

Groupe de travail Réseau  
**Request for Comments : 2685**  
Catégorie : En cours de normalisation  
Traduction Claude Brière de L'Isle

B. Fox, Lucent Technologies  
B. Gleeson, Nortel Networks  
septembre 1999

## Identifiant de réseau privé virtuel

### Statut du présent mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet 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 "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

### Notice de Copyright

Copyright (C) The Internet Society (1999). Tous droits réservés.

### Résumé

Les réseaux privés virtuels IP peuvent s'étendre sur de nombreux systèmes autonomes ou fournisseurs de service. Il y a une exigence pour l'utilisation d'un identifiant de VPN unique au monde afin d'être capable de se référer à un VPN particulier (voir au paragraphe 6.1.1 de la [RFC2764]). Le présent document propose un format pour un identifiant de VPN unique au monde.

## 1. Introduction

Avec l'expansion de l'Internet public et l'extension mondiale de son infrastructure, la détermination d'exploiter cette infrastructure a conduit à étendre l'intérêt pour les réseaux privés virtuels fondés sur IP. Un VPN simule un réseau IP privé sur des infrastructures publiques ou partagées. Les réseaux privés virtuels présentent des avantages à la fois pour le fournisseur de service et pour ses abonnés. Pour les abonnés, un VPN peut étendre les capacités IP d'un site d'entreprise à des bureaux distants et/ou à des utilisateurs avec des services d'intranet, d'extranet, par numérotation. Cette connectivité devrait être réalisée au moindre coût pour l'abonné avec l'économie d'équipement en capital, en fonctionnement, et en services. Le fournisseur de service est capable de faire un meilleur usage de son infrastructure et de son expertise de l'administration de réseau en offrant la connectivité et/ou les services de VPN IP à ses clients.

Il y a de nombreuses façons de mettre en œuvre des services de VPN IP. Le document sur le cadre de VPN fondés sur IP [RFC2764] identifie quatre types de VPN à prendre en charge : les liaisons spécialisées virtuelles, les réseaux virtuels à acheminement privé, les réseaux virtuel à numérotation privée, et les segments de LAN privé virtuel. De plus, de nombreux projets et propositions offrent des méthodes à utiliser par les fournisseurs de service et/ou les clients des fournisseurs de service pour permettre ce service. Les solutions peuvent s'appuyer sur les clients ou sur le réseau. Les solutions fondées sur le réseau peuvent fournir la connectivité et les services à la couche 2 et/ou la couche 3. Les appareils impliqués dans la mise en œuvre de la solution peuvent être des appareils dans les locaux du client (CPE, *Customer Premises Equipment*) des équipements du côté du fournisseur de service, des équipements centraux du fournisseur de service, ou une combinaison de ces appareils.

Alors qu'on discute et débat des diverses méthodes de mise en œuvre de service de VPN, il y a deux points qui font l'objet d'un accord :

- Comme un VPN est privé, il peut utiliser un espace d'adresse privé qui peut se recouvrir avec l'espace d'adresse d'un autre VPN ou celui de l'Internet public.
- Un VPN peut s'étendre sur plusieurs systèmes autonomes (AS, *Autonomous System*) IP ou fournisseurs de service.

Le premier point indique qu'une adresse IP n'a de signification qu'au sein du VPN dans lequel elle existe. Il est nécessaire pour cette raison, d'identifier le VPN dans lequel une adresse IP particulière a une signification, la "portée" de l'adresse IP.

Le second point indique que plusieurs méthodes de mise en œuvre de service VPN peuvent être utilisées pour fournir la connectivité et les services à un seul VPN. Différents fournisseurs de service peuvent employer des stratégies différentes sur la base de leur infrastructure et de leur expertise. Il est souhaitable d'être capable d'identifier tout VPN particulier à toutes les couches et toutes les localisations dans lesquelles il existe, en utilisant le même identifiant de VPN.

## 2. Identifiant mondial de VPN

L'objet d'un identifiant de VPN est d'identifier un VPN. Cet identifiant peut être utilisé de diverses façons selon la méthode de mise en œuvre du service de VPN. Par exemple, l'identifiant de VPN peut être inclus :

- dans une MIB pour configurer des attributs à un VPN, ou pour allouer une interface d'accès physique ou logique à un VPN particulier.
- dans un paquet de contrôle ou de données, pour identifier la "portée" d'une adresse IP privée et le VPN auquel appartiennent les données.

Il est nécessaire d'être capable d'identifier le VPN auquel un paquet de données est associé. L'identifiant de VPN peut être utilisé pour faire cette association, soit explicitement (par exemple, par inclusion de l'identifiant de VPN dans un en-tête d'encapsulation [RFC2684]) ou implicitement (par exemple en incluant l'identifiant de VPN dans un échange de signalisation ATM [MPOA]). La pertinence de l'utilisation de l'identifiant de VPN dans d'autres contextes doit être évaluée avec soin.

Il y a une autre très importante fonction qui peut être réalisée par l'identifiant de VPN. Il peut être utilisé pour définir une "autorité de VPN" qui est chargée de coordonner la connexité et les services employés par ce VPN. L'autorité de VPN peut être l'administrateur du réseau privé ou le principal fournisseur de service. L'autorité de VPN va administrer le VPN et lui servir de principal point de contact. L'autorité peut exporter certaines fonctions et la connexité, établir des accords contractuels avec les différents fournisseurs de service impliqués, et coordonner la configuration, les performances, et la gestion des fautes.

Ces fonctions exigent un VPN qui ait une portée mondiale et soit utilisable dans diverses solutions. Pour être un identifiant de VPN vraiment mondial, le format ne peut pas forcer les hypothèses sur le ou les réseaux partagés. À l'inverse, le format ne devrait pas être défini d'une façon telle qu'il interdise l'utilisation des caractéristiques du réseau partagé. Il est nécessaire de noter que le même VPN peut être identifié à différentes couches du même réseau partagé, par exemple les couches ATM et IP. Les mêmes format et valeur d'identifiant de VPN devraient s'appliquer aux deux couches.

Les méthodes d'utilisation de l'identifiant de VPN sont en dehors du domaine d'application du présent mémoire.

## 3. Exigences de format d'identifiant de VPN global

Le format d'identifiant de VPN devrait satisfaire aux exigences suivantes :

- fournir un identifiant de VPN unique au monde utilisable à travers plusieurs fournisseurs de service,
- permettre la prise en charge d'un identifiant de VPN ne dépendant pas de IP pour être utilisé dans les VPN de couche 2,
- identifier l'autorité de VPN au sein de l'identifiant de VPN.

## 4. Format d'identifiant mondial de VPN

Le format de l'identifiant mondial de VPN est :

3 octets d'identifiant d'autorité organisationnellement unique de VPN (OUI, *Organizationally Unique Identifier*) [OUI] suivis par 4 octets d'indice de VPN identifiant le VPN conformément à OUI

```

0 1 2 3 4 5 6 7 8
+-----+
| VPN OUI (MSB) |
+-----+
|   VPN OUI     |
+-----+
| VPN OUI (LSB) |
+-----+
| Indice VPN (MSB) |
+-----+
| Indice VPN     |
+-----+
| Indice VPN     |
+-----+
| Indice VPN (LSB) |
+-----+
```

Le OUI VPN (IEEE 802-1990) [OUI] identifie l'autorité de VPN. L'autorité de VPN servira de principal administrateur de VPN. L'autorité de VPN peut être la société/organisation à laquelle appartient le VPN ou un fournisseur de service qui fournit l'infrastructure sous-jacente en utilisant son propre réseau partagé et/ou ceux d'autres fournisseurs. Les 4 octets de l'indice de VPN identifient un VPN particulier desservi par l'autorité de VPN.

## 5. Considérations pour la sécurité

Le présent document définit le format de l'identifiant mondial de VPN sans en spécifier l'usage. Cependant, l'association de caractéristiques particulières et de capacités à un identifiant de VPN nécessite l'utilisation de procédures de sécurité standard avec tout usage spécifié. La mauvaise configuration ou la falsification délibérée d'un identifiant de VPN peut avoir pour résultat différentes brèches dans la sécurité, y compris l'interconnexion de VPN différents.

## 6. Références

[RFC2684] D. Grossman, J. Heinanen, "[Encapsulation multiprotocole sur la couche 5](#) d'adaptation ATM", septembre 1999. (*P.S.*)

[RFC2764] B. Gleeson et autres, "Cadre pour les réseaux privés virtuels fondés sur IP", février 2000. (*Information*)

[MPOA] "MPOA v1.1 Addendum on VPN Support", ATM Forum, af-mpoa-0129.000, août 1999, Bernhard Petri, éditeur, document du vote final.

[OUI] <http://standards.ieee.org/regauth/oui/index.html>

## 7. Adresse des auteurs

Barbara A. Fox  
Lucent Technologies  
300 Baker Ave, Suite 100  
Concord, MA 01742-2168  
téléphone : +1-978-287-2843  
mél : [barbarafox@lucent.com](mailto:barbarafox@lucent.com)

Bryan Gleeson  
Nortel Networks  
4500 Great America Parkway,  
Santa Clara, CA 95054  
téléphone : +1-408-855-3711  
mél : [bgleeson@shastanets.com](mailto:bgleeson@shastanets.com)

## 8. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de droits de reproduction ci-dessus et ce paragraphe soient inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définis dans les procédures des normes d'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet ou ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

### Remerciement

Le financement de la fonction d'éditeur des RFC est actuellement fourni par la Internet Society.