Brevet de Technicien Supérieur
Centre: Lycée Technique - Taza

Filière: **Multimédia et Conception Web**
Niveau: **2ème année**

Module:

Réseaux Informatiques

Réalisé par:
Pr. H. EL BOURAKKADI
hamid.elBourakkadi1@usmba.ac.ma

A.F. 2021-2022

Plan du cours

- Chapitre 1: Introduction aux réseaux informatiques
- Chapitre 2: Modèle OSI
- Chapitre 3: Techniques d'adressage d'un réseau local
- Chapitre 4: Service DHCP
- **Chapitre 5: Service DNS**
- Chapitre 6: Service Web

1. Introduction

Pour pouvoir communiquer, chaque machine présente sur un réseau doit avoir un identifiant unique. Avec le protocole IP (Internet protocole), cet identifiant se présente sous la forme d'un nombre d'une longueur de 32 bits. On parle d'adresses IP. Cependant pour un utilisateur, il est difficile de retenir les adresses IP de chaque ordinateur. C'est pourquoi des mécanismes de **résolution de noms** ont été mis en place. Un mécanisme de résolution de noms permet de traduire des noms en adresses IP et inversement.

1. Introduction

- Le premier mécanisme de résolution de noms mis en place sous Windows est **NetBIOS** (NetBIOS Extended User Interface) (IBM:1980)
- un nouveau système de résolution de noms appelé **DNS** (Domain Name System) a été adopté pour Windows 2000/2003/XP afin de corriger les inconvénients (16 caractères, surcharge de la bande passante, pas de hiérarchie, problème d'interopérabilité) du protocole **NetBIOS**.

2. Système DNS

Le système DNS propose :

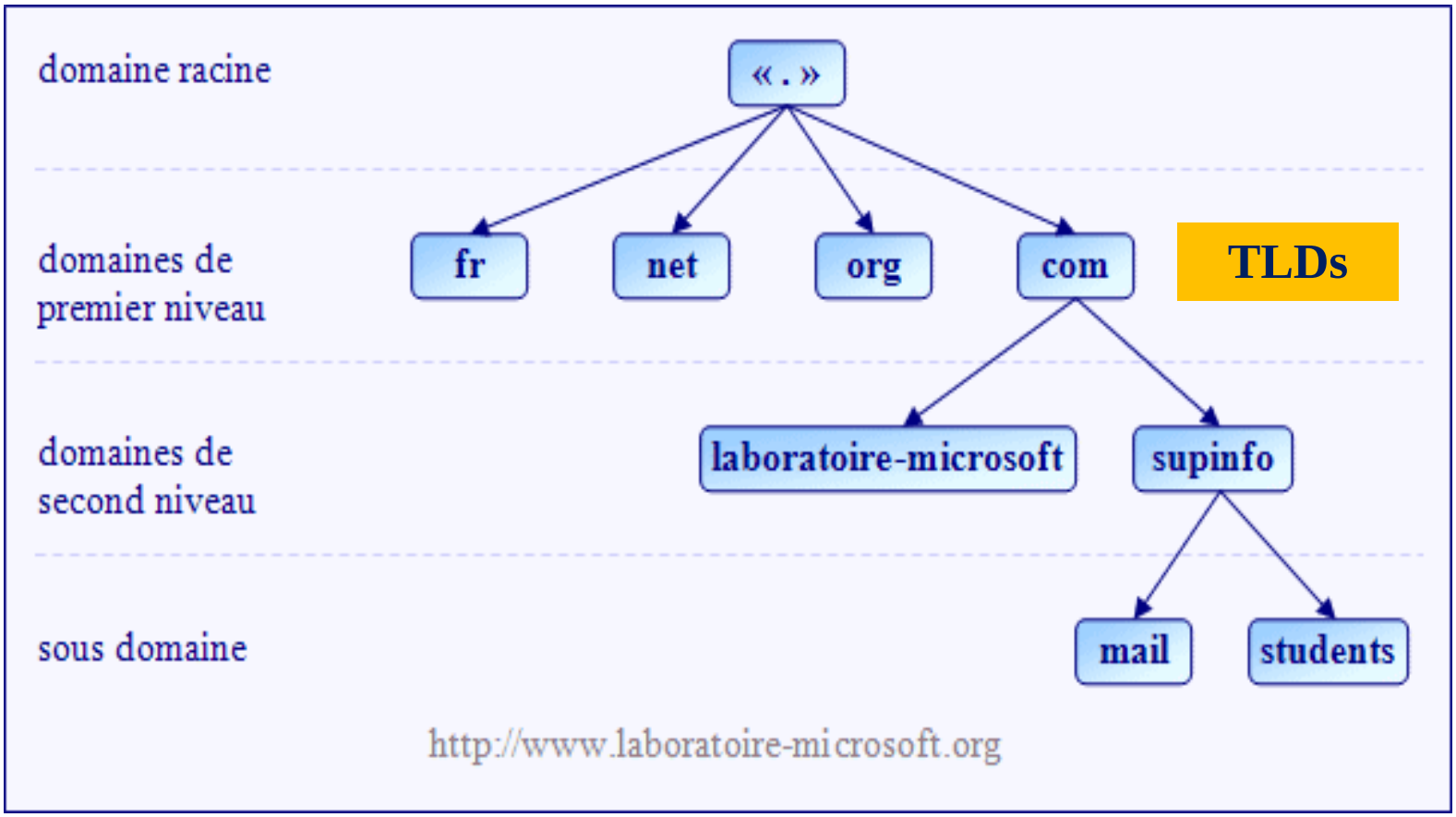


Figure 5.2 : Hiérarchie DNS

2. Système DNS

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). 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
- Le **nom de domaine pleinement qualifié** ou **FQDN** (Fully Qualified Domain Name) = **noms d'hôte** + **suffixe DNS** .

Exemple: CLIENT-11.students.supinfo.com.

- Nom hôte = **CLIENT-11**
- Suffixe DNS = **students.supinfo.com**
- FQDN = **CLIENT-11.students.supinfo.com**

2. Système DNS

Les serveurs de noms

- Les machines appelées **serveurs de nom de domaine** permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau.
- Chaque domaine possède un serveur de noms de domaines, appelé « **serveur de noms primaire** » (**primary domain name server**), ainsi qu'un **serveur de noms secondaire** (**secondary domaine name server**), permettant de prendre le relais du serveur de noms primaire en cas d'indisponibilité.

Le mécanisme consistant à trouver l'adresse IP correspondant au nom d'un hôte est appelé «**résolution de nom de domaine** ».

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

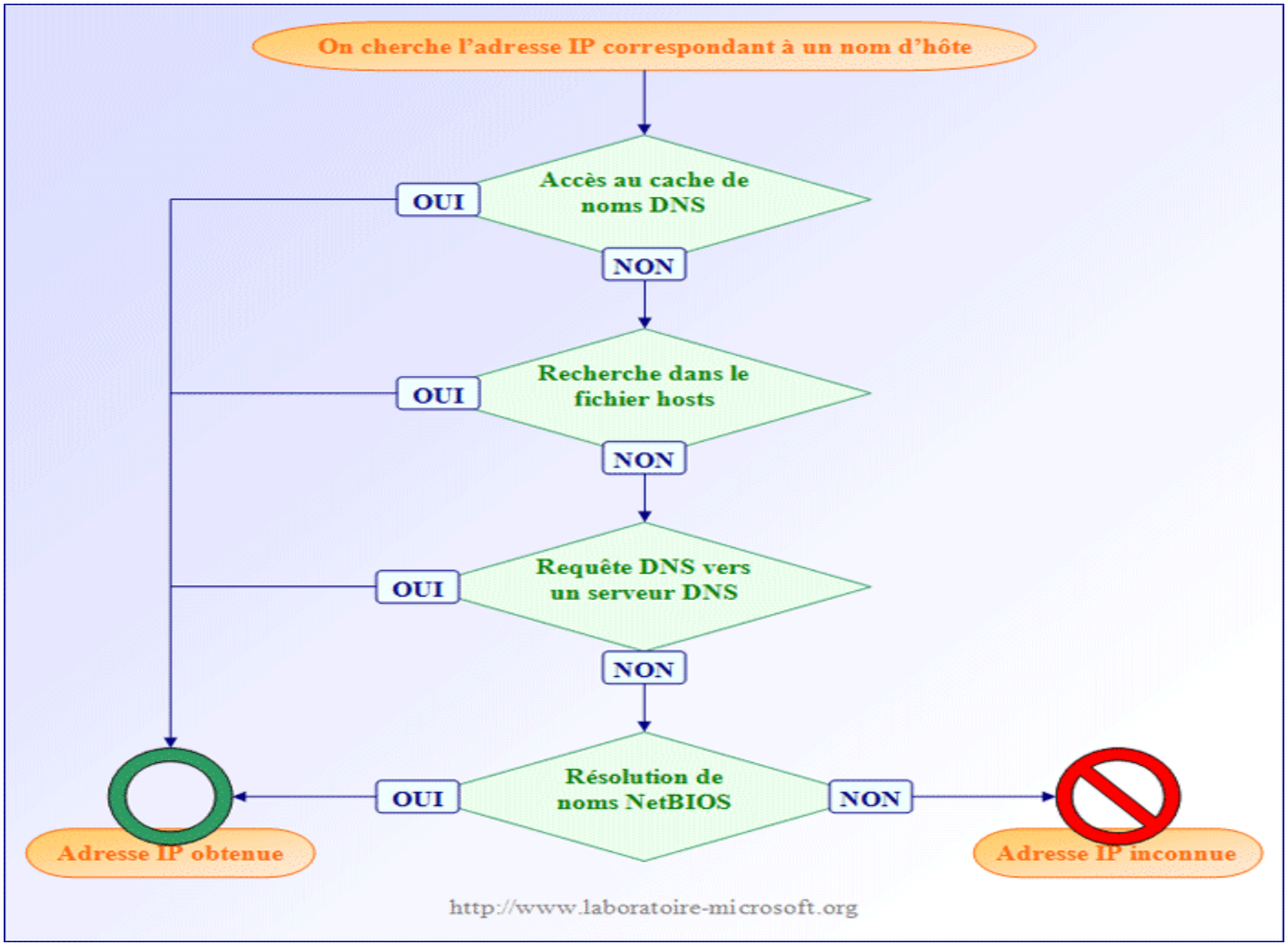


Figure 5.3 : Fonctionnement de la résolution de nom d'hôte.

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

1) Cache de noms DNS

- Le client commence par vérifier si une adresse IP correspondant au nom d'hôte est présente dans **le cache de noms DNS**. Le **cache de noms DNS** contient tous les mappages **noms d'hôte/adresses IP** qui ont été précédemment résolus. Le cache de noms DNS est stocké en mémoire vive ce qui permet d'accélérer le processus de résolution de noms d'hôte lorsque l'utilisateur accède souvent au même serveur.
- On peut afficher le cache de noms DNS en utilisant la commande

  `ipconfig /displaydns`.
- Il est aussi possible de vider cette mémoire cache grâce à la commande

  `ipconfig /flushdns`.

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

2) Fichier hosts

- Si l'adresse IP recherchée n'est pas présente dans le cache de noms DNS, alors le client consulte **le fichier hosts** (qui se trouve dans le disque dur). Ce fichier est situé dans le répertoire

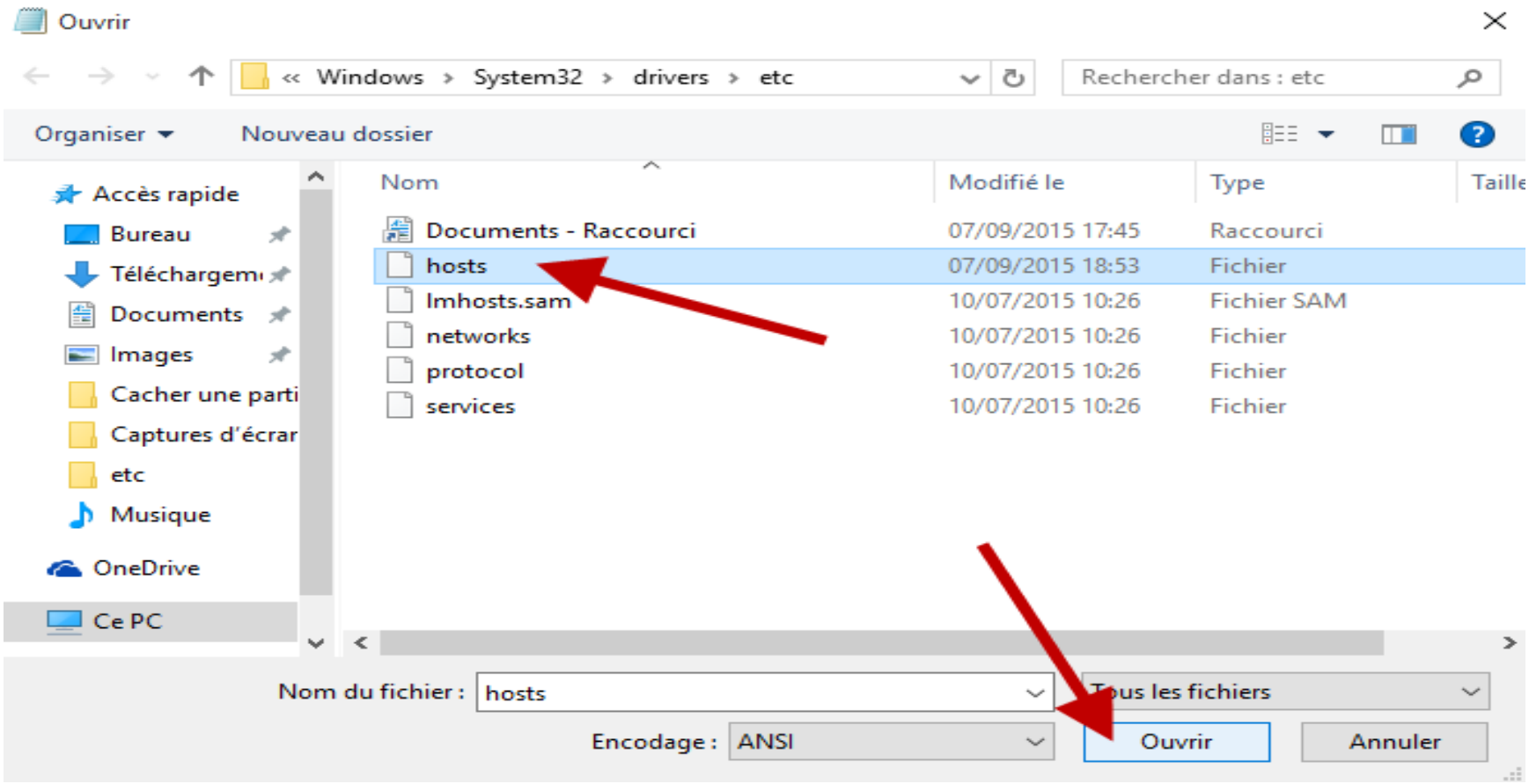
%SYSTEMROOT%\system32\drivers\etc.

Toutes les entrées sont faites de manières statiques. Par défaut, il contient uniquement le mappage entre le nom d'hôte **localhost** et l'adresse IP **127.0.0.1**.

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

2) Fichier hosts



2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

2) Fichier hosts

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Ceci est un exemple de fichier HOSTS utilisé par Microsoft TCP/IP
# pour Windows.
#
# Ce fichier contient les correspondances des adresses IP aux noms d'hô
# Chaque entrée doit être sur une ligne propre. L'adresse IP doit être
# dans la première colonne, suivie par le nom d'hôte correspondant. L'a
# IP et le nom d'hôte doivent être séparés par au moins un espace.
#
# De plus, des commentaires (tels que celui-ci) peuvent être insérés su
# lignes propres ou après le nom d'ordinateur. Ils sont indiqué par le
# symbole '#'.
#
# Par exemple :
#
#      102.54.94.97     rhino.acme.com          # serveur source
#       38.25.63.10     x.acme.com              # hôte client x

127.0.0.1       localhost
```

Figure 5.4: Le fichier hosts

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

3) Serveur DNS

- Si le mappage n'a pas été trouvé dans le fichier hosts, alors le client va envoyer une requête DNS au premier serveur DNS dont l'adresse IP a été définie dans ses paramètres TCP/IP.

- Si le premier serveur DNS est injoignable alors le client envoie une requête au second et ainsi de suite...

- Si aucun serveur DNS n'a été paramétré dans les paramètres TCP/IP du client ou bien si aucun serveur DNS n'est capable de résoudre le nom en adresse IP alors le client passe à la quatrième et dernière étape c'est la résolution de nom **NetBIOS**.

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

4) Résolution de nom NetBIOS

Si le client n'a pas trouvé le mappage recherché alors il considère que l'adresse IP recherchée ne correspond pas à un nom d'hôte mais à un **nom NetBIOS** et lance une résolution de nom NetBIOS.

La résolution de noms NetBIOS se passe en plusieurs étapes :

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

4) Résolution de nom NetBIOS

Etape 1:

- **Le cache de noms NetBIOS**
  - Vérification de la présence de l'adresse IP dans le cache de noms NetBIOS.
  - Pour afficher le cache de noms NetBIOS on utilise la commande **`nbtstat -c`**
  - Pour vider cette mémoire cache grâce à la commande **`nbtstat -r`**
  - Pour afficher le nom NetBIOS on utilise la commade **`nbtstat -n`**

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

4) Résolution de nom NetBIOS

Etape 2:

- **Le serveur WINS**

  Envoie d'une requête au premier **serveur WINS** dont l'adresse IP a été défini dans ses paramètres TCP/IP du client.

Etape 3:

- **Diffusion (Broadcast)**

  Le client cherche l'adresse IP de la machine sur son sous-réseau en réalisant une diffusion (broadcast).

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

4) Résolution de nom NetBIOS

Etape 4:

- **Le fichier lmhosts**

Recherche d'une éventuelle entrée dans le fichier

%SYSTEMROOT%\system32\drivers\etc\lmhosts.

2. Système DNS

2.1. Fonctionnement de la résolution de nom d'hôte côté client

4) Résolution de nom NetBIOS

Les étapes 2 et 3 peuvent **être inversées** ou **non présentes** selon le type de nœud NetBT défini sur le client. Par défaut, le nœud NetBT H (Hybride) est utilisé et il réalise les étapes dans l'ordre ci-dessus.

- Le type de nœud NetBT peut se paramétrer au niveau du serveur DHCP (le type de nœud NetBT correspond à l'option DHCP numéro 46).
- Si à la fin de ce processus aucune adresse IP n'a été trouvée alors le client ne peut pas obtenir l'adresse IP correspondante et ne peut pas joindre la ressource (par exemple un serveur web ou un serveur de fichier). Dans tous les cas le résultat de la requête DNS sera mis dans le cache de noms DNS.

2. Système DNS

2.2. Différents types de requêtes

Un serveur DNS peut recevoir deux types de requêtes DNS :

- **Une 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.
- **Une requête itérative :** Lorsqu'un serveur reçoit une requête itérative, il renvoie **la meilleure réponse qu'il peut donner sans contacter d'autres serveurs DNS** (c'est-à-dire en consultant uniquement sa propre base de données).

2. Système DNS

2.2. Différents types de requêtes

Lorsqu'une machine cliente envoie une requête à un serveur DNS (étape 3 de la résolution de nom d'hôte), elle est **toujours de type récursif.**

Exemple: L'ordinateur client nommé ***client23.laboms.lan*** cherche l'adresse IP correspondant au nom d'hôte ***webserver.laboms.lan***.
il envoie une requête récursive au serveur DNS nommé ***dns1.laboms.lan.*** À partir de cet instant ***dns1.laboms.lan*** a pour obligation de renvoyer une réponse au client. Pour cela il va chercher dans sa **mémoire cache**, puis dans la base de données qu'il héberge et va éventuellement contacter d'autres serveurs DNS. Une fois qu'il a obtenu la réponse (la réponse peut être négative), il la renvoie au client. Dans cet exemple, le serveur DNS a trouvé l'adresse IP recherchée qui est : ***172.16.104.30***. L'ordinateur client peut ensuite contacter le serveur web nommé ***webserver.laboms.lan***.

2. Système DNS

2.2. Différents types de requêtes

Figure 5.5 : Requête récursive.

2. Système DNS

2.2. Différents types de requêtes

Lorsqu'un serveur DNS ne peut pas répondre à la requête récursive d'un client, **il va d'abord essayer de contacter ses redirecteurs**. Si le serveur DNS est paramétré pour utiliser des redirecteurs alors il envoie une requête récursive au premier serveur DNS défini dans sa liste de redirecteurs. Par contre, si le serveur DNS n'a pas de redirecteurs, il va envoyer une **requête itérative** au premier serveur DNS situé dans sa liste de serveur DNS racine.

Le serveur DNS n'envoie donc des requêtes itératives que s'il n'a pas de redirecteurs.

2. Système DNS

2.2. Différents types de requêtes

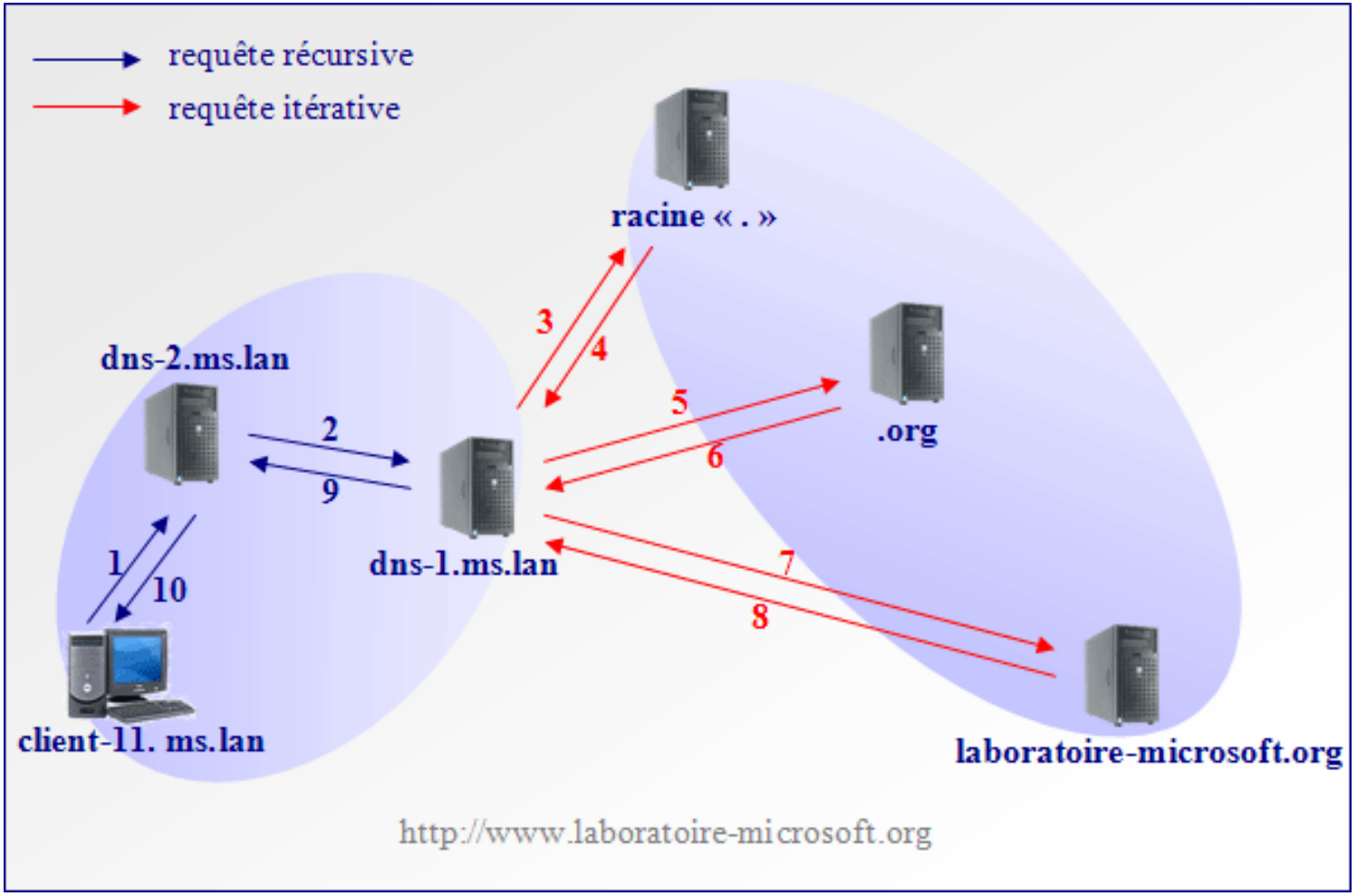


Figure 5.6 : Requêtes DNS récursive/itérative

2. Système DNS

2.2. Différents types de requêtes

Le client nommé **client-11.ms.lan** souhaite accéder au site web du laboratoire **Microsoft**. La procédure de résolution de nom se passe en plusieurs étapes :

1. L'ordinateur client **client-11.ms.lan** commence par chercher l'adresse IP du serveur Web. Pour cela il envoie une requête récursive au premier serveur DNS de sa liste de serveurs DNS soit **dns-2.ms.lan**.

2. Le serveur **dns-2.ms.lan** ne connaît pas la réponse, il envoie donc une requête récursive à **dns-1.ms.lan** qui est le premier serveur DNS de sa liste de redirecteurs.

3. Dans le cas présent **dns-1.ms.lan** ne connaît pas l'adresse IP recherchée et **n'est pas configuré pour utiliser des redirecteurs.** Il envoie donc une **requête itérative** au premier serveur DNS racine parmi sa liste d'indications de racine.

4. Le serveur DNS racine ne connaît pas la réponse mais il sait quel serveur DNS fait autorité pour le domaine **org**. Il renvoie donc l'adresse IP du serveur DNS faisant autorité pour le domaine **org** à **dns-1.ms.lan.**

2. Système DNS

2.2. Différents types de requêtes

5. Le serveur **dns-1.ms.lan** envoie alors une **requête itérative** au serveur DNS du domaine org.
6. Le serveur DNS du domaine **org** ne connaît pas la réponse et renvoie l'adresse IP du serveur DNS faisant autorité pour le domaine **laboratoire-microsoft** au serveur **dns-1.ms.lan**.
7. Le serveur **dns-1.ms.lan** contacte alors le serveur DNS faisant autorité pour la zone laboratoiremicrosoft au moyen d'une **requête itérative**.
8. Le serveur DNS faisant autorité pour la zone **laboratoire-microsoft** possède le mappage dans sa zone de recherche directe locale. Il envoie donc l'adresse IP recherché à dns-1.ms.lan.
9. dns-1.ms.lan transmet la réponse au serveur dns-2.ms.lan.
10. Le serveur **dns-2.ms.lan** fait suivre la réponse au **client** qui peut ensuite joindre le serveur **http** et afficher le site du laboratoire Microsoft.

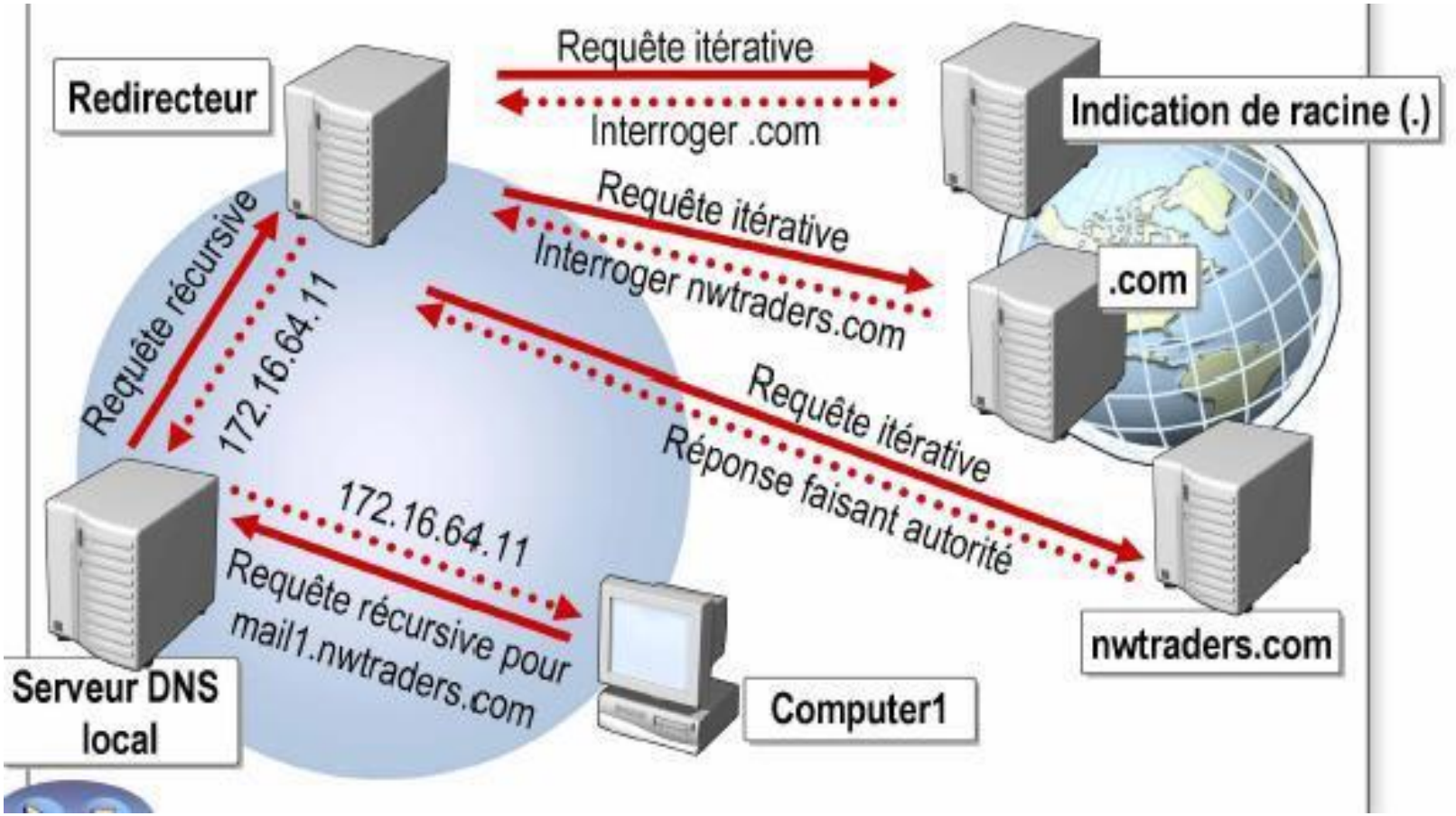
2. Système DNS

2.3. Redirecteurs

- Lorsque le serveur DNS n'est pas capable de résoudre un nom en adresse IP, il va essayer de contacter un autre serveur DNS. On appelle ce serveur **DNS redirecteur**.
- Un redirecteur est un serveur DNS que d'autres serveurs DNS internes désignent comme **responsable du transfert des requêtes** pour la résolution de noms de domaines externes ou hors site. Il est possible de configurer un ou plusieurs redirecteurs pour un domaine précis.

2. Système DNS

2.3. Redirecteurs



2. Système DNS

2.4. Les indications de racine

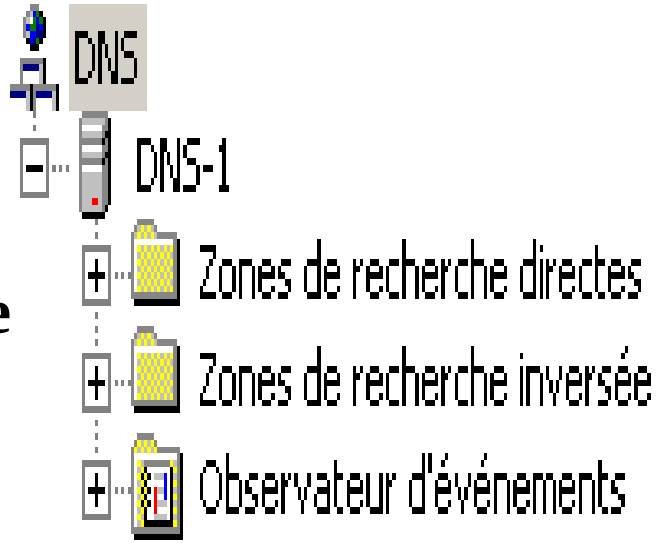
- Lorsque le serveur DNS n'est pas configuré pour utiliser des redirecteurs, il se sert des indications de racine pour résoudre les noms d'hôtes ou les adresses IP appartenant à des zones qu'il n'héberge pas.
- Les indications de racine sont un ensemble de serveurs hébergeant la zone contenant l'enregistrement du domaine racine ou domaine "**.**"
- Les "serveurs DNS racines" sont au nombre de **13 à travers le monde**. Ils appartiennent tous à un même domaine nommé **root-servers.net**.
- Les indications de racine sont stockées dans le fichier **Cache.dns** qui se trouve dans le dossier:

%systemroot%\System32\Dns.

3. Zones DNS primaires et secondaires

3.1. Zones de recherche

La console de gestion du service DNS présente une arborescence simple. Les deux premiers conteneurs listent les zones de recherches alors que le troisième liste les évènements relatifs au service DNS (ex. : Le serveur DNS a démarré). Une **zone de recherche directe** contient des mappages **nom d'hôte / adresse IP** alors qu'une **zone de recherche inversée** contient des mappages **adresse IP / nom d'hôte**. Ainsi, une zone de recherche directe permet de trouver l'adresse IP correspondant à un nom d'hôte alors qu'une zone de recherche inversée permet de trouver un nom d'hôte à partir d'une adresse IP.



3. Zones DNS primaires et secondaires

3.1. Zones de recherche

- Dans le cas d'une recherche directe, le serveur DNS commence par analyser le suffixe DNS pour trouver la zone dans laquelle est situé le nom d'hôte, puis recherche ensuite le mappage à l'intérieur de cette zone.
- Dans le cas d'une recherche indirecte, le serveur DNS ne connaît que l'adresse IP de l'hôte. Il ne peut donc pas utiliser la hiérarchie de l'espace de noms pour retrouver le nom d'hôte. En effet si le serveur devait interroger toutes les zones DNS pour trouver le nom d'hôte, la recherche indirecte prendrait trop de temps et de ressources pour être réellement efficace.
- C'est pourquoi un domaine spécifique, nommé **in-addr.arpa** a été réservé dans l'espace de noms DNS.

3. Zones DNS primaires et secondaires

3.1. Zones de recherche

Ce domaine **in-addr.arpa** est subdivisé en sous-domaines correspondant chacun à un réseau donné. Ainsi le domaine contenant tous les mappages **adresse IP / nom d'hôte** du réseau privé de classe C (la page des adresses IP privées de classe C va de 192.168.0.1 à 192.168.255.254) se nomme **168.192.inaddr.arpa.**

Par exemple, lorsqu'un serveur DNS recherche le nom d'hôte correspondant à l'adresse IP 172.16.16.1, il s'adresse à la zone nommée **16.172.in-addr.arpa**. Selon le plan d'adressage du réseau, il arrive que plusieurs zones de recherches inversées doivent être crées afin de contenir tous les mappages **adresse IP / nom d'hôte** d'un domaine donné.

Par exemple si une entreprise utilise le domaine **laboms.lan** et que son plan d'adressage fait intervenir des adresses IP privés de classes B et des adresses IP privées de classe C alors elle devra créer une zone de recherche directe nommée laboms.lan et deux zones de recherches inversées nommées **16.172.in-addr.arpa** et **168.192.in-addr.arpa**.

3. Zones DNS primaires et secondaires

3.2. Enregistrements de ressources

- Dans un environnement Microsoft, les mappages **nom d'hôte / adresse IP** et **adresse IP / nom d'hôte** sont appelés **enregistrements de ressources**.
- Une **zone DNS** est un ensemble d'enregistrements de ressources appartenant à la même portion de l'espace de noms DNS.
- Un enregistrement de ressource est une **structure de base de données DNS** standard qui contient des informations utilisées pour traiter les requêtes DNS.

3. Zones DNS primaires et secondaires

3.2. Enregistrements de ressources

Liste des principaux types :

- **A :** Les enregistrements de ressources A (pour Adresse d'hôte) sont des mappages entre un nom d'hôte et une adresse IPv4 (adresse IP d'une longueur de **32 bits**). Ils représentent généralement la majorité des enregistrements de ressources des zones de recherches **directes**.
- **AAAA :** Les enregistrements de ressources de ce type sont des mappages entre un nom d'hôte et une adresse IPv6 (adresse IP d'une longueur de **128 bits**).
- **CNAME :** les enregistrements de ressources de type CNAME (Canonical NAME ou nom canonique) sont des mappages entre un **nom d'hôte** et un **autre nom d'hôte**. Ils permettent de créer des **alias** pour un nom d'hôte donné (c'est-à-dire d'associer plusieurs noms d'hôte à une même machine).

3. Zones DNS primaires et secondaires

3.2. Enregistrements de ressources

- **HINFO** : Les enregistrements de ressources de type HINFO (Host INFO ou informations sur l'hôte) spécifient le type de processeur (ex. : INTEL-386) et le système d'exploitation (ex. : WIN32) correspondant à un nom d'hôte.
- **MX** : les enregistrements de ressources de type **MX** (Mail eXchanger) identifient les serveurs de **messageries**. Chaque serveur de messagerie doit aussi disposer d'un enregistrement de ressource A. Il est possible de donner une priorité différente à chaque enregistrement MX.
- **NS** : les enregistrements de ressources de type **NS** (Name Server ou serveur de nom) identifient les serveurs DNS de la zone DNS. Ils sont utilisés dans le cadre de la délégation DNS.

3. Zones DNS primaires et secondaires

3.2. Enregistrements de ressources

- **PTR** : les enregistrements de ressources de type **PTR** (PoinTeR ou pointeur) sont des mappages entre une adresse IP et un nom d'hôte. Ils représentent la majorité des enregistrements des zones de recherches **inversées**.
- **SOA** : les enregistrements de ressources de type **SOA** (Start Of Authority) contiennent le **nom d'hôte** et **l'adresse IP** du serveur DNS qui héberge actuellement la **zone DNS principale**. Il y a un seul enregistrement **SOA** par zone DNS. C'est le **premier** enregistrement crée dans une zone DNS.

3. Zones DNS primaires et secondaires

3.2. Enregistrements de ressources

- **SRV** : les enregistrements de type **SRV** (service) permettent de mapper un nom d'hôte à un type de service donné, ils résolvent les noms des serveurs qui fournissent des services. Ainsi les enregistrements SRV peuvent permettre de retrouver la liste des serveurs HTTP ou bien encore des contrôleurs de domaines. Il est possible de donner une priorité différente à chaque enregistrement SRV.
- **WINS** : les enregistrements de ressources de type WINS indiquent au serveur DNS l'adresse ,IP d'un serveur WINS à contacter en cas d'échec lors de la résolution de nom d'hôte. Les enregistrements WINS ne peuvent être crée que dans une zone de recherche directe.
- **WINS-R** : les enregistrements de ressources de type WINS-R ne peuvent être crée que dans une zone de recherche inversée.

3. Zones DNS primaires et secondaires

3.3. Zones DNS

Une zone de noms ou zone DNS est un ensemble d'enregistrements de ressources appartenant à la même portion de l'espace de noms DNS. Par exemple une zone DNS peut contenir l'ensemble des enregistrements de ressource de type A (c'est-à-dire des mappages noms d'hôte / adresses IP) du domaine **laboms.lan**.

Il existe trois types de zones DNS :

- **Zones principales (Lecture/Écriture)**
- **Zones secondaires (Lecture seule)**
- **Zones de stub**

3. Zones DNS primaires et secondaires

3.3. Zones DNS

- **Zones principales (Lecture/Écriture)** doivent toujours être crées en premier pour une nouvelle zone. Elles peuvent ajouter, modifier et supprimer des enregistrements de ressource.
- **Zones secondaires (Lecture seule)** sont des **copies en lecture seule** d'une zone principale donnée. Elles contiennent toutes les modifications effectuées sur le fichier de la zone principale. Un serveur DNS qui héberge une zone secondaire ne peut pas ajouter ni modifier d'enregistrements de ressource. Les zones secondaires ont donc pour seul intérêt de garantir une tolérance aux pannes et pour réduire les charges pour la zone principale.
- **Zones de stub** sont des copies partielles d'une autre zone. Elle contient uniquement les enregistrements de ressource de types **SOA**, **NS** et **A**.

3. Zones DNS primaires et secondaires

3.3. Zones DNS

- Les enregistrements d'une zone DNS donnée sont stockés localement par le serveur DNS sous la forme d'un fichier.
- Si le serveur DNS joue aussi le rôle de contrôleur de domaine, il est possible de stocker les zones principales et les zones de stub dans le service d'annuaire Active Directory. On parlera alors de **zones intégrées à Active Directory**.
- Cette seconde solution apporte des avantages en termes de performance et de sécurité.

4. Délégation de Zones DNS

4.1. Intérêt de la délégation de zones DNS

Considérons une **arborescence de domaine**, doté d'un domaine parent et de deux sous domaines. La solution la plus simple est de mettre en place un serveur DNS dans le domaine parent avec une zone DNS primaire. Cependant, il peut être intéressant du point de vu des performances de mettre en place 3 serveur DNS (un dans le domaine parents et un dans chaque sous-domaine). Dans ce cas de figure (un serveur DNS dans chaque sous-domaine), **il faut créer des délégations de zones au niveau du serveur DNS appartenant au domaine parent**. Une délégation permet d'autoriser un autre serveur DNS à contrôler une partie des enregistrements de la zone.

4. Délégation de Zones DNS

4.1. Intérêt de la délégation de zones DNS

- Dans l'exemple ci-dessous, le domaine **supinfo.com** est subdivisé en deux sous-domaines nommés **administration.supinfo.com** et **students.supinfo.com**. Chaque domaine possède son propre serveur DNS. Le serveur DNS du domaine parent héberge la zone DNS primaire **supinfo.com**.

- On souhaite déléguer l'administration des enregistrements de ressources du domaine **administration.supinfo.com** et du domaine **students.supinfo.com** aux serveurs DNS respectivement nommés **dns.administration.supinfo.com** et **dns.students.supinfo.com**. Il va donc falloir créer **deux nouvelles délégations** sur le serveur DNS du domaine parent.

4. Délégation de Zones DNS

4.1. Intérêt de la délégation de zones DNS

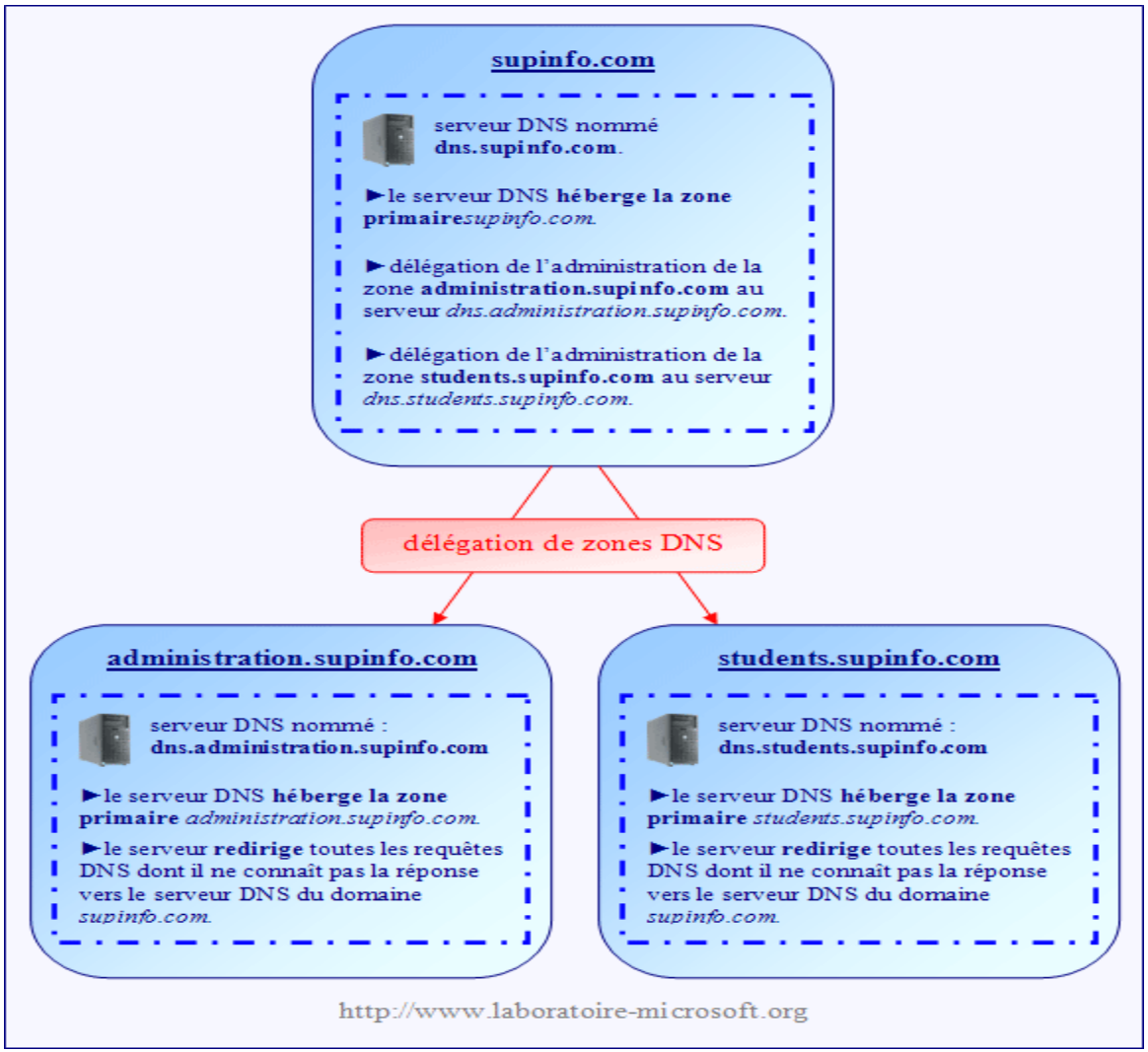


Figure 5.8 : Délégation de Zones

4. Délégation de Zones DNS

4.1. Intérêt de la délégation de zones DNS

- Une fois que les délégations sont créés, les machines clientes situées dans le domaine **supinfo.com** utilisent le serveur DNS situé dans le domaine parent pour résoudre les noms d'hôtes du domaine **supinfo.com** et utilisent les serveurs DNS situés dans les sous-domaines pour résoudre les noms d'hôtes des domaines **administration.supinfo.com** et **students.supinfo.com**.

- **En revanche** les machines clientes situées dans les sous-domaines peuvent uniquement résoudre les noms d'hôtes appartenant à leur sous-domaine. C'est pourquoi **il faut créer un redirecteur pointant vers le serveur DNS du domaine parent sur les serveurs DNS des sous-domaines**.

5. Conclusion

- Nous avons montré à travers ce chapitre **le fonctionnement du système DNS**.

- Le fonctionnement de la résolution de noms d'hôte grâce aux **redirecteurs** et à **la délégation de zones DNS** a ensuite été explicité.

- Nous avons aussi vu comment **les zones DNS intégrées à Active Directory et les zones de stub permettent d'augmenter la sécurité et les performances** du système DNS.