DU Sécurité
Année 2006-2007

LDAP
Lightweigth Directory Access Protocol

Ahmed Mehaoua
Professeur
Université Paris 5

Plan

- Concepts
  - Qu'est-ce qu'un annuaire ?
  - Historique
  - LDAP
- Les applications de LDAP aujourd'hui et demain
- Les logiciels serveurs
- Les clients LDAP
- Bibliographie

Préface

Ce support a été réalisé en utilisant plusieurs sources documentaires dont l'excellent tutorial sur LDAP de L. Mirtain (INRIA).

Concepts : qu'est-ce qu'un annuaire ?

- Un conteneur d'informations organisées
- Exemples d'annuaires courants
  - annuaire téléphonique
  - carnet d'adresses
  - catalogue de vente
  - guides télé

Ce sont des annuaires offline

- Un service d'annuaire électronique, c'est en plus...
  - un protocole qui permet l'accès au contenu
  - une syntaxe qui permet d'interroger la base
- et aussi
  - un modèle de duplication
  - un modèle de distribution des données

Concepts : qu'est-ce qu'un annuaire ?

Spécificités des annuaires électroniques

- dynamiques (informations changent -> + à jour)
- souples (changement aisé type et organisation des données)
- peuvent être sécurisés (qui voit quoi)
- peuvent être personalisés (façon de présenter les données, action sur ses propres données,...)

Pas de requêtes compliquées (comme les jointures en SQL),

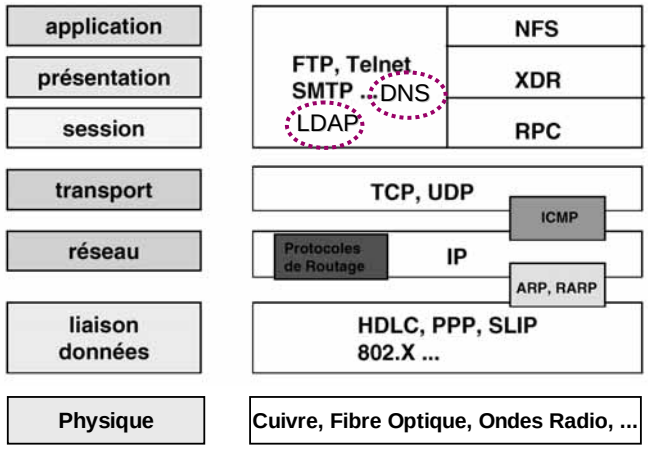
exemple de services d'annuaires que nous utilisons déjà : le DNS

- pour obtenir l'url http://www.sncf.com/ il faut obtenir l'adresse du serveur www.sncf.com -> requête DNS

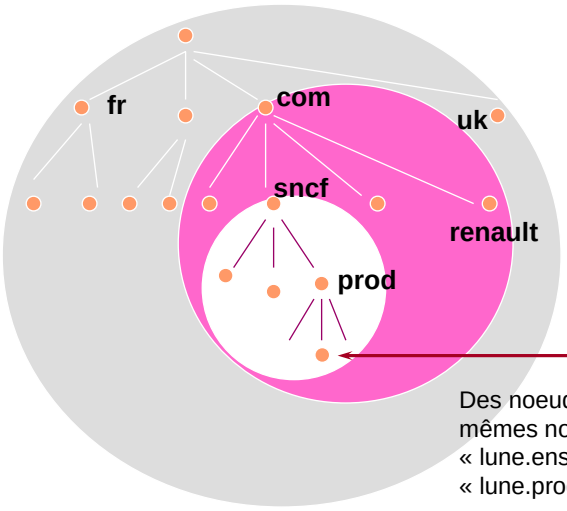
❑ DNS est un exemple d'un service d'annuaire global

- il est distribué entre des serveurs coopérants
- il a un espace de nommage uniforme

Rappel : L'architecture TCP/IP



Annuaire électronique : Le Domain Name System



Domaine complet

Domaine « fr »

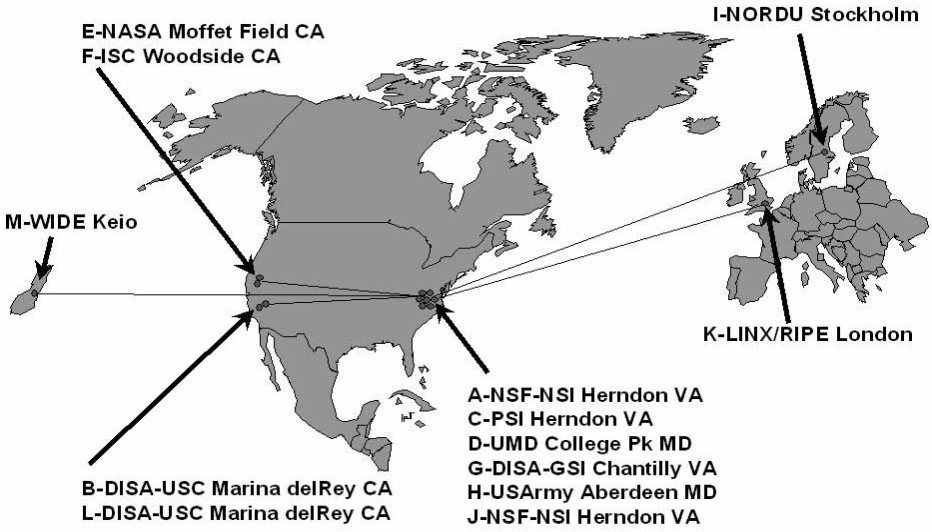
Domaine « uvsq »

noeud « lune.prod.sncf.com »

Des noeuds peuvent avoir les
mêmes noms dans des domaines différents:
« lune.ens.paris5.fr » et
« lune.prod.sncf.com »

DNS Root Servers

Designation, Responsibility, and Locations



Concepts : qu'est-ce qu'un annuaire ?

Caractéristiques comparées des annuaires et base de données

- ❏ rapport lecture/écriture (beaucoup) plus élevé pour les annuaires
- ❏ annuaires plus facilement extensibles (types de données)
- ❏ diffusion à beaucoup plus large échelle
- ❏ distribution des données entre serveurs plus facile avec les annuaires
- ❏ plus grande duplication des informations des annuaires (+ fiable, +performant, + proche des clients)
- ❏ importance des standards -> LDAP
- ❏ performances globales des annuaires plus élevées (en lecture)

Concepts : ce que n'est pas un annuaire

- ❏ approprié à de fréquentes écritures
- ❏ destiné à manipuler des données volumineuses
- ❏ un substitut à un serveur FTP, un système de fichiers,...

Concepts : à quoi peut servir un annuaire en ligne ?

- ❏ chercher (et trouver) des informations mieux et plus vite
- ❏ pour des humains ou des applications
- ❏ gérer (carnets d'adresses, comptes utilisateurs, profils,...)
- ❏ de base de donnée simple
- ❏ à stocker et diffuser des certificats dans une PKI

Les applications de LDAP

- ❏ **Les différents domaines d'application possibles des annuaires LDAP :**
  - → Les applications système
  - → Les applications Intranet/Extranet
  - → Les applications Internet
  - → Les bases de données

Les applications de LDAP : applications systèmes

- **Les applications systèmes**

L'annuaire utilisé pour servir aux besoins des services réseaux tels que l'authentification, le contrôle d'accès, la localisation des imprimantes ou des serveurs de fichier.

Dans ce cas, il est étroitement lié au système d'exploitation.

De plus en plus de fabricants se tournent vers le standard LDAP pour l'implanter dans leur système.

Exemple : Windows 2000, Novell, Solaris, Linux...

Les applications de LDAP : exemples

- **Gestion centralisée de l'authentification et des droits d'accès**
  - → **Remplacer les multiples mots de passe applicatifs/systèmes par une authentification LDAP centralisée.**

Netscape Directory Server - synchronisation des bases utilisateurs Windows NT4 avec base LDAP

Netscape SuiteSpot - serveur de Mail, de News, Web utilisant LDAP pour l'authentification

Cyrus IMAP/POP3' pwcheck_ldap.c - programme externe d'authentification LDAP pour les serveurs IMAP/POP3 de Cyrus.

Apache::AuthLDAP - module d'authentification et de gestion des autorisations d'accès au serveur Web Apache via LDAP.

PADL Software's PAM (Pluggable Authentification Module) & NSS (Name Service Switch) Modules - authentification/lookup redirigés sur LDAP sous Solaris et Linux

Les applications de LDAP : applications intranet

❑ Les applications Intranet

Le service d'annuaire sert typiquement aux applications utiles à l'utilisateur final :

- **accès à des pages Web,**
- **annuaire téléphonique ou pour la messagerie électronique,**
- **profils de configuration... (Netscape suitespot, Lotus Domino...)**

Les applications de LDAP : applications extranet

❑ **Les applications Extranet**

L'annuaire peut servir de base d'information entre un fournisseur et ses sous-traitant, une banque et ses clients...

Ce sont celles mises en œuvre par les ISPs ou les grandes entités industrielles ou universitaires.

L'annuaire sert à gérer les abonnées, les hébergements de services comme le Web et la messagerie.

Les applications de LDAP : bases de données

❑ **Les bases de données**

L'annuaire peut remplacer un SGBD traditionnel dans le cas de données simples, intensivement interrogées, distribuées à large échelle et utilisées par des multiples applications (fichier clientèle, catalogues de fournitures...).

Il peut épauler un SGBD, en étant synchronisé avec lui, pour faciliter la consultation des données ou la mise à jour de certains champs.

Parfois, l'organisation possède plusieurs bases de données déconnectées et gérant des informations redondantes :

- **la paye**
- **le bureau du personnel**
- **les comptes informatiques**
- **les badges d'accès**
- **les cartes de restaurants...**

Un annuaire LDAP peut fédérer les données communes (informations sur les employés), les données sensibles étant gérées dans les SGBD => Meta-Directory.

Les applications de LDAP : exemples

- **Mobilité utilisateur : accès distant des applications aux options, configurations et préférences**
  - → **permettre à l'utilisateur de retrouver son environnement applicatif indépendamment de sa localisation**

Netscape Communicator Roaming Access.
Netscape Calendar nscalUser object class.

- **Gestion des mailing-lists et des aliases mail par LDAP**

Netscape Messenger Server - Serveur de Mail « full LDAP ».
Sendmail 8.9.x : peut utiliser LDAP pour les résolutions d'adresses.
Sympa : gestionnaire de listes de diffusions « LDAP capable »

Concepts : historique

Historiquement sont apparus :

- Bases de comptes de systèmes multi-utilisateurs (70-80)
  - Unix `/etc/passwd`,
  - IBM MVS PROFS
  - ...
- Grapevine (Xerox, début 80)
- Internet Domain Name System (84)
  - service de nommage réseau
  - spécifique mais efficace
- WHOIS
  - bases de contacts

Concepts : historique

- Les annuaires dédiés aux applications
  - Lotus cc:Mail, Notes
  - Unix sendmail /etc/aliases ou /etc/passwd
  - Microsoft Exchange
- Les annuaires Internet (offrent de plus en plus un accès LDAP)
  - Bigfoot, Yahoo's Four11, AnyWho (AT&T), Schwitboard
- Les annuaires système-réseau (NOS)
  - Sun NIS, NIS+
  - Novell NetWare Directory Service (93) (proche d'X500)
  - Microsoft Active Directory (natif LDAP)
- Les annuaires multi-usage
  - X.500 (88-93-97)
  - WHOIS++ (93)
  - CSO (PH)
  - LDAP (93)

Concepts : historique : X.500

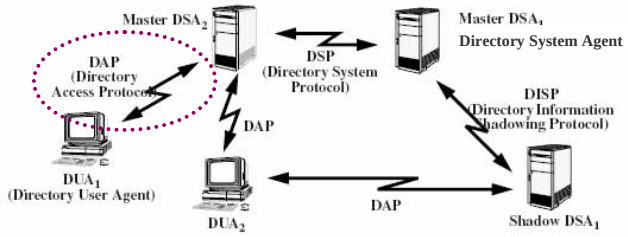
- Standard conçu par les opérateurs télécom pour interconnecter leurs annuaires téléphoniques.
- Destiné à devenir LE service d'annuaire GLOBAL distribué, normalisé et fédérateur.
- Mais conçu aussi pour répondre à tout type de besoin d'annuaire grâce à un modèle de données de type objet et extensible.

- Exemple d'annuaire X.500 :
  - NameFlow Paradise (Piloting An inteRnationAl DIrectory SErvice),
  - SURFNET (nl)...
- Logiciels DSA X.500
  - ISODE Consortium/Quipu,
  - NeXor/XT-Quipu,
  - Control Data/Rialto Global Directory Server

Concepts : historique : X.500

❑ X.500 définit :

- les règles pour nommer les objets et les entités
- les protocoles pour fournir le service d'annuaire
- un mécanisme d'authentification.



X500 = suite (conséquente) : X501, X509, X511, X518, X519, X520, X521, X525

Concepts : historique : X.500

Qualités et défauts d'X500 :

❑ Atouts d'X500 :

- scalability, fonctions de recherche évoluées, distribué (données et administration), ouvert

❑ Défauts d'X500 :

- implémentations (très) lourdes, buggées et difficilement interopérables, basé sur les protocoles ISO, contraire à la culture internet

❑ Echec : les ambitions d'X500 n'ont pas été atteintes

Concepts : historique : LDAP

- En 1993 Lightweight Directory Access Protocol (LDAP) est né de l'adaptation et du dégraissage de X.500 DAP au protocole TCP/IP.
- Deux groupes de travail aboutissent à 2 produits fonctionnant comme frontal X.500 :
  - Directory Assistance Service (DAS) : RFC 1202
  - Directory Interface to X.500 Implemented Efficiently (DIXIE) : RFC 1249

qui convergent finalement vers le standard IETF LDAP.

- LDAPv1 : RFC 1487 Juillet 93
- LDAPv2 : RFC 1777 Mars 95
- LDAPv3 : RFC 2251 Décembre 97

LDAP garde beaucoup d'aspects de X.500 dans les grandes lignes, mais va dans le sens de la simplification et de la performance

Concepts : historique : LDAP

- LDAP est initialement un frontal d'accès à des bases d'annuaires X.500 (translateur LDAP/DAP).
- Devient un annuaire natif (standalone LDAP) utilisant sa propre base de données, sous l'impulsion d'une équipe de l'Université du Michigan (U-M LDAP 3.2 en 95).

(Wengyik Yeong, Steve Kille, Colin Robbins, Tim Howes, Marc Wahl).

- En 96, apparaissent les premier serveurs commerciaux.

Aura pour héritiers :

1. OpenLDAP
2. Serveur Netscape

Une passerelle LDAP/X.500

Concepts : LDAP
LDAP définit :

- le protocole d'accès -- comment accéder à l'information contenue dans l'annuaire,
- un modèle d'information -- le type d'informations contenues dans l'annuaire,
- un modèle de nommage -- comment l'information est organisée et référencée,
- un modèle fonctionnel -- comment on accède et met à jour l'information,
- un modèle de sécurité -- comment données et accès sont protégés,
- un modèle de duplication -- comment la base est répartie entre serveurs,
- des API -- pour développer des applications clientes,

Concepts : LDAP, le protocole

Le protocole définit :

- Comment s'établit la communication client-serveur :
  - commandes pour se connecter ou se déconnecter, pour rechercher, comparer, créer, modifier ou effacer des entrées.
- Comment s'établit la communication serveur-serveur :
  - échanger leur contenu et le synchroniser (replication service)
  - créer des liens permettant de relier des annuaires les uns aux autres (referral service).
- Le format de transport de données :
  - pas l'ASCII (comme pour http, smtp...) mais le Basic Encoding Rules (BER), sous une forme allégée (appelée LBER : Lightweight BER)

Concepts : LDAP, le protocole
Le protocole définit (suite) :

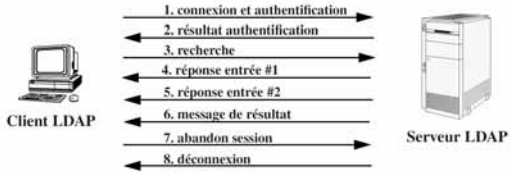
- Les mécanismes de sécurité :
  - méthodes de chiffrement et d'authentification
  - mécanismes de règles d'accès aux données.
- Les opérations de base:
  - interrogation : `search, compare`
  - mise à jour : `add, delete, modify, rename`
  - connexion au service : `bind, unbind, abandon`

Concepts : LDAP, le protocole

- possibilité d'avoir une seule connexion pour passer plusieurs requêtes

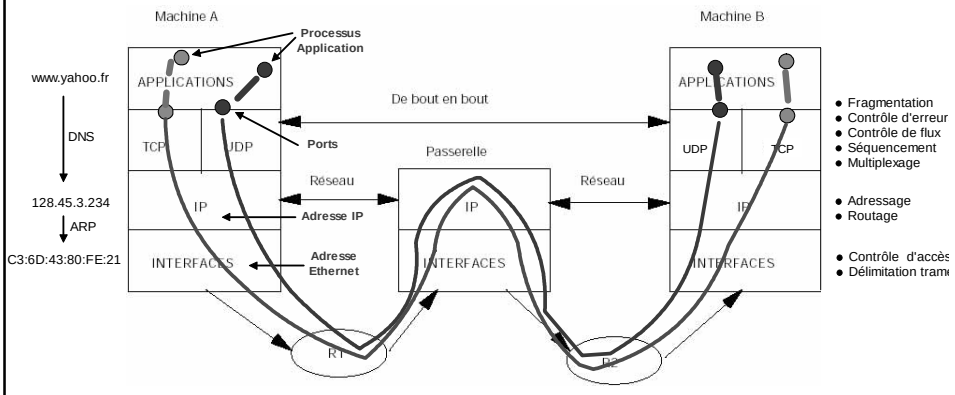
  LDAP utilise le port TCP serveur : 389 (voir RFC 1700)

  Secure LDAP (LDAP over SSL/TLS) utilise le port TCP serveur : 636



- LDAPv3 est conçu pour être extensible sans avoir à modifier la norme grâce à 3 concepts :
  - LDAP extented operations : rajouter une opération, en plus des neuf opérations de base.
  - LDAP controls : paramètres supplémentaires associés à une opération qui en modifient le comportement.
  - Simple Authentification and Security Layer : couche supplémentaire permettant à LDAP d'utiliser des méthodes d'authentification externes.

Rappel : principe de Communication TCP/IP



Concepts : LDAP, modèle d'information

- Le modèle d'information définit le type de données pouvant être stockées dans l'annuaire.
  - L'entrée (Entry) = élement de base de l'annuaire. Elle contient les informations sur un objet de l'annuaire.
  - Ces informations sont représentées sous la forme d'attributs décrivant les caractéristiques de l'objet.
  - Toute sorte de classe d'objet (réel ou abstrait) peut être représentée.
  - Le schéma de l'annuaire définit la liste des classes d'objets qu'il connaît.

Concepts : LDAP, modèle d'information

Schéma

- Le Directory schema est l'ensemble des définitions relatives aux objets qu'il sait gérer (~typedef).
- Le schéma décrit les classes d'objets, les types des attributs et leur syntaxe.
- Chaque entrée de l'annuaire fait obligatoirement référence à une classe d'objet du schéma et ne doit contenir que des attributs qui sont rattachés au type d'objet en question.

- Attributs

Un type d'attribut (ou attribut) est caractérisé par :

- Un nom, qui l'identifie
- Un Object Identifier (OID), qui l'identifie également
- S'il est mono ou multi-valué
- Une syntaxe et des règles de comparaison (matching rules)
- Un format ou une limite de taille de valeur qui lui est associée

Tableau 1 : Exemple d'attributs d'une entrée

type d'attribut	valeur d'attribut
cn:	Barnabé Dupond
uid:	bdupond
telephonenumber:	+33 (0)1 2345 6789
mail:	Barnabe.Dupond@acme.com
roomnumber:	C105

Concepts : LDAP, modèle d'information

- Classes d'objets

Les classes d'objets modélisent des objets réels ou abstraits en les caractérisant par une liste d'attributs optionnels ou obligatoires. Une classe d'objet est définie par :

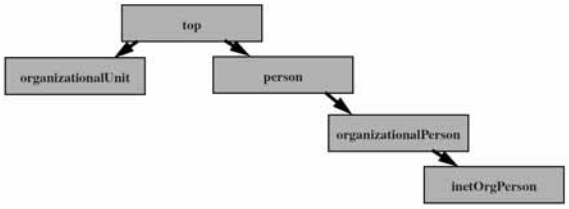
- Un nom, qui l'identifie
- Un OID, qui l'identifie également
- Des attributs obligatoires
- Des attributs optionnels
- Un type (structurel, auxiliaire ou abstrait)

Exemples de classes d'objet :

- une organisation (`o`),
- ses départements (`ou`),
- son personnel (`organizationalPerson`),
- ses imprimantes (`device`),
- ses groupes de travail (`groupofnames`).

Concepts : LDAP, modèle d'information

Les classes d'objets forment une hiérarchie, au sommet de laquelle se trouve l'objet `top`.



- Chaque objet hérite des propriétés (attributs) de l'objet dont il est le fils.
- On précise la classe d'objet d'une entrée à l'aide de l'attribut `objectClass`.
- Il faut obligatoirement indiquer la parenté de la classe d'objet en partant de l'objet `top` et en passant par chaque ancêtre de l'objet.

Concepts : LDAP, modèle d'information

Par exemple, l'objet `inetOrgPerson` à la filiation suivante :

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

L'objet person **a comme attributs :** commonName, surname, description, seeAlso, telephoneNumber, userPassword

L'objet fils organizationalPerson **ajoute des attributs comme :** organizationUnitName, title, postalAddress...

L'objet petit-fils inetOrgPerson **lui rajoute des attributs comme :** mail, labeledURI, uid (userID), photo...

Concepts : LDAP, modèle de nommage

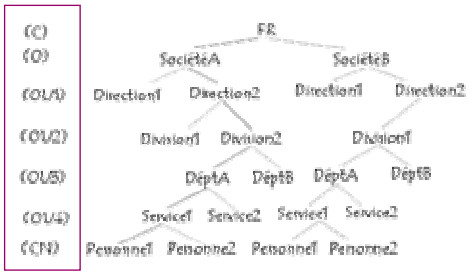
- Le modèle de nommage définit comment sont organisées les entrées de l'annuaire et comment elles sont référencées.
- Les entrées représentent des objets.
- L'organisation de ces objets se fait suivant une structure logique hiérarchique : le Directory Information Tree (DIT).
- Chaque nœud de l'arbre (DIT) correspond à une entrée de l'annuaire le directory specific entry (DSE).
- Au sein de ce DIT, l'identification d'une entrée se fait à l'aide d'un nom, le Distinguish Name (DN).
- Au sommet de l'arbre se trouve l'entrée Suffix ou Root Entry ou BaseDN, qui caractérise une base LDAP.

Concepts : LDAP, modèle de nommage

- Le Directory Information Tree (DIT)

Classification des entrées dans une arborescence hiérarchique (comparable au système de fichier Unix).

Le nommage respecte une hiérarchie normalisée (par l'IETF) pour assurer un espace de nommage LDAP global :

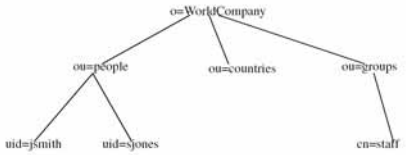


Concepts : LDAP, modèle de nommage

❏ Le Distinguished name (DN)

Référence de manière unique une entrée du DIT (⇔ path fichier UNIX).

Formé de la suite des noms des entrées, en partant de l'entrée et en remontant vers le suffix, séparé par des ",".



Ex : le DN de l'entrée `jsmith` vaut :

`uid=jsmith, ou=people, o=WorldCompany`

Chaque composant du DN est appelé Relative Distinguished Name (RDN).

Le RDN est constitué d'un des attributs de l'entrée (et de sa valeur). Le choix de cet attribut doit assurer que 2 entrées du DIT n'aient pas le même DN.

Concepts : LDAP, modèle fonctionnel

❏ Le modèle fonctionnel décrit le moyen d'accéder aux données et 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 de connexion , d'authentification et de contrôle.

Concepts : 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 qui pointe sur cette entrée.

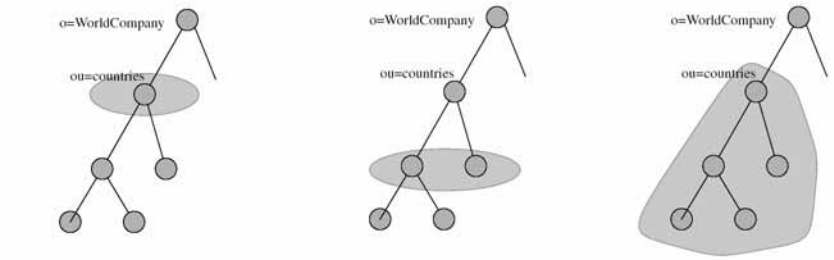
Une requête est composée de 8 paramètres :

Tableau 3 :

`base object`	l'endroit de l'arbre où doit commencer la recherche
`scope`	la profondeur de la recherche
`derefAliases`	si on suit les liens ou pas
`size limit`	nombre de réponses limite
`time limit`	temps maxi alloué pour la recherche
`attrOnly`	renvoie ou pas la valeur des attributs en plus de leur type
`search filter`	le filtre de recherche
`list of attributes`	la liste des attributs que l'on souhaite connaître

Concepts : LDAP, modèle fonctionnel

❏ Le scope



search base = "ou=countries,o=WorldCompany"

search scope = base	search scope = onelevel	search scope = subtree

Concepts : LDAP, modèle fonctionnel

❑ Les filtres de recherche (RFC 2254)

```
(<operator>(<search operation>)(<search operation>)...))
```

Tableau 4 : Exemples de filtres de recherche

(cn=Norbert Durand)	égalité	Nom vaut "Norbert Durand"
(cn=*Mart*)	sous-chaîne	Nom contient "Mart"
(cn~=martin)	approximation	Nom sonne comme "martin"
(employeenumber>=100)	comparaison	Numéro supérieur à 100
(sn=*)	existance	Tous les noms propres
(&(sn=Durand)(l=paris))	ET	Nom vaut "Durand" ET localisation vaut paris
(|(ou=gens)(ou=groupes))	OU	ou vaut gens ou groupes
(!(tel=*))	NON	Toutes les entrées sans attribut téléphone

Ex :

(&(objectclass=inetOrgPerson)(!(mail=*)))Toutes les entrées de type utilisateur sans adresse mail

Concepts : LDAP, modèle fonctionnel : mise à jour

❑ 4 opérations : `add, delete, rename, modify`

Ces quatre opérations nécessitent les droits d'accès appropriés et des prérequis :

- `add, rename` : entrée ne doit pas déjà exister, entrée doit avoir un parent existant
- `add, modify` : les attributs doivent être conformes au schéma
- `delete` : entrée ne doit pas avoir d'enfant

Concepts : LDAP, modèle de sécurité

- Le modèle de sécurité décrit le moyen de protéger les données de l'annuaire des accès non autorisés.
- 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 transactions entre clients et serveurs ou entre serveurs.

Les mécanismes qui peuvent être mis en œuvre sont ceux que l'on retrouve dans nombre de services/serveur de l'Internet :

- L'authentification
- Les signatures électroniques
- Le chiffrement
- Le filtrage réseau
- Les règles d'accès (ACLs LDAP) aux données
- L'audit des journaux

Concepts : LDAP, modèle de sécurité

L'authentification

LDAP est un protocole avec connexion : l'ouverture de session (`bind`) s'accompagne d'une identification et, éventuellement, d'un mot de passe (optionnel en V3).

- Anonymous authentification - accès sans authentification permettant d'atteindre les données sans restrictions d'accès (V2, V3).
- Root DN authentification - accès administrateur (tous les droits) (V2, V3).
- Mot de passe en clair - un DN plus un password qui transite en clair sur le réseau (V2, V3).
- Kerberos V4 (V2)
- Mot de passe + SSL (LDAPS) ou TLS - la session est chiffrée et le mot de passe ne transite plus en clair.
- Certificats sur SSL - échange de certificats SSL (clefs publiques/privées).
- Simple Authentification and Security Layer (SASL) - mécanisme externe d'authentification (V3).

Concepts : LDAP, modèle de sécurité

Le contrôle d'accès

Le serveur attribue à l'utilisateur identifié, des droits d'accès aux données (lecture, écriture, recherche et comparaison), qui lui ont été définis par l'administrateur sous la forme d'ACLs.

Pas encore normalisé par l'IETF donc non compatibles entre serveurs.

- Netscape Directory : sous la forme d'un attribut Access Control Items (`aci`)
- OpenLDAP : sous la forme de directives de contrôle d'accès dans `slapd.conf`

- Les ACLs peuvent être "placées" au niveau des entrées, au sommet de l'arbre ou sur un sous-arbre.
  Elles agissent sur les entrées ou certains de leurs attributs.
  Elles s'appliquent à des individus ou à des groupes, mais aussi suivant les adresses IP ou les noms de domaine des clients ou les jours et heures.
  Le placement et la portée des ACLs dépendent des capacités du logiciel.

Concepts : LDAP, modèle de sécurité

- Expression générique des ACLs :

```
<quoi> <qui> <comment>
      <quoi> : point d'entrée de l'annuaire auquel s'applique la règle
      <qui> : à qui s'appliquent ces droits
      <comment> : opérations autorisées/refusées
```

<comment>	<qui>
Read	Tout le monde
Write	Un utilisateur
Search	Un groupe d'utilisateur
Compare	Une machine
Selfwrite	
Add	
Delete	

Exemple openldap :

```
access to * by self write
      by * read
```

Concepts : LDAP, modèle de sécurité
Le chiffrement

LDAPv3 supporte le chiffrement des transactions (entre clients et serveurs ou entre serveurs) via l'utilisation de SSL (`ldaps`) ou de son successeur, TLS (`startTLS extended operation`).

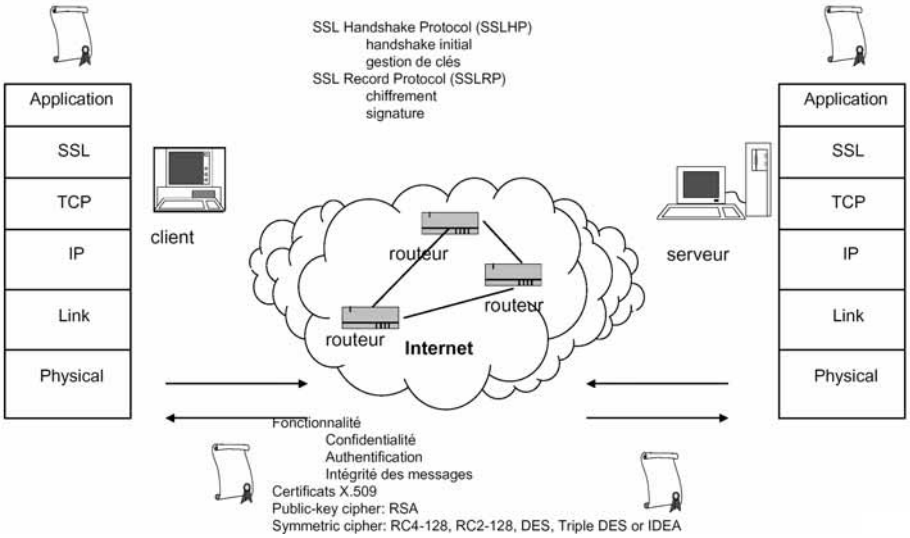
SSL ou TLS servent également pour l'authentification par certificats :

- permet au client de prouver son identité au serveur et, en retour, à celui-ci d'en faire de même vis à vis du client.

Concepts : LDAP, modèle de sécurité
Le chiffrement

- SSL : Secure Socket Layer
- Protocole de sécurité d'Internet pour les connexions point-à-point
- Développé par Netscape pour garantir la sécurité de la transmission de données sur Internet
- Version actuelle : SSL 3.0
- Fournit une connexion sécurisée entre le client et le serveur
- Protocole entre TCP et les protocoles applicatifs
- 2001 : l'IETF rachète le brevet de SSL à Netscape et le rebaptise TLS (Transport Level Security, RFC 2246) (version 1.0)

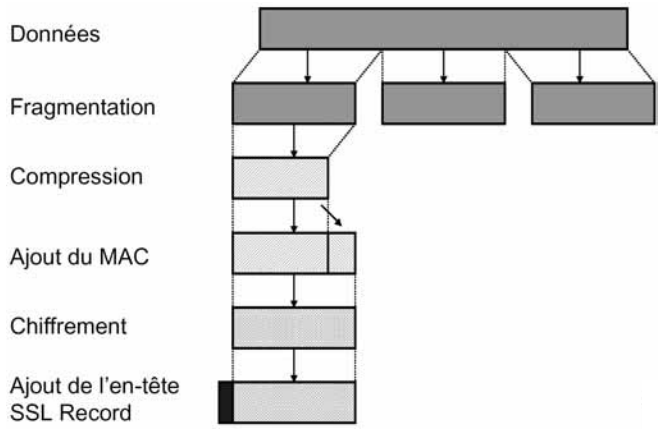
SSL : Secure Socket Layer



SSL Record Protocol

- Ce protocole fournit 2 services à une connexion SSL :
  - Confidentialité : définit une clé secrète pour le chiffrement
  - Intégrité du message : définit une clé secrète pour le calcul de l'empreinte
- SSL Record Protocol : opérations
  - Fragmentation :
    - Le message est fragmenté en blocs de taille maximum 2^{14} octets
  - Compression :
    - Cette opération est prévue dans les spécifications mais non implémentée
  - Calcul du MAC :
    - Utilise la clé secrète
    - Utilise l'algorithme SHA-1 ou MD5
  - Chiffrement :
    - Le message + MAC sont chiffrés avec un chiffrement symétrique
  - Ajout de l'en-tête :
    - 5 octets, composée de longueur du message, version, etc.

SSL Record Protocol



LDAP : APIs

- Ces bibliothèques de programmation permettent de créer des applications annuaire-compatibles.
- Les APIs disponibles actuellement :
  - U-M LDAP SDK -- C (UMICH, OpenLDAP)
  - Innosoft LDAP Client SDK (ILC-SDK) -- C (InnoSoft)
  - Netscape Directory SDK -- Java, C (Netscape)
  - PerLDAP Modules -- Perl (Netscape)
  - Net- LDAPapi -- PERL (GNU)
  - Java Naming and Directory Interface (JUNI) -- Java (SUN)
  - Active Directory Service Interface (ADSI) -- COM (Microsoft)

Logiciels serveurs

A cette date, les logiciels les plus connus sont :

- **OpenLDAP server,**
- **Innosoft's Distributed Directory Server,**
- **Netscape Directory Server,**
- **Sun Microsystems's Directory Services,**
- **IBM's DSSeries LDAP Directory,**
- **University of Michigan's SLAPD.**

D'autres annuaires supportent les requêtes au format LDAP :

- **Novell's NetWare Directory Services (NDS) 3.0,**
- **Microsoft's Active Directory (AD),**
- **Lotus Domino.**

Clients LDAP

- **Accès natif :**
  - **Netscape Communicator**
  - **Microsoft Outlook, NetMeeting**
  - **Netscape SuiteSpot (les serveurs mail, news, web...)**
  - **Oblix (gestionnaire d'annuaire)**
  - **Navigateur Web : URLs LDAP**
  - **U-Mich xaX.500**
  - **GQ (GTK-based LDAP client)**
  - **LDAP Browser/Editor (Java-based LDAP client)**
  - **Applications développées avec un SDK LDAP**
- **Accès via passerelle :**
  - **LDAP vers X.500 et X.500 vers LDAP**
  - **HTTP vers LDAP (web500gw)**
  - **WHOIS++ vers LDAP**
  - **FINGER vers LDAP**
  - **PH/CSO vers LDAP**

Bibliographie

- **RFC2251: « Lightweight Directory Access Protocol (v3) »**
- **RFC2252 : « Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions »**
- **RFC2253 : « Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names »**
- **RFC2254 : « The String Representation of LDAP Search Filters »**
- **RFC2255 : « The LDAP URL Format »**
- **RFC2256 : « A Summary of the X.500(96) User Schema for use with LDAPv3 »**
- **RFC2829 : « Authentication Methods for LDAP »**
- **RFC2830 : « Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security »**
- **RFC3377 : « Lightweight Directory Access Protocol (v3): Technical Specification. »**

- **RFC1617 : « Naming and Structuring Guidelines for X.500 Directory Pilots. » (Status: INFORMATIONAL)**
- **RFC2247 : « Using Domains in LDAP/X.500 Distinguished Names. »**
- **RFC2307 : « An Approach for Using LDAP as a Network Information Service. »**
- **RFC2798 : « Definition of the inetOrgPerson LDAP Object Class. » (Status: INFORMATIONAL)**
- **RFC2820 : « Access Control Requirements for LDAP. » (Status: INFORMATIONAL)**
- **RFC2891 : « LDAP Control Extension for Server Side Sorting of Search Results. »**
- **...**

Bibliographie

- Linuxworld LDAP in action:
  `http://linuxworld.com/linuxworld/lw-1999-07/lw-07-ldap_1.html`
- Linux LDAP services:
  `http://www.rage.net/ldap/`
- OPenLDAP.org:
  `http://www.openldap.org`
- Netscape Deployment Guide:
  `http://developer.netscape.com/docs/manuals/directory/deploy30/index.htm`
- LDAP FAQ:
  `http://www.critical-angle.com/ldapworld/ldapfaq.html`
- LDAP roadmap and FAQ:
  `http://www.kingsmountain.com/ldapRoadmap.shtml`
- LDAP Central
  `http://www.ldapcentral.com/`
- Understanding and deploying LDAP directory services, T. Howes, M. C. Smith, G. Good; Macmillan

→ **http://www.commentcamarche.net/ldap/ldapinst.php3**

www.coagul.org