B1
(2ème séance)

Cours réalisé par : Fabien LAFAGE

1. Finaliser les séances précédentes (si il reste des points à traiter)

- ✔ Installation de Windows Server 2019 terminée (avec Windows Update à jour)

2. Installation du rôle Serveur DNS

✔ Prérequis :

- Nommer correctement le serveur, réfléchir à une nomenclature de nommage et la respecter (dans notre exemple : SRV-WIN2019 limité à 15 caractères)
- Configurer une IP statique pour le serveur (indispensable pour délivrer correctement les futurs services) :
  - VMware => Virtual Network Editor : la VM WindowsServer2016 devrait utiliser VMnet8 (NAT), désactiver « Use local DHCP service... » sur cet adaptateur, le serveur DHCP sera un rôle à installer sur le serveur WindowsServer2016
  - IP fixe sur le serveur ; repérer l'adresse réseau sur l'adaptateur, 192.168.5.0 dans mon cas, donc :
    - IP : 192.168.5.11
    - Masque : 255.255.255.0
    - Routeur : 192.168.5.2
    - DNS : 192.168.5.2
- Penser à installer les outils VMware pour plus de confort
- Formater la dernière partition en NTFS (lecteur D:) (C: 50 Go, D: espace restant,)
- Prendre un cliché instantané : AvantDNS

✔ Différence entre un rôle et une fonctionnalité

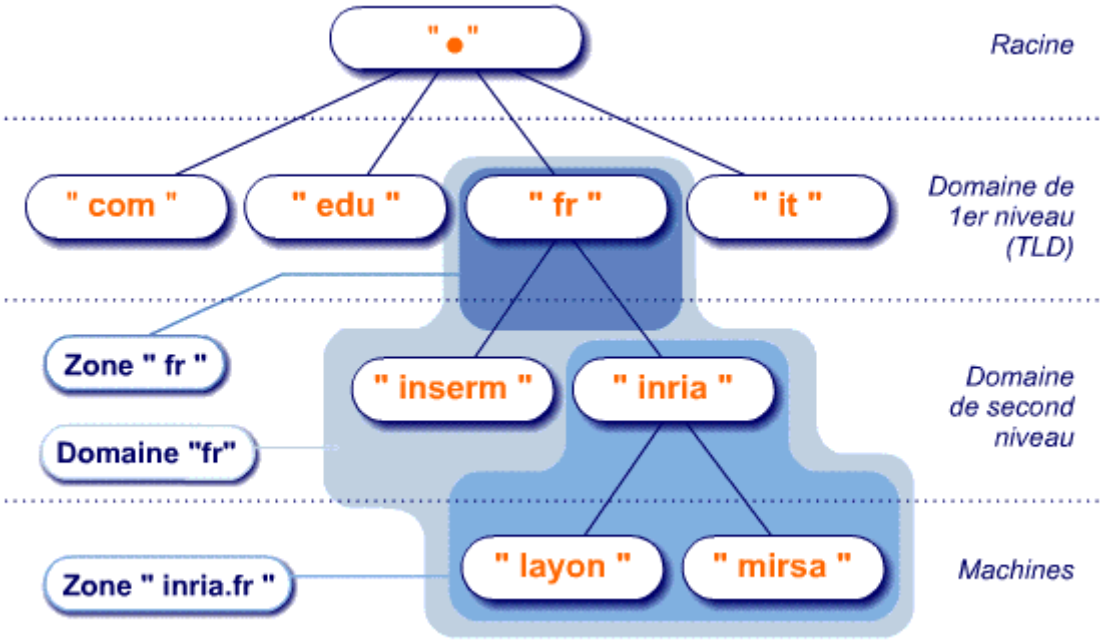
- Rôle : Ensemble de programmes logiciels qui, une fois installés et correctement configurés, permettent à un ordinateur de remplir une fonction spécifique
- Fonctionnalité : Programme logiciel qui, bien qu'il ne fasse pas directement partie des rôles, peut prendre en charge ou augmenter la fonctionnalité d'un ou de plusieurs rôles, ou encore améliorer la fonctionnalité de la totalité du serveur, quels que soient les rôles installés

✔ Rappel : DNS

Certaines informations sont tirées du site : http://www.commentcamarche.net/contents/internet/dns.php3

- Un ordinateur directement connecté à internet dispose d'au moins une adresse IP
- Choix de l'utilisation d'un FQDN (Full Qualified Domain Name) plutôt qu'une IP (plus lisible)
- DNS (Domain Name System) : résolution de noms de domaines et d'adresses (nom de domaine vers IP et inversement)
- Gestion par fichier « hosts » sur l'OS de l'ordinateur lui-même et/ou par une relation client/serveur DNS

- Arborescences d'un DNS :



Information tirée du site : http://www.afnic.fr/doc/formations/autoformation/dns

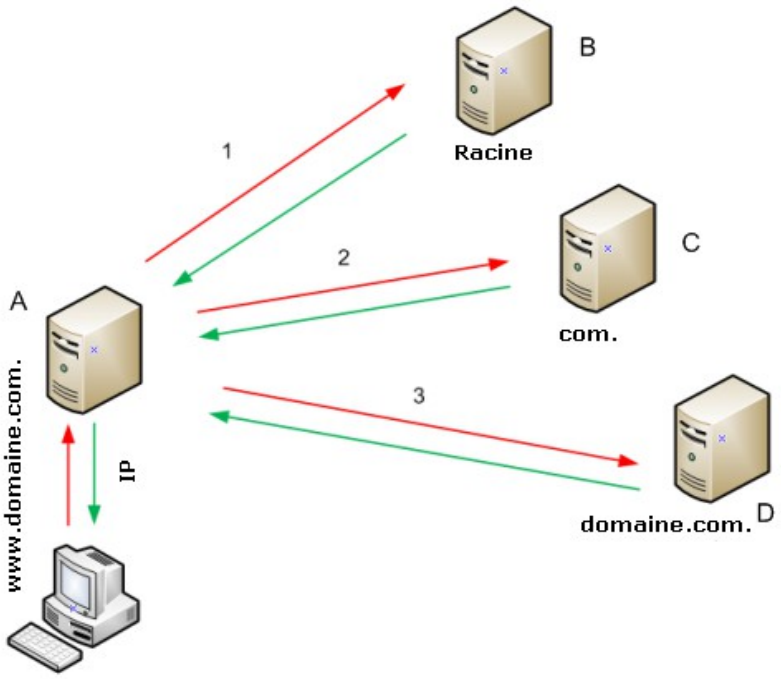
- Exemple : layon.inria.fr.
  - Racine : .
  - TLD (Top Level Domains) : fr
  - Domaine (ou sous-domaine du domaine fr) : inria
  - Machine (ou Hôte) : layon
  - FQDN (Full Qualified Domain Name) : layon.inria.fr.
  - La profondeur maximale de l'arborescence est de 127 niveaux et la longueur maximale d'un nom FQDN est de 255 caractères. L'adresse FQDN permet de repérer de façon unique une machine sur le réseau des réseaux

- Serveurs de noms de domaines :
  - Serveurs de noms racine (TLD) : Il en existe treize, répartis sur la planète, possédant les noms « a.root-servers.net » à « m.root-servers.net »
  - 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
  - Chaque serveur de nom est déclaré dans à un serveur de nom de domaine de niveau immédiatement supérieur, ce qui permet implicitement une délégation d'autorité sur les domaines. Le système de nom est une architecture distribuée, où chaque entité est responsable de la gestion de son nom de domaine. Il n'existe donc pas d'organisme ayant à charge la gestion de l'ensemble des noms de domaines
  - Un serveur de noms définit une zone, c'est-à-dire un ensemble de domaines sur lequel le serveur a autorité

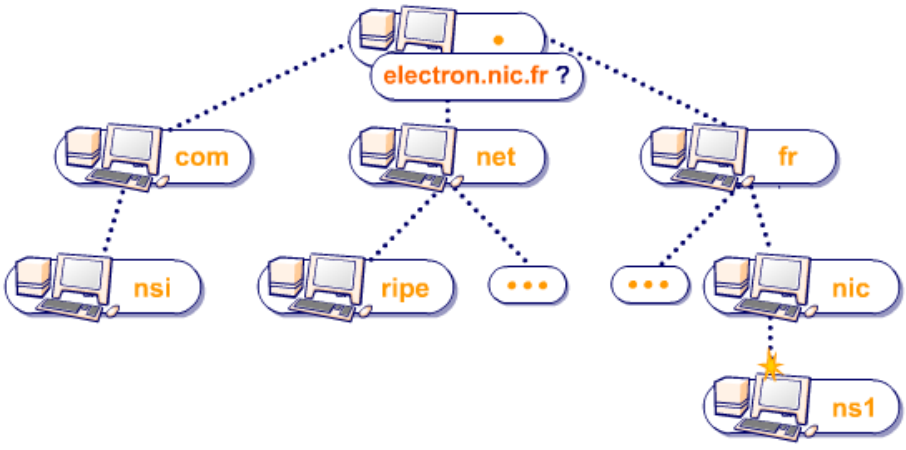
- TLD : il en existe deux catégories, gTLD (generic TLD, ex: .com, .edu, .net etc.) et ccTLD (country code TLD, ex: .fr, .uk, .us etc.)

- Résolution de nom de domaine :

Exemple 1 :



Exemple 2 :

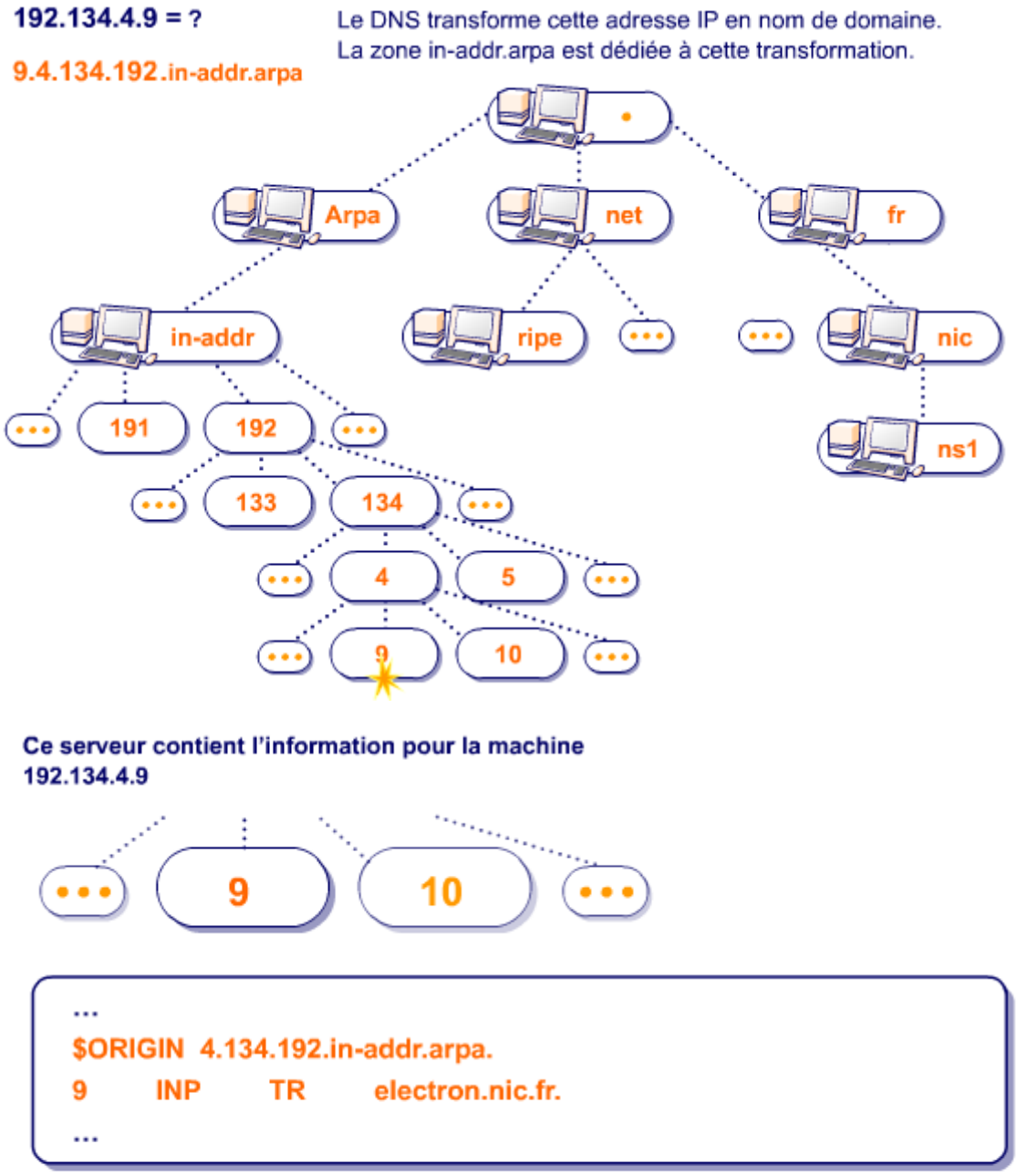


ns1 est le serveur de nom primaire de la zone nic.fr,
et contient donc les informations sur les machines de la zone.

...			
toto	IN	A	192.134.4.8
electron	IN	A	192.134.4.9
www	IN	A	192.134.4.10
...			

electron.nic.fr → 192.134.4.9

– Résolution inverse :



– RR (Resource Records), un enregistrement DNS contient les informations suivantes :

Nom de domaine (FQDN)	TTL	Type	Classe	RData
www.domaine.com.	3600	A	IN	163.5.255.85

- Nom de domaine : le nom de domaine doit être un nom FQDN, c'est-à-dire être terminé par un point. Si le point est omis, le nom de domaine est relatif, c'est-à-dire que le nom de domaine principal suffixera le domaine saisi
- TTL (Time To Live) : espérance de vie des enregistrements d'un domaine, qui permet aux serveurs intermédiaires de connaître la date de péremption des informations et ainsi savoir s'il est nécessaire ou non de la revérifier
- Type : une valeur sur 16 bits spécifiant le type de ressource décrit par l'enregistrement. Le type de ressource peut être un des suivants :
  - A : il s'agit du type de base établissant la correspondance entre un nom canonique et une adresse IP. Par ailleurs il peut exister plusieurs enregistrements A, correspondant aux différentes machines du réseau (serveurs)
  - CNAME (Canonical Name) : il permet de faire correspondre un alias au nom canonique. Il est particulièrement utile pour fournir des noms alternatifs correspondant aux différents services d'une même machine
  - HINFO : il s'agit d'un champ uniquement descriptif permettant de décrire notamment le matériel (CPU) et le système d'exploitation (OS) d'un hôte. Il est généralement conseillé de ne pas le renseigner afin de ne pas fournir d'éléments d'informations pouvant se révéler utiles pour des pirates informatiques
  - MX (Mail eXchange) : correspond au serveur de gestion du courrier. Lorsqu'un utilisateur envoie un courrier électronique à une adresse (utilisateur@domaine), le serveur de courrier sortant interroge le serveur de nom ayant autorité sur le domaine afin d'obtenir l'enregistrement MX. Il peut exister plusieurs MX par domaine, afin de fournir une redondance en cas de panne du serveur de messagerie principal. Ainsi l'enregistrement MX permet de définir une priorité avec une valeur pouvant aller de 0 à 65 535
  - NS : correspond au serveur de noms ayant autorité sur le domaine
  - PTR : un pointeur vers une autre partie de l'espace de noms de domaines
  - SOA (Start Of Authority) : le champ SOA permet de décrire le serveur de nom ayant autorité sur la zone, ainsi que l'adresse électronique du contact technique (dont le caractère « @ » est remplacé par un point)
- Classe : la classe peut être soit IN (correspondant aux protocoles d'internet), soit CH (pour le système chaotique)
- RDATA : il s'agit des données correspondant à l'enregistrement. Voici les informations attendues selon le type d'enregistrement :
  - A : une adresse IP sur 32 bits ;
  - CNAME : un nom de domaine ;
  - MX : une valeur de priorité sur 16 bits, suivi d'un nom d'hôte ;
  - NS : un nom d'hôte ;
  - PTR : un nom de domaine ;
  - SOA : plusieurs champs

✔ Comment installer le rôle Serveur DNS dans Windows Server 2016

- Ajouter des rôles
- Serveur DNS
- Installer
- Voir les fonctionnalités ajoutées
- Lancer le Gestionnaire DNS
- Sélectionner le serveur, action, Configurer un serveur DNS
- Créer des zones de recherche directe et inversée (pour les grands réseaux)
- Créer la zone de recherche directe maintenant
- Zone principale
- Bien définir le nom de sa zone DNS :

ⓘ Étape importante, le fonctionnement de l'AD repose essentiellement sur le service DNS, le choix du nom de domaine doit être réfléchi en amont (changement/migration du nom de domaine très long, changement futur de nom d'entreprise ? nom passe-partout ? ville ? région ? nom de domaine privé ou public ? méthode du split-dns ? choix du TLD ? TLD local à bannir ? TLD plus long que deux lettres ? TLD à éviter : http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains)
(Whois.Net : trouver à qui appartient le domaine)

Choix pour nos tests : contoso.adds

- Créer le nouveau fichier nommé contoso.adds.dns
- Ne pas autoriser les mises à jour dynamiques (plus tard avec AD)
- Créer une zone de recherche inversée
- Zone principale
- IPv4
- 192.168.5 (dans mon cas, vérifier quel est votre réseau)
- Créer le nouveau fichier nommé : 5.168.192.in-addr.arpa.dns
- Ne pas autoriser les mises à jour dynamiques (plus tard avec AD)
- Ne pas rediriger les requêtes (Windows Server 2016 le fait nativement à l'aide des serveurs racines)

- Exécuter nslookup : quelle est votre serveur DNS par défaut ?
- Changer l'IP du serveur DNS primaire de votre carte réseau vers l'IP de votre serveur (qui fait maintenant serveur DNS)
- Exécuter nslookup : quelle est votre serveur DNS par défaut ?
- Créer un nouvel hôte (A) (avec PTR) : srv-win2019 avec votre IP
- Exécuter nslookup : quelle est votre serveur DNS par défaut ?
- Tester si le DNS répond aux requêtes (test avec srv-win2019.contoso.adds)
- Créer un nouvel alias (CNAME), exemple : TestAlias qui pointe sur l'hôte srv-win2019
- Tester si le DNS répond aux requêtes (test ping avec TestAlias.contoso.adds)

✔ Installer/désinstaller/gérer DNS en lignes de commandes

- Installer : [ ]
- Désinstaller : [ ]

- Ajouter une zone de recherche directe, principale :
  - [ ]
- Ajouter une zone de recherche inversée :
  - [ ]
- Créer un nouvel hôte (A) :
  - [ ]
- Créer un nouvel alias (CNAME) :
  - [ ]

- Créer un nouvel hôte (A) vers l'IP de la machine hôte :
  - [ ]
  - tester la réponse de hote.contoso.adds

- Prendre un cliché instantané : ApresDNS

- Commande non approuvée depuis Windows Server 2008 R2, trouver la solution pour installer/désinstaller un rôle avec PowerShell
  - [ ]
  - [ ]
  - [ ]

- Désinstaller le rôle DNS (commande PowerShell)
- Réinstaller le rôle DNS (commande PowerShell)
- Ajouter une zone de recherche directe, principale (commande PowerShell)
- Ajouter une zone de recherche inversée (commande PowerShell)