

## TABLE OF CONTENTS

Introduction .....	1
Getting Started .....	2
825 Crypto Net Commands.....	5
825 Crypto Net Registers .....	6
Appendix A: Parity and Encryption Keys .....	8
Technical Support .....	11

## **Introduction**

The Western DataCom 825 Crypto Net (henceforth referred to as the CN) is a synchronous link-encryption device designed to accept HDLC/SDLC framed data. It uses the NIST approved DES encryption algorithm proven to be successful in the private sector, government, and financial institutions for 15 years.

The Crypto Net is installed between the telco equipment and the communications hardware and requires no changes to existing DCE equipment. The unit's DTE port can be factory configured for either V.35 or RS-232 and can operate at up to 256,000 bps. The DCE port can also be factory configured for either V.35 or RS-232 and can operate at up to 64,000 bps. The 825 also features an asynchronous control port for setup, configuration of registers, and entering of encryption keys.

# Introduction

## Introduction

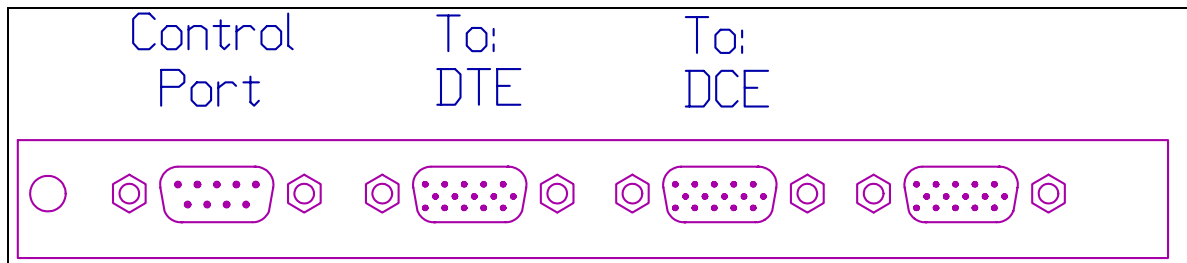


Figure 1: 825 Crypto Net Backpanel

## Installation

### 1. Unpacking/Checklist

825 CNs are shipped in one of two ways depending on whether they are ordered alone or with the Western Datacom WA 1602 stand-alone chassis. Unpack the contents of the shipping carton.

If the 825 CNs were ordered alone, then in addition to this manual each unit should have the following:

- 1 825 Crypto Net
- 1 HD15 male-to-V.35 female cable
- 1 HD15 male-to-V.35 male cable
- 1 DB9 male-to-DB25 female cable
- 1 Warranty Card

#### If ordered with Western DataCom 1814 DSU/CSU

- 1 825 Crypto Net
- 1 HD15 male-to-DB25 male cable
- 1 HD15 male-to-V.35 female cable
- 1 DB9 male-to-DB25 female cable
- 1 Warranty Card

If the 825 CNs were ordered with the WA 1602 chassis, then in addition to the above, each unit will contain the WA 1602 chassis with the 825 CN already mounted, and the power supply.

### 2. Mounting

The 825 CN is a rack-mount card design which is compatible with the Racal Vadic MDS-1 series chassis. Mount according to the following directions.

## Getting Started

**NOTE:** The 825 CNs should be mounted into the chassis with the POWER OFF. If one or more CNs are already mounted in a chassis and the power is ON, make sure to shut the power OFF before mounting any other 825 CN units into that chassis.

2 SLOT CHASSIS If the 825 CN was purchased with the WA 1602 chassis and you have just unpacked from the shipping carton, it is already mounted. Skip this step and go on to step 3. If the CN has been removed, re-mount according to the directions for the 4 slot chassis below.

4 SLOT CHASSIS To mount the CN in a 4-slot chassis, place it horizontally into a slot on the chassis, edge connector first. Carefully guide the circuit board along the set of plastic runners on the left and right side of the slot in the chassis. Continue to slide the unit forward until you feel the edge connector clamp into place. Tighten thumbscrew.

16 SLOT CHASSIS To mount the CN in a 16-slot chassis, place it vertically into a slot on the chassis, edge connector first. Carefully guide the circuit board along the set of plastic runners on the top and bottom of the slot in the chassis. Continue to slide the unit forward until you feel the edge connector clamp into place. Tighten thumbscrew.

### 3. Connection to Control Port

An RS-232 control port is provided on the back of the 825 CN for configuration, control, and monitoring of the CN from an ASCII terminal or a PC which is running terminal emulation software. The configuration for the control port is 9600 baud, 8 data bits, no parity. Set the control terminal to this configuration.

The control port is the DB9 connector mounted on the extreme left of the CN backpanel. Refer to 1. A DB9 male-to-DB25 female control cable is provided to allow the control port to be connected to a standard straight-thru RS-232 cable(not provided) from the control terminal.

To connect to the control port, take the DB9 male end of the control cable and plug it into the control port. Plug the DB25 male end of the RS-232 cable coming from your terminal or Com port into the opposite end(DB25 female) of the control cable.

### 4. Connection to DTE port

Make sure that power to the unit is OFF. Select the HD15 male-to-V.35 female cable. Plug the HD15 male end into the left most HD15 female connector on the backpanel, the connector to the immediate right of the control port. See 1. Plug the other end into the V.35 DTE.

### 5. Connection to DCE port

The CN backpanel provides two HD15 female connectors on the backpanel for connection to DCEs. See 1. With the backpanel facing you, the second HD15 connector from the right is the main DCE port and the extreme right connector is the backup port.

## **Getting Started**

To connect to the DCE, first make sure that power to the unit is OFF. Take the HD15 male-to-V.35 male cable and plug the HD15 male end into the main port(the second HD15 connector from the right). Plug the V.35 male end into the DCE.

NOTE: The backup port should not be used at this time.

This completes the installation procedure.

## **Getting Started**

## Getting Started

Configuration and control of the CN is through a command line interface. The commands should be entered at the COMMAND> prompt. The commands are not case sensitive although they are shown in upper case here. Therefore SHOW, Show, and show will all be interpreted as the same keyword.

### **The Show commands:**

SHOW ID

Displays 8 character ID string.

SHOW S/N

Displays unit serial number.

SHOW REGS

Displays all registers in a tabular format.

SHOW REG *n*

where *n* is the register number. Displays the contents of the register.

### **The Set commands:**

SET ID *string*

where *string* is an 8 character, alphanumeric string. This string is stored in EEROM. It allows user to identify unit.

SET REG *n v*

where *n* is the register number and *v* is the register value.

SET KEY *key*

where *key* is a string of 16 hexadecimal digits. The parity of the entire string must be odd(See description of parity). This command sets the encryption key.

### **The Initialize command:**

INIT REGS

Copies factory default values to all registers.

INIT KEY

Copies factory default key to the storage area.

The factory default key is: 0123456789ABCDEF

## **825 Crypto Net Commands**

## 825 Crypto Net Commands

### REG 0 - DTE Port Speed

- 0 = 56K (Factory default)
- 1 = 64K
- 2 = 96K
- 3 = 128K
- 4 = 192K
- 5 = 256K

This register sets the DTE port speed( the DTE port sources clocks and the DCE port accepts clocks).

NOTE: Changes to this register do not take effect while the unit is on-line, it must be disconnected.

### REG 1 - Bitmapped

BIT	VAL	DEFAULT	User
b7	128	x0=000	
b6	64	x0=000	
b5	32	x0=000	
b4	16	x0=000	
b3	8	x0=000	
b2	4	x1=004	
b1	2	x1=002	
b0	1	x0=000	

=006

bit 0 - Data encoding  
 = 0 NRZ encoding  
 = 1 NRZI encoding

bit 1 - Idle character  
 = 0 Mark idle (FF hex)  
 = 1 Flag idle (7E hex)

bit 2 - TXC clock gap  
 = 0 Disable clock gapping on TXC  
 = 1 Enable clock gapping on TXC

Clock gapping is a hardware technique for implementing flow control in a synchronous environment. Since the CN sources the transmit clock to the DTE and consequently controls the data flow from the DTE, it can effectively halt the flow of data at any instant by holding the clock signal in the state that it is in at that instant, i.e. not allowing transitions. Please note this option should be disabled.

If the DTE being used does support this action, the maximum allowable throughput can be achieved by enabling this option and setting the DTE port speed(Reg 0) to maximum. Now

## 825 Crypto Net Registers

when the CN's DTE transmit buffer fills, the clock is stopped, then restarted when the buffer has room for data again. The net effect is a variable duty cycle clock which tracks the actual throughput rate.

### REG 2 - Bitmapped

BIT	VAL	DEFAULT	User
b7	128	x0=000	
b6	64	x0=000	
b5	32	x0=000	
b4	16	x0=000	
b3	8	x0=000	
b2	4	x0=000	
b1	2	x0=000	
b0	1	x0=000	

=000

#### bit 0 - DTE port's DTR control

= 0 Use DTR signal from DTE

= 1 Ignore DTR signal from DTE

## 825 Crypto Net Registers

This appendix describes parity and its relationship to construction of encryption keys on the Western Datacom 825 Crypto Net.

Data to be transmitted in encrypted format is coded at one end of the line and decoded at the other end before being presented to the DTE. The coding is performed using a unique codeword known as the *working key* that is generated randomly and agreed upon by the two sides during the connection process. The working key is derived from the *encryption key*, which is what gets constructed and entered into the Crypto Net by the user.

The encryption key is defined in the hexadecimal(base 16) number system, which is closely related to the binary(base 2) number system. This relationship will be important to the user who will be defining and storing encryption keys on the 825 CN. The following conversion chart is included as an aid in determining parity.

HEX	BINARY	HEX	BINARY
0	= 0000	8	= 1000
1	= 0001	9	= 1001
2	= 0010	A	= 1010
3	= 0011	B	= 1011
4	= 0100	C	= 1100
5	= 0101	D	= 1101
6	= 0110	E	= 1110
7	= 0111	F	= 1111

To understand parity, first notice how each hex digit converts to four binary digits, which are also known as **bits**. Each bit is either a **1** or a **0**. Parity here simply refers to the number of **1's** in the bit string. If a bit string has an odd number of **1's** it is said to have **odd parity** and if it has an even number of **1's** it is said to have **even parity**. Please note that there is no correspondence between the parity of a binary representation of a number and the concept of even and odd numbers. Numbers like 2, 4, and 8 are even numbers but have odd parity(count the number of **1's**) when expressed in binary form. Numbers like 3, 5, 9 are odd numbers but have even parity(again, count the number of **1's**) when expressed in binary form.

A string of eight bits is referred to as a **byte**. Since hex digits are four bits each, each pair of them would be one byte.

### EXAMPLES:

1. Hex number 9C = <sup>9</sup>1001 <sup>C</sup>1100 = 10011100 (size = 1 byte)
2. Hex number E7 = <sup>E</sup>1110 <sup>7</sup>0111 = 11100111 (size = 1 byte)
3. Hex number D5 = <sup>D</sup>1101 <sup>5</sup>0101 = 11010101 (size = 1 byte)

## 825 Crypto Net Registers

The concept of the parity of a hex digit may be extended to pairs of hex digits, but the situation changes somewhat. The examples above are repeated below with parity indications added. Notice what happens to the parity of a pair of hex digits when combined to form a byte.

### EXAMPLES:

1. Hex number 9C =  $\begin{matrix} 9 & C \\ 1001 & 1100 \\ \text{even} & \text{even} \end{matrix}$  = 10011100 (size = 1 byte)  
**even**

2. Hex number E7 =  $\begin{matrix} E & 7 \\ 1110 & 0111 \\ \text{odd} & \text{odd} \end{matrix}$  = 11100111 (size = 1 byte)  
**even**

3. Hex number D5 =  $\begin{matrix} D & 5 \\ 1101 & 0101 \\ \text{odd} & \text{even} \end{matrix}$  = 11010101 (size = 1 byte)  
**odd**

Notice that when two hex digits, each of even parity are combined, the resulting byte has even parity(EXAMPLE 1) and likewise for two hex digits, each with odd parity(EXAMPLE 2). The only time odd parity results is when a pair of hex digits with opposite parities are combined.

The encryption key consists of 16 hexadecimal digits, which means there are 8 pairs, or equivalently, 8 bytes. Each byte must have odd parity, that is, when the hex digits are grouped by two's from left to right, each pair must consist of either an odd-even combination or an even-odd combination. Entering a key that contains a byte with even parity will render the key invalid.

To construct an encryption key: select 8 pairs of characters - one character from each column for each pair and string them together. The order of the characters in the pair does not matter as long as there is one character from each column.

<u>EVEN</u>	<u>ODD</u>
0	1
3	2
5	4
6	7
9	8
A	B
C	D
F	E

EXAMPLES: 0123456789ABCDEF  
0E3D5B6897A4C2F1 are valid keys.

## **825 Crypto Net Registers**

### **Technical Support**

The Western DataCom Co., Inc. technical support group can be reached at (216) 835-1510 Monday through Friday (except holidays) between the hours of 8:00 a.m. - 5:30 p.m. Eastern Time.

When calling for technical support, please have the following information ready so that the applications engineer may be able to assist you in a timely manner:

- Product serial number
- Firmware revision
- Manual revision date (lower right corner of title page)
- Other equipment being used with the product