



Le service de résolution de noms

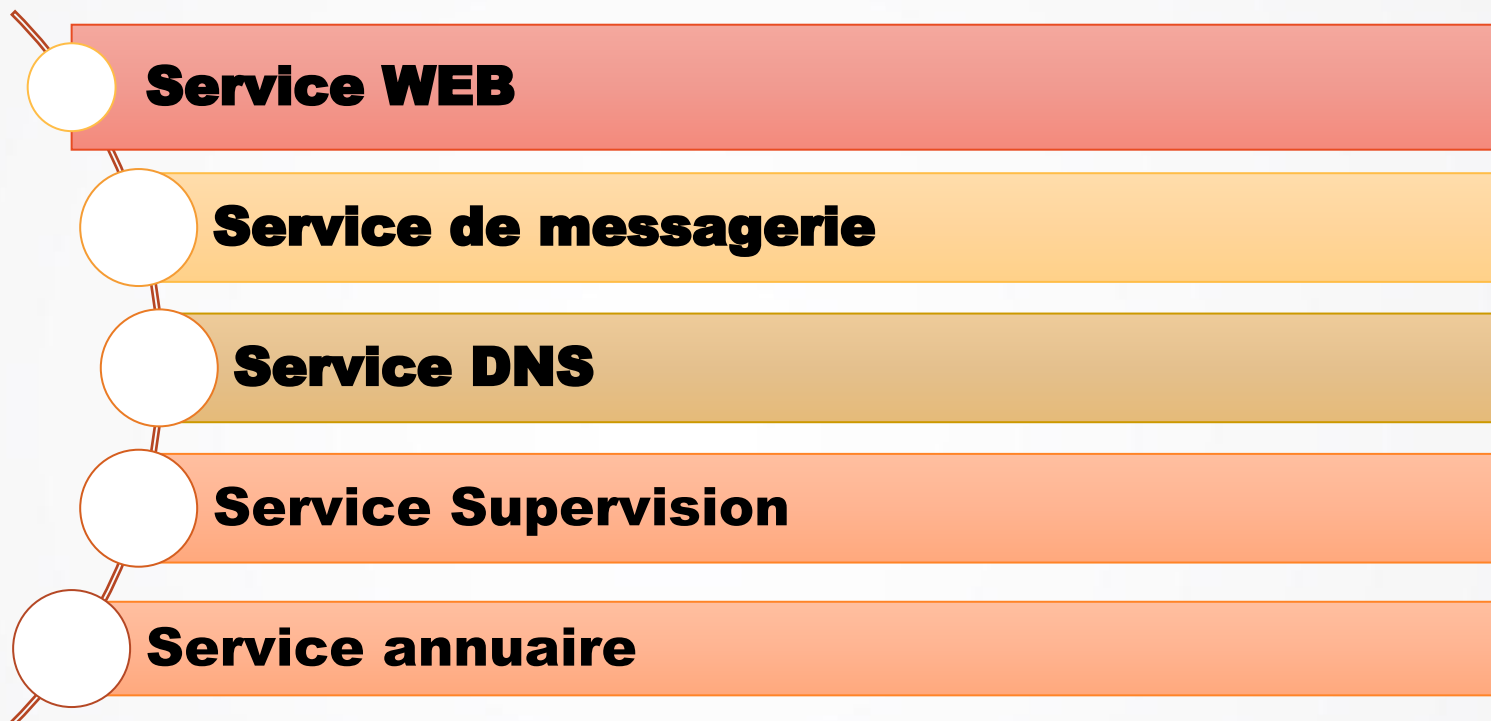
Niveau: 4^{ème}

Sabrina Laffet

Unité Pédagogique: Réseaux

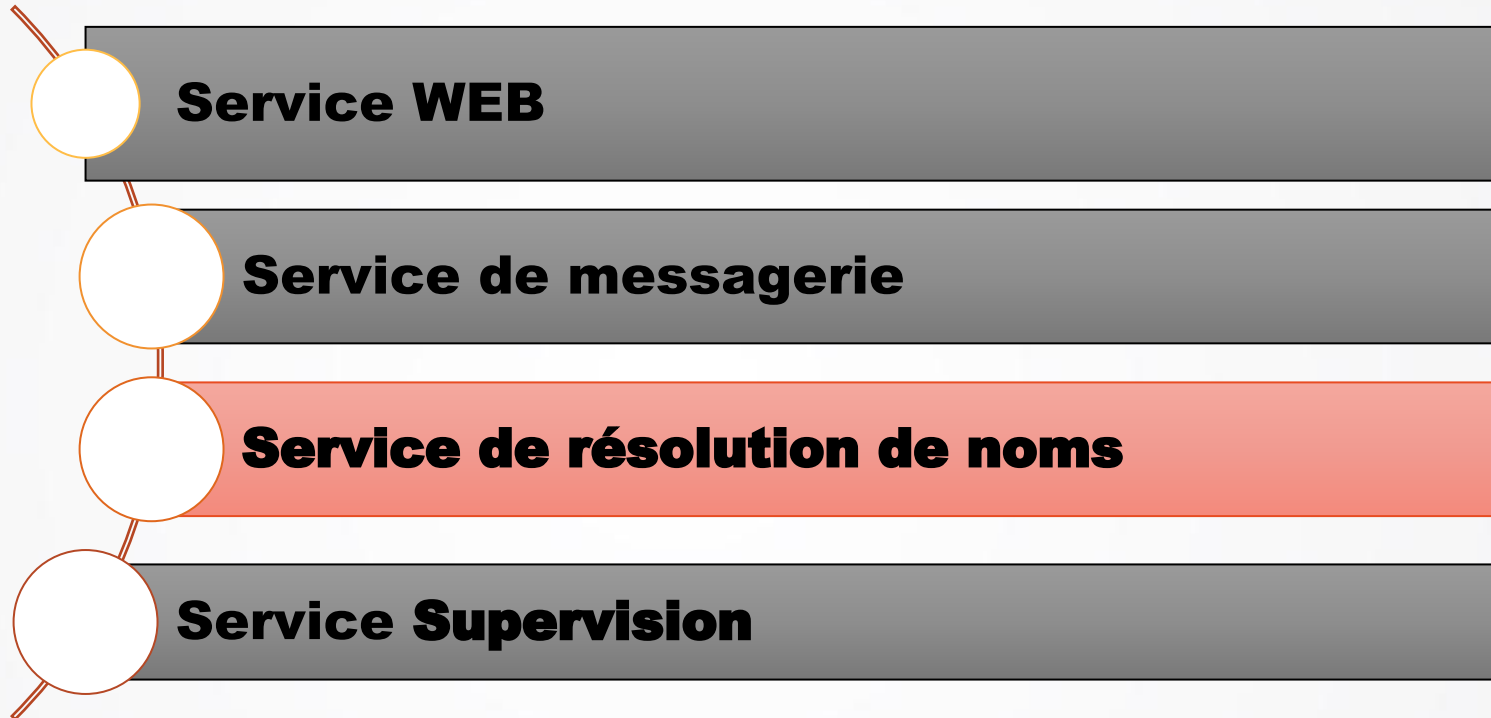
Module : Services et administration des réseaux

► **Structure du Module: SAR**





Cours: Service WEB





Objectifs et Pré requis



Objectifs Généraux

- Comprendre, installer et configurer le service DNS

Objectifs Spécifiques

- Comprendre le principe de DNS
- Maîtriser la notion d'un serveur DNS secondaire et du cache DNS.
- Maîtriser la configuration d'un serveur DNS primaire avec Bind.
- Configuration et tests du serveur de nom Bind.
- Intégration avec le service web

Pré requis

- Réseaux IP et routage , Administration Linux



Plan du Cours

Introduction

Comprendre le principe de DNS

L'hierarchie DNS

Conclusion

Introduction



La plupart des utilisateurs préfèrent en effet un nom convivial comme esprit.tn pour accéder à un ordinateur tel qu'un serveur de messagerie ou un serveur Web au lieu de l'utilisation des adresses IP.

⇒ Utilisation du fichier de résolution locale (hosts.txt) pour la résolution des nom pendant les années 80.



Toute modification dans ce fichier doit être faite sur toutes les machines.



La solution :
DNS

► Présentation



- Le **S**ystème des **N**oms de **D**omaine est un système **hiérarchique** qui assure la correspondance entre des **noms** et des **adresses IP**. Il utilise un protocole de communication client/serveur UDP/TCP sur le port **53**.

Résolution directe

www.esprit.tn



193.95.54.21

Résolution inverse

193.95.54.21



www.esprit.tn

► Le DNS n'est pas bijectif



www.esprit.tn



Serveur 1: Serveur 2:
192.168.1.10 192.168.1.11

Un service peut être déployer sur deux serveurs pour des raison de répartition de charge ou de haute disponibilité.

Dans ce cas, la réponse à la requête de résolution du nom de domaine www.esprit.tn peut être 192.168.1.10 ou bien 192.168.1.11

► Le DNS n'est pas bijectif



Serveur :
192.168.1.10

www.esprit.tn

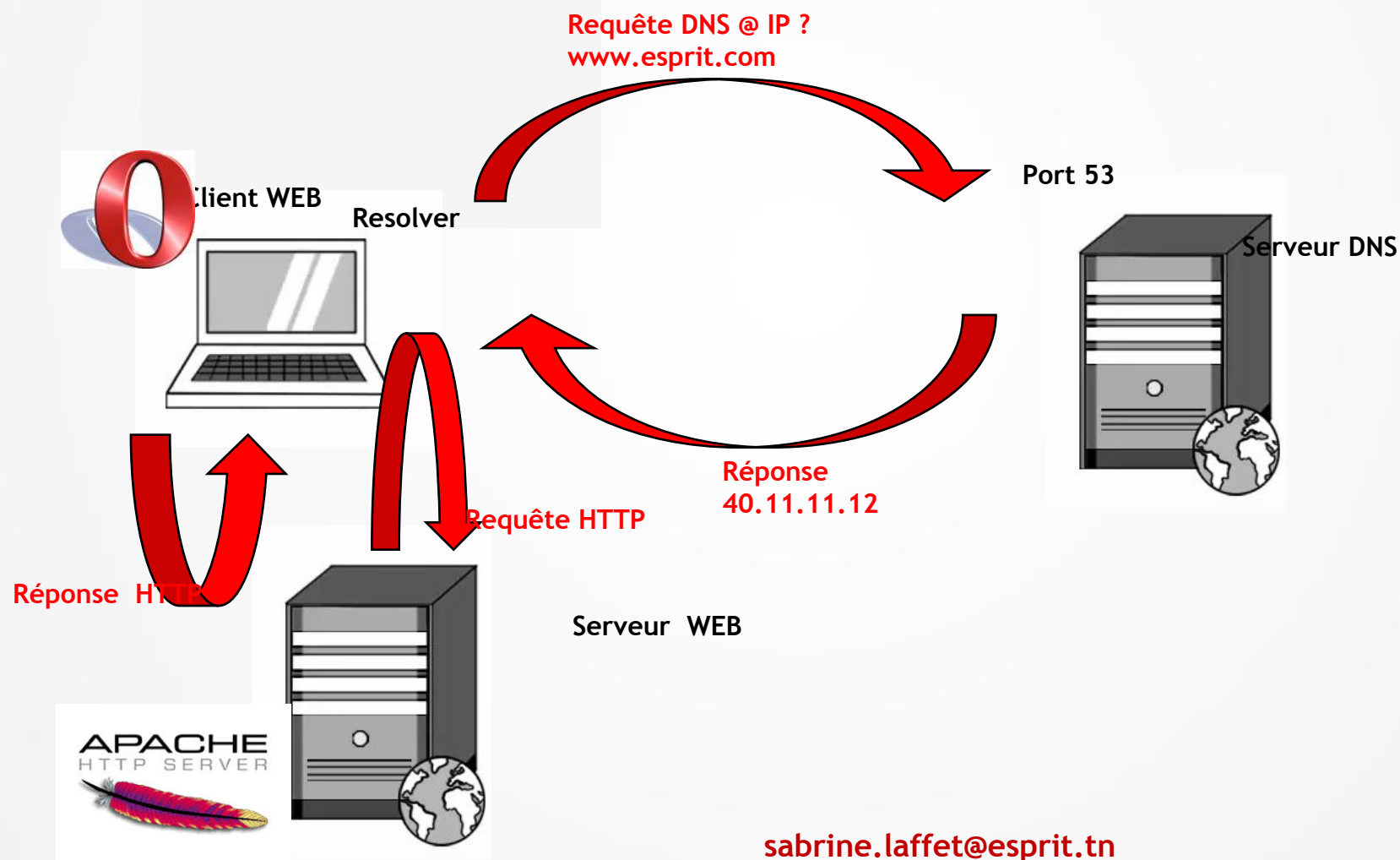
mail.esprit.tn

ftp.esprit.tn

Différents services (web, mail, transfert de fichier ...) peuvent être installer sur la même machine physique.

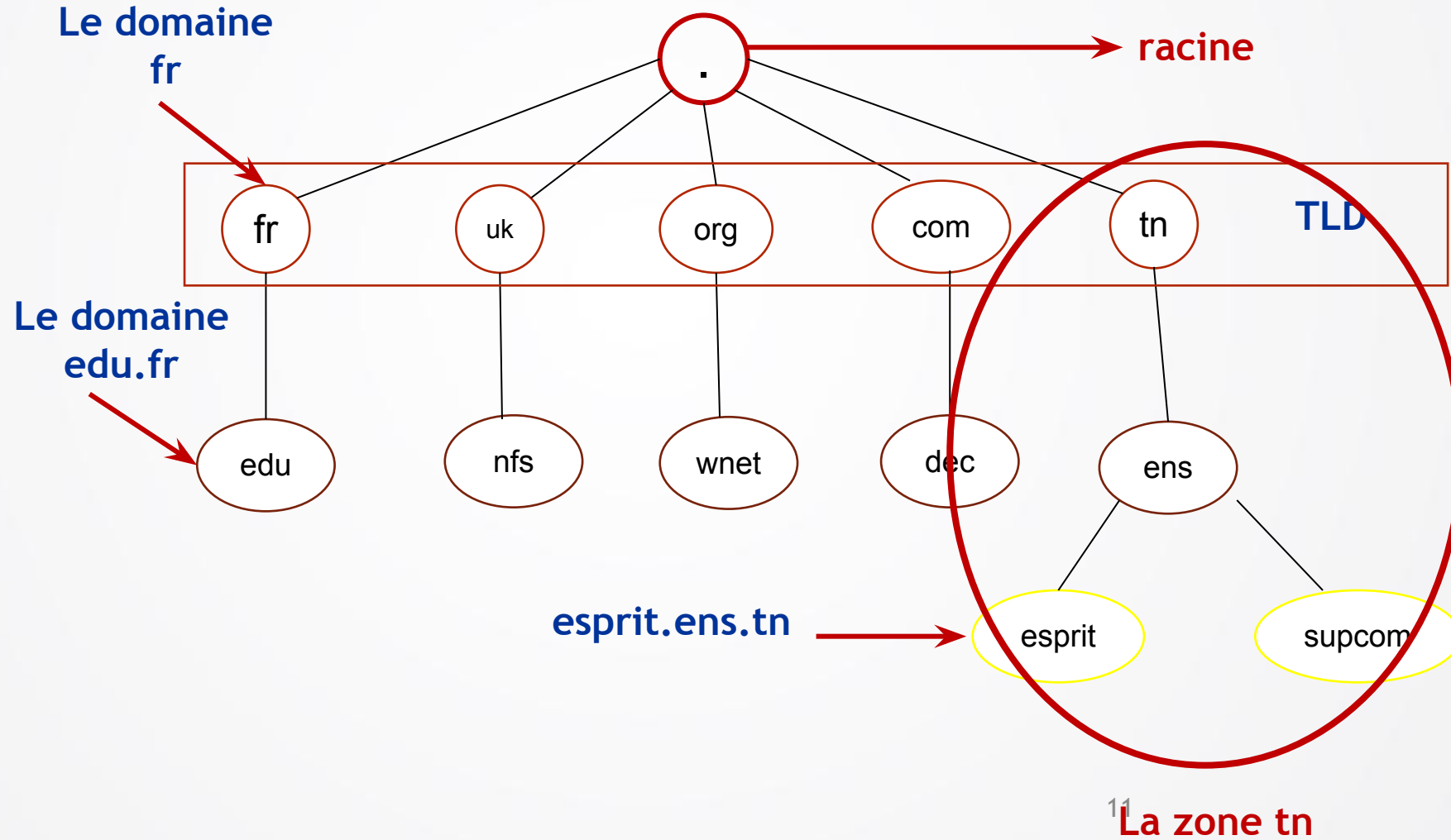
Dans ce cas, la réponse à la requête de résolution du nom de domaine www.esprit.tn , mail.esprit.tn et ftp.esprit.tn est l'adresse 192.168.1.10.

► Architecture du service DNS





L'hierarchie DNS





L'hierarchie DNS

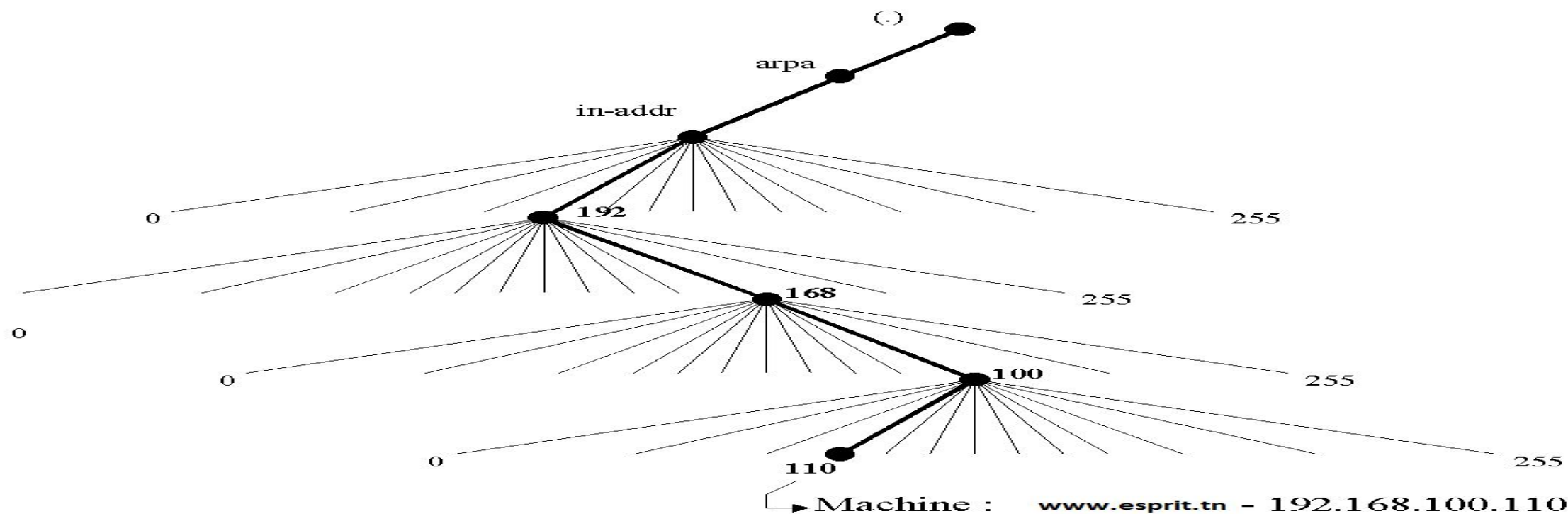


- ✓ Les niveaux supérieurs **TLD (Top Level Domain)** sont organisés au niveau géographique et/ou thématiques .fr .uz .uk .com .mil .
- ✓ Chaque nœud définit un domaine : suite de noms séparés par des points
- ✓ Les nœuds possèdent tous un nom (de 0 à 63 caractères) et correspondant à une ressource (qui peut être vide).
- ✓ Deux nœuds frères ne peuvent pas avoir le même nom.
- ✓ Le nœud racine (*root*) est constitué de 0 caractères
- ✓ Une "zone" est une organisation logique (ou pour être plus précis, une organisation administrative) des domaines. Le rôle d'une zone est principalement de simplifier l'administration des domaines. Le domaine «.com» peut être découpé en plusieurs zones, z1.com, z2.com, ...zn.com. L'administration des zones sera déléguée afin de simplifier la gestion globale du domaine.

► La résolution inverse



- Le processus doit fournir, pour une adresse IP, le nom correspondant.
- Pour cela il y a une zone particulière, in-addr.arpa, qui permet la résolution inverse d'adresse IP.



L'adresse ip 192.168.100.110 correspond au sous-domaine 110.100.168.192.in-addr.arpa qui renvoie le nom qualifié FQDN: www.esprit.tn



L'arborescence

Parcours de l'arbre et nom de domaine

- la descente dans l'arbre est représentée de la droite vers la gauche
- chaque niveau de l'arborescence est séparé par un point

Pour déterminer l'adresse IP correspondante au nom : `www.esprit.ens.tn`.

- 1- trouver un NS (serveur de noms) de la racine «.»
- 2-obtenir le NS de `tn`.
- 3-Interroger le DNS de la zone `tn`. pour un NS de `ens.tn`.
- 4-Le NS de `esprit.ens.tn`.identifie `www`.et renvoi son adresse IP

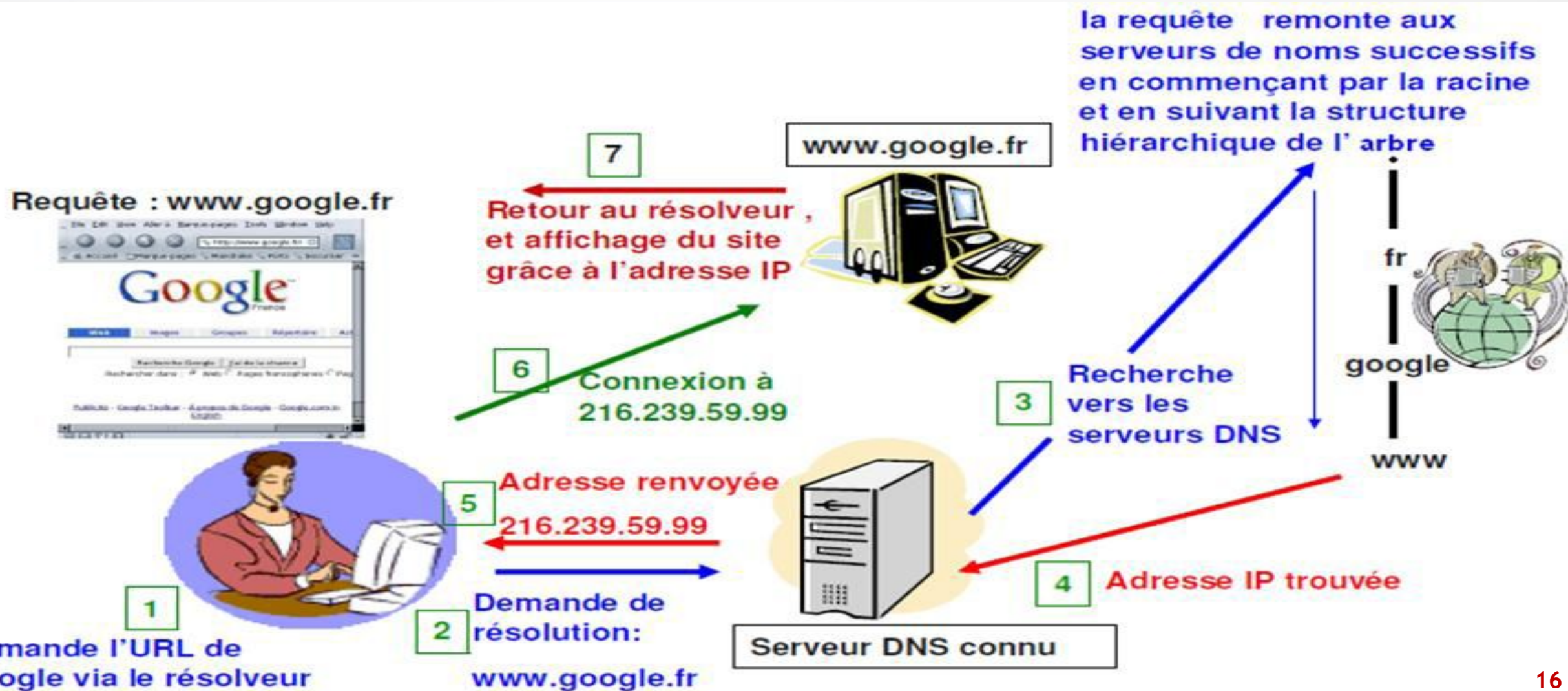
c'est le rôle du resolver

► Les serveurs racines DNS



Ensemble de 13 serveurs (13 Racines DNS) dans le monde gérés par l'ICANN.

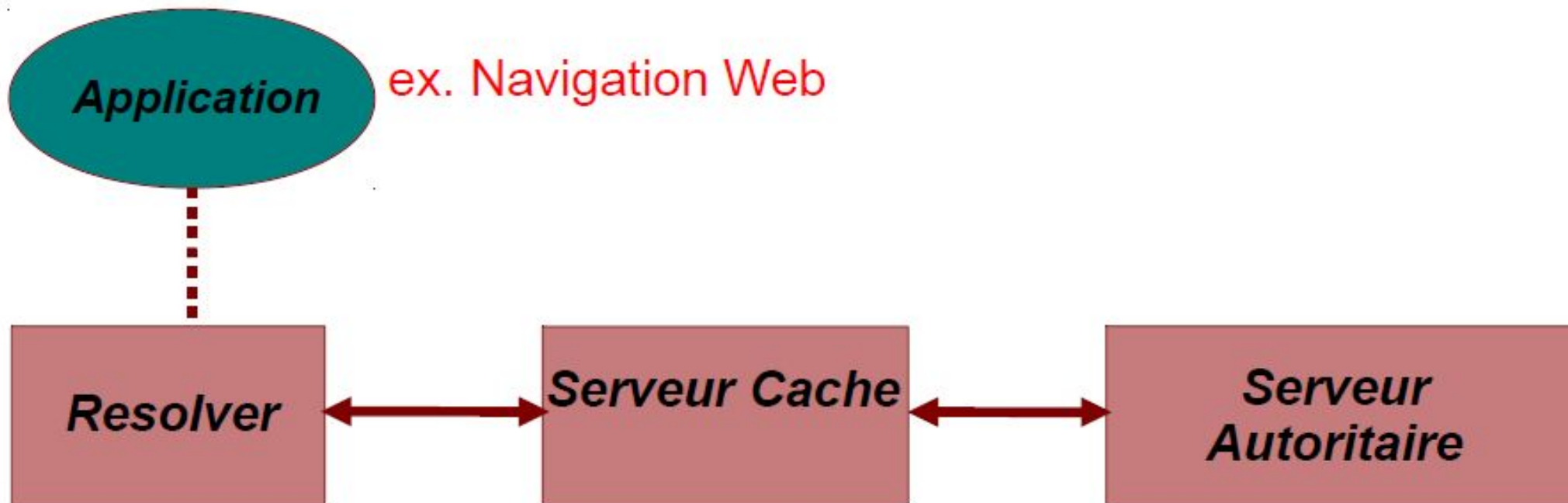
► L'arborescence



► Rôles



Il y a trois rôles impliqués dans le DNS





Rôles

Le RESOLVER

- Prends la demande de l'application,
- Formate la demande dans le paquet UDP
- Envoi la demande au cache DNS

SERVEUR CACHE

- Renvoie la réponse si elle est déjà connue
 - Autrement il recherche un serveur autoritaire qui a l'information
- Cache le résultat pour de requêtes futures

SERVEUR AUTORITAIRE

- Contient l'information réelle mise dans le DNS par le propriétaire du domaine



Le Resolver

Le résolveur de noms (resolver) est un programme qui extrait l'information des serveurs de noms en réponse d'une requête émanant d'un client. Il élabore l'interrogation.

- **Fonctionnement :**

- Contacte un serveur de nom (dont l' (les) adresse(s) est (sont) configurées sur la machine exécutant ce resolver)
- Interprète les réponses
- Retourne l'information au logiciel appelant
- Gestion de cache (dépend de la mise en œuvre)



Le serveur



Le serveur autoritaire (serveur maître)

- Possède une base d'informations d'une zone dont il a l'autorité administrative.

Duplication de DNS (serveur esclaves)

- Les données sont enregistrées sur un serveur autoritaire (maître) et copier vers un (des) serveur(s) autoritaire(s) (esclave(s))
- Pas de différence visible entre les 2 types de serveurs depuis l'Internet, Ces serveurs sont aussi appelés serveurs primaires et secondaires.
- Un serveur peut être primaire pour certaines zones et secondaires pour d'autres



NEXT



1.Installer et configurer: Bind.

2.Configuration et tests du serveur de nom Bind.

3. Intégration avec le service web



► **Le serveur DNS: BIND9**

- - L'implémentation DNS la plus utilisée sur Internet est **Berkeley Internet Name Domain (BIND) software**.
- - La première version de BIND a été conçue par quatre étudiants diplômés de l'Université de Californie (Berkeley) sur la base de BSD 4.3
- L'installation du serveur BIND est très simple sous RedHat
`yum -y install bind bind-utils`

► Définition des zones



```
$TTL 3h
@          IN      SOA      ns.esprit.tn.      hostmaster. esprit.tn. (
                                2009090601      ; Serial
                                8H                ; Refresh
                                2H                ; Retry
                                1W                ; Expire
                                1D )             ; Negative Cache TTL
```

TTL: Time To Live : Indique pendant combien de temps un enregistrement (réponse) peut être gardée en cache

@: Désigne l'origine du domaine. Remplace le nom de domaine donné dans le fichier named.conf pour la zone concernée

SOA: une zone sous l'autorité d'un serveur de noms : SOA.

IN: signifie que l'on a affaire à une zone Internet

NS: Liste des serveurs de noms pour cette zone

► Définition des zones



- **Serial** : incrémenté par l'administrateur de la zone à chaque modification. Permet la détection d'un changement sur la zone et donc la nécessité de la recharger
- **Refresh**: rythme que les serveurs secondaires doivent vérifier le numéro de série sur le primaire
- **Retry**: à quel rythme les serveurs secondaires doivent essayer de contacter le primaire en cas d'échecs
- **Expire** :si le secondaire n'a pu contacter le primaire durant la période définie, il supprime les données locales des zones du primaire
- **Negativecache TTL** : pendant combien de temps un cache peut garder une requête non existante



Merci
Pour Votre Attention