Groupe de travail Réseau
Request for Comments : 2735
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

B. Fox, Equipe Communications
B. Petri, Siemens AG
décembre 1999

Prise en charge de NHRP pour les réseaux virtuels privés

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.

Résumé
Le protocole de résolution de prochain bond (NHRP, *Next Hop Resolution Protocol*) multi accès sans diffusion (NBMA, *non-broadcast multi-access*) est utilisé pour déterminer les adresses de sous réseau NBMA du "prochain bond NBMA" à l'égard d'une adresse de couche d'inter réseautage public (voir la [RFC2332]). Le présent document décrit les améliorations nécessaires pour permettre à NHRP d'effectuer la même fonction pour les adresses de couche inter réseautage privé disponibles dans le cadre d'un service de réseau privé virtuel (VPN, *Virtual Private Network*) sur un réseau NBMA partagé.

1. Introduction

NHRP est une couche inter réseautage public fondée sur un protocole de résolution. Il est implicitement compris dans la [RFC2332] qu'un message de contrôle s'applique à l'espace d'adresses public.

Les fournisseurs de service de services de réseau virtuel privé (VPN) vont offrir aux participants aux VPN des accords de niveau de service (SLA, *service level agreement*) spécifiques qui peuvent inclure, par exemple, des fonctions d'acheminement dédiées et/ou des niveaux de qualité de service spécifiques. Un dispositif particulièrement important d'un service de VPN est la capacité à utiliser un espace d'adresse privé qui peut se chevaucher avec l'espace d'adresses d'un autre VPN ou de l'Internet public. Donc, une telle adresse de couche inter réseautage n'a de signification qu'au sein du VPN dans lequel elle existe. Pour cette raison, il est nécessaire d'identifier le VPN dans lequel une adresse particulière de couche inter réseautage a une signification, la "portée" de l'adresse de couche inter réseautage

Comme les VPN sont déployés sur des réseaux partagés, NHRP peut être utilisé pour résoudre une adresse de VPN privé en une adresse de réseau NBMA partagée. Afin de résoudre correctement une adresse privée de VPN, il est nécessaire que l'appareil NHRP soit capable d'identifier le VPN dans lequel l'adresse a une signification et de déterminer les informations de résolution sur la base de cette "portée".

Comme les services de VPN sont ajoutés à un réseau NBMA en utilisant des appareils NHRP, il peut être nécessaire de prendre en charge le service avec des appareils NHRP auxiliaires qui n'ont pas de connaissance du VPN et ne prennent donc pas explicitement en charge les VPN. Le présent document décrit les exigences pour les entités NHRP "à capacité VPN" pour prendre en charge les services de VPN tout en communiquant avec les entités NHRP aussi bien "à capacité VPN" que "sans capacité VPN".

2. Généralités de la prise en charge de NHRP pour VPN

2.1 Terminologie

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

En plus de la terminologie spécifiée au paragraphe 2.1 de la [RFC2332], les définitions et acronymes suivants sont utilisés :

Instance d'acheminement par défaut – En présence de VPN, tous les paquets sont traités (par exemple, acheminés) dans le contexte d'un VPN spécifique. Lorsque aucun VPN n'est indiqué, un paquet est traité selon un VPN par défaut, c'est-à-dire, une instance d'acheminement par défaut. Cette instance d'acheminement peut être l'Internet public, un VPN particulier, etc. Le terme n'a de signification que pour les entités NHRP "à capacité VPN".

Réseau virtuel privé (VPN) – Dans le contexte ce cette spécification, ce terme est utilisé comme décrit dans la [RFC2685].

À capacité VPN – Une entité NHRP "à capacité VPN" est une entité NHRP qui met en œuvre les améliorations de NHRP pour les VPN comme défini dans le présent document.

Sans capacité VPN – Une entité NHRP "sans capacité VPN" est une entité NHRP qui est déployée au titre d'un seul VPN, mais n'a pas de capacité VPN. Les restrictions qui s'appliquent aux entités NHRP sans capacité VPN sont décrites ci-dessous. Les appareils NHRP tels que spécifiés dans la [RFC2332] sont des exemples d'entités sans capacité de VPN.

Encapsulation de VPN – Encapsulation LLC/SNAP d'une PDU avec l'indication du VPN auquel appartient la PDU. Lorsque le réseau NBMA sous-jacent est en ATM, l'encapsulation de VPN est spécifiée à la section 8 de la [RFC2684].

Identifiant de VPN (VPN-ID) – Dans le contexte de la présente spécification, ce terme est utilisé comme spécifié dans la [RFC2685].

Signalisation VPN – Dans le contexte de la présente spécification, ce terme est utilisé pour noter une méthode indiquant le VPN-ID via la signalisation de contrôle ou des moyens similaires dans le chemin de contrôle.

2.2 Généralités sur la prise en charge de VPN

Lors de la prise en charge de NHRP pour un VPN, il est nécessaire de spécifier à quel VPN s'applique le message NHRP afin de se conformer à l'accord de niveau de service de VPN applicable à ce VPN.

Sur certains réseaux NBMA, il est possible d'établir un chemin de contrôle spécifique du VPN entre les appareils NHRP. Cela est suffisant pour identifier les paquets de contrôle NHRP comme appartenant au VPN "hérité". Cependant, lorsque cette solution n'est pas utilisée, l'appareil NHRP doit spécifier dans la PDU le VPN auquel un paquet NHRP s'applique.

Il n'est pas utile d'ajouter une extension de VPN aux messages de contrôle NHRP parce que il n'est pas exigé des serveurs NHRP de transit qu'ils traitent les extensions à un message de contrôle NHRP (voir le paragraphe 5.3 de la [RFC2332]). Les serveurs NHRP déjà déployés peuvent résoudre le paquet de contrôle au sein de la portée de l'espace d'adresse de couche inter réseautage public au lieu de l'espace d'adresse privé, ce qui cause des problèmes d'acheminement.

Au lieu de cela, un en-tête LLC/SNAP avec une indication de VPN (comme spécifié au paragraphe 4.1 ci-dessous) sera ajouté au début du message de contrôle NHRP. Cette solution permet que le même en-tête LLC/SNAP spécifique du VPN soit ajouté en tête des PDU dans les chemins de contrôle et de données.

3. Fonctionnement de NHRP sur VPN

3.1 Fonctionnement de NHRP à capacité VPN

Lorsque un appareil NHRP à capacité VPN transmet un paquet appartenant à un VPN particulier, cet appareil DOIT être capable d'indiquer le VPN soit :

a) explicitement en utilisant l'en-tête LLC/SNAP spécifique du VPN, soit
b) implicitement par une indication via la signalisation de VPN.

Ceci s'applique aux messages de contrôle NHC-NHS, NHS-NHS, et NHS-NHC ainsi qu'au trafic en court-circuit de NHC à NHC.

Dans le cas a), l'indication du VPN-ID est via un en-tête LLC/SNAP spécifique de VPN spécifié au paragraphe 4.2 ci-dessous. Dans le cas d'un réseau ATM sous-jacent, voir aussi la section 8 de la [RFC2684].

Pour le cas b), la méthode utilisée pour indiquer le VPN-ID via la signalisation de VPN dépend des mécanismes disponibles dans le réseau sous-jacent et sort du domaine d'application du présent mémoire. Une entité NHRP à capacité VPN qui utilise la signalisation de VPN NE DEVRAIT PAS indiquer aussi explicitement le VPN-ID pour une PDU sur le chemin en question.

En transitant par un serveur NHRP, l'identification de VPN PEUT être transmise dans un format différent de celui dans lequel elle a été reçue, cependant, le même VPN-ID DOIT être indiqué pour le message. Par exemple, une PDU reçue avec un en-tête LLC/SNAP contenant un identifiant de VPN peut être transmis sur un chemin de contrôle qui a été établi avec une indication du même VPN sans l'en-tête LLC/SNAP spécifique de VPN. Lorsque une entité NHRP à capacité VPN reçoit un message NHRP d'un appareil NHRP à capacité VPN sans indication de VPN via l'encapsulation de VPN ou la signalisation VPN, le message s'applique à l'instance d'acheminement par défaut prise en charge par l'infrastructure partagée. L'Internet public ou un domaine d'acheminement VPN particulier peut être configuré comme étant l'instance d'acheminement par défaut.

3.2 Interactions d'entités NHRP à capacité VPN et sans capacité VPN

Une entité NHRP à capacité VPN DOIT être capable d'indiquer le VPN-ID d'une des façons spécifiées au paragraphe 3.1 ci-dessus. Elle PEUT participer à plus d'un VPN.

Parce qu'un appareil NHRP sans capacité VPN ne comprend pas le concept de VPN, il ne prend en charge qu'une seule instance d'acheminement. Donc, une entité NHRP sans capacité VPN appartient sans le savoir à exactement un VPN. Tous les paquets inter réseautage envoyés par cette entité sont supposés appartenir à ce VPN. (Noter que si l'Internet actuel fondé sur IPv4 est considéré juste comme un gros VPN, les hôtes rattachés à IPv4 peuvent par exemple être considérés comme étant "contenus" dans ce VPN.)

Pour qu'une entité NHRP sans capacité VPN interagisse avec une entité NHRP à capacité VPN, l'entité NHRP à capacité VPN DOIT être configurée pour associer l'identifiant de VPN correct aux informations reçues de l'entité sans capacité VPN. En d'autres termes, l'entité NHRP à capacité VPN agit comme dans le cas de l'option b) du paragraphe 3.1 où le VPN-ID était indiqué via la signalisation VPN. Cependant, cette association est fournie en utilisant des moyens administratifs qui sortent du domaine d'application du présent document, plutôt que via la signalisation VPN. De plus, on DOIT s'assurer par des moyens administratifs que les entités NHRP sans capacité VPN ne communiquent qu'avec d'autres entités NHRP contenues dans le même VPN, ou avec des entités NHRP à capacité VPN avec des informations préconfigurées sur les identifiants de VPN-ID de ces entités sans capacité VPN.

Les entités NHRP à capacité VPN DEVRONT n'envoyer des informations aux entités NHRP sans capacité VPN que si ces informations appartiennent au VPN dans lequel l'entité sans capacité VPN est contenue. Les informations envoyées à une entité NHRP sans capacité VPN NE DOIVENT PAS inclure d'indication de l'identifiant de VPN.

Pour transférer correctement les paquets de données, il est nécessaire que les clients NHRP à capacité VPN en entrée sachent si leur partenaire est aussi à capacité VPN. Si la sortie est à capacité VPN, le NHC d'entrée va aussi utiliser les moyens décrits au paragraphe 3.1 sur un raccourci NBMA vers ce NHC de sortie pour spécifier le VPN auquel appartiennent les paquets de données.

À cette fin, il est spécifié une autre extension NHRP (en plus de celle spécifiée au paragraphe 5.3 de la [RFC2332]) qui est appelée extension de capacité d'appareil NHRP (voir le paragraphe 4.2 ci-dessous). Cette extension indique actuellement les capacités de VPN des entités NHRP de source et de destination, mais pourrait aussi être utilisée à l'avenir pour d'autres ajouts à NHRP pour indiquer d'autres capacités.

3.3 Traitement de l'extension de capacité d'appareil NHRP

L'extension de capacité d'appareil NHRP DOIT être rattachée à toutes les demandes de résolution NHRP générées par une entité NHRP de source à capacité VPN. L'appareil DEVRAIT régler le champ Capacités de source à indiquer qu'il prend en charge les VPN. Le bit Obligatoire DOIT être réglé à zéro, afin qu'un NHS sans capacité VPN puisse en toute sécurité ignorer l'extension lorsque il transmet la demande. De plus, le bit A (voir le paragraphe 5.2.1 de la [RFC2332]) DEVRAIT être réglé à indiquer que seules des informations de prochain bond d'autorité sont désirées pour éviter des réponses ne faisant pas autorité de la part de serveurs NHRP sans capacité VPN.

Comme un NHS sans capacité VPN n'est pas capable de traiter l'extension de capacité d'appareil NHRP, les administrateurs de réseau DOIVENT éviter les configurations dans lesquelles un client NHRP à capacité VPN est servi d'autorité par un serveur NHRP sans capacité VPN.

Si un NHS de sortie reçoit une demande de résolution NHRP avec une demande d'extension de capacité d'appareil NHRP incluse, il retourne une réponse de résolution NHRP avec une indication de ce que la destination est à capacité VPN en réglant correctement le fanion de capacités de la cible [voir au paragraphe 4.2].

Si un NHS de sortie reçoit une demande de résolution NHRP sans extension de capacité d'appareil NHRP incluse ou avec le fanion de capacités de source qui indique que l'appareil NHRP de source est sans capacité VPN, il PEUT agir d'une des façons suivantes :

- Il PEUT rejeter la demande de résolution NHRP ; cela parce que la destination à capacité VPN sera incapable de déterminer le contexte des informations reçues sur un raccourci NBMA provenant d'une source NHRP sans capacité VPN. C'est le cas par défaut.
- Si la destination est aussi sans capacité VPN, elle PEUT accepter la demande et retourner une réponse de résolution NHRP. Par défaut, les deux clients NHRP sans capacité VPN vont interagir correctement.
- Il PEUT s'offrir lui-même comme destination et résoudre la demande en utilisant sa propre adresse NBMA, si il a les capacités requises.
- Si l'identifiant de VPN indiqué identifie l'instance d'acheminement par défaut de la destination, le NHS PEUT accepter la demande et envoyer une réponse de résolution NHRP correspondante.

L'extension de capacité d'appareil NHRP NE DEVRAIT PAS être incluse dans les messages de demande d'enregistrement NHRP et de réponse.

3.4 Procédures de traitement d'erreur

Si une entité NHRP reçoit une PDU avec un VPN-ID indiqué via l'encapsulation VPN qui est en conflit avec un VPN-ID alloué précédemment à cette communication (par exemple, via la signalisation VPN ou administrativement par configuration) elle DEVRAIT renvoyer à l'envoyeur une indication d'erreur NHRP (voir au paragraphe 5.2.7 de la [RFC2332]) indiquant le code d'erreur 16 (discordance de VPN). Cependant, afin d'éviter certains problèmes de sécurité, une entité NHRP PEUT plutôt éliminer le paquet en silence.

Si une entité NHRP à capacité VPN reçoit un paquet pour un VPN qu'elle ne prend pas en charge, elle DEVRAIT envoyer une indication d'erreur NHRP à l'envoyeur, avec un code d'erreur de 17 (VPN non pris en charge). Cependant, afin d'éviter certains problèmes de sécurité, une entité NHRP PEUT plutôt éliminer le paquet en silence.

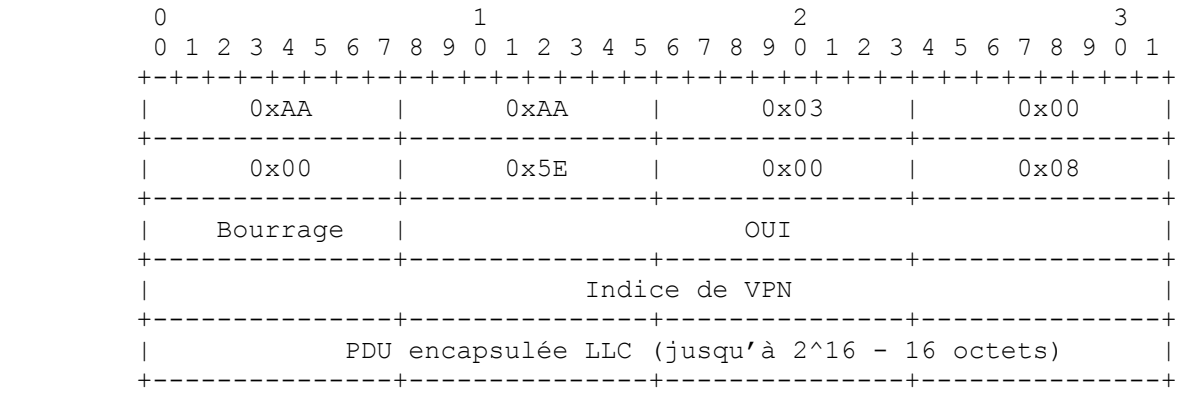
Si un NHS à capacité VPN ne peut pas trouver de chemin pour transmettre un message NHRP en relation avec un VPN, il DEVRAIT renvoyer une indication d'erreur NHRP à l'envoyeur, avec le code d'erreur 6 (adresse de protocole injoignable). Cependant, afin d'éviter certains problèmes de sécurité, une entité NHRP PEUT plutôt éliminer le paquet en silence.

Dans tous les cas, lorsque une indication d'erreur NHRP est retournée par une entité NHRP à capacité VPN, L'identifiant de VPN incorrect qui se rapporte à cette indication DEVRA être indiqué via encapsulation ou signalisation de VPN, sauf lors de l'envoi à un appareil NHRP sans capacité VPN (voir aux paragraphes 3.1 / 3.2 ci-dessus).

4. Formats de paquet NHRP

4.1 Encapsulation de VPN

Le format de l'en-tête d'encapsulation VPN est le suivant :

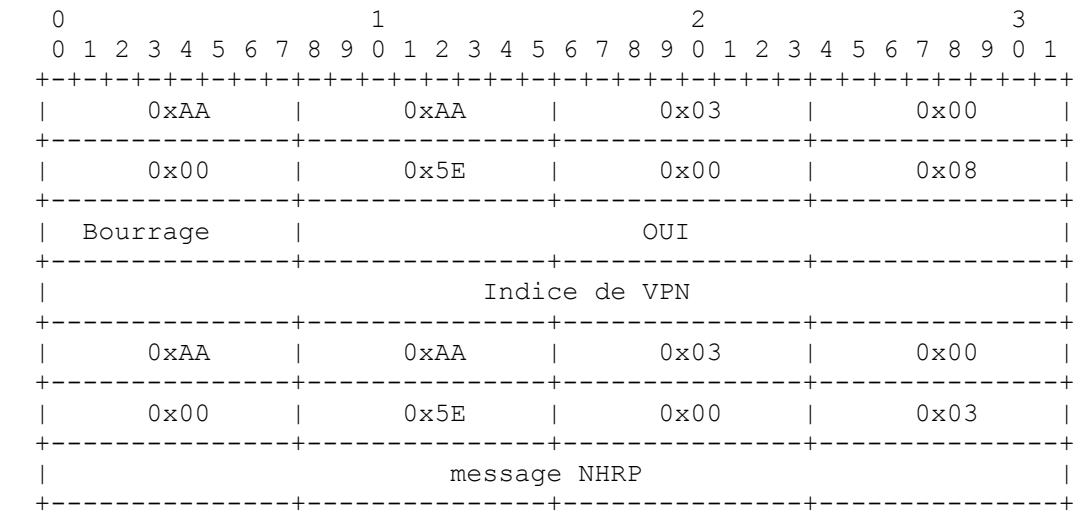


Il comporte les parties suivantes :

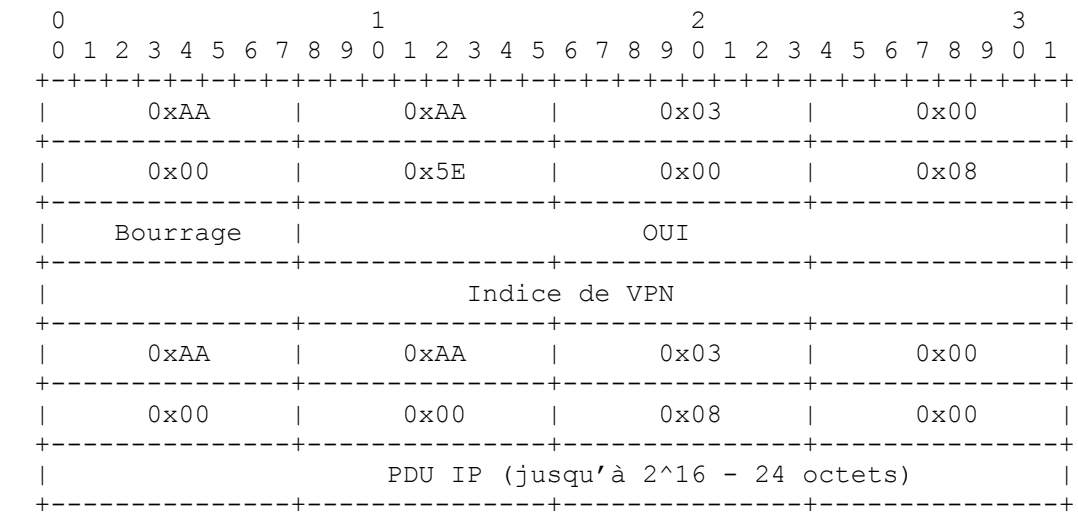
- indication LLC/SNAP (0xAA-AA-03)
- OUI (identifiant unique d'organisation de l'IANA) (0x00-00-5E)

- PID alloué par l'IANA pour l'encapsulation VPN (0x00-08)
- Champ de bourrage (inséré pour l'alignement sur 32 bits) il est codé à 0x00, et est ignoré à réception.
- OUI en rapport avec le VPN (voir la [RFC2685])
- Indice de VPN (voir la [RFC2685]).

Lorsque cet en-tête d'encapsulation est utilisé, le reste de la PDU DOIT être structuré conformément au format LLC/SNAP approprié (c'est-à-dire, qui aurait été utilisé sans l'en-tête d'encapsulation VPN supplémentaire). De façon correspondante, la figure suivante montre comment les messages NHRP sont transférés en utilisant l'encapsulation de VPN :

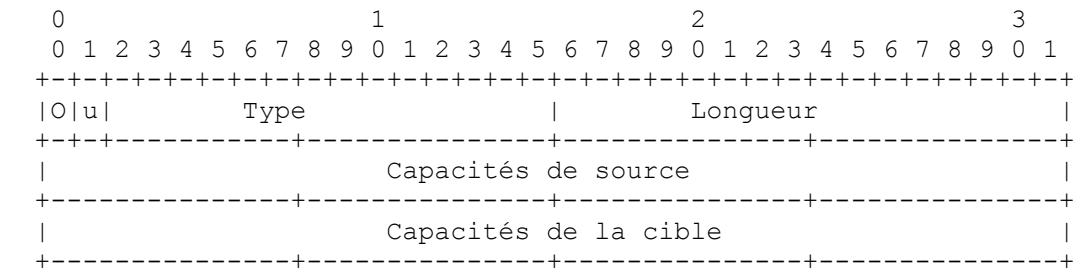


L'exemple suivant montre comment les paquets IP sont transférés par l'encapsulation de VPN :



4.2 Extension de capacités d'appareil NHRP

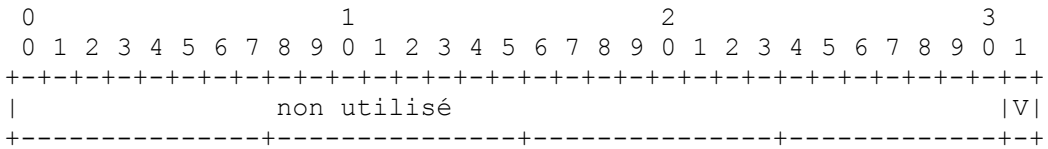
Le format de l'extension de capacités d'appareil NHRP est le suivant :



O : Obligatoire = 0 (extension non obligatoire)

u : Non utilisé et DOIT être réglé à zéro.
Type = 0x0009
Longueur = 0x0008

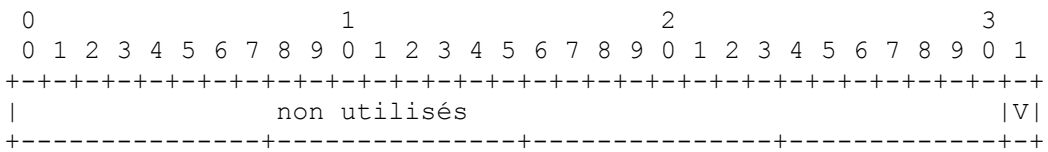
Champ Capacités de source :



Bit V :
0x0 – L'appareil NHRP de source est sans capacité VPN
0x1 – L'appareil NHRP de source est à capacité VPN

Les bits non utilisés DOIVENT être réglés à zéro à l'émission et ignorés à réception.

Champ Capacités de la cible :



Bit V :
0x0 – L'appareil NHRP de destination est sans capacité VPN
0x1 – L'appareil NHRP de destination est à capacité VPN

Les bits non utilisés DOIVENT être réglés à zéro à l'émission et ignorés à réception.

4.3 Codes d'erreur

Les autres codes d'erreur suivants sont définis en plus de ceux spécifiés au paragraphe 5.2.7 de la [RFC2332]):

16 – Discordance de VPN
Ce code d'erreur est retourné par un appareil NHRP à capacité VPN, si il reçoit une PDU avec un VPN-ID dans l'en-tête LLC/SNAP différent du VPN-ID qui a été spécifié précédemment via la signalisation de VPN.

17 - VPN non pris en charge
Ce code d'erreur est retourné par un appareil NHRP à capacité VPN, si il reçoit un message NHRP pour un VPN qu'il ne prend pas en charge.

5. Considérations pour la sécurité

Pour toute application de VPN, il est important que les informations en rapport avec le VPN ne soient pas mal dirigées vers d'autres VPN et ne soient pas accessibles lorsque elles sont transférées à travers une infrastructure publique ou partagée. Il est donc RECOMMANDÉ d'utiliser les fonctions de prise en charge de VPN spécifiées dans le présent document en combinaison avec l'authentification NHRP telle que spécifiée au paragraphe 5.3.4 de la [RFC2332]. Le paragraphe 5.3.4.4 de la [RFC2332] donne aussi des informations supplémentaires sur les considérations générales de sécurité qui se rapportent à NHRP.

Dans les cas où l'entité NHRP ne fait pas confiance à toutes les entités NHRP, ou est incertaine quant à la disponibilité de la chaîne d'authentification NHRP de bout en bout, elle peut utiliser IPsec pour la confidentialité, la protection de l'intégrité, etc.

6. Considérations relatives à l'IANA

L'identifiant de protocole LLC/SNAP 0x00-08 pour l'encapsulation de VPN a déjà été alloué par l'IANA en conjonction avec la [RFC2684]. La présente spécification ne requiert pas l'allocation d'autres identifiants de protocole LLC/SNAP au delà de celui-là.

On notera que l'IANA – en tant que propriétaire de l'OUI en rapport avec les VPN : 0x00-00-5E – est aussi elle-même une autorité de VPN qui peut allouer des indices de VPN pour identifier les VPN. L'utilisation de ces indices de VPN particuliers au sein du contexte de la présente spécification est réservée, et requiert l'allocation et l'approbation de l'IESG conformément à la RFC 2434.

Références

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

[RFC2332] J. Luciani et autres, "Protocole de résolution du prochain bond NBMA (NHRP)", avril 1998. *(P.S.)*

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

[RFC2685] B. Fox, B. Gleeson, "Identifiants de réseaux privés virtuels", septembre 1999. *(P.S.)*

Adresse des auteurs

Barbara A. Fox
Equipe Communications
100 Nagog Park
Acton, MA 01720
téléphone : +1-978-795-2009
mél : bfox@equipecom.com

Bernhard Petri
Siemens AG
Hofmannstr. 51
Munich, Germany, D-81359
téléphone : +49 89 722-34578
mél : bernhard.petri@icn.siemens.de

Déclaration complète de droits de reproduction

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