Groupe de travail Réseau
Request for Comments : 4659
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. De Clercq, Alcatel
D. Ooms, OneSparrow
M. Carugi, Nortel Networks
F. Le Faucheur, Cisco Systems
septembre 2006

Extension de réseau privé virtuel (VPN) IP BGP-MPLS pour VPN IPv6

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit une méthode par laquelle un fournisseur de services peut utiliser son cœur de réseau de commutation de paquets pour fournir des services de réseau privé virtuel (VPN, *Virtual Private Network*) à ses clients IPv6. Cette méthode réutilise, et étend quand nécessaire, la méthode du "VPN IP BGP/MPLS" pour la prise en charge de IPv6. Dans le VPN IP BGP/MPLS, "BGP multi protocoles" est utilisé pour distribuer les chemins de VPN IPv4 sur le cœur de réseau du fournisseur de services, et MPLS est utilisé pour transmettre les paquets de VPN IPv4 sur le cœur de réseau. Le présent document définit une famille d'adresses de VPN IPv6 et décrit la distribution correspondante de chemin de VPN IPv6 dans "BGP multi protocoles".

Le présent document définit la prise en charge du service de VPN IPv6 sur les cœurs de réseau IPv4 et IPv6, et l'utilisation de diverses techniques de tunnelage sur le cœur, incluant MPLS, IP dans IP, l'encapsulation d'acheminement générique (GRE, *Generic Routing Encapsulation*) et les tunnels protégés par IPsec. L'interfonctionnement entre un site IPv4 et un site IPv6 sort du domaine d'application de ce document.

Table des matières

1. Introduction

Le présent document décrit une méthode par laquelle un fournisseur de services peut utiliser son cœur de réseau de commutation de paquets pour fournir des services de réseau virtuel privé à ses clients IPv6.

Cette méthode réutilise, et étend lorsque nécessaire, la méthode du "VPN IP BGP/MPLS" de la [RFC4364] pour la prise en charge de IPv6. En particulier, cette méthode utilise le même "modèle d'échange de trafic" que la [RFC4364], dans laquelle les routeurs côté client ("routeurs CE") envoient leurs chemins IPv6 aux routeurs côté fournisseur de services ("routeurs PE"). BGP ("Border Gateway Protocol", [RFC2858], [RFC4271]) est alors utilisé par le fournisseur de services pour échanger les chemins d'un VPN IPv6 particulier avec les routeurs PE qui sont rattachés à ce VPN IPv6. Finalement, les routeurs PE distribuent aux routeurs CE dans un VPN particulier, les chemins IPv6 provenant des autres routeurs CE dans ce VPN. Comme avec les VPN IPv4, une caractéristique clé de ce "modèle d'échange de trafic" est que les routeurs CE (IPv6) au sein d'un VPN (IPv6) n'échangent pas de trafic les uns avec les autres ; il n'y a pas de "recouvrement" visible pour l'algorithme d'acheminement des VPN (IPv6).

Le présent document adopte les définitions, acronymes, et mécanismes décrits dans la [RFC4364]. Sauf mention contraire, les mécanismes de la [RFC4364] s'appliquent et ne sont pas re-décrits ici.

Un VPN est dit être un VPN IPv6 quand chaque site de ce VPN est à capacité IPv6 et est nativement connecté sur une interface ou sous interface IPv6 au cœur de réseau du fournisseur de services (SP) via un appareil côté fournisseur (PE, *Provider Edge*).

Un site peut être à la fois à capacité IPv4 et à capacité IPv6. L'interface logique sur laquelle les paquets arrivent au PE peuvent déterminer la version IP. Autrement, la même interface logique peut être utilisée pour IPv4 et IPv6, auquel cas une recherche par paquet dans le champ Version de l'en-tête du paquet IP va déterminer la version IP.

Le présent document ne s'occupe que du traitement des communications IPv6 entre hôtes IPv6 situés sur des sites à capacité IPv6. Le traitement de communication IPv4 entre hôtes IPv4 situés sur des sites à capacité IPv4 sort du domaine d'application du présent document et est couvert dans la [RFC4364]. La communication entre un hôte IPv4 situé dans un site à capacité IPv4 et un hôte IPv6 situé dans un site à capacité IPv6 sort du domaine d'application du présent document.

De la même façon que les chemins de VPN IPv4 sont distribués dans la [RFC4364], BGP et ses extensions sont utilisés pour distribuer les chemins d'un site de VPN IPv6 à tous les autres routeurs PE connectés à un site du même VPN IPv6. Les PE utilisent des "tableaux d'acheminement et de transmission de VPN" (VRF, *VPN Routing et Forwarding table*) pour maintenir les informations d'accessibilité et les informations de transmission de chaque VPN IPv6 séparément.

Comme il est fait pour les VPN IPv4 [RFC4364], on permet que chaque VPN IPv6 ait son propre espace d'adresses IPv6, ce qui signifie qu'une adresse donnée peut noter différents systèmes dans des VPN différents. Ceci est réalisé via une nouvelle famille d'adresses, la famille d'adresses VPN-IPv6, de façon similaire à celle d'une famille d'adresses de VPN-IPv4, définie dans la [RFC4364], qui ajoute un discriminant de chemin devant l'adresse IP.

En plus de son fonctionnement sur les chemins commutés d'étiquette MPLS (LSP, *Label Switched Path*) la solution de VPN IPv4 BGP/MPLS a été étendue pour permettre le fonctionnement sur d'autres techniques de tunnelage, incluant des tunnels GRE, des tunnels IP dans IP [RFC4797], des tunnels L2TPv3 [RFC4817], et des tunnels protégés par IPsec [2547-IPsec]. De manière similaire, le présent document permet la prise en charge d'un service de VPN IPv6 sur des LSP MPLS, ainsi que sur d'autres techniques de tunnelage.

Le présent document permet la prise en charge d'un service de VPN IPv6 sur un cœur de réseau IPv4, ainsi que sur un cœur de réseau IPv6. Le service de VPN IPv6 pris en charge est identique dans les deux cas.

La solution de VPN IPv6 définie dans le présent document offre les avantages suivants :

- Du point de vue aussi bien du fournisseur de services que du consommateur, le service de VPN qui peut être pris en charge pour les sites IPv6 est identique à celui qui peut être pris en charge pour les sites IPv4.

- Du point de vue du fournisseur de services, les opérations du service de VPN IPv6 exigent exactement les mêmes facilités, procédures, et mécanismes que ceux du service de VPN IPv4.

- Lorsque les services de VPN IPv4 et de VPN IPv6 sont tous deux pris en charge sur un cœur IPv4, le même ensemble de relations d'échange de trafic MP-BGP et le même maillage de tunnel PE-PE PEUVENT être utilisés pour les deux.

o Le service de VPN IPv6 est indépendant du fonctionnement du cœur sur IPv4 ou IPv6. Ceci est tel que le service de VPN IPv6 pris en charge avant et après une migration du cœur de IPv4 à IPv6 est indistinguable pour le client de VPN.

Noter que la prise en charge des services de VPN IPv4 sur un cœur IPv6 n'est pas couverte par ce document.

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

2. Famille d'adresses VPN-IPv6

Les extensions multi protocoles pour BGP [RFC2858] permettent à BGP de porter des chemins provenant de plusieurs "familles d'adresses". On introduit la notion de "famille d'adresses VPN-IPv6", qui est similaire à la famille d'adresses VPN-IPv4 introduite dans la [RFC4364].

Une adresse VPN-IPv6 est une quantité de 24 octets qui commence par un "discriminant de chemin" (RD, *Route Distinguisher*) de 8 octets et qui se termine par une adresse IP de 16 octets.

L'objet du RD est seulement de permettre de créer des chemins distincts pour un préfixe d'adresse IP commun, qui est similaire au propos du RD défini dans la [RFC4364]. De la même façon qu'il est possible selon la [RFC4364], le RD peut être utilisé pour créer plusieurs chemins différents pour le même système. Ceci peut être réalisé en créant deux chemins de VPN IPv6 différents qui ont la même partie IPv6 mais des RD différents. Cela permet au BGP du fournisseur d'installer plusieurs chemins différents pour le même système et aux politiques d'être utilisées pour décider quels paquets utiliser avec quel chemin.

Aussi, si deux VPN se trouvent utiliser le même préfixe d'adresse IPv6 (notant effectivement des systèmes physiques différents) les PE traduiraient cela en préfixes d'adresse uniques de VPN-IPv6 en utilisant des RD différents. Cela assure que si la même adresse est utilisée dans deux VPN différents, il est possible d'installer deux chemins complètement différents pour cette adresse, un pour chaque VPN.

Comme les adresses de VPN-IPv6 et les adresses IPv6 appartiennent à des familles d'adresses différentes, BGP ne les traite jamais comme des adresses comparables.

Un VRF peut avoir plusieurs chemins de VPN IPv6 de coût égal pour un seul préfixe d'adresse IPv6. Quand l'adresse de destination d'un paquet est confrontée dans un VRF à un chemin VPN-IPv6, seule la partie IPv6 est en fait confrontée.

Le format et le codage du discriminant de chemin sont comme spécifiés dans la [RFC4364].

Quand un site est à capacité IPv4 et IPv6, le même RD PEUT être utilisé pour l'annonce des adresses IPv6 et IPv4. Autrement, un RD différent PEUT être utilisé pour l'annonce des adresses IPv4 et des adresses IPv6. Noter, cependant, que dans la perspective de la présente spécification, les adresses IPv6 et IPv4 vont toujours être traitées dans des contextes séparés, et qu'aucune question et technique d'inter fonctionnement IPv4-IPv6 ne sera discutée.

3. Distribution des chemins de VPN-IPv6

3.1 Distribution des chemins parmi les PE par BGP

Comme décrit dans la [RFC4364], si deux sites d'un VPN se rattachent aux PE qui sont dans le même système autonome, les PE peuvent distribuer les chemins de VPN à chaque autre au moyen d'une connexion du protocole de passerelle bordure interne (iBGP, *internal Border Gateway Protocol*) (IPv4) entre eux. Autrement, chacun peut avoir des connexions iBGP à des réflecteurs de chemin. De même, pour la distribution de chemin de VPN IPv6, les PE peuvent utiliser des connexions iBGP entre eux ou utiliser des connexions iBGP à des réflecteurs de chemin. Pour le VPN IPv6, les connexions iBGP PEUVENT être sur IPv4 ou sur IPv6.

Les routeurs PE échangent, via MP-BGP [RFC2858], des informations d'accessibilité pour les préfixes IPv6 dans les VPN IPv6 et par là s'annoncent eux-mêmes comme prochain bond BGP.

Les règles de codage des informations d'accessibilité et de l'adresse de prochain bond BGP sont spécifiées dans les paragraphes suivants.

3.2 Codage de NLRI de VPN IPv6

Lorsque il distribue les chemins de VPN IPv6, le routeur PE annonceur DOIT allouer et distribuer les étiquettes MPLS avec les chemins de VPN IPv6. Essentiellement, les routeurs PE ne distribuent pas les chemins de VPN IPv6, mais les chemins de VPN IPv6 étiquetés [RFC3107]. Quand le PE annonceur reçoit ensuite un paquet qui a cette étiquette particulière annoncée, le PE va faire sauter cette étiquette de la pile MPLS et traiter le paquet de façon appropriée (c'est-à-dire, le transmettre directement conformément à l'étiquette ou effectuer une recherche dans le contexte IPv6-VPN correspondant).

Les extensions multi protocoles de BGP [RFC2858] sont utilisées pour annoncer les chemins de VPN IPv6 dans les mêmes informations d'accessibilité de couche réseau (NLRI, *Network Layer Reachability Information*) MP_REACH. Les champs Identifiant de famille d'adresse (AFI, *Address Family Identifier*) et Identifiant suivant de famille d'adresse (SAFI, *Subsequent Address Family Identifier*) DOIVENT être réglés comme suit :

- AFI : 2 ; pour IPv6
- SAFI : 128 ; pour VPN-IPv6 étiqueté MPLS

Le champ NLRI lui-même est codé comme spécifié dans la [RFC3107]. Dans le contexte de cette extension, le préfixe appartient à la famille d'adresses VPN-IPv6 et consiste donc en un discriminant de chemin de 8 octets suivi par un préfixe IPv6 comme spécifié à la Section 2, ci-dessus.

3.2.1 Codage du prochain bond BGP

Le codage du prochain bond BGP dépend de si la politique du locuteur BGP est de demander que le trafic de ce VPN IPv6 soit transporté à ce prochain bond BGP en utilisant le tunnelage IPv6 ("locuteur BGP demandant le transport IPv6") ou en utilisant le tunnelage IPv4 ("locuteur BGP demandant le transport IPv4").

La définition de cette politique (de demander le transport sur le tunnelage IPv4 ou le tunnelage IPv6) est de la responsabilité de l'opérateur du réseau et sort du domaine d'application du présent document. Noter qu'il est possible que cette politique demande le transport sur tunnelage IPv4 (respectivement, IPv6) tandis que les locuteurs BGP échangent des informations d'accessibilité de VPN IPv6 sur IPv6 (respectivement, IPv4). Cependant, dans ce cas, un certain nombre d'implications opérationnelles valent d'être considérées. En particulier, une faute non détectée qui affecte le chemin de données du tunnelage IPv4 (respectivement, IPv6) et qui n'affecte pas le chemin de données IPv6 (respectivement, IPv4) pourrait rester indétectée par BGP, ce qui à son tour peut résulter en ce que le trafic tombe dans un trou noir.

Le contrôle de cette politique sort du domaine d'application de ce document et peut se fonder sur la configuration de l'utilisateur.

3.2.1.1 Locuteur BGP demandant le transport IPv6

Quand le trafic de VPN IPv6 est à transporter au locuteur BGP en utilisant le tunnelage IPv6 (par exemple, des LSP MPLS IPv6, des tunnels IPv6 protégés par IPsec) le locuteur BGP DEVRA annoncer un champ Adresse réseau de prochain bond contenant une adresse de VPN-IPv6,
- dont le RD de 8 octets est réglé à zéro, et
- dont l'adresse IPv6 de 16 octets est réglée à l'adresse IPv6 mondiale du locuteur BGP annonceur.

Ceci est potentiellement suivi par une autre adresse de VPN-IPv6,
- dont le RD de 8 octets est réglé à zéro, et
- dont l'adresse IPv6 de 16 octets est réglée à l'adresse IPv6 de liaison locale du locuteur BGP annonceur.

La valeur de la longueur du champ Adresse réseau de prochain bond dans l'attribut MP_REACH_NLRI devra être réglée à 24 quand seulement une adresse mondiale est présente, et à 48 si une adresse de liaison locale est aussi incluse dans le champ Prochain bond.

Si les homologues locuteurs BGP utilisent seulement leur adresse IPv6 de liaison locale (par exemple, dans le cas où un CE IPv6 échange du trafic avec un PE IPv6, où le CE n'a aucune adresse mondiale IPv6, et où l'échange de trafic eBGP est

réalisé sur les adresses de liaison locale) l'adresse inspécifiée de la [RFC4291] est utilisée par le locuteur BGP annonceur pour indiquer l'absence de l'adresse mondiale IPv6 dans le champ Adresse réseau de prochain bond.

L'adresse de liaison locale devra être incluse dans le champ Prochain bond si et seulement si le locuteur BGP annonceur partage un sous réseau commun avec l'homologue sur le chemin annoncé [RFC2545].

Dans tous les autres cas, un locuteur BGP devra annoncer à son homologue dans le champ Adresse réseau de prochain bond seulement l'adresse mondiale IPv6 du prochain bond.

Par conséquent, un locuteur BGP qui annonce un chemin à un homologue interne peut modifier l'adresse réseau du champ Prochain bond en retirant l'adresse IPv6 de liaison locale du prochain bond.

Un exemple de scénario où les deux adresses mondiale IPv6 et de liaison locale devront être incluses dans le champ Adresse de prochain bond BGP est lorsque le service de VPN IPv6 est pris en charge sur un cœur de réseau multi systèmes autonomes (AS) avec redistribution des chemins de VPN IPv6 étiquetés entre les routeurs de bordure de système autonome (ASBR, *Autonomous System Border Router*) des différents AS qui partagent un sous réseau IPv6 commun : dans ce cas, les deux adresses IPv6 mondiale et de liaison locale devront être annoncées par les ASBR.

3.2.1.2 Locuteur BGP demandant le transport IPv4

Quand le trafic de VPN IPv6 est à transporter au locuteur BGP en utilisant le tunnelage IPv4 (par exemple, des LSP MPLS IPv4 , des tunnels IPv4 protégés par IPsec) le locuteur BGP DEVRA annoncer à son homologue un champ Adresse réseau de prochain bond contenant une adresse de VPN-IPv6 :
- dont le RD de 8 octets est réglé à zéro, et
- dont l'adresse IPv6 de 16 octets est codée comme une adresse IPv6 transposée en IPv4 [RFC4291] contenant l'adresse IPv4 du locuteur BGP annonceur. Cette adresse IPv4 doit être acheminable par l'autre locuteur BGP.

3.3 Chemin cible

L'utilisation de chemin cible est spécifié dans la [RFC4364] et s'applique aux VPN IPv6. Le codage de l'attribut communauté étendue est défini dans la [RFC4360].

3.4 Négociation de capacités BGP

Afin que deux PE échangent des NLRI étiquetés de VPN IPv6, ils DOIVENT utiliser la négociation de capacités BGP pour s'assurer qu'ils sont tous deux capables de traiter de façon appropriée de tels NLRI. Ceci est fait comme spécifié dans les [RFC2858] et [RFC3392], en utilisant le code de capacité 1 (multi protocoles BGP) avec les valeurs de AFI et SAFI spécifiées au paragraphe 3.2.

4. Encapsulation

Le routeur PE d'entrée DOIT tunneler les données de VPN IPv6 sur le cœur de réseau vers le routeur PE de sortie identifié comme prochain bond BGP pour le préfixe correspondant de destination de VPN IPv6.

Quand l'adresse IPv6 de 16 octets contenue dans le champ Prochain bond BGP est codée comme adresse IPv6 transposée en IPv4 (voir au paragraphe 3.2.1.2) le PE d'entrée DOIT utiliser le tunnelage IPv4 sauf si il est explicitement configuré à faire autrement. Le PE d'entrée PEUT facultativement permettre, par une configuration explicite, l'utilisation du tunnelage IPv6 quand l'adresse IPv6 de 16 octets contenue dans le champ Prochain bond BGP est codée comme adresse IPv6 transposée en IPv4. Cela va permettre la prise en charge d'environnements de déploiement particuliers où le tunnelage IPv6 est désiré mais où des adresses IPv6 transposées en IPv4 se trouvent utilisées pour l'accessibilité IPv6 des PE au lieu des adresses IPv6 mondiales.

Quand l'adresse IPv6 de 16 octets contenue dans le champ Prochain bond IPv6 n'est pas codée comme adresse transposée en IPv4 (voir au paragraphe 3.2.1.1) le PE d'entrée DOIT utiliser le tunnelage IPv6.

Quand un PE reçoit un paquet d'un CE rattaché, il cherche l'adresse de destination IPv6 du paquet dans le VRF correspondant à ce CE. Cela lui permet de trouver un chemin de VPN-IPv6. Le chemin de VPN-IPv6 va avoir une étiquette

MPLS associée et un prochain bond IPv6 associé. D'abord, cette étiquette MPLS est poussée sur le paquet comme étiquette du bas. Ensuite, ce paquet étiqueté est encapsulé dans le tunnel pour le transport au PE de sortie identifié par le prochain bond IPv6. Les détails de cette encapsulation dépendent de la technique de tunnelage, comme suit :

Comme avec MPLS/BGP pour les VPN IPv4 [RFC4797], quand le tunnelage est fait en utilisant des tunnels IPv4 ou IPv6 (respectivement des tunnels GRE IPv4 ou IPv6) l'encapsulation du paquet étiqueté de VPN IPv6 résulte en un paquet encapsulé MPLS dans IP (respectivement, MPLS dans GRE) comme spécifié dans la [RFC4023]. Quand le tunnelage est fait en utilisant L2TPv3, l'encapsulation du paquet étiqueté de VPN IPv6 résulte en un paquet encapsulé MPLS dans L2TPv3 comme spécifié dans la [RFC4817].

Comme avec MPLS/BGP pour les VPN IPv4, quand le tunnelage est fait en utilisant un tunnel sécurisé par IPsec [2547-IPsec], l'encapsulation du paquet étiqueté de VPN IPv6 résulte en un paquet encapsulé MPLS dans IP ou MPLS dans GRE [RFC4023]. Le mode transport IPsec est utilisé pour sécuriser ce tunnel IPv4 ou GRE du PE d'entrée au PE de sortie.

Quand le tunnelage est fait en utilisant des tunnels IPv4 (qu'ils soient ou non sécurisés par IPsec) le routeur PE d'entrée DOIT utiliser l'adresse IPv4 qui est codée dans le champ Adresse IPv6 transposée en IPv4 du champ Prochain bond BGP comme adresse de destination de l'en-tête IPv4 de tunnelage ajouté devant. Il utilise une de ses adresses IPv4 comme adresse de source de l'en-tête IPv4 de tunnelage ajouté.

Quand le tunnelage est fait en utilisant des tunnels IPv6 (qu'ils soient ou non sécurisés par IPsec) le routeur PE d'entrée DOIT utiliser l'adresse IPv6 qui est contenue dans le champ Adresse IPv6 du champ Prochain bond BGP comme adresse de destination de l'en-tête IPv4 de tunnelage ajouté. Il utilise une de ses adresses IPv4 comme adresse de source de l'en-tête IPv4 de tunnelage ajouté.

Quand le tunnelage est fait en utilisant des LSP MPLS, les LSP peuvent être établis en utilisant toute technique de distribution d'étiquette (LDP [RFC3036], RSVP-TE [RFC3209], etc.).

Quand le tunnelage est fait en utilisant des LSP MPLS, le routeur PE d'entrée DOIT pousser directement l'étiquette de tunnel de LSP sur la pile d'étiquettes du paquet de VPN IPv6 étiqueté (c'est-à-dire, sans ajouter devant aucun en-tête IPv4 ou IPv6). Cette étiquette poussée correspond au LSP qui commence sur le routeur PE d'entrée et se termine sur le routeur PE de sortie. Le champ Prochain bond IPv6 est utilisé pour identifier le routeur PE de sortie et ensuite l'étiquette à pousser sur la pile. Quand l'adresse IPv6 dans le champ Prochain bond IPv6 est une adresse IPv6 transposée en IPv4, l'adresse IPv4 incorporée va déterminer l'étiquette de tunnel à pousser sur la pile d'étiquettes. Dans tout autre cas, l'adresse IPv6 dans le champ Prochain bond IPv6 va déterminer l'étiquette de tunnel à pousser sur la pile d'étiquettes.

Pour assurer l'interopérabilité entre les systèmes qui mettent en œuvre cette architecture de VPN, tous ces systèmes DOIVENT prendre en charge le tunnelage utilisant des LSP MPLS établis par LDP [RFC3036].

5. Types d'adresse

Comme les adresses d'envoi individuel de liaison locale sont définies pour être utilisées seulement sur une seule liaison, elles peuvent être utilisées sur la liaison PE-CE, mais elles ne sont pas prises en charge pour l'accessibilité à travers les sites de VPN IPv6 et ne sont jamais annoncées via le protocole de passerelle bordure multi protocoles (MP-BGP, *MultiProtocol-Border Gateway Protocol*) aux PE distants.

Les adresses mondiales d'envoi individuel sont définies comme identifiant de façon univoque les interfaces partout dans l'Internet IPv6. Les adresses mondiales sont supposées être couramment utilisées au sein et à travers les sites de VPN IPv6. Elles sont évidemment prises en charge par cette solution de VPN IPv6 pour l'accessibilité à travers les sites de VPN IPv6 et annoncées via MP-BGP aux PE distants et sont traitées sans aucune considération spécifique de leur portée mondiale.

En citant la [RFC4193]: "Le présent document définit un format d'adresse IPv6 en envoi individuel qui est unique au monde et est destiné aux communications locales [RFC2460]. Ces adresses sont appelées des adresses locales IPv6 uniques en envoi individuel et sont abrégées dans ce document en adresses IPv6 locales. Elles ne sont pas supposées être acheminables sur l'Internet mondial. Elles sont acheminables à l'intérieur d'une zone plus limitée comme un site. Elles peuvent aussi être acheminées entre un ensemble limité de sites."

La [RFC4193] dit aussi au paragraphe 4.7: "Les adresses IPv6 locales peuvent être utilisées pour des réseaux virtuels privés (VPN, *Virtual Private Network*) inter sites si des chemins appropriés sont établis. Parce que les adresses sont uniques, ces VPN vont travailler de façon fiable et sans qu'il soit besoin de traduction. Ils ont la propriété supplémentaire de continuer à

travailler si les sites individuels sont dénumérotés ou fusionnés."

En accord avec cela, les adresses locales IPv6 uniques en envoi individuel sont prises en charge par la solution de VPN IPv6 spécifiée dans le présent document pour l'accessibilité à travers les sites de VPN IPv6. Donc, l'accessibilité à de telles adresses locales IPv6 uniques en envoi individuel peut être annoncée via MP-BGP aux PE distants et traitées par les PE de la même façon que des adresses d'envoi individuel mondiales.

Les recommandations et considérations pour lesquelles ces types d'adresses pris en charge devraient être utilisés dans des environnements de VPN IPv6 donnés sortent du domaine d'application de ce document.

6. Diffusion groupée

Les opérations de diffusion groupée sortent du domaine d'application de ce document.

7. Transporteur de transporteur

Parfois, un VPN IPv6 peut en fait être le réseau d'un FAI IPv6, avec ses propres politiques d'échange de trafic et d'acheminement. Parfois, un VPN IPv6 peut être le réseau d'un fournisseur de services qui offre des services de VPN à ses propres clients. Des VPN IPv6 comme ceux-là peuvent aussi obtenir un service de cœur de réseau de la part d'un autre fournisseur de services "transporteur de transporteur", en utilisant la méthode de transporteur de transporteur décrite à la Section 9 de la [RFC4364] mais appliquée au trafic IPv6. Toutes les considérations discutées dans la [RFC4364] pour le transporteur de transporteur de VPN IPv4 s'appliquent pour le VPN IPv6, à l'exception que l'utilisation de MPLS (incluant la distribution d'étiquettes) entre le PE et le CE relève des chemins IPv6 à la place de IPv4.

8. Cœur de réseau multi AS

Les mêmes procédures décrites à la Section 10 de la [RFC4364] peuvent être utilisées (et ont les mêmes propriétés d'adaptabilité) pour traiter la situation où deux sites d'un VPN IPv6 sont connectés à des systèmes autonomes différents. Cependant, quelques points supplémentaires devraient être notés quand on applique ces procédures aux VPN IPv6 ; ils sont décrits dans le reste de cette Section.

Approche (a) : connexions de VRF à VRF aux routeurs bordures de l'AS.
Cette approche est l'équivalent pour les VPN IPv6 de la procédure (a) de la Section 10 de la [RFC4364]. Dans le cas de VPN IPv6, IPv6 doit être activé sur les (sous) interfaces inter-ASBR de VRF à VRF. Dans cette approche, les ASBR échangent les chemins IPv6 (par opposition aux chemins de VPN IPv6) et peuvent échanger du trafic sur IPv6 ou sur IPv4. L'échange des chemins IPv6 DOIT être effectué conformément à la [RFC2545]. Cette méthode n'utilise pas de LSP inter AS. On notera enfin qu'avec cette procédure, comme chaque AS met en œuvre indépendamment les procédures intra AS pour les VPN IPv6 décrites dans le présent document, les AS participants peuvent tous utiliser en interne le tunnelage IPv4, ou le tunnelage IPv6 ; ou autrement, certains AS participants peuvent utiliser en interne le tunnelage IPv4 tandis que d'autres utilisent le tunnelage IPv6.

Approche (b) : redistribution EBGP des chemins de VPN IPv6 étiquetés provenant de l'AS à l'AS voisin.
Cette approche est l'équivalent pour les VPN IPv6 de la procédure (b) de la Section 10 de la [RFC4364]. Avec cette approche, les ASBR utilisent EBGP pour redistribuer les chemins de VPN-IPv4 étiquetés aux ASBR dans d'autres AS.
Dans cette approche, IPv6 peut ou non être activé sur les liaisons inter-ASBR car les ASBR qui échangent des chemins de VPN IPv6 peuvent échanger du trafic sur IPv4 ou IPv6 (dans ce cas, IPv6 doit évidemment être activé sur la liaison inter ASBR). L'échange des chemins de VPN IPv6 étiquetés DOIT être effectué conformément aux [RFC2545] et [RFC3107]. Quand le trafic de VPN-IPv6 doit être transporté en utilisant le tunnelage IPv6, le champ Prochaine adresse BGP DEVRA contenir une adresse IPv6. Quand le trafic de VPN-IPv6 doit être transporté en utilisant le tunnelage IPv4, le champ Prochaine adresse BGP DEVRA contenir une adresse IPv4 codée comme adresse IPv6 transposée en IPv4.
Cette approche exige qu'il y ait des LSP inter AS. À ce titre, les considérations (de sécurité) correspondantes décrites pour la procédure (b) à la Section 10 de la [RFC4364] s'appliquent également à cette approche pour IPv6.
Finalement, on note qu'avec cette procédure, comme avec la procédure (a), comme chaque AS met en œuvre indépendamment les procédures intra AS pour les VPN IPv6 décrites dans ce document, les AS participants peuvent tous utiliser en interne le tunnelage IPv4 ou le tunnelage IPv6 ; autrement, certains AS participants peuvent utiliser en interne le

tunnelage IPv4 tandis que d'autres utilisent le tunnelage IPv6.

Approche (c) : redistribution EBGP multi bonds des chemins de VPN IPv6 étiquetés entre AS de source et de destination, avec redistribution EBGP des chemins IPv4 ou IPv6 étiquetés provenant de l'AS à l'AS voisin.
Cette approche est équivalente pour l'échange de chemins de VPN IPv6 aux procédures (c) de la Section 10 de la [RFC4364] pour l'échange de chemins de VPN-IPv4.
Cette approche exige que les AS participants soit utilisent tous le tunnelage IPv4, soit utilisent tous le tunnelage IPv6.
Dans cette approche, les chemins de VPN IPv6 ne sont ni maintenus ni distribués par les routeurs ASBR. Les routeurs ASBR n'ont pas besoin d'être double pile. Un ASBR doit conserver les chemins IPv4 (ou IPv6) étiquetés aux routeurs PE au sein de son AS. Il utilise EBGP pour distribuer ces chemins aux autres AS. Les ASBR dans tout AS de transit vont aussi avoir à utiliser EBGP pour passer les chemins IPv4 (ou IPv6) étiquetés. Il en résulte la création d'un chemin de commutation d'étiquettes IPv4 (ou IPv6) du routeur PE d'entrée au routeur PE de sortie. Maintenant, les routeurs PE dans différents AS peuvent établir des connexions EBGP multi bonds les uns avec les autres sur IPv4 ou IPv6 et peuvent échanger des chemins de VPN IPv6 étiquetés sur ces connexions EBGP. Noter que le champ Prochain bond IPv6 de ces chemins de VPN IPv6 distribués va contenir une adresse IPv6 quand le tunnelage IPv6 est utilisé ou une adresse IPv6 transposée en IPv4 quand le tunnelage IPv4 est utilisé.
Les considérations décrites pour la procédure (c) de la Section 10 de la [RFC4364] à l'égard de l'utilisation possible de réflecteurs de chemin, d'une troisième étiquette, et de LSP s'étendant sur plusieurs AS, s'appliquent également à cette approche de VPN IPv6.

9. Accès à l'Internet à partir d'un VPN

Les méthodes proposées par la [RFC4364] pour accéder à l'Internet IPv4 mondial à partir d'un VPN IPv4 peuvent être utilisées dans le contexte des VPN IPv6 et de l'Internet IPv6 mondial. Noter cependant, que si les paquets IPv6 provenant de sites de VPN IPv6 et destinés à l'Internet IPv6 mondial ont besoin de traverser le cœur de réseau du fournisseur de services, et que si c'est un cœur de réseau uniquement IPv4, ces paquets doivent être tunnelés à travers ce cœur de réseau IPv4.

En clair, comme c'est le cas en-dehors du contexte de VPN, l'accès à l'Internet IPv6 à partir d'un VPN IPv6 exige l'utilisation d'adresses IPv6 mondiales.

En particulier, des adresses IPv6 locales uniques ne peuvent pas être utilisées pour l'accès à l'Internet IPv6.

10. Gestion de VPN

Les considérations de gestion discutées à la Section 12 de la [RFC4364] s'appliquent à la gestion des VPN IPv6.

Lorsque le fournisseur de services gère le CE du site de VPN IPv6, ce fournisseur de services peut choisir d'utiliser IPv4 pour la communication entre l'outil de gestion et le CE pour de tels objets de gestion. Dans ce cas, sans considération de si un site de client IPv4 site est réellement connecté au CE (en plus du site IPv6) le CE fait effectivement partie d'un VPN IPv4 en plus d'appartenir à un VPN IPv6 (c'est-à-dire, le CE est rattaché à un VRF qui prend en charge IPv4 en plus de IPv6). Les considérations présentées dans la [RFC4364], sur la façon de s'assurer que l'outil de gestion peut communiquer avec de tels CE gérés à partir de plusieurs VPN sans permettre une accessibilité non désirée à travers les CE de différents VPN, sont applicables à l'accessibilité IPv4 du VRF auquel le CE se rattache.

Lorsque le fournisseur de services gère le CE du site de VPN IPv6, le fournisseur de services peut choisir d'utiliser IPv6 pour la communication entre l'outil de gestion et le CE pour de tels objets de gestion. Les considérations présentées dans la [RFC4364], sur la façon de s'assurer que l'outil de gestion peut communiquer avec de tels CE gérés à partir de plusieurs VPN sans permettre une accessibilité non désirée à travers les CE de différents VPN, sont applicables à l'accessibilité IPv6 du VRF auquel le CE se rattache.

11. Considérations sur la sécurité

Les extensions définies dans ce document permettent à MP-BGP de propager les informations d'accessibilité sur les chemins de VPN IPv6.

Les considérations de sécurité pour le transport des informations d'accessibilité IPv6 en utilisant BGP sont discutés dans la RFC2545, Section 5, et sont également applicables pour les extensions décrites dans ce document.

Les extensions décrites dans ce document pour l'offre de VPN IPv6 utilisent exactement la même approche que celle décrite dans la [RFC4364]. À ce titre, les mêmes considérations de sécurité s'appliquent à l'égard de la sécurité du plan de données, à la sécurité du plan de contrôle, et à la sécurité des appareils PE et P comme décrit à la Section 13 de la [RFC4364].

12. Qualité de service

Comme tous les mécanismes de qualité de service discutés pour les VPN IPv4 à la Section 14 de la [RFC4364] opèrent de la même façon pour IPv4 et IPv6 (Diffserv, Intserv, ingénierie de trafic MPLS) les considérations de qualité de service discutées dans la [RFC4364] sont également applicables aux VPN IPv6 (et ceci tient, que le tunnelage IPv4 ou le tunnelage IPv6 soit utilisé dans le cœur de réseau.)

13. Adaptabilité

Chacune des considérations d'adaptabilité mentionnées pour les VPN IPv4 à la Section 15 de la [RFC4364] est également applicable aux VPN IPv6.

14. Considérations relatives à l'IANA

Le présent document spécifie (voir au paragraphe 3.2) l'utilisation de l'AFI *(Address Family Identifier)* BGP de valeur 2, ainsi que du SAFI *(Subsequent Address Family Identifier)* BGP de valeur 128, pour représenter la famille d'adresses "VPN-IPv6 Labeled Addresses", qui est définie dans le présent document.

L'utilisation de la valeur d'AFI 2 pour IPv6 est comme actuellement spécifié dans le registre IANA "Address Family Identifier", de sorte que l'IANA n'a pas d'action à effectuer à son égard.

L'utilisation de la valeur de SAFI 128 pour "Adresse de VPN étiqueté MPLS" est comme actuellement spécifié dans le registre IANA "Identifiant suivant de famille d'adresse", de sorte que l'IANA n'a pas d'action à effectuer à son égard.

15. Remerciements

Merci à Gerard Gastaud et Eric Levy-Abegnoli, qui ont contribué au présent document.

In Memoriam
Les auteurs tiennent à remercier de sa précieuse contribution au présent document Tri T. Nguyen, qui est décéde en avril 2002 d'une maladie soudaine.

16. Références

16.1 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)

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par* 5095, 6564 *; D.S ; Remplacée par* RFC8200, STD 86*)*

[RFC2545] P. Marques, F. Dupont, "Utilisation des extensions multi protocoles de BGP-4 pour l'acheminement inter-domaine IPv6", mars 1999. *(P.S.)*

[RFC2858] T. Bates et autres, "Extensions multiprotocoles pour BGP-4", juin 2000. (*Obsolète, voir* RFC4760) *(P.S.)*

[RFC3036] L. Andersson et autres, "Spécification de LDP", janvier 2001. *(Rendue obsolète par la* RFC5036)

[RFC3107] Y. Rekhter et E. Rosen, "Portage des informations d'étiquette dans BGP-4", mai 2001. (*MàJ par* RFC6790, RFC8277)

[RFC3392] R. Chandra et J. Scudder, "Annonces de capacités avec BGP-4", novembre 2002. *(Obsolète, voir* RFC5492)

[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)

16.2 Références pour information

[2547-IPsec] Rosen, De Clercq, Paridaens, T'Joens, Sargor, "Use of PE-PE IPsec in RFC2547 VPNs", Travail en cours, août 2005.

[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)

[RFC4023] T. Worster et autres, "Encapsulation de MPLS dans IP ou encapsulation d'acheminement générique (GRE)", mars 2005. (*MàJ par* RFC5332) *(P.S.)*

[RFC4193] R. Hinden, B. Haberman, "Adresses IPv6 en envoi individuel uniques localement", octobre 2005. *(P.S.)*

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

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. (*MàJ par* 5952 et 6052, 8064) *(D.S.)*

[RFC4797] Y. Rekhter et autres, "Utilisation de l'encapsulation générique d'acheminement (GRE) de bord de fournisseur à bord de fournisseur (PE-PE) ou IP dans les réseaux privés virtuels IP BGP/MPLS", janvier 2007. *(Information)*

[RFC4817] M. Townsley et autres, "Encapsulation de MPLS sur la version 3 du protocole de tunnelage de couche 2", mars 2007. *(P.S.)*

Adresse des auteurs

Jeremy De Clercq
Alcatel
Copernicuslaan 50, 2018 Antwerpen
Belgium
mél : jeremy.de_clercq@alcatel.be

Dirk Ooms
OneSparrow
Belegstraat 13, 2018 Antwerpen
Belgium
mél : dirk@onesparrow.com

Marco Carugi
Nortel Networks S.A.
Parc d'activites de Magny-les-jeunes
Bois CHATEAUFORT
78928 YVELINES Cedex 9 - France
mél : marco.carugi@nortel.com

Francois Le Faucheur
Cisco Systems, Inc.
Village d'Entreprise Green Side - Batiment T3
400, Avenue de Roumanille
06410 Biot-Sophia Antipolis – France
mél : flefauch@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.