Router Teldat

Cifrado

Doc. *DM526* Rev. *8.30*

Marzo, 2000

ÍNDICE

Capítulo 1
Introducción

1. Introducción a la Criptografía

Conceptos Básicos

La criptografía es el arte de transformar información útil en una información aparentemente ininteligible. El servicio básico ofrecido por la criptografía es la confidencialidad de información , aunque también existen :

- chequeo de integridad: porque el mensaje enviado puede haber sido alterado en su trayecto por una entidad no autorizada.
- la autenticación: para verificar la identidad del otro extremo de la comunicación.

Un sistema criptográfico moderno esta basado en un algoritmo y en una clave.

Los algoritmos son conocidos por el público en general. Las claves son la parte secreta de la criptografía.

Confidencialidad, autenticación e integridad son los objetivos primordiales de la seguridad criptográfica.

Diferentes tipos de esquemas de cifrado

El sistema de Clave Secreta (***Secret Key Cryptography***) utiliza una clave secreta sólo conocida por los dos extremos de la comunicación.

Dos de los algoritmos más utilizados son ***DES*** (Data Encryption Standard) e ***IDEA*** (International Data Encryption Algorithm). Una variante del algoritmo Data Encryption Standard es ***TRIPLE DES:*** sus dos claves de 64 bits añaden más seguridad con respecto al algoritmo DES.

DES e ***IDEA*** trabajan con bloques de 64 bits. Dos bloques de datos idénticos producen el mismo bloque después de cifrarlo. Esta característica facilita la labor de intrusión no autorizada. Para eliminar este problema se decidió utilizar la ***REALIMENTACIÓN*** (emplear la información cifrada del bloque anterior para cifrar el bloque actual). Basados en este procedimiento surgieron los algoritmos: DES con CBC, TRIPLE DES con CBC, etc.

El esquema de Clave Pública (***Public Key Cryptography***) se llama también a veces cifrado asimétrico.

Uno de los extremos de la comunicación genera dos claves, una privada (o secreta) y otra pública (esta última puede ser conocida por todo el mundo). Este sistema de clave pública permite el intercambio de información encriptada sin que los dos extremos necesiten almacenar la misma clave secreta. Los algoritmos de clave pública más extendido son ***RSA***, ***El GAMMAL***, ***DIFFIE-HELMANN***, etc. Este aumento de flexibilidad necesita de autenticación. ¿Cómo sabemos que el extremo que nos contesta no es un intruso?. Para contestar esta pregunta se necesitan numerosos protocolos de autenticación y de chequeo de integridad (basados en certificados o firmas) como complementos a los algoritmos de clave pública.

Seguridad

La seguridad de los sistemas criptográficos depende del nivel de protección de la clave secreta. Si esta clave es realmente secreta, los intrusos con malas intenciones tendrán que intentar descifrar la información oculta sin la clave: para conseguir este objetivo existen muchos técnicas, pero todas ellas

implican un tiempo enorme de computación. A modo de ejemplo, un intruso que pruebe todas la claves posibles será capaz de romper la seguridad. Sin embargo puede necesitar toda una vida o mucho más para recorrer todas las claves posibles. En definitiva, según el algoritmo y la longitud de las claves, el intruso encontrará más o menos dificultades en descubrir la información oculta.

Por otra parte, para aumentar la seguridad del sistema de cifrado, se pueden ir cambiando las claves secretas cada cierto tiempo. Un centro gestor de claves es capaz de realizar esta labor de forma automática.

La seguridad de los sistemas de clave secreta depende en gran medida de la confidencialidad de la clave secreta.

2. El sistema de cifrado TELDAT

En este apartado se describen los componentes y las configuraciones de seguridad que ofrece ***TELDAT***.

2.1. Componentes de Seguridad de TELDAT

Componentes	Funcionalidad
ROUTER TELDAT de cifrado.	Router que incorpora la funcionalidad de cifrar las comunicaciones en **FRAME RELAY** y en **X25**.
ROUTER TELDAT de gestión.	Router que comunica el ***CGC*** con los ***ROUTER TELDAT*** de cifrado.
UCI +	Es la Unidad de cifrado. Es capaz de cifrar (descifrar) tráfico hacia (desde) un ***ROUTER TELDAT*** de cifrado**.**
CENTRIX	Equipos que reciben llamadas por **RDSI** de un ***ROUTER TELDAT*** de cifrado y que es capaz de cifrar y descifrar el tráfico procedente de esa llamada.
CGC +	El Centro Gestor de Claves es un equipo que permite cambiar periódicamente las claves secretas de los ***ROUTER TELDAT*** de forma remota a través de un sistema de clave pública.

2.2. Configuraciones de Seguridad.

a) *Router Teldat-Router Teldat*

El ***ROUTER TELDAT*** puede establecer comunicaciones cifradas con otro ***ROUTER TELDAT*** a través de una red **X.25** o **FRAME RELAY**.

Existe la posibilidad de configurar el cifrado (claves, algoritmos de cifrado, etc.) por separado para cada DLCI o para cada pareja de NRI´s. Los algoritmos de encriptación disponibles son ***DES*** (con o sin realimentación, ***CBC***) y ***TRIPLE DES*** (con o sin realimentación, ***CBC***).

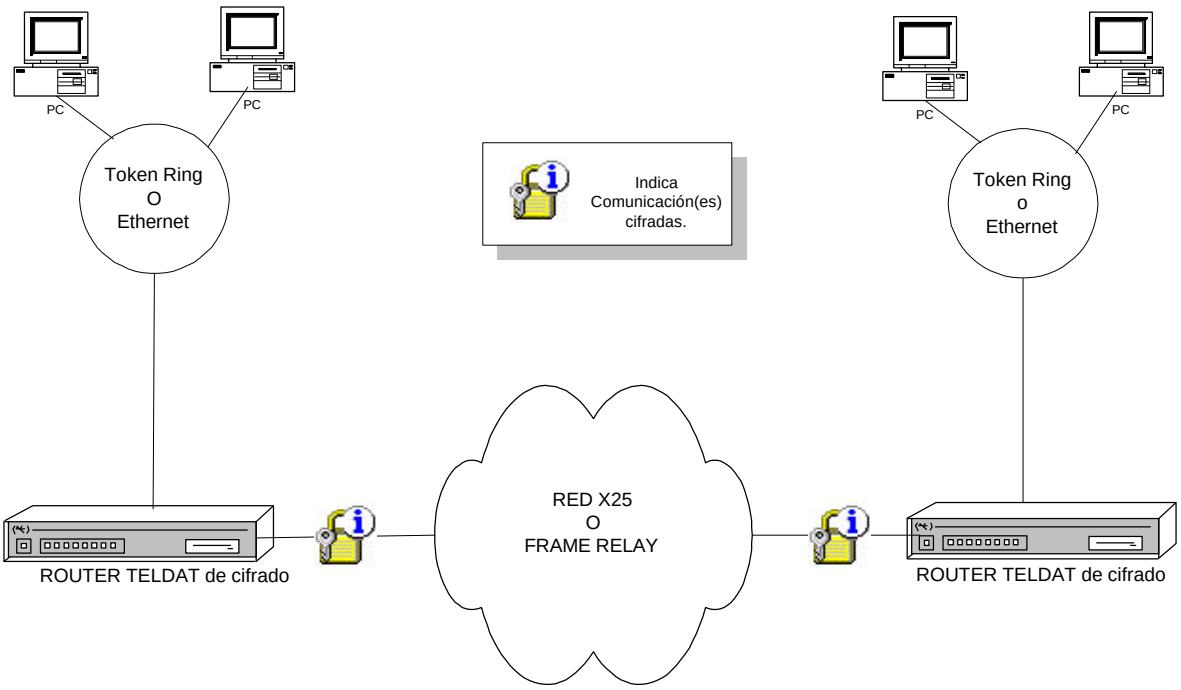

Figura 1: Configuración Router Teldat – Router Teldat

La configuración del cifrado se realiza por consola en cada ROUTER TELDAT.

b) Router Teldat -UCI

El ***ROUTER TELDAT*** puede establecer comunicaciones cifradas con un ***HOST*** a través de una ***UCI*** .

Existe la posibilidad de configurar el cifrado (claves, algoritmos de cifrado, …) por separado para cada DLCI o para cada pareja de NRI´s. Los algoritmos de encriptación disponibles son ***DES*** (con o sin realimentación, ***CBC***) y ***TRIPLE DES*** (con o sin realimentación, ***CBC***).

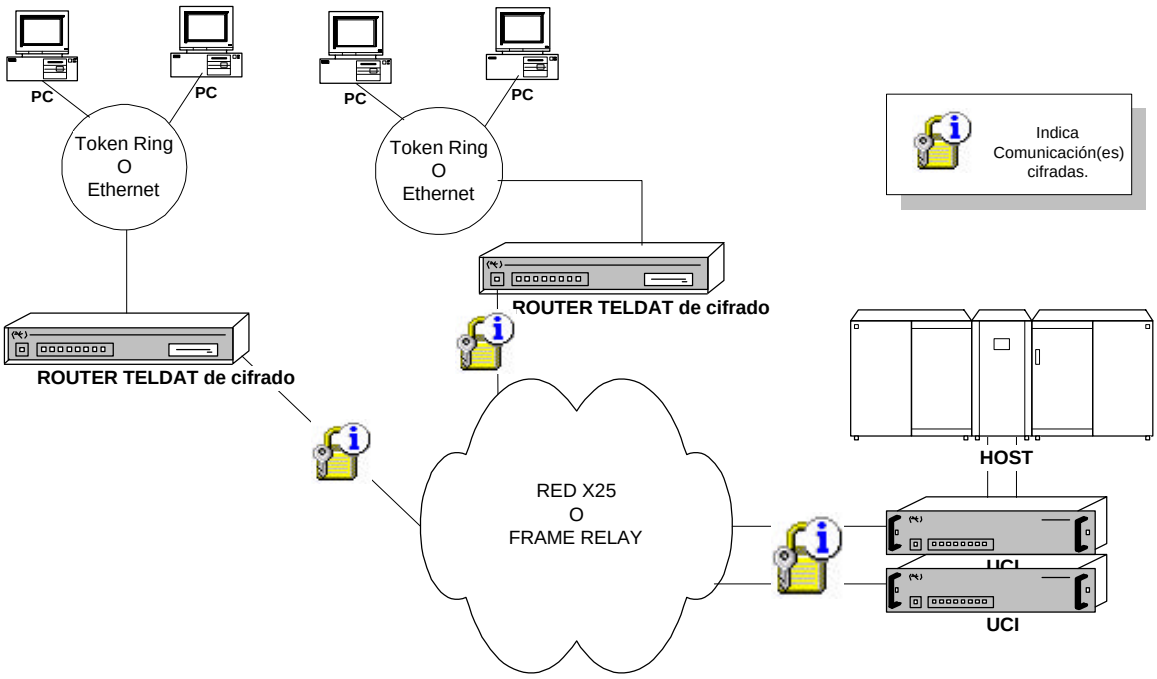

Figura 2: Configuración Router Teldat – UCI

La configuración del cifrado se realiza por consola en cada ROUTER TELDAT.

c) Router sin cifrado - UCI

Las Unidades de cifrado (***UCI***´s) pueden cifrar (descifrar) las comunicaciones salientes (entrantes) por un Router sin la funcionalidad de encriptación. Existe la posibilidad de configurar el cifrado (claves, algoritmos de cifrado, etc.) por separado para cada DLCI o para cada pareja de NRI´s. Los algoritmos de encriptación disponibles son ***DES*** (con o sin realimentación, ***CBC***) y ***TRIPLE DES*** (con o sin realimentación, ***CBC***).

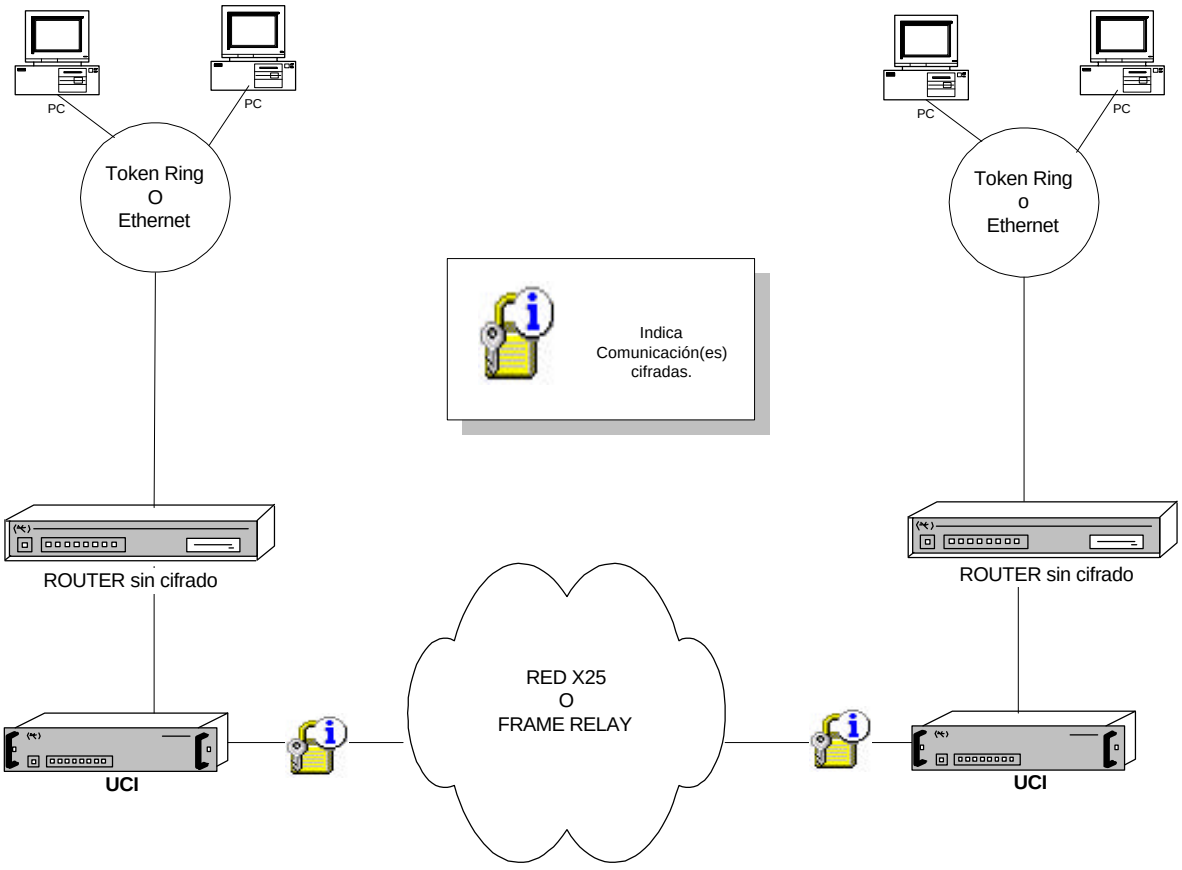

Figura 3: Configuración Router sin cifrado – UCI

d) Router Teldat con CGC

El ***CGC*** cambia la configuración de cifrado (claves y algoritmos de cifrado, etc.) de los ***ROUTER TELDAT*** y las ***UCI´***s a través de la red **WAN** (**X25** o **FRAME RELAY**). El ***ROUTER TELDAT*** de gestión se encarga de enviar la configuración de cifrado por la **WAN** de forma segura (sistema de clave pública RSA).

En caso de caída del enlace **WAN**, existe la posibilidad de transmitir la información cifrada desde el HOST hasta los ***ROUTER TELDAT*** a través de un enlace **RDSI**. Se empleará un ***CENTRIX*** para cifrar la información y enviarla a través de una línea **RDSI**.

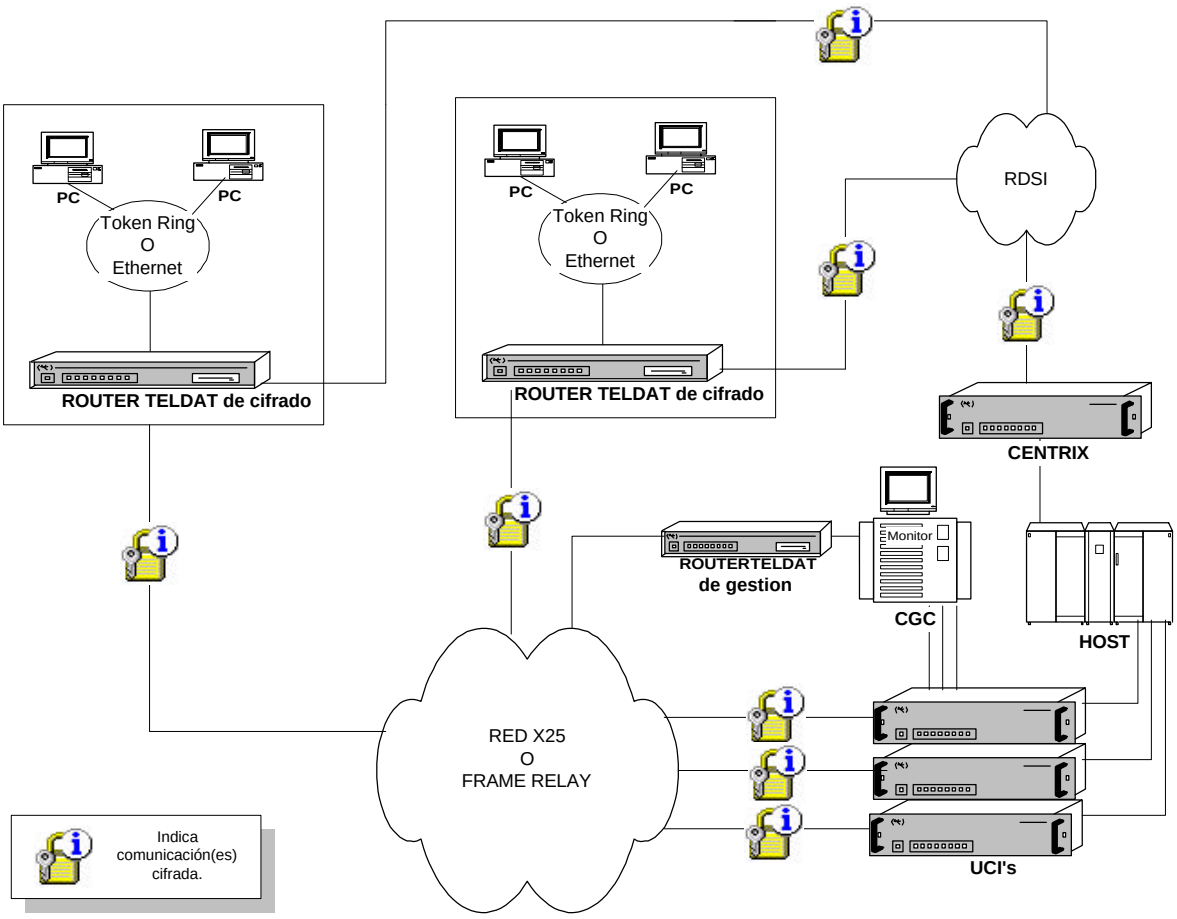

Figura 4: Configuración Router Teldat con CGC

La configuración del cifrado en los ROUTER TELDAT y UCI´s se realiza remotamente desde el CGC.

El CGC periódicamente (de forma automática) puede cambiar las claves secretas de las comunicaciones cifradas para aumentar la seguridad del sistema de criptográfico.

Capítulo 2
Configuración General

1. El Comando UCI

El comando **UCI** permite configurar la unidad de cifrado del ***ROUTER TELDAT***.

Sintaxis:

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

CFG

Este comando muestra la configuración de cifrado del ***ROUTER TELDAT***. Indica el número de DLCI´s y el número de parejas de NRI´s dadas de alta en el módulo de cifrado.

Sintaxis:

```
Config>UCI CFG
```

Ejemplo:

```
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

Este comando permite cambiar la configuración de cifrado del ***ROUTER TELDAT***. El equipo pregunta al usuario sobre cada uno de los parámetros.

Para poder ejecutar este comando se debe conocer la password de usuario, que por defecto es *teldat*.

Los cambios no tendrán efecto hasta después de reiniciar el equipo.

Sintaxis:

```
Config>UCI CHANGE CFG
```

Ejemplo:

```
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)
```

Los cambios que se pueden realizar en la configuración de cifrado con este comando son:

- "Interruption mode (y/other)?" permite habilitar (deshabilitar) el modo de interrupción de funcionamiento de la tarjeta de cifrado.
- Al inicializar el equipo se puede realizar un test a la tarjeta de cifrado con el algoritmo RSA si se responde afirmativamente a "Test RSA when starting (y/other)?"
- El número máximo de NRI´s se puede especificar.
- Habilita la comprobación de que las tramas recibidas son de cifrado si se responde "YES".

KEYS

Cambio de las claves de sesión por consola. No se utiliza en este equipo.

MODE

Permite cambiar el modo de trabajo del equipo de cifrado a transparente y a la inversa.

Para poder ejecutar este comando se debe conocer la password de usuario, que por defecto es *teldat*.

La ejecución de este comando tienen efecto inmediato.

Sintaxis:

```
Config>UCI MODE
```

Ejemplo:

```
Config>UCI MODE

User Password? ******

GENERAL STATUS: ENCRYPT(Yes/No)? y

    Updating encrypt configuration...
```

"UCI MODE" permite cambiar el modo de trabajo únicamente de los DLCI's y de las parejas de NRI's dados de alta en el módulo de cifrado.

USER_PASSWORD

Permite modificar el password de usuario. El conocimiento de esta password concede ciertos derechos, como por ejemplo, cambiar la configuración de cifrado del ***ROUTER TELDAT***.

Para poder ejecutar este comando se debe conocer el password de usuario, que por defecto es *"teldat"*.

La ejecución de este comando tienen efecto inmediato.

Sintaxis:

```
Config>UCI USER_PASSWORD
```

Ejemplo:

```
Config>UCI USER_PASSWORD

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

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

TABLE

Muestra una tabla con los interfaces FR activos en memoria estática, el número de DLCIs y el número de NRI´s dados de alta en el sistema de cifrado.

Sintaxis:

```
Config>UCI TABLE
```

Ejemplo:

```
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
```

Capítulo 3
Configuración del Interfaz Frame Relay

1. Introducción

En este capítulo se describen los comandos de configuración del cifrado para los circuitos del interfaz **FRAME RELAY**.

- Dar de alta el cifrado en un circuito **FRAME RELAY**.
- Configurar el cifrado en un circuito **FRAME RELAY** : cambiar modo, claves etc…
- Dar de baja el cifrado en un circuito **FRAME RELAY**.
- Listar la configuración de cifrado del interfaz **FRAME RELAY**.

Los comandos tratados en este capítulo se encuentran en el menú de configuración del interfaz **FRAME RELAY** en uso.

2. Alta de cifrado de un circuito

Cuando se añade el DLCI o cuando se modifica la configuración del DLCI, se permite dar de alta el cifrado del circuito si se responde afirmativamente a la pregunta : "Encrypt Information?".

El cifrado del circuito dado de alta se configura automáticamente en modo ***DES*** sin ***CBC***.

Sintaxis:

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

o

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

Ejemplo 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>
```

Ejemplo 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>
```

El cifrado del circuito dado de alta se configura automáticamente en modo DES sin CBC con una clave por defecto.

Esta configuración por defecto se puede modificar con el comando SET ENCRYPTION.

3. El Comando SET ENCRYPTION

El comando "SET ENCRYPTION" permite modificar el cifrado en un circuito del interfaz **FRAME RELAY**. Este comando configura el cifrado en un circuito dado de alta anteriormente.

Para poder ejecutar este comando se debe conocer la password de usuario, que por defecto es "*teldat*".

Sintaxis:

```
FR config>SET ENCRYPTION
```

Ejemplo:

```
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>
```

- ***Se puede elegir entre varios algoritmos de cifrado (DES con o sin CBC , TRIPLE DES con o sin CBC) o modo transparente. En TRIPLE DES, se introducen dos claves, y en DES se introduce una sola clave. Las claves se deben de introducir dos veces seguidas para confirmarlas.***
- ***Un DLCI configurado por el CGC, no puede ser modificado por consola.***

4. Baja de cifrado en un circuito

Cuando se modifica la configuración del DLCI, se permite dar de baja el cifrado del circuito si se responde “NO” a la pregunta : “Encrypt Information?”.

Sintaxis:

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

Ejemplo:

```
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. El Comando LIST ENCRYPTION

El comando LIST ENCRYPTION permite listar la configuración de cifrado de todos los circuitos dados de alta en el módulo de cifrado. La respuesta a la pregunta, "CGC?", permite ver si el circuito ha sido configurado por CGC o por consola.

El comando LIST ENCRYPTION permite listar la configuración de cifrado de todos los DLCI´s que se han dado de alta. Se indica el algoritmo de encriptación utilizado: ***DES*** o ***TRIPLE DES***(***3DES***) con o sin ***CBC***. Si el circuito dado de alta no se cifra, se señaliza como ***CLEAR***(***CLR***).

Sintaxis:

```
FR config>LIST ENCRYPTION
```

Ejemplo:

```
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>
```

- ***Un circuito dado de alta en el módulo de cifrado puede estar configurado en modo transparente (Clear). Los datos enviados (recibidos) por ese circuito no se cifran (descifran).***
- ***Toda modificación realizada en la configuración del cifrado tiene efecto inmediato grabándose automáticamente en memoria no volátil.***

Capítulo 4
Configuración en X25

1. Introducción

En este capítulo se describen los comandos de configuración del cifrado para cada pareja de NRI´s de **X.25**.

- Establecer/eliminar el cifrado en las parejas de NRI´s.
- Listar la configuración de cifrado de **X.25**.

Los comandos tratados en este capítulo se encuentran en el menú de configuración de **X.25**.

2. El Comando SET ENCRYPTION

El comando "SET ENCRYPTION" permite dar de alta o de baja el cifrado para una pareja de NRI´s .

También permite establecer la Confirmación Extremo a Extremo ("GLOBAL CONFIRMATION") y la Fragmentación Estándar ("STANDARD FRAGMENTATION").

Sintaxis:

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

SET ENCRYPTION UP

Este comando da de alta el cifrado para una pareja de NRI´s.

Para poder ejecutar este comando se debe conocer la password de usuario, que por defecto es "*teldat*".

Se puede elegir entre varios algoritmos de cifrado (***DES*** con o sin ***CBC*** , ***TRIPLE DES*** con o sin ***CBC***) o modo en modo transparente. En ***TRIPLE DES***, se introducen dos claves, y en ***DES*** se introduce una sola clave. Las claves se deben de introducir dos veces seguidas para confirmarlas**.**

Sintaxis:

```
X25 Config>SET ENCRYPTION UP
```

Ejemplo:

```
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>
```

- ***Se puede elegir entre varios algoritmos de cifrado (DES con o sin CBC , TRIPLE DES con o sin CBC) o modo en modo transparente. En TRIPLE DES, se introducen dos claves, y en DES se introduce una sola clave. Las claves se deben de introducir dos veces seguidas para confirmarlas.***

SET ENCRYPTION DOWN

Este comando da de baja el cifrado para una pareja de NRI's.

Para poder ejecutar este comando se debe conocer la password de usuario, que por defecto es "*teldat*".

El equipo pregunta al usuario sobre la pareja de NRI´s a dar de baja.

Sintaxis:

```
X25 Config>SET ENCRYPTION DOWN
```

Ejemplo:

```
X25 Config>SET  ENCRYPTION DOWN

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

Another(Yes/No)?

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

SET ENCRYPTION CONFIRMATION

Este comando establece o elimina la Confirmación Extremo a Extremo ("GLOBAL CONFIRMATION") para todas las parejas de NRI's. No tiene ningún efecto sobre los conectados configurados por el CGC.

Para poder ejecutar este comando se debe conocer la password de usuario, que por defecto es "*teldat*".

Sintaxis:

```
X25 Config>SET ENCRYPTION CONFIRMATION
```

Ejemplo:

```
X25 Config> SET ENCRYPTION CONFIRMATION

X25 ENCRYPTION CONFIGURATION

Entry   Called NRI      Calling NRI     Type CBC CGC
======= =============== =============== ==== === ===
0       333333          444444          DES  No  No
1       444444          555555          3DES No  No
2       999999          888888          CLR  --  No

Last configured NRI's date: 14/02/00 13:15:29
X25 Config>
```

SET ENCRYPTION FRAGMENTATION

Este comando establece o elimina la Fragmentación Estándar ("STANDARD FRAGMENTATION") para todas las parejas de NRI's. No tiene ningún efecto sobre los conectados configurados por el CGC.

Para poder ejecutar este comando se debe conocer la password de usuario, que por defecto es "*teldat*".

Sintaxis:

```
X25 Config>SET ENCRYPTION FRAGMENTATION
```

Ejemplo:

```
X25 Config>SET ENCRYPTION FRAGMENTATION

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

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

- ***Los comandos "SET ENCRYPTION CONFIRMATION" y "SET ENCRYPTION FRAGMENTATION" no tiene ningún efecto sobre los conectados del CGC. Los conectados del CGC tendrán su propia configuración de Fragmentación Estándar y de Confirmación Extremo a Extremo.***
- ***Toda modificación realizada en la configuración del cifrado tiene efecto inmediato grabándose automáticamente en memoria no volátil.***
- ***Un DLCI configurado por el CGC, no puede ser modificado por consola.***

3. El Comando LIST ENCRYPTION

El comando LIST ENCRYPTION permite listar la configuración de cifrado de todos las parejas de NRI´s que se han dado de alta. Se indica el algoritmo de encriptación utilizado: ***DES*** o ***TRIPLE DES***(***3DES***) con o sin ***CBC***. Si el conectado dado de alta no se cifra, se señalizará como ***CLEAR***(***CLR***).

Adicionalmente, se indica si el conectado ha sido configurado por el ***CGC*** o por consola.

Sintaxis:

```
X25 Config>LIST ENCRYPTION
```

Ejemplo:

```
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>
```

Capítulo 5
Monitorización del Cifrado

1. Introducción

En este capítulo se describen los comandos de monitorización del cifrado para el interfaz **FRAME RELAY** y **X.25**.

- Estadísticas de cifrado.
- Historial de llamadas **X.25** con cifrado.

Los comandos tratados en este capítulo se encuentran en el menú principal de monitorización.

2. Comandos

El comando ***UCI*** permite visualizar estadísticas de cifrado del ***ROUTER TELDAT***.

Sintaxis:

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

HELP_STATISTICS

Muestra información sobre el significado de los campos de estadísticos.

Sintaxis:

```
+UCI HELP_STATISTICS
```

Ejemplo:

```
+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

Pone a cero los contadores de estadísticas de cifrado y comienza una nueva sesión de toma de datos. Al ejecutar este comando, el equipo ofrece al usuario la opción de inicialización de estadísticas de cifrado para un circuito en concreto.

Sintaxis:

```
+UCI INIT_STATISTICS
```

Ejemplo:

```
+UCI INIT_STATISTICS

dlci encrypt statistics (<ENTER> = All)?

+
```

STATISTICS

Muestra estadísticas relativas a cifrado.

Sintaxis:

```
+UCI STATISTICS
```

Ejemplo:

```
+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

+
```

Las estadísticas se dividen en tres apartados, paquetes recibidos, paquetes transmitidos y paquetes procesados.

- Paquetes recibidos: se indican los paquetes recibidos cifrados (“ENCRYPTED”) y descifrados (“DECRYPTED”). Además aparecen los estadísticos de tramas erróneas : la trama recibida tenía una longitud excesiva o no coincidía con la indicada en la cabecera de cifrado (“TOO LARGE”), error en la recepción de trama (“FAILURE”), imposibilidad de transmitir trama recibida porque el destino no esta preparado (“WITHOUT.LINE”), imposible de descifrar la trama recibida (“WRONG.ENCRYPT”), no hay suficiente memoria para la trama que se quiere transmitir(“WITHOUT.MEM”).
- Paquetes transmitidos: análogamente se indican los paquetes recibidos cifrados y descifrados.
- Paquetes procesados: contabiliza los paquetes procesados en el router cifrados (“ENCRYPTED”), descifrados (“DECRYPTED”), cifrados con la clave por defecto (“DEC.KEY.DEF”) o los paquetes en modo transparente (“TRANSPARENT”).

LINE_X25

Lista las últimas llamadas enviadas en **X.25**:

- El canal del nivel de enlace esta indicado en el campo: “CHANN”.
- “IN TABLES” indica que la pareja de NRI´s esta dada de alta en el módulo de cifrado.
- “PSSWD CHANGE” indica que ha habido cambio de claves automático en el modo CBC al establecerse la conexión.

Sintaxis:

```
+UCI LINE_X25
```

Ejemplo:

```
+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

Borra todo la lista de llamadas enviadas en **X.25**.

Sintaxis:

```
+UCI RESET_LINE_X25
```

Ejemplo:

```
+UCI RESET_LINE_X25

    Encrypted / decrypted calls list reset
+
```

Capítulo 6
Problemas de Configuración

1. Incompatibilidad con el CGC

La configuración del cifrado por consola no es compatible con la configuración del cifrado a través del Centro Gestor de Claves(***CGC***). No se puede trabajar a la vez con parejas (de DLCI´s o de NRI´s) configurados por el ***CGC*** y con circuitos configurados por consola.

2. Comprobaciones Utiles

En caso de que el cifrado no funcione correctamente, se comprobará que:

- "Flag Crypto" debe estar en el mismo estado (activo u inactivo) en los dos extremos.

- Se ha configurado la misma clave en las ***UCI***´s y en las oficinas para un mismo DLCI o pareja de NRI´s.

- El modo general en la ***UCI*** y en las oficinas es "Encrypt".

- Cuando se configura el cifrado FRAME RELAY en una oficina (por el ***CGC***) , anteriormente debe de estar configurado el DLCI con la opción de cifrado activada("Encrypt: YES").

- Verificar que no hemos reseteado una oficina antes de que se haya grabado la configuración de cifrado en disco. Si esto se ha producido, volver a introducirla la configuración de cifrado.

- No se puede intercambiar la configuración de cifrado del disquete entre ***ROUTERS TELDAT*** diferentes. Cada configuración de cifrado funciona únicamente en la oficina que la creó.

- Sólo para configuración por consola.

  -"Fragmentación Estándar" (Standard Fragmentation) es la misma en la oficina y en la ***UCI*** con la que esta enfrentada.

  -Cuando se actualiza el software de la versión 7.5 a la nueva versión de cifrado, se obtiene: NO hay "Fragmentación Estándar " (Standard Fragmentation) y NO hay "Confirmación Global" (Global Confirmation). Si esta configuración no es adecuada para su red **X.25**, debe modificarla con "SET ENCRYPTION CONFIMATION" o "SET ENCRYPTION FRAGMENTATION".