

855 FrameGuard

Frame Relay Encryptor

September 13, 1999

Introduction	1
Diagram	2
Theory of Operation.....	3
Getting Started	4
855 FrameGuard Commands	6
855 FrameGuard Registers.....	8
Appendix A: Parity and Encryption Keys	10
Technical Support	12

855 FrameGuard

The Western DataCom Co., Inc. 855 FrameGuard - Frame Relay Encryptor (henceforth referred to as the 855) is a synchronous DES hardware encryption device developed to secure data transferred over both public and private frame relay networks. It uses FIPS PUB 46-2 DES Encryption approved by the NIST (National Institute of Standards and Technology) to encrypt the data payload attached to each individual DLCI (Data Link Connection Identifier). With the DLCI still intact the data can find its destination anywhere in the frame relay network. The 855 can be setup to encrypt any and all DLCI's that the user deems necessary and pass the remaining DLCI's transparently, with no affect to the overall network traffic.

The 855 are designed to be installed between a FRAD or Router and the DCE, and require no changes to existing equipment; see diagram 1. The unit's DTE port is factory configured for V.35 and can operate up to 2,048,000 BPS. The DCE port can be factory configured for either V.35 or RS-232 operation, and can operate from 9,600 BPS up to E1 (2,048,000 BPS) link speeds. The 855 also feature an asynchronous control port for setup, configuration of DLCI's, and the storage of security parameters.

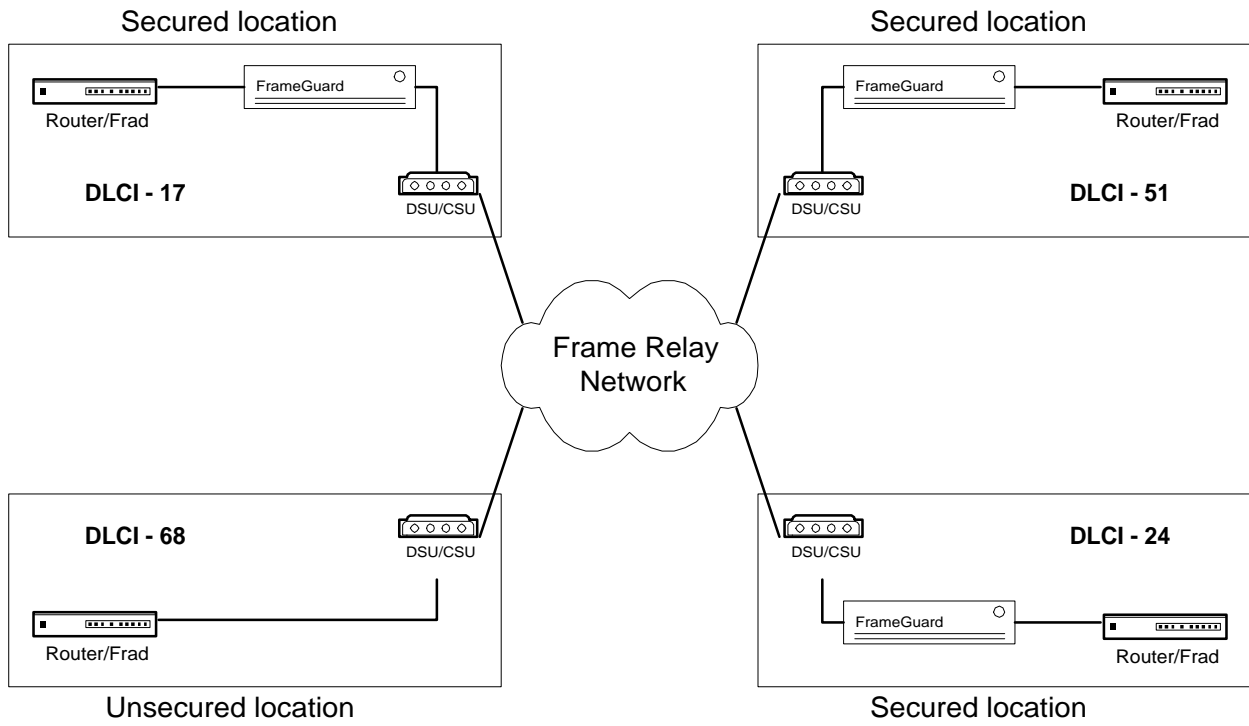
There are two methods of network management that Western DataCom provides for the FrameGuard. These two methods were developed based on the premise that security managers would not want to connect a device used to secure their network directly on the Ethernet where anyone has access to it. The first method is a cost-effective method utilizing high speed DES encrypting modems to communicate with remote FrameGuard's for configuration changes and key management. The "security officer" uses a Western DataCom CryptoCom pocket DES encryption modem to link to various remote sites that house a CryptoCard DES encryption modem along with a FrameGuard frame relay encryptor in a WA1602, 2-slot chassis. The officer calling into these remote sites would be required to enter a Personal Identification Number, PIN, into the host CryptoCom prior to gaining authorization to dial out. Once authorized the security officer can connect to remote sites and securely make configuration changes. If an attempt is made to connect to these remote DES modems by another source the connection is instantly terminated. The CryptoCard also has the ability to invoke caller ID security, which causes the modem to answer only when it has determined that the call is originating from the proper source.

The second method is to use the FrameGuard's auto key change function. With this function enabled the FrameGuard automatically changes the encryption key for every frame of data it passes. This continuous changing to the encryption key not only strengthens the security but also eliminates the need for tedious key management.

For more information please contact your local Western DataCom Co., Inc., distributor or call 800-262-3311 and speak to someone in our sales department.

855 FrameGuard

Diagram 1:



855 FrameGuard

Theory of Operation

In diagram 1, on page 2, only DLCI's 24, 51 & 17 are secured with encryption. DLCI 68 is passing transparently through the network without encryption. In this network each FrameGuard would contain DLCI's 24, 51 & 17 in its DLCI table. More information regarding the DLCI table is provided later in this manual.

Each site has its own unique DLCI that are supplied by the carrier service. When configuring FrameGuard's the user will need to know the DLCI's for each site that is going to be encrypted. Figure 1 shows four sites each with its respective DLCI. Each DLCI refers to that location only and does not necessarily relate to other sites in the wide area network scheme. If you are unsure of the DLCI's in your network contact the carrier service providing your company with the frame relay service. Their technicians will be able to assist you with any questions you may have.

In point-to-point applications, there are two methods of operation. The first would be operating a frame relay service from point A to point B. In this case the DLCI's would still come from the carrier service providing you with your frame relay circuits. Second is operating a dedicated link from point A to point B, not frame relay (i.e. DSU/CSU-A to DSU/CSU-B). In this case the user is not using a frame relay service, they are only operating a frame relay protocol that is generated by the DTE equipment which typically is a router. This method requires the user to issue its own DLCI during the configuration process of the routers. The DLCI should be the same in both locations. More information regarding DTE setup is available from the manufacturer of such equipment.

The 855 continuously monitor the incoming and outgoing data packets for frames that contain a DLCI that the user has specified to be secured. When such a frame is found the FrameGuard encrypts the payload of the frame with a 56-bit encryption key and leaves the DLCI intact. With the DLCI untouched the frame is forwarded to its destination. At the destination the FrameGuard decrypts this information and forwards it to the DTE equipment where it can then be distributed to the local area network. For frames that do not require security the FrameGuard simply passes them to their destination.

855 FrameGuard

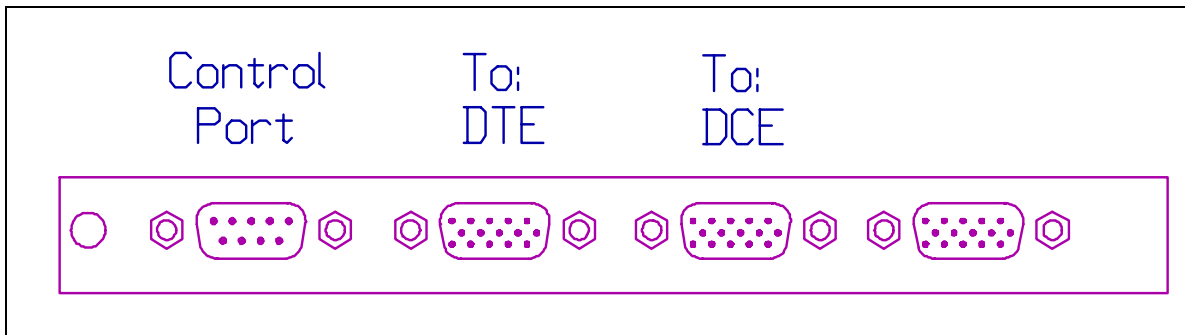


Figure 1: 855 FrameGuard Backpanel

Installation

1. Unpacking/Checklist

855's are shipped in one of two ways depending on whether they are ordered alone or with the Western DataCom WA1602 stand-alone chassis. Unpack the contents of the shipping carton.

If the 855's were ordered alone, then in addition to this manual each unit should have the following:

- 1 855 FrameGuard firmware revision 5.81 or later
- 1 HD15 male-to-V.35 female cable
- 1 HD15 male-to-V.35 male cable
- 1 DB9 male-to-DB25 female cable

If the 855's were ordered with the WA1602 chassis, then in addition to the above, each unit will contain the WA1602 chassis with the 855 FrameGuard already mounted, and one power supply.

2. Mounting

The FrameGuard is a rack-mount card design, which is compatible with the Racal Vadic MDS-1 series chassis and the WA1600 Western DataCom series chassis. Install according to the following directions.

NOTE: The 855 FrameGuard's should be mounted into the chassis with the POWER OFF. If one or more 855's are already mounted in a chassis and the power is ON, make sure to shut the power OFF before mounting any other units into that chassis.

855 FrameGuard

2 SLOT CHASSIS If the 855 was purchased with the WA1602 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 855 has been removed, re-mount according to the directions for the 4 slot chassis below.

4 SLOT CHASSIS To mount the 855 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 855 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 FrameGuard for configuration, control, and monitoring 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 (Emulate VT100).

The control port is the DB9 connector mounted on the extreme left of the 855 backpanel. Refer to **Figure 1**. A DB9 male-to-DB25 female converter 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 or PC.

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 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 **Figure 1**. Connect the other end to the V.35 DTE cable.

855 FrameGuard

5. Connection to DCE port

The FrameGuard provides two HD15 female connectors on the backpanel for connection to DCE's, see **Figure 1**. With the backpanel facing you, the second HD15 connector from the right is the primary DCE port and the extreme right connector is the backup port.

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). Connect the V.35 male end to the DCE cable.

This completes the installation procedure. Turn power on to the FrameGuard.

855 FrameGuard

Configuration:

Configuration and control of the 855 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. To get the command prompt to appear simply strike the enter key on your terminal or PC. **NOTE: with the exception of the SET ENC command all other configuration changes must be followed by a reset or a cycle of power.**

The Show commands:

`SHOW STATS`

Displays status on FrameGuard.

`SHOW ID`

Displays 8 character Identification string.

`SHOW S/N`

Displays unit serial number.

`SHOW REGS`

Displays all registers in a matrix format.

`SHOW REG n`

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

`SHOW ENC`

Displays a table of the DLCI's that are currently being encrypted.

The Set commands:

`SET ID string`

Where *string* is an 8 character, alphanumeric string identification. This string is stored in EEROM. It allows user to identify various units within the network.

`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 in Appendix A). This command sets the encryption key.

855 FrameGuard

SET ENC *n dcli*

where *n* equals on or off, and *DLCI* equals the DLCI to be encrypted. Valid DLCI's are 1 thru 1022, and you can select groups of DLCI's to turn of and on. Example: SET ENC ON 1 - 5 will turn encryption on for DLCI's 1 through 5. **This command is the only command that takes effect immediately upon entering the string.**

The Initialize command:

INIT REGS

Restores factory configuration.

INIT KEY

Restores factory default encryption key. This key should be used for initial testing of units. The factory default key is: 0123456789ABCDEF

Reset command:

<control> R

Software reset. Allows user to reset unit without cycling the power.

855 FrameGuard

Configuration Registers:

Although the FrameGuard is shipped from the factory with the optimum configuration settings there are some applications that require special changes for operation. The following register offer these settings, and can be changed using the set reg n v command.

REG 0 - DTE Port Speed

- 0 = 56K
- 1 = 64K
- 2 = 96K
- 3 = 128K
- 4 = 192K
- 5 = 256K
- 6 = 384K
- 7 = 512K
- 8 = 768K
- 9 = 1024K
- 10 = 1536K
- 11 = **2048K - Factory default**

This register sets the DTE port speed. This speed is what the DTE device will use for data transmission.

NOTE: Changes to this register do not take effect while the unit is on-line, the link must be dropped to accept changes, (control R will have the same affect).

REG 1 - NRZI Data Encoding, Flag or Mark Idle, Clock Gapping

- 0 = NRZ Data Encoding, Mark Idle, No Clock Gapping
- 1 = NRZI Data Encoding, Mark Idle, No Clock Gapping
- 2 = NRZ Data Encoding, Flag Idle, No Clock Gapping
- 3 = NRZI Data Encoding, Flag Idle, No Clock Gapping
- 4 = NRZ Data Encoding, Mark Idle, Clock Gapping
- 5 = NRZI Data Encoding, Mark Idle, Clock Gapping
- 6 = NRZ Data Encoding, Flag Idle, Clock Gapping - default**
- 7 = NRZI Data Encoding, Flag Idle, Clock Gapping

NRZ & NRZI data encoding are to methods of parity checking of data. Most of today's equipment uses NRZ. Flag and Mark idle are what is sent between frames to fill voids. Flag idles are most prominent. Clock gapping is a method of flow controlling data to keep buffers from overflowing when CIR's (committed information rates) are at their highest.

855 FrameGuard

Clock gapping is a hardware technique for implementing flow control in a synchronous environment. Since the 855 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 may not operate with older DTE devices, the only equipment that Western DataCom has experienced problems with is some older IBM™ equipment.

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 its maximum of 2.048Mbps. Now when the FrameGuard'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. If this action is not supported, simply disable clock gapping by setting reg 1 to a 2, and adjust the DTE clock to match that of the link speed.

REG 2 - Bit-mapped

The only time a connection can occur with the FrameGuard is when DTR is asserted or in a logical high state. Most equipment supplies DTR, if your equipment does set this register to DTR normal. If your equipment does not supply DTR then set this register to ignore DTR.

0 = DTR normal

1 = Ignore DTR - default

REG 4 - Data Carrier Detect (DCD) & Clear To Send (CTS) control

The FrameGuard also allows for control of Data Carrier Detect (DCD) and Clear to Send (CTS). These signals come from the DCE, and in general should be left normal.

0 = CTS normal, DCD normal - default

1 = Ignore CTS, DCD normal

2 = CTS normal, ignore DCD

3 = Ignore CTS, ignore DCD

855 FrameGuard

REG 40 - DTE signal status (DTR & RTS); Read Only

This register is used to indicate whether or not the FrameGuard is seeing the proper signals from the DTE equipment it is connected to. This register should only be read when DTE equipment is attached to the FrameGuard.

- 0 = DTR off, RTS off
- 1 = DTR on, RTS off
- 2 = DTR off, RTS on
- 3 = DTR on, RTS on - during connection

REG 41 - DCE signal status (CTS & DCD); Read Only

This register is used to indicate whether or not the FrameGuard is seeing the proper signals from the DCE equipment it is connected to. Again this register should only be read when DCE equipment is attached to the FrameGuard's primary DCE port.

- 0 = CTS off, DCD off
- 1 = CTS on, DCD off
- 2 = CTS off, DCD on
- 3 = CTS on, DCD on - during connection**

855 FrameGuard

Appendix A

This appendix describes parity and its relationship to construction of encryption keys on the Western DataCom 855 FrameGuard.

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 FrameGuard 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 users who will be defining and storing encryption keys on the 855. The following conversion chart is included as an aid in determining parity of encryption keys.

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 a four digit binary number, 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 one **byte**. Since hex digits are four bits each, each pair of them would then be one byte.

855 FrameGuard

EXAMPLES:

1. Hex number 9C = $\begin{matrix} 9 & C \\ 1001 & 1100 \end{matrix} = 10011100$ (size = 1 byte)
2. Hex number E7 = $\begin{matrix} E & 7 \\ 1110 & 0111 \end{matrix} = 11100111$ (size = 1 byte)
3. Hex number D5 = $\begin{matrix} D & 5 \\ 1101 & 0101 \end{matrix} = 11010101$ (size = 1 byte)

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 = $\begin{matrix} 9 & C \\ 1001 & 1100 \end{matrix} = 10011100$ (size = 1 byte)
even even even
2. Hex number E7 = $\begin{matrix} E & 7 \\ 1110 & 0111 \end{matrix} = 11100111$ (size = 1 byte)
odd odd even
3. Hex number D5 = $\begin{matrix} D & 5 \\ 1101 & 0101 \end{matrix} = 11010101$ (size = 1 byte)
odd even 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.

855 FrameGuard

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 within each pair.

<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 both valid keys.

EXAMPLES: 0**F**23456789ABCDEF
0E3D5B6897**B**4C2F1 - are both invalid keys.

NOTE: The FrameGuard will automatically correct any encryption key that has been incorrectly entered.

855 FrameGuard

Technical Support

The Western DataCom Co., Inc. technical support group can be reached at (216) 835-1510 extension 20, Monday through Friday (except holidays) between the hours of 9:00 a.m. - 6:00 p.m. Eastern Standard 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 name and serial number
- Firmware revision
- Manual revision date (lower right corner of title page)
- Other equipment being used with the product
- Network setup (i.e. link speeds, DTE devices, etc.)

Note: information regarding product name, serial number and firmware revision can be gotten from the SHOW STATS command.