Groupe de travail Réseau
**Request for Comments : 3122**
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

A. Conta
Transwitch Corporation
juin 2001

# Extensions à la découverte de voisin IPv6 pour la spécification de découverte inverse

**Statut de ce mémoire**
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.
*(La présente traduction incorpore les errata 2819 et 3696)*



**Résumé**
Le présent mémoire décrit des extensions à la découverte de voisin IPv6 qui permettent à un nœud de déterminer et d'annoncer une adresse IPv6 correspondant à une certaine adresse de couche liaison. Ces extensions sont appelées Découverte inverse de voisin. La découverte inverse de voisin (IND, *Inverse Neighbor Discovery*) a été à l'origine développée pour les réseaux en relais de trame, mais elle peut aussi s'appliquer à d'autres réseaux avec un comportement similaire.

## Table des Matières



## 1. Introduction

Le présent document définit des extensions à la découverte de voisin (ND, *Neighbor Discovery*) IPv6 [RFC2461]. Les extensions sont appelées découverte inverse de voisin (IND, *Inverse Neighbor Discovery*) IPv6. L'IND permet à un nœud de connaître l'adresse de couche liaison d'un nœud distant directement connecté pour apprendre les adresses IPv6 de ce nœud. Un nœud qui utilise IND envoie des sollicitations et reçoit des annonces pour une ou plusieurs adresses IPv6 qui correspondent à une adresse de couche liaison connue.

La découverte inverse de voisin a été à l'origine développée pour les réseaux en relais de trame, mais peut aussi s'appliquer aux autres réseaux avec un comportement similaire.

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].

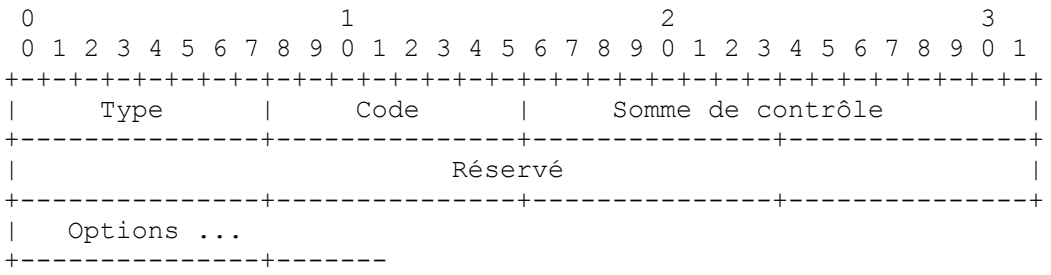
Il y a un certain nombre de similitudes et de différences entre les mécanismes décrits ici et ceux définis pour l'ARP inverse pour IPv4 dans la [RFC2390] ou ses documents de remplacement.

## 2. Messages de découverte inverse de voisin

Les messages suivants sont définis :

### 2.1 Message Sollicitation de découverte inverse de voisin

Un nœud envoie un message de sollicitation de découverte inverse de voisin pour demander une adresse IPv6 correspondant à une adresse de couche liaison du nœud cible tout en fournissant aussi sa propre adresse de couche liaison à la cible. Comme les adresses IPv6 du nœud distant ne sont pas connues, les sollicitations de découverte inverse de voisin (IND) sont envoyées comme diffusions groupées IPv6 tous nœuds [RFC2460], [RFC2590], [RFC2427]. Cependant, au niveau de la couche liaison, une sollicitation IND est envoyée directement au nœud cible, identifié par l'adresse de couche liaison connue.




Adresse de source : une adresse IPv6 allouée à l'interface à partir de laquelle ce message est envoyé.

Adresse de destination : L'adresse de diffusion groupée IPv6 Tous-les-nœuds. Cette adresse est spécifiée dans son format de portée liaison, qui est FF02::1.

Limite de bonds : 255

En-tête d'authentification : si une association de sécurité existe pour l'en-tête d'authentification IP entre l'envoyeur et la destination, l'envoyeur DEVRAIT alors inclure cet en-tête.

Champs ICMP :
Type : 141
Code : 0
Somme de contrôle : somme de contrôle ICMP. Voir la [RFC2463].
Réservé : ce champ n'est pas utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

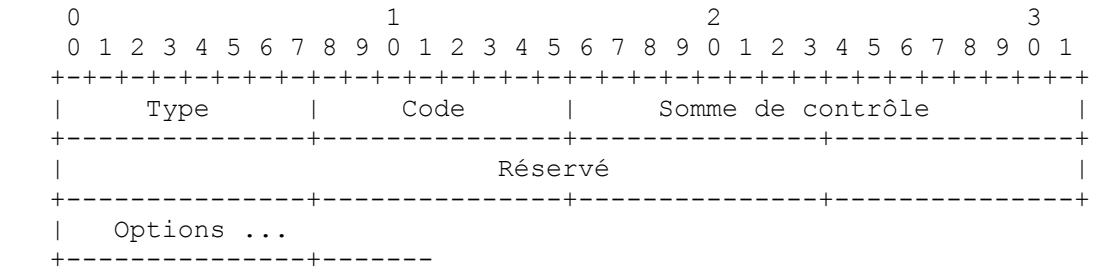
Options exigées : le nœud envoyeur DOIT envoyer les options suivantes dans le message Sollicitation:
Adresse de source de couche liaison : adresse de couche liaison de l'envoyeur.
Adresse cible de couche liaison : adresse de couche liaison du nœud cible.

Autres options valides : le nœud envoyeur PEUT choisir d'ajouter des options dans le message Sollicitation :
Liste d'adresses de source : liste de la ou des adresses IPv6 de l'interface identifiée par l'adresse de source de couche liaison. Cette option est définie à la section 3.
MTU : la MTU configurée pour cette liaison [RFC2461].

De futures versions du présent protocole pourront ajouter d'autres types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas et continuer le traitement du message.

### 2.2 Message Annonce de découverte inverse de voisin

Un nœud envoie des annonces de découverte inverse de voisin en réponse aux sollicitations de découverte inverse de voisin.




Champs IP :
Adresse de source : adresse allouée à l'interface d'où l'annonce est envoyée.
Adresse de destination : adresse de source d'une invocation de sollicitation de découverte inverse de voisin.
Limite de bonds : 255
En-tête d'authentification : si une association de sécurité existe pour l'en-tête d'authentification IP entre l'envoyeur et l'adresse de destination, l'envoyeur DEVRAIT alors inclure cet en-tête.

Champs ICMP :
Type : 142
Code : 0
Somme de contrôle : somme de contrôle ICMP. Voir la [RFC2463].
Réservé : champ de 32 bits non utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Options exigées : le nœud envoyeur DOIT envoyer les options suivantes dans le message Annonce :
Adresse de source de couche liaison : adresse de couche liaison du nœud qui transmet le message Annonce.
Adresse cible de couche liaison : adresse de couche liaison du nœud qui a transmis le message Sollicitation.
Liste d'adresses cibles : liste d'une ou plusieurs adresses IPv6 de l'interface identifiée par l'adresse cible de couche liaison dans le message de sollicitation de découverte inverse de voisin qui a invité à cette annonce. Cette option est définie à la Section 3.

Autres options valides : le nœud envoyeur PEUT choisir d'ajouter l'option suivante dans le message Annonce :
MTU : MTU configurée pour cette liaison [RFC2461].

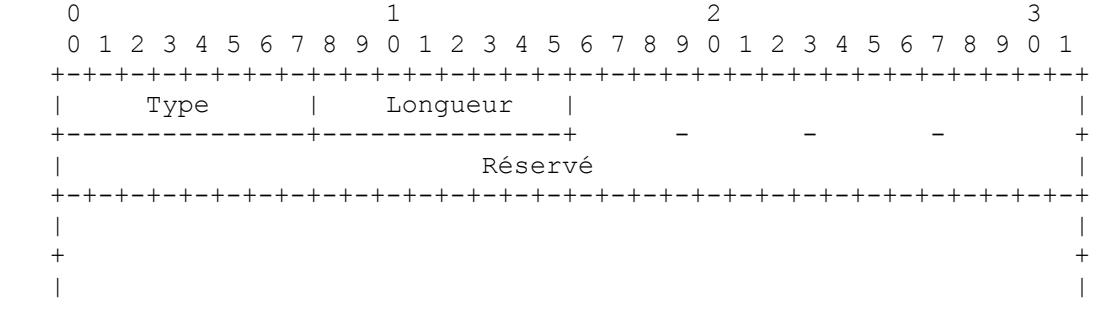
De futures versions du présent protocole pourront ajouter d'autres types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas et continuer le traitement du message.

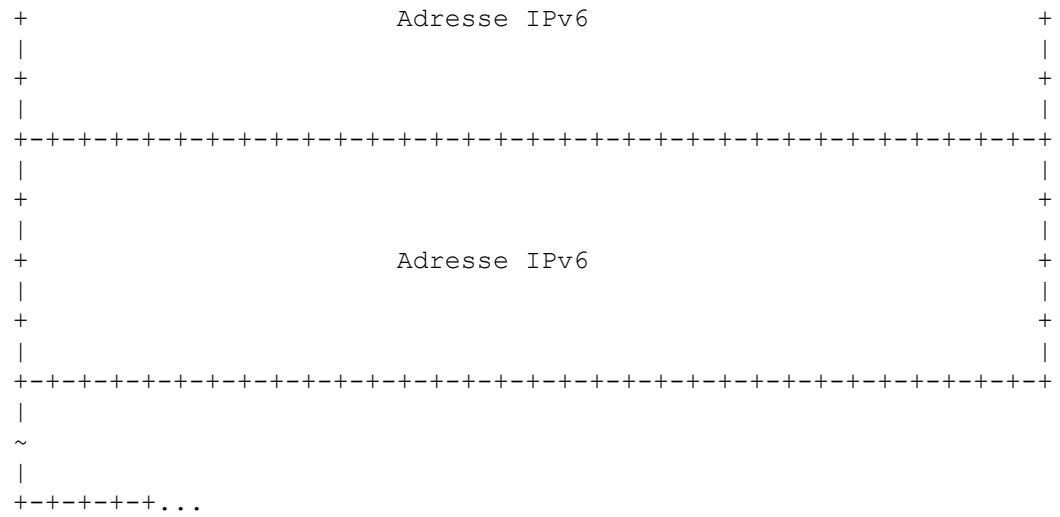
## 3. Formats des options de découverte inverse de voisin

Les messages de découverte inverse de voisin incluent des options de découverte de voisin [RFC2461] ainsi que des options spécifiques de découverte inverse de voisin : la liste d'adresses de source et la liste des adresses cibles.

### 3.1 Liste des adresses de source/cible

Les options Liste d'adresses de source et Liste des adresses cibles sont des options en TLV (type, longueur, champ de taille variable) (voir le paragraphe 4.6 de la [RFC2461] avec les champs suivants :






Champs :

Type : 9 pour la liste d'adresses de source, 10 pour la liste d'adresses cible.

Note : Ces valeurs de type d'option devraient être allouées à partir de la famille de valeurs de découverte de voisin IPv6.

Longueur : longueur de l'option (incluant les champs Type, Longueur, et Réservé) en unités de 8 octets. La valeur minimum pour Longueur est 3, pour une adresse IPv6.

Réservé : ce champ n'est pas utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Adresses IPv6 : une ou plusieurs adresses IPv6 de l'interface.

Description : la liste des adresses de source contient une liste d'adresses IPv6 de l'interface identifiée par l'adresse de source de couche liaison. La liste des adresses cibles contient une liste des adresses IPv6 de l'interface identifiée par l'adresse cible de couche liaison. Le nombre d'adresses "n" dans la liste est calculé sur la base de la longueur de l'option :

n = (Longueur - 1)/2 (Longueur est le nombre de groupes de 8 octets)

La liste des adresses de source DOIT tenir dans un message Sollicitation d'IND. Donc, dans le cas où toutes les adresses IPv6 d'une interface ne tiennent pas dans un message, l'option ne contient pas une liste complète. Pour une liste complète des adresses IPv6, un nœud devrait s'appuyer sur le message Annonce d'IND.

La liste des adresses cibles DEVRAIT être la liste complète des adresses de l'interface identifiée par l'adresse cible de couche liaison. Si la liste des adresses IPv6 d'une interface ne tient pas dans un message d'annonce d'IND, un ou plusieurs messages d'annonce d'IND, avec les mêmes champs que le premier message, DEVRAIENT suivre. La ou les options de liste d'adresses cibles du second message, et des suivants DEVRAIENT contenir le reste des adresses IPv6 de l'interface identifiée par l'adresse cible de couche liaison, qui ne tenait pas dans le premier message.

Note : La portée du mécanisme de découverte inverse de voisin est limitée à la découverte d'adresse IPv6, c'est-à-dire, à fournir des informations de transposition d'adresse. Donc, il n'y a aucune disposition ou règle concernant la façon dont un nœud utilise les adresses qui ont été retournées dans un message de découverte inverse. De plus, aucun type particulier d'adresse IPv6 n'est exclu de la liste d'adresses de source ou de cible. Par exemple, si une interface a configuré manuellement et autoconfiguré des adresses, y compris des temporaires, en envoi individuel, en diffusion groupée, etc..., la liste ne devrait en exclure aucune.

Note 2 : Une mise en œuvre NE DOIT PAS envoyer de dupliqués dans la liste d'adresses IPv6.

## 4. Protocole de découverte inverse de voisin

L'IND fonctionne essentiellement de la même façon que la ND [RFC2461] : le solliciteur d'une adresse IP de cible envoie sur une interface un message de sollicitation ; le nœud cible répond par un message d'annonce qui contient les informations demandées. Les informations apprises PEUVENT être mémorisées dans l'antémémoire de découverte de voisin [RFC2461], ainsi que les structures d'adresse IPv6 qui peuvent être associées à l'interface.

### 4.1 Traitement au nœud d'envoi

Un nœud solliciteur formate un message Sollicitation d'IND comme défini précédemment, il encapsule le paquet pour la couche de liaison spécifique et l'envoie directement au nœud cible. Bien que l'adresse IP de destination soit l'adresse de diffusion groupée Tous-les-nœuds, le message n'est envoyé qu'au nœud cible. Les champs significatifs pour le protocole IND sont l'adresse IP de source, l'adresse de source de couche liaison, l'adresse de couche liaison cible, et la MTU. Cette dernière peut être utilisée à régler la valeur optimum de la MTU pour la liaison.

Tout en attendant une réponse, l'envoyeur DEVRAIT retransmettre les messages Sollicitation d'IND approximativement toutes les fois qu'arrive à expiration le temporisateur de retransmission [RFC2461], même en l'absence de trafic supplémentaire pour le voisin. Les retransmissions DOIVENT être limitées en débit à au plus une sollicitation par voisin tous les RetransTimer intervalles.

Si aucune annonce d'IND n'a été reçue après MAX_MULTICAST_SOLICIT [RFC2461] sollicitations, la résolution d'adresse inverse a échoué. Si l'envoi de sollicitations était exigé par une couche supérieure, le module envoyeur DOIT notifier l'erreur à la couche supérieure par un mécanisme approprié (par exemple, en retournant une valeur provenant d'un appel de procédure).

### 4.2 Traitement au nœud de réception

#### 4.2.1 Traitement des messages de sollicitation de découverte inverse de voisin

Pour chaque sollicitation d'IND, le nœud receveur DEVRAIT formater en réponse une annonce d'IND appropriée en utilisant la paire d'adresses de couche liaison de source et de cible ainsi que l'adresse de source IPv6 provenant du message Sollicitation d'IND.

Si un nœud met à jour l'antémémoire de découverte de voisin avec les informations apprises des messages IND, le nœud receveur de la sollicitation d'IND DEVRAIT faire la transposition adresse IPv6/adresse de couche liaison de l'envoyeur – c'est-à-dire, l'adresse IP de source et l'adresse de source de couche liaison provenant du message de sollicitation dans son antémémoire de ND [RFC2461] comme il le ferait pour une sollicitation de ND.

Parce que les nœuds IPv6 peuvent avoir plusieurs adresses IPv6 par interface, un nœud qui répond à une sollicitation d'IND DEVRAIT retourner dans l'option Liste d'adresses cibles une liste contenant une ou plusieurs adresses IPv6 correspondant à l'interface identifiée par le champ Adresse cible de couche liaison dans le message de sollicitation. La liste NE DOIT PAS contenir de dupliqué.

#### 4.2.2 Traitement des messages Annonce de voisin inverse

Si un nœud met à jour l'antémémoire de découverte de voisin avec des informations apprises de messages d'IND, le nœud receveur de l'annonce d'IND DEVRAIT mettre dans son antémémoire de ND [RFC2461] la transposition d'adresse IPv6/adresse de couche liaison de l'envoyeur – c'est-à-dire, les adresses IP provenant de la liste des adresses cibles et de l'adresse source de couche liaison provenant du message d'annonce d'IND, comme il le ferait pour une annonce de ND.

### 4.3 Validation de message

Les messages de découverte inverse de voisin sont validés comme suit :

#### 4.3.1 Validation des sollicitations de découverte inverse de voisin

Un nœud DOIT éliminer en silence tout message reçu de sollicitations inverse de voisin qui ne satisfait pas à toutes les vérifications de validité suivantes :

- Le champ Limite de bonds IP a une valeur de 255, c'est-à-dire, le paquet n'aurait pas eu la possibilité d'avoir été transmis par un routeur.
- Si le message comporte un en-tête d'authentification IP, le message s'authentifie correctement.
- La somme de contrôle ICMP est valide.
- Le code ICMP est 0.
- La longueur ICMP (déduite de la longueur IP) est de 24 octets ou plus.
- L'adresse cible de couche liaison est une option requise et DOIT être présente.

- L'adresse de source de couche liaison est une option requise et DOIT être présente.
- Toutes les options incluses ont une longueur supérieure à zéro.

Le contenu du champ Réservé, et de toute option non reconnue, DOIT être ignoré. De futurs changements rétro compatibles au protocole pourront spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; les changements non rétro compatibles pourront utiliser des valeurs de code différentes.

Le contenu de toute option de découverte de voisin [RFC2461] qui n'est pas spécifié comme étant utilisé avec le message de sollicitation de découverte inverse de voisins DOIT être ignoré et le paquet traité comme normal. La seule option définie qui peut apparaître à côté des options requises est l'option MTU.

Toute sollicitation inverse de voisin qui satisfait aux vérifications de validité est appelée une "sollicitation valide".

### 4.3.2 Validation of annonces de découverte inverse de voisin

Un nœud DOIT éliminer en silence tout message d'annonce de découverte inverse de voisin reçu qui ne satisfait pas à toutes les vérifications de validité suivantes :

- Le champ Limite de bonds IP a la valeur de 255, c'est-à-dire, le paquet n'a pas eu la possibilité d'avoir été transmis par un routeur.
- Si le message comportait un en-tête d'authentification IP, le message s'authentifie correctement.
- La somme de contrôle ICMP est valide.
- Le code ICMP est 0.
- La longueur ICMP (déduite de la longueur IP) est de 48 octets ou plus.
- L'option Adresse de source de couche liaison est présente.
- L'option Adresse cible de couche liaison est présente.
- L'option Liste d'adresses cibles est présente.
- La longueur de l'option Liste d'adresses cibles est d'au moins 3.
- Toutes les autres options incluses ont une longueur supérieure à zéro.

Le contenu des champs Réservé, et de toute option non reconnue, DOIT être ignoré. De futurs changements rétro compatibles du protocole peuvent spécifier le contenu des champs Réservé ou ajouter de nouvelles options ; des changements non rétro compatible peuvent utiliser des valeurs de code différentes.

Le contenu de toute option définie [RFC2461] qui n'est pas spécifiée pour être utilisée avec les messages Annonce de découverte inverse de voisin DOIT être ignoré et le paquet traité comme normal. La seule option définie qui peut apparaître à côté des options exigées est l'option MTU.

Une annonce de voisin inverse qui réussit les vérifications de validité est appelées une "annonce valide".

## 5. Considérations sur la sécurité

Lorsque ils sont employés sur des circuits virtuels point à point, comme c'est le cas avec les réseaux en relais de trame, les messages de découverte inverse de voisin sont moins sensibles aux attaques en usurpation d'identité à partir de nœuds situés sur la liaison, comme ce serait le cas avec des liaisons en diffusion.

Comme la découverte de voisin, le protocole réduit l'exposition aux menaces provenant de nœuds hors liaison en l'absence d'authentification en ignorant les paquets d'IND reçus d'envoyeurs hors de la liaison. Il est vérifié que le champ Limite de bonds de tous les paquets reçus contient 255, la valeur légale maximum. Comme les routeurs décrémentent la limite de bonds sur tous les paquets qu'ils transmettent, les paquets reçus qui contiennent une limite de bonds de 255 doivent avoir été générés par un voisin.

Les échanges de paquets de protocole de découverte inverse de voisin peuvent être authentifiés en utilisant l'en-tête d'authentification IP [RFC2402]. Un nœud DEVRAIT inclure un en-tête d'authentification lors de l'envoi de paquets de découverte inverse de voisin si une association de sécurité à utiliser avec l'en-tête d'authentification IP existe pour l'adresse de destination. Les associations de sécurité peuvent avoir été créées par configuration manuelle ou par l'opération d'un protocole de gestion de clés.

La correction des en-têtes d'authentification reçus dans les paquets de découverte inverse de voisin DOIT être vérifiée et les paquets avec une authentification incorrecte DOIVENT être ignorés.

En cas d'utilisation avec le relais de trame, pour éviter un échec de vérification d'authentification de sécurité IP, le

prétraitement spécifique du relais de trame d'un message Sollicitation de découverte de voisin qui contient une option Adresse de source de couche liaison en format DLCI DOIT être fait par le nœud receveur après qu'il a achevé le traitement de sécurité IP.

Il DEVRAIT être possible à l'administrateur de système de configurer un nœud à ignorer tout message de découverte inverse de voisin qui n'est pas authentifié en utilisant soit l'en-tête d'authentification, soit l'encapsulation de charge utilise de sécurité. Un tel commutateur DEVRAIT par défaut admettre les messages non authentifiés.

Les questions de confidentialité sont traitées par les documents d'architecture de sécurité IP [RFC2401] et le document d'encapsulation de charge utile de sécurité [RFC2406].

## 6. Considérations relatives à l'IANA

Il a été demandé à l'IANA d'allouer deux nouvelles valeurs de type ICMPv6, comme décrit aux paragraphes 2.1 et 2.2. Ils ont été alloués à partir de la gamme informative de messages, comme défini au paragraphe 2.1 de la RFC2463. Il n'y avait pas de valeurs de code ICMPv6 définies pour ces types (autre que 0) ; de futures allocations seront à faire comme action de normalisation comme défini dans la RFC2434.

Il a aussi été demandé à l'IANA d'allouer deux nouveaux types ICMPv6 d'option de découverte de voisin comme défini au paragraphe 3.1. Aucune révision externe n'a été nécessaire.

## 7. Remerciements

Merci à Steve Deering, Thomas Narten et Erik Nordmark pour les discussions sur l'idée de découverte de voisin inverse. Merci à Thomas Narten, et Erik Nordmark, et aussi à Dan Harrington, Milan Merhar, Barbara Fox, Martin Mueller, et Peter Tam pour leur relecture attentive.
On doit aussi reconnaître que des parties du texte de la présente spécification sont inspirées du texte de la découverte de voisin IPv6 [RFC2461].

## 8. Références

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir www.iana.org)*)

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

[RFC2390] T. Bradley, C. Brown et A. Malis, "Protocole de résolution inverse d'adresse", septembre 1998. *(D.S.)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4835)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303)

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

[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

[RFC2463] A. Conta, S. Deering, "Protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4443) *(D.S.)*

[RFC2427] C. Brown, A. Malis, "Interconnexion multi protocole sur relais de trame", septembre 1998. (STD0055)

[RFC2590] A. Conta, A. Malis, M. Mueller, "Spécification de la transmission de paquets IPv6 sur les réseaux en relais de trame", mai 1999. *(P.S.)*

## 9. Adresse de l'auteur

Alex Conta
Transwitch Corporation
3 Enterprise Drive
Shelton, CT 06484
USA
téléphone : +1-203-929-8810
mél : aconta@txc.com

## Appendice A Découverte de voisin inverse avec des réseaux en relais de trame

Le présent appendice documente les détails de l'utilisation de la découverte inverse de voisin sur les réseaux en relais de trame, qui étaient trop spécifiques pour faire partie du contenu plus général des sections précédentes.

### A.1 Introduction

La découverte inverse de voisin (IND) s'applique spécifiquement aux nœuds de relais de trame. Les circuits virtuels permanents (PVC, *permanent virtual circuit*) en relais de trame et les circuit virtuels commutés (SVC, *switched virtual circuit*)) sont identifiés dans un réseau en relais de trame par un identifiant de connexion de liaison de données (DLCI, *Data Link Connection Identifier*). Chaque DLCI définit une seule connexion virtuelle pour un nœud de relais de trame à travers un réseau de zone étendue (WAN, *wide area network*). Un DLCI a en général une signification locale.

Au moyen de messages de signalisation spécifiques, un réseau en relais de trame peut annoncer à un nœud un nouveau circuit virtuel avec son DLCI correspondant. Le DLCI identifie un circuit virtuel à un nœud, et peut être utilisé comme l'équivalent d'une adresse de couche liaison d'un nœud distant, permettant à un nœud d'identifier au niveau de la couche liaison le nœud à l'autre extrémité du circuit virtuel. Par exemple dans la Figure 1, le nœud A (nœud local) identifie le circuit virtuel au nœud B (nœud distant) au moyen du DLCI = 30. Cependant, le message de signalisation ne contient pas d'information sur le DLCI utilisé par un nœud distant pour identifier le circuit virtuel au nœud local, qui pourrait être utilisé comme l'équivalent de l'adresse de couche liaison locale. Par exemple dans la Figure 1, le nœud B (nœud distant) peut identifier le circuit virtuel au nœud A au moyen du DLCI = 62.

De plus, le message qui est transmis au niveau de la couche liaison et est complètement indépendant du protocole IPv6 ne comporte aucune information d'adressage IPv6. La découverte inverse de voisin est un protocole qui permet à un nœud de relais de trame de découvrir l'équivalent d'une adresse locale de couche liaison, c'est-à-dire que l'identifiant au moyen duquel les nœuds distants identifient le nœud, et plus important, de découvrir les adresses IPv6 de l'interface à l'autre extrémité du circuit virtuel, identifiée par l'adresse de couche liaison distante.

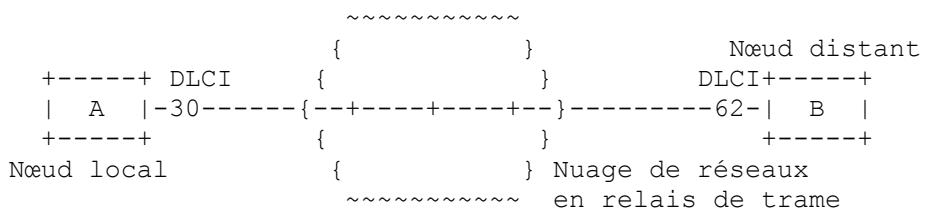



**Figure 1.**

Le protocole de découverte inverse de voisin (IND) IPv6 permet à un nœud de relais de trame de faire une découverte dynamique du DLCI par lequel un nœud distant identifie le circuit virtuel. Il permet aussi à un nœud d'apprendre les adresses IPv6 d'un nœud à l'extrémité distante d'un circuit virtuel.

### A.2 Message de découverte inverse de voisin

Les nœuds de relais de trame génèrent comme suit des messages de découverte inverse de voisin.

### A.2.1 Message Sollicitation de découverte inverse de voisin

L'envoyeur d'une sollicitation de découverte inverse de voisin ne connaît pas les adresses IPv6 du nœud distant, mais il connaît l'équivalent de l'adresse de couche liaison du nœud distant. Les sollicitations de découverte inverse de voisin (IND) sont envoyées comme diffusions groupées Tous-les-nœuds IPv6 [RFC2460], [RFC2590], [RFC2427]. Cependant, au niveau de la couche liaison, une sollicitation d'IND est envoyée directement au nœud cible, identifié par l'adresse de couche liaison (DLCI) connue.

Les champs du message, qui sont remplis suivant des considérations spécifiques du relais de trame sont :

Adresse de source de couche liaison
Pour le nœud de relais de trame envoyeur, l'adresse de source de couche liaison est l'équivalent de l'adresse de couche liaison par laquelle le nœud distant identifie la source de ce message. L'envoyeur peut n'avoir aucune connaissance de ces informations. Si l'envoyeur connaît ces informations, il DEVRAIT les inclure dans le champ, autrement, il DEVRAIT le laisser à zéro (vide). Ces informations, si elles sont présentes, peuvent être utilisées pour des besoin de débogage du réseau. Sans considération de l'action de l'envoyeur sur ce champ, avant tout traitement de découverte inverse de voisin, le receveur de ce message remplace ce champ, qu'il soit rempli ou non par l'envoyeur, par les informations portées par l'en-tête de relais de trame dans le champ DLCI. Le champ est codé en format DLCI comme défini par la [RFC2590].

Adresse cible de couche liaison
Pour le nœud de relais de trame envoyeur, le champ Adresse cible de couche liaison est rempli avec la valeur commue comme l'équivalent de l'adresse de couche liaison du nœud cible. Cette valeur est le DLCI du VC au nœud cible. Il est codé en format DLCI [RFC2590].

Pour illustrer la génération d'un message Sollicitation d'IND par un nœud de relais de trame, considérons l'exemple du Nœud A (Figure 1.) qui envoie une sollicitation d'IND au Nœud B. Les champs du message Sollicitation vont avoir les valeurs suivantes :
Au Nœud A (envoyeur du message Sollicitation d'IND) :
Adresse de source de couche liaison : DLCI = inconnu (écrasé par le receveur).
Adresse cible de couche liaison : DLCI = 30.
Au Nœud B (receveur du message Sollicitation d'IND) :
Adresse de source de couche liaison : DLCI = 62 (remplie par le receveur).
Adresse cible de couche liaison : DLCI = 30.

Note: Pour le relais de trame, les deux adresses ci-dessus sont en format Q.922 (DLCI), qui peut avoir 10 (par défaut), ou 23 bits significatifs d'adressage [RFC2590]. La longueur d'option (adresse de couche liaison) est exprimée en unités de 8 octets, donc, le DLCI devra être extrait des 8 octets sur la base du champ EA (bit 0) des second, troisième, ou quatrième octets (EA = 1). Les champs C/R, FECN, BECN, DE dans l'adresse Q.922 n'ont pas de signification pour IND et sont réglés à 0 [RFC2590].

MTU : La valeur mise dans l'option MTU est la MTU pour le circuit virtuel identifié par le DLCI connu [RFC2590].

### A.2.2 Message Annonce de découverte inverse de voisin

Un nœud de relais de trame envoie des annonces de découverte inverse de voisin en réponse aux sollicitations de découverte inverse de voisin.

Les champs du message, qui sont remplis suivant des considérations spécifiques du relais de trame sont :

Adresse de source de couche liaison
Pour le relais de trame, ce champ est copié du champ Adresse cible de couche liaison de la sollicitation de découverte inverse de voisin. Il est codé en format DLCI [RFC2590].

Adresse cible de couche liaison
Pour le relais de trame, ce champ est copié du champ Adresse de source de couche liaison de la sollicitation de découverte inverse de voisin. Il est codé en format DLCI [RFC2590].

Par exemple, si le Nœud B (Figure 1.) répond à une sollicitation d'IND envoyée par le Nœud A. avec une annonce d'IND, ces champs auront les valeurs suivantes :

Au Nœud B (envoyeur du message d'annonce) :
Adresse de source de couche liaison : DLCI = 30 (c'était la cible dans le message de sollicitation).
Adresse cible de couche liaison : DLCI = 62 (c'était la source dans le message de sollicitation).

Au Nœud A (receveur du message d'annonce provenant de B).
Adresse de source de couche liaison : DLCI = 30 (c'était la cible dans le message de sollicitation).
Adresse cible de couche liaison : DLCI = 62 (c'était la source dans le message de sollicitation).

Liste d'adresses cibles
C'est la liste d'une ou plusieurs adresses IPv6 de l'interface identifiée par l'adresse cible de couche liaison dans le message de sollicitation de découverte inverse de voisin qui a invité à cette annonce.

MTU : c'est la MTU configurée pour cette liaison (circuit virtuel) [RFC2461].

Note Dans le cas d'un réseau en relais de trame, les messages d'IND sont envoyés sur un circuit virtuel, qui agit comme une liaison virtuelle. Si le circuit virtuel se rompt, tous les participants au circuit reçoivent des messages de signalisation de couche de liaison appropriés, qui peuvent être propagés aux couches supérieures, incluant IPv6.

### A.3 Protocole de découverte inverse de voisin

Cette section de l'appendice ne traite que des aspects de la découverte inverse de voisin qui sont spécifiques des réseaux en relais de trame.

#### A.3.1 Traitement au nœud d'envoi

Un nœud de relais de trame solliciteur formate un message de sollicitation d'IND comme défini dans les paragraphes précédents, encapsule le paquet pour la couche de liaison de relais de trame [RFC2590] et l'envoie au nœud cible de relais de trame. Bien que l'adresse IP de destination soit l'adresse de diffusion groupée IPv6 Tous-les-nœuds, le message n'est envoyé qu'au nœud cible de relais de trame. Le nœud cible est le nœud distant connu sur la liaison représentée par le circuit virtuel.

#### A.3.2 Traitement au nœud receveur

##### A.3.2.1 Traitement des messages de sollicitation de voisin inverse

Un nœud de relais de trame, avant tout autre traitement, remplace dans l'adresse de source de couche liaison la valeur existante de DLCI par la valeur de DLCI provenant de l'en-tête de relais de trame de la trame contenant le message. La valeur de DLCI doit être formatée de façon appropriée dans le champ Adresse de source de couche liaison [RFC2590]. Cette opération est exigée pour permettre une interprétation correcte des champs dans la suite du traitement du message de sollicitation d'IND.

Pour un nœud de relais de trame, la valeur de MTU provenant du message de sollicitation PEUT être utilisée pour régler la MTU du receveur à une valeur qui soit plus optimale, au cas où cela n'aurait pas été déjà fait au moment de la configuration de l'interface.

##### A.3.2.2 Traitement des messages d'annonce de voisin inverse

Le nœud de relais de trame receveur de l'annonce d'IND PEUT mettre la transposition d'adresse IPv6/adresse de couche liaison de l'envoyeur – c'est-à-dire les adresses IP cible et l'adresse de source de couche liaison provenant du message d'annonce d'IND – dans son antémémoire de ND [RFC2461] comme il le ferait pour une annonce de ND.

De plus, le nœud de relais de trame receveur de l'annonce d'IND PEUT mémoriser l'adresse cible de couche liaison provenant du message comme valeur de DLCI à l'extrémité distante du VC. Cette valeur de DLCI est l'équivalent de l'adresse de couche liaison par laquelle le nœud distant identifie le receveur.

Si le nœud receveur de l'annonce d'IND a un réservoir d'adresses IPv6, et si la mise en œuvre le permet, il peut décider d'apparier des adresses IPv6 locales spécifiques à des adresses IPv6 spécifiques provenant de la liste cible dans les communications ultérieures sur le VC. Plus précisément, un tel appariement peut se fonder sur le fait que les adresses IPv6 sont sur le même sous réseau, c'est-à-dire ont le même préfixe.

## Déclaration complète de droits de reproduction

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