Groupe de travail Réseau
**Request for Comments: 5512**
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

P. Mohapatra, Cisco Systems, Inc.
E. Rosen, Cisco Systems, Inc.
avril 2009

# Identifiant de famille d'adresse suivante (SAFI) d'encapsulation BGP et attribut d'encapsulation de tunnel de BGP



**Résumé**
Dans certaines situations, le transport d'un paquet d'un locuteur du protocole de passerelle frontière (BGP, *Border Gateway Protocol*) à un autre (le prochain bond BGP) exige que le paquet soit encapsulé par le premier locuteur BGP et désencapsulé par le second. Pour prendre en charge ces situations, il y a besoin d'un accord entre les deux locuteurs BGP à l'égard des "informations d'encapsulation", c'est-à-dire, le format de l'en-tête d'encapsulation ainsi que les contenus des divers champs de l'en-tête.

Les informations d'encapsulation n'ont pas besoin d'être signalées pour tous les types d'encapsulation. Dans les cas où la signalisation est requise (comme dans le protocole de tunnelage de couche 2 (L2TPv3, *Layer Two Tunneling Protocol - Version 3*) ou l'encapsulation d'acheminement générique (GRE, *Generic Routing Encapsulation*) avec clé) le présent document spécifie une méthode par laquelle les locuteurs BGP peuvent se signaler l'un à l'autre les informations d'encapsulation. La signalisation est faite par l'envoi de mises à jour BGP en utilisant l'identifiant de famille d'adresse d'encapsulation suivante (SAFI, *Encapsulation Subsequent Address Family Identifier*) et l'identifiant IPv4 ou IPv6 de famille d'adresse (AFI, *Address Family Identifier*). Dans les cas où aucune information d'encapsulation n'a besoin d'être signalée (comme avec GRE sans clé) le présent document spécifie une communauté BGP étendue qui peut être attachée aux messages BGP UPDATE qui portent des préfixes de charge utile afin d'indiquer le type de protocole d'encapsulation à utiliser.

## Table des matières

## 1. Introduction

Considérons le cas d'un routeur R1 qui transmet un paquet IP P. Soit D l'adresse de destination IP de P. R1 doit chercher D dans son tableau de transmission. Supposons que le chemin de "meilleure correspondance" pour D soit le chemin Q, où Q est un chemin distribué par BGP dont le "prochain bond BGP" est le routeur R2. Et supposons de plus que les routeurs le long du chemin de R1 à R2 ont des entrées pour R2 dans leurs tableaux de transmission, mais N'ONT PAS d'entrées pour D dans leurs tableaux de transmission. Par exemple, le chemin de R1 à R2 peut faire partie d'un "noyau sans BGP", où il n'y a pas du tout de chemins distribués par BGP dans tout le noyau. Ou, comme dans la [RFC5565], D peut être une adresse IPv4 alors que les routeurs intermédiaires le long du chemin de R1 à R2 peuvent seulement prendre en charge IPv6.

Dans des cas comme celui-la, afin que R1 transmette correctement le paquet P, il doit encapsuler P et envoyer P "à travers un tunnel" à R2. Par exemple, R1 peut encapsuler P en utilisant GRE, L2TPv3, IP dans IP, etc., où l'adresse de destination IP de l'en-tête d'encapsulation est l'adresse de R2.

Afin que R1 encapsule P pour le transport à R2, R1 doit savoir quel protocole d'encapsulation utiliser pour transporter les différentes sortes de paquets à R2. R1 doit aussi savoir comment remplir les divers champs de l'en-tête d'encapsulation. Avec certains types d'encapsulation, cette connaissance peut être acquise par défaut ou par configuration manuelle. D'autres protocoles d'encapsulation ont des champs comme un identifiant de session, une clé, ou un mouchard, qui doivent être remplis. Il ne serait pas souhaitable d'exiger de chaque locuteur BGP qu'il soit configuré manuellement avec les informations d'encapsulation pour chacun de ses prochains bonds BGP.

Dans le présent document, on spécifie un moyen par lequel BGP lui-même peut être utilisé par un locuteur BGP donné pour dire aux autres locuteurs BGP "si vous avez besoin d'encapsuler des paquets pour me les envoyer, voici les informations dont vous avez besoin pour former correctement l'en-tête d'encapsulation". Un locuteur BGP signale ces informations aux autres locuteurs BGP en utilisant une valeur distinctive de SAFI, le SAFI Encapsulation. Le SAFI Encapsulation peut être utilisé avec l'AFI pour IPv4 ou avec l'AFI pour IPv6. L'AFI IPv4 est utilisé quand les paquets encapsulés sont à envoyer en utilisant IPv4 ; l'AFI IPv6 est utilisé quand les paquets encapsulés sont à envoyer en utilisant IPv6.

Dans une mise à jour BGP donnée, les informations d'accessibilité de la couche réseau (NLRI, *Network Layer Reachability Information*) du SAFI Encapsulation consistent en l'adresse IP (dans la famille spécifiée par les AFI) du générateur de cette mise à jour. Les informations d'encapsulation sont spécifiées dans l'attribut BGP "encapsulation de tunnel'" (spécifié plus loin). Cet attribut spécifie les protocoles d'encapsulation qui peuvent être utilisés ainsi que toutes informations supplémentaires (si il en est) qui sont nécessaires pour utiliser correctement ces protocoles. D'autres attributs, par exemple, des communautés ou des communautés étendues, peuvent aussi être inclus.

Comme les informations d'encapsulation sont codées comme un attribut, on pourrait se demander si un nouveau SAFI est réellement nécessaire. Après tout, un locuteur BGP pourrait simplement rattacher l'attribut encapsulation de tunnel à chaque préfixe (comme Q dans notre exemple) qu'il annonce. Mais avec cette technique, tout changement dans les informations d'encapsulation causerait un très grand nombre de mises à jour. Sauf si quelqu'un veut réellement spécifier des informations d'encapsulation différentes pour chaque préfixe, il est bien préférable d'avoir un mécanisme dans lequel un changement des informations d'encapsulation cause l'annonce par le locuteur BGP d'une seule mise à jour. À l'inverse, quand les préfixes sont modifiés, les informations d'encapsulation de tunnel n'ont pas besoin d'être échangées.

Dans la présente spécification, un seul SAFI est utilisé pour porter les informations pour tous les protocoles d'encapsulation. On pourrait avoir pris une autre approche consistant à définir un nouveau SAFI pour chaque protocole d'encapsulation. Cependant, avec l'approche spécifiée, les informations d'encapsulation peuvent passer de façon transparente et automatique à travers lcs locuteurs BGP intermédiaires (par exemple, les réflecteurs de chemin) qui ne comprennent pas nécessairement les informations d'encapsulation. Cela fonctionne parce que l'attribut Encapsulation est défini comme attribut transitif facultatif. De nouvelles encapsulations peuvent donc être ajoutées sans qu'il soit besoin de reconfigurer de système BGP intermédiaire. Si on ajoute une nouvelle encapsulation requise en utilisant un nouveau SAFI, les informations pour cette encapsulation ne passeraient pas à travers les systèmes BGP intermédiaires à moins que ces systèmes soient reconfigurés pour prendre en charge le nouveau SAFI.

Pour les protocoles d'encapsulation où aucune informations d'encapsulation n'ont besoin d'être signalées (comme dans GRE sans clé) le routeur de sortie PEUT quand même vouloir spécifier le protocole à utiliser pour transporter les paquets

provenant du routeur d'entrée. Le présent document spécifie à cette fin une nouvelle communauté étendue BGP qui peut être rattachée aux messages UPDATE qui portent des préfixes de charge utile.

## 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. Format d'encapsulation NLRI

Les NLRI, définies ci-dessous, sont portées dans les messages UPDATE BGP [RFC4271] en utilisant les extensions BGP multi protocoles [RFC4760] avec un AFI de 1 ou 2 (IPv4 ou IPv6) [IANA-AF] et une valeur de SAFI de 7 (appelée un SAFI Encapsulation).

Les NLRI sont codées dans un format défini à la Section 5 de la [RFC4760] (un couple de forme <longueur, valeur>). Le champ Valeur est structuré comme suit :

```
+-----------------------------------------------+
|   Adresse de point d'extrémité (variable)     |
+-----------------------------------------------+
```

- Adresse de point d'extrémité : ce champ identifie le locuteur BGP qui génère la mise à jour. C'est normalement une des adresses d'interface configurées au routeur. La longueur de l'adresse de point d'extrémité dépend de l'AFI annoncé. Si l'AFI est réglé à IPv4 (1), alors l'adresse de point d'extrémité est une adresse IPv4 de 4 octets, tandis que si l'AFI est réglé à IPv6 (2), l'adresse de point d'extrémité est une adresse IPv6 de 16 octets.

Un message de mise à jour qui porte l'attribut MP_REACH_NLRI ou MP_UNREACH_NLRI avec le SAFI Encapsulation DOIT aussi porter les attributs BGP obligatoires : ORIGIN, AS_PATH, et LOCAL_PREF (pour les voisins IBGP) comme défini dans la [RFC4271]. De plus, un tel message de mise à jour peut aussi contenir tout attribut facultatif de BGP, comme l'attribut Communauté ou Communauté étendue, pour influencer une action sur le locuteur receveur.

Quand un locuteur BGP annonce les NLRI Encapsulation via BGP, il utilise sa propre adresse comme prochain bond BGP dans l'attribut MP_REACH_NLRI ou MP_UNREACH_NLRI. L'adresse de prochain bond est réglée sur la base de l'AFI dans l'attribut. Par exemple, si l'AFI est réglé à IPv4 (1), le prochain bond est codé comme une adresse IPv4 de quatre octets. Si l'AFI est réglé à IPv6 (2), le prochain bond est codé comme une adresse IPv6 de 16 octets du routeur. Chez le routeur receveur, le prochain bond BGP d'un tel message de mise à jour est validé en effectuant une opération de recherche récurrente de chemin dans le tableau d'acheminement.

Le choix du meilleur chemin des NLRI Encapsulation est gouverné par le processus de décision mentionné au paragraphe 9.1 de la [RFC4271]. Les données d'encapsulation portées par d'autres attributs dans le message sont à utiliser par le routeur receveur seulement si les NLRI ont un meilleur chemin.

## 4. Attribut d'encapsulation de tunnel

L'attribut Encapsulation de tunnel est un attribut transitif facultatif qui est composé d'un ensemble de codages de Type-Longueur-Valeur (TLV). Le code de type de l'attribut est 23. Chaque TLV contient les informations correspondant à une technologie de tunnel particulière. Le TLV est structuré comme suit :

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type de tunnel (2 octets)    |        Longueur (2 octets)    |
+---------------+---------------+---------------+---------------+
|                                                               |
```

```
|                              Valeur                           |
|                                                               |
+---------------+---------------+---------------+---------------+
```

* Type de tunnel (2 octets) : identifie le type de technologie de tunnelage signalée. Le présent document définit les types suivants :
  - L2TPv3 sur IP [RFC3931] : Type de tunnel = 1
  - GRE [RFC2784] : Type de tunnel = 2
  - IP dans IP [RFC2003] [RFC4213] : Type de tunnel = 7
  Les types inconnus sont ignorés et sautés à réception.

* Longueur (2 octets) : nombre total d'octets du champ Valeur.

* Valeur (variable) : composée de multiples sous TLV. Chaque sous TLV consiste en trois champs : un type d'un octet, une longueur d'un octet, et zéro, un ou plusieurs octets de valeur. Le sous TLV est structuré comme suit :

```
+-----------------------------------+
|    Type de sous TLV (1 octet)     |
+-----------------------------------+
|    Longueur de sous TLV (1 octet) |
+-----------------------------------+
|   Valeur de sous TLV (variable)   |
|                                   |
+-----------------------------------+
```

* Type de sous TLV (1 octet) : chaque type de sous TLV définit une certaine propriété sur le TLV tunnel qui contient ce sous TLV. Les types suivants sont définis dans ce document :
  - Encapsulation : type de sous TLV = 1
  - Type de protocole : type de sous TLV = 2
  - Couleur : type de sous TLV = 4

  Quand le TLV est traité par un locuteur BGP qui va effectuer l'encapsulation, tout sous TLV inconnu DOIT être ignoré et sauté. Cependant, si le TLV est compris, le TLV entier NE DOIT PAS être ignoré juste parce que il contient un sous TLV inconnu.

* Longueur de sous TLV (1 octet) : nombre total d'octets du champ Valeur de sous TLV.

* Valeur de sous TLV (variable) : les codages du champ Valeur dépendent du type de sous TLV énumérés ci-dessus. Les paragraphes qui suivent définissent en détail le codage.

### 4.1 Sous TLV Encapsulation

La syntaxe et la sémantique du sous TLV Encapsulation sont déterminées par le type de tunnel du TLV qui contient ce sous TLV.

Quand le type de tunnel du TLV est L2TPv3 sur IP, la structure du champ Valeur du sous TLV Encapsulation est la suivante :

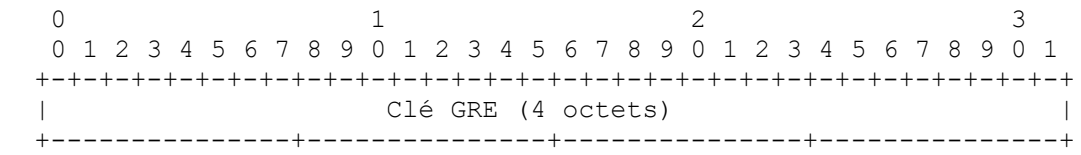
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Identifiant de session (4 octets)            |
+---------------+---------------+---------------+---------------+
|                                                               |
|                      Mouchard (variable)                      |
|                                                               |
+---------------+---------------+---------------+---------------+
```

* Identifiant de session : valeur non zéro de 4 octets allouée en local par le routeur annonceur qui sert de clé de recherche dans le contexte du paquet entrant.

* Mouchard : valeur facultative, de longueur variable (codée en octets -- de 0 à 8 octets) utilisée par L2TPv3 pour vérifier l'association d'un message de données reçu à la session identifiée par l'identifiant de session. La génération et l'usage de la valeur de mouchard est comme spécifié dans la [RFC3931].

  La longueur du mouchard n'est pas codée explicitement, mais peut être calculée comme (longueur de sous TLV - 4).

Quand le type de tunnel du TLV est GRE, la structure du champ Valeur du sous TLV Encapsulation est la suivante :




* Clé GRE : champ de 4 octets [RFC2890] qui est généré par le routeur annonceur. La méthode réelle d'obtention de la clé sort du domaine d'application de ce document. La clé est insérée dans l'en-tête d'encapsulation GRE des paquets de charge utile envoyés par les routeurs d'entrée au routeur annonceur. Elle est destinée à être utilisée pour identifier des informations de contexte supplémentaires sur la charge utile reçue.

Noter que la clé est facultative. Sauf si une valeur de clé est annoncée, le sous TLV Encapsulation GRE NE DOIT PAS être présent.

### 4.2 Sous TLV Type de protocole

Le sous TLV Type de protocole PEUT être codé pour indiquer le type des paquets de charge utile qui vont être encapsulés avec les paramètres de tunnel qui sont signalés dans le TLV. Le champ Valeur du sous TLV contient un type de protocole de 2 octets qui est un des types définis dans [IANA-AF] comme ETHER TYPE.

Par exemple, si on veut utiliser trois sessions L2TPv3, une portant des paquets IPv4, une portant des paquets IPv6, et une portant des paquets MPLS, le routeur de sortie va inclure trois TLV de type Encapsulation L2TPv3, spécifiant chacun un identifiant de session différent et un type de charge utile différent. Le sous TLV Type de protocole pour eux va être IPv4 (type de protocole = 0x0800), IPv6 (type de protocole = 0x86dd), et MPLS (type de protocole = 0x8847), respectivement. Cela informe les routeurs d'entrée des informations d'encapsulation appropriées à utiliser avec chacun des types de protocole. L'insertion de l'identifiant de session spécifié aux routeurs d'entrée permet à la sortie de traiter correctement les paquets entrants, en accord avec leur type de protocole.

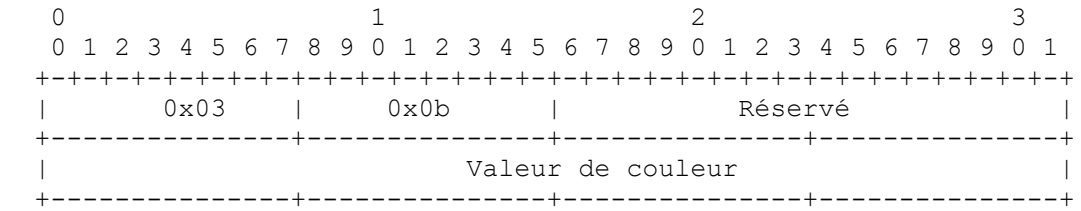
L'inclusion de ce sous TLV dépend du type de tunnel. Il DOIT être codé pour le type de tunnel L2TPv3. Par ailleurs, le sous TLV type de protocole n'est pas exigé pour les tunnels IP dans IP ou GRE.

### 4.3 Sous TLV Couleur

Le sous TLV Couleur PEUT être codé comme moyen de colorier le TLV Tunnel correspondant. Le champ Valeur du sous TLV contient une communauté étendue qui est définie comme suit :

#### 4.3.1 Communauté Couleur étendue

La communauté Couleur étendue est une communauté étendue opaque [RFC4360] avec le codage suivant :




La valeur de l'octet de poids fort d champ Type étendu est 0x03, qui indique qu'il est transitif. La valeur de l'octet de moindre poids du champ Type étendu pour cette communauté est 0x0b. La valeur de couleur est définie par l'utilisateur et configurée localement sur les routeurs. La même communauté de couleur étendue peut alors être attachée aux messages UPDATE qui contiennent des préfixes de charge utile. De cette façon, le locuteur BGP peut exprimer le fait qu'il s'attend à

ce que des paquets correspondant à ces préfixes de charge utile soient reçus avec un en-tête d'encapsulation de tunnel particulier.

### 4.4 Choix du type de tunnel

Un locuteur BGP peut inclure plusieurs TLV Tunnel dans l'attribut Tunnel. Le locuteur receveur PEUT avoir des politiques locales définies pour choisir des types de tunnel différents pour des ensembles/types différents de préfixes de charge utile reçus du même locuteur BGP. Par exemple, si un locuteur BGP inclut à la fois des types de tunnel L2TPv3 et GRE dans l'attribut Tunnel et si il annonce aussi des préfixes IPv4 et IPv6, le routeur d'entrée peut avoir une politique locale définie pour choisir L2TPv3 pour les préfixes IPv4 (pourvu que le type de protocole reçu dans l'attribut Tunnel corresponde) et GRE pour les préfixes IPv6.

De plus, le message UPDATE d'encapsulation SAFI peut contenir un sous TLV Couleur pour certains ou tous les TLV Tunnel. Le locuteur BGP DEVRAIT alors attacher une communauté Couleur étendue aux préfixes de charge utile pour choisir les types appropriés de tunnel.

Dans un déploiement multi fabricants qui a des routeurs qui prennent en charge différentes technologies de tunnelage, inclure un sous TLV Couleur dans le message UPDATE d'encapsulation SAFI peut servir comme mécanisme de classification (par exemple, l'ensemble A de routeurs pour GRE et l'ensemble B de routeurs pour L2TPv3). Le routeur d'entrée peut alors choisir les données d'encapsulation de façon appropriée lors de l'envoi des paquets à un routeur de sortie.

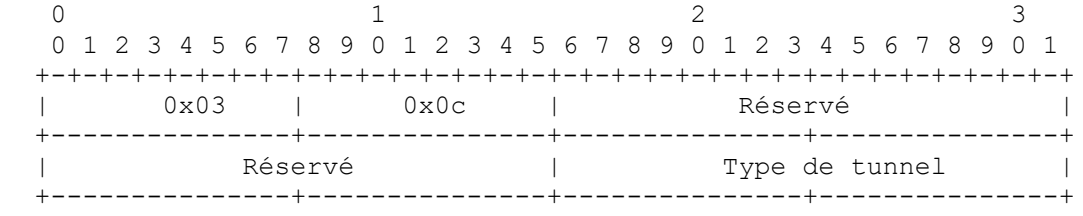
Si un locuteur BGP génère une mise à jour pour le préfixe P avec la couleur C et avec lui-même comme prochain bond, il DOIT alors aussi générer une mise à jour d'encapsulation SAFI qui contient la couleur C.

Supposons qu'un locuteur BGP reçoive une mise à jour pour le préfixe P avec la couleur C, que la procédure de décision BGP ait choisi le chemin dans cette mise à jour comme le meilleur chemin pour P, et que prochain bond soit le nœud N, mais qu'une mise à jour d'encapsulation SAFI générée du nœud N contenant la couleur C n'ait pas été reçue. Dans ce cas, aucun chemin pour P ne va être installé dans le tableau de transmission tant que la mise à jour d'encapsulation SAFI correspondante n'est pas reçue, ou que le processus de décision BGP choisisse un chemin différent.

Supposons qu'un locuteur BGP reçoive une mise à jour "non colorée" pour le préfixe P, avec le prochain bond N, et que le locuteur BGP ait aussi reçu un SAFI Encapsulation généré par N, spécifiant une ou plusieurs encapsulations qui peuvent ou non être colorées. Dans ce cas, le choix d'encapsulation est l'affaire de la politique locale. La seule "politique par défaut" nécessaire est de choisir une des encapsulations prises en charge par le locuteur.

### 4.5 Communauté étendue d'encapsulation BGP

On définit ici une communauté étendue BGP opaque qui peut être attachée aux messages BGP UPDATE pour indiquer le protocole d'encapsulation à utiliser pour envoyer des paquets d'un routeur d'entrée à un routeur de sortie. En considérant notre exemple de la Section 1, R2 PEUT inclure cette communauté étendue, en spécifiant un type de tunnel particulier à utiliser dans le message UPDATE qui porte le chemin de Q à R1. Ceci est utile si il n'y a pas d'informations d'encapsulation explicites à signaler en utilisant le SAFI Encapsulation pour un protocole de tunnelage (comme GRE sans clé).




La valeur de l'octet de poids fort du champ Type étendu est 0x03, qui indique qu'il est transitif. La valeur de l'octet de moindre poids du champ Type étendu est 0x0c.

Les deux derniers octets du champ Valeur codent un type de tunnel comme défini dans le présent document.

Pour l'interopérabilité, un locuteur qui prend en charge le SAFI Encapsulation DOIT mettre en œuvre la communauté étendue d'encapsulation.

## 5. Annonce de capacité

Un locuteur BGP qui souhaite échanger des informations de point d'extrémité de tunnel doit utiliser le code de capacité d'extensions multi protocoles comme défini dans la [RFC4760], pour annoncer la paire correspondante de (AFI, SAFI).

## 6. Traitement d'erreur

Quand un locuteur BGP rencontre une erreur lors de l'analyse de l'attribut d'encapsulation de tunnel, le locuteur DOIT traiter le UPDATE comme un retrait des chemins existants des NLRI de SAFI d'encapsulation incluses, ou éliminer le UPDATE si de tels chemins n'existent pas. Une entrée de journal d'événements devrait être enregistrée pour une analyse locale.

## 7. Considérations sur la sécurité

Les considérations sur la sécurité applicables aux canaux virtuels peuvent être trouvées dans le cadre de maillage [RFC5565]. En général, les questions de sécurité des protocoles de tunnel signalé par un SAFI Encapsulation sont hérités.

Si un tiers est capable de modifier des informations utilisées pour former les en-têtes d'encapsulation, pour choisir un type de tunnel, ou pour choisir un tunnel particulier pour un type de charge utile particulier, les paquets de données d'utilisateur peuvent finir par être mal acheminés, mal livrés, et/ou éliminés.

## 8. Considérations relatives à l'IANA

L'IANA a alloué la valeur 7 dans le registre "Famille d'adresses suivante", dans la gamme "Action de normalisation", à "Encapsulation SAFI", avec le présent document comme référence.

L'IANA a alloué la valeur 23 dans le registre des "Attributs de chemin BGP", à "Attribut Encapsulation de tunnel", avec le présent document comme référence.

L'IANA a alloué deux nouvelles valeurs dans le registre du type "Communauté BGP opaque étendue". Toutes deux sont de la gamme transitive. La première nouvelle valeur est appelée "Communauté de couleur étendue" (0x030b), et la seconde est appelée "Communauté d'encapsulation étendue" (0x030c). Le présent document est la référence pour les deux allocations.

L'IANA a établi un registre pour les "Types de tunnel d'attribut d'encapsulation de tunnel BGP". C'est un registre de valeurs de deux octets (0 à 65535) à allouer selon le principe du premier arrivé, premier servi. Les allocations initiales sont les suivantes :

| **Nom de tunnel** | **Type** |
|---|---|
| L2TPv3 sur IP | 1 |
| GRE | 2 |
| IP dans IP | 7 |

L'IANA a établi un registre pour les "Sous TLV d'attribut d'encapsulation de tunnel BGP". C'est un registre de valeurs de 1 octet (0 à 255) à allouer sur la base d'une "action de normalisation/allocation précoce". Le présent document est la référence. Les allocations initiales sont :

| **Nom de sous TLV** | **Type** |
|---|---|
| Encapsulation | 1 |
| Type de protocole | 2 |
| Couleur | 4 |

## 9. Remerciements

La présente spécification s'appuie sur un travail antérieur de Gargi Nalawade, Ruchi Kapoor, Dan Tappan, David Ward, Scott Wainner, Simon Barber, et Chris Metz. Les auteurs actuels souhaitent les remercier de leur contribution.

Les auteurs tiennent à remercier John Scudder, Robert Raszuk, Keyur Patel, Chris Metz, Yakov Rekhter, Carlos Pignataro, et Brian Carpenter de leurs précieux commentaires et suggestions.

## 10. Références

### 10.1 Références normatives

[RFC2003] C. Perkins, "Encapsulation de IP dans IP", octobre 1996. (*MàJ par* RFC 3168, RFC 6864, Errata) *(P.S.)*

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

[RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, "Encapsulation d'acheminement générique (GRE)", DOI 10.17487/RFC2784, mars 2000.

[RFC2890] G. Dommety, "Extensions de clé et de numéro de séquence à GRE", septembre 2000. *(P.S.)*

[RFC3931] J. Lau et autres, "Protocole de tunnelage de couche deux - version 3 (L2TPv3)", DOI 10.17487/RFC3931, mars 2005. *(P.S.)*

[RFC4213] E. Nordmark, R. Gilligan, "Mécanismes de transition de base pour hôtes et routeurs IPv6", 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, RFC9072)

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

[RFC4760] T. Bates, R. Chandra, D. Katz et Y. Rekhter, "Extensions multi protocoles pour BGP-4", janvier 2007.

### 10.2 Références pour information

[IANA-AF] "Address Family Numbers," http://www.iana.org.

[RFC5565] J. Wu, Y. Cui, C. Metz, E. Rosen, "Cadre de maillage de passage logiciel", juin 2009. *(P. S.)*

## Adresse des auteurs

Pradosh Mohapatra
Cisco Systems, Inc.
170 Tasman Drive
San Jose, CA, 95134
mél : pmohapat@cisco.com

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