

Laboratoire DNS (90 min)

0	Introduction	sudo ./c 2
---	--------------	------------

Prérequis Avoir effectué le §1 pour préparer cette séance de labo

Objectifs §2 : Etudier les mécanismes DNS du poste client. Travail individuel.
§3 : Tester avec nslookup. Travail individuel.
§4 : Configurer un serveur DNS

Cadre Ce labo s'effectue par groupe de 2

Session Ouvrir une session Windows 7 administrateur : compte=albert username=admin

Action Copier sur le bureau le dossier partagé \\10.2.1.1\doclabo\RPI\2_DNS contenant les fichiers utiles

1	Arborescence DNS	maison
---	------------------	--------

Objectif Illustrer pratiquement l'arborescence DNS à l'aide d'outils spécifiques

Action Utiliser le site <http://www.root-servers.org> pour visualiser la redondance présente dans les 13 (A – M) serveurs DNS root

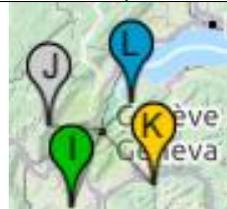


The screenshot shows the 'Root Servers' website interface. At the top, there are tabs for root servers A through M, with 'A' selected. Below the tabs, the details for root server A are displayed:

- Operator:** Verisign, Inc.
- Locations:** Sites: 5
 - Frankfurt, DE
 - Hong Kong, HK
 - London, UK
 - Los Angeles, US
 - New York, US
- IPs:** IPv4: 198.41.0.4, IPv6: 2001:503:BA3E::2:30

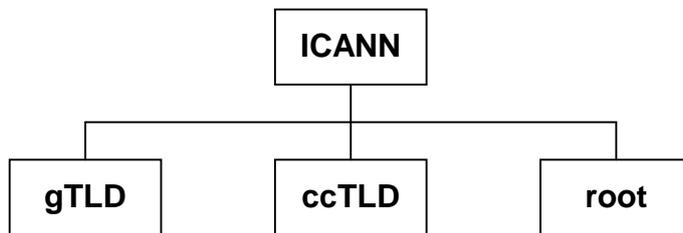
Q1a Combien de lieux géographiques possèdent un serveur root A ? 5

Q1b Combien y a-t-il de serveur root à Genève ?

	<p>4</p> <ul style="list-style-type: none">root I appartenant à NetNoderoot J appartenant à Verisignroot K appartenant à RIPE → http://www.ripe.net/ Réseaux IP Européensroot L appartenant à ICANN → http://www.icann.org/
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Remarque ICANN (*Internet Corporation for Assigned Names and Numbers*) a été créé en novembre 1998 pour harmoniser l'adressage (DNS & IP) sur internet
Plus de détail sous <http://www.icann.org/en/about/learning/faqs>

Structure



List of Top Level Domain <http://data.iana.org/TLD/tlds-alpha-by-domain.txt>

Generic Top Level Domain <http://www.icann.org/en/resources/registries/listing>

Country Code Top Level Domain <http://www.iana.org/domains/root/db/>

Action Utiliser le service whois pour connaître xxx
<http://whois.domaintools.com/>
<http://www.whois.net/>
Voir aussi <http://fr.wikipedia.org/wiki/Whois>
Voir aussi <http://www.iana.org/cgi-bin/whois>

Action Utiliser <http://www.ip-address.com/> pour connaître l'adresse IP que vous utilisez sur internet
Utile en cas de translation d'adresse

Action Utiliser l'excellent outil <http://www.intodns.com/> pour poser un avis sur la configuration d'un serveur DNS
IntoDNS checks the health and configuration and provides DNS report and mail servers report. And provides suggestions to fix and improve them, with references to protocols' official documentation.

Q1c Quels sont les points de configuration à améliorer pour la zone tdeig.ch ?
Placez-les par ordre de gravité

2	Mécanismes DNS du poste client	20'
----------	---------------------------------------	------------

Objectif Comprendre les principaux mécanismes du client DNS et les risques potentiels tels qu'une équivalence FQDN : IP erronée

But 2.1 Quel est mon serveur DNS ?

Remarque Utiliser le schéma du réseau → http://www.tdeig.ch/Schema_Reseau.pdf

Action Typier la commande `ipconfig /all` pour analyser la configuration réseau

Q2a A quoi correspond IP = 10.2.0.1 ?

Q2b Pourquoi des valeurs identiques pour certains champs ?

But 2.2 Quel est le contenu du cache DNS ?

Action Typier la commande `ipconfig /displaydns` pour afficher le contenu du cache DNS de votre PC.
Effectuer un ping sur un FQDN non présent dans le cache

Test Contrôler cette nouvelle entrée dans le cache DNS

- But 2.3** Durée de vie
- Les mécanismes DNS font un large usage de mémorisations intermédiaires dans le cache DNS du poste de travail et dans les caches DNS des divers serveurs DNS traversés.
- Action** Ouvrir le navigateur pour sélectionner divers liens puis observer la durée de vie (commande `ipconfig /displaydns` - champ Time To Live) de chaque équivalence présente dans votre cache DNS.
- Q2c** Qui fixe cette durée de vie ?
- Q2d** Quel est l'intérêt de choisir une durée de vie longue ?
- Q2e** Quel est l'intérêt de choisir une durée de vie courte ?
- Remarque** Des attaques sophistiquées et très efficaces ont sévi vers 2008
Voir les fichiers **Cache_Poisoning.pdf** et **TinyDNS.pdf** du dossier partagé sur 10.2.1.1
- But 2.4** Effacer le contenu du cache DNS ?
- Remarque** Vous pouvez effacer le contenu de ce cache puis entrer à nouveau les commandes ping précédentes afin de contrôler précisément le contenu de ce cache.
- Action** Effacer le contenu de ce cache avec la commande `ipconfig /flushdns`
- Test** Contrôler que le cache DNS est vide
- But 2.5** Modifier le fichier **hosts** pour rediriger les requêtes destinées à www.company.com sur l'adresse IP = 129.194.9.50
- Remarque** Issu du monde Unix, le fichier **C:\WINDOWS\System32\drivers\etc\hosts** en conserve le nom sous Windows sans extension
- Action** Lancer Notepad (Start – Programs – Accessories) pour contrôler qu'il n'est pas possible de modifier ce fichier
- Action** Elever les privilèges de Notepad (clic droit puis Run as administrator) puis ajouter l'équivalence `129.194.9.50 www.company.com`
- Test** Contrôler avec un navigateur (Google Chrome ou Internet Explorer) que la requête <http://www.company.com> est redirigée sur cette adresse IP
- Q2f** Comment le client DNS fonctionne-t-il ? Dans quel ordre gère-t-il le fichier host et le cache ?

3	nslookup	20'
----------	-----------------	------------

- Objectif** Utiliser la commande nslookup.exe qui permet de tester les serveurs DNS
Les commandes à entrer sont en rouge
- Action** Lancer **nslookup** dans un Command Prompt
- Remarque** Par défaut **nslookup** utilise le serveur DNS 10.2.0.1 présent dans la configuration
Voir Q2b
- But 3.1** Serveur autoritaire
- Q3a** Quel est le serveur autoritaire (soa = start of authority) de la zone bluewin.ch ?
- set type=soa**
bluewin.ch

- But 3.2** Serveurs secondaires
- Q3b** Cette zone possède-t-elle des serveurs secondaires ?
- ```
set type=ns
bluewin.ch
```
- But 3.3** Serveur de messagerie
- Q3c** Quels sont les serveurs smtp de messagerie pour cette zone ?
- ```
set type=mx  
bluewin.ch
```
- But 3.4** Réponse autoritaire
- Q3d** La réponse est-elle autoritaire = La réponse provient-elle d'un serveur autoritaire ?
- ```
set type=a
www.google.ch
```
- But 3.5** Répartition de charge (load balancing) côté serveur DNS
- Q3e** Combien de serveurs répondent à lb.tdeig.ch ?
- ```
lb.tdeig.ch
```
- But 3.6** Répartition de charge (load balancing) côté client DNS
- Q3f** Comment faire côté client pour utiliser ces 3 adresses IP ?
- But 3.7** Serveurs root
- Action** `root`
- Q3g** A quoi sert la commande précédente ?
- Action** `www.cern.ch`
- Q3h** Pourquoi n'obtenez-vous pas d'adresse IP ?
- But 3.8** Utiliser un serveur DNS par défaut autre que 10.2.0.1
- Action** `server adr_IP` en choisissant une `adr_IP`
- Q3i** A quoi sert la commande précédente ?

Objectif Configurer le PC A2-A16 comme serveur DNS
Ce serveur DNS va gérer la **zone privée xyz**
Utiliser un serveur DNS simple → choix de MaraDNS car bind est trop complexe
<https://openclassrooms.com/courses/maradns-comme-serveur-dns>

Action Répéter §2.1 du labo DHCP pour charger image CentOS

Se connecter avec le compte=**root** pass=**rootroot**
ping www.unige.ch pour tester l'accès à internet (ctrl-C pour terminer)

Installer le serveur à partir des sources

```
yum -y install gcc
```

```
yum -y install wget
```

```
wget http://maradns.samiam.org/download/2.0/2.0.11/maradns-2.0.11.tar.bz2
```

```
tar -xjf maradns-2.0.11.tar.bz2
```

```
cd maradns-2.0.11
```

```
make
```

```
make install      MaraDNS service is installed at /etc/init.d/maradns.
```

Débrancher le câble Ethernet du **PC CentOS**

Débrancher le câble Ethernet du **PC Win7**

Relier ces 2 PCs avec 1 câble court

Configurer **PC Win7** avec IP=192.168.1.1

Configurer **PC CentOS** avec IP=192.168.1.10

```
ifconfig eth0 192.168.1.10 netmask 255.255.255.0
```

Tester avec ping depuis PC Win7 et depuis PC CentOS

Editer le fichier **/etc/mararc**

```
# csv2 zone files mandatory in authoritative mode
csv2 = {}
```

```
# zone = xyz
csv2["xyz."] = "db.xyz"
#csv2["example.com."] = "db.example.com"
```

```
ipv4_bind_addresses = "192.168.1.10"
```

```
# The directory of zone files
chroot_dir = "/etc/maradns"
```

Editer le fichier **/etc/maradns/db.xyz**

```
www.xyz.      10.10.10.10 ~
1b.xyz.      10.10.10.11 ~
1b.xyz.      10.10.10.12 ~
```

Démarrer le service

```
/etc/init.d/maradns start
```

Tester avec nslookup, ping et IE (ipconfig /displaydns)

Synthèse

Les mécanismes basés sur le protocole DNS sont riches.

Le §4 présente une configuration minimale avec 1 client DNS et 1 un serveur autoritaire

Le §2 détaille les principaux mécanismes du client

Le firewall du labo fait croire qu'il est serveur DNS aux clients de l'intranet ; en fait il ne fait que transiter chaque requête vers un serveur DNS de l'arborescence étudiée au §1 ; suite dans le cours Sécurité des Systèmes d'Information

Au §3, nslookup vous permet d'effectuer des requêtes avec le serveur DNS de votre choix