Réseau et UNIX

Sergey Kirgizov

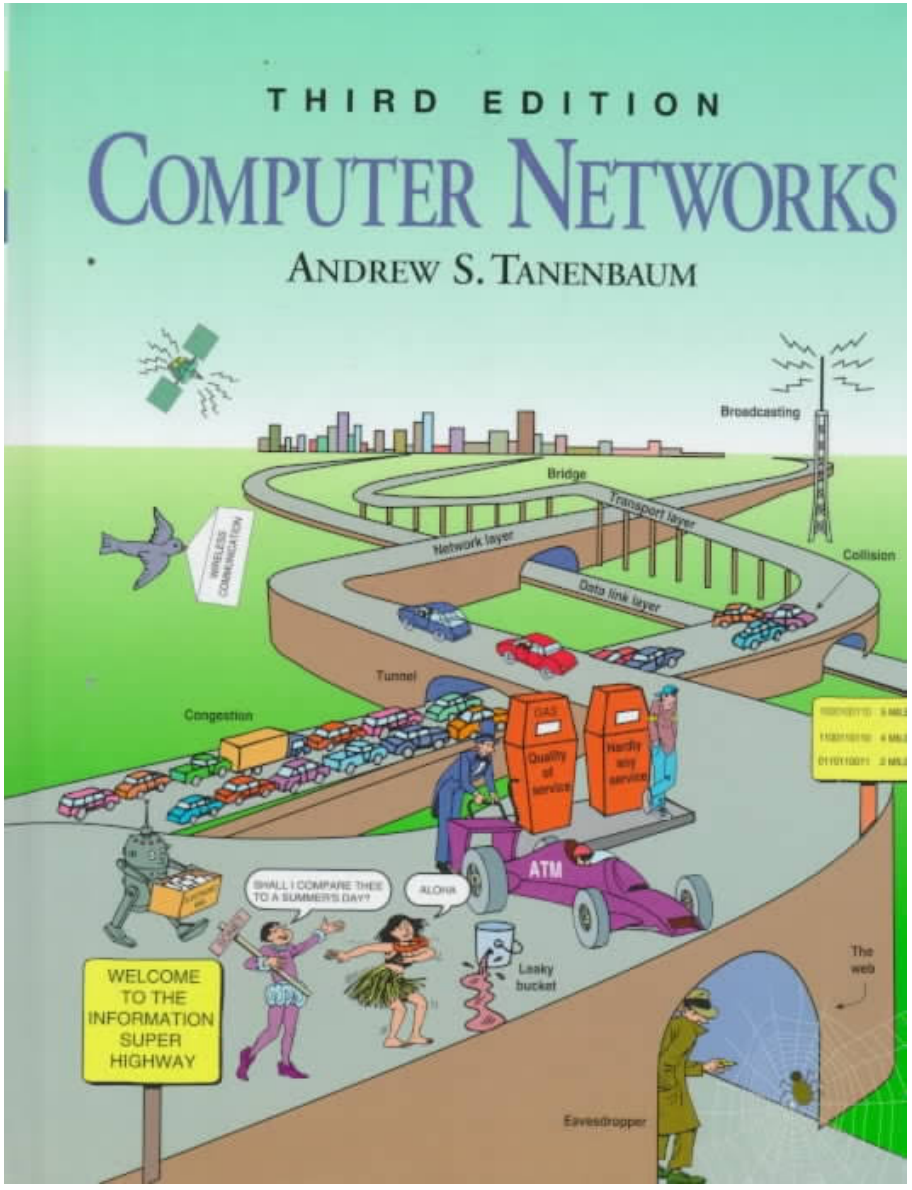
Quelques éléments de base

- Le livre d'Andrew Tanenbaum
- Standard Internet, RFC
- Différents niveaux de protocoles

Quelques commandes shell

- Ouvrir des connexions
- Voir l'état des connections

Very good book



RFC — Request for Comments

Les requests for comments (RFC), littéralement «demande de commentaires », sont une série numérotée de documents officiels décrivant les aspects et spécifications techniques de l'Internet, ou de différents matériels informatiques (routeurs, serveur DHCP). Peu de RFC sont des standards, mais tous les documents publiés par l'IETF sont des RFC.

— Wikipedia

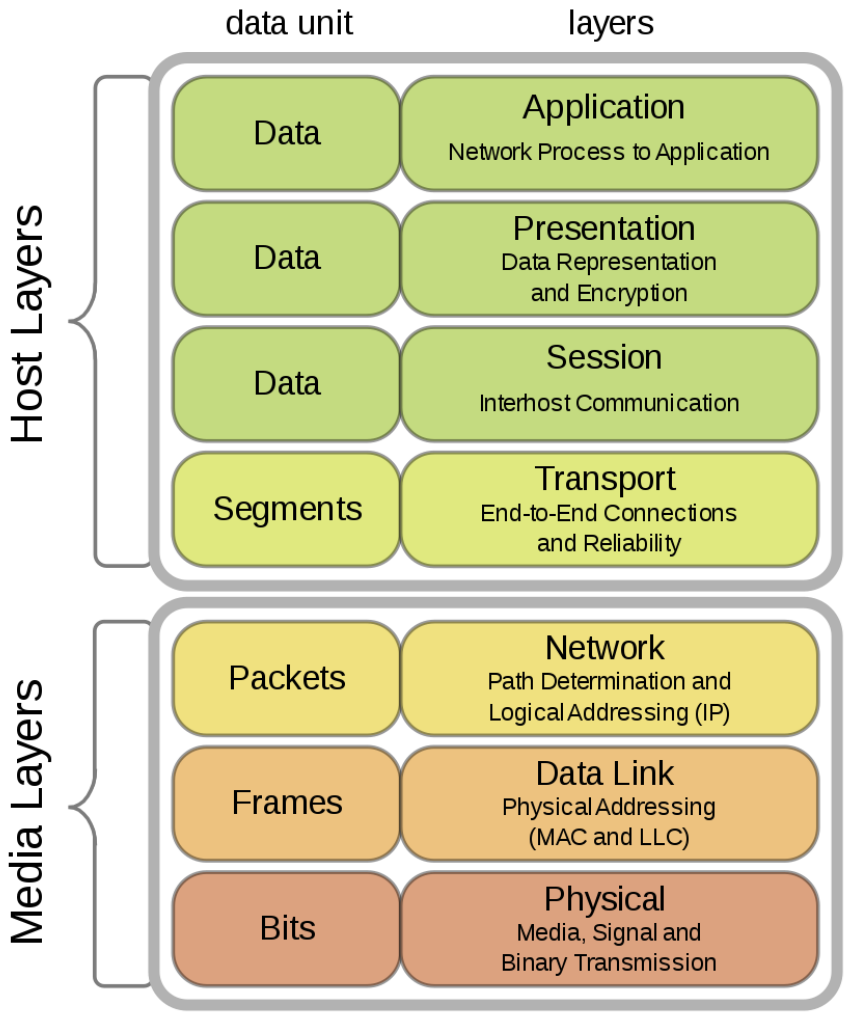
Steve Crocker, l'inventeur des Requests For Comment

Steve Crocker, l'inventeur des Requests For Comment (RFC) créées en 1969. Il est aussi l'auteur de la première RFC.

Exemples

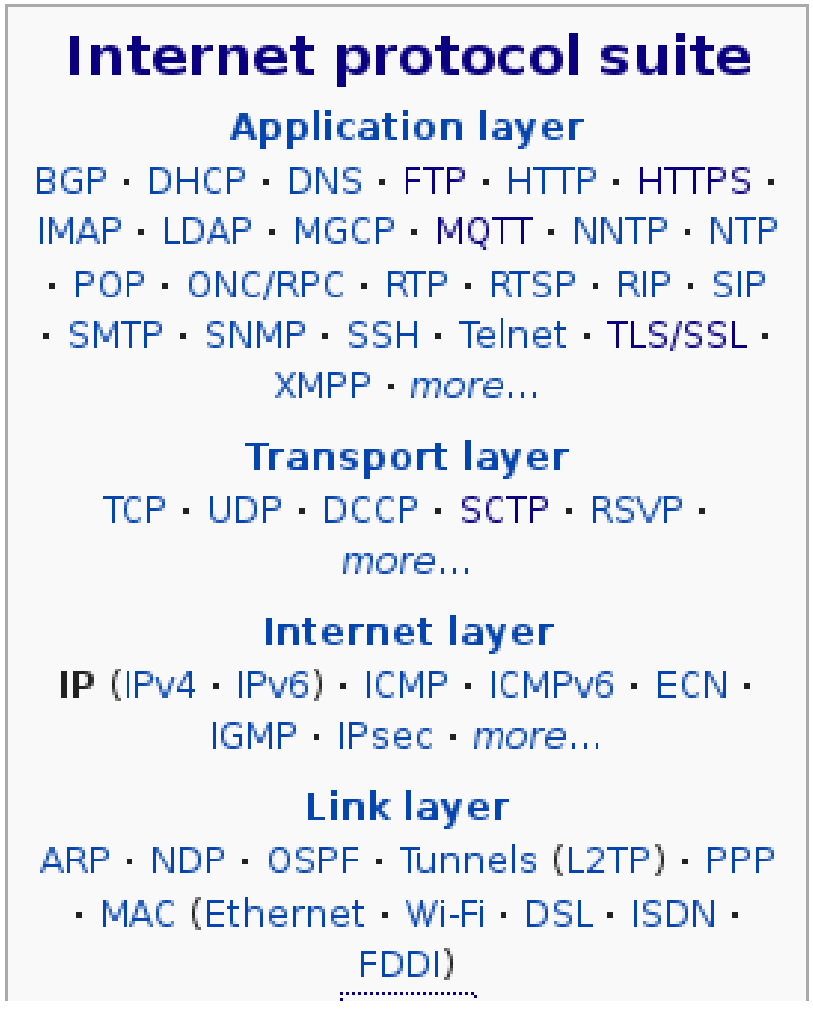
- IP `https://tools.ietf.org/html/rfc791`
- TCP `https://tools.ietf.org/html/rfc793`
- HTTP `https://tools.ietf.org/html/rfc2616`
- Email Address Specification
  `https://tools.ietf.org/html/rfc5322#section-3.4`
- Internet par pigeons voyageurs
  `https://tools.ietf.org/html/rfc1149`

Niveaux de communcation, modèle OSI



Offnfopt @ Wikipedia

Suite des protocoles Internet



https://en.wikipedia.org/wiki/Internet_protocol_suite

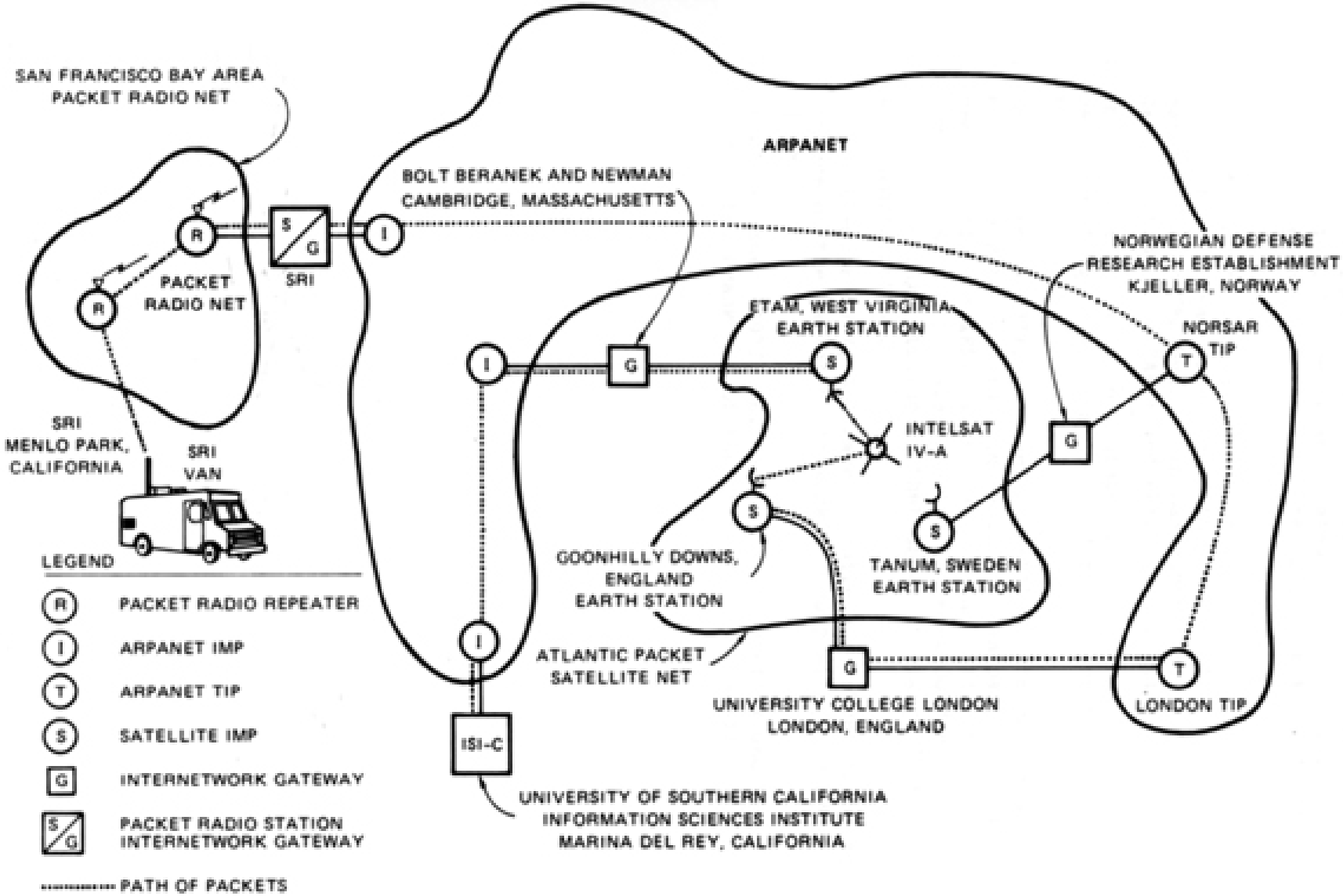
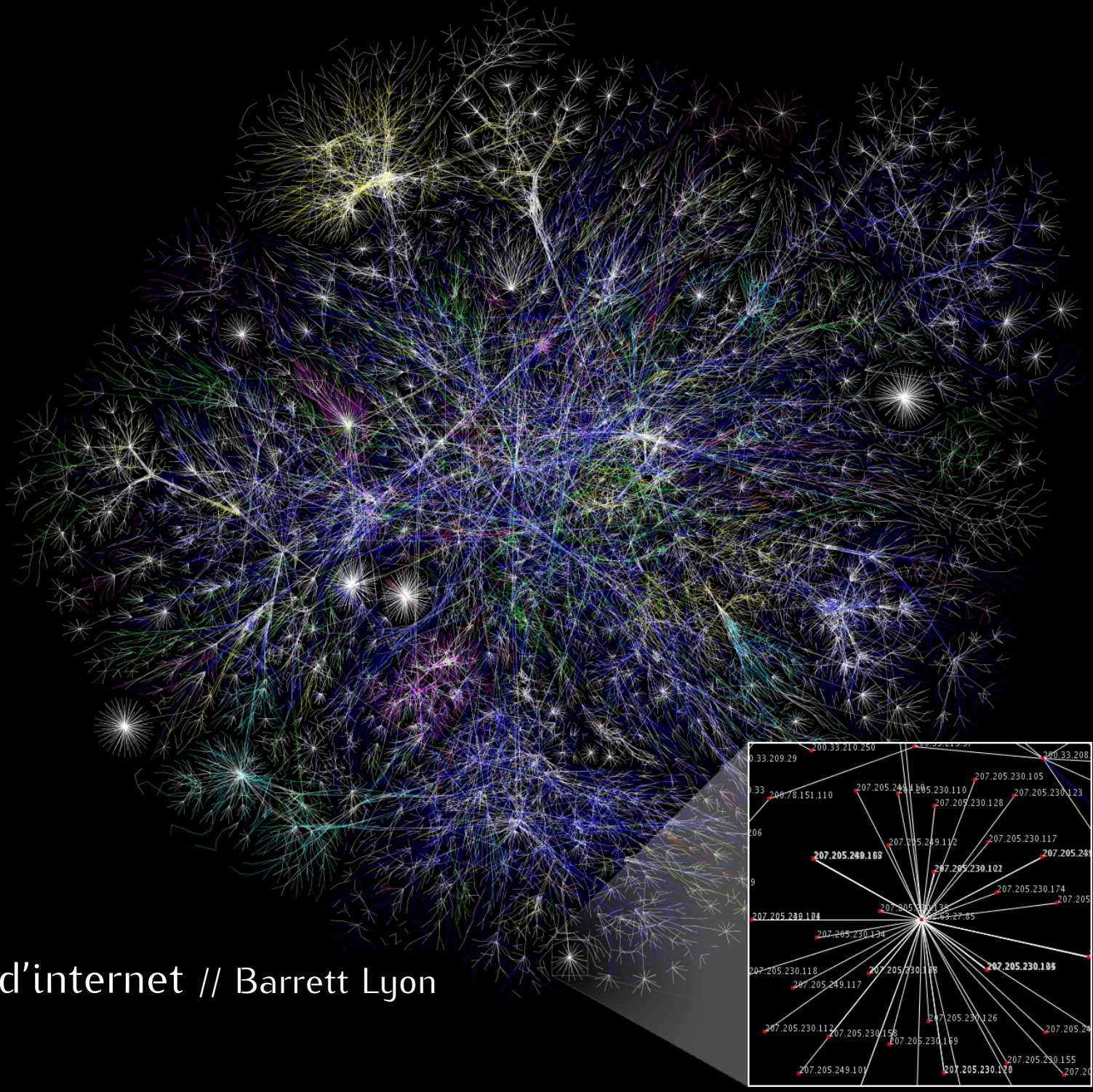


Diagram of the first internetworked connection // SRI International // 1977

The Packet Radio Van was a van refitted by Don Cone at SRI International, and equipped with technology that was used in the first two-way internetworked transmission on August 27, 1976, and the first three-way internetworked transmission on November 22, 1977 ; the latter of which is considered the start of the Internet.
`https://en.wikipedia.org/wiki/Packet_Radio_Van`

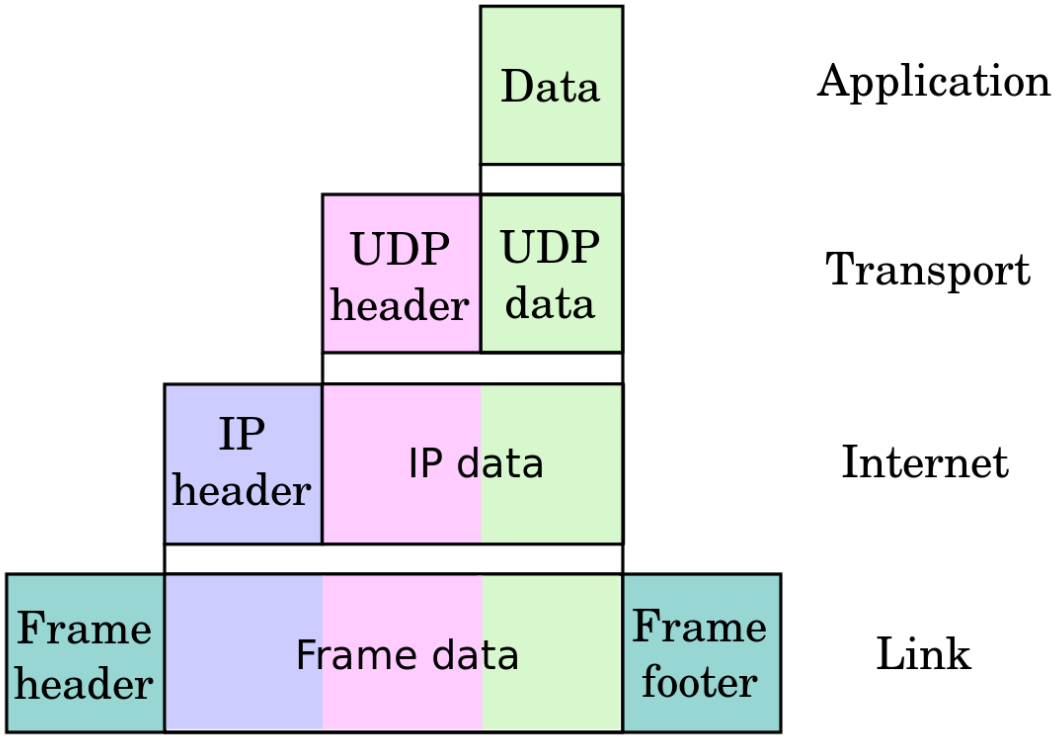


Carte d'internet // Barrett Lyon

Une autre carte d'internet

https://internet-map.net/

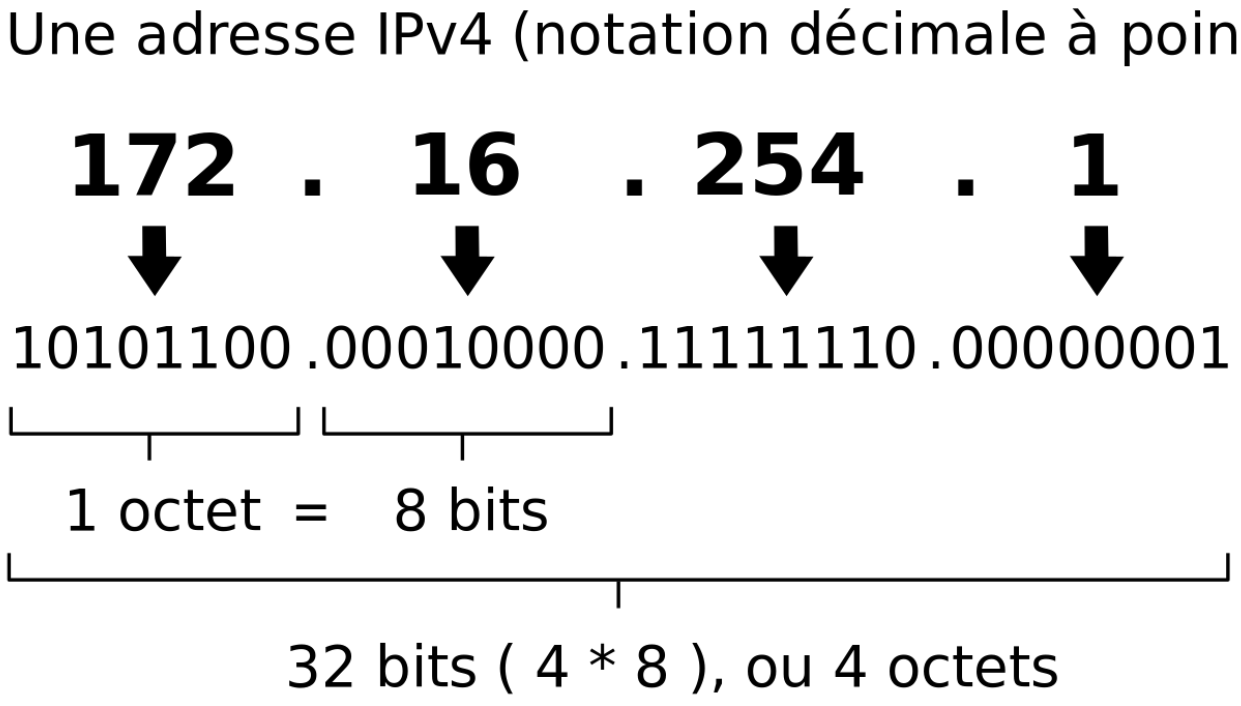
Encapsulation of application data descending through the layered IP architecture



Cburnett et Kbrose @ Wikipedia

Adresse IP v4

L'en-tête IP contient diverses méta-informations, y compris l'adresse de la machine.



Star Trek Man @ Wikipedia

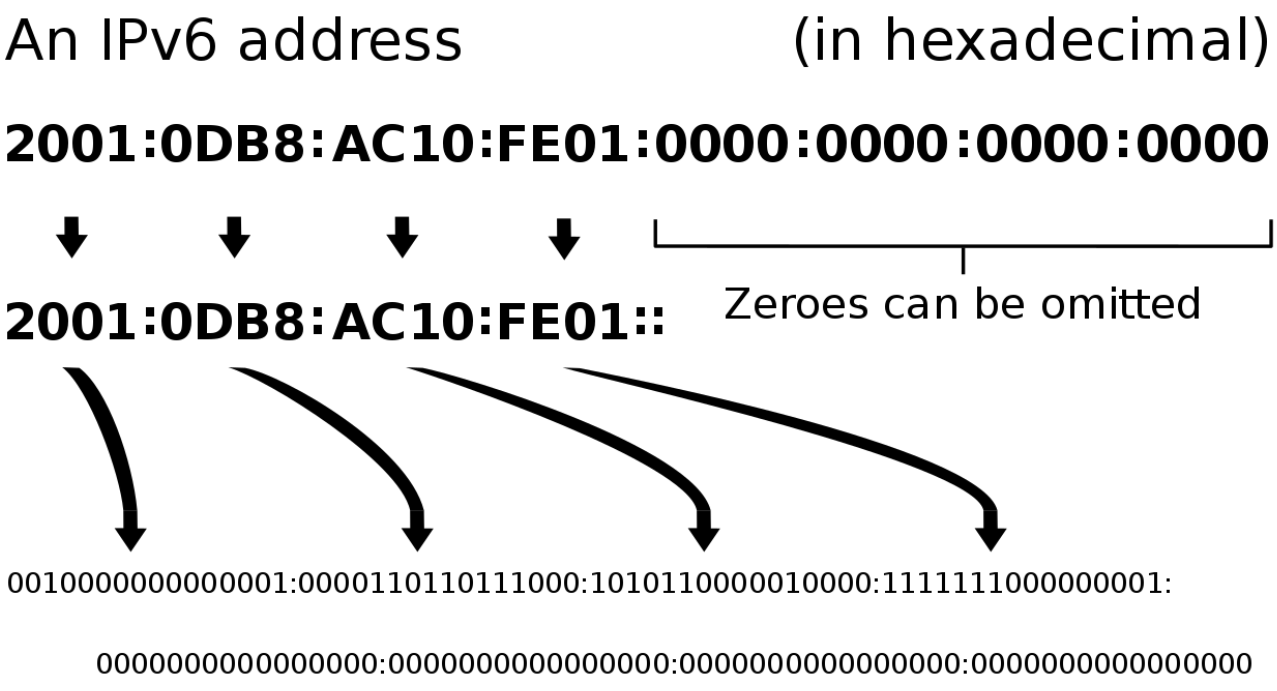
En-tête IPv4

En-tête IPv4

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
Version d'IP				Longueur de l'en-tête				Type de service								Longueur totale															
Identification																Indicateur			Fragment offset											
Durée de vie								Protocole								Somme de contrôle de l'en-tête															
Adresse source																															
Adresse destination																															
Option(s) + remplissage																															

https://fr.wikipedia.org/wiki/IPv4

Adresse IP v6



Wikipedia

ICMP

ICMP (Internet Control Message Protocol) est un protocole qui permet le contrôle des erreurs de transmission. En effet, comme le protocole IP ne gère que le transport des paquets et ne permet pas l'envoi de messages d'erreur, c'est grâce à ce protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau. Il est détaillé dans la RFC 792.

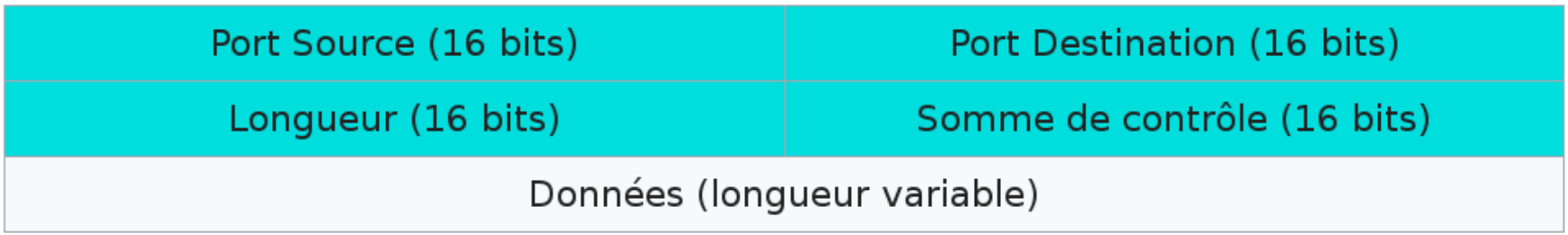
`https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol`
`https://tools.ietf.org/html/rfc792`

UDP - User Datagram Protocol

En plus d'adresse IP on a le numero de port.
65 536 ports distincts par machine.

UDP - User Datagram Protocol

L'en-tête d'un datagramme UDP :



https://fr.wikipedia.org/wiki/User_Datagram_Protocol
https://tools.ietf.org/html/rfc768

TCP - Transmission Control Protocol

Un protocole de transport fiable :

- l'ordre des paquets est préservé
- accusés de réception
- retransmission en cas d'erreur
- adaptations du débit de transmission

Plus de confiance, plus de complexité par rapport à udp

`https://tools.ietf.org/html/rfc793`

HTTP - Hypertext Transfer Protocol

L'un des protocoles les plus populaires de la 7e couche du modèle OSI.

Il a été inventé pour la transmission des documents HTML.

Mais actuellement les gens l'utilisent à d'autres fins : transmission des vidéos, contrôle de robots, allumage d'une cafetière, Web API.

```
josh@blackbox:~$ telnet en.wikipedia.org 80
Trying 208.80.152.2...
Connected to rr.pmtpa.wikimedia.org.
Escape character is '^]'.
GET /wiki/Main_Page http/1.1
Host: en.wikipedia.org
```

Request

```
HTTP/1.0 200 OK
Date: Thu, 03 Jul 2008 11:12:06 GMT
Server: Apache
X-Powered-By: PHP/5.2.5
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Language: en
Vary: Accept-Encoding,Cookie
X-Vary-Options: Accept-Encoding;list-contains=gzip,Cookie;string-contains=enwikiToken;string-contains=enwikiLoggedOut;string-contains=enwiki_session;
string-contains=centralauth_Token;string-contains=centralauth_Session;string-contains=centralauth_LoggedOut
Last-Modified: Thu, 03 Jul 2008 10:44:34 GMT
Content-Length: 54218
Content-Type: text/html; charset=utf-8
X-Cache: HIT from sq39.wikimedia.org
X-Cache-Lookup: HIT from sq39.wikimedia.org:3128
Age: 3
X-Cache: HIT from sq38.wikimedia.org
X-Cache-Lookup: HIT from sq38.wikimedia.org:80
Via: 1.0 sq39.wikimedia.org:3128 (squid/2.6.STABLE18), 1.0 sq38.wikimedia.org:80 (squid/2.6.STABLE18)
Connection: close
```

Response headers

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">
        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
                        <meta name="keywords" content="Main Page,1778,1844,1863,1938,1980 Summer Olympics,2008,2008 Guizhou riot,2008 Jerusal
...
''' This content has been removed to save space
'''
"Non-profit organization">nonprofit</a> <a href="http://en.wikipedia.org/wiki/Charitable_organization" title="Charitable organization">charity</a>.<b
r /></li>
                                <li id="privacy"><a href="http://wikimediafoundation.org/wiki/Privacy_policy" title="wikimedia:Privacy policy">Privac
y policy</a></li>
                                <li id="about"><a href="/wiki/Wikipedia:About" title="Wikipedia:About">About Wikipedia</a></li>
                                <li id="disclaimer"><a href="/wiki/Wikipedia:General_disclaimer" title="Wikipedia:General disclaimer">Disclaimers</a>
</li>
                        </ul>
                </div>
</div>

                <script type="text/javascript">if (window.runOnloadHook) runOnloadHook();</script>
<!-- Served by srv93 in 0.050 secs. --></body></html>
```

Response body

HTTP Exemple // TheJosh @ Wikipedia

Quelques commandes shell

Configuration réseaux

Commandes utiles

- `ifconfig` - configure a network interface
- `route` - show / manipulate the IP routing table
- `iwconfig` - configure a wireless network interface
- `ip` - show / manipulate routing, devices, policy routing and tunnels

Telnet

Example

telnet towel.blinkenlights.nl
telnet telehack.com

Netcat de Hobbit

NAME

nc - TCP/IP swiss army knife

SYNOPSIS

nc [-options] hostname port[s] [ports] ... nc -l -p port [-options] [hostname] [port]

DESCRIPTION

netcat is a simple unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities. Netcat, or "nc" as the actual program is named, should have been supplied long ago as another one of those cryptic but standard Unix tools. ...

AUTHOR

This manual page was written by Joey Hess <joeyh@debian.org> and Robert Woodcock <rcw@debian.org>, cribbing heavily from Netcat's README file. Netcat was written by a guy we know as the Hobbit <hobbit@avian.org>

COPYRIGHT de Hobbit

COPYRIGHT

Netcat is entirely my own creation, although plenty of other code was used as examples. It is freely given away to the Internet community in the hope that it will be useful, with no restrictions except giving credit where it is due. No GPLs, Berkeley copyrights or any of that nonsense. The author assumes NO responsibility for how anyone uses it. If netcat makes you rich somehow and you're feeling generous, mail me a check. If you are affiliated in any way with Microsoft Network, get a life. Always ski in control. Comments, questions, and patches to hobbit@avian.org.

Net Cat family

`https://en.wikipedia.org/wiki/Netcat`

- **Traditional nc** écrit par *Hobbit*, dernière version 1.10 (March 20, 1996)
- **OpenBSD Netcat**, Eric Jackson, 1.98 (July 3, 2010)
- **GNU Netcat**, Giovanni Giacobbi, 0.7.1 (January 11, 2004)
- **Netcat 6**, Mauro Tortonesi et al., 1.0 (January 19, 2006)
- **ncat**, Fyodor et al., 7.70 (Mars 20, 2018)
- **pnetcat, socat, sock, socket, sbd**, etc...

`https://en.wikipedia.org/wiki/Talk:Netcat#Variants`

ncat --broker

Les connexions simultanées ne sont pas possibles avec netcat traditionnel. `ncat` est plus avancé, il a un mode `-broker`, permettant à plusieurs parties de communiquer entre elles.

Serveur

```
ncat --listen --broker -p 1025
```

Client 1

```
nc SERVER.HOSTNAME.OR-IP.ADRESS 1025
```

Client 2

```
telnet SERVER.HOSTNAME.OR-IP.ADRESS 1025
```

Client 3

```
ncat SERVER.HOSTNAME.OR-IP.ADRESS 1025
```

Traceroute

La commande **traceroute** imprime les adresses des mashines-routeurs sur le chemin vers le serveur

Traceroute exemple

```
user@machine:/home$ % traceroute fr.wikipedia.org
traceroute to rr.knams.wikimedia.org (145.97.39.155), 30 hops max, 38 byte packets
 1  80.67.162.30 (80.67.162.30)  0.341 ms  0.300 ms  0.299 ms
 2  telehouse2-gw.netaktiv.com (80.67.170.1)  5.686 ms  1.656 ms  0.428 ms
 3  giga.gitoyen.net (80.67.168.16)  1.169 ms  0.704 ms  0.563 ms
 4  62.4.73.27 (62.4.73.27)  2.382 ms  1.623 ms  1.297 ms
 5  ge5-2.mpr2.cdg2.fr.above.net (64.125.23.86)  1.196 ms ge9-4.mpr2.cdg2.fr.above.net (64.125.23.102)  1
 6  so-5-0-0.cr1.lhr3.uk.above.net (64.125.23.13)  41.900 ms  9.658 ms  9.118 ms
 7  so-7-0-0.mpr1.ams5.nl.above.net (64.125.27.178)  23.403 ms  23.209 ms  23.703 ms
 8  64.125.27.221.available.above.net (64.125.27.221)  19.149 ms so-0-0-0.mpr3.ams1.nl.above.net (64.125.2
 9  PNI.Surfnet.ams1.above.net (82.98.247.2)  16.834 ms  16.384 ms  16.129 ms
10  af-500.xsr01.amsterdam1a.surf.net (145.145.80.9)  21.525 ms 20.645 ms  24.101 ms
11  kncsw001-router.customer.surf.net (145.145.18.158)  20.233 ms 16.868 ms  19.568 ms
12  gi0-24.csw2-knams.wikimedia.org (145.97.32.29)  23.614 ms  23.270 ms  23.574 ms
13  rr.knams.wikimedia.org (145.97.39.155)  23.992 ms  23.050 ms 23.657 ms
```

netstat

Extrait du man

netstat - Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

Exemples

- `netstat -apt`
  affiche toutes les connexions TCP et les programmes associés
- `netstat -apu`
  les connexions UDP et les programmes associés
- `netstat -apx`
  affiche toutes les connexions type “Socket UNIX” et les programmes associés

Les sockets UNIX sont une sorte de réseau local, limitée à une seule machine.

Questions ?

Bonus !

https://en.wikipedia.org/wiki/List_of_Unix_commands