UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.272

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(03/2000)

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Interconexión de sistemas abiertos – Protocolos de seguridad

Compresión y privacidad de datos por redes de retransmisión de tramas

Recomendación UIT-T X.272

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	**X.270–X.279**
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.272

Compresión y privacidad de datos por redes de retransmisión de tramas

Resumen

Esta Recomendación define el servicio de compresión y privacidad de datos por redes de retransmisión de tramas. La presencia de un servicio de compresión de datos (DC) en una red se traducirá por un aumento de su caudal efectivo.

Por otro lado, la creciente demanda de transmisión de datos sensibles a través de redes públicas requiere dispositivos que garanticen la privacidad de los datos. Para obtener relaciones de compresión óptimas es necesario comprimir los datos antes de criptarlos. En consecuencia, es conveniente que en la especificación del servicio de compresión de datos se especifiquen medios que permitan negociar también protocolos de criptación de datos. Como la tarea de comprimir datos y después criptarlos exige una intensa actividad de cálculo, se han propuesto algunos protocolos en los que las operaciones de compresión y de criptación de datos se refunden en una sola (compresión securizada de datos). Este servicio combinado se designa por servicio de compresión y privacidad de datos por retransmisión de tramas.

Orígenes

La Recomendación UIT-T X.272, preparada por la Comisión de Estudio 7 (1997-2000) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la CMNT el 31 de marzo de 2000.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la CMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Introducción

La presente Recomendación especifica los procedimientos para obtener la compresión y privacidad de datos por retransmisión de tramas. Trata el campo de control que utiliza tramas de información no numerada (UI, *unnumbered information*). No trata las tramas de información numerada (tramas I).

Recomendación UIT-T X.272

Compresión y privacidad de datos por redes de retransmisión de tramas

1 Ámbito

Esta Recomendación abarca los protocolos empleados para negociación y encapsulación de compresión de datos, la compresión securizada de datos, autenticación y criptación por retransmisión de tramas. Estos protocolos se basan en el protocolo de control del enlace (IETF RFC 1661) [13], el protocolo de control de criptación (IETF RFC 1968) [14], y el protocolo de criptación DES (IETF RFC 1969) [15], que son protocolos del tipo punto a punto (PPP, *point-to-point protocol*).

Esta Recomendación se aplica a tramas de información no numerada (UI, *unnumbered information*) encapsuladas por el procedimiento del anexo E a la Recomendación Q.933 [7]. Trata la compresión y privacidad de datos en conexiones virtuales permanentes (PVC, *permanent virtual connections*) y conexiones virtuales conmutadas (SVC, *switched virtual connections*).

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones, por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

[1] UIT-T I.122 (1993), *Marco para los servicios portadores en modo trama*.

[2] UIT-T I.233.1 (1991), *Servicio portador RDSI con retransmisión de tramas*.

[3] UIT-T I.370 (1991), *Gestión de la congestión para el servicio portador RDSI de retransmisión de tramas*.

[4] UIT-T E.164 (1991), *Plan de numeración para la RDSI*.

[5] UIT-T Q.922 (1992), *Especificación de la capa de enlace de datos de la RDSI para servicios portadores en modo trama*.

[6] UIT-T Q.921 (1993), *Interfaz usuario-red de la RDSI – Especificación de la capa de enlace de datos*.

[7] UIT-T Q.933 (1995), *Sistema de señalización digital de abonado N.º 1 – Especificaciones de señalización para el control y la monitorización de la situación de conexiones virtuales conmutadas y permanentes en modo trama*.

[8] UIT-T Q.931 (1993), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de llamada básica*.

[9] UIT-T Q.850 (1993), *Utilización de los elementos de información causa y ubicación en el sistema de señalización digital de abonado N.º 1 y en la parte usuario de la RDSI del sistema de señalización N.º 7*.

[10] UIT-T Q.951 (1993), *Descripción de la etapa 3 para servicios suplementarios de identificación de números que utilizan el sistema de señalización de abonado digital N.º 1*.

[11] UIT-T X.36 Enmienda 1 (1996), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para redes públicas de datos que prestan servicios de transmisión de datos con retransmisión de tramas por circuitos especializados.*

[12] UIT-T X.121 (1992), Plan de numeración internacional para redes públicas de datos.

[13] IETF RFC 1661/STD 51 (1994), *The Point-Point Protocol*.

[14] IETF RFC 1968 (1996), *The PPP Encryption Control Protocol (ECP)*.

[15] IETF RFC 1969 (1996), *The PPP DES Encryption Protocol (DESE)*.

[16] IETF RFC 1570 (1994), *PPP LCP Extensions*.

[17] IETF RFC 1993 (1996), *PPP Gandalf FZA Compression Protocol*.

[18] IETF RFC 1340 (1992), *Assigned Numbers*.

[19] IETF RFC 1994 (1996), *PPP Challenge Handshake Authentication Protocol (CHAP)*.

[20] IETF RFC 1974 (1996), *PPP Stac LZS Compression Protocol*.

[21] IETF RFC 1829 (1995), *The ESP DES-CBC Transform*.

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

3.1 antiexpansión: Método para inhibir la expansión de datos de usuario debida a la codificación de compresión.

3.2 contexto de compresión de datos: Vocabulario y otras informaciones para detección de errores y sincronización, creados y mantenidos por entidades pares para codificar/decodificar datos de usuario.

3.3 función de compresión de datos: Entidad que efectúa la codificación de compresión de datos, decodificación, detección de errores, sincronización, y negociación.

3.4 definición de función de compresión de datos: Especificación que describe el formato y procedimientos utilizados por una función de compresión de datos para transportar datos de usuario y primitivas de control.

3.5 decodificador: Entidad que descomprime datos de usuario.

3.6 codificador: Entidad que comprime datos de usuario.

3.7 memoria intermedia de historia: Tipo de vocabulario utilizado para compresión de datos.

3.8 0x: Designa números hexadecimales.

3.9 octeto de verificación longitudinal (LCB, *longitudinal check byte*): Se calcula para cada trama de la manera siguiente:

1) se aplica el operador OR exclusivo (XOR) a 0xFF y al primer octeto de la cabida útil, y se almacena el resultado. Seguidamente,
2) se aplica el operador XOR al resultado así obtenido y al octeto siguiente de la cabida útil, obteniéndose un nuevo resultado con el se generará el valor siguiente, y así sucesivamente para cada octeto subsiguiente de la cabida útil.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas.

A Bit de autenticación (*authentication bit*)

ACK Acuse de recibo (*acknowledgement*)

CBC Concatenación de bloques cifrado (*cipher block chaining*)

CCP Protocolo de control de compresión (*compression control protocol*)

C/D Control/datos (*control/data*)

CHAP Protocolo de autenticación de invitación de toma de contacto (*challenge handshake authentication protocol*)

C_Mode-1 Modo 1 de compresión de datos por defecto (*default data compression mode 1*)

C/R Encabezamiento de trama (*frame header*) descrito en UIT-T Q.922

C/U Comprimido/no comprimido (*compressed/uncompressed*)

DC Compresión de datos (*data compression*)

DCCI Identificador de contexto de compresión de datos (*data compression context identifier*)

DCFD Definición de función de compresión de datos (*data compression function definition*)

DCP Protocolo de compresión de datos (*data compression protocol*)

DCPCP Protocolo de control DCP (*DCP control protocol*)

DES Norma de criptación de datos (*data encryption standard*)

DLCI Identificador de control de enlace de datos (*data link control identifier*)

DTE Equipo terminal de datos (*data terminal equipment*)

E_Mode-1 Modo 1 de criptación de datos por defecto (*default data encryption mode 1*)

Ext. Bit de extensión (*extension bit*)

FCS Secuencia de verificación de trama (*frame check sequence*) descrita en UIT-T Q.922

FECN Encabezamiento de trama (*frame header*) descrito en UIT-T Q.922

FR Retransmisión de tramas (*frame relay*)

FRCP Protocolo de compresión y privacidad de datos por retransmisión de tramas (*frame relay compression and privacy protocol*)

FZA Algoritmo de compresión securizada de datos (*secure data compression algorithm*)

LCB Octeto de verificación longitudinal (*longitudinal check byte*)

LCP Protocolo de control de enlace (*link control protocol*)

LZS Algoritmo de compresión de datos (*data compression algorithm*)

NLPID Identificador de protocolo de capa de red (*network layer protocol identifier*)

OUI Identificador único de organización (*organization unique identifier*)

PDU Unidad de datos de protocolo (*protocol data unit*)

PVC Conexión virtual permanente (*permanent virtual connection*)

RA Acuse de recibo de reiniciación (*reset acknowledge*)

S_Mode-1 Modo 1 de compresión securizada de datos por defecto (*default secure compression mode 1*)

SCA Algoritmo de compresión securizada de datos (*secure data compression algorithm*)

SVC Conexión virtual conmutada (*switched virtual connection*)

XOR Operador booleano OR exclusivo (*booelan exclusive OR*)

5 Convenios

En esta Recomendación se utilizan ciertas palabras y construcciones gramaticales para precisar el significado de distintos elementos. Estas palabras y construcciones gramaticales son las siguientes:

- "Tener que", el tiempo futuro del modo indicativo de los verbos, u "obligatorio" indican que el elemento en cuestión es un requisito cuyo cumplimiento es imperativo.

- "Deber" indica que el elemento, aunque no obligatorio, es muy deseable.
- "Poder" o "facultativo" indican que el elemento no es obligatorio y que el implementador puede tenerlo o no en cuenta según sus necesidades.
- "No aplicable" indica que el elemento está fuera del ámbito de la presente Recomendación.

6 Visión general

Esta Recomendación especifica la encapsulación de protocolo de compresión y privacidad de datos por retransmisión de tramas (FRCP, *frame realy compression and privacy protocol*) a través de redes de retransmisión de tramas. Permite la negociación e implementación de varias facilidades tales como procedimientos de autenticación, facilidad de compresión de datos, facilidad de compresión securizada de datos, y facilidad de criptación de datos. El FRCP proporciona dos modos de funcionamiento para la facilidad de criptación:

- E_Mode-1: E_Mode-1 es el modo por defecto y es obligatorio para toda implementación que soporte la facilidad de criptación. Permite la negociación de parámetros de encripción. El algoritmo de criptación por defecto propuesto es, la clave de 56 bits de la norma de criptación de datos (DES, *data encryption standard*) con concatenación de bloques cifrado (CBC, *cipher block chaining*) [21]. La clave secreta de la norma de criptación de datos (DES) compartida entre las partes comunicantes tiene una longitud total de ocho octetos. De los 64 bits de estos ocho octetos, 56 bits forman la clave utilizada por el algoritmo de la norma de criptación de datos (DES). La clave de 56 bits está contenida en los siete bits más significativos de los ocho octetos, siendo el bit menos significativo de cada octeto el bit de paridad.
- E_Mode-2. E_Mode-2 es facultativo y permite la negociación completa de algoritmos de criptación, tanto de algoritmos estándar como de algoritmos de propiedad privada, así como la negociación de los parámetros correspondientes. Este modo se basa en el protocolo de control de criptación para los protocolos punto a punto (PPP, *point to point protocol*) [14]. Este modo puede utilizarse para soportar claves de criptación de longitud superior a 56 bits. El tamaño de la clave es específico del vendedor.

El FRCP proporciona asimismo dos modos de funcionamiento para la facilidad de compresión securizada de datos:

- S_Mode-1: S_Mode-1 es el modo obligatorio y emplea los algoritmos y formatos de trama por defecto definidos en la presente Recomendación. S_Mode-1 proporciona un protocolo de negociación simple para ofrecer el servicio de compresión securizada de datos con parámetros por defecto. El algoritmo de compresión securizada de datos requiere la utilización de una clave de criptación. La clave de criptación compartida entre las partes comunicantes tiene una longitud de ocho octetos. Esta clave se compone de una cantidad utilizada de 56 bits, la cual se almacena como cantidad de 64 bits (ocho octetos), empleándose como bit de paridad el bit menos significativo de cada octeto.
- S_Mode-2: S_Mode-2 es facultativo y permite la negociación completa de algoritmos de compresión securizada de datos y los parámetros correspondientes.

El FRCP proporciona además dos modos de funcionamiento para la facilidad de compresión de datos:

- C_Mode-1: C_Mode-1 es el modo obligatorio y utiliza los algoritmos y formatos de trama por defecto definidos en la presente Recomendación. C_Mode-1 proporciona un protocolo de negociación simple para ofrecer el servicio de compresión de datos con parámetros por defecto.

- C_Mode-2: C_Mode-2 es facultativo y permite la negociación completa de algoritmos de compresión de datos, tanto de algoritmos estándar como de algoritmos de propiedad privada, y sus parámetros correspondientes.

7 Modelo de referencia

El término "**DTE**" en el contexto de esta Recomendación no está circunscrito a la función de equipo terminal. Indica un usuario de la red en un sentido funcional general, usuario que, a su vez, podría ser otra red (incluso de otro tipo).

El servicio FRCP facilita una comunicación eficaz en términos de una mayor velocidad de paquetes/tramas que la que podría obtenerse de una manera securizada si se negociara la opción de privacidad. Cuando se utiliza entre los DTE, como se muestra en la figura 1, el procedimiento de compresión de datos y privacidad es transparente a la red o redes de retransmisión de tramas entre el DTE transmisor y el receptor.

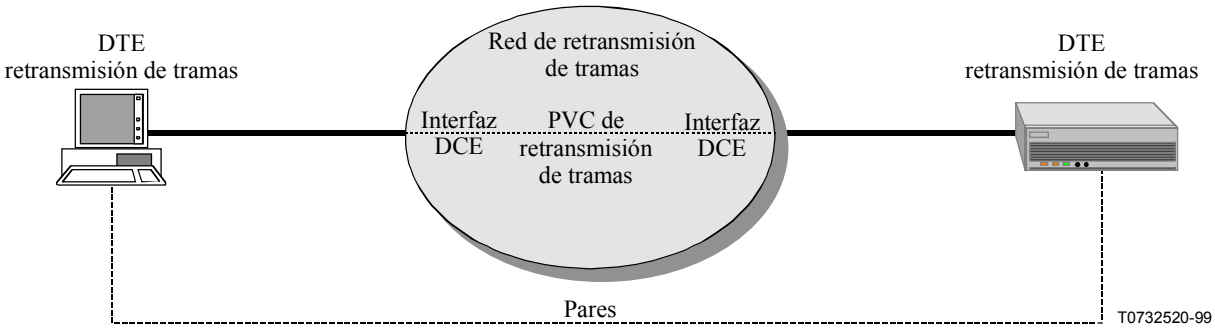

Figura 1/X.272 – Diagrama de referencia

En el curso de la negociación de las facilidades soportadas, el protocolo de compresión de datos y privacidad por retransmisión de tramas pasa por diferentes fases. Estas fases, en su orden, son la siguientes:

1) Fase de establecimiento de la conexión virtual: Esta fase está controlada por los procedimientos de señalización para PVC o SVC [1] a [12] y está fuera del ámbito de la presente Recomendación. La fase FRCP comienza después de que se ha establecido la conexión virtual.

2) Fase de autenticación: Cuando se utiliza, la autenticación inicial de la entidad par debe efectuarse antes de la(s) fases(s) de compresión de datos o criptación. Las subsiguientes invitaciones a autenticación , si están soportadas por el protocolo de autenticación escogido, pueden efectuarse en la fase de transferencia de datos, en texto ordinario, sin utilizar facilidades de criptación, compresión securizada, ni compresión (simple).

3) Fase de negociación de criptación: Se utiliza para negociar el modo y los parámetros que habrán de utilizarse para la criptación durante la fase de transferencia de datos.

4) Fase de negociación de compresión securizada de datos: Se utiliza para negociar el modo y los parámetros que se emplean para la compresión securizada de datos durante la fase de transferencia de datos.

5) Fase de negociación de compresión de datos: Se utiliza para negociar el modo y los parámetros que se emplean para la compresión de datos durante la fase de transferencia de datos.

6) Fase de transferencia de datos: En esta fase se efectúa la transferencia de mensajes comprimidos en forma securizada o comprimidos (simplemente), en lenguaje cifrado; estos mensajes pueden incluir datos de usuario e información de control.

8 Especificación del modo común

En esta cláusula se definen los formatos de trama y los procedimientos comunes a todas las facilidades FRCP.

8.1 Formato general de las tramas

La estructura general de las tramas FRCP soporta la encapsulación de información de control o la transferencia de datos. Todas las tramas se envían por la conexión virtual de retransmisión de tramas entre sistemas de extremo. El contenido de las tramas es transparente a la red de retransmisión de tramas. Las tramas de control contienen la información que es esencial para la negociación de las facilidades de autenticación, criptación, compresión securizada de datos, compresión de datos y sus parámetros correspondientes. El bit C/D del FRCP distingue entre tramas de control y tramas de datos. Para tramas de control el bit C/D se fija a 1. Para la negociación de la información de control se utiliza el formato general de las tramas de control FRCP descrito en la siguiente figura 2.

Descripción								Octeto
Dirección Q.922 (2 octetos) (nota)								1 2
Control (UI: 0x03)								3
NLPID (0xB0)								4
Encabezamiento FRCP								
Ext. 1	Reserva	Reserva	Reserva	Reserva	I	D	C/D 1	5
Cabida útil FRCP								6 n
FCS (2 octetos)								n+1 n+2

NOTA – La dirección de retransmisión de tramas se presenta en formato de 2 octetos a título ilustrativo. Los formatos de dirección de 3 y 4 octetos no están prohibidos

Figura 2/X.272 – Formato de la trama de control del protocolo de compresión y privacidad de datos por retransmisión de tramas

La dirección de retransmisión de tramas Q.922 [5] en la figura 2 se presenta en formato de dos octetos. Sin embargo, el FRCP no prohíbe la utilización de los formatos de dirección con un tercer y cuarto octeto. Véase el cuadro 1.

Cuadro 1/X.272 – Formato de la trama de control del protocolo de compresión y privacidad de datos por retransmisión de tramas

Campo	Descripción
Dirección Q.922	Estructura de dirección de retransmisión de tramas definida en UIT-T Q.922 [5]
Control	Trama de información no numerada (UI) (x03) para retransmisión de tramas Q.922 [5]
NLPID	ID de protocolo de capa de red
Encabezamiento FRCP	El encabezamiento de protocolo FRCP consta de lo siguiente: • Ext.: Bit de extensión, fijado a uno • Reserva: Bits de reserva para uso futuro, fijados a 0 • ID (dos bits): Este campo especifica la facilidad utilizada. Las facilidades se definen a continuación: I D 0 0 Reservado 0 1 Compresión 1 0 Comprensión securizada 1 1 Criptación • A: Bit de autenticación. Sólo puede fijarse a 1 cuando C/D = 1. Indica que la trama contiene información de autenticación • Bit de control/datos (C/D) 0 Trama de datos 1 Trama de control
Cabida útil FRCP	Información de control o datos, según los valores a que se hayan fijado los bits del encabezamiento FRCP.
FCS	Secuencia de verificación de trama Q.922

Si el bit C/D está fijado a 1, la trama es una trama de control. El campo ID se utiliza en este caso para negociar diversas facilidades del FRCP. Las facilidades se negocian una por una en el orden indicado en 8.2. Los detalles del formato de trama se dan en secciones conexas. Si el bit A está fijado a 1, se hace caso omiso del campo ID pues se trata de una trama de autenticación.

Si el bit C/D está fijado a 0, la trama es una trama de datos. El formato de la trama de datos depende de la facilidad o facilidades FRCP que se han negociado. La figura 3 representa el formato general de la trama de datos FRCP. La descripción de los diversos campos se presenta en el cuadro 2.

Descripción								Octeto
Dirección Q.922 (2 octetos) (nota)								1 2
Control (UI: 0x03)								3
NLPID (0xB0)								4
Encabezamiento FRCP								
Ext. 1	C/U	RA	RR	O	P	T	C/D 0	5
Cabida útil FRCP								6 n
FCS (2 octetos)								n+1 n+2

NOTA – La dirección de retransmisión de tramas se presenta en formato de 2 octetos a título ilustrativo. Los formatos de dirección de 3 y 4 octetos no están prohibidos.

Figura 3/X.272 – Formato de la trama de datos del protocolo de privacidad por retransmisión de tramas

Cuadro 2/X.272 – Formato de la trama de datos del protocolo de privacidad por retransmisión de tramas

Campo	Descripción
Dirección Q.922	Estructura de dirección de retransmisión de tramas que contiene DLCI, FECN, BECN, DE y C/R. El bit C/R no se utiliza
Control	Trama de información no numerada (UI) (x03) Q.922 para retransmisión de tramas
NLPID	ID de protocolo de capa de red de ISO/CEI TR 9577
FRCP Header	El encabezamiento de protocolo FRCP consta de lo siguiente: • Bit de extensión – Fijado a uno, pero incluido con miras a futuras mejoras. • Comprimido/no comprimido (C/U): Puesto a 1 para indicar que los datos no están comprimidos. • Reset_Ack (RA): Puesto a 1 para indicar el acuse de recibo de una reiniciación de una historia de compresión o de una historia de criptación. La distinción entre los tipos de historias viene dada por los bits O, P, T. • Reset_Request (RR): Puesto a 1 para indicar la petición de una reiniciación de una historia de compresión o de una historia de criptación. La distinción entre los tipos de historias viene dada por los bits O, P, T. • Bit de control/datos (C/D): Puesto a 0 para indicar una trama de datos. • Opción de protocolo (OPT, *protocol option*): Relaciona los datos con el correspondiente protocolo de acuerdo con la siguiente asignación: O P T 0 0 0 Reservado 0 0 1 Criptación 0 1 0 Compresión securizada 0 1 1 Compresión 1 0 0 Compresión y criptación 1 0 1 Compresión securizada y criptación x x x Todos los demás están reservados

Cuadro 2/X.272 – Formato de la trama de datos del protocolo de privacidad por retransmisión de tramas (*fin*)

Campo	Descripción
Cabida útil FRCP	Datos que son comprimidos o criptados, según la facilidad o facilidades FRCP que se hayan negociado
FCS	Secuencia de verificación de trama Q.922

8.2 Negociación de facilidades

En la etapa de negociación, el bit C/D del encabezamiento FRCP se fija a 1 para indicar que la trama es una trama de control. El formato de la trama de control permite la negociación de varias facilidades. Cada facilidad se negocia por separado. El orden de negociación de las facilidades es el siguiente:

- Si está configurada la autenticación, hay que comenzar por la autenticación de las entidades pares. Si la etapa de autenticación finaliza con éxito, pueden negociarse otras facilidades. Por el contrario, si la etapa de autenticación no finaliza con éxito, hay que terminar la conexión.
- Si está configurada la opción de criptación, hay que negociarla seguidamente. Si la negociación tiene éxito, pueden negociarse a continuación otras opciones. Por el contrario, si la negociación de la criptación fracasa, hay que terminar la conexión.
- Si está configurada la opción de compresión securizada de datos, hay que negociar esta opción seguidamente. Si la negociación tiene éxito, hay que efectuar una compresión securizada de los datos antes de antes de enviarlos por el enlace. Si la negociación de la compresión securizada fracasa, la etapa de transferencia de datos puede proseguir sin una compresión securizada de datos si, y solamente si, la facilidad de criptación está configurada y ha sido negociada con éxito. De no ser así, hay que terminar la conexión.
- La opción de compresión de datos puede ser configurada y negociada siempre que la opción de compresión securizada de datos no esté configurada. Si la opción de compresión de datos está configurada, esta opción se negocia a continuación. Si la negociación tiene éxito, se pueden enviar por el enlace datos comprimidos. Si la opción de criptación está configurada y se ha negociado con éxito, los datos tienen que estar criptados. Si no está configurada ninguna otra opción más, se pueden transmitir por el enlace datos no comprimidos si la negociación de la facilidad de compresión de datos no tuvo éxito. En otro caso, hay que criptar los datos antes de transmitirlos por el enlace.
- Si en la negociación se sigue un orden diferente del mencionado, hay que terminar la conexión. El orden de negociación se recapitula en el siguiente cuadro 3:

Cuadro 3/X.272 – Orden de negociación de las facilidades

Facilidad solicitada / **Facilidad negociada**	**Autenticación**	**Criptación**	**Compresión securizada**	**Compresión**
Ninguna	Proseguir	Proseguir	Proseguir	Proseguir
Autenticación	Proseguir	Proseguir	Proseguir	Proseguir
Criptación	Terminar	Proseguir	Proseguir	Proseguir
Compresión securizada	Terminar	Terminar	Proseguir	Terminar

Cuadro 3/X.272 – Orden de negociación de las facilidades (*fin*)

Facilidad solicitada / Facilidad negociada	Autenticación	Criptación	Compresión securizada	Compresión
Compresión	Terminar	Terminar	Terminar	Proseguir
Autenticación, criptación	Proseguir	Proseguir	Proseguir	Proseguir
Autenticación, criptación, compresión securizada	Proseguir	Proseguir	Proseguir	Terminar
Autenticación, compresión	Proseguir	Terminar	Terminar	Proseguir
NOTA – Después de la negociación con éxito de cualquier facilidad, todas las tramas intercambiadas en una conexión deben ser encapsuladas utilizando el formato FRCP.				

9 Facilidad de autenticación

Esta facilidad se utiliza para autenticar dos dispositivos por medio de un protocolo de autenticación preseleccionado. La facilidad de autenticación es facultativa. Si se desea autenticación, una implementación deberá efectuar la autenticación inicial antes de invocar las facilidades de criptación, compresión securizada de datos, o compresión.

Los paquetes de autenticación se identifican mediante el bit **A** en el encabezamiento FRCP de una trama de control (C/D = 1). En general, se utilizan las características de autenticación del protocolo PPP [19]. El protocolo de autenticación se negocia en la fase de establecimiento de la comunicación en el caso de conexiones virtuales PVC y SVC. El protocolo de autenticación se identifica en los octetos 6, 7, y 7a, si es aplicable. Los octetos 8-n contienen información de autenticación u opciones de configuración en un formato de paquete de autenticación específico de del protocolo identificado en los grupos de octetos 6 y 7.

El mecanismo de autenticación FRCP soporta los protocolos de autenticación definidos para PPP, tales como el protocolo de autenticación extensible (EAP, *extensible authentication protocol*), que, por su parte, soporta varios protocolos de autenticación, el protocolo de autenticación de invitación de toma de contacto (CHAP, *challenge handshake authentication protocol*) y el protocolo de autenticación de contraseña (PAP, *password authentication protocol*), todos los cuales son protocolos punto a punto (PPP). Una información detallada sobre los protocolos de autenticación PPP puede encontrarse en cada una de las normas RFC [13] a [16,] sobre autenticación de PPP.

La autenticación es una autenticación entre entidades pares. Esto entraña que cada entidad tiene que autenticar a la otra antes de que pueda cursarse tráfico bidireccional por la conexión.

9.1 Formato de la trama de autenticación

El formato de la trama de autenticación se presenta en la siguiente figura 4. Véase también el cuadro 4.

Descripción								Octeto
Información de dirección de retransmisión de tramas, control y NLPID								1-4
Encabezamiento FRCP								
Ext. 1	Reserva 0	Reserva 0	Reserva 0	I 0	D 0	A 1	C/D 1	5
ID de protocolo de autenticación (Nota 2)								6 7
Algoritmo de autenticación (Nota 2)								7a* (Nota 1)
Formato de paquete de autenticación (Nota 2)								8 n
FCS (2 octetos)								n+1 n+2

NOTA 1 – El octeto 7a sólo está presente si los octetos 6 y 7 indican CHAP (xC223).

NOTA 2 – El contenido y formato se han definido según RFCs sobre PPP.

Figura 4/X.272 – Formato general de la trama de autenticación

Cuadro 4/X.272 – Formato general de la trama de autenticación

Campo	Descripción
DLCI, control y NLPID	Véase 8.1 para detalles
Encabezamiento FRCP	• Ext.: Bit de extensión puesto a 1 • Reserva: Bit de reserva para uso futuro puesto a 0 • Campo ID puesto a 00 • Bit de autenticación (A) puesto a 1 • Bit de control/datos (C/D) – puesto a 1
ID de protocolo de autenticación (octetos 6 y 7)	Identifica el protocolo de autenticación que habrá de utilizarse, por ejemplo, PAP, CHAP, etc. Véase IETF RFC 1340 [18] para detalles
Algoritmo de autenticación (octeto 7a)	Si está presente, identifica el método de autenticación CHAP que habrá de utilizarse. Véase IETF RFC 1994 [19] para detalles. Sólo está presente si los octetos 6 y 7 indican CHAP
Formato del paquete de autenticación (octetos 8-n)	En general, utiliza el formato de paquete del método de autenticación PPP específico
FCS	Secuencia de verificación de trama Q.922

9.2 Formato del paquete de autenticación

Los paquetes de tipo PPP se encapsularán en los octetos 8-n de la trama antes presentada. Estos paquetes tienen el formato general: código, identificador, longitud, valores. Por ejemplo, en el caso de CHAP se utiliza el formato de paquete de IETF RFC 1994 [19] sección 4, como se representa en la figura 5 y se describe en el cuadro 5.

Descripción	Octeto
Código	8
Identificador	9
Longitud (2 octetos)	10 11
Valores/datos, definidos por el protocolo de autenticación	12 n

Figura 5/X.272 – Formato del paquete de autenticación

Cuadro 5/X.272 – Estructura de las primitivas de control FRCP

Campo	Descripción
Código	Tomado del método de autenticación PPP indicado en los octetos 6-7a. Indica el tipo de paquete o mensaje, por ejemplo petición, respuesta, etc.
Identificador	Un número de transacción para correlacionar una petición con una respuesta. Se envía en la petición y se refleja en eco en la respuesta
Longitud (2 octetos)	Incluye: código, identificador, longitud, y todas las opciones de configuración
Opciones de configuración	Valores/datos según el protocolo de autenticación PPP utilizado. Para detalles, véanse los métodos de autenticación PPP específicos, por ejemplo CHAP, EAP, PAP, etc.

9.3 Procedimientos de autenticación

Se siguen los procedimientos descritos en el documento RFC aplicable al protocolo de autenticación PPP utilizado. Por ejemplo, si el protocolo de autenticación PPP configurado es CHAP (0xCC23), se siguen los procedimientos descritos en IETF RFC 1994 [19].

10 Facilidad de criptación

La facilidad de criptación se encarga de habilitar e inicializar algoritmos de criptación de datos en ambos extremos del enlace. Para la criptación se utiliza un mecanismo de intercambio de paquetes similar al protocolo de control del enlace (LCP, *link control protocol*) PPP [16].

La utilización de la facilidad de criptación se negocia entre dispositivos pares. El modo y los algoritmos se seleccionan independientemente para cada sentido de transmisión de una conexión virtual. Esto se recapitula en el cuadro 6.

Cuadro 6/X.272 – Cuadro de transiciones del E_Mode-1

Solicitado	Configurado	
	E_Mode-1	**E_Mode-2**
E_Mode-1	Responder con E_Mode-1 y usar E_Mode-1.	Responder con E_Mode-1 y usar E_Mode-1.
E_Mode-2	Responder con E_Mode-1 y usar E_Mode-1.	Responder con E_Mode-2 y usar E_Mode-2.

Se supone que cada dispositivo par tiene una clave inicial para uso en la criptación. El método para poner la clave en conocimiento de ambos dispositivos comunicantes está fuera del ámbito de la presente Recomendación. La negociación de la criptación tiene que finalizar con éxito para poder pasar a la fase de transferencia de datos. Una vez efectuada a negociación hay que criptar todas las tramas de datos intercambiadas por una conexión virtual.

10.1 Especificación del E_Mode-1

La criptación E_Mode-1 tiene que estar soportada si la facilidad de criptación está implementada en el DTE. El E_Mode-1 utiliza la norma de criptación de datos (DES) con una clave de 56 bits, con concatenación de bloques cifrado (CBC) [21]. El texto en lenguaje cifrado se transfiere utilizando el formato de paquete definido en la sección 10.1.4 Formato de trama para la transferencia de datos en el E_Mode-1.

10.1.1 Formatos de las tramas de control del E_Mode-1

Estas tramas se utilizan para negociar parámetros del E_Mode-1. Véanse la figura 6 y el cuadro 7.

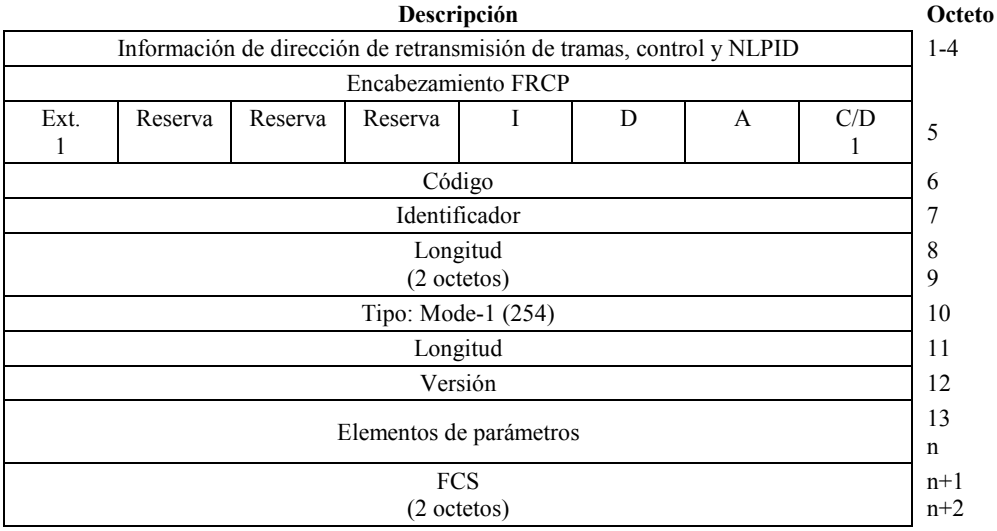

Figura 6/X.272 – Trama de control E_Mode-1

Cuadro 7/X.272 – Trama de control E_Mode-1

Campo	Descripción
DLCI, control y NLPID	Véase 8.1 para detalles
Encabezamiento FRCP	• Ext.: Bit de extensión = 1 • Reserva: Bits de reserva para uso futuro, puestos a 0 • Campo ID (2 bits) puesto a 11 • Bit de autenticación (A) = 0 • Bit de control/datos (C/D) puesto a 1
Código	Decimal para 1 Config-Req; Decimal para 2 Config-Ack
Identificador	Un número de transacción para correlacionar una petición con una respuesta. Se envía en la petición y se refleja en eco en la respuesta correspondiente
Longitud (2 octetos)	Incluye: código, identificador, longitud y todas las opciones de configuración

Cuadro 7/X.272 – Trama de control E_Mode-1 (*fin*)

Campo	Descripción
Tipo	254 (decimal) – indica E_Mode-1 Los tipos 245 a 253 inclusive y el tipo 255 están reservados.
Longitud	Varía según el número de parámetros
Versión	Número de versión del FRCP de criptación puesto a 1
Elementos de parámetros	Cero o más elementos de parámetros E_Mode-1. Véase 10.1
FCS	Secuencia de verificación de trama Q.922

10.1.1.1 Elementos de parámetros del E_Mode-1

El identificador de elemento de parámetro identifica un elemento de parámetro. La longitud es la longitud del elemento de parámetro completo, incluido el campo ID de elemento de parámetro y el campo longitud. El campo valores da los distintos valores de parámetros. Los elementos de parámetros constan de un número entero de octetos. Comienzan después del octeto 12 de la opción de configuración E_Mode-1. Véase la figura 7.

Descripción	Octeto
ID de elemento de parámetro	a
Longitud	b
Valores de elementos de parámetros	c m

Figura 7/X.272 – Estructura general del elemento de parámetro E_Mode-1

10.1.1.1.1 Vector inicial del E_Mode-1

Los algoritmos para la concatenación de bloques cifrado (CBC) de la norma de criptación de datos (DES) requieren un vector de inicialización (IV, *initialization vector*) que tiene el mismo tamaño del bloque. La inclusión del parámetro vector inicial en la petición de configuración (Config-Req) es obligatoria. La presencia del parámetro vector inicial en Config-Req indica la palabra-de-ocasión (*nonce*) inicial, de 64 bits, que el dispositivo emisor utilizará para la concatenación de bloques cifrado (CBC). El Config-Ack acusa recibo del vector inicial. El parámetro vector inicial no se envía en el Config-Ack. Véanse la figura 8 y el cuadro 8.

ID de vector inicial								1
0	0	0	0	0	0	0	1	
Longitud: 10								2
Palabra-de-ocasión inicial (8 octetos)								3 10

Figura 8/X.272 – Elemento de parámetro vector inicial (palabra-de-ocasión inicial)

Cuadro 8/X.272 – Elemento de parámetro vector inicial (palabra-de-ocasión inicial)

Campo	Descripción
ID de vector inicial	Octeto que identifica el parámetro vector inicial
Longitud	10 (decimal)
Palabra-de-ocasión inicial	Cantidad de 64 bits utilizada por el dispositivo par para criptar el primer paquete transmitido. Para dar protección contra reproducciones fraudulentas, el dispositivo debe ofrecer un valor diferente durante cada negociación.

10.1.1.1.2 Intercambio y actualización de claves del E_Mode-1

E-Mode-1 soporta clave de criptación estática. Los procedimientos de intercambio y actualización de claves están fuera del ámbito de esta Recomendación.

10.1.2 Formato de trama para la transferencia de datos en el E_Mode-1

El algoritmo de la norma de criptación de datos (DES) trabaja con bloques de ocho octetos. Esto requiere a menudo la inserción de relleno al final de los datos de usuario no criptados. Al final de los datos de usuario hay que añadir un octeto (longitud del relleno) que indica la longitud del relleno insertado. En consecuencia, antes del proceso de criptación se calcula la longitud de los datos de usuario más el octeto longitud del relleno. Si esta longitud no es un múltiplo entero de 8 octetos, se añade como relleno un número tal de octetos que asegure que la longitud total sea un múltiplo de 8 octetos. Se aconseja que los octetos insertados como relleno tenga un contenido aleatorio de datos. El número de octetos insertados como relleno puede variar de 0 a 255, lo que permite ocultar la longitud real de los datos. El número de octetos añadidos se indica en el octeto longitud del relleno. Este octeto es el último de la trama. A continuación se cripta la totalidad de la trama, incluidos los datos de usuario, los octetos insertados como relleno y el octeto longitud del relleno. Tras el proceso de descriptación, los octetos insertados como relleno y el octeto longitud del relleno son separados de los datos de usuario y suprimidos, y no podrán tenerse en cuenta.

En la figura 9 se presenta el formato de la trama FRCP para la transmisión de datos en lenguaje cifrado, solamente. Véase también el cuadro 9.

Descripción								Octeto
Información de dirección de retransmisión de tramas, control y NLPID								1-4
Encabezamiento FRCP								
Ext. 1	C/U	RA	RR	0	P	T	C/D 0	5
Número secuencial								7
Datos de usuario (nota)								8 m
Relleno (nota)								m n-1
Longitud del relleno (nota)								n
LCB								n+1
FCS (2 octetos)								n+2 n+3

NOTA – Este campo está criptado.

Figura 9/X.272 – Formato de trama para la transferencia de datos E_Mode-1

Cuadro 9/X.272 – Formato de trama para la transferencia de datos E_Mode-1

Campo	Descripción
DLCI, control y NLPID	Véase 8.1 para detalles.
Encabezamiento FRCP	El encabezamiento del protocolo FRCP consta de lo siguiente: • Bit de extensión – Puesto a 1, pero incluido para futuras mejoras • Comprimido/no comprimido (C/U): Puesto a 1 para indicar que los datos no están comprimidos. • Reset_Ack (RA): No aplicable, puesto a 0. • Reset_Request (RR): No aplicable, puesto a 0. • Opción de protocolo (OPT): Puesto a O P T 0 0 1 para especificar criptación. • Bit de control/datos (C/D): Puesto a 0 para indicar una trama de datos
Número secuencial	Número asignado secuencialmente por el criptador, que comienza por 0 y se incrementa modulo 256.
Datos de usuario	Datos de usuario criptados
Relleno	Octetos, preferiblemente de contenido aleatorio, insertados con el fin de asegurar que la longitud total de los datos de usuario y del octeto longitud del relleno sea un múltiplo de 8 octetos.
Longitud del relleno	Número de octetos de relleno que se añaden a la longitud de datos de usuario más 1 para asegurar que la longitud total de los datos es un múltiplo de 8 octetos. Este octeto es el último octeto de la trama.
LCB	Octeto de verificación longitudinal – se calcula sobre texto ordinario de los octetos 7 a n.
FCS	Secuencia de verificación de trama Q.922

10.1.3 Procedimientos de control del E_Mode-1

El E_Mode-1 del FRCP proporciona un protocolo de negociación simple para habilitar la función de privacidad con el algoritmo y los valores de parámetros por defecto. Una vez habilitado y correctamente negociado el FRCP, es necesario criptar la transferencia de datos al sistema de extremo par. Para inhabilitar el FRCP, una implementación puede forzar la conexión virtual al estado inactivo, o enviar un petición E_Mode-1 y no enviar una respuesta E_Mode-1.

La negociación de la facilidad de criptación comienza cuando se establece la conexión virtual (VC). Se utiliza el término V_0 para designar una conexión virtual inactiva, y el término V_1 para designar una conexión virtual activa. Se pasa a la fase de inicialización una vez establecida la conexión virtual de retransmisión de tramas, siempre que el usuario haya configurado FRCP en el DTE. Se pasa a la fase de operación una vez que se haya finalizado con éxito la fase de inicialización. En la fase de operación se utiliza el término f_1 para designar la negociación con éxito de una facilidad, y el término f_0 para designar la negociación fallida de una facilidad. Las PDU de datos del FRCP sólo se transfieren cuando el E_Mode-1 está en la fase f_1. Las PDU de control del FRCP pueden transferirse en cualquier fase.

10.1.3.1 Estados del E_Mode-1

The FRCP E_Mode-1 en cualquiera de los dos lados de una conexión de retransmisión de tramas puede encontrarse en uno de los estados siguientes:

Inhabilitado (f_0):

La facilidad FRCP no existe (cuando una VC pasa de V_0 a V_1 y/o la negociación fracasa).

Petición iniciada (I_1):

Se ha enviado un mensaje de petición de configuración E_Mode-1 al dispositivo par. Se espera la respuesta a la petición propia y la petición de configuración del dispositivo par.

Petición recibida (I_3):

Se ha recibido un mensaje de petición de configuración E_Mode-1 del dispositivo par. Se envían al dispositivo par una respuesta de configuración a su mensaje de petición, y una petición de configuración (Config-Req). Se espera la respuesta a la petición propia.

Espera de petición (I_2):

Se ha recibido la respuesta de configuración a la petición propia y se espera la petición de configuración del dispositivo par.

Operacional (f_1):

La negociación de E_Mode-1 ha finalizado con éxito.

Para asegurarse de que el proceso de negociación ha finalizado, con éxito o sin éxito, se define un temporizador de compleción de toma de contacto y un contador de número tentativas hasta un máximo. El temporizador de compleción de toma de contacto incluye el tiempo necesario para efectuar el proceso de toma de contacto para la negociación. El contador de número de tentativas hasta un máximo indica el número de veces que un dispositivo intenta el proceso de negociación. A continuación se indican los valores por defecto preferidos para la negociación E_Mode-1 de cualquiera de las facilidades tratadas en esta Recomendación.

Parámetro	**Valor por defecto**
Temporizador de compleción de toma de contacto	3 segundos
Contador de número de tentativas hasta un máximo	10 (en decimal)

El diagrama de estados para el proceso de negociación de E_Mode-1 se muestra en la figura 10.

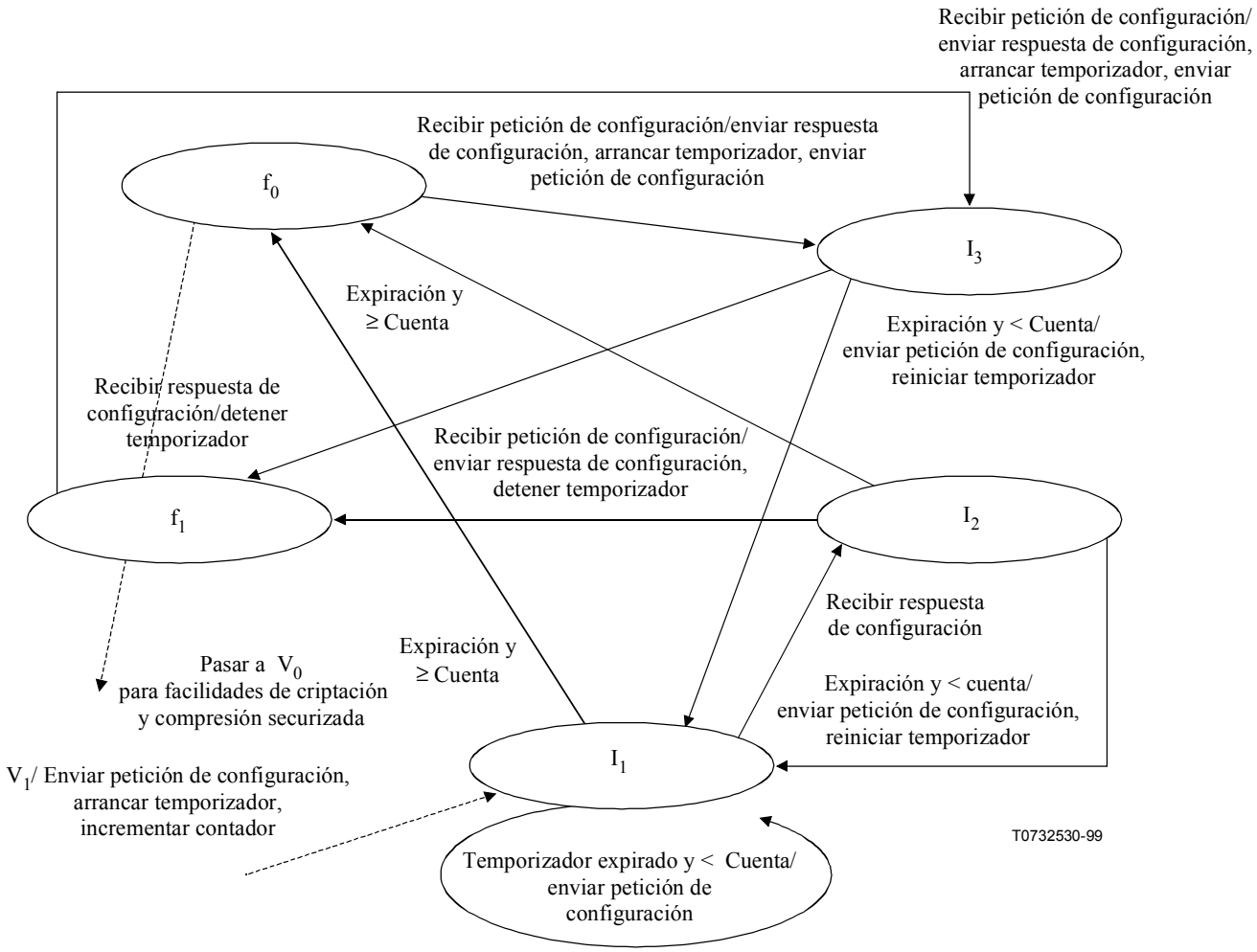

Figura 10/X.272 – Diagrama de estados de E_Mode-1

10.1.3.2 Petición de inicialización

La inicialización de E_Mode-1 cuando se establece una conexión virtual de retransmisión de tramas con una entidad par y el usuario habilita administrativamente una función de privacidad por retransmisión de tramas. Los procedimientos de negociación FRCP se inician enviando un mensaje Config-Req a la entidad par; se arranca un temporizador de compleción de toma de contacto y se pasa al estado *petición iniciada (I_1)*.

Al recibir un mensaje de respuesta de configuración, la entidad pasará al estado *espera de petición (I_2)*. Cuando se recibe una Config-Req de la entidad par se aplica el siguiente procedimiento:

1) En el caso de llamadas en el estado *petición iniciada (I_1)*, se envía un mensaje de respuesta de configuración, se pasa al estado *petición recibida (I_3)*.

2) En el caso de llamadas en el estado *espera de petición (I_2)*, se envía un mensaje de respuesta de configuración; se detiene el temporizador de compleción de toma de contacto; se envía una primitiva de respuesta de configuración que señala que la negociación está completa; se pasa al estado operacional f_1.

Si el temporizador de compleción de toma de contacto expira antes de que haya concluido el procedimiento de toma de contacto y el número de tentativas es menor que el valor del contador de número de tentativas hasta un máximo, se aplica el siguiente procedimiento:

1) En el caso de llamadas en el estado *petición iniciada (I_1)*, se envía un mensaje Config-Req a la entidad par; se rearranca un temporizador de compleción de toma de contacto, y se incrementa el número de mensajes Config-Req que se han enviado a la entidad par.

2) En el caso de llamadas en el estado *espera de petición (I_2)*, se envía un mensaje Config-Req a la entidad par; se rearranca un temporizador de compleción de toma de contacto; y se pasa al estado *petición iniciada (I_1)*.

10.1.3.3 Recepción de una petición de configuración

Al recibir una petición de configuración de la entidad par en el estado f_0, se envía un mensaje de respuesta de configuración; se arranca un temporizador de compleción de toma de contacto; se incrementa el número de mensajes que se han enviado a la entidad par, y se pasa estado *petición recibida (I_3)*.

Al recibir un mensaje de respuesta de configuración en el estado *petición recibida (I_3)*, se detiene el temporizador de compleción de toma de contacto; se pasa al estado operacional f_1.

Si el temporizador de compleción de toma de contacto expira antes de que haya finalizado el procedimiento de toma de contacto y el número de tentativas repetidas es menor que la cuenta, se envía un mensaje Config-Req; se rearranca el temporizador de compleción de toma de contacto.

10.1.3.4 Fase operacional

Cuando se recibe un mensaje Config-Req de la entidad par, en el caso de llamadas en el estado *operacional* f_1, se envía un mensaje de respuesta de configuración; se envía un mensaje Config-Req; se rearranca el temporizador de compleción de toma de contacto, y se pasa al estado *petición recibida (I_3)*.

10.1.3.5 Fase de inhabilitación

Se entrará en la fase de inhabilitación de E_Mode-1, fase f_0, cuando se libera una conexión virtual de retransmisión de tramas con una entidad par (transición de V_1 a V_0) o cuando la negociación ha fracasado. Si al expirar un periodo del temporizador de compleción de toma de contacto se ha rebasado el valor del contador de número de tentativas hasta un máximo, se retorna a la fase f_0 . Si la negociación fracasa y no se alcanza la fase f_1, hay que liberar la conexión virtual.

10.1.4 Criptación de datos de usuario del E_Mode-1

Una vez finalizada la negociación entre las entidades pares que intervienen en la criptación, y que ambas se encuentren en el estado operacional, las tramas se criptan mediante los procedimientos descritos en esta cláusula.

El método de criptación E_Mode-1 utilizado para crear el texto en lenguaje cifrado es la norma de criptación de datos (DES) en el modo concatenación de bloques cifrado (CBC), y clave de 56 bits. El vector inicial para el modo CBC se deduce de la palabra-de-ocasión explícita de 64 bits, intercambiada en el curso de la negociación E_Mode-1. Si las entidades pares no intercambian una palabra-de-ocasión, dicha palabra tiene que ser coordinada y configurada en las respectivas entidades pares de la conexión virtual. El CBC de criptación se extiende más allá de cada cabida útil y pasa a la siguiente. Se utiliza un número secuencial para detectar cuándo una trama recibida está fuera de secuencia.

Cuando se deben enviar datos, los datos se rellenan hasta alcanzar la siguiente longitud múltiplo de 8 octetos, como se describe en 10.1.2, para formar una cabida útil en lenguaje cifrado. El octeto de verificación longitudinal (LCB) se calcula para cada cabida útil en lenguaje cifrado. El criptador cifra la cabida útil del lenguaje cifrado y el resultado se coloca en la trama como se muestra en la figura 9. El emisor incrementa módulo 256 el número secuencial. El emisor añade el LCB al final de la cabida útil y envía la trama por el enlace.

El receptor comienza por examinar el número secuencial para determinar si la trama está en secuencia o se ha perdido una trama. Si se ha perdido una trama, los últimos 8 octetos del texto en lenguaje cifrado se mantienen como el vector inicial para la trama siguiente, y se descarta la trama recibida. Si la trama está en secuencia, el receptor descifra los campos identificados en la figura 9 y calcula el LCB. El LCB calculado se compara con el LCB recibido. Si no concuerdan, los últimos 8 octetos de los datos se mantienen como el vector inicial para la trama siguiente, y se descarta la trama recibida. Si los LCB concuerdan, se procesan los datos descifrados, para lo cual se les suprime el relleno.

10.2 Especificación del E_Mode-2

El soporte de la criptación E_Mode-2 comprende en la totalidad de los procedimientos de negociación de IETF RFC 1968. Estos procedimientos permiten que dos dispositivos pares de retransmisión de tramas negocien y converjan en métodos y parámetros de criptación para uso en una conexión virtual entre los mismos. Por lo general, se utilizan los formatos y procedimientos de control de IETF RFC 1968 [14],según los cuales pueden negociarse métodos de criptación diferentes para cada sentido de transmisión de la conexión virtual.

10.2.1 Formatos de las tramas de control del E_Mode-2

Estas tramas se utilizan para negociar parámetros del E_Mode-2. Véanse la figura 11 y el cuadro 10.

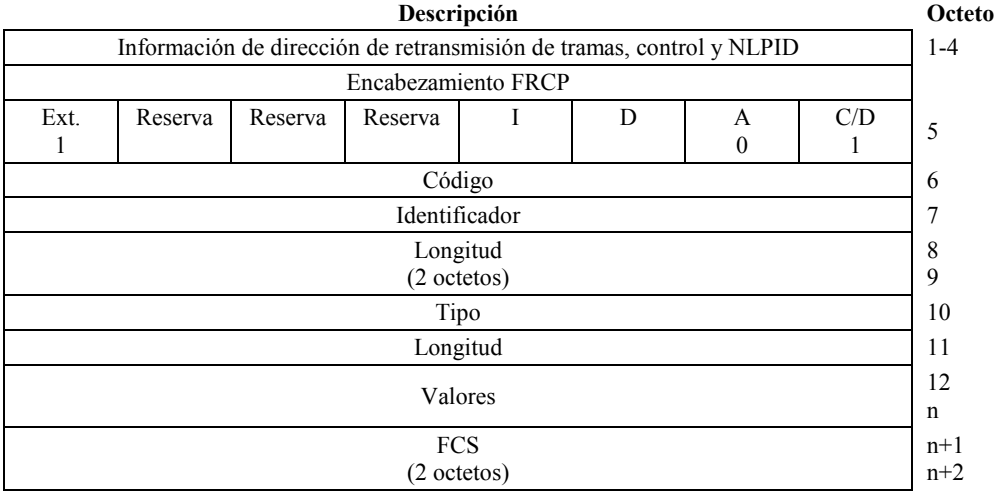

Figura 11/X.272 – Trama de control FRCP de E_Mode-2

Cuadro 10/X.272 – Trama de control de E_Mode-2

Campo	Descripción
DLCI, control y NLPID	Véase 8.1 para detalles
Encabezamiento FRCP	• Ext.: Bit de extensión puesto a 1 • Reserva: Bits de reserva puestos 0 • ID (2 bits) puesto a 11 • Bit de autenticación (A) = 0 • Bit de control/datos (C/D) puesto a 1
Código	Véanse IETF RFC 1661 sección 5 LCP Packet Formats e IETF RFC 1968 sección 3 Additional Packets. (Valores dados en decimal)

Cuadro 10/X.272 – Trama de control de E_Mode-2 (*fin*)

Campo	Descripción
Identificador	Véanse IETF RFC 1661 sección 5 LCP Packet Formats e IETF RFC 1968 sección 3 Additional Packets.
Longitud (2 octetos)	Véanse IETF RFC 1661 sección 5 LCP Packet Formats e RFC 1968 sección 3 Additional Packets. Incluidos: código, identificador, longitud y datos de todas las opciones de configuración
Tipo	Véanse RFC 1968 sección 4 ECP Configuration Options, 4.1 Proprietary Encryption OUI y 4.2 Publicly Available Encryption Types. En esta Recomendación el tipo 254 (decimal) está reservado e indica FRCP E_Mode-1. Además los tipos 245 a 253 inclusive y el tipo 255 están reservados.
Longitud	Longitud de opción de configuración, incluidos los campos tipo, longitud y valores.
Valores	Cero o más octetos, que contienen datos determinados por las opciones de configuración definidas en IETF RFC 1968 sección 4.
FCS	Secuencia de verificación de trama Q.922

10.2.2 Negociación del E_Mode-2

El E_Mode-2 del protocolo de privacidad de los datos por la retransmisión de tramas encapsula el mismo mecanismo de intercambio de paquetes que el protocolo de control de criptación (IETF RFC 1968) [14] (de tipo PPP), que a su vez ha sido diseñado tomando como modelo el protocolo de control del enlace (IETF RFC 1661) [13] (también de tipo PPP). E_Mode-2 utilizará los procedimientos descritos en las secciones 3.1 y 4.3 de IETF RFC 1968, con los mismos formatos de trama descritos en 8.2. Las siguientes excepciones son aplicables a las secciones 3.1 y 4.3 de IETF RFC 1968 [14], y a la sección 4 of IETF RFC 1661 (a la que se hace referencia):

- En cualquier momento en que el dispositivo receptor reciba la Config-Req E_Mode-1 comenzará la negociación E_Mode-1.
- Una entidad puede, en cualquier momento, salir de E_Mode-2 y entrar en la fase de inicialización de E_Mode-1.
- Si, en un momento dado cualquiera, una entidad que soporta E_Mode-2 se encuentra en E_Mode-1 y recibe una petición de configuración E_Mode-2, puede comenzar la negociación de E_Mode-2.

NOTA – Los eventos ascendentes/descendentes (de capa inferior) para la automatización deben ser generados según la situación de la conexión virtual, dada por los protocolos de señalización de la PVC y la SVC. No deberán tenerse en cuenta los paquetes E_Mode-2 recibidos antes de esta fase. Antes de intercambiar datos encriptados, la entidad tiene que haber pasado al estado f_1 .

10.2.3 Transferencia de datos en el E_Mode-2

Este formato se utiliza para transferir datos cifrados en E_Mode-2. Es similar a E_Mode-1 representado en la figura 9 y descrito en el cuadro 9.

11 Facilidad de compresión de datos

La facilidad de compresión de datos se encarga de habilitar e iniciar algoritmos de compresión de datos en ambos extremos del enlace. Para la compresión de datos se utiliza un mecanismo de intercambio de paquetes similar al del protocolo de control del enlace (LCP, *link control protocol*) [13] (de tipo PPP). La utilización de la facilidad de compresión de datos se negocia entre dispositivos pares. El modo y los algoritmos se seleccionan independientemente para cada sentido de transmisión de una conexión virtual. El protocolo de control FRCP proporciona los siguientes servicios para compresión de datos:

– Encapsulación de datos de usuario codificados y primitivas de negociación dentro de unidades de datos de protocolo FRCP para el transporte entre entidades pares FRCP.
– Negociación de opciones de configuración FRCP.
– Sincronización de las entidades pares emisora y receptora, incluyendo:
  • Detección de la pérdida de la sincronización y señalización para la resincronización entre entidades pares.
  • Protección antiexpansión, que permite la señalización del modo comprimido/no comprimido del codificador al decodificador par.
  • Codificación de datos de usuario en datos de usuario, para convertirlos en datos de usuario comprimidos, de acuerdo con uno o más algoritmos diferentes, públicos o privados.
  • Decodificación de datos de usuario comprimidos, para convertirlos en datos de usuario no comprimidos.

Esta Recomendación soporta la negociación de algoritmos de compresión de datos, públicos o privados, facultativos. Los detalles de los algoritmos de propiedad privada deben ser publicados por los vendedores en documentos de la descripción de función de compresión de datos (DCFD, *data compression function description*). La DCFD en combinación con la presente Recomendación es suficiente para asegurar la interoperabilidad de los FRCP suministrados por distintos fabricantes.

11.1 Encapsulación de la compresión de datos en el C_Mode-1

Para las implementaciones que incluyen la facilidad de compresión de datos, el soporte de C_Mode-1 es obligatorio. El C_Mode-1 consiste en una simple toma de contacto para habilitar el algoritmo de compresión de datos por defecto , y sus parámetros, en ambos sentidos de transmisión de la conexión virtual. El algoritmo de compresión de datos por defecto es el descrito en [20].

11.1.1 Formatos de tramas de control del C_Mode-1

Estas tramas se utilizan para negociar parámetros C_Mode-1. Véanse la figura 12 y el cuadro 11.

Descripción								Octeto
Dirección Q.922 (2 octetos) (nota)								1 2
Control (UI: 0x03)								3
NLPID (0xB0)								4
Encabezamiento FRCP								
Ext. 1	Reserva	Reserva	Reserva	I	D	A	C/D 1	5
Código								6
Identificador								7
Longitud (2 octetos)								8 9
Tipo								10
Longitud de opción de configuración								11
Revisión								12
FCS (2 octetos)								13 14

NOTA – La dirección de retransmisión de tramas se presenta en formato de 2 octetos a título ilustrativo. Los formatos de dirección de 3 y 4 octetos no están prohibidos.

Figura 12/X.272 – Trama de control C_Mode-1

Cuadro 11/X.272 – Trama de control C_Mode-1

Campo	Descripción
Dirección Q.922	Véase 8.1 para detalles.
Control	Véase 8.1 para detalles.
NLPID	Véase 8.1 para detalles.
Encabezamiento FRCP	El encabezamiento de protocolo FRCP consiste en lo siguiente: • Ext.: Bit de ampliación, puesto necesariamente a 1. • Reserva: Bits de reserva para uso futuro puestos a 0. • ID (2 bits) puesto a 01. • Bit de autenticación (A) – Puesto a 0. • Bit de control/datos (C/D) – Puesto a 1.
Código	Puesto a 1 para petición de configuración (Config-Req) Puesto a 2 para acuse de recibo de configuración (Config-Ack)
Identificador	Un número de transacción para correlacionar una petición con una respuesta. Se envía en la petición y se refleja en eco en la respuesta correspondiente.
Longitud	Dos octetos de longitud. El valor se fija a 7, que es en el número total de octetos de la trama, sin contar: dirección Q.922, control, NLPID, y encabezamiento FRCP.
Tipo	254 (en decimal) – indica C_Mode-1 Los tipos 254 a 253 inclusive y el tipo 255 están reservados.
Longitud de opción de configuración	Puesto a 3 (decimal) para indicar la longitud de los campos tipo, longitud de opción de configuración, y revisión.
Revisión	El actual campo revisión tiene que fijarse a 1.
Cabida útil FRCP	Información de control o datos para transferencia, según el valor que se haya dado a los bits del encabezamiento FRCP.
FCS	Secuencia de verificación de trama Q.922

11.1.2 Procedimientos de control del C_Mode-1

El C_Mode-1 de compresión de datos del FRCP proporciona un protocolo de negociación simple para habilitar el servicio de compresión de datos con el algoritmo y los valores de parámetros por defecto. Una vez efectuada correctamente la negociación de FRCP, la transferencia de datos al sistema de extremo par puede ser comprimida. Para inhabilitar el FRCP, una implementación puede forzar la conexión virtual al estado inactivo, o enviar una petición C_Mode-1 y no enviar una respuesta C_Mode-1.

11.1.2.1 Estados del C_Mode-1

Igual que 10.1.3.1.

11.1.2.2 Petición de inicialización del C_Mode-1

Igual que 10.1.3.2.

11.1.2.3 Recepción de una petición de configuración

Igual que 10.1.3.3.

11.1.2.4 Fase operacional

Igual que 10.1.3.4.

11.1.2.5 Fase de inhabilitación

Igual que 10.1.3.5.

11.1.3 Formatos de transferencia de datos del C_Mode-1

En esta cláusula se describe el método de encapsulación para compresión de datos FRCP cuando sólo está habilitada la opción de compresión de datos. Se describe también los procedimientos antiexpansión y los procedimientos de sincronización.

El formato general de trama se describe en la figura 13. En esta figura, el bit C/D del encabezamiento FRCP se ha puesto a 0 para indicar que se trata de una trama de datos. Se utilizan los bits C/U, RA RR para los procedimientos antiexpansión y los procedimientos de sincronización.

11.1.3.1 Formato de la señalización antiexpansión

La señalización antiexpansión (bit C/U) puede proporcionarse del codificador al decodificador en un sentido de transmisión de la conexión de compresión de datos FRCP para indicar si la cabida útil FRCP asociada está o no comprimida. El emisor fijará C/U = 1 cuando se haya efectuado codificación de compresión sobre los datos de usuario. El emisor fijará C/U = 0 cuando no se haya efectuado codificación de compresión sobre los datos de usuario. Cuando C/U = 1, el decodificador decodificará la cabida útil FRCP. Cuando C/U = 0, el decodificador no decodificará la cabida útil FRCP. Cuando el bit C/D está puesto a "0" no habrá campo número secuencial, ni campo LCB.

La actual implementación de la revisión del C-Mode-1 requiere que el codificador comprima todas las tramas de datos, incluso si se ha producido expansión de datos. El algoritmo LZS proporciona una mínima expansión de los datos; para una información detallada sobre la expansión LZS, véase [20]. Para la implementación de C-Mode-1 es necesario que la conexión se establezca de manera que trate un tamaño máximo de trama que incluya el escenario de caso más desfavorable de la expansión de los datos.

11.1.3.2 Formato de la señalización de sincronización

El FRCP proporciona procedimientos de sincronización para la recuperación tras una pérdida de la sincronización entre entidades pares FRCP. La retransmisión de tramas no garantiza un transporte fiable de las PDU del FRCP. Los decodificadores de la función FRCP generalmente no recuperan en el caso de las PDU en las que se ha abandonado la decompresión, que son erróneas, o que están incorrectamente ordenadas, y propagan los errores catastróficamente hasta que son reiniciados a un estado conocido. En la presente Recomendación se utiliza el número secuencial y el LCB para detectar la pérdida de sincronización. Se proporciona señalización de sincronización entre entidades pares FRCP por medio de los bits RR y RA del encabezamiento de las PDU de datos del FRCP. Los bits RR y RA pueden ser señalizados en un encabezamiento FRCP que acompañe a la cabida útil FRCP; pueden también señalizarse mediante un encabezamiento FRCP que no tenga ligada ninguna cabida útil (véase la figura 14). Se proporcionan señales RR y RA distintas para permitir la resincronización independiente de uno o ambos sentidos de transmisión de la conexión FRCP.

El decodificador detecta la pérdida de sincronización cuando recibe una trama con un número secuencial erróneo o un LCB erróneo. Si el decodificador detecta una pérdida de sincronización en el sentido distante a local de la conexión FRCP, generará una señal RR poniendo a "1" el bit RR en una nueva PDU de datos FRCP vacía, o en la siguiente PDU de datos FRCP que contenga datos de usuario destinados a la entidad par FRCP distante. Una vez generado un bit RR puesto a "1", toda PDU de datos FRCP recibida en el sentido distante a local de ese contexto FRCP que contenga datos de usuario comprimidos (C/U = 1) será descartada hasta que se reciba para ese contexto un bit RR puesto a "1". La señal con el bit RR puesto a "1" puede repetirse para aumentar la fiabilidad. Si el receptor detecta un bit RR puesto a "1" en el sentido distante a local, reinicia su codificador a un estado conocido. El codificador generará una señal con el bit RA puesto a "1" en una nueva PDU de datos FRCP vacía o en la siguiente PDU de datos FRCP que contenga datos de usuario destinados a

la entidad par FRCP local. Cuando un receptor FRCP local recibe una señal con el bit RA puesto a "1" en el sentido distante a local del contexto FRCP, reiniciará su historia para ese contexto a un estado conocido. El receptor FRCP local decodificará todo dato de usuario en la PDU de datos de FRCP que contenga el bit RA puesto a "1" y todas las PDU de datos FRCP subsiguientes hasta que detecte otra pérdida de sincronización.

El bit C/U se pondrá a "0" en las tramas de sincronización (cuando los bits RR y RA estén puestos a 1). Además, toda trama de sincronización FRCP contendrá un número secuencial válido. Al detectar un bit RA puesto a "1", el decodificador reiniciará su número secuencial actual al recibido de la trama de sincronización. En consecuencia, el siguiente número secuencial esperado puede calcularse módulo 256 a partir del número secuencial recibido.

Para asegurar la sincronización inicial entre dos entidades pares después de que éstas hayan negociado con éxito el C_Mode-1, el codificador fijará el bit RA a "1" en la primera PDU para indicar que la historia está en un estado conocido. El decodificador ignorará todas las tramas comprimidas hasta que obtenga tal trama. Para aumentar la fiabilidad, el decodificador enviará una petición de reiniciación al codificador distante.

11.1.3.3 Cabida útil de la compresión de datos del C_Mode-1

El contenido de la cabida útil FRCP será un número entero de octetos. El formato de la cabida útil FRCP se presenta a continuación. Véanse la figura 13 y el cuadro 12.

Dirección Q.922, control y NLPID								1-4
Encabezamiento FRCP								
Ext. 1	C/U	RA	RR	O	P	T	C/D 0	5
Número secuencial								6
Cabida útil de compresión de datos FRCP								7 n
LCB								n+1
FCS (2 octetos)								n+2 n+3

Figura 13/X.272 – Trama de transferencia de datos E_Mode-1

Cuadro 12/X.272 – Trama de transferencia de datos E_Mode-1

Campo	Descripción
Dirección Q.922	Véase 8.1 para detalles
Control	Véase 8.1 para detalles
NLPID	Véase 8.1 para detalles
Número secuencial	Se inicializa a 1 y se incrementa módulo 256 después de cada trama. NOTA 1 – Este octeto se añade al final de la cabida útil comprimida. Este octeto no será comprimido.
Encabezamiento FRCP	El encabezamiento de protocolo FRCP Protocol consta de lo siguiente: • Ext.: Bit de extensión puesto necesariamente a 1; se incluye con miras a futuras mejoras • Bit comprimido/no comprimido (C/U): Puesto a 1 para indicar que los datos no están comprimidos • Reset_Ack (RA): No aplicable, puesto a 0 • Reset_Request (RR): No aplicable, puesto a 0 • Opción de protocolo (OPT): Puesto a: O P T 0 1 1 para especificar compresión • Bit control/datos (C/D): Puesto a 0 para indicar una trama de datos
Cabida útil de compresión de datos	Trama conforme a Rec. Q.933 Anexo E que fue comprimida
Número secuencial	Se inicializa a 1 y se incrementa módulo 256 después de cada trama. NOTA 2 – Este octeto se añade al final de la cabida útil comprimida. Este octeto no será comprimido.
LCB	Se calcula sobre los datos de usuario originales incluyendo el número secuencial. El LCB no se comprime.
FCS	Secuencia de verificación de trama Q.922

En la figura 14 se describe la estructuración de una PDU vacía.

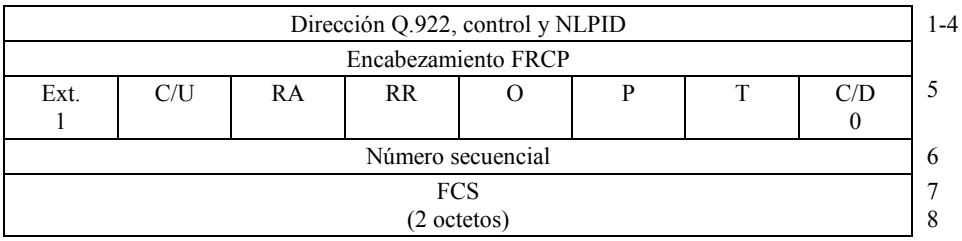

Figura 14/X.272 – PDU de FRCP vacía

11.2 Encapsulación de la compresión de datos del C_Mode-2

El soporte de C_Mode-2 es facultativo. Este modo de funcionamiento de la compresión de datos proporciona la capacidad de negociar DCFDs y sus parámetros correspondientes.

11.2.1 Formatos de tramas de control del C_Mode-2

Estas tramas se utilizan para negociar parámetros C_Mode-2. Véanse la figura 15 y el cuadro 13.

Descripción								Octeto
Dirección Q.922 (2 octetos) (nota)								1 2
Control (UI: 0x03)								3
NLPID (0xB0)								4
Encabezamiento FRCP								
Ext 1	Reserva	Reserva	Reserva	I	D	A	C/D 1	5
Código								6
Identificador								7
Longitud (2 octetos)								8 9
Tipo								10
Longitud de opción de configuración								11
OUI (3 octetos)								12 13 14
Subtipo								15
Valores								16
FCS (2 octetos)								17 18

NOTA – La dirección de retransmisión de tramas se presenta en formato de 2 octetos a título ilustrativo. Los formatos de dirección de 3 y 4 octetos no están prohibidos.

Figura 15/X.272 – Trama de control C_Mode-2

Cuadro 13/X.272 – Trama de control C_Mode-2

Campo	Descripción
Dirección Q.922	Véase 8.1 para detalles
Control	Véase 8.1 para detalles
NLPID	Véase 8.1 para detalles
Encabezamiento FRCP	El encabezamiento de protocolo FRCP consta de lo siguiente: • Ext.: Bit de ampliación, puesto necesariamente a 1 • Reserva: Bit reservado para uso futuro puesto a 0 • ID (2 bits) puesto a 01 • Bit de autenticación (A) – Puesto a 0 • Bit de control/datos (C/D) – Puesto a 1
Código	Puesto a 1 para Config_Req Puesto a 2 para Config_Ack
Identificador	Un número de transacción para correlacionar una petición con una respuesta. Se envía en la petición y se refleja en eco en la respuesta correspondiente
Longitud	Dos octetos de longitud. El valor se fija 7, que es el número total de octetos de la trama sin contar: dirección Q.922, control, NLPID, y encabezamiento FRCP

Cuadro 13/X.272 – Trama de control C_Mode-2 (*fin*)

Campo	Descripción
Tipo	0 C_Mode-2 23 LZS 254 FRCP C_Mode-1 Los tipos 245 a 253 inclusive y el tipo 255 están reservados Los números están en decimal
Longitud de opción de configuración	Puesta a 6 más el número de octetos en el campo valores
OUI	Identificador único de la organización (del vendedor)
Subtipo	Se utiliza para seleccionar entre múltiples DCFD de un mismo vendedor
Valores	Serán cero o más octetos. Pueden contener datos adicionales para cada protocolo de distintos vendedores, y pudieran incluir la opción de uso de múltiples historias para cada conexión
FCS	Secuencia de verificación de trama Q.922

11.2.2 Mensaje de control del C_Mode-2

El C_Mode-2 de FRCP permite la negociación de la DCFD específica del vendedor. La negociación se basa en los formatos de paquetes LCP definidos en la sección 5 de IETF RFC 1661 [13], con un conjunto único de opciones de configuración. Los paquetes LCP con códigos 1 a 7 son obligatorios. Los otros paquetes LCP especificados en IETF RFC 1661 son facultativos.

Los puntos de código de la opción de configuración FRCP que están asignados actualmente se describen a continuación:

Opción de configuración

23 LZS

254 FRCP C_Mode-1

255 Reservado para uso futuro.

C_Mode-2 utilizará la automatización de estados finitos descrita en las secciones 3 y 4 de IETF RFC 1661 [13] con las siguientes excepciones:

1) Si la automatización de estados finitos FRCP del C_Mode-2 pasa al estado f_0 debido a la expiración del periodo de temporización para la negociación y/o al rebasamiento del valor de un contador, la entidad pasará a la fase de inicialización del C_Mode-1.

2) Una entidad puede, en cualquier momento, abandonar el C_Mode-2 y entrar en la fase de inicialización de C_Mode-1.

3) Si, en cualquier momento, una entidad que funciona en el C_Mode-2 recibe una petición C_Mode-1, pasará a la fase de inicialización del C_Mode-1.

4) Si una entidad que soporta el C_Mode-2 se encuentra en ese momento en el C_Mode-1 y recibe una Config-Req de C_Mode-2, puede comenzar la negociación de C_Mode-2.

Para poder comunicar las PDU de datos FRCP, el FRCP tiene que haber pasado al estado f_1.

12 Facilidad de compresión securizada de datos

La facilidad de compresión securizada de datos se encarga de habilitar e iniciar algoritmos de compresión securizada de datos en ambos extremos del enlace. Para la compresión securizada de datos se utiliza un mecanismo de intercambio de paquetes similar al del protocolo de control del enlace (LCP), que es un protocolo punto a punto (PPP). La utilización de la facilidad de compresión securizada de datos se negocia entre dispositivos pares. El modo y los algoritmos se seleccionan independientemente para cada sentido de transmisión de una conexión virtual. El FRCP soporta la descripción de función de compresión de datos (DCFD), la cual se define en distintos documentos y que, en combinación con la presente Recomendación, es suficiente para asegurar la interoperabilidad del FRCP en el caso diferentes fabricantes suministran la misma función FRCP. El FRCP soporta procedimientos de detección de la pérdida de la sincronización y procedimientos de resincronización.

12.1 Encapsulación de la compresión de datos del S_Mode-1

El soporte de S_Mode-1 es obligatorio para las configuraciones de usuario que tienen habilitada la facilidad de compresión securizada de datos. La negociación de S_Mode-1 consiste en una simple toma de contacto para habilitar el algoritmo de compresión securizada (SCA, *secure compression algorithm*) de datos por defecto y sus correspondientes parámetros para uno u otro sentido de transmisión de la conexión virtual.

El algoritmo de compresión de datos por defecto es FZA, descrito en [17]. El algoritmo FZA utiliza un lenguaje cifrado de tren de datos para actualizar aleatoriamente su modelo de compresión interna de datos. Para utilizar el lenguaje cifrado de tren de datos se necesita una clave de criptación o una semilla inicial para deducir la clave. Los procedimientos para el intercambio de claves y para la actualización de las claves están fuera del ámbito de la presente Recomendación. Además, al igual que los algoritmos tradicionales de compresión de datos, FZA requiere que los diccionarios del emisor y del receptor se mantengan sincronizados. FZA criptará los datos si se desactiva la opción de compresión securizada.

12.1.1 Formatos de tramas de control del S_Mode-1

Las tramas utilizadas para negociar los parámetros S_Mode-1 tienen el formato presentado en la figura 6 con los bits Ext. y C/D del octeto de encabezamiento FRCP puestos a 1. El valor del campo ID del encabezamiento FRCP se fijará a 10. El valor del campo tipo de la trama se fijará a 254 decimal.

12.1.2 Procedimientos de control del S_Mode-1

Igual que 10.1.1.

12.1.2.1 Elementos de parámetros del S_Mode-1

Igual que 10.1.1.1.

12.2 Formato de transferencia de datos del S_Mode-1

En esta cláusula se describe el método de encapsulación para la compresión securizada de datos como la única facilidad configurada. Se describen también los procedimientos antiexpansión y de sincronización. El formato de trama general se presenta en la figura 16. En esta figura, el bit C/D del encabezamiento FRCP se pone a 0 para indicar se trata de una trama de datos. Los bits C/U, RA y RR se utilizan para los procedimientos antiexpansión y de sincronización.

12.2.1 Formato de la señalización antiexpansión

La señalización antiexpansión (controlada por el bit C/U) debe proporcionarse del codificador al decodificador en un sentido de transmisión de la conexión de compresión de datos FRCP para indicar si la compresión utilizada para la cabida útil FRCP asociada es o no una compresión securizada. El emisor debe fijar C/U = "1" cuando se haya aplicado compresión securizada a los datos de usuario. Cuando C/U = "1", el decodificador decodificará la cabida útil FRCP a la que se ha aplicado la compresión securizada.

El emisor puede fijar C/U = "0" cuando se ha aplicado compresión securizada a los datos de usuario. Sin embargo, hay que criptar los datos mediante el modo de criptación FZA antes de transmitirlos por el enlace. En otro caso, hay que aplicar siempre compresión securizada a los datos antes de transmitirlos por el enlace, incluso si ha habido expansión de datos. Cuando C/U = 0, el decodificador securizado decriptará, mediante el modo de criptación FZA, la cabida útil FRCP criptada. El campo número secuencial se criptará e incluirá en la PDU de FRCP. Además, el campo LCB tiene que estar presente.

12.2.1.1 Formato de la señalización de sincronización

Igual que 11.1.3.2.

12.2.1.2 Cabida útil de datos FRCP del S_Mode-1

El contenido de la cabida útil FRCP se define de acuerdo con la DCFD. La cabida útil FRCP tiene que ser un número entero de octetos. Véanse la figura 16 y el cuadro 14.

<table>
<tr><td colspan="8">Dirección Q.922, control y NLPID</td><td>1-4</td></tr>
<tr><td colspan="8">Encabezamiento FRCP</td><td></td></tr>
<tr><td>Ext.
1</td><td>C/U</td><td>RA</td><td>RR</td><td>O</td><td>P</td><td>T</td><td>C/D
0</td><td>5</td></tr>
<tr><td colspan="8">Cabida útil de compresión securizada de datos FRCP</td><td>6</td></tr>
<tr><td colspan="8">Número secuencial</td><td>n</td></tr>
<tr><td colspan="8">LCB</td><td>n+1</td></tr>
<tr><td colspan="8">FCS
(2 octetos)</td><td>n+2
n+3</td></tr>
</table>

Figura 16/X.272 – Trama de transferencia de datos S_Mode-1

Cuadro 14/X.272 – Trama de transferencia de datos S_Mode-1

Campo	Descripción
Dirección Q.922	Véase 8.1 para detalles.
Control	Véase 8.1 para detalles.
NLPID	Véase 8.1 para detalles.
Encabezamiento FRCP	El encabezamiento de protocolo FRCP consta de lo siguiente: • Ext.: Bit de extensión, necesariamente puesto 1 • Comprimido/no comprimido (C/U) • Reset_Ack (RA) • Reset_Request (RR) • Opción de protocolo (OPT): Puesto a: O P T 0 1 0 para especificar compresión securizada • Bit control/datos (C/D): Puesto a 0 para indicar una trama de datos
Cabida útil de compresión de datos	Trama Q.933 Anexo E que está comprimida
Número secuencial	Se inicializa a 1 y se incrementa módulo 256 después de cada trama. NOTA – Este octeto se añade al final de los datos de usuario y se le ha aplicado compresión securizada
LCB	LCB se calcula sobre los datos de usuario originales, incluido el número secuencial
FCS	Secuencia de verificación de trama Q.922

12.3 Encapsulación de la compresión de datos del S_Mode-2

El soporte de S_Mode-2 es facultativo y proporciona la capacidad para habilitar o inhabilitar el FRCP, así como para negociar las DCFD y sus correspondientes parámetros.

12.3.1 Formatos de tramas de control del S_Mode-2

Estas tramas se utilizan para negociar parámetros S_Mode-2. Véanse la figura 17 y el cuadro 15.

Descripción								Octeto
Dirección Q.922 (2 octetos) (nota)								1 2
Control (UI: 0x03)								3
NLPID (0xB0)								4
Encabezamiento FRCP								
Ext. 1	Reserva	Reserva	Reserva	I	D	A	C/D 1	5
Código								6
Identificador								7
Longitud (2 octetos)								8 9
Tipo								10
Longitud de opción de configuración								11
OUI (3 octetos)								12 13 14
Subtipo								15
Valores								16
FCS (2 octetos)								17 18

NOTA – La dirección de retransmisión de tramas se presenta en formato de 2 octetos a título ilustrativo. Los formatos de dirección de 3 y 4 octetos no están prohibidos.

Figura 17/X.272 – Trama de control S_Mode-2

Cuadro 15/X.272 – Trama de control S_Mode-2

Campo	Descripción
Dirección Q.922	Véase 8.1 para detalles
Control	Véase 8.1 para detalles
NLPID	Véase 8.1 para detalles
Encabezamiento FRCP	El encabezamiento de protocolo FRCP consiste en lo siguiente: • Ext.: Bit de extensión, necesariamente puesto a 1 • Reserva: Bits de reserva, necesariamente puestos a 0 • ID (2 bits) fijado a "10" • Bit de autenticación (A) – Puesto a 0 • Bit de control/datos (C/D) – Puesto a 1
Código	Puesto a 1 para Config_Req Puesto a 2 para Config_Ack
Identificador	Un número de transacción para correlacionar una petición con una respuesta. Se envía en la petición y se refleja en eco en la respuesta correspondiente
Longitud	Dos octetos de longitud. El valor se fija 7, que es el número total de octetos de la trama, sin contar: dirección Q.922, control, NLPID, y encabezamiento FRCP
Tipo	0 S_Mode-2 254 FRCP S_Mode-1 Los tipos 245 a 253 inclusive y el tipo 255 están reservados Números en decimal

Cuadro 15/X.272 – Trama de control S_Mode-2 (*fin*)

Campo	Descripción
Longitud de opción de configuración	Fijada a 6 más el número de octetos en el campo valores
OUI	Identificador único de la organización (del vendedor)
Subtipo	Se utiliza para seleccionar entre múltiples DCFDs de un mismo vendedor
Valores	Serán cero o más octetos. Pueden contener datos adicionales para cada protocolo de distintos vendedores, y pudieran incluir la opción de uso de múltiples historias para cada conexión
FCS	Secuencia de verificación de trama Q.922

12.3.2 Mensaje de control del S_Mode-2

El S_Mode-2 del FRCP permite la negociación de DCFD específica del vendedor. La negociación se basa en los formatos de paquete LCP definidos en la sección 5 de IETF RFC 1661 [13]. Los detalles son similares a los de las especificaciones del E_Mode-2 presentadas en 10.2.

El S_Mode-2 utilizará la automatización de estados finitos descrita en las secciones 3 y 4 de IETF RFC 1661 [13] con las siguientes excepciones:

1) Si la automatización de estados finitos FRCP del S_Mode-2 pasa al estado f_0 debido a la expiración del periodo de negociación y/o al rebasamiento del valor de un contador, la entidad pasará a la fase de inicialización S_Mode-1.
2) Una entidad puede, en cualquier momento, abandonar el S_Mode-2 y entrar en la fase de inicialización del S_Mode-1.
3) Si, en cualquier momento, una entidad que funciona en el S_Mode-2 recibe una petición S_Mode-1, pasará a la fase de inicialización del S_Mode-1.
4) Si una entidad que soporta el S_Mode-2 se encuentra en un momento dado en el S_Mode-1 y recibe una Config-Req. S_Mode-2, puede comenzar la negociación del S_Mode-2.

13 Encapsulación de la transferencia de datos FRCP en el caso de múltiples facilidades

En esta cláusula se describe el formato de las tramas FRCP cuando se configuran y se negocian con éxito múltiples facilidades.

13.1 Criptación de datos y compresión securizada de datos

En esta cláusula se examina la encapsulación de tramas que incluyen la utilización de las facilidades de compresión securizada y de criptación. Los algoritmos utilizados son los adoptados para los modos de funcionamiento E_Mode-1 y S_Mode-1. El tratamiento del vector de inicialización (IV) para el E_Mode-1 es similar al descrito en 10.1.1.1.

Para implementaciones en las que las opciones de criptación y compresión securizada han sido configuradas y negociadas con éxito. Primeramente, a los datos de usuario se les aplica la compresión securizada utilizando el algoritmo SCA del S_Mode-1. Se calculará un LCB sobre los datos de usuario originales, en bruto. El LCB se añade al final de los datos comprimidos en forma securizada, como se muestra a continuación:

Descripción	Octeto
Datos de usuario comprimidos en forma securizada	1 k
LCB calculado sobre los datos de usuario originales en bruto	k+1

Los datos comprimidos y LCB (k + 1 octetos) se tratan entonces como los nuevos datos de usuario que habrán de ser cifrados por el criptador. El criptador rellenará los datos hasta el siguiente múltiplo de 8 octetos como se describe en 10.1.2, antes de cifrarlos. Antes de la etapa de criptación se calcula un octeto de verificación longitudinal (LCB) sobre los datos comprimidos en forma securizada y el LCB (k + 1 octetos), los octetos de relleno y el octeto de longitud del relleno. A continuación, se criptan los datos y se calcula un número secuencial que habrá de insertarse en la trama como se describe en la figura 18. El emisor incrementa módulo 256 el número secuencial. Seguidamente, el emisor añade el LCB al final de la cabida útil y envía la trama por el enlace.

En el extremo de recepción, el receptor comienza por examinar el número secuencial para determinar si se ha perdido una trama. Si se ha perdido una trama, los últimos 8 octetos del texto en lenguaje cifrado se mantienen como el vector inicial para la trama siguiente y la trama recibida se descarta. Se enviará una petición de reiniciación a la entidad par emisora para pedirle que reinicie la historia de la compresión securizada. Para efectuar esto se ponen a 1 los bits RR y RA como se describe en las cláusulas conexas. No se proporcionarán datos del descriptador al codificador hasta que se reciba un acuse de recibo de reiniciación de la entidad par emisora.

Si la trama está en secuencia, el receptor descifra los campos identificados en la figura 9 y calcula el LCB. El LCB calculado se compara con el LCB recibido. Si no concuerdan, los últimos 8 octetos de los datos se mantienen como el vector inicial para la trama siguiente, y la trama recibida se descarta. Se enviará una petición de reiniciación a la entidad par emisora para pedirle que reinicie la historia de la compresión securizada. Para efectuar esto se ponen a 1 los bits RR y RA como se describe en las cláusulas conexas. No se proporcionarán datos del descriptador al codificador hasta que se haya recibido un acuse de recibo de reiniciación de la entidad par emisora. Si los LCB concuerdan, los datos descifrados se procesan suprimiéndoles el número secuencial, el relleno, el octeto de longitud del relleno y el octeto de verificación longitudinal (LCB). Los datos se reenvían entonces al decodificador, donde se les aplica una etapa de decompresión securizada. El decodificador calcula el LCB sobre los datos no comprimidos. Si el LCB concuerda, el codificador reenvía los datos a la capa superior. Si no concuerda, se enviará una petición de reiniciación a la entidad par emisora para pedirle que reinicie la historia de la compresión securizada. Esto se efectúa poniendo a 1 los bits RR y RA como se describe en las cláusulas conexas. No se proporcionarán datos del decriptor al codificador hasta que se reciba un acuse de recibo de reiniciación de la entidad par emisora.

En el periodo durante el cual el decriptor espera la recepción de un acuse de recibo de reiniciación del emisor indicativo de que las historias están sincronizadas, el decriptor mantendrá los últimos 8 octetos del texto en lenguaje cifrado como el vector inicial para la trama siguiente y descartará la trama recibida.

Cuando la opción de compresión securizada está combinada con la opción de criptación, los datos se pasarán siempre a través del compresor securizado y del criptador. Esto es así porque el algoritmo FZA criptará los datos si la opción de compresión está desactivada. En consecuencia, cualquiera que sea el valor del bit C/U del encabezamiento FRCP, el descriptador proporcionará al decodificador securizado los datos para las tramas con número secuencial y LCB correctos. Véase también el cuadro 16.

Descripción								Octeto
Información de dirección de retransmisión de tramas, control y NLPID								1-4
Encabezamiento FRCP								5
Ext. 1	Reservado	Reservado	Reservado	I	D	A	C/D 0	
Número secuencial								6
Datos de usuario comprimidos en forma securizada (nota) (k + 1 octetos)								7 m
Relleno (nota)								m n-1
Longitud del relleno (nota)								n
LCB								n+1
FCS (2 octetos)								n+2 n+3

NOTA – Este campo está criptado.

Figura 18/X.272 – Formato de trama de transferencia de datos comprimidos en forma securizada y criptados

Cuadro 16/X.272 – Formato de trama de transferencia de datos comprimidos en forma securizada y criptados

Campo	Descripción
DLCI, control y NLPID	Véase 8.1 para detalles
Encabezamiento FRCP	El encabezamiento de protocolo FRCP consiste en lo siguiente: • Ext.: Bit de extensión, fijado necesariamente a 1 • Comprimido/no comprimido (C/U): Puesto a 1 para indicar que los datos están comprimidos • Reset_Ack (RA): Puesto a 1 por el emisor si acusa recibo de la petición de reiniciación de la entidad par distante • Reset_Request (RR): Puesto a 1 por el receptor si se requiere sincronización de la compresión securizada • Opción de protocolo (OPT): Puesta a: O P T 1 0 1 para especificar criptación • Bit de control/datos (C/D): Puesto a 0 para indicar una trama de datos
Número secuencial	Número asignado secuencialmente por el encriptor, que comienza por 0 y se incrementa módulo 256
Datos de usuario	Los datos de usuario son primeramente comprimidos y después criptados. Los datos tienen que ser primeramente decriptados y después decodificados
Relleno	Véase 10.1.2 para detalles
Longitud del relleno	Véase 10.1.2 para detalles
LCB	Octeto de verificación longitudinal – se calcula sobre texto comprimido de octetos 7 a n
FCS	Secuencia de verificación de trama Q.922

El número secuencial y el LCB son generados por el encriptor. Los octetos 8 a m se aplican a la entrada del decodificador. Tras la detección de la pérdida de la sincronización debida a un número secuencial incorrecto o a un LCB incorrecto, hay que resincronizar las historias de la compresión poniendo a 1 los bits RR y RA como se describe en las cláusulas conexas.

13.2 Criptación y datos comprimidos

Si las facilidades de compresión y criptación de datos están configuradas y han sido negociadas con éxito, los datos de usuario son primeramente comprimidos, y después criptados. El proceso es el mismo descrito en 11.1 con la diferencia de que cuando el bit C/U está puesto a 1 para indicar ausencia de compresión, los datos no se reenvían al decodificador.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos y comunicación entre sistemas abiertos**
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2001