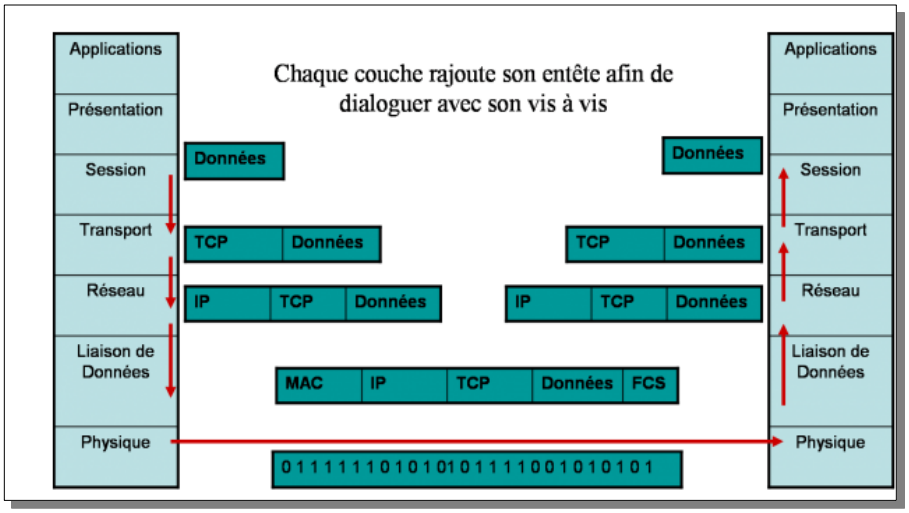
Objectifs

- Utiliser quelques commandes de base systèmes et réseaux
- Utiliser l'analyseur de trafic réseau « Wireshark »
- Analyser les données et flux résultants des protocoles (ARP, ICMP……)

I/ Les modèles OSI et TCP/IP



TCP/IP est un modèle comprenant 4 couches :

Couche	Nom	Description
4	Application	Couches 7 à 5 du modèle OSI
3	Transport	Qualité de transmission
2	Internet	Sélection du chemin
1	Accès au réseau	Reprend les couches 1 et 2 du modèle OS

II/ Comparaison entre OSI et TCP/IP

Ces deux modèles sont très similaires, dans la mesure où les 2 sont des modèles de communication à couche et utilisent l'encapsulation de données. On remarque cependant deux différences majeures :

- TCP/IP regroupe certaines couches du modèle OSI
- TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau Internet actuel

III/ Capture et analyse de trames associées à la commande ping

Wireshark est un analyseur de protocoles (analyseur de paquets) utilisé pour dépanner les réseaux, effectuer des analyses, développer des logiciels et des protocoles et s'informer. Un analyseur de paquets (ou analyseur de réseaux ou de protocoles) est un logiciel permettant d'intercepter et de consigner le trafic des données transférées sur un réseau de données. Une capture réseau est comme une photo à un instant t de ce qui transite sur un réseau informatique.

IV/ Découvrir Wireshark

Pour pouvoir capturer des données, vous devez d'abord vous connecter au réseau depuis l'ordinateur sur lequel Wireshark est installé et exécuter Wireshark.

Question n°1

Relevez l'adresse Ip de votre PC, l'adresse de la passerelle et la noter.

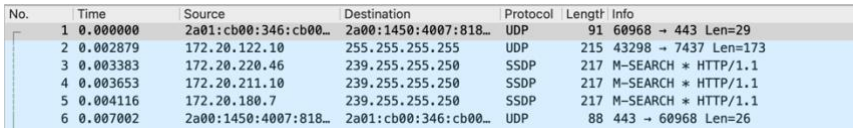
Question n°2

Lancer Wireshark et sélectionner l'interface de votre connexion réseau.

Vous devez obtenir un résultat similaire à celui-ci-dessous composé de 3 fenêtres

Fenêtre 1 :

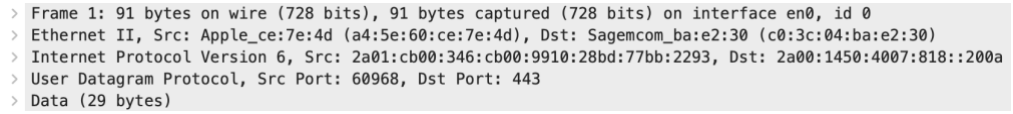
La liste des paquets capturés disponibles en dessous de la barre de menu avec un affichage synthétique du contenu des paquets



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2a01:cb00:346:cb00…	2a00:1450:4007:818…	UDP	91	60968 → 443 Len=29
2	0.002879	172.20.122.10	255.255.255.255	UDP	215	43298 → 7437 Len=173
3	0.003383	172.20.220.46	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4	0.003653	172.20.211.10	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5	0.004116	172.20.180.7	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
6	0.007002	2a00:1450:4007:818…	2a01:cb00:346:cb00…	UDP	88	443 → 60968 Len=26

Fenêtre 2 :

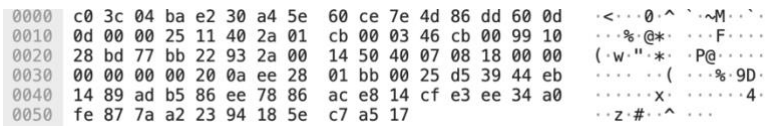
La décomposition exacte du paquet actuellement sélectionné dans la liste. Cette décomposition permet de visualiser les champs des en tête des protocoles ainsi que l'imbrication des différentes couches de protocoles connus.



```
> Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ce:7e:4d (a4:5e:60:ce:7e:4d), Dst: Sagemcom_ba:e2:30 (c0:3c:04:ba:e2:30)
> Internet Protocol Version 6, Src: 2a01:cb00:346:cb00:9910:28bd:77bb:2293, Dst: 2a00:1450:4007:818::200a
> User Datagram Protocol, Src Port: 60968, Dst Port: 443
> Data (29 bytes)
```

Fenêtre 3 :

Cette zone contient la capture affichée en hexadécimal et en ASCII.



```
0000  c0 3c 04 ba e2 30 a4 5e  60 ce 7e 4d 86 dd 60 0d   ·<···0·^ `·~M··`·
0010  0d 00 00 25 11 40 2a 01  cb 00 03 46 cb 00 99 10   ···%·@*· ···F····
0020  28 bd 77 bb 22 93 2a 00  14 50 40 07 08 18 00 00   (·w·"·*· ·P@·····
0030  00 00 00 00 20 0a ee 28  01 bb 00 25 d5 39 44 eb   ···· ··( ···%·9D·
0040  14 89 ad b5 86 ee 78 86  ac e8 14 cf e3 ee 34 a0   ·····x· ·····4·
0050  fe 87 7a a2 23 94 18 5e  c7 a5 17                  ··z·#··^ ···
```

Le trafic sur un réseau étant très important, il est nécessaire de mette en place des filtres, c'est-à-dire sélectionner les communications destinées uniquement à votre carte, ou bien encore sélectionner un type de protocole.

Question n°3

Repérez les différentes colonnes de la fenêtre 1, indiquez le type de contenu affiché dans ces différentes colonnes.

Question n°4

Effectuer une recherche de façon à définir les termes : trame Ethernet et protocole Ethernet (citez vos sources)

Question n°5

Donner le format d'une trame Ethernet, citez les différents champs.

La carte réseau voit passer beaucoup de trafic, il est parfois difficile de repérer les trames qui nous intéressent, d'où la nécessité d'ajouter des filtres. Wireshark permet de mettre en place des filtres pour isoler uniquerment les trames qui nous intéressent, on peut filtrer par adresse ou par protocole.

Question n°6

Expliquer la différence entre filtre de capture et filtre d'affichage au niveau de Wireshark.

Question n°7

Quel filtre faut-il utiliser pour afficher seulement les trames :

- à destination de votre PC ?
- qui partent de votre PC ?
- qui partent de votre PC et à destination de votre PC ?

Question n°8

Lancer la console et exécuter la commande permettant de vider la table arp de votre poste puis taper : ping 172.20.120.254.

Question n°9

Stopper la capture Wireshark lorsque l'invite de commande réapparait à la console, sauvegarder le fichier sous le nom capture1ping et effectuer une capture d'écran du résultat.

Ne pas hésiter à consulter les annexes situées en pages 6, 7 et 8 pour répondre aux différentes questions qui suivent.

Question n°10

Quels sont les protocoles indiqués lors d'une commande ping ?

Etude du paquet IP correspondant au premier message ARP Request

Caractéristiques Ethernet :

Question n°11

Que transporte la trame Ethernet ?

Question n°12

Quelle est l'adresse Mac source de la trame Ethernet ?

Question n°13

Quelle est l'adresse Mac destination trame Ethernet ?

Caractéristiques ARP Request

Question n°14

Quelle est la taille du préambule ? Quelle est la taille des données transportées ?

Question n°15

Quelle est la valeur du champ Protocol Type contenu dans le message ARP ?

Question n°16

Quelle est l'adresse IP source du paquet ARP ?

Question n°17

Quelle est l'adresse IP destination du paquet ?

Question n°18

Quelle est l'adresse Mac source incluse dans le message ARP ?

Question n°19

Quelle est l'adresse Mac destination incluse dans le message ARP ?

Analyse du message ICMP

Caractéristiques Ethernet :

Question n°20

Quelle est l'adresse Mac source de la trame Ethernet ?

Question n°21

Quelle est l'adresse MAC destination trame Ethernet ?

Sélectionner les octets de données du message de requête message ICMP « Echo Request »

Question n°22

Quelle est la taille de l'en tête ? Quelle est la taille des données transportées ?

Question n°23

Quel est le type du message ICMP ?

Question n°24

Quel est son identificateur ?

Question n°25

Quel est le numéro de séquence ?

Question n°26

Quelle est la valeur du champ Protocol type ?

Question n°27

Quelle est la valeur du champ Time to Live ?

V/ Capture et analyse associée à la commande tracert

Lancer Wireshark

Lancer une console et taper la commande tracert www.cisco.com

Arrêter la capture lorsque l'invite de commande réapparait à la console puis sauvegarder le fichier sous le nom « capture2traceroute », effectuez aussi une capture d'écran des résultats dans la console

Question n°28

Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ?

Il est probable que les paquets ICMP soient précédés d'un jeu de questions/réponses DNS, UDP, ICMP.

Question n°29

Relever l'adresse IP renvoyée avec la réponse DNS. @I associée à www.cisco.com

Question n°30

Quelle est l'adresse IP destination du premier paquet contenant le message UDP ?

Question n°31

Quelles sont les valeurs des champs Protocol Type et Time to Live ?

Question n°32

Comparer l'adresse IP destination relevée avec celle de la réponse DNS.

(Noter les valeurs caractéristiques de l'en-tête IP en vue d'une utilisation ultérieure)

Question n°33

Combien d'octets de données sont présents dans ce message de requête ?

Question n°34

Quelles sont les @ IP source et destination du paquet de la première réponse ICMP Time Exceeded ?

Question n°35

Quel est le type de message ICMP ? (Les champs Type, message ICMP Echo Request.) Comparer les valeurs caractéristiques de cet en-tête avec celles notées ci-avant.

Question n°36

Est-ce que le message ICMP contient de nouveaux octets de données ?

Question n°37

Combien de messages UDP sont émis avec la même valeur de champ TTL dans l'en-tête de paquet IP ?

Question n°38

Quelles sont les adresses IP source des paquets ICMP Time Exceeded ?

Question n°39

Comparer ces adresses avec celles données lors de l'exécution de la commande traceroute.

Question n°40

Quel est le type du message ICMP reçu lorsque l'hôte destinataire est atteint ?

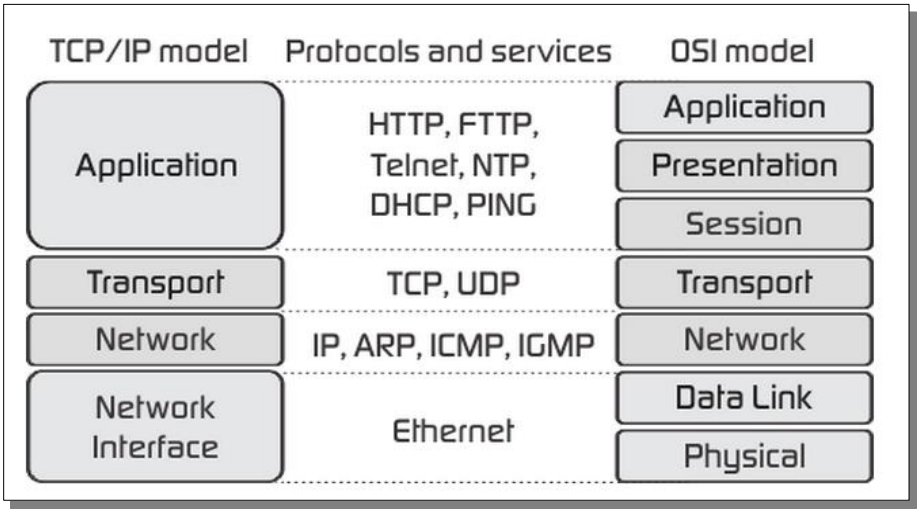
Question n°41

Comment calculer les temps affichés par la commande tracert à partir des valeurs données dans la colonne Time de la fenêtre des trames capturées ?

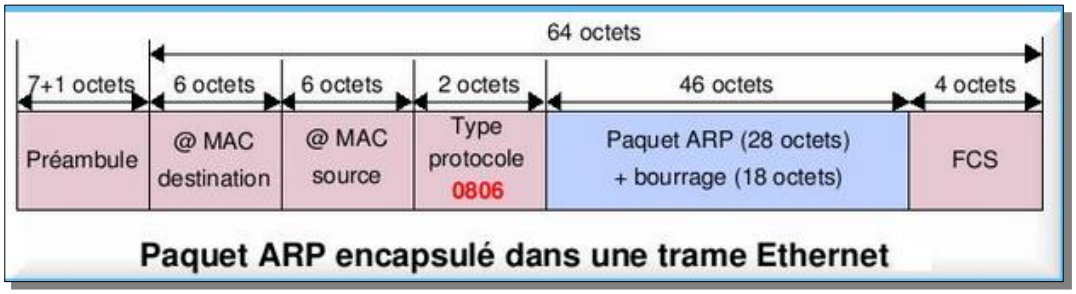
Remarque : faire une recherche sur la commande tracert pour obtenir la signification des différentes valeurs de temps pour atteindre une destination.

Annexes :

Commande ping et protocoles associés, encapsulation de données :

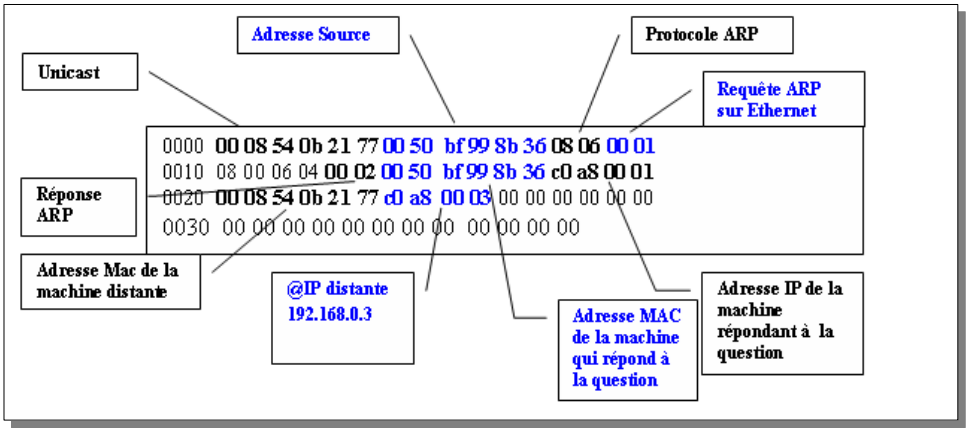


Trame Ethernet et ARP



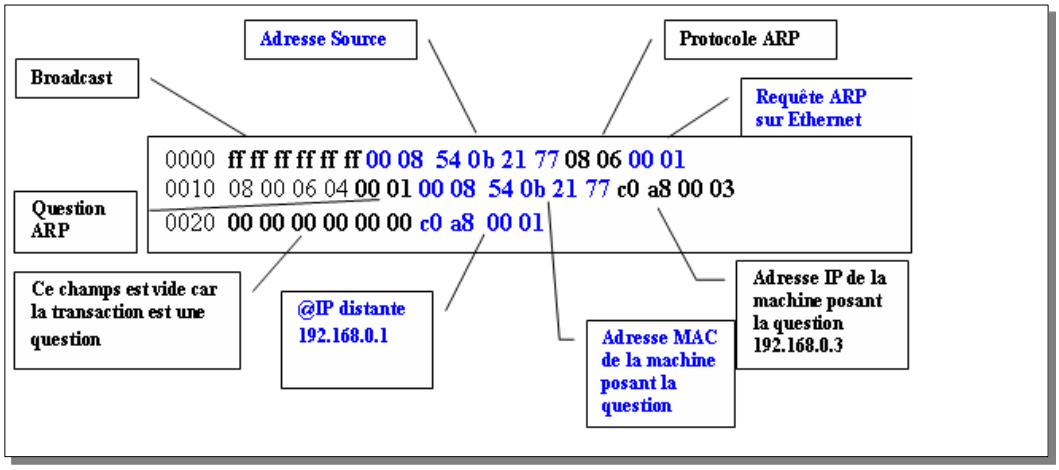
Arp request :

La question de type Arp Request se présente sous cette forme : « Je suis l'hôte « 00 08 54 0b 21 77», Est-ce que l'hôte possédant l'adresse Ip 192.168.0.1 peut me retourner son adresse physique ? ». Voici la traduction de cette requête saisie grâce à Wireshark.



ARP Reply :

L'hôte destinataire qui va se reconnaître va pouvoir d'un coté alimenter sa table de conversion et répondre à l'hôte source en envoyant une trame comportant son adresse physique. Voici la traduction de cette réponse saisie grâce à Wireshark.



Le protocole ICMP

Ping s'appuie sur le protocole ICMP, permettant de diagnostiquer les conditions de transmissions. Il utilise ainsi deux types de messages du protocole (sur les 18 proposés par ICMP) :

- Le type 0 correspondant à une commande "echo request", émis par la machine source ;
- Le type 8 correspondant à une commande "echo reply", émis par la machine destinataire

A intervalles réguliers (par défaut chaque seconde), la machine source (celle sur laquelle la commande ping est exécutée) envoie une commande "echo request" à la machine cible. Dès réception du paquet "echo reply", la machine source affiche une ligne contenant un certain nombre d'informations. En cas de non réception de la réponse, une ligne indiquant "délai dépassé" s'affichera.

exemple :

ECHORequest & ECHOReply sont utilisées pour voir si une destination est accessible et fonctionne. A la réception d'un message ECHORequest, le destinataire doit répondre par un message ECHOReply.