Groupe de travail Réseau
Request for Comments : 2753
Catégorie : Information
Traduction Claude Brière de L'Isle

R. Yavatkar, Intel
D. Pendarakis, IBM
R. Guerin, Université de Pennsylvanie
janvier 2000

Cadre pour un contrôle d'admission fondé sur la politique

1. Introduction

Les groupes de travail de l'IETF Services intégrés (appelé "int-serv") et RSVP [RFC2205] ont développé des extensions à l'architecture IP et le modèle de service "au mieux" de sorte que les applications ou les usagers finaux peuvent demander une qualité (ou des niveaux) de service spécifique à partir d'un inter-réseau, en plus du service IP au mieux actuel. Les efforts récents du groupe de travail Services différenciés se sont aussi portés sur la définition des mécanismes qui prennent en charge des services de qualité de service agrégée. Le modèle "int-serv" pour ces nouveaux services exige une signalisation explicite des exigences de QS (Qualité de service) de la part des points d'extrémité et la fourniture du contrôle d'admission et du trafic chez les routeurs de services intégrés. Les normes proposées pour RSVP [RFC2205] et pour les services intégrés [RFC2211], [RFC2212] sont des exemples, respectivement, de nouveau protocole d'établissement de réservation, et de définitions de nouveaux services. Avec le modèle int-serv, certains flux de données reçoivent un traitement préférentiel par rapport aux autres flux ; le composant de contrôle d'admission ne prend en compte que la demande de réservation de ressource du demandeur et la capacité disponible pour déterminer si il peut accepter ou non une demande de QS. Cependant, le mécanisme int-serv ne comporte pas un aspect important du contrôle d'admission : les gestionnaires de réseau et les fournisseurs de service doivent être capables de surveiller, contrôler, et mettre en application l'utilisation des ressources et services du réseau sur la base des politiques déduites de critères tels que l'identité des usagers et des applications, des exigences de trafic/bande passante, de considérations de sécurité, et de l'heure ou du jour. De même, les mécanismes diff-serv doivent aussi tenir compte des politiques qui impliquent divers critères tels que l'identité du consommateur, les points d'entrée, et ainsi de suite.

Le présent document s'occupe de la spécification du cadre de la fourniture du contrôle fondé sur la politique des décisions de contrôle d'admission. En particulier, il se concentre sur le contrôle fondé sur la politique du contrôle d'admission qui utilise RSVP comme exemple de mécanisme de signalisation de la qualité de service. Bien que ce travail soit centré sur le contrôle d'admission fondé sur RSVP, le document dégage un cadre qui peut servir au contrôle d'admission fondé sur la politique dans d'autres contextes de qualité de service. On explique que le contrôle fondé sur la politique doit être applicable à différents types et qualités de services offerts dans le même réseau, et notre objectif est de considérer de telles extensions chaque fois que possible.

On commence par une liste de définitions à la Section 2. La Section 3 fait la liste des exigences et des objectifs du mécanisme utilisé pour contrôler et mettre en application l'accès à une meilleure QS. On expose ensuite les éléments d'architecture du cadre à la Section 4 qui décrit aussi les fonctions attendues de chaque composant. La Section 5 expose des exemples de politiques, des scénarios possibles, et les politiques de soutien pour ces scénarios. La Section 6 spécifie les exigences pour qu'un protocole client-serveur communique entre un serveur de politique (PDP) et son client (PEP) et évalue l'adéquation de certains protocoles existants à cet égard.

2. Terminologie

Les termes qui suivent sont utilisé dans le présent document.

Domaine administratif : collection de réseaux soumis au même contrôle administratif et groupés pour les besoins de l'administration.

Élément ou nœud de réseau : les routeurs, commutateurs, concentrateurs sont des exemples de nœuds de réseau. Ils sont les

entités où doivent être prises les décisions d'allocation de ressource et où ces décisions doivent être mises en application. Un routeur RSVP qui alloue une partie de la capacité d'une liaison (ou d'une mémoire tampon) à un flux particulier et s'assure que seuls les flux admis ont accès à ses ressources réservées est un exemple d'élément de réseau intéressant dans notre contexte.

Dans le présent document, on utilise indifféremment les termes de routeur, élément de réseau, et de nœud de réseau, mais ils devraient être interprétés par référence à un élément de réseau.

Protocole de signalisation de la QS : c'est un protocole de signalisation qui porte une demande de contrôle d'admission pour une ressource, par exemple, RSVP.

Politique : c'est la combinaison de règles et de services dans laquelle les règles définissent les critères de l'accès et de l'usage de la ressource.

Contrôle de politique : c'est l'application de règles pour déterminer si l'accès à une ressource particulière devrait être accordé ou non.

Objet de politique : il contient des informations qui se rapportent à la politique comme des éléments de politique, et ils sont portés dans une demande ou une réponse qui se rapporte à une décision d'allocation de ressource.

Élément de politique : subdivision des objets de politique; qui contient l'unité d'information nécessaire pour l'évaluation des règles de politique. Un seul élément de politique peut porter une identification d'usager ou d'application tandis qu'un autre élément de politique va porter des accréditifs d'usager ou des informations de carte de crédit. Les éléments de politique eux-mêmes sont supposés être indépendants du protocole de signalisation de QS utilisé.

Point de décision de politique (PDP) : c'est le point où sont prises les décisions de politique.

Point de mise en application de politique (PEP) : c'est le point où sont appliquées les décisions de politique.

Nœud ignorant de la politique (PIN, *Policy Ignorant Node*) : c'est un élément de réseau qui ne prend pas explicitement en charge le contrôle de politique utilisant les mécanismes définis dans le présent document.

Ressource : c'est quelque chose qui a une valeur dans une infrastructure de réseau à laquelle des règles ou des critères de politique sont appliques avant d'accorder l'accès. On peut citer comme exemples de ressources les mémoires tampon dans un routeur et la bande passante sur une interface.

Fournisseur de service : il contrôle l'infrastructure du réseau et peut être responsable de la facturation et de la comptabilité des services.

Modèle d'état conditionnel : l'état conditionnel *(Soft state)* est une forme du modèle à états pleins qui gère la péremption de l'état installé au PEP ou au PDP. C'est une façon automatique de supprimer l'état en présence de défaillances de la communication ou d'un élément de réseau. Par exemple, RSVP utilise le modèle à états conditionnels pour installer l'état de réservation sur les éléments de réseau le long du chemin d'un flux de données.

État installé : c'est une nouvelle et unique demande faite à partir d'un PEP à un PDP qui doit être explicitement supprimée.

Nœud de confiance : c'est un nœud qui est dans les limites d'un domaine administratif (AD) et est de confiance, au sens que les demandes de contrôle d'admission provenant d'un tel nœud n'ont pas nécessairement besoin d'une décision de PDP.

3. Objectifs et exigences du contrôle d'admission fondé sur la politique

Dans cette section, on décrit les objectifs et les exigences des mécanismes et protocoles conçus pour fournir le contrôle fondé sur la politique sur les décisions de contrôle d'admission.

- Politiques et mécanismes : un point important à noter est que le cadre n'inclut aucune discussion d'un comportement spécifique d'une politique ni n'exige l'usage de politiques spécifiques. La cadre souligne plutôt les éléments et mécanismes de l'architecture qui sont nécessaires pour permettre une large variété de politiques possibles.

- Spécifique de RSVP : les mécanismes doivent être conçus pour satisfaire les exigences de contrôle fondés sur la politique spécifiques du problème de réservation de la bande passante en utilisant RSVP comme protocole de

signalisation. Cependant, notre objectif est de permettre l'application de ce cadre pour les contrôle d'admission impliquant d'autres types de ressources et de services de QS (par exemple, Diff-Serv) pour autant qu'ils ne divergent pas de notre objectif central.

- Prise en charge de la préemption : les mécanismes conçus doivent inclure la prise en charge de la préemption. Par préemption, on veut dire la capacité à retirer un état précédemment installé en faveur de l'acceptation d'une nouvelle demande de contrôle d'admission. Par exemple, dans le cas de RSVP, la préemption implique la capacité à retirer une ou plusieurs réservations actuellement installées pour faire de la place à une nouvelle de mande de réservation de ressource.

- Prise en charge de nombreux styles de politiques : les mécanismes conçus doivent inclure la prise en charge de nombreuses politiques et configurations de politiques, incluant des accords de service bilatéraux et multilatéraux et des politiques fondées sur la notion de priorité relative. En général, la détermination et la configuration de politiques viables est de la responsabilité du fournisseur de service.

- Fourniture des informations de surveillance et de comptabilité : les mécanismes doivent inclure la prise en charge de l'état de la politique de surveillance, de l'utilisation des ressources, et fournir les informations d'accès. En particulier, doivent être inclus les mécanismes qui fournissent les informations d'usage et d'accès qui peuvent être utilisés pour les besoins de la comptabilité et la facturation.

- Tolérance aux fautes et récupération : les mécanismes conçus sur la base de ce cadre doivent inclure des dispositions pour la tolérance aux fautes et la récupération des cas de défaillance telles que celles des PDP, des interruptions dans la communication incluant des partitions de réseau (et les fusions qui s'ensuivent) qui séparent un PDP de ses PEP associés.

- Prise en charge des nœuds ignorants de la politique (PIN, *Policy-Ignorant Node*) : la prise en charge des mécanismes décrits dans ce document ne devrait pas être obligatoire pour tous les nœuds d'un réseau. Le contrôle d'admission fondé sur la politique pourrait être mis en application sur un sous-ensemble des nœuds, par exemple, les nœuds frontière au sein d'un domaine administratif. Ces nœuds capables de politique fonctionneraient comme nœuds de confiance du point de vue des nœuds ignorants de la politique dans ce domaine administratif.

- Adaptabilité : une des exigences importantes du mécanisme conçu pour le contrôle de politique est l'adaptabilité. Les mécanismes doivent s'adapter au moins dans la même mesure que RSVP au sens de s'accommoder de plusieurs flux et nœuds de réseau sur le chemin d'un flux. En particulier, l'adaptabilité doit être considérée lorsque on spécifie un comportement par défaut pour la fusion d'objets de données de politique, et la fusion ne devrait pas résulter en la duplication d'éléments ou objets de politique. Il y a plusieurs domaines sensibles en termes d'adaptabilité pour le contrôle de politique sur RSVP. D'abord, on ne devrait pas s'attendre à ce que chaque nœud à capacité de politique d'une infrastructure contacte un PDP distant. Cela pourrait éventuellement causer de longs délais pour la vérification des demandes qui doivent voyager bond par bond. Ensuite, RSVP est capable d'établir des réservations de ressource réservations pour des flux en diffusion groupée. Cela implique que le modèle de contrôle de politique soit capable de servir les exigences particulières de grands flux en diffusion groupée. Donc, l'architecture de contrôle de politique doit s'adapter au moins aussi bien que RSVP sur la base de facteurs tels que la taille des messages RSVP, le temps requis pour que le réseau serve une demande RSVP, le temps de traitement local requis par nœud, et la mémoire locale consommée par nœud.

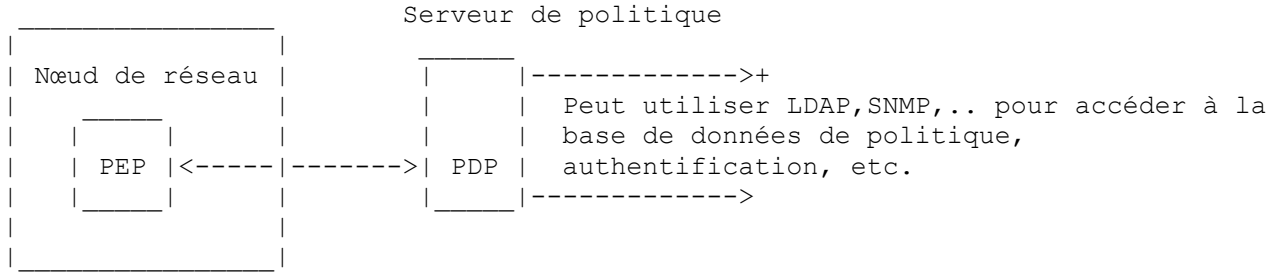
- Considérations de sécurité et de déni de service : l'architecture de contrôle de politique doit être sûre en ce qui concerne les aspects suivants. D'abord, les mécanismes proposés dans le cadre doivent minimiser les menaces de vol et de déni de service. Ensuite, elle doit s'assurer que les entités (telles que les PEP et les PDP) qui sont impliqués dans le contrôle de politique peuvent vérifier leurs identité respectives et établir la confiance nécessaire avant de communiquer.

4. Éléments d'architecture

Les deux principaux éléments architecturaux du contrôle de politique sont le point de mise en application de politique (PEP, *Policy Enforcement Point*) et le point de décision de politique (PDP, *Policy Decision Point*). La Figure 1 montre une configuration simple qui implique ces deux éléments ; le PEP est un composant au nœud de réseau et le PDP est une entité distante qui peut résider dans un serveur de politique. Le PEP représente le composant qui fonctionne toujours sur le nœud à capacité de politique. Il est le point auquel sont en fait mises en application les décisions de politique. Les décisions de politique sont principalement prises au PDP. Le PDP lui-même peut faire usage de mécanismes et protocoles supplémentaires pour réaliser des fonctionnalités supplémentaires telles que l'authentification de l'usager, la comptabilité, la mémorisation des informations de politique, etc. Par exemple, le PDP va vraisemblablement utiliser un service de répertoire fondé sur LDAP pour mémoriser et restituer les informations de politique [SCHEMA]. Le présent document ne

comporte pas d'exposé sur ces mécanismes et protocoles supplémentaires ni sur la façon de les utiliser.

L'interaction de base entre les composants commence avec le PEP. Le PEP va recevoir une notification ou un message qui exige une décision de politique. Au vu d'un tel événement, le PEP formule alors une demande de décision de politique et l'envoie au PDP. Cette demande de contrôle de politique de la part d'un PEP au PDP peut contenir un ou plusieurs éléments de politique (encapsulés dans un ou plusieurs objets de politique) en plus des informations de contrôle d'admission (telles qu'une spécification de flux *(flowspec)* ou la quantité de bande passante demandée) dans le message ou événement d'origine qui a déclanché la demande de décision de politique. Le PDP retourne la décision de politique et le PEP met alors en application la décision de politique en acceptant ou en rejetant la demande de la façon appropriée. Le PDP peut aussi retourner des informations supplémentaires au PEP qui incluent un ou plusieurs éléments de politique. Ces informations ne sont pas nécessairement associées à une décision de contrôle d'admission. Elles peuvent plutôt être utilisées pour formuler un message d'erreur ou un message sortant/transmis.



PDP peut utiliser des mécanismes et protocoles supplémentaires pour les besoins de la comptabilité, de l'authentification, la mémorisation des politiques, etc.

Figure 1 : Configuration simple avec les principaux composants d'architecture de contrôle de politique

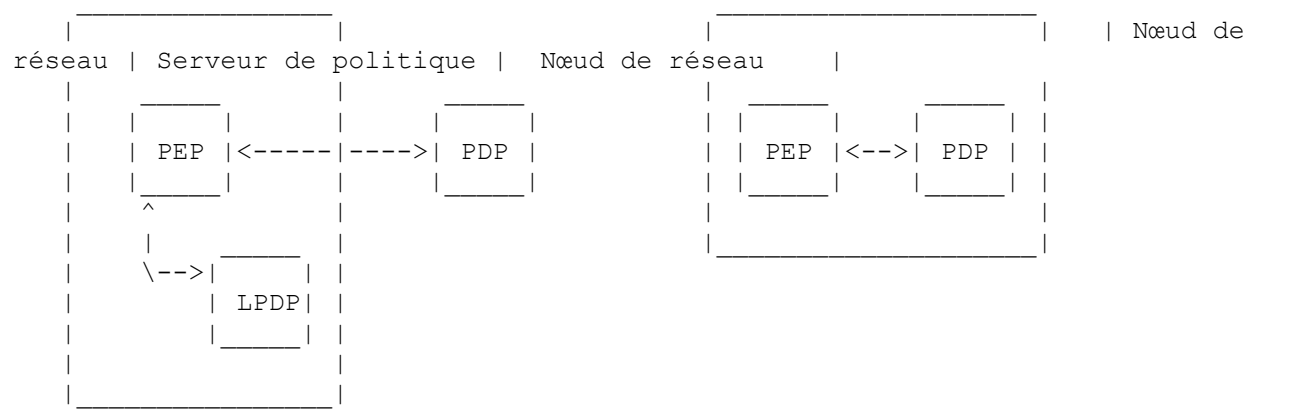
Le PDP peut facultativement contacter d'autres serveurs externes, par exemple, pour accéder à la configuration, pour l'authentification de l'utilisateur, pour les bases de données de comptabilité et de facturation. Les protocoles définis pour la gestion de réseau (SNMP) ou l'accès à des répertoires (LDAP) peuvent être utilisés pour ces communications. Bien que le type d'accès et les protocoles spécifiques utilisés puissent varier parmi les différentes mises en œuvre, certaines de ces interactions auront des implications à l'échelle du réseau et pourraient impacter l'interopérabilité de différents appareils.

D'une importance particulière est le "langage" utilisé pour spécifier les politiques mises en œuvre par le PDP. Le nombre de politiques applicables à un nœud de réseau peut éventuellement être assez grand. En même temps, ces politiques vont présenter une forte complexité, en termes de nombre de champs utilisés pour arriver à une décision, et une large gamme de décisions. De plus, il est vraisemblable que plusieurs politiques pourraient être applicables au même profil de demande. Par exemple, une politique peut prescrire le traitement des demandes provenant d'un groupe d'utilisateurs généraux (par exemple, les employés d'une entreprise) aussi bien que le traitement des demandes provenant de membres spécifiques de ce groupe (par exemple, les gestionnaires de l'entreprise). Dans cet exemple, le profil d'utilisateur "gestionnaires" entre dans la spécification de deux politiques, une générale et une autre plus spécifique.

Pour traiter la complexité des décisions de politique et assurer une application cohérente et logique des politiques à l'échelle du réseau, le langage de spécification de la politique devrait assurer une transposition sans ambiguïté d'un profil de demande en action de politique. Il devrait aussi permettre la spécification de la séquence d'application des différentes règles de politique et/ou la priorité associée à chacune. Certaines de ces questions sont traitées dans [SCHEMA].

Dans certains cas, la simple configuration indiquée à la Figure 1 peut n'être pas suffisante car il peut être nécessaire d'appliquer des politiques locales (par exemple, des politiques spécifiées dans des listes de contrôle d'accès) en plus des politiques appliquées au PDP distant. De plus, il est possible que le PDP soit colocalisé avec le PEP sur le même nœud de réseau. La Figure 2 montre les configurations possibles.

Les configurations montrées aux Figures 1 et 2 illustrent la souplesse de la division du travail. D'un côté, un serveur de politique centralisé, qui pourrait être chargé des décisions de politique au nom de plusieurs nœuds de réseau dans un domaine administratif, pourrait mettre en œuvre des politiques sur une grande échelle, communes à travers le domaine administratif. D'un autre côté, les politiques qui dépendent d'informations et conditions locales pour un routeur particulier et qui sont plus dynamiques, pourraient être mieux mises en en œuvre localement, au routeur.



La configuration de gauche montre un point de décision local au nœud de réseau et la configuration de droite montre un PEP et un PDP colocalisés sur le même nœud.

Figure 2 : Deux autres configurations possibles de contrôle de politique sur les composants architecturaux

Si il est disponible, le PEP va d'abord utiliser le LPDP pour prendre une décision locale. Cette décision partielle et la demande de politique d'origine sont ensuite envoyées au PDP qui va prendre une décision finale (outrepassant éventuellement celle du LPDP). On doit noter que le PDP agit comme autorité en dernier ressort pour la décision retournée au PEP et que le PEP doit mettre en application la décision prise par le PDP. Finalement, si un état partagé a été établi pour la demande et la réponse entre le PEP et le PDP, il est de la responsabilité du PEP de notifier au PDP que la demande d'origine n'est plus utilisée.

Sauf spécification contraire, on supposera la configuration de gauche de la Figure 2 dans la suite de ce document.

Dans ce modèle de contrôle de politique, le module PEP au nœud de réseau doit suivre les étapes suivantes pour prendre une décision de politique :

1. Lorsque un événement ou message local invoque le PEP pour une décision de politique, celui-ci crée une demande qui comporte les informations provenant du message (ou de l'état local) qui décrivent la demande de contrôle d'admission. De plus, la demande comporte les éléments de politique appropriés, comme décrit ci-dessous.
2. Le PEP peut consulter une base de données locale de configuration pour identifier un ensemble d'éléments de politique (appelé ensemble A) qui seront évalués localement. La configuration locale spécifie les types d'éléments de politique qui sont évalués en local. Le PEP passe la demande avec l'ensemble A au point de décision local (LPDP) et récolte le résultat du LPDP (appelé "résultat partiel" et qu'on notera D(A)).

3. Le PEP passe alors la demande avec TOUS les éléments de politique et D(A) au PDP. Le PDP applique les politiques sur la base de tous les éléments de politique et de la demande, et prend une décision (qu'on va appeler D(Q)). Il combine alors son résultat avec le résultat partiel D(A) en utilisant une opération de combinaison pour prendre une décision finale.

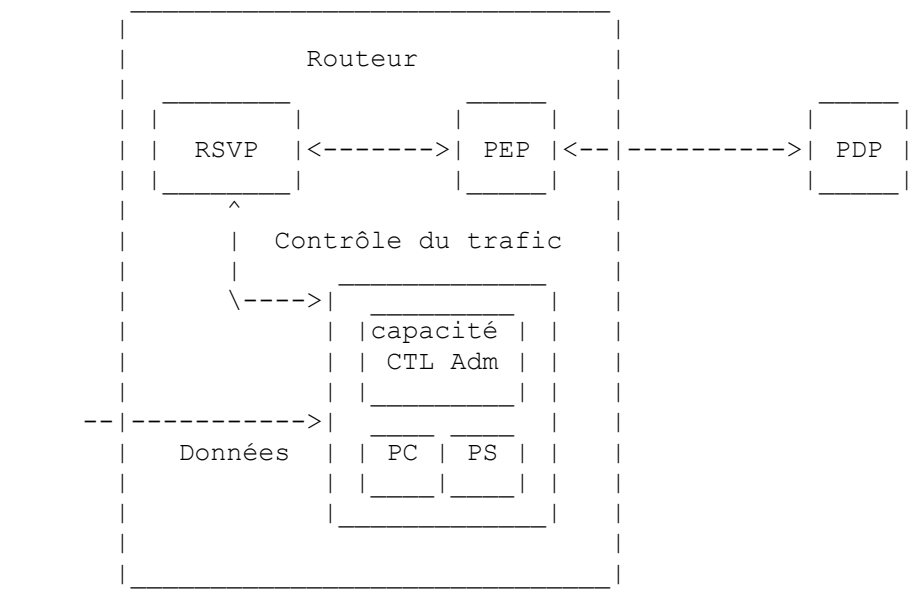
4. Le PDP retourne la décision finale de politique (obtenue de l'opération de combinaison) au PEP.

Noter que dans le modèle ci-dessus, le PEP DOIT contacter le PDP même si aucun objet (ou l'objet NUL) de politique n'est reçu dans la demande de contrôle d'admission. Cette exigence aide à garantir qu'une demande ne puisse outrepasser un contrôle de politique en omettant des éléments de politique dans une demande de réservation. Cependant, le traitement en "court circuit" est permis, c'est-à-dire, si le résultat de D(A), ci-dessus, est "non", il n'est alors pas besoin de poursuivre le traitement de politique au PDP. Cependant, le PDP doit être informé de l'échec du traitement local de politique. Cela s'applique de même au cas où le traitement de politique réussit mais où le contrôle d'admission (au niveau de la gestion de ressource du fait de capacités indisponibles) échoue ; là encore, le PDP doit être informé de l'échec.

On notera aussi que le PDP peut, à tout moment, envoyer une notification asynchrone au PEP pour changer une décision antérieure ou générer un message d'erreur/avertissement de politique.

4.1 Exemple d'un routeur RSVP

Dans le cas d'un routeur RSVP, la Figure 3 montre l'interaction entre un PEP et les autres composants int-serv au sein du routeur. Pour les besoins de l'exposé, on représente tous les composants du traitement en rapport avec RSVP par un seul module RSVP, mais un exposé plus détaillé de l'interaction exacte et des interfaces entre RSVP et le PEP est fourni dans un autre document [RFC2750].



PC = Classeur de paquet, PS = Programmeur de paquet

Figure 3 : Relations entre le PEP et les autres composants int-serv au sein d'un routeur RSVP.

Lorsque un message RSVP arrive au routeur (ou qu'un événement en rapport avec RSVP exige une décision de politique) le module RSVP est supposé passer la demande (correspondant à l'événement ou au message) à son module PEP. Le PEP va utiliser le PDP (et le LPDP) pour obtenir la décision de politique et la communiquer en retour au module RSVP.

4.2 Fonction supplémentaires au PDP

Normalement, le PDP retourne la décision finale de politique sur la base d'une demande de contrôle d'admission et des éléments de politique associés. Cependant, il devrait être possible que parfois le PDP demande au PEP (ou au module de contrôle d'admission à l'élément de réseau où réside le PEP) de générer des messages d'erreur en rapport avec la politique. Par exemple, dans le cas de RSVP, le PDP peut accepter une demande et permettre l'installation et transmettre une réservation à un bond précédent, mais en même temps, peut souhaiter générer un message d'avertissement/erreur à un nœud aval (NHOP) pour l'avertir de conditions telles que "il se peut que votre demande soit supprimée dans 10 minutes, etc." Au fond, on a besoin de la capacité de créer des erreurs et/ou avertissements sur la politique et de les propager en utilisant le protocole natif de signalisation de QS (comme RSVP). De telles erreurs de politique retournées par le PDP doivent être capables aussi de spécifier si la demande de réservation devrait encore être acceptée, installée, et transmise pour permettre de continuer le traitement normal de RSVP. En particulier, quand un PDP renvoie une erreur, il spécifie que :

1. le message qui a généré la demande de contrôle d'admission devrait continuer d'être traité comme d'habitude, mais un message d'erreur (ou d'avertissement) sera envoyé dans l'autre direction et inclura les objets de politique fournis dans ce message d'erreur,
2. ou, qu'une erreur est retournée, mais que le message RSVP ne devrait pas être transmis comme d'habitude.

4.3 Interactions entre PEP, LPDP, et PDP chez un routeur RSVP

Tous les détails du traitement du message RSVP et les interactions associées entre les différents éléments dans un routeur RSVP (PEP, LPDP) et un PDP figurent dans d'autres documents [RFC2750], [RFC2749]. Dans ce qui suit sont énumérés quelques points saillants qui se rapportent au cadre :

* Le LPDP est facultatif et peut être utilisé pour prendre des décisions sur la base d'éléments de politique traités en local. Par contre, le LPDP peut devoir aller dans des entités externes (comme un serveur de répertoire ou un serveur d'authentification, etc.) pour prendre ses décisions.
* Le PDP est à états pleins et peut prendre des décisions même si aucun objet de politique n'est reçu (par exemple, prendre des décisions sur la base d'informations comme des spécifications de flux et des objets de session dans les messages RSVP). Le PDP peut consulter d'autres PDP, mais la discussion des communications et de la coordination inter PDP sort du domaine d'application du présent document.
* Le PDP envoie des notifications asynchrones au PEP chaque fois que nécessaire pour changer des décisions antérieures, générer des erreurs, etc.
* Le PDP exporte les informations utiles pour la surveillance de l'utilisation et les besoins de la comptabilité. Un exemple

de mécanisme utile à cette fin est une MIB ou une base de données relationnelle. Cependant, le présent document ne spécifie aucun mécanisme particulier pour cela et la discussion d'un tel mécanisme sort du domaine d'application de ce document.

4.4 Position des éléments de politique dans un réseau

En permettant la division du travail entre un LPDP et un PDP, l'architecture de contrôle de politique autorise un déploiement étagé en permettant aux routeurs des degrés variés de sophistication, pour ce qui concerne le contrôle de politique, pour communiquer avec les serveurs de politique. La Figure 4 décrit un exemple d'ensemble de nœuds appartenant à trois domaines administratifs (AD) différents. (Dans ce cas, chaque AD pourrait correspondre à un fournisseur de service différent). Les nœuds A, B et C appartiennent au domaine administratif AD-1, et sont renseignés par le PDP PS-1, alors que D et E appartiennent respectivement à AD-2 et AD-3. E communique avec le PDP PS-2. En général, on s'attend à ce qu'il y ait au moins un PDP par domaine administratif.

Les nœuds de réseau à capacité de politique vont du très basique, comme E, qui n'a pas de LPDP et doit donc s'appuyer sur un PDP externe pour chaque opération de traitement de politique, à l'autosuffisant, comme D qui met essentiellement en application à la fois un LPDP et un PDP en local, au routeur.

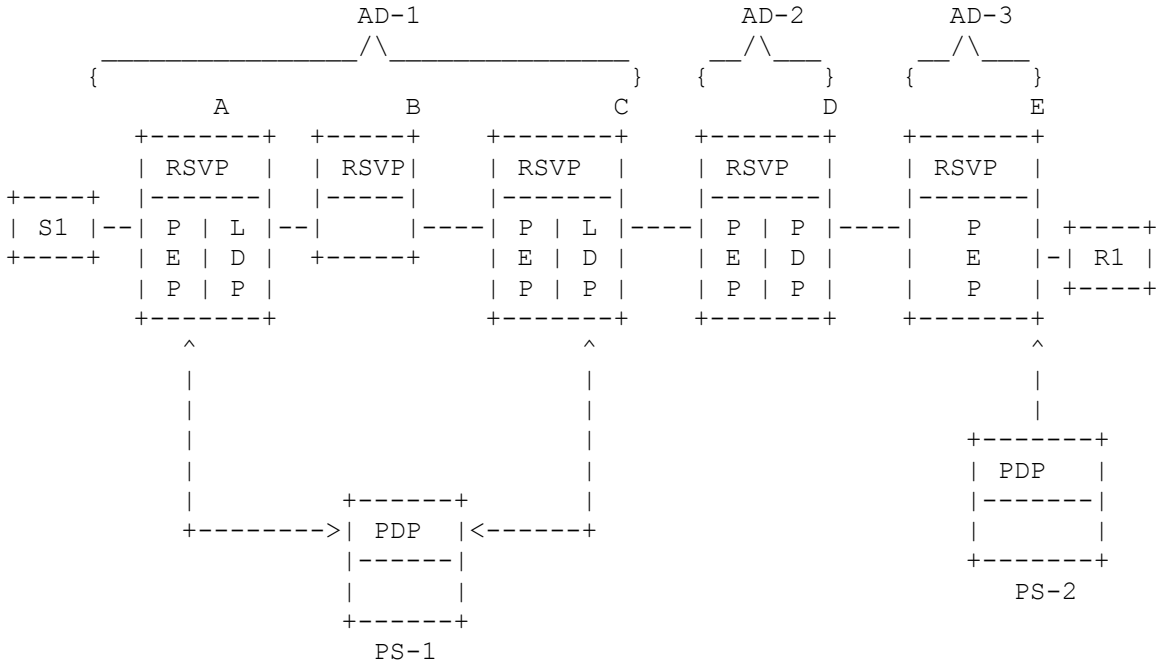


Figure 4 : Position des éléments de politique dans un internet

5. Exemple de politiques, de scénarios, et de prise en charge de politique

Dans ce qui suit sont présentés des exemples de politiques désirées et de scénarios qui exigent un contrôle de politique que le cadre de contrôle de politique devrait être capable de prendre en charge. Dans certains cas sont mentionnées une ou des approches possibles pour réaliser les objectifs désirés, avec une liste des problèmes qui restent à résoudre.

5.1 Politiques de contrôle d'admission fondées sur des facteurs tels que l'heure, l'identité de l'usager, ou des accréditifs

Le contrôle de politique doit être capable d'exprimer et de mettre en application des règles pour des durées limitées. Par exemple, un groupe d'usagers peut être autorisé à faire des réservations à un certain niveau seulement durant les heures creuses. De plus, le contrôle de politique doit aussi prendre en charge les politiques qui prennent en compte l'identité ou les accréditifs des usagers qui demandent un service ou ressource particulier. Par exemple, une demande de réservation RSVP peut être refusée ou acceptée sur la base des accréditifs ou de l'identité fournie dans la demande.

5.2 Accord bilatéral entre fournisseurs de service

Jusqu'à il y a peu, les accords d'usage entre les fournisseurs de service pour le trafic franchissant leurs frontières avaient été assez simples. Par exemple, deux FAI peuvent se mettre d'accord pour accepter tout le trafic de l'un vers l'autre, souvent sans effectuer aucune comptabilité ni facturation pour le "trafic étranger" transporté. Cependant, avec la disponibilité de mécanismes de qualité de service fondés sur les services intégrés et différenciés, la différenciation de trafic et les garanties de qualité de service sont introduites dans l'Internet. Comme les FAI commencent à vendre à leurs abonnés différents niveaux de service et qu'ils peuvent différencier les différentes sources de trafic, ils vont aussi chercher des mécanismes pour se facturer les uns les autres le trafic (et les réservations) qui transite par leurs réseaux. Une incitation supplémentaire pour établir de tels mécanismes est l'asymétrie potentielle dans la base de consommateurs que vont exploiter les différents fournisseurs. Les FAI centrés sur le trafic d'entreprise vont vraisemblablement faire face à une plus forte demande pour des services réservés que ceux qui desservent le marché grand public. L'absence de schémas de comptabilité sophistiqués pour le trafic inter FAI pourrait conduire à une allocation inefficace des coûts entre les différents fournisseurs de service.

Les accords bilatéraux peuvent rentrer dans les deux grandes catégories locale ou globale. Du fait de la complexité du problème, on s'attend à ce que dans un premier temps seuls les premiers soient mis en œuvre. Dans ces accords locaux, les fournisseurs qui gèrent un nuage de réseau ou un domaine administratif passent un contrat avec leur plus proche point de contact (voisin) pour établir des règles de base et des arrangements pour le contrôle d'accès et la comptabilité. Ces contrats sont essentiellement locaux et ne s'appuient pas sur des accords globaux ; par conséquent, un nœud de politique conserve les informations sur ses seuls nœuds voisins. En se référant à la Figure 4, ce modèle implique que le fournisseur AD-1 a établi des accords avec AD-2, mais pas avec AD-3, pour l'usage de leurs réseaux réciproques. Le fournisseur AD-2, à son tour, a mis en place des accords avec AD-3 et ainsi de suite. Et donc, lors de la transmission d'une demande de réservation pour AD-2, le fournisseur AD-2 va facturer à AD-1 l'utilisation de toutes les ressources au delà du réseau de AD-1. Ces informations sont obtenues en appliquant de façon récurrente les accords bilatéraux à chaque frontière entre les fournisseurs (voisins) jusqu'à atteindre le receveur de la demande de réservation. Pour mettre en œuvre ce schéma dans l'architecture de contrôle de politique, les nœuds frontière doivent ajouter un objet de politique approprié au message RSVP avant de le transmettre au réseau d'un fournisseur voisin. Cet objet de politique va contenir des informations telles que l'identité du fournisseur qui les a générées et l'équivalent d'un numéro de compte sur lequel puissent être accumulées les factures. Comme les accords ne se font qu'entre des nœuds voisins, les objets de politique doivent être réécrits lorsque les messages RSVP franchissent les frontières des domaines administratifs ou les réseaux du fournisseur.

5.3 Politiques de contrôle d'admission fondées sur la priorité

Dans de nombreux réglages, il est utile de distinguer entre les réservations sur la base d'un certain niveau "d'importance". Par exemple, cela peut être utile pour éviter que la première réservation à laquelle est accordée l'utilisation de certaines ressources soit capable d'accaparer ces ressources pour une durée indéterminée. De même, cela peut être utile de permettre que des appels d'urgence puissent passer même durant les périodes d'encombrement. De telles fonctionnalités peuvent être prises en charge en associant des priorités aux demandes de réservation, et en convoyant ces informations de priorité avec les autres informations de politique.

Sous sa forme de base, la priorité associée à une réservation détermine directement les droits d'une réservation aux ressources qu'elle demande. Par exemple, en supposant que les priorités soient exprimées par des entiers dans la gamme de 0 à 32, 32 étant la plus forte priorité, une réservation de priorité, disons, 10, va toujours être acceptée si la quantité de ressources détenue par les réservations de priorité inférieure est suffisante pour satisfaire à ses exigences. En d'autres termes, dans le cas où il n'y a pas assez de ressources libres (bande passante, mémoires tampons, etc.) sur un nœud pour satisfaire la demande de priorité 10, le nœud va tenter de libérer les ressources nécessaires en préemptant les réservations existantes de priorité inférieure.

Il y a un certain nombre d'exigences associées à la prise en charge des priorités et à leur fonctionnement correct. Tout d'abord, le contrôle du trafic au routeur doit être au courant des priorités, c'est-à-dire, classer les réservations existantes selon leur priorité, afin qu'il soit capable de déterminer combien préempter et lesquelles, lorsqu'il doit satisfaire une demande de réservation de priorité supérieure. Ensuite, il est important que les préemptions soient faites de façon cohérente sur les différents nœuds, afin d'éviter des instabilités transitoires. Enfin, et peut-être le plus important, la fusion des priorités doit être organisée avec soin et son impact clairement compris au titre de la définition de politique qui y est associée.

Des trois exigences ci-dessus, la fusion des informations de priorité est la plus complexe et mérite une discussion supplémentaire. La complexité de la fusion des informations de priorité provient du fait que cette fusion doit être effectuée en plus de la fusion des informations de réservation. Lorsque les informations de réservation (FLOWSPEC) sont identiques, c'est-à-dire, des réservations homogènes, la fusion a seulement besoin de considérer les informations de priorité, et la simple règle de conserver la plus forte priorité donne une réponse adéquate. Cependant, dans le cas de réservations hétérogènes, la *nature bidimensionnelle* de la paire (FLOWSPEC, priorité) rend difficile leur classement et donc leur fusion. Une description du traitement des différents cas des objets de priorité RSVP est présentée dans [RFC2751].

5.4 Carte d'appel ou jetons prépayés

Un modèle de popularité croissante dans le réseau téléphonique est celui de la carte prépayée. Ce concept pourrait aussi être appliqué à l'Internet ; les usagers achètent des "jetons" qui peuvent être utilisés ultérieurement pour accéder aux services du réseau. Lorsque un usager fait une demande de réservation au moyen, par exemple, d'un message RESV de RSVP, il fournit un numéro d'identification univoque du "jeton", enveloppé dans un objet de politique. Le traitement de cet objet par des routeurs à capacité politique a pour résultat de décrémenter la valeur, ou le nombre d'unités de service restantes, de ce jeton.

En se référant à la Figure 4, on suppose que le receveur R1 dans le domaine administratif AD3 veut demander une réservation pour un service généré en AD1. R1 génère un objet de données de politique de type PD(prc, CID), où "prc" note une carte prépayée et CID est le numéro d'identification de la carte. Avec les autres objets de politique portés dans le message RESV, cet objet est reçu par le nœud E, qui le transmet à son PEP, le PEP_E, qui, à son tour, contacte le PDP PS-3. PS-3 conserve en local ou a un accès distant à une base de données de numéros de cartes prépayées. Si la quantité de crédit restant dans CID est suffisante, le PDP accepte la réservation et l'objet de politique est retourné au PEP_E. Deux problèmes doivent être résolus ici :

* Quelle est la portée de ces charges ?

* Quand ces charges (sous la forme du décrément du crédit restant) sont elles appliquées ?

La réponse à la première question se rapporte au modèle d'accord bilatéral en place. Si par ailleurs le fournisseur AD-3 a établi des accords avec AD-2 et AD-1, il pourrait facturer le coût de la réservation complète jusqu'à l'envoyeur S1. Dans ce cas, PS-2 déplace l'objet PD(prc,CID) du message RESV sortant.

D'un autre côté, si AD-3 n'a pas mis en place d'accord bilatéral, il va simplement facturer CID pour le coût de la réservation au sein de AD-3 puis transmettre PD(prc,CID) dans le message RESV sortant. Les PDP suivants dans les autres domaines administratifs vont facturer CID pour leurs réservations respectives. Comme plusieurs entités lisent (le crédit restant) et écrivent (pour diminuer le crédit) sur la même base de données, une certaine coordination et contrôle de concurrence peut être nécessaire. Les questions relatives à la localisation, à la gestion, à la coordination de la base de données de carte de crédit (ou outil similaire) sortent du domaine d'application du présent document.

Un autre problème de ce scénario est de déterminer quand le crédit est épuisé. Le PDP devrait contacter périodiquement la base de données pour imputer ses charges au CID ; si le crédit restant est nul, il doit y avoir un mécanisme pour le détecter et causer la révocation ou la fin des privilèges accordés sur la base du crédit.

Concernant la question de savoir quand initier la facturation, cela ne devrait idéalement n'arriver qu'après la réussite de la demande de réservation. Dans le cas de facturations locales, cela pourrait être communiqué par le routeur au PDP.

5.5 Restrictions spécifiées par l'envoyeur sur les réservations du receveur

La capacité des envoyeurs à spécifier des restrictions aux réservations, sur la base de l'identité du receveur, sur le nombre de receveurs ou sur le coût de la réservation peut être utile dans de futures applications réseau. Un exemple en pourrait être toute application dans laquelle l'envoyeur paye pour le service livré aux receveurs. Dans un tel cas, l'envoyeur peut vouloir supporter le coût de la réservation, pour autant qu'elle satisfasse à certains critères, par exemple, si elle est générée par un receveur qui appartient à une liste de contrôle d'accès (ACL, *access control list*) et satisfait à une limite de coût. (Noter que cela peut permettre la formation de groupes de diffusion groupée "fermés").

Dans le cadre de contrôle d'admission fondé sur la politique, un tel schéma pourrait être réalisé en faisant que l'envoyeur génère des objets de politique appropriés, portés dans un message PATH, qui installe l'état dans les routeurs sur le chemin des receveurs. En acceptant les réservations, les routeurs auront à comparer les demandes RESV aux états installés.

Différentes solutions peuvent être bâties pour suivre ce scénario dont la description précise sort du domaine d'application du présent document.

6. Interaction entre PEP et PDP

Dans le cas d'un PDP externe survient le besoin d'un protocole de communication entre le PEP et le PDP. Afin de permettre l'interopérabilité entre les différents fabricants d'éléments de réseautage et les serveurs (externes) de politique, ce protocole devrait être normalisé.

6.1 Exigences du protocole de PEP à PDP

La présente section décrit un ensemble d'exigences générales du protocole de communication entre le PEP et un PDP externe.

* Fiabilité : La sensibilité des informations de contrôle de politique nécessite un fonctionnement fiable. La perte non détectée d'interrogations ou réponses de politique peut conduire à un fonctionnement incohérent du contrôle du réseau et est clairement inacceptable pour des actions telles que la facturation et la comptabilité. Une option pour assurer la fiabilité est de réutiliser TCP comme protocole de transport.

* Faibles délais : Les exigences de délai des décisions de politique qui se rapportent aux protocoles de signalisation de la QS sont supposées être assez strictes. Le protocole de PEP à PDP devrait n'ajouter qu'une petite quantité de délai au délai de réponse subi par les interrogations envoyées par le PEP au PDP.

* Capacité à porter des objets opaques : Le protocole devrait permettre de livrer des objets opaques auto identifiants, de longueur variable, tels que des messages RSVP, Les objets de politique RSVP et les autres objets qui pourraient être définis avec l'introduction de nouvelles politiques. Le protocole ne devrait pas avoir à changer chaque fois qu'un nouvel objet est introduit dans l'échange.

* Prise en charge de transactions bidirectionnelles à l'initiative du PEP : Le protocole doit permettre des transactions bidirectionnelles (échanges de demande-réponse) entre un PEP et un PDP. En particulier, les PEP doivent être capables d'initier des demandes de décision de politique, la renégociation d'une décision de politique prise antérieurement, et l'échange d'informations de politique. Dans une certaine mesure, cette exigence est intimement liée à l'objectif de satisfaire à l'exigence d'un contrôle d'admission spécifique de RSVP, fondé sur la politique. Les événements de signalisation RSVP tels que l'arrivée des messages de rafraîchissement RESV, les fins de temporisation d'état, et la fusion de réservations exigent qu'un PEP (tel qu'un routeur RSVP) demande une décision de politique au PDP à tout moment. De même, le PEP doit être capable de faire rapport des informations de surveillance et des changements d'état de politique au PDP à tout moment.

* Prise en charge de notification asynchrone : Ceci est exigé pour permettre à la fois au serveur de politique et au client de se notifier l'un l'autre un changement asynchrone de l'état, c'est-à-dire, un changement qui n'est pas déclanché par un message de signalisation. Par exemple, le serveur aurait besoin de notifier au client si une réservation particulière doit se terminer du fait de l'arrivée à expiration des accréditifs ou de la balance des comptes d'un usager. De même, le client doit informer le serveur du rejet d'une réservation qui est dû à une défaillance du contrôle d'admission.
* Traitement des groupes de diffusion groupée : Le protocole devrait prendre des dispositions pour le traitement des décisions de politique qui se rapportent aux groupes de diffusion groupée.
* Spécification de la qualité de service : Le protocole devrait permettre une spécification précise du niveau d'exigences de service dans les demandes de PEP transmises au PDP.

7. Considérations sur la sécurité

Le tunnel de communication entre les clients de politique et les serveurs de politique devrait être sécurisé par l'utilisation d'un canal IPSEC [RFC1825]. Il est conseillé que ce tunnel fasse usage des deux protocoles d'en-tête d'authentification (AH, *Authentication Header*) et d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) afin de fournir la confidentialité, l'authentification de l'origine des données, l'intégrité et la prévention des répétitions.

Dans le cas du mécanisme de signalisation RSVP, l'authentification de message RSVP MD5 [RFC2747] peut être utilisée pour sécuriser les communications entre les éléments de réseau.

8. Références

[RFC1825] R. Atkinson, "Architecture de sécurité pour le protocole Internet", août 1995. *(Rendue obsolète par la RFC2401)*

[RFC2138] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Service d'authentification distante d'utilisateur appelant (RADIUS)", avril 1997. (*Obsolète, voir* RFC2865) *(P.S.)*

[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.)*

[RFC2747] F. Baker, B. Lindell, M. Talwar, "Authentification cryptographique RSVP", janvier 2000. (*MàJ par* RFC3097) *(P.S.)*

[RFC2749] S. Herzog, et autres, "Utilisation de COPS avec RSVP", janvier 2000. *(P.S.)*

[RFC2750] S. Herzog, "Extensions à RSVP pour le contrôle de politique", janvier 2000. *(P.S.)*

[RFC2751] S. Herzog, "Élément de politique de priorité par préemption signalée", janvier 2000. (*Obsolète, voir* RFC3181) *(P.S.)*

[SCHEMA] Rajan, R., et al., "Schema for Differentiated Services and Integrated Services in Networks", Non publiée.

9. Remerciements

Le présent travail est le fruit de discussions avec de nombreux membres du groupe RAP, parmi lesquels Jim Boyle, Ron Cohen, Laura Cunningham, Dave Durham, Shai Herzog, Tim O'Malley, Raju Rajan, et Arun Sastry.

10. Adresse des auteurs

Raj Yavatkar	Dimitrios Pendarakis	Roch Guerin
Intel Corporation	IBM T.J. Watson Research Center	University of Pennsylvania
2111 N.E. 25th Avenue,	P.O. Box 704	Dept. of Electrical Engineering
Hillsboro, OR 97124	Yorktown Heights	200 South 33rd Street
USA	NY 10598	Philadelphia, PA 19104
téléphone : +1 503-264-9077	téléphone : +1 914-784-7536	téléphone : +1 215 898-9351
mél : raj.yavatkar@intel.com	mél : dimitris@watson.ibm.com	mél : guerin@ee.upenn.edu

11. Déclaration complète de droits de reproduction

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