MODULE #1

243-575-RK (3-2-3)

SURVEILLANCE DE SYSTÈMES EN TÉLÉCOMMUNICATIONS

Enseignants : Sébastien Richard

MODULE #1

PROTOCOLE SNMP

Enseignants : Sébastien Richard

MODULE #1 – Protocole SNMP

- Définition du protocole SNMP
- Fonctionnement du SNMP
- Rôle du protocole SNMP
- Versions SNMP

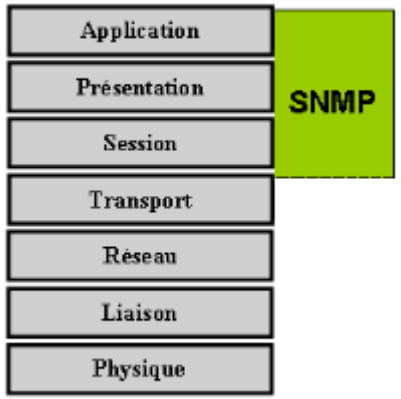
MODULE #1 – Protocole SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole de gestion de réseau. Il permet aux travailleurs dans le domaine (administrateurs réseau, technologue en télécommunications, etc…) de gérer les équipements du réseau et de visualiser les problèmes avec des logiciels qui supportent le SNMP.

Ainsi, il est possible de diagnostiquer et régler des problèmes sur le réseau.

MODULE #1 – Protocole SNMP

Le protocole SNMP est un protocole de la couche application qui fournit un format de message pour la communication entre les gestionnaires/superviseurs SNMP et les agents. SNMP fournit un langage commun, un standard afin de surveiller et gérer les périphériques du réseau.



MODULE #1 – Protocole SNMP

Le fonctionnement du protocole SNMP est simple à comprendre. Il est basé sur trois composantes principales.

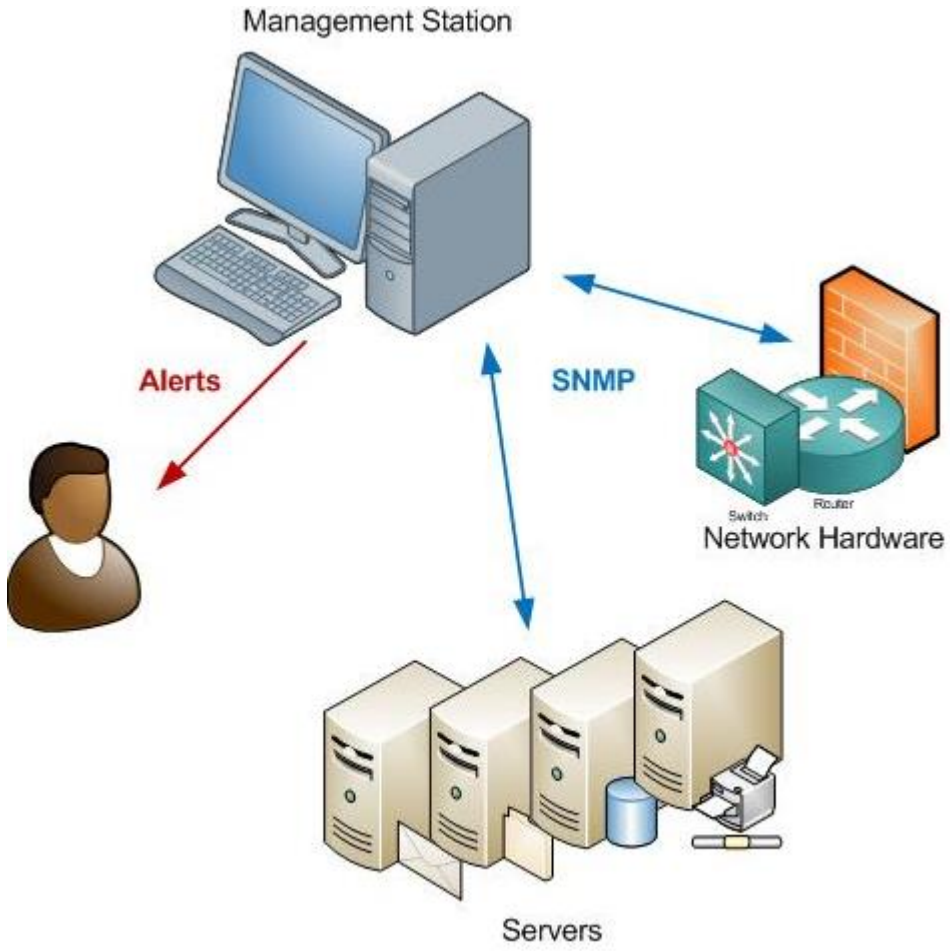
- Le **Superviseur**
- Les **Agents**
- Les **MIB**

MODULE #1 – Protocole SNMP

Superviseur:

Le superviseur est la console qui permet de gérer les requêtes de supervision SNMP.

Cette console est opérée par un administrateur qui, à partir de son poste, peut visualiser les requêtes SNMP.



MODULE #1 – Protocole SNMP

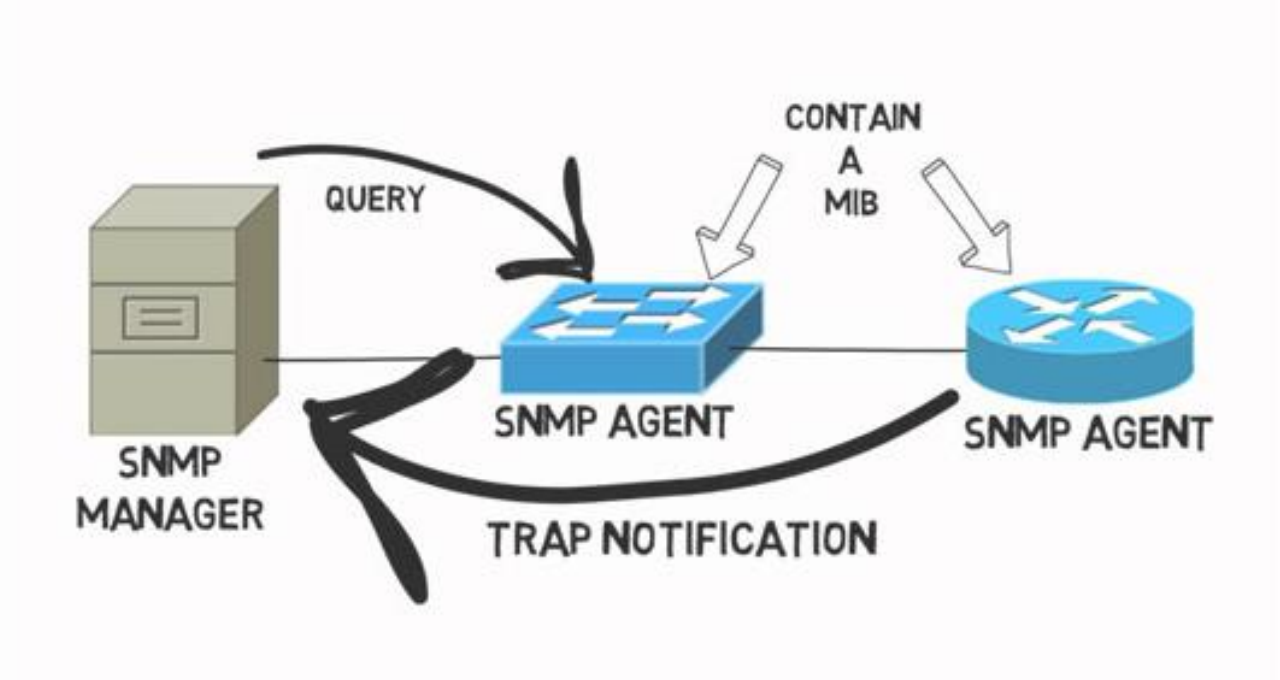
Superviseur:

Le superviseur SNMP est un système qui contrôle et surveille les activités des hôtes réseau à l'aide de SNMP.

Il envoie des requêtes aux agents afin de savoir l'états de ceux-ci sur différents objets.

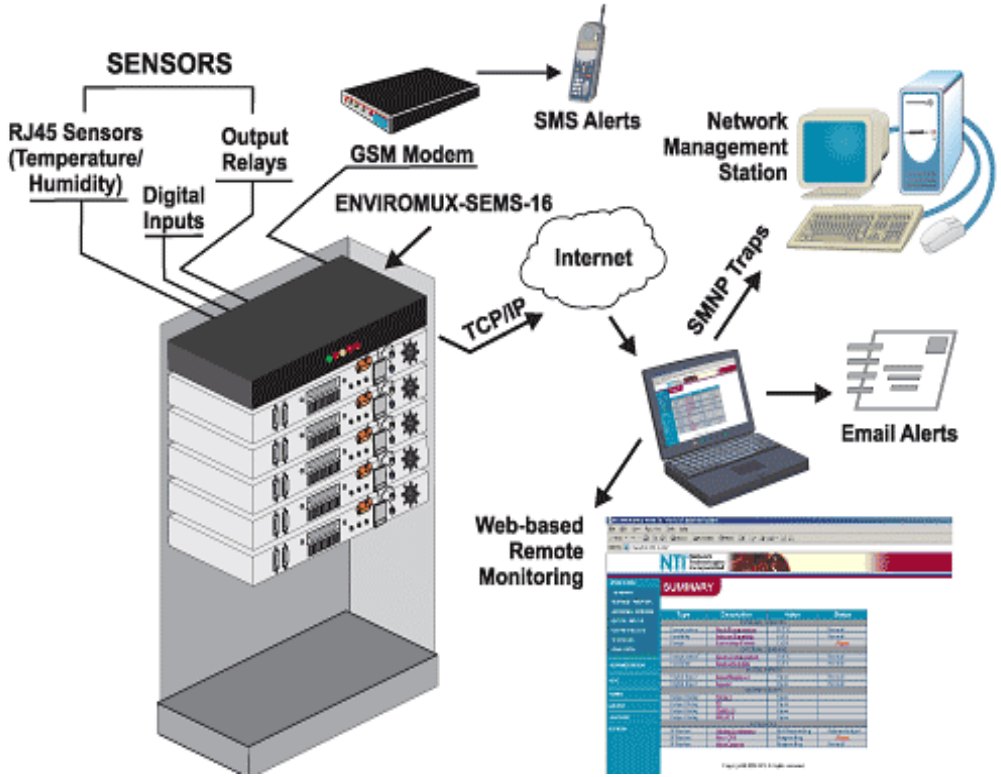
Par la suite, le superviseur reçoit de la part des agents, des notifications (Trap) sur ces différents objets qu'il sera possible de visualiser à partir d'un logiciel SNMP.

À partir de cela, il est possible de voir ce qui se passe en temps réel sur le réseau.

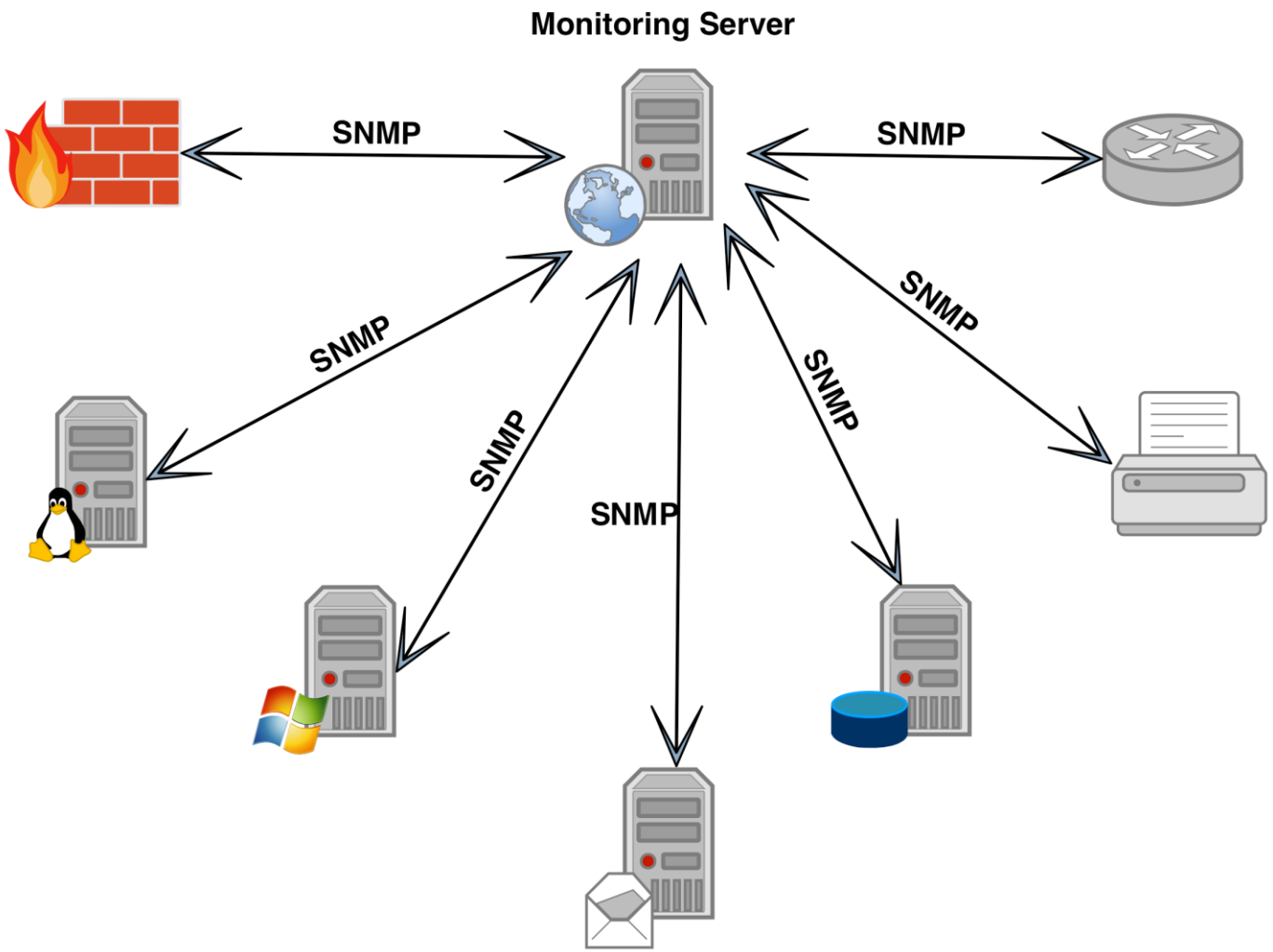


MODULE #1 – Protocole SNMP

Il est aussi possible d'être avisé par courriel ou par message texte de tout changement sur le réseau, selon des préférences configurées.



MODULE #1 – Protocole SNMP

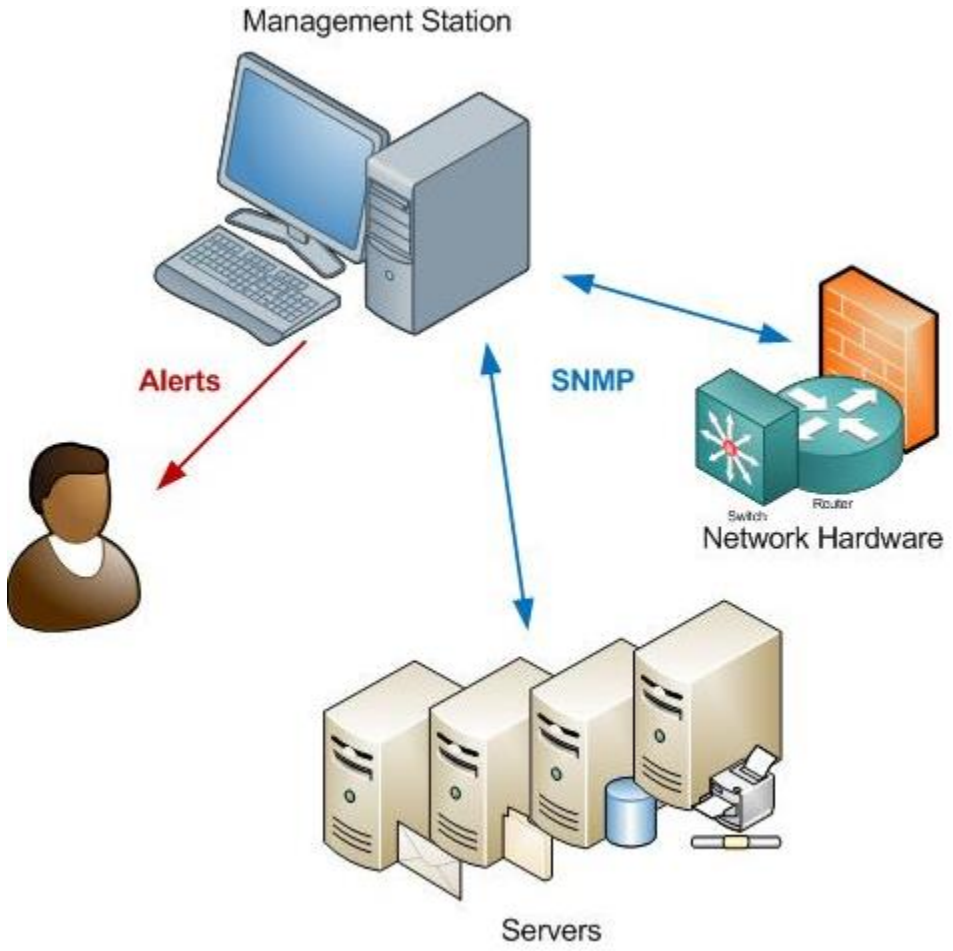


MODULE #1 – Protocole SNMP

Agents:

Les agents SNMP sont ceux qui envoient des « Trap », qui sont en réalité des informations sur différents objets.

L'agent SNMP est le composant logiciel d'un périphérique que l'on désire surveiller. Il gère les données sur l'état du périphérique et signale ces données, le cas échéant, aux systèmes de gestion. L'agent réside sur le périphérique que l'on veut gérer.



MODULE #1 – Protocole SNMP

Agents:

Pour être capable de visualiser les notifications/ Trap des agents SNMP sur le logiciel SNMP du superviseur, **il faut activer le service SNMP sur les agents**. Si ces services ne sont pas activés, le superviseur ne recevra aucunes notifications venant de cet agent.

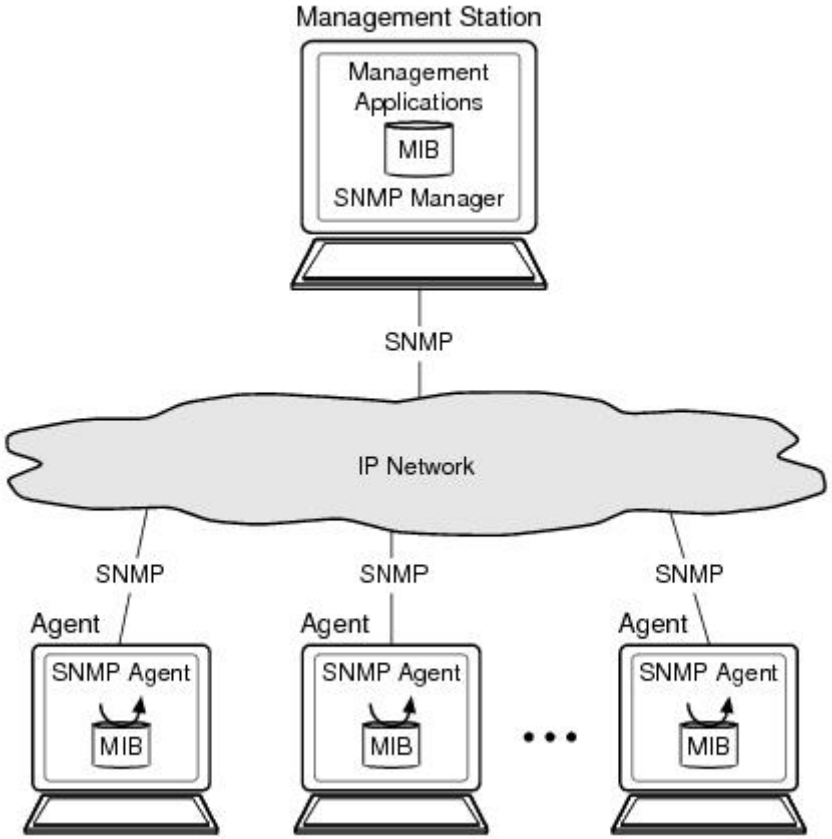
MODULE #1 – Protocole SNMP

Les MIB et les OID :

Deux concepts importants de SNMP : les OID (*object identifier*) et les MIB (*management information base*)
La MIB est la base des informations de gestion. Il y a :

- des informations à consulter,
- des paramètres à modifier,
- des alarmes à émettre…

Tout ceci, en principe, de façon indépendante du matériel et du logiciel. Il faut donc que SNMP permette de retrouver ces informations et d'agir sur les paramètres de façon indépendante du matériel, comme du logiciel.



MODULE #1 – Protocole SNMP

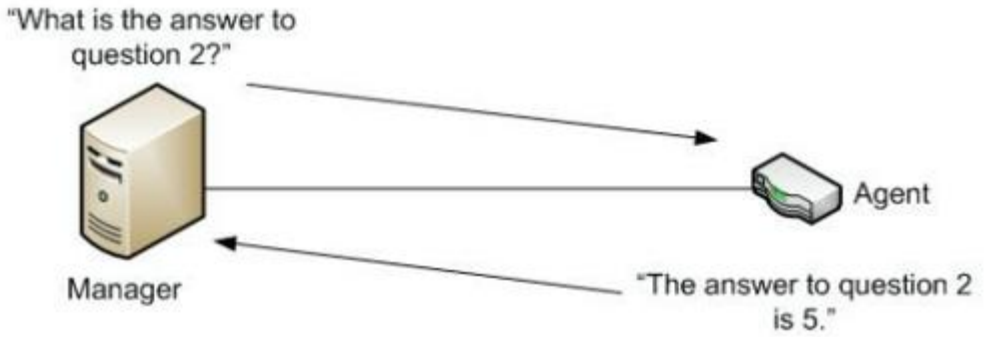
Une MIB (*management information base*) se présente donc comme une base de données normalisée, qui permettra de lire et d'écrire sur les équipements distants, de façon également normalisée. Ce sera à l'agent lui-même de faire l'interface entre les informations récupérables sur la plateforme où il est installé et le jargon utilisé par SNMP.

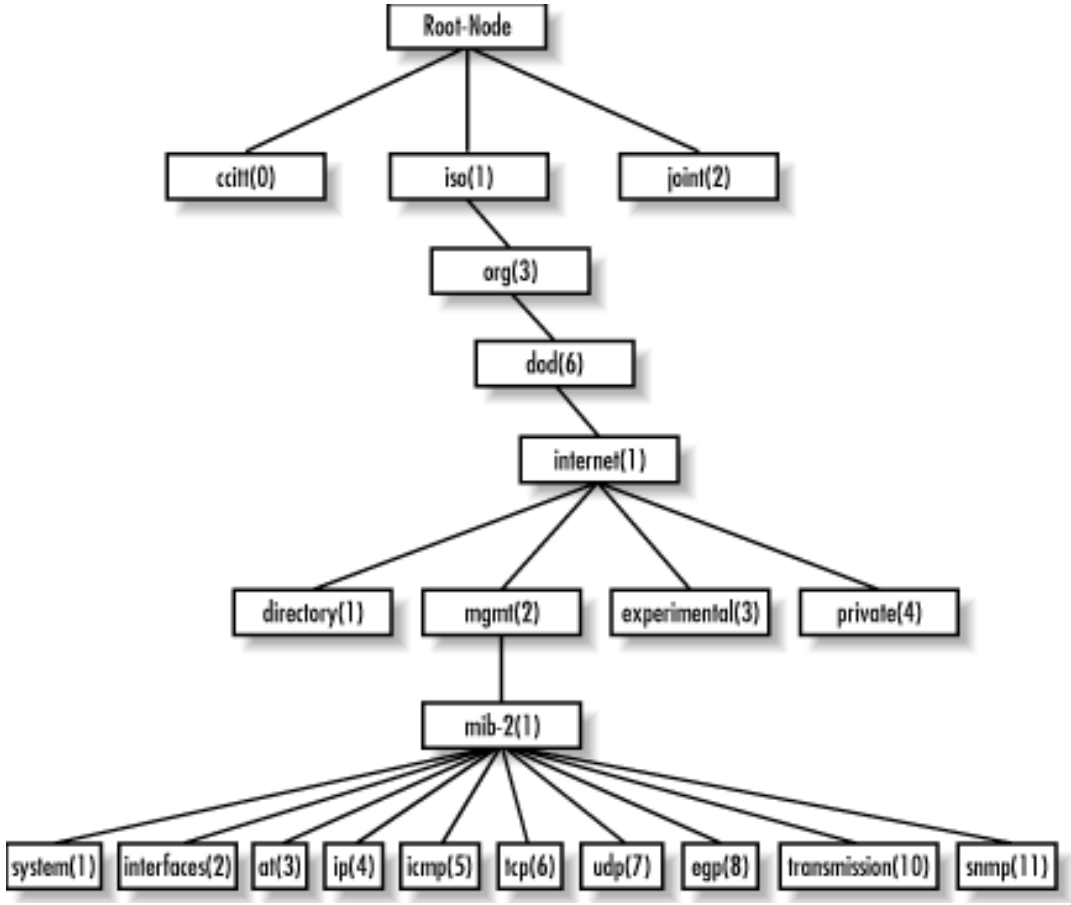
Pour illustrer le tout, la MIB contient la liste des questions que le superviseur SNMP peut demander à l'agent. De son côté, l'agent collecte toutes les données concernant toutes ces questions et les enregistre dans la MIB.

L'agent organise et met à jour tous ces paramètres, réglages et autres dans la MIB. Le superviseur (**NMS** Network Management system) fait des requêtes auprès de l'agent qui lui partage à son tour les informations de la base de données.

MODULE #1 – Protocole SNMP

Exemple simplifié du fonctionnement d'une MIB





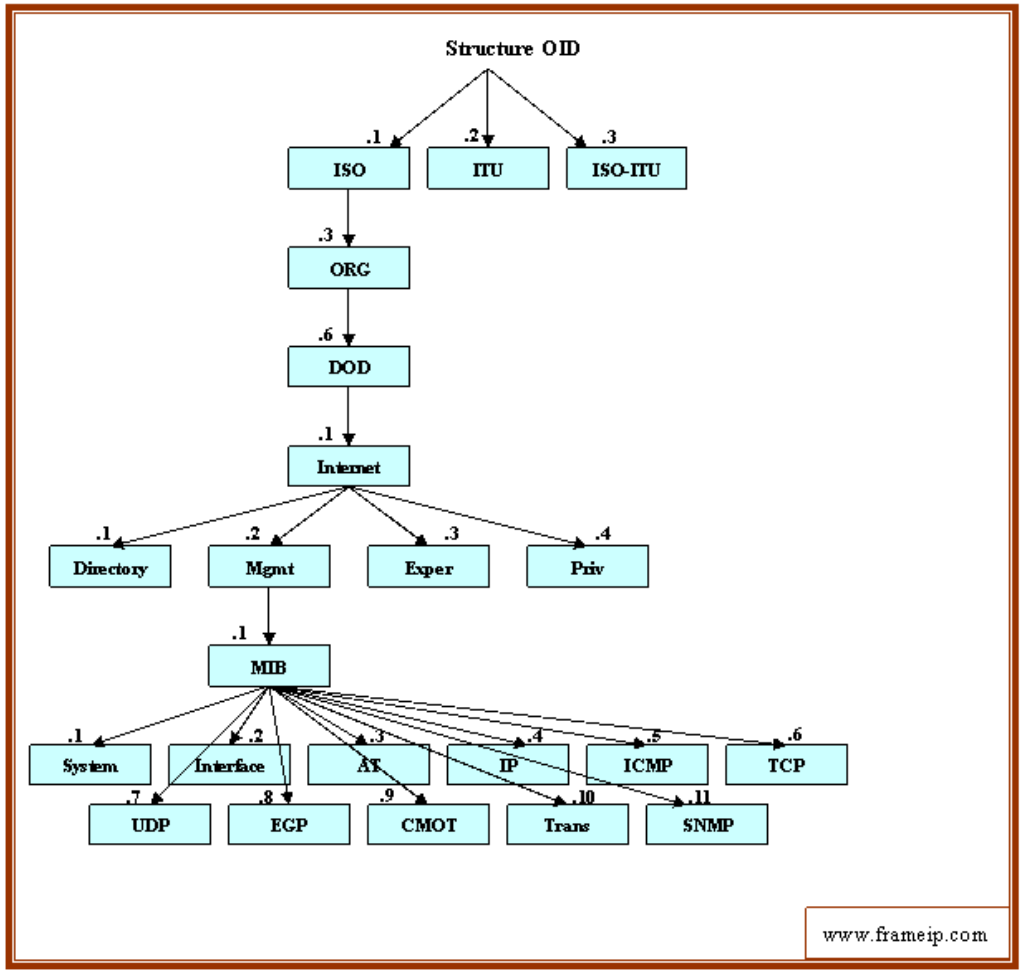
MODULE #1 – Protocole SNMP

La MIB est une structure arborescente dont chaque noeud est défini par un nombre ou **OID** (Object Identifier). Elle contient une partie commune à tous les agents SNMP en général, une partie commune à tous les agents SNMP d'un même type de matériel et une partie spécifique à chaque constructeur. Chaque équipement à superviser possède sa propre MIB. Non seulement la structure est normalisée, mais également les appellations des diverses rubriques.

Ces appellations ne sont présentes que dans un souci de lisibilité. En réalité, chaque niveau de la hiérarchie est repéré par un index numérique et SNMP n'utilise que celui-ci pour y accéder.

MODULE #1 – Protocole SNMP

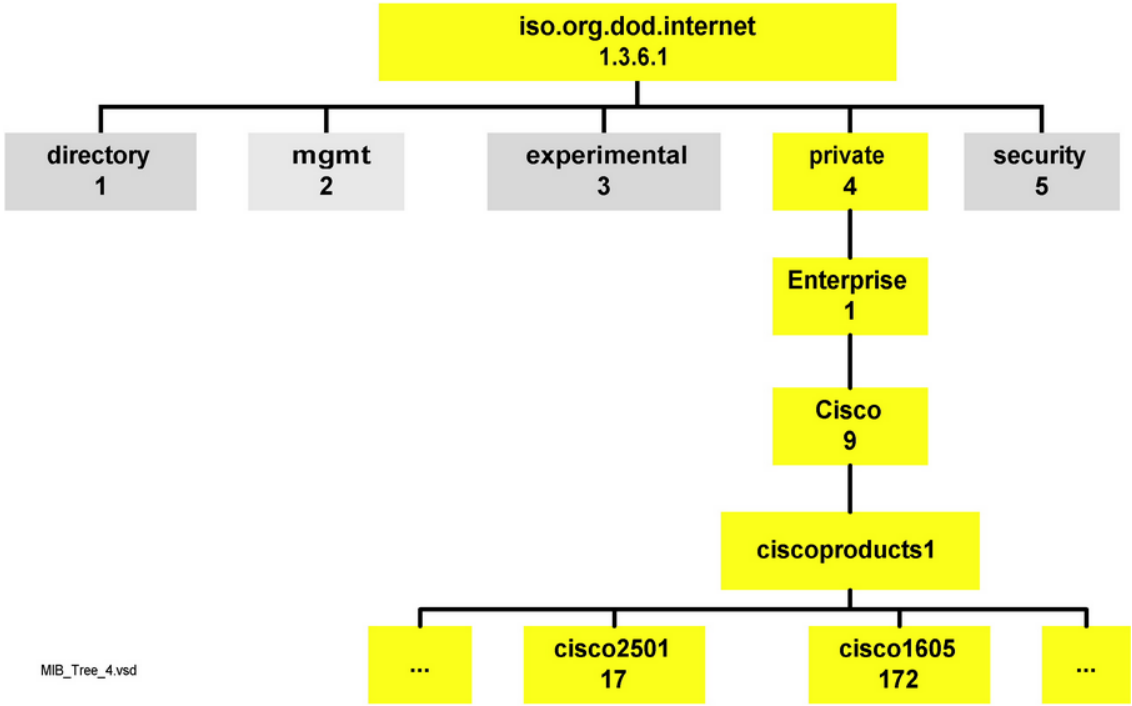
Voici un exemple de structure de table MIB :



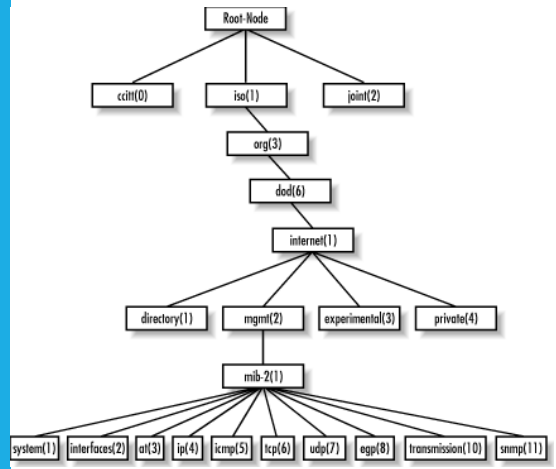
MODULE #1 – Protocole SNMP

Ainsi, pour interroger les différentes variables d'activité sur un appareil, il faudra explorer son arborescence MIB.

Ensuite, pour accéder aux variables souhaitées, on utilisera **l'OID** (**Object Identification**) qui désigne l'emplacement de la variable à consulter dans la MIB. On aura par exemple sur un commutateur Cisco l'OID (.1.3.6.1.4.1.9.9.109.1.1.1.1.6) désignant le taux de charge du CPU.



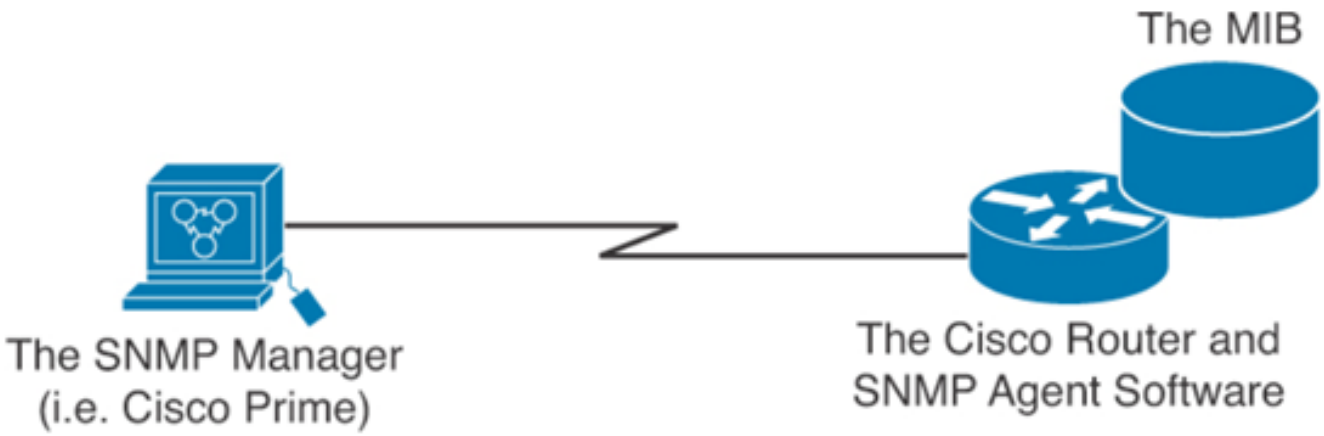
MODULE #1 – Protocole SNMP



Subtree Name	OID	Description
system	*1.3.6.1.2.1.1*	Defines a list of objects that pertain to system operation, such as the system uptime, system contact, and system name.
interfaces	*1.3.6.1.2.1.2*	Keeps track of the status of each interface on a managed entity. The *interfaces* group monitors which interfaces are up or down and tracks such things as octets sent and received, errors and discards, etc.
at	*1.3.6.1.2.1.3*	The address translation (*at*) group is deprecated and is provided only for backward compatibility. It will probably be dropped from MIB-III.
ip	*1.3.6.1.2.1.4*	Keeps track of many aspects of IP, including IP routing.
icmp	*1.3.6.1.2.1.5*	Tracks things such as ICMP errors, discards, etc.
tcp	*1.3.6.1.2.1.6*	Tracks, among other things, the state of the TCP connection (e.g., *closed*, *listen*, *synSent*, etc.).
udp	*1.3.6.1.2.1.7*	Tracks UDP statistics, datagrams in and out, etc.
egp	*1.3.6.1.2.1.8*	Tracks various statistics about EGP and keeps an EGP neighbor table.
transmission	*1.3.6.1.2.1.10*	There are currently no objects defined for this group, but other media-specific MIBs are defined using this subtree.
snmp	*1.3.6.1.2.1.11*	Measures the performance of the underlying SNMP implementation on the managed entity and tracks things such as the number of SNMP packets sent and received.

MODULE #1 – Protocole SNMP

Un agent SNMP contient des variables MIB dont les valeurs peuvent être demandées ou modifiées par le gestionnaire SNMP via les opérations Get ou Set. Un gestionnaire peut obtenir une valeur d'un agent ou stocker une valeur dans cet agent.

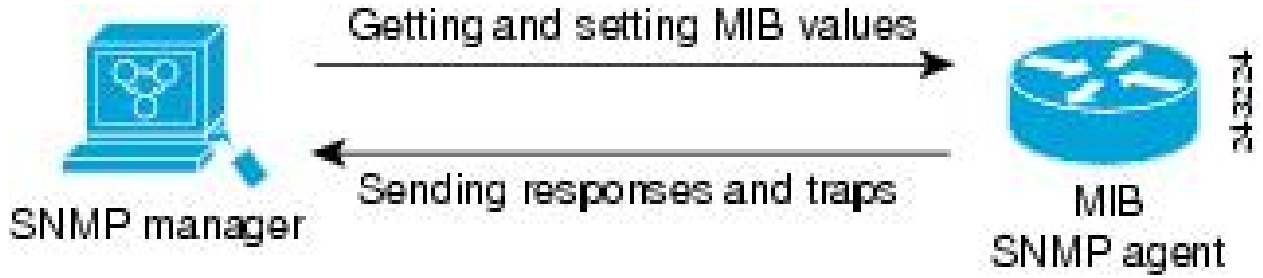


MODULE #1 – Protocole SNMP

Interactions Superviseur / Agents:

La figure ci-dessous illustre les communications entre le gestionnaire SNMP et l'agent. Un gestionnaire envoie des demandes d'agent pour obtenir et définir des valeurs MIB. L'agent répond à ces demandes.

Indépendamment de cette interaction, l'agent peut envoyer au gestionnaire des notifications non sollicitées (traps ou informations) pour informer le gestionnaire des conditions du réseau.



MODULE #1 – Protocole SNMP

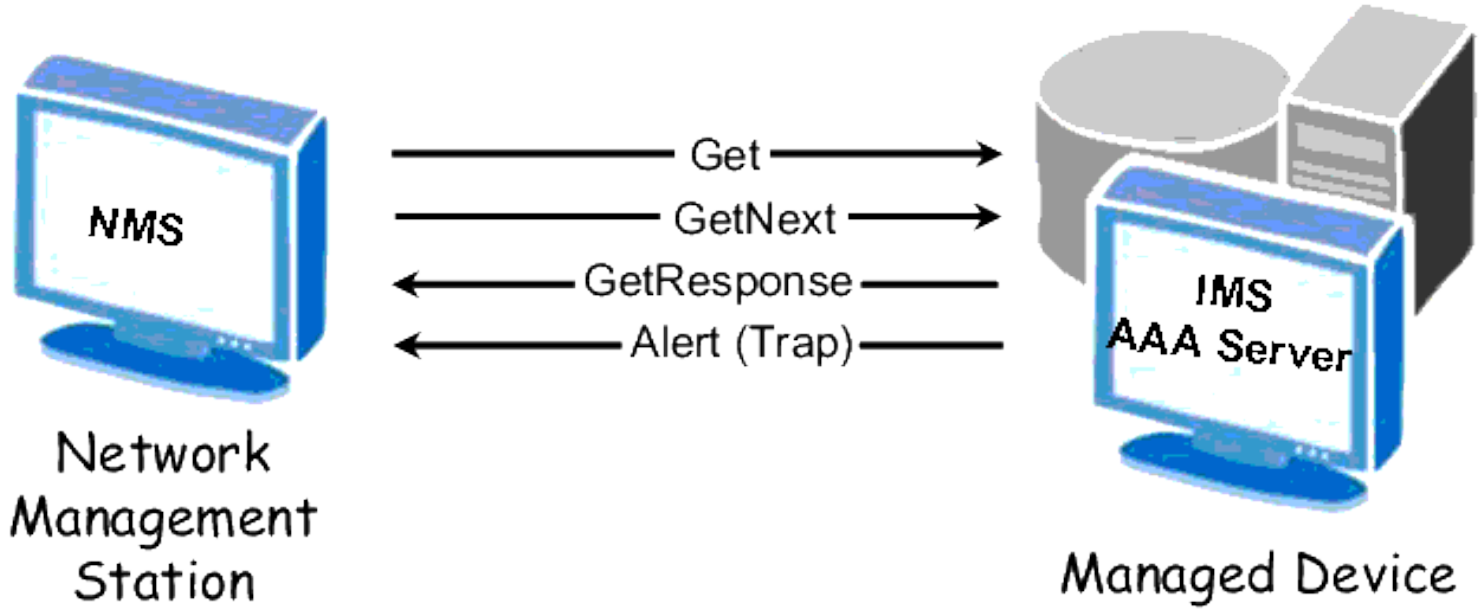
Opérations SNMP:

Les applications SNMP exécutent les opérations suivantes pour extraire des données, modifier des variables et envoyer des notifications.

- SNMP Get
- SNMP Set
- SNMP Notifications

MODULE #1 – Protocole SNMP

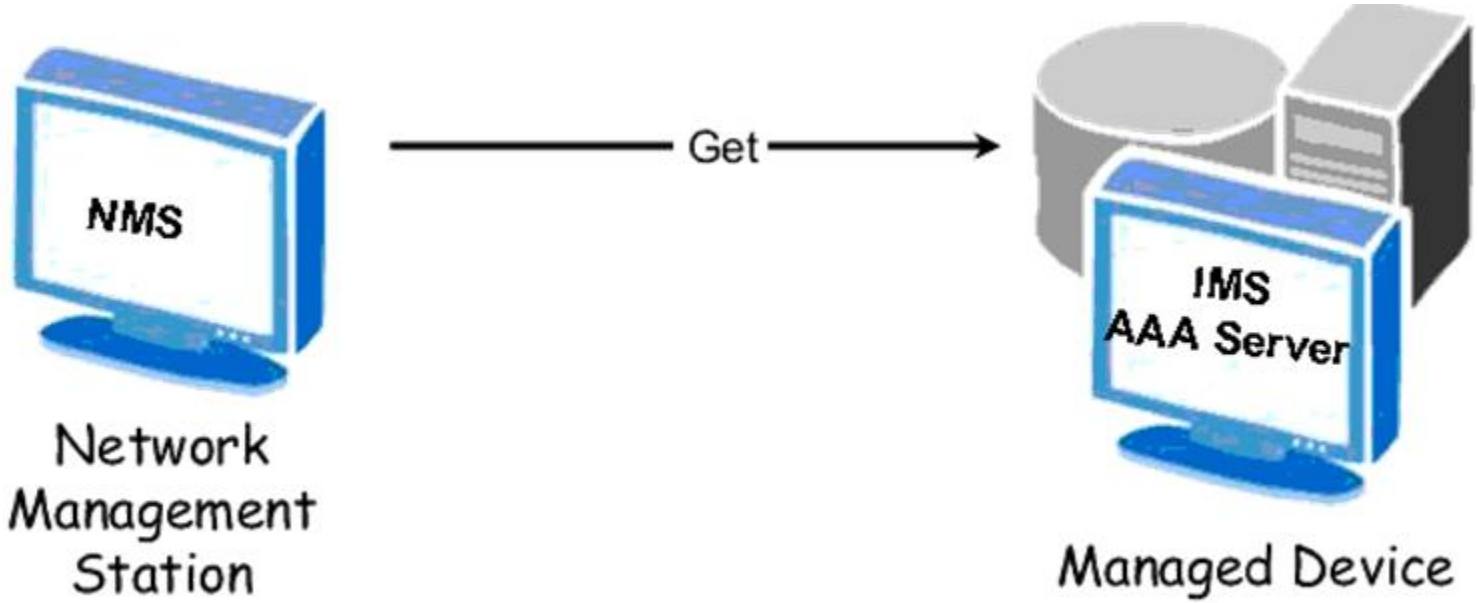
Opérations SNMP:



MODULE #1 – Protocole SNMP

SNMP Get :

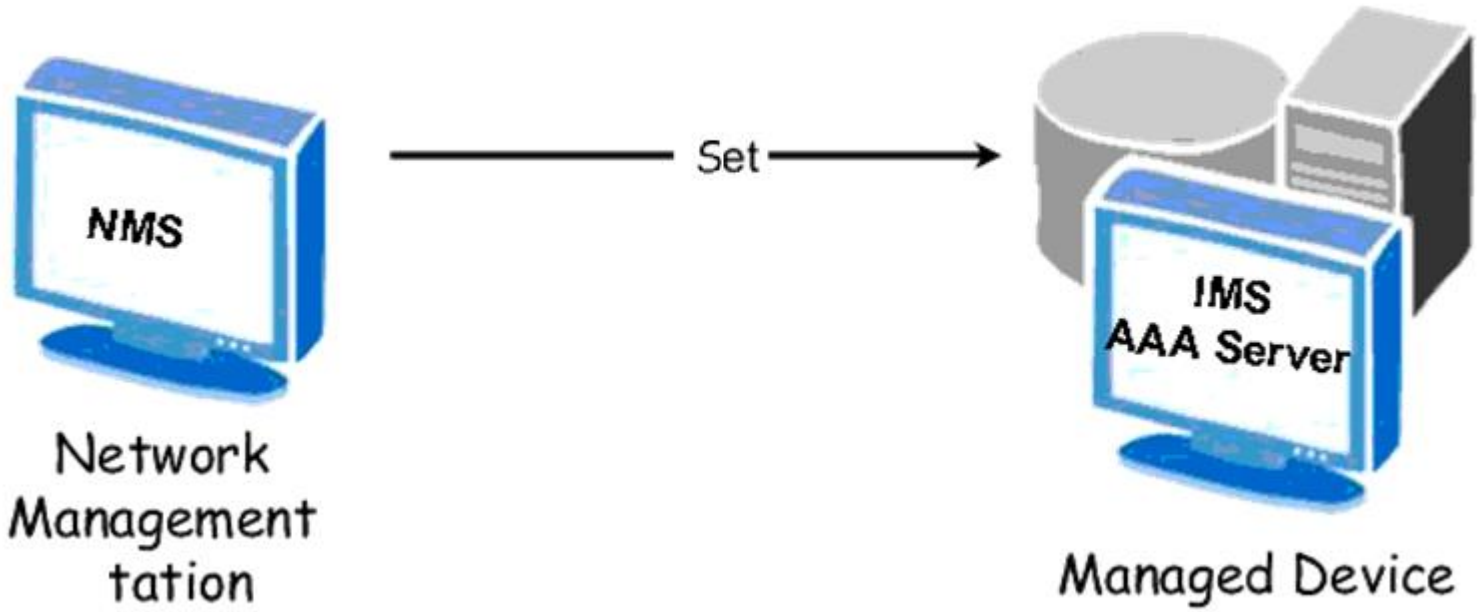
L'opération « Get » est effectué afin d'extraire des variables d'objets SNMP.



MODULE #1 – Protocole SNMP

SNMP Set :

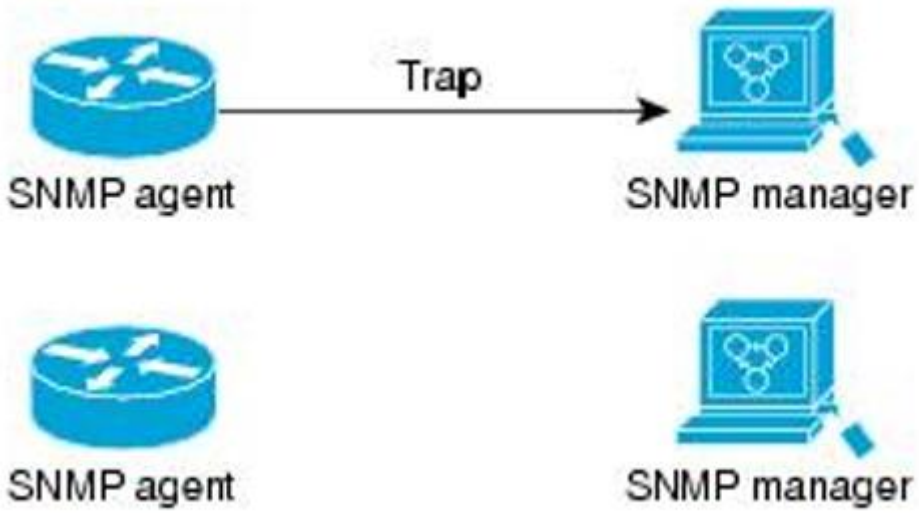
L'opération « Set » est utilisé pour modifier une variable d'objet SNMP.



MODULE #1 – Protocole SNMP

SNMP Notifications :

Une fonctionnalité clé de SNMP est sa capacité à générer des notifications non sollicitées à partir d'un agent SNMP.



MODULE #1 – Protocole SNMP

Versions SNMP:

Les logiciels Cisco IOS supportent 3 versions de SNMP, soit :

- **SNMPv1** - Simple Network Management Protocol: un standard Internet complet, défini dans RFC 1157. La sécurité est basée sur les chaînes de la communauté.

- **SNMPv2c -** est une mise à jour des opérations de protocole et des types de données de SNMPv2p (SNMPv2 Classic) et utilise la communauté modèle de sécurité basé sur SNMPv1

- **SNMPv3 -** fournit un accès sécurisé aux périphériques en authentifiant et en chiffrant les paquets sur le réseau.

MODULE #1 – Protocole SNMP

Communautés:

Pour que les agents communiquent avec le gestionnaire SNMP, il y a un élément très important à prendre en considération lors de la configuration. Cet élément est la communauté.

Pour que les gestionnaires captent les notifications (traps) venant des agents, il faut spécifier le nom d'une communauté.

Ces communautés seront utilisées à la fois par le gestionnaire et par les agents. Une fois la configuration effectuée, cela permet de recevoir les informations sur le logiciel de gestion SNMP.

MODULE #1 – Protocole SNMP

La chaîne de communauté (*community string*) n'est en réalité qu'un mot de passe en texte clair (sans cryptage). Toutes les données envoyées en texte clair sur un réseau sont vulnérables au reniflement et à l'interception de paquets. Il existe deux types de chaînes de communauté dans SNMP version 1 et 2 :

- Lecture seule (RO): donne un accès en lecture seule aux objets MIB, qui est plus sûr et préféré à une autre méthode.
- Lecture-écriture (RW): donne un accès en lecture et en écriture aux objets MIB. Cette méthode permet au gestionnaire SNMP de **modifier** la configuration du routeur / commutateur géré. Soyez donc prudent avec ce type.

La chaîne de communauté définie sur le gestionnaire SNMP doit correspondre à l'une des chaînes de communauté des agents pour que celui-ci puisse accéder aux agents.

MODULE #1 – Protocole SNMP

SNMPv3 apporte des améliorations significatives pour remédier aux faiblesses de sécurité présentes dans les versions antérieures. Le concept de chaîne de communauté n'existe pas dans cette version. SNMPv3 fournit une communication beaucoup plus sécurisée utilisant des entités, des utilisateurs et des groupes. Ceci est réalisé en mettant en œuvre trois nouvelles fonctionnalités principales:

- Intégrité du message: s'assurer qu'un paquet n'a pas été modifié en transit.
- Authentification: en utilisant un hachage de mot de passe (basé sur les algorithmes HMAC-MD5 ou HMAC-SHA) pour garantir que le message provient d'une source valide sur le réseau.
- Confidentialité (cryptage): en utilisant le cryptage (cryptage DES 56 bits, par exemple) pour crypter le contenu d'un paquet.

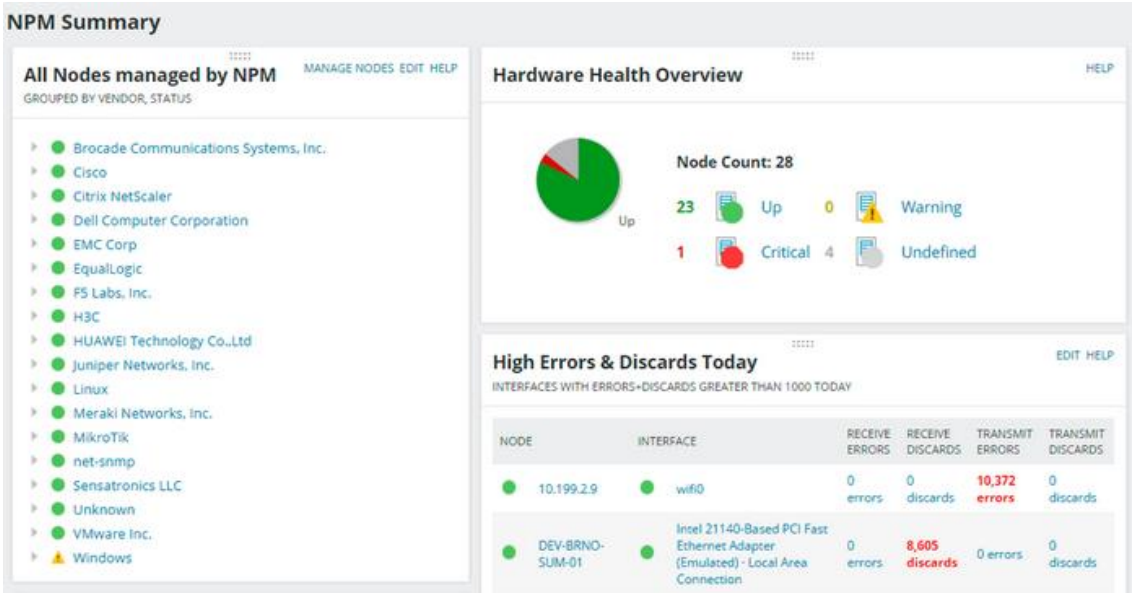
MODULE #1 – Protocole SNMP

Bien que SNMPv3 offre une meilleure sécurité, SNMPv2c reste toutefois plus courant. Cisco prend en charge SNMPv3 dans ses routeurs depuis la version 12.0.3T d'IOS.

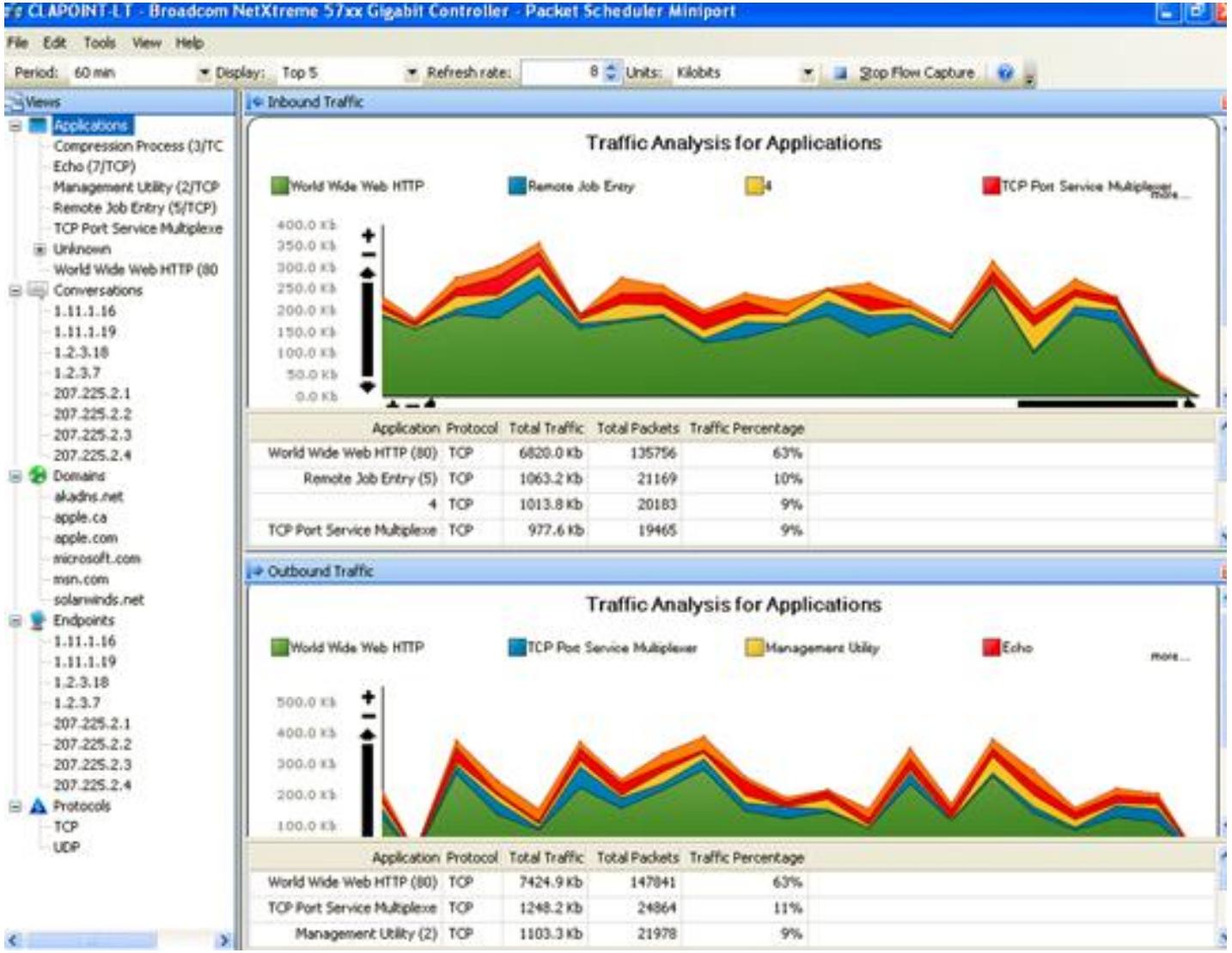
MODULE #1 – Protocole SNMP

Logiciel de gestion SNMP (superviseur) :

Pour visualiser les notifications SNMP sur le réseau, il faut qu'un logiciel de gestion SNMP s'occupe de capter les OID et de retourner de façon visuelle le tout à l'écran afin de faire de la surveillance sur le réseau en temps réel.



MODULE #1 – Protocole SNMP



MODULE #1 – Protocole SNMP

La surveillance a pour but de prévenir les problèmes et d'intervenir avant que ces problèmes affectent l'efficacité des système de télécommunications.

Lorsque l'on ne peut pas prévenir un problème et que ce problème survient sans avertissements, alors les outils de surveillance joue un autre rôle qui est tout aussi important et primordial. Ils serviront à diagnostiquer, à cibler, à localiser une ou des pannes sur les réseaux de télécommunications.

Cela améliore grandement la vitesse de résolution des pannes donc permet d'être plus efficace pour remettre les systèmes fonctionnels.

Plus un système de surveillance est complet et détaillé, plus on peut isoler le problème par simple visualisation du logiciel et par le fait même pointer précisément le problème à distance!

MODULE #1 – SOLARWINDS

Le logiciel de surveillance de réseau conçu par *Solarwinds*, appelé *Network Performance Monitor* ou encore *NPM*, est l'un des logiciels de surveillance les plus populaires présentement dans l'industrie.

Il sera aussi le logiciel utilisé dans le cadre de ce cours. Le serveur *NPM* vous permettra de collecter les différentes données des équipements que vous devrez surveiller. Une démonstration vous sera faite en classe afin de vous initier à son fonctionnement. Pour plus d'information, veuillez vous rendre à l'adresse suivante. Vous y trouverez toute la documentation utile afin d'implémenter votre solution de surveillance.

https://support.solarwinds.com/Success_Center/Network_Performance_Monitor_(NPM)/NPM_Documentation/Network_Performance_Monitor_Getting_Started_Guide