Les Annuaires : LDAP

Plan

- Concepts

Origines de LDAP

La norme LDAP

1. Concept de Nommage

- **Nommage (Naming)**
  - Association d 'un nom à un objet
    - objet : fichier, usager, machine, service distant …
    - Liaison (binding)
      - terme pour désigner une association

- **Exemples:**
  - DNS
    - www.prism.uvsq.fr vers l 'adresse IP correspondante
  - FileSystem DOS
    - c:\bin\autoexec.bat vers un fichier
  - CORBA, RMI, ...

1. Concept de Nommage ...

- **Convention du nommage**
  - règles de représentation des noms
    - DNS : identifiants séparés par des . (dot)
    - FS Unix : identifiants séparés par des /
    - FS Dos : nom d 'unité :\ puis identifiants séparés par des \
    - LDAP : cn=Rosanna Lee, o=Sun, c=US
- **Contexte**
  - sous-ensemble de liaison
    - sun.com; /usr; o=Sun, c=US sont des contextes
- **Naming System**
  - ensemble de contextes connectés utilisant la même convention de nommage
- **NameSpace**
  - ensemble de noms utilisés par un Naming Service

1. Concept d 'Annuaire ...

- **Annuaire (Directory)**
  - extension du nommage
    - les objets ont aussi des attributs:
      - une imprimante peut avoir des attributs vitesse, resolution, couleur
      - une personne peut avoir un attribut bureau, email
  - organisation généralement hiérarchique

- **Exemple**
  - Novell NDS, Solaris NIS, ISO X500, LDAP, ...

1. Concept d 'Annuaire ...

- **Recherche (query) dans l 'Annuaire**
  - expression logique
  - sur le nom
    - sur une partie du nom
  - sur la valeur des attributs
    - search filter

      (appelé aussi reverse lookup ou content-based searching)

Plan

Concepts

- Origines de LDAP

La norme LDAP

DSML

JNDI

2. Origines de LDAP

- **X500**
  - Standard ISO conçu par les opérateurs telecom pour interconnecter leurs annuaires téléphoniques
- **LDAP (Lightweight Directory Access Protocol)**
  - Proposé par l 'IETF en 1995 (http://www.ietf.org/rfc/)
  - Simplification de ISO X500 :
    - basé sur X500 DAP et adapté à l'Internet
    - même convention de nommage, API facile à utiliser
    - basé sur TCP/IP (plutôt que les couches ISO) :
      - RFC 1487(v1), RFC 1777(v2), RFC 2251(v3)
    - La plupart des éléments manipulés sont des chaînes de caractères
  - Première implantation de l' Univ. Michigan en 1995
  - Produits commerciaux :
    - IBM, Microsoft, Netscape, Oracle, Sun, …

2. LDAP : Concepts

- **Qu'est-ce qu'un annuaire ?**
  - **base de données spécialisée (BD hiérarchique)**
    - 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

Plan

Concepts

Origines de LDAP

- La norme LDAP

DSML

JNDI

La norme LDAP

Protocole

Modèle d'information

Modèle de nommage

Modèle fonctionnel

Modèle de sécurité

Modèle de duplication

Architecture

3. 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.

3. 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

3. 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***

3. 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

3. 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)

3. 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

3. 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.

3. LDAP : modèle de nommage

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

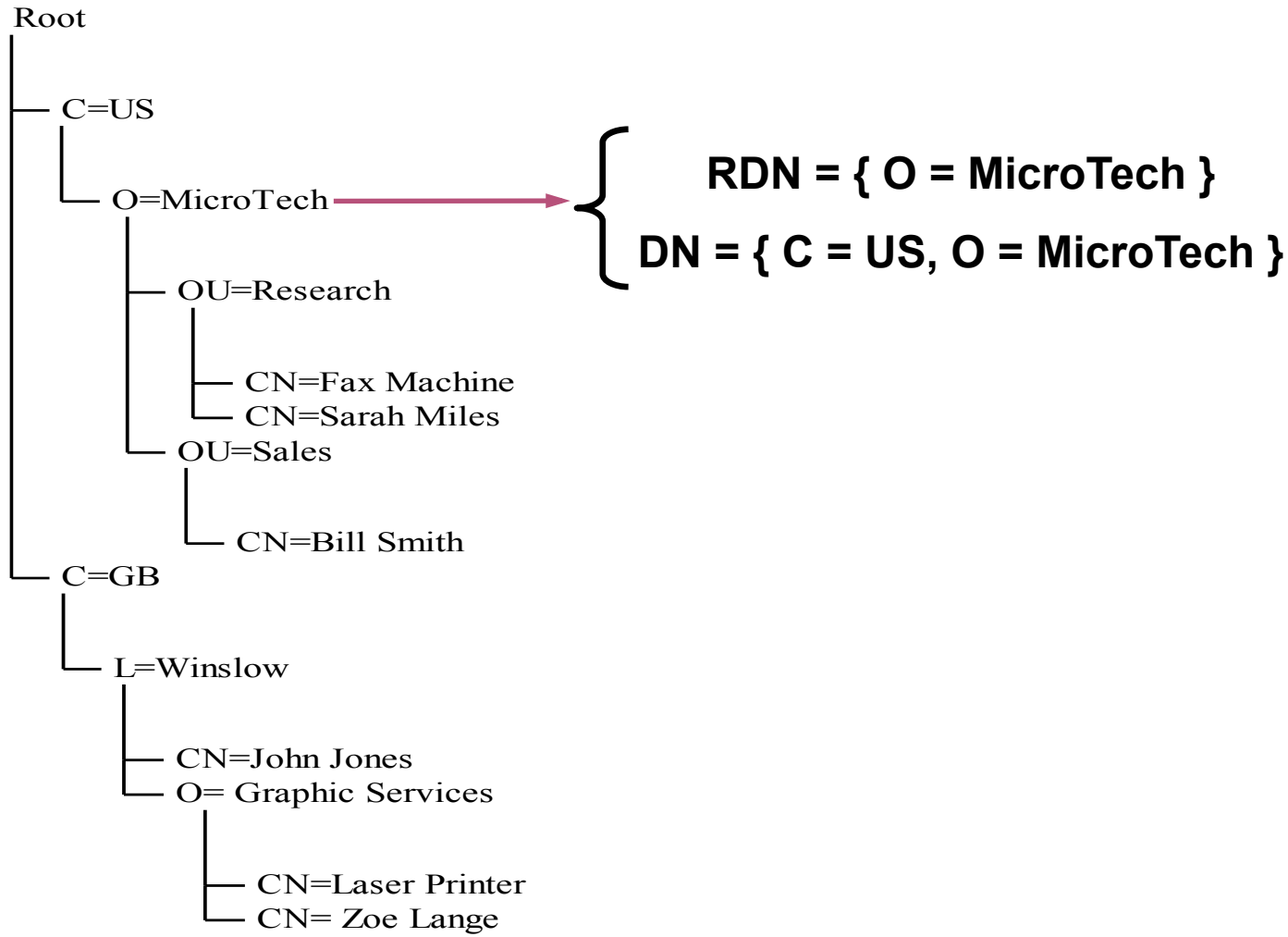
      ex : **RDN = { O = MicroTech }**
    - Distinguished Name (DN)

      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

3. LDAP : modèle de nommage

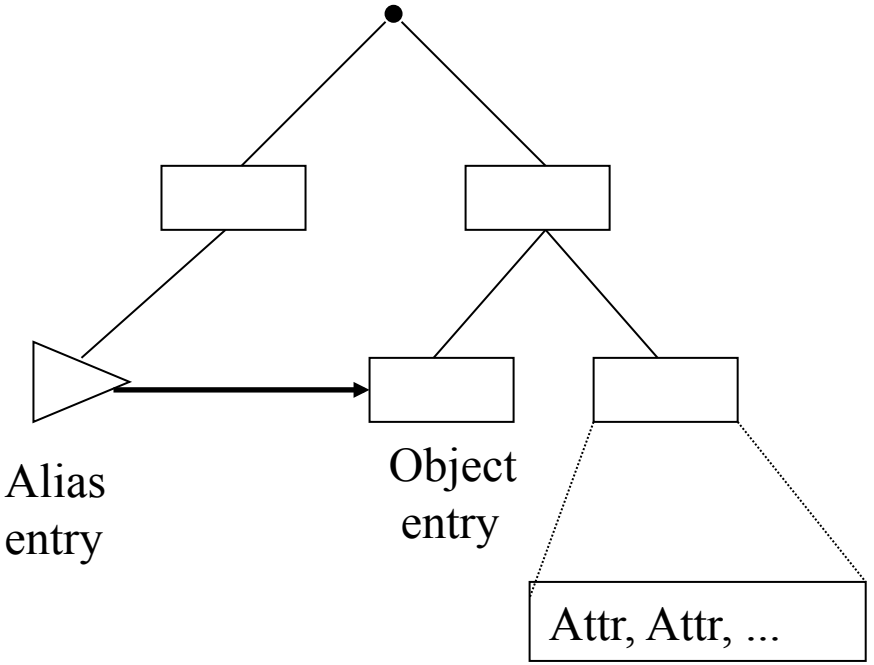
- **Exemple d'annuaire :**



3. LDAP : modèle de nommage

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

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

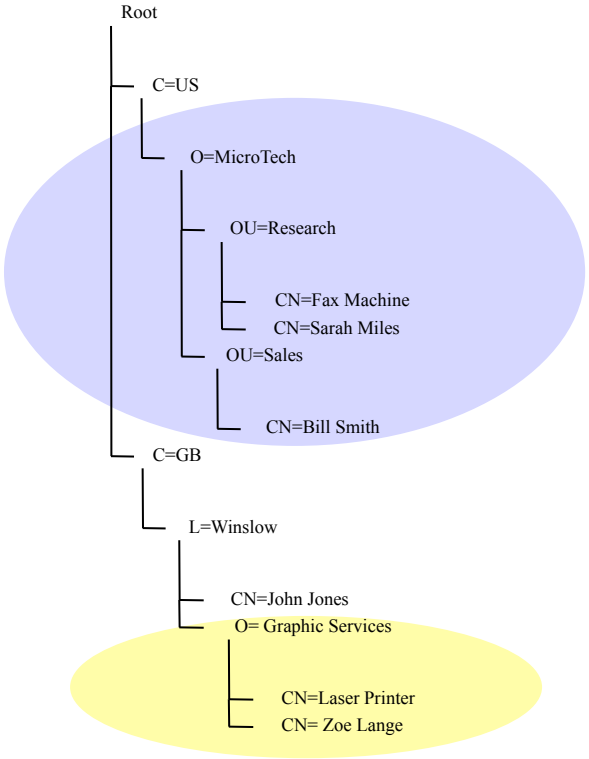


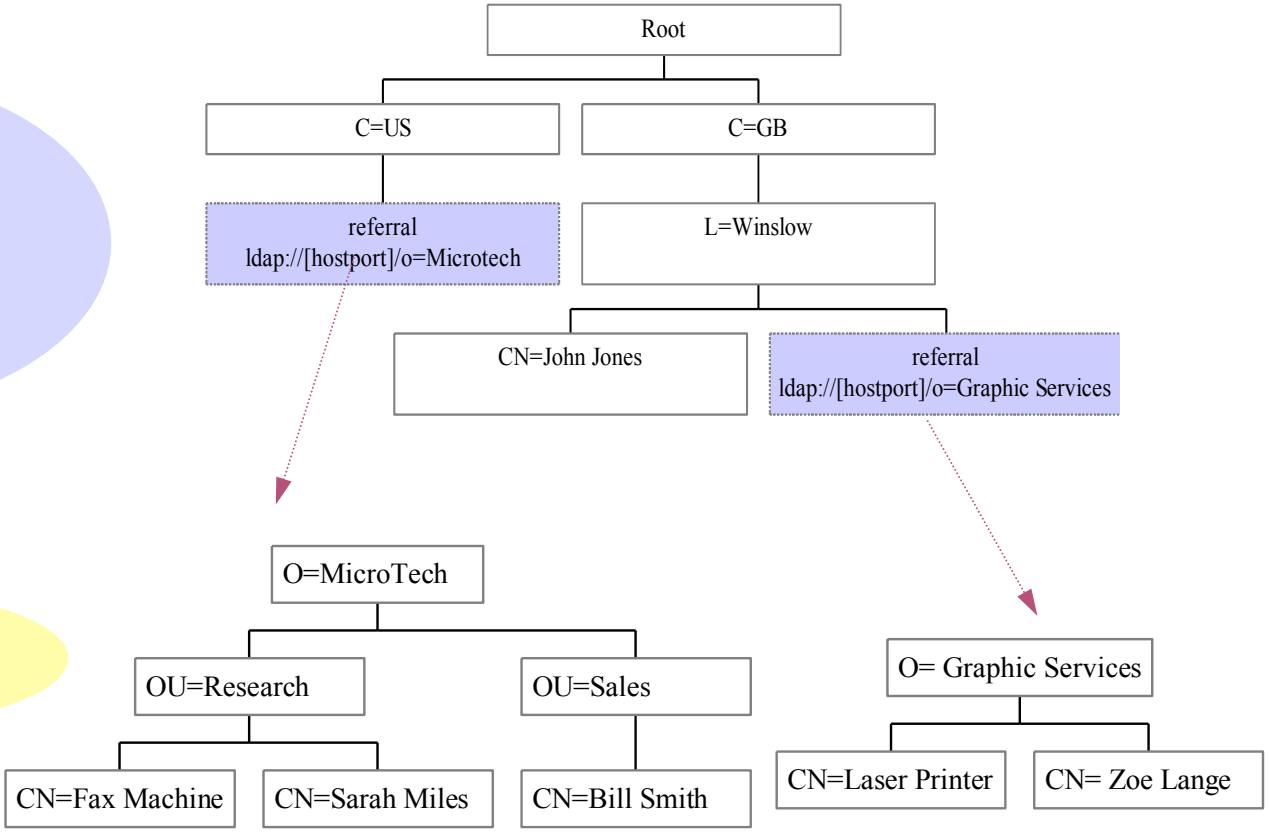
3. LDAP : modèle de nommage

- **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 :
    - 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

3. LDAP : modèle de nommage





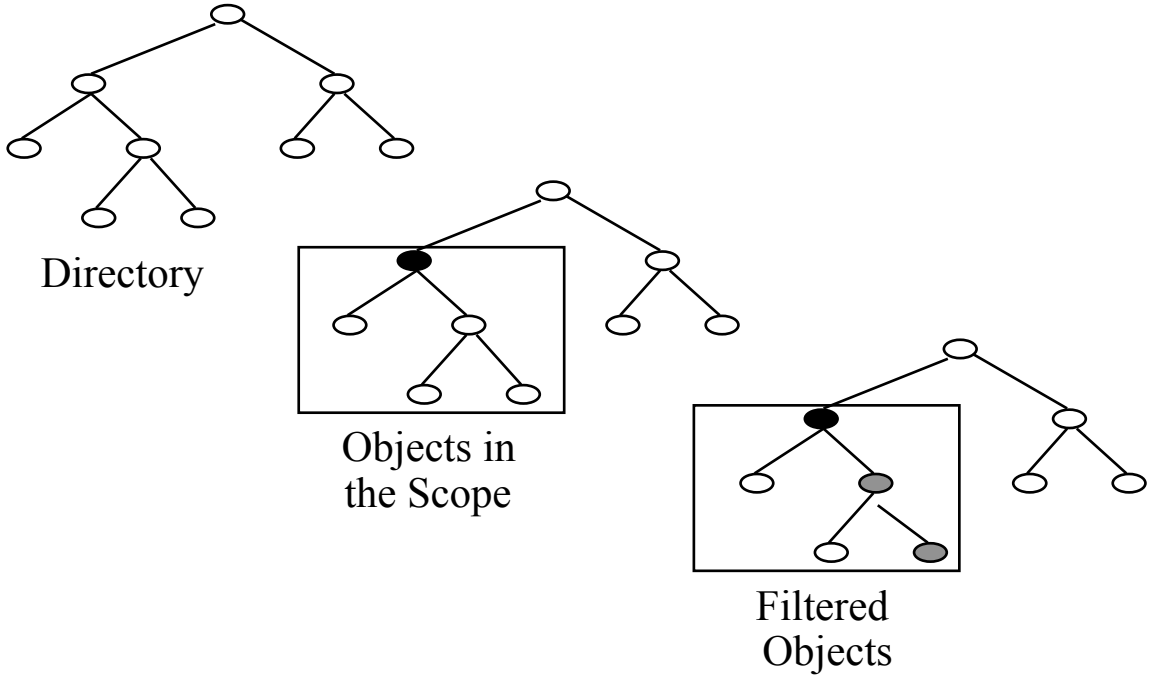
3. LDAP : modèle fonctionnel

- **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

3. 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**
  - Base Object : DN du nœud racine de la recherche
  - Différents niveaux pour le scope : base, one and sub
  - Le filtre est composé de prédicats testant les valeurs ou l'existence des attributs



3. 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*)

3. 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

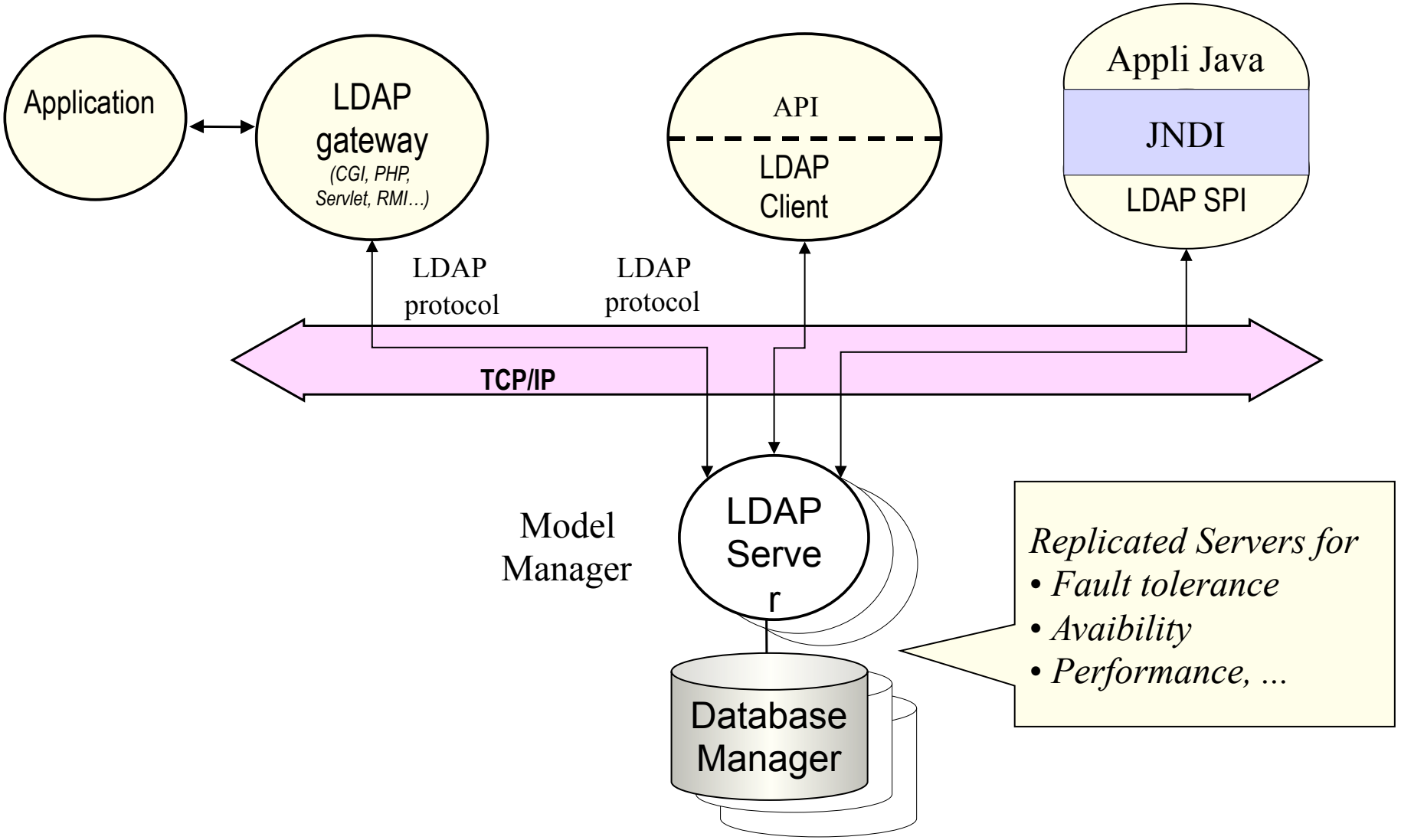
3. LDAP : modèle de sécurité

- **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

3. 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 »

3. LDAP : Architecture



3. Conclusion

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

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