Groupe de travail Réseau
Request for Comments : 4172
Catégorie : Sur la voie de la normalisation

C. Monia, Consultant
R. Mullendore, McDATA
F. Travostino, Nortel
W. Jeong, Troika Networks
M. Edwards, Adaptec (UK) Ltd.
septembre 2005

Traduction Claude Brière de L'Isle

iFCP – protocole de réseautage de mémorisation de canal fibre Internet

Résumé
Le présent document spécifie une architecture et un protocole de passerelle à passerelle pour la mise en œuvre de la fonction de tissu de canal fibre sur un réseau IP. Cette fonction est fournie au moyen du protocole TCP pour le transport de trame de canal fibre et les services de tissu réparti spécifiés par les normes de canal fibre. L'architecture permet l'inter réseautage des appareils de canal fibre par des régions dont l'accès est fait par une passerelle avec les propriétés d'isolement des fautes des systèmes autonomes et l'adaptabilité du réseau IP.

Table des matières

1. Introduction

1.1 Conventions utilisées dans le document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Sauf spécification contraire les quantités numériques sont données en valeurs décimales.

Tous les diagrammes qui représentent des ordres de bits et d'octets, incluant la représentation de structures définie par les normes de canal fibre, suivent les conventions de l'IETF selon lesquelles le bit 0 est le bit de poids fort, et le premier octet adressable est dans le coin supérieur gauche. Cette convention de l'IETF diffère de celle utilisée pour les normes de canal fibre INCITS T11, dans lesquelles le bit 0 est le bit de moindre poids.

1.1.1 Structures de données internes à une mise en œuvre

Pour faciliter la spécification du comportement requis, le présent document peut définir et se référer à des structures de données internes au sein de la mise en œuvre iFCP. De telles structures ne sont destinées qu'à des fins d'explication et n'ont pas besoin d'être instanciées dans une mise en œuvre comme décrit dans cette spécification.

1.2 Objet du document

Le présent document qui est sur la voie de la normalisation spécifie un protocole pour la mise en œuvre de services de transport sur canal fibre sur un réseau TCP/IP. Certaines portions du document contiennent des matériaux provenant de normes établies par les groupes de travail INCITS T10 et T11. Ces matériaux sont inclus ici à des fins d'information. Les informations d'autorité sont données dans les documents de normalisation appropriés du NCITS.

Les portions d'autorité du présent document spécifient la transposition des mises en œuvre de protocole de canal fibre conformes aux normes dans TCP/IP. Cette transposition inclut des sections de ce document qui décrivent le "protocole iFCP" (voir la Section 5).

2. Introduction à iFCP

iFCP est un protocole de passerelle à passerelle qui fournit des services de tissu canal fibre aux appareils canal fibre sur un réseau TCP/IP. iFCP utilise TCP pour assurer le contrôle d'encombrement, la détection d'erreurs, et la récupération. Le principal objectif de iFCP est de permettre l'interconnexion et la mise en réseau des appareils canal fibre existants au débit du câble sur un réseau IP.

Le protocole et la méthode de traduction d'adresse de trame décrite dans le présent document permettent le rattachement des appareils de mémorisation de canal fibre à un tissu fondé sur IP au moyen de passerelles transparentes.

Le protocole réalise cette transparence en permettant que le trafic normal de trames de canal fibre passe directement à travers la passerelle, avec des dispositions, lorsque nécessaire, pour intercepter et émuler le tissu de services requis par un appareil canal fibre.

2.1 Définitions

On présente ici les termes nécessaires pour décrire les concepts utilisés dans le présent document.

Mode de traduction d'adresse -- mode de fonctionnement de passerelle dans lequel la portée des adresses de tissu N_PORT, pour les appareils à rattachement local, est local à la région de passerelle iFCP dans laquelle résident les appareils.

Mode d'adresse transparent -- mode de fontionnement de passerelle dans lequel la portée des adresses de tissu N_PORT, pour tous les appareils canal fibre, est unique au tissu iFCP lié auquel appartient la passerelle.

Tissu iFCP lié -- union de deux régions de passerelles ou plus configurées pour interopérer en mode d'adresse transparent.

Identifiant de domaine -- valeur contenue dans l'octet de poids fort d'une adresse de N_PORT canal fibre de 24 octets.

F_PORT -- interface utilisée par un N_PORT pour accéder à la fonction de tissu de commutation de canal fibre.

Tissu -- d'après [FC-FS] : "L'entité qui interconnecte les N_PORT qui lui sont rattachés et est capable d'acheminer les trames en utilisant seulement les informations d'adresse de la trame de canal fibre."

Accès de tissu -- interface à travers laquelle un N_PORT accède à un tissu canal fibre. Le type d'accès de tissu dépend de la topologie du tissu canal fibre. Dans la présente spécification, toutes les interfaces d'accès de tissu sont considérées comme fonctionnellement équivalentes.

FC-2 -- couche des services de transport canal fibre, décrite dans [FC-FS].

FC-4 -- transposition de canal fibre d'un protocole de couche supérieure, comme [FCP-2], la transposition de canal fibre en SCSI.

Appareil canal fibre -- entité qui met en œuvre la fonction à laquelle on accède par un protocole d'application FC-4.

Réseau canal fibre -- tissu canal fibre natif et tous les nœuds canal fibre rattachés.

Nœud canal fibre -- collection d'un ou plusieurs N_PORT contrôlés par un niveau au dessus de la couche FC-2. Un nœud est rattaché à un tissu canal fibre au moyen de l'interface N_PORT, décrite dans [FC-FS].

Région de passerelle -- portion d'un tissu iFCP auquel on accède à travers une passerelle iFCP par un N_PORT rattaché à distance. Les appareils canal fibre dans la région consistent en tous ceux qui sont rattachés localement à la passerelle.

iFCP -- protocole discuté dans le présent document.

Trame iFCP -- trame de canal fibre encapsulée en accord avec la spécification d'encapsulation de trame FC [RFC3643] et la présente spécification.

Portail iFCP -- entité qui représente le point auquel un appareil logique ou physique iFCP est rattaché au réseau IP. L'adresse réseau du portail iFCP consiste en l'adresse IP et le numéro d'accès TCP auquel est envoyée une demande quand la connexion TCP est créée pour une session iFCP (voir au paragraphe 5.2.1).

Session iFCP -- association composée d'une paire de N_PORT et d'une connexion TCP qui porte le trafic entre eux. Une session iFCP peut être créée par suite d'une opération PLOGI d'établissement de canal fibre.

iSNS -- fonction de serveur et protocole IP qui fournit des services de nom de mémorisation dans un réseau iFCP. Les services de nom de canal fibre sont mis en œuvre par un serveur de nom iSNS, comme décrit dans la [RFC4171].

Appareil à rattachement local -- par rapport à une passerelle, c'est un appareil canal fibre auquel on accède à travers le tissu canal fibre auquel la passerelle est rattachée.

Appareil logique iFCP -- c'est l'abstraction qui représente un seul appareil canal fibre comme il apparaît sur un réseau iFCP.

N_PORT -- entité iFCP ou canal fibre qui représente l'interface à la fonctionnalité d'appareil canal fibre. Cette interface met en œuvre la sémantique N_PORT de canal fibre, spécifiée dans [FC-FS]. Canal fibre définit plusieurs variantes de cette interface qui dépendent de la topologie du tissu canal fibre. Utilisé dans le présent document, le terme s'applique également à toutes les variantes.

Alias de N_PORT -- adresse de N_PORT allouée par une passerelle pour représenter un N_PORT distant auquel on accède via le protocole iFCP.

Adresse de tissu N_PORT -- adresse d'un N_PORT au sein du tissu canal fibre.

Identifiant de N_PORT -- adresse d'un N_PORT rattaché localement au sein d'une région de passerelle. Les identifiants de N_PORT sont alloués conformément aux règles de canal fibre pour les allocations d'adresses, spécifiées dans [FC-FS].

Adresse réseau de N_PORT -- adresse d'un N_PORT dans le tissu iFCP. Cette adresse consiste en l'adresse IP et le numéro d'accès TCP du portail iFCP et l'identifiant de N_PORT de l'appareil canal fibre rattaché localement.

Établissement d'accès (PLOGI, *Port Login*) -- service de liaison étendu (ELS, *Extended Link Service*) de canal fibre qui établit une session iFCP par l'échange des paramètres d'identification et de fonctionnement entre un N_PORT générateur et un N_PORT répondant.

Appareil rattaché à distance -- par rapport à une passerelle, c'est un appareil canal fibre auquel on accède depuis la passerelle au moyen du protocole iFCP.

Tissu iFCP non lié -- union de deux régions de passerelles ou plus configurée pour interopérer en mode de traduction d'adresse.

3. Concepts de la communication sur canal fibre

Canal fibre est une technologie de série fondée sur la trame, conçue pour la communication à des vitesses de l'ordre du gigabit et avec une redondance et latence faibles d'homologue à homologue entre des appareils.

Cette section contient une discussion des concepts de canal fibre qui forment la base de l'architecture du réseau et protocole iFCP décrite dans ce document. Le lecteur familier avec ces concepts peut passer directement à la Section 4.

Le matériel présenté dans cette section est tiré des spécifications T11 suivantes :
-- Interface de tramage et de signalisation canal fibre , [FC-FS]
-- Tissu de commutation canal fibre -2, [FC-SW2]
-- Services génériques canal fibre , [FC-GS3]
-- Rattachement de boucle de tissu canal fibre, [FC-FLA]

Le lecteur trouvera une description en profondeur de la technologie dans [KEMCMP] et [KEMALP].

3.1 Réseau de canal fibre

L'entité fondamentale de canal fibre est le réseau canal fibre. À la différence d'une architecture de réseau en couches, un réseau canal fibre est largement spécifié par des éléments fonctionnels et leurs interfaces. Comme le montre la Figure 1, ils consistent, partiellement, en :

a) des N_PORT -- les points d'extrémité du trafic canal fibre. Dans les normes canal fibre, les interfaces de N_PORT ont plusieurs variantes, selon la topologie du tissu auquel elles sont rattachées. Utilisé dans la présente spécification, ce terme s'applique à toutes ces variantes.
b) des appareils canal fibre -- ce sont ceux auxquels les N_PORT fournissent l'accès.
c) des accès de tissu -- ce sont les interfaces au sein d'un réseau canal fibre qui fournissent le rattachement à un N_PORT. Les types d'accès de tissu dépendent de la topologie du tissu et sont discutés au paragraphe 3.2.
d) l'infrastructure réseau pour porter les trafic de trames entre les N_PORT.
e) au sein d'un tissu de commutation ou mixte (voir le paragraphe 3.2) un ensemble de serveurs auxiliaires, incluant un serveur de noms pour la découverte des appareils et la résolution des adresses réseau. Les types de service dépendent de la topologie du réseau.

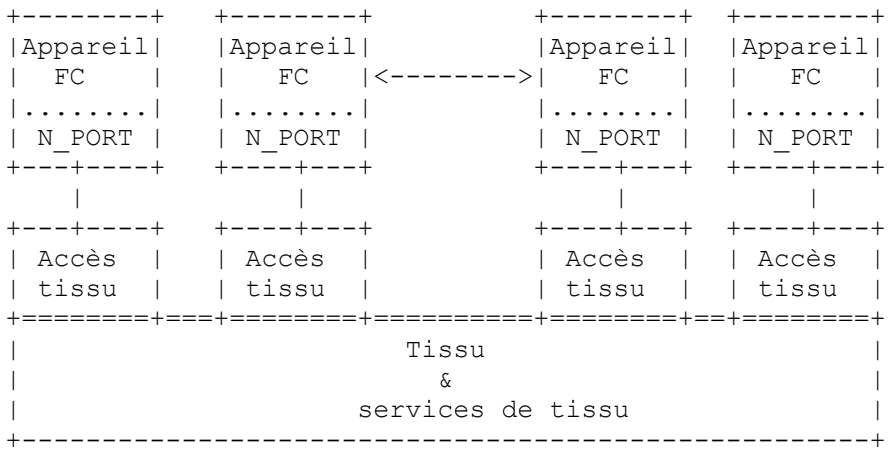


Figure 1 : réseau de canal fibre

Les paragraphes qui suivent décrivent les topologies de réseau canal fibre et donnent une vue d'ensemble du modèle de communications canal fibre.

3.2 Topologies de réseau canal fibre

Les principales topologies de réseau canal fibre consistent en :

a) Boucle arbitrée -- une série de N_PORT connectés ensemble en guirlande. Dans [FC-FS], les N_PORT connectés en boucle sont appelés des NL_PORT. La transmission des données entre les NL_PORT exige un arbitrage pour le contrôle de la boucle d'une manière similaire à celle d'un réseau en anneau à jetons.
b) Tissu commuté -- réseau consistant en éléments de commutation, comme décrit au paragraphe 3.2.1.
c) Tissu mixte -- réseau consistant en commutateurs et boucles "rattachées au tissu". On trouvera une description dans [FC-FLA]. Un N_PORT rattaché à une boucle (NL_PORT) est connecté à la boucle par un L_PORT et accède au tissu au moyen d'un FL_PORT.

Selon la topologie, le N_PORT et ses moyens de rattachement au réseau peuvent être un des suivants :

Topologie de réseau FC	**Interface réseau**	**Variante de N_PORT**
Boucle	L_PORT	NL_PORT
Commuté	F_PORT	N_PORT
Mixte	FL_PORT via L_PORT	NL_PORT
	F_PORT	N_PORT

Les différences dans chaque variante de N_PORT et ses accès de tissu correspondants sont confinées aux interactions entre elles. Pour un N_PORT externe, tous les accès de tissu sont transparents, et tous les N_PORT distants sont fonctionnellement identiques.

3.2.1 Tissus de canal fibre commutés

Un exemple d'un tissu canal fibre multi commuté est montré dans la Figure 2.

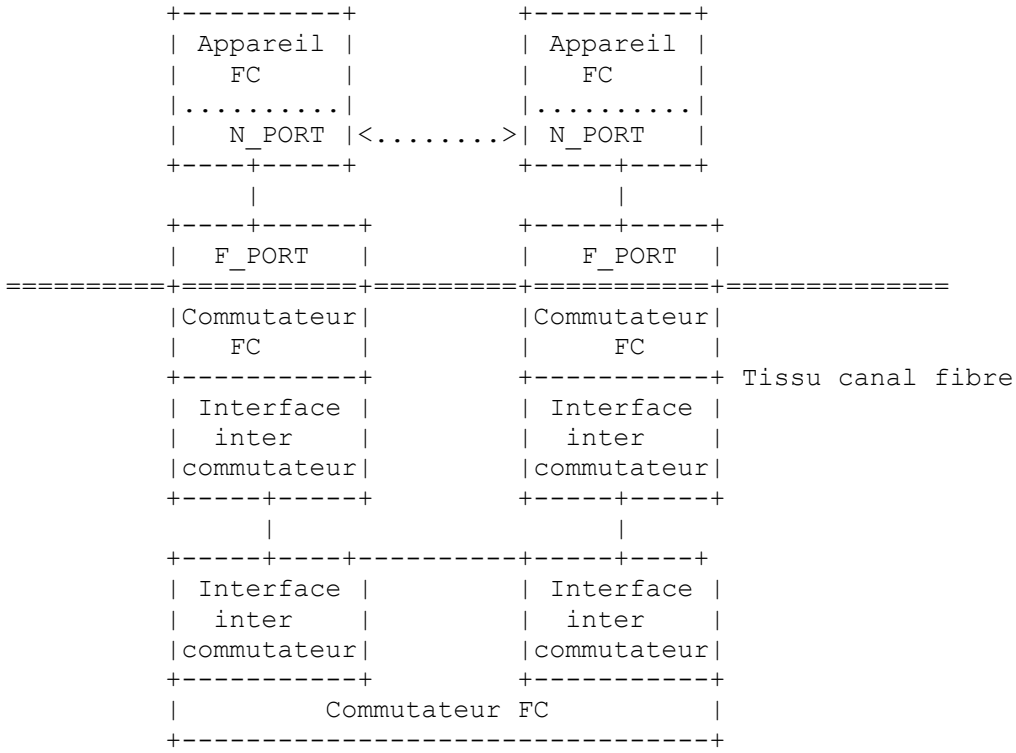


Figure 2. Tissu canal fibre multi commutateurs

L'interface entre les éléments de commutateur est soit une interface propriétaire soit l'interface E_PORT conforme aux normes décrite dans la spécification [FC-SW2].

3.2.2 Tissu canal fibre mixte

Un tissu mixte contient une ou plusieurs boucles arbitrées connectées à un tissu commuté comme le montre la Figure 3.

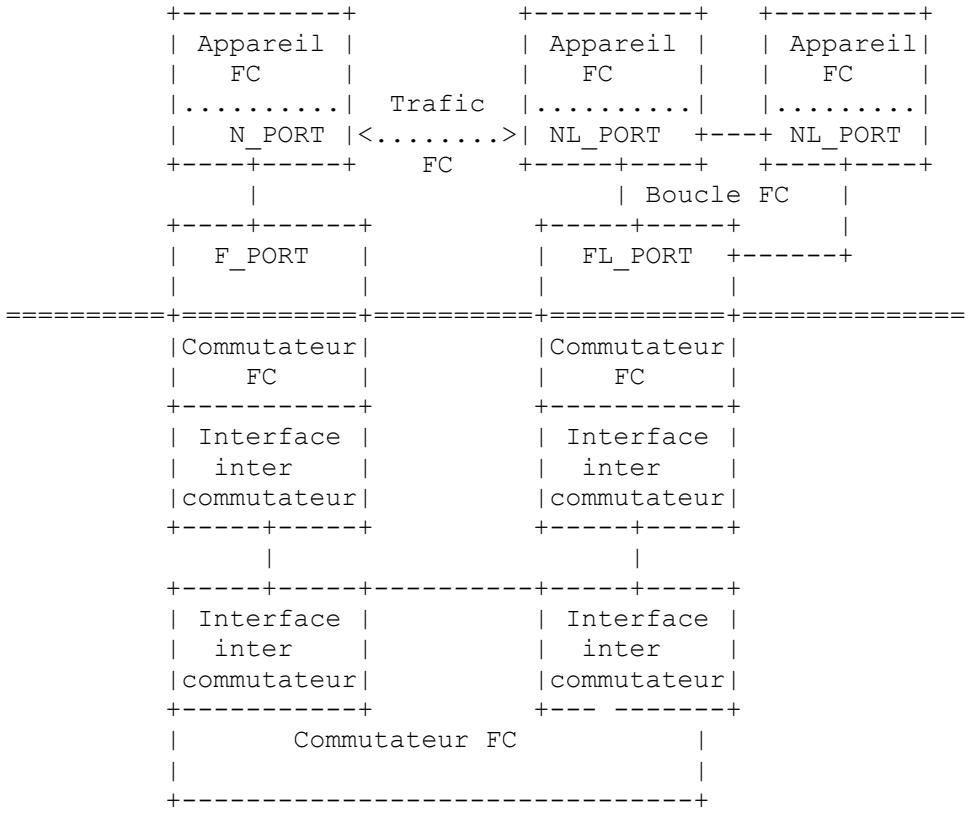


Figure 3. Tissu canal fibre mixte

Comme noté plus haut, le protocole des communications entre les N_PORT homologues est indépendant de la topologie du tissu, de la variante de N_PORT, et du type d'accès de tissu auquel un N_PORT est rattaché.

3.3 Couches et services liaison de canal fibre

Un canal fibre comporte les couches suivantes :
FC-0 -- interface au support physique.
FC-1 -- codage et décodage des données et des informations de contrôle de liaison physique hors bande pour la transmission sur le support physique.
FC-2 -- transfert des trames, séquences, et échanges comprenant les unités d'informations de protocole.
FC-3 -- services communs.
FC-4 -- protocoles d'application comme le protocole canal fibre pour SCSI (FCP).

En plus des couches définies ci-dessus, un canal fibre définit un ensemble d'opérations auxiliaires, dont certaines sont mises en œuvre au sein du tissu de couche transport, appelés services de liaison. Elles sont exigées afin de gérer l'environnement de canal fibre, établir les communications avec d'autres appareils, restituer des informations d'erreur, effectuer la récupération d'erreur, et fournir d'autres services similaires. Certains services de liaison sont exécutés par le N_PORT. D'autres sont mis en œuvre en interne au sein du tissu. Ces services internes sont décrits au paragraphe suivant.

3.3.1 Services de liaison fournis par le tissu

Les serveurs qui sont internes à un tissu commuté traitent certaines classes de demandes de service liaison et de commandes spécifiques de service. Les serveurs apparaissent comme des N_PORT situés aux adresses de tissu de N_PORT bien connues spécifiées dans [FC-FS]. Les demandes de service utilisent les mécanismes standard de canal fibre pour les communications de N_PORT à N_PORT.

Tous les tissus commutés doivent fournir les services suivants :
Serveur de tissu F_PORT -- demandes de services N_PORT pour l'accès au tissu pour les communications.
Contrôleur de tissu -- fournit les informations de changement d'état pour informer les autres appareils FC quand un N_PORT sort du, ou entre dans, le tissu (voir le paragraphe 3.5).
Serveur de répertoire/noms - permet aux N_PORT d'enregistrer les informations dans une base de données, restitue les informations sur les autres N_PORT, et de découvrir les autres appareils comme décrit au paragraphe 3.5.

Un tissu commuté peut aussi mettre en œuvre les services facultatifs suivants :

Adresse/serveur de diffusion -- Transmet des séquencee d'une seule trame, de classe 3 à tous les N_PORT.

Serveur horaire -- destiné à la gestion des temporisateurs d'expiration au niveau du tissu ou des valeurs de temps écoulé ; non estiné à une synchronisation horaire précise.

Serveur de gestion - collecte et rapporte les informations de gestion, telles que l'usage des liaisons, les statistiques d'erreur, la qualité de liaison, et éléments similaires.

Facilitateur de qualité de service - effectue au niveau du tissu la gestion de la bande passante et de la latence.

3.4 Nœuds de canal fibre

Un nœud canal fibre a un ou plusieurs N_PORT rattachés au tissu. Le nœud et ses N_PORT ont les identifiants associés suivants :
a) un identifiant unique au monde pour le nœud.
b) un identifiant unique au monde pour chaque N_PORT associé au nœud.
c) pour chaque N_PORT rattaché à un tissu, une adresse de 24 bits unique pour le tissu avec les propriétés définies au paragraphe 3.7.1. L'adresse de tissu est l'adresse à laquelle les trames sont envoyées.

Chaque identifiant unique au monde est une quantité binaire de 64 bits avec le format défini dans [FC-FS].

3.5 Découverte d'appareil de canal fibre

Dans un tissu commuté ou mixte, les appareils canal fibre et les changements de configuration d'appareil peuvent être découverts au moyen des services fournis par le serveur de noms et le contrôleur de tissu canal fibre.

Le serveur de noms fournit des services d'enregistrement et d'interrogation qui permettent à un appareil canal fibre d'enregistrer sa présence sur le tissu et de découvrir l'existence des autres appareils. Par exemple, un type d'interrogation obtient l'adresse tissu d'un N_PORT à partir de son nom unique au monde de 64 bits. L'ensemble complet des interrogations de serveur de noms canal fibre prises en charge est spécifié dans [FC-GS3].

Le contrôleur de tissu complète les capacités de découverte statique fournies par le serveur de noms par un service qui alerte de façon dynamique un appareil canal fibre chaque fois qu'un N_PORT est ajouté ou retiré à la configuration. Un appareil canal fibre reçoit ces notifications en s'abonnant au service comme spécifié dans [FC-FS].

3.6 Éléments d'information de canal fibre

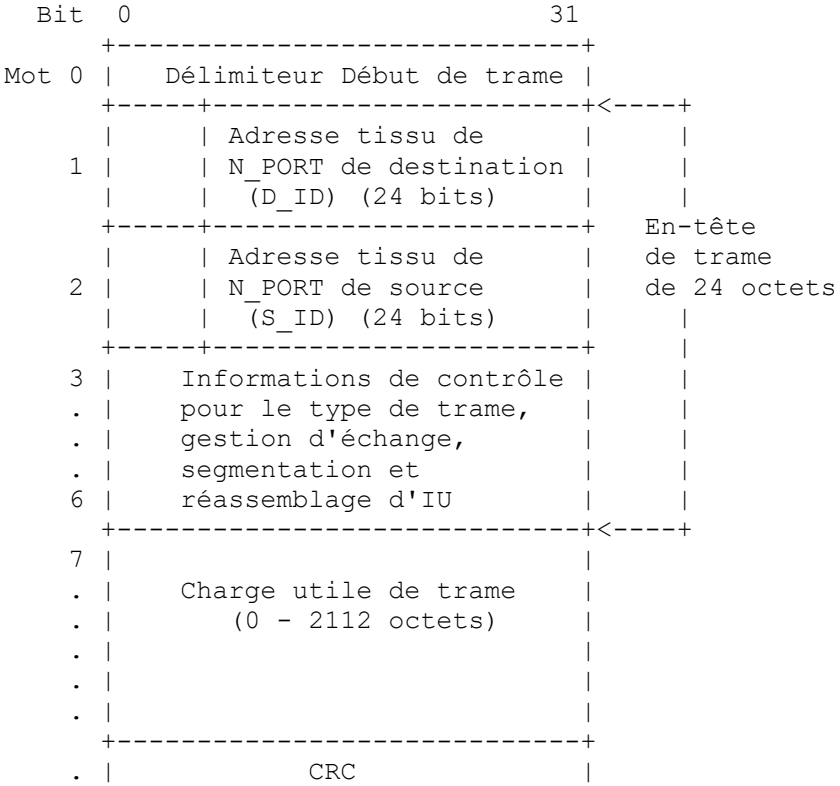
L'élément d'information fondamental dans canal fibre est la trame. Une trame consiste en un en-tête fixe et jusqu'à 2112 octets de charge utile avec la structure décrite au paragraphe 3.7. La taille maximum de trame qui peut être transmise entre une paire d'appareils canal fibre est négociable jusqu'à la limite de charge utile, sur la base de la taille des mémoires tampon de trames dans chaque appareil canal fibre et de l'unité maximum de transmission (MTU) de chemin supportée par le tissu.

Les opérations qui impliquent le transfert d'informations entre les paires de N_PORT sont effectuées par des "échanges". Dans un échange, les informations sont transférées dans une ou plusieurs séries ordonnées de trames, appelées des "séquences".

Dans ce cadre, un protocole de couche supérieure est défini en termes de transactions portées par des échanges. À son tour, chaque transaction consiste en unités d'informations de protocole, dont chacune est portée par une séquence individuelle au sein d'un échange.

3.7 Format de trame canal fibre

Une trame de canal fibre consiste en un en-tête, une charge utile et un CRC de 32 bits encadré par des délimiteurs SOF *(début de fichier)* et EOF *(fin de fichier)*. L'en-tête contient les informations de contrôle nécessaires pour acheminer les trames entre les N_PORT et gérer les échanges et les séquences. Le diagramme qui suit donne une vue schématique de la trame.



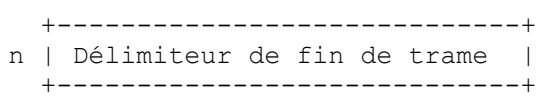


Figure 4. Format de trame canal fibre

Les adresses de tissu de source et de destination de N_PORT incorporées dans les champs S_ID et D_ID représentent les adresses physiques des N_PORT, respectivement d'origine et de réception.

3.7.1 Modèle d'adresse N_PORT

Les adresses de tissu de N_PORT sont des valeurs de 24 bits du format suivant, défini par la spécification canal fibre [FC-FS] :

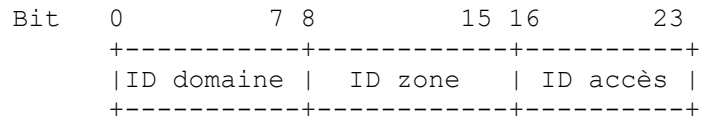


Figure 5. Format d'adresse canal fibre

Un appareil canal fibre acquiert une adresse quand il s'enregistre dans le tissu. De telles adresses sont volatiles et sujettes à changement sur la base des modifications de la configuration du tissu.

Dans un tissu canal fibre, chaque élément de commutation a un identifiant de domaine unique alloué par le commutateur principal. La valeur de l'identifiant de domaine va de 1 à 239 (0xEF). Chaque élément de commutation, à son tour, administre un bloc d'adresses divisé en identifiants de zone et d'accès. Un N_PORT connecté à un F_PORT reçoit une adresse de tissu unique, consistant en l'identifiant de domaine du commutateur enchaîné avec les identifiant de zone et d'accès alloués par le commutateur.

Un NL_PORT rattaché à une boucle (voir la Figure 3) obtient le composant identifiant d'accès *(Port ID)* de son adresse durant le processus d'initialisation de boucle décrit dans [FC-AL2]. Les identifiants de zone et de domaine sont fournis par le tissu lorsque l'enregistrement de tissu (FLOGI, *fabric login*) est exécuté.

3.8 Services de transport de canal fibre

Les N_PORT communiquent au moyen des classes de service suivantes, qui sont spécifiées dans la norme canal fibre [FC-FS] :

Classe 1 - circuit physique dédié qui connecte deux N_PORT.

Classe 2 - connexion de multiplexage de trame avec contrôle de flux de bout en bout et confirmation de livraison.

Classe 3 - connexion de multiplexage de trame sans dispositions pour le contrôle de flux de bout en bout ni confirmation de livraison.

Classe 4 -- service en mode connexion, fondé sur un modèle de circuit virtuel, fournissant la confirmation de livraison avec des garanties de bande passante et de latence.

Classe 6 -- service de diffusion groupée fiable dérivé de la classe 1.

Les classes 2 et 3 sont les services prédominants pris en charge par les systèmes déployés de mémorisation et mise en grappe de canal fibre.

Le service de classe 3 est similaire au service de datagrammes UDP ou IP. Les appareils de mémorisation de canal fibre qui utilisent cette classe de services s'appuient sur la mise en œuvre de ULP pour détecter et récupérer d'erreurs transitoires d'appareil et de transport.

Pour le service de classe 2 et de classe 3, le tissu canal fibre n'est pas obligé de fournir la livraison dans l'ordre des trames sauf si c'est explicitement demandé par l'origine de la trame (et pris en charge par le tissu). Si la livraison dans l'ordre n'est pas activée, il est de la responsabilité du receveur de la trame de reconstruire l'ordre dans lequel les trames ont été envoyées, sur la base des informations de l'en-tête de trame.

3.9 Processus d'enregistrement

Les processus d'enregistrement sont des opérations FC-2 qui permettent à un N_PORT d'établir l'environnement de fonctionnement nécessaire pour communiquer avec le tissu, les autres N_PORT, et les mises en œuvre ULP jointes via le N_PORT. Trois opérations d'enregistrement sont prises en charge :

a) Enregistrement de tissu (FLOGI, *Fabric Login*) -- opération par laquelle le N_PORT enregistre sa présence sur le tissu, obtient les paramètres du tissu, comme les classes de service acceptées, et reçoit son adresse de N_PORT,
b) Enregistrement d'accès (PLOGI, *Port Login*) -- opération par laquelle un N_PORT établit la communication avec un autre N_PORT.
c) Enregistrement de procès (PRLOGI, *Process Login*) -- opération qui établit les communications de procès à procès associées à un ULP FC-4 spécifique, comme FCP-2, la transposition SCSI de canal fibre.

Comme les adresses N_PORT sont volatiles, un N_PORT qui génère une opération d'enregistrement d'accès (PLOGI) exécute une interrogation de serveur de noms pour découvrir l'adresse de canal fibre de l'appareil distant. Un type d'interrogation courant implique l'utilisation du nom unique au monde d'un N_PORT pour obtenir l'adresse de 24 bits du N_PORT canal fibre à laquelle est envoyée la demande PLOGI.

4. Modèle de réseau iFCP

Le protocole iFCP permet la mise en œuvre de la fonction de tissu canal fibre sur un réseau IP dans lequel les composants et la technologie IP remplacent l'infrastructure de commutation et d'acheminement canal fibre décrite au paragraphe 3.2.

L'exemple de la Figure 6 montre un réseau canal fibre avec des appareils rattachés. Chaque appareil accède au réseau par un N_PORT connecté à une interface dont le comportement est spécifié dans [FC-FS] ou [FC-AL2]. Dans ce cas, le N_PORT représente une des variantes décrites au paragraphe 3.2. L'interface au tissu peut être un L_PORT, F_PORT, ou FL_PORT.

Au sein du domaine de l'appareil canal fibre, des entités adressables consistent en d'autres N_PORT et appareils canal fibre internes au réseau qui effectuent les services de tissu définis dans [FC-GS3].

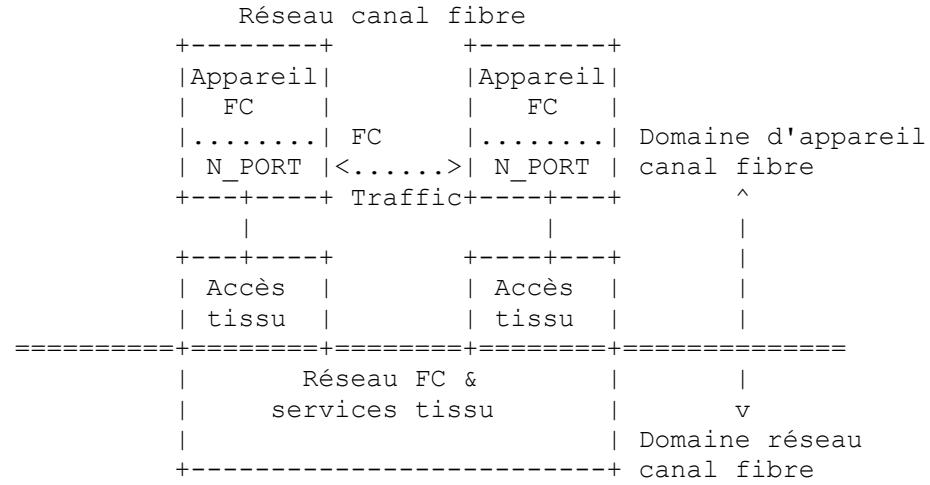
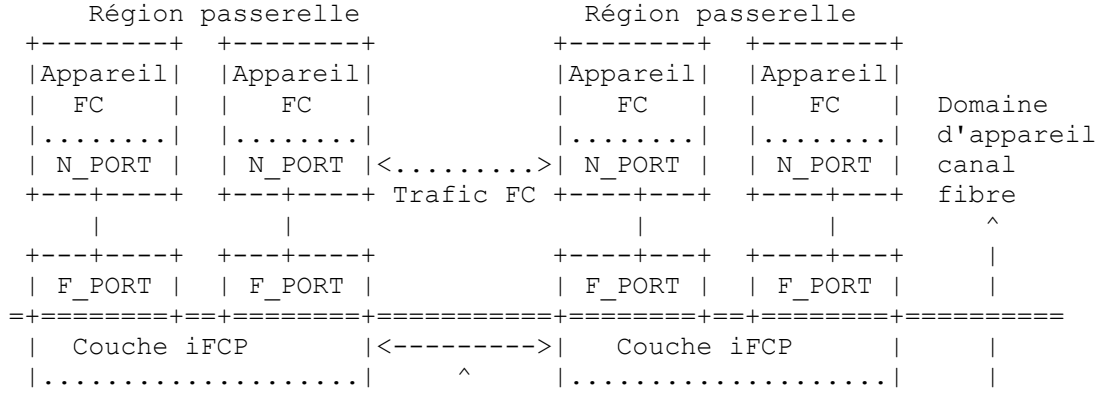


Figure 6 : réseau de canal fibre



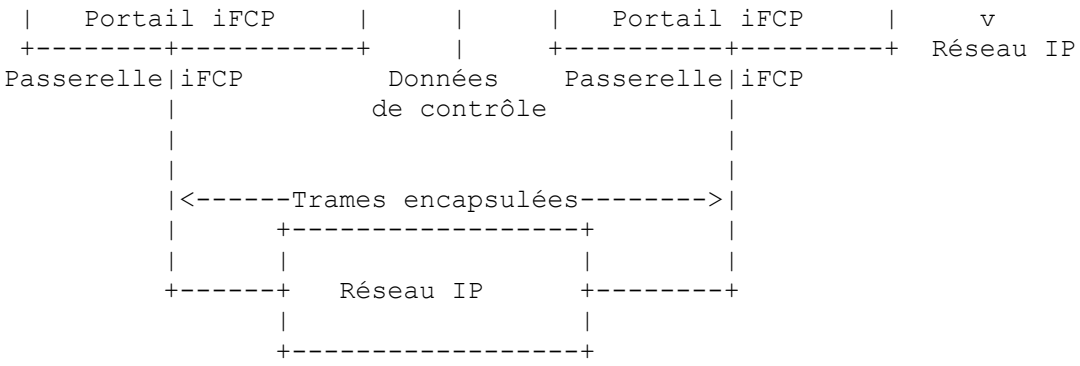


Figure 7 : Exemple de tissu iFCP

La Figure 7 donne un exemple d'équivalent de tissu iFCP. Le tissu consiste en deux régions passerelles, dont chacune est accédée par une seule passerelle iFCP.

Chaque passerelle contient deux F_PORT conformes aux normes et un portail iFCP pour le rattachement au réseau IP. Les appareils canal fibre dans la région sont ceux qui sont connectés localement au tissu iFCP à travers les accès de passerelle au tissu.

Quand on regarde l'accès tissu, la passerelle apparaît comme un élément de commutation de canal fibre. À cette interface les N_PORT distants sont présentés comme des appareils rattachés au tissu. À l'inverse, sur le côté réseau IP, la passerelle présente chaque N_PORT connecté en local comme un appareil canal fibre logique.

En extrapolant au cas général, chaque région de passerelle se comporte comme un système autonome dont la configuration est invisible au réseau IP et aux autres régions passerelles. Par conséquent, en plus du F_PORT montré dans l'exemple, une mise en œuvre de passerelle peut prendre en charge de façon transparente les interfaces canal fibre suivantes :

Liaison inter commutateurs -- une interface canal fibre de commutateur à commutateur utilisée pour accéder à une région contenant des éléments de commutation canal fibre. Une mise en œuvre peut prendre en charge le E_PORT défini par [FC-SW2] ou une des interfaces propriétaires fournies par divers fabricants de commutateurs canal fibre. Dans ce cas, la passerelle agit comme commutateur frontière connectant la région passerelle au réseau IP.

FL_PORT -- interface qui fournit l'accès au tissu pour les appareils canal fibre rattachés à la boucle, comme spécifié dans [FC-FLA].

L_PORT -- interface à travers laquelle une passerelle peut émuler l'environnement de boucle canal fibre spécifié dans [FC-AL2]. Comme exposé à l'appendice B, la passerelle présente les N_PORT accédés à distance comme des appareils rattachés à la boucle.

La manière dont ces interfaces sont fournies par une passerelle est spécifique de la mise en œuvre et sort donc du domaine d'application du présent document.

Bien que chaque région soit connectée au réseau IP à travers une passerelle, une région peut incorporer plusieurs passerelles pour améliorer les performances et la tolérance aux fautes si les conditions suivantes sont satisfaites :

a) Les passerelles DOIVENT coordonner l'allocation des identifiants de N_PORT et des alias afin que chaque N_PORT ait une seule adresse.
b) Tout le trafic iFCP entre une certaine paire de N_PORT local et distant DOIT s'écouler à travers la même session iFCP (voir le paragraphe 5.2.1). Cependant, les sessions iFCP à un certain N_PORT rattaché à distance n'ont pas besoin de traverser la même passerelle.

La coordination des allocations d'adresse et la gestion du flux de trafic sont spécifiques de la mise en œuvre et sortent du domaine d'application de la présente spécification.

4.1 Services de transport iFCP

Les communications de N_PORT à N_PORT qui traversent un réseau TCP/IP exigent l'intervention de la couche iFCP au sein de la passerelle. Cela consiste en les opérations suivantes :

a) Exécution des fonctions d'adressage de trame et de transposition décrites au paragraphe 4.4.

b) Encapsulation des trames de canal fibre pour leur injection dans le réseau TCP/IP et désencapsulation des trames de canal fibre reçues du réseau TCP/IP.
c) Établissement d'une session iFCP en réponse à un PLOGI dirigé sur un appareil distant.

Le paragraphe 4.4 expose le mécanisme d'adressage de trame iFCP et la façon dont il est utilisé pour réaliser la transparence des communications entre les N_PORT.

4.1.1 Services de transport de canal fibre pris en charge par iFCP

Un tissu iFCP prend en charge les services de transport canal fibre de classe 2 et de classe 3, comme spécifié dans [FC-FS]. Un tissu iFCP ne prend pas en charge le service de classe 4, classe 6, ou classe 1 (connexion dédiée). Un N_PORT découvre les classes de service de transport prises en charge par le tissu durant l'enregistrement sur le tissu.

4.2 Découverte d'appareils iFCP et gestion de configuration

Une mise en œuvre de iFCP effectue la découverte d'appareils et la gestion du tissu iFCP au moyen du service de nom de mémorisation sur Internet défini dans la [RFC4171]. L'accès à un serveur iSNS est exigé pour effectuer les fonctions suivantes :
a) Émuler les services fournis par le serveur de noms canal fibre décrit au paragraphe 3.3.1, incluant un mécanisme pour notifier de façon asynchrone à un N_PORT les changements de la configuration du tissu iFCP.
b) Agréger les passerelles dans les tissus iFCP pour l'inter fonctionnement.
c) Segmenter un tissu iFCP en zones canal fibre par la définition et la gestion des portées de découverte des appareils, appelées "domaines de découverte".
d) Mémoriser et distribuer les politiques de sécurité, comme décrit au paragraphe 10.2.9.
e) Mise en œuvre du mécanisme de diffusion canal fibre.

4.3 Propriétés du tissu iFCP

Une collection de passerelles iFCP peut être configurée pour inter fonctionner comme tissu iFCP limité ou non limité.

Les passerelles dans un tissu iFCP limité opèrent en mode d'adresse transparent, comme décrit au paragraphe 4.5. Dans ce mode, la portée d'une adresse de N_PORT canal fibre est au niveau du tissu et est déduite des identifiants de domaine produits par le serveur iSNS à partir d'un réservoir commun. Comme expliqué au paragraphe 4.3.2, le nombre maximum d'identifiants de domaines permis par le canal fibre limite la configuration d'un tissu iFCP limité.

Les passerelles dans un tissu iFCP non limité opèrent en mode de traduction d'adresse, comme décrit au paragraphe 4.6. Dans ce mode, la portée d'une adresse de N_PORT est locale pour une région passerelle. Pour le trafic canal fibre entre les régions, la traduction des adresses de N_PORT incorporées aux trames est effectuée par la passerelle. Comme expliqué plus loin, le nombre d'éléments de commutation et passerelles dans un tissu iFCP non limité peut excéder les limites d'un tissu canal fibre conventionnel.

Toutes les passerelles iFCP DOIVENT prendre en charge les tissus iFCP non limités. La prise en charge des tissus iFCP limités est FACULTATIVE.

La décision de prendre en charge les tissus iFCP limités dans une mise en œuvre de passerelle dépend des considérations de transparence d'adresse, d'adaptabilité de la configuration, et de tolérance aux fautes développées dans les paragraphes qui suivent.

4.3.1 Transparence d'adresse

Bien que les passerelles iFCP dans un tissu non limité se convertissent en adresses N_PORT dans l'en-tête et la charge utile de la trame des messages standard de service de liaison, une passerelle ne peut pas convertir de telles adresses en la charge utile de trafic de trame de canal fibre spécifique de fabricant ou d'utilisateur.

Par conséquent, quoique aussi bien les tissus iFCP limités que non limités prennent en charge les mises en œuvre de protocole conformes aux normes FC-4 et les services de liaisons utilisés par les applications principales de canal fibre, un tissu iFCP limité peut aussi prendre en charge des mises en œuvre de protocole spécifiques du fabricant ou de l'utilisateur et de service de liaison qui portent des identifiants de N_PORT dans la charge utile de trame.

4.3.2 Adaptabilité de configuration

Les limites d'adaptabilité d'une configuration de tissu limité sont une conséquence de la politique d'allocation d'adresse de canal fibre exposée au paragraphe 3.7.1. Comme on l'a noté, un tissu iFCP limité qui utilise ce schéma d'allocation d'adresse est limité à un total combiné de 239 passerelles éléments de commutation canal fibre. Avec l'expansion du système, le réseau peut croître pour inclure de nombreux éléments de commutation et passerelles,dont chacun contrôle un petit nombre d'appareils. Dans ce cas, la limitation du compte de commutateurs et passerelles peut devenir une barrière à l'extension et la pleine intégration du réseau de mémorisation.

Comme les adresses canal fibre de N_PORT dans un tissu iFCP non limité ne sont pas pour tout le tissu, les limites imposées par l'allocatioon d'adresses de canal fibre ne s'appliquent qu'au sein de la région passerelle. À travers les régions, le nombre de passerelles iFCP, d'appareils canal fibre, et d'éléments de commutation qui peuvent être inter connectés n'est pas concerné par ces limites. Pour améliorer l'adaptabilité dans l'échange, les mises en œuvre doivent cependant considérer la surcharge incrémentaire de la conversion d'adresse, ainsi que les questions de transparence d'adresse discutées au paragraphe 4.3.1.

4.3.3 Tolérance aux fautes

Dans un tissu iFCP limité, la réallocation d'adresse causée par une faute ou une reconfiguration, comme l'ajout d'une nouvelle région passerelle, peut se répercuter aux autres régions, causant des perturbations à l'échelle du tissu lorsque de nouvelles adresses de N_PORT sont allouées. De plus, avant qu'une nouvelle passerelle puisse être fusionnée dans le tissu, son serveur iSNS doit être asservi au serveur iSNS dans le tissu limité pour centraliser la fourniture des identifiants de domaines. Dans un tissu iFCP non limité, la coordination des bases de données iSNS exige seulement que les serveurs iSNS échangent entre eux les attributs de clients.

Un tissu iFCP limité a aussi une dépendence accrue à la disponibilité du serveur iSNS, qui doit agir comme autorité centrale d'allocation d'adresses. Si la connexité avec le serveur est perdue, les nouvelles valeurs de DOMAIN_ID ne peuvent pas être automatiquement allouées lorsque des passerelles et des éléments de commutation canal fibre sont ajoutés.

4.4 Modèle d'adresse iFCP N_PORT

Ce paragraphe discute des extensions iFCP au modèle d'adressage canal fibre du paragraphe 3.7.1 qui sont exigées pour l'acheminement transparent des trames entre les N_PORT rattachés en local et à distance.

Dans le protocole iFCP, un N_PORT est représenté par les adresses suivantes :

a) Identifiant de N_PORT de 24 bits : adresse N_PORT canal fibre d'un appareil à rattachement local. Selon le mode d'adressage de passerelle, la portée est locale soit à une région, soit à un tissu iFCP limité. Dans l'un et l'autre mode, les communications entre les N_PORT dans la même région passerelle utilisent l'identifiant de N_PORT.
b) Alias de N_PORT de 24 bits : adresse N_PORT canal fibre allouée par chaque passerelle qui fonctionne en mode traduction d'adresse pour identifier un N_PORT rattaché à distance. Le trafic de trame est intercepté par une passerelle iFCP et dirigé sur un N_PORT rattaché à distance au moyen de l'alias de N_PORT. L'adresse allouée par chaque passerelle est unique dans la portée de la région passerelle.
c) Adresse réseau de N_PORT : tuplet consistant en l'adresse IP de passerelle, le numéro d'accès TCP, et l'identifiant de N_PORT. L'adresse réseau de N_PORT identifie les N_PORT de source et de destination pour le trafic canal fibre sur le réseau IP.

Pour fournir des communications transparentes entre le N_PORT distant et local, une passerelle DOIT entretenir un descripteur de session iFCP (voir au paragraphe 5.2.2.2) reflétant l'association entre l'adresse de canal fibre qui représente le N_PORT distant et l'adresse réseau de N_PORT de l'appareil distant. Pour établir cette association, la passerelle iFCP alloue et gère les adresses de tissu de N_PORT canal fibre comme décrit dans les paragraphes qui suivent.

Dans un tissu iFCP, la passerelle iFCP effectue les fonctions d'allocation des adresses et d'acheminement de trame d'un élément de commutation FC. À la différence d'un commutateur FC, une passerelle iFCP doit cependant aussi diriger les trames sur des appareils externes rattachés à des passerelles distantes sur le réseau IP.

Afin d'être transparente aux appareils FC, la passerelle doit livrer ces trames en utilisant seulement l'adresse de destination de 24 bits de l'en-tête de trame. En exploitant son contrôle de l'allocation d'adresse et de l'accès au trafic de trames qui entre ou sort de la région passerelle, la passerelle est capable de réaliser la transparence nécessaire.

Les adresses de N_PORT au sein d'une région passerelle peuvent être allouées d'une des deux façons suivantes :

a) mode traduction d'adresse - mode d'allocation des adresses de N_PORT dans lequel la portée d'une adresse de N_PORT canal fibre est unique pour la région passerelle. L'adresse d'un appareil distant est représentée dans cette région passerelle par son alias de N_PORT alloué par la passerelle.
b) mode d'adresse transparent - mode d'allocation d'adresse de N_PORT dans lequel la portée d'une adresse de N_PORT canal fibre est unique sur l'ensemble de régions passerelles constituant un tissu iFCP limité.

En mode d'adresse transparent, les passerelles au sein d'un tissu limité coopèrent à l'allocation des adresses aux N_PORT rattachés localement. Chaque passerelle qui contrôle une région est chargée d'obtenir de l'autorité d'allocation des adresses et de distribuer des identifiants de domaines uniques, comme décrit au paragraphe 4.5.1. Par conséquent, dans la portée d'un tissu limité, l'adresse de chaque N_PORT est unique. Pour cette raison, des alias alloués par la passerelle ne sont pas obligés pour représenter les N_PORT distants.

Toutes les mises en œuvre de iFCP DOIVENT prendre en charge les opérations en mode traduction d'adresse. La mise en œuvre du mode d'adresse transparent est FACULTATIVE mais, bien sûr, doit être fournie si des configurations de tissu iFCP limité sont à prendre en charge.

Le mode de fonctionnement de la passerelle est réglable d'une manière spécifique de la mise en œuvre. La mise en œuvre NE DOIT PAS :
a) permettre que le mode soit changé après que la passerelle a commencé le traitement du trafic de trames de canal fibre ;
b) permettre le fonctionnement de plus d'un mode à la fois, ou
c) établir une session iFCP avec une passerelle qui n'est pas dans le même mode.

4.5 Fonctionnement en mode d'adresse transparent

Les considérations et exigences suivantes s'appliquent à ce mode de fonctionnement :
a) les passerelles iFCP en mode d'adresse transparent ne vont pas interopérer avec des passerelles iFCP qui ne sont pas en mode d'adresse transparent.
b) lorsque elles interopèrent avec des élements de commutation canal fibre à rattachement local, chaque passerelle iFCP DOIT supposer le contrôle des allocations de DOMAIN_ID en accord avec la spécification appropriée de norme de protocole canal fibre standard ou spécifique de fabricant. Comme décrit au paragraphe 4.5.1, les valeurs de DOMAIN_ID qui sont allouées aux commutateurs FC internes à la région passerelle doivent être produites par le serveur iSNS.
c) en fonctionnement en mode d'adresse transparent, la traduction d'adresse canal fibre NE DEVRA PAS avoir lieu.

En fonctionnement en mode d'adresse transparent, la passerelle DOIT cependant établir et maintenir le contexte de chaque session iFCP conformément au paragraphe 5.2.2.

4.5.1 Gestion d'idntifiant de domaine en mode transparent

Comme décrit au paragraphe 4.5, chaque passerelle et commutateur de canal fibre dans un tissu iFCP limité a un identifiant de domaine unique. Dans une région passerelle qui contient des éléments de commutation canal fibre, chaque élément obtient un identifiant de domaine en interrogeant le commutateur principal comme décrit dans [FC-SW2] -- dans ce cas, la passerelle iFCP elle-même. La passerelle, à son tour, obtient des identifiants de domaine à la demande du serveur de noms iSNS qui agit comme autorité centrale d'allocation d'adresse. En effet, le serveur iSNS assume le rôle de commutateur principal pour le tissu limité. Dans ce cas, la base de données iSNS contient :
a) la définition d'un ou plusieurs tissus iFCP limités, et
b) pour chaque tissu limitéc, un nom unique au monde qui identifie chaque passerelle dans le tissu. Une passerelle en mode d'adresse transparent DOIT résider dans un tissu limité, et un seul.

En tant que commutateur principal au sein de la région passerelle, une passerelle iFCP en mode d'adresse transparent DEVRA obtenir des identifiants de domaine à utiliser dans la région passerelle en produisant l'interrogation iSNS appropriée, en utilisant son nom mondial.

4.5.2 Incompatibilité avec le mode de traduction d'adresse

Sauf pour les trames de contrôle de session spécifiées à la Section 6, les passerelles iFCP en mode d'adresse transparent NE DEVRONT PAS générer ni accepter de trames qui n'aient pas le bit TRP réglé à un dans le champ Fanions iFCP de l'en-tête d'encapsulation (voir au paragraphe 5.3.1). La passerelle iFCP DEVRA immédiatement terminer toutes les sessions iFCP avec la passerelle iFCP de laquelle elle a reçu de telles trames.

4.6 Fonctionnement en mode de traduction d'adresse

Ce paragraphe décrit le processus de gestion de l'allocation des adresses au sein d'une région passerelle qui fait partie d'un tissu iFCP non limité, incluant la modification des adresses de trames FC incorporées dans l'en-tête de trame pour les trames envoyées et reçues de N_PORT rattachés à distance.

Comme décrit au paragraphe 4.4, la portée des adresses de N_PORT dans ce mode est locale à la région passerelle. Un commutateur principal au sein de la région passerelle, éventuellement la passerelle iFCP elle-même, supervise l'allocation de telles adresses, en accord avec les règles spécifiées dans [FC-FS] et [FC-FLA].

L'allocation des adresses de N_PORT à des appareils rattachés localement est contrôlée par l'élément de commutation auquel l'appareil est connecté.

L'allocation des adresses de N_PORT pour des appareils rattachés à distance est contrôlée par la passerelle par laquelle se fait l'accès à l'appareil distant. Dans ce cas, la passerelle DOIT allouer un alias localement significatif au N_PORT à utiliser à la place de l'identifiant de N_PORT alloué par la passerelle distante. L'alias de N_PORT est alloué durant la découverte d'appareil, comme décrit au paragraphe 5.2.2.1.

Pour effectuer la conversion d'adresse et permettre l'acheminement approprié, la passerelle DOIT établir une session iFCP et générer les informations requises pour transposer chaque alias de N_PORT en le contexte de connexion TCP/IP approprié et les identifiants de N_PORT des N_PORT accédés à distance. Ces transpositions sont créées et mises à jour par les moyens spécifiés au paragraphe 5.2.2.2. Comme décrit dans ce paragraphe, les informations de transposition requises sont représentées par le descripteur de session iFCP reproduit à la Figure 8.

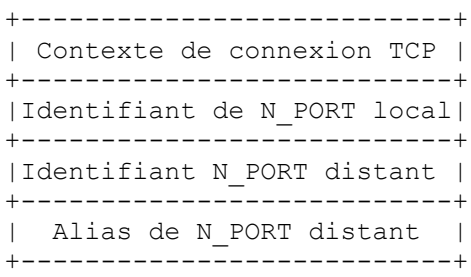
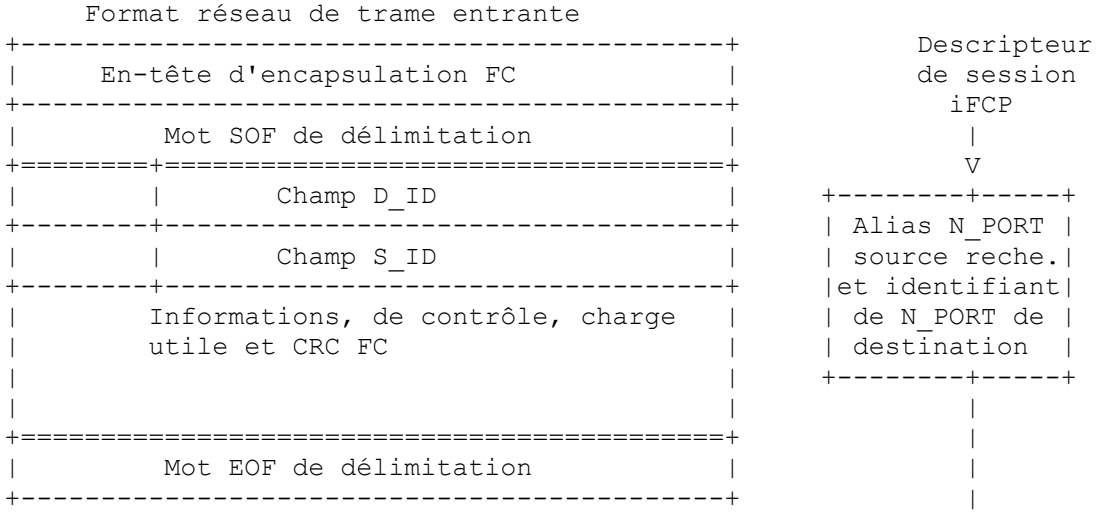


Figure 8. Descripteur de session iFCP (du paragraphe 5.2.2.2)

Sauf pour les trames qui comportent des messages spéciaux de service de liaison (voir au paragraphe 7.2) les trames sortantes sont encapsulées et envoyées sans modification. La traduction d'adresse est différée jusqu'à la réception du réseau IP, comme spécifié au paragraphe 4.6.1.

4.6.1 Traduction d'adresse de trame entrante

Pour les trames entrantes reçue du réseau IP, la passerelle receveuse DEVRA faire référence au descripteur de session pour remplir le champ D_ID avec l'identifiant de N_PORT de destination et le champ S_ID avec l'alias de N_PORT qu'elle lui a alloué. Le processus de traduction pour les trames entrantes est montré par la Figure 9.



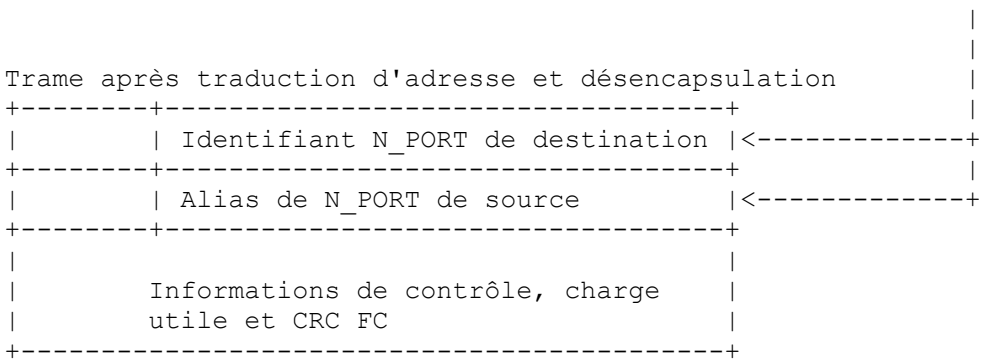


Figure 9. Traduction d'adresse de trame entrante

La passerelle receveuse DEVRA considérer le contenu des champs S_ID et D_ID comme indéfini à la réception. Après le remplacement de ces champs, la passerelle DOIT recalculer le CRC FC.

4.6.2 Incompatibilité avec le mode d'adresse transparent

Les passerelles iFCP en mode traduction d'adresse NE DEVRONT PAS générer ou accepter des trames qui ont le bit TRP établi à un dans le champ Fanions iFCP de l'en-tête d'encapsulation. La passerelle iFCP DEVRA interrompre immédiatement toutes les sessions iFCP avec la passerelle iFCP d'où elle a reçu des trames telles que celles décrites au paragraphe 5.2.3.

5. Protocole iFCP

5.1 Vue d'ensemble

5.1.1 Services de transport iFCP

La principale fonction de la couche de protocole iFCP est de transporter les images de trame de canal fibre entre le N_PORT local et celui rattaché à distance.

Lorsque elle transporte des trames à un N_PORT distant, la couche iFCP encapsule et achemine les trames de canal fibre comprenant chaque unité d'information de canal fibre via une connexion TCP prédéterminée pour le transport à travers le réseau IP.

Lorsque elle reçoit des images de trame de canal fibre du réseau IP, la couche iFCP désencapsulate chaque trame et la livre au N_PORT approprié.

La couche iFCP traite les types de trafic suivants :
a) images de trames FC-4 associées à un protocole d'application canal fibre,
b) trames FC-2 comprenant des demandes et réponses de service de liaison canal fibre,
c) trames de diffusion canal fibre,
d) messages de contrôle iFCP exigés pour établir, gérer, ou terminer une session iFCP.

Pour le trafic de N_PORT FC-4 et la plupart des messages FC-2, la couche iFCP n'interprête jamais le contenu de la charge utile de trame.

iFCP interprête et traite les messages de contrôle iFCP et certains messages de service de liaison, comme décrit au paragraphe 5.1.2.

5.1.2 Prise en charge par iFCP des services de liaison

iFCP doit intervenir dans le traitement des messages de service de liaison canal fibre qui contiennent des adresses de N_PORT dans la charge utile de message ou qui exigent un autre traitement particulier, comme une demande d'établissement de N_PORT (PLOGI).

Dans le premier cas, une passerelle iFCP fonctionnant en mode traduction d'adresse DOIT compléter la charge utile avec des informations supplémentaires qui vont permettre à la passerelle de réception de convertir de telles adresses de N_PORT incorporées à sa trame de référence.

Pour les trames de canal fibre sortantes qui comportent un tel service de liaison, la couche iFCP crée les informations supplémentaires sur la base du contenu de la trame, modifie la charge utile de trame, et transmet ensuite la trame de canal fibre résultante avec les données supplémentaires à travers la connexion TCP appropriée.

Pour les trames iFCP entrantes qui contiennent des trames supplémentaires de service de liaison canal fibre, iFCP doit interprêter la trame, incluant toutes les informations supplémentaires, modifier le contenu de la trame, et transmettre la trame résultante au N_PORT de destination pour la suite du traitement.

Le paragraphe 7.1 décrit le traitement de ces messages de service de liaison plus en détail.

5.2 Transport en flux TCP de trames iFCP

5.2.1 Modèle de session iFCP

Une session iFCP consiste en une paire de N_PORT comprenant les points d'extrémité de la session joints par une seule connexion TCP/IP. Pas plus d'une session iFCP NE DEVRA exister entre une paire de N_PORT donnés.

Un N_PORT est identifié par son adresse réseau, qui consiste en :
a) l'identifiant de N_PORT alloué par la passerelle à laquelle le N_PORT est localement rattaché, et
b) l'adresse de portail iFCP, consistant en son adresse IP et son numéro d'accès TCP.

Comme une seule session iFCP peut exister entre une paire de N_PORT, la session iFCP est identifiée de façon univoque par les adresses réseau des points d'extrémité de la session.

Les connexions TCP qui peuvent être utilisées pour les sessions iFCP entre des paires de portails iFCP sont soit "liées", soit "non liées". Une connexion non liée est une connexion TCP qui ne prend pas activement en charge une session iFCP. Une mise en œuvre de passerelle PEUT établir un réservoir de connexions non liées pour réduire le délai d'établissement de session. De telles connexions TCP préexistantes entre des portails iFCP restent non liées et non affectées jusqu'à ce qu'elles soient allouées à une session iFCP par un message CBIND (voir au paragraphe 6.1).

Quans la couche iFCP crée une session iFCP, elle peut choisir une connexion TCP non liée existante ou établir une nouvelle connexion TCP et envoyer le message CBIND sur cette connexion TCP. Cela alloue la connexion TCP à cette session iFCP.

5.2.2 Gestion de session iFCP

Ce paragraphe décrit les protocoles et structures de données exigés pour établir et terminer une session iFCP.

5.2.2.1 Descripteur de N_PORT distant

Afin d'établir une session iFCP, une passerelle iFCP DOIT conserver les informations qui lui permettent de localiser un N_PORT rattaché à distance. À des fins d'explication, de telles informations sont supposées résider dans un descripteur qui a le format indiqué à la Figure 10.

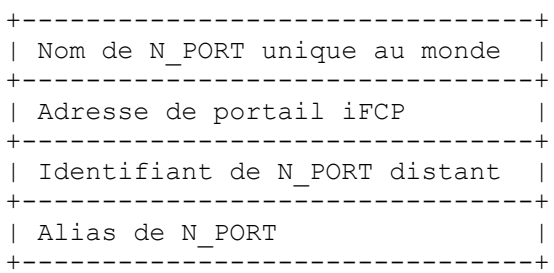


Figure 10. **Descripteur de N_PORT distant**

Chaque descripteur agrège les informations suivantes sur un N_PORT rattaché à distance :

Nom de N_PORT unique au monde -- nom mondial de N_PORT de 64 bits comme spécifié dans [FC-FS]. Un descripteur de N_PORT distant est identifié de façon univoque par ce paramètre.

Adresse de portail iFCP -- l'adresse IP et le numéro d'accès TCP référencés à la création de la connexion TCP associée à une session iFCP sont exigés.

Identifiant de N_PORT -- l'adresse du N_PORT canal fibre allouée à l'appareil distant par la passerelle iFCP distante.
Alias de N_PORT -- adresse de N_PORT canal fibre allouée à l'appareil distant par la passerelle iFCP "locale" quand elle opère en mode traduction d'adresse.

Une passerelle iFCP DEVRA avoir un descripteur et un seul pour chaque N_PORT distant auquel elle accède. Si un descripteur n'existe pas, il DEVRA en être créé un en utilisant les informations retournées par une interrogation au serveur de noms iSNS. De telles interrogations peuvent résulter de :

a) une demande de serveur de noms canal fibre générée par un N_PORT à rattachement local (voir aux paragraphes 3.5 et 9.3) ou
b) une demande CBIND reçue d'un appareil canal fibre distant (voir au paragraphe 5.2.2.2).

Lors de la création d'un descripteur en réponse à une demande CBIND entrante, la passerelle iFCP DEVRA effectuer une interrogation de serveur de noms iSNS en utilisant le nom d'accès mondial du N_PORT distant dans le champ Nom de source N_PORT au sein de la charge utile de CBIND. Le descripteur DEVRA être rempli en utilisant le résultat de l'interrogation.

Après la création du descripteur, une passerelle opérant en mode traduction d'adresse DEVRA créer et ajouter l'alias de 24 bits du N_PORT.

5.2.2.1.1 Mise à jour d'un descripteur de N_PORT distant

Un descripteur de N_PORT distant NE DEVRA être mis à jour QUE comme résultat d'une interrogation iSNS pour obtenir des informations sur le nom d'accès mondial spécifié ou provenant d'informations retournées par une notification de changement d'état iSNS. Suite à une telle mise à jour, un nouvel alias de N_PORT NE DEVRA PAS être alloué.

Avant une telle mise à jour, le contenu d'un descripteur peut être devenu périmé à cause d'un événement qui a invalidé ou déclenché un changement de l'adresse réseau du N_PORT de l'appareil distant, comme une reconfiguration de tissu ou la suppression ou remplacement de l'appareil.

Un effet collatéral d'un tel événement est qu'un appareil canal fibre qui a été ajouté ou dont l'ientifiant de N_PORT a changé n'aura pas d'établissement de N_PORT actif. Par conséquent, le trafic FC-4 dirigé sur un tel N_PORT, à cause d'un descripteur périmé, sera rejeté ou éliminé.

Une fois que le N_PORT générateur a appris la reconfiguration, généralement grâce au mécanisme de notification de changement d'état du serveur de noms, les informations retournées dans la notification ou la recherche suivante de serveur de noms nécessaire pour rétablir la session iFCP vont automatiquement purger de telles données périmées de la passerelle.

5.2.2.1.2 Suppression d'un descripteur de N_PORT distant

Supprimer un descripteur de N_PORT distant est équivalent à libérer l'alias de N_PORT correspondant pour réutilisation. Par conséquent, le descripteur NE DOIT PAS être supprimé alors qu'il y a encore des sessions iFCP qui se réfèrent au N_PORT distant.

Les descripteurs éligibles à la suppression devraient être retirés sur la base d'une politique du dernier arrivé premier sorti.

5.2.2.2 Création d'une session iFCP

Une session iFCP peut être dans un des états suivants :

Ouvert *(OPEN)* -- l'état de la session dans lequel les images de trame de canal fibre peuvent être envoyées et reçues.

Ouverture en cours *(OPEN PENDING)* -- l'état de session après qu'une passerelle a produit une demande CBIND mais qu'une réponse n'a pas encore été reçue. Aucune trame de canal fibre ne peut être envoyée.

La session peut être initiée en réponse à un ELS PLOGI (voir au paragraphe 7.3.1.7) ou pour toute autre raison spécifique de la mise en œuvre.

La passerelle DEVRA créer la session iFCP comme suit :

a) Localiser le descripteur de N_PORT distant correspondant au point d'extrémité de session. Si la session est créée afin de transmettre une trame de canal fibre, le point d'extrémité de session peut être obtenu en faisant référence à l'alias du N_PORT distant contenu dans le champ D_ID de l'en-tête de trame. Si aucun descripteur n'existe, une session iFCP NE DEVRA PAS être créée.

b) Allouer une connexion TCP à la passerelle à laquelle le N_PORT distant est localement rattaché. Une mise en œuvre peut utiliser une connexion existante dans l'état Non lié, ou une nouvelle connexion peut être créée et placée dans l'état Non lié. Quand une connexion est créée, l'adresse IP et le numéro d'accès TCP DEVRONT être obtenus par référence au descripteur de N_PORT distant comme spécifié au paragraphe 5.2.2.1.
c) Si la connexion TCP ne peut pas être allouée ou ne peut pas être créée à cause de ressources limitées, la passerelle DEVRA terminer la création de session.
d) Si la connexion TCP est interrompue pour une raison quelconque avant que la session iFCP entre dans l'état Ouvert, la passerelle DEVRA répondre conformément au paragraphe 5.2.3 et PEUT terminer la tentative de création de session ou PEUT essayer d'établir à nouveau la connexion TCP.
e) La passerelle DEVRA alors produire un message de contrôle de session CBIND (voir au paragraphe 6.1) et placer la session dans l'état Ouverture en cours.
f) Si une réponse CBIND est retournée avec un état autre que "Succès" ou "la session iFCP existe déjà", la session DEVRA être terminée, et la connexion TCP retournée à l'état Non lié.
g) Un état CBIND de "la session iFCP existe déjà" indique que la passerelle distante a initié de façon concurrente une demande CBIND pour créer une session iFCP entre la même paire de N_PORT. Une passerelle qui reçoit une telle réponse DEVRA terminer sa tentative et traiter la demande CBIND entrante conformément au paragraphe 5.2.2.3.
h) Dans une réponse à un état CBIND de "Succès", la passerelle DEVRA placer la session dans l'état Ouvert.

Une fois que la session est placée dans l'état Ouvert, un descripteur de session iFCP DEVRA être créé, contenant les informations montrées à la Figure 11:

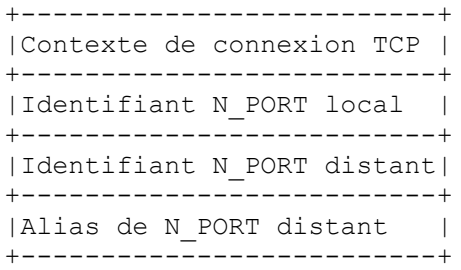


Figure 11. Descripteur de session iFCP

Contexte de connexion TCP -- informations requises pour identifier la connexion TCP associée à la session iFCP.

Identifiant de N_PORT local -- identifiant de N_PORT de l'appareil canal fibre rattaché en local.

Identifiant de N_PORT distant -- identifiant de N_PORT alloué à l'appareil distant par la passerelle distante.

Alias de N_PORT distant -- alias alloué au N_PORT distant par la passerelle locale lorsque elle opère en mode traduction d'adresse. Si elle est dans ce mode, la passerelle DEVRA copier ce paramètre du descripteur de N_PORT distant. Autrement, il n'est pas rempli.

5.2.2.3 Réponse à une demande CBIND

La passerelle qui reçoit une demande CBIND DEVRA y répondre comme suit :
a) Si le receveur a une session iFCP dupliquée dans l'état Ouverture en cours, la passerelle receveuse DEVRA comparer le nom de N_PORT de source dans la charge utile du CBIND entrant avec le nom de N_PORT de destination.
b) Si le nom de N_PORT de source est supérieur, le receveur DEVRA produire une réponse CBIND de "Succès" et DEVRA placer la session dans l'état Ouvert.
c) Si le nom de N_PORT de source est inférieur, le receveur devra produire une réponse CBIND de Échec - la session N_PORT existe déjà. L'état de la session iFCP initié par le receveur DEVRA être inchangé.
d) Si il n'y a pas de session iFCP dupliquée dans l'état Ouverture en cours, la passerelle receveuse DEVRA produire une réponse CBIND. Si un état de Succès est retourné, la passerelle receveuse DEVRA créer la session iFCP et la placer dans l'état Ouvert. Un descripteur de session iFCP DEVRA être créé comme décrit au paragraphe 5.2.2.2.
e) Si il n'existe pas de descripteur de N_PORT distant, il DEVRA en être créé un et il devra être rempli comme décrit au paragraphe 5.2.2.1.

5.2.2.4 Surveillance de la connexité iFCP

Durant des périodes étendues d'inactivité, une session iFCP peut être terminée à cause d'une défaillance de matériel au sein de la passerelle ou de la perte de la connexité TCP/IP. Le premier cas peut se produire lorsque la session traverse un

appareil intermédiaire à états pleins, comme un boîtier NA(P)T ou un pare-feu, qui détecte et purge les connexions qu'il croit inutilisées.

Pour vérifier la vivacité d'une session, effectuer la détection des défaillances de connexité, et éviter la treminaison spontanée de connexion, une passerelle iFCP peut maintenir un bas niveau d'activité de session et surveiller la session en demandant que la passerelle distante transmette périodiquement le message LTEST décrit au paragraphe 6.3. Toutes les passerelles iFCP DEVRONT prendre en charge la varification de vivavité comme décrit dans la présente spécification.

Une passerelle demande le battement de cœur LTEST en spécifiant une valeur non zéro pour l'intervalle de vérifiation de vivacité dans le message de demande ou réponse CBIND comme décrit au paragraphe 6.1. Si les deux passerelles cherchent à surveiller la vivacité, chacune doit régler l'intervalle de vérification de vivacité dans la demande ou réponse CBIND.

À réception d'une telle demande, la passerelle qui fournit le battement de cœur DEVRA transmettre des messages LTEST à l'intervalle spécifié. Le premier message DEVRA être envoyé aussitôt que la session iFCP entre dans l'état Ouvert. Les messages LTEST NE DEVRONT PAS être envoyés quand la session iFCP n'est pas dans l'état Ouvert.

Une session iFCP DEVRA se terminer comme décrit au paragraphe 5.2.3 si :
a) le contenu du message LTEST est incorrect, ou
b un message LTEST n'est pas reçu dans deux fois l'intervalle spécifié ou si la session iFCP a été au repos pendant plus que deux fois l'intervalle spécifié.

La passerelle qui reçoit le message LTEST DEVRA mesurer l'intervalle pour le premier message LTEST attendu à partir du moment où la session est placée dans l'état Ouvert. À partir de là, l'intervalle DEVRA être mesuré par rapport au dernier message LTEST reçu.

Pour maximiser la couverture de la vérification de vivacité, les messages LTEST DEVRAIENT s'écouler à travers tous les composants de passerelle utilisés pour entrer et restituer les trames de canal fibre du réseau IP, incluant les mécanismes pour encapsuler et désencapsuler les trames de canal fibre.

En plus de surveiller une session, les informations de l'en-tête d'encapsulation de message LTEST peuvent aussi être utilisées pour calculer une estimation du délai de propagation du réseau, comme décrit au paragraphe 8.2.1. Cependant, la limite de délai de propagation NE DEVRA PAS être appliquée au trafic LTEST.

5.2.2.5 Utilisation des caractéristiques et réglages de TCP

Ce paragraphe décrit les règles de base de l'utilisation des caractéristiques de TCP dans une session iFCP. Le cœur du protocole TCP est défini dans la [RFC0793]. Les exigences et lignes directrices de la mise en œuvre de TCP sont spécifiées dans la [RFC1122].

Caractéristique	RFC applicables	Statut de la RFC	Niveau d'exigence de l'homologue	Exigence
Garder en vie	[RFC1122] (discussion)	Aucun	Non	Ne devrait pas utiliser
Évitement de petit segment (Nagle)	RFC896]	Standard	Pas dutilisation	Ne devrait pas utiliser
Adaptation de fenêtre	[RFC1323]	Norme proposée	Non	Devrait utiliser
Protection de retour de séquence (PAWS)	[RFC1323]	Norme proposée	Non	DEVRAIT utiliser

Table 1. Utilisation des caractéristiques TCP facultatives

Les paragraphes qui suivent décrivent ces options plus en détail.

5.2.2.5.1 Garder en vie

Garder en vie *(Keep Alive)* accélère la détection et le nettoyage des connexions TCP qui fonctionnent mal en envoyant du trafic quand une connexion serait autrement inactive. Les problèmes sont discutés dans la [RFC1122].

Afin de vérifier plus complètement l'appareil, les applications canal fibre, comme de mémorisation, peuvent mettre en œuvre une fonction équivalente au garder en vie au niveau de la couche FC-4. Autrement, des messages périodiques de vérification de vivacité peuvent être produits comme décrit au paragraphe 5.2.2.4. À cause de ce mécanisme plus complet de bout en bout et des considérations décrites dans la [RFC1122], le "garder en vie" à la couche transport ne devrait pas être mis en œuvre.

5.2.2.5.2 Évitement des "petits" segments

L'algorithme de Nagle décrit dans la [RFC0896] est conçu pour éviter la surcharge des petits segments en retardant la transmission afin d'agglomérer les demandes de transfert en un grand segment. Dans iFCP, de tels petits transferts contiennent souvent des demandes d'entrée/sortie. Le retard de transmission de l'algorithme de Nagle peut diminuer le débit d'entrée/sortie. Donc, l'algorithme de Nagle ne devrait pas être utilisé.

5.2.2.5.3 Adaptation de fenêtre

L'adaptation de fenêtre, comme spécifié dans la [RFC1323], permet le plein usage des liaisons à grande bande passante et à retards de produits et devrait être acceptée par une mise en œuvre de iFCP.

5.2.2.5.4 Protection contre le retour à zéro de séquence (PAWS, *Protection Against Wrapped Sequence*)

Les segments TCP sont identifiés avec des numéros de séquence de 32 bits. Dans les réseaux à grande bande passante et retards de produits, il est possible à plus d'un segment TCP avec le même numéro de séquence d'être en cours sur le réseau. Dans iFCP, la réception d'un tel numéro de séquence déclassé peut causer une livraison de trame déclassée ou la corruption des données. Par conséquent, cette caractéristique DEVRAIT être prise en charge comme décrit dans la [RFC1323].

5.2.3 Terminaison des sessions iFCP

Les sessions iFCP DEVRONT se terminer en réponse à un des événements du Tableau 2:

Événement	Sessions iFCP à terminer
PLOGI terminé avec une réponse LS_RJT	N_PORT homologue.
Notification de changement d'état indiquant la suppression ou reconfiguration de N_PORT.	Toutes les sessions iFCP du N_PORT reconfiguré.
Réponse LOGO ACC provenant du N_PORT homologue.	N_PORT homologue.
Réponse ACC à l'ELS LOGO envoyé au serveur F_PORT (D_ID = 0xFF-FF-FE) (désétablissement de tissu).	Toutes les sessions iFCP provenant du N_PORT générateur.
LOGO N_PORT implicite comme défini dans [FC-FS].	Toutes les sessions iFCP du N_PORT désétabli.
Erreur de message LTEST (voir au paragraphe 5.2.2.4).	N_PORT homologue
Erreur d'encapsulation non fatale comme spécifié au paragraphe 5.3.3	N_PORT homologue
Échec de la connexion TCP associée à la session iFCP.	N_PORT homologue
Réception d'un message UNBIND de contrôle de session.	N_PORT homologue
Passerelle entre dans l'état Non synchronisé (voir au paragraphe 8.2.1).	Toutes les sessions iFCP.
Passerelle détecte un mode d'adresse incorrect avec la passerelle homologue (voir au paragraphe 4.6.2).	Toutes les sessions iFCP avec passerelle homologue.

Tableau 2. Événements de terminaison de session

Si une session se termine à cause d'un mode d'adresse incorrect avec la passerelle homologue, la connexion TCP DEVRA être interrompue au moyen d'une réinitialisation de connexion (RST) sans effectuer de UNBIND. Autrement, si la connexion TCP est toujours ouverte à la suite de l'événement, la passerelle DEVRA fermer la connexion comme suit :

a) arrêter d'envoyer des trames de canal fibre sur la connexion TCP,
b) éliminer tout le trafic entrant, sauf pour un message UNBIND de contrôle de session,
c) si un message UNBIND est reçu, à tout moment, retourner une réponse conformément au paragraphe 6.2,
d) si la terminaison de session n'était pas déclenchée par un message UNBIND, produire le message UNBIND de contrôle de session, comme décrit au paragraphe 6.2,
e) si le message UNBIND s'achève avec l'état de Succès, la connexion TCP PEUT rester ouverte à la discrétion de l'une ou l'autre passerelle et peut être conservé dans un réservoir de connexions non liées afin d'accélérer la création d'une nouvelle session iFCP. Si le UNBIND échoue pour une raison quelconque, la connexion TCP DOIT être terminée. Dans ce cas, la connexion DEVRAIT être interrompue avec une réinitialisation de connexion (RST).

Pour chaque session terminée, le descripteur de session DEVRA être supprimé. Si une session a été terminée par un événement autre qu'un LOGO implicite ou une réponse LOGO ACC, la passerelle devra produire un LOGO au N_PORT rattaché en local au nom du N_PORT distant.

Pour récupérer des ressources, l'une ou l'autre passerelle peut spontanément clore une connexion TCP non liée à tout moment. Si une passerelle termine une connexion avec une opération de clôture de TCP, la passerelle homologue DOIT répondre en exécutant une clôture de TCP.

5.3 Encapsulation de trame de canal fibre

Ce paragraphe décrit l'encapsulation iFCP des trames de canal fibre. L'encapsulation se conforme au format commun d'encapsulation défini dans la [RFC3643], dont des portions sont incluses ici dans un but pratique.

Le format d'une trame encapsulée est montré ci-dessous :

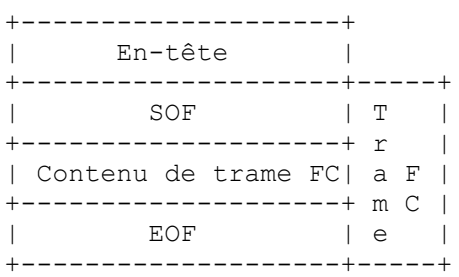


Figure 12 : Format d'encapsulation

L'encapsulation consiste en un en-tête de 7 mots, un mot de délimiteur SOF, la trame FC (incluant le CRC canal fibre), et un mot de délimiteur EOF. Les formats d'en-tête et de délimiteur sont décrits dans les paragraphes qui suivent.

5.3.1 Format d'en-tête d'encapsulation

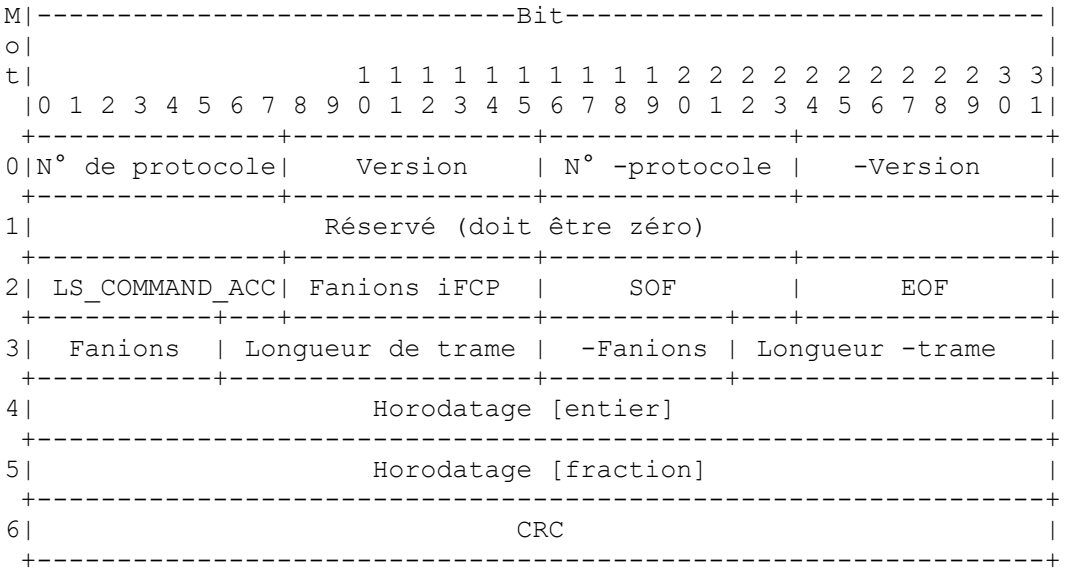


Figure 13. Format d'en-tête d'encapsulation

Champs d'encapsulation communs :

N° de protocole : numéro de protocole alloué par l'IANA qui identifie le protocole utilisant l'encapsulation. Pour iFCP, la valeur allouée par la [RFC3643] est 2.

Version : version d'encapsulation, comme spécifié dans la [RFC3643].

N° de -protocole : complément à un du numéro de protocole.

-Version : complément à un de la version.

Fanions : fanions d'encapsulation (voir en 5.3.1.1).

Longueur de trame : contient la longueur de la trame FC encapsulée entière, incluant l'en-tête d'encapsulation FC et la trame FC (includant les mots SOF et EOF) en unités de mots de 32 bits.

-Fanions : complément à un du champ Fanions.

Longueur de -trame : complément à un du champ Longueur de trame.

Horodatage [entier] : composant entier de l'horodatage de trame, comme spécifié dans la [RFC3643].

Horodatage [fraction] : composant fractionnaire de l'horodatage, comme spécifié dans la [RFC3643].

CRC : CRC d'en-tête. DOIT être valide pour iFCP.

Les champs d'horodatage sont utilisés pour appliquer la limite de durée ce vie de la trame de canal fibre comme décrit au paragraphe 8.2.1.

Champs spécifiques de iFCP :
LS_COMMAND_ACC : pour qu'une réponse spéciale de service de liaison ACC soit traitée par iFCP, le champ LS_COMMAND_ACC DEVRA contenir une copie des bits 0 à 7 de la LS_COMMAND à laquelle le ACC s'applique. Autrement, le champ LS_COMMAND_ACC DEVRA être réglé à zéro.
Fanions iFCP : fanions spécifiques de iFCP (voir ci-dessous).
SOF : copie du codage du délimiteur SOF (voir au paragraphe 5.3.2).
EOF : copie du codage du délimiteur EOF (voir au paragraphe 5.3.2).

Les mots de fanions iFCP ont le format suivant :

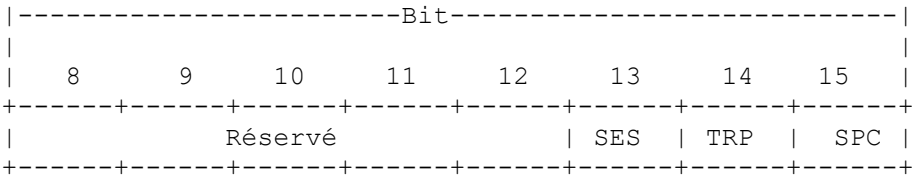


Figure 14. Mots de fanions iFCP

Fanions iFCP :
SES 1 = trame de contrôle de session (TRP et SPC DOIVENT être à 0)
TRP 1 = mode d'adresse transparent activé
0 = mode traduction d'adresse activé
SPC 1 = la trame fait partie d'un message de service de liaison exigeant un traitement spécial par iFCP avant de la transmettre au N_PORT de destination.

5.3.1.1 Fanions communs d'encapsulation

L'usage par iFCP des fanions communs d'encapsulation défini dans la [RFC3643] est montré à la Figure 15 :

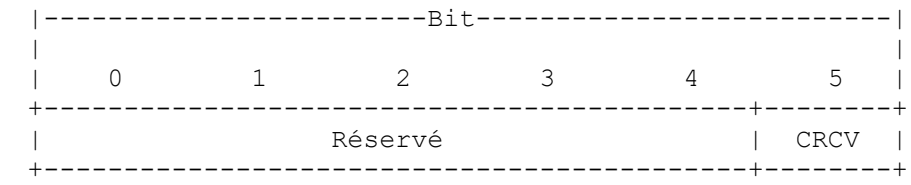


Figure 15. Fanions communs d'encapsulation iFCP

Pour iFCP, le champ CRC DOIT être valide, et CRCV DOIT être réglé à un.

5.3.2 Champs délimiteurs SOF et EOF

Le format des champs de délimiteurs est montré ci-dessous.

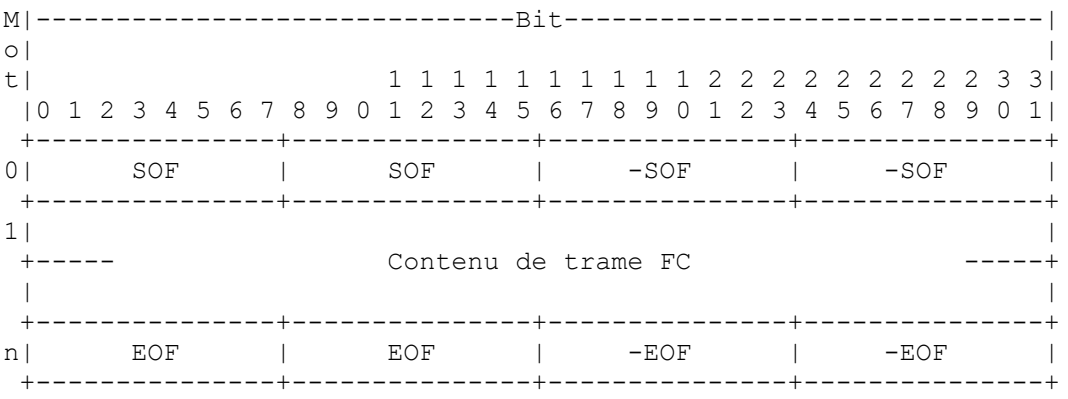


Figure 16. Format d'encapsulation de trame FC

SOF (bits 0-7 et bits 8-15 dans le mot 0) : iFCP utilise le sous ensemble suivant des champs SOF spécifiés dans la [RFC3643]. Par convenance, ils sont reproduits dans le Tableau 3. Les codages d'autorité devraient être pris dans la [RFC3643].

SOF FC	Code SOF
SOFi2	0x2D
SOFn2	0x35
SOFi3	0x2E
SOFn3	0x36

Tableau 3. Traduction des valeurs de FC SOF en contenus de champ SOF

-SOF (bits 16-23 et 24-31 dans le mot 0) : les champs -SOF contiennent le complément à un de la valeur des champs SOF.

EOF (bits 0-7 et 8-15 dans le mot n) : iFCP utilise le sous ensemble suivant des champs EOF spécifiés dans la [RFC3643]. Par convenance, ils sont reproduits dans le Tableau 4. Les codages d'autorité devraient être pris dans la [RFC3643].

EOF FC	Code EOF
EOFn	0x41
EOFt	0x42

Tableau 4. Traduction des valeurs de FC EOF en contenus de champ EOF

-EOF (bits 16-23 et 24-31 dans le mot n) : les champs -EOF contiennent le complément à un de la valeur des champs EOF.

Les mises en œuvre de iFCP DEVRONT placer une copie des codes de délimiteur SOF et EOF dans les champs d'en-tête appropriés.

5.3.3 Encapsulation de trame

Une trame canal fibre à encapsuler DOIT d'abord être validée comme décrit dans [FC-FS]. Toute frame reçue d'un appareil canal fibre rattaché localement qui ne réussit pas les essais de validité de [FC-FS] DEVRA être éliminée par la passerelle.

Si la trame est du service de liaison étendu (ELS, *Extended Link Service*) PLOGI, la création d'une session iFCP, comme décrit au paragraphe 7.3.1.7,peut y précéder l'encapsulation. Une fois la session créée, l'encapsulation de trame DEVRA se poursuivre comme suit.

Les champs S_ID et D_ID dans l'en-tête de trame DEVRONT être référencés pour chercher le descripteur de session iFCP (voir au paragraphe 5.2.2.2). Si il n'existe pas de descripteur de session iFCP, la trame DEVRA être éliminée.

Les types de trame soumis à encapsulation et transmission sur le réseau IP DEVRONT avoir un des délimiteurs SOF du Tableau 3 et un délimiteur EOF du Tableau 4. Les autres types de trame valides DOIVENT être traités en interne par la passerelle comme spécifié dans la spécification canal fibre appropriée.

Si on fonctionne en mode de traduction d'adresse et qu'on traite un message spécial de service de liaison qui exige l'inclusion de données supplémentaires, la passerelle DEVRA formater la charge utile de la trame et ajouter les informations supplémentaires spécifiées au paragraphe 7.1. La passerelle DEVRA alors calculer un nouveau CRC FC sur la trame reformatée.

Autrement, le contenu de la trame NE DEVRA PAS être modifié et la passerelle PEUT encapsuler et transmettre l'image de trame sans recalculer le CRC FC.

Le générateur de la trame DOIT alors créer et remplir l'en-tête et les mots de délimiteur SOF et EOF, comme spécifié aux paragraphes 5.3.1 et 5.3.2.

5.3.4 Désencapsulation de trame

La passerelle receveuse DEVRA effectuer la désencapsulation comme suit :

À réception de la trame encapsulée, la passerelle DEVRA vérifier le CRC d'en-tête. Si le CRC d'en-tête est valide, la passerelle receveuse DEVRA vérifier le champ Fanions iFCP. Si une des conditions d'erreur du Tableau 5 est détectée, la passerelle DEVRA traiter l'erreur comme spécifié au paragraphe 5.2.3.

Condition	Type d'erreur
CRC d'en-tête invalide	Erreur d'encapsulation
SES = 1, TRP ou SPC non 0	Erreur d'encapsulation
SES = 0, TRP incorrect	Mode d'adresse incorrect

Tableau 5. Erreurs d'en-tête d'encapsulation

La passerelle receveuse DEVRA alors vérifier le délai de propagation de trame comme décrit au paragraphe 8.2.1. Si le délai de propagation est trop long, la frame DEVRA être éliminée. Autrement, la passerelle DEVRA vérifier le SOF et le EOF dans l'en-tête d'encapsulation. Une trame DEVRA être éliminée si elle a un code de SOF qui n'est pas dans le Tableau 3 ou un code de EOF qui n'est pas dans le Tableau 4.
La passerelle DEVRA alors désencapsuler la trame comme suit :

a) Vérifier le CRC FC et éliminer la trame si le CRCest invalide.
b) Si elle fonctionne en mode traduction d'adresse, remplacer le champ S_ID par l'alias de N_PORT du générateur de la trame, et le D_ID avec l'identifiant de N_PORT, du receveur de la trame. Les deux paramètres DEVRONT être obtenus du descripteur de session iFCP.
c) Si on traite un message spécial de service de liaison, remplacer la trame par une copie dont la charge utile a été modifiée comme spécifié au paragraphe 7.1.

La trame désencapsulée DEVRA alors être transmise au N_PORT spécifié dans le champ D_ID. Si le contenu de la trame n'a pas été modifié par la passerelle receveuse, un nouveau CRC FC DEVRA être calculé.

6. Messages de contrôle de session TCP

Les messages de contrôle de session TCP sont utilisés pour créer et gérer une session iFCP comme décrit au paragraphe 5.2.2. Ils sont passés entre les portails iFCP homologues et ne sont traités qu'au sein de la couche iFCP.
Le format de message se fonde sur le gabarit étendu de message de service de liaison canal fibre montré ci-dessous .

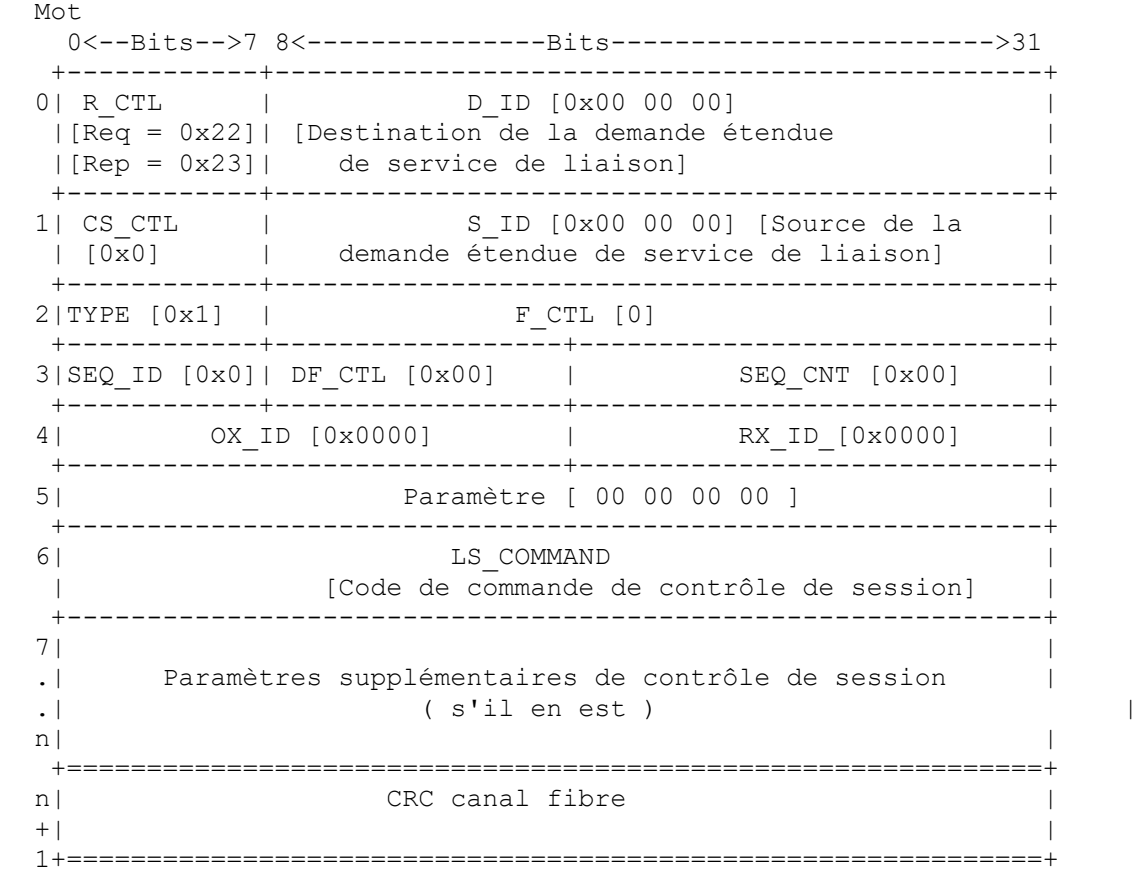


Figure 17. Format du message de contrôle de session

La valeur de LS_COMMAND pour la réponse reste la même que celle utilisée pour la demande.

La trame de contrôle de session se termine par un CRC canal fibre. La trame DEVRA être encapsulée et désencapsulée conformément aux règles spécifiées au paragraphe 5.3.

L'en-tête d'encapsulation pour la trame de service de liaison portant un message de contrôle de session DEVRA être réglé comme suit :

Champs d'en-tête d'encapsulation :
LS_COMMAND_ACC : 0
Fanions iFCP : SES = 1
TRP = 0
INT = 0
Code de SOF : codage SOFi3 (0x2E)
Code de EOF : codage EOFt (0x42)

Les mots d'horodatage d'encapsulation DEVRONT être réglés comme décrit pour chaque type de message.
Les mots de délimiteur SOF et EOF DEVRONT être réglés sur la base des codes de SOF et EOF spécifiés ci-dessus.

Le Tableau 6 fait la liste des valeurs allouées à l'octet 0 du champ LS_COMMAND pour les messages de commande de session iFCP.

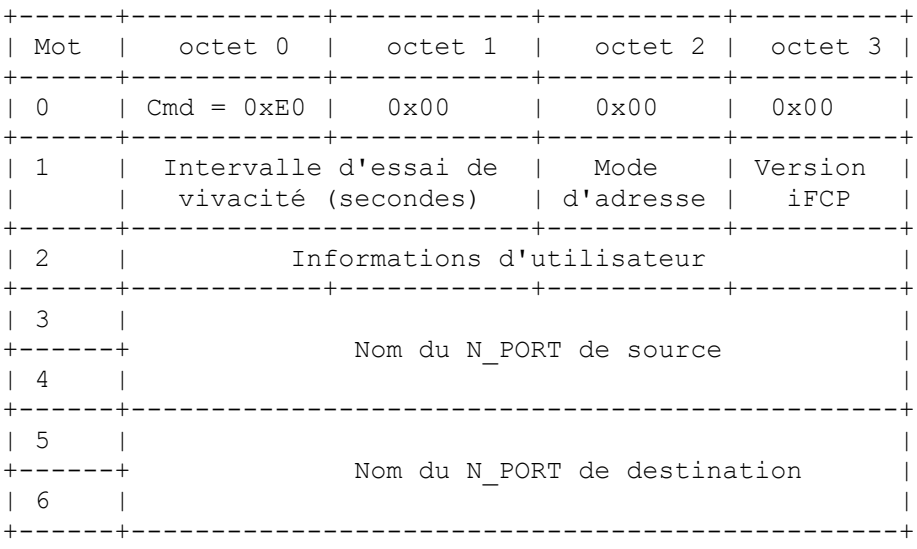
Champ LS_COMMAND, octet 0	**Fonction**	**Mnémonique**	**Prise en charge par iFCP**
0xE0	Connexion liée	CBIND	EXIGÉ
0xE4	Connexion non liée	UNBIND	EXIGÉ
0xE5	Essai de vivacité de connexion	LTEST	EXIGÉ
0x01-0x7F	Spécifique du fabricant		
0x00	Réservé -- non allouable		
Autres valeurs	Réservé		

Tableau 6. Champ de contrôle de session LS_COMMAND, valeurs de l'octet 0

6.1 Lien de connexion (CBIND, *Connection Bind*)

Comme décrit au paragraphe 5.2.2.2, le message CBIND et sa réponse sont utilisés pour lier un établissement de N_PORT à une connexion TCP spécifique et établir une session iFCP. Dans le message de demande CBIND, les N_PORT de source et de destination sont identifiés par leur nom d'accès mondial. Le mot d'horodatage dans l'en-tête d'encapsulation DEVRA être réglé à zéro dans les trames de messages de demande et de réponse.

Voici le format de la demande CBIND.



Mode d'adresse : mode d'adressage de la passerelle génératrice. 0 = mode traduction d'adresse; 1 = mode d'adresse transparent.

Version iFCP : numéro de version iFCP. DEVRA être 1.

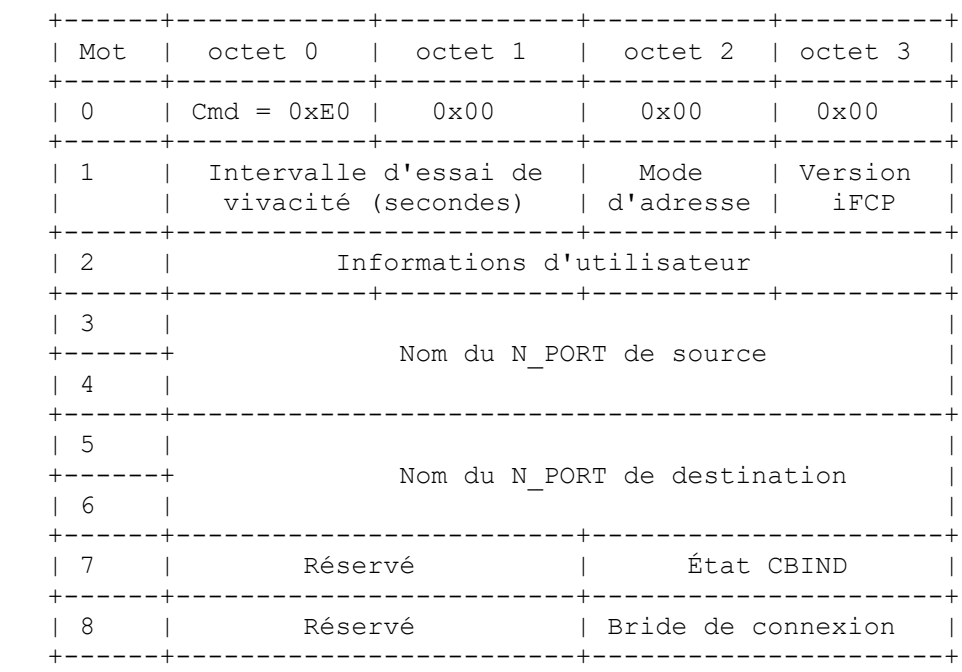
Intervalle d'essai de vicacité : Si il n'est pas zéro, demande que la passerelle receveuse transmette un message LTEST à l'intervalle spécifié en secondes. Si il est à zéro, les messages LTEST NE DEVRONT PAS être envoyés.

Informations d'utilisateur : Contient toutes données désirées par le demandeur. Ces informations DOIVENT recevoir un écho de la part du receveur dans le message de réponse CBIND.

Nom du N_PORT de source : nom d'accès mondial (WWPN) du N_PORT rattaché en local à la passerelle qui génère la demande CBIND.

Nom du N_PORT de destination : nom d'accès mondial (WWPN) du N_PORT rattaché en local à la passerelle qui reçoit la demande CBIND.

Voici le format de la réponse CBIND.



Longueur totale = 36

Mode d'adresse : mode traduction d'adresse de la passerelle qui répond ; 0 = mode traduction d'adresse, 1 = mode d'adresse transparent.

Version iFCP : numéro de vesion iFCP. Doit être réglé à 1.

Intervalle d'essai de vivacité : Si il n'est pas zéro, demande que la passerelle qui reçoit la réponse CBIND transmette un message LTEST à l'intervalle spécifié en secondes. Si c'est zéro, les messages LTEST NE DEVRONT PAS être envoyés.

Informations d'utilisateur : font écho à la valeur reçue dans le champ Informations d'utilisateur du message de demande CBIND.

Nom du N_PORT de source : contient le nom d'accès mondial (WWPN) du N_PORT rattaché localement à la passerelle qui produit la demande CBIND.

Nom du N_PORT de destination : contient le nom d'accès mondial (WWPN) du N_PORT rattaché localement à la passerelle qui produit la réponse CBIND.

État CBIND : indique le succès ou l'échec de la demande CBIND. Les valeurs de CBIND sont données plus loin.

Bride de connexion : contient une valeur allouée par la passerelle pour identifier la connexion. La bride de connexion est exigée quand la demande UNBIND est produite.

État CBIND	**Description**
0	Succès
1 – 15	Réservé
16	Échec – raison non spécifiée
17	Échec – il n'y a pas cet appareil
18	Échec – la session iFCP existe déjà
19	Échec – manque de ressources
20	Échec – mode de traduction d'adresse incompatible
21	Échec – numéro de version de protocole incorrect
22	Échec – passerelle non synchronisée (voir le paragraphe 8.2)
autres	Réservé

6.2. Connexion non liée (UNBIND)

UNBIND est utilisé pour terminer une session iFCP et dissocier la connexion TCP comme décrit au paragraphe 5.2.3.

Le message UNBIND est transmis sur la connexion qui doit être déliée. Les mots d'horodatage dans l'en-tête d'encapsulation devront être mis à zéro dans les trames de message de demande et réponse.

Le format du message de demande UNBIND est le suivant :

Mot	octet 0	octet 1	octet 2	octet 3
0	Cmd = 0xE4	0x00	0x00	0x00
1	Informations d'utilisateur			
2	Réservé		Bride de connexion	
3	Réservé			
4	Réservé			

Informations d'utilisateur : contient toutes données désirées du demandeur. Ces informations DOIVENT avoir un écho de la part du receveur dans le message de réponse UNBIND.

Bride de connexion : contient la valeur allouée par la passerelle provenant de la demande CBIND.

Le format du message de réponse UNBIND est le suivant :

Mot	octet 0	octet 1	octet 2	octet 3
0	Cmd = 0xE4	0x00	0x00	0x00
1	Informations d'utilisateur			
2	Réservé		Bride de connexion	
3	Réservé			
4	Réservé			
5	Réservé		État non lié	

Informations d'utilisateur : font écho à la valeur reçue dans le champ Informations d'utilisateur du message de demande UNBIND.

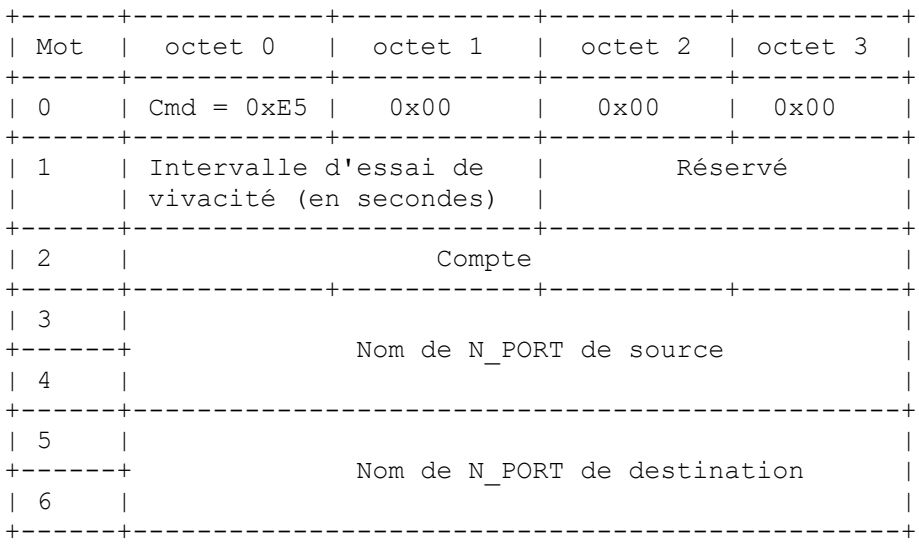
Bride de connexion : fait écho à la bride de connexion spécifiée dans le message de demande UNBIND.

État non lié : Indique le succès ou l'échec de la demande UNBIND comme suit :

État Unbind	**Description**
0	Réussi – pas d'autre état
1 – 15	Réservé
16	Échec – raison non spécifiée
18	Échec – identifiant de connexion invalide
autres	Réservé

6.3 LTEST – essai de vivacité de connexion

Le message LTEST est envoyé à l'intervalle spécifié dans la charge utile de demande ou réponse CBIND. L'horodatage d'encapsulation de LTEST DEVRA être réglé comme décrit au paragraphe 8.2.1 et peut être utilisé par le receveur pour calculer une estimation du délai de propagation. Cependant, la limite de délai de propagation NE DEVRA PAS être appliquée.



Intervalle d'essai de vivacité : copie de l'intervalle d'essai de vivacité spécifié dans le message de demande ou réponse CBIND.

Compte : valeur à accroissement monotone, initialisée à 0 et incrémentée de un à chaque message LTEST successif.

Nom de N_PORT de source : contient une copie du nom de N_PORT de source spécifié dans la demande CBIND.

Nom de N_PORT de destination : contient une copie du nom de N_PORT de destination spécifié dans la demande CBIND.

7. Services de liaison de canal fibre

Les services de liaison fournissent un ensemble de fonctions canal fibre qui permettent à un accès d'envoyer des informations de contrôle ou de demander à un autre accès d'effectuer une fonction de contrôle spécifique.

Il y a trois types de services de liaison :
a) Basique
b) Étendu
c) Spécifique d'ULP (FC-4)

Chaque message de service de liaison (demande et réponse) est porté par une séquence canal fibre et peut être segmenté en pluieurs trames.

La couche iFCP est chargée de transporter les messages de service de liaison à travers le réseau IP. Cela inclut de transposer les messages de service de liaison de façon appropriée du domaine de transport de canal fibre en celui du réseau IP. Ce procès peut exiger un traitement spécial et l'inclusion de données supplémentaires par la couche iFCP.

Chaque service de liaison DOIT être traité conformément à une des règles suivantes :
a) Traversée - le message de service de liaison et sa réponse DOIVENT être livrés au N_PORT receveur par la couche de protocole iFCP sans altérer la charge utile du message. Le message de service de liaison et sa réponse ne sont pas traités par la couche de protocole iFCP.
b) Spécial - s'applique à une demande ou réponse de service de liaison qui exige l'intervention de la couche iFCP avant la transmission au N_PORT de destination. De tels messages peuvent contenir des adresses canal fibre dans la charge utile ou peuvent exiger un autre traitement spécial.
c) Rejet - quand il est produit par un N_PORT rattaché en local, la demande de service de liaison spécifiée DOIT être rejetée par la passerelle iFCP. La passerelle DEVRA retourner une réponse LS_RJT avec un code de cause de 0x0B (Commande non acceptée) et une explication de code de cause de 0x0 (Pas d'explication supplémentaire).

Ce paragraphe décrit le traitement des services de liaison spéciaux, incluant la manière dont les données supplémentaires sont ajoutées à la charge utile du message. L'Appendice A énumère tous les services de liaison et la politique de traitement iFCP qui s'applique à chacun.

7.1 Messages de service de liaison spéciaux

Les messages de service de liaison spéciaux exigent l'intervention de la couche iFCP avant d'être transmis au N_PORT de destination. Cette intervention est requise afin de :
a) servir tout message de service de liaison qui exige un traitement spécial, comme un PLOGI, et
b) servir tout message de service de liaison qui a une adresse de N_PORT dans la charge utile en mode traduction d'adresse seulement.
Sauf si la description du service de liaison spécifie autre chose, la prise en charge de chaque service de liaison spécial est OBLIGATOIRE.

De tels messages DEVRONT être transmis dans une trame de canal fibre avec le format indiqué à la Figure 18 pour les services de liaison étendus ou à la Figure 19 pour les services de liaison FC-4.

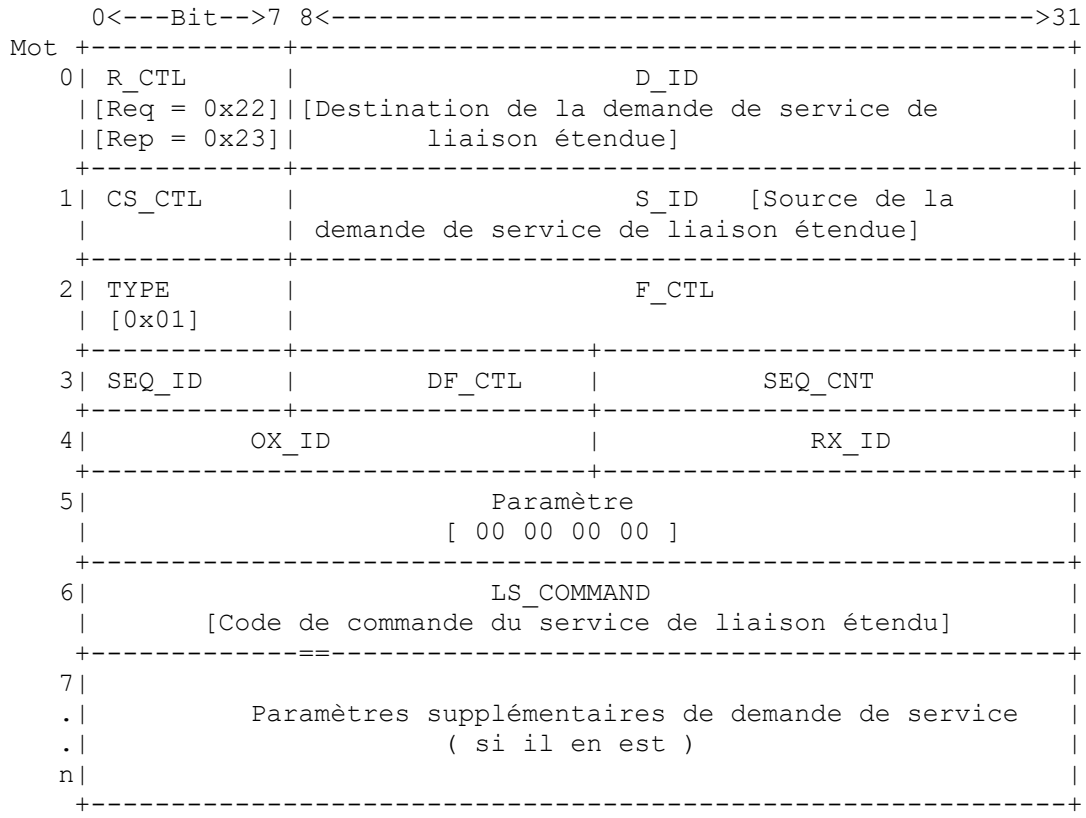


Figure 18. Format d'une trame de service de liaison étendu

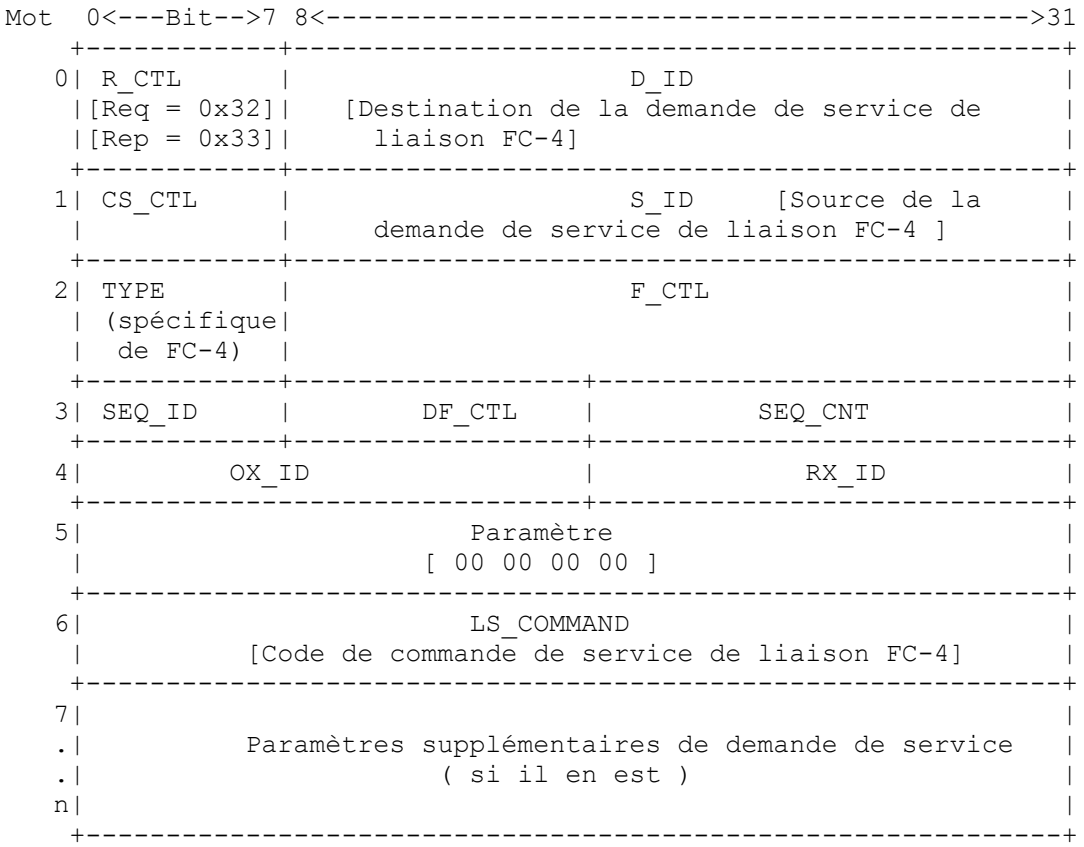


Figure 19. Format d'une trame de service de liaison FC-4

7.2 Services de liaison exigeant une traduction d'adresse de charge utile

Ce paragraphe décrit le traitement des trames de service de liaison qui contiennent des adresses de N_PORT dans la charge utile de trame. De telles adresses NE DEVRONT être traduites QUE lorsque la passerelle fonctionne en mode traduction d'adresse. Lorsque elle fonctionne en mode d'adresse transparent, ces adresses NE DEVRONT PAS être traduites, et de tels messages de service de liaison NE DEVRONT PAS être envoyés comme trames spéciales sauf si un autre traitement de la couche iFCP est requis.

Les données supplémentaires incluent des informations exigées par la passerelle receveuse pour convertir une adresse de N_PORT dans la charge utile en adresse de N_PORT dans l'espace d'adresse de la passerelle receveuse. Les règles suivantes définissent la manière dont de telles données supplémentaires devront être mises en paquet et référencées.

Pour un champ d'adresse de N_PORT, la passerelle génératrice de la trame DOIT régler la valeur dans la charge utile pour identifier le type de traduction d'adresse comme suit :

0x00 00 01 - La passerelle qui reçoit la trame du réseau IP DOIT remplacer le contenu du champ par l'alias de N_PORT du générateur de la trame. Ce type de traduction DOIT être utilisé quand l'adresse à convertir est celle du N_PORT de source.

0x00 00 02 - La passerelle qui reçoit la trame du réseau IP DOIT remplacer le contenu du champ par l'identifiant de N_PORT du N_PORT de destination. Ce type de traduction DOIT être utilisé quand l'adresse à convertir est celle du N_PORT de destination.

0x00 00 03 - La passerelle qui reçoit la trame du réseau IP DOIT faire référence aux données supplémentaires spécifiées pour régler le contenu du champ. Les informations supplémentaires sont l'identifiant mondial de 64 bits du N_PORT, tel qu'établi dans la spécification canal fibre [FC-FS]. Si elle ne fait pas par ailleurs partie de la charge utile du service de liaison, cette information DOIT être ajoutée conformément à la description de service de liaison applicable. Sauf mention contraire, ce type de traduction NE DEVRA PAS être utilisé si l'adresse à convertir correspond à celle du générateur ou du receveur de la trame.

Comme les règles d'adressage de canal fibre interdisent l'allocation d'adresses de tissu avec un identifiant de domaine de 0, les codes ci-dessus ne vont jamais correspondre à des identifiants valides de tissu de N_PORT.

Si la passerelle envoyeuse ne peut pas obtenir l'identifiant mondial d'un N_PORT, elle DEVRA terminer la demande avec un message LS_RJT comme décrit dans [FC-FS]. Le code de cause DEVRA être réglé à 0x07 (Erreur de protocole) et l'explication DEVRA être réglée à 0x1F (Identifiant de N_PORT invalide).

Les données supplémentaires sont envoyées avec les trames de demande de service de liaison, ou :
a) en ajoutant les données nécessaires à la fin de la trame de service de liaison,
b) en étendant la séquence avec des trames supplémentaires.

Dans le premier cas, une nouvelle trame DEVRA être créée dont la longueur inclut les données supplémentaires. La procédure pour étendre la séquence de service de liaison avec des trames additionnelles dépend du type de service de liaison.

Pour chaque champ qui exige la traduction d'adresse, la passerelle receveuse DEVRA faire référence au type de traduction codé dans le champ et le remplacer par l'adresse de N_PORT comme montré au Tableau 7.

Code de type de traduction	**Traduction de N_PORT**
0x00 00 01	Remplace le contenu du champ par l'alias de N_PORT du générateur de la trame.
0x00 00 02	Remplace le contenu du champ par l'identifiant du N_PORT du receveur de la trame.
0x00 00 03	Recherche de N_PORT via une interrogation iSNS. Si rattachement local, remplacer par l'identifiant de N_PORT. Si rattachement distant, remplacer par l'alias de N_PORT du N_PORT distant. Descripteur (voir au paragraphe 5.2.2.1).

Tableau 7. Traduction d'adresse de service de liaison

Pour la traduction de type 3, la passerelle receveuse DEVRA obtenir les informations nécessaires pour remplir le champ dans la charge utile de la trame de service de liaison en convertissant l'identifiant mondial de N_PORT spécifié en une adresse IP de passerelle et identifiant de N_PORT. Ces informations DOIVENT être obtenues par une interrogation de serveur de noms iSNS. Si l'interrogation réussit, la passerelle DEVRA terminer la demande avec un message de réponse LS_RJT comme décrit dans [FC-FS]. Le code de cause DEVRA être 0x07 (Erreur de protocole) et l'explication DEVRA être 0x1F (Identifiant de N_PORT invalide).

Après l'application des données supplémentaires, la passerelle receveuse DEVRA transmettre les trames résultantes de service de liaison au N_PORT de destination sans les informations supplémentaires.

7.3 Services de liaison canal fibre traités par iFCP

Les messages du service de liaison étendu (ELS, *Extended Link Service*) et FC-4 suivants doivent recevoir un traitement spécial.

Messages de service de liaison étendu	**LS_COMMAND**	**Mnémonique**
Interrompre l'échange	0x06 00 00 00	ABTX
Découverte d'adresse	0x52 00 00 00	ADISC
Découverte d'adresse acceptée	0x02 00 00 00	ADISC ACC
Réponse de protocole de résolution d'adresse FC	0x55 00 00 00	FARP-REPLY
Demande de protocole de résolution d'adresse FC	0x54 00 00 00	FARP-REQ
Désétablissement	0x05 00 00 00	LOGO
Établissement d'accès	0x30 00 00 00	PLOGI
Échange en lecture concis	0x13 00 00 00	REC
Acceptation d'échange en lecture concis	0x02 00 00 00	REC ACC
Bloc d'état d'échange de lecture *(Read Exchange Status Block)*	0x08 00 00 00	RES
Acceptation de bloc d'état d'échange en lecture	0x02 00 00 00	RES ACC
Bloc d'état d'erreur de liaison en lecture	0x0F 00 00 00	RLS
Bloc d'état de séquence en lecture	0x09 00 00 00	RSS
Qualificatif de récupération de réinstallation	0x12 00 00 00	RRQ
Initiative de séquence de demande	0x0A 00 00 00	RSI
Examen de la boucle distante *(Scan Remote Loop)*	0x7B 00 00 00	SRL
Désétablissement de processus de tiers	0x24 00 00 00	TPRLO
Acceptation de désétablissement de processus de tiers	0x02 00 00 00	TPRLO ACC

Messages de service de liaison FC-4	**LS_COMMAND**	**Mnémonique**
Échange concis FCP en lecture	0x13 00 00 00	FCP REC
Acceptation d'échange concis FCP en lecture	0x02 00 00 00	FCP REC ACC

Chaque trame de canal fibre encapsulée qui fait partie d'un service de liaison spécial DOIT avoir le bit SPC réglé à un dans le champ Fanions iFCP de l'en-tête d'encapsulation, comme spécifié au paragraphe 5.3.1. Si une réponse de service de liaison ACC exige un traitement spécial, la passerelle qui répond DEVRA placer une copie des bits 0 à 7 de la LS_COMMAND, provenant de la trame de demande de service de liaison, dans le champ LS_COMMAND_ACC de l'en-tête d'encapsulation ACC. Les données supplémentaires (si il en est) DOIVENT être ajoutées comme décrit dans le paragraphe suivant.

Le format de chaque message spécial de service de liaison, incluant les données supplémentaires, lorsque applicable, est montré dans le paragraphe suivant. Chaque description montre le format de base, comme spécifié dans la norme FC applicable, suivi par les données supplémentaires comme le montre l'exemple ci-dessous.

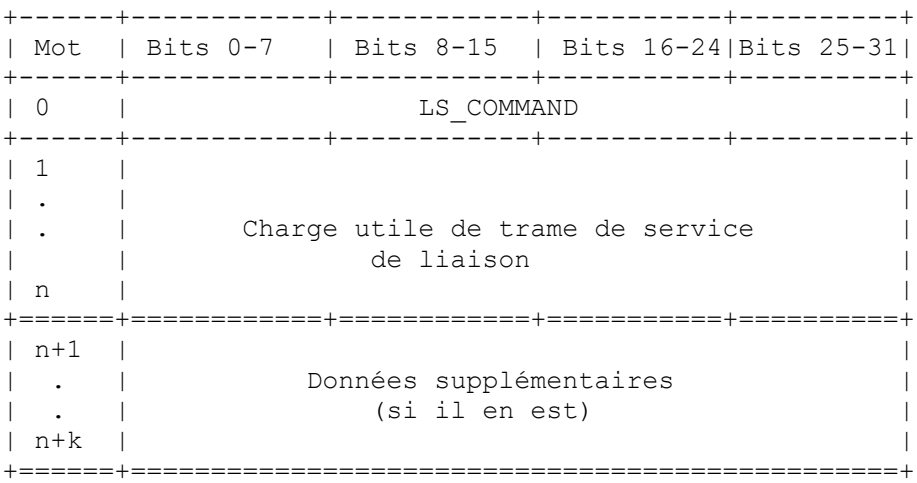


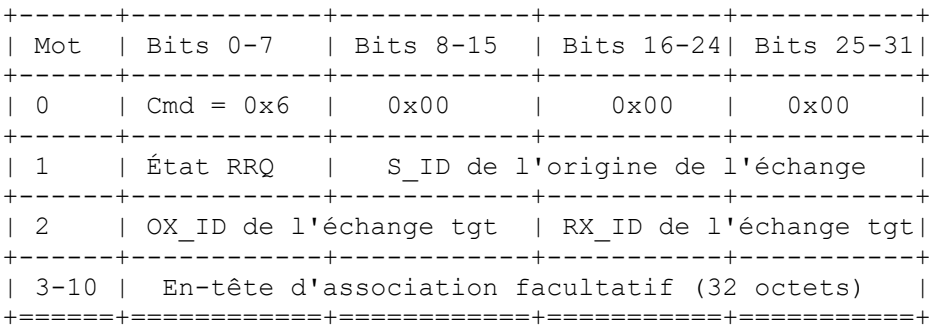
Figure 20. Charge utile de trame spéciale de service de liaison

7.3.1 Services spéciaux de liaison étendus

Les paragraphes qui suivent définissent les services de laison étendus pour lesquels un traitement spécial est requis.

7.3.1.1 Interruption d'échange (ABTX)

Format d'ELS :

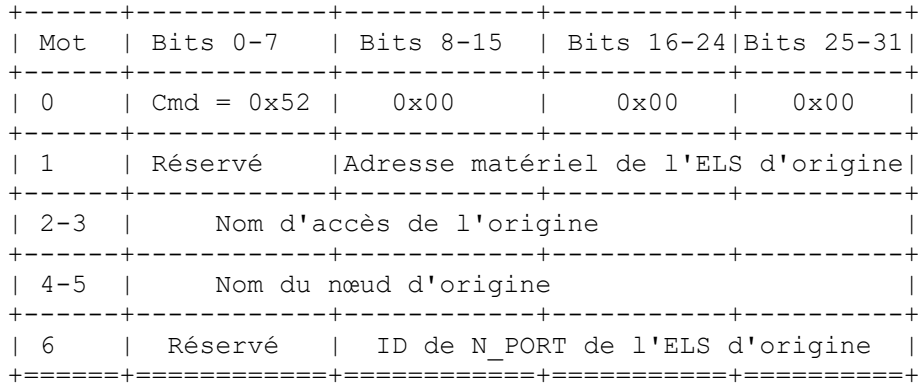


Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
S_ID de l'origine de l'échange	1, 2	N/A

Autre traitement spécial : aucun.

7.3.1.2 Découverte d'adresse (ADISC)

Format d'ELS ADISC :

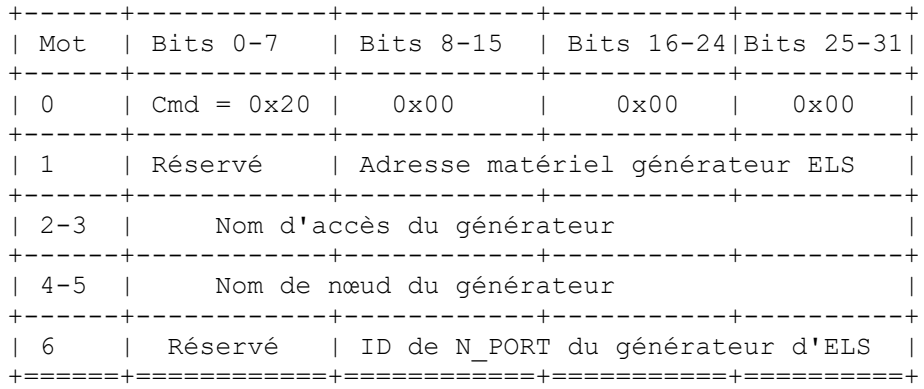


Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x52	0x00	0x00	0x00
1	Réservé	Adresse matériel de l'ELS d'origine		
2-3	Nom d'accès de l'origine			
4-5	Nom du nœud d'origine			
6	Réservé	ID de N_PORT de l'ELS d'origine		

Champs exigeant traduction d'adresse Type de traduction (§ 7.2) Données supplémentaires (seulement type 3)
Identifiant de N_PORT du générateur d'ELS 1 N/A
Autre traitement spécial : L'adresse de matériel du générateur d'ELS DEVRA être à 0.

7.3.1.3 Acceptation de découverte d'adresse (ADISC ACC)

Format de l'ELS ADISC ACC :



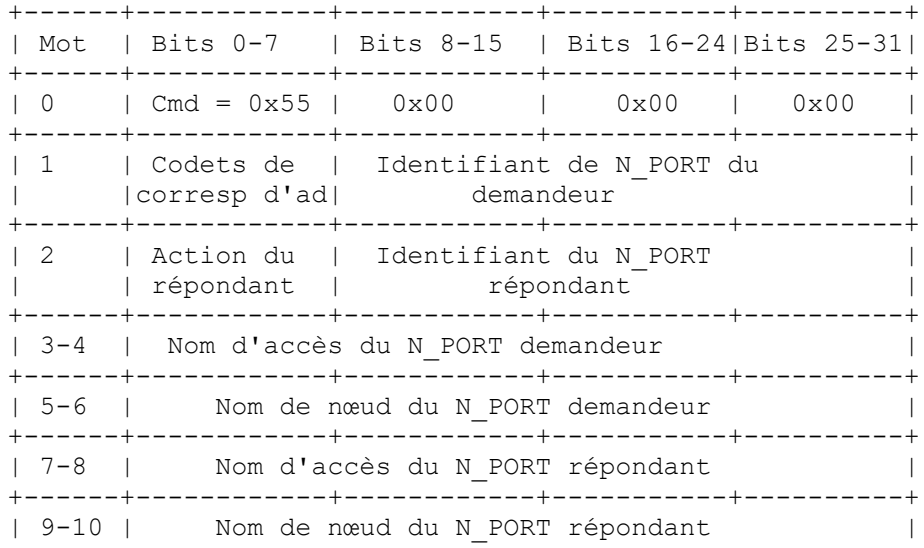
Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x20	0x00	0x00	0x00
1	Réservé	Adresse matériel générateur ELS		
2-3	Nom d'accès du générateur			
4-5	Nom de nœud du générateur			
6	Réservé	ID de N_PORT du générateur d'ELS		

Champs exigeant traduction d'adresse Type de traduction (§ 7.2) Données supplémentaires (seulement type 3)
ID du N_PORT du générateur d'ELS 1 N/A
Autre traitement spécial : l'adresse de matériel de l'ELS générateur DEVRA être réglée à 0.

7.3.1.4 Réponse de protocole de résolution d'adresse FC (FARP-REPLY)

L'ELS FARP-REPLY est utilisé en conjonction avec l'ELS FARP-REQ (voir au paragraphe 7.3.1.5) pour effectuer les services de résolution d'adresse exigés par le protocole [FC-VI] et la transposition de canal fibre entre IP et ARP spécifiée dans la [RFC2625].

Format de l'ELS FARP-REPLY :



Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x55	0x00	0x00	0x00
1	Codets de corresp d'ad	Identifiant de N_PORT du demandeur		
2	Action du répondant	Identifiant du N_PORT répondant		
3-4	Nom d'accès du N_PORT demandeur			
5-6	Nom de nœud du N_PORT demandeur			
7-8	Nom d'accès du N_PORT répondant			
9-10	Nom de nœud du N_PORT répondant			

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
11-14	Adresse IP du N_PORT demandeur			
15-18	Adresse IP du N_PORT répondant			

Champs exigeant traduction d'adresse	Type de Traduction (§ 7.2)	Données supplémentaires (seulement type 3)
Identifiant du N_PORT demandeur	2	N/A
Identifiant du N_PORT répondant	1	N/A

Autre traitement spécial : aucun

7.3.1.5 Demande de protocole de résolution d'adresse FC (FARP-REQ)

L'ELS FARP-REQ est utilisé en conjonction avec le protocole [FC-VI] et la transposition de IP en FC de la [RFC2625] pour effectuer la résolution d'adresse FC dans un tissu FC. L'ELS FARP-REQ est généralement dirigé sur le serveur de diffusion du tissu à l'adresse bien connue 0xFF-FF-FF pour retransmission à tous les N_PORT rattachés.
Le paragraphe 9.4 décrit la mise en œuvre de iFCP de la fonction de serveur de diffusion FC dans un tissu iFCP.
Format de l'ELS FARP_REQ :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x54	0x00	0x00	0x00
1	Codets de corres d'adr	Identifiant du N_PORT demandeur		
2	Action du répondant	Identifiant du N_PORT répondant		
3-4	Nom d'accès du N_PORT demandeur			
5-6	Nom de nœud du N_PORT demandeur			
7-8	Nom d'accès du N_PORT répondant			
9-10	Nom de nœud du N_PORT répondant			
11-14	Adresse IP du N_PORT demandeur			
15-18	Adresse IP du N_PORT répondant			

Champs exigeant traduction d'adresse	Type de Traduction (§ 7.2)	Données supplémentaires (seulement type 3)
Identifiant du N_PORT demandeur	3	Nom d'accès du N_PORT demandeur
Identifiant du N_PORT répondant	3	Nom d'accès du N_PORT répondant

Autre traitement spécial : aucun.

7.3.1.6 Logout (LOGO) and LOGO ACC

Format d'ELS:

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x5	0x00	0x00	0x00
1	Réservé	ID du N_PORT à désétablir		
2-3	Nom d'accès de l'origine du LOGO (8 octets)			

Cet ELS DEVRA toujours être envoyé dans un ELS spécial sans considération du mode de traduction appliqué.

Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
ID du N_PORT à désintaller	1	N/A

Autre traitememnt spécial : voir au paragraphe 5.2.3.

7.3.1.7 Étalissement d'accès (PLOGI, Port Login) et PLOGI ACC

Un ELS PLOGI établit des communications canal fibre entre deux N_PORT et déclenche la création d'une session iFCP si il n'en existe pas déjà une. La demande PLOGI et sa réponse d'acceptation (ACC) portent les informations qui identifient le N_PORT d'origine, incluant une spécification de ses capacités. Si le N_PORT de destination accepte la demande d'établissement, il envoie une réponse Accepte (une trame ACC avec la charge utile PLOGI) spécifiant ses capacités. Cet échange établit l'environnement de fonctionnement pour les deux N_PORT.

La figure suivante est reprise de [FC-FS] et montre le format du message PLOGI pour la demande et pour la réponse d'acceptation (ACC). Un N_PORT rejettera une demande PLOGI en transmettant un message LS_RJT ne contenant pas de charge utile.

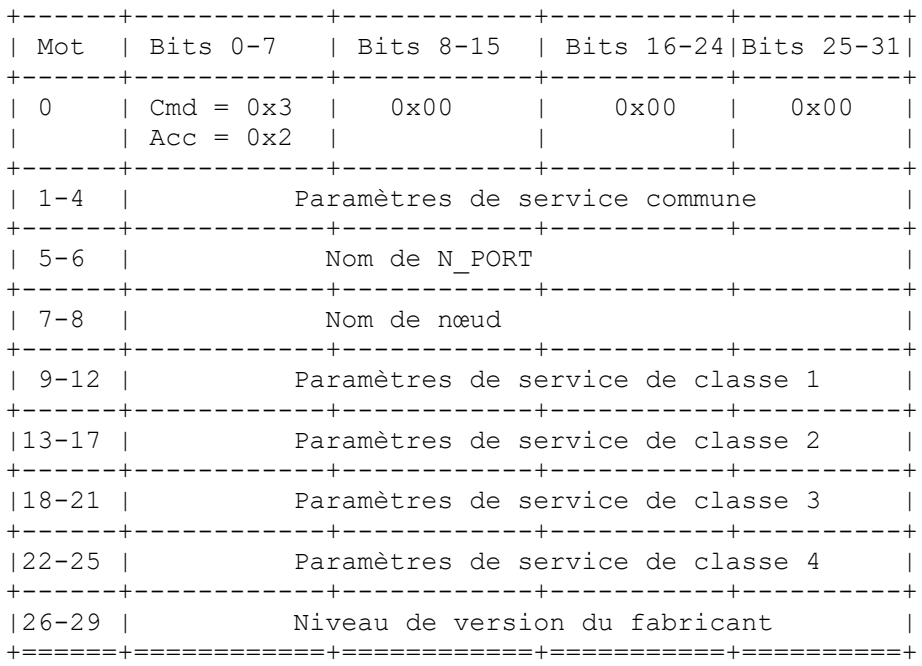


Figure 21. Format des charges utiles de demande PLOGI et ACC

Les détails des champs ci-dessus, incluant les paramètres de service communs et fondés sur la classe, se trouvent dans [FC-FS].

Traitement spécial : comme spécifié au paragraphe 5.2.2.2, une demande PLOGI adressée à un N_PORT rattaché à distance DOIT causer la création d'une session iFCP si il n'en existe pas déjà une. Autrement, les charges utiles PLOGI et PLOGI ACC DOIVENT être passées sans modification au N_PORT de destination en utilisant la session iFCP existante. Dans l'un et l'autre cas, le bit SPC doit être établi dans l'en-tête d'encapsulation de trame comme spécifié au paragraphe 5.3.3. Si le CBIND pour créer la session iFCP échoue, la passerelle qui l'a produit DEVRA terminer le PLOGI avec une réponse LS_RJT. Le code de cause et l'explication de code de cause DEVRONT être choisis dans le Tableau 8 sur la base de l'état d'échec de CBIND.

État d'échec CBIND	Code de cause du LS_RJT	Explication du code de cause LS_RJT
Raison non spécifiée (16)	Demande de commande impossible (0x09)	Pas d'explication supplémentaire (0x00)
Pas de tel appareil (17)	Demande de commande impossible (0x09)	Nom de N_PORT invalide (0x0D)
Manque de ressoures (19)	Demande de commande impossible (0x09)	Ressources insuffisantes pour prendre en charge l'établissement (0x29)
Mode de traduction d'adresse incompatible (20)	Demande de commande impossible (0x09)	Pas d'explication supplémentaire (0x00)
Numéro de version de protocole iFCP incorrect (21)	Demande de commande impossible (0x09) |	Pas d'explication supplémentaire (0x00)
Passerelle non synchrone (22)	Demande de commande impossible (0x09)	Pas d'explication supplémentaire (0x00)

Tableau 8. État de PLOGI LS_RJT pour les échecs de CBIND

7.3.1.8 Échange de lecture concis (REC, *Read Exchange Concise*)

Format de la demande de service de liaison :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x13	0x00	0x00	0x00
1	Réservé	S_ID de l'origine de l'échange		
2	OX_ID		RX_ID	
3-4	Nom d'accès de l'origine de l'échange (8 octets) (seulement pour le type de traduction 3)			

Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
S_ID de l'origine de l'échange	1, 2, ou 3	Nom d'accès de l'origine de l'échange

Autre traitement spécial : aucun.

7.3.1.9 Acceptation d'échange en lecture concis (REC ACC, *Read Exchange Concise Accept*)

Format de la réponse REC ACC :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Acc = 0x02	0x00	0x00	0x00
1	OX_ID		RX_ID	
2	Réservé	Identifiant d'adresse d'origine		
3	Réservé	Identifiant d'adresse du répondant		
4	FC4VALUE (valeur dépendante de FC-4)			
5	E_STAT (état de l'échange)			
6-7	Nom d'accès de l'origine de l'échange (8 octets)			
8-9	Nom d'accès du répondant à l'échange (8 octets)			

Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
Identifiant de l'adresse d'origine	1, 2, ou 3	Nom de l'accès de l'origine de l'échange
Identifiant de l'adresse du répondant	1, 2, ou 3	Nom de l'accès du répondant à l'échange

Quand des données supplémentaires sont nécessaitres, la trame DEVRA toujours être étendue par 4 mots comme montré ci-dessus. Si le type de traduction pour l'identifiant d'adresse d'origine ou l'identifiant d'adresse du répondant est 1 ou 2, le nom d'accès correspondant de 8 octets DEVRA être réglé tout à zéro.
Autre traitement spécial : aucun.

7.3.1.10 Bloc d'état déchange en lecture (RES, *Read Exchange Status Block*)

Format d'ELS :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x13	0x00	0x00	0x00
1	Réservé	S_ID de l'origine de l'échange		
2	OX_ID		RX_ID	

3-10	En-tête d'association (facultativement exigé)
11-12	Nom d'accès d'origine de l'échange (8 octets)

Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
S_ID de l'origine de l'échange	1, 2, ou 3	Nom d'accès d'origine de l'échange

Autre traitement spécial : aucun.

7.3.1.11 Acceptation de bloc d'état déchange en lectur (RES ACC)

Format de l'ELS de réponse d'acceptation :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Acc = 0x02	0x00	0x00	0x00
1	OX_ID		RX_ID	
2	Réservé	ID de N_PORT d'orig. de l'échange		
3	Réservé	ID de N_PORT répondant à l'échange		
4	Bits d'état d'échange			
5	Réservé			
6-n	Paramètres de service et d'état de séquence comme décrit dans [FC-FS]			
n+1-n+2	Nom d'accès de l'origine de l'échange (8 octets)			
n+3-n+4	Nom d'accès du répondant à l'échange (8 octets)			

Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
ID de N_PORT de l'origine de l'échange	1, 2, ou 3	Nom d'accès de l'origine de l'échange
ID de N_PORT du répondant à l'échange	1, 2, ou 3	Nom d'accès du répondant à l'échange

Quand des données supplémentaires sont requises, l'ELS DEVRA être étendu de 4 mots comme montré ci-dessus. Si le type de traduction pour l'identifiant de N_PORT de l'origine de l'échange ou l'identifiant de N_PORT du répondant à l'échange est 1 ou 2, le nom d'accès correspondant de 8 octets DEVRA être réglé tout à zéro.
Autre traitement spécial : aucun.

7.3.1.12 État d'erreur de liaison en lecture (RLS, *Read Link Error Status*)

Format d'ELS :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x0F	0x00	0x00	0x00
1	Réservé	Identifiant de N_PORT		
2-3	Nom de l'accès du N_PORT (8 octets)			

Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
Identifiant de N_PORT	1, 2, ou 3	Nom de l'accès du N_PORT

Autre traitement spécial : aucun.

7.3.1.13 Bloc d'état de séquence en lecture (RSS, *Read Sequence Status Block*)

Format d'ELS :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x09	0x00	0x00	0x00
1	SEQ_ID	S_ID d'origine de l'échange		
2	OX_ID		RX_ID	
3-4	Nom d'accès d'origine de l'échange (8 octets)			

Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
S_ID de l'origine de l'échange	1, 2, ou 3	Nom d'accès de l'origine de l'échange

Autre traitement spécial : aucun.

7.3.1.14 Qualificatif de récupération de réinstallation (RRQ, *Reinstate Recovery Qualifier*)

Format d'ELS :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x12	0x00	0x00	0x00
1	Réservé	S_ID d'origine de l'échange		
2	OX_ID		RX_ID	
3-10	En-tête d'association (facultativement exigé)			

Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
S_ID d'origine de l'échange	1 ou 2	N/A

Autre traitement spécial : aucun.

7.3.1.15 Initiative de demande de séquence (RSI, *Request Sequence Initiative*)

Format d'ELS :

Mot	Bits 0-7	Bits 8-15	Bits 16-24	Bits 25-31
0	Cmd = 0x0A	0x00	0x00	0x00
1	Réservé	S_ID d'origine de l'échange		
2	OX_ID		RX_ID	
3-10	En-tête d'association (facultativement exigé)			

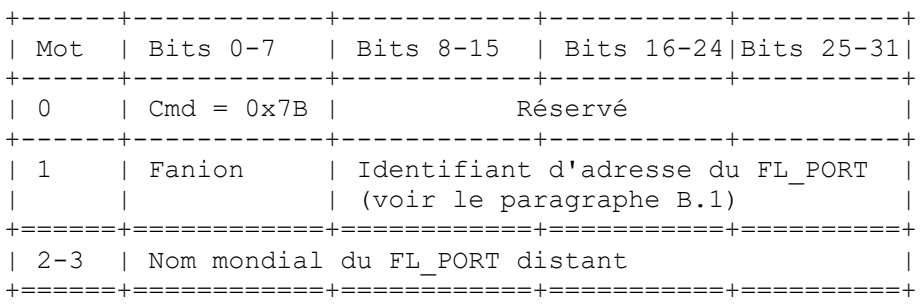
Champs exigeant traduction d'adresse	Type de traduction (§ 7.2)	Données supplémentaires (seulement type 3)
S_ID d'origine de l'échange	1 ou 2	N/A

Autre traitement spécial : aucun.

7.3.1.16 Examen de la boucle distante (SRL, *Scan Remote Loop*)

SRL permet qu'une boucle distante soit examinée pour détecter des changemens de la configuration de l'appareil. Tout changement va déclencher une notification de changement d'état de canal fibre et une mise à jour de la base de données iSNS.

Format d'ELS :



Champs exigeant traduction d'adresse Type de traduction (§ 7.2) Données supplémentaires (seulement type 3)
Identifiant d'adresse du FL_PORT 3 Nom mondial du FL_PORT distant
Autre traitement spécial :
Le champ D_ID est l'adresse du contrôleur de domaine associé à la boucle distante. Le format de l'adresse du contrôleur de domaine est l'hexadécimal "FF FC" || Domain_ID, où Domain_ID est l'alias alloué par la passerelle qui représente la passerelle distante ou l'élément de commutation qui est interrogé. Après traduction par la passerelle distante, le D_ID identifie la passerelle ou élément de commutation à examiner au sein de la région passerelle distante.

Le champ FLAG définit la portée du SRL. Si il est réglé à 0, toutes les interfaces d'accès de boucle sur l'élément de commutation ou passerelle donné sont examinés. Si il est à un, l'interface d'accès de boucle sur la passerelle ou élément de commutation à examiner DOIT être spécifié dans les bits 8 à 31.
Si le champ Fanions est à zéro, la demande SRL NE DEVRA PAS être envoyée comme ELS spécial.
Si le Domain_ID représente un commutateur ou passerelle distant et qu'il n'existe pas de session iFCP avec le contrôleur de domaine distant, le passerelle demandeuse DEVRA créer la session iFCP.

7.3.1.17 Désétablissement de processus de tiers (TPRLO, *Third Party Process Logout*)

TPRLO fournit un mécanisme pour qu'un N_PORT (tiers) supprime une ou plusieurs sessions de processus d'établissement qui existent entre le N_PORT de destination et les autres N_PORT spécifiés dans la commande. Cette commande inclut une ou plusieurs pages de paramètres de désétablissement TPRLO, dont chacun, combiné au N_PORT de destination, identifie un établissement de processus à terminer par la commande.

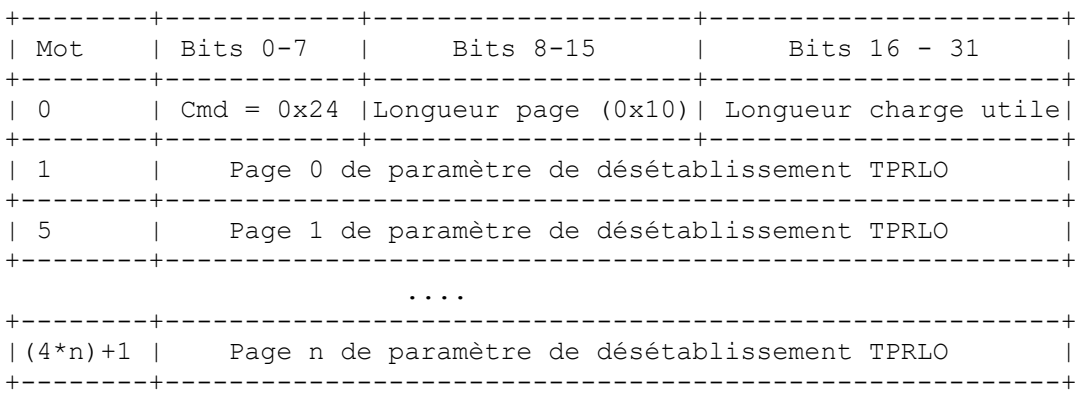
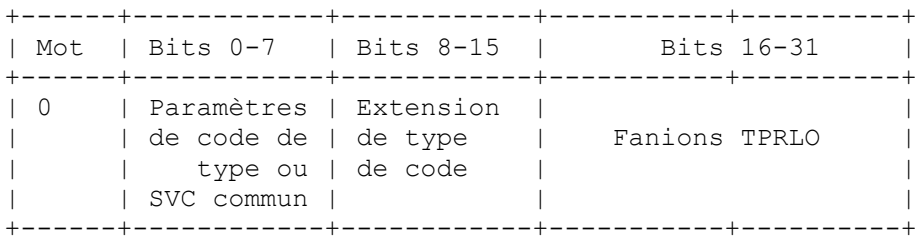


Figure 22. Format de l'ELS TPRLO

Chaque page de paramètre TPRLO contient des paramètres qui identifient une ou plusieurs paires d'images et peuvent être associés à un seul type de protocole FC-4 qui est commun à tous les types de protocoles FC-4 entre la paire d'images spécifiée ou global pour toutes les paires d'images spécifiées. Le format d'une page TPRLO qui exige la traduction d'adresse est montré à la Figure 23. On trouvera des informations supplémentaires sur TPRLO dans [FC-FS].



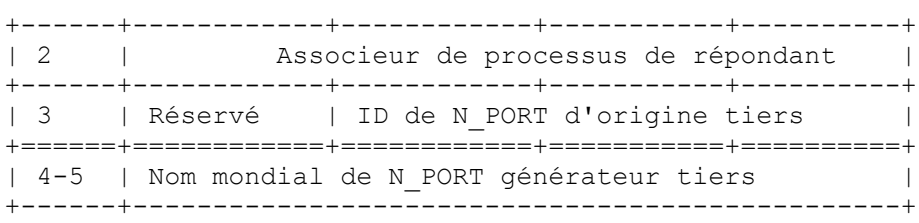


Figure 23. Format d'une page de paramètre TPRLO augmenté

Les fanions TPRLO qui affectent un traitement d'ELS supplémentaire sont comme suit :

Bit 18 : Validité du N_PORT générateur tiers. Établi à un, ce bit indique que le mot 3, bits 8 à 31 (Identifiant de N_PORT générateur tiers, est significatif.

Bit 19 : Désétablissement de traitement global. Établi à un, ce bit indique que toutes les paires d'images pour tous les N_PORT du protocole FC-4 spécifiés devront être invalidés. Quand la valeur de ce bit est un, seule une page de paramètre de désétablissement est permise dans la charge utile TPRLO.

Si le bit 18 a une valeur de zéro et le bit 19 a une valeur de un dans le fanion TPRLO, l'ELS NE DEVRA alors PAS être envoyé comme ELS spécial.

Autrement, la passerelle d'origine DEVRA traiter l'ELS comme suit :
a) le premier mot de la charge utile TPRLO NE DEVRA PAS être modifié ;
b) chaque page de paramètre TPRLO devra être étendue de deux mots comme le montre la Figure 23.
c) Si le bit 18 du mot 0 (Validité de l'identifiant de N_PORT générateur tiers) dans le champ Fanions TPRLO a une valeurs de un, alors l'envoyeur devra placer le nom d'accès mondial du N_PORT de l'appareil canal fibre dans les mots d'extension. L'ID de N_PORT DEVRA être réglé à 3. Autrement, le contenu des mots d'extension et l'ID de N_PORT générateur tiers DEVRA être réglé à zéro.
d) L'ELS générateur DEVRA établir le bit SPC dans l'en-tête d'encapsulation de chaque trame augmentée qui compose l'ELS (voir au paragraphe 5.3.1).
e) Si l'ELS contient une seule page de paramètres TPRLO, le générateur DEVRA augmenter la longueurde trame comme nécessaire pour inclure la page de paramètre étendu.
f) Si l'ELS à augmenter contient plusieurs pages de paramètre TPRLO, les trames FC créées pour contenir la charge utile ELS augmentée NE DEVRONT PAS excéder la taille maximum de trame qui peut êtte acceptée par le N_PORT de destination.

Chaque trame de canal fibre DEVRA contenir un nombre entier de pages de paramètres TPRLO étendus. Le nombre maximum de pages de paramètres TPRLO étendus dans une trame DEVRA être limité au nombre qui peut être contenu sans excéder la limite supérieure ci-dessus. De nouvelles trames résultant de l'extension des pages de TPRLO pour inclure les données supplémentaires DEVRONT être créées en étendant le SEQ_CNT dans l'en-tête de trame de canal fibre. Le SEQ_ID NE DEVRA PAS être modifié.

La passerelle qui reçoit l'ELS TPRLO augmenté DEVRA générer des trames d'ELS à envoyer au N_PORT de destination en copiant le mot 0 de la charge utile de l'ELS et en traitant chaque page de paramètre augmenté comme suit :
a) Si le mot 0, bit 18, a une valeur de un, créer une page de paramètre en copiant les mots 0 à 2 de la page de paramètre augmenté. L'identifiant de N_PORT générateur tiers dans le mot 3 devra être généré par référence aux données supplémentaires, comme décrit au paragraphe 7.2.
b) Si le mot 0, bit 18, a une valeur de zéro, créer une page de paramètre en copiant les mots 0 à 3 de la page de paramètre augmenté.

La taille de chaque trame à envoyer au N_PORT de destination NE DOIT PAS excéder la taille maximum de trame que le N_PORT de destination peut accepter. L'identifiant de séquence dans chaque en-tête de trame DEVRA être copié de l'ELS augmenté, et le compte de séquence DEVRA être à accroissement monotone.

7.3.1.18 Acceptation de désétablissement de tiers (TPRLO ACC, *Third Party Logout Accept*)

Le format de la trame TPRLO ACC est montré par la Figure 24.

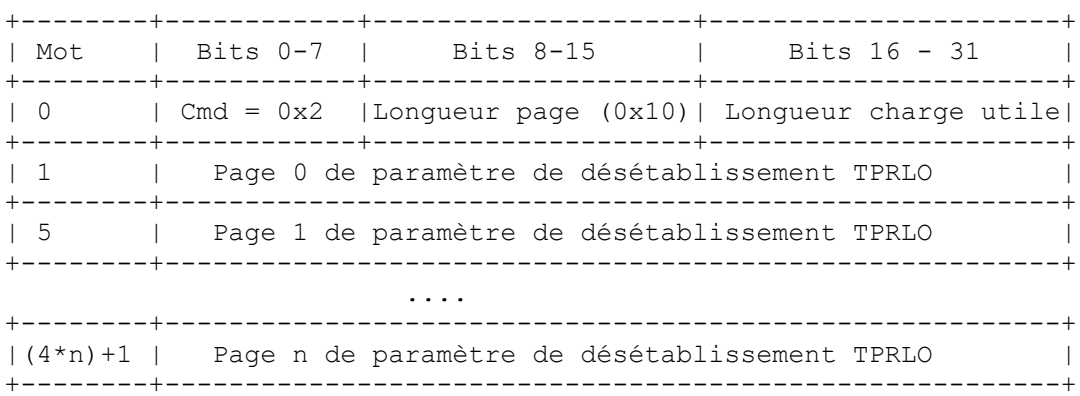


Figure 24. Format de l'ELS TPRLO ACC

Le format de la page de paramètre et les règles pour l'augmentation de page de paramètre sont comme spécifié au paragraphe 7.3.1.17.

7.3.2 Services spéciaux de liaison FC-4

Les paragraphes qui suivent définissent les services de liaison FC-4 pour lesquels un traitement spécial est nécessaire.

7.3.2.1 Services de liaison FC-4 définis par FCP

Le format des trames de service de liaison FC-4 défini par FCP se trouve dans [FCP-2].

7.3.2.1.1 Échange concis en lecture FCP (FCP REC, *FCP Read Exchange Concise*)

Le format de charge utile pour ce service de liaison est identique à celui du service de liaison REC étendu spécifié au paragraphe 7.3.1.8 et DEVRA être traité comme décrit dans ce paragraphe. La version FC-4 va être remplacée par [FCP-2]. Cependant, afin de prendre en charge les appareils mis en œuvre avec les révisions précoces de FCP-2, une passerelle iFCP DOIT prendre en charge les deux versions.

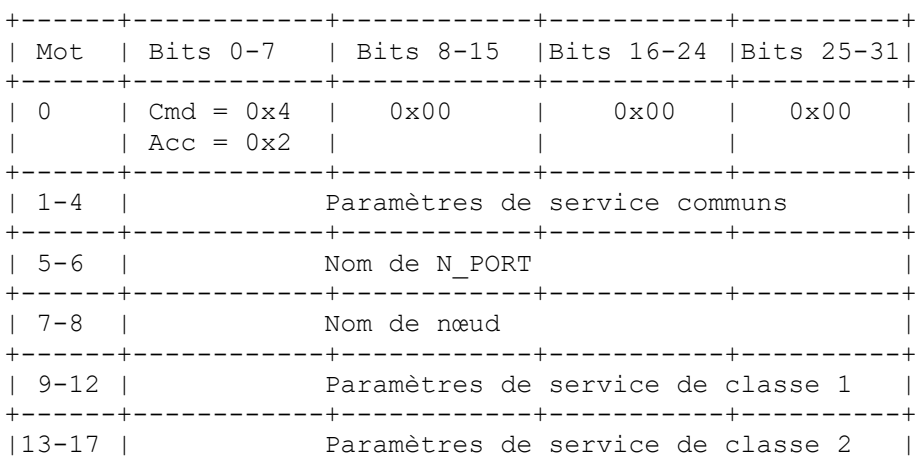
7.3.2.1.2 Acceptation d'échange concis en lecture FCP (FCP REC ACC, *FCP Read Exchange Concise Accept*)

Le format de charge utile pour ce service de liaison est identique à celui du service de liaison étendu REC ACC spécifié au paragraphe 7.3.1.9 et DEVRA être traité comme décrit dans ce paragraphe. La version FC-4 va devenir obsolète avec [FCP-2]. Cependant, afin de prendre en charge les appareils mis en œuvre avec les révisions antérieures de FCP-2, une passerelle iFCP DOIT prendre en charge les deux versions.

7.4 Paramètres de service FLOGI pris en charge par une passerelle iFCP

L'ELS FLOGI est produit par un N_PORT qui souhaite accéder aux services de transport du tissu.

Le format de la demande FLOGI et des charges utiles FLOGI ACC est identique à celui de la demande PLOGI et des charges utiles ACC décrit au paragraphe 7.3.1.7.



```
+------+------------+------------+-----------+----------+
|18-21 |            Paramètres de service de classe 3   |
+------+------------+------------+-----------+----------+
|22-25 |            Paramètres de service de classe 4   |
+------+------------+------------+-----------+----------+
|26-29 |            Niveau de version de fabricant      |
+======+============+============+===========+==========+
```

Figure 25. Format de demande FLOGI et de charge utile ACC

Une description complète de chaque paramètre est donnée dans [FC-FS].

Le tableau suivant décrit les paramètres de service dépendants du protocole qui sont pris en charge par un acccès de tissu rattaché à une passerelle iFCP.

Les paramètres de service portés dans la charge utile d'une demande FLOGI de service de liaison étendu DOIVENT être réglés conformément au Tableau 9.

Paramètres de service	**Classe d'établissement de tissu**			
	1	**2**	**3**	**4**
Validité de classe	n	O	O	n
Options de service				
Mode intermixte	n	n	n	n
Demandes connectées en pile	n	n	n	n
Livraison séquencielle	n	O	O	n
Simplex dédié	n	n	n	n
Domiciliation	n	n	n	n
Classe 1 en mémoire tampon	n	n	n	n
Priorité	n	n	n	n
Contrôle de l'initiateur/receveur				
Synchronisation d'horloge à capacité ELS	n	n	n	n

Table 9. Réglage des paramètres de service FLOGI

Notes:
1) "n" indique un paramètre ou capacité qui n'est pas pris en charge par le protocole iFCP.
2) "O" indique un paraamètre applicable qui DOIT être pris en charge par une passerelle iFCP.

8. Détection d'erreur iFCP

8.1 Vue d'ensemble

Cette Section spécifie les dispositions pour la détection d'erreurs et la récupération en plus de celles de [FC-FS], qui continuent d'être disponibles dans l'environnement de réseau iFCP.

8.2 Prévention de trame périmée

La récupération à partir d'une condition d'erreur de protocole de canal fibre exige que les trames associées à un échange en échec ou interrompu s'écoulent du tissu avant que les ressources de l'échange puissent être réutilisées en toute sécurité.

Comme un tissu canal fibre peut ne pas préserver l'ordre des trames, il n'y a pas de façon déterministe de purger de telles trames. Le tissu garantit plutôt que la durée de vie des trames ne va pas excéder une limite spécifique (R_A_TOV).

R_A_TOV est défini dans [FC-FS] comme "le temps maximum de transit au sein d'un tissu pour garantir qu'une trame perdue ne va jamais sortir du tissu". Par exemple, une valeur de 2 x R_A_TOV est la durée minimum pendant laquelle le générateur d'une demande ELS ou une demande de service de liaison FC-4 doit attendre la réponse à cette demande. La valeur canal fibre par défaut pour R_A_TOV est 10 secondes.

Une passerelle iFCP DEVRA activement appliquer les limites de R_A_TOV comme décrit au paragraphe 8.2.1.

8.2.1 Application des limites R_A_TOV

La limite R_A_TOV de durée de vie des trames DEVRA être appliquée au moyen de l'horodatage dans l'en-tête d'encapsulation (voir au paragraphe 5.3.1) comme décrit dans ce paragraphe.

Le budget pour R_A_TOV DEVRAIT inclure des tolérances pour le délai de propagation à travers les régions passerelles des N_PORT d'envoi et de réception plus le délai de propagation à travers le réseau IP. Ce dernier composant est appelé IP_TOV dans la présente spécification.

IP_TOV devrait être réglé très en dessous de la valeur de R_A_TOV spécifiée pour le tissu iFCP et devrait être mémorisé dans le serveur iSNS. IP_TOV devrait être réglé à to 50 pour cent de R_A_TOV.

Les paragraphes qui suivent décrivent les exigences pour synchroniser les horaires de base des passerelles et les règles pour mesurer et appliquer les limites de délai de propagation.

Le protocole pour synchroniser une base horaire de passerelle est SNTP [RFC2030]. Afin d'assurer que toutes les passerelles sont alignées sur le même horaire, une passerelle DEVRAIT obtenir l'adresse d'un serveur horaire compatible avec SNTP via une interrogation iSNS. Si plusieurs adresses de serveur horaire sont retournées par l'interrogation, les serveurs doivent être synchrones et la passerelle peut utiliser tout serveur de la liste. Autrement, le serveur peut retourner une adresse de groupe de diffusion groupée à l'appui d'un fonctionnement en mode de diffusion à la cantonade *(Anycast)*. Une mise en œuvre de mode de diffusion à la cantonade est comme spécifié dans la [RFC2030], incluant les précautions définies dans le présent document. Le mode de diffusion groupée NE DEVRAIT PAS être utilisé.

Un serveur SNTP peut utiliser toute source de référence horaire spécifiée dans la [RFC2030]. La résolution de la référence horaire DOIT être de 125 millisecondes ou mieux.

La stabilité des bases horaires du serveur SNTP et de la passerelle devrait être de 100 millionièmes ou mieux.

Par rappport à sa base horaire, la passerelle est soit dans l'état synchronisé, soit dans l'état non synchronisé.

Quand elle est dans l'état synchronisé, la passerelle DEVRA :
a) régler le champ Horodatage pour chaque trame sortante en accord avec la base horaire interne de la passerelle ;
b) vérifier le champ Horodataage de chaque trame entrante, suivant la validation du CRC de l'en-tête d'encapsulation, comme décrit au paragraphe 5.3.4 ;
c) si la trame entrante a un horodatage de 0,0 et si aucune des trames de contrôle de la session n'exige un horodatage de 0,0 (voir la Section 6) la trame DEVRA être éliminée ;
d) si la trame entrante a un horodatage non zéro, la passerelle receveuse DEVRA calculer la valeur absolue de l'heure en vol et DEVRA la comparer à la valeur de IP_TOV spécifiée pour le tissu IP ;
e) si le résultat de l'étape (d) excède IP_TOV, la trame encapsulée devra être éliminée. Autrement, la trame devra être désencapsulée comme décrit au paragraphe 5.3.4.

Une passerelle DEVRA entrer dans l'état synchronisé à réception d'une réponse de succès à une interrogation SNTP.

Une passerelle devra entrer dans l'état non synchronisé :
a) à la mise sous tension et avant l'achèvement réussi d'une interrogation au SNTP, et
b) chaque fois que la passerelle perd le contact avec le serveur SNTP, de telle sorte que la base horaire de la passerelle ne puisse plus être en ligne avec celle du serveur SNTP. Le critère pour déterminer la perte de contact est spécifique de la mise en œuvre.

À la suite de la perte de contact, il est recommandé que la passerelle entre dans l'état non synchronisé lorsque la dérive de la base horaire estimée par rapport à la référence SNTP est supérieure à dix pour cent de la limite de IP_TOV. (En supposant que toutes les horloges ont une précision de 1/10000 et que IP_TOV égal 5 secondes, la durée maximum de perte de contact admissible serait d'environ 42 minutes.)

Par suite d'une transition de l'état synchronisé à l'état non synchronisé, une passerelle DOIT interrompre toutes les sessions iFCP comme décrit au paragraphe 5.2.3. Lorsque elle est dans l'état non synchronisé, une passerelle NE DEVRA PAS permittre la création de nouvelles sessions iFCP.

9. Services de tissu pris en charge par une mise en œuvre iFCP

Une mise en œuvre de passerelle iFCP DOIT prendre en charge les services de tissu suivants :

Valeur d'identifiant de N_PORT	Description	Paragraphe
0xFF-FF-FE	serveur F_PORT	9.1
0xFF-FF-FD	contrôleur de tissu	9.2
0xFF-FF-FC	serveur de répertoire/noms	9.3

De plus, une passerelle iFCP PEUT prendre en charge la fonction de serveur de diffusion FC décrite au paragraphe 9.4.

9.1 Serveur F_PORT

Le serveur F_PORT DEVRA prendre en charge l'ELS FLOGI, comme décrit au paragraphe 7.4, ainsi que les ELS suivants spécifiés dans [FC-FS] :
a) demandes de paramètres de service de tissu (FDISC).
b) demande d'état d'erreur de liaison (RLS, *Request Link Status*).
c) valeurs de temporisation de lecture de tissu (RTV, *Read fabric Timeout Value*).

9.2 Contrôleur de tissu

Le contrôleur de tissu DEVRA prendre en charge les ELS suivants comme spécifié dans [FC-FS] :
a) notification de changement d'état (SCN, *State Change Notification*).
b) notification de changement d'état enregistré (RSCN, *Registered State Change Notification*).
c) enregistrement de changement d'état (SCR, *State Change Registration*).

9.3 Serveur de noms/répertoire

Le serveur de répertoire/noms fournit un service d'enregistrement qui permet à un N_PORT d'enregistrer ou d'interroger la base de données pour avoir des informations sur d'autres N_PORT. Les services sont définis dans [FC-GS3]. Les interrogations sont produites comme transactions FC-4 en utilisant le protocole de transport de commandes FC-CT spécifié dans [FC-GS3].

Dans iFCP, chaque demande de serveur de noms DOIT être traduite en l'interrogation iSNS appropriée définie dans la [RFC4171]. La définition des objets serveurs de noms est spécifiée dans [FC-GS3].

Le serveur de noms DEVRA prendre en charge les opérations d'enregistrement et d'interrogation pour le sous type de répertoire 0x02 (serveur de noms) et 0x03 (serveur d'adresse IP) et PEUT prendre en charge les services spécifiques de FC-4 comme défini dans [FC-GS3].

9.4 Serveur de diffusion

Les trames de canal fibre sont diffusées à travers le tissu en les adressant au serveur de diffusion de canal fibre à l'adresse canal fibre bien connue 0xFF-FF-FF. Le serveur de diffusion duplique alors les trames et les livre à chaque N_PORT rattaché dans toutes les zones auxquelles appartient l'appareil générateur. Seul le service de classe 3 (datagrammes) est pris en charge.

Dans un système iFCP, la fonction de diffusion de canal fibre est émulée au moyen d'une architecture à deux niveaux comprenant les éléments suivants :
a) un serveur de diffusion local qui réside dans chaque passerelle iFCP. Le serveur local distribue le trafic de diffusion au sein de la région passerelle et transmet le trafic de diffusion sortant à un serveur global pour la distribution à travers tout le tissu iFCP.
b) un serveur global de diffusion qui redistribue le trafic de diffusion au serveur local dans chaque passerelle participante.
c) un domaine de découverte iSNS qui définit la portée sur laquelle chaque trafic de diffusion est propagé. Le domaine de découverte est rempli avec un serveur de diffusion global et l'ensemble de serveurs locaux qu'il prend en charge.

Les serveurs de diffusion locaux et globaux sont des appareils iFCP logiques qui communiquent en utilisant le protocole iFCP. Les serveurs ont une adresse réseau de N_PORT consistant en une adresse de portail iFCP et un identifiant de N_PORT réglé à l'adresse de canal fibre bien connue du serveur de diffusion FC (0xFF-FF-FF).

Comme noté ci-dessus, un N_PORT génère une diffusion en dirigeant le trafic de trames sur le serveur de diffusion de canal fibre. Le serveur local résidant sur la passerelle distribue une copie de la trame en local et transmet une copie au serveur global pour la redistribution aux serveurs locaux sur les autres passerelles. Le serveur global NE DOIT PAS faire écho d'une trame en diffusion au serveur local d'origine.

9.4.1 Établissement de configuration de diffusion

La configuration de diffusion est gérée avec les facilités fournies par le serveur iSNS par les moyens suivants :

a) un domaine de découverte iSNS est créé et nourri avec l'adresse réseau de N_PORT du serveur global de diffusion. Le serveur global est identifié comme tel en réglant l'attribut d'entité approprié de N_PORT ;
b) en utilisant l'interface de gestion, chaque serveur de diffusion est préréglé avec l'identité du domaine de diffusion.

Durant la mise sous tension, chaque passerelle DEVRA invoquer le service iSNS pour s'enregistrer auprès de son serveur de diffusion local dans le domaine de découverte de diffusion. Après l'enregistrement, le serveur local DEVRA attendre que le serveur de diffusion global établisse une session iFCP.

Le serveur global DEVRA s'enregistrer auprès du serveur iSNS comme suit :

a) le serveur DEVRA interroger le serveur de noms iSNS par attribut pour obtenir le nom d'accès mondial du N_PORT pré configuré pour fournir les services de diffusion globaux.
b) Si le nom d'accès mondial obtenu ci-dessus ne correspond pas à celui du serveur qui produit l'interrogation, le N_PORT NE DEVRA PAS effectuer de fonctions de diffusion globale pour les N_PORT dans ce domaine de découverte.
c) Autrement, le N_PORT serveur global DEVRA s'enregistrer auprès du domaine de découverte et interroger le serveur iSNS pour identifier tous les serveurs locaux actuellement enregistrés.
d) Le serveur de diffusion global DEVRA initier une session iFCP avec chaque serveur de diffusion local dans le domaine. Quand un nouveau serveur local s'enregistre, le serveur global DEVRA recevoir une notification de changement d'état et y répondre en initiant une session iFCP avec le serveur qui vient d'être ajouté. La passerelle DEVRA obtenir ces notifications en utilisant les dispositions de iSNS pour la livraison sans perte.

À réception de la demande CBIND pour initier la session iFCP, le serveur local DEVRA enregistrer le nom d'accès mondial et l'adresse réseau de N_PORT du serveur global.

9.4.2 Gestion de session de diffusion

Après l'établissement de la session initiale de diffusion, le serveur local ou global de diffusion PEUT choisir de gérer la session d'une des façons suivantes, selon les exigences de ressources et le niveau anticipé de trafic de diffusion :

a) Un serveur PEUT garder la session ouverte en continu. Comme les sessions de diffusion sont souvent en sommeil pour de longues périodes, le serveur DEVRAIT surveiller la connexité de la session comme décrit au paragraphe 5.2.2.4.
b) Un serveur PEUT ouvrir la session de diffusion à la demande seulement quand du trafic va être envoyé. Si la session est rouverte par le serveur global, le serveur local DEVRA remplacer l'adresse réseau précédemment enregistrée du serveur de diffusion global.

9.4.3 Serveur global de diffusion en attente

Une mise en œuvre peut désigner un serveur local pour assurer les tâches d'un serveur de diffusion en cas de défaillance. Le serveur local peut utiliser le message LTEST pour déterminer si le serveur global fonctionne et peut prendre les commandes si il ne fonctionne pas.

Quand il prend le contrôle, le serveur en attente doit s'enregistrer auprès du serveur iSNS comme serveur global de diffusion à la place du seveur défaillant et doit s'installer dans le domaine de découverte de diffusion comme spécifié dans les étapes c) et d) du paragraphe 9.4.1.

10. Sécurité de iFCP

10.1 Vue d'ensemble

iFCP s'appuie sur la suite de protocoles IPsec pour fournir des services de confidentialité des données et d'authentification, et il s'appuie sur IKE comme protocole de gestion de clés. Le paragraphe 10.2 décrit les exigences de sécurité provenant de l'environnement de fonctionnement de iFCP, et le paragraphe 10.3 décrit les choix de conception qui en résultent, leurs niveaux d'exigence, et comment ils s'appliquent au protocole iFCP.

Des considérations détaillées sur l'utilisation de IPsec et IKE avec le protocole iFCP se trouvent dans la [RFC3723].

10.2 Menaces et portée de la sécurité d'iFCP

10.2.1 Contexte

iFCP est un protocole conçu pour être utilisé par des appareils passerelles déployés dans des centres de données d'entreprises. De tels environnements ont normalement des passerelles de sécurité conçues pour fournir la sécurité du réseau par l'isolation des réseaux publics. De plus, les données iFCP peuvent avoir à traverser des passerelles de sécurité afin de prendre en charge la connexité de réseau à zone de mémorisation (SAN, *Storage Area Network*) à SAN à travers les réseaux publics.

10.2.2 Menaces pour la sécurité

Les passerelles communicantes iFCP peuvent être l'objet d'attaques, incluant des tentatives d'un adversaire pour :

a) acquérir des données et identités confidentielles en espionnant les paquets de données,
b) modifier les paquets contenant des messages de données et de contrôle iFCP,
c) injecter de nouveaux paquets dans la session iFCP,
d) capturer la connexion TCP qui porte la session iFCP,
e) lancer des attaques de déni de service contre la passerelle iFCP,
f) perturber le processus de négociation de la sécurité,
g) se faire passer pour la passerelle de sécurité légitime, ou
h) compromettre la communication avec le serveur iSNS.

Il est impératif de déjouer ces attaques, étant donné qu'une passerelle iFCP est la dernière ligne de défense pour tout un ilôt de canal fibre, qui peut inclure plusieurs hôtes et commutateurs canal fibre. Pour ce faire, la passerelle iFCP doit mettre en œuvre et peut utiliser la confidentialité, l'authentification de l'origine des données, la protection de l'intégrité, et contre la répétition sur la base du datagramme. La passerelle iFCP doit mettre en œuvre et peut utiliser l'authentification bidirectionnelle des points d'extrémité de communication. Finalement, elle doit mettre en œuvre et peut utiliser une approche adaptable de la gestion de clés.

10.2.3 Interopérabilité avec les passerelles de sécurité

Les réseaux de centre de données d'entreprise sont considérés comme des facilités d'une mission critique qui doivent être isolés et protégés de toutes les menaces possibles contre leur sécurité. De tels réseaux sont généralement protégés par des passerelles de sécurité, qui, au minimum, fournissent un bouclier contre les attaques de déni de service. L'architecture de sécurité de iFCP est capable de démultiplier les services de protection de l'infrastructure de sécurité existante, incluant la protection d'un pare-feu, des services de NAT et de NAPT, et des services de VPN IPsec disponibles sur les passerelles de sécurité existantes. Les considérations concernant l'intervention de boîtiers NAT et NAPT sur les chemins de iFCP-iSNS se trouvent dans la [RFC4171].

10.2.4 Authentification

iFCP est un protocole d'homologue à homologue. Les sessions iFCP peuvent être initiées par l'une ou l'autre des passerelles homologues ou par les deux. Par conséquent, l'authentification bidirectionnelle des passerelles homologues doit être fournie conformément aux niveaux d'exigence spécifiés au paragraphe 10.3.1.

Les identités de N_PORT utilisées dans le processus d'établissement d'accès (PLOGI) devront être considérées comme authentifiées si la demande PLOGI est reçue de la passerelle distante sur une connexion sûre, protégée par IPsec. Il n'est pas exigé que les identités utilisées dans l'authentification restent confidentielles.

10.2.5 Confidentialité

Le trafic iFCP peut traverser des réseaux publics non sûrs, et donc les mises en œuvre doivent avoir des capacités de chiffrement par paquet pour fournir la confidentialité conformément aux exigences du paragraphe 10.3.1.

10.2.6 Changement de clés

Du fait des hauts débits de transfert de données et des quantités de données impliquées, une mise en œuvre de iFCP doit supporter la capacité de changer les clés de chaque association de sécurité de phase 2 aux intervalles de temps dictés par l'espace de numéros de séquence disponible à un certain débit de liaison. Dans le scénario de changement de clés décrit dans la [RFC3723], par exemple, les événements de changement de clés se produisent toutes les 27,5 secondes à 10 Gbit/s.

La passerelle iFCP doit fournir la capacité de secret vers l'avant dans le processus de changement de clé.

10.2.7 Autorisation

Les propriétés de contrôle d'accès de base découlent de l'exigence que les deux passerelles iFCP communicantes soient connues d'un ou plusieurs serveurs iSNS avant qu'elles s'engagent dans les échanges iFCP. L'utilisation facultative des domaines de découverte [RFC4171], des charges utiles d'identité (par exemple, les ID_FQDN), et l'authentification fondée sur le certificat (par exemple, avec des certificats X509 v3) permet des schémas d'autorisation d'une complexité croissante. La définition de tels schémas (par exemple, contrôle d'accès fondé sur le rôle) sort du domaine d'application de cette spécification.

10.2.8 Contrôle de politique

Cette spécification permet que tous les mécanismes de sécurité dans une passerelle iFCP soient administrativement désactivés. Les politiques de sécurité DOIVENT avoir, au plus, la résolution de portail iFCP. Les administrateurs peuvent prendre le contrôle des politiques de sécurité par une interaction adéquatement sécurisée avec une interface de gestion ou avec iSNS.

10.2.9 Rôle iSNS

iSNS [RFC4171] est un invariant dans tous les déploiements de iFCP. Les passerelles iFCP DOIVENT utiliser iSNS pour les services de découverte et PEUVENT utiliser les politiques de sécurité configurées dans la base de données iSNS comme base de la négociation d'algorithme dans IKE. La spécification iSNS définit des mécanismes pour sécuriser la communication entre une passerelle iFCP et un ou des serveurs iSNS. De plus, la spécification indique comment les éléments de politique de sécurité concernant les sessions iFCP individuelles peuvent être restituées des serveurs iSNS.

10.3 Conception de la sécurité iFCP

10.3.1 Technologies disponibles

La technologie applicable à partir de IPsec et IKE est définie dans la suite de spécifications suivante :
[RFC2401] Architecture de sécurité pour le protocole Internet
[RFC2402] En-tête d'authentification IP
[RFC2404] Utilisation de HMAC-SHA-1-96 au sein de ESP et AH
[RFC2405] Algorithme de chiffrement ESP DES-CBC avec valeur d'initialisation explicite
[RFC2406] Encapsulation dans IP de charge utile de sécurité
[RFC2407] Domaine d'interprétation de la sécurité Internet IP pour ISAKMP
[RFC2408] Association de sécurité Internet et protocole de gestion de clé (ISAKMP)
[RFC2409] Échange de clé Internet (IKE)
[RFC2410] Algorithme de chiffrement NULL utilisé avec IPsec
[RFC2451] Algorithmes de chiffrement ESP en mode CBC
[RFC2709] Modèle de sécurité avec IPsec en mode tunnel pour les domaines à NAT

La mise en œuvre de IPsec et IKE est exigée conformément aux lignes directrices suivantes.

La prise en charge de l'encapsulation de la charge utile de sécurité (ESP) [RFC2406] est de mise en œuvre OBLIGATOIRE. Quand ESP est utilisé, l'authentification de l'origine des données, la protection de l'intégrité et la protection contre la répétition paquet par paquet DOIVENT être utilisées.

Pour l'authentification de l'origine des données et la protection de l'intégrité avec ESP, HMAC avec SHA1 [RFC2404] DOIT être mis en œuvre, et la norme de chiffrement évoluée [AES] en mode MAC CBC avec chaînage de bloc de chiffrement étendu DEVRAIT être mis en œuvre conformément à la [RFC3566].

Pour la confidentialité avec ESP, 3DES en mode CBC [RFC2451] DOIT être mis en œuvre, et le chiffrement AES en mode compteur [RFC3686] DEVRAIT être mis en œuvre. Le chiffrement NULL DOIT être aussi pris en charge, comme défini dans la [RFC2410]. DES en mode CBC NE DEVRAIT PAS être utilisé à cause de ses faiblesses inhérentes. Comme il est connu qu'il peut être cassé avec de modestes ressources de calcul, il est inapproprié dans tout scénario de déploiement de iFCP.

Une mise en œuvre conforme du protocole iFCP DOIT mettre en œuvre IPsec ESP [RFC2406] en mode tunnel [RFC2401] et PEUT mettre en œuvre IPsec ESP en mode transport.

En ce qui concerne la gestion de clés, les mises en œuvre de iFCP DOIVENT prendre en charge IKE [RFC2409] pour l'authentification bidirectionnelle des homologues, la négociation des associations de sécurité, et la gestion de clés, en utilisant le DOI IPsec. Il n'est pas exigé que les identités utilisées dans l'authentification restent confidentielles. Le changement de clés manuel NE DOIT PAS être utilisé parce qu'il ne fournit pas la prise en charge nécessaire. Conformément à la [RFC2409], l'authentification de la clé secrète prépartagée est de mise en œuvre OBLIGATOIRE, tandis que l'authentification de l'homologue sur la base du certificat en utilisant des signatures numériques PEUT être mise en œuvre (voir au paragraphe 10.3.3 concernant l'usage des certificats). La [RFC2409] définit les niveaux d'exigence suivants pour les modes d'IKE :
Le mode principal de phase 1 DOIT être mis en œuvre.
Le mode agressif de phase 1 DEVRAIT être mis en œuvre.
Le mode rapide de phase 2 DOIT être mis en œuvre.
Le mode rapide de phase 2 avec charge utile d'échange de clé DOIT être mis en œuvre.

Avec iFCP, le mode principal de phase 1 NE DEVRAIT PAS être utilisé en conjonction avec des clés prépartagées, à cause de la vulnérabilité aux attaques par interposition quand on utilise des clés prépartagées de groupe. Dans ce scénario, le mode agressif DEVRAIT plutôt être utilisé. L'authentification de l'homologue en utilisant les méthodes de chiffrement à clé publique décrites dans la [RFC2409] NE DEVRAIT PAS être utilisée.

Le DOI [RFC2407] assure plusieurs types de charges utiles d'identification.

Lorsque ils sont utilisés pour iFCP, les échanges IKE phase 1 DOIVENT explicitement porter les champs de charge utile d'identification (IDii et IDir). Les mises en œuvre conformes de iFCP DOIVENT utiliser les valeurs de type d'identification ID_IPV4_ADDR, ID_IPV6_ADDR (si la pile de protocole accepte IPv6), ou ID_FQDN. Les valeurs de type d'identification ID_USER_FQDN, Sous réseau IP, Gamme d'adresse IP, ID_DER_ASN1_DN, ID_DER_ASN1_GN NE DEVRAIENT PAS être utilisées. Les valeurs de type d'identification ID_KEY_ID NE DOIVENT PAS être utilisées. Comme décrit dans la [RFC2407], les champs Accès et Protocole dans la charge utile d'identification DOIVENT être réglés à zéro ou à l'accès UDP 500.

Lorsque utilisé pour iFCP, les échanges IKE phase 2 DOIVENT explicitement porter les champs de charge utile d'identification (IDci et IDcr). Les mises en œuvre conformes de iFCP DOIVENT utiliser les valeurs de type d'identification de ID_IPV4_ADDR ou de ID_IPV6_ADDR (selon la version de IP prise en charge). Les autres valeurs de type d'identification NE DOIVENT PAS être utilisées. Comme décrit au paragraphe 5.2.2, la passerelle qui crée la session iFCP doit interroger le serveur iSNS pour déterminer l'accès approprié sur lequel initier la connexion TCP associée. Si l'échange IKE phase 2 est réussi, le répondant à IKE applique les sélecteurs négociés sur les SA IPsec. Toute création ultérieure de session iFCP exigera que l'homologue iFCP interroge son serveur iSNS pour le contrôle d'accès (en accord avec les exigences de création de session spécifiées au paragraphe 5.2.2.1).

10.3.2 Utilisation de IKE et IPsec

Un portail iFCP conforme est capable d'établir une ou plusieurs associations de sécurité (SA, *Security Association*) IKE phase-1 avec un portail iFCP homologue. Une SA phase 1 peut être établie quand un portail iFCP est initialisé ou peut être différée jusqu'à ce que la première connexion TCP avec des exigences de sécurité soit établie.

Une SA IKE phase 2 protège une ou plusieurs connexions TCP au sein du même portail iFCP. Plus précisément, la réussite de l'établissement d'une SA IKE phase 2 résulte en la création de deux SA IPsec unidirectionnelles pleinement qualifiées par le triplet <SPI, adresse IP de destination, ESP>.

Ces SA protègent le processus d'établissement des connexions TCP sous-jacentes et de tout leur trafic TCP ultérieur. Le nombre de connexions TCP dans une SA IPsec, ainsi que le nombre de SA, est en pratique commandé par les considérations de politique de sécurité (c'est-à-dire que les services de sécurité sont définis à la granularité d'une seule SA IPsec) les considérations de qualité de service (par exemple, plusieurs classes de QS au sein de la même SA IPsec augmente les risques de déclassement de paquets, sortant éventuellement de la fenêtre de répétition) et par des considérations de compartementalisation des défaillances. Chaque connexion TCP protégée par une SA IPsec est soit dans l'état non lié, soit liée à une session iFCP spécifique.

En résumé, à tout moment :
- il existe de 0 à M SA IKE phase 1 entre les portails iFCP homologues,
- chaque SA IKE phase 1 a 0 à N SA IKE phase 2, et
- chaque SA IKE phase 2 protège 0 à Z connexions TCP.

La création d'une SA IKE phase 2 peut être déclenchée par une règle de politique fournie par l'intermédiaure d'une interface de gestion ou par des propriétés de portail iFCP enregistrées auprès du serveur iSNS. De même, l'utilisation d'une charge

utile d'échange de clé en mode rapide pour le secret parfait vers l'avant peut être indiquée au moyen d'une interface de gestion ou par une règle de politique de portail iFCP enregistrée auprès du serveur iSNS.

Si une mise en œuvre de iFCP utilise des connexions TCP non liées, et si ces connexions appartiennent à un portail iFCP qui a des exigences de sécurité, les connexions non liées DOIVENT alors être protégées par une SA à tout moment tout comme des connexions liées.

À réception d'un message de suppression IKE phase 2, il n'est pas exigé de terminer les connexions TCP protégées ou de supprimer la SA IKE phase 1 associée. Comme une SA IKE phase 2 peut être associée à plusieurs connexions TCP, terminer ces connexions pourrait en fait être inapproprié et à contre temps.

Pour minimiser le nombre de SA actives de phase 2, IKE phase 2 supprime les messages qui peuvent être envoyés pour les SA de phase 2 dont les connexions TCP n'ont pas traité de trafic de données depuis un certain temps. Pour minimiser l'utilisation des ressources de SA pendant que les connexions TCP associées sont inactives, la création d'une nouvelle SA devrait être différée jusqu'à ce que de nouvelles données soient à envoyer sur ces connexions.

10.3.3 Authentification fondée sur la signature et le certificat

Les mises en œuvre conformes de iFCP PEUVENT prendre en charge l'authentification de l'homologue via des signatures et certificats numériques. Lorsque l'authentification par certificats est choisie au sein de IKE, chaque passerelle iFCP a besoin des accréditifs de certificat de chaque passerelle iFCP d'homologue afin d'établir une association de sécurité avec cet homologue.

Les accréditifs de certificat utilisés par les passerelles iFCP DOIVENT être ceux de la machine. Les accréditifs de certificat PEUVENT être liés à l'interface (adresse IP ou FQDN) de la passerelle iFCP utilisée pour la session iFCP, ou au WWN de tissu de la passerelle iFCP elle-même. Comme la valeur d'un certificat de machine est inversement proportionnelle à la facilité avec laquelle un attaquant peut en obtenir un sous de faux prétextes, il est conseillé que le processus d'enregistrement des certificats de machine soit strictement contrôlé. Par exemple, seuls les administrateurs peuvent avoir la capacité d'enregistrer une machine avec un certificat de machine. Les certificats d'utilisateur NE DEVRAIENT PAS être utilisés par les passerelles iFCP pour l'établissement de SA qui protègent des sessions iFCP.

Si la passerelle n'a pas les accréditifs de certificat de la passerelle iFCP homologue, elle peut alors les obtenir :
a) en utilisant le protocole iSNS pour interroger le ou les certificats de la passerelle homologue mémorisés dans un serveur iSNS de confiance, ou
b) en utilisant la charge utile de demande de certificat (CRP, *Certificate Request Payload*) de ISAKMP [RFC2408] pour demander le ou les certificats directement à la passerelle iFCP homologue.

Quand les chaînes de certificats sont assez longues, les échanges IKE qui utilisent UDP comme transport sous-jacent peuvent donner des fragments IP, qui sont connus pour mal fonctionner sur certains routeurs, pare-feu, et boîtiers NA(P)T intermédiaires. Par suite, les points d'extrémité peuvent être dans l'incapacité d'établir une association de sécurité IPsec.

À cause de ces problèmes de fragmentation, IKE est plus approprié pour un usage intra-domaine. Des solutions connues au problème de fragmentation incluent d'envoyer le certificat de machine d'entrée d'extrémité plutôt que toute la chaîne, réduisant la taille de la chaîne de certificats, et d'utiliser les mises en œuvre de IKE sur un protocole de transport fiable (par exemple, TCP) assisté par la découverte de la MTU de chemin et le code contre les trous noirs conformément à la [RFC2923], ou d'installer des composants réseau qui puissent traiter convenablement les fragments.

Les négociateurs de IKE DEVRAIENT vérifier la liste de révocation de certificat (CRL, *Certificate Revocation List*) [RFC2408] pertinente avant d'accepter un certificat à utiliser dans les procédures d'authentification de IKE.

10.4 iSNS et la sécurité iFCP

Les mises en œuvre de iFCP DOIVENT utiliser iSNS pour les services de découverte et de gestion. Par conséquent, la sécurité du protocole iSNS a un impact sur la sécurité des passerelles iFCP. Pour une discussion des menaces potentielles sur les passerelles iFCP par l'utilisation de iSNS, voir la [RFC4171].

Pour assurer la sécurité des passerelles iFCP dans l'utilisation du protocole iSNS pour les services de découverte et de gestion, le protocole IPsec ESP en mode tunnel DOIT être pris en charge par les passerelles iFCP. Une discussion plus approfondie des exigences de mise en œuvre de la sécurité de iSNS se trouve dans la [RFC4171]. Noter que les exigences de sécutité de iSNS correspondent à celles pour iFCP décrites au paragraphe 10.3.

10.5 Utilisation de iSNS pour distribuer les politiques de sécurité

Une fois que la communication entre les passerelles iFCP et le serveur iSNS a été sécurisée par l'utilisation de IPsec, les passerelles iFCP ont la capacité de découvrir les réglages de sécurité qu'elles ont besoin d'utiliser (ou pas) pour protéger le trafic iFCP. Cela procure un avantage potentiel d'adaptabilité sur la configuration appareil par appareil des politiques individuelles de sécurité pour chaque passerelle iFCP. Cela procure aussi un moyen efficace pour que chaque passerelle iFCP découvre l'utilisation ou la non utilisation de capacités spécifiques de sécurité par les passerelles homologues.

Une discussion plus approfondie sur l'utilisation de iSNS pour distribuer les politiques de sécurité se trouve dans la [RFC4171].

10.6 Politique minimale de sécurité pour une passerelle iFCP

Une mise en œuvre de iFCP peut être capable de désactiver administrativement les mécanismes de sécurité pour un portail iFCP par une interface de gestion ou par des éléments de politique de sécurité réglés dans le serveur iSNS. Par conséquent, les associations de sécurité IKE ou IPsec ne seront établies pour aucune session iFCP qui traverse le portail.

Pour la plupart des réseaux IP, il est inapproprié de supposer une sécurité physique, une sécurité administrative, et une configuration correcte du réseau et de tous les nœuds rattachés (un réseau physiquement isolé dans un laboratoire d'essais peut être une exception). Donc, l'authentification DEVRAIT être utilisée afin de fournir une assurance minimale que les connexions ont été ouvertes initialement avec la contrepartie prévue. La politique de sécurité iFCP minimale déclare seulement qu'une passerelle iFCP DEVRAIT authentifier ses serveurs iSNS comme décrit dans la [RFC4171].

11. Considérations relatives à la qualité de service

11.1 Exigences minimales

Les mises en œuvre de protocole iFCP conformes DEVRONT communiquer correctement de passerelle à passerelle, même à travers une ou plusieurs régions IP intermédiaires "au mieux". Le rythme auquel de telles communications de passerelle à passerelle sont effectuées va cependant largement dépendre du BER, de la perte de paquets, de la latence, et de la gigue subies à travers ces régions IP "au mieux". Plus ces paramètres sont élevés, plus augmentera la différence mesurée entre des comportements iFCP observés et les comportements iFCP de base (c'est-à-dire, comme produits par deux passerelles iFCP connectées directement l'une à l'autre).

11.2 Forte assurance

On s'attend à ce que de nombreux déploiements de iFCP bénéficient d'un haut degré d'assurance concernant le comportement des régions IP intermédiaires, avec pour résultat une forte assurance sur le chemin global de bout en bout, comme elle est directement expérimentée par les applications de canal fibre. Une telle assurance sur les comportements IP découle de ce que les régions IP intermédiaires prennent en charge les techniques standard de qualité de service (QS) qui sont pleinement complémentaires de iFCP, telles que :

a) l'évitement d'encombrement par surprovisionnement du réseau,
b) la QS des services intégrés [RFC1633],
c) la QS des services différenciés [RFC2475], et
d) la commutation d'étiquettes multi protocoles [RFC3031].

On peut charger une classe d'équivalence de transmission (FEC, *forwarding equivalence class*) MPLS avec une signification de classe de QS en plus d'autres considérations telles que la protection et la diversité de chemins. La complémentarité et la compatibilité de MPLS avec les services différenciés est explorée dans la [RFC3270], dans laquelle les bits de PHB sont copié en bits EXP de l'en-tête d'ajustement de MPLS.

Dans la définition la plus générale, deux passerelles iFCP sont séparées par une ou plusieurs régions IP gérées de façon plus indépendante qui mettent en œuvre certaines des solutions de QS mentionnées ci-dessus. Une région IP à capacité de QS prend en charge la négociation et l'établissement d'un contrat de service qui spécifie les services de transmission à travers la région. Un tel contrat et ses règles de négociation sortent du domaine d'application du présent document. Dans le cas de régions IP avec la QS de DiffServ, le lecteur devrait se reporter aux spécifications de niveau de service (SLS) et aux spécifications de conditionnement de service (TCS) (comme définies dans la [RFC3260]). Les autres aspects d'un contrat de service sont supposés être non techniques et échappent donc aux compétence de l'IETF.

Parce que les classes 2 et 3 de canal fibre ne prenne pas actuellement en charge des fractions de garantie de bande passante, et parce que iFCP s'est engagé à prendre en charge la sémantique de canal fibre, il est impossible à une passerelle iFCP de

déduire des exigences de bande passante indépendamment de l'écoulement du trafic de canal fibre. Les exigences sur la bande passante ou sur les autres paramètres de réseau doivent plutôt être réglées administrativement dans une passerelle iFCP, ou dans l'entité qui va réellement négocier le service de transmission au nom de la passerelle. Selon les techniques de qualité de service disponibles, la stipulation d'un service de transmission peut exiger une interaction avec les fonctions traditionnelles du réseau, comme le contrôle d'admission et le courtage de bande passante (via RSVP ou d'autres protocoles de signalisation qu'une région IP peut accepter).

L'administrateur d'une passerelle iFCP peut négocier un service de transmission avec une ou des régions IP pour une, plusieurs, ou toutes les sessions TCP d'une passerelle iFCP utilisées par une passerelle iFCP. Autrement, cette responsabilité peut être déléguée à un nœud en aval. Comme une connexion TCP est dédiée à chaque session iFCP, le trafic dans un N_PORT individuel pour une session de N_PORT peut aussi bien être isolée par un équipement de réseau sans capacité iFCP.

Pour rendre possible la meilleure émulation de canal fibre sur IP, on prévoit que les services de transmission normaux vont spécifier une quantité fixe de bande passante, des pertes nulles, et à un moindre degré de pertinence, une faible latence et une faible gigue. Par exemple, une région IP qui utilise la QS DiffServ peut prendre en charge des SLS de cette nature en appliquant des DSCP EF au trafic iFCP.

12. Considérations relatives à l'IANA

L'accès alloué par l'IANA pour le trafic iFCP est 3420.

Un portail iFCP peut initier une connexion en utilisant tout numéro d'accès TCP cohérent avec sa mise en œuvre de la pile de protocoles TCP/IP, pourvu que chaque numéro d'accès soit unique. Pour empêcher la réception de données périmées associées à une connexion précédente utilisant un certain numéro d'accès, les dispositions de la [RFC1323], Appendice B, DEVRAIENT être respectées.

13. Références normatives

[FC-FS] dpANS INCITS.XXX-200X, "Fibre Channel Framing and Signaling (FC-FS), Rev 1.70, INCITS Project 1331D, février 2002

[FC-GS3] dpANS X3.XXX-200X, "Fibre Channel Generic Services -3 (FC- GS3)", revision 7.01, INCITS Project 1356-D, novembre 2000

[FC-SW2] dpANS X3.XXX-2000X, "Fibre Channel Switch Fabric -2 (FC- SW2)", revision 5.2, INCITS Project 1305-D, mai 2001

[FCP-2] dpANS T10, "Fibre Channel Protocol for SCSI, Second Version", revision 8, INCITS Project 1144D, septembre 2002

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2404] C. Madson, R. Glenn, "Utilisation de HMAC-SHA-1-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obs., voir* RFC4303)

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obs., voir* 4306)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2410] R. Glenn, S. Kent, "L'algorithme de chiffrement NULL et son utilisation avec IPsec", novembre 1998. *(P.S.)*

[RFC2451] R. Pereira, R. Adams, "Algorithmes de chiffrement ESP en mode CBC", novembre 1998. *(P.S.)*

[RFC3566] S. Frankel, H. Herbert, "L'algorithme AES-XCBC-MAC-96 et son utilisation avec IPsec", septembre 2003. *(P.S.)*

[RFC3643] R. Weber et autres, "Encapsulation de trame sur canal Fibre (FC)", décembre 2003. *(P.S.)*

[RFC3686] R. Housley, "Utilisation du mode Compteur de la norme de chiffrement évolué (AES) avec l'encapsulation de la charge utile de sécurité (ESP) dans IPsec", janvier 2004. *(P.S.)*

[RFC3723] B. Aboba et autres, "Protocoles de sécurisation de mémorisation de blocs sur IP", avril 2004. *(P.S.)*

[RFC4171] J. Tseng et autres, "Service de noms de mémorisation sur Internet (iSNS)", septembre 2005. *(P.S.)*

14. Références pour information

[AES] FIPS Publication XXX, "Advanced Encryption Standard (AES)", Draft, 2001, disponible sur http://csrc.nist.gov/publications/drafts/dfips-AES.pdf

[FC-AL2] dpANS X3.XXX-199X, "Fibre Channel Arbitrated Loop (FC-AL-2)", revision 7.0, NCITS Project 1133D, avril 1999

[FC-FLA] TR-20-199X, "Fibre Channel Fabric Loop Attachment (FC- FLA)", revision 2.7, NCITS Project 1235-D, août 1997

[FC-VI] ANSI/INCITS 357:2002, "Fibre Channel Virtual Interface Architecture Mapping Protocol (FC-VI)", NCITS Project 1332-D, juillet 2000.

[KEMALP] Kembel, R., "The Fibre Channel Consultant, Arbitrated Loop", Northwest Learning Associates, 2000, ISBN 0-931836-84-0

[KEMCMP] Kembel, R., "Fibre Channel, A Comprehensive Introduction", Northwest Learning Associates Inc., 2000, ISBN 0-931836-84-0

[RFC0896] J. Nagle, "Contrôle de l'encombrement dans l'inter-réseau IP/TCP", janvier 1984. *(Historique)*

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, octobre 1989. *(MàJ par* RFC6633, 8029)

[RFC1323] V. Jacobson, R. Braden et D. Borman, "Extensions TCP pour de bonnes performances", mai 1992.

[RFC1633] R. Braden, D. Clark et S. Shenker, "Intégration de services dans l'architecture l'Internet : généralités", juin 1994. *(Info.)*

[RFC2030] D. Mills, "Protocole simple de l'heure du réseau (SNTP) version 4 pour IPv4, IPv6 et OSI", octobre 1996. *(Rendue obsolète par la* RFC 4330)

[RFC2405] C. Madson et N. Doraswamy, "Algorithme de chiffrement ESP DES-CBC avec IV explicite", novembre 1998. *(P.S.)*

[RFC2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang et W. Weiss, "Architecture pour services différenciés", décembre 1998. *(MàJ par* RFC3260)

[RFC2625] M. Rajagopal, R. Bhagwat, W. Rickard, "IP et ARP sur canal en fibre", juin 1999. (*Obsolète, voir* RFC4338) *(P.S.)*

[RFC2709] P. Srisuresh, "Modèle de sécurité avec IPsec en mode tunnel pour les domaines à NAT", octobre 1999. *(Information)*

[RFC2923] K. Lahey, "Problèmes de TCP avec la découverte de MTU de chemin", septembre 2000. *(Information)*

[RFC3031] E. Rosen, A. Viswanathan, R. Callon, "Architecture de commutation d'étiquettes multi protocoles", janvier 2001. *(P.S.)* (*MàJ par la* RFC6790)

[RFC3260] D. Grossman, "Nouvelle terminologie et précisions pour Diffserv", avril 2002. *(Information)*

[RFC3270] F. Le Faucheur et autres, "Prise en charge des services différenciés par la commutation d'étiquettes multi-protocoles (MPLS)", mai 2002. *(P.S.)*

Appendice A. Prise en charge par iFCP des services de liaison de canal fibre

Pour les besoins de référence, le présent appendice énumère tous les services de liaison de canal fibre et la manière dont chacun doit être traité par une mise en œuvre de iFCP. Les politiques de traitement iFCP sont définies à la Section 7.

Dans les paragraphes qui suivent, le nom d'un service de liaison spécifique d'un protocole FC-4 particulier est préfixé d'un mnémonique qui identifie le protocole.

A.1 Services de liaison de base

Le tableau suivant montre les services de liaison de base :

Nom	Description	Politique iFCP
ABTS	Interruption de séquence	Transparent
BA_ACC	Acceptation de base	Transparent
BA_RJT	Rejet de base	Transparent
NOP	Non fonctionnement	Transparent
PRMT	Préempté	Rejeté (s'applique seulement à la classe 1)
RMC	Supprimer la connexion	Rejeté (s'applique seulement à la classe 1)

A.2 Services de liaison à passer

Comme spécifié à la Section 7, les demandes de service de liaison du Tableau 10 et les trames de réponse ACC associées DOIVENT être passées au N_PORT receveur sans altérer la charge utile.

Nom	Description
ADVC *(Advise Credit)*	crédit conseillé
CSR *(Clock Synchronization Request)*	demande de synchronisation d'horloge
CSU *(Clock Synchronization Update)*	mise à jour de synchronisation d'horloge
ECHO *(Echo)*	écho
ESTC *(Estimate Credit)*	crédit estimé
ESTS *(Establish Streaming)*	écoulement établi
FACT *(Fabric Activate Alias_ID)*	identifiant d'alias activé par le tissu
FAN *(Fabric Address Notification)*	notification d'adresse de tissu
FCP_RJT *(FCP FC-4 Link Service Reject)*	rejet de service de liaison FC-4 FCP
FCP SRR *(FCP Sequence Retransmission Request)*	demande de retransmission de séquence FCP
FDACT *(Fabric Deactivate Alias_ID)*	identifiant d'alias désactivé par le tissu
FDISC *(Discover F_Port Service Parameters)*	découverte des paramètres de service de F_PORT
FLOGI *(F_Port Login)*	établissement de F_PORT
GAID *(Get Alias_ID)*	obtenir un identifiant d'alias
LCLM *(Login Control List Management)*	gestion de liste de contrôle d'établissement
LINIT *(Loop Initialize)*	initialisation de boucle
LIRR *(Link Incident Record Registration)*	enregistrement d'incident de liaison
LPC *(Loop Port Control)*	contrôle d'accès de boucle

LS_RJT *(Link Service Reject)*	rejet de service de liaison
LSTS *(Loop Status)*	état de boucle
NACT *(N_Port Activate Alias_ID)*	activation d'identifiant d'alias par le N_PORT
NDACT *(N_Port Deactivate Alias_ID)*	désactivation d'identifiant d'alias par le N_PORT
PDISC *(Discover N_Port Service Parameters)*	découverte des paramètres de service du N_PORT
PRLI *(Process Login)*	traitement de l'établissement
PRLO *(Process Logout)*	traitement du désétablissement
QoSR *(Quality of Service Request)*	demande de qualité de service
RCS *(Read Connection Status)*	état de connexion en lecture
RLIR *(Registered Link Incident Report)*	rapport d'enregistrement d'incident de liaison
RNC *(Report Node Capability)*	rapporter les capacités du nœud
RNFT *(Report Node FC-4 Types)*	rapporter les types FC-4 du nœud
RNID *(Request Node Identification Data)*	demande des données d'identification du nœud
RPL *(Read Port List)*	lire la liste des accès
RPS *(Read Port Status Block)*	lire le bloc d'état de l'accès
RPSC *(Report Port Speed Capabilities)*	rapporter les capacités de vitesse de l'accès
RSCN *(Registered State Change Notification)*	notification de changement d'état enregistrée
RTV *(Read Timeout Value)*	lire la valeur de temporisation
RVCS *(Read Virtual Circuit Status)*	lire l'état du circuit virtuel
SBRP *(Set Bit-Error Reporting Parameters)*	régler les paramètres de rapport d'erreurs binaires
SCN *(State Change Notification)*	notification de changement d'état
SCR *(State Change Registration)*	enregistrement de changement d'état
TEST *(Test)*	essai
TPLS *(Test Process Login State)*	essai du processus d'état d'établissement

Tableau 10. Services de liaison à passer

A.3 Services de liaison particuliers

Les services de liaison étendus et FC-4 du Tableau 11 sont traités par une mise en œuvre de iFCP comme décrit dans les paragraphes auxquels se réfère le tableau.

Nom	Description	Paragraphe
ABTX	Interruption d'échange	7.3.1.1
ADISC	Découverte d'adresse	7.3.1.2
ADISC ACC	Acceptation de découverte d'adresse	7.3.1.3
FARP-REPLY	Réponse de protocole de résolution d'adresse canal fibre	7.3.1.4
FARP-REQ	Demande de protocole de résolution d'adresse canal fibre	7.3.1.5
LOGO	Désétablissement de N_PORT	7.3.1.6
PLOGI	Établissement d'accès	7.3.1.7
REC	Échange en lecture concis	7.3.1.8
REC ACC	Acceptation d'échange en lecture concis	7.3.1.9
FCP REC	Échange en lecture concis FCP (voir [FCP-2])	7.3.2.1.1
FCP REC ACC	Échange en lecture concis FCP (voir [FCP-2])	7.3.2.1.2
RES	Bloc d'état d'échange en lecture	7.3.1.10
RES ACC	Acceptation de bloc d'état d'échange en lecture	7.3.1.11
RLS	État d'erreur de liaison en lecture	7.3.1.12
RRQ	Qualificatif de récupération de réinstallation	7.3.1.14
RSI	Demande d'initiative de séquence	7.3.1.15
RSS	Bloc d'état de séquence en lecture	7.3.1.13
SRL	Examen de la boucle distante	7.3.1.16
TPRLO	Désétablissement de processus de tiers	7.3.1.17
TPRLO ACC	Acceptation de désétablissement de processus de tiers	7.3.1.18

Tableau 11. Services de liaison particuliers

Appendice B. Prise en charge de la topologie de boucle de canal fibre

Une topologie de boucle peut être facultativement prise en charge par une mise en œuvre de passerelle d'une des façons suivantes :
a) en mettant en œuvre l'interface de boucle publique FL_PORT spécifiée dans [FC-FLA] ;
b) en émulant l'environnement de boucle privée spécifié dans [FC-AL2].

L'émulation de boucle privée permet le rattachement d'appareils canal fibre qui ne prennent pas en charge les boucles de tissu ou publiques. La passerelle présente de tels appareils au tissu comme si ils étaient rattachés au tissu. À l'inverse, la passerelle présente les appareils au tissu, qu'ils soient rattachés en local ou à distance, comme si ils étaient connectés à la boucle privée.

La prise en charge de boucle privée exige l'émulation par la passerelle des primitives de la boucle et des trames de contrôle spécifiées dans [FC-AL2]. Ces trames et les primitives DOIVENT être émulées en local par la passerelle. Les trames de contrôle de boucle NE DOIVENT PAS être envoyées sur une session iFCP.

B.1 Contrôle à distance d'une boucle publique

Une passerelle PEUT divulguer qu'un appareil rattaché à distance est connecté à une boucle publique. Si elle le fait, elle DOIT aussi fournir des alias qui représentent l'adresse de tissu de boucle (LFA, *Loop Fabric Address*), l'identifiant de domaine, et l'identifiant d'adresse de FL_PORT correspondant à travers lesquels la boucle publique peut être contrôlée à distance.

Le LFA et l'identifiant d'adresse de FL_PORT représentent tous deux un N_PORT qui dessert les demandes de gestion de boucle distante contenues dans les messages de service de liaison étendu LINIT et SRL. Pour prendre ces messages en charge, la passerelle DOIT allouer un alias de NL_PORT afin que l'alias correspondant pour le LFA ou l'identifiant d'adresse de FL_PORT puisse être déduit en réglant le composant Identifiant d'accès de l'alias de NL_PORT à zéro.

Remerciements

Les auteurs sont redevables à ceux qui ont fourni des contributions et qui ont pris le temps de relire attentivement et critiquer la présente spécification, parmi lesquels David Black (EMC), Rory Bolt (Quantum/ATL), Victor Firoiu (Nortel), Robert Peglar (XIOtech), David Robinson (Sun), Elizabeth Rodriguez, Joshua Tseng (Nishan), Naoke Watanabe (HDS) et les membres du groupe de travail IPS. Pour la révision de la politique de sécurité d'iFCP, les auteurs remercient les auteurs du document sur la sécurité d'IPS [RFC3723], parmi lesquels Bernard Aboba (Microsoft), Ofer Biran (IBM), Uri Elzer (Broadcom), Charles Kunziger (IBM), Venkat Rangan (Rhapsody Networks), Julian Satran (IBM), Joseph Tardo (Broadcom), et Jesse Walker (Intel).

Adresse des auteurs

Les commentaires devraient être envoyés à la liste de diffusion ips (ips@ece.cmu.edu) ou aux auteurs.

Charles Monia
7553 Morevern Circle
San Jose, CA 95135
USA
mél : charles_monia@yahoo.com

Rod Mullendore
McDATA
4555 Great America Pkwy
Suite 301
Santa Clara, CA 95054
mél : Rod.Mullendore@MCDATA.com

Franco Travostino
Nortel
600 Technology Park Drive
Billerica, MA 01821 USA
mél : travos@nortel.com

Wayland Jeong
TROIKA Networks, Inc.
2555 Townsgate Road, Suite 105
Westlake Village, CA 91361
tél : 805-371-1377
mél : wayland@TroikaNetworks.com

Mark Edwards
Adaptec (UK) Ltd.
4th Floor, Howard House
Queens Ave, UK. BS8 1SD
tél : +44 (0)117 930 9600
mél : mark_edwards@adaptec.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org .

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.