Lightweight Directory Access Protocol (LDAP)

Thierry Delot

Laboratoire PRiSM
Université de Versailles St-Quentin

LDAP : Concepts

- **qu'est-ce qu'un annuaire ?**
  - Stockage et consultation d'informations
  - Dédié à la lecture plus qu'à l'écriture
  - Accès se fait par recherche multi-critères
- **Un annuaire électronique, c'est en plus :**
  - un protocole d'accès
  - un modèle de distribution
  - un modèle de duplication de l'information
  - un contenu évolutif : des informations complémentaires peuvent être ajoutées
- **Exemple : DNS**
  - www.prism.uvsq.fr → adresse IP correspondante
  - service d'annuaire global : contexte élargi à un intranet ou à l'Internet par opposition à un service local

LDAP : Historique

- **X500 (proposé par l ’ISO)**
  - Standard conçu par les opérateurs telecom pour interconnecter leurs annuaires téléphoniques
  - Les limites :
    - performances “ insuffisantes”
    - utilisation des protocoles ISO
    - Modèle de données de type objet
- **LDAP (“Lightweight Directory Access Protocol”)**
  - basé sur X500 DAP et adapté à l’Internet
    - Même modèle pour le schéma, le nommage et la manipulation
    - API facile à utiliser
    - TCP/IP au lieu des protocoles ISO
    - La plupart des éléments manipulés sont des chaînes de caractères
  - proposé par l’IETF (Internet Engineering Task Force) in 1995
    - standard d ’annuaire sur TCP/IP : RFC 1487(v1), RFC 1777(v2), RFC 2251(v3)
    - Première implémentation à l’université du Michigan
    - Plusieurs produits commerciaux (IBM, Microsoft, Netscape, Oracle, Sun, etc).

Plan

- **Protocole**
- **Modèle d’information**
- **Modèle de nommage**
- **Modèle fonctionnel**
- **Modèle de sécurité**
- **Modèle de duplication**
- **Architecture**

LDAP : protocole

- **Le protocole définit :**
  - comment s'établit la communication client-serveur
    - bind, unbind, abandon
  - comment s'établit la communication serveur-serveur
    - synchronisation (replication service)
    - liens entre différents annuaires (referral service)
  - Transport des données :
    - pas l'ASCII (http, smtp, …) mais Basic Encoding Rules (BER)
  - Les mécanismes de sécurité
    - Méthodes de chiffrement et d'authentification
    - Mécanismes d'accès aux données
  - Les opérations de base
    - search, add, delete, etc.

LDAP : modèle d'information

- **Le modèle d'information définit le type des données pouvant être stockées dans l'annuaire**

- **L'entrée :**
  - Élément de base de l'annuaire
  - Contient les informations sur un objet de l'annuaire
  - Ces informations sont représentées sous forme d'un ensemble de paires (attribut, valeur)
  - Chaque entrée doit appartenir à une classe particulière
  - A chaque attribut est associé un type et une ou plusieurs valeurs
  - Les attributs d'une entrée peuvent être obligatoires ou optionnels

LDAP : modèle d'information

- **Schéma de l'annuaire :**
  - définit pour le serveur l'ensemble des définitions relatives aux objets qu'il sait gérer
  - décrit les classes d'objets, leurs types d'attributs et leur syntaxe
- **Vérification de schéma :**
  - A chaque création d'entrée, le serveur vérifie si elle est conforme à sa (ses) classe(s) d'appartenance
- **Flexibilité du schéma**
  - attributs optionnels
  - attributs multi-valués
- **Avec LDAPv3, obligation pour un serveur de publier son schéma via LDAP en le stockant dans l'entrée *subschema***

LDAP : modèle d'information

- **Attributs :**
  - caractérisés par un nom, un nom alternatif, un type et un Object Identifier (OID)
    - Le type le plus employé : chaînes de caractères, mais également des champs d 'octets pour stocker des images…
  - Attributs opérationnels maintenus par le serveur
    - ex : creatorsName, modifiyTimestamp, …

Exemple d'attributs définissant une entrée

type d'attribut	Valeur d'attribut
cn:	Lætitia Casta
uid:	lcasta
telephonenumber:	+33 (0) 1 4852 7738
mail:	Laetitia.Casta@inria.fr
roomnumber:	C105

LDAP : modèle d'information

- **Classes d'Objets (Object class) :**
  - Spécifie la liste des attributs obligatoires et optionnels
  - 3 Types de classes d 'objets :
    - structurelle : description des objets de l'annuaire (personnes, groupes, ...)
    - auxiliaire : objets qui permettent d 'ajouter des infos complémentaires
    - abstraite : objets basiques de LDAP (top, alias)
  - Ensemble de classes d 'objets standardisées pour assurer l'intéropérabilité mais possibilité d'en définir de nouvelles selon les besoins.
  - Exemples :
    - une organisation : Organization (o)
    - ses départements : OrganizationUnit (ou)

LDAP : modèle d'information

- **Classes d'Objets (Object class) :**
  - La classe d'objet d'une entrée est spécifiée à l'aide de l'attribut *objectclass*
  - Les classes d'objets forment une hiérarchie
    - au sommet de cette hiérarchie se trouve l'objet **top**
    - chaque objet hérite des propriétés (attributs) de l'objet dont il est le fils
- **Exemple :**
  - l 'objet inetOrgPerson a la filiation suivante :

objectclass: top
objectclass: person
objectclass: OrganizationalPerson
objectclass: inetOrgPerson

LDAP : modèle de nommage

- **Directory Information Tree (DIT)**
  - Les entrées gérées par le serveur LDAP sont toutes nommées
  - L'espace de nommage est organisé sous la forme d'un arbre
  - LDAP ne permet pas de limiter les relations de contenance entre classes d'objets : tout est permis.

LDAP : modèle de nommage

- **Nommage hiérarchique des entrées**
  - chaque entrée gérée est nommée de deux manières :
    - Relative Distinguished Name (RDN)

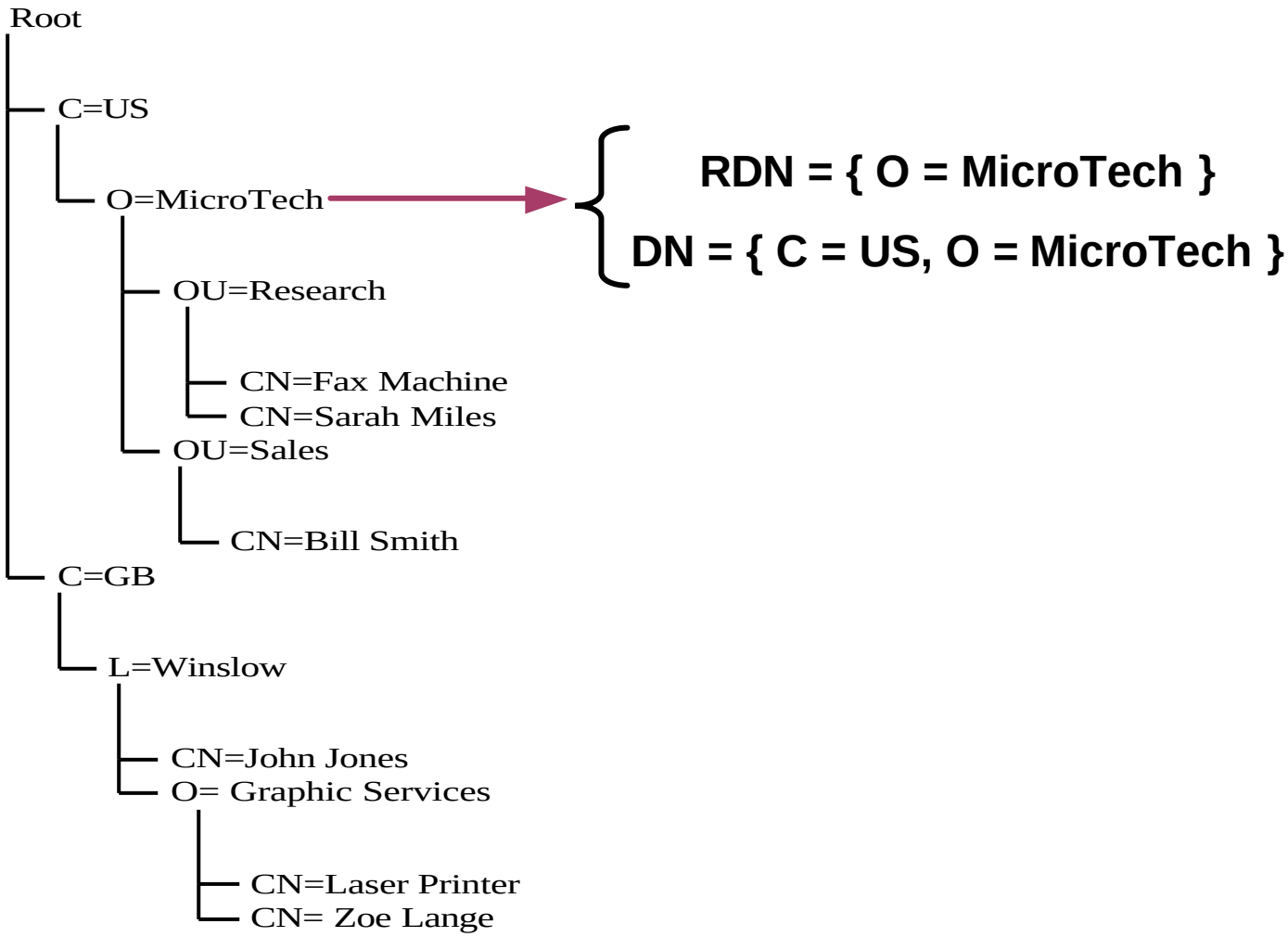
      ex : **RDN = { O = MicroTech }**
    - Distinguished Name (DN)

      ex : **RDN = { C = US, O = MicroTech }**

- **Les hiérarchies de classes et d'instances sont orthogonales**
  - l'objectclass 'person' n'hérite pas de l'objectclass 'organization'
  - une entrée représentant une personne peut avoir comme parent une entrée représentant une organisation

LDAP : modèle de nommage

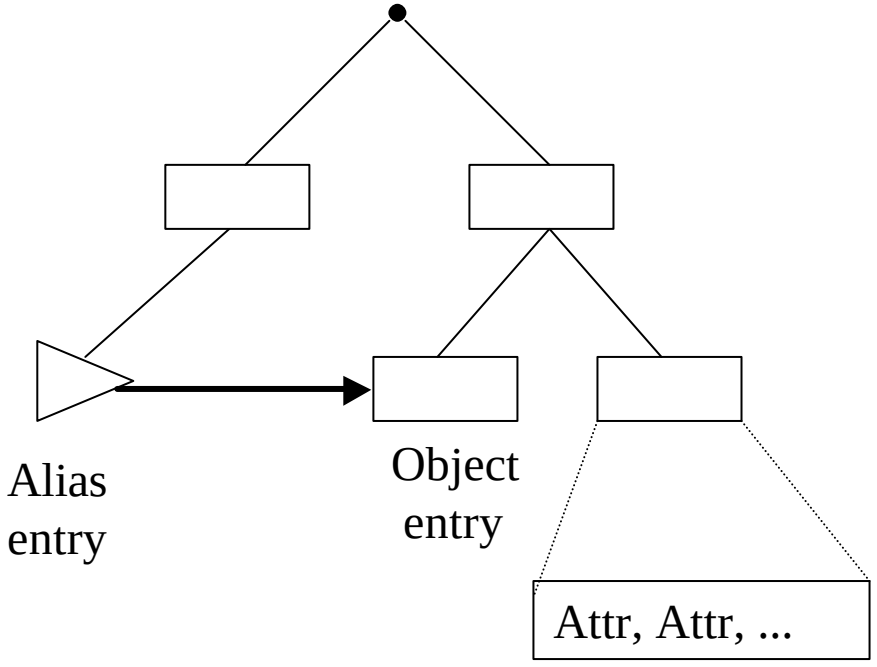
- **Exemple d'annuaire :**



LDAP : modèle de nommage

- **2 types d'objets particuliers :**
  - Alias
  - Referrals

- **Alias : référence entre entrées au sein d'un même annuaire**

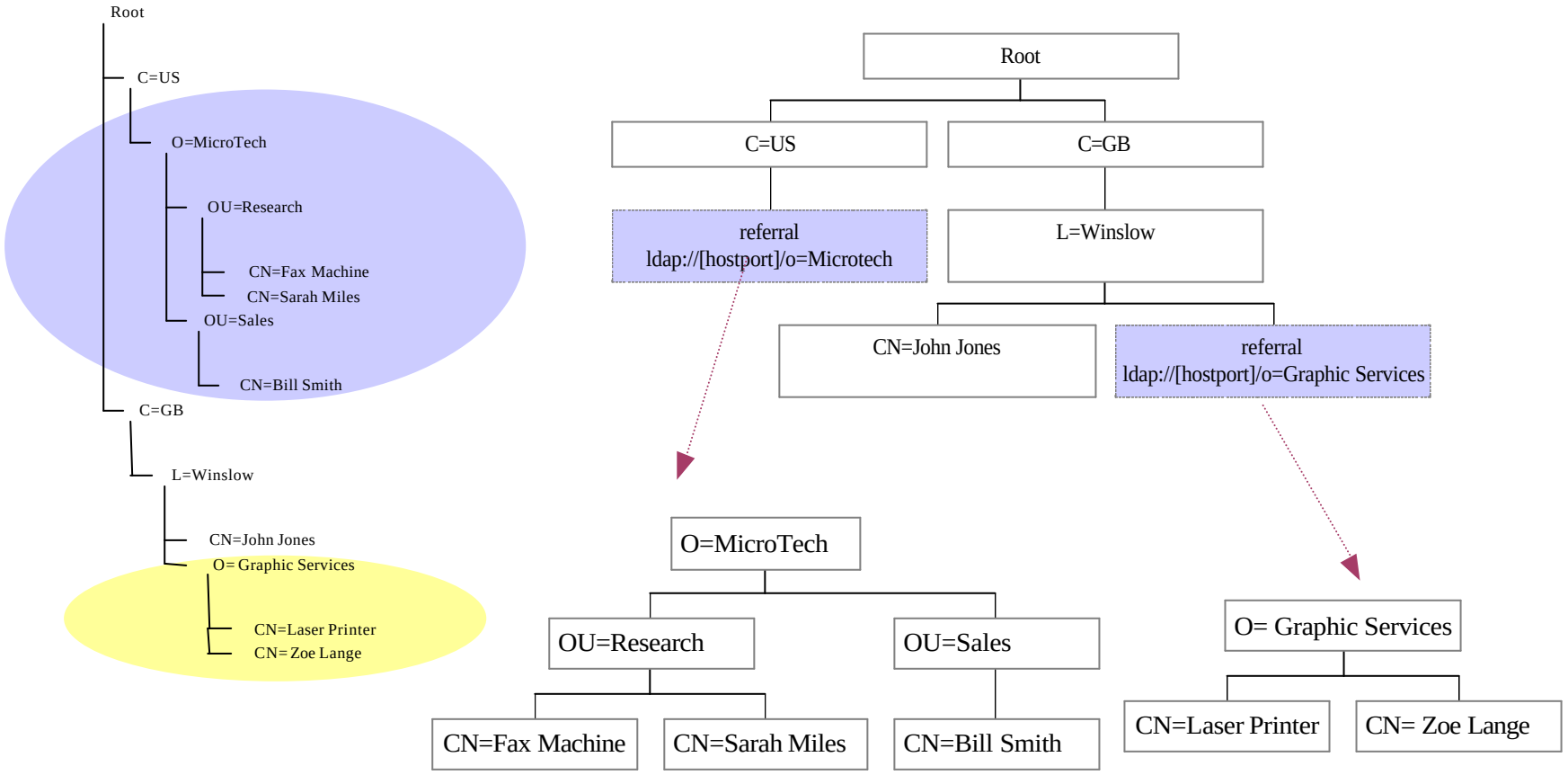


LDAP : modèle de nommage

- **Referrals :**
  - Distribuer la gestion d'un annuaire entre plusieurs serveurs LDAP distincts
  - Chaque serveur gère un sous-ensemble du DIT global
  - Permet la montée en charge en gardant de bonnes performances

- **Gestion de la distribution**
  - La distribution est gérée au niveau du client LDAP, il est responsable de toutes les connexions
  - Permet dans l'Internet de préserver l'autonomie des serveurs car :
    - La bande passante entre un client et serveur et la même qu'entre serveur et serveur
    - Les clients sont suffisamment puissants
    - Limite : tout le travail incombe à l'utilisateur

LDAP : modèle de nommage



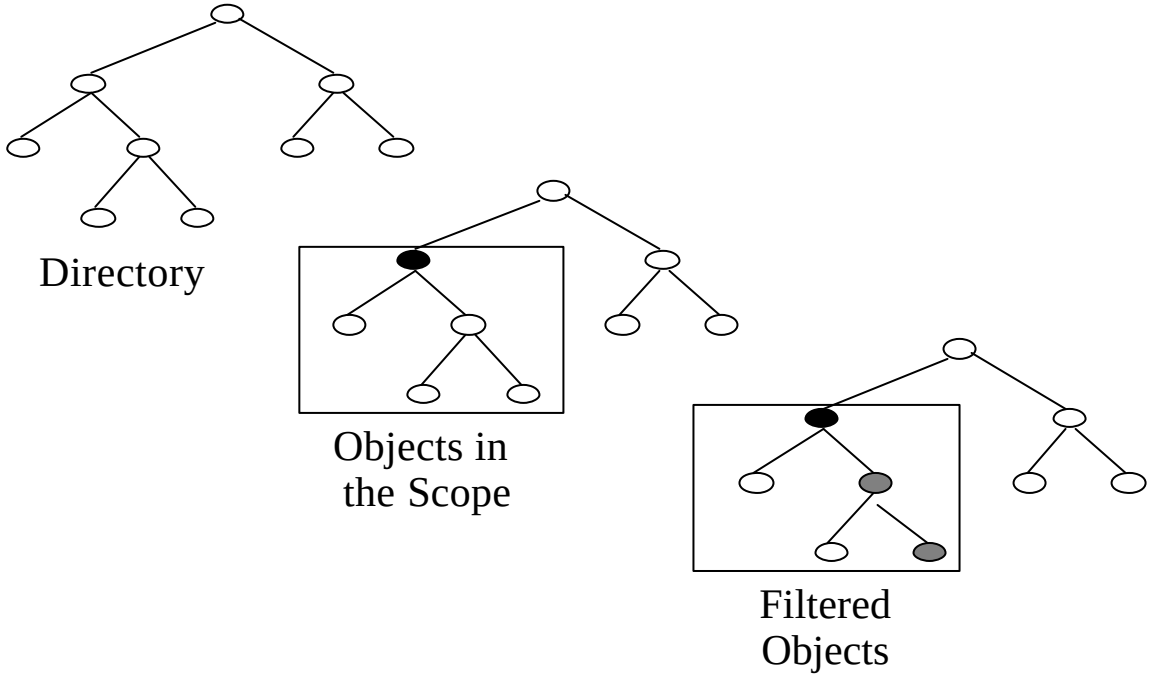
LDAP : modèle fonctionnel

- **Décrit le moyen d'accéder aux données ainsi que les opérations qu'on peut leur appliquer**

- **Le modèle définit :**
  - les opérations d'interrogation
  - les opérations de comparaison
  - les opérations de mise à jour
  - les opérations d'authentification et de contrôle

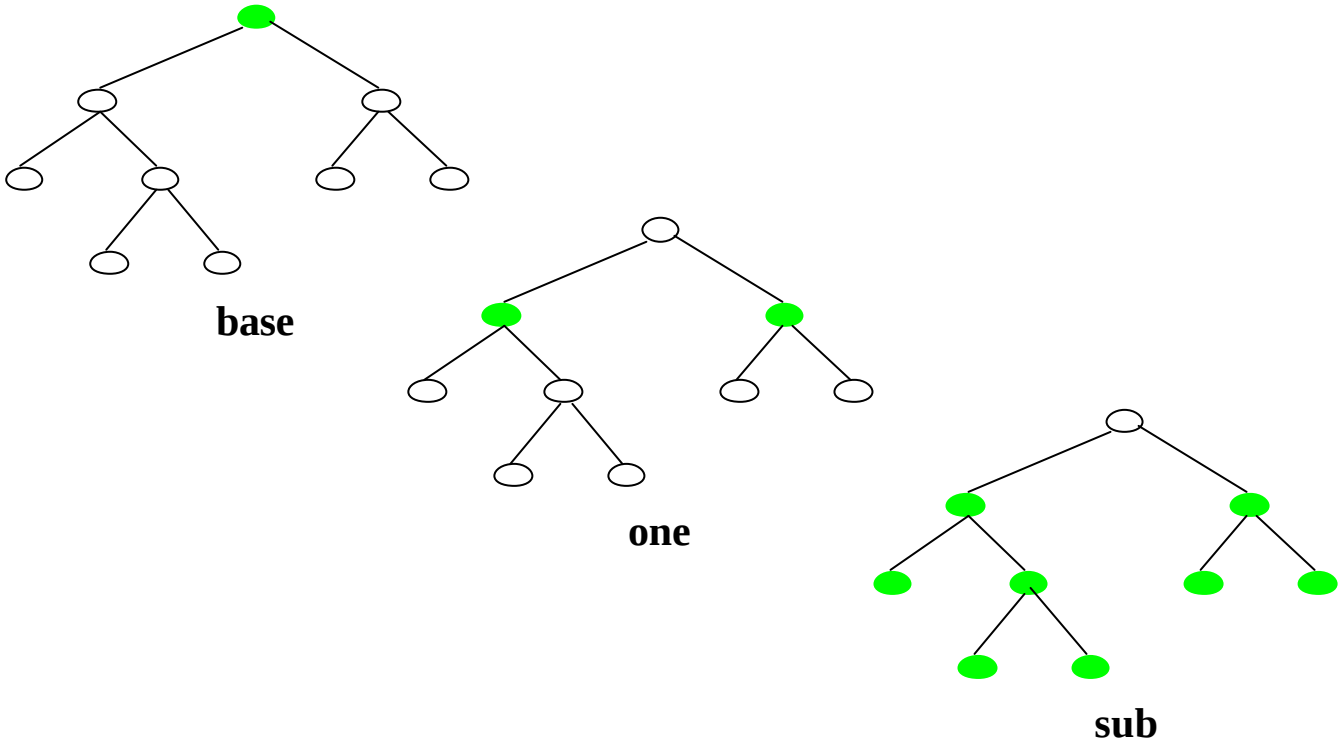
LDAP : modèle fonctionnel

- **Interrogation**
  - LDAP ne fournit pas d'opération de lecture d'entrée
  - Pour connaître le contenu d'une entrée, il faut écrire une requête
- **Scope & Filter**



LDAP : modèle fonctionnel

- **Scope :**
  - 3 niveaux différents :



LDAP : modèle fonctionnel

- **Filter :**
  - Permet de tester l'existence ou les valeurs d'attributs
  - Ex :

    objectclass = person

    telephonenumber = 01*
  - La clause filter d'une requête LDAP est composé d'un ensemble de conjonctions et/ou de disjonctions de filtres simples

LDAP : modèle fonctionnel

- **Modèle des requêtes LDAP**

  base object dn ? scope ? filter

- **Exemples de requêtes :**

  // Toutes les personnes de l'annuaire

  ? sub ? objectclass = person

  // Les départements de recherche de l'organisation Microtech

  c=us, o=microtech ? one ? ou=research

  // Toutes les personnes qui travaillent pour Microtech et dont le nom commence par Bill et qui ont un email chez aol

  c=us, o=microtech ? sub ? (&(cn = Bill*) (mail=*@aol.com))

LDAP : modèle fonctionnel

- **Structure du résultat d'une requête :**
  - **Le résultat d'une requête est composé de la liste des entrées qui sont concernées par le scope et qui vérifient le filtre**
  - **Les liens de contenance entre les objets sont perdus dans les résultats**

- **Des limites sur le temps de recherche ou la taille des résultats souhaités peuvent être spécifiés**

- **LDAP URL : sous-ensemble de l'opération de recherche qui peut être utilisé via un browser Web :**

  ldap://[hostport]/query_expression

  ldap://nldap.com/c=us?sub?(cn=bill*)

LDAP : modèle fonctionnel

- **Les limites des fonctionnalités d'interrogation :**
  - Résultats de requêtes toujours plats
  - Ne permet pas la recherche de chemins
    - « chercher tous les pays qui contiennent une organisation située à Paris »
  - Gestion des referrals
    - Chaining (propagation des requêtes entre les serveurs) pas implémenté car sur l'Internet, la bande passante entre clients et serveurs et la même qu'entre serveurs
    - Le client récupère l'adresse d'un serveur et il lui incombe de l'interroger à son tour s'il est intéressé par les données de ce serveur

LDAP : modèle fonctionnel

- **Opérations de mise à jour :**
  - add :
    - ajouter une nouvelle entrée dans le DIT
  - delete :
    - supprimer une entrée du DIT
  - modify :
    - ajouter des valeurs ou des attributs
    - supprimer des valeurs ou des attributs

- **Des contrôles d'intégrité sont effectués :**
  - Attributs obligatoires
  - Intégrité référentielle
  - etc

LDAP : modèle de sécurité

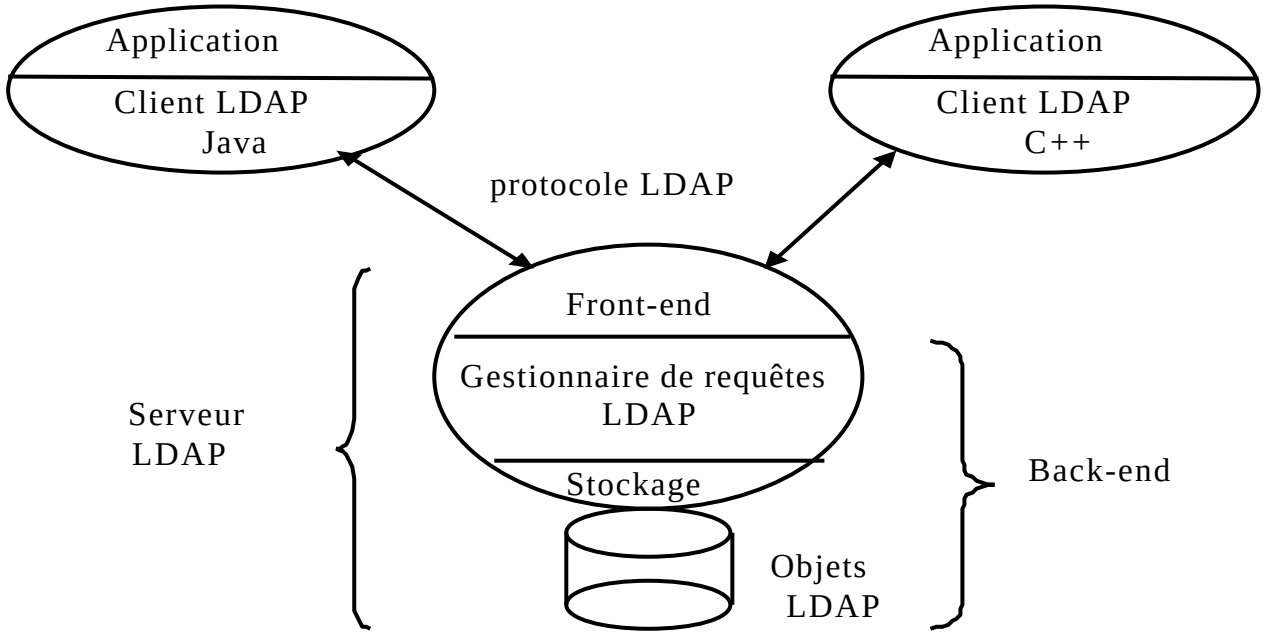
- **Décrit le moyen de protéger les données de l'annuaire des accès non autorisés**

- **Plusieurs niveaux :**
  - authentification lors de l'accès à un service
    - anonymous permet de consulter les données accessibles en lecture pour tous
    - administrateur (tous les droits)
    - mot de passe en clair (DN + password transitent en clair sur le réseau)
    - Mot de passe + SSL ou TLS (la session est chiffrée)
    - Échange de certificats SSL (clés publiques/privées)
    - Simple Authentification and Security Layer (SASL) : mécanisme externe d'authentification (Kerberos, S/Key, GSSAPI)
  - contrôle d'accès
    - définit les droits des différents utilisateurs sur les données
  - chiffrement des transactions entre clients et serveurs ou entre serveurs

LDAP : modèle de duplication

- **Définit comment dupliquer l'annuaire sur plusieurs serveurs**
- **But :**
  - Supporter la montée en charge
  - Résister à une panne d'un serveur ou à une coupure réseau
- **La réplication est supportée dans le modèle LDAP par le protocole LDUP (standard en cours)**
- **Le modèle :**
  - Actuellement, un site maître et des sites esclaves.
  - On duplique tout l'arbre ou uniquement un sous-arbre
  - Des modèles plus compliqués sont à l'étude
    - « on ne duplique que les objets de type personne »

LDAP : Architecture



Conclusion

- **Avantages de LDAP :**
  - Flexibilité
  - Simplicité
  - Efficacité (en consultation)

- **Les lacunes :**
  - Interopérabilité et intégration :
  - Langage d'interrogation relativement limité

Bibliographie

- http://www3.innosoft.com/ldapworld (catalogue des serveurs ldap existants)
- D. Srivastava, Directories : Managing Data for Networked Applications (tutoriel sur LDAP). http://wwww.research.att.com/~divesh
- LDAPv2, http://www.ietf.org/rfc/rfc1777.txt
- LDAPv3, http://www.ietf.org/rfc/rfc2251.txt
- L. Mirtain, Service d'annuaire LDAP, 1999.
- Mark Wilcox , « Implementing LDAP », March 1999, Wrox Press Inc; ISBN: 1861002211
- Rob Weltman, Tony Dahbura , « LDAP Programming with Java » (February 2000), Addison-Wesley Pub Co; ISBN: 0201657589