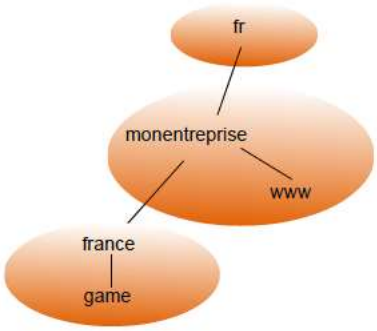
R2.05-- TD 3

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 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

1	0.000000	192.168.1.5	192.168.1.3	DNS	82 Standard query A portugal.entreprise.fr
2	0.001180	192.168.1.3	192.168.1.5	DNS	116 Standard query response A 192.168.1.13

```
Frame 2: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
Ethernet II, Src: 82:d6:79:32:42:db (82:d6:79:32:42:db), Dst: ee:20:01:94:0c:0c (ee:20:01:94:0c:0c)
Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.5 (192.168.1.5)
User Datagram Protocol, Src Port: domain (53), Dst Port: 59044 (59044)
Domain Name System (response)
```

Dialogue 2

1	0.000000	192.168.1.5	192.168.1.3	DNS	85 Standard query A game.france.entreprise.fr
2	0.007953	192.168.1.3	192.168.1.4	DNS	98 Standard query A game.france.entreprise.fr
3	0.008478	192.168.1.4	192.168.1.3	DNS	147 Standard query response A 192.168.1.11
4	0.009700	192.168.1.3	192.168.1.5	DNS	136 Standard query response A 192.168.1.11

```
Frame 4: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits)
Ethernet II, Src: 82:d6:79:32:42:db (82:d6:79:32:42:db), Dst: ee:20:01:94:0c:0c (ee:20:01:94:0c:0c)
Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.5 (192.168.1.5)
User Datagram Protocol, Src Port: domain (53), Dst Port: 33784 (33784)
Domain Name System (response)
```

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

Participant	**Adresse IP**	**Port utilisé**	**Client/serveur**
1			
2			

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

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

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 :

   Ligne 2 :

   Ligne 3 :

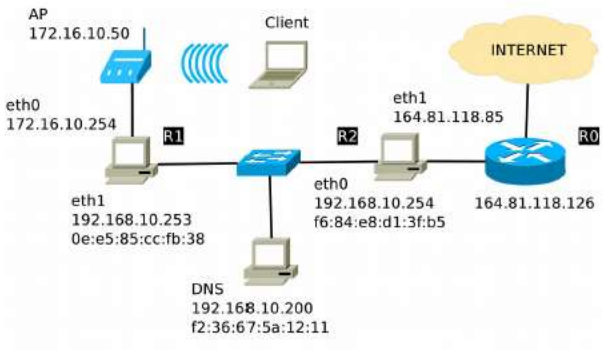
   Ligne 4 :

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

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

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.

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.

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 ?

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 ?

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.

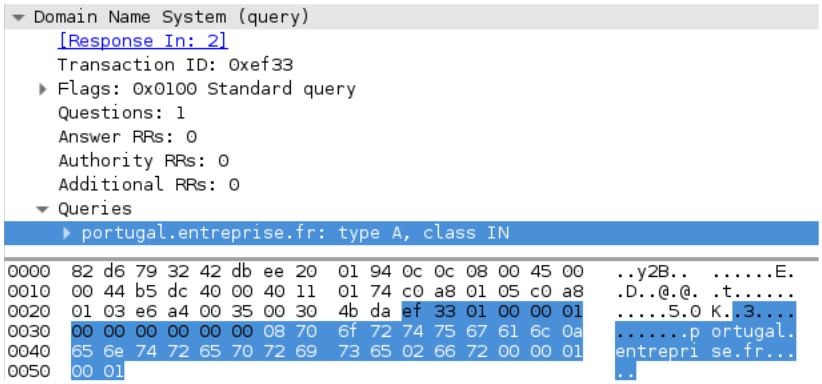
Type de machine	Adresse IP
firewall	192.168.56.254
dns	192.168.56.11
http	192.168.56.15
www	192.168.56.15
files	192.168.56.18

```
_____

_________ IN SOA _____ {
        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   _____

_____   IN   A    _____



; hôtes declares
```

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

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.