



Année universitaire 2020-2021

SUJET UTC505 : Réseaux et Sécurité

Examen 2^e session du 30/04/2021

Responsables : E. GRESSIER-SOUDAN, N. PIOCH

Durée : épreuve réseau elle-même 2h

Consignes

Les étudiants ne doivent pas communiquer entre eux. Et c'est un travail strictement personnel.

Contrevenir à toute obligation correspond à un risque de 5 ans d'exclusion du CNAM.

Pour chaque question il est demandé une justification précise de votre réponse.
Le barème de cet examen correspond à une notation sur 14 points

Sujet de **12 pages**, celle-ci comprise.

Important :

Les étudiants répondent sur les feuilles du sujet d'examen au format word, et si nécessaire complètent leur réponse par des photos qu'ils insèrent dans leur copie réponse. **La version finale de votre composition est remise au format pdf sur moodle.**

Vous générez un seul document et pas un fichier par page !!! Je ne corrigerais qu'un seul document au format pdf qui est d'ailleurs le seul format autorisé dans la configuration moodle pour UTC505.

Attention : Les réponses doivent suivre les questions auxquelles elle se rapportent.

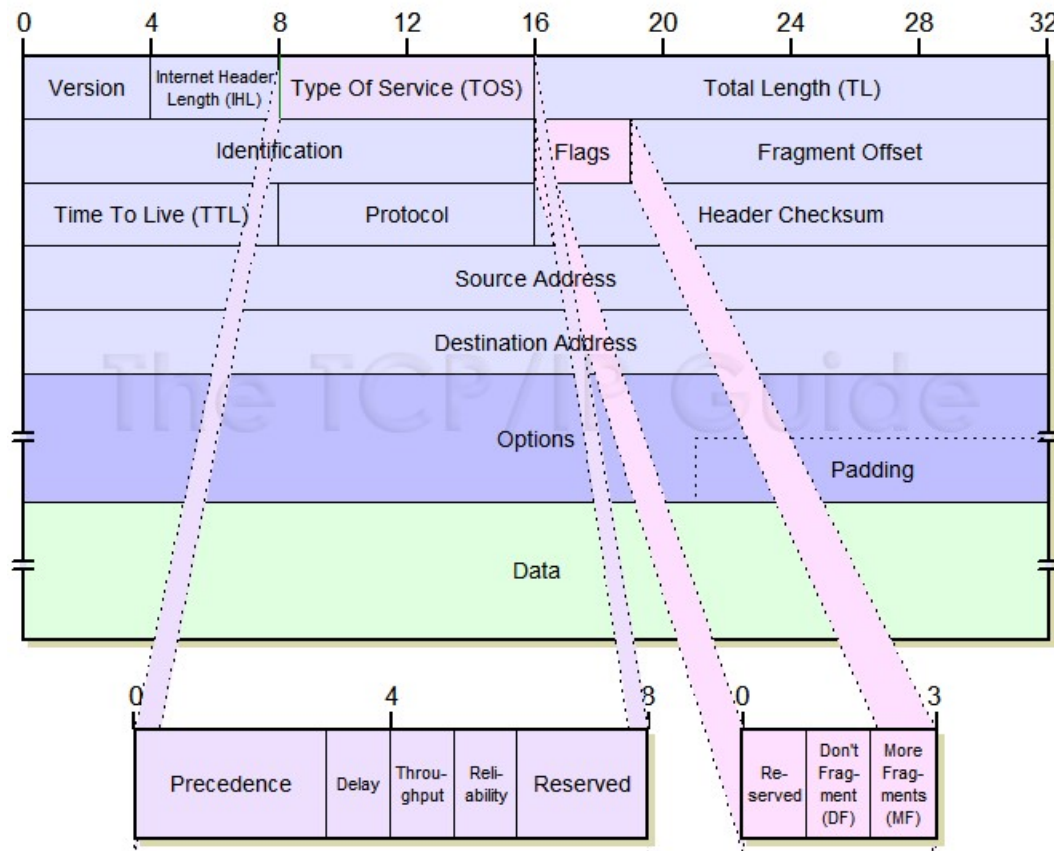
Partie Réseaux (19 points noté sur 14)

Exercice 1 : Analyse de Trace Wireshark (10 points)

On donne la structure d'une trame Ethernet :

Adresse destination	Adresse source	Type	Informations	FCS
6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

On donne la structure du datagramme IP dont son entête en détail, consulté le 23 décembre 2013, Source http://www.tcpipguide.com/free/t_IPDatagramGeneralFormat.htm :



la structure d'un segment TCP dont l'entête en détail, consulté le 23 décembre 2013 source <http://caleudum.wordpress.com/2011/05/08/tcp-header-format/> :

TCP Header																																
Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number (if ACK set)																															
96	Data offset				Reserved				C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size															
128	Checksum																Urgent pointer (if URG set)															
160	Options (if Data Offset > 5)																								padding							
...	...																															

Les indicateurs qui nous intéressent sont :

- URG : Signale la présence de données **urgentes**
- ACK : signale que le segment contient un accusé de réception (**acknowledgement**)
- PSH : données à envoyer et délivrer tout de suite (**push**)
- RST : rupture anormale de la connexion ou refus de demande d'ouverture de connexion (**reset**)
- SYN : demande de **syn**chronisation ou établissement de connexion
- FIN : demande la **fin** de la connexion

Question 1 : On s'intéresse à une trace Wireshark qui formalise un échange client/serveur. On s'intéresse à la trame 44. Elle vous est donnée en hexadécimal ci-après. Ne pas hésiter à utiliser des couleurs différentes pour que vos réponses soient faciles à lire, donc à comprendre et donc à corriger pour vous mettre une note la plus favorable possible. **(1 point)**

Pour chaque question, **0,25 point** :

- Délimiter dans le trace hexadécimale l'entête de la trame Ethernet.
- Délimiter dans le trace hexadécimale l'entête du datagramme IP.
- Délimiter dans le trace hexadécimale l'entête du segment.
- Délimiter dans le trace hexadécimale la partie HTTP.

Juste après la trace hexadécimale de la trame 44, la version Wireshark vous est donnée successivement sur 2 pages pour vous aider.

00 20 af 1b 07 fa 00 e0 29 68 8b fb 08 00 45 00

00 77 c1 e6 40 00 40 06 f7 46 c0 a8 00 01 c0 a8

00 02 0b fc 1f 40 ea 46 fc 03 08 c4 ec 75 50 18

44 70 71 79 00 00 47 45 54 20 2f 20 48 54 54 50

2f 31 2e 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74

3a 20 57 67 65 74 2f 31 2e 35 2e 33 0d 0a 48 6f

73 74 3a 20 31 39 32 2e 31 36 38 2e 30 2e 32 3a

38 30 30 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f

2a 0d 0a 0d 0a

Time	Source	Destination	Protocol	Lengt	Info
44 1.355647	192.168.0.1	192.168.0.2	HTTP	133	GET / HTTP/1.0

Frame 44: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)

Ethernet II, Src: SmcEther_68:8b:fb (00:e0:29:68:8b:fb), Dst: 3Com_1b:07:fa (00:20:af:1b:07:fa)

- > Destination: 3Com_1b:07:fa (00:20:af:1b:07:fa)
- > Source: SmcEther_68:8b:fb (00:e0:29:68:8b:fb)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 119
- Identification: 0xc1e6 (49638)
- ✓ Flags: 0x4000, Don't fragment
 - 0... = Reserved bit: Not set
 - .1.. = Don't fragment: Set
 - ..0. = More fragments: Not set
- Fragment offset: 0
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0xf746 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.1
- Destination: 192.168.0.2

**Longueur de la trame
sans le CRC**

Transmission Control Protocol, Src Port: 3068, Dst Port: 8000, Seq: 1, Ack: 1, Len: 79

Source Port: 3068

Destination Port: 8000

[Stream index: 4]

[TCP Segment Len: 79]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 3930520579

[Next sequence number: 80 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 147123317

0101 = Header Length: 20 bytes (5)

▼ Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

[TCP Flags:AP...]

Window size value: 17520

[Calculated window size: 17520]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x7179 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

```
00 20 af 1b 07 fa 00 e0 29 68 8b fb 08 00 45 00  - ..... )h....E-
00 77 c1 e6 40 00 40 06 f7 46 c0 a8 00 01 c0 a8  -w--@-@- -F-----
00 02 0b fc 1f 40 ea 46 fc 03 08 c4 ec 75 50 18  -....@-F .....uP-
44 70 71 79 00 00 47 45 54 20 2f 20 48 54 54 50  Dpqy--GE T / HTTP
2f 31 2e 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74  /1.0--Us er-Agent
3a 20 57 67 65 74 2f 31 2e 35 2e 33 0d 0a 48 6f  : Wget/1 .5.3--Ho
73 74 3a 20 31 39 32 2e 31 36 38 2e 30 2e 32 3a  st: 192. 168.0.2:
38 30 30 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f  8000--Ac cept: */
2a 0d 0a 0d 0a  *....
```


Question 2 :

En vous aidant de la trace Wireshark et de la trame en hexadécimal, répondez aux questions suivantes et encadrer dans la trace hexadécimale le champ concerné. Chaque réponse à une question compte **0,25 point si votre réponse est CORRECTE ET COMPLETE, 0 SINON. (4 points)**

1. Quelle est l'adresse Ethernet destination en hexadécimal ?	
2. Pourquoi est-ce une adresse unicast ?	
3. Quelle est l'adresse Ethernet source en hexadécimal ?	
4. Le type de la trame en hexadécimal correspond il à la version du protocole dans l'entête du datagramme IP en décimal ? Quelle est la version d'IP ?	
5. Quelle est la longueur de l'entête IP en décimal ? pourquoi ?	
6. Quelle est l'adresse IP source en hexadécimal et en décimal ?	
7. Quelle est l'adresse IP destination en hexadécimal et en décimal ?	
8. Quel est le numéro du protocole transporté dans la charge utile et indiqué par l'entête IP et du datagramme en hexadécimal , confirmer que c'est bien TCP ?	
9. Quelle est la longueur du datagramme en décimal ? Est-ce que cela comprend l'entête IP ?	
10. Quel est le numéro de port source en hexadécimal ?	

11. Quel est le numéro de port destination en hexadécimal ?	
12. Quelle est la longueur de l'entête TCP, y a-t-il des options ?	
13. Quel est la valeur du numéro de séquence absolu dans l'entête TCP en hexadécimal ?	
14. Quel indicateur de l'entête permet de considérer la valeur de l'ACK comme ayant un sens ?	
15. Quel est la valeur du numéro d'ACK absolu dans l'entête TCP en hexadécimal ?	
16. Pourquoi la taille de la charge utile du segment, de 79 octets, est-elle cohérente avec la longueur du datagramme 119 octets ?	

La requête HTTP ci-dessous, contenue dans la trame 44 et extraite de la bande à droite de la partie headécimale est correctement formée. L'URL contenue dans cette requête est elle aussi correctement formée. Cette requête peut vous donner une indication pour répondre à la question 3.

```

  ▾ Hypertext Transfer Protocol
    ▾ GET / HTTP/1.0\r\n
      > [Expert Info (Chat/Sequence): GET / HTTP/1.0\r\n]
        Request Method: GET
        Request URI: /
        Request Version: HTTP/1.0
        User-Agent: Wget/1.5.3\r\n
        Host: 192.168.0.2:8000\r\n
        Accept: */*\r\n
        \r\n
        [Full request URI: http://192.168.0.2:8000/]
        [HTTP request 1/1]
```

Le protocole est HTTP/1.0. Avec http 1.0, le client établit la connexion, envoie une requête, le serveur répond avec la page et ferme immédiatement la connexion TCP sous-jacente.

Question 3 : Puzzle sur une communication TCP (5 points)

Remettre les échanges listés sur chaque ligne dans le bon ordre. La suite correcte représente l'enchaînement des trames qui montre le déroulement d'une connexion TCP entre (192.168.0.1, 3064), navigateur Web, et (192.168.0.2, 8000), serveur Web. On doit retrouver dans l'ordre les 3 phases : ouverture de connexion-transfert de données-fermeture de connexion. On vous donne uniquement l'ordre du premier SYN et la position de la requête GET dans l'enchaînement. **(0,25 point par ligne bien placée, et 0,5 point pour les explications globales)**

Attention, dans les échanges Wireshark les numéros de séquence sont en relatif (ils démarrent à 0), ça facilite.

Pour réussir : se concentrer, faire un schéma d'échanges avec les numéros d'acquittements et les numéros de séquence + taille des données quand c'est possible (ça l'est toujours mais il faut faire des calculs à partir de la taille de la trame capturée par Wireshark, champ "length").

1 - 192.168.0.1 192.168.0.2 TCP 60 3064 → 8000 [SYN] Seq=0 Win=16384 Len=0 MSS=1460

192.168.0.2 192.168.0.1 TCP 54 8000 → 3064 [ACK] Seq=296 Ack=81 Win=32120 Len=0

192.168.0.1 192.168.0.2 TCP 60 3064 → 8000 [ACK] Seq=1 Ack=1 Win=17520 Len=0

192.168.0.1 192.168.0.2 TCP 60 3064 → 8000 [ACK] Seq=80 Ack=296 Win=17520 Len=0

192.168.0.2 192.168.0.1 TCP 348 8000 → 3064 [PSH, ACK] Seq=1 Ack=80 Win=32120 Len=294 [TCP se

192.168.0.2 192.168.0.1 TCP 54 8000 → 3064 [ACK] Seq=1 Ack=80 Win=32120 Len=0

4 - 192.168.0.1 192.168.0.2 HTTP 133 GET / HTTP/1.0

192.168.0.2 192.168.0.1 TCP 54 8000 → 3064 [FIN, ACK] Seq=295 Ack=80 Win=32120 Len=0

192.168.0.2 192.168.0.1 TCP 58 8000 → 3064 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460

192.168.0.1 192.168.0.2 TCP 60 3064 → 8000 [FIN, ACK] Seq=80 Ack=296 Win=17520 Len=0

Expliquer brièvement comment vous trouvez votre réponse.

Exercice 2 : Déterminer un système d'exploitation à partir d'un TTL. (2 points)

On vous donne le résultat de l'exécution d'une commande `tracert` et d'une commande `ping`, quel est le système d'exploitation sur lequel ces commandes ont été exécutées ? Pourquoi ?

```
tracert www.google.com :
1 static.1.241.243.136.clients.your-server.de (136.243.241.1) 0.285 ms
2 core24.fsn1.hetzner.com (213.239.229.53) 0.253 ms
3 core1.fra.hetzner.com (213.239.229.77) 4.818 ms
4 213-239-239-118.clients.your-server.de (213.239.239.118) 4.804 ms
5 172.253.64.118 (172.253.64.118) 4.886 ms
6 fra16s49-in-f4.1e100.net (142.250.185.100) 4.789 ms
```

et

```
ping 142.250.185.100
PING 142.250.185.100 (142.250.185.100) 56(84) bytes of data.
64 bytes from 142.250.185.100: icmp_seq=1 ttl=122 time=4.78 ms
64 bytes from 142.250.185.100: icmp_seq=2 ttl=122 time=4.80 ms
64 bytes from 142.250.185.100: icmp_seq=3 ttl=122 time=4.82 ms
64 bytes from 142.250.185.100: icmp_seq=4 ttl=122 time=4.77 ms
64 bytes from 142.250.185.100: icmp_seq=5 ttl=122 time=4.83 ms
64 bytes from 142.250.185.100: icmp_seq=6 ttl=122 time=4.86 ms
64 bytes from 142.250.185.100: icmp_seq=7 ttl=122 time=4.80 ms
64 bytes from 142.250.185.100: icmp_seq=8 ttl=122 time=4.79 ms
64 bytes from 142.250.185.100: icmp_seq=9 ttl=122 time=4.80 ms
64 bytes from 142.250.185.100: icmp_seq=10 ttl=122 time=4.79 ms
```

```
--- 142.250.185.100 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 4512ms
rtt min/avg/max/mdev = 4.777/4.809/4.863/0.079 ms
```

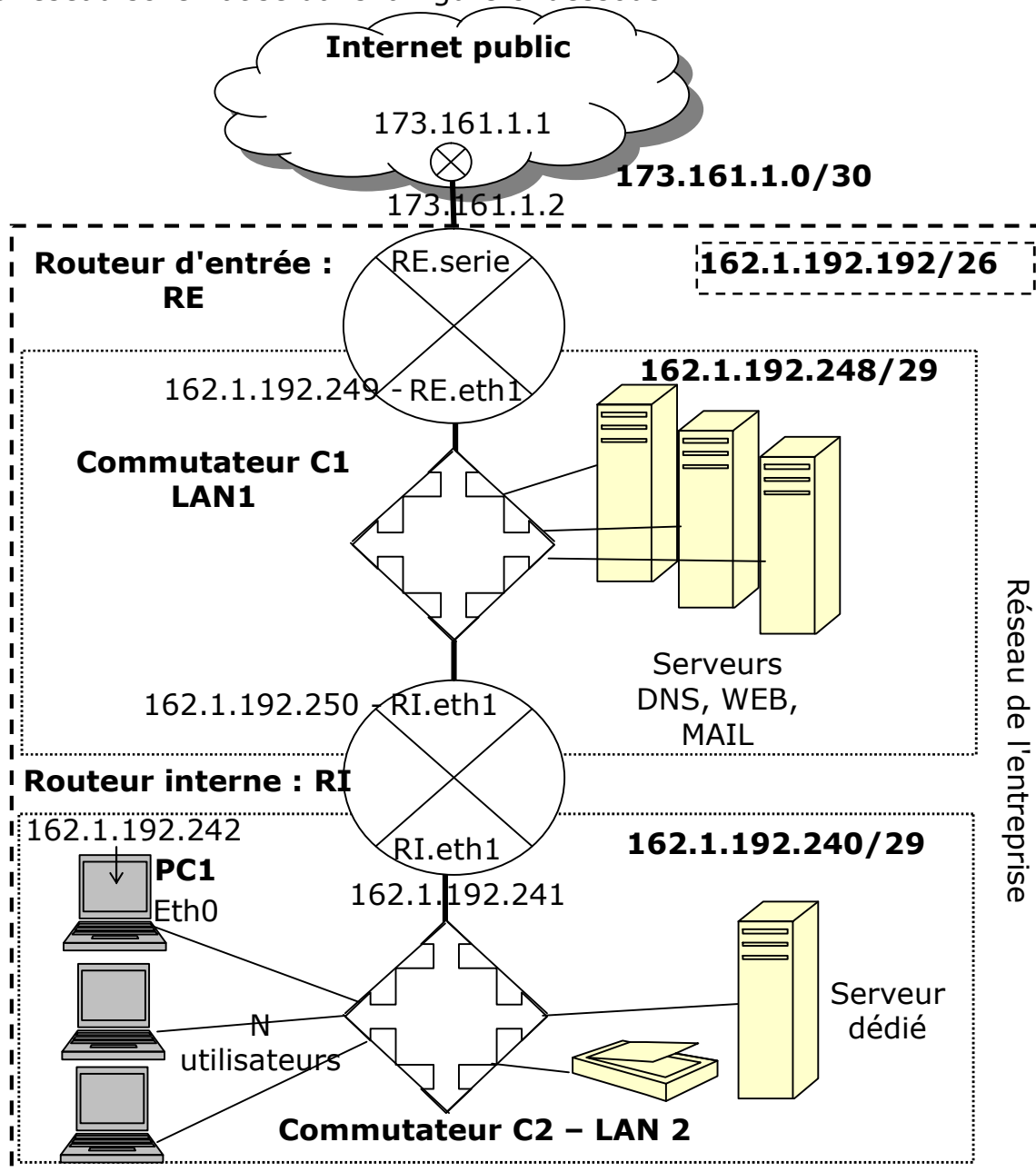
Ci-après la table qui fait correspondre le TTL d'un datagramme IP initialisé depuis l'émetteur avec le système d'exploitation qui fabrique le datagramme :

Système d'exploitation	TTL
Linux	64
FreeBSD	64
Windows	128
HP-UX	255
OpenBSD	255
MacOS X	64

Expliquez brièvement votre réponse et les calculs qui vous ont permis d'arriver au résultat.

Exercice 3 : Routage et Adressage IPv4. (7 points)

Soit le réseau schématisé dans la figure ci-dessous.



Question 1 : Configuration réseau d'un PC utilisateur (1 point)

On vous donne l'extrait du résultat de la commande `ipconfig` sur le poste utilisateur PC1. Chaque bonne réponse compte 0,25 point.

Carte Ethernet Connexion au réseau local filaire eth0 :

```
Suffixe DNS propre à la connexion. . . : mycompany.com
Adresse MAC. . . . . : 00:a0:af:1b:0a:fb
Adresse IPv4 . . . . . :
Masque de sous-réseau. . . . . :
```

- Compléter l'adresse IPv4 manquante.
- Compléter le masque de sous-réseau en notation décimale pointée.
- Quelle est l'adresse de diffusion (broadcast) sur le sous-réseau 162.1.192.240/29, comment l'obtenez-vous ?

- Combien d'adresses d'interface seraient possibles avec ce masque sur ce sous-réseau IP ?

Question 2 : Table de routage d'un PC utilisateur (1 point)

Remplir les cases vides de la table de routage ci-dessous. **0,25 point par case remplie avec la bonne valeur.**

	Réseau/mask	Nxt hop	interface	accessibilité	commentaire
L1			eth0	distant	Route par défaut
L2	127.0.0.0/8	0.0.0.0	lo0	direct	Local host
L3		0.0.0.0		direct	Reste sur LAN2

Question 3 : Donner la table de routage de RE et la table de routage de RI, vous remplirez les tableaux ci-dessous, et vous ajouterez ou supprimerez des lignes si nécessaire. On ne se soucie pas de la métrique. (3 points)

RE	Réseau/mask	Nxt hop	interface	accessibilité	commentaire
L1					Route par défaut
L2					
L3					
L4					

RI	Réseau/mask	Nxt hop	interface	accessibilité	commentaire
L1					Route par défaut
L2					
L3					
L4					

Question 4 : Dimensionnement de l'adressage du réseau (3 points)

Au regard du plan d'adressage porté sur la figure ci-dessus.

Quelle est la valeur maximale de N, on fait l'hypothèse qu'un ordinateur d'utilisateur n'a qu'une seule interface ? **(1 point)**

Si on veut mettre plus d'interfaces dans le LAN 2 que cette valeur max que se passe-t-il ? Proposer une modification du plan d'adressage pour pouvoir augmenter la taille du sous-réseau qui correspond au LAN 2. **(2 points)**