

Réseaux informatiques RXI

Chapitre 7 DNS



Objectifs d'apprentissage

- Savoir décrire la structure hiérarchique des noms de domaines
- Savoir expliquer la hiérarchie des serveurs DNS à l'aide de zones DNS
- Savoir expliquer le processus de résolution d'un nom de domaine
- Savoir nommer les principaux types d'enregistrements gérés par DNS



DNS

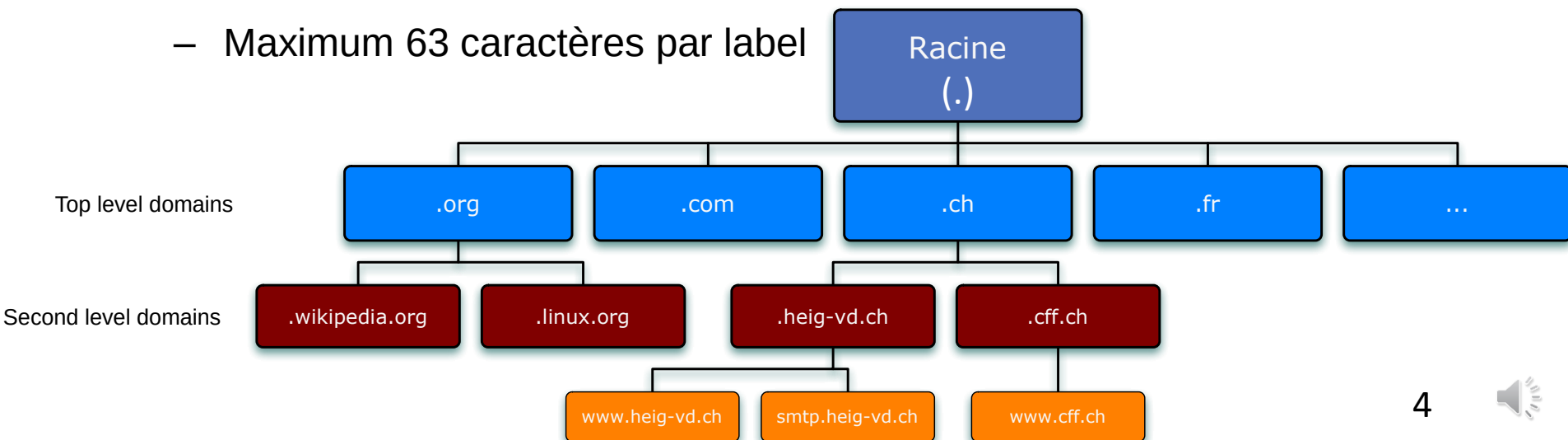
Domain Name System

- Fonction principale
 - Traduction de noms de domaines en adresses IP
- Autres fonctions
 - Définition d'alias
 - Par exemple smtp.gmail.com au lieu de gmail-smtp-msa.l.google.com
 - Recherche du serveur mail pour une adresse e-mail
 - Par exemple bill@hotmail.com → Serveur mail mx1.hotmail.com
 - Répartition de charge
 - Les sites comme www.google.com utilisent plusieurs serveurs
 - DNS permet de répartir facilement la charge sur les serveurs



Espace des noms de domaine

- Les noms de domaines identifient des domaines, sous-domaines, sous-sous-domaines, ..., jusqu'aux hôtes individuels
- Organisés en arborescence
 - Un nom de domaine est donné par la concaténation des **labels** depuis la feuille à la racine séparés par des points
- Syntaxe
 - Non sensible à la casse
 - Maximum 255 caractères
 - Maximum 63 caractères par label



Enregistrements de ressources

- A chaque nœud de l'espace des noms de domaine on peut associer un ensemble d'enregistrement de ressources (Resource Records, RR)
 - Le plus souvent, le RR contient l'adresse IP d'un hôte, mais d'autres informations sont possibles

- Format d'un RR

Nom de domaine	Durée de vie	Classe	Type	Valeur
----------------	--------------	--------	------	--------

- **Durée de vie** : durée maximum en secondes pour garder une copie
 - Typiquement entre 86'400 (un jour) et 60
- **Classe** : contient IN pour Internet
- **Type** : type de l'enregistrement
- **Valeur** : valeur associée au RR



Principaux types d'enregistrement

Type	Signification	Valeur
A	Adresse IPv4	Par exemple 193.134.220.23
AAAA	Adresse IPv6	Par exemple 2a00:1450:4002:803::1017
CNAME	Nom canonique	Nom canonique d'un serveur pour un alias donné. Par exemple gmail-smtp-msa.l.google.com pour smtp.gmail.com
MX	Serveur de messagerie	Nom canonique du serveur de messagerie pour ce domaine Par exemple mailcl1.heig-vd.ch pour heig-vd.ch
NS	Serveur de noms	Nom du serveur DNS responsable pour un domaine. Par exemple dnsext02.heig-vd.ch pour heig-vd.ch
TXT	Texte	Texte ASCII arbitraire
PTR	Pointeur	Nom de domaine pour une adresse IP. Pour la résolution inverse. Par exemple www.heig-vd.ch pour 23.220.134.193.in-addr.arpa
SOA	Description de la zone	Serveur principal, courriel de contact et d'autres informations concernant la zone de ce domaine



Example

- Commande `dig cs.vu.nl ANY`

```
cs.vu.nl. 86264 IN NS ns.vu.nl.
cs.vu.nl. 86264 IN NS star.cs.vu.nl.
cs.vu.nl. 86264 IN NS top.cs.vu.nl.
cs.vu.nl. 86264 IN NS solo.cs.vu.nl.
cs.vu.nl. 86264 IN A 130.37.20.20
cs.vu.nl. 7064 IN MX 10 mx-1.mf.surf.net.
cs.vu.nl. 7064 IN MX 10 mx-a.mf.surf.net.
cs.vu.nl. 86264 IN TXT "Vrije Universiteit - Mathematics
                        and Computer Science"
cs.vu.nl. 86264 IN SOA star.cs.vu.nl.
                        hostmaster.cs.vu.nl.
                        2013041601 7200 3600 2419200 900
```



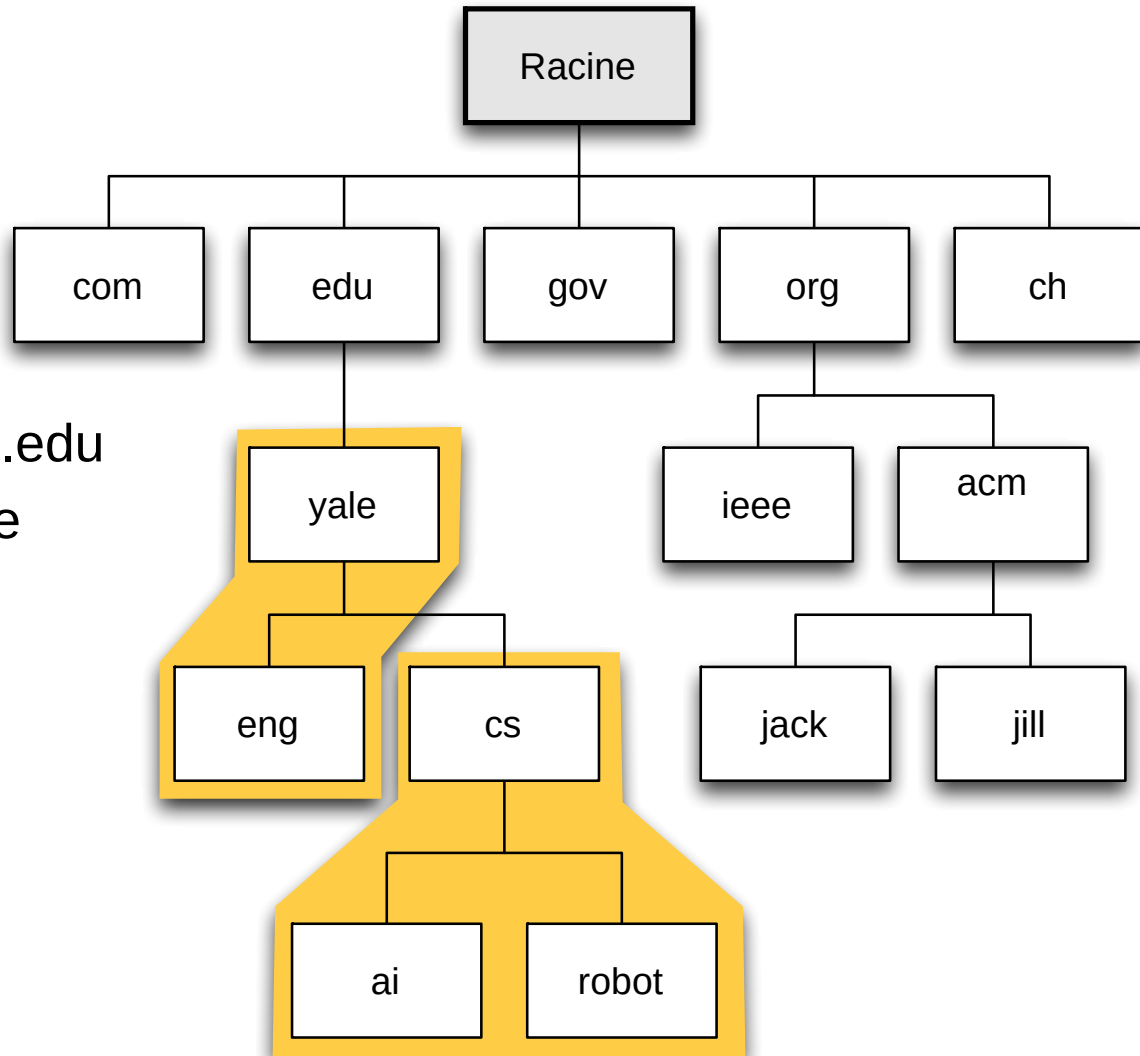
Zones DNS

- DNS est un système hiérarchique et distribués de serveurs
- L'espace des noms DNS est divisé en **zones** distinctes
 - Une zone est une partie de l'arborescence pour laquelle la responsabilité administrative a été déléguée
 - Typiquement une zone dispose d'un serveur DNS primaire et plusieurs serveurs secondaires
 - Une zone peut créer des sous-zones en déléguant l'autorité à d'autres serveurs DNS subordonnés
 - **Le serveur officiel** (*authoritative server*) est celui qui est responsable pour une zone et qui n'a pas délégué la responsabilité



Exemples de zones

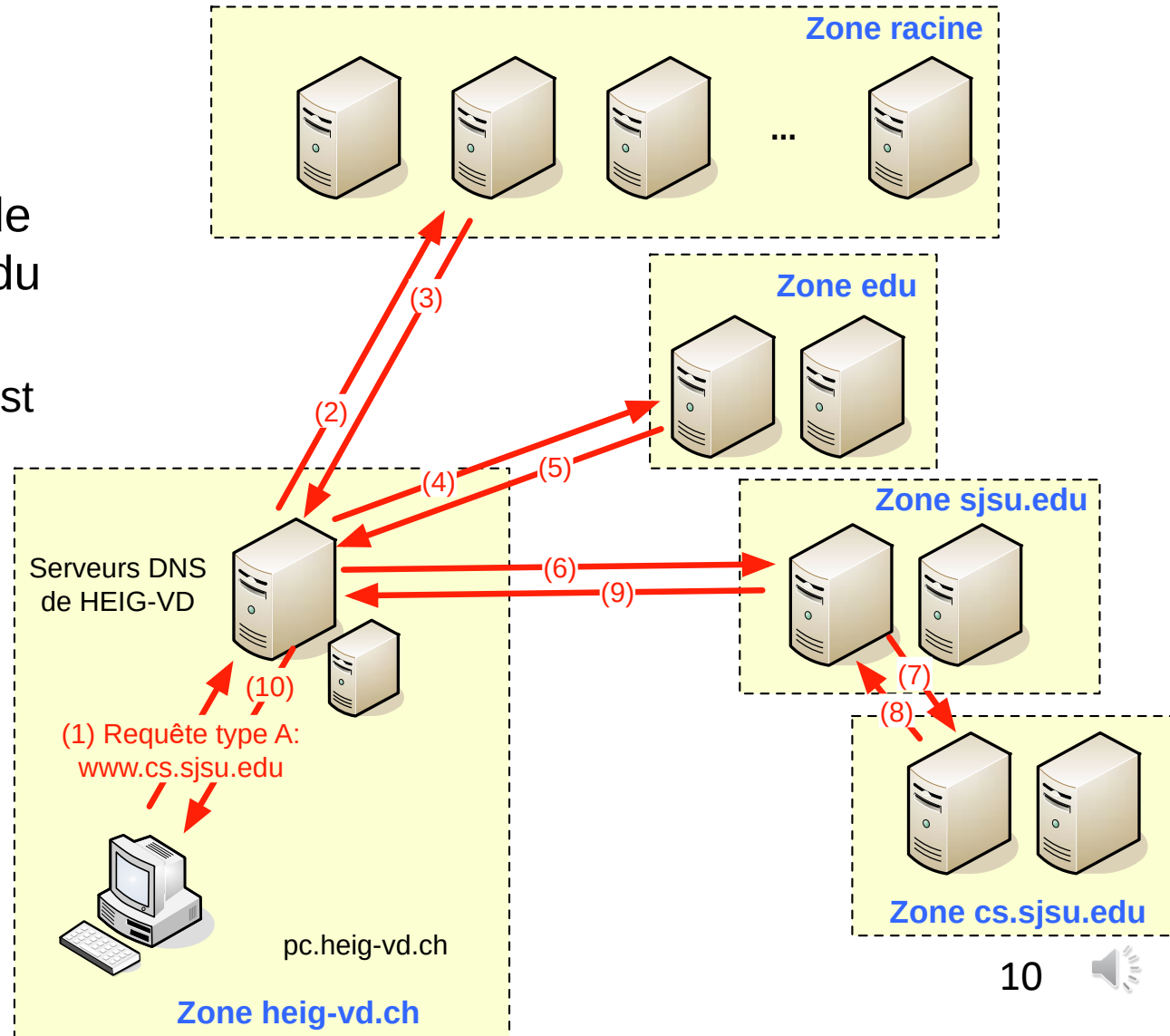
- La racine délègue la responsabilité pour la zone .edu
- La zone .edu délègue la responsabilité pour yale.edu
- La zone yale.edu gère le serveur officiel pour eng.yale.edu
- Elle délègue la responsabilité pour cs.yale.edu à un autre serveur



Requêtes DNS

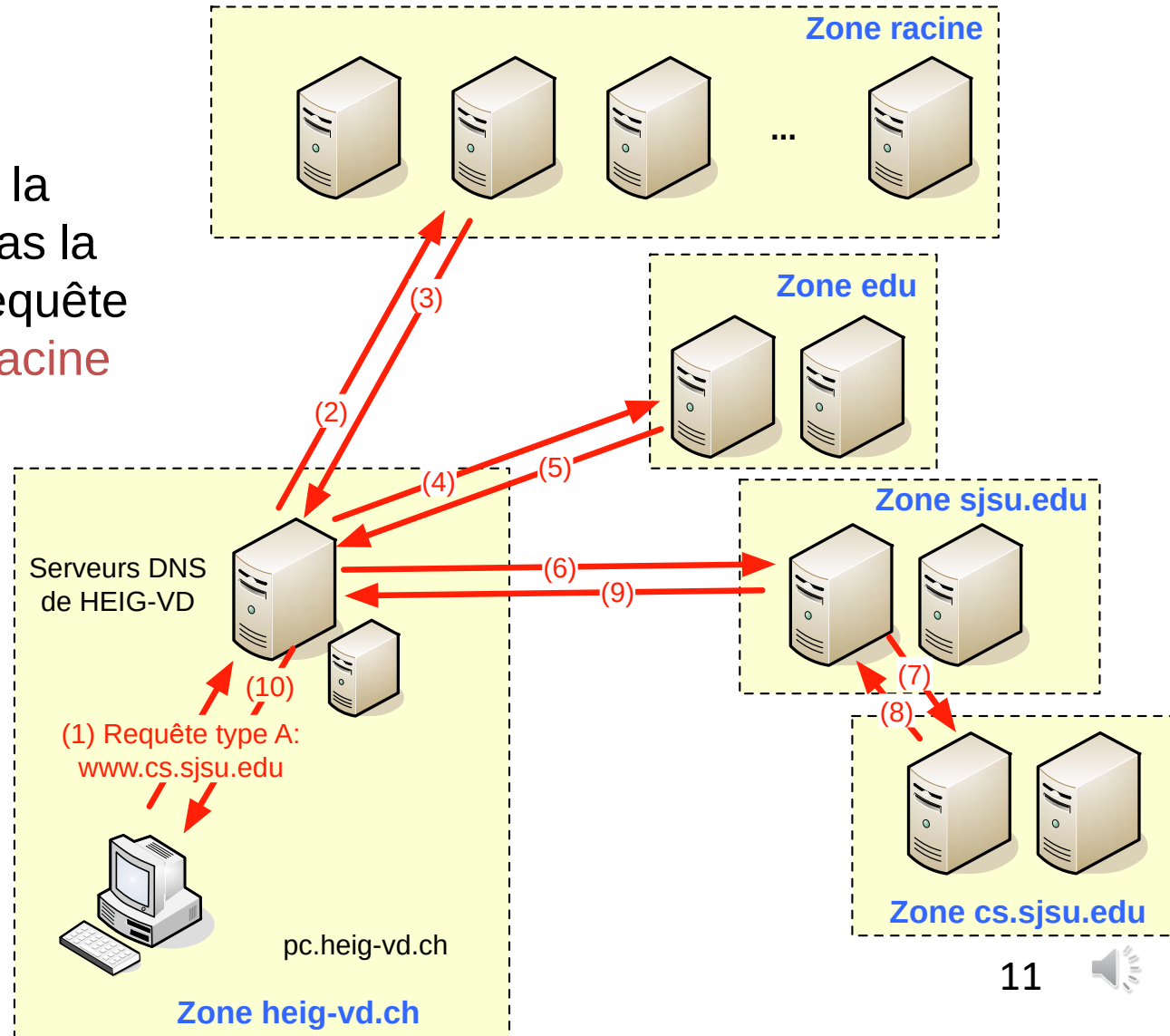
(1) Recherche du nom de domaine `www.cs.sjsu.edu` depuis la HEIG-VD

- La requête type A est envoyée à un des serveurs DNS de la HEIG-VD



Requêtes DNS

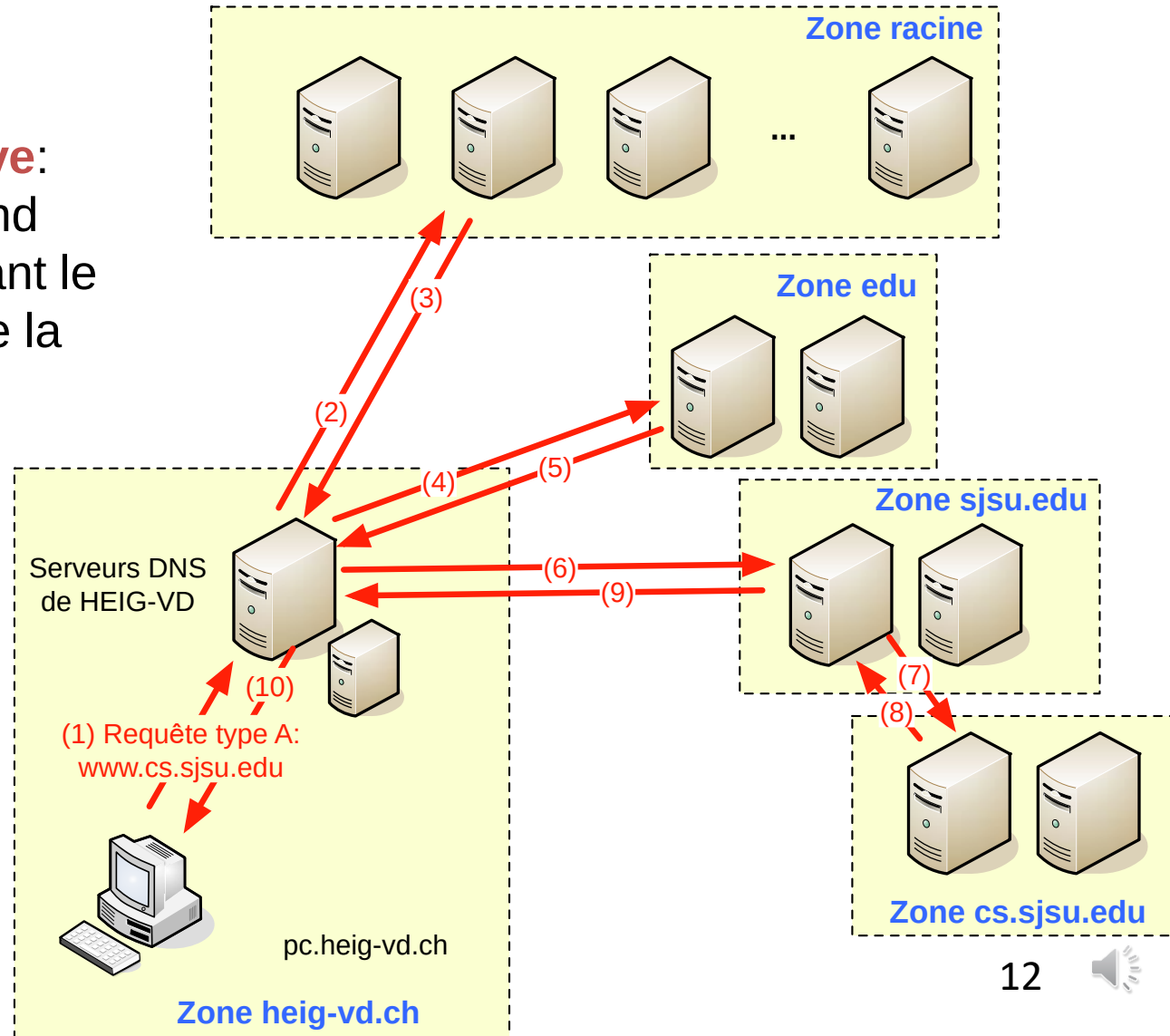
(2) Le serveur DNS de la HEIG-VD ne connaît pas la réponse et envoie la requête à un des 13 **serveurs racine**



Requêtes DNS

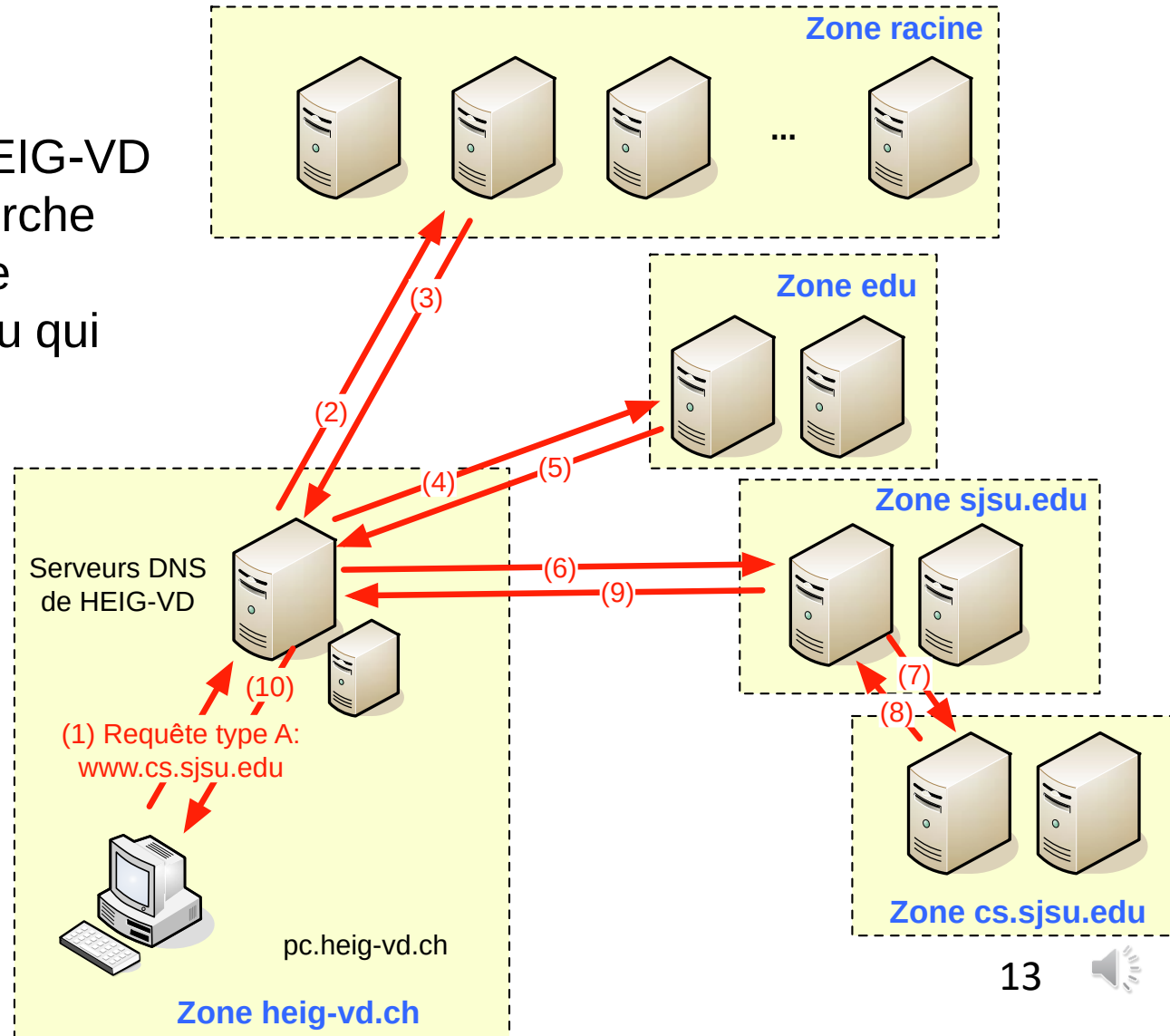
(3) **Recherche itérative**:
le serveur racine répond
directement en indiquant le
serveur DNS officiel de la
zone .edu

D'autres serveurs
DNS sont capables
d'effectuer des
recherches récursives
(cherchent la réponse
finale)



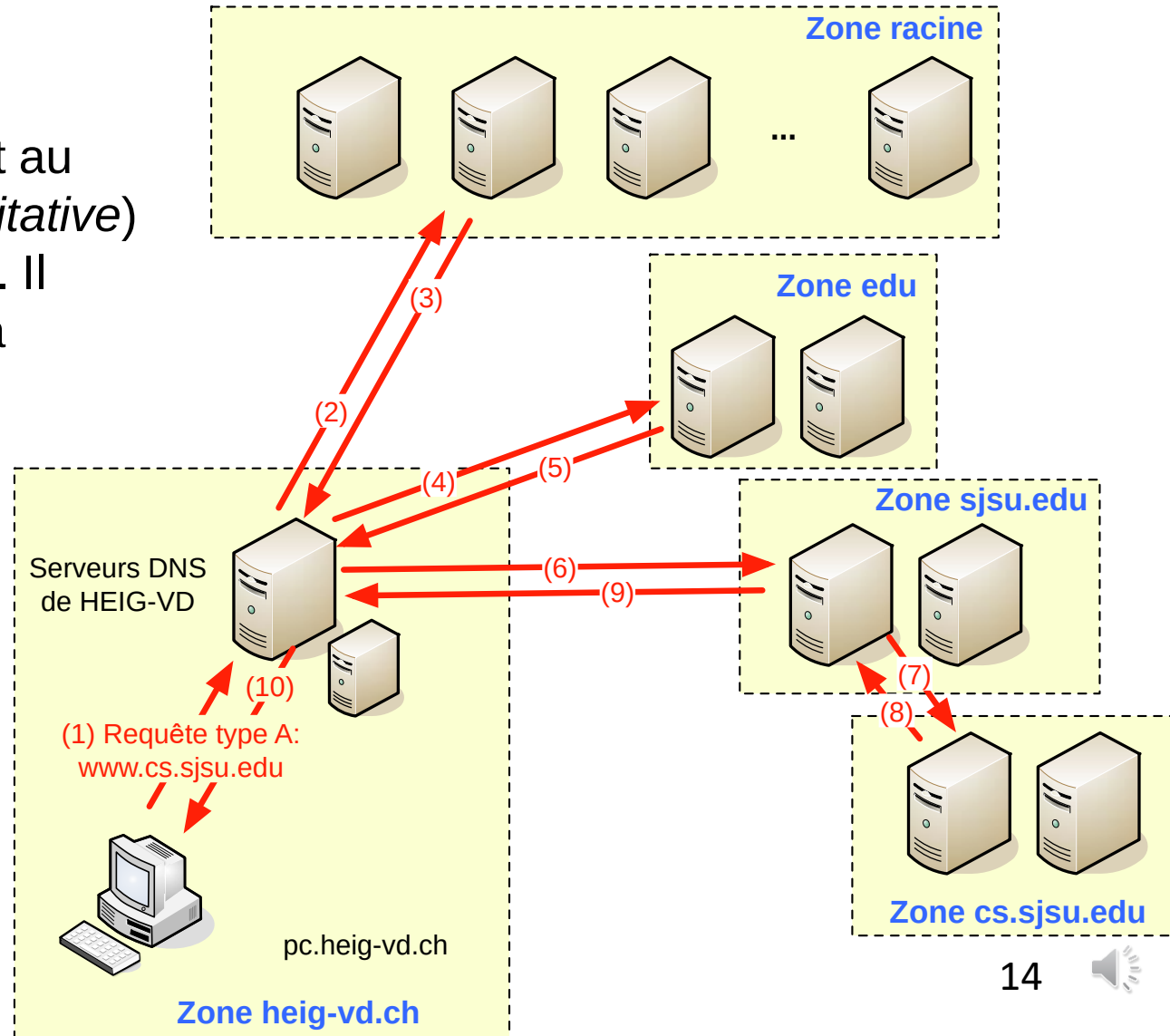
Requêtes DNS

(4) Le serveur de la HEIG-VD continue avec la recherche récursive. Il contacte le serveur de la zone .edu qui lui renvoie le serveur responsable de la zone sjsu.edu



Requêtes DNS

(7) Le requête parvient au serveur officiel (*authoritative*) de la zone cs.sjsu.edu. Il connaît la réponse à la requête et la renvoie.



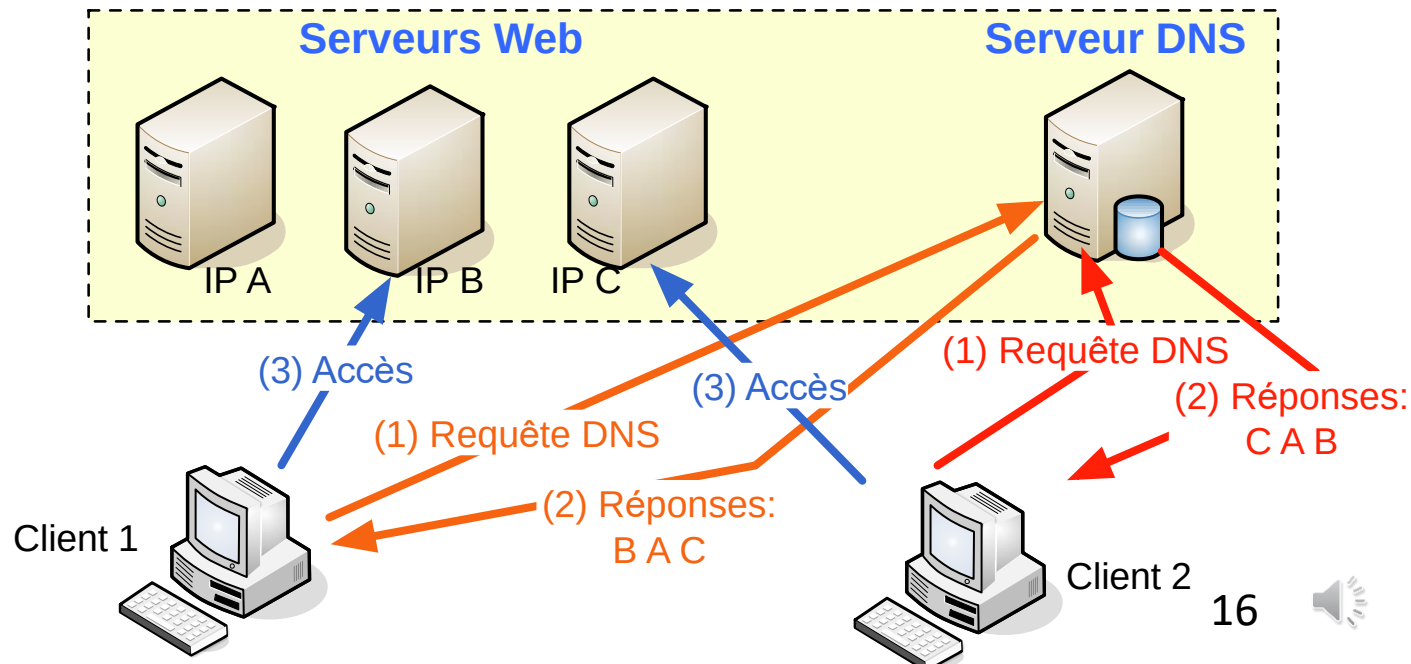
Cache DNS

- Afin de réduire le trafic DNS, un serveur DNS peut garder une copie d'une réponse en cache
 - Le paramètre « Durée de vie » (TTL) d'un enregistrement indique le temps qu'un serveur peut garder une réponse dans son cache
 - Le serveur indique alors dans sa réponse qu'il s'agit d'une réponse non officielle



DNS round-robin

- Le système DNS de réaliser une méthode simple de répartition de charge
- Méthode
 - Un nom de domaine est associé avec plusieurs adresses IP
 - Toutes ces machines réalisent le même service (par exemple serveurs Web pour un site donné)
 - Le serveur DNS effectue une permutation des enregistrements à chaque requête DNS



Sécurité de DNS

DNS a une longue histoire de vulnérabilités et failles

Empoisonnement du cache DNS (plusieurs variantes existent)

1. Un attaquant demande à un serveur DNS victime l'adresse IP de `www.wikipedia.org`
 2. Le serveur DNS effectue une requête récursive et demande au serveur DNS de la zone `wikipedia.org`
 3. L'attaquant envoie une réponse DNS au serveur DNS victime avec une adresse IP fausse
 4. Le serveur victime met l'adresse fausse dans son cache et la distribue lors de requêtes légitimes
- Difficile à réaliser, mais possible
 - Les requêtes/ réponses DNS incluent un numéro que l'attaquant doit deviner
 - Les serveurs DNS utilisent maintenant des ports sources randomisés qu'il faut également deviner



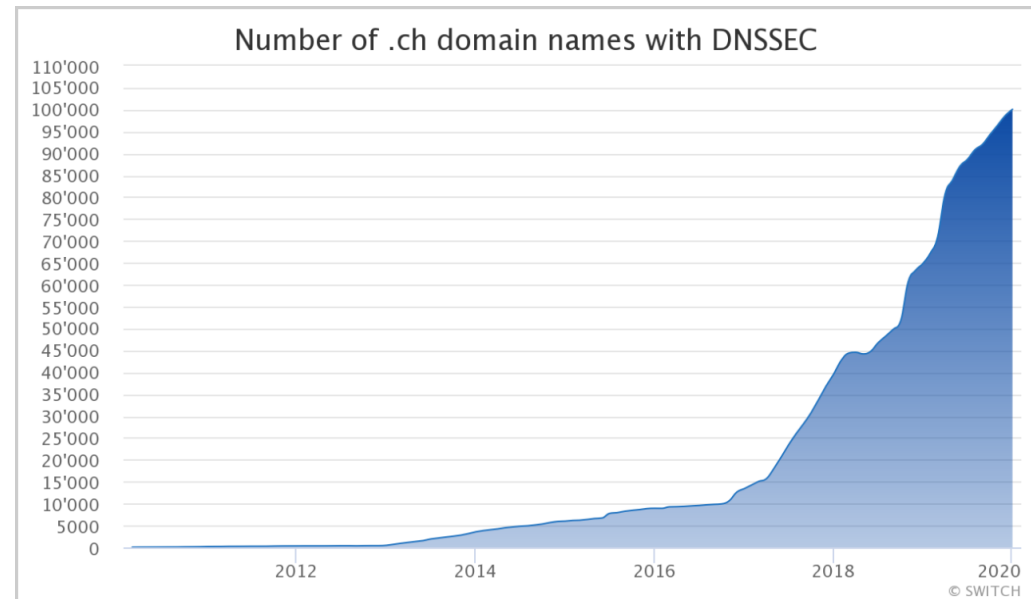
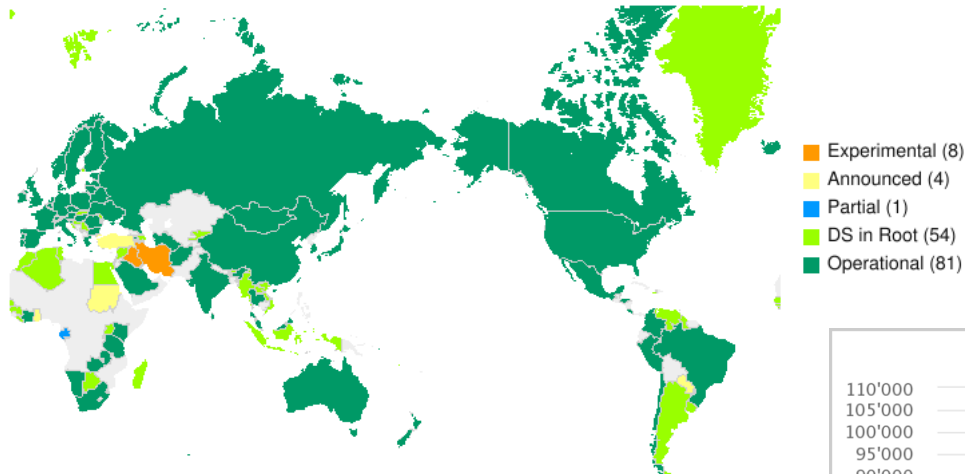
DNSSEC

- DNSSEC vise à sécuriser DNS
- Les réponses DNS sont signées cryptographiquement, mais pas chiffrées
 - Signature avec la clé privée du serveur DNS
 - Une réponse DNS contient un nouvel enregistrement RRSIG avec la signature de l'enregistrement principal de la réponse
- Un client peut obtenir la clé publique du serveur en demandant l'enregistrement du type DNSKEY pour ce serveur DNS
- Les clés d'une zone doivent être signées par la zone supérieure
 - Ceci crée une chaîne de confiance depuis la racine DNS
- Actuellement les serveurs racine et une partie des noms de domaine de premier niveau implémentent DNSSEC



Utilisation de DNSSEC

ccTLD DNSSEC Status on 2019-09-09



Fin du chapitre

