Exercices dirigés

UTC505/USRS4D
-Introduction-

E. Gressier-Soudan

2021-2022

Ce polycopié a été élaboré par l'équipe enseignante "Réseaux et protocoles" à partir d'exercices rédigés par MM. Berthelin, Florin, Gressier-Soudan qu'ils en soient ici remerciés.

ED•Encapsulation et Les 7 couches de protocoles

Après l'exercice 0, cet ED a pour but d'introduire les différentes couches protocolaires et leur rôle. Mais surtout faire découvrir le mécanisme d'encapsulation qui est fondamental et dont on se servira pendant toutes les séances ou presque. Les couches et l'encapsulation sont indissociables.

Exercice 0 : Explorer les différents échanges pour des protocoles bien connus, plus facile à faire avec l'environnement de conteneurs mis à disposition ou avec une machine Linux (exercice facultatif)

- Résolution de nom via le DNS avec la commande dig www.cnam.fr, que se passe-t-il ? pourquoi a-t-on besoin d'une traduction adresse IP-nom de machine ? garder en mémoire le nom de machine rendu par dig www.cnam.fr, appellons le nnn. On peut essayer le DNS aussi avec dig :
  - dig f.root-servers.net NS fr.

    pour avoir la liste des serveurs racine du domaine ".fr" tels qu'ils sont connus des serveurs racine
  - dig -6 k.root-servers.net . ns +bufsize=1024

    pour sortir les adresses IPv6
  - on peut essayer avec l'indicateur "aa" pour avoir la réponse provenant du serveur faisant autorité
- telnet www.cnam.fr 80 en utilisant, et en faisant un GET / http/1.0 puis 2 return successifs. Essayer avec GET / sans paramètres. Puis refaire la même chose pour telnet vers sarek.cnam.fr. Vous venez d'exécuter un protocole de communication simple, que se passe-t-il ?

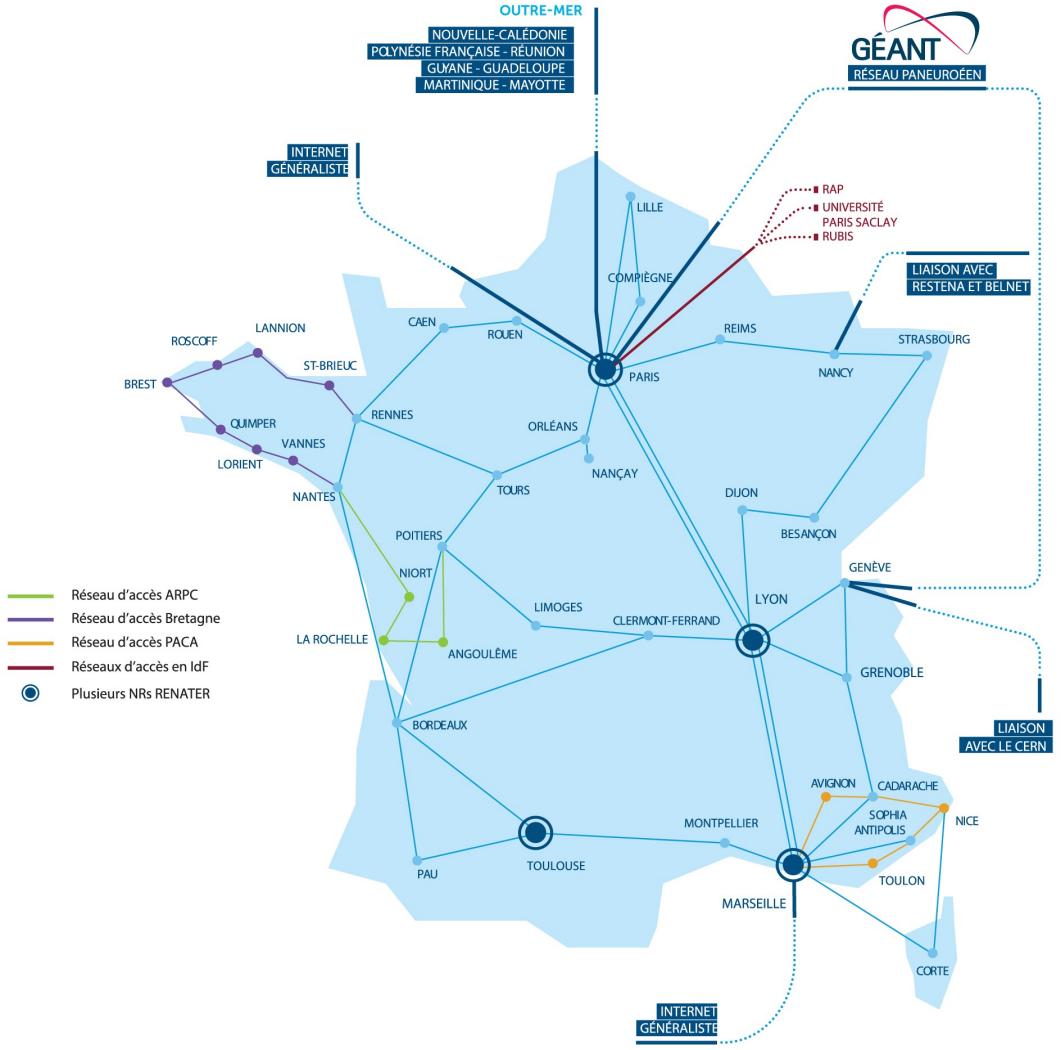
Comment matérialiser les couches d'acheminement d'information

- ping www.cnam.fr, fournit un temps réponse (délai A/R)
- Montrer un chemin entre 2 points de l'Internet depuis votre pc par la commande `traceroute` sous linux et la commande `tracert` sous windows. Et essayer depuis un site externe http://hax.at/trace/trace.php vers votre machine. Quel est votre premier intermédiaire pour aller plus à l'intérieur du cnam depuis la salle de TP ou depuis chez vous ? Quelle adresse IP de cet équipement trouve-t-on dans les deux cas ? Faire un traceroute www.cnam.fr, et retrouver certains réseaux et routeurs à partir de la carte http://www.rap.prd.fr/ressources/nagios.php.

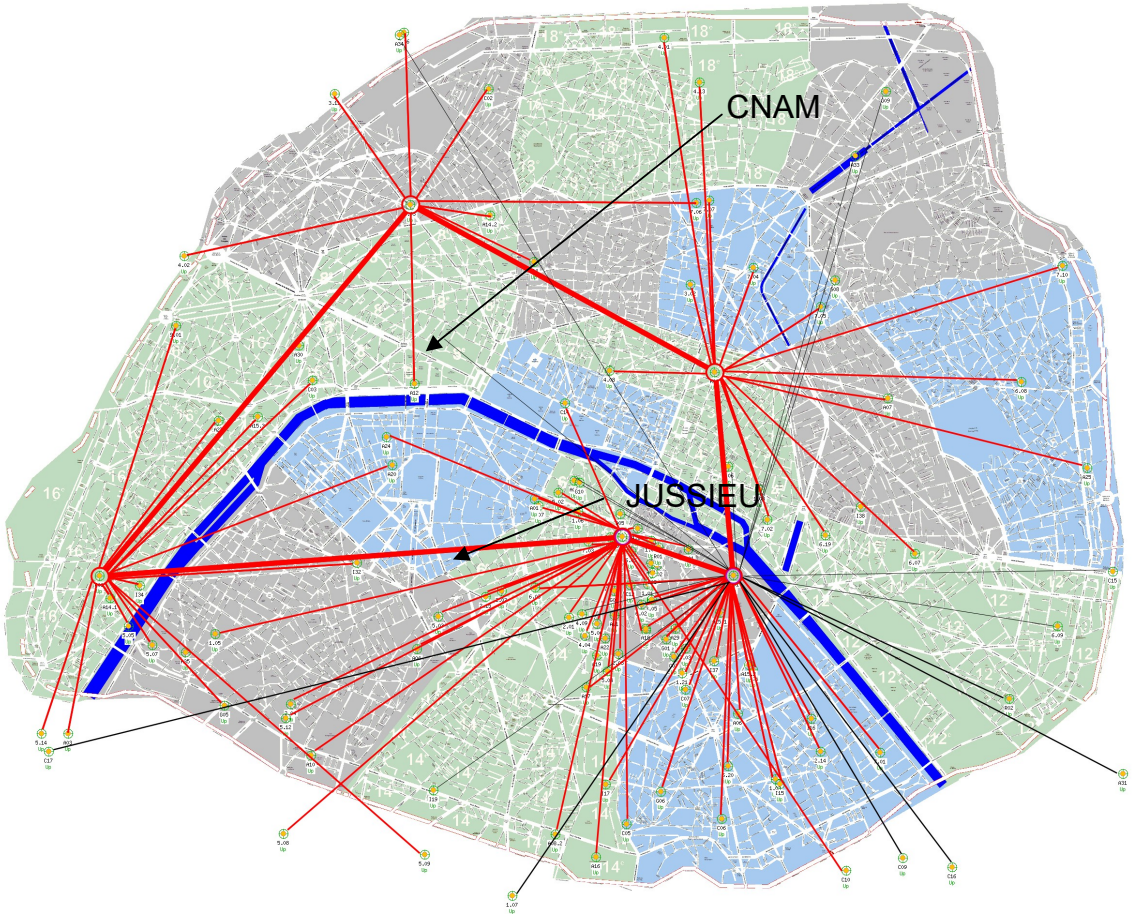
  On peut essayer vers d'autres machines (liste susceptible d'avoir des adresses invalides): www.kyoto-u.ac.jp, www.ru.ac.za,

www.usp.ac.fj, www.mcmurdo.usap.gov

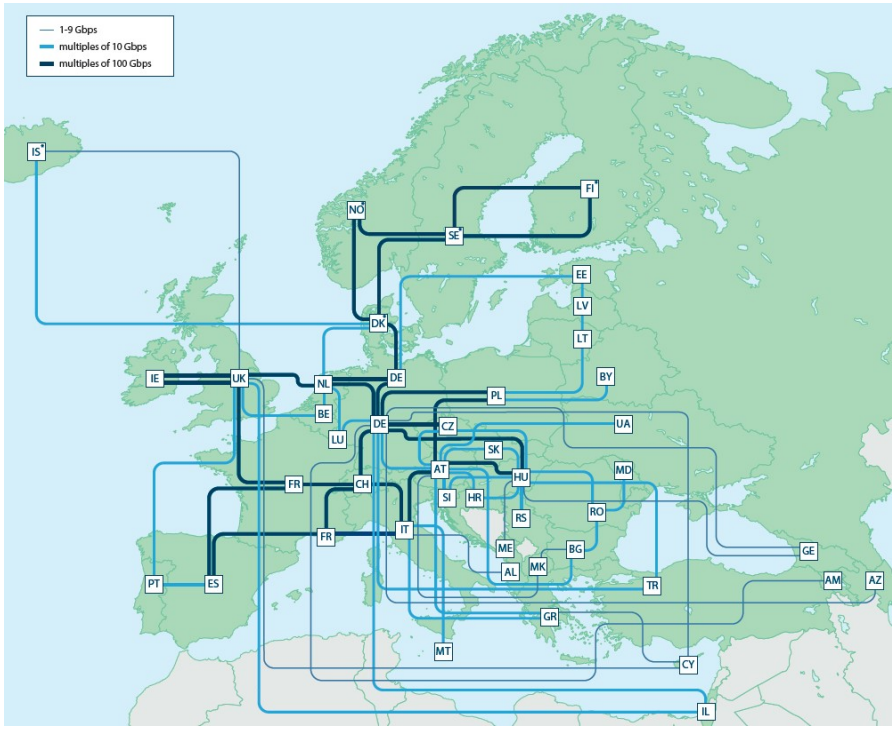
Pour obtenir des informations sur la topologie du réseau RENATER auquel le cnam paris est relié, accéder à https://www.renater.fr/fr/reseau (accédée le 11/02/2020 15h30).



Pour le réseau académique parisien (RAP), la carte peut être consultée à http://www.rap.prd.fr/images/carteRAP.png (accédée le 11/02/2020 à 15h35).

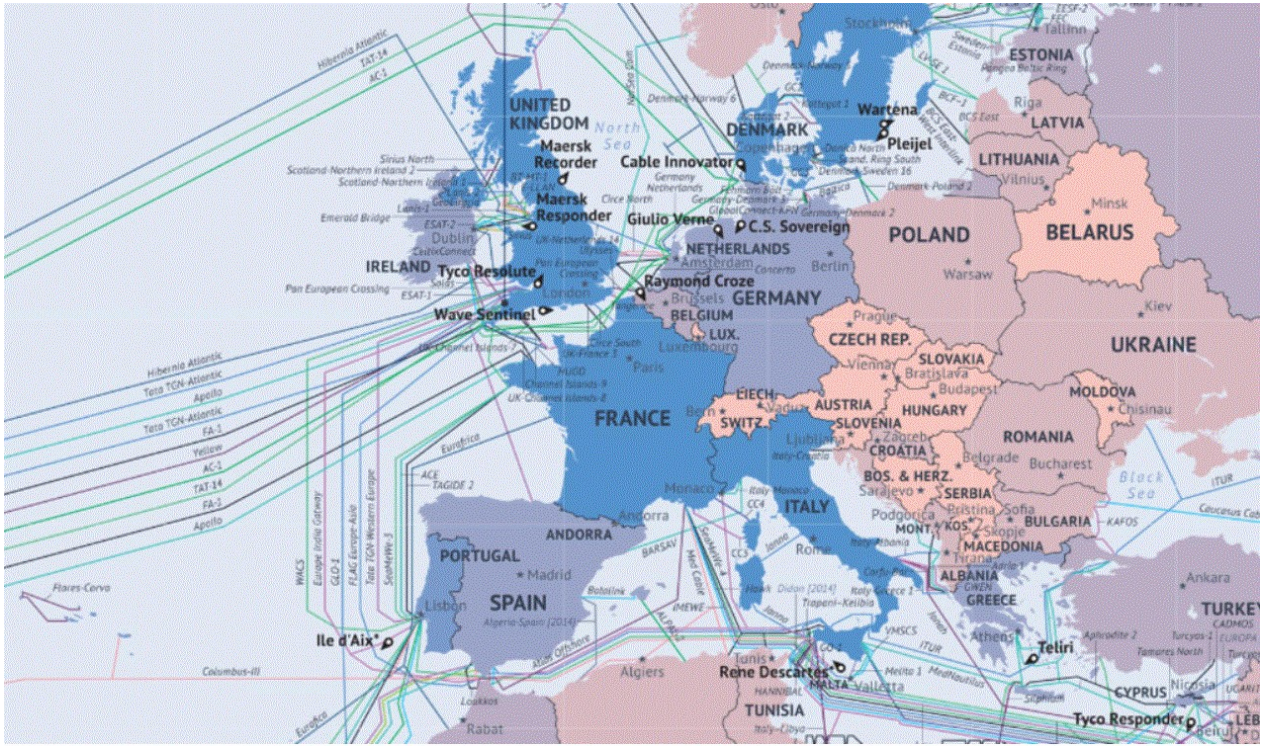


Pour obtenir des informations sur la topologie du réseau d'interconnexion européen geant auquel renater est relié aller voir https://www.geant.org/Networks/Pan-European_network/Documents/GEANT_Topology_Map_December_2018.pdf,(consulté le 11/02/2020 à 15h55)



Et pour l'interconnexion de géant avec les autres continents : https://geant3plus.archive.geant.net/Resources/Media_Library/PublishingImages/maps/GEANT_Project_Global_Connectivity_Sep14_Web_Hi_Res.jpg , consulté le 11/02/2020 à 16h15.

Pour avoir une idée des connexions sous-marines à partir de l'europe, voir la carte au lien https://edition.cnn.com/2014/03/04/tech/gallery/internet-undersea-cables/index.html (consultée le 11/02/2020 à 15h45). Il y a au total 11 cartes qui donnent une idée de la connectivité sous-marine entre tous les continents.



- `ipconfig/all` sous windows ou `ifconfig -a` sous linux, que montre cette commande ?
- `arp -a` que montre cette commande, à quoi sert cette correspondance d'adresses ?
- Accès à la table de routage d'un hôte : `route -n`, éliminer une route avec la commande `del` associée à route, trouver les bons paramètres de la commande.
- Que montre la commande `netstat -a` ? A quoi peuvent correpondre les lignes qui démarrent par TCP ou UDP ou AF_UNIX ? `netstat -at` pour ne récupérer que les connexions TCP.
- Lancer l'outil Wireshark en étant `root` sur la machine, repérer l'adresse IP de votre machine avec `ifconfig`, récupérer l'adresse de hax.at avec nsloopkup, puis filtrer les paquets `ICMP` dans wireshark, enfin lancer un ping depuis le site traceroute.at vers votre machine, et capturer l'échange `ICMP ECHO-REQUEST/ECHO-REPLY`.

- D'autres commandes plus curieuses, que font-elles :
  - `outil de trace dns : dig`
  - `outil de trace ip : mtr`
  - `outil pour comprendre et tester les protocoles de transports et générer du trafic : iperf`
  - `outils sur les tables de routage et les routes : route -n`
  - `informations administratives sur les réseaux : plugin flagfox, whois`
  - `gestion des trames sur interface le : ntop`
  - `scan de port : nmap`
  - `outils snmp : tkined, net-snmp`
  - `outils de simulation libre : omnet, gns3`
- Pour se détendre et jouer avec les outils sans passer par les commandes, on peut aussi prendre conscience de la localisation des machines ou s'habituer avec le DNS, s'exercer à `traceroute`… le site http://www.dnsfrog.com/fr. Accessoirement, il vous donne votre adresse IP… enfin, pas la vôtre probablement, mais le point d'entrée ou de sortie du réseau de votre fournisseur d'accès… question à creuser.

Exercice 1 : Les couches Réseaux et Transport fiable TCP[1], et les niveaux d'encapsulation depuis la trame (couche Liaison) ou le principe des poupées russes/cubes gigognes–à faire soi-même ou accompagné

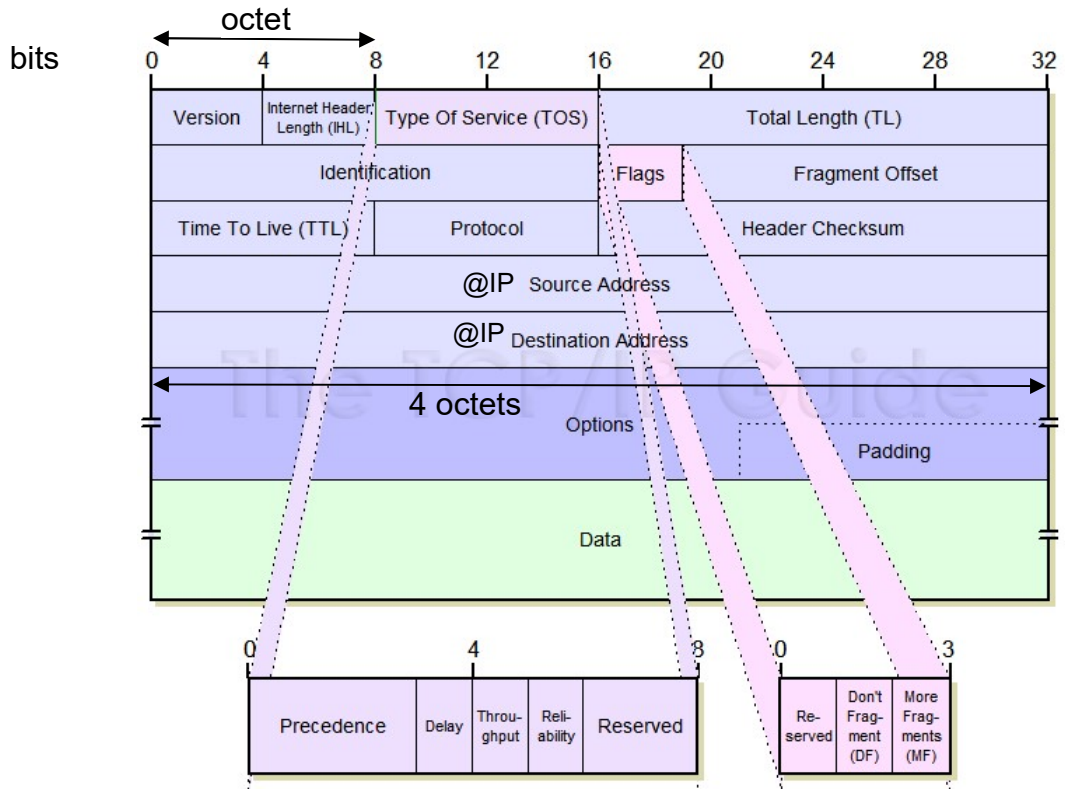
Sources : https://www.lecoledemesreves.com/les-poupees-russes/(28/04/2020) ou https://www.doudouplanet.com/Playskool/Cubes-gigognes.2910.html (06/09/2021) ou https://www.omnisecu.com/tcpip/tcpip-encapsulation-decapsulation.php[2](22/04/2021).

[1] Transmission Control Protocol

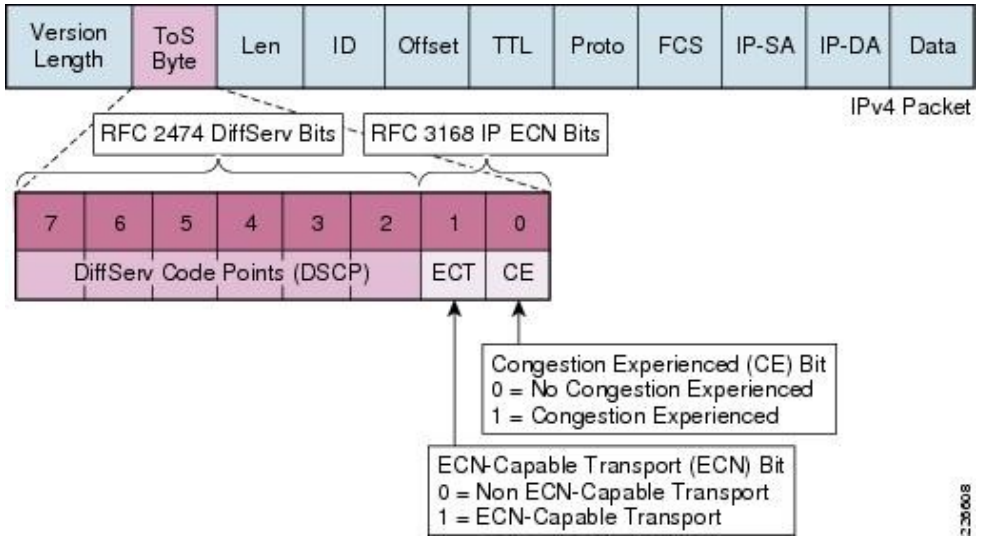
On donne la structure d'une trame Ethernet :

Adresse Destination MAC	Adresse Source MAC	Type	Informations	FCS
6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

On donne la structure de l'entête IP, consultés le 23 décembre 2013, source http://www.tcpipguide.com/free/t_IPDatagramGeneralFormat.htm :



[2] Sur https://www.omnisecu.com/tcpip/tcpip-encapsulation-decapsulation.php, la métaphore des cartons est bien détaillée et intéressante. A regarder !!!!



la même entête avec une représentation en ligne, mais sans la taille des champs (source http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/Medianet_Ref_Gd/chap4.html)

et la structure de l'entête TCP, consultée 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				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
128	Checksum																Urgent pointer (if URG set)															
160 ...	Options (if Data Offset > 5) ...																padding															

IPv4 est défini dans la RFC (Request For Comment) 791 http://www.ietf.org/rfc/rfc791.txt, c'est la version de 1981, Jon Postel, certains champs ont été mis à jour depuis. Par exemple le champ DS vu ci-dessous se superpose au champ TOS

http://tools.ietf.org/html/rfc2474 (RFC2474).

TCP est défini dans la RFC 793 http://tools.ietf.org/html/rfc793, c'est la version de 1981, Jon Postel. Depuis, le protocole a été mis à jour. Par exemple le champ ECN, Explicit Congestion Notification http://tools.ietf.org/html/rfc3168 (RFC3168) a été ajouté et ses circonstances d'utilisation.

Aujourd'hui, la QoS étant déployée dans de nombreux réseaux, le champ TOS peut être redéfini en DSCP Differenciated Service Code qu'on voit dans un autre cours.

Trace d'une communication point à point, prélevée par l'outil SNOOP :

```
ETHER:  ----- Ether Header -----
ETHER:  Packet 3 arrived at 11:42:27.64
ETHER:  Packet size = 64 bytes
ETHER:  Destination = 8:0:20:18:ba:40, Sun
ETHER:  Source      = aa:0:4:0:1f:c8, DEC (DECNET)
ETHER:  Ethertype = 0800 (IP)

IP:   ----- IP Header -----
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         x xx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 40 bytes
IP:   Identification = 41980
IP:   Flags = 0x4
IP:         .1.. .... = do not fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 63 seconds/hops
IP:   Protocol = 6 (TCP)
IP:   Header checksum = af63
IP:   Source address = 163.173.32.65, papillon.cnam.fr
IP:   Destination address = 163.173.128.212, jordan
IP:   No options

TCP:  ----- TCP Header -----
TCP:  Source port = 1368
TCP:  Destination port = 23 (TELNET)
TCP:  Sequence number = 143515262
TCP:  Acknowledgement number = 3128387273
```

```
TCP:  Data offset = 20 bytes
TCP:  Flags = 0x10
TCP:        ..0. .... = No urgent pointer
TCP:        ...1 .... = Acknowledgement
TCP:        .... 0... = No push
TCP:        .... .0.. = No reset
TCP:        .... ..0. = No Syn
TCP:        .... ...0 = No Fin
TCP:  Window = 32120
TCP:  Checksum = 0x3c30
TCP:  Urgent pointer = 0
TCP:  No options

TELNET:  ----- TELNET:   -----
TELNET:  ""
```

A votre avis, à quoi correspondent les étiquettes TCP et TELNET (chercher sur le Web) ?

Trace hexadécimale d'une communication point à point :

```
3   0.00000 papillon.cnam.fr -> jordan       TELNET C port=1368

00: 0800 2018 ba40 aa00 0400 1fc8 0800 4500    .. ..@........E.
16: 0028 a3fc 4000 3f06 af63 a3ad 2041 a3ad    .(.ü@.?..c.. A..
32: 80d4 0558 0017 088d de7e ba77 66c9 5010    ...X.....~.wf.P.
48: 7d78 3c30 0000 0000 0000 0000 0000 0000    }x<0............
```

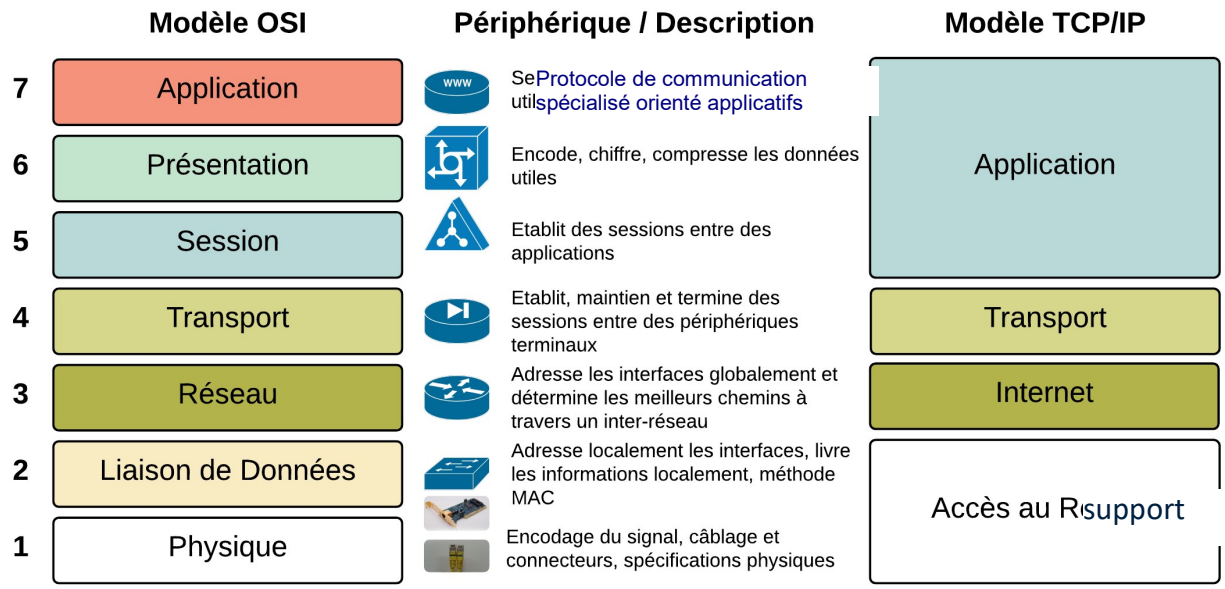
Déterminer le début du datagramme IPv4 dans cette trace.

Déterminer la fin de l'entête du datagramme IPv4.

Déterminer la fin de l'entête TCP.

Combien y a-t-il d'encapsulations successives ?

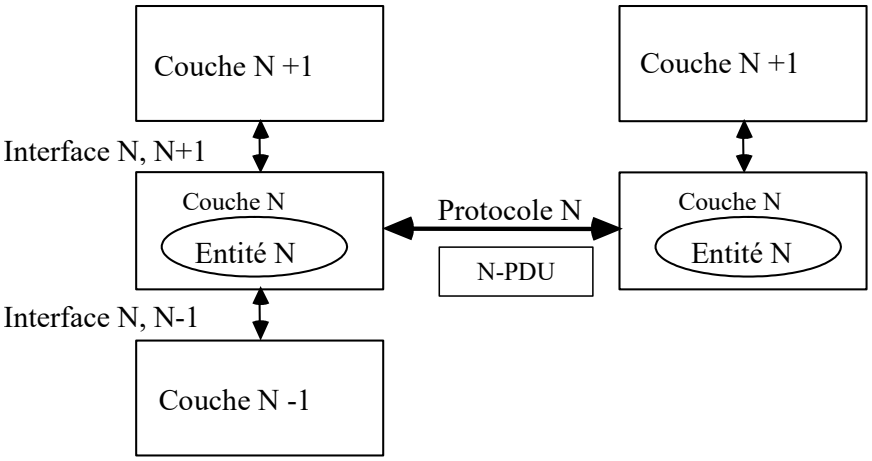
Exercice 2 : Le modèle OSI et le modèle Internet



source : https://cisco.goffinet.org/ccna/fondamentaux/modeles-tcp-ip-osi/, consulté le 24/04/2019 17h45

Dans le contexte du modèle OSI, qu'est qu'une PDU ? Comment cela se décline pour l'Internet ?

On rappelle ci-dessous le dessin donné en cours :



[3]

Merci pour votre attention !!!!!

[3] Troupe d'élite dans BoomBeach de SuperCell, bombardier lanceur de pastèques explosives, https://boombeach.fandom.com/wiki/Melon_Bombardier (29/08/2021)