e i g

Architecture réseau basée sur Windows 2000

- Diplômant : Yann Souchon
- Professeur : Gérald Litzistorf

Sommaire

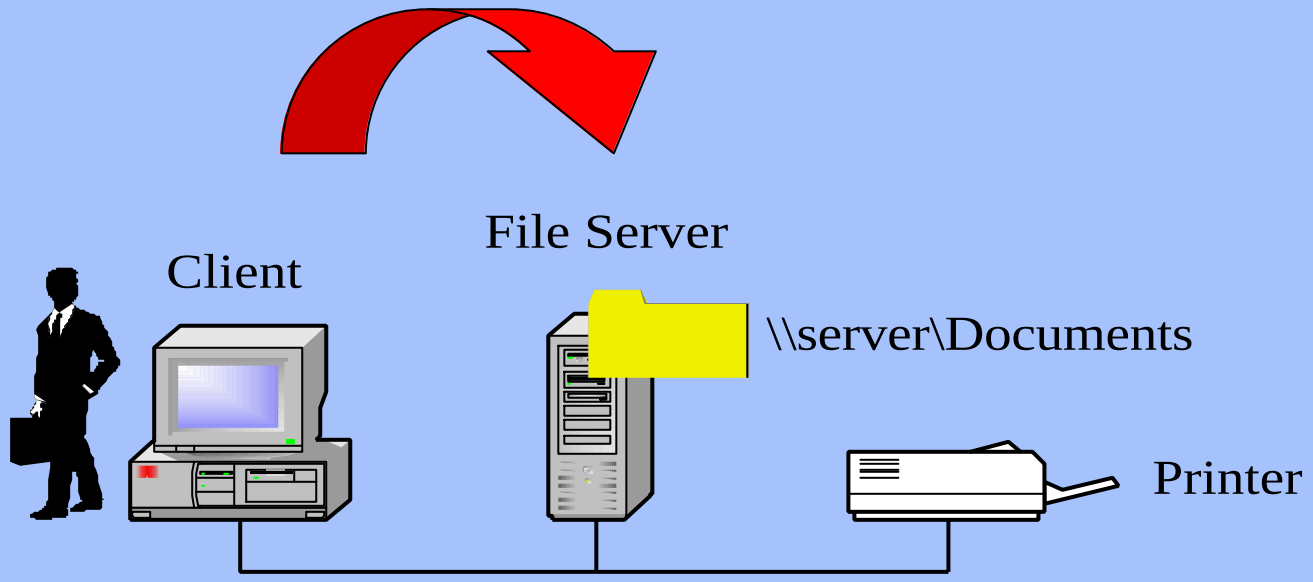
e i g

- Introduction
- Autorisations NTFS
- Structure logique
- Etape 1 : *1 domaine*
- Etape 2 : *2 domaines dans 1 forêt*
- Etape 3 : *2 domaines dans 2 forêts*
- Conclusion

Introduction

e i g

Accès à une ressource partagée ?



Autorisations NTFS

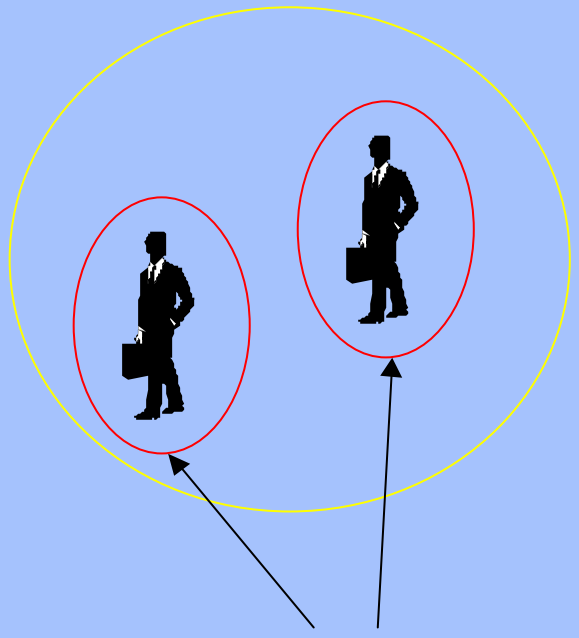
Terminologie

- **Autorisations** (***permissions***) : définissent le type d'accès aux ressources et les actions autorisées sur celles-ci.
- **Droits (*privileges*)** : permettent aux utilisateurs d'exécuter des tâches systèmes.

Autorisations NTFS (2)

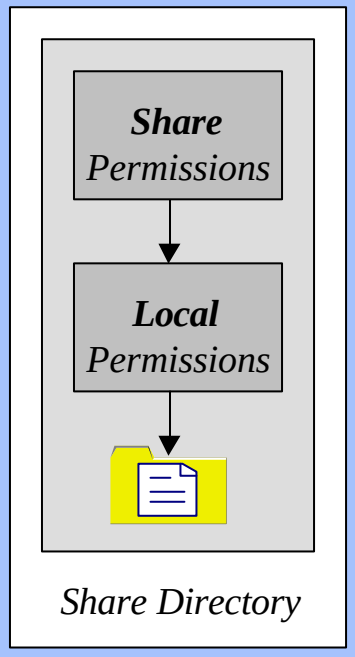
e i g

Groupes d'utilisateurs
(etudiants, professeurs)



Comptes d'utilisateurs
(souchon, litzistorf)

Autorisations au niveau ***dossier***

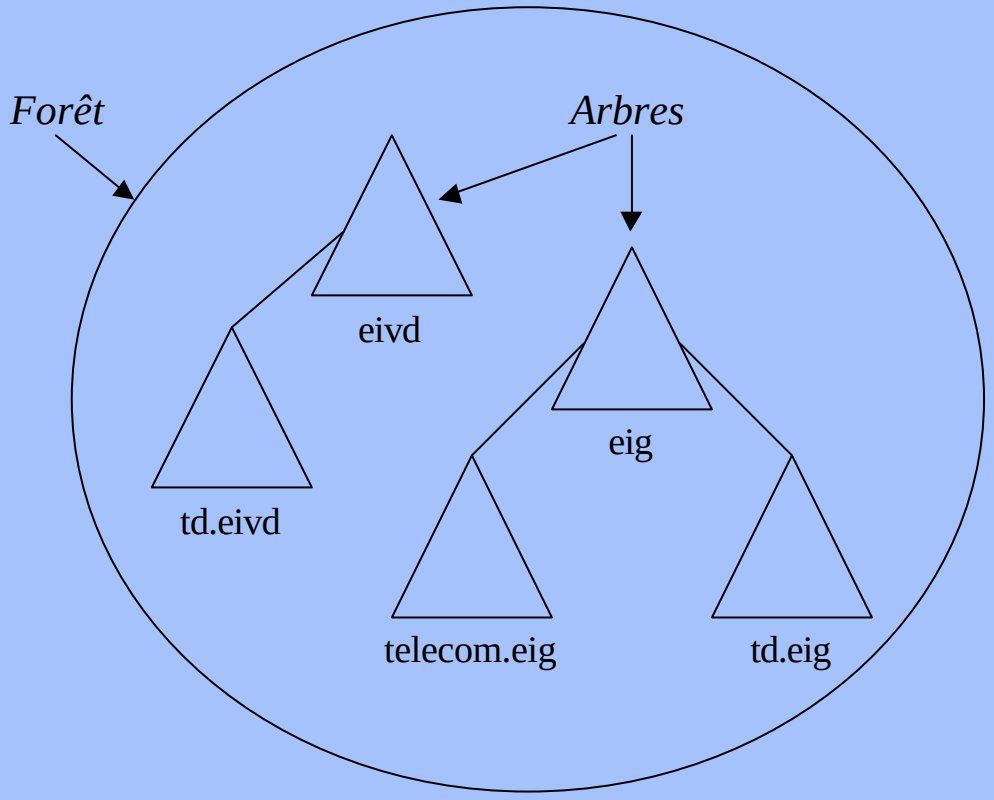


File Server

Autorisations au niveau ***fichier***

Structure logique

Arbres, Forêt



Etape 1 : *1 domaine*

e i g

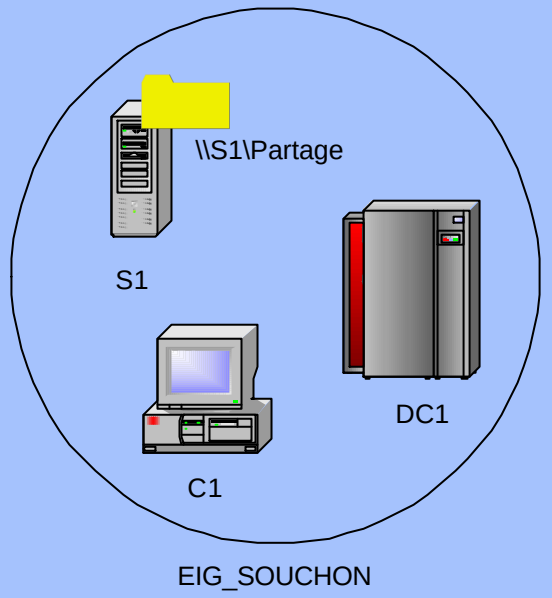
- Objectifs
- Etape 1.1 : *Démarrage d'un ordinateur dans un domaine*
- Etape 1.2 : *Authentification dans un domaine*
- Etape 1.3 : *Accès à une ressource partagée dans un domaine*
- Etape 1.4 : *Audit de la ressource partagée*

Etape 1 : *Objectifs*

e i g

Accès à une ressource dans un domaine

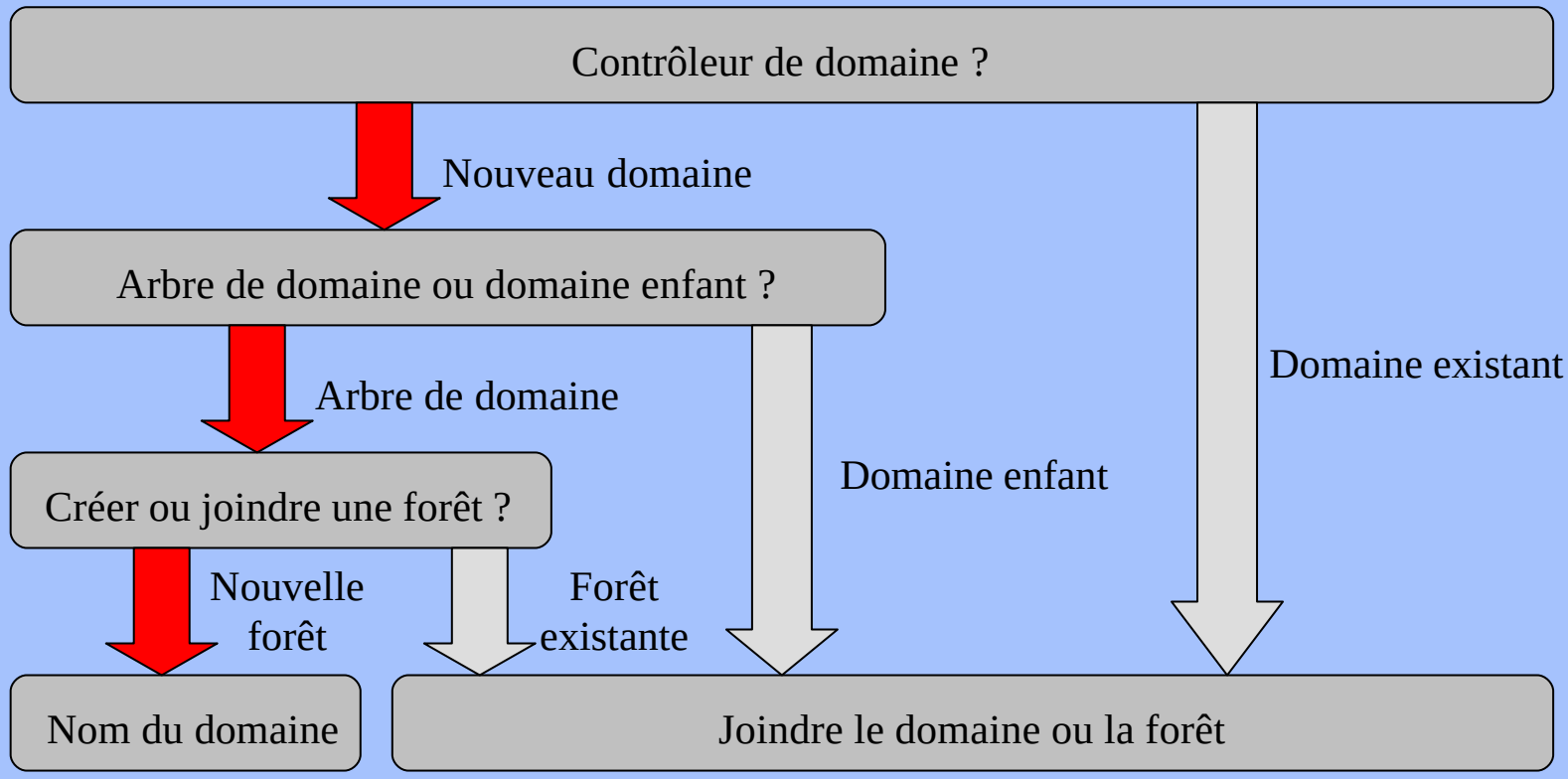
- 1 domaine avec 1 contrôleur de domaine (*DC1*)
- 1 serveur de fichiers avec 1 répertoire partagé (*S1*)
- 1 client (*C1*)
- 1 serveur DNS dynamique (*DNS1*)
- 1 zone d'adressage privée de classe C



Etape 1 : *Configuration*

e i g

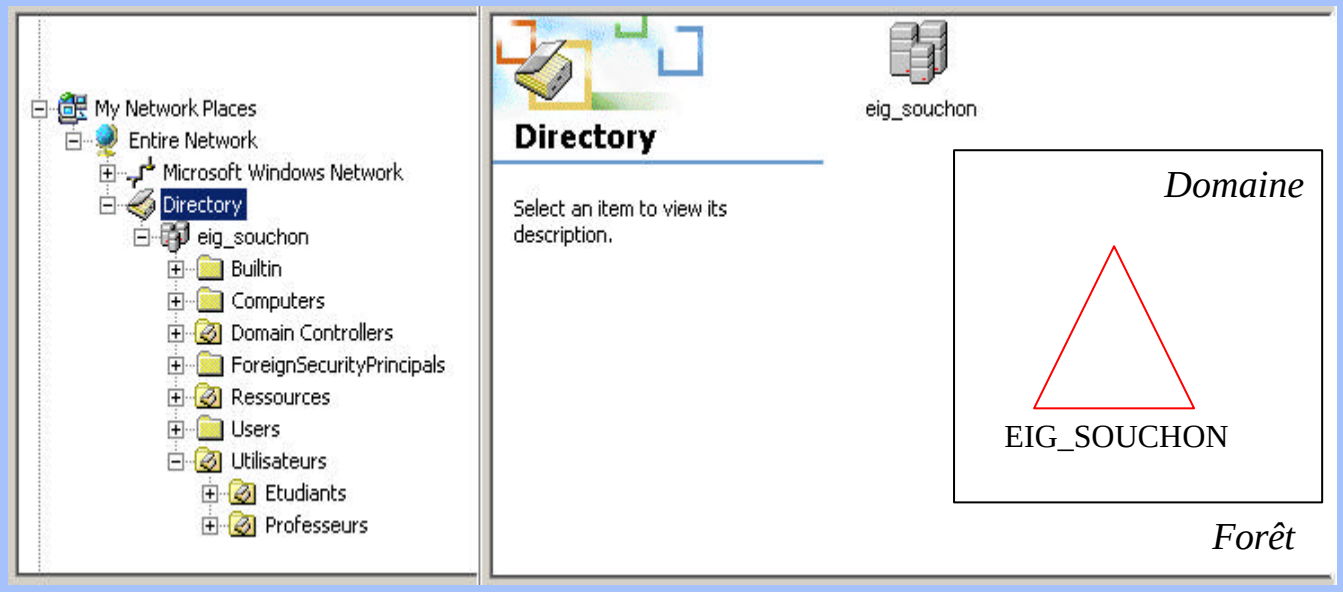
→ **Configuration de DC1**



Etape 1 : *Structure physique / logique*

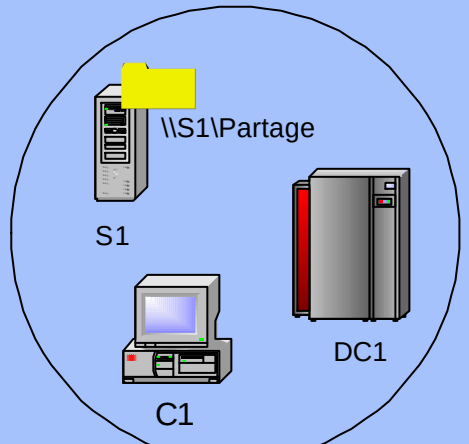
e i g

Structure logique



→ Démonstration 1 : Directory

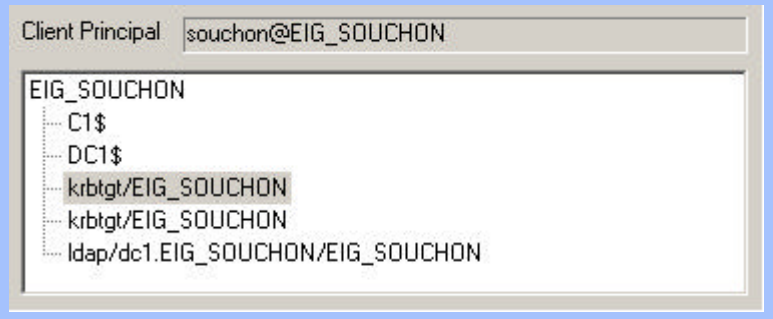
Structure physique



Etape 1.1 : *Démarrage d'un ordinateur dans un domaine*

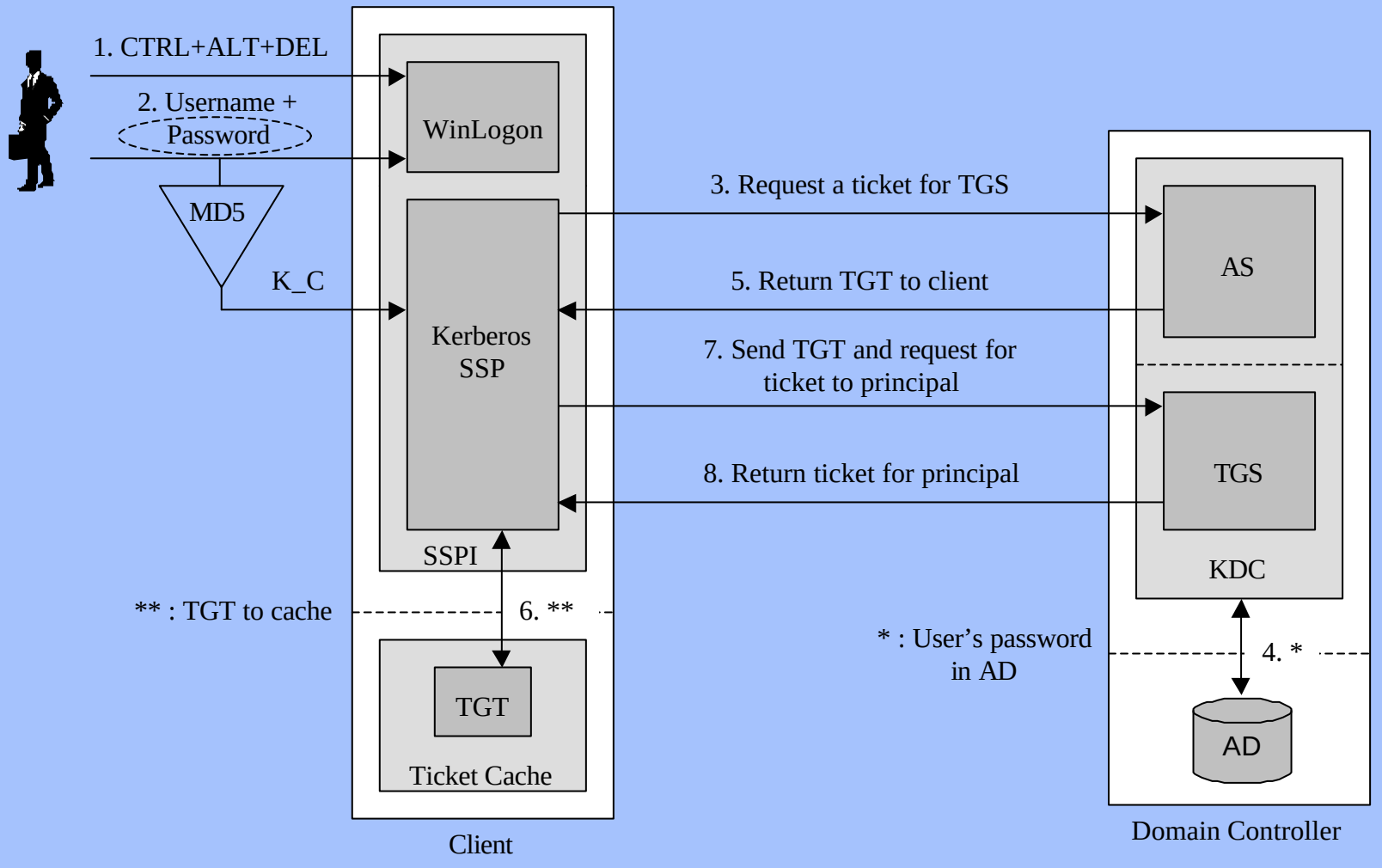
e i g

1. Connexion au réseau
2. Localisation du contrôleur de domaine
3. Synchronisaton de l'horloge
4. Authentification Kerberos
5. Mise à jour du DNS dynamiquement



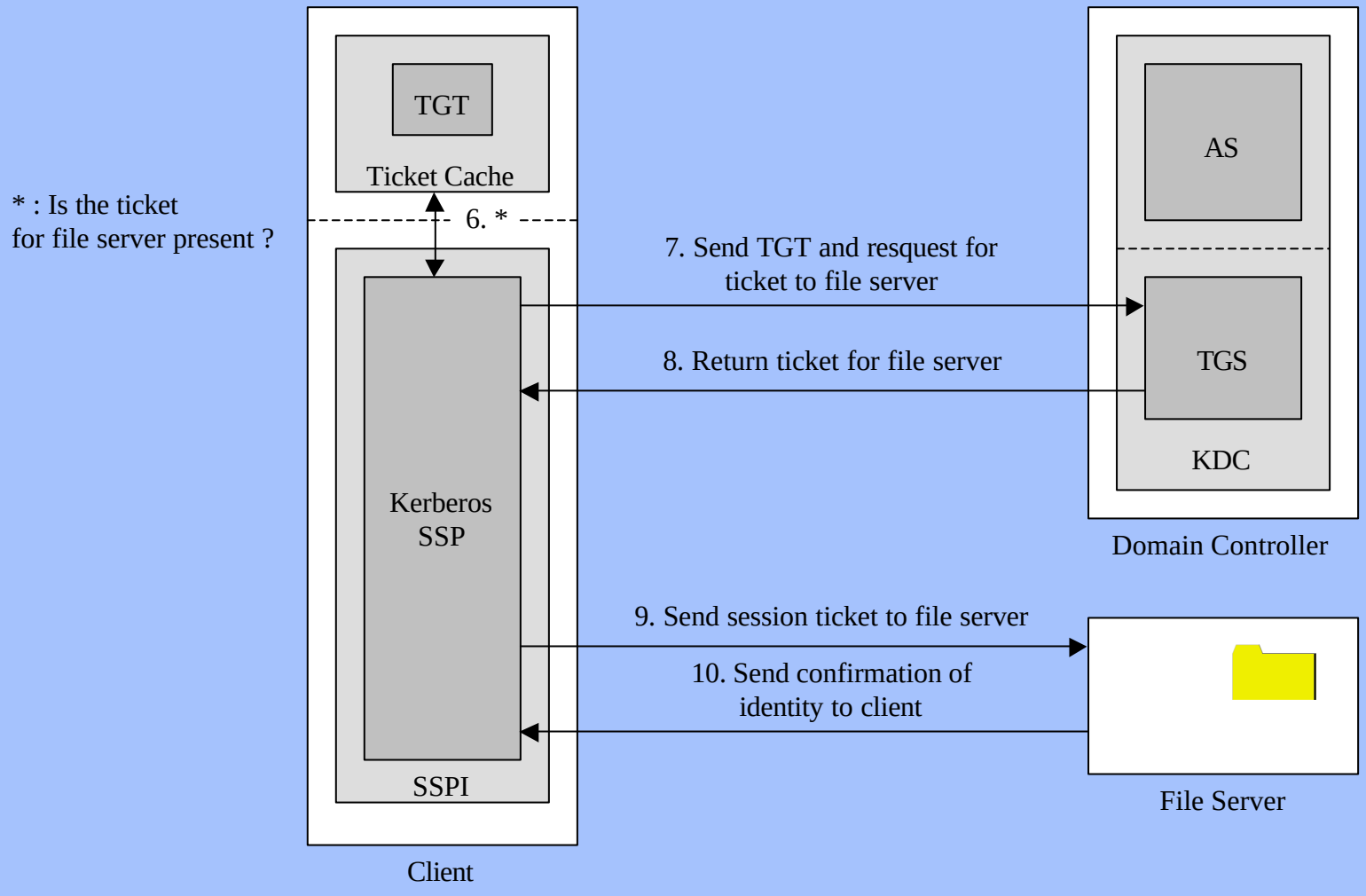
Etape 1.2 : *Authentification dans un domaine*

e i g



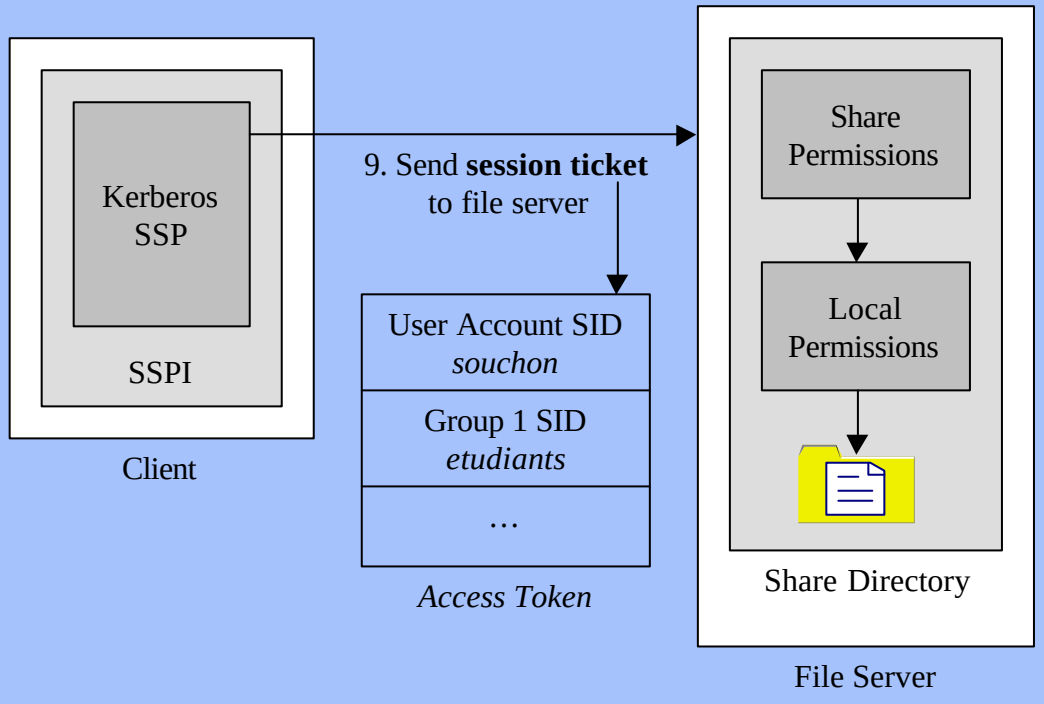
Etape 1.3 : *Accès à une ressource partagée dans un domaine*

e i g



Etape 1.4 : *Audit de la ressource partagée*

e i g



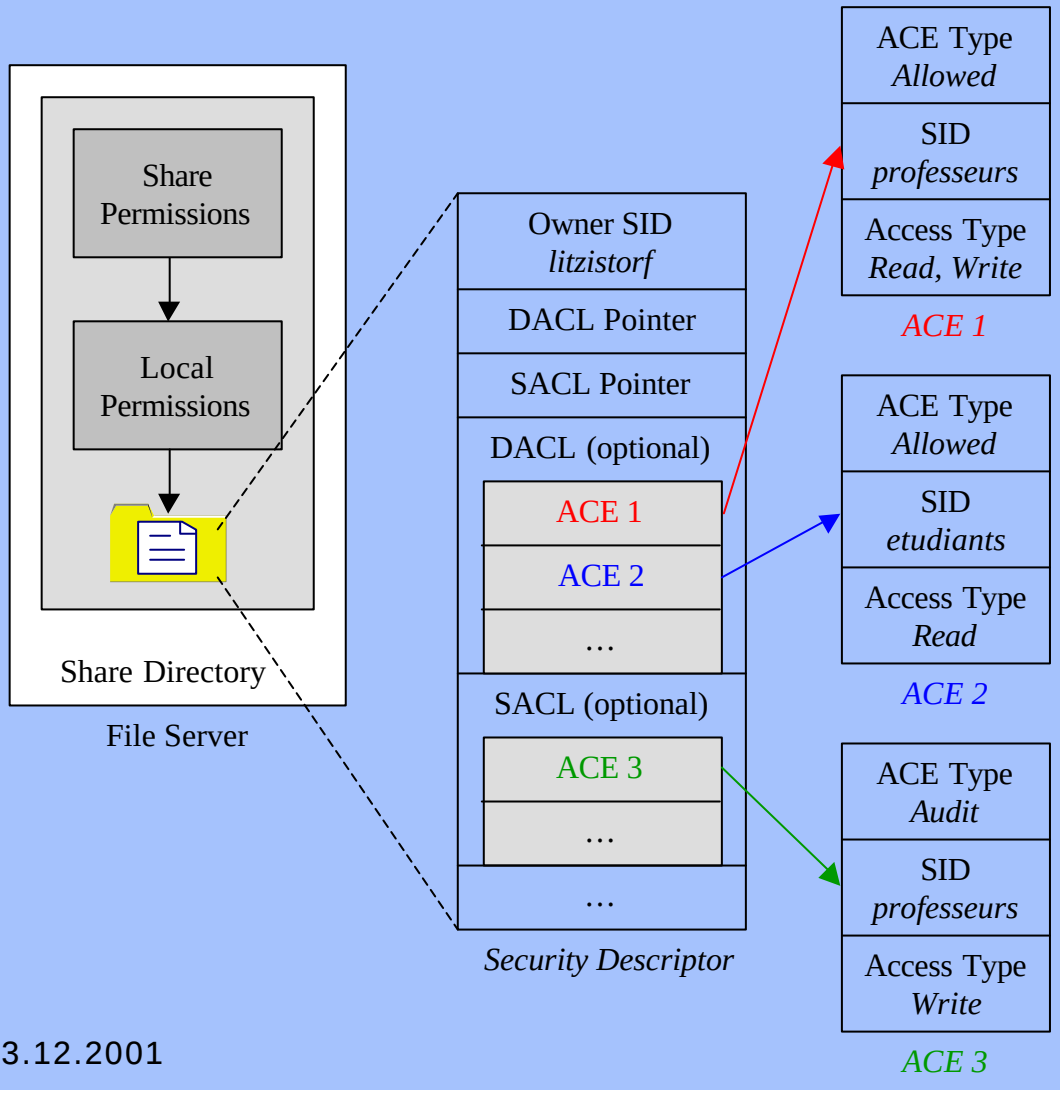
Access Tokens : Les jetons d'accès décrivent l'utilisateur et les **groupes** auxquels il appartient.

SID : Les identificateurs de sécurité sont utilisés à la place des noms pour identifier les éléments (utilisateurs, groupes, ordinateurs) d'une manière **unique**.

→ Démonstration 2 : SID

Etape 1.4 : *Audit de la ressource partagée (2)*

e i g



Security Descriptor : Les descripteurs de sécurité sont des éléments qui identifient un objet, et spécifient les actions possibles et par qui elles le sont (**Qui fait quoi ?**).

DACL (Discretionary Access Control List) : permet de déterminer les **actions** qu'un utilisateur peut accomplir sur cet objet.

SACL (System ACL) : est une liste qui s'occupe d'enregistrer ce qu'un utilisateur a **tenté** de faire avec l'objet.

Etape 2 : *2 domaines dans 1 forêt*

e i g

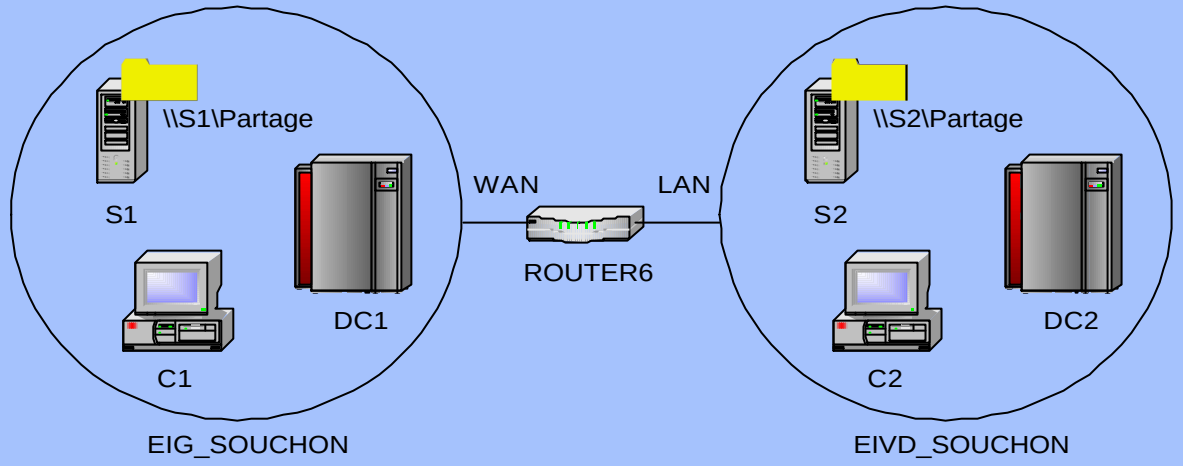
Objectifs

- 2 domaines avec 2 contrôleurs de domaine (*DC1*, *DC2*)
- 2 serveurs de fichiers avec chacun 1 répertoire partagé (*S1*, *S2*)
- 2 clients (*C1*, *C2*)
- 1 routeur Lightning Ethernet II (*ROUTER6*)
- 2 serveurs DNS dynamiques (*DNS1*, *DNS2*)
- 2 zones d'adressages IP privées de classe C

Etape 2 : *Structure physique / logique*

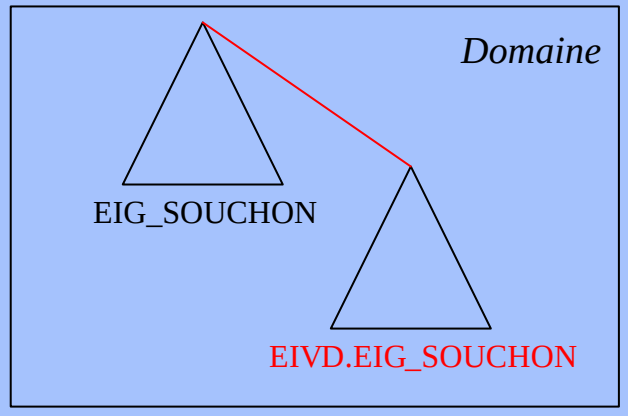
e i g

Structure physique

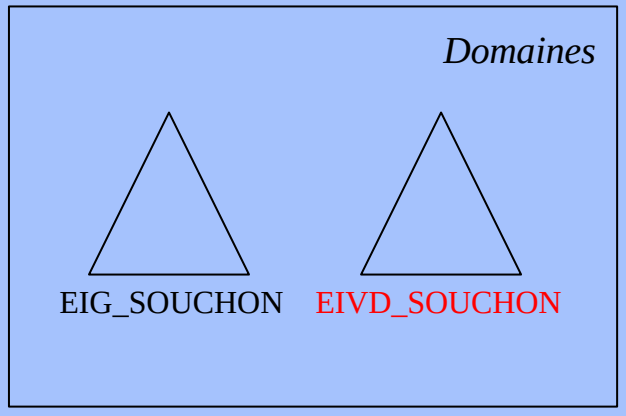


Structure logique

Variante 1 : Arbre et domaine-enfant



Variante 2 : Forêt de domaine



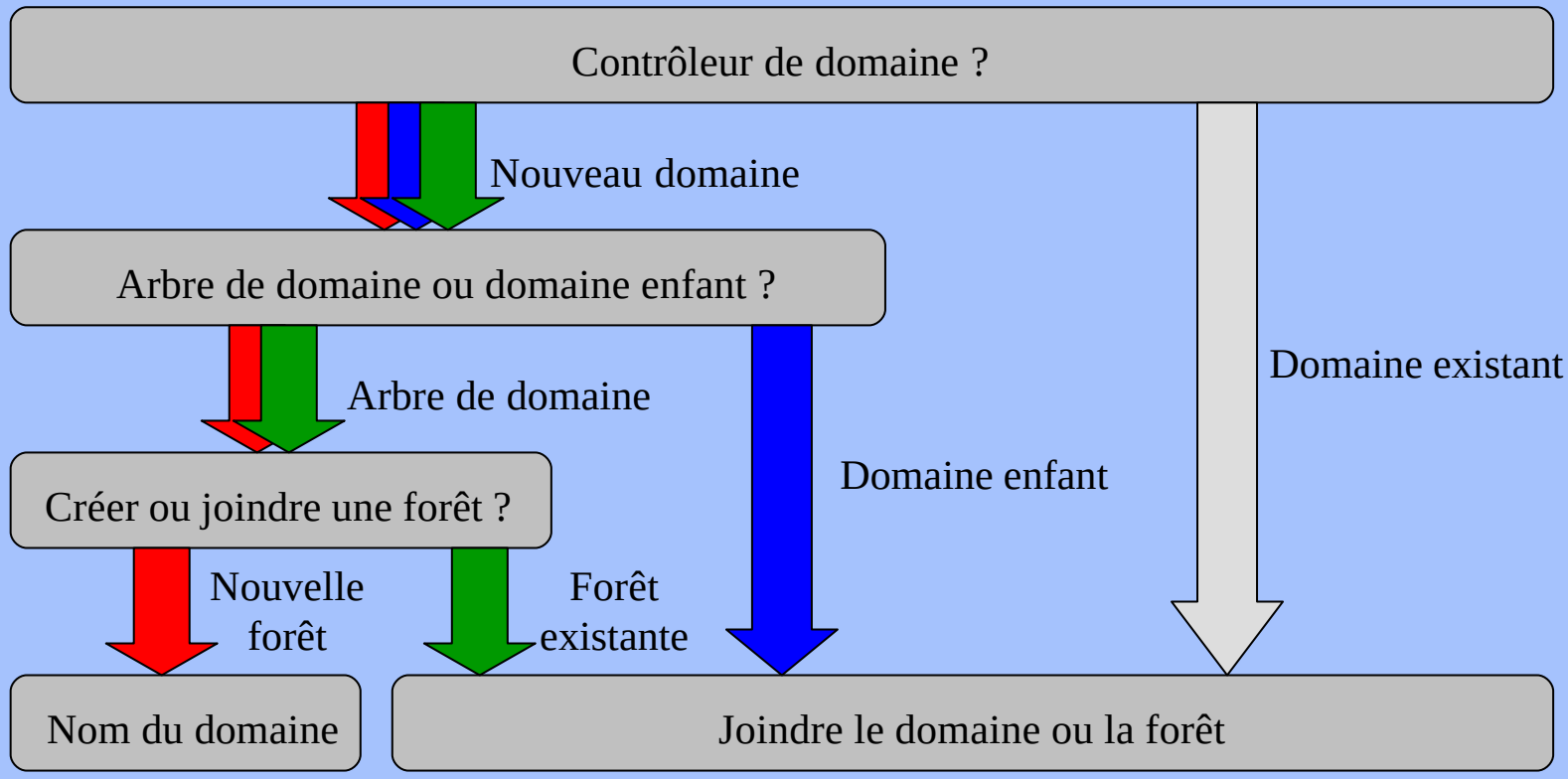
Etape 2 : *Configuration*

e i g

→ **Configuration de DC1**

→ **Configuration de DC2 (variante 1)**

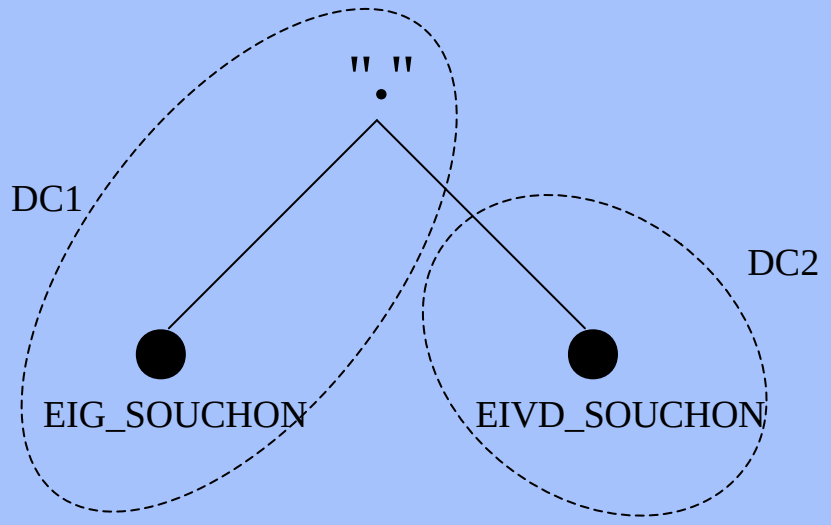
→ **Configuration de DC2 (variante 2)**

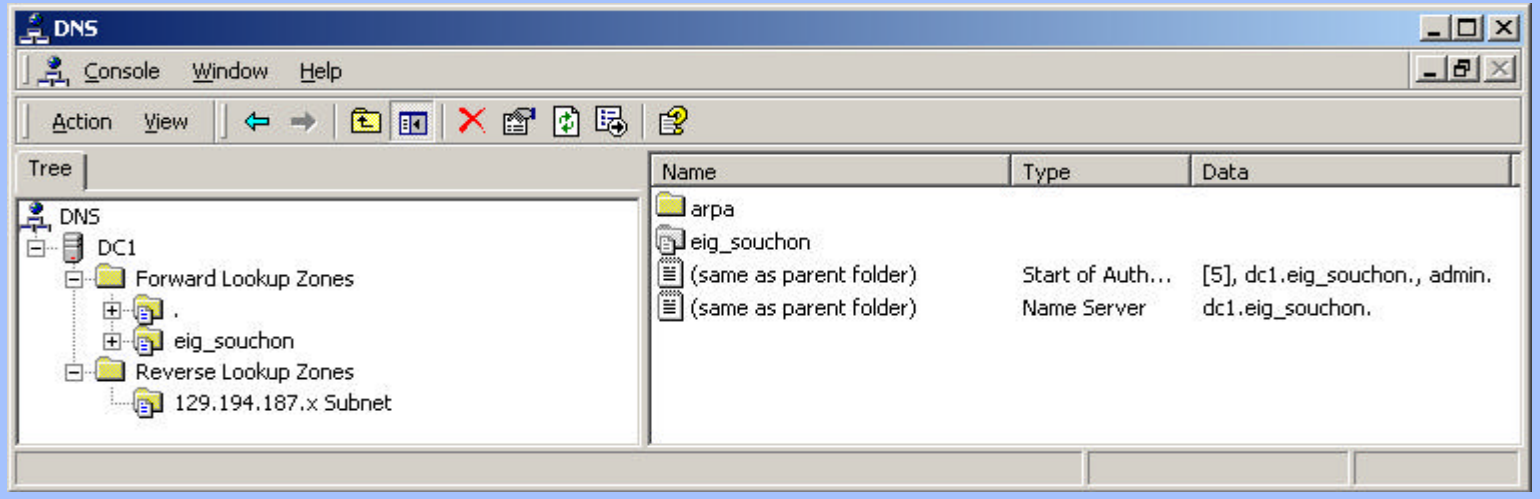


Etape 2.1 : *DNS*

e i g

Structure DNS





Etape 3 : *2 domaines dans 2 forêts*

e i g

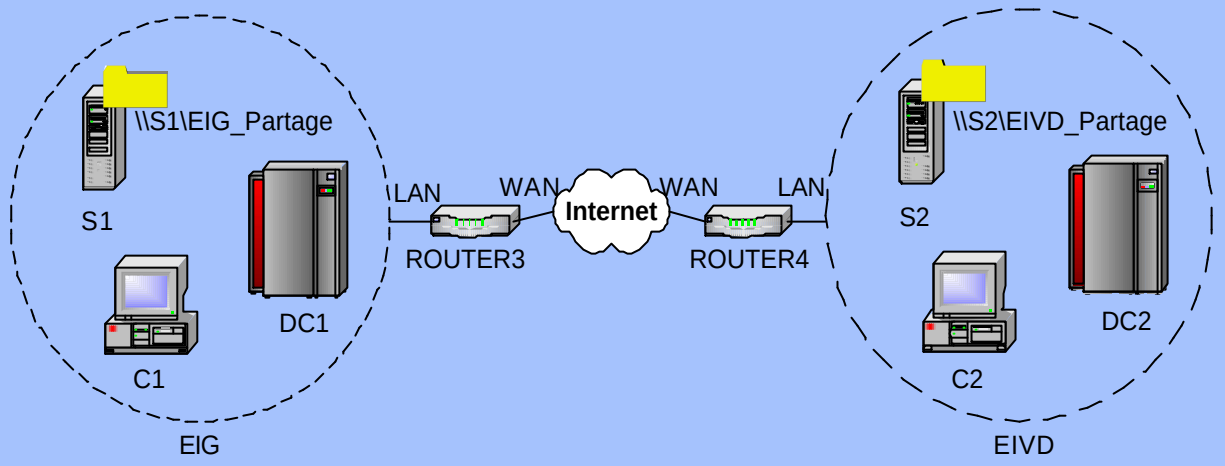
Objectifs

- 2 domaines avec 2 contrôleurs de domaine (*DC1*, *DC2*)
- 2 serveurs de fichiers avec chacun 1 répertoire partagé (*S1*, *S2*)
- 2 clients (*C1*, *C2*)
- 2 routeurs Lightning Ethernet II (*ROUTER3*, *ROUTER4*)
- 2 serveurs DNS dynamiques (*DNS1*, *DNS2*)
- 2 zones d'adressages privées de classe C
- Connexion à internet (NAT)

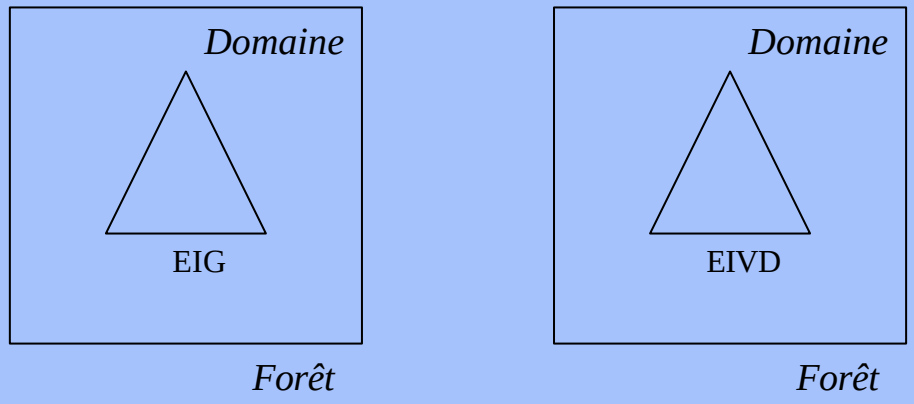
Etape 3 : *Structure physique / logique*

e i g

Structure physique



Structure logique

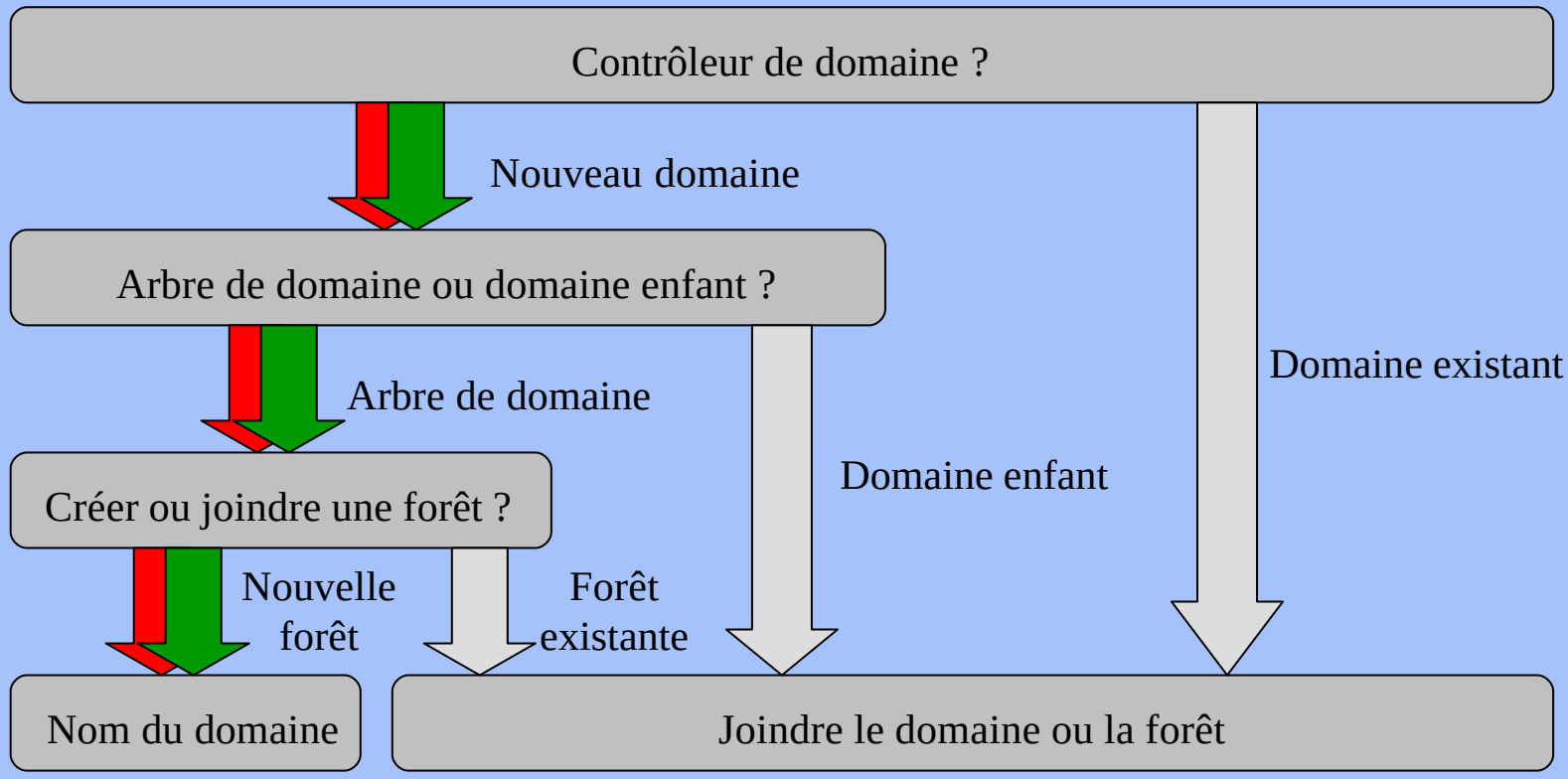


Etape 3 : *Configuration*

e i g

→ **Configuration de DC1**

→ **Configuration de DC2**

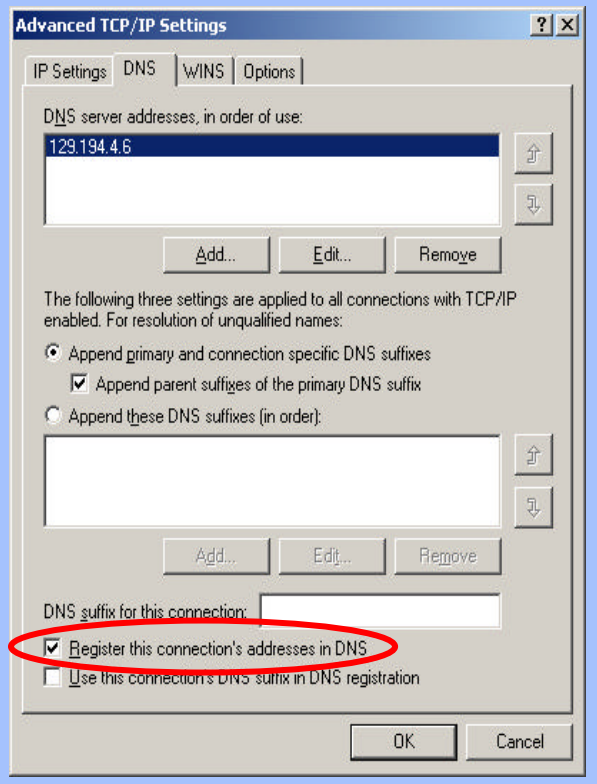


Etape 3.1 : *DNS*

e i g

Nouveautés

- *SRV record type*
  - Localise un service au moyen du serveur DNS
  - RFC 2052
  - **Exemple** : localisation du contrôleur de domaine
- *Dynamic DNS (DDNS)*
  - Simplifie l'administration
  - RFC 2136
  - **Exemple** : mise à jour du DNS directement par le client

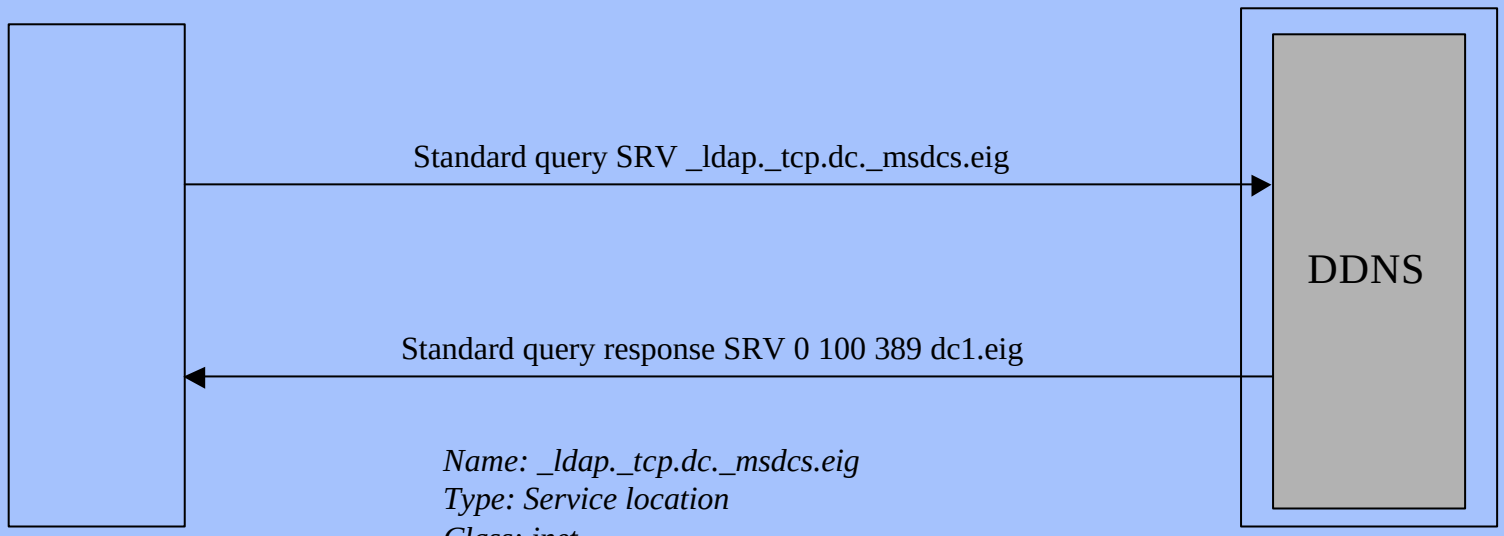


Etape 3.1 : *DNS (2)*

e i g

Exemple : *C1 localise le contrôleur de domaine (AD)*

_Service._Proto.Name TTL Class SRV Priority Weight Port Target

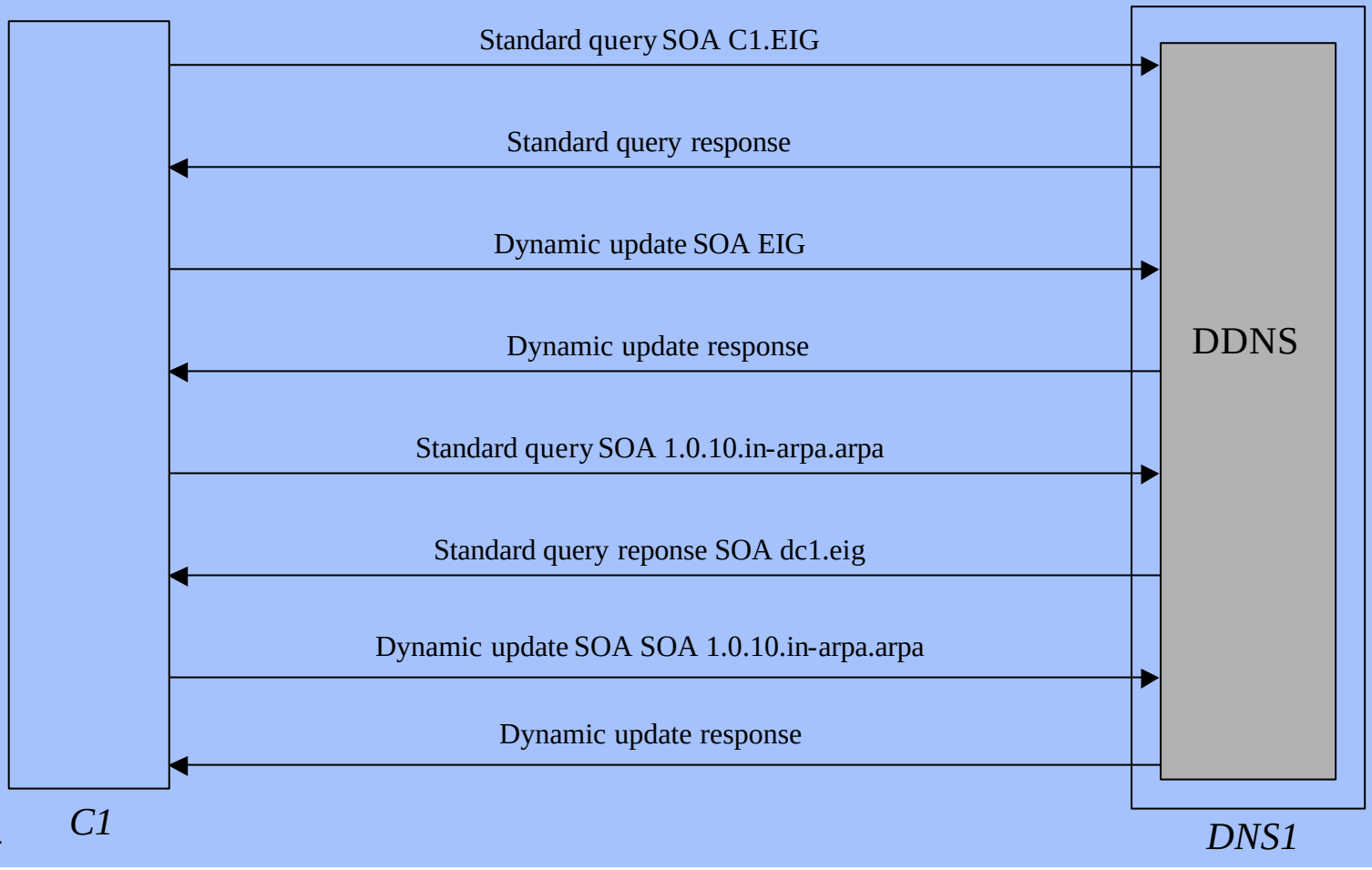


Name: _ldap._tcp.dc._msdcs.eig
Type: Service location
Class: inet
Time to live: 10 minutes
Priority: 0
Weight: 100
Port: 389
Target: dc1.eig

Etape 3.1 : *DNS (3)*

e i g

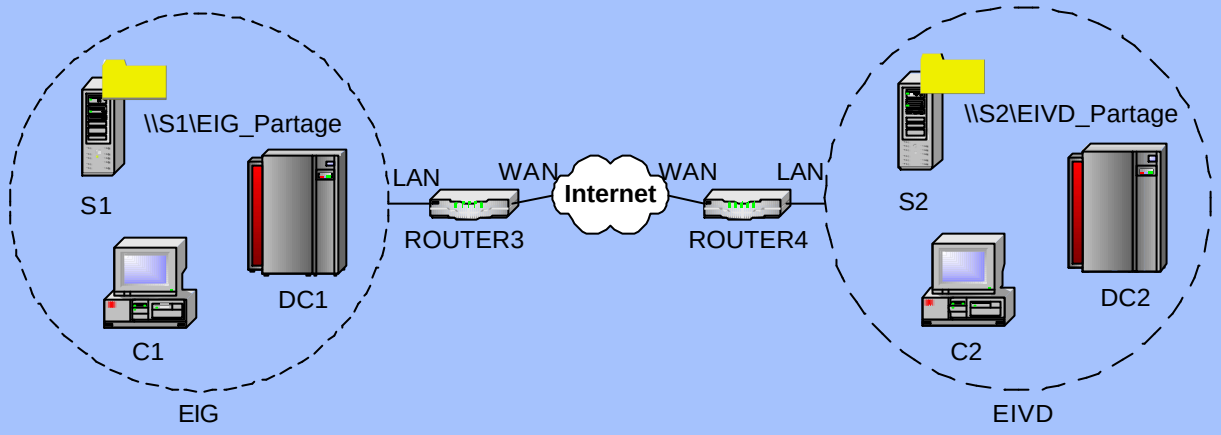
Exemple : *C1 s'enregistre dynamiquement*



Etape 3.1 : *DNS (4)*

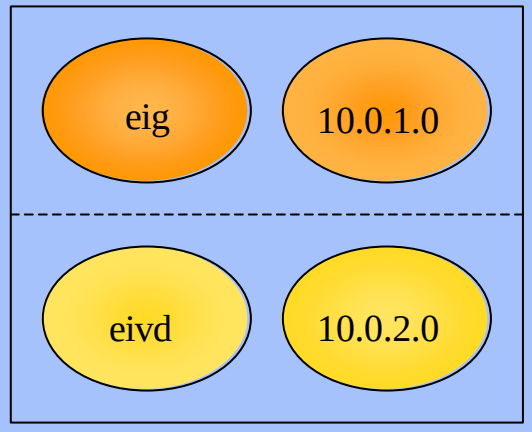
e i g

Configuration des serveurs DNS

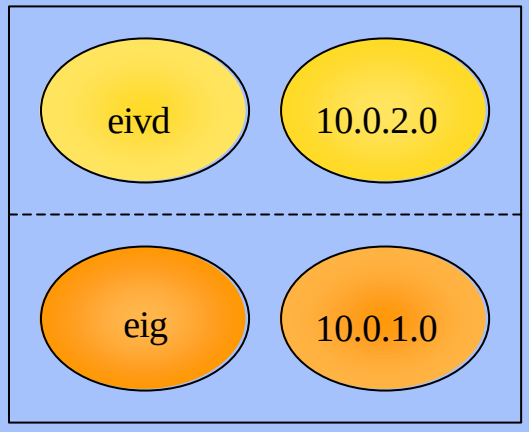


Zones primaires

Zones secondaires



DNS1



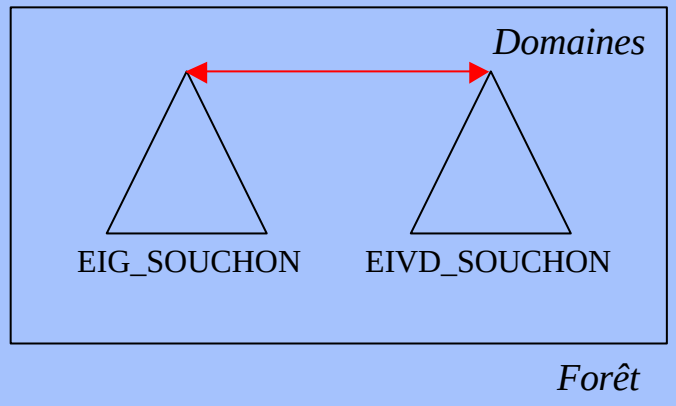
DNS2

Etape 3.2 : *Trust*

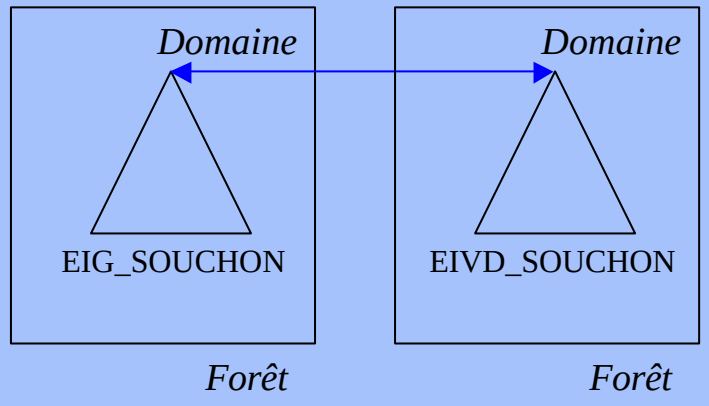
e i g

- 2 types de trust (relations d'approbations) :

Trust implicite

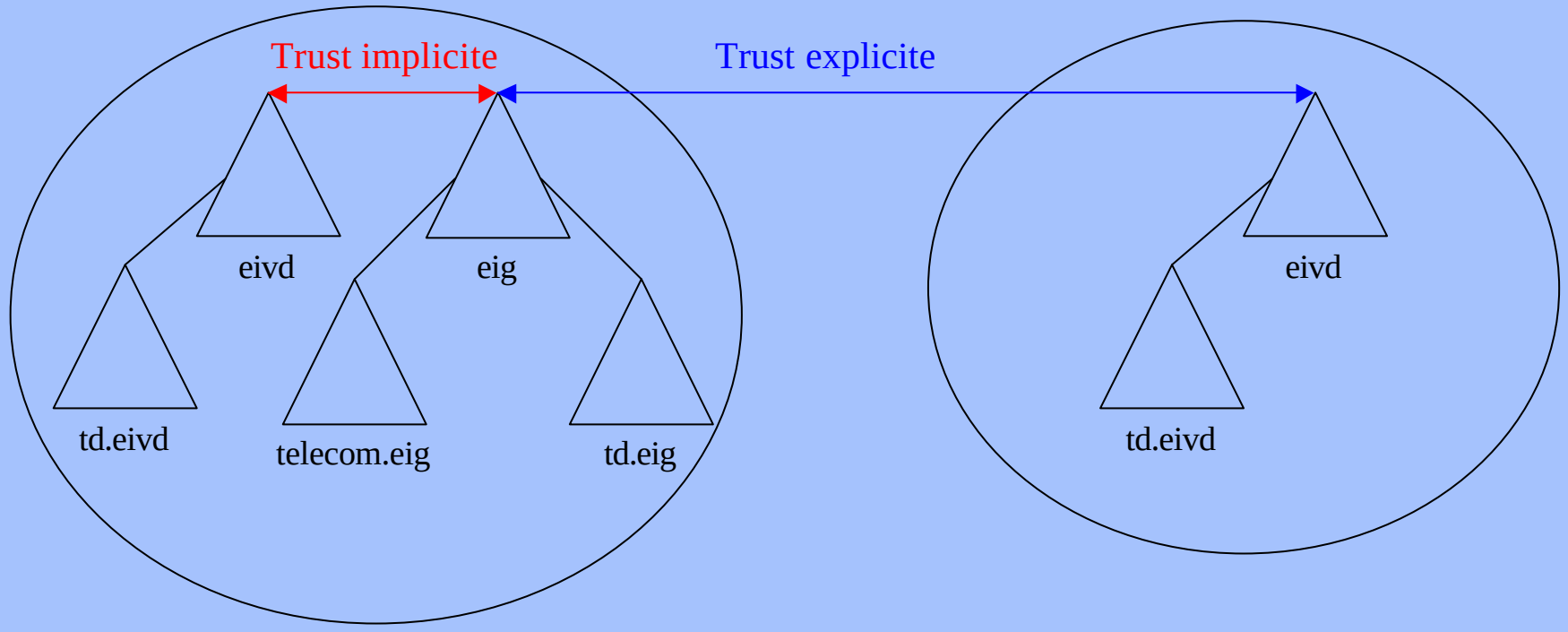


Trust explicite



Etape 3.2 : *Trust (2)*

e i g



→ Démonstration 3 : Authentification

Conclusion

e i g

- Grande souplesse grâce à Active Directory
- Possibilité de désativer NetBIOS
- Protocoles propriétaires
- Encore peu d'entreprises utilisent Windows 2000. Il faut attendre une maturité plus importante (*Service Pack 3)*

Conclusion (2)

e i g

- Théorie
  - Active Directory : 1½ semaines
  - DNS : 1 semaine
- Configuration
  - Etape 1 : 2 semaines
  - Etape 2 : 2½ semaines
  - Etape 3 : 2 semaines
  - Etape 4 : 1½ semaines
- Documentation abondante

Questions