UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.272

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/2000)

SÉRIE X: RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

Interconnexion des systèmes ouverts – Protocoles de sécurité

Compression et secret des données dans les réseaux à relais de trames

Recommandation UIT-T X.272

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalisation et commutation	X.50–X.89
Aspects réseau	X.90–X.149
Maintenance	X.150–X.179
Dispositions administratives	X.180–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200–X.209
Définitions des services	X.210–X.219
Spécifications des protocoles en mode connexion	X.220–X.229
Spécifications des protocoles en mode sans connexion	X.230–X.239
Formulaires PICS	X.240–X.259
Identification des protocoles	X.260–X.269
Protocoles de sécurité	**X.270–X.279**
Objets gérés des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.272

Compression et secret des données dans les réseaux à relais de trames

Résumé

La présente Recommandation définit le service de compression et de secret des données dans les réseaux à relais de trames (FRCP). La présence d'un service de compression de données (DC) dans un réseau augmentera le débit effectif de celui-ci.

Par ailleurs, la croissance de la demande en transmission de données sensibles sur des réseaux publics nécessite des ressources permettant d'assurer le secret de ces données. Afin d'obtenir des taux de compression optimaux, il est essentiel de comprimer les données avant de les crypter. Il est donc souhaitable d'offrir, dans la spécification du service de compression des données, des ressources permettant de négocier également des protocoles de cryptage des données. Etant donné que la tâche de compression puis de cryptage des données exige beaucoup de ressources de calcul, certains protocoles ont été proposés afin d'assurer simultanément la compression des données et leur cryptage (compression de données sécurisée).

Source

La Recommandation X.272 de l'UIT-T, élaborée par la Commission d'études 7 (1997-2000) de l'UIT-T, a été approuvée le 31 mars 2000 selon la procédure définie dans la Résolution 1 de la CMNT.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de la CMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Introduction

La présente Recommandation spécifie les procédures d'exécution de la compression et du secret des données en relais de trames. Elle s'applique aux trames à champ de commande UI (informations non numérotées). Elle ne couvre pas les trames utilisant un champ de commande de type I (informations sur le numéro).

Recommandation UIT-T X.272

Compression et secret des données dans les réseaux à relais de trames

1 Domaine d'application

Le domaine d'application de la présente Recommandation couvre la négociation et l'encapsulation de la compression de données, de la compression sécurisée de données, de l'authentification et du cryptage en relais de trames. Ces protocoles sont fondés sur le protocole de commande de liaison PPP (IETF RFC 1661) [13] et sur le protocole de commande de cryptage PPP (IETF RFC 1968 [14] et 1969 [15]).

La présente Recommandation s'applique aux trames d'information non numérotée (UI, *unnumbered information*) encapsulée conformément à l'Annexe E/Q.933 [7]. Elle traite de la compression et du secret des données sur connexions virtuelles permanentes (PVC, *permanent virtual connection*) comme sur connexions virtuelles commutées (SVC, *switched virtual connection*).

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

[1] UIT-T I.122 (1993), *Cadre pour la fourniture des services supports en mode trame*.

[2] UIT-T I.233.1 (1991), *Service support à relais de trames sur RNIS*.

[3] UIT-T I.370 (1991), *Gestion des encombrements dans le service support à répétition de trames sur RNIS*.

[4] UIT-T E.164 (1991), *Plan de numérotage des télécommunications publiques internationales*.

[5] UIT-T Q.922 (1992), *Spécification de la couche liaison de données RNIS pour les services supports en mode trame*.

[6] UIT-T Q.921 (1993), *Interface usager-réseau du RNIS – Spécification de la couche de liaison de données*.

[7] UIT-T Q.933 (1995), *Système de signalisation d'abonné numérique n° 1 – Spécification de la signalisation pour la commande et la surveillance de l'état des connexions virtuelles commutées et permanentes en mode trame*.

[8] UIT-T Q.931 (1993), *Spécification de la couche 3 de l'interface usager-réseau RNIS pour la commande de l'appel de base*.

[9] UIT-T Q.850 (1993), *Utilisation des indications de cause et de localisation dans le système de signalisation d'abonné numérique n° 1 et le sous-système utilisateur du RNIS du système de signalisation n° 7*.

[10] UIT-T Q.951 (1993), *Description d'étape 3 des services complémentaires d'identification de numéro utilisant le système de signalisation d'abonné numérique n° 1*.

[11] UIT-T X.36, Amendement 1 (1996), *Signalisation des circuits virtuels commutés et améliorations apportées à la signalisation des circuits virtuels permanents*.

[12] UIT-T X.121 (1992), Plan de numérotage international pour les réseaux publics pour données.

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

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

[15] IETF RFC 1969 (1996), *The PPP DES Encryption Protocol (DESE)* (Le protocole de cryptage DES pour liaisons PPP).

[16] IETF RFC 1570 (1994), *PPP LCP Extensions* (extensions du protocole LCP pour liaisons PPP).

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

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

[19] IETF RFC 1994 (1996), *PPP Challenge Handshake Authentication Protocol (CHAP)* (protocole PPP d'authentification par dialogue à énigme) (CHAP).

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

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

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 anti-expansion: méthode permettant d'empêcher l'expansion de données d'utilisateur en raison du codage de compression.

3.2 contexte de compression: données de vocabulaire et autres informations relatives à la détection des erreurs et à la synchronisation, créées et tenues à jour par des entités homologues afin de coder/décoder des données d'utilisateur.

3.3 fonction de compression de données: entité qui exécute le codage de compression de données, le décodage, la détection d'erreur, la synchronisation et la négociation.

3.4 définition de fonction de compression de données: spécification qui décrit le format et les procédures utilisés par une fonction de compression de données pour transporter des données d'utilisateur et des primitives de commande.

3.5 décodeur: entité qui décomprime des données d'utilisateur.

3.6 codeur: entité qui comprime des données d'utilisateur.

3.7 tampon chronologique: type de vocabulaire utilisé pour la compression de données.

3.8 0x: désignation générique des nombres hexadécimaux.

3.9 octet de contrôle longitudinal (LCB, *longitudinal check byte*): l'octet LCB est calculé comme suit pour chaque trame:

1) combinaison par opérateur XOR de l'octet 0xFF avec le premier octet de la charge utile et mémorisation du résultat.

2) ensuite, chaque octet subséquent de la charge utile est combiné par opérateur XOR avec le résultat afin de produire la valeur de résultat suivante.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes.

A bit d'authentification (*authentication bit*)

Ack acquittement (*acknowledgement*)

CBC mode chaînage de blocs chiffrants (*cipher block chaining*)

CCP protocole de commande de compression (*compression control protocol*)

C/D commande/données (*control/data*)

CHAP protocole d'authentification par dialogue à énigme (*challenge handshake authentication protocol*)

C_Mode-1 mode 1 de compression de données par défaut (*default data compression mode 1*)

C/R en-tête de trame (*frame header*) comme décrit dans l'UIT-T Q.922

C/U comprimé/non comprimé (*compressed/uncompressed*)

DC compression de données (*data compression*)

DCCI identificateur de contexte de compression de données (*data compression context identifier*)

DCFD définition de fonction de compression de données (*data compression function definition*)

DCP protocole de compression de données (*data compression protocol*)

DCPCP protocole de commande DCP (*DCP control protocol*)

DES norme de cryptage de données (*data encryption standard*)

DLCI identificateur de connexion de liaison de données (*data link control identifier*)

E_Mode-1 mode 1 de cryptage de données par défaut (*default data encryption mode 1*)

ETTD équipement terminal de traitement de données

Ext. bit d'extension (*extension bit*)

FCS séquence de contrôle de trame (*frame check sequence*) comme décrit dans l'UIT-T Q.922

FECN en-tête de trame (*frame header*) comme décrit dans l'UIT-T Q.922

FR relais de trames (*frame relay*)

FRCP protocole de compression et de secret en relais de trames (*frame relay compression and privacy protocol*)

FZA algorithme de compression sécurisée de données (*secure data compression algorithm*)

LCB octet de contrôle longitudinal (*longitudinal check byte*)

LCP protocole de commande de liaison (*link control protocol*)

LZS algorithme de compression de données (*data compression algorithm*)

NLPID identificateur de protocole de couche réseau (*network layer protocol identifier*)

OUI identificateur unique d'organisation (*organization unique identifier*)

PDU unité de données protocolaire (*protocol data unit*)

PVC connexion virtuelle permanente (*permanent virtual connection*)

RA acquittement de réinitialisation (*reset acknowledge*)

SCA algorithme de compression sécurisée de données (*secure data compression algorithm*)

S_Mode-1 mode 1 de compression sécurisée par défaut (*default secure compression mode 1*)

SVC connexion virtuelle commutée (*switched virtual connection*)

XOR opérateur booléen OU exclusif (*boolean exclusive OR*)

5 Conventions

La présente Recommandation utilise certains mots pour définir la signification de chaque exigence particulière. Ces mots sont les suivants:

- "doit" ou "obligatoire" – indique qu'un élément est une exigence absolue de la présente Recommandation.
- "il convient", "il y a lieu", "devrait", "doit normalement" – indique un élément hautement souhaitable.
- "peut" ou "facultatif" – l'élément n'est pas obligatoire et peut être appliqué ou ignoré selon les besoins du réalisateur.
- "non applicable" – l'élément est hors du domaine d'application de la présente Recommandation.

6 Aperçu général

La présente Recommandation spécifie l'encapsulation du protocole de compression et de secret en relais de trames (FRCP, *frame relay compression and privacy protocol*) dans des réseaux en mode trame. La présente Recommandation autorise la négociation et l'implémentation de plusieurs ressources, dont les suivantes: procédures d'authentification; ressource de cryptage de données; ressource de compression sécurisée de données et ressource de compression de données. Le protocole FRCP assure deux modes d'exploitation pour la ressource de cryptage:

- E_Mode-1, qui est le mode par défaut et qui est obligatoire pour toute implémentation prenant en charge la ressource de cryptage. Il permet la négociation des paramètres de cryptage. L'algorithme de cryptage par défaut est la norme de cryptage des données (DES, *data encryption standard*) avec clés de 56 bits et chaînage des blocs chiffrants (CBC, *cipher block chaining*) [21]. La clé secrète de cette norme DES, partagée entre les parties communicantes, possède une longueur de 8 octets. Elle se compose d'une grandeur de 56 bits qui est utilisée par l'algorithme DES. Cette clé de 56 bits est mémorisée sous la forme d'une grandeur de 64 bits (8 octets), le bit de poids faible de chaque octet étant utilisé comme bit de parité.
- E_Mode-2, qui est un mode facultatif permettant la négociation complète des algorithmes de cryptage, aussi bien normalisés que non normalisés, avec leurs paramètres associés. Ce mode est fondé sur le protocole de commande de cryptage pour liaisons PPP [14]. On peut utiliser ce mode pour prendre en charge des clés de cryptage d'une longueur supérieure à 56 bits. La taille de la clé varie d'un fournisseur à l'autre.

En outre, le protocole FRCP assure deux modes d'exploitation pour la ressource de compression sécurisée de données:

- S_Mode-1, qui est le mode obligatoire utilisant les algorithmes et formats de trame par défaut définis dans la présente Recommandation. Le mode S_Mode-1 offre un protocole de négociation simple permettant d'assurer le service de compression sécurisée de données avec les paramètres par défaut. L'algorithme de compression sécurisée de données nécessite l'utilisation d'une clé de cryptage. Cette clé, qui est partagée entre les parties communicantes, a une longueur de huit octets. Il s'agit d'une grandeur à 56 bits utilisés, qui est stockée en tant que grandeur à 64 bits (huit octets), le bit le moins significatif de chaque octet étant utilisé comme bit de parité.
- S_Mode-2, qui est un mode facultatif permettant une négociation complète des algorithmes de compression sécurisée de données et de leurs paramètres associés.

Par ailleurs, le protocole FRCP assure deux modes d'exploitation pour la ressource de compression de données:

- C_Mode-1, qui est le mode obligatoire utilisant les algorithmes et formats de trame par défaut définis dans la présente Recommandation. Le mode C_Mode-1 offre un protocole de négociation simple permettant d'assurer le service de compression de données avec les paramètres par défaut.
- C_Mode-2, qui est un mode facultatif permettant une négociation complète des algorithmes de compression de données et de leurs paramètres associés.

7 Modèle de référence

Dans le contexte de la présente Recommandation, le terme "**ETTD**" n'est pas limité à la seule fonction d'équipement terminal. Il désigne un utilisateur du réseau dans un sens fonctionnel général, ce réseau pouvant être un autre (type de) réseau.

Le service FRCP facilite une communication efficace en termes de débit plus élevé en mode paquet/trame, avec un transport sécurisé si l'option de secret est négociée. Utilisée entre ETTD, comme représenté sur la Figure 1, la procédure de compression et de secret des données est transparente au ou aux réseaux à relais de trames entre ETTD émetteurs et récepteurs.

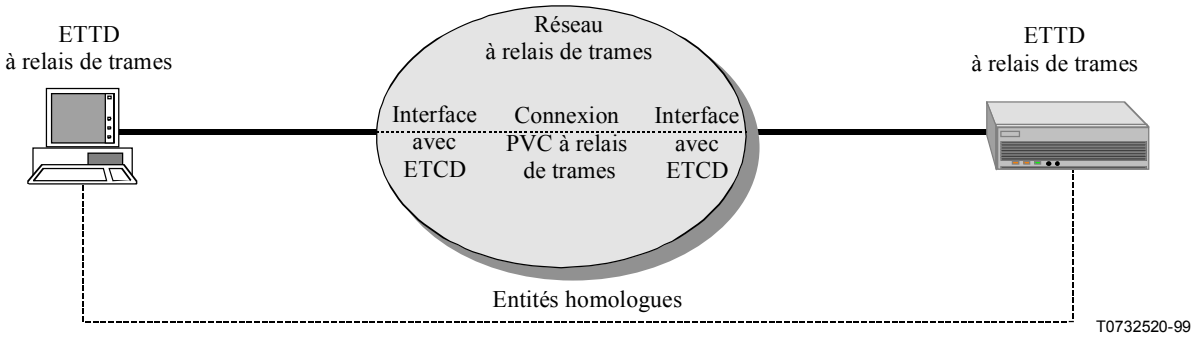


Figure 1/X.272 – Diagramme de référence

Le protocole de compression et de secret en relais de trames fait appel à différentes phases pour négocier les ressources offertes. L'ordre de ces phases est le suivant:

1) établissement d'une connexion virtuelle: cette phase est régie par les procédures de signalisation pour connexions PVC ou SVC [1] à [12] et est hors du domaine d'application de la présente Recommandation. La phase FRCP commence une fois que la connexion virtuelle a été établie;
2) phase d'authentification: lorsqu'elle est utilisée, l'authentification initiale par homologue doit être effectuée avant la ou les phases de compression ou de cryptage des données. Des énigmes d'authentification ultérieures, si elles sont acceptées par le protocole d'authentification choisi, peuvent être posées en texte non codé au cours de la phase de transfert de données, sans utiliser les ressources de cryptage, de compression sécurisée ou de compression simple;
3) phase de négociation du cryptage: utilisée pour négocier le mode et les paramètres à utiliser pour le cryptage au cours de la phase de transfert des données;
4) phase de négociation de la compression sécurisée des données: utilisée pour négocier le mode et les paramètres qui seront utilisés pour la compression sécurisée des données au cours de la phase de transfert des données;

5) phase de négociation de la compression de données: utilisée pour négocier le mode et les paramètres qui seront utilisés pour la compression des données au cours de la phase de transfert des données;

6) phase de transfert des données: transfert de messages chiffrés, comprimés avec ou sans sécurisation, pouvant inclure des données d'utilisateur et des informations de commande.

8 Spécification de mode commun

Le présent paragraphe définit les formats de trame et les procédures que toutes les ressources FRCP ont en commun.

8.1 Format général des trames

La structure générale des trames du protocole FRCP assure l'encapsulation des informations de commande ou le transfert des données. Toutes les trames sont envoyées sur la connexion virtuelle à relais de trames entre systèmes d'extrémité. Le contenu des trames est transparent au réseau à relais de trames. Les trames de commande contiennent les informations qui sont vitales pour la négociation des ressources d'authentification, de cryptage et de compression sécurisée ou non sécurisée des données, ainsi que des paramètres associés à ces ressources. Le bit C/D du protocole FRCP permet de distinguer entre trames de commande et trames de données. Pour les trames de commande, le bit C/D est mis à 1. Le format général des trames de commande du protocole FRCP, décrit dans la Figure 2, est utilisé pour négocier les informations de commande.

Description								Octet
Adresse Q.922 (2 octets) (Note)								1 2
Commande (UI: 0x03)								3
Identificateur NLPID (0xB0)								4
En-tête FRCP								
Ext. 1	Réserve	Réserve	Réserve	Réserve	I	D	C/D 1	5
Charge utile FRCP								6 n
Séquence FCS (2 octets)								n+1 n+2

NOTE – Cette adresse de relais de trames à 2 octets n'est montrée ici qu'à titre d'illustration. Les formats d'adresse à 3 et 4 octets ne sont pas interdits.

Figure 2/X.272 – Format des trames de commande du protocole FRCP

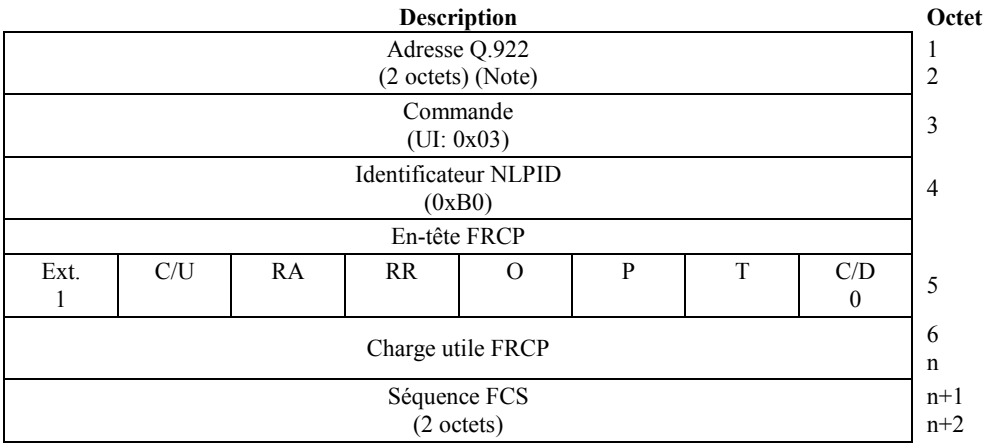
L'adresse de relais de trames Q.922 [5] est représentée dans la Figure 2 en format deux octets. Toutefois, le protocole FRCP n'interdit pas d'utiliser les formats d'adresse avec le troisième et le quatrième octet. Voir Tableau 1.

Tableau 1/X.272 – Format des trames de commande du protocole FRCP

Champ	Description
Adresse Q.922	Structure d'adresse de relais de trames telle que définie dans l'UIT-T Q.922 [5]
Commande	Trame d'information non numérotée (UI, *unnumbered information frame*) (x03) en relais de trames Q.922 [5]
Identificateur NLPID	Identificateur de protocole de couche Réseau
En-tête FRCP	L'en-tête de protocole FRCP se compose des éléments suivants: • ext.: bit d'extension, mis à 1 • réserve: bits de réserve pour usage futur, mis à 0 • ID (deux bits): ce champ spécifie la ressource qui est utilisée. Les ressources sont définies ci-dessous: I D 0 0 réservé 0 1 compression 1 0 compression sécurisée 1 1 cryptage • A: bit d'authentification. Ne peut être mis à 1 que si C/D = 1. Indique que la trame contient des informations d'authentification • Bit de commande/données (C/D) 0 trame de données 1 trame de commande
Charge utile FRCP	Informations de commande ou données de transfert selon la façon dont les bits d'en-tête de protocole FRCP sont positionnés
FCS	Séquence de contrôle de trame Q.922

Si le bit C/D est mis à 1, il s'agit d'une trame de commande. Le champ d'identificateur sert dans ce cas à négocier diverses ressources du protocole FRCP. Ces ressources sont négociées l'une après l'autre, dans l'ordre indiqué au 8.2. Les détails du format de trame sont donnés dans les sections qui s'y rapportent. Si le bit A est mis à "1", le champ d'identificateur n'est pas pris en compte car il s'agit d'une trame d'authentification.

Si le bit C/D est mis à 0, il s'agit d'une trame de données. Le format d'une trame de transfert de données dépend de la ou des ressources FRCP qui ont été négociées. La Figure 3 décrit le format général d'une trame de transfert de données FRCP. Le Tableau 2 décrit les divers champs de cette trame.



NOTE – Cette adresse de relais de trames à 2 octets n'est montrée ici qu'à titre d'illustration. Les formats d'adresse à 3 et 4 octets ne sont pas interdits.

Figure 3/X.272 – Format des trames de données du protocole FRCP

Tableau 2/X.272 – Format des trames de données du protocole FRCP

Champ	Description
Adresse Q.922	Structure d'adresse de relais de trames contenant DLCI, FECN, BECN, DE et C/R. Le bit C/R n'est pas utilisé
Commande	Trame d'information non numérotée (UI) (x03) en relais de trames Q.922
Identificateur NLPID	Identificateur de protocole de couche Réseau selon l'ISO/CEI TR 9577
En-tête FRCP	L'en-tête du protocole FRCP se compose des éléments binaires suivants: • bit d'extension – mis à 1, mais inclus pour amélioration future • comprimées/non comprimées (C/U): mis à 1 indique que les données ne sont pas comprimées • Reset_Ack (RA): mis à 1 pour indiquer l'acquittement d'une réinitialisation d'un historique de compression ou d'un historique de cryptage. La distinction entre les types d'historique est donnée dans les bits O, P et T • Reset_Request (RR): mis à 1 pour indiquer la demande d'une réinitialisation d'un historique de compression ou d'un historique de cryptage. La distinction entre les types d'historique est donnée dans les bits O, P et T • bit de commande/données (C/D): mis à 0 pour indiquer une trame de données • option de protocole (OPT, *protocol option*): met les données en relation avec le protocole associé selon les correspondances suivantes: O P T 0 0 0 champ réservé 0 0 1 cryptage 0 1 0 compression sécurisée 0 1 1 compression 1 0 0 compression et cryptage 1 0 1 compression sécurisée et cryptage x x x toutes les autres valeurs sont réservées
Charge utile FRCP	Données qui sont comprimées ou cryptées, selon la ressource FRCP ou les ressources qui ont été négociées
FCS	Séquence de contrôle de trame Q.922

8.2 Négociation des ressources

Au cours de l'étape de négociation, le bit C/D d'en-tête FRCP est mis à 1 afin d'indiquer que la trame est du type commande. Le format de la trame de commande permet la négociation de plusieurs ressources. Chaque ressource est négociée séparément. La négociation des ressources se fait dans l'ordre suivant:

- si l'authentification est configurée, les entités homologues doivent toujours être authentifiées les premières. Si l'étape d'authentification est exécutée normalement, d'autres ressources peuvent être négociées. Si cependant l'étape d'authentification n'est pas exécutée normalement, la connexion doit être close;
- si l'option de cryptage est configurée, cette option doit être négociée ensuite. Si la négociation est exécutée normalement, d'autres options peuvent être négociées par la suite. Si cependant la négociation du cryptage ne s'exécute pas normalement, la connexion doit être close;
- si l'option de compression sécurisée des données est configurée, cette option doit être négociée ensuite. Si cette négociation est exécutée normalement, les données doivent être comprimées avec sécurisation avant leur envoi sur la liaison. Si la négociation de compression sécurisée ne s'exécute pas normalement, l'étape de transfert des données ne peut commencer sans compression de données que si la ressource de cryptage est configurée et a été normalement négociée. Sinon, la connexion doit être close;
- l'option de compression de données peut être configurée et négociée à condition que l'option de compression sécurisée des données ne soit pas configurée. Si l'option de compression des données est configurée, cette option est négociée ensuite. Si la négociation s'exécute normalement, les données peuvent être envoyées sur la liaison sous forme comprimée. Les données doivent être cryptées si l'option de cryptage est configurée et est correctement négociée. Si aucune autre option n'est configurée et si la négociation de la ressource de compression de données n'est pas exécutée normalement, les données peuvent être transmises sur la liaison en mode non comprimé. Sinon, les données doivent être cryptées avant leur transmission sur la liaison.
- Si l'ordre de négociation ne correspond pas à l'ordre spécifié ci-dessus, la connexion doit être close. L'ordre de négociation est résumé dans le Tableau 3 ci-dessous.

Tableau 3/X.272 – Ordre de négociation des ressources

Ressource demandée **Ressource négociée**	**Authentification**	**Cryptage**	**Compression sécurisée**	**Compression**
Aucune	Exécution	Exécution	Exécution	Exécution
Authentification	Exécution	Exécution	Exécution	Exécution
Cryptage	Terminaison	Exécution	Exécution	Exécution
Compression sécurisée	Terminaison	Terminaison	Exécution	Terminaison
Compression	Terminaison	Terminaison	Terminaison	Exécution
Authentification, Cryptage	Exécution	Exécution	Exécution	Exécution
Authentification, Cryptage, Compression sécurisée	Exécution	Exécution	Exécution	Terminaison
Authentification, Compression	Exécution	Terminaison	Terminaison	Exécution
NOTE – Lorsqu'une ressource a été négociée, toutes les trames échangées sur une connexion doivent être encapsulées à l'aide du format FRCP.				

9 Ressource d'authentification

Cette ressource est utilisée pour authentifier deux dispositifs sur la base d'un protocole d'authentification présélectionné. Cette ressource d'authentification est facultative. Si l'authentification est souhaitée, une implémentation doit effectuer l'authentification initiale avant d'invoquer les ressources de cryptage, de compression sécurisée des données ou de compression de données.

Les paquets d'authentification sont identifiés au moyen du bit **A** contenu dans l'en-tête FRCP d'un message de commande (bit C/D = 1). En général, les caractéristiques d'authentification d'une liaison PPP [19] sont utilisées. Le protocole d'authentification est négocié au cours de l'établissement de la communication pour des connexions PVC ou SVC. Le protocole d'authentification est identifié, si applicable, par les octets 6, 7 et 7a. Les octets 8-n contiennent des informations d'authentification ou des options de configuration dans un format de paquet d'authentification propre au protocole identifié dans les groupes d'octets 6 et 7.

Le mécanisme d'authentification FRCP prend en charge les protocoles d'authentification définis pour les liaisons PPP comme le protocole d'authentification extensible PPP (EAP, *extensible authentication protocol*) qui lui-même prend en charge un certain nombre de protocoles d'authentification, le protocole d'authentification par dialogue à énigme PPP (CHAP, *challenge handshake authentication protocol*) et le protocole d'authentification par mot de passe PPP (PAP, *password authentication protocol*). Les détails des protocoles d'authentification PPP peuvent être consultés dans chacun des documents RFC [13] à [16] concernant une authentification PPP particulière.

L'authentification s'effectue entre entités homologues. Cela implique que les deux homologues doivent s'authentifier réciproquement avant qu'un trafic puisse s'écouler dans les deux sens de la connexion.

9.1 Format des trames d'authentification

Le format des trames d'authentification est indiqué dans la Figure 4 ci-dessous. Voir aussi Tableau 4.

Description								Octet
Informations d'adresse de relais de trames, de commande et d'identificateur NLPID								1-4
En-tête FRCP								
Ext. 1	Réserve 0	Réserve 0	Réserve 0	I 0	D 0	A 1	C/D 1	5
Identificateur de protocole d'authentification (Note 2)								6 7
Algorithme d'authentification (Note 2)								7a* (Note 1)
Format de paquet d'authentification (Note 2)								8 n
FCS (2 octets)								n+1 n+2

NOTE 1 – L'octet 7a n'est présent que si les octets 6 et 7 indiquent le protocole CHAP (xC223).
NOTE 2 – Contenus et formats sont définis selon les RFC relatifs aux liaisons PPP.

Figure 4/X.272 – Format général des trames d'authentification

Tableau 4/X.272 – Format général des trames d'authentification

Champ	Description
DLCI, commande et identificateur NLPID	Voir 8.1 pour les détails
En-tête FRCP	• Ext.: bit d'extension mis à 1 • Réserve: bit de réserve pour usage futur, mis à 0 • Champ ID mis à 00 • Bit d'authentification (A) mis à 1 • Bit de commande/données (C/D) mis à 1
Identificateur de protocole d'authentification (octets 6 et 7)	Identifie le protocole d'authentification à utiliser, par exemple, PAP, CHAP, etc. Voir IETF RFC 1340 [18] pour les détails
Algorithme d'authentification (octet 7a)	Si présent, identifie la méthode CHAP d'authentification à utiliser. Voir IETF RFC 1994 [19] pour les détails. Présent seulement si les octets 6 et 7 indiquent CHAP
Format de paquet d'authentification (octets 8-n)	En général, utilise le format de paquet de la méthode d'authentification PPP spécifique
FCS	Séquence de contrôle de trame Q.922

9.2 Format des paquets d'authentification

Les paquets de type PPP doivent être encapsulés dans les octets 8 à n du format de verrouillage de trame ci-dessus. Ces paquets ont le format général suivant: code, identificateur, longueur, valeurs. Par exemple, dans le cas du protocole CHAP, on utilise le format de paquet de la section 4 du document IETF RFC 1994 [19], comme l'indiquent la Figure 5 et le Tableau 5.

Description	Octet
Code	8
Identificateur	9
Longueur (2 octets)	10 11
Valeurs/Données comme défini par protocole d'authentification	12 n

Figure 5/X.272 – Format des paquets d'authentification

Tableau 5/X.272 – Structure des primitives de commande FRCP

Champ	Description
Code	D'après la méthode d'authentification PPP indiquée dans les octets 6-7a. Indique le type de paquet ou de message, par exemple, demande, réponse, etc.
Identificateur	Numéro de transaction pour corréler une demande avec une réponse. Envoyé dans une demande et renvoyé en écho dans la réponse correspondante
Longueur (2 octets)	Y compris: code, identificateur, longueur et toutes options de configuration
Options de configuration	Valeurs/données selon le protocole PPP d'authentification utilisé. Voir la méthode spécifique d'authentification PPP pour les détails. Par exemple, CHAP EAP, PAP, etc.

9.3 Procédures d'authentification

Voir les procédures décrites dans le document RFC applicable au protocole d'authentification PPP utilisé. Par exemple, si le protocole d'authentification configuré est CHAP (0xCC23), suivre les procédures du IETF RFC 1994 [19].

10 Ressources de cryptage

La ressource de cryptage est chargée d'activer et de lancer des algorithmes de cryptage de données aux deux extrémités de la liaison. Le cryptage fait appel à un mécanisme d'échange de paquets similaire au protocole de commande de liaison PPP (LCP) [16].

L'utilisation de la ressource de cryptage est négociée entre dispositifs homologues. Le mode et les algorithmes sont sélectionnés indépendamment pour chaque sens d'une connexion virtuelle, ce qui est résumé dans le Tableau 6.

Tableau 6/X.272 – Table de transition E_Mode-1

Mode demandé	Mode configuré	
	E_Mode-1	**E_Mode-2**
E_Mode-1	Répondre par E_Mode-1 et utiliser E_Mode-1.	Répondre par E_Mode-1 et utiliser E_Mode-1.
E_Mode-2	Répondre par E_Mode-1 et utiliser E_Mode-1.	Répondre par E_Mode-2 et utiliser E_Mode-2.

L'on part du principe que chaque dispositif homologue possède une clé initiale qui sera utilisé pour le cryptage. La méthode par laquelle cette clé est portée à la connaissance des deux dispositifs communicants est hors du domaine d'application de la présente Recommandation. La négociation du cryptage doit toujours être exécutée correctement avant que le transfert des données soit autorisé. Une fois négociées, toutes les trames de données échangées sur une connexion virtuelle doivent être cryptées.

10.1 Spécification E_Mode-1

Le cryptage E_Mode-1 doit être pris en charge si la ressource de cryptage est implémentée dans un ETTD. Le mode E_Mode-1 utilise la norme de cryptage de données (DES, *data encryption standard*) avec une clé de 56 bits assortie d'un chaînage des blocs chiffrants (CBC, *cipher block chaining*) [21]. Le cryptogramme est transféré dans le format de paquet défini au 10.1.4, Cryptage des données d'utilisateur E_Mode-1.

10.1.1 Format des trames de commande E_Mode-1

Cette trame est utilisée pour négocier les paramètres E_Mode-1. Voir Figure 6 et Tableau 7.

Description								Octet
Adresse de relais de trames, commande et identificateur NLPID								1-4
En-tête FRCP								
Ext. 1	Réserve	Réserve	Réserve	I	D	A	C/D 1	5
Code								6
Identificateur								7
Longueur (2 octets)								8 9
Type: Mode-1 (254)								10
Longueur								11
Version								12
Eléments paramétriques								13 n
FCS (2 octets)								n+1 n+2

Figure 6/X.272 – Trame de commande E_Mode-1

Tableau 7/X.272 – Trame de commande E_Mode-1

Champ	Description
DLCI, commande et identificateur NLPID	Voir 8.1 pour les détails
En-tête FRCP	• Ext.: bit d'extension = 1 • Réserve: bit de réserve pour usage futur, mis à 0 • Champ ID (2 bits) mis à 11 • Bit d'authentification (A) = 0 • Bit de commande/données (C/D) mis à 1
Code	Décimal pour 1 Config-Req; décimal pour 2 Config-Ack
Identificateur	Numéro de transaction pour corréler une demande avec une réponse. Envoyé dans une demande et renvoyé en écho dans la réponse correspondante
Longueur (2 octets)	Y compris: Code, Identificateur, Longueur et toutes options de configuration
Type	254 (décimal) – indique E_Mode-1. Les types 245 à 253 inclusivement ainsi que le type 255 sont réservés.
Longueur	Varie selon le nombre de paramètres
Version	Numéro de version du cryptage FRCP mis à 1
Eléments paramétriques	Zéro ou plus que zéro éléments paramétriques E_Mode-1. Voir 10.1
FCS	Séquence de contrôle de trame Q.922

10.1.1.1 Eléments paramétriques E_Mode-1

L'identificateur d'élément paramétrique désigne un tel élément. Sa longueur est celle de l'élément paramétrique entier, y compris le champ d'identificateur d'élément paramétrique et le champ de longueur. Le champ de valeurs énumère les valeurs paramétriques propres à l'élément. Les éléments paramétriques doivent toujours se composer d'un nombre entier d'octets. Ceux-ci commencent après l'octet 12 de l'option de configuration E_Mode-1. Voir Figure 7.

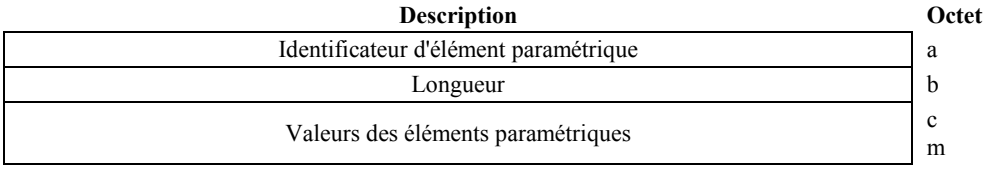


Figure 7/X.272 – Structure générale des éléments paramétriques E_Mode-1

10.1.1.1.1 Vecteur initial E_Mode-1

L'algorithme CBC de la norme DES nécessite un vecteur d'initialisation (IV, *initialization vector*) ayant la même longueur que le bloc. L'inclusion du paramètre de vecteur initial dans la demande de configuration (Config-Req) est obligatoire. La présence du paramètre de vecteur initial dans le message Config-Req désigne le mot de circonstance initial de 64 bits que le dispositif expéditeur utilisera pour le chaînage des blocs chiffrants (CBC). Le message Config-Ack accuse réception du vecteur initial. Le paramètre de vecteur initial n'est pas envoyé dans le message Config-Ack. Voir Figure 8 et Tableau 8.

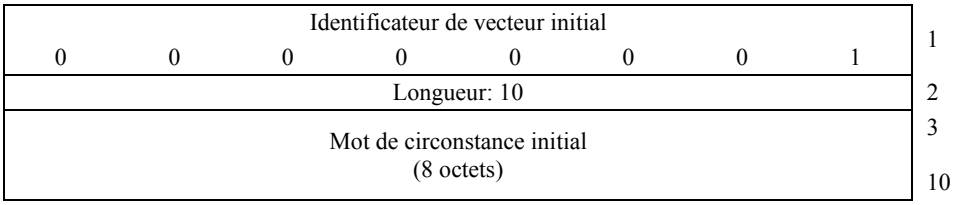


Figure 8/X.272 – Elément paramétrique de vecteur initial (mot de circonstance) E_Mode-1

Tableau 8/X.272 – Paramètre de vecteur initial (mot de circonstance) E_Mode-1

Champ	Description
Identificateur de vecteur initial	Octet désignant le paramètre de vecteur initial
Longueur	10 (décimal)
Mot de circonstance initial	Grandeur de 64 bits qui est utilisée par le dispositif homologue afin d'effectuer le cryptage du premier paquet émis. Pour éviter les attaques par réexécution, il y a lieu que le dispositif offre une valeur différente au cours de chaque négociation

10.1.1.1.2 Echange et mise à jour des clés E_Mode-1

Le mode E_Mode-1 prend en charge la clé de cryptage statique. Les procédures d'échange et de mise à jour des clés sont hors du domaine d'application de la présente Recommandation.

10.1.2 Format de transfert des données E_Mode-1

L'algorithme DES fonctionne sur des blocs de 8 octets, ce qui nécessite fréquemment un bourrage après la fin des données d'utilisateur non cryptées. Un octet (indiquant "longueur de bourrage") doit être ajouté à la fin des données d'utilisateur. La longueur des données d'utilisateur plus l'octet de longueur de bourrage est donc calculée avant le processus de cryptage. Si la longueur, en octets, n'est pas un multiple de 8, des octets supplémentaires sont ajoutés en bourrage pour faire en sorte que la longueur totale s'aligne sur une limite de 8 octets. Il est préféré que les octets de bourrage soient remplis de données aléatoires. Le nombre de ces octets peut aller de 0 à 255 afin de permettre l'occultation de la longueur réelle des données. Le nombre d'octets ajoutés est spécifié dans l'octet de longueur de bourrage, qui est le dernier octet de la trame. La trame complète, y compris les données d'utilisateur, les octets de bourrage et l'octet de longueur de bourrage, est ensuite cryptée. Après le processus de décryptage, les octets de bourrage et l'octet de longueur de bourrage sont extraits des données et doivent être négligés.

La Figure 9 indique le format de la trame FRCP pour l'émission de données chiffrées seulement. Voir également Tableau 9.

Description								Octet
Informations d'adresse de relais de trames, de commande et d'identificateur NLPID								1-4
En-tête FRCP								
Ext. 1	C/U	RA	RR	0	P	T	C/D 0	5
Numéro de séquence								7
Données d'utilisateur (Note)								8 m
Bourrage (Note)								m n-1
Longueur de bourrage (Note)								n
LCB								n+1
FCS (2 octets)								n+2 n+3

NOTE – Ce champ est crypté.

Figure 9/X.272 – Format des trames de transfert de données E_Mode-1

Tableau 9/X.272 – Format des trames de transfert de données E_Mode-1

Champ	Description
DLCI, commande et identificateur NLPID	Voir 8.1 pour les détails.
En-tête FRCP	L'en-tête du protocole FRCP se compose de ce qui suit: • bit d'extension – mis à 1, mais inclus pour amélioration future • comprimées/non comprimées (C/U): mis à 1 pour indiquer que les données ne sont pas comprimées • Reset_Ack (RA): non applicable, mis à 0 • Reset_Request (RR): non applicable, mis à 0 • Option de protocole (OPT): mis à: O P T 0 0 1 pour spécifier le cryptage • bit de commande/données (C/D): mis à 0 pour indiquer une trame de données
Numéro de séquence	Numéro assigné par le crypteur en commençant la séquence par 0 et en l'incrémentant modulo 256
Données d'utilisateur	Données d'utilisateur cryptées
Bourrage	Octets remplis avec des données aléatoires de préférence pour garantir que la longueur totale des données d'utilisateur et l'octet de longueur de bourrage s'aligne sur une limite de 8 octets
Longueur de bourrage	Nombre d'octets de bourrage ajoutés à la longueur des données d'utilisateur plus 1 pour garantir que les données s'alignent sur une limite de 8 octets. Cet octet est le dernier octet dans la trame
LCB	Octet de contrôle longitudinal – calculé sur le texte non codé des octets 7 à n
FCS	Séquence de contrôle de trame Q.922

10.1.3 Procédures de commande E_Mode-1

Le mode E_Mode-1 du protocole FRCP constitue un protocole de négociation simple qui offre la fonction de secret avec l'algorithme et les valeurs paramétriques par défaut. Une fois que le protocole FRCP est activé et correctement négocié, le transfert de données vers le système d'extrémité homologue doit être crypté. Pour désactiver le protocole FRCP, une implémentation peut forcer la connexion virtuelle vers l'état d'inactivité, ou envoyer une demande E_Mode-1 et ne pas envoyer de réponse E_Mode-1.

La négociation de la ressource de cryptage commence lors de l'établissement de la connexion virtuelle. Le terme V_0 est utilisé pour représenter une connexion VC inactive, tandis que le terme V_1 est utilisé pour indiquer une connexion VC active. La phase d'initialisation commence dès l'établissement d'une connexion virtuelle en relais de trames à condition que le protocole FRCP soit configuré par l'utilisateur sur l'ETTD. La phase de fonctionnement commence dès l'achèvement normal de la phase d'initialisation. Au cours de la phase de fonctionnement, le terme f_1 sert à représenter la négociation normale d'une ressource et le terme f_0 sert à indiquer l'échec de la négociation de la ressource. Un achèvement anormal de la phase d'initialisation fait entrer le protocole FRCP dans la phase f_0. Les unités de données PDU de données FRCP ne sont transférées que lorsque E_Mode-1 est dans la phase f_1. Les unités PDU de commande FRCP peuvent être transférées au cours d'une phase quelconque.

10.1.3.1 Etats E_Mode-1

Les états E_Mode-1 du protocole FRCP, qui peuvent exister de part et d'autre de la connexion en relais de trames, sont les suivants:

désactivé (f_0)

la ressource FRCP n'existe pas (lorsqu'une connexion virtuelle passe de V_0 à V_1 que la négociation échoue);

demande émise (I_1)

envoi d'un message de demande de configuration E_Mode-1 à l'entité homologue. Attente de réponse à la demande initiale et à la demande de configuration de l'entité homologue;

demande reçue (I_3)

réception d'un message de demande de configuration E_Mode-1 en provenance de l'entité homologue. Envoi à celle-ci d'une réponse de configuration à son message de demande et d'une demande de configuration (Config-Req). Attente de réponse à la demande initiale;

attente de demande (I_2)

réception d'une réponse de configuration à la demande initiale et attente de la demande de configuration de l'entité homologue;

opérationnel (f_1)

achèvement correct de la négociation E_Mode-1.

Pour assurer l'achèvement, correct ou non, du processus de négociation, un temporisateur d'achèvement du dialogue et un compteur de nombre maximal d'essais sont définis. Le temporisateur d'achèvement du dialogue indique la durée d'exécution du processus de dialogue lors de la négociation. Le compteur de nombre maximal d'essais spécifie le nombre d'essais, par un dispositif, de lancement du processus de négociation. Pour la négociation du mode E_Mode-1 d'une quelconque des ressources de la présente Recommandation, les valeurs par défaut préférées sont indiquées ci-dessous:

Paramètre	Valeur par défaut
Temporisateur d'achèvement du dialogue	3 s
Compteur de nombre maximal d'essais	10 (valeur décimale)

Le diagramme d'états pour l'exécution de la négociation E_Mode-1 est représenté sur la Figure 10.

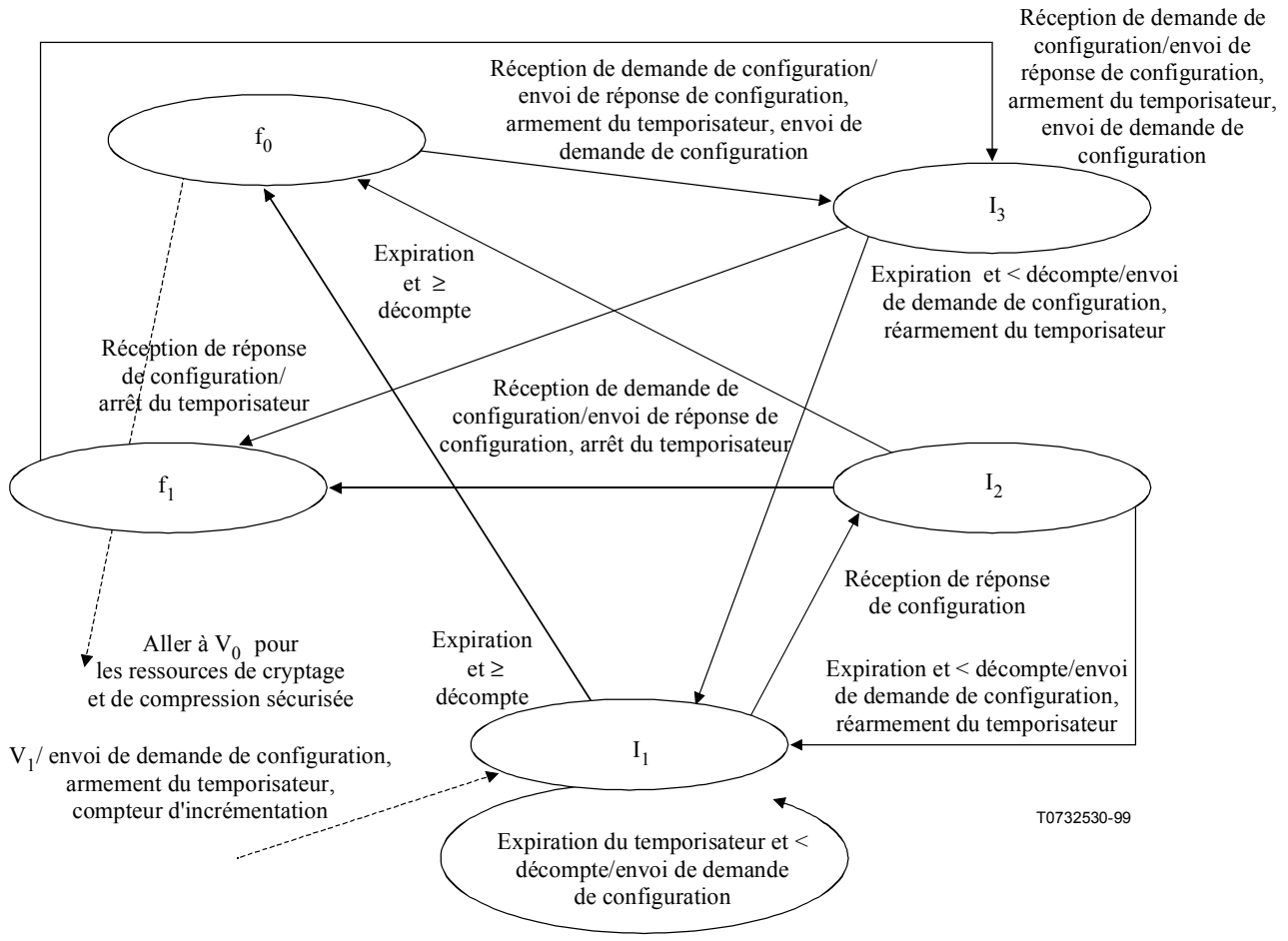


Figure 10/X.272 – Diagramme d'états E_Mode-1

10.1.3.2 Demande d'initialisation

L'initialisation E_Mode-1 commencera lors de l'établissement d'une connexion virtuelle en relais de trames vers une entité homologue et lors de l'activation administrative (par l'utilisateur) d'une fonction de secret en relais de trames. Les procédures de négociation FRCP sont lancées par l'envoi à l'entité homologue d'un message Config-Req, par l'armement d'un temporisateur d'achèvement de dialogue et par l'entrée dans l'état *demande émise (I_1)*.

Dès réception d'un message de réponse de configuration, l'entité doit entrer dans l'état *attente de demande (I_2)*. Lorsqu'une demande Config-Req est reçue de l'homologue, la procédure suivante s'applique:

1) pour les appels dans l'état *demande émise (I_1)*, envoi d'un message de réponse de configuration et entrée dans l'état *demande reçue (I_3)*;

2) pour les appels dans l'état *attente de demande (I_2)*, envoi d'un message de réponse de configuration; arrêt du temporisateur d'achèvement de dialogue; envoi d'une primitive de réponse de configuration indiquant que la négociation est effectuée; entrée dans l'état *opérationnel (f_1)*.

Si le temporisateur d'achèvement du dialogue expire avant que la procédure de dialogue soit terminée et si le nombre d'essais est inférieur au compteur de nombre maximal d'essais, la procédure suivante s'applique:

1) pour les appels dans l'état *demande émise (I_1)*, envoi à l'homologue d'un message Config-Req; réarmement d'un temporisateur d'achèvement de dialogue et incrémentation du nombre de messages Config-Req envoyés à l'homologue;

2) pour les appels dans l'étant *attente de demande (I_2)*, envoi à l'homologue d'un message Config-Req; réarmement d'un temporisateur d'achèvement de dialogue et entrée dans l'état *demande émise (I_1)*.

10.1.3.3 Réception d'une demande de configuration

Dès réception d'une demande de configuration issue de l'entité homologue dans l'état f_0, envoi d'un message de réponse de configuration; envoi d'un message; armement d'un temporisateur d'achèvement de dialogue; incrémentation du nombre de messages Config-Req envoyés à l'homologue et entrée dans l'état *demande reçue (I_3)*.

Dès réception d'un message de réponse de configuration dans l'état *demande reçue (I_3)*, arrêt du temporisateur d'achèvement de dialogue et entrée dans l'état *opérationnel (f_1)*.

Si le temporisateur d'achèvement de dialogue expire avant la fin de la procédure de dialogue et si le nombre d'essais est inférieur au décompte, envoi d'un message Config-Req et réarmement du temporisateur d'achèvement de dialogue.

10.1.3.4 Phase d'état opérationnel

Lorsqu'un message Config-Req est reçu de l'entité homologue pour des appels dans l'état *opérationnel (f_1)*, envoi d'un message de réponse de configuration; envoi d'un message Config-Req; réarmement du temporisateur d'achèvement de dialogue et entrée dans l'état *demande reçue (I_3)*.

10.1.3.5 Phase d'état désactivé

La phase d'état désactivé E_Mode-1 f_0 doit commencer lorsqu'une connexion virtuelle par relais de trames avec une entité homologue est libérée (transition de V_1 à V_0) ou lorsque la négociation a échoué. Si le compteur de nombre maximal d'essais est dépassé lors d'une expiration du temporisateur d'achèvement de dialogue, revenir à la phase f_0. Si la négociation ne parvient pas à atteindre la phase f_1, la connexion virtuelle doit être libérée.

10.1.4 Cryptage des données d'utilisateur E_Mode-1

Une fois que la négociation entre homologues de cryptage est effectuée et que les deux entités homologues sont dans l'état opérationnel, les trames sont cryptées au moyen des procédures du présent paragraphe.

La méthode de cryptage E_Mode-1 utilisée pour créer le cryptogramme est l'algorithme DES avec mode de chaînage des blocs chiffrants (CBC) et clé de 56 bits. Le vecteur initial pour le mode CBC est déduit du mot de circonstance explicite de 64 bits qui est échangé au cours de la négociation du mode E_Mode-1. Si aucun mot de circonstance n'est échangé par les entités homologues, le mode doit être coordonné et configuré chez chaque homologue de la connexion virtuelle. Le mode de cryptage CBC passe au-delà de chaque charge utile vers la suivante. Un numéro de séquence est utilisé pour détecter le moment où une trame n'est pas reçue dans l'ordre correct.

Lorsque des données doivent être envoyées, elles sont bourrées jusqu'au prochain multiple de 8 octets, comme décrit au 10.1.2, afin de former une charge utile de cryptogramme. L'octet LCB est calculé sur la charge utile de cryptogramme. Le crypteur chiffre la charge cryptographique utile et le résultat est positionné dans la trame comme sur la Figure 9. L'expéditeur incrémente le numéro de séquence modulo 256 puis postpose l'octet LCB sur la charge utile et envoie la trame sur la liaison.

Le récepteur vérifie d'abord le numéro de séquence afin de déterminer si une trame a été perdue. Si tel est le cas, les 8 derniers octets du cryptogramme sont conservés en tant que vecteur initial pour la trame suivante et la trame reçue est mise de côté. Si la trame est en séquence, le récepteur déchiffre les champs désignés dans la Figure 9 puis calcule l'octet LCB, qui est comparé à l'octet LCB reçu. S'ils ne concordent pas, les 8 derniers octets des données sont conservés comme vecteur initial pour la prochaine trame et la trame reçue est mise de côté. Si les octets LCB concordent, les données déchiffrées sont traitées par extraction du bourrage.

10.2 Spécification E_Mode-2

La prise en charge du cryptage E_Mode-2 implique les procédures de négociation complètes du document IETF RFC 1968. Ces procédures permettent à deux dispositifs homologues en relais de trames de négocier et de converger vers des méthodes et paramètres de cryptage à utiliser entre eux sur une connexion virtuelle. On utilise en général les formats et procédures de commande IETF RFC 1968 [14], ce qui permet de négocier différentes méthodes de cryptage dans chaque sens de la connexion virtuelle.

10.2.1 Format des trames de commande E_Mode-2

Cette trame est utilisée pour négocier les paramètres E_Mode-2. Voir Figure 11 et Tableau 10.

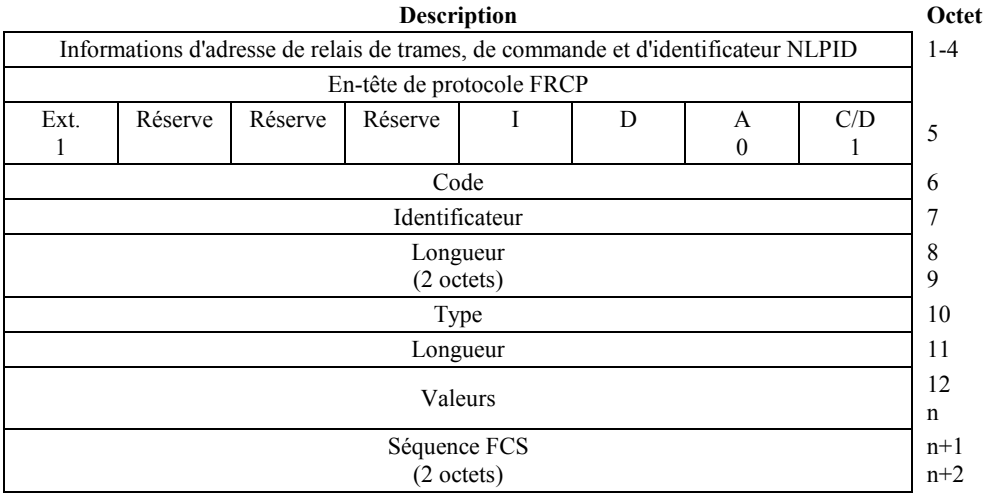


Figure 11/X.272 – Trame E_Mode-2 de commande FRCP

Tableau 10/X.272 – Trame de commande E_Mode-2

Champ	Description
DLCI, commande et identificateur NLPID	Voir 8.1 pour les détails
En-tête FRCP	• Ext.: bit d'extension mis à 1 • Réserve: bit de réserve mis à 0 • ID (2 bits) mis à 11 • Bit d'authentification (A) = 0 • Bit de commande/données (C/D) mis à 1
Code	Voir IETF RFC 1661 section 5: formats de paquet LCP et IETF RFC 1968 section 3: paquets additionnels (valeurs indiquées en notation décimale)
Identificateur	Voir IETF RFC 1661 section 5: formats de paquet LCP et IETF RFC 1968 section 3: paquets additionnels
Longueur (2 octets)	Voir IETF RFC 1661 section 5: formats de paquet LCP et IETF RFC 1968 section 3: paquets additionnels Y compris: données de code, d'identificateur, de longueur et de toutes options de configuration

Tableau 10/X.272 – Trame de commande E_Mode-2 (*fin*)

Champ	Description
Type	Voir IETF RFC 1968 section 4: options de configuration ECP, 4.1: identificateur OUI de cryptage non normalisé et 4.2: types de cryptage disponibles à titre public. Dans la présente Recommandation, le type 254 (décimal) est un champ réservé qui indique le mode E_Mode-1 du FRCP. En outre, les types 245 à 253 inclusivement ainsi que le type 255 sont réservés.
Longueur	Option de longueur de configuration y compris champs de type, longueur et valeur
Valeurs	Zéro ou plus que zéro octet, contenant des données selon détermination par les options de configuration définies dans l'IETF RFC 1968 section 4
FCS	Séquence de contrôle de trame Q.922

10.2.2 Négociation du cryptage E_Mode-2

Le mode E_Mode-2 du protocole de secret en relais de trames encapsule le même mécanisme d'échange de paquets que le protocole ECP de liaison PPP (IETF RFC 1968) [14] qui est à son tour modélisé sur le protocole LCP de liaison PPP (IETF RFC 1661) [13]. Le mode E_Mode-2 doit faire appel aux procédures décrites dans les 3.1 et 4.3 du IETF RFC 1968 au moyen des formats de trame décrits au 8.2. Les exceptions suivantes s'appliquent aux 3.1 et 4.3 du IETF RFC 1968 [14] et à la section 4 du IETF RFC 1661, citée en référence:

- si un message Config-Req est reçu à un moment quelconque, le dispositif récepteur commence la négociation du mode E_Mode-1;
- une entité peut abandonner le mode E_Mode-2 et entrer à tout moment dans la phase d'initialisation du mode E_Mode-1;
- si une entité qui prend en charge le mode E_Mode-2 se trouve en mode E_Mode-1 et reçoit une demande de configuration en mode E_Mode-2, cette entité peut commencer la négociation du mode E_Mode-2.

NOTE – Les événements de montée et de descente (dans les couches inférieures) de l'automate doivent être produits par le statut de connexion virtuelle indiqué par les protocoles de signalisation de connexion PVC ou SVC. Les paquets E_Mode-2 reçus avant cette phase doivent être ignorés. Avant tout échange de données cryptées, l'entité doit arriver à l'état f_1.

10.2.3 Transfert de données E_Mode-2

Ce format est utilisé pour transférer des données chiffrées en mode E_Mode-2. Il est analogue au format E_Mode-1 décrit dans la Figure 9 et dans le Tableau 9 ci-dessus.

11 Ressources de compression des données

La ressource de compression des données est chargée d'activer et de lancer les algorithmes de compression des données aux deux extrémités de la liaison. La compression des données utilise un mécanisme d'échange de paquets similaire au protocole de commande de liaison PPP (LCP, *link control protocol*) [13]. L'utilisation de la ressource de cryptage est négociée entre dispositifs homologues. Le mode et les algorithmes sont sélectionnés indépendamment pour chaque sens d'une connexion virtuelle. Le protocole de commande FRCP assure les services de compression de données ci-après:

– encapsulation des données d'utilisateur codées et des primitives de négociation à l'intérieur d'unités de données protocolaires FRCP (PDU, *protocol data unit*) pour le transport entre utilisateurs FRCP;

– négociation d'options de configuration FRCP;
– synchronisation des entités homologues d'expédition et de réception, y compris ce qui suit:
  • détection des pertes de synchronisme et signalisation pour la resynchronisation entre homologues;
  • protection anti-expansion permettant la signalisation du mode comprimé/non comprimé entre le codeur et le décodeur homologue;
  • codage de données d'utilisateur en données d'utilisateur comprimées conformément à un ou plusieurs d'une série d'algorithmes publics ou privés;
  • décodage de données d'utilisateur comprimées en données d'utilisateur non comprimées.

La présente Recommandation prend en charge la négociation d'algorithmes facultatifs de compression de données, publics ou privés. Les détails des algorithmes privés doivent être publiés par les vendeurs dans les documents relatifs à la description de la fonction de compression des données (DCFD). La description DCFD, associée à la présente Recommandation, suffit pour assurer l'interfonctionnement du protocole FRCP entre constructeurs.

11.1 Encapsulation de la compression de données par l'algorithme C_Mode-1

Pour les implémentations comportant la ressource de compression de données, la prise en charge du mode C_Mode-1 est obligatoire. Ce mode consiste en un simple dialogue permettant d'activer l'algorithme de compression de données par défaut et ses paramètres dans les deux sens de la connexion virtuelle. L'algorithme de compression de données par défaut est tel que décrit en [20].

11.1.1 Format des trames de commande C_Mode-1

Cette trame est utilisée pour négocier des paramètres C_Mode-1. Voir Figure 12 et Tableau 11.

Description								Octet
Adresse Q.922 (2 octets) (Note)								1 2
Commande (UI: 0x03)								3
Identificateur NLPID (0xB0)								4
En-tête FRCP								
Ext. 1	Réserve	Réserve	Réserve	I	D	A	C/D 1	5
Code								6
Identificateur								7
Longueur (2 octets)								8 9
Type								10
Longueur								11
Révision								12
FCS (2 octets)								13 14

NOTE – Cette adresse de relais de trames à 2 octets n'est montrée ici qu'à titre d'illustration. Les formats d'adresse à 3 et 4 octets ne sont pas interdits.

Figure 12/X.272 – Trame de commande C_Mode-1

Tableau 11/X.272 – Trame de commande C_Mode-1

Champ	Description
Adresse Q.922	Voir 8.1 pour les détails
Commande	Voir 8.1 pour les détails
Identificateur NLPID	Voir 8.1 pour les détails
En-tête FRCP	L'en-tête du protocole FRCP se compose de ce qui suit: • Ext.: Le bit d'extension doit être mis à 1 • Réserve: bit de réserve pour usage futur, mis à 0 • ID (2 bits) mis à 01 • Bit d'authentification (A) – mis à 0 • Bit de commande/données (C/D) – mis à 1
Code	Mis à 1 pour demande de configuration (Config-Req) Mis à 2 pour acquittement de configuration (Config_Ack)
Identificateur	Numéro de transaction pour corréler une demande avec une réponse. Envoyé dans une demande et renvoyé en écho dans la réponse correspondante
Longueur	Deux octets en longueur. La valeur est mise à 7, qui comprend le nombre total d'octets des trames sauf: adresse Q.922, commande, identificateur NLPID et en-tête FRCP
Type	254 décimal – indique C_Mode-1 Les types 245 à 253 inclusivement ainsi que le type 255 sont réservés.
Longueur d'option de configuration	Mis à décimal 3 pour indiquer la longueur des champs de type, de longueur d'option de configuration et de révision
Révision	La révision actuelle doit être mise à 1
Charge utile FRCP	Informations de commande ou données de transfert selon la façon dont les bits d'en-tête FRCP bits sont positionnés
FCS	Séquence de contrôle de trame Q.922

11.1.2 Procédures de commande C_Mode-1

La compression de données FRCP dans le mode C_Mode-1 constitue un protocole de négociation simple offrant un service de compression de données avec l'algorithme et les valeurs paramétriques par défaut. Une fois le protocole FRCP correctement négocié, le transfert de données vers le système d'extrémité homologue peut être comprimé. Pour désactiver le protocole FRCP, une implémentation peut forcer la connexion virtuelle à l'état d'inactivité ou envoyer une demande C_Mode-1 et ne pas envoyer de réponse C_Mode-1.

11.1.2.1 Etats C_Mode-1

Comme au 10.1.3.1.

11.1.2.2 Demande d'initialisation C_Mode-1

Comme au 10.1.3.2.

11.1.2.3 Réception d'une demande de configuration

Comme au 10.1.3.3.

11.1.2.4 Phase d'état opérationnel

Comme au 10.1.3.4.

11.1.2.5 Phase de désactivation

Comme au 10.1.3.5.

11.1.3 Formats de transfert des données C_Mode-1

Le présent paragraphe décrit la méthode d'encapsulation pour la compression de données FRCP lorsque seule l'option de compression de données est activée. Le présent paragraphe décrit également les procédures d'anti-expansion et de synchronisation.

Le format général de trame est décrit dans la Figure 13, où le bit C/D de l'en-tête FRCP est mis à 0 pour indiquer qu'il s'agit d'une trame de données. Les bits C/U, RA et RR sont utilisés pour les procédures d'anti-expansion et de synchronisation.

11.1.3.1 Format de signalisation d'anti-expansion

La signalisation d'anti-expansion (C/U) peut être fournie par le codeur au décodeur dans un seul sens de la connexion de compression de données FRCP afin d'indiquer si la charge utile FRCP associée est comprimée ou non. L'expéditeur doit mettre le bit C/U = 1 lorsque le codage de compression a été effectué sur les données d'utilisateur. L'expéditeur doit mettre le bit C/U = 0 lorsque le codage de compression n'a pas été appliqué aux données d'utilisateur. Lorsque C/U = 1, le décodeur doit décoder la charge utile FRCP. Lorsque C/U = 0, le décodeur ne doit pas décoder la charge utile FRCP. Il ne doit pas y avoir de champ de numéro de séquence ou d'octet LCB lorsque le bit C/D est mis à "0".

L'implémentation du mode C_Mode-1 selon la révision actuelle nécessite que le codeur comprime chaque trame de données même si une expansion de données s'est produite. L'algorithme LZS assure une expansion minimale des données, dont les détails se trouvent en [20]. L'implémentation du mode C_Mode-1 implique que la connexion soit réglée de façon à traiter une longueur de trame maximale comportant le scénario du cas le moins favorable d'expansion des données.

11.1.3.2 Format de signalisation de synchronisation

Le protocole FRCP offre des procédures de synchronisation permettant une reprise sur perte de synchronisme entre homologues FRCP. Le relais de trames n'assure pas un transport fiable des unités PDU du protocole FRCP. Les décodeurs à fonction FRCP n'assurent généralement pas la reprise sur décompression d'unités PDU perdues, erronées ou déplacées. Ils propagent les erreurs de manière catastrophique jusqu'à ce qu'ils soient réinitialisés à un état connu. Dans la présente Recommandation, le numéro de séquence et l'octet LCB sont utilisés pour détecter une perte de synchronisme. La signalisation de synchronisation est assurée entre homologues FRCP au moyen des bits RR et RA contenus dans l'en-tête d'unité PDU des données FRCP. Les bits RR et RA peuvent aussi être signalés au moyen d'un en-tête FRCP sans charge utile FRCP jointe (voir Figure 14). Des signaux RR et RA sont émis séparément pour permettre une resynchronisation indépendante d'un des deux sens ou des deux sens d'une connexion FRCP.

Le décodeur détermine la perte de synchronisme lorsqu'il reçoit une trame possédant un numéro de séquence erroné et/ou un octet LCB erroné. Si le décodeur détecte une perte de synchronisme dans le sens distant-local de la connexion FRCP, il doit insérer un signal RR mis à "1" dans une nouvelle unité PDU vide de données FRCP ou dans l'unité PDU suivante de données FRCP contenant des données d'utilisateur destinées à l'homologue FRCP distant. Une fois qu'un signal RR mis à "1" a été émis, toute unité PDU de données FRCP, reçue dans le sens distant-local de ce contexte FRCP et contenant des données d'utilisateur comprimées (bit C/U = 1), doit être rejetée jusqu'à ce qu'un signal RA mis à "1" soit reçu pour ce contexte. Le signal RR mis à "1" peut être répété afin d'augmenter la fiabilité. Si un récepteur détecte un signal RR mis à "1" dans le sens distant-local, il doit réinitialiser son codeur à un état connu. Le codeur doit insérer un signal RA mis à "1" dans une nouvelle unité PDU vide de données FRCP ou dans l'unité PDU suivante de données FRCP contenant des données d'utilisateur destinées à l'homologue FRCP local. Lorsqu'un récepteur FRCP local reçoit un signal RA mis à "1" dans le sens distant-local du contexte FRCP, il doit réinitialiser à un état connu son historique pour ce contexte. Le récepteur FRCP local doit décoder d'éventuelles données d'utilisateur dans l'unité PDU de données FRCP contenant le bit RA mis à "1" et dans tous les unités PDU de données FRCP subséquentes jusqu'à ce qu'une autre perte de synchronisme soit détectée.

Le bit C/U doit être mis à "0" dans les trames de synchronisation FRCP (lorsque le bit RA ou RR est activé). Par ailleurs, toute trame de synchronisation FRCP doit contenir un numéro de séquence valide. Dès détection d'un bit RA activé, le décodeur doit réinitialiser son numéro de séquence actuel à celui qui a été reçu de la trame de synchronisation. Cela permet de calculer modulo 256 le prochain numéro de séquence attendu à partir du numéro de séquence reçu.

Pour assurer la synchronisation initiale entre deux homologues après négociation correcte du mode C_Mode-1 entre deux entités homologues, le codeur doit mettre le bit RA à "1" dans la première unité PDU afin d'indiquer que l'historique se trouve dans un état connu. Le décodeur doit négliger toutes les trames comprimées jusqu'à ce qu'il détecte une telle trame. Pour augmenter la fiabilité, le décodeur doit émettre une demande de réinitialisation à destination du codeur distant.

11.1.3.3 Charge utile de compression de données C_Mode-1

Le contenu de la charge utile FRCP doit être un nombre entier d'octets. Le format de la charge utile FRCP est indiqué ci-dessous. Voir Figure 13 et Tableau 12.

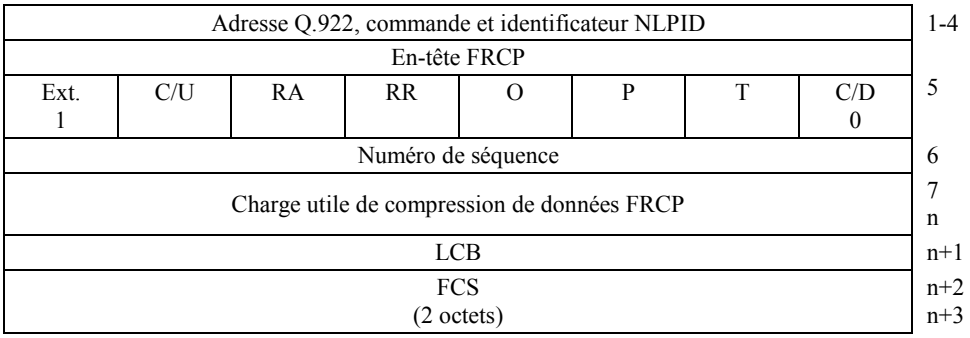


Figure 13/X.272 – Trame de transfert de données C_Mode-1

Tableau 12/X.272 – Trame de données C_Mode-1

Champ	Description
Adresse Q.922	Voir 8.1 pour les détails
Commande	Voir 8.1 pour les détails
Identificateur NLPID	Voir 8.1 pour les détails
Numéro de séquence	Initialisé à 1 et incrémenté modulo 256 après chaque trame NOTE 1 – Cet octet est postposé à la fin de la charge utile comprimée. Cet octet ne doit jamais être comprimé
En-tête FRCP	L'en-tête du protocole FRCP se compose de ce qui suit: • ext.: le bit d'extension doit être mis à 1, mais inclus pour amélioration future • comprimées/non comprimées (C/U): mis à 1 pour indiquer que les données ne sont pas comprimées • Reset_Ack (RA): non applicable, mis à 0 • Reset_Request (RR): non applicable, mis à 0 • option de protocole (OPT): Mis à: O P T 0 1 1 pour spécifier la compression • bit de commande/données (C/D): mis à 0 pour indiquer une trame de données

Tableau 12/X.272 – Trame de données C_Mode-1 (*fin*)

Champ	Description
Charge utile de compression de données	Trame selon Annexe E/Q.933 qui est comprimée
Numéro de séquence	Initialisé à 1 et incrémenté modulo 256 après chaque trame NOTE 2 – Cet octet est postposé à la fin de la charge utile comprimée Cet octet ne doit jamais être comprimé
LCB	Octet LCB calculé sur les données originales d'utilisateur y compris le numéro de séquence. L'octet LCB n'est pas comprimé
FCS	Séquence de contrôle de trame Q.922

Le contenu d'une unité PDU vide est décrit dans la Figure 14:

Adresse Q.922, commande et identificateur NLPID								1-4
En-tête FRCP								
Ext. 1	C/U	RA	RR	O	P	T	C/D 0	5
Numéro de séquence								6
FCS (2 octets)								7 8

Figure 14/X.272 – Unité PDU vide du protocole FRCP

11.2 Encapsulation de la compression de données par l'algorithme C_Mode-2

La prise en charge du mode C_Mode-2 est facultative. Ce mode opérationnel de compression de données offre la capacité de négociation des descriptions DCFD et de leurs paramètres associés.

11.2.1 Format des trames de commande C_Mode-2

Cette trame est utilisée pour négocier les paramètres C_Mode-2. Voir Figure 15 et Tableau 13.

Description								Octet
Adresse Q.922 (2 octets) (Note)								1 2
Commande (UI: 0x03)								3
Identificateur NLPID (0xB0)								4
En-tête FRCP								
Ext. 1	Réserve	Réserve	Réserve	I	D	A	C/D 1	5
Code								6
Identificateur								7
Longueur (2 octets)								8 9
Type								10
Longueur d'option de configuration								11
OUI (3 octets)								12 13 14
Sous-type								15
Valeurs								16
FCS (2 octets)								17 18

NOTE – Cette adresse de relais de trames à 2 octets n'est montrée ici qu'à titre d'illustration. Les formats d'adresse à 3 et 4 octets ne sont pas interdits.

Figure 15/X.272 – Trame de commande C_Mode-2

Tableau 13/X.272 – Trame de commande C_Mode-2

Champ	Description
Adresse Q.922	Voir 8.1 pour les détails
Commande	Voir 8.1 pour les détails
Identificateur NLPID	Voir 8.1 pour les détails
En-tête FRCP	L'en-tête du protocole FRCP se compose de ce qui suit: • Ext.: le bit d'extension doit être mis à 1 • Réserve: bit de réserve pour usage futur, mis à 0 • ID (2 bits) mis à 01 • Bit d'authentification (A) – mis à 0 • Bit de commande/données (C/D) – mis à 1
Code	Mis à 1 pour Config_Req Mis à 2 pour Config_Ack
Identificateur	Numéro de transaction pour corréler une demande avec une réponse. Envoyé dans une demande et renvoyé en écho dans la réponse correspondante
Longueur	Deux octets en longueur. La valeur est mise à 7, qui comprend le nombre total d'octets des trames sauf: adresse Q.922, commande, identificateur NLPID, et en-tête FRCP

Tableau 13/X.272 – Trame de commande C_Mode-2 (*fin*)

Champ	Description
Type	0 C_Mode-2 23 LZS 254 FRCP C_Mode-1 Les types 245 à 253 inclusivement ainsi que le type 255 sont réservés. Les nombres sont en notation décimale
Longueur d'option de configuration	Mis à 6 plus le nombre d'octets dans le champ de valeurs
OUI	Identificateur unique d'organisation (OUI, *organization unique identifier*) du vendeur selon l'IEEE
Sous-type	Utilisé pour sélectionner de multiples descriptions DCFD issues d'un vendeur spécifique
Valeurs	Doit être zéro ou plus que zéro octet. Peut contenir des données additionnelles pour chaque protocole de vendeur, et peut inclure l'option d'utiliser des historiques multiples pour chaque connexion
FCS	Séquence de contrôle de trame Q.922

11.2.2 Message de commande C_Mode-2

Le mode C_Mode-2 du protocole FRCP permet la négociation de descriptions DCFD propres au vendeur. Cette négociation est fondée sur les formats de paquet LCP définis dans la section 5 du document IETF RFC 1661 [13] avec un ensemble unique d'options de configuration. Les paquets LCP possédant les codes 1 à 7 sont requis. Les autres paquets LCP spécifiés dans le document IETF RFC 1661 sont facultatifs.

Les séquences codées des options de configuration FRCP, qui sont actuellement assignées, se présentent comme suit:

option de configuration

23 LZS

254 FRCP C_Mode-1

255 valeur réservée pour utilisation future

Le mode C_Mode-2 doit utiliser l'automate à états finis qui est décrit dans les sections 3 et 4 du document IETF RFC 1661 [13] avec les exceptions suivantes:

1) si l'automate à états finis FRCP de négociation C_Mode-2 entre dans l'état f_0 en raison d'une expiration de la temporisation de négociation et/ou en raison d'un dépassement de la valeur d'un compteur, l'entité doit entrer dans la phase d'initialisation C_Mode-1;

2) une entité peut abandonner le mode C_Mode-2 et entrer à tout moment dans la phase d'initialisation C_Mode-1;

3) si une entité fonctionnant en mode C_Mode-2 reçoit une demande C_Mode-1 à un moment donné, elle doit entrer dans la phase d'initialisation C_Mode-1;

4) si une entité qui prend en charge le mode C_Mode-2 se trouve en mode C_Mode-1 et reçoit une demande de configuration C_Mode-2, cette entité peut commencer la négociation C_Mode-2.

Avant que d'éventuelles unités PDU de données FRCP puissent être communiquées, le protocole FRCP doit arriver à l'état f_1.

12 Ressources de compression sécurisée de données

La ressource de compression sécurisée de données est chargée d'activer et de lancer des algorithmes de compression sécurisée de données aux deux extrémités de la liaison. La compression sécurisée de données fait appel à un mécanisme d'échange de paquets analogue au protocole de commande de liaison PPP (LCP, *link control protocol*). L'utilisation de la ressource de compression sécurisée de données est négociée entre dispositifs homologues. Le mode et les algorithmes sont choisis indépendamment pour chaque sens d'une connexion virtuelle. Le protocole FRCP prend en charge la description de fonction de compression de données (DCFD) qui est définie dans des documents séparés ce qui, en association avec la présente Recommandation, suffit pour assurer l'interfonctionnement du protocole FRCP entre constructeurs offrant la même fonction FRCP. Le protocole FRCP assure la prise en charge des procédures de détection de perte de synchronisme et de resynchronisation.

12.1 Encapsulation de la compression de données S_Mode-1

La prise en charge du mode S_Mode-1 est obligatoire pour les configurations d'utilisateur dont la ressource de compression sécurisée de données est activée. La négociation du mode S_Mode-1 consiste en un simple dialogue afin d'activer l'algorithme de compression sécurisée (SCA, *secure compression algorithm*) par défaut des données et ses paramètres associés pour chaque sens de la connexion virtuelle.

L'algorithme de compression de données par défaut est l'algorithme FZA qui est décrit en [17] et qui utilise un chiffrement de flux par suite de clés afin de mettre à jour de manière aléatoire son modèle interne de compression de données. L'utilisation du chiffrement de flux nécessite une clé de cryptage ou un germe initial pour calculer cette clé. L'échange de clés et la procédure de mise à jour sont hors du domaine d'application de la présente Recommandation. Par ailleurs, comme les algorithmes de compression de données traditionnels, l'algorithme FZA exige que les dictionnaires de l'expéditeur et du récepteur restent synchronisés. L'algorithme FZA chiffrera les données si l'option de compression sécurisée est désactivée.

12.1.1 Format des trames de commande S_Mode-1

Les trames utilisées pour négocier les paramètres S_Mode-1 sont analogues à celles du format indiqué dans la Figure 6 avec les bits Ext. et C/D de l'octet d'en-tête FRCP mis à 1. La valeur du champ d'identificateur dans l'en-tête FRCP doit être mis à 10. La valeur du champ de type dans la trame est mise à la valeur décimale 254.

12.1.2 Procédures de commande S_Mode-1

Comme au 10.1.1.

12.1.2.1 Eléments paramétriques S_Mode-1

Comme au 10.1.1.1.

12.2 Format de transfert des données S_Mode-1

Le présent paragraphe décrit la méthode d'encapsulation pour la compression sécurisée de données FRCP en tant que seule ressource configurée. Par ailleurs, le présent paragraphe décrit les procédures d'anti-expansion et de synchronisation. Le format général de trame est décrit dans la Figure 16, où le bit C/D de l'en-tête FRCP est mis à 0 pour indiquer qu'il s'agit d'une trame de données. Les bits C/U, RA et RR sont utilisés pour les procédures d'anti-expansion et de synchronisation.

12.2.1 Format de signalisation d'anti-expansion

La signalisation d'anti-expansion (C/U) doit être fournie par le codeur au décodeur dans un seul sens de la connexion de compression de données FRCP afin d'indiquer si la charge utile FRCP associée est comprimée avec sécurisation ou non. L'expéditeur doit mettre le bit C/U = 1 lorsque le codage de compression sécurisée a été effectué sur les données d'utilisateur. Lorsque C/U = 1, le décodeur doit décoder la charge utile de compression sécurisée FRCP.

L'expéditeur peut mettre le bit C/U = "0" lorsque le codage de compression sécurisée n'a pas été effectué sur les données d'utilisateur. Cependant, les données doivent être cryptées au moyen du mode de cryptage FZA avant de les envoyer sur la liaison. Sinon, les données doivent toujours être comprimées avec sécurisation avant d'être envoyées sur la liaison même si une expansion de données s'est produite. Lorsque le bit C/U = 0, le décodeur sécurisé doit décrypter la charge utile FRCP cryptée au moyen du mode de cryptage FZA. Le champ de numéro de séquence doit être crypté et inséré dans l'unité PDU du protocole FRCP. Par ailleurs, le champ d'octet LCB doit être présent.

12.2.1.1 Format de signalisation de synchronisation

Comme au 11.1.3.2.

12.2.1.2 Charge utile de données FRCP en mode S_Mode-1

Le contenu de la charge utile FRCP est défini conformément à la description DCFD. La charge utile FRCP doit toujours avoir un nombre entier d'octets. Voir Figure 16 et Tableau 14.

Adresse Q.922, commande et identificateur NLPID								1-4
En-tête FRCP								
Ext. 1	C/U	RA	RR	O	P	T	C/D 0	5
Charge utile de compression sécurisée de données FRCP								6
Numéro de séquence								n
LCB								n+1
FCS (2 octets)								n+2 n+3

Figure 16/X.272 – Trame de transfert de données S_Mode-1

Tableau 14/X.272 – Trame de données S_Mode-1

Champ	Description
Adresse Q.922	Voir 8.1 pour les détails
Commande	Voir 8.1 pour les détails
Identificateur NLPID	Voir 8.1 pour les détails
En-tête FRCP	L'en-tête du protocole FRCP se compose de ce qui suit: • Ext.: le bit d'extension doit être mis à 1 • Comprimées/non comprimées (C/U) • Reset_Ack (RA) • Reset_Request (RR) • Option de protocole (OPT): mis à: O P T 0 1 0 pour spécifier la compression sécurisée • Bit de commande/données (C/D): mis à 0 pour indiquer une trame de données
Charge utile de compression de données	Trame selon Annexe E/Q.933 qui est comprimée
Numéro de séquence	Initialisé à 1 et incrémenté modulo 256 après chaque trame NOTE – Cet octet est postposé aux données d'utilisateur et est comprimé avec sécurisation
LCB	Octet LCB calculé sur les données originales d'utilisateur y compris le numéro de séquence
FCS	Séquence de contrôle de trame Q.922

12.3 Encapsulation de la compression de données S_Mode-2

La prise en charge du mode S_Mode-2 est facultative. Elle permet d'activer ou désactiver le protocole FRCP et de négocier des descriptions DCFD avec leurs paramètres associés.

12.3.1 Format des trames de commande S_Mode-2

Cette trame est utilisée pour négocier des paramètres S_Mode-2. Voir Figure 17 et Tableau 15.

Description								Octet
Adresse Q.922 (2 octets) (Note)								1 2
Commande (UI: 0x03)								3
Identificateur NLPID (0xB0)								4
En-tête FRCP								
Ext. 1	Réserve	Réserve	Réserve	I	D	A	C/D 1	5
Code								6
Identificateur								7
Longueur (2 octets)								8 9
Type								10
Longueur d'option de configuration								11
OUI (3 octets)								12 13 14
Sous-type								15
Valeurs								16
FCS (2 octets)								17 18

NOTE – Cette adresse de relais de trames à 2 octets n'est montrée ici qu'à titre d'illustration. Les formats d'adresse à 3 et 4 octets ne sont pas interdits.

Figure 17/X.272 – Trame de commande S_Mode-2

Tableau 15/X.272 – Trame de commande S_Mode-2

Champ	Description
Adresse Q.922	Voir 8.1 pour les détails
Commande	Voir 8.1 pour les détails
Identificateur NLPID	Voir 8.1 pour les détails
En-tête FRCP	L'en-tête du protocole FRCP se compose de ce qui suit: • Ext.: le bit d'extension doit être mis à 1 • Réserve: le bit de réserve doit être mis à 0 • ID (2 bits) mis à "10" • Bit d'authentification (A) – mis à 0 • Bit de commande/données (C/D) – mis à 1
Code	Mis à 1 pour Config_Req Mis à 2 pour Config_Ack
Identificateur	Numéro de transaction pour corréler une demande avec une réponse. Envoyé dans une demande et renvoyé en écho dans la réponse correspondante
Longueur	Deux octets en longueur. La valeur est mise à 7, qui comprend le nombre total d'octets des trames sauf: adresse Q.922, commande, identificateur NLPID et en-tête FRCP
Type	0 S_Mode-2 254 FRCP S_Mode-1 Les types 245 à 253 inclusivement ainsi que le type 255 sont réservés. Nombres en notation décimale

Tableau 15/X.272 – Trame de commande S_Mode-2 (*fin*)

Champ	Description
Longueur d'option de configuration	Mis à 6 plus le nombre d'octets dans le champ de valeurs
OUI	Identificateur unique d'organisation (OUI) du vendeur
Sous-type	Utilisé pour choisir entre de multiples descriptions DCFD privées issues d'un vendeur spécifique
Valeurs	Doit être zéro ou plus que zéro octet. Peut contenir des données additionnelles pour chaque protocole de vendeur et peut inclure l'option d'utiliser des historiques multiples pour chaque connexion
FCS	Séquence de contrôle de trame Q.922

12.3.2 Message de commande S_Mode-2

Le mode S_Mode-2 du protocole FRCP permet la négociation de descriptions DCFD propres aux vendeurs. Cette négociation est fondée sur les formats de paquet LCP définis dans la section 5 de l'IETF RFC 1661 [13]. Les détails sont analogues aux spécifications E_Mode-2 indiquées dans le 10.2.

Le mode S_Mode-2 doit utiliser l'automate à états finis décrit dans les sections 3 et 4 de l'IETF RFC 1661 [13] avec les exceptions suivantes:

1) si l'automate à états finis FRCP de négociation S_Mode-2 entre dans l'état f_0 en raison d'une expiration de la temporisation de négociation et/ou en raison d'un dépassement de la valeur d'un compteur, l'entité doit entrer dans la phase d'initialisation S_Mode-1;
2) une entité peut abandonner le mode S_Mode-2 et entrer à tout moment dans la phase d'initialisation S_Mode-1;
3) si une entité fonctionnant en mode S_Mode-2 reçoit une demande S_Mode-1 à un moment donné, elle doit entrer dans la phase d'initialisation S_Mode-1;
4) si une entité qui prend en charge le mode S_Mode-2 se trouve en mode S_Mode-1 et reçoit une demande de configuration S_Mode-2, cette entité peut commencer la négociation S_Mode-2.

13 Encapsulation du transfert de données FRCP par ressources multiples

Le présent paragraphe décrit le format des trames de données FRCP lorsque de multiples ressources sont configurées et négociées correctement.

13.1 Cryptage et données de compression sécurisée de données

Le présent paragraphe décrit l'encapsulation de trames impliquant l'utilisation des ressources de compression sécurisée et de cryptage. Les algorithmes utilisés sont ceux qui sont adoptés pour les modes de fonctionnement E_Mode-1 et S_Mode-1. Le traitement du vecteur d'initialisation (IV) pour le mode E_Mode-1 est décrit au 10.1.1.1.

Pour les implémentations dont les options de cryptage et de compression sécurisée sont configurées et négociées correctement, les données d'utilisateurs sont d'abord comprimées avec sécurisation au moyen de l'algorithme SCA du mode S_Mode-1. Un octet LCB doit être calculé d'après les données d'utilisateur brutes et originales. Cet octet LCB est postposé à la fin des données comprimées avec sécurisation, comme indiqué ci-dessous:

Description	Octet
Données d'utilisateur comprimées avec sécurisation	1 k
Octet LCB calculé sur les données d'utilisateur brutes et originales	k+1

Les données comprimées et l'octet LCB (soit k + 1 octets) sont ensuite traitées en tant que nouvelles données d'utilisateur devant être chiffrées par le crypteur. Celui-ci doit effectuer le bourrage des données jusqu'au plus proche multiple de 8 octets comme décrit au 10.1.2 avant de les chiffrer. Un octet LCB est calculé sur les (k + 1 octets) des données comprimées avec sécurisation ainsi que sur l'octet LCB, les octets de bourrage et l'octet de longueur de bourrage, avant la phase de cryptage. Les données sont ensuite cryptées et un numéro de séquence est calculé puis inséré dans la trame comme décrit sur la Figure 18. L'expéditeur incrémente le numéro de séquence modulo 256 puis postpose l'octet LCB à la charge utile et envoie la trame sur la liaison.

A l'extrémité réceptrice, le récepteur commence par vérifier le numéro de séquence pour déterminer si une trame a été perdue. Si tel est le cas, les 8 derniers octets du cryptogramme sont conservés comme vecteur initial pour la trame suivante et la trame reçue est rejetée. Une demande de réinitialisation doit être envoyée à l'homologue expéditeur pour demander que l'historique de compression soit réinitialisé, ce qui s'effectue par un réglage des bits RR et RA conformément aux paragraphes pertinents. Aucune donnée ne doit être fournie au décodeur par le décrypteur avant la réception de l'acquittement de la réinitialisation, en provenance de l'homologue expéditeur.

Si la trame est en séquence, le récepteur déchiffre les champs indiqués dans la Figure 9 et calcule l'octet LCB. Celui-ci est alors comparé à l'octet LCB reçu. S'il n'y a pas concordance, les 8 derniers octets des données sont conservés en tant que vecteur initial pour la trame suivante et la trame reçue est rejetée. Une demande de réinitialisation doit être envoyée à l'homologue expéditeur afin que l'historique de compression sécurisée soit réinitialisé. A cette fin, les bits RR et RA sont réglés comme indiqué dans les paragraphes correspondants. Aucune donnée ne doit être fournie au décodeur par le décrypteur tant qu'un acquittement de réinitialisation n'a pas été reçu de l'homologue expéditeur. Si les octets LCB concordent, les données déchiffrées sont traitées par extraction du numéro de séquence du bourrage, de l'octet de longueur de bourrage et de l'octet LCB. Les données sont ensuite renvoyées au décodeur qui exécute une phase de décompression sécurisée. Le décodeur calcule l'octet LCB d'après les données décomprimées. Si les octets LCB concordent, le décodeur fait suivre les données vers la couche supérieure. Si aucun octet LCB ne concorde, une demande de réinitialisation doit être envoyée à l'homologue expéditeur pour demander la réinitialisation de l'historique de compression sécurisée. A cette fin, les bits RR et RA sont réglés comme décrit dans les paragraphes pertinents. Aucune donnée ne doit être fournie au décodeur par le décrypteur tant qu'un acquittement de réinitialisation n'a pas été reçu de l'homologue expéditeur.

Pendant que le décrypteur attend de recevoir un acquittement de réinitialisation en provenance de l'expéditeur pour indiquer que les historiques sont synchronisés, le décrypteur doit conserver les 8 derniers octets du cryptogramme en tant que vecteur initial pour la prochaine trame et la trame reçue est ignorée.

Lorsque l'option de compression sécurisée est combinée avec l'option de cryptage, les données doivent toujours être acheminées par l'intermédiaire du comprimeur sécurisé et du crypteur parce que l'algorithme FZA cryptera les données si l'option de compression est désactivée. Quelle que soit la valeur du bit C/U dans l'en-tête FRCP, le décrypteur doit donc fournir au décodeur sécurisé les données relatives aux trames possédant un numéro de séquence et un octet LCB corrects. Voir également le Tableau 16.

Description								Octet
Informations d'adresse de relais de trames, de commande et d'identificateur NLPID								1-4
En-tête FRCP								
Ext. 1	Réserve	Réserve	Réserve	I	D	A	C/D 0	5
Numéro de séquence								6
Données d'utilisateur comprimées avec sécurisation (Note) (k + 1 octets)								7 m
Bourrage (Note)								m n-1
Longueur de bourrage (Note)								n
LCB								n+1
FCS (2 octets)								n+2 n+3

NOTE – Ce champ est crypté.

Figure 18/X.272 – Format de trame de transfert de données comprimées avec sécurisation et cryptées

Tableau 16/X.272 – Format de trame de transfert de données comprimées avec sécurisation et cryptées

Champ	Description
DLCI, commande et identificateur NLPID	Voir 8.1 pour les détails
En-tête FRCP	L'en-tête du protocole FRCP se compose de ce qui suit: • Ext.: le bit d'extension doit être mis à 1 • Comprimées/non comprimées (C/U): mis à 1 pour indiquer que les données ne sont pas comprimées • Reset_Ack (RA): mis à 1 par l'expéditeur si celui-ci acquitte la demande de réinitialisation issue de l'homologue distant • Reset_Request (RR): mis à 1 par le récepteur si la resynchronisation de la compression sécurisée est requise • Option de protocole (OPT): Mis à: O P T 1 0 1 pour spécifier le cryptage • Bit de commande/données (C/D): mis à 0 pour indiquer une trame de données
Numéro de séquence	Numéro assigné par le crypteur en commençant la séquence par 0 et en l'incrémentant modulo 256
Données d'utilisateur	Les données d'utilisateur sont d'abord comprimées avec sécurisation, puis cryptées. Les données doivent être d'abord décryptées puis décodées

Tableau 16/X.272 – Format de trame de transfert de données comprimées avec sécurisation et cryptées *(fin)*

Champ	Description
Bourrage	Voir 10.1.2
Longueur de bourrage	Voir 10.1.2
LCB	Octet de vérification longitudinale – calculé sur le texte comprimé des octets 7 à n
FCS	Séquence de contrôle de trame Q.922

Le numéro de séquence et l'octet LCB sont produits par le crypteur. Les octets 8 à m sont injectés dans le décodeur. Dès détection d'une perte de synchronisme due à un numéro de séquence ou octet LCB erroné, les historiques de compression doivent être resynchronisés par réglage des bits RR et RA comme indiqué dans les paragraphes pertinents.

13.2 Cryptage et données comprimées

Si les ressources de compression et de cryptage des données sont configurées et négociées correctement, les données d'utilisateur sont d'abord comprimées puis cryptées. Le processus est analogue à celui du 11.1 sauf que, lorsque le bit C/U est réglé de façon à indiquer l'absence de compression, les données ne sont pas réexpédiées vers le décodeur.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données et communication entre systèmes ouverts**
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects informatiques généraux des systèmes de télécommunication

Genève, 2001