Groupe de travail Réseau
Request for Comments : 5172
RFC rendue obsolète : 2472
Catégorie : Sur la voie de la normalisation

S. Varada, éditeur, Transwitch
mars 2008

Traduction Claude Brière de L'Isle

Négociation de compression de datagramme IPv6 avec le protocole de contrôle IPv6

Résumé
Le protocole point à point (PPP) donne une méthode standard d'encapsulation des informations de protocole de couche réseau sur les liaisons point à point. PPP définit aussi un protocole extensible de contrôle de liaison, et propose une famille de protocole de contrôle du réseau (NCP, *Network Control Protocol*) pour établir et configurer différents protocoles de couche réseau.

Le protocole de contrôle IPv6 (IPV6CP, *IPv6 Control Protocol*) qui est un NCP pour liaisons PPP, permet la négociation des paramètres désirables pour une interface IPv6 sur PPP.

Le présent document définit l'option de compression de datagramme IPv6 qui peut être négociée par un nœud sur la liaison à travers IPV6CP.

Table des Matières

1. Introduction....1
1.1 Spécification des exigences....2
2. Options de configuration IPV6CP....2
2.1 IPv6-Compression-Protocol....2
3. Considérations sur la sécurité....3
4. Considérations relatives à l'IANA....3
5. Considérations de gestion....3
6. Remerciements....3
7. Références....3
7.1 Références normatives....3
7.2 Références pour information....4
Adresse de l'éditeur....4
Déclaration complète de droits de reproduction....4

1. Introduction

PPP [RFC1661] a trois principaux composants :
1) une méthode d'encapsulation des datagrammes sur des liaisons en série,
2) un protocole de contrôle de liaison (LCP, *Link Control Protocol*) pour établir, configurer, et tester la connexion de liaison des données,
3) une famille de protocoles 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 tester la liaison de données. Après l'établissement de la liaison et que les facilités facultatives ont été négociées comme nécessaire pour le LCP, PPP doit envoyer des paquets de NCP pour choisir et configurer un ou plusieurs protocoles de couche réseau. Une fois que chacun des protocoles de couche réseau a été configuré, les datagrammes provenant de chaque protocole de couche réseau peuvent être envoyés sur la liaison. La liaison

va rester configurée pour les communications jusqu'à ce qu'un paquet explicite de LCP ou NCP close la liaison, ou jusqu'à ce qu'un événement externe se produise (panne de courant à l'autre extrémité, abandon de la porteuse, etc.).

Dans la spécification de IPv6 sur PPP [RFC5072], le NCP, ou IPV6CP, pour l'établissement et la configuration de IPv6 sur PPP est défini. La même spécification définit le paramètre Identifiant d'interface, qui peut être utilisé pour générer les adresses IPv6 de liaison locale et uniques au monde, pour la négociation.

Dans la présente spécification, le paramètre de compression à utiliser pour la compression de datagramme IPv6 est défini. Avec la [RFC5072], le présent document rend obsolète la [RFC2472]. Cependant, aucun changement du protocole n'a été introduit par rapport à la RFC 2472.

1.1 Spécification des exigences

Dans ce 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. Options de configuration IPV6CP

Les options de configuration IPV6CP permettent la négociation des paramètres IPv6 désirables. IPV6CP utilise le même format d'option 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 configuraion, la valeur par défaut pour cette option de configuration est supposée.

La seule option IPV6CP définie dans ce document est IPv6-Compression-Protocol. Le champ Type pour cette option IPV6CP est la suivante :

2 IPv6-Compression-Protocol

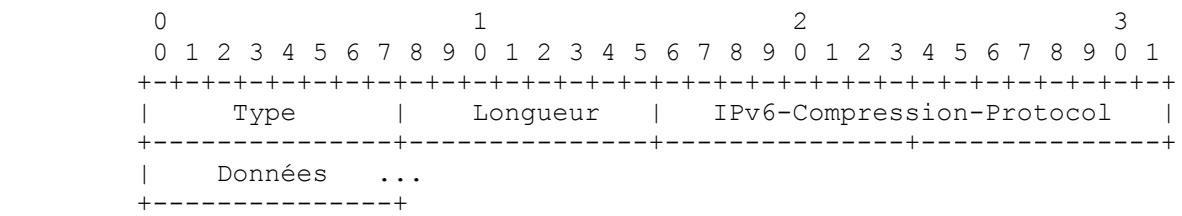
Noter que les valeurs à jour du champ Type d'option IPV6CP sont spécifiées dans la base de données en ligne des "Numéros alloués" tenue par l'IANA [IANA].

2.1 IPv6-Compression-Protocol

Cette option de configuration donne le moyen de négocier l'utilisation d'un protocole de compression de paquet IPv6 spécifique. L'option de configuration IPv6-Compression-Protocol est utilisée pour indiquer la capacité de recevoir des paquets compressés. Chaque extrémité de la liaison DOIT demander séparément cette option si la compression bidirectionnelle est désirée. Par défaut, la compression n'est pas activée.

La compression IPv6 négociée avec cette option est spécifique des datagrammes IPv6 et ne doit pas être confondue avec la compression résultant d'une méthode de compression négociée via le protocole de contôle de compression (CCP, *Compression Control Protocol*) PPP [RFC1962], qui affecte potentiellement tous les datagrammes.

Un résumé du format de l'option de configuration IPv6-Compression-Protocol est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 2

Longueur : ≥ 4

IPv6-Compression-Protocol : le champ IPv6-Compression-Protocol est de deux octets et indique le protocole de compression désiré. Les valeurs pour ce champ sont toujours les mêmes que les valeurs du champ Protocole de couche de liaison des données PPP pour ce même protocole de compression. Les valeurs du champ IPv6-Compression-Protocol ont été allouées dans la [RFC2507], la [RFC3544] pour la compression d'en-tête IP (0061), et la [RFC3241] pour la compression d'en-tête robuste (ROHC, *Robust Header Compression*) (0003). D'autres allocations peuvent être faites dans des documents qui définissent des algorithmes de compression spécifiques.

Données : le champ Données est de zéro, un, ou plusieurs octets et contient des données supplémentaires comme déterminé par le protocole de compression particulier.

La valeur par défaut (en l'absence de négociation de cette option) est de n'avoir pas de protocole de compression IPv6 activé.

3. Considérations sur la sécurité

L'absence de sécurité de liaison appropriée, comme l'authentification, avant les transferts de données peut permettre des attaques par interposition résultant en la perte de l'intégrité et de la confidentialité des données. Les mécanismes qui sont appropriés pour assurer la sécurité de la liaison PPP sont traitées ci-dessous avec les références à un modèle de menace générique.

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

Certaines menaces sont associées aux interactions entre homologues sur une liaison même avec une ou plusieurs des mesures de sécurité ci-dessus. Par exemple, utiliser la méthode d'authentification MD5 [RFC1321] expose à des attaques en répétition, dans lesquelles un attaquant pourrait intercepter et répéter l'identité et le hachage du mot de passe d'une station pour obtenir l'accès à un réseau. L'utilisateur de la présente spécification se réfèrera à la [RFC3748], qui présente un modèle générique de menaces, 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 pour le choix d'une méthode d'authentification pour une application donnée.

4. Considérations relatives à l'IANA

Aucune action spécifique n'est nécessaire pour l'allocation d'une valeur pour le champ Type de l'option de compression de datagramme IPv6 spécifiée ici. L'allocation actuelle est mise à jour dans le registre "PPP IPV6CP CONFIGURATION OPTIONS" pour l'élément IPv6-Compression-Protocol (2) à [IANA]. Cependant, la RFC de référence pour cet élément a été changée en 5172.

Aucune action n'est nécessaire pour l'allocation des valeurs de IPV6-Compression-Protocol, car ces valeurs ont déjà été définies par les autres documents mentionnés au paragraphe 2.1. Les valeurs pour ce champ sont toujours les mêmes que les valeurs du champ Protocole de couche de liaison des données PPP pour le même protocole de compression. Par suite, une future allocation de ces valeurs est gouvernée par la [RFC3818] qui exige le consensus de l'IETF. Les valeurs actuelles sont dans le registre "Types de protocoles de compression IPv6". Cependant la RFC de référence pour ce registre a été changée en 5172.

5. Considérations de gestion

Du point de vue du fonctionnement, l'état de la négociation et l'algorithme de compression sur la liaison devraient être observables par l'opérateur qui gère le réseau. Il n'y a pas d'interface de gestion standard qui couvre cela au moment de la rédaction de la présente spécification.

6. Remerciements

L'éditeur est reconnaissant à Jari Arkko de ses conseils pour le présent document et à James Carlson des ses suggestions utiles. Des remerciements sont aussi dus à D. Haskin et E. Allen pour le travail de spécification fait sur les RFC 2023 et RFC 2472.

7. Références

7.1 Références normatives

[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)

[RFC2507] M. Degermark, B. Nordgren, S. Pink, "Compression d'en-tête IP", février 1999. *(P.S.)*

[RFC3241] C. Bormann, "Compression d'en-tête robuste (ROHC) sur PPP", avril 2002. (*MàJ par* RFC4815) *(P.S.)*

[RFC3544] T. Koren, S. Casner, C. Bormann, "Compression d'en-tête IP sur PPP", juillet 2003. (Remplace RFC2509) *(P.S.)*

[RFC5072] S.Varada et autres, "IP version 6, sur PPP", septembre 2007. (*Remplace* RFC2472) *(D.S , MàJ par* RFC8064)

7.2 Références pour information

[IANA] IANA, http://www.iana.org.

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

[RFC1962] D. Rand, "Protocole de contrôle de compression en PPP (CCP)", juin 1996.

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

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

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

[RFC3818] V. Schryver, "Considérations relatives à l'IANA sur le protocole point à point (PPP)", juin 2004. (BCP0088)

Adresse de l'éditeur

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