Groupe de travail Réseau
Request for Comments : 2996
Catégorie : En cours de normalisation

Y. Bernet, Microsoft
novembre 2000
Traduction Claude Brière de L'Isle

Format de l'objet RSVP DCLASS

Résumé
La signalisation du protocole de réservation de ressource (RSVP, *Resource Reservation Protocol*) peut être utilisée pour demander des services de qualité de service (QS) et améliorer la gérabilité de la QS du trafic d'application dans un réseau à services différenciés (diff-serv ou DS). Lorsque on utilisé RSVP avec des réseaux DS, il est utile d'être capable de porter des codets de service différencié (DSCP, *Differentiated Services Code Point*) dans les objets de message RSVP. Un exemple en est l'utilisation de RSVP pour arranger le marquage des paquets avec un DSCP amont particulier à partir du point d'entrée du réseau DS, chez l'envoyeur ou chez un routeur de sortie du réseau précédent.

L'objet DCLASS est utilisé pour représenter et porter les DSCP au sein des messages RSVP. Le présent document spécifie le format de l'objet DCLASS et expose brièvement son utilisation.

1. Introduction

Cette section décrit les mécanismes d'utilisation de la signalisation RSVP [RFC2205] et de l'objet DCLASS pour effectuer le contrôle d'admission et appliquer la politique de QS au sein d'un réseau à services différenciés [RFC2475]. Elle suppose des envoyeurs et receveurs RSVP standard, et un réseau diff-serv quelque part sur le chemin entre envoyeur et receveur. Au moins un élément de réseau à capacité RSVP réside sur le réseau diff-serv. Cet élément de réseau peut être un point de mise en application de politique (PEP, *Policy Enforcement Point*) [RFC2753] ou peut simplement agir comme agent de contrôle d'admission pour le réseau, admettant ou refusant les demandes de ressource sur la base de la disponibilité des ressources. Dans l'un et l'autre cas, cet élément de réseau interagit avec les messages RSVP qui arrivent de l'extérieur du réseau DS, acceptant les demandes de ressource de la part des envoyeurs et receveurs à capacité RSVP, et convoyant les décisions de contrôle d'admission et d'allocation de ressources du réseau DS au RSVP de niveau supérieur. L'élément de réseau est normalement un routeur et sera considéré comme l'étant pour les besoins du présent document. Ce modèle est décrit plus complètement dans la [RFC2998].

1.1 Utilisation de l'objet DCLASS pour porter les informations de marquage de paquet vers l'amont

La principale utilisation de l'objet DCLASS est de porter les informations de DSCP entre un réseau DS et les nœuds amont qui peuvent souhaiter marquer les paquets avec des valeurs DSCP. En bref, l'envoyeur compose un message RSVP PATH standard et l'envoie vers le receveur. À un certain point, le message PATH atteint le réseau DS. Le message PATH traverse un ou plusieurs éléments de réseau qui sont des PEP et/ou des agents de contrôle d'admission pour le réseau diff-serv. Ces éléments installent l'état approprié et transmettent le message PATH vers le receveur. Si le contrôle d'admission réussit vers l'aval du réseau diff-serv, un message RESV va alors arriver de la direction du receveur. Comme ce message arrive au PEP et/ou aux agents de contrôle d'admission qui sont à capacité RSVP, chacun de ces éléments de réseau doit prendre une décision concernant l'admissibilité du flux signalé au réseau diff-serv.

Si l'élément de réseau détermine que la demande représentée par les messages PATH et RESV est admissible au réseau diff-serv, le niveau de service diff-serv approprié (ou le comportement agrégé) pour le trafic représenté dans la demande RSVP est déterminé. Ensuite, une décision est prise pour marquer les paquets de données arrivant pour ce trafic en utilisant en local la classification MF, ou de demander le marquage en amont des paquets avec les DSCP appropriés. Ce marquage amont pourrait survenir n'importe où avant le point d'entrée du réseau DS. Deux candidats vraisemblables sont l'envoyeur d'origine et le routeur frontière de sortie d'un réseau vers l'amont (DS ou non DS). La décision sur l'endroit où devraient être marqués les paquets RSVP peut être prise par accord ou à travers un protocole de négociation ; les détails sortent du

domaine d'application de ce document.

Si les paquets pour cette demande RSVP sont à marquer en amont, les informations sur les DSCP à utiliser doivent être convoyées de l'élément de réseau à capacité RSVP au point de marquage amont. Ces informations sont convoyées par l'objet DCLASS. Pour ce faire, l'élément de réseau ajoute au message RESV un objet DCLASS contenant un ou plusieurs DSCP correspondants à l'agrégat de comportement. Le message RESV est alors envoyé vers l'amont en direction de l'envoyeur RSVP.

Si l'élément de réseau détermine que la demande RSVP n'est pas admissible au réseau diff-serv, il envoie un message d'erreur RESV vers le receveur. Aucun DCLASS n'est nécessaire.

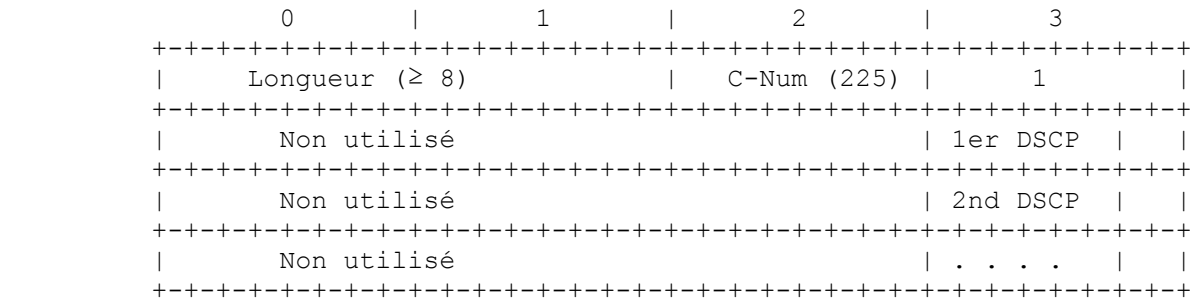
1.2 Utilisations supplémentaires de l'objet DCLASS

L'objet DCLASS est destiné à être un outil général pour transporter les informations de DSCP dans les messages RSVP. Cela peut être utile dans un certain nombre de situations. On donne un exemple ci-dessous à titre de motivation.

Dans cet exemple, on suppose que la décision sur l'agrégat de comportement approprié pour un flux de trafic à support RSVP est prise au routeur de sortie du réseau DS (ou au point de décision de politique qui s'y rapporte) en observant les messages RSVP PATH et RESV et les autres informations nécessaires. Cependant, le marquage réel de paquet doit être fait à l'entrée du réseau. L'objet DCLASS peut être utilisé pour porter les informations de marquage nécessaires entre les routeurs d'entrée et de sortie.

2. Format de l'objet DCLASS

L'objet DCLASS a le format suivant :



Le premier mot contient l'en-tête d'objet RSVP standard (le numéro de classe C-Num pour l'objet DCLASS est 225). Le champ Longueur indique la longueur totale de l'objet en octets. L'en-tête de l'objet est suivie d'un ou plusieurs mots de 32 bits, contenant chacun un DSCP dans les six bits de poids fort de l'octet de moindre poids. Le champ Longueur dans l'en-tête d'objet indique le nombre de DSCP qui sont inclus dans l'objet. Spécifiquement, le nombre d'objets DCLASS présents est égal à (Longueur - 4) / 4.

Le réseau peut retourner plusieurs DSCP dans l'objet DCLASS afin de permettre à l'hôte de faire la différence entre les sous flux au sein d'un agrégat de comportement. Par exemple, dans le cas du groupe de PHB AF de la [RFC2753], le réseau peut retourner les DSCP 001010, 001100, et 001110 correspondants aux niveaux croissants de préséance d'abandon dans la classe 1 du groupe AF de PHB. Noter que le présent document ne fait aucune déclaration concernant la signification de l'ordre des DSCP retournés. Une interprétation plus poussée des ensembles de DSCP dépend du service spécifique demandé par l'hôte et sort du domaine d'application de ce document.

Noter que le numéro de classe C-Num pour l'objet DCLASS est choisi à partir de l'espace des objets de classe inconnue qui devraient être ignorés et transmis par les nœuds qui ne les reconnaissent pas. Ceci est destiné à assurer une rétro compatibilité maximale.

3. Fonction de contrôle d'admission

D'un point de vue de boîte noire, la fonction de contrôle et de politique d'admission revient à la prise de décision d'accepter ou rejeter et à la détermination des DSCP qui devraient être utilisés pour le trafic correspondant. Les détails spécifiques du contrôle d'admission sortent du domaine d'application de ce document. En général, la décision de contrôle d'admission se

fonde à la fois sur la disponibilité des ressources et sur les politiques en matière d'utilisation des ressources dans le réseau diff-serv. La décision de contrôle d'admission prise par des éléments de réseau à capacité RSVP représente les deux considérations.

Pour décider si la demande RSVP est admissible en termes de disponibilité de ressource, un ou plusieurs éléments de réseau à l'intérieur des frontières du réseau diff-serv doivent comprendre l'impact que l'admission va avoir sur les ressources diff-serv spécifiques, ainsi que sur la disponibilité de ces ressources le long du chemin de données pertinent dans le réseau diff-serv.

Pour décider si la demande RSVP est admissible en termes de politique, l'élément de réseau peut utiliser des objets d'identité qui décrivent des usagers et/ou des applications qui peuvent être inclus dans la demande. Le routeur peut agir comme PEP/PDP et utiliser des données provenant d'une base de données de politique pour aider à prendre cette décision.

Voir à l'Appendice A un mécanisme simple pour un contrôle d'admission fondé sur des ressources configurables.

4. Considérations pour la sécurité

L'objet DCLASS porte des informations qui peuvent être utilisées pour demander une QS améliorée de la part d'un réseau DS, de sorte que des modifications inappropriées de l'objet pourraient permettre que des flux de trafic obtiennent un niveau de qualité de service supérieur ou inférieur à celui qui est approprié. En particulier, la modification d'un objet DCLASS par un tiers inséré entre le nœud d'entrée du réseau DS et le marqueur amont constitue une possible attaque de déni de service. Cette attaque est subtile parce que il est possible de réduire la QS reçue à un bas niveau inacceptable sans couper complètement le flux des données, rendant l'attaque plus difficile à détecter.

La possibilité de relever le niveau de QS reçue par une modification inappropriée de l'objet DCLASS est moins significative parce que c'est une sous classe d'une plus large classe d'attaques qui doivent déjà être détectées par le système. La protection doit déjà être en place pour empêcher un hôte de relever son niveau de DS en réception en devinant simplement les "bons" DSCP et en marquant les paquets en conséquence. Si cette protection est à la frontière du réseau DS, il va aussi bien détecter le marquage inapproprié des paquets arrivants causé par les objets DCLASS modifiés. Si cependant, la fonction de protection ainsi que celle de marquage ont été poussées en amont (peut-être chez un tiers de confiance ou un nœud intermédiaire) la transmission correcte de l'objet DCLASS doit être assurée pour empêcher une possible attaque de vol de service.

La simple observation de l'objet DCLASS dans un message RSVP soulève plusieurs questions qui peuvent être vues comme des problèmes de sécurité. La corrélation des valeurs observées d'objet DCLASS avec les demandes RSVP ou les paramètres de classification MF permet à l'observateur de déterminer que des flux différents reçoivent des niveaux de QS différents, ce qui pourrait être une information qui devrait être protégée dans certains environnements. De même, l'observation de l'objet DCLASS peut permettre à l'observateur de déterminer que la QS d'un seul flux a été relevée ou diminuée, ce qui peut signaler des événements significatifs dans la vie de l'application ou de l'utilisateur de ce flux. Finalement, l'observation de l'objet DCLASS peut révéler des informations sur le fonctionnement interne d'un réseau DS qui devraient être utiles pour les observateurs intéressés par les attaques de vol de services.

5. Références

[RFC2998] Y. Bernet et autres, "Cadre de fonctionnement de services intégrés (Intserv) sur réseaux Diffserv", novembre 2000. *(Information)*

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

[RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Protocole de réservation de ressource (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (*MàJ par* RFC2750, RFC3936, RFC4495) *(P.S.)*

[RFC2753] R. Yavatkar, D. Pendarakis, R. Guerin, "Cadre pour le contrôle d'admission fondé sur la politique", janvier 2000. *(Info.)*

[RFC2753] R. Yavatkar, D. Pendarakis, R. Guerin, "Cadre pour le contrôle d'admission fondé sur la politique", janvier 2000. *(Info.)*

6. Remerciements

Merci à Fred Baker et à Carol Iturralde pour leur relecture du document. Merci de leurs contributions à Ramesh Pabbati, Tim Moore, Bruce Davie et Kam Lee.

7. Adresse de l'auteur

Yoram Bernet
Microsoft
One Microsoft Way,
Redmond, WA 98052
USA
téléphone : (425) 936-9568
mél : yoramb@microsoft.com

Appendice A – Contrôle d'admission simple fondé sur les ressources configurables

Les routeurs peuvent utiliser des mécanismes assez sophistiqués pour la prise de décisions de contrôle d'admission, incluant des considérations de politique, divers protocoles de signalisation intra domaine, des résultats de surveillance du trafic, et ainsi de suite. Il est recommandé que les fonctionnalités de base suivantes soient fournies pour permettre un simple contrôle d'admission fondé sur la ressource en l'absence de mécanismes plus sophistiqués. Cette fonctionnalité peut être utilisée avec des routeurs configurables autonomes. Elle s'applique aux demandes RSVP/Intserv standard. Cette fonctionnalité suppose seulement qu'un seul DSCP soit inclus dans l'objet DCLASS, mais peut aussi être étendue pour prendre en charge plusieurs DSCP.

Il doit être possible de configurer deux tableaux dans le routeur. Ils ont décrits ci-dessous.

A.1 Transposition de type de service en DSCP

Un tableau fournit une transposition du type de service Intserv spécifié dans la demande RSVP en un DSCP qui peut être utilisé pour obtenir un service correspondant dans le réseau diff-serv. Ce tableau contient une rangée pour chaque type de service Intserv pour lequel une transposition est disponible. Chaque rangée a le format suivant :

Type de service Intserv : DSCP

Le tableau va normalement contenir au moins trois rangées ; une pou le service garanti, une pour le service à charge contrôlée; et une pour le service au mieux. (Le service au mieux va normalement se transposer en DSCP 000000, mais peut être outrepassé). Il serait possible d'ajouter des rangées pour des types de services indéfinis pour l'instant.

Ce tableau permet aux administrateur de réseau de faire une configuration statique d'un DSCP que le routeur va retourner dans l'objet DCLASS pour une demande RSVP admise. En général, des mécanismes plus sophistiqués et vraisemblablement plus dynamiques peuvent être utilisés pour déterminer le DSCP à retourner dans l'objet DCLASS. Aussi, il est vraisemblable qu'une transposition réelle pour certains services utiliserait plus d'un DSCP, celui-ci dépendant des paramètres d'invocation d'une demande de service spécifique. Dans ce cas, ces mécanismes peuvent outrepasser ou remplacer la transposition fondée sur un tableau statique décrite ici.

A.2 Disponibilité de ressource quantitative

Les demandes Intserv standard sont par nature quantitatives. Elles comportent des paramètres de baquet de jetons qui décrivent les ressources requises par le trafic pour lequel l'admission est demandée. Le second tableau permet à l'administrateur du réseau de faire une configuration statique des paramètres quantitatifs à utiliser par le routeur lors de la prise de décision de contrôle d'admission pour les demandes de service quantitatives. Chaque rangée de ce tableau a la forme suivante :

DSCP : profil de baquet de jetons

La première colonne spécifie les DSCP pour lesquels s'applique le contrôle d'admission quantitatif. La seconde colonne spécifie les paramètres de baquet de jetons qui représentent les ressources disponibles totales dans le réseau diff-serv pour s'accommoder du trafic dans la classe de service spécifiée par le DSCP.

Déclaration complète de droits de reproduction

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