Groupe de travail Réseau
Request for Comments : 1968
Catégorie : En cours de normalisation

G. Meyer, Spider Systems
juin 1996
Traduction Claude Brière de L'Isle

Protocole de contrôle de chiffrement PPP (ECP)

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.

Résumé
Le protocole point à point (PPP) [RFC1661] donne une méthode standard pour transporter des datagrammes multi protocoles sur des liaisons point à point. PPP définit aussi un protocole extensible de contrôle de liaison.

Le présent document définit une méthode pour négocier le chiffrement des données sur les liaisons PPP.

Conventions
Des conventions de langage sont utilisées dans les éléments de spécification de ce document :

- DOIT – l'élément est une exigence absolue de la spécification. DOIT n'est utilisé que lorsque il est en fait exigé pour l'interopération, et non pour essayer d'imposer une méthode particulière aux mises en œuvre lorsque ce n'est pas exigé pour l'interopérabilité.

- DEVRAIT – l'élément devrait être toujours suivi sauf circonstances exceptionnelles.

- PEUT ou facultatif – l'élément est vraiment facultatif et peut être suivi ou ignoré selon les besoins de la mise en œuvre.

Les mots "devrait" et "peut" sont aussi utilisés en minuscules, dans leur sens ordinaire.

Table des Matières

1. Introduction

Afin d'établir des communications sur une liaison PPP, chaque extrémité de la liaison doit d'abord envoyer des paquets LCP pour configurer et vérifier la liaison de données durant la phase d'établissement de la liaison. Après que la liaison a été établie, des facilités facultatives peuvent être négociées en tant que de besoin.

Une de ces facilités est le chiffrement des données. Des méthodes de chiffrement très diverses peuvent être négociées, bien que normalement seulement une méthode soit utilisée dans chaque direction de la liaison.

Un algorithme de chiffrement différent peut être négocié dans chaque direction, pour des questions de vitesse, de coût, de mémoire ou d'autres considérations.

2. Protocole de contrôle de chiffrement (ECP)

Le protocole de contrôle de chiffrement (ECP, *Encryption Control Protocol*) est chargé de configurer et activer les algorithmes de chiffrement des données sur les deux extrémités de la liaison point à point.

ECP utilise le même mécanisme d'échange de paquet que le protocole de contrôle de liaison (LCP, *Link Control Protocol*). Les paquets ECP ne peuvent pas être échangés tant que PPP n'a pas atteint la phase de protocole de couche réseau. Les paquets ECP reçus avant que cette phase soit atteinte devraient être éliminés en silence.

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

Modifications de trame
Le paquet peut utiliser toute modification au format de base de trame qui a été négocié durant la phase d'établissement de liaison.

Champ Protocole de couche de liaison des données
Exactement un paquet ECP est encapsulé dans le champ Informations PPP, où le champ Protocole PPP indique le type hexadécimal 8053 (Protocole de contrôle de chiffrement).
Lorsque le chiffrement de données de liaison individuelle est utilisé sur une connexion à liaisons multiples pour une seule destination [RFC1717], le champ Protocole PPP indique le type hexadécimal 8055 (Protocole de contrôle de chiffrement de liaison individuelle).

Champ Code
ECP utilise (en décimal) les codes 1 à 7 (Demande de configuration, Accusé de réception de configuration, Non accusé de réception de configuration, Rejet de configuration, Demande de terminaison, Accusé de réception de terminaison et Rejet de code) et peut aussi utiliser le code 14 (Demande de rétablissement) et le code 15 (Accusé de réception de rétablissement). Les autres codes devraient être traités comme non reconnus et devraient résulter en un rejet de code.

Négociation
Les paquets ECP ne peuvent pas être échangés jusqu'à ce que PPP ait atteint la phase de protocole de couche réseau. Une mise en œuvre devrait être prête à attendre la fin de l'authentification et de la détermination de la qualité de la liaison avant de cesser d'attendre un accusé de réception de configuration ou une autre réponse.
Une mise en œuvre NE DOIT PAS transmettre de données jusqu'à la réussite de la fin de la négociation d'ECP. Si la négociation d'ECP ne réussit pas, la liaison DEVRAIT être close.

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

2.1 Envoi de datagrammes chiffrés

Avant qu'aucun paquet chiffré puisse être communiqué, PPP doit atteindre la phase de protocole de couche réseau, et le protocole de contrôle de chiffrement doit atteindre l'état Ouvert.

Un paquet chiffré est encapsulé dans le champ Information PPP, où le champ Protocole PPP indique le type hexadécimal 0053 (Datagramme chiffré).

Lorsque on utilise des liaisons PPP multiples sur une seule destination [RFC1717], il y a deux méthodes pour employer le chiffrement des données :

- La première méthode est de chiffrer les données avant de les envoyer sur les liaisons multiples. Le champ Protocole PPP DOIT indiquer le type hexadécimal 0053.

- La seconde est de traiter chaque liaison comme une connexion distincte, qui peut avoir ou non le chiffrement activé. Sur les liaisons qui ont négocié le chiffrement, le champ Protocole PPP DOIT avoir le type hexadécimal 0055 (Datagramme chiffré sur liaison individuelle).

On utilise un seul algorithme de chiffrement dans chaque direction à un moment donné, et cela est négocié avant d'envoyer la première trame chiffrée. Le champ Protocole PPP du datagramme chiffré indique que la trame est chiffrée, mais pas

l'algorithme avec lequel il a été chiffré.

La longueur maximale d'un paquet chiffré transmis sur une liaison PPP est la même que la longueur maximale du champ Information d'un paquet encapsulé dans PPP. Si l'algorithme de chiffrement va probablement augmenter la taille du message au delà de celle-ci, la liaison multiple devrait aussi être négociée pour permettre la fragmentation des trames (même si on utilise qu'une seule liaison).

Si l'algorithme de chiffrement porte un historique entre les trames, l'algorithme de chiffrement doit fournir un moyen de déterminer si il passe les données de façon fiable, ou si il doit exiger l'utilisation d'un transport fiable tel que LAPB [RFC1663].

La compression peut aussi être négociée en utilisant le protocole de contrôle de compression [RFC1962]. Pour assurer l'interopérabilité, le texte en clair DOIT être :
- o d'abord compressé,
- o ensuite chiffré.

Cet ordre a été choisi car il devrait résulter en un résultat plus petit et un chiffrement plus sûr.

3. Paquets supplémentaires

Le format du paquet et les facilités de base sont déjà définies pour LCP dans la [RFC1661].

Les mises à jour des valeurs de code ECP sont spécifiées dans la plus récente version de la RFC "numéros alloués" [RFC1700]. La présente spécification concerne les valeurs suivantes :

14 Demande de rétablissement
15 Accusé de réception de rétablissement

3.1 Demande de rétablissement et Accusé de réception de rétablissement

Description
ECP inclut les codes Demande de rétablissement et Accusé de réception de rétablissement afin de donner un mécanisme pour indiquer un échec du déchiffrement dans une direction de la liaison déchiffrée sans affecter le trafic dans l'autre direction. Certains algorithmes de déchiffrement peuvent ne pas exiger ce mécanisme.

Les algorithmes individuels doivent spécifier un mécanisme pour déterminer comment détecter un échec de déchiffrement. À une détection initiale d'un échec de déchiffrement, une mise en œuvre ECP DEVRAIT transmettre un paquet ECP avec le champ Code réglé à 14 (Demande de rétablissement). Le champ Données peut être rempli avec toutes données désirées.

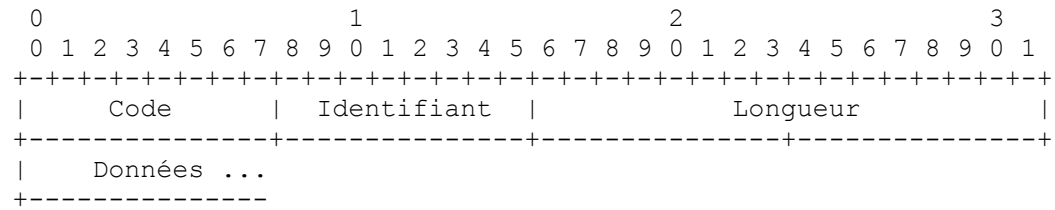
Une fois qu'une Demande de rétablissement a été envoyée, tous les paquets chiffrés reçus sont éliminés. D'autres demandes de rétablissement PEUVENT être envoyées avec le même identifiant, jusqu'à ce qu'un Accusé de réception de rétablissement valide soit reçu.

Lorsque la liaison est occupée, une erreur de déchiffrement est normalement suivie par plusieurs autres avant que l'accusé de réception de rétablissement puisse être reçu. Il n'est pas souhaitable de transmettre des demandes de rétablissement plus fréquemment que le délai d'aller-retour de la liaison, car il en résulterait des demandes de rétablissement redondantes et des accusés de réception de rétablissement qui seraient transmis et traités. Le receveur PEUT choisir de limiter les transmissions de demandes de rétablissement (disons une par seconde) tandis que l'accusé de réception de rétablissement est en cours.

À réception d'une demande de rétablissement, le chiffreur émetteur est rétabli à son état initial. Un paquet ECP DOIT être transmis avec le champ Code réglé à 15 (Accusé de réception de rétablissement) le champ Identifiant copié du paquet Demande de rétablissement, et le camp Données rempli avec toutes données désirées.

À réception d'un Accusé de réception de rétablissement, le déchiffreur receveur est remis à son état initial. Comme il peut y avoir plusieurs accusés de réception de rétablissement en cours, le déchiffreur DOIT être rétabli à chaque Accusé de réception de rétablissement qui correspond à l'identifiant actuellement attendu.

Un résumé des formats de paquet Demande de rétablissement et Accusé de réception de rétablissement est présenté ci-dessous. Les champs sont transmis de gauche à droite.



Code : 14 pour Demande de rétablissement ;
15 pour Accusé de réception de rétablissement.

Identifiant
À l'émission, le champ Identifiant DOIT être changé chaque fois que le contenu du champ Données change, et chaque fois qu'une réponse valide a été reçue pour une demande précédente. Pour les retransmissions, l'identifiant DEVRAIT rester inchangé.
À réception, le champ Identifiant de la demande de rétablissement est copié dans le champ Identifiant du paquet Accusé de réception de rétablissement.

Données
Le champ Données est de zéro, un ou plusieurs octets, et contient des données non interprétées à utiliser par l'envoyeur. Les données peuvent consister en toute valeur binaire et peuvent être de toute longueur de zéro à la MRU établie par l'homologue moins quatre.

4. Options de configuration ECP

Les options de configuration d'ECP permettent la négociation des algorithmes de chiffrement et de leurs paramètres. ECP utilise le même format d'option de configuration que celui défini pour LCP [RFC1661], avec un ensemble d'options distinct.

Les options de configuration, dans ce protocole, indiquent les algorithmes que le receveur accepte ou est capable d'utiliser pour déchiffrer les données envoyées par l'émetteur. Des systèmes peuvent offrir d'accepter plusieurs algorithmes, et en négocier un seul qui sera utilisé.
Des valeurs mises à jour du champ Type de l'option ECP sont spécifiées dans la plus récente RFC "Numéros alloués" [RFC1700]. Les valeurs actuelles sont allouées comme suit :

Option ECP	**Type de compression**
0	OUI
1	DESE

Toutes les mises en œuvre conformes à ECP DEVRAIENT mettre en œuvre l'option ECP 1 – le protocole de chiffrement PPP DES (DESE) [RFC1969].

Les fabricants qui veulent utiliser des chiffrements propriétaires PEUVENT utiliser le mécanisme d'identifiant unique d'organisation (OUI, *Organisationally Unique Identifier*) pour les négocier sans recourir à une demande de numéro d'option alloué par l'autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*). Toutes les autres options de chiffrement sont enregistrées par l'IANA. Au moment de la rédaction du présent mémoire, seul DESE (option 1) est enregistré. D'autres options enregistrées peuvent être trouvées en se référant aux futures versions de la RFC des numéros alloués.

4.1 OUI de chiffrement propriétaire

Description
Cette option de configuration donne un moyen pour négocier l'utilisation d'un protocole de chiffrement propriétaire.

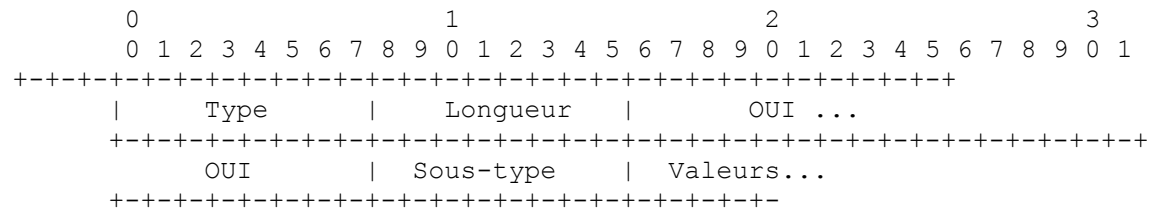
Les protocoles de chiffrement des fabricants se distinguent les uns des autres au moyen d'un identifiant unique d'organisation (OUI), à savoir les trois premiers octets de l'adresse Ethernet du fabricant allouée par la norme IEEE 802.

Comme le premier algorithme de chiffrement qui correspond sera utilisé, il est recommandé que tout OUI d'option de chiffrement soit transmis en premier, avant d'utiliser les options communes.

Avant d'accepter cette option, la mise en œuvre doit vérifier que l'identifiant unique d'organisation (OUI,) identifie un

algorithme propriétaire que la mise en œuvre peut déchiffrer, et que toutes les valeurs de négociation spécifiques du fabricant sont pleinement comprises.

Un résumé du format de l'option de configuration d'OUI de chiffrement propriétaire est présenté ci-dessous. Les champs sont transmis de gauche à droite.



Type : 0

Longueur : ≥ 6

OUI IEEE
Identifiant unique d'organisation IEEE du fabricant , qui sont les trois octets de poids fort d'une adresse physique Ethernet, allouée au fabricant par la norme IEEE 802. Cela identifie l'option comme étant la propriété du fabricant indiqué. Les bits dans l'octet sont en ordre canonique, et l'octet de plus fort poids est transmis en premier.

Sous-type
Ce champ est spécifique de chaque OUI, et indique un type de chiffrement pour cet OUI. Ce champ n'est pas normalisé. Chaque OUI met en œuvre ses propres valeurs.

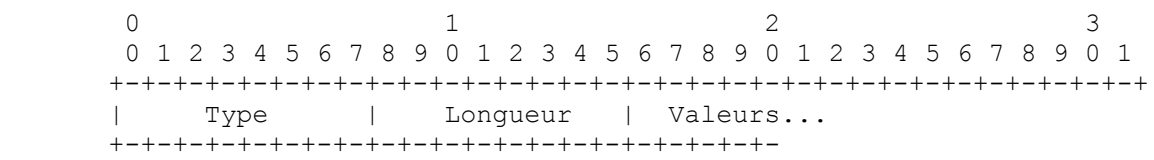
Valeurs
Ce champ fait zéro, un ou plusieurs octets, et contient des données supplémentaires comme déterminé par le protocole de chiffrement du fabricant.

4.2 Types de chiffrement publiquement disponibles

Description
Ces options de configuration donnent un moyen pour négocier l'utilisation d'un algorithme de chiffrement défini publiquement.

Ces protocoles seront rendus disponibles à toutes les parties intéressées, mais peuvent être associés à certaines restrictions d'exportation ou de licence. Pour plus d'informations, se référer aux documents du protocole de chiffrement qui définissent chaque type de chiffrement.

Un résumé du format d'option de configuration du type de chiffrement est présenté ci-dessous. Les champs sont transmis de gauche à droite.



Type : 1 à 254, indique l'option de protocole de chiffrement négociée. DESE [RFC1969] est le type d'option 1. Se référer à la dernière RFC des numéros alloués pour les autres protocoles de chiffrement.

Longueur : ≥ 2

Valeurs
Ce champ fait zéro, un ou plusieurs octets, et contient des données supplémentaires comme déterminé par le protocole de chiffrement.

4.3 Négociation d'un algorithme de chiffrement

ECP utilise les techniques de négociation d'option de LCP pour négocier les algorithmes de chiffrement. À la différence de

la plupart des autres négociations LCP ou NCP d'options multiples, la négociation ECP est supposée converger sur une seule option mutuellement acceptable (algorithme de chiffrement) - ou aucune. Le chiffrement DEVRAIT être négocié dans les deux directions, mais les algorithmes PEUVENT être différents.

Une mise en œuvre qui veut déchiffrer en utilisant un algorithme de chiffrement particulier (ou en utiliser un d'un ensemble d'algorithmes) offre les algorithmes comme options dans une demande de configuration ECP – on appelle cette extrémité le déchiffreur, et on appelle l'homologue le chiffreur.

Un déchiffreur qui prend en charge plus d'un algorithme de chiffrement peut envoyer une demande de configuration contenant soit :
- o une liste ordonnée d'options, avec en premier l'algorithme de chiffrement qui a la plus forte préférence,
- o ou il peut juste offrir son option préférée (qui n'a pas encore été rejeté).

Un chiffreur qui souhaite accepter la première option (parmi plusieurs) PEUT faire un accusé de réception de configuration de TOUTES les options pour indique l'acceptation complète de l'algorithme préféré, cité en premier.

Autrement, si le chiffreur ne reconnaît pas – ou ne veut pas prendre en charge - une option, il DOIT envoyer un Rejet de configuration pour cette option. Lorsque plus d'une option est offerte, le chiffreur DEVRAIT faire un rejet de configuration de toutes les options sauf une seule qui est préférée.

Si le chiffreur fait un rejet de configuration de toutes les options ECP offertes – et si le déchiffreur n'a pas d'autre option (non rejetée) qu'il puisse offrir dans une demande de configuration – le chiffreur DEVRAIT clore la liaison.

Si le chiffreur reconnaît une option, mais si elle n'est pas acceptable à cause des valeurs dans la demande (ou de paramètres facultatifs qui ne sont pas dans la demande) il DOIT envoyer un Non accusé de réception de configuration avec l'option modifiée de façon appropriée. Le Non accusé de réception de configuration DOIT contenir seulement les options qui seront acceptables. Le déchiffreur DEVRAIT envoyer une nouvelle demande de configuration avec seulement l'option préférée, ajustée comme spécifié dans le Non accusé de réception de configuration.

5. Considérations pour la sécurité

La négociation de chiffrement avec PPP est conçue pour assurer la protection contre l'espionnage sur cette liaison. La force de la protection dépend de l'algorithme de chiffrement utilisé et du soin avec lequel est protégé tout 'secret' utilisé par l'algorithme de chiffrement.

On doit reconnaître que la sécurité complète ne peut être obtenue que par la sécurité de bout en bout entre les hôtes.

Références

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

[RFC1663] D. Rand, éditeur, "Transmission fiable en PPP", juillet 1994. *(P.S.)*

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

[RFC1717] K. Sklower et autres, "Protocole PPP multi-liaisons (MP)", novembre 1994. *(P.S.,Obsolète, voir* RFC1990*)*

[RFC1962] D. Rand, "Protocole de contrôle de compression en PPP (CCP)", RFC 1962, juin 1996.

[RFC1969] K. Sklower, G. Meyer, "Protocole de chiffrement en DES sur PPP (DESE)", juin 1996. (*Obsolète, voir* RFC2419) *(Info.)*

Remerciements

Le style et l'approche de ce projet empruntent beaucoup au travail sur le protocole de contrôle de compression [RFC1962].

Adresse du président du groupe de travail

Le groupe de travail peut être contacté via le président actuel :
Karl Fox
Ascend Communications
3518 Riverside Drive, Suite 101
Columbus, Ohio 43221
mél : karl@ascend.com

Adresse de l'auteur

Gerry Meyer
Spider Systems
Stanwell Street
Edinburgh EH6 5NG
Scotland, UK
téléphone : ~ 44 131 554 9424
mél : gerry@spider.co.uk