Teldat Router

Encryption

Doc. *DM726-I* Rev. *10.00*
January, 2003

INDEX

Chapter 1
Introduction

1. Introduction to Cryptography

Basic Concepts

Cryptography is the art of transforming useful information into apparently unintelligible information. The basic service offered by cryptography is information confidentiality, although the following also exists:

- Integrity check: this is because the message being sent may have been altered while being transported by an unauthorized entity.
- Authentication: this is to verify the identity at the other end of the communication.

The modern cryptography system is based on an algorithm and a password.

The algorithms are known to the general public. The passwords are the secret part of cryptography.

> ***Confidentiality, authentication and integrity are the fundamental objectives of cryptography security.***

Different types of encryption schemes

Secret Key Cryptography uses a secret key only known to the two communication ends.

The two most commonly used algorithms are ***DES*** (Data Encryption Standard) and ***IDEA*** (International Data Encryption Algorithm). A variation on the Data Encryption Standard is the ***TRIPLE DES***: their two 64 bit keys provide more security than the DES algorithm.

DES and ***IDEA*** both work in blocks of 64 bits. Two identical data blocks produce the same block after being encrypted. This characteristic makes it easy for malicious intrusion. To avoid this problem it was decided to use the ***REALIMENTATION*** (using encrypted information from the previous block to encrypt the current block). Two algorithms made their appearance based on this procedure: DES with CBC, TRIPLE DES with CBC etc.

The ***Public Key Cryptography*** scheme is also known as asymmetric encryption.

One of the communication ends generates two keys, one private (or secret) and the other public (the latter can be generally known). This public key system permits the exchange of encrypted information without both ends needing to store the same secret key. The most extended public key algorithms are ***RSA, EL GAMMAL, DIFFIE-HELMANN*** etc. This increase in flexibility needs authentication. How do we know that the end responding is not an intruder? Numerous authentication protocols and integrity checks (based on certificates or signatures) are necessary to complement the public key algorithms.

Security

Security of the cryptographic systems depends on the secret key protection level. If this key were really secret, the malicious intruders would have to try and decode the hidden information without the key: there exist many techniques to achieve this objective but they require an enormous amount of computation. As an example, an intruder who tries all the possible keys is capable of breaking the security. However he could need a lifetime or more in order to run through all the possible keys. In short, depending on the algorithm and the length of the keys, the intruder will find it more or less difficult to uncover the hidden information.

In order to increase the security of the encryption system, you can change the secret keys from time to time. A key management center is capable of automatically carrying out this task.

The security of the secret key systems depends to a great degree on the confidentiality of the key.

2. The TELDAT encryption system

In this section, the components and the security configurations offered by ***TELDAT*** are described.

2.1. TELDAT security components

Components	Functionality
TELDAT encryption ROUTER.	This is the router incorporating the encryption functionality for communications in **FRAME RELAY** and **X.25**.
TELDAT management ROUTER.	This router communicates the ***CGC*** (Key Management Center) with the ***TELDAT*** encryption ***ROUTER.***
UCI + (Encryption Unit)	This is the encryption Unit. It is capable of encrypting (decrypting) traffic to (from) a ***TELDAT*** encryption ***ROUTER.***
CENTRIX	These are the devices that receive calls from a ***TELDAT*** encryption ***ROUTER*** through ***ISDN*** and are capable of encrypting (decrypting) traffic proceeding from these calls.
CGC + (Key Management Center)	The Key Management Center (***CGC***) device permits you to periodically and remotely change the secret keys in the ***TELDAT ROUTERs*** through a public key system.

2.2. Security Configurations

a) Teldat Router - Teldat Router

The ***TELDAT ROUTER*** can establish encrypted communications with another ***TELDAT ROUTER*** through an **X.25** or **FRAME RELAY** network.

There does exist the pssibility to separately configure encryption (keys, encryption algorithms etc.) for each DLCI or for each pair of NRI´s. The available encryption algorithms are ***DES*** (with or without feedback, ***CBC***) and ***TRIPLE DES*** (with or without feedback, ***CBC***).

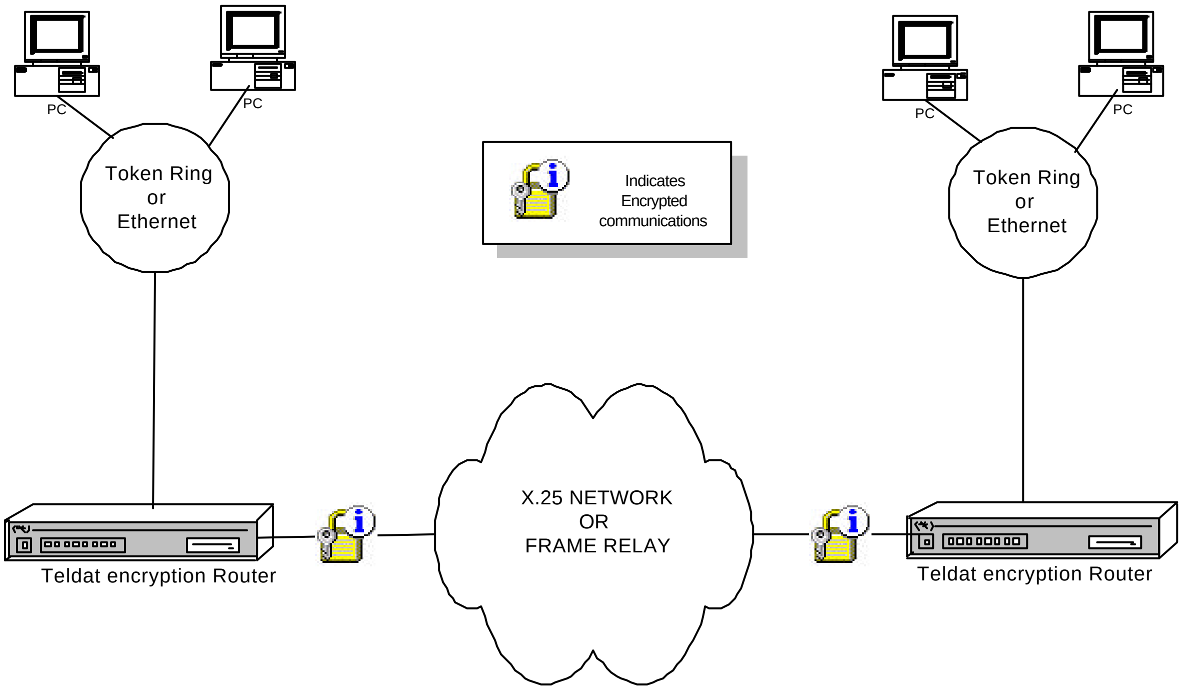

Figure 1: Teldat Router– Teldat Router Configuration

> ***The encryption configuration is carried out through the console in each TELDAT ROUTER.***

b) Teldat Router – UCI (Encryption Unit)

The ***TELDAT ROUTER*** can establish encrypted communications with a ***HOST*** through a ***UCI*** (Encryption Unit).

There does exist the possibility to separately configure encryption (keys, encryption algorithms etc.) for each DLCI or for each pair of NRI´s. The available encryption algorithms are ***DES*** (with or without feedback, ***CBC***) and ***TRIPLE DES*** (with or without feedback, ***CBC***).

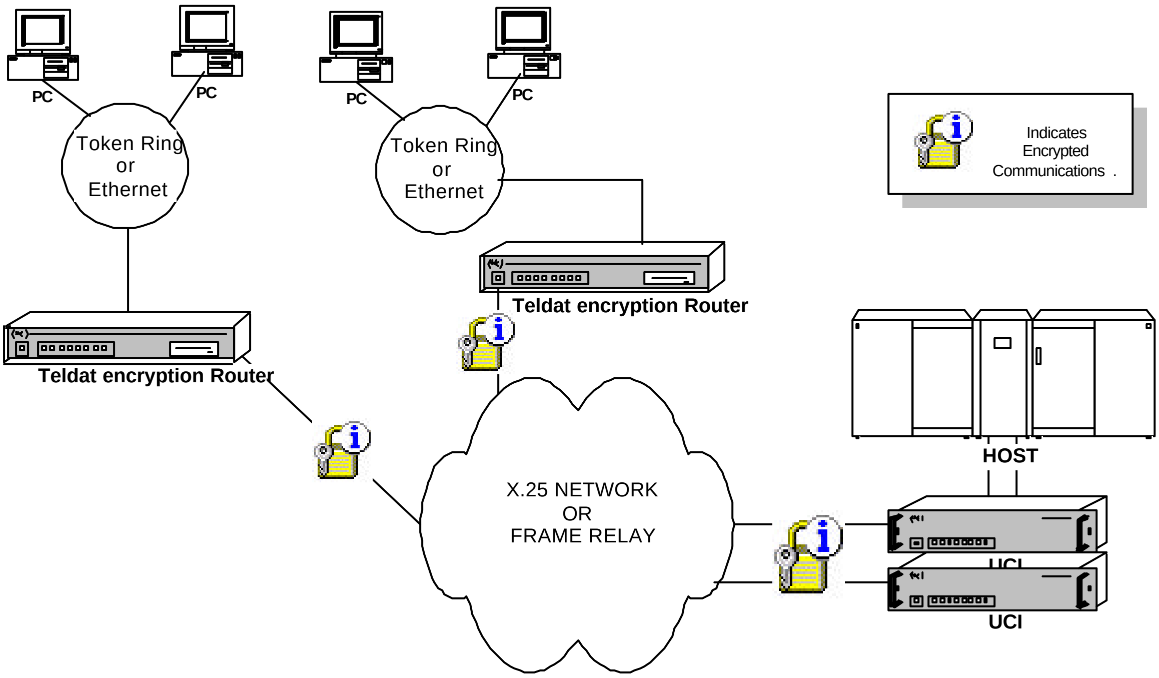

Figure 2: Teldat Router– UCI (Encryption Unit) Configuration

The encryption configuration is carried out through the console in each TELDAT ROUTER.

c) Router without encryption – UCI (Encryption Unit)

The encryption Units (***UCI*´s**) can encrypt (decrypt) the outgoing (incoming) communications through a router without an encryption function.

There does exist the possibility to separately configure encryption (keys, encryption algorithms etc.) for each DLCI or for each pair of NRI´s. The available encryption algorithms are ***DES*** (with or without feedback, ***CBC***) and ***TRIPLE DES*** (with or without feedback, ***CBC***).

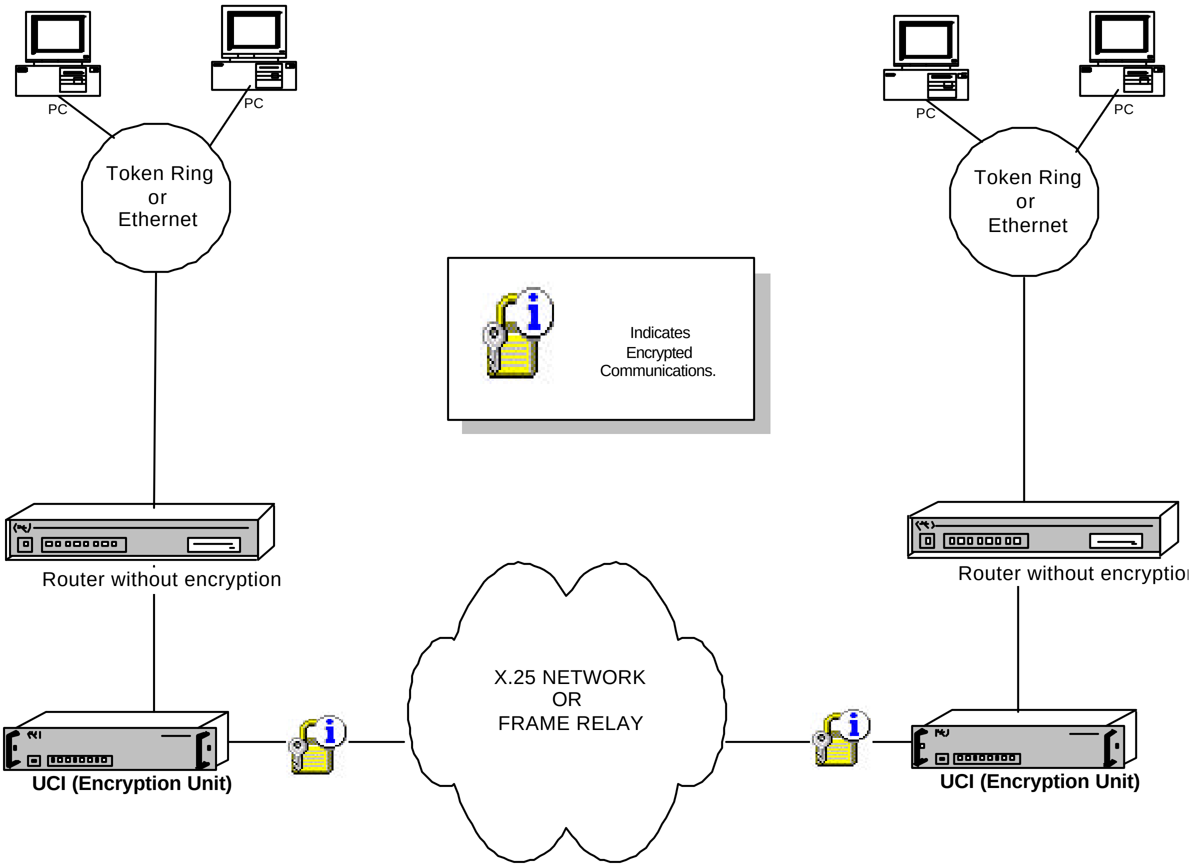

Figure 3: Router without encryption – UCI (Encryption Unit) Configuration

d) TELDAT ROUTER with CGC (Key Management Center)

The ***CGC*** changes the encryption configuration (keys, encryption algorithms etc.) in the ***TELDAT ROUTERs*** and the ***UCI*´s (Encryption Unit) through the **WAN** network (**X25** or **FRAME RELAY**). The ***TELDAT management ROUTER*** controls the transmission of the encryption configuration through the W**AN** using a secure method (RSA public key system).

In cases of a **WAN** link failure, there exists the possibility to transmit encrypted information from the HOST to the ***TELDAT ROUTER*** through an **ISDN** link. A ***CENTRIX*** device is used here to encrypt the information and to transmit it through an **ISDN** line.

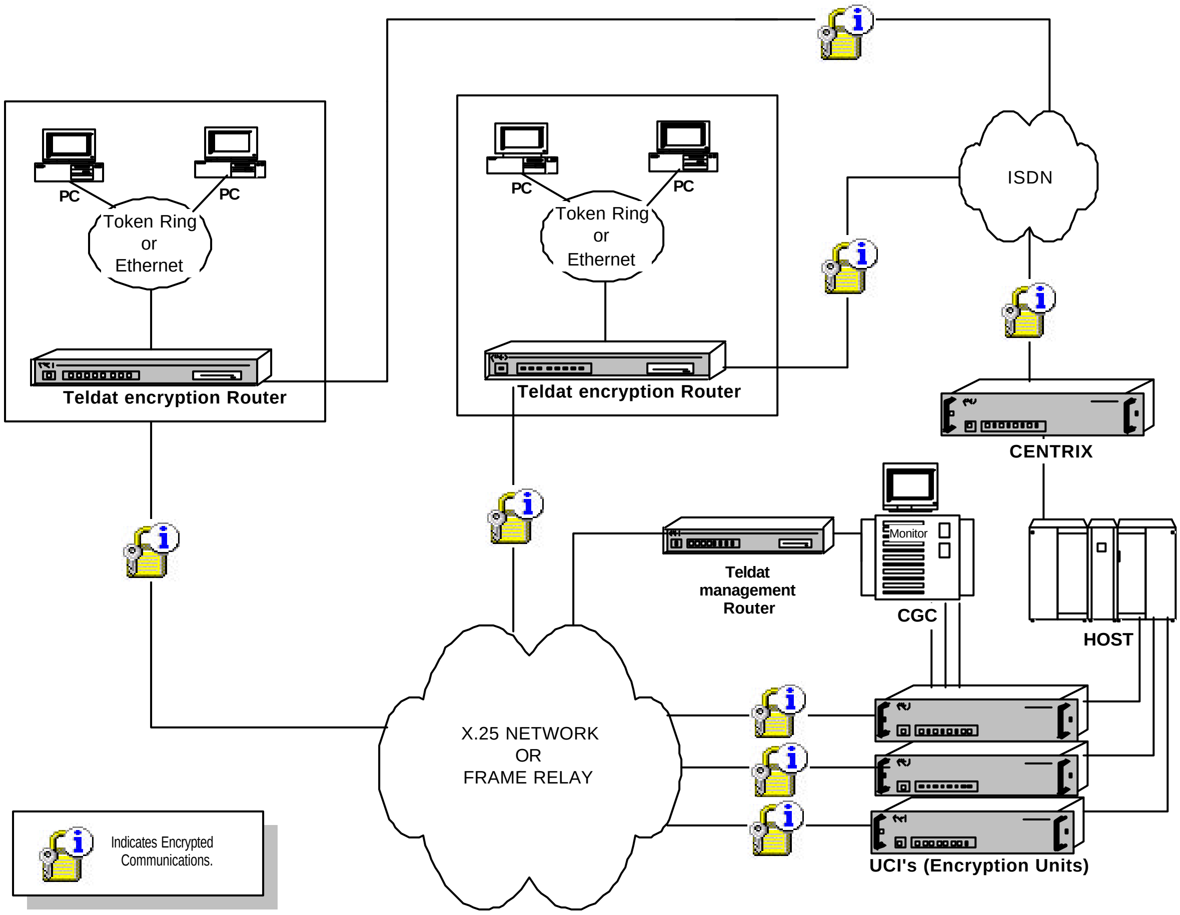

Figure 4: Configuration of a Teldat Router with CGC (Key Management Center)

> ***Encryption configuration in the TELDAT ROUTER and the UCI´s (Encryption Unit) is remotely carried out from the CGC (Key Management Center).***
>
> ***The CGC can periodically (and automatically) change the encrypted communications secret keys in order to increase security in the cryptographic system.***

Chapter 2
General Configuration

1. The UCI Command

The **UCI** command permits you to configure a ***TELDAT ROUTER*** encryption unit.

Syntax:

```
Config>UCI ?
CFG
CHANGE CFG
KEYS
MODE
USER_PASSWORD
TABLE
```

CFG

This command displays the ***TELDAT ROUTER*** encryption configuration. It indicates the number of DLCI´s and the number of NRI pairs registered in the encryption module.

Example:

```
Config>UCI CFG


Configuration $---Revision: 2.1 $$---Name: CIFPLUS_V4.1$
        Encrypt card: TS228c
        DMA transmission NOT ACTIVE
        Interruption mode ACTIVE
        CGC keys management ACTIVE
        Max NRIs = 100
        Flag Crypto ACTIVE
        Test RSA when starting NOT ACTIVE

PRESENT CONFIGURATION:
    Key which encrypts the keys table has changed
    Frame Relay: Number of encrypted interfaces: 2
                 Number of encrypted DLCIs: 2
         #Ifc 1: Frame Relay encrypt configuration read
    X25:         Number of up NRIs: 1
                 Global Confirmation (not NRI´s of CGC): No
                 Standard Fragmentation (not NRI´s of CGC): No
                 X25 encrypt configuration read

GENERAL STATUS: ENCRYPT

Config>
```

CHANGE CFG

This command permits you to change the ***TELDAT ROUTER*** encryption configuration. The device will prompt the user on each one of the parameters.

In order to execute this command, you need to know the user password. This is *teldat* by default.

The changes do not take effect until the device has been restarted.

Example:

```
Config>UCI CHANGE CFG

User Password? ******


Configuration

Interruption mode  (y/other)? (YES)
Test RSA when starting (y/other)? (NO)
Max NRIs (10-500)? (100)
Flag Crypto? (YES)
```

The changes that can be made in the encryption configuration through this command are:

- “Interruption mode (y/other)?” permits you to enable (disable) the encryption card operation interruption mode.
- On starting the device, you can carry out a test on the encryption card with the RSA algorithm if this responds ‘Yes’ to the “Test RSA when starting (y/other)?”
- The maximum number of NRI´s that can be specified.
- Enable the received frames are encrypted check if this responds “YES”.

KEYS

Session key change via the console. This is not used in this device.

MODE

This permits you to change the device operation mode of the encryption device to transparent or vice-versa.

In order to execute this command, you need to know the user password. This is *teldat* by default.

This command takes immediate effect on execution.

Example:

```
Config>UCI MODE

User Password? ******

GENERAL STATUS: ENCRYPT(Yes/No)? y

    Updating encrypt configuration...
```

> ***“UCI MODE” only permits you to change the operation mode for the DLCI’s and the NRI’s pairs registered in the encryption module.***

USER_PASSWORD

This permits you to modify the user password. Knowledge of this password gives the user certain rights such as changing the ***TELDAT ROUTER*** encryption configuration.

In order to execute this command, you need to know the user password. This is “*teldat*” by default.

This command takes immediate effect on execution.

Example:

```
Config>UCI USER_PASSWORD

User Password Update
User Password? ******

New User Password (between 6 and 16 chars)? ******
Reentry new password? ******
User Password updated
```

TABLE

This displays a table containing the active FR interfaces in static memory, the number of DLCIs and NRI´s registered in the encryption system.

Example:

```
Config>UCI TABLE

FR encrypted interfaces ON in static memory: 2

Interface   UP DLCIs in static memory    Last encrypted DLCI's date
--------- ----------------------------  ----------------------------
    1                1                       14/02/00 11:09:03
    2                1                       14/02/00 11:33:39

Number of up NRIs: 1

Last configured NRI's date: 14/02/00 11:04:11
```

Chapter 3
Frame Relay Interface Configuration

1. Introduction

This chapter describes the encryption configuration commands for the **FRAME RELAY** interface circuits.

- Register encryption in a **FRAME RELAY** circuit.
- Configure the encryption in a **FRAME RELAY** circuit: change mode, keys etc.
- Unregister encryption in a **FRAME RELAY** circuit.
- List the **FRAME RELAY** interface encryption configuration.

The commands dealt with in this chapter can be found in the **FRAME RELAY** interface configuration menu being used.

2. Register circuit encryption

When you add the DLCI or modify its configuration, you can register the circuit encryption if you receive a positive response to the question: “Encrypt Information?”

The registered encryption circuit is automatically configured in ***DES*** mode without ***CBC***.

Syntax:

```
FR config>ADD PVC–PERMANENT-CIRCUIT
```

or

```
FR config>CHANGE PVC–PERMANENT-CIRCUIT
```

Example 1:

```
FR config>ADD PVC-PERMANENT-CIRCUIT
Circuit number[16]? 20
Outgoing Committed Information Rate (CIR) in bps[16000]?
Outgoing Committed Burst Size (Bc) in bits[16000]?
Outgoing Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)? yes
Assign circuit name[]?
Inverse ARP (0-Default, 1-Off, 2-On): [0]?

    Updating encrypt configuration...
FR config>
```

Example 2:

```
FR config>CHANGE PVC-PERMANENT-CIRCUIT
Circuit number[16]?
Outgoing Committed Information Rate (CIR) in bps[16000]?
Outgoing Committed Burst Size (Bc) in bits[16000]?
Outgoing Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)? yes
Assign circuit name[]?
Inverse ARP (0-Default, 1-Off, 2-On): [0]?
FR config>
```

The registered encryption circuit is automatically configured in DES mode without CBC with a default key.

This default configuration may be modified through the SET ENCRYPTION command.

3. SET ENCRYPTION Command

The **SET ENCRYPTION** command permits you to modify the **FRAME RELAY** interface circuit encryption. This command configures the encryption in a previously registered circuit.

In order to execute this command, you need to know the user password. This is “*teldat*” by default.

Example:

```
FR config>SET ENCRYPTION

User Password? ******
Circuit number: [16]?
Encrypt mode (DES, Triple DES, Clear): [DES]?
Enable CBC encrypt mode [No]: (Yes/No)? y
New Encrypt Key (8 characters): ********
Rewrite:
New Encrypt Key (8 characters): ********

    Updating encrypt configuration...
FR config>
```

- ***You can choose between various encryption algorithms (DES with or without CBC, TRIPLE DES with or without CBC) or transparent mode. In TRIPLE DES, you must introduce three keys and in DES you introduce a single key. The keys must be introduced twice in consecutive order for confirmation purposes.***
- ***A DLCI configured through the CGC (Key Management Center) cannot be modified through the console.***

4. Unregister circuit encryption

When you modify the DLCI configuration, you can unregister a circuit encryption by responding “NO” to the question: “Encrypt Information?”

Example:

```
FR config>CHANGE PVC-PRMANENT-CIRCUIT
Circuit number[16]?
Outgoing Committed Information Rate (CIR) in bps[16000]?
Outgoing Committed Burst Size (Bc) in bits[16000]?
Outgoing Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)? No
Assign circuit name[]?
Inverse ARP (0-Default, 1-Off, 2-On): [0]?

    Updating encrypt configuration...
FR config>
```

5. LIST ENCRYPTION Command

The **LIST ENCRYPTION** command permits you to list the encryption configuration for all the circuits registered in the encryption module. The response to the question “CGC?”, permits you to see if the circuit has been configured through the CGC or the console.

The **LIST ENCRYPTION** command permits you to list the encryption configuration for all the registered DLCI’s. The encryption algorithm being used is indicated: ***DES*** or ***TRIPLE DES***(***3DES***) with or without ***CBC***. If the registered circuit is not encrypted, it is indicated as ***CLEAR***(***CLR***).

Example:

```
FR config>LIST ENCRYPTION


FRAME RELAY ENCRYPT CONFIGURATION (interface 1):

DLCI      Encrypt mode     CBC?  CGC?
====      ============     ====  ====
16        TRIPLE DES       Yes   No
17        DES              No    No
18        Clear            --    No

Last dlci configured date: 14/02/00 12:23:42
FR config>
```

- ***A circuit registered in the encryption module is configured in transparent mode (Clear). The data sent (received) through this circuit is not encrypted (decrypted).***
- ***All modifications carried out in the encryption configuration take immediate effect and is automatically recorded in the non-volatile memory.***

Chapter 4
X25 Configuration

1. Introduction

In this chapter, the encryption configuration commands for each pair of **X.25** NRI's are described.

- Establish/Remove encryption in the NRI pairs.
- List the **X.25** encryption configuration.

The commands dealt with in this chapter can be found in the **X.25** configuration menu.

2. SET ENCRYPTION Command

The **SET ENCRYPTION** command permits you to register or unregister encryption for an NRI pair.

It also permits you to establish GLOBAL CONFIRMATION and STANDARD FRAGMENTATION.

Syntax:

```
X25 Config>SET ENCRYPTION ?
UP
DOWN
CONFIRMATION
FRAGMENTATION
```

SET ENCRYPTION UP

This command registers encryption for an NRI pair.

In order to execute this command, you need to know the user password. This is "*teldat*" by default.

You can choose between various encryption algorithms (***DES*** with or without ***CBC***, ***TRIPLE DES*** with or without ***CBC***) or clear mode. In ***TRIPLE DES***, you must introduce three keys and in ***DES*** you introduce a single key. The keys must be introduced twice in consecutive order for confirmation purposes.

Example:

```
X25 Config>SET ENCRYPTION UP

User Password? ******
Called NRI? 333333
Calling NRI? 444444
Type (DES, TRIPLE DES, Clear)[DES]? des
Enable CBC [No]: (Yes/No)? y
Key(s) (0xhhhhhhhhhhhhhhhh, abcdabcd)? ********
        Rep: Key(s) (0xhhhhhhhhhhhhhhhh, abcdabcd)? ********
Another(Yes/No)?

    Updating encrypt configuration...
X25 Config>
```

- ***You can choose between various encryption algorithms (DES with or without CBC, TRIPLE DES with or without CBC) or clear mode. In TRIPLE DES, you must introduce three keys and in DES you introduce a single key. The keys must be introduced twice in consecutive order for confirmation purposes.***

SET ENCRYPTION DOWN

This command unregisters encryption for an NRI pair.

In order to execute this command, you need to know the user password. This is "*teldat*" by default.

The device will ask the user which NRI pair to unregister.

Example:

```
X25 Config>SET ENCRYPTION DOWN

User Password? ******
Called NRI? 333333
Calling NRI? 444444

Another(Yes/No)?

    Updating encrypt configuration...
X25 Config>
```

SET ENCRYPTION CONFIRMATION

This command permits you to establish or eliminate GLOBAL CONFIRMATION for all the NRI pairs. This has no effect on the connections configured through GCG (Key Management Center).

In order to execute this command, you need to know the user password. This is "*teldat*" by default.

Example:

```
X25 config> SET ENCRYPTION CONFIRMATION

User Password? ******
 Global Confirmation(Yes/No)? y

    Updating encrypt configuration...
X25 config>
```

SET ENCRYPTION FRAGMENTATION

This command permits you to establish or eliminate "STANDARD FRAGMENTATION" for all the NRI pairs. This has no effect on the connections configured through GCG (Key Management Center).

In order to execute this command, you need to know the user password. This is "*teldat*" by default.

Example:

```
X25 Config>SET ENCRYPTION FRAGMENTATION

User Password? ******
 Standard Fragmentation(Yes/No)? y

    Updating encrypt configuration...
X25 Config>
```

- ***The commands "SET ENCRYPTION CONFIRMATION" and "SET ENCRYPTION FRAGMENTATION" have no effect on the CGC connections. These have their own Standard Fragmentation and Global Confirmation.***
- ***All modifications carried out in the encryption configuration take immediate effect and is automatically recorded in the non-volatile memory.***

3. LIST ENCRYPTION Command

The **LIST ENCRYPTION** command permits you to list the encryption configuration for all the NRI pairs that have been registered. The encryption algorithm being used is indicated: ***DES*** or ***TRIPLE DES***(***3DES***) with or without ***CBC***. If the registered NRI pair is not encrypted, it is indicated as ***CLEAR***(***CLR***).

Additionally this indicates whether the NRI pair has been configured through the ***CGC*** or the console.

Example:

```
X25 Config>LIST ENCRYPTION

X25 ENCRYPTION CONFIGURATION

Entry   Called NRI      Calling NRI     Type CBC CGC
======= =============== =============== ==== === ===
0       333333          444444          DES  No  No
1       444444          5555556         3DES No  No
2       9999999         8888888         CLR  --  No

Last configured NRI's date: 14/02/00 13:15:29

X25 Config>
```

Chapter 5
Encryption Monitoring

1. Introduction

In this chapter, the encryption monitoring commands for each **FRAME RELAY** and **X.25** interface are described.

- Encryption statistics.
- History of the encrypted **X.25** calls.

The commands dealt with in this chapter can be found in the main monitoring menu.

2. Commands

The ***UCI*** (Encryption Unit) permits you to view the ***TELDAT ROUTER*** encryption statistics.

Syntax:

```
+UCI ?
HELP_STATISTICS
INIT_STATISTICS
STATISTICS
LINE_X25
RESET_LINE_X25
```

HELP_STATISTICS

Displays information on the meanings of the statistic fields.

Example:

```
+UCI HELP_STATISTICS

Statistics meanings

RECEIVED FRAMES REJECTED
        TOO_LARGE:      The received frame has, or has not, too large size
                        coincided with encryption header
        FAILURE:        Frame reception failure
        WITHOUT.LINE:   Frame received but impossible to be transmitted to
                        destination because the receiver was not ready
        WRONG.ENCRYPT:  Impossible to encrypt a received frame
        WITHOUT.MEM:    Not enough memory for the transmitted frame

CONTROL FRAMES RECEIVED
        DLCI not between 16 and 1007 (included)

PROCESSED FRAMES
        ENCRYPTED:      Frames encrypted correctly
        DECRYPTED:      Frames decrypted with DLCI key
        DEC.KEY.DEF:    Decrypted frames with the default key, not decrypted
                        with the DLCI key
        TRANSPARENTS:   Transparent frames

TOTAL PROCESSED FRAMES =ENCRYPTED + DECRYPTED +  DES.KEY.DEF + TRANSPARENTS
+
```

INIT_STATISTICS

This returns the encryption statistic counters to zero and begins a new data collection session. On executing this command, the device offers the user the option to initiate the encryption statistics for a specific circuit.

Example:

```
+UCI INIT_STATISTICS

dlci encrypt statistics (<ENTER> = All)?

+
```

STATISTICS

Displays statistics relative to encryption.

Example:

```
+UCI STATISTICS

=============================================================================
                        ENCRYPTION     DECRYPTION     TOTAL
RECEIVED FRAMES  =>     340            340            680

                TOO.LARGE   FAILURE   WITHOUT.LINE  WRONG.ENCRYPT WITHOUT.MEM
 REJECTED FRAMES => 0           0           0           0            0

    CONTROL 0
=============================================================================
                        ENCRYPTION     DECRYPTION     TOTAL
TRANSMITTED FRAMES  =>  340            340            680
    CONFIRMED 0
    WRONG 0
=============================================================================
ENCRYPT
    ENCRYPTED      DECRYPTED      DEC.KEY.DEF    TRANSPARENTS
    340            340            0              0
    TOTAL PROCESSED FRAMES 680
=============================================================================

STATES MACHINE STATUS: TABLE

RECEIVED COMMANDS 21                   REJECTED COMMANDS 0

+
```

The statistics are divided into three sections, received packets, transmitted packets and processed packets.

- Received Packets: indicates received encrypted ("ENCRYPTED") and decrypted ("DECRYPTED") packets. Also the statistics on erroneous frames appears: The received frame is too long, or does not coincide with that indicated in the encryption header ("TOO LARGE"), frame reception error ("FAILURE"), impossible to transmit received header as the destination is not ready ("WITHOUT.LINE"), impossible to decrypt received frame ("WRONG.ENCRYPT"), insufficient memory for the frame you wish to transmit ("WITHOUT.MEM").
- Transmitted packets: encrypted and decrypted received packets are similarly indicated.
- Processed packets: counts the encrypted ("ENCRYPTED"), decrypted ("DECRYPTED"), encrypted with default key ("DEC.KEY.DEF") or in clear ("TRANSPARENT") mode packets processed in the router.

LINE_X25

Lists the last calls sent in **X.25**:

- The link level channel is indicated in the column: "CHANN".
- "IN TABLES" indicates that the NRI pair is registered in the encryption module.
- "PSSWD CHANGE" indicates that there has been an automatic key change in the CBC mode on establishing the connection.

Example:

```
+UCI LINE_X25

                           ENCRYPTED / DECRYPTED CALLS LIST
(*) indicates that the caller of the tables is the actual called, and viceversa

DATE               CALLED          CALLER          CHANN IN TABLES PSSWD CHANGE
=================  =============== =============== ===== ========= ============
14/02/02 14:20:26  444444           333333          20    YES       NO
14/02/02 14:19:55  444444           333333          20    YES       NO
14/02/02 14:19:08  444444           333333          20    YES       NO
+
```

RESET_LINE_X25

Deletes the list of calls sent in **X.25**.

Example:

```
+UCI RESET_LINE_X25

    Encrypted / decrypted calls list reset
+
```

Chapter 6
Configuration Troubleshooting

1. CGC (Key Management Center) incompatibility

The encryption configuration through the console is not compatible with the encryption configuration through the ***CGC***. This means that you cannot work simultaneously with the pairs (DLCI's or NRI's) configured through the ***CGC*** and with the circuits configured through the console.

2. Useful checks

In cases where the encryption is not operating correctly, check the following:

- “Flag Crypto” should be in the same state (active or inactive) at both ends.

- That the same key has been configured in the ***UCI*´s** (encryption units) and in the branches for the same DLCI or NRI pair.

- The general mode in the ***UCI*** and in the branches is “Encrypt”.

- When you configure FRAME RELAY encryption in a branch (through ***CGC***), you need to have previously configured the DLCI with the encryption option activated (“Encrypt: YES”).

- Check that you have not reset a branch before storing the encryption configuration. If this has happened, reintroduce the encryption configuration.

- The encryption configuration cannot be exchanged between distinct ***TELDAT ROUTERs.*** Each encryption configuration only operates in the branch it was created in.