

Groupe de travail Réseau
Request for Comments : 4170
BCP : 110
Catégorie : Bonnes pratiques actuelles
Traduction Claude Brière de L'Isle

B. Thompson, Cisco Systems
T. Koren, Cisco Systems
D. Wing, Cisco Systems

novembre 2005

Tunnelage de RTP compressé multiplexé

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 décrit une méthode pour améliorer l'utilisation de la bande passante des flux RTP sur les chemins réseau qui portent en parallèle plusieurs flux de protocole de transport en temps réel (RTP, *Real-time Transport Protocol*) entre deux points d'extrémité, comme une jonction vocale. La méthode combine des protocoles standard qui fournissent la compression, le multiplexage, et le tunnelage sur un chemin du réseau afin de réduire la bande passante utilisée lorsque plusieurs flux RTP sont portés sur ce chemin.

Table des Matières

1. Introduction.....	1
1.1 La bande passante est-elle coûteuse ?.....	2
1.2 Revue des protocoles.....	2
1.3 Objet du document.....	2
1.4 Choix de CRTP amélioré.....	2
1.5 Réduire les frais généraux de TCRT.....	2
2. Fonctionnement du protocole et extensions recommandées.....	3
2.1 Modèles.....	3
2.2 Compression d'en-tête : ECRTP.....	3
2.3 Multiplexage de PPP.....	4
2.4 Tunnelage : L2TP.....	5
2.5 Formats d'encapsulation.....	5
3. Efficacité de la bande passante.....	6
3.1 Gains de multiplexage.....	6
3.2 Taux de perte de paquet.....	6
3.3 Calcul de bande passante pour applications vocales et vidéo.....	6
4. Exemple de mise en œuvre de TCRT.....	9
4.1 Négociation suggérée de PPP et L2TP pour TCRT.....	10
4.2 Négociation de PPP pour TCRT.....	10
4.3 Négociation de L2TP.....	11
5. Considérations sur la sécurité.....	11
6. Remerciements.....	12
7. Références.....	12
7.1 Références normatives.....	12
7.2 Références pour information.....	13
Adresse des auteurs.....	13
Déclaration complète de droits de reproduction.....	13

1. Introduction

Le présent document décrit une façon de combiner les protocoles existants pour la compression, le multiplexage, et le tunnelage pour économiser la bande passante pour certaines applications RTP.

1.1 La bande passante est-elle coûteuse ?

Sur certaines liaisons, comme les liaisons d'accès d'abonné, le coût de la bande passante est reconnu largement comme un problème significatif. Des protocoles comme RTP compressé (CRTP, *Compressed RTP*) [RFC2508] conviennent bien pour pallier l'inefficacité en bande passante de protocoles comme VoIP sur ces liaisons.

Ce qui n'est cependant pas reconnu par beaucoup est le coût des liaisons WAN à longue distance. Bien que certaines technologies de voix par paquet comme la voix sur ATM (VoAAL2, [I.363.2]) et la voix sur MPLS assurent l'efficacité de la bande passante (parce que ces deux technologies n'utilisent pas d'en-têtes IP, UDP, et RTP) ni VoATM ni VoMPLS ne fournissent d'accès direct à des services de voix par paquet disponibles pour la voix sur IP. Donc, l'objectif de réduction des coûts de liaison WAN est satisfait au dépens de la perte des opportunités d'interconnexion à d'autres réseaux.

TCRTP résout la discordance de bande passante de VoIP, en particulier pour les grandes applications de jonctions vocales.

1.2 Revue des protocoles

La compression d'en-tête est accomplie en utilisant CRTP amélioré (ECRTP, *Enhanced CRTP*) [RFC3545]. ECRTP est une amélioration du CRTP classique [RFC2508] qui fonctionne mieux sur des liaisons à long délai, comme les liaisons de tunnelage de bout en bout décrites dans le présent document. Cette compression d'en-tête réduit les en-têtes IP, UDP, et RTP.

Le multiplexage est accompli en utilisant le multiplexage PPP [RFC3153].

Le tunnelage PPP est accompli en utilisant L2TP [RFC3931].

CRTP fonctionne liaison par liaison ; c'est-à-dire, pour réaliser la compression sur plusieurs bonds de routeur, CRTP doit être employé deux fois sur chaque routeur -- une fois en entrée, une fois en sortie. À l'opposé, TCRTP décrit dans ce document n'exige aucun traitement supplémentaire par routeur pour réaliser la compression d'en-tête. Les en-têtes sont plutôt compressés de bout en bout, économisant la bande passante sur toutes les liaisons intermédiaires.

1.3 Objet du document

Le présent document est principalement concerné par les économies de bande passante pour les applications de voix sur IP (VoIP, *Voice over IP*) sur des réseaux à forts retards. Cependant, les combinaisons de protocoles décrites dans ce document peuvent être utilisées pour fournir des économies de bande passante similaires pour d'autres applications de RTP comme la vidéo, et les économies de bande passante sont incluses pour un exemple d'application de vidéo.

1.4 Choix de CRTP amélioré

CRTP [RFC2508] décrit l'utilisation de la compression d'en-tête RTP sur un transport de couche liaison non spécifié, mais normalement c'est PPP qui est utilisé. Pour que CRTP comprime les en-têtes, il doit être mis en œuvre sur chaque liaison PPP. Une grande quantité de contexte est requise pour réussir à faire fonctionner CRTP, et les exigences de mémoire et de traitement sont élevées, en particulier si plusieurs bonds doivent mettre en œuvre CRTP pour économiser la bande passante sur chacun des bonds. À des débits de liaison supérieurs, la consommation du processeur de CRTP devient prohibitive.

Pour éviter les coûts par bond de CRTP, une solution simpliste serait d'utiliser CRTP avec L2TP pour réaliser CRTP de bout en bout. Cependant, comme décrit dans la [RFC3545], CRTP ne convient que pour les liaisons avec de faibles retards et peu de pertes. Toutefois, lorsque plusieurs bonds de routeur sont impliqués, les attentes de CRTP en matière de faibles délais et pertes ne peuvent plus être satisfaites. De plus, les paquets peuvent arriver dans le désordre.

Donc, le présent document décrit l'utilisation de CRTP amélioré [RFC3545], qui supporte des retards élevés, la perte de paquet, et la perte de l'ordre entre le compresseur et le décompresseur.

1.5 Réduire les frais généraux de TCRTP

Si un seul flux est tunnelé (L2TP) et compressé (ECRTP), il y a peu d'économies de bande passante. Le multiplexage aide à amortir les frais généraux de l'en-tête de tunnel sur de nombreuses charges utiles RTP. Le format de multiplexage proposé par le présent document est le multiplexage de PPP [RFC3153]. Voir les détails au paragraphe 2.3.

L'ordre des paquets pour RTP est déterminé par le numéro de séquence RTP. Pour augmenter la robustesse en cas de perte de paquet ou de désordre des paquets, ECRTP envoie de courts deltas avec la valeur pleine lors des mises à jour des variables de contexte, et répète les mises à jour dans N paquets, où N est une constante d'ingénierie réglée pour la sorte de tuyau sur laquelle ECRTP est utilisé.

À l'opposé, la [RFC3095] compresse le numéro de séquence et une autre couche est nécessaire pour que la [RFC3095] traite la livraison désordonnée des paquets sur un tunnel [RFC4224].

2.3 Multiplexage de PPP

CRTP et ECRTP exigent tous deux qu'un protocole de couche 2 permette d'identifier les différents protocoles. La [RFC1661] est conçue pour cela.

Lorsque CRTP est utilisé à l'intérieur d'un tunnel, la compression d'en-tête associée à CRTP va réduire la taille des en-têtes IP, UDP, et RTP du paquet IP porté dans le tunnel. Cependant, le tunnel lui-même a des frais généraux à cause de son en-tête IP et de l'en-tête de tunnel (les informations nécessaires pour identifier la charge utile tunnelée). Une façon de réduire les frais généraux d'en-tête IP et d'en-tête de tunnel est de multiplexer plusieurs charges utiles RTP dans un seul paquet tunnelé.

La [RFC3153] décrit une encapsulation qui combine plusieurs charges utiles PPP dans une charge utile multiplexée. Le multiplexage PPP permet de multiplexer tous les types de charge utile PPP pris en charge. Cette trame multiplexée est ensuite portée comme une seule charge utile PPPMUX dans le tunnel IP. Cela permet que plusieurs charges utiles RTP soient portées dans un seul paquet tunnel IP et permet d'amortir les frais généraux des en-têtes non compressés IP et de tunnel sur plusieurs charges utiles RTP.

Durant l'établissement PPP du tunnel TCRTP, seuls LCP et IPCP (pour la compression d'en-tête) sont requis --les adresses IP n'ont pas besoin d'être négociées, et l'authentification n'est pas nécessaire. Voir les détails au paragraphe 4.1.

2.3.1 Modifications de transmetteur PPP multiplex pour le tunnelage

Le paragraphe 1.2 de la [RFC3153] décrit un exemple de procédure de transmission qui peut être utilisé pour mettre en œuvre un émetteur PPP multiplex. La procédure de transmission décrite dans ce paragraphe inclut un paramètre MAX-SF-LEN qui est utilisé pour limiter la taille maximum d'une trame PPP multiplex.

Il y a deux raisons de limiter la taille d'une trame PPP multiplex. D'abord, une trame PPPMUX ne devrait jamais excéder l'unité maximale de réception (MRU, *Maximum Receive Unit*) d'une liaison physique. Ensuite, quand une session PPP et ses contrôles de flux associés sont liés à une liaison physique, le paramètre MAX-SF-LEN forme une limite supérieure à la quantité de temps pendant laquelle un paquet multiplex peut être conservé avant transmission. Quand le contrôle de flux pour l'émetteur PPP multiplex est lié à une liaison physique, le débit d'horloge de la liaison physique peut être utilisé pour tirer les trames de l'émetteur PPP multiplex.

Ce type de contrôle de flux limite la quantité maximale de temps qu'une trame PPP multiplex peut être conservée avant d'être transmise à MAX-SF-LEN / Vitesse de liaison.

Les interfaces de tunnel ne sont normalement pas liées aux interfaces physiques. À cause de cela, une interface de tunnel n'a pas de débit de transmission bien connu qui lui soit associé. Cela signifie que le contrôle de flux dans l'émetteur PPPMUX ne peut pas s'appuyer sur l'horloge d'une liaison physique pour tirer les trames de l'émetteur multiplex. Un temporisateur doit plutôt être utilisé pour limiter le temps pendant lequel une trame PPPMUX peut être conservée avant transmission. Le temporisateur avec le paramètre MAX-SF-LEN devrait être utilisé pour limiter le temps de conservation d'une trame PPPMUX avant sa transmission.

Les extensions à la logique de l'émetteur PPPMUX suivantes devraient être effectuées pour l'utilisation avec des tunnels. La logique de contrôle de flux de l'émetteur PPP devrait être modifiée pour collecter les charges utiles entrantes jusqu'à ce qu'un des deux événements suivants se produise :

- 1 un nombre spécifique d'octets, MAX-SF-LEN, est arrivé au multiplexeur, ou
- 2 un temporisateur, appelé T, est arrivé à expiration.

Lorsque l'une ou l'autre condition est satisfaite, la charge utile PPP multiplexée est transmise.

L'objet de MAX-SF-LEN est de s'assurer qu'une charge utile PPPMUX n'excède pas la taille de la MTU de toute liaison physique possible auquel le tunnel peut être associé. La valeur de MAX-SF-LEN devrait être inférieure ou égale au minimum de MRU-2 (taille maximum du champ Longueur) et 16 383 (14 bits) pour toutes les interfaces physiques possibles auxquelles le tunnel peut être associé.

Le temporisateur T donne la limite supérieure du délai pour les interfaces du tunnel. Le temporisateur T est remis à zéro chaque fois qu'une charge utile multiplexée est envoyée à la prochaine couche d'encapsulation. Le comportement de ce temporisateur est similaire à celui de Timer_CU de AAL2 décrit dans [I.363.2]. Chaque émetteur PPPMUX devrait avoir son propre temporisateur T.

Les valeurs optimales pour T vont varier selon le débit auquel on s'attend que les charges utiles arrivent au multiplexeur et le budget délais pour la fonction de multiplexage. Pour les applications vocales, la valeur de T serait normalement de 5 à 10 millisecondes.

2.3.2 Inefficacités de tunnelage

Pour obtenir une efficacité raisonnable de la bande passante en utilisant le multiplexage au sein d'un tunnel L2TP, plusieurs flux RTP devraient être actifs entre la source et la destination d'un tunnel L2TP.

Si la source et la destination du tunnel L2TP sont les mêmes que la source et la destination des sessions ECRTP, la source et la destination doivent alors avoir plusieurs flux RTP actifs pour tirer parti du multiplexage.

À cause de cette limitation, TCRTP est surtout utile pour les applications où de nombreuses sessions RTP fonctionnent entre une paire de points d'extrémité RTP. Le nombre de sessions RTP simultanées RTP requis pour réduire les frais généraux d'en-tête au niveau désiré dépend de la taille de l'en-tête L2TP. Un plus petit en-tête L2TP va résulter en une exigence de moins de sessions RTP simultanées pour produire une efficacité de bande passante similaire à celle de CRTP.

2.4 Tunnelage : L2TP

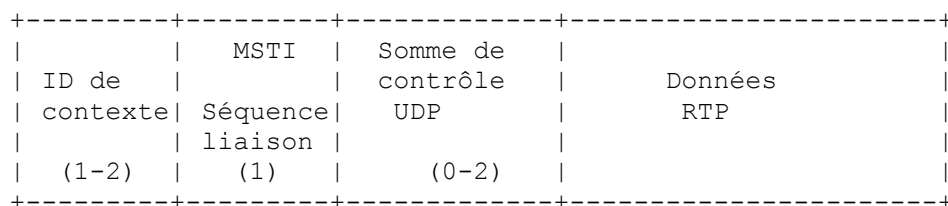
Les tunnels L2TP devraient être utilisés pour tunneler les charges utiles ECRTP de bout en bout. L2TP inclut des méthodes pour tunneler les messages utilisés dans l'établissement de session PPP, comme NCP. Cela permet selon la [RFC3544] de négocier les paramètres de compression/décompression ECRTP.

2.4.1 Tunnelage et DiffServ

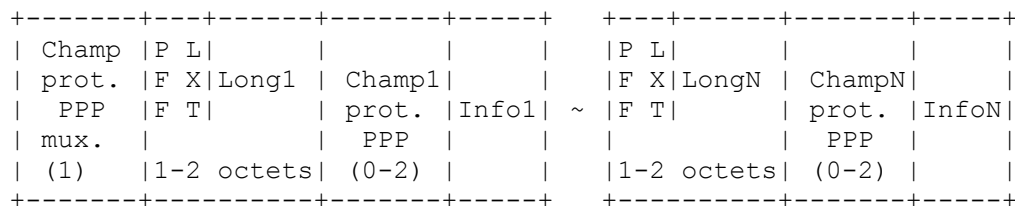
Les flux RTP peuvent être marqués avec les bits Expedited Forwarding (EF), comme décrit dans la [RFC3246]. Quand un tel paquet est tunnelé, l'en-tête de tunnel doit aussi être marqué par les mêmes bits EF, comme exigé par la [RFC3246]. Il est important de ne pas mélanger le trafic EF et non EF dans le même tunnel multiplexé marqué EF.

2.5 Formats d'encapsulation

Le format de paquet pour RTP, compressé avec la compression d'en-tête RTP définie dans ECRTP, est :



Le format de paquet d'un paquet PPP multiplexé comme défini par la [RFC3153] est :



Le format combiné utilisé pour TCRTP avec une seule charge utile est tous les paquets ci-dessus enchaînés. Voici un exemple avec une seule charge utile :

En-tête	Champ	PL			MSTI	Somme de	
IP	proto.	FX	Long1	Champ1	ID	contrôle	Données
(20)	mux.	FT		proto.	contexte	Séqu.	UDP
	(1)	1-2 octets	(0-2)	(1-2)	(1)	(0-2)	
<----- Charge utile IP ----->							
<----- Charge utile PPPmux ----->							

Si le tunnel contient du trafic multiplexé, plusieurs "charges utiles PPPMux" sont transmises dans un paquet IP.

3. Efficacité de la bande passante

L'efficacité attendu de bande passante atteignable avec TCRTP dépend d'un certain nombre de facteurs. Ces facteurs incluent le gain de multiplexage, le taux attendu de perte de paquets à travers le réseau, et les taux de changement des champs spécifiques au sein des en-têtes IP et RTP. Cette section décrit aussi comment TCRTP améliore significativement l'efficacité de la bande passante pour la voix sur IP sur ATM.

3.1 Gains de multiplexage

Le multiplexage réduit les frais généraux associés aux en-têtes de couche 2 et de tunnel. Augmenter le nombre de charges utiles CRTP combinées en une charge utile PPP multiplexée augmente le gain du multiplexage. Lorsque le trafic augmente au sein d'un tunnel, plus de charges utiles sont combinées dans une charge utile multiplexée. Cela va augmenter le gain du multiplexage.

3.2 Taux de perte de paquet

La perte d'un paquet multiplexé cause la perte de paquet pour tous les flux au sein du paquet multiplexé.

Quand le taux de perte attendu dans un tunnel est relativement faible (moins peut-être que 5 %) le fonctionnement robuste (décrit dans la [RFC3545]) devrait être suffisant pour assurer la livraison des changements d'état. Ce fonctionnement robuste est caractérisé par un paramètre N, qui signifie que la probabilité de perte de plus de N paquets adjacents sur le tunnel est faible.

Une valeur de N=1 va protéger contre la perte d'un seul paquet au sein d'une session compressée, au dépens de la bande passante. Une valeur de N=2 va protéger contre la perte de deux paquets à la suite dans une session compressée et ainsi de suite. De plus fortes valeurs de N ont une plus forte contrepartie en bande passante.

La valeur optimale de N va dépendre du taux de perte dans le tunnel. Si le taux de pertes est élevé (peut-être de plus de 5 %) des techniques plus avancées doivent être employées. Ces techniques sortent du domaine d'application de ce document.

3.3 Calcul de bande passante pour applications vocales et vidéo

La formule suivante utilise les facteurs décrits ci-dessus pour modéliser l'usage par flux de la bande passante pour les applications vocales et vidéo. Les variables suivantes sont définies :

SOV-TCRTP, en octets : frais généraux par charge utile de ECRTP et de l'en-tête PPP multiplexé. Cette valeur n'inclut pas les frais généraux supplémentaires de mise à jour des champs ID IP ni Horodatage RTP (voir les détails dans la [RFC3545] pour l'identifiant IP). La valeur suppose l'utilisation du type de charge utile COMPRESSED_RTP. Elle consiste en 1 octet pour l'identifiant de contexte ECRTP, 1 octet pour les fanions COMPRESSED_RTP, 2 octets pour la somme de contrôle UDP, 1 octet pour l'identifiant de protocole PPP, et 1 octet pour le champ Longueur PPP multiplexée. Le total fait 6 octets.

POV-TCRTP, en octets : frais généraux par paquet de ECRTP tunnelé. Ce sont les frais généraux de l'en-tête de tunnel et le type de charge utile PPP multiplexée. Cette valeur fait 20 octets pour l'en-tête IP, 4 octets pour l'en-tête L2TPv3 et un octet pour l'identifiant de protocole PPP multiplexé. Le total fait 25 octets.

TRANSMIT-LENGTH, en millisecondes : durée moyenne d'une transmission (comme une salve de parole pour les flux vocaux).

SOV-TSTAMP, en octets : frais généraux supplémentaires par charge utile de l'en-tête COMPRESSED_UDP qui inclut le champ Horodatage absolu. Cette valeur inclut 1 octet pour le champ de fanions supplémentaire dans l'en-tête COMPRESSED_UDP et 4 octets pour l'horodatage absolu, soit un total de 5 octets.

SOV-IPID, en octets : frais généraux supplémentaires par charge utile de l'en-tête COMPRESSED_UDP qui inclut le champ IPID absolu. Cette valeur inclut 2 octets pour l'IPID absolu. Elle inclut aussi 1 octet pour le champ de fanions supplémentaire dans l'en-tête COMPRESSED_UDP. Le total fait 3 octets.

IPID-RATIO, valeurs d'entier 0 ou 1 : indique la fréquence de mise à jour de l'IPID par le compresseur. Si l'IPID change au hasard et a donc toujours besoin d'être mis à jour, la valeur est 1. Si l'IPID change d'une quantité fixe constante entre les charges utiles d'un flux, IPID-RATIO sera alors 0. La valeur de cette variable ne prend pas en considération la valeur de l'IPID au début d'une transmission vocale ou vidéo, car elle est prise en compte par la variable TRANSMIT-LENGTH. La mise en œuvre de la pile IP d'envoi et de l'application RTP contrôle ce comportement.. Voir au paragraphe 1.1.

NREP, entier (généralement entre 1 et 3) : c'est le nombre de fois que sera répété un champ de mise à jour dans les en-têtes ECRTP pour augmenter le taux de livraison entre le compresseur et le décompresseur. Pour cet exemple, on suppose NREP=2.

PAYLOAD-SIZE, en octets : taille de la charge utile RTP en octets.

MUX-SIZE, entier : nombre de charge utiles PPP multiplexées dans une charge utile PPP multiplexée.

SAMPLE-PERIOD, en millisecondes ; délai moyen entre les transmissions de charges utiles de voix ou vidéo pour chaque flux dans le multiplex. Par exemple, dans les applications vocales, la valeur de cette variable serait de 10 ms si tous les appels ont une période d'échantillonnage de 10 ms.

La formule est :

$$\text{SOV-TOTAL} = \text{SOV-TCRTP} + \text{SOV-TSTAMP} * (\text{NREP} * \text{SAMPLE-PERIOD} / \text{TRANSMIT-LENGTH}) + \text{SOV-IPID} * \text{IPID-RATIO}$$

$$\text{BANDWIDTH} = ((\text{PAYLOAD-SIZE} + \text{SOV-TOTAL} + (\text{POV-TCRTP} / \text{MUX-SIZE})) * 8) / \text{SAMPLE-PERIOD}$$

Le résultat est :

BANDWIDTH, en kilobit/s : bande passante moyenne utilisée par flux vocal ou vidéo.

SOV-TOTAL = quantité totale de frais généraux par charge utile associée à ECRTP tunnelé. Elle inclut les frais généraux par charge utile de ECRTP et PPP, les frais généraux de mise à jour d'horodatage, et ceux de mise à jour de l'IPID.

3.3.1 Exemple de calcul de bande passante vocale

Pour créer un exemple pour une application vocale utilisant les formules ci-dessus, on suppose le scénario d'utilisation suivant. Des flux vocaux compressés utilisent la compression G.729 avec une période de mise en paquets de 20 ms. Dans ce scénario, VAD est activé et la longueur moyenne de salve de parole est de 1500 ms. Le champ IPID change de façon aléatoire entre les charges utiles des flux. Il y a assez de trafic dans le tunnel pour permettre trois charges utiles multiplexées. On applique les valeurs suivantes :

SAMPLE-PERIOD = 20 ms

TRANSMIT-LENGTH = 1500 ms

IPID-RATIO = 1

PAYLOAD-SIZE = 20 octets

MUX-SIZE = 3

Pour cet exemple, la bande passante par appel est de 16,4 kbit/s. Le CRTP classique sur une seule liaison HDLC utilisant les mêmes facteurs donne 12,4 kbit/s.

L'effet de l'IPID peut être grand sur la bande passante par appel. Si l'exemple ci-dessus est recalculé en utilisant un IPID-

RATIO de 0, la bande passante par appel est alors réduite à 13,8 kbit/s. Le CRTP classique sur une seule liaison HDLC, en utilisant ces mêmes facteurs, donne 11,2 kbit/appel.

3.3.2 Tableau de comparaison de bande passante vocale

Les valeurs de bande passante sont les suivantes quand on utilise cinq appels simultanés, pas de détection d'activité vocale (VAD, *voice activity detection*), G.729 avec intervalle de mise en paquet de 20 ms, et pas de prise en compte de frais généraux RTCP :

VoIP sur PPP normal : 124 kbit/s

avec CRTP classique sur une liaison : 50 kbit/s (économise 59 %)

avec TCRTP sur PPP : 62 kbit/s (économise 50 %)

avec TCRTP sur AAL5 : 85 kbit/s (économise 31 %)

3.3.3 Exemple de calcul de bande passante vidéo

Comme TCRTP peut être utilisé pour économiser de la bande passante sur tout type de flux encapsulé RTP, il peut être utilisé pour économiser de la bande passante pour les applications de vidéo. Ce paragraphe donne un exemple d'économies de bande passante fondées sur TCRTP pour de la vidéo codée en MPEG-2.

Pour créer un exemple d'application vidéo utilisant les formules ci-dessus, on supposera le scénario d'utilisation suivant. L'encapsulation RTP des flux système et de transport MPEG est effectuée comme décrit dans la RFC 2250. Les trames de vidéo codées en MPEG-2 sont envoyées en continu, de sorte que la variable TRANSMIT-LENGTH dans la formule de bande passante est essentiellement infinie. Le champ IPID change au hasard entre les charges utiles de flux. Il y a assez de trafic dans le tunnel pour permettre de multiplexer trois charges utiles. On applique les valeurs suivantes :

SAMPLE-PERIOD = 2,8 ms

TRANSMIT-LENGTH = infini

IPID-RATIO = 1

PAYLOAD-SIZE = 1316 octets

MUX-SIZE = 3

Pour cet exemple, la bande passante par flux est de 3,8 Mbit/s. La vidéo MPEG sans compression d'en-tête, utilisant les mêmes facteurs que ci-dessus donne 3,9 Mbit/s. Bien que TCRTP fournisse bien quelques économies de bande passante pour la vidéo, le ratio de transmission des en-têtes sur charge utile est si faible que les économies de bande passante sont insignifiantes.

3.3.4 TCRTP sur ATM

Le transport IP sur AAL5 cause un effet de quantification sur l'utilisation de la bande passante dû à ce que les paquets sont toujours des multiples de cellules ATM.

Par exemple, la taille de charge utile pour G.729 en utilisant des intervalles de mise en paquet de 10 millisecondes est de 10 octets. C'est beaucoup moins que la taille de charge utile d'une cellule ATM (48 octets). Lorsque le CRTP classique [RFC2508] est utilisé sur la base de la liaison, le ratio des frais généraux IP sur la charge utile est assez bon. Cependant, l'encapsulation AAL5 et son bourrage de cellule force toujours la taille minimum de charge utile à être d'une cellule ATM, ce qui résulte en une mauvaise utilisation de la bande passante.

Au lieu de gâcher ce bourrage, le multiplexage de TCRTP permet que ce gaspillage d'espace de la cellule ATM serve à contenir des données utiles. C'est une des principales raisons pour lesquelles le multiplexage a un si grand effet sur l'utilisation de la bande passante avec la voix sur IP sur ATM.

Cette efficacité du multiplexage de TCRTP est similaire au multiplexage de sous cellule AAL2 décrit dans [I.363.2]. À la différence du multiplexage de sous cellule AAL2, l'efficacité du multiplexage de TCRTP n'est cependant pas limitée aux seuls réseaux ATM.

3.3.5 TCRTP sur réseau non ATM

Lorsque TCRTP est utilisé avec d'autres encapsulations de couche 2 qui n'ont pas de taille minimum de PDU, le bénéfice du multiplexage n'est pas aussi grand.

Selon les frais généraux exacts de l'encapsulation de couche 2, le bénéfice du multiplexage peut être légèrement meilleur ou moins bon que la compression d'en-tête CRTP liaison par liaison. Les frais généraux par charge utile du tunnelage CRTP

sont de 4 ou 6 octets. Si le CRTP classique plus les frais généraux de couche 2 est supérieur à cette quantité, le multiplexage TCRTP va consommer moins de bande passante que le CRTP classique quand l'en-tête IP externe est amortis sur un grand nombre de charges utiles.

Le seuil de rentabilité de la charge utile peut être déterminé avec la formule suivante :

$$POV-L2 * MUX-SIZE \geq POV-L2 + POV-TUNNEL + POV-PPPMUX + SOV-PPPMUX * MUX-SIZE$$

Où :

POV-L2, en octets ; frais généraux du paquet de couche 2 : 5 octets pour l'encapsulation HDLC

POV-TUNNEL, en octets ; frais généraux du paquet dus au tunnelage : 24 octets d'en-tête IP et d'en-tête L2TPv3

POV-PPPMUX, en octets ; frais généraux du paquet pour l'identifiant de protocole PPP multiplexé : 1 octet

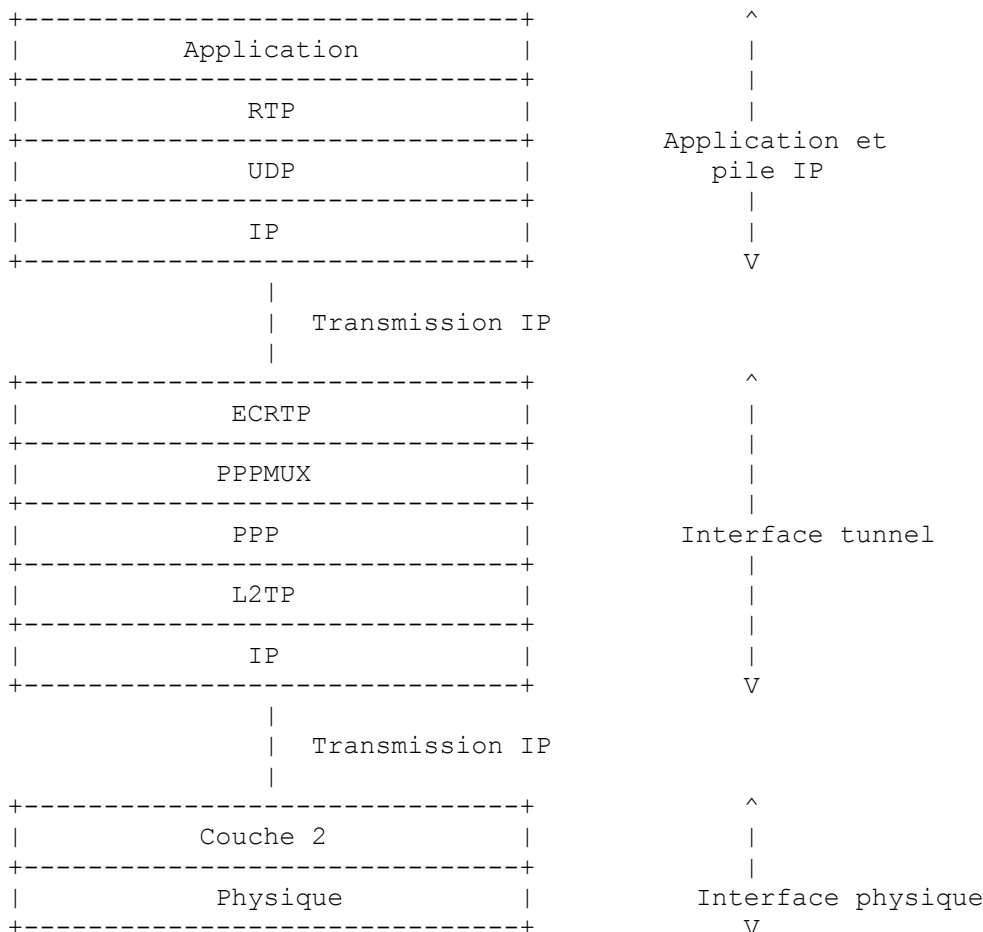
SOV-PPPMUX, en octets ; frais généraux par charge utile de PPPMUX, qui se compose du champ Longueur de charge utile et de l'identifiant de protocole ECRTP. La valeur de SOV-PPPMUX est normalement 1, 2, ou 3.

Si on utilise HDLC comme protocole de couche 2, le seuil de rentabilité (en utilisant la formule ci-dessus) est quand MUX-SIZE = 7. Donc, 7 flux vocaux ou vidéo doivent être multiplexés pour rendre TCRTP aussi efficace en bande passante que la compression CRTP liaison par liaison.

4. Exemple de mise en œuvre de TCRTP

Cette section décrit un exemple de mise en œuvre de TCRTP. Les mises en œuvre de TCRTP peuvent être faites de nombreuses façons pour autant que les exigences des RFC associées sont satisfaites.

Voici le chemin que prend un paquet RTP dans cette mise en œuvre :



Une pile de protocole est configurée pour créer une interface de tunnel L2TP vers un hôte de destination. Le tunnel est configuré à négocier la connexion PPP (en utilisant NCP IPCP) avec compression d'en-tête ECRTTP et PPPMUX. La transmission IP est configurée à acheminer les paquets RTP à ce tunnel. Le numéro d'accès UDP de destination pourrait distinguer les paquets RTP des paquets non RTP.

L'application de transmission rassemble les données RTP provenant d'une source, et formate un paquet RTP. Les couches d'application de niveau inférieur ajoutent les en-têtes UDP et IP pour former un paquet IP complet.

Les paquets RTP sont acheminés à l'interface du tunnel où les en-têtes sont compressés, les charges utiles sont multiplexées, et ensuite les paquets sont tunnelés à l'hôte de destination.

Le fonctionnement du nœud receveur est, inversé, le même que celui du nœud émetteur.

4.1 Négociation suggérée de PPP et L2TP pour TCRTTP

Ce paragraphe décrit les négociations PPP et L2TP nécessaires pour établir une connexion PPP et un tunnel L2TP avec compression d'en-tête L2TP. La négociation est entre deux homologues : Peer1 et Peer2.

4.2 Négociation de PPP pour TCRTTP

Le protocole point à point est décrit dans la [RFC1661].

4.2.1 Négociation de LCP

Le protocole de commande de liaison (LCP, *Link Control Protocol*) est décrit dans la [RFC1661].

4.2.1.1 Établissement de liaison

Peer1	Peer2
Configure-Request (pas d'option)- ->	
	<- Configure-Ack <- Configure-Request (pas d'option)
Configure-Ack ----->	

4.2.1.2 Suppression de liaison

Terminate-Request ----->	Terminate-Ack <-----
--------------------------	-------------------------

4.2.2 Négociation de IPCP

L'échange de protocole est décrit dans les [RFC2507], [RFC1661], et [RFC3545].

Peer1	Peer2
Configure-Request ----->	
Options :	
IP-Compression-Protocol	
Utiliser le protocole 0x61 et les sous paramètres comme décrit dans [RFC3544] et [RFC3545]	
	<---- Configure-Ack <---- Configure-Request Options: IP-Compression-Protocol Utiliser le protocole 0x61 et les sous paramètres comme décrit dans [RFC3544] et [RFC3545]
Configure-Ack ----->	

4.3 Négociation de L2TP

L2TP est décrit dans la [RFC3931].

4.3.1 Établissement de tunnel

```
Peer1                               Peer2
SCCRQ ----->
AVP obligatoires :
Type de message
Version de protocole
Nom d'hôte
Capacités de tramage
Identifiant de tunnel alloué

<--- SCCRQ
AVP obligatoires :
Type de message
Version de protocole
Nom d'hôte
Capacités de tramage
Identifiant de tunnel alloué

SCCCN ----->
AVP obligatoires :
Type de message

<--- ZLB
```

4.3.2 Établissement de session

```
Peer1                               Peer2
ICRQ ----->
AVP obligatoires :
Type de message
Identifiant de session alloué
Numéro de série d'appel

<--- ICRP
AVP obligatoires :
Type de message
Identifiant de session alloué

ICCN ----->
AVP obligatoires :
Type de message
Émission (vitesse de connexion)
Type de tramage

<--- ZLB
```

4.3.3 Suppression de tunnel

```
Peer1                               Peer2
StopCCN ----->
AVP obligatoires :
Type de message
Identifiant de session alloué
Code de résultat

<---
ZLB
```

5. Considérations sur la sécurité

Le présent document décrit une méthode pour combiner plusieurs protocoles existants qui mettent en œuvre la compression, le multiplexage, et le tunnelage de flux RTP. Les attaques sur les technologies composantes de TCRTP

incluent des attaques sur les en-têtes et les charges utiles RTP/RTCP portés dans la session TCRTCP, des attaques sur les en-têtes compressés, des attaques sur la couche de multiplexage, ou des attaques sur la négociation ou le transport du tunnelage. Les problèmes de sécurité associés individuellement à chacune des technologies composantes sont traités par les spécifications respectives, [RFC3545], [RFC3153], [RFC3931], ainsi que dans les considérations sur la sécurité pour RTP lui-même [RFC3550].

Cependant, il peut y avoir des problèmes de sécurité supplémentaires découlant de l'utilisation conjointe de ces technologies composantes. Par exemple, il peut y avoir une augmentation du risque de mauvaise livraison non intentionnelle de paquets provenant d'un flux du multiplex à un autre à cause d'un dysfonctionnement du protocole ou d'erreurs de données à cause de la plus grande condensation des informations d'adressage. Ceci est particulièrement vrai si le tunnel est transmis sur un protocole de couche liaison qui permet la livraison de paquets contenant des erreurs binaires, en combinaison avec une option de tunnel de couche transport qui ne fait pas de somme de contrôle sur toutes les charges utiles.

L'opportunité de mauvaises directions malveillantes peut être accrue par rapport à celles d'un seul flux RTP transporté par lui-même, parce que les informations d'adressage doivent être non chiffrées pour que fonctionnent la compression d'en-tête et les couches de multiplexage.

La principale défense contre la mauvaise livraison est de rendre les données inutilisables aux receveurs imprévus, par des techniques cryptographiques. La méthode de base pour le chiffrement fournie dans la spécification RTP [RFC3550] ne convient pas parce qu'elle chiffre les en-têtes RTP et RTCP ainsi que la charge utile. Cependant, la spécification RTP permet aussi de définir d'autres approches dans des spécifications séparées de profil ou de format de charge utile selon lesquelles seule la portion charge utile du paquet sera chiffrée ; donc, la compression d'en-tête peut s'appliquer aux paquets chiffrés. Un tel profil, [RFC3711], fournit des méthodes pour le chiffrement et l'authentification de message plus sophistiquées et complètes que l'approche de base de la [RFC3550]. Des méthodes supplémentaires peuvent être développées à l'avenir. Une protection cryptographique appropriée devrait être incorporée dans toutes les applications TCRTCP.

6. Remerciements

Nous tenons à remercier les auteurs de la RFC 2508, Stephen Casner et Van Jacobson, et les auteurs de la RFC 2507, Mikael Degermark, Bjorn Nordgren, et Stephen Pink.

Les auteurs tiennent aussi à remercier Dana Blair, Alex Tweedley, Paddy Ruddy, Francois Le Faucheur, Tim Gleeson, Matt Madison, Hussein Salama, Mallik Tatipamula, Mike Thomas, Mark Townsley, Andrew Valencia, Herb Wildfeuer, J. Martin Borden, John Geevarghese, et Shoou Yiu.

7. Références

7.1 Références normatives

- [RFC1661] W. Simpson, éditeur, "[Protocole point à point](#) (PPP)", STD 51, juillet 1994. (*MàJ par la RFC2153*)
- [RFC2507] M. Degermark, B. Nordgren, S. Pink, "[Compression d'en-tête IP](#)", février 1999. (*P.S.*)
- [RFC2508] S. Casner, V. Jacobson, "[Compression d'en-têtes IP/UDP/RTP pour liaisons séries à bas débit](#)", février 1999. (*P.S.*)
- [RFC3153] R. Pazhyannur, I. Ali, C. Fox, "[Multiplexage en PPP](#)", août 2001. (*P.S.*)
- [RFC3246] B. Davie et autres, "[Comportement par bond de transmission accélérée](#)", mars 2002. (*P.S.*)
- [RFC3544] T. Koren, S. Casner, C. Bormann, "[Compression d'en-tête IP sur PPP](#)", juillet 2003. (*Remplace RFC2509*) (*P.S.*)
- [RFC3545] T. Koren et autres, "[RTP compressé amélioré](#) (CRTP) pour liaisons avec retard élevé, perte de paquet et réarrangement", juillet 2003. (*P.S.*)
- [RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "[RTP : un protocole de transport pour les applications](#)

en temps réel", STD 64, juillet 2003. (MàJ par [RFC7164](#), [RFC7160](#), [RFC8083](#), [RFC8108](#))

[RFC3931] J. Lau et autres, "[Protocole de tunnelage de couche deux](#) - version 3 (L2TPv3)", mars 2005. (P.S.)

[I.363.2] Recommandation UIT-T I.363.2, "Spécification de la couche d'adaptation ATM RNIS-LB : AAL type 2", septembre 1997.

7.2 Références pour information

[RFC3095] C. Bormann et autres, "[Compression d'en-tête robuste](#) (ROHC) : cadre et quatre profils", juillet 2001. (MàJ par [RFC3759](#), [RFC4815](#)) (P.S.)

[RFC3711] M. Baugher et autres, "Protocole de [transport sécurisé en temps réel](#) (SRTP)", mars 2004. (P.S.)

[RFC4224] G. Pelletier et autres, "Compression d'en-tête robuste (ROHC) : ROHC sur des canaux qui peuvent réordonner les paquets", janvier 2006. (Information)

Adresse des auteurs

Bruce Thompson
170 West Tasman Drive
San Jose, CA 95134-1706
United States of America
téléphone : +1 408 527 0446
mél : brucet@cisco.com

Tmima Koren
170 West Tasman Drive
San Jose, CA 95134-1706
United States of America
téléphone : +1 408 527 6169
mél : tmima@cisco.com

Dan Wing
170 West Tasman Drive
San Jose, CA 95134-1706
United States of America
mél : dwing@cisco.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.