

NOM (majuscules) : \_\_\_\_\_

Prénom(s) : \_\_\_\_\_

Groupe : \_\_\_\_\_

## Contrôle M2102-- Bases de reseaux

### Consignes :

Vous avez **1h 30** pour répondre aux questions ci-dessous.

Vous pouvez utiliser l'examen pour écrire vos solutions dans les espaces données sous chaque question. Si vous voulez utiliser un autre support pour écrire vos solutions, **veuillez indiquer cela clairement** dans votre examen.

Veuillez **lire le préambule** de l'examen attentivement avant de commencer.

Vous avez le droit à **une page de notes personnelles recto/verso** (en français ou en anglais). Vous n'avez pas le droit à **rien d'autre** (y compris calculatrice, téléphone portable, les feuilles de TD/TP).

La note finale du module est calculée à partir de : votre note de TD (15%), votre note de TP (15%) et votre note d'examen (70%). Tout bonus que vous avez gagné pour la note de l'examen s'applique seulement à cette note-ci, pas aux notes de TP/TD. Inversement, tout bonus pour le TD/TP s'applique seulement à cette note-là.

Bon courage !

Note TD :

Note TP :

Note examen :     /32 =     /20

## Préambule

Cet examen est composé par 4 exercices, qui sont indépendants (vous pouvez les résoudre dans n'importe quel ordre, sans problème).

Dans l'annexe vous avez du matériel qui peut vous aider pour ce contrôle.

Sauf autrement indiqué, la réponse de toute question vous demandant sur un réseau DOIT contenir l'adresse de ce réseau soit en notation CIDR soit avec un masque de réseau. Ceci s'applique par exemple aux questions du type « Indiquez les réseaux dans la figure ci-dessous ».

Vous devez indiquer tout calcul pertinent à chaque réponse -- sinon vous risquez de perdre des points.

Si vous écrivez des réponses en dehors des espaces données sous chaque question, n'oubliez pas d'indiquer cela clairement.

Bonne chance.

## Exercice 1 (5.5 points) : La topologie des réseaux

Une entreprise achète la plage suivante d'adresses : 142.37.200.0/22.

L'entreprise aura besoin de :

- 500 adresses pour son siège principal
- 240 adresses pour un deuxième siège commercial
- 100 adresses pour accueillir des machines dynamiquement dans son troisième centre (relations avec les clients)
- 100 adresses pour les employés du troisième centre.

1. Pour l'adresse réseau donnée ci-dessus, calculez :
  - a. (0.5 points) Son masque de réseau :
  
  
  
  
  
  
  
  
  
  
  - b. (0.5 points) Combien de machines elle peut accueillir :

- c. (0.5 points) Est-ce que le nombre de machines obtenu suffit pour les besoins cités ci-dessus ? Justifiez votre réponse.
- d. (0.25 points) Ecrivez le nombre 200 en binaire, sur 8 bits :
2. (1 point) Pour accueillir les 500 machines de son siège principal, l'entreprise doit partager la plage achetée. Donnez, en notation CIDR et avec un masque de réseau, l'adresse du sous-réseau contenant les 500 machines, ainsi que l'adresse du sous-réseau qui vous reste.

Réseau du siège principal :

Réseau restant :

3. (1 point) De la même façon, donnez les adresses des sous-réseaux correspondant aux 240 machines pour le deuxième siège, et les adresses restantes respectivement (en notation CIDR seulement) :

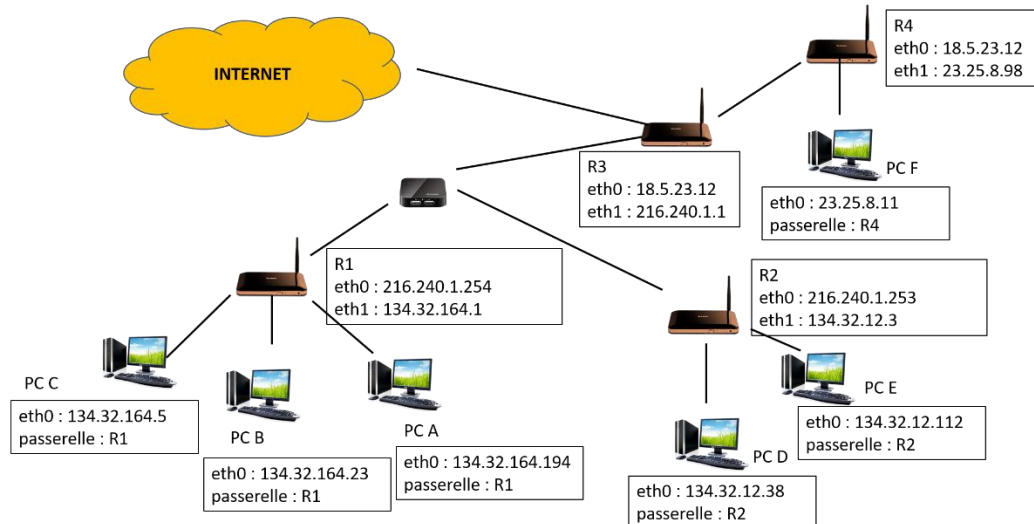
Sous-réseau des 240 machines :

Sous-réseau restant :

4. (0.75 points) Quel est le protocole qui s'occupe de l'attribution dynamique des adresses ? Donnez son nom et son encapsulation.
  
  
  
  
  
  
  
  
  
  
5. Le serveur qui s'occupe de l'attribution dynamique d'adresses pour les clients a l'adresse IP  $x.y.z.w$ , où chaque lettre correspond à un octet de l'adresse IP. Répondez aux questions suivantes :
  - a. (0.5 points) Quel est l'adresse du sous-réseau dans lequel on fait l'attribution dynamique d'adresses ?
  
  
  
  
  
  
  
  - b. (0.25 points) Quelle serait une plage possible pour les adresses des clients (regardez attentivement l'énoncé de l'exercice 1 avant de répondre à cette question) ?
  
  
  
  
  
  
  
  - c. (0.25 points) Quel fichier faut-il configurer pour mettre en place une attribution dynamique d'adresses ?

## Exercice 2 (11.5 points) : IP Forwarding et envoi des messages

Pour cet exercice nous allons travailler sur le réseau dont la topologie est donnée ci-dessous.



Dans cette figure, le texte « passerelle : <nom> » indique la présence d'une passerelle par défaut sur cette machine, notamment la passerelle dont on donne le nom.

La machine  est un Switch.

- (1.5 points) Pour chaque réseau présent dans la figure ci-dessus, indiquez :
  - Son adresse (en notation CIDR seulement)
  - Les machines présentes dans ce réseau (par nom, en soulignant les noms de la/des passerelle.s)

2. (0.75 points) Si nous faisons un `ifconfig` sur la machine PCA la seule interface qui s'affiche est l'interface `lo` de loopback. Quelles sont les commandes à taper pour mettre en place la configuration donnée dans la figure ci-dessus ?
  
3. Nous voulons mettre en place la configuration de la machine R1 tel que cette configuration reste en place même dans le cas où la machine tombe en panne. De plus, la passerelle par défaut de R1 sera R3. Répondez aux questions suivantes :
  - a. (0.5 points) Quel fichier faut-il modifier pour mettre cela en place ?
  
  - b. (1 points) Donnez le contenu de ce fichier.
  
  - c. (0.5 points) Quelle commande faut-il utiliser pour vérifier la bonne mise en place de la passerelle par défaut ?

4. (1 point) Quelles autres commandes faut-il taper **sur R1** pour activer l'activation du routage et pour assurer l'envoi d'un message de PC A vers n'importe quelle machine dans le réseau ?
  
5. Sur PC A on tape la commande `ping -c 1 134.32.164.23`. Répondez aux questions suivantes :
  - a. (0.5 points) Si on veut visualiser le ping sur Wireshark, quel type de message faut-il regarder ?
  
  - b. (0.75 points) Quelle est l'encapsulation du protocole donné à 5a ?
  
  - c. (1 point) L'envoi du ping cause l'envoi d'un autre message à partir de la machine PC A. Quel est cet autre message ? (expliquez le type de message, son rôle, l'expéditeur et le destinataire, son contenu, ainsi que son encapsulation)
  
  - d. (1 point) Quelle est une réponse possible pour le message de la question 5c ? (qui l'envoie, vers qui, quel est son contenu ?)
  
6. (1.5 points) Nous allons supposer que la configuration de la machine R3 a été faite correctement. De plus, cette machine a les passerelles suivantes : R1 vers le réseau contenant PC A, R2 vers le

réseau de PC E et R4 vers le réseau de PC F. Vous pouvez aussi supposer que la configuration de PC F a été mise en place comme dans la figure ci-dessus.

La machine PC A fait un ping vers PC F.

Quel est le résultat de ce ping ? Expliquez et justifiez votre réponse, en indiquant toutes les étapes de l'envoi.

7. (1.5 points) Qui connaîtra l'adresse MAC de la machine R1 au bout de cet envoi ? Justifiez votre réponse.

### Exercice 3 (8.5 points) Netstat et le fonctionnement en réseau

La commande `route -n` utilisée sur une certaine machine M donne le résultat suivant :

Destination	Netmask	Gateway
164.81.20.0	_____	0.0.0.0
192.168.12.0	_____	0.0.0.0
10.25.0.0	255.255.0.0	0.0.0.0
127.0.0.0	_____	0.0.0.0
192.168.11.0	_____	192.168.12.254
10.23.34.21	_____	10.25.0.254



1. (2 points) Expliquez la notion de classe de réseau et indiquez les caractéristiques des réseaux de classe A, B et C.
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
2. Pour la machine sur laquelle on a tapé la commande route ci-dessus, répondez aux questions suivantes :
  - a. (0.25) Combien d'interfaces réseau a-t-elle ?
  
  
  
  
  
  
  
  
  
  
  
  
  - b. (0.75) Cette machine, elle fait partie de quels réseaux ?
  
  
  
  
  
  
  
  
  
  
  
  
  - c. (1 point) Complétez le tableau ci-dessus avec les masques de réseau manquants.
  
  
  
  
  
  
  
  
  
  
  
  
  - d. (0.5 points) Sur la machine en question on ajoute une passerelle par défaut avec l'adresse IP 164.81.20.254. Quelle est la commande utilisée ?
  
  
  
  
  
  
  
  
  
  
  
  
  - e. (0.5 points) Une fois la passerelle par défaut ajoutée quelle sera la ligné ajoutée au tableau ci-dessus ?

3. Sur la machine M la commande `ping -c 1 8.8.8.8` donne le résultat : Destination host unreachable, avec une perte de paquets de 100%. Un administrateur de réseau essaie de diagnostiquer le problème. Il tape la commande `ping -c 1 164.81.20.254`. Ce ping marche parfaitement. Répondez aux questions suivantes :
- a. (0.75 points) Que signifie l'erreur donnée par le ping vers 8.8.8.8 (pas de traduction de l'anglais, sinon une explication de sa signification) ?
  
  
  
  
  
  
  
  
  
  
  - b. (0.75 points) Pourquoi l'administrateur a-t-il tapé la commande `ping -c 1 164.81.20.254` ? (Quel est son rôle, qu'est-ce que l'administrateur a-t-il soupçonné comme problème ?)
  
  
  
  
  
  
  
  
  
  
  - c. (1 point) Etant donné le résultat donné par ces deux commandes, quelle est une conclusion probable faite par l'administrateur de réseau ?
4. (1 point) Qu'est-ce qu'une résolution directe de nom ? Et une résolution inverse ? Quel est le protocole qui s'en occupe ?

## Exercice 4 (6.5 points) Les applications sur le réseau

La commande netstat -tn sur une certaine machine donne le résultat suivant :

```
# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      236 139.162.151.198:22     78.116.61.143:45364    ESTABLISHED
tcp      0      0 139.162.151.198:443   78.116.61.143:51657   FIN_WAIT2
tcp      0      0 139.162.151.198:80    78.116.61.143:51654   FIN_WAIT2
tcp      0      0 139.162.151.198:443   78.116.61.143:51655   FIN_WAIT2
tcp      0      0 139.162.151.198:443   78.116.61.143:51658   ESTABLISHED
```

1. (1.5 points) Vous trouvez dans l'annexe une liste de ports standard. En utilisant cette liste décrivez ce que vous voyez dans la figure ci-dessus.
  
  
  
  
  
  
  
  
  
  
2. (1.5 points) La machine sur laquelle on a tapé la commande netstat ci-dessus on a mis en place un serveur DHCP. Pouvez-vous visualiser cela sur la figure ci-dessus ? Pourquoi/pourquoi pas ?

3. (0.75 points) Expliquez le rôle du protocole utilisé dans la première ligne de la capture ci-dessus.
  
  
  
  
  
  
  
  
  
  
  
  
4. Dans l'annexe nous pouvons voir une capture Wireshark. Répondez aux questions suivantes :
  - a. (0.5 points) Quelles sont les machines qui communiquent dans cette capture ?
  
  
  
  
  
  
  
  
  - b. (0.25 points) Qui est le client et qui est le serveur ?
  
  
  
  
  
  
  
  
  - c. (1 point) Pouvez vous expliquer pourquoi entre chaque échange SSH il y a un paquet TCP ?

## Annexe A

Ports standard :

TCP 21 : FTP

TCP 22 : SSH

TCP 23 : Telnet

TCP 53 : DNS

UDP 67 : DHCP

TCP 80 : HTTP

TCP 443 : HTTPS

Annexe B

No.	Time	Source	Destination	Protocol	Length	Info
48	1.096140455	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3126 Ack=3342 Win=37120 Len=0 TSval=1260771666 TSecr=3979554847
49	1.096219622	139.162.151.198	192.168.1.79	SSHv2	134	Server: Encrypted packet (len=68)
50	1.096252337	139.162.151.198	192.168.1.79	SSHv2	102	Server: Encrypted packet (len=36)
51	1.096323080	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3126 Ack=3350 Win=37120 Len=0 TSval=1260771666 TSecr=3979554847
52	1.144853947	139.162.151.198	192.168.1.79	SSHv2	166	Server: Encrypted packet (len=100)
53	1.186295690	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3126 Ack=3650 Win=37120 Len=0 TSval=1260771756 TSecr=3979554897
54	1.574773732	139.162.151.198	192.168.1.79	SSHv2	150	Server: Encrypted packet (len=84)
55	1.574884530	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3126 Ack=3734 Win=37120 Len=0 TSval=1260772145 TSecr=3979555328
58	6.660727313	192.168.1.79	139.162.151.198	SSHv2	102	Client: Encrypted packet (len=36)
59	6.710450456	139.162.151.198	192.168.1.79	TCP	66	22 → 45364 [ACK] Seq=3734 Ack=3162 Win=39680 Len=0 TSval=3979560462 TSecr=1260777231
60	6.710543395	139.162.151.198	192.168.1.79	SSHv2	102	Server: Encrypted packet (len=36)
61	6.710598231	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3162 Ack=3770 Win=37120 Len=0 TSval=1260777281 TSecr=3979560463
62	6.775194759	192.168.1.79	139.162.151.198	SSHv2	102	Client: Encrypted packet (len=36)
63	6.824428773	139.162.151.198	192.168.1.79	SSHv2	102	Server: Encrypted packet (len=36)
64	6.824535731	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3198 Ack=3806 Win=37120 Len=0 TSval=1260777394 TSecr=3979560577

> Frame 49: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0  
 > Ethernet II, Src: Sfr\_19:18:88 (e4:5d:51:19:18:88), Dst: IntelCor\_54:fd:ad (e4:a7:a0:54:fd:ad)

> [redacted] Src: [redacted] Dst: [redacted]  
 > [redacted] Src Port: [redacted] Dst Port: [redacted], Seq: 3446, Ack: 3126, Len: 68

> SSH Protocol

```

2000  e4 a7 a0 54 fd ad e4 5d 19 18 88 08 00 45 00 ...T...] Q.....E
2010  00 78 a2 86 40 00 35 06 bd 99 8b a2 97 c6 c0 a8 ...x (@.5.....
2020  01 4f 00 16 b1 34 59 2c 1e 67 02 d6 99 39 80 18 ...O..AY, g...9..
2030  01 36 eb 17 00 00 01 01 08 0a ed 33 30 1f 4b 25 ...6.....30 K%
2040  d8 ee 21 1c a2 e1 e2 09 5f e7 01 67 4f 7a e2 a1 ...!....._g0z
2050  e4 c8 90 ad df 91 6d 12 8b f2 70 bc 12 a0 34 bc [redacted]
2060  cb de f7 3f 38 7d b5 e2 c5 4c a1 ee 32 45 72 ac [redacted]
2070  17 12 89 f7 97 8a 19 c8 64 39 c3 80 c2 eb f3 5e [redacted]
2080  d3 27 75 08 5d d9 [redacted]
    
```