

Groupe de travail Réseau
Request for Comments : 3410
RFC rendue obsolète : 2570
 Catégorie : Information
 Traduction Claude Brière de L'Isle

J. Case, SNMP Research, Inc.
 R. Mundy, Network Associates Laboratories
 D. Partain, Ericsson
 B. Stewart, retraité
 décembre 2002

Introduction et déclaration d'applicabilité pour le cadre de gestion normalisé de l'Internet

Statut de ce mémoire

Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune forme de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2002). Tous droits réservés.

Résumé

Le présent document a pour objet de fournir une vue d'ensemble de la troisième version du cadre de gestion normalisé de l'Internet, appelée le cadre SNMP version 3 (SNMPv3). Ce cadre est dérivé du, et s'appuie sur, le cadre originel de gestion normalisé de l'Internet (SNMPv1) et sur le second cadre de gestion normalisé de l'Internet (SNMPv2).

L'architecture est conçue comme modulaire pour permettre l'évolution du cadre au fil du temps.

Le document explique pourquoi on recommande fortement d'utiliser SNMPv3 plutôt que SNMPv1 ou SNMPv2. Le document recommande aussi que les RFC 1157, 1441, 1901, 1909 et 1910 soient retirées et placées au statut d'historique. Le présent document rend obsolète la RFC 2570.

Table des Matières

1. Introduction.....	2
2. Cadre de gestion normalisé de l'Internet.....	2
2.1 Structure de base et composants.....	2
2.2 Architecture du cadre de gestion normalisée de l'Internet.....	3
3. Cadre de gestion SNMPv1.....	3
3.1 Langage de définition des données SNMPv1.....	3
3.2 Informations de gestion.....	4
3.3 Opérations du protocole.....	4
3.4 Sécurité et administration de SNMPv1.....	4
4. Cadre de gestion SNMPv2.....	4
5. Le groupe de travail SNMPv3.....	5
6. Spécifications des modules du cadre SNMPv3.....	6
6.1 Langage de définition des données.....	6
6.2 Modules de MIB.....	7
6.3 Opérations de protocole et transpositions de transport.....	7
6.4 Sécurité et administration de SNMPv3.....	7
7. Résumé des documents.....	8
7.1 Structure des informations de gestion.....	8
7.2 Opérations du protocole.....	9
7.3 Transpositions de transport.....	9
7.4 Instrumentation du protocole.....	9
7.5 Architecture, sécurité et administration.....	9
7.6 Traitement et répartition des messages.....	10
7.7 Applications SNMP.....	10
7.8 Modèle de sécurité fondé sur l'utilisateur.....	10
7.9 Contrôle d'accès fondé sur la vue.....	11
7.10 Coexistence et transition avec SNMPv3.....	11
8. État de normalisation.....	11
8.1 Statut de SMIV1.....	11
8.2 Statut de normalisation de SNMPv1 et SNMPv2.....	12
8.3 Recommandation du groupe de travail.....	12

9. Considérations sur la sécurité.....	12
10. Références.....	13
11. Adresse des éditeurs.....	14
12. Déclaration complète de droits de reproduction.....	14

1. Introduction

Le présent document est une introduction à la troisième version du cadre de gestion normalisé de l'Internet, appelée cadre de gestion SNMP version 3 (SNMPv3) et a plusieurs objets.

D'abord, il décrit les relations entre les spécifications de SNMP version 3 (SNMPv3) et les spécifications du cadre de gestion SNMP version 1 (SNMPv1), du cadre de gestion SNMP version 2 (SNMPv2) et le cadre administratif fondé sur la communauté pour SNMPv2.

Ensuite, il fournit une feuille de route pour les divers documents qui contiennent les spécifications pertinentes.

Enfin, ce document fournit un bref résumé facile à lire du contenu de chacun des documents de spécification pertinents.

Ce document est intentionnellement de nature didactique, et à ce titre peut occasionnellement être "coupable" de simplification. En cas de conflit ou de contradiction entre le présent document et les documents plus détaillés pour lesquels il est un guide de lecture, les spécifications des documents plus détaillés devront prévaloir.

De plus, les documents détaillés tentent de conserver une séparation entre les divers modules composants afin de spécifier des interfaces bien définies entre eux. Le présent document adopte cependant une approche différente et tente de donner une vision intégrée des divers modules composants dans l'intérêt de la lisibilité.

Le présent document est un travail produit par le groupe de travail SNMPv3 de l'équipe d'ingénierie de l'Internet (IETF).

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Cadre de gestion normalisé de l'Internet

La troisième version du cadre de gestion normalisé de l'Internet (le cadre SNMPv3) est dérivé de et s'appuie sur le cadre originel de gestion normalisé de l'Internet (SNMPv1) aussi bien que sur le second cadre de gestion normalisé de l'Internet (SNMPv2).

Toutes les versions (SNMPv1, SNMPv2, et SNMPv3) du cadre SNMP de gestion normalisé de l'Internet partagent la même structure de base et les mêmes composants. De plus, toutes les versions des spécifications du cadre de gestion normalisé de l'Internet suivent la même architecture.

2.1 Structure de base et composants

Une entreprise qui déploie le cadre de gestion normalisé de l'Internet contient quatre composants de base :

- * plusieurs (normalement beaucoup) nœuds gérés, ayant chacun une entité SNMP qui fournit l'accès à distance à l'instrumentation de gestion (traditionnellement appelée un agent) ;
- * au moins une entité SNMP ayant des applications de gestion (normalement appelée un gestionnaire) ;
- * un protocole de gestion utilisé pour convoier les informations de gestion entre les entités SNMP ;
- * des informations de gestion.

Le protocole de gestion est utilisé pour convoier les informations de gestion entre les entités SNMP du type gestionnaires et agents.

Cette structure de base est commune à toutes les versions du cadre de gestion normalisé de l'Internet, c'est-à-dire, SNMPv1, SNMPv2, et SNMPv3.

2.2 Architecture du cadre de gestion normalisée de l'Internet

Les spécifications du cadre de gestion normalisé de l'Internet se fondent sur une architecture modulaire. Ce cadre est plus qu'un simple protocole pour déplacer des données. Il consiste en :

- * un langage de définition des données,
- * des définitions d'informations de gestion (la base de données d'informations de gestion, ou MIB),
- * une définition de protocole,
- * une sécurité et une administration.

Avec le temps, le cadre ayant évolué de SNMPv1, à SNMPv2, puis SNMPv3, les définitions de chacun de ces composants architecturaux se sont enrichies et sont plus claires, mais l'architecture fondamentale est restée cohérente.

La principale motivation de cette modularité était de permettre l'évolution en cours du cadre, comme elle est documentée dans la [RFC1052]. Lorsque envisagée à l'origine, cette capacité était utilisée pour faciliter la transition de la gestion des internets fondée sur SNMP à la gestion fondée sur les protocoles OSI. À cette fin, le cadre a été structuré avec un langage de définition des données indépendant du protocole et une base de données d'informations de gestion ainsi qu'un protocole indépendant de la MIB. Cette séparation était conçue pour permettre le remplacement du protocole fondé sur SNMP sans exiger de redéfinir ou réinstrumenter les informations de gestion. L'histoire a montré que le choix de cette architecture était la bonne décision pour de mauvaises raisons – il s'est trouvé que cette architecture a facilité la transition de SNMPv1 à SNMPv2 et de SNMPv2 à SNMPv3 plutôt que de faciliter une transition de sortie de la gestion fondée sur le protocole simple de gestion de réseau.

Le cadre SNMPv3 construit et étend ces principes architecturaux en :

- * s'appuyant sur ces quatre composants architecturaux de base, en les incorporant dans certains cas par référence au cadre SNMPv2,
- * en utilisant ces mêmes principes de mise en couches dans la définition de nouvelles capacités dans la portion sécurité et administration de l'architecture.

Ceux qui sont familiers de l'architecture du cadre de gestion de SNMPv1 et du cadre de gestion de SNMPv2 vont trouver des concepts similaires dans l'architecture du cadre de gestion de SNMPv3. Cependant, dans certains cas, la terminologie peut être un peu différente.

3. Cadre de gestion SNMPv1

Le cadre de gestion normalisé de l'Internet original (SNMPv1) est défini dans les documents suivants :

- * STD 16, [RFC1155] définit la structure des informations de gestion (SMI, *Structure of Management Information*) qui est le mécanisme utilisé pour décrire et désigner les objets pour les besoins de la gestion.
- * STD 16, [RFC1212] définit un mécanisme de description plus concis pour décrire et désigner les objets d'information de gestion; mais qui est pleinement cohérent avec la SMI.
- * STD 15, [RFC1157] définit le protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*) utilisé pour l'accès par le réseau aux objets gérés et à la notification d'événement. Noter que ce document définit aussi un ensemble initial de notifications d'événement.

De plus, deux documents sont généralement considérés comme accompagnant les trois précédents :

- * le STD 17, [RFC1213] qui contient les définitions de l'ensemble de base des informations de gestion,
- * la [RFC1215] qui définit un mécanisme concis de description pour définir les notifications d'événement, qui sont appelés des filtres (traps) dans le protocole SNMPv1. Elle spécifie aussi les filtres génériques de la RFC1157 en notation concise.

Ces documents décrivent les quatre parties de la première version du cadre SNMP.

3.1 Langage de définition des données SNMPv1

Les deux premiers documents et le dernier, c'est-à-dire, les RFC 1155, 1212, et 1215, décrivent le langage SNMPv1 de définition des données et on s'y réfère souvent collectivement par "SMIv1". Noter que du fait de l'exigence initiale que la SMI soit indépendante du protocole, les deux premiers documents de la SMI ne donnent pas de moyen pour définir des notifications d'événements (traps). À la place, le document de protocole SNMP définit quelques notifications d'événement normalisées (filtres génériques) et fournit un moyen pour définir des notifications d'événement supplémentaires. Le dernier document

spécifie une approche directe pour la définition de notifications d'événements utilisés avec le protocole SNMPv1. Au moment de sa rédaction, il y avait une controverse sur l'utilisation de filtres dans le cadre de gestion normalisée du réseau Internet. C'est à ce titre que la RFC 1215 a été publiée avec le statut de "Information", qui n'a jamais été mis à jour parce qu'on pensait que la seconde version du cadre SNMP remplacerait la première version.

3.2 Informations de gestion

Le langage de définition des données décrit dans les deux premiers documents a d'abord été utilisé pour définir la MIB-I maintenant "historique" qui était spécifiée dans la [RFC1156], et a ensuite été utilisée pour définir la MIB-II spécifiée dans la [RFC1213].

Ensuite, après la publication de la MIB-II, une approche différente de la définition des informations de gestion provenant de l'approche antérieure d'avoir un seul comité de généralistes travaillant sur un seul document pour définir la MIB normalisée de l'Internet. On a plutôt produit des documents de mini MIB en parallèle et réparties entre des groupes mandatés pour produire une spécification pour une portion ciblée de la MIB normalisée de l'Internet et composée de personnes expertes de ces domaines particuliers allant des divers aspects de la gestion de réseau, à la gestion de système, et à la gestion d'applications.

3.3 Opérations du protocole

Le troisième document, STD 15 [RFC1157], décrit les opérations du protocole SNMPv1 effectuées par des unités de données de protocole (PDU, *protocol data units*) sur des listes de liens de variables et décrit le format des messages SNMPv1. Les opérateurs définis par SNMPv1 sont : get (*obtenir*), get-next (*obtenir ensuite*), get-response (*obtenir une réponse*), set-request (*demande d'établissement*), et trap (*filtre*). Il définit aussi la mise en couche typique de SNMP sur un transport sans connexion.

3.4 Sécurité et administration de SNMPv1

Le STD 15 [RFC1157] décrit aussi une approche de la sécurité et l'administration. Beaucoup de ces concepts sont encore utilisés et certains, en particulier la sécurité, sont étendus par le cadre SNMPv3.

Le cadre SNMPv1 décrit l'encapsulation des PDU SNMPv1 dans les messages SNMP entre les entités SNMP et distingue entre les entités d'application et les entités de protocole. Dans SNMPv3, elles sont renommées respectivement applications et moteurs.

Le cadre SNMPv1 introduit aussi le concept de service d'authentification prenant en charge un ou plusieurs schémas d'authentification. En plus de l'authentification, SNMPv3 définit la capacité de sécurité supplémentaire à laquelle on se réfère sous le nom de confidentialité. (Noter qu'une certaine littérature de la communauté de la sécurité décrirait les capacités de sécurité de SNMPv3 comme assurant l'intégrité des données, l'authenticité de la source, et la confidentialité.) La nature modulaire du cadre SNMPv3 permet à la fois des changements et des ajouts aux capacités de sécurité.

Finalement, le cadre SNMPv1 introduit le contrôle d'accès fondé sur un concept appelé une vue de MIB SNMP. Le cadre SNMPv3 spécifie un concept fondamentalement similaire appelé contrôle d'accès fondé sur la vue (*vbac, view-based access control*). Avec cette capacité, SNMPv3 donne le moyen de contrôler l'accès aux informations sur les appareils gérés.

Cependant, alors que le cadre SNMPv1 anticipait la définition de plusieurs schémas d'authentification, il ne définissait aucun autre schéma que d'une authentification triviale fondée sur des chaînes communautaires. C'était une des faiblesses fondamentales reconnues du cadre SNMPv1 mais il fut estimé à l'époque que la définition d'une sécurité de qualité commerciale pourrait faire peser des contraintes sur la conception et des difficultés pour être approuvée parce que "sécurité" signifie des choses différentes pour chacun. De ce fait, et parce que certains utilisateurs n'avaient pas besoin d'une authentification forte, SNMPv1 a imaginé un service d'authentification comme un bloc séparé à définir "plus tard" et le cadre SNMPv3 fournit une architecture à utiliser au sein de ce bloc ainsi qu'une définition pour ses sous-systèmes.

4. Cadre de gestion SNMPv2

Le cadre de gestion SNMPv2 est décrit dans les [RFC1156], [RFC1902], [RFC1903], [RFC1904], [RFC1905] et [RFC1906] et les questions de coexistence et de transition relatives à SNMPv1 et SNMPv2 sont discutées dans la [RFC2576].

SNMPv2 procure plusieurs avantages sur SNMPv1, incluant :

- * des types de données étendus (par exemple, un compteur de 64 bit)
- * une efficacité et des performances améliorées (opérateur get-bulk)

- * une confirmation de notification d'événement (opérateur inform)
- * un traitement plus riche des erreurs (erreurs et exceptions)
- * des ensembles améliorés, en particulier la création et la suppression de rangées
- * un réglage fin du langage de définition des données.

Cependant, le cadre SNMPv2, tel que décrit dans ces documents, est incomplet en ce qu'il ne satisfait pas les objectifs originels de conception du projet SNMPv2. Les objectifs non satisfaits incluent la fourniture de la sécurité et de l'administration en livrant une soit disant sécurité de "qualité commerciale" avec :

- * l'authentification : identification de l'origine, l'intégrité du message, et certains aspects de protection contre la répétition ;
- * la protection de la confidentialité ;
- * l'autorisation et le contrôle d'accès ;
- * et des capacités convenables de configuration et d'administration pour ces caractéristiques.

Le cadre de gestion SNMPv3, tel que décrit dans le présent document et ses documents d'accompagnement, règle ses déficiences significatives.

5. Le groupe de travail SNMPv3

Le présent document et ses documents d'accompagnement ont été produits par le groupe de travail SNMPv3 de l'équipe d'ingénierie de l'Internet (IETF, *Internet Engineering Task Force*). Le groupe de travail SNMPv3 a été mandaté pour préparer des recommandations pour la prochaine génération de SNMP. Le but du groupe de travail était de produire l'ensemble nécessaire de documents qui fournit une seule norme pour la prochaine génération de fonctions centrales de SNMP. Le seul besoin critique de la nouvelle génération est une définition de la sécurité et de l'administration qui rende les transactions de gestion fondées sur SNMP sûres d'une façon utile pour les utilisateurs qui souhaitent utiliser SNMPv3 pour gérer les réseaux, les systèmes qui constituent ces réseaux, et les applications qui résident sur ces systèmes, incluant les transactions de gestionnaire à agent, d'agent à gestionnaire, et de gestionnaire à gestionnaire.

Dans les années qui ont précédé le mandat du groupe de travail, il y avait un certain nombre d'activités visant à incorporer la sécurité et d'autres améliorations à SNMP. Ces efforts incluaient :

- * "Sécurité SNMP" autour de 1991-1992 (RFC 1351 - RFC 1353),
- * "SMP" autour de 1992-1993, et
- * "SNMPv2 fondé sur la partie" (parfois appelé "SNMPv2p") autour de 1993-1995 (RFC 1441 - RFC 1452).

Chacun de ces efforts incorporait une sécurité de qualité commerciale, de force industrielle incluant l'authentification, la confidentialité, l'autorisation, le contrôle d'accès fondé sur la vue, et d'administration, incluant la configuration à distance.

Ces efforts ont nourri le développement du cadre de gestion SNMPv2 comme décrit dans les RFC 1902 à 1908. Cependant, le cadre décrit dans ces RFC n'a pas par lui-même de cadre de sécurité et d'administration fondé sur des normes ; il a été plutôt associé à plusieurs cadres de sécurité et d'administration, incluant :

- * "SNMPv2 fondé sur la communauté" (SNMPv2c) décrit dans la [RFC1901],
- * "SNMPv2u" décrit dans les RFC 1909 et 1910, et
- * "SNMPv2*."

SNMPv2c avait le plus de soutien au sein de l'IETF mais n'avait pas de sécurité ni d'administration tandis que SNMPv2u et SNMPv2* avaient tous deux la sécurité mais manquaient de consensus de soutien au sein de l'IETF.

Le groupe de travail SNMPv3 était mandaté pour produire un seul ensemble de spécifications pour la prochaine génération de SNMP, sur la base d'une convergence des concepts et des éléments techniques de SNMPv2u et SNMPv2*, comme l'avait été suggéré par une équipe conseil qui avait été formée pour fournir une seule recommandation d'approche pour l'évolution de SNMP.

En faisant ainsi, le mandat du groupe de travail définissait les objectifs suivants :

- * accommoder la large gamme d'environnements de fonctionnement aux demandes de gestion ;
- * faciliter le besoin de transition des multiples protocoles antérieurs vers SNMPv3 ;
- * faciliter l'établissement et la maintenance des activités.

Dans le travail initial du groupe de travail SNMPv3, le groupe s'est concentré sur la sécurité et l'administration, incluant :

- * l'authentification et la confidentialité,
- * l'autorisation et le contrôle d'accès fondé sur la vue, et
- * la configuration à distance fondée sur la norme de celles-ci.

Le groupe de travail SNMPv3 n'a pas "réinventé la roue", mais réutilisé les documents du projet Internet SNMPv2, c'est-à-dire, les RFC 1902 à 1908 pour les portions du concept qui étaient en dehors de la portée visée.

Les principaux contributeurs du groupe de travail SNMPv3 et le groupe de travail en général, ont plutôt consacré de considérables efforts à traiter le chaînon manquant -- sécurité et administration -- et ce processus a provoqué des contributions inestimables à l'état de l'art de la gestion.

Ils ont produit un projet fondé sur une architecture modulaire avec des capacités d'évolution en mettant l'accent sur la mise en couches. Il en résulte que SNMPv3 peut être vu comme SNMPv2 avec des capacités supplémentaires de sécurité et d'administration.

En faisant ainsi, le groupe de travail a réalisé l'objectif de production d'une seule spécification qui a non seulement l'accord de l'IETF mais aussi la sécurité et l'administration.

6. Spécifications des modules du cadre SNMPv3

La spécification du cadre de gestion SNMPv3 est partagée d'une façon modulaire en plusieurs documents. C'est l'intention du groupe de travail SNMPv3 que, avec les soins appropriés, tout document individuel, ou tous, puissent être révisés, mis à niveau, ou remplacés lorsque les exigences changent, qu'une nouvelle compréhension est obtenue, et que de nouvelles technologies deviennent disponibles.

Chaque fois que c'est faisable, l'ensemble initial de documents qui définissent le cadre de gestion SNMPv3 exerce un effet de levier sur les investissements antérieurs de définition et de mise en œuvre du cadre de gestion SNMPv2 en incorporant par référence chacune des spécifications du cadre de gestion SNMPv2.

Le cadre SNMPv3 augmente ces spécifications avec des spécifications pour la sécurité et l'administration pour SNMPv3.

Les documents qui spécifient le cadre de gestion SNMPv3 suivent la même architecture que celle des versions antérieures et peuvent être organisés pour les besoins de l'exposé en quatre catégories principales comme suit :

- * le langage de définition des données,
- * les modules de base de données d'information de gestion (MIB, *Management Information Base*),
- * les opérations du protocole, et
- * la sécurité et l'administration.

Les trois premiers ensembles de documents sont incorporés de SNMPv2. Les documents du quatrième ensemble sont nouveaux pour SNMPv3, mais, comme décrit précédemment, s'appuient sur les travaux significatifs antérieurs.

6.1 Langage de définition des données

Les spécifications du langage de définition des données inclut le STD 58, "Structure des informations de gestion, version 2 (SMIV2)" [RFC2578], et les spécifications qui s'y rapportent. Ces documents sont des mises à jour des [RFC1902], [RFC1903] et [RFC1904] qui ont évolué indépendamment des autres parties du cadre et ont été republiées avec des changements rédactionnels mineurs comme STD 58, [RFC2578], [RFC2579] et [RFC2580] lorsque elles ont été promues du statut de projet de norme à celui de norme à part entière.

La structure des informations de gestion (SMIV2) définit les types fondamentaux de données, un modèle d'objet, et les règles d'écriture et de révision des modules de MIB. Les spécifications qui s'y rapportent incluent le STD 58, RFC2579, RFC2580.

Le STD 58, "Conventions textuelles pour SMIV2" [RFC2579], définit un ensemble initial d'abréviations qui sont disponibles pour l'utilisation au sein de tous les modules de MIB pour l'agrément des lecteurs humains et des rédacteurs.

Le STD 58, "Déclarations de conformité pour SMIV2" [RFC2580], définit le format des déclarations de conformité qui sont utilisés pour décrire les exigences pour les mises en œuvre d'agent et les déclarations de capacités qui peuvent être utilisées pour documenter les caractéristiques de mises en œuvre particulières.

Le terme "SMIV2" est un peu ambigu parce que les utilisateurs du terme l'entendent comme ayant au moins deux significations différentes. Parfois le terme est utilisé pour se référer au langage entier de définition de données du STD 58, défini collectivement comme les RFC 2578 à 2580 tandis que d'autres fois, il est utilisé pour se référer seulement à la portion du langage de définition de données défini dans la RFC 2578. Cette ambiguïté est malheureuse mais pose rarement en pratique un problème significatif.

6.2 Modules de MIB

Les modules de MIB contiennent habituellement des définitions d'objets, peuvent contenir des définitions de notifications d'événements, et incluent parfois des déclarations de conformité spécifiées en termes de groupes appropriés d'objets et de notifications d'événement. À ce titre, les modules de MIB définissent les informations de gestion conservées par l'instrumentation dans les nœuds gérés, rendues accessibles à distance par les agents de gestion, convoyées par le protocole de gestion, et manipulées par les applications de gestion.

Les modules de MIB sont définis conformément aux règles établies dans les documents qui spécifient le langage de définition des données, principalement la SMI complétée par les spécifications concernées.

Il y a un grand nombre, croissant, de modules de MIB en cours de normalisation, comme défini dans la liste mise à jour périodiquement des "Normes officielles des protocoles de l'Internet" [STD0001]. Au moment de la rédaction du présent document, il y a plus de 100 modules de MIB en cours de normalisation avec un nombre total d'objets définis qui dépasse les 10 000. De plus, il y a un nombre encore plus grand de modules de MIB spécifiques d'entreprises définis unilatéralement par divers fabricants, groupes de recherche, consortiums, et autres, résultant en un nombre inconnu et virtuellement innombrable d'objets définis.

En général, les informations de gestion définies dans un module de MIB, sans considération de la version du langage de définition de données utilisé, peuvent être utilisées avec toute version du protocole. Par exemple, les modules de MIB définis dans les termes de la SMI SNMPv1 (SMIv1) sont compatibles avec le cadre de gestion SNMPv3 et peuvent être convoyés par les protocoles qui y sont spécifiés. De plus, les modules de MIB définis dans les termes de la SMI SNMPv2 (SMIv2) sont compatibles avec les opérations du protocole SNMPv1 et peuvent être portées par lui. Cependant, il y a une exception notable : le type de données Counter64 qui peut être défini dans un module de MIB défini dans le format SMIv2 mais qui ne peut pas être porté par un moteur de protocole SNMPv1. Il peut être porté par un moteur SNMPv2 ou SNMPv3, mais ne peut pas l'être par un moteur qui ne prend en charge que SNMPv1.

6.3 Opérations de protocole et transpositions de transport

Les spécifications pour les opérations et les transpositions de transport du cadre SNMPv3 sont incorporées par référence aux deux documents du cadre SNMPv2 qui ont été ultérieurement mis à jour.

La spécification des opérations de protocole se trouve dans le STD 62, "Version 2 des opérations de protocole pour le protocole simple de gestion de réseau (SNMP)" [RFC3416].

Le cadre SNMPv3 est conçu pour permettre que les diverses portions de l'architecture évoluent indépendamment. Par exemple, il se pourrait qu'une nouvelle spécification des opérations de protocole soit définie au sein du cadre pour permettre des opérations de protocole supplémentaires.

La spécification des transpositions de transport se trouve dans le STD 62, "Transpositions de transport pour le protocole simple de gestion de réseau (SNMP)" [RFC3417].

6.4 Sécurité et administration de SNMPv3

La série de documents qui relève de la sécurité et l'administration SNMPv3 définie par le groupe de travail SNMPv3 consiste en sept documents pour l'instant :

RFC 3410, "Introduction et déclarations d'applicabilité pour le cadre de gestion normalisé de l'Internet", qui est le présent document.

STD 62, "Architecture de description des cadres de gestion du protocole simple de gestion de réseau (SNMP)" [RFC3411], décrit l'architecture globale avec un accent particulier sur l'architecture de la sécurité et de l'administration.

STD 62, "Traitement et distribution de message pour le protocole simple de gestion de réseau (SNMP)" [RFC3412], décrit la possibilité de multiples modèles de traitement de message et la portion répartiteur qui peut être incorporée dans un moteur de protocole SNMP.

STD 62, "Applications du protocole simple de gestion de réseau (SNMP)" [RFC3413], décrit les cinq types initiaux d'applications qui peuvent être associés à un moteur SNMPv3 et leurs éléments de procédure.

STD 62, "Modèle de sécurité fondée sur l'utilisateur (USM) pour la version 3 du protocole simple de gestion de réseau (SNMPv3)" [RFC3414], décrit les menaces contre lesquelles la protection est fournie, ainsi que les mécanismes, protocoles, et les données de support utilisés pour fournir la sécurité au niveau du message SNMP avec le modèle de sécurité fondé sur l'utilisateur.

STD 62, "Modèle de contrôle d'accès fondé sur la vue (VACM) pour le protocole simple de gestion de réseau (SNMP)" [RFC3415], décrit comment peut être appliqué le contrôle d'accès fondé sur la vue au sein d'applications de répondeur de commandes et de générateur de notifications.

La [RFC2576], "Coexistence entre les versions 1, 2 et 3 du cadre de gestion de réseau de l'Internet", décrit la coexistence entre le cadre de gestion SNMPv3, le cadre de gestion SNMPv2 et le cadre de gestion original SNMPv1, et est en cours de mise à jour par la RFC3584.

7. Résumé des documents

Les paragraphes qui suivent fournissent un bref résumé de chaque document avec un peu plus de détails que ce qui est donné ci-dessus.

7.1 Structure des informations de gestion

Les informations de gestion sont vues comme une collection d'objets gérés, résidant dans un magasin virtuel d'informations, appelé la base de données d'informations de gestion (MIB, *Management Information Base*). Les collections d'objets qui s'y rapportent sont définis dans les modules de MIB. Ces modules sont écrits dans le langage de définition de données SNMP, qui a évolué depuis un sous ensemble adapté de la notation de syntaxe abstraite numéro un (ASN.1, *Abstract Syntax Notation One*) [ASN.1] de l'OSI. Le STD 58, RFC 2578, 2579, 2580, définit collectivement le langage de définition des données, spécifie les types de base des données pour les objets, spécifie un ensemble cœur de spécifications abrégées pour les types de données appelées conventions textuelles, et spécifie quelques allocations administratives de valeurs d'identifiants d'objets (OID).

La SMI est divisée en trois parties : définitions de modules, définitions d'objets, et définitions de notifications.

- (1) Les définitions de modules sont utilisées pour décrire les modules d'informations. Une macro ASN.1, IDENTITÉ DE MODULE, est utilisée pour porter de façon concise la sémantique d'un module d'informations.
- (2) Les définitions d'objets sont utilisées pour décrire les objets gérés. Une macro ASN.1, TYPE D'OBJET, est utilisée pour porter de façon concise la syntaxe et la sémantique d'un objet géré.
- (3) Les définitions de notifications sont utilisées pour décrire les transmissions non sollicitées des informations de gestion. Une macro ASN.1, TYPE DE NOTIFICATION, est utilisée pour porter de façon concise la syntaxe et la sémantique d'une notification.

Comme noté précédemment, le terme "SMIv2" est un peu ambigu parce que les utilisateurs du terme l'entendent comme ayant au moins deux significations différentes. Parfois, le terme est utilisé pour se référer au langage entier de définition des données du STD 58, défini collectivement dans les RFC 2578 - 2580 tandis que d'autres fois, il est utilisé pour se référer seulement à la portion du langage de définition de données défini dans la RFC 2578. Cette ambiguïté est malheureuse mais est rarement en pratique un problème significatif.

7.1.1 Spécification de la SMI de base

Le STD 58, [RFC2578] spécifie les types de base de données pour le langage de définition des données, qui incluent : Integer32, entiers énumérés, Unsigned32, Gauge32, Counter32, Counter64, TimeTicks, ENTIER, CHAINE D'OCTETS, IDENTIFIANT D'OBJET, IpAddress, Opaque, et BITS. Il alloue aussi des valeurs à plusieurs identifiants d'objet. Le STD 58, RFC 2578 définit aussi les constructions suivantes du langage de définition des données :

- * IMPORTE pour permettre la spécification d'éléments utilisés dans un module de MIB, mais définis dans un autre module de MIB.
- * -IDENTITÉ DE MODULE pour spécifier pour un module de MIB une description et les informations administratives comme les contacts et l'historique des révisions.
- * IDENTITÉ D'OBJET et allocation de valeur d'OID pour spécifier une valeur d'OID.
- * TYPE D'OBJET pour spécifier le type de données, le statut, et la sémantique des objets gérés.
- * Allocation du type de SEQUENCE pour faire la liste des objets colonnaires dans un tableau.
- * Les constructions TYPE DE NOTIFICATION pour spécifier une notification d'événement.

7.1.2 Conventions textuelles

Lors de la conception d'un module de MIB, il est souvent utile de spécifier, en abrégé, la sémantique d'un ensemble d'objets au comportement similaire. On le fait en définissant un nouveau type de données avec un type de données de base spécifié dans la SMI. Chaque nouveau type a un nom différent, et spécifie un type de base avec une sémantique plus restrictive. Ces nouveaux types définis sont appelés des conventions textuelles, et sont utilisés pour la convenance des lecteurs humains du module de MIB et éventuellement par des applications de gestion "intelligentes". C'est l'objet du STD 58, [RFC2579], "Conventions textuelles pour SMIV2, de définir la construction, CONVENTION TEXTUELLE, du langage de définition des données utilisé pour définir de tels types nouveaux et de spécifier un ensemble initial de conventions textuelles disponibles pour tous les modules de MIB.

7.1.3 Déclarations de conformité

Il peut être utile de définir les limites inférieures acceptables de mise en œuvre, ainsi que le niveau réel de mise en œuvre réalisée. C'est l'objet du STD 58, [RFC2580], "Déclarations de conformité pour SMIV2" de définir les constructions du langage de définition des données utilisées à cette fin. Il y a deux sortes de constructions :

- (1) Des déclarations de conformité sont utilisées pour décrire les exigences sur les agents par rapport aux définitions de notification d'objet et d'événement. La construction CONFORMITÉ DE MODULE est utilisée pour porter de manière concise de telles exigences.
- (2) Des déclarations de capacités sont utilisées pour décrire les capacités des agents par rapport aux définitions de notification d'objet et d'événement. La construction CAPACITÉS D'AGENT est utilisée pour porter de manière concise de telles capacités.

Finalement, les collections d'objets en rapports et les collections de notifications d'événements en rapport sont groupées ensemble pour former une unité de conformité. La construction GROUPE D'OBJETS est utilisée pour porter de manière concise les objets et la sémantique d'un groupe d'objets. La construction GROUPE DE NOTIFICATION est utilisée pour porter de façon concise les notifications d'événement et la sémantique d'un groupe de notification d'événement.

7.2 Opérations du protocole

Le protocole de gestion assure l'échange des messages qui transportent les informations de gestion entre les agents et les stations de gestion. La forme de ces messages est une "enveloppe" de message qui encapsule une unité de données de protocole (PDU, *Protocol Data Unit*).

C'est l'objet du STD 62, [RFC3416], "Version 2 des opérations de protocole pour le protocole simple de gestion de réseau (SNMP)", de définir les opérations du protocole par rapport à l'envoi et la réception des PDU.

7.3 Transpositions de transport

Les messages SNMP peuvent être utilisés sur diverses suites de protocoles. C'est l'objet du STD 62, [RFC3417], "Transpositions de transport pour le protocole simple de gestion de réseau (SNMP)", de définir comment les messages SNMP se transposent en un ensemble initial de domaines de transport. D'autres transpositions pourront être définies à l'avenir.

Bien que plusieurs transpositions soient définies, la transposition sur UDP est la préférée. À ce titre, pour assurer le plus haut niveau d'interopérabilité, les systèmes qui choisissent de déployer d'autres transpositions devraient aussi assurer le service de mandataire pour la transposition sur UDP.

7.4 Instrumentation du protocole

L'objet du STD 62, [RFC3418], "Base de données d'informations de gestion (MIB) pour le protocole simple de gestion de réseau (SNMP)" est de définir les objets gérés qui décrivent le comportement de portions d'une entité SNMP.

7.5 Architecture, sécurité et administration

L'objet du STD 62, [RFC3411], "Architecture de description des cadres de gestion du protocole simple de gestion de réseau (SNMP)", est de définir une architecture pour spécifier les cadres de gestion. Bien qu'elle traite des questions générales d'architecture, elle se concentre sur les aspects relatifs à la sécurité et l'administration. Elle définit un certain nombre de termes

utilisés dans tout les cadres de gestion SNMPv3 et, ce faisant, précise et étend les dénominations :

- * des moteurs et applications,
- * des entités (qui fournissent des services, comme les moteurs des agents et gestionnaires),
- * des identités (utilisateurs de services), et
- * des informations de gestion, incluant la prise en charge de contextes logiques multiples.

Le document contient un petit module de MIB qui est mis en œuvre par tous les moteurs de protocole SNMPv3 d'autorité.

7.6 Traitement et répartition des messages

Le STD 62, [RFC3412], "Traitement et distribution de message pour le protocole simple de gestion de réseau (SNMP)", décrit le traitement des messages et la répartition des messages SNMP au sein de l'architecture SNMP. Elle définit les procédures pour répartir d'éventuellement multiples versions de messages SNMP aux modèles de traitement de messages SNMP appropriés, et pour répartir les PDU aux applications SNMP. Le document décrit aussi un modèle de traitement de message – le modèle de traitement de message SNMPv3.

Un moteur de protocole SNMPv3 DOIT prendre en charge au moins un modèle de traitement de message. Un moteur de protocole SNMPv3 PEUT en prendre en charge plus d'un, par exemple dans un système multilingue qui assure la prise en charge simultanée de SNMPv3 et de SNMPv1 et/ou SNMPv2c. Par exemple, un tel système trilingue qui fournit la prise en charge simultanée de SNMPv1, SNMPv2c, et SNMPv3 prend en charge trois modèles de traitement de message.

7.7 Applications SNMP

L'objet du STD 62, [RFC3413], "Applications du protocole simple de gestion de réseau (SNMP)" est de décrire les cinq types d'applications qui peuvent être associées à un moteur SNMP. Ce sont les générateurs de commandes, les répondeurs de commandes, les générateurs de notifications, les receveurs de notifications, et les transmetteurs mandataires.

Le document définit aussi des modules de MIB pour spécifier des cibles d'opérations de gestion (incluant des notifications) pour le filtrage des notifications et pour la transmission par mandataire.

7.8 Modèle de sécurité fondé sur l'utilisateur

Le STD 62, [RFC3414], "Modèle de sécurité fondé sur l'utilisateur (USM) pour la version 3 du protocole simple de gestion de réseau (SNMPv3)" décrit le modèle de sécurité fondé sur l'utilisateur pour SNMPv3. Il définit les éléments de procédure pour fournir la sécurité au niveau du message SNMP.

Le document décrit les deux menaces principales et deux menaces secondaires contre lesquelles la défense est assurée par le modèle de sécurité fondé sur l'utilisateur. Ce sont la modification des informations, l'usurpation d'identité, la modification du flux de messages, et la divulgation.

Le modèle USM utilise MD5 [RFC1321] et l'algorithme de hachage sécurisé [FIPS180-1] comme algorithmes de hachage chiffrés [RFC2104] pour le calcul de résumés pour assurer l'intégrité des données :

- * pour protéger directement contre les attaques de modification des données,
- * pour fournir indirectement l'authentification de l'origine des données, et
- * pour défendre contre les attaques par usurpation d'identité.

Le modèle USM utilise des indicateurs temporels à accroissement monotone synchronisé de façon lâche pour la défense contre certaines attaques de modification de flux de messages. Les mécanismes de synchronisation automatique d'horloge fondés sur le protocole sont spécifiés sans dépendance à des sources horaires tierces et sans les considérations de sécurité concomitantes.

Le modèle USM utilise la norme de chiffrement des données (DES, *Data Encryption Standard*) [FIPS46-1] en mode d'enchaînement du bloc de chiffrement (CBC, *cipher block chaining*) si la protection contre la divulgation est désirée. La prise en charge de DES dans l'USM est facultative, principalement parce que des restrictions à l'exportation et l'usage dans de nombreux pays rendent difficile l'exportation et l'utilisation de produits qui incluent des technologies cryptographiques.

Le document inclut aussi une MIB convenable pour la surveillance et la gestion à distance des paramètres de configuration pour l'USM, incluant la distribution et la gestion des clés.

Une entité peut fournir simultanément la prise en charge de plusieurs modèles de sécurité ainsi que plusieurs protocoles d'authentification et de confidentialité. Tous les protocoles utilisés par l'USM se fondent sur des clés pré-placées, c'est-à-dire, des mécanismes de clé privée. L'architecture SNMPv3 permet l'utilisation de mécanismes et protocoles symétriques et asymétriques (les mécanismes asymétriques sont couramment appelés "cryptographie à clé publique") mais au moment de

cette rédaction, il n'y a pas de modèle de sécurité SNMPv3 sur la voie de la normalisation à l'IETF qui utilise la cryptographie à clé publique.

Des travaux sont en cours pour spécifier comment AES sera utilisé au sein du modèle de sécurité fondé sur l'utilisateur (USM). Cela constituera un document séparé.

7.9 Contrôle d'accès fondé sur la vue

L'objet du STD 62, [RFC3415], "Modèle de contrôle d'accès fondé sur la vue (VACM) pour le protocole simple de gestion de réseau (SNMP)", est de décrire le modèle de contrôle d'accès fondé sur la vue pour son utilisation dans l'architecture SNMP. Le VACM peut être simultanément associé dans une seule mise en œuvre de moteur à plusieurs modèles de traitement de message et plusieurs modèles de sécurité.

Il est possible architecturalement d'avoir plusieurs modèles de contrôle d'accès actifs différents et présents simultanément dans une seule mise en œuvre de moteur, mais on s'attend à ce que ceci soit très rare en pratique et beaucoup moins courant que la prise en charge simultanée de plusieurs modèles de traitement de message et/ou plusieurs modèles de sécurité.

7.10 Coexistence et transition avec SNMPv3

L'objet de la [RFC2576], "Coexistence entre la version 1, la version 2, et la version 3 du cadre normalisé de gestion de réseau Internet", est de décrire la coexistence entre le cadre de gestion SNMPv3, le cadre de gestion SNMPv2 et le cadre de gestion SNMPv1 d'origine. En particulier, ce document décrit quatre aspects de la coexistence :

- * La conversion des documents de MIB du format SMIV1 en SMIV2,
- * la transposition des paramètres de notification,
- * les approches de coexistence entre les entités qui prennent en charge les diverses versions de SNMP dans un réseau multilingue, en particulier le traitement des opérations de protocole dans les mises en œuvre multilingues, ainsi que le comportement des mises en œuvre de mandataires,
- * le modèle de traitement de message SNMPv1 et le modèle de sécurité fondé sur la communauté, qui fournit des mécanismes pour adapter SNMPv1 et SNMPv2c dans le modèle de contrôle d'accès fondé sur la vue (VACM) [RFC3415].

8. État de normalisation

Le lecteur devrait consulter la dernière version de la liste des "Normes Officielles de protocole de l'Internet" [STD0001] pour déterminer l'état de normalisation de tout document.

Cependant, le groupe de travail SNMPv3 a explicitement demandé qu'un texte soit inclus dans le présent document pour préciser le statut de SMIV1, SNMPv1, et SNMPv2c.

8.1 Statut de SMIV1

SMIV1, comme décrit dans le STD 16, RFC 1155 et 1212, a été promu au statut de norme à part entière en 1990 et est resté une norme même après que la SMIV2 ait atteint le statut de norme (voir la [RFC2026] pour plus d'informations sur le processus des normes de l'Internet). Dans de nombreux cas, une norme est déclarée "Historique" lorsque son remplaçant atteint le statut de norme à part entière. Par exemple, la MIB-1 [RFC1156] a été déclarée "Historique" lorsque la MIB-2 [RFC1213] est devenue une norme à part entière. De façon similaire, quand la SMIV2 est devenue une norme, il aurait été raisonnable à ce moment de retirer la SMIV1 et de la déclarer "Historique" mais par suite d'une décision consciente, le STD 16, RFC 1155 et 1212 continue d'avoir le statut de normalisation de "Norme" à part entière mais n'est pas recommandé. Ces documents n'ont pas été déclarés "Historiques" et restent sur la voie de la normalisation parce qu'ils fournissent des références normatives pour d'autres documents sur la voie de la normalisation et ne peuvent pas être déclarés "Historiques" sans rendre les documents qui s'appuient sur elles aussi "Historiques".

Par conséquent, le STD 16 conserve son statut de normalisation mais n'est pas recommandé parce qu'il a été supplanté par les plus récentes spécifications de la SMIV2 qui sont identifiées un peu plus loin dans ce document.

D'un point de vue pratique, comme depuis 1993 il a été avisé pour les utilisateurs du langage de définition des données d'utiliser la SMIV2 pour tous les nouveaux travaux parce que la réalité du marché a occasionnellement exigé la prise en charge de définitions de données dans les deux formats SMIV1 et SMIV2. Bien qu'il y ait des outils largement disponibles à bas prix ou gratuitement pour traduire les définitions de la SMIV2 en définitions SMIV1, il n'est pas pratique de construire des outils automatiques de traduction des définitions de SMIV1 en définitions de SMIV2. Par conséquent, si on travaille principalement en SMIV2, le coût de fourniture des définitions de données dans les deux formats SMIV1 et SMIV2 est trivial. À l'opposé, si on

travaille principalement en format SMIV1, fournir des définitions de données dans les deux formats SMIV1 et SMIV2 est significativement plus coûteux. Les exigences du marché d'aujourd'hui pour fournir les définitions de données dans le format SMIV1 sont très diminuées comparées à celles de 1993, et la SMIV2 continue d'être le format fortement préféré bien que SMIV1 n'ait pas été déclarée "Historique". Bien sûr, l'IETF exige actuellement que les nouveaux modules de MIB soient écrits avec SMIV2.

8.2 Statut de normalisation de SNMPv1 et SNMPv2

Les opérations de protocole via les enveloppes de message SNMPv1 et SNMPv2c ne prennent en charge qu'une authentification triviale fondée sur des chaînes communautaires de texte en clair et par suite, sont fondamentalement non sûres. Lorsque les spécifications SNMPv3 pour la sécurité et l'administration, qui incluent une forte sécurité, ont atteint le statut de norme à part entière, la norme SNMPv1, anciennement STD 15 [RFC1157], et les spécifications expérimentales SNMPv2c décrites dans la [RFC1901] ont été déclarées historiques à cause de leur faiblesse à l'égard de la sécurité et pour émettre le message clair que la troisième version du cadre de gestion standard de l'Internet est le cadre choisi. Les différentes parties de SNMPv2 (SNMPv2p), SNMPv2u, et SNMPv2* ont été déclarées historiques autour de 1995 ou n'ont jamais été mises sur la voie de la normalisation.

Sur un plan pratique, on s'attend à ce qu'un certain nombre de fabricants continuent de produire et que les usagers continueront de déployer et utiliser des mises en œuvre multilingues qui prennent en charge SNMPv1 et/ou SNMPv2c aussi bien que SNMPv3. On notera que le processus des normes de l'IETF ne contrôle pas les actions des fabricants ni des usagers qui peuvent choisir de promouvoir ou déployer des protocoles historiques, tels que SNMPv1 et SNMPv2c, en dépit de leurs insuffisances connues. Cependant, on se s'attend pas à ce que des fabricants produisent, ni que des usagers déploient des mises en œuvre multilingues qui prennent en charge le SNMPv2p fondé sur les parties (SNMPv2p), SNMPv2u, ou SNMPv2*.

Bien sûr, comme décrit ci-dessus, une des spécifications SNMPv3 pour la sécurité et l'administration, la [RFC2576], "Coexistence entre version 1, version 2, et version 3 du cadre de gestion normalisé de l'Internet", traite ces questions.

Il est certainement important que les usagers qui déploient des systèmes multilingues avec des protocoles non sûrs mettent en œuvre toutes les précautions pour s'assurer que les configurations limitent l'accès via SNMPv1 et SNMPv2c de façon appropriée, en respectant la politique de sécurité de leur organisation, tout comme ils devraient veiller à limiter l'accès accordé via SNMPv3 avec un niveau de sécurité sans authentification ni confidentialité, ce qui est en gros équivalent du point de vue de la sécurité. Par exemple, il n'est probablement pas raisonnable de permettre à SNMPv1 ou SNMPv2c un plus haut niveau d'accès que celui fourni aux utilisateurs SNMPv3 non authentifiés, par exemple, il n'est pas raisonnable de faire garder la porte principale par des hommes armés, des chiens d'attaque entraînés, des fossés et des ponts-levis alors qu'on laisse ouverte sans surveillance la porte de derrière.

Le cadre SNMPv1, le cadre SNMPv2 et SNMPv2c ont des capacités limitées pour administrer les protocoles SNMPv1 et SNMPv2c. Par exemple, aucun objet n'est défini pour voir et configurer les communautés ou les destinations pour les notifications (filtres et informations). Le résultat a été des mécanismes définis par les fabricants pour l'administration qui vont des fichiers de configuration de format propriétaire qui ne peuvent être vus ou configurés via SNMP à des définitions d'objets spécifiques de l'entreprise. Le cadre SNMPv3 fournit une approche riche fondée sur les normes pour l'administration qui, par conception, peut être utilisée pour les protocoles SNMPv1 et SNMPv2c. Donc, pour nourrir l'interopérabilité de l'administration des protocoles SNMPv1 et SNMPv2c dans des systèmes multilingues, les mécanismes et objets spécifiés dans les [RFC3413], [RFC3415], et la [RFC2576] devraient être utilisés pour compléter ou remplacer le mécanisme propriétaire équivalent.

8.3 Recommandation du groupe de travail

Sur la base des explications ci-dessus, le groupe de travail SNMPv3 recommande que les RFC 1157, 1441, 1901, 1909 et 1910 soient reclassées comme documents historiques.

9. Considérations sur la sécurité

Comme le présent document est principalement une feuille de route, il n'introduit aucune nouvelle considération sur la sécurité. Le lecteur se reportera aux sections pertinentes de chacun des documents référencés pour des informations sur les considérations de sécurité.

10. Références

- [ASN.1] International Organization for Standardization. International Standard 8824, "Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)", (décembre 1987).
- [FIPS46-1] National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) Publication 46-1 "Data Encryption Standard". Remplace la publication FIPS 46, (janvier 1977 ; confirmée en janvier 1988).
- [FIPS180-1] NIST FIPS 180-1, "Secure Hash Algorithm". (avril 1995) <http://csrc.nist.gov/fips/fip180-1.txt> (ASCII) <http://csrc.nist.gov/fips/fip180-1.ps> (Postscript)
- [RFC1052] V. Cerf, "Recommandations de l'IAB pour le développement de normes de gestion du réseau Internet", avril 1988.
- [RFC1055] J. Romkey, "Non norme pour la [transmission des datagrammes IP](#) sur des lignes en série : SLIP", STD 47, juin 1988.
- [RFC1056] M. Lambert, "PCMAIL : un système de messagerie réparti pour les ordinateurs individuels", juin 1988.
- [RFC1057] Sun Microsystems, Inc. "RPC : Protocole de procédure d'appel à distance", juin 1988.
- [RFC1212] M. Rose et K. McCloghrie, "[Définitions concises de MIB](#)", STD 16, février 1991.
- [RFC1213] K. McCloghrie et M. Rose, "[Base de données d'informations de gestion](#) pour la gestion de réseau des internets fondés sur TCP/IP : MIB-II", STD 17, mars 1991.
- [RFC1215] M. Rose, "Convention pour la définition de filtres à utiliser avec le SNMP", mars 1991. (*Info*)
- [RFC1321] R. Rivest, "Algorithme de [résumé de message MD5](#)", avril 1992. (*Information*)
- [RFC1902] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Structure des informations de gestion pour la version 2 du protocole simple de gestion de réseau (SNMPv2)", janvier 1996. (*Obsolète, voir [RFC2578](#)*) (*D.S.*)
- [RFC1903] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Conventions textuelles pour la version 2 du protocole simple de gestion de réseau (SNMPv2)", janvier 1996. (*Obsolète, voir [RFC2579](#)*) (*D.S.*)
- [RFC1904] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Déclarations de conformité pour la version 2 du protocole simple de gestion de réseau (SNMPv2)", janvier 1996. (*Obsolète, voir [RFC2580](#)*) (*D.S.*)
- [RFC1905] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Opérations de protocole pour la version 2 du protocole simple de gestion de réseau (SNMPv2)", janvier 1996. (*Obsolète, voir [RFC3416](#)*) (*D.S.*)
- [RFC1906] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Transpositions de transport pour la version 2 du protocole simple de gestion de réseau (SNMPv2)", janvier 1996. (*Obsolète, voir [RFC3417](#)*) (*D.S.*)
- [RFC1907] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Base de données d'informations de gestion pour la version 2 du protocole simple de gestion de réseau (SNMPv2)", janvier 1996. (*Obsolète, voir [RFC3418](#)*) (*D.S.*)
- [RFC1908] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Coexistence entre la version 1 et la version 2 du cadre de gestion de réseau standard de l'Internet", janvier 1996. (*Obsolète, voir [RFC2576](#)*) (*D.S.*)
- [RFC2026] S. Bradner, "Le processus de [normalisation de l'Internet](#) -- Révision 3", ([BCP0009](#)) octobre 1996. (*Remplace [RFC1602](#), [RFC1871](#)*) (*MàJ par [RFC3667](#), [RFC3668](#), [RFC3932](#), [RFC3979](#), [RFC3978](#), [RFC5378](#), [RFC6410](#)*)
- [RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : [Hachage de clés pour l'authentification](#) de message", février 1997.
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [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.*)
- [RFC2577] M. Allman, S. Ostermann, "[Considérations sur la sécurité de FTP](#)", mai 1999. (*Information*)

- [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](#))
- [RFC3411] D. Harrington, R. Presuhn, B. Wijnen, "[Architecture de description des cadres de gestion](#) du protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par* [RFC5343](#)) ([STD0062](#))
- [RFC3412] J. Case et autres, "[Traitement et distribution de message](#) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. ([STD0062](#))
- [RFC3413] D. Levi, P. Meyer et B. Stewart, "[Applications du protocole](#) simple de gestion de réseau (SNMP)", STD 62, décembre 2002.
- [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](#))
- [RFC3417] R. Presuhn, éd., "[Transpositions de transport](#) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par* [RFC4789](#)) ([STD0062](#))
- [RFC3418] R. Presuhn, éd., "[Base de données d'informations de gestion](#) (MIB) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. ([STD0062](#))
- [STD0001] "Official Internet Protocol Standards", <http://www.rfc-editor.org/rfcxx00.html> aussi STD0001.

11. Adresse des éditeurs

Jeffrey Case
SNMP Research, Inc.
3001 Kimberlin Heights Road
Knoxville, TN 37920-9716
USA
téléphone : +1 865 573 1434
mél : case@snmp.com

Russ Mundy
Network Associates Laboratories
15204 Omega Drive, Suite 300
Rockville, MD 20850-4601
USA
téléphone : +1 301 947 7107
mél : mundy@tislabs.com

David Partain
Ericsson
P.O. Box 1248
SE-581 12 Linköping
Sweden
téléphone : +46 13 28 41 44
mél : David.Partain@ericsson.com

Bob Stewart
Retraité

12. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2002).

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 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.

Remerciement

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