CHAPITRE III

QUELQUES SERVICES RESEAU

DETAILS DU PLAN

CHAP. III. LES SERVICES RESEAU

1. Annuaire Active Directory
2. Résolution des noms (LLMNR et DNS)
3. Configuration automatique d'adresses IP (DHCP)
4. Service de fichiers (SMB et RPC, FTP et TFTP)
5. Messagerie (SMTP, POP, IMAP)

DETAILS DU PLAN

CHAP. III. LES SERVICES RESEAU

1. Annuaire Active Directory
2. Résolution des noms (LLMR et DNS)
3. Configuration automatique d'adresses IP (DHCP)
4. Service de fichiers (SMB et RPC)
5. Messagerie (SMTP, POP, IMAP)

CHAP. III. LES SERVICES RESEAU

ANNUAIRE

Un annuaire d'entreprise, c'est comme l'annuaire téléphonique, à ceci près qu'il gère plus de choses. Regardons les caractéristiques de l'annuaire téléphonique pour mieux comprendre le concept :

- Il **liste des données** (nom, prénom, numéro de téléphone, adresse)
- Il **organise ces données** (/département/villes/nom)
- Il offre un **moyen de consultation** (en ligne, appli smartphone, format papier)
- Il peut **protéger les données** (liste noir)
- Il est **disponible** de manière permanente

CHAP. III. LES SERVICES RESEAU

ANNUAIRE / QUID ???

- *Un annuaire est une source d'informations utilisée pour stocker des informations sur certains objets importants.*

Dans un système de fichiers, le répertoire (l'annuaire) contient des informations sur des fichiers. Dans un système d'informatique distribuée ou un réseau informatique public comme Internet, il existe de nombreux objets intéressants, comme des imprimantes, des serveurs de télécopie, des applications, des bases de données et d'autres utilisateurs. Les utilisateurs des réseaux veulent trouver et utiliser ces objets, et les administrateurs veulent contrôler leur utilisation.

CHAP. III. LES SERVICES RESEAU

ANNUAIRE =/= Base de données

- **on lit plus souvent** un annuaire qu'on ne le met à jour. Contrairement à un SGBD, un annuaire n'est pas fait pour stocker des informations constamment en mouvement. Il est logique de le structurer différemment et d'organiser les données de manière arborescente (sur un SGBD, la structuration est relationnelle).

CHAP. III. SERVICES RESEAU

ANNUAIRE : LDAP

- Dans l'entreprise, les applications et les serveurs ont besoin des données pour l'authentification, les droits d'accès... autant d'informations difficiles à maîtriser car très volatiles.
- Les annuaires LDAP offrent une réponse à ce problème en proposant de centraliser les informations et, par le biais d'un protocole standardisé, d'y connecter des applications clientes.

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Historique

- Vers les années 1988, l'ITU crée la norme X.500 que l'ISO/IEC publie par la suite. X.500 définit le modèle de données employé par les services d'annuaire. Dans ce modèle, toutes les données d'un annuaire sont stockées dans des rubriques (entrées). Le protocole utilisé pour accéder aux infos des annuaires était le protocole DAP (Directory Access Protocol). Or il est complexe à mettre en œuvre. L'Université du Michigan réfléchit alors à un moyen de pallier à ces problèmes, tout en reprenant les concepts. LDAP est né. Il devient un protocole natif et utilisable indépendamment de X.500. Début 1996 Netscape prend la tête d'une coalition pour promouvoir l'usage de LDAP.

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Historique

Note !!! Aucun service d'annuaire existant n'implémente entièrement la norme X.500, mais tous s'appuient sur ses spécifications fondamentales.

CHAP. III. SERVICES RESEAU

ANNUAIRE : LDAP

- LDAP est un protocole, dont l'acronyme est "Lightweight Directory Access Protocol" (Protocole d'accès à l'annuaire léger) et fonctionne (par défaut) sur le port TCP 389 pour LDAP et 636 pour LDAPS (LDAP over TLS/SSL).
- C’est un protocole de la couche Application (7) du modèle OSI. Il est conçu pour fonctionner au-dessus de TCP, lui même au-dessus d'IP. Par conséquent, les communications avec un annuaire LDAP sont en mode connecté, et les paquets échangés ont une garantie d'intégrité.

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP

LDAP est un protocole réseau pour obtenir des informations sur des objets tels que les utilisateurs de l'entreprise.

De nombreux logiciels (comme les logiciels de messagerie) interrogent un service LDAP afin de récupérer ces informations (notamment les listes de distribution et les adresses email).

L'annuaire LDAP conçu par Microsoft se nomme « Active Directory » (AD)

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP

De nombreux services applicatifs de l'entreprise (ERP, CRM, CMS, sites Web …) nécessitent une authentification.

On peut bien entendu recréer les comptes dans ces applications.

Il vaut mieux configurer ces applications (si elles le permettent) de manière à ce qu'elles valident l'authentification sur notre annuaire LDAP afin de ne rien recréer et centraliser les mots de passe. On peut alors envisager les fonctionnalités Single Sign-on (SSO).

Bien sûr, ce mécanisme est intrinsèque dans un produit Microsoft.

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Principe de Fonctionnement

Les modèles LDAP représentent les services que propose le serveur au client. Bien que la RFC 2251 sépare l'annuaire LDAP en 2 composants : le modèle de données et le modèle de protocole, définissons-le en 4 comme Timothy A. Howes, Mark C. Smith, et Gordon S. Good dans leur livre *Understanding and Deploying LDAP Directory Services* :

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Principe de Fonctionnement

- Le **modèle de nommage** définit comment l'information est stockée et organisée
- Le **modèle fonctionnel** définit les services fournis par l'annuaire (recherche, ajout, ...)
- Le **modèle d'information** définit le type d'informations stockées
- Le **modèle de sécurité** définit les droits d'accès aux ressources

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle de Nommage

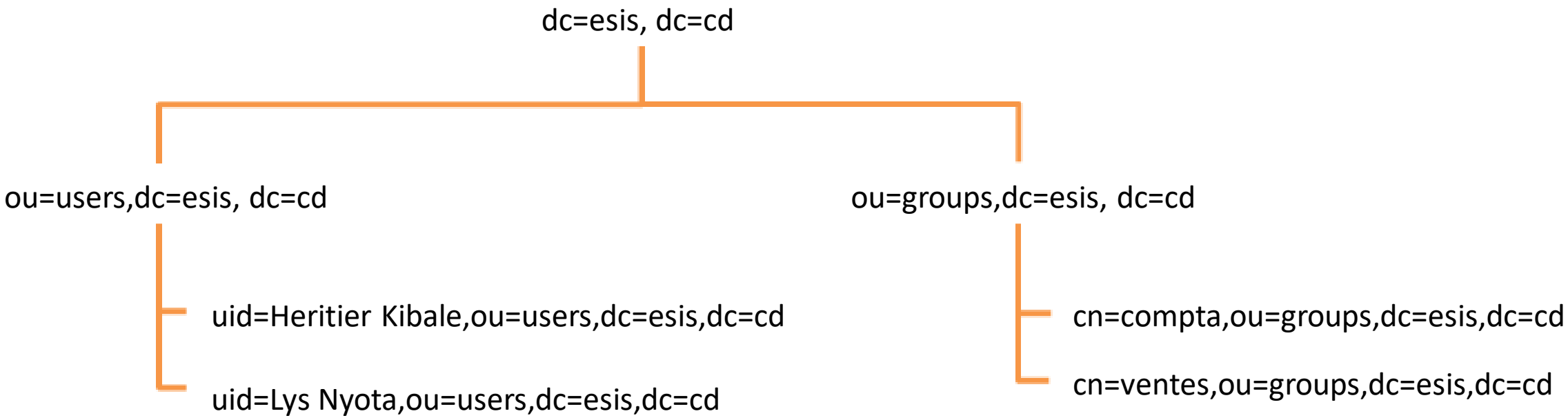
Le modèle de nommage est la manière dont sont organisées les données dans l'annuaire.

Un annuaire a une représentation hiérarchique des données. Ceci signifie que toutes les informations découlent d'une seule et même "racine".

Voici un exemple d'arborescence LDAP pour une société, qui a 2 utilisateurs, Lys Nyota et Heritier Kibale, et 2 groupes, compta et ventes.

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle de Nommage



CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle de Nommage

Cette arborescence est liée au nommage de chaque élément. Un élément marque son appartenance à l'élément supérieur en reprenant le nom, qu'il complète par le sien.

Par exemple, si on prend "*cn=ventes,ou=groups,dc=esis,dc=cd*", on a *ventes > groups > esis.cd*

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle de Nommage

La racine choisie ici est composée du nom du domaine où est hébergé notre serveur LDAP, esis.cd, décomposé en "dc" (Domain Components) pour obtenir dc=esis,dc=cd. L'arbre se découpe ensuite en deux *"ou"* (Organisational Units) qui constituent deux branches : *"users"* et *"groups"*, dans lesquels nous trouvons ensuite les entrées (feuilles) de notre arbre, les utilisateurs et les groupes.

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle de Nommage

C'est une convention que sur un annuaire LDAP la racine soit toujours composée des attributs *"dc"* (Domain Component) associés à chacune des parties du nom de domaine où est hébergé le serveur ("dc=esis,dc=cd").

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle de Nommage

Chaque élément est appelé une **entrée** (*an entry*). Une entrée peut être une branche (*a node*) ou un élément terminal (a leaf).

Une entrée est constituée d'un ensemble d'attributs. Un **attribut** possède un nom, un type et une ou plusieurs valeurs. Les attributs sont définis dans des schémas et sont l'une des caractéristiques de cet élément.

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle de Nommage

- La racine est l'élément supérieur de tous les autres, c'est la base de l'arborescence : *dc=esis,dc=cd*

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Règle de Nommage

La RFC 2253 normalise l'écriture des DN et conseille de ne pas ajouter d'espaces autour du signe "=", ni à la fin du DN. Les espaces sont autorisés par contre pour les valeurs des entrées.

DN correct : uid=Heritier Kibale,cn=ventes,ou=groups,dc=esis,dc=cd

DN incorrect : uid = Heritier Kibale, cn = ventes, ou = groups, dc = esis, dc = cd

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle Fonctionnel

- **La base** est le DN à partir duquel on peut faire une recherche. Par exemple "*dc=esis,dc=cd*" effectuerait une recherche sur tout l'arbre, puisqu'il s'agit de la racine.
- Le scope est le nombre de niveaux sur lesquels l'action va être effectuée. Il existe 3 niveaux différents que nous ne verrons pas ici.

CHAP. III. SERVICES RESEAU

ANNUAIRE LDAP : Modèle de Sécurité

Un annuaire LDAP (Active Directory) participe pleinement à l'infrastructure de sécurité. Le modèle de sécurité distribué s'appuie sur le protocole d'authentification Kerberos (Version 5) du MIT. L'authentification Kerberos est compatible avec la sécurité fondée sur des couples de clés privée/publique. Elle utilise le modèle d'ACL (Access Control List). Les ACL protègent tous les objets d'Active Directory. Elles déterminent qui peut visualiser l'objet et ses attributs, qui peut faire quoi sur l'objet, etc. L'utilisateur qui n'a pas la permission de voir un objet ou un attribut ne saura même pas que celui-ci existe.

Terminologies et concepts d'Active Directory

Domaine :

Selon Microsoft, un domaine est une entité logique vue comme une enveloppe étiquetée. Il reflète le plus souvent une organisation hiérarchique dans une entreprise. Par exemple, le domaine "COMPTA" désigne l'ensemble des machines réseau (stations, imprimantes, etc.) du service Comptabilité, et les comptes utilisateurs qui sont autorisés à s'y connecter.

Le domaine permet à l'administrateur système de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données.

Terminologies et concepts d'Active Directory

Domaine :

Le domaine Windows sert (dans un premier temps) à centraliser les comptes (et donc leurs mots de passe).

Le stockage de ces comptes est assuré par au moins 1 serveur Windows (de préférence au moins 2 qui seront répliqués).
On peut regrouper les comptes dans des objets de type Groupe.
Ce domaine s'appellera l'Active Directory, il stocke des objets (de types divers), et nous verrons qu'il sert à d'autres choses que l'authentification centralisée.

Terminologies et concepts d'Active Directory

Espace de noms et résolution de noms :

N'importe quelle zone délimitée au sein de laquelle un nom donné peut être résolu constitue un espace de noms.

Chaque service d'annuaire est un espace de noms, une aire bien délimitée permettant de résoudre un nom (Active Directory y compris).

La résolution de nom consiste à passer d'un nom à l'objet ou l'information que ce nom représente.

Terminologies et concepts d'Active Directory

Espace de noms et résolution de noms :

N'importe quelle zone délimitée au sein de laquelle un nom donné peut être résolu constitue un espace de noms.

Les programmes de télévision, dans lesquels le nom d'une chaîne est associé à un certain numéro de canal, constituent un exemple d'espaces de noms, de même que le système de fichiers d'un ordinateur, dans lequel le nom d'un fichier est associé au fichier lui-même.

Un annuaire téléphonique constitue un espace de noms dans lequel les noms des abonnés peuvent être résolus en numéros de téléphone.

Terminologies et concepts d’Active Directory

Espace de noms et résolution de noms :

Active Directory constitue un espace de noms dans lequel le nom d'un objet de l'annuaire peut être résolu pour obtenir l'objet lui-même.

Terminologies et concepts d’Active Directory

Objet :

Un objet est un ensemble d'attributs nommé et circonscrit qui représente un élément concret, comme un utilisateur, une imprimante ou une application.

Un attribut est un élément de données qui décrit un certain aspect d’un objet.

Un attribut se compose d’un type et d’une ou plusieurs valeurs.

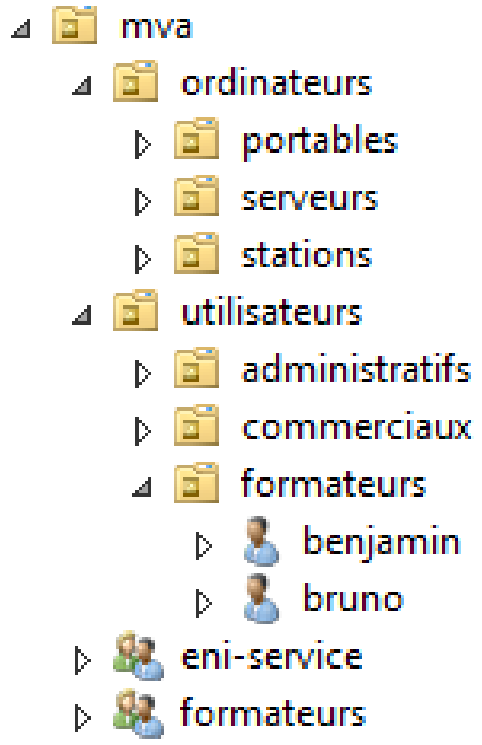
Les attributs comportent des données qui décrivent l’entité identifiée par l'objet de l'annuaire. Les attributs d'un utilisateur, par exemple, peuvent être son prénom, son nom, son numéro de téléphone et son adresse électronique.

Terminologies et concepts d'Active Directory

Unité d'organisation (conteneur) :

Une unité d'organisation est semblable à un objet dans la mesure où il possède des attributs et fait partie de l'espace de noms de Active Directory. Toutefois, contrairement à un objet, il ne représente rien de concret. Ce n'est qu'une enveloppe qui renferme un ensemble d'objets et d'autres conteneurs.

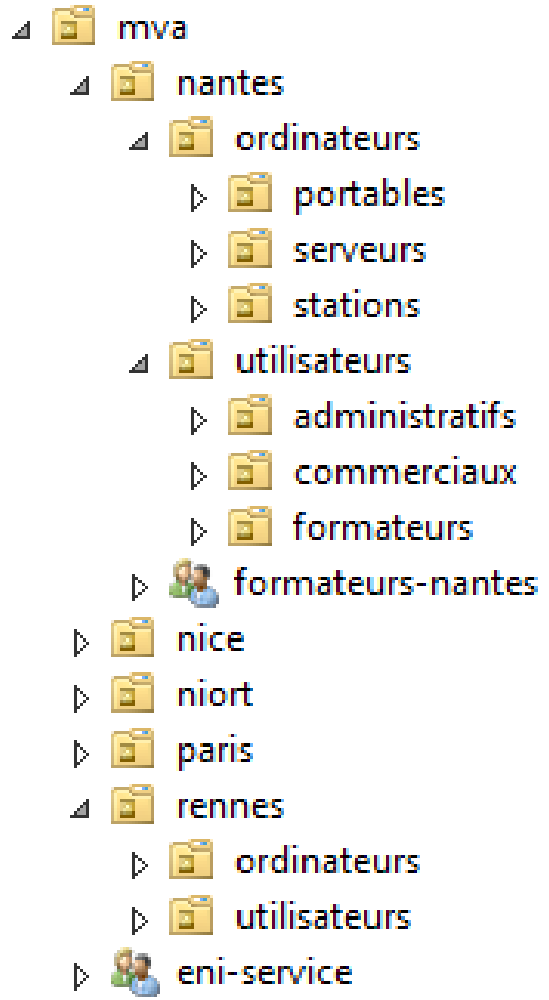
Les unités d'organisation servent à «ranger» de manière hiérarchique les nombreux objets à gérer dans l'AD.



Terminologies et concepts d'Active Directory

Unité d'organisation (conteneur) :

La hiérarchie devra refléter l'organisation fonctionnelle de l'entreprise mais on peut y adjoindre une notion géographique.



Terminologies et concepts d'Active Directory

Arborescence (ou arbre) :

C'est une hiérarchie d'objets et de conteneurs qui montre les relations entre les objets, c-à-d les chemins par lesquels on passe d'un objet à un autre. Les points terminaux (feuilles) d'un arbre (arborescence) sont, en général, des objets.

Les nœuds de l'arbre (endroits d'où partent les branches) sont des conteneurs.

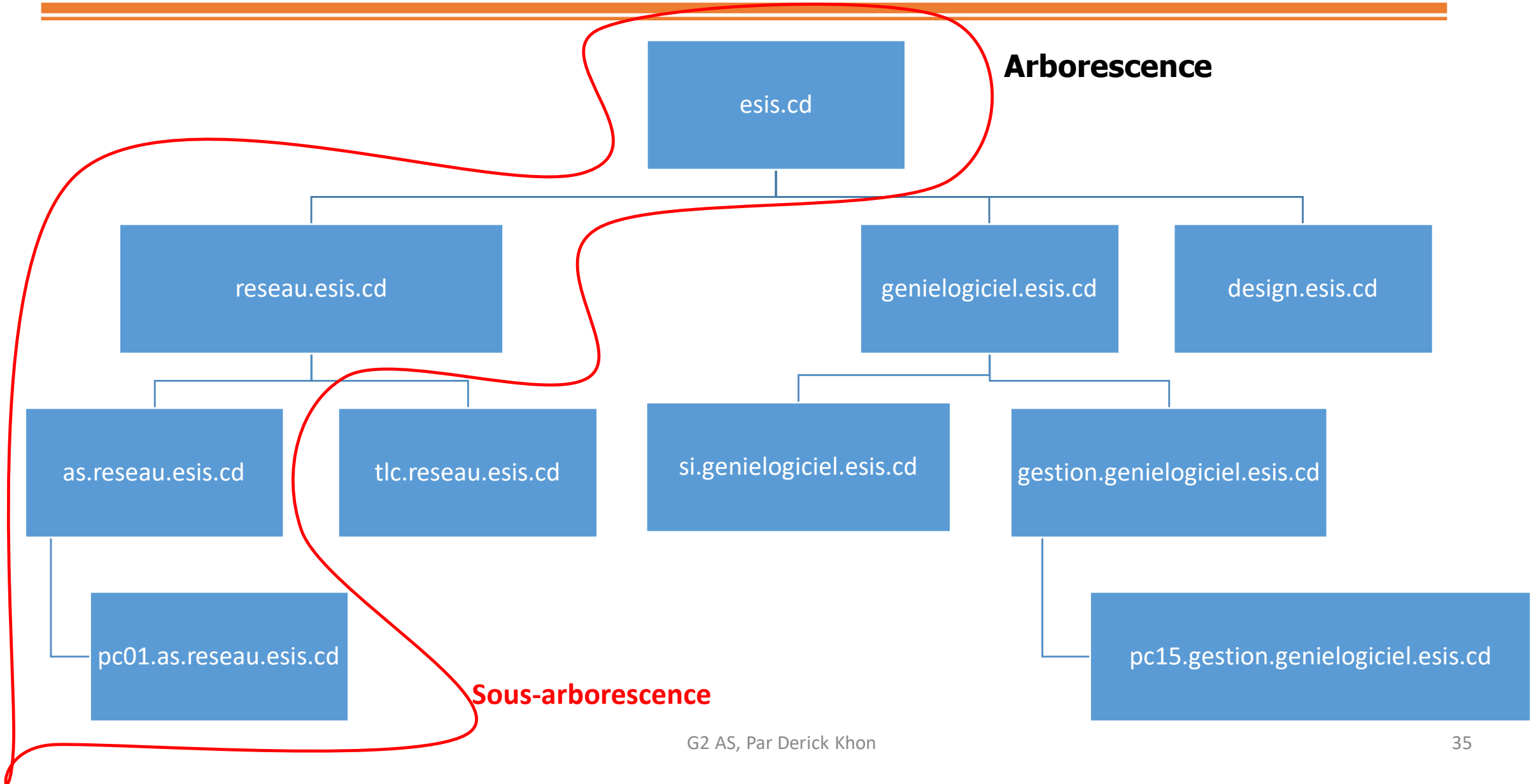
Terminologies et concepts d'Active Directory

Sous-arborescence :

C'est un sous-ensemble non isolé de l'arborescence, contenant tous les membres de chacun des conteneurs qu'il renferme.

La figure ci-dessous montre une arborescence pour esis.cd. Chaque chemin (par ex. de pc01.as.reseau.esis.cd à esis.cd) est une sous-arborescence.

Terminologies et concepts d'Active Directory



CHAP. III. SERVICES RESEAU

Nom unique ou DN

- Chaque objet possède un nom unique ou **DN** (*Distinguished Name*). Le DN est le chemin complet utilisé pour atteindre l'objet à travers la hiérarchie des conteneurs. Il permet à l'objet d'être positionné dans l'arborescence. Il est unique dans l'annuaire.

Par ex. *cn=Lys Nyota, ou=Reseau, dc=esis, dc=cd* est un nom unique qui spécifie l'objet utilisateur « *Lys Nyota* » appartenant à l'OU « *Reseau* », elle-même appartenant au domaine « *esis.cd* ».

CHAP. III. SERVICES RESEAU

Nom relatif distinct ou RDN

- Chaque élément possède également un nom unique relatif ou **RDN** (*Relative Distinguished Name*). Le RDN est la partie du DN de l'élément qui est relative au DN supérieur. Le RDN d'un élément ne permet pas de l'identifier de manière unique dans l'annuaire

Dans l'exemple précédent, le RDN de l'objet utilisateur est *cn=Lys Nyota* et celui de l'objet parent est *« Reseau »*

CHAP. III. SERVICES RESEAU

Schéma

Dans Active Directory (AD), un schéma correspond à tout ce qui constitue l'annuaire Active Directory : les objets, les attributs, les conteneurs, etc.

AD possède un schéma par défaut qui définit les classes d'objets les plus courantes : Utilisateurs, groupes, ordinateurs, unités organisationnelles, stratégies de sécurité et domaines.

Un schéma AD est susceptible des modifications dynamiques.

CHAP. III. SERVICES RESEAU

Catalogue global

Un catalogue global est un contrôleur de domaine contenant une copie de tous les objets Active Directory d'une forêt. Il stocke une copie complète de tous les objets de l'annuaire de son domaine hôte, ainsi qu'une copie partielle de tous les objets des autres domaines de la forêt.

Il permet aux utilisateurs d'effectuer 2 tâches importantes :

- Trouver des informations Active Directory sur toute la forêt, quel que soit l'emplacement de ces données.
- Utiliser des informations d'appartenance à des groupes universels pour ouvrir une session sur le réseau.

RODC (Ready Only Domain Controller)

Si un contrôleur de domaine est physiquement situé à un endroit peu sécurisé, le risque de vol de ce dernier est fortement possible.

Tout contrôleur de domaine possède une copie (certes chiffrée) des mots de passe de tout le monde.

Le vol d'un contrôleur de domaine est donc une forte compromission de la sécurité de toute l'organisation.

C'est pour palier à ce problème qu'on peut installer un contrôleur de domaine en lecture seule (RODC) dans ces emplacements dangereux.

RODC (Ready Only Domain Controller)

Ce n’est pas le fait que le contrôleur de domaine est en lecture seule qui est le plus intéressant, mais le fait qu’il ne stocke pas la copie des mots de passe de tout le monde mais uniquement des utilisateurs que nous avons spécifiés (par défaut personne).

De plus en cas de compromission d’un RODC, il possible (et recommandé) de facilement réinitialiser les mots de passe stockés sur celui-ci.

CHAP. III. SERVICES RESEAU

Forêt

On appelle « **forêt** » le regroupement (par relations d'approbation) de plusieurs arbres possédant le même schéma mais ne possédant pas nécessairement le même espace de nom, afin par exemple de joindre les annuaires de deux entreprises.

CHAP. III. SERVICES RESEAU

Forêt

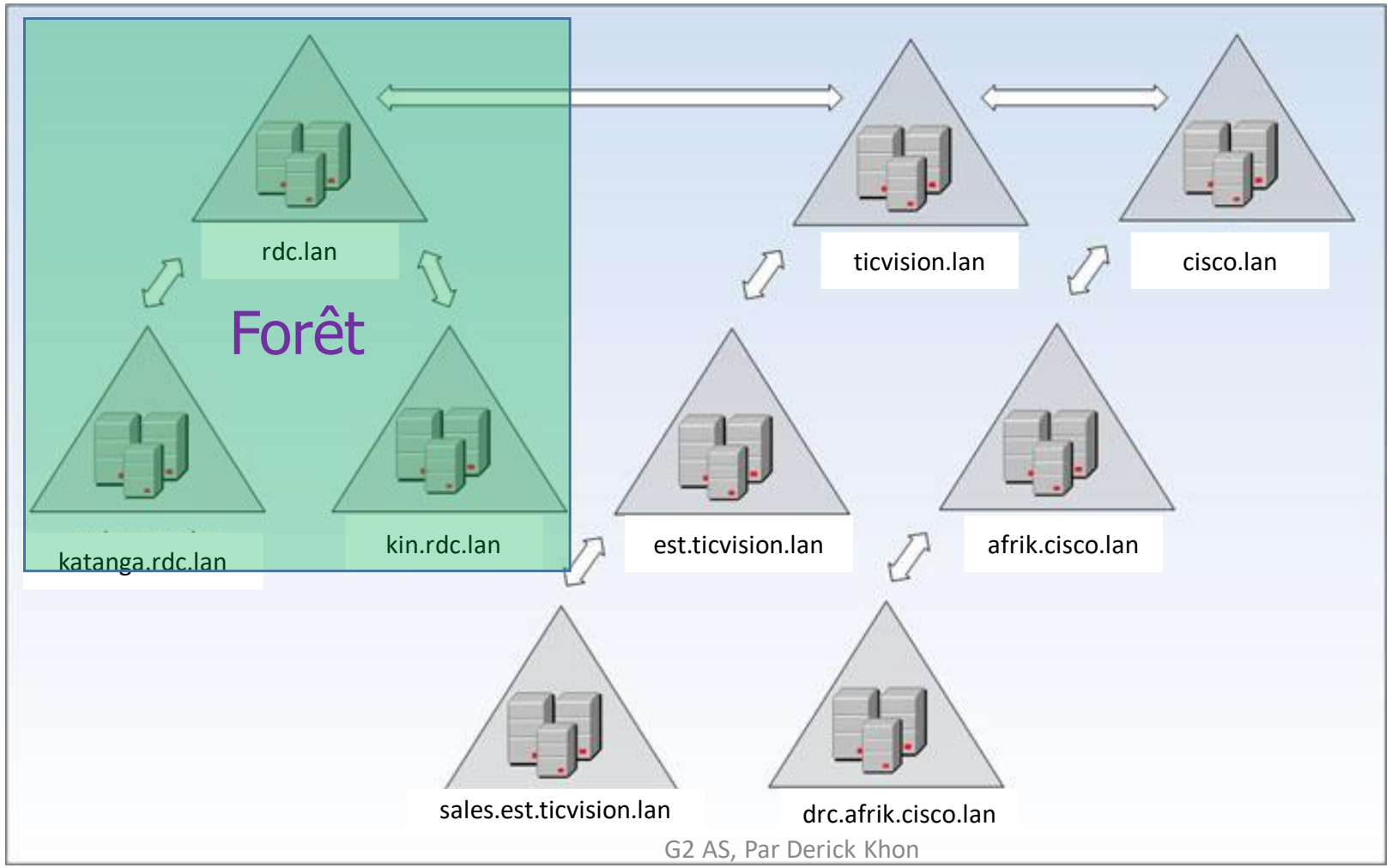
Une forêt Active Directory est la structure qui contient tout l'annuaire AD.

Elle est potentiellement constituée de plusieurs domaines. Mais, généralement, il faut essayer de réduire ce nombre de domaine au minimum (idéalement 1).

Il existe un lien entre les domaines d'une même forêt appelé «relation d'approbation bidirectionnelle transitive». Ces relations permettent à n'importe quel utilisateur d'un domaine d'ouvrir une session sur un ordinateur de n'importe quel domaine au sein de la même forêt.

CHAP. III. SERVICES RESEAU

Forêt



CHAP. III. SERVICES RESEAU

Forêt : Réplication

Il est possible d'avoir plusieurs contrôleurs de domaine pour un même domaine afin de mettre en place une tolérance de panne ainsi qu'une répartition de charge. Afin que tous les **DC** d'un domaine possède une base de donnée (**Active Directory**) à jour, une réplication des informations doit être effectuée entre chacun de ces serveurs.

CHAP. III. SERVICES RESEAU

Forêt : Relations d’approbation

Les relations d'approbation permettent à un utilisateur d'un domaine d'accéder aux ressources d'un autre domaine, et à un administrateur de pouvoir gérer les utilisateurs de l'autre domaine.

L'approbation parent-enfant entre domaines Windows 2008, 2003 ou 2000 est commutative et transitive.

CHAP. III. SERVICES RESEAU

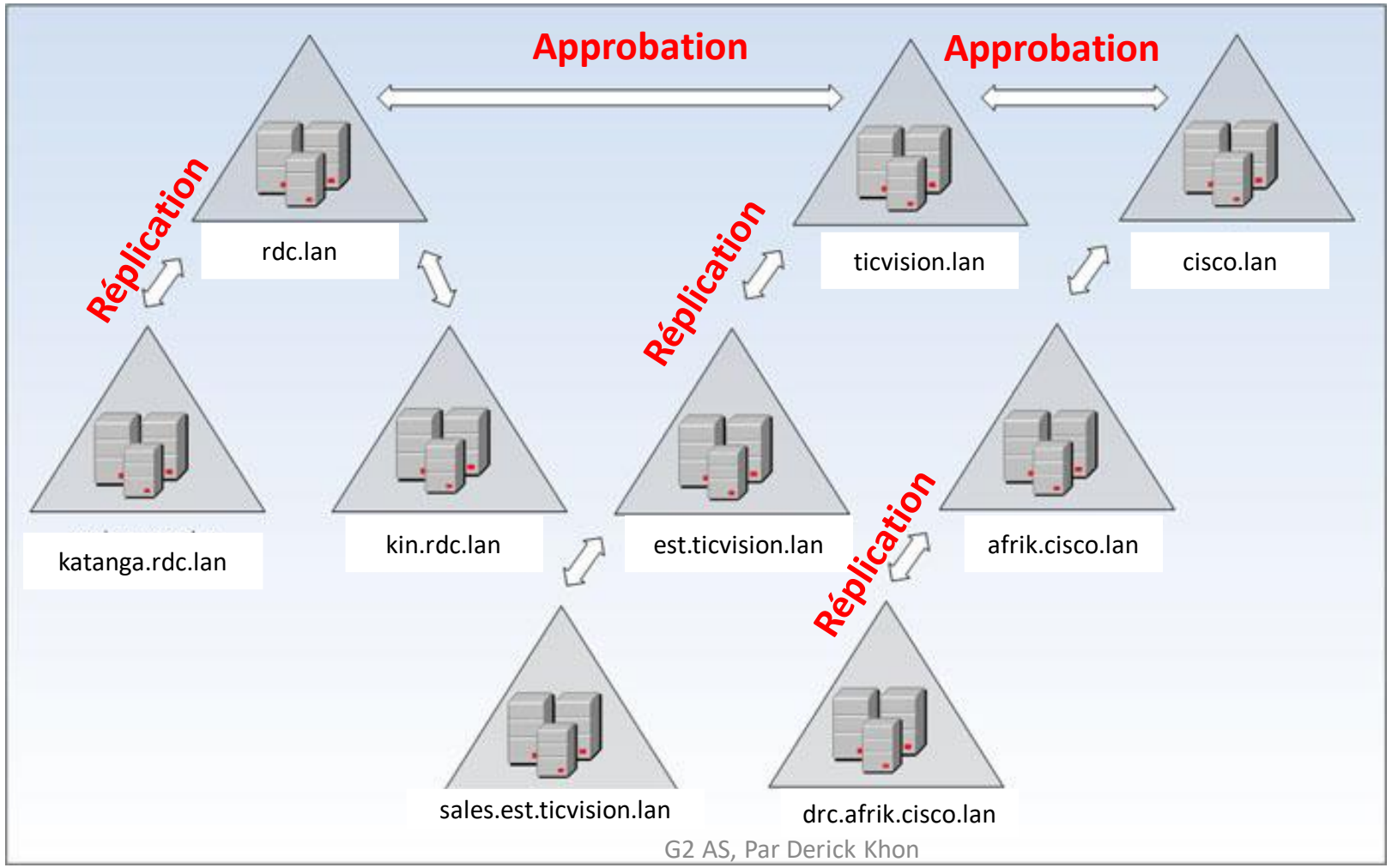
Forêt : Relations d'approbation

Une relation d'approbation est un mécanisme permettant aux utilisateurs authentifiés dans leur domaine de pouvoir accéder aux ressources d'un autre domaine.

Lorsque nous ajoutons un nouveau domaine enfant à un domaine déjà existant (par exemple nous ajoutons le domaine enfant « **reseau** » au domaine « **esis.lan**"), et bien il se configure automatiquement une relation d'approbation transitive bidirectionnelle entre les deux domaines.

CHAP. III. SERVICES RESEAU

Forêt



CHAP. III. SERVICES RESEAU

Sites

Sur un réseau physique, un site représente un ensemble d'ordinateurs connectés par un réseau haut débit, tel qu'un réseau local (LAN). En général, tous les ordinateurs du même site physique résident dans le même bâtiment, ou éventuellement sur le même campus de réseaux.

Dans les services AD DS, un objet de site représente les aspects du site physique que vous pouvez gérer, plus spécifiquement la réplication des données d'annuaire entre les contrôleurs de domaine.

CHAP. III. SERVICES RESEAU

Sites : Gestion d'agences

Par défaut, tous les contrôleurs de domaine sont dans le même site (appelé Default-First-Site-Name).

Cela signifie que la réplication des données d'annuaire entre ces contrôleurs de domaine se produit le plus souvent possible.

Le concept de site géographique est à paramétrer dans l'AD afin de pouvoir définir la fréquence voulue de réplication entre ces sites.

CHAP. III. SERVICES RESEAU

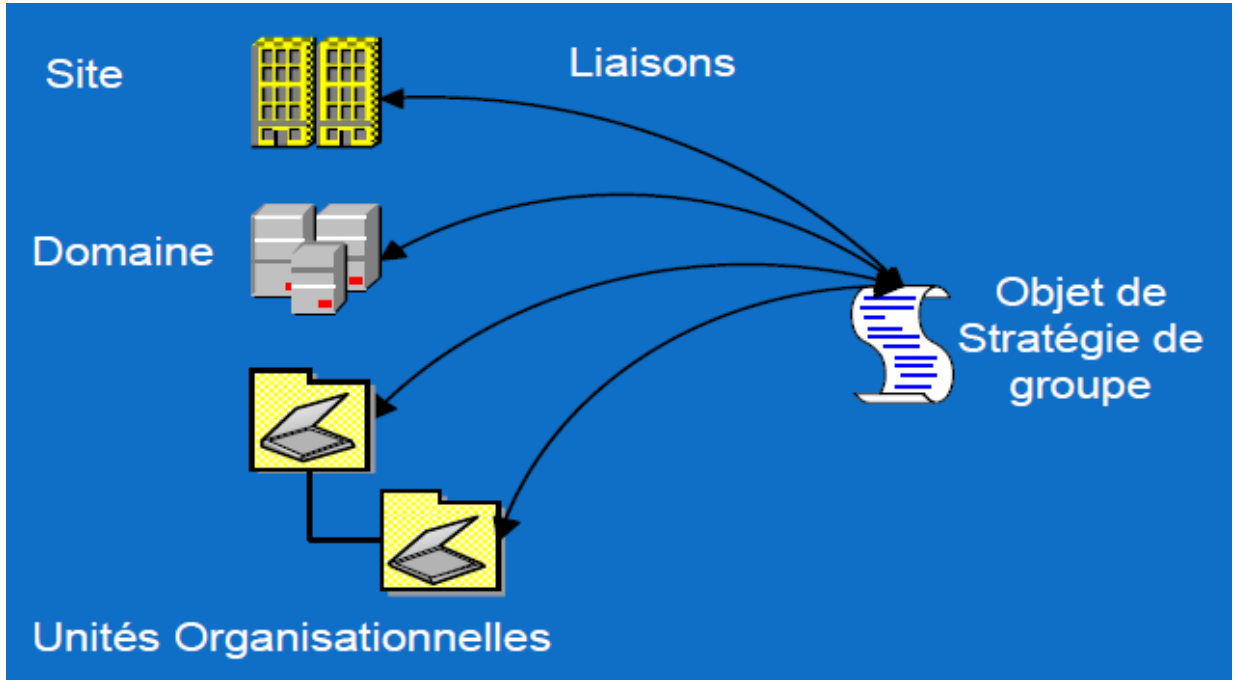
Stratégie de groupe (GPO)

- Les objets de stratégie de groupe (traduction littérale de «Group Policy Object» GPO) sont en fait des ensembles de paramètres visant à influencer certaines clés (et donc réglages) associées à un ordinateur et/ou un utilisateur.
- Elles consistent donc à IMPOSER certains réglages via l'AD et les GPO

CHAP. III. SERVICES RESEAU

GPO : Liaison

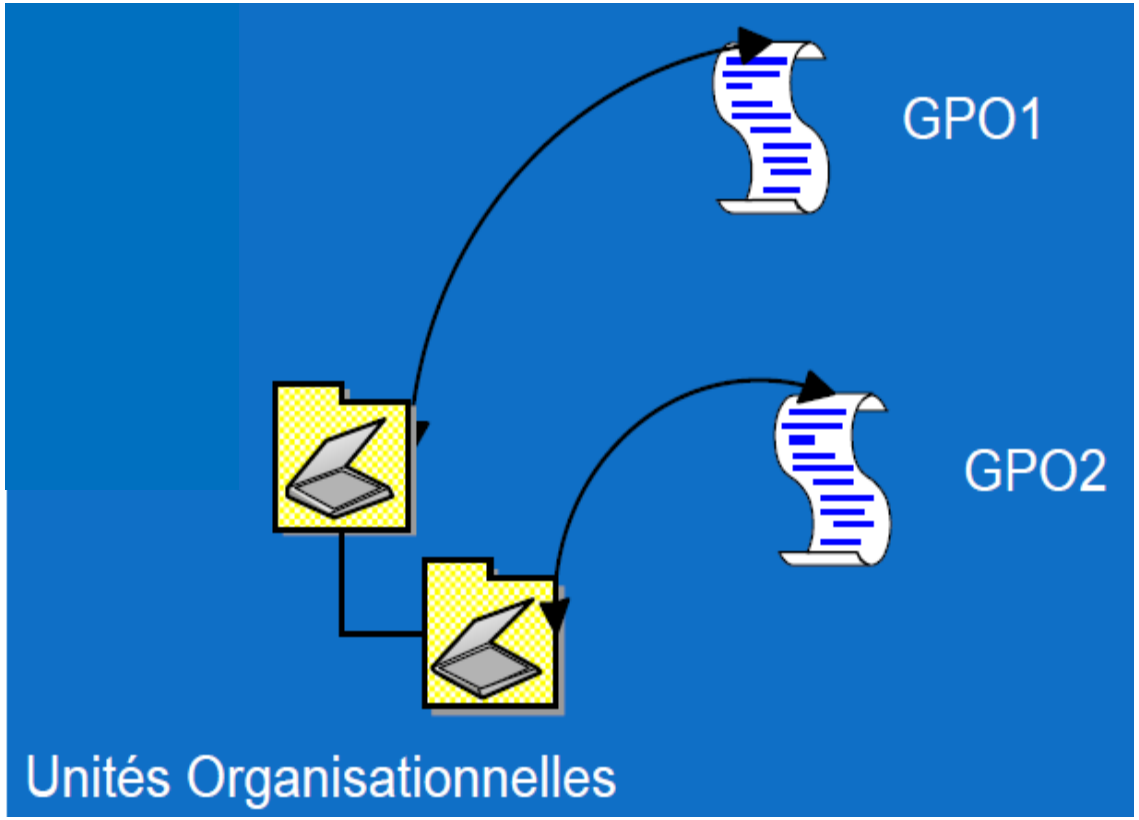
Un GPO est (en soi) un objet autonome contenant une configuration. Il faut l'appliquer à quelque chose grâce à une liaison.



CHAP. III. SERVICES RESEAU

GPO : Héritage et conflits

- Tous les objets utilisateurs et ordinateurs contenus dans les sous-OU héritent des GPO liées à des objets de niveau supérieur dans la hiérarchie Active Directory.
- S'il y a un conflit, c'est le paramètre en conflit du dernier GPO appliqué qui s'applique (c'est-à-dire le GPO lié à l'OU la plus proche de l'objet utilisateur ou ordinateur)



CHAP. III. LES SERVICES RESEAU

1. Annuaire Active Directory
2. Résolution des noms (LLMNR et DNS)
3. Configuration automatique d'adresses IP (DHCP)
4. Service de fichiers (SMB et RPC)
5. Messagerie (SMTP, POP, IMAP)

CHAP. III. SERVICES RESEAU

DNS : Introduction

- Il est connu que toutes les machines (ordinateurs, serveurs, routeurs, etc.) connectées à un réseau ou à Internet possèdent une adresse IP. nous savons, également que c'est cette adresse IP qui permet aux machines de communiquer entre elles.
- Cependant, cela va nous poser un petit problème. Nous avons beau être des êtres humains avec une bonne mémoire, mais notre cerveau n'est pas fait pour retenir des séries de chiffres comme 104.20.55.240. On aimerait mieux avoir à retenir des noms comme **esisalama.org**

CHAP. III. SERVICES RESEAU

DNS : Introduction

- Avoir un système DNS n'est donc pas un problème technique, un réseau informatique tel qu'Internet fonctionne très bien avec des adresses IP, mais cela est un problème de nommage pour permettre un accès simplifié à réseau informatique tel qu'Internet pour nous tous, pauvres êtres humains. Ce système de nommage est le **Domain Name System (DNS)**.

CHAP. III. SERVICES RESEAU

DNS : Introduction

- Le DNS est basé sur des mécanisme de résolution de noms. Un mécanisme de résolution de noms permet de traduire des noms en adresses IP et inversement.
- Avant, chaque machine stockait localement les mappages noms / adresse IP. Avec comme inconvénient une lourde charge administrative. En effet, à chaque ajout de machine dans le réseau ou bien à chaque modification de la configuration d'une machine, il faut éditer manuellement le fichier contenant les mappages noms / adresse IP.

CHAP. III. SERVICES RESEAU

DNS vs Netbios

- Le premier mécanisme de résolution de noms mis en place sous Windows est NetBIOS (NetBIOS Extended User Interface), un protocole créé par IBM dans les années 80. Cette méthode de résolution de noms possède de nombreux inconvénients :

CHAP. III. SERVICES RESEAU

DNS vs Netbios

- Les noms NetBIOS sont **limités à 16 caractères** (15 caractères pour le noms de la machine et un 16è caractère indiquant le type de services hébergés par la machine).
- Le protocole NetBIOS utilise la diffusion (ou broadcast) pour résoudre les noms en adresses IP ce qui **surcharge la bande passante** du réseau.
- Les noms NetBIOS ne possèdent pas de hiérarchie ce qui les rends **inutilisables sur Internet**.
- Le protocole NetBIOS n'est pas utilisé sur les plateformes non Microsoft ce qui pose un problème d'**interopérabilité**.

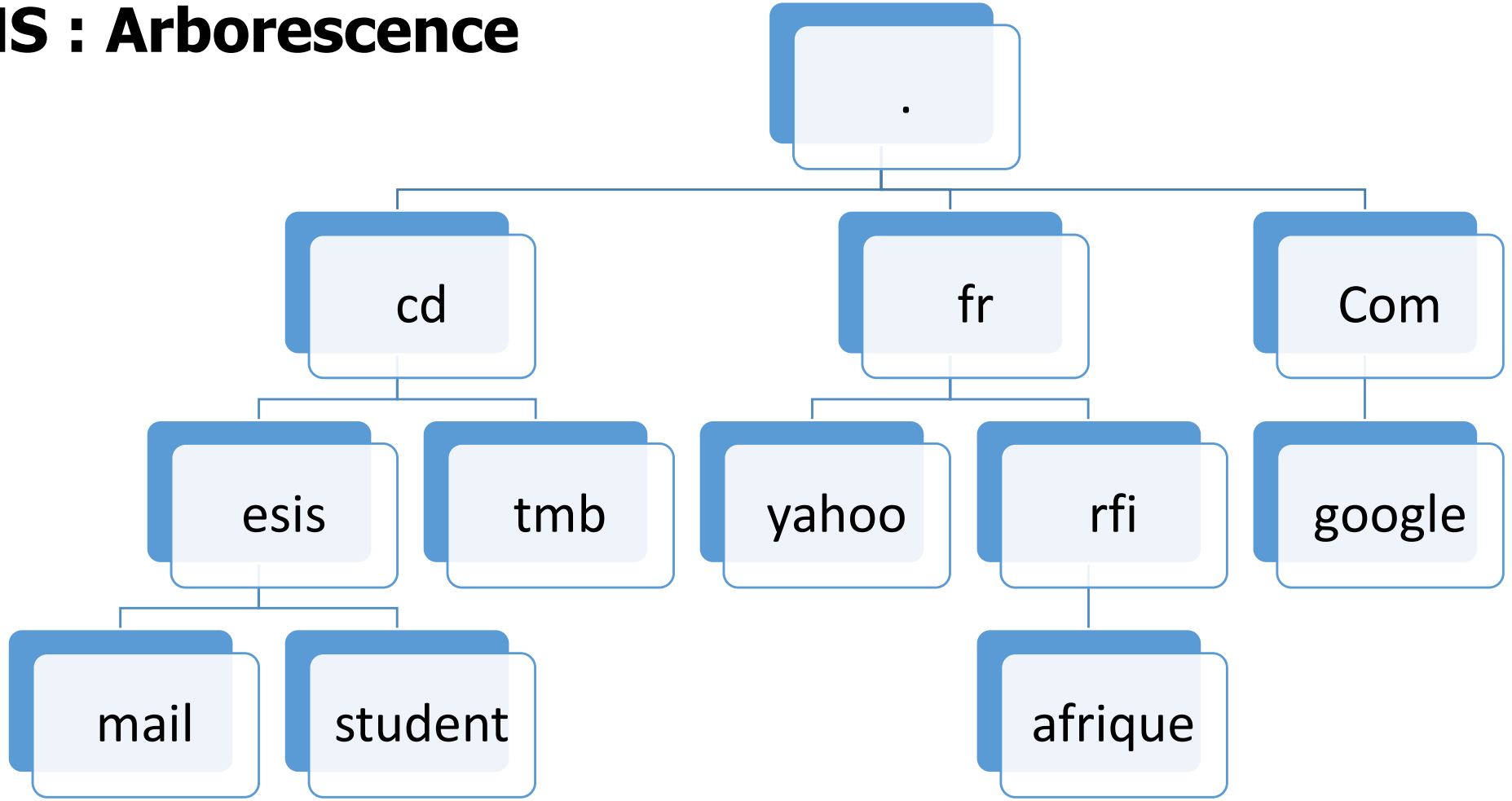
CHAP. III. SERVICES RESEAU

DNS : Présentation

- Le système DNS introduit **une convention de nommage hiérarchique** des domaines qui commence par un domaine racine appelé "**.**". Les domaines situés directement sous le domaine racine sont appelés domaines de premier niveau (Top Level Domain, TLD en anglais). Ils sont gérés par l'ICANN via l'IANA et représentent souvent la localisation géographique (fr, be, eu, cd ...) ou le type de service (com, info, org, gov, ...). Les domaines de second niveau sont disponibles pour les entreprises et les particuliers. (Le DNS utilise le port UDP/TCP 53)
- Enfin une multitude de sous domaines peuvent être créés à l'intérieur d'un domaine de second niveau.

CHAP. III. SERVICES RESEAU

DNS : Arborescence



DNS : Arborescence

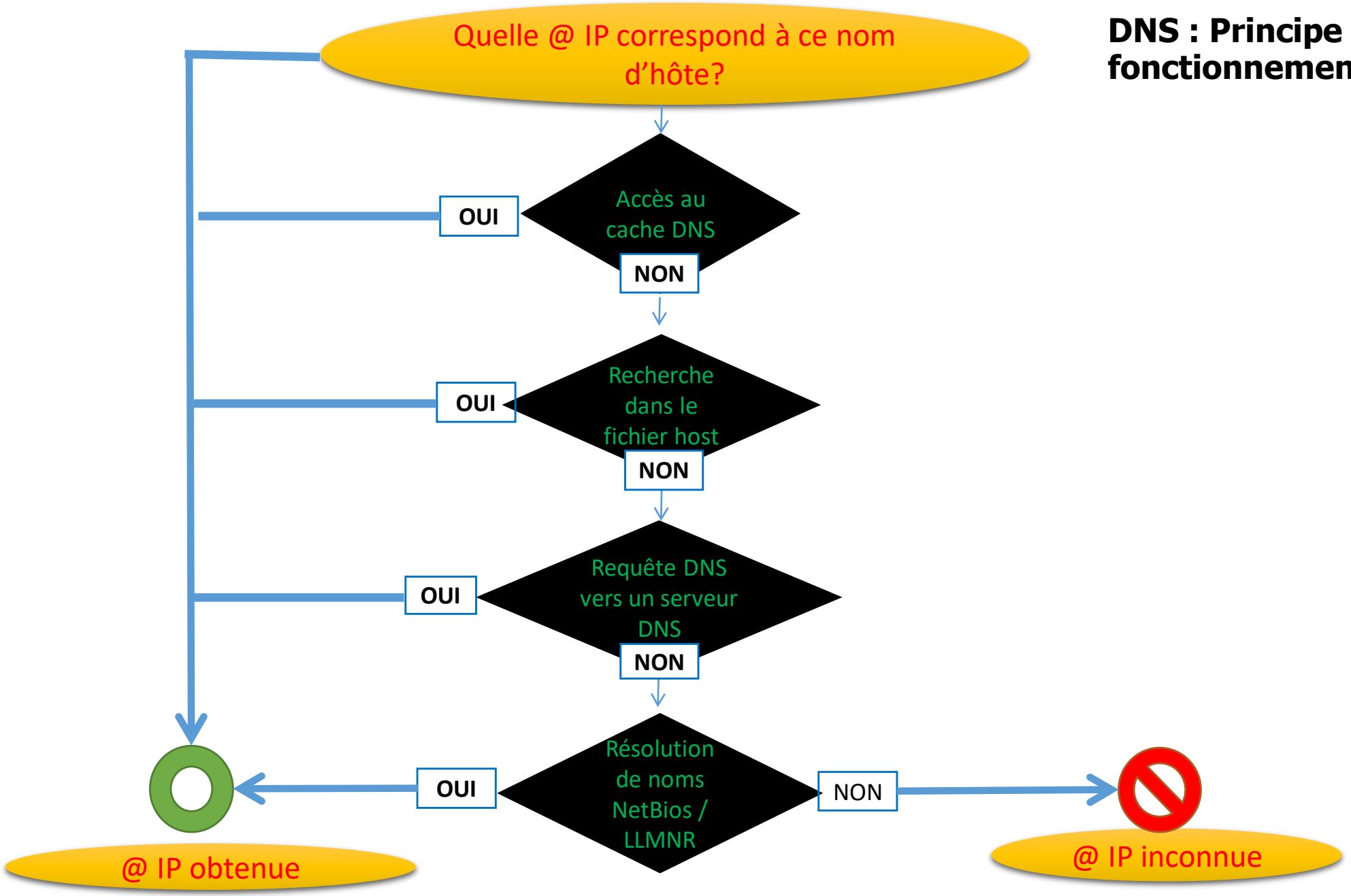
- Les noms de machine utilisant le système DNS sont appelés **noms d'hôtes**. Un nom d'hôte peut contenir jusqu'à 255 caractères alphanumériques (chiffres et lettres) et le caractère trait d'union "-". L'utilisation du caractère "." est interdite car il est réservé afin de séparer un domaine supérieur d'un domaine inférieur.
- En effet, on distingue deux types de noms avec le système DNS :
- le **nom d'hôte** qui représente le nom d'une machine (un ordinateur, une imprimante ou bien encore un routeur).
- le **nom de domaine pleinement qualifié ou FQDN** (Fully Qualified Domain Name).

CHAP. III. SERVICES RESEAU

DNS : Arborescence

- Le FQDN est en fait composé de deux parties : le nom d'hôte et le suffixe DNS. Le suffixe DNS défini la relation entre le domaine auquel appartient la machine et le domaine racine. Par exemple, si l'on considère une machine avec le nom d'hôte *client-11* située dans le domaine *students*, son FQDN est : **client-11.students.esis.cd**
- Structure générale : xxx.yy.zz

DNS : Principe de fonctionnement



DNS : Principe de fonctionnement

- Dans l'architecture du service DNS, chaque partie est responsable du niveau directement en dessous et uniquement de celui-ci. La racine est responsable du domaine .com, le .com de google.com et google.com de www.google.com, etc.
- Bien entendu, Google veut gérer lui-même le domaine google.com. L'organisme qui gère le domaine .com devra **déléguer** donc la gestion de ce nom de domaine à Google.

DNS : Principe de fonctionnement

- Ainsi, chaque personne qui veut posséder un domaine sur Internet peut le louer, mais devra ensuite gérer un serveur DNS pour publier ses adresses.
- Cependant, la plupart des entreprises qui vendent des noms de domaine (qu'on appelle registrar ou hébergeur) proposent de gérer elles-mêmes vos enregistrements DNS.

DNS : Principe de fonctionnement

- Nous avons vu que le DNS est organisé sous forme d'une grosse arborescence, et que chaque partie de l'arborescence peut être gérée par la personne qui la possède.

Mais comment fait-on pour savoir qui possède telle où telle partie et où sont stockées les informations que l'on recherche ?

CHAP. III. SERVICES RESEAU

DNS : Résolution de noms. Comment ça marche ?

- Vous êtes connectés à votre réseau, votre serveur DHCP vous a donné une adresse IP, un masque de sous-réseau et probablement une passerelle par défaut, ainsi qu'un serveur DNS. Imaginez que vous entrez www.ticvision.org dans votre navigateur. Lorsque vous entrez ce nom, votre machine doit commencer par le résoudre en une adresse IP. Vous allez donc demander une résolution au serveur DNS que vous avez reçu par le DHCP. Celui-ci a **deux moyens** pour vous fournir la réponse :

- il connaît lui-même la réponse
- il doit la demander à un autre serveur, car il ne la connaît pas.

CHAP. III. SERVICES RESEAU

DNS : Résolution de noms. Comment ça marche ?

- La plupart du temps, le serveur DNS est bien peu savant et demande à un autre serveur de lui donner la réponse. En effet, **chaque serveur DNS étant responsable d'un domaine** ou d'un petit nombre de domaines, la résolution consiste à aller chercher la bonne information sur le bon serveur.

- Nous voulons donc joindre le site www.ticvision.org et voilà ce que va faire le serveur DNS.
- Tout d'abord, il est évident que cette information ne se trouve pas sur notre serveur, car ce n'est pas lui qui est en charge du Site de TIC VISION.
- Pour obtenir cette résolution, notre serveur va procéder de façon rigoureuse et commencer par là où il a le plus de chance d'obtenir l'information, c'est-à-dire au point de départ de notre arborescence.

CHAP. III. SERVICES RESEAU

DNS : Résolution de noms. Comment ça marche ?

- Il va demander **aux serveurs racine** l'adresse IP de www.ticvision.org. Mais comme les serveurs racine ne sont pas responsables de ce domaine, ils vont le rediriger vers un autre serveur qui peut lui donner une information et qui dépend de la racine, **le serveur DNS de org**.
- Il demande ensuite au serveur DNS de org l'adresse IP de www.ticvision.org. Mais comme auparavant, le serveur org renvoie l'adresse IP du serveur DNS qui dépend de lui, le serveur DNS de ticvision.org.
- Enfin, il demande au serveur DNS de ticvision.org l'adresse IP de www.ticvision.org et là, ça marche : **le serveur de ticvision.org connaît l'adresse IP correspondante** et peut la renvoyer.

On a ainsi l'adresse IP de www.ticvision.org

CHAP. III. SERVICES RESEAU

DNS : Résolution de noms. Comment ça marche ?

- On dit qu'un serveur fournissant la résolution d'un nom de domaine sans avoir eu à demander l'information à quelqu'un d'autre **fait autorité**. Les serveurs DNS utilisent un système de cache pour ne pas avoir à redemander une information de façon répétitive, mais ils ne font pas autorité pour autant, car l'information stockée en cache peut ne plus être valide après un certain temps.

CHAP. III. SERVICES RESEAU

DNS : Résolution de noms. Comment ça marche ?

Cette conversion d'un nom de domaine en adresse IP est dite ***direct DNS*** ou ***résolution directe***

Existe-t-il aussi un protocole pour convertir une adresse IP en nom de domaine ?

Non, c'est inutile. Le DNS sait faire cela, on parle alors de ***reverse DNS*** **et de résolution inverse**.

DNS : Résolution de noms

Résolution de noms directe (Zone directe)

- Dans un réseau IP, lorsqu'une machine A veut communiquer avec une machine B, la machine A connaît le nom FQDN de B.
  Par exemple, lorsqu'on navigue sur le net, on connaît en général le nom FQDN des serveurs qu'on visite (exemple www.google.fr.).
  Pour que A puisse communiquer avec B grâce au protocole IP, A va avoir besoin de connaître l'adresse IP de B.
  A doit posséder un moyen d'effectuer la résolution de noms directe, c'est-à-dire un moyen de trouver l'adresse IP de B à partir de son nom qualifié.

CHAP. III. SERVICES RESEAU

Résolution de noms inverse (Zone inverse)

- La machine B reçoit un datagramme IP en provenance de A. Ce datagramme contient l'adresse IP de A. B peut avoir besoin de connaître le nom FQDN de la machine A.
  B doit donc être capable de trouver le nom FQDN de A à partir de son adresse IP. C'est ce qu'on appelle la résolution de noms inverse.
- La notation de l'@ IP est faite à l'inverse (partie réseau) et on y ajoute **in-addr.arpa**

Ex. Résolution inverse du réseau 192.168.10.0/24 , zone inverse noté : 10.168.192.in-addr.arpa

CHAP. III. SERVICES RESEAU

Link Local Multicast Name Resolution Protocol (LLMNR)

- Conçu pour IPv6, utilisé également avec IPv4
- Requête sur le groupe de multicast IPv4 224.0.0.252
- Réponse en unicast par le nœud qui possède le nom
- Port 5355
- Format de message simulaire à DNS
- Appelé à remplacer NetBios

CHAP. III. LES SERVICES RESEAU

1. Annuaire Active Directory
2. Résolution des noms (LLMNR et DNS)
3. Configuration automatique d'adresses IP (DHCP)
4. Service de fichiers (SMB et RPC)
5. Messagerie (SMTP, POP, IMAP)

DHCP - Rôle

- Un serveur DHCP (*Dynamic Host Configuration Protocol*) a pour rôle de distribuer des adresses IP à des clients pour une durée déterminée.
- Au lieu d'affecter manuellement à chaque hôte une adresse statique, ainsi que tous les paramètres tels que (serveur de noms, passerelle par défaut, nom du réseau),
- 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

- Tous les noeuds critiques du réseau (serveur de nom primaire et secondaire, passerelle par défaut) ont une adresse IP statique ; en effet, si celle-ci variait, ce processus ne serait plus réalisable.

DHCP - Avantages

- Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de **contrôler** l'utilisation des adresses IP de façon **centralisée**. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que toutes les stations aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé. Dans le cas de l'adressage statique, il faudrait manuellement reconfigurer toutes les machines.

DHCP - Avantages

- **Economie d'adresse** : Grâce à DHCP, seules les machines connectées en ligne ont une adresse IP. En effet, imaginons un fournisseur d'accès qui a plus de 1000 clients. Il lui faudrait 5 réseaux de classe C, s'il voulait donner à chaque client une adresse IP particulière. S'il se dit que chaque client utilise en moyenne un temps de connexion de 10 mn par jour, il peut s'en sortir avec une seule classe C, en attribuant, ce que l'on pourrait appeler des "jetons d'accès" en fonction des besoins des clients.
- Les postes itinérants sont plus faciles à gérer
- Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution.

CHAP. III. SERVICES RESEAU

DHCP - Fonctionnement

- Il faut dans un premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP provenant des machines clientes, aussi elle doit avoir une adresse IP fixe. Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP.
- le processus de génération de bail DHCP est utilisé en quatre étapes pour attribuer une adresse IP aux clients. Ce processus est dit DORA. Le fait de comprendre le fonctionnement de chaque étape aidera à résoudre les problèmes survenant lorsque les clients ne parviennent pas à obtenir une adresse IP.

CHAP. III. SERVICES RESEAU

DHCP – Fonctionnement :Création d'un bail (DORA)

Les quatre étapes du processus DORA sont les suivantes :

1. Le client DHCP diffuse un paquet de demande de bail IP « **DHCPDISCOVER** » à chaque ordinateur du sous-réseau, lequel paquet est envoyé sous forme d'une diffusion sur le réseau avec comme adresse IP source 0.0.0.0 et adresse IP destination 255.255.255.255 et son adresse MAC.

   Seul un ordinateur qui a le rôle Serveur DHCP ou un ordinateur ou routeur qui exécute un agent de relais DHCP répond. Dans ce dernier cas, l'agent de relais DHCP transfère le message au serveur DHCP avec lequel il est configuré.
2. Les serveurs DHCP répondent avec un paquet **DHCPOFFER** qui contient une adresse IP proposée au client, une durée de bail et l'adresse IP du serveur

CHAP. III. SERVICES RESEAU

DHCP – Fonctionnement : Création d'un bail (DORA)

3. Le client reçoit le paquet DHCPOFFER. Il peut recevoir des paquets de plusieurs serveurs, auquel cas il sélectionne généralement le serveur qui a répondu le plus rapidement à son paquet DHCPDISCOVER. Il s'agit habituellement du serveur DHCP le plus proche du client. Le client diffuse alors un paquet **DHCPREQUEST** qui contient un identificateur de serveur. Ce dernier indique aux serveurs DHCP qui reçoivent le paquet DHCPOFFER quel serveur le client a choisi d'accepter, ainsi tous les autres serveurs DHCP retirent leur offre et les adresses proposées redeviennent disponibles.

CHAP. III. SERVICES RESEAU

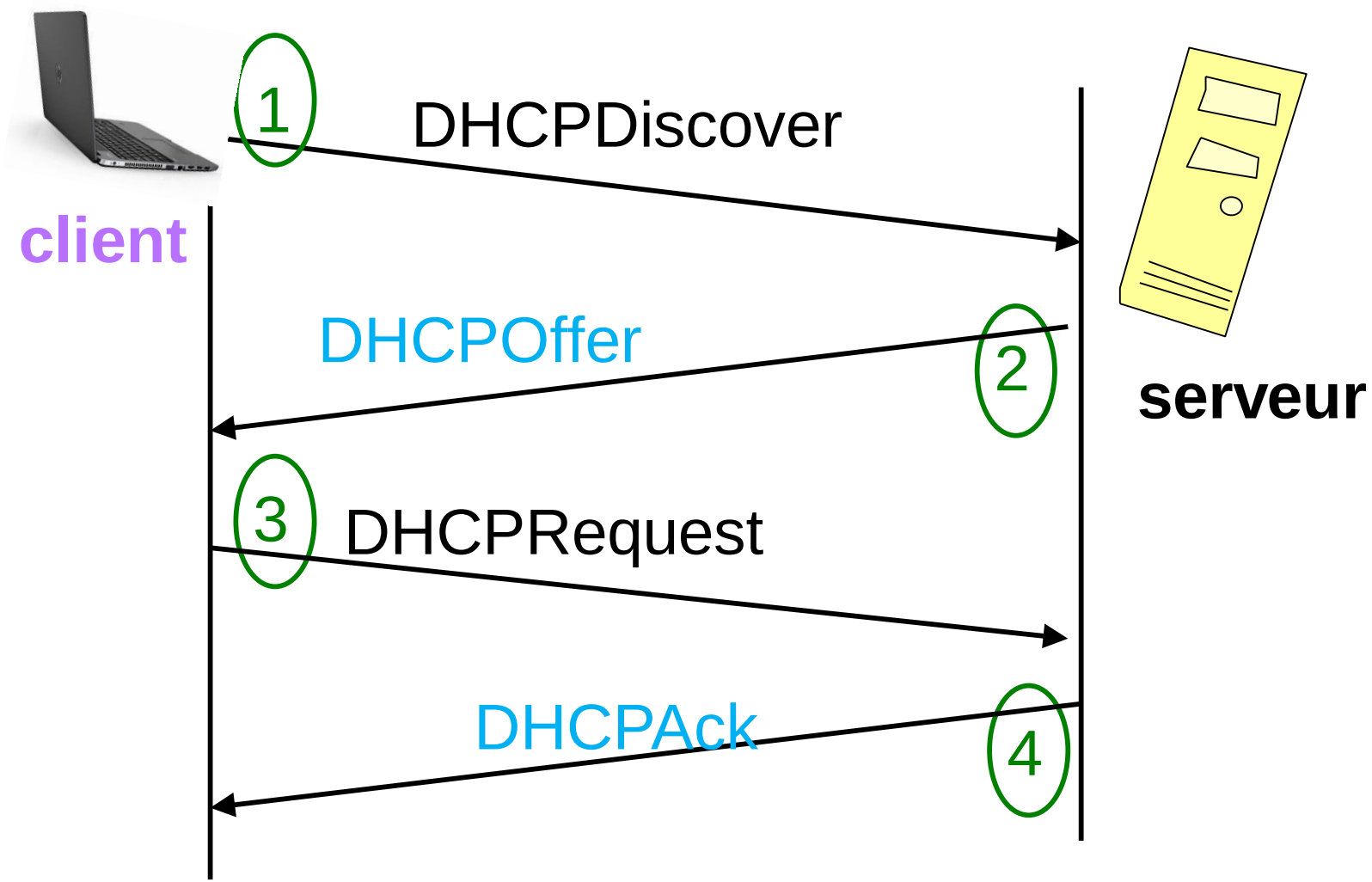
DHCP – Fonctionnement : Création d'un bail (DORA)

4. Les serveurs DHCP reçoivent le paquet DHCPREQUEST. Les serveurs non acceptés par le client utilisent le message comme notification indiquant que le client refuse l'offre du serveur. Le serveur choisi stocke l'adresse IP du client ainsi que le bail dans la base de données DHCP et répond par un message **DHCPACK**. Et le client peut utiliser enfin l'adresse pour se connecter au réseau. Si, pour une raison ou une autre, le serveur DHCP ne peut pas fournir l'adresse contenue dans le paquet DHCPOFFER initial, le serveur DHCP envoie un message DHCPNAK.

DHCP – Fonctionnement

C'est seulement après t0 que le client peut utiliser l'adresse IP communiquée par le serveur jusqu'à t0 + **lease-time**

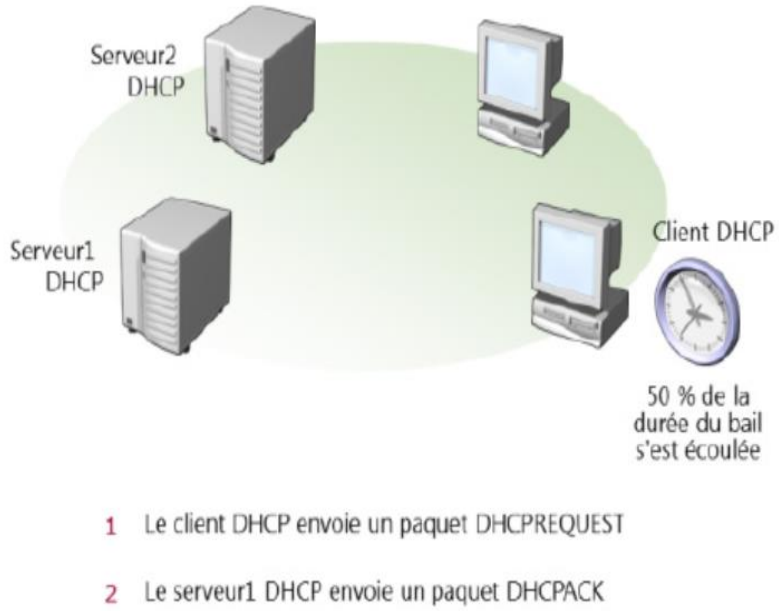
lease-time = Temps de bail



CHAP. III. SERVICES RESEAU

DHCP – Fonctionnement : Renouvellement d'un bail

- Lorsque le bail DHCP atteint 50 % de sa durée totale, le client essaie de le renouveler. Il s'agit d'un processus automatique qui se produit en arrière-plan. Les ordinateurs peuvent utiliser l'adresse IP attribuée par le serveur DHCP sur une longue période s'ils fonctionnent de façon continue sur un réseau sans être arrêtés.
- Pour renouveler le bail de l'adresse IP, le client diffuse un message DHCPREQUEST. Le serveur qui a initialement loué l'adresse IP renvoie au client un message DHCPACK qui contient tous les nouveaux paramètres qui n'existaient pas lors de la création du bail.



CHAP. III. SERVICES RESEAU

DHCP – Fonctionnement : Renouvellement d'un bail

Si le client DHCP ne peut pas contacter le serveur DHCP, alors le client attend que 87,5 pour cent de la durée du bail soient écoulés. Si le renouvellement échoue, ce qui signifie que 100 pour cent de la durée du bail sont écoulés, l'ordinateur client tente d'entrer en contact avec la passerelle par défaut configurée. Si la passerelle ne répond pas, le client suppose qu'il est sur un nouveau sous-réseau et passe à la phase de détection. Il tente alors d'obtenir une configuration IP de n'importe quel serveur DHCP

CHAP. III. SERVICES RESEAU

DHCP – Fonctionnement : Renouvellement d'un bail

Les ordinateurs clients tentent également de renouveler le bail pendant le processus de démarrage ou lorsque l'ordinateur détecte une modification du réseau. Ceci est dû au fait que les ordinateurs clients peuvent avoir été déplacés alors qu'ils étaient hors connexion ; par exemple, un ordinateur portable peut avoir été branché à un nouveau sous-réseau. Si le renouvellement réussit, la période de bail est réinitialisée.

CHAP. III. SERVICES RESEAU

DHCP – Fonctionnement

lorsqu'un client redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine, en émettant un DHCPREQUEST. Si la tentative se solde par un échec, le client continue à utiliser la même adresse IP s'il lui reste du temps sur son bail.

CHAP. III. SERVICES RESEAU

DHCP – Agent de relais : Définition

Un agent de relais DHCP est donc un ordinateur (serveur) ou un routeur qui écoute les messages des clients DHCP et les transmet aux serveurs DHCP sur différents sous-réseaux

CHAP. III. SERVICES RESEAU

DHCP – Agent de relais

DHCP utilise des messages IP pour établir des communications. Par conséquent, les serveurs DHCP sont limités aux communications à l'intérieur de leur sous-réseau IP. Cela signifie que dans bon nombre de réseaux, il existe un serveur DHCP pour chaque sous-réseau IP. Or, si les sous-réseaux sont nombreux, le déploiement de serveurs pour chaque sous-réseau peut s'avérer onéreux. Un même serveur DHCP peut desservir des groupes de sous-réseaux plus petits. Pour pouvoir répondre à une requête d'un client DHCP, le serveur DHCP doit être en mesure de recevoir les requêtes DHCP. Pour cela, vous devez configurer un agent de relais DHCP sur chaque sous-réseau. Un *agent de relais DHCP* est un ordinateur ou un routeur qui écoute les messages des clients DHCP et les transmet aux serveurs DHCP sur différents sous-réseaux.

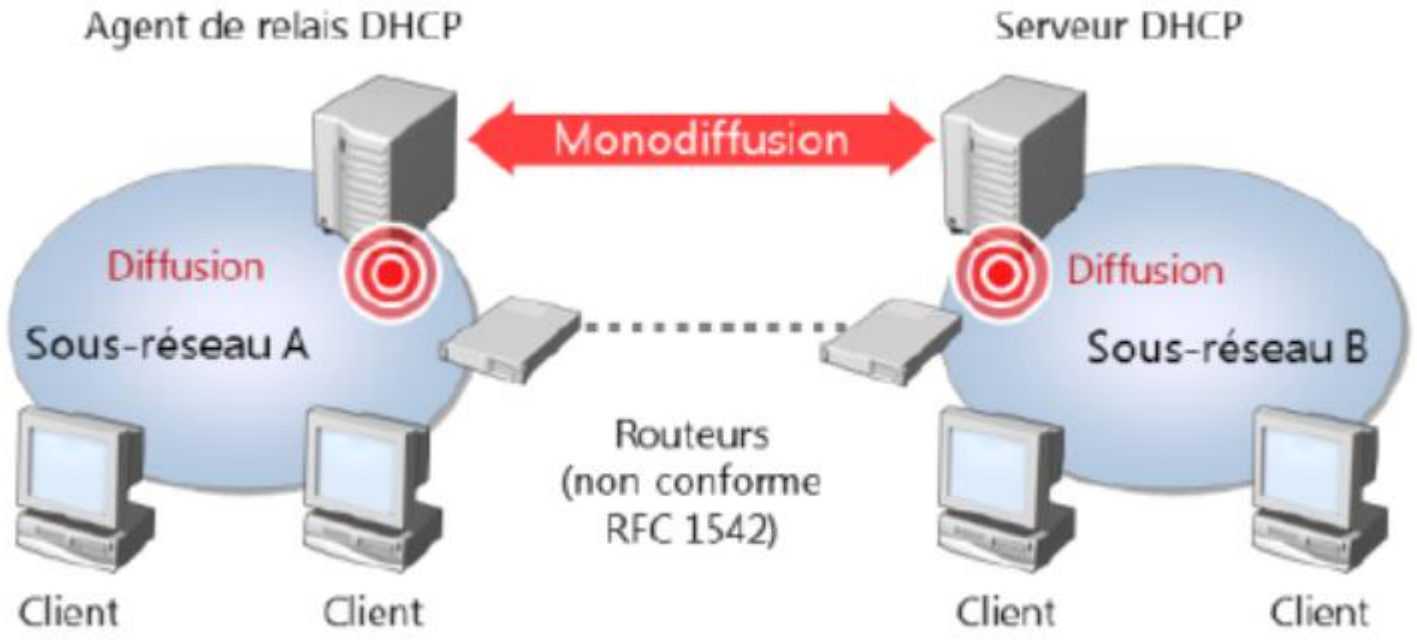
CHAP. III. SERVICES RESEAU

DHCP – Agent de relais

Avec l'agent de relais DHCP, les paquets de diffusion DHCP peuvent être relayés dans un autre sous-réseau IP via un routeur. Ensuite, vous pouvez configurer l'agent de relais DHCP dans le sous-réseau qui a besoin d'adresses IP. En outre, vous pouvez configurer l'agent avec l'adresse IP du serveur DHCP. L'agent pourra ainsi capturer les messages du client et les transférer au serveur DHCP d'un autre sous-réseau. Vous pouvez également relayer des paquets DHCP dans d'autres sous-réseaux à l'aide d'un routeur compatible avec la norme RFC 1542.

CHAP. III. SERVICES RESEAU

DHCP – Agent de relais : Illustration



CHAP. III. SERVICES RESEAU

DHCP – APIPA

Il arrive parfois sur les machines clientes attendant une configuration DHCP que l'on se retrouve après un délai d'attente avec une adresse de type 169.254.X.X. Ces adresses signifient souvent qu'il y a un problème au niveau de l'attribution.

Ces adresses se nomment APIPA pour "**Automatic Private Internet Protocol Addressing**" soit "Adressage automatique du protocole IP". Il s'agit en réalité d'une adresse que la machine va s'attribuer automatiquement si les requêtes DHCP effectuées auparavant échouent.

CHAP. III. SERVICES RESEAU

DHCP – APIPA

L'**APIPA** se trouve dans le réseau **169.254.0.0/16** (De 169.254.0.1 à 169.254.255.254). C'est un réseau privé qui n'est routable ni sur Internet ni ailleurs. Lorsqu'un poste dispose d'une IP en APIPA, il ne pourra communiquer qu'avec d'autres PC configurées en APIPA. Il faut noter que le service APIPA continue de vérifier la présence d'un serveur DHCP dans les environs toutes les cinq minutes, plus concrètement il réémet une requête de type "**DHCP Discover**" en espérant avoir une réponse d'un serveur, s'il obtient une réponse, le service DHCP affectera une IP à la carte réseau et remplacera l'IP APIPA en place.