TP n°3 – ARP

1. Le protocole ARP (Address Resolution Protocol)

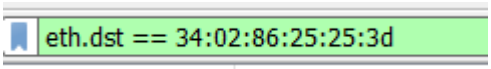
1. Relevez les informations données par la commande arp –a, dans une invite de commandes notamment comptez le nombre d'entrée présentes dans cette table et indiquez à quoi sert cette table.

L'expérience ci-dessous n'est réalisable qu'avec plusieurs machines connectées sur le même réseau local. Après réalisation de l'expérience, pour vous aider à comprendre le fonctionnement du protocole ARP, vous pouvez visualiser la vidéo suivante :
https://unice-my.sharepoint.com/:v:/g/personal/joanna_moulierac_unice_fr/EQEPOjEaC19FhYTSNEXoVscBNaXFElLdfd53dlsIr6z5cQ?e=bp9BPg

2. Démarrez une capture wireshark. L'idéal serait que vous commenciez tous ensemble l'expérience, notamment avec le poste enseignant affiché par vidéo-projecteur. En effet, vous allez pouvoir voir le trafic des tous les postes de la salle.
3. Communiquez avec la machine de votre voisin en envoyant un ping à son adresse IP[1]. Il réalisera en même temps que vous une capture wireshark pour observer les paquets que vous lui transmettez.
4. Combien de paquets sont générés dans votre capture suite à cette commande ? Déduisez-en comment fonctionne un ping.
5. Relancez arp -a. Expliquez les changements que vous observez. Vous devriez pouvoir déduire l'adresse mac de votre voisin.
6. Refaites un ping sur la même adresse. Que constatez-vous sur le temps d'exécution de ce deuxième ping par rapport au tout premier paquet envoyé ?
7. Arrêtez les deux captures wireshark (la vôtre et celle de votre voisin) et confirmez vos observations de la question précédente. Pour voir les paquets qui vous intéressent, filtrez les paquets avec la commande : 'icmp or arp'. Vous devriez notamment vous apercevoir que les échanges ARP lors du deuxième ping n'ont plus lieu. Pourquoi ?
8. Refaites la même expérience en faisant un ping sur www.lemonde.fr.
9. Y-a-t-il une nouvelle entrée dans la table arp correspondant à l'adresse mac du monde ? Pourquoi ?
10. Observez les ICMP Echo request générés dans la capture wireshark lors du ping vers lemonde, quelles sont les adresses mac source et destination présentes dans la couche 2 ? A quelles machines correspondent-elles ?
11. Pour voir tous les paquets dont l'adresse mac destination est celle qui vous intéresse, vous pouvez rentrer le filtre : eth.dst==@mac. Il faut bien évidemment renseigner l'adresse mac qui

[1] Pour réaliser un ping sur des ordinateurs portables windows connectés en WIFI, il faut que vous ajoutiez une règle à votre pare-feu pour autoriser le trafic ICMP entrant sur votre machine. Ainsi, vous pourrez réaliser la même expérience, uniquement entre les autres machines connectées en WIFI. Par contre, l'expérience visée ne fonctionnera pas si vous essayer de réaliser un ping vers les machines de la salle.

nous intéresse.

Exemple : 

12. Dans Statistiques/Conversations, vous pourrez voir tous les paquets qui ont été échangés durant la capture avec la passerelle : il s'agit de tout le trafic qui est destiné hors du réseau local (hors de votre salle de TP).

A la maison : regardez la vidéo sur les mécanismes ARP : https://www.youtube.com/watch?v=xtJ5FnxIUZ8.

2. Le protocole ARP dans wireshark

Ouvrez le fichier `arp.cap` avec wireshark.

1. Identifiez des requêtes et des réponses ARP dans ce fichier de capture. Donnez le numéro d'une requête et d'une réponse associée ainsi que les adresses MAC et IP de la machine qui envoie la requête ainsi que celles de la machine qui répond.

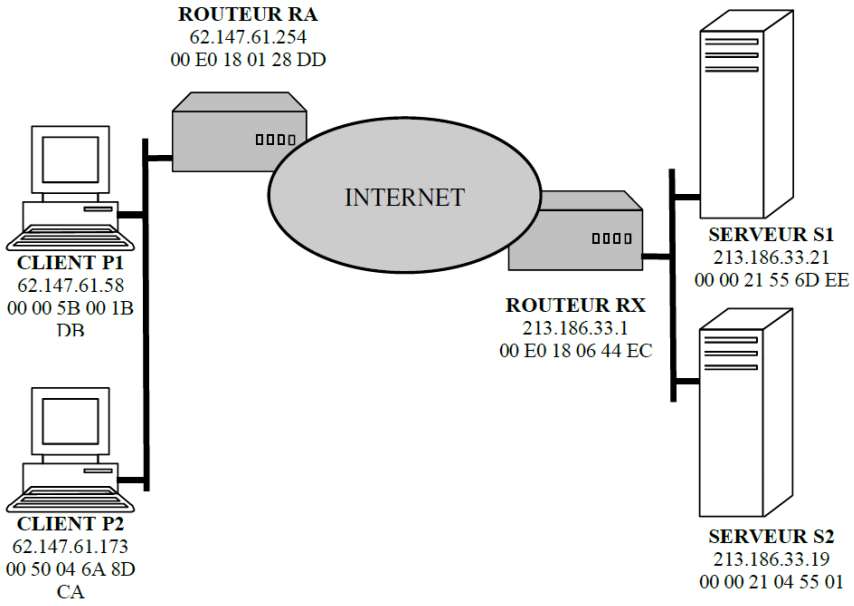
2. Déduisez-en les possibles adresses IP et adresses mac de la machine sur laquelle a été faite la capture.

3. Combien de couches contient une requête ? et une réponse ARP ? ARP est un protocole de quelle couche du modèle OSI?

4. Quel est le champ dans l'entête arp qui permet de distinguer une requête d'une réponse ?

5. Comment est remplie la « target mac address » dans une requête ARP ? Pourquoi ? Comment est-elle remplie dans la réponse arp ? Dans quel champ est contenue l'adresse mac qu'on avait demandé en broadcast ?

3. ARP avec plusieurs réseaux locaux



Le poste CLIENT P2 d'adresse IP 62.147.61.173 va faire une requête HTTP vers le serveur WEB d'adresse IP 213.186.33.19. Cette adresse IP n'appartenant pas à son réseau, le client va donc envoyer sa requête vers son routeur INTERNET, dont il connaît l'adresse IP, pour qu'il puisse l'acheminer.

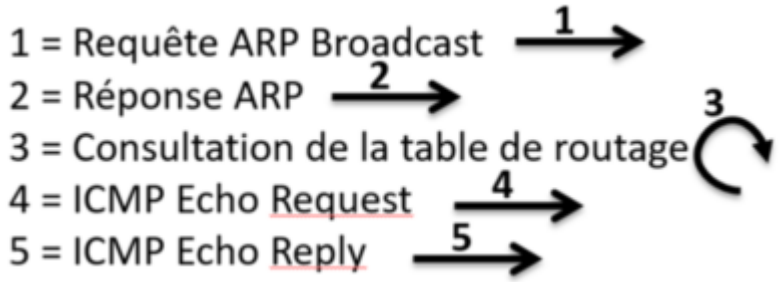
1. Quelles sont les adresses IP Source et destination contenues dans le paquet envoyé par le client P2 ?
2. Quelles sont les adresses mac source et destination contenue dans le paquet envoyé par P2 une fois la résolution ARP établie ?
3. Vous devez donc être capable de compléter le paquet prêt à être envoyé depuis P2 :

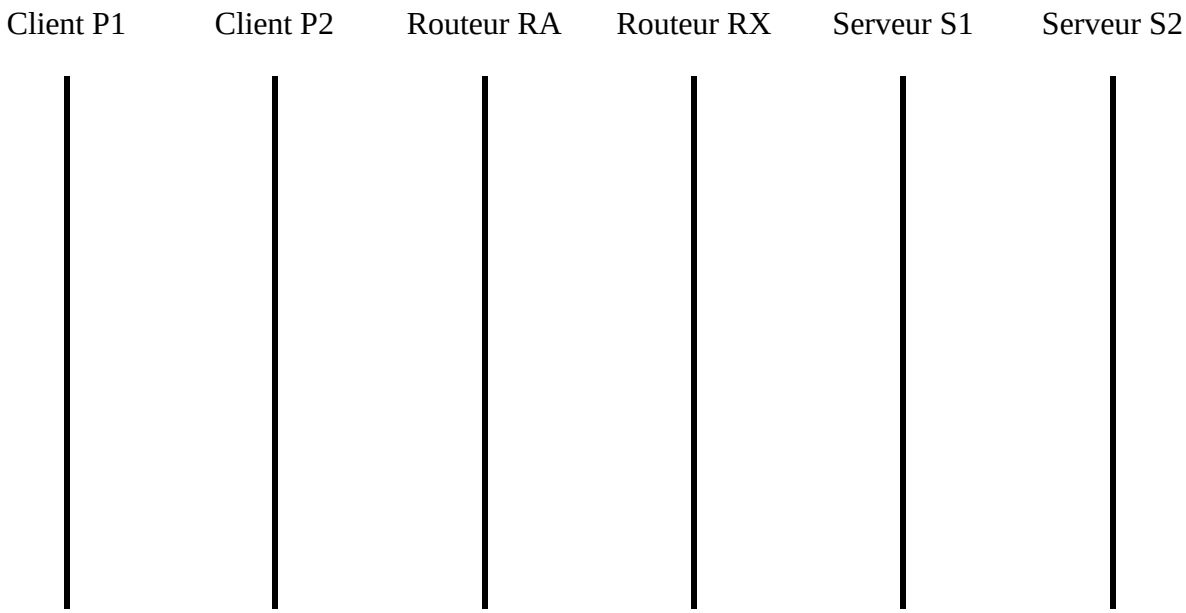
Requête http prête à être envoyée :

Couche 5 : Application (http)	GET /index.html http/1.1
Couche 4 : Transport (tcp)	destination.port = http
Couche 3 : Réseau (IPv4)	IP.src= IP.dst = TTL = Protocole =
Couche 2 : Liaison (ethernet)	@mac_src = @mac_dst = Type =

4. Vous indiquerez ensuite les états du paquet de RA à RX puis de RX à S2 (il faut indiquer quels sont les champs qui sont modifiés dans l'entête à chacune de ces étapes).
5. Vous ferez de même pour le retour de S2 à P2.

6. Représenter sous forme d'un diagramme les échanges (lors d'un ping de P2 vers S2) qui ont lieu en prenant pour hypothèse que toutes les tables ARP sont vides au moment où le paquet arrive sur le routeur. La consultation de la table de routage correspond au calcul du prochain saut en fonction de la destination du paquet.





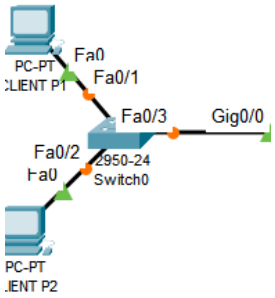
4. ARP avec plusieurs réseaux locaux avec Packet Tracer

Démarrer Packet Tracer et ouvrez le fichier **exo-diagramme.pkt** qui représente la topologie ci-dessus. Vérifiez bien que même les adresses mac correspondent au dessin !

Ne mettez en visible que les filtres **ARP, ICMP et http** dans le mode simulation.

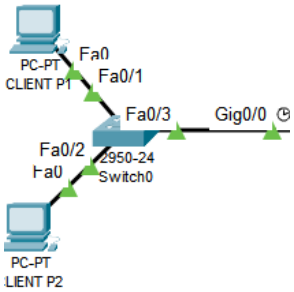
Compte-tenu de la manière de traiter le "Spanning Tree Protocol", Packet Tracer met les interfaces du commutateur en orange en mode réel. Pour corriger cela, cliquer sur l'icône  , et attendre que la lumière passe au vert, puis cliquer sur l'icône **Simulation**.

A l'ouverture du fichier, les ports sont en orange, ils ne sont pas prêts…

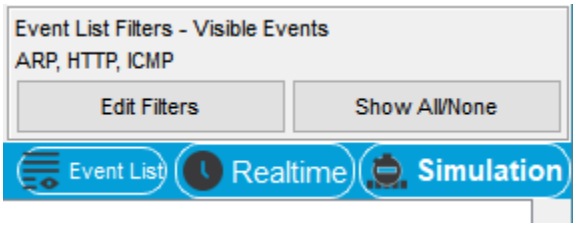


Vous cliquez sur Fast Forward Time (ou alors vous attendez patiemment) :

Ils deviennent prêts :

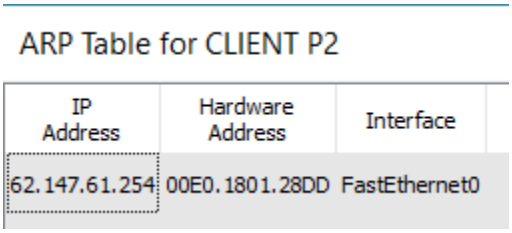


Passez en mode simulation, et assurez-vous que vous avez bien les mêmes filtres qu'indiqué ci-dessous :

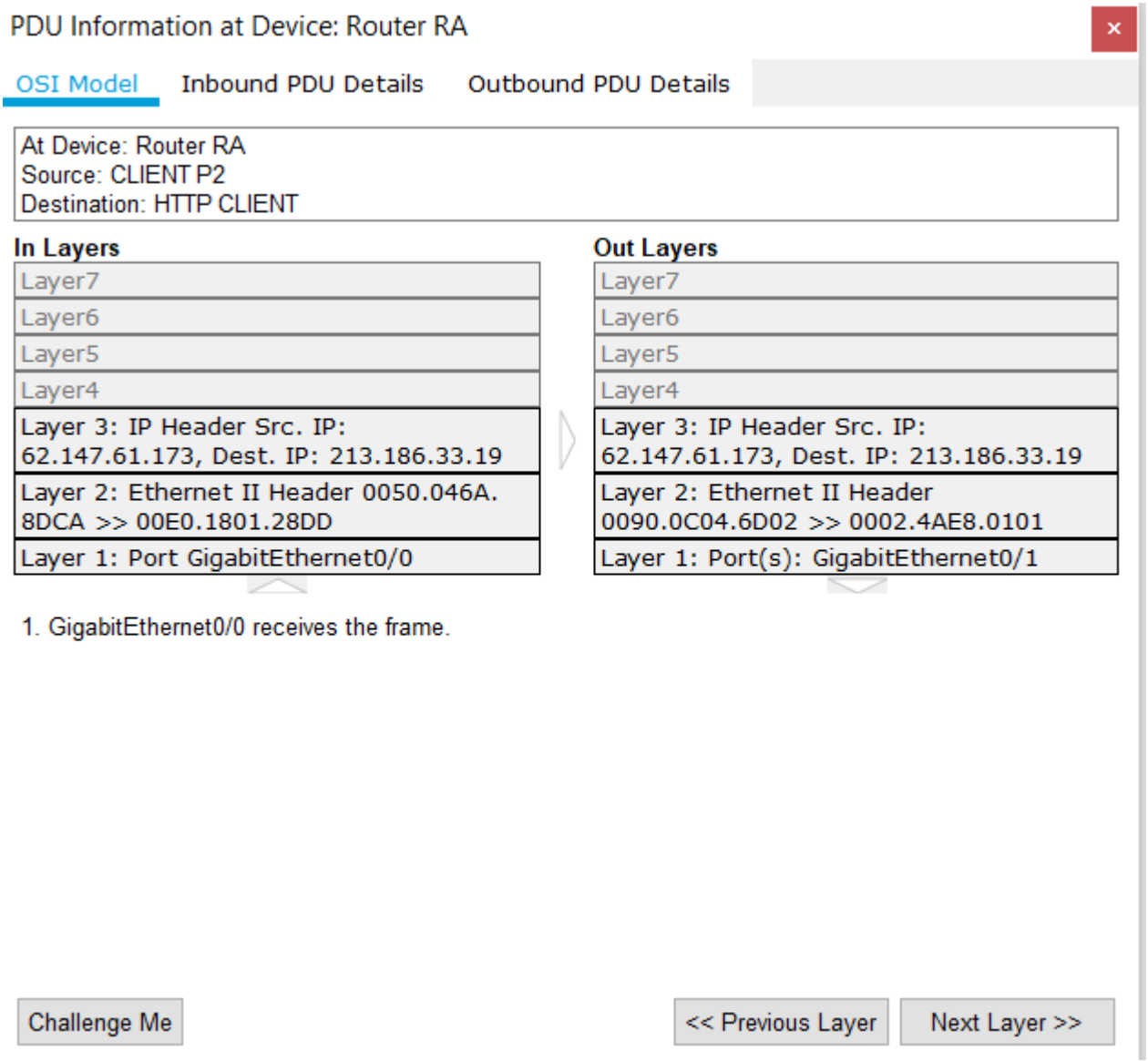


Allez sur Desktop/Web browser de la machine P2 et tapez dans le navigateur l'adresse du serveur WEB : http://213.186.33.19

1. Vérifiez que la résolution ARP (ARP Broadcast puis ARP Replu) a bien eu lieu une fois la communication établie et que les tables sont bien remplies (avec l'outil loupe). Faites des captures d'écran.



2. Voici les informations que vous devez voir le routeur RA lorsque le paquet passe par lui. Identifiez dans la capture ci-dessous à qui appartiennent les @mac et les @IP.



3. Est-ce que vous retrouvez l'adresse mac de S2 dans la table ARP de P2 ? Quelle est l'adresse mac que vous trouvez ?
4. Vérifiez que la table ARP des routeurs soit bien remplie comme ci-dessous. A quoi correspondent les entrées ?

ARP Table for Router RA

IP Address	Hardware Address	Interface
10.0.0.1	0002.4AE8.0101	GigabitEthernet0/1
10.0.0.2	0090.0C04.6D02	GigabitEthernet0/1
62.147.61.58	0000.5B00.1BDB	GigabitEthernet0/0
62.147.61.173	0050.046A.8DCA	GigabitEthernet0/0
62.147.61.254	00E0.1801.28DD	GigabitEthernet0/0

5. Faites un ping à l'aide de l'onglet Desktop/Command Prompt de P2 vers le serveur S2, et remarquez que les échanges ARP n'ont plus lieu car les caches ARP ont déjà été remplis. Listez bien toutes les étapes de la communication, en tapant bien sur « Next layer » dans le paquet. Remarquez bien le paquet tel qu'il est reçu (Inbound) et tel qu'il est envoyé par le routeur (en Outbound). *Vous pouvez effacer éventuellement le cache arp par la commande arp –d sur un commnd Prompt, ou clear arp-cache sur un routeur afin de refaire l'expérience…*

Faites un résumé de cette expérience sous Packet Tracer. Notamment, indiquez à quoi servent les tables de commutation du switch et la table ARP. Quand sont-elles utilisées, et quand sont-elles remplies ? A quel moment avons-nous besoin d'ARP et quand ne l'utilise-t-on plus ?