

Groupe de travail Réseau
Request for Comments : 4570
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle, septembre 2007

B. Quinn, BoxnArrow.com
R. Finlayson, Live Networks, Inc.
juillet 2006

Filtres de source du protocole de description de session (SDP)

Statut de ce mémoire

Le présent document spécifie un protocole de normalisation de l'Internet pour la communauté de l'Internet, qui appelle à la discussion et à des suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Normes de protocole officielles de l'Internet" (STD 1) sur l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright

Copyright (C) The Internet Society (2006).

Résumé

Le présent document décrit comment adapter le protocole de description de session (SDP, *Session Description Protocol*) pour exprimer une ou plusieurs adresses de source comme un filtre de source pour une ou plusieurs adresses "connexion" de destination. Il définit la syntaxe et la sémantique d'un attribut SDP "filtre de source" qui peut faire référence à une ou des adresses IPv4 ou IPv6 comme liste inclusive ou exclusive de sources pour des destinations en diffusion groupée ou en envoi individuel. En particulier, un filtre de source inclusif peut être utilisé pour spécifier une session en diffusion groupée spécifique de source (SSM, *Source-Specific Multicast*).

1 Introduction

Le protocole de description de session [SDP] fournit un format d'utilisation générale pour décrire les sessions multimédia en annonces ou invitations. SDP utilise un format de données entièrement textuel (le sous-ensemble US-ASCII de [UTF-8]) pour maximiser la portabilité dans le transport. SDP ne définit pas un protocole, mais seulement la syntaxe pour décrire une session multimédia avec des informations suffisantes pour découvrir la session et y participer. Les descriptions de session peuvent être envoyées en utilisant un nombre quelconque de protocoles d'application existants pour le transport (par exemple, le protocole d'annonce de session (SAP), SIP, le protocole de diffusion en temps réel (RTSP), la messagerie électronique, et HTTP).

Normalement, les descriptions de session font référence à une adresse IP en diffusion groupée pour l'"adresse de connexion" (destination), à travers des adresses en envoi individuel, mais des noms de domaine pleinement qualifiés (FQDN) PEUVENT aussi être utilisés. L'attribut "filtre de source" défini dans le présent document qualifie le trafic de session en identifiant l'adresse (ou le FQDN) des sources légitimes (envoyeurs). L'intention est que les receveurs utilisent la ou les paires d'adresse de source et de destination pour filtrer le trafic, de sorte que les applications ne reçoivent que le trafic de session légitime.

Les applications qui reçoivent sont supposées utiliser les informations de filtre de source SDP pour identifier le trafic provenant des envoyeurs légitimes, et éliminer le trafic provenant d'envoyeurs illégitimes. Les applications et les hôtes peuvent aussi partager les informations de filtre de source avec des éléments de réseau (par exemple, avec les routeurs qui utilisent [IGMPv3]) afin qu'ils aient la capacité d'effectuer les opérations de filtrage de trafic plus "en amont," plus près de la ou des sources.

L'attribut "filtre de source" peut apparaître au niveau session et/ou au niveau du support.

1.1 Motivation

L'objet d'un filtre de source est d'aider à protéger les receveurs contre le trafic envoyé d'adresses de source illégitimes. Filtrer le trafic peut aider à préserver l'intégrité des contenus et protéger contre les attaques de déni de service (DoS).

Pour les adresses de destination en diffusion groupée, les applications qui reçoivent PEUVENT appliquer les filtres de source en utilisant les API de filtre en diffusion groupée [MSF-API, *Multicast Source Filter API*]. Les hôtes mettront vraisemblablement en œuvre ces API en utilisant des mécanismes du protocole pour acheminer les filtres de source aux routeurs locaux de diffusion groupée. D'autres routeurs en diffusion groupée "amont" PEUVENT appliquer les filtres et fournir par là une gestion explicite de groupe de diffusion et une utilisation efficace des ressources du réseau. Les mécanismes de protocole pour activer ces opérations vont au delà du domaine d'application du présent document, mais leur potentiel est un des motifs des filtres de source SDP.

2 Terminologie

Dans le présent document, les mots clé "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14 [RFC2119].

3 L'attribut "filtre de source"

L'attribut SDP de filtre de source ne change rien à la syntaxe ou sémantique SDP existante, mais définit un format pour les informations supplémentaires de description de session. En particulier, la syntaxe de filtre de source peut prescrire une ou plusieurs adresses en diffusion groupée comme des sources légitimes ou illégitimes pour une (ou toutes) les valeurs de champ "adresse de connexion" des descriptions de session SDP.

Noter que les adresses de source en diffusion groupée spécifiées par cet attribut sont celles qui sont vues par un receveur. Donc, si les adresses de source subissent une traduction en route entre l'expéditeur original et le receveur – par exemple, du fait d'un traducteur d'adresses réseau (NAT, *Network Address Translator*) ou d'un mécanisme de tunnelage – l'attribut SDP "filtre de source", tel que présenté au receveur, ne sera pas juste, à moins que les adresses de source qui y sont ne soient elles aussi traduites en conséquence.

L'attribut filtre de source a la syntaxe suivante :

```
a=source-filter: <filter-mode> <filter-spec>
```

Le <filter-mode> est soit "incl" soit "excl" (respectivement pour inclusion ou exclusion). Le <filter-spec> a quatre sous-composants :

```
<nettype> <address-types> <dest-address> <src-list>
```

Un <filter-mode> de "incl" signifie qu'un paquet entrant n'est accepté que si son adresse de source est dans l'ensemble spécifié par <src-list>. Un <filter-mode> de "excl" signifie qu'un paquet entrant est rejeté si son adresse de source est dans l'ensemble spécifié par <src-list>.

Le premier sous champ, <nettype>, indique le type de réseau, car SDP est indépendant du protocole. Le présent document est le plus pertinent avec la valeur "IN", qui désigne le protocole Internet.

Le second sous champ, <address-types>, identifie la famille d'adresses, et pour les besoins de ce document peut avoir les valeurs de <addrtype> "IP4" ou "IP6". Autrement, lorsque <dest-address> est un FQDN, la valeur PEUT être "*" pour s'appliquer aux deux types d'adresses, car l'un ou l'autre type d'adresse peut être retourné d'une recherche DNS.

Le troisième sous champ, <dest-address>, est l'adresse de destination, qui DOIT correspondre à une ou plusieurs des valeurs de champ "adresse de connexion" de la session. Il peut être une adresse en envoi individuel ou groupée, un FQDN, ou le caractère générique "*" pour correspondre à n'importe laquelle ou toutes les valeurs de "adresse de connexion" de la session.

Le quatrième sous champ, <src-list>, est la liste des hôtes/interfaces de source dans le filtre de source, et consiste en une ou plusieurs adresses en diffusion groupée ou FQDN, séparées par des caractères espace.

Le format et le contenu de ces éléments de sémantique sont déduits de ceux définis dans [SDP] et leur sont compatibles. Pour des précisions, voir l'appendice A du présent document.

3.1 Règles de traitement

Un certain nombre de détails sont à prendre en considération pour l'analyse de la syntaxe du filtre de source SDP.

La valeur <dest-address> dans un attribut a "filtre de source" DOIT correspondre à une valeur de <connection-field> existante dans la description de session. La seule exception est lorsque un caractère générique "*" est utilisé pour indiquer que le filtre de source s'applique à toutes les valeurs de <connection-field>.

Lorsque la valeur <dest-address> est une adresse en diffusion groupée, la valeur du champ NE DOIT PAS inclure les sous champs <ttl> et <number of addresses> tirés de la valeur <connection-address>. Si <connection-address> spécifie plus d'une adresse en diffusion groupée (dans le champ <number of addresses>) un filtre de source, si il en est, doit être établi explicitement pour chacune de ces adresses, en utilisant une ligne "a=source-filter" séparée pour chaque adresse (sauf si un caractère générique "*" est utilisé pour <dest-address>). Voir un exemple au paragraphe 3.2.4.

Lorsque la valeur <addrtype> est le caractère générique "*", la <dest-address> DOIT être soit un FQDN soit un "*" (c'est-à-dire qu'il NE DOIT PAS être une adresse IPv4 ou IPv6). Voir un exemple au paragraphe 3.2.6.

Comme cela a toujours été le cas, le comportement par défaut lorsqu'un attribut de filtre de source n'est pas fourni dans une description de session est que tout le trafic envoyé à la valeur spécifiée de <connection-address> devrait être accepté (c'est-à-dire, de toute adresse de source). La grammaire de filtre de source ne comporte pas de syntaxe pour exprimer "n'exclure aucun" ou "inclure tout."

Comme le <connection-field> standard décrit dans [SDP], la localisation de l'attribut "filtre de source" détermine si il s'applique à la session entière ou seulement à un support spécifique (c'est-à-dire, "niveau session" ou "niveau support"). Un filtre de source de niveau support supplantera toujours complètement un filtre de source de niveau session.

Il n'est pas nécessaire qu'un "filtre de source" soit localisé au même niveau hiérarchique que son <connection-field> correspondant. Ainsi, un <source-filter> de niveau support peut faire référence à une valeur de <connection-field> de niveau session, et un "filtre de source" de niveau session peut être appliqué à toutes les valeurs de <connection-field> de niveau support correspondantes. Voir un exemple au paragraphe 3.2.3.

Une description SDP NE DOIT PAS contenir plus d'un attribut "filtre de source" de niveau session qui couvre la même adresse de destination, ou plus d'un attribut "filtre de source" de niveau support qui couvre la même adresse de destination.

Il n'est pas spécifié de limite au nombre d'entrées admises dans la <src-list> ; cependant, il y a des limites pratiques qui devraient être prises en considération. Par exemple, selon le transport à utiliser pour la description de session, il peut y avoir une limite de la taille totale de la description de session (par exemple, déterminée par la charge utile maximum dans un datagramme). Aussi, lorsque le filtre de source s'applique aux protocoles de commande, il peut y avoir une limite au nombre d'adresses de source qui peuvent être envoyées. Ces limites sont en dehors du domaine d'application du présent document, mais devraient être prises en considération lors de la définition des valeurs de filtre de source pour SDP.

3.2 Exemples

Voici un certain nombre d'exemples qui illustrent comment utiliser l'attribut filtre de source dans certains scénarios courants. On utilise les composants de description de session comme point de départ des exemples qui suivent. Pour chaque exemple, on montre le filtre de source avec les informations supplémentaires pertinentes et on donne une brève explication.

```
<session-description> =
  v=0
  o=The King <Elvis@example.com>
  s=Elvis en personne
  i=Tout Elvis, tout le temps
  u=http://www.example.com/ElvisLive/
  t=0 0
  a=recvonly
  <media-description 1> = m=audio 54320 RTP/AVP 0   <media-description 2> = m=video 54322 RTP/AVP 34
```

3.2.1 Exemple de diffusion groupée spécifique de source

Les adresses en diffusion groupée dans la gamme diffusion groupée spécifique de source (SSM, *Source-Specific Multicast*) exigent une seule adresse d'expéditeur en envoi individuel pour chaque destination en diffusion groupée, de sorte que la spécification de filtre de source donne une correspondance naturelle. Dans cet exemple, un membre de la session devrait recevoir seulement le trafic envoyé de 192.0.2.10 à l'adresse de session en diffusion groupée 232.3.4.5.

```
<session-description>
c=IN IP4 232.3.4.5/127
a=source-filter: incl IN IP4 232.3.4.5 192.0.2.10
<media-description 1>
```

Cet exemple de filtre de source utilise une liste d'inclusion avec une seule "adresse de connexion" en diffusion groupée comme destination et une seule adresse en envoi individuel comme source. Noter que la valeur de l'adresse de connexion correspond à la valeur spécifiée dans connection-field.

Noter aussi que comme le champ connexion est situé dans la section de description de session, le filtre de source s'applique à tous les supports.

De plus, si la description SDP spécifie une session RTP (par exemple, sa ou ses lignes "m=" spécifient "RTP/AVP" comme protocole de transport) la spécification "incl" ne s'appliquera alors pas qu'aux paquets RTP, mais aussi à tous les paquets RTCP qui sont envoyés à l'adresse de diffusion groupée spécifiée. Cela signifie que, par suite de la spécification de "incl", les seuls paquets RTCP en diffusion groupée possibles seront des paquets "Rapport d'envoi" (SR) envoyés depuis l'adresse de source spécifiée.

A cause de cela, une description SDP pour une session RTP en diffusion groupée à source spécifiée (SSM, *Source-Specific Multicast*) DEVRAIT aussi inclure un attribut =rtcp-unicast ... , comme décrit dans [RTCP-SSM] (paragraphe 10.1). Cela spécifie que les paquets RTCP "Rapport de réception" (RR) sont à renvoyer via une adresse d'envoi individuel.

3.2.2 Exemple d'exclusion de envoi individuel

Normalement, une valeur <connection-address> de session SDP est une adresse de diffusion groupée, bien qu'il soit aussi possible d'utiliser soit une adresse d'envoi individuel soit un FQDN. Cet exemple illustre un scénario dans lequel une description de session indique l'adresse de source d'envoi individuel 192.0.2.10 dans un filtre d'exclusion. En effet, cet échantillon de filtre de source dit : "la destination 192.0.2.11 devrait accepter le trafic de toute provenance *excepté* 192.0.2.10."

```
<session-description>
  c=IN IP4 192.0.2.11
  a=source-filter: excl IN IP4 192.0.2.11 192.0.2.10
  <media-description 1>
```

3.2.3 Exemple d'adresse de session multiple

Cet exemple de filtre de source utilise la valeur de caractère générique "*" pour <dest-addr> qui correspond à toutes valeurs de <connection-address>. Et donc, la seule source légitime de trafic envoyé aux adresses de diffusion groupée 232.2.2.2 ou 232.4.4.4 est 192.0.2.10. Le trafic envoyé à partir de toute autre adresse de source en envoi individuel devrait être éliminée par le receveur.

```
<session-description>
  a=source-filter: incl IN IP4 * 192.0.2.10

<media-description 1>
  c=IN IP4 232.2.2.2/127

<media-description 2>
  c=IN IP4 232.4.4.4/63
```

3.2.4 Exemple d'adresse en diffusion groupée multiple

Dans cet exemple, <connection-address> spécifie trois adresses en diffusion groupée : 224.2.1.1, 224.2.1.2, et 224.2.1.3. La première et la troisième de ces adresses sont des filtres de source donnés. Cependant, dans cet exemple la seconde adresse - 224.2.1.2 - n'est *pas* un filtre de source donné.

```
<session-description>
c=IN IP4 224.2.1.1/127/3
a=source-filter: incl IN IP4 224.2.1.1 192.0.2.10
a=source-filter: incl IN IP4 224.2.1.3 192.0.2.42
<media-description 1>
```

3.2.5 Exemple de filtre de source IPv6 en diffusion groupée

Ce simple exemple définit un seul filtre de source de niveau session qui fait référence à une seule paire de source et destination de diffusion groupée IPv6. Le trafic IP en diffusion groupée envoyé à FFOE::11A n'est valide qu'à partir de l'adresse de source en envoi individuel 2001:DB8:1:2:240:96FF:FE25:8EC9.

```
<session-description>
c=IN IP6 FF0E::11A/127
a=source-filter incl IN IP6 FF0E::11A 2001:DB8:1:2:240:96FF:FE25:8EC9
<media-description 1>
```

3.2.6 Exemple de FQDN IPv4 et IPv6

Cet exemple illustre l'utilisation du caractère générique "*" <addrtype>, en conjonction avec des FQDN en diffusion groupée et en source qui peuvent se résoudre en adresses IPv6 ou IPv4, ou les deux. Bien que normalement les adresses en diffusion groupée et de source soient les mêmes (soit toutes deux IPv4 soient toutes deux IPv6), l'utilisation du caractère générique pour addrtype dans le filtre de source permet une asymétrie entre les deux adresses (ainsi une adresse de source IPv4 peut être utilisée avec une adresse IPv6 en diffusion groupée).

```
<session-description>
  c=IN IP4 channel-1.example.com/127
  c=IN IP6 channel-1.example.com/127
  a=source-filter: incl IN * channel-1.example.com src-1.example.com
<media-description 1>
```

3.3 Considérations sur le modèle offre-réponse

L'attribut "filtre de source" n'est pas destiné à être utilisé comme 'offre' dans un échange offre-réponse de SDP [OFFER], parce que les ensembles d'adresses de source ne représentent pas des 'capacités' ou des 'limitations' de l'offreur, et parce que l'offreur n'a pas, en général, une connaissance a priori de la ou des adresses de source IP qui seront incluses dans une réponse. Alors que celui qui répond peut inclure l'attribut "filtre de source" dans sa réponse (par exemple pour désigner une session SSM), celui qui répond DEVRAIT ignorer tout attribut "filtre de source" présent dans l'offre d'origine.

4 Problèmes d'interaction

Définir une liste de sources légitimes pour une adresse de destination en diffusion groupée représente une déviation du modèle de diffusion groupée à partir de toute source (ASM, *Any-Source Multicast*), tel que défini à l'origine dans [IGMPv1]. Le modèle ASM accepte les expéditeurs anonymes et tous les types d'applications de diffusion groupée (par exemple, de beaucoup à beaucoup). L'utilisation d'un filtre de source exclut certains envoyeurs (inconnus ou indésirables), et se prête plus à des applications de diffusion groupée du type un à beaucoup ou peu à peu.

Bien que ces deux modèles aient des caractéristiques et exigences de fonctionnement contrastées, ils peuvent coexister sur le même réseau en utilisant les mêmes protocoles. L'utilisation de filtres de source ne modifie pas la sémantique d'ASM mais permet plus de contrôle de la part des receveurs, à leur discrétion.

5 Considérations pour la sécurité

Voir [SDP] pour des considérations sur la sécurité spécifiques du protocole de description de session en général. La question centrale pertinente pour l'utilisation des filtres d'adresse de source est la question de l'authenticité de l'adresse.

L'utilisation de l'adresse IP de source pour l'authentification est faible, car l'adresses est souvent allouée de façon

dynamique et il est possible à un envoyeur de "parodier" son adresse de source (c'est-à-dire, d'utiliser une autre que la sienne) dans les datagrammes qu'il envoie. Une configuration de routeur appropriée peut cependant réduire la vraisemblance d'envoi d'adresses parodiées vers ou à partir d'un réseau. En particulier, il est recommandé que des routeurs frontière filtrent le trafic de sorte que les datagrammes qui ont des adresses de source invalides ne soient pas transmis (c'est-à-dire que les routeurs abandonnent les datagrammes si l'adresse de source n'est pas locale) [RFC2827]. Ceci n'empêche cependant pas que les adresses de source IP soient parodiées sur un réseau de zone locale (LAN, *Local Area Network*).

Aussi, comme noté à la section 3 ci-dessus, les mécanismes de tunnelage ou de NAT peuvent exiger une traduction correspondante des adresses spécifiées dans l'attribut "filtre de source" SDP, et de plus, peuvent causer la traduction d'un ensemble d'adresses de source originales en un plus petit ensemble d'adresses de source vu par le receveur.

L'utilisation de FQDN pour des valeurs de <dest-address> ou de <src-list> donne une couche d'adressage indirect qui procure une grande souplesse. Cependant, elle expose aussi le filtre de source à tous les inconvénients pour la sécurité que peut avoir le système DNS. S'il n'est pas sécurisé, il est concevable que le serveur DNS puisse retourner des adresses illégitimes.

De plus, si le filtrage de source est mis en œuvre avec le partage des informations du filtre de source avec des éléments de réseau, la sécurité du ou des protocoles qui sont utilisés pour cela (par exemple, [IGMPv3]) devient alors importante pour s'assurer que le trafic légitime (et seulement le trafic légitime) est reçu.

Pour ces raisons, les receveurs NE DEVRAIENT PAS traiter l'attribut SDP "filtre de source" comme étant le seul mécanisme de protection de l'intégrité des contenus reçus.

6 Considérations relatives à l'IANA

Comme recommandé par [SDP] (Appendice B), le nouveau nom d'attribut "source-filter" a été enregistré auprès de l'IANA, comme suit :

Les informations de contact suivantes doivent être utilisées pour tous les enregistrements inclus ici :

Contact : Ross Finlayson
mél : finlayson (at) live555.com
Téléphone : 650-254-1184

Attribut SDP ("att-field"):

Nom d'attribut : source-filter
Forme longue : Source Filter
Type de nom : att-field
Type d'attribut : Niveau session ou niveau support
Soumis à charset : Non
Objet : Voir le présent document
Référence : Le présent document
Valeurs : Voir le présent document, et les enregistrements ci-dessous

7 Remerciements

Les auteurs remercient Dave Thaler et Mark Handley, dont les contributions ont apporté beaucoup de la substance de ce document. Magnus Westerlund a aussi fourni des commentaires précieux pour son édition.

8 Références normatives

- [RFC4234] Crocker, D., Ed. et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", octobre 2005.
- [RFC2119] Bradner, S., "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [SDP] Handley, M., Jacobson, V., et C. Perkins, "SDP : Protocole de description de session", RFC4566, juillet 2006.
- [UTF-8] Yergeau, F., "UTF-8, format de transformation de ISO 10646", STD 63, RFC3629, novembre 2003.

9 Références informatives

- [RFC2827] Ferguson, P. et D. Senie, "Filtrage de l'entrée du réseau" : Combattre les attaques de déni de service qui utilisent la parodie d'adresse de source IP", BCP 38, mai 2000.
- [IGMPv1] Deering, S., "Extensions d'hôte pour la diffusion groupée IP", STD 5, RFC1112, août 1989.
- [IGMPv3] Cain, B., Deering, S., Kouvelas, I., Fenner, B., et A. Thyagarajan, "Protocole de gestion de groupe sur Internet, version 3", RFC3376, octobre 2002.
- [MSF-API] Thaler, D., Fenner, B., et B. Quinn, "Extensions d'interface de prise pour les filtres de source en diffusion groupée", RFC3678, janvier 2004.
- [OFFER] Rosenberg, J. et H. Schulzrinne, "Modèle d'offre/réponse avec le protocole de description de session (SDP)", RFC3264, juin 2002.
- [RTCP-SSM] Chesterfield, J., E. Schooler, J. Ott, "Extensions RTCP pour sessions en diffusion groupée à une seule source avec rétroaction en envoi individuel", Travail en cours, octobre 2004.
- [SSM] Bhattacharyya, S., "Généralités sur la diffusion groupée spécifique d'une source (SSM)", RFC3569, juillet 2003.

Appendice A Syntaxe de l'attribut Filtre de source

Le présent appendice donne une grammaire de BNF augmenté [RFC4234] pour exprimer une liste d'exclusion ou d'inclusion d'une ou plusieurs adresses (IPv4 ou IPv6) en envoi individuel. Il est vu comme une extension de la grammaire pour le protocole de description de session, comme défini dans [SDP]. Il décrit en particulier la syntaxe pour le nouveau champ d'attribut "filtre de source", qui PEUT être un attribut de niveau session ou de niveau support.

La valeur de "dest-address" dans chaque champ de filtre de source DOIT correspondre à une valeur existante de champ de connexion, sauf si la valeur de caractère générique d'adresse de connexion "*" est spécifiée.

source-filter = "source-filter" ":" SP filter-mode SP filter-spec
; SP est le caractère ASCII 'espace' (0x20, défini dans la [RFC4234]).

filter-mode = "excl" / "incl"
; soit mode exclusion soit mode inclusion.

filter-spec = nettype SP address-types SP dest-address SP src-list
; nettype est défini dans [SDP].

address-types = "*" / addrtype
; "*" pour tous les types d'adresse (IP4 et IP6), mais seulement quand <dest-address> et <src-list>
; se réfèrent à des FQDN. addrtype est défini dans [SDP].

dest-address = "*" / basic-multicast-address / unicast-address
; "*" s'applique à toutes les valeurs d'adresse de connexion. unicast-address est défini dans [SDP].

src-list = *(unicast-address SP) unicast-address
; une ou plusieurs adresses de source en envoi individuel (en notation ASCII standard IPv4 ou IPv6)
; ou FQDN. unicast-address est défini dans [SDP].

basic-multicast-address = basic-IP4-multicast / basic-IP6-multicast / FQDN / extn-addr
; c'est-à-dire, comme multicast-address définie dans [SDP], sauf que les champs
; /<tt> et /<number of addresses> ne sont pas inclus. FQDN et extn-addr sont définis dans [SDP].

basic-IP4-multicast = m1 3("." decimal-uchar)
; m1 et decimal-uchar sont définis dans [SDP].

basic-IP6-multicast = hexpart
; hexpart est défini dans [SDP].

Adresse des auteurs

Bob Quinn
BoxnArrow.com
31 Caldwell Road

Ross Finlayson
Live Networks, Inc.
650 Castro St., suite 120-196

Waltham, MA 02453
téléphone : 781-577-1539
mél : rcq@boxnarrow.com

Mountain View, CA 94041
mél : finlayson@live555.com

Déclaration de droit de reproduction

Copyright (C) The Internet Society (2006).

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

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

Propriété intellectuelle

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

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

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

Remerciement

Le financement de la fonction d'édition des RFC est fourni par la Administrative Support Activity (IASA) de l'IETF.