

Groupe de travail Réseau
Request for Comments : 2688
Catégorie : En cours de normalisation

S. Jackowski, Deterministic Networks
D. Putzolu, Intel Architecture Labs
E. Crawley, Argon Networks
B. Davie, Cisco Systems
septembre 1999

Traduction Claude Brière de L'Isle

Transpositions de services intégrés pour réseaux à bas débit

Statut du présent mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet 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 (1999). Tous droits réservés.

Résumé

Un ensemble de documents d'accompagnement décrit une architecture pour la fourniture des services intégrés sur des liaisons à faible débit binaire, comme les lignes de modem, les canaux B du RNIS, et les liaisons sub-T1 [RFC2508] [RFC2686], [RFC2687], [RFC2689]. Les principaux composants de l'architecture sont un ensemble de formats d'encapsulation en temps réel pour les liaisons asynchrones et synchrones à faible débit binaire, une architecture de compression d'en-tête optimisée pour les flux en temps réel, des éléments de protocole de négociation utilisés entre les routeurs (ou entre hôtes et routeurs) et des protocoles d'annonces utilisés par les applications pour permettre cette négociation.

Le présent document définit les transpositions de service des services intégrés de l'IETF pour les liaisons à faible débit binaire, précisément, la charge contrôlée [RFC2211] et la garantie de service [RFC2212]. L'approche prend la forme d'un ensemble de lignes directrices et de considérations pour la mise en œuvre de ces services, ainsi que les critères d'évaluation des éléments qui fournissent ces services.

1. Introduction

En plus des services "au mieux" pour lesquels l'Internet est bien connu, d'autres types de services ("services intégrés") sont en cours de développement et de déploiement dans l'Internet. Ces services prennent en charge un traitement particulier du trafic sur la base de la bande passante, de la latence, et d'autres exigences qui ne peuvent usuellement pas être satisfaites en utilisant le service "au mieux".

Le présent document définit la transposition des services intégrés "charge contrôlée" [RFC2211] et "garanti" [RFC2212] sur les liaisons à faible bande passante. L'architecture et les mécanismes utilisés pour mettre en œuvre ces services sur de telles liaisons sont définis dans un ensemble de documents d'accompagnement. Les mécanismes définis dans ces documents incluent à la fois la compression des flux (pour économiser la bande passante) [RFC2508], [RFC2509] et un ensemble d'extensions au protocole PPP qui permettent la fragmentation [RFC2686] ou la suspension [RFC2686] de gros paquets en faveur de paquets provenant de flux ayant des exigences de service plus contraignantes.

1.1 Langage de spécification

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

2. Problèmes de la fourniture de service contrôlés et garantis

À la différence des autres couches de liaison, les liaisons dont il est question dans le présent document ne fonctionnent que sur des connexions point à point à bas débit. Des exemples de cette sorte de liaisons visées ici incluent les lignes de téléphone, les canaux RNIS, et les liaisons louées à bas débit (1,5 Mbit/s ou moins). De telles liaisons peuvent survenir à différentes positions au sein du chemin de bout en bout :

- d'un hôte à un hôte directement connecté,
- d'un hôte à un appareil d'accès réseau (routeur ou commutateur),

- d'appareil bordure (routeur ou commutateur de sous-réseau) vers un routeur ou commutateur et inversement,
- dans de rares circonstances, une liaison d'un routeur de cœur de réseau à routeur de cœur de réseau.

Ces liaisons représentent souvent le premier ou le dernier bond de large zone dans un vrai service de bout en bout. Noter que ces liaisons peuvent être les plus contraintes en bande passante le long du chemin entre deux hôtes.

Les services utilisés dans la transposition de services intégrés sur ces liaisons ne sont fournis que si les deux points d'extrémité sur la liaison prennent en charge l'architecture et les mécanismes référencés ci-dessus. La prise en charge de ces mécanismes est déterminée durant la négociation PPP. La nature non partagée de ces liaisons, ainsi que le fait que les liaisons point à point sont normalement toutes deux unidirectionnelles (c'est-à-dire que le canal d'envoi et celui de réception sont séparés) permet que toutes les décisions de contrôle d'admission soient prises en local.

Comme décrit dans la [RFC2686] et la [RFC2687], pour les systèmes qui peuvent exercer un contrôle en temps réel de leurs transmissions à une granularité plus fine que les trames HDLC entières, l'approche de suspension/reprise optimise la bande passante disponible en minimisant la redondance d'en-tête associée à la pré-fragmentation MLPPP et peut fournir un meilleur délai. Cependant, cela se fait aux dépens de la préparation des données sortantes et de l'examen de toutes les données entrantes pour les informations de contrôle de suspension/reprise. L'approche de la fragmentation peut être mise en œuvre sans examen supplémentaire du flux de données (au delà du bourrage de bits/octets, qui peut être dans le matériel) et est applicable aux systèmes qui ne fournissent que le contrôle de transmission en mode trame. Le choix entre suspension/reprise et fragmentation devrait être fait sur la base du niveau de contrôle de transmission, de la capacité des éléments à traiter le tramage de style HDLC décrit dans la [RFC2686], et de la redondance du système associée à l'examen octet par octet (exigé par la suspension/reprise).

Pour fournir le service de charge contrôlée ou le service garanti avec l'approche de suspension/reprise, lorsque un paquet pour un flux admis (paquet de QS) arrive durant la transmission d'un paquet au mieux et que la poursuite de la transmission du paquet au mieux violerait les contraintes de délai des flux de service à QS, le paquet au mieux est préempté, les paquets/fragments à QS sont ajoutés à la transmission, et la transmission du paquet au mieux est ensuite reprise : usuellement, toute en une transmission. La station receveuse sépare le paquet au mieux des fragments du paquet à QS incorporés. Il est aussi concevable qu'un paquet d'un flux à QS puisse suspendre un paquet d'un autre flux si la limite de livraison du nouveau paquet est plus tôt que le paquet en cours.

Pour les systèmes qui utilisent la fragmentation, tous les paquets plus longs que le délai maximum tolérable pour les paquets provenant de flux de service améliorés sont fragmentés avant la transmission de sorte qu'un paquet court pour un autre flux peut être intercalé entre des fragments d'un plus grand paquet et satisfaire encore à la limite de transmission pour le flux qui requiert des services améliorés.

Noter que la fragmentation discutée dans le présent document se réfère à la fragmentation PPP multi-liaison (MLPPP) et aux modifications MCMLPPP associées comme décrit dans la [RFC2686], et non à la fragmentation IP ou d'autre couche 3. La fragmentation MLPPP est locale pour la liaison PPP, et n'affecte pas la MTU de bout en bout (IP).

2.1 Calcul d'un "délai acceptable" pour les flux Int-serv

Un routeur qui fournit la charge contrôlée ou le service garanti sur une liaison de série à bas débit a besoin d'avoir quelques notions du "délai acceptable" pour les paquets qui appartiennent à des flux int-serv. Si il utilise la fragmentation, un routeur a besoin de savoir à quelle taille fragmenter les paquets ; si il utilise la suspension/reprise, il a besoin de savoir quand il est approprié de suspendre un paquet pour satisfaire aux objectifs de délai d'un autre paquet.

Malheureusement, il n'y a pas de façon pure et dure de déterminer une seule limite de délai pour un certain flux ; alors que les points d'extrémité d'un flux ont assez d'informations pour déterminer les limites de délai acceptables de bout en bout et faire des demandes de réservation au réseau pour satisfaire ces limites, ils ne communiquent pas un délai "par bond" aux routeurs.

Dans le cas du service garanti [RFC2212], une approche est de laisser l'opérateur du réseau configurer les paramètres sur le routeur qui vont directement affecter ses performances de délai. On observe que le service garanti permet aux routeurs de dévier du modèle de flux fluide idéal et d'annoncer dans quelle mesure il va dévier en utilisant deux termes d'erreur C et D, les termes d'erreur qui dépendent du débit et les termes d'erreur indépendants du débit, définis dans la [RFC2212]. Un opérateur de réseau peut configurer les paramètres de la liaison à bas débit de telle façon que D soit réglé à une valeur de son choix.

Si on utilise la fragmentation de niveau liaison, le routeur qui contrôle une liaison à bas débit peut être configuré avec une certaine taille de fragment. Cela va permettre de calculer un composant du terme d'erreur D sur la base du temps d'envoi d'un fragment sur la liaison. (Noter que D peut avoir d'autres composants comme le délai de la vitesse de la lumière sur la

liaison.) Les détails du calcul de D sont décrits plus loin. De même, si on utilise la suspension/reprise, le routeur peut être configuré avec un paramètre de délai, qui lui permettrait de décider quand il est approprié de suspendre un paquet.

Pour la charge contrôlée (CL, *Controlled Load*) il n'y a pas de terme d'erreur, et le routeur doit décider comment le mieux satisfaire les exigences des réservations admises en utilisant seulement les informations de leurs TSpec. Comme la définition de la charge contrôlée déclare qu'un flux CL avec un taux de Tspec de r devrait recevoir un traitement similaire à celui d'un réseau non chargé de capacité r, les paquets CL ne devraient généralement pas rencontrer de délais de bout en bout significativement supérieurs à b/r + délai de propagation. Il est clair qu'un routeur connecté à une liaison bas débit ne devrait pas introduire un délai supérieur à b/r dû à la transmission d'autres fragments ; idéalement, il devrait introduire un délai substantiellement inférieur à b/r , car d'autres bonds sur le chemin de bout en bout peuvent introduire aussi des délais. Cependant, cela peut être difficile pour des flux avec de très petites valeurs de b.

On s'attend à ce que les mises en œuvre fassent leurs propres compromis sur le niveau auquel placer le délai pour les flux à charge contrôlée. De même, il peut n'être pas possible ou souhaitable de configurer les paramètres qui affectent D à des valeurs arbitrairement basses, car il y a un coût en redondance à fragmenter les paquets à de très petites tailles. À l'inverse, si D est trop grand, certaines applications peuvent trouver qu'elles ne peuvent pas faire une réservation qui satisfasse leurs objectifs de délai.

Pour le reste du présent document, on suppose qu'un routeur a une notion du délai acceptable qu'il peut introduire avant de commencer la transmission d'un paquet. Ce délai s'ajoute à tout délai qu'un paquet pourrait subir par suite d'un algorithme "idéal" de mise en file d'attente qu'utilise le routeur pour programmer les paquets.

3. Transposition de classe de charge contrôlée et de service garanti

La prise en charge des services intégrés sur des liaisons PPP qui mettent en œuvre MCML ou RTF peut être réalisée de plusieurs façons. Des lignes directrices pour transposer ces services sur des liaisons PPP et sur les classes fournies par les mécanismes de suspension/reprise et de fragmentation sont présentées ci-dessous. Noter que ces lignes directrices supposent qu'un minimum de protocole de signalisation soit utilisé pour indiquer la qualité de service désirée à l'expéditeur et au receveur d'un flux sur une liaison PPP.

3.1 Transpositions de classe prédéfinie

Une méthode relativement simple de transposition de classe qui PEUT être utilisée est celle où les valeurs de classes correspondent à des niveaux de service prédéfinis. Dans cet arrangement, tous les flux admis sont groupés en un parmi plusieurs pots, où chaque pot correspond en gros au niveau de service désiré pour les flux qui y sont placés. Voici un ensemble d'exemples de transpositions :

MCML court	MCML long	RTF	Service
0b00	0b0000	0b000	au mieux
NA	0b0001	0b001	réservé
0b01	0b0010	0b010	sensible au délai, sans limite
NA	0b0011	0b011	réservé
NA	0b0100	0b100	réservé
0b10	0b0101	0b101	sensible au délai, limite de 500 ms
NA	0b0110	0b110	sensible au délai, limite de 250 ms
0b11	0b0111	0b111	contrôle réseau

Tableau 1 : Exemple de transpositions de classes en services

Noter que MCML a deux formats, à numéros de séquence courts, et à numéros de séquence longs, ce qui permet deux et quatre bits d'identification de classes. RTF permet trois bits d'identification de classe dans tous les formats.

L'utilisation d'une méthode de transposition par défaut pour allouer les classes aux flux de façon fixe se heurte à certaines limitations. En particulier, tous les flux qui tombent dans un certain pot (qui sont alloués à une classe particulière) vont être programmés par rapport à tous les autres à une granularité de paquets, plutôt qu'au niveau de granularité plus fin du fragment. Il peut en résulter un contrôle d'admission excessivement prudent lorsque le nombre de classes disponibles est petit, comme dans le format de numéro de séquence court de MCML.

3.2 Transpositions de classe prédéfinie et élision de préfixe

Dans le cas où sont attendues moins de réservations que le nombre total de classes négociées pour une liaison PPP, il est possible d'allouer des flux individuels aux numéros de classe fixés. Cette allocation est utile dans le cas où l'identifiant de protocole associé à un ou plusieurs flux est connu au moment de la négociation LCP et que la bande passante de la connexion est relativement petite. Si ces conditions sont remplies, alors, pour ces flux qui sont connus, une classe spécifique peut facultativement leur être allouée et l'option PPP d'élision de préfixe de la [RFC2686] peut être utilisée pour ces classes afin de réaliser une petite économie de bande passante.

3.3 Transpositions de classe dynamique

Dans le cas où des transpositions de classe prédéfinies ne sont pas satisfaisantes, une mise en œuvre PEUT transposer les valeurs de classe en des paquets individuels plutôt que d'allouer les flux à des classes fixes. Ceci peut être parce que les classes que fournissent MCML et RTF peuvent être vues comme des mécanismes de segmentation/fragmentation purement spécifiques de PPP. C'est-à-dire que, alors que le numéro de classe DOIT rester constant sur une base intra paquet, il PEUT varier paquet par paquet pour tous les flux qui transitent sur une liaison PPP. L'allocation réelle de flux particuliers à des classes fixes est inutile, car les numéros de classe ne SONT PAS OBLIGÉS d'avoir d'autre signification que dans le contexte d'identification de l'appartenance des fragments/segments au titre d'un seul paquet. Ce point est suffisamment important pour qu'un exemple en soit donné ci-dessous.

Considérons une liaison PPP qui utilise le format de fragment à numéro de séquence court MCML (c'est-à-dire que quatre classes sont fournies). Supposons qu'en plus de porter du trafic au mieux, cette liaison porte cinq flux de service garanti, A, B, C, D, et E. Supposons de plus que la capacité de la liaison soit de 100 kbit/s et que la latence soit de 100 ms. Finalement, supposons que le trafic au mieux (BE, *Best Effort*) soit suffisant pour garder le tuyau plein à tout moment et que les flux de service garanti (GS, *Guaranteed Service*) A à E soient chacun de 10 kbit/s et que tous aient une limite de délai de 145 ms.

Temps (ms)	Action
0	le trafic BE est mis en file d'attente
0	2 kbit de fragment d'un paquet de 10 kbit de trafic BE envoyés, classe 0 (...)
8	2 kbit de fragment de BE envoyés, classe 0 (10 kbit de paquet BE faits)
9	un paquet de 8 kbit du flux A arrive
10	2 kbit de fragment provenant de A envoyés, classe 1 (début des 8 kbit du paquet du flux A)
11	8 kbit d'un paquet du flux B arrivent
12	2 kbit de fragment de B envoyés, classe 2 (début des 8 kbit du paquet du flux B)
13	des paquets de 8 kbit des flux C, D, et E arrivent
14	2 kbit de fragment de C envoyés, classe 3 (début des 8 kbit du paquet du flux C)
16	2 kbit de fragment de D envoyés, classe 0 (début des 8 kbit du paquet du flux D)
18	2 kbit de fragment de A envoyés, classe 1
20	2 kbit de fragment de B envoyés, classe 2
22	2 kbit de fragment de A envoyés, classe 1
24	2 kbit de fragment de A envoyés, classe 1 (fin des 8 kbit du paquet du flux A)
26	2 kbit de fragment de E envoyés, classe 1 (début des 8 kbit du paquet du flux E)
27	8 kbit du paquet du flux A arrivent
28	2 kbit de fragment de B envoyés, classe 2
30	2 kbit de fragment de C envoyés, classe 3
32	2 kbit de fragment de E envoyés, classe 1
34	2 kbit de fragment de B envoyés, classe 2 (fin des 8 kbit du paquet du flux B)
36	2 kbit de fragment de E envoyés, classe 1
38	2 kbit de fragment du flux A envoyés, classe 2 (début des 8 kbit du paquet du flux A)
(etc.)	

Cet exemple montre plusieurs choses. D'abord, que plusieurs flux PEUVENT partager la même classe, en particulier dans le cas où il y a plus de flux que de classes. Plus important, il n'y a pas de raison qu'un flux particulier doive être alloué à une classe fixe – la seule exigence est que chaque paquet, lorsque fragmenté, DOIT avoir la même valeur de classe allouée à tous les fragments. Au delà de cette exigence le programmeur de liaison peut allouer à chacune des numéros de classe changeants comme nécessaire pour satisfaire aux exigences de réservation.

Une suggestion pour les mises en œuvre de services intégrés sur des liaisons MCML et RTF qui utilisent des transpositions dynamiques est que tout le trafic BE DEVRAIT être logiquement séparé du trafic à QS, et transposé dans une classe fragmentable (classes MCML 0 à 3 en format de fragment à numéro de séquence court, 0 à 15 en format de fragment à numéro de séquence long) ou suspensible (classes RTF 0 à 6). Comme le trafic BE va dans la plupart des mises en œuvre n'être pas programmé pour la transmission sauf lorsqu'une liaison est vide (c'est-à-dire qu'aucun trafic CL ou GS n'est prêt pour la transmission) les mises en œuvres PEUVENT choisir de faire usage du numéro de classe 0 pour le trafic BE.

3.4 Trafic non conforme

Le traitement du trafic à QS non conforme est largement déterminé par les spécifications de service appropriées, mais la mise en œuvre détaillée dans le contexte du présent projet permet une certaine souplesse. La régulation des flux qui contiennent du trafic non conforme DEVRAIT toujours être faite au niveau de granularité du paquet individuel plutôt qu'à un niveau de granularité plus fin. En particulier, dans les cas où un élément de réseau qui programme des flux pour transmission a besoin d'abandonner du trafic non conforme, il DEVRAIT abandonner des paquets entiers plutôt que d'abandonner des fragments individuel de paquets appartenant à du trafic non conforme. Dans les cas où un élément de réseau transmet du trafic non conforme lorsque la bande passante de la liaison est disponible plutôt que d'abandonner le trafic, la mise en œuvre DEVRAIT fragmenter les paquets d'un tel trafic comme si c'était du trafic au mieux.

Il dépend du service de décider si le trafic BE et le trafic non conforme sont traités différemment à l'égard de la transmission (par exemple, le BE reçoit une priorité d'accès à la liaison sur le trafic non conforme) ou si au sein de chaque type de trafic un traitement particulier est accordé aux flux individuels (par exemple., WFQ, RED, etc.).

4. Lignes directrices pour les mise en œuvre

4.1 Effets du bourrage de bit et d'octet iPPP sur le contrôle d'admission

Une importante considération du contrôle d'admission pour les liaisons PPP est la réductions du taux effectif de la liaison due au bourrage de bits. Les algorithmes normaux de bourrage de bit peuvent résulter en une redondance supplémentaire pouvant aller jusqu'à 20 % . Donc, les mises en œuvre de contrôle d'admission pour le service garanti sur des liaisons où le bourrage de bits est utilisé DEVRAIENT prendre le taux de RSpec de tous les flux et le multiplier par 1,2, pour tenir compte des 20 % de redondance provenant du bourrage de bits, lors de la détermination de la possibilité d'admission d'un nouveau flux. Les mises en œuvre de contrôle d'admission pour les réservations de charge contrôlée peuvent utiliser un algorithme similaire avec le taux de crête de la Tspec, ou elles peuvent tenter de mesurer le degré réel d'expansion qui survient sur une liaison due au bourrage de bits. Cette caractérisation peut alors être utilisée pour ajuster la capacité restante calculée de la liaison. De telles mesures doivent être utilisées avec précaution, car le degré de bourrage de bits qui survient peut varier de façon significative, aussi bien de façon inter-flux que intra-flux.

Le bourrage d'octets est aussi utilisé sur de nombreuses liaisons PPP, très fréquemment sur des modems POTS lorsque on se sert du protocole V.42. Le bourrage des octets pose un problème difficile au contrôle d'admission, en particulier dans le cas du service garanti, à cause de sa nature très variable. Dans le pire des cas, le bourrage d'octets peut résulter en un doublement de la taille de trame. Par conséquent, une mise en œuvre stricte du contrôle d'admission pour la charge garantie sur des liaisons PPP à bourrage des octets DEVRAIT doubler la RSpec du trafic de la liaison lors des décisions d'admission de flux. Comme avec le bourrage de bits, les mises en œuvre des algorithmes de contrôle d'admission de service à charge contrôlée pour les liaisons avec bourrage d'octets PEUVENT tenter de déterminer l'expansion moyenne des paquets via l'observation ou PEUVENT utiliser les valeurs de pire cas théorique.

4.2 Considérations sur la compression

L'architecture pour fournir des services intégrés sur des liaisons à faible bande passante utilise plusieurs options PPP pour négocier la configuration de liaison comme décrit dans les [RFC1114], [RFC2508], [RFC2509]. Pour décider d'admettre un flux, le contrôle d'admission DOIT calculer l'impact de ce qui suit sur la taille de la MTU, le débit, et la taille de fragment :

- compression d'en-tête : Van Jacobson ou Casner-Jacobson [RFC1114], [RFC2508], [RFC2509],
- élision de préfixe,
- CCP,
- option d'en-tête de fragment utilisée,
- approche de fragmentation ou de suspension/reprise.

Si une des options de compression est mise en œuvre pour la connexion, le taux réel de transmission, et donc la bande passante requise pour la liaison, sera réduit par la ou les méthodes de compression utilisées.

L'élision de préfixe peut tirer parti de la transposition des flux en classes MLPPP pour éluder les préfixes qui ne peuvent pas être compressés aux couches supérieures. En établissant des accords à travers la liaison, l'envoyeur peut éluder un préfixe pour une certaine classe de trafic et à réception des paquets dans cette classe, le receveur peut restaurer le préfixe.

Les deux gains de compression et d'élision DOIVENT être inclus comme décrit dans la section sur le contrôle d'admission ci-dessous. Noter que la capacité à effectuer la compression à des couches supérieures (par exemple, TCP ou RTP/UDP) peut dépendre de la fourniture d'une indication par l'envoyeur, comme décrit dans la [RFC3006].

4.3 Contrôle d'admission

Le contrôle d'admission DOIT décider si il faut admettre un flux sur la base du débit et du délai. On suppose ce qui suit :

- LinkRate est le débit de la liaison.
- MTU est l'unité de transmission maximale d'un protocole.
- MRU est l'unité de réception maximale pour une certaine liaison.
- CMTU est la taille maximale de la MTU après l'application de la compression.
- eMTU est la taille effective à la couche liaison d'un paquet de la taille de la MTU après la fragmentation de couche liaison et l'ajout des en-têtes de fragment.
- FRAG est la taille de fragment y compris les en-têtes/en-queue de MLPPP.
- Header est la taille de l'en-tête/en-queue/tramage pour MLPPP/Fragments.
- pHeader est la redondance supplémentaire d'en-tête/tramage associée à la suspension/reprise. Cela devrait inclure la redondance de FSE et de pire cas de bourrage.
- pDelay est le temps pris pour suspendre un paquet déjà "en vol", par exemple, à cause du délai nécessaire pour vider la mémoire tampon de sortie FIFO.
- b est la profondeur du pot en octets.
- R est le débit demandé.
- Dlink est la redondance de délai fixée pour la liaison (Modem, DSU, vitesse de la lumière, etc.).
- eRate est le débit effectif après compression et fragmentation.

Le terme Dlink PEUT être configuré par un outil administratif une fois que le réseau est installé ; il peut être déterminé au moyen de mesures en temps réel ; ou il PEUT être disponible à partir du matériel durant l'établissement de la liaison et/ou la négociation PPP. Se référer à l'Appendice A pour d'autres considérations sur les caractéristiques et délais de la liaison PPP.

Le contrôle d'admission DOIT calculer CMTU, eMTU, et eRate pour le service à charge contrôlée, et il DOIT calculer CMTU, eMTU, eRate, et D pour le service garanti :

Pour déterminer si le débit demandé est disponible, le contrôle d'admission DOIT calculer le débit effectif de la demande (eRate) – pire cas – comme suit :

$$\begin{aligned} \text{Nbr_de_Fragments} &= \text{CMTU} \text{ div } (\text{FRAG-en-tête}) \text{ [diviseur entier]} \\ \text{Dernière_Taille_de_Fragment} &= \text{CMTU} \text{ mod } (\text{FRAG-en-tête}) \end{aligned}$$

Si Dernière_Taille_de_Fragment != 0

$$\text{eMTU} = (\text{Nbr_de_Fragments}) * \text{FRAG} + \text{Dernière_Taille_de_Fragment} + \text{En-tête}$$

Autrement

$$\text{eMTU} = (\text{Nbr_de_Fragments}) * \text{FRAG}$$

$$\text{eRate} = \text{eMTU}/\text{CMTU} * \text{R} \text{ [diviseur à virgule flottante]}$$

Le contrôle d'admission DEVRAIT comparer le eRate de la demande à la bande passante restante disponible pour déterminer si le débit demandé peut être délivré.

Pour le service à charge contrôlée, un flux peut être admis tant qu'il y a une bande passante disponible suffisante (après le calcul ci-dessus) pour satisfaire à l'exigence de débit, et si il y a un espace de mémoire tampon suffisant (la somme des tailles de pots de jetons ne dépasse pas la capacité de la mémoire tampon). Bien que certains multiplexages statistiques puissent être faits en calculant l'admissibilité, la nature des liaisons à bas débit binaire pourrait rendre cette approche risquée car tout retard subi pour traiter une surcharge temporaire pourrait être difficile à amortir.

4.4 Calculs de terme d'erreur

Le service garanti exige le calcul des termes d'erreur C et D. C est un terme d'erreur dépendant du débit et il n'y a pas de facteur particulier qui affecte son calcul dans l'environnement de liaison à bas débit. Le terme d'erreur D est calculé à partir du délai inhérent à la liaison (Dlink) plus le pire cas potentiel de délai dû à la transmission d'un autre fragment ou à la redondance de suspension/reprise. Donc, D devrait être calculé comme :

$$D = \text{Dlink} + \text{FRAG}/\text{LinkRate}$$

dans le cas d'une mise en œuvre à fragmentation, et comme

$$D = \text{Dlink} + \text{pHeader} + \text{pDelay}$$

pour une mise en œuvre à suspension/reprise.

4.5 Considérations de programmation

On peut voir le programmeur de liaison comme ayant deux parties, dont la première programme les paquets pour la transmission avant de les passer à la seconde partie du programmeur – le programmeur de niveau liaison – qui est chargé de fragmenter les paquets, les transposant en classes, et faisant la programmation entre les classes.

Dans le mode de transposition dynamique des classes du paragraphe 3.3, pour décider quelle classe allouer à un paquet, le programmeur de niveau liaison devrait tenir compte de la taille des autres paquets actuellement alloués à la même classe. En particulier, les paquets qui ont les contraintes de délai les plus serrées ne devraient pas être affectés à des classes pour lesquelles des paquets relativement gros sont sur le point d'être transmis.

Dans l'approche de transposition de classe aussi bien dynamique que statique, noter que le programmeur de niveau liaison DEVRAIT contrôler quelle quantité de bande passante est allouée à chaque classe à tout moment. Le programmeur devrait allouer la bande passante à une classe conformément à la bande passante réservée pour la somme de tous les flux qui ont actuellement des paquets affectés à la classe. Noter que dans l'exemple du paragraphe 3.3, lorsque des paquets provenant des flux A et E étaient affectés à la même classe (classe 1), le programmeur a alloué plus de bande passante à la classe 1, reflétant le fait qu'il portait du trafic pour des réservations totalisant 20 kbit/s tandis que les autres classes ne portaient que 10 kbit/s.

5. Considérations pour la sécurité

Les considérations générales pour la sécurité pour les liaisons MLPPP et PPP sont traitées respectivement dans les [RFC1990] et [RFC1661]. Les considérations pour la sécurité pertinentes pour RSVP, utilisé comme protocole de signalisation pour les services intégrés, sont exposées dans la [RFC2209].

Une considération de sécurité spécifique pertinente pour la fourniture de la qualité de service sur les liaisons PPP apparaît lorsque on s'appuie sur l'expansion observée ou moyenne théorique durant le contrôle d'admission due au bourrage de bits ou d'octets. Les mises en œuvre fondées sur ces valeurs d'expansion de paquet contiennent une faiblesse potentielle aux attaques de déni de service. Un adversaire pourrait intentionnellement envoyer du trafic qui résulterait en le pire cas d'expansion de paquet par bourrage de bits ou d'octets. Il pourrait en résulter à son tour un non respect des garanties de qualité de service pour les autres flux à cause d'un contrôle d'admission trop permissif. Cette attaque de déni de service potentielle milite fortement en faveur de l'utilisation d'un facteur de pire cas d'expansion dans les calculs de contrôle d'admission, même pour le service à charge contrôlée.

Au delà des considérations mentionnées ci-dessus, le présent document n'introduit pas de nouveau problème de sécurité par dessus ceux exposés dans les documents d'accompagnement de ISSLL [RFC2686], [RFC2687] et [RFC2689] et dans le document AVT [RFC2508]. Toute utilisation de ces transpositions de service suppose que toutes les demandes de service sont authentifiées de façon appropriée.

6. Références

- [RFC1144] V. Jacobson, "[Compression des en-têtes TCP/IP](#) pour les liaisons série à faible débit", février 1990.
- [RFC1661] W. Simpson, éditeur, "[Protocole point à point \(PPP\)](#)", STD 51, juillet 1994. (MàJ par la RFC2153)
- [RFC1990] K. Sklower et autres, "Protocole [multiliasion en PPP](#) (MP)", août 1996. (Remplace [RFC1717](#)) (D.S.)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2209] R. Braden, L. Zhang, "[Protocole de réservation de ressource](#) (RSVP) -- version 1 : règles de traitement de message", septembre 1997. (Information)
- [RFC2211] J. Wroclawski, "Spécification du service d'[élément de réseau à charge contrôlée](#)", septembre 1997. (P.S.)
- [RFC2212] S. Shenker, C. Partridge, R. Guerin, "Spécification de la [qualité de service garantie](#)", septembre 1997. (P.S.)
- [RFC2215] S. Shenker, J. Wroclawski, "[Paramètres généraux de caractérisation](#) pour éléments de réseau à intégration de service",
- [RFC2508] S. Casner, V. Jacobson, "Compression d'en-têtes IP/UDP/RTP pour liaisons séries à bas débit", février 1999.

(P.S.)

- [RFC2509] M. Engan, S. Casner, C. Bormann, "Compression d'en-tête IP sur PPP", février 1999. (*Obsolète, voir RFC3544*) (P.S.)
- [RFC2686] C. Bormann, "[Extension Multi-classe à PPP](#) multi-liaison", septembre 1999. (P.S.)
- [RFC2687] C. Bormann, "[PPP dans une trame de style HDLC](#) orientée temps réel", septembre 1999. (P.S.)
- [RFC2689] C. Bormann, "Fourniture de services intégrés sur liaisons à faible débit", septembre 1999, (*Information*)
- [RFC3006] B. Davie et autres, "Services intégrés en présence de flux compressibles", novembre 2000. (P.S.)

7. Adresse des auteurs

Steve Jackowski
Deterministic Networks, Inc.
245M Mt Hermon Rd, #140
Scotts Valley, CA 95060
USA
téléphone : +1 (408) 813 6294
mél : stevej@DeterministicNetworks.com

David Putzolu
Intel Architecture Labs (IAL)
JF3-206-H10
2111 NE 25th Avenue
Hillsboro, OR 97124-5961
USA
téléphone : +1 (503) 264 4510
mél : David.Putzolu@intel.com

Eric S. Crawley
Argon Networks, Inc.
25 Porter Road
Littleton, MA 01460
USA
téléphone : +1 (978) 486-0665
mél : esc@argon.com

Bruce Davie
Cisco Systems, Inc.
250 Apollo Drive
Chelmsford, MA, 01824
USA
téléphone : +1 (978) 244 8921
mél : bdavie@cisco.com

Remerciements

Le présent document s'appuie largement sur les travaux du groupe de travail ISSLL de l'IETF.

Appendice A Considérations de contrôle d'admission pour les modems POTS

Les protocoles utilisés dans les mises en œuvre actuelles de modems du vieux système de télécommunications traditionnel (POTS, *Plain Old Telecommunications System*) peuvent présenter des changements significatifs de débit de ligne et de délai sur la durée d'une connexion. Les algorithmes de contrôle d'admission et de programmation de liaison utilisés avec ces appareils DOIVENT être prêts à compenser cette variabilité afin de fournir une mise en œuvre robuste des services intégrés.

Le débit de liaison sur les modems POTS est normalement indiqué au moment de la connexion. Cette valeur peut changer sur la durée de la connexion. Le protocole V.34, utilisé dans la plupart des modems POTS, s'adapte aux conditions de la liaison, et est capable de recalibrer le débit de transmission plusieurs fois pendant la durée d'une connexion. Il va normalement en résulter une petite (~10 %) augmentation du débit de transmission sur la connexion initiale dans la première minute d'un appel. Il est important de noter, cependant, que d'autres résultats sont aussi possibles, y compris une diminution de la bande passante disponible. Les algorithmes de contrôle d'admission DOIVENT prendre en compte de tels changements lorsque ils se produisent, et les mises en œuvre DOIVENT être capables de traiter en douceur le cas pathologique où le débit de liaison tombe en fait en dessous de la capacité actuellement réservée d'une liaison.

Le délai subi par le trafic sur les modems POTS peut varier de façon significative dans le temps. À la différence du débit de liaison, le délai ne converge souvent pas vers une valeur stable. Le protocole V.42 est utilisé dans la plupart des modems POTS pour fournir la fiabilité à la couche liaison. Cette fiabilité, qui est mise en œuvre via la retransmission, peut faire subir des délais significatifs aux trames. Les retransmissions volent aussi implicitement de la bande passante de liaison aux autres trafics. Ces délais et les réductions de bande passante de liaison rendent extrêmement difficile d'honorer une réservation de service garanti. Sur une liaison qui est en fait peu ou modérément chargée, un service à charge contrôlée peut dans une certaine mesure accepter de tels événements au titre du comportement d'une liaison à charge légère.

Malheureusement, comme l'utilisation réelle des liaisons augmente, les retransmissions V.42 ont un potentiel de vol de fractions de plus en plus larges de la bande passante disponible, rendant difficile même pour le service à charge contrôlée d'offrir une forte utilisation de la liaison lorsque surviennent les retransmissions.

9. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de droits de reproduction ci-dessus et ce paragraphe soient inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définies dans les procédures des normes d'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet ou ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

Remerciement

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