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

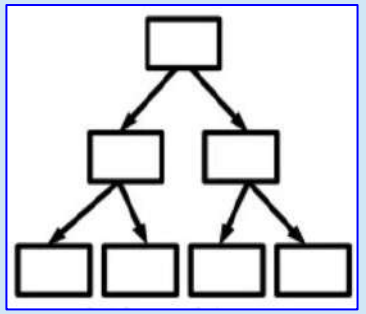
- **Chapitre 1**. Présentation de l'administration réseau,
- **Chapitre 2**. Le service SNMP (Simple Network Management Protocol)
- **Chapitre 3**. Les services annuaires
- **Chapitre 4**. Gestion des utilisateurs et service NFS
- **Chapitre 5**. Service de messagerie et services d'application
- **Chapitre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

Chapitre 3. Les services annuaires

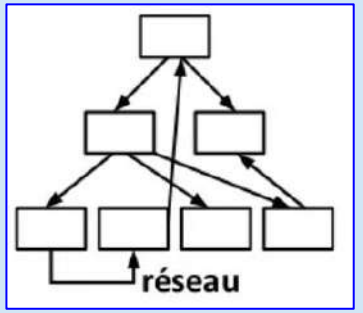
- Les différents services annuaires
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Lightweight Directory Access Protocol (LDAP).
- Autres services annuaires

Service annuaire

- Un **annuaire électronique** est une sorte de base de données permettant de stocker et retrouver facilement des informations sur différents objets (ressources). **Mais ce n'est pas simplement une base de données**.
  - Dédié à la lecture plus qu'à l'écriture
  - L'accès aux données se fait par des recherches multicritères
- Exemple d'annuaires:
  - Carnet d'adresses,
  - Stockage des utilisateurs sous UNIX
  - Annuaire téléphonique,
  - Serveur DNS, ...
- **Service annuaire = Système de stockage de données (Protocole qui permet d'exploiter et de gérer des annuaires).**
- Les données ne sont pas organisées de manière **relationnelle** comme sur les **SGBD classiques** (MySQL, PgSQL, SQLServer, etc.) mais de manière **hiérarchique**.

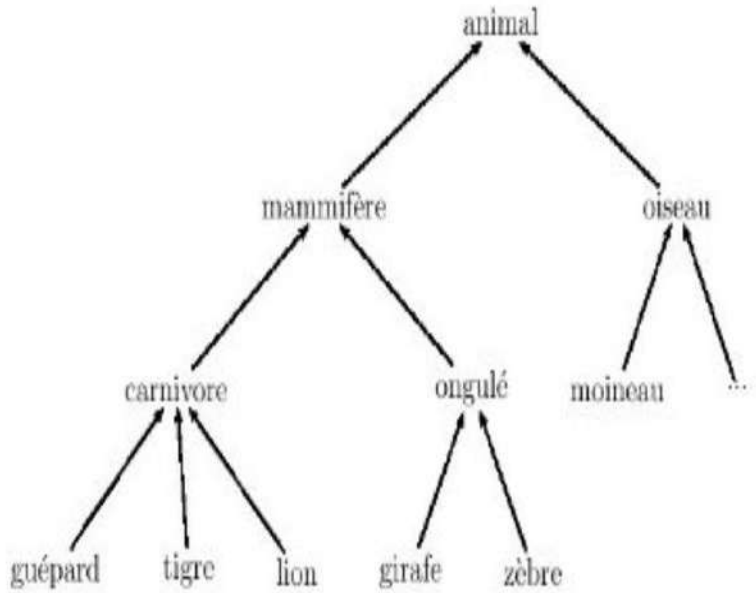


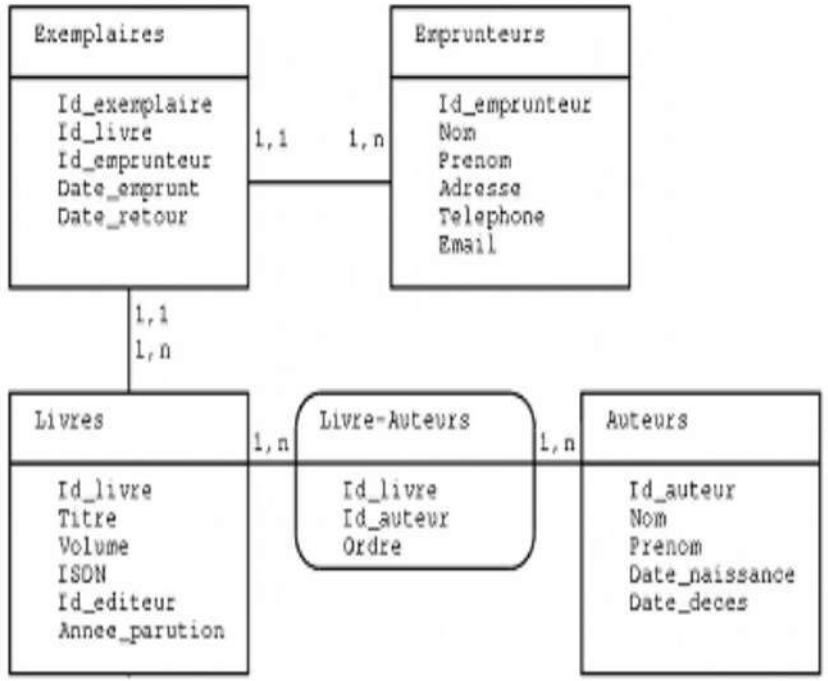
Base hiérarchique



Base relationnelle

Services annuaire vs SGBD classique





Exemple d'organisation hiérarchique	Exemple d'organisation relationnelle

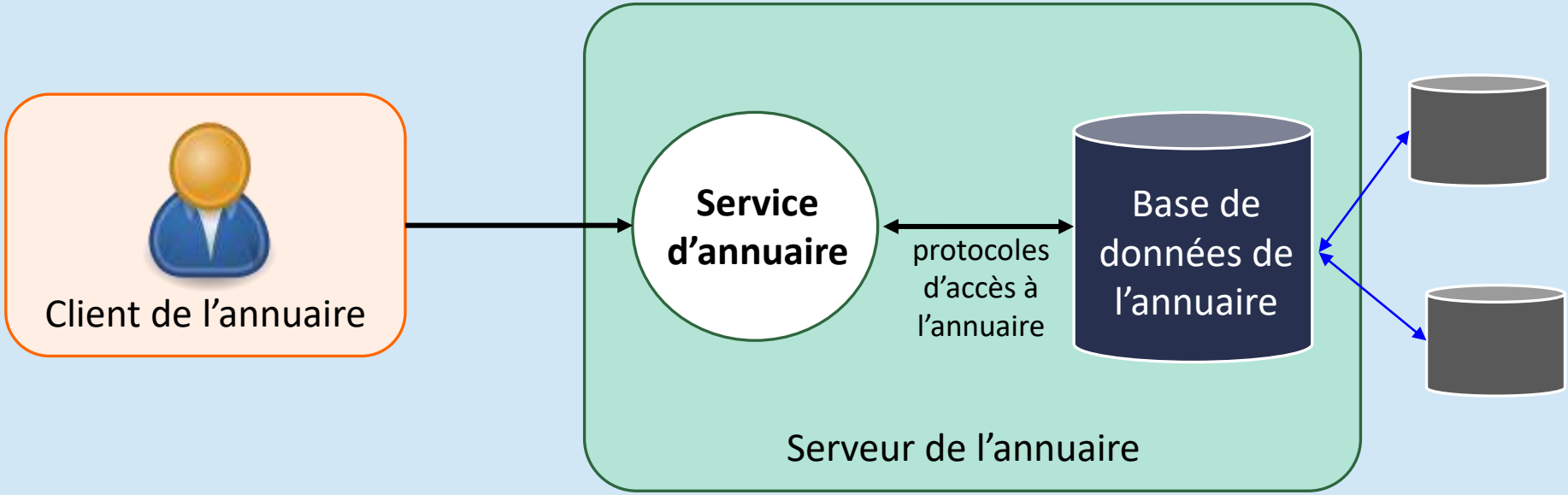
Services annuaire vs SGBD classique

- **Comparaison entre un services d'annuaire et les SGBD classiques.**
  - La consultation des données est **plus rapide** pour l'annuaire par rapport aux SGBD classiques
  - La duplication des données est facilitée pour assurer une meilleure disponibilité.
  - Pas de dépendances entre les objets stockés
  - Le stockage des données peut être réalisé dans un plus faible espace.
- **Les avantages des services d'annuaire sont:**
  - Leur **rapidité** pour accéder aux informations,
  - Les mécanismes de **sécurité** pouvant être mis en œuvre,
  - La **centralisation** des informations et
  - Les possibilités de **redondance** de l'information.

Services annuaire vs SGBD classique

La figure ci dessous illustre l'implantation d'un service d'annuaires type.

- Les clients se connectent au service d'annuaire pour interroger la base de données du service.
- Certains services d'annuaires peuvent échanger des informations avec d'autres.



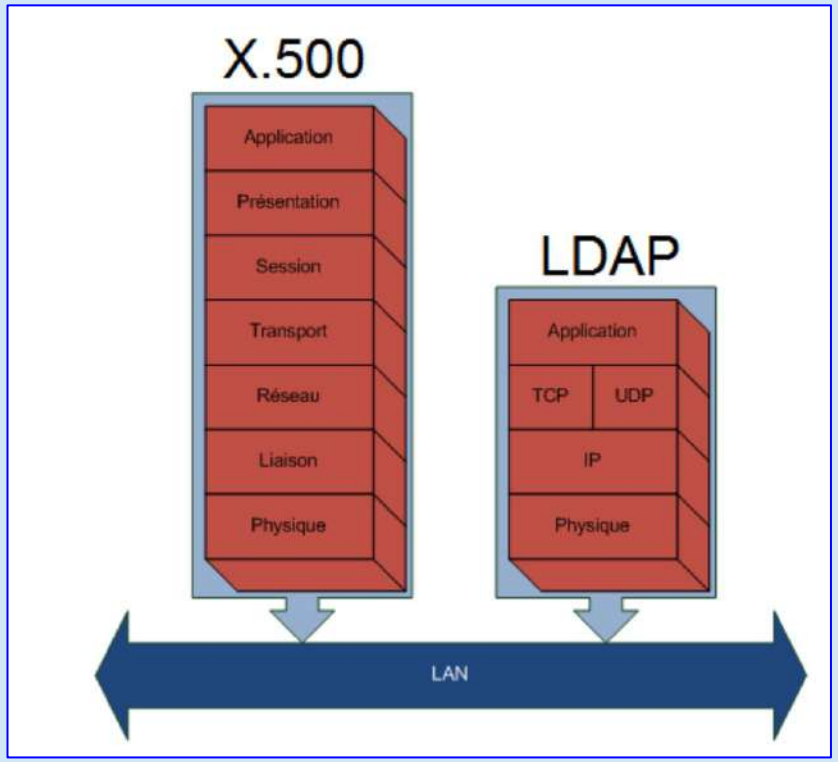
Norme X.500

- **La norme X.500** est une norme importante dans le domaine des services d'annuaire
- Elle a été conçue en 1988 par **l' UIT** pour interconnecter les annuaires téléphoniques des opérateurs télécom.
- **But** : normaliser les services d'annuaire
- Pour cela, elle définit :
  - des règles de nommage pour les données de l'annuaire
  - des protocoles d'accès à l'annuaire (**DAP: Directory Access Protocol**)
  - un mécanisme d'authentification
- **Problème**: cette norme n'a pas abouti car elle ne s'est pas adaptée à l'essor des communications distantes avec le protocole TCP/IP.
- **La norme X.500 utilisait un système compliqué pour communiquer impliquant l'ensemble du modèle OSI ← X.500 lourd et complexe**.
- **Il est donc nécessaire de définir un protocole plus léger et plus simple ← Lightweight DAP**

Protocole LDAP

Il est donc nécessaire de définir un protocole plus léger et plus simple ← Lightweight DAP

- **C'est pour cette raison, que le protocole LDAP a été développé**.
- LDAP (Lightweight Directory Access Protocol) est une adaptation allégée de la norme X.500.
- C'est en 1996 qu'apparaissent les premiers serveurs LDAP commerciaux.
- Il existe 3 versions du protocole LDAP, qui sont :
  - **LDAPv1 (1993 & RFC1487)**
  - **LDAPv2 (1995 & RFC1777)**
  - **LDAPv3 (1997 & RFC2251)**
- **LDAPv3** propose des mécanismes de chiffrement (SSL, ...) et d'authentification permettant de sécuriser l'accès aux informations stockées dans la base.



Protocole LDAP: 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 et des équipements réseau.

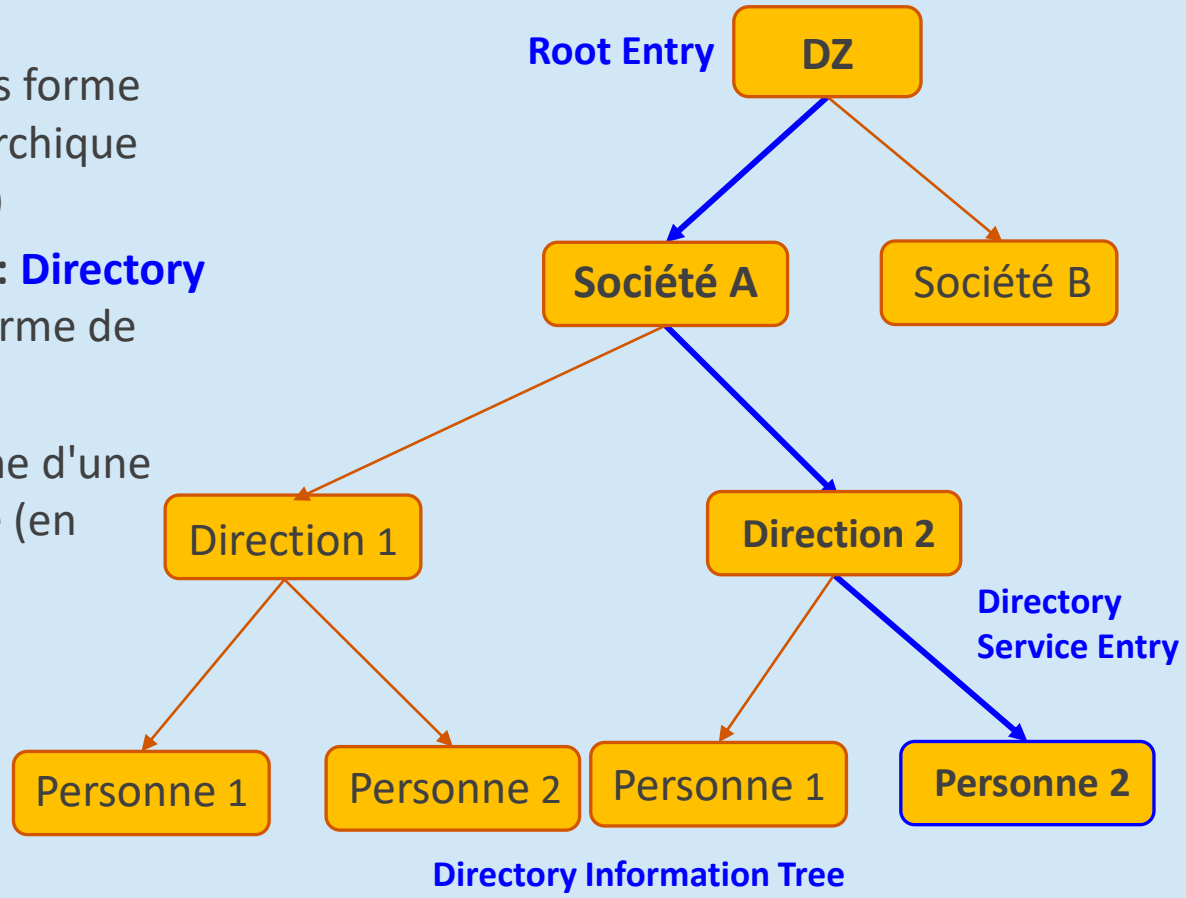
Tout ceci est fait sans remettre en cause les applications existantes

Protocole LDAP

- LDAP définit :
  - **Un modèle d'information** pour définir le type des informations contenues dans l'annuaire,
  - **Un modèle de nommage** pour indiquer comment les informations sont organisées et référencées,
  - **Un modèle fonctionnel** pour indiquer comment accéder aux informations (ex: syntaxe des requêtes),
  - **Un modèle de sécurité** pour indiquer comment protéger l'accès aux données,
  - **Un modèle de duplication :** comment les bases sont répartie entre serveurs,
  - **Un protocole** pour accéder à l'information contenue dans l'annuaire
  - **Des API** : pour développer des applications clientes,
  - **LDIF (LDAP Data Interchange Format)** : un format d'échange de données.

Protocole LDAP : Directory Information Tree

- **DIT** : LDAP présente les informations sous forme d'une arborescence d'informations hiérarchique appelée DIT (**Directory Information Tree**)
- **DES** : Les entrées "Entry" (ou encore **DES: Directory Service Entry**), sont représentées sous forme de branches.
- **Root Entry** : une branche située à la racine d'une ramification est appelée racine ou suffixe (en anglais **Root Entry**).



Protocole LDAP: Entrée

- Une entrée (**entry**) est l'équivalent en programmation orientée objet d'une "**classe d'objet**". Elle regroupe un ensemble **d'attribut** contenant les différentes informations relatives à l'entrée.
- **Exemple:** une entrée de type "**Client**" qui contient plusieurs attribut avec les différentes informations sur le client.
- Un attribut est caractérisé par:
  - un nom
  - un type
  - une méthode de comparaison
  - un « Object Identifier » (IOD)
  - une valeur
- Un attribut peut être possédé par plusieurs classes.
- **Exemple**: une entré de type "**Fournisseur**" peut avoir le même attribut "**cn**" (**common name**) qu'une entrée de type "**Client**"

Exemple d'entrée

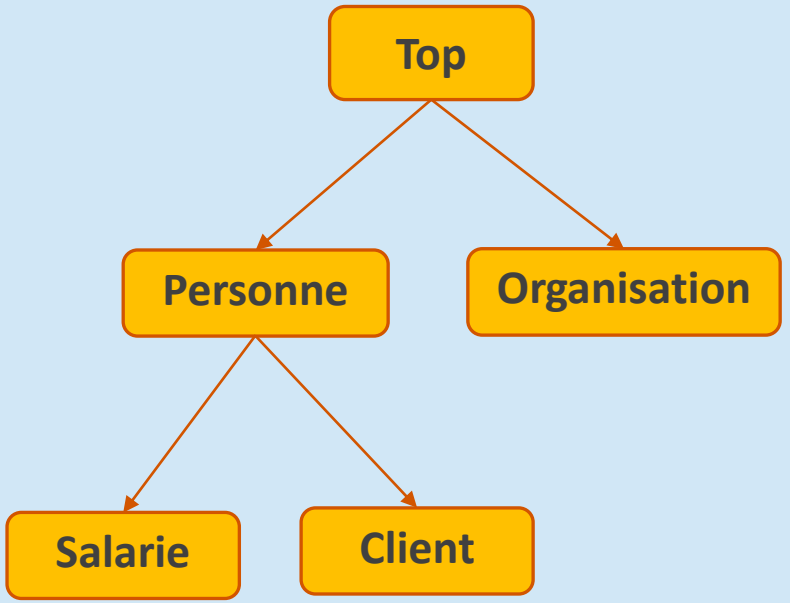
Client	
Type d'attribut	**Valeur d'attribut**
cn:	Joe SMITH
uid	Jsmith
telnumber	03388123456
mail	Joe.smith@gmail.com
solde	100,000,00

Protocole LDAP: Entrée

- Voici une listes des attributs classiques que l'on retrouve sur les entrées d'un service LDAP:
  - **uid** (userid), il s'agit d'un identifiant unique obligatoire
  - **cn** (common name), il s'agit du nom de la personne
  - **gn** (givenname), il s'agit du prénom de la personne
  - **sn** (surname), il s'agit du surnom de la personne
  - **o** (organization), il s'agit de l'entreprise de la personne
  - **u** (organizational unit), il s'agit du service de l'entreprise dans laquelle la personne travaille
  - **dc** (domain component), il s'agit d'un élément du domaine
  - **mail**, il s'agit de l'adresse de courrier électronique de la personne (bien évidemment)

Protocole LDAP : Schéma

- D'une manière générale, tout les types d'entrées (ex: Client, Fournisseur, ...) et leur attributs (ex: cn, ou, ...) sont définis dans un **schéma**.
- **Schéma**: définit l'ensemble des types d'entrées par le service LDAP.
- Chaque entrée de l'annuaire fait obligatoirement référence à une **classe d'objet du schéma**.
- Les types d'entrées sont organisées de manière **hiérarchique**.
  - **Sommet**: le sommet de cette organisation hiérarchique est toujours occupé par le type "**Top**".
  - **Héritage**: cette organisation met en place un système d'héritage où chaque type hérite des attributs de son type parent.
- Sur l'exemple, les types "**Client**" et "**Salarié**" héritent des attributs du type "**Personne**" qui lui même héritent des attributs du type "**Top**".



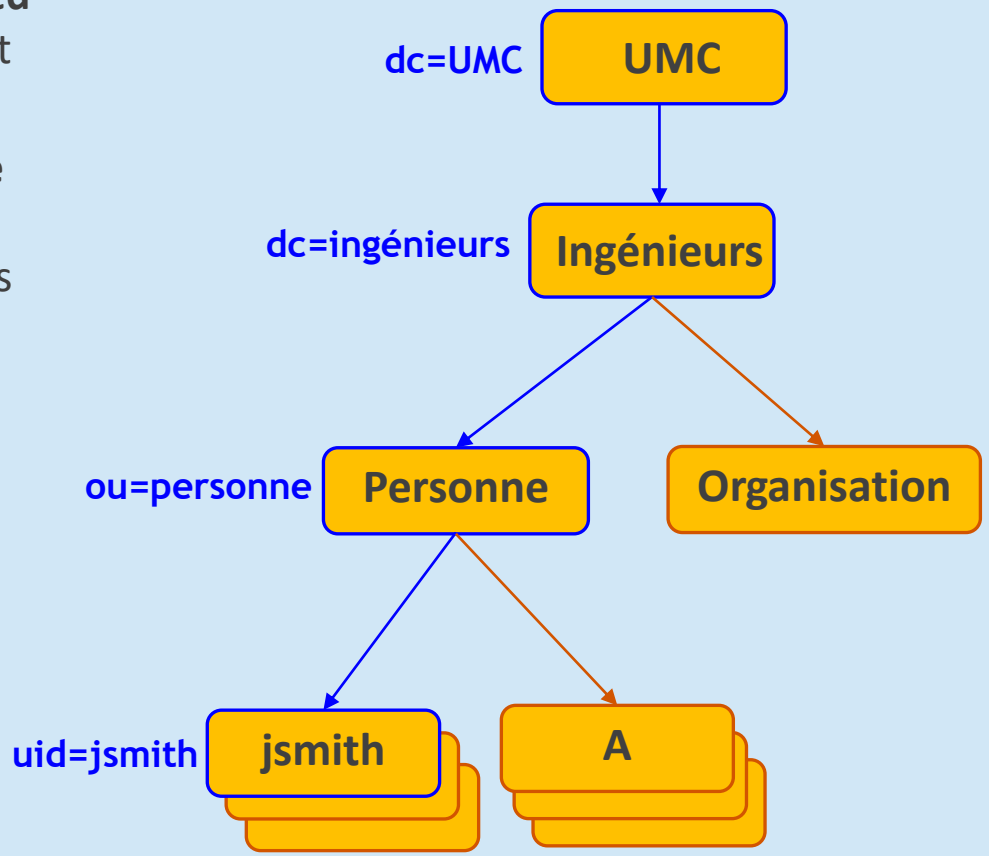
Schéma

Protocole LDAP : Distinguished Name

- Une entrée est indexée par un nom distinct (**DN, Distinguished Name**) permettant d'identifier de manière unique un élément de l'arborescence.
- Chaque élément qui compose le DN est appelé **RDN**: **Relative Distinguish Name**, c'est-à-dire le chemin de l'entrée par rapport à un de ses parents), et en lui ajoutant l'ensemble des nom des entrées parentes.
- Un DN est constitué d'un ensemble d'attribut et de leurs valeurs provenant de chacune des entrées parentes mises bout à bout.
- Voici un exemple de **DN** pour l'entrée **jsmith** :

  DN de l'entrée jsmith = [uid=jsmith, ou=personne, dc=ingénieurs, dc = umlv]

Remarque: il est important de s'assurer que 2 entrées d'un même DIT n'aient pas le même DN. Pour cela, il faut s'assurer que la sélection des attributs composant le DN donne un résultat unique.

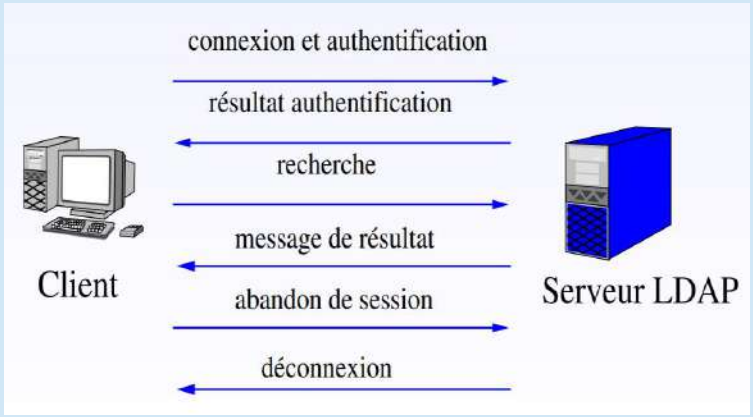


Protocole LDAP : Consultation de données

- LDAP fournit un ensemble de fonctions (procédures) pour effectuer des requêtes sur les données afin de rechercher, modifier, effacer des entrées dans les répertoires.
- Voici la liste des principales opérations que LDAP peut effectuer :
  - **Abandon**: abandonne l'opération précédemment envoyées au serveur
  - **Add**: ajoute une entrée au répertoire
  - **Bind**: initie une nouvelle session sur le serveur LDAP
  - **Compare**: compare les entrées d'un répertoire selon des critères
  - **Delete**: supprime une entrée d'un répertoire
  - **Extended**: effectue des opérations étendues
  - **Rename**: modifie le nom d'une entrée
  - **Search**: recherche des entrées d'un répertoire
  - **Unbind**: termine une session sur le serveur LDAP

Protocole LDAP : Fonctionnement

- LDAP met en place 2 méthodes de communication pour 2 fonctionnalités différentes:
  - **Communication client/serveur**: pour permettre au client d'accéder aux informations contenues sur le serveur. Les opérations de base définies par le protocole LDAP sont:
    - Interrogation: search, compare
    - mise à jour: add, delete, modify
    - connexion: bind, unbind, abandon
  - **Communication serveur/serveur**: pour permettre au serveur de dupliquer ou synchroniser ses informations sur d'autres serveurs.



Ces échanges sont réalisés au format ASCII, des mécanismes d'authentification et de chiffrement sont mis en place pour sécuriser le service

Protocole LDAP : Format d'échange de données LDIF

- LDIF: Lightweight Data Interchange Format.
  - LDIF est un format créé pour décrire les ajouts ou les modifications à réaliser dans un annuaire LDAP.

Service LDAP avec OpenLDAP

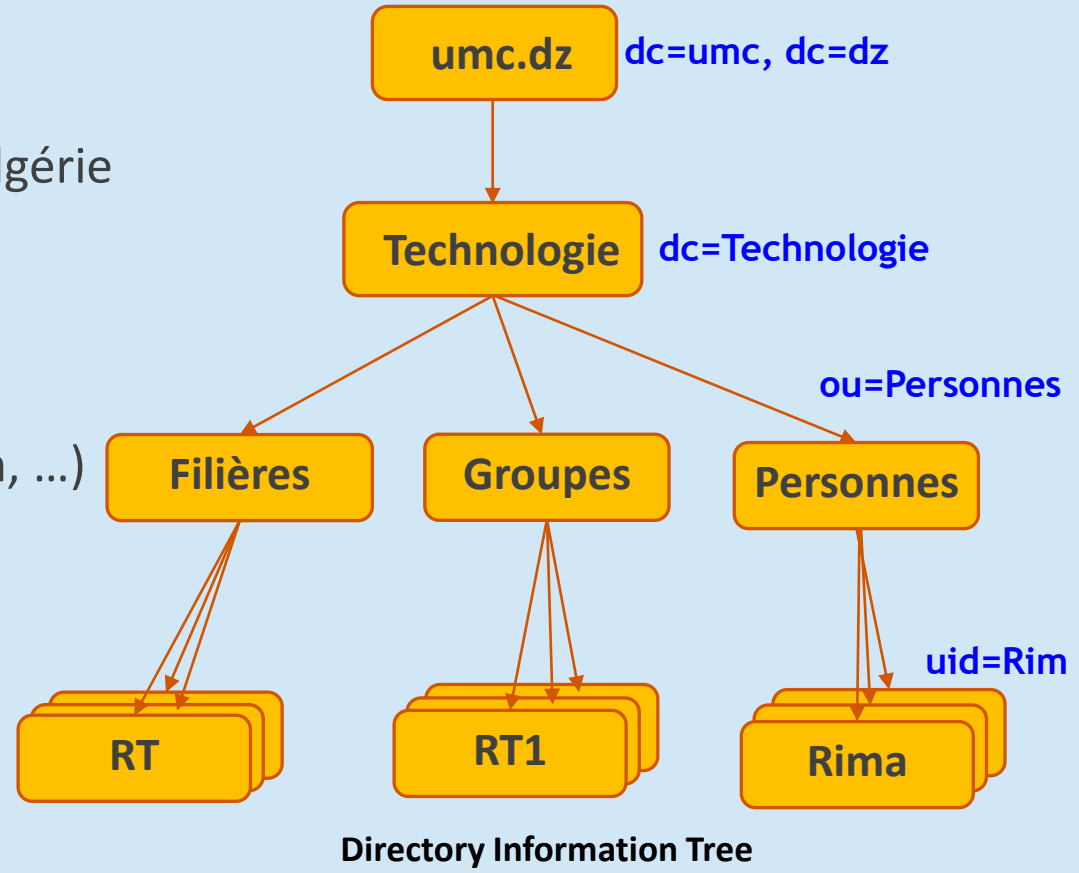
Pour réaliser le déploiement d'un service LDAP, vous pouvez utilisé OpenLDAP.

- Site web: https://www.openldap.org/
- **OpenLDAP** est un serveur LDAP open-source permettant de mettre en place un service LDAP.
- **Déployer un service LDAP**
  - **Etape 1: Conception:** La première étape à réaliser pour déployer un service d'annuaire LDAP est la conception.
  - Cette étape consiste à déterminer :
    - La nature des données
    - L'utilisation que l'on compte en faire
    - La façon de gérer le tout

Service LDAP avec OpenLDAP

Soit l'exemple suivant:

- une organisation: Ecole « Technologie »
- qui se situe à l' UMC, à Constantine, en Algérie
- qui se compose de :
  - filières (RT, ST, Automatique, …)
  - groupes (RT1, RT2, MFPI4, …)
  - personnes (Mohammed, Rima, Karim, …)
- On obtient le DIT suivant:

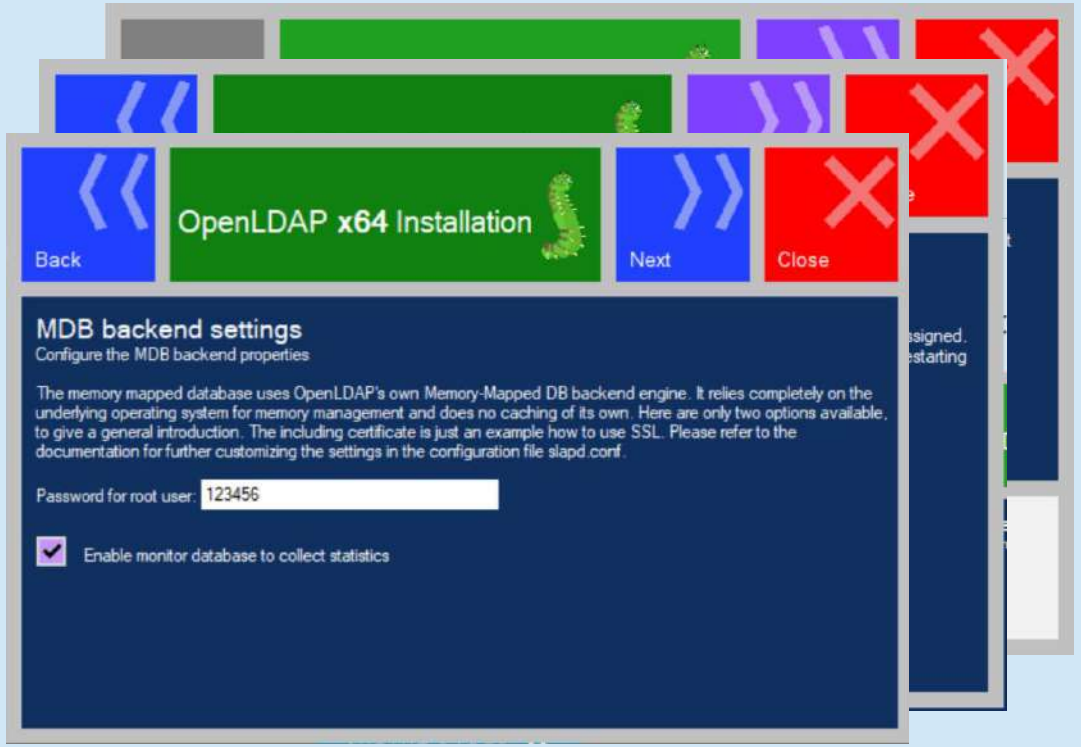


Directory Information Tree

Service LDAP avec OpenLDAP

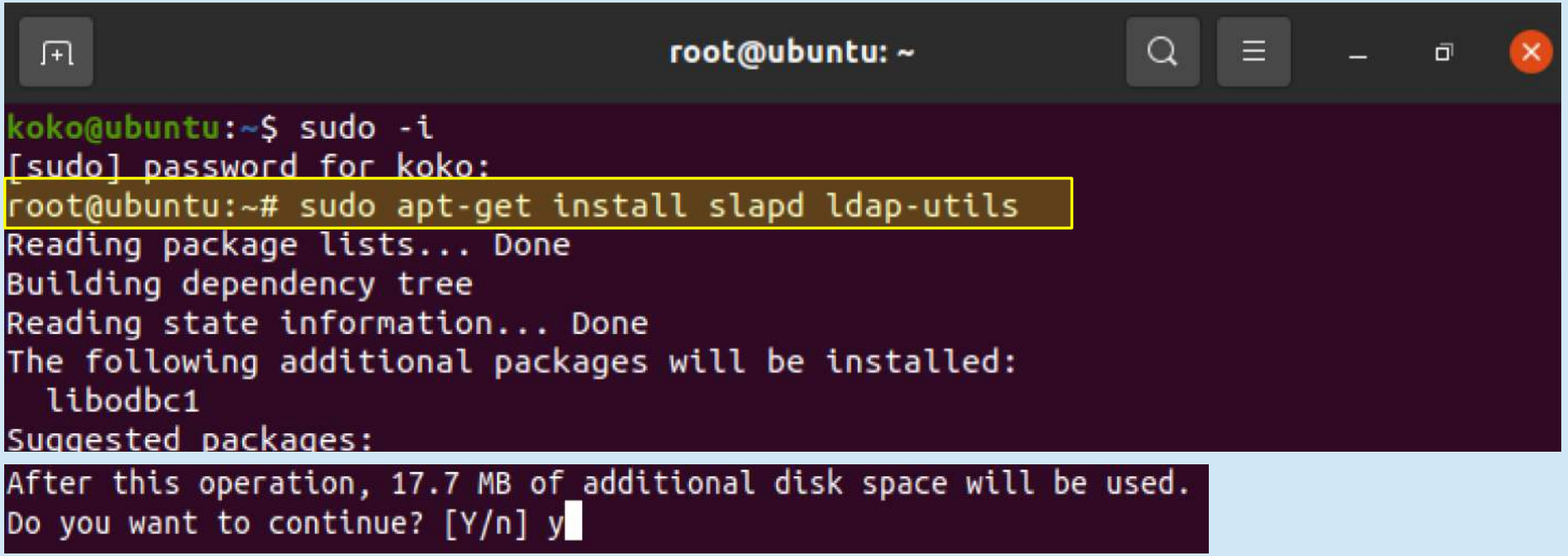
Une fois le DIT définit, on peut passer à l'étape suivante:

- **Etape 2 - Déployer le serveur :** Cette seconde étape consiste à installer et remplir le serveur LDAP. Pour cela, nous devons :"
  - Installer le serveur OpenLDAP
  - Créer un compte administrateur
  - Ajouter les entrées en suivant le DIT



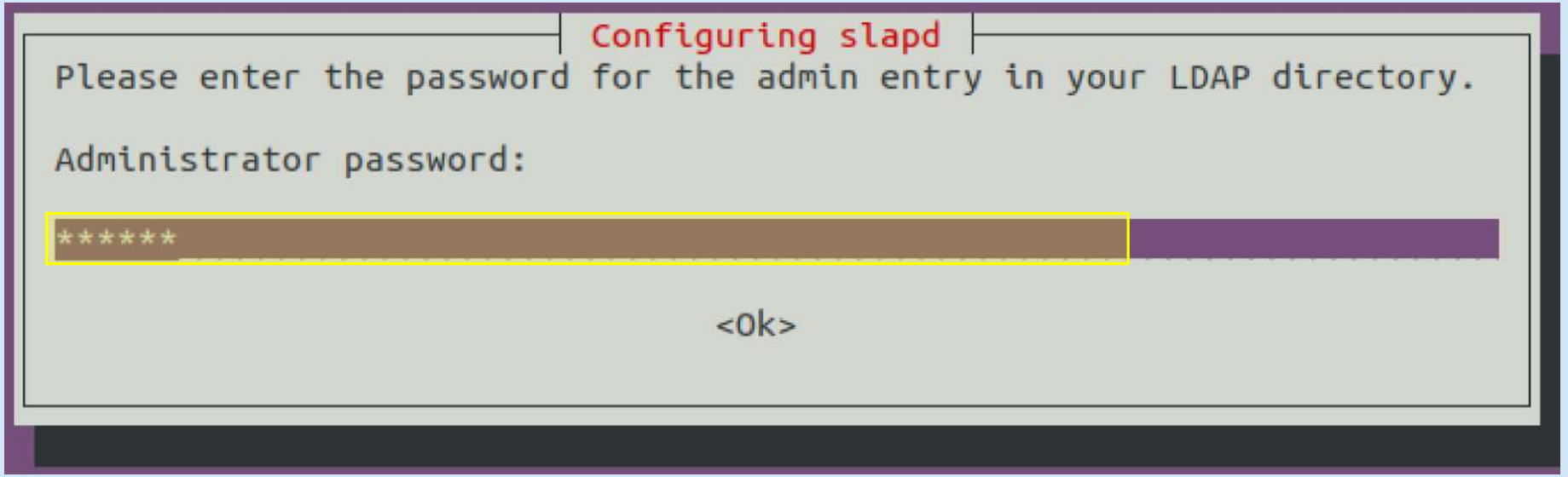
Service LDAP avec OpenLDAP

- Installions du serveur OpenLDAP dans une machine Ubuntu
- Il faut installer les paquets **slapd et ldap-utils.**
- **Ldap-utils:** contient les utilitaires clients pour pouvoir interroger ou modifier l'annuaire.



Service LDAP avec OpenLDAP

- Entrer le mot de passe de l'administrateur de cet annuaire.
- Mot de passe : **123456**



Service LDAP avec OpenLDAP

- Nous allons maintenant utiliser l'outil de configuration **debconf** de Debian pour définir la configuration de base de notre annuaire .
- Commande: sudo dpkg-reconfigure slapd
- Indiquez :
  - **No** pour la première question afin de pouvoir utiliser l'outil de configuration ;
  - Pour nom DNS : **umc.dz** ;
  - Pour nom d'organisation : **umc** ;
  - Le mot de passe administrateur : **123456** ;
  - choisissez le format de base par défaut : **mdb** ;
  - **No** pour savoir si la base doit être supprimée quand slapd est purgé ;
  - **Yes** pour déplacer l'ancienne base de données

```
  Creating LDAP directory... done.
root@ubuntu:~# sudo dpkg-reconfigure slapd
```

Service LDAP avec OpenLDAP

- Comme le DNS est umc.dz, la racine de notre DIT a été configurée à “**dc=umc, dc=dz**”,
- Nous pouvons utiliser la commande **ldapsearch** pour visualiser notre DIT.
- Commande: **sudo ldapsearch -Q -L -Y EXTERNAL -H ldapi:/// -b dc=umc, dc=dz.**
  - **-Q:** active le mode silencieux pour l’authentification SASL
  - **-L:** l’authentification se fera par l’UID et le GID du compte système
  - **-Y:** Afficher le résultat au format LDIF (LDAP Directory Interchange Format)
  - **-H:** l’URI qu’on veut utiliser pour se connecter, ici **ldap:///** (la communication passe par un fichier local plutôt que par le réseau).
  - **-b:** indique le nœud à partir duquel vous voulez faire votre recherche. Ici: dc=umc, dc=dz est la racine donc vous recherchez dans tout le DIT.

Service LDAP avec OpenLDAP

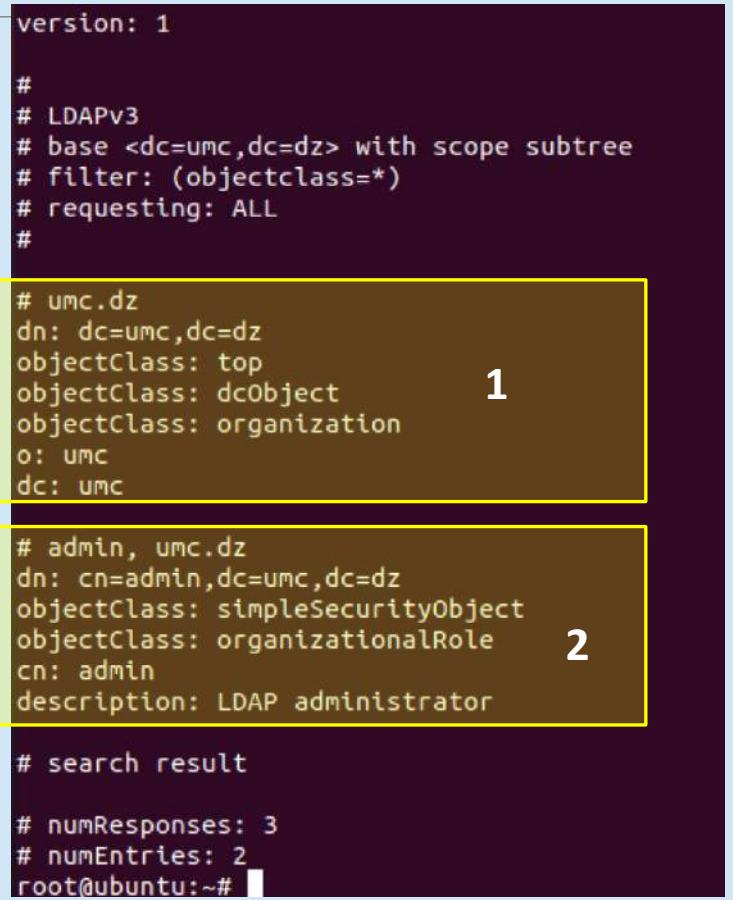
- Comme le DNS est umc.dz, la racine de notre DIT a été configurée à "**dc=umc, dc=dz**",
- Nous pouvons utiliser la commande **ldapsearch** pour visualiser notre DIT.
- Commande: **sudo ldapsearch -Q -L -Y EXTERNAL -H ldapi:/// -b dc=umc, dc=dz.**
  - **-Q:** active le mode silencieux pour l'authentification SASL
  - **-L:** l'authentification se fera par l'UID et le GID du compte système
  - **-Y:** Afficher le résultat au format LDIF (LDAP Directory Interchange Format)
  - **-H:** l'URI qu'on veut utiliser pour se connecter, ici **ldap:///** (la communication passe par un fichier local plutôt que par le réseau).
  - **-b:** indique le nœud à partir duquel vous voulez faire votre recherche. Ici: dc=umc, dc=dz est la racine donc vous recherchez dans tout le DIT.

```
version: 1

#
# LDAPv3
# base <dc=umc,dc=dz> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# umc.dz
dn: dc=umc,dc=dz
objectClass: top
objectClass: dcObject
objectClass: organization
o: umc
dc: umc

# admin, umc.dz
dn: cn=admin,dc=umc,dc=dz
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result

# numResponses: 3
# numEntries: 2
root@ubuntu:~#
```

DIT contient en tout 2 entrées

Service LDAP avec OpenLDAP

- La première entrée est la racine.
  - On la reconnaît au fait qu'elle appartient à la classe d'objet « **dcObject** ».
  - Elle appartient aussi à 2 autres classes d'objets.
    - **O**: organisation
    - **dc**: domain component
- La deuxième entrée est le compte administrateur LDAP, comme l'indique l'attribut « **description** »
  - Il appartient à la classe d'objets « **simpleSecurityObject** » qui représente les comptes d'authentification.

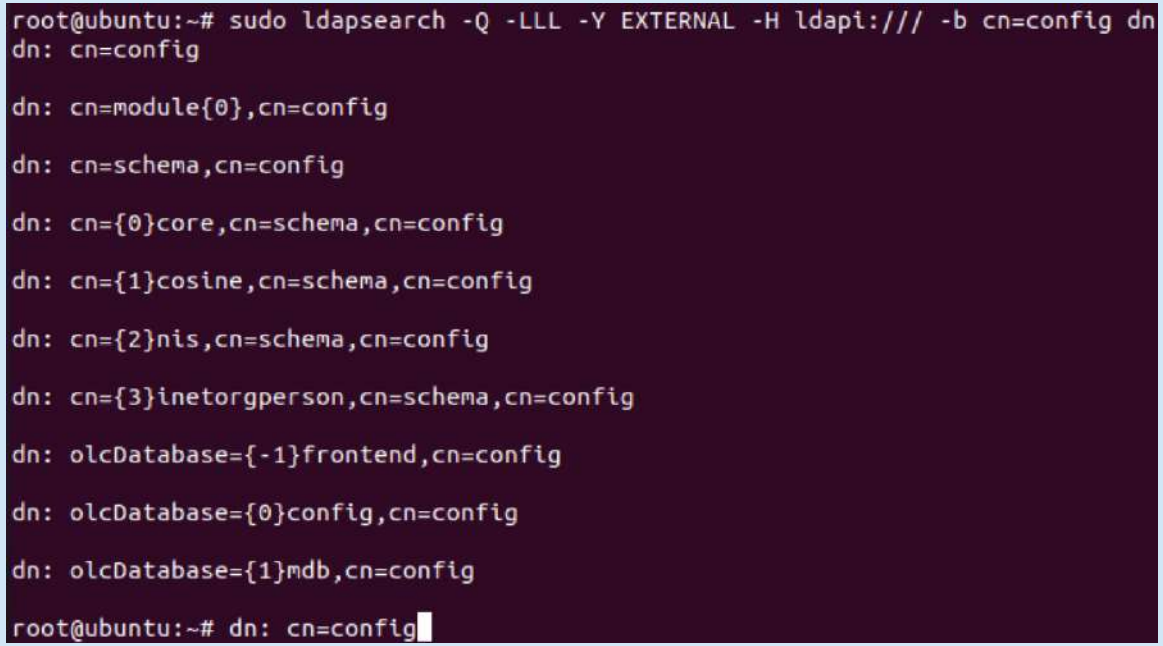


DIT contient en tout 2 entrées

Service LDAP avec OpenLDAP

- La configuration est gérée sous forme d'un DIT dont le suffixe est cn=config.
- Commande pour voir les entrées de cet arbre:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn dn: cn=config
```



Service LDAP avec OpenLDAP

- Pour ajouter de nouveaux nœuds et un premier utilisateur à notre arbre, nous allons utiliser un fichier LDIF.
- Nous allons créer le fichier « **structure.ldif** » suivant:
- Puis, ajouter le fichier avec la commande:

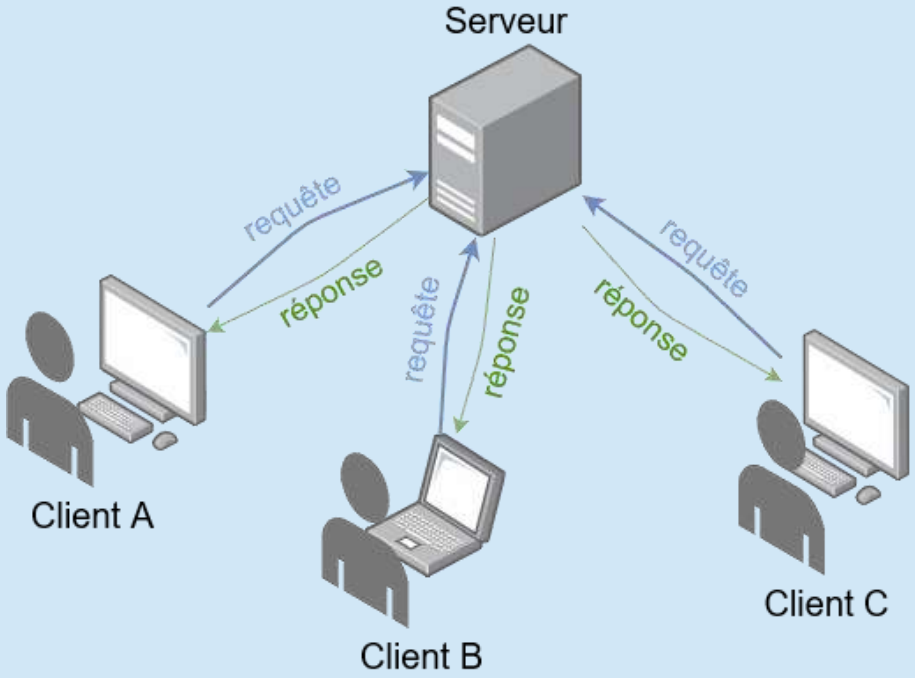
```
sudo ldapadd -x -W -D "cn=admin,dc=umc,dc=dz" -H
ldap://localhost -f structure.ldif.
```

- **-X**: indique une authentification simple par mot de passe
- **-W**: affiche une invite interactive pour taper le mot de passe du compte
- **-D**: pour indiquer le DN du compte à connecter
- **-H**: indique toujours la méthode de connexion choisie
- **-F**: fichier LDIF

```
dn: ou=Technologies dc=umc,dc=dz
objectclass: organizationalUnit
ou: Technologies
description: department technologies

dn: ou=Personnes,ou=Technologies dc=umc,dc=dz
objectclass: organizationalUnit
ou: Personnes
description: Employes de department technologies

dn: ou=groupes,dc=mon-entreprise,dc=com
objectclass: organizationalUnit
ou: Machines
description: Ordinateurs de l entreprise

dn: cn=Marie Dupond,
ou=Personnes,
dc=umc,
dc=dz
objectClass: inetOrgPerson
givenName: Meriem
sn: Dudou
cn: Meriem Dudou
uid: mdudou
userPassword: mdudou
```

Service DHCP

- Le Protocol DHCP (**Dynamic Host Configuration Protocol**) fonctionne sur le **mode client/serveur** et il va permettre a un équipement qui se connecte a un réseau, **d'obtenir une configuration réseau automatiquement**.
  - Adresse IP
  - Masque de sous-réseau
  - Adresse de la passerelle
  - Adresse du serveur DNS
- Offre une configuration fiable et simple des réseaux TCP/IP.
- Contrôle l'utilisation des adresses IP d'une manière centralisée.
- Permet d'eviter les erreurs de configuration.

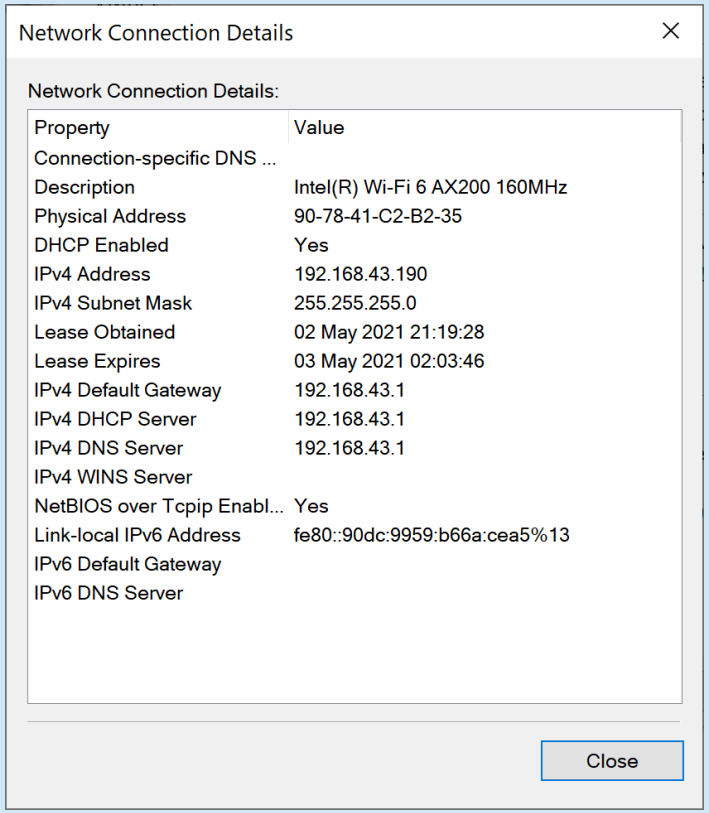


Service DHCP

- Quelques exemples de clients DHCP et de serveurs DHCP
  - **Client DHCP**: n'importe quel équipement se connecter sur un réseau filaire ou en Wi-Fi.

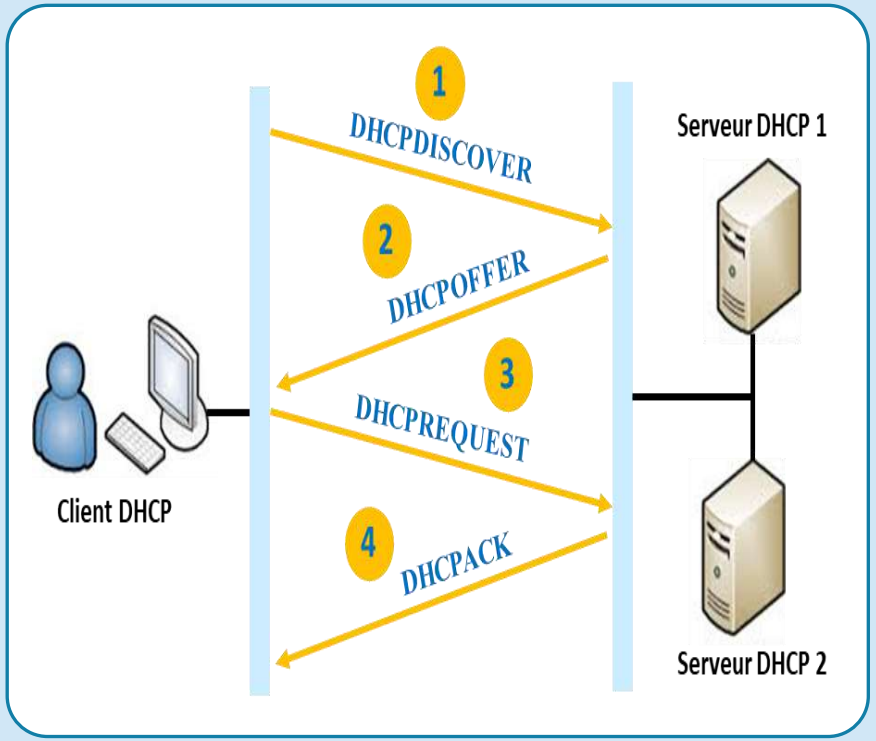
    Exemples: ordinateurs, smartphones, tablettes, serveurs, TV connectée, etc.
  - **Serveur DHCP:** il excite de nombreuses solutions logicielles pour créer un serveur DHCP.

    Exemples: le rôle DHCP sous Windows server, sous linux (paquet: isc-dhcp-server-server), a l'aide d'un routeur, d'un per-feu, etc.



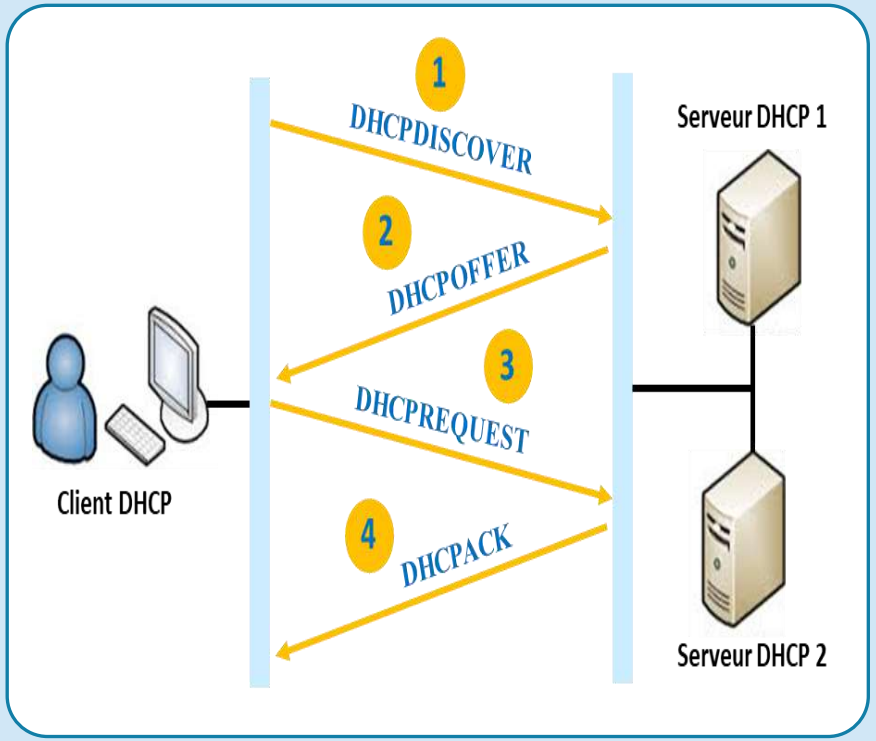
Fonctionnement de DHCP

- Grace au **broadcast**, la machine cliente va tenter de localiser un serveur DHCP disponible sur le réseau afin de négocier avec lui l'obtention d'une adresse IP.
- Au final, la machine obtient ce que l'on appelle, un **Bail DHCP** pour une durée déterminée.
- Utilise un processus en quatre étapes pour louer des informations d'adressage IP aux clients DHCP.
    - Découverte DHCP (Paquet: **DHCPDISCOVER**)
    - Offre DHCP (Paquet: **DHCPOFFER**)
    - Requête DHCP (Paquet: **DHCPREQUEST**)
    - Accusé de reception DHCP (Paquet: **DHCPACK**)



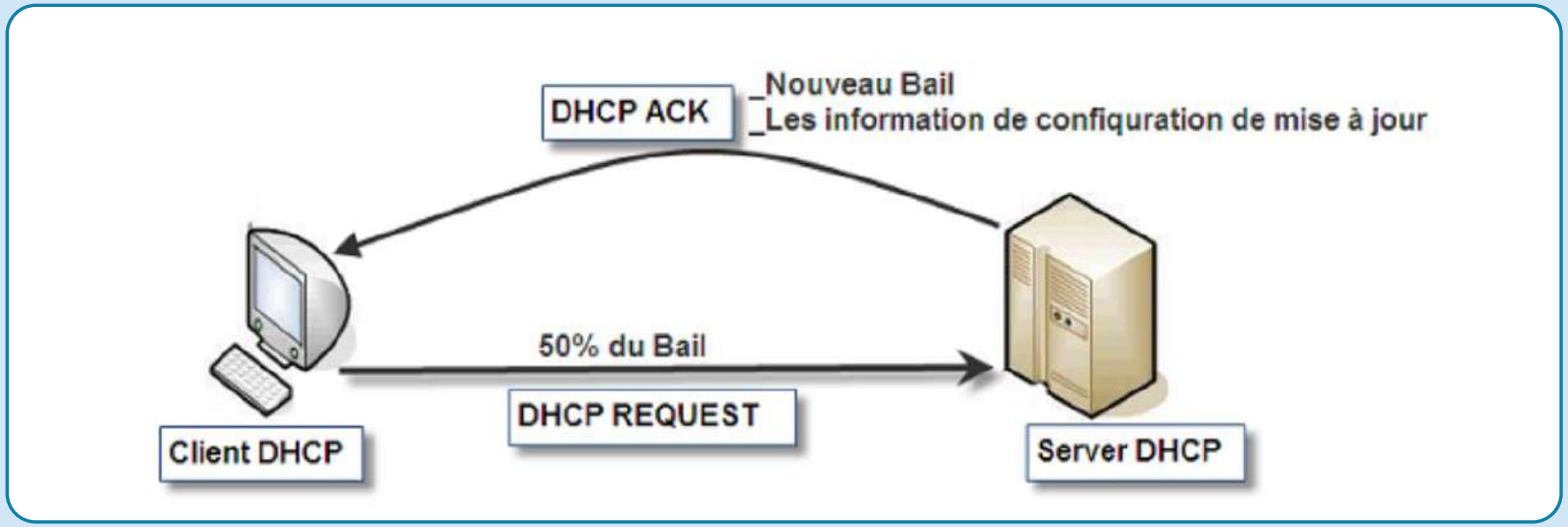
Fonctionnement de DHCP

- Le dialogue est décrit de la manière suivante:
  1. Le client émet une requête de demande de **bail IP** qui est envoyé sous forme d'une diffusion sur le réseau avec adresse IP source (**0.0.0.0**), adresse IP destination (**255.255.255.255**) et adresse **MAC**.
  2. Le serveur DHCP répond en proposant une adresse IP avec une durée de bail et l'adresse IP du serveur DHCP (**DHCOFFER**).
  3. Le client sélectionne la première adresse IP (s'il y a plusieurs serveurs DHCP) reçue et envoie une demande d'utilisation de cette adresse au serveur DHCP (DHCPREQUEST).
  4. Le serveur DHCP accuse réception de la demande et accorde l'adresse en bail (DHCPACK).



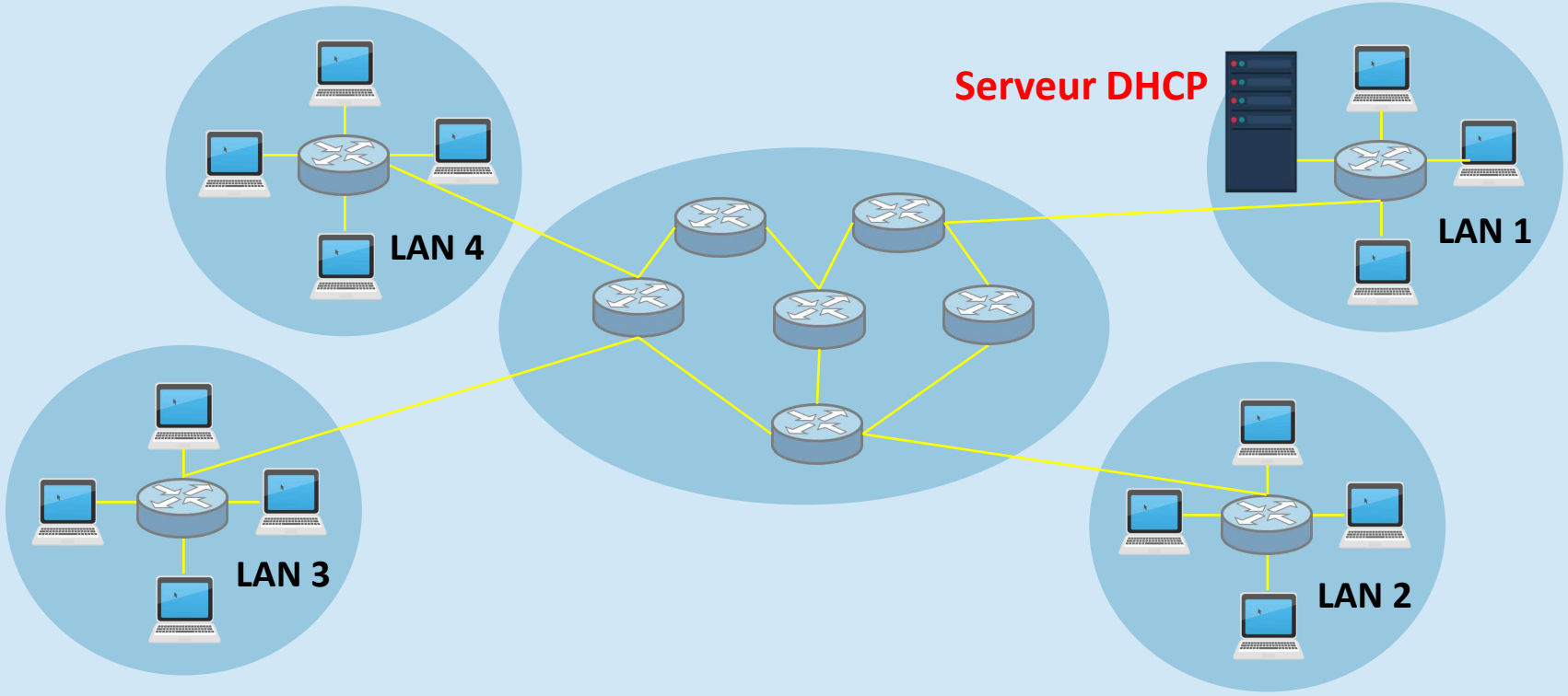
Fonctionnement de DHCP

- Le client DHCP tente automatiquement de renouveler son bail lorsque sa durée a expiré de 50%.
- Lors d'un renouvellement, le client va directement envoyer un paquet **DHCPREQUEST** pour demander une prolongation du Bail.



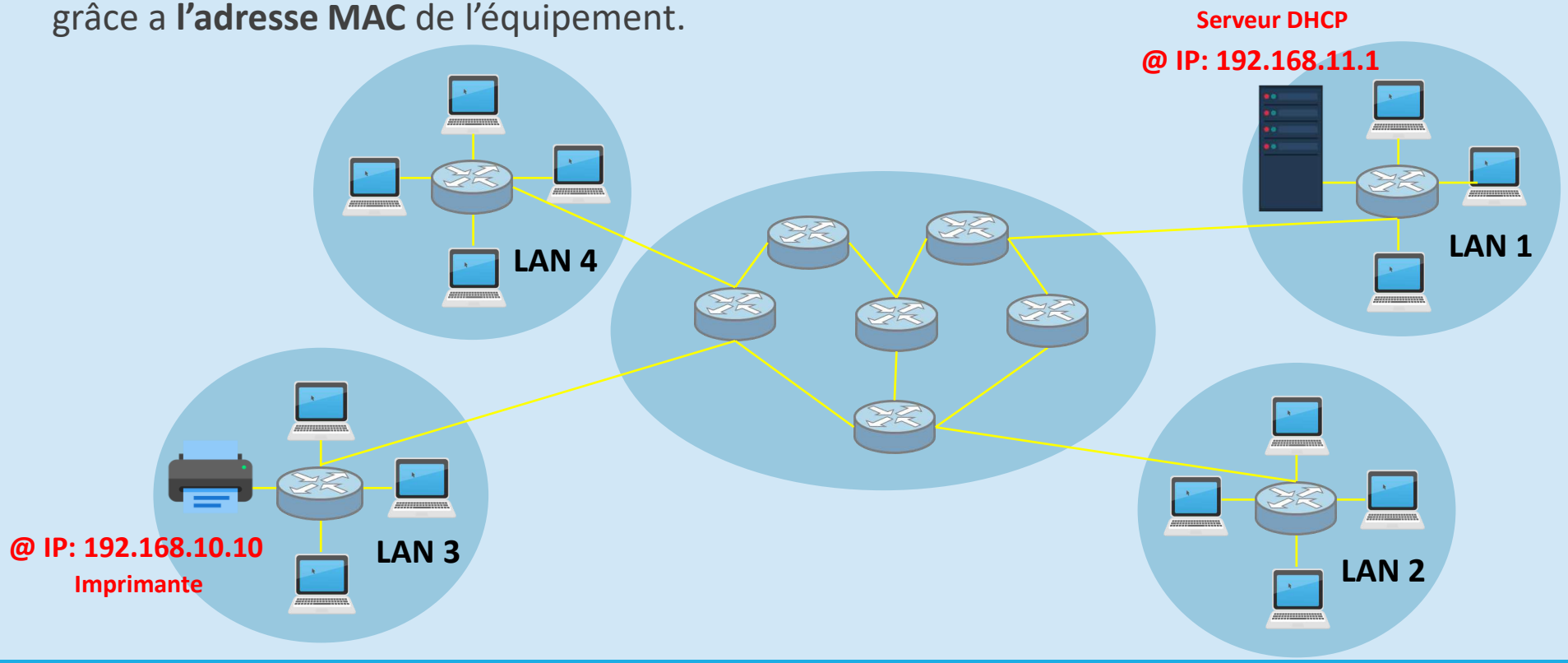
Etendue (Pool) DHCP

- Sur un réseau où l'on trouve plusieurs réseaux différents, que ce soit des **réseaux physiques (LANs) ou logiques (VLANs),** le serveur DHCP doit gérer **les pools d'adresses IP** à distribuer pour chaque réseau. C'est ce que l'on appelle **étendue**.



Réservation DHCP

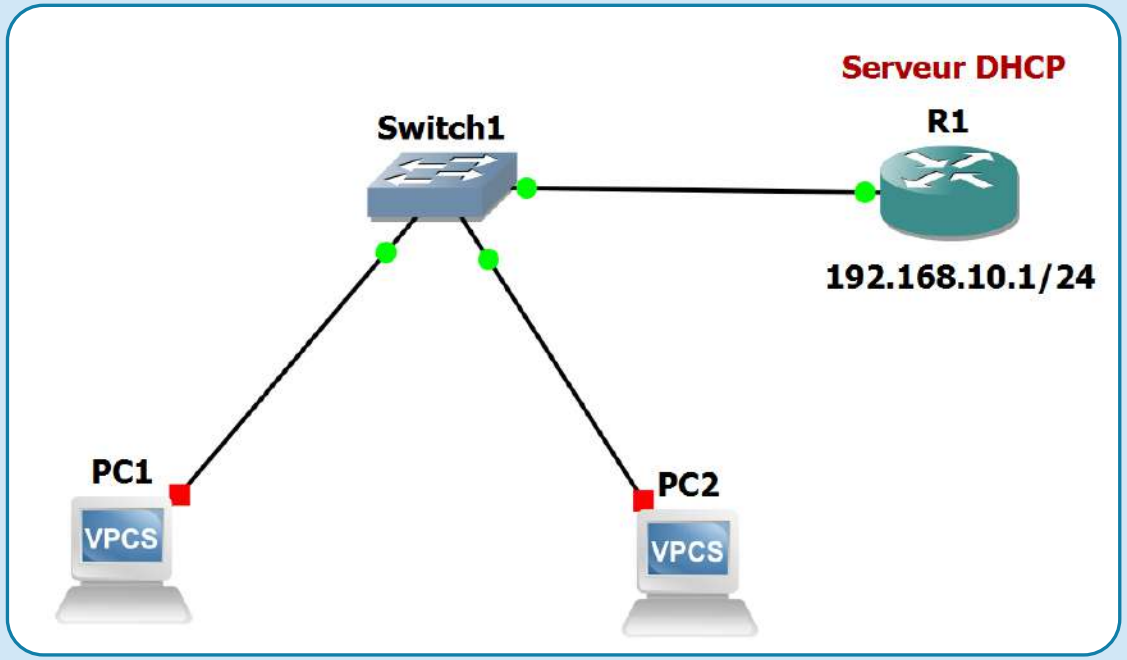
- Une adresse **IP réservée** dans un serveur DHCP ne pourra pas être distribuée, sauf à l'équipement pour lequel elle est destinée. Par exemple, une imprimante, un serveur DNS, etc. Cette association se fait grâce a **l'adresse MAC** de l'équipement.



Fonctionnement de DHCP

- Pour les réseaux de petite taille, les services DHCP peuvent être fournis par un **petit routeur**
- **Méthode de configuration**

1. Configurer l'interface du routeur
2. Exclure les adresses qu'on souhait ne pas distribuer (Ex: celle de la passerelle, ou de machines ayant des adresses fixes).
3. Configuration du service DHCP sur le routeur
4. Configuration des PC1 et PC2 comme clients DHCP



Fonctionnement de DHCP

- Configuration de l'interface du routeur

```
R1#Config t
R1(config)#int f0/1
R1(config-if)#ip add 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1 # show ip interface brief
```

- Exclure les adresses qu'on souhait ne pas distribuer (Ex: celle de la passerelle, ou de machines ayant des adresses fixes).

```
R1#Config t
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
```

Fonctionnement de DHCP

- Configuration du service DHCP sur le routeur

```
R1#Config t
R1(config)#ip dhcp pool LAN1   //On a créé ici un pool DHCP nommé LAN1
R1(dhcp-config)#network 192.168.10.0 255.255.255.0 // Plage d'adresses
R1(dhcp-config)#default-router 192.168.10.1 //passerelle par défaut
R1(dhcp-config)#dns-server 8.8.8.8 //un serveur DNS 8.8.8.8
R1(dhcp-config)#domain-name zarzara.com //nom du domaine
R1(dhcp-config)#lease infinite //durée de bail
R1(dhcp-config)#end
```

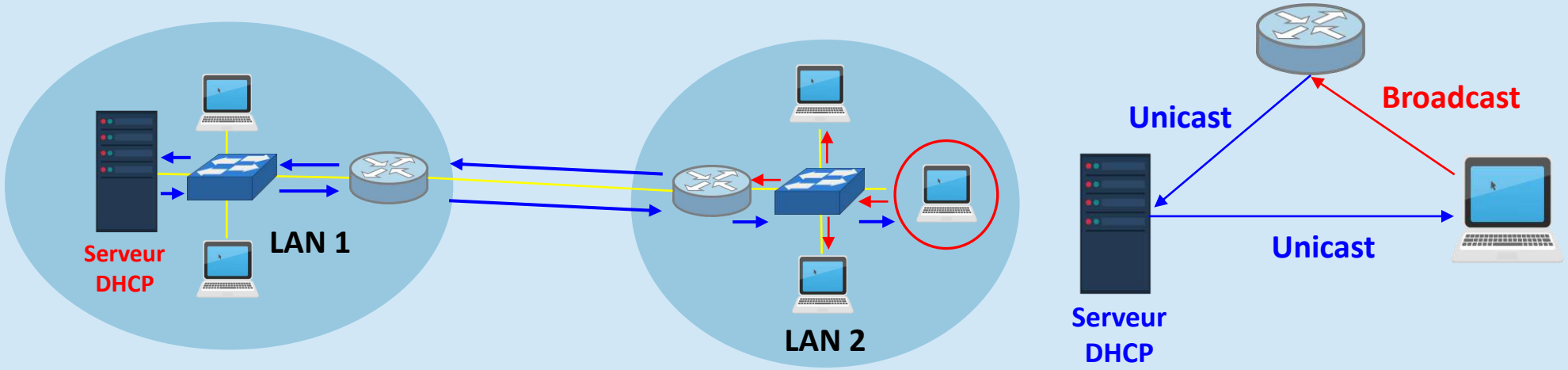
- Configuration des PC1 et PC2 comme clients DHCP

```
PC1>ip dhcp
PC1> show ip
```

```
PC1> Cannot resolve pc2
PC1> sh ip

NAME        : PC1[1]
IP/MASK     : 10.1.0.1/16
GATEWAY     : 10.1.255.254
DNS         : 10.1.255.253
DHCP SERVER : 10.1.255.254
DHCP LEASE  : 0, 4294967295/2147483647/536870911
DOMAIN NAME : zarzara.com
MAC         : 00:50:79:66:68:00
LPORT       : 10001
RHOST:PORT  : 127.0.0.1:10000
MTU:        : 1500
```

Agent de relais DHCP

- Une requête DHCP ne passe pas les retours (broadcast), alors **comment faire pour joindre un serveur DHCP situé sur un autre réseau?**
- **Solution: Agent de relais DHCP (exemple: Routeur, Per-feu).**



Service DNS

- **DNS**: Domain Name System.
- **Le DNS va permettre de traduire les noms de domaine en adresse IP. Les noms de domaine sont plus explicites et plus facile à utiliser**.
- Il permet à des hôtes du réseau de soumettre des requêtes à un serveur DNS afin d'obtenir l'adresse IP d'un hôte connaissant le nom de cet hôte (FQDN).

  Exemple: **www.google.com** ↔ **209.85.229.99**. Cette traduction des noms aux adresses IP doit toujours être réalisée puisque seule l'adresse IP permet de communiquer sur le réseau.
- **Autre usages**: association d'un serveur de messagerie à un nom de domaine.

La résolution DNS

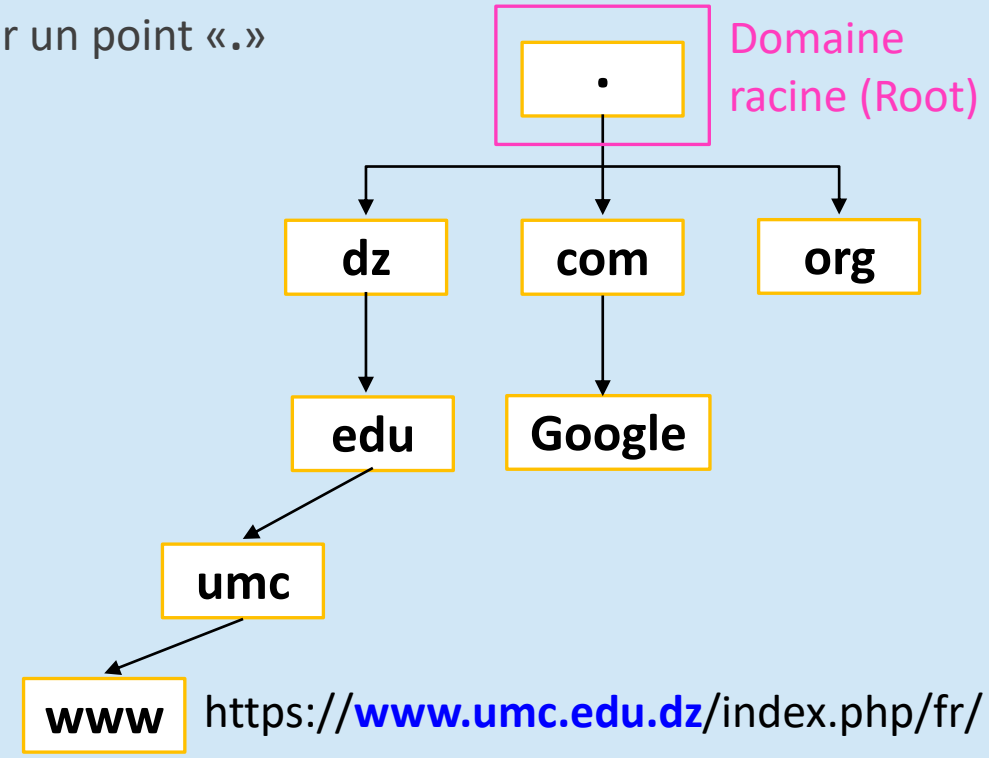
- **Comment retrouver l'adresse IP associée au nom du domaine?.**

  Le DNS possède un modèle hiérarchique dont le sommet est appelé **Domaines racines (Root)**. On représente ce dernier par un point «.»

  Il y a apparemment 13 serveurs racine du DNS dont les noms sont de la forme **lettre.root-servers.net**

  Exemples

  - A.root-servers.net,
  - B.root-servers.net,
  - …,
  - M.root-servers.net,
  - ….



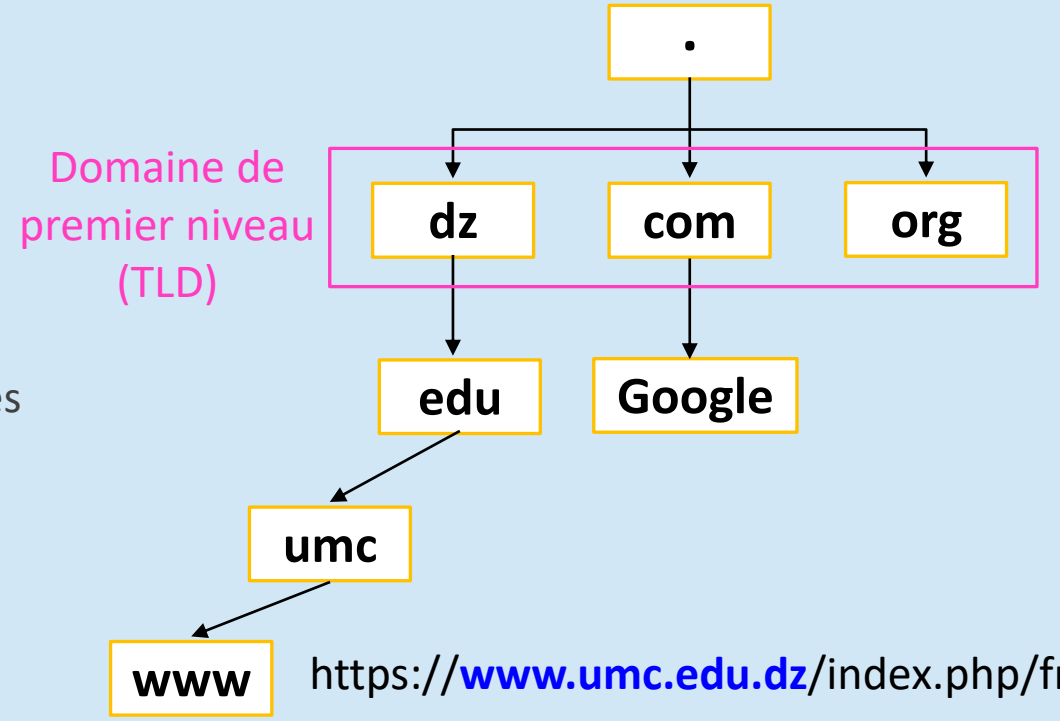
La résolution DNS

- **Comment retrouver l'adresse IP associée a nom du domaine?**.

  TLD: Les domaines se trouvant immédiatement sous la racine sont appelés domaine de premier niveau (**TLD : Top Level Domain**).

  Il existe deux catégories de TLD :

  - **Générique** : les domaines génériques, aussi appelés **gTLD** (pour generic TLD), sont des noms de domaines génériques de niveau supérieur proposant une classification selon le secteur d'activité, comme « .org », « .edu », « .net », « .gov » où « .com ».
  - **Nationaux :** les domaines nationaux, aussi appelés **ccTLD** (pour country code TLD), correspondent aux différents pays et leurs noms correspondent aux abréviations des noms de pays définies par la norme **ISO 3166**, comme **dz** (Algeria), **it** (Italy), **uk** (United Kingdom), **fr** (France), etc.



La résolution DNS

- **Comment retrouver l'adresse IP associée a nom du domaine?**

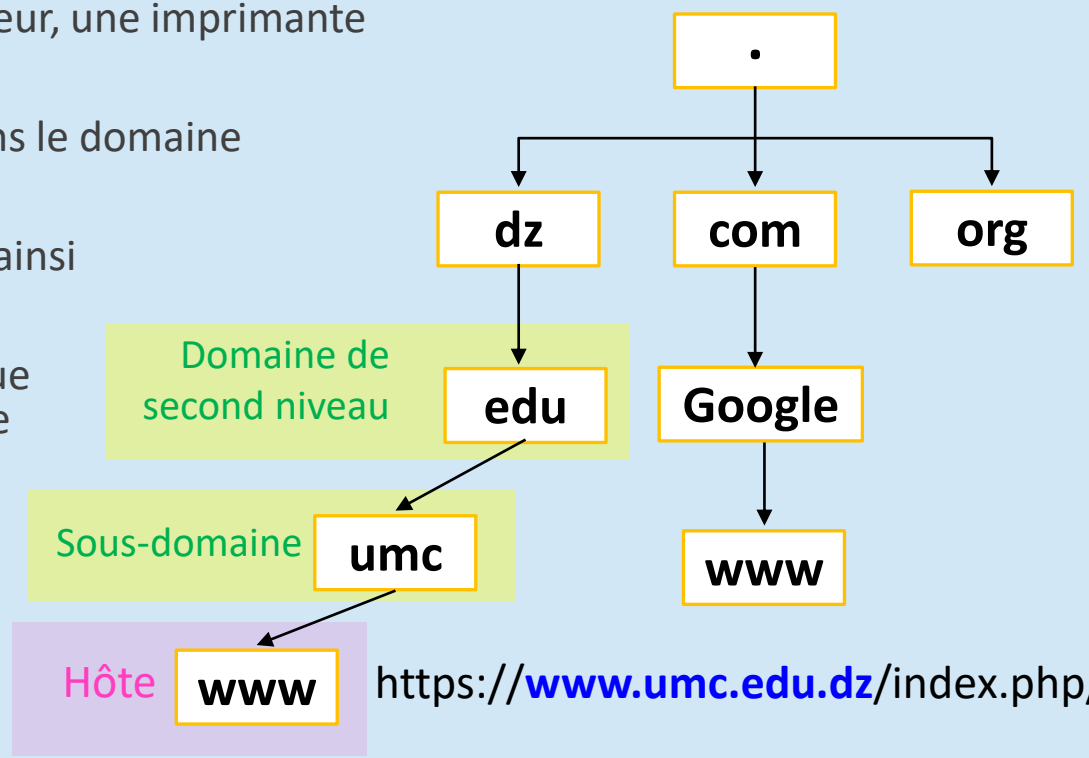
  Hôte: L'extrémité d'une branche est appelée **hôte**, et correspond à une machine ou une entité du réseau (**e.g**. un ordinateur, une imprimante ou bien encore un routeur).

  Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine.

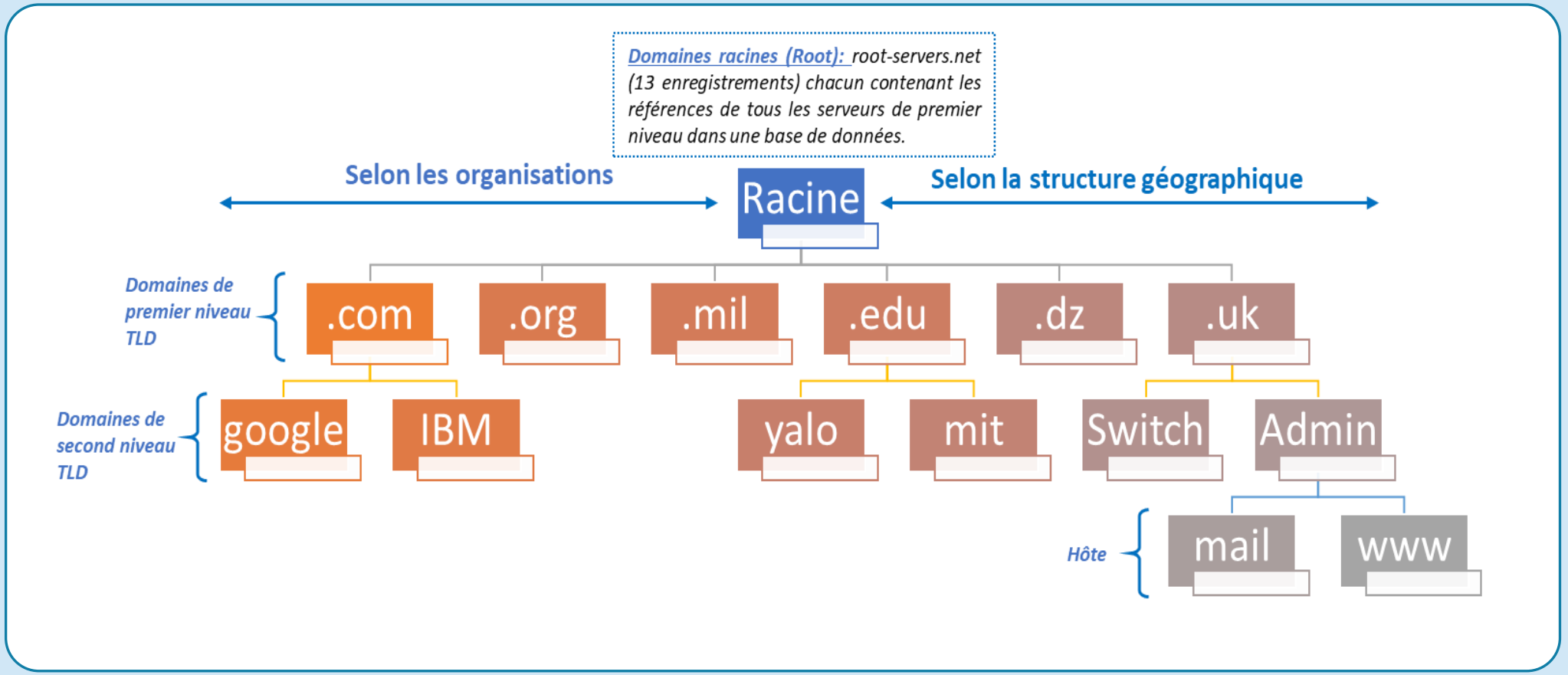
  À titre d'exemple le serveur web d'un domaine porte ainsi généralement le nom **www**.

  Nom de domaine : on appelle nom de domaine chaque nœud de l'arbre. Chaque nœud possède une étiquette (en anglais « label ») d'une longueur maximale de **63 caractères**.

  FQDN : le nom de domaine pleinement qualifié ou FQDN (Fully Qualified Domain Name) est composé de deux parties : les noms d'hôte et le suffixe DNS. Par exemple, **www.umc.edu.dz**.

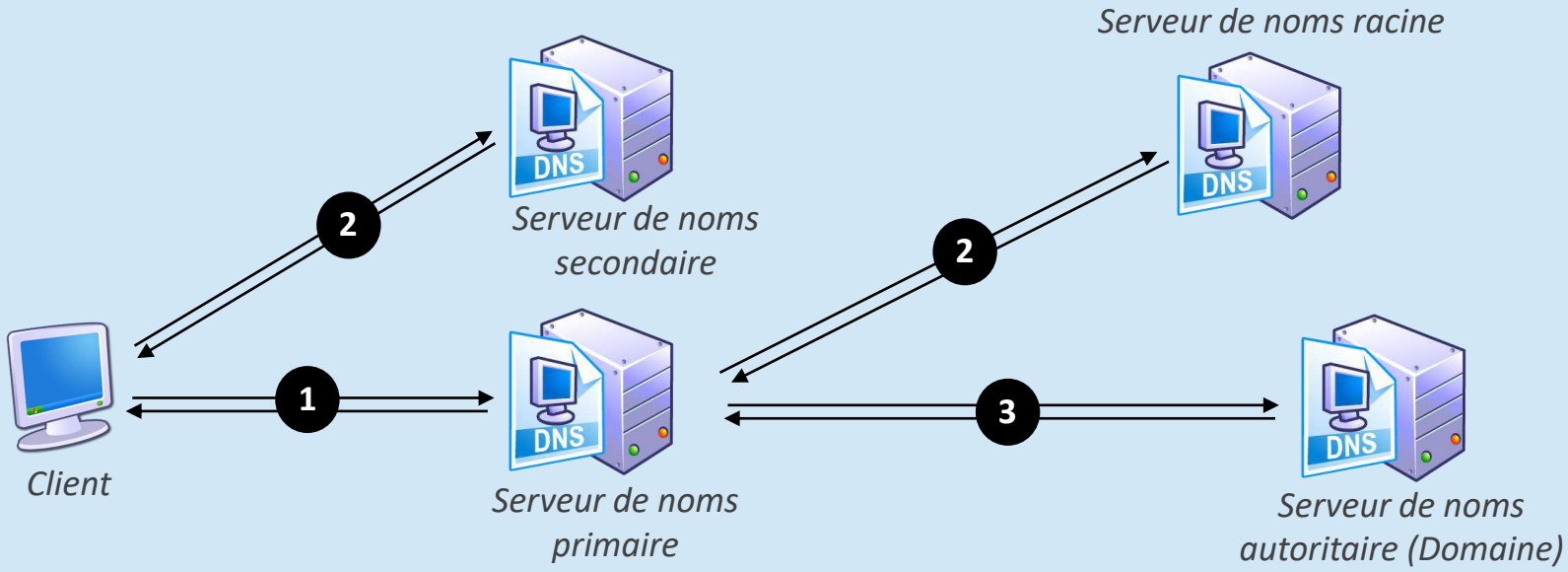


La résolution DNS



La résolution DNS

- Chaque domaine possède un serveur de noms de domaines, appelé **serveur de noms primaire** (Primary domain name server), ainsi qu'un **serveur de noms secondaire** (Secondary domaine name server), permettant de prendre le relais du serveur de noms primaire en cas d'indisponibilité.



La résolution DNS

- **Requête DNS**: est une demande de résolution de noms envoyée à un serveur DNS par un client.
- Les requêtes DNS sont effectuées via le protocole DNS (il s'appuie sur **UDP**, sur le port **53**).
- La résolution d'un nom à l'aide du DNS.

Client
http://www.google.com

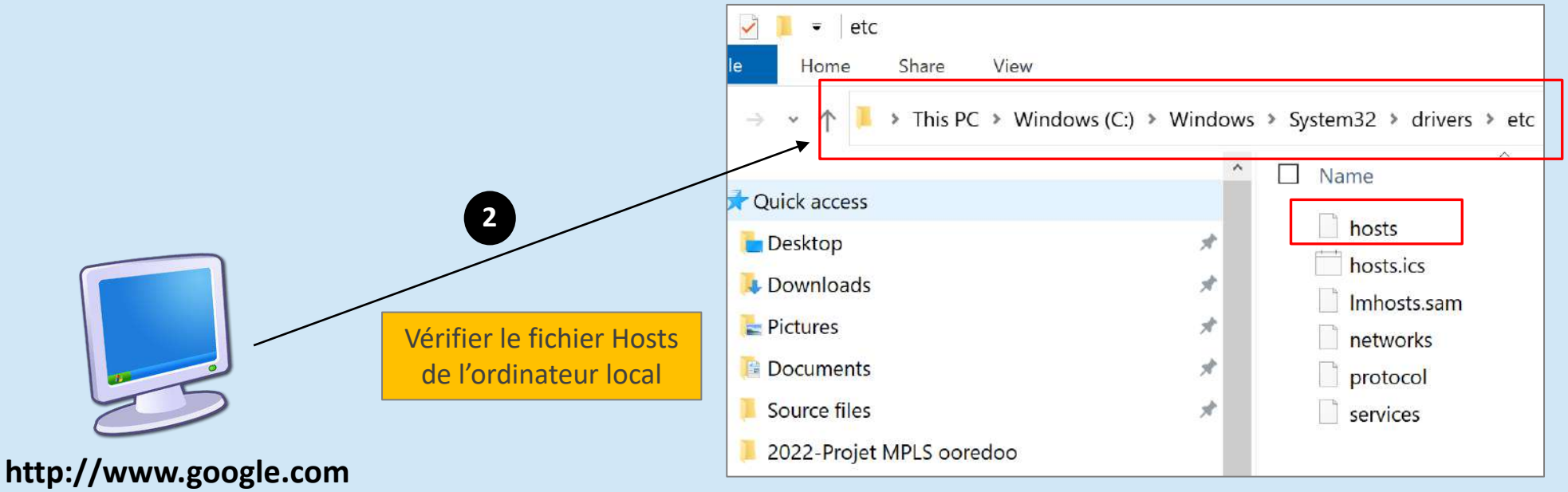
1

Vérifier la cache DNS de l'ordinateur local: la commande **ipconfig /displaydns**

```
Command Prompt
Microsoft Windows [Version 10.0.18363.1440]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\gueltoum bendiab>ipconfig /displaydns

Windows IP Configuration

    safebrowsing.googleapis.com
    ----------------------------------------
    Record Name . . . . . : safebrowsing.googleapis.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 73
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 142.250.200.202

    www.gstatic.com
    ----------------------------------------
    Record Name . . . . . : www.gstatic.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 172
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 142.251.37.227

    ogs.google.com
    ----------------------------------------
    Record Name . . . . . : ogs.google.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 196
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : www3.l.google.com

    Record Name . . . . . : www3.l.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 196
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 142.250.201.14
```

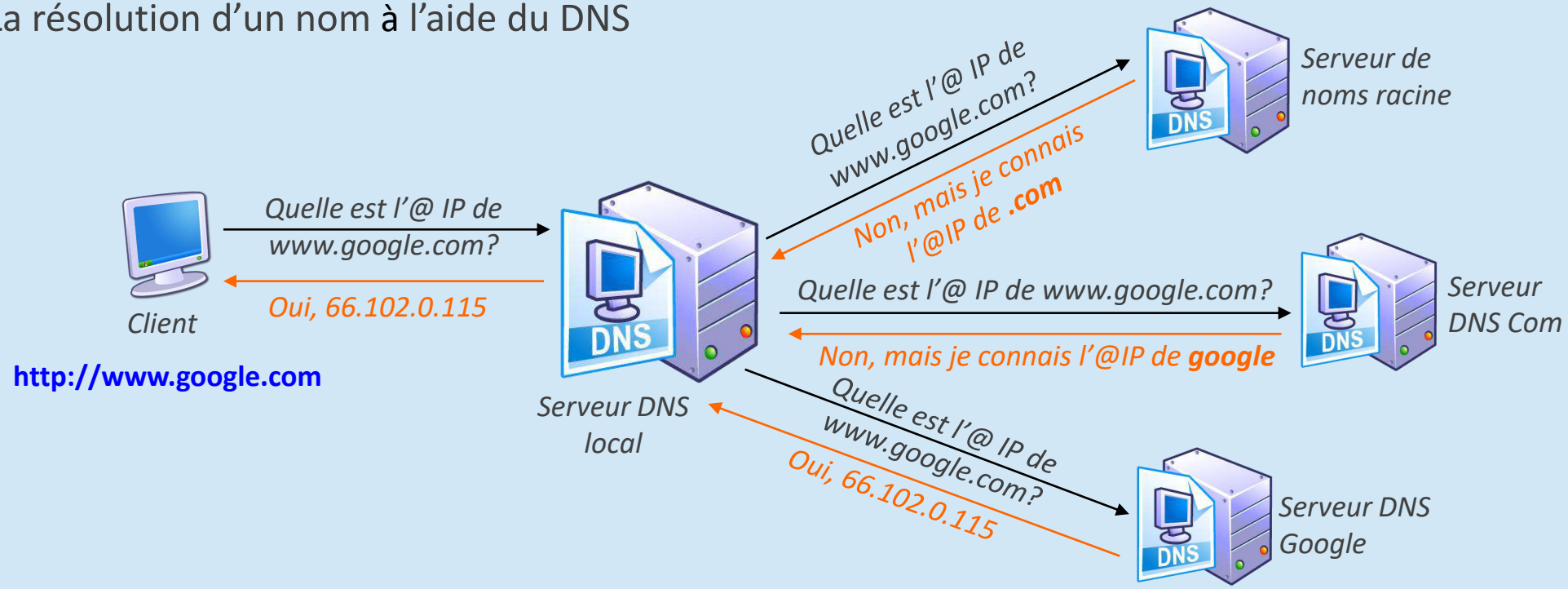
La résolution DNS

- **Requête DNS**: est une demande de résolution de noms envoyée à un serveur DNS.
- Les requêtes DNS sont effectuées via le protocole DNS (il s'appuie sur **UDP**, sur le port **53**).
- La résolution d'un nom à l'aide du DNS



La résolution DNS

- **Requête DNS**: est une demande de résolution de noms envoyée à un serveur DNS.
- Les requêtes DNS sont effectuées via le protocole DNS (il s'appuie sur **UDP**, sur le port **53**).
- La résolution d'un nom à l'aide du DNS



Zone DNS

- **Zone DNS** : se réfère à l'espace administratif dans le DNS. C’est un fichier où se trouvent **les enregistrements d'un domaine**.
- Les fichiers de zone sont gérés sur des **serveurs DNS.**
- Un serveur DNS peut être configuré pour héberger **zéro**, une ou **plusieurs zones**.
- Chaque zone peut faire autorité pour un ou plusieurs domaines DNS, à condition que ces domaines soient contigus dans l’arborescence DNS.

Enregistrements DNS

- **Enregistrements DNS**: Les enregistrements sont les liens entre les adresses IP et les noms, cela sert donc à la résolution de nom. Seuls les administrateurs de la gestion de domaine peuvent lire les informations de ces enregistrements.
- Un enregistrement DNS comporte plusieurs informations comme:
  - **Nom de domaine (FQDN)** : exemple, www.admin.uk,
  - **TTL (Time To Live)** :36000 seconds
    (Au bout de ce temps, la cache du serveur sera réinitialisée).
  - **Type** : exemple, SOA,
  - **Données** : exemple, 136.5.255.85.

```
beacons.gvt2.com
----------------------------------------
Record Name . . . . . : beacons.gvt2.com
Record Type . . . . . : 1
Time To Live  . . . . : 189
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 216.58.198.67
```

Enregistrements DNS

Il existe plusieurs types d'enregistrements DNS comme par exemple :

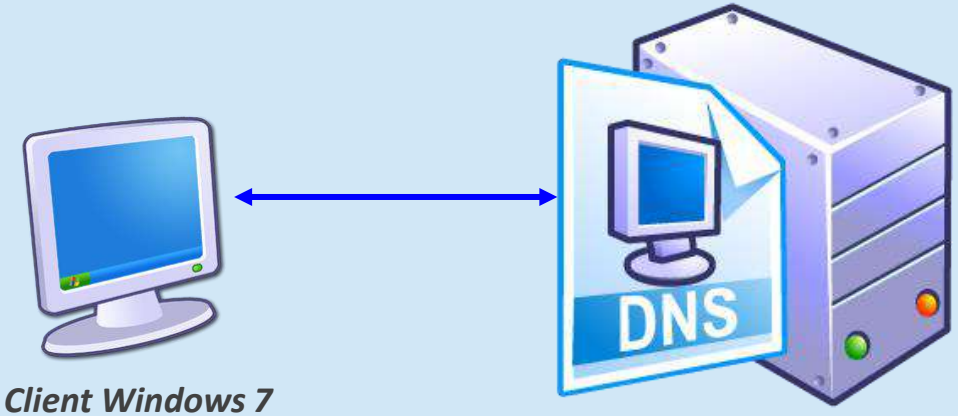
- **SOA (Start Of Authority)** : permet de définir le serveur maitre du domaine,
- **NS (Name Server)** : indique quel nom de serveur a autorité sur le domaine,
- **MX (Exchanger Record)** : gère la liste des serveurs de messageries,
- **A (Address)** : gère la liste des adresses IP (IPv4) des hôtes, et AAAA (IPv6),
- **CNAME (canonical name)**: abréviation de canonique. Elle permet de réaliser un alias (un **raccourci**) d'un hôte vers un autre.
- **PTR** (pointer record): résolution inverse
- **TXT**: enregistrement libre, souvent utiliser pour le SPF (Sender Policy Framework): stocke la liste les serveurs autorisés à envoyer des e-mails depuis un domaine particulier.

```
mail.google.com
----------------------------------------
Record Name . . . . . : mail.google.com
Record Type . . . . . : 5
Time To Live  . . . . : 17
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : googlemail.l.google.com


Record Name . . . . . : googlemail.l.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 17
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 216.58.211.197
```

Configuration d'un Serveur DNS

Nous allons essayer d'installer et de configurer un serveur DNS sous Windows. Pour ce faire, nous allons utiliser la topologie réseau suivante:

- Créer une nouvelle machine virtuelle VMware, puis démarrer la machine virtuelle et installer **Windows 2003 Server** à partir de l'image iso de ce dernier.
- Créer une autre machine virtuelle VMware, puis démarrer la machine virtuelle et installer **Windows 7** à partir de l'image iso de ce dernier
- Serveur DNS :
  - nom →umc,
  - adresse IP→137.59.136.1/16
- Machine cliente :
  - nom →win7,
  - adresse IP→137.59.136.4/16



Client Windows 7
192.168.10.15

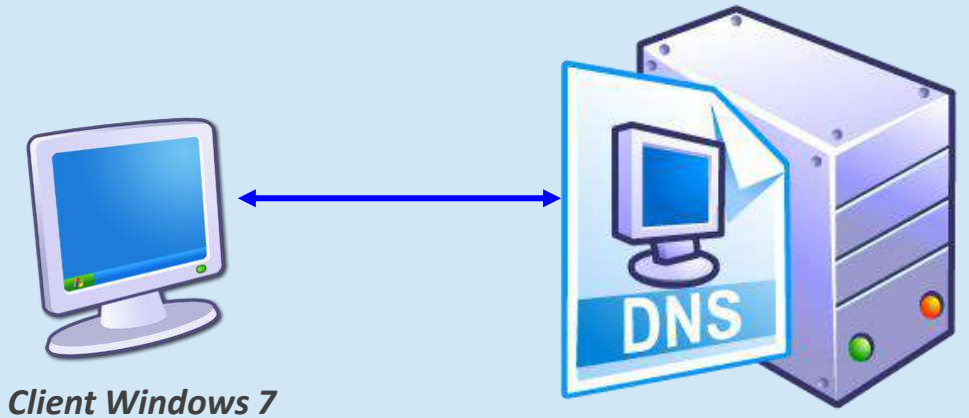
Serveur DNS
192.168.10.3

Configuration d'un Serveur DNS

Nous allons essayer d'installer et de configurer un serveur DNS sous Windows. Pour ce faire, nous allons utiliser la topologie réseau suivante:

- Installer un serveur DNS sur votre serveur, puis vérifier dans le "Server Manager" que le rôle DNS a bien était ajouté.
- Configurer votre serveur DNS selon les paramètres suivants :
  - type de serveur : **primaire**,
  - nom de domaine : **zarzara.edu**,
  - nom de fichier de configuration de votre serveur DNS :**zarzara.edu.umc**,
  - les dresses des DNS public sur lesquels notre serveur ira chercher les noms de site internet sont les célèbres serveurs DNS de google **8.8.8.8** et **8.8.4.4**.

https://dns.google/



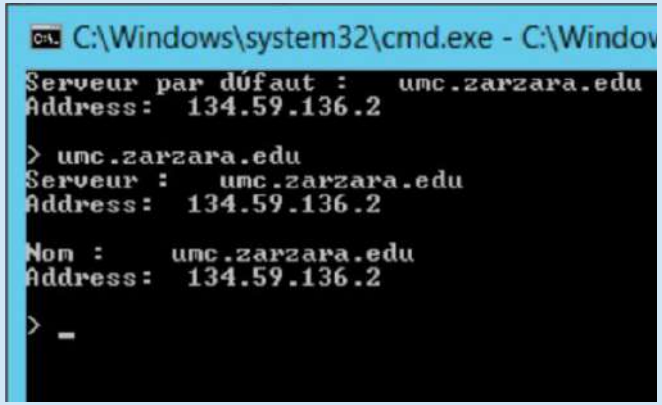
Client Windows 7
192.168.10.15

Serveur DNS
192.168.10.3

Configuration d'un Serveur DNS

La configuration de serveur DNS consiste à créer les deux zones de recherche directe et inversée, nécessaires au fonctionnement du DNS.

- **La zone de recherche directe** prend en charge la résolution des noms d'hôtes en adresses IP.
  - nom de domaine : zarzara.edu,
  - type : Zone principale,
  - fichier de configuration du serveur DNS : zarzara.edu.dns
- **La zone de recherche inversée** effectue la résolution des adresses IP en noms d'hôtes. Cette zone est surtout indispensable pour les serveurs de messagerie.
  - type : Zone principale,
  - identifiant réseau :192.168.10.0,
  - fichier de configuration 0.10.168.192.in-addr.arpa.dns



Après la configuration du serveur DNS, nous avons testé le fonctionnement de ce dernier en utilisant la commande Nslookup (Name System Look Up) pour interroger le serveur et obtenir les informations concernant le domaine