Groupe de travail Réseau
Request for Comments : 4012
RFC rendues obsolètes : 2725, 2622
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

L. Blunk, Merit NetworkLee
J. Damas, Internet Systems Consortium
F. Parent, Hexago
A. Robachevsky, RIPE NCC
mars 2005

Langage de spécification de politique d'acheminement de prochaine génération (RPSLng)

Résumé
Le présent mémoire introduit un nouvel ensemble d'extensions simples au langage spécification de politique d'acheminement (RSPL, *Routing Policy Specification Language*) permettant le langage pour documenter les politiques d'acheminement pour IPv6 et les familles d'adresse de diffusion groupée actuellement utilisées dans l'Internet.

Table des Matières

1. Introduction

La [RFC2622] définit le langage RPSL pour les protocoles d'acheminement en envoi individuel IPv4 et donne une série de lignes directrices pour étendre le langage RPSL lui-même. De plus, des extensions de sécurité au langage RPSL sont spécifiées dans la [RFC2725].

Le présent document propose d'étendre RPSL conformément aux buts et exigences suivants :
o Donner à RPSL une capacité d'extension dans le domaine des familles d'adresses, précisément, de permettre aux

utilisateurs de documenter la politique d'acheminement pour IPv6 et la diffusion groupée.
- o Les extensions devraient être rétro compatibles avec un impact minimal sur les outils et processus existants, suivant la Section 10 de la [RFC2622] sur les lignes directrices pour l'extension de RPSL.
- o Conserver la clarté et la non ambiguïté : les informations RPSL sont utilisées par des humains en plus des outils logiciels.
- o Minimiser la duplication des informations, en particulier lorsque les politiques d'acheminement sont les mêmes pour les différentes familles d'adresses.

L'ajout de la prise en charge de IPv6 et de la diffusion groupée à RPSL conduit à quatre politiques d'acheminement distinctes qui doivent être différenciées dans la présente spécification, à savoir , [IPv4 {envoi individuel|diffusion groupée}, IPv6 {envoi individuel|diffusion groupée}].

2. Spécification de politique d'acheminement pour différentes familles d'adresses

La politique d'acheminement est actuellement spécifiée dans le classe aut-num en utilisant les attributs "import:", "export:", et "default:". Parfois, il est important de distinguer la politique pour différentes familles d'adresses, ainsi que la politique d'acheminement en envoi individuel de celle en diffusion groupée.

Bien que la syntaxe des attributs import, export, et default existants puisse être étendue, cela présenterait des problèmes de rétro compatibilité et pourrait nuire à la clarté des expressions.

En gardant cela présent à l'esprit, les attributs "import:", "export:", et "default:" spécifient implicitement la politique d'envoi individuel IPv4 et resteront comme précédemment définis dans RPSL, et de nouveaux attributs multi protocoles (préfixés par la chaîne "mp-") seront introduits. Ces nouveaux attributs "mp-" sont décrits ci-après.

2.1 Résolution des ambiguïtés

Le même échange de trafic peut être couvert par plus d'un attribut de politique multi protocoles ou par une combinaison d'attributs de politique multi protocoles (lorsque on spécifie une politique d'envoi individuel IPv4) et des attributs précédemment définis de politique d'envoi individuel IPv4. Dans ces cas, les mises en œuvre devraient suivre la règle d'ordre de spécification définie au paragraphe 6.4 de la [RFC2622]. Pour résoudre les ambiguïtés, on utilise l'action correspondant à la première spécification d'échange de trafic.

2.2 Attribut afi Dictionary

Ce paragraphe introduit un nouvel attribut dictionary :

Identifiant de famille d'adresse, <afi>, est une liste RPSL de familles d'adresses pour laquelle une certaine expression de politique d'acheminement devrait être évaluée. <afi> est facultatif au sein des nouveaux attributs multi protocoles introduits dans la classe aut-num. Un pseudo identifiant nommé "any" est défini pour permettre des expressions de politique plus compactes avec une politique d'acheminement convergente.

Les valeurs possibles pour <afi> sont les suivantes :
ipv4.unicast *(IPv4 en envoi individuel)*
ipv4.multicast *(IPv4 en diffusion groupée)*
ipv4 (équivalent à ipv4.unicast, ipv4.multicast)
ipv6.unicast *(IPv6 en envoi individuel)*
ipv6.multicast *(IPv6 en diffusion groupée)*
ipv6 (équivalent à ipv6.unicast, ipv6.multicast)
any (équivalent à ipv4, ipv6)
any.unicast (équivalent à ipv4.unicast, ipv6.unicast)
any.multicast (équivalent à ipv4.multicast, ipv6.multicast)

L'apparition de ces valeurs dans un attribut doit être précédée par le mot clé afi.

Une <afi-list> est défini comme une liste séparée par des virgules d'une ou plusieurs valeurs afi.

2.3 Extensions au dictionnaire RPSL

Afin de prendre en charge les adresses IPv6 spécifiées avec l'attribut de prochain bond rp-attribute, un nouveau type prédéfini de dictionnaire intitulé "ipv6_address" est ajouté au dictionnaire RPSL. La définition de ce type est tirée du paragraphe 2.2 de la [RFC3513].

L'attribut rp-attribute de prochain bond est développé comme suit dans le dictionnaire :

rp-attribute : numéro du routeur de prochain bond dans un chemin statique
opérateur de prochain bond = (union ipv4_address, ipv6_address, enum[self])

Une nouvelle valeur a été ajoutée pour la spécification <protocol> du dictionnaire : MPBGP

MPBGP est compris comme étant le BGP4 avec les extensions multi protocoles (souvent appelé BGP4+). BGP4+ pourrait ne pas pouvoir être utilisé car le caractère '+' n'est pas permis par la spécification RPSL dans les noms de protocoles.

2.4 Types IPv6 RPSL

Le présent document fait référence à trois nouveaux types RPSL IPv6, à savoir , <ipv6-address>, <ipv6-address-prefix>, et <ipv6-address-prefix-range>. Les types <ipv6-address> et <ipv6-address-prefix> sont définis aux paragraphes 2.2 et 2.3 de la [RFC3513]. Le type <ipv6-address-prefix-range> ajoute un opérateur de gamme au type <ipv6-address-prefix>. L'opérateur de gamme est défini à la Section 2 de la [RFC2622].

2.5 mp-import, mp-export, et mp-default

Trois nouveaux attributs de politique sont introduits dans la classe aut-num :
mp-import:
mp-export:
mp-default:

Ces attributs incorporent la spécification afi (famille d'adresse). Noter que la spécification afi est facultative. Si aucune spécification afi n'est présente, l'expression de politique est présumée s'appliquer à toutes les familles de protocoles, à savoir , ipv4.unicast, ipv4.multicast, ipv6.unicast, et ipv6.multicast. Ceci est l'équivalent de la spécification afi "afi any". Les attributs mp-import et mp-export ont tous deux une spécification de politique de base et une spécification de politique structurée plus puissante.

La syntaxe de l'attribut mp-default et de la spécification de politique de base des attributs mp-import et mp-export est la suivante :

Attribut	**Valeur**	**Type**
mp-import	[protocol <protocol-1>] [dans <protocol-2>] [afi <afi-list>] de <mp-peering-1> [action <action-1>; ... <action-N>;] . . . de <mp-peering-M> [action <action-1>; ... <action-N>;] accepte <mp-filter> [;]	facultatif, multi valeurs
mp-export	[protocol <protocol-1>] [dans <protocol-2>] [afi <afi-list>] à <mp-peering-1> [action <action-1>; ... <action-N>;] . . . à <mp-peering-M> [action <action-1>; ... <action-N>;] annonce <mp-filter> [;]	facultatif, multi valeurs
mp-default	[afi <afi-list>] à <mp-peering> [action <action-1>; ... <action-N>;] [réseaux <mp-filter>]	facultatif, multi valeurs

Les politiques mp-import et mp-export peuvent être structurées. Comme avec la [RFC2622], les politiques structurées ne sont recommandées qu'aux utilisateurs RPSL avertis. La syntaxe de politique mp-import structurée est définie ci-dessous. Noter que les deux points à la fin d'un <import-factor> sont obligatoires pour les expressions de politique structurée, et sont facultatifs sur les expressions de politique non structurées. La syntaxe de politique structurée mp-export est exprimée de façon symétrique à l'attribut mp-import. La syntaxe structurée permet des exceptions et des raffinements aux politiques par l'utilisation des mots clés "except" et "refine". De plus, les exceptions et raffinements peuvent spécifier une liste "afi" facultative pour restreindre l'expression de politique à des familles d'adresses particulières.

Noter que la définition permet des raffinements et exceptions subséquents ou "en cascade". La [RFC2622] se réfère de façon incorrecte à cela comme à des expressions "enchâssées". La syntaxe ne permet pas de vraies expressions enchâssées.

<import-factor> ::= de <mp-peering-1> [action <action-1>; ... <action-M>;]
. . .
de <mp-peering-N> [action <action-1>; ... <action-K>;]
accepte <mp-filter>;

<import-term> :: = import-factor | { <import-factor-1>
. . .
<import-factor-N>
}

<import-expression> ::= <import-term> | <import-term> EXCEPT <afi-import-expression> |
<import-term> REFINE <afi-import-expression>

<afi-import-expression> ::= [afi <afi-list>] <import-expression>

mp-import: [protocol <protocol-1>] [into <protocol-2>] <afi-import-expression>

2.5.1 <mp-peering>

<mp-peering> indique l'AS (et le routeur si il est présent) et est défini comme suit :

<mp-peering> ::= <as-expression> [<mp-router-expression-1>] [à <mp-router-expression-2>] | <peering-set-name>

où <as-expression> est une expression sur les numéros d'AS et les ensembles d'AS utilisant les opérateurs ET, OU, et EXCEPT, et l'expression <mp-router-expression> est une expression sur les adresses IPv4 ou adresses IPv6, les noms inet-rtr, et rtr-set utilisant les opérateurs ET, OU, et EXCEPT. L'opérateur binaire "EXCEPT" est l'opérateur soustraction d'ensemble et a la même préséance que l'opérateur ET (il est sémantiquement équivalent à la combinaison ET NON). C'est-à-dire (AS65001 OU AS65002) EXCEPT AS65002" égale "AS65001".

2.5.2 <mp-filter>

L'expression de filtre de politique <mp-filter> est déduite de l'expression de filtre de politique RPSL <filter> définie au paragraphe 5.4 de la [RFC2622]. <mp-filter> étend l'expression <filter> pour permettre la spécification des préfixes et gammes de préfixes IPv6. En particulier, une expression Set Address-Prefix dans une expression <mp-filter> peut inclure des préfixes ou gammes de préfixes IPv4 et IPv6. <mp-filter> est par ailleurs identique à l'expression RPSL <filter>. Les ensembles Address-Prefix sont inclus dans des accolades, '{' et '}'. Le filtre de politique correspond à l'ensemble des chemins dont le préfixe d'adresse de destination est dans l'ensemble . Par exemple :

{ 192.0.2.0/24, 2001:0DB8::/32 } { 2001:0DB8:0100::/48^+, 2001:0DB8:0200::/48^64 }

2.5.3 Exemples de politiques

La famille d'adresses peut être spécifiée dans des expressions de politiques refine ou except suivantes et n'est valide que au sein de l'expression de politique qui la contient.

Donc, dans l'exemple
aut-num: AS65534
mp-import: afi any.unicast from AS65001 accept as-foo;
except afi any.unicast {
from AS65002 accept AS65226;
} except afi ipv6.unicast {
from AS65003 accept {2001:0DB8::/32};
}
le dernier "except" n'est évalué que pour la famille d'adresses IPv6 en envoi individuel, tandis que les autres expressions import- sont évaluées pour les deux familles d'adresses IPv6 et IPv4 d'envoi individuel.

L'évaluation d'une expression de politique est faite en évaluant chacun de ses composants. L'évaluation de peering-sets et filter-sets est contrainte par la famille d'adresses. De telles contraintes peuvent résulter en un <mp-filter> "NOT ANY" ou

un <mp-peering> invalide selon la définition implicite ou explicite de la famille d'adresse dans l'ensemble. Les conflits avec les déclarations explicites ou implicites sont résolus au moment du démarrage durant l'évaluation d'une expression de politique. Une mise en œuvre d'évaluation RPSL peut souhaiter produire un avertissement dans le cas d'un <mp-filter> "NOT ANY". La politique mp-import suivante contient un exemple de <mp-filter> qui devrait être évalué comme "NOT ANY" :
aut-num: AS65002
mp-import: afi ipv6.unicast from AS65001 accept {192.0.2.0/24}

3. Classe route6

La classe route6 est l'équivalent IPv6 de la classe de chemin. Comme avec la classe de chemin, la clé de classe pour la classe route6 est spécifiée par la paire d'attribut route6 et origine. À part l'attribut route6, la classe route6 partage les mêmes noms d'attribut avec la classe de chemin. Bien que les noms d'attributs restent identiques, les attributs inject, components, exports-comps, holes, et mnt-routes doivent spécifier les préfixes et adresses IPv6 plutôt que IPv4. Cette exigence est reflétée par la spécification de <ipv6-router-expression>, <ipv6-filter>, et <ipv6-address-prefix> ci-dessous. <ipv6-address-prefix> a été défini précédemment. <ipv6-filter> se rapporte à <mp-filter> comme défini au paragraphe 2.5.2, à l'exception que seuls les types <ipv6-address-prefix> sont permis. De même, <ipv6-router-expression> se rapporte à <mp-router-expression> comme défini au paragraphe 2.5.1 à l'exception que seuls les types <ipv6-address> sont permis.

Attribut	**Valeur**	**Type**
route6	<ipv6-address-prefix>	obligatoire, clé de classe, valeur unique
origin	<as-number>	obligatoire, clé de classe, valeur unique
member-of	liste de <route-set-name>	facultatif, multi valeurs
inject	[à <ipv6-router-expression>] ... [action <action>] [sur <condition>]	facultatif, multi valeurs
components	[ATOMIC] [[<ipv6-filter>] [protocol <protocol> <ipv6-filter> ...]]	facultatif, valeur unique
aggr-bndry	<as-expression>	facultatif, valeur unique
aggr-mtd	entrant ou sortant [<as-expression>]	facultatif, valeur unique
export-comps	<ipv6-filter>	facultatif, valeur unique
holes	liste de <ipv6-address-prefix>	facultatif, multi valeurs
mnt-lower	liste de <mntner-name>	facultatif, multi valeurs
mnt-routes	liste de <mntner-name> [{liste de <ipv6-address-prefix-range>} ou ANY]	facultatif, multi valeurs

Exemple :
route6: 2001:0DB8::/32
origin: AS65001

4. Mise à jour des classes existantes pour prendre en charge les extensions

4.1 Classe as-set

La classe as-set définit un ensemble de systèmes autonomes (AS, *Autonomous System*), spécifiés soit directement par leur liste dans les attributs membres soit indirectement par référence à un autre as-set ou en utilisant la facilité mbrs-by-ref. Plus important, "dans un contexte qui attend un ensemble de chemins (par exemple, les attributs membres de la classe route-set), [...] un AS-X as-set définit l'ensemble de chemins qui ont leur origine par les AS dans AS-X", (paragraphe 5.3 de la [RFC2622]).

La classe as-set est donc utilisée pour collecter un ensemble de préfixes de chemins, qui peut être restreint à une famille d'adresses spécifique.

La classe as-set existante n'a besoin d'aucune modification. L'évaluation de la classe doit être filtrée pour obtenir les préfixes qui appartiennent à une famille d'adresses particulière en utilisant le mécanisme traditionnel de filtrage en usage dans le système actuel de registre des acheminements de l'Internet (IRR, *Internet Routing Registry*).

4.2 Classe route-set

Cette classe est utilisée pour spécifier un ensemble de préfixes de chemins.

Un nouvel attribut "mp-members:" est défini pour cette classe. Cet attribut permet la spécification des gammes de préfixes d'adresses (address-prefix-ranges) IPv4 ou IPv6.

Attribut	Valeur	Type
mp-members	liste de (<ipv4-address-prefix-range> ou <ipv6-address-prefix-range> ou <route-set-name> ou <route-set-name><range-operator>)	facultatif, multi valeurs

Exemple :
route-set: rs-foo
mp-members: rs-bar
mp-members: 2001:0DB8::/32 # v6 member
mp-members: 192.0.2.0/24 # v4 member

4.3 Classe filter-set

Le nouvel attribut "mp-filter:" définit le filtre de politique de l'ensemble. Un filtre de politique est une expression logique qui, lorsque elle est appliquée à un ensemble de chemins retourne un sous ensemble de ces chemins. Les parts pertinentes de la classe filter-set mise à jour sont indiquées ci-dessous :

Attribut	Valeur	Type
filter-set	<object-name>	obligatoire, valeur unique, clé de classe
filter	<filter>	facultatif, valeur unique
mp-filter	<mp-filter>	facultatif, valeur unique

Où <mp-filter> est défini au paragraphe 2.5.2. Bien que les attributs "filter:" et "mp-filter:" soient de type "facultatif", un filter-set doit contenir un de ces deux attributs. Les mises en œuvre devraient rejeter les instances où les deux attributs sont définis dans un objet, car l'interprétation d'un tel filter-set est indéfinie.

4.4 Classe peering-set

La classe peering-set est mise à jour avec un attribut "mp-peering:".

Attribut	Valeur	Type
peering-set	<object-name>	obligatoire, valeur unique, clé de classe
peering	<peering>	facultatif, multi valeurs
mp-peering	<mp-peering>	facultatif, multi valeurs

Exemple :peering-set: prng-ebgp-peers
mp-peering: AS65002 2001:0DB8::1 at 2001:0DB8::2

Avec <mp-peering> défini au paragraphe 2.5.1. Bien que les attributs "peering:" et "mp-peering:" soient du type "facultatif", un peering-set doit contenir au moins un de ces deux attributs.

4.5 Classe inet-rtr

Deux nouveaux attributs sont introduits dans la classe inet-rtr ; "interface:", qui permet la définition d'interfaces génériques, incluant les informations précédemment contenues dans l'attribut "ifaddr:", ainsi que la prise en charge des définitions de tunnel, et "mp-peer:", qui inclut et étend la fonctionnalité de l'attribut "peer:" existant. La définition de la syntaxe de l'attribut "interface:" est la suivante :

Attribut	Valeur	Type
interface	<ipv4-address> ou <ipv6-address> masklen <mask> [action <action>] [tunnel <remote-endpoint-address>,<encapsulation>]	facultatif, multi valeurs

La syntaxe permet des définitions d'interfaces natives IPv4 et IPv6, ainsi que la définition de tunnels comme interfaces

virtuelles. Sans la définition de tunnel facultatif, cet attribut permet la même fonctionnalité que l'attribut "ifaddr:" mais l'étend pour permettre les adresses IPv6.

Si l'interface est un tunnel, la syntaxe est la suivante :
<remote-endpoint-address> indique l'adresse IPv4 ou IPv6 du point d'extrémité distant du tunnel. La famille d'adresses doit correspondre à celle du point d'extrémité local. <encapsulation> note l'encapsulation utilisée dans le tunnel et est une de {GRE,IPinIP} (noter que les versions externe et interne de protocole IP peuvent être déduites du contexte d'interface -- par exemple, l'encapsulation IPv6 dans IPv4 est juste IPinIP). Les politiques d'acheminement pour ces routeurs devraient être décrites dans les classes appropriées (par exemple, aut-num).

L'attribut "mp-peer:" est défini ci-dessous. La différence entre cet attribut et l'attribut "peer:" est l'inclusion de la prise en charge des adresses IPv6.

Attribut	**Valeur**	**Type**
mp-peer	<protocol> <ipv4-address> <options> ou <protocol> <ipv6-address> <options> ou <protocol> <inet-rtr-name> <options> ou <protocol> <rtr-set-name> <options> ou <protocol> <peering-set-name> <options>	facultatif, multi valeurs

où <protocol> est un nom de protocole, et <options> est une liste séparée par des virgules d'options d'échange de trafic pour <protocol>, comme fournie dans le dictionnaire RPSL.

4.6 Classe rtr-set

La classe rtr-set est étendue par un nouvel attribut, "mp-members:". Cet attribut étend l'attribut "members:" d'origine en permettant la spécification des adresses IPv6. Il est défini comme suit :

Attribut	**Valeur**	**Type**
mp-members	liste de (<inet-rtr-name> ou <rtr-set-name> ou <ipv4-address> ou <ipv6-address>)	facultatif, multi valeurs

5. Extensions à la RFC 2725

La [RFC2725] introduit un modèle d'autorisation pour traiter de l'intégrité de la politique exprimée dans les registres des acheminements. Deux nouveaux attributs ont été définis pour prendre en charge ce modèle d'autorisation :"mnt-routes" et "mnt-lower".

Dans RPSLng, ces attributs sont étendus aux classes route6 et inet6num (décrites ci-dessous). De plus, la syntaxe de l'attribut mnt-routes existant est modifiée pour permettre la spécification facultative des listes de gammes de préfixe IPv6 lorsque elles sont présentes dans les objets de classe inet6num, route6, et aut-num. Cette liste facultative de gammes de préfixes est une liste séparée par des virgules incluses entre des accolades. Dans la classe aut-num, les gammes de préfixes IPv6 peuvent être mêlées à des gammes de préfixes IPv4. Le mot clé "ANY" peut aussi être utilisé à la place des gammes de préfixes. Dans le cas des objets inet6num et route6, "ANY" se réfère à tous les préfixes les plus spécifiques dans le champ de clé de classe. Pour la classe aut-num, "ANY" signifie littéralement n'importe quel préfixe. Lorsque aucun élément d'ensemble supplémentaire n'est spécifié, la valeur par défaut est "ANY". Une définition abrégée de la classe aut-num avec la syntaxe mise à jour pour l'attribut mnt-routes est présentée ci-dessous.

Attribut	**Valeur**	**Type**
aut-num	<as-number>	obligatoire, clé de classe, valeur unique
mnt-routes	liste de <mntner-name> [{liste de (<ipv6-address-prefix-range> ou <ipv4-address-prefix-range>)} ou ANY]	facultatif, multi valeurs

Voici un exemple d'utilisation de mnt-routes. Cet exemple autorise MAINT-65001 à créer des objets route6 avec un AS d'origine de 65002 pour des préfixes d'adresses IPv6 dans la gamme 2001:0DB8::/32^+, et des objets de chemin avec l'AS 65002 comme origine pour les préfixes IPv4 dans la gamme 192.0.2.0/24^+.

aut-num: AS65002
mnt-routes: MAINT-AS65001 {2001:0DB8::/32^+, 192.0.2.0/24^+}

Note : l'inclusion des gammes de préfixes IPv6 dans un attribut mnt-routes dans un objet aut-num peut entrer en conflit

avec les mises en œuvre existantes de RPSL qui ne prennent en charge que les gammes de préfixes IPv4. Cependant, étant donné la rareté des mises en œuvre rapportées de cette gamme de préfixes facultative, il a été considéré qu'il était plus acceptable d'étendre la définition existante de l'attribut mnt-routes dans la classe aut-num plutôt que de créer un nouveau type d'attribut.

Attribut	**Valeur**	**Type**
inet6num	<ipv6-address-prefix>	obligatoire, valeur unique, clé de classe
netname	<netname>	obligatoire, valeur unique
descr	<free-form>	obligatoire, multi valeurs
country	<country-code>	obligatoire, multi valeurs
admin-c	<nic-handle>	obligatoire, multi valeurs
tech-c	<nic-handle>	obligatoire, multi valeurs
remarks	<free-form>	facultatif, multi valeurs
notify	<email-address>	facultatif, multi valeurs
mnt-lower	liste de <mntner-name>	facultatif, multi valeurs
mnt-routes	liste de <mntner-name> [{liste de <ipv6-address-prefix-range>} ou ANY]	facultatif, multi valeurs
mnt-by	liste de <mntner-name>	obligatoire, multi valeurs
changed	<email-address> <date>	obligatoire, multi valeurs
source	<registry-name>	obligatoire, valeur unique

Le <country-code> doit être un identifiant valide de code de pays à deux lettres ISO 3166. <netname> est un nom symbolique pour l'espace d'adresse IPv6 spécifié. Il n'a pas de restriction sur les préfixes RPSL réservés. Ces définitions sont tirées du Manuel de référence de base de données RIPE [RIPE].

5.1 Modèle d'autorisation pour les objets route6

La suppression et la mise à jour d'un objet route6 ne sont pas différentes de celles des autres objets, comme défini dans la [RFC2725]. Les règles de création d'un objet route6 sont répétées ici d'après les règles correspondantes pour l'objet route au paragraphe 9.9 de la [RFC2725].

Lorsque un objet route6 est ajouté, la soumission doit satisfaire à deux critères d'authentification. Il doit correspondre à l'authentification spécifiée dans l'objet aut-num et à celle spécifiée soit dans un objet route6, soit, si aucun objet route6 ne se trouve applicable, un objet inet6num.

Un ajout est soumis avec un numéro d'AS et un préfixe IPv6 comme clé. Si l'objet aut-num n'existe pas sur un route6 à ajouter, l'ajout est alors rejeté. Si le aut-num existe, la soumission est alors vérifiée par rapport aux mainteneurs applicables. Une recherche est alors effectuée sur le préfixe, en cherchant d'abord une correspondance exacte, et ensuite, faute de celle-ci, pour la plus longue correspondance de préfixe moins spécifique que celui spécifié. Si la recherche aboutit, elle va retourner un ou plusieurs objets route6. La soumission doit correspondre à un mainteneur applicable dans au moins un de ces objets route6 pour que l'ajout réussisse. Si la recherche d'un objet route6 échoue, une recherche est alors effectuée pour un objet inet6num qui corresponde exactement au préfixe, ou pour le inet6num le plus spécifique moins spécifique que la soumission de l'objet route6.

Une fois que le aut-num et soit une liste d'objets route6, soit un inet6num sont trouvés, l'autorisation est prise de ces 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 ou mnt-lower ne sont pas pris en compte. En l'absence d'un attribut mnt-routes dans un certain objet, les premiers attributs mnt-lower sont utilisés (seulement si l'objet considéré est un objet inet6num et si il est moins spécifique que l'objet route6 à ajouter). Si aucun attribut mnt-lower applicable n'est trouvé, les attributs mnt-by sont alors utilisés pour cet objet. L'authentification doit correspondre à une des autorisations dans chacun des deux objets.

6. Considérations sur la sécurité

Le présent document décrit des extensions à la [RFC2622] et à la [RFC2725]. Les extensions visent les limitations des documents susmentionnés par rapport à IPv6 et à la diffusion groupée. Les extensions n'introduisent aucune nouvelle fonctionnalité ou menace pour la sécurité.

Bien que les extensions n'introduisent aucune menace supplémentaire pour la sécurité, on devrait noter que la norme RPSL originale [RFC2622] incluait plusieurs mécanismes d'authentification faibles et/ou vulnérables : d'abord, le schéma "MAIL-

FROM", qui peut facilement être défait via une usurpation d'adresse de source de messagerie électronique ; ensuite, le schéma "CRYPT-PW", qui est l'objet d'attaques de dictionnaire et de capture de mot de passe si les objets RPSL sont soumis via des canaux non cryptés comme ceux de la messagerie électronique, et enfin, le mécanisme "NONE", qui n'offre pas de protection aux objets.

7. Remerciements

Les auteurs souhaitent remercier toues les personnes qui ont contribué au présent document à travers de nombreuses discussions, en particulier Ekaterina Petrusha, pour ses très précieuses discussions et suggestions, Shane Kerr, Engin Gunduz, Marc Blanchet, et David Kessens qui ont participé de façon constructive à de nombreuses discussions et Cengiz Alaettinoglu, qui est toujours la référence dans tout ce qui concerne RPSL.

8. Références

8.1 Références normatives

[RFC2622] C. Alaettinoglu et autres, "Langage de spécification de politique d'acheminement (RPSL)", juin 1999. (*MàJ par* RFC4012) *(P.S.)*

[RFC2725] C. Villamizar et autres, "Sécurité du système de politique d'acheminement", décembre 1999. (*MàJ par* RFC4012) *(P.S.)*

[RFC3513] R. Hinden et S. Deering, "Architecture d'adressage du protocole Internet version 6 (IPv6)", avril 2003. (*Obs. voir* RFC4291)

8.2 Références pour information

[RIPE] Damas, J. and A. Robachevsky, "RIPE Database Reference Manual", août 2002.

Adresse des auteurs

Larry Blunk
Merit Network
mél : ljb@merit.edu

Joao Damas
Internet Systems Consortium
mél : Joao_Damas@isc.org

Florent Parent
Hexago
mél : Florent.Parent@hexago.com

Andrei Robachevsky
RIPE NCC
mél : andrei@ripe.net

Déclaration complète de droits de reproduction

prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

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

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

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