimiter is set to 0x0d, the LES920 series will push out its serial buffer when it sees 0x0d (carriage return) in the serial data. This option is disabled by default.
- **Network to Serial Packet Delimiter:** This group of options is the same as the delimiters described above, but they control data flow in the opposite direction. The LES920 series will store data from the network interface in its queue. Until one of the delimiter conditions described above is met, the LES920 series will send the data over to the serial interface.
- **Character Send Interval:** This option specifies the time gap between each character. When set to one second (1000ms), the LES920 series would split the data in the queue and only transmit one character (a byte) every second. The maximum value for this option is 1000 milliseconds or one second. This option is disabled by default.

Serial

- **Serial FIFO:** By default, the LES920 series 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 be 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 of the serial device. Note that disabling this option on baud rates higher than 115200bps would noticeably reduce the data integrity.
- **Serial Buffer:** By default, the LES920 series will empty its serial buffer when a new TCP connection is established. This means that the TCP application will not receive buffered serial data during a TCP link breakage. To keep the serial data when there is no TCP connection and send out the buffered serial data immediately after a TCP connection is established, you can disable this option.

After finishing configuring the COM Port's **Advanced Settings**, click on the **Save & Apply** button to keep the change(s) that you have made. Then, close the **Advanced Settings** browser window by clicking on the **Close** button. You will be returned to the **COM 1 Port Setting** page.

4.9 SNMP/ALERT Settings

The Simple Network Management Protocol (SNMP) is used by network management software to monitor devices in a network, to retrieve the device's network status information, and to configure the device's network parameters. The **SNMP/ALERT Settings** page showed in Figure 4-54 allows you to configure the LES920 series device so that it can be viewed by third-party SNMP software, and it allows the LES920 series to send alert events to an administrator and SNMP trap server.

> SNMP/ALERT Settings

SNMP/ALERT Settings

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

<i>Basic Data Objects</i>	
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 style="border: none; border-bottom: 1px solid #ccc;" type="text" value="v1 / v2c"/>
Read Community	<input type="text" value="public"/>
Write Community	<input type="text" value="private"/>
SNMP Trap Server	
SNMP Trap Server	<input type="text" value="0.0.0.0"/>

Event alert settings

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

Figure 4.54 SNMP/Alert Settings Web Page

The LES920 series provides three basic SNMP fields under the **Basic Data Objects** section. “**System Contact**” is typically used to specify the device's contact information in case of emergency (default value is “contact”); “**System Name**” is typically used to identify this device (default value is “System”); and “**System Location**” is typically 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 entering the two passphrases (or SNMP Community Strings) below it. Note that when the SNMP is unchecked, three setting option lines will not show up as depicted in Figure 4-54. By entering the passphrase for the "**Read Community**," the LES920 series device allows other network management software to read its information. By entering the passphrase for the "**Write Community**," the LES920 series device allows other network management software to read/modify its information. The default LES920 series' SNMP Community Strings (or passphrases) for **Read Community** and **Write Community**, as shown in Figure 4., are "public" and "private," respectively.

Additionally, you can set up a **SNMP Trap Server** in the network to receive and collect all alert messages from the LES920 series. To configure the LES920 series to dispatch alert messages originated from any unexpected incidents, enter the IP Address of the **SNMP Trap Server** in the field shown in Figure 4.. Note that any changes in these settings will take effect after the LES920 series device is restarted.

Under the **SNMP Trap Server** section, there is a list of **Alert Types** under the **Event alert settings** box in Figure 4.. There can be up to two possible actions for each alert event: **Email** and **SNMP Trap**. You can enable the associated action(s) of each alert event by checking the box under the column of **Email** and/or **SNMP Trap**. When the **Email** box is checked and the corresponding event occurs, it will trigger an action for the LES920 series to send an e-mail alert to designated addresses configured in the E-Mail Settings (described in the next section). When the **SNMP Trap** box is checked and the corresponding event occurs, it will trigger an action for the LES920 series to send a trap alert to the designated SNMP Trap server (specified in the above paragraph). There are multiple events that will trigger the alarm from the LES920 series, as listed in Figure 4.. However, some events can only be reported by e-mail. These alerts are useful for security control or security monitoring of the LES920 series device:

- **Warm Start:** This event occurs when the device resets.
- **Authentication Failure:** This event occurs when an incorrect username and/or password are entered, which could indicate unauthorized access to the LES920 series.
- **IP Address Changed:** This event occurs when the LES920 series device's IP address is changed.
- **Password Changed:** This event occurs when the administrator password is changed.

After configuring the **SNMP/Alert Settings**, click on the **Save & Apply** button to keep the change(s) that you have made and to apply your setting(s). The web browser will remain on the **SNMP/Alert Settings** page. If you want to cancel the change(s) and reset all changes back to their original values, click on the **Cancel** button.

Note: "Cold Start" and "LAN Link Down-Relay" options are only available for some specified models. For unsupported models, the "Cold Start" event option will not display on the page.

4.10 E-Mail Settings

When the LES920 series 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 LES920 series to be able to send an e-mail. Figure 4. shows the **E-mail Settings** page in which there are two configurable parts: **E-mail Address Settings** and **E-mail Server**. For the **E-mail Address Settings** part, a **Sender's** e-mail address is required to be entered in the **Sender's** text box which will be used in the **From** field of the e-mail. Note that the maximum length of the sender's email address is 48 characters. For the **Receiver's** text box you can enter multiple recipients which will be used in the email's **To** field. When entering multiple receiver email addresses in the **Receiver's** text box, separate each email 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. ☐ Enable TLS/SSL

User name

Password

Save & Apply Send Test Mail Cancel

Figure 4.55 E-mail Setting Web Page

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



Attention

It is also important to set up the Default Gateway and DNS Servers in the Network Settings properly so that the LES920 series can look up domain names and route the emails to the proper default gateway. Refer to the Default Gateway and DNS Server Settings in Section 4.7.

After configuring the **Email Settings**, click on the **Save & Apply** button to keep the change(s) that you have made and to apply your setting(s). 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, click on the **Cancel** button.

4.11 VPN

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private networks, while benefiting from the private network's functionality, security, and management policies. This is done by establishing a virtual, point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. Figure 4-56 illustrates a VPN scenario of the LES920 series device for your reference.

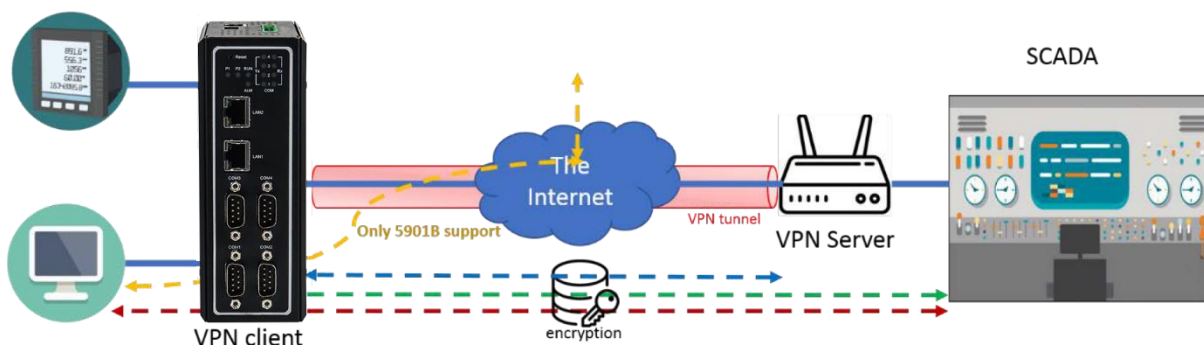


Figure 4.56 VPN Scenario of the LES920 Series

The LES920 series industrial device server supports a number of VPN protocols which are PPTP (Point-to-Point-Tunneling-Protocol), IPsec (Internet Protocol Security), and OpenVPN. In order to configure a VPN, click on the related item in the dedicated VPN sub-menu on the left side of the screen, as shown in Figure 4-57. A detailed description of PPTP is available in Section 4.11.1. IPsec's basic will be discussed in Section 4.11.3 while IPsec related setting will be described in Section 4.11.4. Finally, OpenVPN Settings and Keys are described in Section 4.11.10 and Section 4.11.11, respectively.

```

- VPN
  PPTP
  PPTP Status
  IPsec Settings
  IPsec Status
  OpenVPN Settings
  OpenVPN Keys
  OpenVPN Status

```

Figure 4.57 VPN Menu Structure

4.11.1 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 shows the PPTP configuration page under the PPTP web setting. Currently the LES920 series only supports PPTP client. After settings are completed, click on “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 4.58 PPTP Configuration Page

To enable a PPTP client on the LES920 series, check the box for **Enable PPTP Client** option under the **PPTP Client Settings** as shown in Figure 4-58. Then, configure the following list of options:

- **Always on:** Checking this box will enable the LES920 series to automatically reconnect PPTP in the event of disconnection.
- **PPP Authentication:** This option specifies the authentication algorithm for PPTP which can be either Only **PAP** or **PAP/CHAP/MS-CHAP/MS-CHAPv2**. However, the section should be the same as the PPTP server.
- **PPP Encryption:** This option sets the encryption mode which can be either **Disable** or **MPPE (128bit)**. Once again, this setting should be the same as the PPTP server.

- **Remote IP address:** Enter the IP address of the PPTP server in this field.
- **User Name:** Enter the username of the PPTP client that will be used for authentication.
- **Password:** Enter the password of this PPTP client for authentication.

4.11.2 PPTP Status

To check the PPTP link status, click on the PPTP Status sub-menu under the VPN menu as shown in Figure 4.12. This web page provides information about the Local Virtual IP Address, Remote Virtual Address, and PPTP connection status. This page also allows the user to initiate a connection or disconnect the link using the Connect and Disconnect buttons, respectively. To obtain the latest PPTP status, click on the Refresh button. Table 4.1 summarizes fields and descriptions on this web page.

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

Figure 4.12 PPTP Link Status

Table 4.1 Description of Fields in PPTP Link Status Web Page

Field Name	Description
Local Virtual IP Address	The virtual IP address of PPTP server
Remote Virtual IP Address	The virtual IP address of PPTP server
Status	This field shows the PPTP tunnel connection status: - Disconnect means that no tunnel is established. - Connect means that PPTP tunnel is established. - Connecting means that PPTP tunnel is establishing.
Connect Button	Click on this button to connect to the PPTP server.
Disconnect Button	Click on this button to disconnect from the PPTP server.
Refresh Button	Click on this button to refresh the PPTP tunnel's status on this web page.

4.11.3 IPsec

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

The LES920 series 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 the LES920 series: **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** is used to create a Virtual Private Network (VPN), and it 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** follows:

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** follows:

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 (LES920 series) and a peer device, such as another LES920 series device. Note that this type of connection cannot be used for accessing entire sub-network resources. Figure 4.13 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode**.

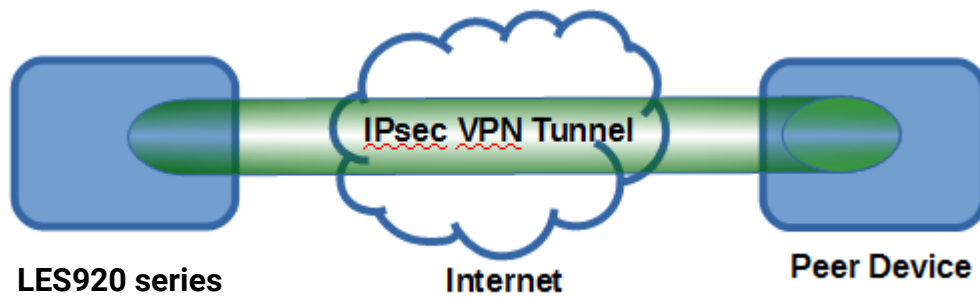


Figure 4.13 Example of Host-to-Host Connection

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 4.14 illustrates a road-warrior application in which the LES920 series can access a remote sub-network resource via a peer gateway. Figure 4-62 illustrates a gateway application in which the LES920 series can passively accept connection requests from remote sides and provide access to the LES920 series' sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

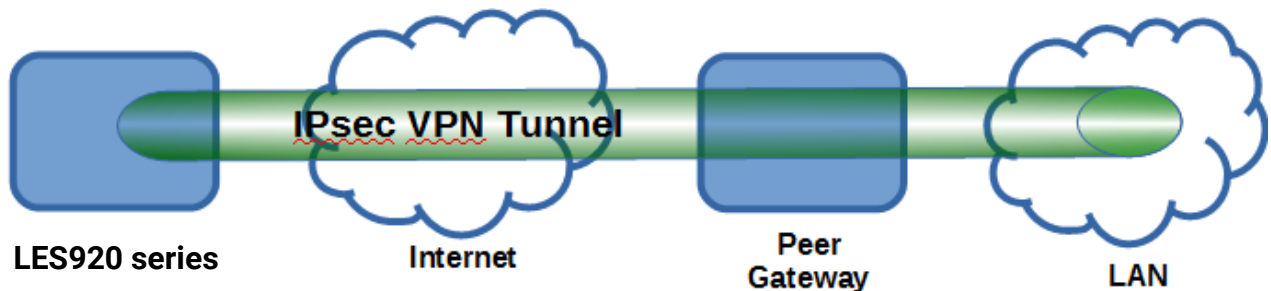


Figure 4.14 Roadwarrior Application using Host-to-Subnet Connection

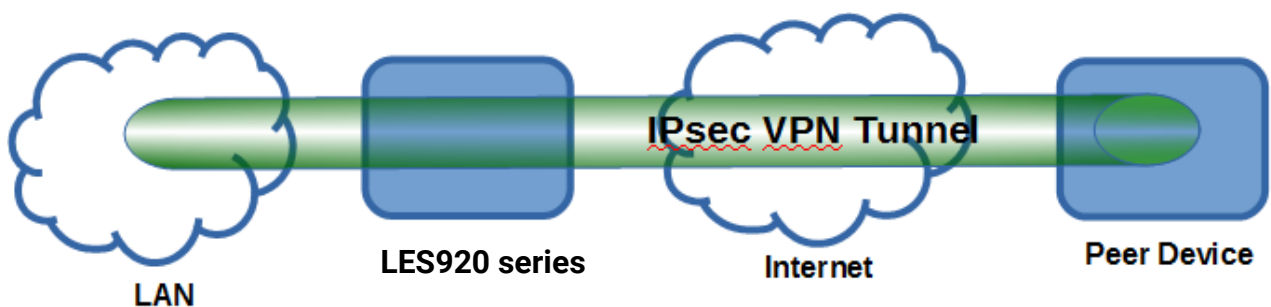


Figure 4.62 Gateway Application using Host-to-Subnet Connection

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 4.15 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 4-64. On the other hand, two different devices on two different subnets (host-host application) can be connected via an IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 4-65. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

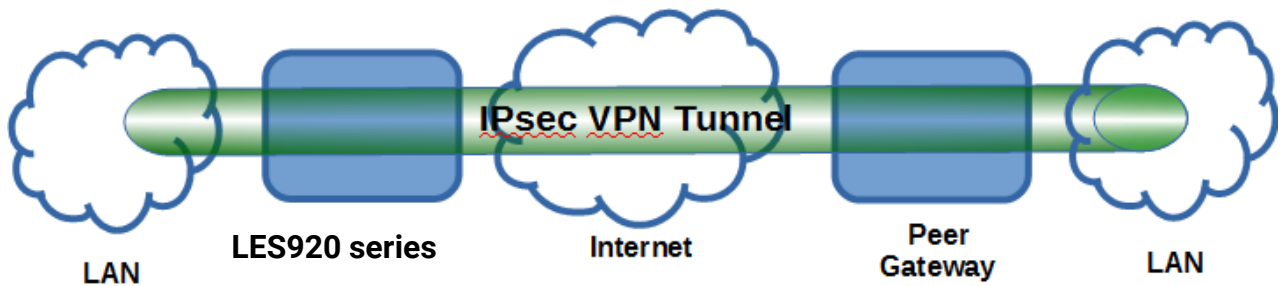


Figure 4.15 An example of network application using a subnet-to-subnet connection via the LES920 series and a peer device

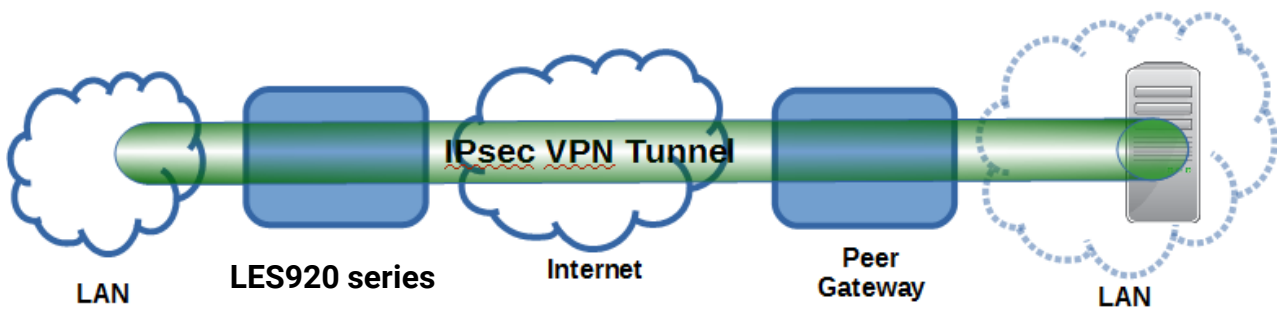


Figure 4.64 An example of host-network application via the subnet-to-subnet connection

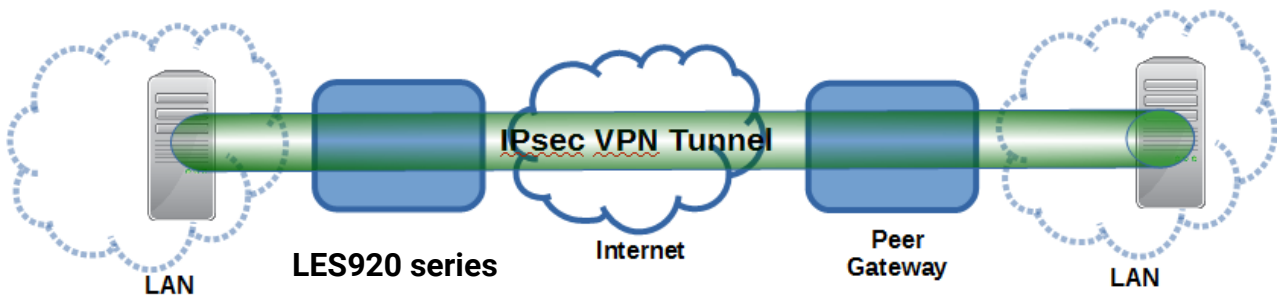


Figure 4.16 An example of host-host application via the subnet-to-subnet connection

In some network configurations, there is an implementation of network address translation (NAT) on its gateway/routers. NAT is typically used to allow private IP addresses on private networks behind gateways/routers with a single public IP address connecting to the public Internet. The internal network devices can 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.

The LES920 series also has a feature called NAT traversal (NAT-T) that allows the IPsec tunnel to pass through the NAT in its network. The LES920 series will activate this option automatically and encapsulate the IPsec packets inside UDP port 4500 to be able to pass through a NAT router.

To provide security service for all types of tunnel connections and applications described above, the LES920 series utilizes the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite. Note that IKE builds upon the Oakley protocol and ISAKMP (Internet Security Association and Key Management Protocol). IKE uses X.509 certificates for authentication either pre-shared or distributed using DNS (preferably with DNSSEC). IKE also uses a Diffie-Hellman key (DH) key exchange to set up a shared session secret from which cryptographic keys are derived. The IPsec security association (SA) is divided into two phases. In phase one, IKE creates an authenticated secure channel between the LES920 series 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 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.

4.11.4 IPsec Settings

Figure 4-66 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.

VPN > IPsec Settings

IPsec Settings

General Settings	
IPsec	<input type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static: <input type="text" value="10.0.50.100"/>
Remote Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: <input type="text" value="192.168.1.0"/> / <input type="text" value="24"/>
Local Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: <input type="text" value="10.0.50.0"/> / <input type="text" value="24"/>
Connection Type	<input type="text" value="Tunnel"/> ▼

Authentication Settings	
Method	<input checked="" type="radio"/> Pre-Shared Key: <input type="text" value="secrets"/>
Local ID	<input type="text" value="IP"/> ▼ <input type="text"/>
Remote ID	<input type="text" value="Any"/> ▼ <input type="text"/>

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.

Save Cancel

Figure 4.17 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:

- **IPsec:** By checking the box for this option, you enable the IPsec feature for the LES920 series.
- **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: Dynamic and Static.
 - **Dynamic:** When you select Dynamic by choosing the Dynamic radio button, the Peer Address or the remote device IP address is not fixed (unknown). Note that when Peer Address is set to dynamic mode, the LES920 series can accept a remote connection request or will be the responder.
 - **Static:** If you know the remote device's IP address, you can choose the radio button for Static option and enter the IP address in the corresponding text box. The LES920 series will be the initiator/responder.
- **Remote Subnet:** This option indicates whether you want to create an IPsec connection to the remote subnetwork. There are also two choices for Remote Subnet access: None (Host Only) and Network.
 - **None (Host Only):** This option indicates that the remote subnet is not supported (no remote subnet), and only host access is supported. The remote end of the IPsec tunnel is a host- or peer-device only.
 - **Network:** This option indicates the Remote Subnet. Enter 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, the Subnet IP Address is 192.168.11.0 and the Subnet mask is 24 bits (from 255.255.255.0).
- **Local Subnet:** This option enables an IPsec connection to the local subnetwork. There are two choices for Local Subnet access:
 - **None (Host Only):** This option specifies that the local subnet is not supported (no local subnet), and only local host access is supported. The local end of the IPsec tunnel is a host or peer device only.
 - **Network:** This option specifies 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, the Subnet IP Address is 192.168.11.0 and the Subnet mask is 24 bits (from 255.255.255.0).
- **Connection Type:** This option specifies the IPsec connection type, which can be either Tunnel mode or Transport mode. 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 **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 passphrase in the corresponding text box. Both ends of the VPN tunnel must use the same secret key or password. The pre-shared key can be 1 to 60 case-sensitive ASCII characters and special symbols.

The next option is the Remote ID. This is used to authenticate the remote certificate during Phase 1 IKE negotiation. To allow both sides of the tunnel to authenticate each other, you must select the local and remote identities and enter the **IDs** in the textboxes behind the **Local ID** and the **Remote ID**. Note that the available options for **Local ID** are **IP address**, **E-mail address**, or **Domain Name** while the available options for **Remote ID** are **Any**, **IP address**, **E-mail address**, or **Domain Name**. Note that if you select “**Any**” for Remote ID, you do not have to enter anything in the text box, and the remote ID will not be verified. If authentication IP is chosen for Remote ID but no IP address is configured in the field and the **Peer Address** is set to **Static Address** type (see above), then the LES920 series will use the static IP as the authentication IP.

The third part of **IPsec Settings** is the **IKE** (Internet Key Exchange) **Settings**. The Internet Key Exchange (IKE) that the LES920 series 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 exchanges information about the encryption algorithms that they support and then establish a temporary secure connection to exchange authentication information.

- The first option is the **Mode** of IKE session which defines how many steps or packets will be used or exchanged during the IKE SA negotiation. You can choose either **Main Mode** or **Aggressive Mode**. The **Main Mode** will send SA proposals, Diffie-Hellman public key, and ISAKMP session authentication in three exchange packets, while the **Aggressive Mode** will put all SA proposals, DH public key, and ISAKMP session authentication 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.
- The second option is the selection of Diffie-Hellman’s group (**DH Group**) of standardized global unique prime numbers and generators that will be used to provide secure asymmetric key exchange. The **DH Group** is used to encrypt this IKE communication. The LES920 series supports two **DH groups** which are **DH Group 2**, which is a 1024-bit modular exponentiation group (MODP), and **DH Group 5**, which is a 1536-bit MODP group.
- The third option is the selection of **Encryption Algorithm** which can be either **AES-128** or **3DES**. This option will select the key size and encryption algorithm to be used in the IKEv1 Phase 1. The default value is **AES-128**.
- The fourth option is the selection of **Authentication Algorithm** which can be either **SHA1** or **MD5**. This option will select which hash algorithm will be used to authenticate packet data in the IKEv1 Phase 1. The default value is **SHA1**.
- The fifth option is the **SA Life Time** which must be set in units of seconds. This value represents the lifetime of the IKE key which is dedicated at Phase 1 between both end host or network. The default **SA Life Time** is 10800 seconds. The configurable range for **SA Life Time** is between 300 to 86400 seconds.

Within the **Phase 2 SA**, there are five security options to be configured. Similar to **Phase 1 SA**, the LES920 series 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, the LES920 series also supports two **DH groups**: **DH Group 2** (1024-bit) and **DH Group 5** (1536-bit).

Then you can proceed to select encryption and authentication algorithms. The 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 **AES128**. The 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 **SHA1**. Finally, the last option is the **SA Life Time** for phase 2, which must be set in units of seconds. The range of this setting can be from 180 to 86400 seconds. The default **SA Life Time** is 3,600 seconds.

The final part of the **IPsec Settings** is the **Dead Peer Detection Settings**. Dead peer detection (DPD) is a mechanism that the LES920 series uses to verify the existence of a remote Internet Key Exchange (IKE) gateway or the peer device of the LES920 series. To detect the peer device, the LES920 series will send encrypted IKE Phase 1 notification payloads (or hello message) to its peer device and wait for DPD acknowledgement from the peer device. If the LES920 series does not receive an acknowledge message during a specific time interval (**DPD timeout**), it will consider that the peer device is dead. Then, the LES920 series 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 LES920 series 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 the LES920 series 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 the LES920 series 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 LES920 series will take the PDP action. The **DPD Timeout** value range from 1 to 65535 seconds. The default value of **DPD Timeout** is 120 seconds. A description of each parameter on the IPsec Tunnels web page is summarized in Table 4.2.

Table 4.2 Description of Parameters in IPsec Tunnels Web Page

Field Name	Description	Default Value
General Settings		
IPsec	Enables the IPsec Tunnel	Disable
NAT Traversal	Enables the NAT Traversal mechanism	Enable
Peer Address	IP address of the remote device which can be dynamic (any address) or static (fixed address)	Dynamic

Field Name		Description	Default Value
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

Field Name		Description	Default Value
	SA Life Time	Value that represents the lifetime of the IKE key which is dedicated in Phase 2 between both end host or network. The available setting ranges is from 180 to 86,400 seconds.	28800
Dead Peer Detection Settings			
DPD Action		Select either Hold or Restart the tunnel's security association for the peer. Note that Hold is suitable for a statistically defined tunnel.	Hold
DPD Interval		Duration of time for sending hello message to the peer device: value from 1 to 65535 seconds.	30 seconds
DPD Timeout		Duration of time to declare that the peer is dead: value from 1 to 65535 seconds.	120 seconds

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

4.11.5 IPsec Status

On this web page, you can check the status of your IPsec connection between the LES920 series and its peer device in different connection types and modes. Peer Address is the IP address of the other device that is connected to the LES920 series. The VPN Tunnel's status is also provided. The Status of the IPsec connection, which can be Disabled, Listening, or Connected, is also listed. Figure 4.18 shows the IPsec Status web page under the IPsec Settings menu. There are three buttons at the end of the web page: Connect, Disconnect, and Refresh. The Connect and Disconnect buttons allow you to establish or tear down the IPsec connection. The Refresh button enables you to check the latest connection status.

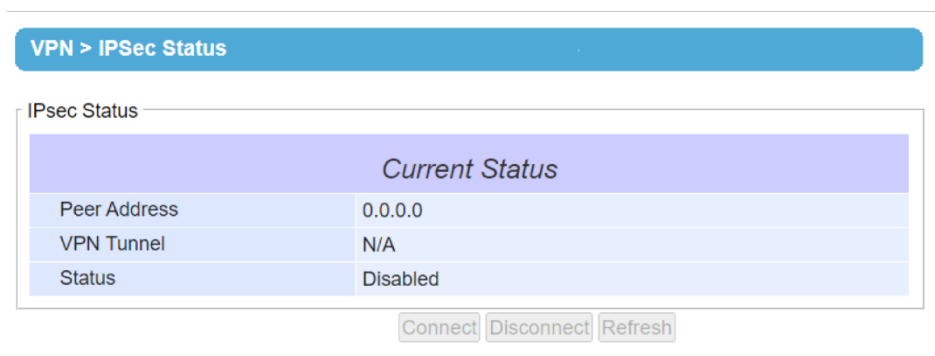


Figure 4.18 IPsec Status Web Page

4.11.6 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 your preference. Refer to the previous section for details regarding **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 for the LES920 series.

4.11.7 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 4.19. Follow the steps provided next for each scenario to set the **General Settings**.

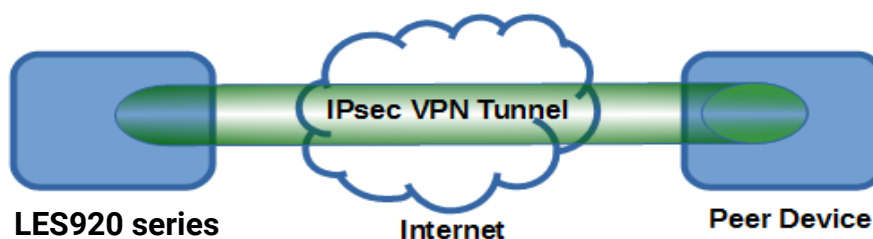


Figure 4.19 IPsec VPN Tunnel with Host-to-Host Topology

Scenario: host-to-host with static peer as shown in Figure 4.20

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
Note: When a peer address is entered as the static address, the LES920 series acts as an **initiator** which takes the initiative and establishes a connection. The LES920 series also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Select the radio button for **None (Host Only)** in the **Remote Subnet** field.
- Since this VPN connection is established on two hosts, the **Connection Type** option can be either **Transport** or **Tunnel**.

General Settings	
IPsec	<input type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static: 10.0.50.100
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 4.20 General Settings for Host-to-Host with Static Peer

Scenario: host-to-host with dynamic peer as shown in Figure 4-70

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
Note: When the VPN connects to a peer with a dynamic IP address, the LES920 series acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- The remaining settings are the same as the host-to-host with static peer scenario described above.

General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static: 10.0.50.100
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 4.21 General Settings for Host-to-Host with Dynamic Peer

4.11.8 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 LES920 series is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in Figure 4.22. Follow the steps provided next for each scenario to set the **General Settings**.

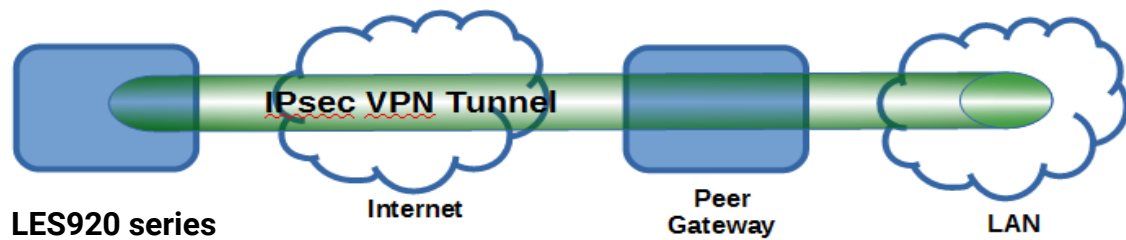


Figure 4.22 IPsec VPN Tunnel with Host-to-Network Topology

Scenario: host-to-network with static peer as shown in Figure 4.23

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
Note: When a peer address is entered as a static address, the LES920 series is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. The LES920 series also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.

General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static: <input type="text" value="10.0.50.100"/>
Remote Subnet	<input type="radio"/> None (Host Only) <input checked="" type="radio"/> Network: <input type="text" value="192.168.1.0"/> / <input type="text" value="24"/>
Local Subnet	<input checked="" type="radio"/> None (Host Only) <input type="radio"/> Network: <input type="text" value="10.0.50.0"/> / <input type="text" value="24"/>
Connection Type	Tunnel <input type="button" value="v"/>

Figure 4.23 General Settings for Host-to-Network with Static Peer

Scenario: host-to-network with dynamic peer as shown in Figure 4.24

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
Note: When a VPN connection is set to a peer with dynamic IP address, the LES920 will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.

General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static: 10.0.50.100
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 4.24 General Settings for Host-to-Network with Dynamic Peer

4.11.9 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 LES920 series is the gateway to a local network in these scenarios. A network-to-network topology for both scenarios is illustrated in Figure 4.25. Follow the steps provided next for each scenario to set the **General Settings**.

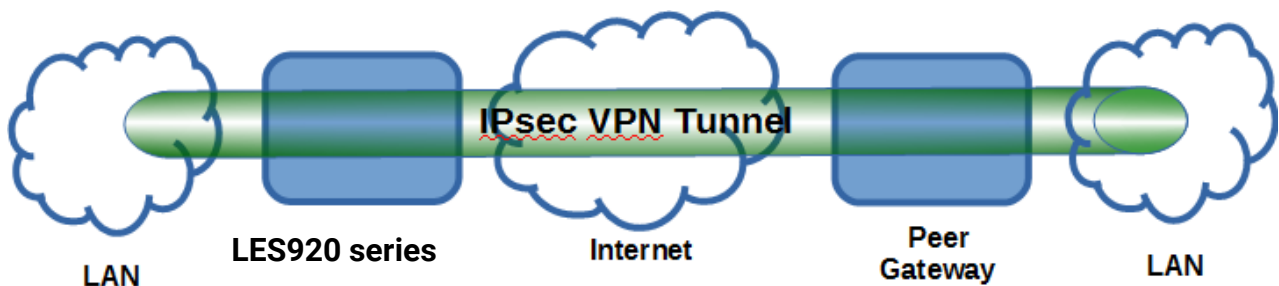


Figure 4.25 IPsec VPN Tunnel with Network-to-Network Topology

Scenario: network-to-network with static peer as shown in Figure 4.26

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
Note: When a peer address is entered as a static address, the LES920 series is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. The LES920 series 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 subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.

IPsec Settings

General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static: 10.0.50.100
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 4.26 General Settings for Network-to-Network with Static Peer

Scenario: network-to-network with dynamic peer as shown in Figure 4.27

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
Note: When a VPN connection is set to a peer with dynamic IP address, the LES920 series 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 subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.

General Settings	
IPsec	<input checked="" type="checkbox"/> Enable
Peer Address	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static: 10.0.50.100
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 4.27 General Settings for Network-to-Network with Dynamic Peer

4.11.10 OpenVPN Setting

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: TAP and TUN. The product can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, you have to specify which type of OpenVPN connection scenario is to be adopted. Currently the LES920 series only supports TUN mode.

In order to configure OpenVPN, click on the VPN tab in the left side of the menu and then **OpenVPN Settings**. The user interface is shown in Figure 4.28.

VPN > OpenVPN Settings

OpenVPN Settings

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 4.28 OpenVPN Setting

The OpenVPN parameters are described below:

OpenVPN: Check this box to enable OpenVPN.

- **Mode:** This parameter specifies what the role of this device will be, which can be either **Server** or **Client**. When choosing server mode, the device will play as server role and will wait for client connection.
- **Protocol:** The user can select the transport layer protocol that will be used for VPN (TCP or UDP).
- **Port:** This parameter defines the port number for TCP/UDP connection.
- **Device Type:** OpenVPN tunnel connection by TUN (Tunnel) mode or TAP mode. Currently the LES920 series only supports TUN (Tunnel) mode.
- **Virtual IP (only when “OpenVPN Server” mode is selected):** This field specifies the server’s virtual IP. Virtual IP will only be available when SSL/TLS is chosen as the Authentication Mode. The Server’s virtual IP address will be 10.8.0.1/24, and the client’s virtual IP address will be 10.8.0.x/24.
- **Local/Remote endpoint IP (only when “OpenVPN Client” mode is selected):** This fields specifies the local and remote endpoint virtual IP address of this OpenVPN gateway. Local/Remote endpoint IP will be available when static key is chosen in Authentication Mode.
- **Authentication Mode:** This parameter specifies the authorization mode of the OpenVPN server. There are two options available:
 - **SSL/TLS and SSL/TLS (TLS Auth):** When OpenVPN uses TLS authorization mode, the CA Cert, Server Cert and DH PEM will be used. See the next Section 4.11.11 for more details.

- **Static Key:** When OpenVPN uses static key authorization, the static key will be used. See the next Section 4.11.11 for more details.
- **Encryption Cipher:** This parameter specifies the Encryption cipher. There are five options available: Blowfish, AES 256, AES 192, AES 128, and Disable. When the Disable option is selected, no encryption will be used.
- **Hash Algorithm:** This parameter specifies the Hash algorithm. There are five options available: SHA1, MD5, SHA 256, SHA 512, and Disable. When the Disable option is selected, no Hash algorithm will be used.
- **Compression:** This parameter specifies whether or not the tunnel packets will be compressed. There are three options available: LZ4, LZO, and Disable. When the Disable option is chosen, the packet will not be compressed.

4.11.11 OpenVPN Keys

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

VPN > OpenVPN Keys

OpenVPN Keys

Current Key Information	
Certificate Authority	<pre>-----BEGIN CERTIFICATE----- MIIEEnjCCA4agAwIBAgIJANF2PvJOIGsEMA0GCSqGSIb 3DQEBCwUAMIGQMwCQYD VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAwD gYDVQQHEwdlc2luY2h1MQ0wCwYD</pre>
Server Certificate	<pre>Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) Signature Algorithm: sha1WithRSAEncryption</pre>
Server Key	<pre>-----BEGIN PRIVATE KEY----- MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKggSkAg EAAoIBAQQDdcJ08jV4begz1 7YT/OQoCzJviDtmD0+rCG+XHj8E+w+IGlxiTMzwRZ6q O0sl/iUHIXBsUMV9P7B+W</pre>
Diffie Hellman parameters	<pre>-----BEGIN DH PARAMETERS----- MIIBCAKCAQEYaj6yGkOUXNnznNfZIH9CUY250P0Tdd YfF8OwaL7jm8jVKiUWeuqU +DbGEw2QRDazrsNj3qaDzP84ZXJxxlJD1tCXdUPQ0G NeL4ItIguF2H6I5M/0RxFU</pre>

Figure 4.29 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 server certificate's information. You can check the information if you use upload server certificate file.
- **Server Key:** It shows the server key's information. You can check the information if you use upload server key file.
- **Diffie Hellman parameters:** It shows the Diffie Hellman parameter information.

When the LES920 series acts as OpenVPN server, you can define your 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 as shown in Figure 4.30. Fill in the parameters and click on the **“Generation Keys & Apply”** button.

OpenVPN Keys Generation

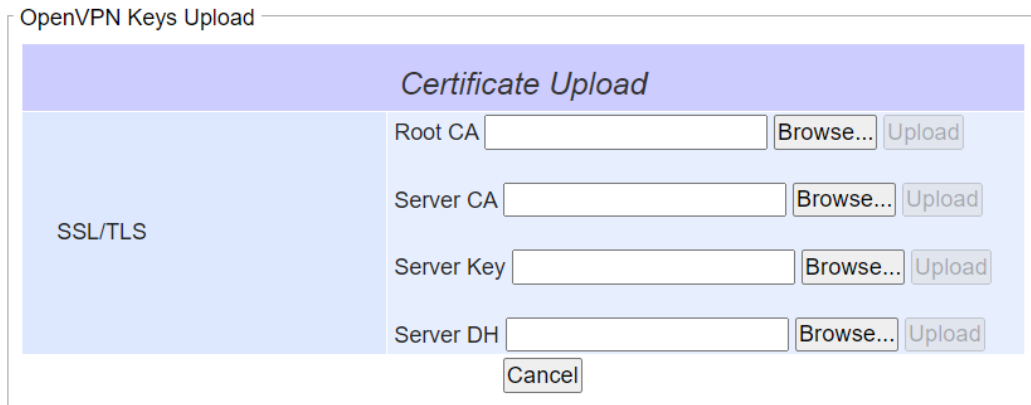
Certificate Information	
Country Code	<input type="text" value="TW"/>
State	<input type="text" value="Taiwan"/>
City	<input type="text" value="Hsinchu"/>
Organization	<input type="text"/>
Organizational Unit	<input type="text"/>
Email Address	<input type="text"/>
Common Name (Read Only)	<input type="text"/>
Expire time (Read Only)	<input type="text" value="10"/> (years)
<input type="button" value="Generation Keys & Apply"/>	

Figure 4.30 Certification Information

To generate OpenVPN keys, complete the information under the Certificate Information box in Figure 4.30. The following list briefly describes each field in the Certificate Information box:

- **Country Code:** Enter the country's ISO code in this field.
- **State:** Enter the name of the state (if applicable), in this field.
- **City:** Enter the city's name in this field.
- **Organization:** Enter the organization's name in this field.
- **Organization Unit:** Enter the organization's unit or section in this field.
- **Email Address:** Enter an email address in this field.
- **Common Name:** This is the server's name. (Read only)
- **Expire time:** This is 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 4.31 will appear, and it will allow you to import the related server or client certificates.



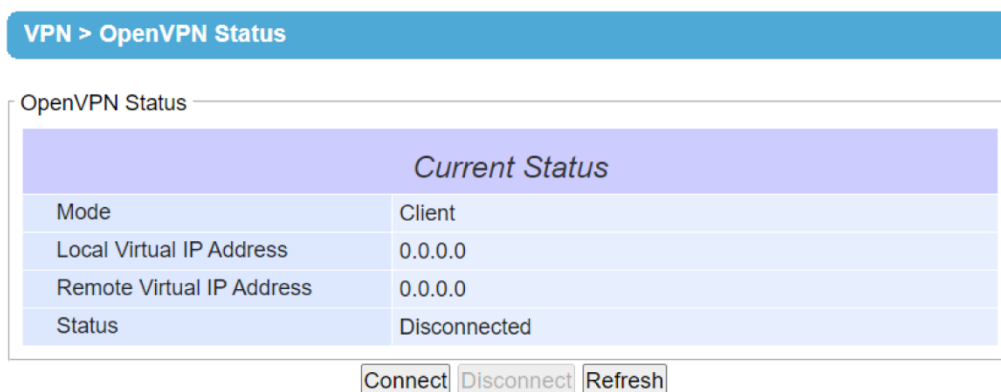
The image shows a web interface titled "OpenVPN Keys Upload". It features a light blue sidebar on the left with the text "SSL/TLS". The main area has a purple header "Certificate Upload". Below the header, there are four rows of input fields, each with a "Browse..." button and an "Upload" button. The rows are labeled "Root CA", "Server CA", "Server Key", and "Server DH". At the bottom center, there is a "Cancel" button.

Figure 4.31 Certificate Upload

Click on the **Browse** button to select your own server or client certificate, and then click on the **Upload** button. When the LES920 series acts as an OpenVPN server, use the **Export All Keys** button to download all the necessary certificates including CA.crt, CA.key, and the certificate and the key for the client side.

4.11.12 OpenVPN Status

In order to check the current OpenVPN connection status, click on "OpenVPN status" in the VPN menu on the left side of the screen. A web page similar to Figure 4.32 or Figure 4.33 will appear, depending on whether OpenVPN is set as a Client or a Server.



The image shows a web page titled "VPN > OpenVPN Status". It contains a table with the following data:

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

Below the table, there are three buttons: "Connect", "Disconnect", and "Refresh".

Figure 4.32 OpenVPN Client Status

A description of each field under the Current Status of OpenVPN when it is in Client mode appears below:

- **Mode:** This indicates the OpenVPN mode that the LES920 series is currently running as.
- **Local Virtual IP address:** This field displays the Local virtual IP address.
- **Remote Virtual Status:** This field displays the Remote virtual IP address.

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

The screenshot shows a web interface for 'VPN > OpenVPN Status'. It contains a table for 'Current Status' and a table for 'Client List'. The 'Current Status' table shows Mode: Server, Local Virtual IP Address: 0.0.0.0, and Status: Deactivated. The 'Client List' table has headers: Common Name, Real Address, Virtual Address, and Since. Below the tables are buttons for 'Activate', 'Deactivate', and 'Refresh'.

Current Status	
Mode	Server
Local Virtual IP Address	0.0.0.0
Status	Deactivated

Client List			
Common Name	Real Address	Virtual Address	Since

Figure 4.33 OpenVPN Server Status

The description of each field under the Current Status of OpenVPN when it is in Server mode appears below:

Mode: This indicates the OpenVPN mode that the LES920 series is currently running as.

- **Local Virtual IP address:** This field displays the Local virtual IP address.
- **Status:** This field displays the current status of OpenVPN connection. It can be either be **Deactivated**, **Activating**, **Disconnected**, **Connecting**, or **Connected**.
- **Client List:** This table provide the list of clients and their information, which are **Common Name**, **Real Address**, **Virtual Address**, and **Since** (the time stamp).

4.12 Log Settings

Under the **Log Settings** menu for the web interface of the LES920 series Industrial Serial Device Server, you can configure various data logging for the device. Figure 4.34 lists the sub-menu under the **Log Settings**. It consists of **System Log Settings**, **COM Log Settings**, **Event Log**, and **COM Data log**. Each part of this sub-menu will be described in the following subsections.

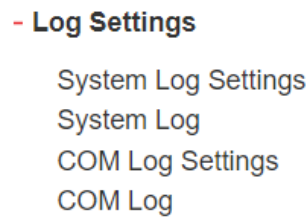


Figure 4.34 General Example of the Log Setting Menu

4.12.1 System Log Settings

The Syslog function is turned on by default and cannot be turned off for the LES920 series. It is used to keep a log for system events and report to an external Syslog server, if necessary. Figure 4.35 shows the **System Log Settings** page under the **Log Settings** menu. A description of each option follows below:

Log Settings > System Log Settings

System Log Settings

Log to Flash	<input type="checkbox"/>
Log Facility	<input checked="" type="checkbox"/> Auth <input checked="" type="checkbox"/> Authpriv <input checked="" type="checkbox"/> Daemon <input checked="" type="checkbox"/> User <input checked="" type="checkbox"/> Local0
Log Level	3: (LOG_ERR) ▼
Log Size	5M ▼
Log to Syslog Server	<input type="checkbox"/>
Server IP Address	0.0.0.0
Server Port Number	514 (1~65535, default=514)

Save & Apply Cancel

Figure 4.35 Log Settings Web Page under Log Settings

- **Log Event to Flash:** When the check box is enabled, the LES920 series 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.

- **Log Facility:** The facility represents the device process that created the Syslog event.

Facility Name	Description
Auth (Authorization)	Security or authorization messages
Authpriv (Private Authorization)	Private security or private authorization messages
Daemon	A miscellaneous system daemon message
User	User level messages
Local0	Locally defined messages

- **Log Level:** The **log level** also known as **log severity**; a smaller log level number means more sensitive.

Log Level	Description
3: (LOG_ERR)	This will log errors and any more sensitive events.
4: (LOG_WARNING)	This will log warnings and any more sensitive events.
6: (LOG_INFO)	This will log some useful information and any more sensitive events.

- **Log Size:** The default total log space is 5MB; the device will overwrite the old logs when the log space is full.
- **Syslog Server:** When the check box is enabled, it will allow the LES920 series 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 the Syslog Server.
- **Server IP Address:** You must specify the IP address of a remote Syslog Server in this field.
- **Server Service Port:** This option allows you to specify the remote Syslog Server Port number between 1 and 65535. Note that the default port number is 514.

After finishing configuring the **Log Settings**, click on the **Save & Apply** button to keep the change(s) that you have made and to apply your setting(s). The web browser will remain on the **Log Settings** page. If you want to cancel the change(s) and reset all changes back to their original values, click on the **Cancel** button.

4.12.2 System Log

This page displays the current event log or system log stored in the LES920 series device. Figure 4.36 shows an example of logged event. In the Severity option, you can choose the level of severity (i.e., Err, Warn, Info) to inspect from the drop-down box. The Modules option allows you to view only the log from today or all available logs.

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

Log Settings > System Log

System Log

System Log

Severity	Err ▾
Modules	<input checked="" type="checkbox"/> All

Show entries
Search:

#	Time	Sev.	Message
1	Jan 01, 1970 17:40:43	ERR	[Sys] [Dial] No SIM card detected!

Showing 1 to 1 of 1 entries

Previous
Next

Figure 4.36 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. Click on the “**Previous**” link to go to the last page of the log, and click on the “**Next**” button to go to the next page. At the top of the **System Log** table, there are three buttons: **Refresh**, **Export Log**, and **Clear Log**. To display the latest event, click on “**Refresh**” button. When you click on the Export Log button, a log file will be saved on to your PC. By clicking on “**Clear Log**” button, you can clear all events stored in the device, and the **System Log** will be empty. A message “No data available in table” will be displayed in the middle of the table. Moreover, you can choose from the drop-down list of 10 or 25 entries for the **Show entries**. Finally, you can search over the **System Log** by entering a keyword in the **Search** box.

4.12.3 COM Log Settings

Transmitted data through the COM port could be logged for recording or debugging purposes. Additionally, the logs could be reported to an external Syslog server as well. Figure 4.37 shows the **COM Log Settings** page under the **Log Settings** menu. A description of each option follows next:

Log Settings > COM Log Settings

COM Log Settings

☒ Log Data Contents Types ☐ HEX ☒ ASCII

COM Ports ☒ COM1

Enable Syslog Server ☒ Enable

IP Address 111.109.0.0

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

Save & Apply Cancel

Figure 4.37 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, the COM logging function will only log the length of data to reduce system load.

Note: The LES920 series 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 you to select the desired logged data's format.
- **COM Ports:** You can select which port(s) will be logged by checking the corresponding boxes.
- **Enable Syslog Server:** Enabling this option would allow you 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 4.12.1).
- **IP Address:** When the Syslog Server is enabled in the previous option, specify the remote Syslog server's IP address in this field.
- **Syslog Server Service Port:** This option allows you to specify the remote Syslog Server Port number between 1 and 65535. Note that the default port number is 514.

After finishing configuring the **COM Log Settings**, click on the **Save & Apply** button to keep the change(s) that you have made and to apply your setting(s). The web browser will remain on the **COM Log Settings** page. If you want to cancel the change(s) and reset all changes back to their original values, click on the **Cancel** button.

4.12.4 COM log

This page displays the current COM log stored in the device. The desired **COM** port number can be selected from the **COM x Log** drop-down list in Figure 4.38, which allows it to display logs from different COM ports. An example of **COM 1 Log** is also shown in Figure 4.38. Each record in the log consists of **Time**, **COM #**, Direction (**T/R**), and **Data**.

Log Settings > COM Log

COM Log

COM 1 Log

Refresh Export Log Clear Log

Show 10 entries Search:

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

Showing 0 to 0 of 0 entries Previous Next

Figure 4.38 COM Datalog Web Page under Log Settings

Under the COM x Log header, there are three buttons: **Refresh**, **Export Log**, and **Clear Log**. The **Refresh** button can be used to update the COM Log table with the latest information. The **Export Log** button will enable you to save the log data onto your PC. The default file name of the exported data log will be "**DataLog.txt**". The **Clear 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 Log** page, there are two hyperlinks which can be used to navigate through all records. Click on the "**Previous**" link to go to the previous log page, and click on the "**Next**" link to go to the next page.

4.13 System Setup

Under the **System Setup** menu for the web interface of the LES920 series Industrial Serial Device Server, you can perform a number of administration tasks for the device. Figure 4.39 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 options will be described in the following subsections.



Figure 4.39 System Setup Menu

4.13.1 Date/Time Settings

Date and time can be set manually or using Network Time Protocol (NTP) to automatically synchronize the date and time of the LES920 series with a Time Server. Figure 4.40 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 of the LES920 series 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, check the box behind the **Sync with NTP Server** option. Then 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 (refer to Section 4.7). The fourth part is **Daylight Saving Time Settings** that can be enabled when **Enable Daylight Saving Time** box is checked. When it is enabled, you 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 4.40.

System Setup > Date/Time Settings

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

Current Date/Time
1 / Jan / 1970 09:55:44

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

NTP Settings
Local NTP Service ☐
Sync with NTP Server ☒
NTP Server time.nist.gov

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 4.40 Date/Time Settings Web Page under System Setup

**Attention**

It is also important to set up Default Gateway and DNS Servers in the Network Settings properly (See Section 4.7), so the LES920 series can look up DNS names and point to the proper NTP server.

After configuring the **Date/Time Settings**, click on the **Save & Apply** button to keep the change(s) that you have made and to apply your setting(s). The web browser will remain on the **Date/Time Settings** page. If you want to cancel the change(s) and reset all changes back to their original values, click on the **Cancel** button.

4.13.2 Admin Settings

The LES920 series allows user and password management through this **Admin Settings** page under the **System Setup** menu. By default, the user name is “**admin**” and the password is “**default**”. To set or change their values, 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 4.41. At the end of the **Admin Settings** web page, there is the **Web mode** part which allow you to select the radio button of normal **HTTP** or **HTTPS** for secure communication with the device’s web user interface (Web UI).

System Setup > Admin Settings

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 4.41 Admin Settings Web Page under System Setup

After finishing configuring the **Admin Settings**, click on the **Save & Apply** button to keep the change(s) that you have made and to apply your setting(s). Another pop-up window will be displayed to re-authenticate the user to access the Web UI of the LES920 series. You must re-enter the username and the password to log into the LES920 series. 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(s) and reset all changes back to their original values, click on the **Cancel** button.

4.13.3 Firmware Upgrade

Updated firmware for the LES920 series is provided by Black Box to fix bugs and optimize performance. It is very important that **the device must NOT be turned off or powered off during the**

firmware upgrade. Before upgrading the firmware, verify that the device has a reliable power source that will not be powered off or restarted during the firmware upgrade process.

To upgrade the firmware, download the latest firmware for your LES920 series model from the support tab on the product page on blackbox.com. 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 on the “**Browse...**” button as shown in Figure 4.42 below to find and choose the new firmware file. Then, tick the checkbox of “**Clear the flash after firmware upgrade**” if it is required to erase the user storage after a successful firmware upgrade, and click on the “**Upload**” button to start the firmware upgrade process. The program will show the upload status. Wait until the uploading process is finished (the amount of time varies depending on the equipment used). Finally, the LES920 series device will then restart itself. In some cases, you might need to reconfigure your LES920 series device. To restore your backup configuration from a file, refer to the procedure in the next subsection.

System Setup > Firmware Upgrade

Firmware Upgrade

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

Clean the flash after firmware upgrade ☐

Select new firmware **Browse...**

Upload

Figure 4.42 Firmware Upgrade Web Page under System Setup

Note 1: if the checkbox for “**Clear the flash after firmware upgrade**” is enabled, user storage will be erased after the firmware upgrades successfully. The system will be restored to default settings, and the certifications will be regenerated after reboot.

4.13.4 Backup/Restore Settings

Once all the configurations are set and the device is working properly, back up the LES920 series' current configuration. 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 LES920 series devices of similar settings by uploading these settings to all devices.

To back up the configuration, click on the “**Backup**” button under the **Backup Configuration** part as shown in Figure 4.43, and the backup file (ModelName-MACAddress.dat) will be automatically saved on your computer. **It is important NOT to manually modify the saved configuration file with any editor. Any modification to the file may corrupt the file, and it may not be used for later restoration.** Contact Black Box technical support for more information.

To restore the backup configuration, click on the “**Browse**” button under the **Restore Configuration** part as shown in Figure 4.43 to locate the backup configuration file on your computer. Then, click on the “**Upload**” button to upload the backup configuration file to the device. Once the backup configuration file is successfully uploaded, the device will restart. Note that the time needed for this process may vary depending upon the equipment used.

If you need to restore the LES920 series device to its factory default configuration, click on the **Restore** button under the **Restore Factory Default** section, as shown in Figure 4.43.

System Setup > Backup/Restore Configuration

Backup/Restore Configuration

Backup Configuration

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

Backup

Restore Configuration

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

Browse... Upload

Restore Factory Default

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

Restore

Figure 4.43 Backup/Restore Settings Web Page under System Setup

4.13.5 Ping

The LES920 series' Web UI has an interface to call Ping, which is a network diagnostic utility for testing reachability. You can use the Ping function to determine whether the LES920 series can reach the gateway or other devices in the network. To use Ping, enter a destination IP address in the text box behind the Ping To and click on the Start button as shown in Figure 4.44. This process usually takes around 20 seconds. Figure 4.44 represents a successful ping without packet loss from the LES920 series to the address 10.0.50.101 and back, while Figure 4.45 indicates that the connecting device at the address 10.0.50.202 is unreachable and no packets have returned from the transmitted ping packets.

System Setup > Ping

Ping

Only numerical IP address is accepted

Ping To

10.0.50.100

start

```
PING 10.0.50.100 (10.0.50.100): 56 data bytes
64 bytes from 10.0.50.100: seq=0 ttl=64 time=0.513 ms
64 bytes from 10.0.50.100: seq=1 ttl=64 time=0.439 ms
64 bytes from 10.0.50.100: seq=2 ttl=64 time=0.379 ms
64 bytes from 10.0.50.100: seq=3 ttl=64 time=0.292 ms

--- 10.0.50.100 ping statistics ---
4 packets transmitted, 4 packets received, 0%% packet loss
round-trip min/avg/max = 0.292/0.405/0.513 ms
```

Figure 4.44 Ping Web Page under System Setup

System Setup > Ping

Ping

Only numerical IP address is accepted

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 4.45 Unreachable Ping Example

4.14 Reboot

4.14.1 Auto Reboot

To schedule the device reboot at a specific time or period time, enable the “**Auto reboot**” option and select either **Specific time** or **Period time** for the auto reboot policy. Then click on the “**Save**” button at the bottom of the Auto Reboot section as shown in Figure 4-95.

The screenshot displays the 'Reboot' configuration page. At the top is a blue header bar with a white arrow and the text '> Reboot'. Below this is a section titled 'Auto Reboot' with a light blue background. Inside this section is a table with the title 'Auto Reboot Settings'. The table has three rows: 'Auto Reboot' with a checkbox labeled 'Enable' (which is unchecked), 'Policy' with two radio buttons, 'Specific Time' (selected) and 'Period Time' (unselected), and 'Specific Time' with two dropdown menus showing '00' and '00' followed by '(HH : MM)'. Below the table are 'Save' and 'Cancel' buttons. Below the 'Auto Reboot' section is a 'Reboot' section with a light blue background. It contains two lines of text: 'Click **Reboot** button to process system restart.' and 'Please re-configure your local network setting accordingly if this device network setting was changed.' At the bottom of this section is a 'Reboot' button.

Auto Reboot Settings	
Auto Reboot	<input type="checkbox"/> Enable
Policy	<input checked="" type="radio"/> Specific Time <input type="radio"/> Period Time
Specific Time	00 : 00 (HH : MM)

Save Cancel

Reboot

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

Reboot

Figure 4.95 Reboot Web Page

4.14.2 Manual Reboot

To manually reboot the LES920 series device, click on the “**Reboot**” button at the end of the **Reboot** page as shown Figure 4-95. The device will then restart. When the rebooting process is finished, the device will beep twice, and you might need to refresh your web browser to log into the web interface of the LES920 series again.

5 Link Modes and Applications

5.1 Link Mode Configuration

The LES920 series supports three different **Link Modes: TCP Server, TCP Client, and UDP**. The **Link Mode** describes the role of the LES920 series and the connection between the LES920 series device and other remote devices in the network which would like to communicate with serial devices on the LES920 series' 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. A discussion on how to set up different Link Modes properly will be presented in the following sections. Figure 5-1 shows the **Link Mode** options for the **COM 1** port, which can be found on the **COM1** page under the **Serial** menu of Web UI (Refer to Serial Settings in Section 4.8). Note that an LES920 series model with an IO interface will have two COM ports.

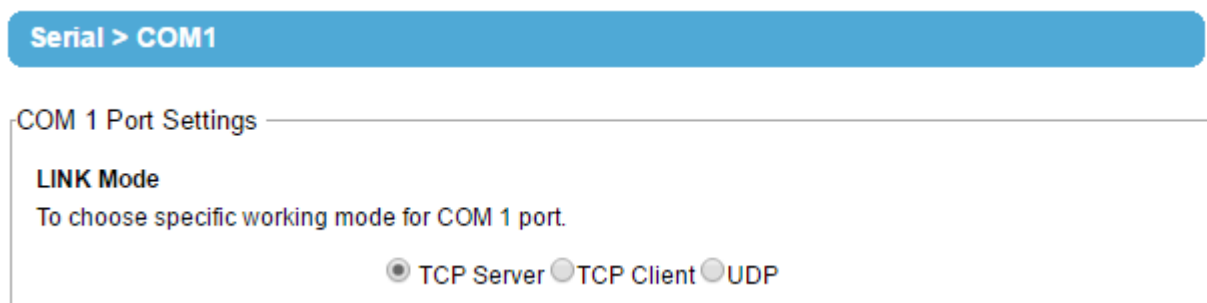


Figure 5.1 Link Mode Options for COM1 Port

5.1.1 Link Mode: Configure LES920 series as a TCP Server

The LES920 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 the LES920 series on a serial bus where a remote host computer is sending a request via an Ethernet network. After the connection is established between the serial device server (LES920 series) 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. Note that this is the LES920 series device's default link mode.

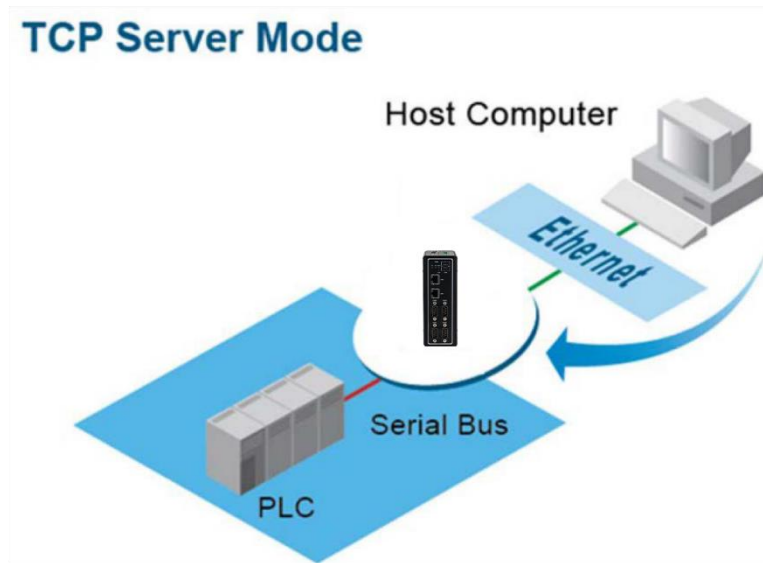


Figure 5.2 LES920 set as a TCP Server Link Mode

The default Link Mode of the LES920 series is the **TCP Server** mode. Figure 5.3 shows an example of the 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 the LES920 series. Instructions follow for configuring the 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. To configure **COM 2** (or any other COM port), follow the same procedure.

Serial > COM1

COM 1 Port Settings

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

☒ TCP Server
 ☐ TCP Client
 ☐ UDP

TCP Server

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

To configure COM 1 port parameters.

Serial Settings

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

Figure 5.4 TCP Server Link Mode Settings under COM 1 Page

- Select the **TCP Server** radio button in the Link Mode options. Note that **TCP Server** is the default Link Mode for the COM port for the LES920 series.
- Under the **TCP Server** section, you will find the following options:
 - **Application:** There are three different communication applications to choose from:
 - **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 LES920 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 needs to pair two serial devices over the Ethernet network.
- **IP Filter:** This option will enable the **Source IP** option below. When this option is checked, the LES920 series 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 the LES920 series). Therefore, 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 the LES920 series) 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 the LES920 series will proceed or behave when it receives requests from remote connected hosts in which we will have the following options:
 - **Request & Response Mode:** Under this mode, the COM port on the LES920 series will hold requests from all other remote connected hosts until the serial device replies; however, unrequested data sent from the serial device would be forwarded to all connected hosts. Additionally, you can specify how a reply message from the serial device will be sent to the remote connected hosts with two possible options:
 - **Reply to requester only:** The COM port will reply to the remote connected host who has requested the data only.
 - **Reply to all:** A reply is sent to all remote connected hosts.
 - **Transparent mode:** The COM port on the LES920 series 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, refer to Section 4.8.2, and, for **Advanced Settings**, refer to Section 4.8.3.
- After finishing configuring the **Link Mode**, scroll down to the bottom of the page and click on the “**Save & Apply**” button to save all the changes that you have made.

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

5.1.2 Link Mode: Configure LES920 series as a TCP Client

The LES920 series can be configured as a TCP client in a 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 LES920 series devices where both LES920 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 LES920 series) and a remote host computer in both directions. This also applies to a Virtual COM application running in the client mode.

TCP Client Mode

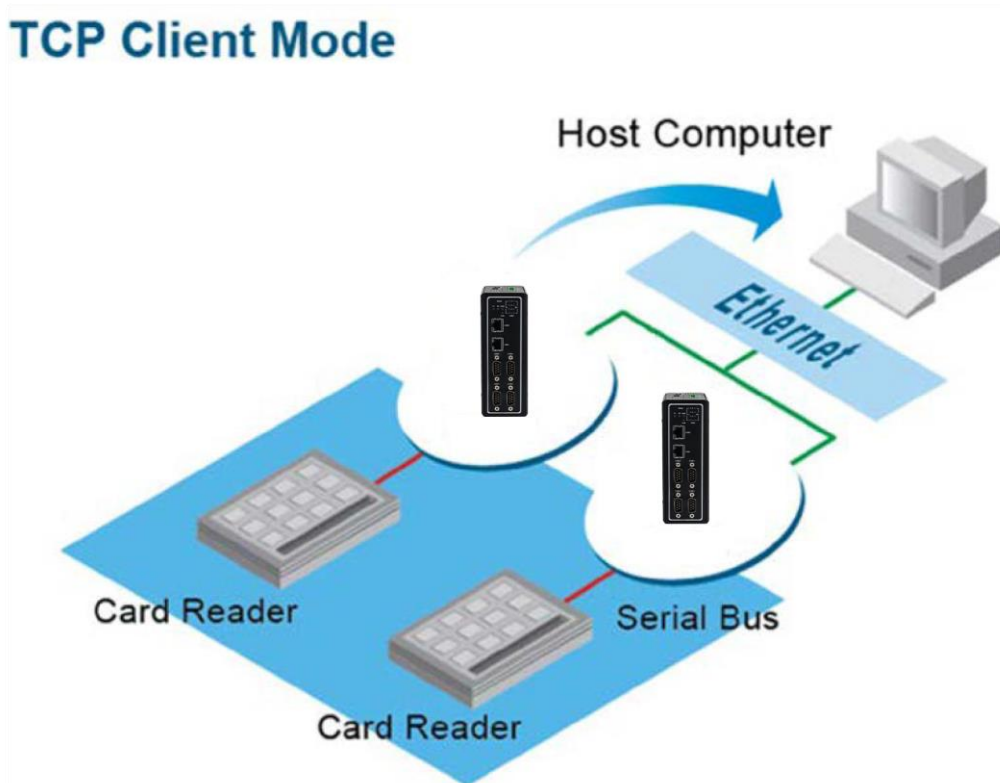


Figure 5.5 Example of LES920 Series Configured as TCP Client Link Mode

Figure 5.6 shows an example of a 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 the LES920 series. Instructions follow for configuring 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	<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 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. To configure COM 2 (or any other COM port), follow the same procedure.

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 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"/> 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 5.7 Setting in TCP Client Link Mode

- Select the **TCP Client** radio button in the **Link Mode** options.
- Under the TCP Client section, you will find the following options:
 - **Application:** Only three communication applications are available here: **RAW**, **Virtual COM**, and **Pair Connection Slave** in which their definitions are the same as described previously in Section 5.1.1.
 - **Destination IP 1:** 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:** Specify the preferred port number of the TCP server program on the remote host in this field. This should match the IP setting of the TCP server program.

- **Backup Destination IP 1:** Specify the preferred **Backup Destination IP** address of the TCP server program on the remote host in this field. Once the Destination IP 1 is unreachable, the LES920 series will send the data to Backup Destination IP 1.
 - **Backup Destination Port 1:** Specify the preferred port number of the TCP server program on the remote host in this field. This should match the IP setting of the TCP server program.
 - **Destination 2:** You can enable a second remote destination for TCP connection if it is necessary by checking on the **Enable** box in this option. Two different TCP servers can be set for redundancy.
 - **Destination IP 2:** 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:** Specify the preferred port number of the second TCP server program on the remote host in this field. This should match the IP setting of the second TCP server program.
 - **Backup Destination IP 2:** Specify the preferred **Backup Destination IP** address of the TCP server program on the remote host in this field. Once the Destination IP 2 is unreachable, the LES920 series will send the data to Backup Destination IP 2.
 - **Backup Destination Port 2:** Specify the preferred port number of the TCP server program on the remote host in this field. This should match the IP setting of the TCP server program.
 - **Response Behavior:** This option specifies how the device will proceed or behave when it receives a request from remote connected hosts. The description of each option is the same as described in the previous subsection (Section 5.1.1 Link Mode: Configure as a TCP Server).
- For other **Serial Settings** on the same configuration page, refer to Section 4.8.2, and, for **Advanced Settings**, refer to Section 4.8.3 COM Configuration: Advanced Settings.
 - After finish configuring the **Link Mode**, scroll down to the bottom of the page and click on the **"Save & Apply"** button to save all the change(s) that you have made.

5.1.3 Link Mode: Configure LES920 series in UDP

Since User Datagram Protocol (UDP) is a faster transport protocol than TCP but it is a connectionless transport protocol, it does not guarantee the delivery of network datagram. The LES920 series also supports connectionless UDP protocol compared to the connection-oriented TCP protocol. The LES920 series can be configured to transfer data using unicast or multicast UDP from the serial device to one or multiple host computers. The data can be transmitted between a serial device and a remote host computer in both directions.

There is no server or client concept on this protocol. All networked devices are called peers or nodes. Therefore, you only need to specify the Local Port that the LES920 series 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 the LES920 series. Two remote host computers, which are on the same Ethernet network as the LES920 series, can both send UDP datagram or messages to the serial display device through the LES920 series.

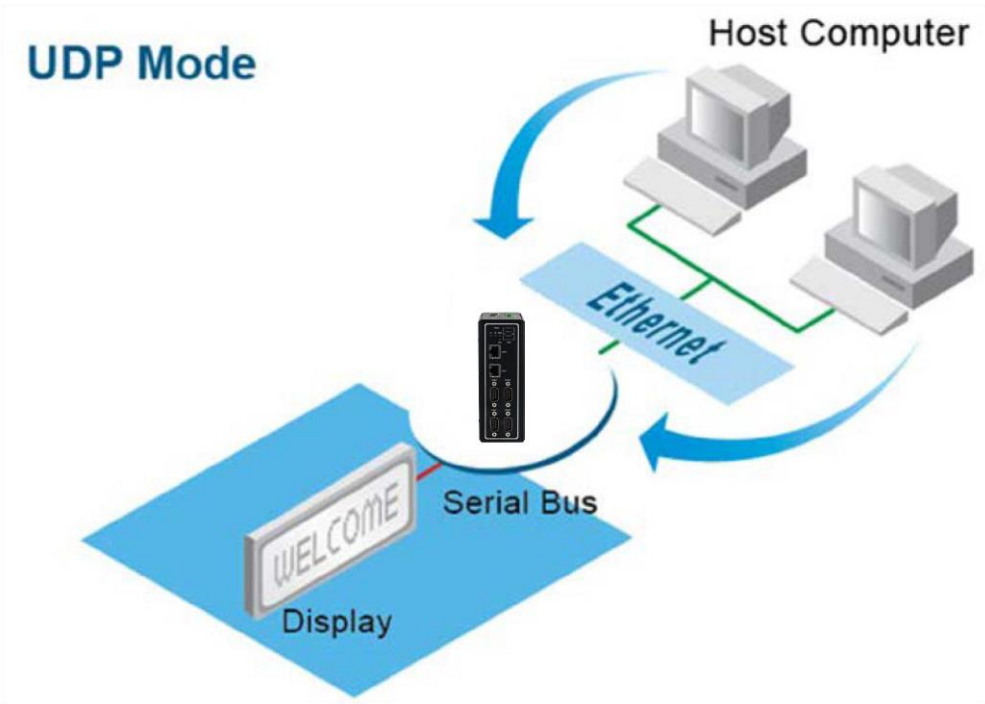


Figure 5.8 Example of the LES920 Series Configured in UDP Link Mode

Figure 5.9 shows an example of a 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. Be aware that even though UDP provides better efficiency in terms of response time and resource usage, it does not guarantee data delivery. We recommend that you utilize UDP only with cyclic polling protocols where each request is repeated and independent, such as Modbus Protocol. Instructions follow for configuring 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 Port: 4660
<input type="checkbox"/> Destination IP Address 3	0	.	0	.	0 ~ 0 Port: 4660
<input type="checkbox"/> Destination IP Address 4	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 5.10. To configure COM 2 (or any other COM port), follow the same procedure.

Serial > COM1

COM 1 Port Settings

Link Mode

To choose specific working mode for COM 1 port.

☐ TCP Server
 ☐ TCP Client
 ☒ UDP

UDP

Local Port: 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

Figure 5.10 UDP Link Mode Setting under COM 1 Page

- Select the UDP radio button in the Link Mode options.
- Under the UDP section, you will find the following options:
 - **Local Port:** This field specifies the local port number for UDP Link Mode on the LES920 series which it will be listening to, and it can be any number between 1 and 65535. Typically a port number larger than 1024 is recommended to avoid conflicting with the well-known port numbers. You should match this setting with the remote UDP program. 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 the LES920 series. The user can define the Begin and End IP Addresses here. Four groups of ranges of IP addresses are allowed. Check the box in front of the corresponding line to enable it. These are the IP Addresses of the remote UDP

programs and the Port that they are listening to. The maximum number of UDP nodes that the LES920 series can handle would highly depend on the traffic load. We have tested that the LES920 series 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, refer to Section 4.8.2, and, for Advanced Settings, refer to Section 4.8.3.
- After finishing configuring the Link Mode, scroll down to the bottom of the page and click on the “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. You will have flexibility in choosing the suitable application that matches your need for serial data communication.

5.2.1 TCP Server Application: Enable Virtual COM

The LES920 series will encapsulate control packets on top of the real data when Virtual COM is enabled. This will allow the Virtual COM port on the Windows® /Linux operating system to access the LES920 series' COM ports. The benefit of using Virtual COM is that rewriting an existing COM program to read IP packets is unnecessary. Therefore, 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 the LES920 series in TCP Server mode with the Virtual COM application enabled. Instructions follow to enable Virtual COM application in TCP Server Link Mode.

Serial > COM1

COM 1 Port Settings

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

☒ TCP Server
 ☐ TCP Client
 ☐ UDP

<i>TCP Server</i>	
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

Figure 5.11 Virtual COM Application in TCP Server Link Mode

- Follow steps in Section 5.1.1 to configure the LES920 series 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 enable Virtual COM application in the LES920 series.
- Scroll down to the bottom of the page and click on the “**Save & Apply**” button to save the changes.
- Configure Virtual COM in the Operating System on the remote host computer. For Windows®,

refer to Chapter 6 for necessary instructions. Record the LES920 series' 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 utility software.

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 the LES920 series 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. LES920 series) to communicate with serial device on the access server's COM port. To do so, refer to Section 5.2.1 (previous section) to enable Virtual COM so that that LES920 series 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. Figure 5.12 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 the LES920 series uses dynamic IP (via DHCP), because setting a static IP address in Virtual COM's Control Panel in the Operating System is not possible. Instructions follow to enable Virtual COM application in TCP Client Link Mode.

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	Virtual COM
Destination IP 1	10.0.50.1
Destination Port 1	4660
Backup Destination IP 1	0.0.0.0
Backup Destination Port 1	0
Destination 2	<input type="checkbox"/> Enable
Destination IP 2	0.0.0.0
Destination Port 2	0
Backup Destination IP 2	0.0.0.0
Backup Destination Port 2	0
Response Behavior	<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 5.12 Virtual COM Application in TCP Client Link Mode

- Follow steps in Section 5.1.2 to configure the LES920 series 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 the LES920 series.
- Scroll down to the bottom of the page and click on the “**Save & Apply**” button to save the changes.
- Configure Virtual COM in the Operating System on the remote host computer. For Windows®, refer to Chapter 6 for necessary instruction. 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 the LES920 series in the TCP Client mode. The RFC 2217 allows a client, which is the LES920 series 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, refer to Section 5.2.3 (previous section) to enable Virtual COM so that the

LES920 series becomes aware of the command names and codes defined in RFC 2217. 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 LES920 Series 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 LES920 series devices to work as a pair. One would be the Pair Connection Master, and the other would be the Pair Connection Slave. Figure 5.13 shows a configuration of the Pair Connection Master application in TCP Server Link Mode. Instructions follow to enable the Pair Connection application and set the LES920 series as Master in TCP Server Link Mode.

Serial > COM1

COM 1 Port Settings

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

☒ TCP Server
 ☐ TCP Client
 ☐ UDP

<i>TCP Server</i>	
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 the LES920 series 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 enable Pair Connection application in the LES920 series.
- Scroll down to the bottom of the page and click on the “**Save & Apply**” button to save the changes.
- Note the Pair Connection Master’s IP address (i.e. The LES920 series’ IP address on your desired network interface (either Ethernet or Wi-Fi)) and Local Port number in order to enter this information in another LES920 series 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 LES920 Series as a Pair Connection Slave

A Pair Connection Slave application is configured for the LES920 series 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 the previous section. Set up a Pair Connection Master on another LES920 series device before proceeding. Instructions follow to enable the Pair Connection application and set this LES920 series device as Slave in TCP Client Link Mode.

Serial > COM1

COM 1 Port Settings

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

☐ TCP Server
 ☒ TCP Client
 ☐ UDP

<i>TCP Client</i>	
Application	Pair Connection Slave ▼
Destination IP 1	10.0.50.1
Destination Port 1	4660
Backup Destination IP 1	10.0.50.2
Backup Destination Port 1	4663
Destination 2	<input checked="" type="checkbox"/> Enable
Destination IP 2	10.0.50.3
Destination Port 2	4664
Backup Destination IP 2	10.0.50.4
Backup Destination Port 2	4665
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 the LES920 series 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 enable the Pair Connection application in the LES920 series device.

- 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 LES920 series device's IP and port number that were set up previously).
- Scroll down to the bottom of the page and click on the “**Save & Apply**” button to save the changes.

5.2.7 TCP Server Application: Enable Reverse Telnet

The Reverse Telnet application is useful if a Telnet program is used to connect to the LES920 series device and the serial interface of the LES920 series device 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 display properly. The LES920 series device 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. The Reverse Telnet application is only available when the LES920 series device is configured as TCP Server Link Mode. Instructions follow to enable Reverse Telnet application under the TCP Server Link Mode.

Serial > COM1

COM 1 Port Settings

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

☒ TCP Server
 ☐ TCP Client
 ☐ UDP

<i>TCP Server</i>	
Application	Reverse Telnet ▼
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 5.15 Reverse Telnet Application in TCP Server Link Mode

- Follow steps in Section 5.1.1 to configure the LES920 series device 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 enable reverse telnet application in the LES920 series device.
- Scroll down to the bottom of the page and click on the **“Save & Apply”** button to save the changes.

6 VCOM Installation & Troubleshooting

6.1 Enabling VCOM

The LES920 device will encapsulate control packets on top of the actual serial data when the Virtual COM (VCOM) Application is enabled. This will allow the Virtual COM port in the Windows®/Linux system to access the LES920 device's COM ports. 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.

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

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

Serial > COM1

COM 1 Port Settings

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

☐ TCP Server
 ☒ TCP Client
 ☐ UDP

<i>TCP Client</i>	
Application	Virtual COM ▼
Destination IP 1	10.0.50.1
Destination Port 1	4660
Backup Destination IP 1	10.0.50.2
Backup Destination Port 1	4663
Destination 2	<input type="checkbox"/> Enable
Destination IP 2	10.0.50.3
Destination Port 2	4664
Backup Destination IP 2	10.0.50.4
Backup Destination Port 2	4665
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 6.2 Enable a Virtual COM Application When Setting the Link Mode as the TCP Client

Virtual COM on the 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 the Virtual COM application diagram. In the diagram, multiple serial servers (i.e. LES920 series devices), in which each one connects to serial device, are connected over an Ethernet hub. The serial devices can be accessed through the TCP/IP network of the hub. 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, and 5. In the LES920 series device's case, the TCP/IP network can be a wired network, such as Ethernet.

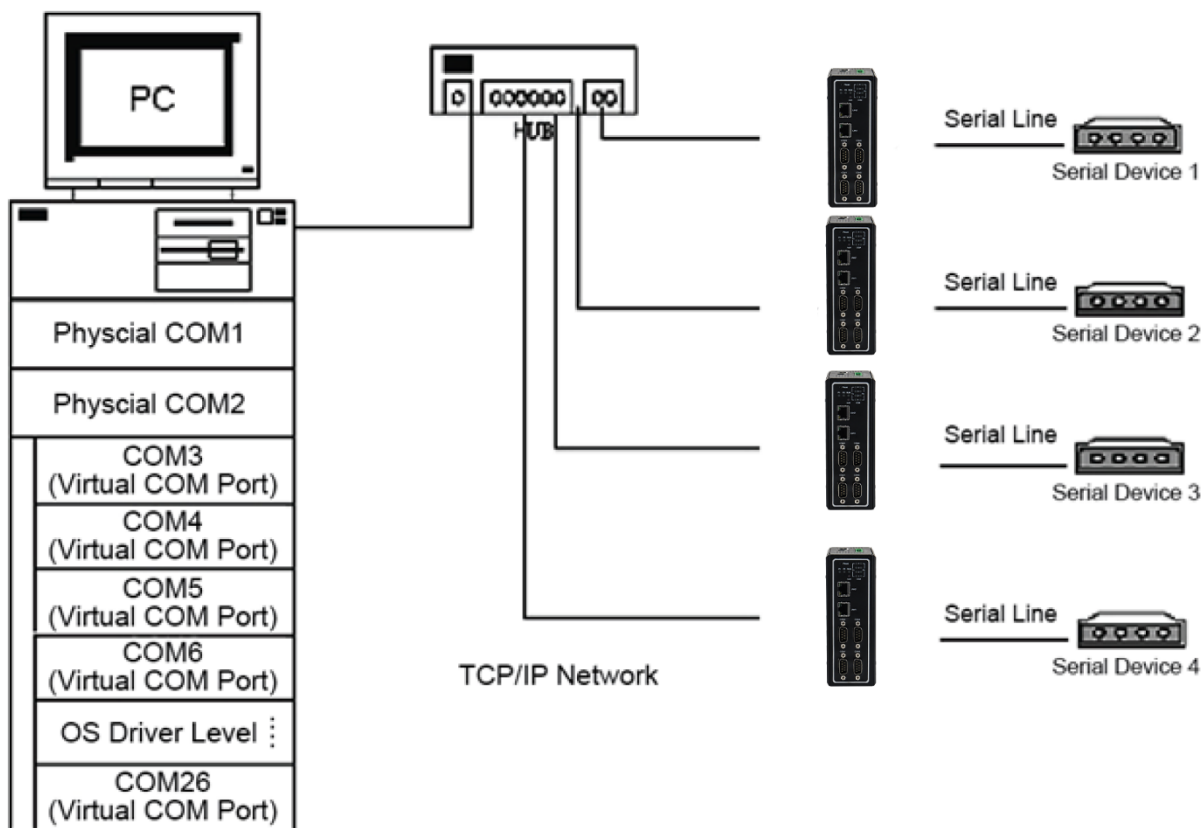


Figure 6.3 An Example Diagram of Virtual COM Application over TCP/IP Network

To enable Virtual COM on a host computer, you will require a software utility or VCOM driver software to emulate the COM port. For the Windows® operating system, a software utility called **Serial/IP** is supported for this purpose. Refer to the 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) from our website. 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. COM port number selection is 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 on the CD or download a copy from our website to install the Virtual COM driver for your operating system. We recommend that you turn off your anti-virus software and try again if the installation fails. At the end of the installation, select at least one Virtual COM port from the Serial/IP Control Panel.

6.1.4 Uninstallation

From the Windows® Start Menu, select Control Panel. Then select Add/Remove Programs. Select Serial/IP Version x.x.x from the list of installed software. Click on 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 the LES920 series and a Windows based PC. Instructions follow 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. the LES920 series device) by logging into the Web UI. It is located under COM 1 or another COM configuration under the Serial menu as described in Section 5.2.1. Figure 6.4 shows how to enable Virtual COM in TCP Server Link Mode in the LES920 series device. For details regarding the Link Mode configuration with Virtual COM, refer to the previous chapter starting from Section 5.1.

Serial > COM1

COM 1 Port Settings

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

☒ TCP Server
 ☐ TCP Client
 ☐ UDP

<i>TCP Server</i>	
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

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

6.2.2 Running Serial/IP Software Utility in Windows®

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

- 1) Click on Windows' Start menu → Select All Programs → Select Serial/IP → Select Control Panel.
- 2) In the Windows' Control Panel, open the Serial/IP applet.
- 3) In the Windows notification area, as shown in
- 4)
- 5) Figure 6.5, right click on the Serial/IP tray icon and click on the Configure... menu to open the Serial/IP's Control Panel.

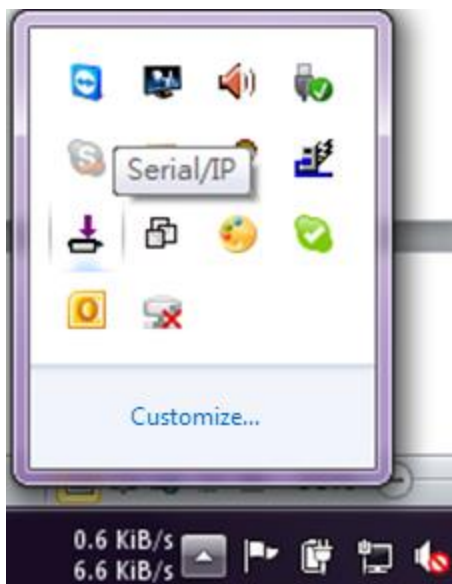


Figure 6.5 Serial/IP Tray Icon on Windows Notification Area

If no Virtual COM port is selected, a “**Select Ports**” dialog window will pop up and ask you 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 an entry in 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. You 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, click on the OK button to proceed.

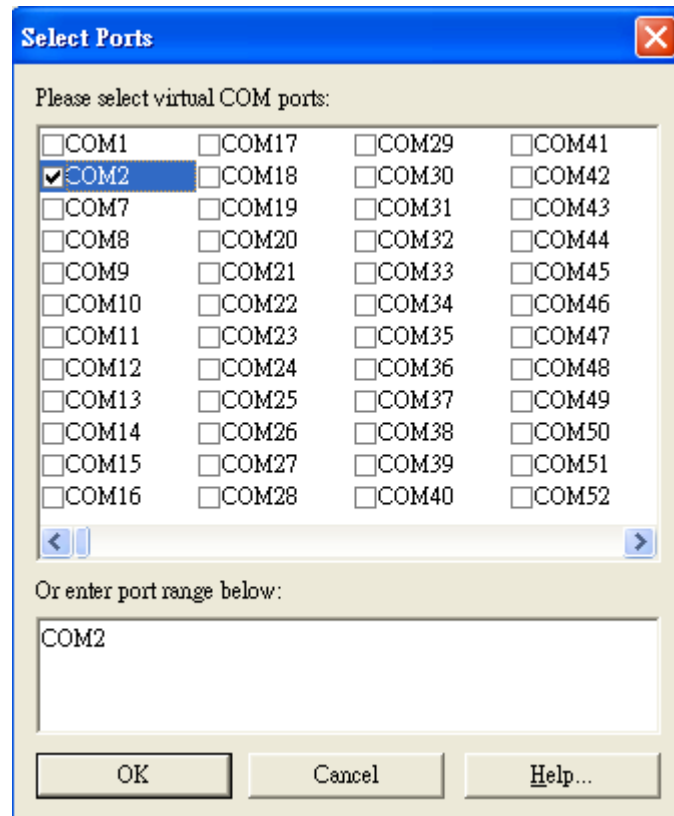


Figure 6.6 A Pop-up Window for Selecting Virtual COM Ports

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

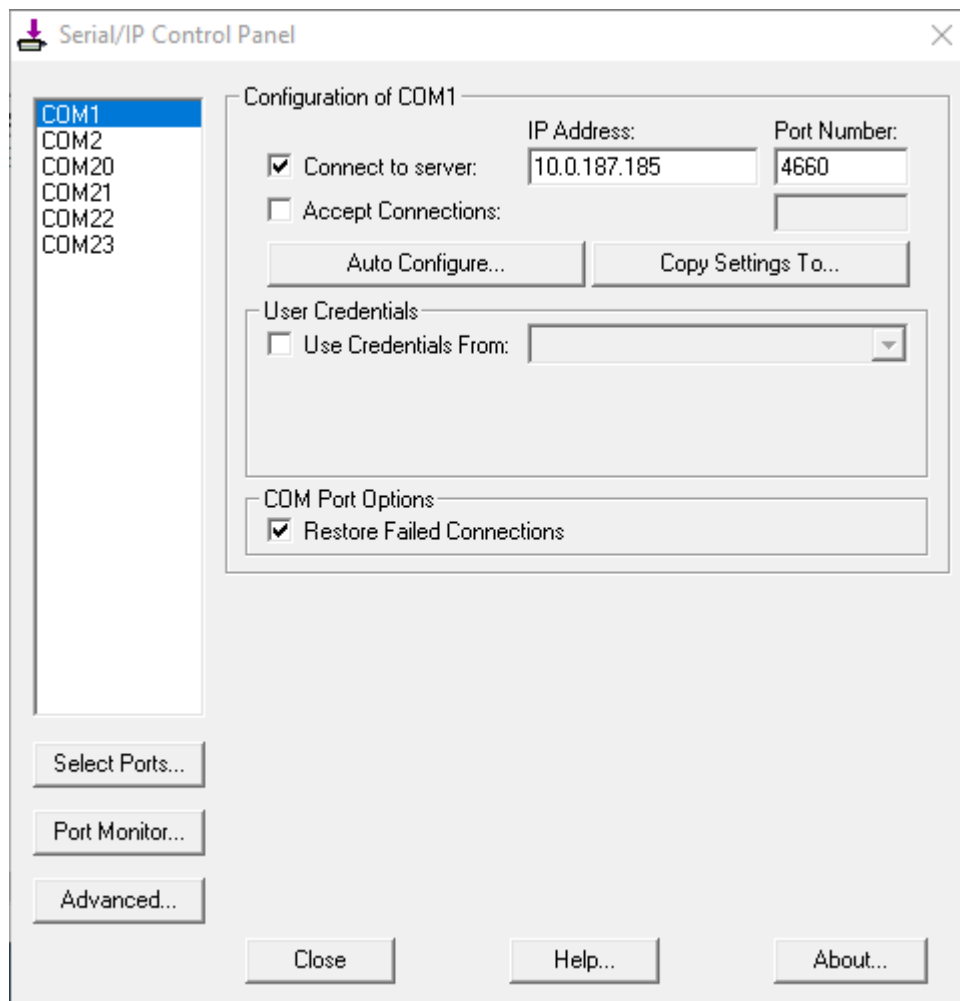


Figure 6.7 Serial/IP Control Panel Window

6.2.3 Configuring VCOM Ports

For each VCOM port selected on the list 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. the LES920 series device) 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 the Connect to Server option (by checking the box in front of it as shown in Figure 6.8) 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. the LES920 series device) 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 the Accept Connections option (by checking the box in front of it) and enter the specified Port Number. This Port Number is the Destination Port of the serial device server. Do not enable the Connect to Server option and Accept Connections option simultaneously.

3. Under **User Credentials** box, you can enable the **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, specify the **Username** and the **Password** in their corresponding text boxes.

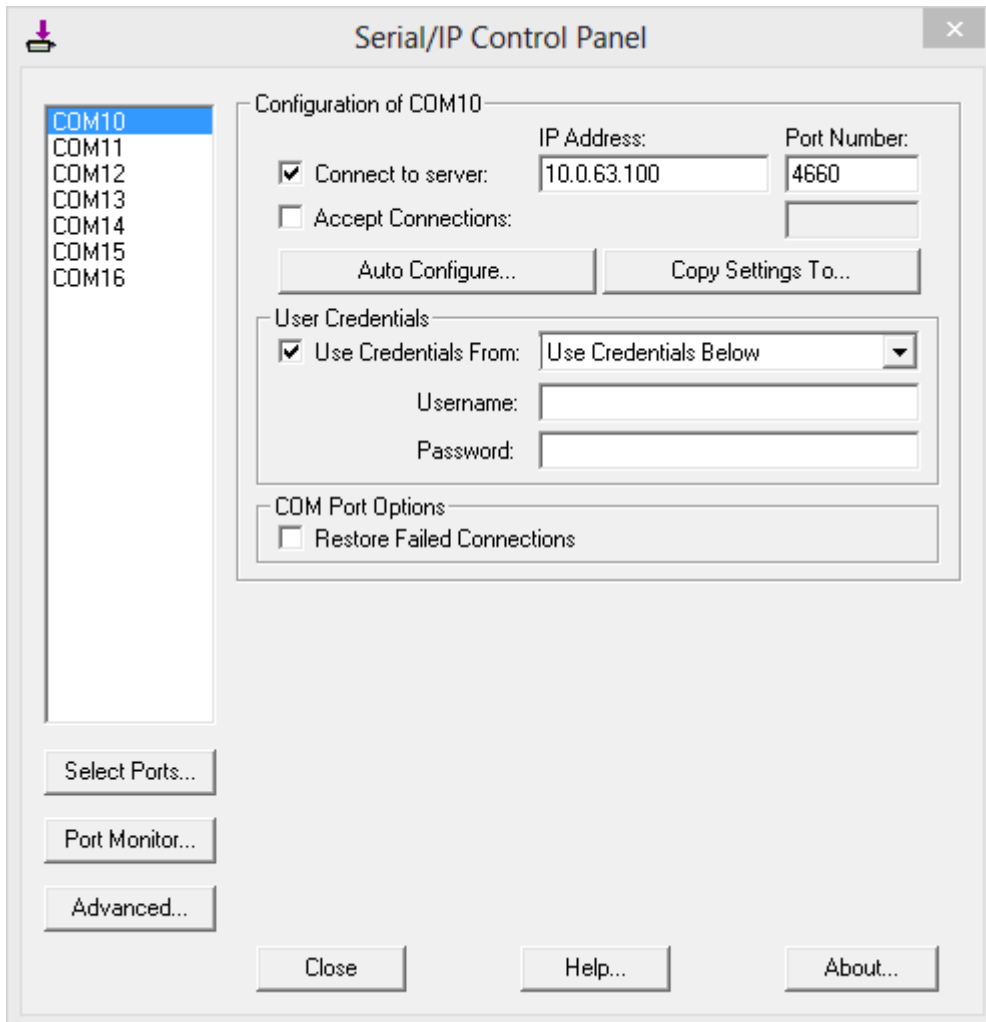


Figure 6.8 Available Options for Use Credential From in Serial/IP Control Panel Version 4.9.10

4. Under the **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 on the **Auto Configure...** button and then click on 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 will 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, click on the **Use Settings**

button at the bottom of the window in Figure 6.10. You can also click on the Copy button to copy the results to the PC's system clipboard.

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

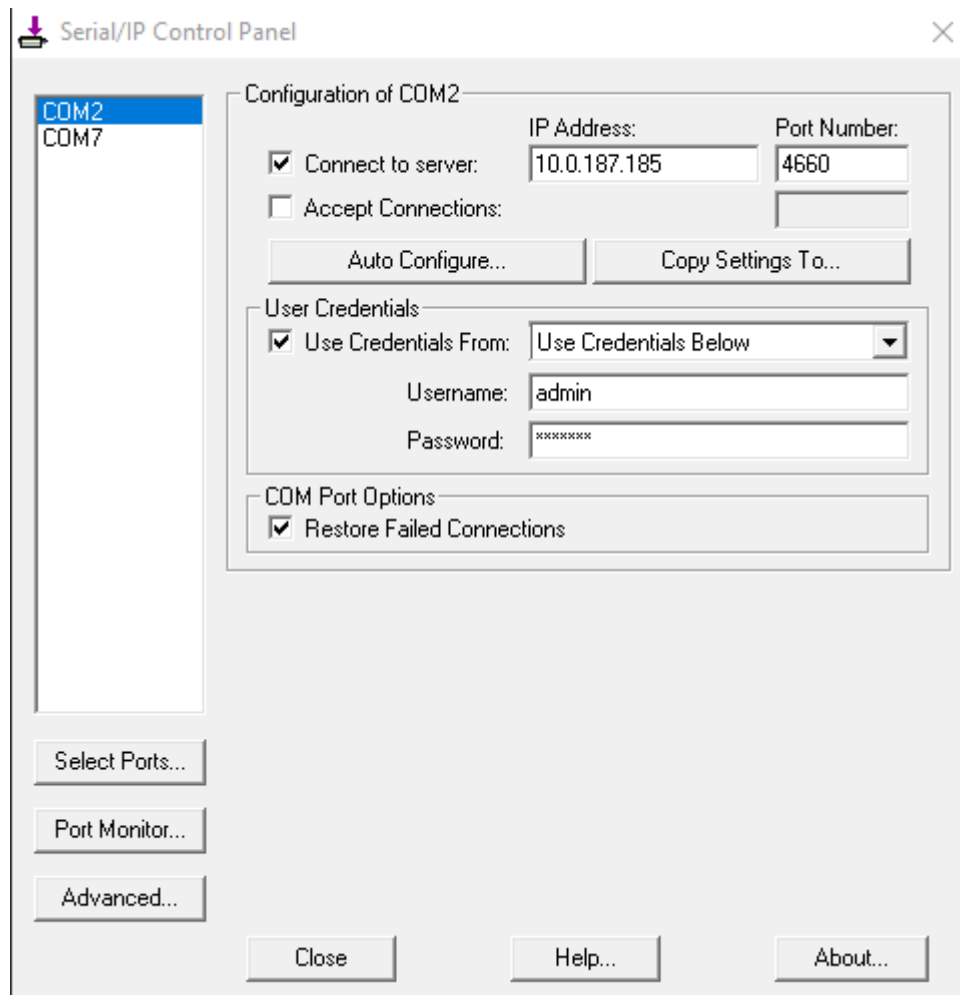


Figure 6.9 Configuring Virtual COM 2 Port as TCP Client

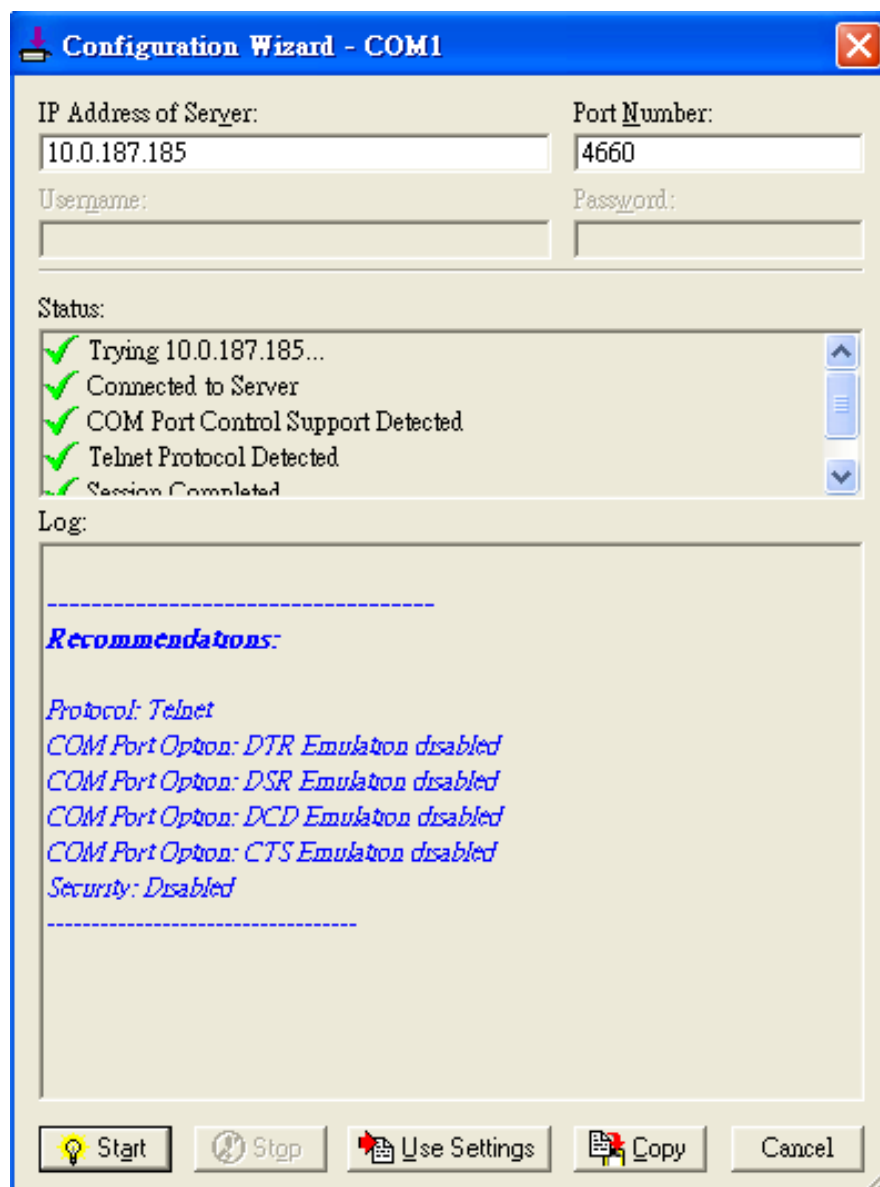


Figure 6.10 Auto Configure (formerly Configuration Wizard) Window for COM 1

6.3 Exceptions

This section lists possible exceptions which may occur when you test 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 troubleshooting 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, verify or correct the VCOM IP address and Port number configuration or the PC’s network configuration.

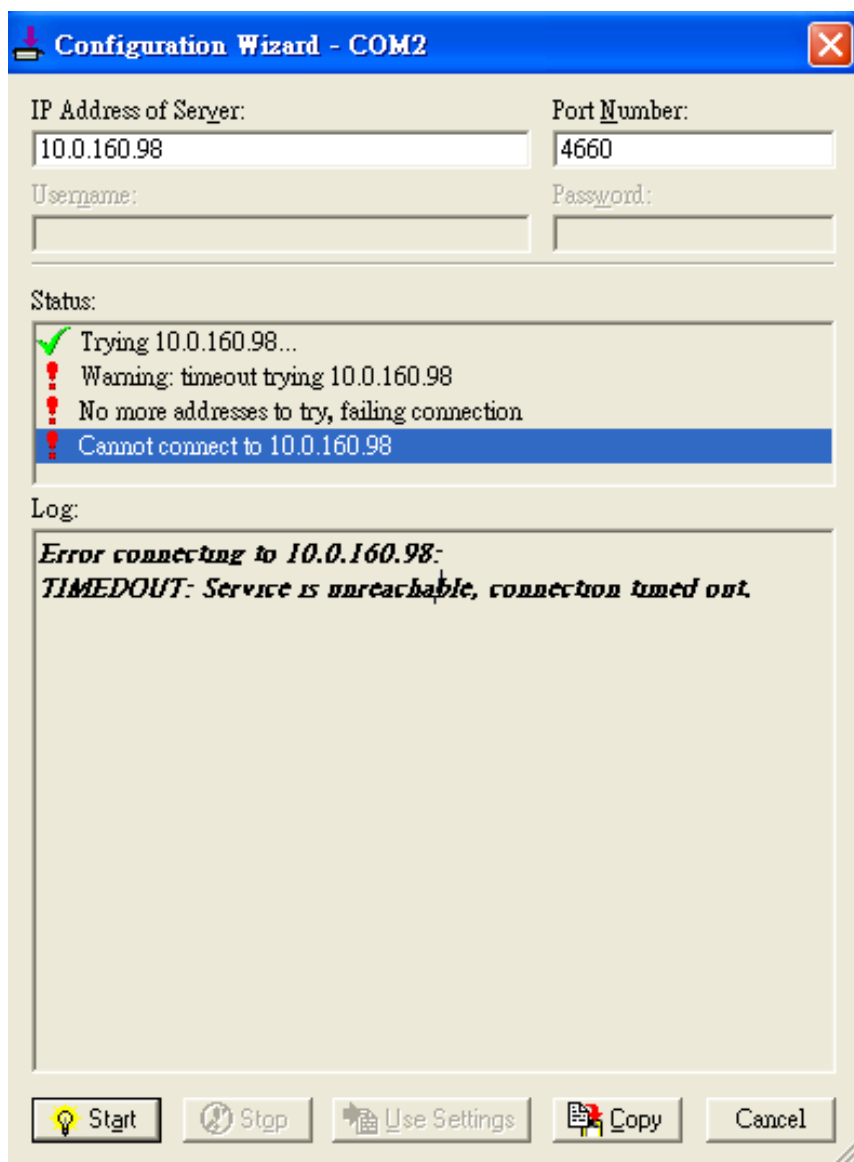


Figure 6.11 Timeout Warning on VCOM Connection

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, enable the Virtual COM option in the serial Device server.

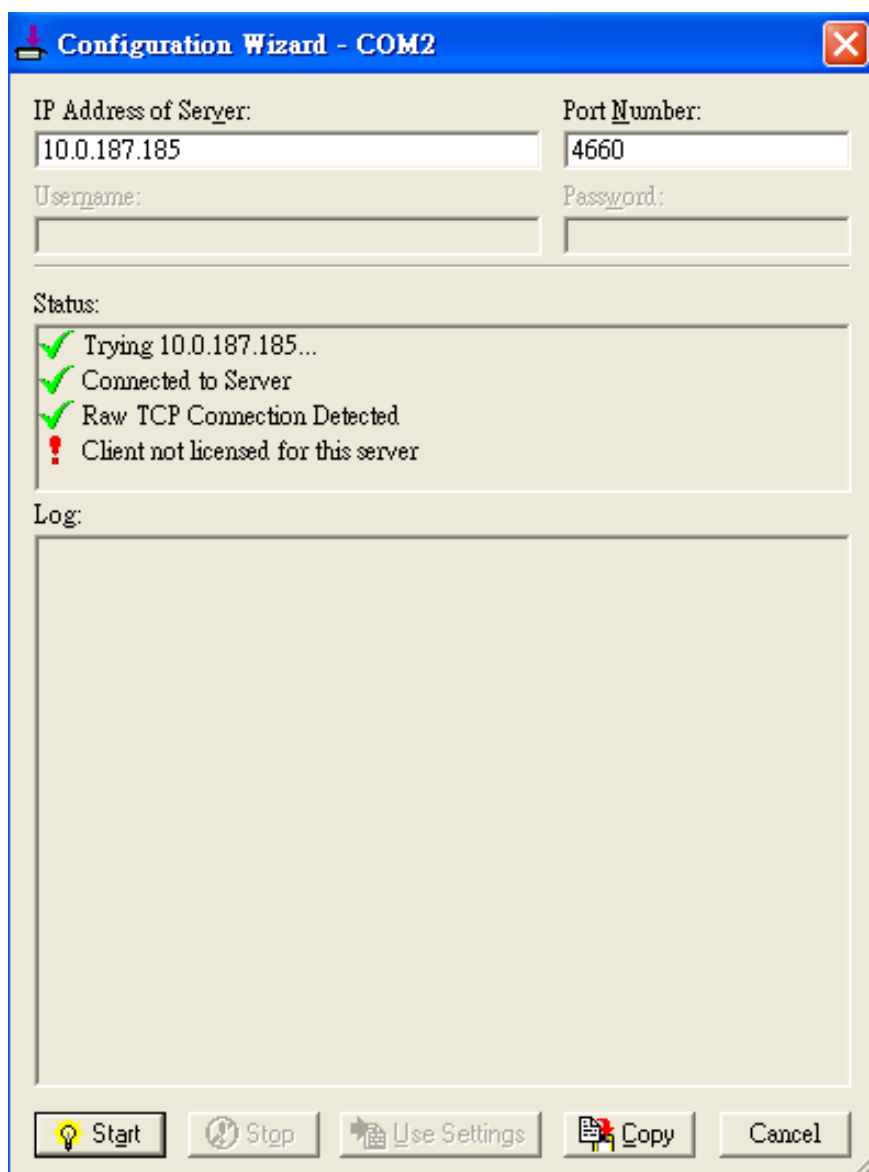


Figure 6.12 Error of Client not licensed for this server

If the status reports with a checkmark 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, there is a licensing issue between the serial gateway (i.e. the LES920 series device) and the Serial/IP Utility Software. Contact Black Box technical support to obtain the correct VCOM software.

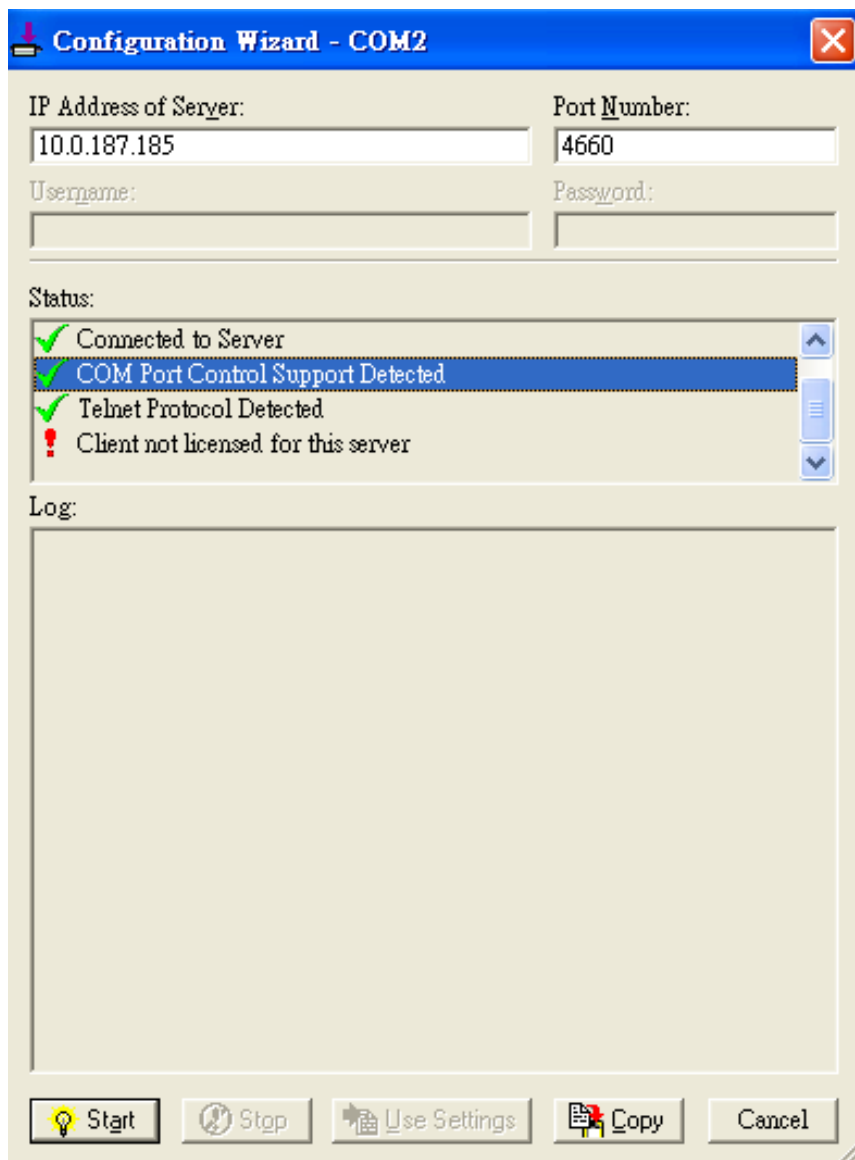


Figure 6.13 Licensing Issue of Serial/IP Utility Software

If the status reports with an exclamation mark with a message “Server requires username/password login,” as shown in Figure 6.14, the VCOM Authentication option in the serial device server (i.e. the LES920 series device) is enabled but the User Credentials option in the Serial/IP utility software is not enabled. Follow the steps in Section 4.13.2 for enabling the user credentials option and entering the username and the password.

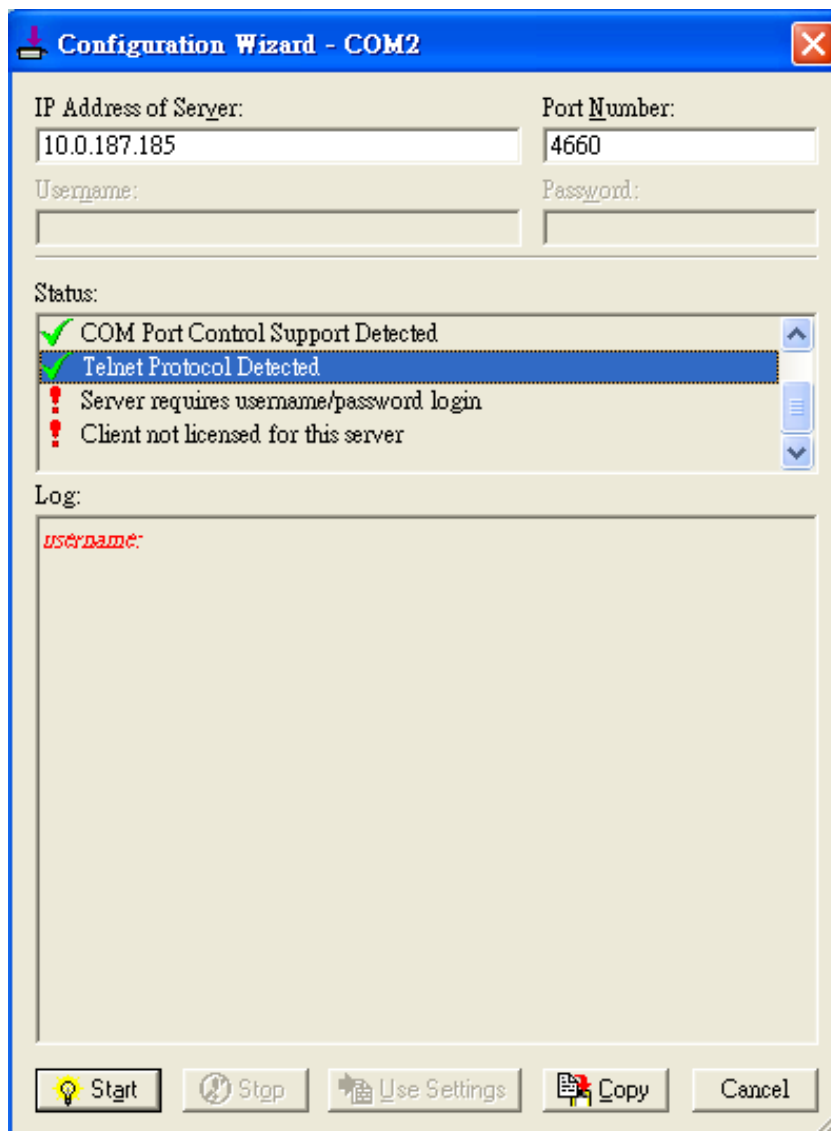


Figure 6.14 VCOM Authentication failed due to Missing Username/Password

If the status reports with an exclamation mark with a message “Username and/or password incorrect,” as shown in Figure 6.15, the wrong username and/or password was entered, and the authentication process failed.

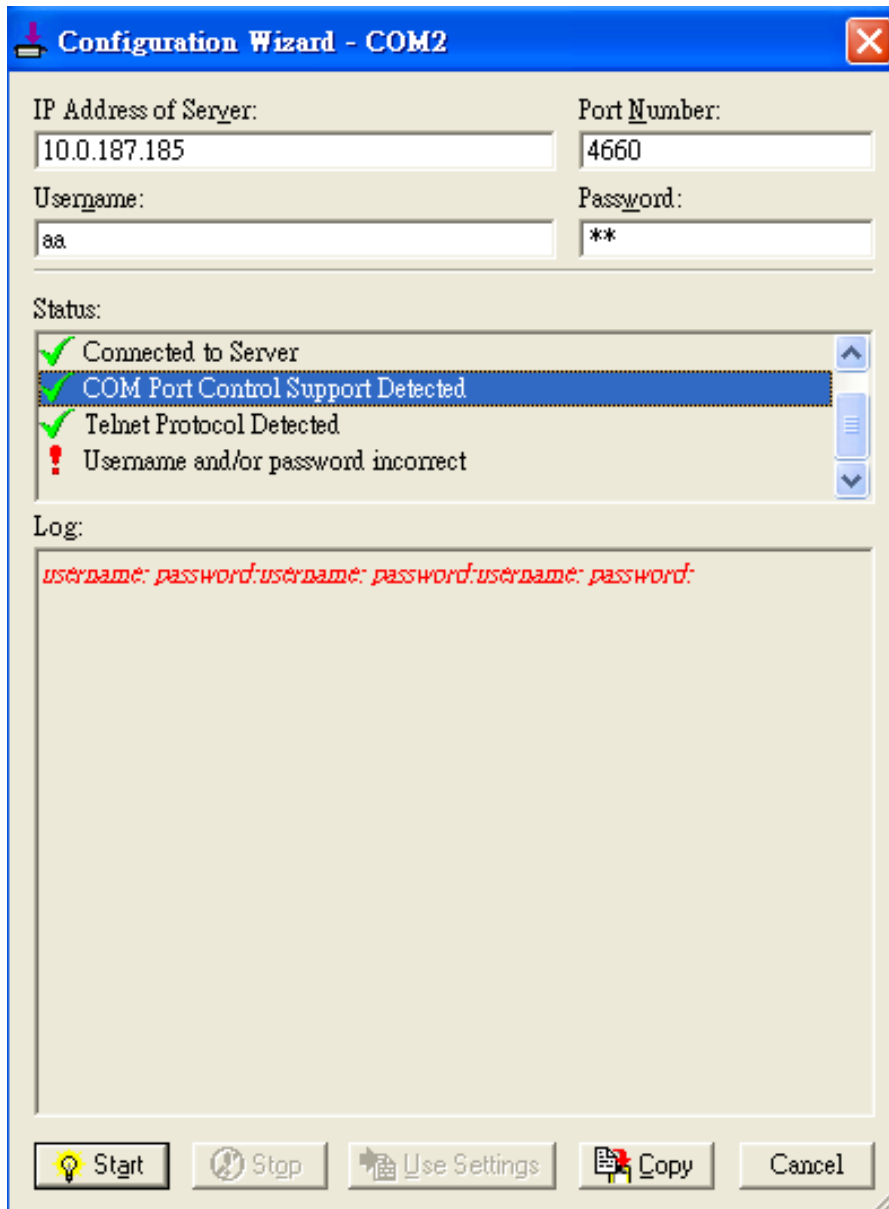


Figure 6.15 VCOM Authentication failed due to incorrect Username and/or Password

If the status reports with an exclamation mark with a message “No login/password prompts received from server,” as shown in Figure 6.16, the User Credentials option in the Serial/IP utility software is enabled but the VCOM Authentication option in the serial device server (i.e. the LES920 series device) is not enabled. Enable the VCOM Authentication option on the LES920 series device by setting a new and non-blank administrator’s Username and Password for the LES920 series device, as described in Section 4.13.2. Note that the Username and the Password for VCOM authentication are the same username and password of the LES920 series device’s Web UI login. The default account, which has the username as “admin” and the password as “default”, is considered as an unsecured account (no authentication option).

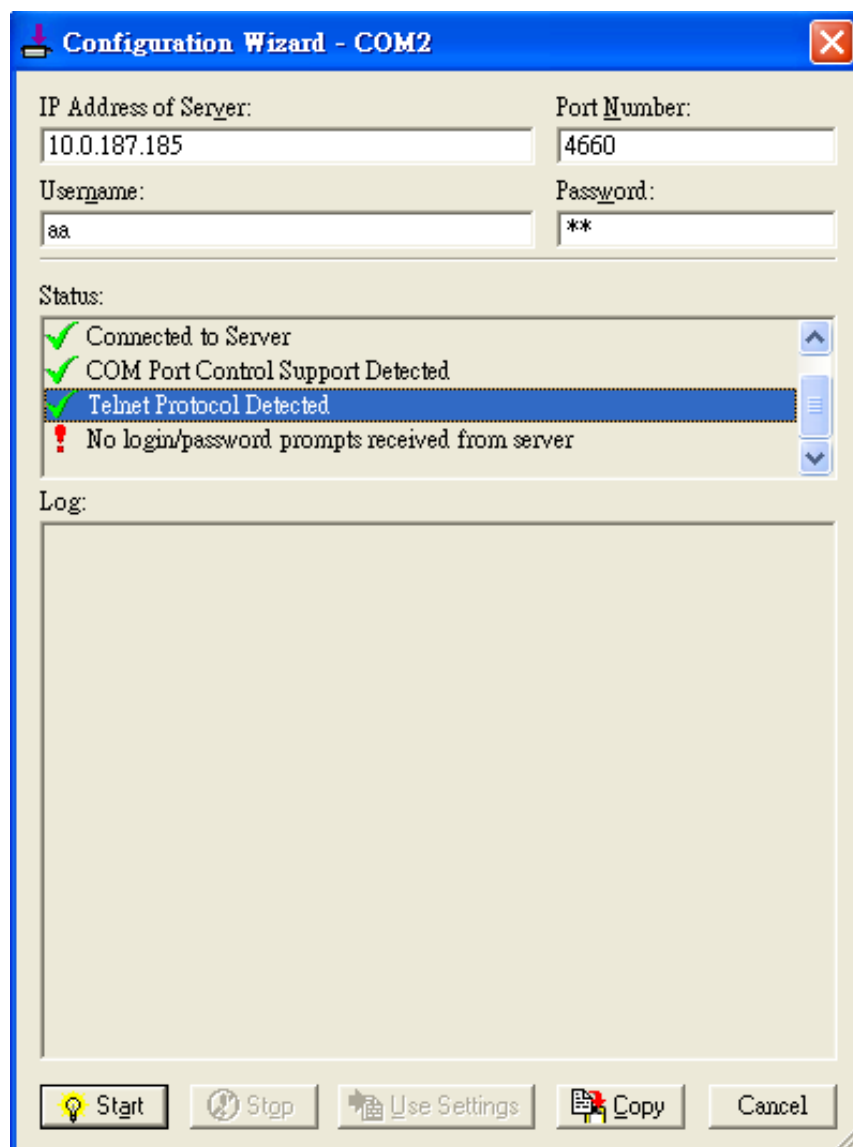


Figure 6.16 VCOM Authentication failed due to disabled VCOM Authentication on the LES920 series device

6.4 Using Serial/IP Port Monitor

Serial/IP Port Monitor is another available utility software. It allows you to monitor the activities or status of the 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:

- In Windows®, click on the Start menu → Select All Programs → Select Serial-IP → Select Port Monitor.
- Double click the Serial/IP tray icon in the notification area.
- In the 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 properly configured to connect to a serial device server (i.e. the LES920 series device), the status will display as Connected. If the Serial/IP utility software cannot find the specified serial device server, the status will display as Offline.

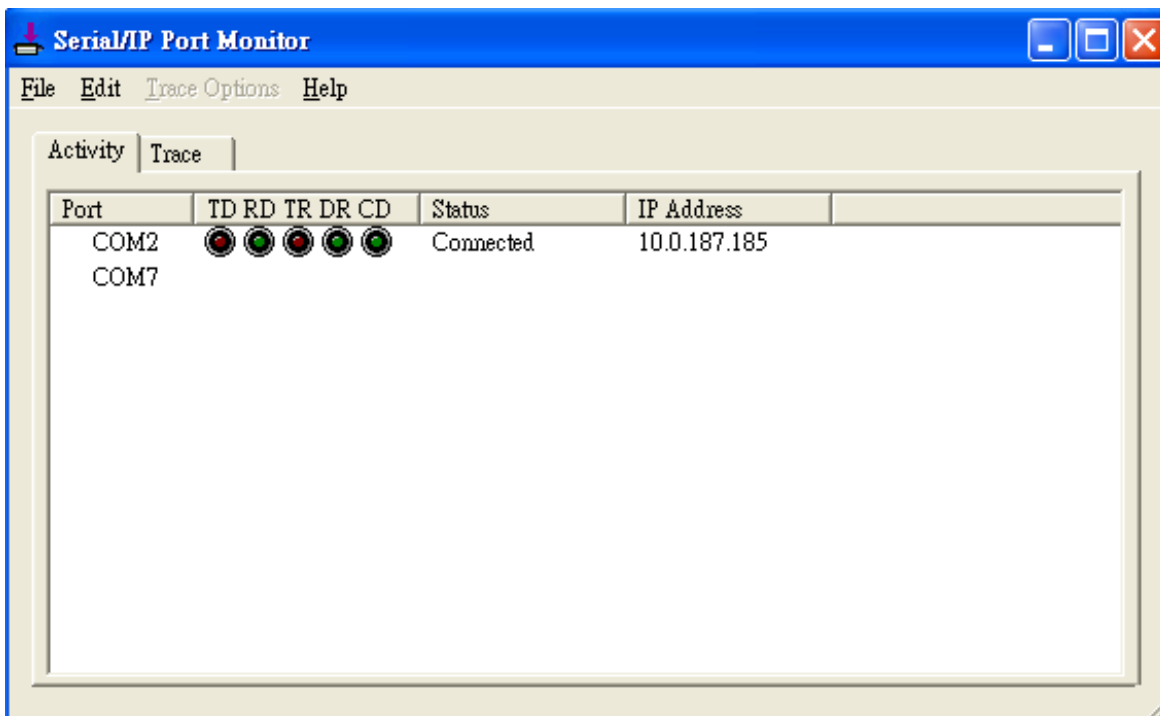


Figure 6.17 Activity Panel of Serial/IP Port Monitor

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

- **Port:** This is the virtual COM port number.
- **Line signal indicators:** The red color means no activity, while green color indicates activity.

- **TD** indicates data is being sent to the server.
- **RD** indicates data is being received from the server.
- **TR** (DTR) is the signal from the application to the server that the application has opened the virtual COM port. The most common use of DTR is to programmatically lower it to signal a modem to disconnect.
- **DR** (DSR) is the signal from the server to the application that a modem or serial device is connected to the server and ready to communicate.
- **CD** (DCD) is the signal from the server to the application that a modem has successfully negotiated a connection with another device.
- **Status:** This indicates the connection status of the software and serial device server which can be **connected** or **offline**.
- **IP Address:** This is the IP address of the serial device server.

Notes:

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

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 a 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 in the **Hex Display** box. Clicking on **Auto Scroll** box will cause the display to show the most recent trace data continuously. To ensure that the Port Monitor's window is always on top of other application's windows, check the **Always on Top** box. If you want to clear the displayed data in Trace panel, click on the **Clear** button.

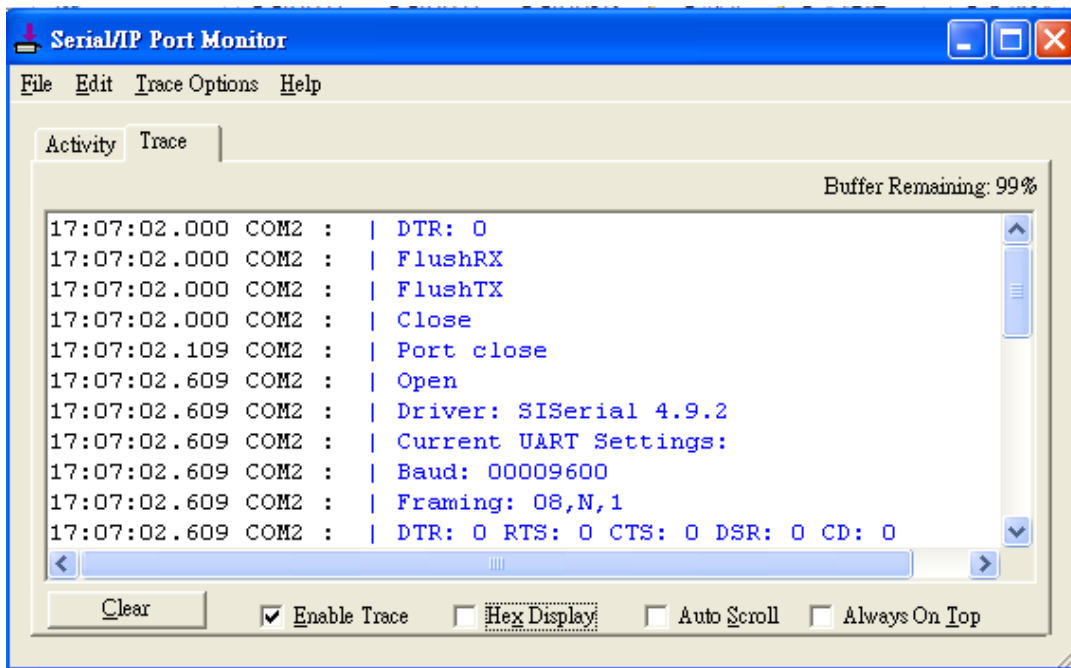


Figure 6.18 Trace Panel of Serial/IP Port Monitor

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

- **File:** To save the log file, which you can send to Black Box technical support for further analysis if problems occur with the Virtual COM connection, 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 of the amount of RAM being used for tracing, which can be normal or large.
 - **System Debug Output:** This menu allows you 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 events will be shown in red and preceded by “«”. The control events will be shown in blue and preceded by “|”.

Notes:

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

6.5 Serial/IP Advanced Settings

In the Serial/IP Control Panel, you can click on the Advanced... button to open the 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. A detailed description of each option and how to set a proxy server will be explained in the following subsections.

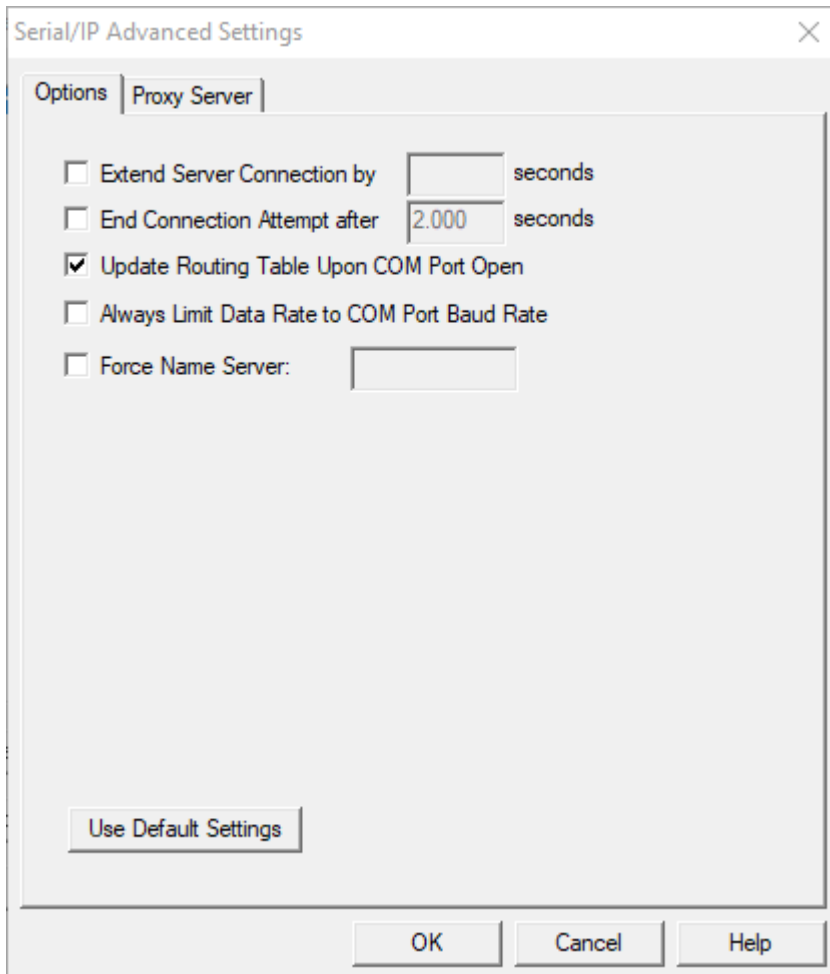


Figure 6.19 Serial/IP Advanced Settings Window

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. A description of each option follows:

- **Extend Server Connection:** When enabled, this option maintains the TCP connection for a specified amount of time after the COM port is closed. The default time value is 8000 milliseconds.

- **End Connection Attempt after:** When enabled, this option terminates pending connection attempts if they do not succeed in the specified time. The default time value is 2000 milliseconds.
- **Update Routing Table Upon COM Port Open:** When enabled, this option maintains the 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 the 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 it 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 you can stop the testing by clicking on the Stop button.

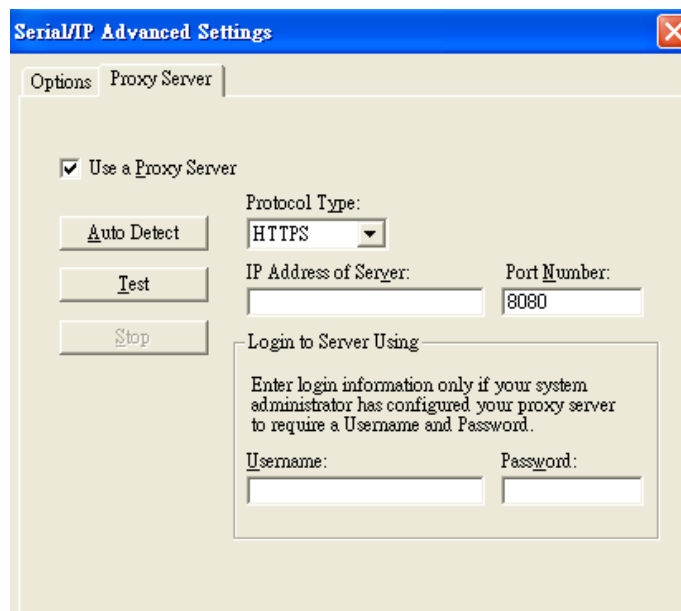


Figure 6.20 Proxy Server Tab under Serial/IP Advanced Settings

7 Specifications

7.1 Hardware

Table 7.1 Hardware Specifications

System			
CPU	32-bit ARM Based TI CPU AM3354 800MHz		
Flash Memory	32MB		
RAM	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 LES920 series only IEEE 802.3af (PoE PD) –selected LES920 series 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 1 tunnel) on LAN (software based)		
Serial			
Serial Interface	RS-232/RS-422/RS-485 Software Selectable (Default: RS-232)		
Serial Connector	Connector Type <ul style="list-style-type: none">Serial Ports (TB-5 or DB-9)		
Protection	16A (optional 3kV)		
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 RUN x 1 ALARM x 1 LAN: • x 2 COM port: • x 4
Power Requirement & EMC	
Input	Redundant 9~48 VDC
Consumption	Max. 7.8W
	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)	55 mm x 145 mm x 113mm (2.17 x 5.17 x 4.45 in)
Enclosure	IP30 protection, metal housing
Environmental	
Temperature	Operations -40° ~ 85°C (-40° ~ +185°F)
	Storage -40° ~ 85°C (-40° ~ +185°F)
Relative Humidity	5% ~ 95%, 55°C, Non-condensing

7.1.1 Pin Assignments

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

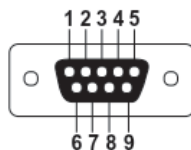


Figure 7.1 DB9 Pin Number

Table 7.2 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-232/RS-422/RS-485 connectors

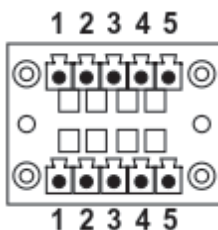


Figure 7.2 Terminal Block (TB-5) Pin Number

Table 7.3 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)

7.1.2 Pin Assignments for LAN Interface

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

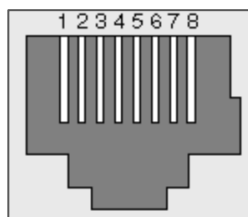








Figure 7.3 Ethernet Port on RJ45 with Pin Numbering

Table 7.4 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-

7.2 LED Indicators

Table 7.5 Color Interpretation of LED Indicators of LES920 Series Devices

Name	Colour	Status	Message
PWR (Power)	 Green	Steady/On	Power On and Power is being supplied
		Off	Power Off and no Power is being supplied
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

7.3 Software

Table 7.6 Software Tools and Utilities

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

8 Warranty

Limited Warranty Conditions

This product has a one-year warranty with options for a one-year and three-year extended warranty.

9 Tech Support/Contact Information

TECH SUPPORT/CONTACT INFORMATION

Visit blackbox.com/discover-bb/global-presence for regional technical support and contact information.

