UMR 6614

COMPLEXE DE RECHERCHE
INTERPROFESSIONNEL EN AEROTHERMOCHIMIE

CNRS – UNIVERSITE et INSA de Rouen

LDAP au CORIA

Journée RESINFO

10 juin 2005

Henri Cavalier

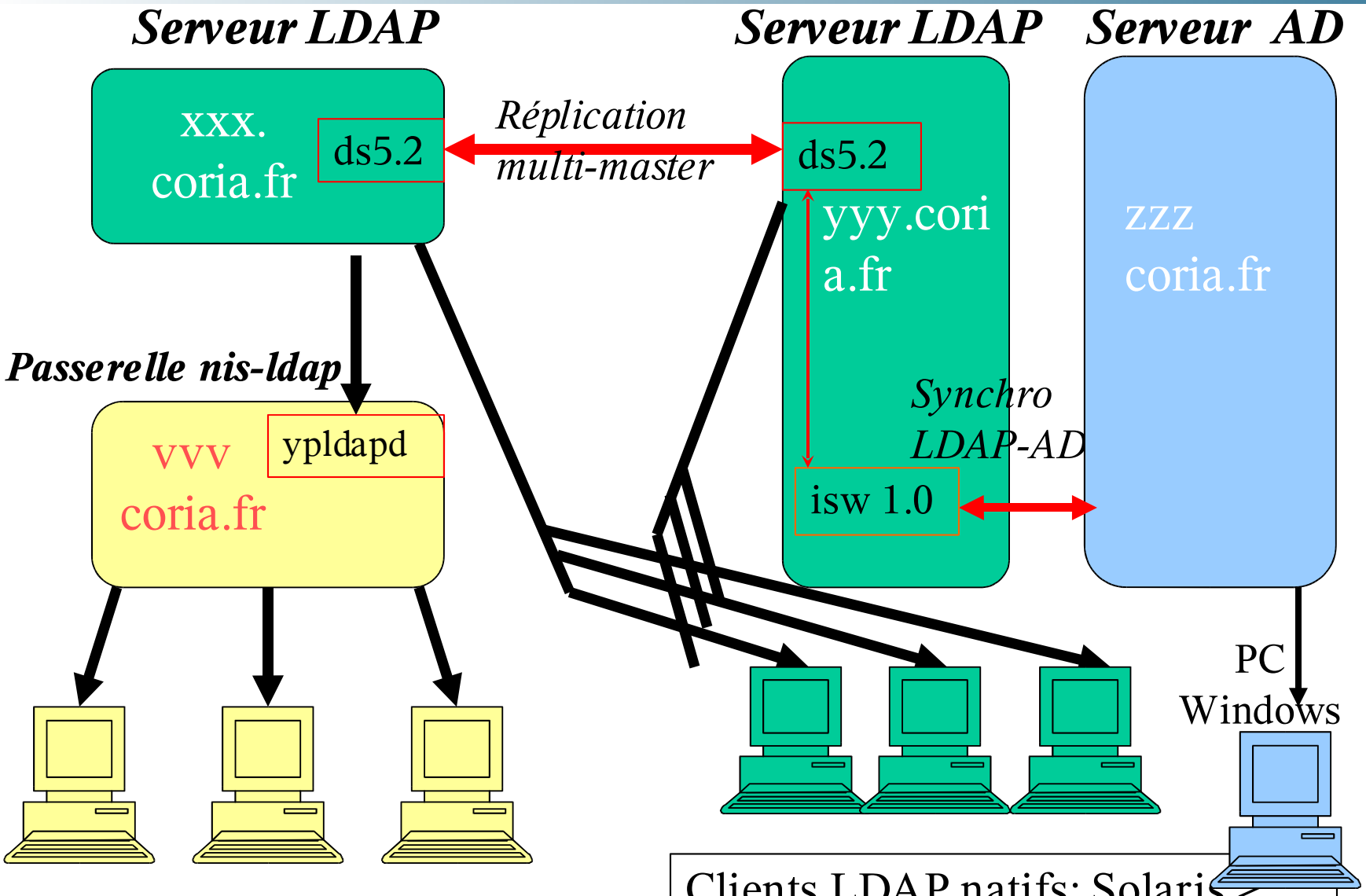
PLAN

- Topologie des serveurs d'annuaire au CORIA
- Passerelle NIS/LDAP: ypldapd (PADL)
- Synchronisation LDAP/AD: ISW (SUN)
- Applications:
  - –Authentification des utilisateurs
  - –Mail :Postfix
  - –Autres …

Serveurs d'annuaire au CORIA

- 3 domaines (coria.fr)
  - –Domaine AD : monde Windows et Samba
  - –Domaine LDAP : authentification sur machines unix récentes et annuaires divers (mail, …)
  - –Domaine NIS: authentification sur machines Unix qui ne supportent pas d'autres services
- Nécessité de synchronisation LDAP/NIS et LDAP/AD

Topologie des serveurs d'annuaire au CORIA



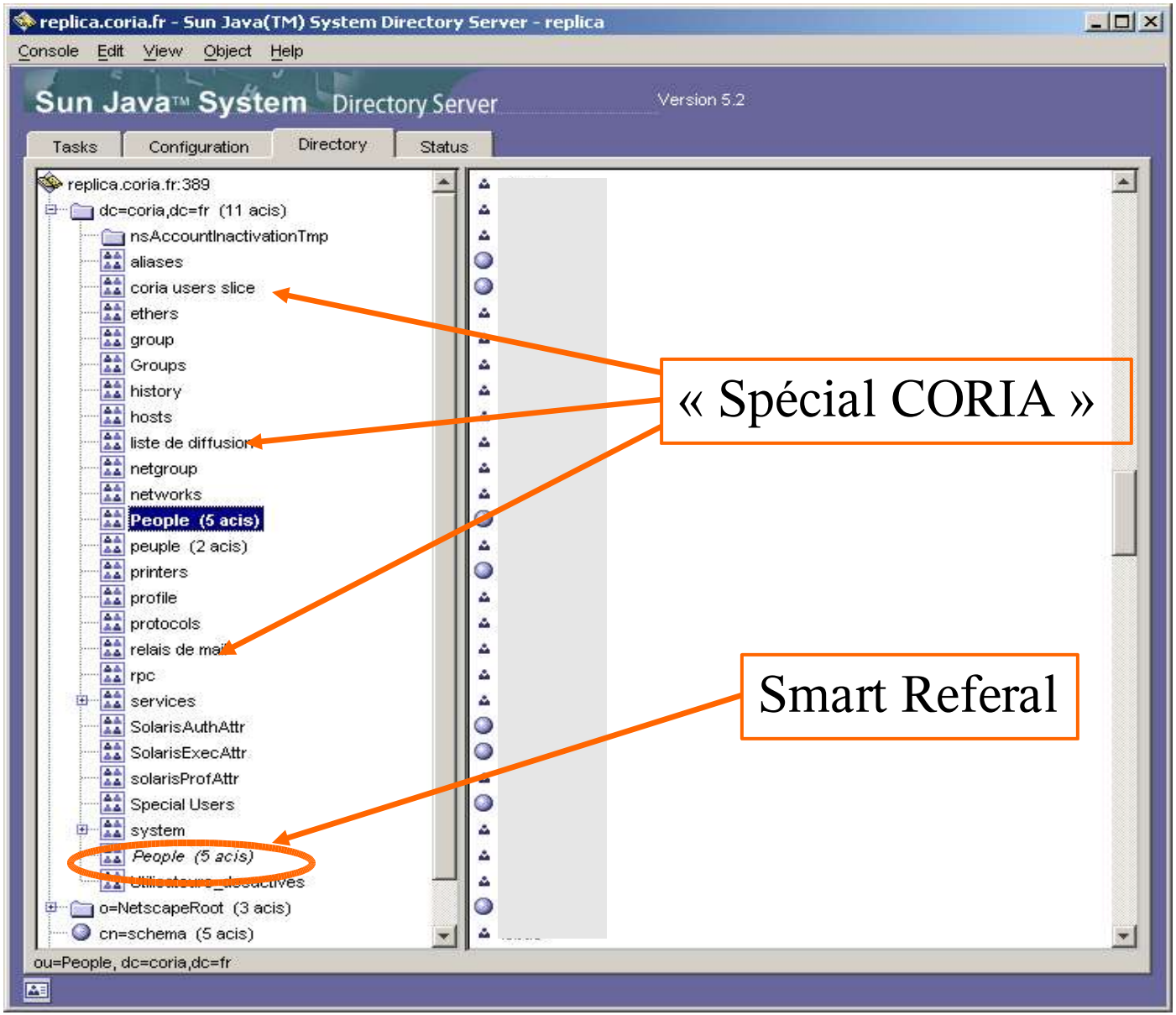
Clients NIS:solaris<2.8, vieux linux, TRU64<5.0, HPUX<11,…

Clients LDAP natifs: Solaris ≥ 2.8, linux récents, TRU64≥5.0, …

Choix d'un serveur LDAP

- Choix de DIRECTORY SERVER (Sun Microsystems):
  - Connaissance de l'OS
  - Disponibilité d'un support Hot Line SUN au CORIA
  - Simplicité de mise en œuvre d'un doublon master-replica en mode multi-masters
  - Disponibilité d'un logiciel de synchronisation LDAP/Active Directory du même éditeur
- Prochainement disponible sous RedHat

SunOne Directory Server



Cas des machines « vieillissantes »

➢Pour certaines machines (vieux linux, Solaris < 2.8, TRU64 < 5, HPUX < 11, …)

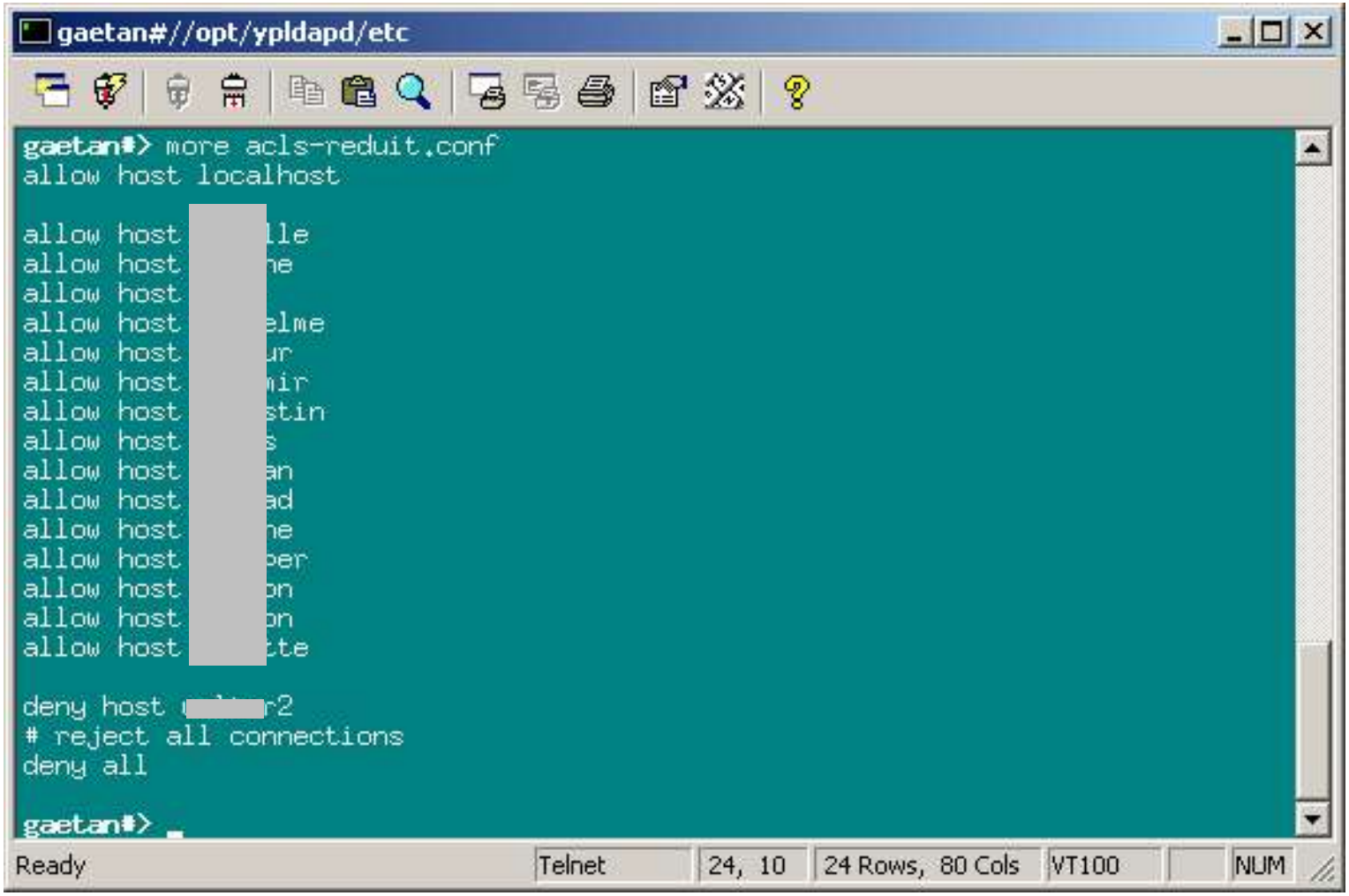
- Utilisation d'un domaine NIS (Partiellement pré-existant)
- Utilisation d'une passerelle NIS/LDAP: ypldapd de PADL

Ypldapd de PADL

Passerelle entre NIS (yp) et LDAP

- Serveur de domaine NIS pour les clients NIS
- Client LDAP
- Les domaines NIS et LDAP ont le même nom
- S'installe sur une machine linux ou solaris préalablement cliente d'un serveur LDAP
- Synchronise les maps NIS périodiquement (10 mn) sur le serveur LDAP
- *Mais la mise à jour des passwd depuis les clients NIS n'est pas possible.*
- Supporte par configuration un minimum de sécurité:
  - Securenets: liste de réseaux sûrs
  - Filters: liste de maps NIS à cacher
  - ACLs: liste de machines ou réseaux allow/deny.

Ypldapd: ACLs



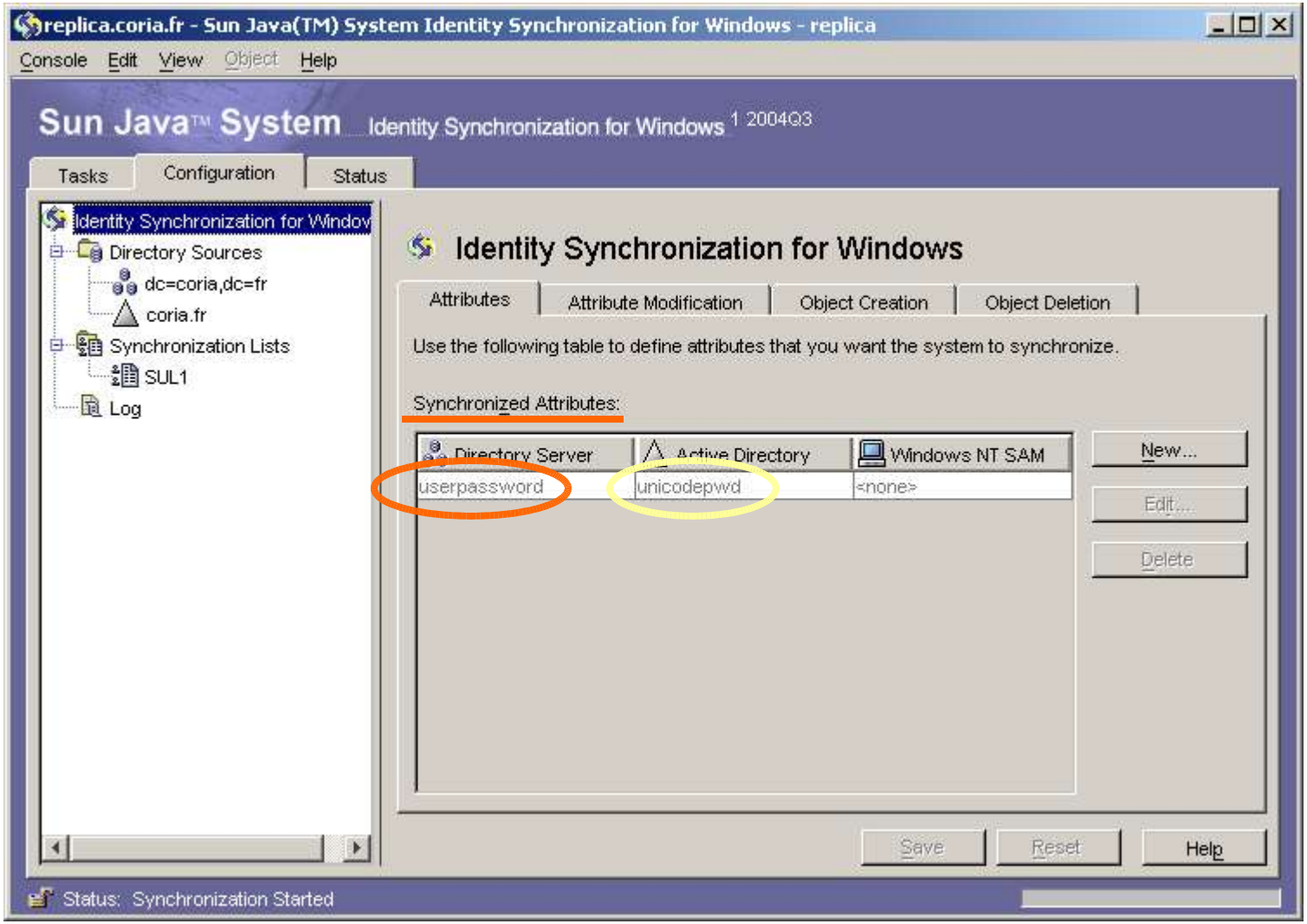
ISW: Identity Synchronization for Windows

- Produit SUN installé sur un des 2 serveurs LDAP
- Assure la synchro bidirectionnelle des mots de passe entre LDAP et AD grâce à des « connecteurs » (Déploiement en cours)
- La réplication multi-masters propage les infos sur le 2ème serveur
- Peut assurer la synchro. à la création des users (Ultérieurement)

ISW: Remarques

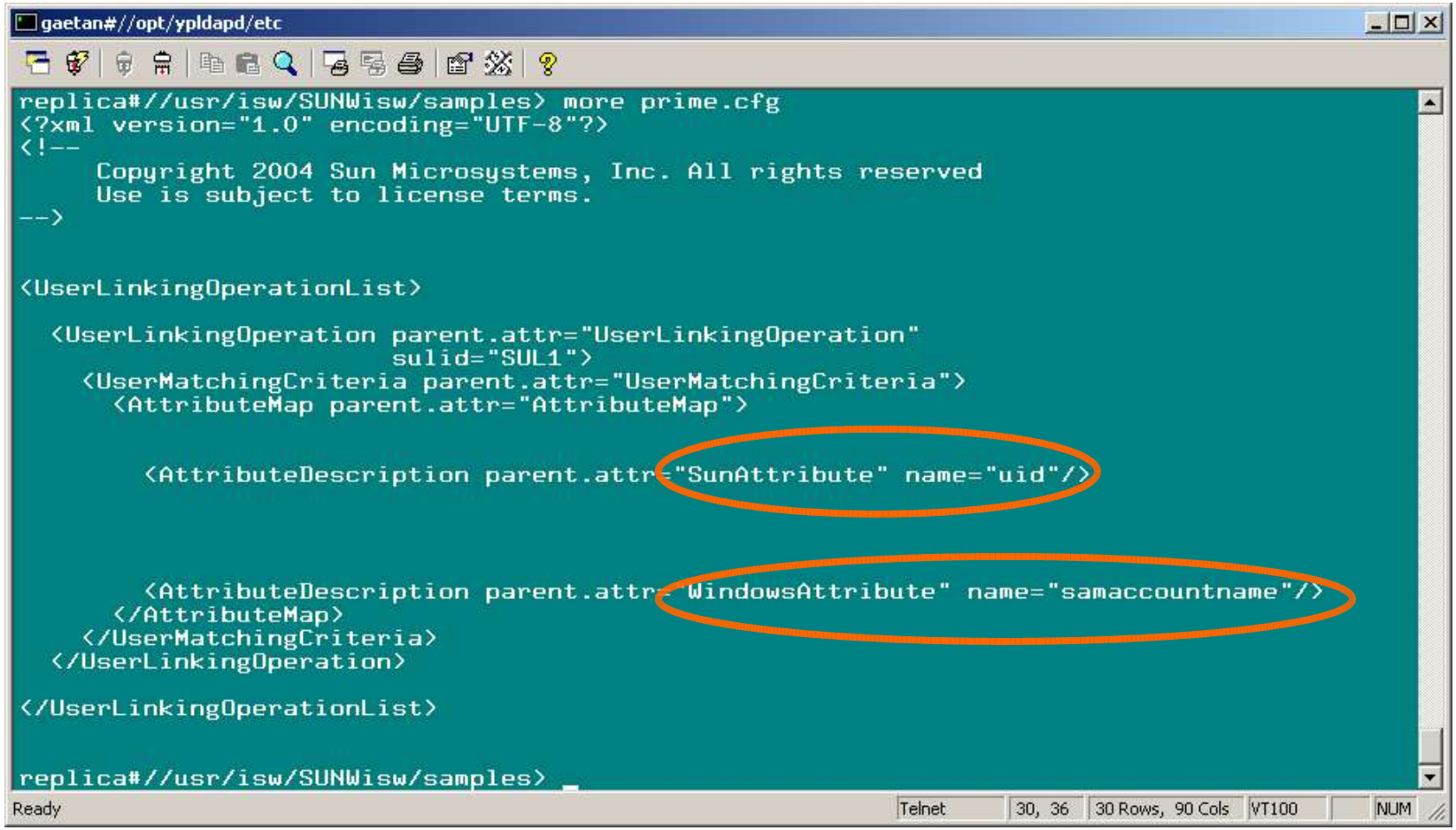
- Les mots de passe sur le DS doivent être au format « crypt » pour les NIS
- la synchronisation des passwd Windows vers Unix n'est pas problématique
- La synchronisation des passwd Unix vers Windows nécessite SSL (LDAPS) et donc la mise en place de certificats sur les 2 serveurs d'annuaire (Certificats CNRS standards)

ISW Console


replica.coria.fr - Sun Java(TM) System Identity Synchronization for Windows - replica
Console Edit View Object Help
Sun Java™ System Identity Synchronization for Windows 1 2004Q3
Tasks Configuration Status
Identity Synchronization for Windov
Directory Sources
dc=coria,dc=fr
coria.fr
Synchronization Lists
SUL1
Log
Identity Synchronization for Windows
Attributes Attribute Modification Object Creation Object Deletion
Use the following table to define attributes that you want the system to synchronize.
Synchronized Attributes:
Directory Server
Active Directory
Windows NT SAM
userpassword
unicodepwd
<none>
New...
Edit...
Delete
Save Reset Help
Status: Synchronization Started

ISW: critères de correspondance

•La correspondance entre les attributs LDAP et AD est effectuée via un fichier de config. au format XML



Applications 1

Authentification des utilisateurs

➢A la création des utilisateurs:

- Gestion de la répartition des « UidNumber »
- A l'instant
  - Pour créer les entrées LDAP utilisation de scripts PERL
  - Entrée directe sur le serveur AD des utilisateurs Windows
- A venir prochainement:
  - A partir d'une interface web, inscription des nouveaux arrivants dans le labo: téléphone, codes divers, création de login unix et windows (à terme par synchro ISW), …

Applications 2

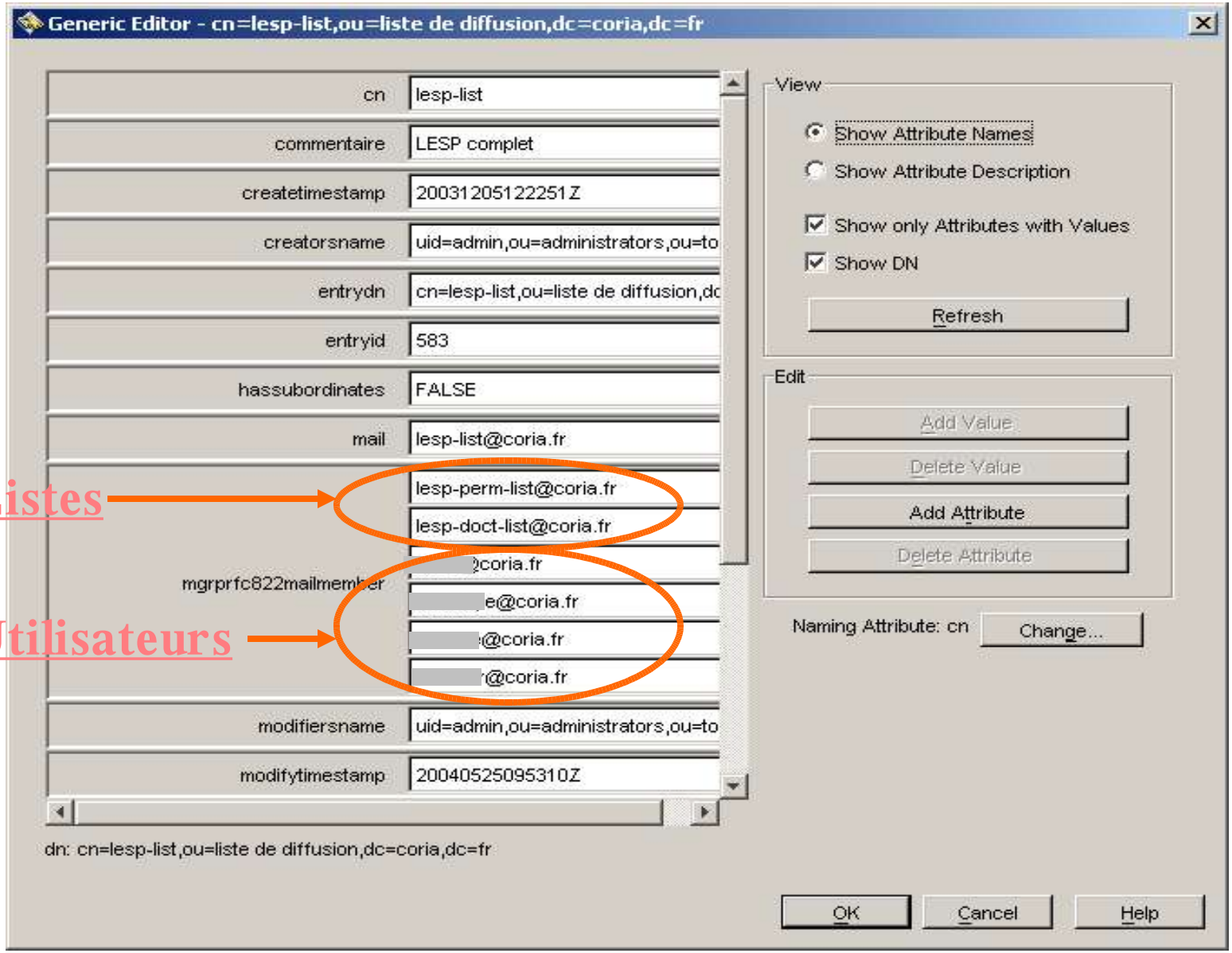
Autres applications

- Mail: ***postfix*** consulte ses informations sur le serveur LDAP
  - Entrée liste de diffusion
  - Entrée relais de mail
  - Entrée utilisateur standard
- Tables dhcp, copiées périodiquement sur le serveur dhcp (indépendance des services par sécurité) (en projet)

Postfix: Liste de diffusion

- Listes gérées en tant qu'alias (passé …)
- « ou » composée de classes « mailgroup »
- Modification du schéma (Non standard)
- Comprend essentiellement 3 objets obligatoires:
  - Nom de la liste
  - mail de la liste (unique)
  - mailMember (multiple) qui peut être lui-même une liste. Exemple:

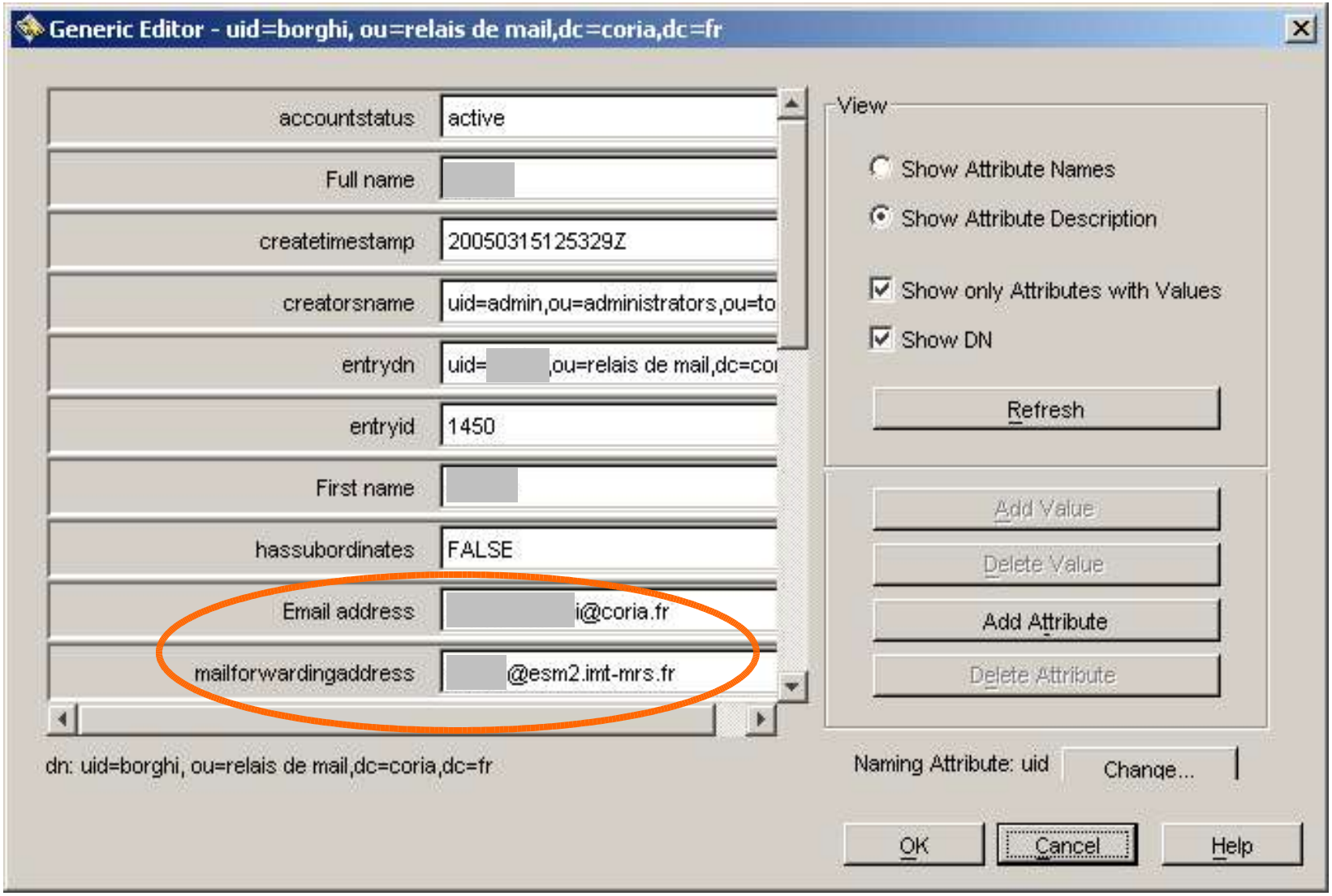
Postfix: Exemple de liste de diffusion



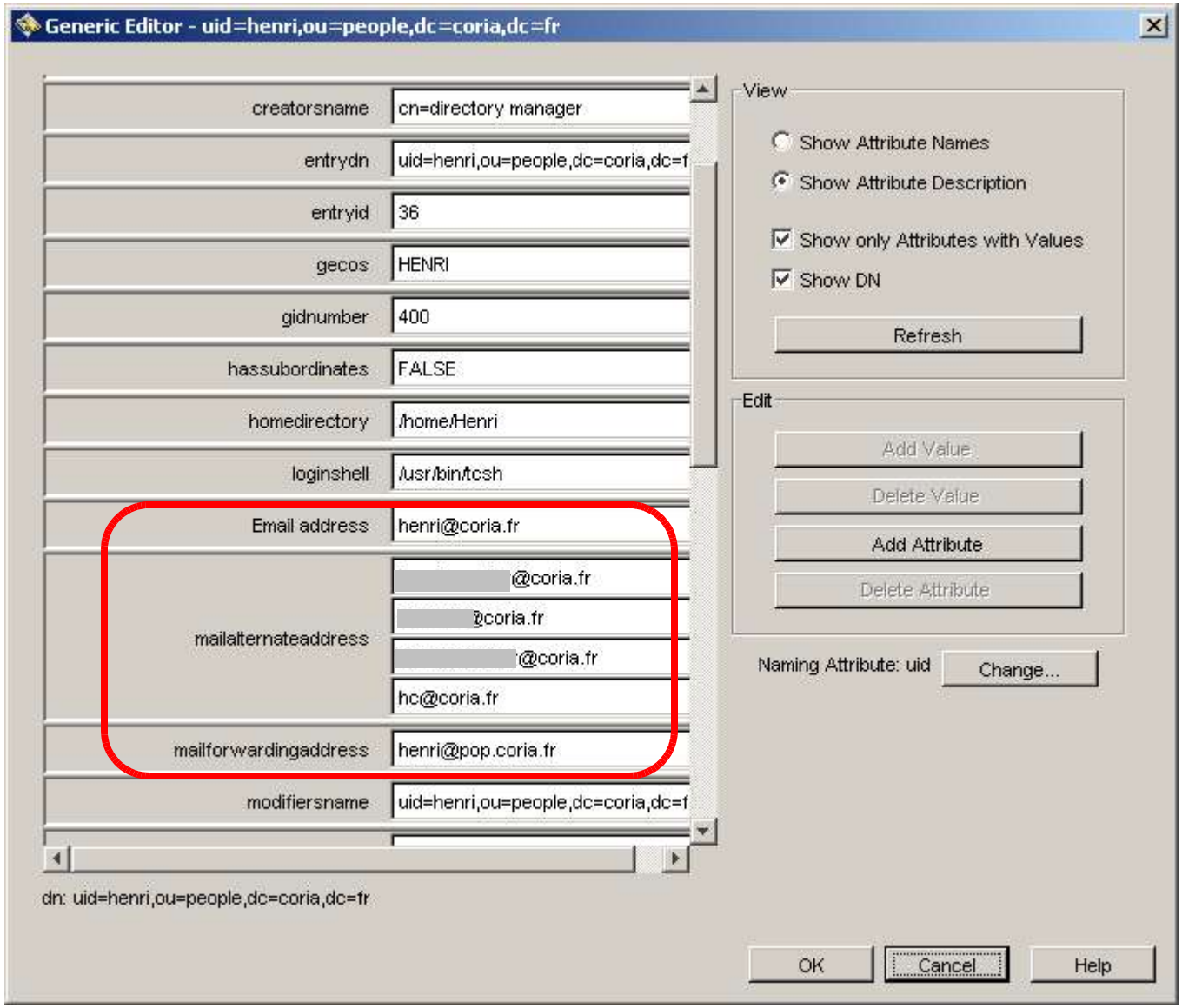
Postfix: relais de mail

- Pour les utilisateurs n'ayant pas de compte local
  - On se limite à renvoyer leur mail vers une adresse extérieure
- « ou » « relais de mail » composée de pseudo-users inaccessibles à l'authentification
- Consultation par postfix après les users standards de « ou=people »

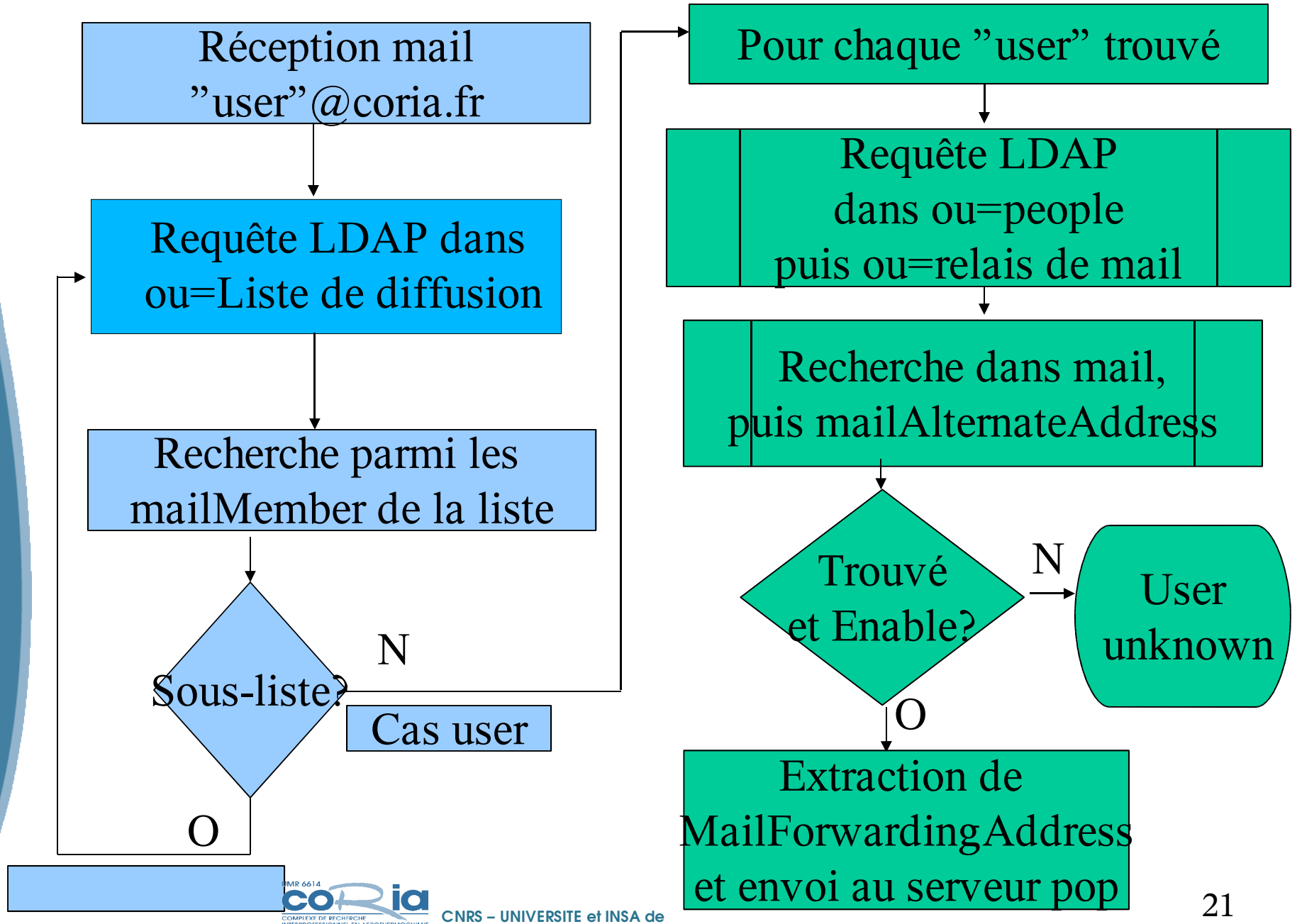
Postfix: Exemple de relais de mail



Postfix: Exemple d'utilisateur



Postfix: requêtes à l'annuaire LDAP



CONCLUSION

- Système actuellement largement surdimen-sionné pour l'utilisation
- Tests de charge à faire quand les applications seront plus nombreuses
- Attention à ne pas installer sur le serveur tous les services *(pas tous les œufs dans le même panier !),* par sécurité et par simplicité de résolution des problèmes. Ex.: DHCP.

CONCLUSION

VOS QUESTIONS

UMR 6614
COMPLEXE DE RECHERCHE INTERPROFESSIONNEL EN AEROTHERMOCHIMIE