

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*



SX-500 and SX-510
Serial Device Server
User's Reference Guide

Part Number 140-00188-180
Revision B

© 2009 Silex Technology America, Inc. All rights reserved.
February 2009

Silex Technology America SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS OF THIS PRODUCT FOR A PARTICULAR PURPOSE. Silex shall not be liable for any errors contained in this manual or for any damages resulting from loss of use, data, profits, or any incidental or consequential damages arising from the use of SILEX products or services. The information contained in this documentation is subject to change without notice.

Information and descriptions contained herein are the property of Silex. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Silex. This publication is subject to change without notice.

The software embedded in this SX-500 serial device server includes the eCos operating system. eCos and certain other software programs used in the SX-500 are licensed under GNU GPL compatible Free Software Licenses (with the eCos exception clause). In compliance with these licenses, you can obtain the relevant source code at no charge by contacting Silex at support@silexamerica.com.

Trademarks

ExtendView is a trademark of Silex Technology America, Inc. All other company or product names referenced in this document may be trademarks or registered trademarks of their respective owners.

Silex Technology America, Inc.

www.silexamerica.com

Contents

About This Reference Guide 1
Safety Precautions 1
Emissions Disclaimer 1
Chapter 1: Introduction 2
Chapter 2 Installing the Serial Device Server Hardware 3
Verify Package Contents 3
Installing the Serial Device Server 3
Monitoring Serial Device Server Status 5
Chapter 3 Configuring the Serial Device Server 7
Basic Configuration Requirements 7
Configuration Methods 8
Using the ExtendView Utility to Configure the Serial Device Server (Ethernet Connection) 9
First-Time IP Address Configuration 13
Using a Web Browser to Configure the Serial Device Server 15
Using the Internal Command Console to Configure the Serial Device Server 17
Chapter 4 Using the Serial Device Server with Your Application 20
Serial Port Emulator 20
Raw TCP connection 21
RFC 2217 Remote Modem Control Support 22
ECable Mode 22
Print Server Mode 23
FTP 23
Console Mode Switching 23
AT Commands 24
SNMP Traps and Email Alerts 24
Chapter 5 Advanced Configuration 26
Factory Default Settings 26
Restoring Factory Default Settings 27
Modifying TCP/IP Settings 27
Configuring SNMP 29
Configuring Serial Port Monitor Alert and Trap Configuration 31
Setting up Email Alerts and SNMP Traps 32
Using AT Modem Commands 33
Standard AT Commands Supported 33
Response Codes 36
Using ExtendView for Bulk Configuration 36
Chapter 6 Troubleshooting 37
Chapter 7 Product Specifications 39
TCP Port Connections 40
Appendix A Advanced Security Configuration 41
Appendix B Console Commands 45
Wireless and Network Security Commands 45
Port Commands 51

Server Information Commands 52
Service Commands 53
String Commands 55
TCP/IP Commands 56
Firmware Update 61
Miscellaneous Commands 62
Help Commands 62
Appendix C Firmware Update Procedures 63
Appendix D Safety and Regulatory Notices 65
Information for United States Users 65
Declaration of Conformity (FCC) (SX-500) 66
Information for Canadian Users (IC notice) (SX-500) 66
Information for European Users (SX-500) 67
Declaration of Conformity (CE) (SX-500) 67
Declaration of Conformity (FCC) (SX-510) 68
Information for Canadian Users (IC notice) (SX-510) 68
Appendix E Silex Contact Information 70

Figures

Figure 1 SX-500 (Wireless Model) and SX-510 2
Figure 2 TCP/IP Window 27
Figure 3 Change Password Window 28
Figure 4 Advanced TCP/IP Configuration Window 29
Figure 5 SNMP Configuration 31

Tables

Table 1 Development Kit Contents 3
Table 2 Status Monitors 5
Table 3 Factory Default Settings 26
Table 4 TCP/IP Settings 28
Table 5 TCP/IP Configuration Settings 29
Table 6 SNMP Commands 30
Table 7 Port Monitor Alert Commands 31
Table 8 AT Commands 33
Table 9 Extended AT Commands 35
Table 10 Response Codes 36
Table 11 Product Specifications 39
Table 12 Radio Performance Specifications 40
Table 13 TCP Port Connections 40
Table 14 Network Commands 45
Table 15 Port Commands 51
Table 16 Server Information Commands 52
Table 17 Service Commands 53
Table 18 String Commands 55
Table 19 TCP/IP Commands 56
Table 20 Firmware Update 61
Table 21 Miscellaneous Commands 62

About This Reference Guide

Safety Precautions

- To prevent damage to the Serial Device Server's electronic circuit components, follow established ESD practices and procedures for handling static-sensitive devices. All ESD-sensitive components must be stored and shipped in ESD-conductive bags or bubble-wrap and labeled as such using the standardized ESD adhesive warning label.
- Ethernet electrical wiring must be at least 6 feet from bare power wiring or lightning rods and associated wires, and at least 6 inches from other types of wire (antenna wires, doorbell wires, wires from transformers to neon signs), steam or hot water pipes, and heating devices.
- Protectors and grounding wire placed by the service provider must not be connected to, removed, or modified by the customer.

Emissions Disclaimer

Regulatory compliance information can be found in Appendix D of this manual. Final emission certification per FCC, CE and other agency requirements are the responsibility of the OEM using any printed circuit assemblies or other items used in this developer's kit in their saleable packaged product.

Chapter 1: Introduction

The SX-500 and SX-510 Serial Device Servers provide a complete solution for connecting serial devices to 802.11 wireless or Ethernet wired networks. The following models are available:

- SX-500-003*x* Ethernet model. The SX-500 Ethernet model includes an RS-232-C device interface, 10Base-T/100Base-T Ethernet network interface, and AC power supply.

- SX-500-103*x* Wireless model. The SX-500 Wireless model includes an RS-232-C device interface, an 802.11b/g wireless LAN interface, a 10-Base-T/100Base-T Ethernet network interface, and an AC power supply.

- SX-510-103*x* Wireless model. The SX-510 wireless model includes an RS-232-C/RS-422/RS-485 device interface, an 802.11a/b/g wireless LAN interface with internal diversity antennas, a 10-Base-T/100Base-T Ethernet network interface, and an AC power supply.

The *x* in the model number designates the country or region (1 = U.S., 3 = Europe, 5 = Japan; for example, SX-500-1031 is an SX-500 wireless model for the U.S.).



Figure 1 SX-500 (Wireless Model) and SX-510

Chapter 2
Installing the Serial Device Server Hardware

The Serial Device Server includes most of the hardware and software components required for installation. The one item that you will need to purchase separately is a cable to connect your serial device to the Serial Device Server (this cable is not included because of the wide variety of connector types used on serial devices).

Verify Package Contents

The Serial Device Server includes the components listed in Table 1. Please ensure that all materials listed are present and free from visible damage or defects before proceeding. If anything appears to be missing or damaged, please contact Silex.

Table 1 Package Contents

Description
SX-500 or SX-510 Base Unit (SX-500 wireless models include an external pole antenna)
Setup Guide
CD-ROM containing ExtendView software, Serial Port Emulator Software, and User's Reference Guide
AC Power Supply with power cord
Warranty Card

Installing the Serial Device Server

Follow the steps below to install the Serial Device Server. The Serial Device Server's factory default settings should be sufficient for most serial connections; however, some of the configuration settings may have to be changed for your particular installation.

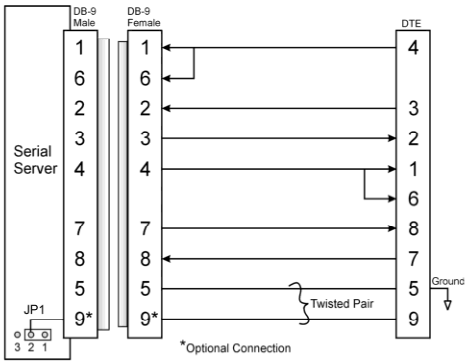
1. Before attempting to install the Serial Device Server, make sure you have installed and set up your serial device as described in the documentation that came with the device.

2. Write down the 12-digit MAC (Media Access Code) address printed on the label located on the bottom of the Serial Device Server (for example: 004017023F96). You may need this number in order to configure the Serial Device Server.

3. If you have a wireless model, connect the antenna to the unit.

4. Connect the Serial Device Server to your serial device. If you are using RS-232, you may use standard PC cabling (you should normally use a null modem crossover cable). The 9-pin connector pinouts and cabling are as follows:

Pin	Description
1	DCD (Data Carrier Detect) Input
6	DSR (Data Set Ready) Input
2	RxD (Receive Data) Input
3	TxD (Transmit Data) Output
4	DTR (Data Terminal Ready) Output
7	RTS (Request To Send) Output
8	CTS (Clear To Send) Input
5	Ground
9	RI (Ring) Input or +5 VDC Power Input (Optional)



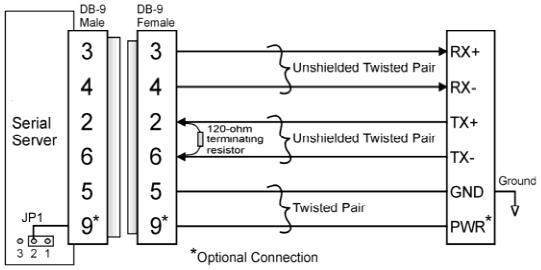
RS-232 connector pinouts and cabling

If you are using RS-422 or RS-485 in full-duplex or half-duplex modes, you will need a special cable. In addition, if the Silex Serial device Server is the last one in a chain, then a 120-ohm resistor should be placed between pins 2 and 6 (for full-duplex mode) or pins 4 and 5 (for half-duplex mode).

IMPORTANT: IF YOU ARE USING RS-422, RS-485, OR RS-485 HALF-DUPLEX, YOU MUST SET THE SERIAL PORT LINE MODE AS DESCRIBED IN CHAPTER 3 OF THIS MANUAL.

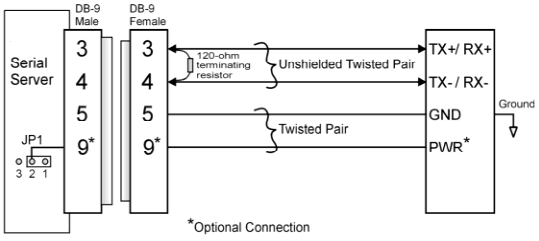
The RS-422 and RS-485 pinouts and cabling are shown in the following diagrams:

Pin	Description
3	TX+ (Transmit) Output
4	TX– (Transmit) Output
2	RX+ (Receive) Input
6	RX– (Receive) Input
5	Ground
9	+5 VDC Power Input (optional)



RS-422/485 full-duplex connector pinouts and cabling

Pin	Description
3	TX+/RX+ (Bi-Directional)
4	TX–/RX– (Bi-Directional)
5	Ground
9	+5 VDC Power Input (optional)



RS-485 half-duplex connector pinouts and cabling

IMPORTANT NOTE: THE SX-510 RS-422/RS-485 INTERFACE HAS NOT BEEN TESTED FOR COMPLIANCE WITH IEC 60601-1-2:2001/EN60601-1-2 MEDICAL EMC OR ANSI/IEEE Std. C95.1-1999, RSS-102 SAR STANDARDS. THEREFORE RS-422/485 SHOULD NOT BE ENABLED IF YOU REQUIRE COMPLIANCE WITH ANY OF THESE STANDARDS.

5. Plug the Serial Device Server power supply adapter into a suitable AC receptacle, and then plug the power supply cable into the Serial Device Server. Alternatively, you can use pin 9 on the 9-pin connector to provide power to the Serial Device Server (1 amp @ +5V is required). The Serial Device Server will run through a sequence of power-up diagnostics for a few seconds.

   - If the Serial Device Server is operating properly, the LEDs will blink momentarily and then go out, the yellow and green LEDs will illuminate if the wireless network is active, and the orange LED will illuminate, indicating the device is receiving power.
   - The unit powers up in the Normal mode, which provides for connection from the network to device(s) connected to the serial port of the Serial Device Server.
   - If the orange LED blinks continuously in a regular pattern, a problem exists. If this is the case, try powering the unit OFF and then ON again.

NOTE: Pin 9 is normally configured for supplying +5V from an external power source in lieu of using the AC power supply adapter. If you wish to use this pin as the Ring Indicator (RI) modem signal on the SX-500 (not available on the SX-510), open the enclosure and move the jumper on connector JP1 onto pins 2 and 3 of this connector.

6. Connect the Serial Device Server to your network through a switch or hub using a category 5 (CAT5) Ethernet cable. Serial Device Server wireless models automatically detect the presence of this cable, and will switch off the wireless networking functionality as long as the cable is plugged in.

NOTE: SILEX RECOMMENDS USING A HARDWIRED ETHERNET CONNECTION FOR CONFIGURING WIRELESS SERIAL DEVICE SERVERS. If you have a wireless Serial Device Server model and cannot use an Ethernet connection, refer to step 4 in the *First Time IP Address Configuration* section of this chapter for instructions on how to set up the Serial Device Server using a completely wireless Ad Hoc environment.

7. The Serial Device Server's IP address must be configured before a network connection is available. If your network offers DHCP (Dynamic Host Configuration Protocol), the Serial Device Server will automatically search for a DCHP server upon power up and obtain an IP address. If your network does not offer DHCP, a static (fixed) IP address must be assigned (see your system administrator for assistance). If you use DHCP, make sure that the length of the DHCP lease is adequate so that the IP address of the Serial Device Server does not change.

Monitoring Serial Device Server Status

You can monitor the Serial Device Server status using the yellow, green and orange LED status indicators on the monitor. Table 2 defines the default functions of the LED status indicators.

Table 2 Status Monitors

Function	State	Status
Power Orange	On	The Serial Device Server is receiving power
	Off	The Serial Device Server is not receiving power
	Blinking	The Serial Device Server power supply is malfunctioning
Network Status Yellow or Green	Yellow Off Green Off	No network activity
	Yellow On Green Off	10base-T network active

Function	State	Status
	Yellow Blinking Green Off	10base-T network data received
	Yellow Off Green On	100base-TX network active
	Yellow Off Green Blinking	100base-TX network data received
	Yellow On Green On	Wireless network active, if WLAN model
	Yellow Blinking Green Blinking	Wireless network data received, if WLAN model

Chapter 3
Configuring the Serial Device Server

This chapter describes the methods for configuring the basic settings of the Serial Device Server, including the IP address, serial port settings, and wireless security. The Serial Device Server also has an extensive range of advanced configuration capabilities that are described in Chapter 5, Appendix A, and Appendix B. The Serial Device Server configuration should be done by a network administrator or another person with technical knowledge of TCP/IP networking and serial communications.

Basic Configuration Requirements

In order to use the Serial Device Server, the following basic parameters must be configured:

TCP/IP Settings:

- IP Address
- Subnet Mask
- Router Address

Note: The TCP/IP settings can be automatically configured using DHCP.

Wireless Configuration Settings:

- SSID
- Mode (Infrastructure or Ad Hoc)
- Channel (required only if using Ad Hoc mode)

Security Settings:

- Wireless Encryption Mode (WPA2, WPA, WPA2-WPA, WEP)
- Wireless Encryption Settings
- Wireless Authentication Mode (WPA-PSK, Open System, Shared Key, TTLS, TLS, LEAP, PEAP, EAP-FAST)
- Wired Authentication Mode (TTLS, TLS, PEAP, EAP-FAST)
- Authentication Settings

Note: There are numerous possible encryption and authentication settings, and every network can have different settings. Please refer to Appendix A for a detailed summary of these settings.

Serial Port Settings (must match the settings of the attached serial device):

- Baud Rate (Speed)
- Parity

- Character Size
- Flow Control
- Line Mode (RS-232, RS-422, RS-485 full-duplex, RS-485 half-duplex; RS-422 and RS-485 are supported on the SX-510 only)

In addition to the above parameters, the Serial Device Server allows you to configure numerous other capabilities. These other capabilities provide you with the unparalleled flexibility to use the Serial Device Server on virtually any 802.11 or Ethernet network with a wide range of serial devices.

Configuration Methods

There are three ways to configure the Serial Device Server:

- *ExtendView.* ExtendView is a simple Graphical User Interface configuration program for Windows. In addition to setting up the initial Serial Device Server configuration, ExtendView also has the advantage of allowing you to perform bulk configuration of multiple Serial Device Servers simultaneously.

- *Internal Web Pages (HTTP).* You can use any standard web browser to access the Serial Device Server internal web pages. These web pages provide an easy-to-use graphical interface for configuring the Serial Device Server. In order to use the internal web pages for the first time, you must assign the Serial Device Server IP address using some other method (for example, DHCP or arp/ping). This initial IP address assignment need only be done one time.

- *Internal Command Console.* The internal command console provides a sophisticated command line interface for advanced users to configure the Serial Device Server. It can be accessed by connecting a serial cable to the serial port and using console mode switching as descried in chapter 4. Once the IP address has been assigned, the internal command console can also be accessed via TELNET, or via ExtendView and the internal web pages.

If you have a Serial Device Server wireless model, Silex recommends that you temporarily plug the Serial Device into a wired Ethernet network during the configuration process. Although it is possible to configure the Serial Device Server with a completely wireless setup, it is much simpler to perform the process using a wired Ethernet connection. This is primarily because the wireless security on most wireless networks prevents the addition of a new wireless device unless all security parameters are first entered into that device. As a result, you must set up a temporary dedicated ad hoc wireless network in order to configure the Serial Device Server in a completely wireless environment (refer to the step 4 in the *First Time IP Address Configuration* section of this chapter for instructions on how to set up the Serial Device Server using a completely wireless Ad Hoc environment).

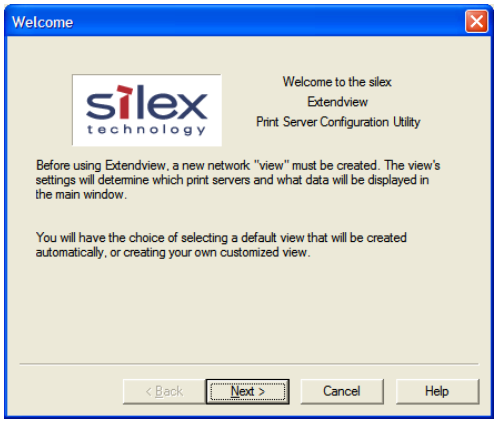
Configuring the Serial Device Server using each of the above methods is described in the following sections of this chapter.

Using the ExtendView Utility to Configure the Serial Device Server (Ethernet Connection)

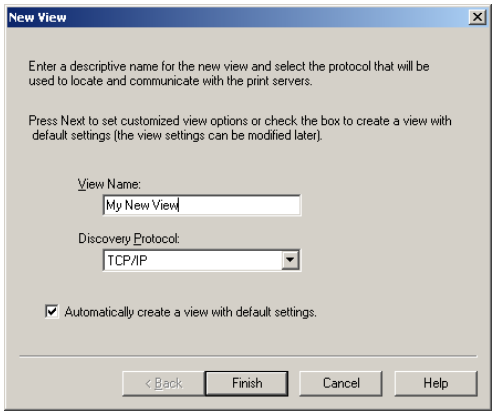
NOTE: Skip this section if you do not have a Windows PC or if you do not have an Ethernet connection available for configuring your Serial Device Server wireless model.

The ExtendView Utility is the easiest way to initially configure the Serial Device Server from a Windows PC because it allows you to directly set the IP address into an unconfigured Serial Device Server, and it allows you to view the IP addresses of all of the Serial Device Servers on your network. It has limited capabilities for configuring 802.1X authentication, but it can be used in conjunction with either the internal web pages or the internal command console for complete configuration capabilities.

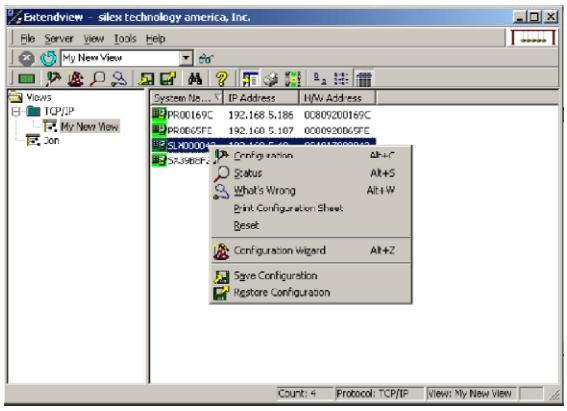
ExtendView is a component of the CD-ROM that is included with the Serial Device Server, or it can be downloaded from the Silex website. To install ExtendView, simply follow the on-screen installation instructions. The Serial Device Server configuration procedure is as follows (please note that the screens may be slightly different than shown, depending on the Serial Device Server model and the firmware and software revision levels).



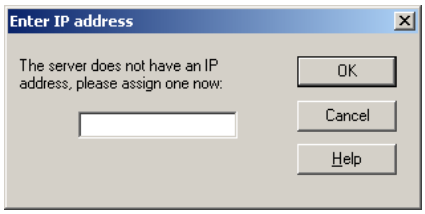
1. Start the ExtendView Utility by clicking on ***Start***, ***Programs, silex technology, ExtendView***, and then ***ExtendView***.



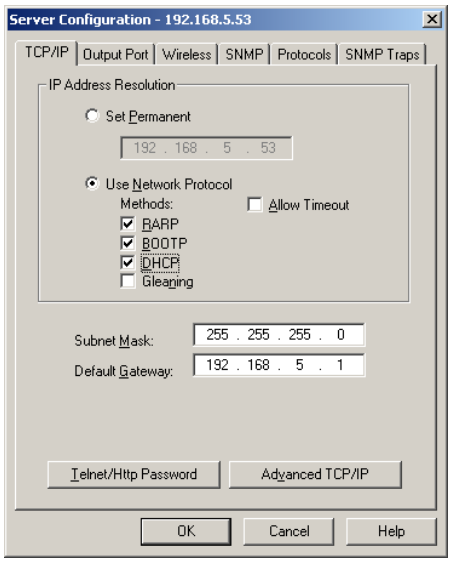
2. When the Welcome screen appears, click on ***Next***, choose any name for your ***View Name***, select ***Automatically create a view with default settings*** (or configure the view to your preferences), and then click ***Finish***.



3. Right-click on the Serial Device Server that you want to configure from the displayed list, and then left-click on ***Configuration***. The default Serial Device Server name is SLX*xxxxxx* (where *xxxxxx* is the last six digits of the MAC address from the label that is affixed to the Serial Device Server).

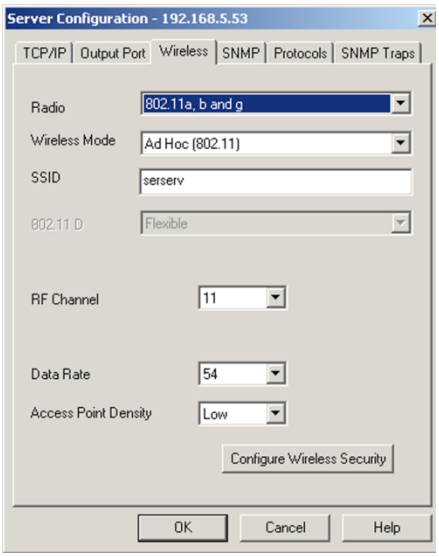


4. If you do not have a DHCP server, you will be asked to manually enter an IP address (if you are not sure what IP address to enter, ask your network administrator). Click ***OK*** when you are finished.



5. The Server Configuration window will appear. Check the IP address setting to make sure it is correct. If necessary, change the Subnet Mask and Gateway. If you have a WINS server, enter its address or click ***Use DHCP to Locate WINS Server.*** If desired, you can configure advanced TCP/IP settings by clicking the ***Advanced TCP/IP*** button (refer to Chapter 5 for information). This advanced configuration can be done at a later time, however.

NOTE: If you are using DHCP on your network, the SX-500 should have acquired valid IP settings at this point and no further configuration is necessary. However, for some installations, a static IP address is preferred. If your DHCP server does not allow the SX-500 to keep its assigned IP address permanently, then you must manually assign an IP address. In this case, use a static IP address outside the range reserved for DHCP (see your DHCP server documentation for details). To assign a static IP address, select *Set Permanent* as the *IP Address Resolution*, and assign a valid static IP address for your network. Click on *OK* to save the new settings.

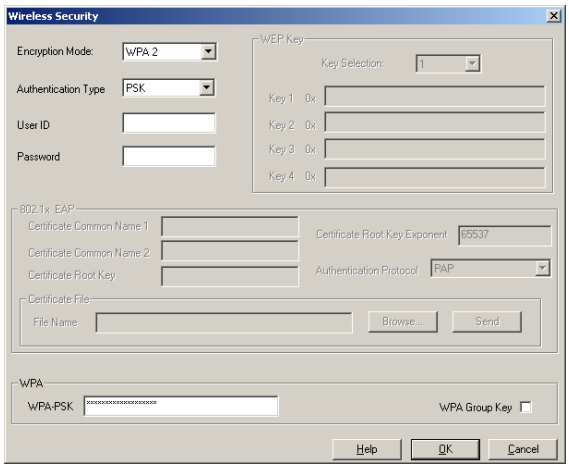


6. Click the **Wireless** tab to configure the 802.11 wireless settings (for wireless models only; skip to the next section if you have a wired model). To operate on an 802.11 network, the Serial Device Server configuration must be configured with the wireless configuration and security parameters necessary for the Serial Device Server to communicate over your wireless network (check with your network administrator if you do not know these parameters).

    - Select either Infrastructure (if you are using an access point) or Ad Hoc (point-to-point) as the wireless mode
    - Enter the SSID for your network
    - If you are using Ad Hoc, select the RF channel (not required for infrastructure)

    The other parameters on this tab do not normally need to be changed (refer to Chapter 5 for information on advanced configuration).

    Now click the ***Configure Wireless Security*** button to configure the wireless security parameters.

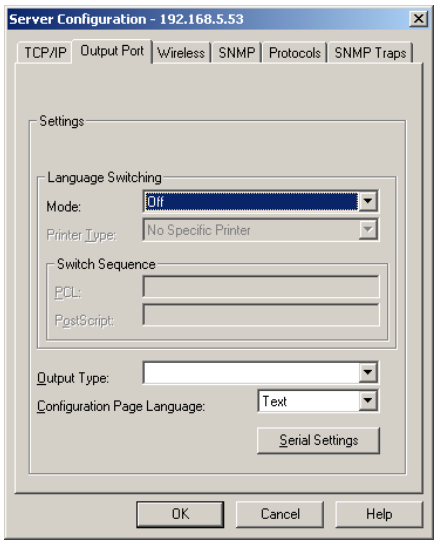


7. If you are using WPA2-PSK, select WPA2 as the Encryption Mode and select PSK as the Authentication Type. If you are using WPA-PSK, select WPA as the encryption mode and select PSK as the Authentication Type. For both WPA2-PSK and WPA-PSK you must enter the Pre-Shared Key for your network and select whether you want a Group Key. Note that it is not necessary to enter a User ID or password.

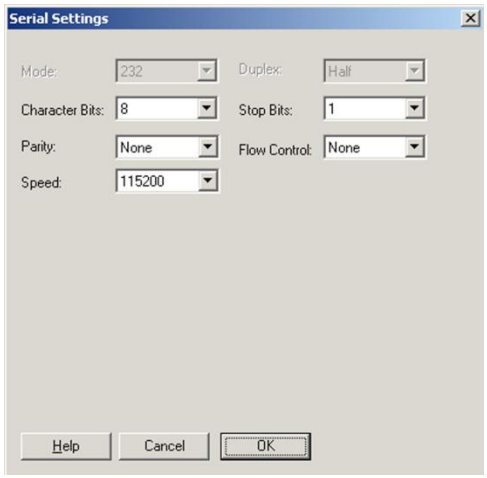
    If you are using WEP, select 128-bit or 64-bit as the Encryption Mode and Open Systems or Shared Key as the Authentication Type. Enter the WEP keys in hexadecimal format, and select the transmit key (Key Selection).

    ExtendView does not fully support configuration of the 802.1X EAP types, so Silex recommends using the internal web pages or internal command console for 802.1X configuration as described later in this chapter.

    Click ***OK*** to return to the Server Configuration window, and then click the I/O port tab to configure the serial port.



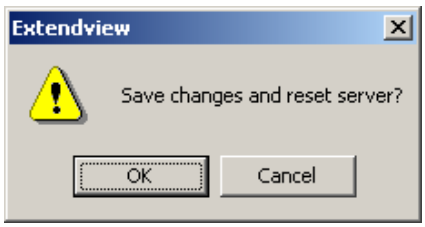
8. You do not need to change any of the settings in this window. Click the ***Serial Settings*** button to configure the serial port.



9. Configure the serial port settings so that they match the settings on your device. For example, if your device is set for 9600bps, odd parity, and XON/XOFF flow control, you must change the settings on the Serial Device Server to these settings.

   If are using either RS-422 or RS-485 (SX-510 only), select 422 or 485 as the Mode. Select Half as the Duplex type if you are using RS-485 half-duplex.

   Click ***OK*** when you are finished to return to the Server Configuration window and then click ***OK*** again.



10. Click ***OK*** to save your changes and reset the Serial Device Server. If you are configuring a Serial Device Server wireless model, unplug the Ethernet cable. You can now use the Serial Device Server on your network. You may skip the remaining sections of this chapter, although this information is useful for future reference.

First-Time IP Address Configuration

NOTE: Skip this section if you have already configured the SX-500 IP address with ExtendView

If you are configuring the Serial Device Server from a non-Windows computer or if you cannot use an Ethernet connection, you must first configure the Serial Device Server IP address. Note that it is only necessary to perform this task one time -- once the address has been configured, the Serial Device Server can be accessed from any computer on the network that has the appropriate privileges. The steps are as follows:

1. If your network has a DHCP server and you can use an Ethernet connection to the Serial Device Server:
    a. Make sure your PC is connected and has access to your network.
    b. Connect an Ethernet cable from your network hub to the Serial Device Server (if you have a wireless Serial Device Server and do not have hardwired capabilities, then you must go to Step 4 below for setup instructions).
    c. Power on the Serial Device Server.
    d. The administration program on most DHCP servers logs the IP address and MAC address of each DHCP client. The MAC address of the Serial Device Server can be found on the label affixed to the unit. If your DHCP server has logged this information, write down the IP address of the Serial Device Server for future reference. You are now ready to configure the Serial Device Server (skip the remainder of this section).
    e. If your DHCP server does not provide client information or if you do not have access to the DHCP server, then you can get the IP address by connecting a serial device such as a printer, a Windows PC running HyperTerminal, or another serial device capable of printing ASCII characters to the serial port the Serial Device Server). Your serial device must be set at 115.2Kbps, 8-bit character size, and no parity.
    f. With the serial device and Serial Device Server switched on and ready, press the ***Reset*** pushbutton on the Serial Device Server. This will cause the Serial Device Server configuration data to be sent to the connected serial device. The serial device should display or print the current IP address assigned to the Serial Device Server by your network DHCP service. Write down this address for future reference. You are now ready to configure the Serial Device Server (skip the remainder of this section).
2. If you can connect the Serial Device Server via Ethernet but do not have a DHCP server, then you must use the following procedure for the first-time IP configuration of the Serial Device Server.
    a. Make sure your PC is connected and has access to your network
    b. Connect an Ethernet cable from your network hub to the Serial Device Server. The Serial Device Server must be on the same network segment as the PC (that is, there can be no router between the Serial Device Server and the PC).
    c. From the Windows Command Prompt (MS-DOS Prompt), the Mac OS X Terminal Utility, or the UNIX/Linux command line, enter the command

        arp –s *ipaddress macaddress*

        ping *ipaddress*

        Where *ipaddress* is the desired IP address of the Serial Device Server and *macaddress* is the MAC address of the Serial Device Server (found on the label affixed to the Serial Device Server). For example:

arp –s 192.168.5.53 00:40:17:00:00:01

ping 192.168.5.53

Note that Windows systems use the format *xx-xx-xx-xx-xx-x*x for the MAC address (for example, 00-0017-00-00-01).

You will see a reply from the Serial Device Server with the number of bytes and other information if the address was successfully set.

If you get an error message or no response, then the IP address was not set. If this is the case, the Serial Device Server may not be at its default configuration. To reset the Serial Device Server to its default settings, hold down the reset pushbutton for more than five seconds.

d. You are now ready to configure the Serial Device Server (skip the remainder of this section).

NOTE: Skip the following step if you have configured IP address of the Serial Device Server using an Ethernet cable.

3. If you are using a wireless connection for the first-time configuration of the Serial Device Server, you must set up a temporary ad hoc wireless connection as described in the following steps. Please note that because this is a fairly complex process, we do not recommend it unless it is not possible to use a wired connection.

    a. Disconnect your PC and the Serial Device Server from your network, and temporarily set the PC settings as follows:

        - IP address: 192.0.0.191
        - Wireless Mode: ***Ad Hoc*** (sometimes referred to as Peer-to-Peer)
        - Channel: ***11***
        - SSID (or wireless network name): ***serserv***

    b. Power on the PC and the Serial Device Server. You can connect to the Serial Device Server by specifying its default IP address of 192.0.0.192 using a web browser as described in the next section. When you have connected to the Serial Device Server, you must then change the IP address and enter the required wireless networking parameters using either the web browser interface or the internal command console (see next two sections) for operation on your wireless network.

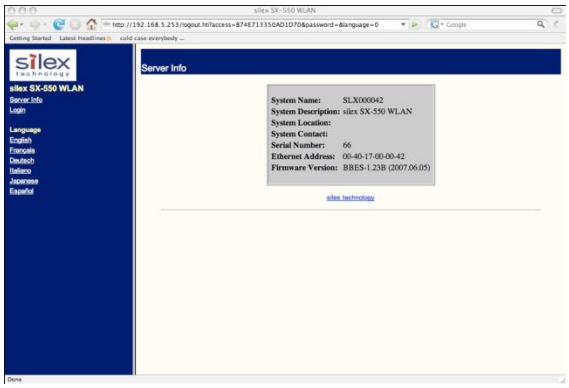
    c. After you complete the entire Serial Device Server configuration process, you must set your PC back to its original network settings.

Using a Web Browser to Configure the Serial Device Server

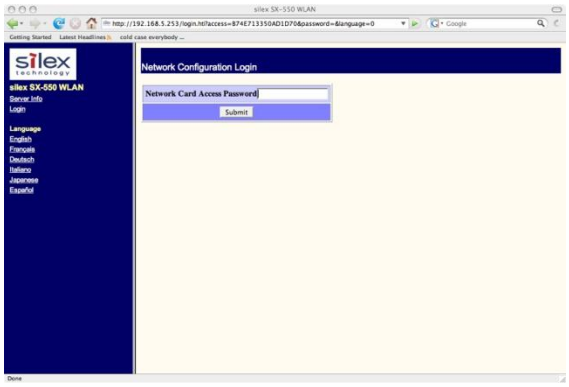
After you have entered an IP address into the Serial Device Server, you can use any standard web browser to access the internal web pages for configuring the Serial Device Server. Simply specify the IP address of the Serial Device Server in your browser and then follow the steps below:

You may skip this section if you have completely configured the SX-500 using ExtendView. However, if you have advanced configuration requirements, such as 802.1X EAP configuration, then you may need to use the internal web pages as described in this section because ExtendView does not support these capabilities.

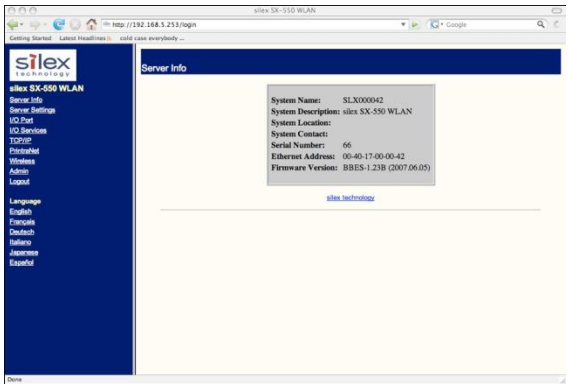
IMPORTANT: You must click the *Submit button* when you have finished configuring an internal web page. If you do not do this, your changes will not be saved.



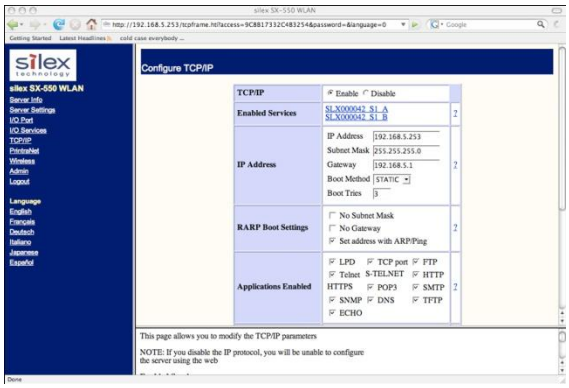
1. When you have connected to the Serial Device Server, you will get the Server Info page. Click ***Login*** on the left side of the screen.



2. Enter the password ***access*** and press ***Submit***.



3. You will return to the Server Info page, but new options will be listed on the left side of the screen. Click on ***TCP/IP***.

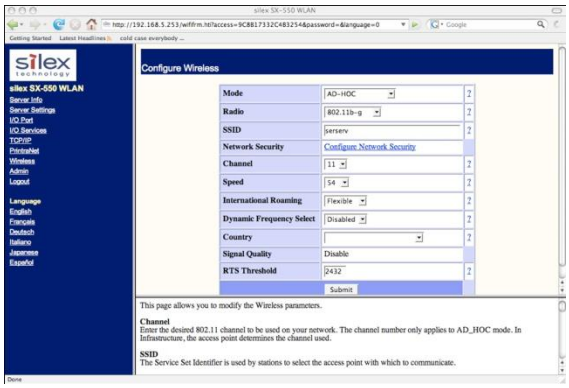


If you used DHCP, verify that the IP address is correctly set. If you used the default 192.0.0.192 IP address, you MUST change it to a new valid IP address. If necessary, change the Subnet Mask and Gateway. It is generally not necessary to change the other parameters on this page (refer to Chapter 5 for advanced configuration information.

Note that on-line help information is available on every configuration page.

Click the ***Submit*** button at the bottom of the window (you may need to scroll) to save your changes.

NOTE: If you are using DHCP on your network, the SX-500 should have acquired valid IP settings at this point and no further configuration is necessary. However, for some installations, a static IP address is preferred. If your DHCP server does not allow the SX-500 to keep its assigned IP address permanently, then you must manually assign an IP address. In this case, use a static IP address outside the range reserved for DHCP (see your DHCP server documentation for details). To assign a static IP address, select *Set Permanent* as the *IP Address Resolution*, and assign a valid static IP address for your network. Click on *OK* to save the new settings.



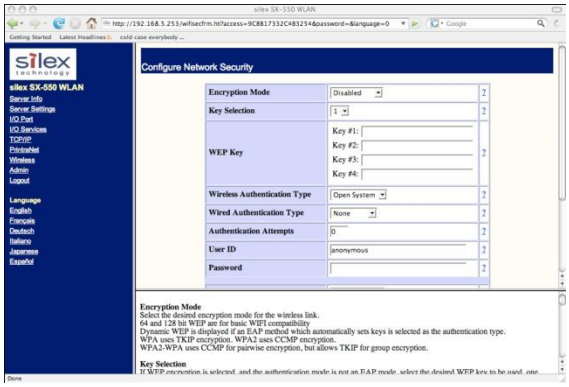
4. Click ***Wireless*** on the left side of the screen to configure the 802.11a/b/g wireless settings (for WLAN models only; skip to the next section if you have an Ethernet model). To operate on an 802.11a/b/g network, the Serial Device Server configuration must be configured with the wireless configuration and security parameters required to allow the Serial Device Server to communicate over your wireless network (check with your network administrator if you do not know these parameters).

    - Select either Infrastructure (if you are using an access point) or Ad Hoc (point-to-point) as the wireless mode
    - Enter the SSID for your network
    - If you are using Ad Hoc, select the RF channel (not required for infrastructure)

    The other parameters on this page do not normally need to be changed (refer to Chapter 5 for information on advanced configuration).

    Click the ***Submit*** button at the bottom of the window (you may need to scroll) to save your changes.

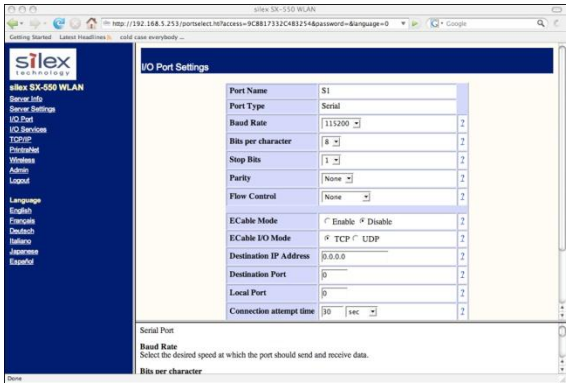
    Now click ***Configure Network Security*** to configure the wireless security parameters.



5. Select the appropriate wireless encryption mode and enter the required settings (check with your network administrator for the proper settings if you do not know them). Appendix A lists the possible encryption settings.

   Click the ***Submit*** button at the bottom of the window (you may need to scroll) to save your changes.

   Now click ***I/O Port*** on the left side of the screen to configure the serial port.



6. Configure the serial port settings so that they match the settings on your device. For example, if your device is set for 9600bps, odd parity, and XON/XOFF flow control, you must change the settings on the Serial Device Server to these settings.

   If you are using RS-422 or RS-485 (SX-510 only), select 422, 485, or 485HD (half-duplex) as the mode.

   Click the ***Submit*** button at the bottom of the window (you may need to scroll) to save your changes.

   When you have finished with all your configuration changes, you must restart the Serial Device Server for these changes to take effect.

   You can skip the remainder of this chapter.

Using the Internal Command Console to Configure the Serial Device Server

You may skip this section if you have completely configured the SX-500 using ExtendView or the SX-500 Internal Web Pages.

The Internal Command Console is a command line oriented method for configuring the Serial Device Server. It provides more comprehensive capabilities than either ExtendView or the Internal Web Pages, but is not as easy to use. Advanced users may prefer to use this method because it is concise, fast, and powerful.

To use the Internal Command Console:

1. To access the Internal Command Console, enter the following command from the Windows Command Prompt (MS-DOS Prompt), Mac OS X Terminal Utility, or UNIX/Linux command line:

telnet *aa.bb.cc.dd*

where aa.bb.cc.dd is the IP address of the Serial Device Server (for example, *telnet 192.168.5.6*).

2. Press <ENTER> and then enter the password *access* at the # prompt. Press <ENTER> at the *Enter Username*> prompt. When you see the *Local*> prompt, you can enter console commands.

3. If you used the default 192.0.0.192 IP address to connect to the Serial Device Server, you MUST change it to a new valid IP address. If necessary, you must also change the Subnet Mask and Router (Gateway). The commands are as follows:

   SET IP ADDRESS *aa.bb.cc.dd*
   SET IP SUBNET *aa.bb.cc.dd*
   SET IP ROUTER *aa.bb.cc.dd*

   where *aa.bb.cc.dd* is the IP address of the Serial Device Server. You can use the command SHOW IP to verify the IP address settings.

4. Enter the basic wireless settings as follows:

SET NW SSID <name>	*[where <name> is the SSID for your network]*
SET NW MODE <mode>	*[where mode is INFRASTRUCTURE or AD-HOC]*
SET NW CHANNEL n	*[where n is 1 to 11; this is only required for AD-HOC MODE]*

5. Use the appropriate SET NW command to set wireless encryption mode and authentication type (check with your network administrator for the proper settings if you do not know them):

SET NW ENC <mode>	*[sets encryption mode, where <mode> is WPA, WPA2, 64, 128, or WPA2-WPA]*
SET NW AUTHTYPE <type>	*[sets authentication type, where <type> is OPEN, SHARED, TTLS, PEAP, WPA-PSK, LEAP, TLS, or FAST].*

   For WPA2-PSK or WPA, enter the command:

SET NW WPAPSK <psk>	*[sets pre-shared key for WPA2 or WPA*, *where <psk> is the key]*
SET NW WPAGROUP <state>	*[enables or disables WPA group key mode, where <state> is ENABLED or DISABLED; default is DISABLED]*

   For WEP (WEP64 or WEP128), use the following commands:

SET NW KEYVAL <key>	*[Sets WEP key, where <key> is 10 hex characters for WEP64 or 26 hex characters for WEP128]*
SET NW KEY# *n*	*[sets the number of the WEP key that will be used as the transmit key, where n=1 to 4; default value is 1]*

   Configuring 802.1X EAP authentication can be complex. Please refer to Appendix A and/or Appendix B for details of the required commands.

6. To set the serial port, enter the following commands:

SET PORT S1 SPEED <baudrate>	*[where <baudrate> is 300 to 921600]*
SET PORT S1 PARITY <parity>	*[where <parity> is ODD, EVEN, MARK, or SPACE]*
SET PORT S1 SIZE <databits>	*[where <databits> is 7 or 8]*
SET PORT S1 FLOW <flowcontrol>	*[where <flowcontrol> is NONE, XON/XOFF, CTS, or DSR]*
SET PORT S1 MODE <line mode>	*[where <line mode> is 232, 422, 485, or 485HD; this command only applies to the SX-510]*

   The console commands are summarized in Appendix B of this manual.

7. When you have finished entering commands type:

   INIT
   EXIT

   These commands will save the configuration and restart the unit. You are now ready to use the Serial Device Server.

IMPORTANT: The console command EXIT must always be used in order to save the changes you made with the internal command Console.

8. Note that you can also access the Internal Command Console in the following ways:

   - *Internal Web Pages.* Use a web browser to connect to the Serial Device Server internal web pages as described earlier in this chapter. After you have logged in, click ***Admin*** on the left side of the screen, and then click ***Console***. You can now enter console commands (you must click ***Enter*** after each command).

   - *ExtendView.* Select the desired Serial Device Server from the ExtendView main menu. Click ***Tools*** on the menu bar, and then click ***Telnet Session***. Press <ENTER> and then enter the password *access* at the # prompt. Press <ENTER> at the *Enter Username>* prompt and you are now ready to enter console commands.

Chapter 4
Using the Serial Device Server with Your Application

The Serial Device Server includes a number of capabilities that enable it to be used in a wide range of applications. These capabilities include:

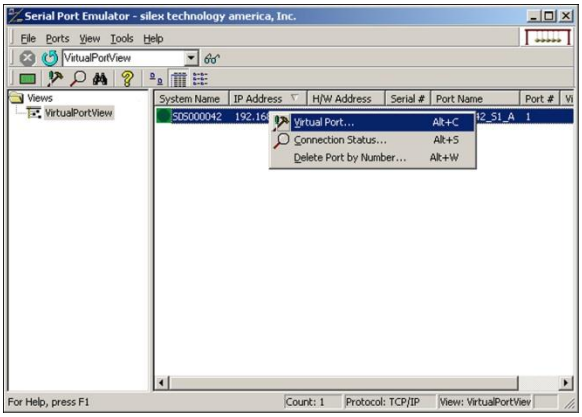
1. Serial Port Emulator (SPE) software
2. Raw TCP connection
3. RFC2217
4. ECable Mode
5. Print Server mode
6. FTP
7. Console mode switching
8. AT commands
9. SNMP traps and Email alerts

These methods are described in the following sections.

Serial Port Emulator

The Serial Port Emulator (SPE) software emulates a standard Windows COM port. That is, it creates a virtual COM port that functions exactly like the Windows COM1 and COM2 serial ports, except that the I/O actually goes out over the Ethernet or WLAN to the Serial Device Server and to the serial device that is connected to the Serial Device Server. As a result, any application program that uses a standard Windows COM port can also use the Serial Port Emulator. The SPE is therefore especially useful if you have existing programs that use Windows COM ports.

The SPE software is a component on the CD-ROM that is included with the Serial Device Server, or it can be downloaded from the Silex website. To install it, double click on the installer icon and follow the installation instructions. When the installation is complete, you can run the SPE software by clicking ***Start -> Programs -> Silex technology -> Serial Port Emulator -> Serial Port Emulator.***



After the Serial Port Emulator software has started, you will see a list of all the configured Serial Device Servers on the network. Right click on the name of the Serial Device Server that you want the virtual COM port to connect to (the default name is SLX*xxxxxx*, where *xxxxxx* is the last six digits of the Serial Device Server MAC address), and then click ***Virtual Port***. You will be asked to select the name of the virtual COM port (for example, COM3).



Click ***OK*** after you have selected the name, and you now ready to use the virtual COM port.

Using virtual COM port is identical to using a normal COM port. For example, if you configure a virtual COM port called COM3, this port will show up as one of the available serial ports when you use the Windows HyperTerminal Accessory program.

Raw TCP connection

You can communicate directly from your application program to the Serial Device Server using a raw TCP connection. This is done by opening a TCP port on the Serial Device Server and then sending and receiving data to this port via a socket or equivalent API. This method is more efficient than using the Serial Port Emulator, and does not require any additional software to be installed on your computer.

If you are using a raw TCP connection, the default TCP port number (you can use any or all of these port numbers) for normal connections. If you want to be able to access your device's modem control signals from your computer system, then the TCP port number is 9200 (this enables RFC 2217 support). You can change the port number, if desired, by modifying one of the Serial Device Server services. To change the TCP port number:

1. Connect to the Serial Device Server with a web browser (see chapter 3 for instructions on doing this);
2. After you have logged in, click ***I/O Services*** on the left side of the page.
3. Click on the service name that you want to change (any one of the services is OK, provided that you are not using the existing TCP port number of that service for a different application).
4. Change the ***Raw TCP Port*** to the desired number (must be greater than 1023).
5. Click ***Submit*** to save your change.

You can test this connection by using the TELNET utility from the Windows Command Prompt (MS-DOS prompt), Mac OS X Terminal Utility, or UNIX/Linux command line as follows:

telnet *ipaddress portnumber*

where i*paddress* is the IP address of the Serial Device Server and *portnumber* is the Serial Device Server TCP port number. For example:

telnet 192.168.5.53 9100

In this example, if you have a serial printer or other device capable of displaying ASCII characters connected to the Serial Device Server serial port, then every character you type should be printed on that serial device (buffered serial devices may need you to type a control character such as a formfeed (CONTROL-L) before the characters are printed).

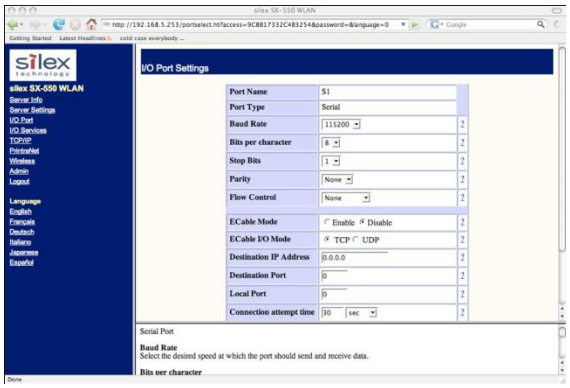
RFC 2217 Remote Modem Control Support

RFC 2217 allows you to access your device's modem control signals over the network. It is especially useful for migrating applications that use modem controls from a direct serial connection to a serial device server network connection. You can utilize RFC 2217 from the Silex Serial Port Emulator software (see below), or by connecting to TCP port 9200 from your application program.

ECable Mode

Normally, it is up the computer to initiate a connection to the Serial Device Server. For some applications, it is desirable for the Serial Device Server to initiate the connection to the computer. The Serial Device Server supports this capability through its ECable feature.

To set ECable mode, use a web browser to access the Serial Device Server internal web pages (see chapter 3 for instructions on using the internal web pages). After you have logged in, click I/O port on the left side of the screen.



You can now enable ECable mode and set the required parameters.

1. Enable ECable mode by clicking the radio button.
2. Enter the address (Destination Address) of the computer or other device that will be communicating with the Serial Device Server)
3. Enter the TCP port number (Destination Port) used by the destination device for communicating with the Serial Device Server (must be greater 1023).
4. If desired, change the ECable Connection Attempt Time. This specifies the time interval between connection attempts. For example, by default the Serial Device Server will try once every 30 seconds to make a connection to the destination device; if it fails to make this connection, it will wait 30 seconds before attempting again. Changing this interval will reduce or increase the amount of network traffic.
5. It is also possible to use UDP instead of TCP for communicating to and from the Serial Device Server. If you wish to use UDP, then:
    a. Select UDP as ECable I/O Mode.

b. Enter the UDP port number (Destination Port) used by the destination device to communicate with the Serial Device Server. This number must be a valid port on the destination device (check the documentation for that device to determine the valid port numbers).
c. Enter the UDP port number (Local Port) used by the Serial Device Server to communicate with the destination device. This number must be greater than 1023, but is otherwise arbitrary.

NOTE: ECable mode cannot be used in conjunction with the Serial Port Emulator software.

Print Server Mode

You can use the Serial Device Server as a standard TCP/IP print server, which is very useful if you are connecting the Serial Device Server to a serial printer. The Serial Device Server supports the following standards:

- *lpr/lpd*. This is one of the most popular ways to print on a TCP/IP network. Check your computer's documentation to determine how to set up an lpr print queue. Usually this simply involves specifying the IP address of the Serial Device Server as the printer's address or host name. Some implementations require a queue name; this name is the name of any of the Serial Device Server services. To see the names of the Serial Device Server services, connect to the Serial Device Server with a web browser (see chapter 3 for instructions on doing this); after you have logged in, click I/O Services on the left side of the page.

- *Port 9100*. This method is used to set up a Windows Standard TCP/IP port or for compatibility with software that supports the HP JetDirect Print Server (for example, HP Web JetAdmin). To use this capability on Windows with the *Add Printer Wizard*, specify that you want to use a ***Local printer attached to this computer*** (not a network printer), and then select ***Create a new port***, specifying ***Standard TCP/IP Port*** as the type of port.

  It is also possible to change the TCP port number from the default 9100 for compatibility with other printer manufacturer's software. To do this, refer to the instructions in the *Raw TCP Connection* section of this chapter.

FTP

The Serial Device Server supports FTP binary or ASCII communications. This can be used, for example, to send the contents of a file from a PC to a device connected to the Serial Device Server using the FTP protocol. To use FTP, simply enter the standard FTP command from your PC with the IP address of the Serial Device Server (for example, ftp 192.168.5.50). When the connection is made, enter any username and password. You can then use the standard FTP *put* command to send the file from the PC to the device connected to the serial port on the Serial Device Server.

Console Mode Switching

The Serial Device Server allows you to dynamically switch the operation of the serial port from normal mode to console mode. This allows your device to control the operation of the Serial Device Server by sending console commands (see chapter 6 and Appendix B for a description of the console commands). Note that console mode can only be entered when there is no connection to a remote host.

To switch the serial port to console mode, you must first define a console string. When the Serial Device Server receives this string on the serial port, it will automatically switch the port to console mode. To define the console string, use a web browser to access the Serial Device Server internal web pages.

After you log in, ***click I/O Port,*** and then select the desired port (S1 for the serial port). When you get the ***I/O Port Settings*** page, enter any desired character string (for example, xyz) as the ***Console Mode String***. Click ***Submit*** to save your string, and then restart the Serial Device Server to make the change take effect.

Alternatively, you can define the console mode string using the console command from TELNET as shown in the following example:

```
SET PORT S1 CONSTR xyz
```

Once you are connected in console mode, you can send any of the console commands listed in Chapter 5. Be sure to terminate each console command with a carriage return (ASCII 13) or linefeed (ASCII 10) character.

When you are finished using the console, you can return to the normal port operation by sending the command EXIT followed by a return or linefeed character.

AT Commands

The Serial Device Server allows you to control the serial port using standard AT modem commands. This allows you, for instance, to initiate connections and to switch between console mode and data mode by sending the appropriate commands. These capabilities are similar to the console mode switching described in the previous section, but have the following advantages:

- Your device can initiate a network connection
- Operation is compatible with software that uses the AT command set

The drawback, however, is that there is a slight delay when switching from data mode to AT command mode.

To use the AT commands, you must first enable this capability using the ***I/O Port Settings*** internal web page for the serial port (S1). Change the ***Port Filter*** setting to AT in order to enable AT mode on that port and press the ***Submit*** button to save the change. You must restart the Serial Device Server to make the change take effect.

You can also use the console to enable the AT capabilities. For example, the command

```
SET PORT S1 FILTER AT
```

enables AT capabilities on the serial port.

Note: If you use the AT commands on the serial port, you cannot use SNMP traps or Email alerts for that port.

The AT commands are described in detail in Chapter 5.

SNMP Traps and Email Alerts

The Serial Device Server allows the user to define various alert conditions based on data received by the serial port. For example, you could cause an alert to occur if a certain user-defined string of characters is received on the serial port. When an alert occurs, it can be sent as an SNMP trap and/or as an Email message.

Details on using these capabilities can be found in Chapter 5.

Chapter 5
Advanced Configuration

The Serial Device Server Serial Device Server is equipped with a default configuration that works with most serial-to-Ethernet connections. You can modify the settings to suit your installation requirements.

The web browser interface is the recommended method for setting advanced configuration parameters (some of the advanced configuration parameters are not accessible via ExtendView). However, regardless of the method to access the configuration parameters, the method for modifying the parameters is virtually identical.

Factory Default Settings

Table 3 displays the configuration parameter descriptions and settings with the default settings indicated in a separate column.

Table 3 Factory Default Settings

Parameter	Description	Settings	Default Setting
Character	Bits per character	7, 8	8
Flow	Flow control	None, XON, XOFF, CTS/RTS	None
Parity	Parity	None, Even, Odd, Mark, Space	None
Speed	Baud rate of bits per second	300, 600,1200, 2400, 3600, 4800, 7200, 9600, 14400,19200, 38400, 57600, 76800, 115200, 230400, 460800, 921600	115200
Stop	Stop bits per character	1, 2	1
Mode	Line mode or serial port protocol	232 (SX-500); 232, 422, 485, 485HD (SX-510)	232
Ecable	ECable mode for TCP connections	Enable, Disable	Disable
Ecaddr	ECable destination IP address	Set by user	N/A

Parameter	Description	Settings	Default Setting
Econn	ECable connection attempt time	1-255 seconds	30 seconds
Ecport	ECable destination TCP port number	Set by user	N/A
Eclport	ECable destination local IP port number (required for E-Cable UDP mode only)	Set by user	N/A
Ectmmsec	Cable connection time resolution	Enable, Disable	Disable
Ecudp	ECable UDP mode	Enable, Disable	Disable

Restoring Factory Default Settings

The factory default settings can be restored at any time To do this, hold down the Reset pushbutton for more than five seconds.

Modifying TCP/IP Settings

You can modify the TCP/IP settings using ExtendView, the web browser interface or the Serial Device Server Serial Device Server's internal configuration console.

To modify TCP/IP settings:

1. Using ExtendView, click the **TCP/IP** tab. The TCP/IP window displays.

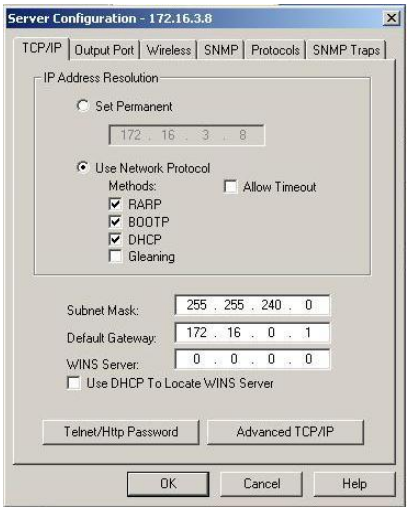


Figure 2 TCP/IP Window

2. Verify the settings, as defined in Table 4.

Table 4 TCP/IP Settings

Parameter	Setting
IP Address Resolution	Sets the exchanges among network interfaces connected to an Ethernet media segment and maps IP address to Ethernet addresses, Media Access Control (MAC) addresses and hardware addresses. The **Set Permanent** radio button sets the IP address permanent. The IP address must follow the format XXX.XXX.XXX.XXX, where each XXX is a number between 0 and 255. The Use Network Protocol Select radio button determines which IP address at power up.
Subnet Mask	Sets the address of the subnet mask The subnet mask must follow the format XXX.XXX.XXX.XXX, where each XXX is a number between 0 and 255. The default subnet mask is 0.0.0.0. The server interprets a subnet mask of 0.0.0.0 or 255.255.255.255 as no subnet mask specified.
Default Gateway	Sets the default gateway, if your network is attached to other networks
WINS Server	Sets the Windows Internet Naming Service (WINS) address. Values are set by user.
Use DHCP to Locate WINS Server	Uses the automatic location feature in ExtendView to locate the WINS servers.

3. To change the Telnet/HTTP password, click Telnet/HTTP Password. The Change Password window displays.



Figure 3 Change Password Window

Type the new password in the **New Password** field, then in the **Verify Password** field.

Click **OK** to change the password or click **Cancel** to exit.

4. Click **Advanced TCP/IP**. The Advanced TCP/IP Configuration window displays.

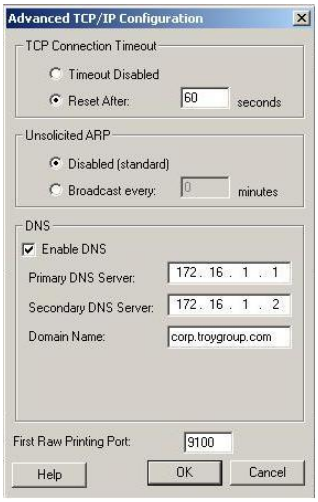


Figure 4 Advanced TCP/IP Configuration Window

5. Configure the settings, as defined in Table 5.

Table 5 TCP/IP Configuration Settings

Parameter	Setting
TCP Connection Timeout	Sets the timeout and reset values for the TCP connections
Unsolicited ARP	Blocks or broadcasts unsolicited ARP
DNS	Sets the DNS addresses

6. To accept changes, click **OK**.

   To cancel, click **Cancel**.

   For additional help, click **Help**.

NOTE: You can configure the same settings using the Web Page configuration. Simply log in using the Serial Device Server IP address and select ***TCP/IP***. For the changes to become effective, click the ***Submi***t button, then reset the Serial Device Server.

Configuring SNMP

The Serial Device Server Serial Device Server contains a Simple Network Management Protocol (SNMP) agent that collects and stores management information for network managers using standard SNMP commands. The management information is referenced as a hierarchically organized database called a Management Information Base (MIB).

To prevent naming conflicts, all of the manageable features of all products from all vendors are arranged in a single tree structure. Each vendor of SNMP equipment has an exclusive section of the MIB Tree.

Each branch of the MIB Tree has a number and name. The path from the top of the tree down to the point of interest forms the name of that point. A name created in this way is known as an Object ID or OID.

Table 6 describes the messages used to communicate between the network manager and the SNMP agent, as defined in RFC 1157. Each SNMP message must contain a Community Name, which is used like a password. The default Community name for the Serial Device Server Serial Device Server is PUBLIC.

Table 6 SNMP Commands

Command	Description
GET	Retrieves management information for a specific managed object contained in the agent. The GET message must contain the OID for the specified object. The response is a GET-RESPONSE message containing either the current value of the requested object, or an indication as to why the request failed.
GET NEXT	Retrieves management information from a non-specific managed object. The GET NEXT contains either a complete OID or a fragment of an OID. The response is a GET-RESPONSE message containing either the OID and data of the item immediately right of the specified OID in the tree or an indication as to why the request failed.
GET RESPONSE	This is the information sent back from the unit in response to the GET, GET NEXT command.
SET	Requests a change to the value of a specified object. The response is a GET-RESPONSE message with either an indication that the requested change had been made or with an indication as to why the request failed.
TRAP	Sends a one-way notification from the agent to the manager that a significant event has occurred. This is the only message initiated by the SNMP agent.

To configure the SNMP server settings:

7. Log into the Serial Device Server internal web pages using a standard web browser. Click ***Server Settings*** to access the screen shown in Figure 10. You can then enter the relevant SNMP information for your network.

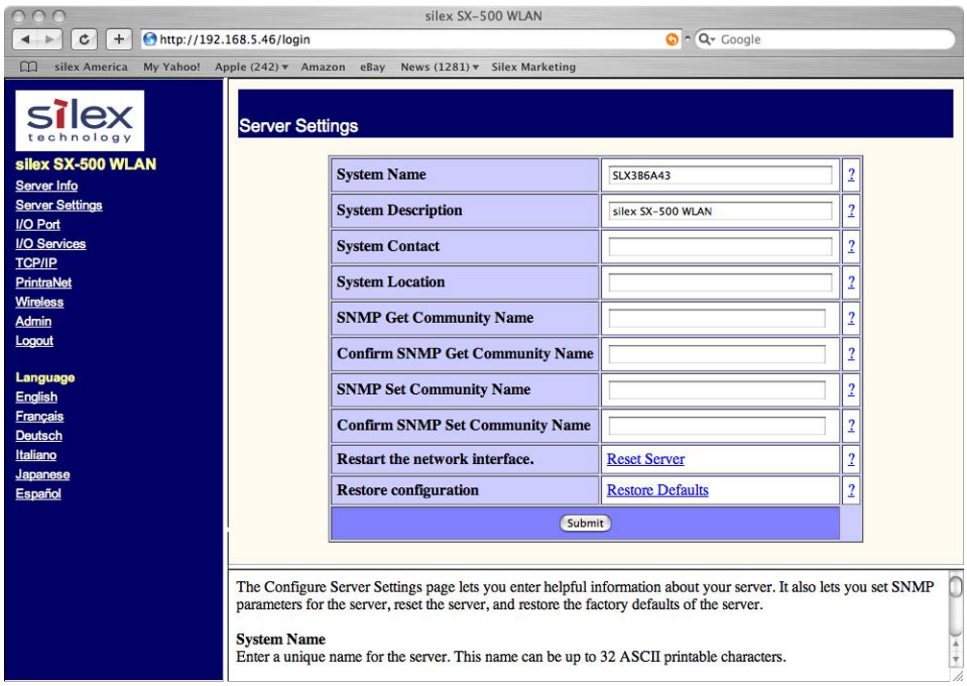


Figure 5 SNMP Configuration

8. Click the ***Submit*** button to save the changes. You must then restart the Serial Device Server to make the changes take effect.

Configuring Serial Port Monitor Alert and Trap Configuration

The Serial Device Server can be configured to scan and compare the data received on the serial port to user-defined strings. A match with a string can be a source for SNMP traps and/or email alerts.

The match strings and corresponding email or web page message strings are configured from the Internal Configuration Console interface (accessible via TELNET).

Table 7 describes the Monitor Alert and Trap Configuration Commands.

Table 7 Port Monitor Alert Commands

Command	Description
SHOW PORT S1 TRIGMON	Shows strings and index numbers being monitored
SET PORT S1 TRIGMON <*trig* #> <string>	Assigns a string to be monitored on the serial port
Example: `Local> show port s1 trigmon` `Index # Monitor String` `------ --------------` `Local> set port s1 trigmon 0 trigger on seeing this string` `Local> show port s1 trigmon` `Index # Monitor String` `------ --------------` `0: trigger on seeing this string`	
SHOW PORT S1 TRIGXMT	Shows email or web page strings associated with TRIGMON index numbers
SET PORT S1 TRIGXMT <index #> <string> Index # = 0 to 7	Assigns email or web page string to specified TRIGMON index number
Example:	

```
Local> show port s1 trigxmt

Index #   Xmit String
------    ---------------
  0:      xmit string 0     <<< default msg string

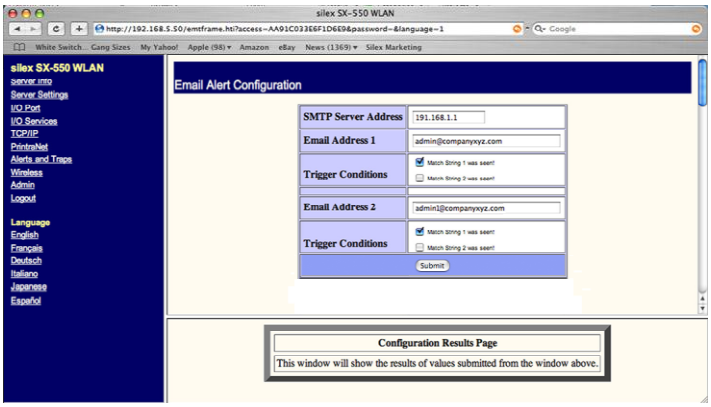
Local> set port s1 trigxmt 0 The trigger string was seen!

Local> show port s1 trigxmt

Index #   Xmit String
------    ---------------
  0:      The trigger string was seen!
```

Setting up Email Alerts and SNMP Traps

After you have created the Serial Port alerts and traps, you can the use the Serial Device Server internal web pages to set up the recipient Email addresses and/or computer systems. After you have logged into the internal web pages, click ***Alerts and Traps*** on the left side of the screen and select either ***Email Alerts*** or ***SNMP IP Traps***. (note that the Alerts and Traps menu item will not appear unless you have previously configured match strings using the Internal Configuration Console as described in the previous section). The Email Alert Configuration screen is shown below.



This screen allows you to define up to eight Email addresses that can receive alert information. Each address can receive any combination of the alerts that you have defined previously. You must enter the IP address of your SMTP server and the Email address(es) where you want the alerts to go. For example, in the above screen, the user has configured two serial port match strings. He has decided to send an alert to the mail address *admin@companyxyz.com* if the first match string is seen on the serial port. If desired, he could create up to seven more Email addresses that could each receive any combination of these alerts.

The SNMP Trap Configuration page works exactly the same way as the Email Alert Configuration page, except that you enter the Trap Community plus the IP address and port of the destination computer(s) instead of the Email information. Up to eight separate IP addresses can be configured with any combination of the alerts that you have defined. Note that you may also use the console command SET IP TRAP n TRIGGER console command (see appendix B) to set up the traps.

When you have finished configuring the alerts, be sure to click the ***Submit*** button to save the settings. You will also need to restart the Serial Device Server in order for the changes to take effect.

Using AT Modem Commands

The Serial Device Server firmware has an optional data filter for configuring using AT style modem commands with the serial port. This feature allows devices with an existing AT command interface to configure the unit, if the AT commands can be properly modified. You must be familiar with the general operation of AT commands. Note that AT command processing is not enabled by default. Use the command SET PORT S1 FILTER AT to enable this feature.

All commands begin with AT and are terminated by a new line unless noted below. While standard AT commands are defined to be 40 characters or less (not including the AT), the server accepts commands of up to 80 characters.

Standard AT Commands Supported

The Serial Device Server recognizes a subset of the standard AT command set. The data channel must be in the command mode for commands to be recognized. The data channel will be in command mode upon power up or reset.

There are two operating modes for the unit when the AT command option is enabled. In command mode, data received from the serial port is passed to the AT command processor, and responses are returned to the serial port. No data is sent to any network application, and any data received from the network is ignored. In data mode, data from the serial port passes to the network application, and vice versa. This is equivalent to the normal serial port operating mode without the AT command option.

Table 8 describes the AT Commands. Table 9 details the Extended AT Commands that allow the configuration of the network server operating parameters. Any AT command received, except the listed commands, are acknowledged with OK status. This allows existing modem applications to transmit commands without causing an error. These include AT<X>n, but not currently AT&<X>n, AT%<X>n, AT\<X>n, where <X> is a letter.

Table 8 AT Commands

Parameter	Command	Description
Enter Command mode	<delay>+++<delay>	If the string +++ is seen in data mode, with no characters sent for 1 second before or after, then command mode is entered.

Parameter	Command	Description
Initiate Connection Command	ATD <destination>	Standard modem dialing command, redefined to initiate an internet connection to a remote computer. Indicates the IP address of the target, and optionally the TCP port number to use for connection. The T or P option (ATDT or ATDP) can be present and has no effect. If present, the IP address must be exactly 12 decimal digits with 3 for each byte of the address. If no IP address is given, then the ECable destination address defined for the port is used. If the destination TCP port is defined, it is separated from the IP address by a '#' character, and is 1 to 5 decimal digits. If TCP port is defined, the ECable destination port defined for the serial port is used. If the destination port is 0, the standard Telnet port (23) is used. If the destination string ends with a semicolon, the server remains in the command mode, not the data mode, once a connection is made. In command mode data is not passed from the remote computer, so data could be lost if the unit stays in command mode. If the connection cannot be attempted, NO CARRIER status is returned. If the connection attempt fails, NO ANSWER status is returned. If the connection succeeds, CONNECT status is returned.
Echo control	ATEn	If n=0, commands are not echoed. If n=1, subsequent commands will be echoed. The default, upon unit reset, is for no echo (ATE0).
Disconnect	ATHn	If n=0, any connection to a remote host is dropped. Other value of n is ignored.
Return to data mode	ATOn	Exits command mode and places the serial port in the data mode. All subsequent data is sent to the network application, if connected, until an enter command mode sequence is received. Any value of n is ignored, if present.
Quiet mode	ATQn	If n = 1, no result codes are returned. If n = 0, result codes are returned to the local device. 0 is the reset default value.
Verbose mode	ATVn	If n = 0 and not in quiet mode, result codes are returned in numerical form. If n = 1, results are returned as text. 1 is the reset default value.

Table 9 Extended AT Commands

Parameter	Command	Description
Console pass through	AT#C<string>	Passes the string to the server configuration console. The string can be any valid console command. Refer to your server documentation for console commands available on your unit. Since this command does not follow the normal AT command format of <command><number>, it must be the last command on the line unless the next command is a '#' command. All characters up to the end of line or a '# will be considered part of the console command. If console quiet mode is not is enabled, then the response will be the standard console task response. Example: `AT#Cset nw ssid silex#Csave`
Console Quiet mode	AT#Qn	If n = 0, a response to a #C command is given. If n = 1, the response is not provided. The default after reset is 1.

Response Codes

Table 10 details the response codes for codes other than #C commands.

Table 10 Response Codes

Numeric Code	Description
0	OK
2	No Carrier
4	Error
5	Connect
8	No Answer

Using ExtendView for Bulk Configuration

The ExtendView Utility has a powerful bulk configuration capability that allows you download configuration information to multiple Serial Device Servers simultaneously. This can save you a significant amount of time compared to configuring each Serial Device Server individually. To use this capability:

1. From the ExtendView menu bar, select ***View*** and then ***Multi-Select Mode***.
2. The display will change slightly so that there is checkbox by each of the Serial Device Servers listed on the main screen. Click the boxes next to each of the Serial Device Servers that you wish to configure.
3. From the ExtendView menu bar, select ***Server*** and then ***Multiple Configuration***. The Configure Multiple Devices window will appear. This Window lets you set parameters such as subnet mask, router address, basic wireless security, and much more. When you have set all of the desired parameters, click OK and the parameters will be downloaded into the selected Serial Device Servers.

Chapter 6
Troubleshooting

If you have experience problems with the Serial Device Server, please check the following troubleshooting steps:

1. Make sure that you are getting power to the Serial Device Server. The orange LED should be on solid if the proper power is being received. If it is not on, check the power supply connections, and if possible, try a different Silex Serial Device Server power supply.

2. Make sure that you have a valid network connection.

    a. Make sure that your network is operating properly (that is, other devices should be able to communicate using the same hub, switch, or access point that the Serial Device Server is connected to).

    b. If you are using hardwired Ethernet, either the yellow LED (for 10Base-T) or the green LED (for 100Base-T) should be lit or blinking. If they are not, make sure that the cable is properly connected, and if possible, try a different Ethernet cable.

    c. If you are using a wireless connection, both the yellow LED and green LED should be lit or blinking. If they are not, double check your wireless settings. The SSID and security parameters must exactly match the requirements of the access point in order for the Serial Device Server to communicate on an infrastructure wireless network. If you are using Ad-Hoc mode, the Serial Device Server must have exactly the same SSID, security parameters, and RF channel as the other wireless device(s) on the network.

    d. Make sure that you have a valid IP address, subnet mask and router address (check with your network administrator to make sure that you have the correct information). You can check to see if the IP address information is correctly set by using the ExtendView utility, by printing a test page (press the RESET pushbutton to send a test page to a printer or terminal connected to the serial port) or by using the PING command from a computer system connected to the network.

3. If you have a valid network connection and IP address, but you cannot communicate with your serial device, then:

    a. Make sure that the settings of the serial port on your device exactly match the settings of the serial port of the Serial Device Server. For example, if your device is set for 9600bps, 8-bit characters, no parity, and RTS/CTS flow control, the Serial Device Server must also have these exact same settings.

b. If you are using RS-422 or RS-485, make sure that you have set the Serial Device Server's serial port line mode as described in Chapter 3.

c. Make sure that have a good cable connection between your serial device and the Serial Device Server. If possible, try a different cable.

d. Make sure that the cable pinouts are correct. In order to communicate properly, the transmit data line on the Serial Device Server must be connected to the receive data line on your serial device, and the receive data line on the Serial Device Server must be connected to the transmit data line on your serial device. Modem signals, if any, must also be connected so that input signals are connected to output signals and vice-versa. Refer to the cable diagrams in Chapter 2 of this manual.

e. Try printing a test page (if your serial device is not capable of directly displaying ASCII character output from the Serial Device Server's serial port, then disconnect the device and connect a serial printer or terminal to the Serial Device Server). If the test page prints OK, then the serial port on the Serial Device Server is working properly. If it does not print, then double check steps 3a, 3b, and 3c.

If none of the above steps solves your problem, then check the Support and Downloads section of the Silex website (www.silexamerica.com). You can also contact Silex support by phone, Email, or fax as follows:

Hours of Operation: Monday-Friday 8:00am-5:00pm MST
Phone: **US toll free:** (866) 765-8761, **International:** 1 (801) 748 - 1199, **Fax:** 1 (801) 748-0730
Email: Tech support: support@silexamerica.com,

Be sure to have the following information ready when you call Silex support:

1. Model number and serial number of the Serial Device Server
2. Firmware version of the Serial Device Server
3. Your hardware and software environment:
    a. Your CPU and operating system
    b. Type of device that you are connecting to the Serial Device Server
    c. Wireless/wired networking environment (for example, access point manufacturer/model, wireless security, routers, etc.)
4. Description of the problem

Chapter 7
Product Specifications

Table 11 Product Specifications

Component	Specifications
Model	SX-500 Serial Device Server, SX-510 Serial Device Server
Processor	Cavium NITROX Soho CN210
RAM Memory	16 Mbytes SDRAM.
Processor Speed	167 MHz
Interfaces Supported	Serial: RS-232-C; SX-510 models also support RS-422 and RS-485 (full and half-duplex) Ethernet: 10/100BaseT Wireless: 802.11b/g (SX-500); 802.11a/b/g (SX-510)
Dimensions	SX-500: 125.73 x 75.11 x 24.08 mm (4.95 x 2.957 x 0.948 inches), not including mounting brackets or connectors SX-510: 110.58 x 7.26 x 25.52 mm (4.35 x3.08 x 1.00 inches), not including connectors
Temperature	0 to 50 degrees C (operating); -20 to 70 degrees C (storage); maximum 20 degrees C change per hour
Humidity	10% to 90% non-condensing
Altitude	3.1km (operating); 9km (storage)
Electrical	Wired models: 500mA@+5VDC Wireless models: 800mA@+5VDC Power provide through external AC adapter (included) or via pin 9 on the 9-pin serial port connector

Table 12 Radio Performance Specifications

Parameter	Specifications
Radio Emission Type	Complies with IEEE 802.11a, b, g, h and j Direct Sequence Spread Spectrum (DSSS) physical layer. (802.11a is supported on SX-510 only)
Operating Frequency	2.412 GHz ~ 2.484 GHz ISM band 5.15 GHz ~ 5.25 GHz ISM band 5.725 GHz ~ 5.825 GHz ISM band (North America only)
Data Modulation Type	Orthogonal Frequency Division Multiplexing (OFDM) Complementary Code Keying (CCK) Differential Quadrature Phase Shift Keying (DQPSK) Differential Binary Phase Shift Keying (DBPSK)
Channel Number	IEEE 802.11b and g: Channels 1 to 11 and 12 to 14 IEEE 802.11a: Channels 36, 40, 44, 48, 149, 153, 157 and 161 (802.11a is supported on SX-510 only)
Data Rate	54 Mbps with fallback rates of 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, and 1 Mbps
Security	Encryption: WEP 64/128 bits, WPA (TKIP), WPA2 (AES) Authentication: WEP Open System and Shared Key; WPA-PSK, WPA2-PSK, 802.1X with LEAP, FAST, TLS, TTLS, and PEAP
Media Access Protocol	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with ACK architecture, 32 bits MAC-layer.
Antenna Connector Type	2 SMT ultra-miniature coaxial connectors
Operating Voltage	5 VDC ± 5%, 600mA (wireless), 500mA (wired)
Bus Interface	Proprietary 70-Pin
Antenna Port Impedance	50 ohm

TCP Port Connections

The Serial Device Server supports port connections over TCP/IP using raw TCP ports only. Table 13 describes the TCP ports allocations.

Table 13 TCP Port Connections

Port	Destination Device
3001	RS-232
9100	RS-232
9200	RFC 2217

Appendix A
Advanced Security Configuration

There are numerous possible security settings. It is therefore important that you verify the appropriate settings with your network administrator. If you enter the settings incorrectly, the Serial Device Server will not be able to communicate on your network. The following table summarizes the wireless settings required for each encryption mode and authentication type:

		Authentication Type							
		Open System	Shared-Key	PSK	802.1x				
					TTLS	LEAP	PEAP	TLS	EAP-FAST
Encryption Mode	Disable	(OK)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	64-Bit WEP	1	1	N/A	N/A	N/A	N/A	N/A	N/A
	128-Bit WEP	1	1	N/A	N/A	N/A	N/A	N/A	N/A
	WPA	N/A	N/A	2, 3	4, 7	4	4, 5	4, 5, 6	4
	WPA2	N/A	N/A	2, 3	4, 7	4	4, 5	4, 5, 6	4
	WPA2-WPA	N/A	N/A	2, 3	4, 7	4	4, 5	4, 5, 6	4
	Dynamic WEP	N/A	N/A	N/A	4, 7	4	4, 5	4, 5, 6	4
	Wired Ethernet Network	N/A	N/A	N/A	4, 7	N/A	4, 5	N/A	4

Basic Configuration Parameters
1. 64/128Bit WEP Key
2. WPA-PSK
3. WPA Group Key

802.1X Configuration Parameters
4. User ID and Password
5. Authentication Server Certificate
6. Private Key
7. Authentication Protocol

To use the above table, select the encryption mode and authentication type you are using. For example, if you are using WPA2 with PSK authentication, you would need to set the WPA-PSK pre-shared key and enable or disable the WPA Group Key. Likewise, if you are using WPA2 with 802.1X TLS authentication, you would need to enter a User ID and Password, an Authentication Certificate, and a Private Key.

The following is a description of the authentication settings used by the Serial Device Server:

Encryption Mode (Wireless Security Only)
The possible Serial Device Server wireless encryption modes include:

- *64 and 128 bit WEP.* These are available for basic WIFI compatibility. Because of known security issues, WEP should be avoided if possible.
- *Dynamic WEP*. Dynamic WEP uses WEP encryption with an 802.1X EAP authentication method. It is not necessary to set keys with this method, because they are automatically assigned.
- *WPA2*. WPA2 is the latest and strongest wireless security standard. It uses CCMP encryption. Like WPA, it can be used either with a pre-shared key or with 802.1X authentication.
- *Wi-Fi Protected Access (WPA*). WPA uses TKIP encryption, and can be used with either a pre-shared key (PSK) or with 802.1X authentication.
- *WPA2-WPA*. This mode combines the capabilities of WPA2 and WPA by using CCMP for pairwise encryption, but allowing TKIP for group encryption.

To set the encryption mode, select the desired mode from the pull down menu on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW ENC <mode>, where <mode> is DISABLE, 64, 128, WPA, OR WPA2.

Note that the encryption mode only applies to wireless networks, so it is not necessary to set this mode if you are using a wired Ethernet network.

Key Selection (Wireless Security Only)
This parameter selects which of the four possible WEP keys will be used as the transmit key (the first key is the default). Select the desired key selection from the pull down menu on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW KEY# *n*, where n is 1, 2, 3, or 4.

WEP Key Value (Wireless Security Only)
Up to four keys can be entered if you are using WEP security. The value of the keys must be entered as hexadecimal digits (up to 10 hex digits for 64 bit WEP or 26 hex digits for 128 bit WEP). Enter the desired key value(s) on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW KEYVAL <key>, where <key> is 10 hex digits for WEP64 or 26 hex digits for WEP128.

Pre-Shared Key (Wireless Security Only)
If you are using WPA2 or WPA with the PSK mode of authentication, the key value or passphrase entered here is used to initialize the session with the access point. If a key value is entered, it must be exactly 64 hex characters. A passphrase must be 8 to 63 displayable characters. Enter the desired PSK on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW WPAPSK <psk>, where <psk> is the key.

WPA Group Key (Wireless Security Only)
If the WPA Group Key mode is enabled, then group keys may be used for data link encryption (the default is disabled). Select whether to enable or disable the WPA Group Key on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW WPAGROUP <state>, where <state> is ENABLED or DISABLED.

Wireless Authentication Type (Wireless Security Only)
This parameter sets the type of authentication to be performed with the network access point (Radius authentication server), or with a peer unit in Ad Hoc mode. The Serial Device Server supports Shared Key and Open System Authentication with WEP, and PSK, TLS, TTLS, LEAP, PEAP, and EAP-FAST with WPA, WPA2, DYNAMIC WEP, and WPA2-WPA.). Select the desired wireless authentication type on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW AUTHTYPE <type>, where <type> is OPEN, SHARED, TTLS, PEAP, WPA-PSK, LEAP, TLS, or EAP-FAST.

Wired Authentication Type (Wired Ethernet Networks Only)
This parameter sets the type of authentication to be performed with a Radius authentication server on a wired Ethernet network. The Serial Device Server supports TLS, TTLS, and PEAP authentication on these types of networks. Select the desired wired authentication type on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW ETHAUTH <type>, where <type> is TTLS, TLS, PEAP, or EAP-FAST.

Authentication Attempts
This parameter sets the number of authentication attempts to make before the Serial Device Server assumes the network has no authentication. If zero (0) is entered, the Serial Device Server attempts to authenticate forever. Enter the number of authentication attempts on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW AUTHTRY *n*, where *n* is the number of attempts (default is 0).

User ID
This parameter is the logon user ID that the Serial Device Server uses to authenticate to the 802.1x-enabled network. The user ID and password must be in the authentication server database. The default user ID is 'anonymous'. Enter the user ID on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW ID <user id>, where <user id> is the user ID (the realm can included in the user id with the separator “@”).

Realm
A realm defines a grouping of users. If a realm is required for your network, it is separated from the user ID by a '@' character. Among other things, realms make it easier to segregate user groups into independently administered databases, to apply policies on a user group basis, and to establish roaming agreements. The default realm if not specified is 'anonymous'. Enter the realm on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW REALM <realm>, where <realm> is the name of the realm.

Password
This parameter is the logon password that the server uses to authenticate to the 802.1x-enabled network. The user ID and password must be in the authentication server database. The password may be a text string, or a string of hex bytes. Enter the password on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW PW <password>, where <password> is the password (default value is *anonymous*).

Authentication Protocol
This parameter determines how the server authenticates itself to the 802.1x-enabled network after an 802.1x session is established. The default is PAP; MSCHAP_V2 is the alternative protocol. Select the desired protocol on the Configure Network Security screen in the Serial Device Server internal web pages, or use the console command SET NW INAP <password>, where <password> is PAP or MSCHAP_V2.

Authentication Certificate
Authentication certificates are used by TLS and PEAP. You can manually enter the certificate information, or you can extract the Root Key and Root Key Exponent from a file on your disk. The required information is as follows:

- **Certificate Root Key** This is the authentication key used to verify the root certificate in the certificate chain provided by the authentication server. To set to null, send leave this field blank. Enter the certificate root key on the Configure Authentication Certificate page in the Serial Device Server internal web pages, or use the console command SET NW CERTKEY <value>, where <value> is the value of the key.

- **Certificate Root Key Exponent** This value must match the authentication server certificate value. The default is 65537 (x10001). Enter the certificate root key on the Configure Authentication Certificate page in the Serial Device Server internal web pages, or use the console command SET NW CERTEXP <value>, where <value> is the hexadecimal value of the key (default is 10001).

- **Certificate Common Name 1 and Certificate Common Name 2** This is the name of the certificate on the primary authentication server (most applications only use a single certificate common name). If both of the common names are set to null, all certificates are accepted. The default is null. Enter the names on the Configure Authentication Certificate page in the Serial Device Server internal web pages or use the console command SET NW CERTCN <name1> or SET NW CERTCN2 <name2> to enter the two certificate common names, where <name1> and <name2> are the desired names.

Private Key (TLS Wireless Security Only)
Private key information or the corresponding public key certificate for the Serial Device Server can be loaded from disk (Private Key Information File) or manually entered. If the file is encrypted, you must enter the passphrase in the passphrase entry field on the Configure Private Key page in the internal web pages of the Serial Device Server (NOTE: At present, only PEM format files are supported). To manually generate a self-signed certificate for the Serial Device Server, the following information is required:

- **Certificate Common Name**
- **Organization name**
- **Organization unit**
- **City name**
- **State name**
- **Country name**
- **Key Size (1024 or 2048)**

You may enter this information on the Configure Private Key page in the internal web pages of the Serial Device Server, or via console commands.

Appendix B
Console Commands

The following tables describe the console commands available from the internal command console. Access the command console through the serial port (if enabled for console mode) or over the network using a Telnet session or a web browser. The console can also be accessed via UART level signals on connector CN5 on the Serial Device Server printed circuit board (this requires you to open the Serial Device Server enclosure and use a special cable; it should only be used by qualified personnel for diagnostic and troubleshooting purposes).

Wireless and Network Security Commands

The following group of commands configures network parameters.

Table 14 Network Commands

Command	Description
SH NW	Displays summary network information Sample output: `WiFi Mode = INFRASTRUCTURE` `WiFi SSID: silex` `Speed = 11` `Regulatory Domain = 704` `WiFi FW Ver = 1F 1.7.1` `AP density = LOW` `TTLS is Disabled` `WEP is Disabled` `Link DOWN`
SH NW SQ	Display wireless network signal quality Sample Output:: `Signal Quality = 93` `Signal Strength = 53` `Noise Level = 135`

Command	Description
SET NW AUTHtype	Sets wireless authentication type The default value is Open System Format: `SET NW AUTHtype [OPEN | SHARED | TTLS | LEAP | PEAP | TLS | FAST | WPA-PSK ]`
SH NW AUTH	Shows wireless authentication type Sample output: `Authentication type= OPEN SYSTEM`
SET NW ETHAUTH	Sets Ethernet wired authentication type The default value is Open System Format: `SET NW ETHAUTH [TTLS | TLS | PEAP ]`
SH NW ETHAUTH	Shows Ethernet wired authentication type Sample output: `Authentication type= PEAP`
SET NW AUTHTRY	Sets number of times the Serial Device Server will attempt to authentication The default value is 0. Format: `SET NW AUTHTRY n`
SH NW AUTHTRY	Shows number of authentication tries. Sample output: `Authentication Try Count = 3`
SET NW CHannel	Sets WLAN ad-hoc channel number The valid numbers are 1 through 11. Format: `SET NW CHannel n`
SET NW ENC	Sets WLAN Encryption Mode. Supported modes are None, 64 bit WEP, 128 bit WEP, WPA, WPA2, WPA2-WPA The default value is Disable. Format: `SET NW ENC  [Disable | 64 | 128 | WPA | WPA2 ]`
SH NW ENC	Shows the wireless encryption mode The deprecated command SH NW WEP also displays this information. Sample output: `WiFi encryption is Disabled`

Command	Description
SET NW KEY#	Selects the WLAN WEP key entry (the WEP key that will be used as the transmit key) The possible values are 1, 2, 3, or 4; the default value is 1. Format: `SET NW KEY#  n`
SET NW KEYVAL	Sets the WLAN WEP key entry to the specified hex value For WEP128, the key is 10 hex characters long; for WEP128, the key is 26 hex characters long; the default value is null. Format: `SET NW KEYVAL <key>`
SET NW MOde	Sets WLAN mode The possible modes are Infrastructure and Ad-Hoc; the default value is Ad-Hoc Format: `SET NW MOde  <mode>`
SH NW MODE	Shows wireless operating mode Sample output: `Wifi mode = AD-HOC (802.11)`
SH NW RADio	Shows the selected radio mode of operation Sample output: `Radio mode is 802.11b-g`
SET NW SPeed	Sets maximum WLAN speed Possible values are 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, and 1; the default value is 54. Format: `SET NW SPeed  n`
SH NW SPEED	Show the maximum wireless data speed in megabits per second Sample output: `Speed = 54`
SET NW SSid	Sets WLAN SSID The default value is *serserv*. Format: `SET NW SSid  <name>`
CL NW SSid	Clears SSID value and allows the server to connect to any AP. Format: `CL NW SSid`
SET NW BSsid	Sets WLAN BSSID to connect to a specific access point's mac address Format: `SET NW BSsid  <value>`
CL NW BSsid	Clears BSSID value and allows the server to use SSID, not a specific AP Format: `CL NW BSsid`

Command	Description
SET NW RTS	Sets WLAN RTS threshold The possible values are between 1 and 3000; the default value is 2432. Format: `SET NW RTS n`
SH NW RTS	Shows wireless RTS threshold Sample output: `Wifi RTS Threshold = 2432`
SH NW STATS	Shows network I/O statistics Sample output: `WiFi statistics:` `TX Unicast frames: 0` `TX Multicast frames: 0` `TX Fragments: 0` `TX Unicast octets: 0` `TX Multicast octets: 0` `TX Deferred: 0` `TX Single retry frames: 0` `TX Multiple retry frames: 0` `TX Retry limit exceeded: 0` `TX Discards: 0` `RX Unicast frames: 0` `RX Multicast frames: 0` `RX Fragments: 0` `RX Unicast octets: 0` `RX Multicast octets: 0` `RX FCS errors: 0` `RX Discards no buffer: 0` `TX Discards wrong SA: 0` `RX Discards WEP undecr: 0` `RX Msg in msg fragments: 0` `RX Msg in Bad msg fragments: 0`
SET NW CERTCN	Sets EAP Common Name The default value is null. Format: `SET NW CERTCN <name>`
SH NW CERTCN	Shows the value of first common name check string The default is null (blank) string. The command SH NW TTCN also returns this information. Sample output: `Common name 1`
SET NW CERTCN2	Sets second EAP Common Name Format: `SET NW CERTCN2 <name>`
SH NW CERTCN2	Shows the value of the second common name check string

Command	Description
	The default is null (blank) string. Sample output: `Common name 2`
SET NW CERTEXP	Sets EAP Certificate Exponent value The default value is 10001 Hex. Format: `SET NW CERTEXP <exponent>`
SH NW CERTEXP	Shows the value of the certificate exponent The deprecated command SH NW TTEXP also returns this value Sample output: `65537 (10001h)`
SET NW CERTKEY	Sets EAP root key Format: `SET NW CERTKEY <key value>`
SET NW ID	Sets authentication User ID This can include the realm separated by @. The default value is anonymous. Sample output: `SET NW ID <user id>`
SH NW ID	Shows the value of the authentication ID, including realm, if applicable The default realm is a null (blank) string. The deprecated command SH NW TTID also returns this data. Sample output: `anonymous@somewhere`
SET NW PW	Sets the password for the 802.1x EAP authentication, if enabled The default value is anonymous. Format: `SET NW PW <password>`
SET NW INAP	Sets EAP inner-authentication protocol The possible protocols are PAP and MSCHAP_V2; the default value is PAP. Format: `SET NW INAP [PAP|MSCHAP_V2]`
SH NW INAP	Shows the inner authentication mode The deprecated command SH NW TTAP also returns this data. Sample output: `Authentication protocol = PAP`
SET NW REALM	Sets the realm portion of the 802.1x EAP authentication ID This value can also be set with the ID command. The default value is null. Format: `SET NW REALM <realm>`

Command	Description
SH NW REALM	Shows the realm associated with the authentication ID, if applicable. The default value is null (blank) string. The deprecated command SH NW TTRE also returns this data. Sample output: `Somewhere`
SET NW WPAGROUP	Enable or disable WPA group key mode. If enabled, group keys can be used for data link encryption. The default value is disabled. Sample output: `SET NW WPAGROUP [ENABLE | DISABLE]`
SH NW WPAAUTO	Shows state of WPA auto connect flag Sample output: `WPA-AUTO Enabled`
SH NW WPAGROUP	Shows state of the allow WPA group keys flag Sample output: `WPA-GROUP Disabled.`
SET NW WPAPSK	Sets WPA PSK pass phrase or hex key. This value is only used if the authentication mode is WPA-PSK or WPA2-PSK. The argument to this command is either a pass phrase of 8 to 63 characters or exactly 64 hex characters representing the 256 bit PSK value. Format: `SET NW WPAPSK <key>`
SET NW WPATRACE	Sets WPA trace level. This command is for diagnostic purposes only. The default value is 0 or disabled. Format: `SET NW WPATRACE nn`
SH NW DISCONN	Displays the current value of the network disconnection timer Sample output: `Disconnect Timer: 5`
SET NW DISCONN	Sets the period of the network link disconnection watchdog timer. In wireless infrastructure mode, this timer monitors the wireless link, and if the unit is not connected to an AP for the time specified, the unit is reset. `SET NW DISCONN nn` `N = 0 watchdog timer is disabled` `1-255 watchdog timer period in minutes` The factory default value is 5 minutes. This timer also controls a receive activity monitor when the wireless network link is connected. If no packets are received during the time specified, and the link remains up, the unit will reset at the end of the time period.

Command	Description
SET NW RESET	This command stops, and then resets the wireless network interface. This will effectively disassociate the unit from an access point if it is connected. If the unit is in wireless infrastructure mode, the unit will then scan and attempt to reconnect to a suitable access point, if one is available. Format: `SET NW RESET`

Port Commands

Table 15 Port Commands

Command	Description
SH PORT	Shows port parameters Sample output: `Port Q-Size Type Attributes` `*S1 0 serial 115200 N 8 1 XON/XOFF`
CLEAR PORT S1 JOB	Aborts the active job on the port. If the remote host is connected, additional data received will be discarded. Format: `CL PORT S1 JOB`
SET PORT S1 FLOW	Sets serial port flow control to NONE, XON/XOFF, CTS, or DSR The default value is none. Format: `SET PORT S1 FLOW <flow>`
SET PORT S1 PARITY	Sets serial port parity to NONE, EVEN, ODD, MARK, or SPACE The default value is none. Format: `SET PORT S1 Parity <parity>`
SET PORT S1 SIZE	Sets data bits on the serial port The default value is 8. Format: `SET PORT S1 SIZE [7 | 8]`
SET PORT S1 SPEED	Sets serial port baud rate. Options for BAUD are 300, 600, 1200, 2400, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600 The default value is 115200. Format: `SET PORT S1 SPEED <baudrate>`
SET PORT S1 STOP	Sets serial port stop bits per character The default value is 1. Format: `SET PORT S1 STOP [1 | 2]`
SET PORT S1 MODE	Sets serial port line mode The default value is 232.

Command	Description
	Format: SET PORT S1 STOP [232 | 422 | 485 | 485D]

Server Information Commands

Table 16 Server Information Commands

Command	Description
SET SERVEr Description	Sets server description string Format: `SET SERVEr DEscription <description-string>`
SET SERVEr NAme	Sets server node name The default value is TWC_xxxxxx, where xxxxxx are the last 6 hex digits of the MAC address. Format: `SET SERVEr NAme <name>`
SET SNMP GETCOMM	Gets community name The default value is public. Format: `SET SNMP GETCOMM <string>`
SET SNMP JETADmin	Enables or disables JetAdmin compatibility The default value is enabled. Format: `SET SNMP JETADmin [ ENable | DIsable]`
SET SNMP SETCOMM1	Sets community 1 name The default value is internal? Format: `SET SNMP SETCOMM1 <string>`
SET SNMP SETCOMM2	Sets community 2 name The default value is Pass. Format: `SET SNMP SETCOMM2 <string>`
SET SNMP CONtact	Sets system contact string The default value is null. Format: `SET SNMP CONtact <string>`
SET SNMP LOCation	Sets system location string The default value is null. Format: `SET SNMP LOCation <string>`
SH SERIAL	Displays serial number of the unit Sample output: `Serial number is 9047595`

Command	Description
SH SERVEr	Shows server parameters Sample output: `Serial Server Serial # 9047595` `Address: 00-40-17-8A-0E-2B  Name: TWC_8A0E2B Number: 0` `Identification:  Network Server` `Enabled Characteristics:` `Link DOWN`
SH SERVEr CO	Shows server network statistics Sample output: `Seconds Since Zeroed: 163  Frames Sent,1 Collision: 26` `Bytes Received:72950  Frames Sent, 2+Collision: 5` `Bytes Sent:18726  Send Failures: 0` `Frames Received:752  Send Failure Reasons: 0` `Frames Sent: 181  Receive Failures:  503` `Multicast Bytes Rcv'd:64474  Receive Failure Reasons: 1` `Multicast Bytes Sent: 2406  Unrecognized Destination: 0` `Multicast Frames Rcv'd:626  Data Overrun: 0` `Multicast Frames Sent:11  User Buffer Unavailable:0` `Frames Sent, Deferred:2014  System Buffer Unavailable:1`
SH SNMP	Shows state of SNMP protocol enable Sample output: `SNMP is Enabled`
SH VErsion	Shows firmware version of print server Protocols supported: NetBIOS SNMP TCP/IP EMail DHCP Sample output: `serial server` `Firmware Ver. 4.19 (2004.10.31)` `Boot Ver. 1.4` `16Mbit Flash`
Zero	Clears and resets the network statistic counters

Service Commands

Table 17 Service Commands

Command	Description
SET SERVI <service name> BOT	Sets beginning of transmission (BOT) string index for service The SH SERVI STRings command displays the available strings and their associated number; the default value is 1. Format: `SET SERVI <service name> BOT  nn`
SET SERVI <service name> EOT	Sets end of transmission (EOT) string index for service The SH SERVI STRings command displays the available strings and their

Command	Description
	associated number; the default value is 1. Format: `SET SERVI <service name> EOT nn`
SH SERVI STRings [*string_num*]	Displays the BOT and EOT strings used in services If *string_num* is provided, then the specific string definition and expansion display. If *string_num* is not provided, then all string definitions display without their expansions. Sample Output: `10: \FF\04\FF\05\FF\06\FF\08`
SET SERVI <service name> FIlter	Sets filter index for service Format: `SET SERVI <service name> FIlter nn`
SH SERVI FILters	Shows filter settings Sample output: **# Service Name Filter** 1 TWC_FFFFFF 0: No Filter 2 BINARY_P1 0: No Filter 3 TEXT_P1 1: Text Substitution m= LF, r= CRLF 4 TWC_FFFFFF_P1_4 0: No Filter 5 TWC_FFFFFF_P1_5 0: No Filter 6 TWC_FFFFFF_P1_AT 4: PostScript Tagged Binary
SET SERVI <service name> FMS	Sets filter 1 text replacement match string index. If the index is zero, the default string of <LF> (line feed) is used. The default value is 0. Format: `SET SERVI <service name> FRM nn`
SET SERVI <service name> FRS	Sets filter 1 text replacement replace string index. If the index is zero, the default string of <CRLF> (carriage return-line feed) is used. The default value is 0. Format: `SET SERVI <service name> FRS nn`
SET SERVI <service name> IP	Enables or disables IP based jobs such as lpd, raw tcp and ftp, on the service The default value is enabled for service 1 and 2, disabled for all others. Format: `SET SERVI <service name> IP [ENable | DIsable]`
SET SERVI <service name> NAme	Changes service name The default value varies by service Format: `SET SERVI <service name> NAme <newname>`
SET SERVI <service	Sets output port associated with a service

Command	Description
name> POrt	The default value is S1. Format: `SET SERVI <service name> POrt <portname>`
SET SERVI <service name> PRIority	Sets priority for service for multiple service transmissions simultaneously The default value is 10. Format: `SET SERVI <service name> PRIority nn`
SH SERVI PRI [*service_num*]	Shows priority of service. If *service_num* is not provided, the priority of all services is listed.
SET SERVI <service name> RECeive	Sets receive only mode for a service This option is required only for host applications that do not operate properly if data is received from the serial device. The default value is disabled. Sample output: `SET SERVI <service name> RECeive [ENable | DIsable]`
SET SERVI <service name> TCP	Sets raw TCP port for service If port number is 0, raw TCP is disabled on service. The default value is 9100 for service 1, 3001 for service 2. Format: `SET SERVI <service name> TCP nn`
SH SERVI SUMmary [*service_num*]	Shows the basic parameters for a specific service. If *service*_num is not provided, parameters for all services are displayed. The command SH SERVI displays the same data as SHOW SERVI SUM.

String Commands

Table 18 String Commands

Command	Description
SET STRing	Set service string table entry String 1 to11 cannot be set or changed. Format: `SET STRing <string #> ”value”`
CL STRing	Clears the service string table entry Format: `CL STRing <string #>`

Command	Description
SH STRing [*string_num*]	Defines the BOT and EOT strings used in services If *string_num* is provided, then the specific string definition and expansion are displayed. If *string_num* is not provided, then all string definitions are displayed without their expansions. Sample output: `1:` `2: \1BE` `3: \04` `4: \1B%-12345X` `5: @PJL` `6: ENTER LANGUAGE=` `7: PCL\0A` `8: POSTSCRIPT\0A` `9: \FF\04\FF\05\FF\06\FF\07` `10: \FF\04\FF\05\FF\06\FF\08` `11: \0C`
SH FILters	Shows the filters that can modify a job stream Sample output: **`#  Filter`** `0  No Filter` `1  Text Substitution` `2  AppleTalk` `3  Text to PostScript` `4  PostScript Tagged Binary` `5  DC1 Special`

TCP/IP Commands

Table 19 TCP/IP Commands

Command	Description
SET IP ACcess	Allows or prevents access to a block of remote addresses The default value is empty list. Format: `SET IP ACcess [EN | DI | ALL] aa.bb.cc.dd {MAsk ee.ff.gg.hh]`
SET IP RANge	Allows or prevents access to a range of remote addresses The default value is empty list. Format: `SET IP RANge [EN | DI | ALL] aa.bb.cc.dd {MAx ee.ff.gg.hh]`
SH IP ACcess	Displays current access list settings Sample output: `All hosts permitted access`

Command	Description
SET IP ADdress	Sets server IP address The default value is 192.0.0.192 Format: `SET IP ADdress aa.bb.cc.dd`
SET IP ARP ENable	Enables or disables setting of IP address with an ARP packet The default value is Enable. Format: `SET ARP [ENable | DIsable]`
SET IP BAnner	Enables or disables printing of job banner on LPD jobs The default value is Disable. Format: `SET IP BAnner [ENable | DIsable]`
SET IP CHKSUM	Enables or disables verification of IP checksum on received packets The default value is Enable. Format: `SET IP CHKSUM [ENable | DIsable]`
SET IP BOot	Sets number of tries for each enabled IP boot method, if not set to static The default value is 3. Format: `SET IP BOot n`
SET IP ENable	Enables or disables all IP based protocols The value is Enable. Format: `SET IP [ENable | DIsable]`
SET IP FTIme	Sets IP timeout If enabled, the IP timeout is measured in seconds. If disable, the IP timeout is in minutes. The default value is Disable. Format: `SET IP FTIme [ENable | DIsable]`
SET IP FTP	Enables or disables FTP protocol The default value is Enable. Format: `SET IP FTP [ENable | DIsable]`
SET IP HTTP	Enables or disables HTTP protocol The default value is Enable. Format: `SET IP HTTP [ENable | DIsable]`
SET IP KEepalive	Sets interval in minutes for sending TCP keepalive packets on a connection The default value is 5 minutes. Format: `SET IP KEepalive n`
SET IP LPD	Enables or disables the LPD protocol

Command	Description
	The default value is Enable. Format: `SET IP LPD [ENable | DIsable]`
SET IP MEthod	Sets method of getting IP address The default value is Auto. Format: `SET IP MEthod [ AUTO | BOOTP | RARP | DHCP | STATIC ]`
SET IP PIng	Sends IP ping packets to test connection to remote host Format: `SET IP PIng aa.bb.cc.dd`
SET IP PRObe	Enables or disables TCP connection probes The default value is Disable. Format: `SET IP PRObe [ENable | DIsable]`
SET IP RARp	Enables setting of default router and/or subnet mask based on RARP IP address set The default value is 0. Format: `SET IP RARp nn` `nn: 0=both 1=no subnet, 2=no router, 3=neither`
SET IP REtry	Enables or disables LPD retry on incomplete job The default value is Disable. Format: `SET IP REtry [ENable | DIsable]`
SET IP ROuter	Sets default router address The default value is 0.0.0.0. Format: `SET IP ROuter aa.bb.cc.dd`
SET IP SUbnet	Sets IP subnet mask The default value is 0.0.0.0. Format: `SET IP SUbnet aa.bb.cc.dd`
SET IP TCP	Enables or disables the raw TCP 9100 protocol The default value is Enable. Format: `SET IP TCP [ENable | DIsable]`

Command	Description
SET IP TELnet	Enables or disables Telnet protocol The default value is Enable. Format: `SET IP TELnet [ENable | DIsable]`
SET IP TFTP	Enables or disables TFTP protocol The default value is Enable. Format: `SET IP TFTP [ENable | DIsable ]`
SET IP TImeout	Sets TCP inactivity timeout. If fast timeout is enabled, the timeout is calculated as seconds. If fast timeout is disabled, the timeout is calculated as minutes. The default value is 1 minute. Format: `SET IP Timeout n`
SET IP WIndow	Sets TCP maximum window size in bytes The default value is 10240. Format: `SET IP WIndow nn`

<table>
<tr><th>Command</th><th colspan="3">Description</th></tr>
<tr><td>SH IP</td><td colspan="3">Shows TCP/IP related parameters
Sample Output:
<pre>IP is enabled
IP address   192.0.0.192   Boot tries   3
Subnet mask   0.0.0.0   Boot method   AUTO
IP Gateway   0.0.0.0   Max window   10240
 (set manually)
LPD banner   disabled   Timeout   1 min
LPD retries are disabled   Keepalive   5 min

Service   Port   TCP port
xxxxxx_S1_A   S1   9100
xxxxxx_S1_B   S1   3001</pre></td></tr>
<tr><td>SET IP TRAP n TRIG <trigger-mask></td><td colspan="3">Specifies the trigger conditions that will cause a trap to be sent. <trigger-mask> is an integer in hex format representing a 32-bit mask as defined below. If the corresponding bit is 1, the trigger condition is enabled to cause the trap.

NOTE: Even if the trigger bit is set by this command, no trap will be entered if the underlying trigger has not been configured.</td></tr>
<tr><td></td><td>Bit#</td><td>Hex Value</td><td>Trigger Condition</td></tr>
<tr><td></td><td>0</td><td>00000001</td><td>Serial Server: Match string 1</td></tr>
<tr><td></td><td>1</td><td>00000002</td><td>Serial Server: Match string 2</td></tr>
<tr><td></td><td>2</td><td>00000004</td><td>Serial Server: Match string 3</td></tr>
<tr><td></td><td>3</td><td>00000008</td><td>Serial Server: Match string 4</td></tr>
<tr><td></td><td>4</td><td>00000010</td><td>Serial Server: Match string 5</td></tr>
<tr><td></td><td>5</td><td>00000020</td><td>Serial Server: Match string 6</td></tr>
<tr><td></td><td>6</td><td>00000040</td><td>Serial Server: Match string 7</td></tr>
<tr><td></td><td>7</td><td>00000080</td><td>Serial Server: Match string 8</td></tr>
<tr><td></td><td>8</td><td>00000100</td><td>Undefined</td></tr>
<tr><td></td><td>9</td><td>00000200</td><td>Undefined</td></tr>
<tr><td></td><td>10</td><td>00000400</td><td>Undefined</td></tr>
<tr><td></td><td>11</td><td>00000800</td><td>Undefined</td></tr>
<tr><td></td><td>12</td><td>00001000</td><td>Undefined</td></tr>
<tr><td></td><td>13</td><td>00002000</td><td>Undefined</td></tr>
<tr><td></td><td>14</td><td>00004000</td><td>Undefined</td></tr>
<tr><td></td><td>15</td><td>00008000</td><td>Undefined</td></tr>
</table>

Firmware Update

Table 20 Firmware Update

Command	Description
SET LOAd ENable	Sets the firmware to perform a soft reset and enter the server boot program after the next Exit command. This command is used for diagnostic purposes only. The default value is Disable. Format: `SET LOAd (ENable | DIsable ]`
SET LOAd HOst	Sets the node name of the Netware boot host. This command is used for diagnostic purposes only. The default value is null>\ Format: `SET LOAd HOst <name>`
SET LOAd IP	Sets source computer IP address for TFTP get operation. The default value is 0.0.0.0. Format: `SET LOAd IP aa.bb.cc.dd`
SET LOAd SOftware	Sets filename on host for TFTP get update Format: `SET LOAd SOftware <filename>`
SET LOAd TFTP	Initiates firmware update using TFTP get operation. The TFTP server address must be set using SET LOAd IP and the filename using SET LOAd SOftware. The server will reset after the firmware update is completed. Format: `SET LOAd TFTP`
SET LOAd XModem	Initiates firmware update using the XModem protocol on the serial console The server will reset after the firmware update is completed. Format: `SET LOAd XModem`
SH LOAd	Shows the firmware update parameters Sample output: `Firmware load is disabled` `Load Host IP = 0.0.0.0` `Software file = xxxx.bin` `Load Host Name =`

Miscellaneous Commands

Table 21 Miscellaneous Commands

Command	Description
SET DEFAULT	Set parameters to factory defaults
EXIT	This command exits the current configuration console session.
SH FATal	Shows fatal error log, if fatal errors exist.
CL FATal	Clears the fatal error log
INIT	Instructs the server to execute a soft reset when the next exit command is executed.
SET PAssword	Sets the server access (read) password
SET POWERON	Sets Power on delay
SH POWERON	Displays Power on delay in seconds
SET PROTect	Sets update password to the string given.
CL PROTect	Sets update password to <null>.
SAVE	Saves the current configuration to non-volatile memory. Without this command, the configuration is not saved unless an EXIT command is performed.
SH TEst	Sends the configuration data via ASCII to the serial port
UNPROTECT	If an update password has been defined (SET PROTECT), this command enters the password to allow configuration items to be modified. After entering this command, the server will prompt for the update password. If entered properly, the user will then be able to execute SET commands to modify the server configuration. This lasts only until the console session is terminated with an EXIT command.

Help Commands

For help, simply enter HELP preceding the command. The correct syntax and a brief description of the commands will display. For example, when inquiring for various commands to display specific IP parameters, type HELP SHOW IP, or for commands to change specific wireless/network security parameters, type HELP SET NWRK.

Appendix C
Firmware Update Procedures

Occasionally it may be necessary to update the Serial Device Server to take advantage of new features or to fix specific problems. The simplest way to perform this update is with the Silex UpdateIP utility for Windows XP and 2000 computers. This utility can be found on the CD-ROM that is included with the Serial Device Server, or it can be downloaded from the *Support & Downloads* section of the Silex website (www.silexamerica.com).

To use UpdateIP:

1. Download the appropriate firmware update file from *the Support & Download* section of the Silex website (www.silexamerica.com) into a directory on your computer.
2. Download or copy the UpdateIP software files into a directory on your computer.
3. Double click the updateip.exe icon to start the UpdateIP application.
4. Click ***OK*** when you get the ***About Update for TCP/IP*** splash screen

Important: Make sure that the UpdateIP application is included as an exception if you have a firewall enabled on your PC.

   on this screen. Click ***OK*.**
7. The program will search the local network for Serial Device Servers. Click ***OK*** when the search process is complete.
8. A list of available Serial Device Servers will appear. Highlight the Serial Device Server(s) that you wish to update.
9. From the menu bar, select ***Update*** and then ***Start*** to update the Serial Device Server(s).

If you cannot use UpdateIP, you can use the trivial file transfer protocol (tftp) to update the Serial Device Server firmware:

1. Download the appropriate firmware update file from the *Support & Downloads* Section of the Silex website (www.silexamerica.com) into a directory on your computer.
2. If you are using Windows 2000, XP, or Vista, enter the following command from the command line of your operating system:

   tftp -i *ipaddress* put *filename* access

   where *ipaddress* is the IP address of the Serial Device Server, *filename* is the file name (and path, if necessary), and "access" is the Serial Device Server password (if you changed this password, use your new password instead of "access"). For example, to download the file tathsti130.bin from the updates directory on your computer into a Serial Device Server with an IP address of 192.168.5.70, you would enter the command:

```
tftp  -i 192.168.5.70  put  /updates/tathsti130.bin  access
```

If you are using a different operating system, please refer to the documentation of that operating system for information on how to use the tftp command. Note that you should specify that the tftp destination file is the Serial Device Server password (“access” by default).

Appendix D
Safety and Regulatory Notices

Information for United States Users

This equipment has been tested and found to comply within the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio and television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver,
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user is cautioned that changes and modifications made to the equipment without the approval of manufacturer could void the user's authority to operate this equipment.

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

The radiated output power of the print server is far below the FCC radio frequency exposure limits. Nevertheless, print server shall be used in such a manner that the potential for human contact during normal operation is minimized.

To satisfy RF exposure requirements, this device (SX-500) and its antenna(s) must operate with a separation distance of at least 20 centimeters from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users must be provided with specific operating instructions for satisfying RF exposure compliance.

Declaration of Conformity (FCC) (SX-500)

According to 47CFR, Part 2 and 15 for Class B Personal Computers and Peripherals; and/or CPU Boards and Power Supplies used with Class B Personal Computers:

We: Silex Technology America, Inc.
Located at: 157 West 7065 South
Salt Lake City, UT 84047, USA

Declare under sole responsibility that the product identified herein, complies with 47CFR Part 2 and 15 of the FCC rules as a Class B digital device FOR HOME OR OFFICE USE. Each product marketed, is identical to the representative unit tested and found to be compliant with the standards. Records maintained continue to reflect the equipment being produced can be expected to be within the variation accepted, due to quantity production and testing on a statistical basis as required by 47CFR §2.909. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Trade Name: silex
Type of Product: Ethernet and Wireless 802.11b and 802.11g-enabled serial server
Model: SX-500

Silex Technology America, Inc. hereby declares that the equipment specified above conforms to the above requirements.

Standards used and met in the assessment:

- CFR Title 47, Part 15, Subpart B and Subpart C; EN55022: 1998 Class B
- FCC ID: N6C-SX10WG

Information for Canadian Users (IC notice) (SX-500)

The term “IC” before the radio certification number only signifies that Industry of Canada technical specifications were met. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations (RSS-210, IC: 4908A-SX10WG).

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment that is installed outdoors is subject to licensing.

This device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen than the equivalent isotropically radiated power (EIRP) is not more than the required for successful communication.

Information for European Users (SX-500)

The server and its built-in 802.11b, and 802.11g wireless technology is in compliance with the Class B Information Technology Equipment requirements and other relevant provisions of European Directive 1999/5/EC. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communications devices. The internal function is a radio device using the 2.4 GHz frequency band (2.400GHz - 2.4845 GHz). It is intended for wireless communication with other 802.11b, and 802.11g-enabled devices in an indoor environment.

The use of 802.11b and 802.11g wireless technology in certain countries may be restricted. Before using 802.11x products, please confirm with the frequency management authority in the country where you plan to use it. Many countries allow indoor use only. In Italy, general authorization is required if used outside. In France, the use of certain channels is restricted outdoors. In some situations or environments, the use of 802.11x wireless technology might be restricted by the proprietor of the building or responsible representatives of the organization, for example, in airplanes, in hospitals or in any other environment where the risk of interference with other devices or services is perceived or identified as harmful.

If you are uncertain of the policy that applies to the use in a specific organization or environment, you are encouraged to ask for authorization to use 802.11x wireless technology prior to switching it on. Consult your physician or the manufacturer of personal medical devices (pacemakers, hearing aids, etc.) regarding any restrictions on the use of 802.11x wireless technology.

silex cannot be responsible for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product.

Declaration of Conformity (CE) (SX-500)

Manufacturer: Silex Technology America, Inc.
157 West 7065 South
Salt Lake City, UT 84047, USA
Telephone: (801) 748-1199

Product: Ethernet and Wireless 802.11b and 802.11g-enabled serial server
Model No.: SX-500

Silex Technology America, Inc. hereby declares that the above-referenced product, to which this declaration relates, in is conformity with the provisions of:

Council Directives 1999/5/EC, Radio Equipment and Telecommunications Terminal Equipment.

Standards used and met in the assessment:

- EN301 489-1
- EN301 489-17
- EN300 328

The documents required by this Directive are maintained at the corporate headquarters of Silex Technology America, Inc., 157 West 7065 South, Salt Lake City, UT 84047, USA

Declaration of Conformity (FCC) (SX-510)

According to 47CFR, Part 2 and 15 for Class B Personal Computers and Peripherals; and/or CPU Boards and Power Supplies used with Class B Personal Computers:

We: Silex Technology America, Inc.
Located at: 157 West 7065 South
Salt Lake City, UT 84047, USA

Declare under sole responsibility that the product identified herein, complies with 47CFR Part 2 and 15 of the FCC rules as a Class B digital device FOR HOME OR OFFICE USE. Each product marketed, is identical to the representative unit tested and found to be compliant with the standards. Records maintained continue to reflect the equipment being produced can be expected to be within the variation accepted, due to quantity production and testing on a statistical basis as required by 47CFR §2.909. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Trade Name: Silex
Type of Product: Ethernet and Wireless 802.11b/g and 802.11a-enabled serial server
Model: SX-510
Silex Technology America, Inc. hereby declares that the equipment specified above conforms to the above requirements.

Information for Canadian Users (IC notice) (SX-510)

The term “IC” before the radio certification number only signifies that Industry of Canada technical specifications were met. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations (RSS-210).

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment that is installed outdoors is subject to licensing.

This device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen than the equivalent isotropically radiated power (EIRP) is not more than the required for successful communication.

The SX-510 complies with standards for the following countries:

USA:

- FCC Standard: Part 15, Subpart B, Subpart C and subpart E
- FCC ID: N6C-SX510
- Medical EMC: IEC 60601-1-2:2001
- Safety: UL 60950-1 (CSA Mark)
- SAR: ANSI/IEEE Std. C95.1-1999
- IP Rating: IP21

Canada:

- IC Standard: RSS-210
- IC: 4908A-SX510
- Medical EMC: IEC 60601-1-2:2001
- Safety: CSA 60950-1
- SAR: RSS-102
- IP Rating: IP21

IMPORTANT NOTE: THE SX-510 RS-422/RS-485 INTERFACE HAS NOT BEEN TESTED FOR COMPLIANCE WITH IEC 60601-1-2:2001/EN60601-1-2 MEDICAL EMC OR ANSI/IEEE Std. C95.1-1999, RSS-102 SAR STANDARDS. THEREFORE RS-422/485 SHOULD NOT BE ENABLED IF YOU REQUIRE COMPLIANCE WITH ANY OF THESE STANDARDS.

Appendix E
Silex Contact Information

Silex Technology America, Inc.
www.silexamerica.com
Technical Support: support@silexamerica.com
Sales: sales@silexamerica.com
Tel: (801) 748-1199 8:00 to 5:00 Mountain Time
Tel: (866) 765-8761 toll-free
Fax: (801) 748-0730

Silex Technology Europe GmbH
www.silexeurope.com
Tel: +49-2159-67500
Tel: 0800-7453938 German toll free
Email: contact@silexeurope.com

Silex Technology Beijing, Inc.
www.silex.com.cn
Tel: +86-10-8497-1430
Email: contact@silex.com.cn

Corporate Headquarters
Silex Technology, Inc.
www.silex.jp
Tel: +81-6-6730-3751
Email: support@silex.jp



Silex Technology America, Inc.
www.silexamerica.com

Part Number 140-00188-180

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP