Groupe de travail Réseau
Request for Comments : 5109
RFC rendues obsolètes : 2733, 3009
Catégorie : En cours de normalisation

A. Li, éditeur
décembre 2007

Traduction Claude Brière de L'Isle

Format de charge utile RTP pour la correction d'erreur directe générique

Statut du présent mémoire

Le présent document spécifie un protocole 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 "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document spécifie un format de charge utile pour la correction, d'erreur directe (FEC, *Forward Error Correction*) générique pour les données de support encapsulées dans RTP. Il se fonde sur l'opération OU exclusif (parité). Le format de charge utile décrit dans le présent document permet aux systèmes d'extrémité d'appliquer une protection en utilisant divers niveaux et longueurs de protection, en plus de l'utilisation de diverses tailles de groupe de protection pour s'adapter aux différentes caractéristiques de support et de canal. Il permet une récupération complète des paquets protégés ou une récupération partielle des parties critiques de la charge utile selon l'état des pertes du paquet. Ce schéma est complètement compatible avec les hôtes qui n'ont pas la capacité de FEC, de façon que dans un groupe de diffusion les receveurs qui ne mettent pas en œuvre la FEC puissent continuer de travailler en ignorant simplement les données de protection. La présente spécification rend obsolètes les RFC 2733 et 3009. La FEC spécifiée dans le présent document n'est pas rétrocompatible avec celle des RFC 2733 et 3009.

Table des matières

1. Introduction

La nature des applications en temps réel implique qu'elles ont généralement des exigences de délai plus strictes que les transmissions de données normales. Il en résulte que la retransmission des paquets perdus n'est généralement pas une option valide pour de telles applications. Dans ces cas, une meilleure méthode pour tenter de récupérer les informations des paquets perdus est la correction d'erreur directe (FEC, *Forward Error Correction*). La FEC est une des principales méthodes utilisées pour se protéger contre la perte de paquet sur les réseaux à commutation de paquets [9, 10]. En particulier, l'utilisation des codes de correction d'erreur traditionnels, tels que les codes de parité, de Reed-Solomon, et de Hamming, ont eu de nombreuses applications. Pour appliquer ces mécanismes, le soutien d'un protocole est exigé. Les RFC 2733 [9] et RFC 3009 [11] définissaient un de ces protocoles de FEC. Cependant, dans ces deux RFC quelques champs (les champs P, X, et CC) de l'en-tête RTP sont spécifiés d'une façon qui n'est pas cohérente avec celle dont ils sont conçus dans RTP [1]. Cela empêche la vérification de la validité de façon indépendante de la charge utile des paquets RTP.

Le présent document étend la FEC définie dans la RFC 2733 et la RFC 3009 pour inclure une protection d'erreur non égale sur les données de la charge utile. Il spécifie un algorithme général avec les deux RFC précédentes comme cas particulier. La présente spécification répare aussi les incohérences sus-mentionnées des RFC 2733 et RFC 3009, et les rend obsolètes. Prière de noter que la charge utile spécifiée dans le présent document n'est pas rétro-compatible avec la RFC 2733 et la RFC 3009. Parce que la charge utile spécifiée dans ce document est signalée par des MIME différents de ceux de la RFC 3009, il n'y a pas de problème d'erreur d'identification des différentes versions de parité de FEC dans l'échange de capacité. Pour les FEC de parité spécifiées ici et dans les RFC 2733 et RFC 3009, les données de charge utile sont inchangées et des données de FEC additionnelles sont envoyées avec elles pour protéger les données de charge utile. Et donc, la communication des données de charge utile va s'écouler sans problème entre les hôtes de version FEC de parité différente et les hôtes qui ne mettent pas en œuvre la FEC de parité. Les receveurs avec une FEC incompatible avec celle de l'hôte d'envoi ne seront pas capables de bénéficier des données de FEC supplémentaires, aussi est il recommandé que les hôtes existants qui mettent en œuvre les RFC 2733 et 3009 se mettent à jour dès que possible pour suivre la présente spécification.

Le présent document définit un format de charge utile pour RTP [1] qui permet la correction d'erreur directe générique de support en temps réel. Dans ce contexte, générique signife que le protocole FEC est (1) indépendant de la nature du support à protéger, soit-il audio, vidéo, ou autre ; (2) assez souple pour supporter une grande variété de configurations de FEC ; (3) conçu pour être adaptable, de sorte que la technique de FEC puisse être facilement modifiée sans signalisation hors bande ; et (4) tolérant pour un certain nombre de mécanismes de transport de paquet FEC différents.
De plus, dans de nombreux scénarios, la bande passante des connexions du réseau est une ressource très limitée. D'un autre côté, la plupart des schémas traditionnels de FEC ne sont pas conçus pour une utilisation optimale des ressources limitées de bande passante. Une amélioration souvent utilisée est la protection d'erreur inégale qui fournit les différents niveaux de protection pour les différentes parties du flux de données, dont l'importance est variable. Les schémas de protection d'erreur inégale peuvent habituellemnt faire une utilisation plus efficace de la bande passante pour fournir une meilleure protection globale des flux de données contre la perte. Un soutien du protocole approprié est essentiel pour réaliser les mécanismes de protection d'erreur inégale. L'application de la plupart des schémas de protection d'erreur inégale exige d'avoir connaissance de l'importance des différentes parties du flux des données. Pour cette raison, la plupart de ces schémas sont conçus pour un type de support particulier conformément à la structure du support protégé, et par conséquent, ne sont pas génériques.

Dans le présent document, l'algorithme et le protocole de FEC sont définis pour la correction d'erreur directe générique pour un support en temps réel. L'algorithme particulier défini ici est appelé protection de niveau non pair (ULP, *Uneven Level Protection*). Les données de charge utile sont protégées par un ou plusieurs niveaux de protection. Les niveaux de protection inférieurs peuvent fournir une meilleure protection en utilisant de plus petites tailles de groupes (par rapport aux niveaux de protection plus élevés) pour générer le paquet de FEC. Comme nous le montrerons plus loin, les applications audio/vidéo vont généralement bénéficier des schémas de protection d'erreur inégale qui donnent plus de protection au début de chaque paquet tel que ULP. Les données qui sont plus proches du début du paquet sont en général plus importantes et tendent à porter plus d'informations que les données qui se trouvent plus loin derrière dans le paquet.

Il est bien connu que dans beaucoup de flux multimédia la partie de données la plus importante est toujours au début du paquet de données. C'est une pratique courante de la conception du codec dans la mesure où le début du paquet est plus proche du marqueur de resynchronisation de l'en-tête et donc sera plus vraisemblablement décodé correctement. De plus, presque tous les formats de supports ont les en-têtes de trame au début du paquet, ce qui est la partie la plus vitale du paquet.

Pour les flux vidéo, la plupart des formats modernes ont des modes de partition des données facultatifs pour améliorer la résilience à l'erreur, dans lesquels les données d'en-tête de macrobloc vidéo et les données du coefficient de transformation en cosinus discret (DCT, *Discrete Cosine Transform*) sont séparés dans leurs partitions individuelles. Par exemple, dans la Recommandation UIT-T H.263 version 3, il y a la syntaxe de partage des données facultatives de l'Annexe V. Dans le profil visuel simple de MPEG-4, il y a le mode de partage des données facultatives. Lorsque ces modes sont activés, les partitions de l'en-tête de macrobloc (MB) vidéo et du vecteur de mouvement (qui sont très importants pour la qualité de la reconstruction vidéo) sont transmises dans la ou les partitions au début du paquet vidéo alors que les partitions de coefficient DCT résiduelles (qui sont moins importantes) sont transmises dans la partition proche de la fin du paquet. Parce que les données sont rangées en ordre d'importance décroissante, il serait bénéfique de fournir plus de protection au début du paquet dans la transmission.

Pour les flux audios, les flux binaires générés par de nombreux nouveaux codecs audio contiennent aussi des données de classes d'importances différentes. Ces différentes classes sont ensuite transmises en ordre d'importance décroissante. Appliquer plus de protection au début du paquet serait aussi bénéfique dans ce cas. Même pour les flux audios de signifcation uniforme, des techniques diverses de décalage temporel et d'étirement peuvent être appliquées pour récupérer partiellement des paquets de données audio.

Les applications audio/vidéo vont généralement bénéficier des algorithmes de FEC spécifiés dans ce document. Avec l'ULP, l'efficacité de la protection de la charge utile du support peut encore être améliorée. Le présent document spécifie le protocole et l'algorithme d'application de la FEC générique aux charges utiles de supports RTP.

2. Terminologie

Les termes suivants sont utilisés tout au long du présent document :

Charge utile du support : Données d'utilisateur brutes, non protégées qui sont transmises de l'envoyeur. La charge utile du support est placée dans un paquet RTP.

En-tête de support : L'en-tête RTP pour le paquet contenant la charge utile du support.

Paquet de support : La combinaison de la charge utile du support et de l'en-tête support est appelée paquet de support.

Paquet de FEC : Les algorithmes de FEC chez l'émetteur prennent en entrée les paquets de support. Ils sortent à la fois les paquets de support qui leurs sont passés, et les paquets nouvellement générés appelés paquets de FEC, qui contiennent des données de support redondantes utilisées pour la correction d'erreur. Les paquets de FEC sont formatés conformément aux règles spécifiées dans le présent document.

En-tête de FEC : Les informations d'en-tête contenues dans un paquet de FEC.

En-tête de niveau FEC : Les informations d'en-tête contenues dans un paquet de FEC pour chaque niveau.

Charge utile de FEC : La charge utile d'un paquet de FEC. Elle peut être divisée en plusieurs niveaux.

Associé : Un paquet de FEC est dit être "associé" à un ou plusieurs paquets de support (ou vice versa) lorsque ces paquets de support sont utilisés pour générer le paquet de FEC (en utilisant l'opération du OU exclusif). Il se réfère seulement aux paquets utilisés pour générer la charge utile de FEC de niveau 0, sauf mention contraire explicite.

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 la [RFC2119].

3. Fonctionnement de base

Le format de charge utile décrit ici est utilisé lorsque l'envoyeur dans une session RTP veut protéger le flux de support qu'il envoie avec la FEC de parité générique. La FEC prise en charge par ce format se fonde sur une simple opération de parité de OU exclusif (OUX). L'envoyeur prend les paquets dans le flux de support qui doit être protégé et détermine les niveaux de protection pour ces paquets et la longueur de la protection pour chaque niveau. Les données sont groupées comme décrit ci-dessous à la Section 7. L'opération OUX est appliquée à travers la charge utile pour générer les informations de FEC. Les résultats, suivant les procédures définies ici, sont des paquets RTP contenant des informations de FEC. Ces paquets peuvent être utilisés chez le receveur pour récupéer les paquets ou des parties des paquets utilisés pour générer les informations de FEC.

Le format de charge utile pour la FEC contient les informations qui permettent à l'envoyeur de dire au receveur exactement quels paquets de support sont protégés par le paquet de FEC, et les niveaux et longueurs de protection pour chacun de ces niveaux. Spécifiquement, chaquet paquet de FEC contient un gabarit de décalage m(k) pour chaque niveau de protection. Si le bit i dans le gabarit m(k) est mis à 1, le numéro de paquet de support N + i est protégé par ce paquet de FEC au niveau k. N est appelé la base de numéro de séquence, et est aussi envoyé dans le paquet de FEC. La quantité de données qui est protégée au niveau k est indiquée par L(k), qui est aussi envoyé dans le paquet de FEC. La longueur de protection, le gabarit de décalage, le type de charge utile, et la base de numéro de séquence identifient pleinement le code de parité appliqué pour générer le paquet de FEC avec peu de redondance. Un ensemble de règles décrites au paragraphe 7.4 définit comment devrait être établi le gabarit pour différents niveaux de protection, avec des exemples à la Section 10.

Le présent document décrit aussi les procédures de transmission de tous les paramètres de fonctionnement de la protection dans la bande. Cela autorise une grande souplesse pour l'envoyeur ; l'envoyeur peut adapter la protection aux conditions actuelle du réseau et être certain que les receveurs peuvent toujours faire usage de la FEC pour la récupération.

Chez le receveur, la FEC et le support original sont reçus tous deux. Si aucun des paquets de support n'est perdu, les paquets de FEC peuvent être ignorés. Dans l'éventualité d'une perte, les paquets de FEC peuvent être combinés avec d'autres supports reçus pour récupérer tout ou partie des paquets de support manquants.

4. Codes de parité

Pour faire court, on définit la fonction f(x,y,..) comme l'opérateur OUX (parité) appliqué aux blocs de données x,y,... Le résultat de cette fonction est un autre bloc, appelé le bloc de parité. Pour simplifier, on suppose ici que le bloc de parité est calculé comme le OUX au bit près des blocs d'entrée. La procédure exacte est spécifiée à la Section 8.

La protection des blocs de données qui utilisent des codes de parité est accomplie en générant un ou plusieurs blocs de parité sur un groupe de blocs de données. Pour la meilleure efficacité, les blocs de parité doivent être générés par des combinaisons linéairement indépendantes des blocs de données. La combinaison particulière est appelée un code de parité. Le format de charge utile utilise les codes de parité OUX.

Par exemple, considérons un code de parité qui génère un seul bloc de parité sur deux blocs de données. Si les paquets de support originaux sont a,b,c,d, les paquets générés par l'envoyeur sont :

```
a        b        c        d              <-- flux de support
           f(a,b)             f(c,d)      <-- flux de FEC
```

où l'écoulement du temps se fait de gauche à droite. Dans cet exemple, le schéma de correction d'erreur (on utilise de façon interchangeable les termes schéma et code) introduisent une redondance de 50 %. Mais si b est perdu, a et f(a,b) peuvent être utilisés pour récupérer b.

Il peut être utile de souligner qu'il y a de nombreux autres types de code de correction d'erreur directe qui peuvent aussi être utilisés pour protéger la charge utile en dehors du code de parité OUX. Un exemple notable en est le code Reed-Solomon, et il y en a bien d'autres [12]. Cependant, le code de parité OUX est utilisé ici à cause de son efficacité et de sa simplicité à la fois dans la conception du protocole et dans sa mise en œuvre. Ceci est particulièrement important pour la mise en œuvre dans des nœuds à ressources limitées.

5. Protection de niveau non pair

Comme on peut le voir à partir de l'exemple simple ci-dessus, la protection des données dépend de la taille du groupe. Dans l'exemple ci-dessus, la taille du groupe est 2. Aussi si l'un des trois paquets (deux paquets de charge utile et un paquet de FEC) est perdu, les données de la charge utile d'origine peuvent toujours être récupérées.

En général, l'opération de protection de la FEC est un compromis entre la bande passante et la force de la protection. Plus il y a de paquets de FEC générés comme fraction des paquets de support de la source, plus la protection contre la perte sera forte, mais plus grande sera la bande passante consommée par les flux combinés.

Comme c'est souvent le cas dans la plupart des charges utiles de support, toutes les parties des paquets ne sont pas de la même importance. En utilisant cette propriété, on peut éventuellement réaliser une utilisation plus efficace de la bande passante du canal en appliquant une protection inégale contre l'erreur, c'est à dire, en appliquant une protection différente aux différentes parties du paquet. Plus de bande passante est dépensée pour la protection des parties les plus importantes, alors que moins de bande passante le sera sur les parties les moins importantes.

Les paquets sont séparés en sections d'importance décroissante, et une protection de force différente est appliquée à chaque portion - les sections sont appelées "niveaux". L'opération de protection est appliquée indépendamment à chaque niveau. Un seul paquet de FEC peut porter des données de parité pour plusieurs niveaux. Cet algorithme est appelé protection de niveau non pair (ULP, *uneven level protection*).

La protection de ULP est illustrée à la Figure 1 ci-dessous. Dans cet exemple, deux paquets de FEC ULP protègent quatre paquets de charge utile.

Le paquet de FEC ULP n° 1 a seulement un niveau, qui protège les paquets A et B. Au lieu d'appliquer l'opération de parité à la totalité des paquets A et B, il ne protège qu'une certaine longueur des données des deux paquets. La longueur, qui peut être choisie et changée de façon dynamique durant une session, est appelée la longueur de protection.

Le paquet de FEC ULP n° 2 a deux niveaux de protection. Le niveau de protection 0 est le même que pour le paquet de FEC ULP n° 1 excepté qu'il fonctionne sur les paquets C et D. Le niveau de protection 1 utilise l'opération de parité appliquée sur les données provenant des paquets A, B, C et D. Noter que le niveau de protection 1 fonctionne sur un ensemble de paquets différent du niveau 0 et a une longueur de protection différente du niveau 0, et ainsi sont tous les autres niveaux. Les informations sont toutes convoyées dans la bande selon les protocoles spécifiés par le présent document.

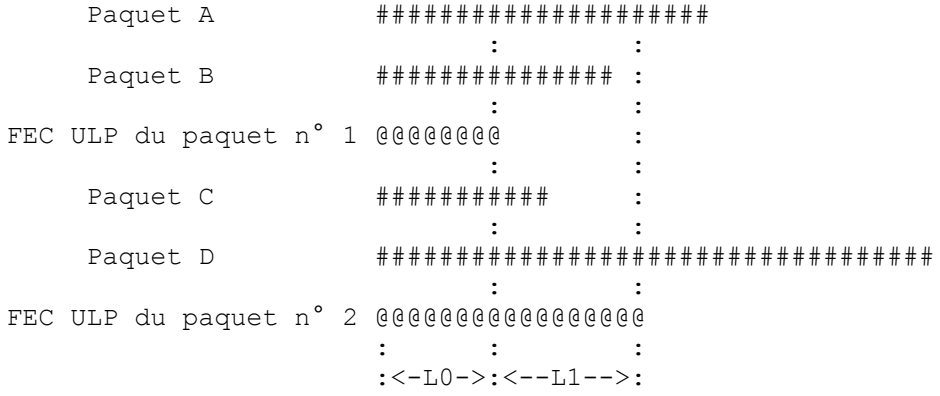


Figure 1 : Protection de niveau inégal

Comme indiqué dans l'introduction, les flux de support ont habituellement leurs parties les plus importantes au début du paquet. Il est normalement utile d'avoir la plus forte protection dans les niveaux les plus proches du début du paquet, et une protection plus faible dans les niveaux plus éloignés. L'algorithme d'ULP donne une telle protection de FEC.

La FEC ULP fournit non seulement plus de protection au début du paquet (ce qui est le plus important), mais évite aussi autant que possible les scénarios les moins efficaces où une section antérieure d'un paquet n'est pas récupérable alors qu'une section postérieure peut être récupérée (et doit souvent être éliminée).

6. Structure du paquet de support RTP

Le formatage des paquets du support n'est pas affecté par la FEC. Si la FEC est envoyée sous un flux séparé, les paquets du support sont envoyés comme si il n'y avait pas de FEC.

Cette approche présente l'avantage que les receveurs qui ne prennent pas en charge la FEC peuvent interpréter les paquets de support. Cette compatibilité avec les receveurs sans capacité de FEC est particulièrement utile pour les scénarios de diffusion groupée. La redondance pour l'utilisation du schéma de FEC n'est présente que dans les paquets de FEC, et peut être aisément surveillée et ajustée en retraçant la quantité de FEC utilisée.

7. Structure du paquet de FEC

7.1 Structure de paquet

Un paquet de FEC est construit en plaçant un en-tête de FEC et un ou plusieurs en-têtes et charges utiles de niveau de FEC dans la charge utile RTP, comme le montre la Figure 2 :

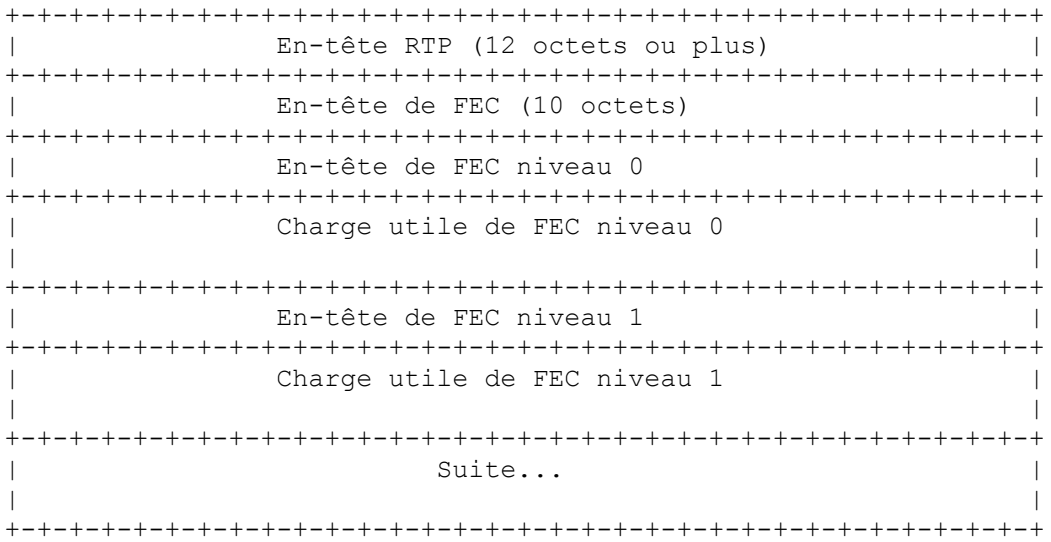


Figure 2 : Structure de paquet de FEC

7.2 En-tête RTP pour les paquets de FEC

L'en-tête RTP pour les paquets de FEC n'est utilisé que lorsque la FEC est envoyée dans un flux distinct du flux de la charge utile protégée (comme défini à la Section 14). Donc, une grande partie de l'exposé ci-dessous ne s'applique qu'à ce scénario. Tous les champs dans l'en-tête RTP des paquets de FEC sont utilisés conformément à la RFC 3550 [1], et certains d'entre eux sont précisés ci-dessous.

Marqueur : Ce champ n'est pas utilisé pour ce type de charge utile, et DEVRA être mis à 0.

Source de synchronisation (SSRC) : La valeur SSRC DEVRA être la même que la valeur SSRC du flux de support qu'elle protège.

Numéro de séquence (SN) : le numéro de séquence a la définition standard - il DOIT être supérieur de un au numéro de séquence du paquet de FEC transmis précédemment.

Horodatage (TS) : l'horodatage DOIT être réglé à la valeur de l'horloge RTP du support à l'instant de la transmission du paquet de FEC. Donc, la valeur TS dans les paquets de FEC est toujours d'accroissement monotone.

Type de charge utile : le type de charge utile pour les paquets de FEC est déterminé par des moyens dynamiques hors bande. Selon la RFC 3550 [1], les participants RTP qui ne peuvent pas reconnaître un type de charge utile doivent l'éliminer. Cela permet la rétro compatibilité. Les mécanismes de FEC peuvent alors être utilisés dans un groupe de

diffusion groupée avec un mélange de receveurs à capacité de FEC et sans capacité de FEC, en particulier lorsque la protection FEC est envoyée comme codage redondant (voir la Section 14). Dans de tels cas, la protection de FEC aura un type de charge utile qui n'est pas reconnu par les receveurs sans capacité de FEC, et ne sera donc pas prise en considération.

7.3 En-tête de FEC pour les paquets de FEC

L'en-tête de FEC fait 10 octets. Le format de l'en-tête est donné à la Figure 3 et consiste en un fanion d'extension (le bit E), le fanion de gabarit long (le bit L), un champ de récupération P, un champ de récupération X, un champ de récupération CC, un champ de récupération M, un champ de récupération PT, un champ de base SN, un champ de récupération TS, et un champ de longueur de récupération.

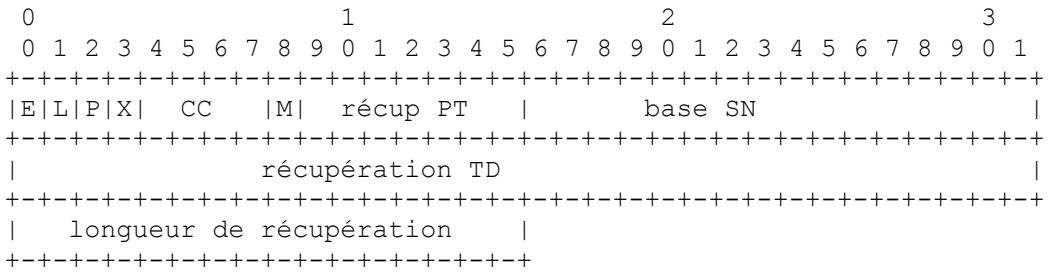


Figure 3 : Format d'en-tête de FEC

Le bit E est le fanion d'extension réservé pour indiquer toute future extension à la présente spécification. Il DEVRA être réglé à 0, et DEVRAIT être ignoré par le receveur.

Le bit L indique si le gabarit long est utilisé. Lorsque le bit L n'est pas établi, le gabarit est de 16 bits. Lorsque le bit L est mis, le gabarit fait alors 48 bits.

Le champ de récupération P, le champ de récupération X, le champ de récupération CC, le champ de récupération M, et le champ de récupération PT sont obtenus via l'opération de protection appliquée aux valeurs P, X, CC, M, et PT correspondantes provenant de l'en-tête RTP des paquets de support associés au paquet de FEC.

Le champ de base SN DOIT être réglé au plus faible numéro de séquence, en tenant compte du retour à zéro, des paquets de support protégés par la FEC (à tous les niveaux). Cela permet à l'opération de FEC de s'étendre sur tout chaîne d'au plus 16 paquets lorsque le champ L est mis à 0, ou de 48 paquets lorsque le champ L est réglé à 1, et ainsi de suite.

Le champ de récupération TS est calculé via l'opération de protection appliquée aux horodatages des paquets de support associés à ce paquet de FEC. Cela permet de récupérer complètement l'horodatage.

Le champ de récupération de longueur est utilisé pour déterminer la longueur de tout paquet récupéré. Il est calculé via l'opération de protection appliquée à la représentation de 16 bits non signés rangés dans l'ordre du réseau des sommes des longueurs (en octets) de la charge utile de support, de la liste CSRC, de l'extension et du bourrage de chacun des paquets de support associé à ce paquet de FEC (en d'autres termes, la liste CSRC, l'extension RTP, et le bourrage des paquets de charge utile de support, si ils sont présents, sont "comptés" au titre de la charge utile). Cela permet à la procédure de FEC d'être appliquée même lorsque les longueurs des paquets de support protégés ne sont pas identiques. Par exemple, suposons qu'un paquet de FEC soit généré en appliquant l'opération OUX à deux paquets de support. La longueur de la charge utile des deux paquets de support est, respectivement, 3 (0b011) et 5 (0b101) octets. Le champ de récupération de longueur est alors codé par 0b011 xor 0b101 = 0b110.

7.4 En-tête de niveau de FEC pour les paquets de FEC

L'en-tête de niveau de FEC est de 4 ou 8 octets (en fonction du bit L dans l'en-tête de FEC). Les formats des en-têtes sont montrés à la Figure 4.

Les en-têtes de niveau de FEC consistent en un champ Longueur de protection et un champ Gabarit. Le champ Longueur de protection fait 16 bits. Le champ Gabarit fait 16 bits (quand le bit L n'est pas mis) ou 48 bits (quand le bit L est mis).

Le champ Gabarit dans l'en-tête de niveau de FEC indique quels paquets sont associés au paquet de FEC au niveau actuel. Il est de 16 ou 48 bits selon la valeur du bit L. Si le bit i dans le gabarit est réglé à 1, le paquet de support avec le numéro de

séquence N + i est alors associé à ce paquet de FEC, où N est le champ SN de base dans l'en-tête du paquet de FEC. Le bit de poids fort dans le gabarit correspond à i = 0, et le bit de moindre poids à i = 15 lorsque le bit L est mis à 0, ou à i = 47 lorsque le bit L est mis à 1.

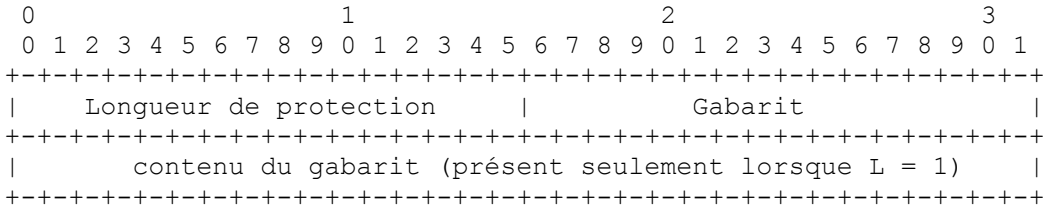


Figure 4 : Format d'en-tête de niveau ULP

Le réglage du champ Gabarit doit respecter les règles suivantes :

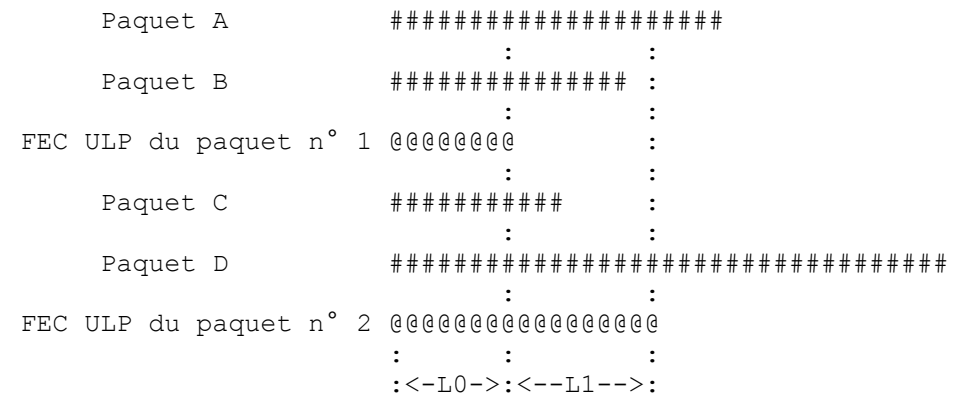
a. Un paquet de support DEVRA être protégé une seule fois à chaque niveau de protection supérieur au niveau 0. Un paquet support PEUT être protégé plus d'une fois au niveau 0 par différents paquets, pourvu que la longueur de protections du niveau 0 de ces paquets soit égale.

b. Pour qu'un paquet support soit protégé au niveau p, il DOIT aussi être protégé au niveau p-1 dans tout paquet de FEC. Prière de noter que le niveau de protection p pour qu'un paquet support puisse être dans un paquet de FEC qui est différent de celui qui contient le niveau de protection p-1 pour le même paquet support.

c. Si un paquet de FEC ULP contient une protection au niveau p, il DOIT aussi contenir la protection au niveau p-1. Noter que la combinaison de paquets de charge utile qui est protégée au niveau p peut être différente de celle du niveau p-1.

La raison de la règle (a) est que plusieurs protections augmentent la complexité de la mise en œuvre de la récupération. Aux niveaux supérieurs, la protection multiple offre un avantage décroissant, de sorte que son application est restreinte au niveau 0 pour une mise en œuvre plus simple. La raison de la règle (b) est que le décalage de protection (pour chaque paquet associé) n'est pas signalé explicitement dans le protocole. Avec cette restriction, le décalage peut être facilement déduit des longueurs de protection des niveaux. La raison de la règle (c) est que le niveau de protection n'est pas indiqué explicitement. Cette règle est mise pour spécifier implicitement les niveaux.

Un exemple des combinaisons de protection est illustré à la Figure 5 ci-dessous. C'est le même exemple que celui donné dans la Figure 1. Ce même exemple est aussi donné plus en détail au paragraphe 10.2 pour illustrer comment sont réglés les champs dans les en-têtes.



N° de paquet de charge utile	Paquet de FEC ULP qui protège au niveau	
	L0	L1
A	n° 1	n° 2
B	n° 1	n° 2
C	n° 2	n° 2
D	n° 2	n° 2

Figure 5 : Exemple de combinaison de protection

Dans cet exemple, le paquet de FEC ULP n° 1 a seulement le niveau de protection 0. Le paquet de FEC ULP n° 2 a les niveaux de protection 0 et 1. En lisant le tableau, on voit que le paquet de charge utile A est protégé par le paquet de FEC ULP n° 1 au niveau 0, par le paquet de FEC ULP n° 2 au niveau 1, et ainsi de suite. On peut aussi voir facilement sur le tableau que le paquet de FEC ULP n° 2 protège au niveau 0 les paquets de charge utile C et D, au niveau 1 les paquets de charge utile A-D, et ainsi de suite. Pour des exemples supplémentaires plus détaillés, se reporter à la Section 10, Exemples.

La charge utile des paquets de FEC ULP de chaque niveau est l'opération de protection (OUX) appliquée à la charge utile de support et au bourrage des paquets de support associés au paquet de FEC ULP à ce niveau. Les détails sont décrits à la Section 8 sur l'opération de protection.

La taille des paquets de FEC ULP est déterminée par les longueurs de protection choisies pour l'opération de protection. Dans l'exemple ci-dessus, le paquet de FEC ULP n° 1 a la longueur L0 (plus la redondance d'en-tête). Le paquet de FEC ULP n° 2 avec deux niveaux a la longueur L0+L1 (plus la redondance d'en-tête). Il est plus long que certains des paquets qu'il protège (les paquets B et C dans cets exemple) et est plus court que certaine des paquets qu'il protège (les paquets A et D dans cet exemple).

Noter qu'il est possible que le paquet de FEC (non ULP et ULP) soit plus grand que le plus long des paquets de support qu'il protège parce que la redondance provenant des en-têtes et/ou si une longueur de protection importante est choisie pour ULP. Cela pourrait causer des difficultés si il en résulte que le paquet de FEC excède la taille d'unité maximum de transmission pour le chemin sur lequel il est envoyé.

8. Fonctionnement de la protection

Les paquets de FEC sont formés à partir d'une "chaîne binaire de FEC" qui est générée à partir des données des paquets de support RTP protégés. Plus précisément, la chaîne binaire FEC est le OU exclusif au bit près des "chaîne binaires protégées" des paquet de support RTP protégés.

La procédure suivante PEUT être suivie pour l'opération de protection. D'autres procédures PEUVENT être utilisées, mais le résultat final DOIT être identique à celui décrit ici.

8.1 Génération de l'en-tête de FEC

Dans le cas de l'en-tête de FEC, les chaînes binaires protégées (longues de 80 bits) sont générées pour chaque paquet de support à protéger au niveau 0 de FEC. Il est formé par l'enchaînement des champs suivants ensemble dans l'ordre spécifié :

- Les 64 premiers bits de l'en-tête RTP (64 bits)
- La représentation sur 16 bits non signée dans l'ordre du réseau de la longueur du paquet de support en octets moins 12 (pour l'en-tête RTP fixe), c'est-à-dire, la somme des longueurs de tous les champs suivants, s'ils sont présents : la liste CSRC, l'en-tête d'extension, la charge utile RTP, et le bourrage RTP (16 bits)

Après que la chaîne binaire de FEC est formée en appliquant l'opération de parité sur les chaînes binaires protégées, l'en-tête de FEC est généré à partir de la chaîne binaire de FEC comme suit :

Les deux premiers bits (de poids fort) dans la chaîne binaire de FEC sont sautés. Le bit suivant de la chaîne binaire de FEC sont écrits dans le bit P de récupération de l'en-tête de FEC dans le paquet de FEC. Le bit suivant dans la chaîne binaire de FEC est écrit dans le bit E de récupération de l'en-tête de FEC. Les 4 bits suivants de la chaîne binaire de FEC sont écrits dans le champ CC de récupération de l'en-tête de FEC. Le bit suivant est écrit dans le bit M de récupération de l'en-tête de FEC. Les 7 bits suivants de la chaîne binaire de FEC sont écrits dans le champ PT de récupération dans l'en-tête de FEC. Les 16 bits suivants sont sautés. Les 32 bits suivants de la chaîne binaire de FEC sont écrits dans le champ TS de récupération dans l'en-tête de FEC. Les 16 bits suivants sont écrits dans le champ Longueur de récupération dans l'en-tête de paquet.

8.2 Génération de la charge utile de FEC

Pour la génération de la charge utile de FEC, les chaînes binaires protégées sont simplement les paquets RTP protégés. La chaîne binaire de FEC est donc le OU exclusif au bit près de ces paquets de support RTP protégés. De telles chaînes binaires de FEC doivent être générées pour chaque niveau, car le groupe de paquets de charge utile protégés peut être

différent pour chaque niveau. Si les longueurs des paquets RTP protégés ne sont pas égales, chaque paquet plus court DOIT être bourré à la longueur du paquet le plus long par l'ajout de l'octet 0 à la fin.

Pour le niveau de protection n (n = 0, 1, ...), seuls Ln octets de données sont réglés comme données de charge utile de FEC de niveau n après l'en-tête ULP de niveau n. Les données sont les Ln octets de données commençant par le $(Sn + 13)^{ème}$ octet dans la chaîne binaire de FEC, où :

$$Sn = \sum(Li : 0 <= i < n).$$

Li est la longueur de protection du niveau i, et S0 est défini comme étant 0. La raison de l'omission des 12 premiers octets est que cette information est déjà protégée par l'en-tête de FEC.

9. Procédures de récupération

Les paquets de FEC permettent aux systèmes d'extrémité de récupérer de leurs pertes de paquets de support. La présente section décrit la procédure pour effectuer cette récupération.

La récupération exige deux opérations distinctes. La première détermine quels paquets (de support et de FEC) doivent être combinés afin de récupérer un paquet manquant. Une fois cela fait, la seconde étape est en fait de reconstruire les données. La seconde étape DOIT être effectuée comme décrit ci-dessous. La première étape PEUT se fonder sur tout algorithme du choix de la mise en œuvre. Différents algorithmes résultent en un compromis entre complexité et capacité à récupérer les paquets manquants, si possible.

Les paquets de charge utile perdus peuvent être récupérés en totalité ou en partie selon la situation des données perdues du fait de la nature de la protection d'erreur inégale (lorsque elle est utilisée). La récupération partielle du paquet peut être détectée en vérifiant la longuieur de récupération du paquet restituée de l'en-tête de FEC par rapport à la longueur des données de charge utile récupérées.

9.1 Reconstruction de l'en-tête RTP

Soit T la liste des paquets (de FEC et de support) qui peuvent être combinés pour récupérer un paquet de support xi au niveau 0. La procédure est la suivante :

1. Pour les paquets de support en T, calculer les 80 premiers bits de la chaîne binaire protégée suivant la procédure décrite pour générer l'en-tête de FEC à la section précédente.

2. Pour le paquet de FEC en T, la chaîne binaire de FEC est l'en-tête de FEC de 80 bits.

3. Calculer la chaîne binaire de récupération comme OU exclusif au bit près de la chaîne binaire protégée générée sur tous les paquets de support dans T et la chaîne binaire de FEC générée sur tous les paquets de FEC dans T.

4. Créer un nouveau paquet avec l'en-tête RTP standard de 12 octets et pas de charge utile.

5. Régler la version du nouveau paquet à 2. Sauter les 2 premiers bits dans la chaîne binaire de récupération.

6. Régler le bit Bourrage dans le nouveau paquet au prochain bit dans la chaîne binaire de récupération.

7. Régler le bit Extension dans le nouveau paquet au prochain bit dans la chaîne binaire de récupération.

8. Régler le champ CC aux 4 procahins bits dans la chaîne binaire de récupération.

9. Régler le bit marqueur dans le nouveau paquet au prochain bit dans la chaîne binaire de récupération.

10. Régler le type de charge utile dans le prochain paquet au 7 procahins bits dans la chaîne binaire de récupération.

11. Régler le champ SN dans le nouveau paquet à xi. Sauter les 16 bits suivants dans la chaîne binaire de récupération.

12. Régler le champ TS dans le nouveau paquet aux 32 procahins bits dans la chaîne binaire de récupération.

13. Prendre les 16 prochains bits de la chaîne binaire de récupération. Quel que soit l'entier non signé que cela représente

(en supposant l'ordre du réseau) prendre ce nombre d'octets de la chaîne binaire de récupération et les ajouter au nouveau paquet. Cela représente la liste CSRC, la charge utile d'extension, et le bourrage de la charge utile RTP.

14. Régler la SSRC du nouveau paquet à la SSRC du flux de support qu'il protège, c'est-à-dire, à la SSRC du flux de support auquel le flux de FEC est associé.

Cette procédure va récupérer l'en-tête d'un paquet RTP jusqu'au champ SSRC.

9.2 Reconstruction de la charge utile RTP

Soit T la liste des paquets (de FEC et de support) qui peuvent être combinés pour récupérer un paquet de support xi à un certain niveau de protection. La procédure est la suivante :

1. Supposons que nous reconstruisons les données pour le niveau n, la première étape est d'obtenir la longueur de protection du niveau n (Ln) d'après l'en-tête ULP du niveau n.

2. Pour les paquets de FEC dans T, la chaîne binaire de FEC du niveau n est la charge utile de la FEC de niveau n, c'est-à-dire, les Ln octets de données suivant l'en-tête ULP de niveau n.

3. Pour les paquets de support dans T, la chaîne binaire protégée de niveau n est de Ln octets de données commençant par le (Sn + 13)ème octet du paquet. Sn est le même que défini au paragraphe 8.2. Noter que la protection de niveau 0 commence à partir du 13ème octet du paquet de support après le champ SSRC. Les informations des 12 premiers octets sont protégées par l'en-tête de FEC.

4. Si une des chaînes binaires protégées de niveau n générées à partir des paquets de support est plus courte que la longueur de protection du niveau actuel, la bourrer jusqu'à cette longueur. Le bourrage d'octet 0 DOIT être ajouté à la fin de la chaîne binaire.

5. Calculer la chaîne binaire de récupération comme OU exclusif au bit près de la chaîne binaire protégée de niveau n générée à partir de tous les paquets de support dans T et de la chaîne binaire de FEC de niveau n générée à partir de tous les paquets de FEC dans T.

6. La chaîne binaire de récupération du niveau de protection actuel tel que généré ci-dessus est combinée par l'enchaînement des chaînes binaires de récupération de tous les autres niveaux pour former le paquet de support (complètement ou partiellement) récupéré. Noter que la chaîne binaire récupérée de chaque niveau de protection DOIT être placée à la localisation correcte dans le paquet de support récupéré pour ce niveau sur la base des réglages de longueur de protection.

7. La longueur totale du paquet de support récupéré est restituée par l'opération de récupération au niveau de protection 0 du paquet de support récupéré. Ces informations peuvent être utilisées pour vérifier si l'opération de récupération complète (à tous les niveaux) a récupéré le paquet dans toute sa longueur.

Les données protégées au plus bas niveau de protection sont récupérables dans une majorité de cas si les données du plus fort niveau protégé sont récupérables. Cette procédure (conjointement avec la procédure pour les niveaux de protection inférieurs) va normalement récupérer à la fois l'en-tête et la charge utile d'un paquet RTP jusqu'à la longueur de protection du niveau en vigueur.

10. Exemples

Dans les deux premiers exemples considérés ci-dessous (paragraphes 10.1 et 10.2) on suppose que les flux de FEC sont envoyés à travers une session RTP distincte, comme décrit au paragraphe 14.1. Pour ces exemples, on suppose que quatre paquets de support sont à envoyer, A, B, C, et D, à partir de SSRC 2. Leurs numéros de séquence sont 8, 9, 10, et 11, respectivement, et ils ont respectivement des horodatages de 3, 5, 7, et 9. Les paquets A et C utilsent le type de charge utile 11, et les paquets B et D utilisent le type de charge utile 18. Le paquet A a 200 octets de charge utile, le paquet B en a 140, le paquet C 100, et le paquet D 340. Les paquets A et C ont leur bit marqueur établi.

Le troisième exemple (paragraphe 10.3) illustre le cas d'envoi des données de FEC comme données redondantes avec les paquets de charge utile.

10.1 Exemple qui offre une protection similaire à celle de la RFC 2733

On peut protéger les quatre paquets de charge utile sur toute leur longueur à un seuk niveau avec un paquet de FEC. Cela offre une protection similaire à celle de la RFC 2733. Le schéma est celui indiqué à la Figure 6.

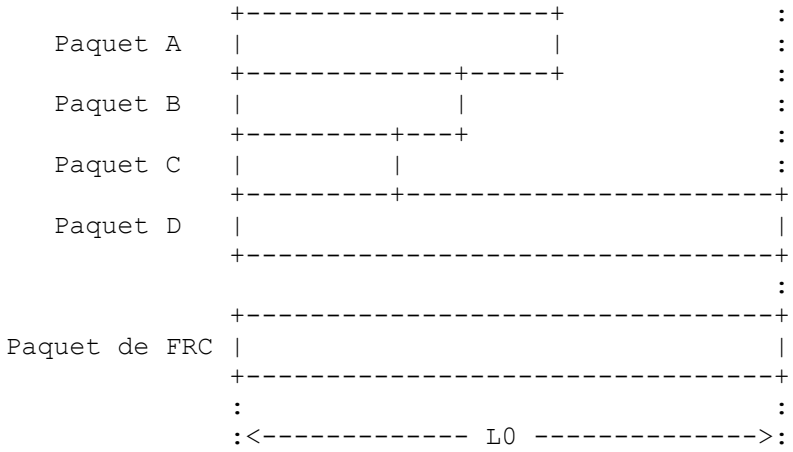
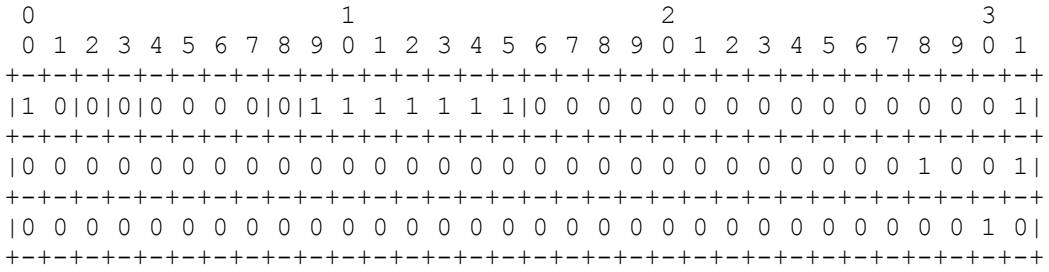


Figure 6 : Schéma de FEC avec une protection à un seul niveau

Un paquet de FEC est généré à partir de ces quatre paquets. On suppose que le type de charge utile 127 est utilisé pour indiquer un paquet de FEC. L'en-tête RTP résultant est indiqué à la Figure 7.

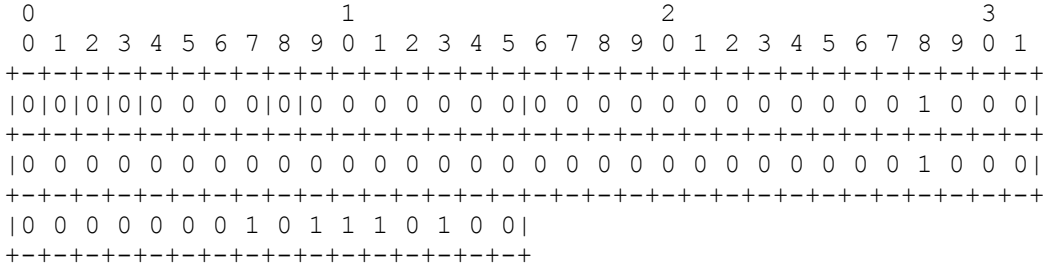
L'en-tête de FEC dans le paquet de FEC est indiqué à la Figure 8.

L'en-tête de niveau de FEC pour le niveau 0 est indiqué à la Figure 9.



Version : 2
Bourrage : 0
Extension : 0
Marqueur : 0
PT : 127
SN : 1
TS : 9
SSRC : 2

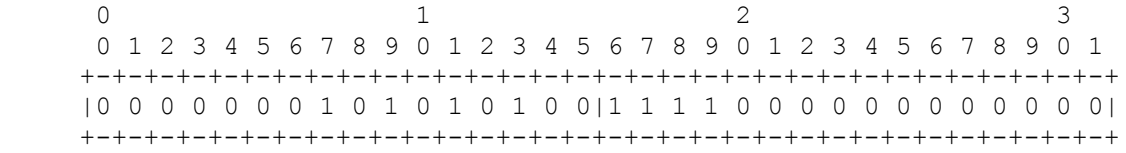
Figure 7 : En-tête RTP de paquet de FEC



E : 0 [cette spécification]
L : 0 [gabarit court de 16 bits]

P rec. : 0 [0 OUX 0 OUX 0 OUX 0]
X rec. : 0 [0 OUX 0 OUX 0 OUX 0]
CC rec. : 0 [0 OUX 0 OUX 0 OUX 0]
M rec. : 0 [1 OUX 0 OUX 1 OUX 0]
PT rec. : 0 [11 OUX 18 OUX 11 OUX 18]
SN base : 8 [min(8,9,10,11)]
TS rec. : 8 [3 OUX 5 OUX 7 OUX 9]
len. rec. : 372 [200 OUX 140 OUX 100 OUX 340]

Figure 8 : En-tête de FEC de paquet de FEC



L0 : 340 [le plus long de 200, 140, 100, et 340]
gabarit : 61440 [avec les bits 1, 2, 3, et 4 marqués en conséquence pour les paquets 8, 9, 10, et 11]

La longueur de charge utile pour le niveau 0 est 340 octets.

Figure 9 : En-tête de niveau de FEC (niveau 0)

10.2 Exemple avec deux niveaux de protection

Un exemple plus complexe utilise la FEC à deux niveaux. Le niveau 0 de FEC va fournir une plus grande protection au début des paquets de charge utile. Le niveau 1 de FEC va appliquer une protection supplémentaire au reste des paquets. Ceci est illustré par la Figure 10. Dans cet exemple, L0 = 70 et L1 = 90.

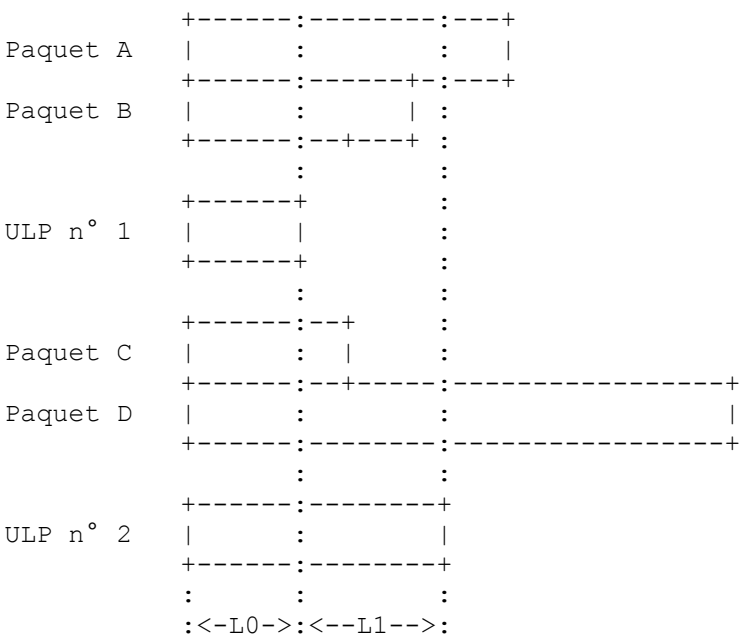
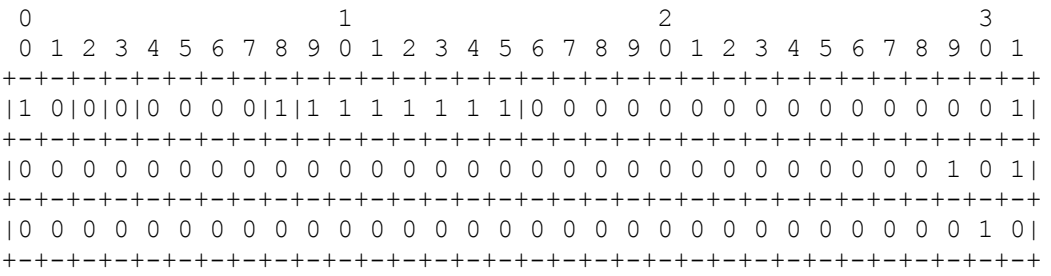


Figure 10 : Schéma de FEC ULP avec protection de niveau 0 et de niveau 1

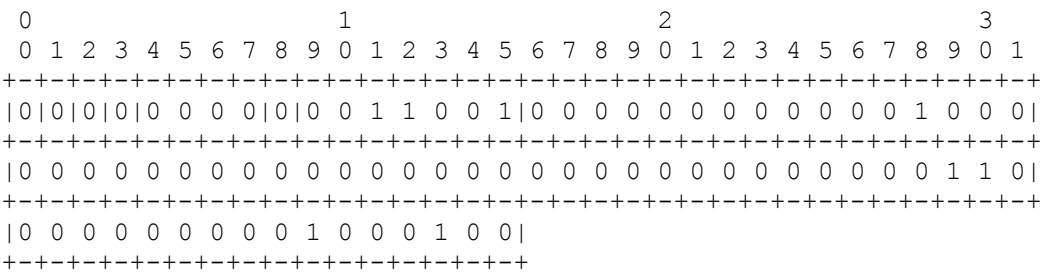
Il va en résulter deux paquets de FEC – n° 1 et n° 2.

Le paquet de FEC ULP n° 1 aura l'en-tête RTP montré à la Figure 11. L'en-têtede FEC pour le paquet de FEC ULP n° 1 sera celui montré à la Figure 12. L'en-tête ULP de niveau 0 pour le n° 1 sera celui montré à la Figure 13.



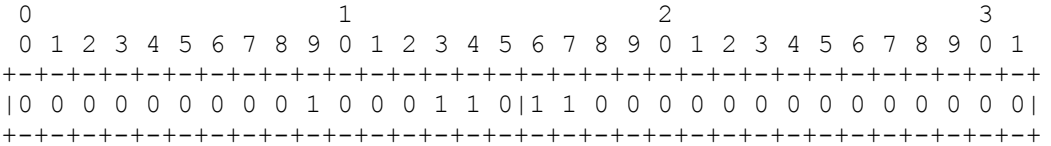
Version : 2
Bourrage : 0
Extension : 0
Marqueur : 1
PT : 127
SN : 1
TS : 5
SSRC : 2

Figure 11 : En-tête RTP du paquet de FEC n° 1



E : 0 [cette spécification]
L : 0 [gabarit court à 16 bits]
P rec. : 0 [0 OUX 0 OUX 0 OUX 0]
X rec. : 0 [0 OUX 0 OUX 0 OUX 0]
CC rec. : 0 [0 OUX 0 OUX 0 OUX 0]
M rec. : 0 [1 OUX 0 OUX 1 OUX 0]
PT rec. : 25 [11 OUX 18]
SN base : 8 [min(8,9)]
TS rec. : 6 [3 OUX 5]
len. rec. : 68 [200 OUX 140]

Figure 12 : En-tête de FEC Header of ULP FEC Paquet #1

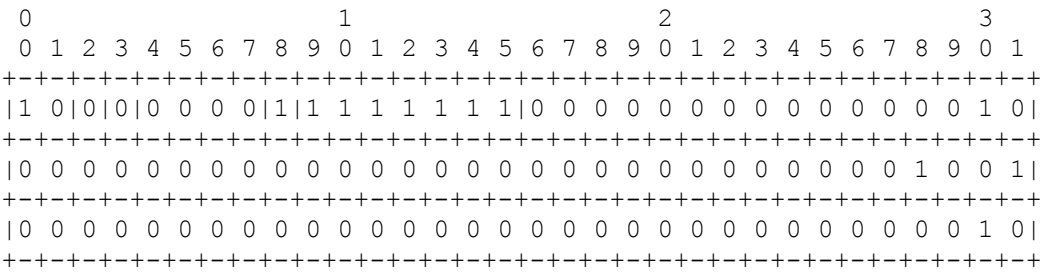


L0 : 70
gabarit : 49152 [avec les bits 1 et 2 marqués en consaquence pour les paquets 8 et 9]

La longueur de charge utile pour le niveau 0 est de 70 octets.

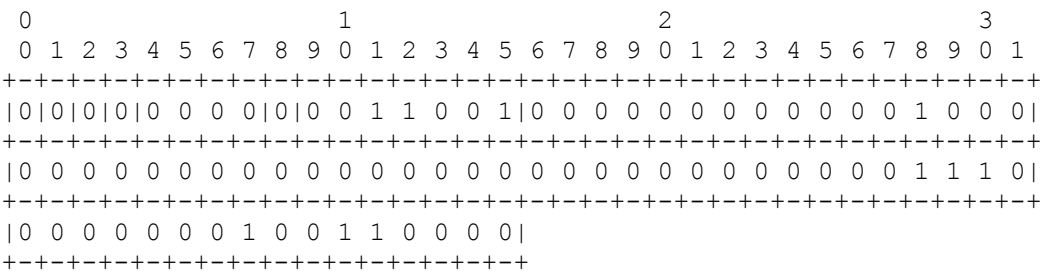
Figure 13 : En-tête de niveau de FEC (niveau 0) pour le paquet de FEC n° 1

Le paquet de FEC résultant n° 2 aura l'en-tête RTP indiqué à la Figure 14. L'en-tête de FEC pour le paquet de FEC n° 2 sera comme indiqué à la Figure 15. L'en-tête ULP de niveau 0 pour le n° 2 sera comme indiqué à la Figure 16. L'en-tête ULP de niveau 1 pour le n° 2 sera comme indiqué à la Figure 17.



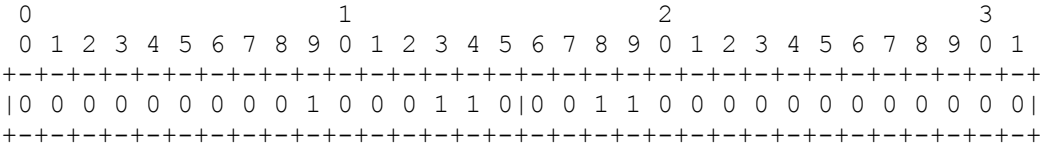
Version : 2
Bourrage : 0
Extension : 0
Marqueur : 1
PT : 127
SN : 2
TS : 9
SSRC : 2

Figure 14 : En-tête RTP du paquet de FEC n° 2



E : 0 [cette spécification]
L : 0 [gabarit court à 16 bits]
P rec. : 0 [0 OUX 0 OUX 0 OUX 0]
X rec. : 0 [0 OUX 0 OUX 0 OUX 0]
CC rec.: 0 [0 OUX 0 OUX 0 OUX 0]
M rec. : 0 [1 OUX 0 OUX 1 OUX 0]
PT rec. : 25 [11 OUX 18]
SN base : 8 [min(8,9,10,11)]
TS rec. : 14 [7 OUX 9]
len. rec. : 304 [100 OUX 340]

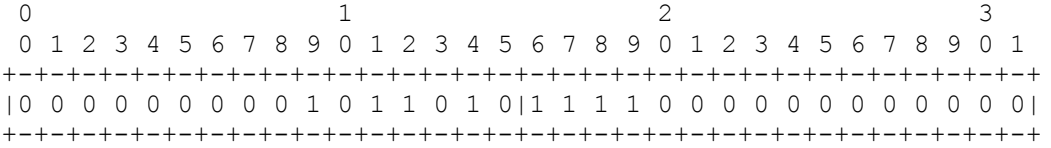
Figure 15 : En-tête de FEC du paquet de FEC n° 2



L0 : 70
gabarit : 12288 [avec les bits 3 et 4 marqués en conséquence pour les paquets 10 et 11]

La longueur de charge utile pour le niveau 0 est de 70 octets.

Figure 16 : En-tête de niveau de FEC (niveau 0) pour le paquet de FEC n° 2



L1 : 90
gabarit : 61440 [avec les bits 1, 2, 3, et 4 marqués en conséquence pour les paquets 8, 9, 10, et 11]

La longueur de charge utile pour le niveau 1 est de 90 octets.

Figure 17 : En-tête de niveau de FEC (niveau 1) pour le paquet de FEC n° 2

10.3 Exemple avec FEC comme codage redondant

Cet exemple illustre la FEC envoyée comme codage redondant dans le même flux que la charge utile. On suppose que cinq paquets de support sont à envoyer, A, B, C, D, et E, à partir de SSRC 2. Leurs numéros de séquence sont respectivement 8, 9, 10, 11, et 12, et ils ont respectivement les horodatages 3, 5, 7, 9, et 11. Toutes les données de support sont codées avec un codage principal (et la FEC comme codage redondant protège seulement le codage principal) et utilisent le type de charge utile 11. Le paquet A a 200 octets de charge utile, le paquet B en a 140, le paquet C 100, le paquet D 340, et le paquet E 160. Les paquets A et C ont leur bit marqueur établi.

Le schéma de FEC que nous utilisons sera à un niveau, comme illustré par la Figure 6 au paragraphe 10.1. La longueur de protection L0 = 340 octets.

Une mise en paquet à codage redondant est utilisée avec le type de charge utile 100. Le type de charge utile de la FEC est supposé être 127. Les quatre premier paquets de RED, de RED n° 1 à RED n° 4, contiennent chacun un paquet de support individuel, respectivement, A, B, C, ou D. Les données de FEC qui protègent les données de support dans les quatre premiers paquets de support sont générés. Le cinquième paquet, RED n° 5, contient ces données de FEC comme codage redondant avec le paquet de support E.

Paquet RED n° 1 : Paquet de support A
Paquet RED n° 2 : Paquet de support B
Paquet RED n° 3 : Paquet de support C
Paquet RED n° 4 : Paquet de support D
Paquet RED n° 5 : Paquet de FEC, paquet de support E

Les paquets RES n° 1 à n° 4 vont avoir la structure indiquée à la Figure 18. L'en-tête RTP du paquet RED n° 1 est comme indiqué à la Figure 19, avec tous les autres paquets RED dans un format similaire avec les numéros de séquence et les horodatages correspondants. L'en-tête de bloc de codage principal des paquets RED est indiqué à la Figure 20.

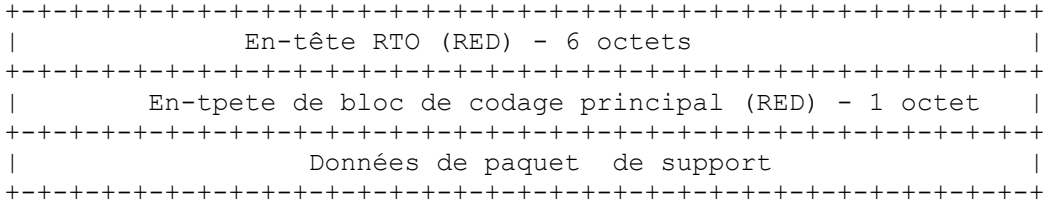
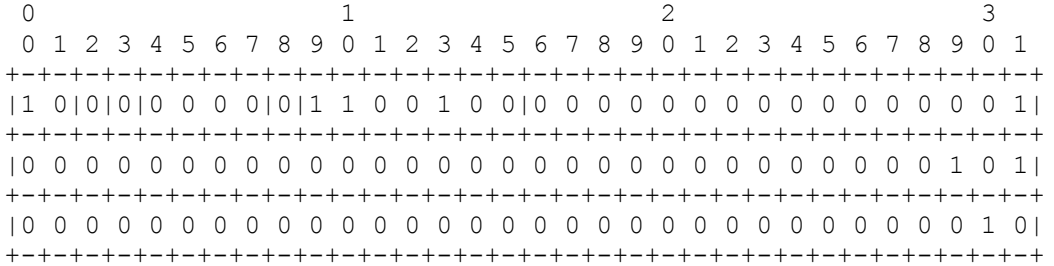


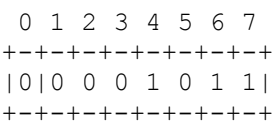
Figure 18 : Structure de paquet RED – seulement des données de support



Version : 2
Bourrage : 0
Extension : 0
Marqueur : 0 [Même si le paquet de support A a le marqueur établi]
PT : 100 [Type de charge utile pour RED]
SN : 1

TS : 5
SSRC : 2

Figure 19 : En-tête RTP du paquet RED n° 1



Bit F : 0 [Ce sont les données du codage principal]
Bloc PT : 11 [C'est le type de charge utile du support]

Figure 20 : En-tête du bloc de codage principal

Les données de FEC ne sont pas générées directement à partir des paquets RED, mais à partir des paquets RTP virtuels qui contiennent les données de paquet de support. Ces paquets RTP virtuels peuvent être générés très facilement à partir des paquets RED incluant ou non le codage redondant. La conversion des paquets RED en paquets RTP virtuels est faite simplement en (1) retirant tous les en-têtes de bloc RED et les données de codage redondant, et (2) remplaçant le PT dans l'en-tête RTP par le PT du codage principal.

Note : Dans le format de charge utile pour le codage redondant comme spécifié par la RFC 2198, le bit marqueur est perdu aussitôt que le codage principal est porté dans les paquets RED. Ainsi le bit marqueur ne peut pas être récupéré, que la FEC soit ou non utilisée.

Comme mentionné ci-dessus, le paquet RED n° 5 va contenir les données de FEC (qui protègent les paquets de support A, B, C, et D) ainsi que les données du paquet de support E. La structure du paquet RED n° 5 est illustrée par la Figure 21.

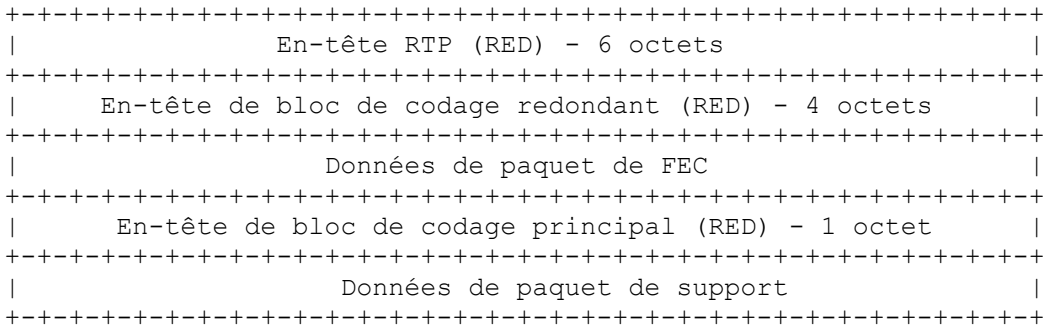
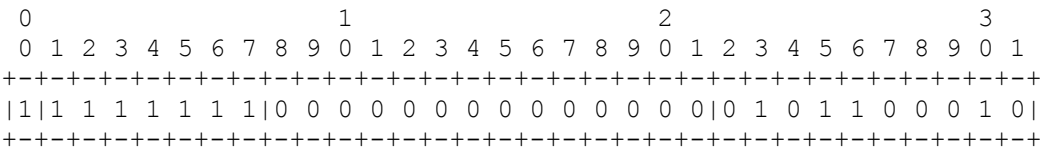


Figure 21 : Structure de paquet RED – avec données de FEC

L'en-tête RTP des paquets RED avec FEC incluse est le même qu'à la Figure 19, avec leurs numéros de séquence et les horodatages correspondants.

Dans le paquet RED n° 5, l'en-tête de bloc de codage redondant pour le bloc de données du paquet de FEC est indiqué ci-dessous à la Figure 22. Il va être suivi par les données du paquet de FEC, qui, dans ce cas, incluent un en-tête de FEC (10 octets comme indiqué à la Figure 8), un en-tête ULP de niveau 0 (4 octets comme indiqué à la Figure 9), et les données de niveau ULP 0 (340 octets comme établi pour le niveau 0). Ceux-ci sont suivis par le bloc de codage principal qui contient les données du paquet support E.



Bit F : 1 [Ce sont les données de codage redondant]
Bloc PT : 127 [Le type de charge utile dynamique pour la FEC]
Décalage TS : 0 [L'instance à laquelle sont transmises les données de FEC]
Longueur de bloc : 354 [en-tête de FEC (10 octets) plus en-tête ULP de niveau 0 (4 octets) et données ULP de niveau 0 (340 octets)]

Figure 22 : En-tête de bloc de codage redondant

11. Considérations pour la sécurité

Il y a deux façons d'utiliser la FEC avec chiffrement dans des communications sécurisées : l'une est d'appliquer la FEC sur des charges utiles déjà chiffrées, et l'autre est d'appliquer la FEC avant le chiffrement. Le premier cas se rencontre lorsque la FEC est nécessaire à un nœud qui n'est pas de confiance durant la transmission après le chiffrement des données de support. Le second cas se rencontre lorsque les données de support sont protégées par FEC avant leur transmission à travers un transport sûr.

Comme la charge utile protégée par cette FEC est faite de paquets RTP, appliquer la FEC sur des charges utiles chiffrées est principalement applicable dans le cas de RTP sécurisé (SRTP) [13]. Comme la FEC applique l'opérateur OUX sur la charge utile, les paquets de FEC devraient être cryptographiquement aussi sûrs que la charge utile originale. Dans de tels cas, un chiffrement supplémentaire des paquets de FEC n'est pas nécessaire.

Dans l'exposé qui suit, on suppose que la FEC est appliquée à la charge utile avant le chiffrement. L'utilisation de la FEC a des implications sur l'usage et le changement des clés de chiffrement. Comme les paquets de FEC consistent en fait en un flux distinct, il y a un certain nombre de combinaisons sur l'usage du chiffrement. Parmi elles :

- Le flux de FEC peut être chiffré, alors que le flux de support ne l'est pas.
- Le flux de support peut être chiffré, alors que le flux de FEC ne l'est pas.
- Le flux de support et le flux de FEC sont tous deux chiffrés, mais utilisent la même clé.
- Le flux de support et le flux de FEC sont tous deux chiffrés, mais utilisent des clés différentes.

Les trois premières exigeraient que tous les protocoles de signalisation de niveau application utilisés aient la capacité d'utiliser la FEC, et donc d'échanger les clés et de négocier l'usage du chiffrement séparément sur le support et sur les flux de FEC. Dans le dernier cas, aucun de ces mécanismes supplémentaires n'est nécessaire. Les deux premiers cas présentent une violation de mise en couche, car les paquets de FEC ULP ne devraient pas être traités différemment des autres paquets RTP. Chiffrer juste un seul flux peut aussi rendre possibles certaines attaques de texte en clair connu. Pour ces raisons, les applications qui utilisent le chiffrement DEVRAIENT chiffrer les deux flux, c'est à dire, les deux dernières options.

De plus, parce qu'il y a un potentiel d'affaiblissement du chiffrement par les relations connues entre la charge utile de support et les données de FEC pour certains chiffrements, des clés de chiffrement différentes DOIVENT être utilisées pour chaque flux lorsque la charge utile de support et les données de FEC sont envoyées dans des flux distincts. Noter que lorsque SRTP [13] est utilisé pour la sécurité des sessions RTP, des clés différentes pour chaque session RTP sont exigées par la spécification SRTP.

Le changement des clés de chiffrement est une autre question cruciale qui doit être réglée. Considérons le cas où deux paquets a et b sont envoyés avec le paquet de FEC qui les protège. Les clés utilisées pour chiffrer a et b sont différentes, et quelle clé devrait donc être utilisée pour décoder le paquet de FEC ? En général, les vieilles clés doivent être mises en antémémoire afin que lorsque les clés changent pour le flux de support, les vieilles clés puissent être utilisées jusqu'à ce qu'il soit déterminé que la clé a changé aussi pour les paquets de FEC ULP. De plus, la nouvelle clé DEVRAIT être utilisée pour chiffrer les paquets de FEC qui sont générés à partir d'une combinaison de paquets de charge utile chiffrés par les clés anciennes et nouvelles. L'envoyeur et le receveur ont besoin de définr comment est effectué le chiffrement et comment sont utilisées les clés.

L'altération des données de FEC et des paquets peut avoir un gros impact sur l'opération de reconstruction. Une attaque qui changerait quelques bits des données de FEC peut avoir un effet significatif sur le calcul et la récupération des paquets de charge utile. Par exemple, changer le champ Longueur de recouvrement peut résulter en la récupération d'un paquet trop long. Aussi, la complexité calculatoire de la récupération peut facilement être affectée jusqu'à au moins un ordre de grandeur. Selon le scénario d'application, il peut être utile d'effectuer un examen de santé de la charge utile et des données de FEC reçues avant d'effectuer l'opération de récupération et de déterminer la validité des données restituées par l'opération de récupération avant de les utiliser.

12. Considérations sur l'encombrement

Un autre problème de l'utilisation de la FEC est son impact sur l'encombrement du réseau. Dans de nombreuses situations, la perte de paquet dans le réseau est produite par les encombrements. Dans de tels scénarios, l'ajout de la FEC lorsque on rencontre une augmentation des pertes du réseau devrait être évité. Si elle est utilisée à grande échelle, il peut en résulter une augmentation de l'encombrement et une défaillance éventuelle due à l'encombrement. Les applications peuvent inclure de plus fortes protections tout en réduisant en même temps la bande passante pour les paquets de charge utile. Dans tous les

cas, les mises en œuvre NE DOIVENT PAS augmenter substantiellement la quantité totale de bande passante utilisée (ce qui inclut la charge utile et la FEC) lorsque les pertes du réseau augmentent.

Les considérations générales sur le contrôle de l'encombrement lors du transport de données RTP s'appliquent; voir RTP [1] et tout profil RTP applicable (par exemple, RTP/AVP [14]). Une exigence supplémentaire si le service au mieux est utilisé est que les utilisateurs de ce format de charge utile DOIVENT surveiller les pertes de paquet pour s'assurer que le taux de perte de paquet reste dans des limites acceptables.
La perte de paquet est considérée comme acceptable si un flux TCP à travers le même chemin de réseau, et rencontrant les mêmes conditions de réseau, réaliserait un débit moyen, mesuré sur une échelle de temps raisonnable, qui ne serait pas inférieur à celui que réalise le flux RTP. Cette condition peut être satisfaite en mettant en œuvre des mécanismes de contrôle d'encombrement pour adapter le taux de transmission (ou le nombre de couches souscrites pour une session de diffusion groupée en couches), ou en s'arrangeant pour qu'un receveur quitte la session si le taux de pertes est trop élevé.

13. Considérations relatives à l'IANA

Quatre nouveaux sous-types de supports ont été enregistrés auprès de l'IANA, comme le décrit la présente section. Cet enregistrement est fait en utilisant le gabarit d'enregistrement [3]et selon la RFC 3555 [4].

13.1 Enregistrement de audio/ulpfec

Nom du type : audio
Nom du sous-type : ulpfec
Paramètres exigés :
taux : c'est le taux d'horodatage RTP qui est utilisé pour marquer l'heure de transmission du paquet de FEC dans un flux séparé. Dans les cas où il est envoyé comme données redondantes à un autre flux, le taux DEVRA être le même que celui du codage principal qu'il sert à protéger. Quand il est utilisé dans un flux séparé, le taux DEVRA être supérieur à 1000 Hz, pour donner une résolution suffisante aux opérations de RTCP. Le taux choisi PEUT être toute valeur supérieure à 1000 Hz mais il est RECOMMANDÉ qu'il corresponde au taux du support que ce flux protège.

Paramètres facultatifs :
unseulniveau : il spécifie si un seul niveau de protection de FEC est utilisé. Les valeurs permises sont 0 et 1. Si 1 est signalé, un seul niveau de protection de FEC DEVRA être utilisé dans le flux. Si 0 est signalé, plus d'un niveau de protection de PEUT être utilisé. S'il est omis, il a la valeur par défaut de 0.

Éléments pour le codage : Ce format est décrit au paragraphe 4.8 du document [3] et contient des données binaires.

Éléments pour la sécurité : Les mêmes considérations pour la sécurité s'appliquent à ces enregistrements de type de support que pour leurs charges utiles, qui sont détaillées dans la RFC 5109.

Éléments pour l'interopérabilité : aucune

Spécification publiée : RFC 5109

Applications qui utilisent ce type de support : applications multi supports qui cherchent à améliorer la résilience à la perte par l'envoi de données supplémentaires avec le flux de support.

Informations supplémentaires : aucune

Nom et adresse de messagerie de la personne à contacter pour des informations complémentaires :
Adam Li adamli@hyervision.com
Groupe de travail Transport audio/vidéo de l'IETF

Utilisation prévue : commune

Restrictions d'utilisation : ce type de support dépend du tramage RTP, et n'est donc défini que pour le transfert via RTP [1]. Le transport au sein d'autres protocoles de tramage NE DEVRA PAS être défini car c'est un mécanisme de robustesse pour RTP.

Auteur : Adam Li adamli@hyervision.com

Contrôleur des changements : Groupe de travail Transport audio/vidéo de l'IETF sur délégation de l'IESG.

13.2 Enregistrement de video/ulpfec

Nom du type : video
Nom du sous-type : ulpfec
Paramètres exigés :
Paramètres exigés :
taux : c'est le taux d'horodatage RTP qui est utilisé pour marquer l'heure de transmission du paquet de FEC dans un flux séparé. Dans les cas où il est envoyé comme données redondantes à un autre flux, le taux DEVRA être le même que celui du codage principal qu'il sert à protéger. Quand il est utilisé dans un flux séparé, le taux DEVRA être supérieur à 1000 Hz, pour donner une résolution suffisante aux opérations de RTCP. Le taux choisi PEUT être toute valeur supérieure à 1000 Hz mais il est RECOMMANDÉ qu'il corresponde au taux du support que ce flux protège.

Paramètres facultatifs :
unseulniveau : il spécifie si un seul niveau de protection de FEC est utilisé. Les valeurs permises sont 0 et 1. Si 1 est signalé, un seul niveau de protection de FEC DEVRA être utilisé dans le flux. Si 0 est signalé, plus d'un niveau de protection de PEUT être utilisé. S'il est omis, il a la valeur par défaut de 0.

Éléments pour le codage : Ce format est décrit au paragraphe 4.8 du document [3] et contient des données binaires.

Éléments pour la sécurité : Les mêmes considérations pour la sécurité s'appliquent à ces enregistrements de type de support que pour leurs charges utiles, qui sont détaillées dans la RFC 5109.

Éléments pour l'interopérabilité : aucune

Spécification publiée : RFC 5109

Applications qui utilisent ce type de support : applications multi supports qui cherchent à améliorer la résilience à la perte par l'envoi de données supplémentaires avec le flux de support.

Informations supplémentaires : aucune

Nom et adresse de messagerie de la personne à contacter pour des informations complémentaires :
Adam Li adamli@hyervision.com
Groupe de travail Transport audio/vidéo de l'IETF

Utilisation prévue : commune

Restrictions d'utilisation : ce type de support dépend du tramage RTP, et n'est donc défini que pour le transfert via RTP [1]. Le transport au sein d'autres protocoles de tramage NE DEVRA PAS être défini car c'est un mécanisme de robustesse pour RTP.

Auteur : Adam Li adamli@hyervision.com

Contrôleur des changements : Groupe de travail Transport audio/vidéo de l'IETF sur délégation de l'IESG.

13.3 Enregistrement de text/ulpfec

Nom du type : text
Nom du sous-type : ulpfec
Paramètres exigés :
Paramètres exigés :
taux : c'est le taux d'horodatage RTP qui est utilisé pour marquer l'heure de transmission du paquet de FEC dans un flux séparé. Dans les cas où il est envoyé comme données redondantes à un autre flux, le taux DEVRA être le même que celui du codage principal qu'il sert à protéger. Quand il est utilisé dans un flux séparé, le taux DEVRA être supérieur à 1000 Hz, pour donner une résolution suffisante aux opérations de RTCP. Le taux choisi PEUT être toute valeur supérieure à 1000 Hz mais il est RECOMMANDÉ qu'il corresponde au taux du support que ce flux protège.

Paramètres facultatifs :
unseulniveau : il spécifie si un seul niveau de protection de FEC est utilisé. Les valeurs permises sont 0 et 1. Si 1 est

signalé, un seul niveau de protection de FEC DEVRA être utilisé dans le flux. Si 0 est signalé, plus d'un niveau de protection de PEUT être utilisé. S'il est omis, il a la valeur par défaut de 0.

Éléments pour le codage : Ce format est décrit au paragraphe 4.8 du document [3] et contient des données binaires.

Éléments pour la sécurité : Les mêmes considérations pour la sécurité s'appliquent à ces enregistrements de type de support que pour leurs charges utiles, qui sont détaillées dans la RFC 5109.

Éléments pour l'interopérabilité : aucune

Spécification publiée : RFC 5109

Applications qui utilisent ce type de support : applications multi supports qui cherchent à améliorer la résilience à la perte par l'envoi de données supplémentaires avec le flux de support.

Informations supplémentaires : aucune

Nom et adresse de messagerie de la personne à contacter pour des informations complémentaires :
Adam Li adamli@hyervision.com
Groupe de travail Transport audio/vidéo de l'IETF

Utilisation prévue : commune

Restrictions d'utilisation : ce type de support dépend du tramage RTP, et n'est donc défini que pour le transfert via RTP [1]. Le transport au sein d'autres protocoles de tramage NE DEVRA PAS être défini car c'est un mécanisme de robustesse pour RTP.

Auteur : Adam Li adamli@hyervision.com

Contrôleur des changements : Groupe de travail Transport audio/vidéo de l'IETF sur délégation de l'IESG.

13.4 Enregistrement de application/ulpfec

Nom du type : application
Nom du sous-type : ulpfec
Paramètres exigés :
Paramètres exigés :
taux : c'est le taux d'horodatage RTP qui est utilisé pour marquer l'heure de transmission du paquet de FEC dans un flux séparé. Dans les cas où il est envoyé comme données redondantes à un autre flux, le taux DEVRA être le même que celui du codage principal qu'il sert à protéger. Quand il est utilisé dans un flux séparé, le taux DEVRA être supérieur à 1000 Hz, pour donner une résolution suffisante aux opérations de RTCP. Le taux choisi PEUT être toute valeur supérieure à 1000 Hz mais il est RECOMMANDÉ qu'il corresponde au taux du support que ce flux protège.

Paramètres facultatifs :
unseulniveau : il spécifie si un seul niveau de protection de FEC est utilisé. Les valeurs permises sont 0 et 1. Si 1 est signalé, un seul niveau de protection de FEC DEVRA être utilisé dans le flux. Si 0 est signalé, plus d'un niveau de protection de PEUT être utilisé. S'il est omis, il a la valeur par défaut de 0.

Éléments pour le codage : Ce format est décrit au paragraphe 4.8 du document [3] et contient des données binaires.

Éléments pour la sécurité : Les mêmes considérations pour la sécurité s'appliquent à ces enregistrements de type de support que pour leurs charges utiles, qui sont détaillées dans la RFC 5109.

Éléments pour l'interopérabilité : aucune

Spécification publiée : RFC 5109

Applications qui utilisent ce type de support : applications multi supports qui cherchent à améliorer la résilience à la perte par l'envoi de données supplémentaires avec le flux de support.

Informations supplémentaires : aucune

Nom et adresse de messagerie de la personne à contacter pour des informations complémentaires :
Adam Li adamli@hyervision.com
Groupe de travail Transport audio/vidéo de l'IETF

Utilisation prévue : commune

Restrictions d'utilisation : ce type de support dépend du tramage RTP, et n'est donc défini que pour le transfert via RTP [1]. Le transport au sein d'autres protocoles de tramage NE DEVRA PAS être défini car c'est un mécanisme de robustesse pour RTP.

Auteur : Adam Li adamli@hyervision.com

Contrôleur des changements : Groupe de travail Transport audio/vidéo de l'IETF sur délégation de l'IESG.

14. Multiplexage de la FEC

Les paquets de FEC peuvent être envoyés au receveur avec la charge utile protégée principalement d'une des deux façons suivantes : dans un flux séparé, ou dans le même flux comme codage redondant. Les options de configuration DOIVENT être indiquées hors bande. La présente section décrit aussi comment cela peut se faire en utilisant le protocole de description de session (SDP), spécifié dans la RFC 2327 [8].

14.1 FEC comme flux séparé

Lorsque les paquets de FEC sont envoyés dans un flux séparé, plusieurs éléments d'informations doivent être convoyés :
- o l'adresse et l'accès auquel la FEC est à envoyer,
- o le numéro de type de charge utile pour la FEC,
- o quel flux de support protège la FEC.

Il n'y a pas d'allocation statique de type de charge utile pour la FEC, de sorte que l'allocation dynamique des numéros de type de charge utile DOIT être utilisée. La SSRC du flux de FEC DOIT être réglée à celle du flux de charge utile protégé. L'association du flux de FEC à son flux correspondant est faite par groupement de ligne dans SDP [5] avec la sémantique de FEC [6] ou d'autre moyens externes.

Suivant les principes exposés au paragraphe 5.2 de la RFC 3550 [1], le multiplexage du flux de FEC et de son flux de charge utile associé est normalement fourni par l'adresse de destination du transport (adresse réseau et numéro d'accès), qui est différent pour chaque session RTP. L'envoi de la FEC avec la charge utile dans une seule session RTP et le multiplexage par le seul SSRC ou type de charge utile empêche : (1) l'utilisation de chemins réseau ou d'allocations de ressources réseau différentes pour la charge utile et les données de protection de FEC; (2) la réception d'un sous ensemble du support si elle est désirée, en particulier pour les hôtes qui ne comprennent pas la FEC ; et (3) les mises en œuvre receveuses qui utilisent un processus distinct pour les différents supports. De plus, le multiplexage de la FEC avec les flux de données de charge utile va affecter la synchronisation et l'espace des numéros de séquence du flux de charge utile original, ce qui est normalement indésirable. Aussi, le flux de FEC et le flux de charge utile DEVRAIENT être envoyés par deux sessions RTP distinctes, et le multiplexage par type de charge utile en une seule session RTP DEVRAIT être évité. De plus, la FEC et la charge utile NE DOIVENT PAS être multiplexées par SSRC en une seule session RTP car elles ont toujours la même SSRC.

Comme tout flux de support, le numéro d'accès et le numéro de type de la charge utile pour le flux de FEC sont convoyés dans leur ligne dans SDP. Il n'y a pas d'allocation statique de type de charge utile pour la FEC, de sorte que l'allocation dynamique des numéros de type de charge utile DOIT être utilisée. La liaison avec le numéro est indiquée par un attribut rtpmap. Le nom utilisé dans cette liaison est "ulpfec". L'adresse sur laquelle est le flux de FEC est convoyée dans sa ligne c correspondante.

La relation d'association entre le flux de FEC et le flux de charge utile qu'il protège est convoyée à travers un groupement de lignes de support dans SDP (RFC 3388) [5] en utilisant la sémantique de FEC (RFC 4756) [6]. Le flux de FEC et le flux de charge utile protégée forment un groupe de FEC.

Ce qui suit est un exemple de SDP pour une application de FEC dans une session de diffusion groupée :

v=0

```
o=adam 289083124 289083124 IN IP4 host.example.com
s=ULP FEC Seminar
t=0 0
c=IN IP4 224.2.17.12/127
a=group:FEC 1 2
a=group:FEC 3 4
m=audio 30000 RTP/AVP 0
a=mid:1
m=application 30002 RTP/AVP 100
a=rtpmap:100 ulpfec/8000
a=mid:2
m=video 30004 RTP/AVP 31
a=mid:3
m=application 30004 RTP/AVP 101
c=IN IP4 224.2.17.13/127
a=rtpmap:101 ulpfec/8000
a=mid:4
```

La présence de deux lignes "a=group" dans cette description de session SDP indique qu'il y a deux groupes de FEC. Le premier groupe de FEC, comme indiqué par la ligne "a=group:FEC 1 2", consiste en un flux 1 (un flux audio utilisant le MIC [14]) et un flux 2 (le flux de FEC protecteur). Le flux de FEC est envoyé au même groupe de diffusion groupée et a la même durée de vie (TTL, *Time to Live*) que le flux audio, mais un numéro d'accès supérieur de deux. Le second groupe de FEC, indiqué par la ligne "a=group:FEC 3 4", consiste en un flux 3 (un flux vidéo) et un flux 4 (le flux de FEC protecteur). Le flux de FEC est envoyé à une adresse de diffusion groupée différente, mais a le même numéro d'accès (30004) que la charge utile du flux vidéo.

14.2 FEC comme codage redondant

Lorsque le flux de FEC est envoyé comme codec secondaire dans le format de codage redondant, cela doit être signalé au moyen de SDP. Pour ce faire, les procédures définies dans la RFC 2198 [7] sont utilisées pour signaler l'utilisation du codage redondant. Le type de charge utile de FEC est indiqué de la même façon que pour tout autre codec secondaire. La FEC DOIT seulement protéger le codec principal, avec la charge utile du moteur de FEC provenant des paquets RTP virtuels créés à partir des données du codec principal. Les paquets RTP virtuels peuvent être très facilement convertis à partir des paquets de la RFC 2198 en simplement : (1) retirant tous les en-têtes supplémentaires et les données de codage redondant, et (2) remplaçant le type de charge utile dans l'en-tête RTP par celui du codec principal.

Note : Dans le format de charge utile pour le codage redondant comme spécifié par la RFC 2198, le bit marqueur est perdu aussitôt que le codage principal est porté dans les paquets RED. Ainsi, le bit marqueur ne peut pas être récupéré, que la FEC soit utilisée ou non.

Parce que les données de FEC (y compris l'en-tête ULP) sont envoyées dans les mêmes paquets que la charge utile protégée, les données de FEC sont associées à la charge utile protégée en étant englobées dans le même flux.

Lorsque le flux de FEC est envoyé comme codec secondaire dans le format de codage redondant, cela peut être signalé au moyen de SDP. Pour ce faire, les procédures définies dans la RFC 2198 [7] sont utilisées pour signaler l'utilisation du codage redondant. Le type de charge utile de FEC est indiqué de la même façon que pour tout autre codec secondaire. Un attribut rtpmap DOIT être utilisé pour indiquer une allocation dynamique de numéro de type de charge utile pour les paquets de FEC. La FEC DOIT ne protéger que le codec principal.

Par exemple:

```
m=audio 12345 RTP/AVP 121 0 5 100
a=rtpmap:121 red/8000/1
a=rtpmap:100 ulpfec/8000
a=fmtp:121 0/5/100
```

Cette description SDP indique qu'il y a un seul flux audio, qui peut comporter du MIC (format de support 0), du DVI (format de support 5), du codage redondant (indiqué par le format de support 121, qui est lié à red par l'attribut rtpmap), ou de la FEC (format de support 100, qui est liée à ulpfec par l'attribut rtpmap). Bien que le format de FEC soit spécifié comme un codage possible pour ce flux, la FEC NE DOIT PAS être envoyée elle-même pour ce flux. Sa présence dans la ligne m n'est exigée que parce que les codecs non principaux doivent être énumérés ici, conformément à la RFC 2198. L'attribut fmtp indique que le format de codage redondant peut être utilisé, avec DVI comme codage secondaire et la FEC

comme codage tertiaire.

14.3 Considération sur l'offre et la réponse

Certaines précautions sont nécessaires lorsque SDP est utilisé pour un échange offre/réponse [15].

Le paramètre "unseulniveau" est déclaratfe. Pour les flux déclarés en envoi seul, la valeur indique si un seul niveau de FEC sera envoyé. Pour les flux déclarés en réception seule ou en envoi/réception, la valeur indique ce que le receveur accepte de recevoir.

Lorsque la FEC est envoyée sur un flux séparé et signalée par un groupement de lignes de supports dans SDP (RFC 3388) [5] utilisant la sémantique de la FEC (RFC 4756) [6], le côté offreur DOIT mettre en œuvre à la fois la RFC 3388 et la RFC 4756. Les règles pour l'offre/réponse dans la RFC 3388 et la RFC 4756 DEVFRONT être suivies avec les précautions supplémentaires suivantes. Pour tous les offreurs avec FEC, le répondant PEUT refuser la session de FEC séparée en réglant l'accès à 0, et retirer l'attribut "a=group" qui groupe cette session de FEC avec la session RTP qui est protégée. Si le répondant accepte l'usage de la FEC, le répondant accepte simplement la FEC de session RTP et le groupage dans l'offre en incluant le même groupage dans la réponse. Noter que le rejet de la FEC de session RTP n'empêche pas les sessions de support d'être acceptées et utilisées sans FEC.

Lorsque le flux de FEC est envoyé comme codec secondaire dans le format de codage redondant (RFC 2198) [7], le côté offreur peut indiquer le flux de FEC comme spécifié au paragraphe 14.2. Le répondant PEUT rejeter le flux de FEC en retirant le type de charge utile pour le flux de FEC. Pour accepter l'usage de la FEC, le répondant doit inclure dans la réponse le type de charge utile de FEC. Noter que dans les cas où le format de redondance de charge utile [7] est utilisé avec la FEC comme le seul codec secondaire, lorsque le flux de FEC est rejeté, le type codage redondant de charge utile DEVRAIT être aussi retiré.

15. Déclaration d'application

Le présent document décrit un protocole générique de correction d'erreur directe qui prend en charge une gamme d'algorithmes de parité de courts blocs de FEC, tels que de codes de parité simples et entrelacés. Le schéma est limité à l'entrelacement de codes de parité sur une distance de 48 paquets. Cet algorithme de FEC est pleinement compatible avec les hôtes qui n'ont pas de capacité de FEC. Comme la charge utile du support n'est pas altérée et que la protection est envoyée comme une information supplémentaire, les receveurs qui ne disposent pas de la capacité de FEC générique, comme spécifié dans le présent document, peuvent simplement ignorer les informations supplémentaires de FEC et traiter la charge utile principale du support. Cette interopérabilité est particulièrement importante pour la compatibilité avec les hôtes existants, et aussi dans le scénario où de nombreux hôtes différents ont besoin de communiquer les uns avec les autres en même temps, comme durant une diffusion groupée.

L'algorithme de FEC générique spécifié dans le présent document est aussi un algorithme de protection générique avec les caractéristiques suivantes : (1) il est indépendant de la nature du support à protéger, que ce support soit audio, vidéo, ou autre ; (2) il est assez souple pour accepter une grande diversité de mécanismes et réglages de FEC ; (3) il est conçu pour s'adapter, de sorte que les paramètres de FEC peuvent être facilement modifiés sans avoir recours à la signalisation hors bande ; et (4) il accepte un certain nombre de mécanismes différents pour le transport des paquets de FEC.

La FEC spécifiée ici fournit aussi à l'utilisateur des capacités de protection d'erreur inégale. D'autres algorithmes peuvent aussi fournir la capacité de protection d'erreur inégale par d'autres moyens. Par exemple, un schéma de protection d'écrasement inégal (UXP, *Unequal Erasure Protection*) a été proposé au groupe de travail AVT dans "Un format de charge utile RTP pour une transmission résiliente à l'écrasement de flux multi supports progressif". Le schéma UXP applique une protection d'erreur inégale aux charges utiles de supports par l'entrelacement du flux de charge utile à protéger avec les informations de redondance supplémentaires obtenues en utilisant des opérations Reed-Solomon.

En altérant la structure de la charge utile du support protégé, le schéma UXP sacrifie la rétro compatibilité avec les terminaux qui ne prennent pas en charge UXP. Cela rend plus difficile d'appliquer UXP lorsque la rétro compatibilite est désirée. Dans le cas de ULP, la charge utile du support reste cependant non altérée et peut toujours être utilisée par les terminaux. La protection supplémentaire peut simplement être ignorée si les terminaux récepteurs n'acceptent pas ULP.

En même temps, et aussi parce que la structure de la charge utile du support est altérée dans UXP, UXP offre la capacité unique de changer la taille du paquet indépendamment de la structure originale de la charge utile du support et de la protection appliquée, et est seulement soumis à la contrainte de redondance du protocole. Cette propriété est utile dans des scénarios où l'altération de la taille de paquet du support est désirée au niveau transport.

À cause de l'entrelacement utilisé dans UXP, des retards vont être introduits à la fois du côté du codage et du décodage. Pour UXP, toutes les données au sein d'un bloc de transmission doivent arriver avant que le codage puisse commencer, et un nombre raisonnable de paquets doit être reçu avant qu'un bloc de transmission puisse être décodé. Le schéma ULP introduit peu de délai du côté du codage. Du côté du décodage, les paquets correctement reçus peuvent être livrés immédiatement. Un retard n'est introduit dans ULP que lorsque surviennent des pertes de paquet.

Comme UXP est un schéma d'entrelacement, les erreurs irrécupérables qui surviennent dans les données protégées par UXP résultent normalement en un certain nombre de trous corrompus dans le flux de charge utile. Dans ULP, d'un autre côté, les erreurs irrécupérables dues à la perte de paquet dans le flux binaire apparaissent normalement comme des pièces manquantes contiguës à la fin des paquets. Selon le codage du flux de charge utile de support, de nombreuses applications peuvent trouver plus aisé d'analyser et d'extraire les données d'un paquet avec seulement une pièce manquante contiguë à la fin d'un paquet plutôt qu'avec plusieurs trous corrompus, en particulier lorsque les trous ne coïncident pas avec les frontières des fragments qui sont décodables indépendamment.

L'opération de vérification de parité du ou exclusif (OUX) utilisée par ULP est plus simple et plus rapide que les opérations plus complexes exigées par les codes Reed-Solomon. Cela fait que ULP convient mieux pour les applications où le coût du calcul est une contrainte.

Comme exposé ci-dessus, les schémas ULP et UXP appliquent tous deux la protection d'erreur inégale au flux de support RTP, mais chacun utilise une technique différente. Les deux schémas ont leurs propres caractéristiques originales, et chacun peut s'appliquer à des scénarios ayant des exigences différentes.

16. Remerciements

Les auteurs suivants ont apporté des contributions significatives au présent document : Adam H. Li, Fang Liu, John D. Villasenor, Dong-Seek Park, Jeong-Hoon Park, Yung-Lyul Lee, Jonathan D. Rosenberg, et Henning Schulzrinne. Les auteurs tiennent aussi à remercier de leurs suggestions de nombreuses personnes dont en particulierStephen Casner, Jay Fahlen, Cullen Jennings, Colin Perkins, Tao Tian, Matthieu Tisserand, Jeffery Tseng, Mark Watson, Stephen Wenger et Magnus Westerlund.

17. Références

17.1 Références normatives

[1] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, RFC 3550, juillet 2003.

[2] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[3] N. Freed et J. Klensin, "Spécifications du type de support et procédures d'enregistrement", BCP 13, RFC 4288, décembre 2005.

[4] S. Casner, "Enregistrement du type de support des formats de charge utile RTP", RFC 4855, février 2007.

[5] G. Camarillo, G. Eriksson, J. Holler et H. Schulzrinne, "Groupage des lignes de support dans le protocole de description de session (SDP)", RFC 3388, décembre 2002.

[6] A. Li, "Sémantique du groupage de correction d'erreur directe dans le protocole de description de session", RFC 4756, novembre 2006.

[7] C. Perkins, I. Kouvelas, O. Hodson, V. Hardman, M. Handley, J. Bolot, A. Vega-Garcia et S. Fosse-Parisis, "Charge utile RTP pour données audio redondantes", RFC 2198, septembre 1997.

[8] M. Handley, V. Jacobson et C. Perkins, "SDP : Protocole de description de session", RFC 4566, juillet 2006.

17.2 Références informatives

[9] J. Rosenberg et H. Schulzrinne, "Format de charge utile RTP pour la correction d'erreur directe générique", RFC 2733, décembre 1999.

[10] C. Perkins et O. Hodson, "Options pour réparer un support de direct", RFC 2354, juin 1998.

[11] J. Rosenberg et H. Schulzrinne, "Enregistrement des types MIME parityfec", RFC 3009, novembre 2000.

[12] M. Luby, L. Vicisano, J. Gemmell, L. Rizzo, M. Handley et J. Crowcroft, "Bloc de construction de correction

d'erreur directe (FEC)", RFC 3452, décembre 2002. *(Rendue obsolète par la RFC 5052)*

[13] M. Baugher, D. McGrew, M. Naslund, E. Carrara et K. Norrman, "Protocole de transport sécurisé en temps réel (SRTP)", RFC 3711, mars 2004.

[14] H. Schulzrinne et S. Casner, "Profil RTP pour conférences audio et vidéo avec contrôle minimal", STD 65, RFC 3551, juillet 2003.

[15] J. Rosenberg et H. Schulzrinne, "Modèle d'offre/réponse avec le protocole de description de session (SDP)", RFC 3264, juin 2002.

Adresse de l'éditeur

Adam H. Li10194 Wateridge Circle #152
San Diego, CA 92121
USA
télephone : +1 858 622 9038
mél : adamli@hyervision.com

Déclaration de copyright

Propriété intellectuelle

Remerciement

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