

Groupe de travail Réseau
Request for Comments : 4164
 Catégorie : Sur la voie de la normalisation
 Traduction Claude Brière de L'Isle

G. Pelletier, Ericsson

août 2005

Compression d'en-tête robuste : duplication de contexte pour profil ROHC

Statut de ce 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 "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.

Notice de copyright

Copyright (C) The Internet Society (2005).

Résumé

Le présent document définit la duplication de contexte, un complément de la procédure d'initialisation de contexte qui se trouve dans la compression d'en-tête robuste (ROHC, *Robust Header Compression*) spécifiée dans la RFC 3095. Les profils qui définissent la prise en charge de la duplication de contexte peuvent utiliser le mécanisme décrit ici pour établir un nouveau contexte fondé sur un autre contexte déjà existant. La duplication de contexte est introduite pour réduire les frais généraux de la procédure d'établissement de contexte. Elle peut être particulièrement utile pour la compression de plusieurs flux de courte durée de vie qui peuvent apparaître simultanément ou presque simultanément, comme des flux TCP de courte durée de vie.

Table des Matières

1. Introduction.....	2
2. Terminologie.....	2
3. Duplication de contexte pour les profils ROHC.....	3
3.1 Considérations de robustesse.....	3
3.2 Duplication des champs de contrôle.....	3
3.3 États et logique de compresseur.....	3
3.3.1 État Duplication de contexte (CR).....	4
3.3.2 Automate à états avec duplication de contexte.....	4
3.3.3 Logique de transition d'état.....	4
3.3.3.1 Sélection du contexte de base, transition vers le haut.....	5
3.3.3.2 Approche optimiste, transition vers le haut.....	5
3.3.3.3 Accusés de réception facultatifs (ACK), transition vers le haut.....	5
3.3.3.4 ACK négatifs (NACK), transition vers le bas.....	5
3.4 Logique de décompresseur.....	6
3.4.1 Duplication et initialisation de contexte.....	6
3.4.2 Reconstruction et vérification.....	6
3.4.3 Actions sur échec.....	6
3.4.4 Logique des retours.....	6
3.5 Formats de paquet.....	7
3.5.1 CRC dans le paquet IR-CR.....	7
3.5.1.1 CRC à 7 bits.....	7
3.5.1.2 CRC à 8 bits.....	7
3.5.2 Format général du paquet IR-CR.....	7
3.5.3 Propriétés de l'identifiant de contexte de base (BCID).....	8
4. Considérations sur la sécurité.....	9
5. Remerciements.....	9
6. Références.....	9
6.1 Références normatives.....	9
6.2 Références pour information.....	9
Appendice A. Format général du paquet IR-CR (pour information).....	9
A.1 Structure générale.....	9
A.2 Information de duplication spécifiques du profil.....	10

Appendice B Duplication de contexte inter profils (pour information).....	10
B.1 Définition de la prise en charge de la duplication de contexte inter profils.....	10
B.2 Compatibilité entre différents profils.....	11
Adresse de l'auteur.....	11
Déclaration complète de droits de reproduction.....	11

1. Introduction

Il y a souvent une certaine redondance entre les champs d'en-tête des différents flux qui passent à travers la même paire de compresseur-décompresseur. Cela signifie que certaines des informations nécessaires pour initialiser le contexte pour décompresser les en-têtes d'un nouveau flux peuvent être déjà présentes au décompresseur. Il peut être souhaitable de réutiliser ces informations et de supprimer une partie des frais généraux normalement exigés pour l'initialisation d'un nouveau contexte de compression d'en-tête au compresseur comme au décompresseur.

Réduire les frais généraux de la procédure d'établissement de contexte est particulièrement utile lorsque plusieurs connexions (ou flux) de courte durée se produisent simultanément, ou presque simultanément, entre la même paire de compresseur-décompresseur. Comme chaque nouveau flux de paquets exige que la plupart des informations d'en-tête soient envoyées durant la phase d'initialisation avant que de plus petits en-tête compressés puissent être utilisés, une multitude de connexions de courte durée peut réduire de façon significative le gain global de la compression d'en-têtes.

La duplication de contexte permet d'omettre certains champs d'en-tête, comme les adresses IP de source et/ou destination (16 octets chacune pour IPv6) dans le type de paquet spécial Initiation et rafraîchissement (IR) spécifiquement défini pour la duplication. Elle permet aussi que d'autres champs soient, comme les accès de source et/ou de destination, soit omis, soit envoyés en forme compressée depuis le tout premier paquet du flux d'en-tête compressé.

La duplication de contexte est définie ici comme un mécanisme ROHC général. Le bénéfice de la duplication de contexte ne se limite pas à un protocole particulier et sa prise en charge peut être définie pour tout profil ROHC.

En particulier, la duplication de contexte est applicable à la compression de TCP parce que de nombreux transferts TCP sont de courte durée de vie ; une analyse du comportement des champs d'en-tête TCP/IP sur de nombreuses connexions de courte durée se trouve dans la [RFC4413]. De plus, la [RFC4163] introduit des considérations et exigences pour le profil ROHC-TCP [RFC4996] pour compresser efficacement de tels transferts TCP à courte durée de vie.

Pour les profils qui prennent en charge ce mécanisme, le compresseur effectue la duplication de contexte en réutilisant ou en créant une copie d'un contexte existant, c'est-à-dire, un contexte de base, pour créer le contexte dupliqué. Le contexte dupliqué est alors mis à jour pour correspondre aux champs d'en-tête du nouveau flux. Le compresseur envoie alors au décompresseur un paquet qui contient une référence au contexte de base choisi, avec des données pour les champs qui doivent être mis à jour lors de la création du contexte dupliqué. Finalement, le décompresseur crée le contexte dupliqué sur la base de la référence au contexte de base avec les données non compressées et compressées du paquet reçu.

Le présent document spécifie la procédure de duplication de contexte pour les profils ROHC. Il définit la logique générale de compresseur et décompresseur utilisée durant la duplication de contexte, ainsi que le format général du paquet IP spécial requis pour cette procédure. Les profils qui définissent la prise en charge de la duplication de contexte doivent spécifier plus en détails le ou les formats spécifiques de ce paquet.

Les fondamentaux du cadre ROHC se trouvent dans la [RFC3095]. On suppose tout au long du présent document qu'ils sont bien compris du lecteur.

2. Terminologie

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

Le présent document réutilise des termes qui se trouvent dans la [RFC3095]. De plus, le présent document définit les termes suivants :

Contexte de base : c'est le contexte qui a été validé par le compresseur et le décompresseur. Le compresseur peut utiliser un contexte de base comme référence lors de la construction d'un nouveau contexte utilisant la duplication.

CID de base (BCID) : l'identifiant de contexte de base est le CID utilisé pour identifier le contexte de base, à partir duquel peuvent être extraites les informations nécessaires pour la duplication de contexte.

Duplication de contexte : c'est le mécanisme qui initialise un nouveau contexte sur la base d'un autre contexte déjà existant (un contexte de base).

3. Duplication de contexte pour les profils ROHC

Pour les profils qui définissent sa prise en charge, la duplication de contexte peut être utilisée comme solution de remplacement à la procédure d'initialisation de contexte de la [RFC3095]. Noter que pour de tels profils, seul le décompresseur est obligé de prendre en charge la duplication de contexte ; l'utilisation du paquet IR-CR est facultative pour le compresseur.

Cette section décrit la logique de compresseur et de décompresseur ainsi que le format général du paquet IR utilisé avec la duplication de contexte.

3.1 Considérations de robustesse

La duplication de contexte diffère de la procédure d'initialisation définie dans la [RFC3095] en ce qu'elle est capable de réaliser un certain niveau de compression à partir du premier paquet utilisé pour initialiser le contexte pour un nouveau flux. Donc, il est d'une particulière importance que la procédure de duplication de contexte soit robuste. Cela exige que soit utilisé un contexte de base convenable pour la duplication, que l'intégrité du paquet d'initialisation soit garantie, et finalement que le résultat du processus de duplication soit vérifié.

Les principaux mécanismes utilisés pour réaliser la robustesse de la procédure de duplication de contexte sont le choix du contexte de base (fondé sur des retours antérieurs du décompresseur) et l'utilisation de sommes de contrôle. Spécifiquement, le compresseur doit avoir une confiance suffisante dans la validité du contexte de base choisi pour la duplication et sa disponibilité au décompresseur avant d'initier la procédure de duplication. Donc, la façon la plus fiable de choisir le contexte de base est de choisir un contexte pour lequel au moins la partie statique à dupliquer a été acquittée préalablement par le décompresseur.

De plus, la présence d'un CRC couvrant les informations qui initialisent le contexte assure l'intégrité de l'en-tête IR utilisé pour la duplication. Finalement, un CRC supplémentaire calculé sur l'en-tête original non compressé permet au décompresseur de valider l'en-tête reconstruit et le résultat du processus de duplication.

3.2 Duplication des champs de contrôle

Les champs de contrôle sont des champs qui sont soit transmis d'un compresseur ROHC à un décompresseur ROHC, soit déduits sur la base du comportement des autres champs, mais ne font pas partie de l'en-tête non compressé lui-même.

Ils peuvent être utilisés pour contrôler le comportement de compression et décompression, en particulier, l'ensemble de formats de paquet à utiliser. Les champs de contrôle sont spécifiques du profil. Des exemples de ces champs incluent les fanions NBO et RND [RFC3095], qui indiquent, respectivement, si le champ IP-ID est dans l'ordre des octets du réseau et le type de comportement du champ. Un autre exemple est le paramètre qui indique le mode de fonctionnement [RFC3095].

Le IR-CR diffère du paquet IR [RFC3095] en ce que son objet est entièrement de spécifier quelle partie du contexte de base est dupliquée et de porter les informations complémentaires nécessaires pour créer un nouveau contexte. À cause de cela, un profil qui prend en charge l'utilisation du paquet IR-CR DEVRAIT définir pour chaque champ de contrôle si la valeur du champ est dupliquée à partir du contexte de base en le nouveau contexte, ou si sa valeur est réinitialisée.

De plus, un compresseur NE DOIT PAS initier la duplication de contexte alors qu'un champ de contrôle qui n'est pas réinitialisé par duplication est mis à jour, par exemple, durant la prise de contact pour une transition de mode [RFC3095].

3.3 États et logique de compresseur

La compression avec ROHC commence normalement dans l'état IR, où les paquets IR doivent être envoyés pour initialiser un nouveau contexte chez le décompresseur. Les paquets IR incluent tous les champs statiques et non statiques de l'en-tête original en forme non compressée plus des informations supplémentaires. Le compresseur reste dans l'état IR jusqu'à ce

qu'il soit sûr que le décompresseur a reçu les informations.

La duplication de contexte fournit un mécanisme facultatif pour compléter la procédure d'initialisation de ROHC. Elle définit un type de paquet, le paquet IR pour la duplication de contexte (IR-CR), qui peut être utilisé pour initialiser un nouveau contexte. Par conséquent, l'état Duplication de contexte (CR) est introduit dans l'automate à états du compresseur pour renfermer la logique supplémentaire exigée pour l'utilisation du paquet IR-CR.

Pour les profils qui définissent la prise en charge de la duplication de contexte, le compresseur peut donc transiter directement de l'état IR à l'état CR si un contexte déjà existant peut être choisi comme contexte de base pour duplication. Ceci remplace effectivement tous les paquets IR/IR-DYN envoyés durant la procédure d'établissement de contexte par un paquet IR-CR.

3.3.1 État Duplication de contexte (CR)

L'objet de l'état CR est d'initialiser un nouveau contexte en réutilisant un contexte déjà existant. Dans cet état, le compresseur envoie une combinaison d'informations non compressées et compressées, avec une référence à un contexte de base plus des informations supplémentaires. Donc, les informations d'en-tête qui relèvent de ces champs à dupliquer ne sont pas envoyées.

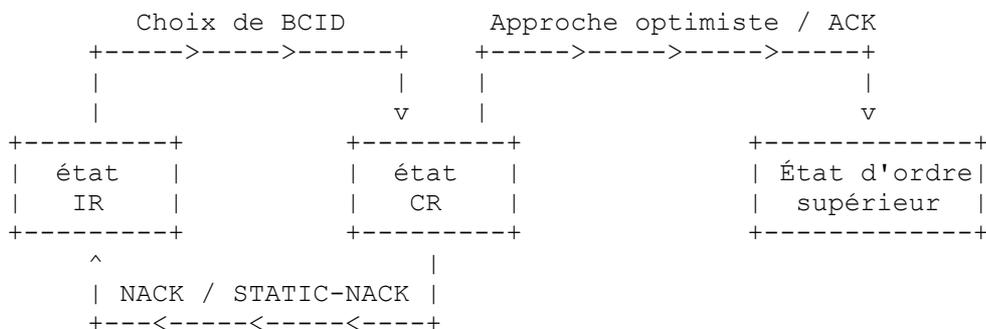
Le compresseur reste dans l'état CR jusqu'à ce qu'il soit sûr que le décompresseur a reçu correctement les informations de duplication.

3.3.2 Automate à états avec duplication de contexte

Le compresseur commence toujours dans l'état de compression inférieur (IR), et transite à l'état de duplication de contexte (CR) sous la contrainte que le compresseur puisse choisir un contexte de base convenable pour le flux à compresser (voir aussi au paragraphe 3.3.3.1).

La transition de l'état CR à un état de compression supérieur (par exemple, l'état CO pour la [RFC4996]) se fonde sur le principe de l'approche optimiste ou sur des retours reçus du décompresseur.

La figure ci-dessous montre l'état supplémentaire pour le compresseur. Les détails des transitions d'état et de logique de compression sont donnés dans les paragraphes qui suivent la figure.



Noter que la duplication de contexte est un complément de la procédure normale d'initialisation pour les profils ROHC qui la prennent en charge. Donc, la transition du compresseur à l'état CR est un ajout facultatif à l'automate à états, et n'affecte pas les transitions déjà existantes entre l'état IR et le ou les états d'ordre supérieur.

3.3.3 Logique de transition d'état

Les décisions sur la transition de et vers l'état CR sont prises au compresseur sur la base de :

- la disponibilité d'un contexte de base
- des retours positifs provenant du décompresseur (accusés de réception -- ACK)
- des retours négatifs provenant du décompresseur (accusés de réception négatifs -- NACK)
- du niveau de confiance concernant la décompression sans erreur d'un paquet

La duplication de contexte est conçue pour opérer sur des liaisons où un canal de retour est disponible. C'est nécessaire pour s'assurer que les informations utilisées pour créer un nouveau contexte sont synchronisées entre le compresseur et le décompresseur. De plus, la duplication de contexte peut aussi utiliser les retours provenant du décompresseur au compresseur pour repasser à l'état IR et pour la transition FACULTATIVE améliorée vers l'avant vers un état à taux de compression supérieur.

Le format qui doit être utilisé par tous les profils pour le champ de retours au sein du format général ROHC est spécifié au paragraphe 5.2.2 de la [RFC3095] ; les informations de retour sont structurées en utilisant deux formats possibles : FEEDBACK-1 et FEEDBACK-2. En particulier, FEEDBACK-2 peut porter un des trois types possibles d'informations de retour : ACK, NACK, ou STATIC-NACK.

3.3.3.1 Sélection du contexte de base, transition vers le haut

Le compresseur peut initier une transition à l'état CR à partir de l'état IR quand un contexte de base convenable peut être identifié. Pour effectuer cette transition, le compresseur choisit un contexte qui a été précédemment acquitté par le décompresseur comme le contexte de base. Le contexte choisi DOIT avoir été acquitté par le décompresseur en utilisant l'option CRC (voir aussi au paragraphe 5.7.6.3 de la [RFC3095]) dans le message de retour. La partie statique du contexte de base à dupliquer DOIT avoir été acquittée par le décompresseur et le contexte de base DOIT être valide au moment de la duplication.

Cela implique aussi qu'il n'est pas permis à un compresseur d'utiliser le mécanisme de duplication de contexte si un canal de retour n'est pas présent. Cependant, on note que la présence du canal de retour ne donne pas la garantie qu'un contexte de base choisi pour duplication n'a pas été corrompu après qu'il a été acquitté, ou qu'il fait toujours partie de l'état géré par le décompresseur quand le IR-CR est reçu.

Plus précisément, la [RFC3095] définit l'identifiant de contexte (CID) comme une référence aux informations d'état (c'est-à-dire, au contexte) utilisé pour la compression et la décompression. Plusieurs flux de paquets, ayant chacun son propre contexte, peuvent donc partager un canal, et l'espace de CID avec sa représentation au sein des formats de paquet peut être négocié au titre de l'état du canal. Cependant, parce que la [RFC3095] ne définit pas explicitement la gestion de l'état de contexte entre le compresseur et le décompresseur, en particulier pour les flux en mode connexion (par exemple, TCP) un seul haut degré de confiance peut être réalisé lors du choix d'un contexte de base.

Dans le cas où les retours ne sont pas utilisés par le décompresseur, le compresseur peut devoir revenir périodiquement à l'état IR. Dans ce cas, la même logique s'applique pour le retour à l'état d'ordre supérieur via l'état CR : un contexte de base, acquitté précédemment et convenable pour la duplication, doit être re-sélectionné.

Les critères selon lesquels un contexte existant est un contexte de base convenable pour la duplication pour un nouveau flux relèvent des mises en œuvre.

Chaque fois que les informations de séquençage provenant du dernier accusé de réception reçu sont disponibles, le compresseur PEUT les utiliser pour déterminer quel champ peut être dupliqué pour éviter de dupliquer des champs qui ont changé de façon significative depuis l'état correspondant au paquet acquitté.

3.3.3.2 Approche optimiste, transition vers le haut

La transition à un état d'ordre supérieur peut être réalisée selon le principe de l'approche optimiste. Cela signifie que le compresseur peut effectuer une transition à l'état supérieur quand il est sûr que le décompresseur a reçu assez d'informations pour décompresser correctement les paquets envoyés conformément à l'état de plus forte compression.

En général, il y a de nombreuses approches où le compresseur peut obtenir de telles informations. Le compresseur peut obtenir cette confiance en envoyant plusieurs paquets IR-CR avec les mêmes informations.

3.3.3.3 Accusés de réception facultatifs (ACK), transition vers le haut

Un ACK peut être envoyé par le décompresseur pour indiquer qu'un contexte a été initialisé avec succès durant la duplication de contexte.

À réception d'un ACK, le compresseur peut supposer que la procédure de duplication de contexte a réussi et transiter de son état initial (par exemple, l'état IR) à un état de compression supérieur.

3.3.3.4 ACK négatifs (NACK), transition vers le bas

Un STATIC-NACK envoyé par le décompresseur peut indiquer que le décompresseur n'a pas pu initialiser un contexte valide durant la duplication de contexte, et que le contexte correspondant a été invalidé.

À réception d'un STATIC-NACK, le compresseur DOIT revenir à son état initial sans contexte. Le compresseur DEVRAIT aussi s'abstenir d'envoyer des paquets IR-CR en utilisant le même contexte de base, au moins jusqu'à ce qu'un accusé de réception suivant la réception du STATIC-NACK rende ce contexte convenable pour la duplication (paragraphe 3.3.3.1). Le

compresseur DEVRAIT réinitialiser le contexte du décompresseur en utilisant un paquet IR.

Un NACK envoyé par le décompresseur peut indiquer qu'un contexte valide a bien été initialisé mais que la décompression d'un ou plusieurs paquets suivants a échoué.

À réception d'un NACK, le compresseur PEUT supposer que la partie statique du contexte du décompresseur est valide, mais que la partie dynamique est invalide ; le compresseur peut agir en conséquence.

3.4 Logique de décompresseur

3.4.1 Duplication et initialisation de contexte

À réception d'un paquet IR-CR, le décompresseur détermine d'abord son contenu (paragraphe 5.2.6 de la [RFC3095]). Le profil indiqué dans le paquet IR-CR détermine comment il sera traité. Si le CRC (de 8 bits) ne vérifie pas le paquet, le paquet DOIT être éliminé.

Si le profil indiqué dans le paquet IR-CR définit l'utilisation du CID de base, et si son champ correspondant est présent avec le format de paquet, ce champ est utilisé pour identifier le contexte de base ; autrement, le CID est utilisé.

3.4.2 Reconstruction et vérification

Le décompresseur crée un nouveau contexte en utilisant les informations présentes dans le paquet IR-CR avec le contexte de base identifié, et décompresse l'en-tête original.

Le CRC calculé sur l'en-tête original non compressé et porté au sein de la partie spécifique du profil des en-têtes IR-CR (CRC de 7 bits) DOIT être utilisé pour vérifier la décompression.

Lorsque la décompression est vérifiée et réussie, le décompresseur initialise ou met à jour le contexte avec les informations reçues dans l'en-tête courant. Le décompresseur DEVRAIT envoyer un ACK quand il réussit à valider le contexte suite à la décompression d'un ou plusieurs paquets IR-CR.

Autrement, si l'en-tête reconstruit échoue à la vérification du CRC, aucun changement (initialisation ou mise à jour) du contexte NE DOIT être effectué. Lorsque le décompresseur ne réussit pas à valider l'en-tête, les actions spécifiées au paragraphe 3.4.3 sont réalisées.

3.4.3 Actions sur échec

Pour les profils qui prennent en charge la duplication de contexte, la logique de retour d'un décompresseur est similaire à celle utilisée pour l'initialisation de contexte, décrite dans la [RFC3095].

Précisément, lorsque le décompresseur échoue à valider le contexte suite à la décompression d'un ou plusieurs paquets IR-CR initiaux, il DOIT invalider le contexte et rester dans son état initial. De plus, le décompresseur DEVRAIT envoyer un STATIC-NACK. En particulier, une mise en œuvre de décompresseur qui effectue une gestion stricte de mémoire, comme la suppression des informations d'état de contexte lorsque elle sait qu'un flux en mode connexion (par exemple, TCP) est terminé, DEVRAIT envoyer un STATIC-NACK dans ce cas. Autrement, il y a un risque que le compresseur conserve un CID spécifique comme candidat potentiel pour une tentative de duplication ultérieure, alors qu'en fait il ne reste pas suffisamment d'état dans le décompresseur pour que ce CID agisse comme CID de base.

Si le contexte a été bien validé à partir de la décompression d'un ou plusieurs paquets initiaux IR-CR, le décompresseur DEVRAIT envoyer un NACK lorsque la vérification du contexte échoue suite à la décompression d'un ou plusieurs paquets IR-CR suivants.

3.4.4 Logique des retours

Le décompresseur DEVRAIT utiliser l'option CRC (voir le paragraphe 5.7.6.3 de la [RFC3095]) lors de l'envoi de retours correspondants à un paquet IR ou IR-CR.

3.5 Formats de paquet

Le format du paquet IR-CR a été conçu avec les contraintes suivantes :

a) il doit être possible soit d'écraser un CID durant la duplication de contexte, soit d'utiliser un CID différent du CID de

- base pour le contexte dupliqué ;
- b) il doit être possible d'inclure ou exclure sélectivement du format de paquet des champs qui peuvent être duplicables ;
- c) il doit être possible que certains champs potentiellement duplicables soient représentés dans le format de paquet en utilisant une forme compressée ou non compressée ;
- d) il doit être possible au décompresseur de vérifier le succès d'une procédure de duplication ;
- e) on prévoit que les profils, autres que ROHC-TCP [RFC4996] définiront aussi la prise en charge de la duplication de contexte. Il est donc souhaitable que le format de paquet soit indépendant du profil.

3.5.1 CRC dans le paquet IR-CR

Le paquet IR, défini dans la [RFC3095], est utilisé pour communiquer les parties statiques et/ou dynamiques d'un contexte, et initialise normalement le contexte. Par exemple, les chaînes statiques et dynamique des paquets IR peuvent contenir une représentation non compressée de l'en-tête original.

Le format du paquet IR inclut un CRC de 8 bits, calculé sur la partie initiale du paquet IR. Ce CRC est destiné à protéger toutes les informations qui initialisent le contexte. En particulier, sa couverture inclut toujours toutes les informations de CID ainsi que le profil utilisé pour interpréter le reste du paquet IR.

L'objet du CRC de 8 bits est de s'assurer de l'intégrité de l'en-tête IR lui-même. Les profils peuvent étendre la couverture de ce CRC pour inclure l'en-tête IR entier, permettant donc la vérification de l'intégrité de l'en-tête non compressé entier. Cependant, comme le format du paquet IR est commun à tous les profils ROHC et vérifié au titre du traitement initial d'un décompresseur ROHC (voir au paragraphe 5.2.6 de la [RFC3095]) les profils ne peuvent pas définir ce CRC au delà de sa couverture.

La [RFC3095] définit aussi un CRC de 3 bits et un CRC de 7 bits pour les en-têtes compressés, utilisés pour vérifier la décompression appropriée et valider le contexte. Ce type de CRC est calculé sur l'en-tête original non compressé, car il n'est pas suffisant pour protéger seulement les données compressées échangées entre le compresseur et le décompresseur pour s'assurer d'une reconstruction robuste de l'en-tête original.

Donc, il y a une claire distinction d'objet entre le CRC de 8 bits qu'on trouve dans le paquet IR et le CRC de 3 bits ou 7 bits qu'on trouve dans les en-têtes compressés. Avec la duplication de contexte, où le paquet IR-CR peut contenir les informations compressées aussi bien que non compressées et omettre entièrement les champs duplicables, cette distinction n'existe plus.

Les profils qui prennent en charge la duplication de contexte DOIVENT définir un CRC sur l'en-tête original non compressé au titre des informations spécifiques de profil dans le paquet IR-CR. C'est nécessaire pour permettre à un décompresseur de vérifier que le processus de duplication a réussi.

3.5.1.1 CRC à 7 bits

Le CRC de 7 bits dans le paquet IR-CR est calculé sur tous les octets de l'en-tête original entier, avant duplication, de la même manière qu'au paragraphe 5.9.2 de la [RFC3095]. Le contenu initial du registre de CRC est pré réglé tout à 1. Le polynôme de CRC utilisé pour le CRC de 7 bits dans l'IR-CR est : $C(x) = 1 + x + x^2 + x^3 + x^6 + x^7$.

3.5.1.2 CRC à 8 bits

La couverture du CRC à 8 bits dans le paquet IR-CR ne dépend pas du profil, par opposition au paquet ROHC IR(-DYN) (voir aux paragraphes 5.2.3 et 5.2.4 de la [RFC3095]). Il DOIT couvrir le paquet entier, sauf la charge utile. En particulier, cela inclut le CID ou tout octet ajouté au CID ainsi que le champ CID de base, si il est présent. Pour les profils qui définissent l'usage du CID de base au sein du format de paquet de l'IR-CR comme facultatif, ce CRC DOIT aussi couvrir les informations utilisées pour indiquer la présence de ce champ dans le paquet. Le contenu initial du registre CRC est d'être pré réglé tout à 1. Le polynôme de CRC utilisé pour le CRC de 8 bits dans le IR-CR est : $C(x) = 1 + x + x^2 + x^8$.

3.5.2 Format général du paquet IR-CR

Le mécanisme de duplication de contexte exige un format de paquet IR dédié qui identifie de façon univoque le paquet IR-CR. Ce paquet communique les parties statiques et dynamiques du contexte dupliqué. Il peut aussi communiquer une référence à un contexte de base.

À l'égard de l'extensibilité du type de paquet IR définie dans la [RFC3095], la prise en charge de la duplication peut être ajoutée en utilisant la partie spécifique du profil du paquet IR. Noter qu'il y a un bit, (x), qui est laissé dans l'en-tête IR pour les "informations spécifiques de profil". La définition de ce bit est spécifique du profil. Donc, les profils qui prennent en

charge la duplication de contexte PEUVENT utiliser ce bit comme un fanion indiquant si le paquet est IR ou IR-CR. Noter aussi que les profils peuvent définir une autre méthode pour identifier le paquet IR-CR au sein des informations spécifiques de profil, au lieu d'utiliser ce bit.

L'en-tête IR-CR associe un CID à un profil, et initialise le contexte en utilisant le mécanisme de duplication de contexte. Il n'est pas recommandé d'utiliser ce paquet pour réparer un contexte endommagé.

Le IR-CR a le format général suivant :

```

  0   1   2   3   4   5   6   7
  ---
:      Octet d'ajout au CID      : pour petits CID et (CID != 0)
+---+---+---+---+---+---+---+
| 1   1   1   1   1   1   0   x | octet de type IR
+---+---+---+---+---+---+---+
:                                  :
/      0-2 octets de CID          / 1-2 octets pour grands CID
:                                  :
+---+---+---+---+---+---+---+
|          Profil                | 1 octet
+---+---+---+---+---+---+---+
|          CRC                   | 1 octet
+---+---+---+---+---+---+---+
|                                |
/Informations spécifiques profil/ longueur variable
|                                |
+---+---+---+---+---+---+---+
|                                |
/      Charge utile              / longueur variable
|                                |
+---+---+---+---+---+---+---+

```

x : Informations spécifiques de profil : interprétées selon le profil indiqué dans le champ Profil.

Profil : profil à associer au CID. Dans le paquet IR-CR, l'identifiant de profil est abrégé aux 8 bits de moindre poids (LSB). Il choisit le plus fort numéro de profil dans le paramètre d'état de canal PROFILES qui correspond aux 8 LSB donnés (voir aussi la [RFC3095]).

CRC : CRC de 8 bits calculé en utilisant le polynôme du paragraphe 3.5.1.2.

Informations spécifiques de profil : le contenu de cette partie du paquet IR-CR est défini par les profils individuels. Ces informations sont interprétées conformément au profil indiqué dans le champ Profil. Il DOIT inclure un CRC de 7 bits sur l'en-tête original non compressé en utilisant le polynôme du paragraphe 3.5.1.1. Il inclut aussi les informations de sous en-tête statique et dynamique utilisées pour la duplication ; donc, les champs d'en-tête qui sont dupliqués et leurs méthodes respectives de codages sortent du domaine d'application du présent document.

Charge utile : c'est la charge utile du paquet original correspondant, si il en est.

3.5.3 Propriétés de l'identifiant de contexte de base (BCID)

Le CID de base au sein du format de paquet de IR-CR peut recevoir une valeur différente de celle de l'identifiant de contexte associé au nouveau flux (c'est-à-dire, BCID != CID) ; autrement, le contexte de base est écrasé avec le nouveau contexte par le processus de duplication.

Lorsque le canal utilise de petits CID, un champ de quatre bits au sein du format de paquet de IR-CR représente de façon minimale le BCID avec une valeur de 0 à 15. En particulier, les quatre bits de Add-CID utilisés avec les petits CID [RFC3095] ne sont pas nécessaires pour le BCID, car ces informations sont déjà fournies par le CID du paquet IR-CR lui-même. Quand de grands CID sont utilisés, le BCID est représenté dans le IR-CR avec un ou deux octets, et il est codé de la même façon que les grands CID [RFC3095].

4. Considérations sur la sécurité

Le présent document ajoute un mécanisme de remplacement pour que les profils ROHC augmentent l'efficacité de leur compression lors de l'initialisation d'un nouveau contexte, en réutilisant les informations déjà existantes au décompresseur. Cela se fait en introduisant une nouvelle logique de transition d'état, une nouvelle logique de retours, et un nouveau type de paquet – tous fondés sur la logique et les formats de paquet déjà définis dans la [RFC3095].

À cet égard, le présent document ne semble pas ajouter de nouvelles faiblesses à de potentielles attaques à celles déjà énumérées dans la [RFC3095]. Cependant, il augmente l'impact potentiel de ces attaques en créant des dépendances entre plusieurs contextes. Spécifiquement, la corruption d'un contexte peut faire échouer les tentatives du compresseur d'initialiser un autre contexte au décompresseur, ou de propager un autre contexte, si le compresseur utilise un contexte corrompu comme base de duplication.

5. Remerciements

L'auteur tient à remercier Richard Price, Kristofer Sandlund, Fredrik Lindstroem, Zhigang Liu, et HongBin Liao de leurs précieux apports, ainsi que Mark West et Lars-Erik Jonsson qui ont également été mandatés par le groupe de travail comme réviseurs du document.

6. Références

6.1 Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (MàJ par [RFC8174](#))
- [RFC3095] C. Bormann et autres, "[Compression d'en-tête robuste](#) (ROHC) : cadre et quatre profils", juillet 2001. (MàJ par [RFC3759](#), [RFC4815](#)) (P.S.)

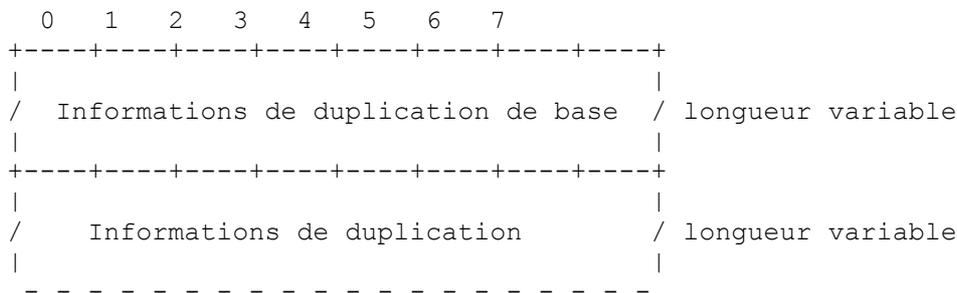
6.2 Références pour information

- [RFC4163] L-E. Jonsson, "Compression d'en-tête robuste (ROHC) : exigences pour la compression d'en-tête TCP/IP", août 2005. (*Information*)
- [RFC4413] M. West, S. McCann, "Comportement du champ TCP/IP", mars 2006. (*Information*)
- [RFC4996] G. Pelletier et autres, "Compression d'en-tête robuste (ROHC) : un profil pour TCP/IP (ROHC-TCP)", juillet 2007. (P.S.)
- [RFC4997] R. Finking, G. Pelletier, "Notation formelle pour la compression d'en-tête robuste (ROHC-FN)", juillet 2007. (P.S.)

Appendice A. Format général du paquet IR-CR (pour information)

A.1 Structure générale

Cette section donne un exemple du format des informations spécifiques du profil au sein du format général de IR-CR.

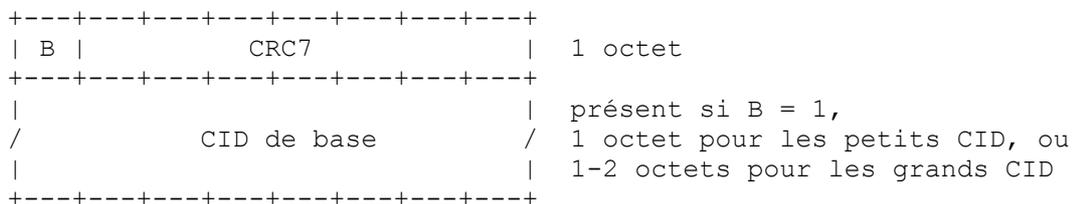


Informations de duplication de base : le contenu de cette partie du paquet IR-CR est défini par les profils individuels. Ces informations sont interprétées conformément au profil indiqué dans le champ Profil. Il DOIT inclure un CRC de 7 bits sur l'en-tête original non compressé en utilisant le polynôme du paragraphe 3.4.1.1. Voir l'Appendice A.2.

Informations de duplication : le contenu de cette partie du paquet IR-CR est aussi défini par les profils individuels. Cette partie contient les informations de sous en-tête statique et dynamique utilisées pour la duplication. Comment ces informations sont structurées est spécifique du profil ; les profils peuvent définir le contenu de ce champ en utilisant une structure de chaîne (chaînes de duplication statiques et dynamiques) ou en définissant des formats d'en-tête pour la duplication (par exemple, ROHC-TCP [RFC4996]).

A.2 Information de duplication spécifiques du profil

Ce paragraphe donne un exemple plus détaillé du format possible du champ d'informations de duplication décrit à l'Appendice A.1.



B : B = 1 indique que le champ CID de base est présent.

CRC7 : CRC sur l'en-tête original non compressé. Ce CRC de 7 bits est calculé selon le paragraphe 3.4.1.1.

CID de base : le CID qui identifie le contexte de base utilisé pour la duplication.

Appendice B Duplication de contexte inter profils (pour information)

La duplication de contexte définie dans le présent document ne prend pas explicitement en charge le concept de duplication de contexte entre les profils. Cependant, il peut être intéressant de développer de nouveaux profils de compression.

La duplication de contexte inter profils exigerait que le décompresseur ait accès aux structures de données provenant du contexte de base, qui appartient à un profil différent de celui qui utilise la duplication. Ces informations devront être rendues disponibles dans un format cohérent avec les structures de données et la ou les méthodes de codage utilisées pour tous les champs d'en-tête qui vont être dupliqués.

B.1 Définition de la prise en charge de la duplication de contexte inter profils

Un profil ROHC décrit comment compresser une pile de protocole spécifique, et inclut un ou plusieurs ensembles de formats de paquets. Les formats de paquets vont normalement compresser les en-têtes de protocole par rapport à un

contexte de valeurs de champs à partir des en-têtes précédents dans un flux. Ce contexte peut aussi contenir des données de contrôle. Donc, les formats de paquets spécifient une transposition entre la version non compressée et la version compressée d'un champ de protocole.

Cette transposition est réalisée par l'utilisation d'une ou plusieurs méthodes de codage, qui sont simplement des fonctions appliquées pour compresser ou décompresser un champ. Une méthode de codage est à son tour définie en utilisant un nom, un ensemble de paramètres de fonction, et une expression formelle (c'est-à-dire, en utilisant le ROHC-FN [RFC4997]) ou une description textuelle (c'est-à-dire, de la [RFC3095]) de son comportement.

Pour compresser un ou plusieurs champs d'une pile de protocole spécifique, différents profils peuvent définir leurs formats de paquet en utilisant différentes méthodes de codage, ou en utilisant une variante d'une technique similaire. Un exemple typique de cette dernière est une compression de liste, comme utilisé pour les en-têtes d'extension IP. Cela implique que les entrées de contexte pour un champ appartenant à une pile de protocole spécifique peuvent différer dans leur contenu, leur représentation, et leur structure d'un profil à l'autre.

Par conséquent, un profil qui prend en charge la duplication de contexte peut seulement utiliser un contexte de base provenant d'un autre profil qui prend explicitement en charge le concept d'un contexte de base. C'est-à-dire, les profils existants qui ne prennent pas en charge ce concept doivent être d'abord mis à niveau pour s'assurer qu'ils peuvent exporter les entrées de données de contexte nécessaires qui utilisent une représentation qui ait un sens durant la duplication.

Précisément, la duplication de contexte inter profils exigerait que les mises en œuvre de décompresseur (y compris celles qui existent) des autres profils soient mises à jour lors de l'ajout de la prise en charge d'un profil qui utilise la duplication de contexte. Donc, la duplication de contexte inter profils ne peut être vue comme un problème spécifique de la mise en œuvre.

Le compresseur doit savoir si le décompresseur supporte la duplication de contexte inter profils avant d'initier la procédure. Le compresseur doit aussi savoir quels contextes (appartenant à quels profils) peuvent être utilisés comme contexte de base. Donc, un compresseur ne peut pas initier la duplication de contexte en utilisant un contexte de base qui appartient à un profil différent, sauf si ce profil fournit explicitement la transposition appropriée pour ses entrées de contexte ou si ce profil est défini formellement comme utilisant ROHC-FN [RFC4997] d'une manière qui rende les deux profils compatibles. L'ensemble des profils négociés pour le canal (voir aussi la [RFC3095]) peut alors être utilisé pour déterminer si un contexte pour un profil spécifique peut être utilisé comme contexte de base.

B.2 Compatibilité entre différents profils

La compatibilité entre profils, lors de la duplication d'un champ pour une pile de protocole particulière, peut être exprimée comme suit : un champ qui est compressé par différents profils est compatible pour la duplication inter profils si il est défini dans l'ensemble des formats de paquets qui utilisent les mêmes fonctions de transposition entre ses versions non compressée et compressée.

Par exemple, le champ Adresse IP de destination qui, sur la base des formats de paquet et des stratégies de compression définies dans la [RFC3095], est implicitement compressé en utilisant une méthode de codage équivalente à la méthode static() définie dans ROHC-FN [RFC4997].

En particulier, pour les profils qui définissent leurs formats de paquets en utilisant une notation formelle telle que ROHC-FN [RFC4997], deux méthodes différentes de codage ne peuvent pas avoir le même nom. Donc, un champ d'une pile de protocole est dit être compatible pour la réplique entre deux profils différents si il a une définition équivalente au sein des formats de paquets respectifs.

Adresse de l'auteur

Ghyslain Pelletier
Box 920
Ericsson AB
SE-971 28 Lulea,
Sweden
téléphone : +46 8 404 29 43
fax : +46 920 996 21
mél : ghyslain.pelletier@ericsson.com

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

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

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

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

Remerciement

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