3 TP 03 – ANALYSE DU TRAFIC RESEAU (2/2) – ETHERNET ET ARP

Continuons l'étude du fonctionnement des protocoles réseaux via l'analyse du trafic en utilisant Wireshark. Dans ce TP, deux protocoles sont à considérer, à savoir le protocole Ethernet et le protocole ARP.

3.1 PREREQUIS

Ce TP nécessite d'avoir des notions sur Wireshark, pour cela il requiert la réalisation du TP n° 02 (sur Wireshark). Aussi, il exige la compréhension du principe d'encapsulation.

3.2 ENCAPSULATION DANS LA PILE TCP/IP

Selon le principe d'encapsulation, les informations du protocole de la couche *N* sont ajoutées en entête du bloc de données provenant du protocole de la couche supérieure *N+1*. Autrement dit, le bloc de données provenant de la couche *N+1* est encapsulé dans le champ « Données » du paquet du protocole de la couche *N*, dont l'entête contient les informations de protocole de la couche *N*.

Ainsi, le dernier bloc de données transmis dans le média de transport et capturé par Wireshark, qui est une trame Ethernet, contient dans son entête une *succession* des entêtes de tous les protocoles encapsulés dans cette trame. Ces entêtes sont tous des données de contrôle, et les données utiles (de l'utilisateur) sont contenu dans le champs données du protocole de la couche « Application ».

Exemple. Pour un message HTTP l'ordre d'encapsulation est « HTTP-TCP-IP-Ethernet » (voir Figure 8a). Noter que pour Wireshark, il sera affiché inversement « Ethernet-IP-TCP-HTTP » (déjà vu dans TP 2, section 2.2.4). La structure de la trame capturée par Wireshark est illustrée dans la Figure 8b.

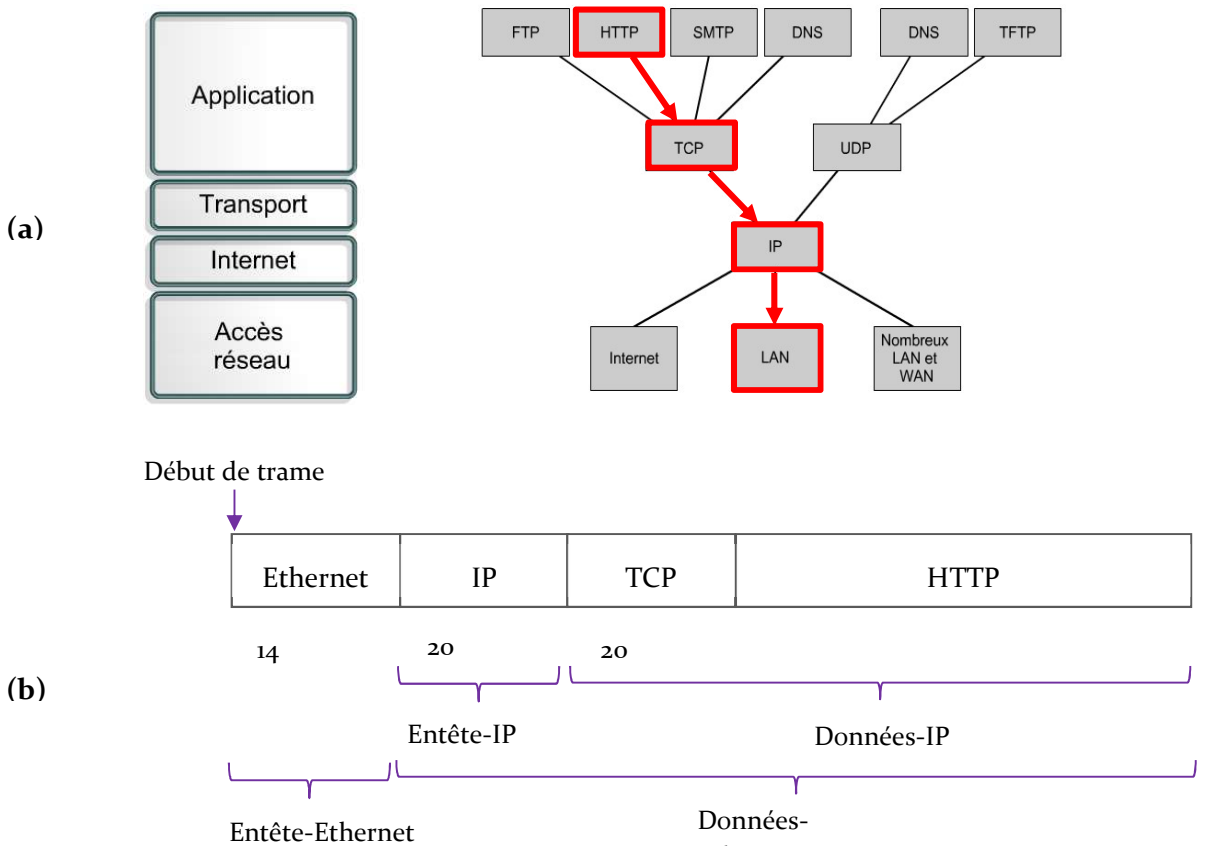


Figure 9. *Ordre d'encapsulation d'un message HTTP.*

La trame Ethernet contient l' « Entête Ethernet » et le champ « Données Ethernet ». Ce dernier contient le paquet IP dont la structure n'est pas reconnue par la couche Ethernet, et ainsi c'est à la couche supérieure de déterminer son en-tête et ses données. De même pour le champ Données IP qui contient le message TCP, et ainsi de suite. La Figure 9 illustre la structure (ainsi que la succession des entêtes des différents protocoles encapsulés) pour un message http capturé.

La taille des en-têtes d'un paquet peut être calculée en sachant sa structure (les différents champs qui les constituent), pour cela voir *Annexe*. Par exemple, l'entête Ethernet est de 14 octets, l'entête IP et TCP sont de 20 octets chacun. Noter que la taille de l'entête peut variable, qui est le cas de l'entête HTTP.

Wireshark affiche aussi, tout en bas dans la barre d'état, la taille l'entête du protocole sélectionné dans la zone (2). Dans la Figure 9, la barre d'état indique que la taille de l'entête Ethernet est de 14 octets.

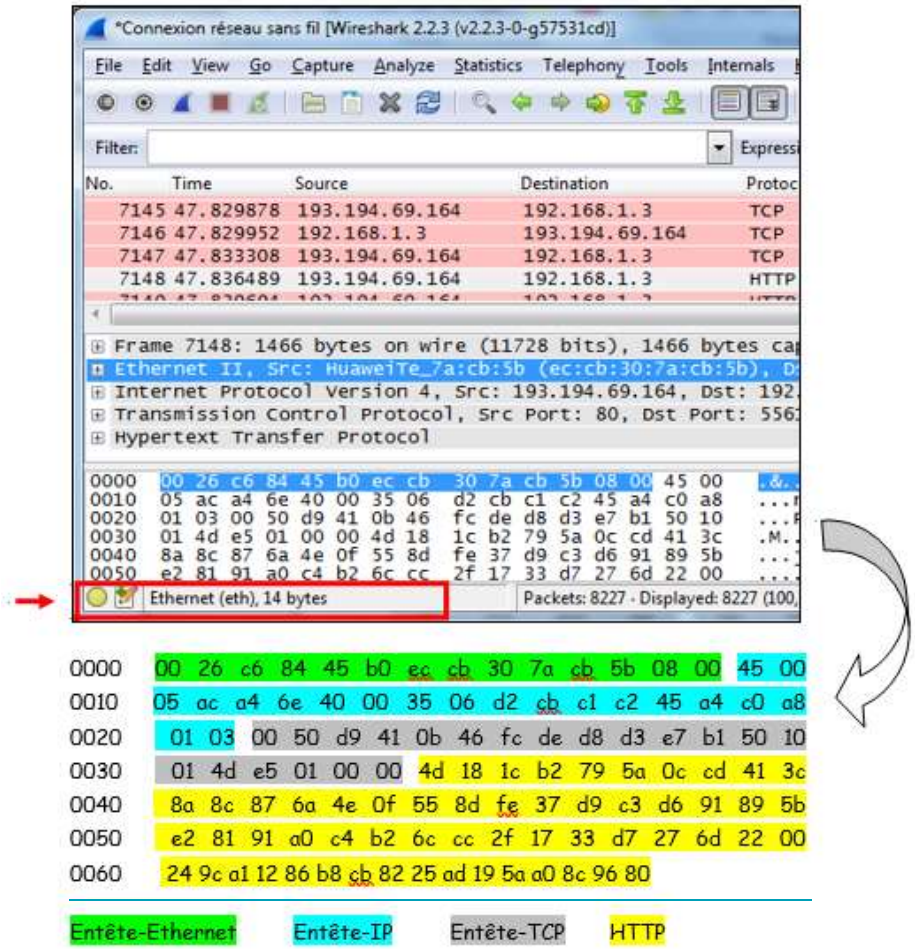
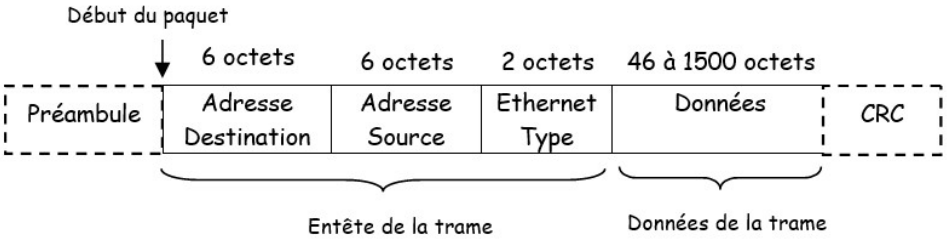


Figure 10. *Entêtes des différents protocoles utilisés pour l'envoie d'un paquet HTTP.*

3.3 PROTOCOLE ETHERNET

Voici la structure de la trame Ethernet. Pour plus de détail voir *Annexe*.



Soit un trafic réseau capturé à l'aide de Wireshark (Figure 10). Sélectionner un paquet dans la zone (1), et dans la zone (2) appuyer sur [+] du niveau Ethernet pour voir les différents champs d'en-tête Ethernet.

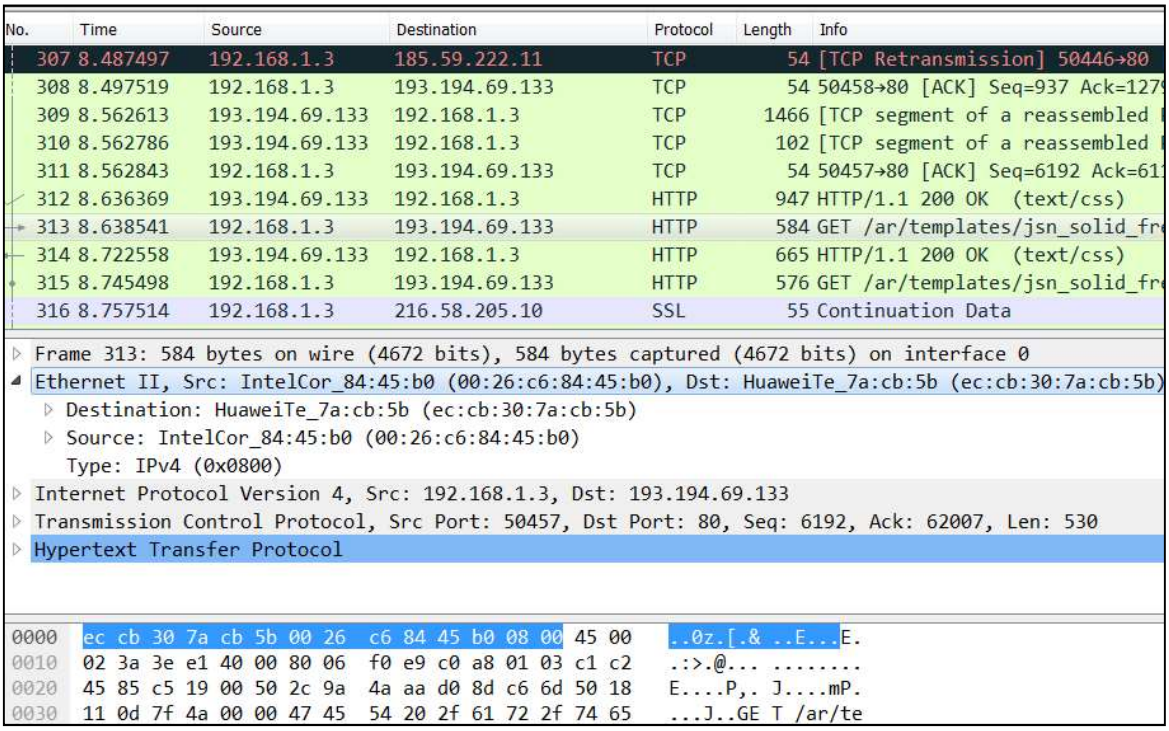


***Figure 11**. Entête Ethernet afficher par Wireshark.*

Noter que :

- Le champ « Préambule » ne figure pas dans la trame car il ne contient pas de données utiles, et il est seulement un mécanisme pour aider la carte réseau à identifier le début de la trame.
- Il y a une adresse de destination et une adresse source. Wireshark déchiffre les 3 premiers octets de l'adresse et nous indique le fabricant de la carte. Par exemple Huawei.
- Les trames Ethernet sont généralement de type "Ethernet II". Ceci est connu grâce au champ « Type ». Noter que dans le cas d'une trame Ethernet I (IEEE 802.3), il y a le champ « Longueur » au lieu de « Type », et qui indique la longueur de la trame Ethernet.
- Le champ « Type » contient une valeur hexadécimale qui indique le protocole de la couche supérieure concerné par la trame. Par exemple, si sa valeur est 0x0080 donc la trame est destinée au protocole IP, et ainsi le champ « Données » de la trame Ethernet contient le paquet IP.
- Le champ « Données » commence par l'en-tête du protocole de la couche Internet (dans le cas de la figure, c'est l'entête du paquet IP).
- Le champ « Données » peut contenir des données de remplissage dans le cas d'une trame de taille inférieure à 64 octets.
- Il n'y a pas de champ CRC. Il existe mais il est invisible pour le système ou pour Wireshark, car il est directement utilisé (consommé) par l'équipement (niveau Ethernet) qui envoi et/ou reçoit les trames où il calcule la somme de contrôle et vérifie la présence d'erreurs.

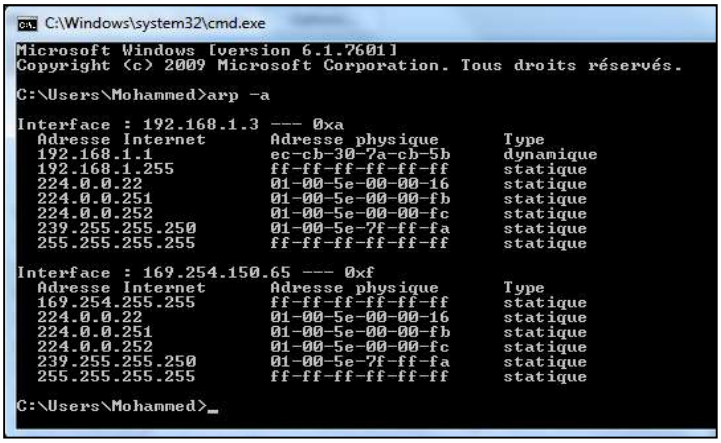
N.B. Lorsqu'une trame Ethernet arrive à un ordinateur, la couche Ethernet doit remettre le paquet contenu dans la trame au protocole correspondant de la couche supérieure qui est la couche Internet (il peut être IP ou ARP, etc.). La question est comment le protocole Ethernet le sait-il ? Aussi, une fois reçu par le protocole correspondant de la couche supérieure (par exemple le protocole IP), lui aussi doit être en mesure de déterminer à quel protocole de la couche supérieure (Transport) est destiné (TCP ou UDP). La réponse

est que les protocoles utilisent une information (un champ) dans leur en-tête pour déterminer le protocole concerné dans la couche supérieure. Dans le cas d'Ethernet c'est le champ « Type ».

3.3.1 Le protocole ARP

ARP est utilisé pour trouver l'adresse Ethernet (l'@ MAC) correspondante à une adresse IP locale. Les combinaisons [@IP - @MAC] sont sauvegardées dans une mémoire cache qui peut être manipulée en utilisant des commandes comme suit :

1. *Consulter le cache ARP.* Taper la commande « arp –a » dans l'invite de commande.

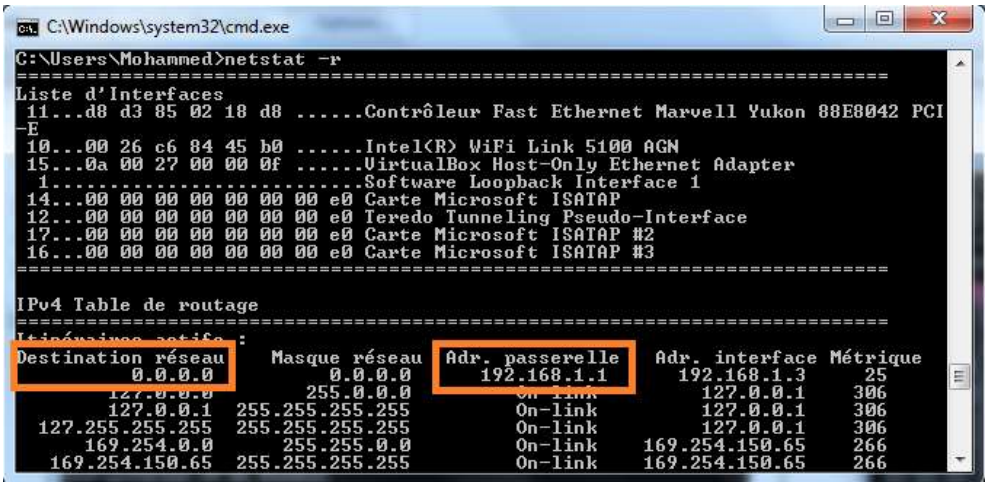


2. *Supprimer une entrée dans le cache ARP.* Lancer l'invite de commande cette fois-ci en cliquant avec le bouton droit et en choisissant « exécuter en tant qu'administrateur ». Ensuite, taper la commande :
   "arp –d @IP de la passerelle"
   Par exemple, pour effacer l'@IP 192.168.1.1 de la cache ARP, on tape : arp –d 192.168.1.1

3.3.1.1 Capture d'un trafic ARP

Dans la salle de TP, la connexion d'un ordinateur au réseau internet se fait selon le schéma dans la Figure 11. Toute requête lancée par l'ordinateur passe par la passerelle. Ceci est aussi le schéma de connexion de l'ordinateur de la maison connecté à Internet à travers un modem. Dans ce cas, ce modem est la passerelle. Rappeler que la passerelle est l'équipement (généralement un routeur) local que la machine utilise pour se connecter au réseau internet.

N.B. Pour connaitre l'adresse IP de la passerelle, on utilise la commande « **netstat –r** ». L'adresse de la passerelle est celle correspondante à la destination par défaut 0.0.0.0.



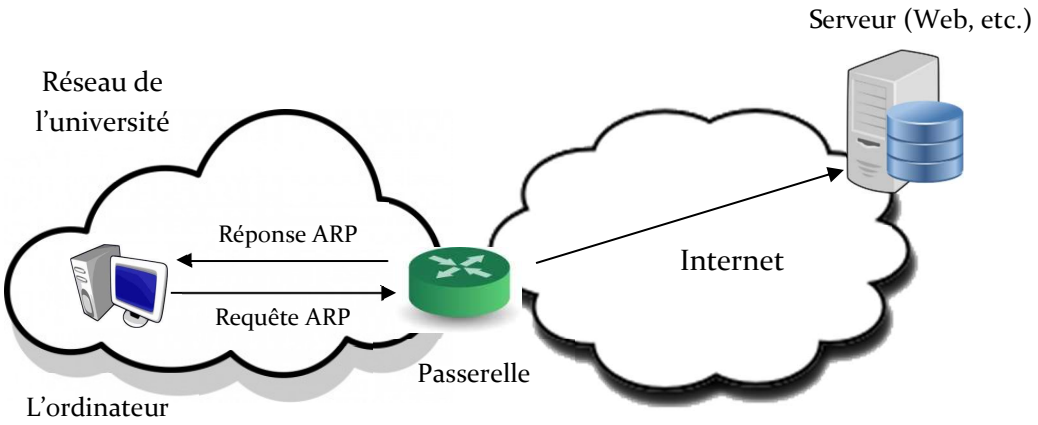
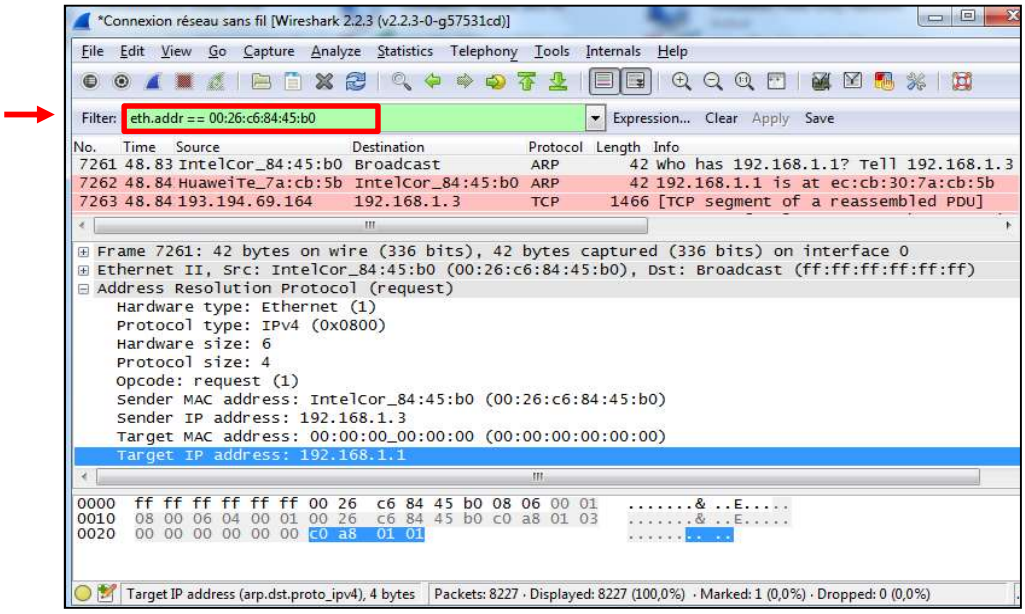


***Figure 12**. Schéma de connexion d'un ALN au réseau Internet.*

En utilisant le navigateur web pour charger une page web (ex. la page Google), pour que la requête puisse être envoyée au serveur, l'ordinateur doit connaitre l'@MAC de la passerelle, et ainsi il va utiliser le protocole ARP pour la trouver. L'échange de paquets ARP capturé par Wireshark a donné ceci :



Noter qu'un filtre est appliqué pour n'afficher que les paquets ARP correspondent à l'adresse MAC de la machine sur laquelle on travaille. Pour ce faire, on tape : "eth.addr == @MAC de la machine".

Il existe deux types de paquets ARP (distingués par la colonne Info de la zone 1) :

1. *Paquet Demande :* La ligne Info de ce paquet contient « Who has @IP », dans cet exemple c'est : « Who has 192.168.1.1 ? » (Voir la trame n° 7261).
2. *Paquet Réponse :* La ligne Info de ce paquet contient « @IP is at @MAC », voir la trame n°7262.

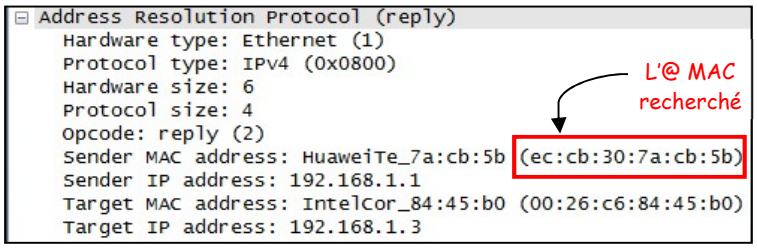
Sélectionner la trame n°7261 et cliquer sur [+] de « Adresse Resolution Protocol » dans la zone (2). Les champs suivants s'affichent :

- « Hardware Type » et « Protocol Type » : qui indiquent que la carte réseau dont on cherche son @ physique est une carte Ethernet, et on dispose de son adresse logique qui est une @IP.
- « Hardware size » et « Protocol size » : définissent la taille de l'@ physique (matériel) et celle logique (protocole) sur 6 octets et 4 octets, respectivement.
- « Opcode » : contient la valeur (1) qui indique qu'il s'agit d'une requête.

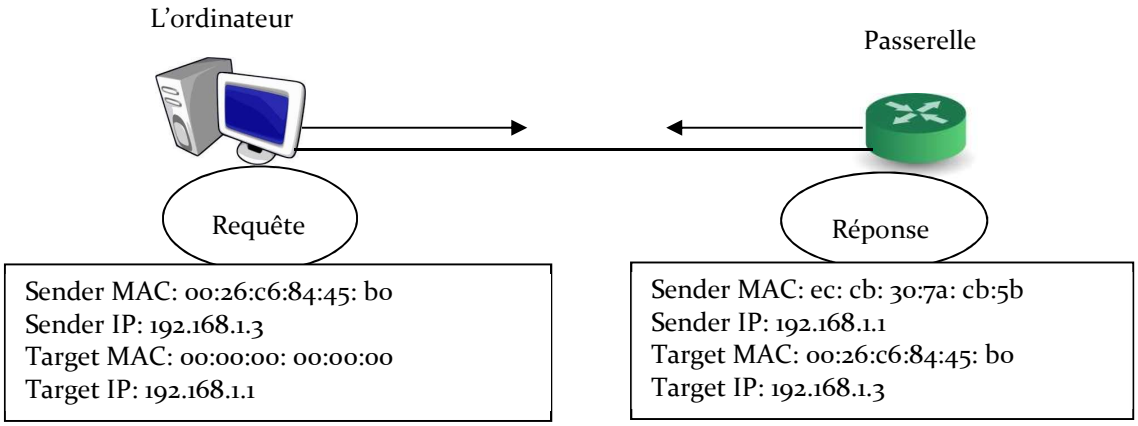
- « Sender MAC » « Sender IP » « Target MAC » et « Target IP » : définissent, respectivement, l'@ MAC (Ethernet) et IP de l'émetteur, et l'@ MAC et IP du destinataire.

Sélectionner la trame n°7262 et cliquer sur [+] de « Adresse Resolution Protocol », les champs qui changent de valeurs par rapport à la trame précédente sont :

- « Opcode » où il contient la valeur Reply (2) qui veut dire que c'est une trame de réponse.
- « Sender MAC » « Sender IP » « Target MAC » et « Target IP » : où leurs valeurs sont inversées (Sender devient Target et Target devient Sender) puisque le destinataire devient lui l'émetteur.



Dans le paquet de requête, l'émetteur connaît ses @ MAC et IP ainsi que l'adresse IP de la cible (c'est l'adresse IP pour laquelle on cherche l'@ MAC), donc il les remplit. L'@ MAC cible n'est pas connue, pour cela il met 00 : 00 : 00 : 00 : 00 :00. Cette adresse sera remplie par l'expéditeur une fois il reçoit la demande ARP.



3.4 TRAVAIL DEMANDE

3.4.1 Trame Ethernet

Capturez un trafic réseau comme suit : lancez une capture Wireshark, ensuite chargez une page web (ex. Google) via votre navigateur. Arrêtez la capture après un moment.

1. Donnez le n° d'un paquet contenant un message GET de HTTP.
2. Quelle est l'adresse de destination dans ce paquet ? Est-ce l'adresse Ethernet de votre ordinateur ?
3. Donnez le n° d'un paquet contenant un message OK de HTTP.
4. Est-ce l'adresse du serveur web hébergeant la page web demandée ? Expliquez.
5. Quelle est l'adresse de broadcast Ethernet ? Donnez le numéro d'une trame de diffusion Ethernet ?
6. Quel champ dans l'en-tête Ethernet permettant de déterminer à quel protocole de la couche supérieure la trame est destinée ?
7. Donner les exemples (n° du paquet capturé) pour des paquets destinés aux protocoles : IP, ARP. Quelle est la valeur de ce champ dans les deux cas ?

8. Pour paquet HTTP combien d'octets depuis le début de la trame Ethernet jusqu'au début du message HTTP ?

3.4.2 Paquet ARP

Dans cette partie, on essaie de faire en sorte que la machine utilise le protocole ARP pour découvrir l'adresse MAC du routeur local (la passerelle). Ensuite on analyse le trafic capturé.

1. Quelle est l'adresse IP de la passerelle ?
2. L'@IP de la passerelle existe-elle dans e cash ARP ?
3. Effacer l'@IP de la passerelle de la cache ARP.
4. Lancer une capture en utilisant Wireshark, et utilise le navigateur web pour charger une page web. Une fois le trafic ARP est capturé, arrêter la capture.
5. Filtre les paquets capturés pour n'afficher que les paquets ARP de votre machine (utiliser l'@MAC de votre machine).
6. Donnez le n° d'un paquet ARP demande ?
7. Quel est le n° de son paquet ARP réponse ?
8. Dans le fenêtre de capture, comment différencier les deux paquets ?
9. Quelle est la valeur du champ « Opcode » pour chacun des deux paquets ?
10. Quelle est la taille de l'en-tête ARP pour une demande ? Qu'en est-il d'une réponse ?
11. Combien d'octets depuis le début de la trame Ethernet jusqu'au champ « Opcode » du paquet ARP ?
12. Quelle est l'adresse MAC cible pour le paquet ARP demande ?
13. Quel champ qui désigne quel est le protocole de la couche 3 qui utilise ARP ? quelle est sa valeur pour le cas du paquet demande ?
14. La réponse ARP est-elle diffusée ou non ? pourquoi ?
15. Compléter le schéma suivant par les informations des deux paquets ARP :