Administration et Sécurité des Réseaux

(Licences.Pro : G.L & RSI)

ÉLABORÉ PAR

DIDIER FREDERYCK MBANJOCK

jdmbanjock@gmail.com

2021 - 2022

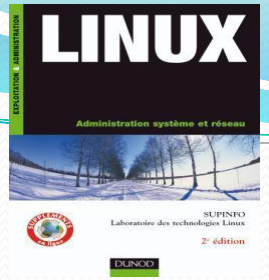
Pré-requis

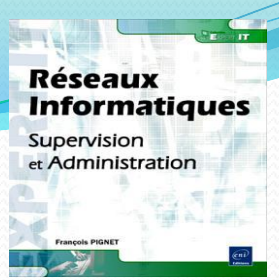
- Systèmes d'information.
- Systèmes informatiques.
- Réseau Internet.
- Réseaux informatiques.
- Les Principaux Protocoles des Réseaux.
- L'Adressage IP et les Techniques de Routage.
- Les plans d'adressage, de Nommage et de Routage.

Objectifs du Chapitre

- Connaître les protocoles applicatifs de l'Internet et savoir mettre en place les services associés sous Linux et sous Windows.
- Manipulation des notions/outils nécessaires à un administrateur réseaux.
- Mise en place d'une plateforme d'administration.
- Déploiement d'une solution d'Administration d'un Réseau.
- Utiliser les Outils de Planification de l'Administration.

Références





🕮	**Titre**	**: "Administration système et réseau"**
	Maison d'édition	: DUNOD
	Auteur	: Laboratoire SUPINFO des technologies LINUX
	Année	: 19/03/2008
🕮	**Titre**	**: "Supervision et Administration"**
	Maison d'édition	: ENI
	Auteur	: François Pignet
	Année	: 10/12/2007
🕮	**Titre**	**: "Essential SNMP"**
	Maison d'édition	: O'REILLY
	Auteur	: Douglas R. MAURO, Kevin J. SCHMIDT
	Année	: 23/09.2005

🖙	**Site 1**	: http://www.misfu.com/information-sur-le-fichier-196.html Ce site nous propose un très bon support de Cours SNMP
🖙	**Site 2**	: http://christian.caleca.free.fr/snmp/principe.htm Ce site a été fait par un expert dans le domaine systèmes et réseaux, offre une excellente alternative par rapport aux autres sites.
🖙	**Site 3**	: http://www.irisa.fr/prive/bcousin/Cours/ Ce site propose plusieurs cours, TP, TD et examens en formats PDF dans le domaine des services réseaux.

PLAN: Introduction à L'Administration et Sécurité des réseaux.

I. Introduction
II. Définitions
III. Les Taches de L'Administrateur Réseaux.
IV. Les Problèmes qui Imposent l'Administration.
V. Les Domaines d'activités et les Objectifs.
VI. Les Principes Fondamentaux de l'Administration.
VII. Organisation logique (critères, types de décisions…)
VIII. Architectures et modèles d'administration.
IX. Les Solutions d'Administration, de Supervision et de Sécurité.

I. Introduction

Le système d'information et les réseaux sont aujourd'hui des éléments critiques de la compétitivité de l'entreprise. De mauvaises performances de ceux-ci se déclinent en pertes de productivité et, les indisponibilités de services se traduisent en pertes de vente, irrégularités d'exploitation ou interruption de la production.

La qualité du service global rendu aux utilisateurs doit être garantie, ce qui implique la maîtrise d'un ensemble complexe de systèmes, réseaux, middleware et applications. Cela doit se faire à un coût minimal.

C'est l'enjeu des activités liées à l'administration de réseaux (et plus généralement du système d'information) que d'offrir cette maîtrise au meilleur coût. Les éléments essentiels à maîtriser sont :

- les coûts,
- la Qualité de service (Qos),
- la Réactivité.

De nos jours, le réseau est en train de devenir obligatoire pour tout le domaine de la vie. La gestion des réseaux est donc indispensable. Il faut régulièrement fairerecours à des techniques d'administration pour pouvoir contrôler son fonctionnement mais aussi afin d'exploiter au mieux les ressources disponibles, et de rentabiliser au maximum les investissements réalisés.

Quelques Rappels

- **Un système d'information : est l'ensemble des éléments** participants à la gestion, au **stockage**, au **traitement**, au **transport** et à la **diffusion** de l'information au sein de l'organisation.
- **Un système informatique :** est **l'ensemble des équipements** destinés au traitement automatique de l'information permettant d'acquérir, de stocker, de traiter et de communiquer des données.
- **Réseau Informatique:** ensemble d'ordinateurs et périphériques interconnectés les uns aux autres grâce à de lignes de transmissions spécialisées afin d'échanger des données de plusieurs natures.

II. Définition : Administration Réseaux

- C'est l'ensemble des moyens mis en œuvre pour garantir l'efficacité du système et sa disponibilité, pour assurer la surveillance des coûts et la planification des évolutions.
- L'Administration de Réseaux englobe tous les moyens mis en œuvre pour :
  - Offrir aux utilisateurs une qualité de service donnée et garantir cette qualité de service,
  - Permettre et guider l'évolution du système en fonction (du trafic, des nouvelles applications des nouvelles technologies),
  - Représente la partie Opérationnelle d'un système soit:
    - La surveillance du Réseau Informatique (système informatique, équipements réseaux…),
    - Support technique,
    - Gestion : des couts, des ressources, du personnel utilisateurs du système.

En plus des protocoles qui fournissent des services de niveau réseau et des programmes d'applications qui utilisent ces services, les administrateurs ont besoin de logiciels qui, dans un réseau, permettent de traiter les problèmes de fonctionnement, de contrôler le routage et de signaler les machines qui ont des comportements anormaux. L'ensemble de ces activités correspond à l'administration de réseaux.

III. Les tâches d'Administration

Actions en temps réel

- **A partir de la connaissance de l'état du fonctionnement du réseau (surveillance et diagnostic des incidents, mesure de la charge réelle, maintenance, contrôle..) l'administrateur devra agir sur celui-ci et assurer la sécurité.**

Actions différées

- **Elles permettent de planifier, optimiser, quantifier et gérer les évolutions du réseau (statistiques, comptabilité, facturation, prévention, évaluation des charges…)**

Actions préventives

- **Elles permettent d'avoir une vision à moyen et long terme, d'évaluer des solutions alternatives, de construire des "benchmarks", de choisir de nouvelles générations de produits, d'envisager les configurations, décider du plan d'extension, de vérifier la pertinence de la solution réseau pour un problème donné.**

IV. Quelques Problèmes qui suscitent l'Administration

- **Les Collisions locales**
  - Des collisions locales sur le réseau sont produites par des stations émettant simultanément. Des taux de collisions élevés laissent supposer que le problème se situe au niveau du câblage.
- **Les Collisions tardives**
  - Les collisions tardives sont celles qui se produisent au-delà du cadre des collisions de 512 bits (les collisions normales se produisent dès les premiers octets d'une transmission). Ces collisions peuvent avoir deux origines. On peut avoir à faire avec une station défectueuse (carte, transceiver etc.) qui n'est plus conforme à la convention CSMA/CD. La station considérée n'"écoute" plus la ligne avant d'émettre.
- **Les Trames écourtées**
  - Ce sont des trames qui sont plus courtes que le minimum requis de 64 octets. Ces trames écourtées sont souvent le produit de cartes ou de pilotes réseau défectueux.

➢Les Trames trop longues ("jabber")

Les trames dont la longueur dépasse les 1518 octets autorisés sont appelées "jabber" (trames "bavardes"). Leur origine est là encore à chercher dans des cartes ou des pilotes réseau défectueux.

➢"Negative frame check sequence" (FCS)

Il s'agit d'une trame dont les octets de contrôle, situés en fin de trame, ne correspondent pas à la somme des bits de la trame, calculée en guise de contrôle. Ceci indique une erreur de transmission, due à une carte réseau défectueuse, à un mauvais câblage ou à des rayonnements perturbateurs.

➢Les Trames fantômes

Une trame fantôme ressemble à une trame de données normale à laquelle on aurait amputée sa séquence initiale ("starting delimiter" **10 10 10 11**).

V. Rôle d'un Administrateur Réseau

- Le rôle d'un administrateur réseau consiste (entre autres) à :
  - Mettre en place et maintenir l'infrastructure du réseau (organisation, . . .).
- Installer et maintenir les services nécessaires au fonctionnement du réseau.
- Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- Gérer les "logins" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, . . .).
- Gérer les systèmes de fichiers partagés et les maintenir.
- L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

VI. Les Domaines d'activités de l'Administration.

- **Besoin d'une administration des réseaux: pourquoi ?**
  - Passage d'une administration de quelques ordinateurs (multi-utilisateurs) à l'administration d'un réseau d'ordinateurs et d'équipements variés (périphériques, commutateurs, ponts, routeurs …) provenant de différents constructeurs et ayant différents systèmes d'exploitations.
  - De nouveaux services réseaux doivent être mis en place (supports pour le développement d'application client serveurs, serveurs de noms, serveurs de disques, serveurs de bases de données …)
- **La nécessité d'outils inter-opérables d'administration et donc de standards**
  - Modèle de l'ISO : CMIP, CMISE …
  - Modèle de l'Internet : SNMP

- **Ces activités sont aussi communément classées de la façon suivante** :

—

la supervision : (monitoring) consiste à surveiller les systèmes et récupérer les informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique (polling) ou par remontée non sollicitée d'information de la part des équipements de réseau eux-mêmes. Cela recoupe plutôt les activités appartenant à la « gestion des anomalies » et la « gestion des performances » de l'ISO ;

l'administration : désigne plus spécifiquement les opérations de contrôle « à froid » du réseau, avec la gestion des configurations, de la sécurité, etc. ;

l'exploitation : désigne l'ensemble des activités qui permettent de traiter les problèmes opérationnels sur le réseau, ce qui recouvre la supervision, mais aussi la maintenance, le support et l'assistance technique.

Les cinq Domaines d'activités de l'Administration

L'ISO (International Standard Organization) a regroupé les activités d'administration de réseaux en cinq domaines fonctionnels ou les 5 SMFA (Spécific Management Function Area) :

— la gestion des anomalies (Pannes);

— la gestion de la comptabilité ;

— la gestion des performances ;

— la gestion des configurations ;

— la gestion de la sécurité.

- L'**ISO**, en partenariat avec l'UIT-T, ne spécifie aucun système d'administration de réseau, mais simplement un cadre architectural : OSI Management Framework (ISO 10040).
- Cette administration s'appuie sur trois modèles :
  - Un modèle organisationnel,
  - Un modèle informationnel,
  - Un modèle fonctionnel.

A. Le modèle Fonctionnel

1. La gestion des Pannes (erreurs)

Détection, localisation, isolation, réparation

- L'administrateur doit être prévenu dès qu'un problème survient : câble coupé, routeur hors service ...
- Il pourra alors isoler l'incident et remédier à la panne. Les techniques d'alerte sont sonores ou visuelles.
- L'Optimisation des ressources et des moyens.
- Le Diagnostic rapide de toute défaillance (externe, coupure d'un lien public, ou interne, panne d'un routeur).
- On retrouve aussi :
  - Surveillance et traitement des alarmes.
  - Localisation et diagnostic des incidents.
  - Mémorisation des anomalies (journalisation).
  - Définition des opérations curatives.

2. La gestion des Configurations

- Identification des ressources.
- Installation, initialisation, paramétrage, reconfiguration.
- Collecte des informations utiles et sauvegarde d'un historique.

- Consiste à maintenir un inventaire précis des ressources matérielles (type, équipement,. . .) et logicielles (version, fonction,. . .).
- Connaître la répartition géographique des équipements gérés.

3. La gestion des Performances

- Évaluation: collecter les données et établir des statistiques sur les performances (temps de réponse, taux d'utilisation, débit, taux d'erreur, disponibilité).
- Gestion de trafic : satisfaire les besoins des **users** (à qui attribuer un grand débit…).

- Mettre en œuvre des moyens permettant d'évaluer le comportement des objets gérés.
- Déterminer si la **QoS** est rendue aux utilisateurs.
- On retrouve aussi :
  - La collecte d'information (audit)
    - Mesure de trafic
    - Temps de réponse
    - Taux d'erreurs
  - Le stockage (archivage)
  - L'interprétation des mesures (calcul de charge)

4. La gestion de la Comptabilité

- Gérer la charge des ressources pour empêcher toute surcharge (congestion).
- Gérer le coût d'utilisation des ressources et les facturer.
- Gérer le quota d'exploitation de la ressource (imprimante, disques, scanners ...).
- Cette fonction permet essentiellement d'imputer les coûts du réseau à ses utilisateurs selon l'usage réel des moyens (comptabilité analytique).
- On retrouve :
  - Définition des centres de coût,
  - Mesure des dépenses (structure) et répartition,
  - Mesure des consommations par service,
  - Imputation des coûts.

5. La gestion de la Sécurité

- **But**: protéger les ressources du réseau et du système d'administration.
- **Comment**: Assurer les services de la sécurité (authentification, confidentialité, intégrité, disponibilité et non répudiation).
- Moyen : cryptographie + logiciel de supervision + audit + firewall + surveillance des journaux d'évènements.
- Journal de sécurité,
- Journal système,
- Journal application.

Security Management : Gestion de la sécurité

- Regroupe tous les domaines de la sécurité afin d'assurer l'intégrité des informations traitées et des objets administrés :
  - Contrôle d'accès au réseau,
  - Confidentialité des données,
  - Intégrité des données,
  - Authentification,
  - Non désaveu.

B. Le modèle Organisationnel

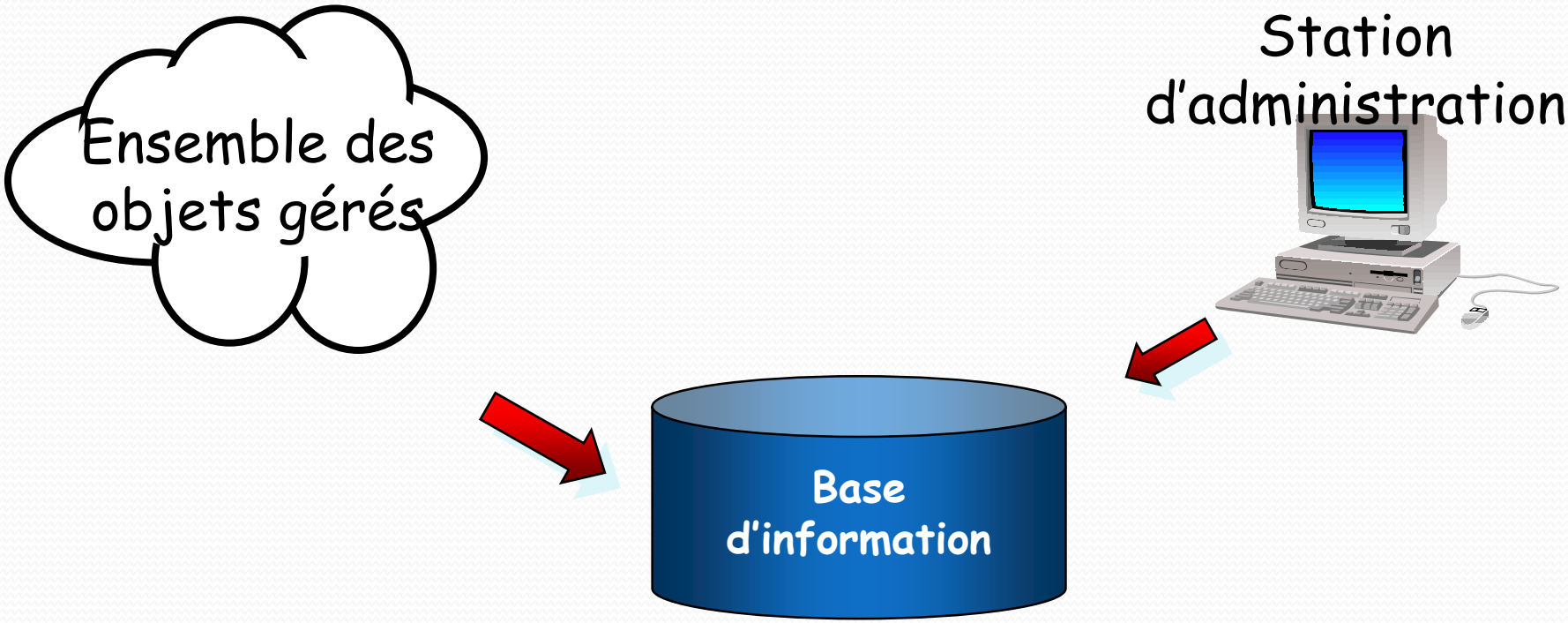
- Ce modèle fournit les moyens de transfert des informations de gestions entre les objets administrés.
- Il définit également un dialogue (le **CMIP** : Common Management Information Protocol ISO 9596), lequel utilise les primitives suivantes :
  - Get, cet élément de service est utilisé par le gérant 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.

C. Le modèle Informationnel

- **Ce standard décrit une méthode de définition des données d'administration.**
- **L'ensemble des éléments gérés est orienté objet et constitue une MIB (Management Information Base : ISO 10165) qui contient toute les informations administratives sur ces objets :**
  - **Ponts,**
  - **Routeurs,**
  - **Cartes,**
  - **Passerelles,**
  - **Commutateurs,**
  - **Concentrateurs.**

VII. Les Principes Fondamentaux de l'Administration Réseaux.

- **L'administration d'un réseau suppose l'existence d'une base d'information décrivant l'ensemble des objets administrés.**



A. Le Principe Général.

- Sur le point de l'administration, un système de réseau informatique se compose d'un ensemble d'objets qu'un système d'administration surveille et contrôle. Chaque objet est géré localement par un processus appelé **Agent** qui transmet régulièrement ou sur sollicitation les informations de gestion relatives à son état et aux événements qui le concernent au système d'administration.
- Le système d'administration comprend un processus (**manager ou gérant**) qui peut accéder aux informations de gestion de la **MIB** locale via un protocole d'administration comme **SNMP** ou **CMIP** de qui le met en relation avec les divers agents.
- Le principe se repose donc sur les échanges :
  - D'une part, entre une base d'informations appelée **MIB**(Management Information Base) et l'ensemble des éléments administrés (**objets**) ;
  - D'autre part, entre les éléments administrés et le système d'administration.

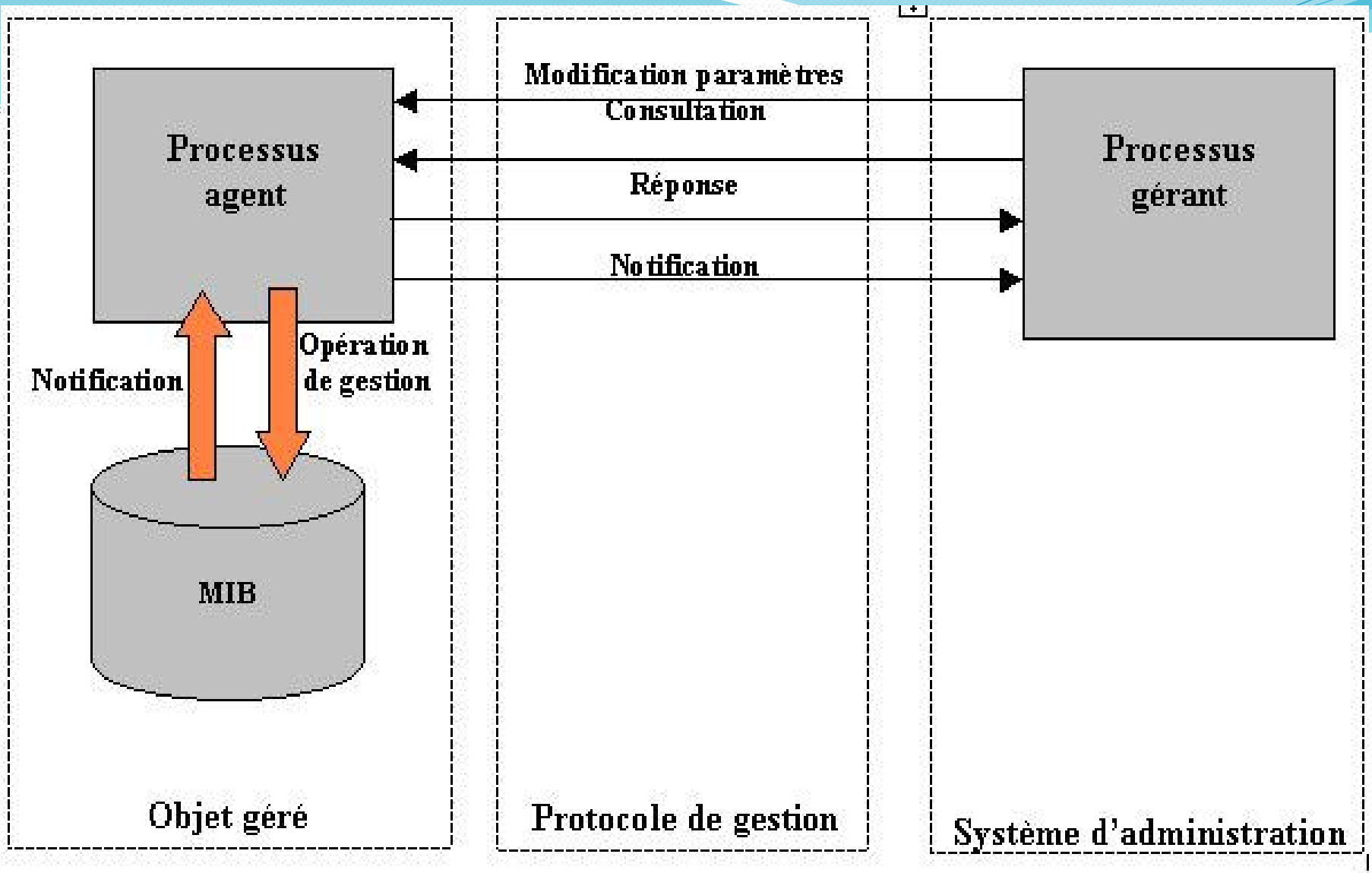
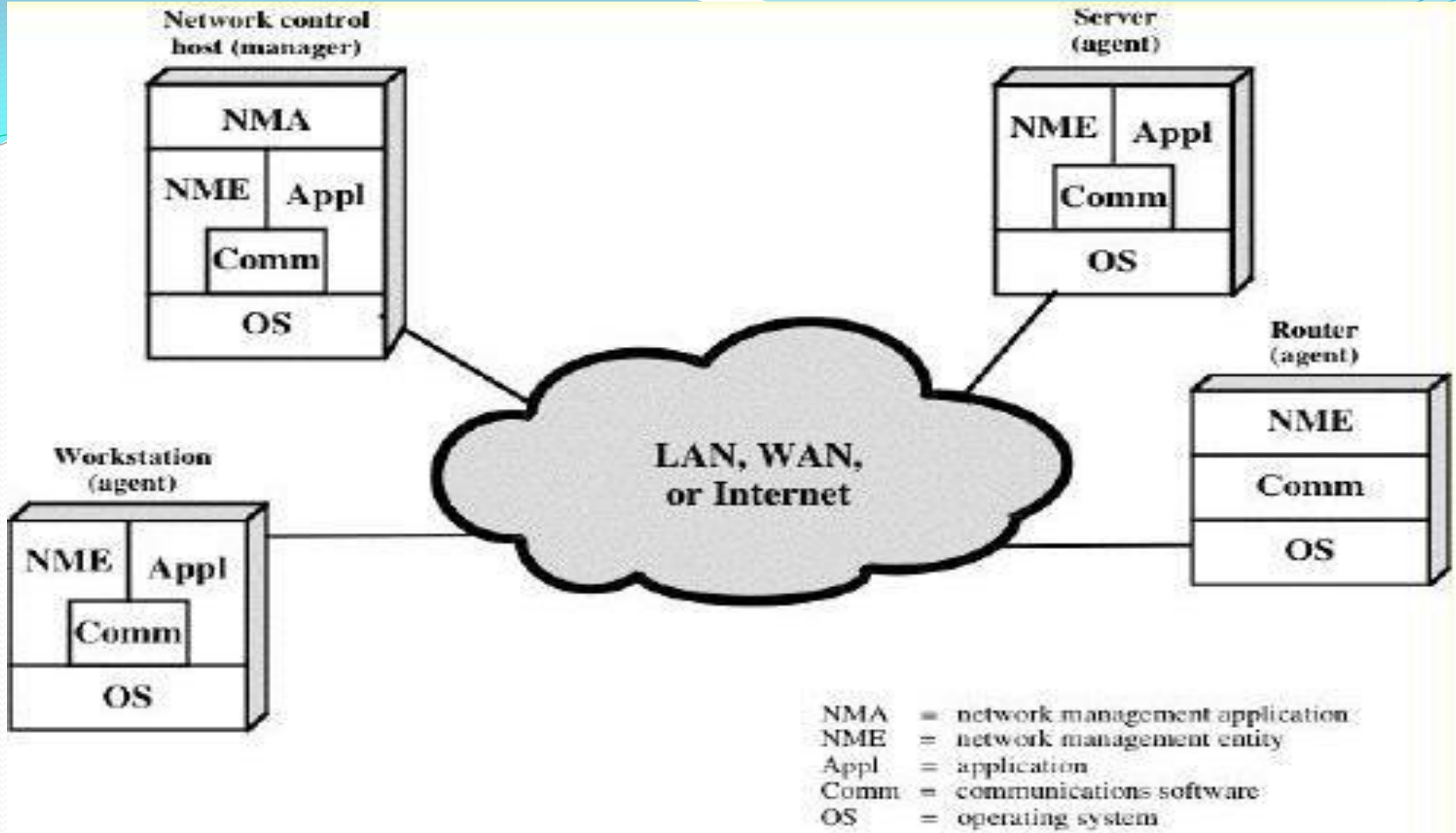


Fig.1 - Structure fonctionnelle d'une d'administration réseau

B. Architecture d'administration

- La figure ci-dessous présente une architecture classique d'administration appelé le modèle Gérant/ Agent (Manager/Agent). Le système est composant d'une entité d'administration et des entités de gestion (NME) qui sont géré par cette entité et un
- protocole pour la gestion comme CMIP ou SNMP.


Network control host (manager)
NMA
NME
Appl
Comm
OS
Server (agent)
NME
Appl
Comm
OS
Router (agent)
NME
Comm
OS
LAN, WAN, or Internet
Workstation (agent)
NME
Appl
Comm
OS
NMA = network management application
NME = network management entity
Appl = application
Comm = communications software
OS = operating system

Chaque entité dans le réseau a un Agent pour l'opération de gestion, une base de données stockées dans MIB et assume les travaux ci-dessous :

- Collecter des informations statistiques concernant à la communication, les opérations de réseau.
- Stocker les informations localement dans les **MIBs**.
- Répondre les commands de l'entité de contrôle de réseau, inclus :
  - Transmet des informations statistiques à l'entité d'administration de réseau, modifie les paramètres, donne des informations d'état…

L'entité d'administration a une entité de gestion (**NME**) et aussi un logiciel pour gérer le réseau appelé **NMA** (Network Management Application). NMA contient une interface permettant l'administrateur fait des opérations de gestion.

VIII. Organisation Logique de L'Administration Réseau

Les Critères pour une organisation logique

- **Critères informationnels :**
  - Ensembles des informations servant à gérer le réseau.
  - Informations en provenance des équipements du réseau, des utilisateurs, des mesures effectuées.
  - Informations décrivant les différents composants du système (adresses, comptes utilisateurs, données de droit d'accès…).
- **Critères fonctionnels :**
  - Ensembles des fonctions servant à gérer le réseau
  - Ajout d'utilisateur, définition des droit d'accès, autorisation à un port, augmentation du débit d'un port…

- **Critères temporels:**
  - Évolution du système (matériel + logiciel),
  - À court terme (journalière),
  - Moyen terme : des jours à quelques mois,
  - Long terme : des mois à une année.
- **Critères de discipline:**
  - Administration des utilisateurs, des fournisseur de services

- **Doit respecter les quatre critères déjà cités**
  - Informationnels,
  - Fonctionnel,
  - Temporel,
  - Discipline.
- **Englobe (plan):**
  - Les services de gestion du réseau réel,
  - Les services de gestion du réseau logique,
  - La gestion des performances,
  - La gestion de la planification.

- **Les services de gestion du réseau réel : activités à court terme qui gère les données en provenance du système**
  - Collecter les données,
  - Exécuter toutes les fonctions du service,
  - Prendre en compte les alertes et notifier les évènements,
  - Déterminer et identifier les problèmes,
  - Contrôler la configuration du système,
  - Activer/ désactiver un élément du système,
  - Assurer la maintenance technique.

- **Les services de gestion du réseau Logique : activités à Moyen terme basées sur les données stockées.**
  - Supprimer les information de gestion inutiles,
  - Évaluer le niveau de la **QoS**.
  - Pouvoir maintenir un inventaire complet du système.
  - Gérer et interpréter les problèmes et les anomalies répertoriées,
  - Pouvoir évaluer le trafic,
  - Contrôler la sécurité (essayer d'exécuter des attaques),
  - Faire la comptabilité du système,
  - Gérer la modification (conserver des traces).

- Pour répondre aux besoins d 'administration du réseau Internet, l'**IETF** (**I**nternet **E**ngineering **T**ask **F**orce) a créé, en 1988, un protocole : **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol).
- Objectifs de SNMP :
  - Fédérer en un standard unique des protocoles multiples liés aux équipementiers.
  - Déploiement rapide et à moindre coût.

  - **Approche Pratique du Protocole SNMP par le biais d'un TPE avec Simulation Pratique.**