Groupe de travail Réseau
Request for Comments : 3417
STD : 62
RFC rendue obsolète : 1905
Catégorie : Norme

Traduction Claude Brière de L'Isle

Éditeur de cette version : R. Presuhn, BMC Software, Inc.
Auteurs de la version précédente :
J. Case, SNMP Research, Inc.
K. McCloghrie, Cisco Systems, Inc.
M. Rose, Dover Beach Consulting, Inc.
S. Waldbusser, International Network Services

décembre 2002

Transpositions de transport pour le protocole simple de gestion de réseau (SNMP)

Statut du présent mémoire

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

Résumé

Le présent document définit le transport de messages du protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*) sur divers protocoles. Le présent document rend obsolète la RFC1906.

Table des Matières

1. Introduction

Pour une revue détaillée des documents qui décrivent le cadre actuel de gestion de l'Internet normalisé, prière de se référer à la section 7 de la [RFC3410].

On accède aux objets gérés via une mémoire d'informations virtuelle, appelée base de données d'informations de gestion (MIB, *Management Information Base*). On accède généralement aux objets d'une MIB au moyen du protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*). Les objets dans la MIB sont définis à l'aide de mécanismes définis dans la structure des informations de gestion (SMI, *Structure of Management Information*). Le présent mémoire spécifie un module de MIB conforme à SMIv2, qui est décrit dans le STD 58, [RFC2578], [RFC2579] et [RFC2580].

Le présent document, Transpositions de transport pour le protocole simple de gestion de réseau, définit comment le protocole de gestion [RFC3416] peut être porté sur diverses suites de protocoles. L'objet du présent document est de définir comment SNMP se transpose sur un ensemble initial de domaines de transport. Au moment de la rédaction du présent document, un travail est en cours pour définir une transposition IPv6, décrite dans la [RFC3419]. D'autres transpositions pourront être définies à l'avenir.

Bien que plusieurs transpositions soient définies, la transposition à UDP sur IPv4 est la transposition préférée pour les systèmes qui prennent en charge IPv4. Les systèmes qui mettent en œuvre IPv4 DOIVENT mettre en œuvre la transposition à UDP sur IPv4. Pour maximiser l'interopérabilité, les systèmes qui acceptent d'autres transpositions DEVRAIENT aussi fournir l'accès via la transposition en UDP sur IPv4.

Dans le présent document, les mots clé "DOIT", "NE DOIT PAS", "EXIGE", "DEVRAIT" NE DEVRAIT PAS", "RECOMMANDE", "NON RECOMMANDÉ", "PEUT", et "FACULTATIF" doivent être interprétés comme décrit dans le BCP 14, [RFC 2119].

2. Définitions

DÉFINITIONS SNMPv2-TM ::= DÉBUT

IMPORTATIONS :
IDENTITÉ DE MODULE, IDENTITÉ D'OBJET, snmpModules, snmpDomains, snmpProxys DE SNMPv2-SMI
CONVENTION TEXTUELLE DE SNMPv2-TC;

IDENTITÉ DE MODULE : snmpv2tm
DERNIÈRE MISE À JOUR : "200210160000Z" (16 octobre 2002 à minuit)
ORGANISATION : "Groupe de travail SNMPv3 de l'IETF"
INFORMATIONS DE CONTACT :
"messagerie du groupe de travail : snmpv3@lists.tislabs.com
pour s'abonner : snmpv3-request@lists.tislabs.com
Coprésident : Russ Mundy
Adresse postale : Network Associates Laboratories, 15204 Omega Drive, Suite 300, Rockville, MD 20850-4601, USA
mél : mundy@tislabs.com
téléphone : +1 301-947-7107
Coprésident : David Harrington
Adresse postale : Enterasys Networks, 35 Industrial Way, P. O. Box 5004, Rochester, New Hampshire 03866-5005, USA
mél : dbh@enterasys.com
téléphone : +1 603-337-2614
Éditeur: Randy Presuhn
Adresse postale : BMC Software, Inc., 2141 North First Street, San Jose, CA 95131, USA
mél : randy_presuhn@bmc.com
téléphone : +1 408-546-1006 "
DESCRIPTION : "Module de MIB pour les transpositions de transport SNMP. Copyright (C) The Internet Society (2002). Cette version de ce module de MIB fait partie de la RFC 3417 ; voir les notices légales complètes dans la RFC elle-même. "
REVISION "200210160000Z" *(16 octobre 2002 à minuit)*
DESCRIPTION : "Précisions, publiée comme RFC 3417."
REVISION "199601010000Z" *(1er janvier 1996 à minuit)*
DESCRIPTION : "Précisions, publiée comme RFC 1906."

REVISION "199304010000Z" *(1er mars 1993 à minuit)*
DESCRIPTION : "Version initiale, publiée comme RFC 1449."
::= { snmpModules 19 }

-- SNMP sur UDP sur IPv4

IDENTITÉ D'OBJET snmpUDPDomain
STATUT : actuel
DESCRIPTION : "Domaine de transport SNMP sur UDP sur IPv4. L'adresse de transport correspondante est du type SnmpUDPAddress."
::= { snmpDomains 1 }

SnmpUDPAddress ::= CONVENTION TEXTUELLE
CONSEIL D'AFFICHAGE : "1d.1d.1d.1d/2d"
STATUT : actuel
DESCRIPTION : "Représente une adresse UDP sur IPv4 :

octets	**contenu**	**codage**
1-4	adresse IP	ordre des octets du réseau
5-6	accès UDP	ordre des octets du réseau "

SYNTAXE : CHAINE D'OCTETS (TAILLE (6))
-- SNMP sur OSI

IDENTITÉ D'OBJET snmpCLNSDomain
STATUT : actuel
DESCRIPTION : "SNMP sur domaine de transport CLNS. L'adresse de transport correspondante est du type SnmpOSIAddress."
::= { snmpDomains 2 }

IDENTITÉ D'OBJET snmpCONSDomain
STATUT : actuel
DESCRIPTION : "SNMP sur domaine de transport CONS. L'adresse de transport correspondante est du type SnmpOSIAddress."
::= { snmpDomains 3 }

SnmpOSIAddress ::= CONVENTION TEXTUELLE
CONSEIL D'AFFICHAGE : "*1x:/1x:"
STATUT : actuel
DESCRIPTION : "Représente une adresse de transport OSI :

octets	**contenu**	**codage**
1	longueur de NSAP	'n' est un entier non signé (0 ou de 3 à 20)
2..(n+1)	NSAP	représentation concrète binaire
(n+2)..m	TSEL	chaîne de (jusqu'à 64) octets "

SYNTAXE : CHAINE D'OCTETS (TAILLE (1 | 4 à 85))

-- SNMP sur DDP

IDENTITÉ D'OBJET snmpDDPDomain
STATUT : actuel
DESCRIPTION : "SNMP sur domaine de transport DDP. L'adresse de transport correspondante est du type SnmpNBPAddress."
::= { snmpDomains 4 }

SnmpNBPAddress ::= CONVENTION TEXTUELLE
STATUT : actuel
DESCRIPTION : "Représente un nom NBP :

octets	**contenu**	**codage**
1	longueur de l'objet	'n' est un entier non signé
2..(n+1)	objet	chaîne de (jusqu'à 32) octets
n+2	longueur du type	'p' est un entier non signé
(n+3)..(n+2+p)	type	chaîne de (jusqu'à 32) octets
n+3+p	longueur de zone	'q' est un entier non signé
(n+4+p)..(n+3+p+q)	zone	chaîne de (jusqu'à 32) octets

Pour les comparaisons, les chaînes sont insensibles à la casse. Toutes les chaînes peuvent contenir tout octet autre que 255 (hex ff)."
SYNTAXE : CHAINE D'OCTETS (TAILLE (3 à 99))

-- SNMP sur IPX

IDENTITÉ D'OBJET snmpIPXDomain
STATUT : actuel
DESCRIPTION : "SNMP sur domaine de transport IPX. L'adresse de transport correspondante est du type SnmpIPXAddress."
::= { snmpDomains 5 }

SnmpIPXAddress ::= CONVENTION TEXTUELLE
CONSEIL D'AFFICHAGE : "4x.1x:1x:1x:1x:1x:1x.2d"
STATUT : actuel
DESCRIPTION : "Représente une adresse IPX :

octets	**contenu**	**codage**
1-4	numéro de réseau	ordre des octets du réseau
5-10	adresse physique	ordre des octets du réseau
11-12	numéro de prise	ordre des octets du réseau "

SYNTAXE : CHAINE D'OCTETS (TAILLE (12))

-- Pour mandataire de SNMPv1 (RFC 1157)

IDENTIFIANT D'OBJET rfc1157Proxy ::= { snmpProxys 1 }

IDENTITÉ D'OBJET rfc1157Domain
STATUT : déconseillé
DESCRIPTION : "Domaine de transport pour SNMPv1 sur UDP sur IPv4. L'adresse de transport correspondante est du type SnmpUDPAddress."
::= { rfc1157Proxy 1 }

-- ::= { rfc1157Proxy 2 } cet OID est obsolète.

FIN

3. SNMP sur UDP dans IPv4

C'est la transposition de transport préférée.

3.1 Mise en série

Chaque instance d'un message est mise en série (c'est-à-dire, codée conformément aux conventions de [BER]) sur un seul datagramme UDP [RFC0768] sur IPv4 [RFC0791], en utilisant l'algorithme spécifié à la Section 8.

3.2 Valeurs bien connues

Il est suggéré que les administrateurs configurent leurs entités SNMP qui prennent en charge les applications de répondeur de commandes à écouter sur l'accès UDP 161. De plus, il est suggéré que les entités SNMP qui prennent en charge les applications de receveur de notification soient configurées à écouter l'accès UDP 162.

Lorsque une entité SNMP utilise cette transposition de transport, elle doit être capable d'accepter des messages jusqu'à une taille de 484 octets inclus. Il est recommandé que les mises en œuvre soient capables d'accepter des messages d'une taille allant jusqu'à 1472 octets. La mise en œuvre de valeurs supérieures est encouragée chaque fois que possible.

4. SNMP sur OSI

Cette transposition de transport est facultative.

4.1 Mise en série

Chaque instance d'un message est mise en série sur une seule TSDU [IS8072] [IS8072A] pour le service de transport en mode sans connexion (CLTS, *Connectionless-mode Transport Service*) OSI, en utilisant l'algorithme spécifié Section 8.

4.2 Valeurs bien connues

Il est suggéré que les administrateurs configurent leurs entités SNMP qui prennent en charge les applications de répondeur de commandes à écouter sur le sélecteur de transport "snmp-l" (qui consiste en six caractères ASCII) lorsque elles utilisent un service réseau en mode sans connexion pour réaliser le CLTS. De plus, il est suggéré que les entités SNMP qui prennent en charge les applications de receveur de notification soient configurées à écouter sur le sélecteur de transport "snmpt-l" (qui consiste en sept caractères ASCII, six lettres et un tiret) lorsque elles utilisent un service réseau en mode sans connexion pour réaliser le CLTS. De même, lorsque elles utilisent un service réseau en mode connexion pour réaliser le CLTS, les sélecteurs de transport suggérés sont "snmp-o" et "snmpt-o", pour respectivement les répondeurs de commandes et les receveurs de notification.

Lorsque une entité SNMP utilise cette transposition de transport, elle doit être capable d'accepter des messages qui font au moins 484 octets. La mise en œuvre de valeurs supérieures est encouragée chaque fois que possible.

5. SNMP sur DDP

Cette transposition de transport est facultative.

5.1 Mise en série

Chaque instance d'un message est mise en série sur un seul datagramme DDP [APPLETALK], en utilisant l'algorithme spécifié Section 8.

5.2 Valeurs bien connues

Les messages SNMP sont envoyés en utilisant le type 8 de protocole DDP. Les entités SNMP qui prennent en charge les applications de répondeur de commandes écoutent sur la prise DDP numéro 8, tandis que les entités SNMP qui prennent en charge les applications de receveur de notification écoutent sur la prise DDP numéro 9.

Les administrateurs doivent configurer leurs entités SNMP qui prennent en charge les applications de répondeur de commandes à utiliser le type NBP "Agent SNMP" (qui consiste en dix caractères ASCII) tandis que celles qui prennent en charge les applications de receveur de notification doivent être configurées à utiliser le type NBP "traiteur de filtre SNMP" (qui consiste en dix-sept caractères ASCII).

Le nom NBP pour les entités SNMP qui prennent en charge les répondeurs de commandes et les receveurs de notification devrait être stable – les noms NBP ne devraient pas changer plus souvent que l'adresse IP d'un nœud TCP/IP normal. Il est suggéré que le nom NBP soit conservé dans une forme de mémorisation stable.

Lorsque une entité SNMP utilise cette transposition de transport, elle doit être capable d'accepter des messages qui font au moins 484 octets. La mise en œuvre de valeurs supérieures est encouragée chaque fois que possible.

5.3 Discussion sur l'adressage AppleTalk

La suite de protocoles AppleTalk possède certaines caractéristiques qui ne se manifestent pas dans la suite TCP/IP. La stratégie de dénominations de AppleTalk et la nature dynamique de l'allocation d'adresses peuvent causer des problèmes aux entités SNMP qui souhaitent gérer des réseaux AppleTalk. Les nœuds TCP/IP ont une adresse IP associée qui les distingue les uns des autres. À l'opposé, les nœuds AppleTalk n'ont généralement pas de telles caractéristiques. L'adresse de niveau réseau, bien que souvent relativement stable, peut changer à chaque réamorçage (ou plus fréquemment).

Donc, lorsque SNMP est transposé sur DDP, les nœuds sont identifiés par un "nom", plutôt que par une "adresse". Et donc tous les nœuds AppleTalk qui mettent en œuvre la présente transposition sont obligés de répondre aux recherches NBP et de confirmer (par exemple, met en œuvre le bout de protocole NBP) ce qui garantit qu'une transposition de nom NBP en

adresse DDP sera possible.

En déterminant l'identité SNMP à enregistrer pour une entité SNMP, il est suggéré que l'identité SNMP soit un nom associé à d'autres services réseaux offerts par la machine.

Les recherches NBP, qui sont utilisées pour transposer les noms NBP en adresses DDP, peuvent causer de grandes quantités de trafic réseau ainsi que la consommation de ressources de CPU. Il est aussi un fait que la capacité à effectuer une recherche NBP est sensible à certaines perturbations du réseau (comme les incohérences de tableau de zone) qui n'empêcheraient pas des communications AppleTalk directes entre deux entités SNMP.

Donc, il est recommandé que les recherches NBP soient rarement utilisées, principalement pour créer une antémémoire de transpositions de nom en adresse. Ces transpositions en antémémoire devraient alors être utilisées pour tout trafic SNMP ultérieur. Il est recommandé que les entités SNMP qui prennent en charge des applications de générateur de commandes conservent cette antémémoire entre les réamorçages. Cette antémémoire peut aider à minimiser le trafic réseau, à réduire la charge de CPU sur le réseau, et permettre (dans une certaine mesure) de résoudre les problèmes lorsque le mécanisme de base de traduction de nom en adresse est rompu.

5.3.1 Comment acquérir des noms NBP

Une entité SNMP qui prend en charge les applications de générateur de commandes peut avoir une liste préconfigurée de noms d'entités SNMP "connues" qui prennent en charge les applications de répondeur de commandes. De même, une entité SNMP qui prend en charge les applications de générateur de commande ou de receveur de notification peut interagir avec un opérateur. Finalement, une entité SNMP qui prend en charge les applications de générateur de commandes ou de receveur de notification peut communiquer avec toutes les entités SNMP qui prennent en charge les applications de répondeur de commandes ou de générateur de notification dans un ensemble de zones ou réseaux.

5.3.2 Quand changer des noms NBP en adresses DDP

Quand une entité SNMP utilise une entrée d'antémémoire pour adresser un paquet SNMP, elle devrait tenter de confirmer la validité de la transposition, si celle-ci n'a pas été confirmée dans les dernières T1 secondes. Cette durée de vie d'entrée d'antémémoire, T1, a une valeur minimum par défaut de 60 secondes, et devrait être configurable.

Une entité SNMP qui prend en charge une application de générateur de commandes peut décider de renseigner son antémémoire avant de communiquer réellement avec une autre entité SNMP. En général, on s'attend à ce qu'une telle entité puisse vouloir conserver certaines transpositions "plus courantes" que d'autres, par exemple, les nœuds qui représentent l'infrastructure du réseau (par exemple, les routeurs) peuvent être réputés "plus importants".

Noter qu'une entité SNMP qui prend en charge les applications de générateur de commandes ne devrait pas renseigner son antémémoire toute entière à l'initialisation ; elle devrait plutôt tenter des résolutions sur une durée étendue (peut-être dans un ordre prédéterminé ou une priorité configurée). Chacune de ces résolutions pourrait, en fait, être une recherche générique dans une certaine zone.

Une entité SNMP qui prend en charge les applications de répondeur de commandes ne doit jamais renseigner son antémémoire. Lors de la génération d'une réponse, une telle entité n'a pas besoin de confirmer une entrée d'antémémoire. Une entité SNMP qui prend en charge les applications de génération de notification ne devrait faire des recherches NBP (ou des confirmations) que quand elle a besoin d'envoyer un filtre ou une information SNMP.

5.3.3 Comment changer des noms NBP en adresses DDP

Si le seul élément d'information disponible est le nom NBP, une recherche NBP devrait alors être effectuée pour transformer ce nom en adresse DDP. Cependant, si il y a un élément d'information d'état, il peut être utilisé comme indication pour effectuer une confirmation NBP (qui envoie un message en envoi individuel à l'adresse réseau qui est supposée être la cible de la recherche de nom) pour voir si les informations périmées sont, en fait, encore valides.

Une transposition de nom NBP en adresse DDP peut aussi être confirmée implicitement en utilisant seulement des transactions SNMP. Par exemple, une entité SNMP qui prend en charge les applications de générateur de commandes qui produit une opération de restitution pourrait aussi restituer les objets pertinents du groupe NBP [RFC1742] pour l'entité SNMP qui prend en charge l'application de répondeur de commandes. Ces informations peuvent alors être corrélées avec l'adresse DDP de source de la réponse.

5.3.4 Que se passe t-il si NBP est cassé

Dans certaines circonstances, il peut y avoir connexité entre deux entités SNMP, mais la machinerie de transposition NBP

peut être cassée, par exemple,

- o le mécanisme NBP FwdReq (transmettre la recherche NBP au réseau de rattachement local) peut être en panne sur un routeur sur le réseau de l'autre entité ; ou
- o le mécanisme NBP BrRq (demande de diffusion NBP) peut être en panne sur un routeur sur le propre réseau de l'entité ;
- o ou NBP peut être en panne sur le nœud de l'autre entité.

Une entité SNMP qui prend en charge les applications de générateur de commande et qui est dédiée à la gestion AppleTalk pourrait choisir d'atténuer certaines de ces défaillances en mettant directement en œuvre la portion routeur de NBP. Par exemple, une telle entité peut déjà connaître toutes les zones sur l'internet AppleTalk et les réseaux sur lesquels chaque zone apparaît. Sur une recherche NBP qui échoue, l'entité pourrait envoyer une FwdReq NBP au réseau dans lequel l'entité SNMP qui prend en charge l'application de répondeur de commandes ou de générateur de notification était localisée en dernier. Si cela échoue, la station pourrait alors envoyer une LkUp NBP (paquet de recherche NBP) comme diffusion groupée dirigée (DDP) à chaque numéro de réseau sur ce réseau. Des défaillances ci-dessus (seules) cette approche combinée va résoudre le cas où soit le mécanisme BrRq à FwdReq du routeur local est cassé, soit le mécanisme FwdReq à LkUp du routeur distant est cassé.

6. SNMP sur IPX

Cette transposition de transport est facultative.

6.1 Mise en série

Chaque instance d'un message est mise en série sur un seul datagramme IPX [NOVELL], en utilisant l'algorithme spécifié à la Section 8.

6.2 Valeurs bien connues

Les messages SNMP sont envoyées en utilisant le type 4 de paquet IPX (c'est-à-dire, le protocole d'échange de paquet).

Il est suggéré que les administrateurs configurent leurs entités SNMP qui prennent en charge les applications de répondeur de commandes à écouter sur la prise IPX 36879 (900f en hexadécimal). De plus, il est suggéré que celles qui prennent en charge les applications de receveur de notification soient configurées à écouter sur la prise IPX 36880 (hexadécimal 9010).

Lorsque une entité SNMP utilise cette transposition de transport, elle doit être capable d'accepter des messages d'au moins 546 octet. La mise en œuvre de valeurs supérieures est encouragée chaque fois que possible.

7. Mandataire pour SNMPv1

Historiquement, afin de prendre en charge un mandataire pour SNMPv1, comme défini dans la [RFC2576], il était réputé utile de définir un domaine de transport, rfc1157Domain, qui indique la transposition de transport pour les messages SNMP comme défini dans la [RFC1157].

8. Mise en série en utilisant les règles de codage de base

Lorsque les règles de codage de base (BER, *Basic Encoding Rules*) [BER] sont utilisées pour la mise en série :

(1) Lors du codage du champ Longueur, seule la forme définie est utilisée ; l'utilisation du codage de la forme indéfinie est interdite. Noter que lorsque on utilise la forme définie longue, il est permis d'utiliser plus que le nombre minimum d'octets de longueur nécessaires pour coder le champ Longueur.

(2) Lors du codage du champ Valeur, la forme primitive devra être utilisée pour tous les types simples, c'est-à-dire, ENTIER, CHAINE D'OCTETS, et IDENTIFIANT D'OBJET (IMPLICITE ou explicite). La forme construite de codage devra être seulement utilisée pour les types structurés, c'est-à-dire, une SEQUENCE ou une SEQUENCE IMPLICITE.

(3) Lors du codage d'un objet dont la syntaxe est décrite en utilisant la construction BITS, la valeur est codée comme une CHAINE D'OCTETS, dans laquelle tous les bits désignés dans (la définition de) la chaîne binaire, en commençant par

le premier bit et en continuant jusqu'au dernier bit, sont placés dans les bits 8 (bit de poids fort) à 1 (bit de moindre poids) du premier octet, suivis par les bits 8 à 1 de chaque octet suivant, suivis par autant de bits que nécessaire de l'octet final suivant, en commençant par le bit 8. Les bits restants, si il en est, de l'octet final sont mis à zéro à l'émission et ignorés à réception.

Ces restrictions s'appliquent à tous les aspects du codage ASN.1, incluant les enveloppes de message, les unités de données de protocole et les objets de données qu'ils contiennent.

8.1 Exemple d'utilisation

Comme exemple d'application des règles de codage de base, supposons qu'on veuille coder une instance de la PDU GetBulkRequest [RFC3416] :

```
[5] IMPLICIT SEQUENCE {
      request-id      1414684022,
      non-repeaters   1,
      max-repetitions 2,
      variable-bindings {
         { name sysUpTime, value { unSpecified NULL } },
         { name ipNetToMediaPhysAddress, value { unSpecified NULL } },
         { name ipNetToMediaType, value { unSpecified NULL } }
      }
   }
```

En appliquant les BER, ceci peut être codé (en hexadécimal) comme :

```
[5] IMPLICIT SEQUENCE         a5 82 00 39
   INTEGER                    02 04 54 52 5d 76
   INTEGER                    02 01 01
   INTEGER                    02 01 02
   SEQUENCE (OF)              30 2b
      SEQUENCE                30 0b
         OBJECT IDENTIFIER    06 07 2b 06 01 02 01 01 03
         NULL                 05 00
      SEQUENCE                30 0d
         OBJECT IDENTIFIER    06 09 2b 06 01 02 01 04 16 01 02
         NULL                 05 00
      SEQUENCE                30 0d
         OBJECT IDENTIFIER    06 09 2b 06 01 02 01 04 16 01 04
         NULL                 05 00
```

Noter que le SEQUENCE initial dans cet exemple n'a pas été codé en utilisant le nombre minimum d'octets de longueur. (Le premier octet de la longueur, 82, indique que la longueur du contenu est codée dans les deux octets qui suivent.)

9. Notice sur la 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 le 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.

10. Remerciements

Le présent document est le fruit des travaux du groupe SNMPv3. Des remerciements particuliers sont adressés dans l'ordre alphabétique aux membres suivants du groupe de travail : Randy Bush, Jeffrey D. Case, Mike Daniele, Rob Frye, Lauren Heintz, Keith McCloghrie, Russ Mundy, David T. Perkins, Randy Presuhn, Aleksey Romanov, Juergen Schoenwaelder, Bert Wijnen.

La présente version du document, éditée par Randy Presuhn, se fonde à l'origine sur les travaux d'une équipe de conception dont les membres étaient : Jeffrey D. Case, Keith McCloghrie, David T. Perkins, Randy Presuhn, Juergen Schoenwaelder.

Les versions précédentes de ce document, éditées par Keith McCloghrie, étaient le résultat de travaux significatifs de quatre contributeurs majeurs : Jeffrey D. Case, Keith McCloghrie, Marshall T. Rose, Steven Waldbusser.

De plus, il faut aussi remercier les contributeurs du groupe de travail SNMPv2 aux versions précédentes. En particulier, des remerciements sont adressés pour les contributions de :

Alexander I. Alten	Jeff Johnson	Aleksey Romanov
Dave Arneson	Michael Kornegay	Shawn Routhier
Uri Blumenthal	Deirdre Kostick	Jon Saperia
Doug Book	David Levi	Juergen Schoenwaelder
Kim Curran	Daniel Mahoney	Bob Stewart
Jim Galvin	Bob Natale	Kaj Tesink
Maria Greene	Brian O'Keefe	Glenn Waters
Iain Hanson	Andrew Pearson	Bert Wijnen
Dave Harrington	Dave Perkins	
Nguyen Hien	Randy Presuhn	

11. Considérations relatives à l'IANA

Le module de MIB SNMPv2-TM exige l'allocation d'un seul identifiant d'objet pour son MODULE-IDENTITY. L'IANA a alloué cet identifiant d'objet dans la sous arborescence snmpModules, définie dans le module de MIB SNMPv2-SMI.

12. Considérations sur la sécurité

Par lui-même SNMPv1 n'est pas un environnement sûr. Même si le réseau lui-même est sûr (par exemple en utilisant IPsec), même alors, il n'y a pas de contrôle sur qui est autorisé à utiliser ce réseau sûr pour accéder et faire les opérations GET/SET (lire/changer) sur les objets accessibles par une application de répondeur de commandes.

Il est recommandé que les mises en œuvre considèrent les dispositifs de sécurité fournis par le cadre SNMPv3. Précisément, l'utilisation du modèle de sécurité fondé sur l'utilisateur STD 62, [RFC3414] et le modèle de contrôle d'accès fondé sur la vue STD 62, [RFC3415] est recommandée.

Il est alors de la responsabilité du consommateur/utilisateur de s'assurer que l'entité SNMP qui donne l'accès à une MIB est configuré de façon appropriée pour donner l'accès aux objets aux seuls principaux (usagers) qui ont des droits légitimes pour leur faire subir les opérations GET ou SET (changer).

13. Références

13.1 Références normatives

[BER] Organisation Internationale de Normalisation. "Systèmes de traitement de l'information - Interconnexion des systèmes ouverts - Spécification des règles de codage de base pour la notation de syntaxe abstraite numéro un

(ASN.1)". Norme internationale 8825, décembre 1987.

[IS8072] Organisation Internationale de Normalisation. "Systèmes de traitement de l'information - Interconnexion des systèmes ouverts - Définition du service de transport". Norme internationale 8072, juin 1986.

[IS8072A] Organisation Internationale de Normalisation. "Systèmes de traitement de l'information - Interconnexion des systèmes ouverts - Définition du service de transport - Addendum 1 : Transmission en mode sans connexion". Norme internationale 8072/AD 1, décembre 1986.

[RFC0768] J. Postel, "Protocole de datagramme d'utilisateur (UDP)", (STD 6), 28 août 1980.

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

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

[RFC2578] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Structure des informations de gestion, version 2 (SMIv2)", avril 1999. (STD0058)

[RFC2579] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Conventions textuelles pour SMIv2", avril 1999. (STD0058)

[RFC2580] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Déclarations de conformité pour SMIv2", avril 1999. (STD0058)

[RFC3414] U. Blumenthal, B. Wijnen, "Modèle de sécurité fondée sur l'utilisateur (USM) pour la version 3 du protocole simple de gestion de réseau (SNMPv3)", décembre 2002. (STD0062)

[RFC3415] B. Wijnen, R. Presuhn, K. McCloghrie, "Modèle de contrôle d'accès fondé sur la vue (VACM) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

[RFC3416] R. Presuhn, éd., "Version 2 des opérations de protocole pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

13.2 Références pour information

[APPLETALK] Sidhu, G., Andrews, R. and A. Oppenheimer, "Inside AppleTalk" (second edition). Addison-Wesley, 1990.

[NOVELL] "Network System Technical Interface Overview". Novell, Inc., juin 1989.

[RFC1157] J. Case, M. Fedor, M. Schoffstall et J. Davin, "Protocole simple de gestion de réseau", STD 15, mai 1990. *(Historique)*

[RFC1742] S. Waldbusser et K. Frisa, "Base de données d'informations de gestion II pour AppleTalk", déc.1994. *(Info)*

[RFC2576] R. Frye, D. Levi, S. Routhier, B. Wijnen, "Coexistence entre les version 1, version 2 et version 3 du cadre de gestion de réseau de l'Internet" mars 2000. (*Obsolète, voir* RFC3584) *(P.S.)*

[RFC3410] J. Case et autres, "Introduction et déclarations d'applicabilité pour le cadre de gestion standard de l'Internet", décembre 2002. *(Information)*

[RFC3419] M. Daniele, J. Schoenwaelder, "Conventions textuelles pour les adresses de transport", décembre 2002. *(P.S.)*

14. Changements par rapport à la RFC 1906

Le présent document ne diffère de la RFC 1906 que par des améliorations rédactionnelles. Le protocole est inchangé.

15. Adresse de l'éditeur

Randy Presuhn
BMC Software, Inc.
2141 North First Street
San Jose, CA 95131
USA
téléphone : +1 408 546-1006
mél : randy_presuhn@bmc.com

16. Déclaration complète de droits de reproduction

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