

Année universitaire 2018-2019

SUJET UTC505 : Réseaux et Sécurité

Examen 1^e session du 26/06/2019

Responsables : *E. GRESSIER-SOUUDAN, N. PIOCH*

Durée : 2 heures 30

Consignes

Calculatrice autorisée sur un équipement différent du téléphone mobile.

Tous documents autorisés

**Les téléphones mobiles sont interdits
autres équipements communicants autorisés mais Internet interdit.**

Les étudiants ne doivent pas communiquer entre eux.

Contrevénir 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 21 points

Sujet de **15 pages**, celle-ci comprise.

Important : Les étudiants répondent sur les feuilles du sujet d'examen, et si nécessaire complètent leur réponse sur une copie double en faisant référence à quelle question correspond quelle réponse.

Bien mettre le numéro des questions avec leurs réponses sur la copie.

Vous rendrez une copie double au moins afin de donner les informations d'usage (nom, prénom...) et de récupérer un numéro de copie que vous ajouterez sur les feuilles du sujet d'examen. La copie doit être remise aux surveillants avec le coin cacheté.

Vous rendez le sujet rempli avec vos réponses à la fin de l'examen.

→ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

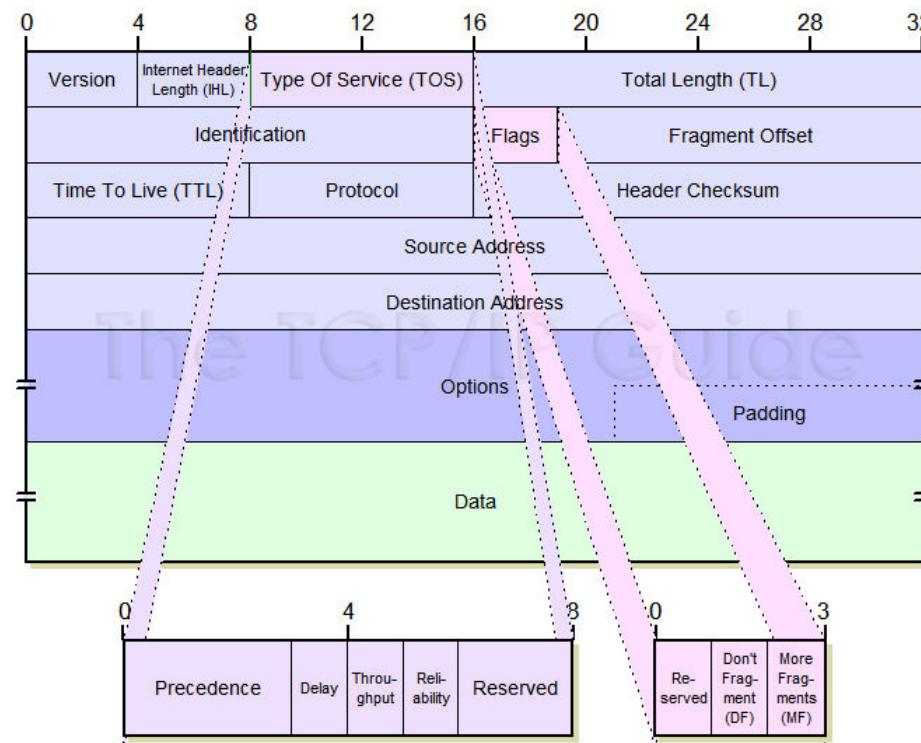
1/15

Exercice 1 : Partie Réseaux (16 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 R	E C E G	U R C K	A P S H	P R S T	R S Y N	S Y I N	F	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 (**reset**)
- SYN : demande de **synchronisation** ou établissement de connexion
- FIN : demande la **fin** de la connexion

On s'intéresse à une trace Wireshark qui formalise un échange client/serveur. Elle vous est donnée ci-dessous.

1 0.000000	10.20.144.150	10.20.144.151	TCP	74 35974 → 21 [SYN] Seq=0 Win=32648 Len=0 MSS=1380 WS=1 TSval=1657560000 TSecr=0
2 0.000320	10.20.144.151	10.20.144.150	TCP	78 21 → 35974 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1356 WS=1 TSval=1657390000 TSecr=1
3 0.000570	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [ACK] Seq=1 Ack=1 Win=32648 Len=0 TSval=1657560000 TSecr=1657390000
4 0.060630	10.20.144.151	10.20.144.150	FTP	106 Response: 220-QTCP at fran.csg.stercomm.com.
5 0.275440	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [ACK] Seq=1 Ack=37 Win=32648 Len=0 TSval=1657560500 TSecr=1657390000
6 0.275760	10.20.144.151	10.20.144.150	FTP	126 Response: 220 Connection will close if idle more than 5 minutes.
7 0.276140	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [ACK] Seq=1 Ack=93 Win=32648 Len=0 TSval=1657560500 TSecr=1657390000
8 4.216600	10.20.144.150	10.20.144.151	FTP	81 Request: USER cdts3500
9 4.217350	10.20.144.151	10.20.144.150	FTP	91 Response: 331 Enter password.
10 4.217630	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=16 Ack=114 Win=32648 Len=0 TSval=1657564500 TSecr=1657394000
11 7.639420	10.20.144.150	10.20.144.151	FTP	81 Request: PASS cdts3500
12 7.843260	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [PSH, ACK] Seq=114 Ack=31 Win=16384 Len=0 TSval=1657397500 TSecr=1657568000
13 8.184000	10.20.144.151	10.20.144.150	FTP	95 Response: 230 CDTS3500 logged on.
14 8.184360	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=31 Ack=139 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
15 8.185040	10.20.144.150	10.20.144.151	FTP	72 Request: SYST
16 8.185260	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [PSH, ACK] Seq=139 Ack=37 Win=16384 Len=0 TSval=1657398000 TSecr=1657568500
17 8.192750	10.20.144.151	10.20.144.150	FTP	147 Response: 215 OS/400 is the remote operating system. The TCP/IP version is "V5R2M0".
18 8.193000	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=37 Ack=216 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
19 8.193570	10.20.144.150	10.20.144.151	FTP	80 Request: SITE NAMEFMT
20 8.193780	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [PSH, ACK] Seq=216 Ack=51 Win=16384 Len=0 TSval=1657398000 TSecr=1657568500
21 8.194900	10.20.144.151	10.20.144.150	FTP	105 Response: 250 Now using naming format "0".
22 8.195140	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=51 Ack=251 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
23 8.195700	10.20.144.150	10.20.144.151	FTP	71 Request: PWD
24 8.195910	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [PSH, ACK] Seq=251 Ack=56 Win=16384 Len=0 TSval=1657398000 TSecr=1657568500
25 8.197050	10.20.144.151	10.20.144.150	FTP	106 Response: 257 "CDTS3500" is current library.
26 8.197280	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=56 Ack=287 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
27 20.765720	10.20.144.150	10.20.144.151	FTP	72 Request: PASV
28 20.766000	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [PSH, ACK] Seq=287 Ack=62 Win=16384 Len=0 TSval=1657410500 TSecr=1657581000
29 20.787770	10.20.144.151	10.20.144.150	FTP	121 Response: 227 Entering Passive Mode (10,20,144,151,62,141).
30 20.788010	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=62 Ack=338 Win=32648 Len=0 TSval=1657581000 TSecr=1657410500

La trace ne tenant pas sur une seule page, la suite vous est donnée page suivante, seule la trame 30 est commune aux deux images, c'est juste pour faire le lien.

30 20.788010	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=62 Ack=338 Win=32648 Len=0 TSval=1657581000 TSecr=1657410500
31 20.797560	10.20.144.150	10.20.144.151	TCP	74 35976 → 16013 [SYN] Seq=0 Win=32768 Len=0 MSS=1380 WS=1 TSval=1657581000 TSecr=0
32 20.797850	10.20.144.151	10.20.144.150	TCP	78 16013 → 35976 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1356 WS=1 TSval=1657410500 TSecr=1657581000
33 20.798130	10.20.144.150	10.20.144.151	TCP	66 35976 → 16013 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=1657581000 TSecr=1657410500
34 20.798250	10.20.144.150	10.20.144.151	FTP	91 Request: RETR qgpl/apkeyf.apkeyf
35 20.798450	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [PSH, ACK] Seq=338 Ack=87 Win=16384 Len=0 TSval=1657410500 TSecr=1657581000
36 21.202190	10.20.144.151	10.20.144.150	FTP	132 Response: 150 Retrieving member APKEYF in file APKEYF in library QGPL.
37 21.202460	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=87 Ack=400 Win=32648 Len=0 TSval=1657581500 TSecr=1657411000
38 21.313290	10.20.144.151	10.20.144.150	FTP-DA..	509 FTP Data: 439 bytes (PASV) (RETR qgpl/apkeyf.apkeyf)
39 21.393980	10.20.144.151	10.20.144.150	TCP	70 16013 → 35976 [FIN, PSH, ACK] Seq=440 Ack=1 Win=32768 Len=0 TSval=1657411500 TSecr=1657581000
40 21.394160	10.20.144.151	10.20.144.150	FTP	113 Response: 250 File transfer completed successfully.
41 21.394310	10.20.144.150	10.20.144.151	TCP	66 35976 → 16013 [ACK] Seq=1 Ack=441 Win=32768 Len=0 TSval=1657581500 TSecr=1657411500
42 21.394430	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=87 Ack=443 Win=32648 Len=0 TSval=1657581500 TSecr=1657411500
43 22.169470	10.20.144.150	10.20.144.151	TCP	66 35976 → 16013 [FIN, PSH, ACK] Seq=1 Ack=441 Win=32768 Len=0 TSval=1657582500 TSecr=1657411500
44 22.169800	10.20.144.151	10.20.144.150	TCP	70 16013 → 35976 [PSH, ACK] Seq=441 Ack=2 Win=32768 Len=0 TSval=1657412000 TSecr=1657582500
45 31.007220	10.20.144.150	10.20.144.151	FTP	72 Request: QUIT
46 31.007560	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [PSH, ACK] Seq=443 Ack=93 Win=16384 Len=0 TSval=1657421000 TSecr=1657591500
47 31.007750	10.20.144.151	10.20.144.150	FTP	101 Response: 221 QUIT subcommand received.
48 31.007830	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [FIN, PSH, ACK] Seq=474 Ack=93 Win=16384 Len=0 TSval=1657421000 TSecr=1657591500
49 31.008000	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=93 Ack=474 Win=32648 Len=0 TSval=1657591500 TSecr=1657421000
50 31.008810	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [FIN, PSH, ACK] Seq=93 Ack=474 Win=32648 Len=0 TSval=1657591500 TSecr=1657421000
51 31.008840	10.20.144.150	10.20.144.151	TCP	66 35974 → 21 [PSH, ACK] Seq=94 Ack=475 Win=32648 Len=0 TSval=1657591500 TSecr=1657421000
52 31.009050	10.20.144.151	10.20.144.150	TCP	70 21 → 35974 [PSH, ACK] Seq=475 Ack=94 Win=16384 Len=0 TSval=1657421000 TSecr=1657591500

Pour vous aider, on donne aussi une vue très résumée des échanges sur les différentes connexions :

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.20.144.150	35974	10.20.144.151	21	44	3569		23	1618		21	1951	0.000000	31.0090
10.20.144.150	35976	10.20.144.151	16013	8	999		4	272		4	727	20.797560	1.3722

Question 1 : Dans la trace deux ouvertures de connections TCP peuvent être observées ? Donner le numéro de la trame, pour chaque connexion où la demande d'ouverture de connexion est initialisée. Comment reconnaissiez vous que ce sont des ouvertures de connexion ? Ces connexions sont-elles complètes, c'est-à-dire sont-elles bien fermées dans la trace ? (**2 points**)

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de regraphie le cas échéant.

Numéro de copie :

Question 2 : Pour chaque connexion dans la trace, quelle est l'adresse IP et le numéro de port de l'application qui initie la connexion ? **(1 point)**

Question 3 : Pour chaque connexion dans la trace, quelle est l'adresse IP et le numéro de port de l'application qui accepte l'ouverture de connexion ? **(1 point)**

On s'intéresse en particulier à la trame 31.

No.	Time	Source	Destination	Protocol	Length	Info
31	20.797560	10.20.144.150	10.20.144.151	TCP	74	35976 → 16013 [SYN] Seq=0 Win=32768 Len=0 MSS=1380 WS=1 TSval=1657581000 TSecr=0
32	20.797850	10.20.144.151	10.20.144.150	TCP	78	16013 → 35976 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1356 WS=1 TSval=1657410500 TSecr=1657581000
33	20.798130	10.20.144.150	10.20.144.151	TCP	66	35976 → 16013 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=1657581000 TSecr=1657410500

► Frame 31: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

▼ Ethernet II, Src: IbmRisc6_9c:14:fe (00:06:29:9c:14:fe), Dst: IbmRisc6_9c:14:ae (00:06:29:9c:14:ae)

- Destination: IbmRisc6_9c:14:ae (00:06:29:9c:14:ae)
- Source: IbmRisc6_9c:14:fe (00:06:29:9c:14:fe)
- Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 10.20.144.150, Dst: 10.20.144.151

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 60
- Identification: 0x2d80 (11648)
- Flags: 0x4000, Don't fragment
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0xd7e6 [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.20.144.150
- Destination: 10.20.144.151

▼ Transmission Control Protocol, Src Port: 35976, Dst Port: 16013, Seq: 0, Len: 0

- Source Port: 35976
- Destination Port: 16013
- [Stream index: 1]
- [TCP Segment Len: 0]
- Sequence number: 0 (relative sequence number)
- [Next sequence number: 0 (relative sequence number)]
- Acknowledgment number: 0
- 1010 = Header Length: 40 bytes (10)
- Flags: 0x002 (SYN)
- Window size value: 32768
- [Calculated window size: 32768]
- Checksum: 0x2e86 [unverified]

0000	00	06	29	9c	14	ae	00	06	29	9c	14	fe	08	00	45	00	..))	E
0010	00	3c	2d	80	40	00	40	06	d7	e6	0a	14	90	96	0a	14	<-	@	@	
0020	90	97	8c	88	3e	8d	01	f9	8b	d8	00	00	00	00	a0	02	..	>	
0030	80	00	2c	86	00	00	02	04	05	64	01	03	03	00	01	01	..	,	d	
0040	08	0a	62	cc	ad	c8	00	00	00	00	00	00	00	00	00	00	.	b	

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de regraphie le cas échéant.
Numéro de copie :

Question 4 : Analyse de trame (4 points)

- Délimiter l'entête de la trame Ethernet dans la capture en hexadécimal ci-dessous. (**0,25 point**)
- Délimiter l'entête du datagramme IP dans la capture en hexadécimal ci-dessous. (**0,25 point**)
- Délimiter l'entête du segment TCP dans la capture en hexadécimal ci-dessous. (**0,25 point**)

Ne pas hésiter à utiliser des couleurs différentes pour que votre réponse soit facile à lire.

0000 00 06 29 9c 14 ae .00 06 29 9c 14 fe 08 00 45 00

0010 00 3c 2d 80 40 00 40 06 d7 e6 0a 14 90 96 0a 14

0020 90 97 8c 88 3e 8d 01 f9 8b d8 00 00 00 00 a0 02

0030 80 00 2c 86 00 00 02 04 05 64 01 03 03 00 01 01

0040 08 0a 62 cc ad c8 00 00 00 00

Attention la colonne la plus à gauche numérote les lignes et cette numérotation est hexadécimale.

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.[_](#)

Numéro de copie :

8/15

Retrouver les champs suivants dans la trace hexadécimale ci-dessus :

- Quelle est l'adresse Ethernet destination en **hexadécimal** ? (**0,25 point**)
- Quelle est l'adresse Ethernet source en **hexadécimal** ? (**0,25 point**)
- Quel est le type de la trame en **hexadécimal** ? (**0,25 point**)
- Quelle est la version du protocole IP en **décimal** ? (**0,25 point**)
- Quelle est la longueur de l'entête IP en **décimal** ? (**0,25 point**)
- Quelle est l'adresse IP source en **hexadécimal** ? (**0,25 point**)
- Quelle est l'adresse IP destination en **hexadécimal** ? (**0,25 point**)
- Quel est le numéro du protocole indiqué par l'entête IP et transporté dans la charge utile du datagramme IP en **héxadécimal**, c'est TCP ou UDP ? (**0,25 point**)
- Quelle est la longueur totale du datagramme **en décimal** ? (**0,25 point**)
- Quel est le numéro de port source en **héxadécimal** ? (**0,25 point**)
- Quel est le numéro de port destination en **héxadécimal** ? (**0,25 point**)
- Quel est la valeur du numéro de séquence absolu dans l'entête TCP en **hexadécimal** ? (**0,25 point**)
- Quel est le seul "flag" positionné dans l'entête TCP ? (**0,25 point**)

Question 5 : On vous donne aussi le graphe synthétique des échanges ci-après. On a placé sur le graphe, autant de fois que nécessaire, les appels systèmes de l'API socket (en langage C pour une machine de type Unix). Y a-t-il des erreurs à propos de l'usage de ces primitives et au rôle client ou serveur, si oui, lesquelles, proposer une correction. Justifier brièvement votre réponse. **(2 points)**



➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de regraphie le cas échéant.

Numéro de copie :

10/15

Question 6 : Le texte ci-dessous représente des échanges entre le client et le serveur. Ce sont des échanges protocolaires de la couche 7 du modèle OSI. Commenter ce qui se passe entre le client et le serveur. (**1 point**)

```
220-QTCP at fran.csg.stercomm.com.  
220 Connection will close if idle more than 5 minutes.  
USER cdts3500  
331 Enter password.  
PASS cdts3500  
230 CDT3500 logged on.  
SYST  
215 OS/400 is the remote operating system. The TCP/IP version is "V5R2M0".  
SITE NAMEFMT  
250 Now using naming format "0".  
PWD  
257 "CDTS3500" is current library.  
PASV  
227 Entering Passive Mode (10,20,144,151,62,141).  
RETR qgpl/apkeyf.apkeyf  
150 Retrieving member APKEYF in file APKEYF in library QGPL.  
250 File transfer completed successfully.  
QUIT  
221 QUIT subcommand received.
```

Question 7 : Combien d'octets échangés pour chaque sens dans la connexion la plus interne qui démarre au temps $t=20.797560\text{ms}$, qui se termine au temps $t=22.169800\text{ms}$ dans le graphe. Cet échange est, d'ailleurs, marqué en couleur rosée dans le graphe des échanges. Expliquer votre raisonnement. **(2 points)**

On vous donne l'extrait du résultat de la commande `ipconfig` sur l'équipement d'adresse IP 10.20.144.150 :

Carte Ethernet Connexion au réseau local filaire eth0 :

```
Suffixe DNS propre à la connexion. . . : mbi.moc
Adresse IPv4. . . . . : 10.20.144.150
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 10.20.144.202
```

Carte réseau sans fil Connexion réseau sans fil wif0 :

```
Suffixe DNS propre à la connexion. . . : mbi.moc
Adresse IPv4. . . . . : 10.30.144.050
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 10.30.144.252
```

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

Question 8 : Paramètres de configuration de l'équipement (**1 point**)

- Donner la notation compacte pour le masque en /n. (**0,25 point**)
- Donner l'adresse de réseau IP associée correspondant à chacune des interfaces. (**0,25 point**)
- Donner l'adresse IP du routeur associé pour chacun des réseaux IP auxquels ces interfaces appartiennent. (**0,25 point**)
- Donner l'adresse de diffusion associée à chacun des réseaux IP apparaissant dans les résultats ci-dessus. (**0,25 point**)

Question 9 : Quand l'équipement met en fonctionnement uniquement sa carte Ethernet on a la table de routage locale suivante active:

	Réseau/mask	Next hop	métrique	accessibilité	interface
I1	0.0.0.0/0	10.20.144.202	10	distant	eth0
I2	127.0.0.0/8	0.0.0.0	0	direct	lo0
I3	10.20.0.0/16	0.0.0.0	0	direct	eth0

Quelle ligne de la table de routage emprunte le datagramme d'adresse IP destination 10.30.144.10 pour sortir du routeur et atteindre cette destination ? Expliquez brièvement votre réponse. (**1 point**)

Question 10 : En reprenant la trame 31, que se passe-t-il si le datagramme doit être fragmenté lors de la traversée du routeur ? (**1 point**)

Exercice 2 : Question de cours (3 points)

1. Expliquez sommairement la différence entre SEM et TSCM. Pour chacun, fournir un exemple concret de problème repéré par ces actions de surveillance.

2. Pourquoi a-t-on besoin de faire certifier les clés publiques en cryptographie à clé publique ?

3. Pourquoi est-ce inutile en cryptographie symétrique ? Dans ce cas, expliquez comment on s'assure d'utiliser la bonne clé.

Exercice 3 : Sécurité inconditionnelle (2 points)

La sécurité inconditionnelle du masque à usage unique a été expliquée en cours via un exemple où l'on chiffre le message « SECRET » avec la clé « XOSAUF » pour obtenir « PSURYY ». À partir du moment où l'algorithme est respecté, et donc où la clé de chiffrement a été irrémédiablement détruite immédiatement après utilisation, le cryptogramme « PSURYY » est indéchiffrable, quel que soit le temps et la puissance informatique qu'on y consacre.

Expliquez pourquoi ce système est inconditionnellement sûr, en français compréhensible (pas d'équation mathématique) et 6 lignes au maximum.