Groupe de travail Réseau
Request for Comments : 5553
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

A. Farrel, éd., Old Dog Consulting
R. Bradford, Cisco Systems, Inc.
JP. Vasseur, Cisco Systems, Inc.
mai 2009

Extensions au protocole de réservation de ressource (RSVP) pour la prise en charge de clé de chemin

Résumé
Les chemins de commutation d'étiquette (LSP, *Label Switched Path*) pris par l'ingénierie du trafic (TE, *Traffic Engineering*) de commutation d'étiquettes multi-protocoles (MPLS, *Multiprotocol Label Switching*) et MPLS généralisé (GMPLS, *Generalized MPLS*) peuvent être calculés par des éléments de calcul de chemin (PCE, *Path Computation Element*). Lorsque le LSP TE traverse plusieurs domaines, comme des systèmes autonomes (AS, *Autonomous System*) le chemin peut être calculé par plusieurs PCE qui coopèrent, chacun étant responsable du calcul d'un segment du chemin.

Pour préserver la confidentialité de la topologie au sein de chaque AS, les PCE prennent en charge un mécanisme pour cacher le contenu d'un segment d'un chemin (comme le segment de chemin qui traverse un AS) appelé le segment confidentiel de chemin (CPS, *Confidential Path Segment*) en codant le contenu comme un sous objet Clé de chemin (PKS, *Path Key Subobject*) et en incorporant ce sous objet dans le résultat de son calcul de chemin.

Le présent document décrit comment porter les sous objets Clé de chemin dans les objets Chemin explicite (ERO, *Explicit Route Object*) et les objets Chemin enregistré (RRO, *Record Route Object*) dans le protocole de réservation de ressource (RSVP, *Resource Reservation Protocol*) de façon à faciliter la confidentialité dans la signalisation des LSP TE inter-domaines.

Table des matières

1. Introduction....2
1.1 Conventions utilisées dans ce document....2
1.2 Scénario d'utilisation....2
2. Terminologie....3
3. Sous objet Clé de chemin RSVP-TE....3
3.1 Règles de traitement de l'objet Chemin explicite....4
3.2 Rapport de segments de clé de chemin dans les objets Record Route....5
4. Considérations sur la sécurité....5

5. Considérations de gestion....6
5.1 Contrôle de fonction par configuration et politique....6
6. Considérations relatives à l'IANA....7
6.1 Sous objets de l'objet Explicit Route....7
6.2 Sous objets de l'objet Record Route....7
6.3 Codes et valeurs d'erreur....8
7. Références....8
7.1 Références normatives....8
7.2 Références pour information....8
Adresse des auteurs....8

1. Introduction

Les chemins de commutation d'étiquette (LSP) pris par l'ingénierie du trafic (TE) de commutation d'étiquettes multi-protocoles (MPLS) et MPLS généralisé (GMPLS) sont signalés en utilisant les extensions TE au protocole de réservation de ressources (RSVP-TE) [RFC3209], [RFC3473]. Les chemins suivis par les LSP TE MPLS et GMPLS peuvent être calculés par les éléments de calcul de chemin (PCE) [RFC4655].

Lorsque le LSP TE traverse plusieurs domaines [RFC4726], comme des systèmes autonomes (AS) le chemin peut être calculé par plusieurs PCE qui coopèrent, chacun étant responsable du calcul d'un segment du chemin. Pour préserver la confidentialité de la topologie avec chaque AS, le protocole de communication de PCE (PCEP, *PCE Communications Protocol*) [RFC5440] prend en charge un mécanisme pour cacher le contenu d'un segment d'un chemin, appelé le segment confidentiel de chemin (CPS, *Confidential Path Segment*) en codant le contenu comme un sous objet Clé de chemin (PKS, *Path Key Subobject*) [RFC5520].

Le présent document définit les extensions au protocole RSVP-TE nécessaires pour prendre en charge l'utilisation des sous objets Clé de chemin (PKS) dans la signalisation MPLS et GMPLS en les incluant dans les objets Chemin explicite (ERO, *Explicit Route Object*) et les objets Chemin enregistré (RRO, *Record Route Object*) afin de faciliter la confidentialité dans la signalisation des LSP TE inter-domaines.

1.1 Conventions utilisées dans ce document

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

1.2 Scénario d'utilisation

La Figure 1 montre un réseau simple constitué de deux AS. Un LSP est désiré de l'entrée de AS-1 à la sortie de AS-2. Comme décrit dans la [RFC4655], le routeur de commutation d'étiquettes (LSR, *Label Switching Router*) d'entrée agit comme client de calcul de chemin (PCC, *Path Computation Client*) et envoie une demande à son PCE (PCE-1). PCE-1 peut calculer le chemin au sein de AS-1 mais n'a pas de visibilité sur AS-2. Donc PCE-1 coopère avec PCE-2 pour compléter le calcul de chemin.

Cependant, PCE-2 ne veut pas partager les informations sur le chemin à travers AS-2 avec des nœuds extérieur à l'AS. Donc, comme décrit dans la [RFC5520], PCE-2 rapporte le segment de chemin AS-2 en utilisant un PKS plutôt que les détails explicites du chemin.

PCE-1 peut maintenant retourner le chemin à signaler au LSR d'entrée dans une réponse de calcul de chemin avec le segment AS-2 toujours caché comme PKS.

Pour établir le LSP, le LSR d'entrée signale en utilisant RSVP-TE et code le chemin rapporté par PCE-1 dans l'objet de chemin explicite (ERO). Ce processus est normal pour RSVP-TE mais exige que le PKS soit aussi inclus dans l'ERO, en utilisant les mécanismes définis dans le présent document.

Quand le message de signalisation (le message Path RSVP-TE) atteint ASBR-2 (routeur de bordure de système autonome (ASBR, *Autonomous System Border Router*)) il consulte PCE-2 pour "décoder" le PKS et retourne le segment de chemin explicite expansé à ASBR-2. (Les informations que PCE-2 utilise pour décoder le PKS sont codées au sein du PKS lui-

même.) Le PKS est remplacé dans l'ERO par les informations expansées sur le chemin.

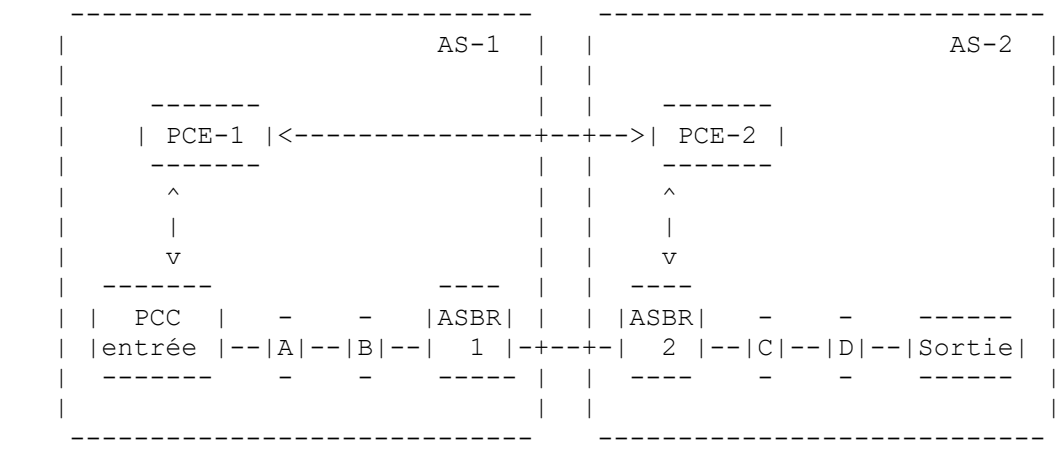

Figure 1 : Réseau simple pour monstrer l'usage du PKS

Noter que PCE-2 peut dans certains cas être co-localisé avec ASBR-2.

2. Terminologie

CPS *(Confidential Path Segment)* : segment de chemin confidentiel. Segment d'un chemin qui contient des nœuds et liaisons dont la politique de l'AS exige qu'ils ne soient pas divulgués en dehors de l'AS.

PCE *(Path Computation Element)* : élément de calcul de chemin. Entité (composant, application, ou nœud de réseau) qui est capable de calculer un chemin de réseau sur la base d'un graphe de réseau et d'appliquer des contraintes de calcul.

PKS *(Path Key Subobject)* : sous objet Clé de chemin. Sous objet d'un objet Chemin explicite qui code un CPS afin de préserver la confidentialité.

3. Sous objet Clé de chemin RSVP-TE

Le sous objet Clé de chemin (PKS) peut être porté dans l'objet Chemin explicite (ERO) d'un message Path RSVP-TE [RFC3209]. Le PKS est un sous objet de longueur fixe contenant une clé de chemin et un identifiant de PCE. La clé de chemin est un identifiant ou jeton utilisé pour représenter le CPS au sein du contexte du PCE identifié par l'identifiant de PCE. L'identifiant de PCE identifie le PCE qui peut décoder la clé de chemin en utilisant une adresse accessible IPv4 ou IPv6 du PCE. Dans la plupart des cas, le PCE décodeur est aussi le PCE qui a calculé la clé de chemin et le chemin associé. À cause des variantes IPv4 et IPv6, deux sous objets sont définis comme suit :

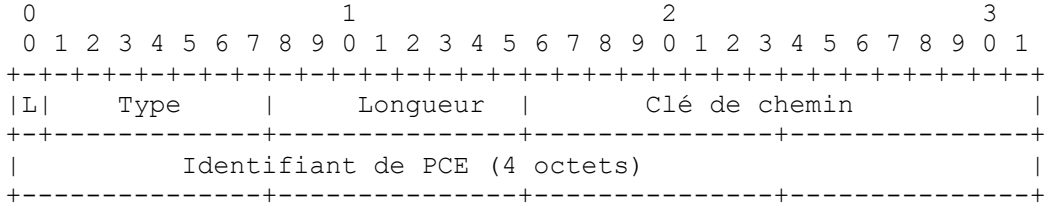

Figure 2 : Sous objet Clé de chemin RSVP-TE utilisant une adresse IPv4 pour l'identifiant de PCE

L : le bit L NE DEVRAIT PAS être établi, afin que le sous objet représente un bond strict dans le chemin explicite.

Type : type de sous objet pour une clé de chemin avec un identifiant de PCE de 32 bits comme alloué par l'IANA.

Longueur : contient la longueur totale du sous objet en octets, incluant les champs Type et Longueur. La longueur est

toujours 8.

Identifiant de PCE : identifiant de 32 bits du PCE qui peut décoder cette clé. L'identifiant DOIT être unique au sein de la portée du domaine que traverse le CPS et DOIT être compris par le LSR qui va agir comme PCC pour l'expansion du PKS. L'interprétation de l'identifiant de PCE est soumise à la politique du domaine local. Ce PEUT être une adresse IPv4 du PCE qui est toujours accessible et PEUT être une adresse qui est restreinte au domaine dans lequel se tient le LSR qui est invoqué pour étendre le CPS. D'autres valeurs qui n'ont pas de signification en dehors du domaine (par exemple, l'identifiant de routeur du PCE) PEUVENT être utilisées pour accroître la sécurité ou la confidentialité.

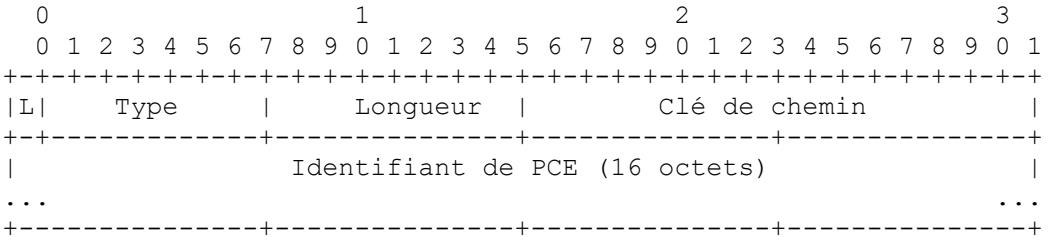

Figure 3 : Sous objet Clé de chemin RSVP-TE utilisant une adresse IPv6 pour l'identifiant de PCE

L : comme ci-dessus.

Type : type de sous objet pour une clé de chemin avec un identifiant de PCE de 128 bits comme alloué par l'IANA.

Longueur : contient la longueur totale du sous objet en octets, incluant les champs Type et Longueur. La longueur est toujours 20.

Identifiant de PCE : identifiant de 128 bits du PCE qui peut décoder cette clé. L'identifiant DOIT être unique au sein de la portée du domaine que traverse le CPS et DOIT être compris par le LSR qui va agir comme PCC pour l'expansion du PKS. L'interprétation de l'identifiant de PCE est soumise à la politique du domaine local. Ce PEUT être une adresse IPv6 du PCE qui est toujours accessible, et PEUT être une adresse restreinte au domaine dans lequel se tient le LSR invoqué pour expanser le CPS. D'autres valeurs qui n'ont pas de signification en dehors du domaine (par exemple, l'identifiant de routeur TE IPv6) PEUVENT être utilisées pour augmenter la sécurité (voir la Section 4).

Note : ces deux sous objets sont portés dans les messages PCEP comme défini dans la [RFC5520].

3.1 Règles de traitement de l'objet Chemin explicite

Les règles de traitement de base d'un ERO ne sont pas modifiées. Voir les détails dans la [RFC3209]. En particulier, un LSR n'est pas obligé de "regarder" dans l'ERO au delà du premier sous objet qui n'est pas local.

La [RFC5520] exige que tout fragment de chemin généré par un PCE qui contient un PKS soit tel que le PKS soit immédiatement précédé par un sous objet qui identifie l'extrémité de tête du PKS (par exemple, une interface entrante ou un identifiant de nœud). Cette règle est étendue au PKS dans l'ERO de sorte que les règles suivantes sont définies :

- Si un LSR reçoit un message Path où le premier sous objet de l'ERO est un PKS, il DOIT répondre avec un message PathErr portant la combinaison de code/valeur d'erreur "Problème d'acheminement" / "Mauvais sous objet initial".

- Si un LSR supprime tous les sous objets locaux d'un ERO portés dans un message Path (conformément aux procédures de la [RFC3209]) et trouve que le sous objet suivant est un PKS, il DOIT tenter de résoudre le PKS en un CPS.

La résolution du PKS PEUT prendre une des formes suivantes ou utiliser une autre technique sous réserve de la politique locale et de la mise en œuvre de réseau.

o Le LSR peut utiliser l'identifiant de PCE contenu dans le PKS pour contacter le PCE identifié en utilisant PCEP [RFC5440] et demander que le PKS soit expansé.

o Le LSR peut contacter tout PCE en utilisant PCEP [RFC5440] pour demander que le PKS soit expansé, en s'appuyant sur la coopération entre les PCE.

o Le LSR peut utiliser les informations dans le PKS pour indexer un CPS qui lui a été fourni précédemment par le PCE qui a généré le PKS.

Si un CPS est déduit, le fragment de chemin DEVRAIT être inséré dans l'ERO du message Path comme remplacement direct du PKS. D'autres traitements du CPS et de l'ERO sont permis comme décrit dans la [RFC3209].

Ce traitement peut donner lieu aux cas d'erreur suivants :

o L'identifiant de PCE ne peut pas être confronté à un PCE pour décoder le PKS. Le LSR envoie un message PathErr avec le code d'erreur "Problème d'acheminement" et la nouvelle valeur d'erreur "PCE-ID inconnu pour l'expansion de PKS" (voir le paragraphe 6.3).

o Le PCE identifié par le PCE-ID ne peut pas être joint. Le LSR envoie un message PathErr avec le code d'erreur "Problème d'acheminement" et la nouvelle valeur d'erreur "PCE injoignable pour l'expansion de PKS" (voir le paragraphe 6.3).

o Le PCE est incapable de décoder le PKS, peut-être parce que la clé de chemin a expiré. Le LSR envoie un message PathErr avec le code d'erreur "Problème d'acheminement" et la nouvelle valeur d'erreur "Clé de chemin inconnue pour l'expansion de PKS" (voir le paragraphe 6.3).

o Le PKS ne peut pas être décodé pour des raisons de politique. Le LSR envoie un message PathErr avec le code d'erreur "Échec de contrôle de politique" et la valeur d'erreur "Échec de politique inter-domaines".

o L'ajout de CPS à l'ERO cause un message Path devenu trop grand. Le LSR PEUT remplacer une partie de l'ERO par des bonds lâches [RFC3209] ou par un autre PKS, conformément à la politique locale, si la perte de spécificités au sein du chemin explicite est acceptable. Si le LSR est incapable de prendre des mesures pour réduire la taille de l'ERO, il DOIT envoyer un message PathErr avec le code d'erreur "Problème d'acheminement" et la nouvelle valeur d'erreur "ERO trop grand pour la MTU" (voir le paragraphe 6.3).

- Un LSR qui est invoqué pour traiter un PKS au sein d'un ERO mais qui ne reconnaît pas le sous objet, va réagir conformément à la [RFC3209] et envoyer un message PathErr avec la combinaison de valeur/code d'erreur "Problème d'acheminement" / "Mauvais objet Chemin explicite".

3.2 Rapport de segments de clé de chemin dans les objets Record Route

L'objet Record Route (RRO) est utilisé dans RSVP-TE pour enregistrer le chemin traversé par un LSP. Le RRO peut être présent sur un message Path et sur un message Resv. L'intention de la [RFC3209] est qu'un RRO sur un message Resv qui est reçu par un LSR d'entrée est convenable pour être utilisé comme ERO sur un message Path envoyé à ce LSR pour réaliser un LSP identique.

Le PKS offre une solution de remplacement qui peut être plus utile pour les diagnostics. Quand le message de signalisation traverse une limite de domaine, le segment de chemin qui doit être caché (c'est-à-dire, un CPS) PEUT être remplacé dans le RRO par un PKS. Dans le cas d'un RRO sur un message Resv, le PKS utilisé DEVRAIT être celui originellement signalé dans l'ERO du message Path. Sur un message Path, le PKS DEVRAIT identifier le LSR remplaçant le CPS et fournir une clé de chemin qui puisse être utilisée pour expanser le segment de chemin. Dans le premier cas, la clé de chemin et son expansion DEVRAIENT être conservées par le LSR qui effectue la substitution pendant au moins la durée de vie du LSP. Dans les deux cas, l'expansion du PKS DEVRAIT être rendue disponible aux outils de diagnostic sous le contrôle de la politique locale.

4. Considérations sur la sécurité

Les interactions de protocole requises par les mécanismes décrits dans le présent document sont en point à point et peuvent être authentifiées et rendues sûres comme décrit dans les [RFC5440] et [RFC3209]. Les interactions de protocole pour PCEP sont énumérées dans la [RFC5520], tandis que les considérations générales pour sécuriser RSVP-TE dans les réseaux MPLS-TE et GMPLS peuvent être trouvées dans la [RFC5920].

Donc, les questions de sécurité peuvent être traitées en utilisant les techniques standard pour sécuriser et authentifier les communications en point à point. De plus, il est RECOMMANDÉ que le PCE qui fournit une expansion de PKS vérifie que le LSR qui a produit la demande d'expansion du PKS est l'extrémité de tête du CPS résultant.

Plus de protection peut être fournie en utilisant pour identifier le PCE décodeur un identifiant de PCE qui n'a de signification qu'au sein du domaine qui contient le LSR à la tête du CPS. Ce peut être une adresse IP qui est seulement accessible de l'intérieur du domaine ou une valeur non d'adresse. La première exige la configuration de la politique sur les PCE ; la seconde exige une politique à l'échelle du domaine.

Les questions de sécurité spécifiques suivantes doivent être considérées.

- Confidentialité du CPS. La question est de savoir si d'autres éléments de réseau peuvent sonder un PCE sur l'expansion des PKS, générant éventuellement des clés de chemin au hasard. On peut se protéger contre cela en permettant seulement que l'expansion de PKS réussisse si elle est demandée par le LSR qui est à l'extrémité de tête du CPS résultant. Dans des circonstances spécifiques, l'expansion de PKS pourrait aussi être permise par des stations de gestion configurées.
  Le CPS lui-même peut rester confidentiel car il est échangé dans les protocoles PCEP et RSVP-TE en utilisant les mécanismes de sécurité standard définis pour ces protocoles.

- Détermination des informations par sondage. En plus du sondage décrit ci-dessus, un nœud pourrait déduire les informations des réponses d'erreur qui sont générées quand l'expansion de PKS échoue comme décrit au paragraphe 3.1. Tout LSR qui détermine que la fourniture d'un des codes d'erreur détaillés décrits au paragraphe 3.1 pourrait fournir trop d'informations qui pourraient être utilisées au titre d'une attaque systématique PEUT simplement utiliser le code/valeur d'erreur "Échec de contrôle de politique" / "Échec de politique inter-domaines" dans tous les cas.

- Authenticité de la clé de chemin. Un souci est que la clé de chemin dans le PKS soit altérée ou falsifiée, conduisant à une expansion erronée de la clé de chemin et à l'utilisation de mauvais CPS. La conséquence serait un mauvais ERO dans un message Path, causant l'établissement incorrect du LSP et résultant en un usage incorrect de ressource de réseau, le déroutement du trafic sur un site où il peut être intercepté, ou l'échec de l'établissement du LSP. Ces problèmes peuvent être prévenus en protégeant les échanges de protocole dans PCEP et RSVP-TE en utilisant les techniques de sécurité décrites dans les [RFC5440], [RFC3209], et [RFC5920].

- Résilience aux attaques de déni de service (DoS). Un PCE peut être attaqué par une inondation de demandes d'expansion de clé de chemin -- ce problème est traité dans la [RFC5520] et sort du domaine d'application du présent document. Une autre attaque pourrait consister en l'envoi d'une inondation de messages Path RSVP-TE avec des PKS délibérément parasites. Cette attaque est prévenue en s'assurant de l'intégrité des messages Path en utilisant les mécanismes standard de sécurité de RSVP-TE et en appliquant le modèle de sécurité de la chaîne de confiance de RSVP-TE.

5. Considérations de gestion

5.1 Contrôle de fonction par configuration et politique

La politique forme une partie importante de l'utilisation des PKS dans les ERO et les RRO. Des politiques locales et au niveau du domaine DEVRAIENT être disponibles pour la configuration dans une mise en œuvre.

- Traitement d'un ERO contenant un PKS. Comme décrit au paragraphe 3.1, un LSR qui reçoit un message Path contenant un PKS peut être configuré à rejeter le message Path selon la politique.

- Traitement d'une demande de PKS à un PCE. Comme décrit au paragraphe 3.1, dans la [RFC5520], et dans la [RFC5394], un PCE peut être configuré avec une politique concernant comment il devrait traiter les demandes d'expansion de PKS.

- Expansion de PKS. Le paragraphe 3.1 explique que le PKS peut être expansé par le LSR local, le PCE spécifique identifié dans le PKS, tout PCE agissant comme mandataire, ou par une autre méthode. Le comportement du LSR doit être configurable en local mais est soumis à la politique au niveau du domaine.

- Interprétation de l'identifiant de PCE. L'interprétation du composant PCE-ID des PKS est sujette à la politique du domaine local et doit être configurable comme telle. Voir les Sections 3 et 4 pour les options.

- ERO trop grand. Le comportement d'un LSR quand il trouve que l'ajout d'un CPS à l'ERO est cause que le message Path est trop gros est un choix de mise en œuvre. Cependant, les mises en œuvre peuvent choisir de fournir une configuration de comportement comme décrit au paragraphe 3.1.

- Masquer le RRO. Comme décrit au paragraphe 3.2, un routeur de bordure peut choisir de masquer des segments du chemin en les remplaçant par des PKS. Ce comportement doit être configurable, avec par défaut de ne pas cacher de partie du RRO.

- Inspection/décodage de PKS par des outils de diagnostic. Un PCE peut permettre l'accès à partir d'outils de gestion ou de diagnostic pour demander l'expansion d'un PKS. Noter que ceci doit être régulé avec le comportement de sécurité et de confidentialité décrit à la Section 4.

- Cacher les codes de cause. Un LSR peut prendre en charge la configuration de politique locale pour cacher les codes de cause associé à l'échec d'expansion d'un PKS et, comme décrit dans la Section 4, rapporter toutes les erreurs comme des échecs de politique.

Le traitement d'un segment de chemin comme CPS, et sa substitution dans un ERO PCRep par un PKS, est une fonction de PCE et est décrite dans la [RFC5520].

6. Considérations relatives à l'IANA

6.1 Sous objets de l'objet Explicit Route

L'IANA tient un registre appelé "Paramètres du protocole de réservation de ressources (RSVP)" avec un sous registre appelé "Noms, numéros, et types de classes".

Dans ce sous registre, il y a une définition de l'objet EXPLICIT_ROUTE avec le numéro de classe de 20. La définition de l'objet énumère un certain nombre de sous objets acceptables pour le type de classe 1.

L'IANA a alloué deux autres sous objets comme décrit dans la Section 3. L'entrée résultante dans le registre est comme suit :

20 EXPLICIT_ROUTE [RFC3209]
Types de classe ou C-Types :
1 Type 1 Explicit Route [RFC3209]
Type de sous objet :
64 Clé de chemin avec identifiant de PCE de 32 bits [RFC5553]
65 Clé de chemin avec identifiant de PCE de 128 bits [RFC5553]

Note : la [RFC5520] définit le PKS à utiliser dans PCEP. L'IANA a alloué les mêmes numéros de sous objet à utiliser dans RSVP-TE que ceux alloués pour le PKS dans PCEP. Les numéros ci-dessus sont les mêmes que dans la [RFC5520].

6.2 Sous objets de l'objet Record Route

L'IANA tient un registre appelé "Paramètres du protocole de réservation de ressources (RSVP)" avec un sous registre appelé "Noms, numéros, et types de classes".

Dans ce sous registre, il y a une définition de l'objet ROUTE_RECORD (aussi appelé objet RECORD_ROUTE) avec le numéro de classe de 21. La définition de l'objet énumère un certain nombre de sous objets acceptables pour le type de classe 1.

L'IANA a alloué deux autres sous objets comme décrit dans la Section 3. L'entrée résultante dans le registre est comme suit :

21 ROUTE_RECORD [RFC3209]
(aussi appelé RECORD_ROUTE)
Types de classe ou C-Types :
1 Type 1 Route Record [RFC3209]
Type de sous objet :
64 Clé de chemin avec identifiant de PCE de 32 bits [RFC5553]
65 Clé de chemin avec identifiant de PCE de 128 bits [RFC5553]

Note : il est demandé à l'IANA d'utiliser les mêmes numéros de sous objet que ceux définis pour l'objet EXPLICIT_ROUTE au paragraphe 6.1.

6.3 Codes et valeurs d'erreur

L'IANA tient un registre appelé "Paramètres du protocole de réservation de ressources (RSVP)" avec un sous registre appelé "Codes d'erreur et sous codes de valeur d'erreur définis mondialement".

Dans ce sous registre, il y a une définition du code d'erreur "Problème d'acheminement" avec la valeur de code d'erreur de 24. La définition énumère un certain nombre de valeurs d'erreur qui peuvent être utilisées avec ce code d'erreur.

L'IANA a alloué d'autres valeurs d'erreur à utiliser avec ce code d'erreur comme décrit au paragraphe 3.1. L'entrée résultante dans le registre est comme suit :
24 Problème d'acheminement [RFC3209]

Ce code d'erreur a les sous codes de valeur d'erreur définie mondialement de :
31 = Identifiant de PCE inconnu pour l'expansion de PKS [RFC5553]
32 = PCE injoignable pour l'expansion de PKS [RFC5553]
33 = Clé de chemin inconnue pour l'expansion de PKS [RFC5553]
34 = ERO trop grand pour la MTU [RFC5553]

7. Références

7.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

[RFC3209] D. Awduche, et autres, "RSVP-TE : Extensions à RSVP pour les tunnels LSP", décembre 2001. (*Mise à jour par* RFC3936, RFC4420, RFC4874, RFC5151, RFC5420, RFC6790)

[RFC3473] L. Berger, "Extensions d'ingénierie de protocole - trafic de signalisation de réservation de ressource (RSVP-TE) de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", janvier 2003. *(P.S., MàJ par 4003, 4201, 4420, 4783, 4784, 4873, 4974, 5063, 5151,* 8359)

7.2 Références pour information

[RFC4655] A. Farrel, J.-P. Vasseur et J. Ash, "Architecture fondée sur l'élément de calcul de chemin (PCE)", août 2006.

[RFC4726] A. Farrel et autres, "Cadre pour l'ingénierie de trafic inter domaine de commutation d'étiquettes multi protocoles", novembre 2006. *(Information)*

[RFC5394] I. Bryskin et autres, "Cadre du calcul de chemin avec capacité de politique", décembre 2008. *(Information)*

[RFC5440] JP. Vasseur et autres, "Protocole de communication d'élément de calcul de chemin (PCEP)", mars 2009. *(P. S. ; MàJ par* RFC7896, RFC8253, RFC8356, RFC9488)

[RFC5520] R. Bradford, éd., JP. Vasseur, A. Farrel, "Préservation de la confidentialité topologique dans le calcul de chemin inter-domaine en utilisant le mécanisme du chemin à clé", avril 2009. *(P. S.)*

[RFC5920] L. Fang, "Cadre de sécurité pour réseaux MPLS et GMPLS", juillet 2010. *(Information)*

Adresse des auteurs

Adrian Farrel
Old Dog Consulting
mél : adrian@olddog.co.uk

Rich Bradford
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA - 01719
USA
mél : rbradfor@cisco.com

Jean-Philippe Vasseur
Cisco Systems, Inc
11, Rue Camille Desmoulins
L'Atlantis
92782 Issy Les Moulineaux
France
mél : jpv@cisco.com