

# Illustration du Modèle Réseau en Couches

Guillaume Urvoy-Keller, Quentin Jacquemart

8 mai 2021

## 1 Introduction

Le but de ce TP est d'illustrer le modèle en couches utilisé dans Internet. Ce modèle constitue une référence dans le monde des réseaux. C'est avant tout des raisons pratiques qui sont à l'origine de sa création et qui peuvent se résumer en "quand vous avez un problème complexe à résoudre (ici, transférer des paquets entre applications sur un réseau), découpez le en une suite de problèmes plus petits".

Le modèle TCP/IP est aussi souvent appelé modèle OSI. Stricto sensu, la couche physique n'appartient pas au modèle TCP/IP d'ailleurs, mais au modèle OSI. Il est illustré figure 1.

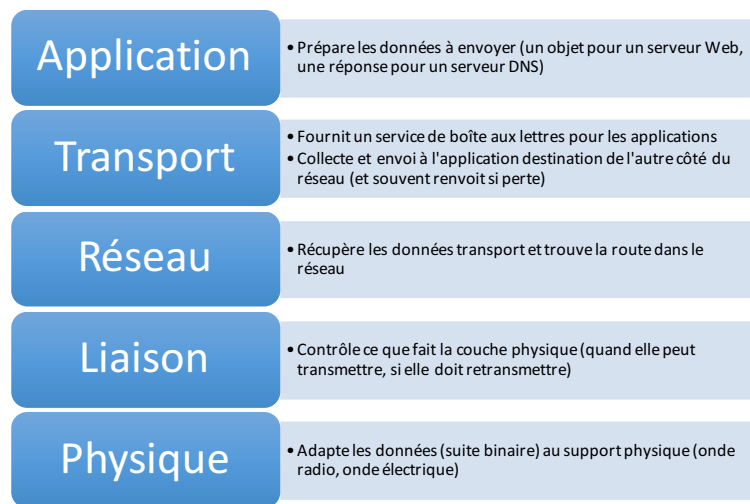


FIGURE 1 – Modèles en couche

## 2 Couche Applications : nombre d'objets et nombre de source d'une page Web

### 2.1 Avec un navigateur

Nous allons utiliser dans un premier temps des fonctionnalités de Chrome ou Firefox qui permettent de suivre les échanges protocolaires au niveau de la couche applicative : le protocole HTTP.

- Ouvrir Firefox ... ou Chrome
- Démarrez la console de surveillance réseau : Outils > Développement > Console Réseau sur Firefox et depuis le menu accessible à droite de l'écran – voir Figure 2 – Plus d'outils > Outils de Développement.

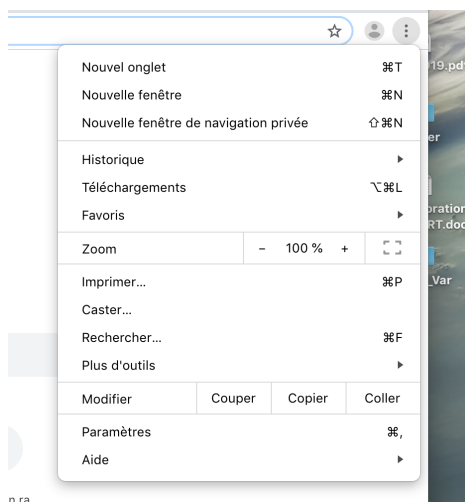


FIGURE 2 – Accès à outils monitoring réseau sous Chrome

1. Nous allons d'abord ouvrir un site Web avec une architecture simple : <http://www.i3s.unice.fr/~urvoy/>
  - (a) Combien d'objets sont présents dans cette page ?

**Réponse : Il faut compter le nombre d'objets qui ont été téléchargés via un GET qui doit s'être conclu par un code de retour 200 OK.  
On voit 8 codes 200 ici donc il y a 8 objets.**

Name	Status	Domain	Type	Initiator	Size	Time
~urvoy/	302	www.i3s.unice.fr	document / Redirect	Other	257 B	
~urvoy/	200	www.i3s.unice.fr	document	~urvoy/	2.5 kB	
avatar.jpg	200	www.i3s.unice.fr	jpeg	(index)	86.4 kB	
main.js	200	www.i3s.unice.fr	script	(index)	483 B	
normalize.min.css	200	www.i3s.unice.fr	stylesheet	(index)	1.1 kB	
style.css	200	www.i3s.unice.fr	stylesheet	(index)	1.5 kB	
css?family=Inter Source+Serif+Pro	200	fonts.googleapis.com	stylesheet	(index)	700 B	
UcCO3FwrK3iLTeHuS_fvQMwCp50KnlMw2boKoduknMEVulyfAZ9hp-Ek_-EeA.woff	200	fonts.gstatic.com	font	css?family=Inter Source+Serif+Pro	21.7 kB	
nelQzD-QpwxpaWvjeD0X88SAceauXQ-oAGlyY0.woff2	200	fonts.gstatic.com	font	css?family=Inter Source+Serif+Pro	20.0 kB	

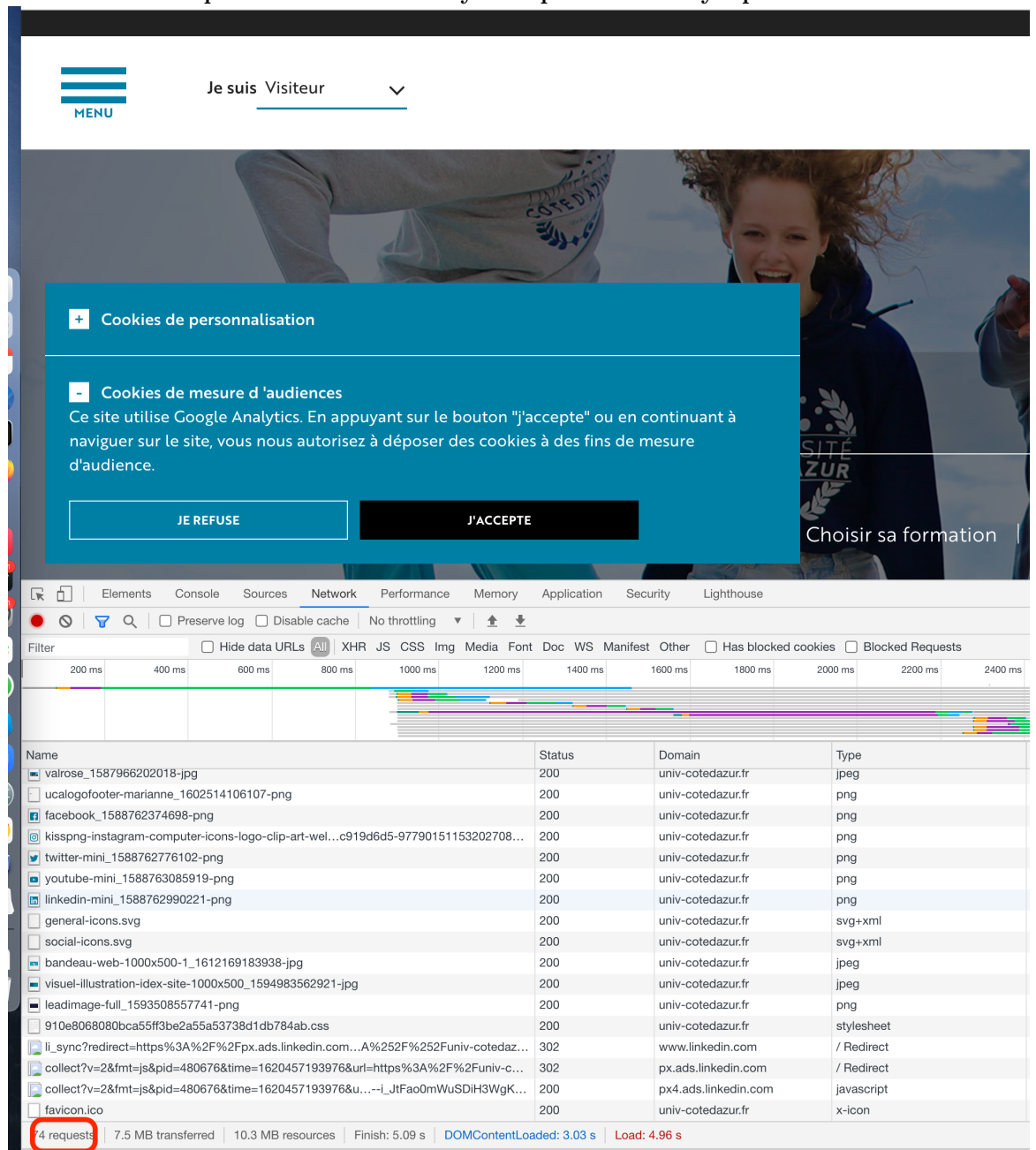
- (b) Tous les objets sont-ils bien téléchargés ?

**Réponse : Le premier objet demandé a mené à un code de retour 302, qui est une redirection, car on a demandé <http://www.i3s.unice.fr/~urvoy/> alors**

que le serveur n'est configuré que pour répondre en https. Si on avait tapé `https://www.i3s.unice.fr/~urvoy/`, on ne verrait pas cette redirection.

2. Nous allons maintenant analyser un site plus complexe `https://univ-cotedazur.fr/`. Ouvrez le. Il faut sans doute plusieurs secondes avant que tout soit téléchargé.
  - (a) Combien y a-t-il de requêtes faites ?

**Réponse :** La situation est beaucoup plus complexe ici avec un site riche. Sous Chrome, l'outil reporte le nombre de requêtes faites dans le cadre en bas de la fenêtre d'analyse. On en voit, dans mon cas, 74. Vous pourriez voir un chiffre différent si vous avez passé la première étape d'acceptation des cookies et que du contenu est dynamiquement envoyé par le serveur.



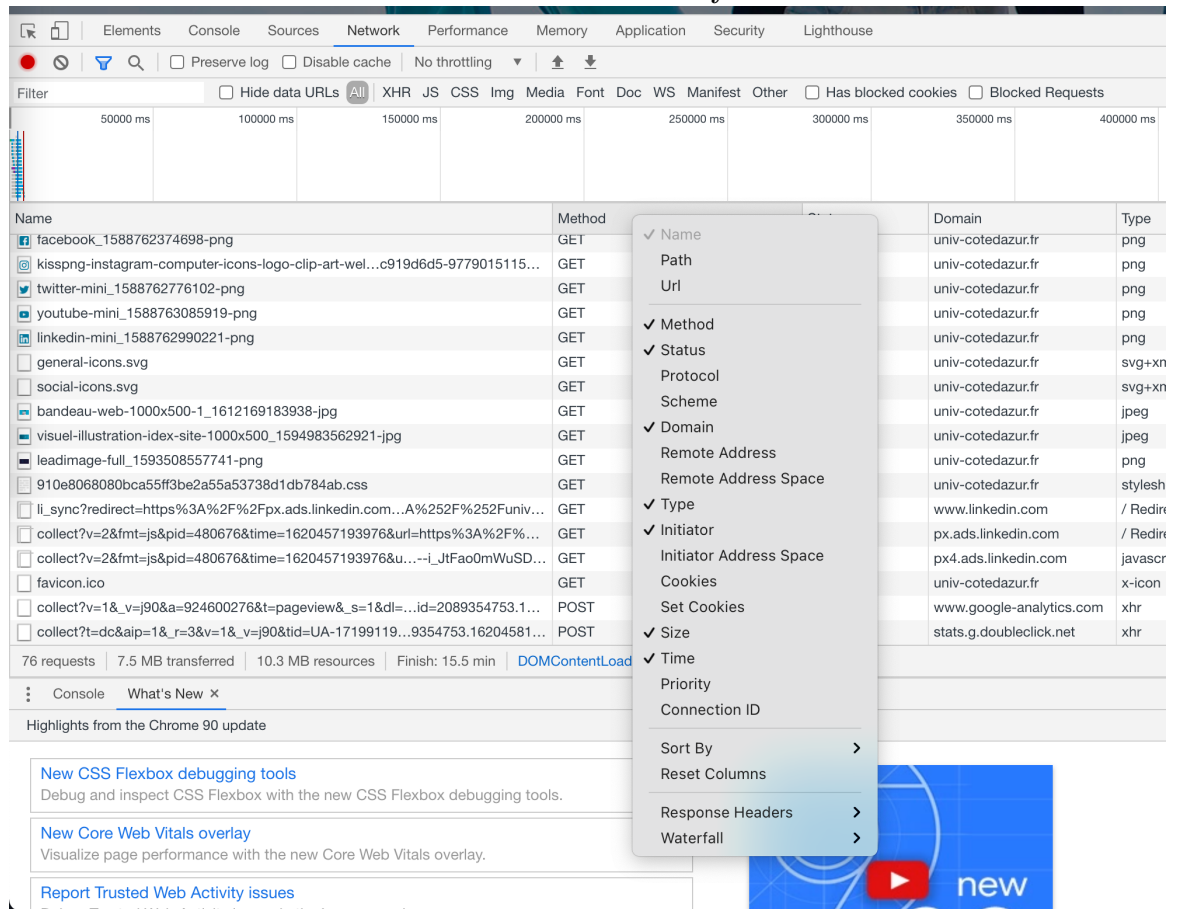
The screenshot shows a web browser with a cookie consent dialog in the foreground. The dialog has two buttons: "JE REFUSE" and "J'ACCEPTÉ". Below the dialog, the Chrome DevTools Network tab is open, displaying a list of requests. The summary at the bottom of the Network tab shows 74 requests, 7.5 MB transferred, 10.3 MB resources, and a load time of 4.96 s.

Name	Status	Domain	Type
valrose_1587966202018-jpg	200	univ-cotedazur.fr	jpeg
ucalogofooter-marianne_1602514106107-png	200	univ-cotedazur.fr	png
facebook_1588762374698-png	200	univ-cotedazur.fr	png
kisspng-instagram-computer-icons-logo-clip-art-wel...c919d6d5-97790151153202708...	200	univ-cotedazur.fr	png
twitter-mini_1588762776102-png	200	univ-cotedazur.fr	png
youtube-mini_1588763085919-png	200	univ-cotedazur.fr	png
linkedin-mini_1588762990221-png	200	univ-cotedazur.fr	png
general-icons.svg	200	univ-cotedazur.fr	svg+xml
social-icons.svg	200	univ-cotedazur.fr	svg+xml
bandeau-web-1000x500-1_1612169183938-jpg	200	univ-cotedazur.fr	jpeg
visuel-illustration-idex-site-1000x500_1594983562921-jpg	200	univ-cotedazur.fr	jpeg
leadimage-full_1593508557741-png	200	univ-cotedazur.fr	png
910e8068080bca55ff3be2a55a53738d1db784ab.css	200	univ-cotedazur.fr	stylesheet
li_sync?redirect=https%3A%2F%2Fpx.ads.linkedin.com...A%252F%252FUniv-cotedaz...	302	www.linkedin.com	/ Redirect
collect?v=2&fmt=js&pid=480676&time=1620457193976&url=https%3A%2F%2FUniv-c...	302	px.ads.linkedin.com	/ Redirect
collect?v=2&fmt=js&pid=480676&time=1620457193976&u...-JtFao0mWuSDiH3WgK...	200	px4.ads.linkedin.com	javascript
favicon.ico	200	univ-cotedazur.fr	x-icon

74 requests | 7.5 MB transferred | 10.3 MB resources | Finish: 5.09 s | DOMContentLoaded: 3.03 s | Load: 4.96 s

(b) Quel est le type des requêtes, appelées aussi **méthodes** dans le jargon HTTP ? **Réponse**

**: Sous Chrome, on ne voit pas directement la colonne méthode, il faut l'ajouter en faisant un clic droit dans la barre du haut où il y a le nom des colonnes.**



Si on accepte pas les cookies, on ne voit que des GET. Si on les accepte, on voit deux requêtes en plus : on passe de 74 à 76. Ce sont des requêtes de type POST (voir figure ci-après) qui correspondent à l'envoi de données, directement vers Google Analytics et un autre service d'analyse qu'UCA doit utiliser pour les statistiques sur les visites sur son site

Name	Method	Status	Domain	Type
facebook_1588762374698-png	GET	200	univ-cotedazur.fr	png
kisspng-instagram-computer-icons-logo-clip-art-wel...c919d6d5-9779015115...	GET	200	univ-cotedazur.fr	png
twitter-mini_1588762776102-png	GET	200	univ-cotedazur.fr	png
youtube-mini_1588763085919-png	GET	200	univ-cotedazur.fr	png
linkedin-mini_1588762990221-png	GET	200	univ-cotedazur.fr	png
general-icons.svg	GET	200	univ-cotedazur.fr	svg+xml
social-icons.svg	GET	200	univ-cotedazur.fr	svg+xml
bandeau-web-1000x500-1_1612169183938-jpg	GET	200	univ-cotedazur.fr	jpeg
visuel-illustration-idex-site-1000x500_1594983562921-jpg	GET	200	univ-cotedazur.fr	jpeg
leadimage-full_1593508557741-png	GET	200	univ-cotedazur.fr	png
910e8068080bca55f3be2a55a53738d1db784ab.css	GET	200	univ-cotedazur.fr	stylesheet
li_sync?redirect=https%3A%2F%2Fpx.ads.linkedin.com...A%252F%252FUniv...	GET	302	www.linkedin.com	/ Redirect
collect?v=2&fmt=js&pid=480676&time=1620457193976&url=https%3A%2F%...	GET	302	px.ads.linkedin.com	/ Redirect
collect?v=2&fmt=js&pid=480676&time=1620457193976&u...-i_UtFao0mWuSD...	GET	200	px4.ads.linkedin.com	javascript
favicon.ico	GET	200	univ-cotedazur.fr	x-icon
collect?v=1&_v=j90&a=924600276&t=pageview&_s=1&dl=...id=2089354753.1...	POST	200	www.google-analytics.com	xhr
collect?t=dc&aip=1&_r=3&v=1&_v=j90&tid=UA-17199119...9354753.16204581...	POST	200	stats.g.doubleclick.net	xhr

76 requests | 7.5 MB transferred | 10.3 MB resources | Finish: 15.5 min | DOMContentLoaded: 3.03 s | Load: 4.96 s

(c) De combien de sites distincts, appelés aussi **domaines**, proviennent ces objets? (vous pouvez ordonner de manière croissante/décroissante une colonne en cliquant dessus).

**Réponse :** Il faut classer la colonne **Domain** pour voir les domaines qui envoient des données pour cette page. Voici le haut de la colonne :

atus	Domain	Type
2	www.linkedin.com	/ Redir
0	www.google-analytics.com	xhr
0	www.google-analytics.com	script
0	univ-cotedazur.fr	docurr
0	univ-cotedazur.fr	svg+xml
0	univ-cotedazur.fr	script
0	univ-cotedazur.fr	script
0	univ-cotedazur.fr	png
0	univ-cotedazur.fr	png
0	univ-cotedazur.fr	png
0	univ-cotedazur.fr	png
0	univ-cotedazur.fr	png
0	univ-cotedazur.fr	png
0	univ-cotedazur.fr	png

**On trouve :**

- **linkedin.com**
- **googleanalytics**
- **univ-cotedazur.fr**
- et plusieurs autres à la fin de la liste (oui, le dernier est un peu louche, il vient d'UCA, mais on ne le voit pas comme domaine, je ne sais pas pourquoi) :

univ-cotedazur.fr	png
univ-cotedazur.fr	png
univ-cotedazur.fr	script
univ-cotedazur.fr	stylesheet
stats.g.doubleclick.net	xhr
snap.licdn.com	script
px4.ads.linkedin.com	javascript
px.ads.linkedin.com	/ Redirect
px.ads.linkedin.com	/ Redirect
code.jquery.com	script
cdn.curator.io	script
cdn.curator.io	stylesheet
cdn.curator.io	stylesheet
cdn-univ.fr	stylesheet
cdn-univ.fr	script
cdn-univ.fr	script
	svg+xml

## 2.2 Sans navigateur

Le protocole HTTP est un protocole en mode texte (par opposition au binaire). Un être humain peut donc l'utiliser pour interagir avec un serveur Web. Il faut néanmoins être capable d'envoyer les commandes HTTP au travers d'un canal de communication. Dans la figure ci-dessous, nous utilisons l'utilitaire telnet pour établir un canal TCP avec le serveur <http://packetor.com>.

**Sous Windows, utilisez** <https://vfsync.org/vm.html> pour avoir accès à une machine Linux en ligne.

```
guillaumes-macbook-pro-3 $ telnet packetor.com 80
Trying 52.6.124.79...
Connected to packetor.com.
Escape character is '^]'.
GET / HTTP/1.1 'Ce que j ai tape'
Host: packetor.com 'Ce que j ai tape'

'A partir de la ligne ci-apres, le retour du serveur'
HTTP/1.1 200 OK
Date: Sat, 24 Apr 2021 19:25:30 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 4884
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<HTML lang="en">
<HEAD>
  <META http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <META name="viewport" content="width=device-width, initial-scale=1">
  <META name="description" content="Online hex-dump network packet decoder.
    Analyzes protocol structure and fields of network packets in
    hexadecimal format." />
  <TITLE>Packetor - Online network Packet Analyzer / Decoder</TITLE>
  <LINK rel="icon" type="image/png" href="images/favicon.png" />
  <LINK rel="stylesheet" href="css/style.css" type="text/css">
  <LINK rel="stylesheet" href="http://fonts.googleapis.com/css?family=Patua+
    One%7COpen+Sans:400,400italic" type="text/css">
  <SCRIPT type="text/javascript" src="js/tools.js"></SCRIPT>
  <SCRIPT async type="text/javascript" src="js/CollapsibleLists.js"></SCRIPT>
```

```

<SCRIPT data-ad-client="ca-pub-8585436679638637" async src="https://pagead2
.googleadsyndication.com/pagead/js/adsbygoogle.js"></SCRIPT>
</HEAD>
<BODY onload="showRandomPacket();">
  <HEADER>
    <NAV>
[....]

```

1. Isolez la partie contrôle (en-tête HTTP) et la partie correspondant à l'objet Web.

**Réponse :** On voit bien les deux parties, contrôle puis données, avec une ligne blanche entre les deux.

```

guillaumes-macbook-pro-3 $ telnet packetor.com 80
Trying 52.6.124.79...
Connected to packetor.com.
Escape character is '^]'.
GET / HTTP/1.1 'Ce que j ai tape'
Host: packetor.com 'Ce que j ai tape'

'A partir de la ligne ci-apres, le retour du serveur'
HTTP/1.1 200 OK
Date: Sat, 24 Apr 2021 19:25:30 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 4884
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<HTML lang="en">
<HEAD>
  <META http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <META name="viewport" content="width=device-width, initial-scale=1">
  <META name="description" content="Online hex-dump network packet decoder.
  Analyzes protocol structure and fields of network packets in
  hexadecimal format." />
  <TITLE>Packetor - Online network Packet Analyzer / Decoder</TITLE>
  <LINK rel="icon" type="image/png" href="images/favicon.png" />
  <LINK rel="stylesheet" href="css/style.css" type="text/css">
  <LINK rel="stylesheet" href="http://fonts.googleapis.com/css?family=Patua+
  One%7COpen+Sans:400,400italic" type="text/css">
  <SCRIPT type="text/javascript" src="js/tools.js"></SCRIPT>
  <SCRIPT async type="text/javascript" src="js/CollapsibleLists.js"></SCRIPT>
  <SCRIPT data-ad-client="ca-pub-8585436679638637" async src="https://pagead2
  .googleadsyndication.com/pagead/js/adsbygoogle.js"></SCRIPT>
</HEAD>
<BODY onload="showRandomPacket();">
  <HEADER>
    <NAV>
[....]

```

Partie contrôle, utile pour HTTP, mais pas pour le navigateur qui veut juste l'objet qui vient après

Objet de type html (voir partie contrôle qui indique text/html)

2. Est-ce que le téléchargement de l'objet s'est bien fait ?

**Réponse :** 200 OK dans la partie contrôle

3. Quel est le type de ce objet ?

**Réponse :** Il suffit de regarder Content-Type qui indique que c'est de l'HTML

### 3 Couche Transport

Nous allons ici simplement visualiser les connexions de niveau transport en cours dans votre machine.

1. Utilisez le terminal précédent ou ouvrez en un nouveau et tapez la commande netstat pour afficher les connexions tcp en cours.  
Sous Windows et Mac OS :

```
netstat -n -p tcp
```

Sous Linux :

```
netstat -n -p -t
```

Réponse : Voilà un exemple sur ma machine ci-dessous. Il y a une ligne par connexion. Les “Local Address” et “Foreign address” sont une représentation qui concatène les adresses IP et les ports. Des fois elles sont séparées par un simple point comme ici, des fois par deux points. Il faut donc lire, pour la première connexion :

“ Il y a une connexion TCP entre l’adresse IP 192.168.1.38 (ma machine) depuis le port 60863 (qui identifie une application, ici Firefox) vers l’adresse IP 162.125.19.131 et le port 443 (qui est le port HTTPS).”

```
(base) guillaumes-macbook-pro-3:~ urvoy$ netstat -n -p tcp
Active Internet connections
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4      0      0 192.168.1.38.60863     162.125.19.131.443     ESTABLISHED
tcp4      0      0 192.168.1.38.60564     52.19.19.59.80         ESTABLISHED
tcp4      0      0 192.168.1.38.60563     52.19.19.59.80         ESTABLISHED
tcp4      0      0 192.168.1.38.59238     162.125.19.9.443      ESTABLISHED
tcp4      0      0 192.168.1.38.58657     162.125.19.131.443    ESTABLISHED
tcp4      0      0 192.168.1.38.56866     17.57.146.169.5223    ESTABLISHED
tcp4      0      0 192.168.1.38.55550     52.38.124.88.443      ESTABLISHED
tcp4      0      0 127.0.0.1.54687        127.0.0.1.55549       ESTABLISHED
tcp4      0      0 127.0.0.1.55549        127.0.0.1.54687       ESTABLISHED
tcp4      0      0 192.168.1.38.54875     20.54.36.229.443      ESTABLISHED
tcp4      0      0 192.168.1.38.54824     194.57.138.240.443    ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49470 fe80::aede:48ff:.49264 ESTABLISHED
tcp4      0      0 192.168.1.38.49464     3.122.180.233.443     ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49454 fe80::aede:48ff:.49269 ESTABLISHED
tcp6      0      0 2a01:cb1d:618:9b:49410 2a00:1450:4007:8.443  CLOSE_WAIT
tcp6      0      0 2a01:cb1d:618:9b:49407 2a00:1450:4007:8.443  CLOSE_WAIT
tcp6      0      0 2a01:cb1d:618:9b:49405 2a00:1450:4007:8.443  CLOSE_WAIT
tcp6      0      0 2a01:cb1d:618:9b:49404 2a00:1450:4007:8.443  ESTABLISHED
tcp6      0      0 2a01:cb1d:618:9b:49348 2a00:1450:400c:c.5228 ESTABLISHED
tcp4      0      0 127.0.0.1.60012        127.0.0.1.49268       ESTABLISHED
tcp4      0      0 127.0.0.1.60014        127.0.0.1.49267       ESTABLISHED
tcp4      0      0 127.0.0.1.49268        127.0.0.1.60012       ESTABLISHED
tcp4      0      0 127.0.0.1.49267        127.0.0.1.60014       ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49266 fe80::aede:48ff:.49267 ESTABLISHED
tcp6      0      0 2a01:cb1d:618:9b:49198 2a03:2880:f242:c.443  ESTABLISHED
tcp4      0      0 192.168.1.38.49174     3.127.214.178.443     ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49172 fe80::aede:48ff:.49256 ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49170 fe80::aede:48ff:.49255 ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49161 fe80::aede:48ff:.49262 ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49157 fe80::aede:48ff:.49272 ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49160 fe80::aede:48ff:.49249 ESTABLISHED
tcp6      0      0 fe80::aede:48ff:.49153 fe80::aede:48ff:.59602 ESTABLISHED
tcp4      0      0 127.0.0.1.60532        127.0.0.1.54687       TIME_WAIT
tcp4      0      0 192.168.1.38.60533     35.244.247.133.443    TIME_WAIT
tcp4      0      0 192.168.1.38.60992     18.195.126.72.443     TIME_WAIT
(base) guillaumes-macbook-pro-3:~ urvoy$ █
```

2. L’adresse IP du serveur Web `www.i3s.unice.fr` est `134.59.130.2`. Ouvrez une seconde fenêtre de commande (cmd) et ouvrez un canal telnet comme précédemment (`telnet www.i3s.unice.fr 80`).

Réponse : Vous devez obtenir quelque chose comme cela. L’important est de voir écrit “Connected to...” car cela indique que la connexion TCP est établie

```
(base) guillaumes-macbook-pro-3:~ urvoy$ telnet www.i3s.unice.fr 80
Trying 134.59.130.2...
Connected to niouze.i3s.unice.fr.
Escape character is '^]'.

```

3. Retapez la commande `netstat` précédente et donnez l’identifiant complet de la connexion entre votre telnet et le serveur `www.i3s.unice.fr`. Rappel : cet identifiant identifie des processus applicatifs s’exécutant sur des machines. On bien les deux niveaux d’adressage (machine et



processus).

**Réponse :** On voit bien en deuxième la connexion vers 134.59.130.2 qui est le serveur de l'I3S. On peut remarquer que le port est bien 80 au niveau du serveur, ce qui correspond à ce qu'on a tapé dans telnet.

```
(base) guillaumes-macbook-pro-3:~ urvoy$ netstat -n -p tcp
Active Internet connections
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4      0      0 192.168.1.38.63114     162.125.19.9.443      ESTABLISHED
tcp4      0      0 192.168.1.38.63093     134.59.130.2.80       ESTABLISHED
tcp4      0      0 192.168.1.38.62784     162.125.19.131.443    ESTABLISHED
tcp4      0      0 192.168.1.38.62396     162.125.19.131.443    ESTABLISHED
tcp4      0      0 192.168.1.38.62090     162.125.19.131.443    ESTABLISHED
tcp4      0      0 192.168.1.38.60564     52.19.19.59.80        ESTABLISHED
tcp4      0      0 192.168.1.38.60563     52.19.19.59.80        ESTABLISHED
tcp4      0      0 192.168.1.38.56866     17.57.146.169.5223    ESTABLISHED
tcp4      0      0 192.168.1.38.55550     52.38.124.88.443      ESTABLISHED
tcp4      0      0 192.168.1.38.54687     177.0.0.1.55540       ESTABLISHED
```

## 4 Couche Réseau

### 4.1 Obtention des paramètres courants

**Sous Windows :**

Depuis l'invite de commande, tapez la commande :

```
ipconfig /all
```

Vous pouvez aussi obtenir ces informations depuis Panneau de Configuration > Réseau et Internet > Centre Réseau et Partage puis cliquez sur la connexion Wifi et demandez les détails.

**Sous Linux :**

```
ip address show # Fournit les adresses IP
ip route show # Fournit la passerelle par défaut (ligne default)
more /etc/resolv.conf # Fournit le résolveur DNS par défaut
```

**Sous MacOS :**

```
ifconfig # Fournit les adresses IP
netstat -r -n # Fournit la passerelle par défaut (ligne default)
more /etc/resolv.conf # Fournit le résolveur DNS par défaut
```

1. Identifiez l'adresse IP de votre machine

**Réponse :** La copie d'écran ci-dessous sur un PC Windows nous indique que l'adresse IP est 192.168.1.27.

```

Invite de commandes
Adresse physique . . . . . : A8-A7-95-60-6C-67
DHCP activé . . . . . : Oui
Configuration automatique activée . . . . . : Oui

Carte réseau sans fil Wi-Fi :

Suffixe DNS propre à la connexion . . . : home
Description . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
Adresse physique . . . . . : A8-A7-95-60-6C-67
DHCP activé . . . . . : Oui
Configuration automatique activée . . . : Oui
Adresse IPv6 . . . . . : 2a01:cb1d:618:9b00:ec2:abb2:c81b:3310(préféré)
Adresse IPv6 temporaire . . . . . : 2a01:cb1d:618:9b00:4d5b:3e98:7e3f:cb7c(préféré)
Adresse IPv6 de liaison locale . . . . : fe80::ec2:abb2:c81b:3310%18(préféré)
Adresse IPv4 . . . . . : 192.168.1.27(préféré)
Masque de sous-réseau . . . . . : 255.255.255.0
Bail obtenu . . . . . : vendredi 7 mai 2021 14:46:07
Bail expirant . . . . . : dimanche 9 mai 2021 09:57:30
Passerelle par défaut . . . . . : fe80::1a62:2cff:feaf:3699%18
192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAD DHCPv6 . . . . . : 162047893
DUID de client DHCPv6 . . . . . : 00-01-00-01-10-F9-50-B5-FC-3F-DB-5E-12-52
Serveurs DNS . . . . . : fe80::1a62:2cff:feaf:3699%18
192.168.1.1
NetBIOS sur Tcpip . . . . . : Activé
Liste de recherche de suffixes DNS propres à la connexion :
home

```

Sous une machine Unix, il faut utiliser `netstat -r -n` pour trouver les routes. La passerelle par défaut correspond à la ligne "default" et c'est encore 192.168.1.1 car mon mac et le PC précédent sont sur le même réseau :

```

(base) guillaumes-macbook-pro-3:~ urvoy$ netstat -r -n
Routing tables

Internet:
Destination      Gateway          Flags           Netif Expire
default          192.168.1.1     UGScg          en7
127              127.0.0.1       UCS            lo0
127.0.0.1        127.0.0.1       UH             lo0
169.254          link#13         UCS            en7      !
192.168.1        link#13         UCS            en7      !
192.168.1.1/32   link#13         UCS            en7      !
192.168.1.1     18:62:2c:af:36:99 UHLWIir       en7      1177
192.168.1.27    link#13         UHLWII        en7      !
192.168.1.29    5c:f7:e6:20:c7:48 UHLWII        en7      862
192.168.1.38/32 link#13         UCS            en7      !
192.168.1.255   ff:ff:ff:ff:ff:ff UHLWII        en7      !

```

2. Identifiez l'adresse IP de la passerelle par défaut. Quel est son rôle ?

Réponse : La passerelle est 192.168.1.1. Il faut retenir qu'une passerelle est un routeur qui permet donc de passer d'un réseau IP à un autre. Ici, elle permet de passer du réseau de ma maison au réseau de mon opérateur (Orange)

3. Identifiez le ou les serveurs DNS de votre machine ?

Réponse : Il y a deux serveurs DNS, 192.168.1.1, la box et une adresse IPv6 fe80 : : ... . En fait, la box prend la requête de votre machine locale et l'envoie aux serveurs DNS d'Orange qui font la résolution nom adresse IP (notamment). Sous Unix, on doit lire le fichier /etc/resolv.conf et chercher les lignes nameserver. On trouve les mêmes adresses que pour le PC :

```

(base) guillaumes-macbook-pro-3:~ urvoy$ more /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
search home
nameserver fe80::1a62:2cff:feaf:3699
nameserver 2a01:cb1d:618:9b00:1a62:2cff:feaf:3699
nameserver 192.168.1.1

```

4. Que se passerait-il si on retirait l'adresse IP de la passerelle ?

**Réponse :** On peut toujours contacter les machines du réseau local, mais on ne peut plus sortir du réseau local de la maison

5. Idem pour les serveurs DNS

**Réponse :** On a une connectivité totale à Internet si la passerelle est bien configurée mais il faut utiliser les adresses IP et on ne peut plus utiliser les noms courants comme google.com

## 4.2 Le DNS

Ouvrez à nouveau une invite de commande. Nous allons utiliser l'utilitaire nslookup pour faire des requêtes DNS.

1. Faites une requête simple pour trouver l'adresse IP du serveur Web de l'UCA. Il suffit de taper :  
nslookup www.univ-cotedazur.fr  
La réponse est sous la partie answer.

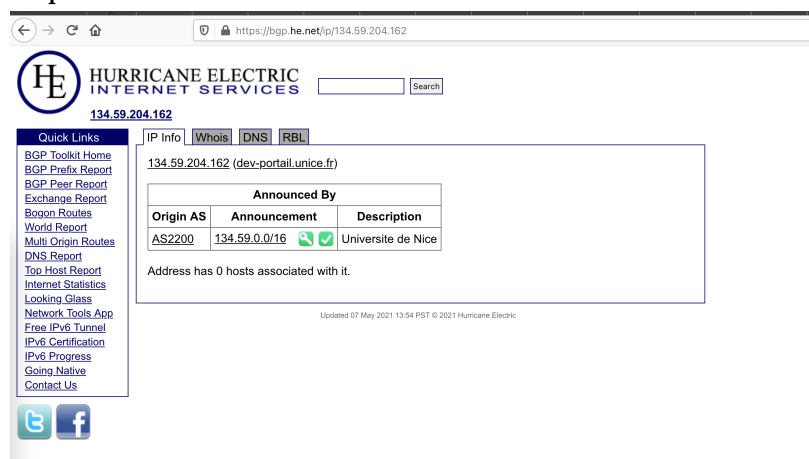
**Réponse :** La réponse est 134.59.204.162, en dernière ligne.

```
(base) guillaumes-macbook-pro-3:~ urvoy$ nslookup www.univ-cotedazur.fr
Server:         2a01:cb1d:618:9b00:1a62:2cff:feaf:3699
Address:       2a01:cb1d:618:9b00:1a62:2cff:feaf:3699#53
```

```
Non-authoritative answer:
www.univ-cotedazur.fr canonical name = univ-cotedazur.fr.
Name:   univ-cotedazur.fr
Address: 134.59.204.162
```

2. Vérifiez avec <https://bgp.he.net/> qu'il s'agit bien d'une adresse de l'UCA.

**Réponse :**



The screenshot shows the Hurricane Electric website interface. At the top, there is a search bar and navigation links. The main content area displays the IP address 134.59.204.162 and its associated BGP information. A table titled "Announced By" shows the origin AS as AS2200, with the announcement made by the University of Nice. The table has columns for Origin AS, Announcement, and Description. Below the table, it states "Address has 0 hosts associated with it." The footer of the page includes social media icons for Twitter and Facebook, and a copyright notice for Hurricane Electric.

Announced By		
Origin AS	Announcement	Description
AS2200	134.59.0.0/16	Universite de Nice

3. A quel AS cette adresse IP appartient-elle ?

**Réponse :** Un AS est un numéro pour fournisseur d'accès Internet. Ici, on voit AS2200 qui est Renater, le FAI des universités en France

**HURRICANE ELECTRIC**  
INTERNET SERVICES

AS2200 Renater

Quick Links: BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogn Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, Contact Us

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR | IX

Company Website: <http://www.renater.fr>

Country of Origin: France

Internet Exchanges: 7

Prefixes Originated (all): 75  
Prefixes Originated (v4): 74  
Prefixes Originated (v6): 1

Prefixes Announced (all): 213  
Prefixes Announced (v4): 206  
Prefixes Announced (v6): 7

RPKI Originated Valid (all): 37  
RPKI Originated Valid (v4): 36  
RPKI Originated Valid (v6): 1

RPKI Originated Invalid (all): 0  
RPKI Originated Invalid (v4): 0  
RPKI Originated Invalid (v6): 0

BGP Peers Observed (all): 130  
BGP Peers Observed (v4): 122  
BGP Peers Observed (v6): 76

IPs Originated (v4): 3,140,608  
AS Paths Observed (v4): 1,343  
AS Paths Observed (v6): 605

Average AS Path Length (all): 3.698  
Average AS Path Length (v4): 3.848  
Average AS Path Length (v6): 3.364

AS2200 IPv4 Peers

4. Le DNS est aussi utilisé par votre client mail. Cela permet de taper `guillaume.urvoy-keller@univ-cotedazur.fr` où on voit que **la seconde partie est un domaine Internet et non un serveur de l'UCA**. Si le serveur de mail s'appelait `mail.univ-cotedazur.fr`, il faudrait taper `guillaume.urvoy-keller@mail.univ-cotedazur.fr` Faites maintenant une requête pour trouver les serveurs de mail entrants (ceux que votre client mail contactera si vous voulez nous envoyer des mails) de l'UCA. Il faut faire une requête de `nslookup -type=MX` et mettre à la fin le nom du domaine (pas du serveur Web).

### Réponse :

**Il y a deux serveurs mails `ip-nice06.unice.fr` et `ip-sophia06.unice.fr`. Les nombres 10 et 20 devant sont seulement des poids mis pour donner des priorités.**

```
www.univ-cotedazur.fr canonical name = univ-cotedazur.fr.
Name: univ-cotedazur.fr
Address: 134.59.204.162
```

```
(base) guillaumes-macbook-pro-3:~ urvoy$ nslookup -type=MX univ-cotedazur.fr
Server:      2a01:cb1d:618:9b00:1a62:2cff:feaf:3699
Address:     2a01:cb1d:618:9b00:1a62:2cff:feaf:3699#53
```

```
Non-authoritative answer:
univ-cotedazur.fr      mail exchanger = 10 ip-nice06.unice.fr.
univ-cotedazur.fr      mail exchanger = 20 ip-sophia06.unice.fr.
```

## 5 Structure paquet Internet et structure de l'Internet

### 5.1 Structure paquet

Soit une trame Ethernet capturée sur ma machine, en version hexadécimale :

```
18622caf369900e04c6818b308004500016f000040004006c081c0a801261727a012ec180050857a835ce3e9ebf08018080ab8fa
00000101080a248464b3070da87547454202f646f776e6c6f61642f422f392f312f42393136393634302d3839353322d343031412
d394244352d3943413641393837303746362f536b7944726976654d616e69666573742e786d6c20485454502f312e310d0a486f7
3743a20776c2e646c736572766963652e6d6963726f736f66742e636f6d0d0a43616368652d436f6e74726f6c3a20
6e6f2d63616368650d0a4163636570743a202a2fa20d0a557365722d4167656e743a2044f6e6544726976652f32313035322e30333
1342e303030312043464e6574776f726b2f313232302e312044617277696e2f32302e3332e300d0a4163636570742d4c616e6775616
7653a2066722d66720d0a4163636570742d456e636f64696e673a20677a69702c206465666c6174652c2062720d0a436f6e6e6563
```

74696f6e3a206b6565702d616c6976650d0a0d0a

On voit bien qu'il s'agit d'une suite de bits. Les équipements réseaux - votre machine, un routeur - sont capables de comprendre la structure de ce flux de bits pour extraire par exemple l'adresse IP ou des données de niveau HTTP.

Utilisez le site <http://packetor.com/> qui va décoder la structure de cette trame et indiquez :

- La suite des couches protocolaires rencontrées, en partant de la couche application
- L'adresse IP de ma machine
- Celle du serveur
- Les ports source et destination
- Quel est le type de requête HTTP ?

Réponse : Vous devriez obtenir :

The screenshot shows the Packetor website interface. At the top, there is a hex dump of the packet data:
 

```
0001400201030002000044103030370743a206b6565702d616c6976650d0a0d0a0d0a
65722d4167656e743a204f6e6544726976652f32313035322e
30353
1342e303030312043464e6574776f7726b2f313232302e31204
4617277696e2f32302e332e30000a4163636570742d4c616e6
775616
7653a2066722d66720d0a4163636570742d456e636f64696e6
73a20677069702c206465666c174652c2062720d0a436f6e6
e6563 74696f6e3a206b6565702d616c6976650d0a0d0a
```

 Below the hex dump, there is a button labeled "Decode Packet". Underneath the button, the decoded packet structure is shown:
 

- Frame 1: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits)
- Ethernet II, Src: Realtek\_68:18:b3 (00:e0:4c:68:18:b3), Dst: Sagemcom\_af:36:99 (18:62:2c:af:36:99)
- Internet Protocol Version 4, Src: 192.168.1.38, Dst: 23.39.160.18
- Transmission Control Protocol, Src Port: 60440, Dst Port: 80, Seq: 1, Ack: 1, Len: 315
- Hypertext Transfer Protocol

 The interface also includes a description: "Packetor is an online hex-dump packet analyzer / decoder. It accepts strings of hexadecimal digits as input. Spaces / Newlines are ignored. Just place your packet dump in the box above and hit 'Decode Packet'".

On voit bien qu'il y a une trame Ethernet dans laquelle il y a un paquet IP dans lequel il y a un segment TCP qui transporte un message HTTP.

L'adresse de ma machine est 192.168.1.38. On peut le savoir notamment car le port destination ici est 80, donc le port HTTP. Ainsi ce paquet IP va d'une machine vers un serveur Web et c'est bien l'adresse source qui est ici celle de ma machine (on aurait pu capturer un paquet allant dans l'autre sens et il aurait fallu faire le raisonnement inverse).

Le port source est donc 60440. L'adresse IP du serveur 23.391.160.18.

Pour trouver le type de requête, il faut étendre le niveau HTTP et on voit qu'il s'agit d'un GET.

This screenshot is identical to the previous one, but the decoded packet structure is extended to include the HTTP layer:
 

- GET /download/B/9/1/B9169640-8952-401A-9BD5-9CA6A98707FE/SkyDriveManifest.xml HTTP/1.1\r\n

 The rest of the interface, including the hex dump and the "Decode Packet" button, remains the same.

## 5.2 L'Internet : un réseau de réseaux

### 5.2.1 Depuis chez vous vers l'UCA

1. Ouvrez un terminal sous votre machine Windows : Menu Rechercher puis tapez cmd
2. Tapez la commande `tracert www.univ-cotedazur.fr`
3. Combien de routeurs sont traversés ?
4. A quelle distance en ms est le dernier routeur visible ?
5. Transformer cette durée en km en supposant un signal qui se propage à 200000km/s. Cette distance est "trop grande" car à chaque routeur, il y a une conversion optique-électronique et des temps de traitements informatique (en ms) dans les routeurs eux-mêmes.

#### Réponse : Depuis chez moi, chez Orange, j'obtiens :

```
(base) guillaumes-macbook-pro-3:~ urvoys$ traceroute -q 1 -w 1 www.univ-cotedazur.fr
traceroute to univ-cotedazur.fr (134.59.204.162), 64 hops max, 52 byte packets
 1 livebox (192.168.1.1) 11.663 ms
 2 80.10.239.141 (80.10.239.141) 6.683 ms
 3 ae109-0.ncnic201.rbcj.orange.net (193.253.86.10) 10.424 ms
 4 ae43-0.nimar101.rbcj.orange.net (193.252.103.234) 15.284 ms
 5 ae40-0.nimar102.rbcj.orange.net (193.252.161.22) 11.618 ms
 6 193.252.137.54 (193.252.137.54) 20.749 ms
 7 renater-1.gw.opentransit.net (193.251.254.30) 21.868 ms
 8 te-0-1-0-15-ren-nr-lyon2-rtr-091.noc.renater.fr (193.51.177.8) 36.375 ms
 9 te0-0-0-14-ren-nr-grenoble-rtr-091.noc.renater.fr (193.51.180.211) 35.364 ms
10 te0-1-0-0-ren-nr-cadarache-rtr-091.noc.renater.fr (193.51.177.66) 34.506 ms
11 te0-1-0-2-ren-nr-nice-rtr-091.noc.renater.fr (193.51.177.194) 38.632 ms
12 man-uns-vl979-gi8-5-nice-rtr-021.noc.renater.fr (193.51.191.9) 33.341 ms
13 *
14 *
15 *
16 *
17 *
```

Il y a donc 12 sauts. En fait il y en a sans doute 13 car le serveur Web n'a pas répondu car un pare-feu à bloquer mon trafic pour des raisons de sécurité. C'est pourquoi on obtient des étoiles à la fin.

Le dernier routeur visible est à a peu près 33 ms. Les nombres varient car chaque paquet sonde est indépendant et c'est comme le trafic routier : vous pouvez partir un peu après quelqu'un puis le doubler.

33ms à 200000 km/s donnerait une distance de 6600 km. Bien que l'Interconnexion entre Orange e Relater semble se faire au saut 6 vers Lyon (saut 8), la distance estimée est trop grande. Il y a en fait de nombreuses millisecondes perdues dans les conversions optique-électronique.

### 5.2.2 Depuis les US vers un TGV ☺

Lorsque un paquet (datagramme) traverse l'Internet, il passe au travers de plusieurs routeurs (qui lisent son adresse IP destination et décident vers quelle interface de sortie de le renvoyer). Nous pouvons matérialiser ces routeurs avec la commande `tracert` (tracroute sous linux). Voici le résultat d'un `tracert` entre une machine aux Etats-Unis et un machine connectée dans un TGV entre Paris et Nice. Le `tracert` n'arrive pas directement sur la machine dans le train mais sur un serveur de la SNCF qui fait aussi face d'interface entre le réseau de la SNCF et le reste de l'Internet, comme notre box à la maison.

```
Result for 109.190.253.13; modeset: {SOA-Owner-Query , ICMP-Query }:  
  
tracert.exe to 109.190.253.13 (109.190.253.13), 30 hops max, 38 byte packets  
 1 209.132.180.91 (209.132.180.91) hostmaster@redhat.com 11.815 ms  
 2 transit-2-180-132-209.redhat.com (209.132.180.2) hostmaster@redhat.com 15.117  
   ms  
 3 ip-38-145-63-254.redhat.com (38.145.63.254) noc@redhat.com 15.783 ms  
 4 te0-0-1-1.nr12.b019174-0.phx01.atlas.cogentco.com (38.88.238.29) dns@cogentco.  
   com 16.404 ms  
 5 te0-0-1-0.agr21.phx01.atlas.cogentco.com (154.24.53.149) dns@cogentco.com  
   16.688 ms
```

```
6 be3436.ccr31.phx01.atlas.cogentco.com (154.54.85.73) dns@cogentco.com 17.519 ms
7 be2931.ccr41.lax01.atlas.cogentco.com (154.54.44.86) dns@cogentco.com 20.587 ms
8 be3176.ccr21.sjc01.atlas.cogentco.com (154.54.31.190) dns@cogentco.com 25.626
  ms
9 be3142.ccr41.sjc03.atlas.cogentco.com (154.54.1.194) dns@cogentco.com 25.916 ms
10 sjo-sv5-bb1-a9.ca.us (142.44.208.168) tech@ovh.net 64.354 ms
11 be100-1346.th2-1-a9.fr.eu (37.187.36.198) tech@ovh.net 153.313 ms
12 be100-1043.rbx-g1-nc5.fr.eu (94.23.122.146) tech@ovh.net 157.567 ms
13 *
14 be5.rbx2-pcc2b-a9.fr.eu (91.121.128.193) tech@ovh.net 189.924 ms
15 109.190.253.13 (109.190.253.13) tech@ovh.net 190.701 ms
```

1. Quelle est la suite d'opérateurs Internet (FAI ou entreprises) par où passent les paquets IPs ?

**Réponse :** Il faut regarder les chaînes de caractères des noms (qui sont en correspondance avec des IPs). Il n'y a pas de façon normalisée de donner un nom à un routeur. Cela pourrait être FAI.ville.numéro mais chaque FAI est indépendant et fait comme il l'entend. Notre recherche ici est donc empirique et on trouve redhad puis cogent puis OVH.

2. Où la SNCF héberge-t-elle une partie de son infrastructure ?

**Réponse :** Chez OVH qui est un fournisseur de services cloud. Ici, on apprend que la SNCF déploie des machines virtuelles dans le cloud d'OVH pour faire des applications clés.

3. A quel niveau se fait le saut transatlantique ?

**Réponse :** Il faut trouver où se fait le grand saut en terme de délai. C'est entre les lignes 9 et 10. Le saut fait de l'ordre de 39 ms.

4. Est-ce une connexion au travers d'un satellite géostationnaire ou est-ce une liaison par câble sous-marin ?

**Réponse :** C'est un câble sous-marin car un satellite géostationnaire est à 36 000 km. Le signal devrait donc au minimum parcourir 2 fois cette distance. À la vitesse de la lumière, cela ferait : 240 ms. Donc il s'agit d'un câble sous-marin. Les satellites géostationnaires ne sont plus utilisés pour des liaisons Internet. On peut utiliser des constellations de satellites en orbite basse en revanche pour acheminer du trafic Internet.