Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 8210
RFC mise à jour : 6810
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

R. Bush, Internet Initiative Japan
R. Austein, Dragon Research Labs
septembre 2017

Traduction Claude Brière de L'Isle

Infrastructure de clé publique de ressource (RPKI) pour protocole de routeur, version 1

Résumé
Afin de valider de façon vérifiable les systèmes autonomes d'origine et les chemins de système autonome des annonces de BGP, les routeurs ont besoin d'un mécanisme simple mais fiable pour recevoir les données d'origine et les clés de routeur de l'infrastructure de clé publique de ressource (RPKI, *Resource Public Key Infrastructure*) [RFC6480] provenant d'une antémémoire de confiance. Le présent document décrit un protocole pour les livrer.

Le présent document décrit la version 1 du protocole de routeur RPKI. La RFC 6810 décrit la version 0. Ce document met à jour la RFC 6810.

Statut de ce mémoire
Ceci est un document de l'Internet en cours de normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc8210

Table des matières

1. Introduction

Afin de valider de façon vérifiable les systèmes autonomes (AS, *Autonomous System*) d'origine et les chemins d'AS des annonces de BGP, les routeurs ont besoin d'un mécanisme simple mais fiable pour recevoir les données d'origine de préfixe validées cryptographiquement de l'infrastructure de clé publique de ressource (RPKI, *Resource Public Key Infrastructure*) [RFC6480] et les clés de routeur à partir d'une antémémoire de confiance. Le présent document décrit un protocole pour les livrer. La conception se restreint intentionnellement à être utilisable sur la plupart des plates-formes de la génération actuelle de routeur des fourniseurs d'accès Internet (FAI).

Le présent document met à jour la [RFC6810].

La Section 3 décrit la structure de déploiement, et la Section 4 présente ensuite une vue générale du fonctionnement. Les charges utiles binaires du protocole sont décrites de façon formelle à la Section 5, et les séquences attendues d'unités de données de protocole (PDU, *Protocol Data Unit*) sont décrites à la Section 8. Les options de protocole de transport sont décrites à la Section 9. La Section 10 précise comment les routeurs et antémémoires sont configurés pour se connecter et s'authentifier. La Section 11 décrit les scénarios de déploiement probables. Les considérations traditionnelles sur la sécurité et l'IANA terminent le document.

Le protocole est extensible afin de prendre en charge de nouvelles PDU avec une nouvelle sémantique, si l'expérience du déploiement indique qu'elles sont nécessaires. Les PDU sont munies d'un numéro de version pour le cas où l'expérience du déploiement inviterait à des changements.

1.1 Langage des exigences

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], [RFC8174] quand, et seulement quand ils apparaissent tout en majuscules, comme montré ci-dessus.

1.2 Changements par rapport à la RFC 6810

Ce paragraphe résume les changements significatifs entre la [RFC6810] et le protocole décrit dans le présent document.
- o Ajout du type de PDU Nouvelle clé de routeur (paragraphe 5.10).
- o Ajout de paramètres explicites de temps (paragraphe 5.8, Section 6).

- o Numéro de version de protocole incrémenté de 0 (zéro) à 1 (un).
- o Ajout de la négociation de numéro de version de protocole (Section 7).

2. Glossaire

Les termes suivants sont utilisés avec une signification particulière.

RPKI global : les données d'autorité de RPKI sont publiées dans un ensemble réparti de serveurs à l'IANA, chez les registres Internet régionaux (RIR), les registres Internet nationaux (NIR), et les FAI ; voir la [RFC6481].

antémémoire : une antémémoire est une copie coalescente des données publiées du RPKI global, périodiquement collectées ou rafraîchies, directement ou indirectement, en utilisant le protocole rsync [RFC5781] ou un de ses successeurs. Le logiciel de consommateur d'assertions est utilisé pour collecter et valider les données distribuées de RPKI dans une antémémoire. Faire confiance à cette antémémoire est une affaire entre le fournisseur de l'antémémoire et un consommateur d'assertions.

Numéro de série : "Numéro de série" est un entier non signé de 32 bits strictement croissant qui revient à zéro à 2^32-1. Il note la version logique d'une antémémoire. Une antémémoire incrémente sa valeur quand elle réussit à mettre à jour ses données à partir d'une antémémoire parente ou à partir de données RPKI primaires. Lorsque une antémémoire reçoit des mises à jour, de nouvelles données entrantes et des suppressions implicites sont associées à la nouvelle série mais NE DOIVENT PAS être envoyées tant que la collecte n'est pas achevée. Un numéro de série n'a pas de rapport avec les différentes versions d'antémémoires ou de protocole, ni n'a besoin d'être maintenu à travers les réinitialisations du serveur d'antémémoire. Voir la [RFC1982] sur l'arithmétique de numéro de série du DNS pour de nombreux détails sur le sujet.

Identifiant de session : quand un serveur d'antémémoire démarre, il génère un identifiant de session pour identifier de façon univoque l'instance de l'antémémoire et la lier à la séquence des numéros de série que l'instance d'antémémoire va générer. Cela permet au routeur de redémarrer une session en échec, sachant que le numéro de série qu'il utilise est en rapport avec celui de l'antémémoire.

PDU de charge utile : une PDU de charge utile est un message de protocole qui contient des données à utiliser par le routeur, par opposition à une PDU qui porte les mécanismes de contrôle de ce protocole. Les préfixes et les clés de routeur sont des exemples de PDU de charge utile.

3. Structure de déploiement

Le déploiement de la RPKI pour atteindre les routeurs a la structure à trois niveaux suivante :

GRPKI global : les données d'autorité de la RPKI sont publiées dans un ensemble réparti de serveurs à l'IANA, chez les RIR, les NIR, et les FAI (voir la [RFC6481]).

Antémémoires locales : les antémémoires locales sont un ensemble local de une ou plusieurs antémémoires collectées et vérifiées de données de RPKI. Un consommateur d'assertions, par exemple, routeur ou autre client, DOIT avoir une relation de confiance, et un canal de transport de confiance, avec toute antémémoire qu'il utilise.

Routeurs : un routeur va chercher les données dans une antémémoire locale en utilisant le protocole décrit dans le présent document. Il est dit être un client de l'antémémoire. Il PEUT y avoir des mécanismes pour que le routeur s'assure de l'authenticité de l'antémémoire et pour l'authentifier lui-même auprès de l'antémémoire (voir la Section 9).

4. Vue d'ensemble du fonctionnement

Un routeur établit et garde ouverte une connexion à une ou plusieurs antémémoires avec lesquelles il a des relations de client/serveur. Il est configuré avec une liste semi ordonnée d'antémémoires et établit une connexion avec l'antémémoire, ou ensemble d'antémémoires préférées, qui acceptent les connexions.

Le routeur DOIT choisir, par configuration, l'antémémoire ou ensemble d'antémémoires préférées afin que l'opérateur puisse contrôler la charge sur ses antémémoires et sur le RPKI global.

Périodiquement, le routeur envoie à l'antémémoire le plus récent numéro de série pour lequel il a reçu des données provenant de cette antémémoire, c'est-à-dire, le numéro de série courant du routeur, sous la forme d'une interrogation de série *(Serial Query)*. Quand un routeur établit une nouvelle session avec une antémémoire ou souhaite réinitialiser une relation en cours, il envoie une interrogation de réinitialisation *(Reset Query)*.

L'antémémoire répond à l'interrogation de série avec tous les changements de données qui ont eu lieu depuis le numéro de série donné. Ce peut être l'ensemble nul, auquel cas la PDU Fin de données *(End of Data)* (paragraphe 5.8) est quand même envoyée. Noter que la comparaison de numéro de série utilisée pour déterminer "depuis le numéro de série donné" DOIT prendre en compte le retour à zéro ; voir la [RFC1982].

Quand le routeur a reçu tous les enregistrements de données de l'antémémoire, il règle son numéro de série courant à celui de la PDU Fin de données reçue.

Quand l'antémémoire met à jour sa base de données, elle envoie une PDU Notification à chaque routeur actuellement connecté. C'est l'indication que ce serait maintenant le bon moment pour que le routeur interroge pour une mise à jour, mais c'est seulement une indication. Le protocole exige en tous cas que le routeur interroge périodiquement sur les mises à jour.

Strictement parlant, un routeur pourrait suivre une antémémoire en demandant simplement un ensemble complet des données chaque fois qu'il se met à jour, mais ce serait très inefficace. Le mécanisme de mise à jour incrémentaire fondé sur le numéro de série permet un transfert efficace de juste les enregistrements de données qui ont changé depuis la dernière mise à jour. Comme avec tout protocole de mise à jour fondé sur des transferts incrémentaires, le routeur doit être prêt à revenir à un transfert complet si pour une raison quelconque l'antémémoire est incapable de fournir les données incrémentaires nécessaires. À la différence de certains protocoles de transfert incrémentaires, le présent protocole exige que le routeur fasse une demande explicite pour commencer le processus de reprise ; ceci est délibéré, car l'antémémoire n'a aucun moyen de savoir si le routeur a aussi établi des sessions avec d'autres antémémoires qui peuvent être capables de fournir un meilleur service.

Comme un serveur d'antémémoire doit évaluer les certificats et les autorisations d'origine de chemin (ROA, *Route Origin Authorization*) (voir la [RFC6480]) qui dépendent de l'heure, les horloges des serveurs DOIVENT être correctes à une tolérance d'approximativement une heure.

5. Unités de données de protocole (PDU)

Les échanges entre l'antémémoire et le routeur sont les séquences d'échanges des PDU suivantes selon les règles décrites à la Section 8.

Les champs Réservés (marqués "zéro" dans les diagrammes de PDU) DOIVENT être à zéro à l'émission et DOIVENT être ignorés à réception.

5.1 Champs d'une PDU

Les PDU contiennent les éléments de données suivants :

Version du protocole : entier non signé de 8 bits, actuellement 1, notant la version de ce protocole.

Type de PDU : entier non signé de 8 bits, notant le type de la PDU, par exemple, préfixe IPv4.

Numéro de série : numéro de série de l'antémémoire RPKI quand cet ensemble de PDU a été reçu d'un serveur d'antémémoire en amont ou collecté du RPKI mondial. Une antémémoire incrémente son numéro de série quand celle achève une mise à jour rigoureusement validée à partir d'une antémémoire parente ou du RPKI mondial.

Identifiant de session : entier non signé de 16 bits. Quand un serveur d'antémémoire démarre, il génère un identifiant de session pour identifier l'instance de l'antémémoire et la lier à la séquence des numéros de série que l'instance d'antémémoire va générer. Cela permet au routeur de redémarrer une session défaillante en sachant que le numéro de série qu'il utilise est proportionnel à celui de l'antémémoire. Si, à tout moment après que la version de protocole a été

négociée (Section 7) le routeur ou l'antémémoire trouve que la valeur de l'identifiant de session n'est pas la même que celle de l'autre, la partie qui détecte la discordance DOIT immédiatement terminer la session avec une PDU Rapport d'erreur avec le code 0 ("Données corrompues") et le routeur DOIT purger toutes les données apprises de cette antémémoire.

Noter que les sessions sont spécifiques d'une version de protocole particulière. C'est-à-dire, si un serveur d'antémémoire qui prend en charge plusieurs versions de ce protocole se trouve utiliser la même valeur d'identifiant de session pour plusieurs versions de protocole, et si il se trouve de plus qu'il utilise les mêmes valeurs de numéros de série pour deux sessions ou plus en utilisant le même identifiant de session mais des valeurs de version de protocole différentes, les numéros de série ne sont pas proportionnés. La vérification complète de la proportionnalité des numéros de série exige de comparer la version de protocole, l'identifiant de session, et le numéro de série. Pour réduire le risque de confusion, les serveurs d'antémémoire NE DEVRAIENT PAS utiliser le même identifiant de session sur plusieurs versions de protocole, mais même si ils le font, les routeurs DOIVENT traiter les sessions qui ont des champs Version de protocole différents comme des sessions séparées même si ils se trouvent avoir le même identifiant de session.

Si une antémémoire réutilisait à tort un identifiant de session de sorte qu'un routeur ne réalise pas que la session a changé (l'ancien identifiant de session et le nouvel identifiant de session ont la même valeur numérique) le routeur peut confondre le contenu de l'antémémoire. Le temps que prend le routeur pour découvrir qu'il s'est trompé va dépendre de si les numéros de série sont aussi réutilisés. Si les numéros de série dans l'ancienne et la nouvelle session sont assez différents, l'antémémoire va répondre à l'interrogation de série du routeur par une réinitialisation d'antémémoire, qui va résoudre le problème. Si, cependant, les numéros de série sont proches, l'antémémoire peut répondre par une Réponse d'antémémoire, qui peut n'être pas suffisante pour ramener le routeur à la synchronisation. Dans ce cas, il est probable, mais pas certain, que le routeur va détecter une discordance entre l'état que l'antémémoire attend et son propre état. Par exemple, la réponse d'antémémoire peut dire au routeur d'éliminer un enregistrement que le routeur ne détient pas ou peut lui dire d'ajouter un enregistrement que le routeur a déjà. Dans ce cas, un routeur va détecter l'erreur et réinitialiser la session. Le cas dans lequel le routeur peut rester non synchronisé est quand rien dans la réponse d'antémémoire ne contredit les données actuellement détenues par le routeur.

Utiliser une mémorisation persistante pour l'identifiant de session ou un schéma fondé sur une horloge pour générer les identifiants de session devrait éviter le risque de collisions d'identifiants de session.

L'identifiant de session pourrait être une valeur pseudo aléatoire, une valeur strictement croissante si l'antémémoire a une mémorisation fiable, et cœtera. Une valeur d'horodatage en secondes depuis une époque comme la fonction POSIX time() fait une bonne valeur d'identifiant de session.

Longueur : entier non signé de 32 bits qui a comme valeur le compte d'octets dans la PDU entière, incluant les 8 octets d'en-tête qui incluent le champ Longueur.

Fanions : le bit de moindre poids du champ Fanions est 1 pour une annonce et 0 pour un retrait. Pour une PDU Préfixe (IPv4 ou IPv6), le fanion indique si cette PDU annonce un nouveau droit d'annoncer le préfixe ou le retrait d'un droit annoncé précédemment ; un retrait supprime effectivement une PDU Préfixe annoncée précédemment avec exactement le même préfixe, longueur, Longueur maximum, et numéro de système autonome (ASN, *Autonomous System Number*). De même, pour une PDU Clé de routeur, le fanion indique si cette PDU annonce une nouvelle clé de routeur ou en supprime une précédemment annoncée avec exactement le même numéro d'AS, identifiant de clé sujette, et informations de clé publique sujette.

Les bits restants dans le champ Fanions sont réservés pour une utilisation future. Dans la version de protocole 1, ils DOIVENT être à zéro à l'émission et être ignorés à réception.

Longueur de préfixe : entier non signé de 8 bits notant le plus court préfixe permis par l'élément Préfixe.

Longueur maximum : entier non signé de 8 bits notant le plus long préfixe permis par l'élément Préfixe. Ce NE DOIT PAS être moins que l'élément Longueur de préfixe.

Préfixe : le préfixe IPv4 ou IPv6 du ROA.

Numéro de système autonome : entier non signé de 32 bits représentant un ASN à qui il est permis d'annoncer un préfixe ou associé à une clé de routeur.

Identifiant de clé sujette : valeur de 20 octets d'identifiant de clé sujette (SKI, *Subject Key Identifier*) d'une clé de routeur, comme décrit dans la [RFC6487].

Informations de clé publique sujette : valeur de subjectPublicKeyInfo de la clé d'un routeur, comme décrit dans la [RFC8208]. C'est le codage DER en ASN.1 de la subjectPublicKeyInfo, incluant l'étiquette ASN.1 et les valeurs de longueur de la SEQUENCE subjectPublicKeyInfo.

Intervalle de rafraîchissement : Intervalle entre les interrogations normales de l'antémémoire. Voir la Section 6.

Intervalle d'essais : intervalle entre les essais d'interrogation de l'antémémoire après un échec d'interrogation de l'antémémoire. Voir la Section 6.

Intervalle d'expiration : intervalle durant lequel les données collectées d'une antémémoire restent valides en l'absence d'une interrogation réussi suivante de l'antémémoire. Voir la Section 6.

5.2 Notification de série

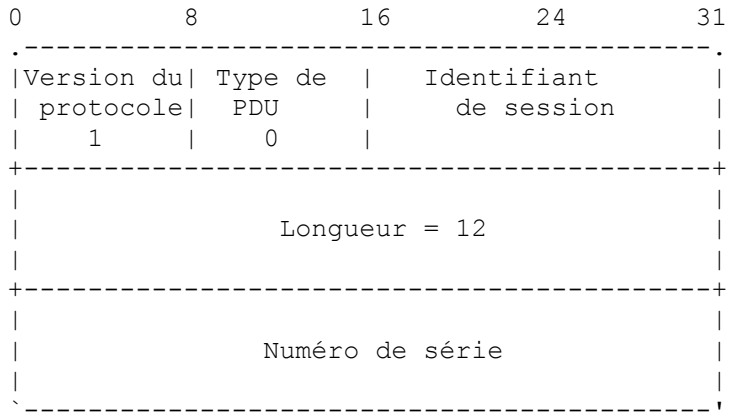
L'antémémoire notifie au routeur qu'elle a de nouvelle données.

L'identifiant de session réassure au routeur que les numéros de série sont proportionnés, c'est-à-dire, que la session d'antémémoire n'a pas été changée.

À réception d'une PDU Notification de série *(Serial Notify)*, le routeur PEUT produire une interrogation de série immédiate (paragraphe 5.3) ou une interrogation de réinitialisation (paragraphe 5.4) sans attendre l'expiration du temporisateur d'intervalle de rafraîchissement (voir la Section 6).

Notification de série est le seul message que l'antémémoire peut envoyer qui n'est pas en réponse à un message du routeur.

Si le routeur reçoit une PDU Notification de série durant la période de démarrage initial où le routeur et l'antémémoire sont encore en négociation pour s'accorder sur une version de protocole, le routeur DOIT simplement ignorer la PDU Notification de série, même si la PDU Notification de série est pour une version de protocole inattendue. Voir les détails à la Section 7.



5.3 Interrogation de série

Le routeur envoie une Interrogation de série *(Serial Query)* pour demander à l'antémémoire toutes les annonces et suppressions qui se sont produites depuis le numéro de série spécifié dans l'interrogation de série.

L'antémémoire répond à cette interrogation par une PDU Réponse d'antémémoire *(Cache Response)* (paragraphe 5.5) si l'antémémoire a un enregistrement (éventuellement nul) des changements depuis le numéro de série spécifié par le routeur, suivi par zéro, une ou plusieurs PDU de charge utile et une PDU Fin de données (paragraphe 5.8).

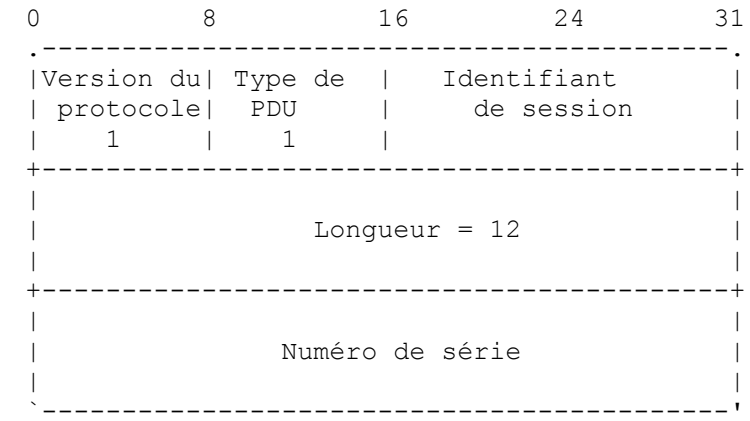
Quand elle répond à une interrogation de série, l'antémémoire DOIT retourner l'ensemble minimum de changements nécessaires pour mettre le routeur en synchronisation avec l'antémémoire. C'est-à-dire que si un préfixe ou clé de routeur particulier a subi plusieurs changements entre le numéro de série spécifié par le routeur et le numéro de série actuel de l'antémémoire, l'antémémoire DOIT fusionner ces changements pour présenter la vue la plus simple de ces changements au routeur. En général, cela signifie que, pour tout préfixe ou clé de routeur particulier, le flux de données va inclure au plus

une suppression suivie par au plus une annonce, et si tous les changements s'annulent, le flux de données ne mentionnera pas du tout le préfixe ou la clé de routeur.

La raison de cette approche est que l'objet entier du protocole RPKI de routeur est de décharger le travail du routeur sur l'antémémoire, et ce devrait donc être la tâche de l'antémémoire de simplifier l'ensemble de changements, réduisant donc le travail du routeur.

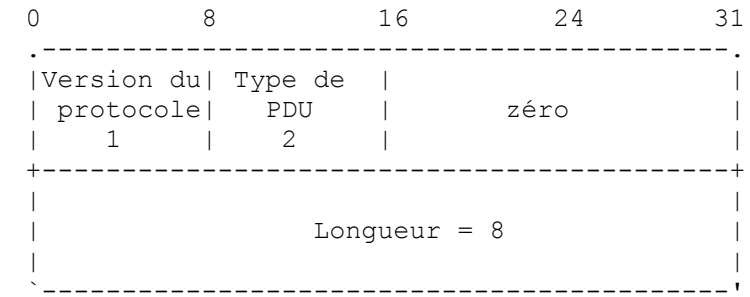
Si l'antémémoire n'a pas les données nécessaires pour mettre à jour le routeur, peut-être parce que ses enregistrements ne vont pas jusqu'au numéro de série de l'interrogation de série, elle répond alors par une PDU Réinitialisation d'antémémoire *(Cache Reset)* (paragraphe 5.9).

L'identifiant de session dit à l'antémémoire quelle instance le routeur attend pour s'assurer que les numéros de série sont proportionnés, c'est-à-dire, que la session de l'antémémoire n'a pas été changée.



5.4. Interrogation de réinitialisation *(Reset Query)*

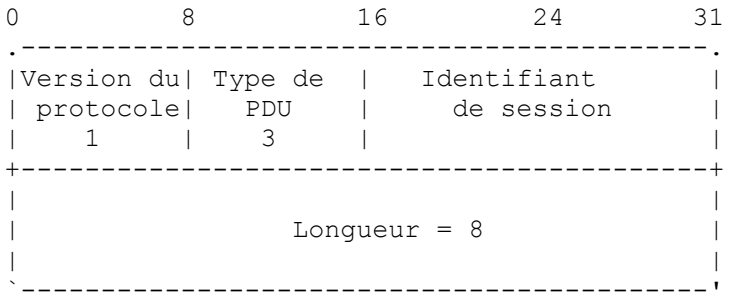
Le routeur dit à l'antémémoire qu'il veut recevoir la totalité de la base de données actives, actuelles, non retirées. L'antémémoire répond par une PDU Réponse d'antémémoire *(Cache Response)* (paragraphe 5.5) suivie par zéro, une ou plusieurs PDU de charge utile et une PDU Fin de données (paragraphe 5.8).



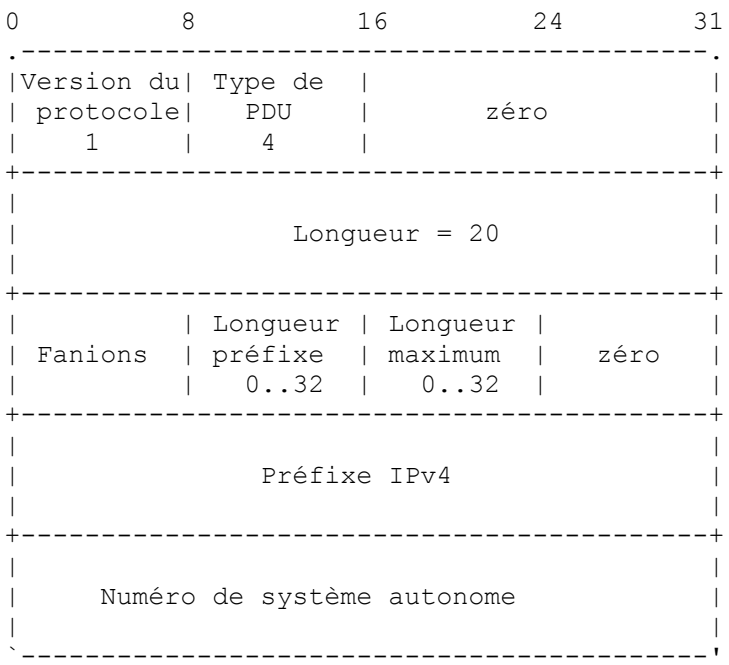
5.5 Réponse d'antémémoire

L'antémémoire répond aux interrogations avec zéro, une ou plusieurs PDU de charge utile. Quand elle répond à une interrogation de série (paragraphe 5.3) l'antémémoire envoie l'ensemble d'annonces et retraits qui se sont produits depuis le numéro de série envoyé par le client routeur. Quand elle répond à une interrogation de réinitialisation (paragraphe 5.4) l'antémémoire envoie l'ensemble de tous les enregistrements de données qu'elle a ; dans ce cas, le champ retraits/annonce dans les PDU de charge utile DOIT avoir la valeur 1 (annonce).

En réponse à une interrogation de réinitialisation, la nouvelle valeur de l'identifiant de session dit au routeur l'instance de la session de l'antémémoire pour une future confirmation. En réponse à une interrogation de série, l'identifiant de session qui est le même assure à nouveau au routeur que les numéros de série sont en proportion, c'est-à-dire, que la session d'antémémoire n'a pas été changée.



5.6 Préfixe IPv4



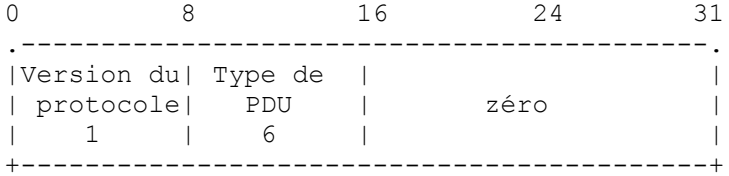
Le bit de moindre poids du champ Fanions est 1 pour une annonce et 0 pour un retrait.

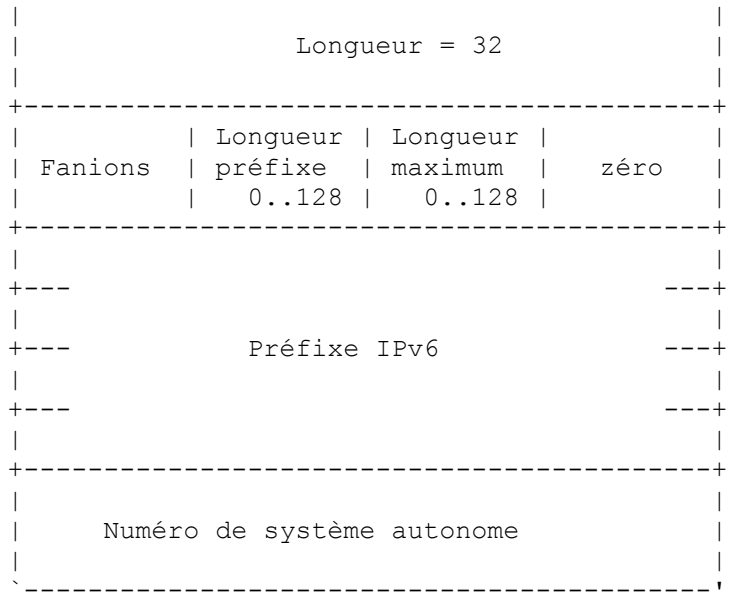
Dans RPKI, rien n'empêche un certificat signant de produire deux ROA identiques. Dans ce cas, il n'y aura pas de différence sémantique entre les objets, simplement une redondance de traitement.

Dans RPKI, il y a aussi un besoin réel de ce qui pourrait apparaître à un routeur comme des PDU IPvX identiques. Cela peut arriver quand un certificat en amont est produit à nouveau ou qu'il y a un transfert de propriété d'adresse qui remonte la chaîne de validation. La ROA va être identique au sens du routeur, c'est-à-dire, avoir le même {Préfixe, Longueur, Longueur maximum, ASN}, mais va avoir un chemin de validation différent dans le RPKI. Ceci est important pour le RPKI mais pas pour le routeur.

Le serveur d'antémémoire DOIT s'assurer qu'il a dit au client routeur d'avoir une et seulement une PDU IPvX pour un unique quartet {Préfixe, Longueur, Longueur maximum, ASN}à tout moment. Si le client routeur reçoit une PDU IPvX avec un {Préfixe, Longueur, Longueur maximum, ASN} identique à un qu'il a déjà actif, il DEVRAIT soulever une erreur Annonce dupliquée reçue.

5.7 Préfixe IPv6



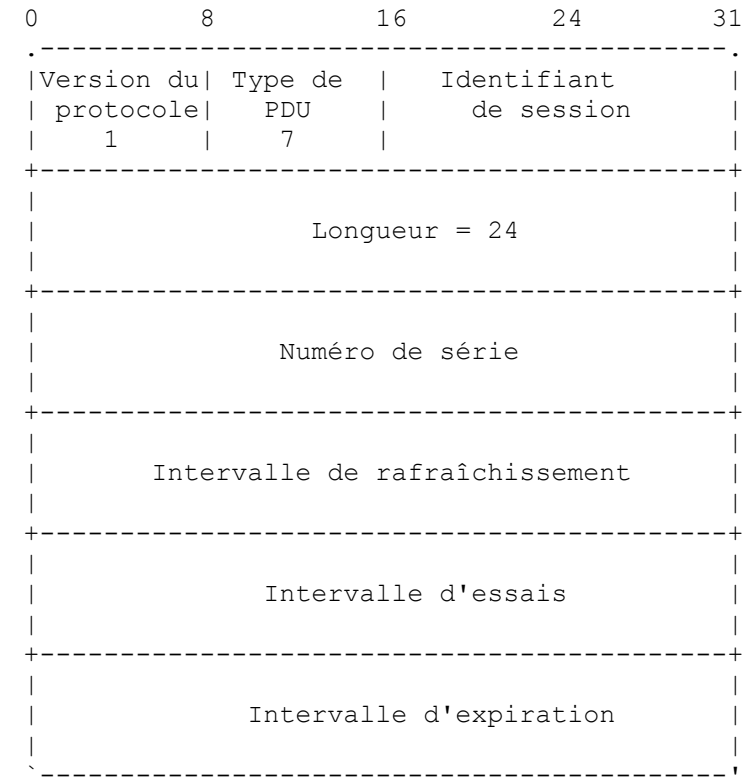


Analogue à la PDU Préfixe IPv4, elle a 96 bits de plus et pas de numéro magique.

5.8 Fin de données

L'antémémoire dit au routeur qu'elle n'a plus de données pour la demande.

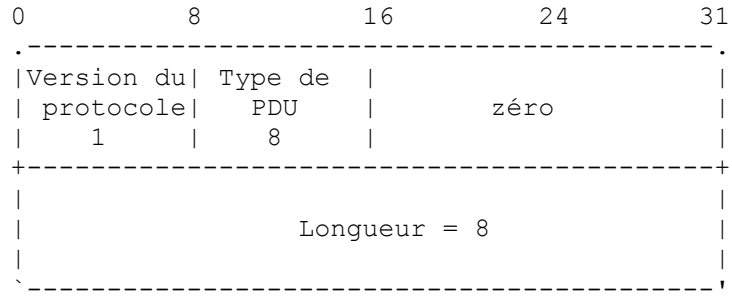
L'identifiant de session et la version du protocole DOIVENT être les mêmes que ceux de la réponse d'antémémoire correspondante qui commençait la séquence (éventuellement nulle) de PDU de charge utile.



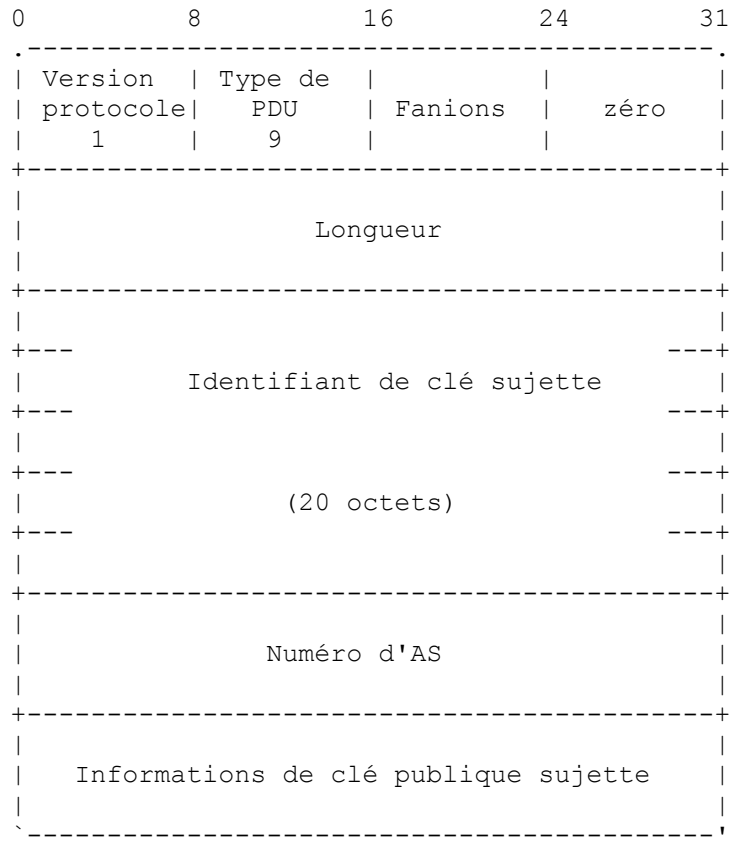
Les intervalles de rafraîchissement, d'essais, et d'expiration sont tous des temps écoulés de 32 bits mesurés en secondes. Ils expriment les paramètres de temps que l'antémémoire s'attend à ce que le routeur utilise pour décider quand envoyer les PDU d'interrogation de série ou d'interrogation de réinitialisation suivantes à l'antémémoire. Voir à la Section 6 les explications sur l'utilisation et la gamme des valeurs permises pour ces paramètres.

5.9 Réinitialisation d'antémémoire

L'antémémoire peut répondre à une interrogation de série en informant le routeur qu'elle ne peut pas fournir une mise à jour incrémentaire à partir du numéro de série spécifié par le routeur. Le routeur doit décider si il produit une interrogation de réinitialisation ou si il passe à une antémémoire différente.



5.10 Clé de routeur



Le bit de moindre poids du champ Fanions est réglé à 1 pour une annonce et à 0 pour un retrait.

Le serveur d'antémémoire DOIT s'assurer qu'il a dit au client routeur d'avoir une et une seule PDU Clé de routeur pour un unique triplet {SKI, ASN, Clé publique sujette} à tout moment. Si le client routeur reçoit une PDU Clé de routeur avec un triplet {SKI, ASN, Clé publique sujette} identique à une qu'il a déjà active, il DEVRAIT soulever une erreur Annonce dupliquée reçue.

Noter qu'un ASN particulier peut apparaître dans plusieurs PDU Clé de routeur avec des valeurs différentes de clé publique sujette, tandis qu'une valeur de clé publique sujette particulière peut apparaître dans plusieurs PDU Clé de routeur avec des ASN différents. Afin de garder la sémantique d'annonce et de retrait aussi simple que possible pour le routeur, ce protocole ne tente pas de compresser l'un ou l'autre de ces cas.

On notera aussi qu'il est possible, bien que très improbable, que plusieurs valeurs distinctes de clé publique sujette se hachent avec le même SKI. Pour cette raison, les mises en œuvre DOIVENT comparer les valeurs de clé publique sujette ainsi que les SKI quand elles détectent des PDU dupliquées.

5.11 Rapport d'erreur

Cette PDU est utilisée par l'une ou l'autre partie pour rapporter une erreur à l'autre.

Les rapports d'erreur ne sont seulement envoyés qu'en réponse aux autres PDU, pas aux erreurs de rapport dans les PDU de rapport d'erreur.

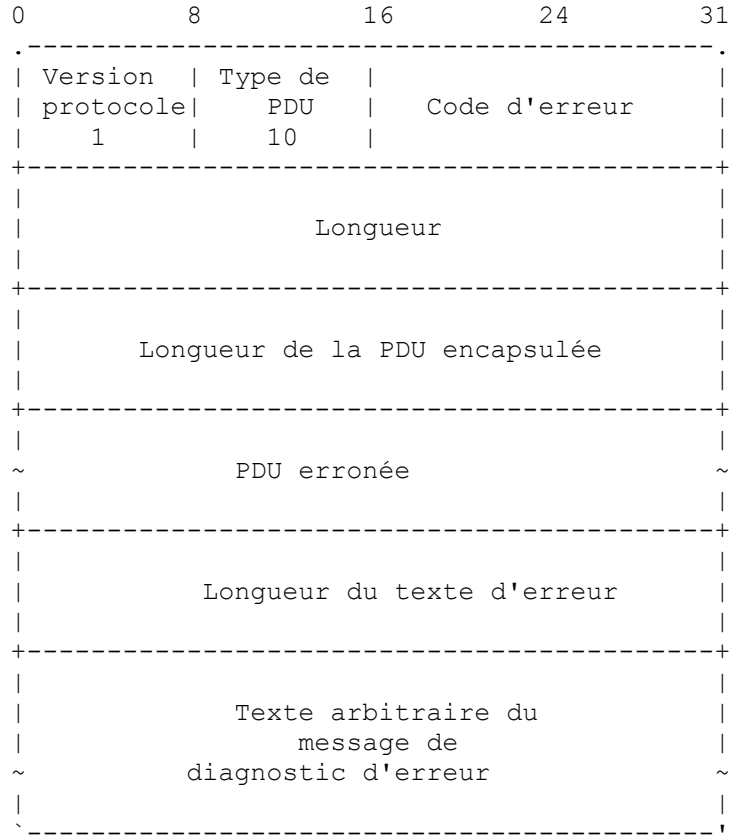
Les codes d'erreur sont décrits à la Section 12.

Si l'erreur est générique (par exemple, "Erreur interne") et non associée à la PDU à laquelle elle répond, le champ PDU erronée DOIT être vide et la longueur du champ PDU encapsulée DOIT être zéro.

Une PDU Rapport d'erreur NE DOIT PAS être envoyée pour une PDU Rapport d'erreur. Si une PDU Rapport d'erreur erronée est reçue , la session DEVRAIT être éliminée.

Si l'erreur est associée à une PDU de longueur excessive, c'est-à-dire, trop longue pour être une PDU légale autre qu'un autre rapport d'erreur, ou une longueur éventuellement corrompue, le champ PDU Erronée PEUT être tronqué.

Le texte de diagnostic est facultatif ; si il n'est pas présent, la longueur du champ Texte d'erreur DOIT être zéro. Si le texte d'erreur est présent, il DOIT être une chaîne codée en UTF-8 (voir la [RFC3629]).



6. Paramètres de temps du protocole

Comme les données que l'antémémoire distribue via le protocole de routeur RPKI sont restituées du système global RPKI à des intervalles qui sont seulement connus de l'antémémoire, seule l'antémémoire peut réellement savoir la fréquence à

laquelle le routeur doit interroger l'antémémoire, ou combien de temps les données vont probablement rester valides (ou, au moins, inchangées). Pour cette raison, ainsi que pour permettre à l'antémémoire un certain contrôle sur la charge que font peser sur elle ses routeurs clients, la PDU Fin de données comporte trois valeurs qui permettent à l'antémémoire de communiquer les paramètres de rythme au routeur :

Intervalle de rafraîchissement : ce paramètre dit au routeur combien de temps attendre avant la prochaine tentative d'interrogation de l'antémémoire et entre les tentatives suivantes, en utilisant une PDU Interrogation de série ou une interrogation de réinitialisation. Le routeur NE DEVRAIT PAS interroger l'antémémoire plus tôt qu'indiqué par ce paramètre. Noter que la réception d'une PDU Notification de série outrepasse cet intervalle et suggère que le routeur produise une interrogation immédiate sans attendre l'expiration de l'intervalle de rafraîchissement. Le décompte de ce temporisateur commence à réception de la PDU Fin de données qu'elle contient.
Valeur minimum permise : 1 seconde.
Valeur maximum permise : 86400 secondes (1 jour).
Valeur recommandée par défaut : 3600 secondes (1 heure).

Intervalle d'essais : ce paramètre dit au routeur combien de temps attendre avant de réessayer une interrogation de série ou une interrogation de réinitialisation qui a échoué. Le routeur NE DEVRAIT PAS réessayer plus tôt qu'indiqué par ce paramètre. Noter qu'une discordance de version de protocole outrepasse cet intervalle : si le routeur a besoin de rétrograder à un numéro de version de protocole inférieur, il PEUT envoyer immédiatement la première interrogation de série ou interrogation de réinitialisation. Le décompte de ce temporisateur commence à l'échec de l'interrogation et recommence après chaque échec suivant jusqu'à ce qu'une interrogation réussisse.
Valeur minimum permise : 1 seconde.
Valeur maximum permise : 7200 secondes (2 heures).
Valeur recommandée par défaut : 600 secondes (10 minutes).

Intervalle d'expiration : ce paramètre dit au routeur combien de temps il peut continuer d'utiliser la version courante des données alors qu'il est incapable d'effectuer une interrogation réussie. Le routeur NE DOIT PAS conserver les données après l'heure indiquée par ce paramètre. Le décompte de ce temporisateur commence à réception de la PDU Fin de données contenue.
Valeur minimum permise : 600 secondes (10 minutes).
Valeur maximum permise : 172800 secondes (2 jours).
Valeur recommandée par défaut : 7200 secondes (2 heures).

Si le routeur a déjà produit une interrogation réussie auprès d'une antémémoire particulière, il DEVRAIT réessayer périodiquement en utilisant l'intervalle d'essais par défaut ci-dessus.

Les antémémoires DOIVENT régler l'intervalle d'expiration à une valeur supérieure à celle de l'intervalle de rafraîchissement ou de l'intervalle d'essais.

7. Négociation de la version de protocole

Un routeur DOIT commencer chaque connexion de transport en produisant une interrogation de réinitialisation ou de série. Cette interrogation va dire à l'antémémoire quelle version de ce protocole le routeur met en œuvre.

Si une antémémoire qui prend en charge la version 1 reçoit une interrogation d'un routeur qui spécifie la version 0, l'antémémoire DOIT descendre à la version de protocole 0 [RFC6810] ou envoyer une PDU Rapport d'erreur de version 1 avec le code d'erreur 4 ("Version de protocole non prise en charge") et terminer la connexion.

Si un routeur qui prend en charge la version 1 envoie une interrogation à une antémémoire qui ne prend en charge que la version 0, il va arriver une des deux choses suivantes :
1. L'antémémoire peut terminer la connexion, peut-être avec une PDU Rapport d'erreur de version 0. Dans ce cas, le routeur PEUT réessayer la connexion en utilisant la version de protocole 0.
2. L'antémémoire peut répondre avec une réponse de version 0. Dans ce cas, le routeur DOIT soit dégrader à la version 0, soit terminer la connexion.

Dans toute les combinaisons de dégradation ci-dessus, les nouvelles caractéristiques de version 1 ne seront pas disponibles, et toutes les PDU auront 0 dans leur champ Version.

Si l'une ou l'autre partie reçoit une PDU contenant une version de protocole non reconnue (ni 0 ni 1) durant cette

négociation, elle DOIT dégrader à une version connue ou terminer la connexion, avec une PDU Rapport d'erreur sauf si la PDU reçue est elle-même une PDU de rapport d'erreur.

Le routeur DOIT ignorer toute PDU Notification de série qu'il pourrait recevoir de l'antémémoire durant cette période initiale de démarrage, sans considération du champ Version de protocole dans la PDU Notification de série. Comme l'identifiant de session et les valeurs de numéros de série sont spécifiques d'une version de protocole particulière, les valeurs dans la notification ne sont pas utiles au routeur. Même si ces valeurs avaient un sens, le seul effet qu'aurait le traitement de la notification serait de déclencher exactement la même interrogation de réinitialisation ou de série que le routeur a déjà envoyée au titre du processus de négociation de version pas encore achevé, de sorte qu'il n'y a rien à gagner à traiter les notifications avant que la négociation de version s'achève.

Les antémémoires NE DEVRAIENT PAS envoyer de PDU Notification de série avant l'achèvement de la négociation de version. Les routeurs DOIVENT cependant traiter de telles notifications (en les ignorant) pour la rétro compatibilité avec les antémémoires qui servent la version de protocole 0.

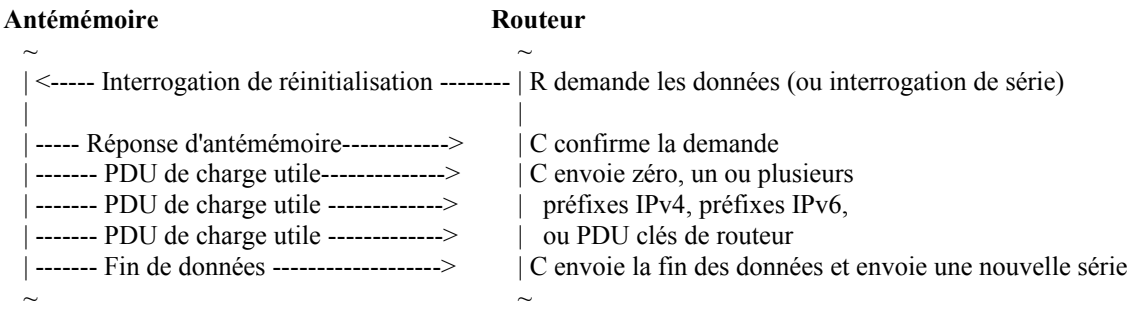
Une fois que antémémoire et routeur se sont accordés sur une version de protocole via le processus de négociation ci-dessus, cette version est stable pour la vie de la session. Voir au paragraphe 5.1 la discussion de l'interaction entre version de protocole et identifiant de session.

Si l'une ou l'autre partie reçoit une PDU pour une version de protocole différente une fois achevée la négociation ci-dessus, cette partie DOIT abandonner la session ; sauf si la PDU contenant la version de protocole inattendue était elle-même une PDU Rapport d'erreur, la partie qui abandonne la session DEVRAIT envoyer un rapport d'erreur avec un code d'erreur de 8 ("Version de protocole inattendue").

8. Séquences du protocole

Les séquences de transmissions de PDU tombent dans quatre conversations comme suit :

8.1 Commencement ou recommencement



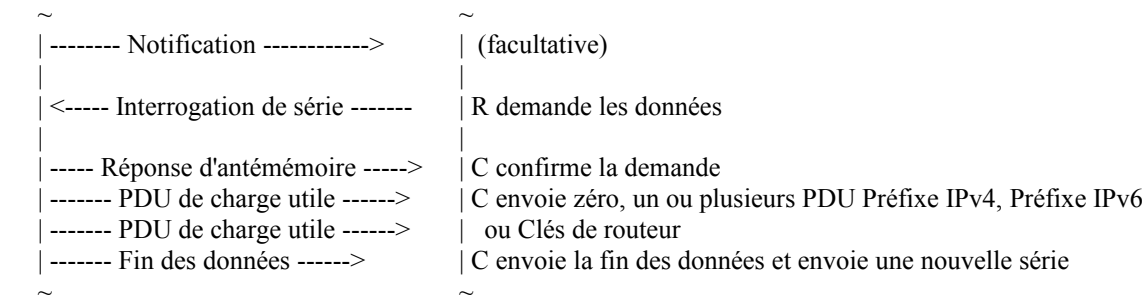
Au premier établissement d'une connexion de transport, le routeur DOIT envoyer une interrogation de réinitialisation ou de série. Une interrogation de série va être appropriée si le routeur a une quantité significative de données non expirées provenant d'une session rompue avec la même antémémoire et se souvient de l'identifiant de session de cette session, et dans ce cas une interrogation de série contenant l'identifiant de session provenant de la session précédente va permettre au routeur de se mettre à jour tout en s'assurant que les numéros de série sont proportionnels et que routeur et antémémoire parlent des versions de protocole compatibles. Dans tous les autres cas, il manque au routeur les données nécessaires pour une resynchronisation rapide et il DOIT donc revenir à une interrogation de réinitialisation.

La séquence d'interrogation de réinitialisation est aussi utilisée quand le routeur reçoit une réinitialisation d'antémémoire, choisit une nouvelle antémémoire, ou craint d'avoir perdu son chemin d'une façon quelconque.

Voir à la Section 7 les détails de la négociation de version.

Pour limiter la durée pendant laquelle une antémémoire doit conserver les données nécessaires pour générer des mises à jour incrémentaires, un routeur DOIT envoyer périodiquement une interrogation de série ou de réinitialisation. Ceci agit aussi comme un mécanisme de maintien en vie au niveau application. Voir à la Section 6 les détails sur la fréquence d'interrogation requise.

8.2 Échange normal

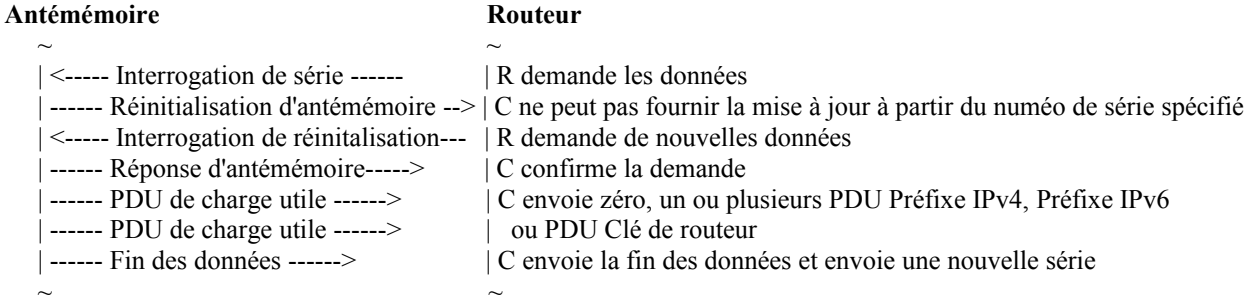


Le serveur d'antémémoire DEVRAIT envoyer une PDU Notification avec son numéro de série actuel quand change le numéro de série de l'antémémoire, dans l'espoir que le routeur PUISSE alors produire une interrogation de série plus tôt qu'il n'aurait fait autrement. C'est analogue au NOTIFY du DNS dans la [RFC1996]. L'antémémoire DOIT limiter le taux d'envoi des notifications de série à pas plus de une par minute.

Quand la couche transport est active et que un temporisateur a expiré au routeur ou que l'antémémoire a envoyé une PDU Notification, le routeur interroge sur de nouvelles données par l'envoi d'une interrogation de série, et l'antémémoire envoie toutes les données plus récentes que le numéro de série dans l'interrogation.

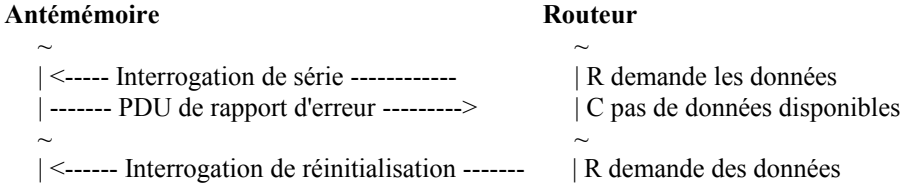
Pour limiter la durée pendant laquelle une antémémoire doit conserver les vieux retraits, un routeur DOIT envoyer périodiquement une interrogation de série ou de réinitialisation. Voir à la Section 6 les détails sur la fréquence d'interrogation requise.

8.3 Pas de mise à jour incrémentaire disponible



L'antémémoire peut répondre à une interrogation de série avec une réinitialisation d'antémémoire, informant le routeur que l'antémémoire ne peut pas fournir une mise à jour incrémentaire à partir du numéro de série spécifié par le routeur. Ce pourrait être parce que l'antémémoire a perdu l'état, ou parce que le routeur a attendu trop longtemps entre les interrogations et que l'antémémoire a purgé les vieilles données dont elle pensait n'avoir plus besoin, ou parce que l'antémémoire a épuisé son espace de mémorisation et devait purger plus tôt de vieilles données. Sans considération de la façon dont cet état est apparu, l'antémémoire répond avec une réinitialisation d'antémémoire pour dire au routeur qu'elle ne peut pas honorer la demande. Quand un routeur reçoit cela, il DEVRAIT tenter de se connecter à toute antémémoire préférée dans sa liste d'antémémoires. Si il n'y a plus d'antémémoires préférées, il DOIT produire une interrogation de réinitialisation et obtenir une nouvelle charge entière de l'antémémoire.

8.4 L'antémémoire n'a pas de données disponibles



| -------- PDU Rapport d'erreur----------> | C Pas de données disponibles
~ ~

L'antémémoire peut répondre à une interrogation de série ou de réinitialisation informant le routeur que l'antémémoire ne peut pas fournir du tout de mise à jour. La cause la plus probable est que l'antémémoire a perdu l'état, peut-être à cause d'un redémarrage, et n'a pas encore récupéré. Bien qu'il soit possible qu'une antémémoire arrive dans un tel état sans éliminer aucune de ses sessions actives, un routeur va plus probablement voir ce comportement quand il se connecte initialement et produit une interrogation de réinitialisation alors que l'antémémoire est encore en train de reconstruire sa base de données.

Quand un routeur reçoit cette sorte d'erreur, il DEVRAIT tenter de se connecter à toute autre antémémoire de sa liste des antémémoires, dans l'ordre des préférences. Si aucune autre antémémoire n'est disponible, le routeur DOIT produire des interrogations de réinitialisation périodiques jusqu'à ce qu'il obtienne une nouvelle charge utilisable de la part de l'antémémoire.

9. Transport

La session de couche transport entre un routeur et une antémémoire porte les PDU binaires dans une session persistante.

Pour empêcher l'usurpation d'identité d'antémémoire et les attaques de DoS par des routeurs illégitimes, il est très souhaitable que le routeur et l'antémémoire soient mutuellement authentifiées. La protection de l'intégrité des charges utiles est aussi désirable pour se protéger contre les attaques par interposition (MITM). Malheureusement, il n'y a pas de protocole pour le faire sur toutes les plates-formes actuellement utilisées. Donc, au moment de la rédaction du présent document, il n'y a pas de transport de mise en œuvre obligatoire qui assure l'authentification et la protection de l'intégrité.

Pour réduire l'exposition aux session abandonnées mais non terminées, les antémémoires et les routeurs DEVRAIENT activer des mécanismes de garde en vie quand ils sont disponibles dans le protocole de transport choisi.

Il est prévu que, quand l'option Authentification TCP (TCP-AO) [RFC5925] sera disponible sur toutes les plates-formes déployées par les opérateurs, elle deviendra le transport de mise en œuvre obligatoire.

Antémémoires et routeurs DOIVENT mettre en œuvre le transport non protégé sur TCP en utilisant l'accès rpki-rtr (323) ; voir la Section 14. Les opérateurs DEVRAIENT utiliser des moyens de procédure, par exemple, des listes de contrôle d'accès (ACL) pour réduire l'exposition aux problèmes d'authentification.

Si TCP non protégé est le transport, antémémoire et routeur DOIVENT être sur le même réseau de confiance et contrôlé.

Si c'est disponible à l'opérateur, antémémoires et routeurs DOIVENT utiliser un des protocoles plus protégés suivants :
- Antémémoires et routeurs DEVRAIENT utiliser le transport TCP-AO [RFC5925] sur l'accès rpki-rtr.
- Antémémoires et routeurs PEUVENT utiliser le transport Secure Shell version 2 (SSHv2) [RFC4252] en utilisant l'accès SSH normal. Voir un exemple au paragraphe 9.1.
- Antémémoires et routeurs PEUVENT utiliser le transport TCP MD5 [RFC2385] en utilisant l'accès rpki-rtr. Noter que TCP MD5 est rendu obsolète par TCP-AO [RFC5925].
- Antémémoires et routeurs PEUVENT utiliser le transport TCP sur IPsec [RFC4301] en utilisant l'accès rpki-rtr.
- Antémémoires et routeurs PEUVENT utiliser la sécurité de couche de transport (TLS) [RFC5246] en utilisant l'accès rpki-rtr-tls (324) ; voir à la Section 14.

9.1 Transport SSH

Pour fonctionner sur SSH, le routeur client établit d'abord une connexion de transport SSH en utilisant le protocole de transport SSHv2, et client et serveur échangent les clés pour l'intégrité et le chiffrement du message. Le client invoque alors le service "ssh-userauth" pour authentifier l'application, comme décrit dans le protocole d'authentification SSH [RFC4252]. Une fois que l'application a bien été authentifiée, le client invoque le service "ssh-connection", aussi appelé protocole de connexion SSH.

Après l'établissement du service ssh-connection, le client ouvre un canal de type "session", qui résulte en une session SSH.

Une fois la session SSH établie, l'application invoque le transport d'application comme un sous système SSH appelé "rpki-rtr". La prise en charge de sous systèmes est une caractéristique de SSHv2 et n'est pas incluse dans SSHv1. Faire

fonctionner ce protocole comme un sous système SSH évite d'avoir besoin que l'application reconnaisse l'invite SSH ou saute les informations étrangères, comme un message système envoyé au démarrage de SSH.

On suppose que routeur et antémémoire ont échangé les clés hors bande par des moyens raisonnablement sécurisés.

Les serveurs d'antémémoire qui prennent en charge le transport SSH DOIVENT accepter l'authentification RSA et DEVRAIENT accepter l'authentification par l'algorithme de signature numérique à courbe elliptique (ECDSA, *Elliptic Curve Digital Signature Algorithm*). L'authentification d'utilisateur DOIT être prise en charge ; l'authentification de l'hôte PEUT être prise en charge. Les mises en œuvre PEUVENT prendre en charge l'authentification par mot de passe. Les routeurs clients DEVRAIENT vérifier la clé publique de l'antémémoire pour éviter les attaques par interposition.

9.2 Transport TLS

Les routeurs clients qui utilisent le transport TLS DOIVENT présenter des certificats côté client pour s'authentifier à l'antémémoire afin de lui permettre de gérer la charge en rejetant la connexion pour les routeurs non autorisés. En principe, tout type de certificat et d'autorité de certification (CA) peut être utilisé ; cependant, en général, les opérateurs d'antémémoire vont vouloir créer leur propre CA à petite échelle et produire les certificats à chaque routeur autorisé. Cela simplifie le roulement des accréditifs ; tout certificat non révoqué, non expiré provenant de la CA appropriée peut être utilisé.

Les certificats utilisés pour authentifier les routeurs clients dans ce protocole DOIVENT inclure une extension subjectAltName [RFC5280] contenant une ou plusieurs identités iPAddress ; lors de l'authentification du certificat du routeur, l'antémémoire DOIT vérifier l'adresse IP de la connexion TLS par rapport à ces identités iPAddress et DEVRAIT rejeter la connexion si aucune des identités de iPAddress ne correspond à la connexion.

Les routeurs DOIVENT aussi vérifier le certificat de serveur TLS de l'antémémoire, en utilisant les identités subjectAltName dNSName comme décrit dans la [RFC6125], pour éviter des attaques par interposition. Les règles et lignes directrices définies dans la [RFC6125] s'appliquent ici, avec les considérations suivantes :

- La prise en charge du type d'identifiant DNS-ID (c'est-à-dire, l'identité dNSName dans l'extension subjectAltName) est EXIGÉE dans les mises en œuvre de serveur et client rpki-rtr qui utilisent TLS. Les autorités de certification qui produisent des certificats de serveur rpki-rtr DOIVENT prendre en charge le type d'identifiant DNS-ID, et le type d'identifiant DNS-ID DOIT être présent dans les certificats de serveur rpki-rtr.

- Les noms DNS dans les certificats rpki-rtr de serveur NE DEVRAIENT PAS contenir le caractère générique "*".

- Les mises en œuvre rpki-rtr qui utilisent TLS NE DOIVENT PAS utiliser des identifiants de nom commun (CN-ID, *Common Name identifier*) ; un champ CN peut être présent dans le nom de sujet du certificat de serveur mais NE DOIT PAS être utilisé pour l'authentification selon les règles décrites dans la [RFC6125].

- Le routeur client DOIT régler son "identifiant de référence" au nom DNS de l'antémémoire rpki-rtr.

9.3 Transport TCP MD5

Si TCP MD5 est utilisé, les mises en œuvre DOIVENT prendre en charge les longueurs de clé d'au moins 80 octets de caractères ASCII imprimables, selon le paragraphe 4.5 de la [RFC2385]. Les mises en œuvre DOIVENT aussi prendre en charge les séquences hexadécimales d'au moins 32 caractères, c'est-à-dire, 128 bits.

Le roulement de clés est problématique avec TCP MD5. Les serveurs d'antémémoire DEVRAIENT prendre en charge la [RFC4808].

9.4 Transport TCP-AO

Les mises en œuvre DOIVENT accepter des longueurs de clés d'au moins 80 octets d'ASCII imprimable. Les mises en œuvre DOIVENT aussi accepter des séquences hexadécimales d'au moins 32 caractères, c'est-à-dire, 128 bits. Les longueurs de code d'authentification de message (MAC) d'au moins 96 bits DOIVENT être acceptées, conformément au paragraphe 5.1 de la [RFC5925].

Les algorithmes de chiffrement et les paramètres associés décrits dans la [RFC5926] DOIVENT être pris en charge.

10. Établissement d'antémémoire de routeur

Une antémémoire a les données d'authentification publique de chaque routeur qu'elle est configurée à prendre en charge.

Un routeur peut être configuré à échanger du trafic avec une sélection d'antémémoires, et une antémémoire peut être configurée à prendre en charge une sélection de routeurs. Chacun doit avoir le nom et les données d'authentification pour chaque homologue. De plus, dans un routeur, cette liste a une valeur de préférence non unique pour chaque serveur. Cette préférence note simplement la proximité, non la confiance, la croyance préférée, etc.. Le routeur client tente d'établir une session avec chaque antémémoire potentiellement serveuse dans l'ordre de préférence et commence ensuite à charger les données à partir de l'antémémoire préférée à laquelle il peut se connecter et s'authentifier. La liste des antémémoires du routeur a les éléments suivants :

Préférence : entier non signé qui note la préférence du routeur pour se connecter à cette antémémoire ; plus la valeur est faible, plus la préférence est grande.

Nom : adresse IP ou nom de domaine pleinement qualifié de l'antémémoire.

Accréditifs d'antémémoire : tout accréditif (comme une clé publique) nécessaire pour authentifier l'identité de l'antémémoire au routeur.

Accréditifs de routeur : tout accréditif (comme une clé privée ou un certificat) nécessaire pour authentifier l'identité du routeur à l'antémémoire.

Due à la nature répartie de RPKI, les antémémoires ne peuvent pas être rigoureusement synchrones. Un client peut détenir des données provenant de plusieurs antémémoires mais DOIT marquer la source des données, car les mises à jour ultérieures DOIVENT affecter les données correctes.

Tout comme il peut y avoir plus d'une autorisation d'origine de route (ROA, *Route Origin Authorization*) couvrante provenant d'une seule antémémoire, il peut y avoir plusieurs ROA couvrants provenant de plusieurs antémémoires. Les résultats sont décrits dans la [RFC6811].

Si des données provenant de plusieurs antémémoires sont détenues, les mises en œuvre NE DOIVENT PAS distinguer entre les sources de données quand elles effectuent la validation des annonces BGP.

Quand une antémémoire de préférence plus élevée devient disponible, si les ressources le permettent, il serait prudent que le client commence à aller chercher à partir de cette antémémoire.

Le client DEVRAIT tenter de conserver au moins un jeu de données, sans considération de si il a choisi une antémémoire différente ou établi une nouvelle connexion à l'antémémoire précédente.

Un client PEUT abandonner les données provenant d'une antémémoire particulière quand il est parfaitement synchronisé avec une ou plusieurs autres antémémoires.

Voir à la Section 6 les détails de ce qu'il convient de faire quand le client n'est pas capable de rafraîchir à partir d'une certaine antémémoire.

Si un client perd la connexité à une antémémoire qu'il utilise ou par ailleurs décide de passer à une nouvelle antémémoire, il DEVRAIT conserver les données de l'antémémoire précédente jusqu'à ce qu'il ait un jeu complet de données provenant d'une ou plusieurs autres antémémoires. Noter que ceci peut être déjà vrai au point de perte de connexion si le client a des connexions à plus d'une antémémoire.

11. Scénarios de déploiement

À des fins d'illustration, on présente trois scénarios de déploiement probables :

Petit site d'extrémité : le petit site d'extrémité multi rattachements peut souhaiter exporter l'antémémoire RPKI à un ou

plusieurs de ses fournisseurs d'accès Internet *(FAI)* en amont. Il va échanger le matériel d'authentification avec le FAI en utilisant un mécanisme hors bande, et leurs routeurs vont se connecter à la ou aux antémémoires d'un ou plusieurs FAI en amont. Les FAI vont probablement déployer des antémémoires destinées à l'usage des abonnés séparées des antémémoires avec lesquelles leurs propres locuteurs BGP échangent du trafic.

Grand site d'extrémité : un plus grand site multi rattachements pourrait faire fonctionner une ou plusieurs antémémoires, les arrangeant en une hiérarchie d'antémémoires clientes, chacune allant chercher chez une antémémoire de service celle qui est la plus proche du RPKI global. Il pourrait configurer des échanges de trafic de repli sur les antémémoires de FAI en amont.

Cœur de réseau de FAI : un grand FAI va probablement avoir une ou plusieurs antémémoires redondantes dans chaque point de préséance majeur, et ces antémémoires vont aller chercher de l'une à l'autre dans une topologie qui dépend du FAI de façon à ne pas faire peser une charge indue sur le RPKI global.

L'expérience des grands déploiements d'antémémoire du DNS a montré que les topologies complexes sont mal avisées, car il est aisé de faire des erreurs dans le graphe, par exemple, de ne pas maintenir une condition sans boucle.

Bien sûr, ce sont des illustrations, et il y a d'autre stratégies de déploiement possibles. On prévoit que minimiser la charge des serveurs du RPKI global sera une considération majeure.

Pour préserver la charge sur les services du RPKI global contre des pointes inutiles, il est recommandé que les antémémoires principales qui se chargent à partir du RPKI global réparti ne le fassent pas toutes au même moment, par exemple, à heure fixe. Choisir un moment aléatoire, peut-être le numéro d'AS du FAI modulo 60, et varier les temps d'inter collecte.

12. Codes d'erreur

Cette section contient une liste préliminaire de codes d'erreur. Les auteurs prévoient des ajouts à la liste durant le développement des mises en œuvre initiales. Il y a un registre IANA qui donne la liste des codes d'erreur valides ; voir la Section 14. Les erreurs qui sont considérées comme fatales DOIVENT causer l'abandon de la session.

0 : Données corrompues (fatal) : le receveur croit que la PDU reçue est corrompue d'une manière non spécifiée par un autre code d'erreur.

1 : Erreur interne (fatal) : la partie qui rapporte l'erreur a rencontré une certaine sorte d'erreur interne sans relation avec le fonctionnement du protocole (plus de mémoire, échec d'une assertion de codage, etc.).

2 : Pas de données disponibles : l'antémémoire se croit en bon ordre de fonctionnement mais est incapable de répondre à une interrogation de série ou de réinitialisation parce qu'elle n'a pas de données utiles disponibles à cet instant. C'est probablement une erreur temporaire et indique certainement que l'antémémoire n'a pas encore achevé de tirer un ensemble de données initiales courantes du système RPKI global après un événement qui a invalidé les données qu'elle pourrait avoir détenu précédemment (réamorçage, partition de réseau, etc.).

3 : Demande invalide (fatal) : le serveur d'antémémoire estime que la demande du client est invalide.

4 : Version de protocole non prise en charge (fatal): la version de protocole n'est pas connue du receveur de la PDU.

5 : Type de PDU non pris en charge (fatal) : le type de PDU n'est pas connu par le receveur de la PDU.

6 : Retrait d'un enregistrement inconnu (fatal) : la PDU reçue a Fanion = 0, mais un enregistrement correspondant (quartet {Préfixe, Longueur, Longueur maximale, ASN} pour une PDU IPvX ou triplet {SKI, ASN, Clé publique sujette} pour une PDU Clé de routeur) n'existe pas dans la base de données du receveur.

7 : Annonce dupliquée reçue (fatal) : la PDU reçue a Fanion = 1, mais un enregistrement correspondant (quartet {Préfixe, Longueur, Longueur maximale, ASN} pour une PDU IPvX ou triplet {SKI, ASN, Clé publique sujette} pour une PDU Clé de routeur) est déjà actif dans le routeur.

8 : Version de protocole inattendue (fatal) : la PDU reçue a un champ Version de protocole qui diffère de la version de protocole négociée à la Section 7.

13. Considérations sur la sécurité

Comme le présent document décrit un protocole de sécurité, beaucoup des aspects qui intéressent la sécurité sont décrits dans les sections pertinentes. Cette section souligne les aspects qui peuvent n'être pas évidents dans les autres sections.

Validation d'antémémoire : afin qu'une collection d'antémémoires comme décrit à la Section 11 garantisse une vue cohérente, elles doivent avoir des ancres de confiance cohérentes à utiliser dans leur processus de validation interne. La distribution d'une ancre de confiance cohérente est supposée être hors bande.

Identification d'antémémoire homologue : le routeur initie une connexion de transport avec une antémémoire, qu'il identifie par son adresse IP ou son nom de domaine pleinement qualifié. Il faut être conscient qu'une attaque du DNS ou de fausse adresse pourrait rendre l'antémémoire correcte injoignable. Aucune session ne serait établie, car les clés d'autorisation ne correspondraient pas.

Sécurité du transport : RPKI s'appuie sur la confiance en un objet, pas en un serveur ou un transport. C'est-à-dire que l'ancre de confiance racine de l'IANA est distribuée à toutes les antémémoires par un moyen hors bande et peut alors être utilisée par chaque antémémoire pour valider les certificats et ROA tout le long de l'arborescence. Les relations entre les antémémoires se fondent sur ce modèle de sécurité d'objet ; donc, le transport inter antémémoires peut être légèrement protégé.

Cependant, le présent document de protocole suppose que les routeurs ne peuvent pas faire la validation du chiffrement. Donc, la dernière liaison, de l'antémémoire au routeur, est sécurisée par l'authentification du serveur et la sécurité de niveau transport. Ceci est dangereux, car l'authentification du serveur et le transport ont des modèles de menaces très différents de celui de la sécurité d'objet.

Donc, la force de la relation de confiance et du transport entre le ou les routeurs et la ou les antémémoires sont critiques. L'acheminement fait un pari sur cela.

Bien qu'on ne puisse pas dire que l'antémémoire doit être sur le même LAN, si seulement à cause du problème d'une entreprise qui veut passer la charge de la tâche d'antémémoire à son ou ses FAI en amont, le caractère local, la confiance, et le contrôle sont des questions très critiques ici. La ou les antémémoires DEVRAIENT réellement être aussi proches, au sens de contrôlées et protégées (contre les attaques de DoS réparties, l'interposition) en transport, jusqu'aux routeurs autant que possible. Elles DEVRAIENT aussi être topologiquement proches afin qu'un minimum de données d'acheminement validées soient nécessaire pour fixer l'accès d'un routeur à une antémémoire.

L'identité du serveur d'antémémoire DEVRAIT être vérifiée et authentifiée par le client routeur, et vice versa, avant l'échange de toutes données.

Les transports qui ne peuvent pas fournir la nécessaire authentification et intégrité (voir la Section 9) doivent s'appuyer sur la conception du réseau et les contrôles de fonctionnement pour fournir la protection contre les attaques par usurpation d'identité/corruption. Comme souligné à la Section 9, TCP-AO est le plan à long terme. Les protocoles qui fournissent l'intégrité et l'authenticité DEVRAIENT être utilisés, et si cela ne se peut pas, c'est-à-dire, si TCP est utilisé comme transport, routeur et antémémoire DOIVENT être sur le même réseau contrôlé de confiance.

14. Considérations relatives à l'IANA

Cette section discute seulement des mises à jour requises dans les registres de protocole existants de l'IANA pour s'accommoder de la version 1 de ce protocole. Voir dans la [RFC6810] les considérations relatives à l'IANA du protocole d'origine (version 0).

Toutes les entrées existantes dans le registre IANA "rpki-rtr-pdu" restent valides pour la version de protocole 0. Tous les types de PDU permis dans la version de protocole 0 sont aussi permis dans la version de protocole 1, avec l'ajout de la nouvelle PDU Clé de routeur. Pour réduire la probabilité de confusion, le numéro de PDU utilisé par la PDU Clé de routeur dans la version de protocole 1 est ici enregistrée comme réservée (et non utilisée) dans la version de protocole 0.

La politique pour ajouter au registre est RFC exigée selon la [RFC8126] ; le document doit être sur la voie de la

normalisation ou expérimental.

Le registre "rpki-rtr-pdu" a été mis à jour comme suit :

Version du protocole	Type	Description de PDU
0-1	0	Notification de série
0-1	1	Interrogation de série
0-1	2	Interrogation de réinitialisation
0-1	3	Réponse d'antémémoire
0-1	4	Préfixe IPv4
0-1	6	Préfixe IPv6
0-1	7	Fin de données
0-1	8	Réinitialisation d'antémémoire
0	9	Réservé
1	9	Clé de routeur
0-1	10	Rapport d'erreur
0-1	255	Réservé

Toutes les entrées existantes dans le registre IANA "rpki-rtr-error" restent valides pour toutes les versions de protocole. La version 1 du protocole ajoute un nouveau code d'erreur :

Code d'erreur	Description
8	Version de protocole inattendue

15. Références

15.1 Références normatives

[RFC1982] R. Elz, R. Bush, "Arithmétique des numéros de série", août 1996, DOI 10.17487/RFC1982, (*MàJ* RFC1034, RFC1035) *(P.S.)*

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", DOI 10.17487/RFC2119, BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998, DOI 10.17487/RFC2385, *(P.S. ; MàJ par la* RFC6691) *; remplacée par* RFC5925)

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003, DOI 10.17487/RFC3629.

[RFC4252] T. Ylonen et C. Lonvick, éd., "Protocole d'authentification Secure Shell (SSH)", janvier 2006, DOI 10.17487/RFC4252, *(P.S .; MàJ par* RFC8308, 8332)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005, DOI 10.17487/RFC4301, *(P.S. ; Remplace la* RFC2401)

[RFC5246] T. Dierks, E. Rescorla, "Version 1.2 du protocole de sécurité de la couche Transport (TLS)", août 2008, DOI 10.17487/RFC5246, *(P.S. ; remplace* RFC3268, 4346, 4366 ; *MàJ* RFC4492 ; *rendue obsolète par la* RFC8446)

[RFC5280] D. Cooper et autres, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", mai 2008, DOI 10.17487/RFC5280, (*P.S. ; Remplace les* RFC3280, RFC4325, RFC4630 ; *MàJ par* RFC8398, 8399)

[RFC5925] J. Touch, A. Mankin, R. Bonica, "Option Authentification de TCP", juin 2010, DOI 10.17487/RFC5925, (*Remplace* RFC2385). *(P. S.)*

[RFC5926] G. Lebovitz, E. Rescorla, "Algorithmes de chiffrement pour l'option Authentification de TCP", juin 2010,

DOI 10.17487/RFC5926, *(P.S.)*

[RFC6125] P. Saint-André, J. Hodges, "Représentation et vérification d'identité de service d'application fondé sur le domaine au sein de l'infrastructure Internet de clé publique utilisant les certificats X.509 (PKIX) dans le contexte de la sécurité de la couche Transport (TLS)", mars 2011, DOI 10.17487/RFC6125, *(P.S.)*

[RFC6487] G. Huston, G. Michaelson, R. Loomans, "Profil pour les certificats de ressource X.509 PKIX", février 2012, DOI 10.17487/RFC6487, *(P.S. ; MàJ par* RFC8209)

[RFC6810] R. Bush et R. Austein, "Infrastructure de clé publique de ressource (RPKI) pour protocole de routeur", janvier 2013, DOI 10.17487/RFC6810, *(MàJ par* RFC8210)

[RFC6811] P. Mohapatra, et autres, "Validation d'origine de préfixe BGP", janvier 2013, DOI 10.17487/RFC6811, *(P;S; ; MàJ par* RFC8481, 8893)

[RFC8126] M. Cotton, B. Leiba, T. Narten, "Lignes directrices pour la rédaction d'une section de considérations relatives à l'IANA dans les RFC", juin 2017. BCP 26, DOI 10.17487/RFC8126, *(Remplace* RFC5226)

[RFC8174] B. Leiba, "Ambiguïté des mots clés en majuscules ou minuscules dans la RFC2119", mai 2017. BCP14, DOI 10.17487/RFC8174, *(MàJ* 2119)

[RFC8208] S. Turner, O. Borchert, "Algorithmes, formats de clé et de signature pour BGPsec", septembre 2017, DOI 10.17487/RFC8208, *(P.S. ; MàJ* RFC7935 *; rendue obsolète par* RFC8608*)*

15.2 Références pour information

[RFC1996] P. Vixie, "Mécanisme de notification rapide des changements de zone (DNS NOTIFY)", août 1996, DOI 10.17487/RFC1996, *(P.S.)*

[RFC4808] S. Bellovin, "Stratégies de changement de clés pour TCP-MD5", mars 2007, DOI 10.17487/RFC4808, *(Information)*

[RFC5781] S. Weiler, D. Ward, R. Housley, "Schéma d'URI rsync", février 2010, DOI 10.17487/RFC5781, *(Information)*

[RFC6480] M. Lepinski, S. Kent, "Infrastructure pour la prise en charge de l'acheminement Internet sécurisé", février 2012, DOI 10.17487/RFC6480, *(Info.)*

[RFC6481] G. Huston, R. Loomans, G. Michaelson, "Profil pour structure de répertoire de certificats de ressource", février 2012, DOI 10.17487/RFC6481, *(P.S.)*

Remerciements

Les auteurs tiennent à remercier Nils Bars, Steve Bellovin, Tim Bruijnzeels, Rex Fernando, Richard Hansen, Paul Hoffman, Fabian Holler, Russ Housley, Pradosh Mohapatra, Keyur Patel, David Mandelberg, Sandy Murphy, Robert Raszuk, Andreas Reuter, Thomas C. Schmidt, John Scudder, Ruediger Volk, Matthias Waehlisch, et David Ward. Des remerciements particuliers vont à Hannes Gredler qui nous a montré les dangers des champs inutiles.

Il ne fait pas de doute que cette liste est incomplète. Nos excuses à tout contributeur dont le nom nous a échappé.

Adresse des auteurs

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, Washington 98110
United States of America
mèl : randy@psg.com

Rob Austein
Dragon Research Labs
mèl : sra@hactrn.net