

TP Ip

Q1: à quelle classe appartiennent les adresses Ip suivantes
195.83.207.xx

Q2: combien d'adresses d'ordinateurs possibles pour une classe A

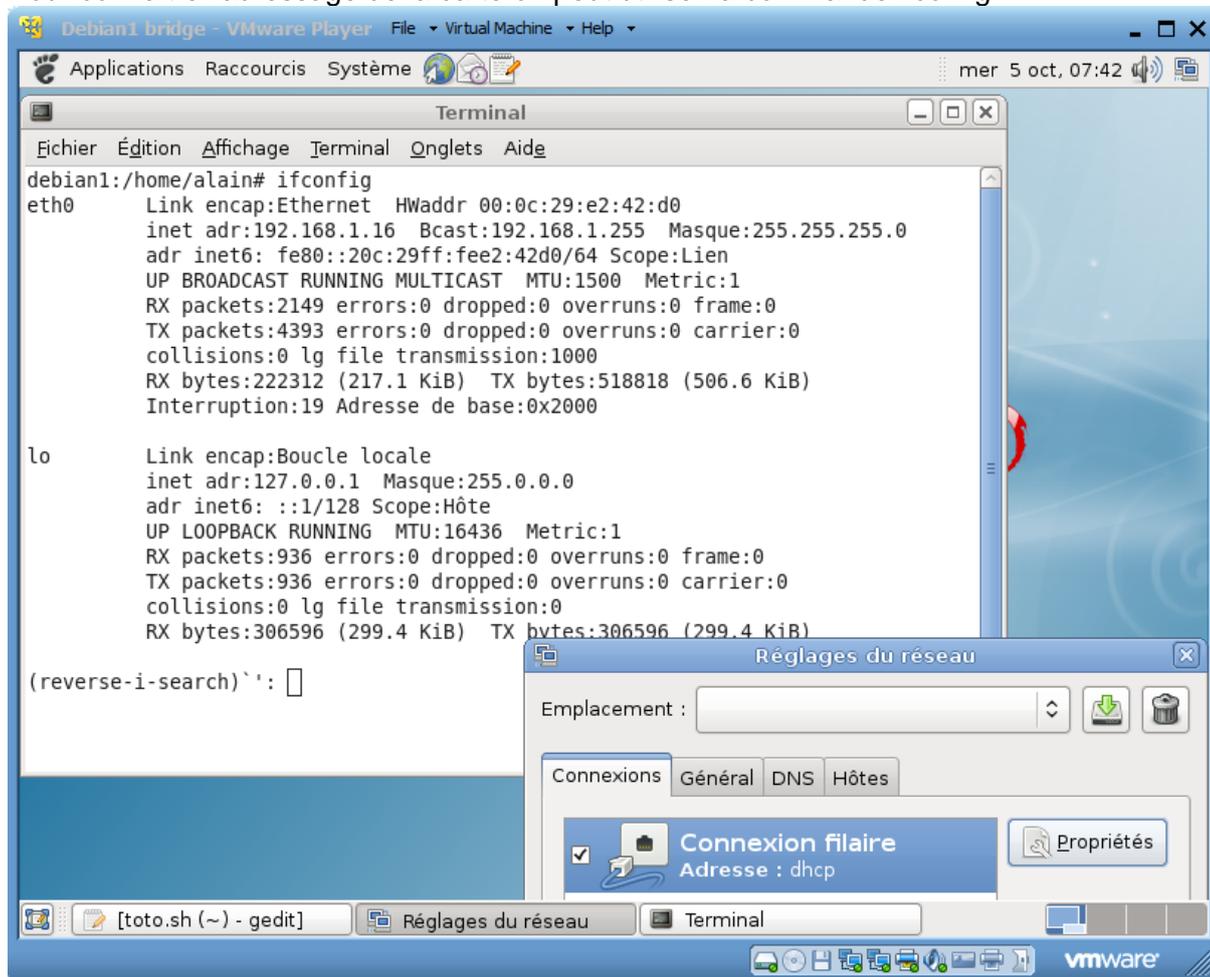
Q3: quelle est l'utilisation du broadcast

Q4: quelle est l'utilisation du multicast

Q5: on souhaite obtenir 4 sous réseaux de 62 machines en classe C 192.168.0.x
donner la solution en définissant les adresses et les masques correspondants pour chaque sous réseau

Paramétrage de la carte réseau sous linux

Pour connaître l'adressage de la carte on peut utiliser la commande ifconfig



Les outils de configuration d'un réseau basé sur IP (notamment **ifconfig**, **route**, **netstat**) sont contenus dans le paquet **net-tools**.

le fichier **/etc/hostname** contient le nom de la machine

Pour paramétrer les adresses Ip de la machine on peut utiliser l'interface graphique

"réglage du réseau" ou utiliser le fichier **/etc/network/interfaces**

iface eth0 inet dhcp (pour un accès dhcp)

ou pour affecter une adresse statique

iface eth0 inet static

adresse 192.168.1.xx xx N° du poste

netmask 255.255.255.0

network 192.168.1.1

gateway 192.168.1.1

dans ce cas il faut rebooter pour que le fichier soit pris en compte ou

faire **ifdown** pour désactiver eth0

puis **ifup** pour réactiver eth0

ou

la commande ifconfig

ifconfig eth0 down /up

Serveur DNS

BIND9

Q6 Installer un serveur de domaine '**mondomaine.fr**'

suivre les consignes d'installation dans ressource

-installer **BIND9**

-installer **Nslookup** ou **dnsutils**

-paramétrer les différents fichiers comme indiqué dans Ressource

(attention vérifier les logs pour être certain de la validation des contenus des différents fichiers)

-tester la syntaxe de vos fichiers de paramétrage

named-checkconf /etc/bind/named.conf

named-checkzone nom_zone fichier-de-zone

installer une machine dans le domaine

tester **nslookup** sur cette machine

tester avec la commande **ping nom-de-la-machine.mondomaine.fr**

Pour démarrer le démon

Après chaque modification des fichiers de configuration, il faut redémarrer le démon :

/etc/init.d/bind9 restart

Attention :

Il est vivement conseillé de regarder les logs pour vérifier que le démarrage du démon s'est correctement effectué :

tail -30 /var/log/syslog

Exemple:

hosts.conf

```
order hosts,bind
multi on
```

hosts:

```
127.0.0.1 localhost.localdomain localhost
192.168.1.21 debian.mondomaine.com debian.mondomain.com
```

resolv.conf:

```
search mondomaine.com
nameserver 192.168.1.21
```

named.conf:

```
zone "mondomaine.com" {
    type master;
    file "/etc/bind/db.mondomaine.com";
    forwarders{};
};
zone "1.168.192.in-addr.arpa"{
    type master;
    file "/etc/bind/db.mondomaine.com.inv";
    forwarders{};
};
```

db.mondomaine.com:

```
$TTL 604800
@ IN SOA debian.mondomaine.com. root.mondomaine.com.(
    1 ; Serial -> N° de série à incrémenter à chaque modif
    ; de ce fichier. Ce N° est utilisé par les
    ; serveurs esclaves pour lui indiquer qu'il
    ; doit mettre à jour sa base. Par commodité
    ; ce n° est une date à l'envers.
    604800 ;Refresh -> A l'expiration du délai Refresh exprimé en
    ; secondes, le serveur esclaves va entrer en
    ; communication avec le maitre et si il ne
    ; le trouve pas, il fera une nouvelle
    ; tentative au bout du délai Retry et si au
    ; bout du délai Expire il considerera que le
    ; serveur n'est plus disponible.
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Minimum -> Durée de vie minimum du cache en secondes
```

```
;**
,
NS debian.mondomaine.com. ;Nom du serveur
debian A 192.168.1.21 ;Adresse IP du
;serveur de noms
```

;** Les lignes suivantes définissent la table entre les noms et les IP

```
debian3 A 192.168.1.15
supmeca1 A 192.168.1.13
```

db.mondomaine.com.inv:

```
$TTL      604800
@         IN      SOA      debian.mondomaine.com. root.mondomaine.com. (
                                20041122
                                604800
                                86400
                                2419200
                                604800 )

                NS      debian.mondomaine.com.

21        PTR      debian.mondomaine.com.
15        PTR      debian3.mondomaine.com.
13        PTR      supmecal.mondomaine.com.
```

Test de trame

Vérifier l'installation de (Ethereal) Wireshark
Lire la notice d'utilisation de Wireshark

Q7 Vérifier les Commande Arp

permet de visualiser le cache arp et de modifier

Arp -a permet de visualiser

Arp -a -d * vide le cache

Arp -N @ip @MAC met en statique dans le cache

Rendre statique l'adresse de la machine sur votre domaine statique dans le cache de votre serveur

Quelle est l'intérêt de rendre ces adresses statiques?

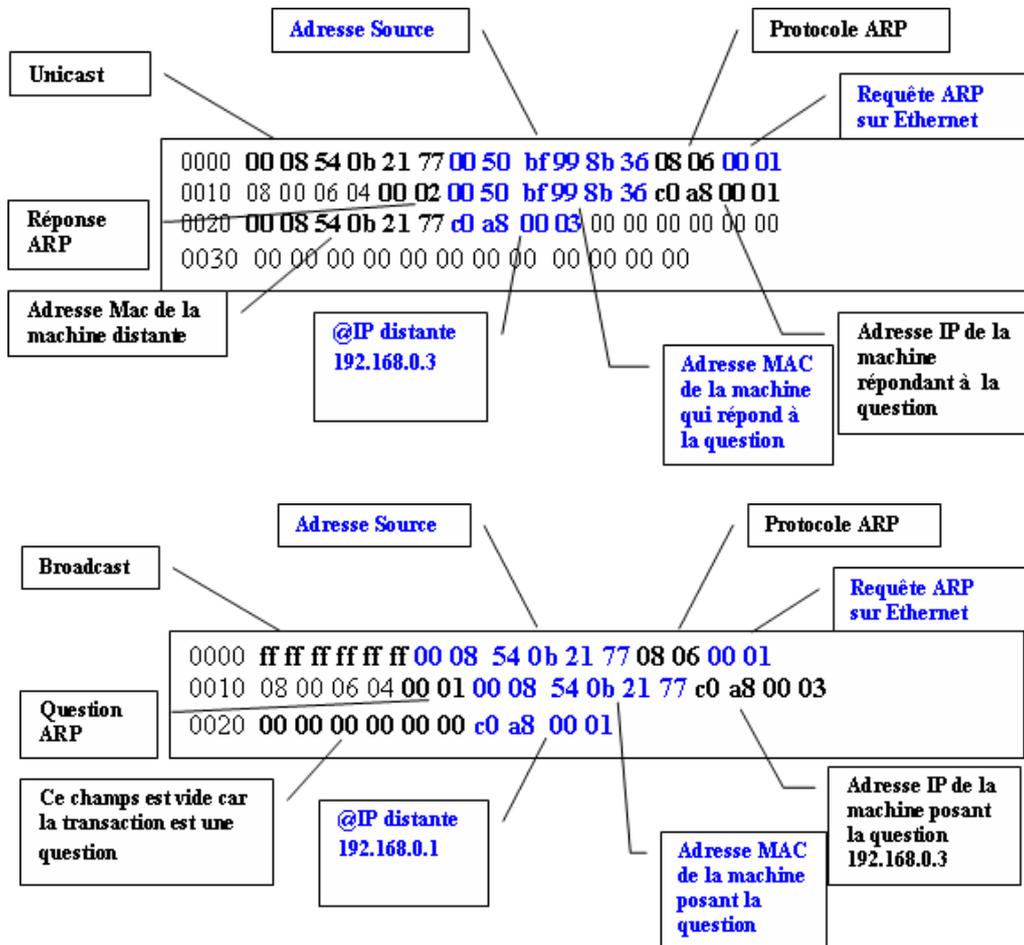
```
C:\Windows\system32>arp -a
Aucune entrée ARP trouvée.

C:\Windows\system32>arp -s 192.168.3.1 00-60-08-9f-35-72

C:\Windows\system32>arp -a

Interface : 192.168.1.14 --- 0xc
Adresse Internet      Adresse physique      Type
192.168.1.1           00-18-e7-2f-58-d8     dynamique
192.168.1.10          00-18-de-cd-3e-77     dynamique
192.168.3.1           00-60-08-9f-35-72     statique
```

exemple de trame



Q8 vérifier la commande **PING**

"pinguer" l'adresse de la machine sur votre domaine

quelle est la signification de 0x0800 au niveau layer 2 ?

quel le type de protocole utiliser par la commande PING ?

trouver le type et code pour le **request**

trouver le type et code pour le **answer**

1	0.000000	Dell_65:36:0b	Broadcast	ARP	who has 192.168.3.1? Tell 192.168.3.14
2	0.000337	3com_9f:35:72	Dell_65:36:0b	ARP	192.168.3.1 is at 00:60:08:9f:35:72
3	0.000356	192.168.3.14	192.168.3.1	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=30/7680, ttl=128)
4	0.000562	192.168.3.1	192.168.3.14	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=30/7680, ttl=64)
5	1.001746	192.168.3.14	192.168.3.1	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=31/7936, ttl=128)
6	1.001964	192.168.3.1	192.168.3.14	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=31/7936, ttl=64)
7	2.003759	192.168.3.14	192.168.3.1	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=32/8192, ttl=128)
8	2.003897	192.168.3.1	192.168.3.14	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=32/8192, ttl=64)
9	3.005758	192.168.3.14	192.168.3.1	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=33/8448, ttl=128)
10	3.006168	192.168.3.1	192.168.3.14	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=33/8448, ttl=64)

Q9 Test du protocole TCP

lancer dans le "browser" navigateur de votre machine

taper "http://IP ou nom de la machine sur votre domaine

vous devez voir la page d'accueil de cette machine

utiliser **Wireshark** pour visualiser l'échange de trame

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.14	192.168.2.2	TCP	64308 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1
2	0.000646	192.168.2.2	192.168.3.14	TCP	http > 64308 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1260 WS=0 SACK_PERM=1
3	0.000728	192.168.3.14	192.168.2.2	TCP	64308 > http [ACK] Seq=1 Ack=1 win=66780 Len=0
4	0.000907	192.168.3.14	192.168.2.2	HTTP	GET / HTTP/1.1
5	0.003062	192.168.2.2	192.168.3.14	HTTP	HTTP/1.1 304 Not Modified
6	0.200018	192.168.3.14	192.168.2.2	TCP	64308 > http [ACK] Seq=512 Ack=205 win=66576 Len=0
7	5.521881	192.168.2.2	192.168.3.14	TCP	http > 64308 [FIN, ACK] Seq=205 Ack=512 win=65024 Len=0
8	5.521949	192.168.3.14	192.168.2.2	TCP	64308 > http [ACK] Seq=512 Ack=206 win=66576 Len=0
9	7.514455	192.168.3.14	192.168.2.2	TCP	64308 > http [FIN, ACK] Seq=512 Ack=206 win=66576 Len=0
10	7.514998	192.168.2.2	192.168.3.14	TCP	http > 64308 [ACK] Seq=206 Ack=513 win=65024 Len=0

Comment est défini le protocole TCP ?
 Quelle est la différence avec le protocole UDP ?

A partir du descriptif du protocole TCP expliquer la séquence des trames.(de manière simple)

Q10 :Extraire l'échange avec le serveur http
 Extraire des trames dans un fichier texte **la requête** et **la réponse http**,
 Vérifier avec l'annexes sur le protocole http que vous retrouver bien les consignes du protocole