Institut Universitaire de Technologie
Aix*Marseille Université

Réseaux & Télécoms

TP Analyse de protocole

ETUDE DU PROTOCOLE IP

1. Liminaire

Chaque question en gras correspond à une question sur le relevé numérique de TP intitulé `Questionnaire Analyse Protocole IP` et disponible sur AMETICE

Ce relevé est noté et comptera comme un bonus.

Quelle est l'adresse mac de votre machine ?

Quelle est l'adresse ip de votre machine ?

Quel est le masque de réseau en notation /n?

Quelle est l'adresse ip de votre passerelle ?

Faites maintenant un ping sur votre passerelle, puis tapez la commande `arp -a`

Quelle est l'adresse mac de la passerelle ?

2. Envoi d'un paquet et étude du protocole ARP

En observant l'affichage précédent, indiquez si les adresses IP et MAC de la machine de votre voisin sont présentes dans le cache ARP ?

Lancez votre capture de trames avec Wireshark, puis sur la ligne de commande exécuter la commande `ping avec l'adresse IP de votre voisin`.
Revenez sur Wireshark et arrêtez la capture des trames.
Enfin, revenez dans la fenêtre DOS et tapez la commande `arp -a`.

Les adresses IP et MAC de la machine de votre voisin sont-elles présentes dans le cache ARP ?

En étudiant la capture de trames :

Y a t-il eu une requête arp avant le premier `echo-request` envoyé ?
A quelle @MAC de destination est envoyée votre requete ARP ?
Est-ce que toutes les requêtes ARP de la capture de trame vous appartiennent ? Pourquoi ?

Y a t-il eu une requête arp vous appartenant avant le second `echo-request` envoyé ? Pourquoi ?

Lancez une nouvelle capture de trames avec Wireshark, puis sur la ligne de commande exécuter la commande `ping 139.124.88.129`. Une fois la commande terminée, revenez sur Wireshark et arrêtez la capture des trames.

Dans la trame envoyée et contenant l'`echo-request`, quelle était l'adresse MAC de destination ?
Pourquoi ?

3. Trafic IP

Lancez une capture de trames. Depuis la fenêtre DOS, lancez la commande `telnet 139.124.88.129` (le username est `tpreseau1a`, et le password est `tpreseau1a`). Une fois connecté sur la machine, tapez la commande `ls`, puis la commande `exit`. Arrêtez alors la capture.

En observant la première trame du protocole telnet, répondez aux questions suivantes :

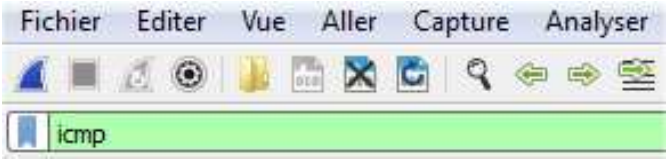
Dans la trame :
Quelle est la valeur du champ `type` dans la trame Ethernet ?
A quel protocole de la couche réseau cette valeur correspond-t-elle ?

Dans le paquet IP :
Quelle est la valeur du champ `TTL` ?
A quoi sert ce champ et comment évolue sa valeur ?
Quelle est sa valeur maximum ?

Quelle est la valeur du champ `Protocol` ?
A quoi sert ce champ ?
A quel protocole de la couche transport cette valeur correspond t-elle ?

4. Traceroute

Lancez une capture de trames en filtrant les message ICMP.

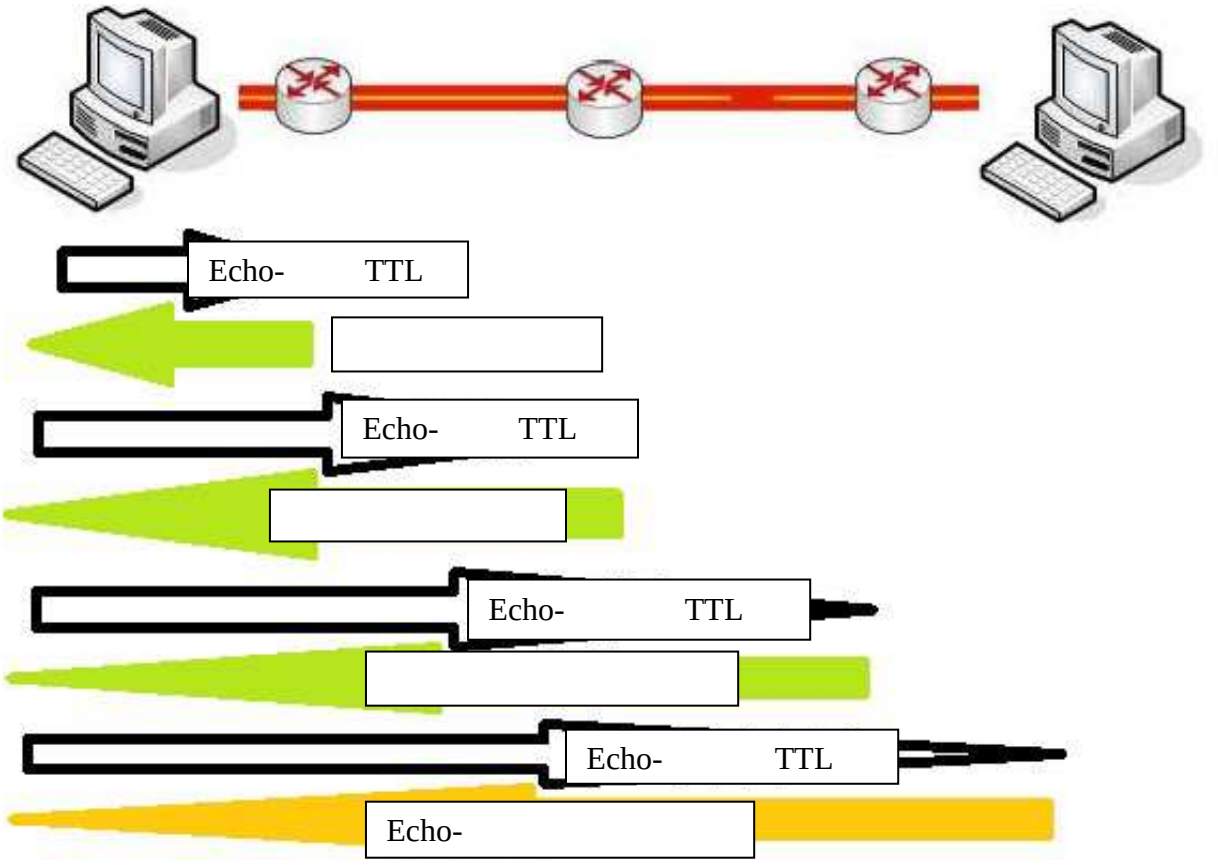


Lancez la commande `tracert www.yahoo.fr`. Une fois trouvée la route pour atteindre le serveur `yahoo`, arrêtez la capture.

Dans quel champ de l'entête IP retrouve-t-on le fait que `tracert` utilise ICMP ?
Quel type de message ICMP envoyez-vous au serveur ?
Quel type de message ICMP renvoient les routeurs intermédiaires?
Quel type de message ICMP le serveur renvoie-t-il à la fin ?

En regardant chaque fois le premier paquet des trois paquets de type `echo request` qui sont envoyés, déterminer comment la valeur du champ TTL évolue ?

Complétez le schéma suivant en indiquant le type des messages icmp et si besoin la valeur du TTL



5. La totale !!!

Récupérez sur l'ENT le fichier `latotale.cap` qui est la capture d'un ping à partir de la machine du prof vers `www.google.fr`.
Info utile : le masque de réseau utilisé par votre PC est /24

Le serveur DNS est-il dans le même réseau que la machine du prof ?

La passerelle est-elle dans le même réseau que la machine du prof ?

La machine hébergeant le site www.google.fr est-elle dans le même réseau que la machine du prof ?

Complétez le tableau suivant :

	Adresse MAC	Adresse IP
Serveur DNS		
Passerelle		
Machine du prof		
Machine hébergeant google		

En étudiant le premier message ICMP, complétez le tableau suivant

	Source	Destination
Adresse MAC		
Adresse IP		

A quoi sert la première requête ARP ?

A quoi sert la deuxième requête ARP ?

Complétez le texte suivant :

La machine du prof veut vérifier que la machine hébergeant le site ..... est bien accessible via le réseau.

Pour cela, elle a besoin de l'adresse …….. de la machine hébergeant ce site et doit donc contacter le serveur .....

Pour contacter ce serveur qui est dans le même réseau, elle doit lui envoyer une requête encapsulée un datagramme ....., lui-même encapsulé dans un paquet ....., lui-même encapsulé dans une trame ..... Elle connaît l'adresse ..... du DNS, et ses propres adresses MAC et IP. Elle doit donc obtenir l'adresse ..... du DNS

Pour cela, elle envoie une requête ARP avec une adresse de destination en ……. de niveau 2. C'est la première requête ARP.

Le serveur DNS, dans sa réponse ARP, lui donne son adresse .....

La machine du prof peut maintenant interroger le DNS, qui en réponse lui donne l'adresse ..... du site à atteindre.

La machine du prof doit maintenant envoyer un echo ..... sur la machine hébergeant le site à atteindre et dont l'adresse IP est .....

Cette machine n'étant pas dans son réseau, il faut envoyer ce message ICMP à la …….

Pour cela, il faut encapsuler le message ICMP dans un paquet ....., lui-même encapsulé dans une trame ..... La machine du prof connaît l'adresse ..... de la passerelle, et ses propres adresses MAC et IP. Elle doit donc obtenir l'adresse…….. de ……..

Pour cela, elle envoie une requête ARP avec une adresse de destination en …… de niveau 2. C'est la seconde requête ARP. La passerelle, dans sa réponse ARP, lui donne son adresse ..... La machine du prof peut maintenant envoyer son message echo ..... et attendre la réponse sous la forme d'un echo .....