L.D.A.P

Lightweight Directory Access Protocol

Qu’est ce qu’un annuaire ?

- Une collection structurée d’informations sur des personnes ou des machines et autres ressources
- Ex:
  - finger
  - whois
  - dns
  - carnet d’adresses électronique
  - /etc/passwd

Problèmes des annuaires traditionnels

- Mise à jours multiples
  - incohérences
  - redondances
  - sécurité
- interfaces différentes
- espace de nommages distincts
- “Îlots de données”
- RECHERCHE DIFFICILE

X.500

- 1988:Série de standards produits par l'ISO , définissant les protocoles et le modèle informationnel pour un service d'annuaire global
  - distribué
  - maintenance décentralisée
  - puissantes capacités de recherche
  - un espace de nommage unifié
  - structure hiérarchique d'objets
- 1993: 2eme mouture
  - sécurité
  - réplication

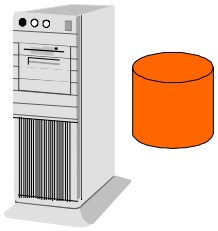
Défauts de X.500

- Basé sur la couche réseau I.S.O
- complexe à mettre en œuvre
- D.A.P (Directory Access Protocol)
- gourmand en ressources
- réalisé par l’ ISO :−)

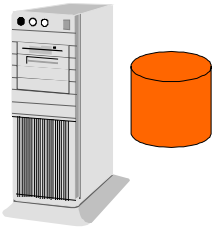
L.D.A.P

- Permet d’accéder à un serveur X.500, ou fonctionne de manière autonome
- Conçu pour tourner au dessus de TCP/IP
- léger
- A.P.I standard

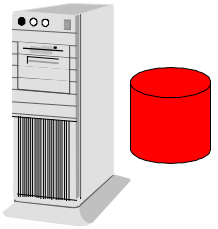
annuaires isolés



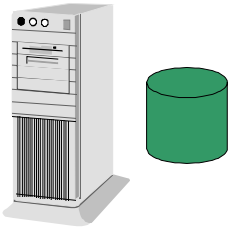
Serveur de fichiers



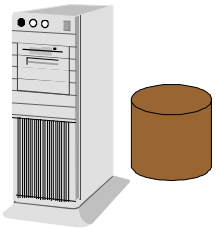
Base RADIUS



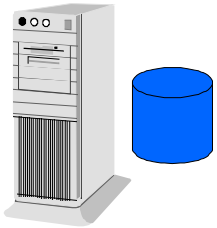
Serveur unix



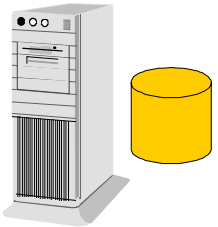
Passerelle Internet



Serveur NT

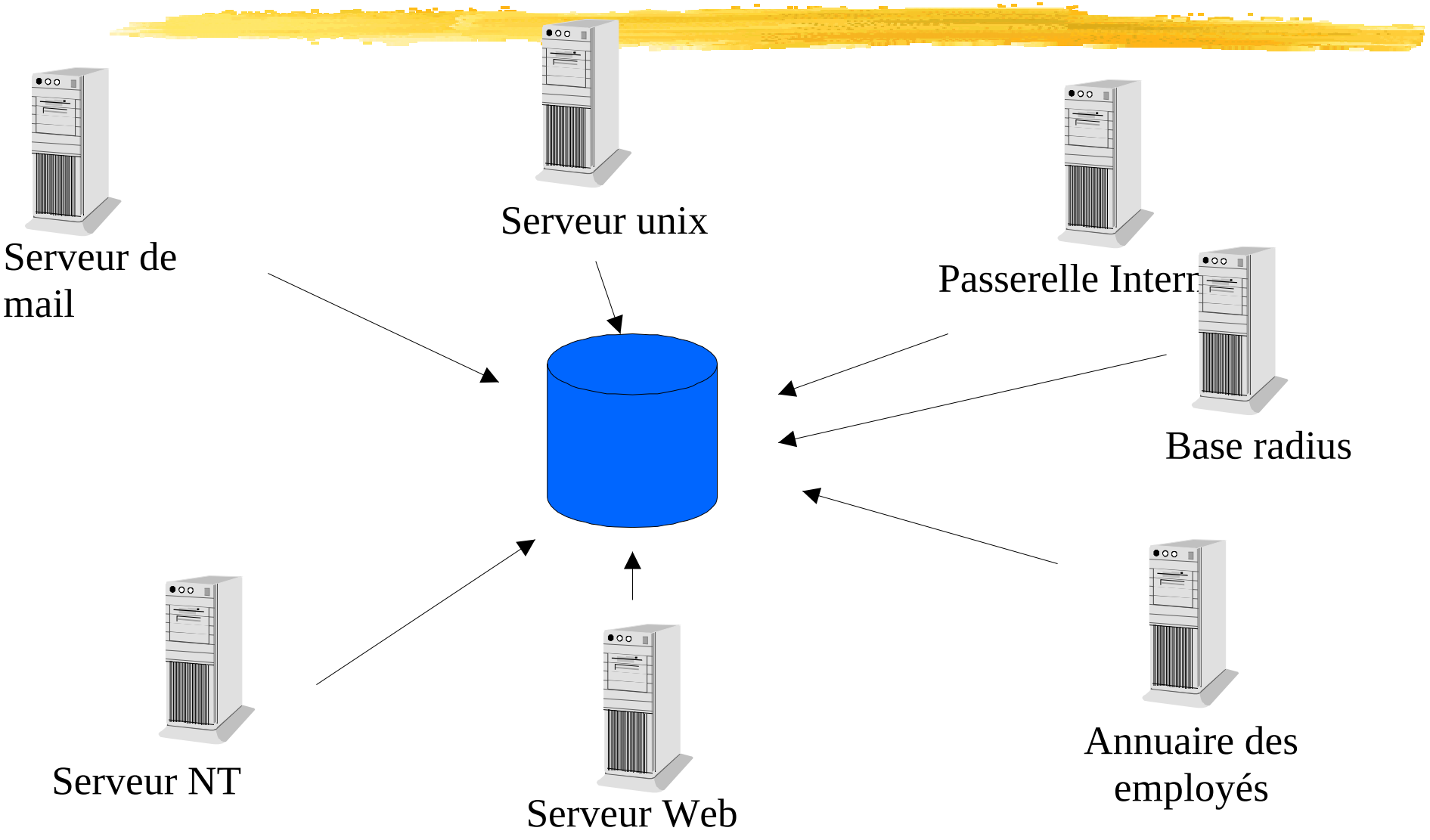


Serveur Web

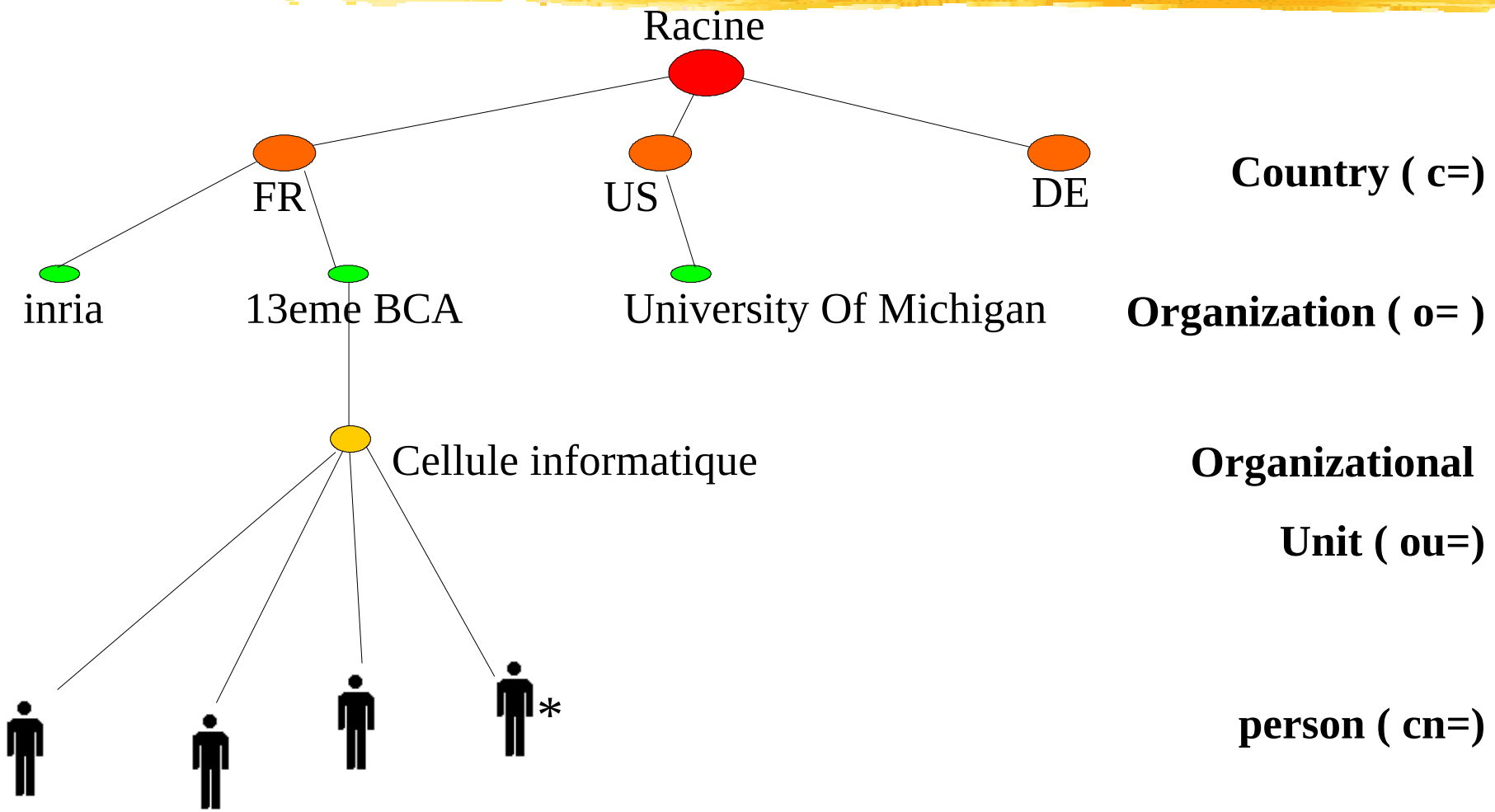


Annuaire des employés

Un annuaire unique



Un annuaire global



(*)DN: Cn=Duhaut Renaud, ou=Cellule informatique, o=13eme BCA, c=FR

Structure d’un annuaire LDAP

- Hiérarchie d’objets nommés.
- Chaque enregistrement comprend :
  - un identifiant unique : DN (Distinguished Name)
  - une ou plusieurs classes (objectclass) définissant les attributs possibles (obligatoires ou facultatifs)
  - des attributs (couple nom : valeur)

DN : Distinguished Name

- Identifiant unique d’un objet dans l’annuaire
- reflète la position de l’enregistrement dans l’annuaire hiérarchique
- Exemple:
  dn: ou=Cellule informatique,o=13eme BCA,c=FR

Exemple d’ objectclass

```
objectclass person
    requires
        objectClass,
        sn,
        cn
    allows
        description,
        mail,
        telephoneNumber,
        GivenName,
        userPassword
```

Classe de l’objet

Attributs obligatoires

Attributs facultatifs

Le format LDIF

```
dn: cn=Emmanuel DECAEN, o=decaen, c=FR
cn: Emmanuel DECAEN
sn: DECAEN
mail: ed@decaen.com
givenname: Emmanuel
objectclass: top
objectclass: person
```

Referrals

- ObjectClass particulière permettant de référencer un autre serveur détenant l’information:
- Exemple:
  dn: ref=“ldap://ldap.guilde.asso.fr/o=Guilde, c=FR”, o=13eme BCA, c=FR

objectclass: referral

Usages : aujourd'hui et demain

- Carnet d'Adresse
- Gestion des utilisateurs et Authentification
- Gestion de parc ou de ressources (salles de réunion par exemple)
- profils utilisateurs
- Annuaire téléphonique
- D.E.N (Directory Enabled Network)
- Radius

Applications

- Browsers Web (Navigator,IE...)
- Clients mail (Eudora)
- Agendas de groupe (Outlook,Lotus Notes, Lotus domino)
- PGP
- Linux Directory Project

- Basé sur la version 3.3 du serveur LDAP de l'université du Michigan
- Open Source
- fonctionne en mode "Stand Alone" ou comme une passerelle vers un annuaire X.500
- Version actuelle : 1.2.3

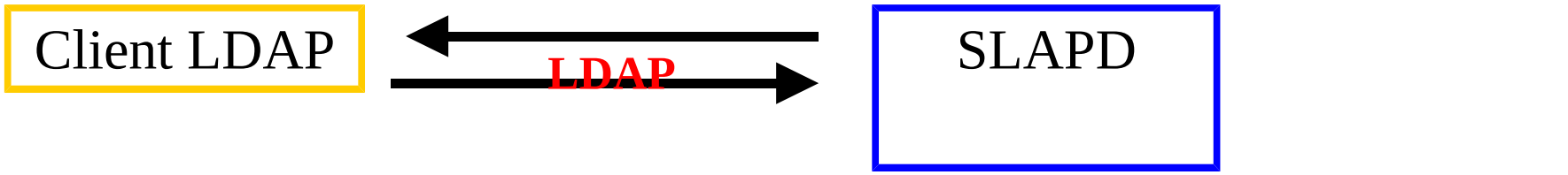
Caractéristiques

- Multiples instances
- Contrôle d’accès
- Réplication (non normalisé)
- API pour l’accès physique à la Base de données
- Multi−Threads

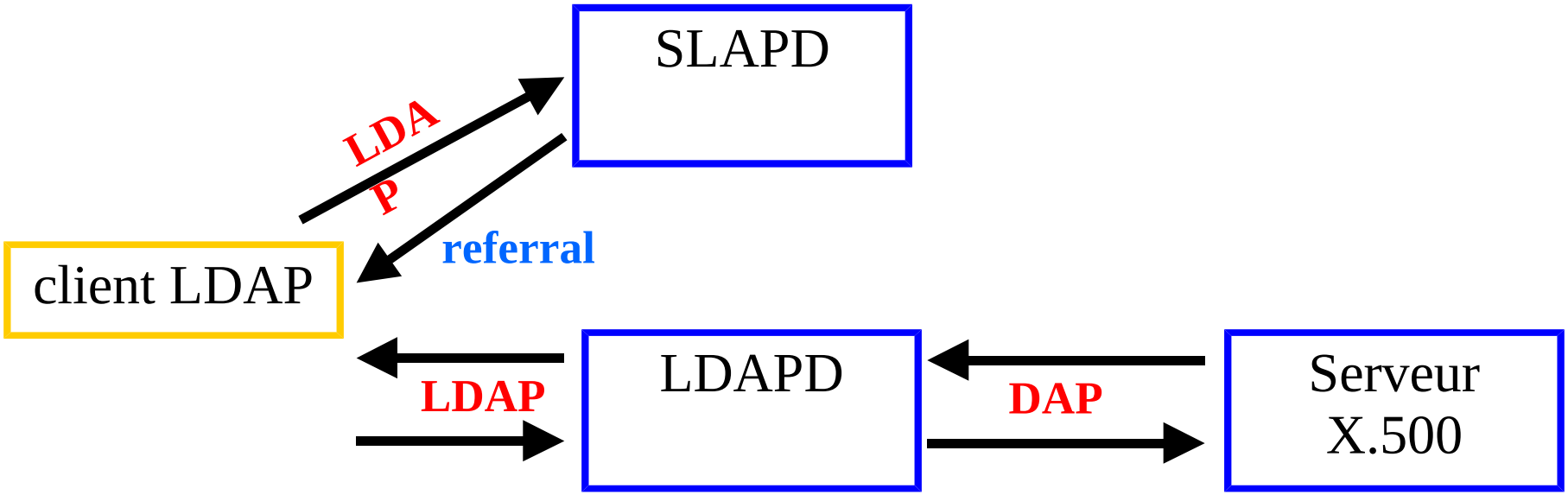
Composants d'openldap

- Serveur SLAPD ou LDAP
- Agent de réplication SLURPD
- Outils clients
  - ldapsearch
  - ldapadd
  - ldapmodify
  - ldapdelete
- Outils d'indexation de la base

Architecture



Service local seulement



Service local avec une passerelle vers X.500

SLAPD.CONF

```
Include             slapd.at.conf
include             slapd.oc.conf
schemacheck off
referral    ldap://ldap.itd.umich.edu
########################################################
# ldbm database definitions
########################################################

database    ldbm
suffix              "dc=your domain, dc=com"
#suffix             "o=Your Organization Name, c=US"
directory   /usr/lib/annuaire
rootdn              "cn=root, dc=your domain, dc=com"
#rootdn             "cn=root, o=Your Organization Name, c=US"
rootpw              secret
```

Linux Directory Project et NSSLDAP

- Remplace NIS
- 2 librairies :
  - /lib/libnss_ldap.so qui fournit l'accès à l'annuaire LDAP au programmes consultant la base des utilisateurs,des machines,des services…
  - /lib/security/pam_ldap.so.1 pour tout ce qui est authentification (repose sur PAM)

Linux Directory Project ou NSSLDAP vs NIS

Avantages par rapport à NIS

- utilise un port prédéfini (filtrage)
- Cryptage des données via SSL
- Authentification
- Access Control List
- plus de possibilités de stockage (certificats par exemple)

References

- RFC 1308: Executive introduction to Directory Services using the X.500 protocol
- RFC 1309: Technical Overview of Directory Services using The X.500 protocol
- RFC 1777: Lightweight Directory Access Protocol
- RFC 1430: A strategic plan for deploying an Internet X.500 Directory Service
- RFC 2307: An approach for using LDAP as a Network Information Service

Webographie

- Projet Openldap :
  http://www.openldap.org
- Serveur LDAP de l'université du Michigan
  http://www.umich.edu/~rsug/ldap/
- FAQ LDAP−X.500
  http://www.stanford.edu/group/networking/directory/x500ldapfaq.html
- Linux Directory Service
  http://www.rage.net/ldap/
- LDAP HOWTO (en français)
  http://**www.linux−france.com/article/serveur/ldap/**

Atelier sur les annuaires LDAP

RENDEZ VOUS

LE 30 JUIN 1999 à 19h30

AU LYCEE Ferdinand Buisson (La NAT)

A VOIRON