Groupe de travail Réseau
Request for Comments : 4822
RFC rendue obsolète : 2082
RFC mise à jour : 2453
Catégorie : En cours de normalisation

R. Atkinson, Extreme Networks
M. Fanto NIST
février 2007
Traduction : Claude Brière de L'Isle
août 2007

Authentification cryptographique RIPv2

Statut du présent mémoire
Le présent document spécifie un protocole normalisé de l'Internet pour la communauté de l'Internet et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des normes officielles de protocole de l'Internet (STD 1) pour l'état de la normalisation et le statut de ce protocole. La diffusion du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright
Copyright (C) IETF Trust (2007).

Note de l'IESG
Afin d'encourager la migration rapide de Keyed-MD5 et de ses faiblesses reconnues, l'IESG a approuvé le présent document bien qu'il ne satisfasse pas aux lignes directrices du BCP 107 (RFC4107). Cependant, l'IESG estime fortement que la gestion de clés automatisée devrait être utilisée pour établir les clés de session et insiste pour que les travaux futurs sur la gestion de clés décrits au paragraphe 5.6 du présent document soient effectués aussitôt que possible.

Résumé
La présente note décrit une révision du mécanisme d'authentification cryptographique RIPv2 spécifié à l'origine dans la RFC2082. Le présent document rend obsolète la RFC2082 et met à jour la RFC2453. Le présent document ajoute des précisions sur la façon dont la famille SHA d'algorithmes de hachage peut être utilisée avec l'authentification cryptographique RIPv2, alors que le document d'origine ne spécifie que l'utilisation de Keyed-MD5. Le présent document précise aussi un problème potentiel avec une attaque active contre ce mécanisme et ajoute un texte significatif dans la section sur les considérations de sécurité.

1 Introduction

La croissance de l'Internet nous a rendu conscients de la nécessité d'améliorer l'authentification des informations d'acheminement. RIPv2 *(Routing information protocol v2 : protocole d'informations d'acheminement, version 2)* fournit un service non authentifié (comme dans un RIP classique), ou une authentification par mot de passe. Tous deux sont vulnérables aux attaques passives largement répandues actuellement sur l'Internet. Des problèmes de sécurité bien cernés existent dans les protocoles d'acheminement [Bell89]. Les mots de passe en clair, spécifiés à l'origine pour être utilisés avec RIPv2, sont généralement perçus comme étant vulnérables à des attaques passives faciles à mettre en œuvre [HA94].

La spécification d'origine de l'authentification cryptographique RIPv2, la RFC2082 [AB97], utilisait le mécanisme cryptographique Keyed-MD5. Bien qu'il n'y ait pas d'informations publiées des attaques contre ce mécanisme, certains rapports [Dobb96a, Dobb96b] suscitent des inquiétudes sur la force réelle de la fonction de hachage cryptographique MD5. De plus, certains utilisateurs finaux, en particulier différentes instances gouvernementales, exigent l'utilisation de la famille des fonctions de hachage SHA de préférence à toute autre fonction de cette sorte pour des raisons politiques. Finalement, la spécification d'origine utilise une construction de hachage dont il est généralement estimé qu'elle est plus faible que la construction HMAC utilisée avec les algorithmes ajoutés dans la présente révision de cette spécification.

Le présent document rend obsolète la spécification d'origine, RFC2082 [AB97]. La présente spécification diffère de la RFC2082 par l'ajout de la prise en charge de la famille SHA d'algorithmes de hachage et de la technique du HMAC, tout en conservant l'algorithme et le mode Keyed-MD5 d'origine. Comme le mécanisme d'authentification cryptographique RIPv2 d'origine était indépendant de l'algorithme, la compatibilité vers l'amont est conservée. Cette exigence de compatibilité vers l'amont empêche de faire des changements de protocole significatifs. Aussi, le présent

document limite les changements à l'ajout de la prise en charge d'une famille supplémentaire d'algorithmes de chiffrement. La spécification d'origine a été très largement mise en œuvre, elle est reconnue pour être bien interopérable, et est aussi très largement répandus.

Les auteurs NE CROIENT PAS que la présente spécification est la réponse ultime à l'authentification RIPv2 et encouragent le lecteur à consulter la section des Considérations sur la sécurité de ce document pour des précisions.

Si l'authentification RIPv2 est désactivée, seules de simples mauvaises configurations sont détectées. Le mécanisme d'authentification RIPv2 d'origine s'appuyait sur des mots de passe en clair réutilisés. L'utilisation de l'authentification par des mots de passe en clair peut protéger contre des mauvaises conformations accidentelles, si elles seules étaient en cause, mais elle n'est d'aucune aide dans une perspective de sécurité. Par la simple capture des informations dans le réseau – directement même à distance – une entité peut lire le mot de passe RIPv2 en clair et utiliser sa connaissance pour injecter de fausses informations dans le système d'acheminement via le protocole d'acheminement RIPv2.

Ce mécanisme est destiné à réduire le risque de réussite d'une attaque passive sur les développements de RIPv2. C'est-à-dire que le développement de ce mécanisme réduit considérablement la vulnérabilité des systèmes d'acheminement fondés sur RIPv2 à une attaque passive. Lorsque l'authentification cryptographique est activée, on transmet le résultat d'une fonction univoque de chiffrement dans le champ d'authentification du paquet RIPv2, au lieu d'envoyer un mot de passe réutilisable en clair dans le paquet RIPv2. La clé d'authentification RIPv2 n'est connue que des parties autorisées de la session RIPv2. La clé d'authentification RIPv2 n'est jamais envoyée en clair sur le réseau.

De cette façon, la protection est assurée contre la falsification ou la modification du message. Alors qu'il est possible de répéter un message jusqu'à ce que le numéro de séquence change, un numéro de séquence peut être utilisé pour réduire les risques de répétition. Le mécanisme ne garantit pas la confidentialité, car les messages restent en clair. Dans la mesure où l'objectif d'un protocole d'acheminement est de faire connaître la topologie de l'acheminement, la confidentialité n'est pas normalement exigée des protocoles d'acheminement.

Les autres raisons pertinentes pour cette approche sont que MD5 et SHA-1 sont tous deux utilisés à d'autres fins et sont donc généralement présents dans les routeurs IP, ainsi que dans certaines formes de gestion de mots de passe.

1.1 Terminologie

Dans le présent document, les mots "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "DECONSEILLE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le [BCP14] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

2 Approche de la mise en œuvre

La mise en œuvre exige l'utilisation d'un format de paquet spécial, de procédures d'authentification particulières, et aussi de contrôles de gestion. Ceux qui mettent en œuvre doivent se souvenir que la section des Considérations sur la sécurité fait partie intégrante de la présente spécification dont elle contient une partie importante.

2.1 Format de PDU RIPv2

Le format de message RIPv2 de base fournit un en-tête de 8 octets avec un registre de vingt octets pour le contenu des données. Lorsque l'authentification cryptographique RIPv2 est activée, on utilise le même en-tête et le même contenu que dans la spécification RIPv2 d'origine, mais le champ de mot de passe "Authentification" de 16 octets de la spécification RIPv2 d'origine est réutilisé afin de contenir une transformée des données d'authentification, un identifiant de clé, la longueur des données d'authentification, et un numéro de séquence non décroissant.

TYPE D'AUTHENTIFICATION
Le "Type d'authentification" est la fonction de hachage cryptographique, qui est indiquée par la valeur 3.

LONGUEUR DE PAQUET RIPv2
Un paquet de 16 bits non signés depuis le début de l'en-tête RIPv2 jusqu'à la fin du paquet RIPv2 normal (non inclus l'en-queue d'authentification).

IDENTIFIANT DE CLÉ
Un champ de 8 bits non signés qui contient l'identifiant de clé ou Key-ID. Cela, combiné avec l'interface réseau, identifie l'association de sécurité RIPv2 utilisée pour ce paquet. L'association de sécurité RIPv2, qui est définie au paragraphe 2.2 ci-dessous, inclut la clé d'authentification qui a été utilisée pour créer les données d'authentification pour ce message RIPv2 et d'autres paramètres. Dans les mises en œuvre qui prennent en charge plus d'un algorithme d'authentification, l'association de sécurité RIPv2 inclut aussi des informations sur l'algorithme d'authentification qui est utilisé pour ce message. Une association de sécurité RIPv2 est toujours associée à une interface, plutôt qu'à un routeur. La clé de chiffrement réelle fait partie de l'association de sécurité RIPv2.

LONGUEUR DES DONNÉES D'AUTHENTIFICATION
Un champ de 8 bits non signés qui contient la longueur en octets du champ d'en-queue des données d'authentification. La présence de ce champ aide à fournir l'indépendance à l'égard de l'algorithme de chiffrement.

DONNÉES D'AUTHENTIFICATION
Ce champ contient les données d'authentification cryptographiques utilisées pour valider ce paquet. La longueur de ce champ est mémorisée dans le champ LONGUEUR DES DONNÉES D'AUTHENTIFICATION ci-dessus.

NUMÉRO DE SÉQUENCE
Un numéro de séquence de 32 bits non signés. Le numéro de séquence DOIT être non décroissant pour tous les messages envoyés à partir d'un routeur de source donné avec une valeur d'identifiant de clé donnée.

L'en-queue d'authentification contient les données d'authentification, qui sont le résultat de la fonction de hachage cryptographique frappé. Voir les paragraphes suivants de cette section pour les détails du calcul de ce champ.

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Commande (1)	Version (1)	Domaine d'acheminement (2)	
0xFFFF		Type d'authentification =0x0003	
Longueur de paquet RIPv2		ID de clé	Longueur des données d'auth.
Numéro de séquence (non décroissant)			
réservé, doit être zéro			
réservé, doit être zéro			
(Longueur de paquet RIPv2 - 24) octets de données			
0xFFFF		0x0001	
Données d'authentification (longueur variable ; 20 octets avec HMAC-SHA1)			

2.2 Association de sécurité RIPv2

La compréhension du concept d'association de sécurité RIPv2 est cruciale pour l'assimilation de la présente spécification. Une association de sécurité RIPv2 contient l'ensemble des paramètres de configuration d'authentification partagée nécessaire pour l'expéditeur légitime ou tout receveur légitime.

Une mise en œuvre DOIT être capable de prendre en charge au moins deux associations de sécurité RIPv2 concurrentes sur chaque interface RIP. Ceci est une exigence fonctionnelle pour la prise en charge du renouvellement des clés. La prise en charge du renouvellement des clés est obligatoire.

L'association de sécurité RIPv2, définie ci-dessous, est choisie par l'envoyeur sur la base de l'interface de routeur sortant. Chaque association de sécurité RIPv2 a une durée de vie et d'autres paramètres de configuration qui lui sont associés. En fonctionnement normal, une association de sécurité RIPv2 n'est jamais utilisée après l'expiration de sa durée de vie. Certains cas particuliers sont exposés plus loin dans le présent document.

Les éléments de données minimum dans une association de sécurité RIPv2 sont les suivants :

IDENTIFIANT DE CLÉ (KEY-ID)
La valeur de KEY-ID de 8 bits non signés sert à identifier l'association de sécurité RIPv2 utilisée pour ce paquet.

Le receveur utilise la combinaison de l'interface sur laquelle le paquet a été reçu et de la valeur de KEY-ID pour identifier de façon univoque l'association de sécurité appropriée.

L'expéditeur choisit quelle association de sécurité RIPv2 utiliser sur la base de l'interface de sortie pour ce paquet RIPv2 et place ensuite la valeur de KEY-ID correcte dans ce paquet. Si plusieurs associations de sécurité RIPv2 valides et actives existent pour une interface de sortie au moment de l'envoi d'un paquet RIPv2, l'envoyeur peut utiliser n'importe laquelle de ces associations de sécurité pour protéger le paquet.

ALGORITHME D'AUTHENTIFICATION
Il spécifie l'algorithme cryptographique et le mode d'algorithme utilisés avec l'association de sécurité RIPv2. Ces informations ne sont jamais envoyées en clair sur le réseau. Comme ces informations ne sont pas envoyées sur le réseau, la mise en œuvre choisit une représentation spécifique pour ces informations. Actuellement, les valeurs suivantes sont possibles : KEYED-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, et HMAC-SHA-512.

CLÉ D'AUTHENTIFICATION
C'est la valeur de la clé d'authentification cryptographique utilisée avec l'algorithme d'authentification associé. Il NE DOIT PAS être envoyé sur le réseau en clair, via aucun protocole. La longueur de cette clé va dépendre de l'algorithme d'authentification utilisé. Les opérateurs devraient veiller à choisir des clés fortes et imprévisibles, en évitant toute clé faible pour l'algorithme utilisé. [ESC05] contient des informations utiles sur les techniques de génération de clés et sur la cryptographie aléatoire.

NUMÉRO DE SÉQUENCE
C'est un nombre de 32 bits non signés. Pour une valeur de KEY-ID et d'expéditeur donnée, ce nombre NE DOIT PAS diminuer. En fonctionnement normal, l'opérateur devrait relancer la session RIPv2 avant d'atteindre la valeur maximale. La valeur initiale utilisée dans le numéro de séquence est arbitraire. Les receveurs DEVRAIENT garder trace du numéro de séquence le plus récent reçu d'un expéditeur donné.

HEURE DE DÉPART
C'est une représentation locale de la date et de l'heure à laquelle cette association de sécurité commence à être valide.

HEURE D'ARRÊT
C'est une représentation locale de la date et de l'heure à laquelle cette association de sécurité devient invalide (c'est-à-dire, quand elle arrive à expiration). Il est permis, mais pas recommandé, qu'un opérateur configure cela à "n'expire jamais". La valeur "n'expire jamais" n'est pas une pratique de fonctionnement recommandée parce qu'elle réduit la sécurité par rapport à des réinitialisations périodiques. Normalement, une association de sécurité RIPv2 est supprimée à son HEURE D'ARRÊT. Cependant, il y a certains cas critiques, qui sont exposés au paragraphe 5.1.

L'en-queue d'authentification consiste en données d'authentification, qui sont le résultat de la fonction de hachage cryptographique retenue. Voir les paragraphes suivants de cette section pour des précisions sur le calcul de ce champ.

2.3 Traitement de l'authentification de base

Lorsque le type d'authentification est "Fonction de hachage cryptographique", le traitement du message est changé en une création et réception de message par rapport à la spécification RIPv2 d'origine dans [Mal94].

La présente section décrit le traitement de message de façon générique. Un traitement supplémentaire dépendant de l'algorithme qui est nécessaire est décrit séparément, dans les paragraphes suivants du présent document. Au moment de la rédaction, il y a deux sortes de traitements dépendants de l'algorithme. L'un couvre l'algorithme "Keyed-MD5". L'autre couvre la famille d'algorithmes "HMAC-SHA1".

2.3.1 Génération du message

Le paquet RIPv2 est créé comme d'habitude, avec les exceptions suivantes :

(1) La somme de contrôle UDP DEVRAIT être calculée, mais PEUT être réglée à zéro parce que tous les mécanismes d'authentification cryptographique de la présente spécification fourniront une protection d'intégrité plus forte que la somme de contrôle UDP standard.
(2) Le champ Type d'authentification indique Authentification cryptographique (3).

(3) Le champ d'authentification "mot de passe" est réutilisé pour mémoriser une réplique du paquet avec les données d'authentification, un identifiant de clé, la longueur des données d'authentification, et un numéro de séquence non décroissant.

Voir aussi au paragraphe 2.2 ci-dessus sur l'association de sécurité RIPv2 pour les autres informations de base importantes.

Lors de la création du paquet RIPv2, on doit suivre le processus suivant :

(1) Le champ Longueur de paquet de l'en-tête RIPv2 indique la taille du corps principal du paquet RIPv2.
(2) Une association de sécurité RIPv2 appropriée est choisie pour être utilisée avec ce paquet, sur la base de l'interface de sortie pour le paquet.
Toute association de sécurité RIPv2 valide pour cette interface de sortie peut être utilisée. Les champs Décalage des données d'authentification, Identifiant de clé, et Longueur des données d'authentification, sont remplis en conséquence.
(3) Le traitement dépendant de l'algorithme intervient alors, soit pour l'algorithme "Keyed-MD5" soit pour la famille d'algorithmes "HMAC-SHA1". Voir aux paragraphes respectifs (ci-dessous) les précisions sur ce traitement dépendant de l'algorithme.
(4) La valeur des données d'authentification résultante est écrite dans le champ Données d'authentification. Le bourrage d'en-queue (s'il en est) n'est pas réellement transmis, car il est entièrement prévisible d'après la longueur du message et l'algorithme d'authentification utilisé.

2.3.2 Réception du message

Lorsque le message est reçu, le processus est inversé :
(1) Les données d'authentification reçues sont mises de côté et mémorisées pour utilisation ultérieure.
(2) L'association de sécurité RIPv2 appropriée est déterminée à partir de la valeur du champ Identifiant de clé et de l'interface sur laquelle le paquet a été reçu. Si il n'y a pas d'association de sécurité RIPv2 valide pour l'identifiant de clé reçu sur l'interface sur laquelle le paquet a été reçu, alors :
(a) tout le traitement du paquet entrant cesse, et
(b) un événement de sécurité DEVRAIT être enregistré par le sous-système RIPv2 du système récepteur. Cet événement de sécurité DEVRAIT indiquer au moins la date/heure à laquelle le mauvais paquet a été reçu, l'adresse IP de source du paquet RIPv2 reçu, la valeur du champ Key-ID, l'interface sur laquelle le mauvais paquet est arrivé, et le fait qu'aucune association de sécurité RIPv2 valide n'a été trouvée pour cette combinaison d'interface et de Key-ID.
(3) Le traitement dépendant de l'algorithme est effectué, en utilisant l'algorithme spécifié par l'association de sécurité RIPv2 appropriée pour ce paquet. Il en résulte un calcul des données d'authentification sur la base des informations du paquet RIPv2 reçu et des informations provenant de l'association de sécurité RIPv2 appropriée pour ce paquet.
(4) Le résultat des données d'authentification calculé est comparé aux données d'authentification reçues.
(5) Si les données d'authentification calculées ne correspondent pas au champ Données d'authentification reçu, alors :
(a) le message DOIT être éliminé sans être traité, et
(b) un événement de sécurité DEVRAIT être enregistré par le sous-système RIPv2 du système récepteur. Cet événement de sécurité DEVRAIT indiquer au moins la date/heure à laquelle le mauvais paquet a été reçu, l'adresse IP de source du paquet RIPv2 reçu, la valeur du champ Key-ID, l'interface sur laquelle le mauvais paquet est arrivé, et le fait que l'authentification RIPv2 a échoué à la réception du paquet.
(6) Si le voisin a été entendu depuis assez peu de temps pour avoir des routes viables dans le tableau d'acheminement local, et si le numéro de séquence reçu est inférieur au dernier numéro de séquence reçu, le message DOIT alors être éliminé sans traitement. Si le numéro de séquence reçu est inférieur au dernier numéro de séquence reçu, le fait DEVRAIT être enregistré comme événement de sécurité. Cet enregistrement d'événement de sécurité DEVRAIT indiquer au moins la date/heure de réception du mauvais paquet, l'adresse IP de source du paquet RIPv2 reçu, et la valeur du champ Key-ID, et le fait qu'un numéro de séquence RIPv2 hors de son ordre ait été reçu.
Lorsque la connexité avec le voisin a été perdue, le receveur DEVRAIT être prêt à accepter soit :
- un message avec un numéro de séquence de zéro.
- un message avec un numéro de séquence supérieur à celui du dernier numéro de séquence reçu.
(7) Les messages acceptables sont maintenant réduits au message RIPv2 lui-même, moins l'en-queue d'authentification, et sont traités normalement (c'est-à-dire, conformément à la spécification RIPv2 de base de la RFC2453 [Mal98]). Le dernier numéro de séquence reçu pour cette association de sécurité RIPv2 et l'expéditeur

est aussi mis à jour.

Note : Un routeur qui a oublié son numéro de séquence courant mais se souvient de son association de sécurité DOIT envoyer son premier paquet avec un numéro de séquence de zéro. Cela laisse une petite ouverture à une attaque en répétition. Pour réduire le risque de telles attaques en empêchant la situation où un routeur a oublié son numéro de séquence en cours, les développeurs DEVRAIENT fournir des mémoires non-volatiles pour tous les composants d'une association de sécurité RIPv2, et les systèmes récepteurs DEVRAIENT fournir des mémoires non-volatiles pour le dernier numéro de séquence reçu de chaque expéditeur. Voir aussi la section sur les considérations sur la sécurité du présent document.

2.4 Traitement Keyed-MD5 dépendant de l'algorithme

Ce paragraphe décrit les étapes du processus dépendant de l'algorithme applicables lorsque l'algorithme d'authentification "Keyed-MD5" est utilisé. La clé d'authentification RIPv2 est toujours de 16 octets lorsque "Keyed-MD5" est utilisé.

(1) La clé d'authentification RIPv2 est ajoutée au paquet RIPv2 en mémoire.

(2) Le bourrage d'en-queue pour MD5 et les champs de longueur de message sont ajoutés en mémoire. Le diagramme ci-dessous montre comment ces ajouts apparaissent lors de la mise en mémoire :

Clé d'authentification
/ (16 octets de long) /
zéro, un ou plusieurs octets de bourrage (comme défini par la RFC1321)
MSW de longueur de message de 64 bits
LSW de longueur de message de 64 bits

(3) Les données d'authentification sont alors calculées conformément à l'algorithme MD5 défini par la RFC1321 [Rivest92].

2.5 Traitement HMAC-SHA1 dépendant de l'algorithme

Ce paragraphe décrit les étapes du traitement pour l'authentification HMAC. Alors que HMAC était documenté à l'origine dans [KMC97], pour la présente spécification, on utilise la terminologie de [FIPS-198]. Bien que la présente spécification ne donne tous les détails que pour l'authentification HMAC qui utilise l'algorithme SHA-1 de l'Institut américain des normes et technologies (NIST) SHA-1 (et ses dérivés directs) le même processus de base pourrait être utilisé avec d'autres fonctions de hachage cryptographiques à l'avenir. Comme le paquet RIPv2 n'est haché qu'une seule fois, la redondance du double hachage dans ce processus est négligeable.

La norme de hachage sécurisé du NIST des États Unis (SHS, *Secure Hash Standard*), définie par [FIPS-180-2], inclut les spécifications pour SHA-1, SHA-256, SHA-384, et SHA-512. La présente spécification définit le traitement pour chacun de ces algorithmes.

Le résultat des calculs de chiffrement (par exemple, HMAC-SHA1) N'EST PAS tronqué pour l'authentification cryptographique RIPv2.

La longueur des données d'authentification est égale à la taille de résumé de message pour l'algorithme de hachage utilisé.

Toute valeur de clé connue pour être faible avec un algorithme défini par la norme de hachage sécurisé du NIST NE DOIT PAS être utilisée avec un tel algorithme dans une mise en oeuvre de la présente spécification. US NIST est l'autorité de source pour la publication d'informations sur les clés faibles pour ces algorithmes.

Dans la description d'algorithme ci-dessous, on utilise la nomenclature suivante, qui est cohérente avec [FIPS-198] :

H est l'algorithme de hachage spécifique, par exemple, SHA-1 ou SHA-256.
Ko est la clé cryptographique utilisée avec l'algorithme de hachage.
B est la taille de bloc de H, mesurée en octets, pas en bits.

Noter que B est la taille de bloc interne, pas la taille du hachage.
Pour SHA-1 et SHA-256 : B == 64.
Pour SHA-384 et SHA-512 : B == 128
L est la longueur du hachage, mesurée en octets, pas en bits.
Par exemple, avec SHA-1, L == 20.
XOR est l'opération OU exclusif.
Opad est la valeur hexadécimale 0x5c répétée B fois.
Ipad est la valeur hexadécimale 0x36 répétée B fois.
Apad est la valeur hexadécimale 0x878FE1F3 répétée (L/4) fois.

(1) PRÉPARATION DE CLÉ
Dans cette application, Ko est toujours long de L octets.

Si la clé d'authentification est longue de L octets, Ko est alors réglé égal à la clé d'authentification. Si la clé d'authentification est plus longue que L octets, Ko est réglé à H(Clé d'authentification). Si la clé d'authentification est plus courte que L octets, Ko est alors réglé à la clé d'authentification avec des zéros ajoutés à la fin de la clé d'authentification de sorte que Ko ait la longueur L octets.

(2) PREMIER HACHAGE
D'abord, le champ Données d'authentification du paquet RIPv2 est rempli avec la valeur Apad.

Puis un premier hachage, aussi appelé hachage interne, est calculé comme suit :
Premier hachage = H(Ko XOR Ipad || (paquet RIPv2))

(3) SECOND HACHAGE
Puis un second hachage, aussi appelé hachage externe, est calculé comme suit :
Second hachage = H(Ko XOR Opad || premier hachage)

(4) RÉSULTAT
Le résultat du second hachage devient les données d'authentification qui sont envoyées dans le champ Données d'authentification du paquet RIPv2. La longueur du champ Données d'authentification est toujours identique à la taille du résumé de message de la fonction de hachage H qui est utilisée.

Cela implique aussi que l'utilisation des fonctions de hachage avec de grandes tailles de sortie va aussi augmenter la taille du paquet qui sera transmis sur le réseau.

3 Procédures de gestion

La gestion des clés est une composante importante de ce mécanisme et une mise en œuvre appropriée est vitale pour fournir le niveau désiré de réduction des risques.

3.1 Exigences pour la gestion des clés

Il est très souhaitable qu'une violation hypothétique de la sécurité dans un des protocoles de l'Internet ne compromette pas automatiquement les autres protocoles de l'Internet. La clé d'authentification de la présente spécification NE DEVRAIT PAS être configurée ou mémorisée en utilisant des protocoles (par exemple, RADIUS) ou des algorithmes de chiffrement qui ont des faiblesses connues.

Les mises en œuvre DOIVENT prendre en charge la mémorisation de plus d'une clé en même temps, bien qu'il soit reconnu qu'une seule clé sera normalement active sur une interface. Les mises en œuvre DOIVENT associer une durée de vie d'association de sécurité spécifique (c'est-à-dire, la date et heure de début de validité et la date et heure de fin de validité) et un identifiant de clé à chaque clé. Les mises en œuvre DOIVENT aussi prendre en charge la distribution manuelle des clés. Un exemple de distribution manuelle de clés est d'avoir l'utilisateur privilégié qui frappe la clé, la durée de vie de la clé, et l'identifiant de clé sur la console du routeur. Un opérateur peut configurer la durée de vie de l'association de sécurité à infini, ce qui signifie que la session n'est jamais réinitialisée. Cependant, il est fortement recommandé à la place que les opérateurs réinitialisent régulièrement, en utilisant une durée de vie d'association de sécurité modérément courte (par exemple, 24 heures).

La présente spécification exige la prise en charge d'au moins deux algorithmes d'authentification, et donc la mise en œuvre DOIT exiger que l'algorithme d'authentification soit spécifié pour chaque clé lorsque les autres informations de clé sont entrées. La suppression manuelle des associations de sécurité actives DOIT être prise en charge.

Il est vraisemblable que l'IETF définira une norme de protocole de gestion de clé à utiliser avec les protocoles d'acheminement. Il est très souhaitable d'utiliser un protocole de gestion de clés normalisé par l'IETF pour distribuer les clés d'authentification RIPv2 parmi les mises en œuvre RIPv2 communicantes. Un tel protocole fournirait un moyen de mesure et réduirait de façon significative la charge administrative humaine. Le champ Key-ID peut être utilisé comme liaison entre RIPv2 et un tel protocole à l'avenir.

Les protocoles de gestion de clé ont une longue histoire de fautes subtiles qui sont souvent découvertes longtemps après que le protocole ait été livré pour la première fois au public. Pour éviter d'avoir à changer toutes les mises en œuvre de RIPv2 en cas de découverte d'une telle faute, les techniques de protocoles de gestion de clé intégrés ont été délibérément omises de la présente spécification.

3.2 Procédures de gestion des clés

Comme avec toutes les méthodes de sécurité qui utilisent des clés, il est nécessaire de changer de façon régulière la clé d'authentification RIPv2. Pour conserver la stabilité de l'acheminement pendant de tels changements, les mises en œuvre DOIVENT être capables de mémoriser et d'utiliser plus d'une clé d'authentification RIPv2 sur une interface donnée en même temps.

Chaque clé devra avoir son propre identifiant de clé (KEY-ID), qui sera mémorisé localement. La combinaison de l'identifiant de clé et de l'interface associée au message identifie de façon univoque l'algorithme d'authentification et la clé d'authentification RIPv2 utilisés.

Comme noté ci-dessus au paragraphe 2.3.1, le créateur du message RIPv2 va choisir une association de sécurité RIPv2 valide à partir des associations de sécurité RIPv2 valides pour cette interface. le receveur DOIT utiliser l'identifiant de clé et l'interface de réception pour déterminer quelle association de sécurité RIPv2 utiliser pour l'authentification du message reçu. Plus d'une association de sécurité RIPv2 PEUT être associée au même moment à une interface. Le receveur NE DOIT PAS simplement essayer toutes les associations de sécurité RIPv2 (c'est-à-dire, les clés) qui pourraient être configurées pour RIPv2 sur l'interface de réception, car cela créerait une attaque de déni de service facilement exploitable sur le sous-système RIP du receveur. (Au moins une mise en œuvre largement utilisée de la version précédente de la présente spécification viole ces exigences à la date de publication de ce document et a des faiblesses de sécurité conséquentes.)

Et donc, il est possible d'avoir une rotation en douceur des associations de sécurité RIPv2 (c'est-à-dire, des clés) sans perdre de messages RIPv2 légitimes du fait d'une clé partagée invalide et sans exiger des gens qu'ils changent toutes les clés d'un coup. Pour garantir une rotation en douceur, chaque système de communication RIPv2 doit être mis à jour avec la nouvelle association de sécurité RIPv2 (y compris la nouvelle clé) plusieurs minutes avant l'arrivée à expiration de l'association de sécurité RIPv2 en cours et plusieurs minutes avant que ne débute la durée de vie de la nouvelle association de sécurité RIPv2. Ainsi, la nouvelle association de sécurité RIPv2 devrait avoir une durée de vie qui débute plusieurs minutes avant l'expiration de la vieille association de sécurité RIPv2. Cela donne le temps à chaque système de prendre connaissance de la nouvelle association de sécurité avant qu'elle ne soit utilisée. Cela garantit aussi que la nouvelle association de sécurité commencera son utilisation, et que l'association de sécurité actuelle cessera son utilisation, avant l'arrivée à expiration de la durée de vie de l'association de sécurité actuelle. Pour la durée du chevauchement des durées de vie des associations de sécurité, un système peut recevoir des messages correspondants à l'une ou l'autre association de sécurité et réussir à authentifier le message. Le Key-ID dans le message reçu sert à choisir l'association de sécurité appropriée (c'est-à-dire, la clé) à utiliser pour l'authentification.

4 Exigences de conformité

Pour la présente spécification, le terme "conformité" a une signification identique à celle "conformité entière".

Les algorithmes d'authentification Keyed-MD5 et HMAC-SHA1 DOIVENT être mis en œuvre par toutes les mises en oeuvre qui revendiquent la conformité. De plus, les algorithmes HMAC-SHA-256, HMAC-SHA-384, et HMAC-SHA-

512 DEVRAIENT être mis en œuvre. MD5 est défini dans [Rivest92]. SHA-1, SHA-256, SHA-384, et SHA-512 ont été définis par le NIST US dans [FIPS-180-2].

Une mise en œuvre conforme PEUT aussi prendre en charge des algorithmes d'authentification supplémentaires, pourvu que ceux-ci soient spécifiés publiquement et de façon ouverte.

La distribution manuelle des clés telle que décrite ci-dessus DOIT être prise en charge par toutes les mises en œuvre conformes. Toutes les mises en œuvre DOIVENT prendre en charge le remplacement en douceur des clés décrit au paragraphe "Procédures de gestion des clés". Cela signifie aussi que les mises en œuvre DOIVENT prendre en charge au moins deux associations de sécurité RIPv2 concurrentes.

La documentation d'usager fournie avec la mise en œuvre devrait contenir des instructions claires sur la façon de configurer la mise en œuvre de telle sorte que le remplacement en douceur des clés se fasse avec succès.

Les mises en œuvre DEVRAIENT prendre en charge un protocole de gestion de clés standard pour la distribution sécurisée des clés d'authentification RIPv2 une fois qu'un tel protocole de gestion des clés sera normalisé par l'IETF.

La section Considérations sur la sécurité du présent document fait partie intégrante de la spécification, et n'est pas une simple discussion sur le protocole.

5 Considérations sur la sécurité

La totalité du présent mémoire décrit et spécifie un mécanisme d'authentification pour le protocole d'acheminement RIPv2 dont on estime qu'il est sécurisé contre les attaques passives. Le terme "attaque passive" est défini dans la RFC1704 [HA94]. L'analyse contenue dans la RFC1704 motivait ce terme. Les attaques passives sont très répandues à présent sur l'Internet [HA94].

La protection contre les attaques actives n'est pas complète dans la présente spécification. La principale question relative aux attaques actives réside dans le besoin de traiter la cas où un autre routeur s'est récemment réinitialisé et où ce routeur ne dispose pas de la mémoire non volatile nécessaire pour se souvenir de la ou des associations de sécurité RIPv2 et du ou des derniers numéros de séquence RIPv2 reçus à travers cette réinitialisation.

5.1 Cas pathologiques connus

Il existe deux cas pathologiques connus qui DOIVENT être traités par les mises en œuvre. Tous deux sont des défaillances du gestionnaire de réseau. Chacune d'elles devrait être excessivement rare en fonctionnement normal.

(1) Durant le remplacement de clés, il peut exister des appareils qui n'ont pas réussi à se configurer avec la nouvelle clé. Donc les routeurs DEVRAIENT mettre en œuvre un algorithme qui détecte les ensembles d'associations de sécurité RIPv2 qui sont en cours d'utilisation par ses voisins, et qui transmette ses messages en utilisant à la fois l'ancienne et la nouvelle association de sécurité RIPv2 (c'est-à-dire, les clés) jusqu'à ce que tous les voisins utilisent la nouvelle association de sécurité ou que la durée de vie de la vieille association de sécurité arrive à expiration. Dans les circonstances normales, ce débit de transmission élevé n'existera que pour un seul intervalle de mise à jour RIP.

(2) Au cas où arriverait à expiration la dernière association de sécurité RIPv2 d'un interface, il serait inacceptable de revenir à une condition de non authentification, et non conseillé d'interrompre l'acheminement. Donc, le routeur DOIT envoyer une notification "expiration de dernière association de sécurité RIPv2" au gestionnaire de réseau (par exemple, via SYSLOG, SNMP, et/ou d'autres moyens) et DEVRAIT traiter cette dernière association de sécurité comme ayant une durée de vie infinie jusqu'à ce que la durée de vie soit étendue, que l'association de sécurité soit supprimée par la gestion de réseau, ou qu'une nouvelle association de sécurité soit configurée.

Dans certaines circonstances, la pratique décrite en (2) peut laisser une ouverture à une attaque active sur le sous-système d'acheminement RIPv2. Donc, toute occurrence réelle d'une expiration d'association de sécurité RIPv2 DOIT causer un événement de sécurité à enregistrer par la mise en oeuvre. Cet élément d'enregistrement DOIT inclure au moins la note de l'expiration de la clé d'authentification RIPv2, la ou les instances de protocole d'acheminement RIP affectées, les interfaces d'acheminement affectées, le Key-ID affecté, et la date et l'heure. Les opérateurs sont invités à vérifier de tels enregistrements au titre des pratiques de sécurité opérationnelle pour aider à détecter les attaques actives

sur le sous-système d'acheminement RIPv2. De plus, les mises en œuvre DEVRAIENT fournir un choix de configuration ("à défaillance sécurisée") pour permettre à un opérateur de réseau de préférer avoir un échec d'acheminement RIPv2 lorsque la dernière clé expire, plutôt que de continuer à utiliser RIPv2 d'une façon non sécurisée.

5.2 Considérations sur la gestion de réseau

L'utilisation de SNMP, et même SNMPv3 avec l'authentification cryptographique et la confidentialité cryptographique activée, pour modifier ou configurer les associations de sécurité RIPv2, ou tout composant de l'association de sécurité (par exemple, la clé de chiffrement) N'EST PAS RECOMMANDÉE. Cette pratique créerait une cascade de faiblesses potentielle, par laquelle la compromission de la mise en œuvre de la sécurité SNMP conduirait inévitablement à la compromission non seulement du tableau d'acheminement local (auquel on peut accéder via SNMP) mais aussi de tous les autres routeurs qui reçoivent des paquets RIPv2 (directement ou indirectement) à partir du routeur compromis.

De même, l'utilisation de protocoles qui ne sont pas conçus et évalués pour l'utilisation en matière de gestion de clés (par exemple, RADIUS, Diameter) pour configurer l'association de sécurité est aussi NON RECOMMANDÉE. Lire les associations de sécurité via SNMP est permis, mais les informations sont à traiter comme sensibles à la sécurité et à protéger en utilisant le mode privé.

Également, l'utilisation de SNMP pour configurer quelle forme d'authentification RIPv2 est utilisée N'EST PAS RECOMMANDÉE à cause d'un problème similaire de défaillances en cascade. Toute révision à venir de la base d'informations de gestion (MIB, *Management Information Base*) [MB94] RIPv2 devrait envisager de rendre l'objet rip2IfConfAuthType en lecture seule. De plus, cet objet aurait besoin d'une nouvelle valeur enum pour s'accommoder du type d'authentification cryptographique RIPv2. Et encore, la déclaration de conformité pour cette MIB n'a pas de MIN-ACCESS pour cet objet. Au minimum, si la MIB est mise à jour, une nouvelle déclaration de conformité DEVRAIT être rédigée pour cet objet, qui lui permette d'être mis en œuvre en lecture seule. Pour l'objet rip2ifConfAuthKey, dans la mesure où il retourne toujours "H" en lecture, le MIN-ACCESS de l'objet dans toute déclaration de conformité révisée DEVRAIT être non accessible si le MIB est mis à jour.

De plus, pour des raisons similaires, toutes les révisions à venir de la base d'informations de gestion RIPv2 DEVRAIENT déconseiller ou omettre tous les objets qui permettraient l'écriture de toute association de sécurité RIPv2 ou de composant d'association de sécurité RIPv2 (par exemple, la clé de chiffrement).

Il est aussi RECOMMANDÉ que toute révision à venir de la base d'informations de gestion RIPv2 prenne en considération l'ajout des objets MIB pour détenir les informations sur tout événement de sécurité RIPv2 qui pourrait survenir, et des objets de MIB qui pourraient être utilisés pour lire l'ensemble des événements de sécurité qui ont été enregistrés par le sous-système RIPv2. Pour chaque événement de sécurité mentionné dans le présent document, il est aussi RECOMMANDÉ que les notifications appropriées soient incluses, avec un MAX-ACCESS de Accessible-for-notify *(accessible à la notification)*, dans toutes futures versions du module MIB RIPv2.

5.3 Considérations sur la gestion des clés

Ces dernières années, la configuration manuelle (par exemple, via une console) a été communément utilisée pour créer et modifier les associations de sécurité RIPv2. Un grand nombre de développements de RIP à grande échelle utilisent aujourd'hui avec succès la configuration manuelle d'associations de sécurité RIPv2. Il y a aussi des sites qui utilisent des scripts (par exemple, en combinant Tcl/Expect, PERL, et SSHv2) avec une base de données de configuration spécifique du site et des connexions de console sécurisées pour gérer de façon dynamique tous les aspects de leurs configurations de routeur, y compris leurs associations de sécurité RIPv2. Cette dernière approche est similaire à l'approche actuelle de l'IETF pour les normes de configuration de réseau (NetConf).

Les efforts récents du groupe de travail Sécurité en diffusion groupée (MSEC, *Multicast Security*) de l'IETF sur la gestion des clés en diffusion groupé paraissent prometteurs. Plusieurs grands développements de RIPv2 ont aussi utilisé le système d'authentification Kerberos. Le travail récent de l'IETF sur l'utilisation de Kerberos pour la négociation de clés sur l'Internet (KINK, *Internet Key Negotiation*) semble aussi pertinent ; on peut utiliser Kerberos pour prendre en charge les fonctions de gestion de clés RIPv2 pour une utilisation sur des sites qui ont déjà développé Kerberos. On peut souhaiter que dans l'avenir l'IETF normalise un protocole de gestion de clés convenable pour la gestion des associations de sécurité RIPv2.

5.4 Considérations sur l'assurance

Les utilisateurs ont besoin de comprendre que la qualité de la sécurité fournie par ce mécanisme dépend entièrement de la force des algorithmes d'authentification mis en œuvre, de la force de la clé utilisée, et de la mise en œuvre correcte du mécanisme de sécurité dans toutes les mises en œuvre RIPv2 communicantes. Ce mécanisme dépend aussi de la préservation de la confidentialité de la clé d'authentification RIPv2 par toutes les parties. Si un seul de ces éléments est incorrect ou insuffisamment sécurisé, aucune sécurité réelle ne peut être procurée aux utilisateurs de ce mécanisme.

L'utilisation de méthodes de développement à forte garantie est RECOMMANDÉE pour les mises en œuvre de la présente spécification, afin de réduire le risque de fautes de mise en œuvre subtiles qui pourraient avoir un impact pernicieux sur la réduction de risque fonctionnel que cherche à apporter la présente spécification.

5.5 Considérations sur la confidentialité et l'analyse de trafic

La confidentialité n'est pas fournie par ce mécanisme. On considère en général qu'un protocole d'acheminement IP n'exige pas la confidentialité, car l'objet de tous les protocoles d'acheminement est de disséminer les informations sur la topologie du réseau.

La protection contre l'analyse du trafic n'est pas fournie non plus. Les mécanismes tels que le chiffrement de liaison en bloc DEVRAIENT être utilisés pour la protection contre les analyses de trafic, en tant que de besoin [CKHD89].

5.6 Autres considérations sur la sécurité

D'autre part, la réception d'un paquet RIPv2 qui utilise l'authentification cryptographique mais contient une valeur de Key-ID invalide ou inconnue pourrait indiquer une attaque active sur le sous-système d'acheminement RIP et est un événement de sécurité significatif. Donc, toute réception effective d'un paquet RIPv2 qui utilise l'authentification cryptographique et contient une valeur de KEY-ID inconnue, expirée, ou invalide par ailleurs DEVRAIT causer un événement de sécurité à enregistrer par la mise en œuvre. L'élément enregistré DEVRAIT comporter au moins le fait que le KEY-ID invalide a été reçu, l'adresse IP de source du paquet contenant le KEY-ID invalide, la ou les interfaces sur lesquelles le paquet a été reçu, le KEY-ID reçu, et la date/heure de l'événement.

On devrait aussi noter une considération subtile sur l'interface d'utilisateur. Si une interface d'utilisateur ne permet que l'entrée de texte lisible par l'homme (par exemple, un mot de passe en format US-ASCII) à utiliser comme clé de chiffrement, un nombre significatif de bits de la clé de chiffrement utilisée devient prévisible, réduisant par là la force de la clé dans ce contexte. Pour cette raison, les mises en œuvre de la présente spécification DEVRAIENT accepter l'entrée de clés d'authentification de chiffrement RIPv2 en format hexadécimal.

5.7 Orientations futures de la sécurité

La spécification et le développement d'une norme de protocole de gestion de clés qui prenne en charge ce mécanisme d'authentification cryptographique RIPv2 serait la prochaine étape significative de la réduction des risques opérationnels et pourrait réellement accroître la facilité de développement et de fonctionnement de ce mécanisme. Une telle spécification va au delà du domaine d'application du présent document. Le travail récent de l'IETF dans les groupes de travail MSEC et KINK paraît prometteur à cet égard. Le travail récent de l'IETF dans le groupe de travail NETCONF sur les méthodes de normalisation de la sécurisation de la gestion de configuration des routeurs est tout aussi pertinent.

Finalement, on observe que ce mécanisme n'est pas le dernier mot sur l'authentification RIPv2. On estime plutôt que ce mécanisme particulier représente une réduction de risque significative par rapport aux méthodes précédentes (par exemple, les mots de passe en clair), bien qu'il reste encore à le mettre en œuvre correctement et aussi à le développer.

Les communautés d'utilisateurs qui estiment que ce mécanisme n'est pas adéquat à leurs besoins sont invitées à prendre en considération l'utilisation des signatures numériques avec RIPv2. [MBW97] spécifie l'utilisation de OSPF avec des signatures numériques ; ce document pourrait être un point de départ de la création d'une telle spécification pour le protocole RIPv2. Les signatures numériques sont significativement moins coûteuses en calcul et sont aussi significativement plus difficiles à mettre en œuvre, comparées au mécanisme spécifié ici. Cependant, il paraît

vraisemblable que la plus grande partie du mécanisme du présent document pourrait être réutilisée avec les signatures numériques.

6 Remerciements

Fred Baker était le coauteur du document d'authentification MD5 sur RIPv2 précédent [AB97]. Le présent document dérive directement de ce document précédent, bien qu'il ait été significativement remanié. Les auteurs actuels tiennent à remercier Bill Burr, Tim Polk, John Kelsey, et Morris Dworkin du (US) NIST pour leur relecture des versions de ce document.

7 Références normatives

[BCP14] Bradner, S., "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC2119, mars 1997.

[Mal98] Malkin, G., "RIP Version 2", STD 56, RFC2453, novembre 1998.

[FIPS-180-2]National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-2, août 2002, <http://csrc.nist.gov/publications/fips/fips180-2/ fips180-2.pdf>.

[FIPS-198] National Institute of Standards and Technology, "The Keyed-Hash Message Authentication Code (HMAC)", FIPS PUB 198, March 2002, <http://csrc.nist.gov/publications/ fips/fips198/fips-198a.pdf>.

8 Références informatives

[AB97] Baker, F. and R. Atkinson, "RIP-2 MD5 Authentication", RFC2082, janvier 1997.

[Bell89] S. Bellovin, "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Volume 19, Number 2, pp. 32-48, avril 1989.

[CKHD89] Cole Jr, Raymond, Donald Kallgren, Richard Hale, and John R. Davis, "Multilevel Secure Mixed-Media Communication Networks", Proceedings of the IEEE Military Communications Conference (MILCOM '89), IEEE, 1989.

[Dobb96a] Dobbertin, H., "Cryptanalysis of MD5 Compress", Technical Report, 2 mai 1996. (Présenté à la session Rump de EuroCrypt 1996.)

[Dobb96b] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes, Vol. 2, No. 2, Summer 1996.

[ESC05] Eastlake, D., 3rd, Schiller, J., et S. Crocker, "Exigence en aléatoire pour la sécurité", BCP 106, RFC4086, juin 2005.

[HA94] Haller N. et R. Atkinson, "Authentification sur l'Internet", RFC 1704, octobre 1994.

[KMC97] Krawczyk H., Bellare M., et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", RFC2104, février 1997.

[Mal94] Malkin, G., "RIP Version 2 – Transport d'informations supplémentaires", RFC1723, novembre 1994.

[MB94] Malkin G. et F. Baker, "Extension MIB de RIP Version 2", RFC1724, novembre 1994.

[MBW97] Murphy S., Badger M., et B. Wellington, "OSPF avec signatures numériques", RFC2154, juin 1997.

[Rivest92] Rivest, R., "L'algorithme de résumé de message MD5", RFC1321, avril 1992.

Adresse des auteurs

R. Atkinson
Extreme Networks
3585 Monroe Street
Santa Clara, CA 95051
USA
Phone: +1 (408) 579-2800
EMail: rja@extremenetworks.com

M. Fanto
(US) National Institute of Standards and Technology
Gaithersburg, MD 20878
USA
Phone: +1 (301) 975-2000
EMail: mattjf@umd.edu
Web: http://csrc.nist.gov

Déclaration de droits de reproduction

Copyright (C) The IETF Trust (2007).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournies sur une base "EN L'ÉTAT" et LE CONTRIBUTEUR, L'ORGANISATION QU'IL OU ELLE REPRÉSENTE OU QUI LE/LA FINANCE (S'IL EN EST), LA INTERNET SOCIETY ET LA INTERNET ENGINEERING TASK FORCE DÉCLINENT TOUTES GARANTIES, EXPRIMÉES OU IMPLICITES, Y COMPRIS MAIS NON LIMITÉES À TOUTE GARANTIE QUE L'UTILISATION DES INFORMATIONS CI ENCLOSES NE VIOLENT AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

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