Groupe de travail Réseau
Request for Comments : 5440
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

JP. Vasseur, éditeur, Cisco Systems
JL. Le Roux, éditeur, France Telecom
janvier 2009

Protocole de communication d'élément de calcul de chemin (PCEP)

Résumé
Le présent document spécifie le protocole de communication d'élément de calcul de chemin (PCEP, *Path Computation Element Communication Protocol*) pour les communications entre un client de calcul de chemin (PCC, *Path Computation Client*) et un élément de calcul de chemin (PCE, *Path Computation Element)* ou entre deux PCE. De telles interactions incluent des demandes de calcul de chemin et des réponses de calcul de chemin ainsi que des notifications d'états spécifiques relatifs à l'utilisation d'un PCE dans le contexte de l'ingénierie de trafic de commutation d'étiquettes multi protocoles (MPLS, *Multiprotocol Label Switching*) et de MPLS généralisé (GMPLS, *Generalized MPLS*). PCEP est conçu pour être souple et extensible afin de permettre l'ajout facile d'autres messages et objets, si d'autres exigences étaient exprimées à l'avenir.

Table des matières

1. Introduction

La [RFC4655] décrit les motivations et l'architecture pour un modèle fondé sur lélément de calcul de chemin (PCE, *Path Computation Element*) pour le calcul de chemins de commutation d'étiquettes d'ingénierie de trafic (LSP TE, *Traffic Engineering Label Switched Path*) de commutation d'étiquettes multiprotocoles (MPLS, *Multiprotocol Label Switching*) et de MPLS généralisé (GMPLS, *Generalized MPLS*). Le modèle permet la séparation du PCE d'avec le client de calcul de chemin (PCC, *Path Computation Client*) et permet la coopération entre les PCE. Cela exige un protocole de communication entre PCC et PCE, et entre les PCE. La [RFC4657] déclare les exigences génériques pour un tel protocole, incluant que le même protocole soit utilisé entre PCC et PCE, et entre les PCE. Des exigences supplémentaires spécifiques de l'application (pour des scénarios comme inter-zones, inter-AS, etc.) ne sont pas incluses dans la [RFC4657], mais il y a l'exigence que toute solution de protocole doit être facilement extensible pour traiter d'autres exigences lorsque elles sont introduites dans des documents d'exigences spécifiques d'application. Des exemples de telles exigences spécifiques d'application sont les [RFC4927], [RFC5376], et [RFC5623].

Le présent document spécifie le protocole d'élément de calcul de chemin (PCEP, *Path Computation Element Protocol*) pour les communications entre un PCC et un PCE, ou entre deux PCE, en conformité avec la [RFC4657]. De telles interactions incluent des demandes de calcul de chemin et des réponses de calcul de chemin ainsi que les notifications des états spécifiques relatifs à l'utilisation d'un PCE dans le contexte de l'ingénierie de trafic MPLS et GMPLS.

PCEP est conçu pour être souple et extensible afin de permettre facilement l'ajout d'autres messages et objets, si des exigences nouvelles devaient être exprimées à l'avenir.

1.1 Langage des exigences

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].

2. Terminologie

La terminologie suivante est utilisé dans ce document.

AS *(Autonomous System)* : système autonome

Chemin explicite : chemin explicite complet du début à la destination ; constitué d'une liste de bonds stricts où un bond peut être un nœud abstrait comme un AS.

Chemin strict/lâche : mélange de bonds stricts et lâches comprenant au moins un nœud lâche représentant la destination, où un bond peut être un nœud abstrait comme un AS.

Homologue PCEP : élément impliqué dans une session PCEP (c'est-à-dire, un PCC ou un PCE).

LSP TE *(Traffic Engineering Label Switched Path)* chemin de commutation d'étiquettes d'ingénierie du trafic

LSP TE inter domaines : LSP TE dont le chemin transite au moins par deux domaines différents où un domaine peut être une zone IGP, un système autonome, ou un sous AS (confédération BGP).

PCC *(Path Computation Client)* client de calcul de chemin : toute application cliente qui demande qu'un calcul de chemin soit effectué par un élément de calcul de chemin.

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

TED *(Traffic Engineering Database)* base de données d'ingénierie du trafic qui contient la topologie et les informations de ressources du domaine. La TED peut être nourrie des extensions IGP ou éventuellement par d'autres moyens.

Zone IGP : zone OSPF ou niveau IS-IS.

Dans ce document, quand on décrit des communications de PCE à PCE, le PCE demandeur joue le rôle de PCC. Cela fait une économie de documentation sans perte de fonction.

Les formats de message dans ce document sont spécifiés en utilisant la notation de format Backus-Naur (BNF) spécifiée dans la [RFC5511].

3. Hypothèses

La [RFC4655] décrit divers types de PCE. PCEP ne fait aucune hypothèse sur la nature du PCE, et donc ne lui impose aucune contrainte.

De plus, on suppose que le PCE a les informations requises (incluant généralement la topologie du réseau et les informations de ressources) afin d'effectuer le calcul d'un chemin pour un LSP TE. De telles informations peuvent être rassemblées par les protocoles d'acheminement ou par d'autres moyens. La façon dont des informations sont rassemblées sort du domaine d'application de ce document.

De même, aucune hypothèse n'est faite sur la méthode de découverte utilisée par un PCC pour découvrir un ensemble de PCE (par exemple, via configuration statique ou découverte dynamique) et sur l'algorithme utilisé pour choisir le PCE. Pour référence, la [RFC4674] définit une liste d'exigences pour la découverte dynamique de PCE et des solutions fondées sur IGP pour une telle découverte de PCE sont spécifiées dans les [RFC5088] et [RFC5089].

4. Vue d'ensemble de l'architecture du protocole (modèle)

Le but de cette section est de décrire le modèle PCEP dans l'esprit de la [RFC4101]. Une vue d'ensemble de l'architecture du protocole (le tableau d'ensemble du protocole) est fournie dans cette section. Les détails du protocole se trouvent dans les sections suivantes.

4.1 Problème

L'architecture fondée sur le PCE utilisée pour le calcul de chemins pour les LSP TE MPLS et GMPLS est décrite dans la [RFC4655]. Quand le PCC et le PCE ne sont pas co-localisés, un protocole de communication entre le PCC et le PCE est nécessaire. PCEP est un tel protocole conçu spécifiquement pour les communications entre un PCC et un PCE ou entre deux PCE en conformité avec la [RFC4657] : un PCC peut utiliser PCEP pour envoyer une demande de calcul de chemin pour un ou plusieurs LSP TE à un PCE, et le PCE peut répondre avec un ensemble de chemins calculés si un ou plusieurs chemins peuvent être trouvés qui satisfont l'ensemble de contraintes.

4.2 Vue d'ensemble de l'architecture du protocole

PCEP opère sur TCP, qui satisfait les exigences pour une messagerie fiable et un contrôle de flux dans autre travail du protocole.

Plusieurs messages PCEP sont définis :

- les messages Open et Keepalive sont utilisés pour respectivement initier et maintenir une session PCEP.
- PCReq : message PCEP envoyé par un PCC à un PCE pour demander un calcul de chemin.
- PCRep : message PCEP envoyé par un PCE à un PCC en réponse à une demande de calcul de chemin. Un message PCRep peut contenir un ensemble de chemins calculés si la demande peut être satisfaite, ou une réponse négative sinon. La réponse négative peut indiquer la raison pour laquelle aucun chemin n'a pu être trouvé.
- PCNtf : message de notification PCEP envoyé par un PCC à un PCE ou envoyé par un PCE à un PCC pour notifier un événement spécifique.
- PCErr : message PCEP envoyé en cas d'occurrence d'une condition d'erreur de protocole.

o message Close : message utilisé pour clore une session PCEP.

L'ensemble de PCE disponibles peut être configuré statiquement sur un PCC ou découvert de façon dynamique. Les mécanismes utilisés pour découvrir un ou plusieurs PCE et pour choisir un PCE sortent du domaine d'application de ce document.

Un PCC peut avoir des sessions PCEP avec plus d'un PCE, et de même un PCE peut avoir des sessions PCEP avec plusieurs PCC.

Chaque message PCEP est vu comme une seule unité de transmission et des parties de messages NE DOIVENT PAS être entrelacées. Donc, par exemple, un PCC qui envoie une PCReq et qui souhaite clore la session, doit achever l'envoi du message de demande avant de commencer d'envoyer un message Close.

4.2.1 Phase d'initialisation

La phase d'initialisation consiste en deux étapes successives (décrites sous forme schématique à la Figure 1):
1) Établissement d'une connexion TCP (prise de contact en 3 phases) entre le PCC et le PCE.
2) Établissement d'une session PCEP sur la connexion TCP.

Une fois la connexion TCP établie, le PCC et le PCE (aussi appelés les "homologues PCEP") initient l'établissement de la session PCEP durant laquelle divers paramètres de session sont négociés. Ces paramètres sont portés dans les messages Open et incluent le temporisateur Keepalive, le DeadTimer, et potentiellement d'autres capacités détaillées et règles de politique qui spécifient les conditions dans lesquelles les demandes de calcul de chemin peuvent être envoyées au PCE. Si la phase d'établissement de session PCEP échoue parce que les homologues PCEP sont en désaccord sur les paramètres de session ou que un des homologues PCEP n'a pas répondu après l'expiration du temporisateur d'établissement, la connexion TCP est immédiatement close. Des essais successifs sont permis mais une mise en œuvre devrait utiliser une procédure de retard exponentiel d'essais d'établissement de session.

Les messages Keepalive sont utilisés pour accuser réception des messages Open, et sont utilisés une fois que la session PCEP a réussi à être établie.

Seulement une session PCEP peut exister entre une paire d'homologues PCEP à tout moment. Une seule connexion TCP sur l'accès PCEP peut exister entre une paire d'homologues PCEP à tout moment.

Les détails sur les messages Open et Keepalive se trouvent respectivement aux paragraphes 6.2 et 6.3,

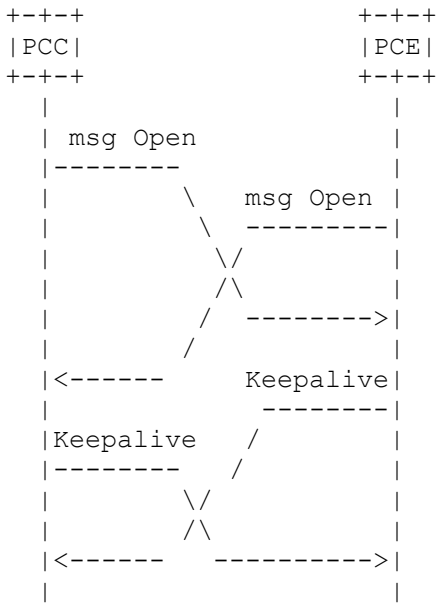


Figure 1 : Phase d'initialisation PCEP (initiée par un PCC)

(Noter qu'une fois la session PCEP établie, l'échange de messages Keepalive est facultatif.)

4.2.2 Maintien en vie de session

Une fois qu'une session a été établie, un PCE ou PCC peut vouloir savoir si son homologue PCEP est toujours disponible.

Il peut s'appuyer sur TCP pour cette information, mais il est possible que la fonction PCEP distante ait échoué sans perturber la connexion TCP. Il est aussi possible de s'appuyer sur les mécanismes incorporés dans les mises en œuvre de TCP, mais celles-ci pourraient ne pas fournir de notifications d'échec qui soient fournies en temps utile. Enfin, un PCC pourrait attendre jusqu'à ce qu'il ait une demande de calcul de chemin à envoyer et pourrait utiliser son échec de transmission ou l'absence de réception de réponse comme preuve que la session a échoué, mais cela est clairement inefficace.

Afin de traiter cette situation, PCEP inclut un mécanisme de maintien en vie fondé sur un temporisateur Keepalive, un DeadTimer, et un message Keepalive *(maintien en vie)*.

Chaque extrémité d'une session PCEP tient un temporisateur Keepalive. Elle redémarre le temporisateur chaque fois qu'elle envoie un message dans la session. Quand le temporisateur expire, elle envoie un message Keepalive. D'autre trafic peut servir de Keepalive (voir au paragraphe 6.3).

Les extrémités de la session PCEP tiennent aussi des DeadTimers *(temporisateur de mort)* et elles redémarrent les temporisateurs chaque fois qu'un message est reçu dans la session. Si une extrémité de la session ne reçoit aucun message avant l'expiration du DeadTimer, elle déclare la session morte.

Noter que cela signifie que le message Keepalive est sans réponse et ne fait pas partie d'une prise de contact de maintien en vie en deux phases comme utilisé dans certains protocoles. Noter aussi que le mécanisme est conçu pour réduire à un minimum la quantité de trafic de maintien en vie sur la session.

Le trafic de maintien en vie sur la session peut être non équilibré selon les exigences des extrémités de la session. Chaque extrémité de la session peut spécifier (par un message Open) le temporisateur Keepalive qu'elle va utiliser (c'est-à-dire, à quelle fréquence elle va transmettre un message Keepalive si il n'y a pas d'autre trafic) et un DeadTimer qu'elle recommande à son homologue d'utiliser (c'est-à-dire, combien de temps l'homologue devrait attendre avant de déclarer la session morte si il ne reçoit pas de trafic). L'extrémité de session peut utiliser des valeurs différentes de temporisateur Keepalive.

La valeur minimum du temporisateur Keepalive est 1 seconde, et elle est spécifiée en unités de 1 seconde. La valeur recommandée par défaut est 30 secondes. Le temporisateur peut être désactivé en le réglant à zéro.

La valeur recommandée par défaut pour le DeadTimer est 4 fois la valeur du temporisateur Keepalive utilisé par l'homologue distant. Cela signifie qu'il n'y a jamais de risque d'encombrer TCP avec des messages Keepalive excessifs.

4.2.3 Demande de calcul de chemin envoyée d'un PCC à un PCE

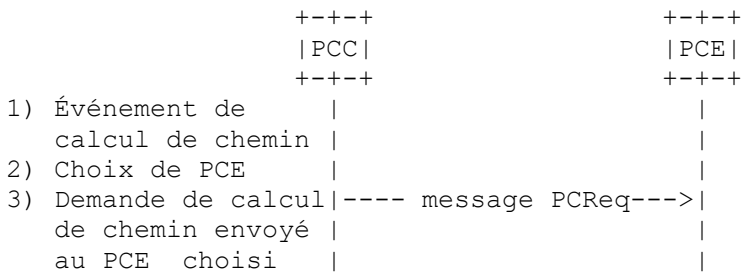


Figure 2 : Demande de calcul de chemin

Une fois qu'un PCC a réussi à établir une session PCEP avec un ou plusieurs PCE, si un événement est déclenché qui exige la calcul d'un ensemble de chemins, le PCC choisit d'abord un ou plusieurs PCE. Noter que le processus de décision de choix de PCE peut avoir eu lieu avant l'établissement de la session PCEP.

Une fois que le PCC a choisi un PCE, il envoie une demande de calcul de chemin au PCE (message PCReq) contenant

divers objets qui spécifient l'ensemble de contraintes et attributs pour le calcul du chemin. Par exemple, "Calculer un chemin de LSP TE avec l'adresse IP de source x.y.z.t, l'adresse IP de destination x'.y'.z'.t', une bande passante de B Mbit/s, une priorité d'établissement/garde P, ...". De plus, le PCC peut désirer spécifier l'urgence de telles demandes en allouant une priorité de demande. Chaque demande est identifiée de façon univoque par un numéro d'identifiant de demande et la paire d'adresses PCC-PCE. Le processus est montré en forme schématique à la Figure 2.

Noter que plusieurs demandes de calcul de chemin peuvent être en cours d'un PCC à un PCE à tout moment.

Les détails sur le message PCReq se trouvent au paragraphe 6.4.

4.2.4 Réponse de calcul de chemin envoyée du PCE à un PCC

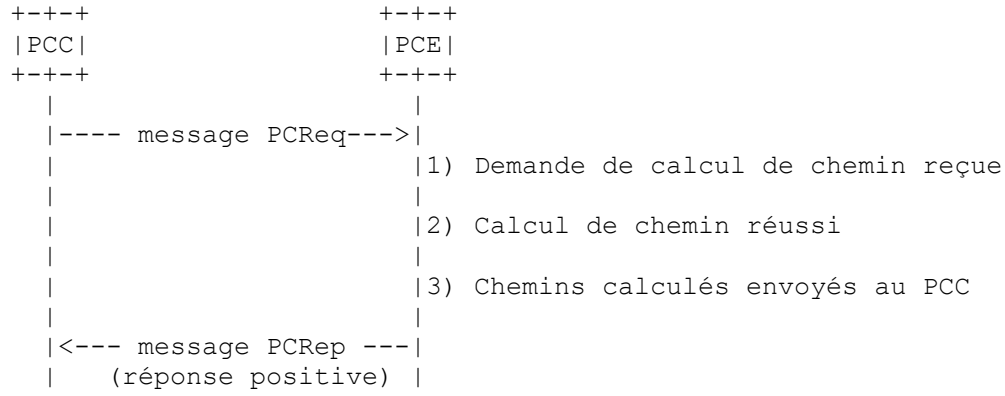


Figure 3a : Demande de calcul de chemin avec calcul de chemin réussi

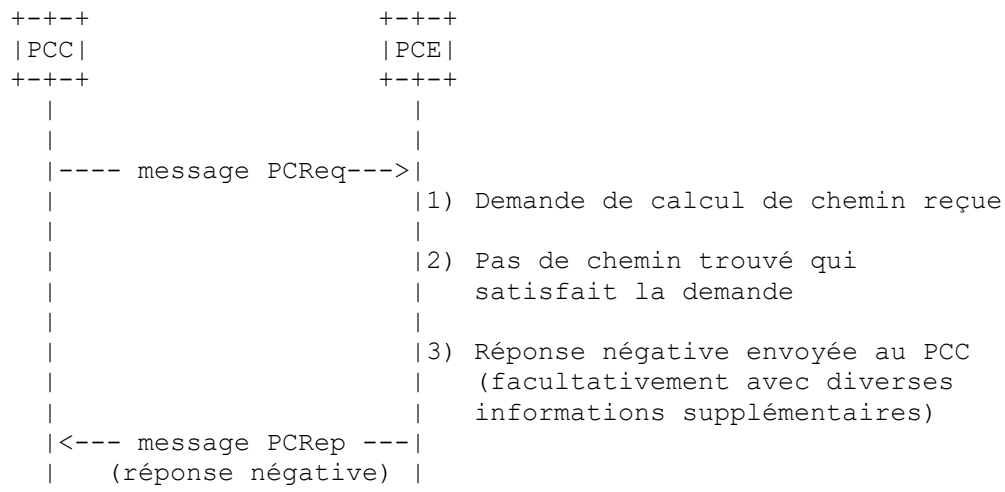


Figure 3b : Demande de calcul de chemin avec échec de calcul de chemin

À réception d'une demande de calcul de chemin du PCC, le PCE déclenche un calcul de chemin, dont le résultat peut être soit :

- Positif (Figure 3a) : le PCE s'arrange pour calculer un chemin qui satisfasse l'ensemble des contraintes exigées. Dans ce cas, le PCE retourne l'ensemble de chemins calculé au PCC demandeur. Noter que PCEP prend en charge la capacité d'envoyer une seule demande qui exige le calcul de plus d'un chemin (par exemple, la calcul d'en ensemble de chemins de diverses liaisons).

- Négatif (Figure 3b) : aucun chemin n'a pu être trouvé qui satisfasse l'ensemble de contraintes. Dans ce cas, un PCE peut fournir l'ensemble de contraintes qui ont conduit à l'échec du calcul de chemin. À réception d'une réponse négative, un PCC peut décider de renvoyer une demande modifiée ou de prendre une autre action appropriée.

Les détails sur le message PCRep se trouvent au paragraphe 6.5.

4.2.5 Notification

Il y a plusieurs circonstances dans lesquelles un PCE peut vouloir notifier à un PCC un événement spécifique. Par exemple, supposons que le PCE se trouve soudainement surchargé, conduisant potentiellement à des temps de réponse inacceptables. Le PCE peut vouloir notifier à un ou plusieurs PCC que certaines de leurs demandes (énumérées dans la notification) ne vont pas être satisfaites ou peuvent rencontrer des délais inacceptables. À réception d'une telle notification, le PCC peut décider de rediriger ses demandes de calcul de chemin sur un autre PCE si un PCE de remplacement se trouve être disponible. De même, un PCC peut désirer notifier à un PCE un événement particulier comme l'annulation de demandes en cours.

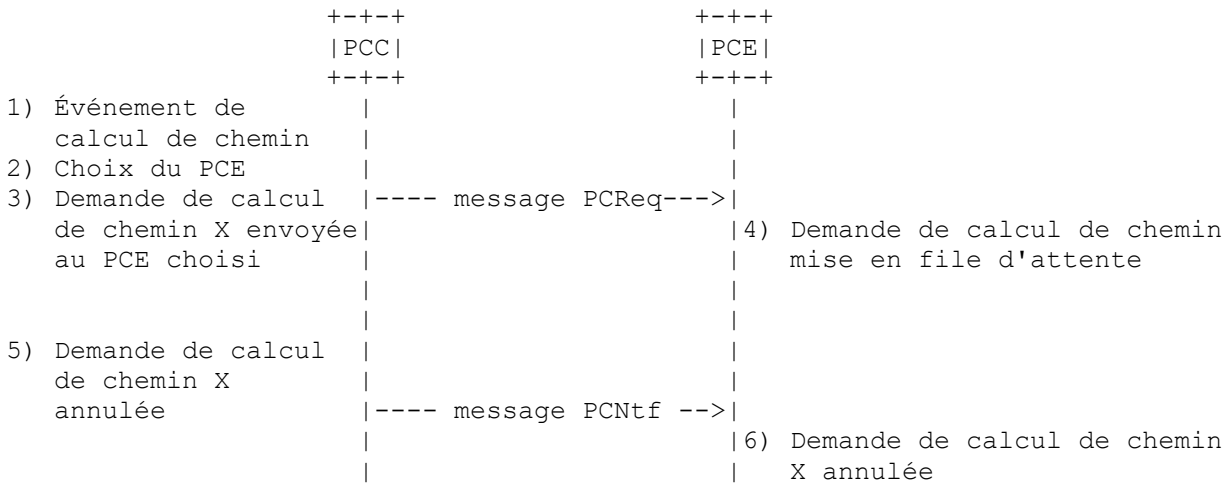


Figure 4 : Exemple de notification du PCC (notification d'annulation) envoyé à un PCE

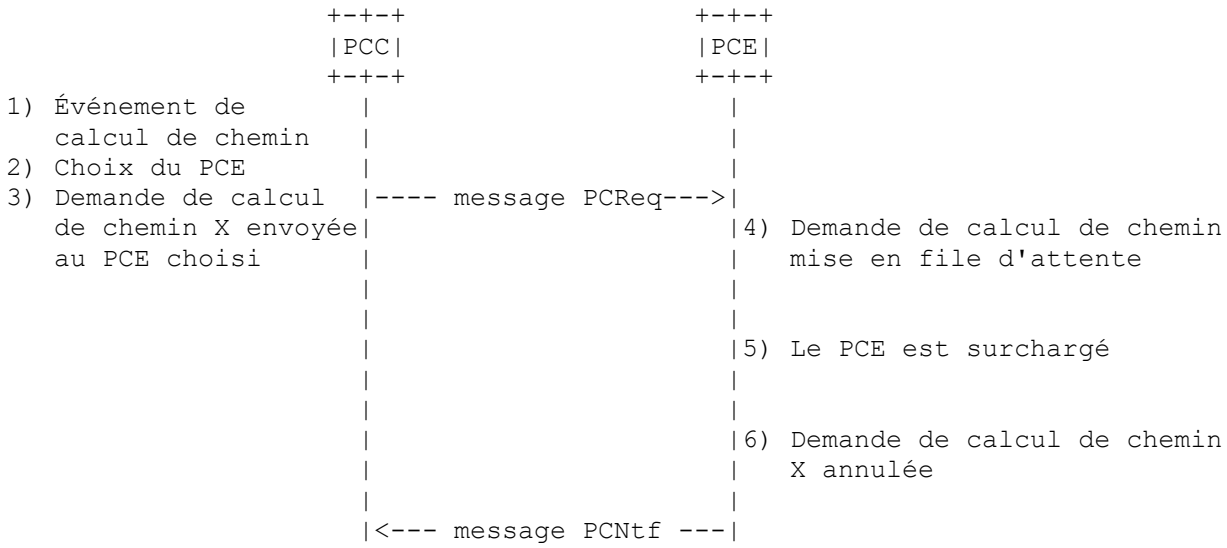


Figure 5 : Exemple de notification de PCE (notification d'annulation) envoyée à un PCC

Les détails du message PCNtf se trouvent au paragraphe 6.6.

4.2.6 Erreur

Le message PCEP Erreur (aussi appelé un message PCErr) est envoyé dans plusieurs situations : quand une condition d'erreur de protocole est rencontrée ou quand la demande n'est pas conforme à la spécification PCEP (par exemple, capacité non prise en charge, réception d'un message avec un objet obligatoire manquant, violation de politique, message inattendu, référence de demande inconnue).

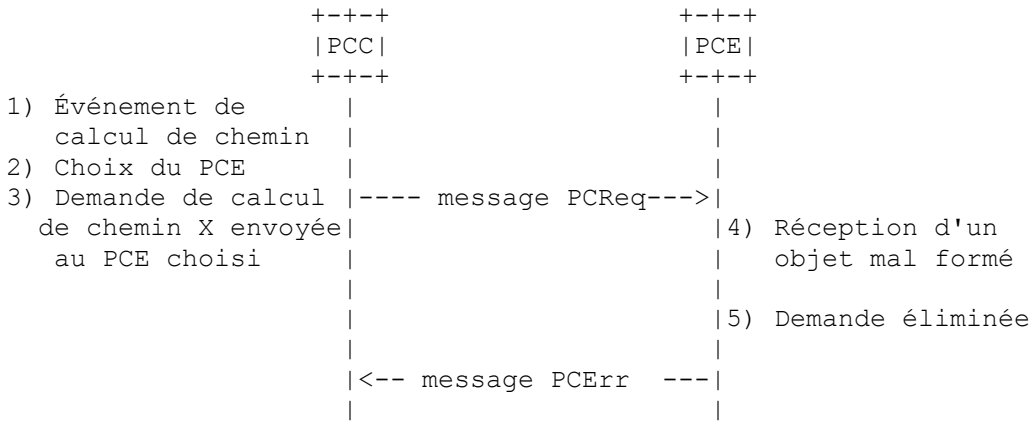


Figure 6 : Exemple de message d'erreur envoyé par un PCE à un PCC en réponse à la réception d'un objet mal formé

Les détails du message PCErr de trouvent au paragraphe 6.7.

4.2.7 Terminaison de la session PCEP

Quand un des homologues PCEP désire terminer une session PCEP, il envoie d'abord un message PCEP Close et ensuite ferme la connexion TCP. Si la session PCEP est terminée par le PCE, le PCC supprime tous les états relatifs aux demandes en cours précédemment envoyées au PCE. De même, si le PCC termine une session PCEP, le PCE supprime toutes les demandes de calcul de chemin en cours envoyées par le PCC en question ainsi que les états qui s'y rapportent. Un message Close peut seulement être envoyé pour terminer une session PCEP qui a été précédemment établie.

Dans le cas de défaillance d'une connexion TCP, la session PCEP est immédiatement terminée.

Les détails sur le message Close se trouvent au paragraphe 6.8.

4.2.8 Session PCEP intermittente ou permanente

Une mise en œuvre peut décider de garder la session PCEP en vie (et donc la connexion TCP correspondante) pendant un temps illimité. (Par exemple, cela peut être approprié quand des demandes de calcul de chemin sont envoyées de façon fréquente afin d'éviter d'ouvrir une connexion TCP chaque fois qu'une demande de calcul de chemin est nécessaire, ce qui entraînerait des délais de traitement supplémentaires.) À l'inverse, dans certaines autres circonstances, il peut être désirable d'ouvrir et fermer systématiquement une session PCEP pour chaque demande PCEP (par exemple, quand l'envoi d'une demande de calcul de chemin est un événement rare).

5. Protocole de transport

PCEP opère sur TCP en utilisant un accès TCP enregistré (4189). Cela permet de satisfaire les exigences de messagerie fiable et de contrôle de flux sans autre travail du protocole. Tous les messages PCEP DOIVENT être envoyés en utilisant l'accès TCP enregistré pour l'accès TCP de source et de destination.

6. Messages PCEP

Un message PCEP consiste en un en-tête commun suivi par un corps de longueur variable constitué d'un ensemble d'objets qui peuvent être obligatoires ou facultatifs. Dans le contexte du présent document, un objet est dit être obligatoire dans un message PCEP quand l'objet DOIT être inclus pour que le message soit considéré comme valide. Un message PCEP avec un objet obligatoire manquant DOIT déclencher un message d'erreur (voir le paragraphe 7.15). À l'inverse, si un objet est facultatif, l'objet peut ou non être présent.

Un fanion appelé le fanion P est défini dans l'en-tête commun de chaque objet PCEP (voir le paragraphe 7.2). Quand ce

fanion est établi dans un objet d'une PCReq, le PCE DOIT prendre en compte les informations portées dans l'objet durant le calcul de chemin. Par exemple, l'objet METRIC défini au paragraphe 7.8 permet à un PCC de spécifier des limites de coût de chemin acceptables. L'objet METRIC est facultatif, mais un PCC peut établir un fanion pour s'assurer que la contrainte est prise en compte. Dans ce cas, si la contrainte ne peut pas être prise en compte par le PCE, celui-ci DOIT déclencher un message d'erreur.

Pour chaque type de message PCEP, des règles sont définies pour spécifier l'ensemble d'objets que le message peut porter. On utilise le format Backus-Naur (BNF) (voir la [RFC5511]) pour spécifier ces règles. Des crochets angulaires se réfèrent à des sous séquences facultatives. Une mise en œuvre DOIT former les messages PCEP en utilisant l'ordre d'objets spécifié dans ce document.

6.1 En-tête commun

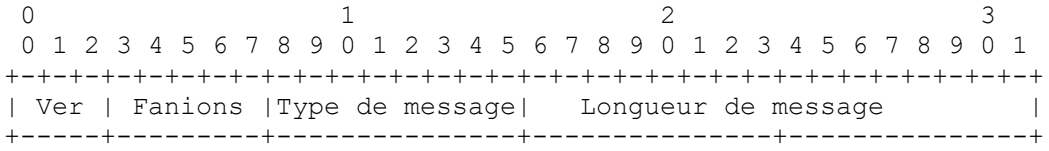


Figure 7 : En-tête commun de message PCEP

Ver (Version) (3 bits) : numéro de version PCEP. La version actuelle est la version 1.

Fanions (5 bits) : aucun fanion n'est actuellement défini. Les bits non alloués sont considérés comme réservés. Ils DOIVENT être réglés à zéro à l'émission et DOIVENT être ignorés à réception.

Type de message (8 bits) : les types de message suivants sont actuellement définis :

Valeur	Signification
1	Open *(ouvert)*
2	Keepalive *(garder en vie)*
3	Demande de calcul de chemin
4	Réponse de calcul de chemin
5	Notification
6	Erreur
7	Close *(fermer)*

Longueur de message (16 bits) : longueur totale du message PCEP incluant l'en-tête commun, exprimé en octets.

6.2. Message Open

Le message Open est un message PCEP envoyé par un PCC à un PCE et par un PCE à un PCC afin d'établir une session PCEP. Le champ Type de message de l'en-tête commun PCEP pour le message Open est réglé à 1.

Une fois la connexion TCP bien établie, le premier message envoyé par le PCC au PCE ou par le PCE au PCC DOIT être un message Open comme spécifié à l'Appendice A.

Tout message reçu avant un message Open DOIT déclencher une condition d'erreur de protocole causant l'envoi d'un message PCErr avec le type d'erreur "échec d'établissement de session PCEP" et la valeur d'erreur "réception d'un message Open invalide ou d'un message non Open" et la tentative d'établissement de session PCEP DOIT être terminée par la clôture de la connexion TCP.

Le message Open est utilisé pour établir une session PCEP entre les homologues PCEP. Durant la phase d'établissement, les homologues PCEP échangent plusieurs caractéristiques de session. Si les deux parties s'accordent sur ces caractéristiques, la session PCEP est bien établie.

Le format d'un message Open est comme suit :

<Message Open>::= <En-tête commun> <OPEN>

Le message Open DOIT contenir exactement un objet OPEN (voir le paragraphe 7.3).

Diverses caractéristiques de session sont spécifiées dans l'objet OPEN. Une fois que la connexion TCP a été bien établie, l'envoyeur DOIT lancer un temporisateur d'initialisation appelé OpenWait après l'expiration duquel, si aucun message Open n'a été reçu, il envoie un message PCErr et libère la connexion TCP (voir les détails à l'Appendice A).

Une fois qu'un message Open a été envoyé à un homologue PCEP, l'envoyeur DOIT lancer un temporisateur d'initialisation appelé KeepWait après l'expiration duquel, si ni un message Keepalive n'a été reçu, ni un message PCErr en cas de désaccord sur les caractéristiques de session, un message PCErr DOIT être envoyé et la connexion TCP DOIT être libérée (voir les détails à l'Appendice A).

Les temporisateurs OpenWait et KeepWait ont une valeur fixe de 1 minute.

À réception d'un message Open, l'homologue PCEP receveur DOIT déterminer si les caractéristiques de session PCEP suggérées sont acceptables. Si au moins une des caractéristiques n'est pas acceptable pour l'homologue receveur, il DOIT envoyer un message d'erreur. Le message d'erreur DEVRAIT aussi contenir l'objet OPEN en question et, pour chaque paramètre de session inacceptable, une valeur de paramètre acceptable DEVRAIT être proposée dans le champ approprié de l'objet OPEN à la place de la valeur originellement proposée. L'homologue PCEP PEUT décider de renvoyer un message Open avec des caractéristiques de session différentes. Si un second message Open est reçu avec le même ensemble de paramètres ou avec des paramètres qui sont encore inacceptables, l'homologue receveur DOIT envoyer un message d'erreur et il DOIT immédiatement clore la connexion TCP. Les détails sur les messages d'erreur se trouvent au paragraphe 7.15. Des essais successifs sont permis, mais une mise en œuvre DEVRAIT utiliser une procédure de retard exponentiel d'essai d'établissement de session.

Si les caractéristiques de session PCEP sont acceptables, l'homologue PCEP receveur DOIT envoyer un message Keepalive (défini au paragraphe 6.3) qui sert d'accusé de réception.

La session PCEP est considérée comme établie une fois que les deux homologues PCEP ont reçu un message Keepalive de leur homologue.

6.3 Message Keepalive

Un message Keepalive est un message PCEP envoyé par un PCC ou un PCE afin de garder la session en état actif. Le message Keepalive est aussi utilisé en réponse à un message Open pour accuser réception d'un message Open reçu et signifier que les caractéristiques de session PCEP sont acceptables. Le champ Type de message de l'en-tête commun PCEP pour le message Keepalive est réglé à 2. Le message Keepalive ne contient aucun objet.

PCEP a son propre mécanisme de maintien en vie utilisé pour s'assurer de la vie de la session PCEP. Cela exige la détermination de la fréquence à laquelle chaque homologue PCEP envoie des messages Keepalive. Des valeurs asymétriques peuvent être choisies ; donc, il n'y a pas de contrainte pour rendre obligatoire l'usage de fréquences identiques de Keepalive par les deux homologues PCEP. Le DeadTimer est défini comme la période après l'expiration de laquelle un homologue PCEP déclare la session morte si aucun message PCEP n'a été reçu (Keepalive ou tout autre message PCEP) ; donc, tout message PCEP agit comme un message Keepalive. De même, il n'y a pas de contrainte qui rende obligatoire l'utilisation de DeadTimer identique par les deux homologues PCEP. La valeur minimum du temporisateur Keepalive est 1 seconde. Les déploiements DEVRAIENT examiner attentivement l'impact de l'utilisation de valeurs faibles pour le temporisateur Keepalive car elles pourraient ne pas donner lieu aux résultats attendus dans des périodes d'instabilité temporaire du réseau.

Les messages Keepalive sont envoyés à la fréquence spécifiée dans l'objet OPEN porté dans un message Open en accord avec les règles spécifiées au paragraphe 7.3. Comme tout message PCEP peut servir de Keepalive, une mise en œuvre peut soit décider d'envoyer des messages Keepalive à intervalle fixe sans considération de si d'autres messages PCEP pourraient avoir été envoyés depuis le dernier message Keepalive envoyé, soit peut décider de différer l'envoi du prochain message Keepalive sur la base du moment auquel le dernier message PCEP (autre qu'un Keepalive) a été envoyé.

Noter que l'envoi de messages Keepalive pour garder la session en vie est facultatif, et les homologues PCEP peuvent décider de ne pas envoyer de messages Keepalive une fois que la session PCEP est établie ; dans ce cas, l'homologue qui ne reçoit pas de messages Keepalive ne s'attend pas à les recevoir et NE DOIT PAS déclarer la session inactive.

Le format d'un message Keepalive est comme suit :

<Message Keepalive>::= <En-tête commun>

6.4 Message Demande de calcul de chemin (PCReq)

Un message Demande de calcul de chemin (aussi appelé un message PCReq) est un message PCEP envoyé par un PCC à un PCE pour demander un calcul de chemin. Un message PCReq peut porter plus d'une demande de calcul de chemin. Le champ Type de message de l'en-tête commun PCEP pour le message PCReq est réglé à 3.

Il y a deux objets obligatoires qui DOIVENT être inclus dans un message PCReq : les objets RP et END-POINTS (voir la Section 7). Si un de ces objets, ou les deux, manque, le PCE receveur DOIT envoyer un message d'erreur au PCC demandeur. Les autres objets sont facultatifs.

Le format d'un message PCReq est comme suit :

<Message PCReq>::= <En-tête commun> [<liste de svec>] <liste de demandes>

où :

<liste de svec>::=<SVEC>[<liste de svec>]
<liste de demandes>::=<demande>[<liste de demandes>]

<demande>::= <RP>
<END-POINTS>
[<LSPA>]
[<BANDWIDTH>]
[<liste de métriques>]
[<RRO>[<BANDWIDTH>]]
[<IRO>]
[<LOAD-BALANCING>]

où :

<liste de métriques>::=<METRIC>[<liste de métriques>]

Les objets SVEC, RP, END-POINTS, LSPA, BANDWIDTH, METRIC, RRO, IRO, et LOAD-BALANCING sont définis à la Section 7. Le cas particulier de deux objets BANDWIDTH est discuté en détail au paragraphe 7.7.

Une mise en œuvre de PCEP est libre de traiter les demandes reçues dans n'importe quel ordre. Par exemple, les demandes peuvent être traitées dans l'ordre de leur réception, réordonnées et se voir allouer une priorité selon la politique locale, réordonnées selon la priorité codée dans l'objet RP (paragraphe 7.4.1) ou traitées en parallèle.

6.5 Message Réponse de calcul de chemin (PCRep)

Le message PCEP Réponse de calcul de chemin (aussi appelé un message PCRep) est un message PCEP envoyé par un PCE à un PCC demandeur en réponse à un message PCReq précédemment reçu. Le champ Type de message de l'en-tête commun PCEP pour le message PCRep est réglé à 4.

La mise en bouquet de plusieurs réponses à un ensemble de demandes de calcul de chemin au sein d'un seul message PCRep est pris en charge par PCEP. Si un PCE reçoit des demandes de calcul de chemin non synchronisées au moyen d'un ou plusieurs messages PCReq provenant d'un PCC demandeur, il PEUT décider de grouper les chemins calculés dans un seul message PCRep afin de réduire la charge du plan de contrôle. Noter que l'inconvénient d'une telle approche est l'introduction de délais supplémentaires pour certaines demandes de calcul de chemin de l'ensemble. À l'inverse, un PCE qui reçoit plusieurs demandes au sein du même message PCReq PEUT décider de fournir chaque chemin calculé dans des messages PCRep séparés ou dans le même message PCRep. Un message PCRep peut contenir des réponses positives et négatives.

Un message PCRep peut contenir un ensemble de chemins calculés correspondants soit à une seule demande de calcul de chemin avec équilibrage de charges (voir le paragraphe 7.16) soit plusieurs demandes de calcul de chemin générées par un PCC demandeur. Le message PCRep peut aussi contenir plusieurs chemins acceptables correspondants à la même

demande.

Le message PCRep DOIT contenir au moins un objet RP. Pour chaque réponse groupée dans un seul message PCReq, un objet RP DOIT être inclus contenant un numéro d'identifiant de demande identique à celui spécifié dans l'objet RP porté dans le message PCReq correspondant (voir au paragraphe 7.4 la définition de l'objet RP).

Si la demande de calcul de chemin peut être satisfaite (c'est-à-dire, si le PCE trouve un ensemble de chemins qui satisfont l'ensemble de contraintes) l'ensemble de chemins calculés spécifié au moyen d'objets Chemin explicite (ERO, *Explicite Route Object*) est inséré dans le message PCRep. L'ERO est défini au paragraphe 7.9. La situation où plusieurs chemins calculés sont fournis dans un message PCRep est discutée en détails au paragraphe 7.13. De plus, quand un PCC demande le calcul d'un ensemble de chemins pour une quantité totale de bande passante au moyen d'un objet LOAD-BALANCING porté dans un message PCReq, le ERO de chaque chemin calculé peut être suivi d'un objet BANDWIDTH comme discuté au paragraphe 7.16.

Si la demande de calcul de chemin ne peut pas être satisfaite, le message PCRep DOIT inclure un objet NO-PATH. L'objet NO-PATH (décrt au paragraphe 7.5) peut aussi contenir d'autres informations (par exemple, les raisons de l'échec du calcul de chemin).

Le format d'un message PCRep est comme suit :

<Message PCRep> ::= <En-tête commun> <liste de réponses>

où :

<liste de réponses>::=<réponse>[<liste de réponses>]

<réponse>::=<RP>
[<NO-PATH>]
[<liste d'attributs>]
[<liste de chemins>]

<liste de chemins>::=<chemin>[<liste de chemins>]

<chemin>::= <ERO><liste d'attributs>

où :

<liste d'attributs>::=[<LSPA>]
[<BANDWIDTH>]
[<liste de métriques>]
[<IRO>]

<liste de métriques>::=<METRIC>[<liste de métriques>]

6.6 Message Notification (PCNtf)

Le message PCEP Notification (aussi appelé le message PCNtf) peut être envoyé soit par un PCE à un PCC, soit par un PCC à un PCE, pour notifier un événement spécifique. Le champ Type de message de l'en-tête commun PCEP pour le message PCNtf est réglé à 5.

Le message PCNtf DOIT porter au moins un objet NOTIFICATION et PEUT contenir plusieurs objets NOTIFICATION si le PCE ou PCC a l'intention de notifier plusieurs événements. L'objet NOTIFICATION est défini au paragraphe 7.14. Le message PCNtf PEUT aussi contenir des objets RP (voir le paragraphe 7.4) quand la notification se réfère à des demandes de calcul de chemin particulières.

Le message PCNtf peut être envoyé par un PCC ou un PCE en réponse à une demande ou de manière non sollicitée.

Le format d'un message PCNtf est comme suit :

<Message PCNtf >::=<En-tête commun> <liste de notify>

<liste de notify>::=<notify> [<liste de notify>]

<notify>::= [<liste d'identifiants de demande>] <liste de notifications>

<liste d'identifiants de demande>::=<RP>[<liste d'identifiants de demande>]

<liste de notifications>::=<NOTIFICATION>[<liste de notifications>]

6.7 Message Erreur (PCErr)

Le message PCEP Erreur (aussi appelé un message PCErr) est envoyé dans plusieurs situations : quand une condition d'erreur de protocole est rencontrée ou quand la demande n'est pas conforme à la spécification PCEP (par exemple, réception d'un message mal formé, réception d'un message où manque un objet obligatoire, violation de politique, message inattendu, référence de demande inconnue). Le champ Type de message de l'en-tête commun PCEP pour le message PCErr est réglé à 6.

Le message PCErr est envoyé par un PCC ou un PCE en réponse à une demande ou de manière non sollicitée. Si le message PCErr est envoyé en réponse à une demande, le message PCErr DOIT inclure l'ensemble d'objets RP relatifs aux demandes de calcul de chemin en cours qui ont déclenché la condition d'erreur. Dans le dernier cas (non sollicité) aucun objet RP n'est inséré dans le message PCErr. Par exemple, aucun objet RP n'est inséré dans un PCErr quand la condition d'erreur s'est produite durant la phase d'initialisation. Un message PCErr DOIT contenir un objet PCEP-ERROR qui spécifie la condition d'erreur PCEP. L'objet PCEP-ERROR est défini au paragraphe 7.15.

Le format d'un message PCErr est comme suit :

<Message PCErr> ::= <En-tête commun> (<liste d'objets d'erreur> [<Open>]) | <erreur> [<liste d'erreurs>]

<liste d'objets d'erreur>::=<PCEP-ERROR>[<liste d'objets d'erreur>]

<erreur>::=[<liste d'identifiant de demande>] <liste d'objets d'erreur>

<liste d'identifiant de demande>::=<RP>[<liste d'identifiant de demande>]

<liste d'erreurs>::=<erreur>[<liste d'erreurs>]

La procédure à réception d'un message PCErr est définie au paragraphe 7.15.

6.8 Message Close

Le message Close est un message PCEP qui est soit envoyé par un PCC à un PCE, soit par un PCE à un PCC afin de clore une session PCEP établie. Le champ Type de message de l'en-tête commun PCEP pour le message Close est réglé à 7.

Le format d'un message Close est comme suit :

<Message Close>::= <En-tête commun> <CLOSE>

Le message Close DOIT contenir exactement un objet CLOSE (voir le paragraphe 6.8). Si plus d'un objet CLOSE est présent, le premier DOIT être traité et les objets suivants ignorés.

À réception d'un message Close valide, l'homologue PCEP receveur DOIT annuler toutes les demandes en instance, il DOIT clore la connexion TCP et NE DOIT PAS envoyer d'autre message PCEP sur la session PCEP.

6.9 Réception de messages inconnus

Une mise en œuvre PCEP qui reçoit un message PCEP non reconnu DOIT envoyer un message PCErr avec la valeur d'erreur de 2 (capacité non prise en charge).

Si un PCC/PCE reçoit des messages non reconnus à un taux égal ou supérieur à MAX-UNKNOWN-MESSAGES

demandes de message inconnu par minute, le PCC/PCE DOIT envoyer un message PCEP CLOSE avec la valeur "Réception d'un nombre inacceptable de messages PCEP inconnus". Une valeur RECOMMANDÉE pour MAX-UNKNOWN-MESSAGES est 5. Le PCC/PCE DOIT clore la session TCP et NE DOIT PAS envoyer d'autre message PCEP sur la session PCEP.

7. Formats d'objet

Les objets PCEP ont un format commun. Ils commencent par un en-tête d'objet commun (voir le paragraphe 7.2). Ceci est suivi par des champs spécifiques de l'objet définis pour chaque objet différent. L'objet peut aussi inclure un ou plusieurs ensembles de données codées en type-longueur-valeur (TLV). Chaque TLV a la même structure décrite au paragraphe 7.1.

7.1 Format de TLV PCEP

Un objet PCEP peut inclure un ensemble de un ou plusieurs TLV facultatifs.

Tous les TLV PCEP ont le format suivant :

Type : 2 octets
Longueur : 2 octets
Valeur : variable

Un objet TLV PCEP est composé de 2 octets pour le type, 2 octets spécifiant la longueur du TLV, et un champ de valeur.

Le champ Longueur défini la longueur de la portion valeur en octets.Le TLV est bourré à un alignement de quatre octets ; le bourrage n'est pas inclus dans le champ Longueur (donc une valeur de trois octets aurait une longueur de 3, mais la taille totale du TLV va être de 8 octets).

Les TLV non reconnus DOIVENT être ignorés.

La gestion par l'IANA de l'espace des codes d'identifiant de type d'objet TLV est décrite à la Section 9.

7.2 En-tête d'objet commun

Un objet PCEP porté dans un message PCEP consiste en un ou plusieurs mots de 32 bits avec un en-tête commun qui a le format suivant :

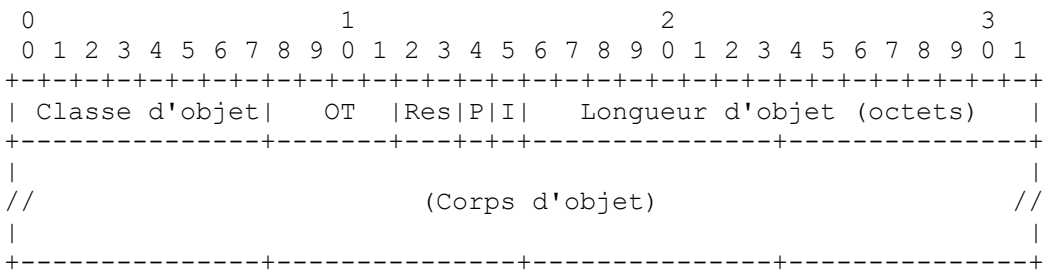


Figure 8 : En-tête d'objet commun PCEP

Classe d'objet (8 bits) : identifie la classe de l'objet PCEP.

OT (Type d'objet) (4 bits) : identifie le type d'objet PCEP.

Les champs Classe d'objet et Type d'objet sont gérés par l'IANA.
Les champs Classe d'objet et Type d'objet identifient de façon univoque chaque objet PCEP.

Fanions Res (2 bits) : champ réservé. Ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Fanion P (Règle de traitement) (1 bit) : le fanion P permet à un PCC de spécifier dans un message PCReq envoyé à un PCE

si l'objet doit être pris en compte par le PCE durant le calcul de chemin ou si il est juste facultatif. Quand le fanion P est établi, l'objet DOIT être pris en compte par le PCE. À l'inverse, quand le fanion P est à zéro, l'objet est facultatif et le PCE est libre de l'ignorer.

Fanion I (Ignore) (1 bit) : le fanion I est utilisé par un PCE dans un message PCRep pour indiquer à un PCC si un objet facultatif a ou non été traité. Le PCE PEUT inclure l'objet ignoré facultatif dans sa réponse et établir le fanion I pour indiquer que l'objet facultatif a été ignoré durant le calcul de chemin. Quand le fanion I est à zéro, le PCE indique que l'objet facultatif a été traité durant le calcul de chemin. L'établissement du fanion I pour des objets facultatifs est purement indicatif et facultatif. Le fanion I n'a pas de signification dans un message PCRep quand le fanion P a été établi dans le message PCReq correspondant.

Si le PCE ne comprend pas un objet avec le fanion P établi ou comprend l'objet mais décide de l'ignorer, le message PCEP entier DOIT être rejeté et le PCE DOIT envoyer un message PCErr avec le type d'erreur "Objet inconnu" ou "Objet non pris en charge" avec l'objet ERO correspondant. Noter que si une PCReq inclut plusieurs demandes, seules les demandes pour lesquelles un objet dont le fanion P établi est inconnu/onn reconnu DOIVENT être rejetées.

Longueur d'objet (16 bits) : spécifie la longueur totale de l'objet incluant l'en-tête, en octets. Le champ Longueur d'objet DOIT toujours être un multiple de 4, et au moins 4. La longueur maximale du contenu d'un objet est 65528 octets.

7.3 Objet OPEN

L'objet OPEN DOIT être présent dans chaque message Open et PEUT être présent dans un message PCErr. Il DOIT y avoir seulement un objet OPEN par message Open ou PCErr.

L'objet OPEN contient un ensemble de champs utilisés pour spécifier la version PCEP, la fréquence de Keepalive, le DeadTimer, et l'identifiant de session PCEP, avec divers fanions. L'objet OPEN peut aussi contenir un ensemble de TLV utilisés pour porter diverses caractéristiques de session comme les capacités détaillées du PCE, les règles de politique, et ainsi de suite. Aucun TLV n'est actuellement défini.

La classe d'objet OPEN est 1.

Le type d'objet OPEN est 1.

Le format du corps d'objet OPEN est comme suit :

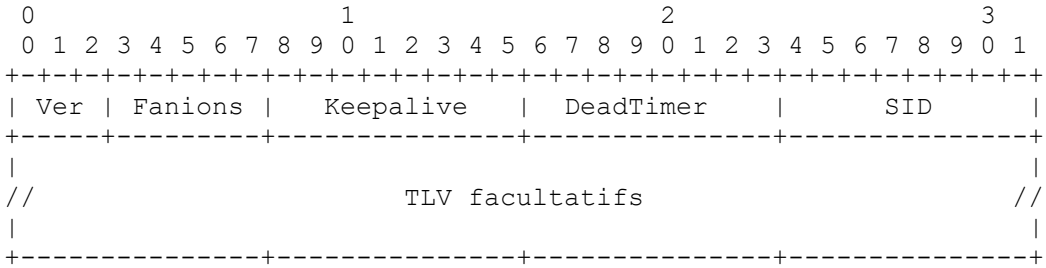


Figure 9 : Format d'objet OPEN

Ver (3 bits) : version PCEP. La version actuelle est 1.

Fanions (5 bits) : aucun fanion n'est actuellement défini. Les bits non alloués sont considérés comme réservés. Ils DOIVENT être réglés à zéro à l'émission et DOIVENT être ignorés à réception.

Keepalive (8 bits) : durée maximum (en secondes) entre deux messages PCEP consécutifs envoyés par l'envoyeur de ce message. La valeur minimum pour le Keepalive est 1 seconde. Quand il est réglé à 0, une fois la session établie, aucun autre message Keepalive n'est envoyé à l'homologue distant. Une valeur RECOMMANDÉE pour la fréquence de Keepalive est 30 secondes.

DeadTimer (8 bits) : spécifie la durée après l'expiration de laquelle l'homologue PCEP peut déclarer que la session avec l'envoyeur du message Open est morte si aucun message PCEP n'a été reçu. Le DeadTimer DEVRAIT être réglé à 0 et DOIT être ignoré si le Keepalive est réglé à 0. Une valeur RECOMMANDÉ pour DeadTimer est 4 fois la valeur de

Keepalive.

Exemple :

A envoie un message Open à B avec Keepalive = 10 secondes et DeadTimer = 40 secondes. Cela signifie que A envoie des messages Keepalive (ou tout autre message PCEP) à B toutes les 10 secondes et B peut déclarer la session PCEP avec A morte si aucun message PCEP n'a été reçu de A dans toute période de 40 secondes.

SID (Identifiant de session PCEP) (8 bits) : numéro de session PCEP non signé qui identifie la session en cours. Le SID DOIT être incrémenté chaque fois qu'une nouvelle session PCEP est établie. Il est utilisé pour les besoins d'enregistrement et de correction. Chaque incrément DEVRAIT avoir une valeur de 1 et peut causer un retour à zéro.

Le SID est utilisé pour préciser les instances de sessions avec le même homologue. Une mise en œuvre PCEP pourrait utiliser une seule source de SID parmi tous les homologues, ou une source pour chaque homologue. La première solution pourrait contraindre la mise en œuvre à seulement 256 sessions concurrentes. La dernière exige potentiellement plus d'état. Il y a un numéro de SID dans chaque direction.

Des TLV facultatifs peuvent être inclus dans le corps d'objet OPEN pour spécifier les caractéristiques du PCC ou PCE. La spécification de tels TLV sort du domaine d'application de ce document.

Quand il est présent dans un message Open, l'objet OPEN spécifie les caractéristiques de session PCEP proposées. À réception de caractéristiques de session PCEP inacceptables durant la phase d'initialisation de session PCEP, l'homologue PCEP receveur (le PCE) PEUT inclure un objet OPEN dans le message PCErr de façon à proposer des valeurs de remplacement acceptables des caractéristiques de session.

7.4 Objet RP

L'objet RP (Request Parameters) DOIT être porté dans chaque message PCReq et PCRep et PEUT être porté dans les messages PCNtf et PCErr. L'objet RP est utilisé pour spécifier diverses caractéristiques de la demande de calcul de chemin.

Le fanion P de l'objet RP DOIT être établi dans les messages PCReq et PCRep et DOIT être à zéro dans les messages PCNtf et PCErr. Si l'objet RP est reçu avec le fanion P réglé incorrectement selon les règles ci-dessus, l'homologue receveur DOIT envoyer un message PCErr avec le type d'erreur 10 et la valeur d'erreur 1. La demande de calcul de chemin correspondante DOIT être annulée par le PCE sans autre notification.

7.4.1 Définition d'objet

La classe d'objet RP est 2.

Le type d'objet RP est 1.

Le format du corps d'objet RP est comme suit :

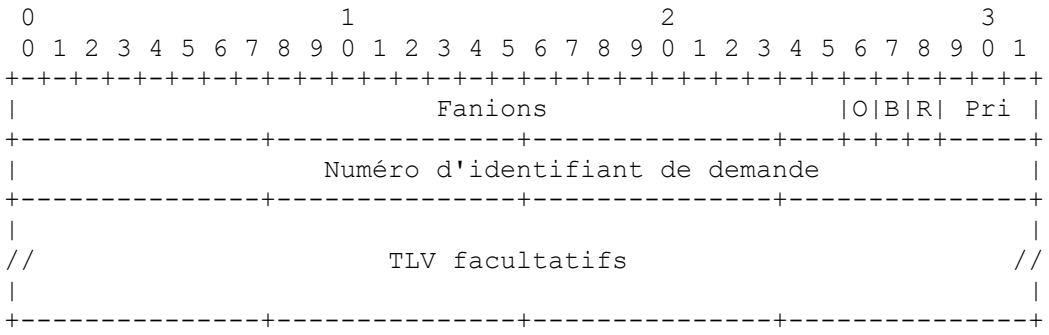


Figure 10 : Format du corps d'objet RP

Le corps d'objet RP a un longueur variable et peut contenir des TLV supplémentaires. Aucun TLV n'est actuellement défini.

Fanions (32 bits) : Les fanions suivants sont actuellement définis :

Pri (Priorité) (3 bits) : le champ Priorité de 1 à 7 peut être utilisé par le PCC demandeur pour spécifier au PCE la priorité de la demande. La décision de la priorité qui devrait être utilisée pour une demande spécifique est une affaire locale ; elle DOIT être réglée à 0 quand elle est inutilisée. De plus, l'utilisation de la priorité de demande de calcul de chemin par le programmeur du PCE est spécifique de la mise en œuvre et sort du domaine d'application de ce document. Noter qu'il n'est pas exigé qu'un PCE prenne en charge le champ Priorité : dans ce cas, il est RECOMMANDÉ que le PCC règle le champ Priorité à 0 dans l'objet RP. Si le PCE ne prend pas en compte la priorité de demande, il est RECOMMANDÉ de régler le champ Priorité à 0 dans l'objet RP porté dans le message PCRep correspondant, sans considération de la valeur de priorité contenue dans l'objet RP porté dans le message PCReq correspondant. Une valeur numérique supérieure du champ de priorité reflète une priorité supérieure. Noter qu'il est de la responsabilité de l'administrateur du réseau d'utiliser les valeurs de priorité d'une manière cohérente à travers les divers PCC. La capacité d'un PCE à prendre en charge la priorité des demandes PEUT être découverte dynamiquement par les PCC au moyen de la découverte de capacité de PCE. Si elle n'est pas annoncée par le PCE, un PCC peut décider de régler la priorité de demande et va apprendre la capacité du PCE à prendre en charge la priorité de demande en observant le champ Priorité de l'objet RP reçu dans le message PCRep. Si la valeur du champ Pri est réglée à 0, cela signifie que le PCE ne prend pas en charge le traitement des priorités de demande : en d'autres termes, la demande de calcul de chemin a été honorée mais sans prendre en compte la priorité de demande.

R (Réoptimisation) (1 bit) : quand il est établi, le PCC demandeur spécifie que le message PCReq se rapporte à la réoptimisation d'un LSP TE existant. Pour tous les LSP TE sauf les LSP de bande passante zéro, quand le bit R est établi, un RRO (voir le paragraphe 7.10) DOIT être inclus dans le message PCReq pour montrer le chemin du LSP TE existant. Aussi, pour tous les LSP TE sauf les LSP de bande passante zéro, quand le bit R est établi, la bande passante existante du LSP TE à réoptimiser DOIT être fournie dans un objet BANDWIDTH (voir le paragraphe 7.7). Cet objet BANDWIDTH est en plus de l'instance de cet objet utilisée pour décrire la bande passante désirée du LSP réoptimisé. Pour les LSP de bande passante zéro, les objets RRO et BANDWIDTH qui rapportent les caractéristiques du LSP TE existant sont facultatifs.

B (Bidirectionnel) (1 bit) : quand il est établi, le PCC spécifie que la demande de calcul de chemin se rapporte à un LSP TE bidirectionnel qui a les mêmes exigences d'ingénierie du trafic, y compris de partage de sort, de protection et restauration, de LSR, de liaisons TE, et de ressources (par exemple, latence et gigue) dans chaque direction. Quand il est à zéro, le LSP TE est unidirectionnel.

O (strict/lâche) (1 bit) : quand il est établi, dans un message PCReq, cela indique qu'un chemin lâche est acceptable. Autrement, quand il est à zéro, cela indique au PCE qu'un chemin exclusivement constitué de bonds stricts est exigé. Dans un message PCRep, quand le bit O est établi, cela indique que le chemin retourné est un chemin lâche ; autrement (quand le bit O est à zéro) le chemin retourné est constitué de bonds stricts.

Les bits non alloués sont considérés comme réservés. Ils DOIVENT être réglés à zéro à l'émission et DOIVENT être ignorés à réception.

Numéro d'identifiant de demande (32 bits) : La valeur du Numéro d'identifiant de demande combinée à l'adresse IP de source du PCC et à l'adresse du PCE identifie de façon univoque le contexte de la demande de calcul de chemin. Le numéro d'identifiant de demande est utilisé pour ôter toute ambiguïté entre les demandes en instance, et donc il DOIT être changé (comme en l'incrémentant) chaque fois qu'une nouvelle demande est envoyée au PCE, et il peut revenir à zéro.

La valeur 0x00000000 est considérée comme invalide.

Si aucune réponse de calcul de chemin n'est reçue du PCE (par exemple, la demande est éliminée par le PCE à cause d'un débordement de mémoire) et si le PCC souhaite envoyer sa demande à nouveau, le même numéro d'identifiant de demande DOIT être utilisé. À réception d'une demande de calcul de chemin provenant d'un PCC avec le même numéro d'identifiant de demande, le PCE DEVRAIT traiter la demande comme une nouvelle demande. Une mise en œuvre PEUT choisir de mettre en antémémoire les réponses de calcul de chemin afin de traiter rapidement les retransmissions sans avoir à traiter deux fois une demande de calcul de chemin (dans le cas où la première demande a été éliminée ou perdue). À réception d'une réponse de calcul de chemin provenant d'un PCE avec le même numéro d'identifiant de demande, le PCC DEVRAIT éliminer en silence la réponse de calcul de chemin.

À l'inverse, des numéros d'identifiant de demande différents DOIVENT être utilisés pour des demandes différentes envoyées à un PCE.

Le même numéro d'identifiant de demande PEUT être utilisé pour des demandes de calcul de chemin envoyées à des PCE différents. La réponse de calcul de chemin est identifiée sans ambiguïté par l'adresse IP de source du PCE qui répond.

7.4.2 Traitement de l'objet RP

Si un message PCReq est reçu qui ne contient pas d'objet RP, le PCE DOIT envoyer un message PCErr au PCC demandeur avec le type d'erreur "Objet exigé manquant" et la valeur d'erreur "Objet RP manquant".

Si le bit O du message RP porté dans un message PCReq est à zéro et si la politique locale a été configurée sur le PCE à ne pas fournir de chemins explicites (par exemple, pour des raisons de confidentialité) un message PCErr DOIT être envoyé par le PCE au PCC demandeur et la demande de calcul de chemin en instance DOIT être éliminée. Le type d'erreur est "Violation de politique" et la valeur d'erreur est "Bit O à zéro".

Quand le bit R de l'objet RP est établi dans un message PCReq, cela indique que la demande de calcul de chemin se rapporte à la réoptimisation d'un LSP TE existant. Dans ce cas, le PCC DOIT aussi fournir le chemin strict/lâche en incluant un objet RRO dans le message PCReq afin d'éviter/limiter le double compte de bande passante si et seulement si le LSP TE est un LSP TE de bande passante non zéro. Si le PCC n'a pas demandé un chemin strict (bit O établi) une réoptimisation peut encore être demandée par le PCC, mais cela exige que le PCE soit à états pleins (garde trace du chemin précédemment calculé avec la liste des bonds stricts associés) soit ait la capacité de restituer le segment complet de chemin exigé. Autrement, le PCC DOIT informer le PCE sur le chemin actif et la liste associée de bonds stricts dans une PCReq. L'absence d'un RRO dans le message PCReq pour un LSP TE de bande passante non zéro (quand le bit R de l'objet RP est établi) DOIT déclencher l'envoi d'un message PCErr avec le type d'erreur "Objet exigé manquant" et la valeur d'erreur "Objet RRO manquant pour réoptimisation".

Si un PCC/PCE reçoit un message PCRep/PCReq qui contient un objet RP se référant à un numéro d'identifiant de demande inconnu , le PCC/PCE DOIT envoyer un message PCErr avec le type d'erreur "Référence de demande inconnue". Ceci est utilisé pour des besoins de débogage. Si un PCC/PCE reçoit des messages PCRep/PCReq avec des demandes inconnues à un taux égal ou supérieur à MAX-UNKNOWN-REQUESTS demandes inconnues par minute, le PCC/PCE DOIT envoyer un message PCEP CLOSE avec une valeur Close de "Réception d'un nombre inacceptable de demandes/réponses inconnues". Une valeur RECOMMANDÉE pour MAX-UNKNOWN-REQUESTS est 5. Le PCC/PCE DOIT clore la session TCP et NE DOIT PAS envoyer d'autre message PCEP sur la session PCEP.

La réception d'un message PCEP qui contient un objet RP se référant à un numéro d'identifiant de demande de 0x00000000 DOIT être traitée de la même façon qu'une demande inconnue.

7.5 Objet NO-PATH

L'objet NO-PATH est utilisé dans les messages PCRep en réponse à un échec de demande de calcul de chemin (le PCE n'a pas pu trouver un chemin satisfaisant l'ensemble de contraintes). Quand un PCE ne peut pas trouver un chemin satisfaisant un ensemble de contraintes, il DOIT inclure un objet NO-PATH dans le message PCRep.

Il y a plusieurs catégories de problèmes qui peuvent conduire à une réponse négative. Par exemple, la chaîne de PCE pourrait être cassée (si il y avait plus d'un PCE impliqué dans le calcul de chemin) ou aucun chemin répondant à l'ensemble de contraintes n'a pu être trouvé. Le champ "NI (Nature du problème)" dans l'objet NO-PATH est utilisé pour rapporter la catégorie d'erreur.

Facultativement, si le PCE prend en charge une telle capacité, l'objet NO-PATH PEUT contenir un TLV facultatif NO-PATH-VECTOR défini ci-dessous et utilisé pour fournir plus d'informations sur les raisons qui ont conduit à une réponse négative. Le message PCRep PEUT aussi contenir une liste d'objets qui spécifient l'ensemble de contraintes qui n'ont pas pu être satisfaites. Le PCE PEUT juste copier l'ensemble d'objets qui ont été reçus et sont la cause de l'échec du calcul ou PEUT facultativement rapporter une valeur suggérée pour laquelle un chemin pourrait avoir été trouvé (dans ce cas, la valeur diffère de la valeur de la demande originale).

La classe d'objet NO-PATH est 3.

Le type d'objet NO-PATH est 1.

Le format du corps de l'objet NO-PATH est comme suit :

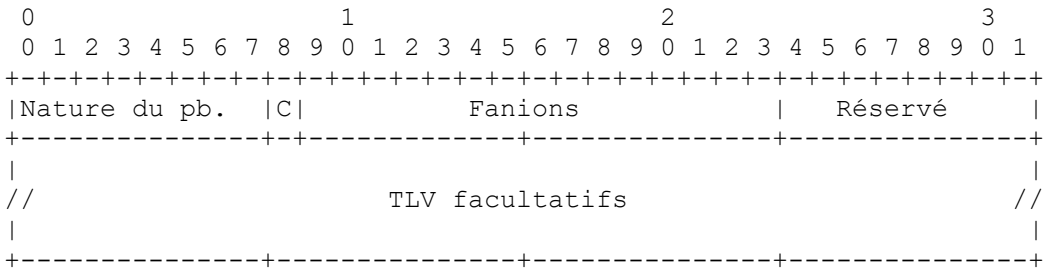


Figure 11 : Format d'objet NO-PATH

Nature du pb. (NI) (8 bits) : Le champ Nature du problème est utilisé pour rapporter la nature du problème qui a conduit à une réponse négative. Deux valeurs sont actuellement définies :
0 : aucun chemin ne satisfait l'ensemble de contraintes n'a pu être trouvé
1 : chaîne de PCE rompue

La valeur du champ Nature du problème peut être utilisée par le PCC pour divers propos :
* ajustement des contraintes avant de produire une nouvelle demande de calcul de chemin,
* choix explicite d'une nouvelle chaîne de PCE,
* enregistrement du type d'erreur pour une autre action de l'administrateur du réseau.

La gestion par l'IANA de l'espace de codes du champ NI est décrite à la Section 9.

Fanions (16 bits).
Le fanion suivant est actuellement défini :

Fanion C (1 bit) : quand il est établi, le PCE indique l'ensemble de contraintes non satisfaites (les raisons pour lesquelles un chemin n'a pas pu être trouvé) dans le message PCRep en incluant les objets PCEP pertinents. Quand il est à zéro, aucun contrainte manquante n'est spécifiée. Le fanion C n'a pas de signification et est ignoré sauf si le champ NI est réglé à 0x00.

Les bits non alloués sont considérés comme réservés. Ils DOIVENT être réglés à zéro à l'émission et DOIVENT être ignorés à réception.

Réservé (8 bits) : ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Le corps de l'objet NO-PATH a une longueur variable et peut contenir des TLV supplémentaires. Le seul TLV actuellement défini est le TLV NO-PATH- VECTOR défini ci-dessous.

Exemple : considérons le cas d'un PCC qui envoie une demande de calcul de chemin à un PCE pour un LSP TE de X Mbit/s. Supposons que le PCE ne peut pas trouver un chemin pour X Mbit/s. Dans ce cas, le PCE doit inclure dans le message PCRep un objet NO-PATH. Facultativement, le PCE peut aussi inclure l'objet original BANDWIDTH afin d'indiquer que la raison de l'échec de calcul est la contrainte de bande passante (dans ce cas, la valeur du champ NI est 0x00 et le fanion C est établi). Si le PCE prend en charge une telle capacité, il peut aussi inclure l'objet BANDWIDTH et rapporter une valeur de Y dans le champ de bande passante de l'objet BANDWIDTH (dans ce cas, le fanion C est établi) où Y se réfère à la bande passante pour laquelle un LSP TE avec les mêmes autres caractéristiques (comme les priorités d'établissement/garde, d'attribut LSP TE, de protection locale, etc.) pourrait avoir été calculé.

Quand l'objet NO-PATH est absent d'un message PCRep, la demande de calcul de chemin a été pleinement satisfaite et les chemins correspondants sont fournis dans le message PCRep.

Un TLV facultatif nommé NO-PATH-VECTOR PEUT être inclus dans l'objet NO-PATH afin de fournir plus d'informations sur les raisons qui ont conduit à une réponse négative.

Le TLV NO-PATH-VECTOR est conforme au format de TLV PCEP défini au paragraphe 7.1 et est composé de 2 octets pour le type, 2 octets spécifiant la longueur du TLV (longueur de la portion Valeur en octets) suivis par un champ de fanions d'une longueur fixe de 32 bits.

Type : 1
Longueur : 4 octets
Valeur : champ de fanions de 32 bits

L'IANA gère l'espace de fanions porté dans le TLV NO-PATH-VECTOR (voir la Section 9).

Les fanions suivants sont actuellement définis :
- o Numéro de bit : 31 - PCE actuellement indisponible
- o Numéro de bit : 30 - destination inconnue
- o Numéro de bit : 29 - source inconnue

7.6 Objet END-POINTS

L'objet END-POINTS est utilisé dans un message PCReq pour spécifier l'adresse IP de source et l'adresse IP de destination du chemin pour lequel un calcul de chemin est demandé. Le fanion P de l'objet EN0-POINTS DOIT être établi. Si l'objet END-POINTS est reçu avec le fanion P à zéro, l'homologue receveur DOIT envoyer un message PCErr avec le type d'erreur 10 et la valeur d'erreur 1. La demande de calcul de chemin correspondante DOIT être annulée par le PCE sans autre notification.

Noter que les adresses de source et destination spécifiées dans l'objet END-POINTS peuvent correspondre à l'adresse de source et destination IP du LSP TE ou de celles d'un segment de chemin. Deux objets END-POINTS (pour IPv4 et IPv6) sont définis.

La classe d'objet END-POINTS est 4.

Le type d'objet END-POINTS est 1 pour IPv4 et 2 pour IPv6.

Le format du corps de l'objet END-POINTS pour IPv4 (type d'objet 1) est comme suit :

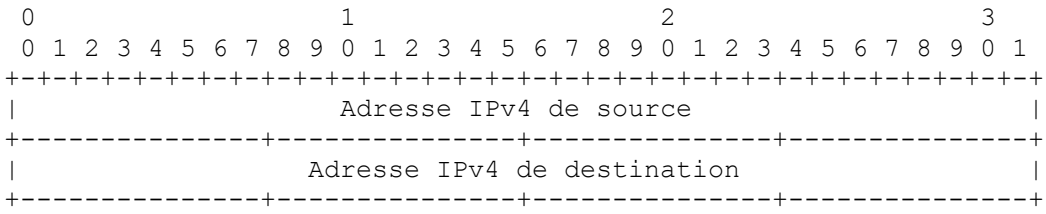


Figure 12 : Format de corps d'objet END-POINTS pour IPv4

The format of the objet END-POINTS for IPv6 (Object-Type=2) est comme suit :

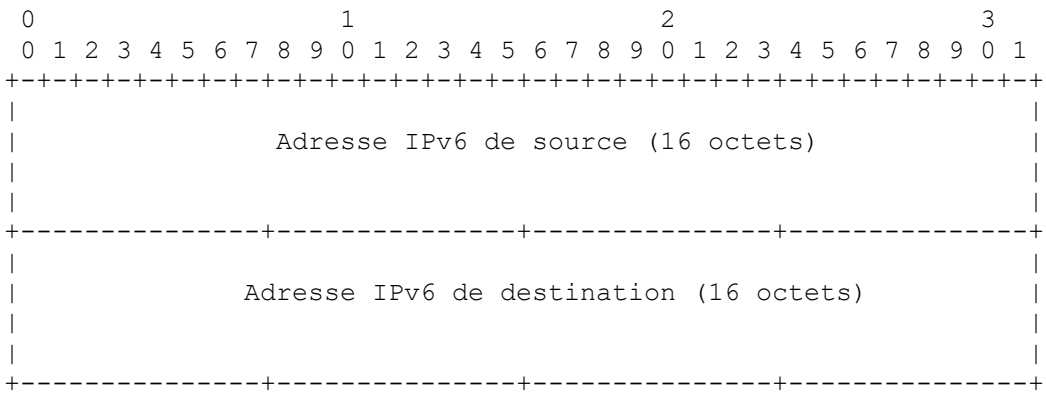


Figure 13 : Format de corps d'objet END-POINTS pour IPv6

Le corps d'objet END-POINTS a une longueur fixe de 8 octets pour IPv4 et 32 octets pour IPv6.

Si plus d'un objet END-POINTS est présent, le premier DOIT être traité et les objets suivants ignorés.

7.7 Objet BANDWIDTH

L'objet BANDWIDTH est utilisé pour spécifier la bande passante demandée pour un LSP TE. La notion de bande passante est similaire à celle utilisée pou la signalisation RSVP dans les [RFC2205], [RFC3209], et [RFC3473].

Si la bande passante demandée est égale à 0, l'objet BANDWIDTH est facultatif. À l'inverse, si la bande passante demandée n'est pas égale à 0, le message PCReq DOIT contenir un objet BANDWIDTH.

Dans le cas de réoptimisation d'un LSP TE, la bande passante du LSP TE existant DOIT aussi être incluse en plus de la bande passante demandée si et seulement si les deux valeurs diffèrent. Par conséquent, deux valeurs de type d'objet sont définies qui se réfèrent à la bande passante demandée et à la bande passante du LSP TE pour lequel la réoptimisation est effectuée.

L'objet BANDWIDTH peut être porté dans les messages PCReq et PCRep.

La classe d'objet BANDWIDTH est 5.

Deux valeurs de type d'objet sont définies pour l'objet BANDWIDTH :
- o Bande passante demandée : le type d'objet BANDWIDTH est 1.
- o Bande passante de LSP TE existant pour lequel une réoptimisation est demandée : le type d'objet BANDWIDTH est 2.

Le format du corps d'objet BANDWIDTH est comme suit :

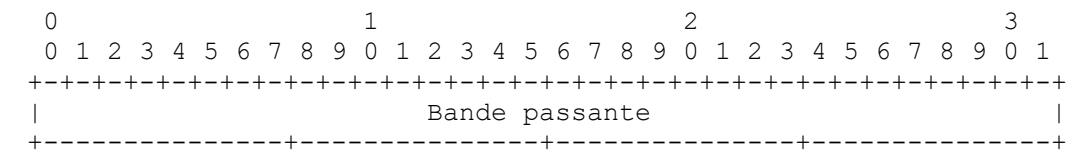


Figure 14 : Format de corps d'objet BANDWIDTH

Bande passante (32 bits) : la bande passante demandée est codée sur 32 bits en format de virgule flottante de l'IEEE (voir [IEEE.754.1985]) exprimée en octets par seconde. Voir le paragraphe 3.1.2 de la [RFC3471] pour un tableau des valeurs couramment utilisées.

Le corps d'objet BANDWIDTH a une longueur fixe de 4 octets.

7.8 Objet METRIC

L'objet METRIC est facultatif et peut être utilisé à plusieurs fins.

Dans un message PCReq, un PCC PEUT insérer un ou plusieurs objets METRIC:

- o Pour indiquer la métrique qui DOIT être optimisée par l'algorithme de calcul de chemin (métrique IGP, métrique TE, compte de bonds). Actuellement, trois métriques sont définies : le coût IGP, la métrique TE (voir la [RFC3785]) et le nombre de bonds traversés par un LSP TE.

- o Pour indiquer une limite au coût du chemin qui NE DOIT PAS être excédé pour que le chemin soit considéré comme acceptable par le PCC.

Dans un message PCRep, l'objet METRIC PEUT être inséré afin de fournir le coût du chemin calculé. Il PEUT aussi être inséré dans une PCRep avec l'objet NO-PATH pour indiquer que la contrainte de métrique n'a pas pu être satisfaite.

Les aspects algorithmiques du calcul de chemin utilisé par le PCE pour optimiser un chemin par rapport à une métrique spécifique sortent du domaine d'application de ce document.

On doit comprendre que de telles métriques de chemin n'ont de signification que si elle sont utilisées de façon cohérente : par exemple, si le délai d'un segment de chemin calculé est échangé entre deux PCE résidant dans des domaines différents, des façons cohérentes de définir le délai doivent être utilisées.

L'absence de l'objet METRIC DOIT être interprétée par le PCE comme une demande de calcul de chemin pour laquelle

aucune contrainte n'a besoin d'être appliquée à toute métrique.

La classe de l'objet METRIC est 6.

Le type d'objet METRIC est 1.

Le format du corps de l'objet METRIC est comme suit :

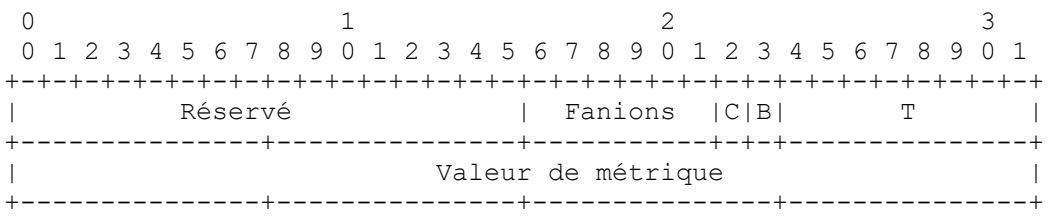


Figure 15 : Format de corps d'objet METRIC

Le corps de l'objet METRIC a une longueur fixe de 8 octets.

Réservé (16 bits) : ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

T (Type) (8 bits) : spécifie le type de métrique.

Trois valeurs sont actuellement définies :
* T=1 : métrique IGP
* T=2 : métrique TE
* T=3 : compte de bonds

Fanions (8 bits) : deux fanions sont actuellement définis :

B (Bound) (1 bit) : quand il est établi dans un message PCReq, la valeur de métrique indique une limite (un maximum) pour la métrique de chemin qui ne doit pas être excédée pour que le PCC considère le chemin calculé comme acceptable. La métrique de chemin doit être inférieure ou égale à la valeur spécifiée dans le champ Valeur de métrique. Quand le fanion B est à zéro, le champ valeur de métrique n'est pas utilisé pour refléter une contrainte de limite.

C (Métrique calculée) (1 bit) : quand il est établi dans un message PCReq, cela indique que le PCE DOIT fournir la valeur de métrique du chemin calculé (si un chemin devait satisfaire la contrainte) dans le message PCRep pour la métrique correspondante.

Les fanions non alloués DOIVENT être réglés à zéro à l'émission et DOIVENT être ignorés à réception.

Valeur de métrique (32 bits) : valeur de la métrique codée sur 32 bits en format de virgule flottante de l'IEEE (voir [IEEE.754]).

Plusieurs objets METRIC PEUVENT être insérés dans un message PCRep ou PCReq pour une demande donnée (c'est-à-dire, pour un RP donné). Pour une demande donnée, il DOIT y avoir au plus une instance d'objet METRIC pour chaque type de métrique avec la même valeur de fanion B. Si, pour une demande donnée, deux instances ou plus d'un objet METRIC avec la même valeur de fanion B sont présentes pour un type de métrique, seule la première instance DOIT être considérée et les autres instances DOIVENT être ignorées.

Pour une demande donnée, la présence de deux objets METRIC du même type avec une valeur différente du fanion B est permise. De plus, il est aussi permis d'insérer, pour une demande donnée, deux objets METRIC avec des types différents qui ont tous deux leur fanion B à zéro : dans ce cas, une fonction objective doit être utilisée par le PCE pour résoudre un problème d'optimisation multi paramètres.

Un objet METRIC utilisé pour indiquer la métrique pour optimiser durant le calcul de chemin DOIT avoir le fanion B à zéro et le fanion C établi à la valeur appropriée. Quand le calcul de chemin se rapporte à la réoptimisation d'un LSP TE existant (auquel cas, le fanion R de l'objet RP est établi) une mise en œuvre PEUT décider de régler le champ Valeur de métrique à la valeur calculée de la métrique du LSP TE à réoptimiser à l'égard du type spécifique de métrique.

Un objet METRIC utilisé pour refléter une limite DOIT avoir le fanion B établi, et le fanion C et le champ Valeur de métrique réglés aux valeurs appropriées.

Dans un message PCRep, sauf si ce n'est pas permis par la politique du PCE, au moins un objet METRIC DOIT être présent qui rapporte la métrique du chemin calculé si le fanion C de l'objet METRIC était établi dans la demande de calcul de chemin correspondante (le fanion B DOIT être à zéro). Le fanion C n'a pas de signification dans un message PCRep. Facultativement, le message PCRep PEUT contenir des objets METRIC supplémentaires qui correspondent à des contraintes de limites ; dans ce cas, la valeur de métrique DOIT être égale à la métrique de chemin calculée correspondante (le fanion B DOIT être établi). Si aucun chemin satisfaisant les contraintes n'a pu être trouvé par le PCE, les objets METRIC PEUVENT aussi être présents dans le message PCRep avec l'objet NO-PATH pour indiquer les contraintes de métrique qui pourraient être satisfaites.

Exemple : si un PCC envoie une demande de calcul de chemin à un PCE où la métrique pour optimiser est la métrique IGP et que la métrique TE ne doit pas excéder la valeur de M, deux objets METRIC sont insérés dans le message PCReq :

- Premier objet METRIC avec B=0, T=1, C=1, valeur de métrique =0x0000

- Second objet METRIC avec B=1, T=2, valeur de métrique =M

Si un chemin satisfait l'ensemble de contraintes peut être trouvé par le PCE et si il n'y a pas de politique qui empêche le retour de la métrique calculée, le PCE insère un objet METRIC avec B=0, T=1, valeur de métrique = coût du chemin IGP calculé. De plus, le PCE peut insérer un second objet METRIC avec B=1, T=2, valeur de métrique = coût du chemin TE calculé.

7.9 Objet Explicit Route

L'objet Chemin explicite (ERO, *Explicit Route Object*) est utilisé pour coder le chemin d'un LSP TE à travers le réseau. Le ERO est porté dans un message PCRep pour fournir le LSP TE calculé si le calcul de chemin a réussi.

Le contenu de cet objet est identique au codage du contenu de l'objet Chemin explicite (ERO) des extensions d'ingénierie de trafic du protocole de réservation de ressources (RSVP-TE, *Resource Reservation Protocol Traffic Engineering*) définies dans les [RFC3209], [RFC3473], et [RFC3477]. C'est-à-dire, l'objet est construit à partir d'une série de sous objets. Tout sous objet ERO RSVP-TE déjà défini ou qui pourrait être défini à l'avenir pour l'usage de l'ERO RSVP-TE est acceptable dans cet objet.

Les types de sous objet ERO PCEP correspondent aux types de sous objet ERO de RSVP-TE.

Comme le chemin explicite est disponible pour la signalisation immédiate par le plan de contrôle MPLS ou GMPLS, la signification de tous les sous objets et champs dans cet objet est identique à celle définie pour l'ERO.

La classe d'objet ERO est 7.

Le type d'objet ERO est 1.

7.10 Objet Reported Route

L'objet Chemin rapporté (RRO, *Reported Route Object*) est exclusivement porté dans un message PCReq afin de rapporter le chemin suivi par un LSP TE pour lequel une réoptimisation est désirée.

Le codage du contenu de cet objet est identique à celui du contenu de l'objet "Route Record Object" défini dans les [RFC3209], [RFC3473], et [RFC3477]. C'est-à-dire, l'objet est construit à partir d'une série de sous objets. Tout sous objet RRO RSVP-TE déjà défini ou qui pourrait être défini à l'avenir pour l'usage de RRO RSVP-TE est acceptable dans cet objet.

La signification de tous les sous objets et champs dans cet objet est identique à celle définie pour le RRO RSVP-TE.

Les types de sous objet RRO PCEP correspondent aux types de sous objet RRO RSVP-TE.

La classe d'objet de RRO est 8.

Le type d' objet RRO est 1.

7.11 Objet LSPA

L'objet LSPA *(LSP Attributes)* est facultatif et spécifie les divers attributs LSP TE à prendre en compte par le PCE durant le calcul de chemin. L'objet LSPA peut être porté dans un message PCReq, ou un message PCRep en cas d'échec de calcul de chemin (dans ce cas, le message PCRep contient aussi un objet NO-PATH, et l'objet LSPA est utilisé pour indiquer l'ensemble de contraintes qui n'ont pas pu être satisfaites). La plupart des champs de l'objet LSPA sont identiques aux champs de l'objet SESSION-ATTRIBUTE (C-Type = 7) défini dans les [RFC3209] et [RFC4090]. Quand il est absent du message PCReq, cela signifie que les priorités d'établissement et de garde sont égales à 0, et qu'il n'y a pas de contraintes d'affinité. Voir au paragraphe 4.7.4 de la [RFC3209] la description détaillée de l'utilisation des affinités de ressource.

La classe d'objet de LSPA est 9.

Le type d'objet de LSPA est 1.

Le format du corps de l'objet LSPA est :

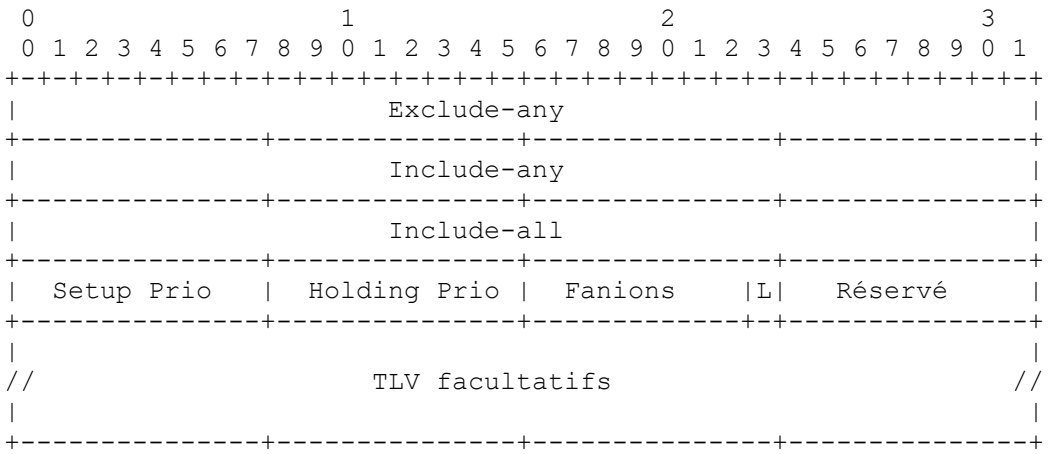


Figure 16 : Format de corps d'objet LSPA

Setup Prio (Priorité d'établissement) (8 bits) : priorité du LSP TE à l'égard de la prise des ressources, dans la gamme de 0 à 7. La valeur 0 est la plus forte priorité. La priorité d'établissement est utilisée pour décider si cette session peut préempter une autre session.

Holding Prio (Priorité de garde) (8 bits) : priorité du LSP TE à l'égard de la conservation des ressources, dans la gamme de 0 à 7. La valeur 0 est la plus forte priorité. La priorité de garde est utilisée pour décider si la session peut être préemptée par une autre session.

Fanions (8 bits)

Fanion L : correspond au bit "Protection locale désirée" ([RFC3209]) de l'objet SESSION-ATTRIBUTE. Quand il est établi, cela signifie que le chemin calculé doit inclure des liaisons protégées avec Fast Reroute comme défini dans la [RFC4090].

Les fanions non alloués DOIVENT être réglés à zéro à l'émission et DOIVENT être ignorés à réception.

Réservé (8 bits) : ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Noter que des TLV facultatifs pourront être définis à l'avenir pour porter des attributs LSP TE en supplément de ceux définis dans la [RFC5420].

7.12 Objet Include Route

L'objet Chemin à inclure (IRO, *Include Route Object*) est facultatif et peut être utilisé pour spécifier que le chemin calculé DOIT traverser un ensemble d'éléments de réseau spécifiés. Le IRO PEUT être porté dans les messages PCReq et PCRep. Quand il est porté dans un message PCRep avec l'objet NO-PATH, le IRO indique l'ensemble d'éléments qui causent l'échec du PCE à trouver un chemin.

La classe d'objet IRO est 10.

Le type d'objet IRO est 1.

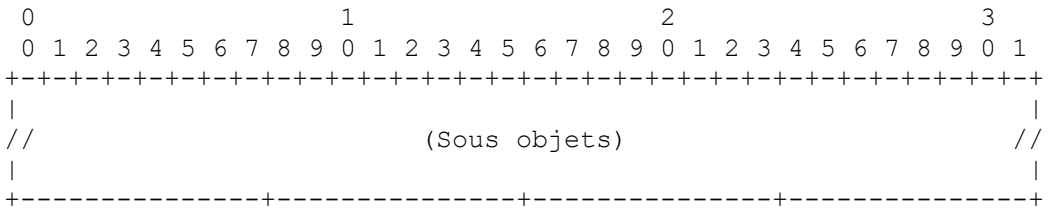


Figure 17 : Format de corps d'objet IRO

Sous objets : le IRO est constitué de sous objets identiques à ceux définis dans les [RFC3209], [RFC3473], et [RFC3477], où le type de sous objet IRO est identique à celui défini dans ces documents.

Les types de sous objet suivants sont pris en charge.

Type	Sous objet
1	préfixe IPv4
2	préfixe IPv6
4	identifiant d'interface non numérotée
32	numéro de système autonome

Le bit L de ces sous objet n'a pas de signification dans un IRO.

7.13 Objet SVEC

7.13.1 Notion de demandes de calcul de chemin dépendant et synchronisé

Demandes de calcul de chemin indépendantes ou dépendantes : les demandes de calcul de chemin sont dites être indépendantes si elles sont sans relation les unes avec les autres. À l'inverse, un ensemble de demandes de calcul de chemin dépendantes est tel que leur calcul ne peut pas être effectué indépendamment de celui de chaque autre (un exemple typique de demandes dépendantes est le calcul d'un ensemble de chemins divers).

Demandes de calcul de chemin synchronisées ou non synchronisées : un ensemble de demandes de calcul de chemin est dit être non synchronisé si leurs traitements respectifs (calculs de chemin) peuvent être effectués par un PCE à la suite et de façon indépendante.

Il y a diverses circonstances où la synchronisation d'un ensemble de calculs de chemin peut être bénéfique ou exigée.

Considérons le cas d'un ensemble de N LSP TE pour lequel un PCC a besoin d'envoyer des demandes de calcul de chemin à un PCE. La première solution consiste en l'envoi de N messages PCReq séparés au PCE choisi. Dans ce cas, les demandes de calcul de chemin sont non synchronisées. Noter que le PCC peut choisir de répartir l'ensemble des N demandes à travers les K PCE pour les besoins d'équilibrage de charge. Considérant que M (M < N) demandes sont envoyées à un PCEi particulier, comme décrit ci-dessus, tel que M demandes puissent être envoyées sous la forme de messages PCReq successifs destinés à PCEi ou groupées dans un seul message PCReq (parce que PCEP permet le groupement de plusieurs demandes de calcul de chemin au sein d'un seul message PCReq). Ceci dit, même dans le cas de demandes indépendantes, il peut être désirable de demander au PCE le calcul de leurs chemins de façon synchronisée qui est susceptible de conduire à des calculs de chemin plus optimaux et/ou de réduire la probabilité de blocage si le PCE est sans état. En d'autres termes, le PCE ne devrait pas calculer les chemins correspondants de manière sérielle et indépendante, mais devrait plutôt calculer "simultanément" leurs chemins. Par exemple, en essayant de calculer "simultanément" les chemins de M LSP TE, on peut permettre au PCE d'améliorer la probabilité de satisfaire plusieurs contraintes.

Considérons le cas de deux LSP TE qui demandent respectivement N1 Mbit/s et N2 Mbit/s, et un délai maximum tolérable de bout en bout pour chaque LSP TE de X ms. Il peut y avoir des circonstances où le calcul du premier LSP TE, sans tenir compte du second LSP TE, peut conduire à l'impossibilité de satisfaire la contrainte de délai pour le second LSP TE.

Un second exemple se rapporte à la contrainte de bande passante. Il est assez facile de donner des exemples où une approche de calculs de chemin en série indépendants va conduire à l'impossibilité de satisfaire les deux demandes (du fait de la fragmentation de bande passante) alors qu'un calcul de chemin synchronisé réussirait à satisfaire les deux demandes.

Un dernier exemple se rapporte à la capacité d'éviter l'allocation de la même ressource à plusieurs demandes, aidant donc à réduire les probabilités d'échec de l'établissement d'appel comparé au calcul en série de demandes indépendantes.

Les calculs de chemin dépendants sont généralement synchronisés. Par exemple, dans le cas du calcul de M chemins divers, si ces chemins sont calculés de façon non synchronisée, cela augmente sérieusement la probabilité de ne pas être capable de satisfaire toutes les demandes (parfois aussi appelé le "problème de la trappe" bien connu).

De plus, cela ne permettrait pas à un PCE de mettre en œuvre des fonctions objectives comme d'essayer de minimiser la somme des coûts de LSP TE. Dans ce cas, les demandes de calcul de chemin doivent être synchronisées: elles ne peuvent pas être calculées indépendamment les unes des autres.

À l'inverse, un ensemble de demandes de calcul de chemin indépendantes peuvent ou non être synchronisées.

La synchronisation d'un ensemble de demandes de calcul de chemin est réalisée en essayant d'utiliser l'objet SVEC qui spécifie la liste des demandes synchronisées qui peuvent être dépendantes ou indépendantes.

PCEP rend en charge les trois modes suivants :
- o Grouper un ensemble de demandes de calcul de chemin indépendantes et non synchronisées,
- o Grouper un ensemble de demandes de calcul de chemin indépendantes et synchronisées (exige l'objet SVEC défini ci-dessous),
- o Grouper un ensemble de demandes de calcul de chemin dépendantes et synchronisées (exige l'objet SVEC défini ci-dessous).

7.13.2 Objet SVEC

Le paragraphe 7.13.1 détaille les circonstances dans lesquelles il peut être souhaitable et/ou exigé de synchroniser un ensemble de demandes de calcul de chemin. L'objet Vecteur de synchronisation (SVEC, *Synchronization VECtor*) permet à un PCC de demander la synchronisation d'un ensemble de demandes de calcul de chemin dépendantes ou indépendantes. L'objet SVEC est facultatif et peut être porté dans un message PCReq.

Le but de l'objet SVEC porté dans un message PCReq est de demander la synchronisation de M demandes de calcul de chemin. L'objet SVEC est un objet de longueur variable qui fait la liste de l'ensemble de M demandes de calcul de chemin qui doivent être synchronisées. Chaque demande de calcul de chemin est identifiée de façon univoque par le numéro d'identifiant de demande porté dans les objets RP respectifs. L'objet SVEC contient aussi un ensemble de fanions qui spécifient le type de synchronisation.

La classe d'objet SVEC est 11.
Le type d'objet SVEC est 1.
Le format du corps d'objet SVEC est comme suit :

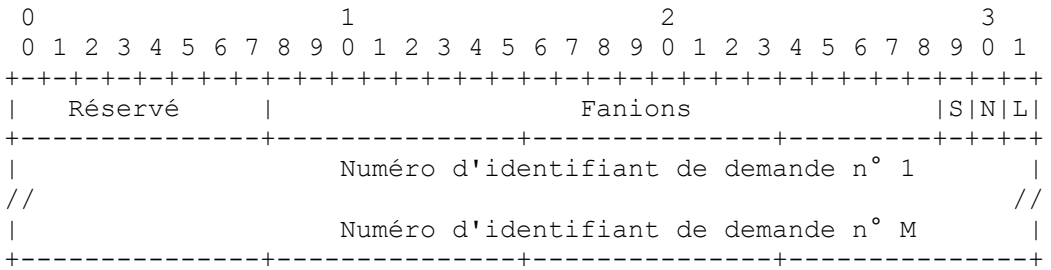


Figure 18 : Format de corps d'objet SVEC

Réservé (8 bits) : ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Fanions (24 bits) : Définit la dépendance potentielle entre l'ensemble de demandes de calcul de chemin.

* Bit L (Liaisons diverses) : quand il est établi, cela indique que les chemins calculés correspondants aux demandes spécifiées par les objets RP suivants NE DOIVENT PAS avoir de liaisons en commun.

* Bit N (Nœuds divers) : quand il est établi, cela indique que les chemins calculés correspondants aux demandes spécifiées par les objets RP suivants NE DOIVENT PAS avoir de nœud en commun.

* Bit S (SRLG divers) : quand il est établi, cela indique que les chemins calculés correspondants aux demandes spécifiées par les objets RP suivants NE DOIVENT PAS partager de groupe de liaisons à risques partagés (SRLG, *Shared Risk Link Group*).

Dans le cas d'un ensemble de M demandes de calcul de chemin synchronisées indépendantes, les bits L, N, et S sont à zéro.

Les fanions non alloués DOIVENT être réglés à zéro à l'émission et DOIVENT être ignorés à réception.

Les fanions définis ci-dessus ne sont pas exclusifs.

7.13.3 Traitement de l'objet SVEC

L'objet SVEC permet à un PCC de spécifier une liste de M demandes de calcul de chemin qui DOIVENT être synchronisées avec une potentielle dépendance. L'ensemble de M demandes de calcul de chemin peut être envoyé dans un seul message PCReq ou plusieurs messages PCReq. Dans ce dernier cas, il est RECOMMANDÉ que le PCE mette en œuvre un temporisateur local (appelé SyncTimer) activé par la réception du premier message PCReq qui contient l'objet SVEC après l'expiration duquel, si toutes les M demandes de calcul de chemin n'ont pas été reçues, une erreur de protocole est déclenchée. Quand un PCE reçoit une demande de calcul de chemin qui ne peut pas être satisfaite (par exemple, parce que le message PCReq contient un objet avec le bit P établi qui n'est pas supporté) le PCE envoie un message PCErr pour cette demande (voir le paragraphe 7.2) le PCE DOIT annuler l'ensemble entier de demandes de calcul de chemin et DOIT envoyer un message PCErr avec le type d'erreur "Demande de calcul de chemin synchronisée manquante".

Noter que de tels messages PCReq peuvent aussi contenir des demandes de calcul de chemin non synchronisées. Par exemple, le message PCReq peut comporter N demandes de calcul de chemin synchronisées qui sont relatives à RP 1, ..., RP N et sont mentionnées dans l'objet SVEC avec toutes autres demandes de calcul de chemin qui sont traitées normalement.

7.14 Objet NOTIFICATION

L'objet NOTIFICATION est exclusivement porté dans un message PCNtf et peut soit être utilisé dans un message envoyé par un PCC à un PCE, soit par un PCE à un PCC afin de notifier un événement.

La classe d'objet NOTIFICATION est 12.

Le type d'objet NOTIFICATION est 1.

Le format du corps d'objet NOTIFICATION est comme suit :

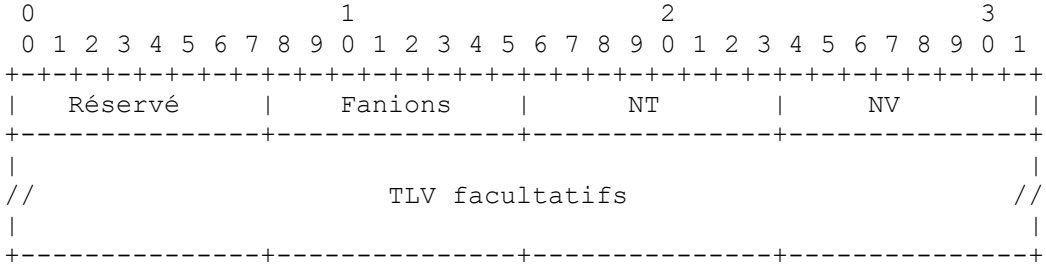


Figure 19 : Format de corps d'objet NOTIFICATION

Réservé (8 bits) : ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Fanions (8 bits) : aucun fanion n'est actuellement défini. Les fanions non alloués DOIVENT être réglés à zéro à l'émission et DOIVENT être ignorés à réception.

NT (Type de notification) (8 bits) : le type de notification spécifie la classe de la notification.

NV (Valeur de notification) (8 bits) : la valeur de notification donne des informations supplémentaires relatives à la nature de la notification.

Le type de notification et la valeur de notification sont tous deux gérés par l'IANA.

Les valeurs suivantes de type de notification et de valeur de notification sont actuellement définies :

- Type de notification = 1 : demande en cours annulée

  * Valeur de notification = 1 : le PCC annule un ensemble de demandes en instance. Un type de notification = 1, valeur de notification = 1 indique que le PCC veut informer un PCE de l'annulation d'un ensemble de demandes en instance. Un tel événement pourrait être déclenché à cause de conditions externes comme la réception d'une réponse positive provenant d'un autre PCE (si le PCC avait envoyé plusieurs demandes à un ensemble de PCE pour la même demande de calcul de chemin) un événement de réseau comme un échec qui rend la demande obsolète, ou tout autre événement local pour le PCC. Un objet NOTIFICATION avec le type de notification = 1, valeur de notification = 1 est porté dans un message PCNtf envoyé par le PCC au PCE. L'objet RP correspondant à la demande annulée DOIT aussi être présent dans le message PCNtf. Plusieurs objets RP peuvent être portés dans le message PCNtf ; dans ce cas, la notification s'applique à tous. Si une telle notification est reçue par un PCC en provenance d'un PCE, le PCC DOIT ignorer en silence la notification et aucune erreur ne devrait être générée.

  * Valeur de notification = 2 : le PCE annule un ensemble de demandes en instance. Un type de notification = 1, valeur de notification = 2 indique que le PCE veut informer un PCC de l'annulation d'un ensemble de demandes en instance. Un objet NOTIFICATION avec le type de notification = 1, valeur de notification = 2 est porté dans un message PCNtf envoyé par un PCE à un PCC. L'objet RP correspondant à la demande annulée DOIT aussi être présent dans le message PCNtf. Plusieurs objets RP peuvent être portés dans le message PCNtf ; dans ce cas, la notification s'applique à tous. Si une telle notification est reçue par un PCE provenant d'un PCC, le PCE DOIT ignorer en silence la notification et aucune erreur ne devrait être générée.

- Type de notification = 2 : PCE surchargé

  * Valeur de notification = 1 : un Type de notification = 2, Valeur de notification = 1 indique au PCC que le PCE est actuellement dans un état de surcharge. Si aucun objet RP n'est inclus dans le message PCNtf, cela indique qu'aucune autre demande ne DEVRAIT être envoyée à ce PCE jusqu'à ce que l'état de surcharge soit terminé : les demandes en instance ne sont pas affectées et vont être servies. Si des demandes en instance ne peuvent pas être servies du fait de l'état de surcharge, le PCE DOIT aussi inclure un ensemble d'objets RP qui identifient l'ensemble de demandes en instance annulées par le PCE et ne seront pas honorées. Dans ce cas, le PCE n'a pas à envoyer de message PCNtf supplémentaire avec le type de notification = 1 et la valeur de notification = 2 car la liste des demandes annulées est spécifiée par l'inclusion de l'ensemble correspondant d'objets RP. Si une telle notification est reçue d'un PCC par un PCE, le PCE DOIT ignorer en silence la notification et aucune erreur ne devrait être générée.

  * Une mise en œuvre de PCE DEVRAIT utiliser un mécanisme à double seuil utilisé pour déterminer si il est dans un état d'encombrement à l'égard de la surveillance de ressources spécifiques (par exemple de CPU, de mémoire). L'utilisation de tels seuils est pour éviter des oscillations entre l'état surchargé/non surchargé qui peut résulter en oscillations de cibles de demande par les PCC.

  * Facultativement, un TLV nommé OVERLOADED-DURATION peut être inclus dans l'objet NOTIFICATION qui spécifie la période durant laquelle aucune autre demande ne devrait être envoyée au PCE. Une fois cette période écoulée, le PCE ne devrait plus être considéré comme étant dans l'état encombré.

    Le TLV OVERLOADED-DURATION est conforme au format de TLV PCEP défini au paragraphe 7.1 et est composé de 2 octets pour le type, 2 octets spécifiant la longueur du TLV (longueur de la portion Valeur en octets) suivi par un champ de valeur de longueur d'un champ de fanions de 32 bits.

Type : 2
Longueur : 4 octets
Valeur : champ de fanions de 32 bits qui indique la durée estimée d'encombrement du PCE en secondes.

* Valeur de notification = 2 : un type de notification = 2, valeur de notification = 2 indique que le PCE n'est plus dans l'état surchargé et est disponible pour traiter de nouvelles demandes de calcul de chemin. Une mise en œuvre DEVRAIT s'assurer qu'un PCE envoie une telle notification à chaque PCC auquel un message Notification (avec le type de notification = 2, valeur de notification = 1) a été envoyé sauf si un TLV OVERLOADED-DURATION avait été inclus dans le message correspondant et si le PCE souhaite attendre l'expiration de cette période avant de recevoir de nouvelles demandes. Si une telle notification est reçue par un PCE d'un PCC, le PCE DOIT ignorer en silence la notification et aucune erreur ne devrait être générée. Il est RECOMMANDÉ de prendre en charge une procédure d'amortissement de notification sur le PCE afin d'éviter de trop fréquentes notifications d'état d'encombrement et de sortie d'état d'encombrement. Par exemple, une mise en œuvre pourrait utiliser une approche d'hystérèse avec un mécanisme de double seuil qui déclenche l'envoi des notifications d'état d'encombrement. De plus, en cas de forte instabilité des ressources du PCE, un mécanisme supplémentaire d'amortissement DEVRAIT être utilisé (linéaire ou exponentiel) pour réguler la fréquence de notification et éviter des oscillations des demandes de calcul de chemin.

Quand un PCC reçoit une indication de surcharge de la part d'un PCE, il devrait considérer l'impact sur le réseau entier. On doit se souvenir que d'autres PCC peuvent aussi recevoir la notification, et donc de nombreuses demandes de calcul de chemin pourraient être redirigées sur d'autres PCE. Cela peut, à son tour, causer plus de surcharge sur les PCE dans le réseau. Donc, une application à un PCC recevant une notification de surcharge devrait envisager d'appliquer une forme de retard (par exemple, exponentiel) au taux auquel elle génère les demandes de calcul de chemin dans le réseau. Ceci est particulièrement le cas lorsque le nombre de PCE rapportant des surcharges augmente.

7.15 Objet PCEP-ERROR

L'objet PCEP-ERROR est exclusivement porté dans un message PCErr pour notifier une erreur de PCEP.

La classe d'objet PCEP-ERROR est 13.

Le type d'objet PCEP-ERROR est 1.

Le format du corps d'objet PCEP-ERROR est comme suit :

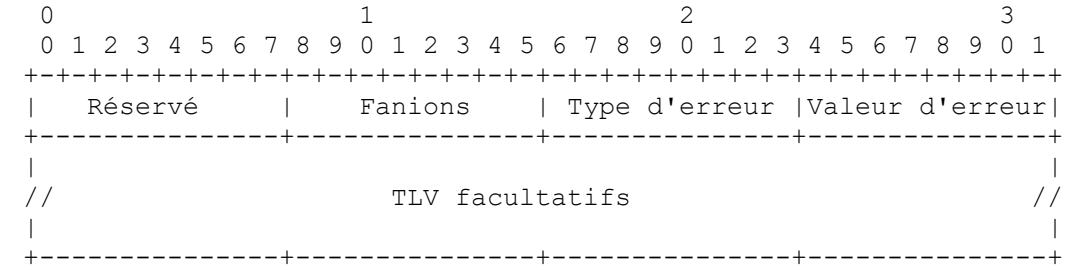


Figure 20 : Format de corps d'objet PCEP-ERROR

Un objet PCEP-ERROR est utilisé pour rapporter une erreur de PCEP et est caractérisé par un type d'erreur qui spécifie le type de l'erreur et une valeur d'erreur qui fournit des informations supplémentaires sur le type d'erreur. Le type d'erreur et la valeur d'erreur sont tous deux gérés par l'IANA (voir la section de considérations relatives à l'IANA).

Réservé (8 bits) : ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Fanions (8 bits) : aucun fanion n'est actuellement défini. Ce champ de fanions DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Type d'erreur (8 bits) : définit la classe de l'erreur.

Valeur d'erreur (8 bits) : fournit des détails supplémentaires sur l'erreur.

Facultativement, l'objet PCEP-ERROR peut contenir des TLV supplémentaires afin de fournir des informations supplémentaires sur l'erreur rencontrée.

Un seul message PCErr peut contenir plusieurs objets PCEP-ERROR.

Pour chaque erreur PCEP, un Type d'erreur et une valeur d'erreur sont définis.

Type d'erreur	Signification
1	Échec d'établissement de session PCEP valeur d'erreur = 1 : réception d'un message Open invalide ou d'un message non Open. valeur d'erreur = 2 : aucun message Open reçu avant l'expiration du temporisateur OpenWait. valeur d'erreur = 3 : caractéristiques de session inacceptables et non négociables. valeur d'erreur = 4 : caractéristiques de session inacceptables mais négociables. valeur d'erreur = 5 : réception d'un second message Open avec des caractéristiques de session encore inacceptables valeur d'erreur = 6 : réception d'un message PCErr proposant des caractéristiques de session inacceptables valeur d'erreur = 7 : pas de message Keepalive ou PCErr reçu avant l'expiration du temporisateur KeepWait
2	Capacité non prise en charge
3	Objet inconnu valeur d'erreur = 1 : classe d'objet non reconnue valeur d'erreur = 2 : type d'objet non reconnu
4	Objet non pris en charge valeur d'erreur = 1 : classe d'objet non prise en charge valeur d'erreur = 2 : type d'objet non pris en charge
5	Violation de politique valeur d'erreur = 1 : bit C de l'objet METRIC établi (demande rejetée) valeur d'erreur = 2 : bit O de l'objet RP établi (demande rejetée)
6	Objet obligatoire manquant valeur d'erreur = 1 : objet RP manquant valeur d'erreur = 2 : objet RRO manquant pour une demande de réoptimisation (bit R de l'objet RP établi) quand la bande passante n'est pas égale à 0. valeur d'erreur = 3 : objet END-POINTS manquant
7	Demande de calcul de chemin synchronisée manquante
8	Référence de demande inconnue
9	Tentative d'établir une seconde session PCEP
10	Réception d'un objet invalide valeur d'erreur = 1 : réception d'un objet avec le fanion P non établi alors que le fanion P doit être établi conformément à la présente spécification.

Les types d'erreur mentionnés ci-dessus sont décrits ci-dessous :

Type d'erreur = 1 : échec d'établissement de session PCEP.

Si un message mal formé est reçu, l'homologue PCEP receveur DOIT envoyer un message PCErr avec le type d'erreur = 1, valeur d'erreur = 1.

Si aucun message Open n'est reçu avant l'expiration du temporisateur OpenWait, l'homologue PCEP receveur DOIT envoyer un message PCErr avec le type d'erreur = 1, valeur d'erreur = 2 (voir les détails à l'Appendice A).

Si une ou plusieurs caractéristiques de session PCEP sont inacceptables par l'homologue receveur et sont non négociables, il DOIT envoyer un message PCErr avec le type d'erreur = 1, valeur d'erreur = 3.

Si un message Open est reçu avec des caractéristiques de session inacceptables mais si ces caractéristiques sont négociables, l'homologue receveur PCEP DOIT envoyer un message PCErr avec le type d'erreur = 1, valeur d'erreur = 4 (voir le paragraphe 6.2 pour les détails).

Si un second message Open est reçu durant la phase d'établissement de session PCEP et si les caractéristiques de session sont encore inacceptables, l'homologue receveur PCEP DOIT envoyer un message PCErr avec le type d'erreur = 1, valeur d'erreur = 5 (voir le paragraphe 6.2 pour les détails).

Si un message PCErr est reçu durant la phase d'établissement de session PCEP et si il contient un message Open proposant des caractéristiques de session inacceptables, l'homologue receveur PCEP DOIT envoyer un message PCErr avec le type d'erreur = 1, valeur d'erreur = 6.

Si ni un message Keepalive ni un message PCErr n'est reçu avant l'expiration du temporisateur KeepWait durant la phase d'établissement de session PCEP, l'homologue receveur PCEP DOIT envoyer un message PCErr avec le type d'erreur = 1, valeur d'erreur = 7.

Type d'erreur = 2 : le PCE indique que la demande de calcul de chemin ne peut pas être honorée parce qu'il ne prend pas en charge une ou plusieurs des capacités requises. La demande de calcul de chemin correspondante DOIT être annulée.

Type d'erreur = 3 ou type d'erreur = 4 : si un message PCEP est reçu qui porte un objet PCEP (avec le fanion P établi) non reconnu par le PCE ou reconnu mais non pris en charge, alors le PCE DOIT envoyer un message PCErr avec un objet PCEP-ERROR (type d'erreur = 3 et 4, respectivement). De plus, le PCE PEUT inclure dans le message PCErr l'objet inconnu ou non pris en charge. La demande de calcul de chemin correspondante DOIT être annulée par le PCE sans autre notification.

Type d'erreur = 5 : si une demande de calcul de chemin est reçue qui n'est pas conforme à une politique acceptée entre le PCC et le PCE, le PCE DOIT envoyer un message PCErr avec un objet PCEP-ERROR (type d'erreur = 5). Le calcul de chemin correspondant DOIT être annulé. Des TLV spécifiques de la politique portés dans l'objet PCEP-ERROR peuvent être définis dans d'autres documents pour spécifier la nature de la violation de politique.

Type d'erreur = 6 : si une demande de calcul de chemin est reçue qui ne contient pas un objet obligatoire, le PCE DOIT envoyer un message PCErr avec un objet PCEP-ERROR (type d'erreur = 6). Si plusieurs objets obligatoires manquent, le message PCErr DOIT contenir un objet PCEP-ERROR par objet manquant. Le calcul de chemin correspondant DOIT être annulé.

Type d'erreur = 7 : si un PCC envoie une demande de calcul de chemin synchronisée à un PCE et si le PCE ne reçoit pas toutes les demandes de calcul de chemin synchronisées mentionnées dans l'objet SVEC correspondant après l'expiration du temporisateur SyncTimer défini au paragraphe 7.13.3, le PCE DOIT envoyer un message PCErr avec un objet PCEP-ERROR (type d'erreur = 7). Le calcul de chemin synchronisé correspondant DOIT être annulé. Il est RECOMMANDÉ que le PCE inclue les TLV REQ-MISSING (défini ci-dessous) qui identifient les demandes manquantes.

Le TLV REQ-MISSING est conforme au format de TLV PCEP défini au paragraphe 7.1 et est composé de 2 octets pour le type, 2 octets spécifiant la longueur du TLV (longueur de la portion Valeur en octets) suivis par un champ de Valeur de longueur fixe de 4 octets.

Type : 3
Longueur : 4 octets
Valeur : 4 octets qui indiquent le numéro d'identifiant de demande qui correspond à la demande manquante.

Type d'erreur = 8 : si un PCC reçoit un message PCRep relatif à une demande de calcul de chemin inconnue, le PCC DOIT envoyer un message PCErr avec un objet PCEP-ERROR (type d'erreur = 8). De plus, le PCC DOIT inclure dans le message PCErr l'objet RP inconnu.

Type d'erreur = 9 : si un homologue PCEP détecte une tentative d'un autre homologue PCEP d'établir une seconde session PCEP, il DOIT envoyer un message PCErr avec le type d'erreur = 9, valeur d'erreur = 1. La session PCEP existante DOIT être préservée et tous les messages suivants relatifs à la tentative d'établissement de la seconde session PCEP DOIVENT être ignorés en silence.

Type d'erreur = 10 : si un homologue PCEP reçoit un objet avec le fanion P non établi bien que le fanion P doive être établi selon la présente spécification, il DOIT envoyer un message PCErr avec le type d'erreur = 10, valeur d'erreur = 1.

7.16 Objet LOAD-BALANCING

Il y a des situations où aucun LSP TE avec une bande passante de X ne pourrait être trouvé par un PCE bien qu'une telle exigence de bande passante pourrait être satisfaite par un ensemble de LSP TE tel que la somme de leurs bandes passantes soit égale à X. Donc, il pourrait être utile pour un PCC de demander un ensemble de LSP TE tel que la somme de leurs bandes passantes soit égale à X Mbit/s, avec des contraintes potentielles sur le nombre de LSP TE et le minimum de bande

passante de chacun de ces LSP TE. Une telle demande est faite en insérant un objet LOAD-BALANCING dans un message PCReq envoyé à un PCE.

L'objet LOAD-BALANCING est facultatif.

La classe d'objet LOAD-BALANCING est 14.

Le type d'objet LOAD-BALANCING est 1.

Le format du corps d'objet LOAD-BALANCING est comme suit :

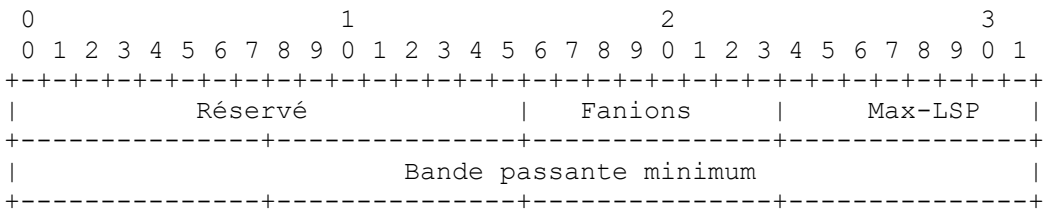


Figure 21 : Format de corps d'objet LOAD-BALANCING

Réservé (16 bits) : ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Fanions (8 bits) : aucun fanion n'est actuellement défini. Le champ Fanions DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Max-LSP (8 bits) : nombre maximum de LSP TE dans l'ensemble.

Bande passante minimum (32 bits) : spécifie le minimum de bande passante de chaque élément de l'ensemble de LSP TE. La bande passante est codée dans un format de virgule flottante de l'IEEE (voir [IEEE.754]) de 32 bits, exprimé en octets par seconde.

Le corps d'objet LOAD-BALANCING a une longueur fixe de 8 octets.

Si un PCC demande le calcul d'un ensemble de LSP TE tel que la somme de leurs bandes passantes soit X, le nombre maximum de LSP TE est N, et chaque LSP TE doit avoir au moins une bande passante de B, il insère un objet BANDWIDTH spécifiant X comme la bande passante requise et un objet LOAD-BALANCING avec les champs Max-LSP et Bande passante minimum réglés respectivement à N et B.

7.17 Objet CLOSE

L'objet CLOSE DOIT être présent dans chaque message Close. Il DOIT y avoir seulement un objet CLOSE par message Close. Si un message Close est reçu contenant plus d'un objet CLOSE, le premier objet CLOSE est celui qui doit être traité. Les autres objets CLOSE DOIVENT être ignorés en silence.

La classe d'objet CLOSE est 15.
Le type d'objet CLOSE est 1.
Le format du corps de l'objet CLOSE est comme suit :

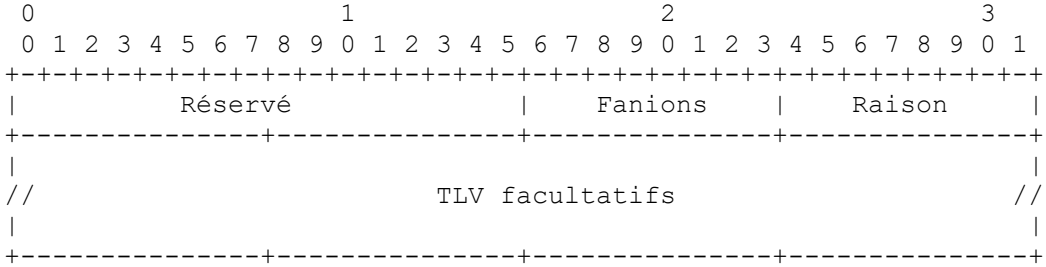


Figure 22 : Format d'objet CLOSE

Réservé (16 bits) : ce champ DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Fanions (8 bits) : aucun fanion n'est actuellement défini. Le champ Fanions DOIT être réglé à zéro à l'émission et DOIT être ignoré à réception.

Raison (8 bits) : spécifie la raison de la clôture de la session PCEP. L'établissement de ce champ est facultatif. L'IANA gère l'espace de codes du champ Raison. Les valeurs suivantes sont actuellement définies :

Valeur de raisons	Signification
1	Aucune explication fournie
2	DeadTimer expiré
3	Réception d'un message PCEP mal formé
4	Réception d'un nombre inacceptable de demandes/réponses inconnues
5	Réception d'un nombre inacceptable de messages PCEP inconnus

Des TLV facultatifs peuvent être inclus dans un corps d'objet CLOSE. La spécification de ces TLV sort du domaine d'application du présent document.

8. Considérations de gestion

Cette section suit les lignes directrices de la [RFC6123].

8.1 Contrôle de fonction et de politique

Une mise en œuvre de PCEP DEVRAIT permettre de configurer les paramètres de session PCEP suivants sur la mise en œuvre :

- les Keepalive et DeadTimer locaux (c'est-à-dire, les paramètres envoyés par l'homologue PCEP dans un message Open),
- les Keepalive et DeadTimer maximum acceptables distants (c'est-à-dire, les paramètres reçus d'un homologue dans un message Open),
- si la négociation est activée ou désactivée,
- si la négociation est permise, les temporisateurs Keepalive et DeadTimer minimum acceptables reçus d'un homologue PCEP,
- le SyncTimer,
- le nombre maximum de sessions qui peuvent être établies,
- le temporisateur de demande, la durée pendant laquelle un PCC attend un réponse avant de renvoyer ses demandes de calcul de chemin (potentiellement à un autre PCE),
- les MAX-UNKNOWN-REQUESTS,
- les MAX-UNKNOWN-MESSAGES.

Ces paramètres peuvent être configurés comme paramètres par défaut pour toute session PCEP à laquelle participe le locuteur PCEP, ou qu'il peut appliquer à une session spécifique avec un certain homologue PCEP ou à un groupe spécifique de sessions avec un groupe spécifique d'homologues PCEP. Une mise en œuvre de PCEP DEVRAIT permettre de configurer l'initiation d'une session PCEP avec un sous ensemble choisi de PCE découverts. Noter que le choix de PCE est un problème local de mise en œuvre. Une mise en œuvre de PCEP DEVRAIT permettre de configurer une session PCEP spécifique avec un homologue PCEP. Cela inclut la configuration des paramètres suivants :

- l'adresse IP de l'homologue PCEP,
- le rôle du locuteur PCEP : PCC, PCE, ou les deux,
- si le locuteur PCEP devrait initier la session PCEP ou attendre l'initiation par l'homologue,
- les paramètres de session PCEP, comme énumérés ci-dessus, si ils diffèrent des paramètres par défaut,
- un ensemble de politiques PCEP incluant le type des opérations admises pour l'homologue PCEP (par exemple, calculs de chemin divers, synchronisation, etc.).

Une mise en œuvre de PCEP DOIT permettre de restreindre l'ensemble d'homologues PCEP qui peuvent initier une session PCEP avec le locuteur PCEP (par exemple, la liste des homologues PCEP autorisés, tous les homologues PCEP de la zone, tous les homologues PCEP de l'AS).

8.2 Modèles d'informations et de données

Un module de MIB PCEP est défini dans la [RFC7420] qui décrit les objets gérés pour modéliser une communication PCEP qui inclut :
- o la configuration et l'état du client PCEP,
- o la configuration et informations de l'homologue PCEP,
- o la configuration et informations de la session PCEP,
- o les notifications pour indiquer les changements de session PCEP.

8.3 Détection et surveillance de vie

PCEP inclut un mécanisme de vérification de maintien en vie de l'activité d'un homologue PCEP et une procédure de notification permettant à un PCE d'annoncer son état de surcharge à un PCC. Aussi, des procédures afin de surveiller l''activité et les performances d'une chaîne de PCE donnée (dans le cas d'un calcul de chemin sur plusieurs PCE) sont définies dans la [RFC5886].

8.4 Vérification de fonctionnement correct

La vérification du fonctionnement correct d'une communication PCEP peut être effectuée en surveillant divers paramètres. Une mise en œuvre de PCEP DEVRAIT fournir les paramètres suivants :
- o temps de réponse (minimum, moyen, et maximum) par homologue PCE,
- o les défaillances de session PCEP,
- o La durée pendant laquelle la session a été dans l'état actif,
- o le nombre de messages corrompus,
- o le nombre d'échecs de calcul,
- o le nombre de demandes pour lesquelles aucune réponse n'a été reçue après l'expiration d'un temporisateur configurable et en vérifiant qu'au moins un chemin existe qui satisfait l'ensemble de contraintes.

Une mise en œuvre de PCEP DEVRAIT enregistrer les événements d'erreur (par exemple, messages corrompus, objets non reconnus).

8.5 Exigences sur les autres protocoles et composants fonctionnels

PCEP ne met aucune nouvelle exigence sur d'autres protocoles. Comme PCEP s'appuie sur le protocole de transport TCP, la gestion de PCEP peut utiliser les mécanismes de gestion de TCP (comme la MIB TCP définie dans la [RFC4022]).

Les mécanismes de découverte de PCE ([RFC5088], [RFC5089]) peuvent avoir un impact sur PCEP. Pour éviter qu'une fréquence élevée de découvertes/disparitions de PCE déclenche une fréquence élevée d'établissements/suppressions de sessions PCEP, il est RECOMMANDÉ d'introduire un amortissement pour l'établissement des sessions PCEP.

8.6 Impact sur le fonctionnement du réseau

Afin d'éviter un impact inacceptable sur le fonctionnement du réseau, une mise en œuvre DEVRAIT permettre d'établir une limite au nombre de sessions qui peuvent être établies sur un locuteur PCEP, et PEUT permettre qu'une limite soit placée sur le taux de messages envoyés par un locuteur PCEP et reçus d'un homologue. Elle PEUT aussi permettre d'envoyer une notification quand un seuil de taux est atteint.

9. Considérations relatives à l'IANA

L'IANA alloue les valeurs des paramètres du protocole PCEP (messages, objets, TLV).

L'IANA établi un nouveau registre de niveau supérieur pour contenir tous les codets et sous registres PCEP.

La politique d'allocation pour chaque nouveau registre est par consensus de l'IETF : les nouvelles valeurs sont allouées par le processus de consensus de l'IETF (voir la [RFC5226]). Spécifiquement, de nouvelles allocations sont faites via des RFC approuvées par l'IESG. Normalement, l'IESG va chercher des informations sur les perspectives d'allocations auprès des personnes appropriées (par exemple, un groupe de travail pertinent si il en existe un).

9.1 Accès TCP

PCEP a été enregistré comme accès TCP 4189.

9.2 Messages PCEP

L'IANA a créé un registre pour les messages PCEP. Chaque message PCEP a une valeur de type de message.

Valeur	Signification	Référence
1	Ouvert	RFC 5440
2	Maintien den vie	RFC 5440
3	Demande de calcul de chemin	RFC 5440
4	Réponse de calcul de chemin	RFC 5440
5	Notification	RFC 5440
6	Erreur	RFC 5440
7	Fermé	RFC 5440

9.3 Objet PCEP

L'IANA a créé un registre pour les objets PCEP. Chaque objet PCEP a une classe d'objet et un type d'objet.

Classe d'objet	Nom	Type d'objet	Référence
1	OPEN	1	RFC 5440
2	RP	1	RFC 5440
3	NO-PATH	1	RFC 5440
4	END-POINTS	1 : adresses IPv4 2 : adresses IPv6	RFC 5440
5	BANDWIDTH	1 : Bande passante demandée 2 : Bande passante d'un LSP TE existant pour lequel une réoptimisation est effectuée	RFC 5440
6	METRIC	1	RFC 5440
7	ERO	1	RFC 5440
8	RRO	1	RFC 5440
9	LSPA	1	RFC 5440
10	IRO	1	RFC 5440
11	SVEC	1	RFC 5440
12	NOTIFICATION	1	RFC 5440
13	PCEP-ERROR	1	RFC 5440
14	LOAD-BALANCING	1	RFC 5440
15	CLOSE	1	RFC 5440

9.4 En-tête commun de message PCEP

L'IANA a créé un registre pour gérer le champ Fanions de l'en-tête commun de message PCEP.

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Aucun bit n'est actuellement défini pour l'en-tête commun de message PCEP.

9.5 Champ de fanions d'objet Open

L'IANA a créé un registre pour gérer le champ Fanions de l'objet OPEN.

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Aucun bit n'est actuellement défini pour le champ Fanions d'objet OPEN.

9.6 Objet RP

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Plusieurs bits sont définis pour le champ de fanions de l'objet RP dans le présent document. Les valeurs suivantes ont été allouées :

Espace de codes du champ Fanions (objet RP)

Bit	Description	Référence
26	strict/lâche	RFC 5440
27	bidirectionnel	RFC 5440
28	réoptimisation	RFC 5440
29-31	priorité	RFC 5440

9.7 Champ de fanions de l'objet NO-PATH

L'IANA a créé un registre pour gérer l'espace de codes des champs NI et Fanions de l'objet NO-PATH.

Valeur	Signification	Référence
0	Aucun chemin satisfaisant l'ensemble de contraintes n'a pu être trouvé	RFC 5440
1	Chaîne de PCE rompue	RFC 5440

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Un bit est défini pour le champ de fanions de l'objet NO-PATH dans le présent document:

Espace de codes du champ Fanions (objet NO-PATH)

Bit	Description	Référence
0	Contrainte non satisfaite indiquée	RFC 5440

9.8 Objet METRIC

L'IANA a créé un registre pour gérer l'espace de codes des champs T et Fanions de l'objet METRIC.
Espace de codes du champ T (objet METRIC)

Valeur	Signification	Référence
1	métrique IGP	RFC 5440
2	métrique TE	RFC 5440
3	compte de bonds	RFC 5440

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Plusieurs bits sont définis dans le présent document. Les valeurs suivantes ont été allouées :

Espace de codes du champ Fanions (objet METRIC)

Bit	Description	Référence
6	métrique calculée	RFC 5440
7	lié	RFC 5440

9.9 Champ de fanions de l'objet LSPA

L'IANA a créé un registre pour gérer le champ Fanions de l'objet LSPA.

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Un bit est défini pour le champ Fanions de l'objet LSPA dans le présent document :

Espace de codes du champ Fanions (objet LSPA)

Bit	Description	Référence
7	Protection locale désirée	RFC 5440

9.10 Champ de fanions de l'objet SVEC

L'IANA a créé un registre pour gérer le champ Fanions de l'objet SVEC.
De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Trois bits sont définis pour le champ de fanions de l'objet SVEC dans le présent document :

Espace de codes du champ Fanions (objet SVEC)

Bit	Description	Référence
21	SRLG divers	RFC 5440
22	Nœuds divers	RFC 5440
23	Liaisons diverses	RFC 5440

9.11 Objet NOTIFICATION

L'IANA a créé un registre pour le type de notification et la valeur de notification de l'objet NOTIFICATION et gère l'espace de codes.

Type de notification	Nom	Référence
1	Demande en cours annulée	RFC 5440
	Valeur de notification	
	1 : PCC annule un ensemble de demandes en instance	

	2 : PCE annule un ensemble de demandes en instance	
2	PCE surchargé	RFC 5440
	Valeur de notification	
	1 : PCE en état encombré	
	2 : PCE plus en état encombré	

L'IANA a créé un registre pour gérer le champ Fanions de l'objet NOTIFICATION.

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Aucun bit n'est actuellement alloué pour le champ Fanions de l'objet NOTIFICATION.

9.12 Objet PCEP-ERROR

L'IANA a créé un registre pour le type d'erreur et la valeur d'erreur de l'objet PCEP-ERROR et gère l'espace de codes.

Pour chaque PCEP-ERROR, un type d'erreur et une valeur d'erreur sont définis.

Type d'erreur	**Signification**	**Référence**
1	Échec d'établissement de session PCEP	RFC 5440
	valeur d'erreur = 1 : réception d'un message Open invalide ou d'un message non Open.	
	valeur d'erreur = 2 : pas de message Open reçu avant l'expiration du temporisateur OpenWait	
	valeur d'erreur = 3 : caractéristiques de session inacceptables et non négociables	
	valeur d'erreur = 4 : caractéristiques de session inacceptables mais négociables	
	valeur d'erreur = 5 : réception d'un second message Open avec des caractéristiques de session encore inacceptables	
	valeur d'erreur = 6 : réception d'un message PCErr proposant des caractéristiques de session inacceptables	
	valeur d'erreur = 7 : pas de Keepalive ou message PCErr reçu avant l'expiration du temporisateur KeepWait	
	valeur d'erreur = 8 : version PCEP non prise en charge	
2	Capacité non prise en charge	RFC 5440
3	Objet inconnu	RFC 5440
	valeur d'erreur = 1 : classe d'objet non reconnue	
	valeur d'erreur = 2 : type d'objet non reconnu	
4	Objet non pris en charge	RFC 5440
	valeur d'erreur = 1 : classe d'objet non prise en charge	
	valeur d'erreur = 2 : type d'objet non pris en charge	
5	Violation de politique	RFC 5440
	valeur d'erreur = 1 : bit C de l'objet METRIC établi (demande rejetée)	
	valeur d'erreur = 2 : bit O de l'objet RP à zéro (demande rejetée)	
6	Objet obligatoire manquant	RFC 5440
	valeur d'erreur = 1 : objet RP manquant	
	valeur d'erreur = 2 : RRO manquant pour une demande de réoptimisation (bit R de l'objet RP établi)	
	valeur d'erreur = 3 : objet END-POINTS manquant	
7	Demande de calcul de chemin synchronisé manquant	RFC 5440
8	Référence de demande manquante	RFC 5440
9	Tentative d'établissement d'une seconde session PCEP	RFC 5440
10	Réception d'un objet invalide	RFC 5440
	valeur d'erreur = 1 : réception d'un objet avec le fanion P non établi bien que le fanion P doive être établi selon la présente spécification.	

L'IANA a créé un registre pour gérer le champ Fanions de l'objet PCEP-ERROR.

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)

- o Description de capacité
- o RFC de définition

Aucun bit n'est actuellement défini pour le champ de fanion de l'objet PCEP-ERROR.

9.13 Champ de fanions de l'objet LOAD-BALANCING

L'IANA a créé un registre pour gérer le champ Fanions de l'objet LOAD-BALANCING.

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Aucun bit n'est actuellement défini pour le champ de fanion de l'objet LOAD-BALANCING.

9.14 Objet CLOSE

L'objet CLOSE DOIT être présent dans chaque message Close afin de clore une session PCEP. Le champ Raison de l'objet CLOSE spécifie la raison de la clôture de la session PCEP. Le champ Raison de l'objet CLOSE est géré par l'IANA.

Raisons :

Valeur	Signification
1	Pas d'explication fournie
2	DeadTimer expiré
3	Réception d'un message PCEP mal formé
4	Réception d'un nombre inacceptable de demandes/réponses inconnues
5	Réception d'un nombre inacceptable de messages PCEP non reconnus

De nouveaux numéros de bits peuvent seulement être alloués par une action de consensus de l'IETF. Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité
- o RFC de définition

Aucun bit n'est actuellement défini pour le champ Fanions de l'objet CLOSE.

9.15 Indicateurs de type de TLV PCEP

L'IANA a créé un registre pour les TLV PCEP.

Valeur	Signification	Référence
1	TLV NO-PATH-VECTOR	RFC 5440
2	TLV OVERLOAD-DURATION	RFC 5440
3	TLV REQ-MISSING	RFC 5440

9.16 TLV NO-PATH-VECTOR

L'IANA gère l'espace de fanions portés dans le TLV NO-PATH-VECTOR défini dans ce document, les numérotant à partir de 0 comme bit de moindre poids.

De nouveaux numéros de bits ne peuvent être alloués que par une action de consensus de l'IETF.

Chaque bit devrait être tracé avec les qualités suivantes :
- o Numéro de bit (en comptant du bit 0 au bit de plus fort poids)
- o Description de capacité

o RFC de définition

Numéro de bit	Nom	Référence
31	PCE actuellement indisponible	RFC 5440
30	Destination inconnue	RFC 5440
29	Source inconnue	RFC 5440

10. Considérations sur la sécurité

10.1 Vulnérabilité

Des attaques contre PCEP peuvent résulter en dommages aux réseaux actifs. Si les réponses au calcul de chemin sont changées, le PCC peut être encouragé à établir des LSP inappropriés. De tels LSP pourraient dévier sur des parties du réseau susceptibles d'espionnage, ou pourraient transiter par des liaisons encombrées ou réservées. Les réponses de calcul de chemin peuvent être attaquées en modifiant le message PCRep, en se faisant passer pour le PCE, ou en modifiant le PCReq pour amener le PCE à effectuer un calcul différent de ce qui était originellement demandé.

Il est aussi possible d'endommager le fonctionnement d'un PCE par diverses attaques de déni de service. de telles attaques peuvent causer l'encombrement du PCE avec pour résultat que les calculs de chemin soient fournis trop lentement pour être utiles aux PCC. Cela pourrait conduire à des temps de récupération plus lents que ce qui est acceptable ou à un retard de l'établissement des LSP. Dans des cas extrêmes, il se peut que des demandes de service ne soient pas satisfaites.

PCEP pourrait être la cible des attaques suivantes :
o Usurpation d'identité (se faire passer pour le PCC ou le PCE)
o Espionnage (interception de message)
o Falsification
o Déni de service

Dans les scénarios inter-AS quand une communication de PCE à PCE est requise, des attaques peuvent être particulièrement significatives avec des implications commerciales ainsi que de niveau service.

De plus, l'usurpation d'identité des demandes et réponses PCEP peut donner à un attaquant des informations sur le fonctionnement du réseau. En voyant simplement les messages PCEP quelqu'un peut déterminer le schéma de l'établissement de service dans le réseau et peut savoir où le trafic est acheminé, rendant par là le réseau susceptible d'attaques ciblées et les données vulnérables dans les LSP spécifiques.

Les paragraphes qui suivent identifient des mécanismes pour protéger PCEP contre des attaques contre la sécurité.

10.2 Techniques de sécurité TCP

Au moment de la rédaction du présent mémoire, TCP-MD5 [RFC2385] est le seul mécanisme de sécurité disponible pour sécuriser les connexions TCP qui sous-tendent les sessions PCEP.

Comme expliqué dans la [RFC2385], l'utilisation de MD5 rencontre des limitations et ne fournit pas un niveau de sécurité aussi élevé qu'on le croyait autrefois. Une mise en œuvre de PCEP qui prend en charge TCP-MD5 DEVRAIT être conçue de telle façon que de plus fortes techniques ou algorithmes de chiffrement qui pourront être spécifiés pour TCP puissent être facilement intégrés à l'avenir.

L'option d'authentification TCP [RFC5925] (TCP-AO) spécifie de nouvelles procédures de sécurité pour TCP, mais n'est pas encore achevée. Comme on estime que la [RFC5925] va offrir une sécurité significativement améliorée pour les applications qui utilisent TCP, les mises en œuvre devraient s'attendre à se mettre à jour aussitôt que l'option d'authentification TCP sera publiée comme RFC.

Les mises en œuvre DOIVENT prendre en charge TCP-MD5 et devraient rendre la fonction de sécurité disponible comme option de configuration.

Les opérateurs vont devoir observer que certaines mises en œuvre déployées de PCEP peuvent précéder l'achèvement de la [RFC5925], et qu'il va être nécessaire de configurer une politique pour des communications sûres entre les locuteurs PCEP qui prennent en charge l'option d'authentification TCP et ceux qui ne le font pas.

Une autre approche pour la sécurité sur le transport TCP est d'utiliser le protocole de sécurité de la couche transport (TLS, *Transport Layer Security* (TLS) [RFC5246]. Cela permet une protection contre l'espionnage, l'altération, et la falsification de message. Mais TLS ne protège pas la connexion TCP elle-même, parce que il n'authentifie pas l'en-tête TCP. Donc, il est vulnérable à des attaques comme de réinitialisation de TCP (ce contre quoi TCP-MD5 ne protège pas). L'utilisation de TLS exigerait, cependant, la spécification de comment PCEP initie la prise de contact TLS et comment il interprète les certificats échangés dans TLS. Cette spécification sort du domaine d'application du présent document, mais pourrait être l'objet de travaux futurs.

10.3 Authentification et intégrité PCEP

Les vérifications d'authentification et d'intégrité permettent au receveur d'un message PCEP de savoir que le message provient certainement du nœud qui prétend l'avoir envoyé et de savoir si le message a été modifié.

Le mécanisme TCP-MD5 [RFC2385] décrit au paragraphe précédent fournit un tel mécanisme sous réserve des problèmes mentionnés dans les [RFC2385] et [RFC4278]. Ces problèmes seront traités et résolus par la [RFC5925].

10.4 Confidentialité PCEP

Assurer la confidentialité de la communication PCEP est d'une importance clé, en particulier dans un contexte inter-AS, où les points d'extrémité de la communication PCEP ne résident pas dans le même AS, car un attaquant qui intercepte un message de PCE pourrait obtenir des informations sensibles sur les chemins et ressources calculés.

La confidentialité de PCEP peut être assurée par le chiffrement. TCP PEUT fonctionner sur des tunnels IPsec [RFC4303] pour fournir le chiffrement requis. Noter que IPsec peut aussi assurer l'authentification et l'intégrité ; dans ce cas, TCP-MD5 ou TCP-AO ne seraient pas nécessaires. Cependant, il y a le problème que IPsec à cette échelle serait difficile à configurer et faire fonctionner. L'utilisation de IPSec avec PCEP sort du domaine d'application du présent document et pourra être traité dans un document séparé.

10.5 Configuration et échange de clé

L'authentification, la protection contre l'altération, et le chiffrement exigent tous l'utilisation de clés par l'envoyeur et le receveur.

Bien que la configuration de clé par session soit possible, il peut être particulièrement coûteux pour les opérateurs (de la même façon que pour le protocole de passerelle frontière (BGP, *Border Gateway Protocol*) comme discuté dans [BGP-SEC]). Si il y a un nombre relativement faible de PCC et PCE dans le réseau, la configuration manuelle de clé PEUT être considérée comme un choix valide par l'opérateur, bien qu'il soit important d'être conscient des vulnérabilités introduites par de tels mécanismes (c'est-à-dire, des erreurs de configuration, l'ingénierie sociale, et la négligence pourraient toutes donner lieu à des brèches de la sécurité). De plus, les clés configurées manuellement vont probablement être moins régulièrement mises à jour ce qui augmente aussi le risque pour la sécurité. Quand il y a un grand nombre de PCC et PCE, l'opérateur pourrait trouver que la configuration et la maintenance de clé est un fardeau significatif car chaque PCC doit être configuré au PCE.

Une solution de remplacement aux clés individuelles est l'utilisation d'une clé de groupe. Une clé de groupe est connue en commun par tous les membres d'un domaine de confiance. Donc, comme les routeurs dans une zone IGP ou un AS font partie d'un domaine de confiance commun [RFC5920], une clé de groupe PCEP PEUT être partagée par tous les PCC et PCE dans une zone ou AS IGP. L'utilisation d'une clé de groupe va considérablement simplifier la tâche de configuration de l'opérateur tout en continuant de sécuriser PCEP contre une attaque de l'extérieur du réseau. Cependant, on doit noter que plus il y a d'entités qui ont accès à une clé, plus grand est le risque que cette clé devienne publique.

Avec l'utilisation d'une clé de groupe, des clés séparées vont devoir être configurées pour les communications de PCE à PCE qui traversent les frontières du domaine de confiance (par exemple, d'AS) mais le nombre de ces relations va probablement être très faible.

La découverte de PCE ([RFC5088] et [RFC5089]) est une caractéristique significative pour la réussite du déploiement de PCEP dans les grands réseaux. Ce mécanisme permet à un PCC de découvrir l'existence de PCE convenables dans le réseau sans nécessiter de configuration. Il devrait être évident que, lorsque des PCE sont découverts et non configurés, le PCC ne peut pas connaître la clé correcte à utiliser. Il y a trois approches possibles de ce problème qui concernent un aspect

de sécurité :

- Les PCC peuvent utiliser une clé de groupe comme discuté précédemment.
- Les PCC peuvent utiliser une forme de protocole sûr d'échange de clé avec le PCE (comme le protocole d'échange de clé Internet version 2 (IKEv2, *Internet Key Exchange protocol v2*) [RFC4306]). L'inconvénient est que les mises en œuvre de IKE sur les routeurs ne sont pas courantes et ceci peut être une barrière au déploiement de PCEP. Les détails sortent du domaine d'application du présent document et pourront être traités dans un document séparé.
- Les PCC peuvent utiliser un serveur de clés pour déterminer la clé à utiliser quand ils parlent au PCE. Dans une certaine mesure, cela déplace juste le problème, car les communications des PCC avec le serveur de clé doivent aussi être sûres (par exemple, en utilisant Kerberos [RFC4120]) mais il peut y avoir un avantage (mineur) d'échelle si le PCC apprend plusieurs PCE et a seulement besoin de connaître un seul serveur de clés. Noter que les serveurs de clé ont actuellement une mise en œuvre très limitée. Les détails sortent du domaine d'application du présent document et pourront être traités dans un document séparé.

Les relations PCEP vont probablement être de longue durée même si les sessions PCEP sont closes et rétablies de façon répétée. Lorsque des relations de protocole persistent pour un grand nombre d'interactions de protocole ou sur une longue période, le changement des clés utilisées par les homologues du protocoles est RECOMMANDÉ [RFC4107]. Noter que TCP-MD5 ne permet pas que la clé soit changée sans clore et rouvrir la connexion TCP ce qui va résulter en la terminaison de la session PCEP et son redémarrage. Cela pourrait n'être pas un problème significatif pour PCEP. Noter aussi que les plans pour l'option d'authentification TCP [RFC5925] vont permettre un changement dynamique de clé pour une connexion TCP active.

Si l'échange de clé est utilisé (par exemple, avec IKE) il est alors relativement simple de prendre en charge des mises à jour dynamiques de clé et de les appliquer à PCEP.

Noter que la gestion de clé dans la bande pour l'option d'authentification TCP [RFC5925] n'est actuellement pas résolue.

La [RFC3562] règle certains des problèmes de la gestion de clé de connexions TCP sûres.

10.6 Politique d'accès

L'accès non autorisé à la fonction de PCE représente une variante des attaques potentielles. Non seulement cela peut être une simple attaque de déni de service (voir le paragraphe 10.7) mais cela pourrait être un mécanisme pour qu'un intrus détermine des informations importantes sur le réseau et les politiques de fonctionnement du réseau simplement en insérant des demandes de calcul boguées. De plus, de fausses demandes de calcul pourraient être utilisées pour prédire où le trafic va être placé dans le réseau quand des demandes réelles sont faites, permettant à l'attaquant de cibler des ressources spécifiques du réseau.

Les PCE DEVRAIENT être configurables à la politique d'accès. Lorsque l'authentification est utilisée, la politique d'accès peut être réalisée par l'échange ou la configuration de clés comme décrit au paragraphe 10.5. Des politiques plus simples PEUVENT être configurées sur des PCE sous la forme de listes d'accès où les adresses IP des PCC légitimes sont énumérées. Les politiques DEVRAIENT aussi être configurables pour limiter les types de demandes de calcul qui sont prises en charge à partir des différents PCC.

Il est RECOMMANDÉ que les violations de politique d'accès soient enregistrées par le PCE et soient disponibles à l'inspection de l'opérateur pour déterminer si des tentatives ont été faites pour attaquer le PCE. Ces mécanismes DOIVENT être légers pout les empêcher d'être utilisés pour soutenir des attaques de déni de service (voir le paragraphe 10.7).

10.7 Protection contre les attaques de déni de service

Les attaques de déni de service (DoS) pourraient être montées au niveau de TCP ou au niveau de PCEP. C'est-à-dire, le PCE pourrait être attaqué à travers des attaques sur TCP ou des attaques au sein de sessions PCEP établies.

10.7.1 Protection contre les attaques de DoS TCP

PCEP peut être la cible d'attaques de DoS TCP, comme par exemple des attaques de SYN, comme c'est le cas pour tous les protocoles qui fonctionnent sur TCP. D'autres spécifications de protocole ont investigué sur ce problème et PCEP peut partager leur expérience. Le lecteur se réfèrera à la spécification du protocole de distribution d'étiquettes (LDP, *Label Distribution Protocol* (LDP) [RFC5036] par exemple. Afin de protéger contre les attaques de DoS TCP, les mises en œuvre de PCEP peuvent prendre en charge les techniques suivantes.

- o PCEP utilise un seul accès enregistré pour toutes les communications. Le PCE DEVRAIT n'écouter les connexions TCP que sur les accès où la communication est attendue.
- o Le PCE PEUT mettre en œuvre une liste d'accès pour rejeter (ou éliminer) immédiatement les tentatives de connexion TCP de la part de PCC non autorisés.
- o Le PCE NE DEVRAIT PAS permettre de connexions TCP parallèles provenant du même PCC sur l'accès PCEP enregistré.
- o Le PCE PEUT exiger l'utilisation de l'option MD5 sur toutes les connexions TCP, et PEUT rejeter (ou éliminer) toute tentative d'établissement de connexion qui n'utilise pas MD5. Un PCE NE DOIT PAS accepter de paquet SYN pour lequel la somme de contrôle du segment MD5 est invalide. Noter cependant que l'utilisation de MD5 exige que le receveur utilise des ressources de CPU pour calculer la somme de contrôle avant qu'il puisse décider d'éliminer un segment SYN par ailleurs acceptable.

10.7.2 Formatage/régulation d'entrée de demandes

Une mise en œuvre de PCEP peut être soumise à des attaques de DoS au sein d'une session PCEP légitime. Par exemple, un PCC pourrait envoyer un très grand nombre de messages PCReq causant l'encombrement du PCE ou causant la mise en file d'attente de demandes d'autres PCC.

Noter que l'utilisation directe du champ Priorité sur l'objet RP pour prioriser les demandes reçues ne fournit aucune protection car l'attaquant pourrait régler toutes les demandes à être de la plus haute priorité.

Donc, il est RECOMMANDÉ que les mises en œuvre de PCE incluent des mécanismes d'entrée de formatage/régulation qui soit réduisent les demandes reçues de tout PCC, soit appliquent des techniques de mise en file d'attente ou de dégradation de priorité aux PCC trop communicatifs.

De tels mécanismes PEUVENT être réglés par défaut, mais DEVRAIENT être disponibles à la configuration. De telles techniques peuvent être considérées comme particulièrement importantes dans les environnements de fournisseur multi services pour protéger les ressources d'un fournisseur de services contre l'utilisation non garantie, trop zélée, ou malveillante par les PCE d'un autre fournisseur de services.

11. Remerciements

Les auteurs tiennent à remercier Dave Oran, Dean Cheng, Jerry Ash, Igor Bryskin, Carol Iturrade, Siva Sivabalan, Rich Bradford, Richard Douville, Jon Parker, Martin German, et Dennis Aristow de leurs très précieux apports. Les auteurs tiennent aussi à remercier Fabien Verhaeghe de très profitables discussions et d'utiles suggestions. David McGrew et Brian Weis on fourni de précieux apports pour la section des considérations sur la sécurité.

Ross Callon, Magnus Westerlund, Lars Eggert, Pasi Eronen, Tim Polk, Chris Newman, et Russ Housley ont fourni d'importantes contributions durant la revue de l'IESG.

12. Références

12.1 Références normatives

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

[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, RFC6780)) *(P.S.)*

[RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998. *(P.S. ; MàJ par la* RFC6691 *; remplacée par* RFC5925)

[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)

[RFC3477] K. Kompella, Y. Rekhter, "Signalisation des liaisons non numérotées dans le protocole de réservation de ressource – ingénierie du trafic (RSVP-TE)", janvier 2003. *(P.S.)*

[RFC4090] P. Pan et autres, "Extensions de réacheminement rapide à RSVP-TE pour les tunnels de LSP", mai 2005. *(P.S. ; MàJ par* RFC8271, RFC8537, RFC8796)

[RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (*Remplace* RFC2434 *; remplacée par* RFC8126)

12.2 Références pour information

[BGP-SEC] Christian, B. et T. Tauber, "BGP Security Requirements", Travail en cours, novembre 2008.

[IEEE.754] IEEE Standard 754, "Standard for Binary Floating-Point Arithmetic", août 1985.

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992, DOI 10.17487/RFC1321, *(Information)*

[RFC3471] L. Berger, éd., "Commutation d'étiquettes multi-protocoles généralisée (GMPLS) : description fonctionnelle de la signalisation", janvier 2003. (*MàJ par* RFC4201, RFC4328, RFC4872, RFC8359) *(P.S.)*

[RFC3562] M. Leech, "Considérations sur la gestion de clés pour l'option de signature MD5 dans TCP", juillet 2003. *(Information)*

[RFC3785] F. Le Faucheur, R. Uppili, A. Vedrenne, P. Merckx et T. Telkamp, "Utilisation de la métrique du protocole de routeur intérieur (IGP) comme seconde métrique d'ingénierie du trafic MPLS", BCP 87, mai 2004.

[RFC4022] R. Raghunarayan, éd., "Base de données d'informations de gestion pour le protocole de contrôle de transmission (TCP)", mars 2005. (*Remplace* RFC2452, RFC2012) *(P.S.)*

[RFC4101] E. Rescorla, IAB, "Écrire des modèles de protocoles", juin 2005. *(Information)*

[RFC4107] S. Bellovin, R. Housley, "Lignes directrices pour la gestion des clés de chiffrement", juin 2005, DOI 10.17487/RFC4107, (BCP0107)

[RFC4120] C. Neuman et autres, "Service Kerberos d'authentification de réseau (V5)", juillet 2005. (*MàJ par* RFC4537, 5021, 6649, 7751, 8062, 8129, 8429)

[RFC4278] S. Bellovin, A. Zinin, "Différence de niveau de normalisation entre l'option de signature MD5 de TCP de la (RFC 2385) et la spécification BGP-4", janvier 2006. *(Information)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

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

[RFC4657] J. Ash. et J.L. Le Roux, éditeurs, "Exigences génériques du protocole de communication par élément de calcul de chemin (PCE)", septembre 2006.

[RFC4674] J. Ash. et J.L. Le Roux, éditeurs, "Exigences pour la découverte d'élément de calcul de chemin (PCE)", octobre 2006. *(Info.)*

[RFC4927] J.-L. Le Roux, éd., "Exigences spécifiques du protocole de communication d'élément de calcul de chemin (PCECP) pour l'ingénierie du trafic inter zones MPLS et GMPLS", juin 2007. *(Information)*

[RFC5036] L. Andersson, I. Minei et B. Thomas, éditeurs, "Spécification de LDP", janvier 2001. (*Remplace* RFC3036) (*MàJ par les* RFC6720 , RFC6790, RFC7552,) *(D.S)*

[RFC5088] JL. Le Roux et autres, "Extensions au protocole OSPF pour la découverte d'élément de calcul de chemin (PCE)", janvier 2008. *(P.S. ; MàJ par* RFC9353*)*

[RFC5089] JL. Le Roux et autres, "Extensions au protocole IS-IS pour la découverte d'élément de calcul de chemin (PCE)", janvier 2008. *(P.S. ; MàJ par* RFC9353*)*

[RFC5246] T. Dierks, E. Rescorla, "Version 1.2 du protocole de sécurité de la couche Transport (TLS)", DOI 10.17487/RFC5246, août 2008. *(P.S.* ; *remplace* RFC3268, 4346, 4366 ; *MàJ* RFC4492 ; *rendue obsolète par la* RFC8446)

[RFC5376] N. Bitar et autres, "Exigences inter AS pour le protocole de communication d'élément de calcul de chemin (PCECP)", novembre 2008. *(Information)*

[RFC5420] A. Farrel et autres, "Codage des attributs pour l'établissement de LSP MPLS en utilisant le protocole de réservation de ressource avec ingénierie du trafic (RSVP-TE)", février 2009. (*Remplace* RFC4420) (*MàJ par* RFC6510) *(P.S.)*

[RFC5511] A. Farrel, "Forme Backus-Naur d'acheminement (RBNF) : syntaxe utilisée pour former les règles de codage dans diverses spécifications de protocole d'acheminement", avril 2009. *(P.S.)*

[RFC5623] E. Oki, T. Takeda, JL. Le Roux, A. Farrel, "Cadre pour l'ingénierie de trafic MPLS et GMPLS inter couche fondée sur PCE", septembre 2009. *(Information)*

[RFC5886] JP. Vasseur, JL. Le Roux, Y. Ikejiri, "Ensemble d'outils de surveillance pour architecture fondée sur l'élément de calcul de chemin (PCE)", juin 2010. *(P. S.)*

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

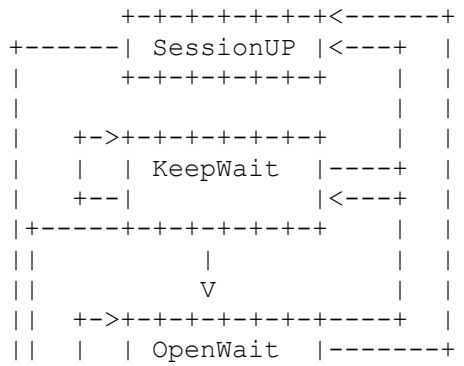
[RFC5925] J. Touch, A. Mankin, R. Bonica, "Option Authentification de TCP", DOI 10.17487/RFC5925, juin 2010. (*Remplace* RFC2385). *(P. S.)*

[RFC6123] A. Farrel, "Inclusion de sections sur la gestion dans les projets du groupe de travail Éléments de calcul de chemin (PCE)", février 2011. *(Historique)*

[RFC7420] A. Koushik, et autres, "Module de MIB du protocole de communication d'élément de calcul de chemin (PCECP)", décembre 2014. *(P.S.)*

Appendice A. Automate à états finis pour PCEP

Cette section décrit l'automate à états finis (FSM, *Finite State Machine*) PCEP.



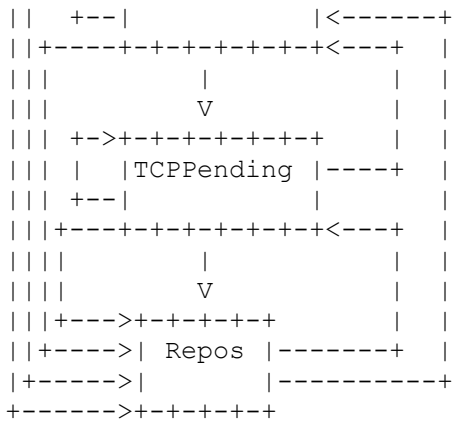


Figure 23 : Automate à états finis de PCEP pour le PCC

PCEP définit l'ensemble de variables suivant :

Connect : temporisateur (en secondes) lancé après avoir initialisé une connexion TCP en utilisant l'accès TCP enregistré par PCEP. La valeur du temporisateur Connect est 60 secondes.

ConnectRetry : nombre de fois que le système a essayé sans succès d'établir une connexion TCP avec un homologue PCEP.

ConnectMaxRetry : nombre maximum de fois que le système essaye d'établir une connexion TCP en utilisant l'accès TCP enregistré par PCEP avant de revenir à l'état Repos. La valeur de ConnectMaxRetry est 5.

OpenWait : temporisateur qui correspond à la durée qu'attend un homologue PCEP pour recevoir un message Open de l'homologue PCEP après l'expiration duquel le système libère la ressource PCEP et revient à l'état Repos. Le temporisateur OpenWait a une valeur fixe de 60 secondes.

KeepWait : temporisateur qui correspond à la durée d'attente d'un homologue PCEP pour recevoir un message Keepalive ou PCErr de l'homologue PCEP après l'expiration duquel le système libère la ressource PCEP et revient à l'état Repos. Le temporisateur KeepWait a une valeur fixe de 60 secondes.

OpenRetry : nombre de fois que le système a reçu un message Open avec des caractéristiques de session PCEP inacceptables.

Les deux variables d'état suivantes sont définies :

RemoteOK : booléen qui est réglé à 1 si le système a reçu un message Open acceptable.

LocalOK : booléen qui est réglé à 1 si le système a reçu un message Keepalive reconnaissant que le message Open envoyé à l'homologue était valide.

État Repos : l'état Repos est l'état initial de PCEP où le PCEP (aussi appelé "le système") attend un événement d'initialisation qui peut être déclenché manuellement par l'utilisateur (configuration) ou déclenché automatiquement par divers événements. Dans l'état Repos, les ressources de PCEP (mémoire, processus potentiels, etc.) sont allouées mais aucun message PCEP n'est accepté d'un homologue PCEP. Le système écoute sur l'accès TCP enregistré pour PCEP.

Les variables suivantes sont initialisées :
TCPRetry = 0,
LocalOK = 0,
RemoteOK = 0,
OpenRetry = 0.

Lorsque il détecte un événement local d'initialisation (par exemple, la configuration par l'utilisateur pour établir une session PCEP avec un homologue PCEP particulier, événement local déclenchant l'établissement d'une session PCEP avec un homologue PCEP comme la détection automatique d'un homologue PCEP) le système :
- initie une connexion TCP avec l'homologue PCEP,
- lance le temporisateur Connect,

- passe à l'état TCPPending.

À réception d'une connexion TCP sur l'accès TCP enregistré pour PCEP, si l'établissement de la connexion TCP réussit, le système :
- envoie un message Open,
- lance le temporisateur OpenWait,
- passe à l'état OpenWait.

Si l'établissement de connexion échoue, le système reste dans l'état Repos. Tout autre événement reçu dans l'état Repos est ignoré.

On s'attend à ce qu'une mise en œuvre utilise un temporisateur à accroissement exponentiel entre les événements d'initialisation générés automatiquement et entre les essais d'établissement de connexion TCP.

État TCPPending :
Si l'établissement de connexion TCP réussit, le système :
- envoie un message Open,
- lance le temporisateur OpenWait,
- passe à l'état OpenWait.

Si l'établissement de connexion TCP échoue (une erreur est détectée durant l'établissement de la connexion TCP) ou le temporisateur Connect expire :
- Si ConnectRetry = ConnectMaxRetry, le système passe à l'état Repos.
- Si ConnectRetry < ConnectMaxRetry, le système :
  1. Initie une connexion TCP avec l'homologue PCEP,
  2. Incrémente la variable ConnectRetry,
  3. Relance le temporisateur Connect,
  4. Reste dans l'état TCPPending.

En réponse à tout autre événement, le système libère les ressources de PCEP pour cet homologue et revient à l'état Repos.

État OpenWait :
Dans l'état OpenWait, le système attend un message Open provenant de son homologue PCEP.

Si le système reçoit un message Open provenant de l'homologue PCEP avant l'expiration du temporisateur OpenWait, le système examine d'abord toutes ses sessions qui sont dans l'état OpenWait ou KeepWait. Si une autre session avec le même homologue PCEP existe déjà (même adresse IP) alors le système effectue la procédure de résolution de collision suivante :
- Si le système a initié la session en cours et si elle a une adresse IP inférieure à celle de l'homologue PCEP, le système ferme la connexion TCP, libère les ressources de PCEP pour la session en cours, et revient à l'état Repos.
- Si la session a été initiée par l'homologue PCEP et si le système a une adresse IP supérieure à celle de l'homologue PCEP, le système ferme la connexion TCP, libère les ressources de PCEP pour la sessionen cours, et revient à l'état Repos.
- Autrement, le système vérifie les attributs de la session PCEP (fréquence de Keepalive, DeadTimer, etc.).

Si une erreur est détectée (par exemple, message Open mal formé, réception d'un message qui n'est pas un message Open, présence de deux objets OPEN) PCEP génère une notification d'erreur, l'homologue PCEP envoie un message PCErr avec le type d'erreur = 1 et la valeur d'erreur = 1. Le système libère les ressources de PCEP pour l'homologue PCEP, ferme la connexion TCP, et passe à l'état Repos.

Si aucune erreur n'est détectée, si OpenRetry = 1, et si les caractéristiques de session sont inacceptables, l'homologue PCEP envoie un PCErr avec le type d'erreur = 1 et la valeur d'erreur = 5, et le système libère les ressources de PCEP pour cet homologue et revient à l'état Repos.

Si aucune erreur n'est détectée, et si les caractéristiques de session sont acceptables au système local, le système :
- envoie un message Keepalive à l'homologue PCEP,
- lance le temporisateur Keepalive,
- règle la variable RemoteOK à 1.

Si LocalOK = 1, le système libère le temporisateur OpenWait et passe à à l'état UP.
Si LocalOK = 0, le système libère le temporisateur OpenWait, lance le temporisateur KeepWait, et passe à l'état KeepWait.

Si aucune erreur n'est détectée, mais si les caractéristiques de session sont inacceptables et non négociables, l'homologue PCEP envoie un PCErr avec le type d'erreur = 1 et la valeur d'erreur = 3, et le système libère les ressources de PCEP pour cet homologue et revient à l'état Repos.

Si aucune erreur n'est détectée, et si OpenRetry est 0, et si les caractéristiques de session sont inacceptables mais négociables (comme la période de Keepalive ou le DeadTimer) alors le système :
- o incrémente la variable OpenRetry,
- o envoie un mesage PCErr avec type d'erreur = 1 et valeur d'erreur = 4 qui contient les caractéristiques de session proposées acceptables.
- o Si LocalOK = 1, le système redémarre le temporisateur OpenWait et reste dans l'état OpenWait.
- o Si LocalOK = 0, le système libère le temporisateur OpenWait, lance le temporisateur KeepWait, et passe à l'état KeepWait.

Si aucun message Open n'est reçu avant l'expiration du temporisateur OpenWait, l'homologue PCEP envoie un message PCErr avec type d'erreur = 1 et valeur d'erreur = 2, le système libère les ressources de PCEP pour l'homologue PCEP, ferme la connexion TCP, et passe à l'état Repos *(Idle)*.

En réponse à tout autre événement, le système libère les ressources de PCEP pour cet homologue et revient à l'état Repos.

État KeepWait :
Dans l'état Keepwait, le système attend la réception d'un Keepalive provenant de l'homologue PCEP accusant réception de son message Open ou un message PCErr en réponse à des caractéristiques de session PCEP inacceptables proposées dans le message Open.

Si une erreur est détectée (par exemple, un message Keepalive mal formé) PCEP génère une notification d'erreur, l'homologue PCEP envoie un message PCErr avec type d'erreur = 1 et valeur d'erreur = 1. Le système libère les ressources de PCEP pour l'homologue PCEP, ferme la connexion TCP, et passe à l'état Repos.

Si un message Keepalive est reçu avant l'expiration du temporisateur KeepWait, alors le système règle LocalOK = 1 et :
- o Si RemoteOK = 1, le système libère le temporisateur KeepWait et passe à l'état UP.
- o Si RemoteOK = 0, le système libère le temporisateur KeepWait, lance le temporisateur OpenWait, et passe à l'état OpenWait.

Si un message PCErr est reçu avant l'expiration du temporisateur KeepWait :
1. Si les valeurs proposées sont inacceptables, l'homologue PCEP envoie un message PCErr avec type d'erreur = 1 et valeur d'erreur = 6, et le système libère les ressources de PCEP pour cet homologue PCEP, ferme la connexion TCP, et passe à l'état Repos.
2. Si les valeurs proposées sont acceptables, le système ajuste ses caractéristiques de session PCEP conformément aux valeurs proposées reçues dans le message PCErr, redémarre le temporisateur KeepWait, et envoie un nouveau message Open. Si RemoteOK = 1, le système redémarre le temporisateur KeepWait et reste dans l'état KeepWait. Si RemoteOK = 0, le système libère le temporisateur KeepWait, lance le temporisateur OpenWait, et passe à l'état OpenWait.

Si ni un Keepalive ni un PCErr n'est reçu après l'expiration du temporisateur KeepWait, l'homologue PCEP envoie un message PCErr avec type d'erreur = 1 et valeur d'erreur = 7, et le système libère les ressources de PCEP pour cet homologue PCEP, ferme la connexion TCP, et passe à l'état Repos.

En réponse à tout autre événement, le système libère les ressources de PCEP pour cet homologue et revient à l'état Repos.

État UP :
Dans l'état UP, le homologue PCEP commence par échanger des messages PCEP selon les caractéristiques de session.

Si le temporisateur Keepalive expire, le système redémarre le temporisateur Keepalive et envoie un message Keepalive.

Si aucun message PCEP (Keepalive, PCReq, PCRep, PCNtf) n'est reçu de l'homologue PCEP avant l'expiration du DeadTimer, le système termine la session PCEP conformément à la procédure définie au paragraphe 6.8, libère les ressources de PCEP pour cet homologue PCEP, ferme la connexion TCP, et passe à l'état Repos.

Si un message mal formé est reçu, le système termine la session PCEP conformément à la procédure définie au paragraphe 6.8, libère les ressources de PCEP pour cet homologue PCEP, ferme la connexion TCP et passe à l'état Repos.

Si le système détecte que l'homologue PCEP essaye d'établir une seconde connexion TCP, il arrête l'établissement de

connexion TCP et envoie un PCErr avec le type d'erreur = 9.

Si la connexion TCP échoue, le système libère les ressources de PCEP pour cet homologue PCEP, ferme la connexion TCP, et passe à l'état Repos.

Appendice B. Variables de PCEP

PCEP définit les variables configurables suivantes :

temporisateur Keepalive : période minimum entre l'envoi de messages PCEP (Keepalive, PCReq, PCRep, PCNtf) à un homologue PCEP. Une valeur suggérée pour le temporisateur Keepalive est 30 secondes.

DeadTimer : période de temporisation après l'expiration de laquelle l'homologue PCEP déclare la session morte si aucun message PCEP n'a été reçu.

SyncTimer : temporisateur utilisé dans le cas d'une demande de calcul de chemin synchronisée utilisant l'objet SVEC défini au paragraphe 7.13.3. Considérons le cas où un message PCReq est reçu par un PCE qui contient l'objet SVEC se référant à M demandes de calcul de chemin synchronisées. Si après l'expiration de SyncTimer toutes les M demandes de calcul de chemin n'ont pas été reçues, une erreur de protocole est déclenchée et le PCE DOIT annuler l'ensemble des demandes de calcul de chemin. Le but du SyncTimer est d'éviter de mémoriser des demandes synchronisées non utilisées pour si l'une d'elles devait être perdue pour une raison quelconque (par exemple, la mauvaise conduite d'un PCC). Donc, la valeur de SyncTimer doit être assez grand pour éviter l'expiration du temporisateur dans des circonstances normales. Une valeur RECOMMANDÉE pour SyncTimer est 60 secondes.

MAX-UNKNOWN-REQUESTS : une valeur RECOMMANDÉE est 5.

MAX-UNKNOWN-MESSAGES : une valeur RECOMMANDÉE est 5.

Appendice C. Contributeurs

Le contenu de ce document est la contribution des personnes mentionnées ci-dessous et des éditeurs mentionnés à la fin du document.

Arthi Ayyangar
Juniper Networks
1194 N. Mathilda Ave
Sunnyvale, CA 94089
USA
mél : arthi@juniper.net

Adrian Farrel
Old Dog Consulting
téléphone : +44 (0) 1978 860944
mél : adrian@olddog.co.uk

Eiji Oki
NTT
Midori 3-9-11
Musashino, Tokyo, 180-8585
JAPAN
mél : oki.eiji@lab.ntt.co.jp

Andrew Dolganow
Alcatel
600 March Road
Ottawa, ON K2K 2E6
CANADA
mél : andrew.dolganow@alcatel.com

Alia Atlas
British Telecom
mél : akatlas@alum.mit.edu

Yuichi Ikejiri
NTT Communications Corporation
1-1-6 Uchisaiwai-cho, Chiyoda-ku
Tokyo, 100-819
JAPAN
mél : y.ikejiri@ntt.com

Kenji Kumaki
KDDI Corporation
Garden Air Tower Iidabashi, Chiyoda-ku,
Tokyo, 102-8460
JAPAN
mél : ke-kumaki@kddi.com

Adresse des éditeurs

JP Vasseur
Cisco Systems
1414 Massachusetts Avenue
Boxborough, MA 01719
USA
mél : jpv@cisco.com

JL Le Roux
France Telecom
2, Avenue Pierre-Marzin
Lannion 22307
FRANCE
mél : jeanlouis.leroux@orange-ftgroup.com