# R2.05-- TD 3

## Contexte

Le sujet aujourd'hui sera le protocole DNS et son fonctionnement, mais également son articulation en réseau avec d'autres protocoles, comme par exemple le ping et l'ARP. Cette année le focus sera la résolution directe, tandis que l'année prochaine nous allons explorer la résolution inverse également.

## Exercice d'entrainement :

1. Donnez quelques avantages pour l'utilisation d'un fichier *hosts* pour faire la résolution directe et inverse. Puis, donnez quelques avantages de l'utilisation d'un serveur DNS.

**SOLUTION** :

Le fichier hosts peut permettre la résolution de nom sans avoir besoin d'une connexion à un serveur DNS. C'est une façon pratique pour faire la résolution de nom dans un petit réseau privé -- certainement si le réseau est non routable. Par contre utiliser le fichier hosts n'est pas pratique à l'échelle. Il est configuré à la main et chaque mise à jour entraine une mise à jour sur chaque machine à part.

L'utilisation du service DNS permet la résolution de nom d'une façon distribuée, qui est plus facile à maintenir. Une mise à jour s'effectue sur une seule machine, le serveur DNS. Ensuite, toute machine demandant une résolution de nom pourra effectuer son habitude comme d'habitude.

2. Dans quel cas peut-il être utile de faire une résolution inverse de nom ?

**SOLUTION** :

Pour rappel : la résolution directe de nom consiste en trouver l'adresse IP d'une machine dont on connait le nom. La résolution inverse nous trouve le nom qui correspond à une adresse IP.

La résolution inverse est particulièrement utile pour tracer qui contacte une machine donnée. Cela pourrait nous aider à savoir qui contacte une de nos machines, par exemple un serveur. La résolution inverse indique les noms des machines dont on récupère les adresses IP.

3. Quel est le FQDN de la machine ***mail*** du domaine ***unilim.fr*** ?

**SOLUTION** :

mail.unilim.fr.  (avec le point à la fin)

4. Quel est le FQDN de la machine 164.81.20.22 lorsqu'on fait la résolution inverse ?

**SOLUTION** :

22.20.81.164.in-addr.arpa.  (avec le point à la fin)

5. Quelle est la cible de la commande ***ping www*** sur la machine ***pc1.mondomaine.fr*** ?

**SOLUTION** :

La machine cherchera dans le sous-domaine indiqué et cherchera : www.mondomaine.fr

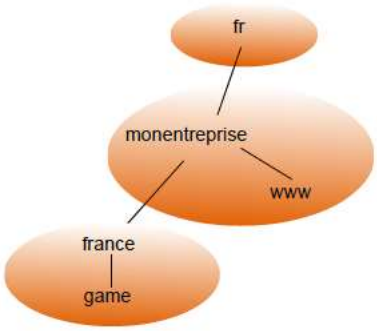
6. Qu'est-ce qui se passe si on essaie de trouver la machine **www.** (avec le point final) ?

**SOLUTION** :

Le point final indique un FQDN, donc on cherchera le TLD www. Comme il n'existe pas, le ping causera une erreur.

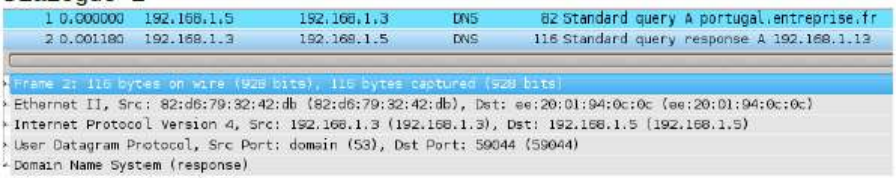
## Exercice 1

Nous partirons sur une machine ***www.monentreprise.fr*** dans la zone d'administration ***monentreprise.fr***.

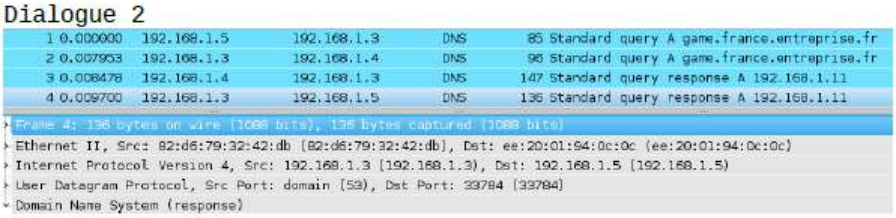



Les échanges captés ci-dessous sont des dialogues DNS.  Etudiez-les en détails, puis répondez aux questions ci-dessous.

Dialogue 1




Dialogue 2




1. Regardez le premier dialogue DNS, puis complétez le tableau ci-dessous :

| Participant | Adresse IP | Port utilisé | Client/serveur |
|---|---|---|---|
| 1 | 192.168.1.5 | 59044 | C |
| 2 | 192.168.1.3 | 53 | S |

2. Quel type de résolution (directe/inverse) est demandée dans le premier dialogue ? Justifiez votre réponse.

**SOLUTION** :

C'est une résolution directe : la demande du client a visé un nom de domaine, tandis que la réponse donnée consiste en une adresse IP.

3. Quel est le nom et l'adresse IP de la machine recherchée dans le premier échange ?

**SOLUTION** :

La requête vise le domaine portugal.entreprise.fr

La réponse indique que l'adresse IP correspondante à portugal.entreprise.fr est 192.168.1.13.

4. Quelles machines participent au deuxième dialogue DNS ? Donnez leurs adresses IPs ainsi que leurs rôles (client/serveur) dans chaque échange (chaque ligne de la capture).

Ligne 1 : 192.168.1.5 est le client DNS dans la première ligne. La machine 192.168.1.3 est le serveur DNS.

Ligne 2 : 192.168.1.3 est le client DNS dans la deuxième ligne. La machine 192.168.1.4 est le serveur DNS.

Ligne 3 : 192.168.1.4 est le serveur DNS dans la troisième ligne. La machine 192.168.1.3 est le client.

Ligne 4 : 192.168.1.3 est le serveur DNS et 192.168.1.5 est le client.

5. Expliquez ce qui se passe dans le deuxième dialogue DNS ci-dessus.

**SOLUTION** :

Un client (192.168.1.5) demande une résolution de nom pour portugal.entreprise.fr à son serveur DNS (192.168.1.3). Celui-ci ne connait pas la réponse à la requête du client, donc il contacte son serveur DNS (192.168.1.4). Ce deuxième serveur connait bien la réponse et fait suivre l'adresse IP du domaine ciblé à la machine 192.168.1.3. Cette dernière fait suivre la réponse au client qui avait fait la demande initiale.

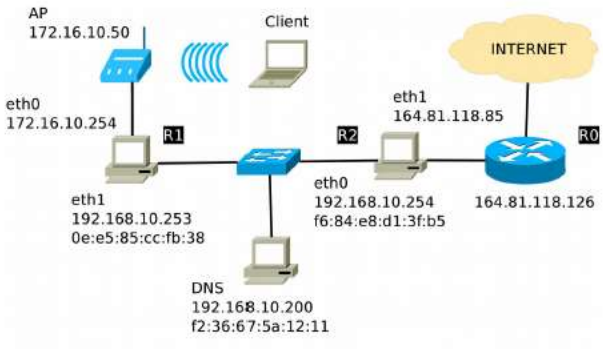
6. Décrivez précisément la fonctionnalité et la nature de la machine dont l'adresse IP est 192.168.1.4.

**SOLUTION** :

La machine 192.168.1.3 n'a pas su répondre à la demande portugal.entreprise.fr car elle ne fait pas autorité sur ce domaine. Au contraire, la machine 192.168.1.4 est un serveur DNS qui fait autorité sur portugal.entreprise.fr.

## Exercice 2

Prenons la topologie suivante, qu'on a déjà vu lors du TD1. Munissez-vous avec votre correction du TD1, pour pouvoir déjà avoir les éléments de topologie (réseaux présents, passerelles, etc.).




Supposons qu'un serveur HTTP, hébergeant le domaine www.exemple.mondomaine.fr. est mis sur une machine dont l'adresse est 172.16.10.33, qui est connectée à la machine R1. Le serveur DNS indiquée dans la figure (en bas) fait autorité sur mondomaine.fr. -- on suppose que le serveur DNS a déjà été configuré. De plus, la machine DNS est le serveur de nom par défaut de toutes les machines dans la figure. On suppose que toute la configuration des adresses IP et du routage a déjà été réalisée.

Finalement, on va considérer que les caches ARP de toutes les machines sont vides.

1. La machine R2 veut faire un ping à l'adresse 172.16.10.33. Donnez la suite de messages, ARP et ICMP, qui doivent s'enchainer pour que le ping passe (et retourne) entre les deux machines. Pour chaque message ARP indiquez : son type (requête/réponse), ainsi que les adresses (IP et MAC) de la source, la destination et la cible. Pour chaque message ICMP indiquez : son type (requête/réponse), ainsi que les adresses (IP et MAC) source et destination.

Le chemin est : R2 → R1 → 172.16.10.33, et au retour, le message prendra la route inverse. Pour le chemin d'aller :

- R2 devra premièrement faire une requête ARP (en broadcast FF :FF :FF… :FF, adresse de l'expéditeur @MAC de R2 eth0, @IP R2 eth0) ciblant la machine R1 eth1 (@IP 192.168.10.253, @MAC 00 :00 :00… :00 car inconnue).
- La réponse ARP viendra de R1, à destination de R2 eth0 (@MAC de R2 eth0, @IP R2 eth0), de l'expéditeur R1 (@IP 192.168.10.253, @MAC R1 eth1) pour la cible R1 eth1 (@IP 192.168.10.253, @MAC R1 eth1).
- Le ping partira de R2, encapsulé en tant que paquet ICMP. @IP src. R2, @IP dst. 172.16.10.33, @MAC src. R2 eth0, @MAC dst R1 eth1

La même chose se passera ensuite pour l'étape R1 → 172.16.10.33 :

- R1 devra premièrement faire une requête ARP (en broadcast FF :FF :FF… :FF, adresse de l'expéditeur @MAC de R1 eth0, @IP R1 eth0) ciblant la machine 172.16.10.33 (@IP 172.16.10.33, @MAC 00 :00 :00… :00 car inconnue).
- La réponse ARP viendra de 172.16.10.33, à destination de R1 eth0 (@MAC de R1 eth0, @IP R1 eth0), de l'expéditeur 172.16.10.33 (@IP 172.16.10.33, @MAC de la machine 172.16.10.33) pour la cible 172.16.10.33 (@IP 172.16.10.33, @MAC de 172.16.10.33).
- Le ping partira de R1, encapsulé en tant que paquet ICMP. @IP src. R2, @IP dst. 172.16.10.33, @MAC src. R1 eth0, @MAC dst adresse de 172.16.10.33

Et pour le retour également (là, 172.16.10.33 aura besoin de l'@MAC de R1 eth0 et R1 de l'@MAC de R2 eth0).

2. On resuppose maintenant que tous les caches ARP sont vides. La machine R2 fait un ping vers www.exemple.mondomaine.fr . Quelles requêtes et réponses se rajoutent aux messages ARP et ping vus précédemment ? Décrivez les contenus de ces messages.

   On aura les messages DNS. La machine R2 fait une demande DNS à destination de son serveur DNS (@IP 192.168.10.200) pour savoir l'adresse IP du site demandé. La réponse indiquera 172.16.10.33 en tant que destination.
   Pour chaque message DNS, il y aura aussi des messages ARP l'accompagnant, demandant l'@ MAC du serveur DNS (et le serveur demandera l'@ MAC de la machine R2 respectivement)

3. Disons que la machine R2 n'avait pas de serveur DNS configuré. Quel aurait été le message d'erreur lorsqu'on tape la commande du ping de la question 2 ?

   **Correction** : Echec temporaire de résolution de nom (DNS)

4. Maintenant supposons que R2 avait, en tant que serveur DNS par défaut, une autre machine 164.81.1.4. Quel effet cette modification aura-t-elle sur les messages listés à la question 2 ?

   **Correction** : au lieu de contacter le serveur DNS de la figure, la machine R2 aurait envoyé ses requêtes à la machine 164.81.1.4. Si le routage est réalisé, aucun problème. À son tour, le serveur 164.81.1.4 aurait demandé qui faisait autorité sur le domaine ci-dessus, et donc la machine 164.81.1.4 aurait fini par demander au serveur DNS de la figure de faire sa résolution.

## Exercice 3

Nous considérons un domaine dont le nom sera ***domaine.org***. Celui-ci contient un nombre de machines, listées ci-dessous avec leurs adresses IP respectives.

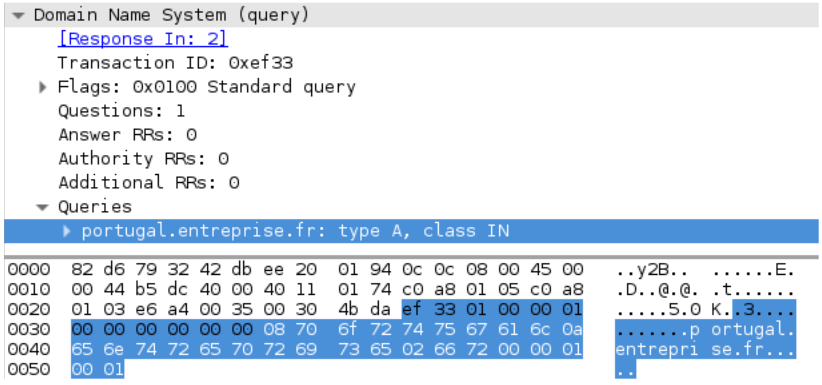
| Type de machine | Adresse IP |
|---|---|
| firewall | 192.168.56.254 |
| dns | 192.168.56.11 |
| http | 192.168.56.15 |
| www | 192.168.56.15 |
| files | 192.168.56.18 |

Complétez ci-dessus le contenu du fichier ***db.domaine.org*** correspondant à ce domaine.

```
$TTL 86400
$ORIGIN domaine.org.
@ IN SOA  dns.domaine.org.   root.dns.domaine.org. {
          2019060201 ; numéro de serie AAAAMMJJNN
          10800 ; rafraîchissement
          3600 ; nouvel essai
          604800 ; obsolète au bout d'une semaine
          86400 ; TTL 1 jour
}

; serveurs de noms

@     IN      NS     dns.domaine.org.

dns     IN      A        192.168.56.11

; hôtes declares

firewall     IN      A        192.168.56.254
http       IN      A        192.168.56.15
files      IN      A        192.168.56.18
www     IN    CNAME    http.domaine.org.
```

# Exercice 6 (difficile)

Voici une capture d'écran pour une certaine requête DNS. Cette requête est reçue sur le port UDP/53.




En regardant cette requête, indiquez quel est le format des messages DNS.

**SOLUTION** :

Les chiffres en noir représentent l'en tête DNS.

0x ef 33 (2 octets) = transaction ID

0x 01 00 (2 octets) = flags & codes : indique une requête.

Nombre de questions (2 octets ) : 1

Nombre de réponses RR (resource records) : 0

Nombre de RR sous autorité : 0 (nombre de registres retournés)

Nombre de RRs en plus retournés : 0

A voir aussi : http://www.networksorcery.com/enp/protocol/dns.htm