Serial Encrypter

TABLE OF CONTENTS

Data Comm for Business, Inc.
PO Box 6329
Champaign, IL 61826-6329
(217) 897-6600
www.dcbnet.com

November 9, 2007
Firmware Version: 1.0

1. DESCRIPTION

The SSE Serial Encrypter is a data privacy encryption module for RS232 and RS485/4-wire applications. It is designed for use in legacy serial applications where block encryption devices may not work. A fixed key design and the self-synchronizing stream cipher eliminates the need for negotiation between the SSE devices and allows use over unidirectional connections.

FEATURES

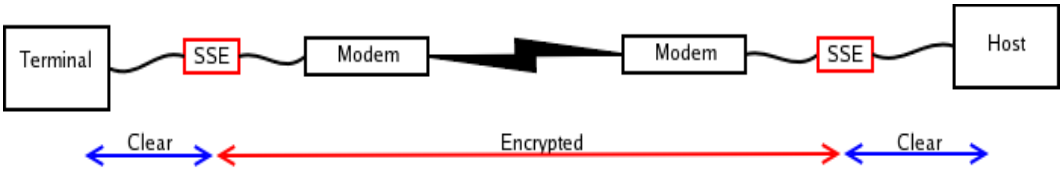
- RoHS compliant.
- Advanced Encryption Standard (AES) with user selectable 128-bit, 192-bit, or 256-bit key.
- 8-Bit Cipher Feedback Mode (CFB8) providing a self-synchronizing stream cipher, suitable for use over non-error corrected serial links.
- Fixed key operation allowing use in unidirectional or bi-directional point-to-point and point-to-multi-point applications.
- Pseudo-Random Number Generator based on ANSI X9.31 Appendix A.2.4 using AES.
- No proprietary algorithms. Users may use a single SSE and terminate the cipher stream with their own application using any AES-CFB8 implementation that follows the NIST guidelines.
- Encryption may be enabled/disabled via control signal, allowing use with dial-up modems or any DCE device that provides a DCD output upon connection.
- Supports standard baud rates from 300 to 57600.
- Typically one character time of latency, per SSE device, in point-to-point mode. A 16 character synchronization string is require upon initial connection.
- Encryption rate, 256-bit mode: 7860 characters-per-second, 192-bit mode: 8960 cps, 128-bit mode: 11520 cps.
- Software selectable RS232 and RS485/4-wire interfaces. May be used as a RS232 to RS485 converter.
- Pass through of two input and two output control signals when used in RS232 mode.
- Ethernet interface for easy to use web based setup. Telnet and serial setup modes also available.
- 9v – 30v DC power (120VAC power supply included)
- 120VAC and 240VAC power supplies available (specify country)
- 48VDC and 125VDC power supplies available
- -40° to +75°C operating temperature range

APPLICATIONS

NOTE
The Clear Text side of the SSE is Port 1. Port 2 is the Encrypted side.

Point-to-point modem connections (dial-up, leased-line, cellular, radio, etc)

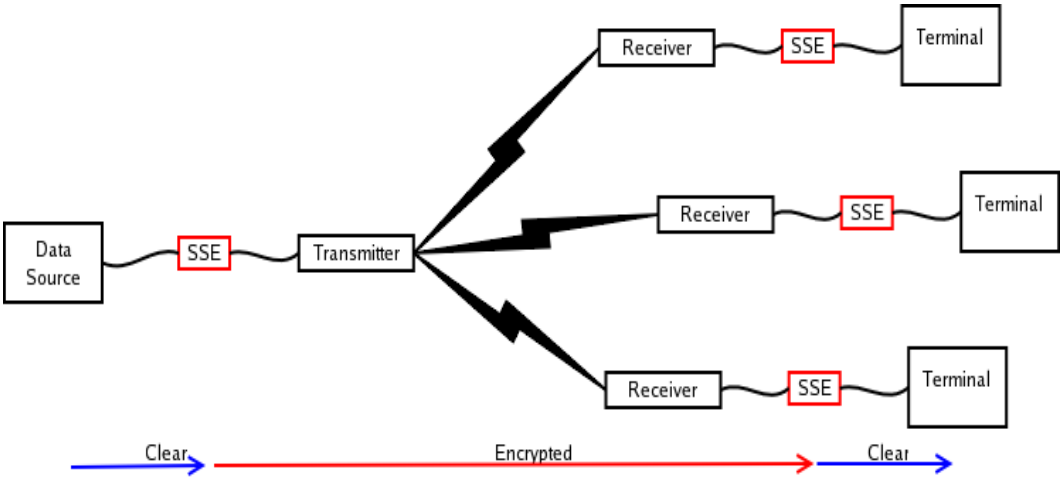
The SSE may be used in modem applications where the SSE is placed between the data source and the modem.



The SSE may be configured to dynamically enter and exit encryption mode based on the state of the carrier signal provided by the modem. This allows the controlling computer to configure and dial the modem. Once the connection is established, the modem will assert carrier causing the SSE to enter encryption mode.

Unidirectional broadcast applications

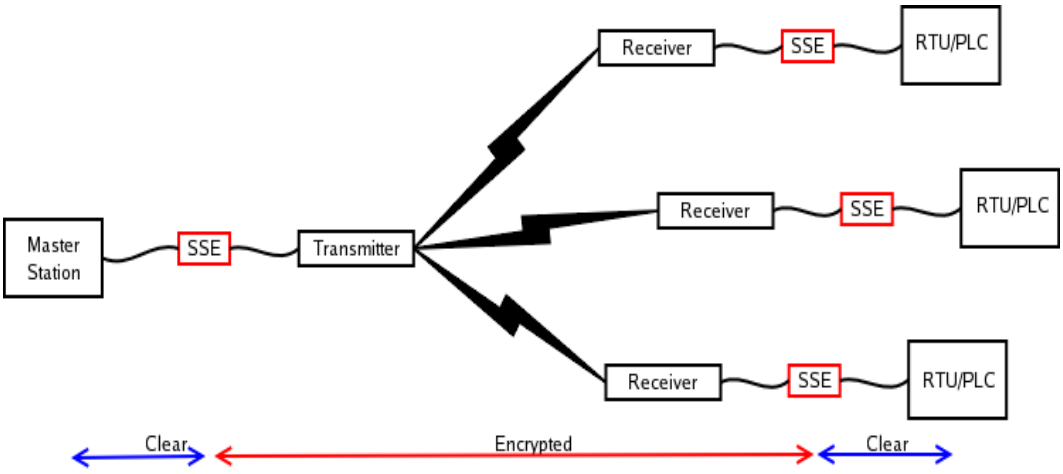
The SSE may be used in broadcast or data-feed applications where a continual stream of data is sent to one or more locations.



The CFB8 encryption mode allows the receivers to come on-line at anytime. The receivers will be able to synchronize to the data stream within 16 character times.

SCADA polling applications

The SSE may be used in point-to-multi-point polling applications provided there are separate channels available for outbound and inbound data.



Additional latency will typically be 2 character times for the Poll Request and 18 character times for the Poll Response.

INAPPROPRIATE APPLICATIONS

The SSE may not be used in point-to-multi-point applications where the master and slave devices all share a single data channel. An example of this would be a RS485/2-wire multi-drop application. This type of application causes the slaves to continually lose synchronization with the master.

The SSE may not be used in 7-bit applications. The SSE uses an 8-bit encryption mode, thus requires an 8-bit data path on the encrypted side of the connection. However it is acceptable to have 7-bit with parity on the clear side provided that the encrypted side is 8-bit no parity. In this case, the parity bit is treated as data and transmitted end-to-end.

The SSE should not be used in applications where the SSE is relied upon for data integrity or user authentication. The SSE is strictly an encryption device providing data privacy. Garbage in will result in garbage out.

SSE Front View

SSE Rear View

2. SPECIFICATIONS

2.1 General

- Two asynchronous RS232 ports
- DE-9P (PC-9pin) connectors, DTE interface
- Speeds to 57.6 Kbps
- Can be configured via RS232 serial port, or via Ethernet port using telnet, or web browser.
- Default IP address: 192.168.0.100

Protocol Features

- Advanced Encryption Standard (AES) with user selectable 128-bit, 192-bit, or 256-bit key.
- 8-Bit Cipher Feedback Mode (CFB8) providing a self-synchronizing stream cipher, suitable for use over non-error corrected serial links.
- Pseudo-Random Number Generator based on ANSI X9.31 Appendix A.2.4 using AES.

2.2 Environmental

- Operational Temperature: -40 to +75 C
- Storage Temperature: -50 to +75 C
- Humidity: <95% Non-condensing

2.3 Physical / Electrical

- Power requirements: 9 to 30 VDC (2 watts)
- 48, 125 VDC and 240 VAC options are available
- Supplied with 120 VAC power supply
- 4 ¼" wide x 3" long x 1" high
- Weight: 7.5 ounces

2.4 Setup Commands

Set LAN Configuration,
Serial Port Configuration
Cipher Configuration
Configuration Access
Display Configuration Settings
Algorithms Test
Reset Configuration to Default
Save and Exit
Exit without Saving

3. INSTALLATION

3.1 Unpacking

The following is included with each unit:

- Unit and external AC power supply
- Serial cable for connection to a PC for initial configuration.
- Manual
- Information regarding warranty, maintenance contracts and repair

3.2 Setup

The SSE must be properly configured before use. See Section 5 for connection and configuration information.

3.3 Connections

The RS-232 serial ports on the SSE are configured as Data Terminal Equipment (DTE). This is the same configuration used on PC COM ports. To connect the SSE to peripheral equipment, use the same cable that would be used to connect that equipment to a PC COM port. See Section 6 for more information.

Connect host and terminal devices to SSE Port 1 (Clear Text). Connect communications equipment to Port 2 (Encrypted).

3.4 Default Configuration

The factory default settings for the SSE are as follows:

IP Address: 192.168.0.100
Serial Ports: RS-232, 57,600, Point-to-Point mode
Encryption: Enabled

To reset the unit to factory defaults perform the following steps:

1. Depress and hold the SETUP switch.
2. Apply power to the SSE.
3. Continue holding the SETUP switch until the RUN indicator begins flashing.
4. Release the SETUP switch and wait for the unit to reset.
5. When the RUN indicator comes on solid, the unit is set to factory default.

4. CONTROLS AND INDICATORS

4.1 Controls

A pushbutton switch to invoke serial port setup is accessible through a small hole on the rear of the unit. Use a paper clip to press the switch.

4.2 Indicators

Indicator	Condition	Meaning
LAN	Yellow	10 MB LAN connection
	Green	100 MB LAN connection
DCD On	ON	COM 2 DCD is ON
Run	ON	Unit has power and is working properly
	Flash	Serial Setup Mode active
Encrypting	ON	Encryption is enabled
Com1 Tx	ON	Serial data out COM 1
Com2 Tx	ON	Serial data out COM 2

5. CONFIGURATION & MANAGEMENT

5.1 Introduction

Initial setup of the SSE is accomplished using serial port Com1. After initial configuration, a web browser or Telnet connection may be used if the unit was configured for LAN operation.

5.2 Connections and Setup

The SSE can be set up through serial port Com1. Connect a PC to serial port 1 using the cable provided. If an asynchronous terminal is used, a null modem cable is required

Use an asynchronous terminal or a PC using a communications program such as HyperTerminal. Set the terminal to 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

Press the Setup switch through the hole in the rear of the case. Pressing the switch will bring up the following screen:

5.3 Serial Mode and Telnet Setup Screens

```
Serial Encrypter V1.0
-----------------------------------------

 Configuration setup.

[Press any key to continue]
```

After pressing any key:

```
 Main Menu
-------------------------------------------
 1  Set LAN Configuration,
 2  Serial Port Configuration
 3  Cipher Configuration
 4  Configuration Access
 5  Display Configuration Settings
 6  Algorithms Test
 7  Reset Configuration to Default
 8  Save and Exit
 0  Exit without Saving

Choose a Number =>
```

To make configuration changes in the following screens, enter the number of the item to change followed by a space and the number of the new setting. When finished, select item 8, Save and Exit, from the main menu.

5.3.1 Set LAN Configuration

```
LOCAL UNIT CONFIGURATION:
 Local Address: 205.166.54.254       MAC Addr: 00:60:E9:02:60:CB
 Gateway Address: (NOT SET)          Subnet Mask: 255.255.255.0


SET LOCAL UNIT CONFIGURATION:
 1  Local IP Address
 2  Gateway IP Address
 3  Subnet Mask
 0  -- Return to previous menu

EXAMPLE: To set local IP address to 192.168.0.10
   => 1 192.168.0.10

Enter Command =>
```

5.3.2 Serial Port Configuration

```
SERIAL PORT CONFIGURATION:
 Baud Rate:        38400
 Baud Offset:      0
 Parity:           NONE
 Stop:             1 Bit
 COM1 Interface:   rs232
 COM2 Interface:   rs232
 Operational Mode: Point-to-Point

SET SERIAL PORT CONFIGURATION:
 1  Baud Rate         [0=57600, 1=38400, 2=19200, 3=9600
                       4=4800,  5=2400,  6=1200,  7=600,  8=300]
 2  Baud Offset       [0=-2.4%, 1=-1.2%, 2=0, 3=+1.2%, 4=+2.4%]
 3  Parity bit        [0=None, 1=Odd, 2=Even, 3=Mark, 4=Space]
 4  Stop bits         [0=1bit, 1=2bits]
 5  COM1 Interface    [0=rs232, 1=rs485/4-wire]
 6  COM2 Interface    [0=rs232, 1=rs485/4-wire]
 7  Operational Mode  [0=P2P, 1=MP-Master, 2=MP-Slave]
 0  -- Return to previous menu.
EXAMPLE: To set the baud rate to 9600
   => 1 3

Enter Command =>
```

5.3.3 Cipher Configuration

```
CIPHER CONFIGURATION:
 Encrypt/Decrypt: enabled
 AES Key Size:    128-bits
 AES Key: 00000000000000000000000000000000

SET CIPHER CONFIGURATION:
 1  Encrypt/Decrypt   [0=disabled, 1=enabled, 2=DCD2 enabled,
                       3=DCD1 & DCD2 enabled]
 2  AES Key Size      [0=128-bits, 1=192-bits, 2=256-bits]
 3  AES Key
 4  Key Control       [0=Hide, 1=Show/Randomize]
 0  -- Return to previous menu.
EXAMPLE: To set the AES Key
   => 3 0123456789abcdef

Enter Command =>
```

5.3.4 Configuration Access

```
CONFIGURATION ACCESS:
 Web Configuration:    ENABLED
 Telnet Configuration: ENABLED
 Firmware Upgrade:     ENABLED
 User ID:
 Password:

SET CONFIGURATION ACCESS:
 1  Web Configuration    [0=ENABLED, 1=DISABLED]
 2  Telnet Configuration [0=ENABLED, 1=DISABLED]
 3  Firmware Upgrade     [0=ENABLED, 1=DISABLED]
 4  Set User ID and Password [userid password]
 5  Clear User ID and Password
 0  -- Return to previous menu

EXAMPLE: To set User ID to root, password toor
   => 4 root toor

Enter Command =>
```

5.3.5 Display Configuration Settings

```
Serial Encrypter: V1.0

LOCAL UNIT CONFIGURATION:
 Local Address: 205.166.54.254       MAC Addr: 00:60:E9:02:60:CB
 Gateway Address: (NOT SET)          Subnet Mask: 255.255.255.0


SERIAL PORT CONFIGURATION:
 Baud Rate:        38400
 Baud Offset:      0
 Parity:           NONE
 Stop:             1 Bit
 COM1 Interface:   rs232
 COM2 Interface:   rs232
 Operational Mode: Point-to-Point

[Press any key to continue]

CIPHER CONFIGURATION:
 Encrypt/Decrypt: enabled
 AES Key Size:    128-bits
 AES Key: 00000000000000000000000000000000

CONFIGURATION ACCESS:
 Web Configuration:    ENABLED
 Telnet Configuration: ENABLED
 Firmware Upgrade:     ENABLED
 User ID:
 Password:

[Press any key to continue]

CURRENT STATISITCS:
 Network packets received:    10676
 Network packets transmitted: 270
 Network packet errors:       0
 COM1 bytes received: 6584920
 COM2 bytes received: 6584936

[Press any key to continue]
```

5.3.6 Algorithms Test

```
ALGORITHM TESTS:
 Time Source..........OK
 AES PRNG Test.........Passed
 AES Key Test.........Passed

[Press any key to continue]
```

5.4 Ethernet Management

For a connection directly to a PC, use an Ethernet crossover cable. DCB part number 9500097. If connecting to an Ethernet hub or switch, use a straight through Ethernet cable. (Patch Cord)

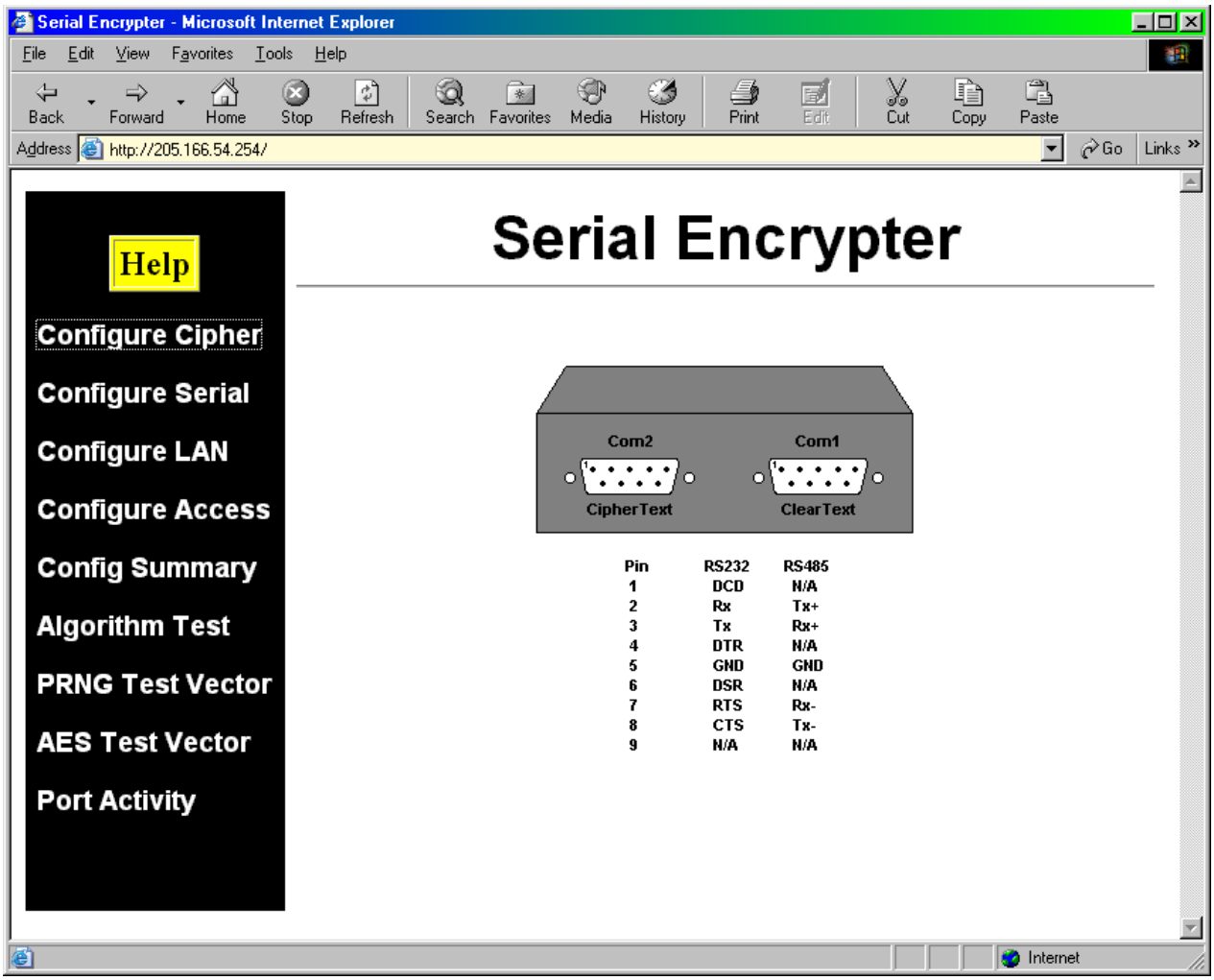
5.4.1 Telnet

Telnet screens are identical to the serial screens

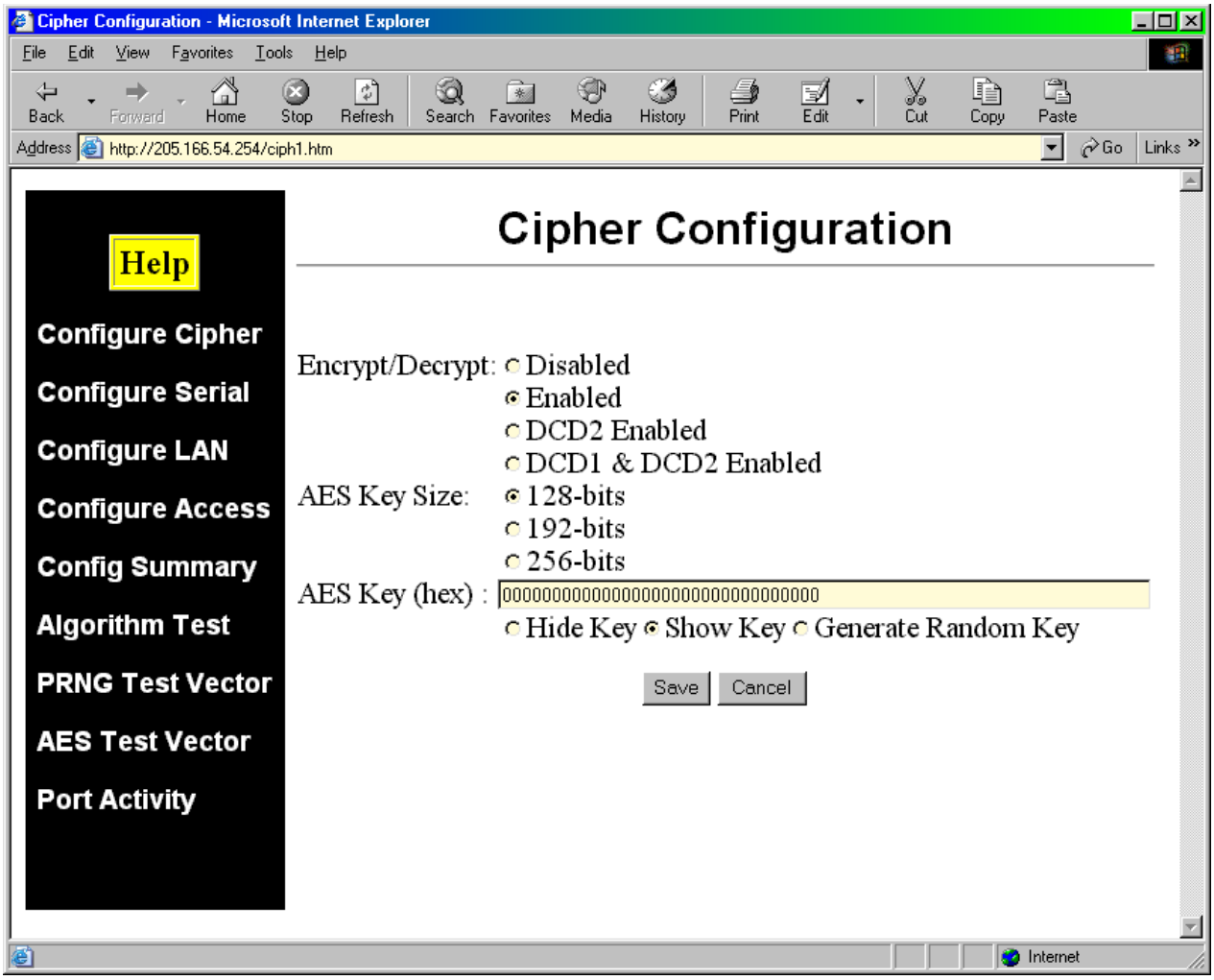
5.4.2 Browser screens:

NOTE
Context sensitive HELP is available for each browser screen.

Main screen

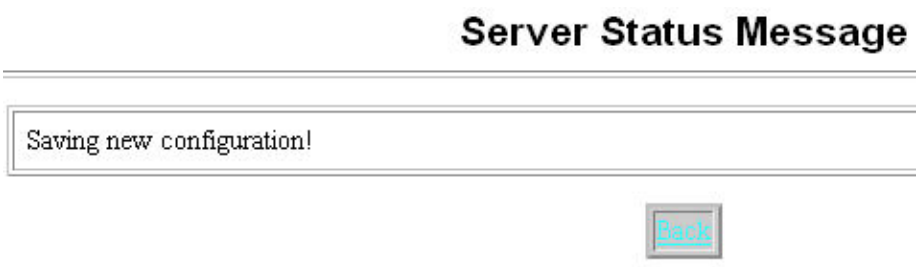


Configure Cipher screen

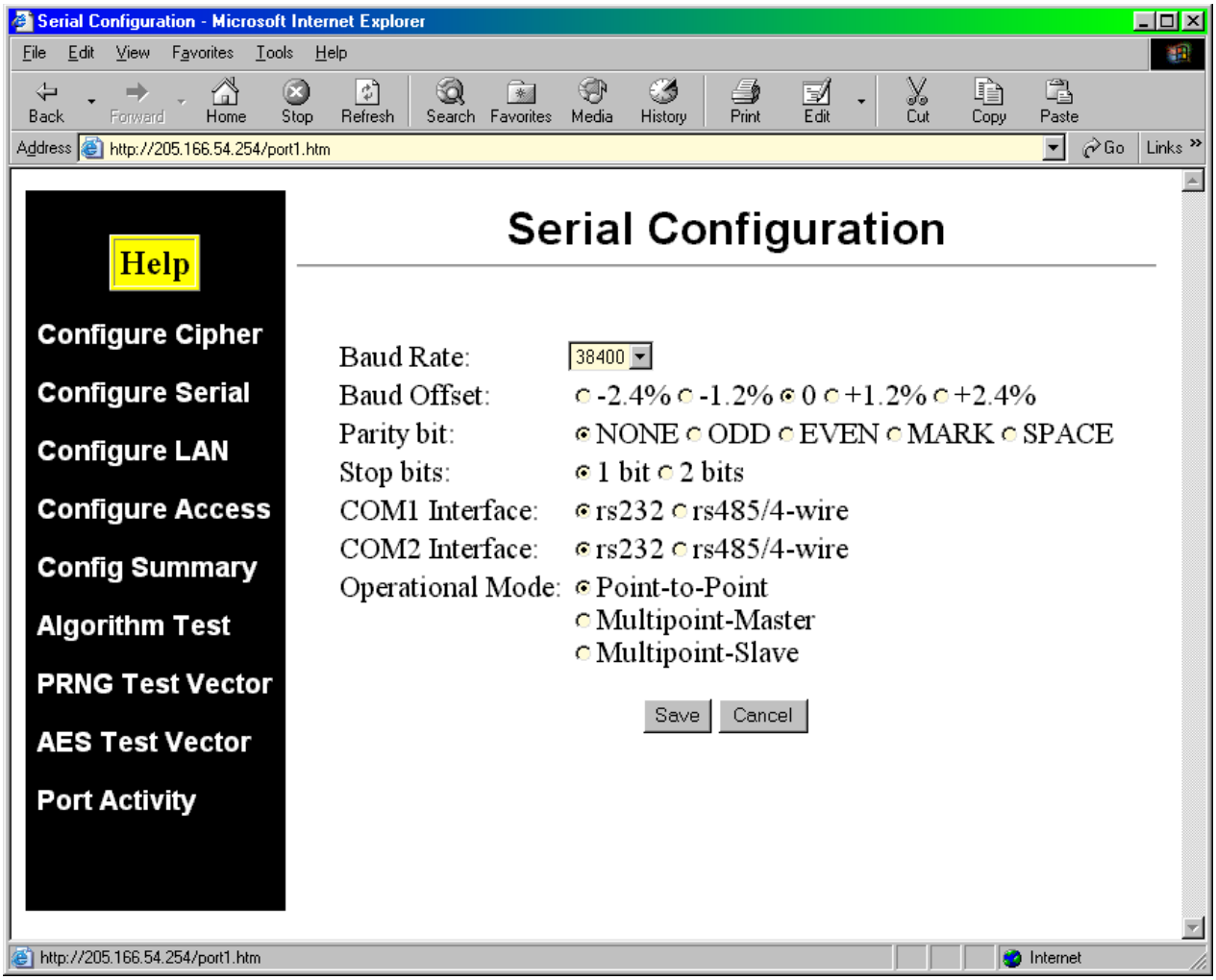


While the SSEs will work right out of the box it is suggested that the AES Key be changed to provide adequate security. The easiest way to do this is to select Generate Random Key in the above screen and click Save. After the configuration is saved, click Back to view the randomly generated key. Now Copy the key and Paste it into all other SSEs that will operate on the same network.

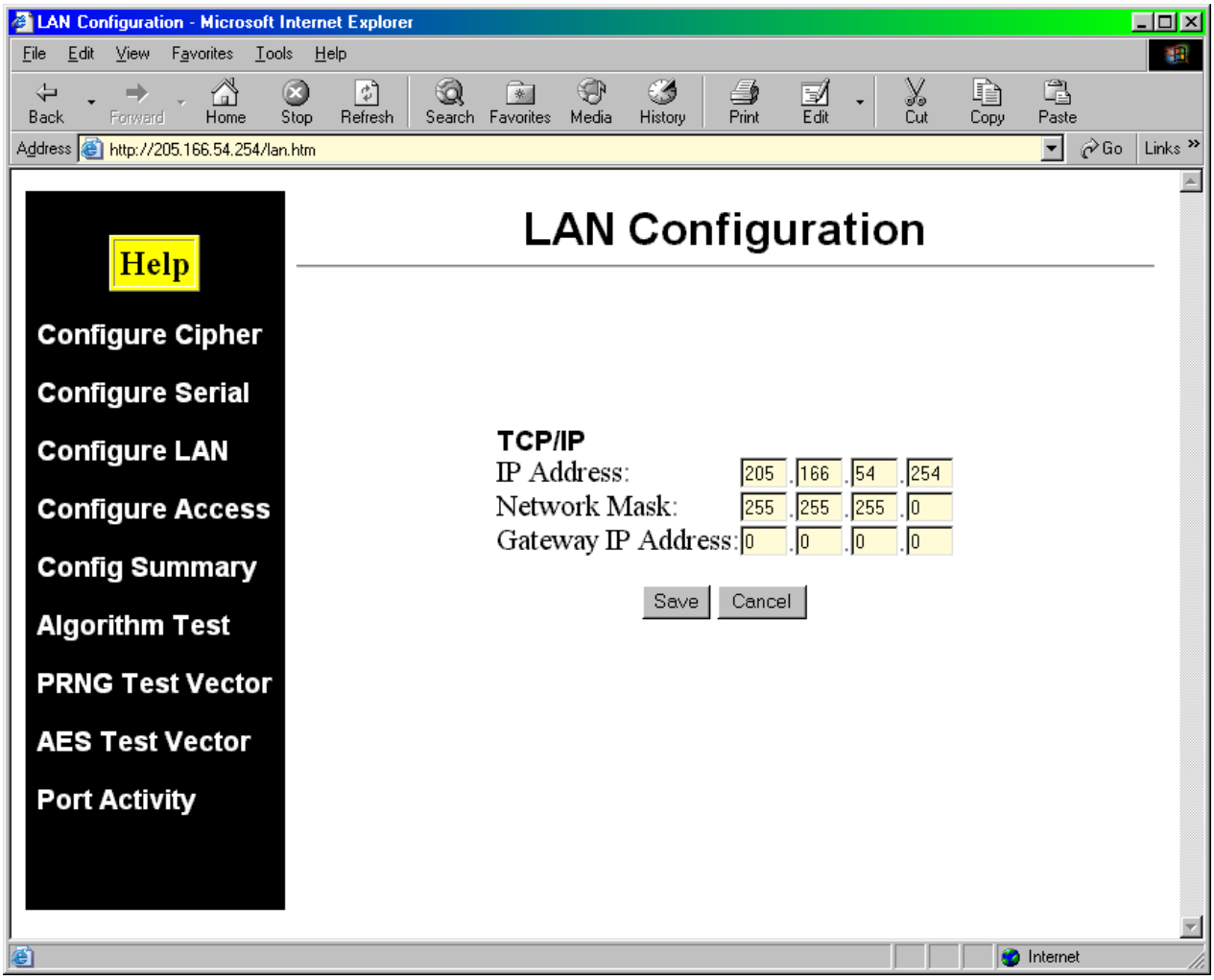
Save screen



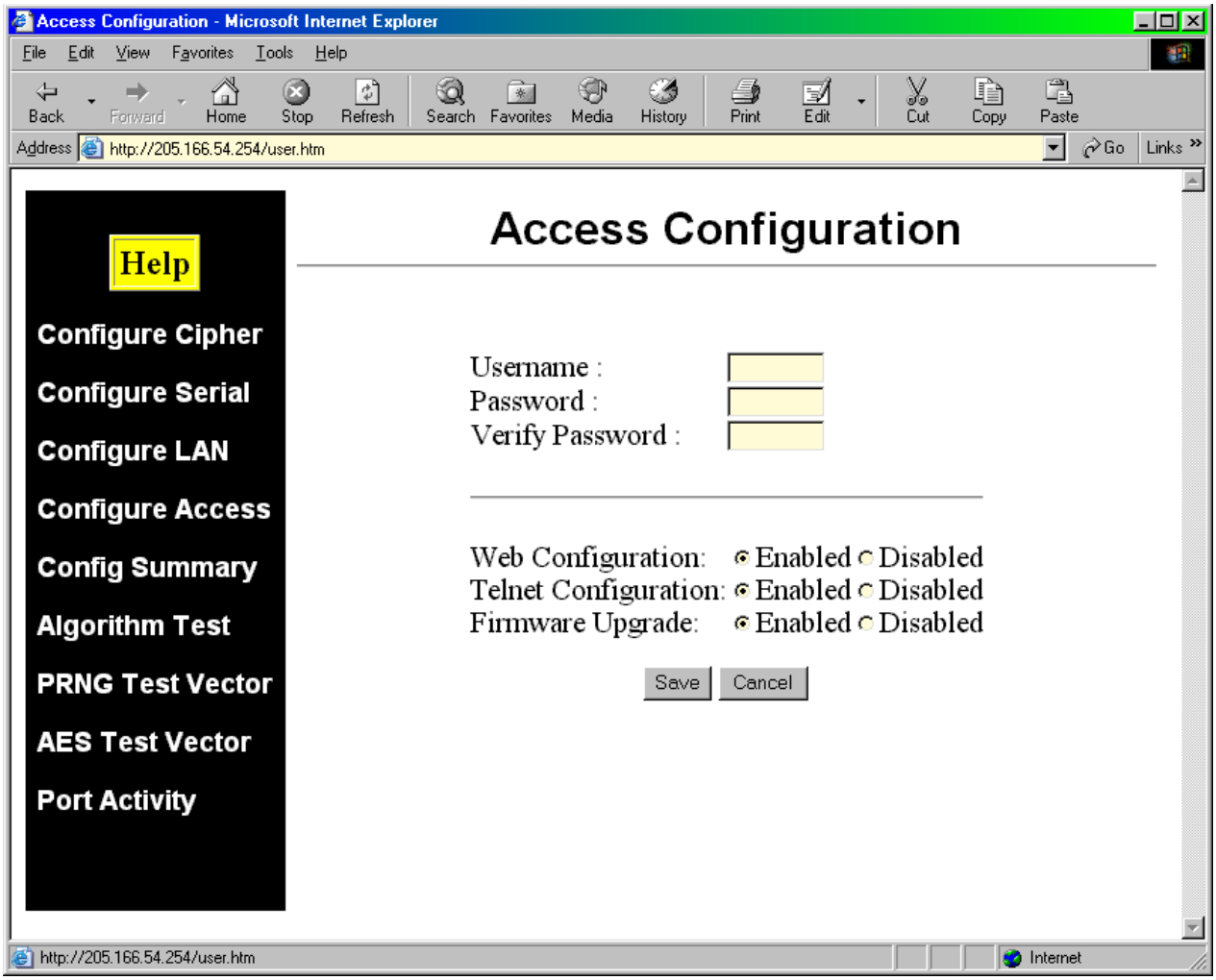
Configure Serial screen



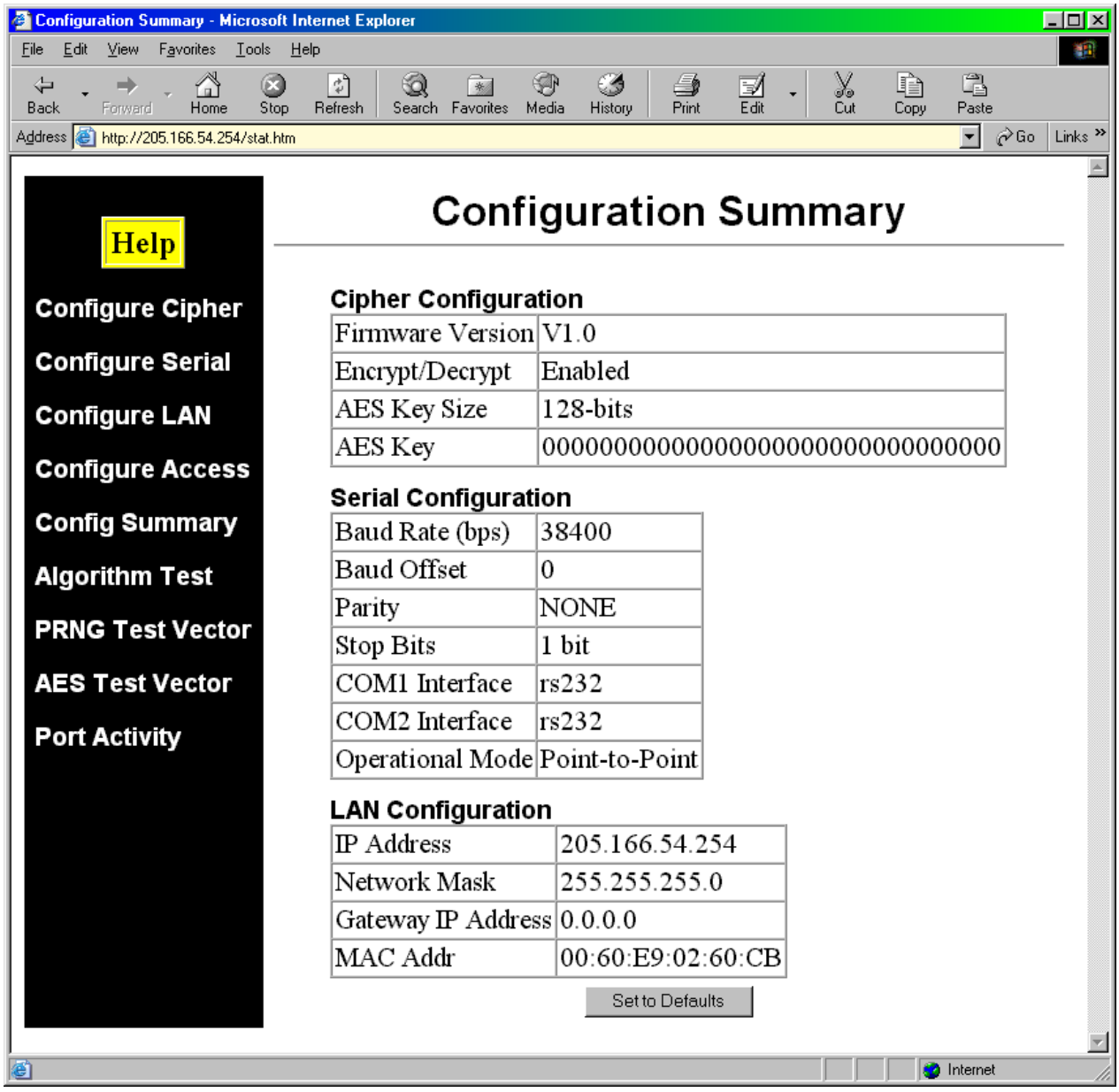
Configure LAN screen



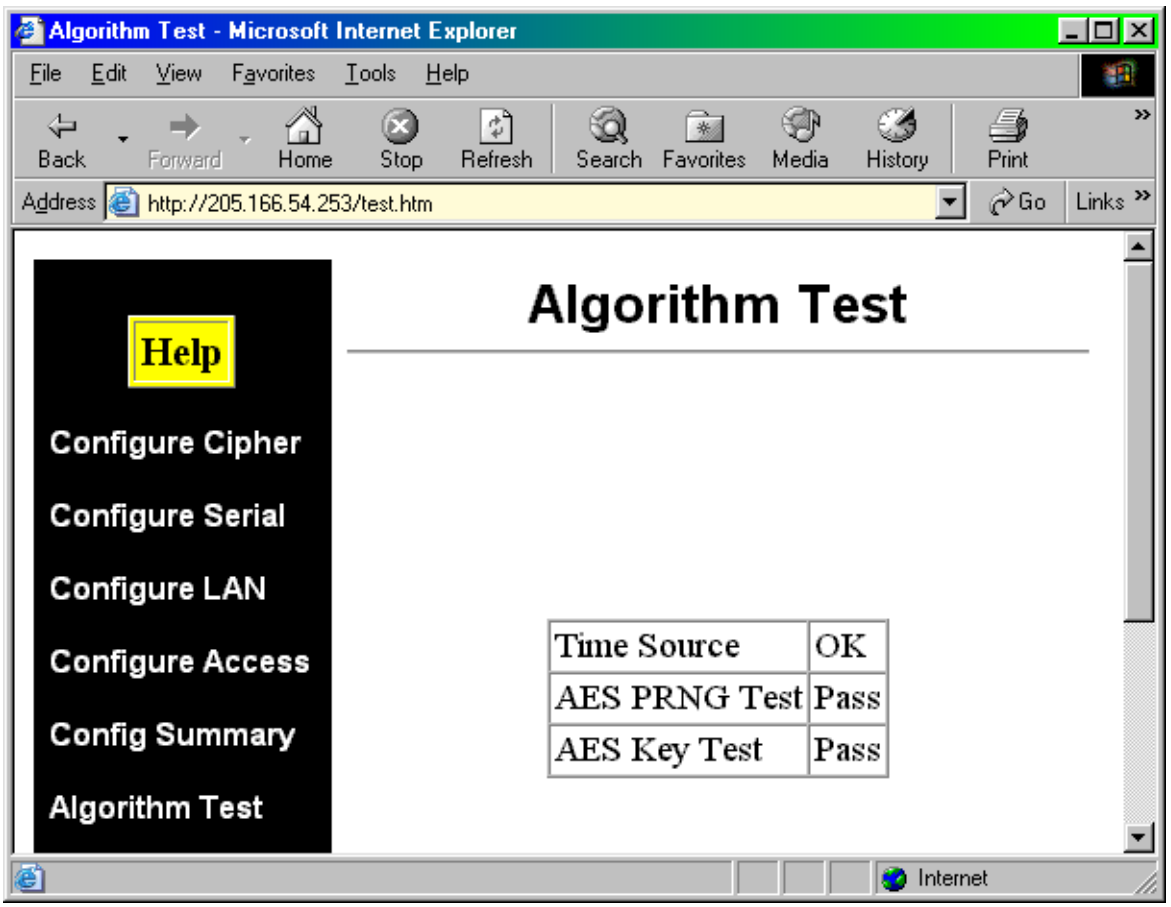
Configure Access screen

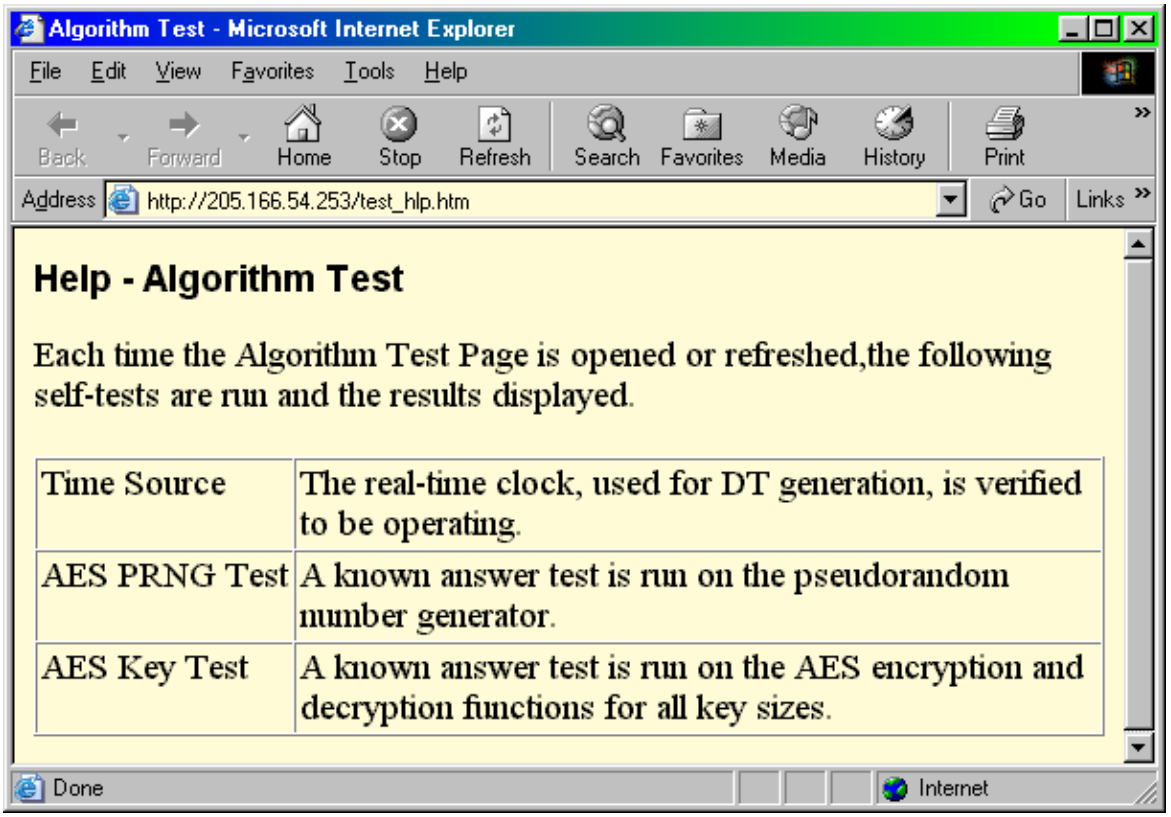


Configuration Summary screen

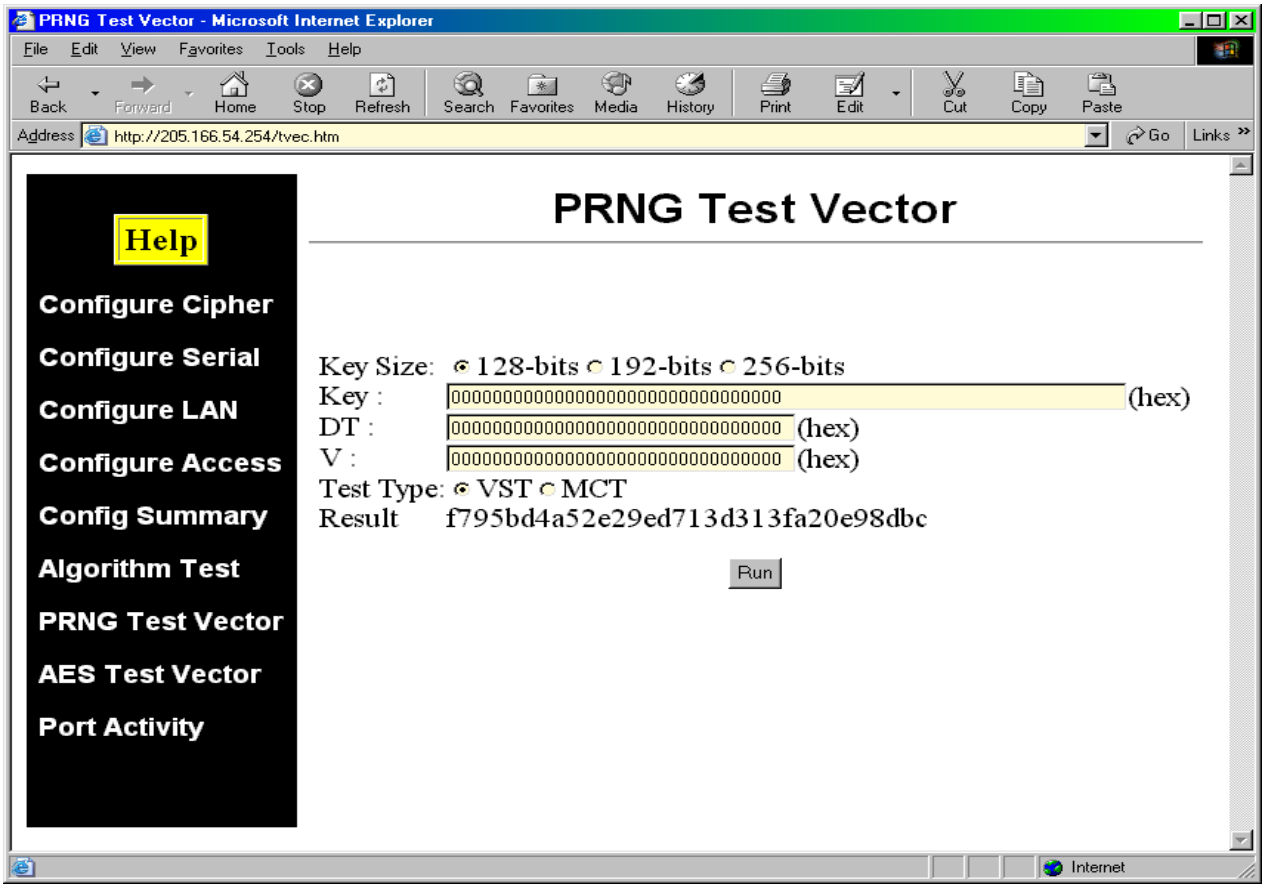


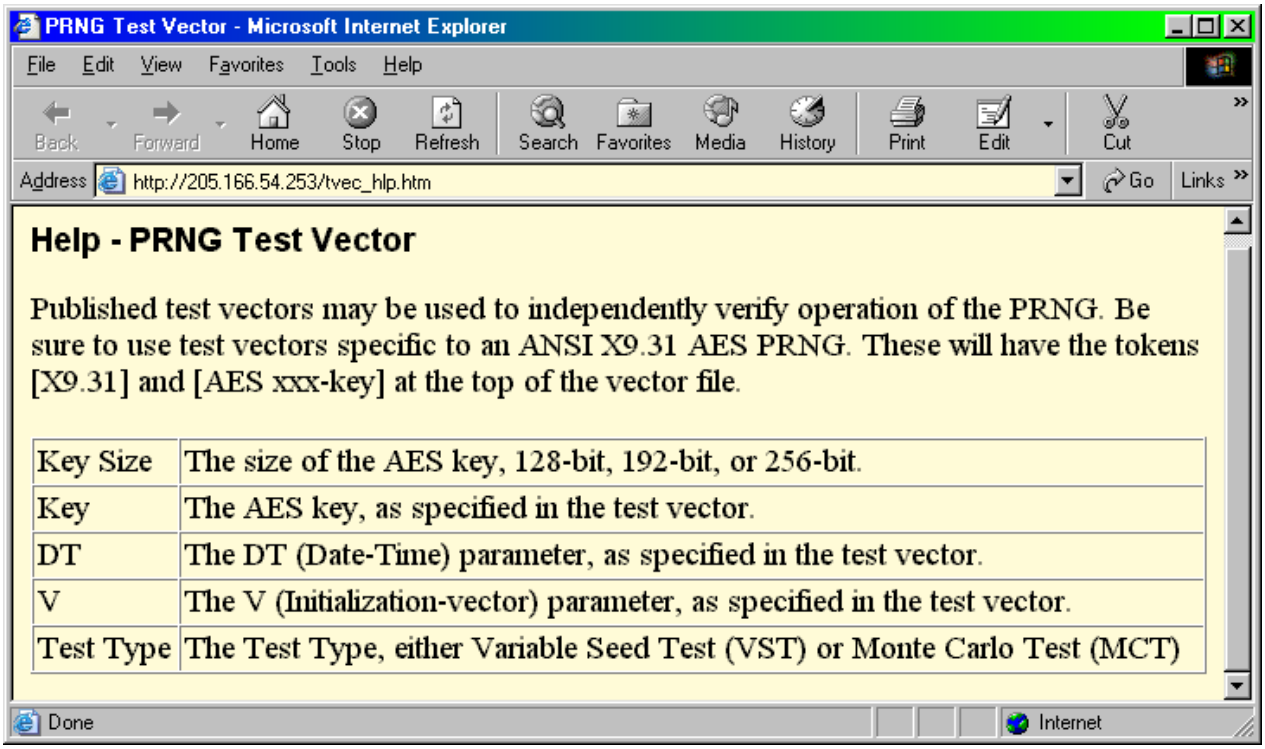
Algorithm Test screen



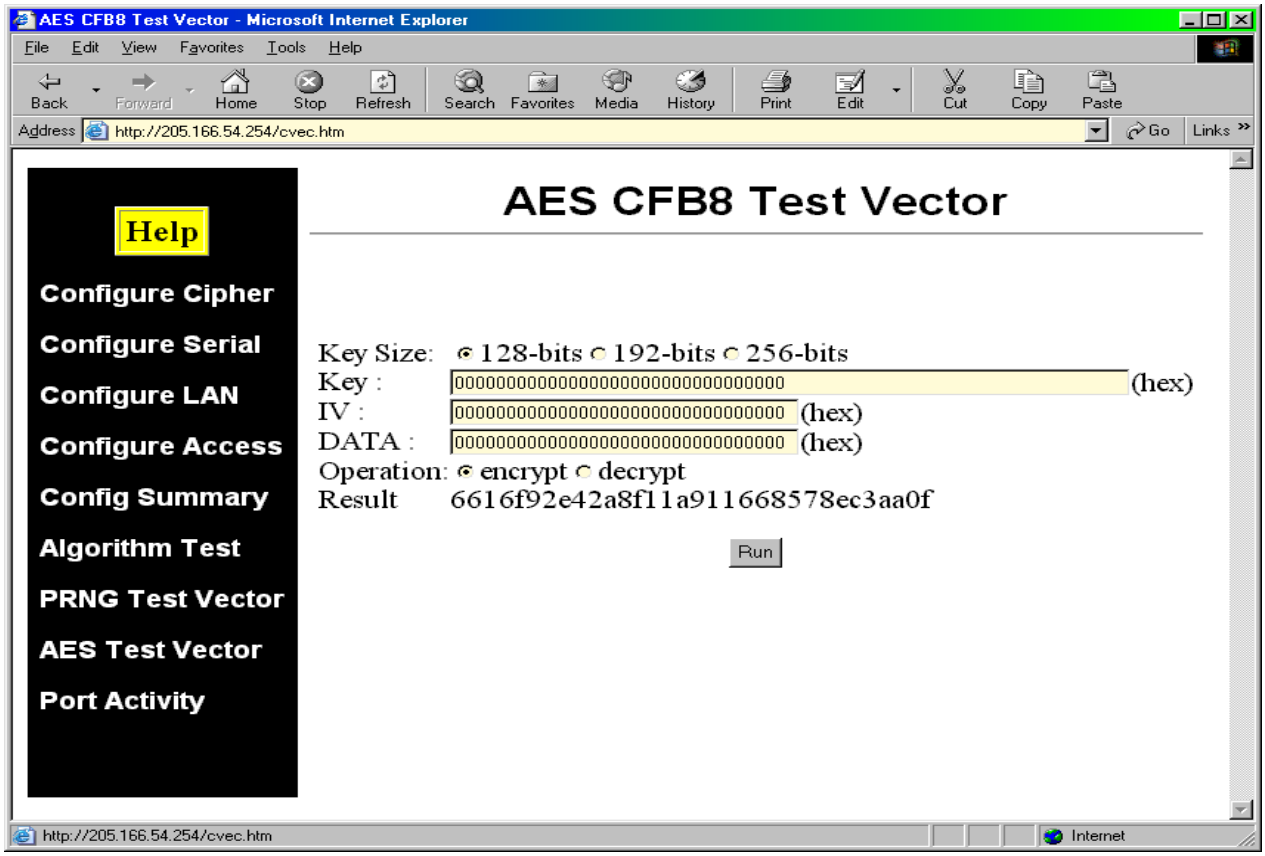


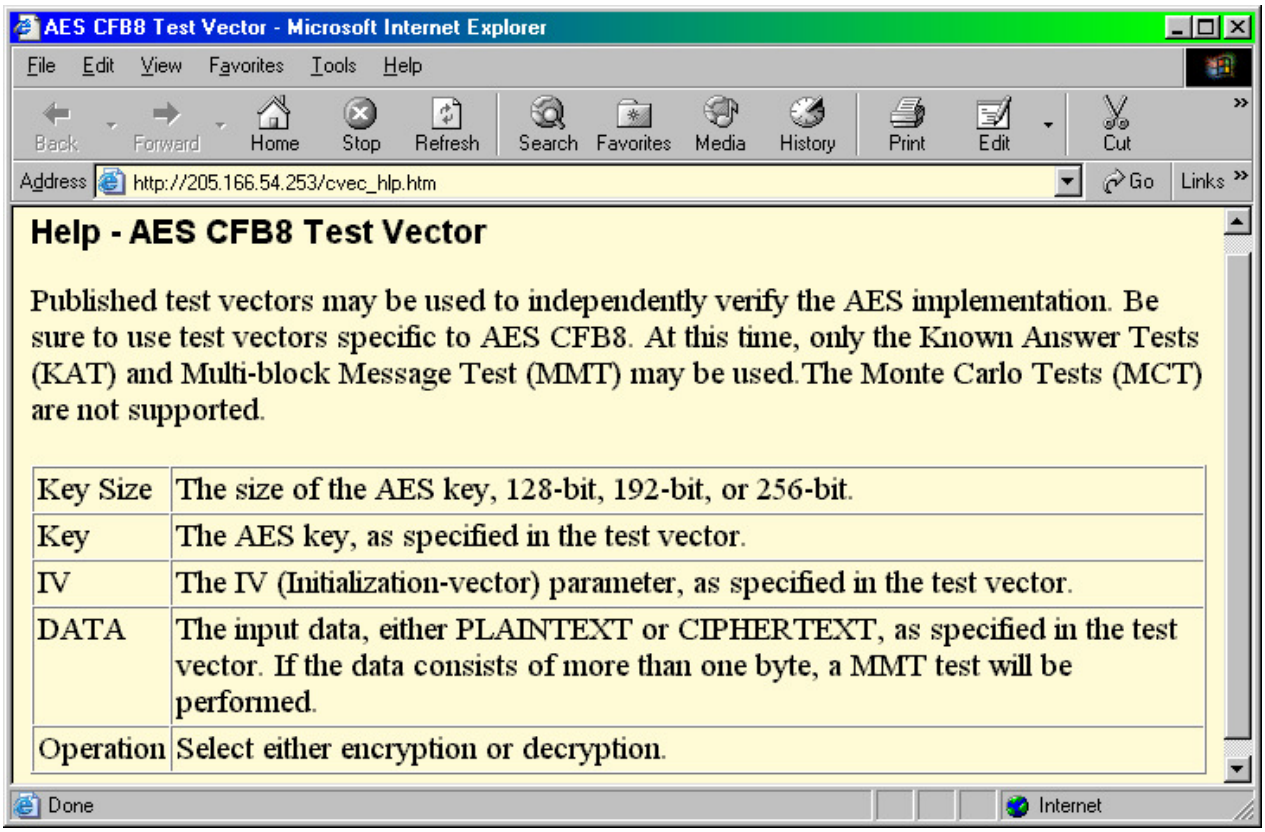
PRNG Test Vector screen



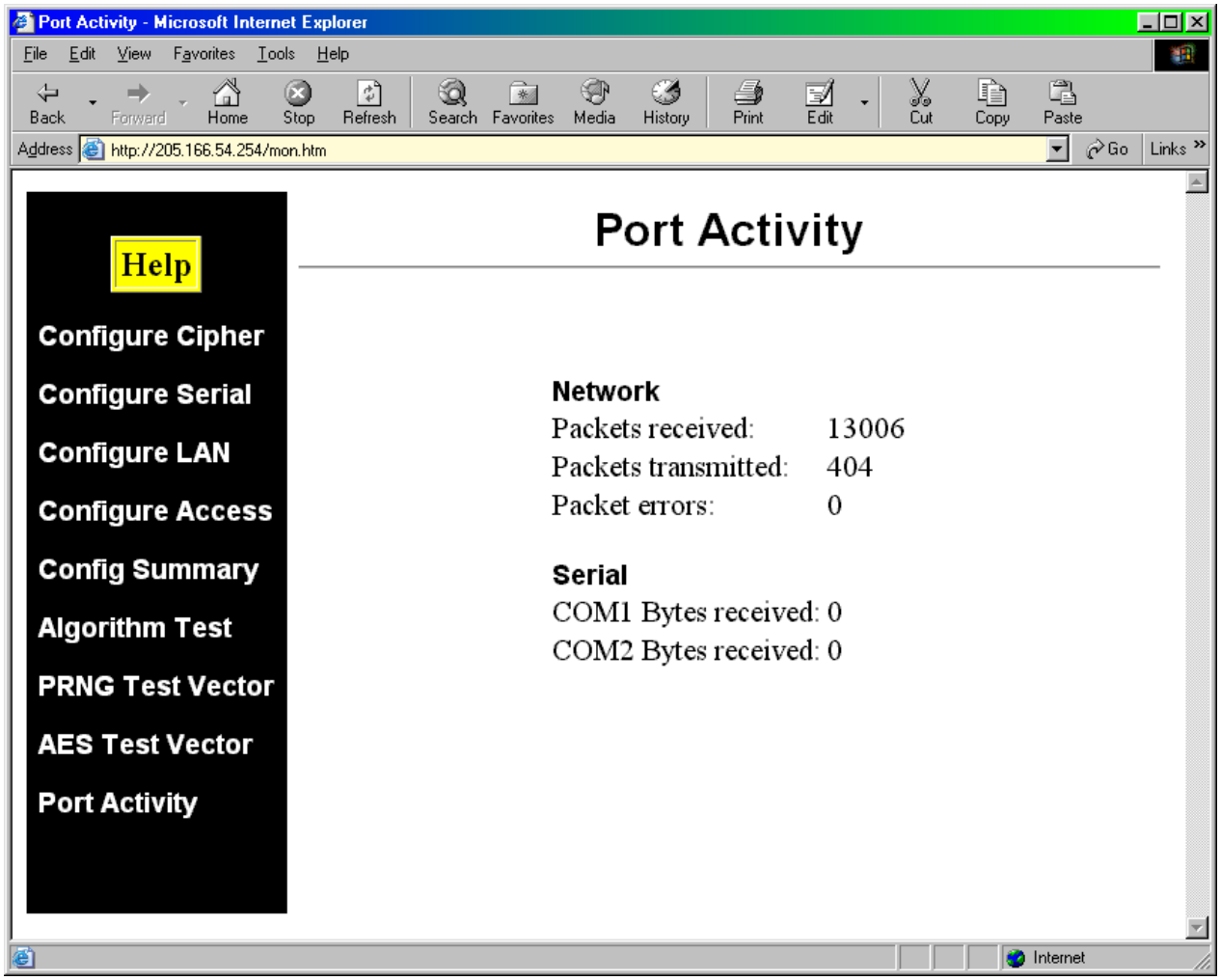


AES Test Vector screen





Port Activity screen



6. INTERFACE SIGNALS AND CABLING

6.1 Introduction

The serial ports on the SSE can be either RS 232 or RS 485 (4-wire). The configuration is changed using the serial port configuration menu.

The default setting is RS 232.

6.2 RS-232 Port Interface (DE-9P)

Pin	Signal	In/Out
1	Carrier Detect	IN
2	Receive Data	IN
3	Transmit Data	OUT
4	Data Terminal Ready	OUT
5	Signal Ground	----
6	Data Set Ready	NOT USED
7	Request to Send	OUT
8	Clear to Send	IN
9	NOT USED	

6.2.1 Internal RS-232 Signal Paths Through the SSE

Com 1		Com 2
TxD<	---------->	<RxD
RxD>	---------->	TxD
RTS<	---------->	<CTS
CTS>	---------->	RTS
DTR<	---------->	<DCD
DCD>	---------->	DTR
DSR	Ignored	DSR

6.3 RS-485 4-Wire Interface (DE-9P)

Pin	Signal	In/Out
1	NOT USED	
2	Tx+	OUT
3	Rx+	IN
4	NOT USED	
5	Ground	----
6	NOT USED	
7	Rx–	IN
8	Tx–	OUT
9	NOT USED	

6.4 Cables

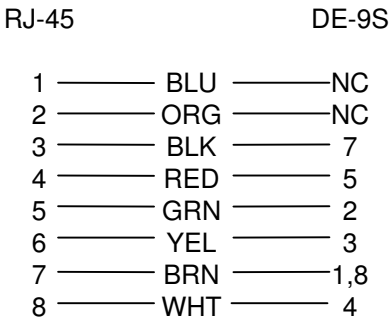
The RS-232 serial ports on the SSE are configured as Data Terminal Equipment (DTE). This is the same configuration used on PC COM ports. To connect the SSE to peripheral equipment, use the same cable that would be used to connect that equipment to a PC COM port.

6.4.1 To connect the SSE clear side port (Com 1) to a PC COM port, use the serial cable provided.

6.4.2 To connect the SSE encrypted side port (Com 2) to a 25 pin modem device, use an IBM modem cable. Available from DCB as P/N 9801009.

6.4.3 To connect the SSE encrypted side port (Com 2) to a 9 pin modem device, use a straight through 9 pin male to female cable. Available from DCB as P/N 9801022.

6.4.4 To connect the SSE to a DCB SR / SR 4 Series Multiplexer Composite port, use the following cable. Adapter available from DCB as P/N 9802067



6.4.5 To connect two SSEs back-to-back for bench testing, use the serial port setup cable provided.

7. TROUBLESHOOTING

When troubleshooting problems, a rational plan can save you many hours of frustration. The following is a brief outline of standard troubleshooting procedures.

1. Gather the facts to determine the exact nature of the problem.
2. Draw a picture of the system showing the equipment at both the host and remote ends and the phone lines or in-house wiring. Use this as a reference to note your observations, test steps and test results. A picture keeps you focused and often saves duplicate effort.
3. Record the front panel indications before changing anything. This is an important part of fact gathering
4. If you change anything, change only one thing at a time.
5. Record your results.

8. WARRANTY

This DCB product is warranted to be free of defects in materials and workmanship for two years. Data Comm for Business, Inc. will repair or replace any equipment proven to be defective within the warranty period. All warranty work is F.O.B. Champaign, IL. This warranty is exclusive of abuse, misuse, accidental damage, acts of God or consequential damages, etc. DCB liability shall not exceed the original purchase price.

All equipment returned for repair must be accompanied by a Returned Material Authorization (RMA) number. To receive an RMA number, call (217) 897-6600 between the hours of 8 AM and 5 PM central time. Equipment must be shipped prepaid to DCB and will be returned at DCB's expense.

Ship returned items to:

Data Comm for Business
2949 County Road 1000E
Dewey, IL 61840
ATTN: RMA (number)

Data Comm for Business, Inc.
PO Box 6329
Champaign, IL 61826-6329

Tel (217) 897-6600
Fax (217) 897-1331
Email support@dcbnet.com