Groupe de travail Réseau
Request for Comments : 4577
RFC mise à jour : 4364
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

E. Rosen, Cisco Systems, Inc.
P. Psenak, Cisco Systems, Inc.
P. Pillay-Esnault, Cisco Systems, Inc.

janvier 2006

OSPF comme protocole de bord fournisseur/consommateur pour les réseaux privés virtuels (VPN) IP BGP/MPLS

Résumé
De nombreux fournisseurs de services offrent des services de réseau privé virtuel (VPN, *Virtual Private Network*) à leurs consommateurs, en utilisant une technique dans laquelle les routeurs de bord consommateur (routeurs CE, *customer edge routers*) sont les homologues d'acheminement des routeurs de bord fournisseur (routeurs PE, *provider edge routers*). Le protocole de passerelle frontière (BGP, *Border Gateway Protocol*) est utilisé pour distribuer les chemins du consommateur à travers le réseau IP dorsal du fournisseur, et la commutation d'étiquettes multi protocoles (MPLS, *Multiprotocol Label Switching*) est utilisée pour tunneler les paquets du consommateur à travers le réseau dorsal du fournisseur. Ceci est appelé un "VPN IP BGP/MPLS". La spécification de base pour les VPN IP BGP/MPLS présume que BGP est le protocole d'acheminement sur l'interface entre un routeur PE et un routeur CE. Le présent document étend cette spécification en permettant que le protocole d'acheminement sur l'interface PE/CE soit le protocole de plus court chemin ouvert en premier (OSPF, *Open Shortest Path First*).

Le présent document met à jour la RFC 4364.

Table des matières

1. Introduction

La [RFC4364] décrit une méthode par laquelle un fournisseur de service (SP, *Service Provider*) peut utiliser son réseau dorsal IP pour fournir un service de réseau privé virtuel (VPN, *Virtual Private Network*) aux consommateurs. Dans cette méthode, des appareils de bord consommateur (CE, *customer's edge*) sont connectés aux routeurs de bord fournisseur (PE, *provider's edge*). Si l'appareil CE est un routeur, alors le routeur PE peut devenir un homologue d'acheminement du routeur CE (dans un certain protocole d'acheminement) et peut, par suite, apprendre les chemins qui conduisent au site du CE et qui ont besoin d'être distribués aux autres routeurs PE qui se rattachent au même VPN.

Les routeurs PE qui se rattachent à un VPN commun utilisent le protocole de passerelle frontière (BGP, *Border Gateway Protocol*) pour distribuer les chemins du VPN les uns aux autres. Un routeur CE peut alors apprendre les chemins pour les autres sites dans le VPN en échangeant du trafic avec son routeur PE rattaché dans un protocole d'acheminement. Les routeurs CE des différents sites n'échangent cependant pas de trafic avec chacun des autres.

On peut s'attendre à ce que de nombreux VPN utilisent OSPF comme protocole de passerelle intérieure (IGP, *Interior Gateway Protocol*) c'est-à-dire, le protocole d'acheminement utilisé par un réseau pour la distribution des chemins internes au sein de ce réseau. Cela ne signifie pas nécessairement que les routeurs PE ont besoin d'utiliser OSPF pour échanger du trafic avec les routeurs CE. Chaque site dans un VPN peut utiliser OSPF comme protocole d'acheminement intra-site, tout en utilisant, par exemple, BGP [RFC4271] ou le protocole d'informations d'acheminement (RIP, *Routing Information Protocol*) [RFC2453] pour distribuer les chemins à un routeur PE. Cependant, il est certainement pratique, quand OSPF est utilisé intra-site, de l'utiliser aussi sur la liaison PE-CE, et la [RFC4364] le permet explicitement.

Comme toutes autres choses, l'utilisation de OSPF sur la liaison PE-CE a des avantages et des inconvénients. L'inconvénient d'utiliser OSPF sur la liaison PE-CE est que cela implique le routeur PE du SP, bien que de façon périphérique, dans l'IGP d'un site de VPN. Les avantages sont cependant que :
- les administrateurs du routeur CE n'ont pas besoin d'avoir d'expertise sur tout autre protocole d'acheminement que OSPF ;
- les routeurs CE n'ont pas besoin de prendre en charge d'autre protocole d'acheminement que OSPF ;
- si un consommateur passe de son réseau à partir d'un réseau dorsal OSPF traditionnel au service de VPN décrit dans la [RFC4364], l'utilisation de OSPF sur la liaison PE-CE facilite les questions de transition.

Il semble probable que certains SP et leurs consommateurs vont résoudre ces compromis en faveur de l'utilisation de OSPF sur la liaison PE-CE. Donc, on doit spécifier les procédures qui doivent être mises en œuvre par un routeur PE afin de rendre cela possible. (Aucune procédure particulière n'est cependant nécessaire dans le routeur CE ; les routeurs CE font juste fonctionner toutes les mises en œuvre de OSPF qu'ils peuvent avoir.)

2. Spécification 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].

3. Exigences

Considérons un ensemble de sites de VPN qui sont vus comme étant dans le même "domaine OSPF". Deux sites sont considérés comme étant dans le même domaine OSPF si il est prévu que les chemins d'un site à l'autre soient considérés comme des chemins intra-réseau. Un ensemble de sites OSPF dans le même domaine va très certainement être en ensemble de sites qui ensemble constituent un "intranet", dont chacun va utiliser OSPF comme protocole d'acheminement intra-site.

Selon la [RFC4364], les chemins de VPN sont distribués parmi les routeurs PE par BGP. Si le PE utilise OSPF pour distribuer les chemins au routeur CE, les procédures standard qui gouvernent les interactions BGP/OSPF [RFC2328] vont causer la livraison des chemins provenant d'un site à un autre dans des annonces d'état de liaison (LSA, *Link State Advertisement*) de type 5, comme des chemins "externes à l'AS". Ceci n'est pas souhaitable ; il vaudrait beaucoup mieux livrer de tels chemins dans des LSA de type 3 (comme chemins inter zones) afin qu'ils puissent être distingués de tous les autres chemins externes à l'AS qui circulent dans le VPN (c'est-à-dire, afin qu'ils puissent être distingués par OSPF des chemins qui réellement ne viennent pas de l'intérieur du VPN). Donc, il est nécessaire que les routeurs PE mettent en œuvre une version modifiée des procédures d'interaction BGP/OSPF.

En fait, on voudrait avoir un ensemble très général de procédures qui permettent à un client de remplacer facilement un réseau dorsal OSPF privé traditionnel par le service de VPN. On voudrait que cette procédure satisfasse l'ensemble d'exigences suivant :

- Les procédures ne devraient pas faire d'hypothèses sur la topologie de OSPF. En particulier, elles ne devraient pas supposer que les sites de clients sont des sites OSPF d'extrémité ou des sites de zone "pas si en bout que cela" (NSSA, *Not So Stubby Area*). Elles ne devraient pas non plus supposer qu'un site de client contient seulement une zone OSPF, ou qu'il n'y a pas de routeurs de zone 0.

- Si les sites de VPN A et B sont dans le même domaine OSPF, alors les chemins provenant de l'un devraient être présentés à l'autre comme des chemins OSPF intra-réseau. En général, cela peut être fait en présentant de tels chemins comme des chemins inter-zones dans des LSA de type 3. Noter que cela permet que deux sites de VPN soient connectés via une "liaison OSPF dérobée". C'est-à-dire, on peut avoir une liaison OSPF entre les deux sites qui est utilisée seulement quand le cœur de réseau de VPN est indisponible. (Cela ne serait pas possible avec les procédures ordinaires d'interaction BGP/OSPF. Les procédures ordinaires présenteraient les chemins via le cœur de réseau de VPN comme des chemins externes à l'AS, et ils ne pourraient jamais être préférés aux chemins intra-réseau.) Cela peut être très utile durant une période de transition d'un réseau dorsal OSPF traditionnel à un cœur de réseau de VPN.

- Il devrait être possible d'utiliser une "liaison OSPF dérobée" entre deux sites, même si les deux sites sont dans la même zone OSPF et si aucun des routeurs rattachés à la liaison dérobée inter sites n'est dans un routeur de zone 0. Cela peut aussi être très utile durant une période de transition, et cela élimine tout besoin de reconfigurer les routeur des sites à être des routeur de bordure de zone (ABR, *Area Border Router*). En supposant qu'il soit désiré d'avoir le chemin via le cœur de réseau de VPN comme préféré au chemin dérobé, le cœur de réseau de VPN lui-même doit être présenté aux routeurs CE à chaque site comme une liaison entre les deux routeurs PE auxquels les routeurs CE sont respectivement rattachés.

- Les routeurs CE, connectés aux routeurs PE du service de VPN, peuvent eux-mêmes fonctionner comme routeurs de réseau dorsal OSPF (zone 0). Un réseau dorsal OSPF peut même consister en plusieurs "segments" qui sont eux-mêmes interconnectés seulement via le service de VPN. Dans un tel scénario, la pleine intercommunication entre sites connectés à différents segments du réseau dorsal OSPF devrait quand même être possible.

- La transition du réseau dorsal OSPF privé traditionnel au service de VPN doit être simple et directe. La transition doit probablement être en plusieurs phases, de sorte que les sites des clients migrent un par un du réseau dorsal OSPF privé traditionnel au service de VPN. Durant la transition, tout site pourrait être connecté au service de VPN, au réseau dorsal OSPF traditionnel, ou aux deux. La connexité complète parmi de tels sites doit être conservée. Comme le service de VPN est destiné à remplacer le cœur de réseau traditionnel, il doit être possible, par un ajustement convenable de la métrique OSPF, de faire que OSPF préfère les chemins qui traversent le cœur de réseau de VPN du SP aux autres chemins qui ne le font pas.

- La métrique OSPF allouée à un certain chemin devrait être portée de façon transparente sur le cœur de réseau de VPN.

Les chemins provenant de sites qui ne sont pas dans le même domaine OSPF vont apparaître comme des chemins externes à l'AS.

On suppose le lecteur familiarisé avec le contenu de la [RFC2328], incluant les types de LSA OSPF, et on se réfère sans autre explication aux LSA de type 1, 2, 3, etc., ainsi qu'avec la [RFC4364].

4. Procédures d'interaction BGP/OSPF pour routeurs PE

4.1 Vue d'ensemble

4.1.1 Instances VRF et OSPF

Un routeur PE qui se rattache à plus d'un domaine OSPF DOIT avoir une instance indépendante de OSPF pour chaque domaine. Si le PE utilise OSPF comme son protocole de passerelle intérieure (IGP, *Interior Gateway Protocol*) l'instance de OSPF fonctionnant comme IGP doit être séparée et indépendante de toute autre instance de OSPF qu'utilise le PE. (Que ces instances soient réalisées comme des processus séparés ou simplement comme des contextes séparés d'un processus commun est une affaire de mise en œuvre.) Chaque interface qui se rattache à un site de VPN n'appartient qu'à une seule instance OSPF.

La [RFC4364] définit la notion de tableau d"acheminement et de transmission de VPN (VRF, *VPN Routing and Forwarding Table*) par site. Chaque VRF est associé à un ensemble d'interfaces. Si un VRF est associé à une interface particulière, et si cette interface appartient à une instance OSPF particulière, alors cette instance OSPF est dite être associée au VRF. Si deux interfaces appartiennent à la même instance OSPF, les deux interfaces doivent alors être associées au même VRF.

Si une interface rattache un PE à un CE, et si cette interface est associée à un VRF, on dit du CE qu'il est associé au VRF.

4.1.2 VRF et chemins

OSPF est utilisé pour distribuer les chemins d'un CE à un PE. Le processus de décision standard d'OSPF est utilisé pour installer les meilleurs chemins distribués par OSPF dans le VRF.

Selon la [RFC4364], BGP est utilisé pour distribuer les chemins de VPN-IPv4 parmi les routeurs PE. Un chemin OSPF installé dans un VRF peut être "exporté" en étant redistribué dans BGP comme chemin de VPN-IPv4. Il peut alors être distribué par BGP aux autres PE. Aux autres PE, un chemin de VPN-IPv4 peut être "importé" par un VRF et peut alors être redistribué dans une ou plusieurs des instances OSPF associées à ce VRF.

L'importation de et l'exportation vers des VRF particuliers est contrôlée par l'utilisation de l'attribut Communautés étendues de cible de chemin (ou, plus simplement cible de chemin (RT, *Route Target*), comme spécifié dans la [RFC4364].

Un chemin VPN-IPv4 est "éligible à l'importation" dans un VRF particulier si sa cible de chemin est identique à une des cibles de chemins importées du VRF. Le processus de décision standard de BGP est utilisé pour choisir, parmi les chemins éligibles à l'import, l'ensemble de chemins de VPN-IPv4 à "installer" dans le VRF.

Si un VRF contient à la fois un chemin distribué par OSPF et un chemin VPN-IPv4 pour le même préfixe IPv4, le chemin distribué par OSPF est alors préféré. En général, cela signifie que la transmission est faite conformément au chemin OSPF. La seule exception à cette règle est en rapport avec la "liaison factice". Si l'interface de prochain bond pour un chemin installé (distribué par OSPF) est la liaison factice, la transmission est faite conformément à un chemin BGP correspondant. Ceci est précisé au paragraphe 4.2.7.4.

Pour satisfaire les exigences de la Section 3, un PE qui installe un chemin particulier dans un certain VRF a besoin de savoir si ce chemin était à l'origine un chemin OSPF et, si il en est ainsi, si l'instance OSPF à partir de laquelle il a été redistribué dans BGP est dans le même domaine que les instances OSPF dans lesquelles le chemin peut être redistribué. Donc, un identifiant de domaine est codé comme un attribut de communautés étendues BGP [RFC4360] et distribué par BGP avec le chemin de VPN-IPv4. La métrique OSPF du chemin et le type de chemin OSPF sont aussi portés comme des attributs BGP du chemin.

4.1.3 Chemins inter zone, intra zone, et externes

Si un PE installe un chemin de VPN-IPv4 particulier (appris via BGP) dans un VRF, et si c'est le chemin préféré BGP pour le préfixe IPv4 correspondant, le chemin IPv4 correspondant est alors "éligible à la redistribution" dans chaque instance OSPF qui est associée au VRF. Par suite, il peut être annoncé à chaque CE dans une LSA.

Si un chemin qui est éligible pour redistribution dans OSPF est en fait redistribué dans une instance OSPF particulière peut dépendre de la configuration. Par exemple, le PE peut être configuré à distribuer seulement le chemin par défaut dans une certaine instance OSPF. Dans ce cas, les chemins qui sont éligibles pour redistribution ne vont en fait pas être redistribués.

Dans ce qui suit, on discute des procédures pour redistribuer un chemin de VPN-IPv4 distribué par BGP dans OSPF ; ce sont les procédures à suivre chaque fois qu'un tel chemin est éligible pour être redistribué dans OSPF et que la configuration n'empêche pas une telle redistribution.

Si le chemin vient d'un domaine OSPF différent de celui de l'instance OSPF dans laquelle il est redistribué, ou si le chemin n'est pas du tout d'un domaine OSPF, alors le chemin est considéré comme un chemin externe.

Si le chemin est du même domaine OSPF que l'instance OSPF dans laquelle il est redistribué, et si il était à l'origine annoncé à un PE comme un chemin externe OSPF ou un chemin NSSA OSPF, il va être traité comme chemin externe. Suivant les procédures normales d'OSPF, les chemins externes peuvent être annoncés au CE dans des LSA de type 5, ou dans des LSA de type 7, ou pas du tout, selon le type de zone à laquelle appartient la liaison PE/CE.

Si le chemin est du même domaine OSPF que l'instance OSPF dans laquelle il est redistribué, et si il était à l'origine annoncé à un PE comme chemin inter zones ou intra zone, le chemin va généralement être annoncé au CE comme un chemin inter zones (dans une LSA de type 3).

Dans un cas particulier, supposons que PE1 se rattache à CE1, et que PE2 se rattache à CE2, où :
- l'instance OSPF contenant la liaison PE1-CE1 et l'instance OSPF contenant la liaison PE2-CE2 sont dans le même domaine OSPF, et
- les liaisons PE1-CE1 et PE2-CE2 sont dans la même zone OSPF A (comme déterminé par le numéro de zone OSPF configurée),

alors PE1 peut envoyer à CE1 une LSA de type 1 annonçant une liaison à PE2, et PE2 peut envoyer à CE2 une LSA de type 1 annonçant une liaison à PE1. La liaison annoncée dans ces LSA est appelée une "liaison factice", et elle est annoncée comme une liaison dans la zone A. Cela fait paraître aux routeurs qui sont dans la zone A comme si le chemin de CE1 à PE1 à travers le réseau du fournisseur de services de PE2 à CE2 était un chemin intra zone. Les liaisons factices sont une caractéristique FACULTATIVE de la présente spécification et sont utilisées seulement quand il est nécessaire d'avoir le réseau du fournisseur de services traité comme une liaison intra zone. Voir au paragraphe 4.2.7 plus de détails sur la liaison factice.

Les détails précis par lesquels un PE détermine le type de LSA utilisé pour annoncer un chemin particulier pour un CE sont spécifiés au paragraphe 4.2.8. Noter que si le VRF est associé à plusieurs instances OSPF, le type de LSA utilisé pour annoncer le chemin pourrait être différent dans différentes instances.

Noter que si un VRF est associé à plusieurs instances OSPF, un certain chemin peut être redistribué dans certaines ou dans toutes ces instances OSPF, selon les caractéristiques de chaque instance. Si il est redistribué dans deux instances OSPF ou plus, il peut être annoncé dans chaque instance en utilisant un type de LSA différent, là encore, selon les caractéristiques de chaque instance.

4.1.4 Les PE et la zone OSPF 0

Au sein d'un domaine OSPF donné, un PE peut se rattacher à plusieurs CE. Chaque liaison PE/CE est allouée (par configuration) à une zone OSPF. Toute liaison peut être allouée à toute zone, zone 0 incluse.

Si un PE se rattache à un CE qui est dans une zone non zéro, alors le PE sert d'ABR pour cette zone.

Les PE peuvent donc être considérés comme des "routeurs de zone 0" OSPF, c'est-à-dire, ils peuvent être considérés comme faisant partie du "réseau dorsal OSPF". Donc, il leur est permis de distribuer des chemins inter zones au CE via des LSA de type 3.

Si le domaine OSPF a des routeurs de zone 0 autres que les routeurs PE, au moins un d'eux DOIT alors être un routeur CE et DOIT avoir une liaison de zone 0 avec au moins un routeur PE. Cette adjacence PEUT être via une liaison virtuelle OSPF. (La capacité d'utiliser une liaison virtuelle OSPF de cette façon est une caractéristique FACULTATIVE.) Ceci est nécessaire pour assurer que les chemins inter-zones et les chemins externes à l'AS peuvent être écoulés entre les routeurs PE et le réseau dorsal OSPF non PE.

Deux sites qui ne sont pas dans la même zone OSPF vont voir le cœur de réseau de VPN comme faisant partie intégrante du réseau dorsal OSPF. Cependant, si il y a des routeurs de zone 0 qui NE sont PAS des routeurs PE, alors le cœur de réseau de VPN fonctionne en fait comme une sorte de réseau dorsal de niveau supérieur, fournissant un troisième niveau hiérarchique au dessus de la zone 0. Cela permet à un réseau dorsal OSPF traditionnel d'être déconnecté durant une période de transition, pour autant que les divers segments se rattachent tous au cœur de réseau de VPN.

4.1.5 Prévention des boucles

Si un chemin envoyé d'un routeur PE à un routeur CE pourrait alors être reçu par un autre routeur PE d'un de ses propres routeurs CE, il serait possible que des boucles d'acheminement se produisent. Pour empêcher cela, un PE établit le bit DN [RFC4576] dans toute LSA qu'il envoie à un CE, et un PE ignore toute LSA reçue d'un CE qui a déjà eu le bit DN envoyé. Les mises en œuvre plus anciennes peuvent, dans certains cas, utiliser une étiquette de chemin OSPF au lieu du bit DN. Voir les paragraphes 4.2.5.1 et 4.2.5.2.

4.2 Détails

4.2.1 Instances OSPF indépendantes dans les PE

Le PE DOIT prendre en charge une instance OSPF pour chaque domaine OSPF auquel il se rattache. Ces instances OSPF fonctionnent indépendamment et ne communiquent pas les chemins aux autres. Chaque instance d'OSPF DOIT être associée à un seul VRF. Si n CE associés à ce VRF fonctionnent sur OSPF sur leurs liaisons PE/CE respectives, ces n CE sont alors des adjacences OSPF du PE dans l'instance d'OSPF correspondante.

Généralement, bien que pas nécessairement, si le PE se rattache à plusieurs CE dans le même domaine OSPF, il va associer

les interfaces à ces PE à un seul VRF.

4.2.2 Identifiant de routeur

Si un PE et un CE communiquent via OSPF, le PE va avoir un identifiant de routeur OSPF qui est valide (c'est-à-dire, unique) dans le domaine OSPF. Plus précisément, chaque instance OSPF a un identifiant de routeur. Différentes instances OSPF peuvent avoir des identifiants de routeur différents.

4.2.3 Zones OSPF

Une liaison PE-CE peut être dans toute zone, zone 0 incluse ; c'est une question de configuration OSPF.

Si un PE a une liaison qui appartient à une zone non zéro, le PE fonctionne comme routeur de bordure de zone (ABR, *Area Border Router*) pour cette zone.

Les PE ne passent pas la topologie d'état de liaison d'un site à un autre (excepté dans le cas où une liaison factice est utilisée ; voir le paragraphe 4.2.7).

Selon le paragraphe 3.1 de la [RFC2328], "le réseau dorsal OSPF contient toujours tous les routeurs de bordure de zone". Les routeurs PE sont donc considérés comme des routeurs de zone 0. Le paragraphe 3.1 de la [RFC2328] exige aussi que la zone 0 soit contiguë. Il s'ensuit que si le domaine OSPF a des routeurs de zone 0 autres que les routeurs PE, au moins l'un d'eux DOIT être un routeur CE, et il DOIT avoir une liaison de zone 0 (éventuellement une liaison virtuelle) pour au moins un routeur PE.

4.2.4 Identifiants de domaine OSPF

Chaque instance OSPF DOIT être associée à un ou plusieurs identifiants de domaine. Ceci DOIT être configurable, et la valeur par défaut (si aucune n'est configurée) DEVRAIT être NUL.

Si une instance OSPF a plusieurs identifiants de domaine, l'un d'eux est considéré comme son identifiant de domaine "principal" ; ceci DOIT être déterminable par configuration. Si une instance OSPF a exactement un identifiant de domaine, il est bien sûr son identifiant de domaine principal. Si une instance OSPF a plus d'un identifiant de domaine, l'identifiant de domaine NUL NE DOIT PAS être l'un d'eux.

Si un chemin est installé dans un VRF par une instance OSPF particulière, l'identifiant de domaine principal de cette instance OSPF est considéré comme l'identifiant de domaine du chemin.

Considérons un chemin, R, qui est installé dans un VRF, par exemple OSPF I1, puis redistribué dans BGP comme chemin de VPN-IPv4, et ensuite installé par BGP dans un autre VRF. Si R a besoin d'être redistribué dans l'instance OSPF I2, associée au dernier VRF, la façon dont R est annoncé dans I2 va dépendre de si l'identifiant de domaine de R est un des identifiants de domaine de I2. Si l'identifiant de domaine de R n'est pas un des identifiants de domaine de I2, alors, si R est redistribué dans I2, R va être annoncé comme un chemin externe à l'AS, sans considération du type de chemin OSPF qu'il a. Si, par ailleurs, l'identifiant de domaine de R est un des identifiants de domaine de I2, la façon dont R est annoncé va dépendre du type de chemin OSPF de R.

Si deux instances OSPF sont dans le même domaine OSPF, alors, soit :
1. elles ont toutes deux l'identifiant de domaine NUL, SOIT
2. chaque instance OSPF a l'identifiant de domaine principal de l'autre comme un de ses propres identifiants de domaine.

Si deux instances OSPF sont dans des domaines OSPF différents, alors soit :
3. elles ont toutes deux l'identifiant de domaine NUL, SOIT
4. aucune instance OSPF n'a l'identifiant de domaine principal de l'autre comme un de ses propres identifiants de domaine.

(Noter que si deux instances OSPF ont chacune l'identifiant de domaine NUL, on ne peut pas dire à partir de l'identifiant de domaine si elles sont dans le même domaine OSPF. Si elles sont dans différents domaines, et si les chemins de l'une sont distribués dans l'autre, les chemins vont apparaître comme chemins intra-réseau, ce qui peut n'être pas ce qui est prévu.)

Un identifiant de domaine est une quantité de huit octets qui est un attribut valide de communautés BGP étendues comme spécifié au paragraphe 4.2.4. Si une certaine instance OSPF a un identifiant de domaine non NUL, quand les chemins

provenant de cette instance OSPF sont distribués par BGP comme chemins VPN-IPv4, les chemins DOIVENT porter l'attribut Communautés étendues d'identifiant de domaine qui correspond à l'identifiant de domaine principal de l'instance OSPF. Si l'identifiant de domaine de l'instance OSPF est NUL, l'attribut Communautés étendues d'identifiant de domaine PEUT être omis quand les chemins provenant de cette instance OSPF sont distribués par BGP ; autrement, une valeur de l'attribut Communautés étendues d'identifiant de domaine qui représente NUL (voir le paragraphe 4.2.4) PEUT être portée avec le chemin.

Si les instances OSPF d'un domaine OSPF portent un ou plusieurs identifiants de domaine non NULS, cette procédure nous permet de déterminer si un chemin de VPN-IPv4 particulier généré par OSPF appartient au même domaine qu'une certaine instance OSPF. On peut alors déterminer si le chemin devrait être redistribué à cette instance OSPF comme chemin inter zones ou comme chemin OSPF externe à l'AS. Les détails se trouvent aux paragraphes 4.2.4 et 4.2.8.1.

4.2.5 Prévention des boucles

4.2.5.1 Le bit DN

Quand une LSA de type 3 est envoyée d'un routeur PE à un routeur CE, le bit DN [RFC4576] dans le champ Options de la LSA DOIT être établi. C'est utilisé pour s'assurer que si un routeur CE envoie cette LSA de type 3 à un routeur PE, le routeur PE ne va pas la redistribuer plus loin.

Quand un routeur PE a besoin de distribuer à un routeur CE un chemin qui vient d'un site extérieur à son domaine OSPF, le routeur PE se présente comme un routeur bordure de système autonome (ASBR, *Autonomous System Border Router*) et distribue le chemin dans une LSA de type 5. Le bit DN [RFC4576] DOIT être établi dans ces LSA pour assurer qu'elle va être ignorée par tout autre routeur PE qui la reçoit.

Des mises en œuvre sont déployées qui n'établissent pas le bit DN, mais utilisent à la place l'étiquetage de chemin OSPF pour s'assurer qu'une LSA de type 5 générée par un routeur PE va être ignorée par tout autre routeur PE qui peut la recevoir. Une étiquette spéciale de chemin OSPF, qu'on appelle étiquette de chemin de VPN (voir le paragraphe 4.2.5.2) est utilisée à cette fin. Pour assurer la rétro compatibilité, toutes les mises en œuvre qui adhèrent à la présente spécification DOIVENT par défaut prendre en charge les procédures d'étiquette de chemin de VPN spécifiées aux paragraphes 4.2.5.2, 4.2.8.1, et 4.2.8.2. Quand il n'est plus nécessaire d'utiliser l'étiquette de chemin de VPN dans un déploiement particulier, son utilisation (en envoi et en réception) peut être désactivée par configuration.

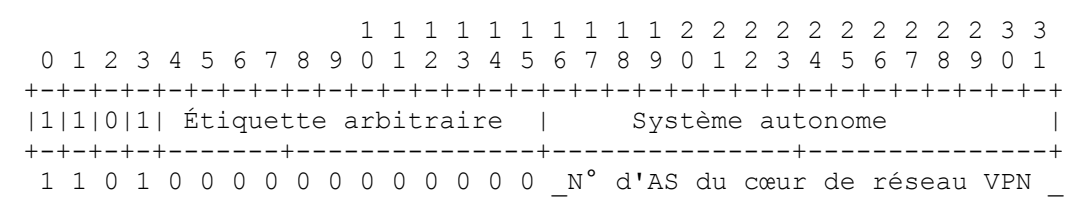
4.2.5.2 Utilisation des étiquettes de chemin OSPF

Si un VRF particulier dans un PE est associé à une instance d'OSPF, il DOIT alors par défaut être configuré avec une valeur spéciale d'étiquette de chemin OSPF, qu'on appelle étiquette de chemin de VPN. Par défaut, cette étiquette de chemin DOIT être incluse dans les LSA de type 5 que génère le PE (par suite de la réception d'un chemin de VPN-IPv4 distribué par BGP, voir au paragraphe 4.2.8) et qu'il envoie à tous les CE rattachés.

La configuration et l'inclusion de l'étiquette de chemin de VPN est requise pour la rétro compatibilité avec les mises en œuvre déployées qui n'établissent pas le bit DN dans les LSA de type 5. L'inclusion de l'étiquette de chemin de VPN peut être désactivée par configuration si il a été déterminé qu'elle n'est plus nécessaire pour la rétro compatibilité.

La valeur de l'étiquette de chemin de VPN est arbitraire mais doit être distincte de toute étiquette de chemin OSPF utilisée dans le domaine OSPF. Sa valeur DOIT donc être configurable. Si le numéro de système autonome du cœur de réseau de VPN est long de deux octets, la valeur par défaut DEVRAIT être une étiquette calculée automatiquement sur la base de ce numéro de système autonome :

Tag = <Automatic = 1, Complete = 1, PathLength = 01>



Si le numéro de système autonome est long de quatre octets, une valeur d'étiquette de chemin DOIT alors être configurée, et elle DOIT être distincte de toute étiquette de chemin utilisée dans le VPN lui-même.

Si un routeur PE a besoin d'utiliser OSPF pour distribuer à un routeur CE un chemin qui vient d'un site extérieur au domaine OSPF du routeur CE, le routeur PE DEVRAIT se présenter au routeur CE comme un ASBR et DEVRAIT rapporter de tels chemins comme chemins externes à l'AS. C'est-à-dire que ces routeurs PE génèrent des LSA de type 5 qui rapportent les chemins extra domaine comme chemins externes à l'AS. Chacune de ces LSA de type 5 DOIT contenir une étiquette de chemin OSPF dont la valeur est celle de l'étiquette de chemin de VPN. Cette étiquette identifie le chemin comme étant venu d'un routeur PE. L'étiquette de chemin de VPN DOIT être utilisée pour s'assurer qu'une LSA de type 5 générée par un routeur PE n'est pas redistribuée dans la zone OSPF à un autre routeur PE.

4.2.5.3 Autres boucles possibles

Les procédures spécifiées dans le présent document assurent que si les informations d'acheminement déduites d'un chemin de VPN-IPv4 distribué par BGP sont distribuées dans OSPF, elles ne peuvent pas être redistribuées dans BGP comme chemin de VPN-IPv4, tant que le bit DN et/ou l'étiquette de chemin de VPN sont maintenus dans le domaine OSPF. Cela n'élimine pas toutes les sources possibles de boucles. Par exemple, si un chemin de VPN-IPv4 BGP est distribué dans OSPF, puis distribué dans RIP (où toutes les informations nécessaires pour empêcher les boucles sont perdues) et ensuite redistribué dans OSPF, il est alors possible qu'il puisse être redistribué dans BGP comme chemin de VPN-IPv4, causant ainsi une boucle.

Donc, une vigilance extrême doit être de mise si il y a une redistribution mutuelle de chemins entre le domaine OSPF et tout domaine d'acheminement tiers (c'est-à-dire, non de cœur de réseau de VPN). Si le domaine d'acheminement tiers est un domaine BGP (par exemple, l'Internet public) les mesures ordinaires de prévention de boucle de BGP vont empêcher le chemin de revenir dans le domaine OSPF.

4.2.6 Traitement des LSA provenant du CE

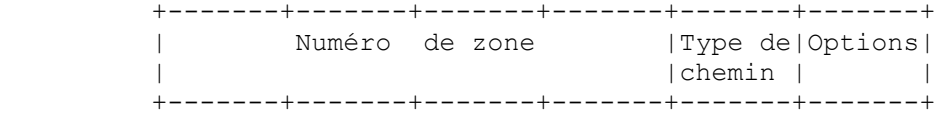
Ce paragraphe spécifie la façon dont un routeur PE traite les LSA OSPF qu'il reçoit d'un routeur CE.

Quand un routeur PE reçoit, d'un routeur CE, une LSA avec le bit DN [RFC4576] établi, les information provenant de cette LSA NE DOIVENT PAS être utilisées par le calcul de chemin. Si une LSA de type 5 est reçue du CE, et si elle a une valeur d'étiquette de chemin OSPF égale à l'étiquette de chemin de VPN (voir au paragraphe4.2.5.2) alors les informations provenant de cette LSA NE DOIVENT PAS être utilisées par le calcul de chemin.

Autrement, le PE doit examiner le VRF correspondant. Pour chaque préfixe d'adresse qui a été installé dans le VRF par une de ses instances OSPF associées, le PE doit créer un chemin de VPN-IPv4 dans BGP. Chacun de ces chemins va avoir les attributs Communautés étendues suivants :

- L'attribut Communautés étendues d'identifiant de domaine OSPF. Si l'instance OSPF qui a installé le chemin a un identifiant de domaine principal non NUL, il DOIT être présent ; si cette instance OSPF a seulement un identifiant de domaine NUL, il PEUT être omis. Cet attribut est codé avec un champ de type de deux octets, et son type est 0005, 0105, ou 0205. Pour la rétro compatibilité, le type 8005 PEUT être utilisé aussi et il est traité comme si c'était 0005. Si l'instance OSPF a un identifiant de domaine NUL, et si l'attribut Communautés étendues d'identifiant de domaine OSPF est présent, alors le champ Valeur de l'attribut doit être tout de zéros, et son champ Type peut être 0005, 0105, 0205, ou 8005.

- L'attribut Communautés étendues de type de chemin OSPF. Cet attribut DOIT être présent. Il est codé avec un champ Type de deux octets, et son type est 0306. Pour assurer la rétro compatibilité, le type 8000 DEVRAIT être accepté aussi et traité comme si c'était le type 0306. Les six octets restants de l'attribut sont codés comme suit :



* Numéro de zone : 4 octets, codant un numéro de zone de 32 bits. Pour les chemins externes à l'AS, la valeur est 0. Une valeur non zéro identifie le chemin comme étant interne au domaine OSPF, et comme étant dans la zone identifiée. Les numéros de zone sont relatifs à un domaine OSPF particulier.

* Type de chemin OSPF : 1 octet, codé comme suit :
** 1 ou 2 pour les chemins intra zone (selon que le chemin vient d'une LSA de type 1 ou de type 2).

** 3 pour les chemins inter zones.
** 5 pour les chemins externes (le numéro de zone doit être 0).
** 7 pour les chemins NSSA.

Noter que les procédures du paragraphe 4.2.8 ne font aucune distinction entre les chemins des types 1, 2, et 3. Si BGP installe un chemin d'un de ces types dans le VRF, et si ce chemin est choisi pour redistribution dans OSPF, il va être annoncé par OSPF dans une LSA de type 3 ou de type 5, selon l'identifiant de domaine.

* Options : 1 octet. Actuellement, ceci est seulement utilisé si le type de chemin est 5 ou 7. Établir le bit de moindre poids dans ce champ indique que le chemin porte une métrique de type 2.

- Attribut Communautés étendues d'identifiant de routeur OSPF. Cet attribut FACULTATIF spécifie l'identifiant de routeur OSPF du système qui est identifié dans l'attribut Prochain bond BGP. Plus précisément, il spécifie l'identifiant de routeur OSPF du PE dans l'instance OSPF qui a installé le chemin dans le VRF à partir duquel ce chemin a été exporté. Cet attribut est codé dans un champ de deux octets, et son type est 0107, avec l'identifiant de routeur lui-même porté dans les quatre premiers octets du champ Valeur. Le type 8001 DEVRAIT être accepté aussi, pour assurer la rétro compatibilité, et devrait être traité comme si c'était 0107.

- Attribut MED (Multi_EXIT_DISC). Par défaut, il DEVRAIT être réglé à la valeur de la distance OSPF associée au chemin, plus 1.

L'intention de tout cela est la suivante : les chemins OSPF provenant d'un site sont convertis en BGP, distribués à travers le cœur de réseau de VPN, et éventuellement reconvertis en chemins OSPF avant d'être distribués dans un autre site. Avec ces attributs, BGP porte assez d'informations sur le chemin pour lui permettre d'être reconverti en OSPF de façon "transparente", juste comme si BGP n'avait pas été impliqué.

Les chemins qu'un PE reçoit dans des LSA de type 4 NE DOIVENT PAS être redistribués à BGP.

Les attributs spécifié ci-dessus sont en plus de tous les autres attributs que les chemins doivent porter conformément à la [RFC4364].

L'attribut Site d'origine, qui est généralement exigé par la [RFC4364], est FACULTATIF pour les chemins qu'un PE apprend d'un CE via OSPF.

L'utilisation de l'attribut Site d'origine pourrait, dans le cas d'un site multi rattachements (c'est-à-dire, un site rattaché à plusieurs routeurs PE) empêcher qu'un chemin intra-site soit réinjecté dans un site à partir du cœur de réseau de VPN. Une telle réinjection n'endommagerait pas l'acheminement, parce que le chemin via le cœur de réseau de VPN serait annoncé dans une LSA de type 3, et donc apparaîtrait comme étant un chemin inter zones ; le chemin intra-zone réel va être préféré. Mais des frais généraux inutiles seraient introduits. Par ailleurs, si l'attribut Site d'origine n'est pas utilisé, un site partitionné va se trouver automatiquement réparé, car le trafic provenant d'une partition pour l'autre va automatiquement voyager via le cœur de réseau de VPN. Donc, l'utilisation d'un attribut Site d'origine est facultatif, de sorte qu'un compromis peut être fait entre le coût des frais généraux accrus et la valeur de la réparation automatique de partition.

4.2.7 Liaisons factices

Ce paragraphe décrit le protocole et les procédures nécessaires pour la prise en charge des "liaisons factices" *(Sham Links)* définies ici. La prise en charge des liaisons factices est une caractéristique FACULTATIVE de la présente spécification.

4.2.7.1 Chemins intra zone

Supposons qu'il y ait deux sites dans la même zone OSPF. Chaque site est rattaché à un routeur PE différent, et il y a aussi une liaison OSPF intra-zone qui connecte les deux sites.

Il est possible de traiter ces deux sites comme un seul site de VPN qui se trouve juste être multi rattachements au cœur de réseau. C'est en fait la chose la plus simple à faire et elle est parfaitement adéquate, pourvu que le chemin préféré entre les deux sites soit via la liaison intra-zone OSPF (une "liaison dérobée") plutôt que via le cœur de réseau de VPN. Il va y avoir des chemins entre les sites qui passent à travers les routeurs PE, mais ces chemins vont apparaître comme étant des chemins inter zones, et OSPF va les considérer comme moins préférables que les chemins intra-zone à travers la liaison dérobée.

Si il est désiré que OSPF préfère les chemins à travers le cœur de réseau plutôt que les chemins à travers la liaison dérobée, alors les chemins à travers le cœur de réseau doivent apparaître comme étant des chemins intra-zone. Pour faire qu'un chemin à travers le cœur de réseau apparaisse comme un chemin intra-zone, il est nécessaire de le faire apparaître comme si il y avait une liaison intra-zone connectant les deux routeurs PE. C'est ce qu'on appelle une "liaison factice". (Si les deux sites se rattachent au même routeur PE, ceci n'est bien sûr pas nécessaire.)

Une liaison factice peut être vue comme une relation entre deux VRF. Si deux VRF sont à connecter par une liaison factice, chaque VRF doit être associé à une "adresse de point d'extrémité de liaison factice", une adresse IPv4 de 32 bits qui est traitée comme une adresse du routeur PE contenant cette VRF. L'adresse de point d'extrémité de liaison factice est une adresse dans l'espace d'adresse du VPN, pas dans l'espace d'adresses du SP. L'adresse de point d'extrémité de liaison factice associée à un VRF DOIT être configurable. Si le VRF est associé à une seule instance OSPF, et si l'identifiant de routeur du PE dans cette instance OSPF est une adresse IP, alors l'adresse de point d'extrémité de liaison factice PEUT par défaut être cet identifiant de routeur. Si un VRF est associé à plusieurs instances OSPF, chaque liaison factice appartient à une seule instance OSPF.

Pour une certaine instance OSPF, un VRF a besoin seulement d'une seule adresse de point d'extrémité de liaison factice, quel que soit le nombre de liaisons factices qu'il a. L'adresse de point d'extrémité de liaison factice DOIT être distribuée par BGP comme une adresse de VPN-IPv4 dont la partie préfixe d'adresse IPv4 est de 32 bits. L'adresse de point d'extrémité de liaison factice NE DOIT PAS être annoncée par OSPF ; si il n’y a pas de chemin BGP pour l'adresse de point d'extrémité de liaison factice, cette adresse va apparaître comme injoignable, de sorte que la liaison factice va apparaître comme morte.

4.2.7.2 Création de liaisons factices

Les liaisons factices sont configurées manuellement.

Pour qu'une liaison factice existe entre deux VRF, chaque VRF doit être configuré à créer une liaison factice avec l'autre, où "l'autre" est identifié par son adresse de point d'extrémité de liaison factice. Pas plus d'une liaison factice avec la même paire d'adresses de point d'extrémité de liaison factice ne doit jamais être créée. La présente spécification n'inclut pas de procédures pour la configuration manuelle de liaison factice d'une seule extrémité.

Noter que des liaisons factices peuvent être créées pour toute zone, zone 0 incluse.

Une liaison factice connectant deux VRF est considérée comme active si et seulement si un chemin pour l'adresse de point d'extrémité distant de 32 bits de la liaison factice a été installé dans le VRF.

L'adresse de point d'extrémité de liaison factice NE DOIT PAS être utilisée comme adresse de point d'extrémité d'une liaison virtuelle OSPF.

4.2.7.3 Protocole OSPF sur liaisons factices

Un paquet de protocole OSPF envoyé sur une liaison factice d'un PE à un autre doit avoir comme adresse IP de source l'adresse de point d'extrémité de liaison factice de l'envoyeur, et comme adresse de destination IP l'adresse de point d'extrémité de liaison factice du receveur. Le paquet va voyager d'un routeur PE à l'autre sur le cœur de réseau de VPN, ce qui signifie qu'on peut s'attendre à ce qu'il traverse plusieurs bonds. À ce titre, son champ TTL (durée de vie) doit être réglé de façon appropriée.

Un paquet de protocole OSPF est considéré avoir été reçu sur une liaison factice particulière si et seulement si les trois conditions suivantes sont satisfaites :

- Le paquet arrive comme paquet MPLS, et sa pile d'étiquettes MPLS fait qu'il va être "livré" à l'adresse de point d'extrémité local de liaison factice.
- L'adresse de destination IP du paquet est l'adresse de point d'extrémité local de liaison factice.
- L'adresse IP de source du paquet est l'adresse de point d'extrémité distant de liaison factice.

Les liaisons factices DEVRAIENT être traitées par OSPF comme des circuits de demande OSPF. Cela signifie que les LSA vont être arrosées sur elles, mais le trafic de rafraîchissement périodique est évité. Noter que, tant que la liaison dérobée est active, l'arrosage de LSA sur la liaison factice ne sert à rien. Cependant, si la liaison dérobée a une défaillance, OSPF n'a pas de mécanisme permettant aux routeurs dans un site de purger rapidement les LSA provenant de l'autre site. Donc, il est quand même nécessaire de conserver la synchronisation entre les bases de données de LSA aux deux sites, et donc l'arrosage sur la liaison factice.

La liaison factice est une liaison non numérotée point à point intra-zone et est annoncée comme liaison de type 1 dans une LSA de type 1.

La métrique OSPF associée à une liaison factice DOIT être configurable (et il DOIT y avoir une configuration par défaut). Si le trafic entre les sites s'écoule via une liaison dérobée ou via le cœur de réseau de VPN (c'est-à-dire, via la liaison factice) dépend des réglages de la métrique de liaison OSPF. Les métriques peuvent être réglées de telle sorte que la liaison dérobée ne soit pas utilisée sauf si, par exemple, la connexité via le cœur de réseau de VPN est défaillante.

L'intervalle de Hello par défaut pour les liaisons factices est de 10 secondes, et l'intervalle par défaut de routeur mort pour les liaisons factices est de 40 secondes.

4.2.7.4 Acheminement et transmission sur liaisons factices

Si un PE détermine que l'interface de prochain bond pour un chemin particulier est une liaison factice, alors le PE NE DEVRAIT PAS redistribuer ce chemin dans BGP comme chemin de VPN-IPv4.

Tout autre chemin annoncé dans une LSA qui est transmise sur une liaison factice DOIT aussi être redistribuée (par le PE qui arrose la LSA sur la liaison factice) dans BGP. Cela signifie que si le chemin préféré (OSPF) pour un certain préfixe d'adresse a la liaison factice comme interface de prochain bond, alors il va aussi y avoir un "chemin BGP correspondant", pour ce même préfixe d'adresse, installé dans le VRF. Selon le paragraphe 4.1.2, le chemin OSPF est préféré. Cependant, quand on transmet un paquet, si le chemin préféré pour ce paquet a la liaison factice comme interface de prochain bond, le paquet DOIT alors être transmis suivant le chemin BGP correspondant. C'est-à-dire, il va être transmis comme si le chemin BGP correspondant était le chemin préféré. Le "chemin BGP correspondant" est toujours un chemin de VPN-IPv4 ; la procédure pour transmettre un paquet sur un chemin de VPN-IPv4 est décrite dans la [RFC4364].

Cette même règle s'applique à tout paquet dont l'adresse de destination IP est l'adresse de point d'extrémité distant d'une liaison factice. De tels paquets DOIVENT être transmis en accord avec le chemin BGP correspondant.

4.2.8 Chemins VPN-IPv4 reçus via BGP

Ce paragraphe décrit comment le routeur PE traite les chemins VPN-IPv4 reçus via BGP.

Si un chemin de VPN-IPv4 reçu par BGP n'est pas installé dans le VRF, rien n'est rapporté au CE. Un chemin reçu ne sera pas installé dans le VRF si le processus de décision BGP considère qu'un autre chemin est préférable. Quand il est installé dans le VRF, le chemin apparaît comme étant un chemin IPv4.

Un chemin BGP installé dans le VRF n'est pas nécessairement utilisé pour la transmission. Si un chemin OSPF pour le même préfixe d'adresse IPv4 a été installé dans le VRF, le chemin OSPF va être utilisé pour la transmission, sauf dans le cas où l'interface de prochain bond du chemin OSPF est une liaison factice.

Si un chemin BGP installé dans le VRF est utilisé pour la transmission, alors le chemin BGP est redistribué dans OSPF et éventuellement rapporté aux CE dans une LSA OSPF. La sorte de LSA, si il en est, à générer dépend de diverses caractéristiques du chemin BGP, détaillées dans les paragraphes suivants de ce document.

La procédure pour transmettre un paquet sur un chemin de VPN-IPv4 est décrite dans la [RFC4364].

Dans ce qui suit, on spécifie ce qui est rapporté, dans les LSA OSPF, par le PE au CE, en supposant que le PE n'est pas configuré à faire plus de résumé ou filtrage des informations d'acheminement avant le rapport au CE.

Quand il y a envoi d'une LSA au CE, il peut être nécessaire d'établir le bit DN. Voir au paragraphe 4.2.5.1 les règles concernant le bit DN.

Lors de l'envoi d'une LSA au CE, il peut être nécessaire d'établir l'étiquette de chemin OSPF. Voir au paragraphe 4.2.5.2 les règles d'établissement de l'étiquette de chemin OSPF.

Quand des LSA de type 5 sont envoyées, l'adresse de transmission est réglée à 0.

4.2.8.1 Chemins externes

Par rapport à une instance OSPF particulière associée à un VRF, un chemin de VPN-IPv4 qui est installé dans le VRF et ensuite choisi comme chemin préféré est traité comme chemin externe si une des conditions suivantes tient :
- Le champ Type de chemin de la communauté étendue de type de chemin OSPF a un type de chemin OSPF de "externe".
- Le chemin vient d'un domaine différent du domaine de l'instance OSPF.

Les règles pour déterminer si un chemin est d'un domaine différent de celui d'une certaine instance OSPF sont les suivantes. L'attribut Communautés étendues d'identifiant de domaine OSPF porté par le chemin est comparé avec le ou les attributs Communautés étendues d'identifiant de domaine OSPF avec lesquels l'instance OSPF a été configurée (si il en est). En général, quand deux de ces attributs sont comparés, tous les huit octets doivent être comparés. Donc, deux attributs Communautés étendues d'identifiant de domaine OSPF sont considérés comme égaux si et seulement si une des trois conditions suivantes est satisfaite :
1. Ils sont identiques sur tous les huit octets.
2. Ils sont identiques dans leurs six octets (champ Valeur) de moindre poids, mais un attribut a deux octets de poids fort (champ Type) de 0005 et l'autre a deux octets de poids fort (champ Type) de 8005. (Cette condition est pour la rétro compatibilité.)
3. Les six octets de moindre poids (champ Valeur) de deux attributs consistent entièrement en des zéros. Dans ce cas, les deux attributs sont considéré comme identiques sans considération de leurs champs Type, et ils sont considérés comme représentant l'identifiant de domaine NUL.

Si un chemin de VPN-IPv4 a un attribut Communautés étendues d'identifiant de domaine OSPF, on dit que ce chemin est dans le domaine identifié. Si le champ Valeur de l'attribut Communautés étendues consiste en zéros, alors le domaine identifié est le domaine NUL, et le chemin est dit appartenir au domaine NUL. Si le chemin n'a pas un attribut Communautés étendues de domaine identifié OSPF, alors le chemin appartient au domaine NUL.

Chaque instance OSPF est associée à un ou plusieurs identifiants de domaine, bien qu'éventuellement seulement à l'identifiant de domaine NUL. Si une instance OSPF est associée à un identifiant de domaine particulier, on dira qu'il appartient au domaine identifié.

Si un chemin de VPN-IPv4 est à redistribuer à une instance particulière, il doit être déterminé si ce chemin et cette instance OSPF appartiennent au même domaine. Un chemin et une instance OSPF appartiennent au même domaine si et seulement si une des conditions suivantes est satisfaite :
1. Le chemin et l'instance OSPF appartiennent chacun au domaine NUL.
2. Le domaine auquel le chemin appartient est le domaine auquel l'instance OSPF appartient. (C'est-à-dire, l'identifiant de domaine du chemin est égal à l'identifiant de domaine de l'instance OSPF, comme déterminé par les définitions données plus haut.)

Si le chemin et le VRF n'appartiennent pas au même domaine, le chemin est traité comme chemin externe.

Si un chemin externe est redistribué dans une instance OSPF, le chemin peut ou non être annoncé à un CE particulier, selon la configuration et le type de zone auxquels la liaison PE/CE appartient. Si le chemin est annoncé, et si la liaison PE/CE appartient à une zone NSSA, il est annoncé dans une LSA de type 7. Autrement, si le chemin est annoncé, il est annoncé dans une LSA de type 5. La LSA va être générée par le PE.

Le bit DN (paragraphe 4.2.5.1) DOIT être établi dans la LSA. L'étiquette de chemin de VPN (voir le paragraphe 4.2.5.2) DOIT être placée dans la LSA, sauf si l'utilisation de l'étiquette de chemin de VPN a été supprimée par configuration.

Par défaut, une valeur de métrique de type 2 est incluse dans la LSA, sauf si le champ Options de l'attribut Communautés étendues de type de chemin OSPF du chemin de VPN-IPv4 spécifie que la métrique devrait être de type 1.

Par défaut, la valeur de la métrique est tirée de l'attribut MED du chemin de VPN-IPv4. Si MED est absent, une valeur de métrique par défaut est utilisée. (La métrique par défaut de type 1 et de type 2 PEUVENT être différentes.)

Noter que cette façon de traiter les chemins externes fait que chaque PE paraît être un ASBR rattaché à tous les chemins externes. Dans un site multi rattachements, il peut en résulter qu'un certain nombre de LSA de type 5 contiennent les mêmes informations.

4.2.8.2 Chemins résumés

Si un chemin et le VRF dans lequel il est importé appartiennent au même domaine, le chemin devrait alors être traité

comme si il avait été reçu dans une LSA OSPF de type 3. Cela signifie que le PE va rapporter le chemin dans une LSA de type 3 au CE. (Noter que ce cas est possible même si le chemin de VPN-IPv4 porte un numéro de zone identique à celui du routeur CE. Cela signifie que si une zone est "partitionnée" de telle sorte que les deux pièces sont connectée seulement via le cœur de réseau de VPN, elle apparaît comme étant deux zones, avec des chemins inter zones entre elles.)

4.2.8.3 Chemins NSSA

Les chemins NSSA sont traités de la même façon que les chemins externes, comme décrit au paragraphe 4.2.8.1.

5. Considérations relatives à l'IANA

La Section 11 de la [RFC4360] invite l'IANA à créer un registre pour les valeurs de champ Type de communautés étendues BGP et Type étendu. Le paragraphe 4.2.6 du présent document alloue de nouvelles valeurs pour le champ Type de communautés étendues BGP. Ces valeurs sont toutes dans la gamme de valeurs que la [RFC4360] déclare comme "sont à allouer par l'IANA, en utilisant la politique de "premier arrivé, premier servi" définie dans la RFC 2434".

Les valeurs de champ Type de communautés étendues BGP allouées au paragraphe 4.2.6 de ce document sont les suivantes :
- identifiant de domaine OSPF : types étendus 0005, 0105, et 0205.
- type de chemin OSPF : type étendu 0306
- identifiant de routeur OSPF : type étendu 0107

6. Considérations sur la sécurité

Les considérations de sécurité qui sont pertinentes en général pour les VPN IP BGP/MPLS sont discutées dans les [RFC4364] et [RFC4365]. On discute seulement ici les considérations de sécurité qui sont spécifiques de l'utilisation de OSPF comme protocole de PE/CE.

Un seul PE peut faire fonctionner OSPF comme IGP du cœur de réseau de SP, ainsi que faire fonctionner OSPF comme IGP de un ou plusieurs VPN. Cela exige l'utilisation de plusieurs instances OSPF indépendantes, afin que les chemins ne soient pas par inadvertance confondus entre le cœur de réseau et un VPN. Les instances OSPF pour les différents VPN doivent aussi être des instances OSPF indépendantes, pour prévenir des fuites par inadvertance de chemins entre VPN.

OSPF fournit un certain nombre de procédures qui permettent que les messages de commande OSPF entre un PE et un CE soient authentifiées. L'authentification cryptographique OSPF DEVRAIT être utilisée entre un PE et un CE. Elle DOIT être mise en œuvre sur chaque PE.

En l'absence d'une telle authentification, il est possible que le CE n'appartienne pas réellement au VPN auquel le PE l'alloue. Il est aussi possible à un attaquant d'insérer des messages usurpés sur la liaison PE/CE, dans l'une ou l'autre direction. Les messages usurpés envoyés au CE pourraient compromettre l'acheminement au site du CE. Les messages usurpés envoyés au PE pourraient résulter en un acheminement impropre du VPN, ou en une attaque de déni de service sur le VPN.

7. Remerciements

Des contributions majeures au présent travail ont été faites par Derek Yeung et Yakov Rekhter.
Merci à Ross Callon, Ajay Singhal, Russ Housley, et Alex Zinin pour leur relecture et leurs commentaires.

8. 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)

[RFC2328] J. Moy, "OSPF version 2", STD 54, avril 1998. *(MàJ par la* RFC6549, RFC8042)

[RFC4360] S. Sangli et autres, "Attribut BGP-4 Communauté étendue", février 2006. *(P.S.)*

[RFC4364] E. Rosen et Y. Rekhter, "Réseaux privés virtuels IP BGP/MPLS", février 2006. (*P.S., MàJ par* RFC4577, RFC4684)

[RFC4576] E. Rosen et autres, "Utilisation d'un bit d'option d'annonce d'état de liaison (LSA) pour empêcher les boucles dans les réseaux privés virtuels (VPN) IP BGP/MPLS", juin 2006. *(P.S.)*

9. Références pour information

[RFC2453] G. Malkin, "RIP version 2", STD 56, novembre 1998. *(Mise à jour par la RFC 4822)*

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608, RFC8212)

[RFC4365] E. Rosen, "Déclaration d'applicabilité pour les réseaux privés virtuels (VPN) IP BGP/MPLS", février 2006. *(Info.)*

Adresse des auteurs

Eric C. Rosen
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
USA
mél : erosen@cisco.com

Peter Psenak
Cisco Systems
BA Business Center, 9th Floor
Plynarenska 1
Bratislava 82109
Slovakia
mél : ppsenak@cisco.com

Padma Pillay-Esnault
Cisco Systems
3750 Cisco Way
San Jose, CA 95134
USA
mél : ppe@cisco.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.