Université des Frères Mentouri Constantine
Faculté des Sciences de la Technologie
Département d'Electronique

Administration des services réseau

Master 1 : Réseau et Télécommunication
2021-2022

DR. GUELTOUM BENDIAB
EMAIL: BENDIAB.KELTHOUM@UMC.EDU.DZ

Prérequis

- Les bases des réseaux informatiques
- Les Protocoles de communication
- Modèle OSI
- Modèle TCP/IP
- Les éléments d’un réseau.

Objectifs du cours

Acquérir les connaissances et les compétences nécessaires pour **l'exploitation**, **l'administration**, **la maintenance** et **la surveillance des réseaux informatiques**. L'étudiant se familiarisera avec des fonctions et des protocoles qui doivent lui permettre de gérer entre autres les:

- les droits d'accès,
- le trafic des données circulant sur le réseau,
- la sauvegarde des données,
- le bon fonctionnement des services notamment les services annuaires,
- les services de messagerie électronique et les services d'applications, etc.

Contenu de la matière

- **Chapitre 1**. Présentation de l'administration réseau,
- **Chapitre 2**. Le service SNMP (Simple Network Management Protocol)
- **Chapitre 3**. Les services annuaires
- **Chapitre 4**. Gestion des utilisateurs et service NFS
- **Chapitre 5**. Service de messagerie et services d'application
- **Chapitre 6**. Contrôleur de domaine

Chapitre 1. Présentation de l'administration réseau

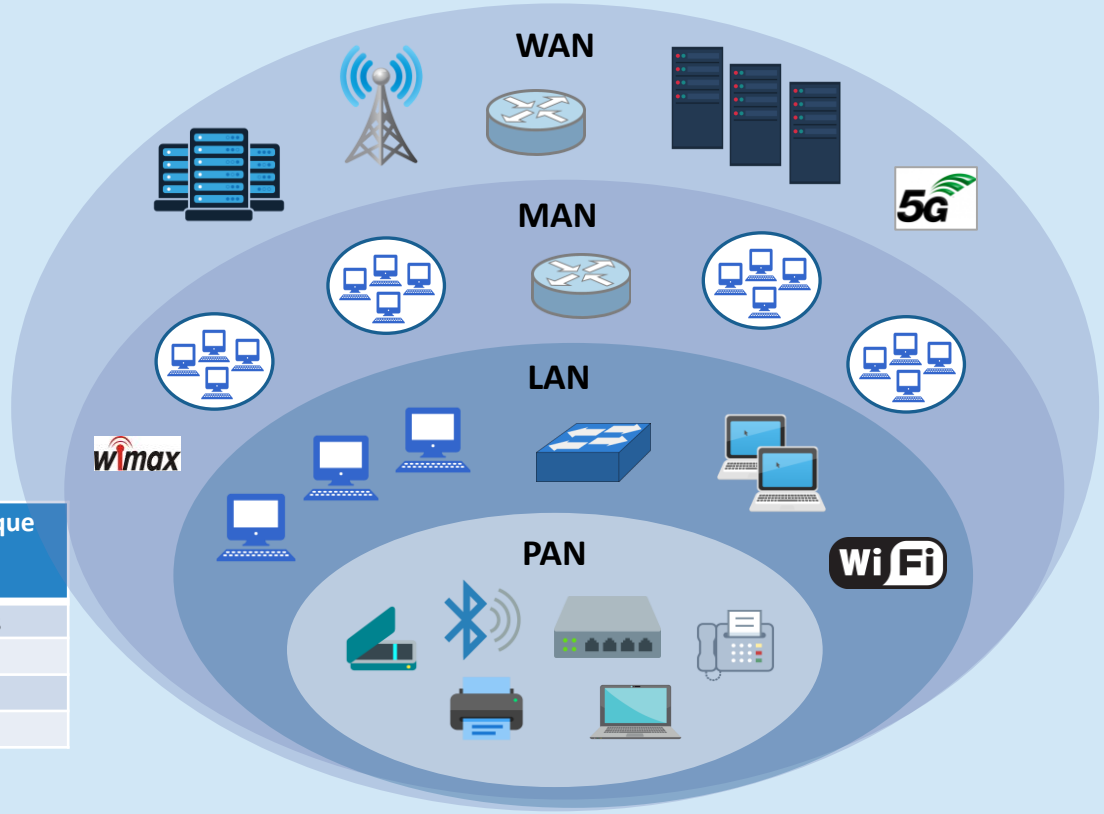
- Objectifs et rôle de l'administration
- Modèle d'administration réseaux
- Réseau clients serveurs
- Les protocoles d'administration
- Les services de la couche d'application
- Notions de ports de service

Réseau informatique

- Un réseau informatique est un ensemble d'ordinateurs interconnectés les uns avec les autres afin qu'ils puissent partager des ressources matérielles et/ou logicielles ainsi que la communication entre processus et entre utilisateurs.
- Avantages:
  - Partage de ressources informatiques matérielles/logicielles,
  - Stockage central de données,
  - Augmentation de la capacité de stockage,
  - Résolution plus rapide des problèmes,
  - Fiabilité,
  - Flexibilité,
  - Réduction des coûts.

Types de Réseaux informatiques

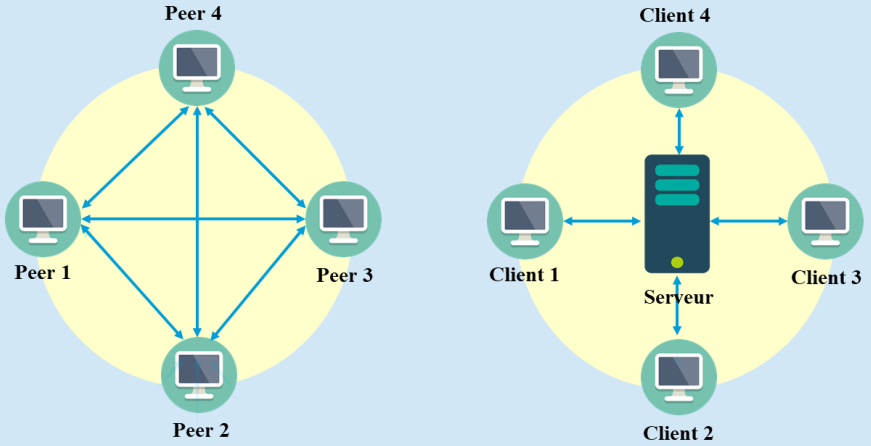
- Les principales catégories de réseaux informatiques selon le **découpage géographique:**
  - **PAN**: Personale Area Network,
  - **LAN**: Local Area Network,
  - **MAN**: Metropolitan Area Network,
  - **WAN**: Wide Area Network)



Type de réseau	Débit	Taille	Etendu géographique
PAN	Inférieur à 1 Mbit/s	1-5 utilisateurs	Dizaines de mètres
LAN	Supérieur à 1 Mbit/s	100 à 1000 utilisateurs	Privée et limitée
MAN	1 à 100 Mbit/s	2 à 1000 abonnées	1 mètre à 100 km
WAN	50 bit/s à 2 Mbit/s	Plusieurs milliers d'abonnés	Plus de 1000 km

Architecture des Réseaux informatiques

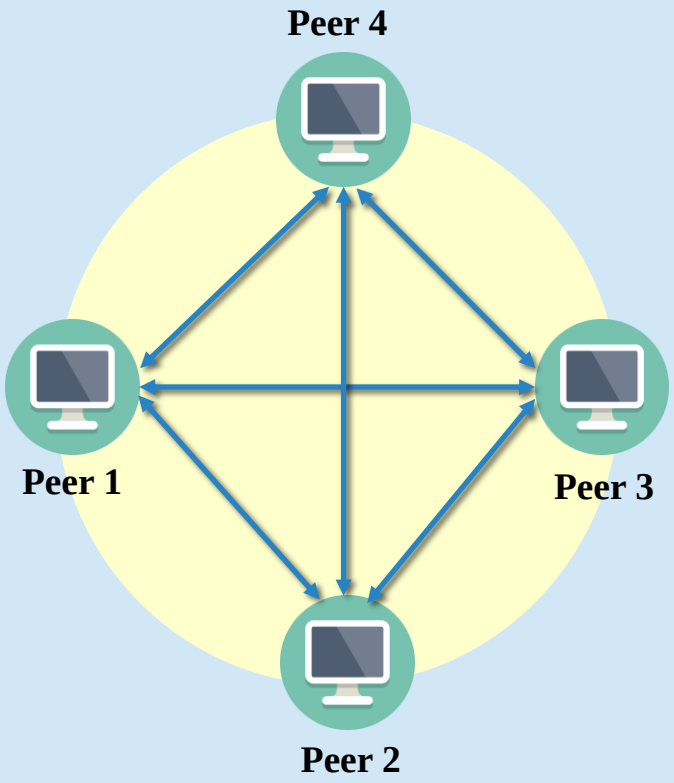
- Fait référence à la façon dont les ordinateurs sont organisés en réseau,
- Définit la manière dans les ordinateurs doivent être connectés pour obtenir le maximum d'avantages du réseau, comme une meilleure évolutivité de la sécurité, du temps de réponse, etc.
- Les deux architectures de réseau informatique les plus connus sont :
  - **Poste à poste (en anglais Peer to Peer, P2P),**
  - **Client/serveur.**



Architecture des Réseaux informatiques

Peer to Peer

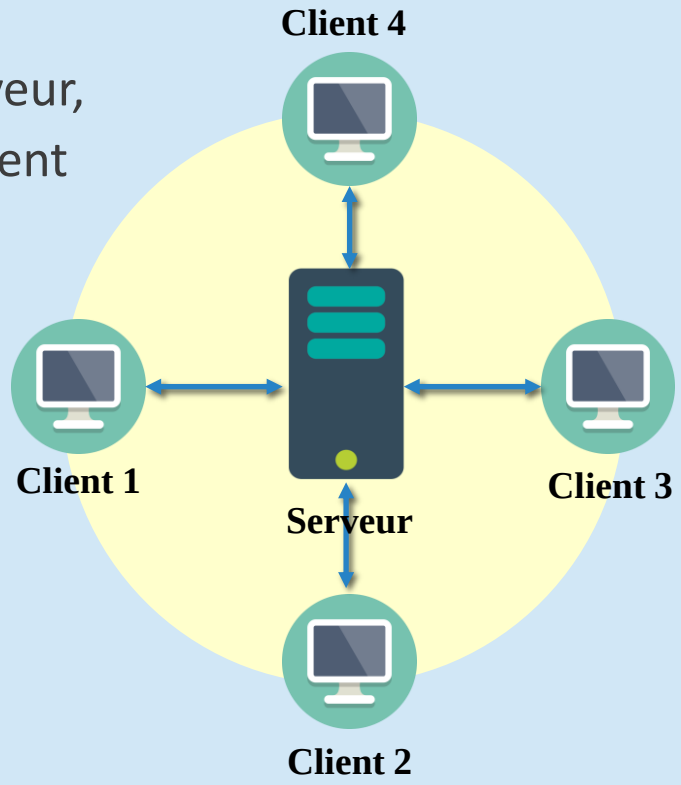
- Chaque nœud agit en tant que client et serveur.
- Le client demande le service et le serveur offre le service.
- Chaque pair a ses propres données
- **Avantage**: moins chers à mettre en œuvre.
- **Inconvénient**: non évolutif : le Peer-to-Peer souffre si le nombre de pairs augmente dans le système.



Architecture des Réseaux informatiques

Client-Serveur

- Il y a un serveur spécifique et des clients connectés au serveur,
- Chaque nœud peut demander des services et peut également fournir de services,
- Les données sont stockées dans un serveur centralisé,
- **Avantage**: plus stable et évolutif.
- **Inconvénient**: lorsque plusieurs clients demandent des services simultanément, le serveur peut être encombré.

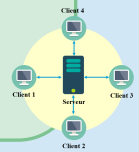


Architecture des Réseaux informatiques

Comparaison des deux types d'architectures

Client-Serveur

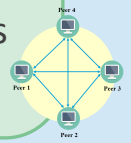
- **Définition**: Il y a un serveur spécifique et des clients spécifiques connectés au serveur,
- **Service**: le client demande le service et le serveur offre le service,
- Les données sont stockées dans un serveur centralisé,
- **La stabilité:** plus stable et évolutif.
- **Le coût**: coûteux à implémenter.
- **Disponibilité**: Lorsque plusieurs clients demandent les services simultanément, un serveur peut être encombré.
- **Gestion de données**: les données sont stockées dans un serveur centralisé.



VS

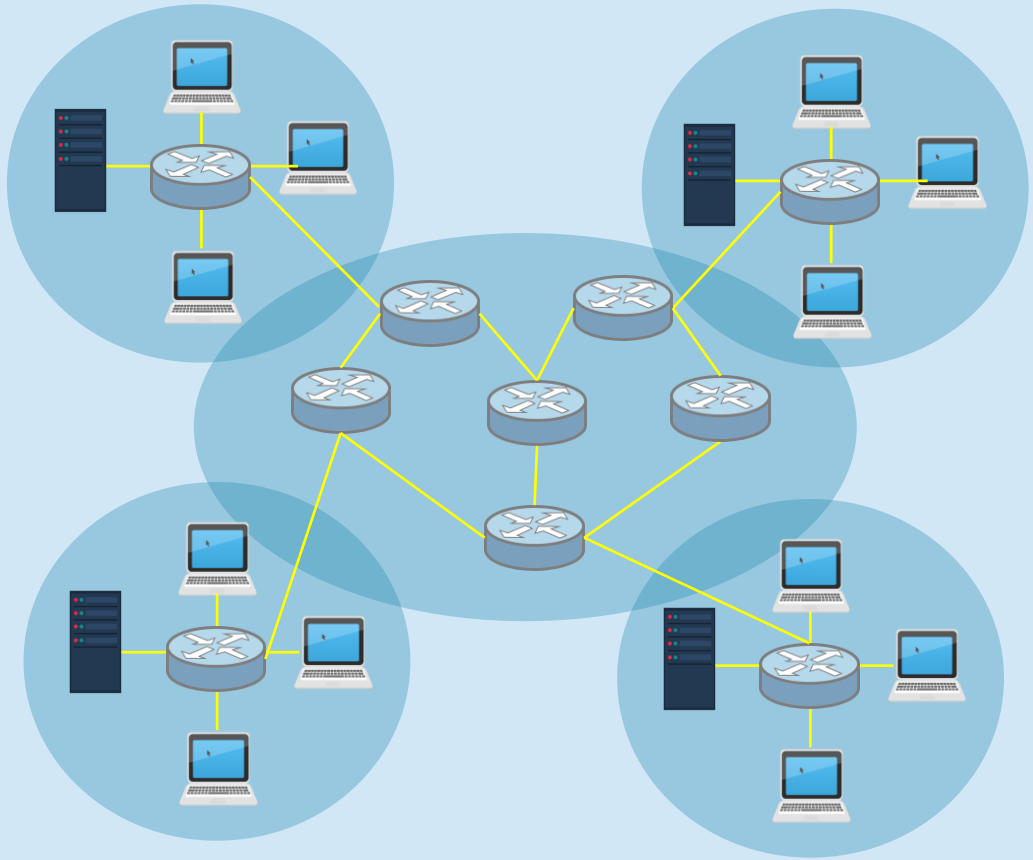
Peer-to-Peer

- **Définition**: chaque nœud agit en tant que client et serveur,
- **Service**: chaque nœud peut demander des services et peut également fournir de services,
- Les données sont stockées dans un serveur centralisé,
- **La stabilité:** non évolutif: le Peer-to-Peer souffre si le nombre de pairs augmente dans le système.
- **Le coût**: moins chers à mettre en œuvre.
- **Disponibilité**: comme les services sont fournis par plusieurs serveurs répartis dans le système peer-to-peer, un serveur n'est pas encombré.
- **Gestion de données**: Chaque pair a ses propres données.



Administration des réseaux informatiques

- Les entités d'un réseau informatique (routeurs, switch, serveurs, hub, PC, imprimante, etc.) peuvent être dispersées sur plusieurs sites.
- Nécessite une **vérification périodique** pour s'assurer quelles fonctionnent correctement, donc, Il faut les superviser (les surveiller).
- L'administration (la supervision) du réseau et des services est **primordiale** pour assurer le bon fonctionnement du réseau.



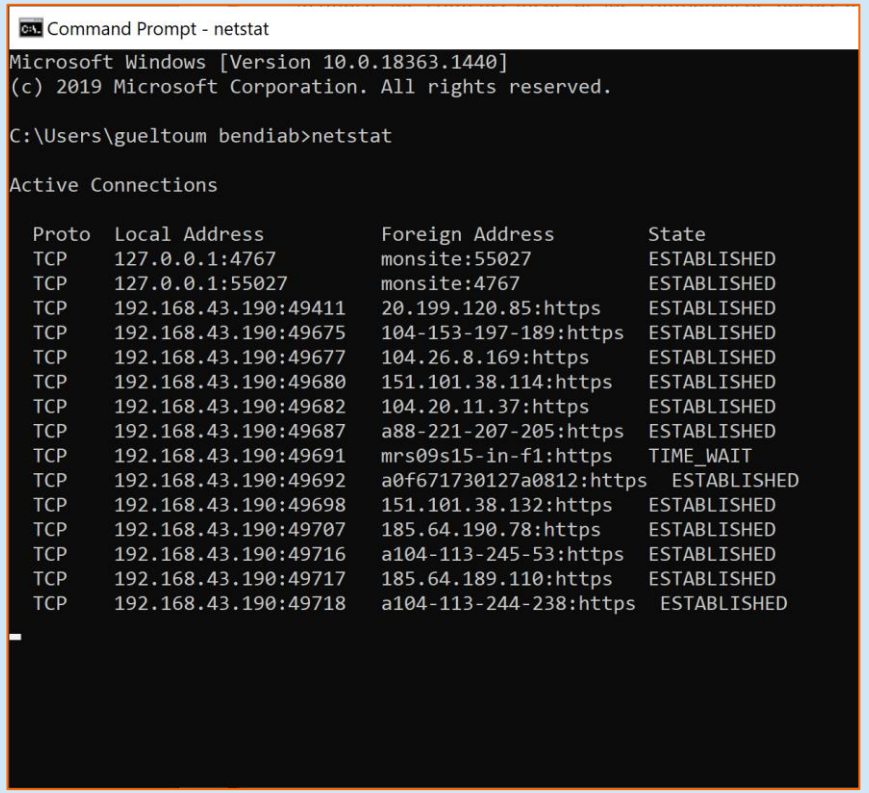
Administration des réseaux informatiques

- 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.
- Objectives:
  - Offrir aux utilisateurs des services de qualité avec des performances optimales.
  - Permettre une utilisation maximale des ressources du réseau avec un coût minimal.
  - Assurer la sécurité et la disponibilité des ressources du réseau à tout moment.
  - Contrôler l'accès au réseau et aux ressources par les utilisateurs.
  - Permettre l'évolution du réseau en incluant de nouvelles fonctionnalités et de nouveaux composants.

Exemples d'outils d'administration

Il est possible d'accéder à des informations **localement** sur une machine en utilisant des commandes système comme:

- **Netstat**: permet de connaître les connexions TCP actives sur la machine sur laquelle la commande est activée, ainsi que lister l'ensemble des ports TCP et UDP ouverts sur l'ordinateur et des statistiques sur un certain nombre de protocoles (IPv4, IPv6, ICMP, etc.).
- **Ping:** permet de tester l'accessibilité d'une autre machine à travers un réseau IP.
- **Traceroute:** suivre les chemins qu'un paquet de données (paquet IP) va prendre pour aller de la machine locale à une autre machine connectée au réseau IP.



Exemples d'outils d'administration

Il est possible d'accéder à des informations **localement** sur une machine en utilisant des commandes système comme:

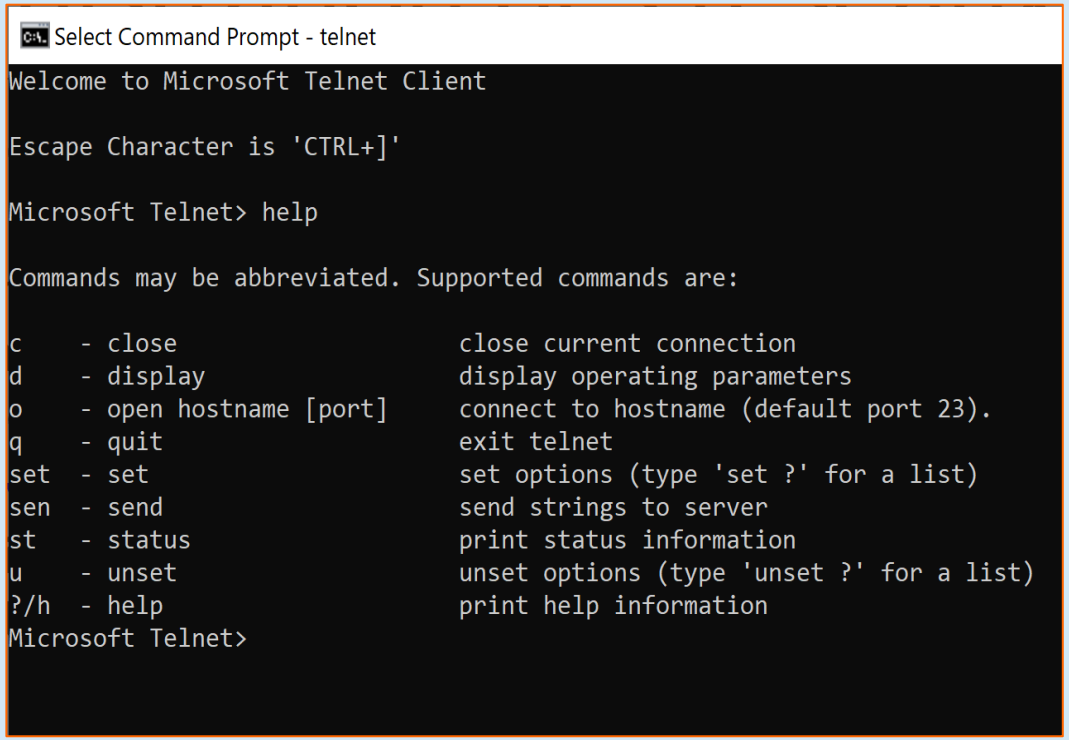
- **Nmap (Network Mapper):** détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant (https://nmap.org/book/man.html).
- **Iperf:** outil de mesure de performance réseau, pour mesurer la bande passante et la qualité d'un lien réseau.
- **Uptime**: pour tester la charge du system.
- **Free/df**: statistiques sur la mémoire et disque
- **Top**: affiche en temps réel la liste des processus système linux.

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

Exemples d'outils d'administration

Il est aussi possible d'accéder à des informations **à distance** sur une machine en utilisant des commandes système comme:

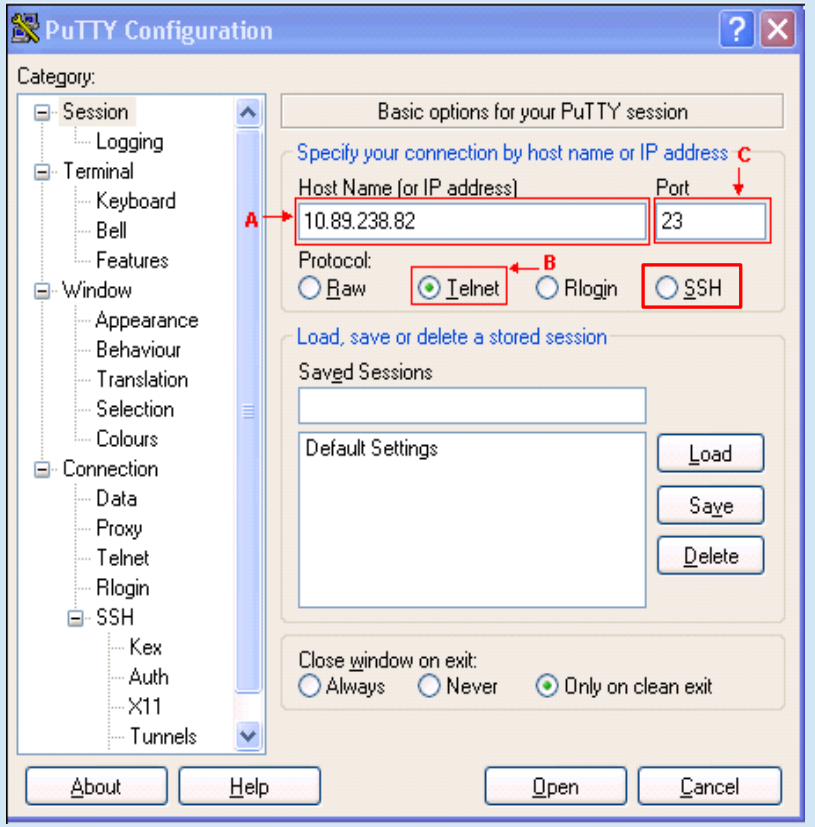
- **Telnet**: ce protocole TCP est largement utilisé pour le contrôle à distance du matériel réseau.
- Pour installer telnet sur Windows 10 :
  - Ouvrir "**Panneau de configuration**".
  - Ouvrir "**Programmes**".
  - Sélectionner l'option "**Activer ou désactiver des fonctionnalités Windows**".
  - Cocher la case "**Client Telnet**"



Exemples d'outils d'administration

Il est aussi possible d'accéder à des informations **à distance** sur une machine en utilisant des commandes système comme:

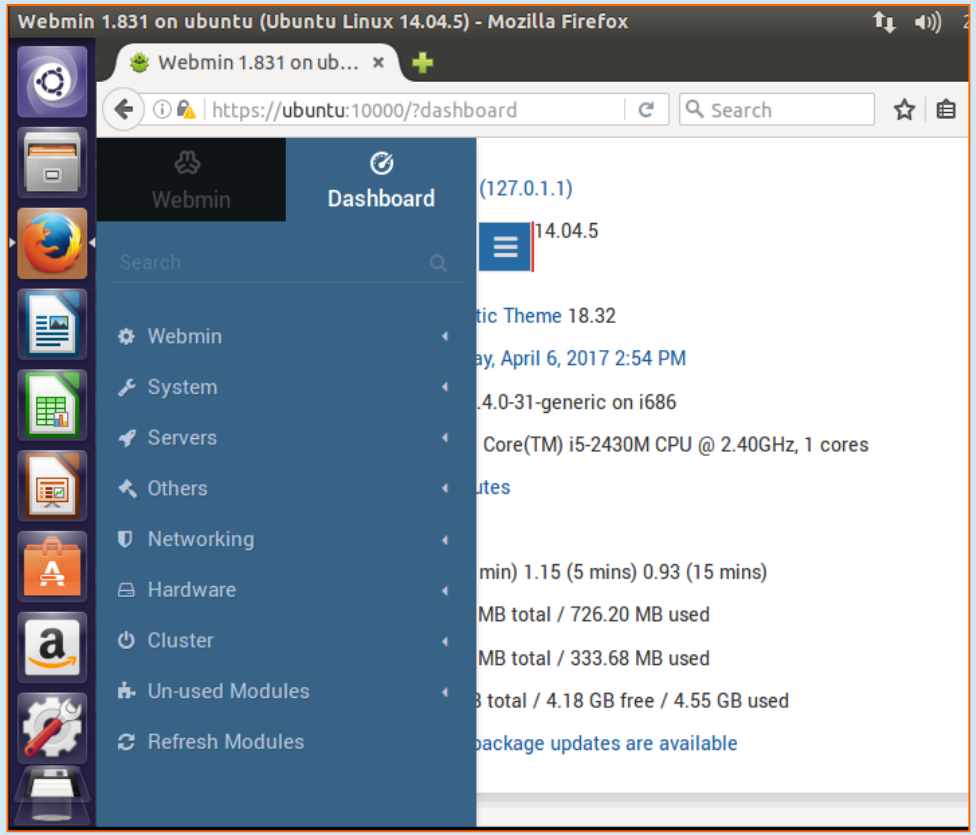
- **Telnet/SSH**: le protocole SSH comble les lacunes de sécurité de telnet en cryptant la transaction via le protocole **SSL**.
- Il permet également d'effectuer des transferts de fichiers entre les deux hôtes (protocole SCP: Secure Copy Protocol).
- **PuTTY** est un outil permettant de se connecter à distance à des serveurs en utilisant les protocoles SSH, Telnet ou Rlogin.



Exemples d'outils d'administration

Il est aussi possible d'accéder à des informations **à distance** via **une interface web**:

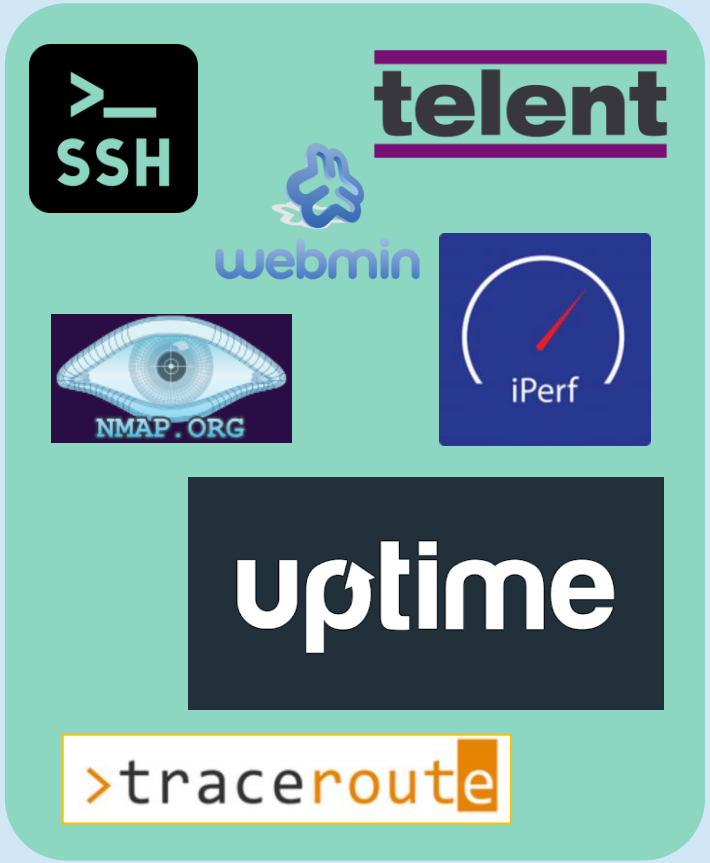
- Ces outils fournit une interface plus intuitive et plus agréable à utiliser que l'interface Telnet.
- **Webmin:** dont le nom vient de la contraction **Web** et **Admin**, est un outil d'administration réseaux open source (licence BSD) basé sur une interface Web pour les serveurs **Unix/Linux** (https://www.webmin.com/).



Exemples d'outils d'administration

Problèmes

- Ces outils ne donnent pas des informations sur le réseau complet.
- Solutions très liées au système d'exploitation et à la machine sur laquelle la commande est activée.
- Très compliquer si le nombre de machine est grand, si les machines sont hétérogènes et si elles sont dispersées sur plusieurs sites.
- La complexité et l'hétérogénéité imposent des **standards** pour l'administration et la définition des **protocoles** pour **l'administration des réseaux informatiques**.



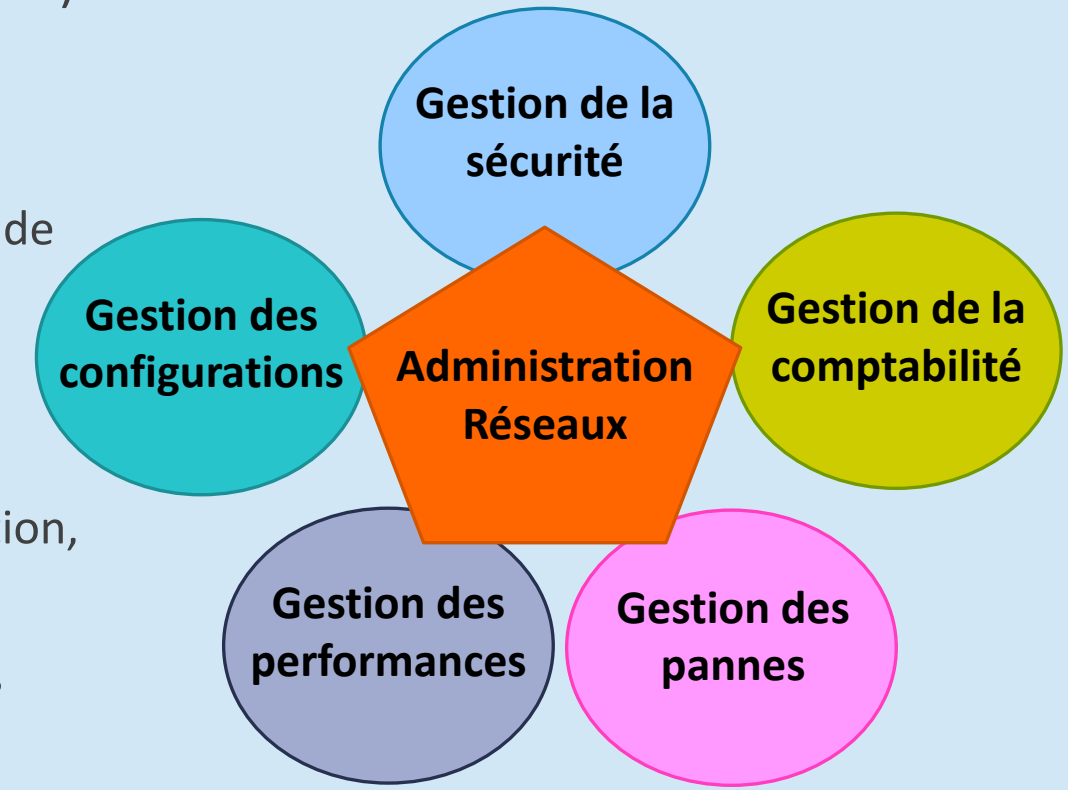
Modèles d'administration des réseaux (ISO)

Les documents **ISO 7498-4** et **ISO 1004** décrivent trois modèles d'administration des réseaux:

- Le modèle fonctionnel (Domaines),
- Le modèle organisationnel,
- Le modèle informationnel (MIB).

Modèle fonctionnel (Domaines)

- L'ISO définit 5 domaines d'administration (gestion):
  - **Gestion des configurations**: Paramétrage des équipements et de la topologie.
  - **Gestion des performances** : Mesures, statistiques de la charge, des flux et des erreurs.
  - **Gestion des pannes**: détection et localisation des défaillances et contournement.
  - **Gestion de la comptabilité**: recensement, facturation, rentabilisation, contrat de maintenance.
  - **Gestion de la sécurité**: protection du réseau et des utilisateurs contre les intrusions et malveillances.



Modèle fonctionnel (Domaines)

- L'ISO définit 5 domaines d'administration (Gestion):
  - **Gestion des configurations**: Paramétrage des équipements et de la topologie.
    - Gérer la configuration matérielle et logicielle et ;
    - Préciser la localisation de l'équipement.
  - **Gestion des performances** : Mesures, statistiques de la charge, des flux et des erreurs.
    - Collecte d'informations et mesure du temps de réponse, taux d'erreurs, etc.
    - Stockage et l'interprétation des mesures dans la MIB (Management Information Base),
    - Calculs de charge du système,
    - Examen des journaux chronologiques de l'état du système.
    - Utilisation des outils de modélisation et simulation permettant d'évaluer l'impact d'une modification de l'un des paramètres du système.

Modèle fonctionnel (Domaines)

- L'ISO définit 5 domaines d'administration (Gestion):
  - **Gestion des pannes**: détection et localisation des défaillances et contournement.
    - 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 journalisation des problèmes, etc.
  - **Gestion de la comptabilité**: recensement, facturation, rentabilisation, contrat de maintenance.
    - Mesure de la consommation réseau par abonné ;
    - Définition des centres de coût ;
    - Mesure des dépenses de structure (coûts fixes) et répartitions ;
    - Mesure des consommations par services ;
    - Imputation (computation) des coûts.

Modèle fonctionnel (Domaines)

- L'ISO définit 5 domaines d'administration (Gestion):
  - **Gestion de la sécurité**: protection du réseau et des utilisateurs contre les intrusions et malveillances.
    - **Contrôles d'accès**: contrôler qui pénètre au réseau et quand;
    - **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.

Triade CIA de la sécurité informatique

Modèle informationnel (MIB)

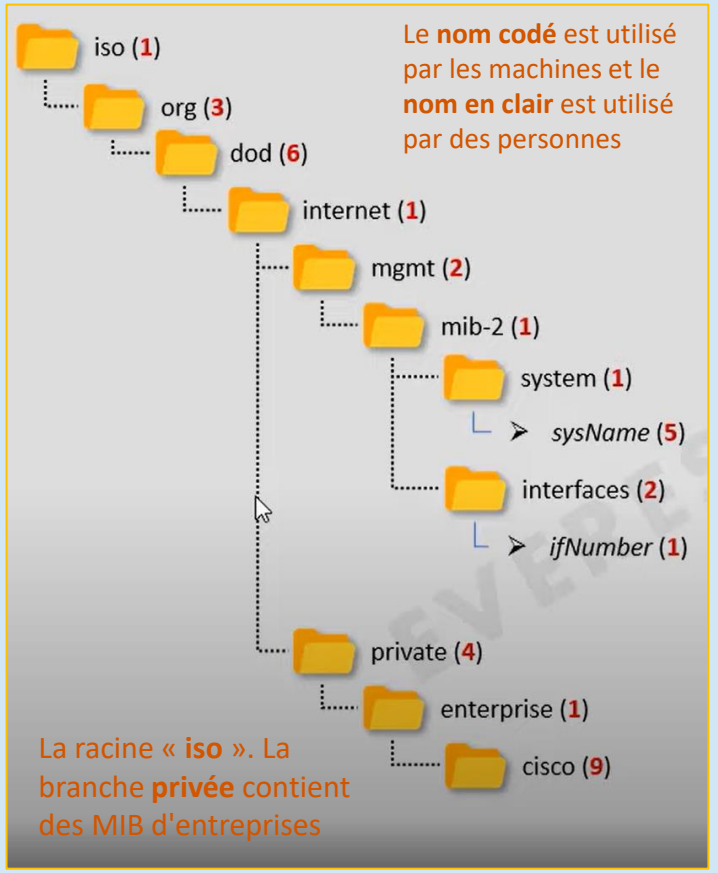
- Chaque équipement du réseau contient des informations de configuration, sur le matériel et les logiciels.
- Ces informations sont définis comme des **objets à gérer**.
- Exemples:
  - **Des machines** (serveur, postes clients), équipées d'un système d'exploitation: charge CPU, utilisation de mémoire, température, occupation des disques, type et version de l'OS, firmware, etc.
  - **Des équipements réseaux** (switch, routeurs, hub, etc.): état de chaque interface, vitesse, VLAN, bande passante, nombre de paquets, adresse IP, etc.
  - …., etc.

Modèle informationnel (MIB)

- **Problème**: l'identification d'un objet dépend du système.
  - Exemple: une interface réseau:
    - Sous **Linux** une interface **Ethernet** est nommée **eth0**.
    - Sous **IOS du Cisco** est nommée **ethernet 0/0**.
- **Comment organiser les objets?** Utiliser une base de données ou MIB (Management Information Base) sous la forme d'une arborescence.
- **Comment identifier d'une façons standards et non ambigu chaque objet?** Utiliser un OID (Object Identifier).

Modèle informationnel (MIB)

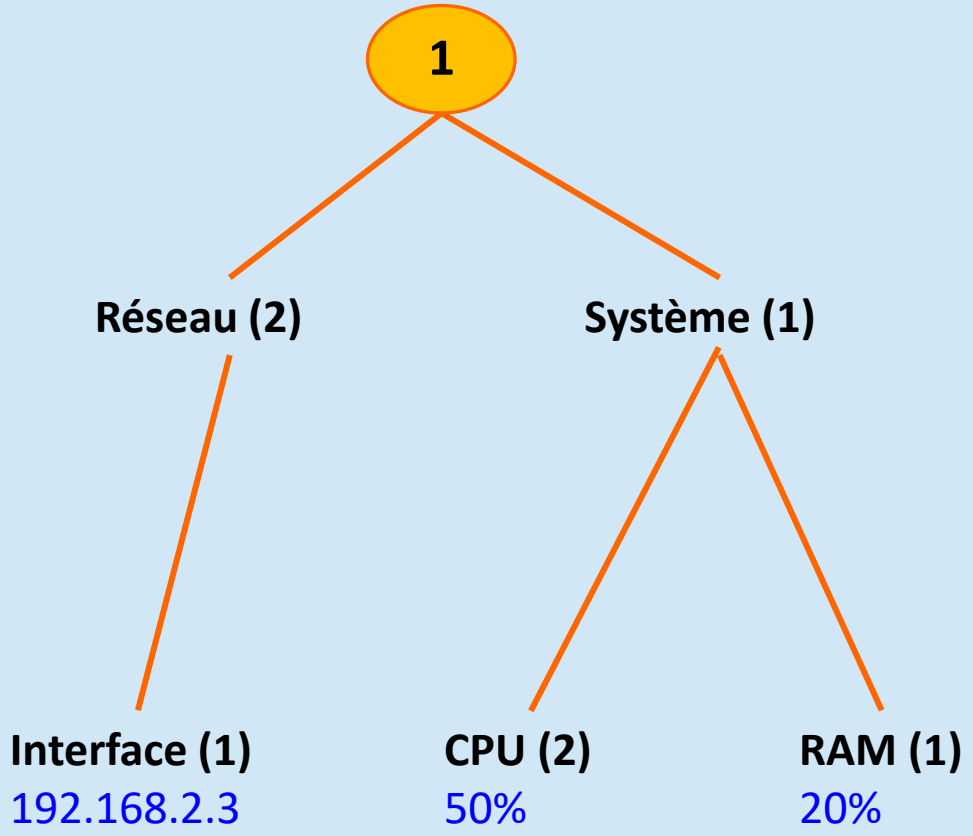
- **La MIB (Management Information Base) (ISO 10165) contient toutes les informations administratives sur les objets gérés.**
  - La structure de la MIB est hiérarchique: les objets sont regroupées en arbre.
  - Chaque objet a un identifiant (**OID, Object Identifiers**), une suite de chiffres séparés par des points, qui l'identifie de façon unique et un nom, décrivant sa position de la racine jusqu'à le nœud correspondant.
  - **Exemple** : « **1.3.6.1.2.1.1** » est l'OID qui est la chaîne de caractères décrivant le nombre d'interfaces réseau dans un équipement réseau (ifNumber).
  - Les feuilles représentent les objets gérés.
  - La plupart des matériels et des logiciels réseaux possèdent une MIB.



http://www.snmplink.org/OnLineMIB/Standards/

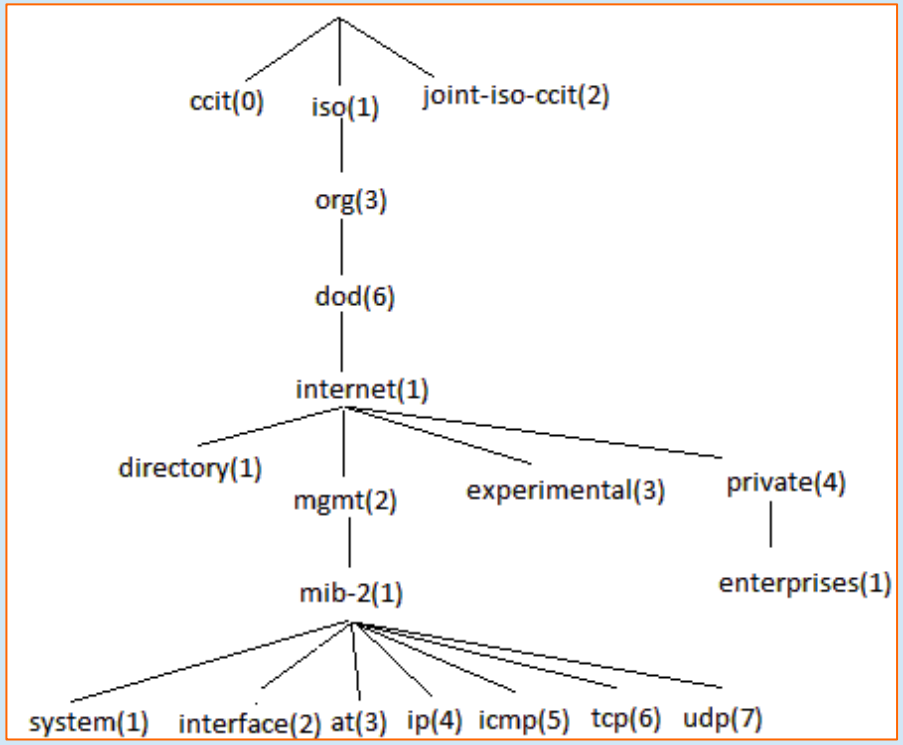
Modèle informationnel (MIB)

- **Exemple d'organisation de la MIB**
  - **Par exemple: une machine possède une interface réseau, un CPU est une mémoire.**
    - **Adresse de l'interface réseau:**
      - Identifiant (OID): **1.2.1**
      - Valeur: 192.168.2.3
    - **Charge de CPU:**
      - Identifiant (OID): **1.1.2**
      - Valeur: 50%
    - **Espace mémoire occupé:**
      - Identifiant (OID): **1.1.1**
      - Valeur: 20%



Modèle informationnel (MIB)

- **Contenu de la MIB:** les éléments de la MIB qui concerne la gestion du réseau sont:
  - **System:** Description des informations système.
  - **Interface**: Description des interfaces réseau.
  - **AT**: Table d'adresses IP pour les correspondances d'adresses MAC.
  - **IP**: Statistiques du protocole IP, adresse cache et table de routage.
  - **ICMP**: Statistiques du protocole ICMP.
  - **TCP**: paramètres TCP est statistiques.
  - **UDP**: Statistiques du protocole UDP.



Modèle informationnel (MIB)

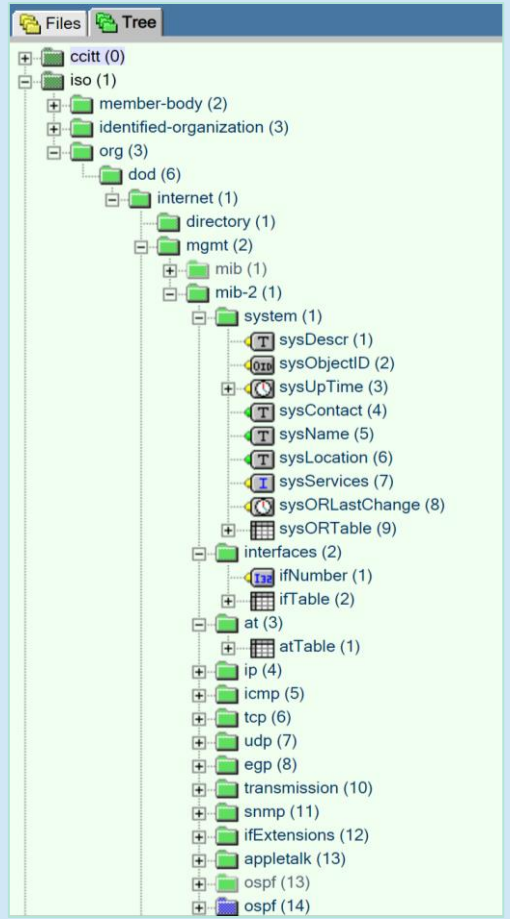
- Un fichier MIB est un document texte écrit en langage ASN.1 (Abstract Syntax Notation 1).
- Un objet est défini par Type (Syntax), mode d'accès (Access), état de définition (Status), description et un Identificateur unique, etc…
  - Syntax : il s'agit d'une chaîne de caractères de taille variant entre 0 et 255.
  - Accès : l'accès à cette variable se fait en lecture ou en écriture.
  - Etat : cette variable existe et est toujours utilisable.
  - Description : il s'agit du nom complet du nœud.
  - Sa place dans l'arborescence : 5ieme propriété de l'objet « system » : On en déduit que cette variable a pour clé la valeur **1.3.6.1.2.1.1.5**.

```
sysName OBJECT-TYPE
    SYNTAX DisplayString (SIZE (0..255))
    MAX-ACCESS read-write
    STATUS Mandatory
    DESCRIPTION   "An   administratively-
          assigned name for this managed
          node.  By  convention,  this  is
          the    node's    fully-qualified
          domain  name.  If  the  name  is
          unknown, the value is the zero-
          length string."
    ::= { system 5 }
```

Modèle informationnel (MIB)

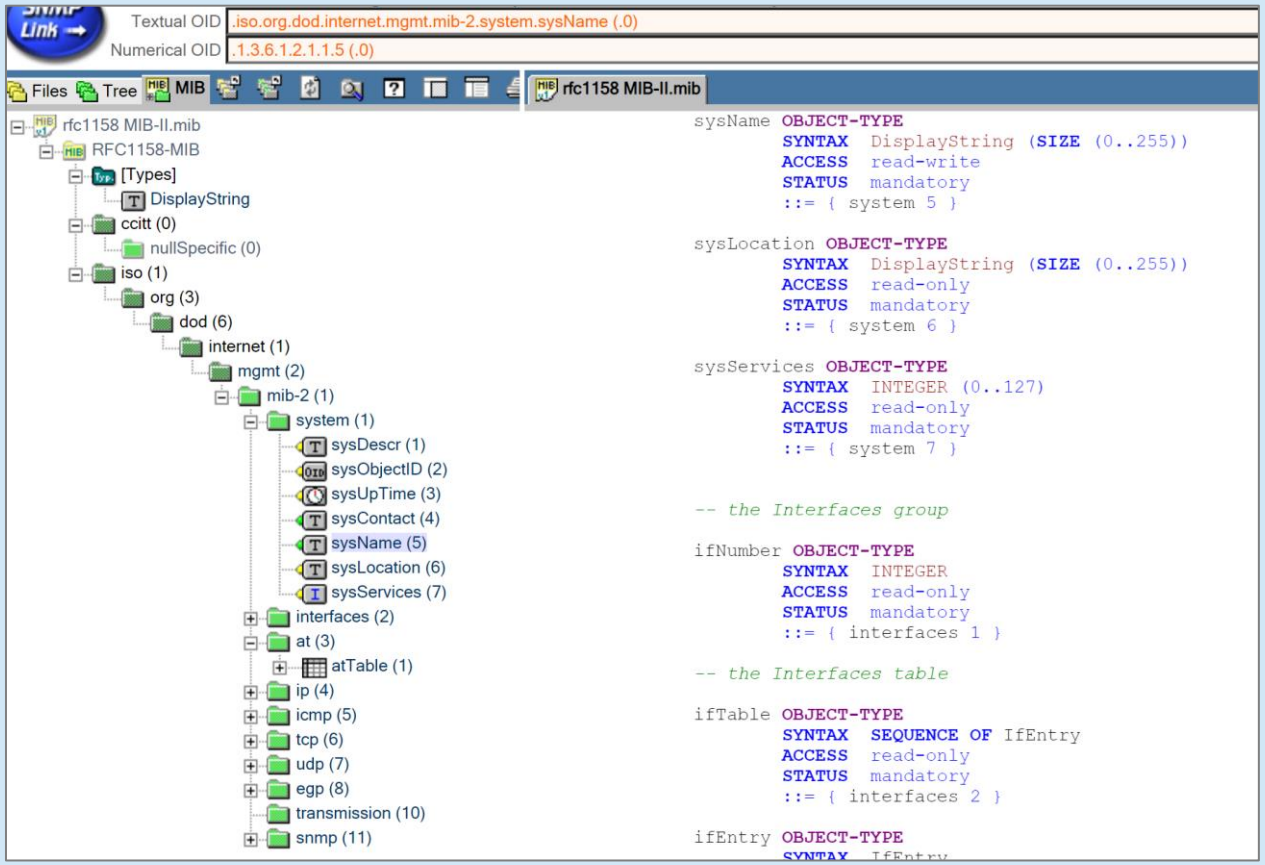
Versions du MIB

- **MIB 1**: une seule MIB spécifique au TCP/IP
- **MIB 2**: Plusieurs MIB (**RFC**), Chaque MIB est spécifique a un type de périphérique (+ 100 MIBs différentes, chacune pour un type d'équipement: routeurs, switch, serveurs, alimentation électrique, etc.
- Les MIBs maintenues par l'Internet Engineering Task Force (**IETF**)



Modèle informationnel (MIB)

Visualisation du MIB (http://www.snmplink.org/OnLineMIB/Standards/)



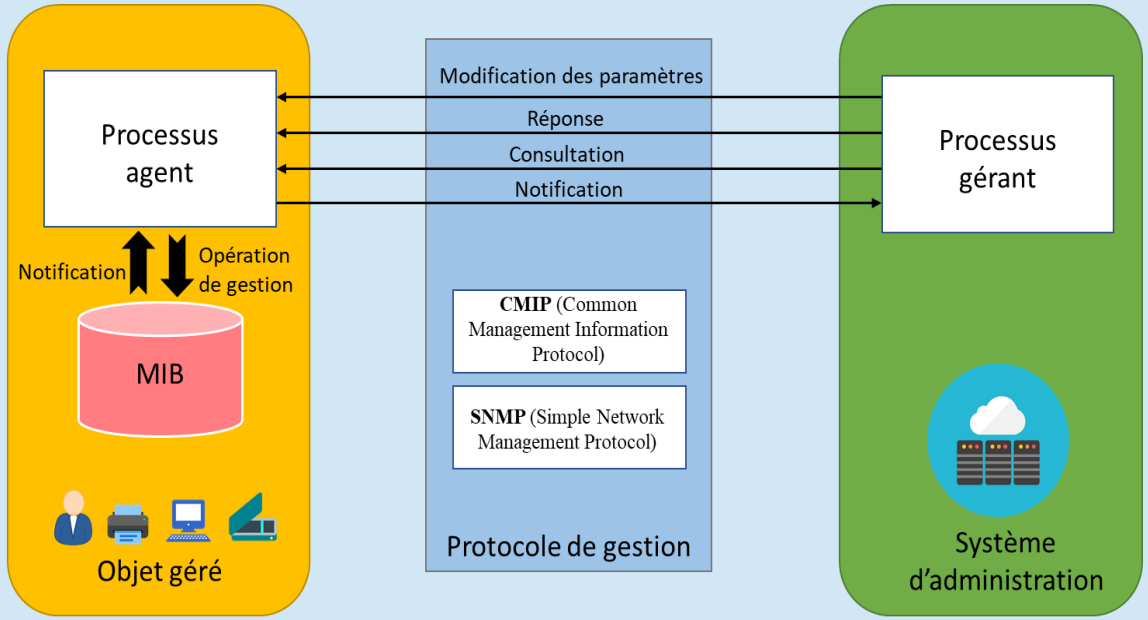
Modèle organisationnel

- Le modèle organisationnel, aussi appelé **modèle architectural** (**MSA** : **Managed System and Agents**),
  - C'est un modèle qui organise l'administration OSI,
  - Il définit la notion de systèmes administrés (**Agents**),
  - Il définit la notion du système Administrant (**Gérant**) (**DMAP**: Distributed Management Application Processus).

Modèle organisationnel

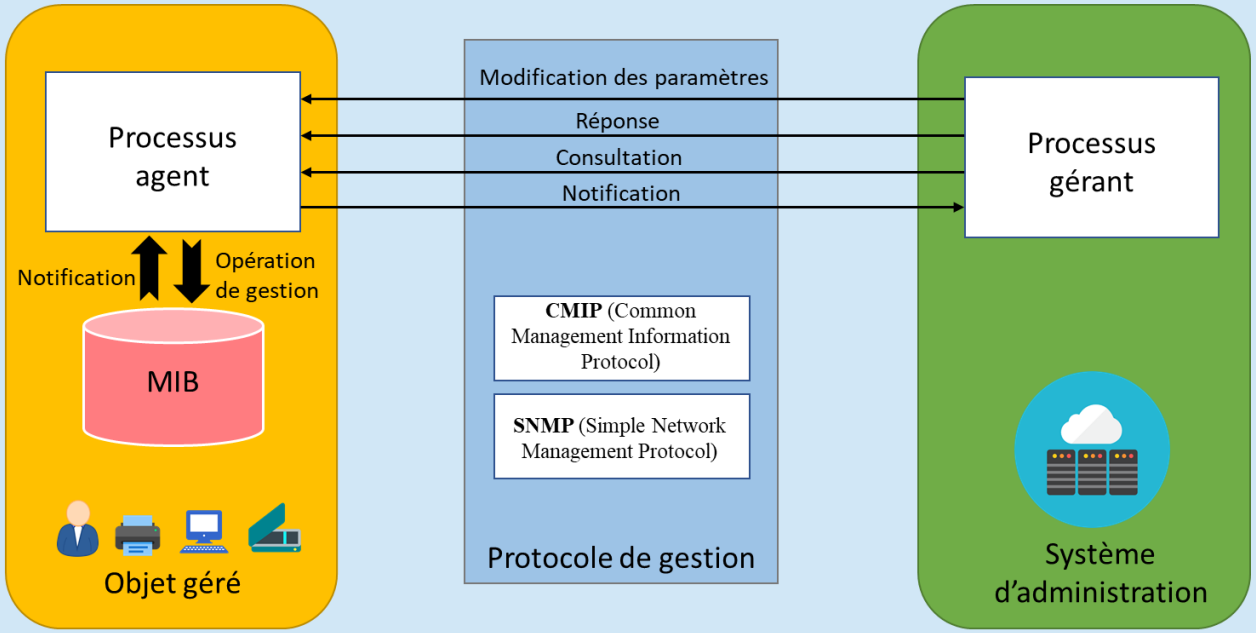
La gestion du système (System Management)

- **Modèle Gérant/Agent (ou Manager/Agent)** : 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 concernent le **système d'administration (gérant).**
- **Principe**: repose sur les échanges entre la MIB et l'ensemble des éléments administrés (objets) et entre les éléments administrés (objets) et le système d'administration.



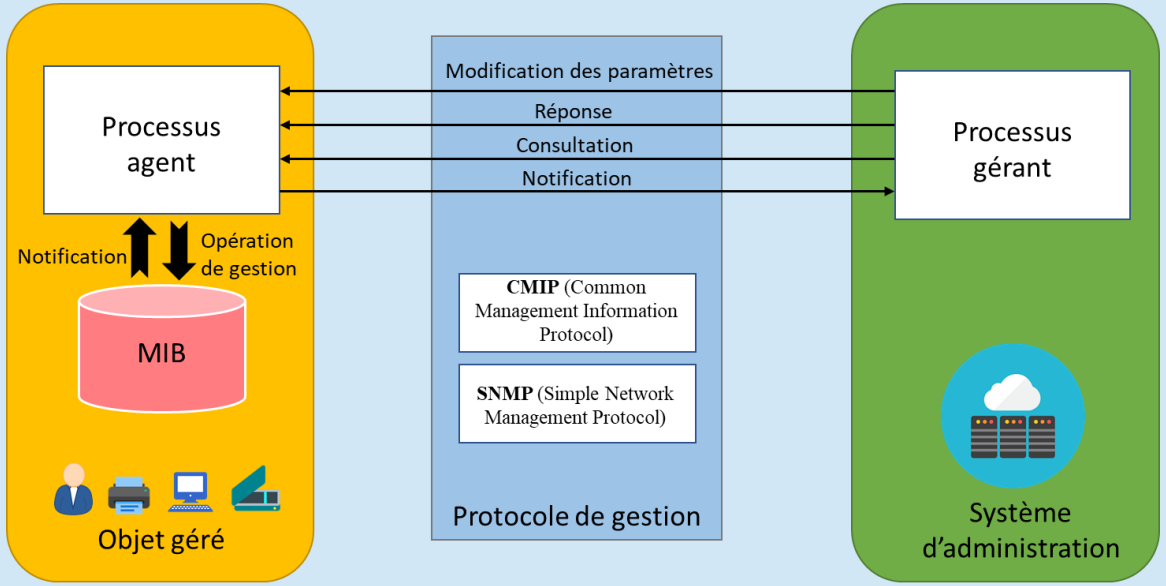
Modèle organisationnel

- La gestion du système (System Management)
  - **Agent:** est un programme exécuté sur un équipement que l'on veut administrer et qui a accès directement aux parties matérielles et logicielles de cet équipement.
  - Il est **interrogé à distance** et fournit les informations ou exécute les instructions demandées avec une certaine possibilité de raisonnement et de communication.



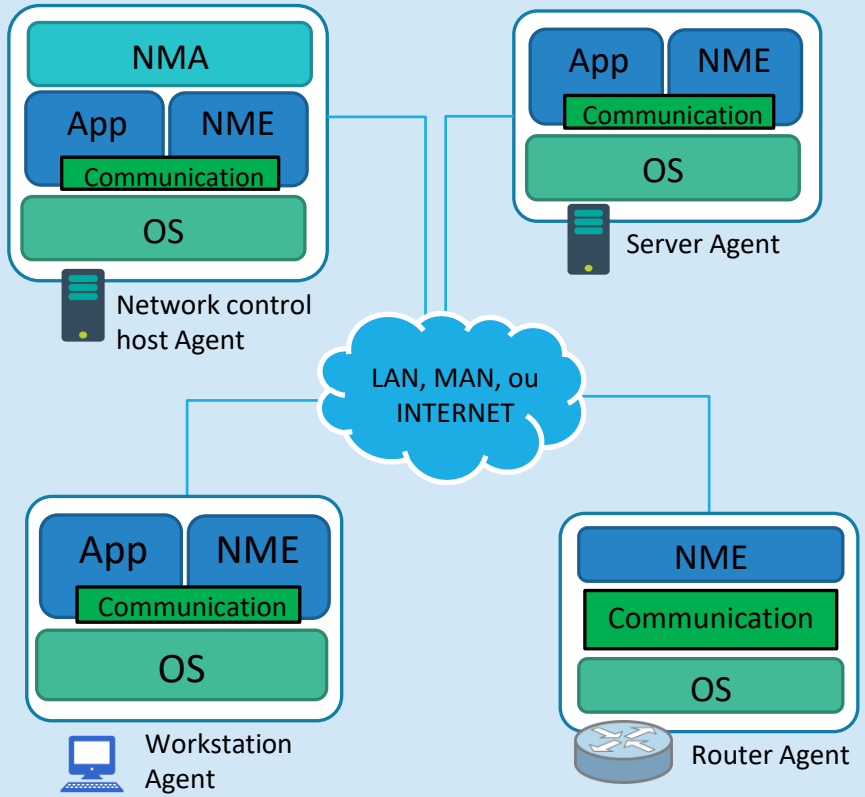
Modèle organisationnel

- La gestion du système (System Management)
  - **Gérant:** un processus qui peut accéder aux informations de gestion de la MIB (Management Information Base) locale via un protocole d'administration comme **SNMP** ou **CMIP**, qui le met en relation avec les divers agents.
  - La **MIB** contient toutes les informations administratives sur les objets gérés. Seul le processus agent a accès à la MIB et le processus manager accède aux données via le processus agent.



Modèle organisationnel

- Système d'administration NMS (Network Management System) à base des agents
  - Le système est composé d'une entité d'administration (**NMA**) et des entités de gestion (**NME**) qui sont géré par cette entité et un protocole pour la gestion comme **CMIP** ou **SNMP**.
    - **NMA:** Network Management Application.
    - **NME**: Network Management Entity.
  - Les équipements réseaux gérés (objets) contiennent les agents ou **NME**, et les équipements administrateurs contiennent l'application **NMA**.
  - **NMA (console d'administration)** contient une interface permettant à l'administrateur du réseau d'effectuer des opérations de gestion du réseau à distance



Protocoles d'administration

Protocole spécifique à l'administration réseau:

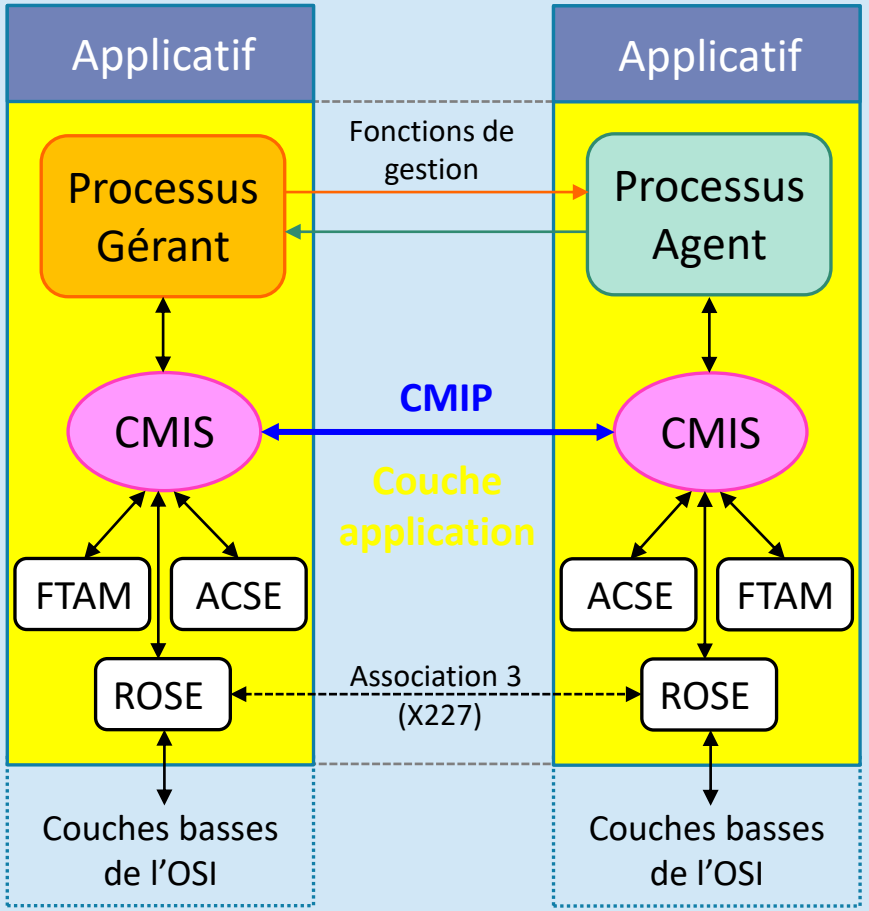
- Le protocole CMIP (Common Management Information Protocol) (**ISO**)
- Le proto SNMP (Simple Network Management Protocol) (**IETF**)
- NETCONF (Network configuration protocol) (**IETF**)
- SYSLOG (System Logging Protocol)
- WEBEM (Web-Based Enterprise Management)

Protocole CMIP

- **CMIP/CMIS** « Common Management Information Protocol/Common Management Information Service » est le modèle de gestion des réseaux de **l'OSI**.
- Défini dans la recommandation UIT-T X.711, et la norme internationale **ISO/CEI 9596-1**
- Il fournit une implémentation pour les services définis par le service commun d'information de gestion (CMIS).
- Le CMIP utilise les primitives de service CMIS suivantes :
  - **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.

Protocole CMIP

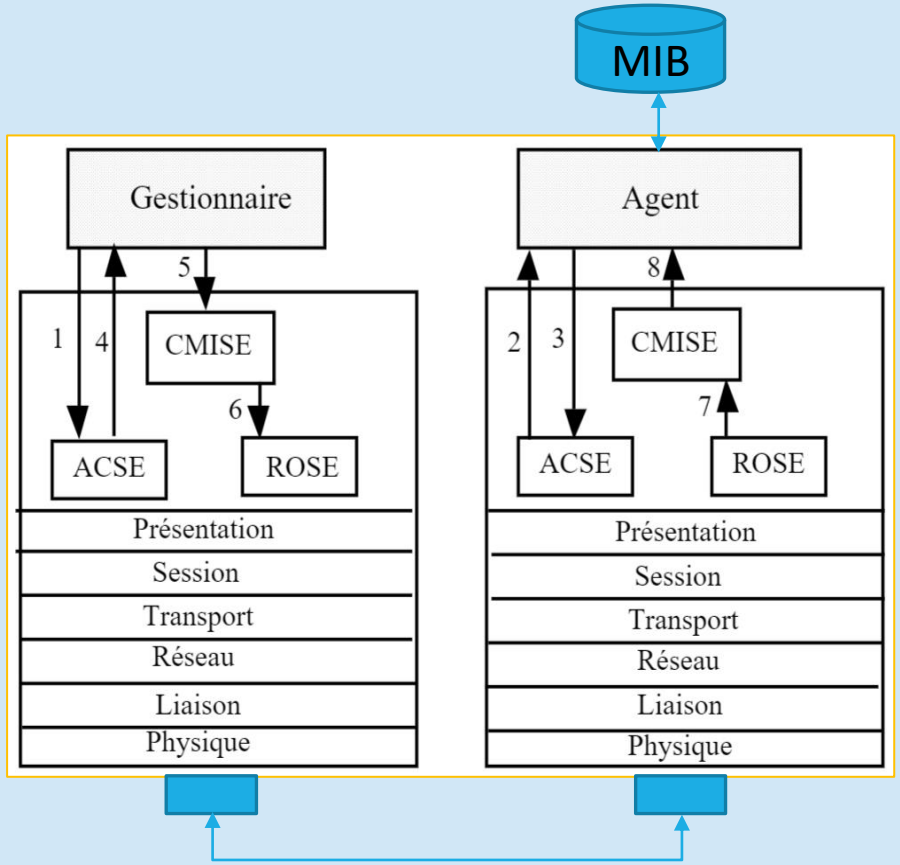
- CMIP est implémenté en association avec les protocoles ACSE et ROSE.
  - ACSE: Association Control Service Element
  - ROSE: Remote Operation Service Element
- ACSE est utilisé pour gérer les connexions entre les applications de gestion (**agents CMIP**). ACSE vérifie les identités des entités d'application, et pourrait appliquer un contrôle de sécurité et d'authentification.
- ROSE est utilisé pour toutes les interactions d'échange de données.
- **FTAM** (File Transfer Access and Management) est une application de transfert de fichier fiable référencée sous la norme **ISO 8571**.



Protocole CMIP

Exemple illustratif: considérons qu'un gestionnaire désire connaître auprès d'un agent l'état opérationnel d'un commutateur **ATM**.

- Il s'agira donc de lire la valeur de l'attribut état opérationnel de l'objet commutateur dans la MIB de l'agent.
- Le gestionnaire commence par établir une connexion avec l'agent en invoquant le service offert par **ACSE**.
  Etapes: **1**, **2**, **3** et **4**.
- Une fois l'association établie, le gestionnaire utilise le service offert par **CMIS** afin d'émettre une requête de lecture de l'objet et de recevoir la réponse. Etapes: **5**, **8**.
- **ROSE**, dont les services sont utilisés par CMISE, supporte l'émission de la requête et l'envoi de la réponse. Etapes **6**, **7**



Protocole CMIP

Avantages:

- Implémente des solutions de sécurité tels que le contrôle d'accès et l'authentification
- Plus riche: envoi et recevoir **11** types de PDU (Data Protocol Unit).
- Un protocole d'administration de réseau complet.

Inconvénients:

- Moins repandus et a du mal à s'implémenter dans un environnement TCP/IP (CMIP est basé sur le modèle OSI)
- Utilise 10 fois plus de ressources que SNMP et donc supporté par beaucoup moins de réseaux que SNMP.

Chapitre 2. Protocole SNMP

- **Protocole SNMP :**
  - **Présentation et Historique du SNMP**
  - **Les principes,**
  - **Configuration,**
  - **Avantages et Inconvénients**

Protocole SNMP: Présentation

- SNMP (Simple Network Management Protocol) est un protocole de gestion de réseaux proposé par **l'IETF (Internet Engineering Task Force)** dans les années 1980 et a évolué en plusieurs versions.
  - **SNMPv1**: la première version de SNMP, a été publiée en **mai 1990** dans RFC 1155 et RFC 1157.
  - **SNMPv2**: la version révisée avec quelques extensions (**Get BLUK**: plusieurs Get dans un seul message) a été publiée en **avril 1993** . Elle est défini dans RFC 1901, RFC 1905 et RFC 1906.
  - **SNMPv3:** Facilite la configuration à distance des entités SNMP. Elle ajoute également à la fois le cryptage et l'authentification, ce qui en fait la version **la plus sécurisée** à ce jour. Cette version est défini par RFC 1905, RFC 1906, RFC 2571, RFC 2572, RFC 2574 et RFC 2575 (**janvier 1998**).
- Il est actuellement le protocole le plus utilisé pour la gestion et la surveillance des équipements de réseaux dans des réseaux hétérogènes complexes.
- Il est supporté par la quasi-totalité des terminaux.

Protocole SNMP: Présentation

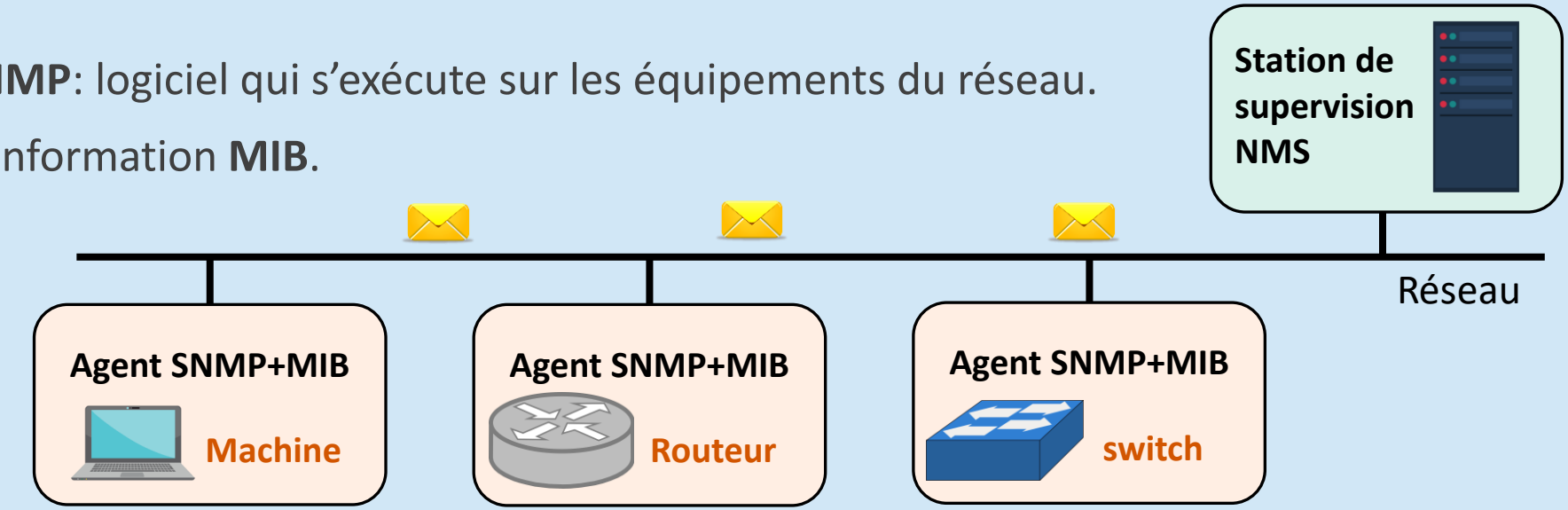
- SNMP est un protocole de la famille TCP/IP (Internet Protocol), et peut donc être utilisé sur tous les réseaux de type Internet.
- Il exploite les capacités du protocole de transport **UDP** (User Datagram Protocol),
- Deux ports sont désignés pour l'utilisation de SNMP :
  - **Port 161** pour les requêtes à un agent SNMP.
  - **Port 162** pour l'écoute des alarmes (**Trapes**) destinées à la station d'administration.

Process	Protocol	Port Number
Request receipt by the agent	UDP	161
Manager's communication with the agent	UDP	161
Notification receipt by the manager	UDP	162
Agent's notification generation		Any available port
Request receipt	TLS/DTLS	10161
Notification receipt	TLS/DTLS	10162

Protocole SNMP: Principes

L'environnement de gestion SNMP est constitué de plusieurs composantes :

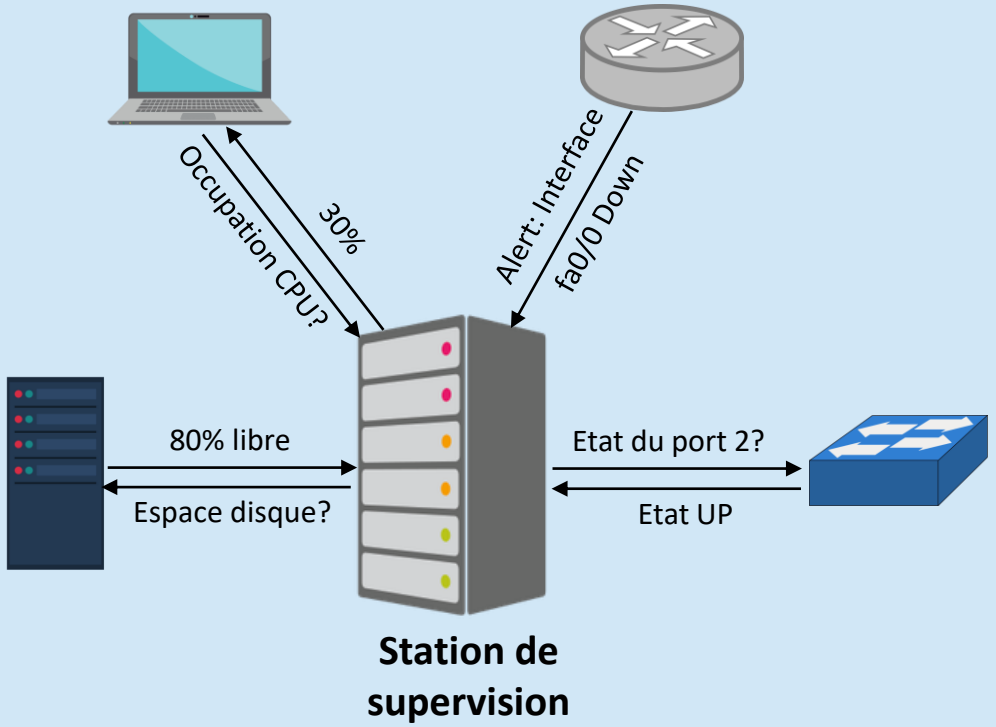
- Une station de gestion de réseau (**NMS-Network Management Stations**): c'est la console de supervision qui permet d'interroger les agents (requêtes SNMP).
- Des éléments de réseaux à superviser (**NE : Network Elements**): routeur, switch, firewall serveur, etc.
- **Un agent SNMP**: logiciel qui s'exécute sur les équipements du réseau.
- Une base d'information **MIB**.



Protocole SNMP: Principes

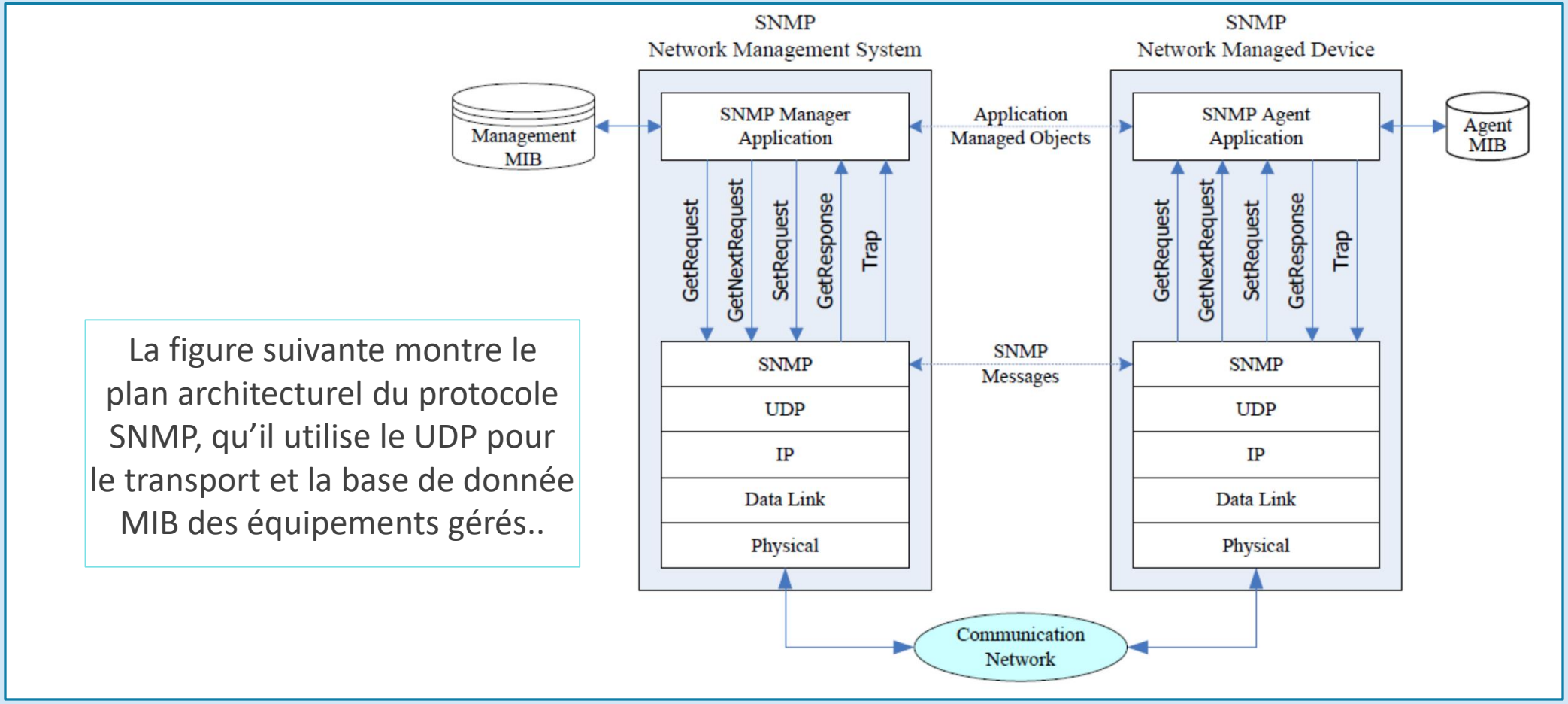
Rôle d'un agent SNMP

- **Un agent SNMP**: est une fonction logicielle intégrée à la plupart des équipements de réseau: routeur, switch, firewall serveur, etc.
- Il est responsable du **traitement des requêtes SNMP** provenant de la station de supervision.
- L'agent envoi des **alertes (Trapes)** à la station de supervision, en cas d'un problème au niveau d'un équipement de réseau (sur le port UDP 162).
- L'agent doit être configuré pour envoyer les Trapes à la station de supervision.



Protocole SNMP: Principes

La figure suivante montre le plan architecturel du protocole SNMP, qu'il utilise le UDP pour le transport et la base de donnée MIB des équipements gérés..



Protocole SNMP: Commandes

Commandes SNMP: SNMP est un protocole de type requête/réponse:

- Get: demande d'une information à l'agent (la valeur correspondant à l'information demandée).
- Getnext: demander l'information suivante à l'agent. On utilise cette commande, à la suite d'une requête Get, afin d'obtenir directement le contenu de la variable suivante.
- Getbulk: pour connaître la valeur de plusieurs variables : cela évite d'effectuer plusieurs requêtes Get en série, améliorant les performances (implémenté dans SNMPv2).
- Set: permet de définir la valeur d'une variable de l'agent administré. Cela permet d'effectuer des modifications sur le matériel/logiciel.
- Trap: Lorsqu'un événement survient chez l'agent, celui-ci envoi une Trap (un message d'information à la station d'administration : celle-ci pourra alors la traiter et agir en conséquence. S'il s'agit par exemple de la coupure d'un lien réseau, cela permet à l'administrateur réseau d'en être immédiatement informé.
- Inform: Parfois, il peut être intéressant pour l'agent d'obtenir une réponse à une Trap qu'il a émise, afin d'obtenir confirmation que celle-ci a bien été reçue et analysée : c'est l'objectif de la commande Inform. Elle est implémentée dans SNMPv2.

Protocole SNMP: Commandes

Lorsqu'une commande est expédiée à un agent, on attend de celui-ci une réponse. Plusieurs cas peuvent se produire :

- Aucune réponse (Temps d'attente dépassé),
- Erreur dans la requête,
- La requête a réussi.

Protocole SNMP: Commandes

Cas d'aucune réponse (Temps d'attente dépassé): plusieurs cas sont susceptibles de produire une absence de réponse de la part du matériel interrogé :

- SNMP est basé sur UDP et il peut arriver que les paquets n'arrivent pas à destination. Dans ce cas, le temps d'attente de réponse finit par s'écouler et il convient alors de réémettre la requête.
- Si l'authentification échoue (mauvaise communauté, mot de passe incorrect), l'agent peut ne pas répondre à la requête.
- Le temps d'attente de réponse peut être paramétré dynamiquement et il est possible que le temps défini soit trop court pour permettre à la réponse de revenir.
- Enfin, dans le pire des cas, il est possible qu'il n'y ait pas d'agent SNMP disponible sur le matériel interrogé. Nous ne pouvons en conséquence avoir de réponse à notre requête

Protocole SNMP: Commandes

Cas d'erreur dans la requête: plusieurs cas sont susceptibles de conduire au renvoi d'une erreur :

- Lorsqu'on l'on essaie d'écrire sur une variable en lecture seule
- Lorsque l'on essaie de définir la valeur d'une variable avec un type de données incorrect (si l'on essaie d'écrire une chaîne de caractères dans une variable de type entier par exemple).
- Lorsque la variable n'existe pas.
- Lorsque la trame SNMP est incorrecte (corruption, longueur non valide…).
- Lorsque l'authentification SNMPv3 a échoué.

Cas de réussite: lorsque la requête à l'agent SNMP réussit, celui-ci nous envoie la valeur de la variable à laquelle on a accédé (que ce soit en lecture ou en écriture).

Exemples de transactions SNMP

- **Exemple 1:** Nous voulons connaître le nom, le temps de fonctionnement et d'autres informations sur les interfaces d'un routeur. Nous considérerons que la communauté d'accès est « **TdS** » et que l'adresse de ce routeur est « **172.17.67.253** ». Nous effectuons une requête de type **Get** sur le routeur comme suit:

```
$ snmpget -c TdS 172.17.67.253 .1.3.6.1.2.1.1.5
system.sysName = router-exemple
$
```

- **Exemple 2:** Il est nécessaire, pour parcourir toute la branche, d'effectuer une requête de type «**walk**», qui constitue en fait une série de requêtes **Get** et **5**. On obtient ainsi la liste de toutes les variables de la branche :

```
$ snmpwalk -c TdS 172.17.67.253 .1.3.6.1.2.1.1
system.sysDescr = Cisco Internetwork Operating System Software
system.sysObjectID = OID: enterprises.9.1.172
system.sysUpTime = Timeticks: (9360890) 1 day, 2:00:08.90
system.sysContact = KindMan@fleming.u-psud.fr
system.sysName = router-exemple
system.sysLocation = Résidence Fleming
system.sysServices = 78
$
```

Exemples de transactions SNMP

- **Exemple 3:** Essayons par exemple de modifier la description de l'endroit où le matériel se trouve (system.sysLocation, .1.3.6.1.2.1.1.6). Cela se fait par le biais de la commande **snmpset**. Il est également nécessaire de lui fournir le type de données utilisé (ici « s » pour « string, chaîne de caractères ») :

```
$ snmpset -c TdS 172.17.67.253 .1.3.6.1.2.1.1.6 s "chez moi"
system.sysLocation = chez moi
$
```

- Nous pouvons vérifier que la commande a bien été prise en compte:

```
$ snmpget -c TdS 172.17.67.253 .1.3.6.1.2.1.1.6
system.sysLocation = chez moi
$
```

- **Exemple 4:** La MIB standard fournit des informations sur l'état des interfaces réseaux du matériel interrogé. L'OID « set iso.org.dod.internet.mgmt.mib2.interfaces.ifNumber » nous permet de connaître le nombre d'interfaces.

```
$ snmpget -c TdS 172.17.67.253 .1.3.6.1.2.1.2.1.0
interfaces.ifNumber.0 = 4
```

Exemples de transactions SNMP

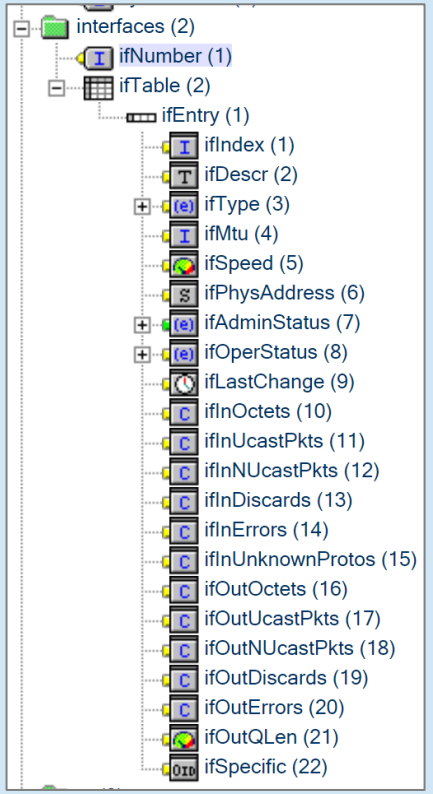
- **Exemple 4:** Les interfaces sont alors regroupées dans un tableau « .interfaces.ifTable » contenant la liste des propriétés de chaque interface. Si nous désirons par exemple **connaître le type des interfaces**, il nous faudra interroger l'OID « interfaces.ifTable.ifEntry.ifType » :

```
$ snmpwalk -c TdS 172.17.67.253 .1.3.6.1.2.1.2.2.1.3
interfaces.ifTable.ifEntry.ifType.1 = ethernetCsmacd(6)
interfaces.ifTable.ifEntry.ifType.2 = ethernetCsmacd(6)
interfaces.ifTable.ifEntry.ifType.3 = propPointToPointSerial(22)
interfaces.ifTable.ifEntry.ifType.4 = other(1)
```

  - Le tableau est indexé de 1 à 4.
  - Les interfaces n°1 et n°2 sont de types « ethernet ».
  - L'interface n°3 est de type « pppSerial »
  - L'interface n°4 est de type inconnue (ou de type défini par le constructeur).

- Nous pouvons connaître l'état de chacune des interfaces en interrogeant la propriété ifOperStatus (état courant de l'interface, ix=8) de l'objet ifEntry :

```
$ snmpwalk -c TdS 172.17.67.253 .1.3.6.1.2.1.2.2.1.8
interfaces.ifTable.ifEntry.ifOperStatus.1 = up(1)
interfaces.ifTable.ifEntry.ifOperStatus.2 = up(1)
interfaces.ifTable.ifEntry.ifOperStatus.3 = down(2)
interfaces.ifTable.ifEntry.ifOperStatus.4 = up(1)
```



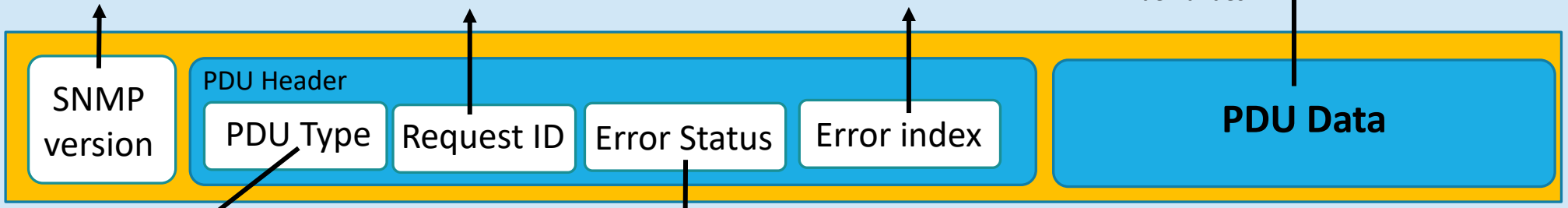
Trame SNMP

Version SNMP: utiliser pour envoyer le paquet vers le bon module de décodage

Le « **Request ID** » permet à la station de gestion d'associer les réponses à ses requêtes.

Le **Error Index** indique, en cas d'erreur, ou celle-ci se situe dans la requête.

Information utiles: les valeurs demandées ou les réponses à des demandes



Le **type de PDU** décrit le type de requête, de réponse ou d'alerte.

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

Le « **Error Status** » est l'indicateur du type d'erreur. Si aucune erreur ne s'est produite, le champ Error index est mis à zéro (0).

Community : C'est le contrôle d'accès utilisée par SNMP. Pour les version SNMPv1 et SNMPv2, la communauté est transportée en clair sur le réseau, ce qui pose de gros problèmes de sécurité.

```
⊞ Frame 2 (120 bytes on wire, 120 bytes captured)
⊞ Ethernet II, Src: Cisco_3e:e3:c0 (00:12:80:3e:e3:c0), Dst: 00:00:00_00:00:
⊞ Internet Protocol, Src: 172.16.30.254 (172.16.30.254), Dst: 192.168.101.2
⊟ User Datagram Protocol, Src Port: snmp (161), Dst Port: 3187 (3187)
    Source port: snmp (161)
    Destination port: 3187 (3187)
    Length: 86
    Checksum: 0xb712 [correct]
⊟ Simple Network Management Protocol
    Version: 1 (0)
    Community: public
    PDU type: RESPONSE (2)
    Request Id: 0x00000025
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.4.1.9.2.1.58.0 (SNMPv2-SMI::enterprises.9.2
    Value: INTEGER: 16
    Object identifier 2: 1.3.6.1.4.1.9.2.1.57.0 (SNMPv2-SMI::enterprises.9.2
    Value: INTEGER: 16
    Object identifier 3: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
    Value: Timeticks: (11915034) 1 day, 9:05:50.34
```

Protocole SNMP

Avantages

- SNMP est très simple comme son nom l'indique
- Largement rependu sur le marché
- N'alourdit pas le système et fonctionne même si le réseau subit à des graves problèmes
- Facilement extensible

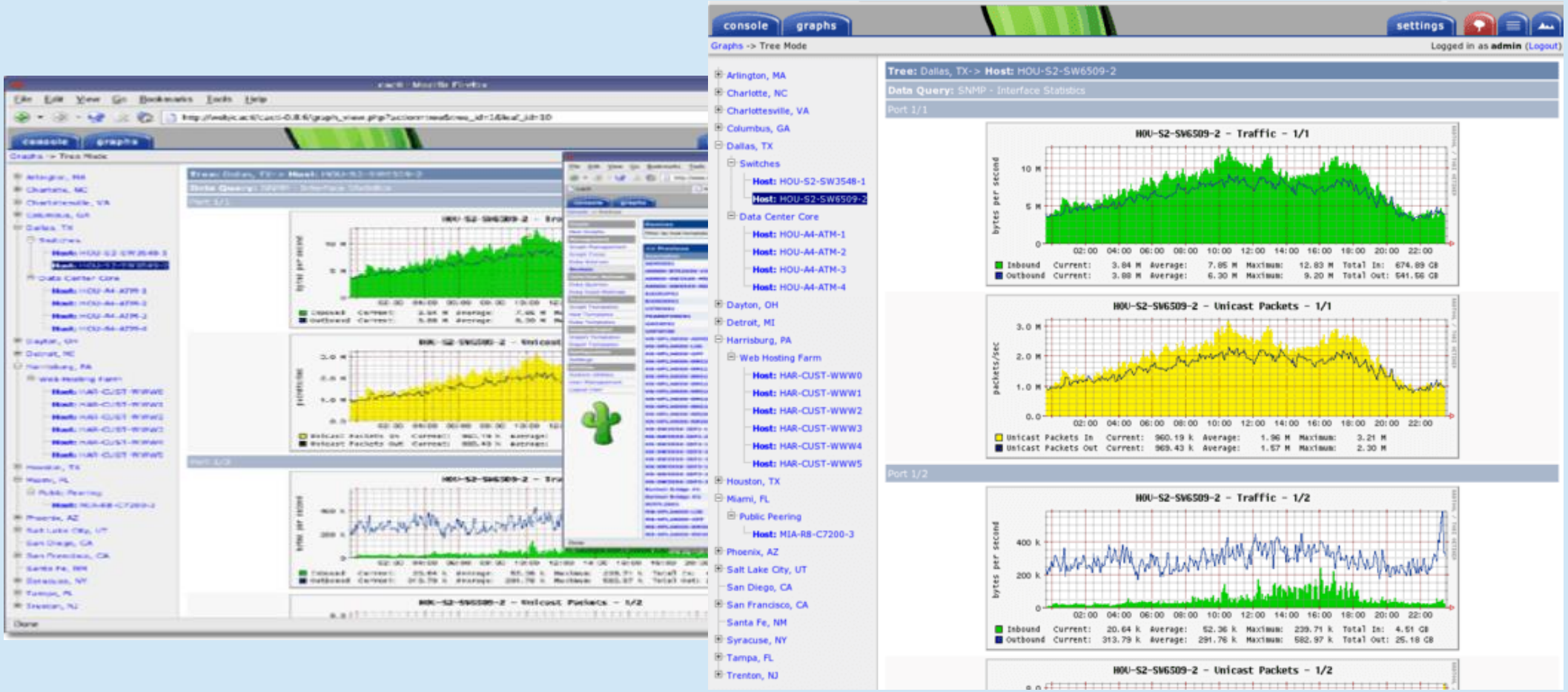
Inconvénients

- Envoi et recevoir uniquement 5 types de PDU (11 PDU pour CMIP)
- Une des plus grandes faiblesses du protocole SNMP est l'absence d'un mécanisme adéquate de sécurité évident qui subsiste sur les premières versions de SNMP (v1 et v2). C'est dans ce but qu'a donc été développée la dernière version (v3) de SNMP. Depuis 2002 celle-ci a été décrétée comme standard pour ce protocole. Pourtant la version 1 reste encore beaucoup utilisée et peu d'entreprises évoluent en passant en sur la dernière version..

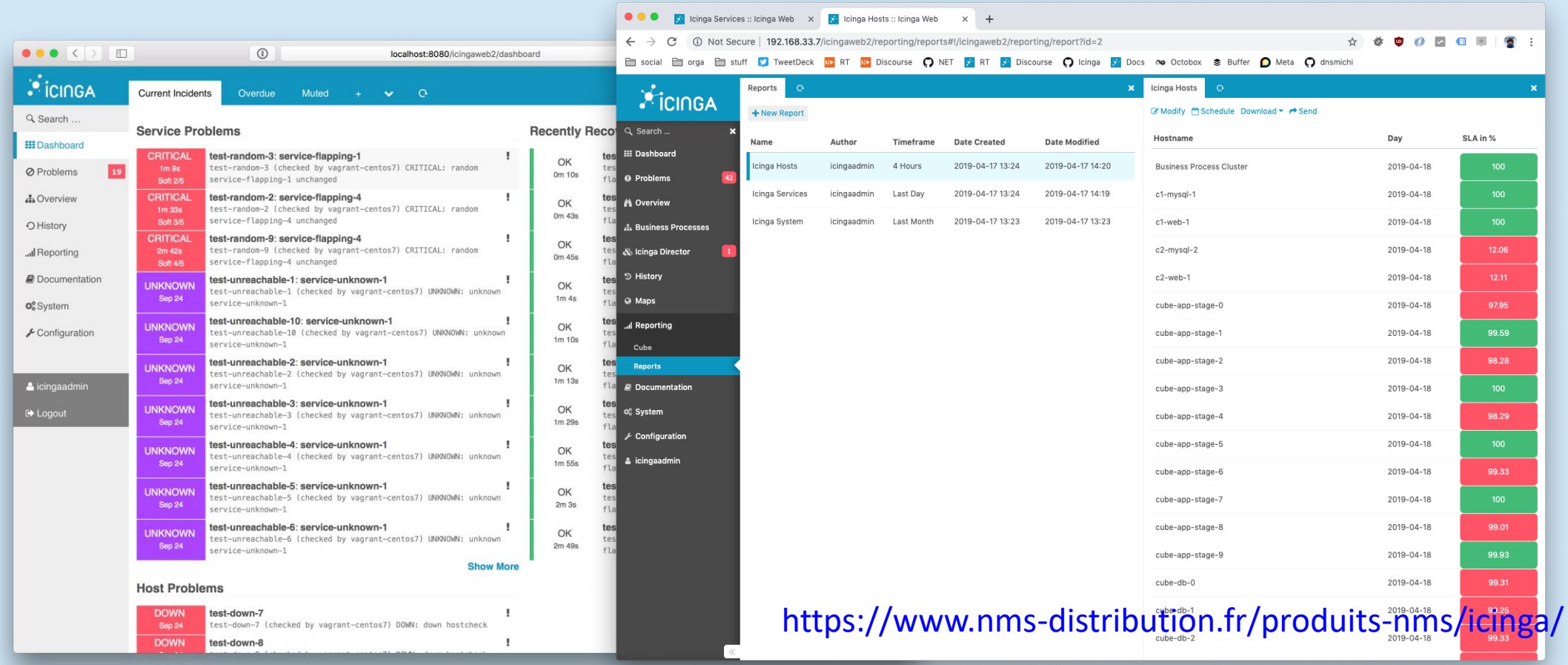
Logiciels de supervision: NAGIOS

Lien: https://www.nagios.com/products/nagios-xi/#features

Logiciels de supervision: CACTII

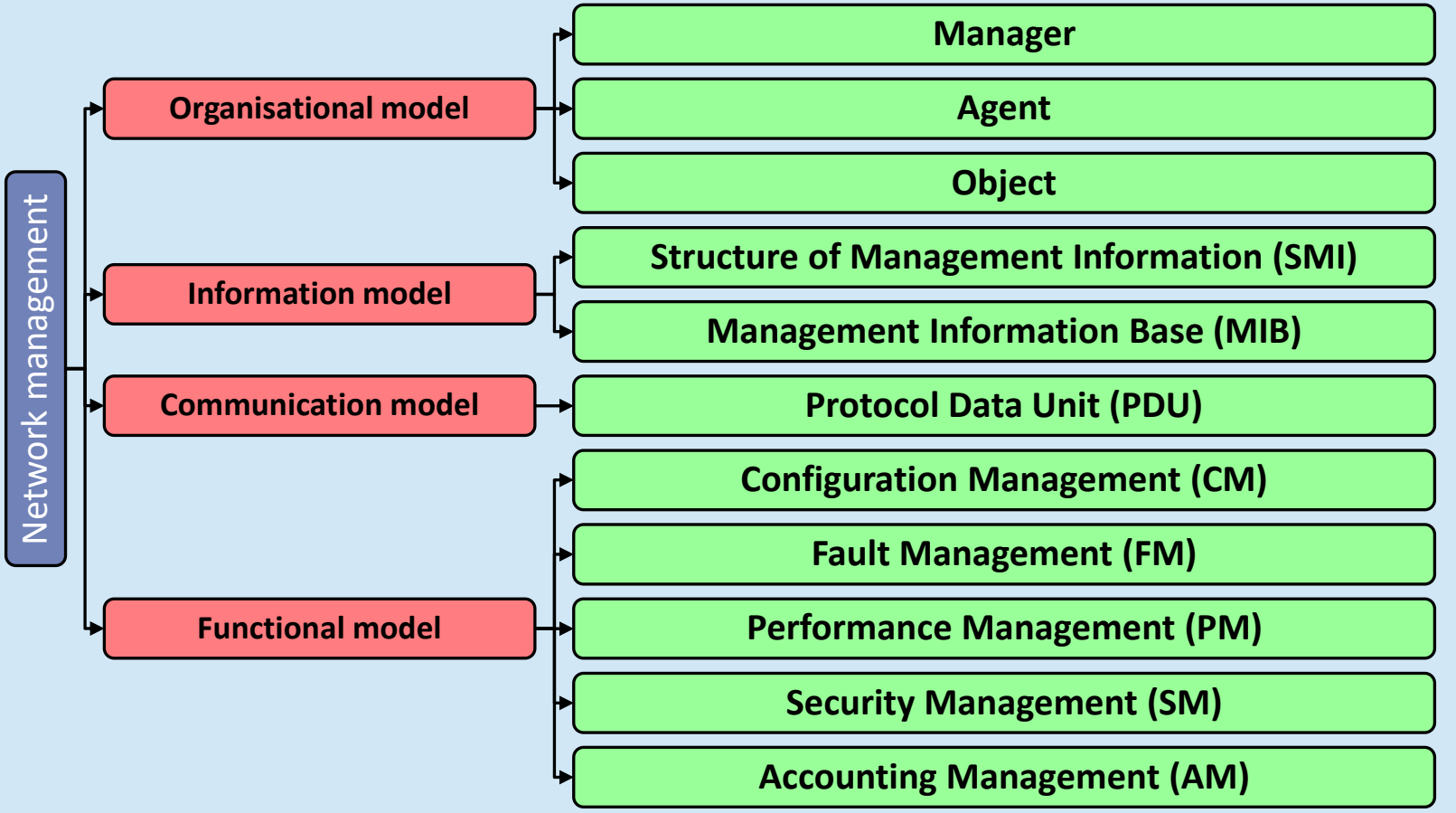


Logiciels de supervision: ICINGA



https://www.nms-distribution.fr/produits-nms/icinga/

Conclusion


Network management
Organisational model
Information model
Communication model
Functional model
Manager
Agent
Object
Structure of Management Information (SMI)
Management Information Base (MIB)
Protocol Data Unit (PDU)
Configuration Management (CM)
Fault Management (FM)
Performance Management (PM)
Security Management (SM)
Accounting Management (AM)