Groupe de travail Réseau
Request for Comments : 3821
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

M. Rajagopal
E. Rodriguez
R. Weber
juillet 2004

Canal fibre sur TCP/IP (FCIP)

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Canal fibre sur TCP/IP (FCIP) décrit les mécanismes qui permettent l'interconnexion des îlots de réseau de zone de mémorisation de canal fibre sur des réseaux fondés sur IP pour former un réseau de zone de mémorisation en un seul assemblage de canal fibre. FCIP s'appuie sur les services réseau fondés sur IP pour fournir la connexité entre les îlots de réseau de zone de mémorisation sur des réseaux de zone locale, des réseaux de zone métropolitaine, ou des réseaux de grande zone.

Table des Matières

1. Objet, motifs, et objectifs

Avertissement aux lecteurs familiarisés avec le canal fibre : les normes de canal fibre et celles de l'IETF utilisent le même ordre de transmission des octets. Cependant, la numérotation des bits et des octets est différente. Voir les précisions à l'Appendice A.

Le canal fibre (FC, *Fibre Channel*) est une technologie de réseautage à la vitesse du gigabit ou de plusieurs gigabit/s principalement utilisée pour mettre en œuvre des réseaux à zone de mémorisation (SAN, *Storage Area Network*). Voir à la Section 2 des informations sur la façon dont le canal fibre est normalisé et les relations de la présente spécification avec les normes du canal fibre. On trouvera une description générale du canal fibre dans [34].

La présente spécification décrit les mécanismes qui permettent l'interconnexion d'îlots de SAN canal fibre sur des réseaux IP pour former un SAN unifié dans une seule structure de canal fibre. Le motif de la définition de ces mécanismes d'interconnexion est le désir de connecter physiquement des sites de FC distants pour permettre un accès à distance aux disques, une sauvegarde des mémoires, et un reflet en direct.

Les normes de canal fibre ont choisi des distances nominales entre des éléments de commutation qui sont moindres que les distances disponibles dans un réseau IP. Comme les technologies de canal fibre et de réseautage IP sont compatibles, il est logique de se tourner vers le réseautage IP pour étendre les distances admissibles entre les éléments de commutation de canal fibre.

L'hypothèse fondamentale posée dans la présente spécification est que le trafic de canal fibre est porté sur le réseau IP d'une manière telle que la structure de canal fibre et tous les appareils de canal fibre sur la même structure sont inconscients de la présence du réseau IP. Cela signifie que les datagrammes FC doivent être livrés dans les délais qui se conforment aux spécifications de canal fibre existantes. Le trafic FC peut s'étendre sur des LAN, des MAN, et des WAN, pour autant que cette hypothèse fondamentale soit respectée.

Les objectifs du présent document sont :
1) de spécifier l'encapsulation et la transposition des trames de canal fibre (FC) en utilisant l'encapsulation de trame FC de [19],
2) d'appliquer le mécanisme décrit en 1) à une structure FC utilisant un réseau IP comme interconnexion entre deux îles ou plus dans une structure FC,
3) de traiter tous les aspects de FC concernant le tunnelage du trafic FC sur un réseau fondé sur IP, y compris la sécurité, l'intégrité des données (les pertes), l'encombrement, et les performances. Cela sera accompli en utilisant la suite de protocoles existante spécifiée par l'IETF,
4) être compatible avec les normes FC référencées. Bien que de nouveaux travaux puissent être entrepris dans le comité T11 pour optimiser et améliorer les structures FC, la présente spécification EXIGE la conformité aux seules normes FC référencées,
5) être compatible avec toutes les normes de l'IETF applicables afin que le réseau IP utilisé pour étendre une structure FC puisse être utilisé concurremment pour d'autres objets raisonnables.

Les objectifs du présent document n'incluent pas d'utiliser un réseau IP en remplacement de l'interconnexion de boucle régulée de canal fibre. Aucune définition n'est fournie pour encapsuler les signaux de primitive de boucle pour leur transmission sur un réseau IP.

Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans le BCP 14, RFC2119 [1].

2. Relations avec les normes de canal fibre

2.1 Normes pertinentes de canal fibre

FC est normalisé comme une famille de normes nationales américaines développées par le comité technique T11 de l'INCITS (*InterNational Committee for Information Technology Standards*, comité international pour les normes des technologies de l'information). Le T11 a spécifié un certain nombre de documents qui décrivent les protocoles, le fonctionnement et les services de canal fibre. Les documents du T11qui intéressent les lecteurs de la présente spécification incluent (sans s'y limiter) :

- FC-BB – Cœur de réseau de canal fibre *(Fibre Channel Backbone)* [2]
- FC-BB-2 – Cœur de réseau de canal fibre -2 [3]
- FC-SW-2 – Structure de commutation de canal fibre *(Fibre Channel Switch Fabric)* -2 [4]
- FC-FS – Tramage et signalisation de canal fibre [5]

FC-BB et FC-BB-2 décrivent les relations entre une structure FC et des technologies d'interconnexion non définies par les normes de canal fibre (par exemple, ATM et SONET). FC-BB-2 est le document de canal fibre qui décrit les relations entre FC et TCP/IP, y compris l'utilisation par FC de FCIP.

FC-SW-2 décrit les composants de commutation d'une structure FC et FC-FS décrit le format de trame FC et les caractéristiques de contrôle de base du canal fibre.

Des informations supplémentaires concernant les activités du T11 sont disponibles sur le site du comité à www.t11.org

2.2 Position de cette spécification dans les normes de canal fibre

Lorsqu'on examine le défi lancé par le transport de trames FC sur un réseau IP, il est logique de diviser l'effort de normalisation entre les exigences de TCP/IP et les exigences du canal fibre. La présente spécification couvre les exigences de TCP/IP pour le transport des trames FC ; les documents de canal fibre décrits au paragraphe 2.1 couvrent les exigences du canal fibre.

La présente spécification ne traite que des exigences nécessaires pour utiliser correctement un réseau IP comme un conduit pour les trames FC. Le résultat est une spécification pour une entité FCIP (voir au paragraphe 5.4).

Un produit qui tunnelle une structure FC à travers un réseau IP DOIT combiner l'entité FCIP avec une entité FC (voir le paragraphe 5.3) en utilisant une interface spécifique de la mise en œuvre. Les exigences que fait peser la présente spécification sur une entité FC pour réaliser une livraison appropriée des trames FC sont résumées dans l'Appendice H. On trouvera plus d'informations sur les entités FC dans les normes de canal fibre et on trouvera un exemple d'entité FC dans FC-BB-2 [3].

On ne tentera pas de définir une API spécifique entre une entité FCIP et une entité FC. L'approche est de spécifier les interactions fonctionnelles nécessaires entre une entité FCIP et une entité FC (qui sont toutes deux nécessaires pour transmettre des trames FC à travers un réseau IP) mais de permettre aux mises en œuvre de choisir comment réaliser ces interactions.

3. Terminologie

La présente section définit les termes utilisés pour décrire les concepts de FCIP.

Nœud d'extrémité FC – Appareil FC qui utilise les services de connexion fournis par la structure FC.

Entité FC – Composant fonctionnel de canal fibre spécifique qui se combine avec une entité FCIP pour former une interface entre une structure FC et un réseau IP (voir au paragraphe 5.3).

Structure FC – Entité qui interconnecte divers Nx_Ports (voir [5]) qui lui sont rattachés, et est capable d'acheminer des trames FC en utilisant seulement les informations d'identifiant de destination d'un en-tête de trame FC (voir l'Appendice F).

Entité de structure FC – Élément spécifique de canal fibre contenant un ou plusieurs Interconnect_Ports (voir FC-SW-2 [4]) et une ou plusieurs paires d'entités FC/FCIP. Pour les détails sur les entités de structure FC, voir FC-BB-2 [3].

Trame FC – Unité de base du transfert de données sur canal fibre (voir l'Appendice F).

Portail de réception de trame FC – Point d'accès à travers lequel une trame FC et un horodatage entrent dans un moteur de données FCIP en provenance de l'entité FC.

Portail de transmission de trame FC – Point d'accès à travers lequel une trame FC reconstituée et un horodatage quittent un moteur de données FCIP pour l'entité FC.

Paire d'entité FC/FCIP – Combinaison d'une entité FC et d'une entité FCIP.

Moteur de données FCIP (FCIP_DE) – Composant d'une entité FCIP qui traite l'encapsulation/désencapsulation de trame FC, et la transmission des trames FCIP à travers une seule connexion TCP (voir au paragraphe 5.6).

Entité FCIP – Entité responsable des échanges de protocole FCIP sur le réseau IP et englobe les FCIP_LEP et le module de contrôle et services FCIP (voir au paragraphe 5.4).

Trame FCIP – C'est une trame FC plus l'en-tête d'encapsulation de trame FC [19], codée en SOF et EOF, qui contient la trame FC (voir le paragraphe 5.6.1).

Liaison FCIP – Une ou plusieurs connexions TCP qui connectent un FCIP_LEP à un autre (voir le paragraphe 5.2).

Point d'extrémité de liaison FCIP (FCIP_LEP) – Composant d'une entité FCIP qui traite une seule liaison FCIP et contient un ou plusieurs FCIP_DE (voir au paragraphe 5.5).

Portail receveur de trame encapsulée – Point d'accès TCP à travers lequel est reçue une trame FCIP provenant du réseau IP au moyen d'un moteur de données FCIP.

Portail transmetteur de trame encapsulée – Point d'accès TCP à travers lequel est transmise une trame FCIP vers le réseau IP par un moteur de données FCIP.

Trame spéciale FCIP (FSF) – Trame FC spécialement formatée qui contient des informations utilisées par le protocole FCIP (voir la Section 7).

4. Résumé du protocole

Le protocole FCIP se résume comme suit :

1) La principale fonction d'une entité FCIP est de transmettre des trames FC, employant l'encapsulation de trame FC comme décrit dans [19].

2) Vues dans la perspective du réseau IP, les entités FCIP sont des homologues et communiquent en utilisant TCP/IP. Chaque entité FCIP contient un ou plusieurs points d'extrémité TCP dans le réseau fondé sur IP.

3) Vues dans la perspective de la structure FC, les paires d'entités FCIP, combinées avec leurs entités FC associées, transmettent les trames FC entre les éléments de la structure FC. Les nœuds d'extrémité FC ne connaissent pas l'existence de la liaison FCIP.

4) Les signaux de primitive FC, les séquences de primitives et les trames FC de classe 1 ne sont pas transmises à travers une liaison FCIP parce qu'elles ne peuvent pas être codées en utilisant l'encapsulation de trame FC [19].

5) Le chemin (route) pris par une trame FC encapsulée suit les procédures normales d'acheminement du réseau IP.

6) Une entité FCIP PEUT contenir plusieurs points d'extrémité de liaison FCIP, mais chaque point d'extrémité de liaison FCIP (FCIP_LEP) communique avec exactement un autre FCIP_LEP.

7) Lorsque plusieurs FCIP_LEP sont utilisés avec plusieurs FCIP_DE, le choix de quel FCIP_DE utiliser pour encapsuler et transmettre une certaine trame FC est couvert dans FC-BB-2 [3]. Les entités FCIP ne participent pas activement à l'acheminement des trames FC.

8) Le module de contrôle et de services FCIP PEUT utiliser les caractéristiques de qualité de service de TCP/IP (voir au paragraphe 10.2).

9) Il est nécessaire de configurer statiquement ou de façon dynamique chaque entité FCIP avec les adresses IP et les numéros d'accès TCP qui correspondant aux entités FCIP avec lesquelles on s'attend à initier la communication. Si la découverte dynamique des entités FCIP participantes est prise en charge, la fonction DEVRA être effectuée en utilisant le protocole de localisation de service (SLPv2, *Service Location Protocol*) [17]. Il sort du domaine d'application de la présente spécification de décrire une méthode de configuration statique pour la découverte d'entité FCIP participante. Se reporter au paragraphe 8.1.2.2 pour la description détaillée de la découverte dynamique des entités FCIP participantes en utilisant SLPv2.

10) Avant de créer une connexion TCP avec une entité FCIP homologue, l'entité FCIP qui tente de créer la connexion TCP DEVRA déterminer statiquement ou dynamiquement l'adresse IP, l'accès TCP, le nom mondial espéré de la structure d'entité FC, les paramètres de la connexion TCP, et les informations de qualité de service.

11) Les entités FCIP ne participent pas activement à la découverte des identifiants de source et destination FC. La découverte des adresses FC (accessibles via l'entité FCIP) est fournie par des techniques et protocoles au sein de l'architecture FC, comme décrit dans FC-FS [5] et FC-SW-2 [4].

12) Pour prendre en charge la sécurité du réseau IP (voir la section 9), les entités FCIP DOIVENT :
   1) mettre en œuvre l'authentification protégée cryptographiquement et l'intégrité des données cryptographiques reliées par des clés au processus d'authentification, et
   2) mettre en œuvre les dispositifs de sécurité pour la confidentialité des données.

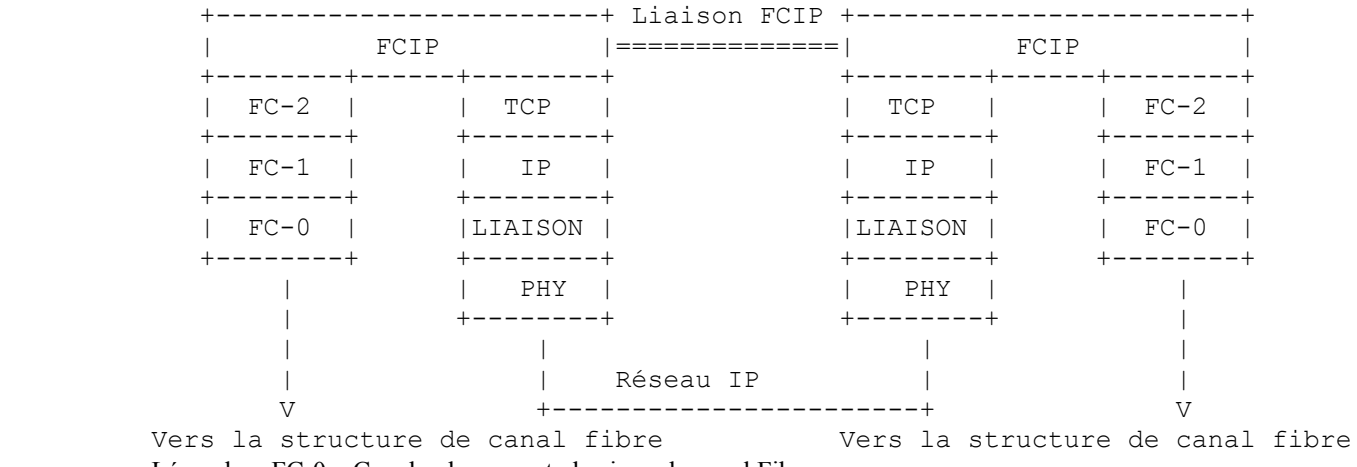
13) Sur une connexion TCP individuelle, la présente spécification s'appuie sur TCP/IP pour livrer un flux d'octets dans le même ordre que celui de son envoi.

14) La présente spécification suppose la présence, et exige l'utilisation, des mécanismes TCP et FC de perte et de corruption des données. Les dispositifs de détection et de récupération d'erreur décrits dans la présente spécification complètent et prennent en charge ces mécanismes existants.

5. Modèle FCIP

5.1 Modèle du protocole FCIP

Les relations entre FCIP et les autres protocoles sont illustrées à la Figure 1.



Légende : FC-0 – Couche de support physique de canal Fibre
FC-1 – Couche de codage et décodage canal Fibre
FC-2 – Couche de tramage et contrôle de flux canal Fibre
TCP – Protocole de contrôle de transmission
IP – Protocole Internet
LIAISON – Couche liaison IP
PHY – Couche physique IP

Figure 1 : Modèle de la pile de protocoles FCIP

Noter que l'objectif du protocole FCIP est de créer et entretenir une ou plusieurs liaisons FCIP pour transporter des données.

5.2 Liaison FCIP

La liaison FCIP est l'unité de base du service fourni par le protocole FCIP à une structure FC. Comme le montre la Figure 2, une liaison FCIP connecte deux portions d'une structure FC en utilisant un réseau IP comme transport pour former une seule structure FC.

Figure 2 : Modèle de liaison FCIP

Aux points où les extrémités de la liaison FCIP rencontrent les portions de la structure FC, une entité FCIP (voir le paragraphe 5.4) se combine avec une entité FC comme décrit au paragraphe 5.3 pour servir d'interface entre FC et IP.

Une liaison FCIP DEVRA contenir au moins une connexion TCP et PEUT contenir plus d'une connexion TCP. Les points d'extrémité d'une seule connexion TCP sont des moteurs de données FCIP (voir au paragraphe 5.6). Les points d'extrémité d'une seule liaison FCIP sont des points d'extrémité de liaison FCIP (voir au paragraphe 5.5).

5.3 Entité FC

Une mise en œuvre qui tunnelle une structure FC à travers un réseau IP DOIT combiner une entité FC avec une entité FCIP (voir au paragraphe 5.4) pour former une interface complète entre la structure FC et le réseau IP comme montré à la Figure 3. Une entité de structure FC peut contenir plusieurs instances de la paire d'entités FC/FCIP montrée sur les deux côtés gauche ou droit de la Figure 3.

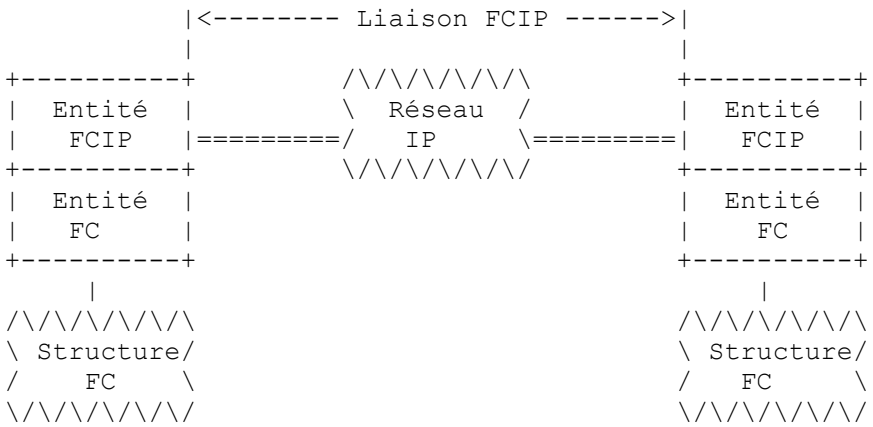


Figure 3 : Modèle pour deux paires d'entités FC/FCIP connectées

En général, la combinaison d'une liaison FCIP et de deux paires d'entités FC/FCIP est destinée à fournir un transport non cœur de réseau canal Fibre entre les composants de canal Fibre. Par exemple, cette combinaison peut être utilisée pour fonctionner comme la connexion filaire entre deux commutateurs canal Fibre.

L'interface entre les entités FC et FCIP est spécifique de la mise en œuvre. Les exigences fonctionnelles qu'impose à une entité FC la présente spécification sont énumérées à l'Appendice H. On trouvera plus d'informations sur les entités FC dans les normes de canal Fibre et un exemple d'entité FC se trouve dans FC-BB-2 [3].

5.4 Entité FCIP

Le modèle d'une entité FCIP est montré à la Figure 4.

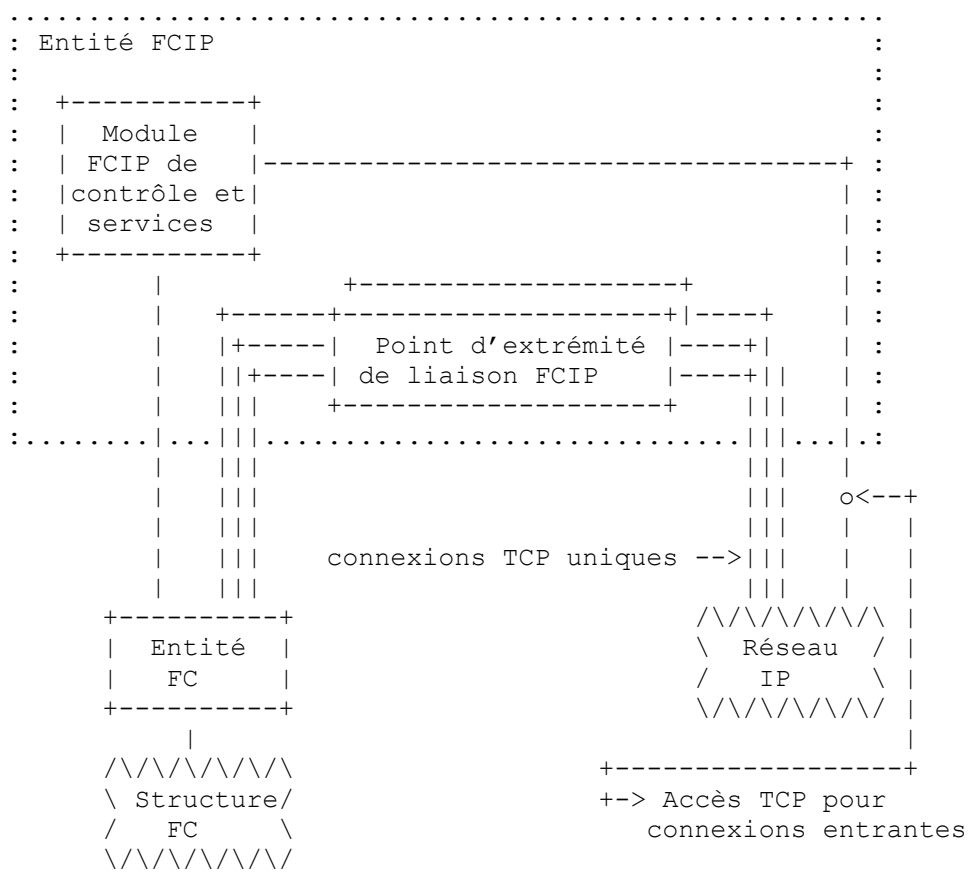


Figure 4 : Modèle d'entité FCIP

L'entité FCIP reçoit les demandes de connexion TCP au nom des FCIP_LEP qu'elle gère. À l'appui de cela, l'entité FCIP est le seul possesseur d'au moins une combinaison d'accès TCP/adresse IP utilisée pour former les connexions TCP. L'accès TCP peut être l'accès FCIP bien connu à une certaine adresse IP. Un produit d'interface de structure FC au réseau IP DEVRA fournir à chaque paire d'entité FC/FCIP contenue dans le produit une combinaison unique de valeurs d'identifiant mondial d'entité FC et d'identifiant d'entité FC/FCIP (voir la Section 7).

Une entité FCIP contient un module FCIP de contrôle et de services pour contrôler l'initialisation de la liaison FCIP, la dissolution de la liaison, et pour fournir à l'entité FC une interface aux dispositifs clés du réseau IP.

Les interfaces avec les dispositifs du réseau IP sont spécifiques de la mise en œuvre, cependant, une prise en charge fonctionnelle de TCP/IP est EXIGÉE par le présent document, ce qui inclut :
- les connexions TCP - voir au paragraphe 8
- la sécurité - voir au paragraphe 9
- les performances - voir au paragraphe 10
- la découverte dynamique - voir au paragraphe 8.1.2.2

Les points d'extrémité de liaison FCIP dans une entité FCIP fournissent les dispositifs d'encapsulation de trame FC et de transmission de FCIP.

5.5 Point d'extrémité de liaison FCIP (FCIP_LEP)

Comme le montre la figure 5, les points d'extrémité de la liaison FCIP contiennent un moteur de données FCIP pour chaque connexion TCP dans la liaison FCIP.

Figure 5 : Modèle de point d'extrémité de liaison FCIP

Chaque fois qu'une connexion TCP est formée avec une nouvelle paire d'entités FC/FCIP (y compris toutes les actions décrites au paragraphe 8.1) l'entité FCIP DEVRA créer un nouveau point d'extrémité de liaison FCIP contenant un moteur de données FCIP.

Un FCIP_LEP est un point transparent de traduction de données entre une entité FC et un réseau IP. Une paire de FCIP_LEP qui communiquent sur une ou plusieurs connexions TCP crée une liaison FCIP pour joindre deux îles d'une structure FC, produisant une seule structure FC.

Le réseau IP sur lequel communiquent les deux FCIP_LEP ne connaît pas les charges utiles FC qu'il porte. De même, les nœuds d'extrémité FC connectés à la structure FC ne connaissent pas le transport fondé sur TCP/IP employé dans la structure de la structure FC.

Un FCIP_LEP utilise les mécanismes normaux de contrôle de flux fondés sur TCP pour gérer ses ressources internes et les faire correspondre avec la taille de fenêtre de récepteur TCP annoncée (voir aux paragraphes 8.3.2 et 8.5). Un FCIP_LEP PEUT communiquer avec sa contrepartie d'entité FC locale pour coordonner le contrôle de flux.

5.6 Moteur de données FCIP (FCIP_DE)

Le modèle pour un des multiples FCIP_DE qui PEUVENT être présents dans un FCIP_LEP est montré à la Figure 6.

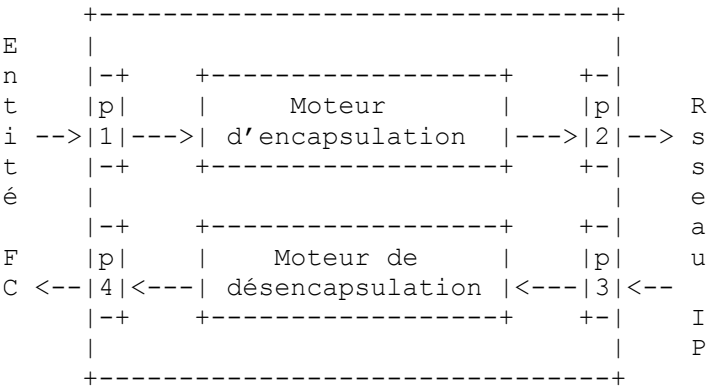


Figure 6 : Modèle de moteur de données FCIP

Les données entrent et sortent du FCIP_DE par quatre portails (p1 à p4). Les portails ne traitent ni n'examinent aucune des données qui les traversent. Ce sont seulement les points d'accès désignés auxquels le FCIP_DE s'interface avec le monde extérieur. Les noms des portails sont les suivants :

p1) Portail récepteur de trame FC : C'est l'interface à travers laquelle une trame FC et un horodatage entrent dans un FCIP_DE en venant d'une entité FC.

p2) Portail émetteur de trame encapsulée : c'est l'interface TCP à travers laquelle une trame FCIP est transmise au réseau IP par un FCIP_DE.

p3) Portail récepteur de trame encapsulée : c'est l'interface TCP à travers laquelle une trame FCIP est reçue du réseau IP par un FCIP_DE.

p4) Portail émetteur de trame FC : c'est l'interface à travers laquelle une trame FC reconstituée et un horodatage sortent d'un FCIP_DE vers l'entité FC.

Le travail du FCIP_DE est fait par les moteurs d'encapsulation et de désencapsulation. Les moteurs ont deux fonctions :
1) encapsuler et désencapsuler les trames FC en utilisant le format d'encapsulation décrit dans "Encapsulation de trame FC" [19] et au paragraphe 5.6.1 du présent document, et
2) détecter les erreurs de transmission de données et effectuer une récupération minimale d'erreur comme décrit au paragraphe 5.6.2.

Les données s'écoulent à travers une paire de FCIP_DE connectés au réseau IP par les sept étapes suivantes :

1) Une trame FC et un horodatage arrivent au portail de réception de trame FC et sont passés au moteur d'encapsulation. La trame FC est supposée avoir été traitée par l'entité FC conformément aux règles FC applicables et n'est pas validée par le FCIP_DE. Si l'entité FC est dans l'état Non synchronisé par rapport à une base horaire, comme décrit dans la spécification d'encapsulation de trame FC [19], l'horodatage livré avec la trame FC DEVRA être zéro.

2) Dans le moteur d'encapsulation, le format d'encapsulation décrit dans Encapsulation de trame FC [19] et au paragraphe 5.6.1 de ce document DEVRA être appliqué pour préparer la trame FC et l'horodatage associé pour transmission sur le réseau IP.

3) La trame FC encapsulée entière (aussi dite trame FCIP) DEVRA être passée au portail émetteur de trame encapsulée où elle DEVRA être insérée dans le flux d'octets TCP.

4) La transmission de la trame FCIP sur le réseau IP suit toutes les règles de fonctionnement de TCP. Cela inclut, mais ne s'y limite pas, la livraison dans l'ordre des octets dans le flux, comme spécifié par TCP [6].

5) La trame FCIP arrive à l'entité FCIP partenaire où elle entre dans le FCIP_DE à travers le portail receveur de trame encapsulée et est passée au moteur de désencapsulation pour traitement.

6) Le moteur de désencapsulation DEVRA valider le flux d'octets TCP entrant comme décrit au paragraphe 5.6.2.2 et DEVRA désencapsuler la trame FC et l'horodatage associé conformément au format d'encapsulation décrit dans "Encapsulation de trame FC" [19] et au paragraphe 5.6.1 de ce document.

7) En l'absence d'erreur, la trame FC désencapsulée et l'horodatage DEVRONT être passés au portail émetteur de trame FC pour livraison à l'entité FC. Le traitement des erreurs est exposé au paragraphe 5.6.2.2.

Chaque trame FC qui arrive au portail de réception de trame FC DEVRA être transmise sur le réseau IP comme décrit aux étapes 1 à 4 ci-dessus. En l'absence d'erreur, les octets de données qui arrivent au portail receveur de trame encapsulée DEVRONT être désencapsulés et transmis au portail émetteur de trame FC comme décrit aux étapes 5 à 7.

5.6.1 Encapsulation FCIP de trames FC

L'encapsulation FCIP de trames FC emploie l'encapsulation de trame FC [19].

Les caractéristiques de l'encapsulation de trame FC qui sont particulières aux protocoles individuels DEVRONT être appliquées comme suit pour l'encapsulation FCIP des trames FC.

Le champ Protocol# DEVRA contenir 1 conformément à l'annexe sur les considérations relatives à l'IANA de "Encapsulation de trame FC" [19].

Le champ Spécifique du protocole DEVRA avoir le format montré à la Figure 7. Noter que les nombres de mot dans la Figure 7 se rapportent à l'en-tête complet d'encapsulation de trame FC, et non au champ spécifique du protocole.

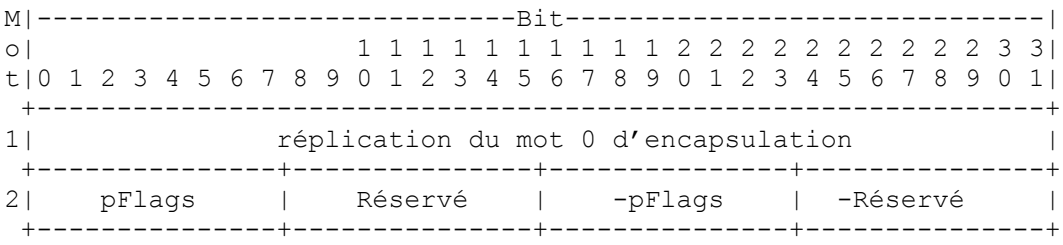


Figure 7 : Utilisation par FCIP des spécificités du champ Protocole d'encapsulation de trame FC

Le mot 1 du champ spécifique du protocole DEVRA contenir une exacte copie du mot 0 dans "Encapsulation de trame FC" [19].

Le champ pFlags (fanions spécifiques du protocole) donne des informations sur l'usage spécifique du protocole de l'en-tête d'encapsulation FC. La Figure 8 montre les bits pFlags définis.

Figure 8 : Bits du champ pFlags

Le bit SF (Trame spéciale) indique si la trame FCIP est une trame FC encapsulée ou une trame FSF (trame FCIP spéciale, voir la Section 7). Lorsque la trame FCIP contient une trame FC encapsulée, le bit SF DEVRA être à 0. Lorsque la trame FCIP est une FSF, le bit SF DEVRA être 1.

La FSF DEVRA n'être envoyée que lors des premiers octets transmis dans chaque direction sur une connexion TCP nouvellement formée et une seule FSF DEVRA être transmise dans chaque direction à la fois (voir au paragraphe 8.1). Après cela, toutes les trames FCIP DEVRONT avoir le bit SF réglé à 0.

Le bit Ch (Changé) indique si une FSF en écho a été altérée intentionnellement (voir au paragraphe 8.1.3). Le bit Ch DEVRA être 0 sauf si le bit FSF est 1. Lorsque la FSF initiale de la connexion TCP est envoyée, le bit Ch DEVRA être 0. Si le receveur d'une demande de connexion TCP fait écho à la FSF sans aucun changement, le bit Ch DEVRA alors continuer d'être à 0. Si le receveur d'une demande de connexion TCP altère la FSF avant d'y faire écho, le bit Ch DEVRA alors être changé en 1.

Le champ -pFlags DEVRA contenir le complément à un du contenu du champ pFlags.

Le Tableau 1 résume l'usage des bits pFlags SF et Ch.

SF	Ch	D'origine ou écho	Validité/Description
0	0	n/a	trame FC encapsulée
0	1	n/a	toujours illégale
1	0	d'origine	FSF d'origine
1	1	d'origine	toujours illégale
1	0	écho	écho FSF sans changement
1	1	écho	écho FSF avec changements

Note 1 : Les échos FSF peuvent contenir des changements qui résultent d'erreurs de transmission, nécessitant la comparaison entre les octets FSF envoyés et reçus par la FSF d'origine décrite au paragraphe 8.1.2.3.
Note 2 : La position des colonnes dans ce tableau ne reflète pas la position des bits SF et Ch dans le champ pFlags.

Tableau 1 : Résumé de l'utilisation du bit pFlags SF et Ch

Les bits pFlags Réservé DEVRONT être 0.

Le champ Réservé (bits 23-16 du mot 2) DEVRA contenir 0.

Le champ -Réservé (bits 7-0 du mot 2) DEVRA contenir 255 (ou 0xFF).

Le fanion CRCV (CRC Valide) DEVRA être réglé à 0.

Le champ CRC DEVRA être réglé à 0.

Dans FCIP, les codes SOF et EOF marqués comme Classe 2, Classe 3, et Classe 4 dans l'encapsulation de trame FC [19] sont légaux.

5.6.2 Détection et récupération d'erreur de moteur de données CIP

5.6.2.1 Assistance TCP avec la détection et la récupération d'erreur de données

TCP [6] exige la livraison en ordre, la génération de sommes de contrôle TCP, et la vérification des sommes de contrôle TCP. Donc, le flux d'octets passé de TCP au FCIP_LEP sera dans l'ordre et sans erreurs détectables par la somme de contrôle TCP. Le FCIP_LEP s'appuie sur TCP pour effectuer ces fonctions.

5.6.2.2 Erreurs dans les en-têtes FCIP et élimination de trames FCIP

Les octets livrés à travers le portail receveur de trame encapsulée qui ne sont pas correctement délimités comme défini par l'encapsulation de trame FC [19] sont considérés comme étant en erreur.

L'échec des champs Protocol# et Version dans l'en-tête FCIP à contenir les valeurs définies pour une trame FCIP DEVRA être considéré comme une erreur.

De plus, certaines erreurs dans l'encapsulation vont résulter en la perte de la synchronisation du FCIP_DE avec les trames FC dans le flux d'octets à l'entrée du portail receveur de trame encapsulée.

Le champ Longueur de trame dans l'en-tête d'encapsulation de trame FC est utilisé pour déterminer où est situé dans le flux de données le prochain en-tête FC encapsulé. Les essais suivants DEVRONT être effectués pour vérifier la synchronisation avec le flux d'octets entrant dans le portail receveur de trame encapsulée, et la synchronisation DEVRA être considérée comme perdue si un des essais échoue :

1) validation du champ Longueur de trame -- 15 < Longueur de trame < 545 ;
2) comparaison du champ Longueur de trame avec son complément à un ; et
3) un EOF valide se trouve dans le mot précédant le début du prochain en-tête FCIP comme indiqué par le champ Longueur de trame, à vérifier comme suit :
    1) les bits 24-31 et 16-23 contiennent des valeurs légales d'EOF identiques (la liste des valeurs légales d'EOF est dans "Encapsulation de trame FC" [19]) ; et
    2) les bits 8-15 et 0-7 contiennent le complément à un de la valeur de l'EOF trouvée dans les bits 24-31.

Note : La gamme des valeurs valides de longueur de trame est déduite comme suit : l'en-tête de trame FCIP fait sept mots, dont chacun est nécessaire pour les valeurs codées de SOF et EOF, l'en-tête de trame FC fait six mots, et le CRC FC exige un mot, ce qui donne une longueur de trame de base de 16 (7+1+1+6+1) mots, si aucune charge utile FC n'est présente. Comme la charge utile FC est facultative, toute valeur de longueur de trame supérieure à 15 est valide. La taille maximum de charge utile FC est de 528 mots, ce qui signifie que toute valeur de longueur de trame jusqu'à et y compris 544 (528+16) est valide.

Si la synchronisation est perdue, la trame FC NE DEVRA PAS être transmise à l'entité FC et une récupération ultérieure DEVRA être traitée comme défini au paragraphe 5.6.2.3.
En plus des essais ci-dessus, la validité et le positionnement des informations de trame FCIP suivantes DEVRAIENT être utilisés pour détecter les erreurs d'encapsulation qui peuvent ou non affecter la synchronisation :

a) complément à un du champ Protocol# (1 essai) ;
b) complément à un du champ Version (1 essai) ;
c) duplication du mot 0 d'encapsulation dans le mot 1 (1 essai) ;
d) champ Réservé et son complément à un (2 essais) ;
e) champ Fanions et son complément à un (2 essais) ;
f) champ CRC est égal à zéro (1 essai) ;
g) champs SOF et champs de complément à un (4 essais) ;
h) format et valeurs de l'en-tête FC (1 essai) ;
i) CRC de la trame FC (2 essais) ;
j) informations d'en-tête d'encapsulation de trame FC dans la prochaine trame FCIP (1 essai).

Au moins 3 des 16 essais de la liste ci-dessus DEVRONT être effectués. L'échec d'un des essais réellement effectués

DEVRA indiquer une erreur d'encapsulation et la trame FC NE DEVRA PAS être transmise à l'entité FC. De plus, de telles erreurs DEVRAIENT être examinées attentivement, car certaines peuvent être des erreurs de synchronisation.

Chaque fois que le FCIP_DE élimine des octets livrés au travers du portail receveur de trame encapsulée, il DEVRA causer une notification de l'entité FCIP à l'entité FC de la condition et fournir une description convenable de la raison de l'élimination des octets.

La charge de la récupération des données éliminées revient à l'entité FC et aux autres composants de la structure FC, et elle sort du domaine d'application de la présente spécification.

5.6.2.3 Échecs de synchronisation

Si un FCIP_DE détermine qu'il ne peut pas trouver le prochain en-tête de trame FCIP dans le flux d'octets qui entre dans le portail receveur de trame encapsulée, le FCIP_DE DEVRA faire une des actions suivantes :

a) clore la connexion TCP [6] [7] et notifier à l'entité FC la raison de la clôture ;
b) récupérer la synchronisation en cherchant dans les octets livrés par le portail receveur de trame encapsulée un en-tête de trame FCIP valide ayant les propriétés correctes (voir au paragraphe 5.6.2.2) et en éliminant les octets livrés par le portail receveur de trame encapsulée jusqu'à ce que soit trouvé un en-tête de trame FCIP valide ; ou
c) tenter de récupérer la synchronisation comme décrit en b) et si la synchronisation ne peut pas être récupérée, clore la connexion TCP comme décrit en a), y compris la notification à l'entité FC de la raison de la clôture.

Si le FCIP_DE tente de récupérer la synchronisation, l'algorithme de resynchronisation utilisé DEVRA satisfaire les exigences suivantes :

a) éliminer ou identifier avec un EOFa (voir à la section F.1) les trames FC et fragments de trames FC identifiés avant que la synchronisation ait été à nouveau complètement vérifiée. Le nombre de trames FC non transmises peut varier selon l'algorithme utilisé ;
b) revenir à la transmission des trames FC à travers le portail d'émission de trame FC après que la synchronisation sur le flux de trames FCIP transmis a été vérifiée ; et
c) clore la connexion TCP/IP si l'algorithme se termine sans que soit vérifiée la réussite de la synchronisation. La probabilité de l'échec de la synchronisation et le temps nécessaire pour déterminer si la synchronisation a réussi ou non peuvent varier selon l'algorithme utilisé.

Un exemple d'algorithme satisfaisant à ces exigences se trouve à l'Appendice D.

La charge de la récupération de l'élimination de trames FCIP durant le processus facultatif de resynchronisation décrit dans cette section incombe à l'entité FC et aux autres composants de la structure FC, et sort du domaine d'application de la présente spécification.

6. Vérification des temps de transit des trames FC dans le réseau IP

FC-BB-2 [3] définit comment sont effectuées les mesures du temps de transit du réseau IP, sur la base des exigences établies dans la spécification de l'encapsulation de trame FC [19]. Le choix de faire peser ces exigences de mise en œuvre sur l'entité FC se fonde sur le désir d'inclure le temps de transit à travers les entités FCIP dans le calcul du temps de transit du réseau IP subi par les trames FC.
Chaque trame FC qui entre dans le FCIP_DE à travers le portail de réception de trame FC DEVRA être accompagnée par une valeur d'horodatage que le FCIP_DE DEVRA placer dans les champs Horodatage [entier] et Horodatage [fraction] de l'en-tête d'encapsulation de la trame FCIP qui contient la trame FC. Si aucune valeur d'horodatage synchronisé n'est disponible pour accompagner la trame FC entrante, une valeur de zéro DEVRA être utilisée.
Chaque trame FC qui sort du FCIP_DE à travers le portail d'émission de trame FC DEVRA être accompagnée par la valeur d'horodatage tirée de la trame FCIP qui encapsulait la trame FC.

L'entité FC DEVRA utiliser des horloges internes convenables et des services de canal Fibre ou un serveur SNTP version 4 [26] pour établir et entretenir la valeur de temps synchronisé requise. L'entité FC DEVRA vérifier que l'entité FC avec laquelle elle communique sur une liaison FCIP utilise la même source de synchronisation, de services de canal Fibre ou d'un serveur SNTP.

Noter que comme la structure FC est supposée avoir une seule valeur d'heure synchronisée, s'appuyer sur les services de canal Fibre signifie qu'une seule valeur d'heure synchronisée est nécessaire pour tous les FCIP_DE, sans considération de leurs caractéristiques de connexion.

7. Trame FCIP spéciale (FSF)

7.1 Format de trame FCIP spéciale

La Figure 9 montre le format de FSF.

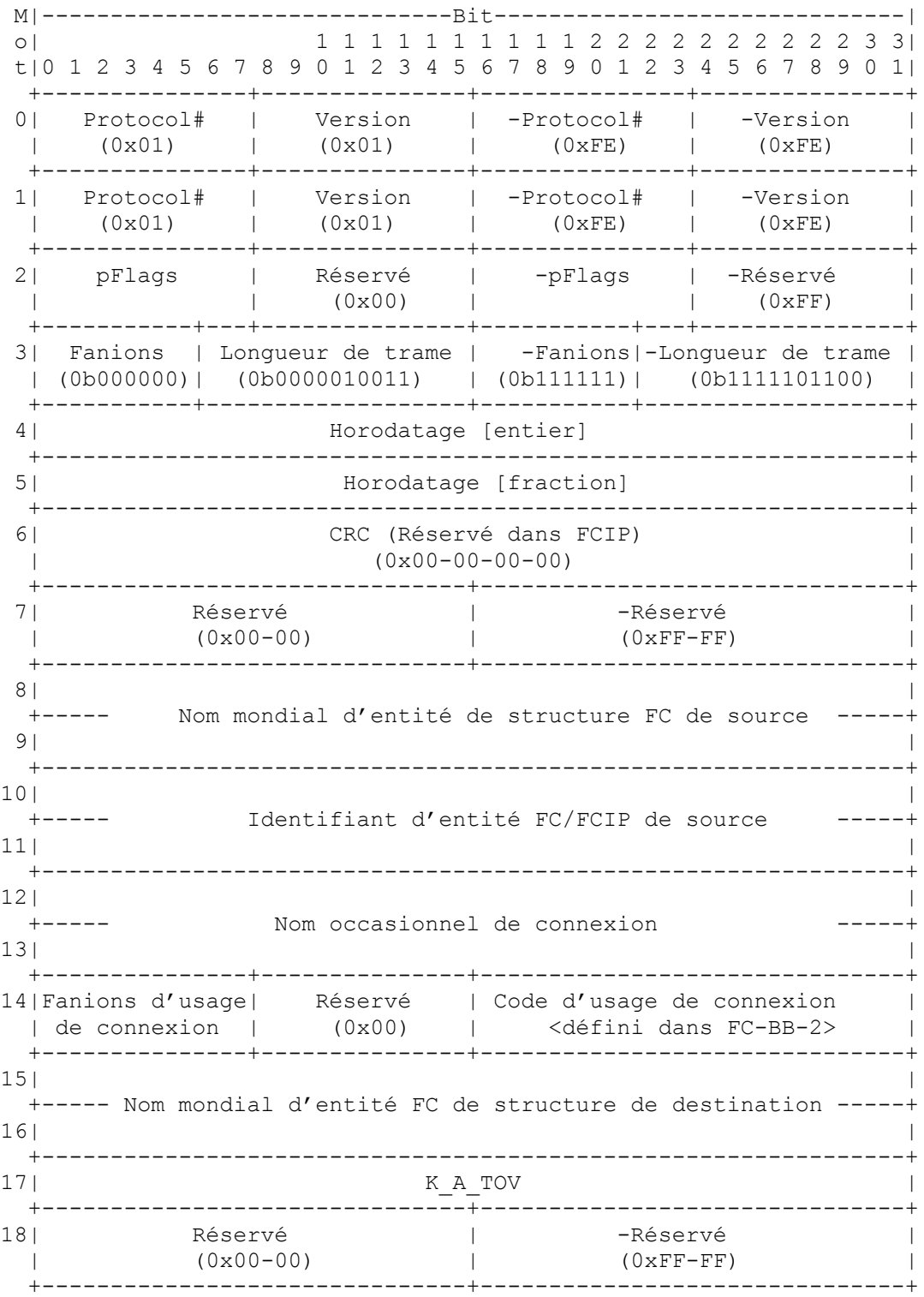


Figure 9 : Format FSF

La FSF DEVRA n'être envoyée que comme les premiers octets transmis dans chaque direction sur une connexion TCP nouvellement formée, et seulement une FSF DEVRA être transmise dans chaque direction.

Le contenu de la FSF DEVRA être comme décrit pour les trames FC encapsulées, sauf pour les champs décrits dans cette section.

Toutes les FSF DEVRONT avoir le bit pFlags SF réglé à 1 (voir au paragraphe 5.6.1).

Le champ Nom mondial d'entité de structure FC de source DEVRA contenir l'identifiant de nom canal Fibre [5] pour l'entité de structure FC associée à la paire d'entités FC/FCIP qui génère (par opposition à celle qui fait écho à) la FSF. Par exemple, si l'entité de structure FC est un commutateur FC, le champ Nom mondial d'entité de structure FC DEVRA contenir le Nom_de_commutateur [4]. Le nom mondial d'entité de structure FC de source DEVRA être unique au monde.

Le champ Identifiant d'entité FC/FCIP de source DEVRA contenir un identifiant unique pour la paire d'entités FC/FCIP qui génère (par opposition à faire écho à) la FSF. La valeur est allouée par l'entité de structure FC dont le nom mondial apparaît dans le champ Nom mondial d'entité de structure FC de source.

Note : La combinaison des champs Nom mondial d'entité FC de source et Identifiant d'entité FC/FCIP de source identifie de façon univoque chaque paire d'entités FC/FCIP dans le réseau IP.

Le champ Nom occasionnel de connexion devra contenir un nombre aléatoire de 64 bits généré pour identifier de façon univoque une seule demande de connexion TCP. Afin de fournir une sécurité suffisante pour le nom occasionnel de connexion, les recommandations d'aléa pour la Sécurité [9] DEVRAIENT être suivies.

Le champ Fanions d'usage de connexion identifie les types de valeurs de SOF [19] à porter sur la connexion comme le montre la Figure 10.

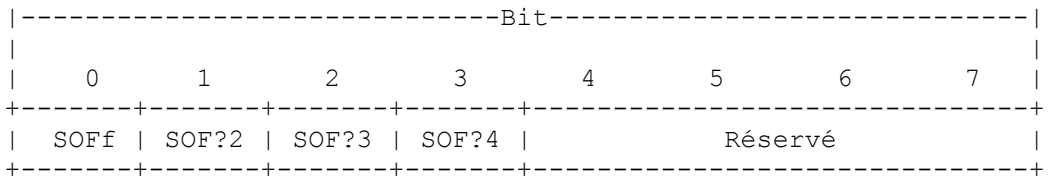


Figure 10 : Format du champ Fanions d'utilisation de connexion

Si le bit SOFf est à un, les trames FC qui contiennent SOFf sont alors destinées à être portées sur la connexion.
Si le bit SOF?2 est à un, les trames FC qui contiennent SOFi2 et SOFn2 sont alors destinées à être portées sur la connexion.
Si le bit SOF?3 est à un, les trames FC qui contiennent SOFi3 et SOFn3 sont alors destinées à être portées sur la connexion.
Si le bit SOF?4 est à un, les trames FC qui contiennent SOFi4, SOFn4, et SOFc4 sont alors destinées à être portées sur la connexion.

Tous les bits SOFf, SOF?2, SOF?3, et SOF?4 PEUVENT être réglés à un, ou aucun ne l'est. Si tous les bits SOFf, SOF?2, SOF?3, et SOF?4 sont à zéro, alors les types de trames FC destinés à être portés sur la connexion n'ont pas de relation spécifique avec le code SOF.

L'entité FCIP NE DEVRA PAS mettre en application l'usage SOF décrit par le champ Fanions d'usage de connexion et DEVRA seulement utiliser le contenu du champ comme décrit ci-dessous.

Le champ Code d'usage de connexion contient des informations définies par canal Fibre concernant l'usage prévu de la connexion comme spécifié dans FC-BB-2 [3].

L'entité FCIP DEVRA utiliser le contenu des champs Fanions d'usage de connexion et Code d'usage de connexion pour localiser les réglages appropriés de QS dans la base de données "partagée" des informations de connexion TCP (voir au paragraphe 8.1.1) et appliquer ces réglages à une connexion nouvellement formée.

Le champ Nom mondial d'entité de structure FC de destination PEUT contenir l'identifiant_de_nom de canal Fibre [5] pour l'entité de structure FC associée à la paire d'entités FC/FCIP qui fait écho (par opposition à celle qui la génère) à la trame spéciale.

Le champ K_A_TOV DEVRA contenir la valeur de la temporisation de garde en vie FC à appliquer à la nouvelle connexion TCP comme spécifié dans FC-BB-2 [3].

Pour chaque nouvelle demande de connexion TCP entrante et les FSF suivantes reçues, l'entité FCIP DEVRA envoyer le contenu des champs Nom mondial d'entité de structure FC de source, Identifiant FC/FCIP de source, Fanions d'usage de connexion et Code d'usage de connexion à l'entité FC avec les autres informations de connexion (par exemple, les informations de FCIP_LEP et de FCIP_DE).

7.2 Vue générale de l'utilisation de FSF dans l'établissement de connexion

Lorsque une nouvelle connexion TCP est établie, une trame spéciale FCIP fait un aller-retour à partir de l'entité FCIP qui initie l'opération de connexion TCP jusqu'à l'entité FCIP qui reçoit la demande de connexion TCP et retour. Cet usage de la FSF sert trois fonctions :

- identification des points d'extrémité de la liaison FCIP,
- transport de quelques paramètres critiques partagés par la paire d'entités FC/FCIP impliquées dans la liaison FCIP,
- découverte de la configuration (utilisée à la place de SLP seulement lorsque permis par les politiques de sécurité du site)

Les exigences spécifiques du format et du protocole pour cet usage de la FSF se trouvent aux paragraphes 7.1 et 8.1.2.3. Le présent paragraphe donne une vue générale de l'usage de la FSF sans faire état des exigences.

Comme FCIP est seulement un tunnel pour une structure de canal Fibre et parce que la structure a son propre algorithme complexe d'établissement de liaison qui peut être employé pour de nombreux besoins d'établissement de liaison FCIP, il est souhaitable de minimiser la complexité de l'usage de la FSF durant l'établissement de la connexion TCP. Cela dit, cet usage de FSF n'est pas un mécanisme de connexion ni de négociation de paramètres. Une seule FSF fait transiter chaque connexion TCP nouvellement établie comme les premiers octets envoyés dans chaque direction.

Note : Cet usage de la FSF ne peut pas être entièrement éliminé parce qu'une connexion TCP nouvellement créée doit être associée à la liaison FCIP correcte avant que l'initialisation de la connexion par la structure FC puisse commencer.

Les premiers octets envoyés de l'initiateur de la demande de connexion TCP au receveur sont une FSF qui identifie à la fois l'envoyeur et celui que l'envoyeur pense être le receveur. Si le contenu de cette FSF est correct et acceptable pour le receveur, un écho inchangé de la FSF est renvoyé à l'envoyeur. Ce processus d'envoi/écho est le seul ensemble d'actions qui permette que la connexion TCP soit utilisée pour porter le trafic de la structure FC. Si le processus d'envoi et d'écho inchangé ne se fait pas, l'algorithme suivi à l'une des extrémités de la connexion TCP ou aux deux résulte en la clôture de la connexion TCP (voir au paragraphe 8.1 les exigences spécifiques de l'algorithme).

Note : Du fait des limitations de l'utilisation de la FSF et de l'exigence qu'il soit fait écho de la FSF sans changement avant qu'il soit permis à une connexion TCP de porter des données d'utilisateur, aucune vérification d'erreur au delà de celles fournies par TCP n'est réputée nécessaire.

Comme décrit ci-dessus, le principal objet de l'utilisation de la FSF durant l'établissement de la connexion TCP est d'identifier la liaison FCIP à laquelle appartient la nouvelle connexion TCP. À partir de cela, il n'est pas très difficile d'imaginer d'utiliser la FSF comme un outil simplifié de découverte de configuration, et le mécanisme d'une telle utilisation est décrit au paragraphe 8.1.

Cependant, l'utilisation de la FSF pour la découverte de la configuration ne dispose pas de la large gamme de capacités offerte par SLPv2 et il lui manque en particulier les capacités de sécurité de SLPv2. Pour cette raison, l'utilisation de la FSF pour la découverte de la configuration n'est pas appropriée dans tous les environnements. Donc, le choix d'utiliser la FSF aux fins de découverte est un choix de politique à inclure dans la base de données "partagée" d'établissement de connexion TCP décrite au paragraphe 8.1.1.

Lorsque la découverte de configuration fondée sur la FSF est activée, les règles normales d'établissement de connexion TCP précisées ci-dessus sont modifiées comme suit.

Normalement, l'algorithme exécuté par une entité FCIP qui reçoit une FSF comporte de vérifier que ses propres informations d'identification dans la FSF qui arrive sont correctes et de clore la connexion TCP si elles ne le sont pas. Cela peut être vu comme l'exigence que l'initiateur d'une demande de connexion TCP sache à l'avance l'identité de l'entité FCIP qui est la cible de cette demande (en utilisant SLP, par exemple) et que la FSF dise effectivement, "je pense que je parle à X". Si l'interlocuteur de l'autre extrémité de la demande de connexion TCP est réellement Y, il répond tout simplement.

La découverte fondée sur la FSF permet que le "je pense que je parle à X" soit remplacé par "Dites moi, s'il vous plait, à qui j'ai l'honneur de parler ?", qui se fait en remplaçant une valeur explicite dans le champ Nom mondial d'entité de structure FC de destination par zéro.

Si la politique de l'entité FCIP receveuse permet la découverte fondée sur la FSF, le zéro est remplacé par la valeur correcte de Nom mondial d'entité de structure FC de destination dans la FSF en écho. Cela est encore soumis au règles d'envoi avec un écho inchangé, et la clôture de connexion TCP survient après la réception de la FSF en écho par l'initiateur de la connexion TCP.
En dépit de la clôture de la connexion TCP, l'initiateur de la connexion TCP sait cependant maintenant le nom mondial d'entité de structure FC de destination correct de l'entité FCIP à une certaine adresse IP et une séquence ultérieure

d'établissement de connexion TCP réussira probablement.

Le bit Ch dans le champ pFlags (voir au paragraphe 5.6.1) permet une différenciation entre les changements de la FSF résultant d'erreurs de transmission et les changements qui résultent d'actes intentionnels du receveur de la FSF.

8. Gestion de connexion TCP

8.1 Établissement de connexion TCP

8.1.1 Modèle d'établissement de connexion

La description du processus d'établissement de connexion est un modèle pour les interactions entre une entité FC et une entité FCIP durant l'établissement de la connexion TCP. Le modèle est décrit en terme de base de données "partagée" que l'entité FCIP consulte pour déterminer les propriétés des connexions TCP à former combiné avec des invocations de sous-programmes à l'entité FC lorsque les connexions sont bien établies. Que l'entité FC contribue aux informations de la base de données "partagée" n'est pas critique pour ce modèle. Cependant, le fait que l'entité FCIP PEUT consulter la base de données à tout moment pour déterminer ses actions par rapport à l'établissement de la connexion TCP est important.

Il est important de se rappeler que cette description est seulement un modèle pour les interactions entre une entité FC et une entité FCIP. Toute mise en œuvre qui a les mêmes effets sur la structure FC et le réseau IP que ceux décrits en utilisant le modèle satisfait aux exigences de la présente spécification. Par exemple, une mise en œuvre peut remplacer la base de données "partagée" par un sous-programme d'interface entre les entités FC et FCIP.

8.1.2 Création de nouvelles connexions TCP

8.1.2.1 Création non dynamique de nouvelles connexions TCP

Lorsque une entité FCIP découvre qu'une nouvelle connexion TCP doit être établie, elle DEVRA déterminer l'adresse IP à laquelle la connexion TCP est à faire et établir toutes les caractéristiques de sécurité IP activées pour cette adresse IP comme décrit à la Section 9. Puis, l'entité FCIP DEVRA déterminer les informations suivantes sur la nouvelle connexion en plus de l'adresse IP :

- le nom mondial d'entité de structure FC de destination attendu de la paire d'entités FC/FCIP entre lesquelles la connexion TCP est faite,
- les paramètres de connexion TCP (voir au paragraphe 8.3),
- les informations de qualité de service (voir la Section 10).

Sur la base de ces informations, l'entité FCIP DEVRA générer une demande de connexion TCP [6] à l'accès FCIP bien connu 3225 (ou autre numéro d'accès spécifique de la configuration) à l'adresse IP spécifiée.

Si la demande de connexion TCP est rejetée, l'entité FCIP DEVRA agir pour limiter la répétition inutile de tentatives d'établissement de connexions similaires. Par exemple, l'entité FCIP peut attendre 60 secondes avant d'essayer à nouveau d'établir la connexion.

Si la demande de connexion TCP est acceptée, l'entité FCIP DEVRA suivre les étapes décrites au paragraphe 8.1.2.3 pour achever l'établissement d'un nouveau FCIP_DE.

Il est RECOMMANDÉ qu'une entité FCIP n'initie pas de demande de connexion TCP à une autre entité FCIP si les demandes de connexion TCP entrantes de cette entité FCIP ont déjà été acceptées.

8.1.2.2 Création dynamique de nouvelles connexions TCP

Si la découverte dynamique des entités FCIP participantes est prise en charge, la fonction DEVRA être effectuée en utilisant le protocole de localisation de service (SLPv2) [17] de la manière définie pour l'usage de FCIP [20].

En découvrant que la découverte dynamique peut être utilisée, l'entité FCIP DEVRA activer les caractéristiques de sécurité IP pour le processus de découverte SLP comme décrit dans [20] puis :

1) déterminer le ou les domaines de découverte FCIP à utiliser dans le processus de découverte dynamique ;
2) établir un agent de service SLPv2 pour annoncer la disponibilité de cette entité FCIP aux entités FCIP homologues dans le ou les domaines de découverte FCIP identifiés ; et
3) établir un agent d'utilisateur SLPv2 pour localiser les annonces de service pour les entités FCIP homologues dans le ou les domaines de découverte FCIP identifiés.

Pour chaque entité FCIP homologue découverte dynamiquement au travers de l'agent d'utilisateur SLPv2, l'entité FCIP DEVRA établir tous les dispositifs de sécurité IP activés pour l'adresse IP découverte comme décrit à la Section 9 et ensuite déterminer les informations suivantes sur la nouvelle connexion :
- le nom mondial d'entité de structure FC de destination attendu de la paire d'entités FC/FCIP avec laquelle la connexion TCP est constituée,
- les paramètres de connexion TCP (voir au paragraphe 8.3)
- les informations de qualité de service (voir la Section 10).

Sur la base de ces informations, l'entité FCIP DEVRA générer une demande de connexion TCP [6] à l'accès FCIP bien connu 3225 (ou autre numéro d'accès spécifique de la configuration) à l'adresse IP spécifiée par l'annonce de service. Si la demande de connexion TCP est rejetée, agir pour limiter la répétition inutile des tentatives d'établir des connexions similaires. Si la demande de connexion TCP est acceptée, l'entité FCIP DEVRA suivre les étapes décrites au paragraphe 8.1.2.3 pour achever l'établissement d'un nouveau FCIP_DE.

Il est recommandé qu'une entité FCIP n'initie pas de demande de connexion TCP avec une autre entité FCIP si des demandes de connexion TCP entrantes provenant de cette entité FCIP ont déjà été acceptées.

8.1.2.3 Établissement de connexion après une demande Connexion TCP réussie

Qu'une création non dynamique de connexion TCP (voir au paragraphe 8.1.2.1) ou une création dynamique de connexion TCP (voir au paragraphe 8.1.2.2) soit utilisée, les étapes décrites dans ce paragraphe DEVRONT être suivies pour achever le processus d'établissement de connexion TCP.

Après que la demande de connexion TCP a été acceptée, l'entité FCIP DEVRA envoyer une trame spéciale FCIP (FSF, voir la Section 7) comme premiers octets transmis sur la connexion nouvellement formée, et conserver une copie de ces octets pour les comparaisons ultérieures. Tous les champs de la FSF DEVRONT être remplis comme décrit à la section 7, en particulier :
- le champ Nom mondial d'entité de structure FC de source DEVRA contenir le nom mondial d'entité de structure FC pour la paire d'entités FC/FCIP qui a généré la demande de connexion TCP ;
- le champ Identifiant d'entité FC/FCIP de source DEVRA contenir un identifiant univoque qui est alloué par l'entité de structure FC dont le nom mondial apparaît dans le champ Nom mondial d'entité de structure FC de source ;
- le champ Nom occasionnel de connexion DEVRA contenir un nombre aléatoire de 64 bits qui diffère en valeur de toute valeur de nom occasionnel de connexion récemment utilisé. Afin de fournir une sécurité suffisante pour le nom occasionnel de connexion, les recommandations d'aléa pour la sécurité [9] DEVRAIENT être suivies; et
- le champ Nom mondial d'entité de structure FC de destination DEVRA contenir 0 ou le nom mondial attendu d'entité de structure FC pour la paire d'entités FC/FCIP dont la destination est la demande de connexion TCP.

Après l'envoie de la FSF sur la connexion nouvellement formée, l'entité FCIP DEVRA attendre l'écho de la FSF comme premiers octets reçus sur la connexion nouvellement formée.

L'entité FCIP PEUT appliquer une temporisation de pas moins de 90 secondes pendant qu'elle attend l'écho des octets de FSF. Si la temporisation arrive à expiration, l'entité FCIP DEVRA clore la connexion TCP et notifier à l'entité FC la raison de la clôture.

Si l'écho des octets de FSF ne correspond pas exactement aux octets de FSF envoyés (des mots 7 à 17 inclus) ou si le champ Nom mondial d'entité de structure FC de destination en écho contient zéro, l'entité FCIP DEVRA clore la connexion TCP et notifier à l'entité FC la raison de la clôture.

L'entité FCIP ne DEVRA effectuer les étapes suivantes que si les octets de l'écho de la FSF correspondent exactement aux octets de FSF envoyés (mots 7 à 17 inclus).

1) Instancier les conditions appropriées de qualité de service (voir la Section 10) sur la connexion TCP nouvellement créée,
2) si l'adresse IP et l'accès TCP auxquels la connexion TCP a été faite ne sont associés à aucun autre FCIP_LEP, créer un nouveau FCIP_LEP pour la nouvelle liaison FCIP,
3) créer un nouveau FCIP_DE au sein du FCIP_LEP nouvellement créé pour desservir la nouvelle connexion TCP, et
4) informer l'entité FC des nouveaux FCIP_LEP, FCIP_DE, nom mondial d'entité de structure FC de destination, fanions d'usage de connexion, et code d'usage de connexion.

8.1.3 Traitement des demandes de connexion TCP entrantes

L'entité FCIP DEVRA écouter les demandes de nouvelle connexion TCP [6] sur l'accès FCIP bien connu (3225). Une entité FCIP PEUT aussi accepter et établir des connexions TCP sur un numéro d'accès TCP autre que l'accès FCIP bien connu, comme configuré par l'administrateur de réseau d'une manière qui sort du domaine d'application de la présente spécification.

L'entité FCIP DEVRA déterminer les informations suivantes sur la connexion demandée :
- si la base de données "partagée" (voir au paragraphe 8.1.1) permet la connexion demandée,
- si l'établissement de la sécurité IP a été effectuée pour les dispositifs de sécurité IP activés sur la connexion (voir la Section 9).

Si la connexion demandée n'est pas admise, l'entité FCIP DEVRA rejeter la demande de connexion en utilisant les moyens TCP appropriés. Si la connexion demandée est admise, l'entité FC DEVRA s'assurer que les dispositifs de sécurité IP requis sont activés et accepter la demande de connexion TCP.

Après l'acceptation de la demande de connexion TCP, l'entité FCIP DEVRA attendre la FSF envoyée par le générateur de la demande de connexion TCP (voir au paragraphe 8.1.2) comme premiers octets reçus sur la connexion acceptée.

L'entité FCIP PEUT appliquer une temporisation de pas moins de 90 secondes pour l'attente des octets de la FSF. Si la temporisation arrive à expiration, l'entité FCIP DEVRA clore la connexion TCP et notifier à l'entité FC la raison de la clôture.

Note : Une méthode pour attaquer la sécurité du processus de formation de la liaison FCIP (détaillé au paragraphe 9.1) dépend du fait qu'une demande de connexion TCP soit gardée ouverte sans envoyer de FSF. Les mises en œuvre devraient garder cela en mémoire pour le traitement des demandes de connexion TCP lorsque la FSF n'est pas envoyée à temps.

À réception de la FSF envoyée par le générateur de la demande de connexion TCP, l'entité FCIP DEVRA inspecter le contenu des champs suivants :
- Nom occasionnel de connexion,
- Nom mondial d'entité de structure FC de destination,
- Fanions d'usage de connexion, et
- Code d'usage de connexion.

Si le champ Nom occasionnel de connexion contient une valeur identique à celle du nom occasionnel reçu le plus récemment de la même adresse IP, l'entité FCIP DEVRA clore la connexion TCP et notifier à l'entité FC la raison de la clôture.
Si une entité FCIP reçoit une FSF dupliquée durant le processus de formation de la liaison FCIP, elle DEVRA clore cette connexion TCP et notifier à l'entité FC la raison de la clôture.

Si le Nom mondial d'entité de structure FC de destination contient 0, l'entité FCIP DEVRA effectuer une des trois actions suivantes :
1) laisser le champ Nom mondial d'entité de structure FC de destination et le bit Ch tous deux à 0 ;
2) changer le champ Nom mondial d'entité de structure FC de destination pour qu'il corresponde au nom mondial d'entité de structure FC associé à l'entité FCIP qui a reçu la demande de connexion TCP et changer le bit Ch à 1 ; ou
3) clore la connexion TCP sans envoyer de réponse.

Le choix entre les actions ci-dessus dépend de l'usage prévu pour l'entité FCIP. L'entité FCIP peut consulter la base de données "partagée" lors du choix entre les actions ci-dessus :
a) si le nom mondial d'entité de structure FC de destination contient une valeur différente de zéro qui ne correspond pas au nom mondial d'entité de structure FC associée à l'entité FCIP qui a reçu la demande de connexion TCP, ou
b) si le contenu des champs Fanions d'usage de connexion et Code d'usage de connexion n'est pas acceptable pour l'entité FCIP qui a reçu la demande de connexion TCP, l'entité FCIP DEVRA alors prendre une des deux mesures suivantes :
    1) changer le contenu des champs inacceptables en valeurs correctes/acceptables et régler le bit Ch à 1 ; ou
    2) clore la connexion TCP sans envoyer de réponse.

Si l'entité FCIP fait des changements au contenu de la FSF, elle DEVRA aussi régler le bit Ch à 1.

Si des changements ont été faits à la FSF reçue durant le traitement décrit ci-dessus, les étapes suivantes DEVRONT être effectuées :
1) la FSF changée DEVRA être renvoyée en écho à l'origine de la demande de connexion TCP comme les seuls octets transmis sur la connexion acceptée ;

2) la connexion TCP DEVRA être close (l'entité FC n'a pas besoin d'être notifiée de la clôture de la connexion TCP dans ce cas parce que cela n'indique pas une erreur) ; et
3) tous les traitements supplémentaires décrits dans ce paragraphe DEVRONT être sautés.

Les étapes restantes de ce paragraphe ne DEVRAIENT être effectuées que si l'entité FCIP n'a pas changé le contenu des champs susmentionnés en valeurs correctes/acceptables.

Si les valeurs des champs Nom mondial d'entité de structure FC de source et Identifiant d'entité FC/FCIP de source dans la FSF ne correspondent pas au nom mondial d'entité de structure FC de source et à l'identifiant d'entité FC/FCIP de source associés à un autre FCIP_LEP, l'entité FCIP DEVRA :
1) faire écho de la FSF inchangée à l'origine de la demande de connexion TCP comme premiers octets transmis sur la connexion acceptée ;
2) instancier les conditions appropriées de qualité de service (voir au paragraphe 10.2) sur la connexion TCP nouvellement créée, en considérant les champs Fanions d'usage de connexion et Code d'usage de connexion, et les informations de la base de données "partagée" (voir au paragraphe 8.1.1) selon ce qui est approprié,
3) créer un nouveau FCIP_LEP pour la nouvelle liaison FCIP,
4) créer un nouveau FCIP_DE au sein du FCIP_LEP nouvellement créé pour desservir la nouvelle connexion TCP, et
5) informer l'entité FC des nouveaux FCIP_LEP, FCIP_DE, nom mondial d'entité de structure FC de source, identifiant d'entité FC/FCIP de source, fanions d'usage de connexion, et code d'usage de connexion.

Si les valeurs des champs Nom mondial d'entité de structure FC de source et Identifiant d'entité FC/FCIP de source dans la trame spéciale FCIP correspondent au nom mondial d'entité de structure FC de source et à l'identifiant d'entité FC/FCIP de source associés à un FCIP_LEP existant, l'entité FCIP DEVRA :
1) Demander que l'entité FC authentifie la source de la demande de connexion TCP (voir FC-BB-2 [3]), en fournissant les informations suivantes à l'entité FC pour les besoins de l'authentification :
   a) nom mondial d'entité de structure FC de source,
   b) identifiant d'entité FC/FCIP de source, et
   c) nom occasionnel de connexion.

   L'entité FCIP NE DEVRA PAS utiliser la nouvelle connexion TCP jusqu'à ce que l'entité FC ait authentifié la source de la demande de connexion TCP. Si l'entité FC indique que la demande de connexion TCP ne peut pas être correctement authentifiée, l'entité FCIP DEVRA clore la connexion TCP et sauter toutes les étapes restantes de ce paragraphe.

   La définition de l'entité FC DEVRA inclure un mécanisme d'authentification à utiliser en réponse à une source de demande de connexion TCP qui communique avec la paire d'entités FC/FCIP partenaires sur une liaison FCIP existante. Ce mécanisme d'authentification devrait utiliser une connexion TCP authentifiée antérieurement dans la liaison FCIP existante pour authentifier le nom occasionnel de connexion envoyé dans le processus d'établissement de la nouvelle connexion TCP. L'entité FCIP DEVRA traiter l'échec de cette authentification comme un échec d'authentification pour le processus d'établissement de la nouvelle connexion TCP.
2) Faire écho de la FSF inchangée à l'origine de la demande de connexion TCP comme premiers octets transmis sur la connexion acceptée ;
3) instancier les conditions de qualité de service appropriées (voir au paragraphe 10.2) sur la connexion TCP nouvellement créée, en considérant les champs Fanions d'usage de connexion et Code d'usage de connexion, et les informations de la base de données "partagée" (voir au paragraphe 8.1.1) selon le cas approprié,
4) créer un nouveau FCIP_DE au sein du FCIP_LEP existant pour desservir la nouvelle connexion TCP, et
5) informer l'entité FC des nouveaux FCIP_LEP, Nom mondial d'entité de structure FC de source, Identifiant d'entité FC/FCIP de source, Fanions d'usage de connexion, Code d'usage de connexion, et FCIP_DE.

Noter que l'origine des demandes de connexion TCP utilise l'adresse IP et l'accès TCP pour identifier quelles connexions TCP appartiennent aux FCIP_LEP, tandis que le receveur des demandes de connexion TCP utilise les champs Nom mondial d'entité de structure FC de source, et Identifiant d'entité FC/FCIP de source de la FSF pour identifier quelle connexion TCP appartient à quels FCIP_LEP. Pour cette raison, une entité FCIP qui génère et reçoit à la fois des demandes de connexion TCP est dans l'incapacité de faire correspondre les FCIP_LEP associés aux demandes de connexion TCP générées aux FCIP_LEP associés aux demandes de connexion TCP reçues.

8.1.4 Établissement de connexions simultanées

Si deux entités FCIP effectuent simultanément des opérations d'ouverture, deux connexions TCP sont alors formées et le SF génère à une extrémité sur une connexion et à l'autre extrémité sur l'autre. L'établissement de connexion se poursuit comme décrit ci-dessus sur les deux connexions, et les étapes décrites ci-dessus résultent en la formation correcte de deux liaisons FCIP entre les mêmes entités FCIP.
Ce n'est pas une erreur. Le canal Fibre est parfaitement capable de traiter deux connexions approximativement égales entre des éléments de structure FC.

La décision d'établir des paires de liaisons FCIP de cette manière est considérée comme étant une décision de politique du site qui peut être couverte dans la base de données "partagée" décrite au paragraphe 8.1.1.

8.2 Clôture des connexions TCP

L'entité FCIP DEVRA fournir un mécanisme avec accusé de réception par lequel l'entité FC soit capable de causer la clôture d'une connexion TCP existante à tout moment. Cela permet à l'entité FC de clore les connexions TCP qui produisent trop d'erreurs, etc.

8.3 Paramètres de connexion TCP

Afin de fournir une gestion efficace des ressources de FCIP_LEP ainsi que des liaisons FCIP, l'examen de certains paramètres de connexion TCP est recommandé.

8.3.1 Option d'accusé de réception sélectif TCP

L'option d'accusé de réception sélectif de la RFC 2883 [18] permet au receveur d'accuser réception de plusieurs paquets perdus en un seul ACK, permettant une récupération plus rapide. Une entité FCIP PEUT négocier l'utilisation du SACK TCP et l'utiliser pour une récupération plus rapide de paquets perdus et de trous dans l'espace des numéros de séquence TCP.

8.3.2 Option d'adaptation de fenêtre TCP

L'option TCP Adaptation de fenêtre [8] permet que des tailles de fenêtre TCP plus grandes que la limite de 16 bits soient annoncées par le receveur. Il est nécessaire de permettre que les données remplissent le tuyau disponible dans les gros réseaux. Cela implique aussi que le tampon du côté de l'envoyeur TCP corresponde au produit (bande passante * délai) de la connexion TCP. Un FCIP_LEP utilise les mécanismes disponibles en local pour régler une taille de fenêtre qui corresponde aux ressources locales de mémoire tampon disponibles et au débit désiré.

8.3.3 Protection contre le retour à zéro de numéro de séquence

Il est RECOMMANDÉ que les entités FCIP mettent en œuvre une protection contre le retour à zéro des numéros de séquence PAWS [8]. Il est tout à fait possible qu'au sein d'une seule connexion, les numéros de séquence TCP reviennent à zéro au sein d'une fenêtre de temporisation.

8.3.4 Option TCP_NODELAY

Les entités FCIP devraient désactiver l'algorithme de Nagle, comme décrit dans la RFC 1122 [7] paragraphe 4.2.3.4. Traditionnellement, cela peut se faire en réglant l'option TCP_NODELAY à un à l'interface TCP locale.

8.4 Considérations sur les connexions TCP

En mode repos, une option "garder en vie" de connexion TCP est normalement utilisée pour garder une connexion en vie. Cependant, cette temporisation est très longue et peut empêcher la détection précoce d'une perte de connexité. Afin de faciliter une détection plus rapide de la perte de connexité, les entités FC DEVRAIENT mettre en œuvre une forme de détection de défaillance de connexion de canal Fibre (voir FC-BB-2 [3]).

Lorsque une entité FCIP découvre que la connexité TCP a été perdue, l'entité FCIP DEVRA notifier à l'entité FC la défaillance en incluant les informations sur la raison de la défaillance.

8.5 Transposition de contrôle de flux entre TCP et FC

L'entité FCIP et l'entité FC sont connectées, respectivement, au réseau IP et à la structure FC, et elles ont besoin de suivre les mécanismes de contrôle de flux de TCP et de FC, qui travaillent de façon indépendante l'un de l'autre.

Ce paragraphe donne des lignes directrices sur la façon dont l'entité FCIP peut transposer le contrôle de flux TCP en notifications d'état chez l'entité FC.

Il y a deux scénarios dans lesquels la gestion du contrôle de flux devient cruciale :

1) Lorsque il y a une discordance de vitesse de ligne entre les interfaces FC et IP.
   Bien qu'il soit RECOMMANDÉ que les deux interfaces FC et IP aux entités respectivement FC et FCIP aient des vitesses comparables, il est possible de porter du trafic FC sur un réseau IP qui a une vitesse de ligne et un taux d'erreurs binaires différents.

2) Lorsque la structure FC ou le réseau IP rencontre de l'encombrement.
   Même lorsque la structure FC ou le réseau IP ont tous deux des vitesses comparables, durant le cours du fonctionnement, la structure FC ou le réseau IP pourraient rencontrer de l'encombrement dû à des conditions transitoires.

L'entité FC utilise les mécanismes de canal Fibre pour le contrôle de flux au portail de réception de trame FC sur la base des informations fournies par l'entité FCIP en ce qui concerne les contraintes de flux au portail émetteur de trame encapsulée. L'entité FCIP utilise les mécanismes de TCP pour le contrôle de flux au portail receveur de trame encapsulée sur la base des informations fournies par l'entité FC en ce qui concerne les contraintes de flux au portail émetteur de trame FC.

La coordination de ces mécanismes de contrôle de flux, dont l'un est fondé sur le crédit et l'autre est fondé sur la fenêtre, dépend de concepts délicats qui sortent du domaine d'application de la présente spécification.

9. Sécurité

FCIP utilise la suite de protocoles IPsec pour assurer les services de confidentialité et d'authentification des données, et IKE comme protocole de gestion de clé. La présente section décrit les exigences des divers composants de ces protocoles tels qu'utilisés par FCIP, sur la base des environnements de fonctionnement de FCIP. Des considérations supplémentaires sur l'utilisation de IPsec et IKE avec le protocole FCIP se trouvent dans la RFC3723 [21]. En cas de conflit entre les exigences de [21] et celle qui sont déclarées dans le présent document, ce sont celles du présent document qui prévalent.

9.1 Modèles de menace

L'utilisation d'un réseau de large zone ordinaire, comme un réseau IP, comme remplacement fonctionnel d'un câblage physique introduit des problèmes de sécurité qu'on ne rencontre normalement pas dans une structure de canal Fibre. Le câblage d'interconnexion FC est normalement protégé physiquement contre l'accès de l'extérieur. Les réseaux IP publics permettent à des parties hostiles d'impacter la sécurité de l'infrastructure de transport.

L'effet général est que la sécurité d'une structure FC n'est aussi bonne que celle de l'entité réseau IP qui porte les liaisons FCIP utilisées par cette structure FC. Les grandes classes d'attaques suivantes sont possibles :

1) Des éléments de canal Fibre non autorisés peuvent obtenir l'accès à des ressources par une structure et des processus canal Fibre normaux. Bien que ce soit une menace sérieuse, la sécurisation des structures de canal Fibre sort du domaine d'application du présent document. Sécuriser le réseau IP est la question examinée par cette spécification.

2) Des agents non autorisés peuvent surveiller et manipuler le trafic canal Fibre qui s'écoule sur des supports physiques utilisés par le réseau IP et accessibles à l'agent.

3) Des connexions TCP peuvent être capturées et utilisées pour instancier une liaison FCIP invalide entre deux entités FCIP homologues.

4) Des trames FCIP valides et invalides peuvent être injectées sur les connexions TCP.

5) La charge utile d'une trame FCIP peut être altérée ou transformée. La somme de contrôle TCP, les vérifications de complément à un de FCIP, et le CRC de trame FC ne protégent pas contre cela parce que tous peuvent être modifiés ou régénérés par un adversaire malveillant et déterminé.

6) Des agents non autorisés peuvent se faire passer pour des entités FCIP valides et perturber le bon fonctionnement de la structure de canal Fibre.

7) Des attaques de déni de service peuvent être montées en injectant des demandes de connexion TCP et autres opérations consommatrices de ressources.

8) Un adversaire peut lancer diverses attaques contre le processus de découverte [17].

9) Un attaquant peut exploiter le mécanisme d'authentification de FSF du processus de formation de la liaison FCIP (voir au paragraphe 8.1.3). L'attaquant pourrait observer le contenu de la FSF envoyée sur une connexion initiale d'une liaison FCIP et utiliser le nom occasionnel observé, l'identifiant d'entité FC/FCIP de source, et d'autres contenus de la FSF pour former une liaison FCIP utilisant la propre connexion préalablement établie de l'attaquant, tout en remettant à zéro/bloquant la connexion observée. Bien que l'utilisation d'une temporisation pour la réception de la FSF réduise le risque de cette attaque, elle est possible. Voir au paragraphe 9.3.1 comment se protéger contre cette attaque spécifique.

L'architecture existante de sécurité IPsec et sa suite de protocoles [10] offre une protection contre ces menaces. Une entité FCIP DOIT mettre en œuvre les portions de la suite des protocoles IPsec comme décrit dans cette section.

9.2 Modèles de déploiement de fabrique FC et de réseau IP

Dans le contexte do l'activation d'un tunnel FCIP sûr entre des SAN FC, il est utile de noter les caractéristiques suivantes du réseau IP de déploiement :

1) Les entités FCIP partagent une relation d'homologue à homologue. Donc, l'administration des politiques de sécurité s'applique à toutes les entités FCIP d'une manière égale. Cela diffère d'une vraie relation client-serveur, où il y a une différence inhérente dans la façon dont les politiques de sécurité sont administrées.
2) L'administration de la politique ainsi que le déploiement et la configuration de la sécurité sont restreintes à l'ensemble des entités FCIP, fixant par là moins d'exigences à un mécanisme d'adaptation. Par exemple, la validation des accréditifs peut être relâchée jusqu'au point où le déploiement d'un ensemble de clés pré partagées est une technique viable.
3) Les connexions TCP et le réseau IP se terminent à l'entité FCIP. La granularité d'une mise en œuvre de sécurité est au niveau du point d'extrémité du tunnel FCIP (ou de l'entité FCIP) à la différence des autres applications où il y a une terminaison des connexions TCP au niveau usager. Les objets de niveau usager ne sont pas contrôlables ou visibles par les entités FCIP. Toute la sécurité de niveau usager qui se rapporte à FCIP est de la responsabilité des normes de canal Fibre et sort du domaine d'application de la présente spécification.
4) Lorsque une entité FCIP est déployée, ses adresses IP vont normalement être allouées de façon statique. Cependant, la prise en charge de l'allocation dynamique des adresses IP, comme décrit en [33], bien que normalement non exigée, ne peut pas être exclue.

9.3 Composants de la sécurité de FCIP

Les mises en œuvre conformes à la sécurité FCIP DOIVENT mettre en œuvre ESP et l'authentification cryptographique et l'intégrité des données fondées sur la suite de protocoles IPsec [10], ainsi que la confidentialité en utilisant les algorithmes et les transformations comme décrit dans la présente section. Aussi, les mises en œuvre de FCIP DOIVENT satisfaire aux exigences de gestion sûre de clés de la suite de protocoles IPsec.

9.3.1 Authentification et confidentialité IPsec ESP

Les entités FCIP DOIVENT mettre en œuvre IPsec ESP [12] en mode tunnel pour assurer l'intégrité des données et la confidentialité. Les entités FCIP PEUVENT mettre en œuvre IPsec ESP en mode transport, si les considérations de déploiement exigent l'utilisation du mode transport. Lorsque ESP est utilisé, l'authentification de l'origine des données par paquet, la protection de l'intégrité, et la protection contre la répétition DOIVENT être utilisées.

Si la confidentialité n'est pas activée mais que l'intégrité des données est activée, ESP avec le chiffrement NUL [15] DOIT être utilisé.

IPsec ESP pour l'authentification de message calcule un hachage cryptographique sur la charge utile qui est protégée. Alors que IPsec ESP exige que les mises en œuvre conformes prennent en charge certains algorithmes pour déduire ce hachage, les mises en œuvre de FCIP :

- DOIVENT mettre en œuvre HMAC avec SHA-1 [11]
- DEVRAIENT mettre en œuvre AES en mode MAC CBC avec les extensions XCBC [23]
- DES en mode CBC NE DEVRAIT PAS être utilisé à cause de ses faiblesses inhérentes.

Pour la confidentialité ESP, les entités FCIP :

- DOIVENT mettre en œuvre 3DES en mode CBC [16]
- DEVRAIENT mettre en œuvre AES en mode CTR [22]
- DOIVENT mettre en œuvre le chiffrement NUL [15].

9.3.2 Gestion de clé

Les entités FCIP DOIVENT prendre en charge IKE [14] pour l'authentification d'homologue, la négociation d'associations de sécurité (SA, *Security Association*), et la gestion de clés en utilisant le DOI d'IPsec [13]. La gestion de clé manuelle NE DEVRA PAS être utilisée pour établir une SA car cela ne fournit pas les éléments nécessaires pour les changements de clés (voir au paragraphe 9.3.3). Les mises en œuvre FCIP conformes DOIVENT prendre en charge l'authentification d'homologue en utilisant des clés pré partagées et PEUVENT prendre en charge l'authentification d'homologue en utilisant des certificats numériques. L'authentification d'homologue utilisant les méthodes de chiffrement à clé publique développées aux paragraphes 5.2 et 5.3 de IKE [14] NE DEVRAIT PAS être utilisée.

IKE Phase 1 établit un canal sûr, authentifié par un MAC pour les communications utilisées par IKE phase 2. Les mises en œuvre de FCIP DOIVENT prendre en charge le mode principal IKE et DEVRAIENT prendre en charge le mode agressif.

Les échanges IKE phase 1 DOIVENT explicitement porter les champs d'identification de charge utile (IDii et IDir). Les mises en œuvre conformes de FCIP DOIVENT utiliser les valeurs de type d'identification ID_IPV4_ADDR, ID_IPV6_ADDR (si la pile de protocoles 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, et 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 en [13], les champs Accès et Protocole dans la charge utile d'identification DOIVENT être réglés à zéro ou à l'accès UDP 500.

Les entités FCIP négocient les paramètres pour la SA durant IKE phase 2 en utilisant seulement le "mode rapide". Pour les entités FCIP engagées en "mode rapide" IKE, il n'est pas exigé de secret parfait de transmission (PFS, *Perfect Forward Secrecy*). Les mises en œuvre de FCIP DOIVENT utiliser les valeurs de type d'identification de ID_IPV4_ADDR ou de ID_IPV6_ADDR (sur la base de la version IP acceptée). D'autres valeurs de type d'identification NE DOIVENT PAS être utilisées.

Comme le nombre de SA de phase 2 peut être limité, des messages de suppression de phase 2 peuvent être envoyés pour les SA inactives. La réception d'un message de suppression de phase 2 NE DEVRAIT PAS être interprétée comme une raison pour supprimer une liaison FCIP ou une de ses connexions TCP. Lorsque il y a une nouvelle activité sur cette liaison inactive, une nouvelle SA de phase 2 DOIT être rétablie.

Pour une certaine paire d'entités FCIP, la même négociation IKE phase 1 peut être utilisée pour toutes les négociations de phase 2 ; c'est-à-dire que toutes les connexions TCP qui sont en faisceau dans la seule liaison FCIP peuvent partager les mêmes résultats de phase 1.

Des changements de clés répétés en utilisant le "mode rapide" sur le même secret partagé vont réduire les propriétés cryptographiques de ce secret au fil du temps. Pour surmonter cela, la phase 1 DEVRAIT être invoquée périodiquement pour créer un nouveau jeu de secrets IKE partagés et les paramètres de sécurité qui s'y rapportent.

L'établissement de IKE phase 1 exige la distribution de clés et d'entités FCIP suivante :
- elles DOIVENT prendre en charge les clés IKE pré partagées,
- elles PEUVENT prendre en charge l'authentification d'homologue fondée sur le certificat utilisant des signatures numériques,
- elles NE DEVRAIENT PAS utiliser l'authentification d'homologue utilisant les méthodes de chiffrement à clé publique exposées aux paragraphes 5.2 et 5.3 de [14].

Lorsque des clés pré partagées sont utilisées, le mode principal IKE n'est utilisable que lorsque les deux homologues d'une liaison FCIP utilisent des adresses IP allouées de façon statique. Lorsque est tentée la prise en charge de l'allocation dynamique des adresses IP en conjonction avec le mode principal, l'utilisation de clés pré partagées de groupe serait forcée, et l'utilisation de clés pré partagées de groupe en combinaison avec le mode principal n'est pas recommandée car elle expose l'environnement déployé à des attaques par interposition. Donc, si l'un ou l'autre homologue d'une liaison FCIP utilise des adresses allouées de façon dynamique, le mode agressif DEVRAIT être utilisé et le mode principal NE DEVRAIT PAS être utilisé.

Lorsque on utilise des signatures numériques, le mode principal IKE ou le mode agressif IKE peuvent être utilisés. Dans tous les cas, l'accès aux informations de secret mémorisé en local (clés pré partagées, ou clé privée pour signature numérique) DOIT être convenablement protégé, car la compromission d'informations secrètes rend nulles les propriétés de sécurité des protocoles IKE/IPsec. De tels mécanismes sortent du domaine d'application du présent document. La prise en charge des groupes Oakley IKE [27] n'est pas exigée.

Pour les besoins de l'établissement d'une liaison FCIP sûre, les deux entités FCIP participantes consultent une base de données de politique de sécurité (SPD, *Security Policy Database*). La SPD est décrite au paragraphe 4.4.1 de IPsec [10].

Les entités FCIP peuvent avoir plus d'une interface et adresse IP, et il est possible qu'une liaison FCIP contienne plusieurs connexions TCP dont les adresses IP de point d'extrémité FCIP sont différentes. Dans ce cas, une SA IKE phase 1 est établie pour chaque paire d'adresse IP de point d'extrémité FCIP. Au sein de IKE phase 1, les mises en œuvre FCIP doivent prendre en charge les charges utiles d'identité ID_IPV4_ADDR, ID_IPV6_ADDR (si la pile de protocoles accepte IPv6) et ID_FQDN. Si les adresses de point d'extrémité FCIP sont allouées de façon dynamique, il peut être avantageux d'utiliser ID_FQDN, et pour cette raison, la charge utile d'identité IP_FQDN DOIT être acceptée. Les autres charges utiles d'identité (ID_USER_FQDN, ID_DER_ASN1_GN, ID_KEY_ID) NE DEVRAIENT PAS être utilisées.

À la fin d'une négociation IKE réussie, les deux entités FCIP mémorisent les paramètres de la SA dans leur base de données de SA (SAD). La SAD est décrite au paragraphe 4.4.3 de IPsec [10]. La SAD contient l'ensemble des entrées actives de la SA, chaque entrée contenant le compteur de débordement de séquence, le compteur de numéro de séquence, la fenêtre anti répétition, et la durée de vie de la SA. Les entités FCIP DEVRONT employer une durée de vie de SA par défaut d'une heure, et une fenêtre anti répétition par défaut de 32 numéros de séquence.

Lorsque une connexion TCP est établie entre deux FCIP_DE, deux SA unidirectionnelles sont créées pour cette connexion et chaque SA est identifiée sous la forme d'un indice de paramètre de sécurité (SPI, *Security Parameter Index*). Une SA est associée au flux de trafic entrant et l'autre SA est associée au flux de trafic sortant. Les FCIP_DE à chaque extrémité de la connexion TCP DOIVENT tenir les SPI pour ses deux trames encapsulées FCIP entrante et sortante.

Les entités FCIP PEUVENT fournir une gestion administrative de l'utilisation de la confidentialité. Ces interfaces de gestion DEVRAIENT être fournies de façon sûre, afin d'empêcher un attaquant de subvertir le processus de sécurité en attaquant l'interface de gestion.

9.3.3 Questions de protection contre la répétition d'ESP et de changement de clés

Les entités FCIP DOIVENT mettre en œuvre la protection contre la répétition à l'égard du retour à zéro du numéro de séquence ESP, comme décrit dans [14]. De plus, sur la base de l'algorithme de chiffrement et du nombre de bits dans la taille du bloc de chiffrement, la validité de la clé peut être compromise. Dans les deux cas, la SA doit être rétablie.

Les entités FCIP DOIVENT utiliser les résultats de la négociation IKE phase 1 pour initier l'échange IKE hase 2 "mode rapide" et établir de nouvelles SA.

Pour permettre une transition en douceur des SA, il est RECOMMANDÉ que les deux entités FCIP rafraîchissent le SPI lorsque le compteur de numéros de séquence atteint 2^31 (c'est-à-dire, la moitié de l'espace des numéros de séquence). Il est aussi RECOMMANDÉ que le receveur opère avec plusieurs SPI pour la même connexion TCP pendant une période de 2^31 paquets de numéros de séquence avant de périmer un SPI.

Lorsque un nouveau SPI est créé pour la direction sortante, le côté envoyeur DEVRA commencer de l'utiliser pour toutes les nouvelles trames FCIP encapsulées. Les trames qui sont soit en vol, soit envoyées à cause des retransmissions TCP, etc., PEUVENT utiliser soit le nouveau SPI, soit celui qui est en cours de remplacement.

9.4 Fonctionnement de liaison FCIP sécurisée

9.4.1 Étapes de l'initialisation de liaison FCIP

Les mises en œuvre de FCIP peuvent permettre d'activer et désactiver les mécanismes de sécurité à la granularité d'une liaison FCIP. Si ils sont activés, les étapes d'initialisation de liaison FCIP suivantes DOIVENT être respectées.

Lorsque une liaison FCIP est initialisée, avant que toute connexion TCP FCIP soit établie, la SPD locale est consultée pour déterminer si IKE phase 1 a été achevé avec l'entité FCIP dans l'entité FCIP homologue, comme identifié par le nom mondial (WWN, *World Wide Name*)

Si la phase 1 est déjà achevée, IKE phase 2 se poursuit. Autrement, IKE phase 1 DOIT être achevé avant que IKE phase 2 puisse commencer. Les transactions de IKE phase 1 et phase 2 utilisent l'accès UDP 500. Si IKE phase 1 échoue, l'initialisation de la liaison FCIP se termine et elle notifie à l'entité FC les raisons de la terminaison. Autrement, l'initialisation de la liaison FCIP passe à l'initialisation de la connexion TCP.

Comme décrit au paragraphe 8.1, les entités FCIP échangent une FSF pour former une liaison FCIP. L'utilisation de la confidentialité ESP est une contre mesure efficace contre tous les risques perçus pour la sécurité de la FSF.

9.4.2 Associations de sécurité (SA) de connexion TCP

Chaque connexion TCP DOIT être protégée par une SA IKE phase 2. Le trafic provenant d'une ou plusieurs connexions TCP peut s'écouler au sein de chaque SA IPsec phase 2. Bien qu'il soit possible à une SA IKE phase 2 de protéger plusieurs connexions TCP, tous les paquets d'une connexion TCP sont protégés en utilisant seulement une SA IKE phase 2.

Si différents réglages de qualité de service sont appliqués aux connexions TCP, il est conseillé d'utiliser une SA IPsec différente pour ces connexions. Tenter d'appliquer une qualité de service différente aux connexions traitées par la même SA IPsec peut résulter en un changement de l'ordre, et tomber en dehors de la fenêtre de répétition. Pour les détails, voir [21].

Les mises en œuvre FCIP n'ont pas besoin de vérifier que les adresses IP et les numéros d'accès dans le paquet correspondent à une valeur par connexion mémorisée en local, laissant cette vérification à la couche IPsec.

Une mise en œuvre est libre d'effectuer plusieurs négociations IKE phase 2 et les mettre en antémémoire dans ses SPI locaux, bien que les entrées dans de telles antémémoires puissent être purgées par les réglages courants de durée de vie de SA.

9.4.3 Traitement des violations d'intégrité et de confidentialité des données

À réception d'un datagramme, lorsque le paquet ESP échoue à une vérification d'intégrité, le receveur DOIT abandonner le datagramme, ce qui va déclancher la retransmission TCP. Si de nombreux datagrammes sont ainsi abandonnés, une entité FCIP receveuse PEUT clore la connexion TCP et notifier à l'entité FC la raison de la clôture.

Une mise en œuvre DEVRAIT suivre les lignes directrices pour l'examen de tous les événements ESP selon la Section 7 de IPsec [10].

Les vérifications d'intégrité DOIVENT être effectuées si la confidentialité est activée.

10. Performances

10.1 Considérations de performances

Traditionnellement, les liaisons entre les composants de structure FC ont été caractérisés par une faible latence et un haut débit. L'objet de FCIP est de fournir des fonctionnalités équivalentes à ces liaisons en utilisant un réseau IP, où une faible latence et un haut débit ne sont pas aussi certains. Il s'ensuit que les entités FCIP et leurs contreparties d'entités FC seront probablement intéressées par une utilisation optimale du réseau IP.

Il existe de nombreuses options pour s'assurer d'un haut débit et d'une faible latence appropriées pour les distances impliquées dans le réseau IP. Par exemple, un réseau IP privé pourrait être construit pour le seul usage d'entités FCIP. Les options qui sont dans le domaine d'application de la présente spécification sont exposées ici.

Une option pour augmenter la probabilité que les flux de données FCIP vont subir une faible latence et un haut débit est celle des techniques de qualité de service IP exposées au paragraphe 10.2. Cette option peut avoir une certaine valeur lorsque elle est appliquée à une seule connexion TCP. Selon la sophistication de l'entité FC, d'autres valeurs peuvent être obtenues en ayant plusieurs connexions TCP avec des caractéristiques de QS différentes.

Il y a de nombreuses raisons pour qu'une entité FC puisse demander la création de plusieurs connexions TCP au sein d'un FCIP_LEP. Ces raisons incluent le désir de fournir des services différenciés pour différentes connexions de données TCP entre des FCIP_LEP, ou une préférence pour mettre séparément en file d'attente différents flux de trafic n'ayant pas d'exigences de livraison ordonnée communes.

Au moment de la création d'une nouvelle connexion TCP, l'entité FC DEVRA spécifier à l'entité FCIP les caractéristiques de QS (y compris mais non limitées au comportement IP par bond) à utiliser pour la durée de vie de cette connexion. Cela PEUT se faire en ayant :

a) un seul jeu de caractéristiques de QS pour toutes les connexions TCP ;
b) un jeu par défaut de caractéristiques de QS que l'entité FCIP applique en l'absence d'instructions différentes de la part de l'entité FC ; ou
c) un mécanisme sophistiqué pour échanger les informations d'exigence de QS entre entité FC et entité FCIP chaque fois qu'est créée une nouvelle connexion TCP.

Une fois établies, les caractéristiques de QS d'une connexion TCP NR DEVRONT PAS être changées, car la présente spécification ne fournit aucun mécanisme pour que l'entité FC contrôle de tels changements. Le mécanisme pour fournir

des caractéristiques de QS différentes dans FCIP est l'établissement de connexions TCP différentes et de leurs FCIP_DE associés.

Lorsque FCIP est utilisé avec un réseau qui a un produit (bande passante*délai) élevé, il est RECOMMANDÉ que les FCIP_LEP utilisent les mécanismes de TCP (adaptation de fenêtre et protection contre le retour à zéro du numéro de séquence) pour les gros réseaux longs (LFN, *Long Fat Network*) comme défini dans la RFC1323 [24].

10.2 Prise en charge de la qualité de service IP

De nombreuses méthodes pour fournir la QS ont été envisagées ou proposées. Cela inclut (mais ne se limite pas à) ce qui suit :

- commutation d'étiquette multi-protocoles (MPLS) -- RFC3031 [32]
- architecture de services différenciés (diffserv) -- RFC2474 [28], RFC2475 [29], RFC2597 [30], et RFC2598 [31] -- et d'autres formes de comportement par bond (PHB, *per-hop-behavior*)
- intégration de services, RFC1633 [25]
- IEEE 802.1p

L'objet de la présente spécification n'est pas de spécifier une forme particulière de QS IP, mais plutôt de ne spécifier que les questions qui doivent être réglées pour maximiser l'interopérabilité entre les équipements FCIP qui ont été fabriqués par des équipementiers différents.

Il est RECOMMANDÉ qu'une certaine forme de QS préférentielle soit utilisée pour que le trafic FCIP minimise la latence et l'abandon de paquet. Aucune forme particulière de QS n'est recommandée.

Si on met en œuvre un comportement de qualité de service IP par bond, il est RECOMMANDÉ qu'il interopère avec diffserv (voir la RFC 2474 [28], RFC 2475 [29], RFC 2597 [30], et RFC 2598 [31]).

Si aucune forme de QS préférentielle n'est mise en œuvre, le champ DSCP DEVRAIT être réglé à '000000' pour éviter les impacts négatifs sur d'autres composants et services de réseau qui pourraient être causés par un usage incontrôlé de valeurs différentes de zéro dans le champ DSCP.

11. Références

11.1 Références normatives

Les références de cette section étaient actuelles au moment de l'approbation de la présente spécification. Celle-ci est destinée à fonctionner avec les plus récentes versions des documents référencés et il est recommandé de rechercher les plus récentes versions des documents de référence.

[1] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", RFC2119, BCP 14, mars 1997.

[2] ANSI INCITS.342:2001, "Fibre Channel Backbone (FC-BB)", 12 décembre 2001.

[3] ANSI INCITS.372:2003, "Fibre Channel Backbone -2 (FC-BB-2)", 25 juillet 2003.

[4] ANSI INCITS.355:2001, "Fibre Channel Switch Fabric -2 (FC-SW-2)", 12 décembre 2001.

[5] ANSI INCITS.373:2003, "Fibre Channel Framing et Signaling (FC-FS)", 27 octobre 2003.

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

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

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

[9] D. Eastlake, 3rd et autres, "Recommandations d'aléa pour la sécurité", RFC1750, décembre 1994. *(Info., remplacée par la* RFC4086)

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

voir RFC4301)

[11] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", RFC2104, février 1997.

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

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

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

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

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

[17] E. Guttman et autres, "Protocole de localisation de service, version 2", RFC2608, juin 1999. (*MàJ par* RFC3224) *(P.S.)*

[18] S. Floyd et autres, "Extension à l'option d'accusé de réception sélectif (SACK) pour TCP", RFC2883, juillet 2000. *(P.S.)*

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

[20] D. Peterson, "Découverte de canal fibre sur des entités TCP/IP (FCIP) en utilisant le protocole de localisation de service version 2 (SLPv2)", RFC3822, juillet 2004. *(P.S., MàJ par* RFC7146*)*

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

[22] S. Frankel, R. Glenn, S. Kelly, "Algorithme de chiffrement AES-CBC et utilisation avec IPsec", RFC3602, septembre 2003. *(P.S.)*

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

11.2 Références pour information

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

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

[26] D. Mills, "Protocole simple de l'heure du réseau (SNTP) version 4 pour IPv4, IPv6 et OSI", RFC2030, octobre 1996. *(Obsolète, voir* RFC4330*)*

[27] H. Orman, "Protocole OAKLEY de détermination de clés", RFC2412, novembre 1998. *(Information)*

[28] K. Nichols, S. Blake, F. Baker et D. Black, "Définition du champ Services différenciés (DS) dans les en-têtes IPv4 et IPv6", RFC2474, décembre 1998. (*MàJ par* RFC3168, RFC3260) *(P.S.)*

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

[30] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, "Groupe PHB Transmission assurée", RFC2597, juin 1999. (*MàJ par* RFC3260) *(PS)*

[31] V. Jacobson, K. Nichols, K. Poduri, "PHB Transmission expédiée", RFC2598, juin 1999. (*Obsolète, voir* RFC3246) *(P.S.)*

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

[33] B. Patel et autres, "Protocole de configuration dynamique des hôtes (DHCPv4) Configuration du mode tunnel IPsec", RFC3456, janvier 2003. *(P.S.)*

[34] Kembel, R., "The Fibre Channel Consultant: A Comprehensive Introduction", Northwest Learning Associates, 1998.

12. Remerciements

Les développeurs de la présente spécification remercient M. Jim Nelson de son assistance sur les questions de relations FC-FS.

Les développeurs de la présente spécification expriment leur reconnaissance à M. Mallikarjun Chadalapaka et M. David Black pour leur très utile relecture détaillée.

Appendice A Guide de numérotation des bits et octets de canal fibre

Les normes de canal Fibre et de l'IETF utilisent toutes deux le même ordre de transmission des octets. Cependant, le numérotage des bit et des octets est différent.

Le numérotage des bits et des octets de canal Fibre peut être observé si l'en-tête de structure des données, montré à la Figure 11, est coupé et collé au dessus de la Figure 7, Figure 9, et Figure 17.

```
 |------------------------------Bit-------------------------------|
M|                                                                |
o|3 3 2 2 2 2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 1 1                     |
t|1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0|
```

Figure 11 : Structure des données de numérotation de bit et d'octet de canal fibre

La numérotation des bits de canal Fibre pour le champ pFlags peut être observée si l'en-tête de la structure de données, montré à la Figure 12, est coupé et collé au sommet de la Figure 8.

```
|---------------Bit-------------------|
|                                     |
| 31   30   29   28   27   26   25   24 |
```

Figure 12 : Numérotation des bits fanions de canal fibre

La numérotation des bits de canal Fibre pour le champ Fanion d'usage de connexion peut être observé si l'en-tête de structure de données, montré à la Figure 13, est coupé et collé au sommet de la Figure 10.

```
|------------------------------Bit-------------------------------|
|                                                                |
|   31       30       29       28       27       26       25       24  |
```

Figure 13 : Numérotation des bits des fanions d'usage de connexion de canal Fibre

Appendice B Considérations relatives à l'IANA

L'IANA a fait les allocations d'accès suivantes à FCIP :
- fcip-port 3225/tcp FCIP
- fcip-port 3225/udp FCIP

L'IANA a changé l'autorité de ces allocations d'accès pour faire référence à la présente RFC.

L'utilisation de UDP avec FCIP est prohibée bien que l'IANA y ait alloué un accès.

L'encapsulation de trame FC utilisée par la présente spécification emploie la valeur de Protocol# 1, comme décrit dans l'Appendice Considérations relatives à l'IANA de la spécification d'encapsulation de trame FC [19].

Appendice C Utilisation des adresses et identifiants par FCIP

Pour la prise en charge des traducteurs d'adresse réseau, FCIP n'utilise pas les adresses IP pour identifier les entités FCIP ou les FCIP_LEP. La seule utilisation des adresses IP pour identification survient lors de l'initialisation de nouvelles demandes de connexion TCP (voir au paragraphe 8.1.2.3) où l'adresse IP de destination de la demande de connexion TCP est utilisée pour répondre à la question "des demandes de connexion TCP précédentes ont elles été faites à la même entité FCIP de destination ?" La correction de cette assertion est vérifiée par l'envoi du nom mondial d'entité de structure FC de destination dans la trame spéciale FCIP (FSF) et que c'est la valeur envoyée par l'entité FCIP qui reçoit la demande de connexion TCP et la FSF (voir au paragraphe 8.1.3).

Pour les besoins du traitement des demandes de connexion TCP entrantes, l'entité FCIP de source est identifiée par les champs Nom mondial d'entité de structure FC de source et Identifiant d'entité FC/FCIP de source dans la FSF envoyée de la demande de connexion TCP ou au receveur de la connexion TCP comme les premiers octets qui suivent la demande de connexion TCP (voir aux paragraphes 8.1.2.3 et 8.1.3).

FC-BB-2 [3] donne les définitions de chacun des champs de FSF suivants :
- Nom mondial d'entité de structure FC de source,
- Identifiant d'entité FC/FCIP de source,
- Nom mondial d'entité de structure FC de destination.

Comme décrit au paragraphe 8.1.3, les entités FCIP distinguent leurs FCIP_LEP entre :
- les connexions résultant de demandes de connexion TCP initiées par l'entité FCIP, et
- les connexions résultant de demandes de connexion TCP reçues par l'entité FCIP.

Au sein de chacun de ces deux groupes, les informations suivantes sont utilisées pour identifier chaque FCIP_LEP :
- Nom mondial d'entité de structure FC de source,
- Identifiant d'entité FC/FCIP de source,
- Nom mondial d'entité de structure FC de destination.

Appendice D Exemple d'algorithme de récupération de synchronisation

Le contenu de cette annexe est pour information.

La synchronisation peut être récupérée comme spécifié au paragraphe 5.6.2.3. Un exemple d'algorithme pour chercher les octets livrés au portail receveur de trame encapsulée pour un en-tête de trame FCIP valide est fourni dans cette annexe.

Cette resynchronisation utilise le principe qu'un flux de données FCIP valide doit contenir au moins un en-tête valide tous les 2176 octets (longueur maximum d'une trame FC encapsulée). Bien que d'autres schémas de données contenant des en-têtes apparemment valides puissent être contenus dans le flux, la validité du CRC FC ou de la trame FCIP du schéma de données contenu dans le flux de données va toujours être soit interrompu par, soit resynchronisé avec, les en-têtes de trame FCIP valides.

Considérons le cas montré à la Figure 14. Une série de courtes trames FCIP, peut-être provenant d'une trace, sont incorporées dans de plus grandes trames FCIP, peut-être par suite d'un fichier de trace qui est transféré d'un disque sur un autre. Les en-têtes pour les trames FCIP courtes sont notées SFH et les en-têtes de longues trames FCIP sont marqués LFH.

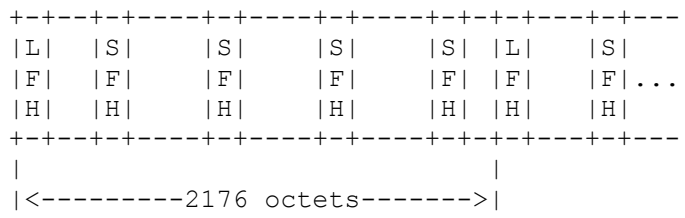


Figure 14 : Exemple de flux de données de resynchronisation

Une tentative de resynchronisation qui débute juste à droite d'un LFH va trouver plusieurs trames SFH FCIP avant de découvrir qu'elles ne représentent pas le flux transmis des trames FCIP. Cependant, dans plus ou moins 2176 octets, la tentative de resynchronisation va rencontrer un SFH dont la longueur ne correspond pas au prochain SFH parce que le LFH va tomber au milieu de la trame FCIP courte, poussant le prochain en-tête plus loin dans le flux d'octets.

Noter que l'algorithme de resynchronisation ne peut pas transmettre de trame FC prospective au portail émetteur de trame FC parce que, jusqu'à l'achèvement de l'établissement de la synchronisation, on n'est pas certain que ce qui ressemblait à une trame FCIP en soit réellement une. Par exemple, un SFH peut contenir de façon fortuite une longueur qui pointe exactement sur le début d'un LFH. Le LFH identifierait le début correct d'une trame FCIP transmise, mais cela ne garantit d'aucune façon que le SFH était aussi un en-tête correct de trame FCIP.

Il existe des flux de données qui ne peuvent pas être resynchronisés par cet algorithme. Si on rencontre un tel flux de données, l'algorithme cause la clôture de la connexion TCP.

La resynchronisation suppose que des procédures de sécurité et d'authentification en dehors de l'entité FCIP protègent le flux de données valide contre le remplacement par un flux de données intrus contenant des données FCIP valides.

Les étapes suivantes sont un exemple de la façon dont un FCIP_DE peut se resynchroniser avec le flux de données entrant au portail receveur de trame encapsulée.

1) Recherche de candidat et d'en-têtes forts :
   Le flux de données entrant au portail receveur de trame encapsulée est parcouru à la recherche de 12 octets à la suite contenant les valeurs requises pour :
   a) le champ Protocole,
   b) le champ Version,
   c) le complément à un du champ Protocole,
   d) le complément à un du champ Version,
   e) la réplique de l'encapsulation du mot 0 dans le mot 1, et
   f) le champ pFlags et son complément à un.

   Si un tel groupe de 12 octets est trouve, le FCIP_DE suppose qu'il a identifié les octets 0-2 d'un candidat en-tête d'encapsulation FCIP.

   Tous les octets jusque et y compris l'octet du candidat en-tête sont éliminés.

   Si aucun candidat en-tête n'a été trouvé après avoir cherché sur un nombre spécifié d'octets supérieur à un certain multiple de 2176 (longueur maximum de trame FCIP) la resynchronisation a échoué et la connexion TCP/IP est close.

   Le mot 3 du candidat en-tête contient les champs Longueur de trame et Fanions et leurs compléments à un. Si les champs sont cohérents avec leurs compléments à un, le candidat en-tête est considéré comme un candidat en-tête fort. Le champ Longueur de trame est utilisé pour déterminer où devrait être le prochain candidat en-tête fort dans le flux d'octets et le processus continue à l'étape 2).

2) Utiliser plusieurs candidats en-tête forts pour localiser un candidat en-tête vérifié :
   La Longueur de trame dans un candidat en-tête fort est utilisée pour sauter les octets entrants jusqu'à ce que soit atteinte la localisation attendue du prochain candidat en-tête fort. Les essais décrits à l'étape 1) sont ensuite appliqués pour voir si un autre candidat en-tête fort a pu être localisé.

   Tous les octets sautés et tous les octets dans tous les candidats en-tête forts traités sont éliminés.

   On continue de vérifier les candidats en-tête forts de cette façon pendant au moins 4352 octets (deux fois la longueur maximum d'une trame FCIP). Si à un moment, une vérification échoue, le traitement recommence à l'étape 1 et un compteur d'essais est incrémenté. Si le compteur d'essais excède 3 essais, la resynchronisation a échoué et la connexion TCP est close, et on notifie à l'entité FC la raison de la clôture.

   Après avoir vérifié les candidats en-tête pendant au moins 4352 octets, le prochain en-tête identifié est un candidat en-tête vérifié, et le traitement continue à l'étape 3).

Note : Si un candidat en-tête fort faisait partie du contenu de données d'une trame FCIP, la trame FCIP définie par ce candidat en-tête fort ou un suivant va finalement croiser un en-tête réel dans le flux de données. Par suite, il va soit identifier l'en-tête réel comme candidat en-tête fort, soit il va perdre à nouveau la synchronisation à cause des 28 octets supplémentaire de la longueur, retournant à l'étape 1, comme décrit ci-dessus.

3) Utiliser plusieurs candidats entête forts pour localiser un candidat en-tête vérifié :
   Les octets entrants sont inspectés et éliminés jusqu'à atteindre le prochain candidat en-tête vérifié. L'inspection des octets entrants inclut d'essayer les autres candidats en-tête en utilisant les critères décrits à l'étape 1. Chaque candidat en-tête vérifié est confronté aux essais énumérés au paragraphe 5.6.2.2 comme ce serait normalement le cas.

   Les candidats en-tête vérifiés continuent d'être localisés et vérifiés de cette façon pendant un minimum de 4352 octets (deux fois la longueur maximum d'une trame FCIP). Si tous les candidats en-tête vérifiés rencontres sont valides, le candidat en-tête vérifié en dernier est un en-tête valide. À ce point, le FCIP_DE arrête d'éliminer les octets et commence la désencapsulation FCIP normale, incluant pour la première fois depuis que la synchronisation a été perdue, la livraison des trames FC à travers le portail émetteur de trame FC conformément aux règles FCIP normales.

   Si des candidats en-tête vérifiés sont invalides mais satisfont à toutes les exigences d'un candidat en-tête fort, incrémenter le compteur d'essais et retourner à l'étape 2). Si des candidats en-tête vérifiés sont invalides et échouent à satisfaire aux essais de candidat en-tête fort, ou si l'inspection des octets entre les candidats en-tête vérifiés découvre des candidats en-têtes, incrémenter le compteur d'essais et retourner à l'étape 1. Si le compteur d'essais excède 4 essais, la resynchronisation a échoué et la connexion TCP/IP est close.

On trouvera à la Figure 15 un diagramme de flux pour cet algorithme.

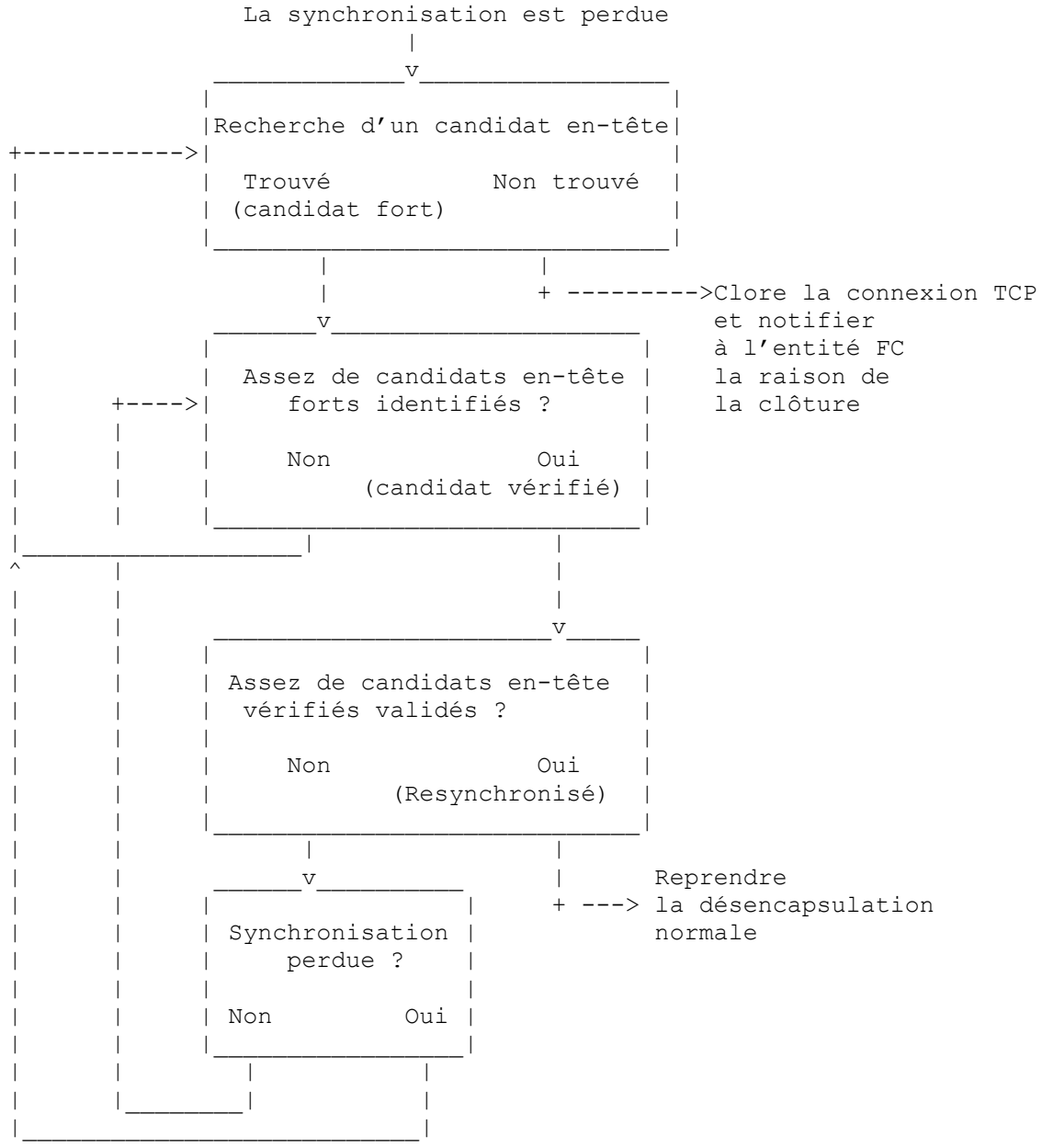


Figure 15 : Diagramme des flux d'un exemple simple de synchronisation

Appendice E Relations entre FCIP et IP sur FC (IPFC)

Le contenu de cette annexe est pour information.

IPFC (RFC 2625) décrit l'encapsulation de paquets IP dans les trames FC. Cela est destiné à faciliter la communication IP sur un réseau FC.

FCIP décrit l'encapsulation de trames FC dans des segments TCP, qui à leur tour sont encapsulés dans des paquets IP pour être transportés sur un réseau IP. Il ne tient pas compte du type de trame FC qui est encapsulée. Donc, la trame FC peut en fait contenir un paquet IP comme décrit dans la spécification IP sur FC (RFC 2625). Dans ce cas, le paquet de données va avoir :

- un en-tête de liaison de données
- un en-tête IP
- un en-tête TCP
- un en-tête FCIP
- un en-tête FC
- un en-tête IP

Note : Les deux en-têtes IP ne seront pas identiques l'un à l'autre. L'un aura des informations relevant de la destination finale, alors que l'autre aura des informations relevant de l'entité FCIP.

Les deux documents mettent l'accent sur des objectifs différents. Comme mentionné ci-dessus, une mise en œuvre de FCIP va conduire à l'encapsulation d'IP au sein d'IP. Bien que peut-être inefficace, cela ne devrait pas conduire à des problèmes avec la communication IP. Mais attention : si un appareil de canal Fibre encapsule des paquets IP dans une trame FC (par exemple, un appareil IPFC) et si cet appareil communique avec un appareil qui fonctionne avec IP sur un support non FC, un second appareil IPFC peut avoir besoin d'agir comme passerelle entre les deux réseaux. Ce scénario n'est pas spécifiquement traité par FCIP.

Il n'y a rien dans l'une et l'autre spécifications pour empêcher qu'un seul appareil mette en œuvre FCIP et IP sur FC (IPFC), mais ceci est spécifique de la mise en œuvre, et sort du domaine d'application du présent document.

Appendice F Format de trame FC

Note : Toutes les utilisations des mots "caractère" ou "caractères" dans cette section se réfèrent au codage de liaison 8bit/10bit par lequel chaque "caractère" de 8 bits au sein d'une trame de liaison est codé comme un "caractère" de 10 bits pour la transmission sur la liaison. Ces mots ne se réfèrent pas à ASCII, Unicode, ou toute autre forme de caractères de texte, bien que les octets provenant de tels caractères se produisent comme des "caractères" de 8 bits pour ce codage. Cet usage est fait ici pour la cohérence avec les normes ANSI T11 qui spécifient le canal Fibre.

Le contenu de cette annexe est pour information.

Toutes les trames FC ont un format standard (voir FC-FS [5]) tout comme les protocoles 802.x des LAN. Cependant, la taille exacte de chaque trame FC varie selon la taille des champs variables. La taille des champs variables va de 0 à 2112 octets comme le montre le format de trame FC de la Figure 16, ce qui résulte en la taille minimum de trame FC de 36 octets et la taille maximum de trame FC de 2148 octets. Les longueurs de trame FC valide sont toujours un multiple de quatre octets.

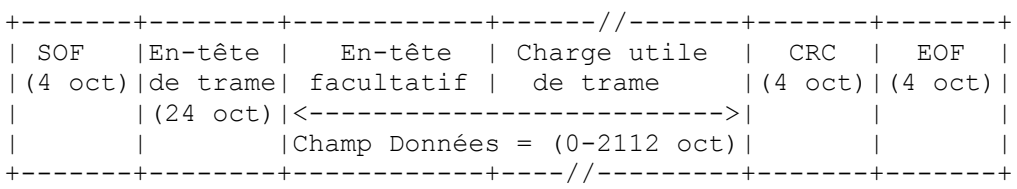


Figure 16 : Format de trame FC

Délimiteurs SOF et EOF

Sur une liaison FC, début de trame (SOF, *Start-of-Frame*) et fin de trame (EOF, *End-Of-Frame*) sont appelés des ensembles ordonnés et sont envoyés comme des mots particuliers construits à partir du caractère virgule 8B/10B (K28.5) suivi par trois caractères de données 8B/10B supplémentaires les rendant identifiables de façon univoque dans le flux de données.

Sur une liaison FC, le délimiteur SOF sert à identifier le début d'une trame FC et prépare le receveur à la réception de

trame FC. Le SOF contient des informations sur la classe de service de la trame FC, sa position au sein d'une séquence, et dans certains cas, sur l'état de la connexion.

Le délimiteur EOF identifie la fin de la trame FC et la trame FC finale d'une séquence. De plus, il sert à forcer l'anéantissement des éventuelles disparités. Le EOF est utilisé pour terminer la connexion dans les classes de service en mode connexion.

Un délimiteur EOF particulier appelé EOFa (*End Of Frame - Abort*) est utilisé pour terminer une trame FC partielle résultant d'un disfonctionnement dans une liaison durant la transmission. Comme une entité FCIP fonctionne comme une liaison de transmission par rapport au reste de la structure FC, les FCIP_DE peuvent utiliser EOFa dans leurs procédures de récupération d'erreur.

Il est donc important de préserver les informations portées par les délimiteurs à travers les réseaux fondés sur IP, afin que l'entité FCIP receveuse puisse reconstruire correctement la trame FC dans son format de SOF et EOF d'origine avant de le transmettre à sa destination FC ultime sur la liaison FC.

Lorsque une trame FC est encapsulée et est envoyée sur une interface en mode octet, les délimiteurs SOF et EOF sont représentés comme des séquences de quatre octets consécutifs, qui portent les informations d'équivalent de classe de service et de terminaison de trame FC comme ensembles ordonnés FC.

La représentation de SOF et EOF dans une trame FC d'encapsulation est décrite dans "Encapsulation de trame FC" [19].

En-tête de trame
L'en-tête de trame FC est transparent pour l'entité FCIP. L'en-tête de trame FC fait 24 octets et a plusieurs champs associés à l'identification et au contrôle de la charge utile. Les normes FC actuelles permettent jusqu'à trois champs d'en-tête facultatifs [5] :
- En-tête_réseau (16 octets)
- En-tête_d'association (32 octets)
- En-tête_d'appareil (jusqu'à 64 octets).

Charge utile de trame
La charge utile de trame FC est transparente pour l'entité FCIP. Une charge utile de niveau application FC est appelée une unité d'information au niveau FC-4. Ceci est transposé dans la charge utile de trame FC de la trame FC. Une grande unité d'information est segmentée en utilisant une structure consistant en séquences FC. Normalement, une séquence consiste en plus d'une trame FC. FCIP ne conserve aucune information d'état concernant les relations des trames FC au sein d'une séquence FC.

CRC (contrôle de redondance cyclique)
Le CRC FC fait quatre octets et utilise le même polynôme de 32 bits que dans FDDI et il est spécifié dans ANSI X3.139 "Interface de données réparties sur fibre". Cette valeur de CRC est calculée sur l'en-tête FC entier et la charge utile FC ; elle n'inclut pas les délimiteurs SOF et EOF.

Note : Lorsque les trames FC sont encapsulées dans des trames FCIP, le CRC de la trame FC n'est pas touché par l'entité FCIP.

Appendice G Format d'encapsulation de FC

Cette annexe contient une reproduction du "Format d'encapsulation FC" [19] car il s'applique aux trames FCIP qui encapsulent des trames FC. Les informations de cette annexe ne sont pas destinées à représenter la trame spéciale FCIP (FSF) qui est décrite à la Section 7.

Les informations de cette annexe étaient correctes au moment de l'approbation de la présente spécification. Les informations de cette annexe sont seulement pour information.

Si il existe des différences entre les informations données ici et la spécification de format d'encapsulation FC [19], c'est cette dernière qui a la préséance.

Si il existe des différences entre les informations données ici et le contenu du paragraphe 5.6.1, c'est le contenu du paragraphe 5.6.1 qui a la préséance.

La Figure 17 applique les exigences du paragraphe 5.6.1 et du format de trame d'encapsulation FC qui résultent en un

résumé du format de trame FC. Lorsque FCIP exige des valeurs spécifiques, ces valeurs sont données en hexadécimal entre parenthèses. Les exigences détaillées pour l'utilisation par FCIP du format d'encapsulation FC sont au paragraphe 5.6.1.

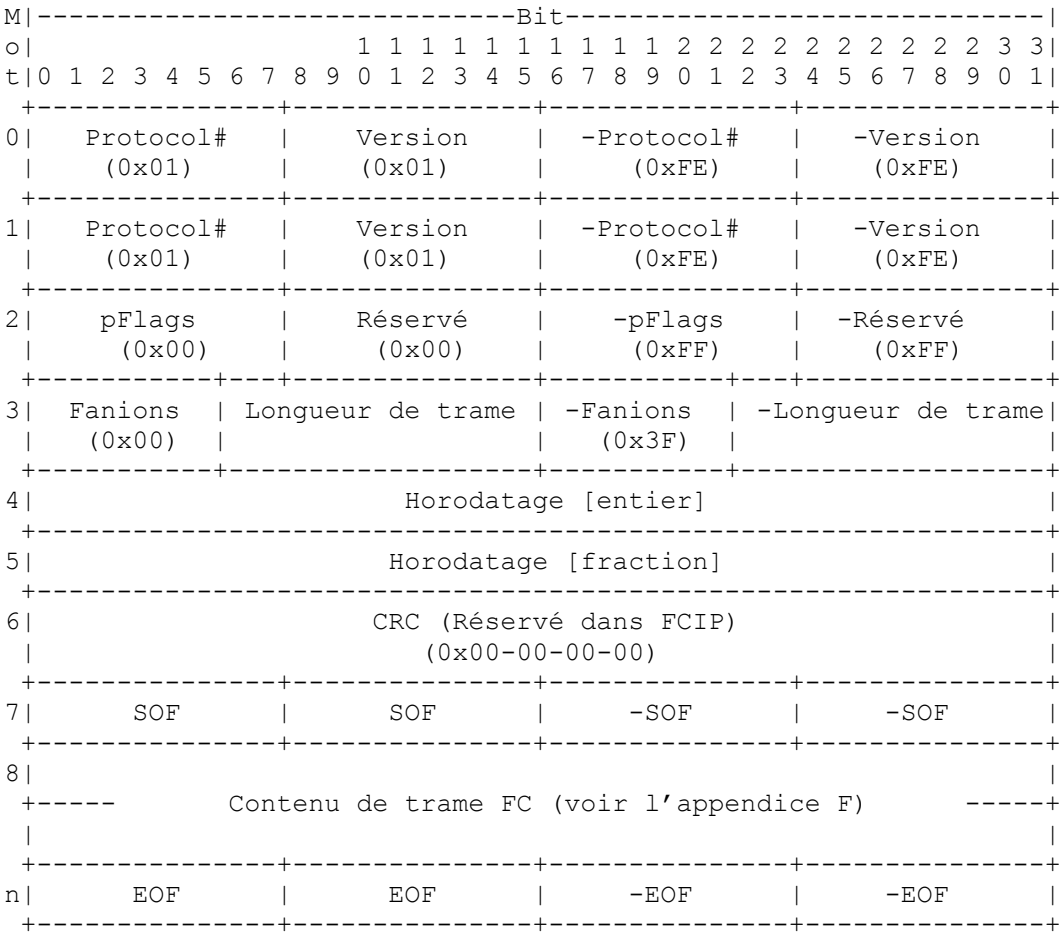


Figure 17 : Format de trame FCIP

Les noms des champs sont généralement descriptifs de leur contenu et on se reportera à la spécification du format d'encapsulation FC [19] pour les détails. Les noms de champs précédés d'un signe moins sont les valeurs de complément à un du champ désigné.

Note : La Figure 17 ne représente pas la FSF qui est décrit à la Section 7.

Appendice H – Exigences de FCIP pour les entités FC

Le contenu de cette annexe est pour information pour FCIP mais peut être considéré comme normatif sur FC-BB-2.

Les capacités exigées par FCIP d'une entité FC incluent que :

1) l'entité FC doit livrer les trames FC au moteur de données FCIP correct (au point d'extrémité de liaison FCIP correct) ;
2) chaque trame FC livrée à un FCIP_DE doit être accompagnée d'une valeur horaire synchronisée avec l'horloge tenue par l'entité FC à l'autre extrémité de la liaison FCIP (voir la Section 6). Si une valeur horaire synchronisée n'est pas disponible, une valeur de zéro doit accompagner la trame FC ;
3) lorsque des trames FC sortent de moteurs de données FCIP via le portail émetteur de trame FC, l'entité FC devrait les transmettre à la structure FC. Cependant, avant de transmettre une trame FC, l'entité FC doit calculer le temps de transit de bout en bout pour la trame FC en utilisant la valeur horaire fournie par le FCIP_DE (tirée de l'en-tête FCIP) et une valeur horaire synchronisée (voir la Section 6). Si le temps de transit de bout en bout excède les exigences de la structure FC, l'entité FC est responsable de l'élimination de la trame FC ;
4) la seule garantie d'ordre de livraison fournie par FCIP est la livraison correctement ordonnée des trames FC entre une paire de moteurs de données FCIP. FCIP s'attend à ce que l'entité FC mette en œuvre toutes les autres exigences d'ordre de livraison de trame ;
5) lorsque est reçue une demande de connexion TCP et que cette demande ajouterait une nouvelle connexion TCP à un FCIP_LEP existant, l'entité FC doit authentifier la source de la demande de connexion TCP avant que soit permise

l'utilisation de la nouvelle connexion TCP ;

6) l'entité FC peut participer à la détermination des connexions TCP permises, des paramètres de connexion TCP, de l'usage de la qualité de service, et de l'usage de sécurité en modifiant les interactions avec l'entité FCIP qui sont modélisées comme une base de données "partagée" au paragraphe 8.1.1 ;
7) l'entité FC peut exiger que l'entité FCIP effectue des demandes de clôture TCP ;
8) l'entité FC peut récupérer des défaillances de connexion ;
9) l'entité FC doit récupérer des événements que l'entité FCIP ne peut pas traiter, tels que :
   a) perte de synchronisation avec les en-têtes de trame FCIP à partir du portail receveur de trame encapsulée exigeant le rétablissement de la connexion TCP ; et
   b) récupération des trames FCIP qui sont éliminées par suite de problèmes de synchronisation (voir aux paragraphes 5.6.2.2 et 5.6.2.3) ;
10) l'entité FC doit travailler en coopération avec l'entité FCIP pour gérer la problèmes de contrôle de flux dans le réseau IP ou dans la structure FC ;
11) l'entité FC peut vérifier les échecs de connexions TCP.

Noter que les normes de canal Fibre doivent être consultées pour une compréhension en profondeur des exigences qui portent sur une entité FC.

Le Tableau 2 montre les interactions explicites entre l'entité FCIP et l'entité FC.

Section de référence	**Condition**	**Information/paramètre passé et direction**	
		Entité FCIP --->	**<--- Entité FC**
5.6 Moteur de données FCIP	Trame FC prête pour transfert IP		Fournit la trame et l'horodatage FC au portail receveur de trame FC
	Trame FCIP reçue du réseau IP	Fournit la trame et l'horodatage FC au portail émetteur de trame FC	
5.6.2.2 Erreurs des en-têtes FCIP et élimination des trames FCIP	FCIP_DE élimine les octets livrés par le portail receveur de trame encapsulée	Informe l'entité FC que des octets ont été éliminés avec la cause.	
5.6.2.3 Échecs de synchronisation	L'entité FCIP ferme la connexion TCP sur échec de synchronisation.	Informe l'entité FC que la connexion TCP a été close et la raison de la clôture.	
8.1.2.3 Établissement de connexion suivant une demande de connexion TCP réussie	La réception de l'écho de FSF prend trop longtemps or le contenu de la FSF a changé.	Informe l'entité FC que la connexion TCP a été close et la raison de la clôture.	
8.1.2.1 Création non dynamique de nouvelles connexions TCP	Création de nouvelles connexions TCP sur la base des informations de la base de données "partagée"	Informe l'entité FC de nouveau ou existant FCIP_LEP et nouveau FCIP_DE avec le WWN d'entité de structure FC de destination, fanions d'usage de connexion, code d'usage de connexion et nom occasionnel de connexion	
8.1.2.2 Création dynamique d'une nouvelle connexion TCP	Création d'une nouvelle connexion TCP sur la base d'une annonce de service SLP et des informations de la base de données "partagées"	Informe l'entité FC de nouveau ou existant FCIP_LEP et nouveau FCIP_DE avec le WWN d'entité de structure FC de destination, fanions d'usage de connexion, code d'usage de connexion et nom occasionnel de connexion	
8.1.3 Traitement d'une demande de connexion TCP entrante	Création d'une nouvelle connexion TCP sur la base d'une demande de connexion TCP entrante et des informations de la base de données "partagées"	Informe l'entité FC de nouveau ou existant FCIP_LEP et nouveau FCIP_DE avec le WWN d'entité de structure FC de source, l'identifiant d'entité FC/FCIP de source, fanions d'usage de connexion, code d'usage de connexion et nom occasionnel de connexion	

8.1.3 Traitement de demandes de connexion TCP entrantes	Une demande de connexion TCP veut ajouter une nouvelle connexion TCP à un FCIP_LEP existant	Demande à l'entité FC d'authentifier la source de la demande de connexion TCP	Réponse Oui ou Non sur le point de savoir si la source de la demande de connexion TCP peut être authentifiée
8.1.3 Traitement de demandes de connexion TCP entrantes	La réception de la FSF prend trop longtemps ou duplique une valeur de nom occasionnel de connexion	Informe l'entité FC que la connexion TCP a été close et raison de la clôture	
8.2 Clôture des connexions TCP	L'entité FC détermine qu'une connexion TCP doit être close	Accusé de réception de la clôture de la connexion TCP	Identification du FCIP_DE dont la connexion TCP doit être close.
8.4 Considérations sur la connexion TCP	Découverte que la connexité TCP a été perdue	Informe l'entité FC que la connexion TCP a été close et raison de la clôture	
9.4.1 Étapes d'initialisation de la liaison FCIP	IKE phase 1 a échoué, résultant en la terminaison de l'initialisation de la liaison	Informe l'entité FC que la connexion TCP ne peut être ouverte et raison de l'échec	
9.4.3 Traitement des violations d'intégrité et de confidentialité des données	Détection d'un nombre excessif de datagrammes abandonnés et clôture de la connexion TCP	Informe l'entité FC que la connexion TCP a été close et raison de la clôture	
RFC 3723 Traitement des discordances de paramètres de SA	Connexion TCP close à cause d'un problème de discordance des paramètres de SA	Informe l'entité FC que la connexion TCP a été close et raison de la clôture	
WWN *(World Wide Name)* = Nom mondial			

Tableau 2 : Interactions de la paire d'entités FC/FCIP

Remerciements aux éditeurs et contributeurs

Durant le développement de la présente spécification, Murali Rajagopal, Elizabeth Rodriguez, Vi Chau, et Ralph Weber se sont succédé comme éditeur. Raj Bhagwat a contribué substantiellement aux concepts FCIP de base initiaux. Venkat Rangan a contribué à la section Sécurité et continue de coordonner les questions de sécurité dans le groupe de travail IPS et à l'IETF. Andy Helland a contribué à une substantielle révision de la section Performances, l'alignant sur les concepts de QS de TCP/IP. Dave Peterson a contribué à la section de découverte dynamique et à l'édition de la RFC3822. Anil Rijhsinghani a contribué aux matériaux qui se rapportent à la MIB FCIP et à l'édition du document de MIB FCIP. Bob Snively a contribué aux matériaux de détection et récupération d'erreur incluant le gros de l'annexe sur l'exemple de récupération de synchronisation. Lawrence J. Lamers a contribué à de nombreuses idées centrées sur la compatibilité de FCIP avec les appareils B_Port. Milan Merhar a contribué à plusieurs des modifications conceptuelles de FCIP nécessaires pour la prise en charger des NAT. Don Fraser a contribué au matériel se rapportant à la détection et au rapport de défaillance de liaison. Bill Krieg a contribué à la restructuration des paragraphes sur l'établissement de la connexion TCP qui les rendent plus cohérents quand à leur déroulement dans le temps, et plus lisibles.

Plusieurs dirigeants du comité T11 ont soutenu cet effort et ont conseillé les éditeurs de la présente spécification en ce qui concerne la coordination avec les documents et projets du T11. Ce sont Jim Nelson (tramage et signalisation), Neil Wanamaker (tramage et signalisation), Craig Carlson (services génériques), Ken Hirata (commutation), Murali Rajagopal (cœur de réseau), Steve Wilson (commutation), et Michael O'Donnell (protocoles de sécurité).

Adresse des éditeurs et contributeurs

Neil Wanamaker
Akara
10624 Icarus Court
Austin, TX 78726
USA
téléphone : +1 512 257 7633
mél : nwanamaker@akara.com

Ralph Weber
ENDL Texas, representing Brocade
Suite 102 PMB 178
18484 Preston Road
Dallas, TX 75252
téléphone : +1 214 912 1373
mél : roweber@ieee.org

Elizabeth G. Rodriguez
Dot Hill Systems Corp.
6305 El Camino Real
Carlsbad, CA 92009
USA
téléphone : +1 760 431 4435
mél : elizabeth.rodriguez@dothill.com

Steve Wilson
Brocade Comm. Systems, Inc.
1745 Technology Drive

Bob Snively
Brocade Comm. Systems, Inc.
1745 Technology Drive

David Peterson
Cisco Systems - SRBU
6450 Wedgwood Road

San Jose, CA. 95110
USA
téléphone : +1 408 333 8128
mél : swilson@brocade.com

San Jose, CA 95110
USA
téléphone : +1 408 303 8135
mél :: rsnively@brocade.com

Maple Grove, MN 55311
USA
téléphone : +1 763 398 1007
mél : dap@cisco.com

Donald R. Fraser
Hewlett-Packard
301 Rockrimmon Blvd., Bldg. 5
Colorado Springs, CO 80919
USA
téléphone : +1 719 548 3272
mél : Don.Fraser@HP.com

R. Andy Helland
LightSand Communications, Inc.
375 Los Coches Street
Milpitas, CA 95035
USA
téléphone : +1 408 404 3119
mél : andyh@lightsand.com

Raj Bhagwat
LightSand Communications, Inc.
24411 Ridge Route Dr.
Suite 135
Laguna Hills, CA 92653
téléphone : +1 949 837 1733 x104
mél : rajb@lightsand.com

Bill Krieg
Lucent Technologies
200 Lucent Lane
Cary, NC 27511
USA
téléphone : +1 919 463 4020
mél : bkrieg@lucent.com

Michael E. O'Donnell
McDATA Corporation
310 Interlocken Parkway
Broomfield, CO 80021
USA
téléphone : +1 303 460 4142
mél : modonnell@mcdata.com

Anil Rijhsinghani
McDATA Corporation
310 Interlocken Parkway
Broomfield, CO 80021
USA
téléphone : +1 508 870 6593
mél : anil.rijhsinghani@mcdata.com

Milan J. Merhar
43 Nagog Park
Pirus Networks
Acton, MA 01720
USA
téléphone : +1 978 206 9124
mél : Milan@pirus.com

Craig W. Carlson
QLogic Corporation
6321 Bury Drive
Eden Prairie, MN 55346
USA
téléphone : +1 952 932 4064
mél : craig.carlson@qlogic.com

Venkat Rangan
Rhapsody Networks Inc.
3450 W. Warren Ave.
Fremont, CA 94538
USA
téléphone : +1 510 743 3018
mél : venkat@rhapsodynetworks.com

Lawrence J. Lamers
SAN Valley Systems, Inc.
6320 San Ignacio Ave.
San Jose, CA 95119-1209
USA
téléphone : +1 408 234 0071
mél : ljlamers@ieee.org

Murali Rajagopal
Broadcom Corporation
16215 Alton Parkway
Irvine,CA 92619
USA
téléphone : +1 949 450 8700
mél : muralir@broadcom.com

Ken Hirata
Vixel Corporation
15245 Alton Parkway, Suite 100
Irvine, CA 92618
USA
téléphone : +1 949 788 6368
mél : ken.hirata@vixel.com

Vi Chau
mél : vchau1@cox.net

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 assuré par la Internet Society.