

TD2 : Séquence communication sur un modèle client/serveur

Lors d'une communication entre un client et un serveur, des trames contenant les données utiles circulent sur le réseau.

Cette activité a pour objectif d'analyser le contenu le séquençement des trames transmises.



Protocole ICMP

Une commande ping est une commande bas niveau qui permet de vérifier la disponibilité d'une machine distante. Cette commande s'exécute sur la console d'un ordinateur en spécifiant l'adresse IP du destinataire que l'on souhaite vérifier.

La **commande ping émise** depuis un client d'adresse 192.168.1.201 à destination d'un serveur d'adresse 192.168.1.11 a reçu **les réponses suivantes** :

```
desktop ~ $ ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.530 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.502 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.515 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=64 time=0.524 ms
```

La tableau suivant contient la copie d'une trame de 98 octets envoyée lors du ping depuis un hôte source vers un hôte de destination. Cette trame a été récupérée grâce au logiciel Wireshark lancé sur le client. :

```
0000 b8 27 eb a0 9a 17 00 e0 6f 2c 4a b1 08 00 45 00
0010 00 54 00 00 40 00 40 01 b6 20 c0 a8 01 c9 c0 a8
0020 01 6f 08 00 ef e1 0f 6c 00 01 46 10 2f 5e 00 00
0030 00 00 b9 6f 0b 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
0060 36 37
```

Analyse de la trame émise

1- A partir de la description des entêtes des différents protocoles mis en jeu, **compléter** les tableaux suivants en indiquant les valeurs hexadécimales correspondantes :

x Décodage de l'entête Ethernet

Adresse MAC source	Adresse MAC destination	Type de trame

x Décodage de l'entête IP

Version du protocole IP	Longueur de la trame	Valeur du TTL	Protocole utilisé	Adresse IP source	Adresse IP destination

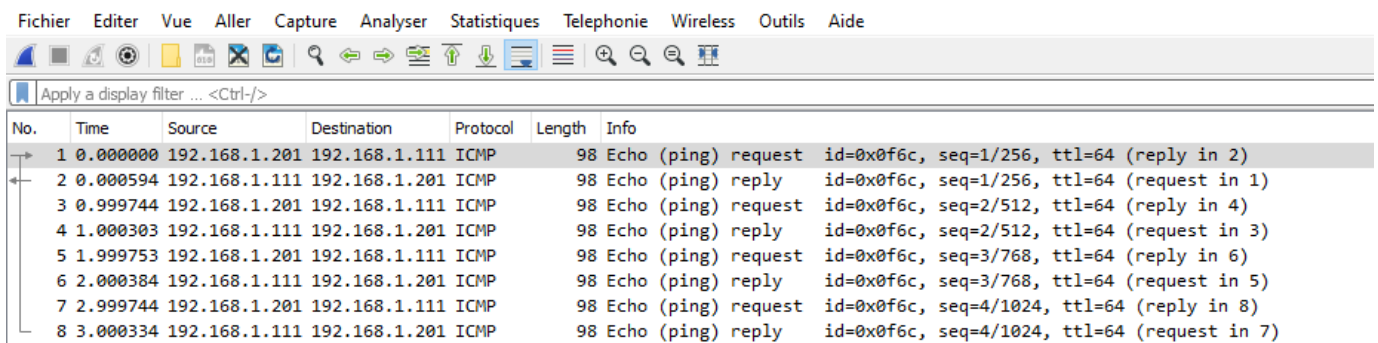
x Décodage de l'entête ICMP

Type	Code	Identifiant	Numéro de séquence

Remarque : Les octets restants sont les données transmises.

Analyse de la capture par Wireshark

2- **Indiquer** à quelle ligne de la capture d'écran Wireshark correspond la trame analysée précédemment.



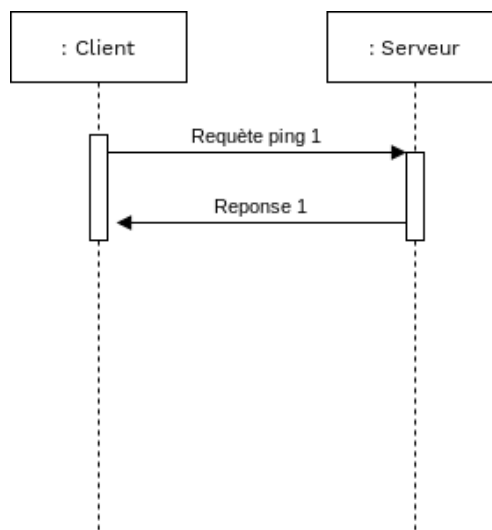
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.201	192.168.1.111	ICMP	98	Echo (ping) request id=0xf6c, seq=1/256, ttl=64 (reply in 2)
2	0.000594	192.168.1.111	192.168.1.201	ICMP	98	Echo (ping) reply id=0xf6c, seq=1/256, ttl=64 (request in 1)
3	0.999744	192.168.1.201	192.168.1.111	ICMP	98	Echo (ping) request id=0xf6c, seq=2/512, ttl=64 (reply in 4)
4	1.000303	192.168.1.111	192.168.1.201	ICMP	98	Echo (ping) reply id=0xf6c, seq=2/512, ttl=64 (request in 3)
5	1.999753	192.168.1.201	192.168.1.111	ICMP	98	Echo (ping) request id=0xf6c, seq=3/768, ttl=64 (reply in 6)
6	2.000384	192.168.1.111	192.168.1.201	ICMP	98	Echo (ping) reply id=0xf6c, seq=3/768, ttl=64 (request in 5)
7	2.999744	192.168.1.201	192.168.1.111	ICMP	98	Echo (ping) request id=0xf6c, seq=4/1024, ttl=64 (reply in 8)
8	3.000334	192.168.1.111	192.168.1.201	ICMP	98	Echo (ping) reply id=0xf6c, seq=4/1024, ttl=64 (request in 7)

Figure 1: Relevé Wireshark du ping

3- **Ouvrir** le fichier **PING.PCAP** avec Wireshark et **vérifier** l'ensemble des réponses précédentes.

Chronologie de la communication

4- **Compléter** avec des flèches, le diagramme de séquence suivant afin de représenter la capture des trames figure 1



De la même manière, une capture a été réalisée lors de l'accès d'un poste client vers un poste serveur (nano ordinateur Raspberry Pi) hébergeant un site web.

Pour obtenir cette page web, l'utilisateur entre classiquement l'adresse web sur son navigateur et appuie sur entrée. Les trames situées après la trame numéro 8 correspondent aux échanges entre le client et le serveur après que l'utilisateur ait appuyé sur la touche entrée.



5- **Ouvrir** le fichier **HTTP.PCAP** dans Wireshark

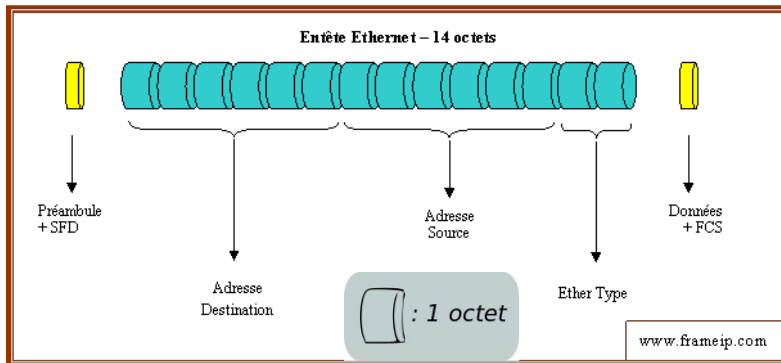
6- **Indiquer** les deux types de protocoles que l'on y rencontre et leur fonction.

7- **Indiquer** les adresses IP et MAC de la machine qui héberge le site et celles de la machine sur laquelle le navigateur a été lancé.

8- **Préciser** le nombre d'éléments qui compose le site web auquel le navigateur accède.

Composition des entêtes des protocoles utilisés par la commande PING

Détail de l'entête du protocole Ethernet



Préambule et SFD : Non relevés → permet de synchroniser l'envoi et de démarrer la trame

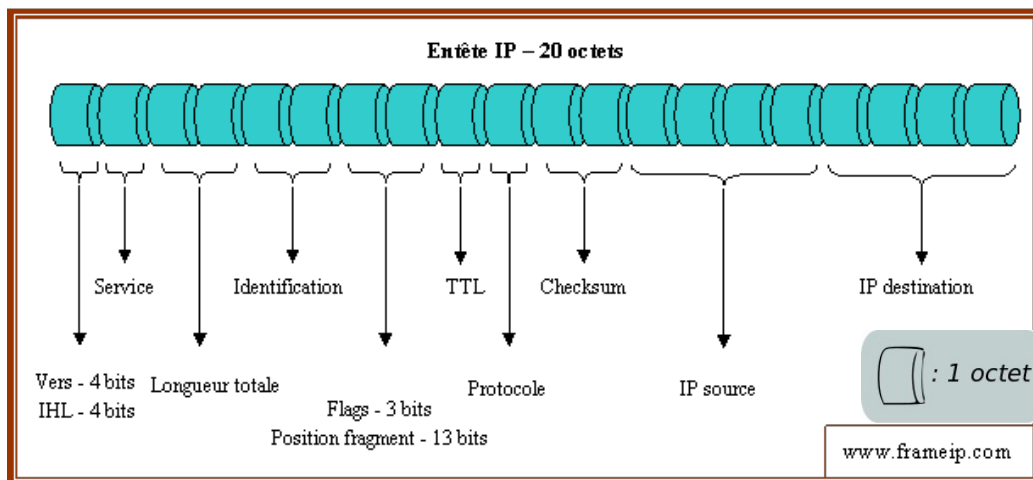
Adresse destination : 6 octets représentant l'adresse MAC du destinataire

Adresse source : 6 octets représentant l'adresse MAC de la source

Ether Type : 2 octets indiquant le type de protocole inséré dans le champ donnée :

0x6000 : DEC / 0x0609 : DEC / 0x0600 : XNS / 0x0800 : IPv4 / 0x0806 : ARP /
0x8019 : Domain / 0x8035 : RARP / 0x809B : AppleTalk / 0x8100 : 802.1Q / 0x86DD :
IPv6

Détail de l'entête du protocole IP



Détail de l'entête du protocole ICMP

