Table des matières

Fiche pédagogique:

Objectifs pédagogiques	2.2 Architecture fonctionnelle d'un système communicant
Connaissances visées	Modèle en couche des réseaux, protocoles et encapsulation des données Adresse physique (Mac) du protocole Ethernet et adresse logique (IP) du protocole IP
Prérequis	• Activité_IPConfig • Codage ASCII • Adresse logique (IP) • Masque de sous réseau • DHCP, DNS • Topologie d'un réseau Ethernet • Savoir faire une copie d'écran partielle (impécr + mspaint)
Matériel	• Un PC
Logiciel	• wireshark
Évaluation	• QCM
Remarques	• Travailler sur le document numérique (copies partielles d'écran)

1 Ping

La commande ping permet de tester la présence sur le réseau d'une machine dont on connait l'adresse IP ou le nom (host Name), Elle permet également d'avoir une idée de la rapidité de communication avec cette machine.

🗋 Après avoir ouvert la fenêtre cmd.exe (voir activité ipcconfig) lancer dans cette fenêtre la commande:

`ping  10.139.54.199` (*adresse IP du PC video projecteur)*

observation:

remplacer cette copie d'écran par la copie de votre écran

```
C:\>ping 192.168.0.5

Envoi d'une requête 'Ping'  192.168.0.5 avec 32 octets de données :
Réponse de 192.168.0.5 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.5 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.5 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.5 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

🗋 Tester le commande: ping "*adresse mac du PC video projecteur*"

conclusion:

🗋 Tester le commande: ping 184XP (nom du PC video projecteur de la salle 205)

conclusion:

La commande ping fonctionne également avec l' adresse internet d'une machine en dehors du réseau:

🗋 Tester la commande: **`ping  sti2d.free.fr`**

remplacer cette copie d'écran par la copie de votre écran

```
C:\>ping sti2d.free.fr

Envoi d'une requête 'ping' sur perso169-g5.free.fr [212.27.63.169] avec 32 octets de données :
Réponse de 212.27.63.169 : octets=32 temps=66 ms TTL=59
Réponse de 212.27.63.169 : octets=32 temps=69 ms TTL=59
Réponse de 212.27.63.169 : octets=32 temps=65 ms TTL=59
Réponse de 212.27.63.169 : octets=32 temps=66 ms TTL=59

Statistiques Ping pour 212.27.63.169:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 65ms, Maximum = 69ms, Moyenne = 66ms
```

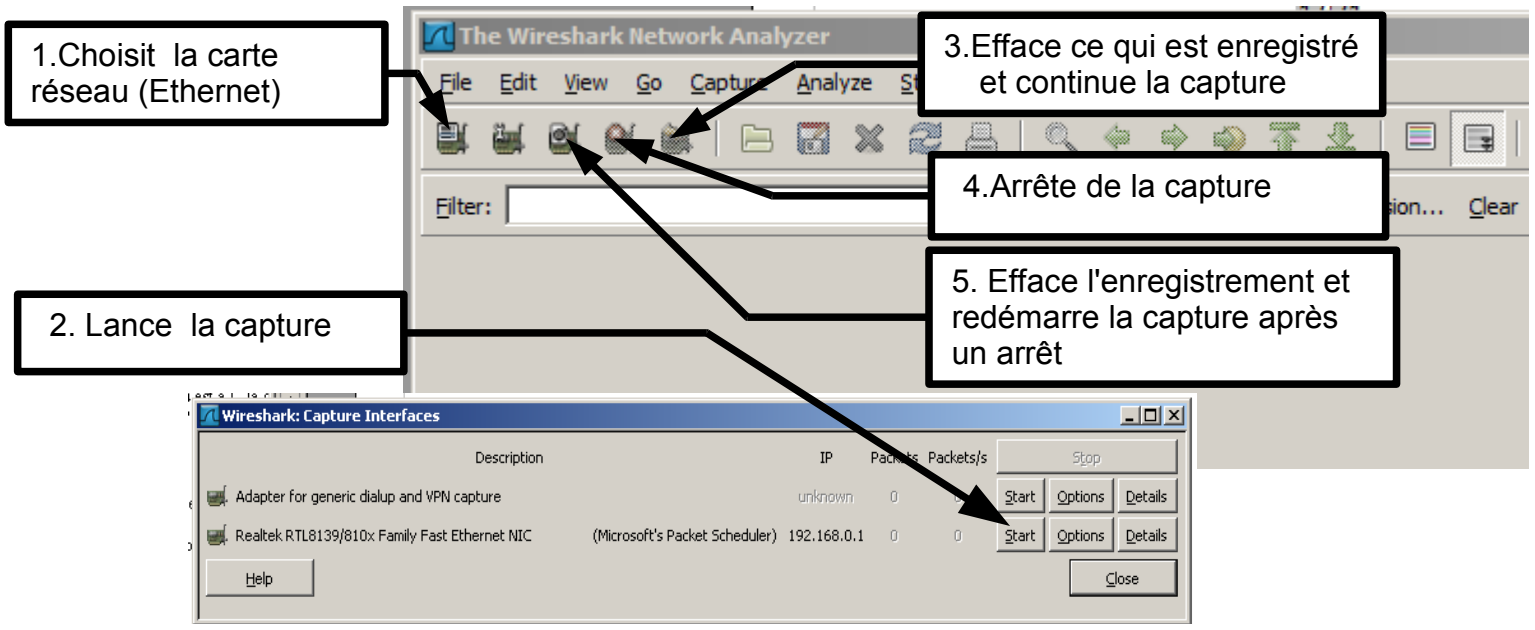
🗋 Comparer les durées moyennes des ping pour le PC videoprojecteur et pour la machine qui héberge le site "sti2d.free.fr et conclure

2 Utilisation de Wireshark

Wireshark est un logiciel qui permet d'enregistrer et d'analyser les informations qui circulent sur le câble réseau relier à un PC.

2.1 Enregistrement des trames

🗋 Pour lancer Wireshark, cliquer sur l'icône:  . La fenêtre suivante apparaît:



On se propose d'enregistrer les informations circulant pendant l'exécution de la commande: **`ping 10.139.54.199`**

Pour cela il faut:

- ouvrir une fenêtre cmd.exe et écrire la commande **`ping 10.139.54.199` sans la valider avec la touche entrée.**
- ouvrir wireshark
- organiser les fenêtres de façon à les voir toutes les deux
- lancer la capture dans la fenêtre wireshark (1 et 2)
- revenir dans la fenêtre cmd.exe et valider la commande avec la touche entrée
- retourner dans la fenêtre wireshark et arrêter la capture dès que la commande ping est terminée (4)
- enregistrer la capture dans le dossier Mes documents sous le nom: ping_video.pcap

observation:

remplacer cette copie partielle d'écran par la copie partielle de votre écran

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.5	192.168.0.255	BROWSER	Browser Election Request
2	0.788179	192.168.0.5	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
3	1.000119	192.168.0.5	192.168.0.255	BROWSER	Browser Election Request
4	1.695335	00:26:2d:af:d2:ac	Broadcast	ARP	Who has 192.168.0.5? Tell 192.168.0.6
5	1.695683	QuantaCo_e9:41:3b	00:26:2d:af:d2:ac	ARP	192.168.0.5 is at 00:1e:68:e9:41:3b
6	1.695704	192.168.0.6	192.168.0.5	ICMP	Echo (ping) request
7	1.695874	192.168.0.5	192.168.0.6	ICMP	Echo (ping) reply
8	1.999765	192.168.0.5	192.168.0.255	NBNS	Registration NB ESMOULINS<1d>
9	2.707243	192.168.0.6	192.168.0.5	ICMP	Echo (ping) request
10	2.707656	192.168.0.5	192.168.0.6	ICMP	Echo (ping) reply
11	2.749692	192.168.0.5	192.168.0.255	NBNS	Registration NB ESMOULINS<1d>
12	3.394012	fe80::3d6a:28d8:6e81:	ff02::c	SSDP	M-SEARCH * HTTP/1.1
13	3.499590	192.168.0.5	192.168.0.255	NBNS	Registration NB ESMOULINS<1d>
14	3.721172	192.168.0.6	192.168.0.5	ICMP	Echo (ping) request
15	3.721624	192.168.0.5	192.168.0.6	ICMP	Echo (ping) reply
16	3.788035	192.168.0.5	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
17	4.249612	192.168.0.5	192.168.0.255	NBNS	Registration NB ESMOULINS<1d>
18	4.735325	192.168.0.6	192.168.0.5	ICMP	Echo (ping) request
19	4.735718	192.168.0.5	192.168.0.6	ICMP	Echo (ping) reply
20	4.999607	192.168.0.5	192.168.0.255	NBNS	Registration NB <01><02>__MSBROWSE__<02><(
21	5.005225	192.168.0.5	239.255.255.250	SSDP	NOTIFY * HTTP/1.1

Chaque ligne correspond à un "paquet" d'informations appelé aussi une trame(Frame) ou datagramme. Parmi toutes ces trames certaines n'ont rien à voir avec la commande ping. Seules les trames dont le protocol est ICMP correspondent à l'exécution de cette commande (voir colonne Info).

Utilisation d'un filtre (Filter)

Pour ne conserver à l'écran que les trames ICMP:

- Taper **icmp** dans la fenêtre Filter: et cliquer sur Apply

observation: remplacer cette copie d'écran par la copie de votre écran

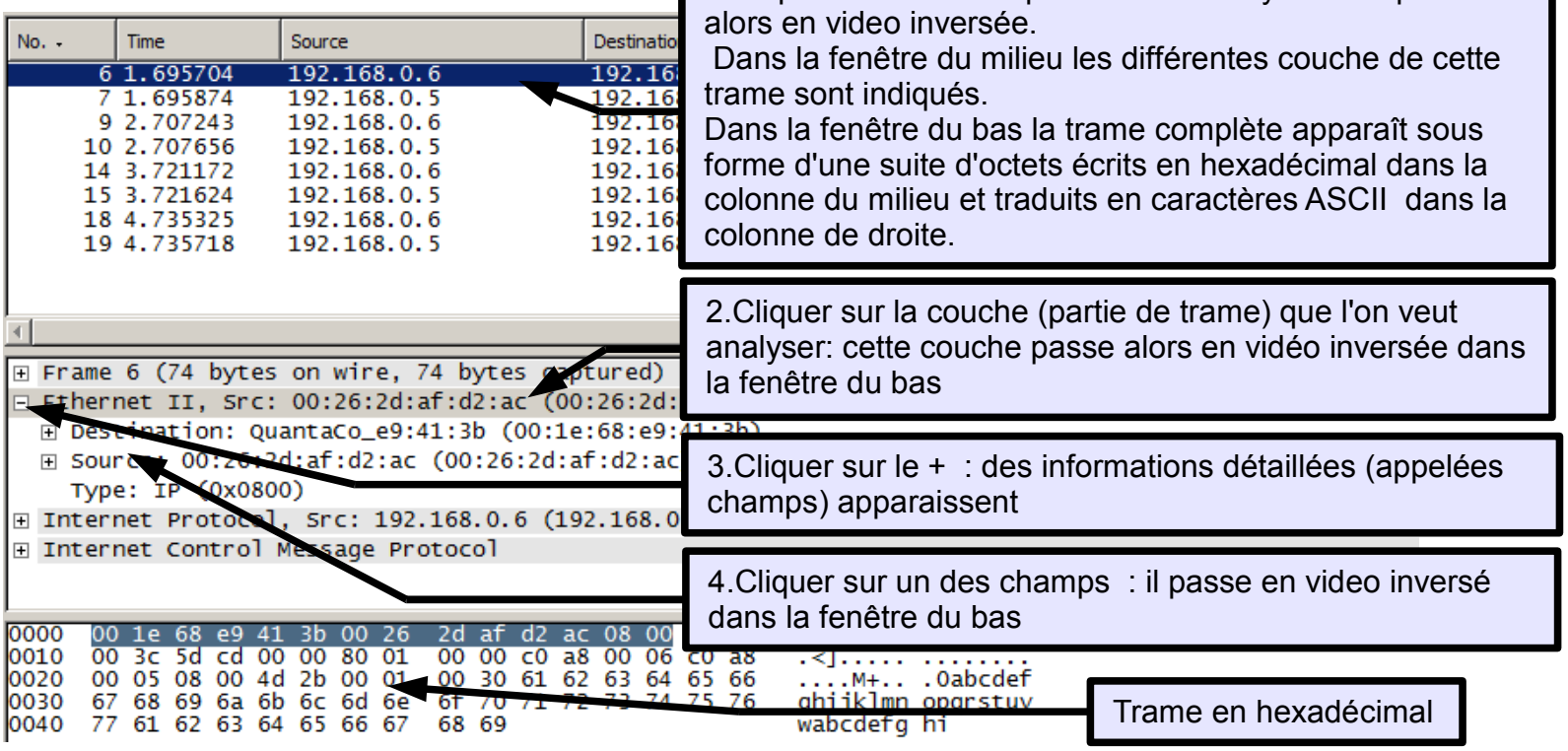
No.	Time	Source	Destination	Protocol	Info
6	1.695704	192.168.0.6	192.168.0.5	ICMP	Echo (ping) request
7	1.695874	192.168.0.5	192.168.0.6	ICMP	Echo (ping) reply
9	2.707243	192.168.0.6	192.168.0.5	ICMP	Echo (ping) request
10	2.707656	192.168.0.5	192.168.0.6	ICMP	Echo (ping) reply
14	3.721172	192.168.0.6	192.168.0.5	ICMP	Echo (ping) request
15	3.721624	192.168.0.5	192.168.0.6	ICMP	Echo (ping) reply
18	4.735325	192.168.0.6	192.168.0.5	ICMP	Echo (ping) request
19	4.735718	192.168.0.5	192.168.0.6	ICMP	Echo (ping) reply

Il ne reste que 8 trames correspondant à une alternance de requêtes (request) et de réponses (reply).

Les requêtes circulent du PC (source) dont l'adresse IP est: _____

au PC (destination) dont l'adresse IP est: _____

2.2 *Analyse d'une trame:*



Dans l'exemple ci dessus:

- la trame n°6 comporte 3 couches: la couche Ethernet, la couche Internet Protocol et la couche Internet Control Message Protocol
- La couche Ethernet de cette trame comporte elle même 3 champs:le champ Destination, le champ Source et le champ Type
- La couche Ethernet de la trame n°6 a été sélectionné; on remarque que cette couche comporte 14 octets:
  00 1e 68 e9 41 3b 00 26 2d af d2 ac 08 00

3 Couche Ethernet:

3.1 *structure*

🗅 A partir de la capture réalisée précédemment (ping_video.pcap), appliquer un filtre icmp et sélectionner la couche Ethernet de la deuxième trame (ping reply). Compléter alors le tableau suivant:

contenu														
champs	Adresse MAC destination						Adresse MAC source						Type*	

*Le champ Type définit la couche suivante: 08 00 = couche IP ; 08 06 = couche arp

🗅 Observer les autres trames: elle commencent toute par une couche de type Ethernet.

3.2 Rôle

La couche Ethernet permet aux trames de circuler sur le réseau.

Supposons que les machines d'un réseau sont reliées par un hub. Si une machine envoie une trame, celle ci arrive à toutes les autres machines. Le champ "Adresse MAC destination" de la couche Ethernet permet aux machines réceptrices de savoir si la trame leur est destinée.

Supposons maintenant que les machines d'un réseau sont reliées par un switch. Si une machine envoie une trame, celle ci arrive au switch. Le champ "Adresse MAC destination" de la couche ethernet permet au switch de savoir à qui la trame est destinée.

Ainsi dans tous les cas la trame arrive à son destinataire.

4 Couche Internet Protocol (IP):

4.1 structure

🗅 A partir de la capture réalisée précédemment (ping_video.pcap), appliquer un filtre icmp et sélectionner la couche IP de la deuxième trame (ping reply). Compléter alors le tableau suivant:

contenu												
champs	V	H	Serv.	Length		Identification		Offset		Time	Pro.	checksum

contenu								
champs	IP source				IP destination			

Signification des principaux champs:

- V: **Version** (1 quartet) il s'agit de la version du protocole IP que l'on utilise (actuellement on utilise la version 4)
- H: **Header lenght** (1 quartet), c'est le nombre de groupes de 4 octets constituant la couche IP (nota : la valeur par défaut est 5, soit 5*4octets=20octets).
- Serv: **Type de service** (1 octet)
- Lenght: **Longueur totale** (2 octets), indique la taille totale de la trame en octets (sans la couche Ethernet). La taille de ce champ étant de 2 octets, la taille totale d'une trame ne peut pas dépasser 65536 octets.
- Identification (2 octets)
- Offset (2 octets)
- Time: **Durée de vie** (1 octet) appelée aussi TTL, pour Time To Live. Ce champ indique le nombre maximal de routeurs à travers lesquels la trame peut passer. Ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit la trame. Cela évite l'encombrement du réseau.
- **Protocole** (1 octet) : ce champ, permet de savoir quel est le protocole de la couche suivante.
  exemples ICMP : 0x01 TCP : 0x06 UDP: 0x11
- Checksum**: Somme de contrôle** de l'en-tête,(2 octets) : ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de la trame.
- **Adresse IP source** (4 octets) : Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre
- **Adresse IP destination** (4 octets) : adresse IP du destinataire du message.

4.2 Rôle

La couche IP permet à une machine de dialoguer avec une autre machine qui n'est pas sur le même réseau.

Si une machine A envoie une trame à une machine B n'appartenant pas au même réseau, A envoie la trame à la passerelle, qui fait partie du réseau de A (Adresse MAC destination= passerelle) mais dans la couche IP l'adresse est l'IP de la machine B.

5 Couche ICMP (Internet Control Message Protocol)

5.1 structure

🗅 A partir de la capture réalisée précédemment (ping_video.pcap), appliquer un filtre icmp et sélectionner la couche ICMP de la première trame (ping requeqst).

🗅 Compléter le tableau en indiquant les noms et les nombres d'octets des 6 champs constituant cette couche:

nom du champ	Type	Code				
nombre d'octet	1					

- Observer les différentes trames et en déduire le rôle du champ Type.

- Observer les différentes trames et en déduire le rôle du champ Sequence number.

5.2 Modélisation SysML

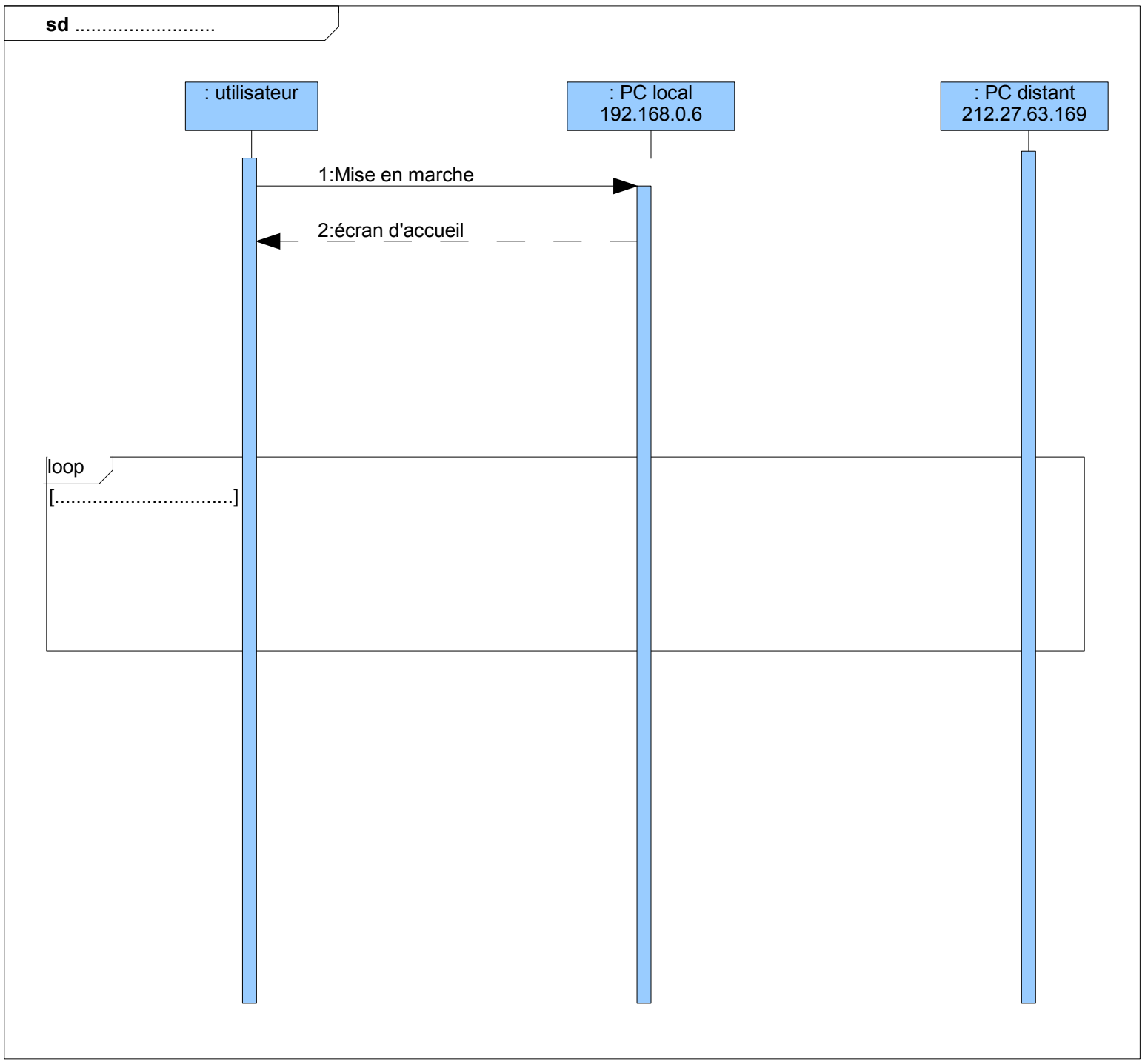
- Compléter le diagramme de séquence correspondant au cas d'utilisation "effectuer un ping"

```
C:\Windows\system32\cmd.exe

C:\>ping 212.27.63.169

Envoi d'une requête 'Ping'  212.27.63.169 avec 32 octets de données
Réponse de 212.27.63.169 : octets=32 temps=64 ms TTL=59
Réponse de 212.27.63.169 : octets=32 temps=66 ms TTL=59
Réponse de 212.27.63.169 : octets=32 temps=65 ms TTL=59
Réponse de 212.27.63.169 : octets=32 temps=66 ms TTL=59

Statistiques Ping pour 212.27.63.169:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 64ms, Maximum = 66ms, Moyenne = 65ms
```



6 Exercices:

a *QCM*

Ping fonctionne avec: □ une adresse IP □ une adresse MAC □l'adresse d'un site internet □ le nom d'une machine

Une trame est composée de plusieurs couches □vrai □faux

Une couche est composée de plusieurs trames □vrai □faux

Une couche est composée de plusieurs champs □vrai □faux

La première couche d'une trame est toujours □une couche IP □une couche Ethernet □une couche ARP

La couche qui permet la circulation des informations dans un réseau est: □la couche IP □la couche Ethernet

la couche qui permet la circulation des informations sur internet est: □la couche IP □la couche Ethernet

b *Analyse d'une trame*

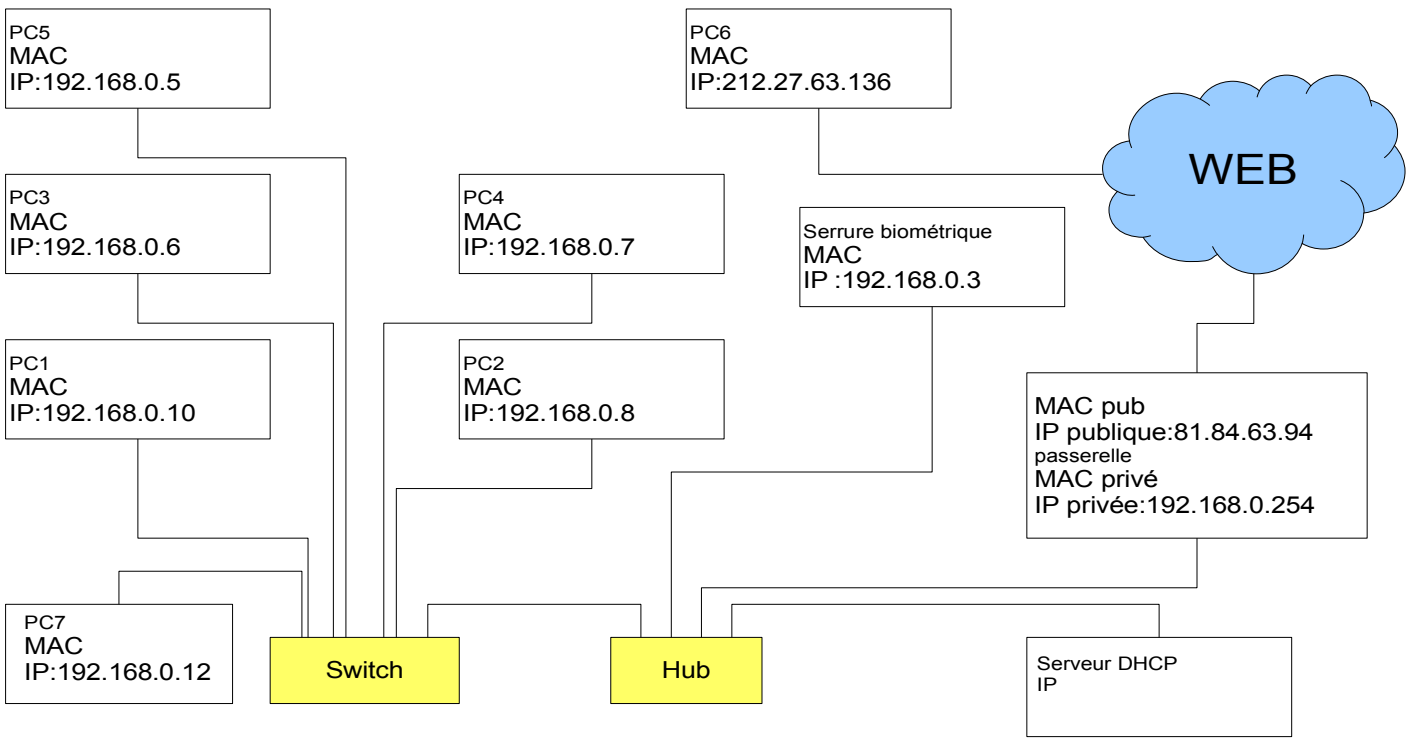
On a relevé la trame suivante (RT.pcap tramme5):

```
0000  00 26 2d af d2 ac 00 30  f9 01 b2 a0 08 00 45 00   .&-....0 ......E.
0010  00 28 3c 3b 40 00 40 06  7d 32 c0 a8 00 0c c0 a8   .(<;@.@. }2......
0020  00 06 00 50 c0 4f 87 05  bd 53 a4 13 60 39 50 10   ...P.O.. .S..`9P.
0030  02 e8 22 44 00 00 00 00  00 00 00 00              ..."D.... ....
```

- □ Encadrer et repérer la couche ethernet (colonne hexadécimal)
- □ Encadrer et repérer la couche la couche IP.
- □ Quel est le protocole de la couche suivante (non encadrée)?
- □ Compléter le tableau:

Adresse MAC source	
IP source (décimal)	
Adresse MAC destination	
IP destination (décimal)	

- □ Repérer la machine source et la machine destination sur le schéma suivant
- □ Compléter sur ce schéma les adresses MAC source et destination
- □ Colorier sur le schéma le chemin emprunté par la trame



c *Analyse d'une trame*

- Reprendre les questions précédentes avec la trame suivante (RT.pcap trame 21):

```
0000  00 26 2d af d2 ac 00 07  cb 18 45 c9 08 00 45 00   .&-..... ..E...E.
0010  00 28 7c c0 40 00 3b 06  ee bd d4 1b 3f 88 c0 a8   .(|.@.;. ....?...
0020  00 06 00 50 c0 51 0f c4  69 3d 34 e2 cd 84 50 10   ...P.Q.. i=4...P.
0030  00 36 9f 42 00 00 00 00  00 00 00 00              .6.B.... ....
```

- Encadrer et repérer la couche ethernet (colonne hexadécimal)
- Encadrer et repérer la couche la couche IP.
- Quel est le protocole de la couche suivante (non encadrée)?
- Compléter le tableau:

Adresse MAC source	
IP source (décimal)	
Adresse MAC destination	
IP destination (décimal)	

- Repérer la machine source et la machine destination sur le schéma suivant
- Compléter sur ce schéma les adresses MAC source et destination
- Colorier sur le schéma le chemin emprunté par la trame