INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.272

(03/2000)

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

Open Systems Interconnection – Security Protocols

Data compression and privacy over frame relay networks

ITU-T Recommendation X.272

(Formerly CCITT Recommendation)

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	**X.270–X.279**
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation X.272

Data compression and privacy over frame relay networks

Summary

This Recommendation defines Data Compression and Privacy Service for Frame Relay networks. The presence of a data compression service in a network will increase the effective throughput of the network.

On the other hand, the increasing demand for transmitting sensitive data across public networks requires facilities for ensuring the privacy of the data. In order to achieve optimum compression ratios, it is essential to compress the data before encrypting it. Hence, it is desirable to provide facilities in the specification of the data compression service to negotiate data encryption protocols as well. Since the task of compressing and then encrypting the data is computational intensive, efficiency is achieved through providing simultaneous data compression and encryption (secure data compression).

Source

ITU-T Recommendation X.272 was prepared by ITU-T Study Group 7 (1997-2000) and approved under the WTSC Resolution 1 procedure on 31 March 2000.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSC Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Introduction

This Recommendation specifies the procedures for performing Data Compression and Privacy over Frame Relay. This Recommendation applies to Unnumbered Information (UI) control field frames. This Recommendation does not cover frames that use a Number Information (I) control field.

ITU-T Recommendation X.272

Data compression and privacy over frame relay networks

1 Scope

The scope of this Recommendation covers the negotiation and encapsulation of Data Compression, Secure data compression, authentication and encryption over frame relay. These protocols are based on PPP Link Control Protocol (IETF RFC 1661) [13] and PPP Encryption Control Protocol (IETF RFC 1968 [14] and 1969 [15]).

This Recommendation applies to Unnumbered Information (UI) frames encapsulated using Q.933 Annex E [7]. It addresses data compression and privacy on both permanent virtual connections (PVC) and switched virtual connections (SVC).

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T I.122 (1993), *Framework for frame mode bearer services*.

[2] ITU-T I.233.1 (1991), *ISDN frame relaying bearer service*.

[3] ITU-T I.370 (1991), *Congestion management for the ISDN frame relaying bearer service.*

[4] ITU-T E.164 (1991), *Numbering plan for the ISDN.*

[5] ITU-T Q.922 (1992), *ISDN data link layer specification for frame mode bearer services.*

[6] ITU-T Q.921 (1993), *ISDN user-network interface – Data link layer specification.*

[7] ITU-T Q.933 (1995), *Digital subscriber signalling system No. 1 (DSS1) Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring.*

[8] ITU-T Q.931 (1993), *ISDN user-network interface layer 3 specification for basic call control.*

[9] ITU-T Q.850 (1993), *Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part.*

[10] ITU-T Q.951 (1993), *Stage 3 description for number identification supplementary services using DSS1.*

[11] ITU-T X.36 Amendment 1 (1996), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for public data network providing frame relay data transmission service by dedicated circuit.*

[12] ITU-T X.121 (1992), *International numbering plan for public data networks.*

[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 Terms and definitions

This Recommendation defines the following terms:

3.1 anti-expansion: A method to inhibit the expansion of user data due to compression encoding.

3.2 data compression context: A vocabulary and other information for error detection and synchronization, created and maintained by peers to encode/decode user data.

3.3 data compression function: An entity that performs the data compression encoding, decoding, error detection, synchronization and negotiation.

3.4 data compression function definition: A specification that describes the format and procedures used by a data compression function to transport user data and control primitives.

3.5 decoder: An entity that decompresses user data.

3.6 encoder: An entity that compresses user data.

3.7 history buffer: The type of vocabulary used for data compression.

3.8 0x stands for hexadecimal numbers.

3.9 longitudinal check byte (LCB): The LCB is calculated for each frame by:

1) exclusive ORing 0xFF to the first octet of the payload and storing the result. Then,

2) each subsequent octet of the payload is XORed to the result generating the next value of the result.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

A	Authentication bit
Ack	Acknowledgement
CBC	Cipher Block Chaining
CCP	Compression Control Protocol
C/D	Control/data
CHAP	Challenge Handshake Authentication Protocol
C_Mode-1	Default Data Compression Mode 1
C/U	Compressed/uncompressed
C/R	Frame Header as described in ITU-T Q.922
DC	Data Compression
DCCI	Data compression context identifier
DCFD	Data Compression Function Definition
DCP	Data Compression Protocol

DCPCP	DCP Control Protocol
DES	Data Encryption Standard
DLCI	Data Link Control Identifier
DTE	Data Terminal Equipment
E_Mode-1	Default Data Encryption Mode 1
Ext.	Extension Bit
FCS	Frame Check Sequence as described in ITU-T Q.922
FECN	Frame Header as described in ITU-T Q.922
FR	Frame Relay
FRCP	Frame Relay Compression and Privacy Protocol
FZA	Secure Data Compression Algorithm
LCB	Longitudinal Check Byte
LCP	Link Control Protocol
LZS	Data Compression Algorithm
NLPID	Network Layer Protocol Identifier
OUI	Organization Unique Identifier
PDU	Protocol Data Unit
PVC	Permanent Virtual Connection
RA	Reset Acknowledge
SCA	Secure Data Compression Algorithm
S_Mode-1	Default Secure Compression Mode 1
SVC	Switched Virtual Connection
XOR	Boolean Exclusive OR

5 Conventions

This Recommendation uses some words for defining the significance of each particular requirement. These words are:

- Must, Shall, or Mandatory – The item is an absolute requirement of this Recommendation.
- Should – The item is highly desirable.
- May or Optional – The item is not compulsory, and may be followed or ignored according to the requirements of the implementor.
- Not Applicable – the item is outside the scope of this Recommendation.

6 Overview

This Recommendation specifies the encapsulation of Frame Relay Compression and Privacy Protocol (FRCP) over frame relay networks. This Recommendation allows the negotiation and implementation of several facilities. The list includes: Authentication procedures; Data encryption facility; Secure Data compression facility and Data Compression facility. The FRCP provides two modes of operation for the encryption facility:

- E_Mode-1: E_Mode-1 is the default mode and is mandatory for any implementation that supports the encryption facility. It allows negotiation of encryption parameters. The proposed default encryption algorithm is the Data Encryption Standard (DES) 56-bit key with Cipher Block Chaining (CBC) [21]. The secret Data Encryption Standard (DES) key shared between the communicating parties is eight octets in length. This key consists of a 56-bit quantity used by the Data Encryption Standard (DES) algorithm. The 56-bit key is stored as a 64-bit (eight octet) quantity, with the least significant bit of each octet used as a parity bit.

- E_Mode-2: E_Mode-2 is optional and allows full negotiation of encryption algorithms, both standard and proprietary, and their associated parameters. This mode is based on the Encryption Control Protocol for PPP [14]. This mode can be used to support encryption keys that are greater than 56 bits in length. The size of the key is vendor specific.

In addition, the FRCP provides two modes of operation for the secure data compression facility:

- S_Mode-1: S_Mode-1 is the mandatory mode and uses the default algorithms and frame formats defined in this Recommendation. S_Mode-1 provides a simple negotiation protocol to enable secure data compression service with default parameters. The secure data compression algorithm requires the use of an encryption key. The encryption key shared between the communicating parties is eight octets in length. This key consists of a 56-bit quantity used that is stored as a 64-bit (eight octets) quantity, with the least significant bit of each octet used as a parity bit.
- S_Mode-2: S_Mode-2 is optional and allows full negotiation of secure data compression algorithms and their associated parameters.

Furthermore, the FRCP provides two modes of operation for the data compression facility:

- C_Mode-1: C_Mode-1 is the mandatory mode and uses the default algorithms and frame formats defined in this Recommendation. C_Mode-1 provides a simple negotiation protocol to enable data compression service with default parameters.
- C_Mode-2: C_Mode-2 is optional and allows full negotiation of data compression algorithms, both standard and proprietary, and their associated parameters.

7 Reference Model

The term "**DTE**" in the context of this Recommendation is not restricted to only the function of Terminal Equipment. It indicates a user of the network in a general functional sense, which itself might be another (type of) network.

The FRCP service facilitates efficient communication in terms of a higher packet/frame rate, that could be transported in a secure fashion if the privacy option is negotiated. When used between DTEs, as shown in Figure 1, the data compression and privacy procedure is transparent to Frame Relay network(s) between the transmitting and receiving DTEs.

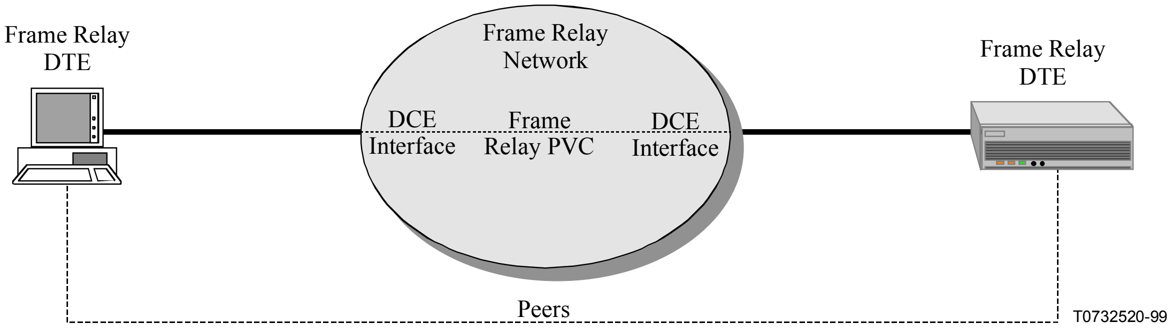


Figure 1/X.272 – Reference diagram

The Frame Relay Compression and Privacy Protocol relies on different phases in order to negotiate the supported facilities. The order of the phases is as follows:

1) VC Establishment: This phase is controlled by the signalling procedures for PVC or SVC [1] to [12] and is outside the scope of this Recommendation. The FRCP phase starts after the VC has been established.
2) Authentication phase: When used, initial peer authentication must be done prior to the data compression or encryption phase(s). Subsequent authentication challenges, if supported by the chosen authentication protocol, may be done during the data transfer phase, in clear text without the use of the encryption, secure compression and compression facilities.
3) Encryption negotiation phase: Used to negotiate the mode and parameters to be used for encryption during the data transfer phase.
4) Secure Data compression negotiation phase: Used to negotiate the mode and parameters that are used for secure data compression during the data transfer phase.
5) Data compression negotiation phase: Used to negotiate the mode and parameters that are used for data compression during the data transfer phase.
6) Data Transfer Phase: Transfer of ciphered, secure compressed or compressed messages which may include user data, and control information.

8 Common mode specification

This clause defines the frame formats and procedures common to all FRCP facilities.

8.1 General frame format

The general frame structure of FRCP supports the encapsulation of control information or the transfer of data. All frames are sent on the frame relay virtual connection between end systems. The frame contents are transparent to the frame relay network. Control frames contain the information that is vital to negotiating the authentication, encryption, secure data compression, data compression facilities and their associated parameters. The C/D bit in the FRCP distinguishes between control and data frames. For control frames, the C/D bit is set to 1. The general FRCP control frame format in Figure 2 is used to negotiate control information.

<table>
<tr><th colspan="8">Description</th><th>Octet</th></tr>
<tr><td colspan="8">Q.922 Address
(2 octets) (Note)</td><td>1
2</td></tr>
<tr><td colspan="8">Control
(UI: 0x03)</td><td>3</td></tr>
<tr><td colspan="8">NLPID
(0xB0)</td><td>4</td></tr>
<tr><td colspan="8">FRCP Header</td><td rowspan="2">5</td></tr>
<tr><td>Ext.
1</td><td>Spare</td><td>Spare</td><td>Spare</td><td>Spare</td><td>I</td><td>D</td><td>C/D
1</td></tr>
<tr><td colspan="8">FRCP Payload</td><td>6
n</td></tr>
<tr><td colspan="8">FCS
(2 octets)</td><td>n+1
n+2</td></tr>
</table>

NOTE – The 2 octets frame relay address is shown here for illustrative purposes. The 3-and 4-octet address formats are not prohibited.

Figure 2/X.272 – Frame Relay Privacy Protocol Control Frame Format

The Q.922 [5] frame relay address in Figure 2 is shown in two octets format. However, the FRCP does not prohibit the use of the third and fourth octet address formats. See Table 1.

Table 1/X.272 – Frame Relay data Compression and Privacy Protocol Control Frame Format

Field	Description
Q.922 Address	Frame Relay Address structure as defined in ITU-T Q.922 [5]
Control	Frame Relay Q.922 [5] Unnumbered information frame (UI) (x03)
NLPID	Network Layer Protocol ID
FRCP Header	The FRCP Protocol Header consists of the following: • Ext.: Extension bit, set to one • Spare: Spare bits for future use, set to 0 • ID (two bits): This field specifies the facility that is used. The facilities are defined below: I D 0 0 Reserved 0 1 Compress 1 0 Secure compress 1 1 Encrypt • A: Authentication bit. Can only be set to 1 when C/D = 1. Indicates that frame contains authentication information • Control/Data (C/D) bit 0 Data Frame 1 Control Frame
FRCP Payload	Control information or transfer data depending on how the FRCP header bits are set
FCS	Q.922 Frame Check Sequence

If the C/D bit is set to 1, the frame is a control frame. The ID field is used in this case to negotiate various facilities of the FRCP. The facilities are negotiated one at a time in the order given in 8.2. The details of the frame format are given in the related sections. If the A bit is set to "1", the ID filed is ignored, since the frame is an authentication frame.

If the C/D bit is set to 0, the frame is a data transfer frame. The format of a data transfer frame is dependent on the FRCP facility or facilities that have been negotiated. In Figure 3, the general format of FRCP data transfer frame is depicted. The description of the various fields is given in Table 2.

Description								Octet
Q.922 Address (2 octets) (Note)								1 2
Control (UI: 0x03)								3
NLPID (0xB0)								4
FRCP Header								
Ext 1	C/U	RA	RR	O	P	T	C/D 0	5
FRCP Payload								6 n
FCS (2 octets)								n+1 n+2

NOTE – The 2 octets frame relay address is shown here for illustrative purposes. The 3-and 4-octet address formats are not prohibited.

Figure 3/X.272 – Frame Relay Privacy Protocol Data Frame Format

Table 2/X.272 – Frame Relay data Compression and Privacy Protocol Data Frame Format

Field	Description
Q.922 Address	Frame Relay Address structure containing DLCI, FECN, BECN, DE and C/R. The C/R bit is not used
Control	Frame Relay Q.922 Unnumbered information frame (UI) (x03)
NLPID	Network Layer Protocol ID from ISO/IEC TR 9577
FRCP Header	The FRCP Protocol Header consists of the following: • Extension bit – Set to one, but included for future enhancement • Compressed/Uncompressed (C/U): Set to 1 indicates that data is uncompressed • Reset_Ack (RA): Set to 1 to indicate the acknowledgement of a reset of a compression history or an encryption history. The distinction between the type of histories is given in the O, P, T bits • Reset_Request (RR): Set to 1 to indicate the request of a reset of a compression history or an encryption history. The distinction between the type of histories is given in the O, P, T bits • Control/Data (C/D) bit: Set to 0 to indicate a data frame • Protocol option (OPT): Relates to the data to the associated protocol according to the following assignment: O P T 0 0 0 Reserved 0 0 1 Encryption 0 1 0 Secure Compression 0 1 1 Compression 1 0 0 Compressed and Encrypted 1 0 1 Secure Compressed and Encrypted x x x All others are reserved
FRCP Payload	Data that is compressed or encrypted, depending on the FRCP facility or facilities that have been negotiated
FCS	Q.922 Frame Check Sequence

8.2 Negotiation of facilities

During the negotiation stage, the FRCP Header C/D bit is set to 1 to indicate that the frame is a control frame. The format of the control frame enables the negotiation of several facilities. Each facility is negotiated separately. The order of the facility negotiation is given below:

- If authentication is configured, the peers must be authenticated first. If the authentication stage is successful, other facilities can be negotiated. However, if the authentication stage is not successful, the connection must be terminated.
- If the encryption option is configured, this option must be negotiated next. If the negotiation is successful, other options can be subsequently negotiated. However, if the encryption negotiation fails, the connection must be terminated.
- If the secure data compression option is configured, this option must be negotiated next. If the negotiation is successful, data must be secure compressed before sending it on the link. If the secure compression negotiation fails, then the data transfer stage can proceed with no secure data compression if and only if the encryption facility is configured and has been successfully negotiated. Otherwise, the connection must be terminated.
- The data compression option can be configured and negotiated provided that the secure data compression option is not configured. If the data compression option is configured, this option is negotiated next. If the negotiation is successful, data can be sent on the link in a compressed fashion. The data must be encrypted if the encryption option is configured and is negotiated successfully. In the case that no other options are configured, data can be transmitted on the link in uncompressed fashion if the negotiation of the data compression facility is not successful. Otherwise, the data must be encrypted before its transmission on the link.
- If the order of negotiation does not follow the order as specified above, the connection must be terminated. The order of negotiation is summarized in the Table 3 below:

Table 3/X.272 – Order of facility negotiation

Facility Requested	**Authenticate**	**Encrypt**	**Secure Compress**	**Compress**
Facility Negotiated				
None	Proceed	Proceed	Proceed	Proceed
Authenticate	Proceed	Proceed	Proceed	Proceed
Encrypt	Terminate	Proceed	Proceed	Proceed
Secure Compress	Terminate	Terminate	Proceed	Terminate
Compress	Terminate	Terminate	Terminate	Proceed
Authenticate, Encrypt	Proceed	Proceed	Proceed	Proceed
Authenticate, Encrypt, Secure Compress	Proceed	Proceed	Proceed	Terminate
Authenticate, Compress	Proceed	Terminate	Terminate	Proceed

NOTE – After the successful negotiation of any facility, all frames exchanged on a connection must be encapsulated using FRCP format.

9 Authentication facility

This facility is used to authenticate two devices based on a preselected authentication protocol. The authentication facility is optional. If authentication is desired, an implementation must perform the initial authentication before invoking the encryption, secure data compression or data compression facilities.

Authentication packets are identified via the **A** bit in the FRCP header of a control message (C/D = 1). In general the authentication features of PPP [19] are used. The authentication protocol is negotiated during the call establishment for PVCs or SVCs. The authentication protocol is identified in octets 6, 7, and 7a, if applicable. Octets 8-n contain authentication information or configuration options in an authentication packet format specific to the protocol identified in octet groups 6 and 7.

The FRCP authentication mechanism supports the authentication protocols defined for PPP, such as, the PPP Extensible Authentication Protocol (EAP) which itself supports a number of authentication protocols, the PPP Challenge Handshake Authentication Protocol (CHAP) and the PPP Password Authentication Protocol (PAP). Details of the PPP authentication protocols may be found in each of the individual PPP authentication RFCs [13] to [16].

The authentication is peer to peer. This implies that both peers must authenticate each other before bidirectional traffic can flow across the connection.

9.1 Authentication frame format

The authentication frame format is given in Figure 4 below. See also Table 4.

Description								**Octet**
Frame Relay address, control and NLPID information								1-4
FRCP Heade								
Ext. 1	Spare 0	Spare 0	Spare 0	I 0	D 0	A 1	C/D 1	5
Authentication Protocol ID (Note 2)								6 7
Authentication Algorithm (Note 2)								7a* (Note 1)
Authentication Packet Format (Note 2)								8 n
FCS (2 octets)								n+1 n+2

NOTE 1 – Octet 7a is only present if octets 6 and 7 indicate CHAP (xC223).

NOTE 2 – Contents and formats are defined from PPP RFCs.

Figure 4/X.272 – General Authentication Frame Format

Table 4/X.272 – General Authentication Frame Format

Field	Description
DLCI, control and NLPID	See 8.1 for details
FRCP Header	• Ext.: Extension bit set to 1 • Spare: Spare bit for future use set to 0 • ID field set to 00 • Authentication (A) bit set to 1 • Control/Data (C/D) bit set to 1
Authentication Protocol ID (octets 6 and 7)	Identifies the authentication protocol to be used, e.g. PAP, CHAP, etc. See IETF RFC 1340 [18] for details
Authentication Algorithm (Octet 7a)	If present, identifies the CHAP authentication method to be used. See IETF RFC 1994 [19] for details. Only present if octets 6 and 7 indicate CHAP
Authentication Packet Format (octets 8-n)	In general, uses packet format of specific PPP authentication method
FCS	Q.922 Frame Check Sequence

9.2 Authentication packet format

The PPP style packets shall be encapsulated within octets 8-n of the frame format above. These packets are of the general format: Code, Identifier, Length, Values. For example, in the CHAP case, the packet format of IETF RFC 1994 [19] section 4 is used, as depicted in Figure 5 and described in Table 5.

Description	Octet
Code	8
Identifier	9
Length (2 octets)	10 11
Values/Data as defined by authentication protocol	12 n

Figure 5/X.272 – Authentication Packet Format

Table 5/X.272 – FRCP Control Primitive Structure

Field	Description
Code	From PPP Authentication method indicated in octets 6-7a. It indicates the type of packet or message, e.g. Request, Response, etc.
Identifier	A transaction number to correlate a request with a response. Sent in request and echoed in corresponding response
Length (2 octets)	Including: Code, Identifier, Length and all Configuration Options
Configuration Options	Values/Data depending on the PPP Authentication protocol used. See specific PPP Authentication method for details, e.g. CHAP EAP, PAP, etc.

9.3 Authentication procedures

Follow the procedures described in the applicable RFC for the PPP authentication protocol used. For example, if the authentication protocol configured is CHAP (0xCC23) then follow the procedures in IETF RFC 1994 [19].

10 Encryption facilities

The encryption facility is responsible for enabling and initiating data encryption algorithms on both ends of the link. Encryption uses a similar packet exchange mechanism as the PPP Link Control Protocol (LCP) [16].

The use of the encryption facility is negotiated between peer devices. The mode and algorithms are selected independently for each direction of a virtual connection. This is summarized in Table 6 below:

Table 6/X.272 – E_Mode-1 Transition Table

Requested	Configured	
	E_Mode-1	**E_Mode-2**
E_Mode-1	Respond with E_Mode-1 and use E_Mode-1.	Respond with E_Mode-1 and use E_Mode-1.
E_Mode-2	Respond with E_Mode-1 and use E_Mode-1.	Respond with E_Mode-2 and use E_Mode-2.

It is assumed that each peer device has an initial key to be used for encryption. The method by which the key becomes known to both communicating devices is outside the scope of this Recommendation. Encryption negotiation must be completed successfully before allowing transfer of data. Once negotiated all data frames exchanged on a VC must be encrypted.

10.1 E_Mode-1 Specification

E_Mode-1 encryption must be supported if the encryption facility is implemented in DTE. E_Mode-1 uses the Data Encryption Standard (DES) with 56-bit key with Cipher Block Chaining, (CBC) [21]. The cyphertext is transferred using the packet format defined in 10.1.4 E_Mode-1 Data Transfer Procedures.

10.1.1 E_Mode-1 Control Frame Formats

This frame is used to negotiate E_Mode-1 parameters. See Figure 6 and Table 7.

<table>
<tr><th colspan="8">Description</th><th>Octet</th></tr>
<tr><td colspan="8">Frame Relay address, control and NLPID information</td><td>1-4</td></tr>
<tr><td colspan="8">FRCP Header</td><td></td></tr>
<tr><td>Ext.
1</td><td>Spare</td><td>Spare</td><td>Spare</td><td>I</td><td>D</td><td>A</td><td>C/D
1</td><td>5</td></tr>
<tr><td colspan="8">Code</td><td>6</td></tr>
<tr><td colspan="8">Identifier</td><td>7</td></tr>
<tr><td colspan="8">Length
(2 octets)</td><td>8
9</td></tr>
<tr><td colspan="8">Type: Mode-1 (254)</td><td>10</td></tr>
<tr><td colspan="8">Length</td><td>11</td></tr>
<tr><td colspan="8">Version</td><td>12</td></tr>
<tr><td colspan="8">Parameter Elements</td><td>13
n</td></tr>
<tr><td colspan="8">FCS
(2 octets)</td><td>n+1
n+2</td></tr>
</table>

Figure 6/X.272 – E_Mode-1 Control Frame

Table 7/X.272 – E_Mode-1 Control Frame

Field	Description
DLCI, control and NLPID	See 8.1 for details
FRCP Header	• Ext.: extension bit = 1 • Spare: Spare bits for future use, set to 0 • ID field (2 bits) set to 11 • Authentication (A) bit = 0 • Control/Data (C/D) bit set to 1
Code	Decimal for 1 Config-Req; Decimal for 2 Config-Ack
Identifier	A transaction number to correlate a request with a response. Sent in request and echoed in corresponding response
Length (2 octets)	Including: Code, Identifier, Length and all Configuration Options
Type	254 (decimal) – indicate E_Mode-1. Types 245 to 253 inclusive and type 255 are reserved
Length	Varies depending on number of parameters
Version	Version number of the encryption FRCP set to 1
Parameter Elements	Zero or more of the E_Mode-1 parameter elements. See 10.1
FCS	Q.922 Frame Check Sequence

10.1.1.1 E_Mode-1 Parameter Elements

The Parameter Element ID identifies a parameter element. The length is the length of the whole parameter element including the Parameter Element ID field and the Length field. The Values field lists the individual parameter values of the element. The parameter elements must consist of an integral number of octets. These start after octet 12 of E_Mode-1 configuration option. See Figure 7.

Description	Octet
Parameter Element ID	a
Length	b
Parameter Element Values	c m

Figure 7/X.272 – E_Mode-1 General Parameter Element Structure

10.1.1.1.1 E_Mode-1 Initial Vector

The Data Encryption Standard (DES) CBC block cipher algorithms requires an Initialization Vector (IV) that is the same size as the block size. Inclusion of the initial vector parameter in the configure request (Config-Req) is mandatory. The presence of the initial vector parameter in the Config-Req indicates the 64-bit initial nonce the sending device will use for the cipher block chaining (CBC). The Config-Ack acknowledges receipt of the initial vector. The initial vector parameter is not sent in the Config-Ack. See Figure 8 and Table 8.

Initial Vector ID 0 0 0 0 0 0 0 1	1
Length: 10	2
Initial Nonce (8 octets)	3 10

Figure 8/X.272 – E_Mode-1 Initial Vector (Nonce) Parameter Element

Table 8/X.272 – E_Mode-1 Initial Vector (Nonce) Parameter

Field	Description
Initial Vector ID	Octet identifying the initial vector parameter
Length	10 (decimal)
Initial Nonce	64-bit quantity that is used by the peer device to encrypt the first packet transmitted. To guard against replay attacks the device should offer a different value during each negotiation

10.1.1.1.2 E_Mode-1 Key Exchange and Update

E_Mode-1 supports static encryption key. The key exchange and update procedures are beyond the scope of this Recommendation.

10.1.2 E_Mode-1 Data Transfer Format

The Data Encryption Standard (DES) algorithm operates on blocks of eight octets. This often requires padding after the end of the unencrypted user data. An octet (Pad Length) indicating the length of the padding must be added at the end of the user data. Hence, before the encryption process the length of the user data plus the Pad Length octet are computed. If the length in octets is not a multiple of 8, then extra octets are added as a pad to ensure that the total length aligns with an eight octets boundary. It is preferred that the padded octets be filled with random data. The number of padded octets can range from 0 to 255 to permit the hiding of actual data length. The number of added octets is specified in the Pad Length octet. This octet is the last octet in the frame. The whole frame including the user data, padded octets and the Pad Length octet is then encrypted. After the decryption process, the padded octets and the Pad Length octet is removed from the data and must be ignored.

The format of the FRCP frame for transmitting only ciphered data is given in Figure 9. See also Table 9

<table>
<tr><th colspan="8">Description</th><th>Octet</th></tr>
<tr><td colspan="8">Frame Relay address, control and NLPID information</td><td>1-4</td></tr>
<tr><td colspan="8">FRCP Header</td><td></td></tr>
<tr><td>Ext.
1</td><td>C/U</td><td>RA</td><td>RR</td><td>0</td><td>P</td><td>T</td><td>C/D
0</td><td>5</td></tr>
<tr><td colspan="8">Sequence Number</td><td>7</td></tr>
<tr><td colspan="8">User Data
(Note)</td><td>8
m</td></tr>
<tr><td colspan="8">Padding
(Note)</td><td>m
n-1</td></tr>
<tr><td colspan="8">Pad Length (Note)</td><td>n</td></tr>
<tr><td colspan="8">LCB</td><td>n+1</td></tr>
<tr><td colspan="8">FCS
(2 octets)</td><td>n+2
n+3</td></tr>
</table>

NOTE – This field is encrypted.

Figure 9/X.272 – E_Mode-1 Data Transfer Frame Format

Table 9/X.272 – E_Mode-1 Data Transfer Frame Format

Field	Description
DLCI, control and NLPID	See 8.1 for details
FRCP Header	The FRCP Protocol Header consists of the following: • Extension bit – Set to one, but included for future enhancement • Compressed/Uncompressed (C/U): Set to 1 to indicate that data is uncompressed • Reset_Ack (RA): Not applicable, set to 0 • Reset_Request (RR): Not applicable, set to 0 • Protocol option (OPT): Set to: O P T 0 0 1 to specify encryption • Control/Data (C/D) bit: Set to 0 to indicate a data frame
Sequence Number	Number assigned by the encryptor sequentially starting with 0 and incremented modulo 256
User Data	Encrypted user data
Padding	Bytes filled with random data preferably to ensure that the total length of user data and the Pad Length Byte aligns with an 8-octet boundary
Pad Length	Number of pad octets added to the length of user data plus 1 to ensure that the data aligns with an 8-octet boundary. This octet is the last octet in the frame
LCB	Longitudinal Check Byte – calculated on cleartext of octets 7 through n
FCS	Q.922 Frame Check Sequence

10.1.3 E_Mode-1 Control procedures

FRCP E_Mode-1 provides a simple negotiation protocol to enable privacy function with the default algorithm and parameter values. Once FRCP is enabled and successfully negotiated, data transfer to the peer end system must be encrypted. To disable FRCP, an implementation may force the virtual connection to the inactive state, or send an E_Mode-1 request and not send a E_Mode-1 response.

The negotiation of the encryption facility starts when the VC is established. The term V_0 is used to represent an inactive VC connection, while the term V_1 is used to indicate an active VC connection. The Initialization phase is entered upon frame relay virtual connection establishment provided that FRCP is configured by the user on the DTE. The operation phase is entered upon the successful completion of the Initialization phase. In the operation phase, the term f_1 is used to represent the successful negotiation of a facility, and the term f_0 is used to indicate the failure of negotiation of the facility. Thus, unsuccessful completion of the Initialization phase causes FRCP to enter the f_0 phase. FRCP data PDUs are transferred only when E_Mode-1 is in the f_1 phase. FRCP control PDUs may be transferred in any phase.

10.1.3.1 E_Mode-1 States

The FRCP E_Mode-1 states which may exist on either side of the frame relay connection are:

Disabled (f_0)

FRCP facility does not exist (when a VC goes V_0 from to V_1 and/or negotiation fails).

Request Initiated (I_1)

An E_Mode-1 configuration request message has been sent to the peer. Awaiting response to own request and peer configure request.

Request Received (I_3)

An E_Mode-1 configuration request message has been received from the peer. Configure response to peer request message and a configure request (Config-Req) are sent to the peer. Awaiting response to own request.

Awaiting Request (I_2)

Received configure repose to own request and waiting for the peer configure request.

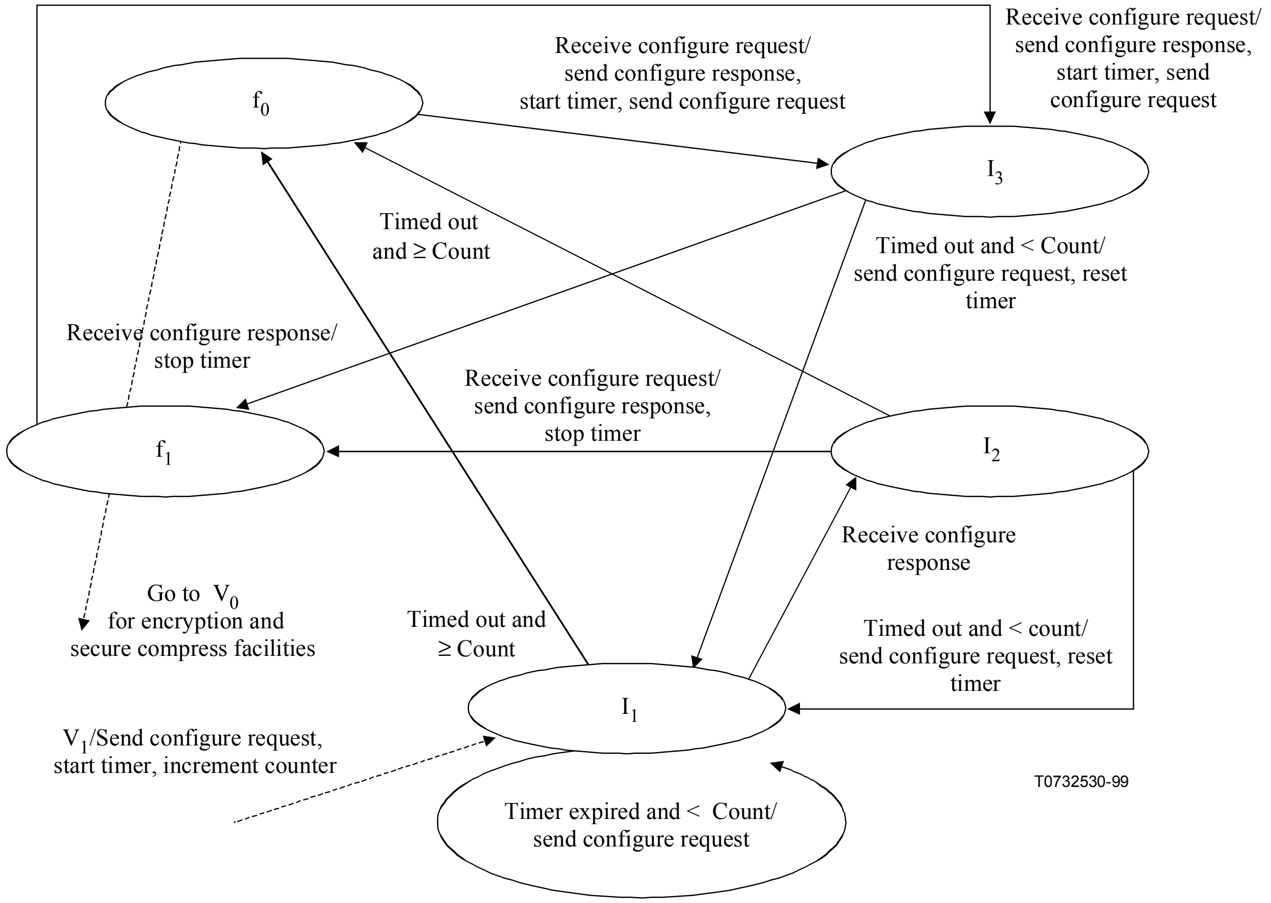
Operational (f_1)

E_Mode-1 negotiation completed and is successful.

In order to ensure the completion of the negotiation process whether successful or not a handshake completion timer and a maximum retry counter are defined. The handshake completion timer includes the time that it takes to perform the handshake process of negotiation. The maximum retry counter specifies the number of times the negotiation process is attempted by a device. For Mode-1 negotiation of any of the facilities in this Recommendation, the preferred default values are provided below:

Parameter	Default Value
Handshake Completion Timer	3 seconds
Maximum Counter	10 in decimal

The state diagram for performing the E_Mode-1 negotiation is given in Figure 10.



Receive configure request/
send configure response,
start timer, send configure request
Receive configure request/
send configure response,
start timer, send
configure request
f_0
I_3
Timed out
and ≥ Count
Timed out and < Count/
send configure request, reset
timer
Receive configure response/
stop timer
Receive configure request/
send configure response,
stop timer
f_1
I_2
Receive configure
response
Go to V_0
for encryption and
secure compress facilities
Timed out and
≥ Count
Timed out and < count/
send configure request, reset
timer
I_1
V_1/Send configure request,
start timer, increment counter
Timer expired and < Count/
send configure request
T0732530-99

Figure 10/X.272 – E_Mode-1 State Diagram

10.1.3.2 Initialization Request

The E_Mode-1 Initialization will start when a frame relay virtual connection to a peer is established and FR privacy function is administratively enabled (by the user). FRCP negotiation procedures are initiated, by sending a Config-Req message to the peer; start a handshake completion timer and enter *Request Initiated (I_1)* state.

Upon receiving a configure response message, the entity shall enter *Awaiting Request (I_2)* state. When a Config-Req is received from the peer, the following procedures apply:

1) For calls in *Request Initiated (I_1)* state, send a configure response message; enter *Request Received (I_3)* State.

2) For calls in *Awaiting Request (I_2)* state, send a configure response message; Stop handshake completion timer; send a configure response primitive that the negotiation is complete; enter operational f_1 state.

If the handshake completion timer expires before the handshake procedure is completed and the number of retries are less than the maximum retry counter, the following procedures apply:

1) For calls in *Request Initiated (I_1)* state, send a Config-Req message to the peer; restart a handshake completion timer, and increment the number of Config-Req messages that has been sent to the peer .

2) For calls in *Awaiting Request (I_2)* state, send a Config-Req message to the peer; restart a handshake completion timer; and enter *Request Initiated (I_1)* state.

10.1.3.3 Receipt of a Configuration Request

Upon receipt of a configuration request from the peer in f_0 state, send a configure response message; send a message; start a handshake completion timer; increment the number of Config-Req messages that has been sent to the peer and enter *Request Received (I_3)* state.

Upon receiving a configure response message in the *Request Received (I_3)* state, stop the handshake completion timer; enter operational f_1 state.

If the handshake completion timer expires before the handshake procedure is completed and the number of retries are less than the count, send a Config-Req message; restart the handshake completion timer.

10.1.3.4 Operational Phase

When a Config-Req message is received from the peer, for calls in the *operational* f_1 state, send a configure response message; sending a Config-Req message; restart the handshake completion timer and enter *Request Received (I_3)* state.

10.1.3.5 Disable Phase

The E_Mode-1 disabled phase f_0 shall be entered when a frame relay virtual connection to a peer is released (transition from V_1 to V_0) or when the negotiation has failed. If maximum retry counter is exceeded on a handshake completion timer expiry, return to the f_0 phase. If the negotiation fails to reach the f_1 phase the VC must be released.

10.1.4 E_Mode-1 User Data Encryption

Once the negotiation between the encryption peers is completed and both peers are in the operational state, frames are encrypted using the procedures in this clause.

The E_Mode-1 encryption method used to create the ciphertext is the Data Encryption Standard (DES) with Cipher Block Chaining (CBC) mode, 56-bit key. The initial vector for the CBC mode is deduced from the explicit 64-bit nonce, exchanged during E_Mode-1 negotiation. If no Nonce is exchanged by the peers, it must be coordinated and configured in the respective peers of the virtual connection. The encryption CBC extends beyond each payload to the next. A sequence number is used to detect when a received frame is out of order.

When data is to be sent, the data is padded to the next multiple of 8 octets as described in 10.1.2 to form a cipher payload. The LCB is calculated on the cipher payload. The encryptor ciphers the cipher payload and the result is positioned into the frame as in Figure 9. The sender increments the sequence number modulo 256. The sender then appends the LCB onto the payload and sends the frame on the link.

The receiver first checks the sequence number to determine if a frame was lost. If a frame was lost, the last 8 octets of the ciphertext are kept as the initial vector for the next frame and the received frame is discarded. If the frame is in sequence, the receiver deciphers the fields identified in Figure 9 and calculates the LCB. The calculated LCB, is compared to the received LCB. If they do not match the last 8 octets of the data are kept as the initial vector for the next frame and the received frame is discarded. If the LCBs match, the deciphered data is then processed by removing the padding.

10.2 E_Mode-2 Specification

E_Mode-2 encryption support consists of the full negotiation procedures of IETF RFC 1968. These procedures allow two peer frame relay devices to negotiate and converge on encryption methods and parameters to be used between them on a virtual connection. In general the control formats and procedures of IETF RFC 1968 [14] are used, whereby, different encryption methods may be negotiated in each direction of the virtual connection.

10.2.1 E_Mode-2 Control Frame Formats

This frame is used to negotiate Mode-2 parameters. See Figure 11 and Table 10.

<table>
<tr><th colspan="8">Description</th><th>Octet</th></tr>
<tr><td colspan="8">Frame Relay address, control and NLPID information</td><td>1-4</td></tr>
<tr><td colspan="8">FRCP Header</td><td></td></tr>
<tr><td>Ext.
1</td><td>Spare</td><td>Spare</td><td>Spare</td><td>I</td><td>D</td><td>A
0</td><td>C/D
1</td><td>5</td></tr>
<tr><td colspan="8">Code</td><td>6</td></tr>
<tr><td colspan="8">Identifier</td><td>7</td></tr>
<tr><td colspan="8">Length
(2 octets)</td><td>8
9</td></tr>
<tr><td colspan="8">Type</td><td>10</td></tr>
<tr><td colspan="8">Length</td><td>11</td></tr>
<tr><td colspan="8">Values</td><td>12
n</td></tr>
<tr><td colspan="8">FCS
(2 octets)</td><td>n+1
n+2</td></tr>
</table>

Figure 11/X.272 – E_Mode-2 FRCP Control Frame

Table 10/X.272 – E_Mode-2 Control Frame

Field	Description
DLCI, control and NLPID	See 8.1 for details
FRCP Header	• Ext.: Extension bit set to 1 • Spare: Spare bits set to 0 • ID (2 bits) set to 11 • Authentication (A) bit = 0 • Control/Data (C/D) bit set to 1
Code	See IETF RFC 1661 section 5 LCP Packet Formats and IETF RFC 1968 section 3 Additional Packets (Values given in decimal)
Identifier	See IETF RFC 1661 section 5 LCP Packet Formats and IETF RFC 1968 section 3 Additional Packets
Length (2 octets)	See IETF RFC 1661 section 5 LCP Packet Formats and IETF RFC 1968 section 3 Additional Packets Including: Code, Identifier, Length and all Configuration Options data
Type	See IETF RFC 1968 section 4 ECP Configuration Options, 4.1 Proprietary Encryption OUI and 4.2 Publicly Available Encryption Types. In this Recommendation type 254 (decimal) is reserved and indicates FRCP E_Mode-1. Furthermore, types 245 to 253 inclusive and type 255 are reserved.
Length	Length of Configuration option including Type, Length and Values fields
Values	Zero or more octets, containing data as determined by the configuration options defined in IETF RFC 1968 section 4
FCS	Q.922 Frame Check Sequence

10.2.2 E_Mode-2 Negotiation

E_Mode-2 of Frame Relay Privacy Protocol encapsulates the same packet exchange mechanism as the PPP Encryption Control Protocol (IETF RFC 1968) [14] which is in turn modelled on the PPP Link Control Protocol (LCP) (IETF RFC 1661) [13]. E_Mode-2 shall use the procedures described in sections 3.1 and 4.3 of IETF RFC 1968 using the frame formats described in 8.2. The following exceptions apply to sections 3.1 and 4.3 of IETF RFC 1968 [14] and referenced section 4 of IETF RFC 1661:

- If at any time E_Mode-1 Config-Req is received the receiving device will begin E_Mode-1 negotiation.
- An entity may abandon E_Mode-2 and enter E_Mode-1 initialization phase at any time.
- If an entity that supports E_Mode-2 is currently in E_Mode-1 and receives E_Mode-2 Configure Request, it may begin E_Mode-2 negotiation.

NOTE – The (lower layer) Up/Down events for the automaton should be generated by the virtual connection status given by the PVC and SVC signalling protocols. E_Mode-2 packets received before this phase should be ignored. Before any encrypted data is exchanged, the entity must reach the f_1 state.

10.2.3 E_Mode-2 Data Transfer

This format used for transferring ciphered data in E_Mode-2 is similar to E_Mode-1 and is given in Figure 9 and described in Table 9.

11 Data Compression Facilities

The data compression facility is responsible for enabling and initiating data compression algorithms on both ends of the link. Data compression uses a similar packet exchange mechanism as the PPP Link Control Protocol (LCP) [13]. The use of the data compression facility is negotiated between peer devices. The mode and algorithms are selected independently for each direction of a virtual connection. The FRCP control protocol provides the following services for data compression:

– Encapsulation of encoded user data and negotiation primitives within FRCP protocol data units (PDUs) for transport between FRCP peers.

– Negotiation of FRCP configuration options.

– Synchronization of the sender and receiver peers, including:
  - Detection of loss of synchronization and signalling for resynchronization between peers.
  - Anti-expansion protection that enables the signalling of compressed/uncompressed mode from the encoder to the peer decoder.
  - Encoding of user data into compressed user data according to one or more of a variety of public or proprietary algorithms.
  - Decoding of compressed user data into uncompressed user data.

This Recommendation supports the negotiation of optional public or proprietary data compression algorithms. The details of proprietary algorithms must be published by the vendors in data compression function description (DCFD) documents. The DCFD, in combination with this Recommendation, are sufficient to assure interoperability of FRCP among manufacturers.

11.1 C_Mode-1 Data Compression Encapsulation

For implementations that include the data compression facility, the support of C_Mode-1 is mandatory. The C_Mode-1 consists of a simple handshake to enable the default data compression algorithm and its parameters for both directions of the VC. The default data compression algorithm is LZS as described in [20].

11.1.1 C_Mode-1 Control Frame Formats

This frame is used to negotiate C_Mode-1 parameters. See Figure 12 and Table 11.

<table>
<tr><th colspan="8">Description</th><th>Octet</th></tr>
<tr><td colspan="8">Q.922 Address
(2 octets) (Note)</td><td>1
2</td></tr>
<tr><td colspan="8">Control
(UI: 0x03)</td><td>3</td></tr>
<tr><td colspan="8">NLPID
(0xB0)</td><td>4</td></tr>
<tr><td colspan="8">FRCP Header</td><td></td></tr>
<tr><td>Ext.
1</td><td>Spare</td><td>Spare</td><td>Spare</td><td>I</td><td>D</td><td>A</td><td>C/D
1</td><td>5</td></tr>
<tr><td colspan="8">Code</td><td>6</td></tr>
<tr><td colspan="8">Identifier</td><td>7</td></tr>
<tr><td colspan="8">Length
(2 octets)</td><td>8
9</td></tr>
<tr><td colspan="8">Type</td><td>10</td></tr>
<tr><td colspan="8">Configuration Option Length</td><td>11</td></tr>
<tr><td colspan="8">Revision</td><td>12</td></tr>
<tr><td colspan="8">FCS
(2 octets)</td><td>13
14</td></tr>
</table>

NOTE – The 2 octets frame relay address is shown here for illustrative purposes. The 3-and 4-octet address formats are not prohibited.

Figure 12/X.272 – C_Mode-1 Control Frame

Table 11/X.272 – C_Mode-1 Control Frame

Field	Description
Q.922 Address	See 8.1 for details
Control	See 8.1 for details
NLPID	See 8.1 for details
FRCP Header	The FRCP Protocol Header consists of the following: • Ext.: Extension bit must be set to one • Spare: Spare bits for future use set to 0 • ID (2 bits) set to 01 • Authentication (A) bit – Set to 0 • Control/Data (C/D) bit – Set to 1
Code	Set to 1 for configure request (Config-Req) Set to 2 for configure acknowledge (Config_Ack)
Identifier	A transaction number to correlate a request with a response. Sent in request and echoed in corresponding response
Length	Two octets in length. The value is set to 7, which consists of the total number of octets of the frame excluding: Q.922 Address, Control, NLPID, and FRCP Header
Type	254 decimal – indicates C_Mode-1 Types 245 to 253 inclusive and type 255 are reserved
Configuration Option Length	Set to decimal 3 to indicate the length of the Type, Configuration Option Length and Revision fields

Table 11/X.272 – C_Mode-1 Control Frame (*concluded*)

Field	Description
Revision	Current revision must be set to 1
FRCP Payload	Control information or transfer data depending on how the FRCP Header bits are set
FCS	Q.922 Frame Check Sequence

11.1.2 C_Mode-1 Control procedures

FRCP data compression C_Mode-1 provides a simple negotiation protocol to enable data compression service with the default algorithm and parameter values. Once FRCP is successfully negotiated, data transfer to the peer end system may be compressed. To disable FRCP, an implementation may force the virtual connection to the inactive state, or send a C_Mode-1 request and not send a C_Mode-1 response.

11.1.2.1 C_Mode-1 States

Same as 10.1.3.1.

11.1.2.2 C_Mode-1 Initialization Request

Same as 10.1.3.2.

11.1.2.3 Receipt of a Configuration Request

Same as 10.1.3.3.

11.1.2.4 Operational Phase

Same as 10.1.3.4.

11.1.2.5 Disable Phase

Same as 10.1.3.5.

11.1.3 C_Mode-1 Data Transfer Formats

This clause describes the encapsulation method for the FRCP data compression when only the data compression option is enabled. Furthermore, this clause will also describe the anti-expansion and synchronization procedures.

The general frame format is depicted in Figure 13. In the figure, the C/D bit in the FRCP header is set to 0 to indicate that the frame is a data frame. The C/U, RA and RR bits are used for the anti-expansion and synchronization procedures.

11.1.3.1 Anti-expansion Signalling Format

Anti-expansion signalling (C/U) may be provided from the encoder to the decoder in one direction of the FRCP data compression connection to indicate if the associated FRCP Payload is compressed or not. The sender must set C/U = 1 when the compression encoding has been performed on the user data. The sender must set C/U = 0 when the compression encoding has not been performed on the user data. When C/U = 1, the decoder must decode the FRCP Payload. When C/U = 0, the decoder must not decode the FRCP Payload. There shall be no Sequence Number field or LCB field when the C/D bit is set to "0".

The current revision implementation of C-Mode-1 requires that the encoder compress every frame of data even if data expansion has occurred. The LZS algorithm provides minimum expansion on data, the details of LZS expansion are found in [20]. The implementation of C-Mode-1 requires that the connection be set to handle a maximum frame size that includes the worst-case scenario of the expansion of the data.

11.1.3.2 Synchronization Signalling Format

The FRCP provides synchronization procedures to recover from a loss of synchronization between FRCP peers. Frame relay does not assure reliable transport of FRCP PDUs. FRCP function decoders commonly do not recover from decompressing dropped, erroneous, or miss-ordered PDUs and propagate errors catastrophically until they are reset to a known state. In this Recommendation, the sequence number and LCB are used to detect the loss of synchronization. Synchronization signalling is provided between FRCP peers via the RR and RA bits in the FRCP data PDU Header. The RR and RA may be signalled in an FRCP Header that accompanies a FRCP Payload; they may also be signalled via a FRCP Header without an attached FRCP Payload, see Figure 14. Separate RR and RA signals are provided to allow independent resynchronization of either or both directions of a FRCP connection.

The decoder determines the loss of synchronization when it receives a frame with a wrong sequence number and/or a wrong LCB. If the decoder detects a loss of synchronization in the remote-to-local direction of the FRCP connection, it must generate an RR signal that is set to "1", on a new empty FRCP data PDU or on the next FRCP data PDU containing user data destined for the remote FRCP peer. Once an RR set to "1" has been generated, any FRCP data PDUs received in the remote-to-local direction of that FRCP context that contain compressed user data (C/U=1) must be discarded until an RA set to "1" is received for that context. The RR signal that is set to "1" may be repeated to increase reliability. If a receiver detects an RR set to "1" in the remote-to-local direction, it shall reset its encoder to a known state. The encoder must generate an RA signal set to "1" on a new empty FRCP data PDU or on the next FRCP data PDU containing user data destined for the local FRCP peer. When a local FRCP receiver receives an RA signal set to "1" in the remote-to-local direction of the FRCP context, it must reset its history for that context to a known state. The local FRCP receiver must decode any user data in the FRCP data PDU containing the RA set to "1" and all subsequent FRCP data PDUs until another loss of synchronization is detected.

The C/U bit must be set to "0" in FRCP synchronization frames (when the RR or RA bits are set). Furthermore, any FRCP synchronization frame must contain a valid sequence number. Upon detection of a set RA bit, the decoder must reset its current sequence number to the one received from the synchronization frame. Thus, the next expected sequence number can be derived modulo 256 from the received sequence number.

To ensure initial synchronization between two peers upon the successful negotiation of C_Mode-1 between two peers, the encoder must set the RA bit to "1" on the first PDU to indicate that the history is in a known state. The decoder must ignore all compressed frames until it gets such a frame. To increase reliability, the decoder must initiate a reset request to the remote encoder.

11.1.3.3 C_Mode-1 Data Compression Payload

The contents of the FRCP Payload must be an integer number of octets. The format of the FRCP payload is given below, see Figure 13 and Table 12:

Q.922 Address, Control and NLPID								1-4
FRCP Header								
Ext. 1	C/U	RA	RR	O	P	T	C/D 0	5
Sequence Number								6
FRCP Data Compression Payload								7 n
LCB								n+1
FCS (2 octets)								n+2 n+3

Figure 13/X.272 – C_Mode-1 Data Transfer Frame

Table 12/X.272 – C_Mode-1 Data Frame

Field	Description
Q.922 Address	See 8.1 for details
Control	See 8.1 for details
NLPID	See 8.1 for details
Sequence Number	Initialized to 1 and incremented after each frame Modulo 256 NOTE 1 – This octet is appended at the end of the compressed payload. This octet must not be compressed
FRCP Header	The FRCP Protocol Header consists of the following: • Ext.: Extension bit must be set to one, but included for future enhancement • Compressed/Uncompressed (C/U): Set to 1 to indicate that data is uncompressed • Reset_Ack (RA): Not applicable, set to 0 • Reset_Request (RR): Not applicable, set to 0 • Protocol option (OPT): Set to: O P T 0 1 1 to specify compression • Control/Data (C/D) bit: Set to 0 to indicate a data frame
Data Compression Payload	Q.933 Annex E frame that it compressed
Sequence Number	Initialized to 1 and incremented after each frame Modulo 256 NOTE 2 – This octet is appended at the end of the compressed payload. This octet must not be compressed
LCB	LCB computed on the original user data including the sequence number. The LCB is not compressed
FCS	Q.922 Frame Check Sequence

The contents of an empty PDU are depicted in Figure 14:

<table>
<tr><td colspan="8">Q.922 Address, Control and NLPID</td><td>1-4</td></tr>
<tr><td colspan="8">FRCP Header</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">Sequence Number</td><td>6</td></tr>
<tr><td colspan="8">FCS
(2 octets)</td><td>7
8</td></tr>
</table>

Figure 14/X.272 – Empty FRCP PDU

11.2 C_Mode-2 Data COMPRESSION ENCAPSULATION

The support of C_Mode-2 is optional. This data compression operational mode provides the capability to negotiate DCFDs and their associated parameters.

11.2.1 C_Mode-2 Control Frame Formats

This frame is used to negotiate C_Mode-2 parameters. See Figure 15 and Table 13.

<table>
<tr><th colspan="8">Description</th><th>Octet</th></tr>
<tr><td colspan="8">Q.922 Address
(2 octets) (Note)</td><td>1
2</td></tr>
<tr><td colspan="8">Control
(UI: 0x03)</td><td>3</td></tr>
<tr><td colspan="8">NLPID
(0xB0)</td><td>4</td></tr>
<tr><td colspan="8">FRCP Header</td><td></td></tr>
<tr><td>Ext.
1</td><td>Spare</td><td>Spare</td><td>Spare</td><td>I</td><td>D</td><td>A</td><td>C/D
1</td><td>5</td></tr>
<tr><td colspan="8">Code</td><td>6</td></tr>
<tr><td colspan="8">Identifier</td><td>7</td></tr>
<tr><td colspan="8">Length
(2 octets)</td><td>8
9</td></tr>
<tr><td colspan="8">Type</td><td>10</td></tr>
<tr><td colspan="8">Configuration Option Length</td><td>11</td></tr>
<tr><td colspan="8">OUI
(3 octets)</td><td>12
13
14</td></tr>
<tr><td colspan="8">Subtype</td><td>15</td></tr>
<tr><td colspan="8">Values</td><td>16</td></tr>
<tr><td colspan="8">FCS
(2 octets)</td><td>17
18</td></tr>
</table>

NOTE – The 2-octet frame relay address is shown here for illustrative purposes. The 3-and 4-octet address formats are not prohibited.

Figure 15/X.272 – C_Mode-2 Control Frame

Table 13/X.272 – C_Mode-2 Control Frame

Field	Description
Q.922 Address	See 8.1 for details
Control	See 8.1 for details
NLPID	See 8.1 for details
FRCP Header	The FRCP Protocol Header consists of the following: • Ext.: Extension bit must be set to one • Spare: Spare bit for future use set to 0 • ID (2 bits) set to 01 • Authentication (A) bit – Set to 0 • Control/Data (C/D) bit – Set to 1
Code	Set to 1 for Config_Req Set to 2 for Config_Ack
Identifier	A transaction number to correlate a request with a response. Sent in request and echoed in corresponding response
Length	Two octets in length. The value is set to 7, which consists of the total number of octets of the frame excluding: Q.922 Address, Control, NLPID, and FRCP Header
Type	0 C_Mode-2 23 LZS 254 FRCP C_Mode-1 Types 245 to 253 inclusive and type 255 are reserved Numbers are in decimal
Configuration Option Length	Set to 6 plus the number of octets in the Values field
OUI	Vender's Organization Unique Identifier
Subtype	Used to select between multiple DCFDs from a specific vender
Values	Shall be zero or more Octets. Can contain additional data for each vendor protocol, and may include the option of using multiple histories per connection
FCS	Q.922 Frame Check Sequence

11.2.2 C_Mode-2 Control Message

The FRCP C_Mode-2 allows the negotiation of vendor specific DCFD. The negotiation is based on the LCP packet formats defined in section 5 of IETF RFC 1661 [13], with a unique set of Configurations options. The LCP packets with codes 1 through 7 are required. The other LCP packets specified in IETF RFC 1661 are optional.

The FRCP Configuration Option code points that are currently assigned are described below:

Configuration Option

23	LZS
254	FRCP C_Mode-1
255	Reserved for future use

C_Mode-2 shall use the finite-state automaton described in sections 3 and 4 of IETF RFC 1661 [13] with the following exceptions:

1) If the C_Mode-2 negotiate FRCP finite-state automaton enters the f_0 because of negotiation time out and/or exceeding the value of a counter, the entity shall enter the C_Mode-1 Initialization phase.
2) An entity may abandon C_Mode-2 and enter the C_Mode-1 initialization phase at any time.
3) If an entity operating in C_Mode-2 receives a C_Mode-1 Request at any time, it shall enter the C-Mode-1 Initialization phase.
4) If an entity that supports C_Mode-2 is currently in C_Mode-1 and it receives a C_Mode-2 Configure-Request, it may begin C_Mode-2 negotiation.

Before any FRCP data PDUs may be communicated, FRCP must reach the f_1 state.

12 Secure Data Compression Facilities

The secure data compression facility is responsible for enabling and initiating secure data compression algorithms on both ends of the link. Secure data compression uses a similar packet exchange mechanism as the PPP Link Control Protocol (LCP). The use of the secure data compression facility is negotiated between peer devices. The mode and algorithms are selected independently for each direction of a virtual connection. The FRCP supports data compression function description (DCFD) that are defined by separate documents that, in combination with this Recommendation, is sufficient to assure interoperability of FRCP among manufacturers providing the same FRCP Function. The FRCP provides support for loss-of-synchronization detection and resynchronization procedures.

12.1 S_Mode-1 Data Compression Encapsulation

The support of S_Mode-1 is mandatory for user configurations that have the secure data compression facility enabled. The negotiation of S_Mode-1 consists of a simple handshake to enable the default data secure compression algorithm (SCA) and its associated parameters for either direction of the VC.

The default data compression algorithm is FZA as described in [17]. The FZA algorithm uses a stream cipher to randomly update its internal data compression model. The use of stream cipher requires an encryption key or an initial seed to derive the key. The key exchange and update procedure are beyond the scope of this Recommendation. Furthermore, like traditional data compression algorithms, FZA requires that dictionaries of the sender and receiver to remain synchronized. The FZA will encrypt the data if the secure compression option is turned off.

12.1.1 S_Mode-1 Control Frame Formats

The frames used to negotiate S_Mode-1 parameters is similar to the format given in Figure 6 with the Ext. and C/D bits in the FRCP Header octet set to 1. The value of ID field in the FRCP Header must be set to 10. The value of the Type field in the frame is set to decimal 254.

12.1.2 S_Mode-1 Control procedures

Same as 10.1.1.

12.1.2.1 S_Mode-1 Parameter Elements

Same as 10.1.1.1.

12.2 S_Mode-1 Data Transfer Format

This clause describes the encapsulation method for the FRCP secure data compression as the only configured facility. Furthermore, this clause will also describe the anti-expansion and synchronization procedures. The general frame format is depicted in Figure 16. In the figure, the C/D bit in the FRCP header is set to 0 to indicate that the frame is a data frame. The C/U, RA and RR bits are used for the anti-expansion and synchronization procedures.

12.2.1 Anti-expansion Signalling Format

Anti-expansion signalling (C/U) should be provided from the encoder to the decoder in one direction of the FRCP data compression connection to indicate if the associated FRCP payload is secure compressed or not. The sender must set C/U = "1" when the secure compression encoding has been performed on the user data. When C/U = "1", the decoder must decode the FRCP secure compress payload.

The sender can set C/U = "0" when the secure compression encoding has not been performed on the user data. However, the data must be encrypted using FZA encryption mode before sending it on the link. Otherwise, the data must always be securely compressed before sending it on the link even if data expansion has occurred. When C/U = 0, the secure decoder must decrypt the encrypted FRCP payload using FZA encryption mode. The sequence number field must be encrypted and included in the FRCP PDU. Furthermore, the LCB field must be present.

12.2.1.1 Synchronization Signalling Format

Same as 11.1.3.2.

12.2.1.2 S_Mode-1 FRCP Data Payload

The contents of the FRCP Payload are defined according to the DCFD. The FRCP Payload must be an integer number of octets. See Figure 16 and Table 14.

Q.922 Address, Control and NLPID								1-4
FRCP Header								
Ext. 1	C/U	RA	RR	O	P	T	C/D 0	5
FRCP Secure Data Compression Payload								6
Sequence Number								n
LCB								n+1
FCS (2 octets)								n+2 n+3

Figure 16/X.272 – S_Mode-1 Data Transfer Frame

Table 14/X.272 – S_Mode-1 Data Frame

Field	Description
Q.922 Address	See 8.1 for details
Control	See 8.1 for details
NLPID	See 8.1 for details
FRCP Header	The FRCP Protocol Header consists of the following: • Ext.: Extension bit must be set to one • Compressed/Uncompressed (C/U) • Reset_Ack (RA) • Reset_Request (RR) • Protocol option (OPT): Set to: O P T 0 1 0 to specify secure compression • Control/Data (C/D) bit: Set to 0 to indicate a data frame
Data Compression Payload	Q.933 Annex E frame that it compressed
Sequence Number	Initialized to 1 and incremented after each frame Modulo 256 NOTE – This octet is appended to the user data and is secure compressed
LCB	LCB computed on the original user data including the sequence number
FCS	Q.922 Frame Check Sequence

12.3 S_Mode-2 Data Compression Encapsulation

S_Mode-2 support is optional and provides the capability to enable or disable FRCP, to negotiate DCFDs and their associated parameters.

12.3.1 S_Mode-2 Control Frame Formats

This frame is used to negotiate S_Mode-2 parameters. See Figure 17 ans Table 15.

<table>
<tr><th colspan="8">Description</th><th>Octet</th></tr>
<tr><td colspan="8">Q.922 Address
(2 octets) (Note)</td><td>1
2</td></tr>
<tr><td colspan="8">Control
(UI: 0x03)</td><td>3</td></tr>
<tr><td colspan="8">NLPID
(0xB0)</td><td>4</td></tr>
<tr><td colspan="8">FRCP Header</td><td></td></tr>
<tr><td>Ext.
1</td><td>Spare</td><td>Spare</td><td>Spare</td><td>I</td><td>D</td><td>A</td><td>C/D
1</td><td>5</td></tr>
<tr><td colspan="8">Code</td><td>6</td></tr>
<tr><td colspan="8">Identifier</td><td>7</td></tr>
<tr><td colspan="8">Length
(2 octets)</td><td>8
9</td></tr>
<tr><td colspan="8">Type</td><td>10</td></tr>
<tr><td colspan="8">Configuration Option Length</td><td>11</td></tr>
<tr><td colspan="8">OUI
(3 octets)</td><td>12
13
14</td></tr>
<tr><td colspan="8">Subtype</td><td>15</td></tr>
<tr><td colspan="8">Values</td><td>16</td></tr>
<tr><td colspan="8">FCS
(2 octets)</td><td>17
18</td></tr>
</table>

NOTE – The 2-octet frame relay address is shown here for illustrative purposes. The 3-and 4-octet address formats are not prohibited.

Figure 17/X.272 – S_Mode-2 Control Frame

Table 15/X.272 – S_Mode-2 Control Frame

Field	Description
Q.922 Address	See 8.1 for details
Control	See 8.1 for details
NLPID	See 8.1 for details
FRCP Header	The FRCP Protocol Header consists of the following: • Ext.: Extension bit must be set to one • Spare: Spare bits must be set to 0 • ID (2 bits) set to "10" • Authentication (A) bit – Set to 0 • Control/Data (C/D) bit – Set to 1
Code	Set to 1 for Config_Req Set to 2 for Config_Ack
Identifier	A transaction number to correlate a request with a response. Sent in request and echoed in corresponding response
Length	Two octets in length. The value is set to 7, which consists of the total number of octets of the frame excluding: Q.922 Address, Control, NLPID, and FRCP Header
Type	0 S_Mode-2 254 FRCP S_Mode-1 Types 245 to 253 inclusive and type 255 are reserved Numbers in decimal

Table 15/X.272 – S_Mode-2 Control Frame *(concluded)*

Field	Description
Configuration Option Length	Set to 6 plus the number of octets in the Values field
OUI	Vender's Organization Unique Identifier
Subtype	Used to select between multiple proprietary DCFDs from a specific vendor
Values	Shall be zero or more Octets. Can contain additional data for each vendor protocol, and may include the option of using multiple histories per connection
FCS	Q.922 Frame Check Sequence

12.3.2 S_Mode-2 Control Message

FRCP S_Mode-2 allows the negotiation of vendor specific DCFD. The negotiation is based on the LCP packet formats defined in section 5 of IETF RFC 1661 [13]. The details are similar to E_Mode-2 specifications as given in 10.2.

S_Mode-2 shall use the finite-state automaton described in sections 3 and 4 of IETF RFC 1661 [13] with the following exceptions:

1) If the S_Mode-2 negotiate FRCP finite-state automaton enters the f_0 because of negotiation time out and/or exceeding the value of a counter, the entity shall enter the S_Mode-1 Initialization phase.
2) An entity may abandon S_Mode-2 and enter the S_Mode-1 initialization phase at any time.
3) If an entity operating in S_Mode-2 receives an S_Mode-1 Request at any time, it shall enter the S_Mode-1 Initialization phase.
4) If an entity that supports S_Mode-2 is currently in S_Mode-1 and it receives a S_Mode-2 Config-Req, it may begin S_Mode-2 negotiation.

13 Multi-facility FRCP Data Transfer Encapsulation

This clause describes the format of FRCP data frames when multiple facilities are configured and successfully negotiated.

13.1 Encryption and Secure Data Compression Data

This clause discusses the encapsulation of frames that include the use of the secure compression and encryption facilities. The algorithms that are used are those that are adopted for E-Mode-1 and S-Mode-1 modes of operation. The handling of the Initialization Vector (IV) for E-Mode-1 is as described in 10.1.1.1.

For implementations that have the encryption and secure compression options configured and successfully negotiated, the user data is secure compressed first using the default SCA of S-Mode-1. An LCB must be computed on the original raw user data. The LCB is appended at the end of the secure compressed data as shown below:

Description	Octet
Secure Compressed User Data	1 k
LCB Computed on the original raw user data	k+1

The compressed data and the LCB (k + 1 Bytes) are then treated as the new user data that must be ciphered by the encryptor. The encryptor must pad the data to the next multiple of 8 octets as described in 10.1.2 before ciphering it. An LCB is computed on the (k + 1 octets) secure compressed data and LCB, the pad octets and the Pad Length octet before the encryption step. The data is then encrypted and a sequence number is computed to be inserted in the frame as described in Figure 18. The sender increments the sequence number modulo 256. The sender then appends the LCB onto the payload and sends the frame on the link.

At the receiving end, the receiver first checks the sequence number to determine if a frame was lost. If a frame was lost, the last 8 octets of the ciphertext are kept as the initial vector for the next frame and the received frame is discarded. A reset request must be sent to the sending peer requesting that the secure compression history be reset. This is achieved by setting the RR and RA bits as described in the related clauses. No data must be provided from the decryptor to the decoder until a reset acknowledgement is received from the sending peer.

If the frame is in sequence, the receiver deciphers the fields identified in Figure 9 and calculates the LCB. The calculated LCB is compared to the received LCB. If they do not match, the last 8 octets of the data are kept as the initial vector for the next frame and the received frame is discarded. A reset request must be sent to the sending peer requesting that the secure compression history be reset. This is achieved by setting the RR and RA bits as described in the related clauses. No data must be provided from the decryptor to the decoder until a reset acknowledgement is received from the sending peer. If the LCBs match, the deciphered data is then processed by removing the sequence number, padding, Pad Length octet and LCB. The data is then forwarded to the decoder, where a secure decompression step is performed. The decoder computes the LCB on the uncompressed data. If the LCB matches the decoder forward the data to the upper layer. In the event of no LCB match, a reset request must be sent to the sending peer requesting that the secure compression history be reset. This is achieved by setting the RR and RA bits as described in the related clauses. No data must be provided from the decryptor to the decoder until a reset acknowledgement is received from the sending peer.

During the time that the decryptor is awaiting the receipt of a reset acknowledgement from the sender to indicate the that the histories are synchronized, the decryptor must keep the last 8 octets of the ciphertext as the initial vector for the next frame and the received frame is discarded.

When the secure compression option is combined with the encryption option, the data must always be passed through the secure compressor and the encryptor. This is because FZA will encrypt the data if the compression option is tuned off. Hence, regardless of the value of the C/U bit in the FRCP Header, the decryptor must provide the data to the secure decoder for frames with correct sequence number and LCB. See also Table 16.

Description								Octet
Frame Relay address, control and NLPID information								1-4
FRCP Header								
Ext. 1	Reserved	Reserved	Reserved	I	D	A	C/D 0	5
Sequence Number								6
Secure Compressed User Data (Note) (k+1 Bytes)								7 m
Padding (Note)								m n-1
Pad Length (Note)								n
LCB								n+1
FCS (2 octets)								n+2 n+3

NOTE – This field is encrypted.

Figure 18/X.272 – Secure Compressed and Encrypted Data Transfer Frame Format

Table 16/X.272 – Secure Compressed and Encrypted Data Transfer Frame Format

Field	Description
DLCI, control and NLPID	See 8.1 for details
FRCP Header	The FRCP Protocol Header consists of the following: • Ext.: Extension bit must be set to one • Compressed/Uncompressed (C/U): Set to 1 to indicate that data is uncompressed • Reset_Ack (RA): Set to 1 by the sender if it is acknowledging the reset request from the remote peer • Reset_Request (RR): Set to 1 by the receiver if secure compression resynchronization is required • Protocol option (OPT): Set to: O P T 1 0 1 to specify encryption • Control/Data (C/D) bit: Set to 0 to indicate a data frame
Sequence Number	Number assigned by the encryptor sequentially starting with 0 and incremented modulo 256
User Data	User data is secure compressed first and then encrypted. Data must be decrypted first and then decoded
Padding	See 10.1.2
Pad Length	See 10.1.2
LCB	Longitudinal Check Byte – calculated on compressed text of octets 7 through n
FCS	Q.922 Frame Check Sequence

The sequence number and LCB are generated by the encryptor. Octets 8 to m are fed to the decoder. Upon detection of loss of synchronization due to wrong sequence number or wrong LCB, the compression histories must be resynchronized by setting the RR and RA bits as described in the related clauses.

13.2 Encryption and Compressed Data

If the data compression and encryption facilities are configured and successfully negotiated, the user data is compressed first and then encrypted. The process is the same as subclause 11.1 with the exception that when the C/U bit is set to indicate no compression, the data is not forwarded to the decoder.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communications**
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2001