Groupe de travail Réseau
Request for Comments : 2725
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

C. Villamizar, Avici
C. Alaettinoglu, ISI
D. Meyer, Cisco
S. Murphy, TIS
décembre 1999

Sécurité du système de politique d'acheminement

Résumé
Les spécifications de la base de données RIPE et le langage RPSL définissent les langages utilisés comme base pour la représentation des informations dans un système de politique d'acheminement. Un répertoire des informations de systèmes de politique d'acheminement est appelé un registre d'acheminement. Un registre d'acheminement fournit le moyen d'échanger les informations nécessaires pour traiter des nombreuses questions d'importance pour le fonctionnement de l'Internet. La mise en œuvre et le déploiement d'un système de politique d'acheminement doit maintenir un certain degré d'intégrité pour avoir une certaine utilité opérationnelle. Le présent document traite du besoin d'assurer l'intégrité des données en fournissant un modèle d'authentification et d'autorisation.

Table des Matières

1. Généralités

Le registre des acheminements de l'Internet (IRR, *Internet Routing Registry*) a évolué pour satisfaire aux besoins de coordination à l'échelle de l'Internet. Ce besoin a été décrit dans la [RFC1787], une RFC pour information préparée au nom de l'IAB. Le résumé suivant figure à la Section 7 de la RFC1787.

Bien qu'assurer la coordination à l'échelle de l'Internet puisse être de plus en plus difficile, car l'Internet continue de grandir, la stabilité et la cohérence de l'acheminement à l'échelle de l'Internet pourraient être significativement améliorées si les informations sur les exigences d'acheminement dans les diverses organisations pouvaient être partagées à travers les frontières des organisations. De telles informations pourraient être utilisées dans une grande variété de situations allant de la détection des fauteurs de troubles à la détection et l'élimination des exigences d'acheminement conflictuelles. L'échelle de l'Internet implique que les informations devraient être réparties. Des travaux sont en cours pour établir des répertoires de ces informations (registres d'acheminement) ainsi que pour développer des outils qui analysent et utilisent ces informations.

Un registre d'acheminement doit assurer un certain degré d'intégrité pour pouvoir être utile. Le degré d'intégrité requis dépend de l'usage du système de politique d'acheminement.

Une utilisation initialement prévue des systèmes de politique d'acheminement comme la base de données RIPE était une capacité de conseil, documentant les politiques d'acheminement prévues pour les besoins de la chasse aux erreurs. Dans ce rôle, une forme d'authentification très faible était réputée suffisante.

L'IRR est de plus en plus utilisé pour des besoins qui ont une plus forte exigence d'intégrité des données et de sécurité. Le présent document traite des questions d'intégrité des données et de sécurité qui sont cohérentes avec l'usage de l'IRR et qui évitent de compromettre l'intégrité des données et la sécurité, même si l'IRR est réparti entre des répertoires moins dignes de confiance.

2. Fondements

Un système antérieur de politiques d'acheminement utilisé dans le NSFNET, la base de données de politique d'acheminement (PRDB, *policy routing database*) donnait un moyen pour déterminer qui était autorisé à annoncer des préfixes spécifiques au cœur de réseau NSFNET. Le besoin d'une base de données de politique a été reconnu dès 1989 [RFC1102], [RFC1104]. En 1991, la base de données était en place [RFC1222]. L'authentification a été accomplie en exigeant la confirmation et c'était un processus intensivement manuel. Cela résolvait le problème pour le NSFNET, mais était orienté vers la garde de la politique d'acheminement d'une seule organisation.

Les problèmes sont devenus plus difficiles depuis. De nouvelles exigences sont apparues.

1. Il y a besoin de représenter les politiques d'acheminement de nombreuses organisations.
2. L'acheminement inter domaine sans classe (CIDR, *Classless Interdomain Routing*), le chevauchement de préfixes, la complexité croissante des politiques d'acheminement, et les besoins d'agrégation, ont introduit de nouvelles exigences.
3. Il y a besoin d'assurer l'intégrité des données et de déléguer l'autorité pour les données qui représentent des ressources allouées spécifiquement à des personnes ou organisations multiples.
4. Il y a besoin d'assurer l'intégrité des données et de répartir la mémorisation des sous-ensembles de données entre plusieurs répertoires.

L'effort RIPE se concentre spécifiquement sur le premier problème et les besoins de la communauté européenne. Son prédécesseur, le PRDB, visait les besoins d'une seule organisation, le NSF. Les formats de la base de données RIPE tels que décrits dans la [RFC1786] étaient à la base de l'IRR d'origine.

Les protocoles d'acheminement eux-mêmes ne donnent pas d'assurance que l'origine d'un chemin est légitime et peut

réellement atteindre la destination déclarée. La nature de CIDR permet que des préfixes plus spécifiques outrepassent des préfixes moins spécifiques [RFC1517], [RFC1518], [RFC1519]. Même avec une origine signée du chemin, il n'y a pas de moyen pour déterminer si un préfixe plus spécifique est légitime et devrait outrepasser un chemin moins spécifique annoncé sans un moyen pour déterminer qui est autorisé à annoncer des préfixes spécifiques. Manquer à le faire ne donne aucune assurance d'intégrité des informations d'acheminement globales et laisse une opportunité pour une forme très efficace d'attaque de déni de service.

Le langage de système de politique d'acheminement (RPSL, *Routing Policy System Language*) [RFC2280], [RFC2650] était une étape très importante de l'évolution de la représentation des données qui était largement dirigée vers le traitement du second groupe de besoins. Le PRDB améliorait le CIDR en 1993 [RFC1482] et la base de données RIPE permettait l'entrée de préfixes de CIDR depuis le début, mais RPSL fournit de nombreuses améliorations nécessaires qui incluent la prise en charge explicite de l'agrégation.

Le présent document vise le troisième groupe des besoins identifiés ci-dessus.

Alors que la mise en œuvre actuelle qui accepte une authentification faible ne garantit pas l'intégrité des données, elle fournit de nombreux mécanismes pour s'assurer que toutes les parties impliquées sont notifiées des changements faits à la base de données, que le changement soit malveillant ou prévu. Cela fournit une protection inadéquate contre les ajouts. Comme le logiciel est de plus en plus utilisé pour configurer les parties majeures de l'infrastructure de l'Internet, il n'est pas considéré qu'il soit encore adéquat de connaître les changements indésirables et d'avoir la capacité de les effacer. Des mécanismes de sécurité plus actifs doivent donc être développés pour empêcher de tels problème avant qu'ils surviennent.

Un document distinct sera nécessaire pour traiter du quatrième groupe de besoins.

3. Hypothèses implicites de politique

Le modèle d'autorisation code certaines politiques pour l'allocation des numéros d'adresse, des numéros d'AS, et pour les annonces des chemins. Un petit nombre limité d'hypothèses de politiques sont implicites du modèle d'autorisation.

1. Les numéros d'adresse sont alloués de façon hiérarchisée. L'IANA délègue des portions de l'espace d'adresse aux registraires régionaux (actuellement ARIN, APNIC et RIPE) qui à leur tour délèguent l'espace d'adresses à leurs membres, qui peuvent allouer les adresses à leurs clients.
2. Les numéros d'AS sont alloués soit individuellement, soit en petits blocs par les registraires. Des blocs de numéros d'AS sont alloués aux registraires, et ainsi l'allocation est hiérarchisée.
3. Les chemins ne devraient être annoncés qu'avec le consentement du détenteur du numéro d'AS d'origine de l'annonce, et avec le consentement du détenteur de l'espace d'adresse.
4. Les registraires de numéros d'AS et d'adresses IP peuvent être des entités différentes des registraires d'acheminement.

Pour les sous-ensembles d'un de ces trois espaces d'allocation, adresses réseau, numéros d'AS, et chemins, ces restrictions peuvent être assouplies ou désactivées en spécifiant une méthode d'autorisation très faible ou une méthode d'authentification de "aucune". Cependant, même quand aucun mécanisme d'authentification n'est utilisé, toutes les parties impliquées peuvent avoir notification des changements qui sont survenus grâce à l'utilisation de l'attribut existant "notify".

4. Portée de la couverture de sécurité

Le présent document est destiné seulement à fournir un modèle d'authentification et d'autorisation pour s'assurer de l'intégrité des données de politique dans un registre. Seules l'authentification et l'autorisation des ajouts, suppressions, et changements dans la base de données sont couverts par le présent document. L'authentification et l'autorisation des interrogations de la base de données sont explicitement hors de son domaine d'application. L'authentification mutuelle des interrogations, c'est-à-dire l'authentification de l'origine de l'interrogation et du répertoire à partir duquel les résultats de l'interrogation sont obtenus, est aussi en dehors de ce domaine.

5. Organisation du document

On suppose, tout au long de ce document, que le lecteur est familiarisé avec RIPE-181 [RFC1786] et RPSL [RFC2280]. Les buts sont décrits à la Section 6. Les sections 7 à 9 donnent les descriptions des changements et les discutent. La Section 10 donne un bref résumé des formats et de la sémantique des données. Les appendices C à E donnent une discussion technique supplémentaire, des exemples, et des considérations sur le déploiement.

La Section 6 sur les buts et exigences donne une description plus détaillée des questions et identifie des problèmes spécifiques qui doivent être résolus, dont plusieurs exigent un certain degré de coopération dans la communauté de l'Internet.

La Section 7 sur la représentation des données fournit les caractéristiques de RPSL et les formats pour les représentations externes des informations.

La Section 8 sur le modèle d'authentification décrit les pratiques courantes, propose des méthodes d'authentification supplémentaires, et décrit les mécanismes d'extension si des méthodes supplémentaires sont nécessaires à l'avenir.

La Section 9 sur le modèle d'autorisation décrit les moyens pour déterminer si une transaction contient l'autorisation nécessaire pour ajouter, modifier, ou supprimer des objets de données spécifiques, sur la base des exigences d'authentification déclarées dans les objets de données en question.

La Section 10 sur les résumés des formats de données donne des référence concises aux formats des données et aux étapes du traitement des transactions.

La Section C sur la discussion technique contient une discussion des compromis techniques.

La Section D donne des exemples tirés des expériences de fonctionnement passé avec l'IRR.

La Section E décrit des questions de déploiement et discute des moyens de résolution possibles.

6. Buts et exigences

L'Internet est un réseau ouvert. Cette ouverture et la grande échelle de l'Internet peuvent présenter des problèmes de fonctionnement. Les faiblesses techniques qui permettent que de mauvaises configurations ou un fonctionnement erratique dans des parties du réseau se propagent au monde entier ou qui permettent potentiellement de simples attaques de déni de service devraient être éliminées dans la mesure du possible. L'intégrité des informations d'acheminement est critique pour assurer que le trafic va où il est supposé aller.

Un mauvaise configuration accidentelle peut diriger le trafic vers des routeurs qui ne peuvent pas atteindre une destination pour laquelle ils ont annoncé l'accessibilité. Cela est couramment causé par des chemins statiques mal configurés bien qu'il y ait de nombreuses autres causes potentielles. Les chemins statiques sont souvent utilisés pour fournir une accessibilité apparente constante à des destinations à un seul rattachement. Certains des plus grands fournisseurs d'accès Internet (FAI) ont littéralement des milliers de chemins statiques dans leurs réseaux. Ils sont souvent entrés manuellement par les opérateurs. Une faute de frappe peut détourner du trafic d'une destination complètement sans rapport vers un routeur qui n'a pas d'accès réel à la destination annoncée. Cela peut arriver et arrive en fait assez régulièrement. De plus, des erreurs de mise en œuvre ou des mauvaises configurations sévères qui résultent en la perte des informations de chemin d'AS BGP ou en une altération de la longueur du préfixe peuvent résulter en l'annonce de grands ensembles de chemins. Bien que considérablement plus rare, en quelques occasions où cela est arrivé, les résultats ont été catastrophiques.

Lorsque il existe un potentiel de mauvaise configuration accidentelle dans une partie éloignée de l'Internet qui affecte l'Internet global, il y a aussi un potentiel pour la malveillance. Par exemple, il a été démontré accidentellement qu'une panne de plusieurs heures sur une institution majeure peut être causée par un ordinateur portable et un compte téléphonique si les précautions appropriées ne sont pas prises. Le compte téléphonique n'a pas besoin d'être chez le même fournisseur que celui utilisé par l'institution majeure.

Le potentiel d'erreur est augmenté par la préférence de CIDR pour les chemins plus spécifiques [RFC1519]. Si une institution annonce un seul chemin d'une certaine longueur et si un routeur distant annonce un chemin plus spécifique couvrant les hôtes critiques, le chemin plus spécifique, si il est accepté, est préféré sans aucune considération de pondération administrative ou de tous attributs de protocole d'acheminement.

Il est nécessaire de fournir une forme de vérification de la validité de l'annonce de chemin. Les vérifications d'aujourd'hui sont normalement faites à l'égard de l'AS frontière qui annonce le chemin. Cela empêche d'accepter des chemins provenant de l'ensemble d'AS de bordure qui pourraient ne pas annoncer légitimement le chemin. Ces vérifications s'appuient sur l'utilisation des informations enregistrées dans l'IRR pour générer les listes de préfixes qui pourraient être annoncées par un AS bordure spécifique. Les vérifications peuvent aussi être faites à l'égard de l'AS d'origine. Si les informations de politique étaient suffisamment remplies, des vérifications pourraient être faites à l'égard du chemin d'AS entier, mais ce n'est pas encore faisable.

L'utilisation d'un registre des acheminements peut aussi rendre plus difficile d'utiliser les préfixes sans autorisation comme le sont les préfixes non alloués ou les préfixes alloués à d'autres personnes.

En résumé, les problèmes visés sont :
- o de localiser l'impact d'une mauvaise configuration accidentelle faite par des fournisseurs Internet pour le seul réseau de ce fournisseur ;
- o d'éliminer la possibilité qu'un client d'un fournisseur Internet utilise une mauvaise configuration malveillante de l'acheminement comme attaque de déni de service si le chemin du fournisseur filtre ses clients. De localiser le déni de service chez ce fournisseur Internet seulement si le fournisseur de service Internet immédiat ne filtre pas le chemin de ses clients mais que d'autres fournisseurs filtrent le chemin dans l'échange de chemins au point d'échange inter fournisseurs ;
- o d'éliminer les utilisations non autorisées de l'espace d'adresses.

Si les données sont critiques au sein d'un registre d'acheminement, la capacité à changer les données doit alors être contrôlée. Des autorités centralisées peuvent fournir le contrôle mais la centralisation peut conduire à des problèmes d'échelle (et n'est pas politiquement correcte).

L'allocation d'adresse et de nom est déjà déléguée. Comme la délégation peut être en dehors des registraires, elle est au moins un peu répartie [RFC2050]. Les numéros de systèmes autonomes (AS, *Autonomous System*) sont alloués par les mêmes autorités. Il y a un sens à déléguer l'espace des numéros d'acheminement d'une manière similaire à celle des allocations d'adresse et de numéro d'AS. La nécessité de cette délégation d'autorité à de nombreux registraires augmente la difficulté de maintenir l'intégrité du corps des informations dans sa totalité.

En premier lieu, la base de données peut être administrée plus ou moins centralement, avec l'autorité accordée à de nombreuses parties pour changer les informations. C'est le cas avec l'IRR actuel. Il y a un très petit nombre de répertoires de confiance et un très grand nombre de parties autorisées à faire les changements. Le contrôle doit être exercé sur qui peut faire les changements et quels changements ils peuvent faire. La distinction entre qui et quoi sépare l'authentification de l'autorisation.
- o L'authentification est le moyen de déterminer qui tente de faire un changement.
- o L'autorisation est la détermination de si une transaction qui passe une vérification d'authentification spécifique est autorisée à effectuer une certaine opération.

Différentes portions de la base de données vont requérir des méthodes différentes d'authentification. Certaines applications vont exiger une authentification fondée sur un chiffrement fort. Dans d'autres cas, le logiciel qui prend en charge le chiffrement fort peut n'être pas nécessaire ou peut n'être pas légalement disponible. C'est pour cette raison que plusieurs méthodes d'authentification doivent être prises en charge, choisies sur la base de l'objet à travers la spécification des méthodes d'authentification dans l'attribut d'objet "auth" du mainteneur. Les méthodes d'authentification peuvent aller de la très faible vérification d'intégrité des données à des signatures cryptographiquement fortes. Le modèle d'autorisation doit être sûr que l'utilisation de vérifications d'intégrité faibles dans des parties de la base de donnés ne compromet pas l'intégrité globale de la base de données.

Des exigences supplémentaires s'imposent au modèle d'autorisation si la base de données est largement répartie avec des délégations faites à des parties qui peuvent n'être pas dignes de confiance ou dont la pratique de sécurité peut présenter des faiblesses. Ce problème doit être traité dans le modèle d'autorisation afin de permettre une évolution ultérieure vers un registre d'acheminement plus réparti.

Les numéros de système autonome peuvent être délégués en blocs et subdélégués en tant que de besoin, et ensuite les numéros d'AS individuels sont alloués. L'allocation des adresses est une simple hiérarchie numérique. L'allocation de chemin est un peu plus compliquée. Les attributs clés dans un objet route (clé par rapport à son unicité) contiennent à la fois un préfixe d'adresse et un numéro d'AS, appelé l'AS d'origine. L'ajout d'un objet route doit être validé par rapport aux critères d'autorisation à la fois pour l'AS et pour le préfixe d'adresse. Les objets route peuvent exister pour le même préfixe avec plusieurs valeurs d'AS d'origine à cause de la pratique courante du multi rattachement qui n'exige pas un AS d'origine unique. Il n'y a souvent pas de corrélation entre l'AS d'origine d'un préfixe et l'AS d'origine des préfixes plus spécifiques qui le chevauchent.

On doit s'accommoder de nombreux cas de fonctionnement. Certains des plus courants sont énumérés ci-dessous. Ils sont examinés plus en détails dans l'Appendice D avec la discussion des compromis techniques dans l'Appendice C.
- o allocation simple d'adresse hiérarchique et de chemin
- o agrégation et chemins multi rattachement plus spécifiques
- o adresses indépendantes du fournisseur et AS d'origine multiples
- o fournisseurs de service Internet changeants
- o périodes de grâce de dénumérotage

Le modèle d'autorisation doit s'accommoder de diverses politiques concernant l'allocation de l'espace d'adresses et ne peut rendre obligatoire l'utilisation d'un seul modèle. Il n'y a pas de normalisation des politiques d'allocation d'adresse bien qu'il existe des lignes directrices [RFC2008], [RFC2050]. On doit pouvoir choisir objet par objet si l'autorisation permet la récupération de l'espace d'adresses et cela peut différer entre les parties de la base de données. Cette question est discutée plus avant dans l'Appendice C.

7. Représentation des données

RPSL donne une description complète des contenus d'un répertoire d'acheminement [RFC2280]. De nombreux objets de données RPSL restent inchangés par rapport aux spécifications RIPE et RPSL fait référence à la spécification RIPE-181 telle que mentionnée dans la [RFC1786]. RPSL donne une représentation des données externes. Les données peuvent être mémorisées différemment en interne dans un registre d'acheminement.

Certains types d'objet ou attributs de la base de données doivent être ajoutés au RPSL pour enregistrer la délégation d'autorité et améliorer les mécanismes d'authentification et d'autorisation. Ces ajouts sont très minimes et sont décrits aux sections 8 et 9.

Une certaine forme d'encapsulation doit être utilisée pour échanger les données. L'encapsulation de fait a été celle qu'acceptent les outils RIPE, un fichier de texte en clair ou du texte en clair dans le corps d'un message électronique dans le format de la RFC-822 avec les informations nécessaires pour l'authentification déduites des en-têtes du message ou du corps du message. Merit a légèrement modifié cela en utilisant la portion signée PGP d'un fichier de texte en clair ou la portion signée PGP du corps d'un message électronique. Ces formes très simples d'encapsulation conviennent pour la soumission initiale d'une transaction de la base de données.

L'encapsulation des soumissions de transactions du registre, d'interrogations et de réponses du registre, et des échanges entre les registraires, sortent du domaine d'application du présent document. L'encapsulation des soumissions de transaction du registre et des échanges entre les registraires sort du domaine d'application du présent document.

8. Modèle d'authentification

Les objets mainteneurs servent de conteneur pour garder les filtres d'authentification. Une référence à un mainteneur au sein d'un autre objet définit l'autorisation d'effectuer des opérations sur l'objet ou sur un ensemble d'objets en rapport. Le mainteneur est normalement référencé par un nom dans les attributs mnt-by des objets. Plus de détails sur l'utilisation des mainteneurs sont fournis au paragraphe 9.1.

Le mainteneur contient un ou plusieurs attributs "auth". Chaque attribut "auth" commence par un mot clé qui identifie la méthode d'authentification, suivi par les informations d'authentification nécessaires pour appliquer cette méthode. La méthode PGPKEY est légèrement différente syntaxiquement en ce qu'elle est une sous chaîne.

Les méthodes d'authentification actuellement prises en charge incluent ce qui suit. Noter que pgp-from est remplacé par pgpkey (voir la Section 10 et la [RFC2726]).

mail-from : C'est une vérification d'authentification très faible et elle est déconseillée. Les informations d'authentification sont une expression régulière sur des caractères ASCII. Le mainteneur est authentifié si les champs from ou reply-to de l'en-tête de message de la RFC-822 correspondent à cette expression régulière. Comme la falsification de message est assez facile, c'est une forme d'authentification très faible.

crypt-pw : C'est une autre forme faible d'authentification. Les informations d'authentification sont un mot de passe fixe chiffré en format UNIX crypt. Le mainteneur est authentifié si la transaction contient le mot de passe en clair du mainteneur. Comme le mot de passe est en clair dans les transactions, il peut être capturé par espionnage. Comme la forme chiffrée du mot de passe est exposée, elle est soumise à des attaques pour deviner le mot de passe.

pgp-from : Ce format est remplacé par "pgpkey" de sorte que le certificat de clé publique sera disponible pour les répertoires distants. C'est l'extension PGP de Merit. Les informations d'authentification sont une identité de signature pointant sur un anneau de clé publique externe. Le mainteneur est authentifié si la transaction (actuellement la portion PGP signée d'un message électronique) est signée par la clé privée correspondante.

pgpkey : Ce mot clé prend la forme "PGPKEY-hhhhhhhh", où "hhhhhhhh" est la représentation en hexadécimal de l'identifiant de quatre octets de la clé publique PGP utilisée pour l'authentification. Le certificat de clé publique

est mémorisé dans un objet séparé comme décrit dans la [RFC2726].

Les répertoires peuvent choisir d'interdire l'ajout d'attributs "auth" qui spécifient des formes plus faibles d'authentification et/ou d'interdire leur utilisation dans les soumissions de transaction locale. Les répertoires sont invités à interdire l'ajout des attributs "auth" avec la méthode "pgp-from" déconseillée.

Toute technique de signature numérique peut en principe être utilisée pour l'authentification. Les transactions devraient être signées en utilisant plusieurs techniques de signature numérique pour permettre aux répertoires ou miroirs qui n'utilisent qu'un sous ensemble des techniques de vérifier au moins une des signatures. Le choix des techniques de signature numérique sort du domaine d'application du présent document.

9. Modèle d'autorisation

Le modèle d'autorisation doit s'accommoder des exigences mentionnées à la Section 6. Un dispositif clé du modèle d'autorisation est la reconnaissance que l'autorisation pour l'ajout de certains types d'objets de données doit être déduite des objets de données qui s'y rapportent.

Avec plusieurs répertoires, des objets qui ne se trouvent pas dans RPSL sont nécessaires pour contrôler les délégations d'AS et de nouveaux attributs sont nécessaires dans les objets existants pour contrôler la subdélégation. La définition des objets RPSL utilisés pour mettre en œuvre un système de registres d'acheminement réparti sort du domaine d'application du présent document.

9.1 Objets mainteneurs

Les objets mainteneurs servent de conteneur pour garder les filtres d'authentification. Les méthodes d'authentification sont décrites à la Section 8. Le mainteneur peut être référencé par le nom dans d'autres objets, en particulier dans les attributs mnt-by de ces objets.

Les mainteneurs eux-mêmes contiennent des attributs mnt-by. Dans certains cas, le mnt-by dans un mainteneur fera référence au mainteneur lui-même. Dans ce cas, l'autorisation de modifier le mainteneur est fournie à un ensemble (normalement très limité) d'identités. Il est de bonne pratique de créer un mainteneur contenant une longue liste d'identités autorisées à faire des types spécifiques de changements mais ont l'attribut mnt-by du mainteneur qui fait référence à un mainteneur beaucoup plus restrictif qui contrôle plus strictement les changement à l'objet mainteneur lui-même.

L'attribut mnt-by est obligatoire dans tous les objets. Il existe certaines données sans attribut mnt-by. Un attribut mnt-by manquant est interprété comme l'absence de tout contrôle sur les changements. Ceci est fortement déconseillé et la plupart des répertoires ne le permettent plus.

Une référence de mainteneur supplémentaire peut survenir à travers du nouvel attribut, "mnt-routes", et est utilisé dans les objets aut-num, inetnum et route. L'attribut "mnt-routes" est une extension à RPSL et est décrit en détail à la Section 10.

Un attribut mnt-routes dans un objet aut-num permet l'ajout d'objets route avec ce numéro d'AS comme origine des mainteneurs énumérés. Un attribut mnt-routes dans un objet inetnum permet l'ajout d'objets route avec des préfixes de correspondance exacte ou plus spécifiques. Un attribut mnt-routes dans un objet route permet l'ajout d'objets route avec correspondance exacte ou des préfixes plus spécifiques. Un attribut mnt-routes ne permet pas de changement à l'objet aut-num, inetnum, ou route s'il apparaît. Un attribut mnt-routes peut facultativement être restreint à ne s'appliquer qu'à un sous ensemble de chemins plus spécifiques.

Lorsque "mnt-routes" ou "mnt-lower" sont applicables, tout mainteneur référencé dans le "mnt-by" s'applique encore. L'ensemble de mainteneurs applicables pour toute vérification faite est l'union de "mnt-routes" ou "mnt-lower" et de "mnt-by". Par exemple, lorsque on autorise qu'un logiciel d'objet route cherche sur "mnt-routes", si il n'existe pas, cherche à "mnt-lower", si il n'existe pas, cherche à "mnt-by".

9.2 Objets as-block et aut-num

Un objet "as-block" est nécessaire pour déléguer une gamme de numéros d'AS à un certain répertoire. C'est nécessaire pour l'autorisation et aussi pour éviter d'avoir à faire une recherche exhaustive dans tous les répertoires pour trouver un AS spécifique. Cette recherche ne poserait pas de problème aujourd'hui, mais en serait un si on utilise un répertoire d'acheminements plus réparti. Les problèmes de répartition de registre sortent du domaine d'application du présent document.

L'objet "as-block" rend aussi possible de séparer l'allocation des numéros d'AS de l'enregistrement des politiques d'acheminement d'AS.

as-block : AS1321 - AS1335

L'objet "aut-num" décrit la politique d'acheminement pour un AS et est critique pour la configuration du routeur de cet AS et pour l'analyse effectuée par un autre AS. Pour les besoins du présent document, il est suffisant de considérer le aut-num seulement comme un fourre-tout qui identifie l'existence d'un AS et donne le moyen d'associer l'autorisation à cet AS lors de l'ajout d'objets "route".

L'objet "as-block" n'est proposé ici que comme un moyen d'enregistrer la délégation de blocs de numéros d'AS sur d'autres registres et le faisant de donner les moyens d'orienter les interrogations et de prendre en charge le caractère hiérarchique des autorisations à travers plusieurs répertoires.

9.3 Objets inetnum

L'objet "inetnum" existe pour prendre en charge l'allocation d'adresse. Pour les registres de numéros externes, comme ceux qui utilisent "[r]whoisd[++]" l'objet "inet-num" peut servir d'enregistrement secondaire qui est ajouté lorsque est faite une allocation d'adresse dans la base de données d'autorité. De tels enregistrements pourraient être ajoutés par un registraire d'adresses tel que ARIN à titre de service gratuit pour le registraire d'acheminement correspondant.

inetnum : 193.0.0.0 - 193.0.0.255
source : IANA

9.4 Objets route

Il y a actuellement assez peu d'objets route dans plus d'un registre. Assez peu sont enregistrés avec un AS d'origine pour lequel ils n'ont jamais été annoncés. Il y a une raison légitime pour être dans plus d'un AS d'origine.

L'objet "route" est utilisé pour enregistrer les chemins qui peuvent apparaître dans le tableau d'acheminement mondial. La prise en charge explicite de l'agrégation est fournie. Les objets Route existent à la fois pour la configuration des filtres d'informations d'acheminement utilisés pour isoler les incidents d'annonces d'acheminement erronés (Section 6) et pour prendre en charge les diagnostics de problèmes de réseau.

9.5 Attributs reclaim et no-reclaim

Un attribut reclaim est nécessaire dans les objets as-block, inetnum et route. L'attribut reclaim permet de garder un contrôle sur un AS plus spécifique, une adresse IP ou un espace de chemin en permettant de modifier et supprimer des privilèges sans considération du mnt-by dans l'objet lui-même.

L'attribut reclaim donne les moyens de mettre en application le prêt d'adresse. Il permet le nettoyage dans des cas où des entités cessent d'exister ou comme dernier moyen de tri pour corriger des erreurs telles que celles où des parties se ferment elles-mêmes l'accès à leurs propres objets. Pour spécifier tous les objets plus spécifiques, la valeur de l'attribut reclaim devrait être "ALL" *(TOUS)*. Pour permettre un contrôle plus fin, on peut spécifier un ensemble de préfixes.

Un attribut no-reclaim peut être utilisé pour fournir des exceptions explicites. Un attribut reclaim ne peut être ajouté à un objet existant que si l'ajout de attribut reclaim ne supprime pas l'autonomie des objets plus spécifiques existants qui sont couverts par le nouvel attribut reclaim.

1. Un attribut reclaim peut être ajouté à un objet existant si il n'existe pas de correspondance exacte ou si des objets plus spécifiques se chevauchent avec le nouvel attribut reclaim, ou

2. si le soumettant figure sur la liste de mainteneur pointée par le mnt-by des objets qui sont chevauchés, ou

3. si un objet chevauché figure sur la liste d'un attribut no-reclaim dans l'objet où le reclaim est ajouté.

De façon similaire, un soumettant ne peut supprimer un attribut no-reclaim d'un objet que lorsque ce soumettant est le seul mainteneur cité dans les attributs mnt-by d'un objet chevauché. Si le soumettant n'est pas cité comme un des mainteneurs pointés par l'attribut mnt-by pour un ou plusieurs objets chevauchés, il n'est alors pas permis au soumettant de supprimer l'attribut no-reclaim.

Si ni l'attribut reclaim ni l'attribut no-reclaim ne sont présents, les objets plus spécifiques d'un certain objet ne peuvent alors pas être modifiés par le mainteneur de l'objet moins spécifique sauf si le mainteneur est aussi cité comme mainteneur dans l'objet plus spécifique. Cependant, l'ajout d'un nouvel objet route ou inetnum doit réussir l'authentification du plus grand préfixe moins spécifique au titre de la vérification d'authentification décrite au paragraphe 9.9.

Voir à la Section 10 la description complète des attributs reclaim et no-reclaim.

9.6 Autres objets

Beaucoup des objets RPSL auxiliaires n'ont pas de hiérarchie naturelle comme les numéros d'AS, les adresses Internet et les chemins qui ont une hiérarchie numérique. Quelques exemples sont les objets "mainteneurs", "personnes" et "rôle". Pour ces objets, l'absence de hiérarchie induit deux problèmes.

1. Il n'y a pas de hiérarchie qui puisse être exploitée pour diriger les interrogations sur d'autres registres. À un certain point, la stratégie d'interrogation consistant à chercher tous les registres connus devient impraticable.
2. Il n'y a pas de hiérarchie sur laquelle l'autorisation des ajouts puisse se fonder.

Le premier problème peut être réglé en considérant l'espace de noms pour chacun des objets auxiliaires comme n'étant unique qu'au sein de la base de données locale et en utilisant des références explicites à un répertoire externe lorsque nécessaire. Pour spécifier une référence de répertoire externe, la clé d'objet est précédée du nom du répertoire et du délimiteur "::". Par exemple, une bretelle NIC peut prendre la forme "RIPE::CO19". Il y a actuellement le désir de garder les bretelles NIC univoques, de sorte qu'on utilisera la convention de dénomination d'ajouter un tiret et le nom du répertoire. Ajouter devant le nom du répertoire fournit un espace de nom unique car un objet dans la base de données RIPE faisant référence à "CO19" serait interprété comme "RIPE::CO19" par défaut, mais il serait encore possible d'interroger ou de faire référence à "IANA::CO19". Il n'est absolument pas possible d'oublier accidentellement d'adhérer aux conventions lors d'un ajout et on s'accommode des objets existants, y compris les cas où des conflits de noms se sont déjà produits.

Le second problème peut être partiellement réglé en utilisant un système de référents pour l'ajout des mainteneurs et en exigeant que tout autre objet soit soumis par un mainteneur enregistré par l'IANA. Le système de référents permettrait à tout mainteneur existant d'ajouter un autre mainteneur. Cela peut être utilisé en parallèle avec l'ajout d'autres types d'objets pour prendre en charge la maintenance de ces objets. Par exemple, lors de l'ajout d'un sous domaine à la hiérarchie de "domaine" (dans le répertoire RIPE où les domaines sont aussi traités) même lors de l'ajout d'un nouveau domaine à un domaine relativement plat tel que "com", il y a déjà un mainteneur pour le domaine existant. Le mainteneur existant peut ajouter le mainteneur qui sera nécessaire pour le nouveau domaine en plus de l'ajout du nouveau domaine, et donner au nouveau mainteneur le droit de le modifier.

Une organisation qui se trouve présente pour la première dois sur l'Internet va recevoir un mainteneur. Ce mainteneur peut faire une liste d'un petit nombre d'employés de confiance qui sont autorisés à modifier le mainteneur lui-même. L'organisation peut alors ajouter elle-même un autre mainteneur faisant une liste d'un plus grand ensemble des employés mais énumérant les mainteneurs plus restreints dans les attributs mnt-by des mainteneurs eux-mêmes. L'organisation peut alors ajouter des gens et des objets rôle en tant que de besoin et tous autres objets nécessaires et comme l'autorisation le permet.

9.7 Objets avec des noms d'AS hiérarchiques

De nombreux objets RPSL n'ont pas une hiérarchie naturelle en propre mais permettent une hiérarchie de noms. Des exemples en sont les types d'objet "as-set" et "route-set". Un as-set peut avoir un nom ne correspondant à aucune hiérarchie de dénomination comme "AS-Foo" ou il peut avoir un nom hiérarchisé de la forme "AS1:AS-Bar".

Lorsque on utilise pas un nom hiérarchique, l'autorisation pour des objets tels que "as-set" et "route-set" correspond aux règles pour les objets sans hiérarchie décrits au paragraphe 9.6.

Si des noms hiérarchisés sont utilisés, l'ajout d'un objet doit alors être autorisé par le aut-num dont la clé est désignée par quelque chose à gauche de la colonne de droite du nom de l'objet ajouté. L'autorisation est déterminée d'abord en utilisant la référence du mainteneur mnt-lower, ou si elle est absente, en utilisant la référence mnt-by.

9.8 Traitement de l'interrogation

Une interrogation peut devoir s'étendre sur plusieurs répertoires. Toutes les interrogations devraient être dirigées vers un répertoire local qui peut refléter le répertoire racine et les autres répertoires. Actuellement, chaque répertoire IRR reflète tous les autres répertoires. De cette façon, il peut être répondu à l'interrogation par le répertoire local mais qui tire les données des autres répertoires.

Lorsque il est appliqué à plusieurs répertoires, le mécanisme ci-dessous suppose l'existence d'un attribut pour la traversée des répertoires. La définition de cet attribut est considérée comme un problème de répartition des registres et sort du domaine d'application du présent document.

Pour les types d'objets qui ont une hiérarchie naturelle, tels que aut-num, inet-num, et route, la recherche commence à la base de données racine et suit la hiérarchie. Pour les types d'objets qui n'ont pas de hiérarchie naturelle, comme les objets mainteneur, personne, et rôle, la recherche est confinée à une base de données par défaut sauf si une base de données est spécifiée. La base de données par défaut est la même que celle d'un objet dont il est fait référence si l'interrogation est lancée par le besoin de suivre une référence. Autrement, la base de données par défaut est généralement la base de données locale ou celle établie par défaut par le répertoire. La base de données par défaut peut être spécifiée dans l'interrogation elle-même comme décrit au paragraphe 9.7.

En l'absence d'un attribut pour traverser plusieurs registres, une recherche de tous les répertoires est nécessaire. Avec de tels attributs, la recherche se déroulerait comme suit. En cherchant un AS, on peut consulter l'attribut de délégation dans les blocs d'AS, pour déplacer la recherche vers les données des autres répertoires. L'AS est finalement trouvé ou bien la recherche échoue. La recherche d'un inetnum est similaire. Les inetnum moins spécifiques peuvent renvoyer la recherche sur d'autres bases de données. Finalement, le inetnum le plus spécifique est trouvé et son statut (alloué ou non alloué) peut être déterminé. La définition des attributs pour la traversée des répertoires est considérée comme un problème de répartition des registres et sort du domaine d'application du présent document.

La recherche d'un chemin en présence d'attributs pour la traversée de plusieurs registres est similaire sauf que la recherche peut déboucher sur plus d'un répertoire. Le chemin le plus spécifique dans un répertoire peut être plus spécifique que le plus spécifique d'un autre. En cherchant un objet route, il peut y avoir du sens à retourner le chemin le plus spécifique qui soit plus spécifique que ne le demande l'interrogation sans considération du répertoire qui contient ce chemin plutôt que de retourner un chemin de chaque répertoire qui contient un chemin chevauchant moins spécifique.

9.9 Ajout à la base de données

Lorsque il est appliqué à plusieurs répertoires, le mécanisme suivant suppose l'existence d'un attribut pour la traversée des répertoires. La définition de cet attribut est considérée comme un problème de répartition de registre et sort du domaine d'application du présent document.

Le répertoire racine doit être rempli initialement à une certaine époque avec quelques entrées. Un mainteneur initial est nécessaire pour ajouter d'autres mainteneurs. L'attribut referral-by peut être réglé à se référer à lui-même dans ce cas particulier (la Section 10 décrit referral-by). Lors de l'ajout d'un inetnum ou d'un objet route, il doit exister une correspondance exacte ou un chevauchement moins spécifique. Un objet route peut être ajouté sur la base d'une correspondance exacte ou d'un inetnum moins spécifique. Le répertoire racine doit être initialement rempli avec l'allocation d'un inetnum couvrant le préfixe 0/0, indiquant qu'il existe une certaine autorité d'allocation d'adresse. De la même façon, un as-block initial est nécessaire pour couvrir la gamme complète des numéros d'AS.

Lors de l'ajout d'un objet sans hiérarchie naturelle, la recherche d'un objet existant suit la procédure mentionnée au paragraphe 9.8.

Lors de l'ajout d'un aut-num (un AS) on utilise la même procédure que dans une interrogation pour déterminer le répertoire approprié pour l'ajout et pour déterminer quel mainteneur s'applique. La séquence d'objets AS-block et de délégations de répertoires est suivie. Si le aut-num n'existe pas, la soumission doit alors correspondre à l'authentification spécifiée dans le mainteneur pour le AS-block le plus spécifique afin d'être ajouté.

La procédure pour ajouter un inetnum est similaire. La séquence de blocs inet-num est suivie jusqu'à ce que le plus spécifique soit trouvé. La soumission doit correspondre à l'authentification spécifiée dans le mainteneur pour le inetnum le plus spécifique chevauchant l'ajout.

Ajouter un objet route est un peu plus compliqué. La soumission de l'objet route doit satisfaire à deux critères d'authentification. Elle doit correspondre à l'authentification spécifiée dans le aut-num et à l'authentification spécifiée soit dans un objet route, soit à un inetnum si aucun objet route applicable n'est trouvé.

Un ajout est soumis avec un numéro d'AS et un préfixe comme sa clé. Si l'objet existe déjà, la soumission est alors traitée comme une modification (voir le paragraphe 9.10). Si le aut-num n'existe pas sur un ajout de chemin, l'ajout est alors rejeté (voir à la Section C la discussion des compromis). Si le aut-num existe, la soumission est alors vérifiée par rapport au mainteneur applicable. Une recherche est alors faite sur le préfixe pour trouver d'abord une correspondance exacte. Si la recherche de correspondance exacte échoue, une recherche est faite sur la correspondance de plus long préfixe qui soit moins spécifique que le préfixe spécifié. Si cette recherche réussit, elle va retourner un ou plusieurs objets route. La

soumission doit correspondre à un mainteneur applicable dans au moins un de ces objets route pour que l'ajout réussisse. Si la recherche d'un objet route échoue, une recherche est alors effectuée sur un inetnum qui corresponde exactement au préfixe ou à l'inetnum le plus spécifique qui soit moins spécifique que la soumission d'objet route. La recherche d'un inetnum ne devrait jamais échouer mais elle peut retourner une gamme non allouée ou réservée. L'état de l'inetnum doit être "alloué" et la soumission doit correspondre au mainteneur.

Ayant trouvé un AS et soit un objet route, soit un inetnum, l'autorisation est tirée de ces deux objets. L'objet mainteneur applicable est tout objet référencé par les attributs mnt-routes. Si un ou plusieurs attributs mnt-routes sont présents dans un objet, les attributs mnt-by ne sont pas pris en compte. En l'absence d'un attribut mnt-routes dans un objet, les attributs mnt- sont utilisés pour cet objet. L'authentification doit correspondre à une de celle des autorisations dans chacun des deux objets.

Si l'ajout d'un objet route ou d'un inetnum contient un attribut reclaim, tout objet plus spécifique du même type doit alors être examiné. L'attribut reclaim ne peut être ajouté que si il n'y a pas de chevauchement plus spécifique ou si l'authentification sur l'ajout est présente dans l'autorisation d'un objet moins spécifique dont un attribut reclaim couvre la gamme de préfixes, ou si l'authentification sur l'ajout est autorisée pour la modification de tous les préfixes plus spécifiques existant couverts par l'ajout.

9.10 Modification ou suppression d'objets de la base de données

Lors de la modification ou suppression de tout objet existant, on effectue une recherche sur l'objet comme décrit au paragraphe 9.8. Si la soumission correspond à un mainteneur applicable pour l'objet, l'opération peut alors se faire. Un mainteneur applicable pour une modification est tout mainteneur référencé par l'attribut mnt-by dans l'objet. Pour les objets route et inet-num, un mainteneur applicable peut être cité dans un objet moins spécifique avec un attribut reclaim.

Si la soumission est pour un objet route, une recherche est faite sur tous les objets route et inetnum moins spécifiques. Si la soumission est pour un inetnum, une recherche est faite pour tous les inetnum moins spécifiques. Si la soumission échoue à l'autorisation dans l'objet lui-même mais correspond à l'attribut reclaim dans un des objets moins spécifiques, l'opération peut alors se faire. La Section C contient une discussion des raisons de l'utilisation de l'attribut reclaim.

Une modification d'un objet inetnum qui ajoute un attribut reclaim ou retire un attribut no-reclaim doit être vérifiée par rapport à tous les inetnum existants qui sont plus spécifiques. On doit faire la même vérification de l'attribut reclaim que celle faite lors d'un ajout lorsque un attribut reclaim est ajouté par une modification (voir au paragraphe 9.9).

Une suppression est considérée comme un cas particulier de l'opération modify. L'objet supprimé peut rester dans la base de données avec un attribut "supprimé", auquel cas le mnt-by peut toujours être consulté pour retirer l'attribut "supprimé".

10. Résumés du format des données

Les données RIPE-181 [RFC1786] et RPSL [RFC2280] sont représentées en externe comme du texte ASCII. Les objets consistent en un ensemble d'attributs. Les attributs sont des paires [nom valeur]. Un seul attribut est représenté comme une seule ligne avec le nom suivi par deux-points suivi par des caractères d'espace (espace, tabulation, ou continuation de ligne) et suivi par la valeur. Au sein d'une valeur, toute espace est équivalente à une seule espace. La continuation de ligne est prise en charge par une barre oblique inverse à la fin de la ligne ou par la ligne suivante qui commence par une espace. Lorsque ils sont transférés, les attributs externes sont généralement cassés en lignes plus courtes en utilisant la continuation de ligne, bien que ce ne soit pas une exigence. Un objet est représenté en externe comme une série d'attributs. Les objets sont séparés par des lignes blanches.

Il y a environ 80 types d'attribut dans le schéma RIPE actuel et environ 15 types d'objets. Certains des attributs sont obligatoires dans certains objets. Certains attributs peuvent apparaître plusieurs fois. Un ou plusieurs attributs peuvent former une clé. Il peut être exigé de certains attributs ou ensembles d'attributs qu'ils soient uniques sur tous les répertoires. Certains des attributs peuvent faire référence à un champ clé dans un type d'objet et il peut être exigé qu'ils soient une référence valide. Certains attributs peuvent être utilisés dans des recherches inverses.

Un passage en revue du schéma RIPE ou RPSL tout entier serait trop long pour qu'il soit inclus ici. Seules les différences du schéma sont décrites.

10.1 Changements au schéma RIPE/RPSL

Un nouveau type d'objet et plusieurs attributs sont ajoutés au schéma RIPE/RPSL. Il y a des changements significatifs aux règles qui déterminent si l'ajout d'un objet est autorisé.

Le nouveau type d'objet est indique ci-dessous. Le premier attribut indiqué est l'attribut clé et sert aussi comme nom du type d'objet.

as-block	clé	obligatoire	seul	unique
descr	facultatif	multiple		
remarks	facultatif	multiple		
admin-c	obligatoire	multiple		
tech-c	obligatoire	multiple		
notify	facultatif	multiple		
mnt-by	obligatoire	multiple		
changed	obligatoire	multiple		
source	obligatoire	seul		

Dans le type d'objet ci-dessus, seul l'attribut clé "as-block" est nouveau :

as-block : Cet attribut fournit la gamme de numéros d'AS pour un objet "as-block". Le format est deux numéros d'AS incluant la sous-chaîne "AS" séparée par un délimiteur "-" et une espace facultative avant et après le délimiteur.

Afin de prendre en charge une authentification plus forte, les mots clés suivants sont ajoutés à l'attribut "auth" :

pgp-from : Le reste de l'attribut donne la chaîne qui identifie une identité PGP dont la clé publique est détenue dans un anneau de clés externe. L'utilisation de cette méthode est déconseillées en faveur de la méthode "pgpkey".

pgpkey : Voir la [RFC2726].

Pour désactiver l'authentification et donner la permission à tout le monde, la méthode d'authentification "none" est ajoutée. Elle n'a pas d'argument.

Un changement supplémentaire est qu'il est permis à l'attribut "auth" d'exister dans un objet "person" ou "role". La méthode "auth" "role" ou "person" peut être utilisée pour se référer à un objet rôle ou personne et prendre le champ "auth" dans ces objets. Les mises en œuvre doivent veiller à détecter les références en boucle et à terminer une expansion ou les références déjà visitées.

Quelques attributs sont ajoutés au schéma. Ce sont :

mnt-routes : L'attribut mnt-routes peut apparaître dans un objet aut-num, inet-num, ou route. Cet attribut fait référence à un objet mainteneur qui est utilisé pour déterminer l'autorisation d'ajout des objets route. Après la référence au mainteneur peut suivre une liste facultative de gammes de préfixes (comme défini dans RPSL) entre des accolades ou le mot clé "ANY". Lorsque aucun élément supplémentaire n'est spécifié, on a par défaut "ANY" ou tous les plus spécifiques. L'attribut mnt-routes est facultatif et multiple. Voir les détails de l'utilisation au paragraphe 9.1.

mnt-lower : L'attribut mnt-lower peut apparaître dans un objet inetnum, route, as-block ou aut-num. Cet attribut fait référence à un objet mainteneur. Lorsque il est utilisé dans un objet inetnum ou route, son effet est le même que celui d'un "mnt-routes" mais ne s'applique qu'aux préfixes plus spécifiques que le préfixe de l'objet dans lequel il est contenu. Dans un objet as-block, mnt-lower permet l'ajout d'objets as-block ou aut-num plus spécifiques. Dans un objet aut-num, l'attribut mnt-lower spécifie un mainteneur qui peut être utilisé pour ajouter des objets avec des noms hiérarchisés comme décrit au paragraphe 9.7.

reclaim : L'attribut reclaim peut apparaître dans un objet as-block, aut-num, inet-num, ou route. Tout objet du même type à un rang inférieur de la hiérarchie peut être modifié ou supprimé par le mainteneur de l'objet contenant un attribut reclaim. La valeur de l'attribut est un ensemble ou une gamme d'objets de même type où la syntaxe de l'ensemble ou gamme est définie dans RPSL. Voir au paragraphe 9.5 les restrictions à l'ajout des attributs reclaim.

no-reclaim : L'attribut no-reclaim est utilisé avec l'attribut reclaim. L'attribut no-reclaim a un effet négatif sur tout attribut reclaim qu'il chevauche. Voir au paragraphe 9.5 les restrictions à la suppression des attributs no-reclaim.

referral-by : Cet attribut est exigé dans l'objet mainteneur. Il ne peut jamais être altéré après l'ajout du mainteneur. Cet attribut se réfère au mainteneur qui a créé ce mainteneur. Il peut être multiple si plus d'une signature apparaît dans la transaction qui crée l'objet.

auth-override : Un attribut auth-override peut être ajouté, supprimé ou changé par une transaction soumise par le

mainteneur cité dans le referral-by. Un auth-override ne peut être ajouté à un mainteneur que si ce mainteneur a été inactif pendant les 60 jours précédents. L'attribut auth-override lui-même contient seulement la date à laquelle l'attribut va faire effet et qui doit être au moins 60 jours après la date en cours sauf si il y a déjà l'autorisation de modifier le mainteneur. Lorsque la date du auth-override est atteinte, ceux qui sont identifiés par le mainteneur dans le referral-by ont l'autorisation de modifier le mainteneur. Cet attribut existe comme moyen de nettoyage si le détenteur d'un mainteneur ne répond plus et ne peut prendre effet que si ce mainteneur ne retire pas le auth-override en réponse à la notification automatique qui se produit lors des changements.

L'attribut existant "mnt-by" fait références au type d'objet "maintainer". L'attribut "mnt-by" est maintenant obligatoire dans tous les types d'objets. Un nouveau mainteneur peut être ajouté par tout mainteneur existant. L'attribut "referral-by" est maintenant obligatoire dans l'objet "maintainer" pour garder une trace du mainteneur qui a fait l'ajout et ne peut jamais être changé. Les mainteneurs ne peuvent pas être supprimés tant qu'ils sont référencés ailleurs par un attribut "referral-by".

A. Fonctionnalité centrale et non centrale

La plupart des objets et attributs décrits dans le présent document sont essentiels pour le cadre d'autorisation. On dit qu'ils font partie de la fonctionnalité "cœur". Quelques attributs cités ici sont considérés comme "non cœur".

Les attributs "reclaim" et "no-reclaim" sont pratiques pour la souplesse de la mise en œuvre du prêt d'adresse.

L'attribut "auth-override" est pratique pour faciliter la récupération dans un environnement où les données des répertoires sont redistribuées d'une façon ou d'une autre.

L'attribut "referal-by" est un dispositif "cœur". Un registre individuel peut exprimer son autonomie en créant un mainteneur auto référencé, dont le "referal-by" pointe sur lui-même. D'autres registres peuvent décider au cas par cas si ils considèrent comme valide une telle entrée. Un registre peut ne permettre au "referal-by" que de se référer à un mainteneur spécifique sous le contrôle du registre. Cette restriction est un problème purement local pour le registre.

B. Exemples

Les exemples ci-dessous laissent de côté certains attributs exigés qui ne sont pas nécessaires pour illustrer l'utilisation des objets et attributs décrits dans le présent document. Les manquants sont admin-c, tech-c, changed, source. Manquent aussi les attributs comme mnt-nfy, dont l'utilisation est de bonne pratique mais n'est pas strictement requise.

Pour faire quelque chose, il faut un mainteneur. À un certain moment, un seul mainteneur est rempli dans un répertoire et ce mainteneur a un referal-by qui pointe sur lui-même. Toutes les autres références de referal-by peuvent être retracées jusqu'à ce mainteneur. À ce moment, le as-block AS0- AS65535 et le inetnum 0.0.0.0-255.255.255.255 sont aussi alloués. D'autres objets auxiliaires peuvent aussi être nécessaires pour l'amorçage.

```
mntner:      ROOT-MAINTAINER
auth:        pgpkey-12345678

mnt-by:      ROOT-MAINTAINER
referal-by:  ROOT-MAINTAINER
```

Ce mainteneur racine peut ajouter un mainteneur de niveau supérieur pour certaines organisations.

```
mntner:      WIZARDS
descr:       Personnel technique de haut niveau
auth:        pgpkey-23456789
auth:        pgpkey-3456789a
mnt-by:      WIZARDS
referal-by:  ROOT-MAINTAINER
```

Ce mainteneur peut en ajouter un autre qui a des capacités plus limitées.

```
mntner:      MORTALS
descr:       Fait les opérations quotidiennes
auth:        pgpkey-456789ab
```

```
auth:        pgpkey-56789abc
auth:        pgpkey-6789abcd
mnt-by:      WIZARDS
referal-by:  WIZARDS
```

Noter que WIZARDS peut changer son propre objet mainteneur et l'objet mainteneur MORTALS mais que MORTALS ne le peut pas.

À un certain moment un as-block est alloué et cassé. Dans l'exemple ci-dessous, un espace de numéros privé est utilisé.

```
as-block:    AS65500-AS65510
mnt-by:      SOME-REGISTRY
mnt-lower:   WIZARDS
```

Noter qu'un registre a le contrôle sur l'objet qu'il a créé qui représente l'allocation, mais qu'il a donné à la partie à laquelle l'allocation a été faite la capacité de créer des objets plus spécifiques. En dessous de cet as-block, un aut-num est ajouté. Noter que l'importation et l'exportation sont normalement requises pour un aut-num mais on ne les montre pas ici.

```
aut-num:     AS65501
mnt-by:      WIZARDS
mnt-lower:   MORTALS
```

Dans le aut-num ci-dessus, le mainteneur WIZARDS peut modifier le aut-num lui-même. Le mainteneur MORTALS peut ajouter des objets route en utilisant cet AS comme origine si ils ont aussi l'autorisation pour l'espace de numéros IP dans un route ou inetnum moins spécifique.

On a aussi besoin d'une allocation d'inetnum. Dans cet exemple, le inetnum est alloué à une organisation complètement différente. Là encore, des attributs sont omis qui seraient normalement nécessaires dans un inetnum.

```
inetnum:     192.168.144.0-192.168.151.255
mnt-by:      SOME-REGISTRY
mnt-lower:   FAI
reclaim:     ALL
```

Le FAI mainteneur peut ajouter des inetnum ou route plus spécifiques avec son espace d'adresses. Noter que le registraire a déclaré leur capacité à réclamer l'espace d'adresses.

Si le FAI souhaite réclamer toutes les allocations mais que certaines sous allocations lui ont résisté, on pourrait obtenir quelque chose comme ce qui suit, dans lequel il va réclamer seulement la moitié supérieure d'une allocation (si elle est éventuellement restée inutilisée).

```
inetnum:     192.168.144.0-192.168.147.255
mnt-by:      FAI
mnt-lower:   EBG-COM
reclaim:     192.168.146/23+
```

Si on suppose que le mainteneur EBG-COM et le mainteneur MORTALS veulent ajouter un objet route, une façon de le faire est que les deux parties signent. Si EBG-COM n'a pu pour une raison quelconque agréger et allouer une seule route de niveau supérieur (ce qui est inexcusable de nos jours) ou si il y avait une préférence pour une raison quelconque pour éviter l'approche de la signature conjointe sur une soumission, l'une ou l'autre partie pourrait donner à l'autre la permission de faire l'ajout. Un mnt-routes pourrait être ajouté au aut-num ou un mnt-lower pourrait être ajouté à un inetnum.

```
aut-num:     AS65501
mnt-by:      WIZARDS
mnt-lower:   MORTALS
mnt-routes:  EBG-COM {192.168.144/23}
```

Avec ce changement au aut-num, le mainteneur EBG-COM pourrait ajouter un chemin avec pour origine AS65501, mais seulement avec une gamme d'adresses limitée.

```
route:       192.168.144/24
origin:      AS65501
descr:       Ces idiots ne s'agrègent pas
```

mnt-by: EBG-COM
mnt-by: FICTION::MORTALS

Noter que lorsque le mainteneur EBG-COM ajoute l'objet, ils permettent au mainteneur MORTALS la capacité de le modifier.

Si un objet a fini dans un autre répertoire, un seul mainteneur pourrait encore être utilisé. Dans l'exemple ci-dessus, la notation FICTION::MORTALS indique que l'objet route est dans un répertoire différent et plutôt qu'un dupliqué du mainteneur, une référence est faite au répertoire dans lequel réside l'objet MORTALS.

Dans l'exemple ci-dessous, une paire de route-sets est ajoutée et des noms hiérarchiques sont utilisés.

route-set: AS65501:Customers
mnt-by: WIZARDS
mnt-lower: MORTALS

route-set: AS65501:Customers:EBG-COM
mnt-by: MORTALS
mnt-lower: EBG-COM

Supposons que dans l'objet 192.168.144/24 ci-dessus, seul le mainteneur EBG-COM soit cité. Si EBG-COM fait faillite, n'a plus besoin d'espace d'adresses, et cesse de répondre, il pourrait être difficile de supprimer cet objet. Le mainteneur cité dans l'attribut referral-by de EBG-COM pourrait être contacté. Il pourrait ajouter un attribut auth-override à l'objet EBG-COM. Ensuite, il pourrait modifier l'objet EBG-COM et ensuite tous les objets avec EBG-COM dans le mnt-by.

mntner: EBG-COM
mnt-by: EBG-COM
auth-override: 19990401

Les exemples ci-dessus s'écartent significativement de la réalité. Ils fournissent une simple illustration de l'usage du type d'objets et des attributs décrits dans le présent document et on espère que cela sera utile à quelque chose.

C. Discussion technique

Il y a eu quelques compromis techniques. Certains de ces compromis, la solution choisie, et les solutions de remplacement sont exposés ici. Voici une liste partielle de ces questions.

1. Faut-il pencher du côté de la permissivité et affaiblir les contrôles d'autorisation ou risquer la possibilité d'ériger des barrières à l'enregistrement des informations.
2. Faut-il prendre en charge la mise en application du prêt d'adresse ou fournir à l'utilisateur plus petit ou final le contrôle ultime sur l'enregistrement des préfixes qu'il utilise.
3. Que faire des plus vieux objets qui ne se conforment pas aux nouvelles exigences concernant l'autorisation, l'authentification, et la prise en compte minimale, ou de validité discutable.

C.1 Relâchement des exigences pour les besoins des registres

Si l'exigence qu'existe un aut-num est relâchée, il est alors possible à n'importe qui d'utiliser un numéro d'AS non alloué ou d'utiliser un numéro d'AS alloué pour lequel l'aut-num n'a pas été entré. Poser des exigences à l'entrée de aut-num présuppose la coopération de l'autorité d'allocation d'adresses Internet (si elle est séparée du registraire d'acheminement). L'autorité d'allocation d'adresses doit accepter de présenter des demandes pour remplir l'esquisse de aut-num de la partie pour laquelle l'allocation a été faite. Ces aut-num doivent inclure une référence à un mainteneur. Une demande à l'autorité d'allocation d'adresses doit donc inclure une référence à un mainteneur existant.

La capacité d'ajouter des objets route est aussi liée à l'existence d'objets route ou inetnum moins spécifiques. L'autorité d'allocation d'adresses Internet (si elle est séparée du registraire d'acheminement) doit aussi accepter de présenter des demandes d'ajout d'enregistrements inetnum pour la partie à laquelle l'espace d'adresse est déjà alloué.

L'autorité d'allocation d'adresses Internet devrait aussi ajouter des inetnum et des aut-num pour les nouvelles allocations. Pour le faire, il doit exister un mainteneur. Si une partie se connecte à l'Internet, elle peut obtenir un mainteneur en faisant une demande au fournisseur de service Internet auquel elle est connectée. Une fois qu'elle a un mainteneur, elle peut faire une demande d'espace d'adresse ou de numéro d'AS. Le mainteneur peut contenir une clé publique pour une méthode d'autorisation cryptographiquement forte ou pourrait contenir une vérification d'autorisation "crypt-key" ou "mail-to" si

cela est considéré comme adéquat par la partie enregistreuse. De plus, une autorité d'allocation d'adresse devrait vérifier que la demande d'un numéro d'AS ou d'un espace d'adresse correspond aux critères d'autorisation du mainteneur. Actuellement, seuls les registraires eux-mêmes peuvent ajouter des mainteneurs. Cela devient un problème pour le registraire, en particulier pour vérifier les clés publiques. Cette exigence est relâchée en permettant aux mainteneurs existants d'ajouter des mainteneurs. Malheureusement, la traçabilité n'existe pas pour les mainteneurs existants. L'exigence devrait alors être assouplie de telle sorte que les mainteneurs existants puissent rester mais que seuls les mainteneurs existants qui ont un attribut "referral-by" puissent ajouter des mainteneurs. Le "referral-by" ne peut pas être modifié. Cette exigence peut être légèrement assouplie afin qu'un "referral-by" puisse être ajouté à un mainteneur par un mainteneur existant avec un "referral-by". Cela permettra d'ajouter la traçabilité aux mainteneurs existants et ces mainteneurs pourront alors ajouter de nouveaux mainteneurs.

Vérifier sur les ajouts initiaux qu'une partie est bien celle qu'elle prétend être est un des problèmes que rencontrent actuellement les registraires de numéros d'AS et d'adresses. Ce problème est réduit en permettant aux mainteneurs existants d'ajouter des mainteneurs. Cela peut en fait rendre plus facile d'obtenir des mainteneurs et donc plus facile l'enregistrement. L'autorité des numéros doit quand même vérifier que l'AS ou l'espace d'adresses est réellement nécessaire à la partie qui fait la demande.

Les vérifications d'autorisation faites durant l'ajout des objets route qui se réfèrent aux objets AS et aux inetnum s'appuient fortement sur la coopération des autorités d'allocation des adresses de l'Internet. Les autorités de numérotation doivent enregistrer les as-block, aut-num, ou inetnum selon l'allocation d'espace de numéros d'AS ou d'adresses. Si seulement un sous ensemble des autorités de numérotation coopère, un inetnum ou un as-block peut être créé qui couvre l'espace qu'alloue le registraire et exige essentiellement une allocation nulle (par exemple, une authentification "crypt-pw" où le mot de passe est donné dans les remarques dans l'objet ou son mainteneur) ou ceux qui obtiennent des adresses de la part des autorités de numérotation auront des problèmes pour s'enregistrer dans le registre des acheminements. Le modèle d'autorisation prend en charge l'une et l'autre option, bien qu'il soit préférable que les autorités de numérotation coopèrent et que le problème ne se produise jamais en pratique.

Les exigences sur les mainteneurs peuvent être légèrement assouplies pour les mainteneurs existants pour rendre l'enregistrement plus facile. Assouplir les exigences sur d'autres objets peut mettre en échec le modèle d'autorisation, et n'est donc pas une option.

C.2 Question de prêts d'adresse

La question de savoir si des contrats de prêts devraient pouvoir être mis en application touche au problème de qui devrait en fin de compte être capable d'exercer le contrôle sur les allocations d'espace d'adresses. Le registraire d'acheminement ferait bien de rester aussi neutre que possible à l'égard des disputes entre tiers. Le "reclaim" et "no-reclaim" sont conçus pour permettre l'un ou l'autre résultat sur la décision de savoir si le détenteur d'un objet inetnum ou route moins spécifique peut exercer le contrôle sur les sous allocations dans le registre. Le registraire d'acheminement lui-même doit décider si il conserve lui-même le contrôle, et si il en décide ainsi, il devrait déclarer très clairement sous quelles conditions le registraire va intervenir. Un registraire pourrait même aller jusqu'à déclarer qu'il ne va intervenir dans une telle dispute qu'après sa résolution en justice et l'émission d'une ordonnance du tribunal.

Lorsque une allocation est faite par un registraire, celui-ci devrait garder un attribut "reclaim" dans l'objet le moins spécifique et faire une forte déclaration de politique disant que le privilège reclaim ne sera pas utilisé sauf dans des circonstances particulières très clairement définies (qui devraient au minimum inclure une décision de justice). Si l'allocation est encore subdivisée, la partie qui subdivise l'allocation et celle qui accepte la sous allocation doivent décider si un "reclaim" peut être gardé par le détenteur de l'allocation moins spécifique ou si un "no-reclaim" doit être ajouté, transférant le contrôle au détenteur du plus spécifique. Le registraire n'est pas impliqué dans cette décision. Des paires différentes de tiers peuvent arriver à des décisions différentes en ce qui concerne le "reclaim" et les restrictions contractuelles sur son utilisation qui peuvent être exprimées en dehors du registre sous la forme d'un contrat légal et finalement résolues par les tribunaux dans le cas d'une dispute caractérisée.

En retenant les droits du "reclaim", le registraire conserve la capacité de se soumettre à une décision de justice. Cela ne peut vraiment devenir un problème dans un environnement de registraire réparti où les registraires vont revérifier l'autorisation des transactions faites ailleurs et peuvent échouer à traiter les tentatives d'un autre registraire de se soumettre à une décision de justice en outrepassant l'autorisation normale de changer le contenu du registre si un reclaim n'est pas présent.

C.3 Traitement des données non conformes ou anciennes et discutables

Certaines des plus récentes exigences incluent d'exiger que tous les objets fassent référence à un objet mainteneur responsable de l'intégrité de l'objet et d'exiger que la traçabilité de la création des mainteneurs soit enregistrée dans les

objets maintainer afin qu'on puisse la retracer au cas où un mainteneur ne répondrait plus. Dans le cas où les informations de contact seraient absentes ou incorrectes à partir des objets et où il y aurait des question sur la validité des objets, le mainteneur peut être contacté. Si le mainteneur ne répond pas, le mainteneur qui a autorisé l'ajout de ce mainteneur peut être contacté pour mettre à jour les informations de contact sur le mainteneur ou pour confirmer que l'entité n'existe plus ou n'utilise plus activement l'Internet ou le registre.

Il existe de nombreux objets route pour lesquels il n'y a pas de mainteneur et pour lesquels il n'existe pas d'objet inetnum et AS. Certains contiennent l'attribut maintenant obsolète guardian plutôt qu'un mnt-by.

Il n'est pas pratique de purger inconditionnellement les vieilles données qui n'ont pas de mainteneur ou ne se conforment pas à la hiérarchie des autorisations. Il doit être exigé des nouveaux ajouts qu'ils se conforment aux nouvelles exigences (autrement, les exigences n'ont pas de sens). Les nouvelles exigences peuvent être imposées en exigeant que les modifications se conforment aux nouvelles exigences.

Une grande quantité de données discutables existent dans le registre actuel. L'exigence que tous les objets aient des mainteneurs et l'exigence d'une meilleure traçabilité des mainteneurs eux-mêmes peut rendre plus facile de déterminer les informations de contact même lorsque les objets ne sont pas mis à jour pour refléter les changements des informations de contact.

Il n'est pas déraisonnable d'exiger des informations de contact valides sur les données existantes. Une grande quantité de données paraissent être inutilisées, comme les objets route pour lesquels aucune annonce n'a été vue depuis de nombreux mois ou années. On devrait tenter de joindre les contacts cités dans l'objet, dans le mainteneur si il en est un, puis jusqu'à la chaîne de referral-by de mainteneur si il y en a une, et utiliser les informations de contact du numéro de registre ou de l'AS d'origine si il n'y a pas de traçabilité du mainteneur à suivre. L'expérience accumulée jusqu'à maintenant indique que la vaste majorité des suppressions identifiées en comparant les préfixes enregistrés aux chemins de rebut sera positivement confirmée (permettant la suppression) ou il n'y aura pas de réponse du fait d'informations de contact invalides (dans de nombreux cas, les informations de contact IRR pointent sur nsfnet-admin@merit.edu).

En permettant au registraire de modifier (ou supprimer) tout objet qui est déconnecté de la traçabilité du mainteneur, le nettoyage devient possible (bien que la falsification de l'en-tête de message puisse dans de nombreux cas avoir le même effet, il est préférable d'enregistrer le fait que le registraire a fait lui-même le nettoyage). De façon similaire, un mécanisme peut être nécessaire à l'avenir pour permettre au mainteneur d'outrepasser dans le referral-by les privilèges de mainteneur dans une référence de mainteneur si tous les contacts sont devenus sans réponse pour un mainteneur. Le mainteneur referral-by a la permission d'ajouter un attribut "auth-override" qui devient utilisable comme un "auth" dans les 60 jours du moment de l'ajout. Le mainteneur lui-même serait notifié du changement et pourrait retirer l'attribut "auth-override" avant qu'il devienne effectif et s'enquérir de la raison pour laquelle il a été ajouté et corriger le problème existant. Cela peut être pris en charge immédiatement ou ajouté plus tard si nécessaire.

D. Cas de fonctionnement courants

En principe, l'allocation d'adresse et l'allocation de chemin devraient être hiérarchisées avec une hiérarchie correspondant à la topologie physique. En pratique, ce n'est souvent pas le cas pour de nombreuses raisons. Les raisons principales sont que la topologie n'est pas une arborescence structurée stricte et que la topologie peut changer. Plus précisément :

1. La topologie de l'Internet n'est pas une arborescence structurelle stricte.
    - Au niveau supérieur, le réseau ressemble plutôt à un maillage modérément dense.
    - Près du niveau inférieur, de nombreux rattachements à l'Internet sont des multi rattachements à plus d'un fournisseur Internet.
2. La topologie de l'Internet peut changer et change effectivement.
    - De nombreux rattachements changent de fournisseur pour obtenir un meilleur service ou de meilleures conditions.
    - Les fournisseurs de service peuvent modifier des adjacences pour obtenir un meilleur service ou conditions de transit.
    - Les fournisseurs de service peuvent disparaître complètement en dispersant leurs rattachements ou ils peuvent fusionner.

La dénumérotation est vue comme un moyen pratique d'entretenir une stricte hiérarchie numérique [RFC2008]. Il est aussi connu que la dénumérotation des réseaux IPv4 peut être difficile [RFC2008], [RFC2072], [RFC2073]. On examine d'abord le cas simple où la hiérarchie existe encore. On examine ensuite les cas de fonctionnement où la topologie initiale n'est pas structurée en arborescence ou les cas où la topologie change.

D.1 Allocation d'adresse hiérarchique simple et allocation de chemin

C'est le cas le plus simple. De large gammes de inetnum sont allouées aux registraires d'adresses. Ces registraires allouent à leur tour de plus petites gammes pour un usage direct ou pour de grandes entités topologiques lorsque les allocations selon la topologie peuvent réduire la quantité d'informations d'acheminement nécessaires (pour promouvoir une meilleure agrégation de chemin).

Les objets AS sont alloués comme le dicte la topologie en fonction des besoins d'AS supplémentaires [RFC1519]. Les objets Route peuvent être enregistrés par ceux qui ont l'autorisation donnée par l'AS et par le possesseur de l'adresse. Cela ne pose jamais de problème lorsque le mainteneur de l'AS et le inetnum sont le même. Lorsque ils diffèrent, le fournisseur peut donner la permission d'ajouter des objets route pour leur AS, ou la partie à qui est alloué l'espace d'adresses peut donner au fournisseur la permission d'ajouter des objets route pour son espace d'adresses, ou les deux parties peuvent signer la transaction. La permission est donnée en ajoutant des attributs au mainteneur.

D.2 Agrégation et chemins plus spécifiques multi rattachement

L'agrégation ne pose normalement pas de problème si un fournisseur agrège l'espace d'adresses qui lui est alloué et fait des sous allocations en interne et/ou à ses clients. En fait, le fournisseur est supposé faire comme cela. Cela ne pose pas de problème même si l'objet route pour l'agrégation est ajouté après les objets route plus spécifiques car seulement les objets moins spécifiques sont considérés.

Potentiellement, l'agrégation est un problème si un fournisseur ou un ensemble de fournisseurs prévoit d'agréger un espace d'adresses qui n'a jamais été explicitement alloué comme un bloc à ces fournisseurs mais reste plutôt l'allocation d'un registraire d'adresses. On peut s'attendre à ce que ces grandes agrégations restent peu courantes, mais il est assez facile de s'en accommoder. Des super agrégats de ce type vont généralement être formés par des entités topologiquement proches qui se sont aussi arrangées pour tirer des allocations d'adresses adjacentes. En effet, le registraire doit donner la permission de former de tels super agrégats soit en donnant la permission de le faire dans le mnt-routes d'un inetnum, soit en signant la soumission avec les autres parties.

D.3 Adresses indépendantes du fournisseur et AS à origine multiple

Les adresses indépendantes du fournisseur et les arrangements multi rattachements qui utilisent plusieurs AS d'origine présentent un problème similaire au multi rattachement. Le mainteneur de l'espace d'adresses et le mainteneur de l'AS ne sont pas les mêmes. La permission peut être accordée en utilisant mnt-routes ou plusieurs signatures peuvent apparaître sur la soumission.

D.4 Changement de fournisseur de service Internet

Un changement de fournisseur de service Internet est similaire au multi rattachement. Une différence mineure est que l'AS pour le chemin le plus spécifique sera l'AS du nouveau fournisseur plutôt que l'AS du client multi rattachement. La permission peut être accordée en utilisant mnt-routes ou plusieurs signatures peuvent apparaître sur la soumission.

D.5 Périodes de grâce de dénumérotation

Les périodes de grâce de dénumérotation permettent à un fournisseur qui veut garder intacte une allocation d'adresse pour permettre à un client qui a choisi de passer à un autre fournisseur de dénuméroter graduellement son réseau et de restituer ensuite l'espace d'adresses après l'achèvement du dénumérotage. La question de savoir si il faut exiger le dénumérotage immédiat ou offrir une période de grâce de dénumérotage et combien de temps cela devrait durer ou si elle devrait être indéfinie a été le sujet d'âpres discussions. Le modèle d'autorisation peut accepter qu'il n'y ait pas de période grâce, une période finie, ou une période indéfinie. L'attribut "reclaim" décrit au paragraphe 9.1 donne le moyen de mettre fin à la période de grâce.

E. Considérations de déploiement

Cette section décrit les considérations de déploiement. L'intention est de soulever les problèmes et de discuter des approches plutôt que de fournir un plan de déploiement.

L'utilisation de registres d'acheminement n'est pas encore universellement acceptée. Il reste encore des fournisseurs Internet qui ne voient pas de raisons de fournir l'assurance supplémentaire de la précision des informations d'acheminement décrites à la Section 6. Plus précisément, les avantages sont vus comme étant insuffisants pour en justifier le coût. Cela a été dans une large mesure causé par l'incapacité d'un très gros fabricant de routeurs jusqu'à recemment à

traiter des listes de préfixes de la taille nécessaire pour spécifier la politique d'acheminement sur la base du préfixe.

Une autre raison citée est que le filtrage sur la base du préfixe dans un environnement où les informations du registre des acheminement sont incomplètes ou imprécises peut interférer avec la connexité.

Il y a clairement un problème de masse critique à l'égard de l'utilisation des registres d'acheminements. Une minorité de fournisseurs utilise l'IRR existant pour filtrer sur la base du préfixe. Une autre minorité de fournisseurs ne prend pas en charge l'IRR et s'abstient généralement d'enregistrer les préfixes jusqu'à ce qne des problèmes de connexité soient rapportés. La majorité des fournisseurs enregistre les préfixes mais ne met pas en œuvre un strict filtrage par préfixe.

Déployer de nouveaux mécanismes d'authentification n'a pas de conséquences néfastes. Cela a été prouvé avec le déploiement de PGP par Merit.

Pour déployer un nouveau mécanisme d'autorisation, une question majeure est d'avoir à faire avec des données existantes d'origine très douteuse. Un très grand nombre d'objets route se réfèrent à des préfixes qui n'ont pas été annoncés depuis de nombreuses années. D'autres objets route se réfèrent à des préfixes qui ne sont plus annoncés avec l'AS d'origine avec lequel ils sont enregistrés (certains étaient enregistrés dès le début de façon incorrecte). Il y a de nombreuses causes à cela.

1. Durant la transition du NSFNET PRDB au RADB, un grand nombre de préfixes ont été enregistrés avec un AS d'origine correspondant à l'AS frontière à laquelle le NSFNET avait en jour entendu les annonces de chemin. Le PRDB ne prenait pas en charge l'AS d'origine, de sorte que l'AS frontière était utilisé. Beaucoup de ces chemins n'étaient plus utilisés à cette époque et sont maintenant acheminés avec un soumettant cité comme "nsfnet-admin@merit.edu".
2. Lorsque CIDR a été déployé, les agrégats ont remplacé des préfixes plus spécifiques précédemment annoncés séparément. Les objets route pour les préfixes plus spécifiques n'ont jamais été retirés des registres d'acheminement.
3. Certains préfixes ne sont tout simplement plus utilisés. Certains réseaux ont été dénumérotés. Certains réseaux n'existent plus. Souvent, les informations des registres d'acheminement ne sont pas retirées.
4. Comme les adjacences d'AS de fournisseur ont changé et comme les clients finaux changent de fournisseurs, l'AS d'origine réel change souvent. Cela est rarement reflété par un changement dans le registre d'acheminement.

Des inexactitudes continueront de se produire à cause des raisons ci-dessus, sauf la première. L'autorisation hiérarchique assure une plus grande traçabilité. Lorsque les contacts des objets spécifiques ne répondent plus, la remontée de la hiérarchie des autorisations devrait aider à identifier les parties qui ont antérieurement fourni l'autorisation. Ces contacts peuvent avoir encore des autorisations suffisantes pour effectuer le nettoyage nécessaire. Cette question est discutée à la Section C.

Une grande quantité d'informations manquent actuellement dans l'IRR. Quelques AS n'ont pas d'aut-num. Un nombre non négligeable de données n'ont pas de mainteneur et la grande majorité des mainteneurs utilise seulement les plus faibles des méthodes d'authentification. Les registraires ne peuvent pas faire grand chose pour corriger cela. La solution par défaut dans les cas d'objets manquants nécessaires pour l'autorisation est de ne pas faire du tout de vérification d'authentification.

Les étapes de la transition sont les suivantes :

1. Ajouter et utiliser de plus forts modèles d'autorisation.
2. Faire les modifications de schéma nécessaires pour prendre en charge les délégations.
3. Ajouter les attributs de délégation nécessaires pour la traversée des interrogations.
4. Fonder la traversée d'interrogation sur les délégations plutôt que sur une recherche dans tous les registres connus.
5. Obtenir la coopération des registres d'adresse pour remplir les entrées "inetnum" en continu.
6. Ajouter la prise en charge de l'autorisation hiérarchique pour les types d'objets critiques "aut-num", "inetnum" et "route".
7. Ajouter l'exigence que l'objet de base de données soit utilisé ou ait des informations de contact valides et si des interrogations sont faites par le registraire, une réponse d'une personne de contact indiquant que l'objet sert à quelque chose si cela n'apparaît pas clairement.
8. Commencer à purger les données qui ne sont clairement pas utilisées et pour lesquelles il n'y a pas d'informations de contact valides ou il n'y a pas de réponse de la part du contact.

Le déploiement de l'autorisation hiérarchisée exige la coopération des registraires d'acheminement existants. Un nouveau code devra être déployé. Dans certains cas, des ressources minimales de développement sont disponibles et une inertie substantielle existe à cause de la dépendance aux répertoires actuels et de la nécessité d'éviter les interruptions.

Si l'autorisation hiérarchisée des objets route dépend de l'existence des informations d'enregistrement d'adresse, un minimum de coopération est nécessaire entre les registres d'adresses actuellement séparés. L'étendue de la coopération consiste à envoyer des transactions à signature chiffrée du registre d'adresses au registre de numéros lorsque les allocations d'adresses sont faites, ou à fournir un accès équivalent aux nouvelles allocations d'adresse.

Actuellement, la plupart des registres retournent les résultats d'interrogations provenant de tous les répertoires connus en

utilisant leurs copies miroirs. Les autorisations inter registres ne sont pas encore mises en œuvre. Les changements minimaux de schéma doivent être effectués pour prendre en charge la capacité à déléguer les objets pour lesquels il y a une hiérarchie d'autorisation et pour prendre en charge les interrogations et les références aux autres répertoires. Dans le cas des délégations d'AS, le "as-block" doit être créé seulement pour les besoins de traversée.

F. Pseudocode d'autorisation d'objet Route

La liste suivante passe brièvement en revue les concepts de base.

1. La soumission d'objet route doit satisfaire à deux critères d'authentification. Elle doit répondre à l'authentification spécifiée dans le aut-num et à l'authentification spécifiée soit dans un objet route, soit, si on ne trouve aucun objet route applicable, dans un inetnum.

2. Lors d'une vérification d'autorisation de préfixe, un correspondance exacte de préfixe d'objet route est d'abord vérifiée. Si il n'y a pas une correspondance exacte, on recherche alors une correspondance du plus long préfixe moins spécifique que le préfixe. Si la recherche de préfixe de chemin échoue, on effectue alors une recherche d'un inetnum qui corresponde exactement au préfixe ou du plus spécifique inetnum qui soit moins spécifique que la soumission d'objet route.

   La recherche d'un inetnum ne devrait jamais échouer mais elle peut retourner une gamme non allouée ou réservée. L'état inetnum doit être "alloué" et la soumission doit réussir l'examen de l'autorisation de son mainteneur afin d'obtenir l'autorisation d'un inetnum. De sorte qu'une gamme d'inetnum non allouée ou réservée causera l'échec de la soumission de l'objet route.

3. Un objet route doit réussir l'examen de l'autorisation des deux objets référencés aut-num et route ou inetnum. L'autorisation devra être vérifiée en utilisant le ou les mainteneurs référencés d'abord dans le ou les attributs "mnt-routes". Si cette vérification échoue, les attributs "mnt-lower" sont vérifiés. Si cette vérification échoue, on utilise les attributs "mnt-by" pour la vérification d'autorisation.

4. L'attribut "reclaim" peut apparaître dans les objets inetnum, route et as-block et fournir un moyen pour prendre en charge le prêt d'adresse. "reclaim" donne l'autorisation sur des objets plus spécifiques, sans considération du "mnt-by" dans l'objet. La valeur d'un attribut "reclaim" peut être une liste ou ensemble d'objets pour assurer une plus fine granularité de contrôle.

L'attribut "reclaim" est important pour cette discussion car il affecte l'authentification de préfixe/origine lors de la soumission d'un nouvel objet route.

L'attribut "no-reclaim" est utilisé pour fournir des exceptions explicites.

Le pseudocode suivant illustre l'algorithme utilisé pour vérifier la bonne autorisation d'une soumission d'objet route.

Cas n° 1. Ajout d'objet route (c'est-à-dire, il n'existe pas de correspondance exacte de préfixe/origine).

```
/* D'abord, vérification de l'autorisation de aut-num */

si ( l'objet aut-num référence n'existe pas ou si l'autorisation du aut-num échoue )
     échec d'autorisation

/* On vérifie ensuite l'autorisation du préfixe */

si ( on trouve un ou des chemins moins spécifiques avec le plus long préfixe ) [
  si ( l'autorisation échoue pour au moins un des chemins moins spécifiques )
     échec d'autorisation

/* on vérifie maintenant un attribut "reclaim" */

  si ( l'objet a un attribut "reclaim" ) [
   si ( il n'en exister pas de plus spécifique
        OU si il en existe un moins spécifique qui réussit l'autorisation et a un attribut "reclaim"
        OU si tous les chemins plus spécifiques réussissent l'autorisation de modifier )
     l'autorisation réussit
```

```
    autrement
       l'autorisation échoue
     ] autrement
      l'autorisation réussit
   ]

/* il n'y a pas de chemin moins spécifique à vérifier pour l'authentification de préfixe, donc il faut essayer d'obtenir
    l'autorisation d'un objet inetnum */

si ( ( un inetnum est trouvé avec une correspondance exacte
       OU est moins spécifique et son état est "alloué" )
       ET un mainteneur référencé par le inetnum réussit l'autorisation )
    l'autorisation réussit

/* si il n'y a pas d'objet inetnum ou route, l'autorisation échoue. Cela ne devrait jamais arriver si la base de données est
    initialisée correctement. */
    autrement
       l'autorisation échoue

Cas n° 2.  Modification/suppression d'objet Route (c'est-à-dire, il existe une correspondance exacte de préfixe/origine).

si ( le mnt-by réussit l'autorisation )
  l'autorisation réussit

/* si l'autorisation ne réussit pas à partir de l'objet correspondant, on peut encore obtenir l'autorisation à partir d'un chemin
    moins spécifique si il a un attribut "reclaim" et réussit à l'autorisation */

si ( un objet route ou inetnum moins spécifique réussit l'autorisation
      ET a un attribut "reclaim" applicable à l'objet à modifier )
  l'autorisation réussit
 autrement
  l'autorisation échoue
```

Remerciements

Le présent document tire des idées de nombreuses discussions et contributions des groupes de travail de l'IETF Routing Policy System et RIPE Routing. Des projets antérieurs au présent document mentionnaient Carol Orange comme co-auteur. Carol Orange a fait des contributions au présent document lorsque elle était à RIPE.

Gerald Winters a fourni le pseudocode dans un message à la liste de diffusion RIPE dbsec et qui a servi de base pour le pseudocode de l'Appendice F. Susan Harris a fourni des commentaires et de nombreuses corrections rédactionnelles.

Références

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la* RFC5322)

[RFC1102] D. Clark, "Acheminement selon la politique dans les protocoles de l'Internet", mai 1989.

[RFC1104] H. Braun, "Modèles d'acheminement selon la politique", juin 1989.

[RFC1222] H. Braun et Y Rekhter, "Avancement de l'architecture d'acheminement du NSFNET", mai 1991. *(Info)*

[RFC1482] M. Knopper et S. Richardson, "Prise en charge de l'agrégation dans la base de données d'acheminement NSFNET fondé sur la politique", juin 1993. *(Historique)*

[RFC1517] IESG, R. Hinden, "Déclaration d'applicabilité de la mise en œuvre de l'acheminement inter domaine sans classe", septembre 1993. *(Historique)*

[RFC1518] Y. Rekhter et T. Li, "Architecture pour l'allocation d'adresses IP avec CIDR", septembre 1993. *(Historique)*

[RFC1519] V. Fuller, T. Li, J. Yu et K. Varadhan, "Acheminement inter domaine sans classe (CIDR) : stratégie d'allocation et d'agrégation d'adresses", septembre 1993. *(D.S., rendue obsolète par la* RFC4632)

[RFC1786] T. Bates, E. Gerich, L. Joncheray, J-M. Jouanigot, D. Karrenberg, M. Terpstra, J. Yu, "Représentation des politiques d'acheminement IP dans un registre d'acheminement (ripe-81++)", mars 1995. *(Information)*

[RFC1787] Y. Rekhter, "Acheminement dans un Internet multi fournisseurs", avril 1995. *(Information)*

[RFC1930] J. Hawkinson, T. Bates, "Lignes directrices pour la création, sélection, et l'enregistrement d'un système autonome (AS)", mars 1996. (BCP0006)

[RFC2008] Y. Rekhter, T. Li, "Implications des diverses politiques d'allocation d'adresse pour l'acheminement Internet", octobre 1996. (BCP0007)

[RFC2050] K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg, J. Postel, "Lignes directrices pour l'allocation des adresses IP par les registraires Internet", novembre 1996. *(Remplace* RFC1466) (BCP0012)

[RFC2072] H. Berkowitz, "Guide du dénumérotage des routeurs", janvier 1997. (*MàJ par* RFC4192) *(Information)*

[RFC2073] Y. Rekhter, P. Lothberg, R. Hinden, S. Deering, J. Postel, "Format IPv6 d'adresse en envoi individuel fondée sur le fournisseur", janvier 1997. (*Obsolète, voir* RFC2374) *(P.S.)*

[RFC2280] C. Alaettinoglu, T. Bates, E. Gerich, D. Karrenberg, D. Meyer, M. Terpstra, C. Villamizar, "Langage de spécification des politiques d'acheminement (RPSL)", janvier 1998. (*Obsolète, voir* RFC2622) *(P.S.)*

[RFC2650] D. Meyer, J. Schmitz, C. Orange, M. Prior, C. Alaettinoglu, "RPSL pratique", août 1999. *(Information)*

[RFC2726] J. Zsako, "Authentification de PGP pour mise à jour de base de données RIPE", décembre 1999. *(P.S.)*

Considérations pour la sécurité

Le présent document traite principalement des règles d'autorisation pour faire des ajouts, suppression et changements aux répertoires d'informations de politiques d'acheminement. L'authentification de ces transactions par des moyens cryptographiques forts est traitée par la [RFC2726], référencée tout au long du présent document. Les règles d'autorisation sont conçues de telles sorte que l'intégrité de toute transaction puisse être vérifiée de façon indépendante par toute partie qui reflète un répertoire pour s'assurer que les règles sont respectées. Pour réaliser cela, le miroir doit contenir des données déjà connues comme étant correctement autorisées. En d'autres termes, le miroir doit être complet et les vérifications d'authentification et d'autorisation doivent être faites en continu lorsque les changements au répertoire sont reçues et traitées dans l'ordre.

L'authentification seule ne fournit pas un modèle de sécurité complet. Les pratiques courantes spécifient l'autorisation pour les seules suppressions et modifications, et pas pour les ajouts. Les règles d'autorisation fournies ici complètent le modèle

de sécurité pour les ajouts, les suppressions, et les changements en définissant très explicitement les règles d'ajout et en précisant les procédures de traitement des exceptions telles que celle des organisations qui ont cesssé d'exister et donc ne répondent plus du tout.

L'authentification et l'autorisation des interrogations est explicitement déclarée être en dehors du domaine d'application du présent document.

Adresse des auteurs

Curtis Villamizar	Cengiz Alaettinoglu	David M. Meyer	Sandy Murphy
Avici Systems	ISI	Cisco	Trusted Information Systems
mél : curtis@avici.com	mél : cengiz@ISI.EDU	mél : dmm@cisco.com	mél : sandy@tis.com

Déclaration complète de droits de reproduction

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