

# ADMINISTRATION DES SERVICES RÉSEAUX

<http://www.academiepro.com/enseignants-104-Chaabani.Nizar.html>

# DHCP

Dynamic Host Configuration Protocol  
DHCP [RFC 2131 - 1997 ]

# BUT

3

- Permet à un ordinateur qui se connecte sur un réseau local d'obtenir et de configurer dynamiquement et automatiquement :
  - ▣ Son adresse IP
  - ▣ masque de son sous-réseau
  - ▣ passerelle par défaut
  - ▣ adresse IP du serveur DNS
  - ▣ nom de son domaine

# Pourquoi utiliser le protocole DHCP ?

4

Le protocole DHCP simplifie et réduit le travail administratif grâce à l'usage de la configuration automatique du protocole TCP/IP

## Configuration manuelle du protocole TCP/IP

- Les adresses IP sont entrées manuellement sur chaque ordinateur client
- Risque d'entrer une adresse IP incorrecte ou non valide
- Une configuration incorrecte peut entraîner des problèmes de réseau
- Surcharge administrative sur les réseaux dont les ordinateurs sont souvent déplacés

Administration Services RX

## Configuration automatique du protocole TCP/IP

- Les adresses IP sont automatiquement fournies aux ordinateurs clients
- Les clients utilisent toujours des informations de configuration correctes
- La configuration du client est automatiquement mise à jour pour refléter les modifications dans la structure du réseau

Nizar chaabani

# Fonctionnement

5

- Lorsque vous connectez un ordinateur sur le réseau il n'a aucune connaissance de son adresse IP
- Par contre il connaît:
  - ▣ son adresse Mac
  - ▣ L'adresse de broadcast

# Fonctionnement : étape 1

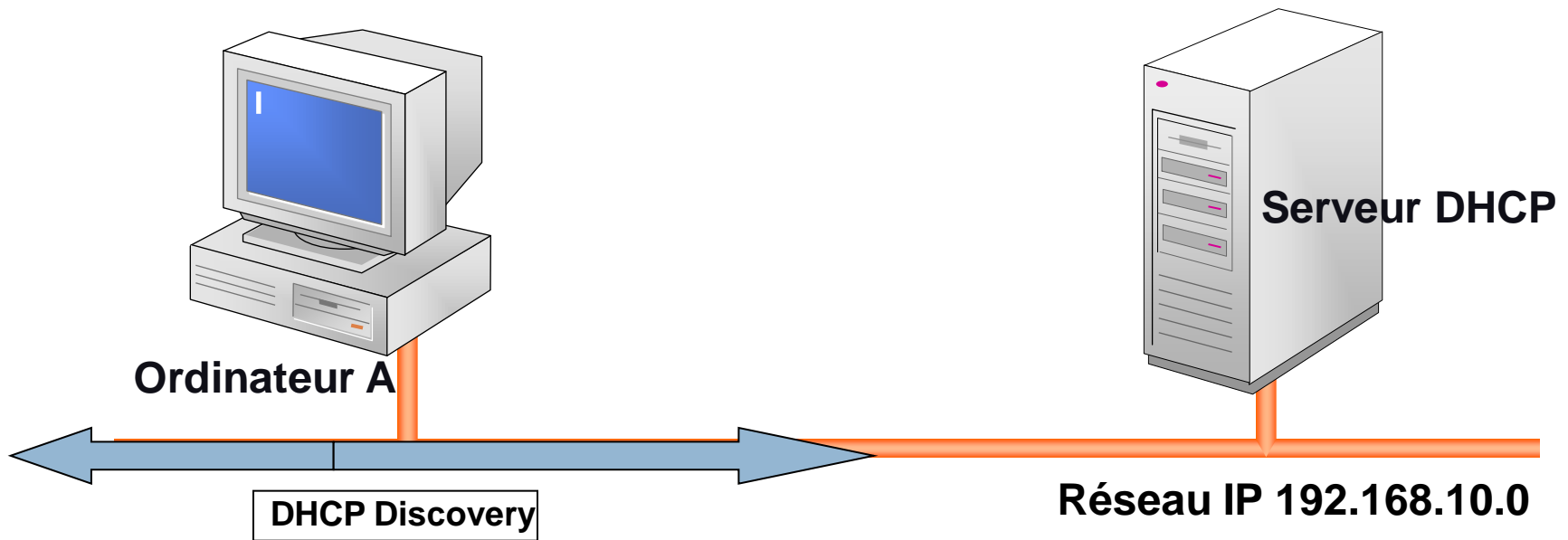
6



□ Le client A démarre, il n'a pas d'adresse IP

# Fonctionnement : étape 2

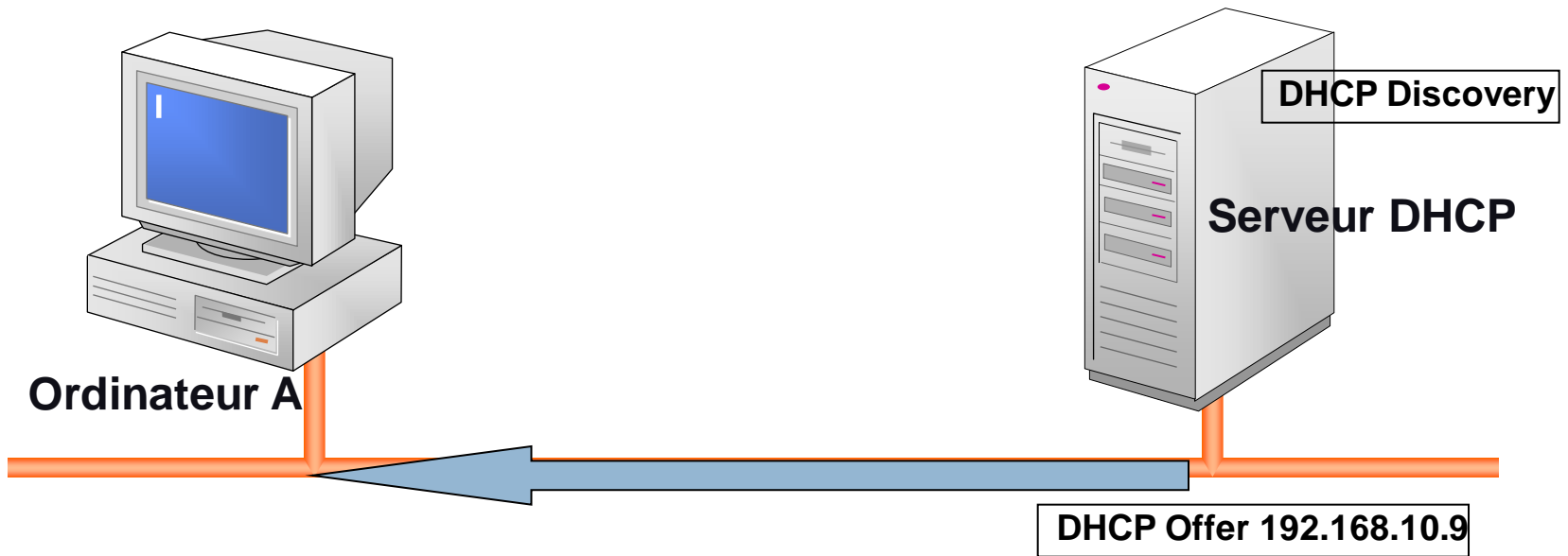
7



- L'ordinateur A émet un paquet de découverte d'un serveur DHCP

# Fonctionnement : étape 3

8

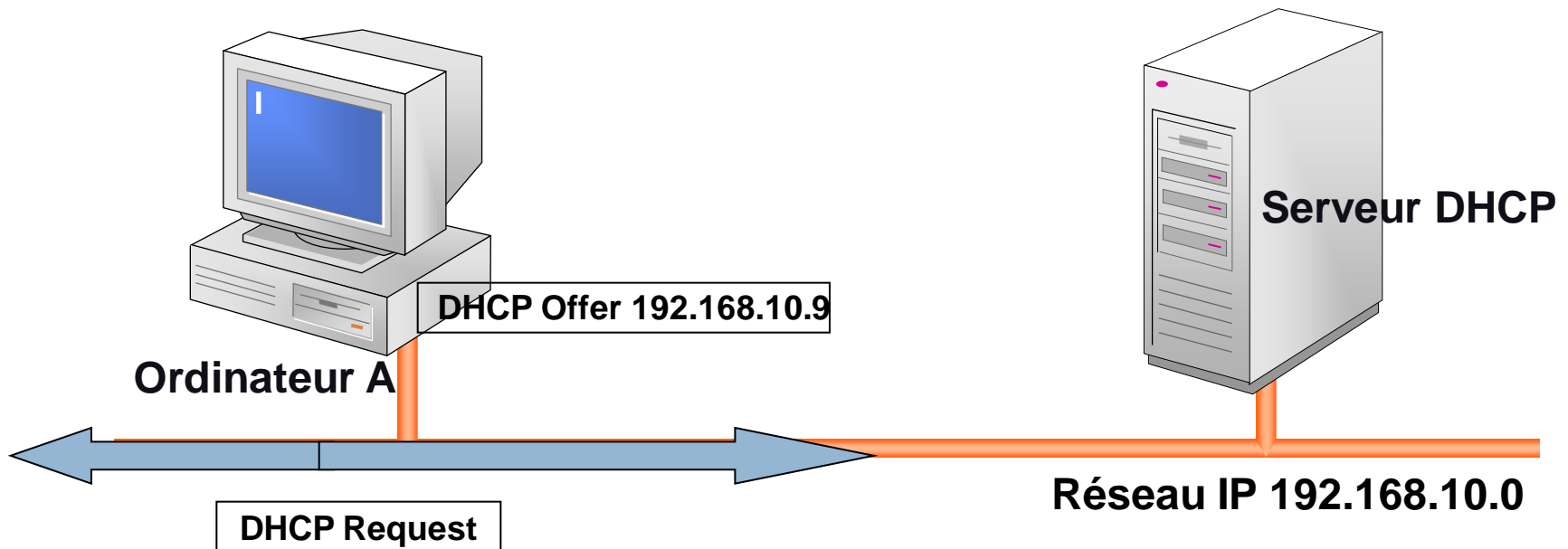


- Le serveur DHCP propose une configuration IP au client



# Fonctionnement : étape 4

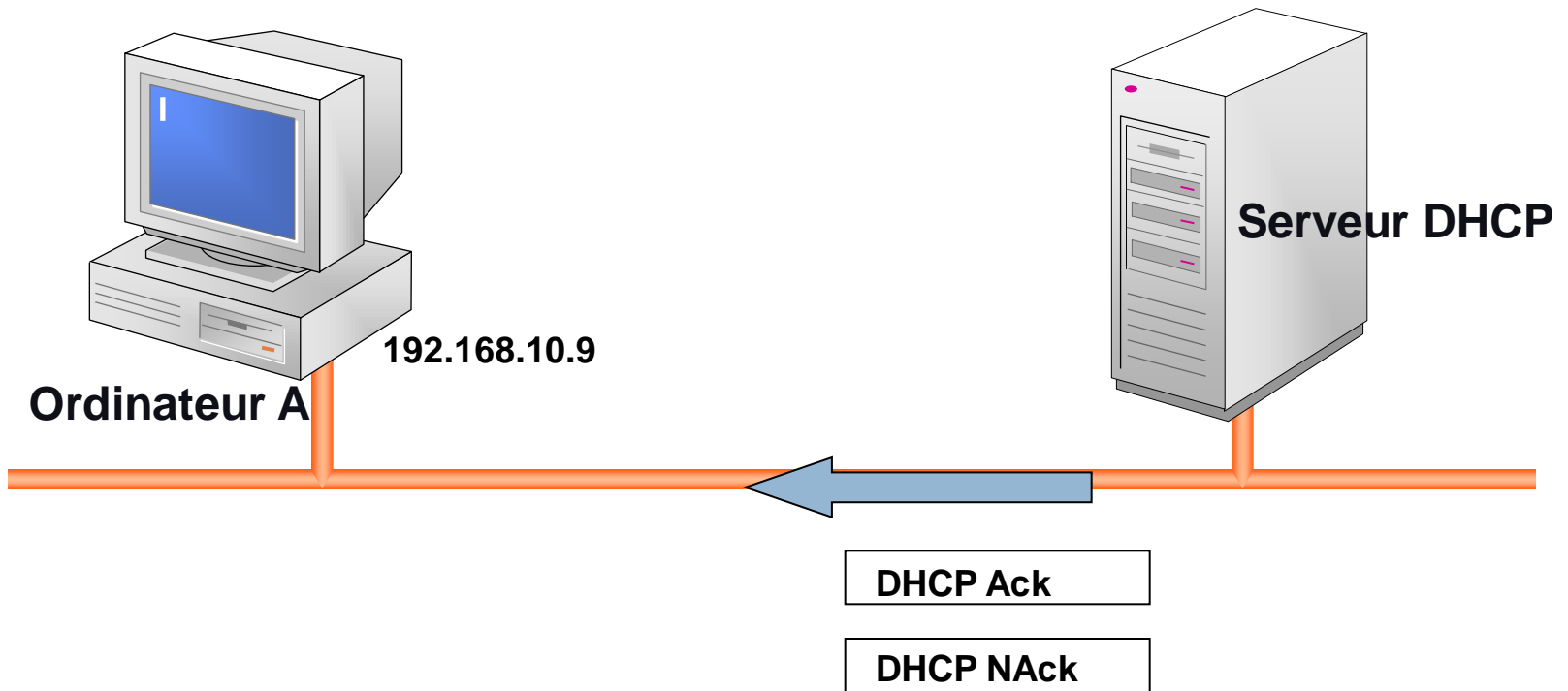
9



- L'ordinateur annonce (par diffusion)  
accepter ou non la configuration IP

# Fonctionnement : étape 5

10

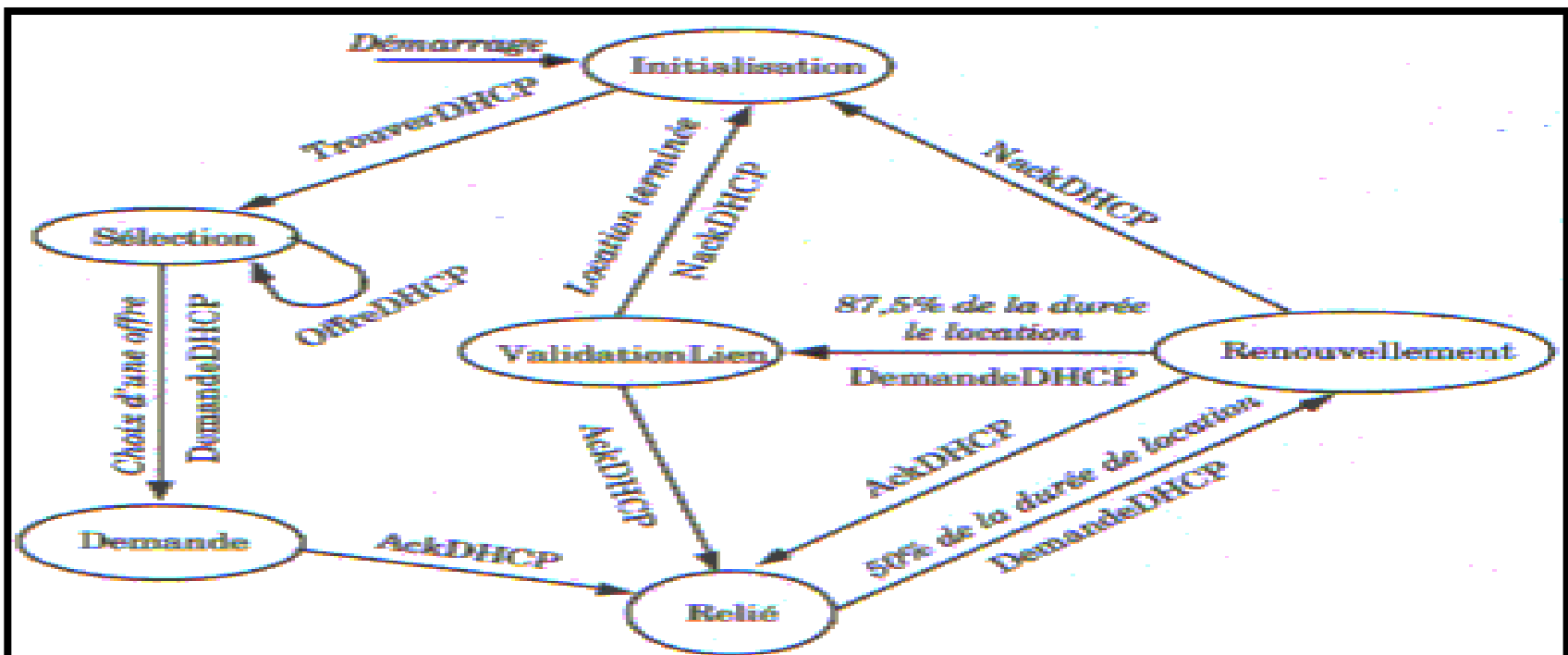


□ Le serveur acquitte ou non la réponse du client

# Fonctionnement du DHCP

11

## □ Le diagramme d'états



**Figure 2** — Les six états principaux par lesquels passe un client DHCP ainsi que les événements ou les messages qui provoquent les transitions.

# Gestion des adresses IP

- Une adresse obtenue par DHCP est valide :
  - pour une période donnée (bail, *lease*)
- La durée du bail est paramétrable :
  - en général 48 heures (minimum : 1h)
  - possibilité de prolonger le bail

# Gestion des adresses IP

13

- Possibilité de réserver des adresses IP à certaines adresses MAC
- Le serveur DHCP peut fournir dans son offre de nombreux paramètres IP :
  - @ passerelle
  - @ serveurs : DNS, WINS
  - ...

# Mise en œuvre de DHCP

14

- Côté client :
  - Sélectionner l'attribution automatique d'adresse IP (on parle de « client DHCP »)
- Côté serveur :
  - Installer le service DHCP
  - Autoriser le serveur DHCP (le rendre actif)
  - Définir la ou les plages d'adresses (étendues), les exclusions d'adresses et la durée du bail ...

# Demande de bail/adresse IP

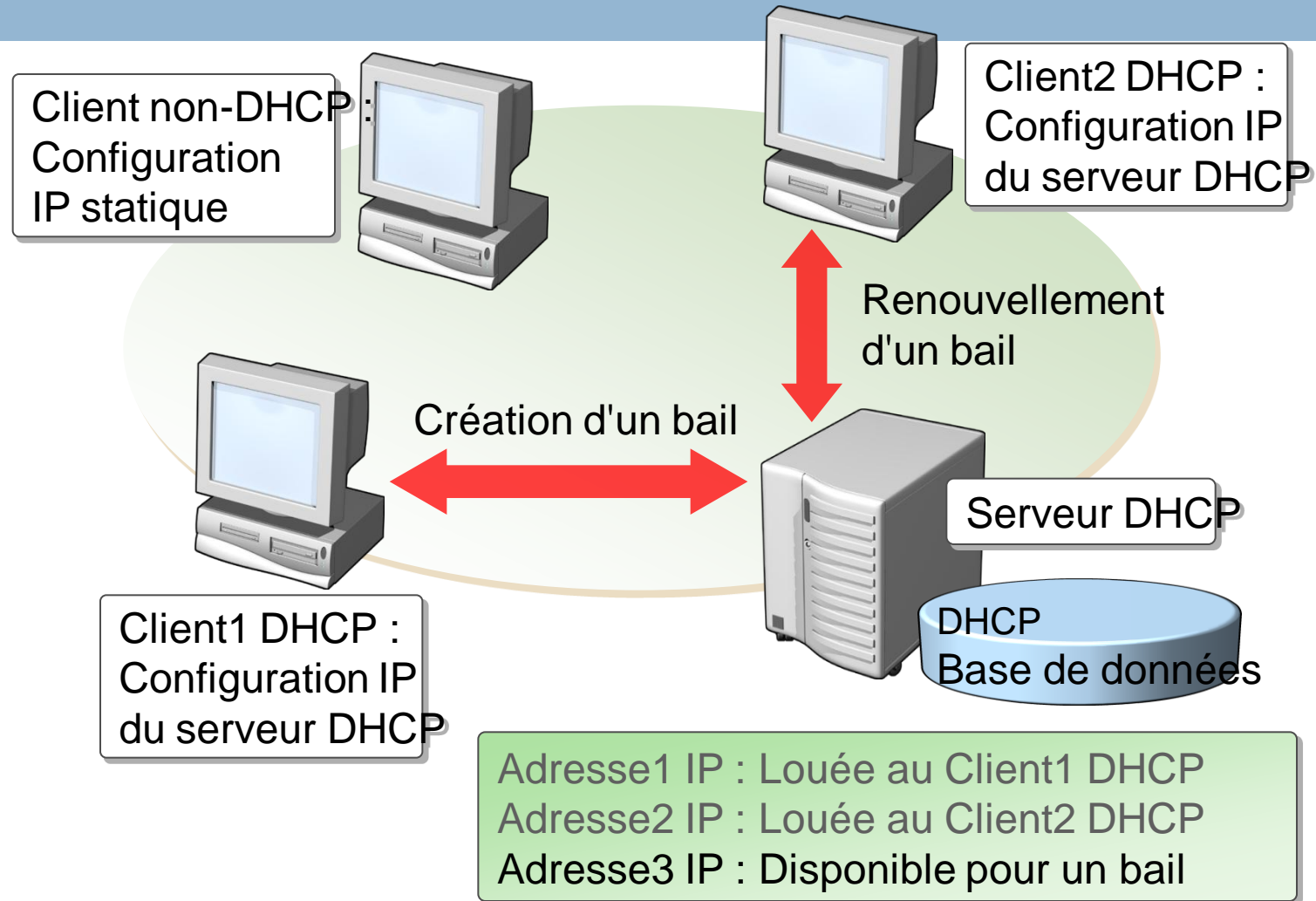
15

- Le poste client vient de se connecter, il n'a pas d'adresse IP
- En DHCP une adresse IP n'est fournie que pour un temps donné : Le bail. C'est pourquoi on parle de demande de bail plutôt que d'adresse IP

Un bail a une durée : **lease-time**

# Comment le protocole DHCP alloue des adresses IP

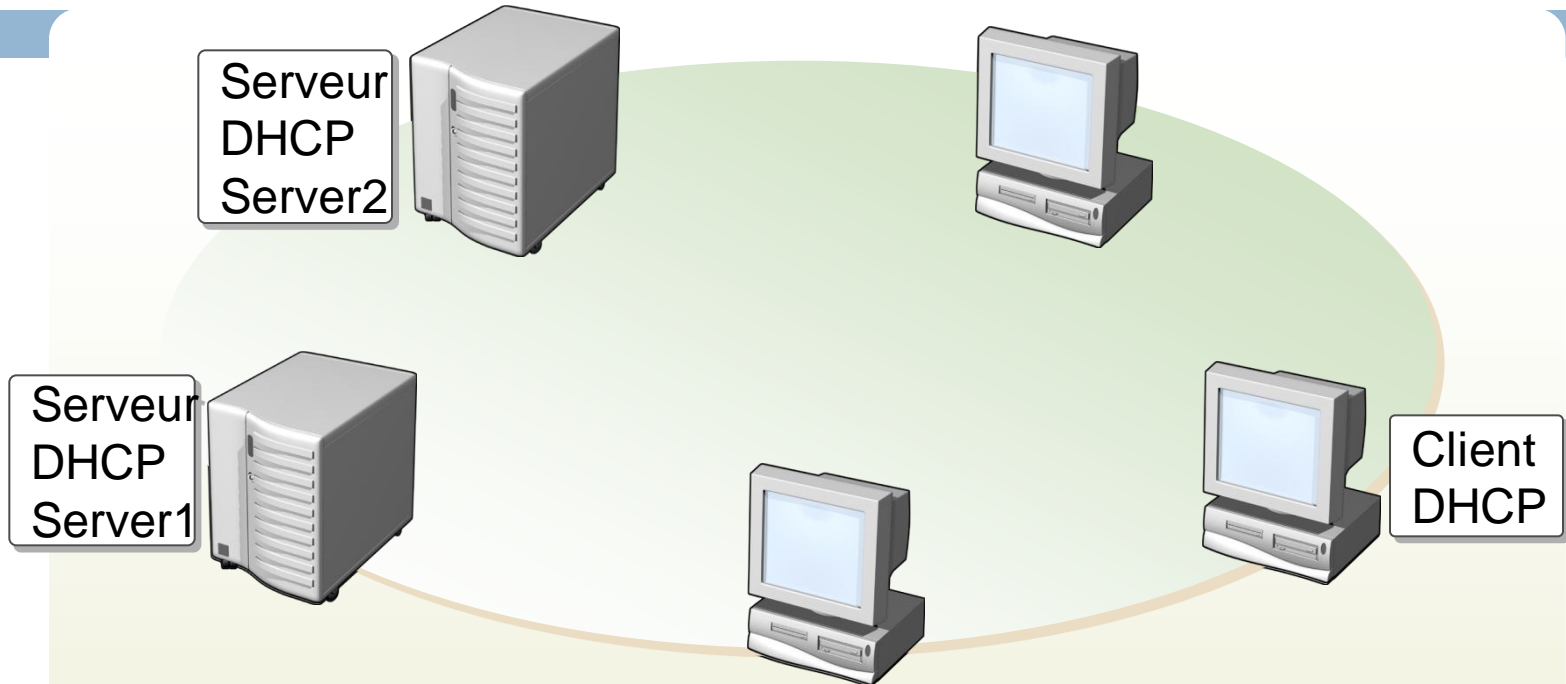
16





# Comment fonctionne le processus de création d'un bail DHCP

17

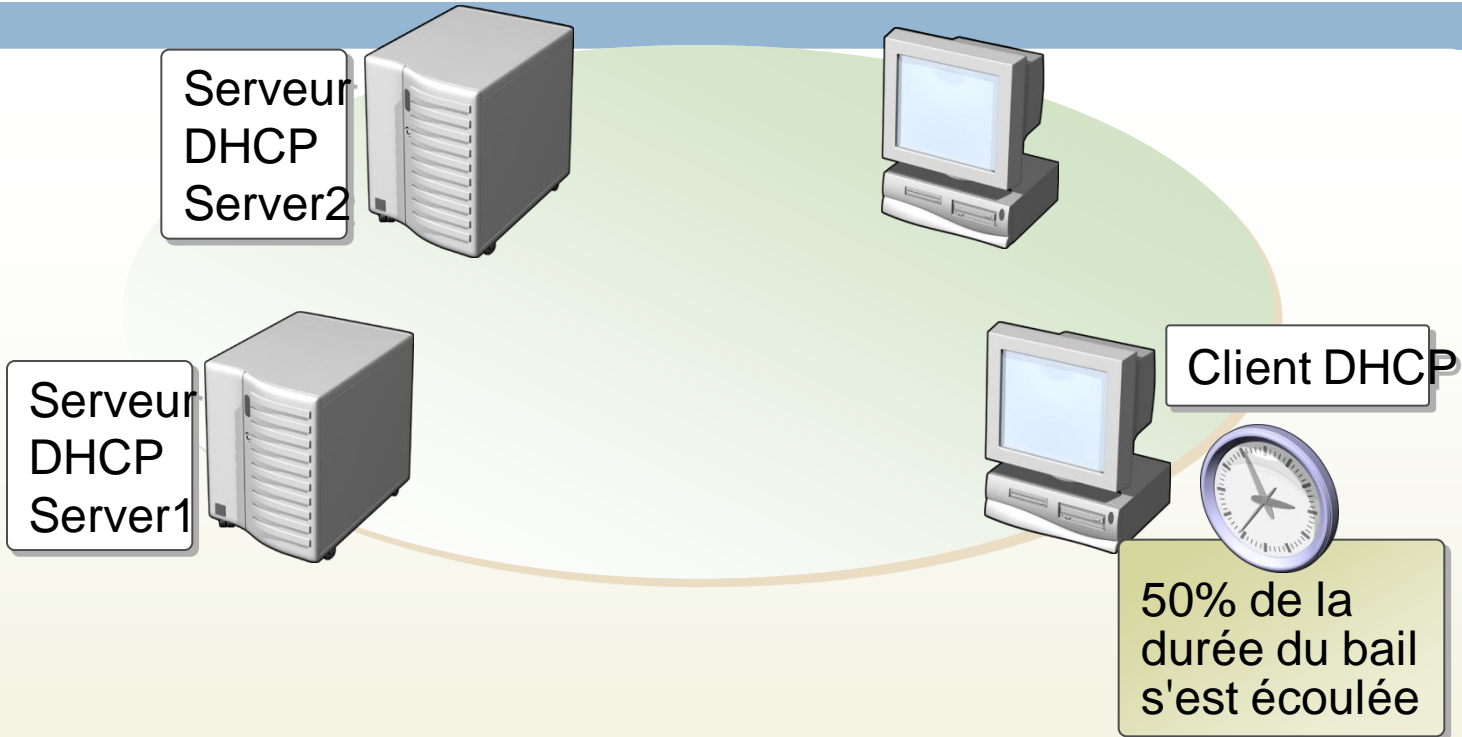


- 1 Le client DHCP diffuse un paquet DHCPDISCOVER
- 2 Le client DHCP diffuse un paquet DHCPOFFER
- 3 Le client DHCP diffuse un paquet DHCPREQUEST
- 4 Le serveur DHCP Server1 diffuse un paquet DHCPACK



# Comment fonctionne le processus de renouvellement d'un bail DHCP

18

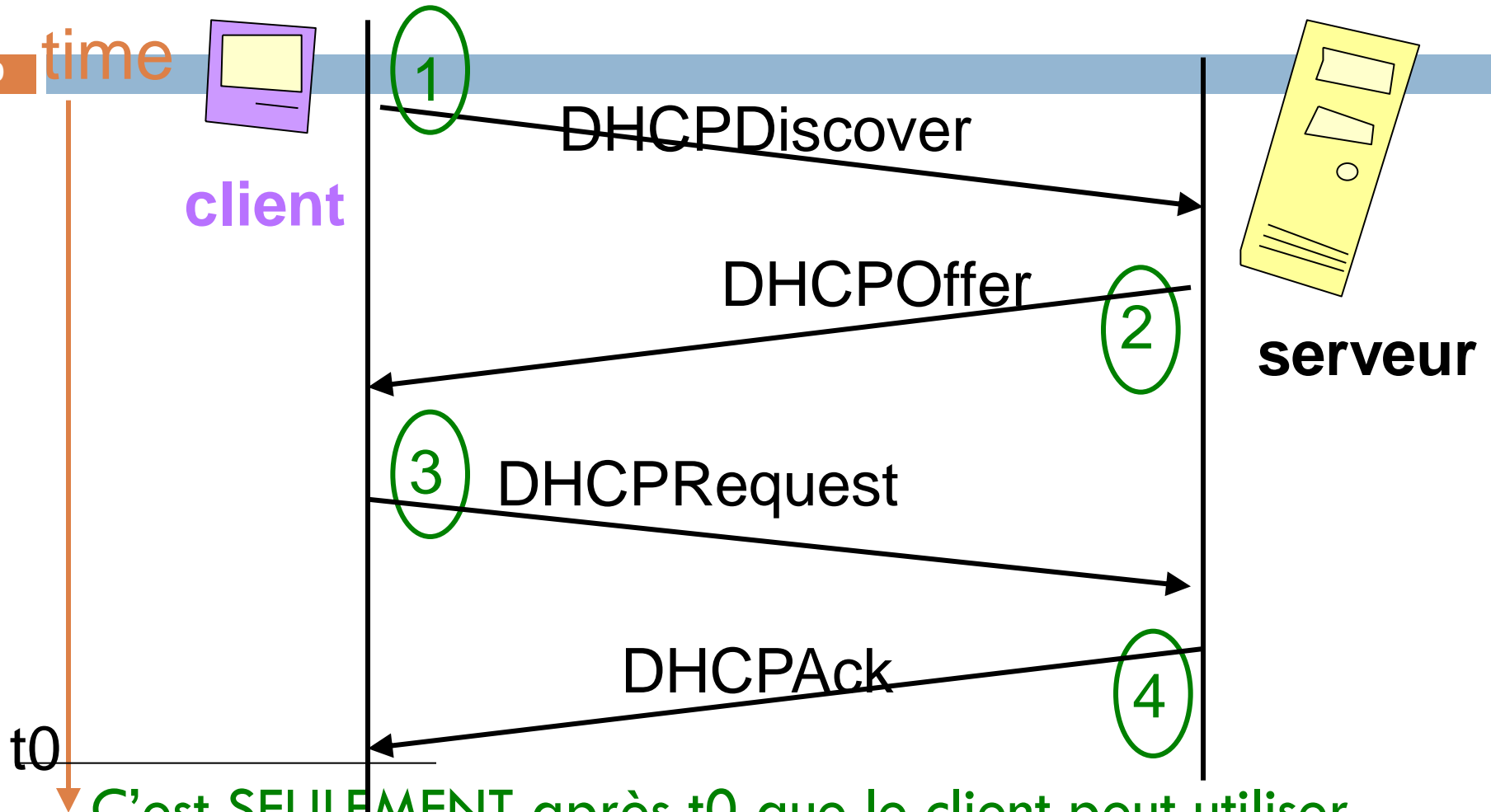


**1** Le client DHCP envoie un paquet DHCPREQUEST

**2** Le serveur DHCP Server1 envoie un paquet DHCPACK

# Demande de bail - UN serveur DHCP

19



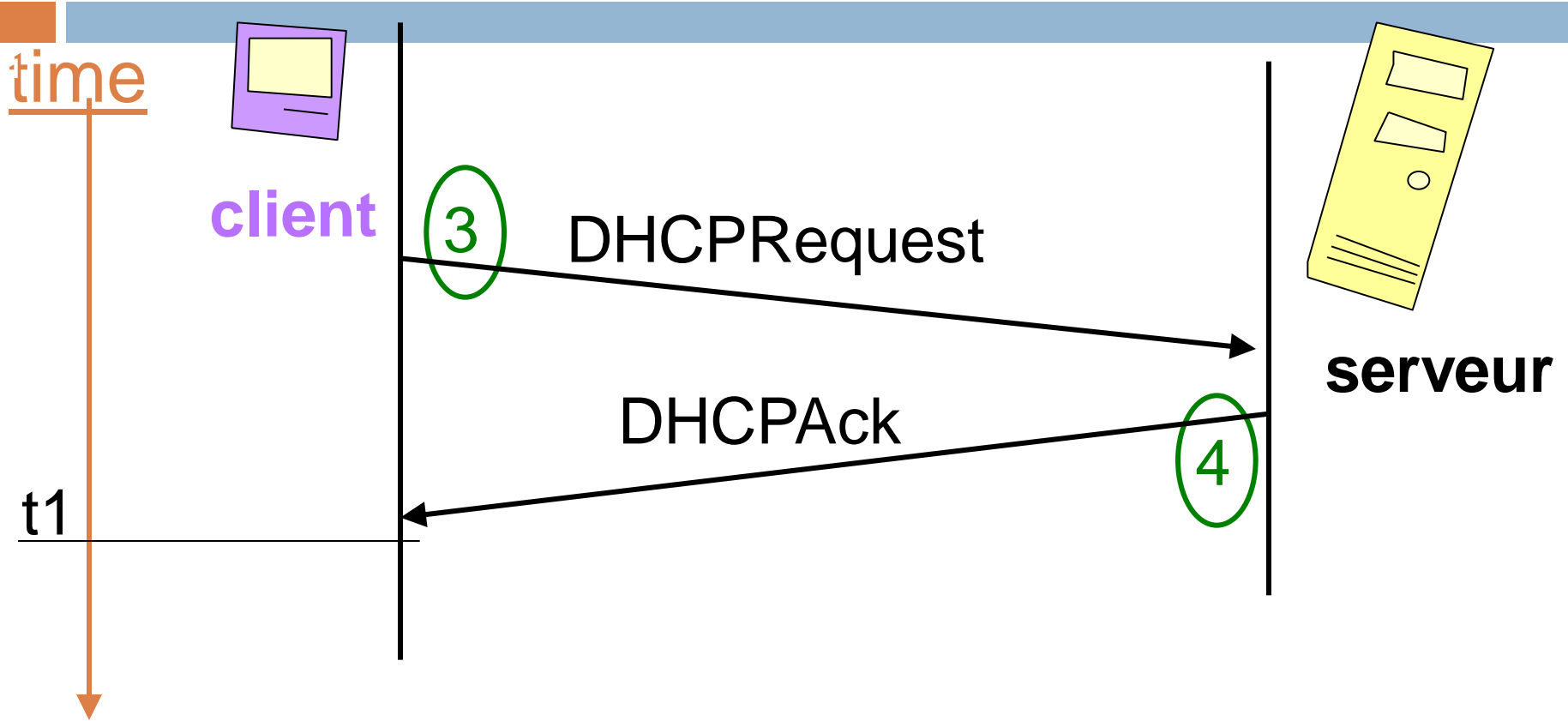
C'est SEULEMENT après  $t_0$  que le client peut utiliser l'adresse IP communiquée par le serveur jusqu'à  $t_0 + \text{lease-time}$

# Trames DHCP

20

- **DHCPDISCOVER** : Permet de trouver un serveur DHCP. La trame est une trame de « broadcast », elle est envoyée à l'adresse 255.255.255.255. Le client n'ayant pas d'adresse prend l'adresse 0.0.0.0
- **DHCPOFFER** : contient une proposition de bail, l'adresse IP du serveur et l'adresse Mac du client.
- **DHCPREQUEST** : indique à tous les serveurs quel bail il a accepté et/ou demande de renouvellement de bail
- **DHCPACK** : le serveur confirme le bail.

# Demande de renouvellement de bail



Le client peut utiliser l'adresse IP communiquée par le serveur jusqu'à  $t1 + \text{lease-time}$

# Les paquets IP échangés Lors d'un renouvellement de bail

22

Source	Destination	Protocol Info
192.168.0.9	192.168.0.253	DHCPRequest
192.168.0.253	192.168.0.9	DHCPAck

# Message DHCP

# Message DHCP

24

## Envoyé par le Client

- **DHCPDISCOVER** demande de localisation des serveurs DHCP
- **DHCPREQUEST** demande de bail
- **DHCPDECLINE** refus d'adresse IP, elle est déjà utilisée
- **DHCPRELEASE** libération son bail
- **DHCPINFORM** demande de paramètres locaux (autre qu'une adresse IP)



# Message DHCP

25

## Envoyé par le Serveur

- **DHCPOFFER** réponse à un DHCPDISCOVER
- **DHCPACK** contient des paramètres et l'adresse IP du client
- **DHCPNAK** refus de bail

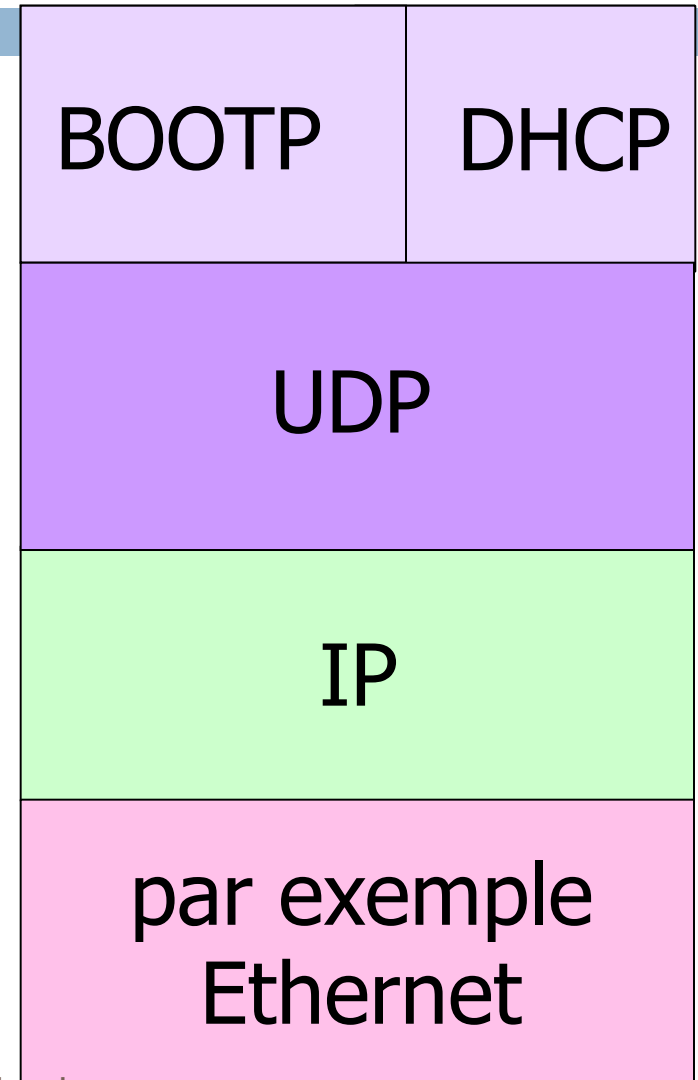
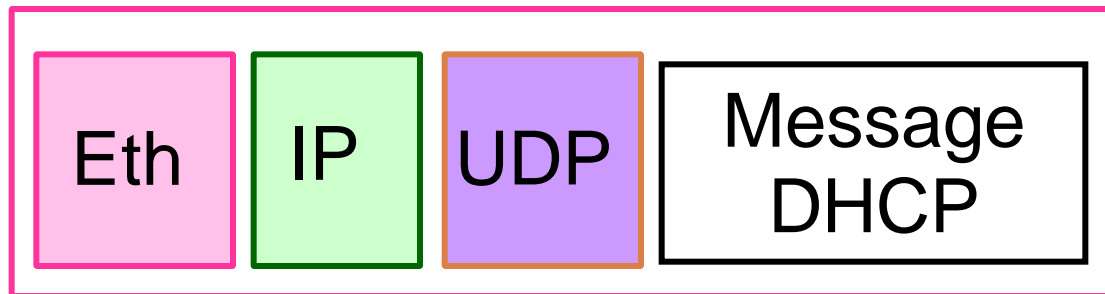
# Problème de l'œuf et de la poule

Encapsulation d'un message DHCP

# Encapsulation d'un message DHCP

27

**Trame contenant un message « DHCP »**



# Trame contenant un message DHCP

28

Ethernet

Adresse physique de l'émetteur  
Adresse physique du destinataire de la trame

IP

Adresse IP source  
Adresse IP destinataire du paquet IP

UDP

Port source  
Port destination du datagramme

Message DHCP

# Le Problème de l'oeuf et la poule

Niveau  
physique

29

A moment de la demande de bail,

- Est-ce que le client connaît son adresse physique ?
- Est-ce que le client connaît l'adresse physique du serveur DHCP ?



# Le Problème de l'oeuf et la poule

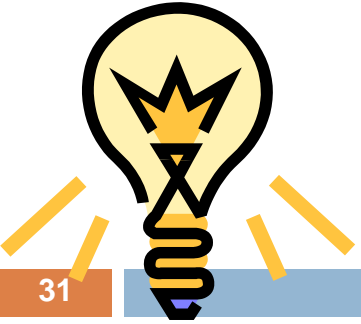
Niveau  
réseau

30

A moment de la demande de bail,

- Est-ce que le client connaît l'adresse IP du serveur DHCP ?
- Est-ce que le client connaît son adresse IP ?
- Est-ce que le serveur DHCP connaît l'adresse IP du client?

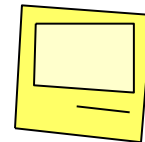
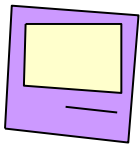




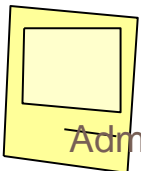
# DIFFUSION niveau physique

- Diffusion (broadcast) distribution de la requête DHCP à tous les postes connectés

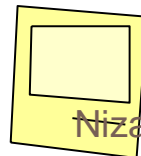
Client  
DHCP



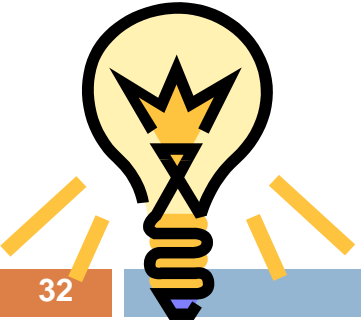
Adresse de  
diffusion:  
ff:ff:ff:ff:ff:ff



Administration Services RX



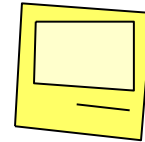
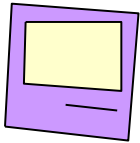
Nizar chaabani



# DIFFUSION niveau réseau

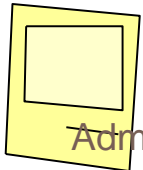
- Diffusion (broadcast) distribution de la requête DHCP à tous les postes connectés

Client  
DHCP

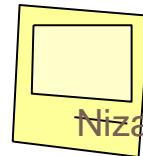


Utilisation de  
l'adresse IP de  
diffusion générique

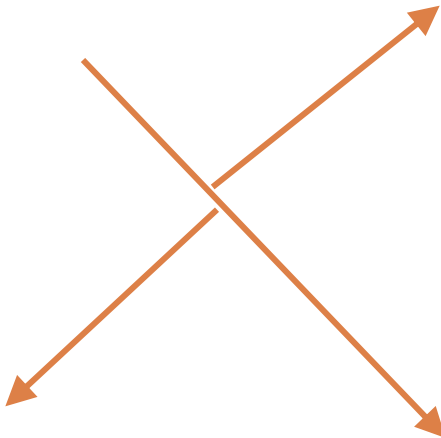
255.255.255.255



Administration Services RX



Nizar chaabani

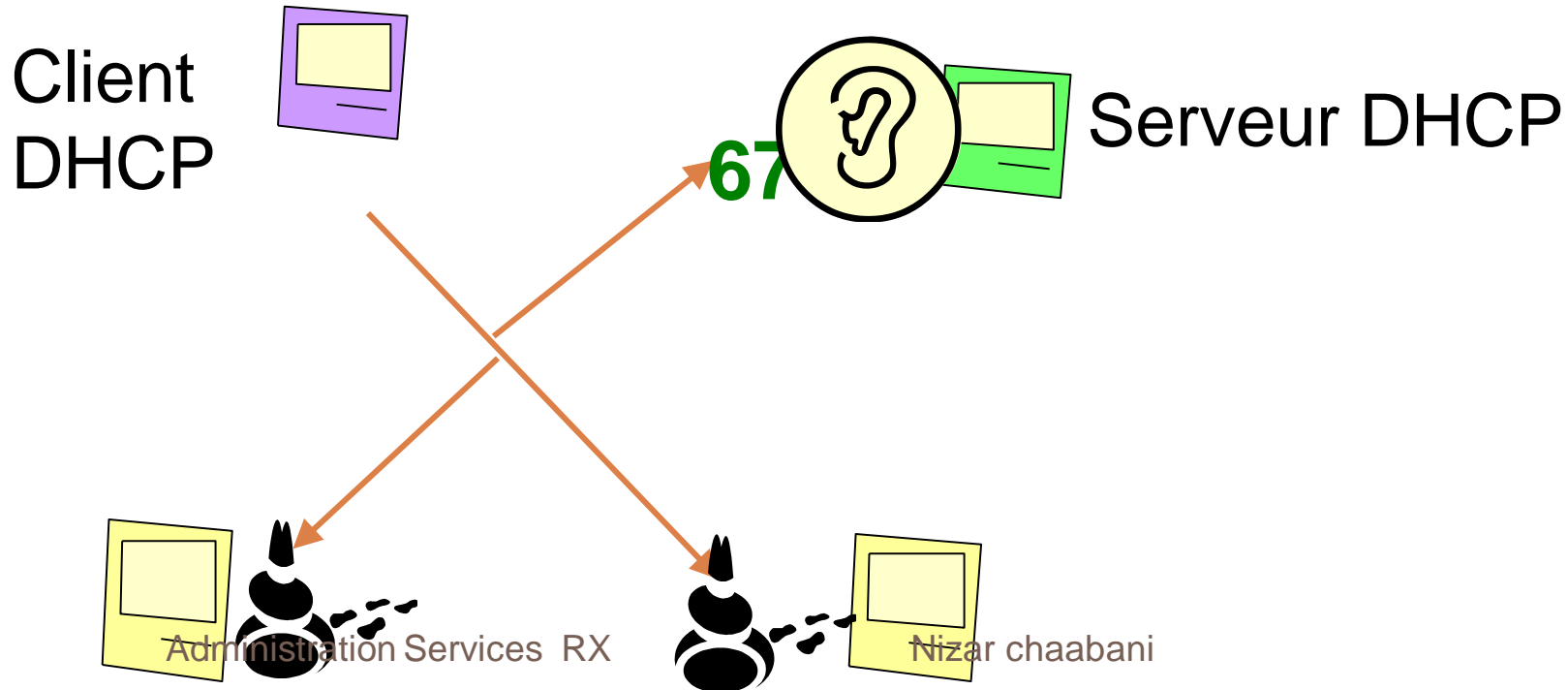




# Niveau Transport - requêtes

33

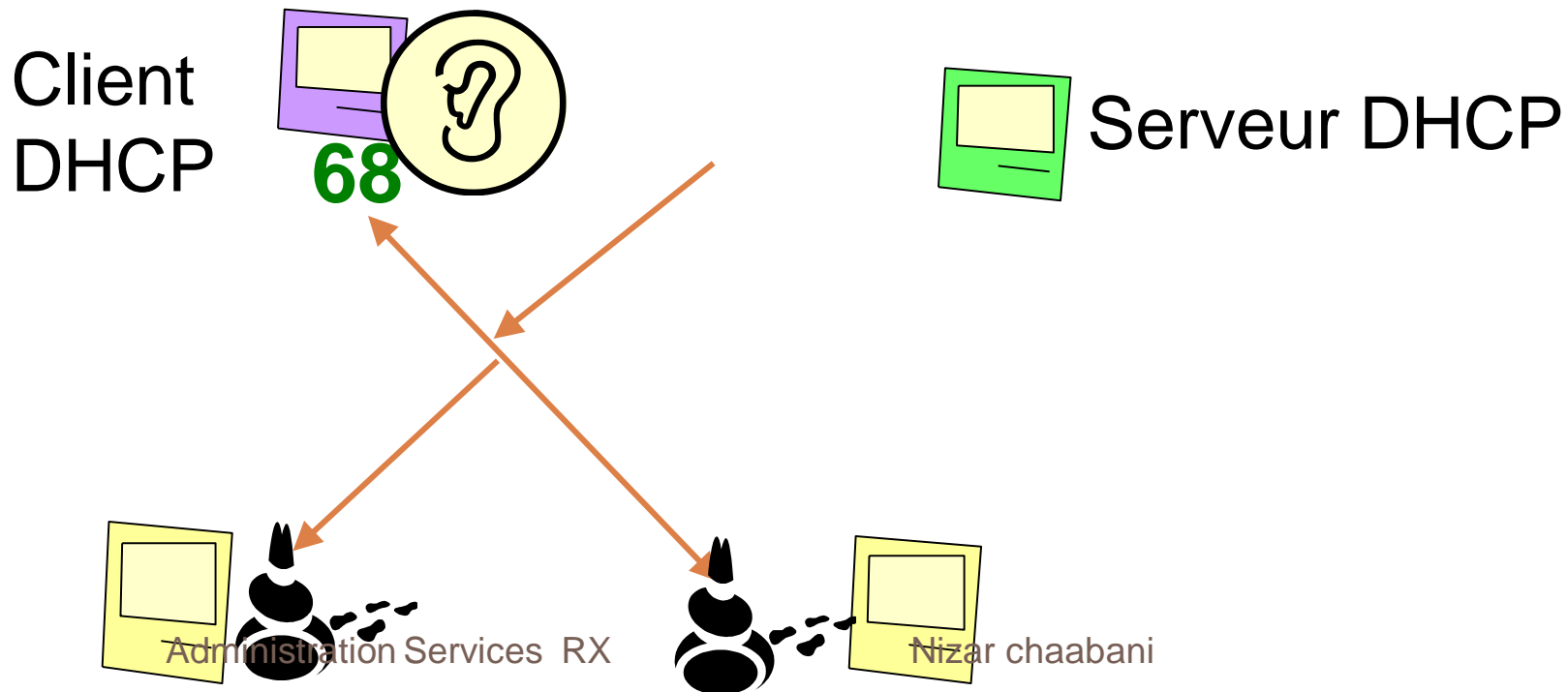
- Le client DHCP envoie la requête sur le port 67. Le serveur DHCP écoute sur le port 67.



# Niveau Transport - réponses

34

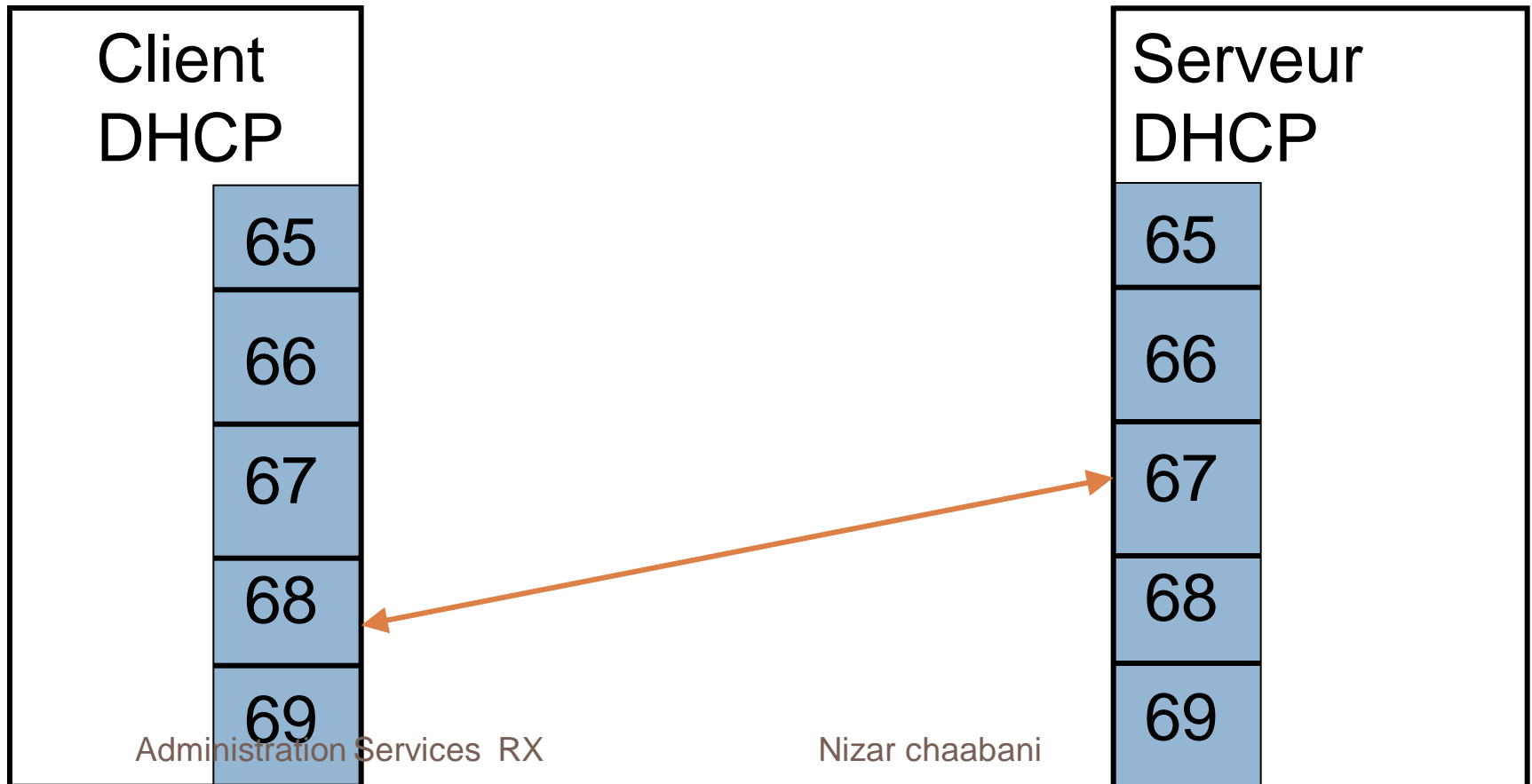
- Le serveur DHCP envoie la requête sur le port 68.  
Le client DHCP écoute sur le port 68.



# DHCP : le client utilise un port réservé

35

- Port serveur DHCP 67
- Port Client DHCP 68



# Trame contenant un DHCPDiscover

36

Ethernet

00:20.8f:b9:49:37

ff:ff:ff:ff:ff:ff

IP

0.0.0.0

255.255.255.255

UDP

68

67

Adresse  
physique du  
client DHCP

Trame contenant  
DHCPDiscover

37

00:20:8f:b9:49:37  
ff:ff:ff:ff:ff:ff

adresse  
physique de  
diffusion

Adresse  
IP  
« neutre »

0.0.0.0  
255.255.255.255

Adresse IP  
de  
diffusion  
générique

Port  
source  
datagramme

68  
67

Message  
DHCPDiscover

# Trame contenant un DHCPOffer

38

Ethernet

00.00.b4:bb:7d:ee

00:20.8f:b9:49:37

IP

192.168.0.253

UDP

67

68

Message DHCPOffer

# DHCP Offer

Adresse  
physique du  
serveur DHCP

00.00.b4:bb:7d:ee

adresse  
physique  
du client

00:20.8f:b9:49:37

Adresse  
IP serveur  
DHCP

192.168.0.253

Port  
source  
datagramme

67

68

Message DHCP Offer

# Trame contenant un DHCPRequest

40

Ethernet

00:20.8f:b9:49:37

ff:ff:ff:ff:ff:ff

IP

0.0.0.0

255.255.255.255

UDP

68

67

Message DHCPRequest



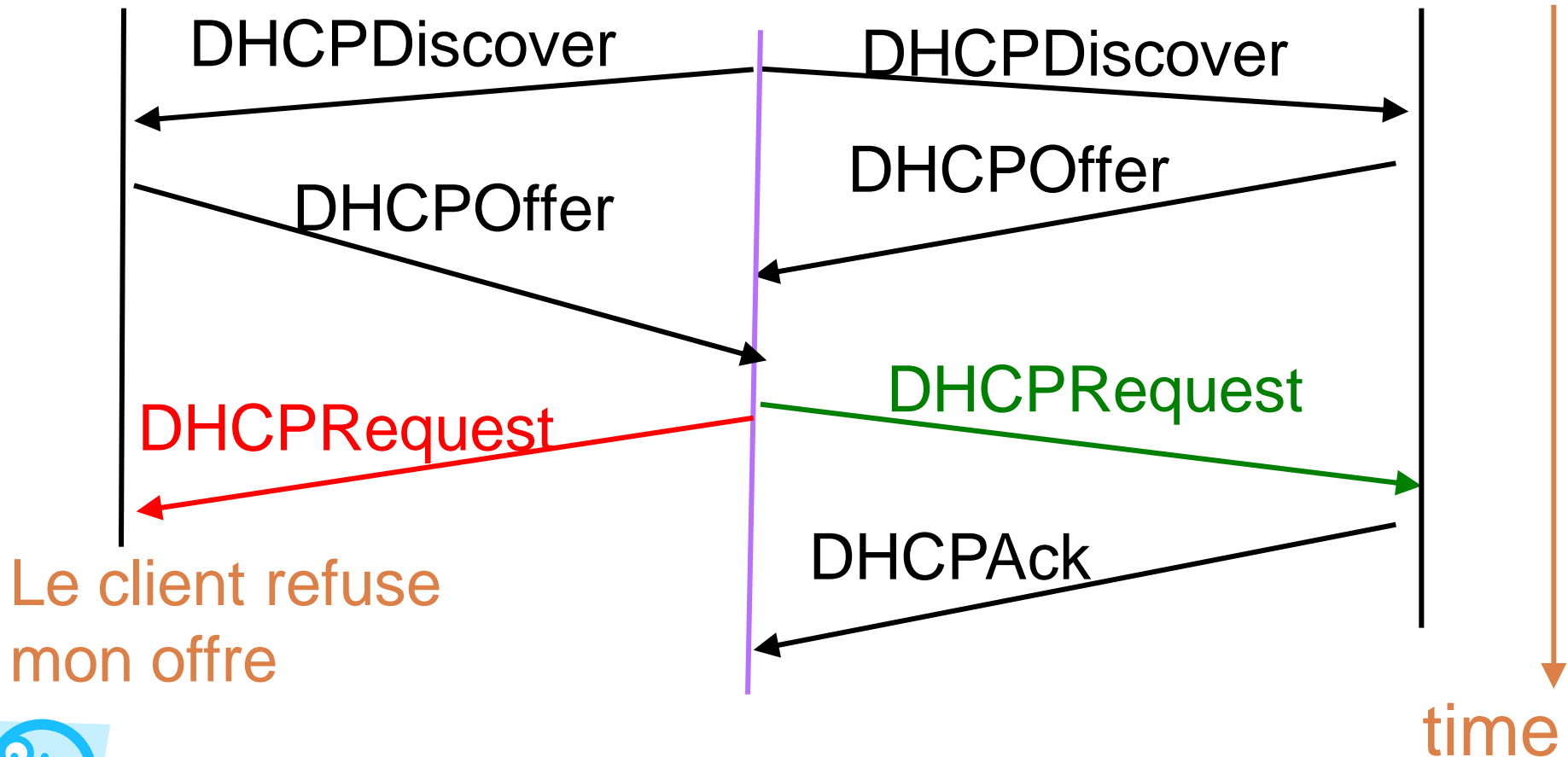
# Demande de baux DES serveurs DHCP

41

**serveur**

**client**

**serveur**



## Bilan des échanges lors d'une demande de bail

# Les paquets IP échangés

43

Source	Destination	Protocol Info
0.0.0.0	255.255.255.255	DHCPDiscover

**# le serveur DHCP vérifie que l'adresse IP qu'il veut offrir n'est pas utilisée**

Serveur DHCP	Broadcast	ARP 192.168.0.9?
--------------	-----------	------------------

192.168.0.253		DHCPOffer
---------------	--	-----------

0.0.0.0	255.255.255.255	DHCPRequest
---------	-----------------	-------------

192.168.0.253	192.168.0.9	DHCPACK
---------------	-------------	---------

**# le client vérifie via ARP que personne n'utilise sa nouvelle adresse**

Client DHCP	Broadcast	ARP 192.168.0.9?
-------------	-----------	------------------

# Format d'un message DHCP

# Dynamic Host Configuration Protocol

45

DHCP a été conçu comme complément de BOOTP-Bootstrap Protocol –

BOOTP: [RFC 951 - 1985]

- Protocole de démarrage
- Une station récupère les informations pour s'amorcer (« booter ») sur un serveur « d'amorçage » distant

# Format d'un message BOOTP

46

OP	HTYPE	HLEN	HOPS
identifiant session			
secs		flags	
adresse IP client (écrit par le client)			
adresse IP client (proposée par le serveur)			
serveur adresse IP			
gaterway adresse IP			
adresse physique du client			
nom du serveur			
Fichier d'amorçage			
OPTION			

Administration Services RX

Nizar chaabani

# Format d'un message DHCP

47

OP	HTYPE	HLEN	HOPS
identifiant session			
secs		flags	
adresse IP client (écrit par le client)			
adresse IP client (proposée par le serveur)			
serveur adresse IP			
gaterway adresse IP			
adresse physique du client			
nom du serveur			
Fichier d'amorçage			
OPTIONS définies dans DHCP			

Administration Services RX

Nizar chaabani



# SERVICES DNS

<http://www.academiepro.com/enseignants-104-Chaabani.Nizar.html>



# Résolution de Noms et Résolution inverse

49

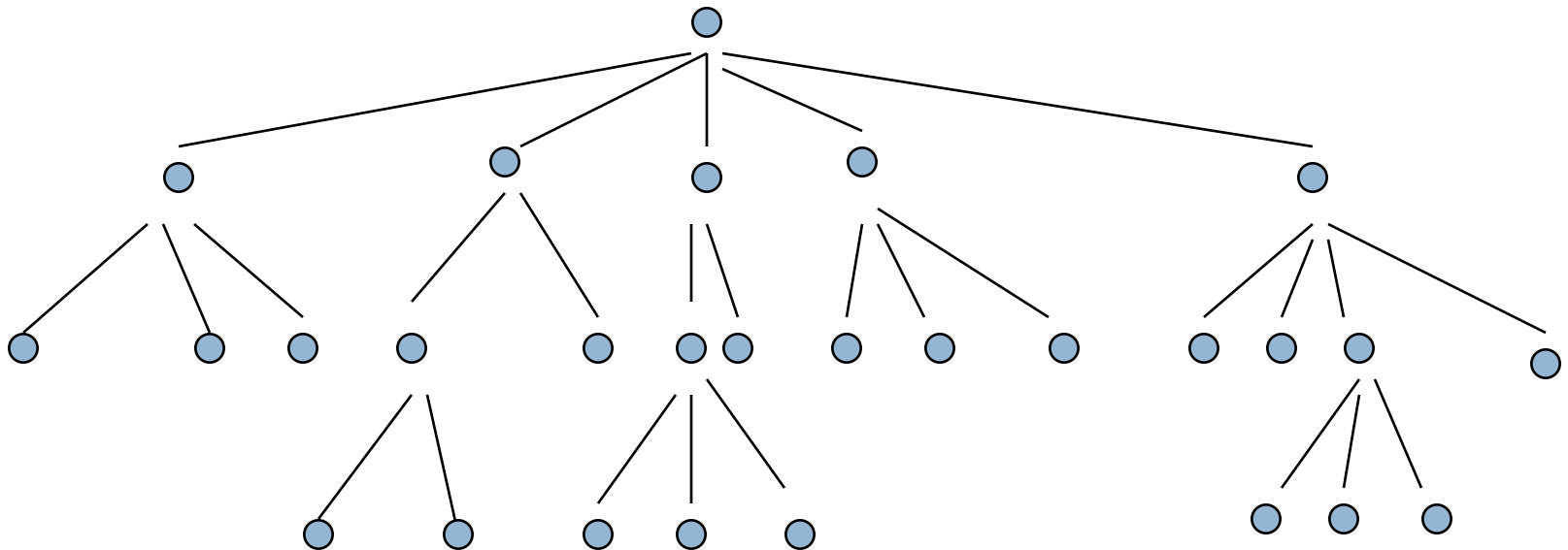
- Depuis 1984, les systèmes ont recours principalement à **DNS** pour la résolution de noms
- Adresse sous forme de nom plus agréable à manipuler qu'une adresse IP
- a **résolution de nom (forward lookup)** permet de trouver une adresse IP à partir d'un nom

la **résolution inverse (reverse lookup)** permet de trouver un nom à partir d'une adresse IP

# L'espace Nom de domaine

50

- Chaque unité de donnée dans la base DNS est indexée par un nom
- Les noms constituent un chemin dans un arbre inversé appelé **l'espace Nom de domaine**
- Organisation similaire à un système de gestion de fichiers



- Chaque noeud est identifié par un nom
- Racine appelée root, identifiée par «.»
- 127 niveaux au maximum

# Domaines racine

51

- Le système DNS impose peu de règles de nommage :
  - ▣ noms < 63 caractères
  - ▣ majucules et minuscules non significatives
  - ▣ pas de signification imposée pour les labels
- Le premier niveau de l'espace DNS fait exception à la règle :
  - ▣ 7 domaines racines prédéfinis :
    - com : organisations commerciales ; ibm.com
    - edu : organisations concernant l'éducation ; mit.edu
    - gov : organisations gouvernementales ; nsf.gov
    - mil : organisations militaires ; army.mil
    - net : organisations réseau Internet ; worldnet.net
    - org : organisations non commerciales ; eff.org
    - int : organisations internationales ; nato.int
  - ▣ arpa : domaine réservé à la résolution de nom inversée
  - ▣ organisations nationales : fr, uk, de, it, us, au, ca, se, etc.

# Lecture des noms de domaine

52

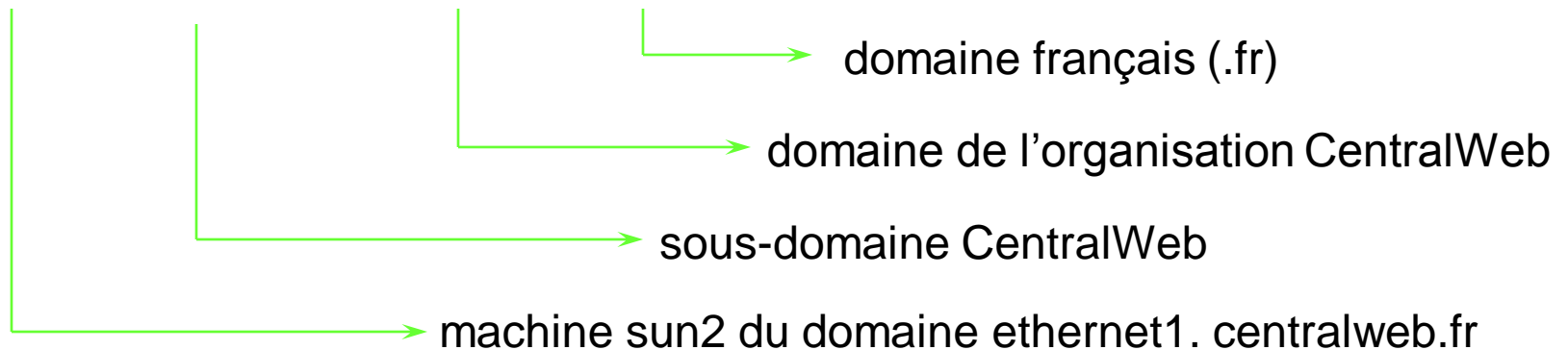
- A l'inverse de l'adressage IP la partie la plus significative se situe à gauche de la syntaxe :

sun2.ethernet1.centralweb.fr / 193.148.37.201

← vers le plus significatif

vers le plus significatif →

sun2. ethernet1. centralweb.fr



# Principes de résolution

53

- ✓ La communication entre clients et serveurs des services des noms utilise le **protocole dns** à partir des protocoles udp et tcp, usuellement le port 53.
- ✓ Le format des trames dns est identique dans le sens client/serveur (question) et serveur/client (réponse).

# Parcours de l'arborescence

54

Pour déterminer l'adresse ip correspondant au nom :

[www.security.com.fr](http://www.security.com.fr).

Il faut trouver :

- un **NS** (serveur de noms) de la racine .
- interroger pour un obtenir **NS** de [fr](http://fr).
- Interroger pour un **NS** de [com.fr](http://com.fr).
- Le **NS** de [security.com.fr](http://security.com.fr) identifie [www](http://www).

# D.N.S. Signifie, selon les cas, plusieurs choses

55

- **Domain Name System** : l'ensemble des organismes qui gèrent les noms de domaine.
- **Domain Name Service** : le protocole qui permet d'échanger des informations à propos des domaines.

**Domain Name Server** : un ordinateur sur lequel fonctionne un logiciel serveur qui comprend le protocole DNS et qui peut répondre à des questions concernant un domaine.

# Structure des domaines

56

- La structure des domaines est de forme hiérarchique avec :
  - ▣ **un niveau haut : le domaine racine,**
  - ▣ **des noeuds identifiés par des labels (organisés en niveaux)**
- Les Top Level Domain les plus courants sont organisés en deux types de domaines :
  - ▣ **Les domaines génériques**
  - ▣ **Les domaines géographiques**



# Les ZONES

57

- La base de données de nom est divisée en sections appelées **zones**
- Une **Zone** représente une partie de l'espace de nom de Domaine, a des fins de gestion.
- Données qui décrivent chaque zones :
  - ▣ Les données générales sur chaque nœuds de la zone
  - ▣ Les données qui définissent le nœud supérieur de la zone
  - ▣ Les données qui décrivent les sous zones
  - ▣ Les données qui permettent d'accéder aux serveurs de noms qui gèrent les sous zones.

# Types de Serveurs

58

- **Le serveur primaire** : serveur d'autorité sur sa zone : il tient à jour un fichier appelé "fichier de zone", qui établit les correspondances entre les noms et les adresses IP des « hosts » de sa zone.
- **Le serveur secondaire** : obtient les données de zone via le réseau, à partir d'un autre serveur de nom qui détient l'autorité pour la zone considérée. Il est capable de répondre aux requêtes de noms Ip (partage de charge), et de secourir le serveur primaire en cas de panne..
- **Le serveur cache** ne constitue sa base d'information qu'à partir des réponses des serveurs de noms. Il inscrit les correspondances nom / adresse IP dans un cache avec une durée de validité limitée (Ttl) ; il n'a aucune autorité sur le domaine : il n'est pas responsable de la mise à jour des informations contenues dans son cache, mais il est capable de répondre aux requêtes des clients Dns.
- **les serveurs racine** : ils connaissent les serveurs de nom ayant autorité sur tous les domaines racine. Les serveurs racine connaissent au moins les serveurs de noms pouvant résoudre le premier niveau (.com, .edu, .fr, etc.) si les serveurs racine sont inopérationnels, il n'y a plus de communication sur l'Internet

# Le principe

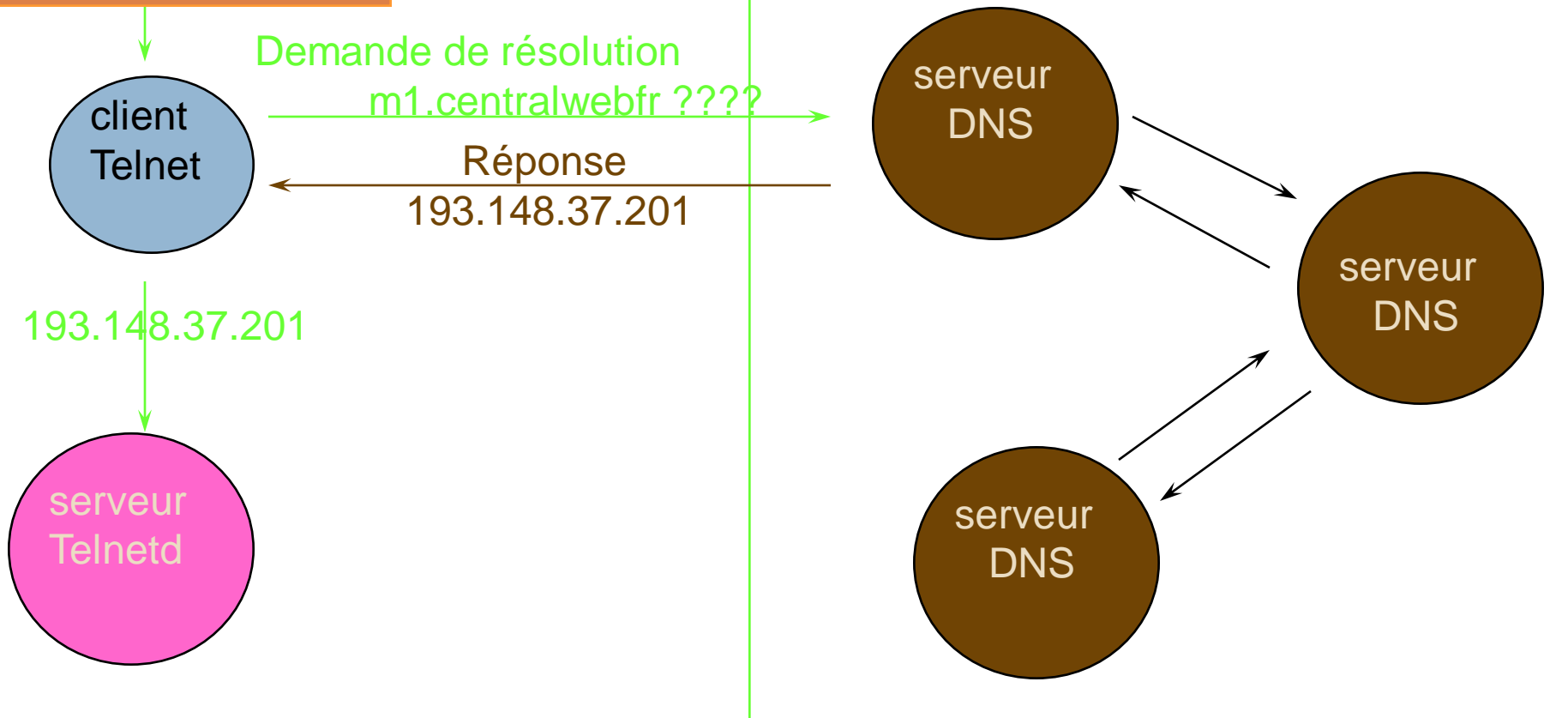
59

- basé sur le modèle client / serveur
- le logiciel client interroge un serveur de nom; typiquement :
  - ▣ l'utilisateur associe un nom de domaine à une application ; exemple :  
`telnet m1.centralweb.fr`
  - ▣ l'application cliente requiert la traduction du nom de domaine auprès d'un serveur de nom (DNS) : cette opération s'appelle la résolution de nom
  - ▣ le serveur de nom interroge d'autres serveurs de nom jusqu'à ce que l'association `nom de domaine / adresse IP` soit trouvée
- le serveur de nom retourne l'adresse IP au logiciel client : `193.148.37.201`
- le logiciel client contacte le serveur (`telnetd`) comme si l'utilisateur avait spécifié une adresse IP : `telnet 193.148.37.201`

# Principe (illustration)

60

```
$ telnet m1.centralweb.fr
```



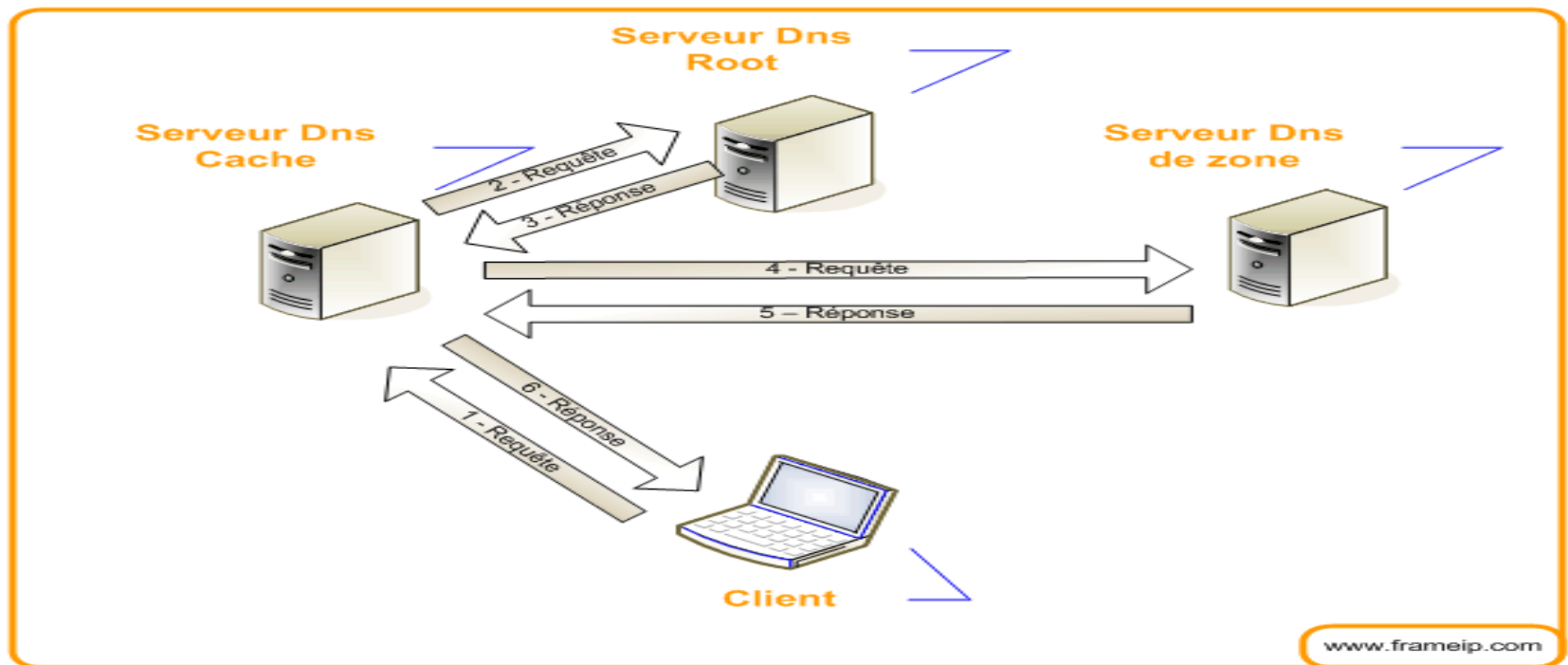
# Resolution inverse

61

- Consiste a obtenir le nom de domaine à partir de l'adresse IP
  - ▣ pour faciliter la compréhension des humains
  - ▣ pour des raisons de sécurité
- Plus délicate que nom -> IP car le système DNS est organisé pour la résolution de nom ==> recherche exhaustive ???

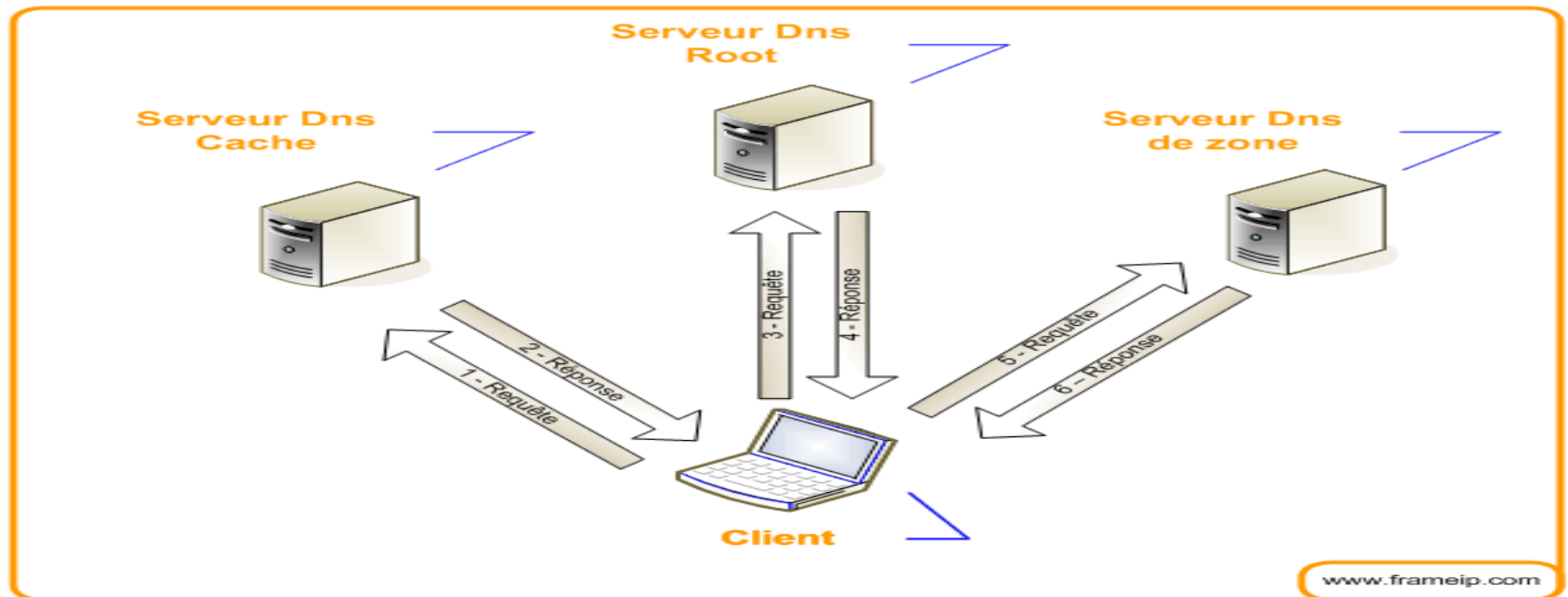
# Requête récursive

- Lorsqu'un serveur DNS reçoit une requête récursive, il doit donner **la réponse la plus complète possible**. C'est pourquoi le serveur DNS est souvent amené à **joindre d'autres serveurs** de noms dans le but de trouver la réponse exacte.



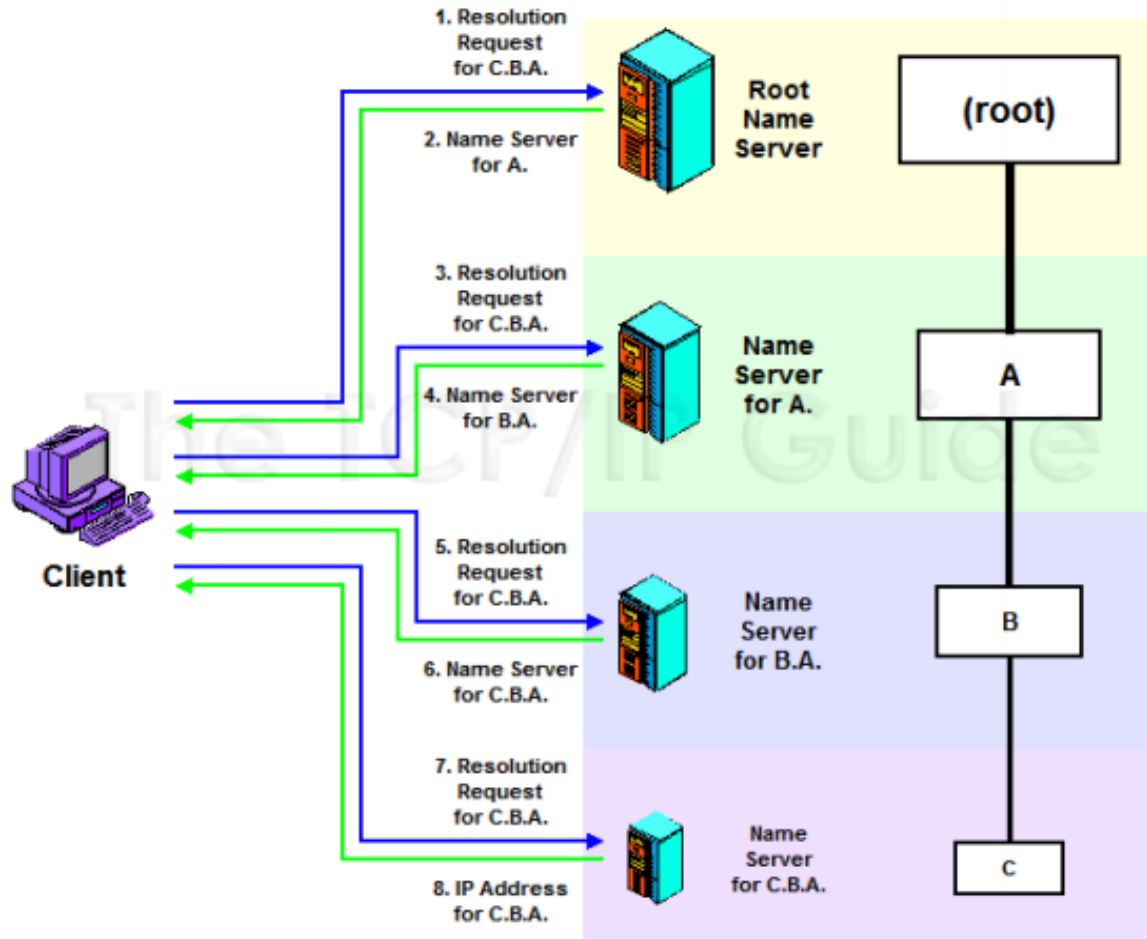
# Requête itérative

- Lorsqu'un serveur reçoit une requête itérative, il renvoie la meilleure réponse qu'il peut donner **sans contacter d'autres serveurs**



# Résolution Itérative

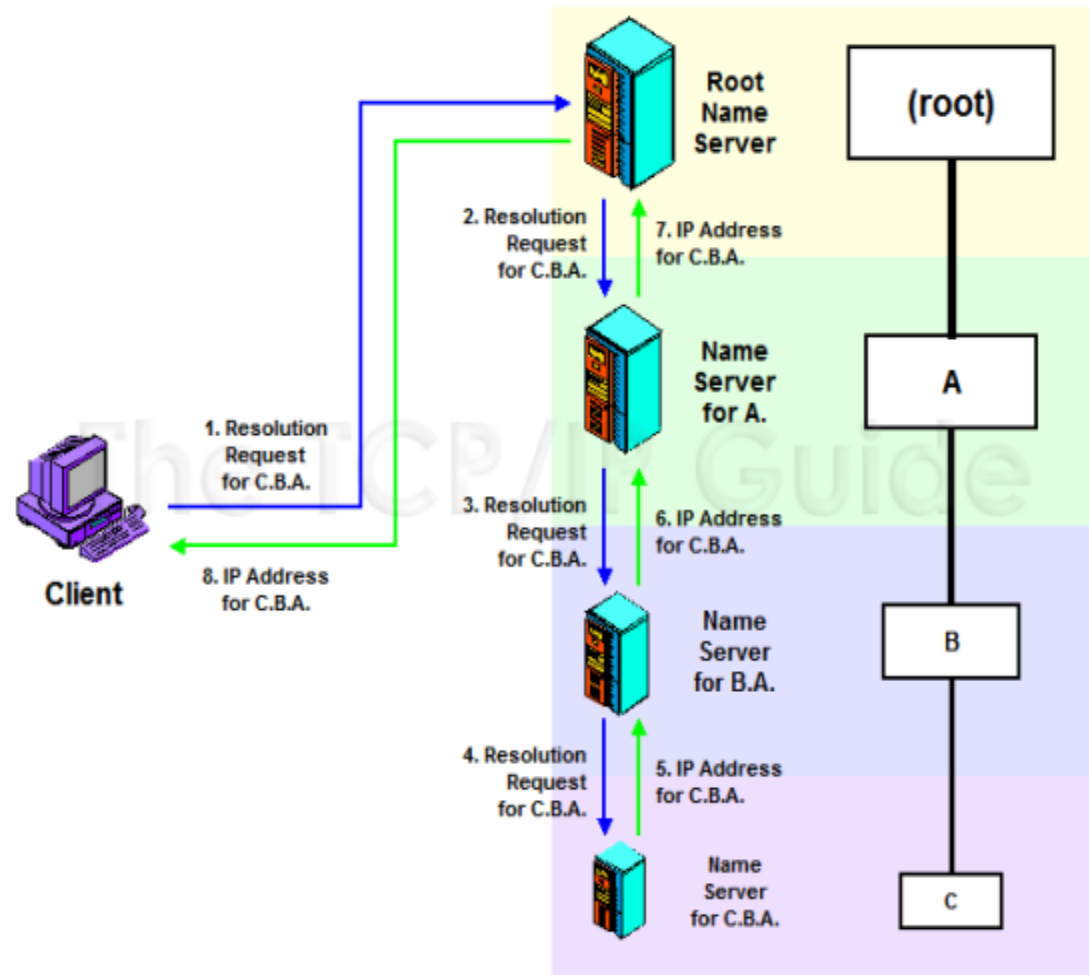
- Le client envoie une requête itérative
- Réponse par l'adresse IP ou le nom d'un autre serveur qui contient l'information ou est plus proche d'elle
- Le client original doit répéter la requête pour le nouveau serveur



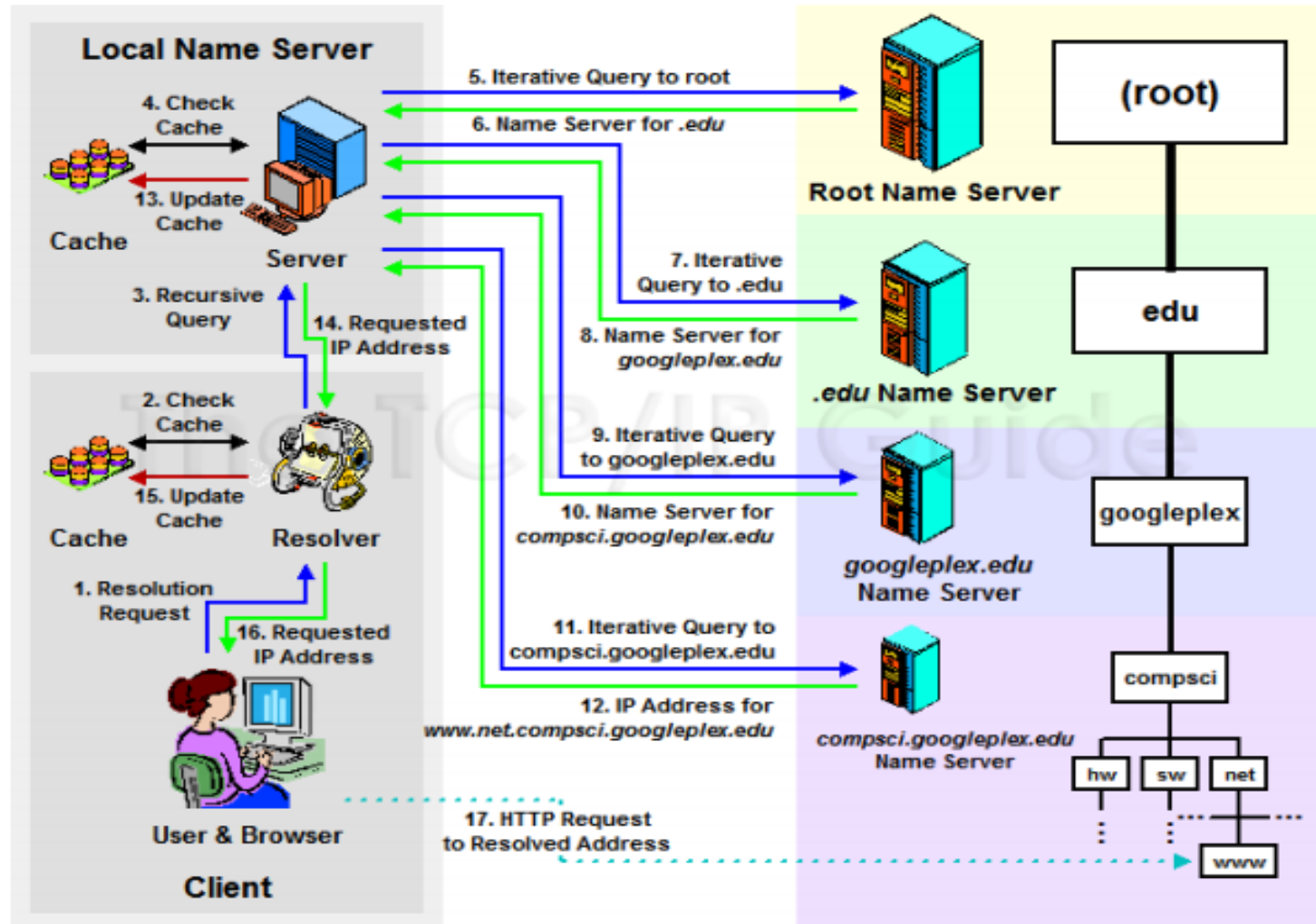


# Résolution Récursive

- Le client envoie une requête récursive
- Le serveur répond par l'adresse IP ou joue le rôle de client
- Le client original envoie une seule requête

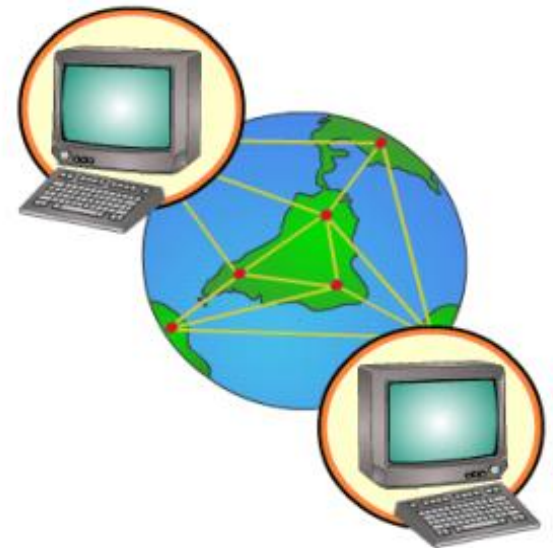


# Exemple de résolution de nom

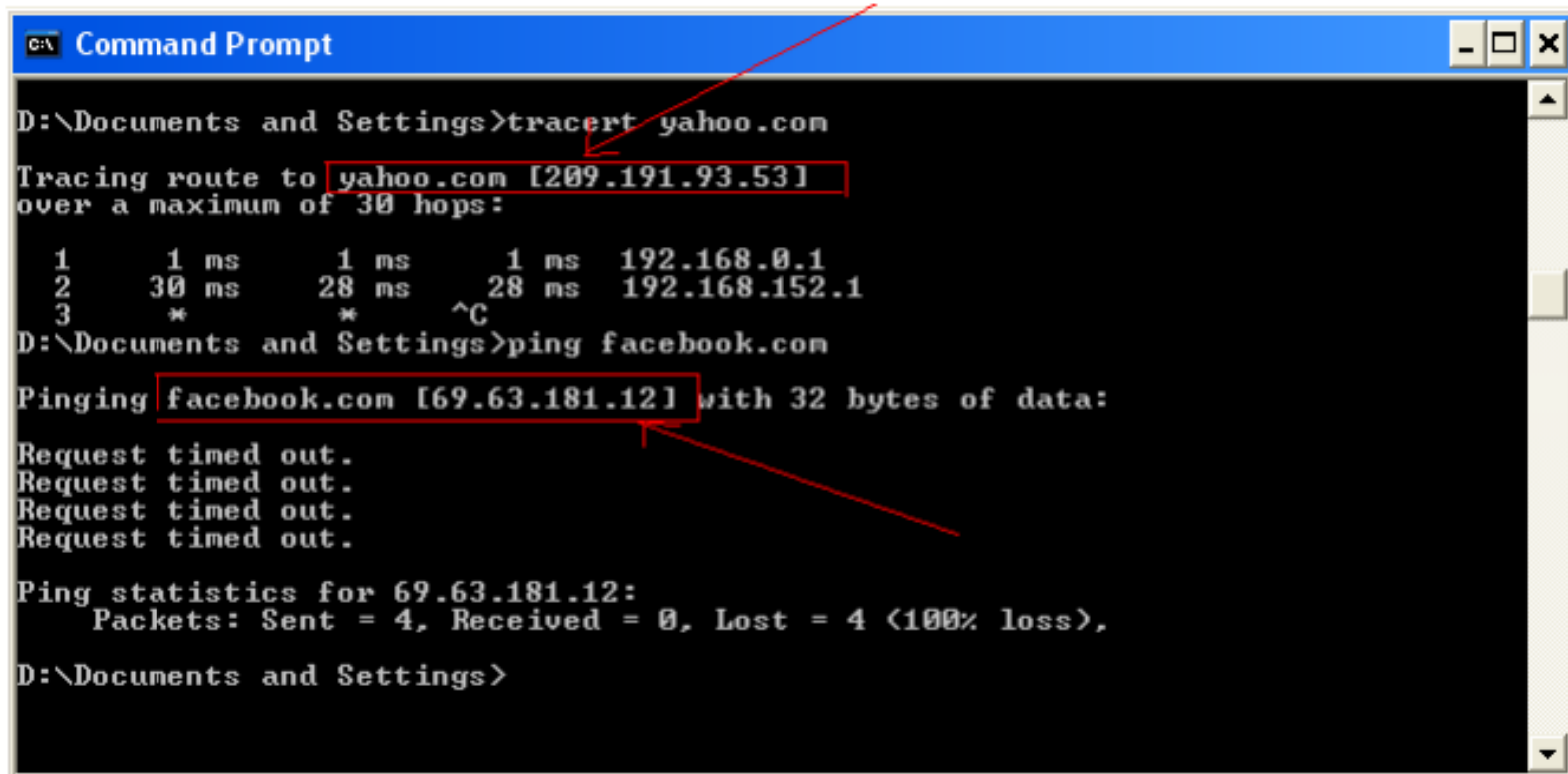


# Les applications du DNS (1)

- Le World Wide Web n'est pas la seule application utilisant DNS
- DNS rend service à toute application pouvant utilisé un nom de domaine
- FTP, Traceroute, Ping



# Les applications du DNS (2)



The screenshot shows a Windows Command Prompt window with a blue title bar labeled "C:\ Command Prompt". The command prompt displays the following text:

```
D:\Documents and Settings>tracert yahoo.com
Tracing route to yahoo.com [209.191.93.53]
over a maximum of 30 hops:
  1      1 ms      1 ms      1 ms    192.168.0.1
  2     30 ms     28 ms     28 ms    192.168.152.1
  3      *        *        ^C
D:\Documents and Settings>ping facebook.com
Pinging facebook.com [69.63.181.12] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 69.63.181.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
D:\Documents and Settings>
```

Two red arrows point to the IP addresses in the output: one points to `209.191.93.53` in the `tracert` command, and the other points to `69.63.181.12` in the `ping` command.

# Protocoles de la couche Transport

- DNS utilise TCP et UDP pour envoyer ses messages
- Les messages classiques sont courts => utilise UDP
  - DNS lui-même gère la détection et la retransmission (2 à 5 sec) des requêtes perdues
  - Limite du message UDP pour DNS est de 512 octets
- Pour l'échange de larges informations tel que le « zone transfer », TCP est utilisé
- TCP/UDP Port number 53

- ❑ La commande dig permet d'interroger des serveurs DNS (man dig), elle accepte des paramètres plus fins que la commande nslookup (man nslookup) qui existe également sous windows, mais un peu différente
- ❑ Les commandes Netsh pour DHCP offre un outil de ligne de commande utile à l'administration des serveurs DHCP et fournit une solution alternative équivalente à la gestion sur console. Elles sont utiles dans les cas suivants :



# LDAP LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL

<http://www.academiepro.com/enseignants-104-Chaabani.Nizar.html>

# Définitions et concepts

72

- Un annuaire est un conteneur d'informations organisées.
  
- Exemples d'annuaires courants
  - ▣ annuaire téléphonique : Les Pages Jaunes
  - ▣ carnet d'adresses
  - ▣ catalogue de vente
  
- Un annuaire global célèbre très utilisé : DNS
  - ▣ il a un espace de nommage uniforme
  - ▣ il est distribué entre des serveurs coopérants



# Définitions et concepts

73

- Un annuaire est une base de données, mais une base de données n'est pas un annuaire
  - Lecture
  - Performance
  - Extensibilité
  - Communication entre serveurs
- Un annuaire n'est pas :
  - approprié à de fréquentes écritures
  - destiné à manipuler des données volumineuses
  - un substitut à un serveur FTP, un système de fichiers,...

# Qu'est-ce qu'un annuaire

74

- Répertoire en ligne, dynamique
- Possibilité de faire des recherches
- Contrôle d'accès à l'information

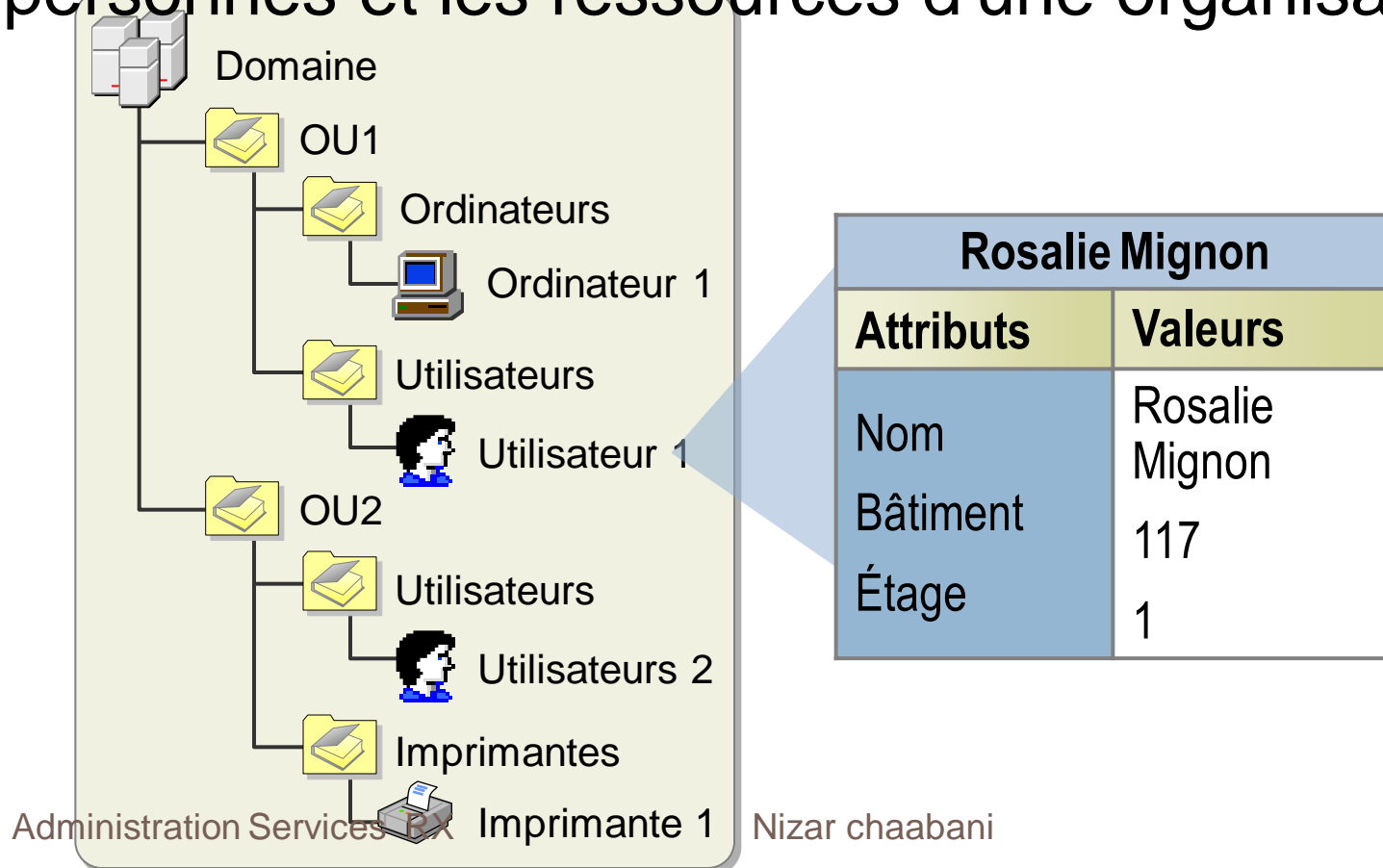
Ce n'est pas:

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

# Définition d'un service d'annuaire

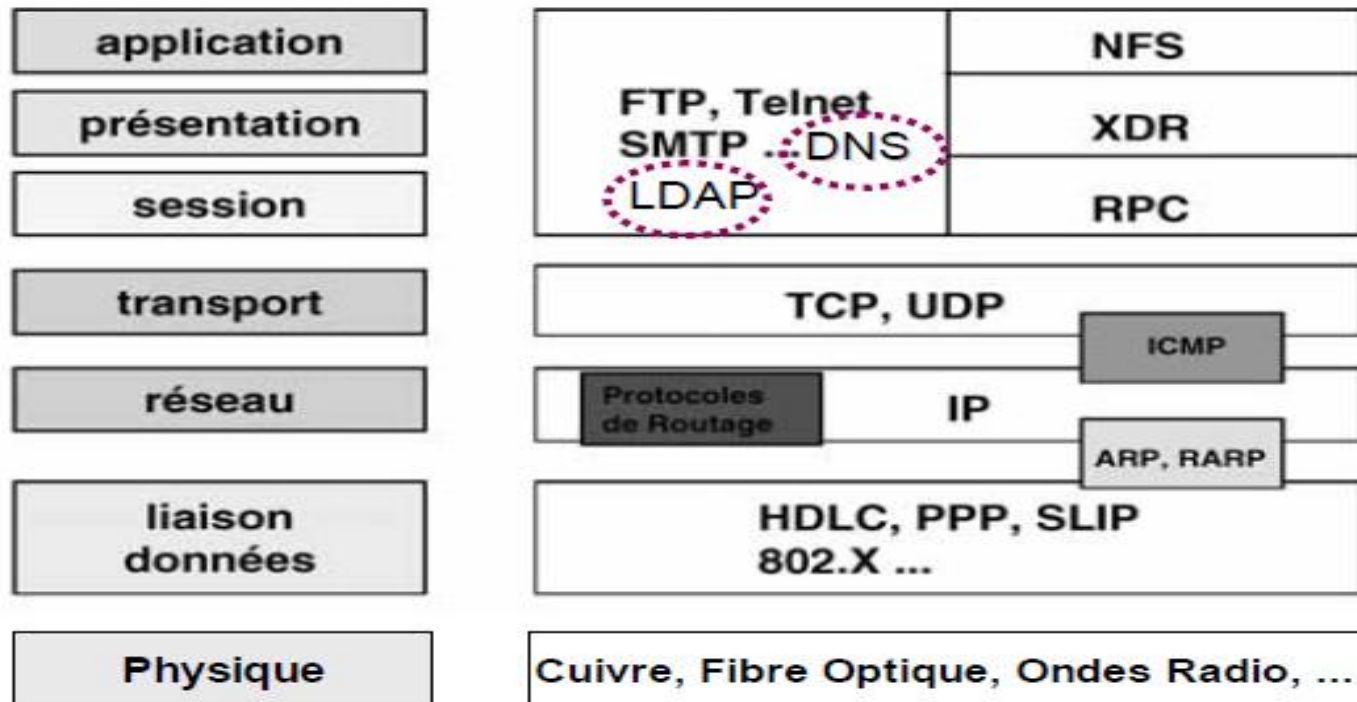
75

- Un référentiel d'informations structuré sur les personnes et les ressources d'une organisation



Nizar chaabani

## Rappel : L'architecture TCP/IP



## 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

# Facettes de LDAP

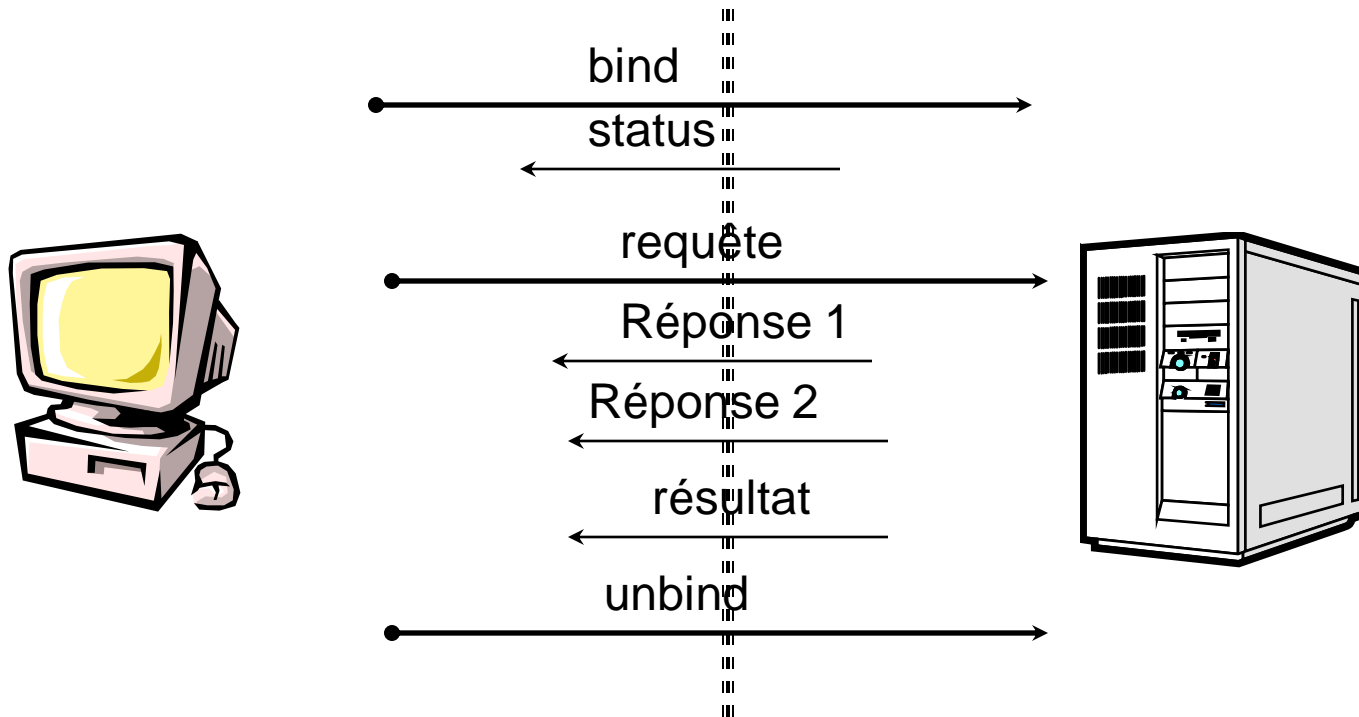
78

LDAP définit :

- le **protocole** -- comment accéder à l'information contenue dans l'annuaire,
- un **modèle d'information** -- le type d'information contenu dans l'annuaire,
- un **modèle de nommage** -- comment l'information est organisée et référencée,
- un **modèle fonctionnel** -- comment on accède à 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,
- **LDIF** -- un format d'échange de données.

# Protocole (2): client-serveur

79



**L'authentification est faite pendant le bind.**

# Modèle de nommage / modèle d'information

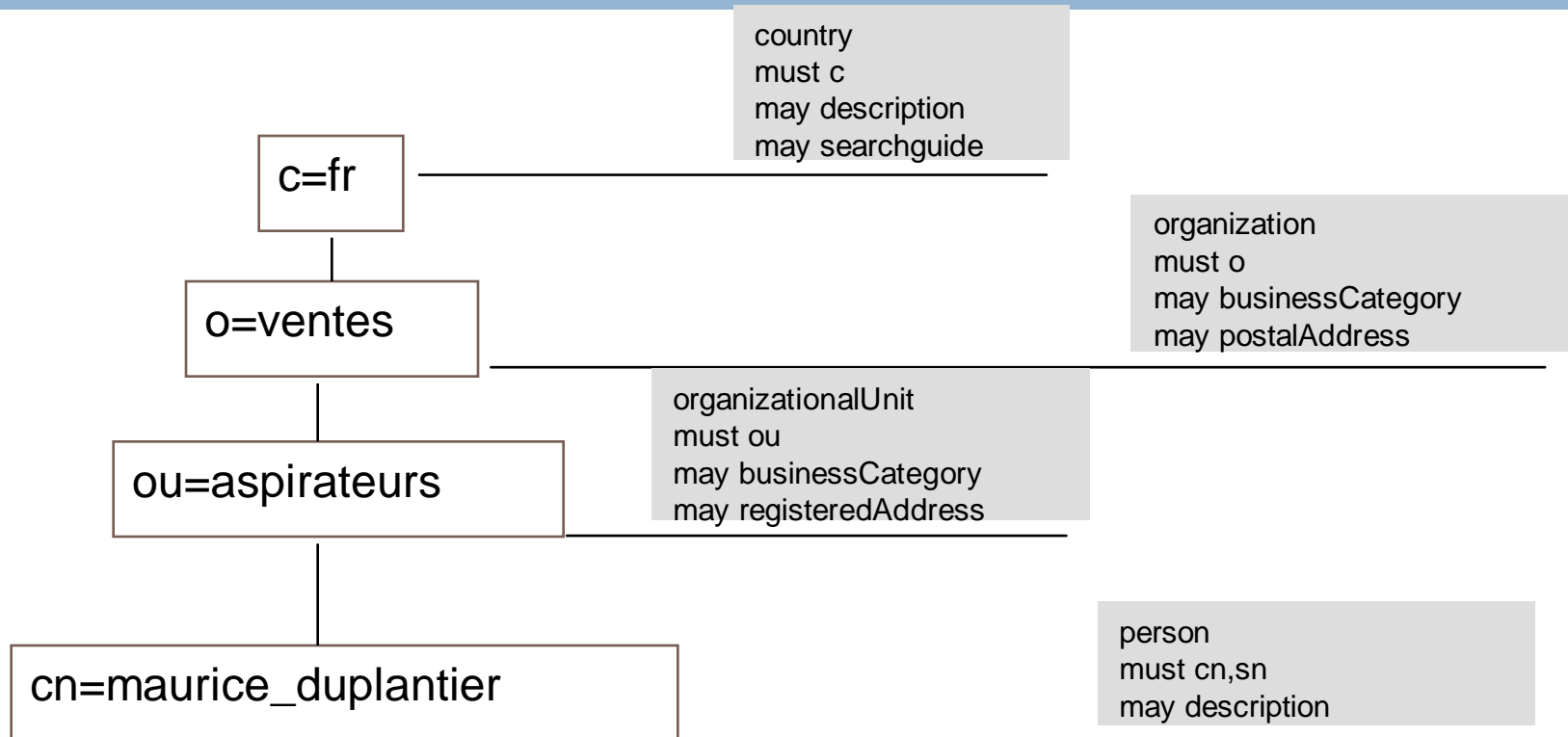
80

Le **modèle de nommage** définit comment sont organisées les entrées de l'annuaire et comment elles sont référencées.

Le **modèle d'information** définit le type de données pouvant être stockées dans l'annuaire.



# Modèle de nommage / modèle d'information

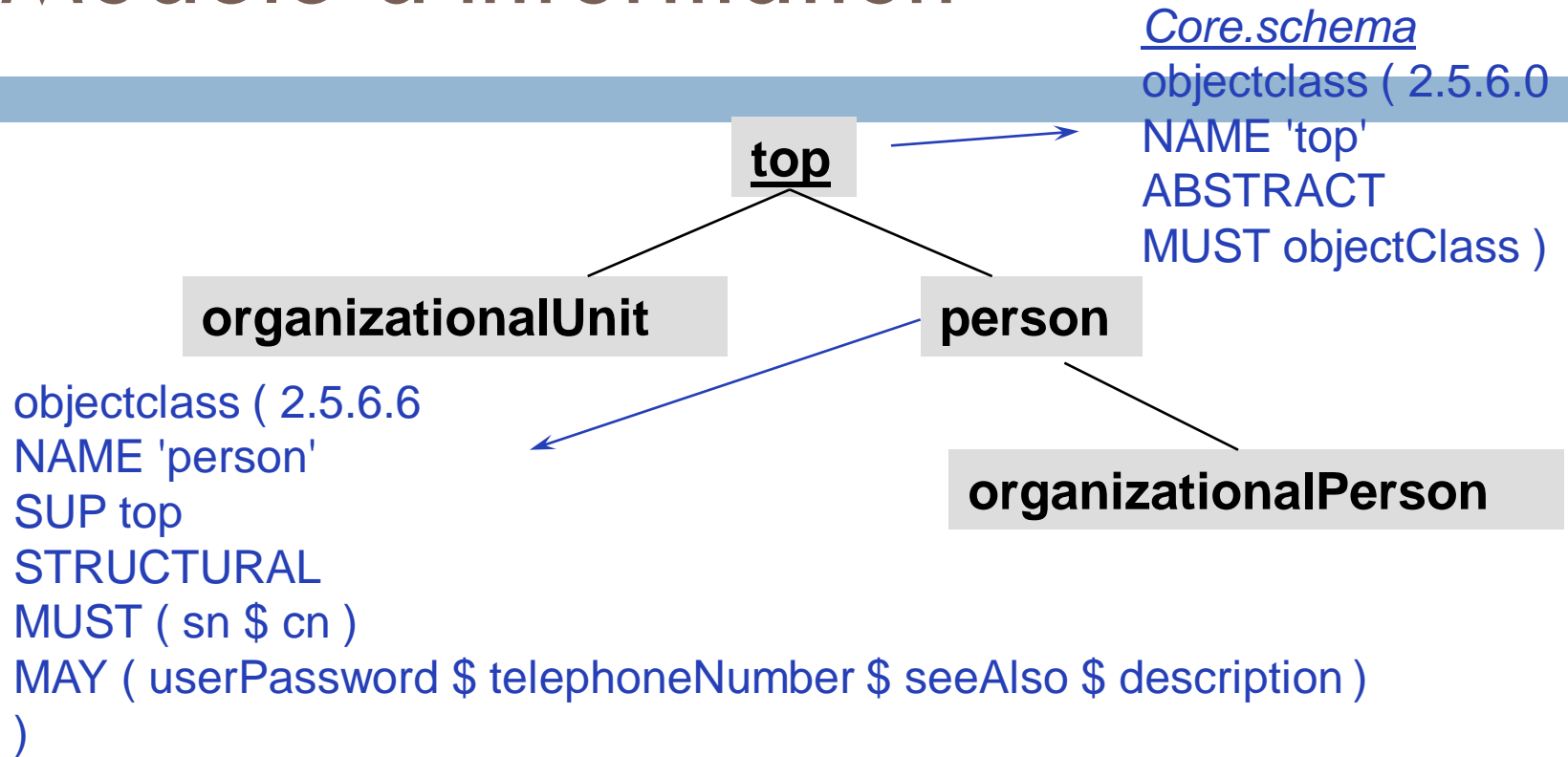


modèle de nommage

modèle d'information

# Modèle d'information

82



- ❑ Les classes d'objets forment une hierarchie, au sommet de laquelle on trouve l'objet top
- ❑ Chaque classe d'objet hérite des attributs de la classe père

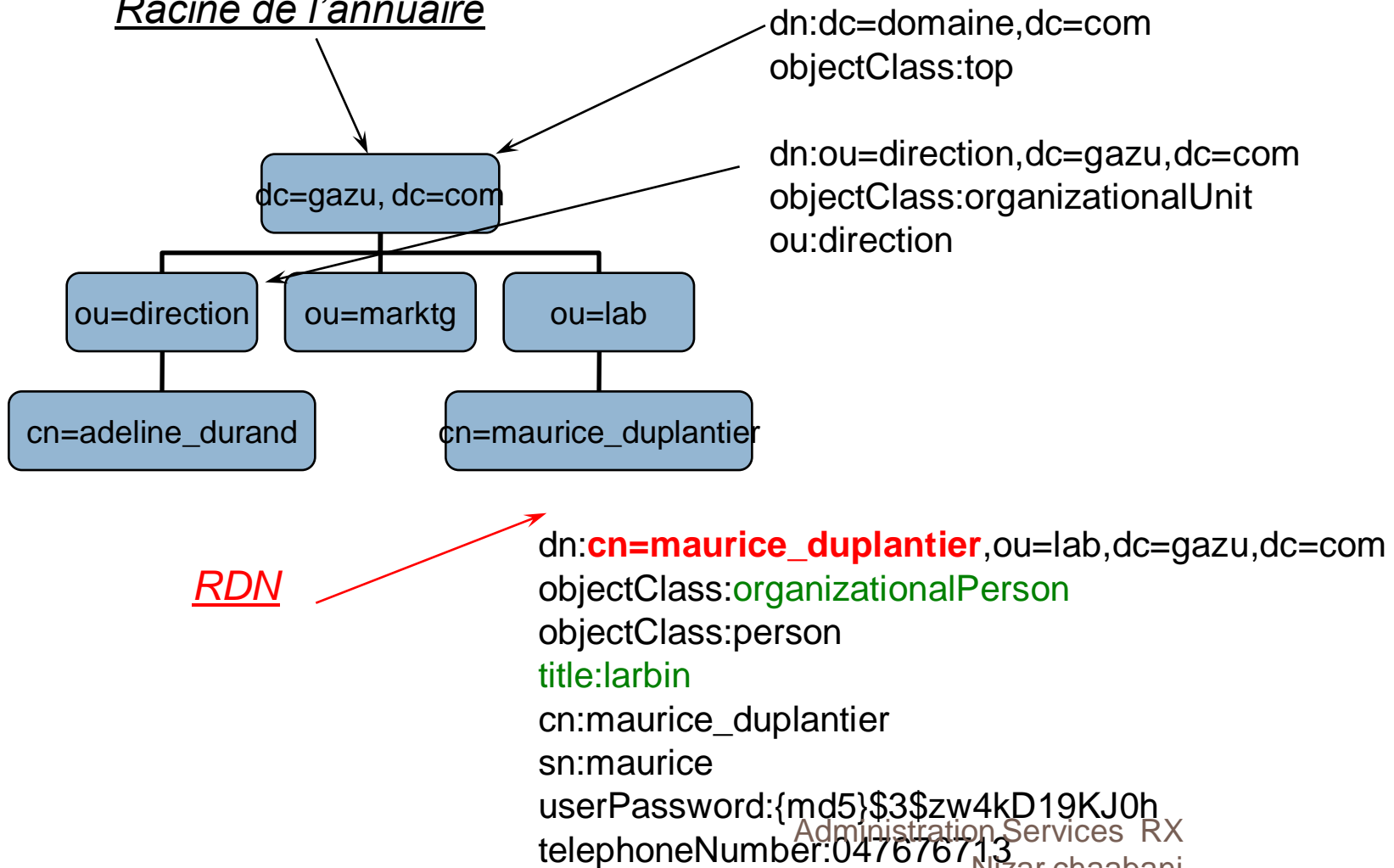
# Le modèle de nommage

83

- ❑ Organisation des entrées : structure logique arborescente, le directory information tree (DIT)
- ❑ Chaque objet est une instance d'objet
- ❑ Chaque entrée est identifiée par un nom, le DN=distinguished name
- ❑ Le “suffix” définit l'espace de nommage dont le serveur a la gestion
- ❑ Un noeud de l'arbre (entrée de l'annuaire) est appelé DSE (directory service entry)
- ❑ Sommet de l'arbre: BaseDN ou rootDSE racine de l'arbre

# Le modèle de nommage

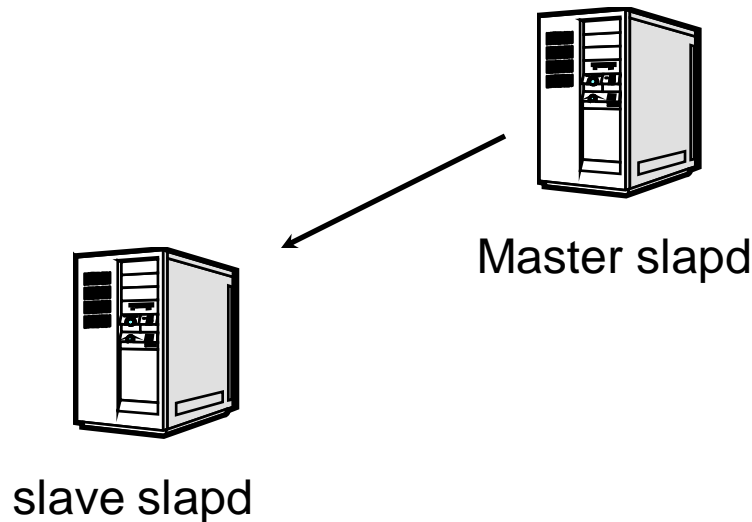
## Racine de l'annuaire



# Duplication: *replication*

85

- Le modèle de duplication (replication service) définit comment dupliquer l'annuaire sur plusieurs serveurs.
- Pas encore standard, mais est proposé par la plupart des serveurs.
- L'IETF prépare le protocole LDUP.



# vulnérabilités

86

- Déni de service
  - ▣ Codes BER semi-valides, requete malformées => freeze
  - ▣ Mesures compensatoires
    - Firewall
    - Opérations signées
- Buffer overflow
  - ▣ Attaquant récupère les privilèges système, ou privilège de la database
  - ▣ Mesures compensatoires
    - Tourner ldap en chroot



# CONFIGURATION DE WINDOWS SERVER ACTIVE DIRECTORY

<http://www.academiepro.com/enseignants-104-Chaabani.Nizar.html>

# L'Active Directory

88

- La mise en place d'un domaine Windows 200x passe par l'installation :
    - ▣ D'un annuaire appelé par Microsoft "Active Directory"
    - ▣ D'un serveur DNS
- (Le serveur DHCP n'est pas nécessaire dans un premier temps)



# L'Active Directory

89

- L'Active Directory de Microsoft est le service d'annuaire fourni par Windows 200x Server (abandon de la notion de base de comptes intégrée dans la base de registre)
- L'Active Directory supporte les protocoles suivants :
  - ▣ TCP/IP : protocole réseau
  - ▣ DNS : la gestion des noms de domaine Windows 200x repose sur ce service.

# L'Active Directory

90



L'Active Directory supporte les protocoles suivants :

- **DHCP** : Distribution d'adresses IP. Il renseigne le DNS sur les adresses distribuées (DHCP dynamique).
- **SNTP** : protocole de distribution de l'heure.  
Toutes les machines W2k doivent être synchronisées car l'authentification Kerberos se base sur un ticket horodaté.

# L'Active Directory

91

- L'Active Directory supporte les protocoles suivants :
  - ▣ **LDAP** : protocole d'accès à l'annuaire
  - ▣ **KERBEROS** : permet l'authentification
  - ▣ **LDIF** : permet la synchronisation de l'annuaire  
(*Lightweight Data Interchange Format*)

# L'Active Directory

92

**Racine .lyc**

Un domaine Windows 2000 comprendra un ou plusieurs serveurs. Les objets du domaine sont décrits dans l'Active Directory.

**Domaine tsinfo.lyc**  
Serveur : infosrv1  
(infosrv1.tsinfo.lyc)

**Serveur : infosrv2**  
(infosrv2.tsinfo.lyc)

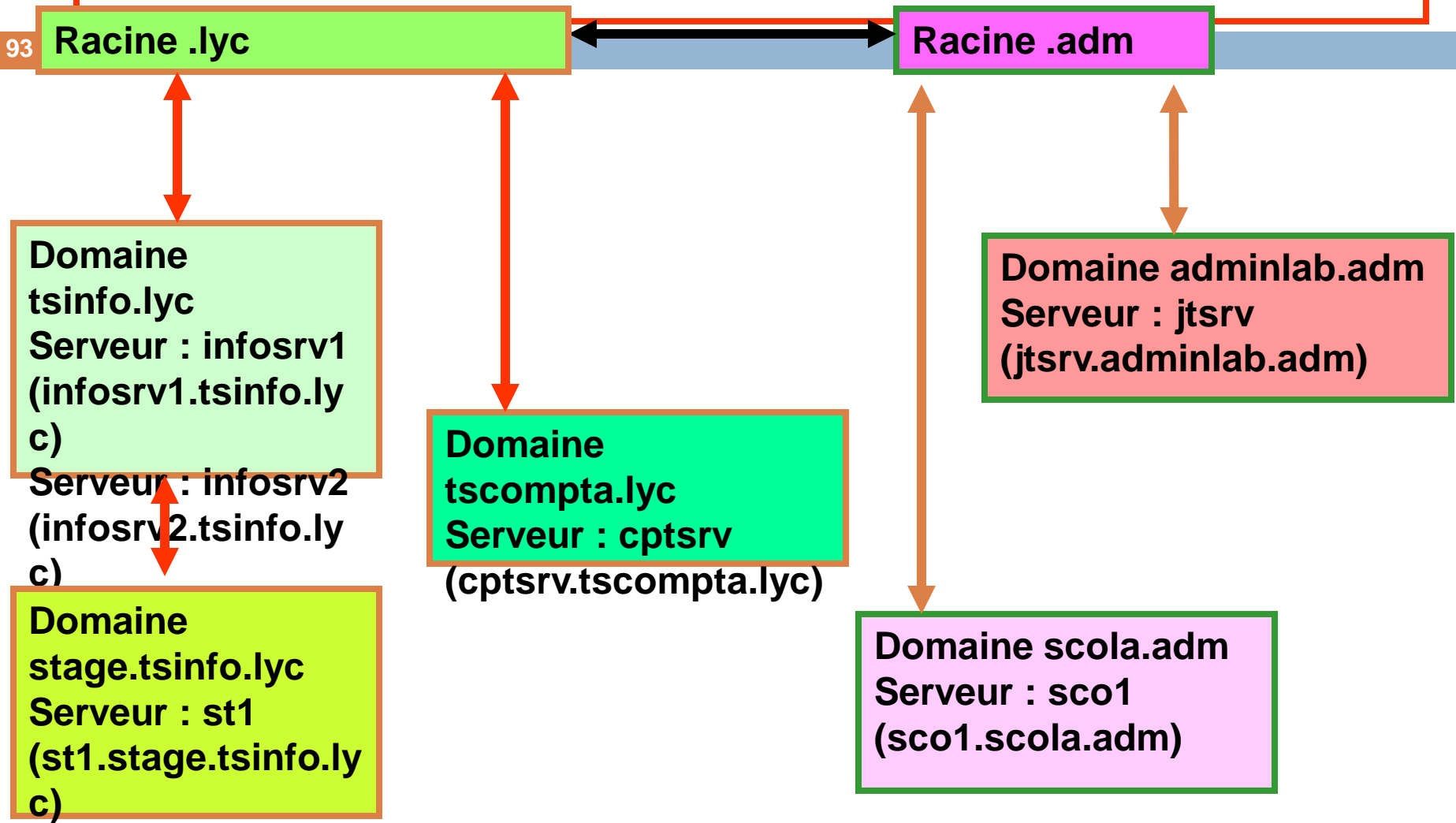
**Domaine stage.tsinfo.lyc**  
Serveur : st1  
(st1.stage.tsinfo.lyc)

**Domaine tscompta.lyc**  
Serveur : cptsrv  
(cptsrv.tscompta.lyc)

D'autres domaines peuvent être créés. Ils sont reliés entre eux **hiérarchiquement** par des **relations des d'approbation** **bidirectionnelles transitives**

**Les domaines ainsi reliés forment un ARBRE**

# L'Active Directory



Les **ARBRES** ainsi reliés forment une **FORET**

# L'Active Directory

94

Les objets de l'Active Directory sont :

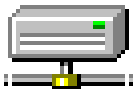


- Un compte d'utilisateur

- Un ordinateur



- Un dossier partagé publié



- Un groupe

- Une imprimante publiée



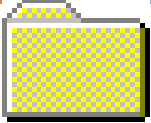
- Un contact

- Un objet contact est un compte qui ne dispose d'aucune autorisation de sécurité. Vous ne pouvez pas vous connecter au réseau en tant que contact. Les contacts représentent les utilisateurs externes dans le cadre de la messagerie par exemple



# L'Active Directory

95



Les objets de l'Active Directory sont

- Une unité organisationnelle
- Les unités d'organisation sont utilisées comme conteneurs pour organiser de façon logique des objets d'annuaire tels que les utilisateurs, les groupes et les ordinateurs ...

# L'Active Directory

96

Tous les objets ont des attributs, par exemple :

- ▣ Nom et prénom d'un utilisateur
- ▣ Nom de partage d'un dossier

Certains attributs sont obligatoires (nom de l'utilisateur)  
d'autres sont facultatifs (son numéro de téléphone)



# L'Active Directory

97

L'ensemble des attributs sont définis dans le **SCHEMA**

Le composant enfichable *Schema Active Directory* permet de modifier le schéma pour ajouter des attributs (attention, il est impossible d'en supprimer).

# Exemple de création d'une A.D

98

- L'objectif de cet exemple est de créer 2 forêts **bts** et **sts**.
- La forêt **bts** sera composée de 2 arbres.
  - ▣ Le premier arbre composé :
    - Du domaine : **mozart** géré par les serveurs **vienne** et **valse** ;
    - Du sous-domaine : **vivaldi** géré par le serveur **saisons**.

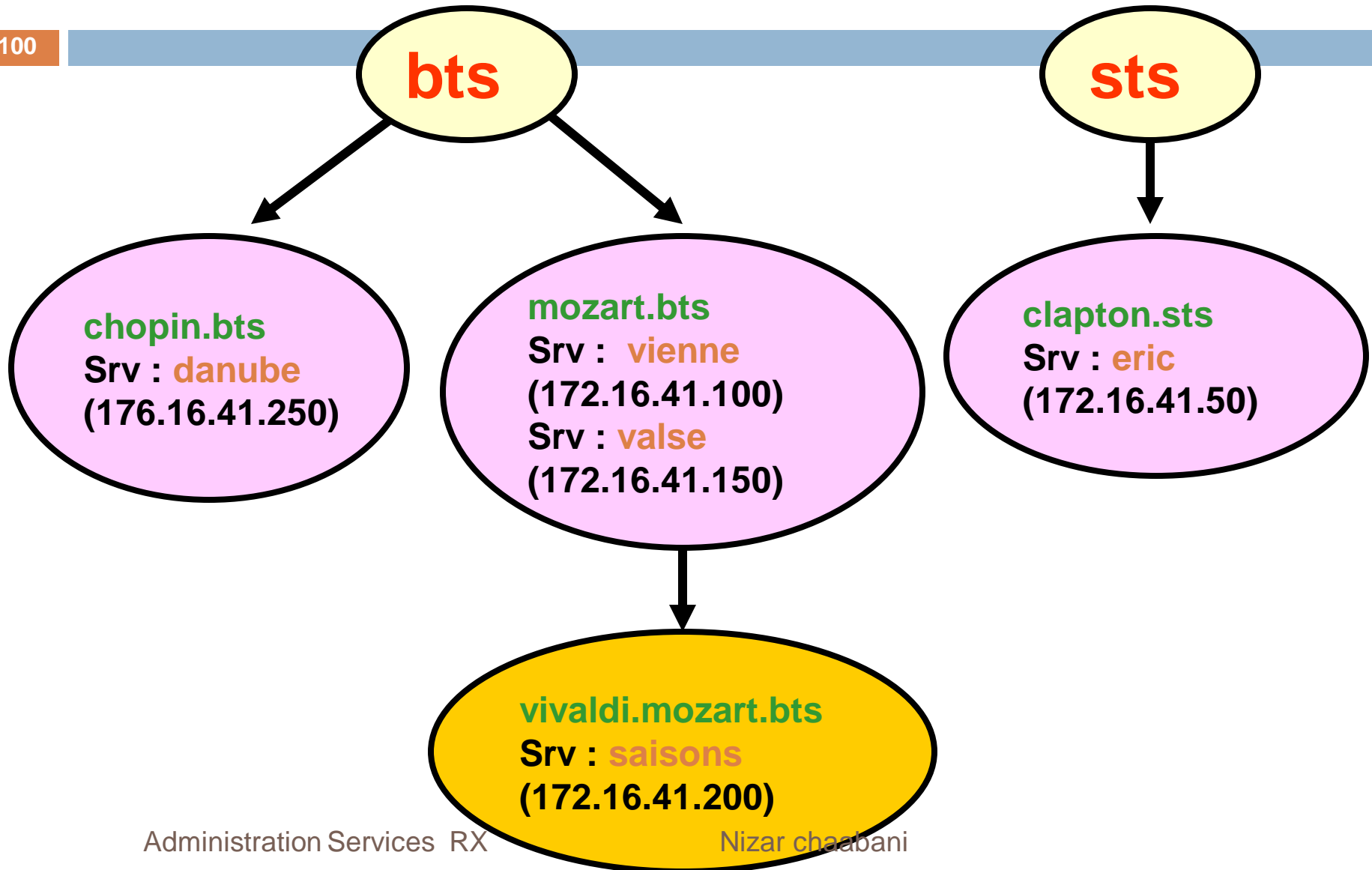
# Exemple de création d'une A.D

99

- La forêt **bts** sera composée de 2 arbres.
  - L'arbre (domaine) : *chopin* géré par le serveur *danube*.
- La forêt **sts** sera composée de l'arbre (domaine) : *clapton* géré par le serveur *eric*.

# Exemple de création d'une A.D

100



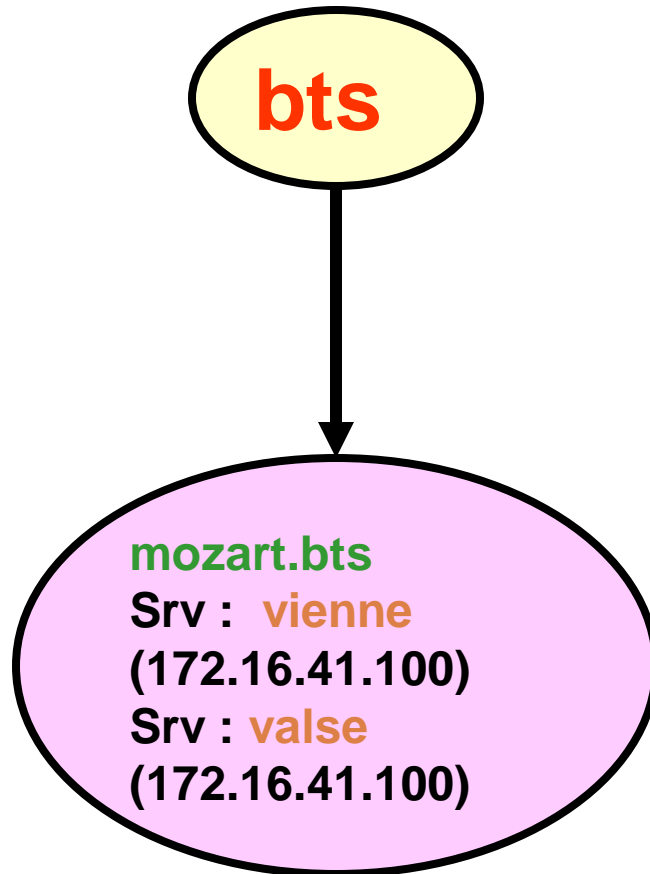
# Première étape (1)

101

## Installation de l'Active Directory sur le serveur VIENNE

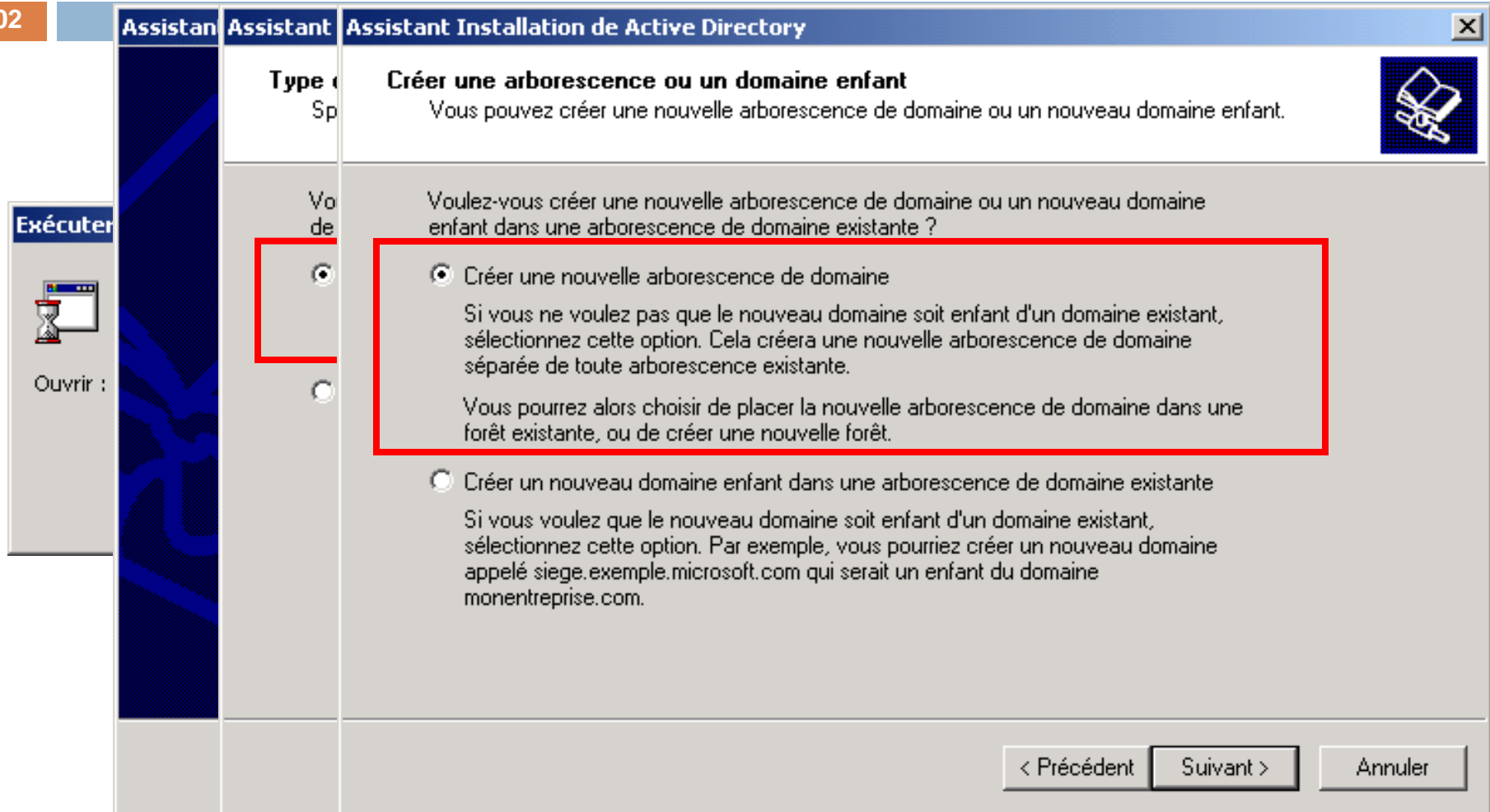
### Rappel :

Lors de la 1<sup>ère</sup> partie de l'installation du système, le futur serveur à été appelé : VIENNE



# Première étape (1)

102



# Première étape (1)

Assist	Assista	Assista	Assistan	Assistant Installation de Active Directory
Créer	Nouveau	Non	Empl	
			S	<b>Volume système partagé</b> Spécifiez quel dossier doit être partagé en tant que volume système.
			P	Le dossier Sysvol stocke la copie pour le serveur des fichiers publics du domaine. La
			d	liste du contenu du dossier Sysvol est répliquée vers tous les contrôleurs de domaine
			O	dans le domaine.
			E	Le dossier Sysvol doit être situé sur un volume NTFS 5.0.
			C	Entrez un emplacement pour le dossier Sysvol.
			O	Emplacement du dossier :
			E	<input type="text" value="C:\WINNT\SYSVOL"/> <input data-bbox="1406 748 1586 801" type="button" value="Parcourir..."/>
			C	
				<input data-bbox="1296 1148 1470 1196" type="button" value=" &lt; Précédent "/> <input data-bbox="1476 1148 1649 1196" type="button" value=" Suivant &gt; "/> <input data-bbox="1676 1148 1856 1196" type="button" value=" Annuler "/>

# Première étape (1)

104

**Assistant Installation de Active Directory**

**Configurer le mot de passe administrateur de Restauration des services d'annuaire**

Spécifiez un mot de passe d'administrateur à utiliser lors du démarrage de l'ordinateur en mode Restauration des services d'annuaire.

Entrez et confirmez le mot de passe que vous voulez attribuer au compte de l'administrateur de ce serveur, qui sera utilisé lorsque l'ordinateur sera démarré en mode Restauration des services d'annuaire.

Mot de passe :

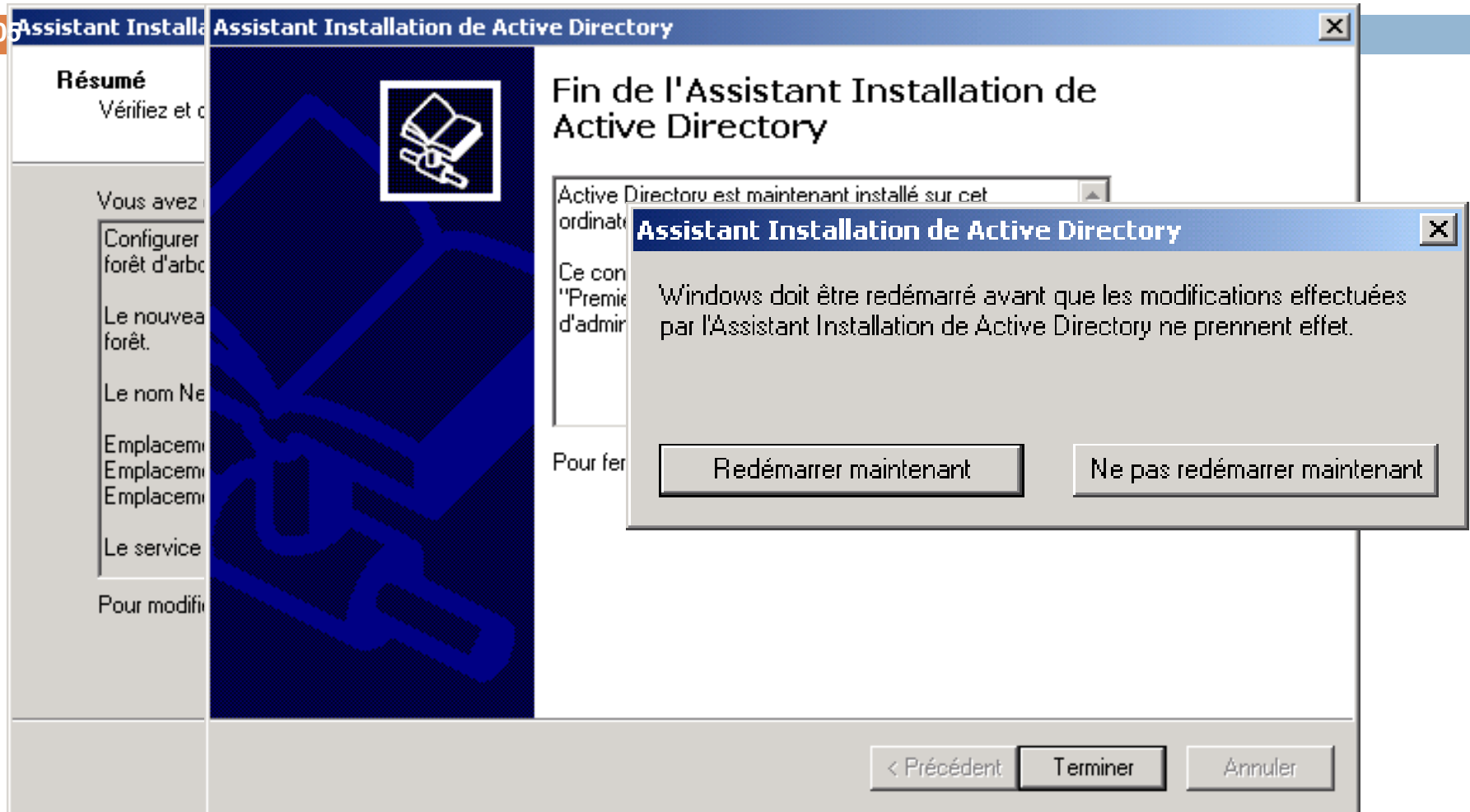
Confirmer le mot de passe :

< Précédent   Suivant >   Annuler



# Première étape (1)

105



# Première étape (1)

106

Favoris réseau

**Utilisateurs et ordinateurs Active Directory**

Console Fenêtre ?

Action Affichage

Arbre

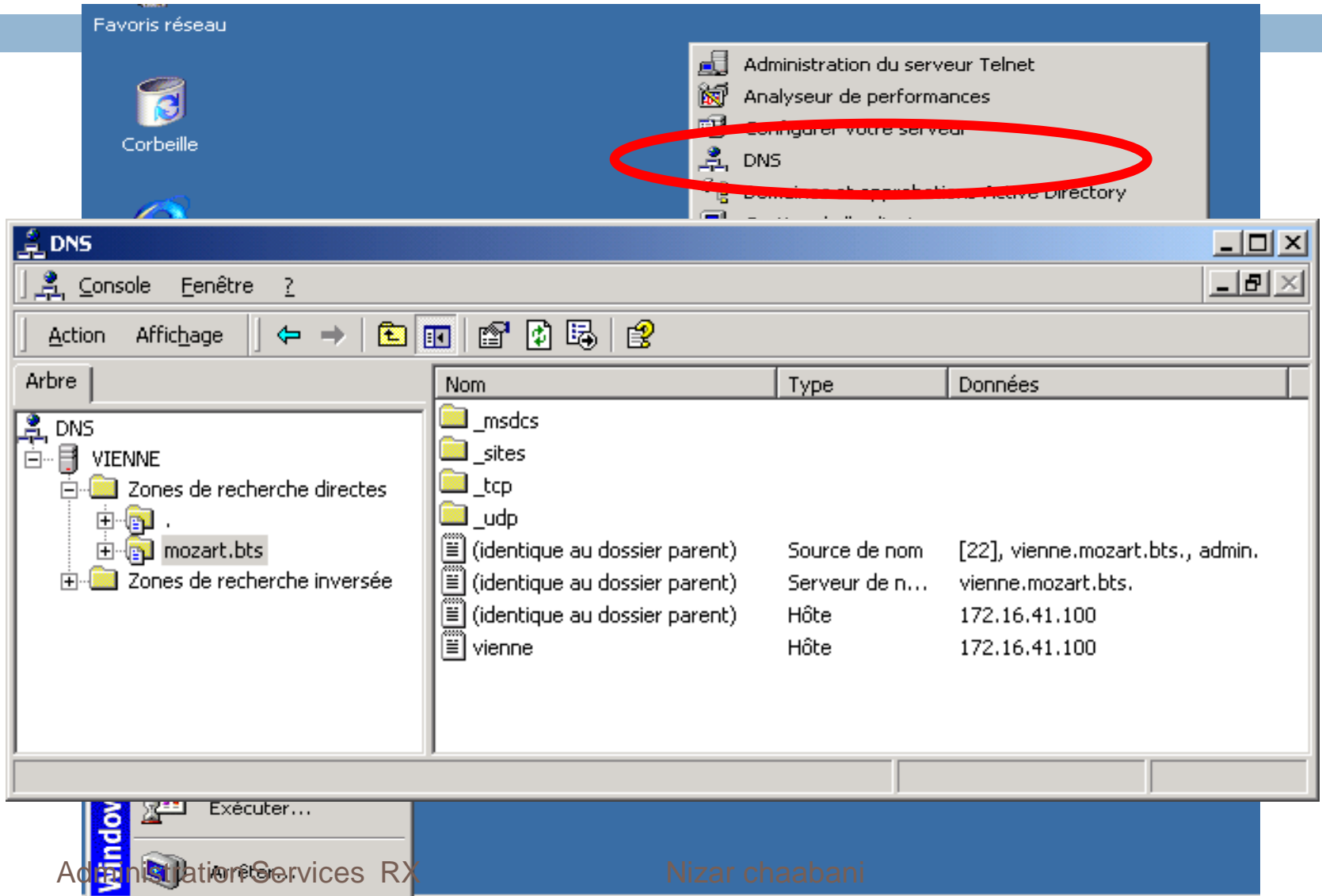
- Utilisateurs et ordinateurs Active Dire
  - mozart.bts
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Users

Users 16 objets

Nom	Type	Description
Administrateurs de l'entreprise	Groupe de sécurité - Global	Administrateurs
Administrateurs du schéma	Groupe de sécurité - Global	Administrateurs
Admins du domaine	Groupe de sécurité - Global	Administrateurs
Contrôleurs de domaine	Groupe de sécurité - Global	Tous les contrôl
DnsAdmins	Groupe de sécurité - Domaine local	Groupe des adm
DnsUpdateProxy	Groupe de sécurité - Global	Les clients DNS
Éditeurs de certificats	Groupe de sécurité - Global	Agents de certif
Invité	Utilisateur	Compte d'utilisa
Invités du domaine	Groupe de sécurité - Global	Tous les invités
krbtgt	Utilisateur	Compte de serv
LeChef	Utilisateur	Compte d'utilisa
Ordinateurs du domaine	Groupe de sécurité - Global	Toutes les statio
Propriétaires créateurs de la stratégie de groupe	Groupe de sécurité - Global	Les membres de
Serveurs RAS et IAS	Groupe de sécurité - Domaine local	Les serveurs de
TsInternetUser	Utilisateur	Ce compte utilis
Utilisa. du domaine	Groupe de sécurité - Global	Tous les utilisate

# Première étape (1)

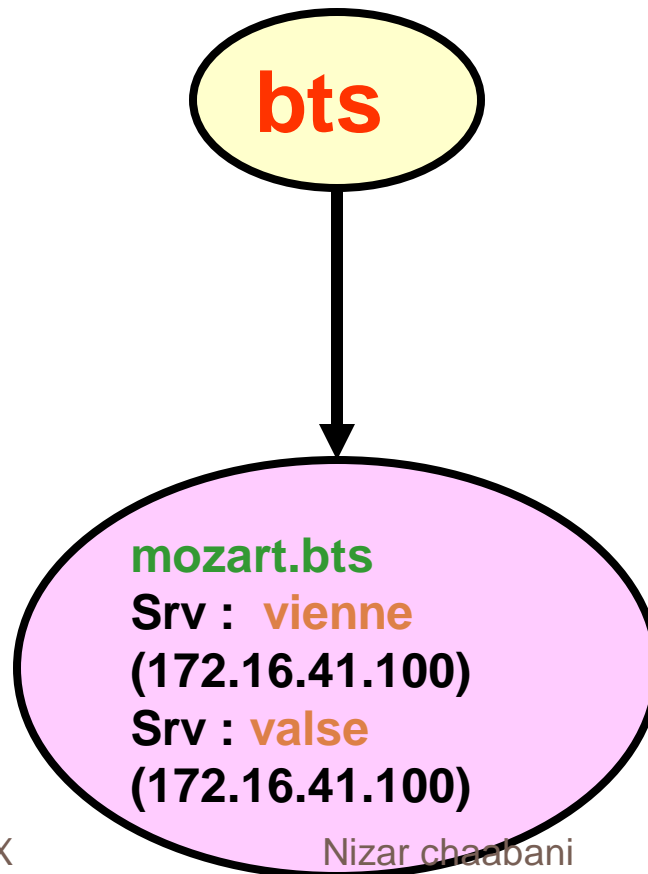
107



# Première étape (2)

108

## Installation d'un second serveur sur le domaine mozart.bts (serveur VALSE)



# Première étape (2)

109

**Configuration préalable :**  
**"Pointer" sur le serveur DNS qui gère l'Active Directory du domaine mozart.bts**

**Propriétés de Protocole Internet (TCP/IP)**

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 172 . 16 . 41 . 150

Masque de sous-réseau : 255 . 255 . 0 . 0

Passerelle par défaut : . . .

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 172 . 16 . 41 . 100

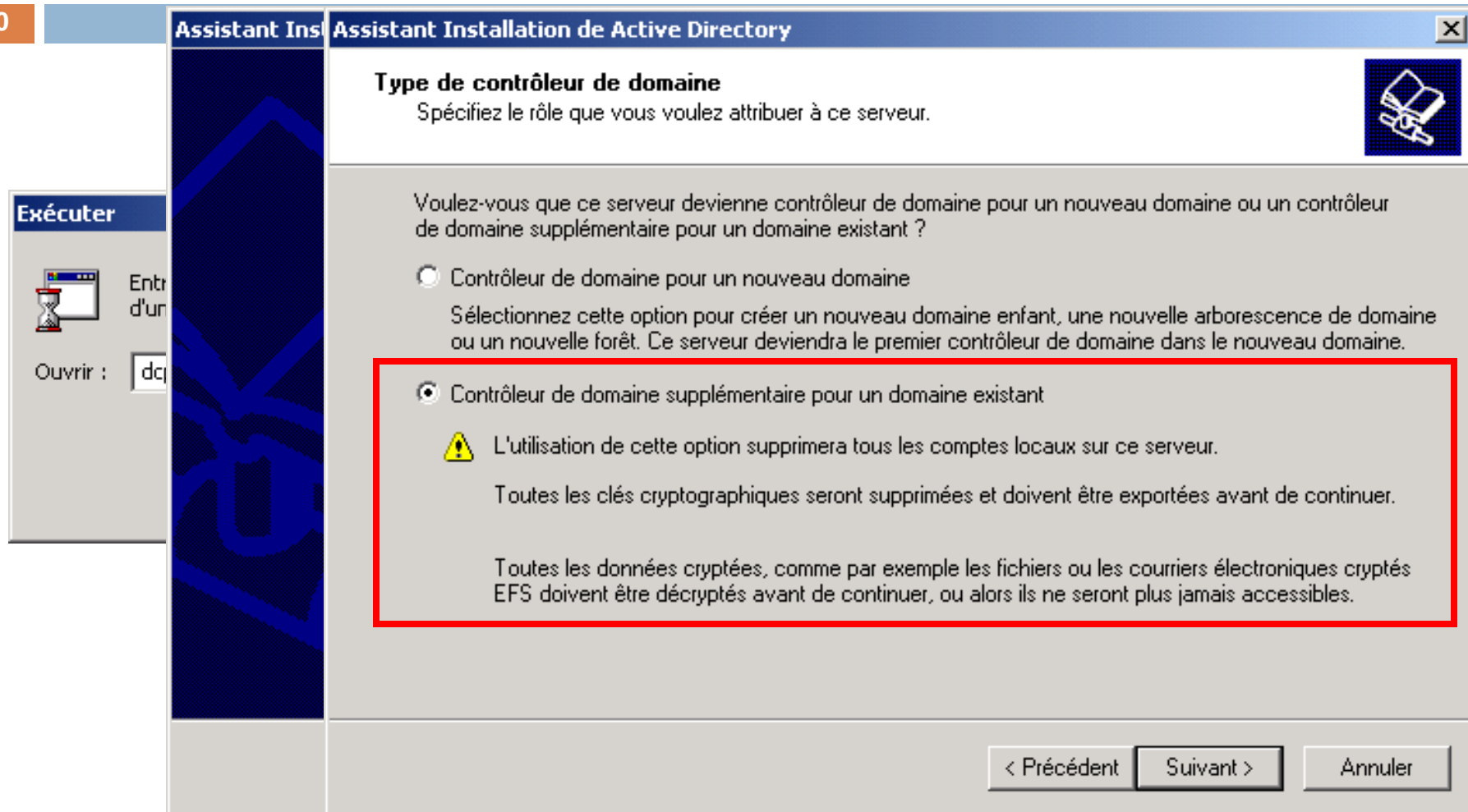
Serveur DNS auxiliaire : . . .

Avancé...

OK Annuler

# Première étape (2)

110



# Première étape (2)

11

Assista	Assistant	Assistant I	Assistant Installation de Active Directory
Info	Contrô Sp su	Emplac Spé	<b>Volume système partagé</b> Spécifiez quel dossier doit être partagé en tant que volume système.
	En co	Pou don	Le dossier Sysvol stocke la copie pour le serveur des fichiers publics du domaine. La liste du contenu du dossier Sysvol est répliquée vers tous les contrôleurs de domaine dans le domaine.
	Po	Où v	Le dossier Sysvol doit être situé sur un volume NTFS 5.0.
	No me	Emp C:\	Entrez un emplacement pour le dossier Sysvol.
		Où v	Emplacement du dossier : C:\WINNT\SYSVOL
		Emp C:\	Parcourir...
			< Précédent   Suivant >   Annuler

# Première étape (2)

112

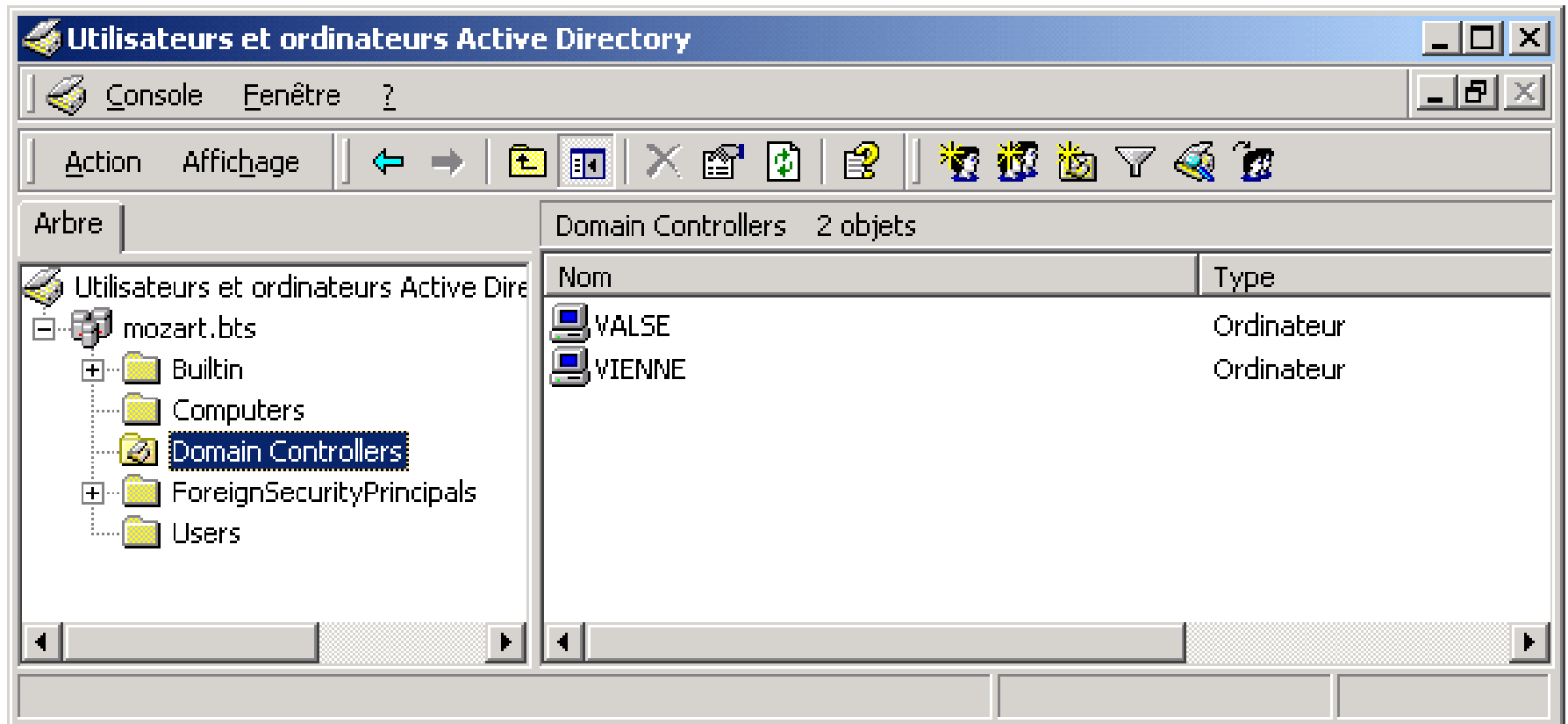




# Première étape (2)

113

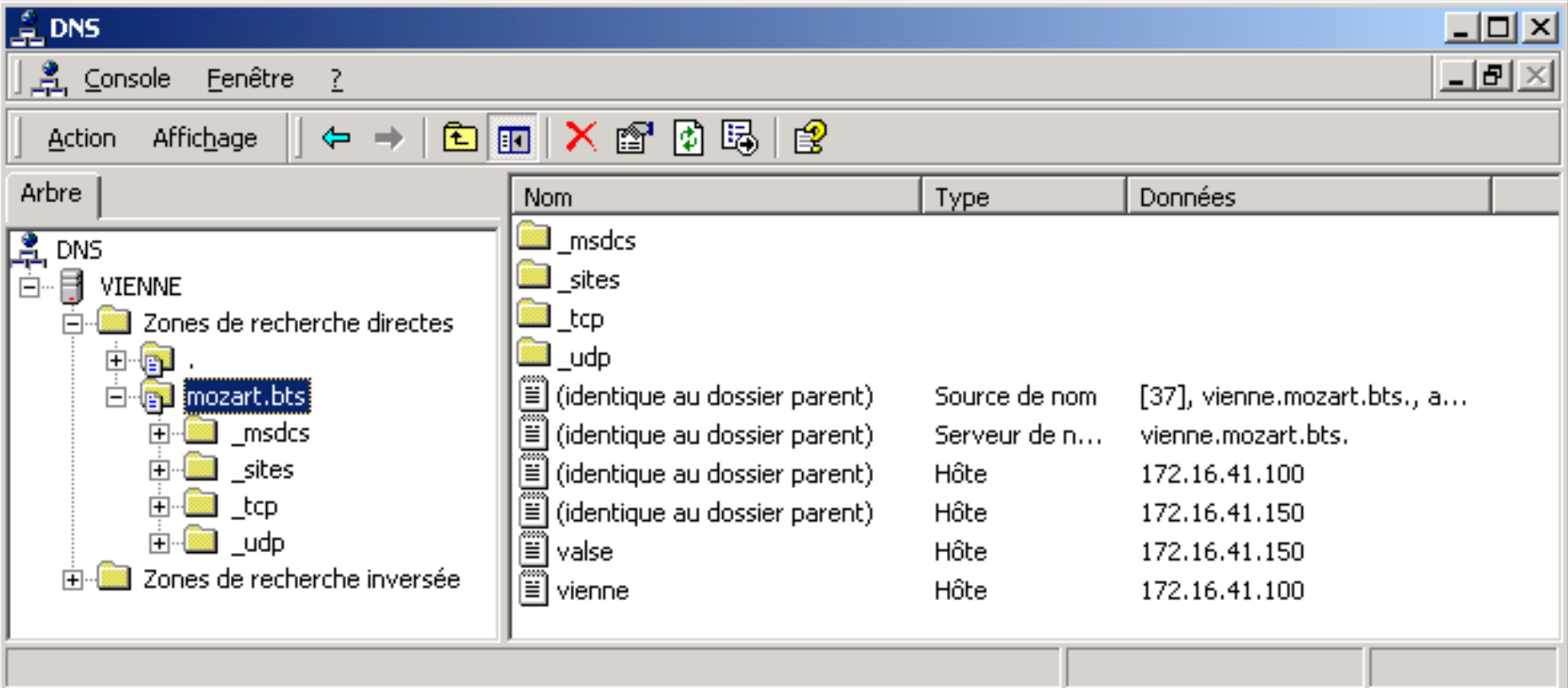
## Résultat dans l'Active Directory



# Première étape (2)

114

## Résultat dans le serveur DNS (VIENNE)



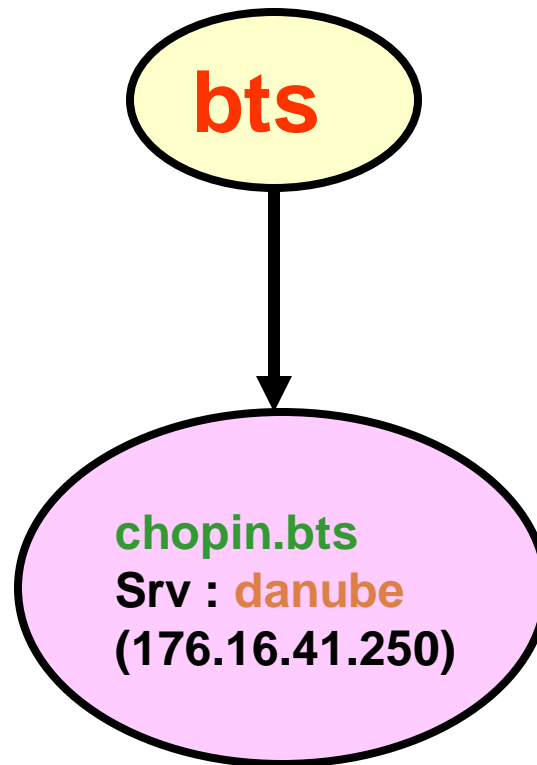
The screenshot displays the Windows DNS console. The left pane shows the tree structure of the DNS server 'VIENNE'. Under 'Zones de recherche directes', the zone 'mozart.bts' is selected. The right pane shows a list of records for this zone.

Nom	Type	Données
_msdcs		
_sites		
_tcp		
_udp		
(identique au dossier parent)	Source de nom	[37], vienne.mozart.bts., a...
(identique au dossier parent)	Serveur de n...	vienne.mozart.bts.
(identique au dossier parent)	Hôte	172.16.41.100
(identique au dossier parent)	Hôte	172.16.41.150
valse	Hôte	172.16.41.150
vienne	Hôte	172.16.41.100

# Deuxième étape

115

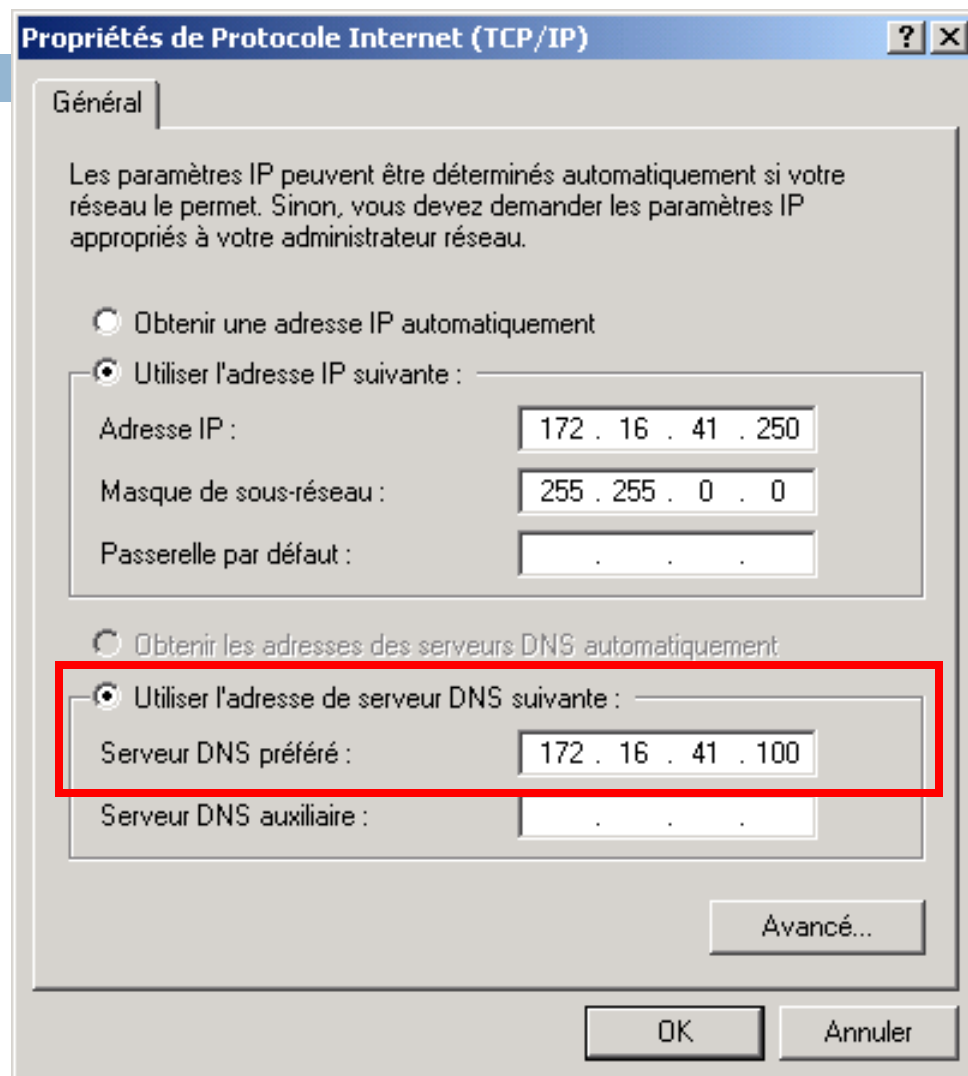
## Installation d'un second domaine : chopin.bts



# Deuxième étape

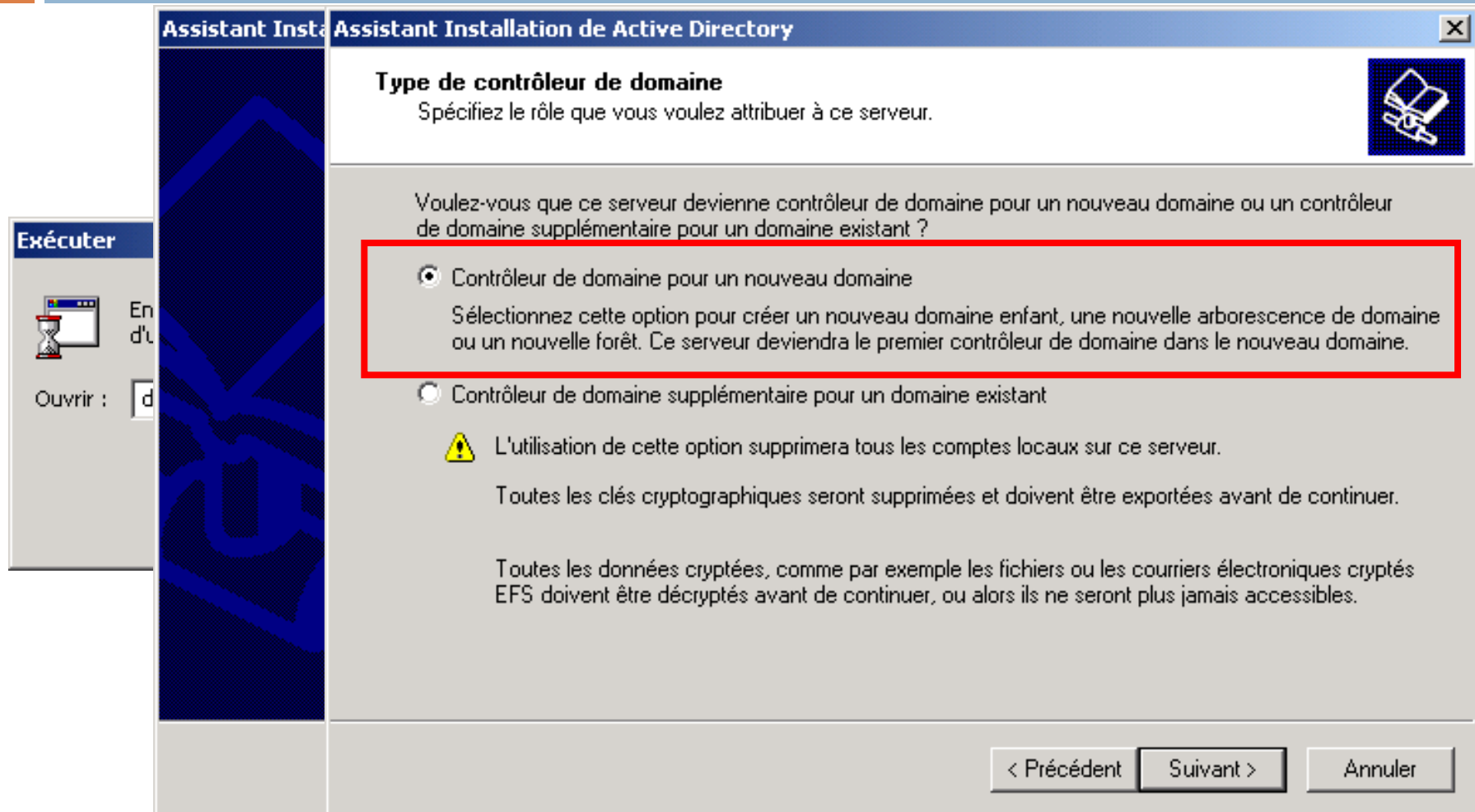
116

**Configuration préalable :**  
**"Pointer" sur le serveur DNS qui gère l'Active Directory du domaine mozart.bts, premier serveur ayant été installé.**

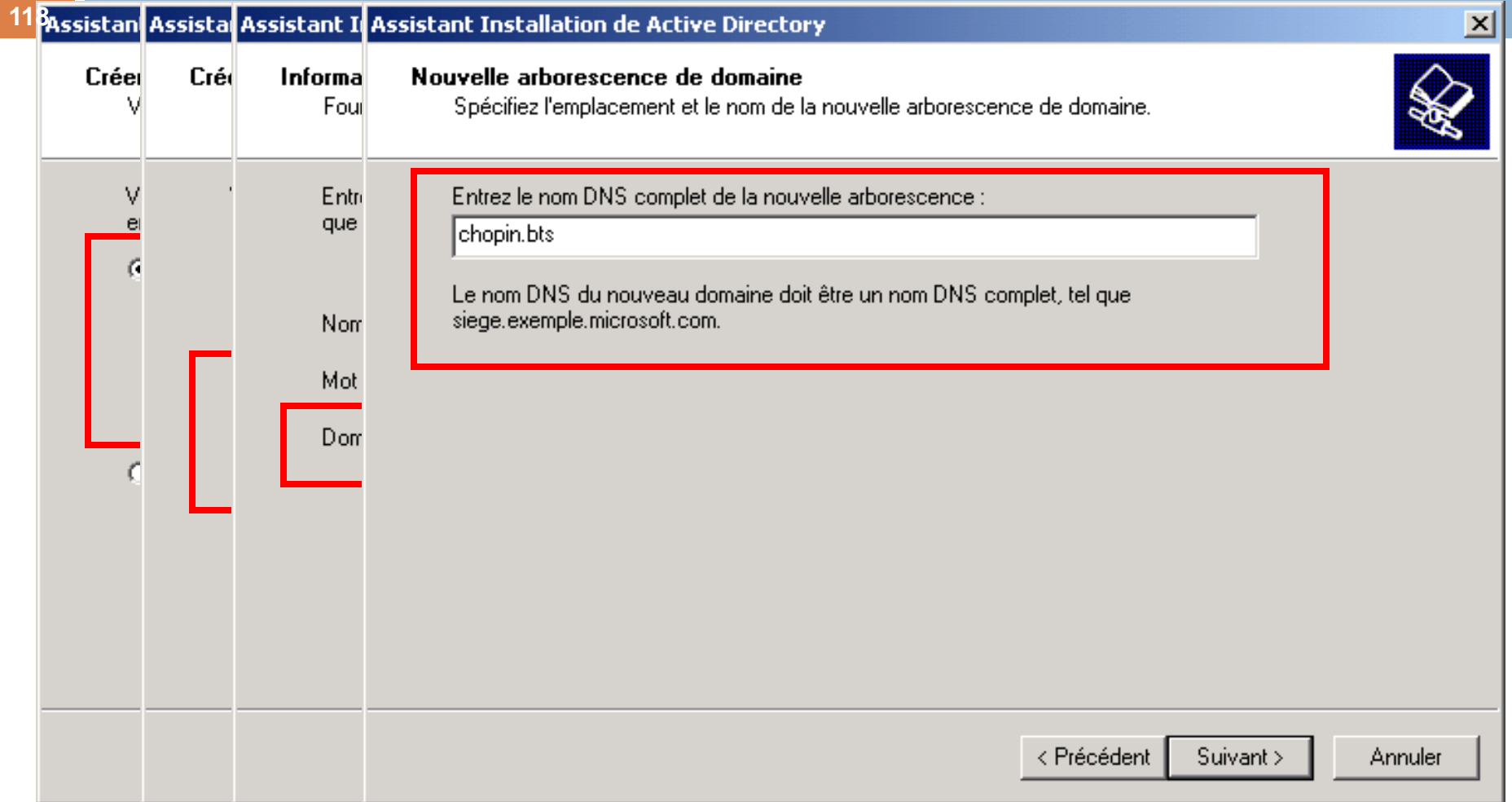


# Deuxième étape

117



## Deuxième étape



# Deuxième étape

119

Assist	Assista	Assistant In	Assistant Installation de Active Directory
No	Emp	Volume s Spéci	<b>Configurer le serveur DNS</b> L'Assistant peut configurer le serveur DNS de votre nouveau domaine.
		Le do liste d Assi	<div><p>Le service DNS n'est pas disponible. Voulez-vous que cet Assistant installe et configure un serveur DNS pour votre nouveau domaine ?</p><p><input checked="" type="radio"/> Oui, je veux installer et configurer le service DNS sur cet ordinateur (recommandé)</p><p><input type="radio"/> Non, j'installerai et je configurerai le service DNS moi-même</p></div>
			<div>&lt; Précédent   Suivant &gt;   Annuler</div>

## 12

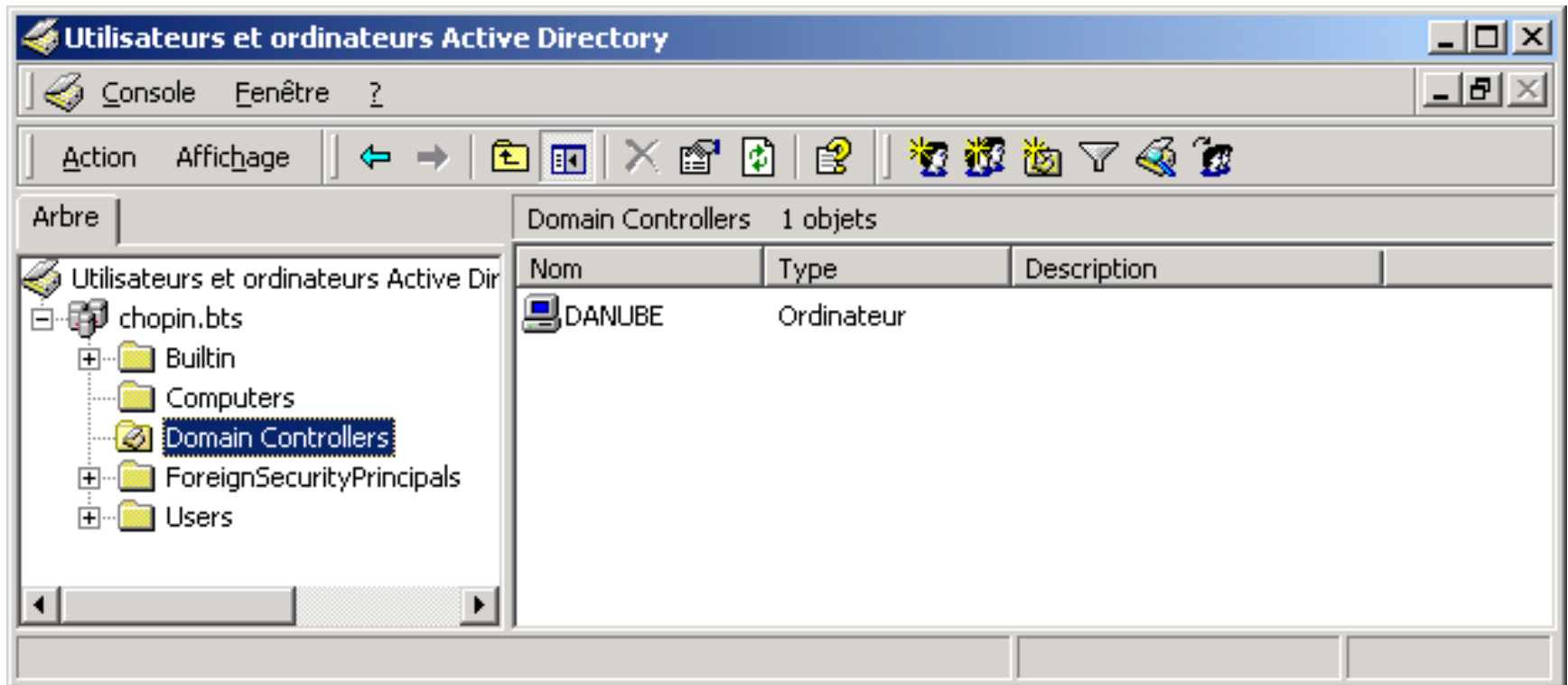




# Deuxième étape

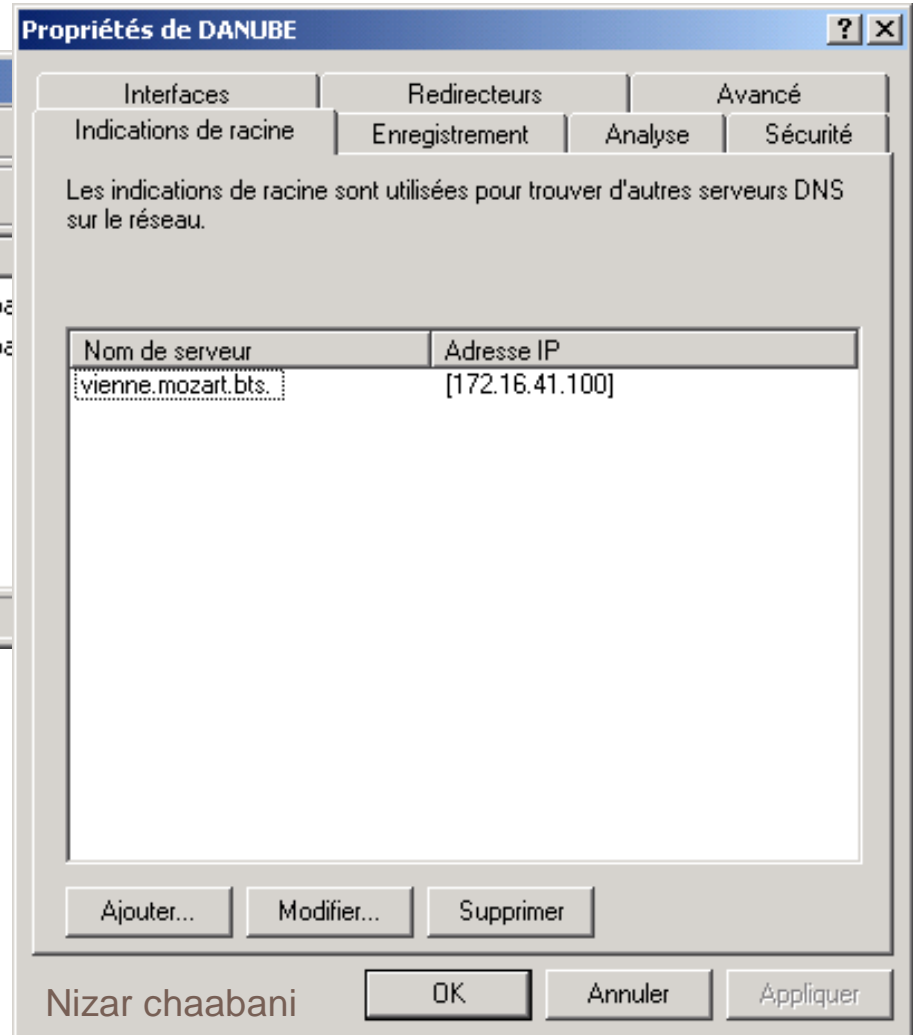
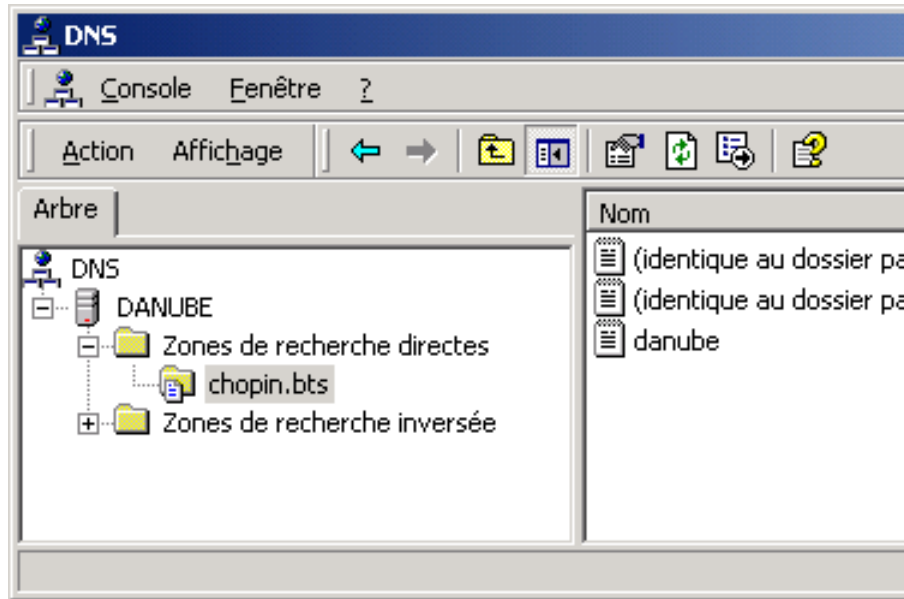
121

## Résultat dans l'Active Directory



# Deuxième étape

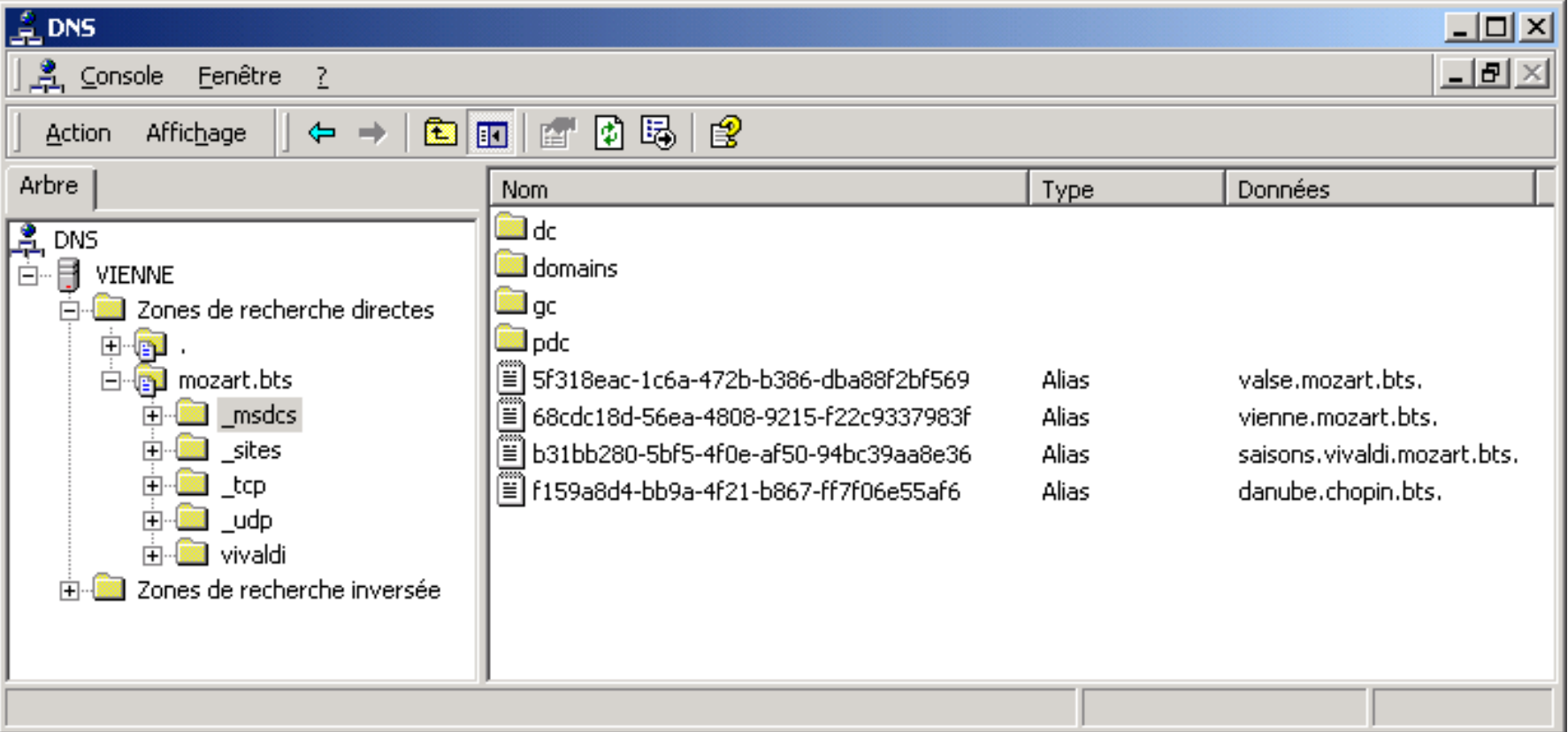
## 122 Résultat dans le serveur DNS (DANUBE)



# Deuxième étape

123

## Résultat dans le serveur DNS (VIENNE)



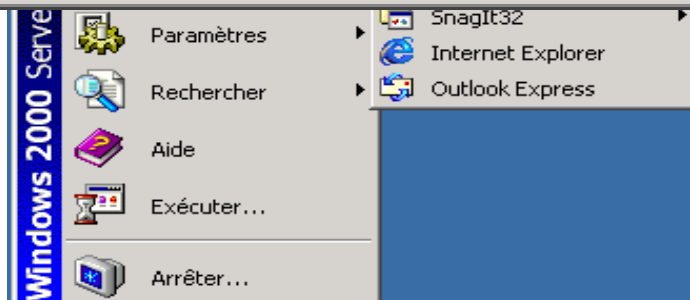
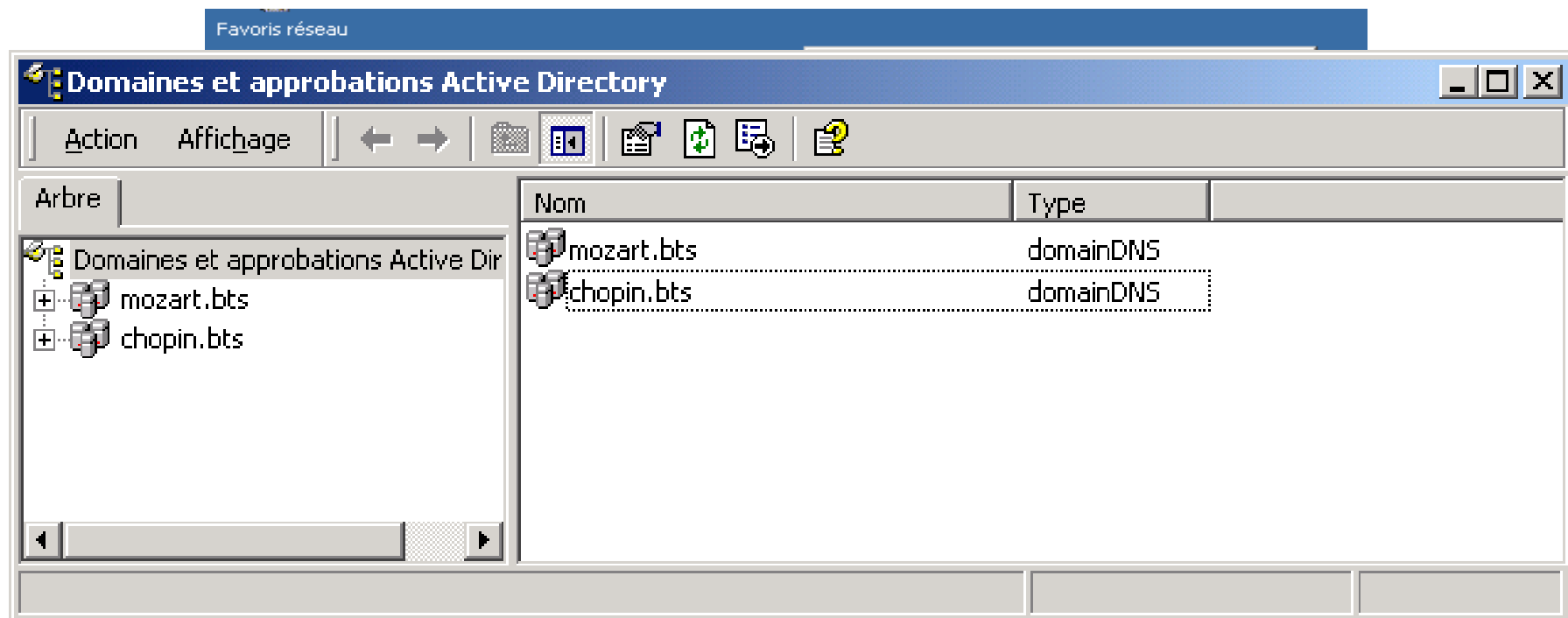
The screenshot displays the DNS console for the VIENNE server. The left pane shows the tree structure with 'Zones de recherche directes' expanded, showing 'mozart.bts' and its sub-zones. The right pane shows a list of records, including four Alias records with GUIDs and their corresponding target domain names.

Nom	Type	Données
dc		
domains		
gc		
pdc		
5f318eac-1c6a-472b-b386-dba88f2bf569	Alias	valse.mozart.bts.
68cdc18d-56ea-4808-9215-f22c9337983f	Alias	vienne.mozart.bts.
b31bb280-5bf5-4f0e-af50-94bc39aa8e36	Alias	saisons.vivaldi.mozart.bts.
f159a8d4-bb9a-4f21-b867-ff7f06e55af6	Alias	danube.chopin.bts.

# Deuxième étape

## Relations d'approbations entre les domaines

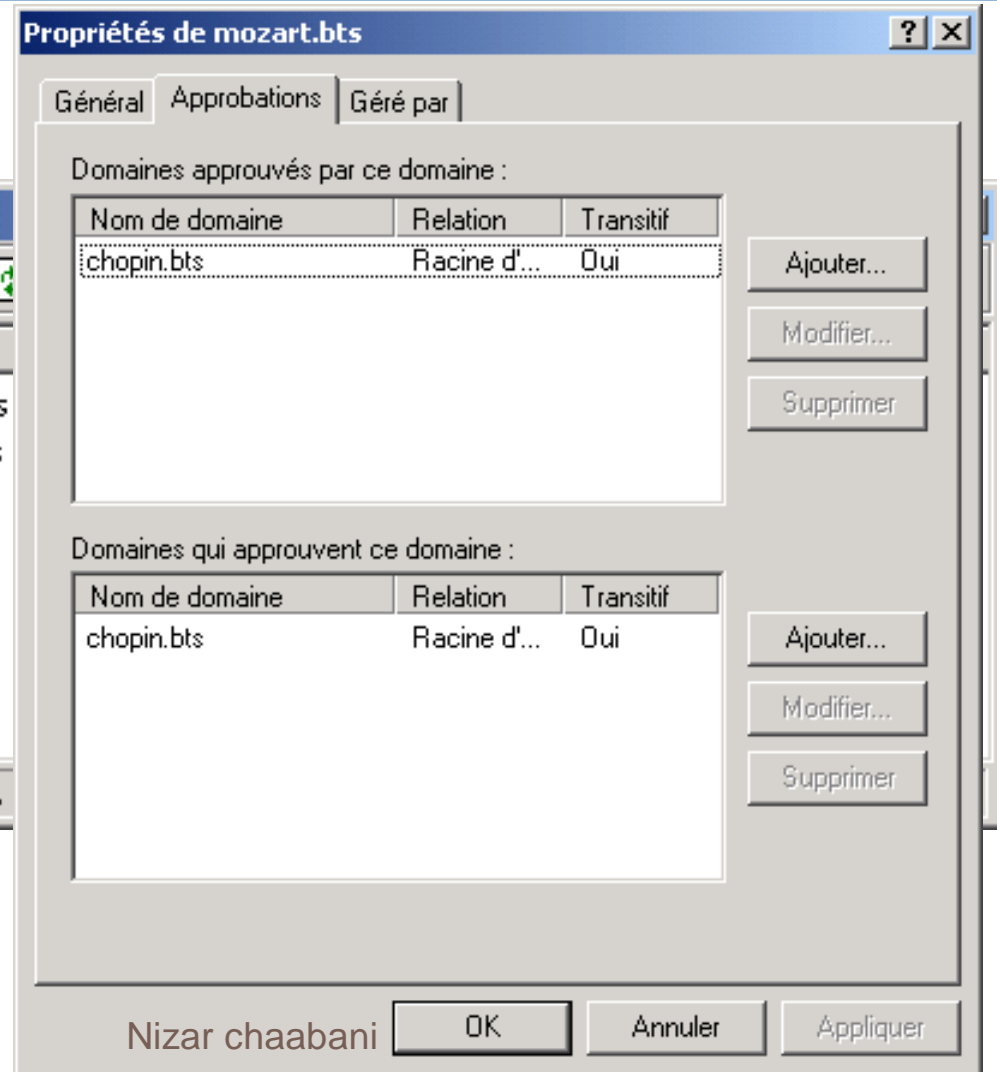
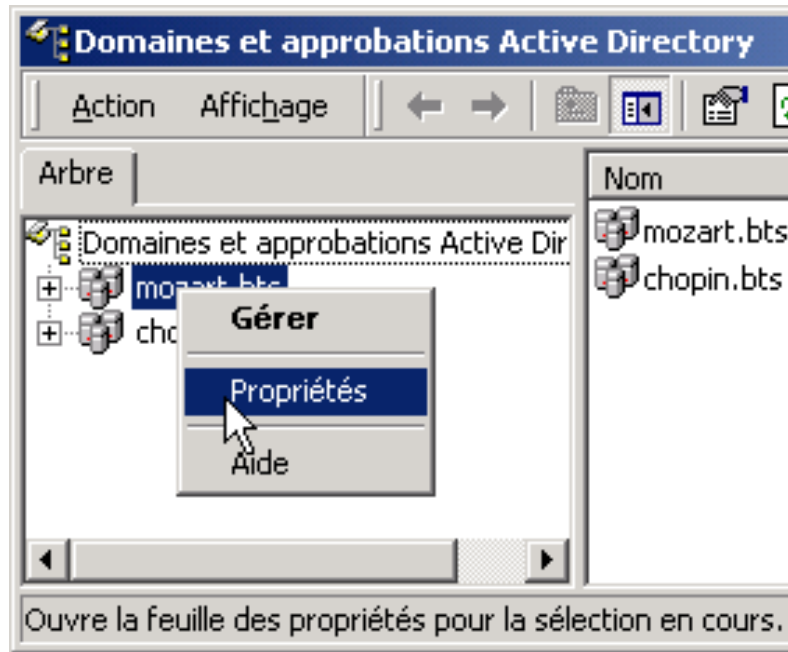
124



# Deuxième étape

## Relations d'approbations entre les domaines

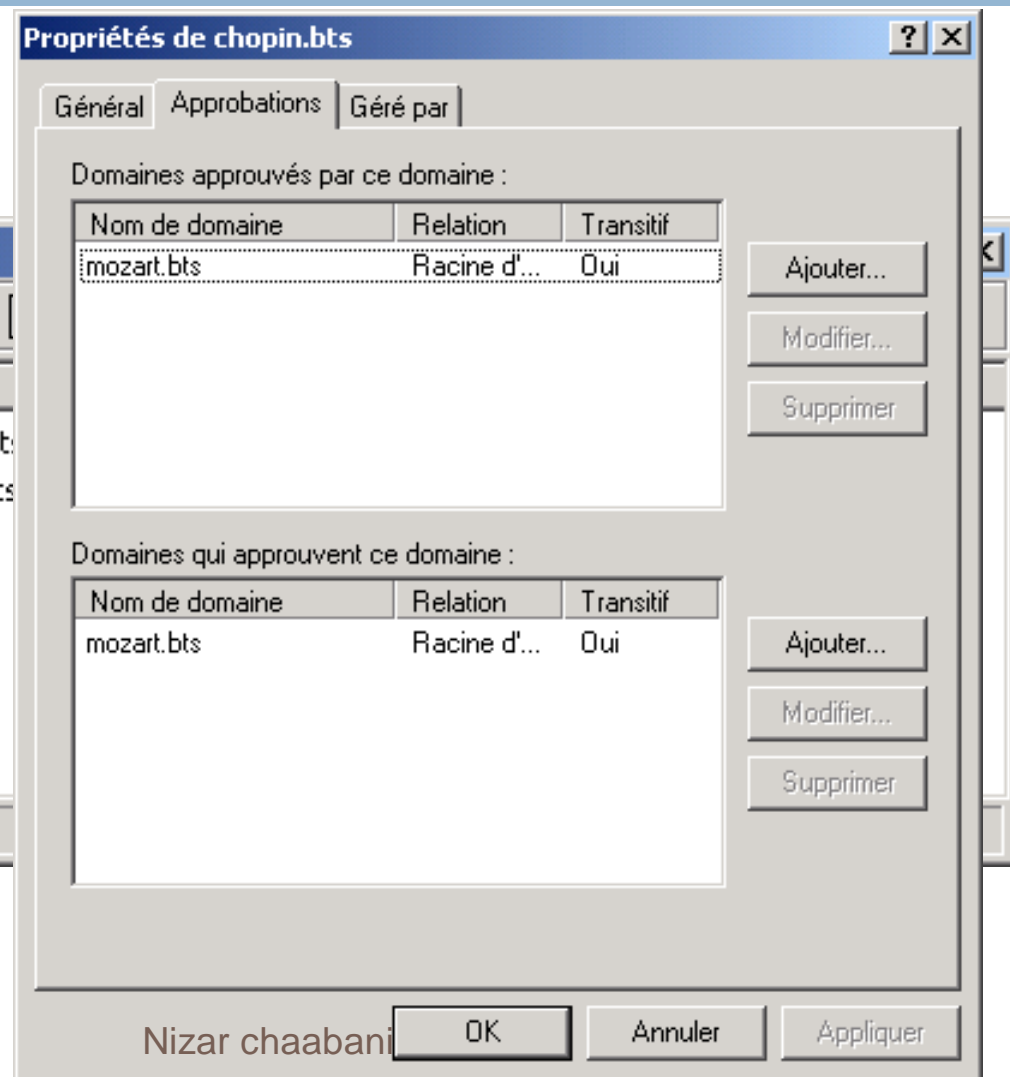
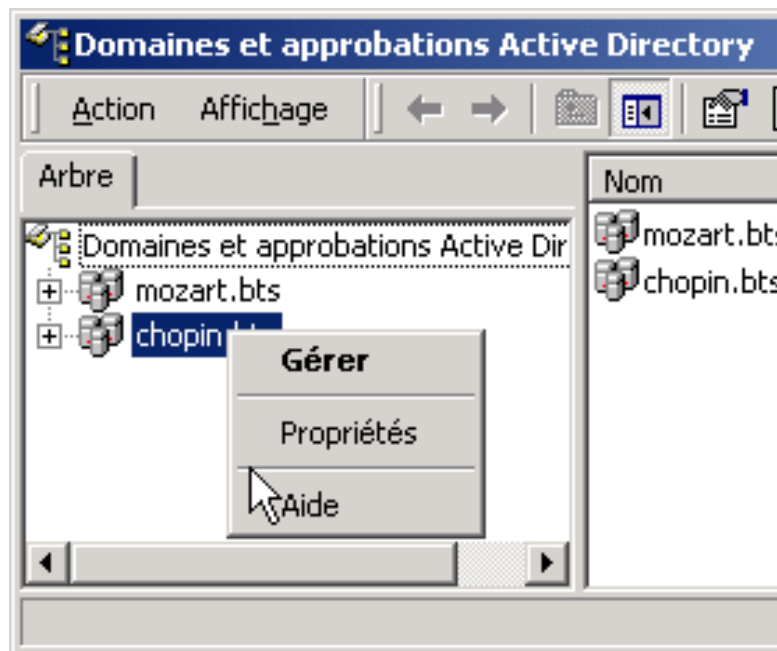
125



# Deuxième étape

## Relations d'approbations entre les domaines

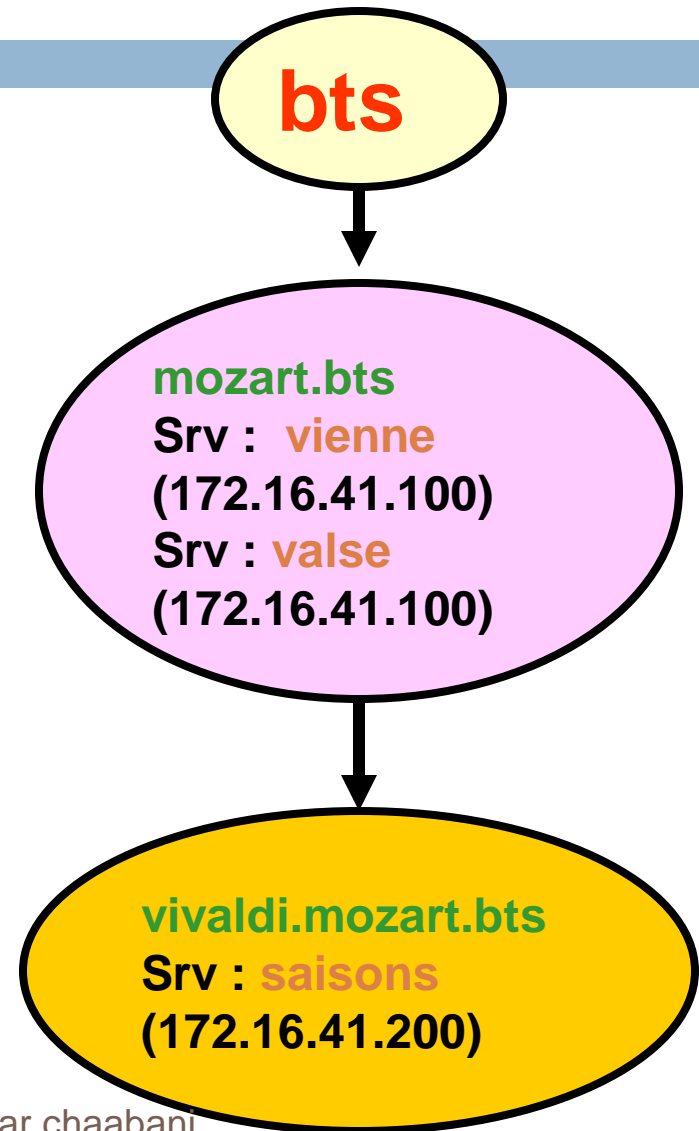
126



# Troisième étape

127

Création du sous-domaine vivaldi



# Troisième étape

128

**Configuration préalable :**  
**"Pointer" sur le serveur DNS qui gère l'Active Directory du domaine moztart.bts, premier serveur ayant été installé.**

Propriétés de Protocole Internet (TCP/IP)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 172 . 16 . 41 . 200

Masque de sous-réseau : 255 . 255 . 0 . 0

Passerelle par défaut : . . .

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 172 . 16 . 41 . 100

Serveur DNS auxiliaire : . . .

Avancé...

OK Annuler



# Troisième étape

129

**Assistant Installation de Active Directory**

**Informations d'identification réseau**  
Fournissez un nom d'utilisateur réseau et un mot de passe.

Entrez le nom d'utilisateur, le mot de passe et le domaine d'utilisateur du compte réseau que vous souhaitez utiliser pour cette opération.

Nom d'utilisateur :


Mot de passe :

Domaine :

< Précédent   Suivant >   Annuler

# Troisième étape

130

Assist	Assista	Assist	Assista	Assistant Installation de Active Directory
Ins	Non	Err	Vok	
				<b>Autorisations</b> Sélectionnez les autorisations par défaut pour les objets Utilisateurs et Groupes.  Certains programmes serveur, tels que le service d'accès distant Windows NT, lisent des informations stockées sur les contrôleurs de domaine.  <input type="radio"/> Autorisations compatibles avec les serveurs de versions antérieures à Windows 2000 Sélectionnez cette option si vous exécutez des programmes serveur sur des serveurs de versions antérieures à Windows 2000 ou sur des serveurs Windows 2000 membres de domaines de versions antérieures à Windows 2000.   Les utilisateurs anonymes peuvent lire les informations sur ce domaine.  <input checked="" type="radio"/> <b>Autorisations compatibles uniquement avec les serveurs Windows 2000</b> Sélectionnez cette option si vous n'exécutez des programmes serveur que sur des serveurs Windows 2000 membres de domaines Windows 2000. Seuls les utilisateurs authentifiés peuvent lire les informations sur ce domaine.
				<div>&lt; Précédent</div> <div>Suivant &gt;</div> <div>Annuler</div>

# Troisième étape

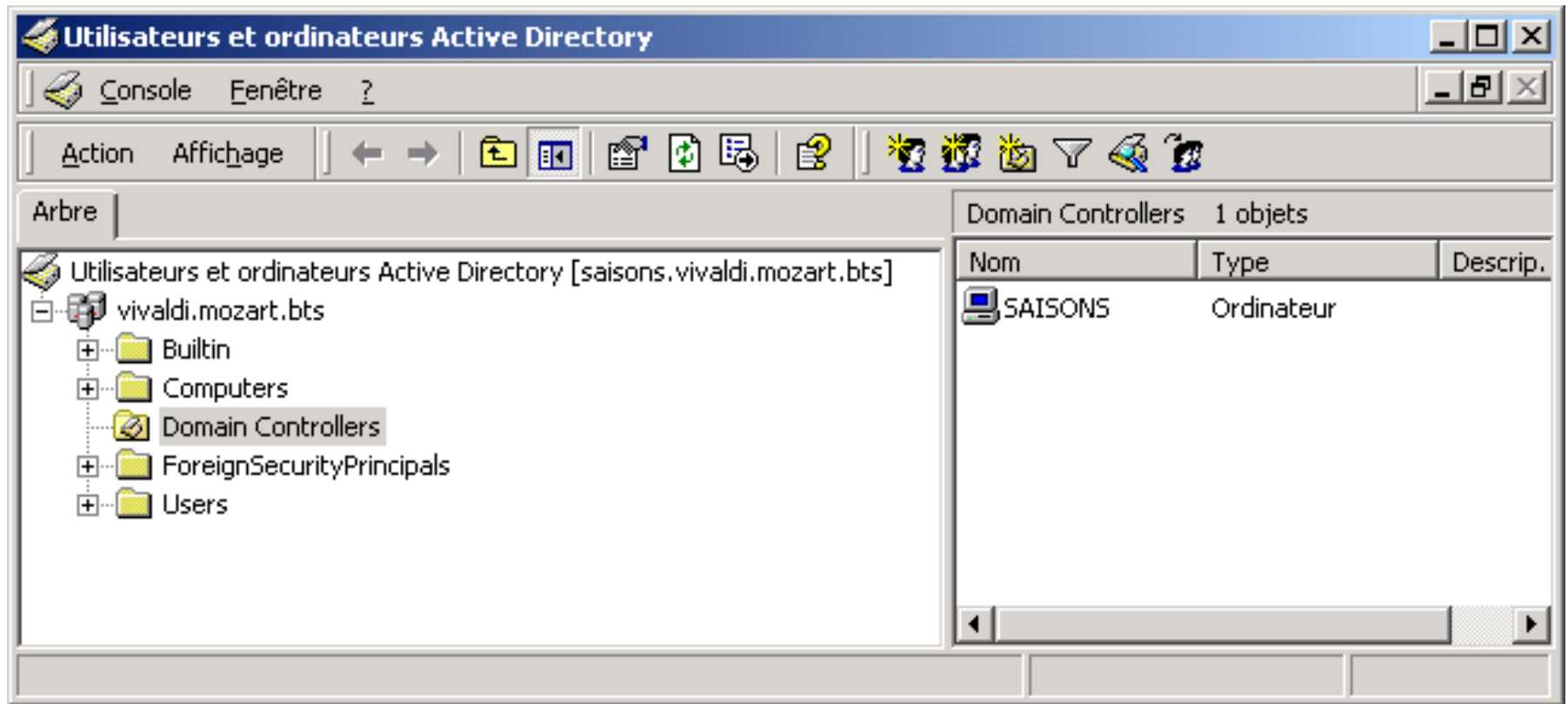
134



# Troisième étape

132

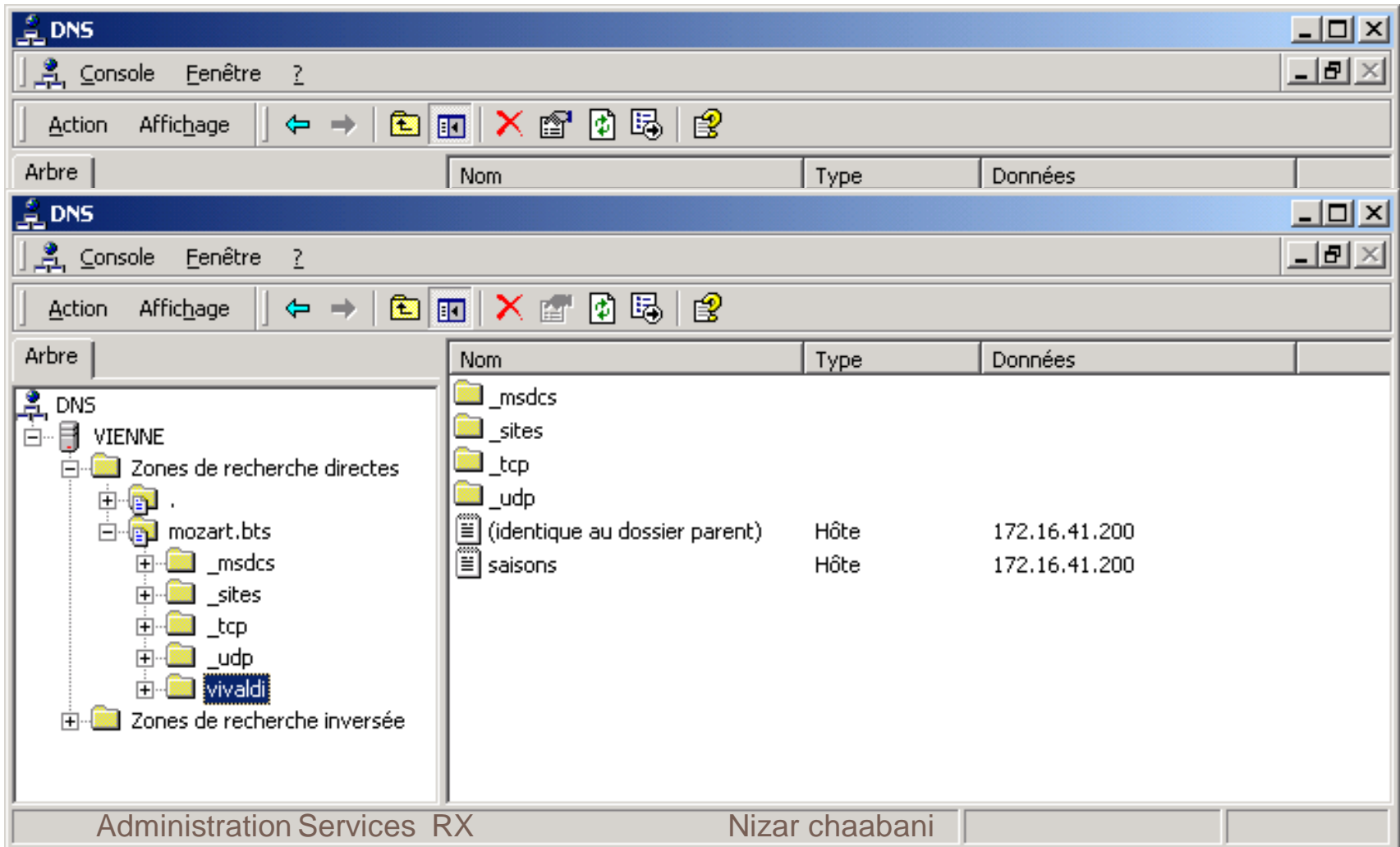
## Résultat dans l'Active Directory



# Troisième étape

133

## Résultat dans le serveur DNS (VIENNE)



The screenshot displays the DNS console interface. The left pane shows the tree structure of the DNS configuration for the VIENNE server. The right pane shows a list of records.

**Tree Structure (Left Pane):**

- DNS
  - VIENNE
    - Zones de recherche directes
      - .
        - mozart.bts
          - \_msdcs
          - \_sites
          - \_tcp
          - \_udp
          - vivaldi
    - Zones de recherche inversée

**Records List (Right Pane):**

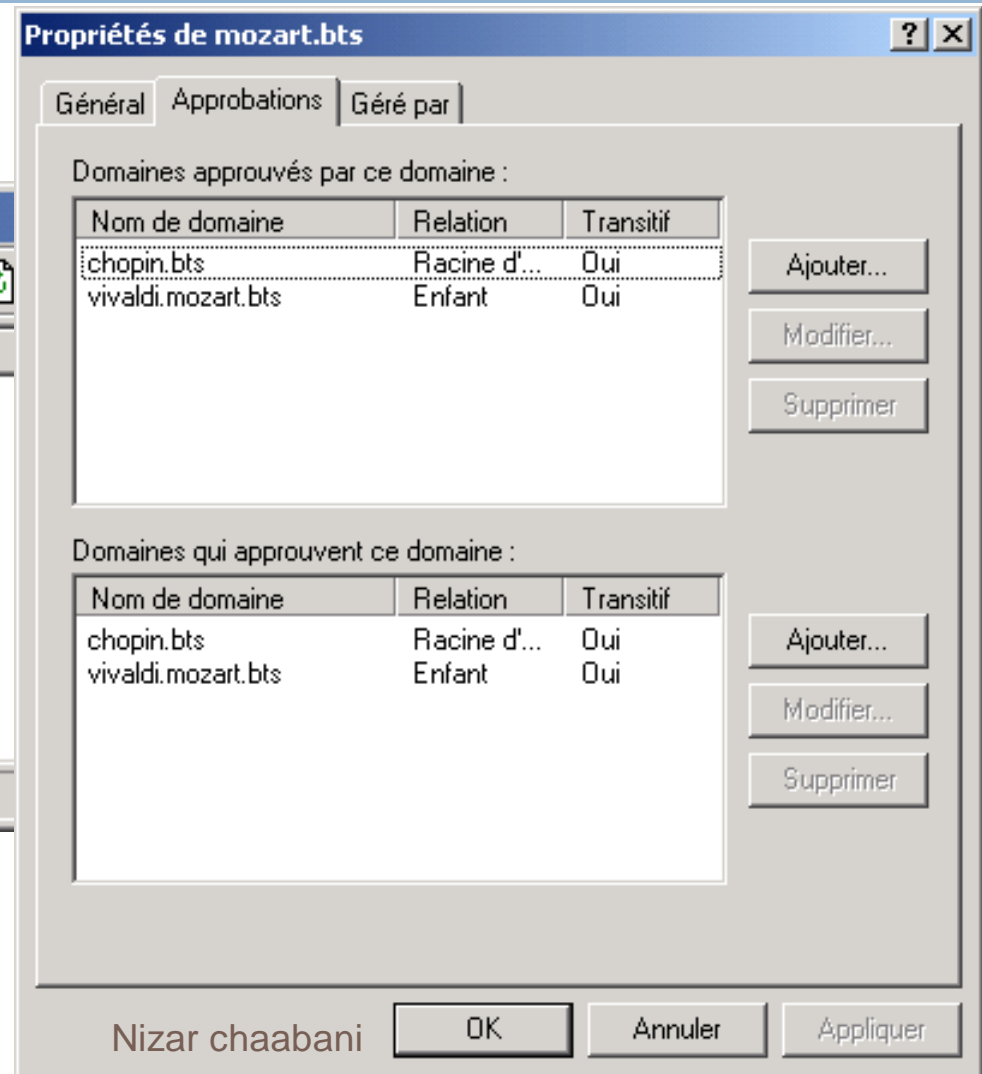
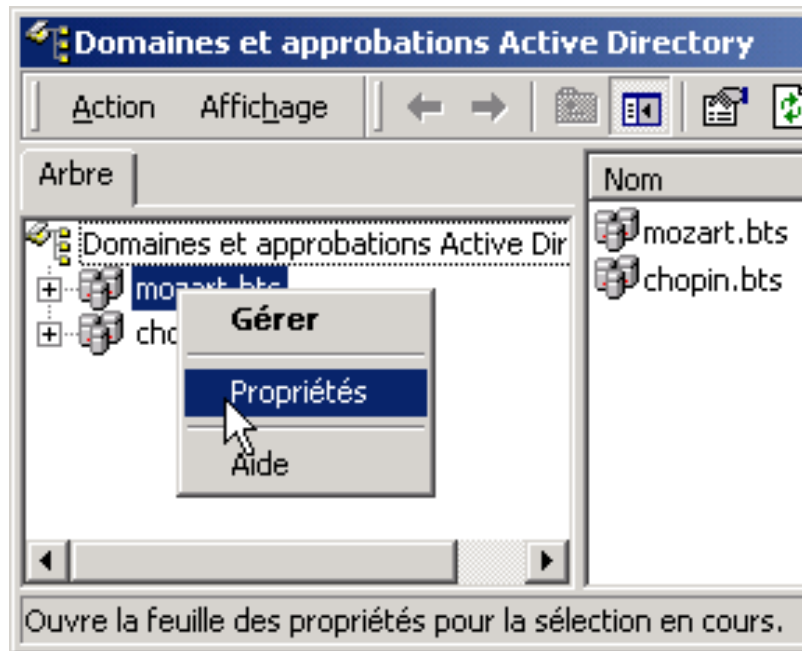
Nom	Type	Données
_msdcs		
_sites		
_tcp		
_udp		
(identique au dossier parent)	Hôte	172.16.41.200
saisons	Hôte	172.16.41.200

Administration Services RX Nizar chaabani

# Troisième étape

## Relations d'approbations entre les domaines

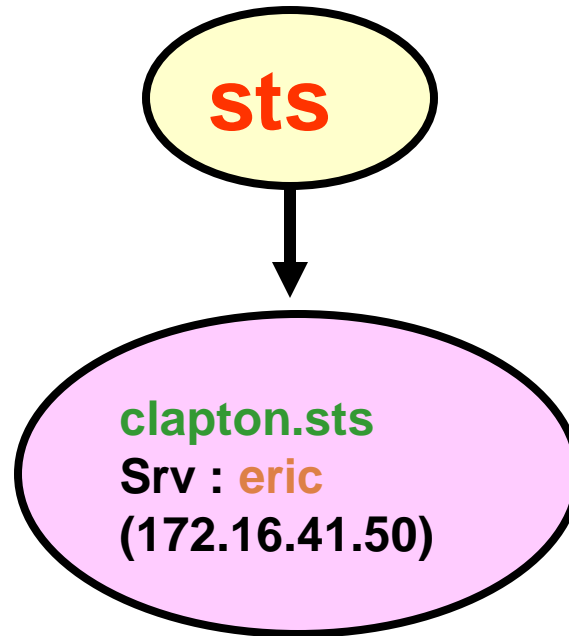
134



# Quatrième étape

135

Création de l'arborescence "sts"  
et du domaine "clapton.sts"



# Quatrième étape

136

Assista Assistant Ins Assistant Installation de Active Directory

Type de c  
Spécifi

Créer une arborescence ou un domaine enfant  
Vous pouvez créer une nouvelle arborescence de domaine ou un nouveau domaine enfant.

Voulez-vous créer une nouvelle arborescence de domaine ou un nouveau domaine enfant dans une arborescence de domaine existante ?

☒ Créer une nouvelle arborescence de domaine  
Si vous ne voulez pas que le nouveau domaine soit enfant d'un domaine existant, sélectionnez cette option. Cela créera une nouvelle arborescence de domaine séparée de toute arborescence existante.  
Vous pourrez alors choisir de placer la nouvelle arborescence de domaine dans une forêt existante, ou de créer une nouvelle forêt.

☐ Créer un nouveau domaine enfant dans une arborescence de domaine existante  
Si vous voulez que le nouveau domaine soit enfant d'un domaine existant, sélectionnez cette option. Par exemple, vous pourriez créer un nouveau domaine appelé `siège.exemple.microsoft.com` qui serait un enfant du domaine `monentreprise.com`.

< Précédent Suivant > Annuler



# Quatrième étape

137

Assistant	Assistant	Assistant I	Assistant Installation de Active Directory
Créer	Nouv	Nom de	<b>Emplacement de la base de données et du journal</b> Spécifiez les emplacements de la base de données et du journal Active Directory.
S	S	Spé	
V	E	Ceci	Pour de meilleures performances et une meilleure récupération, stockez la base de données et le journal sur des disques durs distincts.
G	S	iden	Où voulez-vous stocker la base de données Active Directory ?
	a	entre	Emplacement de la base de données :
	N	Nom	<input type="text" value="C:\WINNT\NTDS"/> <input data-bbox="1406 691 1586 743" type="button" value="Parcourir..."/>
	c		
			Où voulez-vous stocker le journal Active Directory ?
			Emplacement du journal :
			<input type="text" value="C:\WINNT\NTDS"/> <input data-bbox="1406 882 1586 935" type="button" value="Parcourir..."/>
			<input data-bbox="1296 1182 1476 1235" type="button" value=" &lt; Précédent "/> <input data-bbox="1476 1182 1655 1235" type="button" value=" Suivant &gt; "/> <input data-bbox="1682 1182 1862 1235" type="button" value=" Annuler "/>

# Quatrième étape


138

**Assistant Installation de Active Directory**

**Autorisations**  
Sélectionnez les autorisations par défaut pour les objets Utilisateurs et Groupes.

Certains programmes serveur, tels que le service d'accès distant Windows NT, lisent des informations stockées sur les contrôleurs de domaine.

☒ Autorisations compatibles avec les serveurs de versions antérieures à Windows 2000  
Sélectionnez cette option si vous exécutez des programmes serveur sur des serveurs de versions antérieures à Windows 2000 ou sur des serveurs Windows 2000 membres de domaines de versions antérieures à Windows 2000.

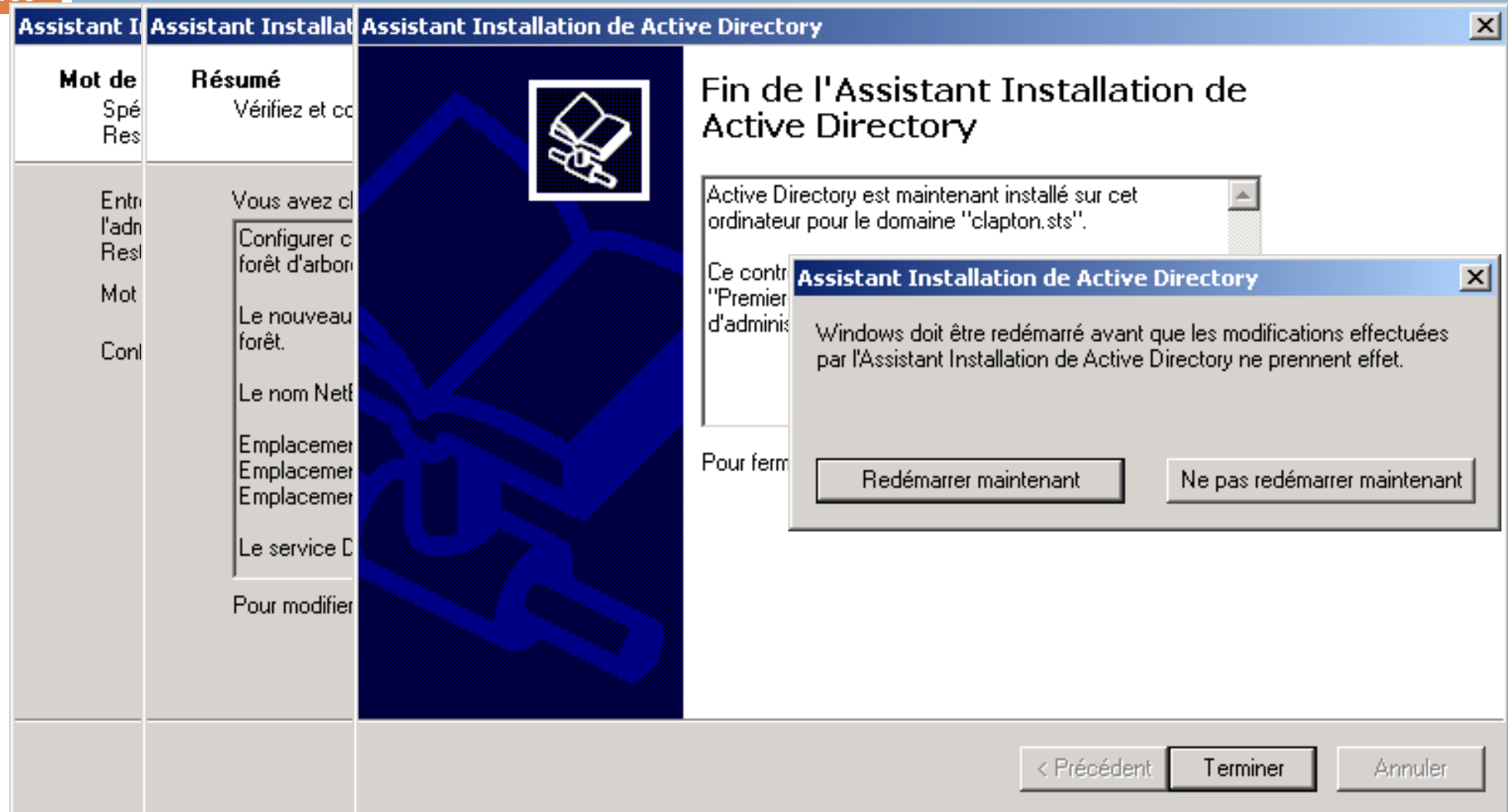
 Les utilisateurs anonymes peuvent lire les informations sur ce domaine.

☒ Autorisations compatibles uniquement avec les serveurs Windows 2000  
Sélectionnez cette option si vous n'exécutez des programmes serveur que sur des serveurs Windows 2000 membres de domaines Windows 2000. Seuls les utilisateurs authentifiés peuvent lire les informations sur ce domaine.

< Précédent   Suivant >   Annuler

# Quatrième étape

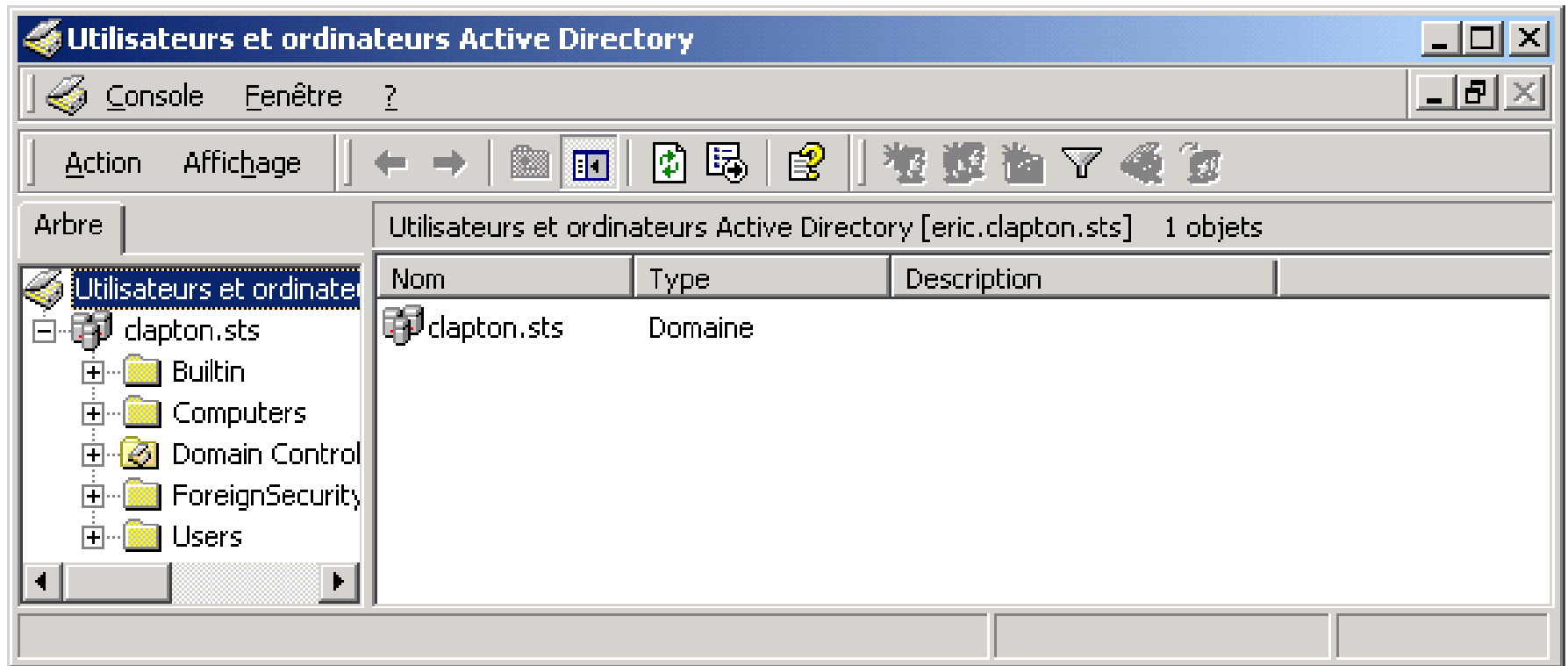
139



# Quatrième étape

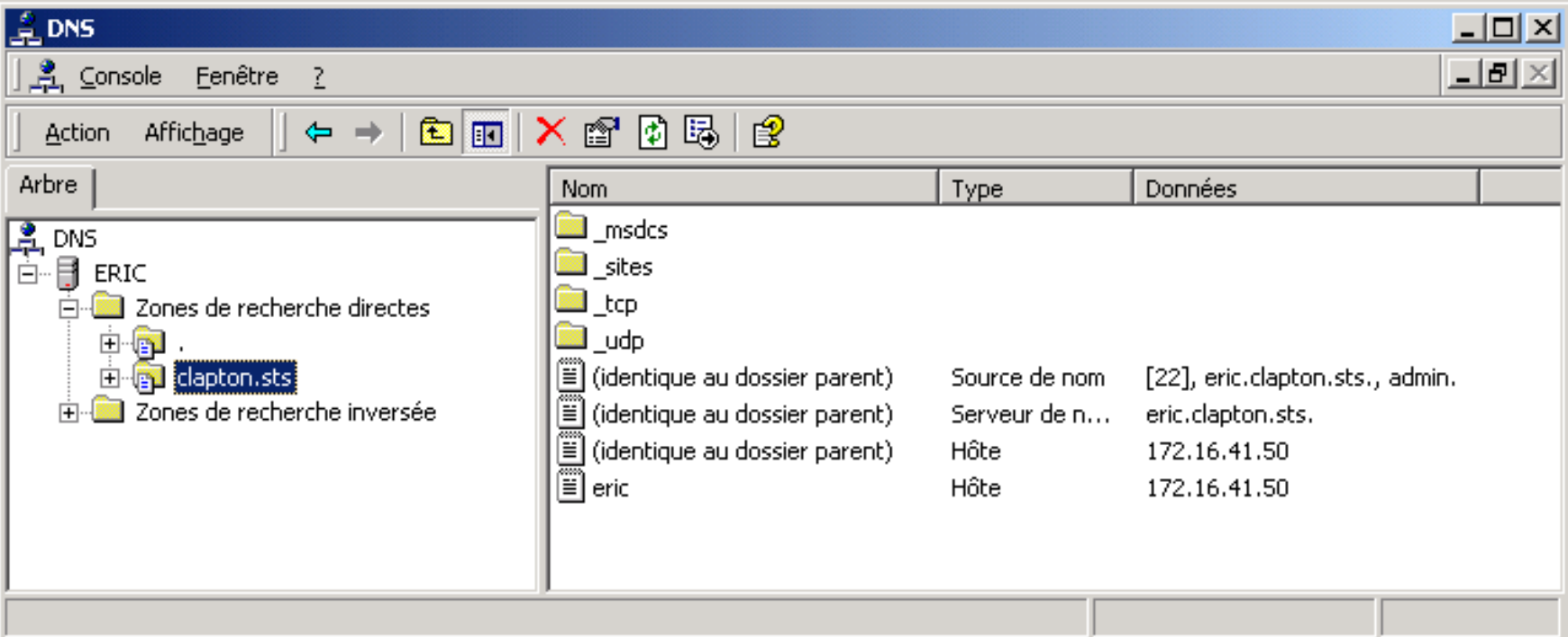
140

## Résultat dans l'Active Directory



# Quatrième étape

## 141 Résultat dans le serveur DNS (ERIC)



The screenshot displays the Windows DNS console. The left pane shows the tree structure with the following nodes:

- DNS
  - ERIC
    - Zones de recherche directes
      - . (parent)
      - eric.clapton.sts (selected)
    - Zones de recherche inversée

The right pane shows a list of records for the selected zone. The table below represents the data shown in the console:

Nom	Type	Données
_msdcs		
_sites		
_tcp		
_udp		
(identique au dossier parent)	Source de nom	[22], eric.clapton.sts., admin.
(identique au dossier parent)	Serveur de n...	eric.clapton.sts.
(identique au dossier parent)	Hôte	172.16.41.50
eric	Hôte	172.16.41.50



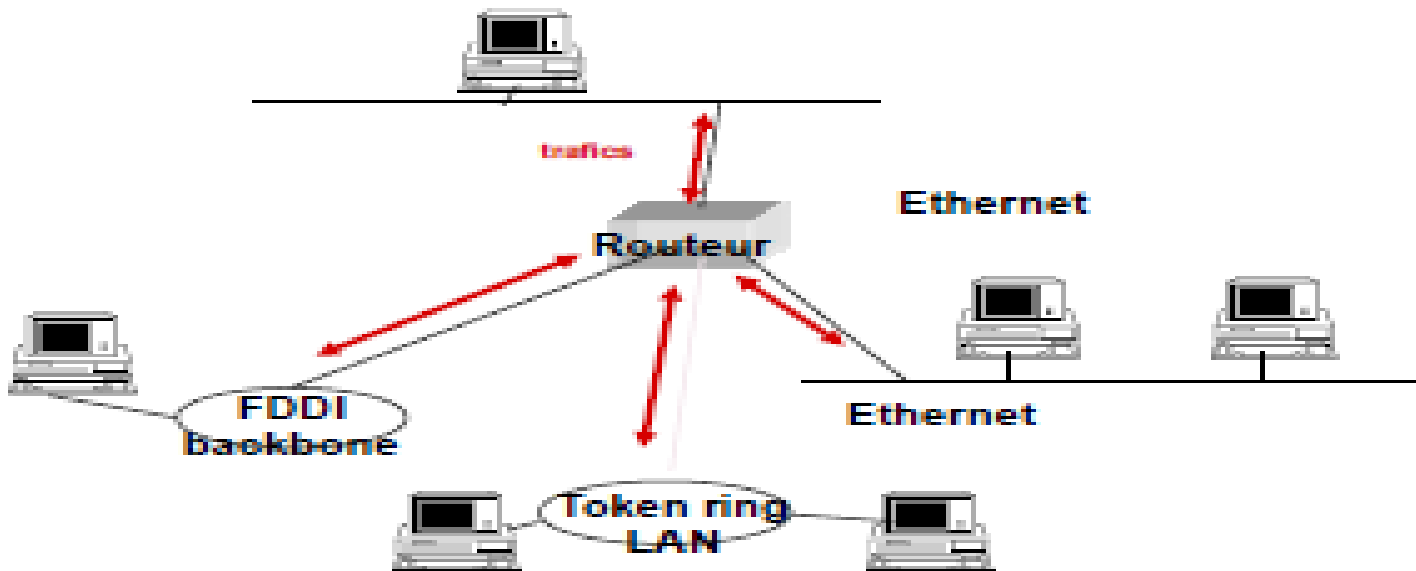
# LE PROTOCOLE SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

<http://www.academiepro.com/enseignants-104-Chaabani.Nizar.html>

# SNMP : Motivation

143

- Nécessité d'avoir un protocole permettant de remonter des informations sur l'activité des différentes ressources du réseau (les serveurs, les routeurs, les hubs, etc).



# Qu'est ce que le protocole SNMP ?

144

- SNMP est un protocole de gestion réseaux
- Il s'appuie sur 4 composantes principales :
  - ✓ Des agents
  - ✓ Un ou plusieurs managers
  - ✓ Une MIB (Management Information Base)
  - ✓ Des trames



# Modèle d 'administration SNMP

145

Une administration SNMP est composée de trois types d'éléments :

- ✓ des **agents chargés de superviser un équipement**. On parle d'**agent** SNMP installé sur tout type d'équipement.
- ✓ une ou plusieurs **stations de gestion capables d'interpréter les données**
- ✓ une **MIB (Management Information Base) décrivant les informations** gérées (objets administrés).
- ❖ SNMP permet **la supervision, le contrôle et la modification** des paramètres des éléments du réseau.

# Le modèle OSI

146

	Modèle OSI	Modèle TCP/IP (protocole)
7	Application	<b>SNMP</b>
6	Présentation	
5	Session	
4	Transport	<b>UDP</b>
3	Réseau	<b>IP</b>
2	Liaison	Interface réseau
1	Physique	

# Présentation de SNMP

147

Protocole d'administration de machines supportant TCP/IP

- SNMP Version 1 (SNMPv1)

Mécanisme de sécurité basé sur la notion de communauté (mot de passe en clair dans les requêtes et réponses)

- SNMP Version 2 (SNMPv2)

Introduit deux nouveaux types de paquets get-bulk-request et inform-request (communication entre plate-formes)

- SNMP Version 3 (SNMPv3)

Introduit de nouveaux mécanismes de sécurité (authentification forte et confidentialité)

# Présentation de SNMP

148

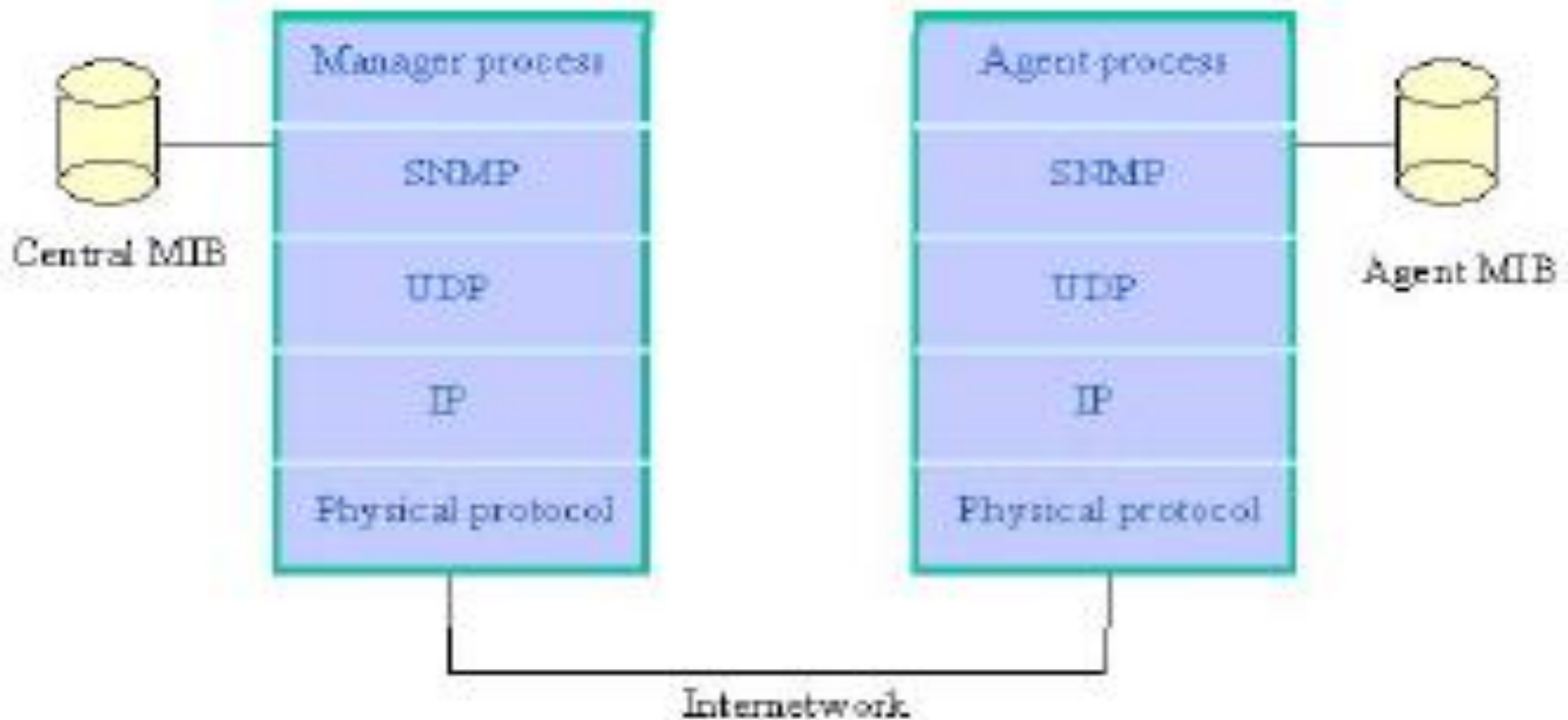
Répond à un grand nombre de besoins :

- ❖ Administrer à distance des machines indépendamment de leur architecture
- ❖ Disposer d'une cartographie du réseau
- ❖ Fournir un inventaire précis de chaque machine
- ❖ Mesurer la consommation d'une application
- ❖ Signaler les dysfonctionnements

# L 'architecture de SNMP

149

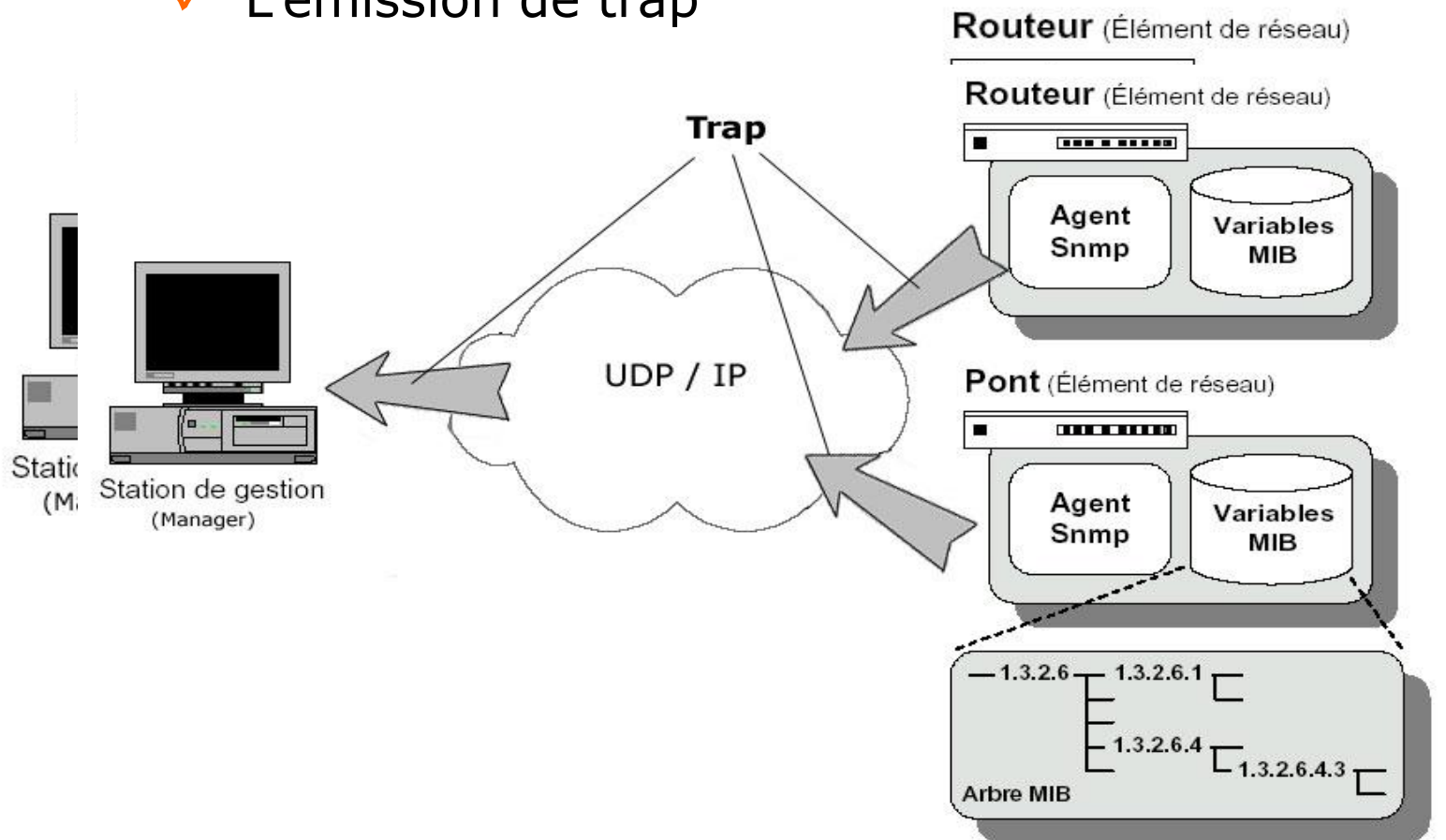
SNMP fonctionne au dessus de UDP



# La remontée d'informations

➤ Nous avons le choix entre deux méthodes complètement différentes mais qui peuvent être complémentaires :

- ✓ Le polling
- ✓ L'émission de trap



# Les requêtes SNMP

151

- Recherche d'informations :
  - ✓ **GetRequest** : recherche d'une variable sur un agent.
  - ✓ **GetNextRequest** : recherche de la variable suivante.
  - ✓ **GetBulkRequest** : recherche d'un groupe de variables
- Envoie d'informations
  - ✓ **Trap** : détection d'un incident
- Modification de valeurs :
  - ✓ **SetRequest** : permet de changer la valeur d'une variable d'un agent.

# Les réponses SNMP

152

Une seule réponse existe.

Elle est différente s'il y a une erreur ou non.

➤ Aucune erreur :

**GetResponse** : renvoie la ou les valeurs souhaitées

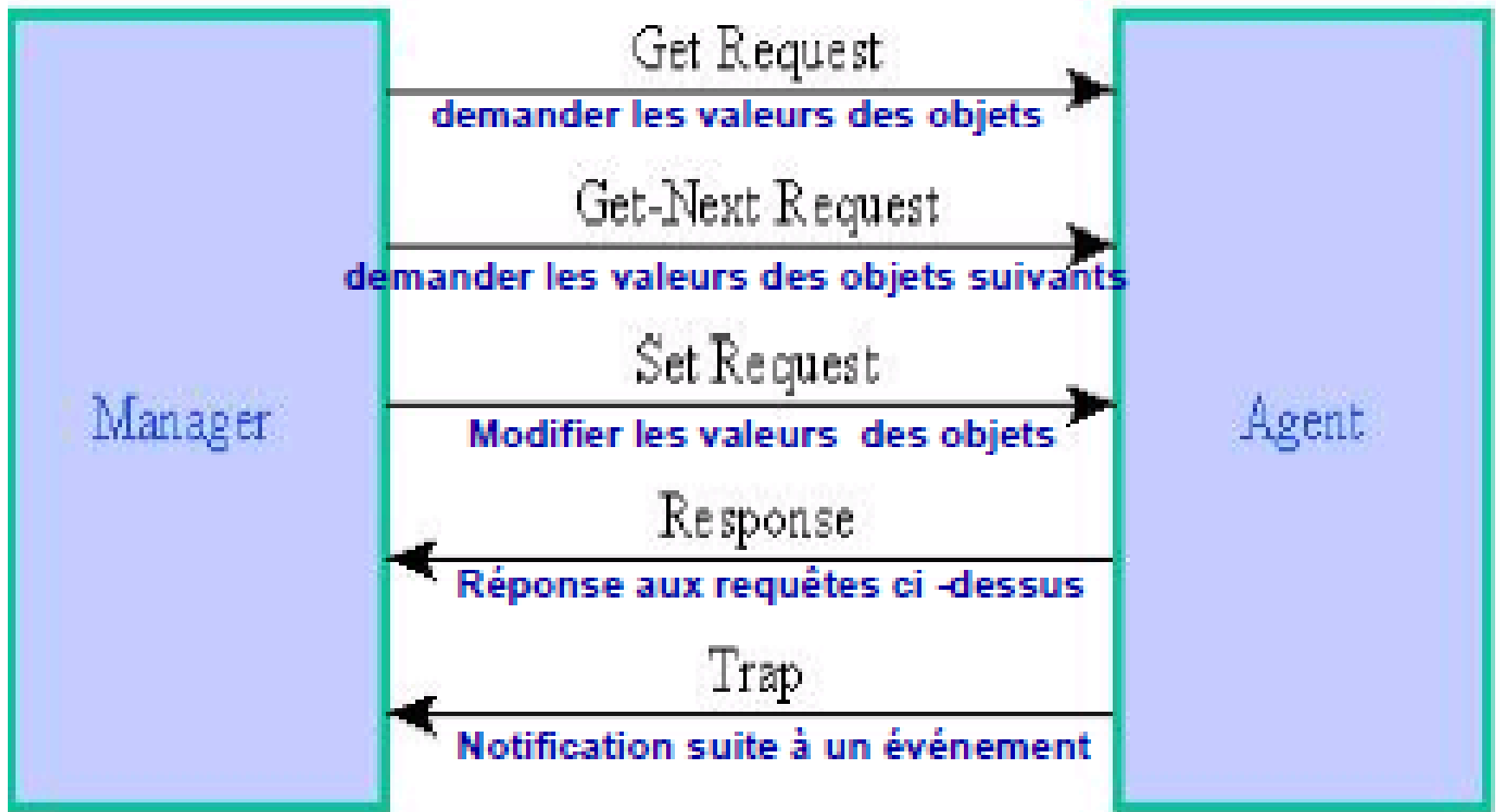
➤ En cas d'erreur :

**GetResponse** mais accompagné d'un *NoSuchObject*



# Les PDUs SNMP

153

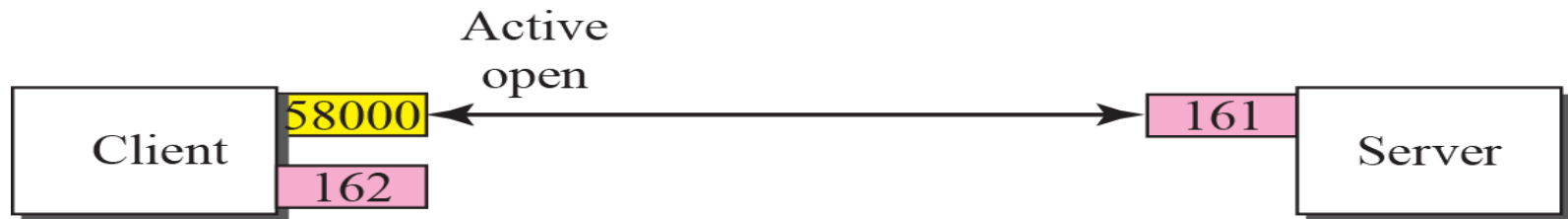


# Les Ports SNMP

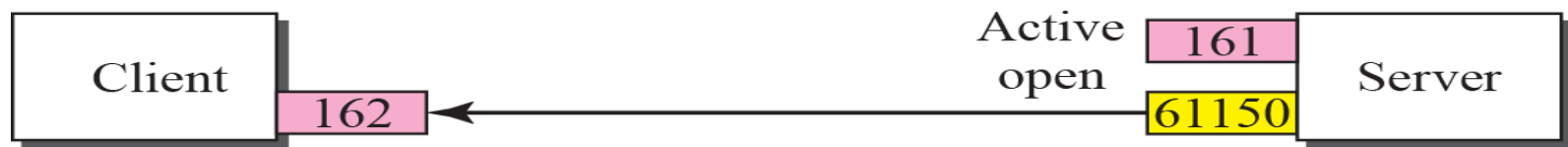
154



a. Passive open by both client and server



b. Exchange of request and response messages



c. Server sends trap message

# MIB (Management Information Base)

155

- Ensemble d'objets structurés de manière arborescente

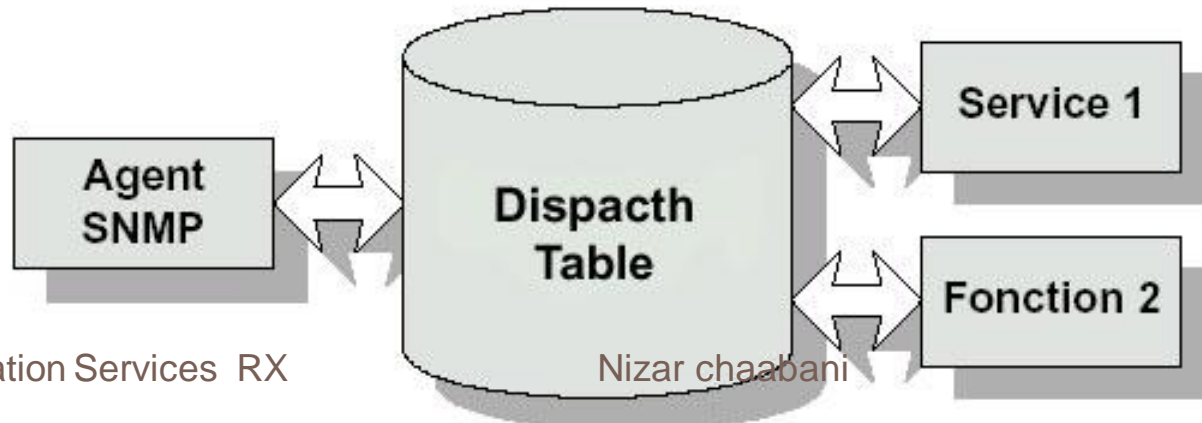
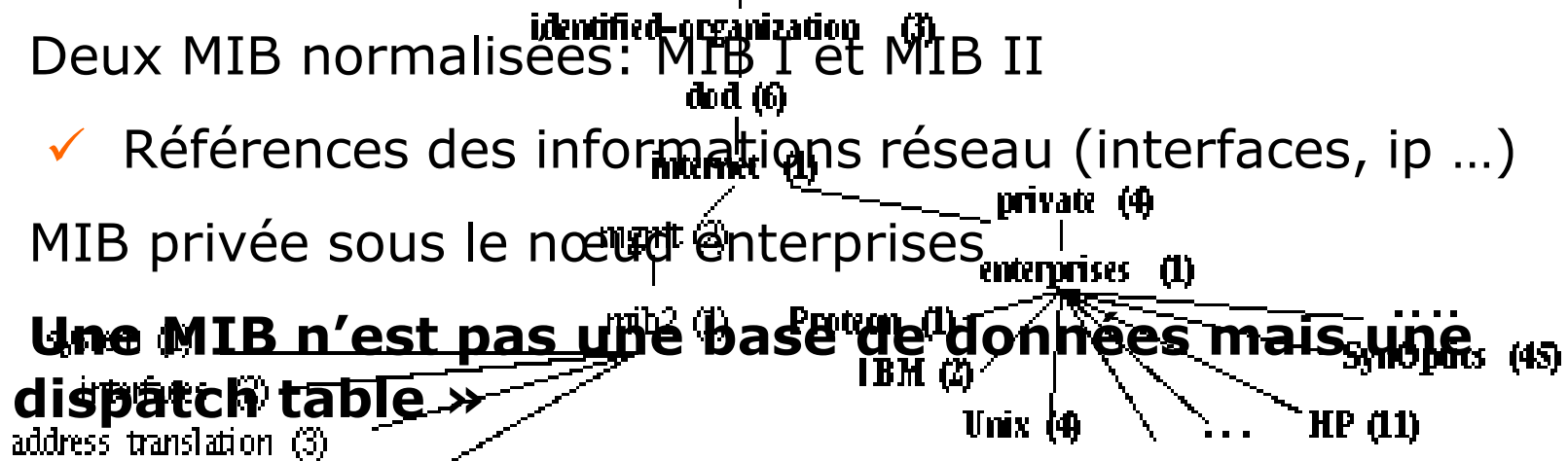
- Accès à un objet via un Object Identifier (OID)

- Deux MIB normalisées: MIB I et MIB II

- ✓ Références des informations réseau (interfaces, ip ...)

- MIB privée sous le nœud enterprises

- **Une MIB n'est pas une base de données mais une « dispatch table »**



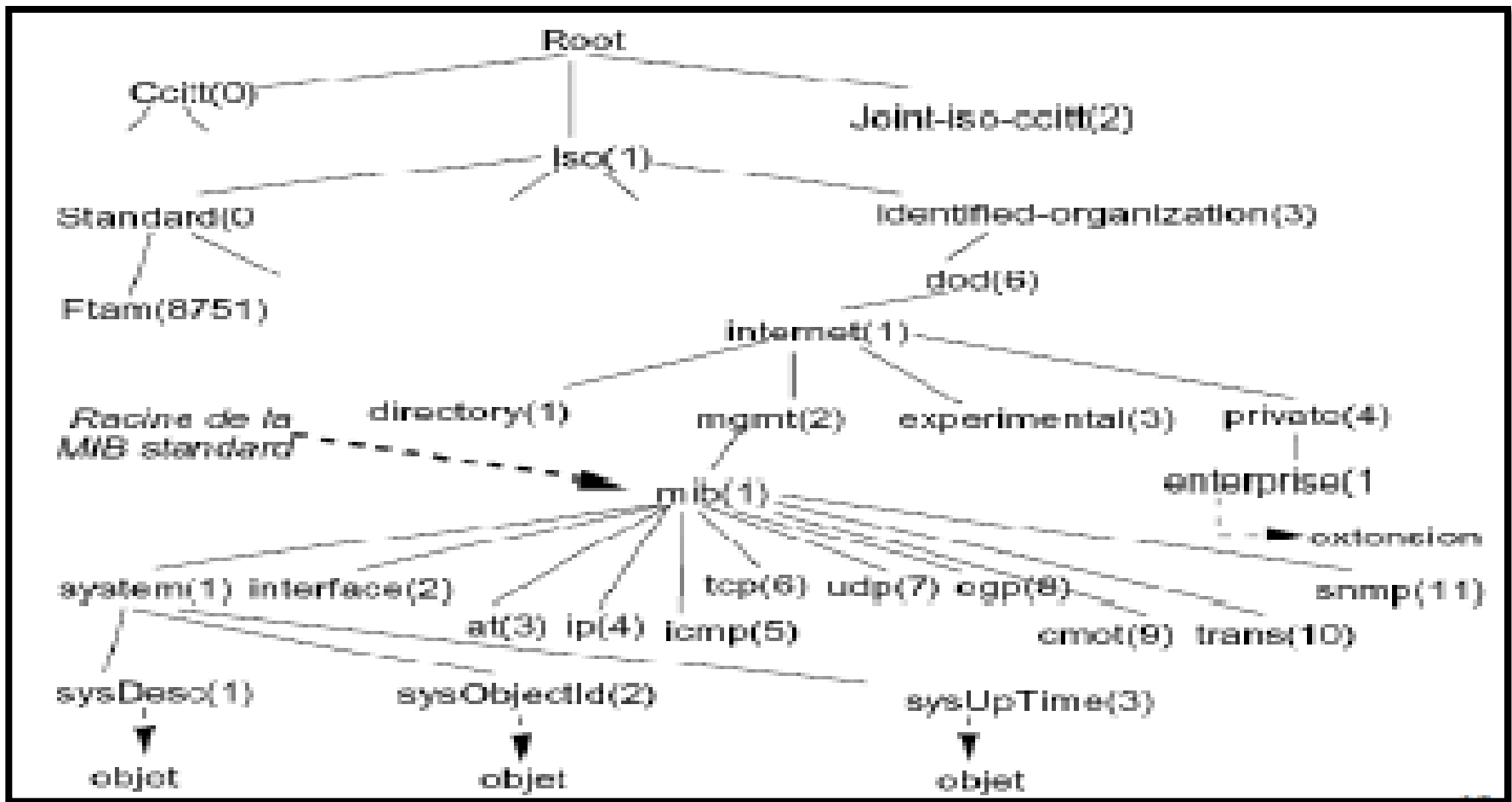
# La MIB (Management Information Base)

156

- 1 ressource à gérer = 1 objet
- Les objets administrables sont une abstraction des ressources physiques (interfaces, équipements, etc.) et logiques (connexion TCP, paquets IP, etc.)
- **MIB : collection structurée d'objets reconnus par les agents**
- Chaque noeud dans le système doit maintenir une MIB qui reflète l'état des ressources gérées
  - Une entité d'administration peut accéder aux ressources du noeud en lisant les valeurs de l'objet ou en les modifiant
- **MIB: 2 objectifs**
- ✓ Un schéma commun : SMI (Structure of Management Information)
- ✓ Une définition commune des objets et de leur structure

# Arbre des MIB accessibles

157



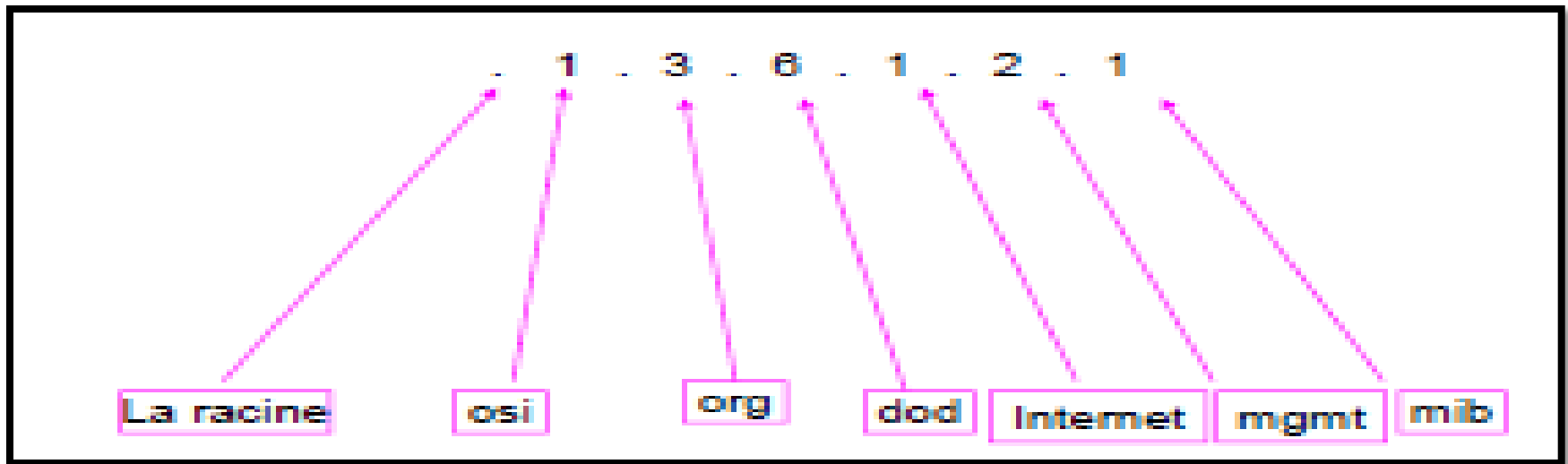
# Identificateur d'un objet de la MIB

158

Identificateur d'un objet:

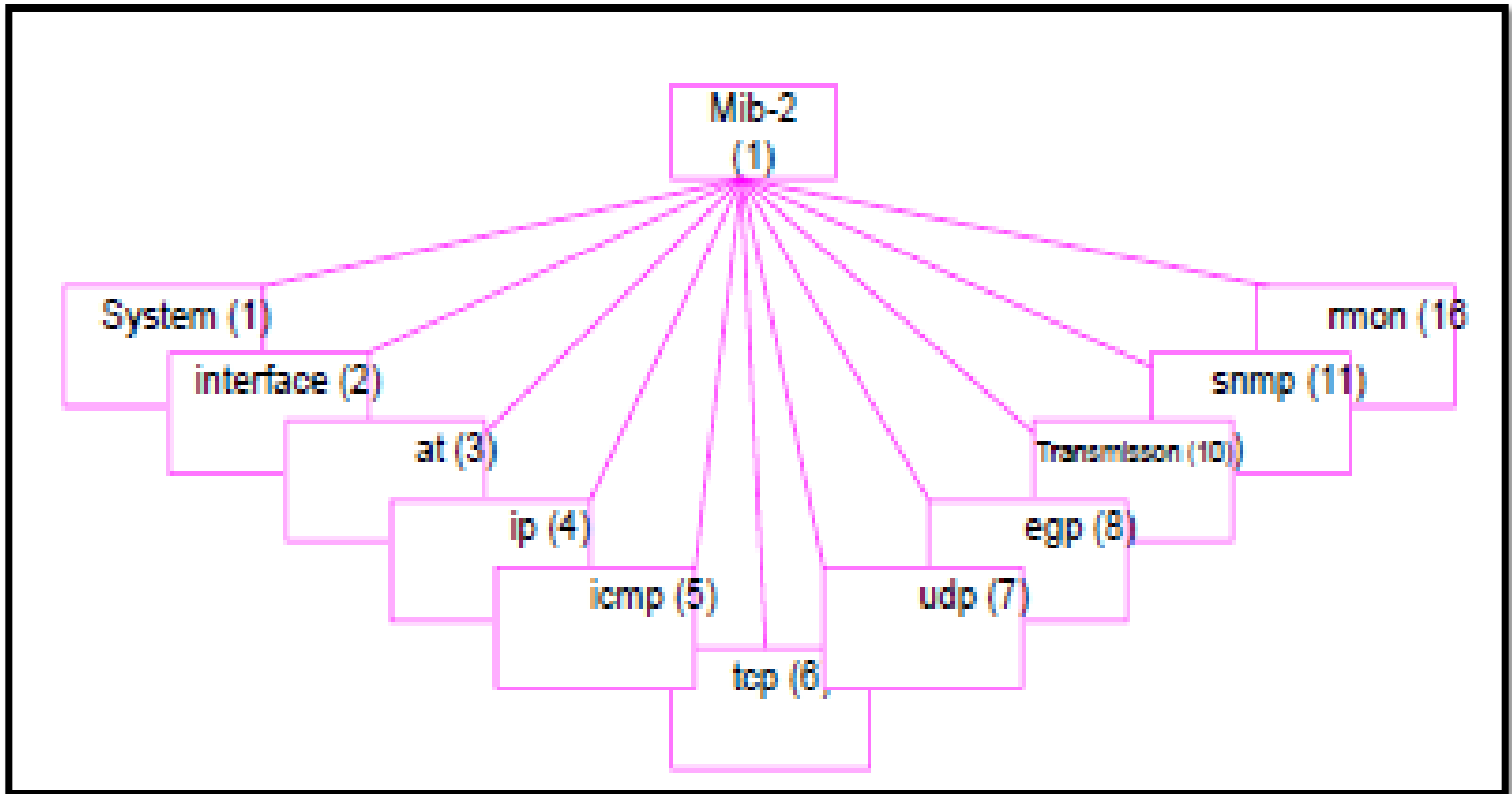
Identificateur unique = séquence d'entiers dont chacun représente la position de ces successeurs dans l'arbre.

Exemple: **identificateur de l'objet MIB :**



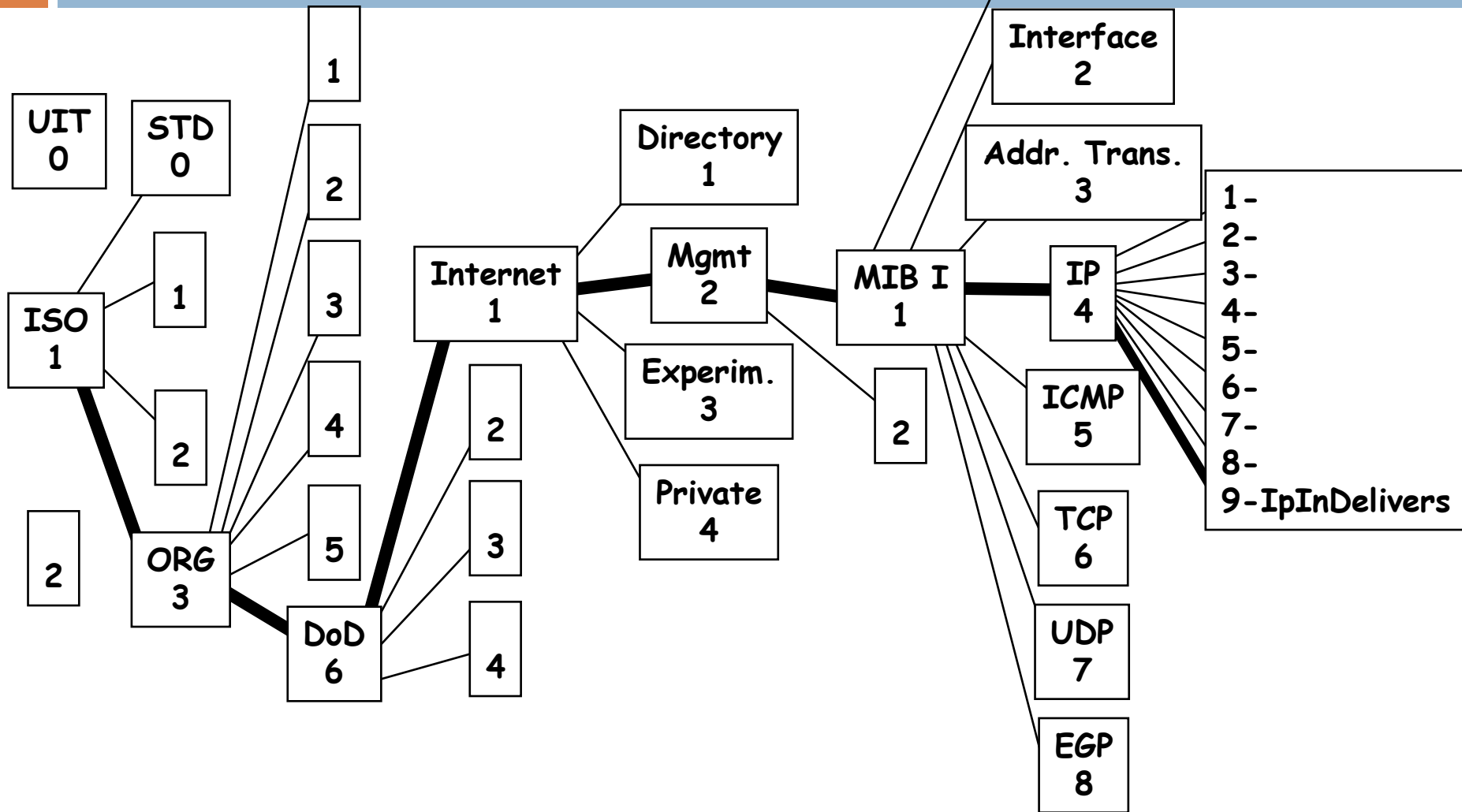
# Le groupe MIB-2

159



1 - 3 - 6 - 1 - 2 - 1 - 4

160





# La structure numérique de la MIB

161

- **system**                    **1.3.6.1.2.1.1**
- **interfaces**                **1.3.6.1.2.1.2**
- **at**                         **1.3.6.1.2.1.3**
- **ip**                         **1.3.6.1.2.1.4**
- **icmp**                      **1.3.6.1.2.1.5**
- **tcp**                        **1.3.6.1.2.1.6**
- **udp**                        **1.3.6.1.2.1.7**
- **egp**                        **1.3.6.1.2.1.8**
- **rmon**                      **1.3.6.1.2.1.9**
- **transmission**            **1.3.6.1.2.1.10**
- **snmp**                      **1.3.6.1.2.1.11**

# Requête SNMP

162

- Les formats des requêtes SNMP sont spécifiées par une description en ASN.1 (Abstract Syntax Notation 1).
- Le principe de la syntaxe de transfert est que chaque valeur transmise contient trois champs :
  - ▣ Un identificateur
  - ▣ La longueur en octets du champ de données
  - ▣ Le champ de données



# Requête SNMP

163

Le format des messages SNMP comprend plusieurs champs :

Tag	Longueur du message	Versio n	Community Name	Le champ PDU
-----	---------------------------	-------------	-------------------	-----------------

- ▣ Le champ Tag identifie le type de la trame.
- ▣ Le champ Longueur contient la longueur totale de la trame.
- ▣ Le champ Version est utilisé pour une compatibilité entre les différentes versions SNMP.
- ▣ Le champ community Name contient le nom de la communauté utilisée dans le processus d'authentification.

# Requête SNMP

164

Le format des messages SNMP comprend plusieurs champs :

Tag	Longueur du message	Versio n	Community Name	Le champ PDU
-----	---------------------------	-------------	-------------------	-----------------

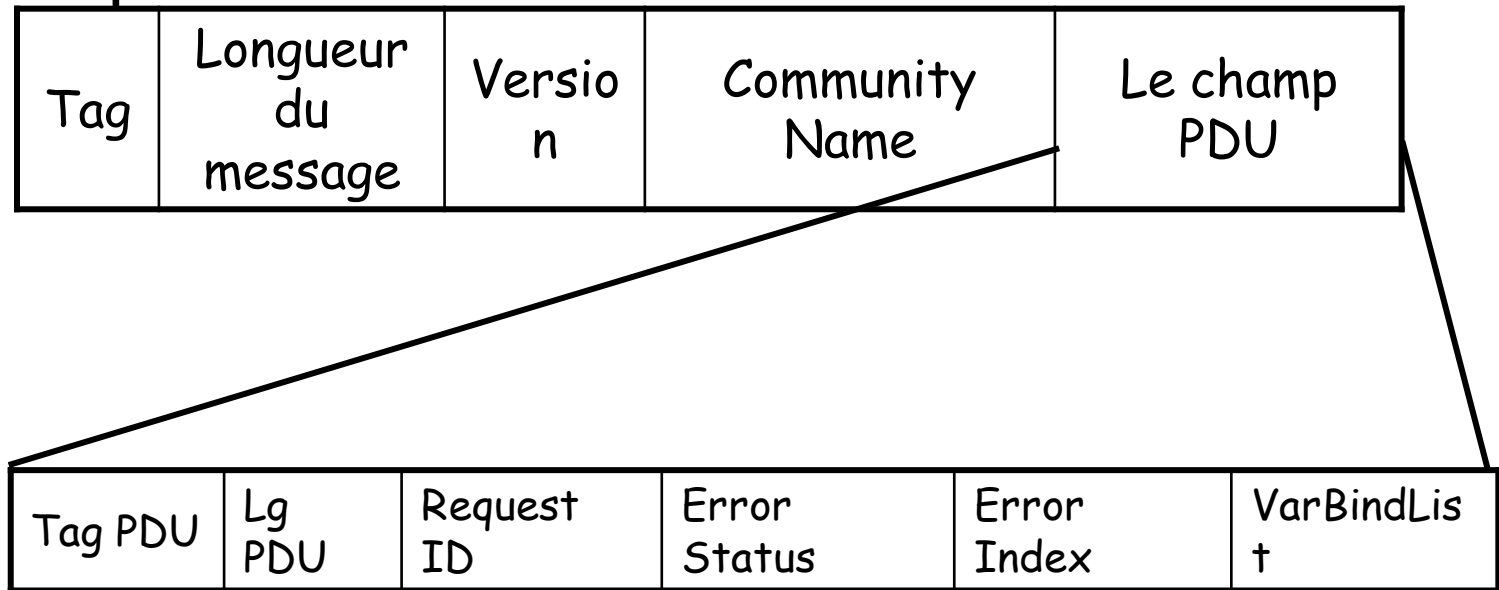
Le champ PDU comprend 5 valeurs :

- La PDU GetRequest
- La PDU GetNextRequest
- La PDU SetRequest
- La PDU GetRespons
- La PDU Trap

# Requête SNMP

165

Le format des messages SNMP comprend plusieurs champs :



Format d'une PDU

# Structure des informations d 'Administration (SMI)

166

- ☐ La MIB contient des éléments simples (scalaire et tableaux à deux dimensions de scalaires)
- ☐ **SMI (Structure of Management information) : donne les règles de définition, d'accès et d'ajout des objets dans la MIB (méta-modèle)**
- ☐ **Objectifs : encourager la simplicité et l'extension de la base d 'informations d'Administration :**
- ☐ Représentation identique des objets >>> rendre un objet accessible de la même manière sur chaque entité du réseau
- ☐ L 'objet administré peut être considéré d 'être composé d 'un type d 'objet et une instance.
- ☐ SMI définit le type d 'objets et non leur instance.

# Structure des informations d 'Administration (SMI)

167

## **Un objet possède :**

- un nom (Descripteur + identificateur d 'objet)
- une syntaxe utilisant ASN.1 (Abstract Syntax Notation)
- une définition qui est un texte de description de l 'objet
- un accès qui spécifie les droits d 'accès à l 'objet (read only, read-write or not accessible)
- Un statut qui spécifie si l 'objet est courant (mandatory ou optional) ou obsolète.
- un schéma de codage BER (Basic Encoding Rules)

# Structure des informations d 'Administration (SMI)

168

Les caractéristiques d 'un objet sont regroupées dans la définition d 'une macro qui définit la structure d 'un type d 'objet :

**OBJECT-TYPE MACRO ::=**

**BEGIN**

**TYPE NOTATION ::=**

**"SYNTAX" type (TYPE ObjectSyntax)**

**"ACCESS" Access**

**"STATUS" Status**

**VALUE NOTATION ::= value (VALUE ObjectName)**

**Access ::= "read-only »|"read-write"|"write-only"|"not-accessible"**

**Status ::= "mandatory«|"optional«|"obsolete"|"deprecated"**

**END**



# Structure des informations d 'Administration (SMI)

169

**atIndex OBJECT-TYPE**

**SYNTAX Integer**

**ACCESS read-write**

**STATUS mandatory**

**DESCRIPTION « Numéro d'interface logique.»**

**::= { atEntry 1 }**

# Exemple de fichier ASN.1

170

```
ACCELANCE-MIB DEFINITIONS ::= BEGIN
```

Identification d'un  
fichier ASN.1

```
...  
accelance MODULE-IDENTITY
```

```
...  
::= { enterprises 9697 }
```

Rattachement de la branche  
*Accelance* à la branche *enterprises* via  
l'OID 9697

```
general OBJECT IDENTIFIER ::= { accelance 1 }
```

Affectation de la branche  
*general* à la branche  
*accelance* via l'OID 1

```
...  
release OBJECT-TYPE  
    SYNTAX      DisplayString  
    MAX-ACCESS  read-only  
    STATUS      current  
    DESCRIPTION  
        "Type d'OS utilisé"  
    ::= { general 1 }
```

Définition de la variable *release*

&

Rattachement de celle-ci à la  
branche *general*

- Désormais nous pouvons accéder à la variable *release* de la manière suivante :

Administration Services RX Nizar chaabani  
**.iso.dod.internet.private.enterprises.accelance.general.release.0**

# Mécanismes de sécurité de SNMP

171

L 'autorisation est l 'intersection entre le mode d 'accès défini par la communauté et l 'accès à l 'objet défini parmi les caractéristiques de l 'objet.

Mode d'accès	read-only	read-write	write-only	not-accessible
read-only	3	3	1	1
read-write	3	2	4	1

où les classes sont définies par :

1 no right	3 get, get-next, trap
2 get, get-next, set, trap	4 set, trap



172

INSTITUT SUPERIEUR DES ETUDES TECHNOLOGIQUES DE SILIANA

<http://www.academiepro.com/enseignants-104-Chaabani.Nizar.html>

Administration Services RX

Nizar chaabani