

Linux Administration

- Université de La Rochelle

Lundi

- **Matin**
 - **Accueil**
 - **Les utilisateurs**
 - **Création / suppression**
 - **Gestion des Quotas**
- **Après midi**
 - **Mise en réseau**
 - **Serveur DHCP**

Mardi

- **Matin**
 - Mise en oeuvre de serveurs DNS maître et esclave
- **Après midi**
 - Découverte LDAP
 - Authentification centralisée
 - Répertoires personnels distants
 - Mise place serveur LDAP

Mercredi

- **Matin**
 - **SAMBA LDAP**
 - **Construction d'un PDC avec SAMBA**
- **Après midi**
 - **Questions diverses**
 - **Évaluation**

Les utilisateurs

- Création / suppression
- Les quotas

gestion des utilisateurs

- les utilisateurs sont gérés par :
 - /usr/sbin/useradd | groupadd
 - /usr/sbin/userdel | groupdel
 - /usr/sbin/usermod | groupmod
 - /usr/bin/passwd
- Les fichiers concernés sont
 - /etc/passwd
 - /etc/group
 - /etc/shadow

TP1

En vous aidant du fameux manuel

- Créez un utilisateur
 - Robert Bidochon
 - Login : rbidochon
 - Password : bidoche
 - Répertoire : /home/bd/rbidochon
 - Groupe principal users
 - Groupe secondaire **tpuser**

TP1

- Modifiez votre utilisateur
 - Maintenant on l'appelle Raymonde
 - Login : rbidochon
 - Password : RayCharles2;
 - Répertoire : /home/bd/rbidochon
 - Groupe principal utilisatrices
 - Groupes secondaires users et tpuser

TP 2

- Écrivez un script bash qui crée les utilisateurs dont la liste est contenue dans un fichier texte à définir
- Vous trouverez sur <http://enseignant.tp.org/RPM/divers/> un outil pour générer des mots de passe et qui va nous servir à chiffrer.
- Syntaxe :
`makepasswd -p <mot de passe> -e shmd5`

TP 2

```
if [ <condition> ]
then
    for [ <condition> ]
    do
        user=
        pass=
        login=
        nom=
        /usr/sbin/useradd -c "$nom" -p $pass $login
        let i=$i+1
    done
else
    echo "vous n'êtes pas root"
fi
```

Les quotas

- Concernent un système de fichiers (une partition) dans sa totalité
- Concernent des utilisateurs et/ou des groupes
- Définissent des limites en blocs et/ou inodes
- Définissent des limites «soft» et/ou «hard»

TP Quotas

- 10.2.10.88/Administration/TP_quotas.html

Mise en Réseau

- Pérenne
- Volatile

Mise en réseau pérenne

- Configuration des interfaces
 - Red Hat : `/etc/sysconfig/network-scripts/ifcfg_ethX`
 - Debian : `/etc/network/interfaces`
- DNS : `/etc/resolv.conf`
- Passerelle par défaut
 - Paramètre «GATEWAY» dans le fichier de configuration d'interface
 - Définir plusieurs passerelles sur plusieurs interfaces => ???

Routage

- Routes statiques
 - ajouter des lignes «route add» dans /etc/rc.d/rc.local (/etc/init.d/rc.local pour debian)
- Forwarding : /etc/sysctl.conf
 - net.ipv4.ip_forward=1

Routage statique

- Red Hat

```
/etc/sysconfig/static-routes  
GATEWAY0=192.168.55.0  
NETMASK0=255.255.255.0  
ADDRESS0=192.168.1.254  
  
GATEWAY1=10.164.234.112  
NETMASK1=255.255.255.240  
ADDRESS1=192.168.1.253
```

- Debian

```
•/etc/network/interface  
auto eth0  
iface eth0 inet static  
address 192.168.1.2  
netmask 255.255.255.0  
gateway 192.168.1.254  
up route add -net 192.168.2.0  
netmask 255.255.255.0 gw  
192.168.2.1  
down route del -net 192.168.2.0  
netmask 255.255.255.0 gw  
192.168.2.1
```

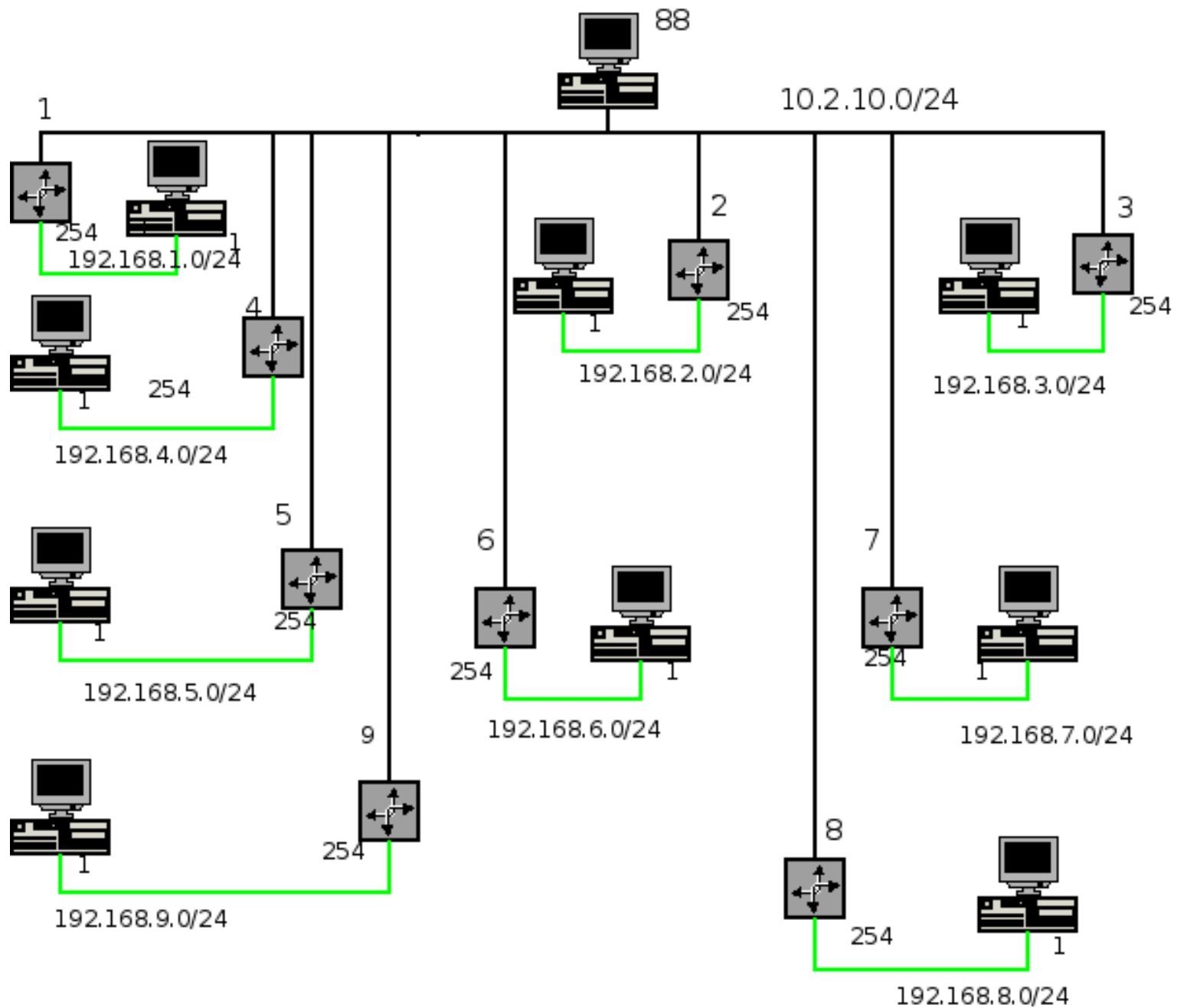
Mise en réseau volatile

- /sbin/ifconfig
- /sbin/dhclient
- /sbin/route
- /sbin/sysctl

Interfaces virtuelles

- Ajouter une adresse à une interface physique
- `/sbin/ifconfig eth0:1 ...`
- Red Hat :
`/etc/sysconfig/network-scripts/ifcfg_eth0:1`
- Debian :
`/etc/network/interfaces`

TP Routage



DHCP

Dynamic Host Configuration Protocol

DHCP

- Couche 7 !
- Permet l'auto configuration de la pile IP
- Fonctionnement client/serveur
- Extension de BOOTP
- DHCP fonctionne sur UDP

Coté client

- Recherche de serveurs DHCP
- Demande de bail
- Renouvellement du bail

Dialogue initial

Client

Serveur (s)

~~DHCP DISCOVERY
MAC em « client » MAC dest broadcast
IP em 0.0.0.0 IP dest broadcast~~ →

← ~~DHCP OFFER
MAC em « serveur » MAC dest broadcast
IP em « serveur » IP dest unicast ou broadcast~~

~~DHCP REQUEST
MAC em « client » MAC dest broadcast
IP em 0.0.0.0 IP dest broadcast~~ →

← ~~DHCP ACK
MAC em « serveur » MAC dest broadcast
IP em « serveur » IP dest unicast ou broadcast~~

Options client

- Le client peut suggérer une adresse
- Le client peut choisir entre plusieurs serveurs
- Le client peut demander des paramètres spécifiques
- Le client peut suggérer un bail

Bail

- La configuration obtenue a une durée limitée
- A la moitié de cette durée, le client cherche à renouveler le bail auprès du serveur (unicast)
- Avant la fin du bail, le client cherche à renouveler le bail en broadcast
- A l'expiration du bail, le client relance la procédure initiale

Renouvellement de bail

Client

Serveur (s)

DHCP REQUEST
MAC em « client » MAC dest « serveur »
IP em « client » IP dest « serveur »

DHCP ACK
MAC em « serveur » MAC dest « client »
IP em « serveur » IP dest « client »

Coté serveur

- Affectation statique des adresses basée sur l'adresse MAC
- Affectation dynamique dans une plage
- Combinaison des deux

Coté serveur

- Les serveurs peuvent transmettre en plus de l'adresse IP
 - La passerelle par défaut
 - Les serveurs DNS
 - Le nom d'hôte
 - Le nom de domaine
 - Les prévisions météo
 - Prochain serveur / nom de fichier

Mise en oeuvre

- TP dhcp

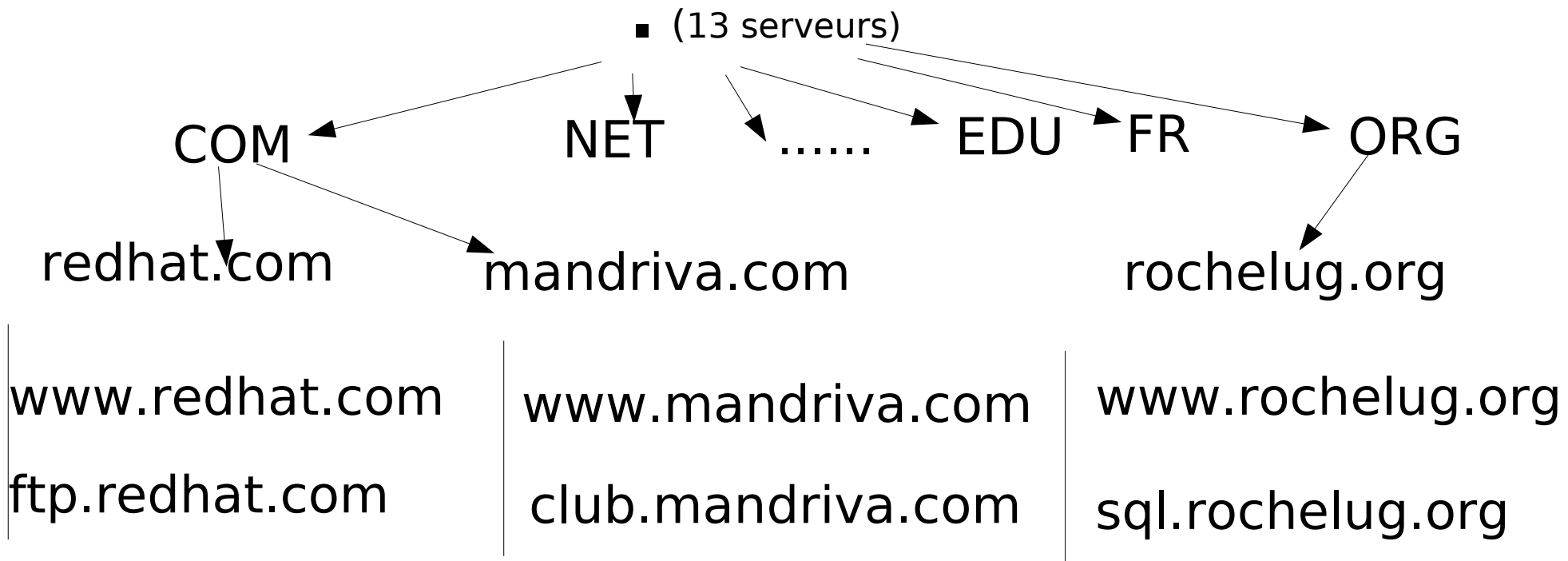
DNS

- Domain Name System

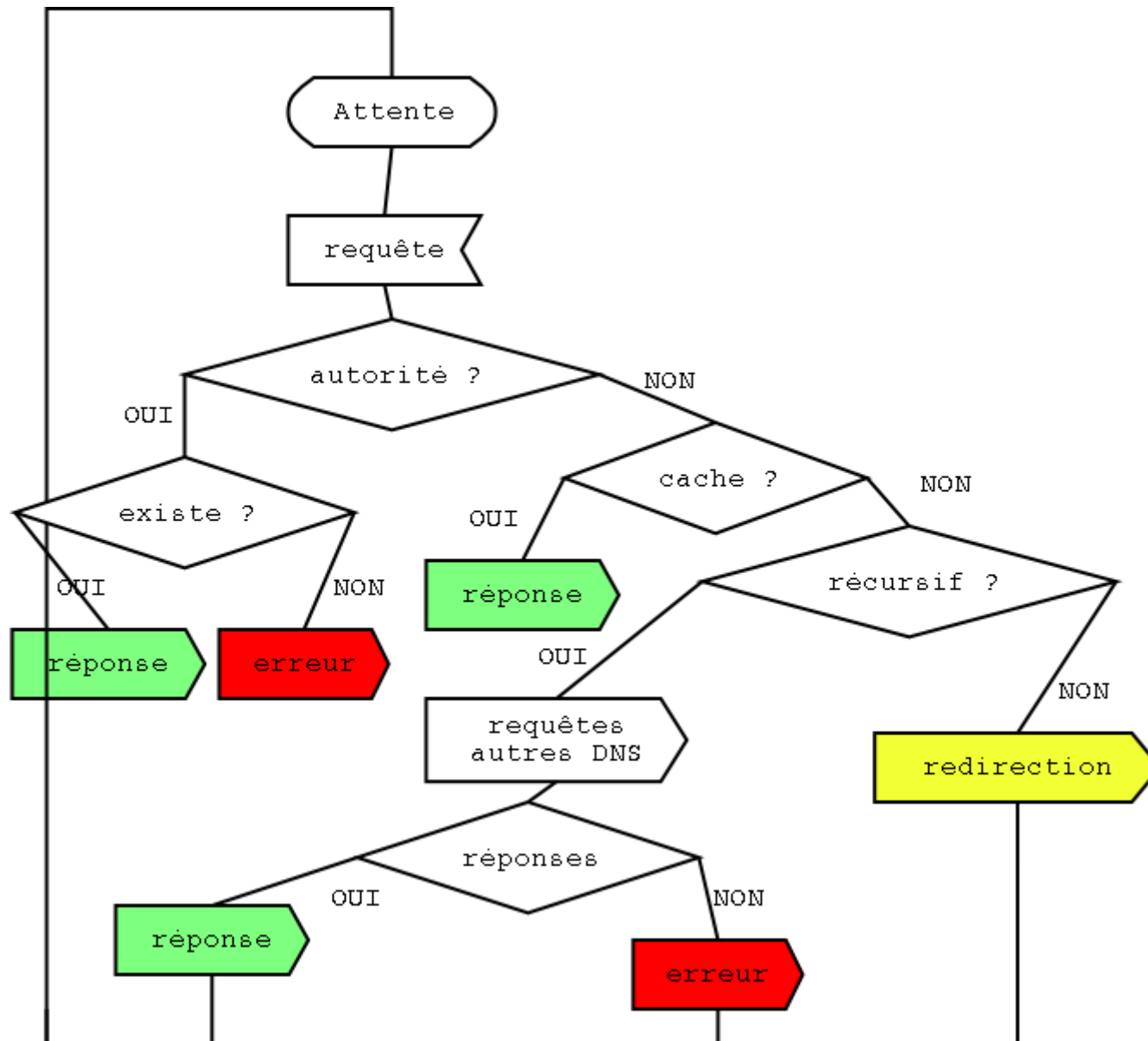
DNS

- Le système DNS est un arbre mondial
- Chaque serveur implémente une ou plusieurs feuilles
- Les serveurs publics mettent en cache les informations venant d'autres serveurs (souvent)
- Les serveurs privés doivent être conçus comme les publics

Hiérarchie DNS



Interrogation DNS



4 configurations

- Maître
- Esclave
 - Maître et esclaves doivent être sur des réseaux distants !
- Cache-seulement
- retransmission

Fichiers

- /etc
 - named.conf : configuration du serveur
- /var
 - named
 - named.ca
 - localhost.zone
 - localhost_inverse.zone
 - mon_domaine.zone
 - mon_domaine_inverse.zone

named.conf

```
options {
  directory "/var/named";
}
zone "." IN {
  type hint;
  file "named.ca";
};
zone "mon_domaine" IN {
  type master;
  file "mon_domaine.zone";
  allow-update { none; };
};
zone "0.168.192.in-addr.arpa" IN {
  type master;
  file "mon_domaine_inverse.zone";
  allow-update { none; };
};
zone "localhost" IN {
  type master;
  file "localhost.zone";
  allow-update { none; };
};
zone "0.0.127.in-addr.arpa" IN {
  type master;
  file "localhost_inverse.zone";
  allow-update { none; };
};
```

fichiers de zone

\$TTL <time-to-live>

```
@ IN SOA <primary-name-server> <hostmaster-email> (  
    <serial-number>  
    <time-to-refresh>  
    <time-to-retry>  
    <time-to-expire>  
    <minimum-TTL> )
```

} esclaves

Fichiers de zone (suite)

IN NS dns1.domain.com.

IN NS dns2.domain.com.

IN MX 10 mail.domain.com.

IN MX 20 mail2.domain.com.

IN A 10.0.1.5

server1 IN A 10.0.1.5

server2 IN A 10.0.1.7

dns1 IN A 10.0.1.2

dns2 IN A 10.0.1.3

ftp IN CNAME server1

Fichier de zone

\$TTL 86400

@ IN SOA ns.mon_domaine toto.mon_domaine.com. (

2006061042 ; serial

3H ; refresh

15M ; retry

1W ; expiry

1D) ; minimum

IN NS ns.mon_domaine.com.

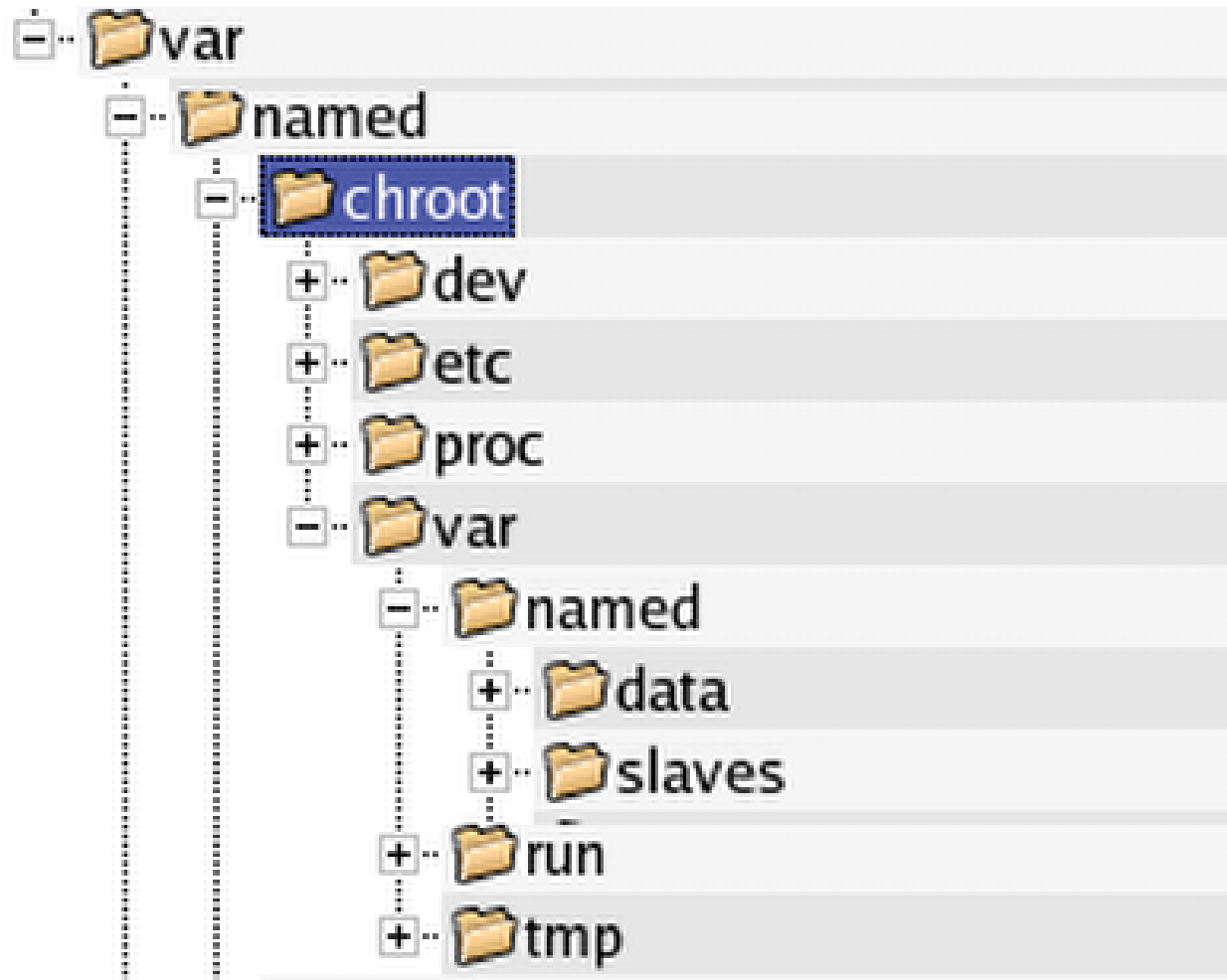
ns IN A 192.168.0.1

www IN A 192.168.0.2

Chroot

- Service très attaqué => souvent «chrooté»
- Une arborescence minimale est constituée
- On change la racine de l'arborescence (pour notre démon uniquement)

Chroot



Exercice

- TP DNS

Authentication

- Locale
- Centralisée

Authentication

- Fichiers :
 - /etc/passwd
 - /etc/group
 - /etc/shadow
- NIS
 - obsolète
- SMB
 - Si PDC sur le réseau
- LDAP
- ...

PAM

- Plugable authentication module
- Implémente une couche d'abstraction entre les applications et les systèmes d'authentification
- La configuration est dans `/etc/pam.d/`
 - le login utilise `login` et `system-auth`
- Utiliser les outils de votre distribution
 - `authconfig` (fedora)
 - `drakauth` (mandriva)
 - `main gauche ET main droite` (debian)

Fichiers

- /etc/nsswitch
- /etc/pam_ldap.conf
- /etc/ldap.conf
- /etc/openldap/ldap.conf
- /etc/pam.d/system-auth
- /etc/libnss-ldap.conf
- Ces fichiers varient suivant la distribution...

LDAP

- Light-weight Directory Access Protocol
- Implémente un annuaire (mondial) compatible X400
- Compact et protocole réseau léger
- Authentification des utilisateurs
- Gestions des droits pour la consultation ou la modification
- Base de données spécialisée

LDAP

- Annuaire :
 - Est plus souvent lu qu'écrit
 - Les données sont présentées de manière hiérarchique
 - Les mécanismes de recherche sont performants
 - Les résultats sont organisés
- Annuaire réparti

Structure Objet

- Généricité de la structure
- Classes structurantes
 - définissent la structure
- Classes auxiliaires
 - définissent les données
- Les objets sont accédés par :
 - Object identifier OID => pour les machines
 - Nom unique DN=> pour les cyborgs

Attributs

- OID
- Nom
- Syntaxe et règles de comparaison
- Mono ou multivalués
- Indicateur d'usage
- Format

Attributs courants

- uid : identifiant présumé unique
- o : organization
- ou : organization unit
- cn : common name
- givenname
- sn : surname
- mail
- photo ...

Schémas LDAP

- Les classes et les attributs sont définis dans des schémas normalisés.
- En théorie il est possible de les étendre
- Respecter la hiérarchie
- Respecter la syntaxe
- En pratique on trouve tout ce qu'on veut dans les schémas existants

Schémas

attributetype (2.16.840.1.113730.3.1.241

NAME 'displayName'

DESC 'RFC2798: preferred name to be used when displaying entries'

EQUALITY caseIgnoreMatch

SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15

SINGLE-VALUE)

Schéma (exemples)

attributetype (2.5.4.4 NAME ('sn' 'surname')
DESC 'RFC2256: last (family) name(s) for which the
entity is known by'
SUP name)

attributetype (2.5.4.35 NAME 'userPassword'
DESC 'RFC2256/2307: password of user'
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{128})

Schéma (exemples)

```
objectclass ( 1.3.6.1.4.1.1466.344 NAME 'dcObject'  
  DESC 'RFC2247: domain component object'  
  SUP top AUXILIARY MUST dc )
```

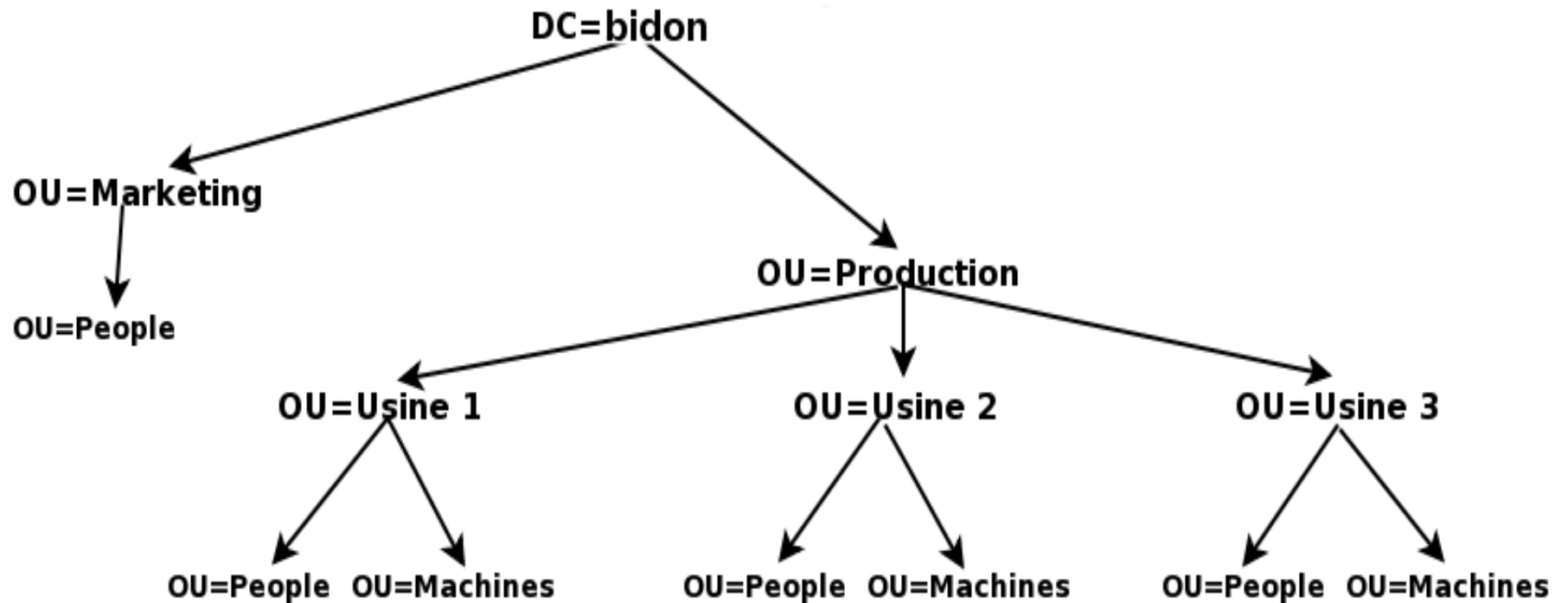
```
objectclass ( 2.5.6.6 NAME 'person'  
  DESC 'RFC2256: a person'  
  SUP top STRUCTURAL  
  MUST ( sn $ cn )  
  MAY ( userPassword $ telephoneNumber $ seeAlso $  
  description ) )
```

Organisation LDAP

- Chaque annuaire est supposé être une partie de l'Annuaire mondial
- Chaque feuille est identifiée par un « dn » distinguished name UNIQUE
- Pour éviter une recherche mondiale, on identifie l'annuaire par un « BaseDN »
- Le Base DN est souvent composé avec le nom de domaine (DNS) de l'organisation, lequel est unique
- Énoncé par « dc=domaine,dc=tld »

Exemple

DC=FR



DN=uid=rbidochon,OU=people,ou=usine 1,ou=production,dc=bidon, dc=fr
CN=Bidochon Robert
SN=Bidochon
givenname=Robert
mail=robert.bidochon@bidon.fr
...

Exemple

dc=univ-lr,dc=fr

ou=people

ou=groups

Robert

Raymonde

Paul

Lettres

Droit

Sciences

Population de l'annuaire

- Graphique
 - gq
 - phpldapadmin
 - Divers clients java
- Texte
 - ldap-tools
 - Avec utilisation de fichiers au format LDIF

LDIF (init)

dn: dc=univ-lr,dc=fr
dc: univ-lr
dc: fr
o: univ-lr.fr
objectClass: top
objectClass: dcObject
objectClass: organization

dn: ou=people,dc=univ-lr,dc=fr
dc: univ-lr
ou: people
objectClass: top
objectClass: dcObject
objectClass: organizationalUnit

dn: ou=groups,dc=univ-lr,dc=fr
dc: univ-lr
ou: groups
objectClass: top
objectClass: dcObject
objectClass: organizationalUnit

LDIF (groupe)

dn: cn=sciences,ou=groups,dc=univ-lr,dc=fr

objectClass: top

objectClass: dcObject

objectClass: posixGroup

dc: univ-lr

cn: sciences

gidNumber:1001

LDIF (user)

- dn: uid=toto,ou=people,dc=univ-lr,dc=fr
- loginShell: /bin/bash
- objectClass: top
- objectClass: dcObject
- objectClass: person
- objectClass: posixAccount
- objectClass: shadowAccount
- dc: univ-lr
- cn: Bidochon
- uid: rbidochon
- uidNumber: 1001
- homeDirectory: /home/rbidochon
- sn: Robert Bidochon
- gidNumber: 1001

Commandes

- `ldapadd` : ajoute une entrée dans l'annuaire
- `ldapdelete` : ?? une entrée dans l'annuaire
- `ldapmodrdn` : renomme une entrée de l'annuaire
- `ldapsearch` : cherche et affiche une entrée de l'annuaire
- `ldapmodify` : modifie une entrée de l'annuaire
- `ldappasswd` : change le mot de passe d'une entrée de l'annuaire
- *`ldapadd -x -v -D cn=Manager,dc=my-domain,dc=com -W < init.ldif`*
 - *x* authentication simple
 - *v* verbeux
 - *D* bind dn
 - *W* demande le mot de passe

Exercice

- TP LDAP 1

Serveur openLDAP

- Porte le joli nom de slapd
- Configuration dans `/etc/openldap/slapd.conf`
- Les schémas sont dans `/etc/openldap/schema/` ou dans `/usr/share/openldap/schema` ou ailleurs

Configuration

- 1^{ère} partie : général
 - inclure les schémas qui vont bien
 - emplacement des certificats
 - Contrôle d'accès général
 - ...

Configuration

- 2^{ème} partie : l'annuaire
 - type de base de données
 - basedn appelé aussi suffixe
 - dn et mot de passe de l'administrateur
 - contrôle d'accès
 - index
 - réplicats

Exercice

- TP LDAP 2

Samba-Ldap

- Samba contrôleur de domaine
- Mots de passe (passdb backend)
 - smbpasswd
 - tdbsam
 - ldapsam

Configuration

- LDAP => Schéma samba
- SAMBA
 - passdb backend = ldapsam:ldap://<adresse>
 - suffixes général, users, machines et groups
 - commandes d'ajout suppression
- TP smbLdap