Groupe de travail Réseau
Request for Comments : 5072
RFC rendue obsolète : 2472
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

S. Varada, éd., Transwitch
D. Haskins
E. Allen

septembre 2007

IP version 6 sur PPP

Résumé
Le protocole point à point (PPP, *Point-to-Point Protocol*) fournit une méthode standard d'encapsulation des informations de protocole de couche réseau sur les liaisons point à point. PPP définit aussi un protocole de contrôle de liaison extensible, et propose une famille de protocole de contrôle de réseau (NCP, *Network Control Protocol*) pour établir et configurer différents protocoles de couche réseau.
Le présent document définit la méthode pour envoyer des paquets IPv6 sur des liaisons PPP, le NCP pour établir et configurer IPv6 sur PPP, et la méthode pour former des adresses IPv6 de liaison locale sur des liaisons PPP.
Il spécifie aussi les conditions pour effectuer la détection d'adresse dupliquée sur les adresses d'envoi individuel IPv6 globales configurées pour les liaisons PPP par l'autoconfiguration d'adresses à état plein ou sans état.
Le présent document rend obsolète la RFC 2472.

Table des Matières

1. Introduction

PPP a trois composants principaux :
1) Une méthode pour encapsuler les datagrammes sur des liaisons de série.
2) Un protocole de contrôle de liaison (LCP, *Link Control Protocol*) pour établir, configurer, et vérifier les connexions de liaison des données.
3) Une famille de protocole de contrôle du réseau (NCP, *Network Control Protocol*) pour établir et configurer différents protocoles de couche réseau.

Afin d'établir les communications sur une liaison en point à point, chaque extrémité de la liaison PPP doit d'abord envoyer des paquets de LCP pour configurer et vérifier les liaisons de données. Après l'établissement de la liaison et la négociation

des facilités facultatives comme nécessaire par le LCP, PPP doit envoyer des paquets de NCP pour choisir et configurer un ou plusieurs protocoles de couche réseau. Une fois que chaque protocole de couche réseau choisi a été configuré, les datagrammes de chaque protocole de couche réseau peuvent être envoyés sur la liaison.

Dans le présent document, le NCP pour établir et configurer IPv6 sur PPP est appelé le protocole de contrôle IPv6 (IPV6CP).

La liaison va rester configurée pour les communications jusqu'à ce que des paquets explicites de LCP ou NCP closent la liaison, ou jusqu'à ce que un événement externe se produise (défaillance d'alimentation à l'autre extrémité, abandon de la porteuse, etc.).

Le présent document rend obsolète la spécification antérieure de la [RFC2472]. Les changements par rapport à la RFC 2472 sont énumérés à l'Appendice B.

1.1 Spécification des exigences

Dans le présent document, plusieurs mots sont utilisés pour signifier les exigences de la spécification.

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

2. Envoi des datagrammes IPv6

Avant que des paquets IPv6 puissent être communiqués, PPP DOIT atteindre la phase de protocole de couche réseau, et le protocole de contrôle IPv6 DOIT atteindre l'état Ouvert.

Exactement un paquet IPv6 est encapsulé dans le champ Information des trames de couche de liaison des données PPP où le champ Protocole indique le type hex 0057 (Protocole Internet version 6).

La longueur maximum d'un paquet IPv6 transmis sur une liaison PPP est la même que la longueur maximum du champ Informations d'une trame de couche de liaison des données PPP. Les liaisons PPP qui prennent en charge IPv6 DOIVENT permettre que le champ Informations soit au moins aussi grand que la taille de MTU minimum de liaison requise pour IPv6 [RFC2460].

3. Protocole de contrôle de réseau PPP pour IPv6

Le protocole de contrôle IPv6 (IPV6CP, *IPv6 Control Protocol*) est chargé de configurer, activer, et désactiver les modules de protocole IPv6 sur les deux extrémités de la liaison point à point. IPV6CP utilise le même mécanisme d'échange de paquets que LCP. Les paquets IPV6CP ne peuvent pas être échangés avant que PPP ait atteint la phase de protocole de couche réseau. Les paquets IPV6CP qui sont reçus avant cette phase devraient être éliminés en silence.

Le protocole de contrôle IPv6 est exactement le même que LCP [RFC1661] avec les exceptions suivantes :

Champs de protocole de couche de liaison des données : exactement un paquet IPV6CP est encapsulé dans le champ Informations des trames de couche de liaison des données PPP où le champ Protocole indique le type hex 8057 (Protocole de contrôle IPv6).

Champ Code : seuls les codes 1 à 7 (Demande de configuration, Accusé de réception de configuration, Configure-Nak, Rejet de configuration, Demande de terminaison, Accusé de réception de terminaison et Code rejeté) sont utilisés. Les autres codes devraient être traités comme non reconnus et devraient résulter en un "Code rejeté".

Temporisations : les paquets IPV6CP ne peuvent pas être échangés avant que PPP ait atteint la phase de protocole de couche réseau. Une mise en œuvre devrait être prête à attendre que l'authentification et la détermination de la qualité de liaison se finissent avant de finir la temporisation d'attente d'un accusé de réception de configuration ou autre réponse. Il est suggéré qu'une mise en œuvre n'abandonne qu'après une intervention de l'utilisateur ou une durée configurable.

Types d'option de configuration : IPV6CP a un ensemble distinct d'options de configuration.

4. Options de configuration IPV6CP

Les options de configuration IPV6CP permettent la négociation des paramètres IPv6 désirables. IPV6CP utilise le même format d'options de configuration que défini pour LCP [RFC1661] mais avec un ensemble d'options distinct. Si une option de configuration n'est pas incluse dans un paquet Demande de configuration, la valeur par défaut pour cette option de configuration est supposée.

Les valeurs à jour du champ Type d'option IPV6CP sont spécifiées dans la base de données en ligne des "Numéros alloués" tenue par l'IANA [IANA]. L'allocation de valeur actuelle est la suivante :

1 : Identifiant d'interface
La seule option IPV6CP définie dans le présent document est l'identifiant d'interface. Toutes les autres option de configuration IPV6CP qui pouraient être définies à l'avenir seront définies dans des documents distincts.

4.1 Identifiant d'interface

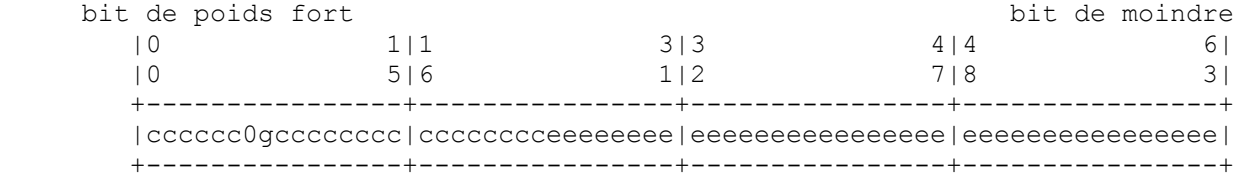
Description : cette option de configuration fournit un moyen de négocier un identifiant d'interface unique de 64 bits à utiliser pour l'autoconfiguration d'adresse [RFC4862] à l'extrémité locale de la liaison (voir la Section 5). Une demande de configuration doit contenir exactement une instance de l'option Identifiant d'interface [RFC1661]. L'identifiant d'interface DOIT être unique au sein de la liaison PPP; c'est-à-dire, à l'achèvement de la négociation, différentes valeurs d'identifiant d'interface sont à choisir pour les extrémités de la liaison PPP. L'identifiant d'interface peut aussi être unique sur une portée plus large.

Avant que cette option de configuration soit demandée, une mise en œuvre choisit ses projets d'identifiant d'interface. La valeur non zéro du projet d'identifiant d'interface DEVRAIT être choisie de telle façon que la valeur soit unique pour la liaison et, de préférence, reproductible de façon cohérente à travers les initialisations de l'automate à états finis de IPV6CP (cloture er réouverture administrative, réamorçages, etc.). La raison de la préférance pour un identifiant d'interface unique reproductible de façon cohérente plutôt qu'un identifiant d'interface complètement aléatoire est de fournir la stabilité des adresses de portée mondiale (voir l'Appendice A) qui peuvent être formées à partir de l'identifiant d'interface.

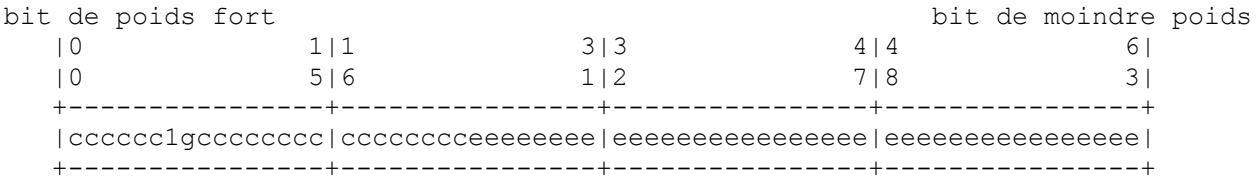
En supposant que les bits de l'identifiant d'interface sont numérotés de 0 à 63 en ordre canonique des bits, où le bit de poids fort est le bit numéro 0, le bit numéro 6 est le bit "u" (bit universel/local dans la terminologie IEEE EUI-64 [EUI-64]) qui indique si l'identifiant d'interface est ou non fondé sur un identifiant IEEE unique au monde (EUI-48 ou EUI-64 [EUI-64]) (voir le cas 1 ci-dessous). Il est réglé à un (1) si un identifiant IEEE unique au monde est utilisé pour déduire l'identifiant d'interface, et il est réglé à zéro (0) autrement.

Les méthodes suivantes sont dans l'ordre de préférence pour le choix des projets d'identifiant d'interface :

1) Si un identifiant IEEE mondial (EUI-48 ou EUI-64) est disponible n'importe où sur le nœud, il devrait être utilisé pour construire le projet d'identifiant d'interface du fait de ses propriétés d'unicité. Quand on extrait un identifiant IEEE mondial d'un autre appareil sur le nœud, on devrait faire attention que l'identifiant extrait soit présenté en ordre canonique [RFC2469].
   La seule transformation d'un identifiant EUI-64 est d'inverser le bit "u" (bit universel/local dans la terminologie IEEE EUI-64).
   Par exemple, pour un identifiant EUI-64 unique au monde de forme:

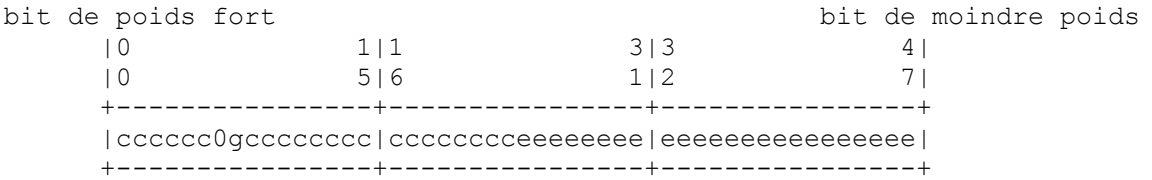


   où les "c" sont les bits de l'identifiant d'entreprise alloué, "0" est la valeur du bit universel/local pour indiquer la portée mondiale, "g" est le bit groupe/individuel, et les "e" sont les bits de l'identifiant d'extension, l'identifiant d'interface IPv6 serait de la forme :

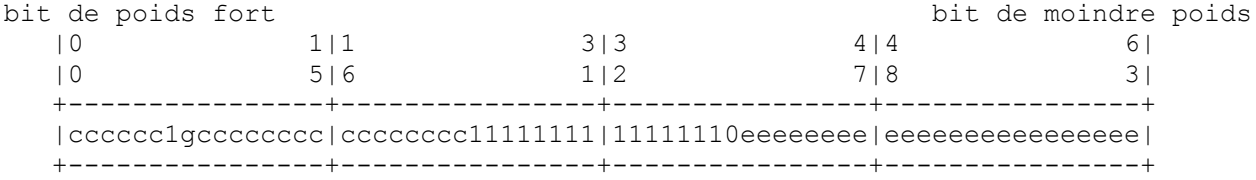


Le seul changement est l'inversion de la valeur du bit universel/local.

Dans le cas d'un identifiant EUI-48, il est d'abord converti en format EUI-64 en insérant deux octets, avec des valeurs hexadécimales de 0xFF et 0xFE, au milieu du MAC de 48 bits (entre les portions company_id et identifiant d'extension de la valeur EUI-48). Par exemple, pour un identifiant unique au monde EUI-48 de 48 bits de la forme :



où les "c" sont les bits de l'identifiant d'entreprise alloué, "0" est la valeur du bit universel/local pour indiquer la portée mondiale, "g" est le bit groupe/individuel, et les "e" sont les bits de l'identifiant d'extension, l'identifiant d'interface IPv6 serait de la forme :



2) Si un identifiant IEEE mondial n'est pas disponible, une source d'unicité différente devrait être utilisée. Les sources d'unicité suggérées incluent des adresses de couche de liaison, des numéro de série de machine, etc. Dans ce cas, le bit "u" de l'identifiant d'interface DOIT être réglé à zéro (0).

3) Si une bonne source d'unicité ne peut pas être trouvée, il est recommandé que soit généré un nombre aléatoire. Dans ce cas, le bit "u" de l'identifiant d'interface DOIT être réglé à zéro (0).

De bonnes sources [RFC1661] d'unicité ou d'aléa sont exigées pour que la négociation d'identifiant d'interface réussisse. Si ni un nombre unique ni un nombre aléatoire ne peuvent être générés, il est recommandé qu'une valeur de zéro soit utilisée pour l'identifiant d'interface transmis dans la demande de configuration. Dans ce cas, l'homologue PPP peut fournir un identifiant d'interface valide non à zéro dans sa réponse comme décrit ci-dessous. Noter que si au moins un des homologues PPP est capable de générer des numéros séparés non à zéro pour lui-même et son homologue, la négociation d'identifiant va réussir.

Quand une demande de configuration est reçue avec l'option Configuration d'identifiant d'interface et si l'homologue receveur met en œuvre cette option, l'identifiant d'interface reçu est comparé à l'identifiant d'interface de la dernière demande de configuration envoyée à l'homologue. Selon le résultat de la comparaison, une mise en œuvre DOIT répondre d'une des deux façons suivantes :

Si les deux identifiants d'interface sont différents mais si l'identifiant d'interface reçu est zéro, un Configure-Nak est envoyé avec une valeur d'identifiant d'interface non zéro suggérée pour que l'homologue distant l'utilise. Un tel identifiant d'interface suggéré DOIT être différent de l'identifiant d'interface de la dernière demande de configuration envoyée à l'homologue. Il est recommandé que la valeur suggérée soit reproducible de façon cohérente à travers les initialisations de l'automate à états finis IPV6CP (cloture et réouverture administrative, réamorçages, etc). Le bit "u" (universel/local) de l'identifiant suggéré DOIT être réglé à zéro (0) sans considération de sa source sauf si l'identifiant EUI-48/EUI-64 unique au monde déduit est fourni pour l'usage exclusif de l'homologue distant.

Si les deux identifiants d'interface sont différents et si l'identifiant d'interface reçu n'est pas zéro, l'identifiant d'interface DOIT être acquitté, c'est-à-dire, un accusé de réception de configuration est envoyé avec l'identifiant d'interface demandé,

ce qui signifie que l'homologue qui répond accepte l'identifiant d'interface demandé.

Si les deux identifiants d'interface sont égaux et ne sont pas à zéro, un Configure-Nak DOIT être envoyé spécifiant une valeur différente non à zéro d'identifiant d'interface suggéré pour l'usage de l'homologue distant. Il est recommandé que la valeur suggérée soit reproductible de façon cohérente à travers les initialisations de l'automate à états finis IPV6CP (cloture et réouverture administrative, réamorçages, etc). Le bit "u" (universel/local) de l'identifiant suggéré DOIT être réglé à zéro (0) sans considération de sa source sauf si l'identifiant unique au monde EUI-48/EUI-64 dérivé est fourni pour l'usage exclusif de l'homologue distant.

Si les deux identifiants d'interface sont égaux à zéro, la négociation d'identifiant d'interface DOIT être terminée en transmettant le Rejet de configuration avec la valeur d'identifiant d'interface réglée à zéro. Dans ce cas, un identifiant d'interface unique ne peut pas être négocié.

Si une demande de configuration est reçue avec l'option Configuration d'identifiant d'interface et si l'homologue receveur ne met pas en œuvre cette option, un Rejet de configuration est envoyé.

Une nouvelle demande de configuration NE DEVRAIT PAS être envoyée à l'homologue tant que le traitement normal causerait son envoi (c'est-à-dire, jusqu'à ce qu'un Configure-Nak soit reçu ou que le temporisateur de redémarrage arrive à expiration [RFC1661]).

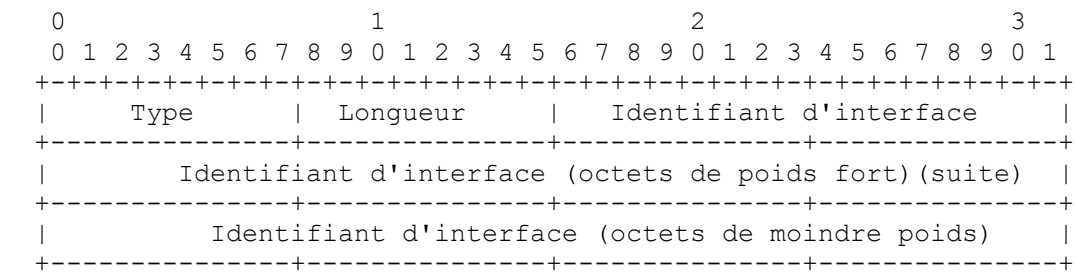
Une nouvelle demande de configuration NE DOIT PAS contenir l'option Identifiant d'interface si un Rejet de configuration d'identifiant d'interface valide est reçu.

La réception d'un Configure-Nak avec un identifiant d'interface suggéré différent de celui du dernier Configure-Nak envoyé à l'homologue indique un identifiant d'interface unique. Dans ce cas, une nouvelle demande de configuration DOIT être envoyée avec la valeur de l'identifiant suggéré dans le dernier Configure-Nak provenant de l'homologue. Mais si l'identifiant d'interface reçu est égal à celui envoyé dans le dernier Configure-Nak, un nouvel identifiant d'interface DOIT être choisi. Dans ce cas, une nouvelle demande de configuration DEVRAIT être envoyée avec le nouveau projet d'identifiant d'interface. Cette séquence (transmission de demande de configuration, réception de la demande de configuration, transmission du Configure-Nak, réception du Configure-Nak) pourrait se produire quelques fois, mais il est extrêmement improbable qu'elle de produise de façon répétée. Il est plus probable que les identifiants d'interface choisis à l'une et l'autre extrémité vont rapidement diverger, terminant la séquence.

Si la négociation de l'identifiant d'interface est exigée, et si l'homologue n'a pas fourni l'option dans sa demande de configuration, l'option DEVRAIT être ajoutée à un Configure-Nak. Le projet de valeur d'identifiant d'interface donnée doit être acceptable comme identifiant d'interface distant ; c'est-à-dire, elle devrait être différente de la valeur d'identifiant choisie pour l'extrémité locale de la liaison PPP. La prochaine demande de configuration de l'homologue peut inclure cette option. Si la prochaine demande de configuration n'inclut pas cette option, l'homologue NE DOIT PAS envoyer un autre Configure-Nak avec cette option incluse. Il devrait supposer que la mise en œuvre de l'homologue ne prend pas en charge cette option.

Par défaut, une mise en œuvre DEVRAIT tenter de négocier l'identifiant d'interface pour son extrémité de la connexion PPP.

Le format de l'option Configuration d'identifiant d'interface est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 1

Longueur : 10

Identifiant d'interface : identifiant d'interface de 64 bits, qui va très probablement être unique sur la liaison, ou zéro si une bonne source d'unicité ne peut pas être trouvée.

Par défaut : si aucun identifiant d'interface valide ne peut être négocié avec succès, aucune valeur d'identifiant d'interface par défaut ne devrait être supposée. Les procédures pour récupérer d'un tel cas ne sont pas spécifiées. Une approche est de configurer manuellement l'identifiant d'interface de l'interface.

5. Autoconfiguration sans état et adresses de liaison locale

L'identifiant d'interface des adresses d'envoi individuel IPv6 [RFC4291] d'une interface PPP DEVRAIT être négocié dans la phase IPV6CP de l'établissement de la connexion PPP (voir le paragraphe 4.1). Si aucun identifiant d'interface valide n'a été négocié avec succès, les procédures pour récupérer d'une telle situation ne sont pas spécifiées. Une approche est de configurer manuellement l'identifiant d'interface de l'interface.

L'identifiant d'interface négocié est utilisé par l'extrémité locale de la liaison PPP pour autoconfigurer une adresse d'envoi individuel de liaison locale IPv6 pour l'interface PPP. Cependant, on NE DEVRAIT PAS supposer que le même identifiant d'interface est utilisé pour configurer des adresses d'envoi individuel mondiales pour l'interface PPP en utilisant l'autoconfiguration d'adresse IPv6 sans état [RFC4862]. L'homologue PPP PEUT générer un ou plusieurs identifiants d'interface, par exemple, en utilisant une méthode décrite dans la [RFC4941], pour autoconfigurer une ou plusieurs adresses d'envoi individuel mondiales.

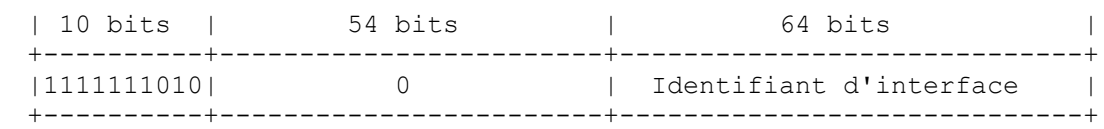
Tant que l'identifiant d'interface est négocié dans la phase IPV6CP de l'établissement de la connexion PPP, il est redondant d'effectuer la détection d'adresse dupliquée (DAD, *Duplicate Address Detection*) au titre du protocole d'autoconfiguration d'adresse IPv6 sans état [RFC4862] sur l'adresse de liaison locale IPv6 générée par l'homologue PPP. Il peut aussi être redondant d'effectuer la DAD sur des adresses d'envoi individuel mondiales configurées (en utilisant un identifiant d'interface qui est négocié durant IPV6CP ou généré, par exemple, selon la [RFC4941]) pour l'interface au titre du protocole d'autoconfiguration d'adresse IPv6 sans état [RFC4862] pourvu que les deux conditions suivantes soient satisfaites :

1) Les préfixes annoncés par des messages Annonce de routeur par le routeur d'accès qui termine la liaison PPP sont exclusifs de la liaison PPP.

2) Le routeur d'accès qui termine la liaison PPP n'autoconfigure aucune adresse IPv6 d'envoi individuel mondiale à partir des préfixes qu'il annonce.

Donc, il est RECOMMANDÉ que pour les liaisons PPP avec l'option Identifiant d'interface IPV6CP activée et qui satisfont les deux conditions sus-mentionnées, la valeur par défaut de la variable d'autoconfiguration DupAddrDetectTransmits de la [RFC4862] soit réglée à zéro par la gestion du système. Les réseaux 3GPP2 sont un exemple d'une technologie qui utilise PPP pour permettre à un hôte d'obtenir une adresse IPv6 mondiale en envoi individuel et satisfait les deux conditions sus-mentionnées [X.S0011]. Les réseaux 3GPP en sont un autre exemple ([TS-29.061], [TS-23.060]).

Adresses de liaison locale : les adresses de liaison locales des interfaces PPP ont le format suivant :



Les 10 bits de poids fort de l'adresse sont le préfixe de liaison locale FE80::. 54 bits de zéro bourrent l'adresse entre le préfixe de liaison locale et les champs d'identifiant d'interface.

6. Considérations sur la sécurité

Le manque de sécurité de la liaison, comme l'authentification, déclenche des soucis de sécurité soulevés dans la [RFC4862] quand la méthode de l'autoconfiguration d'adresse sans état est employée pour la génération d'adresses IPv6 mondiales en envoi indivuel à partir d'identifiants d'interface qui sont soit négociés par IPV6CP soit générés, par exemple, en utilisant une méthode décrite dans la [RFC4941]. Donc, les mécanismes qui sont appropriés pour s'assurer de la sécurité de la

liaison PPP sont traités ci-dessous, avec la référence à un modèle générique de menace.

Les mécanismes qui sont appropriés pour s'assurer de la sécurité de la liaison PPP sont : 1) les listes de contrôle d'accès qui appliquent des filtres au trafic reçu sur la liaison pour appliquer la politique d'admission, 2) un protocole d'authentification qui facilite les négociations entre homologues [RFC3748] pour choisir une méthode d'authentification (par exemple, MD5 [RFC1321]) pour la validation de l'homologue, et 3) un protocole de chiffrement qui facilite les négociations entre homologues pour choisir les algorithmes de chiffrement (ou crypto-suites) pour assurer la confidentialité des données [RFC1968].

Certaines menaces sont associées aux interactions avec l'homologue sur une liaison PPP même avec une ou plusieurs des mesures de sécurité ci-dessus en place. Par exemple, en utilisant la méthode d'authentification MD5 [RFC1321] on s'expose à une attaque en répétition, où un attaquant pourrait intercepter et répéter le hachage de l'identité et du mot de passe d'une station pour obtenir l'accès à un réseau. Il est conseillé à l'utilisateur de la présente spécification de se référer à la [RFC3748] qui présente un modèle de menace générique, pour comprendre les menaces qui pèsent sur la sécurité d'une liaison. La référence à la [RFC3748] donne aussi un cadre pour spécifier les exigences du choix d'une méthode d'authentification pour une application.

7. Considérations relatives à l'IANA

L'IANA a alloué la valeur 1 au champ Type de l'option Identifiant d'interface de datagramme IPv6 spécifiée dans le présent document. L'allocation actuelle est mise à jour dans [IANA].

8. Remerciements

Le présent document emprunte à l'option de numéro magique LCP et à ce titre se fonde partiellement sur des travaux antérieurs du groupe de travail PPP.

L'éditeur remercie de leurs apports les membres de la communauté IPv6 pour la mise à jour de la RFC 2472. Merci, en particulier, à Pete Barany et Karim El Malki de leurs contributions techniques. Merci aussi à Alex Conta de sa relecture attentive, à Stephen Kent de son aide sur les aspects de sécurité, et à Spencer Dawkins et Pekka Savola de leur aide. Finalement, l'auteur remercie Jari Arkko de son initiative pour mener cette spécification à son terme.

9. Références

9.1 Références normatives

[EUI-64] IEEE, "Guidelines For 64-bit Global Identifier (EUI-64)", http://standards.ieee.org/regauth/oui/tutorials/EUI64.html

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153)

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

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

[RFC2472] D. Haskin, E. Allen, "IP version 6 sur PPP", décembre 1998. (*Obsolète, voir* RFC5072, RFC5172) *(P.S.)*

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

[RFC4862] S. Thomson et autres, "Auto configuration d'adresse IPv6 sans état", septembre 2007. (*Remplace* RFC2462) *(D.S.)*

[RFC4941] T. Narten et autres, "Extensions de confidentialité pour l'auto configuration d'adresse sans état dans IPv6", septembre 2007. (*D.S. ; remplace* RFC3041 ; r*emplacée par* RFC8981*)*

9.2 Références pour information

[IANA] IANA, "Assigned Numbers," http://www.iana.org/numbers.html

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

[RFC1968] G. Meyer, "Protocole de contrôle de chiffrement en PPP (ECP)", juin 1996. *(P.S.)*

[RFC2469] T. Narten, C. Burton, "Avertissement sur l'ordre canonique des adresses de couche Liaison", décembre 1998. *(Info.)*

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (*MàJ par* RFC6422 et RFC6644, RFC7227 *; rendue obsolète par* RFC8415)

[RFC3748] B. Aboba et autres, "Protocole extensible d'authentification (EAP)", juin 2004. *(P.S., MàJ par* RFC5247)

[TS-29.061] 3GPP TS 29.061 V6.4.0, "Interworking between the Public Land Mobile Network (PLMN) Supporting packet based services and Packet Data Networks (PDN) (Release 6)", avril 2005.

[TS-23.060] 3GPP TS 23.060 v6.8.0, "General Packet Radio Service (GPRS); Service description; Stage 2 (Release 6)", mars 2005.

[X.S0011] 3GPP2 X.S0011-002-C v1.0, "cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Services", septembre 2003.

Appendice A. Adresses de portée mondiale

Un nœud sur la liaison PPP crée des adresses d'envoi individuel mondiales par des mécanismes d'autoconfiguration d'adresse sans état ou à états pleins. Dans l'autoconfiguration d'adresse sans état [RFC4862], le nœud s'appuie sur les préfixes de sous réseau annoncés par le routeur via les messages Annonce de routeur pour obtenir les adresses d'envoi individuel mondiales d'un identifiant d'interface. Dans l'autoconfiguration d'adresse à états pleins, l'hôte s'appuie sur un serveur à états pleins, comme DHCPv6 [RFC3315], pour obtenir les adresses d'envoi individuel mondiales.

Appendice B. Changements par rapport à la RFC 2472

Les changements suivants ont été faits depuis la RFC 2472 "IPv6 sur PPP" :

- Des mises à jour mineures aux Sections 3 et 4.
- Mise à jour du texte du paragraphe 4.1 pour inclure la référence à l'Appendice A et des précisions du texte.
- Suppression du paragraphe 4.2 sur le protocole de compression IPv6 fondée sur la recommandation de l'IESG, et création d'un nouveau document sur la voie de la normalisation pour couvrir la négociation du protocole de compression de datagramme IPv6 en utilisant IPV6CP.
- Mise à jour du texte de la Section 5 pour : (a) permettre l'utilisation d'un ou plusieurs identifiants d'interface générés par un homologue, en plus de l'ajout de l'utilisation de l'identifiant d'interface négocié entre les homologues de la liaison, dans la création d'adresses d'envoi individuel mondiales pour l'interface PPP locale, et (b) identifier les cas de DAD de création d'adresses non de liaison locale.
- Ajout de nouvelles références et mise à jour des références.

- Ajout de l'Appendice A

Adresse des auteurs

Dimitry Haskin

Ed Allen

Srihari Varada
TranSwitch Corporation
3 Enterprise Dr.
Shelton, CT 06484. US.
téléphone : +1 203 929 8810
mél : varada@ieee.org

Déclaration complète de droits de reproduction