

Département de génie informatique et génie logiciel

INF3405

Réseaux Informatiques

Hiver 2019

Rapport du TP2 : Projet en réseaux informatiques

Gestionnaire de fichier

Soumis à Émilie Dion-Paquin

Julien Legault 1847125

Abdellah Rahmani 1965352

Le 28 mars 2019

**INTRODUCTION :**

**6.1 Exécutez la commande ipconfig /all et Inscrivez le nom de votre poste, l’adresse IPv4, le masque de sous-réseau, l’adresse MAC, la passerelle par défaut pour vos deux systèmes virtuels.**

Poste : L4708-12

**Windows7\_A**

Adresse IPv4 : 192.168.79.139

Masque du sous-réseau = 255.255.255.0

Adresse MAC : 00-0C-29-6E-CA-D4

Passerelle par défaut : 192.168.79.2

**Windows7\_B**

Adresse IPv4 : 192.168.79.140

Masque du sous-réseau = 255.255.255.0

Adresse MAC : 00-0C-29-8E-E7-12

Passerelle par défaut : 192.168.79.2

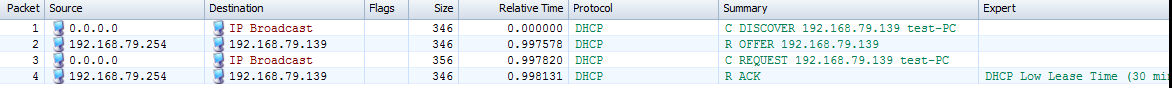
**8. Partie DHCP (Dynamic Host Configuration Protocol)**

Les réseaux réaffectent généralement les adresses correctes aux périphériques lors de leur première connexion. Dans des conditions normales, un périphérique peut continuer à utiliser une adresse IP indéfiniment, toutefois, des problèmes liés au DHCP et au matériel réseau peuvent entraîner des conflits IP, ce qui necessite d’actualiser l’adresse IP en utilisant les commandes «ipconfig/release» et « ipconfig/renew » .

La commande «ipconfig/release» permet de libérer l’adresses IP.

La commande « ipconfig /renew » ordonne au client DHCP de redemander une adresse IP au serveur DHCP du routeur. Après le renouvellement, Windows peut recevoir la même adresse IP qu’avant, ce qui est normal car l’effet recherché consiste à rompre l’ancienne connexion et à en démarrer une nouvelle indépendement des numéros d’adresse impliqués

**8.1- Mécanisme d’attribution d’une nouvelle adresse IP à un client qui veut se joindre à un réseau :**



L’attribution d’une nouvelle adresse IP se fait à travers un échage de messages entre le client DHCP et le serveur DHCP comme suit :

1- Le client DHCP envoie au serveur DHCP un message « découverte/recherche » (DHCP discover) afin de découvrir les serveurs DHCP et de les aviser du besoin de paramètres TCP/IP.

2-Un ou plusieurs serveurs DHCP ayant reçu le message « découverte » réponderont par un message « offre DHCP » (DHCP offer) afin de proposer les paramètres TCP/IP au client.

3- Ensuite, le client envoie à l’un des serveurs DHCP (un seul) un message  «Requete DHCP » (DHCP request) par lequel il accepte sa proposition et refuse automatiquement les offres des autres serveurs afin qu’ils puissent relacher les adresses IP qu’ils lui auraient reservé.

4- Finalement, le serveur DHCP répond par un message « Acceptation /confirmation  DHCP» (DHCP Acknowlegde) contenant les parametres TCP/IP.

**Client DHCP**

**Serveur DHCP**

**DHCP Discover**

**DHCP Request**

**DHCP Offer**

**Client Acknowledge**

**8.2 Donnez la séquence d’encapsulation des protocoles utilisés pour le paquet DHCP DISCOVER. Présentez une capture d’écran du contenu du paquet DHCP DISCOVER.**

Les paquets DHCP discover utilisent l’encapsulation suivante :

Adresse physique du client DHCP : 00 :0C :29 :6E :CA :D4

Adresse physique de diffusion : FF :FF :FF :FF :FF :FF

Ethernet

IP

Adresse IP source (neutre) : 0.0.0.0

Adresse IP de destination (de diffusion) : 255.255.255.255

Port source : 68

Port de destination : 67

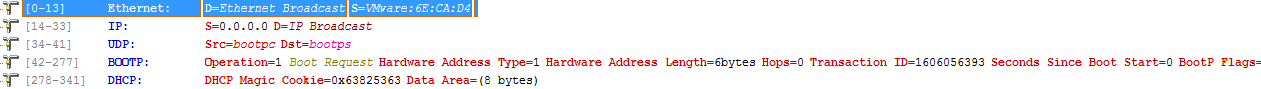
UDP

Transaction ID

Adresse physique du client DHCP : 00 :0C :29 :6E :CA :D4

Bootp

Message DHCP Discover

****

**8.3 En se basant sur vos observations en 8.1, quelles opérations DHCP se sont effectuées en broadcast? Selon vous, pourquoi certaines de ces opérations doivent absolument être faites en broadcast?**

A partir de la capture effectuée en 8.1, Les deux opérations ayant été effectuées en broadcast sont « Discover » et « Reequest ».

L’opération « Discover » est toujours effectuée en mode broadcast afin de repérer tous les serveurs DHCP disponibles. De mème, L’opération « Request » est toujours effectuée en mode braodcast afin de permettre aux serveurs DHCP -pour lesquels l’offre est refusée – de relacher l’adresse IP qu’ils ont reservé au client : le message « DHCP Request » contient les identifiants du serveur pour lequel l’offre est aceptée, ce dernier reçoit ce message et reconnait ses identifiants, il répond alors par un « Acknowledgment », tandis que tous les autres serveurs, voient que les identifiants ne leurs correspondant pas, ils relachent alors l’adresse IP qu’il ont reservé pour le client.

Les opérations «Offer » et « Acknowledgment » peuvent etre soi en broadcast ou bien en unicast.

**8.4 Serait-il possible d’utiliser le protocole TCP de la couche 4 pour toutes requêtes DHCP? Si oui, dites comment, sinon pourquoi est-il impossible d’utiliser TCP pour les requêtes DHCP?**

Il n’est pas possible d’utiliser le protocole TCP de la couche 4 pour les requêtes DHCP, car DHCP utilise un service sans connexion se basant sur UDP. Le port UDP 67 est le port de destination du serveur, et le port 68 est utilisé par le client. Ces deux ports sont les mêmes pour le protocole Bootp

**Trame DHCP OFFER :**

**8.5 Quel est le rôle de la trame DHCP offer ?**

La trame DHCP offer permet d’informer le client DHCP des différents serveurs DHCP disponibles.

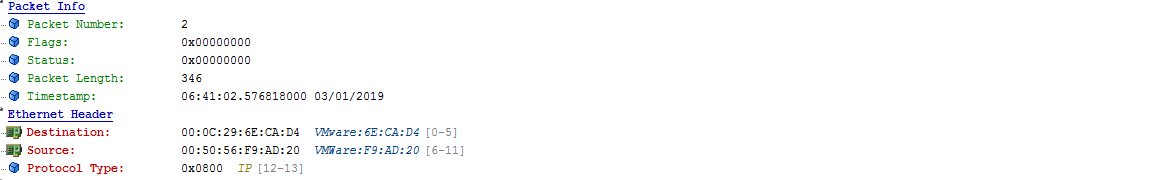
**8.6 Quel champ, dans le paquet, indique que ce message est un DHCP offer ? Spécifiez le champ et sa valeur.**

Le champ qui indique qu’il s’agit d’un message offer est « Message type »  et a « 2 » pour valeur :

DHCP - Dynamic Host Configuration Protocol 🡪 Message Type🡪Message Type:2 Offer [284]



**8.7 À quel poste correspond l’adresse MAC dans le champ Destination de l’entête Ethernet? Et celui du champ Source?**



-L’adresse MAC dans le champ « Destination » correspond à la machine virtuelle du client DHCP.

-L’adresse MAC dans le champ « Source » correspond à la machine du serveur DHCP (la vrai machine : celle du lab ? ).

**8.8 À quelle machine appartient l’adresse IP source?**

-L’adresse IP « Source » correspond à la machine du serveur DHCP (la vrai machine : celle du lab ? ).

**8.9 Quelle est la taille de l’entête Ethernet que vous observez?**

La taille de l’entête Ethernet observée est de 14 bytes (6 bytes pour l’adresse MAC de destination, 6 bytes pour l’adresse MAC source, et 2 bytes pour le champ « Protocol type ».)

**8.10 Quelle est la valeur du champ Protocole Type et que signifie-t-elle ?**

La valeur des champs « Protocol type » en hexadécimal est : 0x0800

cette valeur représente le type (Ethertype), elle détermine le protocole utilisé au niveau 3 : protocole IP dans notre cas.

**8.11 Dans l’entête DHCP, quelle est la signification du champ IP Address Lease Time ?**

IP Address Lease Time est la durée de bail DHCP : c’est la durée en minutes ou en secondes pendant laquelle un périphérique réseau peut utiliser une adresse IP sur un réseau. L'adresse IP est réservée à ce périphérique jusqu'à l'expiration de la réservation.

**8.12 Que désigne le champ Client IP Addr Given By Srvr? Quelle est l’utilité de ce champ?**

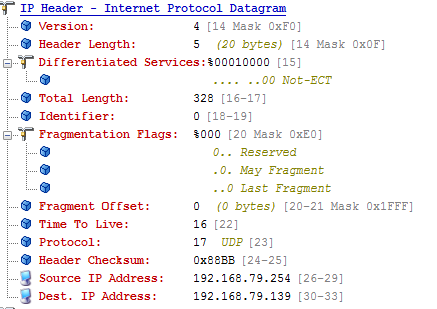
C’est l’adresse IP que propose le serveur DHCP au client comme « offre » suite à un message Discover broadcast, elle permet de renouveler le bail du client.

**8.13 Quelle est l’entête suivante de la trame (niveau 3 du modèle OSI) ?**

L’entête du niveau 3 du modèle OSI correspond à l’entête IP

**8.14 Quelle est la taille de l’entête de niveau 3 du modèle OSI que vous observez?**

La taille de l’entête IP est de 20 bytes :



**8.15 Nommez le protocole de niveau supérieur (niveau 4 du modèle OSI) utilisé par DHCP.**

Le protocole de niveau 4 du modèle OSI utilisé par DHCP est le « User Datagram Protocol » UDP.

**8.16 Quelle est la taille de l’entête de niveau 4 du modèle OSI que vous observez?**

L’entête du protocole UDP est d’une longueur de 8 bytes.

2 bytes pour chacun des champs : Port source, port destination, le champs length, et UDP checksum

**8.17 Dans combien de temps la machine Windows 7 doit-elle revalider avec le serveur DHCP son adresse IP?**

A partir de la question 8.11 ; la valeur du champ IP Address Lease Time est de 1800 minutes, la machine Windows devra donc revalider son adresse IP dans 30 heures.

**9. Partie ARP (Address Résolution Protocol)**

Le protocole de résolution d'adresse (ARP) est un protocole de communication utilisé pour découvrir l'adresse de la couche liaison, telle qu'une adresse MAC, associée à une adresse de couche réseau donnée, généralement une adresse IPv4.

**9.1 Quelle est l’utilité de la cache ARP?**

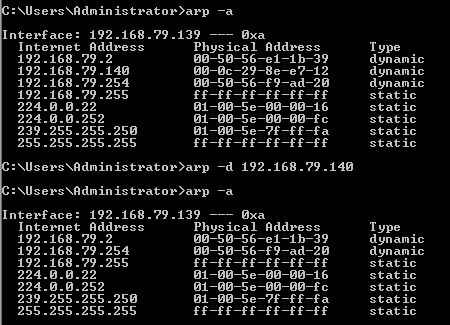
Un ordinateur A souhaitant émettre une trame Ethernet à un ordinateur B du même sous réseau dont il connaît l’adresse IP, effectuera une requête ARP en broadcast : « quelle adresse physique est associée à cette adresse IP ». Toutes les machines du sous réseau vont recevoir la requête, mais seule la machine B qui possède cette adresse IP répondra en envoyant à la machine A une réponse ARP indiquant l’adresse MAC qui lui est associée. Ensuite, la machine A crée une entrée dans son cache ARP à partir des données contenues dans la requête ARP qu’elle vient de recevoir, cette entrée lui permettra de transmettre les paquets à la bonne machine.

La cache ARP est une table qui maintient la correspondance entre les adresses IP et les adresses MAC d'un réseau local, elle sert à éviter de refaire une requête ARP à chaque paquet IP à émettre. Ses entrées sont effacées apres un certain temps de non utilisation.

La commande « arp –a » permet d’afficher son contenu.

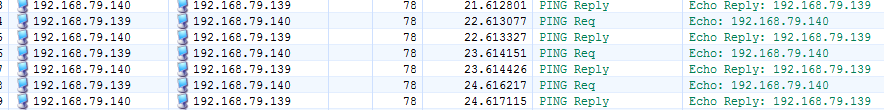
**9.2 Dans votre client Windows7\_A, et dans une fenêtre de commande (DOS), exécutez la commande arp –a qui permet d’afficher le contenu de votre cache ARP ? Si l’adresse de Windows7\_B y apparaît, enlevez-la avec la commande arp –d 192.168.xx.xxx. Vérifiez qu’elle n’y est plus.**

**Démarrez l’analyseur de protocole.**



**9.3 Lancez une commande qui permet de vérifier votre connectivité avec Windows7\_B. Arrêtez l’analyseur de protocole et sauvegardez la capture réalisée. Lancez à nouveau la commande arp -a. Que remarquez-vous ?**

Apres avoir lancé la commande « ping » qui permet une connexion avec la machine Windows7\_B, puis exécuté la commande « arp –a », nous voyons bien que le couple adresse IP –adresse MAC de la machine Windows7\_B réapparait à nouveau dans la table ARP de la machine Windows7\_A.



Paquets capturés de la commande Ping entre les machine A et B

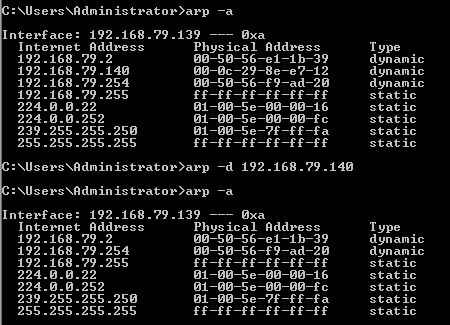
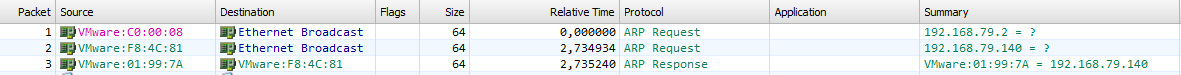


Table ARP de la machine A mise à jour

Après avoir lancé la commande « ping  IP Windows\_B», la machine Windows7\_A met en attente les paquets qu’elle devrait transmettre à la machine B, pendant ce temps, elle a effectué une requête ARP en broadcast afin d’obtenir l’adresse MAC correspondant à l’adresse IP de la machine B, cette dernière répond par un message « ARP response » fournissant son adresse MAC, la machine Windows7\_A peut donc mettre à jour sa table ARP et commencer à transmettre les paquets vers la machine Windows7\_B. A la fin de cette transmission, si aucun paquet n’est échangé avec la machine B, son entrée (couple IP-MAC) sera supprimée de la table ARP de la machine Wiindows7\_A.



ARP request et ARP response entre les machines A et B

PS : cette figure a été prise d’une capture effectuée sur une machine différente du laboratoire

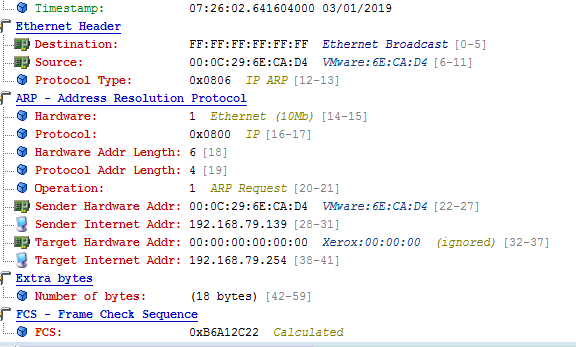
**9.4 Dans l’analyseur de protocole, quelle est la longueur (size) des trames ARP ?**

La longueur des trames ARP est de 64 bytes

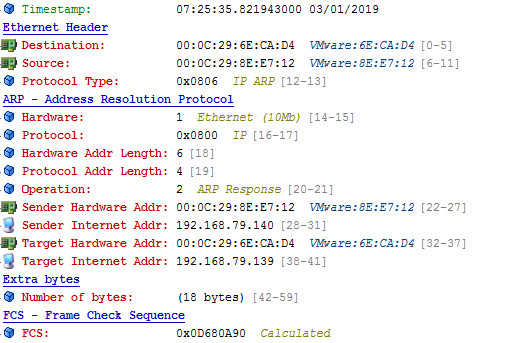
**9.5 Quelle est la valeur numérique du champ Protocol type de l’en-tête Ethernet (Ethertype) d'une trame ARP ? Que signifie-t-elle ?**

Ce champ indique quel est le protocole de niveau supérieur utilisé dans le champ "donnée", dans notre cas, il est d’une valeur hexadécimale égale à **0x0806** , cette valeur correspond à **Address Resolution Protocol (ARP).**

**9.6 En se basant sur le contenu d’un paquet ARP Request et ARP Response, qu’est-ce qui différencie une requête ARP d’une réponse ARP dans le protocole ARP ?**



**ARP Request**

****

**ARP Response**

C’est le champ « Operation » de l’entête ARP qui permet de différencier entre les deux, dans le cas d’un « ARP Request » il est égal à 1, et dans le cas d’un « ARP Response » il est égal à 2.

**9.7 À quel noeud réseau correspond l’adresse MAC de la source de la réponse ARP?**

L’adresse MAC source de la réponse ARP correspond à la machine Wndows7\_B

**9.8 À quel noeud réseau correspond l’adresse MAC de la destination de la réponse ARP?**

L’adresse MAC destination de la réponse ARP correspond à la machine Wndows7\_A

**9.9 Quelle est la séquence d’encapsulation d’une requête ARP ?**

Un paquet ARP est encapsulé dans un paquet Ethernet comme suit :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ethernet | | | | |
| Adresse MAC de destination (6 bytes)  FF :FF :FF :FF :FF :FF | Adresse MAC source  (6 bytes)  00 :0C :29 :6E :CA :D4 | Type  (2bytes)  0x0806 | ARP | CRC (4bytes) |
| Paquet ARP request |

**9.10 Quel champ de la réponse ARP possède l’information recherchée par la requête ARP lancée par un client d’un réseau?**

L’information recherchée (adresse MAC de la machine Windows7\_B) se trouve dans le champs « Sender Hardware Addr » :  00 :0C :29 : 8E :E7 :12

**9.11 Qu’est-ce qu’il y a de particulier à la fin des données d’une trame ARP juste avant le champ FCS (CRC de 32 bits) ? Quel pourcentage de la taille de la trame ce champ occupe-t-il? Pourquoi ce champ est-il nécessaire dans les requêtes ARP?**

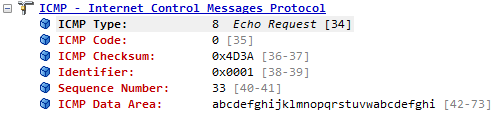
**là je ne suis pas sùr si l’on devrait parler de CRC ou de Timestamp !!**

A la fin des données d’une trame ARP, on trouve le champ CRC (cyclic redundancy check) qui est un outil permettant de détecter les erreurs de transmission. Il occupe 6,25 % de la taille de la trame.

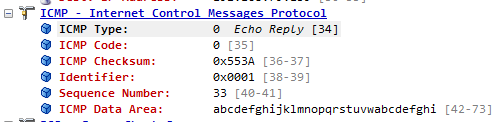
On trouve aussi le champ « Timestamp » indiquant la validité de la durée de vie d'un paquet, il sert à tracer les fausses entrées ARP et à éviter la génération de plusieurs demandes ARP. Il occupe 12,5 % de la taille de la trame.

**10. Partie PING**

**10.1 Quel est le champ ICMP qui différencie les requêtes par rapport aux réponses PING et quelles sont les valeurs impliquées ?**



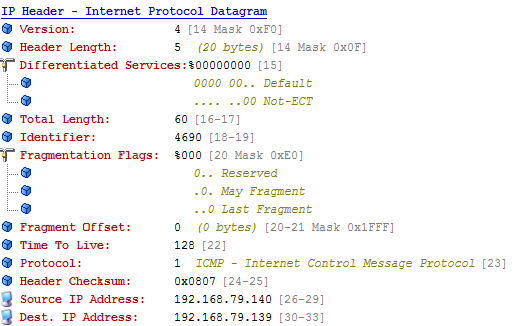
**ICMP Request**



**ICMP Reply**

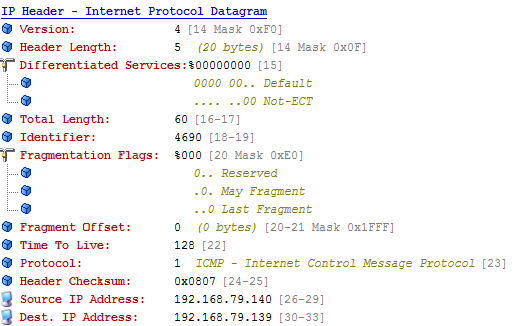
Le champ qui différencie les requêtes des réponses est « ICMP Type », il prend la valeur 8 pour une requête, et la valeur 0 pour une réponse.

**10.2 Quelle est la version du protocole IP utilisée ?**



C’est la version 4 du protocole IP qui est utilisée : IPv4

**10.3 Quelle est la valeur du champ TTL (Time To Live). À quoi sert ce champ ?**

****

La valeur du champ TTL est de 128. Ce champ indique le nombre maximal de routeurs de transit. Il est codé sur huit bits, ce qui permet de spécifier des valeurs initiales (par le système d’exploitation) allant de 1 à 255. Quand un routeur de transit arrive à la valeur 0 après avoir décrémenté ce champ, le paquet est détruit et un paquet « ICMP 11 Time Exceeded » est envoyé vers la source afin d’éviter –en cas d’un problème de routage- qu'un paquet boucle à l'infini.

**10.4 Quelle est la séquence d’encapsulation d'une trame PING ?**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Trame Ethernet | | | | | | | |
| MAC destination 6 bytes | MAC source 6 bytes | Protocol Type  2 bytes | Paquet IP | | | | |
| … | IP source | IP  destination | Paquet ICMP | |
| Control data | ICMP data |

**CONCLUSION :**