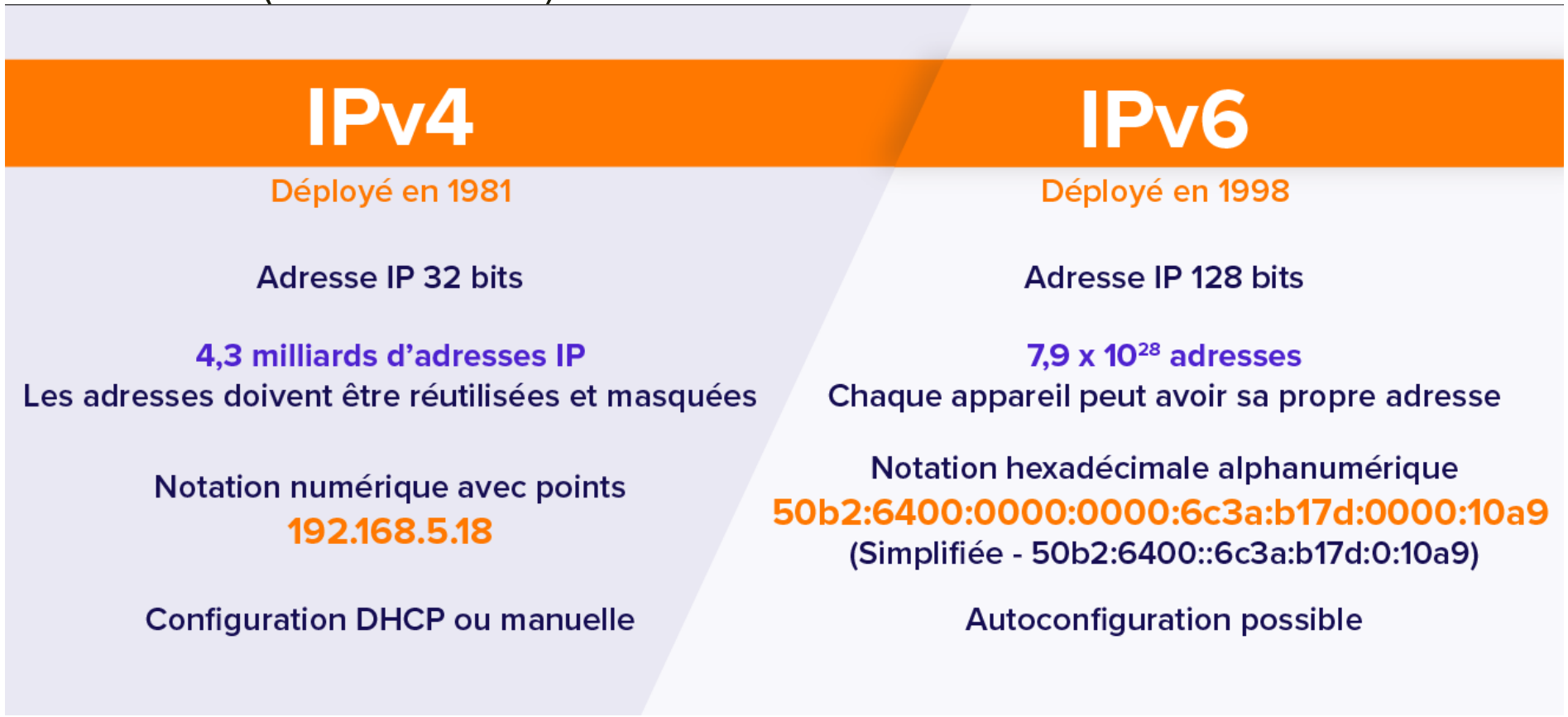
ADMINISTRATION DES RÉSEAUX

CHAPITRE 2 - DNS

Mohamed Yassine SAMIRI
my.samiri@gmail.com

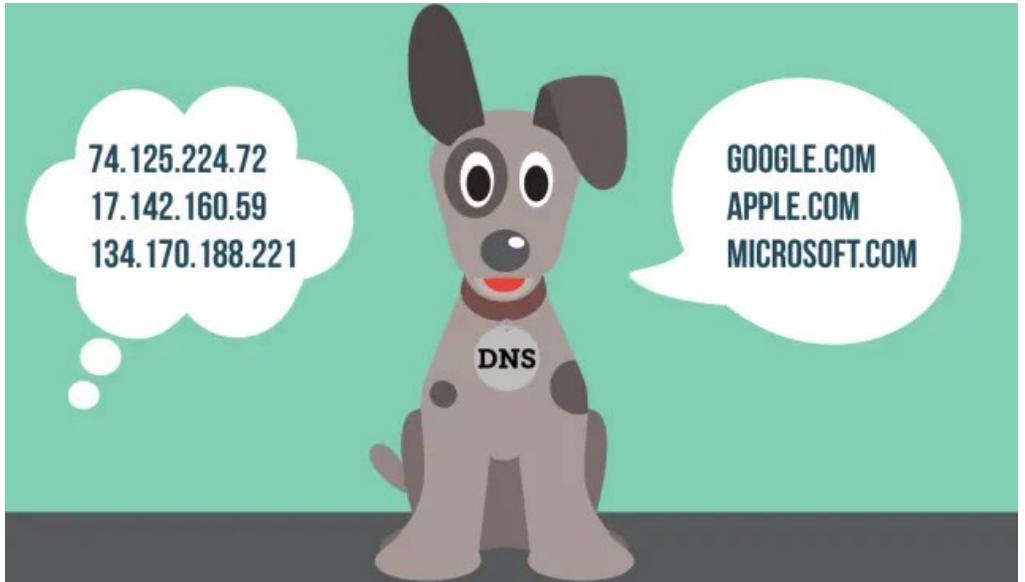
Problématique

- Les ordinateurs connectés à un réseau, (Internet par exemple), possèdent tous une adresse IP
- Ces adresses IP sont représentées au format numérique. Elles existent en deux versions (IPv4 et IPv6).



Problématique

- Il n'est pas évident pour un être humain de retenir ces numéros lorsque le nombre d'adresses IP devient important.
- Nous avons beau être des êtres humains avec une bonne mémoire, notre cerveau n'est pas fait pour retenir des séries de chiffres comme **190.253.78.250**. On aimerait mieux avoir à retenir des noms comme **upm.ac.ma**
- **Solution :** un mécanisme permettant d'associer à une adresse IP un nom intelligible, humainement plus simple à retenir.



1ère solution: Fichiers Hosts et LMHosts

- Au départ, chaque machine stockait localement les mappages

  noms / adresse IP
- Un mappage est une correspondance entre un nom et une adresse IP.
- Ce système a l'inconvénient de demander une trop lourde charge administrative
- 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

2ème solution: NetBios

- Le premier mécanisme de résolution de noms mis en place sous Windows est NetBIOS (Network Basic Input Output System)
- Cette méthode de résolution de noms a de nombreux inconvénients :
  - *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.*

Solution actuelle: Le système DNS

- Le DNS (Dynamic Naming System)
- Proposé par Paul. Mockapetris (ISI et MIT) en 1987. (RFC1034)

https://www.youtube.com/watch?v=Xt9r_Ae5Crw

- Le système DNS (Dynamic Naming System) introduit une convention de nommage hiérarchique des domaines qui commence par un domaine racine appelé ".".

Solution actuelle: Le système DNS

- Ce système propose :
  - *un espace de noms hiérarchique permettant de garantir l'unicité d'un nom dans une structure arborescente.*
  - *un système de serveurs distribués permettant de rendre disponible l'espace de noms.*
  - *un système de clients permettant de « résoudre » les noms de domaines, c'est-à-dire interroger les serveurs afin de connaître l'adresse IP correspondant à un nom.*

DNS: un arbre avec des branches

Une arborescence ordonnée

- Le système DNS, vous l'utilisez tous les jours quand vous naviguez sur Internet. Lorsque vous voulez accéder à WWW.GOOGLE.COM, le système DNS se charge de convertir (on parle de **résolution**) le nom du site web demandé en adresse IP.
- Un nom de domaine se décompose en plusieurs parties. Prenons l'exemple suivant : **WWW.GOOGLE.COM**
  - *Chaque partie est séparée par un point.*
  - *On trouve **l'extension** en premier (en premier, mais **en partant de la droite**) ; on parle de **Top Level Domain (TLD).***
  - *Il existe des TLD nationaux (ma, us, fr, de, es, etc.) et les TLD génériques (com, org, net, biz, etc.).*

DNS: un arbre avec des branches

Top Level Domain (TLD).

- *Il existe plus de 700 TLD*
- *2000 nouveau TLD on été déposé en attente d'être approuvés par l'IANA*

Consulter la liste des TLD:

- *https://www.iana.org/domains/root/db*

DNS: un arbre avec des branches

Une arborescence ordonnée

Ici, on a le découpage suivant : **WWW.GOOGLE.COM**

- Il existe une infinité de possibilités pour **la deuxième partie** après le TLD.
- Cela correspond à tous les sites qui existent : google.ma, facebook.com, ovh.net, twitter.com, etc.
- Comme vous le voyez, **google.com** est un sous-domaine de **com**. Le domaine **com** englobe tous les sous-domaines finissant par **com**.

DNS: un arbre avec des branches

Une arborescence ordonnée

Ici, on a le découpage suivant : **WWW.GOOGLE.COM**

- La troisième partie est exactement comme la seconde.
- On y retrouve généralement le fameux "WWW", ce qui nous donne des noms de domaine comme www.facebook.com.
- www peut soit être **un sous-domaine** de google.com, mais dans ce cas il pourrait y avoir encore des machines ou des sous-domaines à ce domaine, soit être directement **le nom d'une machine**.
  Ici, www est le nom d'une machine dans le domaine google.com.
- On peut bien entendu ajouter autant de troisièmes parties que nécessaire, ce qui peut vous conduire à avoir un nom de domaine comme :
  WWW.UPM.123.NEW.SUPER.GOOGLE.COM

Anatomie d’un nom DNS

DNS suit des règles pour nommer les ordinateurs.

Les noms DNS sont segmentés

- Les noms DNS sont organisés en éléments séparés par des points.
- Par exemple, le nom d'ordinateur MONPC.UPM.AC.MA est constitué de quatre parties.
- Chaque partie du nom ne peut pas excéder **63 caractères** de longueur et le nom entier ne peut dépasser les **255 caractères au total**.

Anatomie d’un nom DNS

Nom de domaine internationalisé (RFC 5890)

- Un nom de domaine Internet qui peut contenir des caractères non définis par le standard ASCII et la RFC 1123.
- Parmi ces caractères, on trouve notamment les lettres accentuées courantes dans de nombreuses langues européennes

- Le 1er Nom de domaine arabe
  - http://وزارة-الأتصالات.مصر

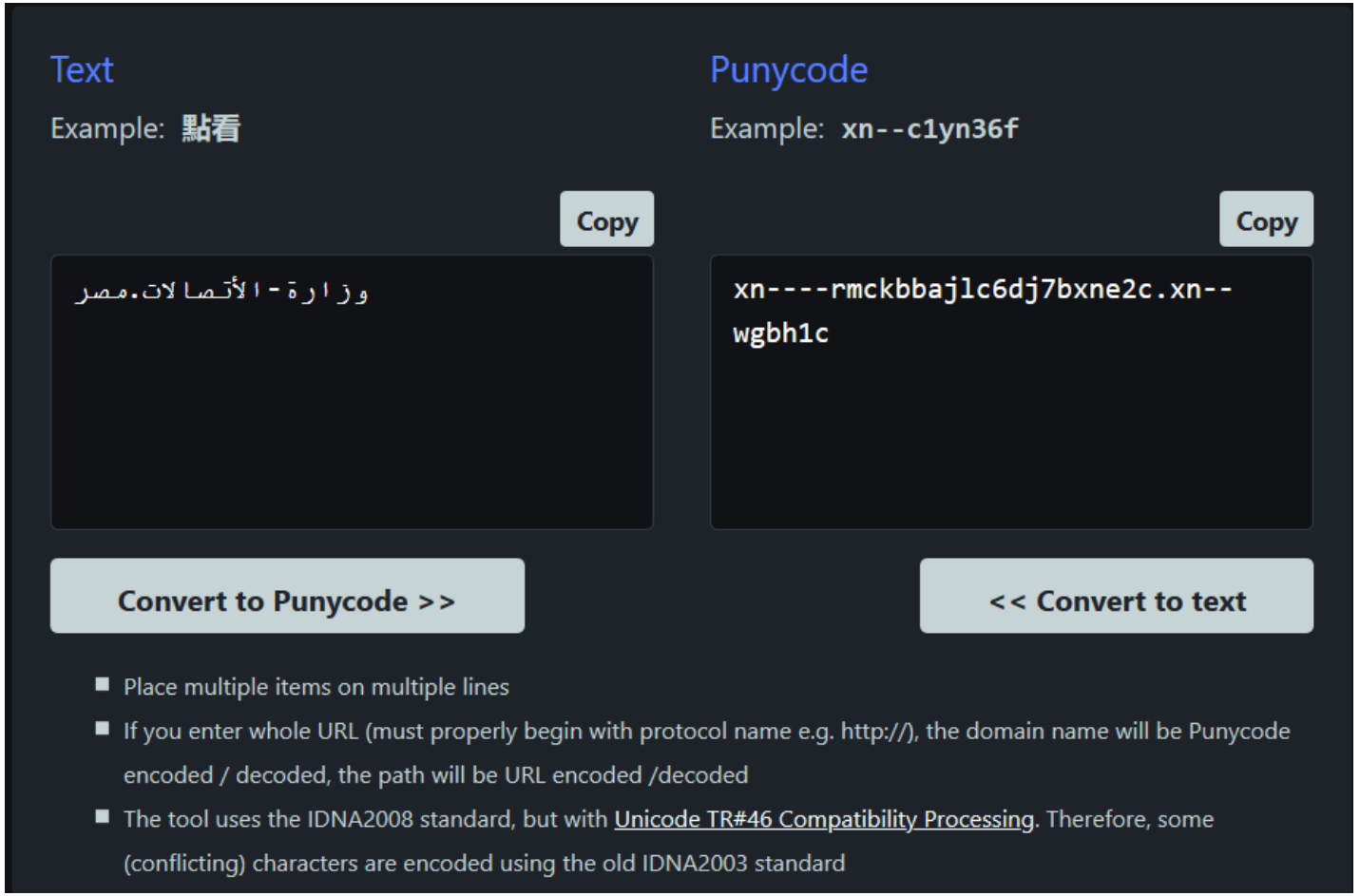
Anatomie d’un nom DNS

Nom de domaine internationalisé (RFC 5890)

-http://وزارة-الأتصالات.مصر/ ce nom de domaine est converti en punnycode avant sont traitement.

-Punycode est la fonction Standardisée pour convertir Les labels des noms de domaine non-ASCII en ASCII acceptable par le DNS.

-*l'IETF a décidé que le* ***punytranscodage*** *serait au niveau des applications et non de l'accès réseau.*



Anatomie d’un nom DNS

Le **nom de l'ordinateur** correspond à la partie la **plus à gauche**

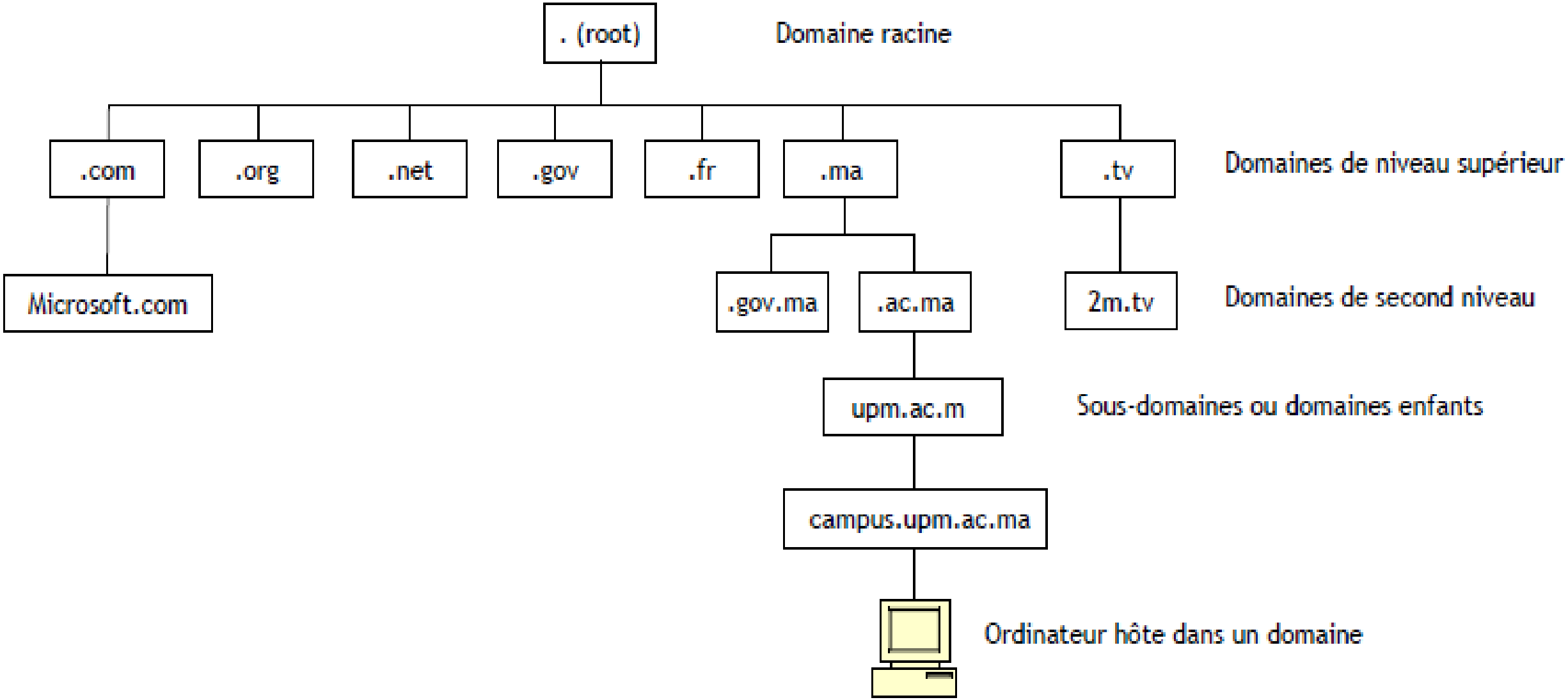
- Lorsque vous décomposez un nom DNS, l'élément le plus à gauche correspond au nom de l'ordinateur,
- les autres éléments situés à droite correspondant au domaine DNS ou suffixe DNS.
- Par exemple, dans le nom d'ordinateur MONPC.UPM.AC.MA, il y a deux parties à repérer :

  MONPC + UPM.AC.MA

- soit :

  nom ordinateur + nom de domaine/suffixe DNS

Niveaux de domaines



Anatomie d’un nom DNS

Comment fonctionne une hiérarchie DNS ou un espace de noms DNS ?

- La responsabilité de l'enregistrement des relations entre les noms et les adresses IP est assurée localement : si vous faites pointer votre navigateur sur **WWW.UPM.AC.MA**, votre serveur DNS local essaie de déterminer l'adresse IP de **WWW.UPM.AC.MA** et pour cela, il se met rapidement en contact avec le serveur DNS du domaine **UPM** pour résoudre ce nom.
- Autrement dit, c'est grâce à ce serveur que vous pouvez trouver l'ordinateur **WWW** dans le domaine **UPM.AC.MA.**

Anatomie d’un nom DNS

Présentation de la hiérarchie : lecture de gauche à droite:

- Prenons l'exemple d'un PC dont le nom complet est **MONPC.CAMPUS.UPM.AC.MA**, afin de voir comment fonctionne la hiérarchie. Que nous indiquent les emplacements des points dans le nom (autrement dit, les parties du nom) ?
- Tout d'abord, nous savons que le nom de l'ordinateur est **MONPC.** Ensuite, nous savons que son domaine est **CAMPUS.UPM.AC.MA.** Mais **CAMPUS.UPM.AC.MA**, qu'est-ce que c'est ?
- Eh bien en lisant de gauche à droite, vous voyez que campus est un sous-domaine ou domaine enfant d'un autre domaine nommé **UPM.AC.MA.**
- Cela signifie que celui qui a créé le domaine **CAMPUS.UPM.AC.MA** avait besoin de l'autorisation de la personne responsable du domaine **UPM.AC.MA** pour créer son domaine.

Anatomie d’un nom DNS

Présentation de la hiérarchie : lecture de gauche à droite:

- Ensuite, avançons vers la droite et examinons **UPM.AC.MA**. À quoi correspond ce domaine? C'est un domaine enfant d'un domaine simplement nommé **AC.MA**.
- Pour créer le domaine **UPM.AC.MA**, quelqu'un a eu besoin de contacter les personnes responsables du domaine **ac.ma** et d'obtenir l'autorisation de créer un sous-domaine de **AC.MA** appelé **UPM**.
- De la même manière **AC** est un sous domaine de **MA**.

Anatomie d’un nom DNS

Présentation de la hiérarchie : lecture de gauche à droite:

- Mais d'où provient le domaine **MA** ? S'agit-il de l'enfant d'un autre domaine ? En fait, **MONPC.CAMPUS.UPM.AC.MA** n'est pas à strictement parler un nom DNS complet.
- Le nom complet, c’est **MONPC.CAMPUS.UPM.AC.MA.**
  - *Quelle est la différence ?*
- Observez à nouveau : le nom correct se termine par **un point**, inclus dans le nom. Le domaine "**MA.**" est en fait un domaine enfant du domaine tout simplement nommé « **.** », qui est la «racine » de la hiérarchie DNS.

Anatomie d’un nom DNS

Fully Qualified Domain Name

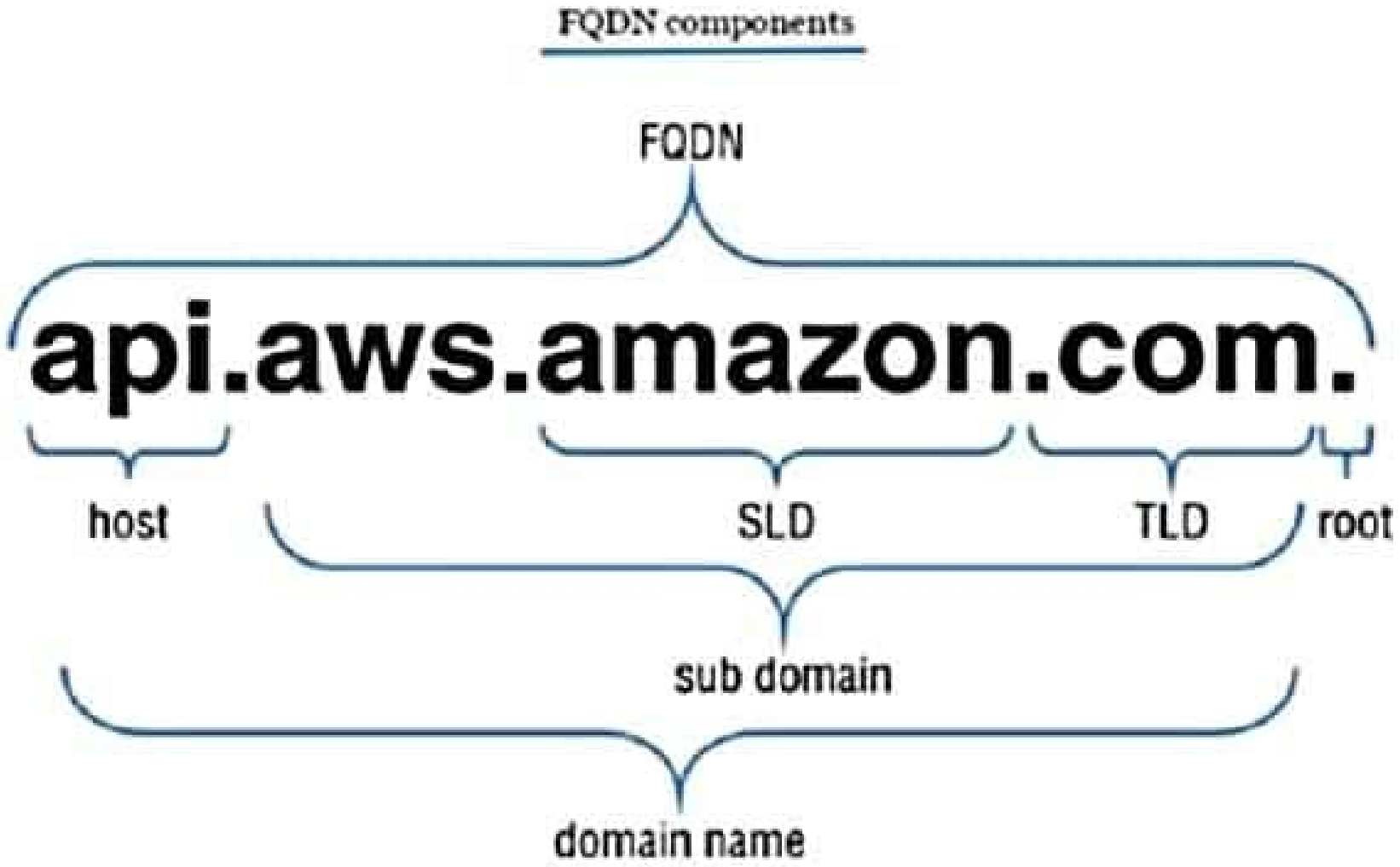
- Chaque "partie« du domaine **MONPC.CAMPUS.UPM.AC.MA.** est appelée **label** et l'ensemble des labels constitue un **FQDN : *Fully Qualified Domain Name***.
- Ce **FQDN est unique**.
- Par convention, un FQDN se finit par un point, car au-dessus des TLD (*Top Level Domain)* il y a **la racine du DNS**, tout en haut de l'arbre.
- Ce point disparaît lorsque vous utilisez les noms de domaine avec votre navigateur, mais vous verrez qu'il deviendra très important lorsque nous configurerons notre propre serveur DNS.

Anatomie d’un nom DNS

Importance du FQDN

- Si jamais vous administrez un réseau, et que vous possédez le domaine mondomaine.com, vous pouvez vous amuser à ajouter dans votre serveur DNS une machine qui s'appellera **www.facebook.com.mondomaine.com.**
- Ainsi, dès qu'une personne qui utilise votre serveur DNS demande **www.facebook.com** en oubliant de mettre le . à la fin, elle sera envoyée vers votre la machine **www.facebook.com.mondomaine.com.** !

Anatomie d’un nom DNS



Anatomie d’un nom DNS

La résolution en pratique

- 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.GOOGLE.COM dans votre navigateur. Lorsque vous entrez ce nom, votre machine doit commencer par le résoudre en une adresse IP.

Anatomie d’un nom DNS

La résolution en pratique

- 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.*
- La plupart du temps, votre 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.

Anatomie d’un nom DNS

La résolution en pratique

- Nous voulons donc joindre le site WWW.GOOGLE.COM voilà ce que va faire mon 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 GOOGLE.
- 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.

Anatomie d’un nom DNS

La résolution en pratique

- Il va demander **aux serveurs racine** l'adresse IP de WWW.GOOGLE.COM . 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 .COM.**
- Il demande ensuite au serveur DNS de com l'adresse IP de WWW.GOOGLE.COM . Mais comme auparavant, le serveur **COM** renvoie l'adresse IP du serveur DNS qui dépend de lui, le serveur DNS de **GOOGLE.COM**
- Enfin, il demande au serveur DNS de **GOOGLE.COM** l'adresse IP de WWW.GOOGLE.COM et là, ça marche : **le serveur de GOOGLE.COM connaît l'adresse IP correspondante** et peut la renvoyer.

Anatomie d’un nom DNS

Serveur d’autorité

- 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.

Administrez vos propres domaines de niveau supérieur : à u sage interne uniquement !

- Bien que l'Internet public n'utilise qu'une poignée de domaines de niveau supérieur, cela ne signifie pas que vous ne pouvez pas créer d'autres domaines à vous quelquefois.

- Un serveur DNS qui est parfaitement capable de résoudre des noms sur Internet, peut héberger également un domaine «invisible » de l'Internet public en utilisant un nom de domaine avec un domaine de niveau supérieur non standard (par exemple notreclasse.local).

Domaines de second niveau : recherche dans la hiérarchie

- Vous pouvez créer un domaine de second niveau avec l'autorisation du propriétaire du domaine parent. Pour créer votre domaine de second niveau, le domaine parent ne doit faire qu'une seule chose: « déléguer » la responsabilité des noms pour votre domaine de second niveau à un ordinateur donné.

Domaines de troisième niveau: domaines enfants et sous-domaines

- Supposons à présent que je choisisse de diviser mon domaine en sous-domaines ou domaines enfants. Supposons que je crée un sous-domaine nommé www.upm.ac.ma.
- Les domaines racine et ma ne sont pas capables de résoudre www dans le domaine upm.ac.ma parce qu'ils ont délégué la responsabilité de résolution de noms pour upm.ac.ma à un groupe de serveurs DNS (ceux du domaine upm.ac.ma).
- Plus spécifiquement, le domaine racine contient des enregistrements appelés NS (Name Server ou serveur de noms) qui délèguent la responsabilité pour le domaine ma aux serveurs DNS de "ma" et les serveurs DNS du domaine "ma" contiennent des enregistrements NS qui délèguent la responsabilité de serveur de noms pour le domaine upm.ac.ma aux serveurs de upm.ac.ma.

Domaines de troisième niveau: domaines enfants et sous-domaines

- Pour créer un sous-domaine de upm.ac.ma, il faut deux choses :

1. Tout d'abord, il faut transformer l'un des ordinateurs en un serveur DNS pour le sous-domaine campus.upm.ac.ma. Cet ordinateur devra bien évidemment se trouver connecté à Internet de manière permanente.
2. Ensuite, j'aurais besoin de dire au reste du monde d'aller consulter leur serveur pour résoudre les noms dans le domaine campus.upm.ac.ma. Pour cela, je déléguerai la responsabilité de serveur de noms, en plaçant un enregistrement NS dans ma base de données DNS upm.ac.ma qui dit : « Il y a un sous domaine nommé campus dans le domaine upm.ac.ma et si vous souhaitez rechercher des noms dans ce domaine, ne m'interrogez pas moi, mais l'autre serveur DNS, celui de campus ».

Les zones, les domaines et la délégation

- Qu'est-ce qu'une zone ? C'est un terme spécifique à DNS qui désigne « la plage d'adresses Internet dont s'occupe ce serveur DNS ». Prenons l'exemple de l'Université Privée de Marrakech *(upm.ac.ma).*
- Comme l'Université a plusieurs établissements, on a décidé de créer des domaines enfants, campus.upm.ac.ma et vatel.upm.ac.ma.
- Certains ordinateurs resteront dans le domaine supérieur upm.ac.ma (le serveur Web par exemple, **www.upm.ac.ma**), mais de nombreuses machines seront appelées soit **monpc.campus.upm.ac.ma**, soit **monpc.vatel.upm.ac.ma**.

Les zones, les domaines et la délégation

- Pourquoi diviser le domaine en domaines enfants ?
- Il peut y avoir plusieurs raisons, mais la plus évidente peut être la simplicité du système de nommage : un simple coup d'oeil au nom de l'ordinateur permet de déterminer à quel établissement il appartient.
- Le serveur de **upm.ac.ma** a «délégué» la résolution des noms pour **campus.upm.ac.ma** à un serveur DNS à "**campus**" et a «délégué» la résolution des noms pour **vatel.upm.ac.ma** à un autre serveur DNS à « vatel ».

Les zones, les domaines et la délégation

- **upm.ac.ma** constitue toujours un seul et unique domaine, mais ses responsabilités DNS ont été dispersées.
- Comment donc appeler ces sous-ensembles de domaines pour lesquels de nouveaux serveurs DNS d'upm sont les serveurs d'autorité ?
- On parle alors de « zones DNS » ou tout simplement de « zones ».

Zones de recherche directe et inversée

- La tâche principale de DNS, qui consiste à convertir des noms d'hôtes en adresses IP.

- DNS peut cependant aussi faire l'inverse. Vous pouvez demander à un serveur DNS : « Quel est le nom d'hôte associé à l'adresse IP 205.22.42.19 ? ».

Zones de recherche directe et inversée

- Le processus de conversion d'un nom d'hôte en une adresse IP est appelé résolution de nom directe.

- Le processus de conversion d'une adresse IP en un nom d'hôte correspondant est appelé résolution de nom inversée.

Zones de recherche directe et inversée

- DNS conserve des informations relatives à un domaine donné comme **fruit.com** dans des fichiers appelés « fichiers de zone», fruit.com possède ainsi un fichier de zone que DNS peut utiliser pour retrouver l'adresse IP de **kiwi.fruit.com.**

- Mais où se tourne DNS pour retrouver le nom d'hôte associé à l'adresse IP 205.22.42.19 ?

Zones de recherche directe et inversée

- Les autorités d'Internet distribuent des blocs d'adresses. Il existe une zone DNS appelée « **zone de recherche inversée** » pour chaque réseau Internet.
- Ainsi, en supposant que **fruit.com** travaille avec le réseau suivant **205.22.42.0**, quelqu'un a pour tâche de conserver une zone de recherche inversée pour 205.22.42.0.

Zones de recherche directe et inversée

- Le nom de la zone de recherche inversée est cependant étrange. Pour le construire, prenez la notation décimale à points que les autorités vous donnent (faites disparaître la partie que vous contrôlez) et inversez-les, puis ajoutez "**.in-addr.arpa**" à la fin du nom.

- Ainsi, la personne en charge de **205.22.42.0** créerait une zone de recherche inversée **42.22.205.in-addr.arpa.**

Zones de recherche directe et inversée

- Exercice :

Donner le nom de la zone de recherche inversée des adresses suivantes:

- *164.109.0.0/16*
- *4.0.0.0/8*
- *200.120.50.0/24*

Zones de recherche directe et inversée

- Solution:

- 164.109.0.0/16- Un réseau de classe B, abandonnerait les deux zéros et inverserait les deux octets restants pour produire le nom de zone inversée **109.164.in-addr.arpa.**
- •4.0.0.0/8- Un réseau de classe A, posséderait la zone inversée

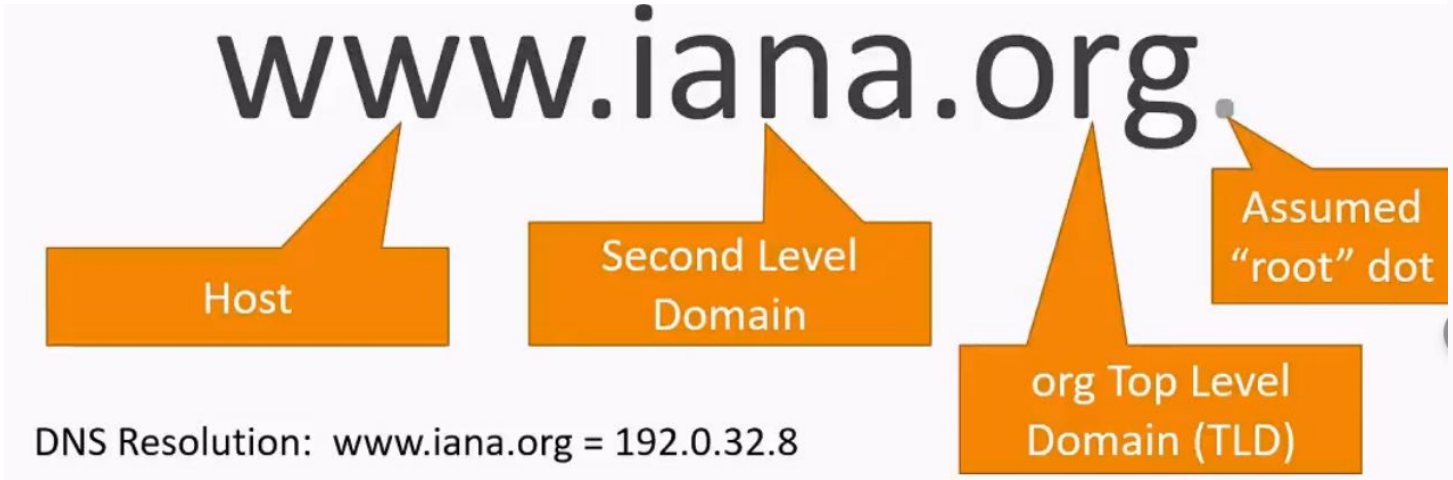
  4. in-addr.arpa.
- •200.120.50.0/24 - Un réseau de classe C, abandonnerait le dernier octet (0) et inverserait les nombres pour obtenir le nom de zone inversée **50.120.200.in-addr.arpa**.

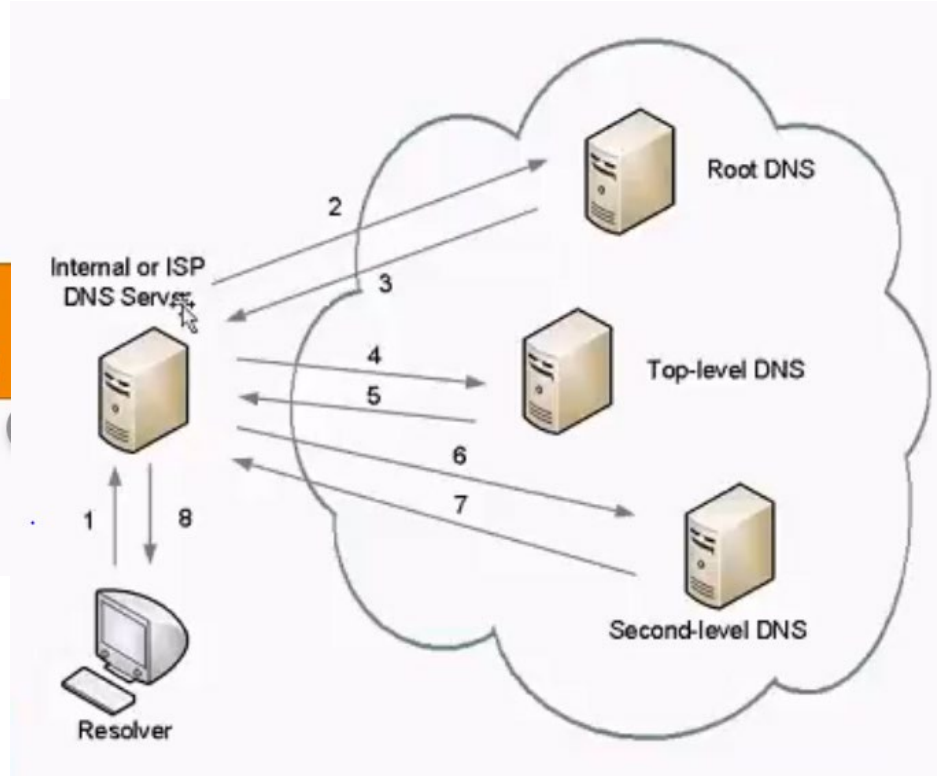
Quelles sont les principales utilisations des enregistrements PTR ?

Les utilisations courantes du DNS inversé incluent :

- **Anti-spam :** Certains filtres anti-spam utilisent le reverse DNS pour vérifier les noms de domaine des adresses électroniques et voir si les adresses IP associées sont susceptibles d'être utilisées par des serveurs de messagerie légitimes.
- **Dépannage des problèmes de livraison des e-mails :** Les filtres anti-spam effectuant ces vérifications, les problèmes de livraison des e-mails peuvent résulter d'un enregistrement PTR mal configuré ou manquant. Si un domaine n'a pas d'enregistrement PTR, ou si l'enregistrement PTR contient le mauvais domaine, les services de messagerie peuvent bloquer tous les e-mails provenant de ce domaine.
- **Journalisation :** Les journaux du système n'enregistrent généralement que les adresses IP ; une recherche DNS inverse peut les convertir en noms de domaine pour des journaux plus lisibles par l'homme.

Comment DNS fonctionne du point de vue du client ?





Types d'enregistrements DNS de base

- Les bases de données DNS contiennent plusieurs types

Enregistrements SOA (Start of Authority)

- Chaque domaine possède un enregistrement de source de nom appelé enregistrement SOA (Start of Authority).
- Il s'agit de l'enregistrement qui nomme le serveur DNS principal pour le domaine, fournir une adresse de courrier électronique d'un administrateur du domaine et spécifie la durée pendant laquelle les données peuvent être conservées dans le cache des serveurs secondaires.
- Un DNS principal d'une zone contient la seule copie en lecture/écriture de la zone ; les serveurs secondaires, dont on peut avoir autant d'exemplaires qu'on le souhaite, contiennent des copies en lecture seule de la zone, en cas de besoin).

Enregistrements SOA (Start of Authority)

- Il alerte également le monde extérieur lorsque n'importe quel enregistrement de domaine a changé, à l'aide d'un numéro de série.
- Les serveurs DNS secondaires peuvent utiliser cette indication pour voir si les données sur le serveur principal ont changé, auquel cas ils doivent obtenir des mises à jour de la part du serveur DNS principal.

Enregistrements SOA (Start of Authority)

- Syntaxe:

domaine IN SOA "serveur DNS" "email administrateur«

(N° de série

Rafraîchissement

Nb_essais

Expiration

Minimum)

Enregistrements SOA (Start of Authority)

- **N° de série:** représente le n° de version de ce fichier de zone. En pratique, on choisi la date de la dernière mise à jour formatée en "**AAAAMMJJNN** avec NN le nombre de révisions à la date indiquée. Ce N° doit être incrémenté à chaque mise à jour pour quel es modifications soient prisent en compte.
- **Rafraîchissement:** (en secondes), indique l'intervalle de temps qui sépare deux vérifications de mise à jour du serveur secondaire (le serveur secondaire ne mettra jamais à jour sa copie de zone si on n'a pas incrémenté le n° de série.
- **Nb_essais:** (en secondes) indique le temps pendant lequel les serveurs secondaires doivent attendre avant un nouvel essai si le serveur ne répond pas à leur demande de mise à jour
- **Expiration :** (en secondes) indique le temps pendant lequel les serveurs secondaires doivent conserver leurs données.
- **Minimum:** (en secondes) ou durée de vie, c'est le temps durant lequel les clients gardent les informations dans leur cache.

Enregistrements SOA (Start of Authority)

- Exemple:

upm.ac.ma. IN SOA dns.upm.ac.ma. user.upm.ac.ma. (

2023030210

10800

3600

43200

3600)

Enregistrements A (hôtes)

- L'enregistrement le plus simple, qui indique qu'un ordinateur **monpc.upm.ac.ma** se trouve à une adresse IP **196.x.y.z** (autrement dit, l'enregistrement qui met en correspondance des noms et des adresses IP) est appelé « enregistrement A » ou « enregistrement d'hôte ».
- Les enregistrements d'hôtes sont généralement les plus nombreux.

- Syntaxe: nom_machine IN(internet) A Adresse IP
- Exemple: monpc.upm.ac.ma. IN A 212.217.51.4

Enregistrements PTR

- Les enregistrements DNS PTR sont utilisés dans les recherches DNS inversées.
- Une recherche DNS inverse est l'inverse de ce processus : il s'agit d'une requête qui part de l'adresse IP et recherche le nom de domaine.

Syntaxe: @IP_Inversée	IN(internet)	PTR	NomDuDomaine
Exemple: 34.216.184.93.in-addr.arpa.	IN	PTR	upm.local.

Enregistrements NS/serveur de noms (serveur DNS)

- Les enregistrements de serveurs de noms (appelés NS, pour Name Server, dans un fichier de zone) définissent les serveurs de noms dans le domaine.
- Vous pouvez utiliser les enregistrements NS pour déléguer l'autorité à un sous-domaine (une zone).

Enregistrements NS/serveur de noms (serveur DNS)

Syntaxe: domaine IN NS serveur

- Exemple:

upm.ac.ma. IN NS dns.upm.ac.ma.

dep.upm.ac.ma. IN NS dnsp.dep.upm.ac.ma.

Cet enregistrement indiquerait : « Pour résoudre des noms pour un nom.upm.ac.ma, rendez-vous à dns.upm.ac.ma et pour résoudre des noms pour dep.upm.ac.ma, rendez-vous à dnsp.dep.upm.ac.ma».

Enregistrements CNAME (alias)

- Bien souvent, vous aurez besoin qu'un hôte puisse répondre à plusieurs noms différents. Par exemple, le serveur Web propose aussi un serveur ftp.
- Le but est de prendre une adresse IP particulière et de lui donner plusieurs noms. Pour cela, il faut utiliser des alias, ou enregistrements CNAME (Canonical NAME ou nom canonique).

Enregistrements CNAME (alias)

- Syntaxe:

Alias IN CNAME nom serveur

- Exemple:

ftp IN CNAME www.upm.ac.ma.

- Dans cet exemple, **ftp.upm.ac.ma** et **www.upm.ac.ma** pointent vers le même serveur.

Enregistrements MX (serveur de messagerie)

- Lorsque j'envoie un message à user@upm.ac.ma, j'indique au programme de messagerie que je souhaite que le message soit transmis à une personne appelée "user" et que "user" possède un compte sur un serveur dans le domaine upm.ac.ma.

- Ce que je n'ai pas dit à mon programme de messagerie, c'est l'endroit exact où envoyer le courrier pour user, c'est-à-dire le nom de son serveur de messagerie.

Enregistrements MX (serveur de messagerie)

- Si l'importance de ce fait ne vous apparaît pas immédiatement, considérez cela : si vous savez que mon domaine se nomme upm.ac.ma, comment savez-vous où trouver mon serveur Web ou mon serveur FTP ?
- C'est possible parce que le DNS inclut ce que l’on appelle un enregistrement MX ou enregistrement de serveur de messagerie, qui répond à la question : « Quel ordinateur est le serveur de messagerie pour upm.ac.ma ? ».

Enregistrements MX (serveur de messagerie)

- L'enregistrement MX possède un numéro de « priorité », grâce auquel, vous indiquez au système DNS le serveur de messagerie que vous préférez (les valeurs les plus petites étant préférées aux plus grandes).
- Syntaxe:

Domaine	IN	MX	préférence	serveur de messagerie

- La valeur préférence n'est utile que si on dispose de plusieurs serveur de messagerie
- Exemple:

upm.ac.ma.	IN	MX	10	serv1.upm.ac.ma.
upm.ac.ma	IN	MX	50	serv2.upm.ac.ma.

Exemple de configuration DNS

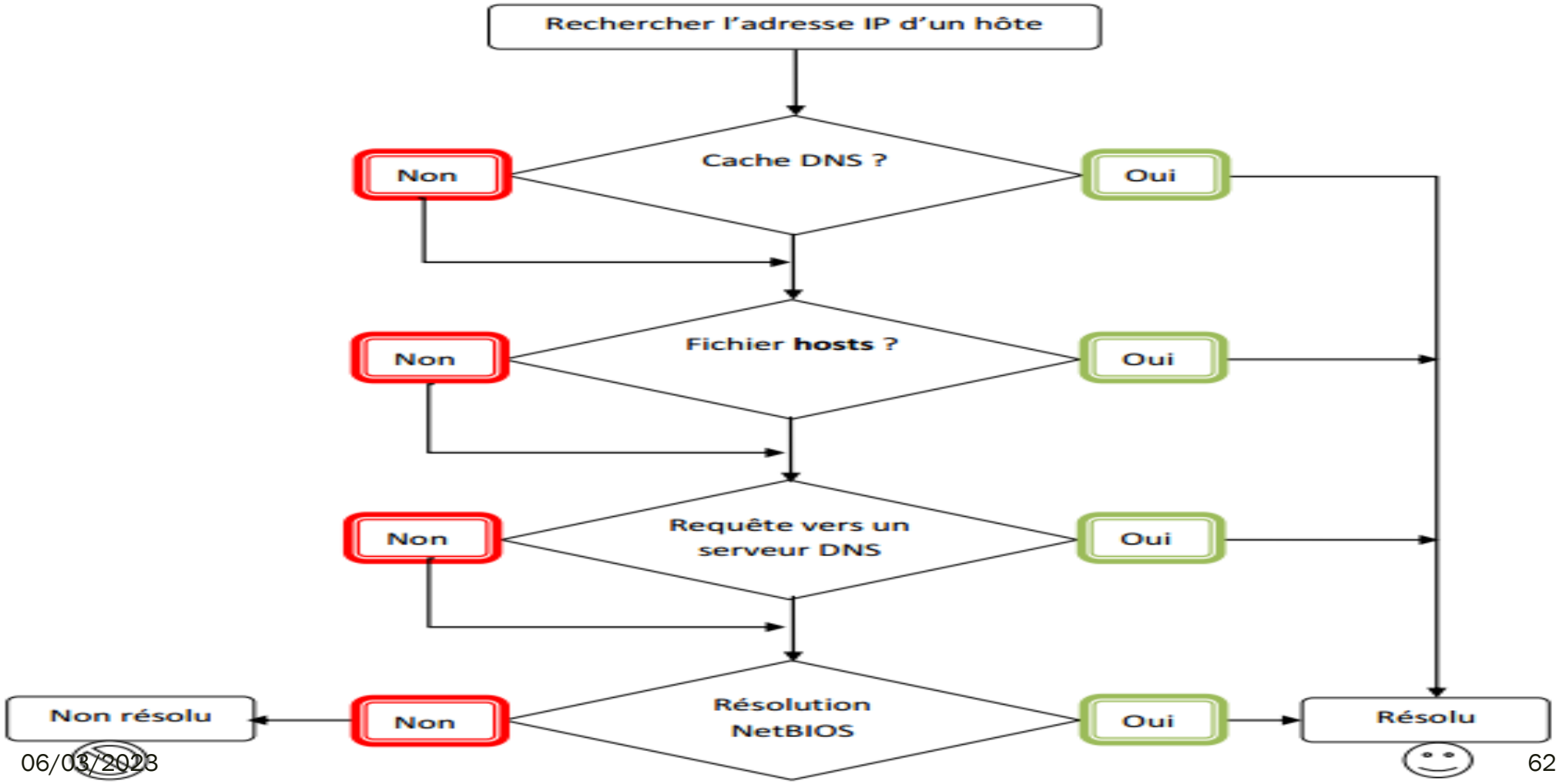
- Voici des exemples de paramètres DNS pour un domaine utilisé avec les services Google Cloud.
- Le TTL détermine le temps qu'il faudra pour que toute modification que vous apportez maintenant entre en vigueur.
- Notez que vous n'utilisez pas le nom de domaine réel dans vos paramètres DNS. Au lieu de cela, vous utilisez le symbole @ pour indiquer le nom de domaine.

```
 GNU nano 2.5.3                    File: /etc/bind/db.upm.local

$TTL    604800 ;

$ORIGIN upm.local.

@       IN      SOA     ns1.upm.local. admin.upm.local. (
                        2018030101      ; Serial
                         3600           ; Refresh
                          3000          ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

@       IN      NS      ns1.upm.local.
@       IN      NS      ns2
@       IN      MX      10 mx1
@       IN      MX      20 mx2
ns1     IN      A       192.168.1.101
ns2     IN      A       192.168.1.102
mx1     IN      A       192.168.1.103
mx2     IN      A       192.168.1.104
cours   IN      A       192.168.1.105
www     IN      A       192.168.1.106
blog    IN      CNAME   www
```

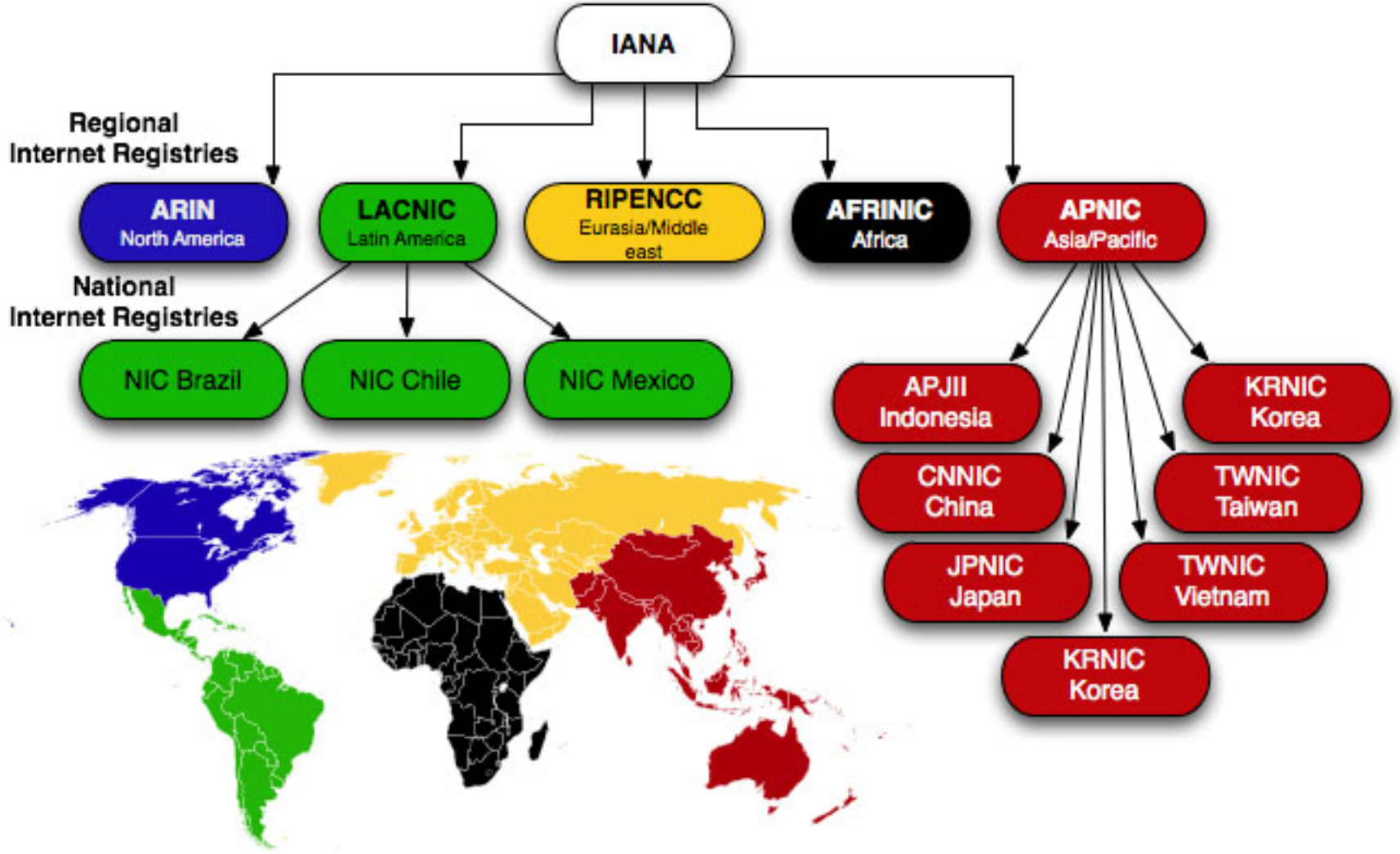
Comment DNS fonctionne du point de vue du client ?

- La première chose que doit faire le client avant de pouvoir se connecter au serveur web ou bien au serveur de fichier est de trouver son adresse IP à partir de son nom d'hôte. 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.**

Comment DNS fonctionne du point de vue du client ?

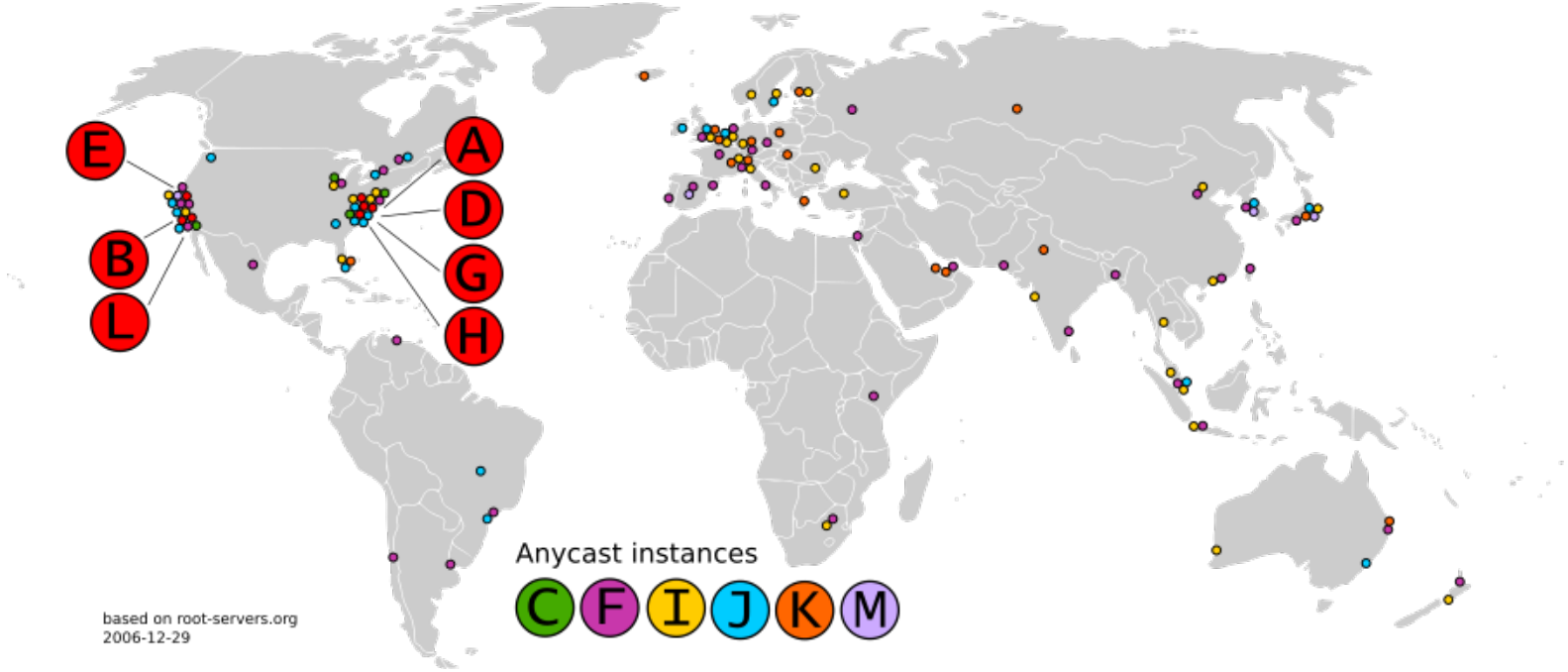


Comment les adresses IP sont distribuées ?



Le Root, c’est quoi .

- 13 serveurs root (+1300 serveurs secondaires) gérés par 12 organisations sur les 6 continents



Liste des serveurs root :

https://www.iana.org/domains/root/servers

https://root-servers.org/

LE DNSSEC (*Domain Name System Security Extensions*) RFC 4033

- DNSSEC permet de sécuriser les données envoyées par le DNS. Contrairement à d'autres protocoles comme TLS, il ne sécurise pas juste un canal de communication mais il protège les données, les enregistrements DNS, de bout en bout.

- DNSSEC signe cryptographiquement les enregistrements DNS et met cette signature dans le DNS. Ainsi, un client DNS méfiant peut récupérer la signature et, s'il possède la clé du serveur, vérifier que les données soient correctes.

LE DNSSEC (*Domain Name System Security Extensions*) RFC 4033

- Ce mécanisme repose sur une hiérarchie de clés cryptographiques commençant à la racine du DNS. Les clés cryptographiques pour la racine du DNS sont gérées par l'ICANN (Internet Corporation for Assigned Names and Numbers).

- Ces clés cryptographiques sont déposées dans deux installations sécurisées à plus de 4000 kilomètres de distance, et sont protégées par plusieurs couches de sécurité physique telles que la sécurité des bâtiments, des caméras, des cages et des coffre-forts surveillés.

les sept clés secrètes du DNSSEC

- La couche la plus secrète de la sécurité physique est un appareil spécialisé dénommé module matériel de sécurité HSM (hardware security module)
- Un module HSM résiste aux altérations physiques. Par exemple, si quelqu'un tente d'ouvrir le système ou même de le faire tomber, le HSM efface toutes les clés entreposées afin d'éviter toute atteinte à son intégrité.

les sept clés secrètes du DNS

- Le système qui a été conçu pour opérer un HSM requiert le présence de beaucoup de gens. Parmi eux, certains sont des membres de la communauté technique du monde entier, connus sous le nom de représentants de confiance de la communauté , et d'autres appartiennent au personnel de l'ICANN.
- Chaque personne joue un rôle spécifique dans l'activation de l'HSM, qui a lieu au cours d'un événement régulier que nous appelons une « cérémonie de clés ».

Pour visionner la cérémonie qui a eu lieu le 27 Février 2019

- https://www.youtube.com/watch?v=b3MbIq0z43I

les sept clés secrètes du DNS

Pour visionner la cérémonie qui a eu lieu le 23 Avril 2020

https://www.youtube.com/watch?v=_yIfMUjv-UU

sources

https://en.wikipedia.org/wiki/NetBIOS

https://support.google.com/a/answer/48090?hl=fr

https://www.icann.org/fr

https://doc.ubuntu-fr.org/bind9

https://tools.ietf.org/html/rfc2929

https://openclassrooms.com/fr/courses/857447-apprenez-le-fonctionnement-des-reseaux-tcp-ip/857163-le-service-dns

https://www.itu.int/ITU-T/worksem/multilingual/papers/s2paper-sabouni.pdf

https://tools.ietf.org/html/draft-farah-adntf-adns-guidelines-03

http://jean-françois.jefsey.com/

https://www.iana.org/domains/root/files

https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains