Pr. Youness KHOURDIFI, PhD en Informatique
Professeur à la Faculté Polydisciplinaire – Khouribga –
Université Sultan Moulay Slimane – Béni Mellal –
Consultant IT : SQL 2016 Database Administration,
Core Infrastructure 2016, Azure Solutions Architect
Expert, Data Analyst Associate, Ingénieur DevOps.
y.khourdifi@usms.ma

AUTOMATISATION DES RÉSEAUX

Année Universitaire : 2022/2023

Système de notation

- Contrôles continus → 60%
- Travaux pratiques → 20%
- Comptes rendus des TP et exposés → 20%

L'environnement de travail

- Préparation d'un ordinateur pour la virtualisation
  - VirtualBox
- Installation du système d'exploitation Linux sur un ordinateur virtuel
  - Ubuntu 14.04.3 (20.04) LTS
- GNS3

OBJECTIFS :

Les objectifs d'automatisation des réseaux sont :

- Simplifier et optimiser la gestion des réseaux informatiques en automatisant les tâches répétitives et complexes.
- Il permet de configurer, déployer et gérer efficacement les équipements réseau, ce qui améliore la qualité de service et la disponibilité du réseau.
- Il peut aussi réduire les erreurs humaines, accélérer les déploiements et améliorer la sécurité du réseau.

Contenu

Elément Automatisation des réseaux Programme :

- 1. Introduction à l'administration des réseaux informatiques
- 2. La supervision des réseaux informatiques
  - 2.4. Modèles de l'administration des réseaux selon les modèles de Référence OSI & TCP/IP.
  - 2.5. Le protocole de gestion réseaux SNMP.
  - 2.6. Les logiciels de supervision réseaux informatiques (OpenSource et propriétaires)
  - 2.7. Les plates-formes d'administration des réseaux informatiques.
- 3. Introduction aux technologies d'automatisation des réseaux :
  - 3.4. Hight Level (Systèmes de gestion de la configuration)
  - 3.5. Low Level (Interfaces d'appareils « API »)

Programme des TP :

- TP 1 : Utilisation du logiciel Nagios Core pour la supervision d'un réseau
- TP 2 : Utilisation du logiciel CACTI pour la supervision d'un réseau
- TP 3 : Utilisation du logiciel PRTG Network Monitor pour la supervision et le recueille des statistiques sur un réseau

Contenu

Elément Technologie Devnet :

- 1. Introduction au Devnet
- 2. Compréhension et Utilisation des APIs REST
- 3. Plateformes Cisco DevNet
- 4. Déploiement et sécurité des applications
- 5. Infrastructure et automatisation

Programme des TP :

- TP 1 : Utilisation des SandBox
- TP 2 : Orchestration des services réseaux

Chapitre

Introduction à l’administration des réseaux informatiques

I. 1. Introduction à l'administration des réseaux informatiques :

Présentation de l'administration réseau :

- Lorsqu'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.
- Cette complexité croissante conduit à la perte des ressources du réseau et à des mauvaises performances, qui 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 (Nagios, PRTG Network Monitor, CACTI, …)

I. 1. Introduction à l'administration des réseaux informatiques :

Présentation de l'administration réseau :

- L'administration de réseaux informatiques est le processus de gestion et de maintien du bon fonctionnement d'un réseau informatique.
- Cela peut inclure des tâches telles que la configuration du matériel et des logiciels du réseau, la surveillance des performances du réseau, le dépannage des problèmes et la garantie de la sécurité du réseau.

I. 1. Introduction à l'administration des réseaux informatiques :

Présentation de l'administration réseau :

- Un réseau informatique est un ensemble de dispositifs interconnectés, tels que des ordinateurs, des serveurs et des routeurs, qui communiquent entre eux pour partager des ressources et des informations.
  - Il existe différents types de réseaux, notamment les réseaux locaux (LAN), les réseaux étendus (WAN) et l'Internet.

L'impact des réseaux dans la vie quotidienne :

- Les réseaux facilitent l'apprentissage
- Les réseaux facilitent la communication
- Les réseaux facilitent notre travail
- Les réseaux facilitent le divertissement

I. 1. Introduction à l'administration des réseaux informatiques :

Présentation de l'administration réseau :

- En tant qu'administrateur réseau, vous serez responsable de la mise en place et de la maintenance de l'infrastructure réseau, qui comprend les composants matériels et logiciels qui composent le réseau.
- Cela comprend la configuration des routeurs, des commutateurs et d'autres équipements de réseau afin de garantir la fluidité de la circulation des données entre les dispositifs.
- La surveillance du réseau sera également assurée pour identifier et résoudre les problèmes qui peuvent survenir.
- Cela peut inclure la surveillance du trafic réseau, la recherche d'erreurs et l'identification des goulets d'étranglement qui peuvent être à l'origine de la lenteur des performances.

I. 1. Introduction à l'administration des réseaux informatiques :

- L'administrateur réseau est également chargé d'assurer la sécurité du réseau.
- Cela comprend la mise en place de pare-feu, de systèmes de détection d'intrusion et d'autres mesures de sécurité pour protéger le réseau contre les accès et les attaques non autorisés.
- Dans l'ensemble, l'administration de réseau est un domaine critique de l'informatique qui joue un rôle essentiel dans le bon fonctionnement de l'entreprise en maintenant l'intégrité et la sécurité des réseaux informatiques de l'organisation.

I. 1. Introduction à l'administration des réseaux informatiques :

Objectifs et rôle de l'administration :

Les principaux objectifs d'un administrateur réseau sont d'assurer le bon fonctionnement et les performances du réseau informatique d'une organisation, ainsi que de maintenir la sécurité et l'intégrité du réseau et des données qu'il contient.

Le rôle d'un administrateur de réseau comprend :

- Installer, configurer et entretenir le matériel et les logiciels du réseau;
- Surveiller les performances du réseau et résoudre les problèmes lorsqu'ils surviennent;
- Assurer la sécurité du réseau en mettant en œuvre des mesures de sécurité telles que des pare-feu et des systèmes de détection des intrusions;
- Gérer et entretenir les serveurs du réseau, tels que les serveurs de courrier électronique et les serveurs Web;

I. 1. Introduction à l'administration des réseaux informatiques :

- Gérer et maintenir les utilisateurs et les autorisations du réseau;
- Gérer et maintenir les sauvegardes du réseau et les plans de reprise en cas de panne ou d'incident;
- Maintenir le réseau à jour avec les derniers logiciels et correctifs de sécurité;
- Gérer et maintenir les données et les informations de l'organisation.

En résumé, l'administrateur réseau est chargé de garantir la disponibilité, la fiabilité et la sécurité du réseau informatique de l'organisation, qui est essentiel à son succès.

I. 1. Introduction à l'administration des réseaux informatiques :

Les modèles d'administration réseaux :

Il existe plusieurs modèles différents utilisés pour l'administration des réseaux, notamment :

- **Centralisé :** Toutes les tâches de gestion du réseau sont effectuées par un administrateur ou un groupe central.
- **Décentralisé :** Les tâches de gestion du réseau sont réparties entre plusieurs administrateurs ou groupes.
- **Hiérarchique :** les tâches de gestion du réseau sont organisées selon une structure hiérarchique, les administrateurs de niveau supérieur étant responsables des parties les plus importantes du réseau.
- **Hybride :** Une combinaison de deux ou plusieurs des modèles précédents.

I. 1. Introduction à l'administration des réseaux informatiques :

Les modèles d'administration réseaux :

- **Distribué :** L'ensemble des tâches de gestion du réseau est effectué par les périphériques réseau eux-mêmes, avec peu ou pas d'intervention humaine.

Chaque modèle a ses propres avantages et inconvénients, et le meilleur modèle pour une organisation donnée dépendra de facteurs tels que la taille et la complexité du réseau, le niveau de sécurité requis et les ressources disponibles.

I. 1. Introduction à l'administration des réseaux informatiques :

Réseau clients serveurs :

Dans un réseau client-serveur, il existe deux principaux types de périphériques : les clients et les serveurs.

- Un client est un appareil qui demande des services ou des ressources à un serveur.
- Les clients peuvent être des ordinateurs, des smartphones, des tablettes ou d'autres appareils qui se connectent à un réseau.
- Un serveur est un dispositif qui fournit des services ou des ressources aux clients. Les serveurs peuvent être des systèmes informatiques ou des logiciels spécialisés qui gèrent des tâches spécifiques, comme le stockage de fichiers, la messagerie électronique, l'hébergement Web ou la gestion de bases de données.
- Dans un réseau client-serveur, les clients envoient des requêtes au serveur, et le serveur répond en fournissant les services ou les ressources demandés. La communication entre le client et le serveur peut se faire à l'aide de divers protocoles tels que TCP/IP, HTTP, FTP et bien d'autres encore.

I. 1. Introduction à l'administration des réseaux informatiques :

- Les réseaux client-serveur peuvent être utilisés dans divers environnements tels que les réseaux de petits bureaux, les réseaux de grandes entreprises et même sur Internet.
- Ils offrent un moyen centralisé de gérer et de distribuer des ressources et des services aux clients, ce qui permet une meilleure organisation et une meilleure évolutivité.
- L'un des principaux avantages d'un réseau client-serveur est qu'il permet une gestion et une maintenance aisées du réseau, car toutes les ressources et tous les services sont centralisés sur les serveurs, et les clients n'y accèdent qu'en cas de besoin.

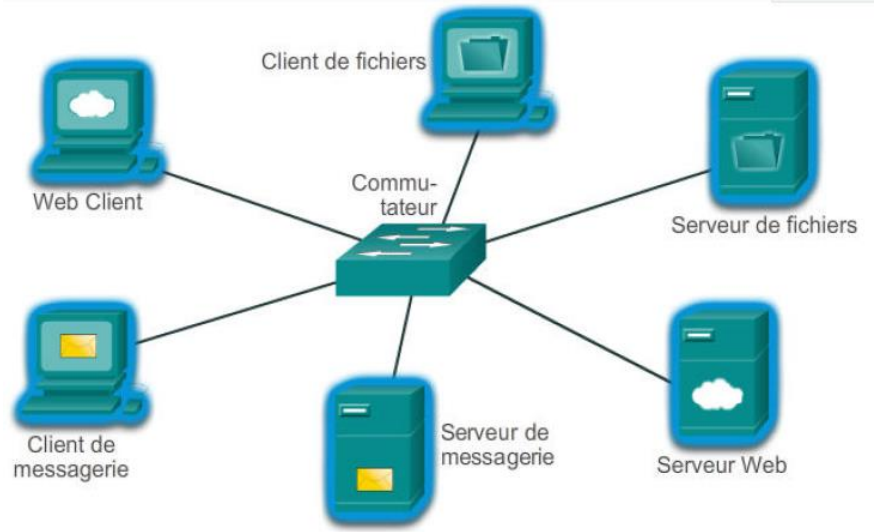
I. 1. Introduction à l'administration des réseaux informatiques :

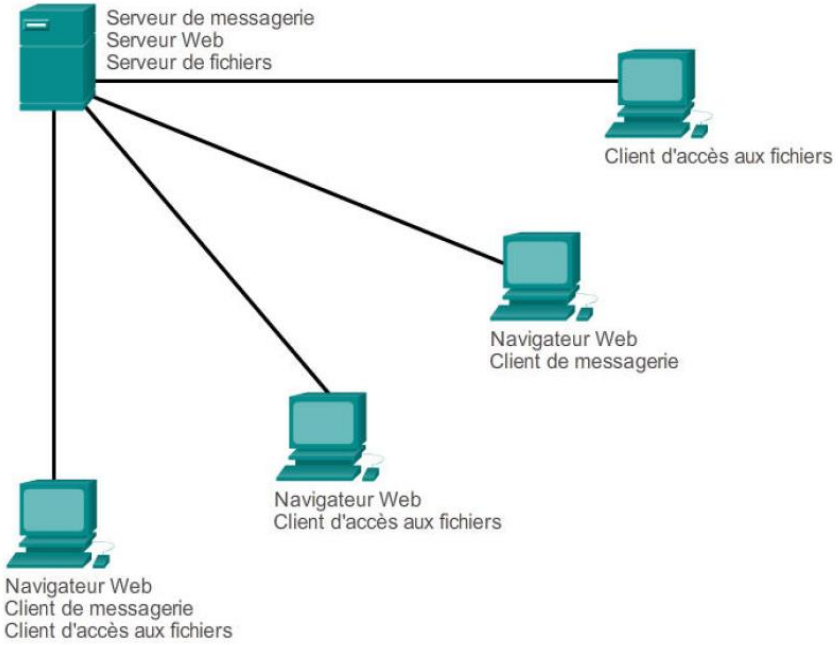
Plusieurs éléments clés constituent un réseau client-serveur :

- **Les clients :** Ce sont les ordinateurs ou les appareils utilisés par les utilisateurs pour accéder aux données sur le réseau et les traiter. Il peut s'agir d'ordinateurs de bureau, d'ordinateurs portables, de tablettes et de smartphones.
- **Serveurs :** Ce sont les ordinateurs ou les appareils qui stockent et gèrent les données et les services sur le réseau. Ils peuvent inclure des serveurs de fichiers, des serveurs de messagerie, des serveurs Web et des serveurs de bases de données.
- **Système d'exploitation du réseau :** Il s'agit du logiciel qui fonctionne sur les serveurs et les clients et qui contrôle la communication et le transfert de données entre eux.

I. 1. Introduction à l'administration des réseaux informatiques :

- **Matériel de réseau :** Il s'agit des routeurs, commutateurs, concentrateurs et autres dispositifs physiques qui relient les clients et les serveurs et leur permettent de communiquer entre eux.
- **Les protocoles :** Ce sont les règles et les normes qui régissent la communication entre les clients et les serveurs sur le réseau.
  - Les exemples incluent TCP/IP, FTP, HTTP et SMTP.





I. 1. Introduction à l'administration des réseaux informatiques :

Les protocoles d'administration réseau :

- Chaque fournisseur de réseau propose des outils permettant de mettre en place la gestion du réseau . De ce fait, si l'on dispose de plusieurs systèmes hétérogènes, il est très difficile de faire coopérer les différents outils de gestion de réseau de chaque système.
- Cependant L'échange d'informations entre systèmes hétérogènes a été rendu possible par l'intermédiaire de la normalisation de l'ISO.
- C'est ainsi que des protocoles d'administration ont vu le jour.
- Les protocoles d'administration permettent à la plate forme de gestion d'aller chercher les informations sur les éléments de réseaux et aussi de changer les paramètres sur ces derniers. De plus, ils permettent à la plate forme de gestion de recevoir des alertes provenant des éléments de réseaux

I. 1. Introduction à l'administration des réseaux informatiques :

C'est quoi un protocole réseau ?

Un protocole réseau est un ensemble de règles et de normes qui régissent la communication et le transfert de données entre les périphériques d'un réseau. Ces protocoles définissent le format des données transmises, ainsi que les méthodes utilisées pour transmettre, recevoir et traiter les données.

I. 1. Introduction à l'administration des réseaux informatiques :

Les protocoles d'administration réseau :

Il existe plusieurs protocoles qui sont couramment utilisés dans l'administration des réseaux pour gérer et maintenir les réseaux informatiques. Il s'agit notamment de :

- **CMIP (Common Management Information Protocol)** est un protocole de gestion de réseau utilisé pour gérer et surveiller les équipements réseau tels que les commutateurs, les routeurs et les serveurs. Il est basé sur le protocole de gestion de réseau OSI (Open Systems Interconnection) et utilise une architecture client-serveur pour permettre aux administrateurs de collecter des informations sur l'état des dispositifs et de configurer à distance les équipements..
- **SNMP (Simple Network Management Protocol) :** Ce protocole est utilisé pour surveiller et gérer les périphériques réseau tels que les routeurs, les commutateurs et les serveurs. Il permet aux administrateurs réseau de recueillir des données sur les performances du réseau, ainsi que de configurer et de contrôler les périphériques réseau à distance. SNMP il est basé sur le protocole CMIP.

I. 1. Introduction à l'administration des réseaux informatiques :

- **Telnet :** Ce protocole permet aux administrateurs réseau d'accéder et de contrôler à distance des périphériques réseau tels que des routeurs et des commutateurs à l'aide d'une interface en ligne de commande.
- **SSH (Secure Shell) :** Ce protocole est similaire à Telnet, mais il fournit une connexion sécurisée et cryptée entre les administrateurs réseau et les périphériques réseau.
- **FTP (File Transfer Protocol) :** Ce protocole est utilisé pour transférer des fichiers entre les ordinateurs d'un réseau. Il permet aux administrateurs réseau de télécharger des fichiers vers et depuis des serveurs et d'autres périphériques réseau.
- **SMTP (Simple Mail Transfer Protocol) :** Ce protocole est utilisé pour transférer le courrier électronique entre les serveurs. Il permet aux administrateurs réseau de gérer et de maintenir les systèmes de courrier électronique sur le réseau.

I. 1. Introduction à l'administration des réseaux informatiques :

- **DHCP (Dynamic Host Configuration Protocol) :** Ce protocole est utilisé pour attribuer automatiquement des adresses IP aux périphériques d'un réseau. Il permet aux administrateurs réseau de gérer et de maintenir facilement les attributions d'adresses IP sur le réseau.
- **DNS (Domain Name System) :** Ce protocole est utilisé pour traduire les noms de domaine en adresses IP. Il permet aux administrateurs réseau de gérer et de maintenir la résolution des noms de domaine sur le réseau.

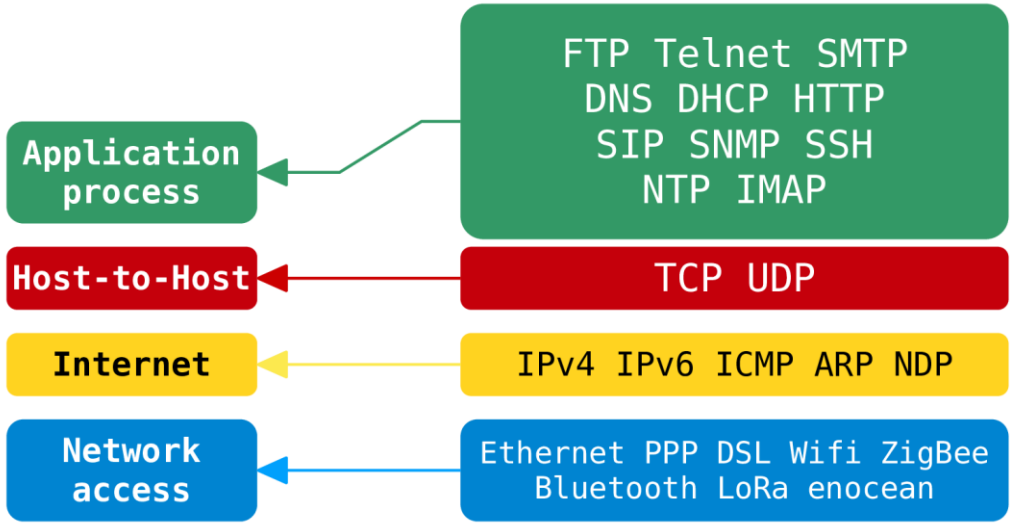
I. 1. Introduction à l'administration des réseaux informatiques :

Modèles inter-réseaux OSI et TCP/IP :

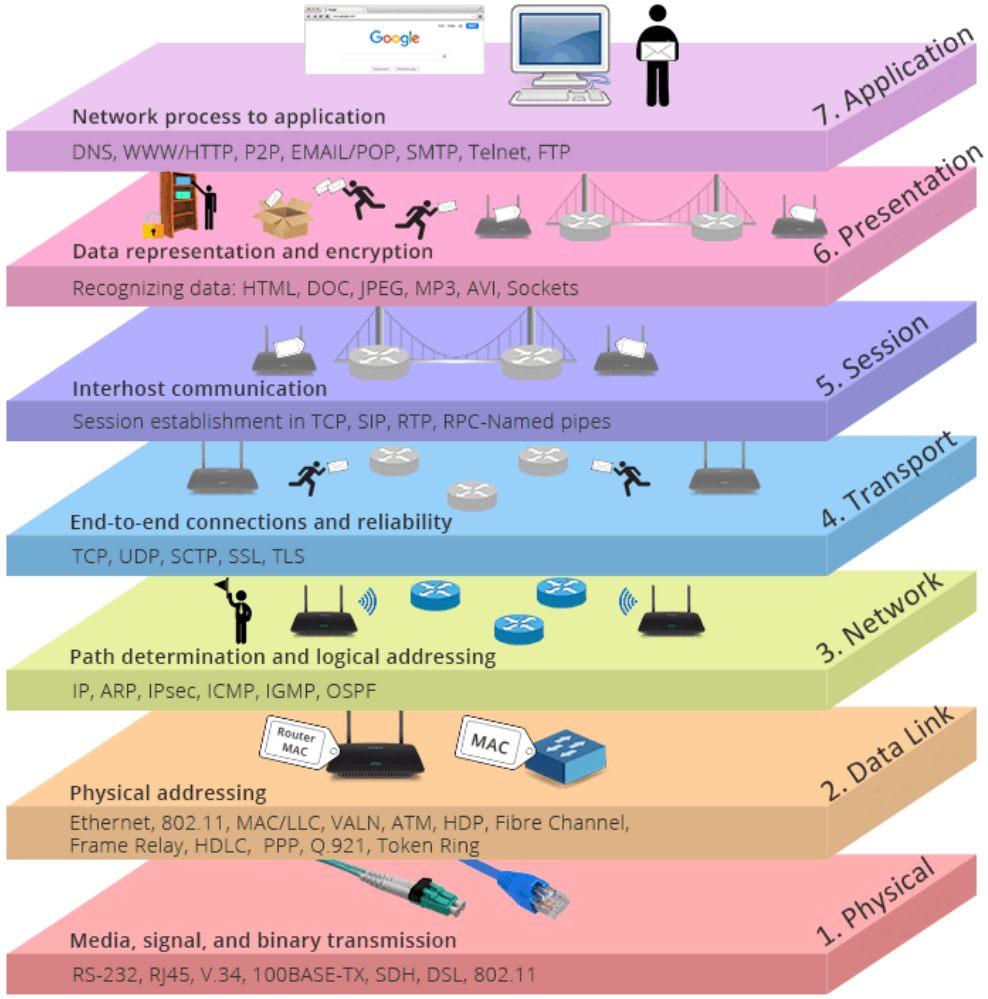
- Le modèle OSI (Open Systems Interconnection) est un modèle de référence pour les réseaux informatiques qui définit 7 couches logicielles, chacune ayant des fonctions et des responsabilités spécifiques. Les couches sont : la couche physique, la couche de liaison de données, la couche réseau, la couche transport, la couche session, la couche présentation et la couche application.
- Le modèle TCP/IP (Transmission Control Protocol / Internet Protocol) est un autre modèle de référence pour les réseaux informatiques, utilisé principalement pour les réseaux d'Internet. Il définit 4 couches logicielles : l'accès au réseau, l'Internet, la transport et l'application.
- Les deux modèles ont des fonctions similaires, mais ils ont des différences significatives dans la manière dont ils les implémentent.
- Le modèle OSI est plus général et abstrait, tandis que le modèle TCP/IP est plus spécifique aux réseaux d'Internet. Il est important de noter que les deux modèles ne sont pas nécessairement mutuellement exclusifs, ils peuvent être utilisés ensemble pour une meilleure compréhension des réseaux.

I. 1. Introduction à l'administration des réseaux informatiques :

Modèles inter-réseaux :



Le Modèle TCP/IP



Le Modèle OSI

I. 1. Introduction à l'administration des réseaux informatiques :

Les services de la couche d'application :

La couche application est la couche la plus élevée du modèle de référence OSI.

Elle est chargée de fournir des services qui prennent directement en charge des programmes d'application spécifiques et des processus d'utilisateur final. Certains des principaux services fournis par la couche application sont les suivants :

- **Le transfert de fichiers :** des services tels que FTP (File Transfer Protocol) et SFTP (Secure File Transfer Protocol) permettent aux utilisateurs de transférer des fichiers entre ordinateurs sur un réseau.
- **Le courrier électronique :** des services tels que SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol) et IMAP (Internet Message Access Protocol) permettent aux utilisateurs d'envoyer et de recevoir des messages électroniques.
- **Connexion à distance** : des services tels que Telnet et SSH (Secure Shell) permettent aux utilisateurs de se connecter à distance à d'autres ordinateurs sur un réseau et de les contrôler.

I. 1. Introduction à l'administration des réseaux informatiques :

- **Services Web :** Des services tels que HTTP (Hypertext Transfer Protocol) et HTTPS (HTTP Secure) permettent aux utilisateurs d'accéder à des pages et des applications Web et d'interagir avec elles.
- **Partage de fichiers :** Des services tels que NFS (Network File System) et CIFS (Common Internet File System) permettent aux utilisateurs de partager et d'accéder à des fichiers sur d'autres ordinateurs du réseau.
- **Impression :** Des services tels que LPD (Line Printer Daemon) et SMB (Server Message Block) permettent aux utilisateurs d'imprimer sur des imprimantes connectées au réseau.
- **Accès aux bases de données :** Des services tels que ODBC (Open Database Connectivity) et JDBC (Java Database Connectivity) permettent aux utilisateurs d'accéder à des bases de données sur un réseau et d'interagir avec elles.

I. 1. Introduction à l'administration des réseaux informatiques :

- **Services d'annuaire :** Les services tels que LDAP (Lightweight Directory Access Protocol) et Kerberos permettent aux utilisateurs d'accéder aux données des utilisateurs et de les authentifier dans un annuaire centralisé.

Ces services permettent aux utilisateurs de partager et d'accéder aux données, de communiquer entre eux et d'utiliser diverses ressources du réseau depuis différents endroits.

Ce ne sont là que quelques exemples des nombreux services fournis au niveau de la couche application. D'autres services tels que le DNS (Domain Name System) et le SNMP (Simple Network Management Protocol) sont également fournis à cette couche en fonction des besoins et des exigences de l'organisation.

I. 1. Introduction à l'administration des réseaux informatiques :

Composants de base du réseau :

Les composants de base d'un réseau comprennent:

- **Les hôtes:** Les ordinateurs et les périphériques qui utilisent le réseau pour communiquer entre eux, et qui sont situé à l'extrémité d'un communication : par exemple un poste client et un serveur sont des hôtes terminaux.
- **Les commutateurs et les routeurs:** Les commutateurs connectent les hôtes entre eux au niveau de la couche 2 (liaison de données) du modèle OSI, tandis que les routeurs connectent les réseaux entre eux au niveau de la couche 3 (réseau) du modèle OSI, et il permet aussi de transférer le trafic et transférer le trafic IP grâce à sa table de routage vers les bonnes destinations.

Périphérique terminal

Routeur

Commutateur Couche 2

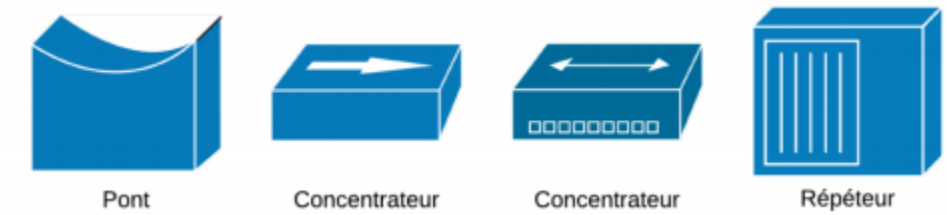
I. 1. Introduction à l'administration des réseaux informatiques :

- **Les câbles et les connecteurs:** Les câbles et les connecteurs physiques relient les hôtes, les commutateurs et les routeurs.
- **Les protocoles de communication:** Les protocoles de communication définissent les règles et les conventions utilisées pour la transmission des données sur le réseau.
- **Les périphériques de sécurité:** Les pares-feux, les systèmes de détection d'intrusion et les autres périphériques de sécurité protègent le réseau contre les attaques et les intrusions.
- **Pont, concentrateur et Répéteur :** Les "Ponts", "Concentrateurs" et "Répéteurs" sont des éléments aujourd'hui plus conceptuels que réels (sauf dans certains déploiement en Wi-Fi). Un pont (bridge) filtre le trafic entre deux segments physiques en fonction des adresses MAC. Le point d'accès Wi-Fi est une sorte de pont.

I. 1. Introduction à l'administration des réseaux informatiques :

Un concentrateur (hub) est un périphérique qui concentre les connexions et étend le segment physique. À la différence du commutateur, le trafic sort par tous ses ports ; il ne prend aucune décision quant au trafic. En Ethernet, il était souvent identifié comme un répéteur multi-ports, ils ont été progressivement remplacés par des commutateurs de telle que ce matériel de "concentration" n'est plus fabriqué depuis longtemps.

Un répéteur (repeater) étend le signal entre deux ou plusieurs segments. Il ne prend aucune décision quant au trafic à transférer. On peut encore trouver des répéteurs dans les architectures Wi-Fi.



I. 1. Introduction à l'administration des réseaux informatiques :

❑ Matériel sans-fil :

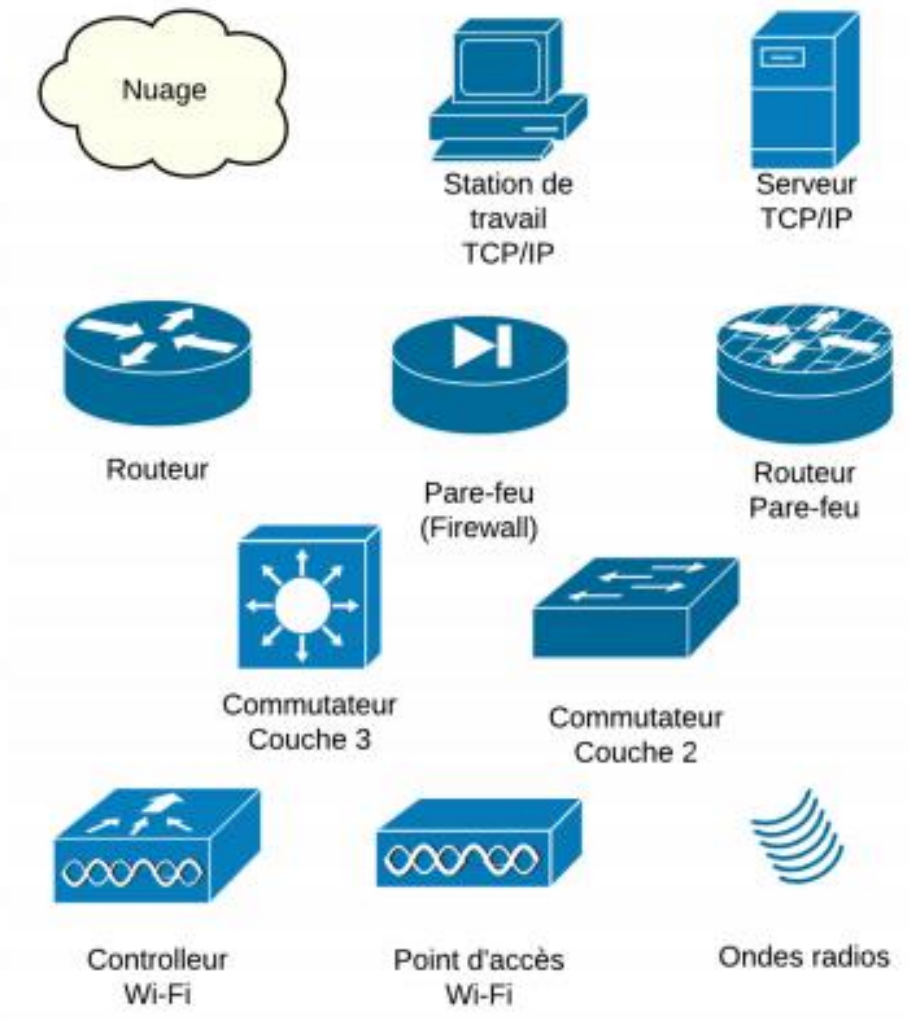
Avec des points d'accès légers (Lightweight AP), le Wireless LAN Controller (WLC) prend en charge les fonctions d'association ou d'authentification des APs, ces derniers devenant des interfaces physiques fournissant la connectivité. Le contrôleur fournit l'intelligence, la gestion, la configuration des APs. Il participe à une vue unifiée du réseau filaire et sans-fil.

I. 1. Introduction à l'administration des réseaux informatiques :

Composants de base du réseau :

- Chacun de ces périphériques est associé à une couche du modèle OSI avec "L" pour "Layer" :

Périphérique	Couche
Routeur (Router)	L3
Commutateur (Switch) L3	L2/L3
Commutateur (Switch) L2	L2
Pont (Bridge)	L2
Concentrateur (Hub)	L1
Répéteur (Repeater)	L1
Contrôlleur WLAN	L2/L3/L7
Point d'accès sans-fil (AP) Wi-Fi	L1/L2
Carte réseau (NIC)	L2
Hôte terminal	L3/L4/L7



Composants de base du réseau

I. 1. Introduction à l'administration des réseaux informatiques :

Notions des ports de service :

- Les ports de service sont des numéros utilisés pour identifier les différents services réseau sur un ordinateur.
- Ils permettent aux paquets de données de être acheminés vers le service approprié sur un ordinateur.
- Les ports de service sont généralement divisés en deux catégories : les ports connus et les ports privés.
- Les ports connus sont utilisés pour les services courants tels que HTTP (port 80), HTTPS (port 443), FTP (port 21), etc.
- Les ports privés, quant à eux, sont utilisés pour les services personnalisés ou non couramment utilisés.

I. 1. Introduction à l'administration des réseaux informatiques :

- Il existe une plage de ports numériques allant de 0 à 65535. Les ports allant de 0 à 1023 sont réservés pour les services système et sont généralement utilisés par les administrateurs système.
- Les ports allant de 1024 à 65535 sont utilisés pour les services utilisateurs et peuvent être utilisés pour les services personnalisés.
- Il est important de noter que certains ports, tels que le port 22 pour SSH, sont souvent utilisés pour accéder à un système à distance et peut être la cible d'une attaque. Il est donc important de configurer les pare-feu et les autres mesures de sécurité pour protéger ces ports de service critiques.

Chapitre 2

La supervision des réseaux informatiques

II. La supervision des réseaux informatiques :

2.1.La supervision informatique, qu'est-ce que c'est ?

- La supervision informatique est un processus qui consiste à surveiller et à gérer les systèmes informatiques et les réseaux pour assurer leur bon fonctionnement, détecter et résoudre les problèmes; et la disponibilité et la performance.
- Elle implique l'utilisation d'outils de surveillance pour détecter les problèmes et les résoudre rapidement pour maintenir la qualité des services informatiques.
- La supervision informatique peut également inclure la surveillance des performances, de la disponibilité, des événements, la gestion des sauvegardes, la sécurité des données et la planification de la maintenance préventive.

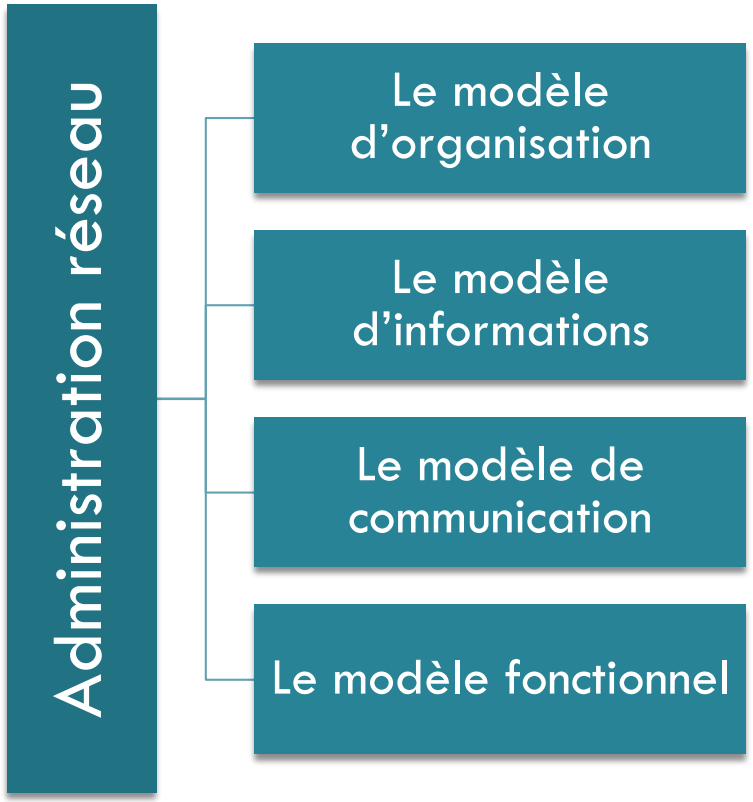
II. La supervision des réseaux informatiques :

2.2.Le modèle d'administration des réseaux selon le modèle de Référence OSI :

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.

II. La supervision des réseaux informatiques :

2.2.1.Le modèle d'organisation :

Le modèle d'organisation décrit les composants de l'administration réseau, par exemple administrateur, agent, et ainsi de suite, avec leurs relations.

- Le modèle organisationnel, aussi appelé modèle architectural (Managed System and Agents (MSA) ou Système Administré et Agent) : c'est un modèle qui organise l'administration OSI, définit la notion de systèmes administrés (Agents) et définit la notion du système Administrant (DMAP : Distributed Management Application Processus).

II. La supervision des réseaux informatiques :

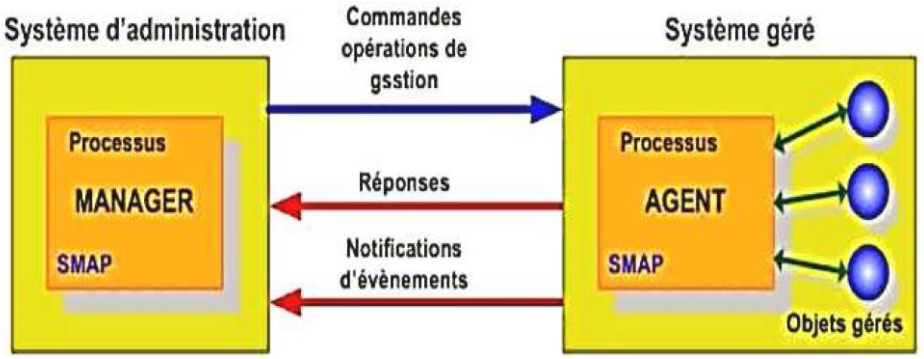
2.2.1.Le modèle d'organisation :

- Le modèle organisationnel définit trois types d’activité :
  - **La gestion du système (System Management) ;**
  - **La gestion de couche (Layer Management) ;**
  - **Les opérations de couche (Layer Operations).**

II. La supervision des réseaux informatiques :

2.2.1.1.La gestion du système (System Management) :

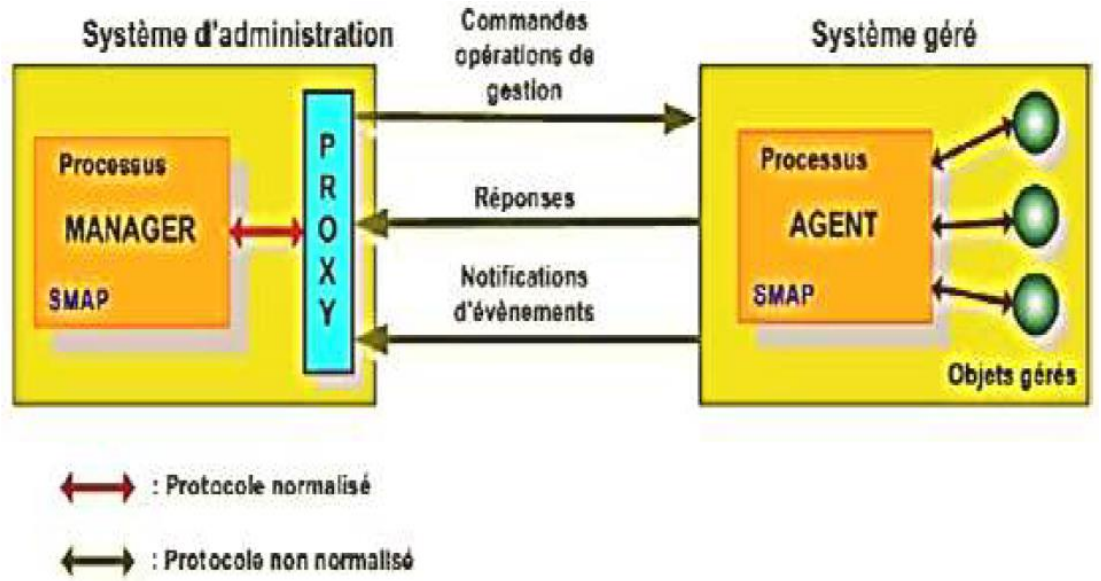
- La gestion du système (SMAE : System Management Application Entity) met en relation deux processus Manager et Agent.
- Le protocole standardisé de niveau application CMIP «Common Management Information Protocol» est utilisé.
- Le Manager envoie des messages de commandes à ses Agents; ceux-ci lui retournent les résultats des opérations effectuées dans des messages de réponses.



Modèle de Gestion Manager –Agent

II. La supervision des réseaux informatiques :

- Dans le modèle précèdent, l'Agent n'utilise pas les mêmes normes ou la même syntaxe de communication que le Manager, une entité tierce appelée « Proxy-Agent » permet d'adapter le protocole de l'Agent et de convertir ses données au format du Manager. Le proxy-Agent est situé soit au niveau de l'Agent, soit au niveau du Manager.



Modèle de Gestion Manager –Agent avec l'agent Proxy

II. La supervision des réseaux informatiques :

2.2.1.2.La gestion de couche (Layer Management) :

- La gestion de couche (ou protocole de couche),fournit les moyens de transfert des informations de gestion entre les sites administrés. C'est un dialogue horizontal (CMIP, Common Management Information Protocol, ISO 9596).
- Les opérations de couche (N), ou protocole de couche (N) supervisent une connexion de niveau N.

II. La supervision des réseaux informatiques :

- Ces opérations utilisent les protocoles OSI classiques pour le transfert d'information.
- C'est par exemple : Le CMIP utilise les primitives de service suivantes (CMISE : Common Management Information Service Element) :
  - Get : il est utilisé par le gérant pour lire la valeur d'un attribut ;
  - Set : fixe la valeur d'un attribut ;
  - Event : permet à un agent de signaler un événement ;
  - Create : génère un nouvel objet ;
  - Delete : permet à l'agent de supprimer un objet.

II. La supervision des réseaux informatiques :

2.2.1.3.Les opérations de couche (Layer Operations) :

- Elles concernent les mécanismes mis en oeuvre pour administrer l'unique instance d'une communication entre 2 entités homologues. Les opérations de couche N (protocole de Couche N) supervisent une connexion de niveau N en utilisant un certain nombre de primitive de service. Il s'agit d'un dialogue Vertical assuré par le CMIS (Common Management Information Service).

II. La supervision des réseaux informatiques :

2.2.2.Le modèle d'informations :

- **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.
- Un modèle informationnel aussi appelé «Management Information Base (MIB)» ou « Base de l'Information d'Administration» est un modèle qui constitue la base de données des informations d'administration en énumérant les objets administrés et les informations s'y rapportant (attributs). L'ensemble des objets gérés constitue la MIB (ISO 10165). La MIB contient toutes les informations administratives sur les objets gérés (ponts, routeurs, cartes,…). La norme ne spécifie aucune organisation particulière des données ; Seul, le processus agent a accès à la MIB et le processus manager accède aux données via le processus agent.

II. La supervision des réseaux informatiques :

2.2.3.Le modèle de communication :

- **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.

II. La supervision des réseaux informatiques :

2.2.4.Le modèle fonctionnel :

- **Le modèle fonctionnel** concerne les applications d'administration réseau qui résident sur la station d'administration réseau (NMS).
- Ce compte cinq domaines fonctionnels, parfois appelés le modèle FCAPS (Faults, Configuration, Accounting, Performance, Security):

II. La supervision des réseaux informatiques :

2.2.4.1.La gestion des anomalies ou de panne (Fault Management) :

Elle a pour objectif de faire le diagnostic rapide de toute défaillance interne ou externe du système (par exemple la panne d'un routeur). Ces pannes peuvent être d'origine interne résultant d'un élément en panne ou d'origine externe dépendant de l'environnement du système (coupure d'un lien publique).

Cette gestion implique :

- La surveillance des alarmes (filtre, report, …) ; il s'agit de surveiller le système et de détecter les défauts. On établit un taux d'erreurs et un seuil à ne pas dépasser.
- Le traitement des anomalies ;
- La localisation et le diagnostic des incidents (séquences de tests) la journalistique des problèmes, etc.

II. La supervision des réseaux informatiques :

2.2.4.2.La gestion de la configuration (Configuration Management) :

Elle a pour objectif d'identifier de manière unique chaque objet administré par un nom ou un identificateur d'objet (OID : Object Identifier).

Il s'agit également de :

- Gérer la configuration matérielle et logicielle et ;
- Préciser la localisation géographique.

II. La supervision des réseaux informatiques :

2.2.4.3.La gestion des performances (Performance Management) :

Elle a pour objectif de contrôler, à évaluer la performance et l'efficacité des ressources comme le temps de réponse, le débit, le taux d'erreur par bit, la disponibilité (aptitude à écouler du trafic et à répondre aux besoins de communication pour lequel la ressource a été mise en service).

Elle comprend :

- La collecte d'informations, statistiques (mesure du trafic, temps de réponse, taux d'erreurs, etc.), le stockage et l'interprétation des mesures (archivage des informations statistiques dans la MIB, calculs de charge du système, tenue et
- examen des journaux chronologiques de l'état du système).
- Elle est réalisée à l'aide d'outil de modélisation et simulation permettant d'évaluer l'impact d'une modification de l'un des paramètres du système.

II. La supervision des réseaux informatiques :

2.2.4.4.La gestion de la sécurité (Security Management) :

Elle couvre tous les domaines de la sécurité afin d'assurer l'intégrité des informations traitées et des objets administrés.

L'ISO a défini cinq services de sécurité :

- Les contrôles d'accès au réseau ;
- La confidentialité (les données ne sont communiquées qu'aux personnes, ou processus autorisés) ;
- L'intégrité (les données n'ont pas été accidentellement ou volontairement modifiées ou détruites) ;
- L'authentification (l'entité participant à la communication est bien celle déclarée) ;
- La non-répudiation (impossibilité pour une entité de nier d'avoir participé à une transaction).

Pour cela l'ISO utilise les mécanismes d'encryptage, l'authentification des extrémités (source et destinataire) et le contrôle des accès aux données. Notons également que c'est au niveau de la gestion de sécurité que l'on trouve la notion de configuration du serveur AAA3 (Authentification – Authorization – Accounting).

II. La supervision des réseaux informatiques :

2.2.4.5.La gestion de la comptabilité (Accounting Management) :

Elle permet de connaitre les charges des objets gérés, les coûts de la consommation… cette évaluation est établie en fonction du volume et la durée des transmissions.

La gestion de la comptabilité comporte les taches suivantes :

- la consommation réseau par abonné ;
- la définition des centres de coût ;
- la mesure des dépenses de structure (coûts fixes) et répartitions ;
- la mesure des consommations par services ;
- l'imputation des coûts.

II. La supervision des réseaux informatiques :

2.3.Le modèle d'administration des réseaux selon le modèle de Référence TCP/IP:

Le Standard de fait dans l'administration des réseaux TCP/IP, le protocole SNMP (Simple Network Management Protocol) est proche des concepts ISO. Cependant, non orienté objet SNMP confond la notion d'attribut et d'objet. Issu du protocole de gestion des passerelles IP (SGMP, Simple Gateway Monitoring Protocol – RFC 1028), SNMP est décrit dans la RFC 1157.

Une grande majorité des logiciels de supervision sont basés sur le protocole SNMP qui existe depuis de nombreuses années. La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information ;
- Visualiser l'architecture du système ;
- Analyser les problèmes ;
- Déclencher des alertes en cas de problèmes ;
- Effectuer des actions en fonction des alertes ;
- Réduire les attaques entrantes.

II. La supervision des réseaux informatiques :

A quoi servent les RFC ?

- Un RFC (Request for Comments) est un document purement technique publié par l'IETF (Internet Engineering Task Force).
- Les RFC sont principalement utilisées pour développer un protocole de réseau « standard », une fonction d'un protocole de réseau ou toute autre caractéristique liée à la communication réseau.
- Les RFC ont été utilisés pour la première fois lors de la création des protocoles ARPANET, qui sont venus établir ce qui est devenu Internet aujourd'hui.
- Elles continuent à être publiés de manière continue au fur et à mesure de l'évolution de la technologie sous-jacente à Internet.

II. La supervision des réseaux informatiques :

De nombreuses technologies de réseaux informatiques populaires ont été documentées dans les RFC, notamment:

- Les RFC 1155 qui spécifient comment les objets gérés sont représentés dans les bases d'informations (SMI, Structure of Management Information). SMI utilise la notation ASN1 (Abstract Syntax Notation 1) ;
- Les RFC 1156 et 1213 qui définissent les MIB (MIB I et MIB II). Les MIB décrivent les objets gérés (attributs ISO). Une MIB particulière (RMON MIB, Remote Monitor Network MIB) est spécifié pour les réseaux locaux (Ethernet et Token Ring), les objets RMON sont implémentés dans des sondes d'analyse et de surveillance. Cependant en environnement commuté, les sondes RMON n'ont accès qu'aux segments sur lesquels elles sont installées.

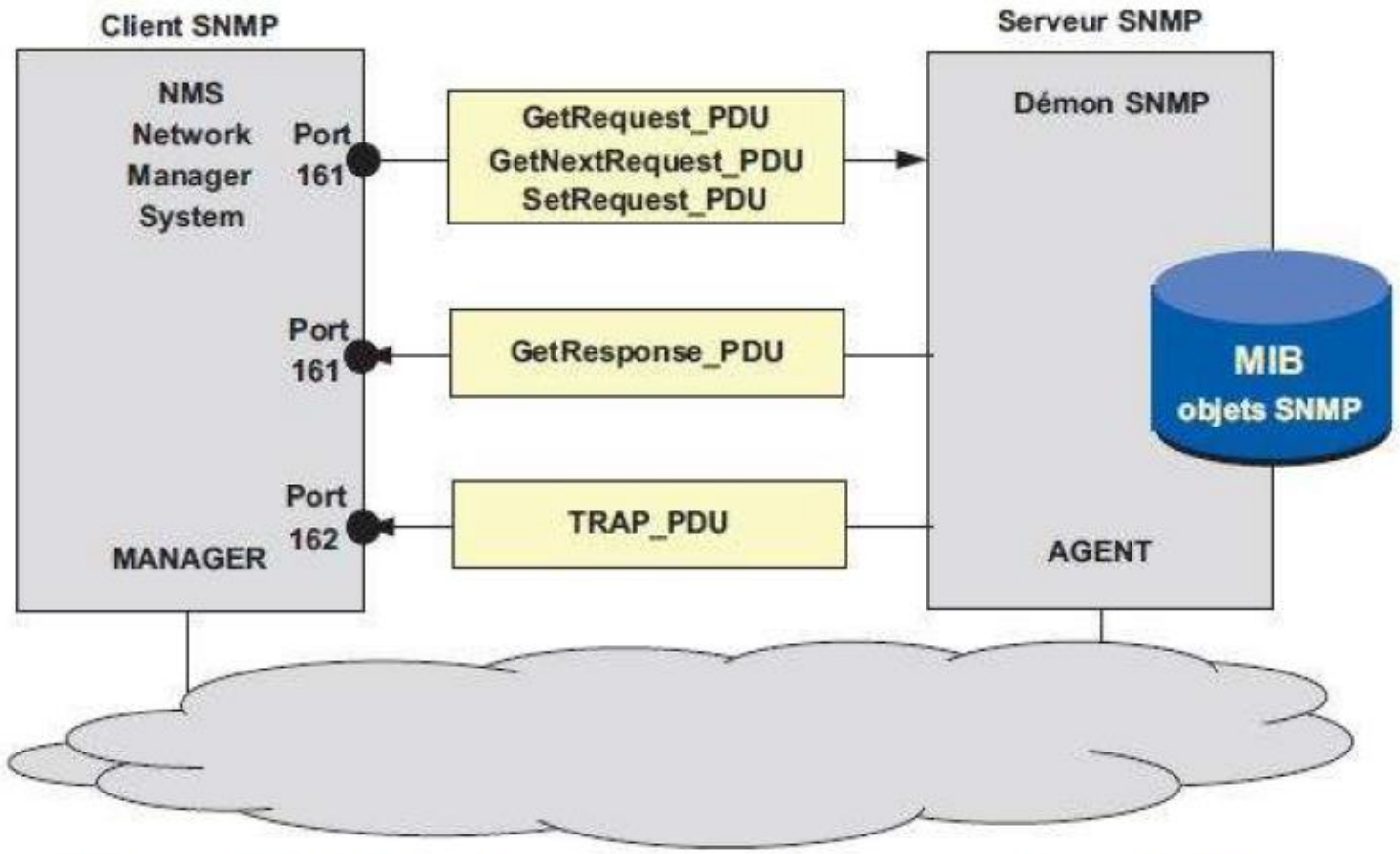
II. La supervision des réseaux informatiques :

Pour assurer un accès aux différents éléments des réseaux commutés, une sonde spécifique a été définie (RFC 2613, SMON, Switched RMON). Le SNMP spécifie les échanges entre la station d'administration et l'agent. S'appuyant sur UDP (User Datagram Protocol), SNMP est en mode non connecté. De ce fait, les alarmes (trap) ne sont pas confirmées. La plus grande résistance aux défaillances d'un réseau d'un protocole en mode datagrammes vis-à-vis d'un protocole en mode connecté ainsi que la rapidité des échanges justifient le choix d'UDP. Les messages SNMP permettent de lire la valeur (exemple : compteur de collisions) d'un objet administré (attribut d'ISO) (GetRequest et GetNextRequest), de modifier la valeur d'un objet (SetRequest).

L'agent administré répond à ces sollicitations par le message GetResponse. Le message Trap est émis sur l'initiative de l'agent qui notifie ainsi, à l'administrateur, qu'une condition d'alarme a été détectée..

II. La supervision des réseaux informatiques :

2.3.Le modèle d'administration des réseaux selon le modèle de Référence TCP/IP:



Principe d'administration des réseaux informatiques selon TCP/IP

II. La supervision des réseaux informatiques :

2.3.1. Les MIB (Management Information Base) :

- Les MIB décrivent les objets gérés, en définissent le nommage, ils en précisent le type, le format et les actions.
- Les différentes valeurs des objets ne sont pas contenues dans la MIB, mais dans des registres externes que l'agent vient consulter à la demande du manager. La RFC 1213 (MIB II) formalise une structure de définition des objets.
- Ainsi, l'objet « SysUpTime » qui mesure le temps, en centième de seconde, depuis que l'agent a été réinitialisé, est de type TimeTicks (type de variable défini dans la Structure of Management Information, TimeTicks mesure le temps en centièmes de seconde) et est accessible uniquement en lecture (read_only). Cet objet obligatoire (mandatory) est le troisième objet décrit dans la MIB system.

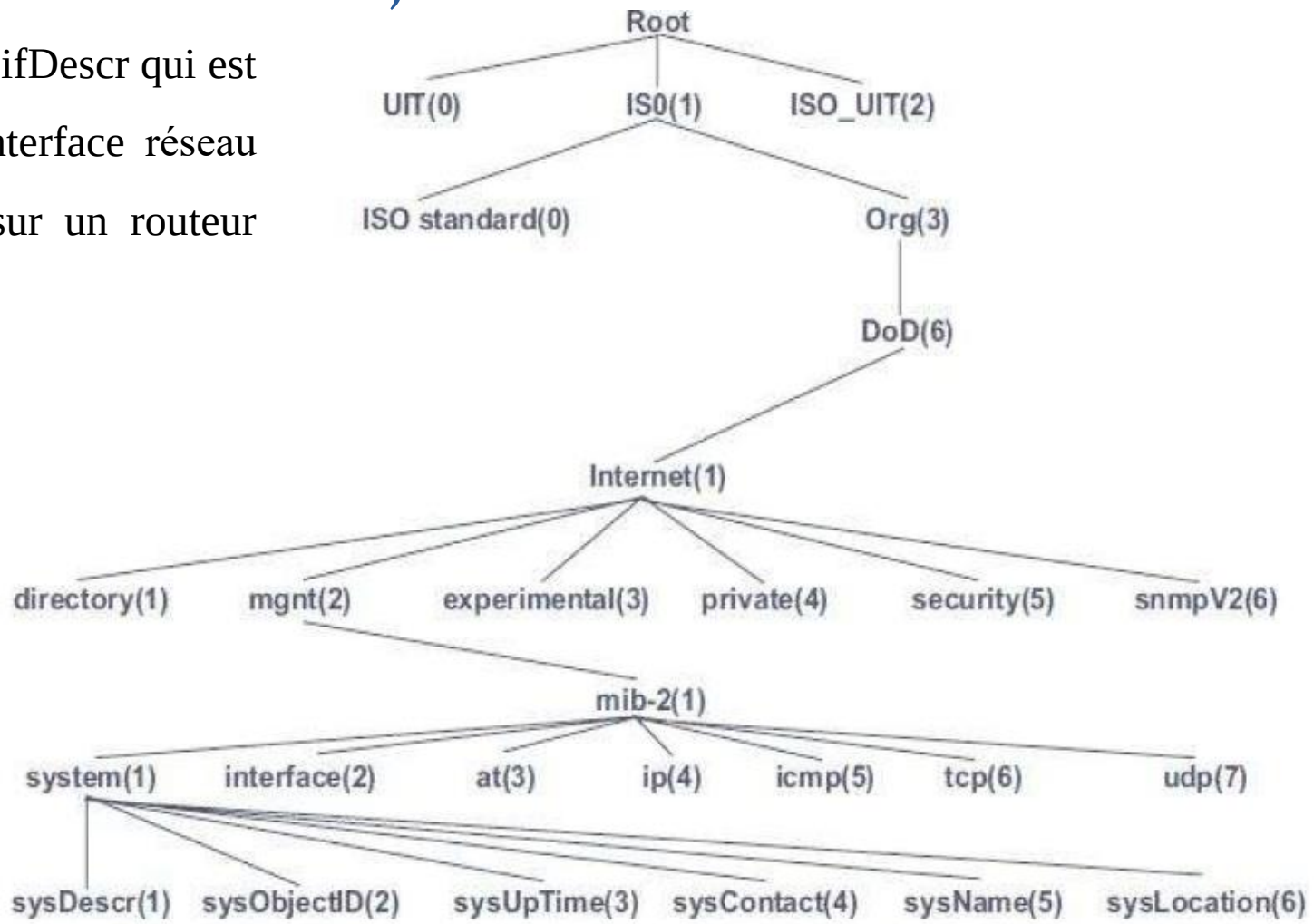
II. La supervision des réseaux informatiques :

- Les objets (variables) gérés par les MIB sont désignés selon une hiérarchie définie par l'ISO selon un arbre dit « arbre de nommage ».
- Chaque organisation de normalisation possède une entrée au premier niveau. Les différentes branches permettent de nommer un objet de manière unique. Les MIB standard établies par l'IETF appartiennent à la branche « internet » et sont classées dans la sous-branche mgmt(2).
- Chaque information a un OID (Object identifier), une suite de chiffres séparés par des points, qui l'identifie de façon unique et un nom, indiqué dans le document qui décrit la MIB.

II. La supervision des réseaux informatiques :

2.3.1. Les MIB (Management Information Base) :

Par exemple, **1.3.6.1.2.1.2.2.1.2** est l'OID ifDescr qui est la chaîne de caractères décrivant une interface réseau (comme eth0 sur Linux ou Ethernet0 sur un routeur Cisco).



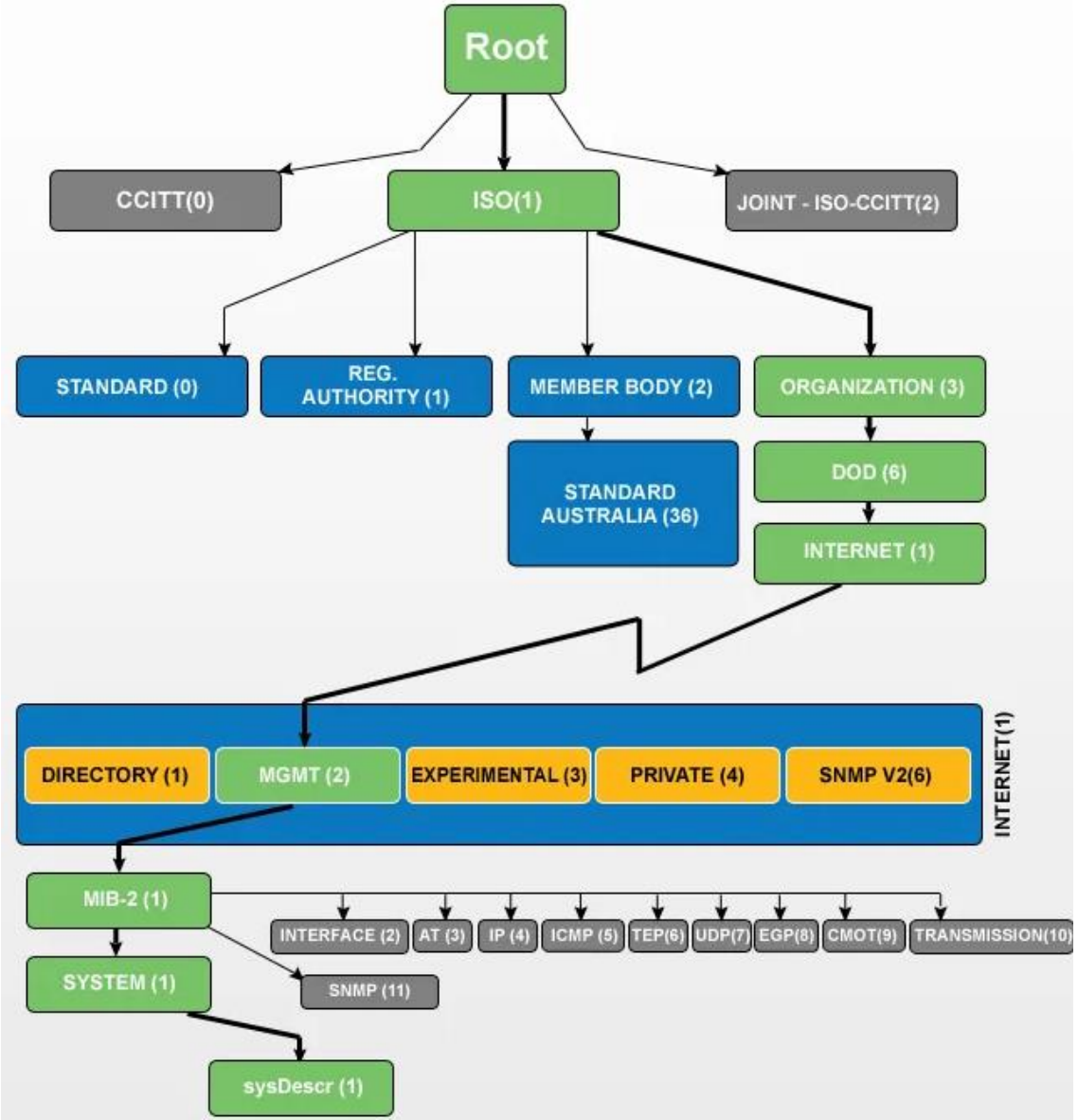
Arbre de nommage des objets dans l'administration TCP/IP

2.3.1. Les MIB :

- Par exemple :

l'OID dans RFC1213 pour "**sysDescr**" est

.1.3.6.1.2.1.1.1



II. La supervision des réseaux informatiques :

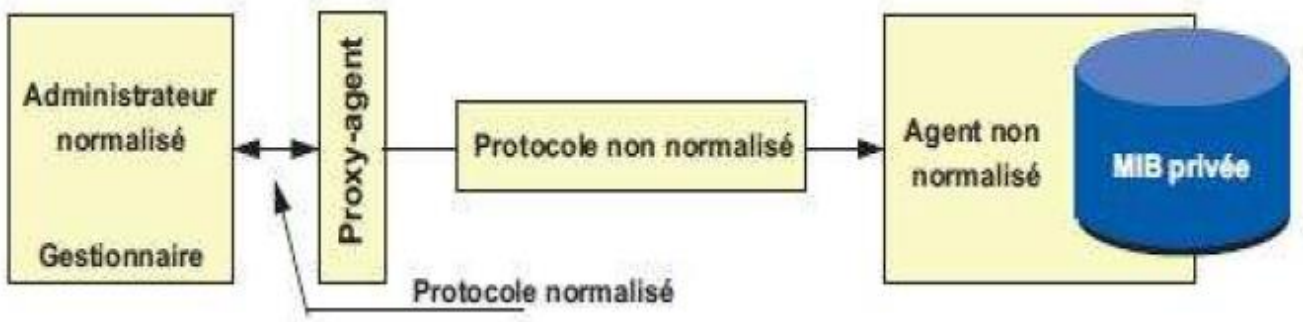
- Lorsqu'une entreprise veut définir son propre ensemble de variables de gestion, elle va enregistrer son numéro d'objet sous le noeud iso.org.dod.internet.private.entreprise.
- Ces MIB seront dites privées.
- Elles correspondent à la racine 1.3.6.1.4.1.

```
2
  IBM
    Bob Moore
      remoore@us.ibm.com
3
  Carnegie Mellon
    Mark Poepping
      host-master@andrew.cmu.edu
4
  Unix
    Keith Sklower
      sklower@okeeffe.berkeley.edu
5
  ACC
    Art Berggreen
      art@SALT.ACC.COM
6
  TWG
    John Lunny
      jlunny@eco.twg.com
7
  CAYMAN
    Beth Miaoulis
      beth@cayman.com
8
  PSI
    Marty Schoffstahl
      schoff@NISC.NYSER.NET
9
  ciscoSystems
    Dave Jones
      davej@cisco.com
10
  NSC
    John Lyman
      lyman@network.com
11
  Hewlett-Packard
    Harry Lynch
      harry.lynch@hp.com
12
  Epilogue
    Karl Auerbach
      karl@cavebear.com
```

II. La supervision des réseaux informatiques :

2.3.1. Les MIB (Management Information Base) :

- Il faut également rappeler que l'accès aux variables des MIB dites privées est assuré par un agent spécifique qui effectue les conversions nécessaires : le proxy-agent.
- Le proxy-agent permet ainsi le dialogue entre deux systèmes d'administration différents.
- Le principe du proxy-agent est illustré ci-dessous. Celui-ci peut être localisé dans le serveur pour l'utilisation d'une MIB privée, ou dans le manager si l'agent serveur n'est pas conforme au standard (conversion de protocole).



Principe d'un proxy-agent (mandataire).

II. La supervision des réseaux informatiques :

2.4. Le protocole de gestion réseaux SNMP:

- Le protocole SNMP est né pour répondre aux difficultés de surveillance et de maintien des réseaux informatiques.
- Le protocole SNMP (Simple Network Management Protocol) est utilisé pour gérer les réseaux informatiques.
- Il permet à des dispositifs de surveillance de réseau, tels que des ordinateurs, des routeurs et des commutateurs, de collecter des informations sur l'état des équipements de réseau et de les surveiller pour détecter les erreurs et les problèmes de performance.
- SNMP est un protocole standard et largement utilisé, ce qui facilite la gestion et la surveillance des réseaux complexes.

II. La supervision des réseaux informatiques :

- La première version du protocole d'administration SNMP, intitulée SNMP v1, a été finalisée en 1990.
- Ce protocole permet :
  - **de modifier la configuration des équipements ;**
  - **de détecter et d'analyser les problèmes du réseau par interrogation ou remontée d'alarmes ;**
  - **de surveiller ses performances et ;**
  - **de réaliser des statistiques.**
- Dans cette première version, le protocole est défini par un standard IETF (Internet Engineering Task Force) intitulé RFC 1157 (Request For Comments) « A Simple Network Management Protocol (SNMP) » datant de mai 1990. Le but de cette architecture est de faciliter son utilisation, d'être suffisamment extensible pour être compatible dans le futur et qu'elle soit indépendante de l'architecture et des mécanismes des hôtes ou serveurs particuliers. (IETF, 1990).

II. La supervision des réseaux informatiques :

- La sécurité de SNMPv1 est basée sur des noms de communautés qui sont utilisés comme des mots de passe pour accéder à une arborescence de données de l'équipement appelée MIB (Management Information Base). Le nom de la communauté est transmis en clair dans le message SNMP.
- La première version n'étant pas sécurisée, le protocole SNMP a ainsi évolué en une deuxième version finalisée en janvier 1996, intitulée SNMPv2C (RFC 1901 à 1908). La sécurité de cette version est encore faible car elle s'appuie sur le modèle de SNMPv1 en réutilisant les noms de communauté, d'où la lettre C de SNMPv2C. Cependant, elle comble des lacunes de la version 1, en particulier au niveau de la définition des objets, du traitement des notifications et du protocole lui même.
- Une troisième version finale, intitulé SNMPv3, a et approuvée comme projet de norme en avril 1999. Elle est devenue un standard en décembre 2002 (RFC 3410 à 3418). Elle a pour but principal d'assurer la sécurité des échanges.

II. La supervision des réseaux informatiques :

2.4.1. Historique du protocole SNMP :

- Principes de sécurité identiques à SNMPv1.
- Optimise la communication.
- Permet la communication entre les gestionnaire.
- Possible d'envoyer plusieurs requêtes à la fois (Get-Bulk).

SNMPv2u
et SNMPv2* avec RFC – 1901

Le protocole SNMP a été développé dans les années **1980** par la communauté de recherche sur les réseaux informatiques (Internet Research Task Force, IRTF). La première version de SNMP, appelée SNMPv1, a été publiée en **1988** et était destinée à la gestion de petits réseaux.

RFC 1155
SNMP v1

- Une sécurisation très faible.
- Pas de communication entre les gestionnaires.

SNMPv2p

RFC – 1441
SNMP v2 C

En **1991**, SNMPv2 a été publié, apportant des améliorations telles que la gestion des erreurs, la sécurité renforcée et des fonctionnalités de notification d'événements.

En **1998**, SNMPv3 a été publié, apportant des améliorations supplémentaires telles que l'authentification et la confidentialité des données.

RFC – 3411
SNMP v3

- Comme SNMPv2.
- Authentification forte entre manager et agent.
- Cryptage et chiffrement des données.

II. La supervision des réseaux informatiques :

2.4.2. Fonctionnement de SNMP :

- SNMP est un protocole situé entre la couche 4 et la couche 7 du modèle OSI. Il s'appuie sur le protocole de télécommunication UDP (User Datagram Protocol).
- Le paquet UDP est encapsulé dans un paquet IP (Internet Protocol). UDP est plus simple à utiliser que TCP (Transmission Control Protocol) car il fonctionne en mode non connecté. Le mode non connecté n'oblige pas les deux entités à établir une connexion entre elles avant de transférer des données puis de mettre fin à leur connexion. En revanche, UDP ne permet pas de savoir si les datagrammes sont bien arrivés et s'ils sont arrivés dans un ordre différent de celui d'émission.

II. La supervision des réseaux informatiques :

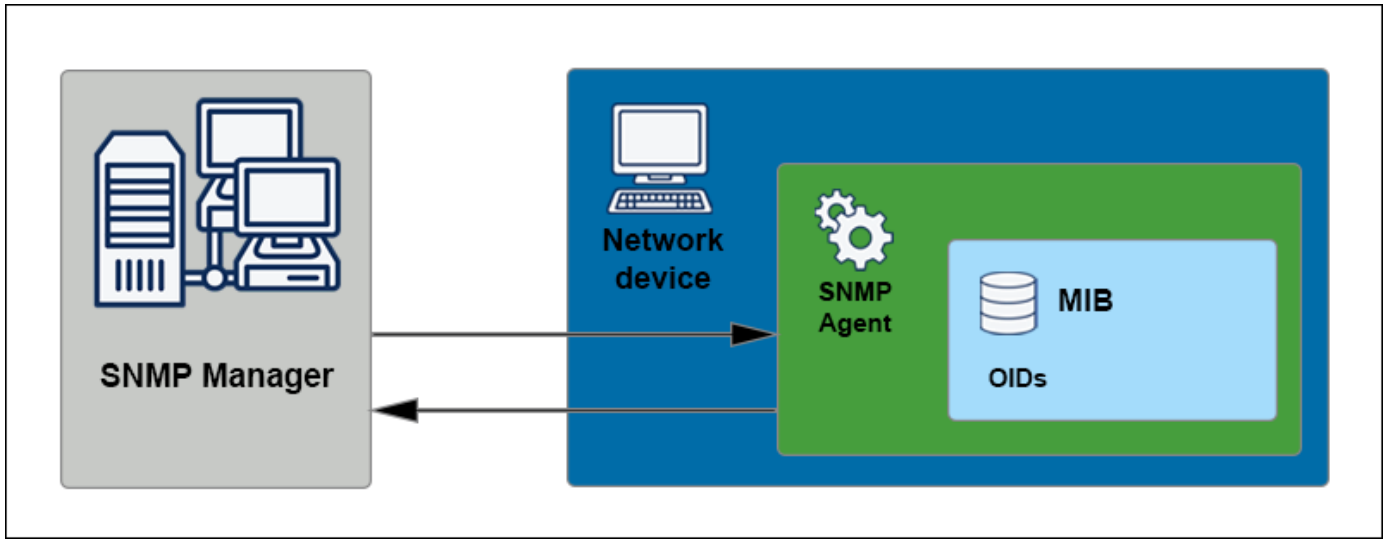
2.4.2. Le modèle organisationnel de l'administration réseau SNMP comporte quatre éléments :

- **Un système de gestion de réseau (NMS - network management system) :** Gère les éléments de réseau sur un réseau.
- **Agent SNMP :** Le logiciel qui s'exécute sur le matériel ou le service surveillé, collecte les données métriques et exécute les opérations demandées dans la MIB du périphérique géré.
- **Une base d'informations de gestion (MIB) :** La MIB est une base de données d'informations qui contient les paramètres des périphériques gérés.

II. La supervision des réseaux informatiques :

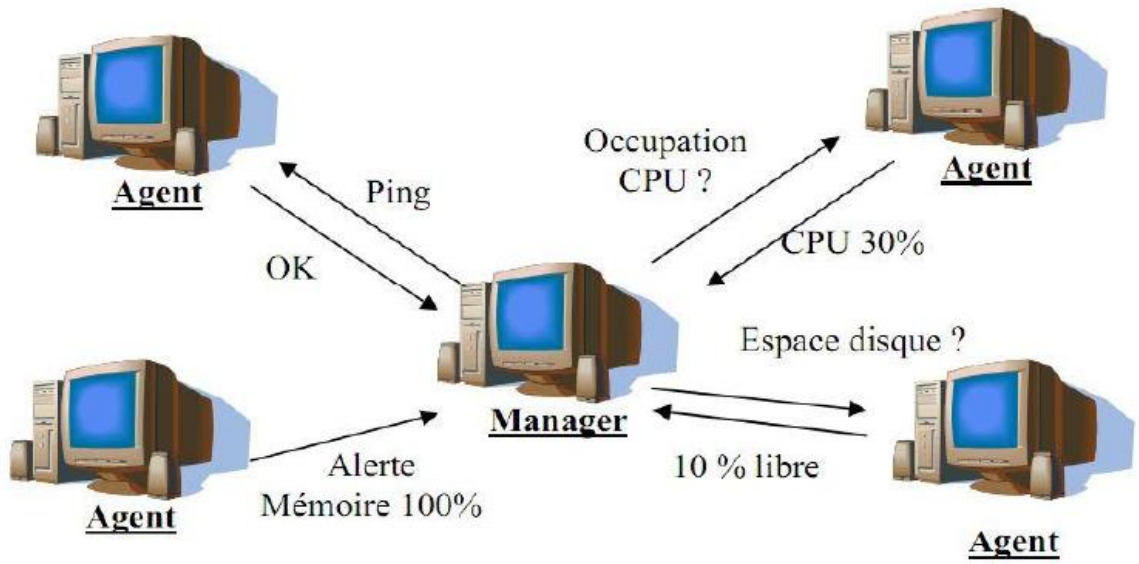
2.4.2. Le protocole SNMP contient les composants clés suivants :

- **Appareil géré :** Nœud du réseau (routeurs, serveurs d'accès, commutateurs, concentrateurs, etc.) contenant l'agent SNMP et la MIB (Management Information Base).

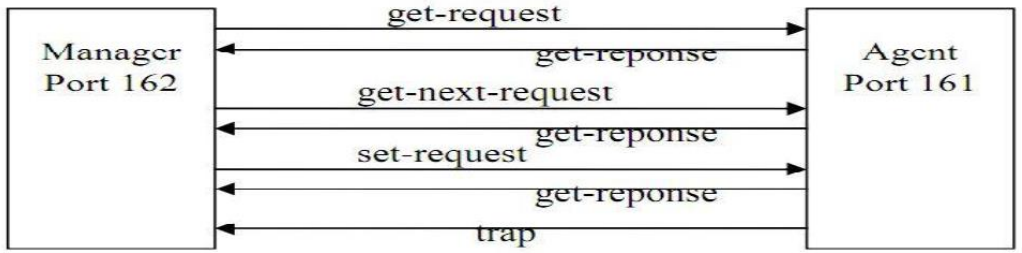


II. La supervision des réseaux informatiques :

Il existe 4 types de requêtes SNMP :
- Get-request : le manager snmp demande une information à un agent snmp
- Get-next-request : le manager snmp demande l'information suivante à l'agent snmp
- Set-request : le manager snmp met à jour une information sur un agent snmp
- Trap : l'agent snmp envoie une alerte au manager



Plusieurs types d'alertes sont alors possibles :
- ColdStart : Démarrage de la machine.
- WarmStart : Arrête de la machine.
- LinkDown : Désactivation de la liaison.
- LinkUp : Activation de la liaison.
- AuthentificationFailure : Erreur de l'authentification.



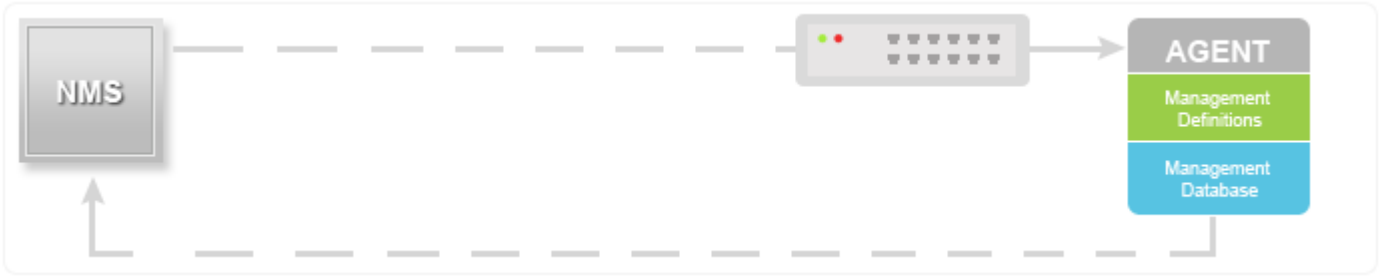
Exemple d'échange SNMP

Les réponses sont du type suivant :
- Get-response : L'information a bien été transmise.
- NoSuchObject : Aucune variable n'a été trouvée.
- NoAccess : Les droits d'accès ne sont pas bons.
- NoWritable : La variable ne peut être écrite.

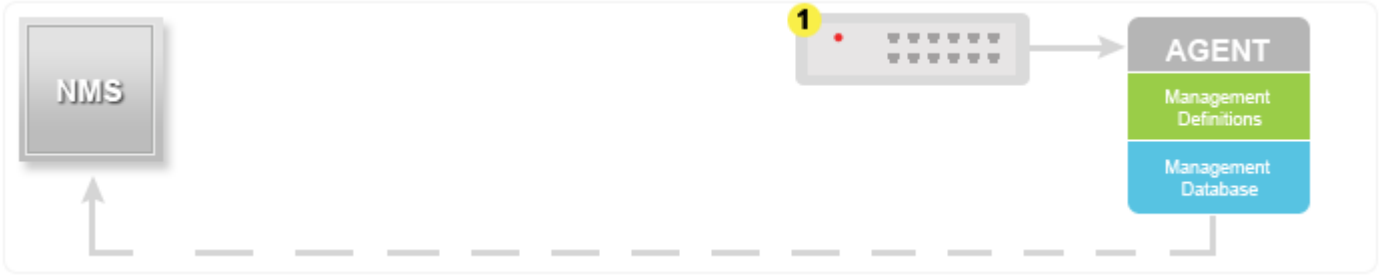
II. La supervision des réseaux informatiques :

2.4.2. Fonctionnement de SNMP :

GET/GET NEXT/GET BULK/SET.



TRAP

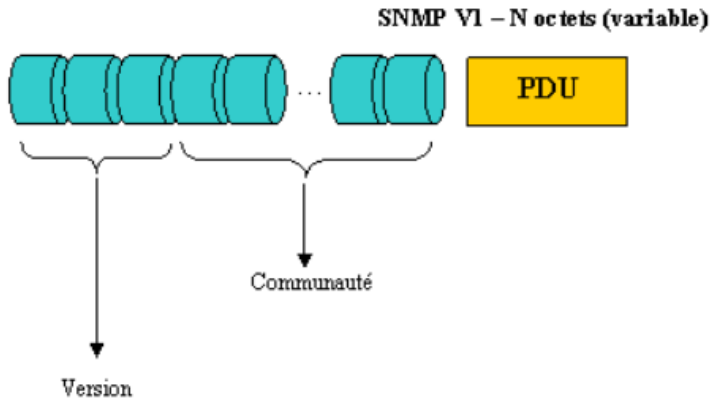


II. La supervision des réseaux informatiques :

2.4.3. La trame SNMPv1 :

La trame SNMPv1 est complètement encodée en ASN.1 [ISO 87]. Les requêtes et les réponses ont le même format.

❑ **La version** la plus utilisée est encore la version 1. Plusieurs versions 2 ont été proposées par des documents de travail, mais malheureusement, aucune d'entre elles n'a jamais été adoptée comme standard. La version 3 est actuellement en voie d'être adoptée. On place la valeur zéro dans le champ version pour SNMPv1, et la valeur 3 pour SNMPv3.

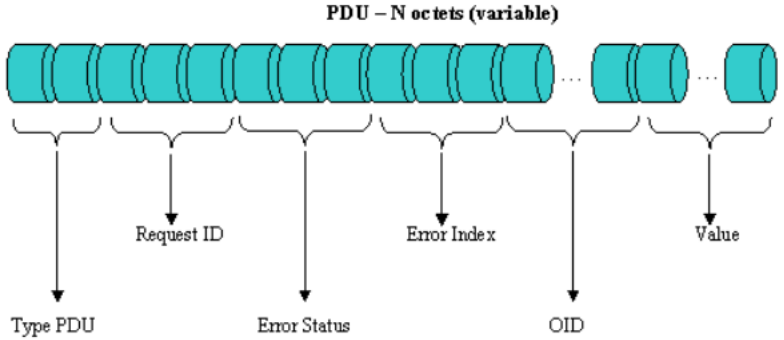


❑ **La communauté** permet de créer des domaines d'administration. La communauté est décrite par une chaîne de caractères. Par défaut, la communauté est « PUBLIC».

❑ **Le PDU** (Packet Data Unit).

II. La supervision des réseaux informatiques :

2.4.3. La trame SNMPv2C :



Le « **PDU type** » décrit le type de requête, de réponse ou d'alerte.
Les valeurs associées à ces champs.

- PDU=0 : Get-request
- PDU=1 : Get next-request
- PDU=2 : Get response
- PDU=3 : Set request
- PDU=4 : Trap

Le « **Request ID** » permet à la station de gestion d'associer les réponses à ses requêtes.
Le « **Error Status** » est l'indicateur du type d'erreur.
Si aucune erreur ne s'est produite, ce champ est mis à zéro.
Les réponses négatives possibles sont décrites dans le tableau suivant :

- Réponse=NoAccess : Accès non permis
- Réponse=WrongLengh : Erreur de longueur
- Réponse=WrongValue : Valeur erronée
- Réponse=WrongType : Type erroné
- Réponse=WrongEncoding : Erreur d'encodage
- Réponse=NoCreation : Objet non crée
- Réponse=ReadOnly : Ecriture non permise
- Réponse=NoWritable : Ecriture non permise
- Réponse=AuthrisationError : Erreur d'autorisation

II. La supervision des réseaux informatiques :

2.4.4. Les améliorations de SNMPv2c et SNMPv3 :

- SNMPv2c a introduit quelques nouveaux types, mais sa nouveauté majeure est l'opération GETBULK, qui permet à une plate forme de gestion, de demander en bloc de plusieurs variables consécutives dans la MIB de l'agent. Généralement, on demande autant de variables que l'on peut mettre dans un paquet SNMP. Ceci règle un problème majeur de performance dans SNMPv1. Avec la version 1, la plate forme est obligée de faire un GETNEXT et d'attendre la réponse pour chaque variable de gestion.
- Par contre la version 3 du protocole SNMP vise essentiellement à inclure la sécurité des transactions. La sécurité comprend l'identification des parties qui communiquent et l'assurance que la conversation soit privée, même si elle passe par un réseau public.

Cette sécurité est basée sur 2 concepts :

- **USM (User-based Security Model)**
- **VACM (View- based Access Control Model)**