SUJET UTC505 : Introduction à la cyberstructure de l'Internet

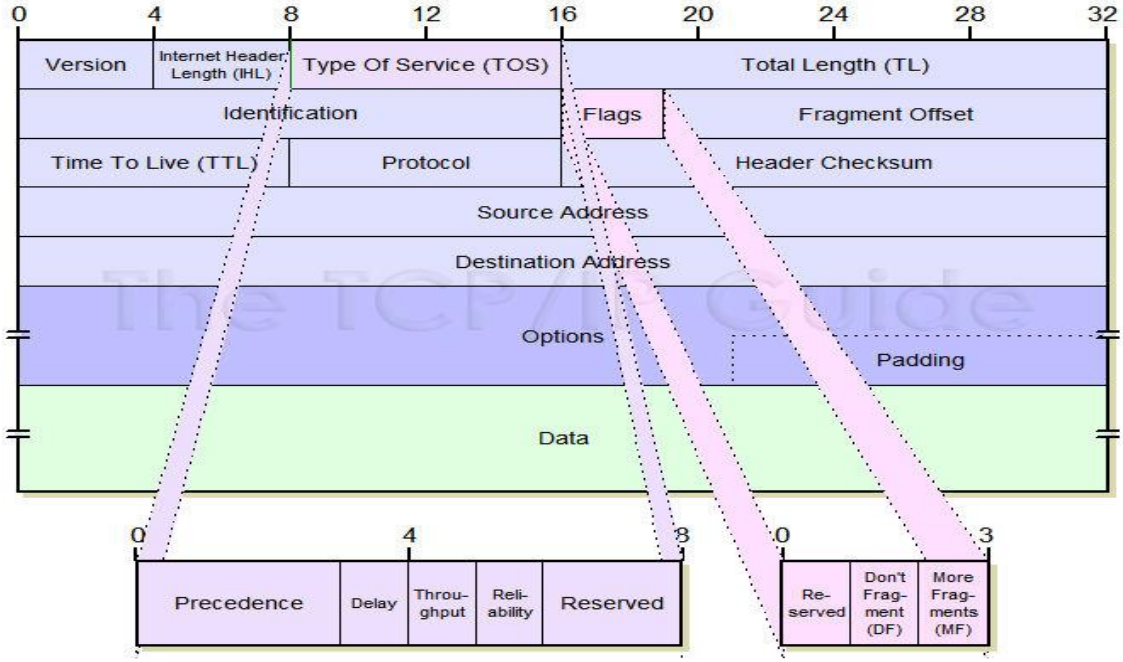
Session 2023

Exercice 1 (9 points) :

On donne la structure d'une trame Ethernet :

Adresse Dest	Adresse Src	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



la structure d'un segment TCP dont l'entête en détail :

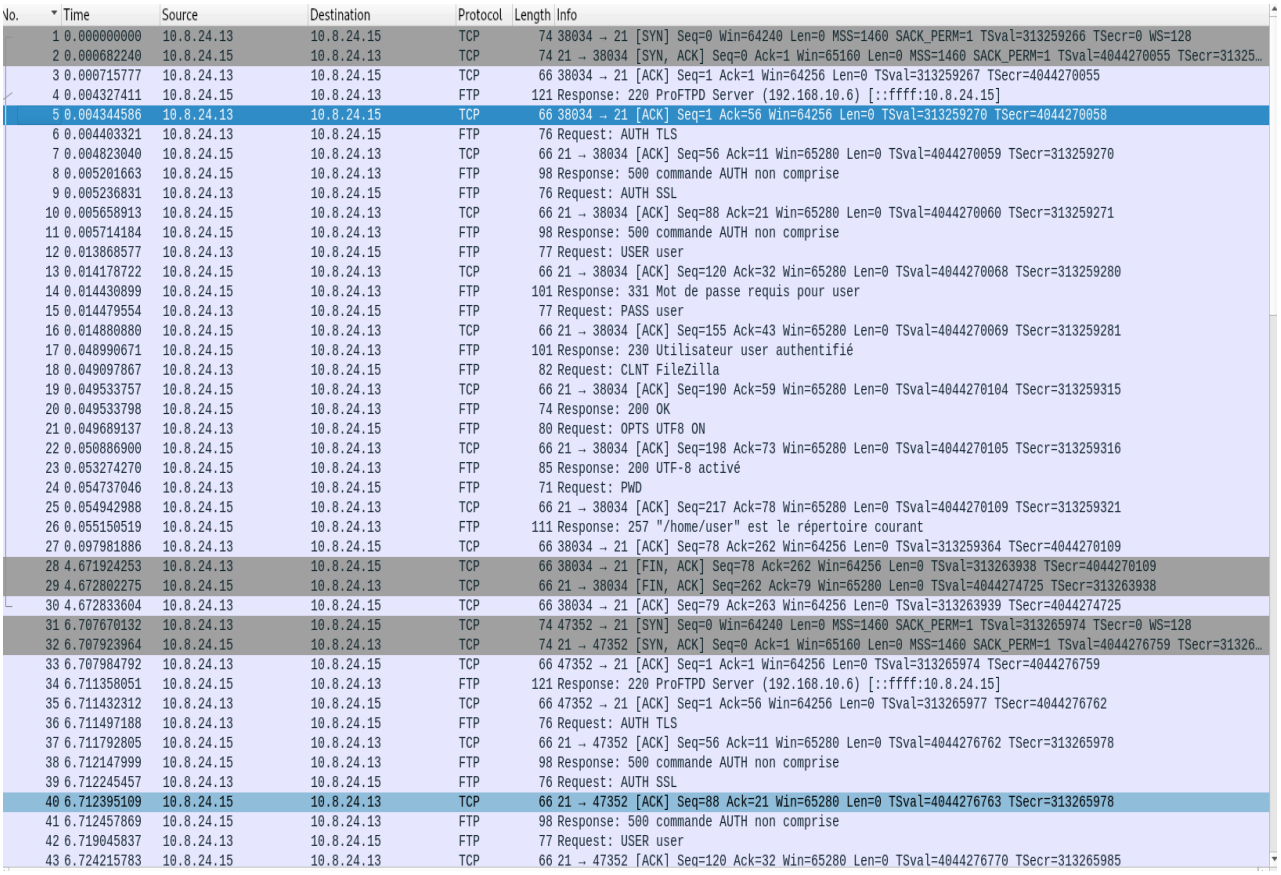
TCP Header

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				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	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.



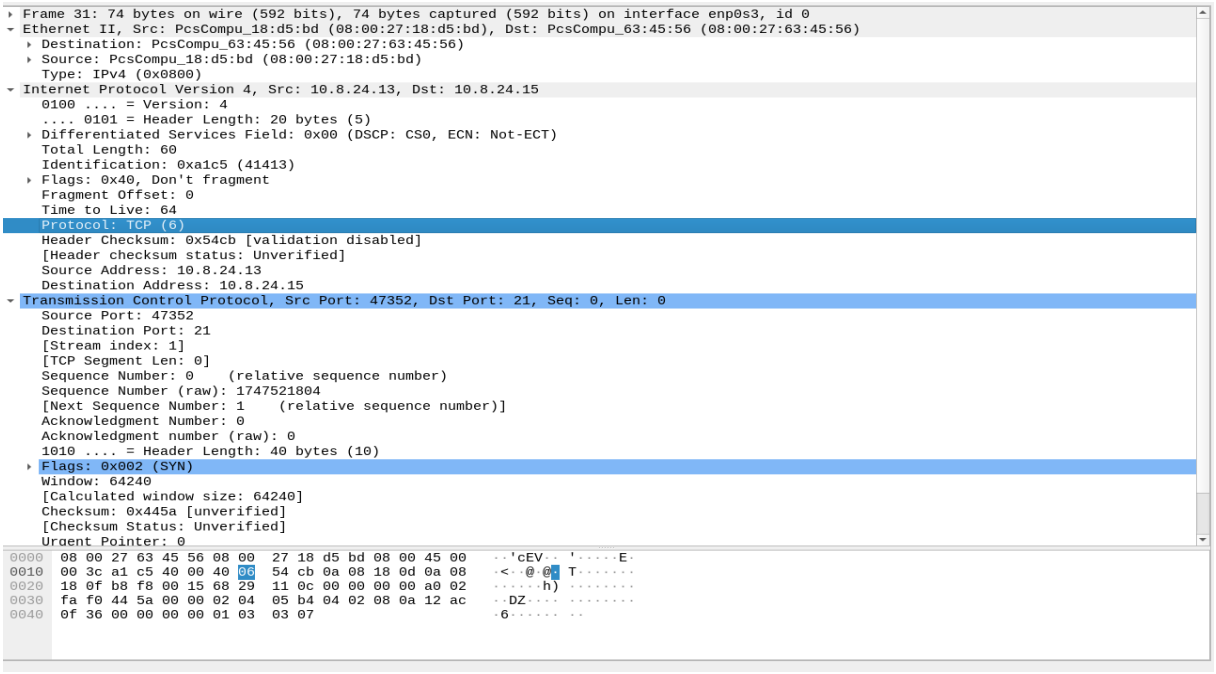
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.8.24.13	10.8.24.15	TCP	74	38034 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=313259266 TSecr=0 WS=128
2	0.000682240	10.8.24.15	10.8.24.13	TCP	74	21 → 38034 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4044270055 TSecr=31325…
3	0.000715777	10.8.24.13	10.8.24.15	TCP	66	38034 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=313259267 TSecr=4044270055
4	0.004327411	10.8.24.15	10.8.24.13	FTP	121	Response: 220 ProFTPD Server (192.168.10.6) [::ffff:10.8.24.15]
5	0.004344586	10.8.24.13	10.8.24.15	TCP	66	38034 → 21 [ACK] Seq=1 Ack=56 Win=64256 Len=0 TSval=313259270 TSecr=4044270058
6	0.004403321	10.8.24.13	10.8.24.15	FTP	76	Request: AUTH TLS
7	0.004823040	10.8.24.15	10.8.24.13	TCP	66	21 → 38034 [ACK] Seq=56 Ack=11 Win=65280 Len=0 TSval=4044270059 TSecr=313259270
8	0.005201663	10.8.24.15	10.8.24.13	FTP	98	Response: 500 commande AUTH non comprise
9	0.005236831	10.8.24.13	10.8.24.15	FTP	76	Request: AUTH SSL
10	0.005658913	10.8.24.15	10.8.24.13	TCP	66	21 → 38034 [ACK] Seq=88 Ack=21 Win=65280 Len=0 TSval=4044270060 TSecr=313259271
11	0.005714184	10.8.24.15	10.8.24.13	FTP	98	Response: 500 commande AUTH non comprise
12	0.013868577	10.8.24.13	10.8.24.15	FTP	77	Request: USER user
13	0.014178722	10.8.24.15	10.8.24.13	TCP	66	21 → 38034 [ACK] Seq=120 Ack=32 Win=65280 Len=0 TSval=4044270068 TSecr=313259280
14	0.014430899	10.8.24.15	10.8.24.13	FTP	101	Response: 331 Mot de passe requis pour user
15	0.014479554	10.8.24.13	10.8.24.15	FTP	77	Request: PASS user
16	0.014880880	10.8.24.15	10.8.24.13	TCP	66	21 → 38034 [ACK] Seq=155 Ack=43 Win=65280 Len=0 TSval=4044270069 TSecr=313259281
17	0.048990671	10.8.24.15	10.8.24.13	FTP	101	Response: 230 Utilisateur user authentifié
18	0.049097867	10.8.24.13	10.8.24.15	FTP	82	Request: CLNT FileZilla
19	0.049533757	10.8.24.15	10.8.24.13	TCP	66	21 → 38034 [ACK] Seq=190 Ack=59 Win=65280 Len=0 TSval=4044270104 TSecr=313259315
20	0.049533798	10.8.24.15	10.8.24.13	FTP	74	Response: 200 OK
21	0.049689137	10.8.24.13	10.8.24.15	FTP	80	Request: OPTS UTF8 ON
22	0.050886900	10.8.24.15	10.8.24.13	TCP	66	21 → 38034 [ACK] Seq=198 Ack=73 Win=65280 Len=0 TSval=4044270105 TSecr=313259316
23	0.053274270	10.8.24.15	10.8.24.13	FTP	85	Response: 200 UTF-8 activé
24	0.054737046	10.8.24.13	10.8.24.15	FTP	71	Request: PWD
25	0.054942988	10.8.24.15	10.8.24.13	TCP	66	21 → 38034 [ACK] Seq=217 Ack=78 Win=65280 Len=0 TSval=4044270109 TSecr=313259321
26	0.055150519	10.8.24.15	10.8.24.13	FTP	111	Response: 257 "/home/user" est le répertoire courant
27	0.097981886	10.8.24.13	10.8.24.15	TCP	66	38034 → 21 [ACK] Seq=78 Ack=262 Win=64256 Len=0 TSval=313259364 TSecr=4044270109
28	4.671924253	10.8.24.13	10.8.24.15	TCP	66	38034 → 21 [FIN, ACK] Seq=78 Ack=262 Win=64256 Len=0 TSval=313263938 TSecr=4044270109
29	4.672802275	10.8.24.15	10.8.24.13	TCP	66	21 → 38034 [FIN, ACK] Seq=262 Ack=79 Win=65280 Len=0 TSval=4044274725 TSecr=313263938
30	4.672833604	10.8.24.13	10.8.24.15	TCP	66	38034 → 21 [ACK] Seq=79 Ack=263 Win=64256 Len=0 TSval=313263939 TSecr=4044274725
31	6.707670132	10.8.24.13	10.8.24.15	TCP	74	47352 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=313265974 TSecr=0 WS=128
32	6.707923964	10.8.24.15	10.8.24.13	TCP	74	21 → 47352 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4044276759 TSecr=31326…
33	6.707984792	10.8.24.13	10.8.24.15	TCP	66	47352 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=313265974 TSecr=4044276759
34	6.711358051	10.8.24.15	10.8.24.13	FTP	121	Response: 220 ProFTPD Server (192.168.10.6) [::ffff:10.8.24.15]
35	6.711432312	10.8.24.13	10.8.24.15	TCP	66	47352 → 21 [ACK] Seq=1 Ack=56 Win=64256 Len=0 TSval=313265977 TSecr=4044276762
36	6.711497188	10.8.24.13	10.8.24.15	FTP	76	Request: AUTH TLS
37	6.711792805	10.8.24.15	10.8.24.13	TCP	66	21 → 47352 [ACK] Seq=56 Ack=11 Win=65280 Len=0 TSval=4044276762 TSecr=313265978
38	6.712147999	10.8.24.15	10.8.24.13	FTP	98	Response: 500 commande AUTH non comprise
39	6.712245457	10.8.24.13	10.8.24.15	FTP	76	Request: AUTH SSL
40	6.712395109	10.8.24.15	10.8.24.13	TCP	66	21 → 47352 [ACK] Seq=88 Ack=21 Win=65280 Len=0 TSval=4044276763 TSecr=313265978
41	6.712457869	10.8.24.15	10.8.24.13	FTP	98	Response: 500 commande AUTH non comprise
42	6.719045837	10.8.24.13	10.8.24.15	FTP	77	Request: USER user
43	6.724215783	10.8.24.15	10.8.24.13	TCP	66	21 → 47352 [ACK] Seq=120 Ack=32 Win=65280 Len=0 TSval=4044276770 TSecr=313265985

Question 1 : Dans la trace des ouvertures de connections TCP peuvent être observée. Donner le numéro dess trame où la demande d'ouverture de connexion est initialisée. Comment reconnaissez-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**)

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 :



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  08 00 27 63 45 56 08 00  27 18 d5 bd 08 00 45 00
0010  00 3c a1 c5 40 00 40 06  54 cb 0a 08 18 0d 0a 08
0020  18 0f b8 f8 00 15 68 29  11 0c 00 00 00 00 a0 02
0030  fa f0 44 5a 00 00 02 04  05 b4 04 02 08 0a 12 ac
0040  0f 36 00 00 00 00 01 03  03 07
```

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

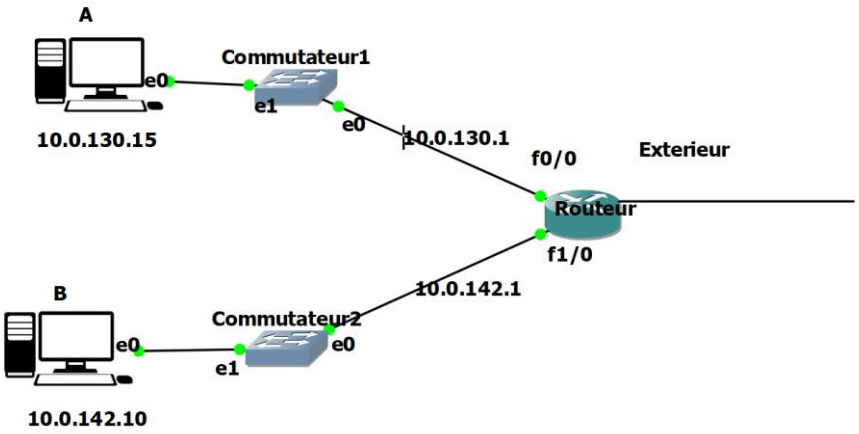
Retrouver les champs suivants dans la trace hexadécimale ci-dessus :

- 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 : 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 : Routage Adressage (**5 points**)
Pour une expérimentation on a construit un réseau très simple en utilisant le bloc d'adresses IPV4 10.0.0.0/16. C'est une plage d'adresses définie dans la RFC1918, adresses privées non routables.



Dans la configuration, on a un routeur qui relie deux réseaux locaux Ethernet au moyen de deux ports/interfaces notés sur la figure f0/0 et f1/0.

- Une machine A, connectée au réseau local Ethernet raccordé par l'interface f0/0 du routeur a pour sa carte réseau, l'adresse 10.0.130.15.

- Une machine B, connecté au réseau local Ethernet raccordé par l'interface f1/0 du routeur, à l'adresse 10.0.142.10.

On a défini, pour les deux sous réseaux IP (les équipements connectés au commutateur 1 comme A et au commutateur 2 comme B) le même masque 255.255.128.0.

Question 1 : Quelle est la notation du masque 255.255.128.0 en notation compacte, c'est-à dire en /n ? (**0,25 point**)

Question 2 : Combien d'interfaces peut contenir un réseau avec un tel masque ? (**0,25 point**)

Question 3 : Quelle est l'adresse IP du réseau auquel A appartient ? (**0,25 point**)

Question 4 : Quelle est l'adresse de diffusion du réseau auquel A appartient ? (**0,25 point**)

Question 5 Quelle est la table de routage de A sachant qu'elle contient au moins le réseau loopback (réseau uniquement de la machine, 127.0.0.0/8), et la route par défaut ? (**1 point**)

Question 6 A émet un message vers B en utilisant sa table de routage. Expliquez ce qui se passe en particulier si un datagramme parti de A arrive à atteindre B. (**1 point**)

Question 7 : Est-ce que A et B appartiennent au même sous-réseau IP ? Si oui, dans l'hypothèse où on doit corriger le masque, on ne souhaite pas changer les adresses IP des machines du réseau. Quel serait le bon masque pour que cela soit 2 sous-réseaux IP différents. Le "bon masque" est à interpréter comme "masque qui permet d'avoir le plus de numéros d'interface possibles". (**2 points**)

Exercice 3 : (6 points)

Question 1 : Amélie reçoit un appel téléphonique d'une personne qui prétend représenter des services informatiques et qui lui demande de confirmer son nom d'utilisateur et son mot de passe à des fins d'audit. Quelle menace cet appel téléphonique représente-t-il pour la sécurité ? Justifiez votre réponse **(1 point)**

- Manipulation psychologique
- Courrier indésirable
- DDoS
- Enregistrement anonyme des frappes

Question 2 : Dans cette question on demande aux étudiants de répondre de manière très précise à chacune des questions. Chaque réponse sera accompagnée de deux ou trois phrases d'argumentation

1) Définir la cryptographie asymétrique. Quel sont ses avantages/désavantages par rapport à la cryptographie symétrique ? **(1 point)**

2) Est-ce que les affirmations suivantes sont-elles vraies **(1 point)**
   - Ma clé publique peut être distribuée à tous mes correspondants ou seulement le destinataire de mon message.
   - Pour envoyer un message confidentiel, je le chiffre avec la clé publique ou la clé privée de mes correspondant

3) Quel est le rôle central en cryptographie de Diffie-Hellman ? **(1 point)**

4) A quoi sert un certificat ? Pourquoi toujours avoir une date limite de validité ? Que sont les algorithmes dont il est question ? **(1 point)**

5) Citez trois algorithmes de chiffrement asymétriques ? quelle est l'algorithme le plus utilisé actuellement ? **(1 point)**