Chapitre 1 : Rappel et Notion

Couche du modèle OSI :

7	Application	Accès aux services
6	Présentation	Gestion de la syntaxe des données
5	Session	Contrôle le dialogue entre les applications
4	Transport	Qualité de la transmission de bout en bout
3	Réseau	Sélection du chemin & adressage logique
2	Liaison de données	Adressage physique (Adresse MAC)
1	Physique	Transmission sur le support physique

Couche du modèle TCP/IP :

C'est un modèle de 4 couches :

4	Application	Couches 5 à 7 du modèle OSI
3	Transport	Qualité de la transmission
2	Internet	Sélection du chemin (routage)
1	Accès Réseau	Couches 1 & 2 du modèle OSI

OSI / TCP IP :

7	Application		Application	4
6	Présentation			
5	Session			
4	Transport		Transport	3
3	Réseau		Internet	2
2	Liaison de données		Accès Réseau	1
1	Physique			

Les Points Communs et Différence entre ces deux modèles :

Points communs

- Modèles en couches
- Couche Application similaire mais avec des services différents

Différences

- Le modèle OSI est utilisé comme un modèle de référence
- La pile protocolaire TCP/IP est plus couramment utilisée

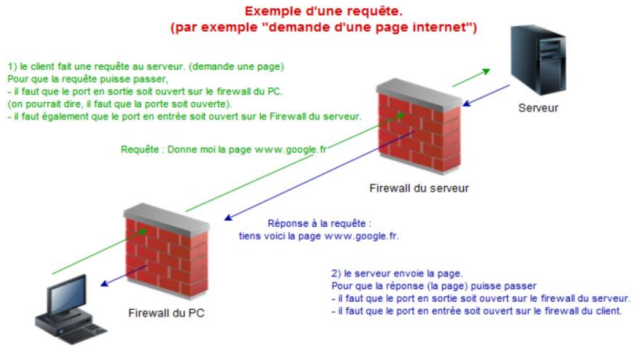
Les PDUS 5 Protocole Data Unit :

7	Application	Donnée
6	Présentation	
5	Session	
4	Transport	Segment
3	Réseau	Paquet
2	Liaison de données	Trame
1	Physique	Bit

Architecture Client Serveur :

- ✓ Le client initie l'échange
- ✓ Le serveur est à l'écoute d'une requête cliente éventuelle
- ✓ Le service rendu = traitement effectué par le serveur

Notion des ports :



⇨ L'unicité de la communication est assurée grâce à une SOCKET, (adresse IP + Numéro de port).

Numéros codés sur 16 bits :

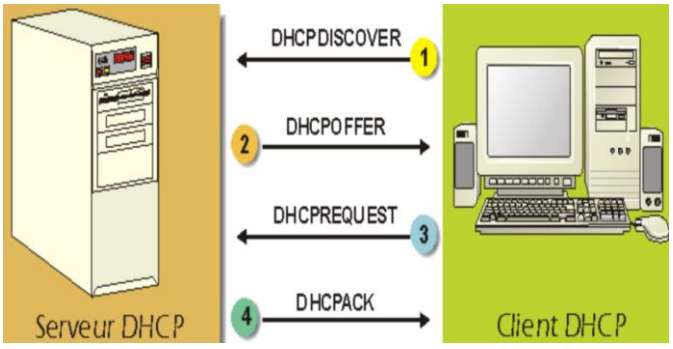
1ère plage : 0 – 1023 PORTS CONNUS

2ème plage : 1024- 49151 PORTS ENREGISTRES

3ème plage : 49152-65535 PORTS DYNAMIQUES/PRIVES

PROTOCOLE DHCP :

DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau).



DHCPDISCOVER :(pour localiser les serveurs DHCP disponibles)

DHCPOFFER : (réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres)

DHCPREQUEST : (requête diverse du client pour par exemple prolonger son bail)

DHCPACK : (réponse du serveur qui contient des paramètres et l'adresse IP du client)

Les commandes utilitaires :

1) **Ifconfig :**

⇨ La commande affiche l'état de vos cartes réseaux.

⇨ Affecter une IP/Masque pour une interface réseau temporairement

Syntaxe : ifconfig [nom interface] [IP] netmask

⇨ Création d'interface alias

Syntaxe : ifconfig [nom interface]:[numéro alias] [ip] netmask

⇨ Activer la carte réseau:

syntaxe : ifconfig [nom interface] [up / down]

⇨ Désactiver la carte reseau

Syntaxe : ifconfig eth0 down

2) **Ping:**

⇨ Il permet de vérifier l'existence d'une machine sur les réseaux et de détecter bon nombre de problèmes concernant votre configuration IP

Syntaxe : ping localhost

Exemple : ping 192.168.24.3

Pour envoyer seulement 5 requêtes :

ping 192.168.24.3 –t 5

On augmente la taille des paquets envoyés à 128Ko

ping -s 128 192.168.24.3

3) **Route :**

⇨ Affecter l'IP de la passerelle par défaut pour une interface

Syntaxe : route add default gw [IP de la paserelle]

Exemple :

route add default gw 192.168.0.254

4) **Traceroute :**

⇨ Problème d'accès d'une machine ou d'un réseau, et ping confirme ceci Mais plusieurs routeurs intermédiaires et vous voulez savoir à quel niveau vous avez un problème.

Exemple : traceroute mailserver1

⇨ L 'option « -n » de traceroute damande l'affichage de l'adresse IP du serveur et non pas le nom

Configurer le nom de la machine :

1) **Pour afficher le nom de la machine, la commande**

hostname

2) **Pour changer le nom de la machine, le fichier**

/etc/hostname

Configurer l'adresse DNS :

1) **Pour configurer l'adresse IP du DNS, le fichier :**

/etc/resolv.conf

Syntaxe du fichier :

#la liste des serveurs de nom

```
nameserver   193.95.66.11
nameserver   8.8.8.8
```

Le fichier /etc/nsswitch.conf : Il permet d'indiquer comment doit se faire la résolution d'adresse (sur la ligne "hosts"). Par exemple, la suite hosts :
Files , dns , nis , signifie qu'on cherche d'abord dans les fichiers locaux (i.e. fichier /etc/hosts), puis qu'on interroge le serveur DNS, et enfin qu'on interroge le serveur NIS

Les lignes passwd, shadow, et group : Il contrôle la manière avec laquelle linux authentifie les utilisateurs et gère les groupes.

Arrêter le service :

⇨ **Pour Karmic :**

sudo service network-manager stop

⇨ **Pour Jaunty :**

Sudo /etc/init.d/NetworkManager stop

Chapitre 2 : Le Service WEB

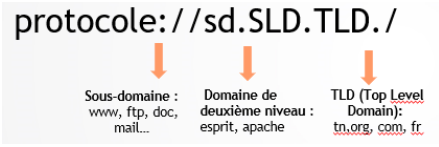
Architecture du service WEB :

Apache :

- Le plus populaire des serveurs HTTP.
- Il est produit par la « Apache Software Foundation ».
- C'est un logiciel libre fourni sous la licence spécifique Apache.

Protocoles HTTP/HTTPS :

HTTP : (***Hypertext Transfer Protocol***) port par défaut 80. L'adresse de la page se découpe ainsi :



Port 80 : pour le mode non sécurisé (http)
Port 443 : pour le mode sécurisé (https).

Types Requêtes :

- **GET :** demande des informations et la ressource désignée
- **HEAD :** demande des informations concernant la ressource
- **POST :** envoie de données (formulaire vers le serveur) et demande la ressource désignée
- **PUT** : enregistrement du corps de la requête à l URL indiquée
- **DELETE :** suppression de la ressource désignée par l 'URL

Types réponses :

Ces codes sont utilisés par le serveur pour informer le client de la manière dont sa requête a été traitée

- **1xx** Information
- **2xx** Succès.
- **3xx** Redirection → une procédure supplémentaire doit être exécutée pour satisfaire la requête
- **4xx** Erreur du client WEB.
- **5xx** Erreur du serveur WEB

Exemple : 500 = erreur interne au serveur

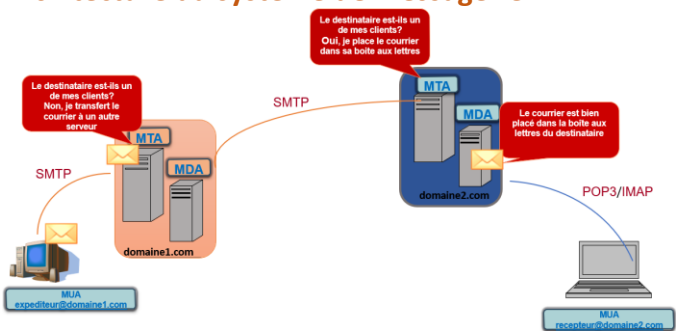
Notion de VirtualHost :

Virtual Host permet d'héberger plusieurs sites web sur un même serveur.
Il peut être divisé en trois principales catégories :

- **Par Nom :** la machine ne possède qu'une seule adresse IP et ce sont les noms des sites qui vont aiguiller la requête
- **Par Port :** la machine possède une ou plusieurs adresses IP, mais elle peut différencier les sites par port logique
- **Par IP :** la machine serveur possède plusieurs adresses IP, et chacune mène vers un site distinct

Chapitre 3 : Le Service de Messagerie

Architecture du système de messagerie :



MUA (Mail User Agent): C'est le client de messagerie
MTA Mail transfert Agent) : c'est le logiciel pour serveur de transmission. Il s'occupe d'envoyer les mails entre les serveurs.
MDA (Mail Delivery Agent) : c'est le logiciel de distribution du courrier électronique et représente la dernière étape de la chaîne d'envoi d'un mail. Il est plutôt associé aux protocoles POP et IMAP.
SMTP : Simple Mail Transfert Protocol
POP3 : Post Office Protocol
IMAP : Internet Message Access Protocol

Itinéraire d'un message électronique :

1. Lors de l'envoie d'un mail, le MUA le transmet à l'MTA (configurer au niveau de notre client messagerie) grâce au protocole SMTP.
2. De MTA en MTA, le message transite jusqu'à l'MTA qui a en charge la messagerie du domaine du destinataire toujours grâce au protocole SMTP.
3. Il le passe alors (avec tous les autres messages entrant pour ce domaine) à l'MDA qui distribue ces courriers entrants dans les boites aux lettres concernées.
4. Lorsque le destinataire consulte sa boite de réception (qui se trouve sur le serveur MDA), il reçoit le mail grâce au protocole POP3 ou IMAP.

Les Protocoles :

Protocoles d'envoie de message

SMTP : (Simple Mail Transfert Protocol RFC 821) port par défaut 25

- C'est un protocole de messagerie qui a pour objectif de faire transiter les mails vers les serveurs de messagerie afin que les utilisateurs puissent consulter leurs mails.
- Il permet de transférer les courriers d'un serveur à un autre.
- Il achemine un message jusqu'à la boite aux lettres
- Il définit les standards du courrier électronique

Protocoles de réception de message :

POP3 vs IMAP :

	POP3 : Post Office Protocol RFC 1939	IMAP : Internet Message Access Protocol RFC 2060
Port	110	143
Consultation	Hors connexion	Une connexion constante au serveur de messagerie.
Stockage	Stocker les courriers dans l'ordinateur. Utilisation minimale des ressources du serveur.	Stocker les courriers dans le serveur. Gérer l'espace disque du serveur.
Accès	Gérer un seul accès. Gérer une seule boite aux lettres.	Gérer plusieurs accès simultanés. Gérer plusieurs boîtes aux lettres.
Gestion	Permet une gestion des messages en local après téléchargement => recherches et tris plus rapide et efficace.	Permet une gestion simplifiée de la messagerie en cas de mobilité de l'utilisateur.

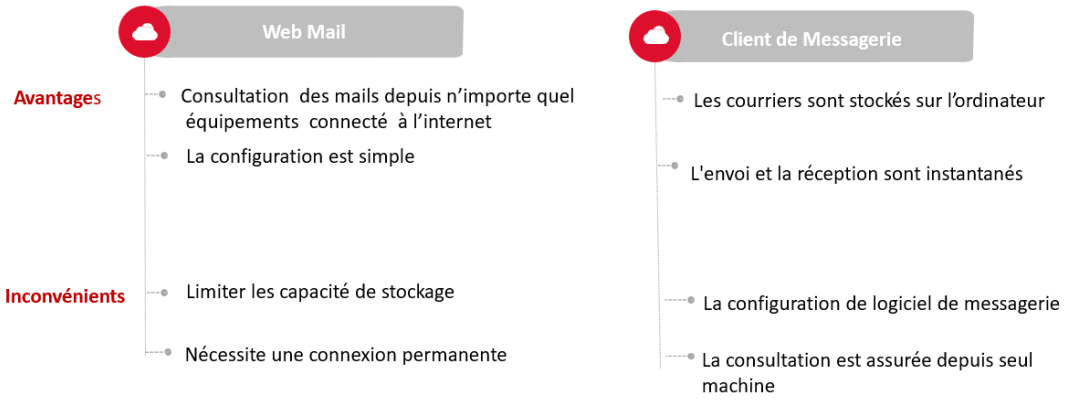
14

Applications de messagerie :

Il existe deux façons d'envoyer et de recevoir du courrier électronique : **Le Web Mail et le Client de Messagerie**

- La première consiste à se connecter à un serveur de messagerie en ouvrant le navigateur internet (Internet Explorer, chrome.) **C'est le Web Mail**.
- La deuxième méthode consiste à utiliser **un client de messagerie** préalablement installé sur votre ordinateur et paramétré (Outlook, Thunderbird, etc.)

Les différents clients de messagerie



Conclusion :

- ⇨ La messagerie électronique, un service réseau très répandu, par sa simplicité et sa vitesse d'exécution
- ⇨ Lorsque l'utilisateur rédige un courrier, il fait généralement appel à une application connue sous le nom de client de messagerie.
- ⇨ Le client de messagerie permet l'envoi des messages vers un serveur de messagerie bien déterminé.
- ⇨ Ce serveur place les messages reçus dans la boîte aux lettres du destinataire.
- ⇨ Un moyen de communication majeur dans l'entreprise, entre entreprises ou entre particuliers.
- ⇨ Une attente de plus en plus importante vis à vis de la messagerie : intégration de la circulation d'information, outils de travail coopératifs.
- ⇨ Une évolution permanente des messageries standards ou propriétaires vers les standards Internet.

Chapitre 4 : Domain Name Système (DNS) où Service de Résolution de Nom

La plupart des utilisateurs préfèrent en effet un nom convivial comme esprit.tn pour accéder à un ordinateur tel qu'un serveur de messagerie ou un serveur Web au lieu de l'utilisation des adresses IP.

⇒ Utilisation du fichier de résolution locale (hosts.txt) pour la résolution des noms pendant les années 80.

- ✖ **Toute modification dans ce fichier doit être faite sur toutes les machine**
- **Solution : DNS**

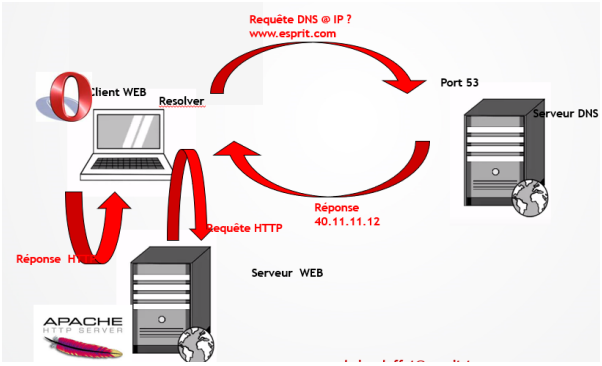
Le Système des Noms de Domaine est un système hiérarchique qui assure la correspondance entre des noms et des adresses IP. Il utilise un protocole de communication client/serveur UDP/TCP sur le port 53

Le DNS n'est pas bijectif :

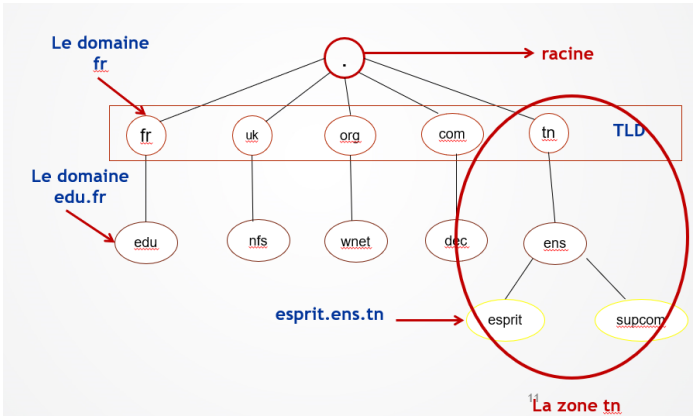
⇨ Un service peut être déployer sur deux serveurs pour des raison de répartition de charge ou de haute disponibilité. Dans ce cas, la réponse à la requête de résolution du nom de domaine www.esprit.tn peut être 192.168.1.10 ou bien 192.168.1.11

⇨ Différents services (web, mail, transfert de fichier …) peuvent être installer sur la même machine physique. Dans ce cas, la réponse à la requête de résolution du nom de domaine www.esprit.tn, mail.esprit.tn et ftp.esprit.tn est l'adresse 192.168.1.10.

Architecture du service DNS :



La hiérarchie DNS :



- ✓ Les niveaux supérieurs TLD (Top Level Domain) sont organisés au niveau géographique et/ou thématiques .fr .uz .uk .com .mil .
- ✓ Chaque nœud définit un domaine : suite de noms séparés par des points
- ✓ Les nœuds possèdent tous un nom (de 0 à 63 caractères) et correspondant à une ressource (qui peut être vide).
- ✓ Deux nœuds frères ne peuvent pas avoir le même nom.
- ✓ Le nœud racine (*root*) est constitué de 0 caractères
- ✓ Une "zone" est une organisation logique (ou pour être plus précis, une organisation administrative) des domaines. Le rôle d'une zone est principalement de simplifier l'administration des domaines. Le domaine «.com» peut être découpé en plusieurs zones, z1.com, z2.com, …zn.com. L'administration des zones sera déléguée afin de simplifier la gestion globale du domaine.

L'arborescence:

Pour déterminer l'adresse IP correspondante au nom : www.esprit.ens.tn.

1-Trouver un NS (serveur de noms) de la racine «.»
2-Obtenir le NS de tn.
3-Interroger le DNS de la zone tn. Pour un NS de ens.tn.
4-Le NS de esprit.ens.tn. Identifie www. Et renvoi son adresse IP.

C'est le Rôle de Resolver.

Rôles :

Il y a trois rôles impliqués dans le DNS :

Le RESOLVER

- Prends la demande de l'application,
- Formate la demande dans le paquet UDP
- Envoi la demande au cache DNS

Son Fonctionnement :

Le résolveur de noms (resolver) est un programme qui extrait l'information des serveurs de noms en réponse d'une requête émanant d'un client. Il élabore l'interrogation

- ⇨ Contacte un serveur de nom (dont l' (les) adresse(s) est (sont) configurées sur la machine exécutant ce resolver)
- ⇨ Interprète les réponses
- ⇨ Retourne l'information au logiciel appelant
- ⇨ Gestion de cache (dépend de la mise en œuvre)

SERVEUR CACHE

- Renvoie la réponse si elle est déjà connue
- Autrement il recherche un serveur autoritaire qui a l'information
- Cache le résultat pour de requêtes futures

SERVEUR AUTORITAIRE

- Contient l'information réelle mise dans le DNS par le propriétaire du domaine

Le Fonctions de ces deux serveurs :

Le serveur autoritaire (serveur maître)

Possède une base d'informations d'une zone dont il a l'autorité administrative.

Duplication de DNS (serveur esclaves)

- ⇨ Les données sont enregistrées sur un serveur autoritaire (maître) et copier vers un (des) serveur(s) autoritaire(s) (esclave(s))
- ⇨ Pas de différence visible entre les 2 types de serveurs depuis l'Internet.
- ⇨ Ces serveurs sont aussi appelés serveurs primaires et secondaires.
- ⇨ Un serveur peut être primaire pour certaines zones et secondaires pour d'autres.

Le serveur DNS : BIND9 :

L'implémentation DNS la plus utilisée sur Internet est **Berkeley Internet Name Domain (BIND) software**

L'installation du serveur BIND :

yum -y install bind bind-utils

```
$TTL  3h
@       IN      SOA     ns.esprit.tn.       hostmaster. esprit.tn. (
                        2009090601          ; Serial
                        8H                  ; Refresh
                        2H                  ; Retry
                        1W                  ; Expire
                        1D )                ; Negative Cache TTL
```

TTL : Time To Live : Indique pendant combien de temps un enregistrement (réponse) peut être gardée en cache

@ : Désigne l'origine du domaine. Remplace le nom de domaine donné dans le fichier named.conf pour la zone concernée

SOA : une zone sous l'autorité d'un serveur de noms : SOA.

IN : signifie que l'on a affaire à une zone Internet

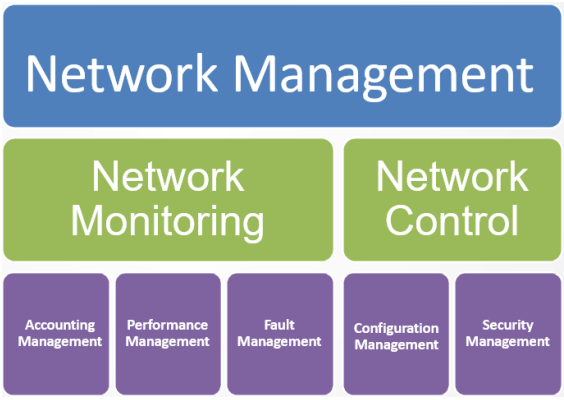
NS : Liste des serveurs de noms pour cette zone

SOA parameters are :

- **Serial :** incrémenté par l'administrateur de la zone à chaque modification. Permet la détection d'un changement sur la zone et donc la nécessité de la recharger
- **Refresh:** rythme auqeul les serveurs secondaires doivent vérifier le numéro de série sur le primaire
- **Retry:** à quel rythme les serveurs secondaires doivent essayer de contacter le primaire en cas d'échecs
- **Expire :** si le secondaire n'a pu contacter le primaire durant la période définie, il supprime les données locales des zones du primaire
- **Negativecache TTL :** pendant combien de temps un cache peut garder une requête non existante

Chapitre 5 : Le Service Supervision

Nos réseaux sont entourés de menaces, ce qui va entraîner des temps d'arrêt et des pertes de données
Donc la solution est : **Network management**



What Is Network management ?

- ⇨ Il aide une organisation à atteindre ses objectifs de disponibilité, de performances et de sécurité
- ⇨ Aide une organisation à mesurer dans quelle mesure les objectifs de conception sont atteints et à ajuster les paramètres du réseau s'ils ne sont pas atteints
- ⇨ Aide une organisation à analyser le comportement actuel du réseau, à appliquer les mises à niveau de manière appropriée et à résoudre tout problème lié aux mises à niveau

Network management Requirements :

- ✓ Fault management
- ✓ Accounting management
- ✓ Configuration management
- ✓ Performance management
- ✓ Security management

Fault Management : Les installations qui permettent la détection, l'isolement et la correction d'un fonctionnement anormal de l'environnement OSI.

Il implique les étapes suivantes :

- ✓ Découvrir d'où vient la panne,
- ✓ Isoler le défaut,
- ✓ Modifier le réseau et reconfigurer sans le composant défaillant,
- ✓ Réparer ou remplacer le composant défaillant.
- ✓ Restaurez le réseau à son état initial.

Accounting Management :

Les facilités qui permettent d'établir des redevances pour l'utilisation des objets gérés et d'identifier les coûts pour l'utilisation de ces objets gérés

- ✓ Les gestionnaires de réseau suivent l'utilisation des ressources réseau par utilisateur final ou par classe d'utilisateurs finaux
- ✓ Un utilisateur final ou un groupe d'utilisateurs finaux peut abuser de ses privilèges d'accès et surcharger le réseau aux dépens des autres utilisateurs
- ✓ Les utilisateurs finaux peuvent faire une utilisation inefficace du réseau, et le gestionnaire de réseau peut aider à modifier les procédures pour améliorer les performances
- ✓ Le gestionnaire de réseau est plus facile à planifier pour la croissance du réseau si l'activité de l'utilisateur final est connue de manière suffisamment détaillée

Configuration Management :

- ✓ Configuration Management concerne :
- ✓ Initialiser un réseau,
- ✓ Arrêt progressif de tout ou partie du réseau,
- ✓ Maintenir, ajouter et mettre à jour les relations entre les composants et l'état des composants eux-mêmes pendant le fonctionnement du réseau.

Performance Management :

- ✓ Monitoring des activités sur le réseau,
- ✓ Permet à performance management d'effectuer des ajustements pour améliorer les performances du réseau

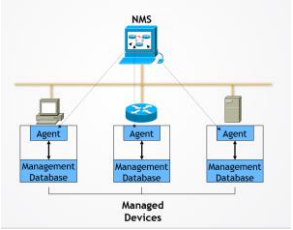
Security Management :

Les Aspects de la sécurité OSI sont essentiels pour faire fonctionner correctement la gestion de réseau OSI et protéger les objets gérés.

Network Management Systems :

A network management system est un ensemble d'outils de surveillance et de contrôle de réseau :

- ✓ A managed device est un nœud de réseau qui collecte et stocke des informations de gestion,
- ✓ Un agent est un logiciel de network-management qui réside dans un a managed device,
- ✓ A network-management system (NMS) exécute des applications pour afficher les données de gestion, surveiller et contrôler managed devices et communiquer avec les agents



Network Management Protocols

1987: OSI approach

- Common Management Information Protocol (**CMIP**)
  - CMIP is the management (application layer) protocol
- Common Management Information Service (**CMIS**)
  - CMIS is the service interface to CMIP

1989 : Simple Network Management Protocol (SNMP)

- It is defined by IETF (Internet Engineering Task Force). It is an application layer protocol
- CMIP/CMIS is being replaced by SNMP.
- SNMP uses the concept of manager and agent

Simple Network Management Protocol (SNMP)

Qu'est-ce que c'est?

⇨ Un protocole qui facilite l'échange d'informations de gestion entre les périphériques réseau,

⇨ Fait partie de la suite TCP/IP

Pourquoi a-t-il été développé ?

⇨ Pour contrôler et surveiller l'état des périphériques réseau,

En quoi est-ce bénéfique ?

Permet aux administrateurs réseau de :

⇨ Gérer les performances du réseau

⇨ Rechercher et résoudre les problèmes de réseau

⇨ Planifier la croissance du reseau

Composants de base SNMP:

Network Management station (manager)

⇨ Collecte et stocke les informations de gestion et met ces informations à la disposition de NMS à l'aide de SNMP

⇨ Peut-être un poste de travail ou un PC

Network Management System (NMS)

⇨ Exécute des applications qui surveillent et contrôlent les périphériques gérés

⇨ Fondamentalement, il fonctionnera sur le gestionnaire

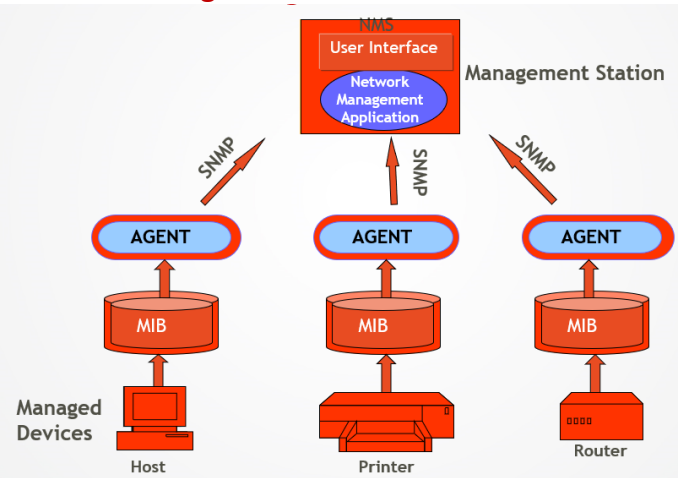
Agent :

processus s'exécutant sur chaque nœud géré collectant des informations sur le périphérique sur lequel il s'exécute.

Management Information Base (MIB)

Utilisé à la fois par le gestionnaire et l'agent pour stocker et échanger des informations de gestion

Network Management Architecture



SNMP MIB

- Every management station or an agent in an SNMP architecture maintains a local database having information related to the network management.
- This virtual information store is called MIB-objects database
- An SNMP MIB contains definitions and information about the properties of managed resources and the services that the agents support.
- The manageable features of resources, as defined in an SNMP MIB, are called managed objects

Managed Objects :

Chapitre 6: Service Annuaire

Un annuaire est un conteneur d'informations organisées. C'est Un système de stockage de données. IL est Organisé d'une manière hiérarchique et Dérivé des BDD relationnelles.

Un annuaire global célèbre très utilisé : DNS

⇨ Il a un espace de nommage uniforme
⇨ Il est distribué entre des serveurs coopérants

Annuaire Electronique VS Base de données :

- Les données sont stockées de manière hiérarchique dans l'annuaire, tandis que les bases de données dites "relationnelles" stockent les enregistrements de façon tabulaire
- Un annuaire électronique est conçu pour être consulté, bien plus que mis à jour.
- L'extensibilité dans l'annuaire : L'ajout d'attributs, l'équivalent des champs dans les bases de données relationnelles, est facile à réaliser. Il ne nécessite pas, par exemple, de reconstruction de la base.

L'annuaire LDAP:

LDAP Lightweight Directory Access Protocol :

Héritier de l'annuaire X500 (proposé par l'ISO) :

- Standard conçu par les opérateurs télécom pour interconnecter leurs annuaires téléphoniques
- X500 adapté à l'internet

Objectifs :

- Fournir aux utilisateurs des informations fiables, facilement accessibles
- Permettre aux utilisateurs de mettre à jour eux-mêmes leurs informations personnelles
- Rendre les informations accessibles de façon contrôlée
- Eviter la redondance d'informations : un seul annuaire pour l'ensemble des services
- Faciliter la gestion (administration) des postes de travail, des équipements réseau

Annuaire: caractéristiques:

- **Dynamique :** Les informations peuvent être mises à jour en temps réel simplement par un administrateur
- **Souple :** Il est facile de rajouter de nouveaux attributs.
- **Sécurisés** : Les annuaires permettent de contrôler l'accès aux informations par différents critères.
- **Personnalisés :** la possibilité de définir la façon de présenter les données

Terminologies:

Objet : Un objet est un ensemble particulier d'attributs qui représente quelque chose de concret, trois grandes catégories d'objets :

- **Les ressources (par exemple les imprimantes),**
- **Les services (par exemple le courrier électronique),**
- **Les utilisateurs (comptes utilisateurs et groupes).**

Attribut : Un attribut est un élément de données qui décrit un certain aspect d'un objet.

Conteneur : C'est simplement une enveloppe, qui renferme des objets et d'autres conteneurs.

Le schéma : correspond à tout ce qui constitue l'annuaire : les objets, les attributs, les conteneurs

L'annuaire LDAP définit 5 modèles

- **Un modèle d'information** : le type de données contenues dans l'annuaire
- **Un modèle de nommage :** comment l'information est organisée et référencée
- **Un modèle fonctionnel** : une syntaxe des requêtes permettant l'interrogation de la base et la mise à jour des informations
- **Un modèle de sécurité** : comment les données et les accès sont protégés
- **Un modèle de duplication : c**omment la base est répartie entre serveurs

Le modèle information:

Définit le type de données pouvant être stocké dans l'annuaire.

Entrée/Objet : élément de base de l'annuaire ; elle contient les informations sur un objet de l'annuaire

- contient les données
- regroupe un ensemble d'attributs

Exemples de classes d'objet :

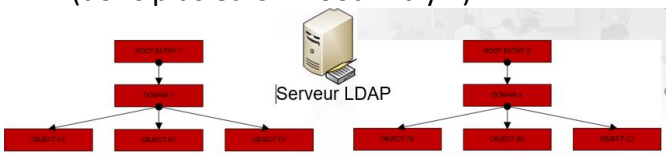
- ✔ une entreprise (*o*)
- ✔ ses différents départements(*ou*)
- ✔ ses employés (organizationalPerson)
- ✔ ses imprimantes (devices)
- ✔ Ses groupes de travail(groupofnames)

Toutes les classes d'objets et leurs attributs sont définis dans un schéma (arbre)
Chaque entrée de l'annuaire fait obligatoirement référence à une **classe d'objet** du **schéma**

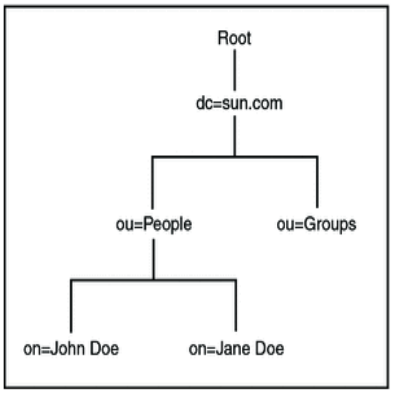
Le modèle de nommage :

Il définit comment sont organisées les entrées de l'annuaire et comment elles sont référencées
Cette organisation est représentée par le Directory Information Tree : (DIT)

- Une « Root Entry » correspond à l'espace de nommage géré par le serveur
- Un serveur LDAP peut gérer plusieurs arbres (donc plusieurs « Root Entry »)



- Distinguish Name (DN) : référence de manière **unique** une entrée du DIT
- DN : constitué d'un ensemble d'attributs et de leurs valeurs provenant de chacune des entrées parentes mises bout à bout.
- Chaque composant du DN est appelé « Relative Distinguish Name » (RDN)



DN de l'entrée Jane : [cn=JaneDoe, ou=People, dc=sun.com]

⇨ On doit s'assurer que 2 entrées du DIT n'aient pas le même DN

Le modèle fonctionnel :

Il décrit: les moyens d'accès aux données et les opérations applicables aux données

Les opérations possibles sont :

⇨ **opérations d'interrogation :** search

⇨ **opérations de comparaison :** compare

⇨ **opérations de mise à jour :** add, delete, rename, modify

⇨ **Opérations d'authentification et de contrôle :** bind, unbind, abandon

Le modèle de sécurité :

Il décrit le moyen de protéger les données de l'annuaire.

La sécurité se fait à plusieurs niveaux

- ✔ Par l'authentification pour se connecter au service
- ✔ Par un modèle de contrôle d'accès aux données
- ✔ Par le chiffrement des communications

Pour **l'authentification**, LDAPv3 propose plusieurs choix:

- ✔ **Anonymous authentification :** accès sans authentification
- ✔ **Root DN authentification :** accès administrateur
- ✔ **Mot de passe + SSL ou TLS :** accès chiffré
- ✔ **Certificats sur SSL :** accès avec échange de clé (publique/privée)

Le modèle de duplication:

Il définit comment dupliquer l'annuaire sur d'autres serveurs.

Intérêt de **dupliquer un serveur LDAP** :

- ✔ Pallier une panne de l'un des serveurs, coupure de réseaux, …
- ✔ Répartir la charge du service
- ✔ Garantir une qualité de service (temps de réponse)

Les logiciels serveurs

- Active Directory
- Lotus Domino
- OpenLDAP

Les logiciels clients

- Microsoft Outlook, NetMeeting
- Netscape Communicator
- LDAP Browser