ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Norme et Standard d'administration réseau

www.ofppt.info

OFPPT

DIRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

SECTEUR NTIC

Sommaire

1. Présentation de l'administration réseau

Alors qu'un réseau évolue et s'étend, il devient une ressource de plus en plus cruciale et indispensable pour l'organisation.
À mesure que des ressources réseau sont mises à la disposition des utilisateurs, le réseau devient plus complexe et sa gestion devient plus compliquée. La perte de ressources réseau et les mauvaises performances sont les conséquences de cette augmentation de la complexité et ne sont pas acceptables pour les utilisateurs. L'administrateur doit gérer activement le réseau, diagnostiquer les problèmes, empêcher certaines situations de survenir et fournir les meilleures performances réseau possibles aux utilisateurs. Il arrive un moment où les réseaux deviennent trop étendus pour être administrés sans outils de gestion automatiques.

L'administration réseau implique les tâches ci-dessous:

- La surveillance de la disponibilité du réseau
- L'amélioration de l'automatisation
- La surveillance des temps de réponse
- La mise en place de fonctionnalités de sécurité
- Le réacheminement du trafic
- Le rétablissement de la fonctionnalité
- L'enregistrement d'utilisateurs

Les forces qui régissent l'administration réseau sont présentées et expliquées ci-dessous :

- **Contrôle des ressources de l'entreprise** – Si les ressources réseau ne sont pas gérées de façon efficace, elles n'offrent pas les résultats exigés par une bonne administration.

- **Contrôle de la complexité** – Avec la croissance massive du nombre de composants réseau, d'utilisateurs, d'interfaces, de protocoles et de constructeurs, la perte de contrôle du réseau et de ses ressources constitue une menace pour l'administration.

- **Amélioration du service** – Les utilisateurs attendent des services similaires ou améliorés lorsque le réseau s'étend et que les ressources deviennent plus dispersées.

- **Équilibrage des divers besoins** – Diverses applications doivent être mises à la disposition des utilisateurs à un niveau donné de support, avec des exigences spécifiques en termes de performances, de disponibilité et de sécurité.

- **Réduction des temps d'arrêt** – Assurer la haute disponibilité des ressources au moyen d'une conception redondante adéquate.

- **Contrôle des coûts** – Surveillance et contrôle de l'utilisation des ressources, de manière à satisfaire l'utilisateur pour un coût raisonnable.

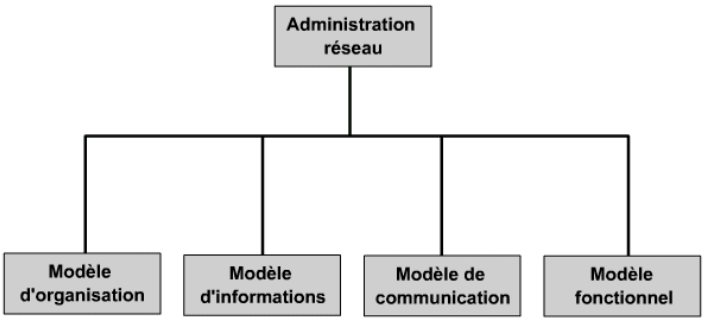
Certains termes élémentaires d'administration réseau sont présentés à la figure

Terme	Définition
SNMP	SNMP (Simple Network Management Protocol) est une norme universelle définie par l'IETF, destinée à la gestion des ressources réseau.
MIB	La base d'informations de management (MIB - Management Information Base) est la structure/la définition des données d'un objet géré.
RMON	RMON (Remote Monitoring) est une spécification d'agent/MIB définissant les fonctions de surveillance des équipements distants.
RFC	Les requêtes pour commentaires (Request For Comments ou RFC) sont des documents émis par l'IETF. Certaines ont été adoptées en tant que normes Internet.
NMS	La station d'administration réseau (Network Management Station) est une station SNMP conçue pour l'administration des équipements réseau. Il s'agit généralement d'une " boîte " UNIX ou NT qui exécute HP Openview, SunNET Mgr ou NetView pour AIX.

2. OSI et le modèle d'administration réseau

L'organisme international de normalisation ISO (*International Standards Organization*) a créé un comité visant à produire un modèle pour l'administration réseau, sous la direction du groupe OSI.
Ce modèle se décline en quatre parties:

- Le modèle d'organisation
- Le modèle d'informations
- Le modèle de communication
- Le modèle fonctionnel



Ceci constitue une vue du haut en bas de l'administration réseau, divisée en quatre sous-modèles et reconnue par la norme OSI.

Le modèle d'organisation décrit les composants de l'administration réseau, par exemple administrateur, agent, et ainsi de suite, avec leurs relations. La disposition de ces composants mène à différents types d'architecture, décrits plus loin dans ce document.

Le modèle d'informations est relatif à la structure et au stockage des informations d'administration réseau. Ces informations sont stockées dans une base de données, appelée base d'informations de management (MIB). L'ISO a établi la structure des informations d'administration (SMI) pour définir la syntaxe et la sémantique des informations d'administration stockées dans la MIB. Les MIB et les SMI sont étudiées en profondeur ultérieurement.
Le modèle de communication traite de la manière dont les données d'administration sont transmises entre les processus agent et administrateur. Il est relatif au protocole d'acheminement, au protocole d'application et aux commandes et réponses entre égaux.

Le modèle fonctionnel concerne les applications d'administration réseau qui résident sur la station d'administration réseau (NMS). Le modèle d'administration OSI compte cinq domaines fonctionnels, parfois appelés le modèle FCAPS:

- Les erreurs
- La configuration
- La comptabilité
- Les performances
- La sécurité

Ce modèle d'administration réseau a largement été adopté par les constructeurs au titre de méthode utile de description des besoins de n'importe quel système d'administration réseau.

3. Normes SNMP et CMIP

Pour permettre l'interopérabilité de l'administration sur de nombreuses plates-formes réseau différentes, des normes d'administration s'avèrent nécessaires pour que les constructeurs puissent les mettre en oeuvre et y adhérer. Deux normes principales ont émergé:

- Le protocole SNMP (*Simple Network Management Protocol*) – Communauté IETF
- Le protocole CMIP (*Common Management Information Protocol*) – Communauté des télécommunications

Le protocole SNMP désigne un ensemble de normes d'administration, notamment un protocole, une spécification de structure de base de données et un ensemble d'objets de données.

SNMP a été adopté comme norme pour les réseaux Internet TCP/IP en 1989 et est devenu très populaire. Une mise à niveau, le protocole SNMP version 2c (SNMPv2c) a été adoptée en 1993. SNMPv2c permet de prendre en charge les stratégies d'administration réseau centralisées et distribuées et offre des améliorations au niveau de la structure des informations d'administration (SMI), des opérations de protocole, de l'architecture d'administration et de la sécurité. Il a été conçu pour fonctionner sur les réseaux OSI, ainsi que les réseaux TCP/IP.

Depuis, SNMPv3 a été mis en circulation. Pour résoudre les défauts de sécurité de SNMPv1 et SNMPv2c, SNMPv3 fournit un accès sécurisé aux MIB en authentifiant et en cryptant les paquets acheminés sur le réseau.

CMIP est un protocole de gestion de réseaux OSI créé et normalisé par l'ISO pour la surveillance et le contrôle de réseaux hétérogènes.

4. Fonctionnement du protocole SNMP

SNMP est un protocole de la couche d'application conçu pour faciliter l'échange d'informations d'administration entre les équipements réseau.

En utilisant SNMP pour accéder aux données d'informations d'administration, telles que le nombre de paquets par seconde envoyés sur une interface ou le nombre de connexions TCP ouvertes, les administrateurs réseau peuvent mieux gérer les performances du réseau et mieux rechercher et résoudre les problèmes.

Aujourd'hui, SNMP constitue le protocole le plus répandu pour gérer divers interréseaux commerciaux, universitaires et de recherche.

L'activité de normalisation se poursuit à mesure que les constructeurs développent et mettent sur le marché des applications de pointe d'administration SNMP. SNMP est un protocole simple, mais ses fonctions sont suffisamment efficaces pour gérer les problèmes liés à l'administration des réseaux hétérogènes.

Le modèle organisationnel de l'administration réseau SNMP comporte quatre éléments:

- La station d'administration
- L'agent de supervision
- La base d'informations de management
- Le protocole de gestion de réseau

La NMS est généralement une station de travail autonome, mais elle peut être mise en oeuvre sur plusieurs systèmes. Elle contient un ensemble de logiciels appelés l'application d'administration réseau (NMA). La NMA comporte une interface utilisateur permettant aux administrateurs autorisés de gérer le réseau. Elle répond à des commandes utilisateur et à des commandes envoyées aux agents de supervision sur l'ensemble du réseau.

Les agents de supervision sont les plates-formes et les équipements clés du réseau et les autres hôtes, routeurs, passerelles et concentrateurs équipés du protocole SNMP qui permet de les gérer. Ils répondent à des requêtes d'informations et des requêtes d'action émises par la NMS, telles que l'interrogation, et peuvent fournir à la NMS des informations très importantes, mais non demandées, telles que les Traps.

Toutes les informations de supervision d'un agent en particulier sont stockées dans la base d'informations de management de cet agent. Un agent peut effectuer un suivi des éléments suivants:

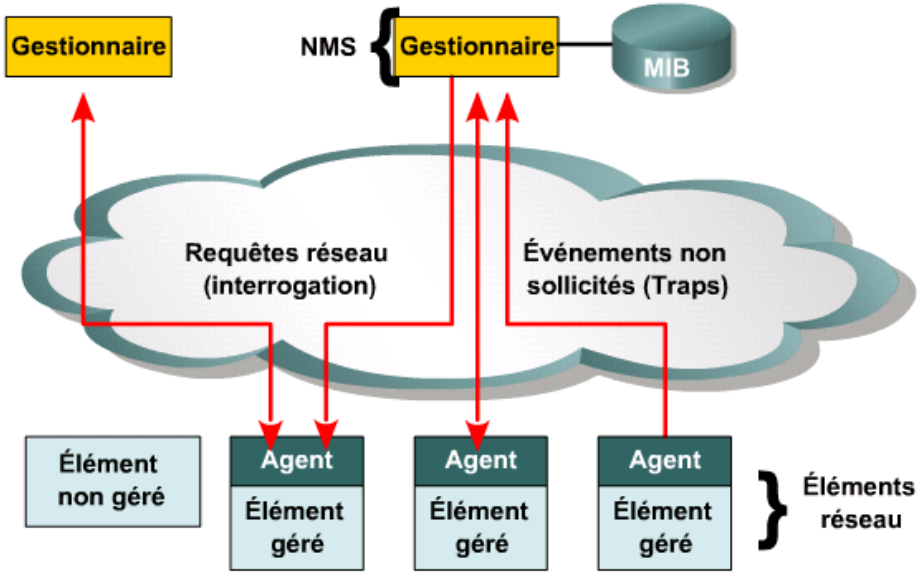
- Le nombre et l'état de ses circuits virtuels
- Le nombre de certains types de messages d'erreur reçus
- Le nombre d'octets et de paquets entrant et sortant de l'équipement

- La longueur maximale de la file d'attente de sortie pour les routeurs et autres équipements interréseaux
- Les messages de broadcast envoyés et reçus
- Les interfaces réseau qui se désactivent et s'activent

Le NMS exécute une fonction de surveillance en récupérant les valeurs dans la MIB. La NMS peut occasionner l'exécution d'une action au niveau d'un agent. La communication entre la station d'administration et l'agent est réalisée par un protocole d'administration réseau de la couche d'application. Le protocole SNMP utilise le protocole UDP (*User Datagram Protocol*) et communique sur les ports 161 et 162. Il est fondé sur un échange de messages. Il existe trois types de message courants:

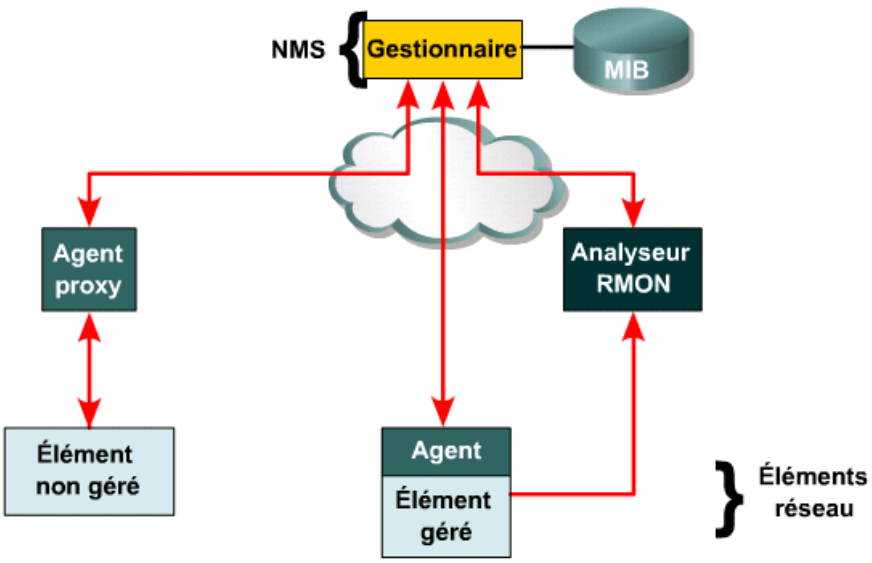
- **Get** – Permet à la station d'administration de récupérer la valeur des objets MIB à partir de l'agent.
- **Set** – Permet à la station d'administration de définir la valeur des objets MIB au niveau de l'agent.
- **Trap** – Permet à l'agent d'avertir la station d'administration lors d'événements significatifs.

Ce modèle est appelé modèle à deux niveaux. Toutefois, il présuppose que tous les éléments du réseau peuvent être administrés par SNMP.



Cela n'est pas toujours le cas, car certains équipements disposent d'une interface d'administration propriétaire.

Dans ces cas de figure, un modèle à trois niveaux s'avère nécessaire.



Une station d'administration réseau qui souhaite obtenir des informations ou contrôler ce nœud propriétaire communique avec un agent proxy.

L'agent proxy traduit alors la requête SNMP de la station d'administration en un formulaire approprié au système cible, puis utilise le protocole d'administration propriétaire approprié pour communiquer avec ce système cible. Les réponses entre la cible et le proxy sont traduites en messages SNMP et renvoyées à la station d'administration.

Les applications d'administration réseau déchargent souvent des fonctionnalités de gestion réseau à un analyseur distant (RMON). Cet analyseur RMON recueille localement des informations d'administration, puis la station d'administration réseau récupère régulièrement un résumé de ces données.

La NMS est une station de travail ordinaire, utilisant un système d'exploitation classique. Elle dispose d'une grande quantité de mémoire vive, qui lui permet d'héberger toutes les applications d'administration exécutées simultanément. La station d'administration utilise une pile de protocoles de réseau typique, telle que TCP/IP. Les applications d'administration réseau s'appuient sur le système d'exploitation hôte et sur l'architecture de communication. Les applications d'administration réseau peuvent, par exemple, être Ciscoworks2000, HP Openview et SNMPv2c.

Comme mentionné précédemment, la station d'administration peut être une station de travail autonome centralisée qui envoie des requêtes à tous les agents, quel que soit leur emplacement. Dans un réseau distribué, une architecture décentralisée s'avère plus appropriée, avec

une NMS locale au niveau de chaque site. Ces NMS distribuées peuvent fonctionner dans une architecture client-serveur, dans laquelle une NMS sert de serveur maître et les autres de clients. Les clients envoient leurs données au serveur maître pour centraliser le stockage.

Une autre possibilité consiste à attribuer une responsabilité égale à toutes les NMS distribuées, chacune disposant de ses propres bases de données de management, de telle sorte que les informations d'administration soient distribuées sur les NMS homologues.

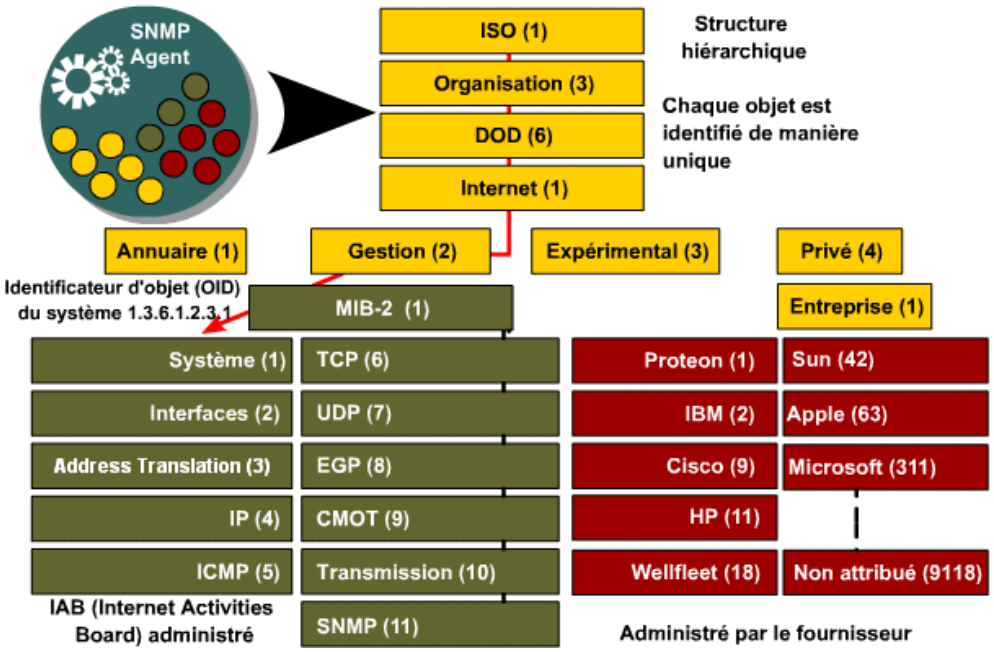
5. Structure des informations d'administration et des MIB

Une MIB permet de stocker les informations structurées représentant les éléments de réseau et leurs attributs. La structure par elle-même est définie dans une norme dénommée SMI, qui définit les types de données pouvant être utilisés pour stocker un objet, la manière dont ces objets sont nommés et celle dont ils sont cryptés pour être transmis sur un réseau.

Les MIB sont des référentiels très structurés d'informations concernant un équipement. Il existe de nombreuses bases MIB standard, mais il existe un plus grand nombre encore de MIB propriétaires, conçues pour administrer exclusivement les équipements de différents constructeurs.

La MIB SMI d'origine a été subdivisée en huit groupes différents, pour un total de 114 objets administrés. D'autres groupes ont été ajoutés pour définir MIB-II, qui remplace désormais MIB-I.

Tous les objets administrés de l'environnement SNMP sont organisés en une structure hiérarchique ou arborescente. Les objets feuille de l'arborescence, c'est-à-dire les éléments qui apparaissent dans le bas du diagramme, sont les objets administrés. Chaque objet administré représente une ressource, une activité ou une information associée à gérer. Un identificateur d'objet unique, à savoir un nombre en notation séparée par des points, identifie chaque objet administré. Chaque identificateur d'objet est décrit en notation de syntaxe abstraite (ASN.1).

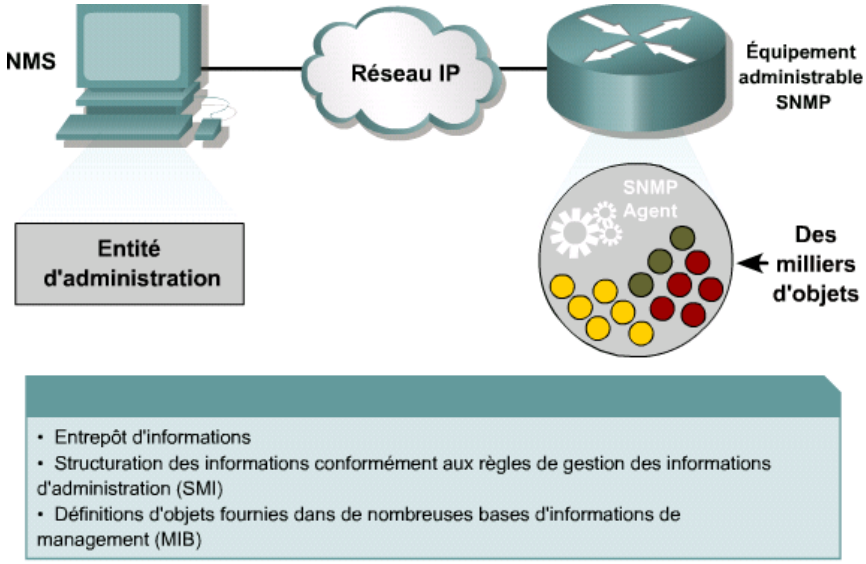


Le protocole SNMP utilise ces identificateurs d'objet pour identifier les variables MIB à récupérer ou à modifier. Les objets dans le domaine public sont décrits dans les présentations des MIB fournies dans les requêtes pour commentaires (RFC). Celles-ci peuvent facilement être consultées à l'adresse:

Tous les constructeurs sont encouragés à faire connaître leurs définitions de MIB. Une fois qu'une valeur d'entreprise assignée a été fournie, le constructeur est responsable de la création et de la gestion des sous-arborescences. http://www.ietf.org

6. Protocole SNMP

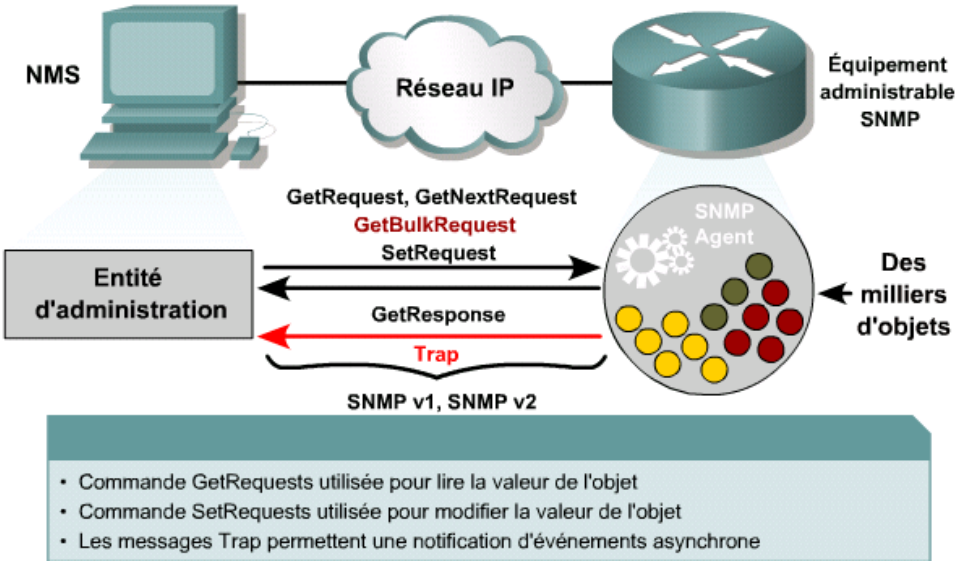
L'agent est une fonction logicielle intégrée à la plupart des équipements de réseau, tels que les routeurs, les commutateurs, les concentrateurs administrés, les imprimantes et les serveurs.



Il est responsable du traitement des requêtes SNMP provenant de la station d'administration. Il est également responsable de l'exécution de routines de gestion de variables définies dans les diverses bases MIB prises en charge.

L'interaction entre la station d'administration et l'agent est facilitée par le protocole SNMP. Le terme « simple » vient du nombre limité de types de messages faisant partie de la spécification initiale du protocole. La stratégie a été conçue pour faciliter aux développeurs l'établissement de fonctions d'administration dans les équipements de réseau. La spécification initiale du protocole est désignée par l'acronyme SNMPv1 (version 1).

Trois types de messages SNMP sont émis pour une NMS. Il s'agit des messages **GetRequest**, **GetNextRequest** et **SetRequest**.



Ces trois messages sont reconnus par l'agent sous la forme d'un message GetResponse. Un agent peut émettre un message de Trap en réponse à un événement agissant sur la MIB et sur les ressources sous-jacentes.

Le développement de SNMPv2c a permis de résoudre certaines limitations de SNMPv1. L'amélioration la plus remarquable a été l'introduction du type de message **GetBulkRequest** et l'ajout de compteurs sur 64 bits à la MIB. La récupération d'informations à l'aide de GetRequest et de GetNextRequest constituait une méthode peu efficace de collecte. Avec SNMPv1, il était seulement possible de solliciter une variable à la fois. GetBulkRequest résout cette faiblesse en permettant de recevoir plus d'informations à la suite d'une seule requête. Deuxièmement, les compteurs sur 64 bits résolvent le problème des compteurs à la rotation trop rapide, en particulier avec des liaisons à vitesse élevée telles que Gigabit Ethernet.

L'entité d'administration est également appelée station d'administration ou NMS. C'est elle qui est responsable de la sollicitation d'informations auprès de l'agent. Les sollicitations sont fondées sur des requêtes très spécifiques. La station d'administration dispose de plusieurs méthodes pour traiter les informations récupérées. Ces informations récupérées peuvent être consignées en vue d'une analyse ultérieure, affichées dans un utilitaire graphique, ou comparées à des valeurs préconfigurées pour vérifier si une condition en particulier a été remplie.

La station d'administration ne sert pas seulement à récupérer des données. Elle comporte également une fonction permettant de modifier une valeur sur l'équipement administré. Cette fonctionnalité permet à un administrateur de configurer un équipement au moyen du protocole SNMP.

L'interaction entre la station d'administration et l'équipement administré occasionne du trafic sur le réseau. Il est donc recommandé d'être prudent lorsque lors de l’introduction des stations d'administration sur le réseau.

Les stratégies de surveillance trop agressives peuvent nuire aux performances du réseau. La bande passante est alors plus sollicitée, ce qui peut constituer un problème dans les environnements de WAN. Par ailleurs, la surveillance a un impact sur les performances des équipements surveillés, puisque ceux-ci sont censés traiter les requêtes de la station d'administration. Ce traitement ne doit pas prendre la priorité sur les services de production.

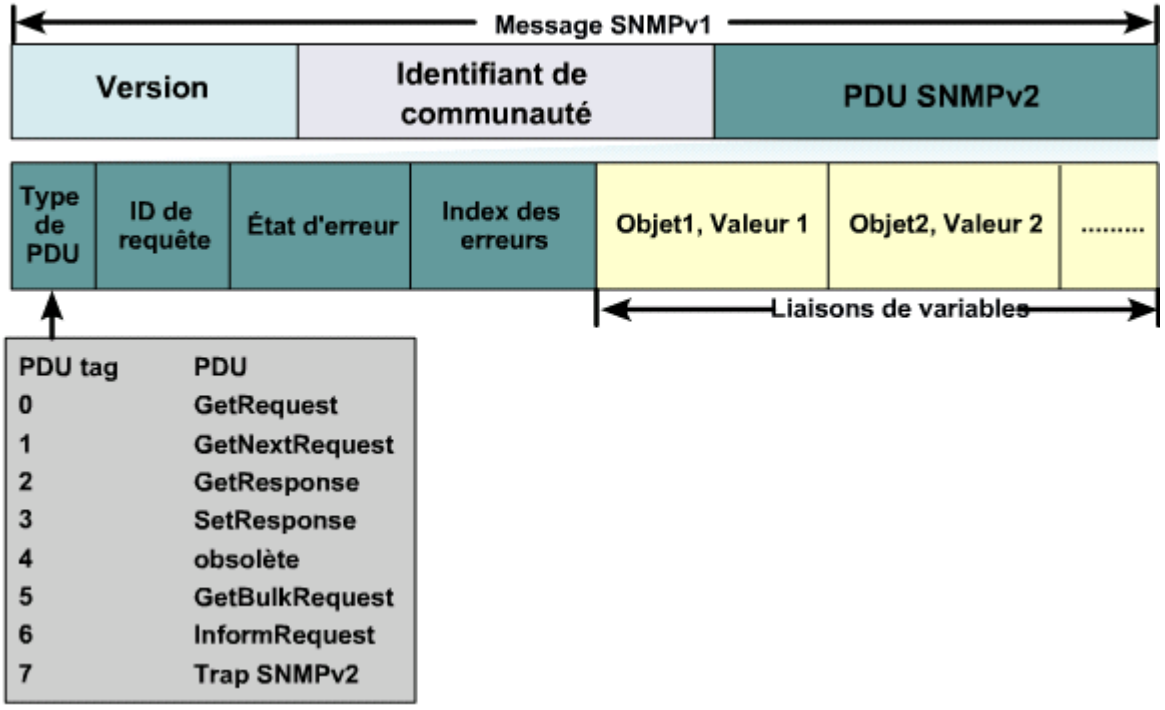
En règle générale, une quantité minimale d'informations doit être interrogée aussi rarement que possible. Déterminez les équipements et les liaisons les plus stratégiques, ainsi que le type de données nécessaire. Le protocole SNMP utilise le protocole d'acheminement UDP (User Diagram Protocol). Étant donné qu'UDP fonctionne sans connexion et n'est pas fiable, il se peut que le protocole SNMP perde des messages. Le

protocole SNMP lui-même n'est pas censé garantir la livraison et c'est donc l'application utilisant SNMP qui doit s'occuper des messages perdus.

Chaque message SNMP contient une chaîne en texte clair, que l'on appelle identifiant de communauté. L'identifiant de communauté s'utilise comme un mot de passe pour limiter l'accès aux équipements administrés. SNMPv3 a résolu les préoccupations de sécurité mises en évidence par la transmission de l'identifiant de communauté en texte clair.

Un exemple de message SNMPv2c est présenté à la figure. Une présentation détaillée du protocole est fournie dans la norme Internet RFC1905.

SNMPv2c utilise des PDU SNMPv2, mais les encapsule au format SNMPv1



Le fait que cette chaîne de communauté soit en texte clair n'est pas surprenant pour quiconque a étudié la suite de protocoles IP (*Internet Protocol*). En effet, tous les champs spécifiés dans cette suite de protocoles sont en texte clair, à l'exception des spécifications d'authentification et de cryptage.

L'identificateur de communauté était essentiellement une marque de réservation de sécurité jusqu'à ce que le groupe de travail SNMPv2 puisse ratifier les mécanismes de sécurité. Les efforts étaient présentés au groupe de travail SNMPv3. Toutes les applications d'administration SNMP doivent être configurées avec les identificateurs de communauté appropriés. Certaines entreprises modifient fréquemment les valeurs de leurs identificateurs de communauté pour réduire les risques d'activités malveillantes entraînées par une utilisation non autorisée du service SNMP.

Malgré la faiblesse associée à l'authentification par communauté, les stratégies d'administration s'appuient toujours sur SNMPv1. Les équipements Cisco prennent en charge les types de message et les fonctions de sécurité enrichies de SNMPv3, mais la plupart des logiciels d'administration ne gèrent pas SNMPv3.

SNMPv3 accepte l'existence simultanée de plusieurs modèles de sécurité.

7. Protocole CMIP

7.1. Présentation

CMIP (Common Management Information Protocol) est un protocole de gestion développé par ISO. Il peut être comparé au SNMP car les deux protocoles utilisent des tables MIB pour effectuer leur travail.

Par contre, leur fonctionnement est plutôt différent puisque dans le protocole CMIP, la station de management, ne va pas chercher elle-même les informations; elle attend que les stations rapportent leur état.

Il y a donc une grande différence de performance par rapport au SNMP. Les ressources des appareils sont énormément plus utilisées avec le CMIP, dans un rapport approximatif de 10 fois.

7.2. Principe

Son but : Normaliser les aspects de gestionnaire de gestion de réseaux, qui entraînent des échanges protocolaires entre systèmes ouverts.

Le protocole CMIP est une norme de L'ISO, les applications utilisant CMIP on été divisé en 5 domaines fonctionnels :

Gestion des configurations : comprend la modification et le stockage des configurations de tous les équipements du réseau.

Gestion des anomalies : recouvre la détection, l'isolement et la correction des pannes survenant sur un équipement. Un historique des évènements est également disponible.

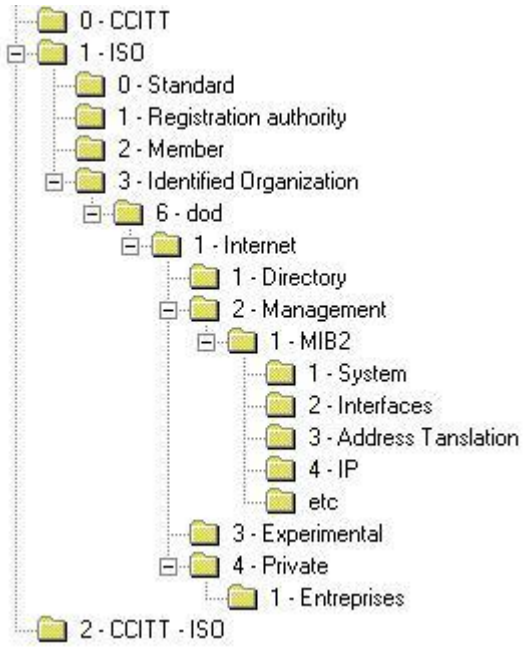
Gestion des performances : comprend la collecte des données et l'analyse statistique permettant la création de tableaux de bord. Ce domaine est essentiellement lié à l'évolution du réseau (permet de planifier les changements à apporter afin d'améliorer les performances du réseau.).

Gestion de la comptabilité : évalue la répartition de charges et le coût des ressources.

Sécurisation des données : politique de sécurité, contrôle d'accès, authentification, cryptage et historique des tentatives d'intrusion. cryptage et historique des tentatives d'intrusion.

CMIP est un protocole totalement orienté « connexion » c'est-à-dire que chaque message est acquitté.

CMIP est basé sur un principe de notification et d'évènements. Il gère chaque variable comme étant un objet.



Pour indiquer le passage à un sous-objet on utilise le point (.). Chaque nœud a un nom et un numéro unique.

SNMP utilise plutôt le code numérique de l'objet afin de diminuer la taille des trames de requêtes.

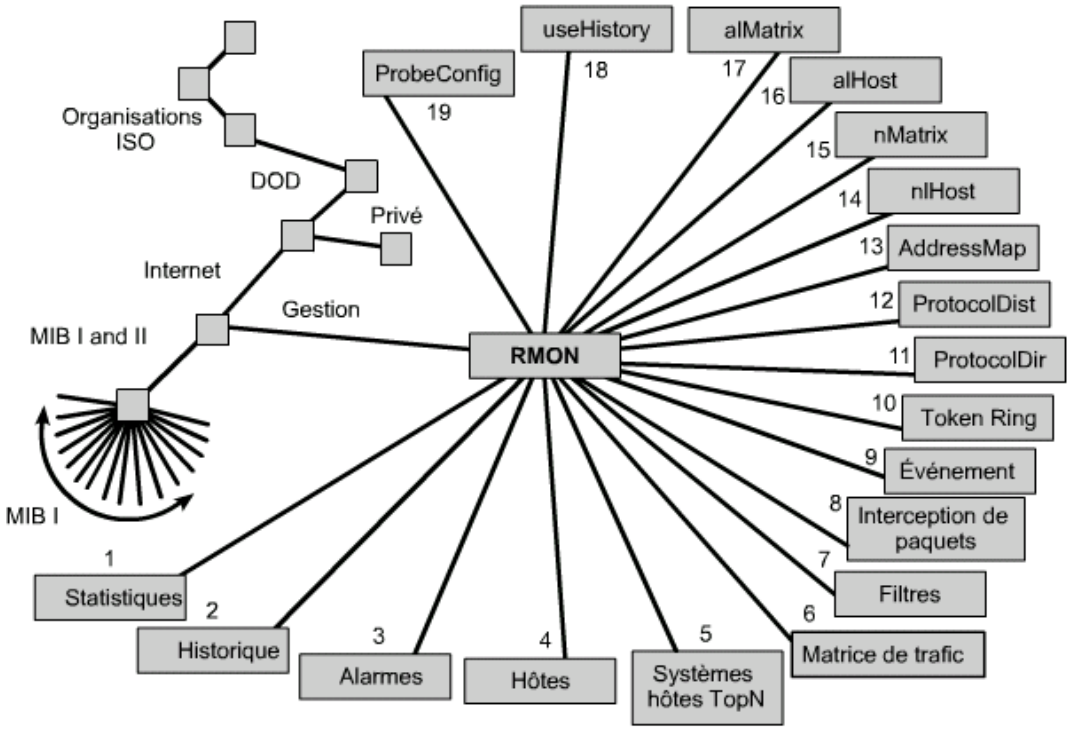
On peut ajouter des MIBs propriétaires pour avoir des informations supplémentaires sur les appareils (Cisco, HP, Alcatel, ...).

Le codage utilisé pour représenter la MIB et les messages SNMP est ASN1-BER.

8. RMON

L'analyseur RMON représente un grand pas en avant dans l'administration d'interréseaux. Il définit une MIB de surveillance à distance qui complète MIB-II et fournit à l'administrateur des informations précieuses sur le réseau. RMON offre la caractéristique remarquable de n'être qu'une spécification d'une MIB, sans modification du protocole SNMP sous-jacent, mais qui permet d'étendre considérablement la fonctionnalité SNMP.

Avec MIB-II, l'administrateur réseau peut obtenir des informations qui sont purement locales à certains équipements individuels.



Imaginons un réseau local comprenant plusieurs équipements, chacun d'entre eux doté d'un agent SNMP. Une station d'administration SNMP peut recevoir des informations sur la quantité de trafic entrant et sortant de chaque équipement, mais avec MIB-II, elle ne peut pas être informée facilement du trafic global du réseau local.
L'administration réseau dans un environnement d'interréseaux nécessite généralement un moniteur par sous-réseau.

La norme RMON, à l'origine appelée IETF RFC 1271, et maintenant RFC 1757, a été conçue pour fournir une surveillance et des diagnostics proactifs aux réseaux locaux distribués. Des dispositifs de surveillance, appelés agents ou analyseurs, placés sur des segments stratégiques du réseau permettent de créer des alarmes définies par l'utilisateur, ainsi que de rassembler une multitude de statistiques vitales grâce à l'analyse de chaque trame d'un segment.

La norme RMON répertorie les fonctions de surveillance dans neuf groupes correspondant aux topologies Ethernet, plus un dixième dans RFC 1513 pour les paramètres spécifiques à Token Ring. La norme RMON a été développée dans le but d'être déployée comme une architecture distribuée dans laquelle les agents et les analyseurs communiquent avec une station d'administration centralisée, c'est-à-dire un client, au moyen du protocole SNMP. Ces agents ont défini des structures MIB SNMP pour les neuf ou dix groupes RMON Ethernet ou Token Ring, ce qui permet une interopérabilité entre les constructeurs d'outils de diagnostic RMON. Les groupes RMON sont définis ci-dessous:

- **Groupe de statistiques** – Tient à jour les statistiques d'erreur et d'utilisation du sous-réseau ou du segment en cours de supervision. Il s'agit, par exemple, de l'utilisation de la bande passante, du broadcast, du multicast, de l'alignement CRC, des fragments, et ainsi de suite.
- **Groupe de l'historique** – Conserve des échantillons statistiques périodiques du groupe des statistiques et les stocke en vue d'une extraction ultérieure. Il s'agit, par exemple, de l'utilisation, du nombre d'erreurs et du nombre de paquets.
- **Groupe des alarmes** – Permet à l'administrateur de configurer l'intervalle et le seuil d'échantillonnage pour tout élément enregistré par l'agent. Il s'agit, par exemple, des valeurs absolues et relatives, ou des seuils en augmentation ou en diminution.
- **Groupe des systèmes hôtes** – Définit la mesure des différents types de trafic en provenance et à destination des systèmes hôtes connectés au réseau. Il s'agit, par exemple, des paquets envoyés ou reçus, des octets envoyés ou reçus, des erreurs et des paquets de broadcast et de multicast.
- **Groupe des systèmes hôtes TopN** – Génère un rapport des systèmes hôtes TOPN en s'appuyant sur les statistiques du groupe des systèmes hôtes.
- **Groupe des matrices de trafic** – Stocke les erreurs et les statistiques d'utilisation relatives aux paires de nœuds qui communiquent sur le réseau. Il s'agit, par exemple, des erreurs, des octets et des paquets.
- **Groupe des filtres** – Moteur de filtrage qui génère un flux de paquets à partir de trames correspondant au schéma défini par l'utilisateur.
- **Groupe d'interception des paquets** – Définit la méthode de mise en tampon interne des paquets qui répondent aux critères de filtrage.
- **Groupe des événements** – Permet de consigner des événements, également appelés pièges générés, à l'intention de l'administrateur, avec date et heure. Il s'agit par exemple de rapports personnalisés s'appuyant sur le type d'alarme

Mettre l'accent sur un point particulier

Note d'attention particulière.

Pour approfondir le sujet....

Proposition de références utiles permettant d'approfondir le thème abordé

Sources de référence

Citer les auteurs et les sources de référence utilisées pour l'élaboration du support