Réseaux : 5° partie

1970 : NCP (Network Control Program)
1971 : FTP (1980), Telnet (1983)
1972 : Courriel - email
1973 : Ethernet (1976)
1974 : TCP/IP
1979 : Usenet
1980 : IPv4, TCP, UDP, FTP
1981 : ICMP
1982 : SMTP
1983 : Telnet, DNS
1985 : NTP
1985 : BOOTP
1989 : WWW
1990 : HTTP
1988 : IRC
1993 : DHCP
1995 : SSH
1996 : HTTP 1.0, POP3, RTP, ICQ
1998 : IPv6, Jabber (XMPP)
1999 : MSN (Microsoft)
2002 : BitTorrent
...

Bibliographie

- "TCP/IP sous Linux" de JF Bouchaudy - Formation Tsoft © Ed. Eyrolles
- "TCP/IP Administration de réseau" de Craig Hunt © Ed. O'Reilly
- "Les protocoles TCP/IP et Internet" d'Eric Lapaille © NetLine 1999
- "Technique des réseaux locaux sous Unix" de L. Toutain © Ed. Hermes
- "Pratique des réseaux locaux d'entreprise" de JL Montagnier © Ed. Eyrolles
- "Transmission et Réseaux" de S. Lohier et D. Present © ED. DUNOD
- Les sites www.frameip.com, fr.wikipedia.org, www.w3.org, etc ...

Les commandes de base

Description	*Linux*	*Windows*
Configurer une interface réseau	ifconfig	ipconfig, netsh, net
Afficher les connexions réseau, les tables de routage, les statistiques des interfaces, ...	netstat	netstat
Envoyer des datagrammes ICMP ECHO_REQUEST à des hôtes sur un réseau	ping	ping
Afficher le chemin qu'un paquet IP va prendre pour aller d'une machine A à une machine B	traceroute	tracert
Suivre le chemin qu'un paquet IP va prendre pour aller d'une machine A à une machine B pour découvrir le MTU à utiliser sur ce chemin	tracepath	
Afficher et manipuler la table de routage IP	route	route
Manipuler la table ARP du système	arp	arp
Outil d'analyse et de capture réseau	ethereal/wireshark tcpdump	ethereal/wireshark windump
Outil d'exploration réseau et analyseur de sécurité	nmap	nmap
Fournir un moyen de communication TCP bi-directionnel et orienté octet (caractère)	telnet	telnet, putty
Lire et écrire en utilisant TCP ou UDP	netcat	netcat
Remarque :		
Accès aux options des commandes	nom_commande -h nom_commande --help	nom_commande /?
Accès à la documentation	man nom_commande	

Les fichiers de configuration

Description	*Linux*	*Windows*
Configuration réseau	**Fichiers texte dans /etc/ /proc/net**	**Panneau de configuration Base de registre (regedit)**

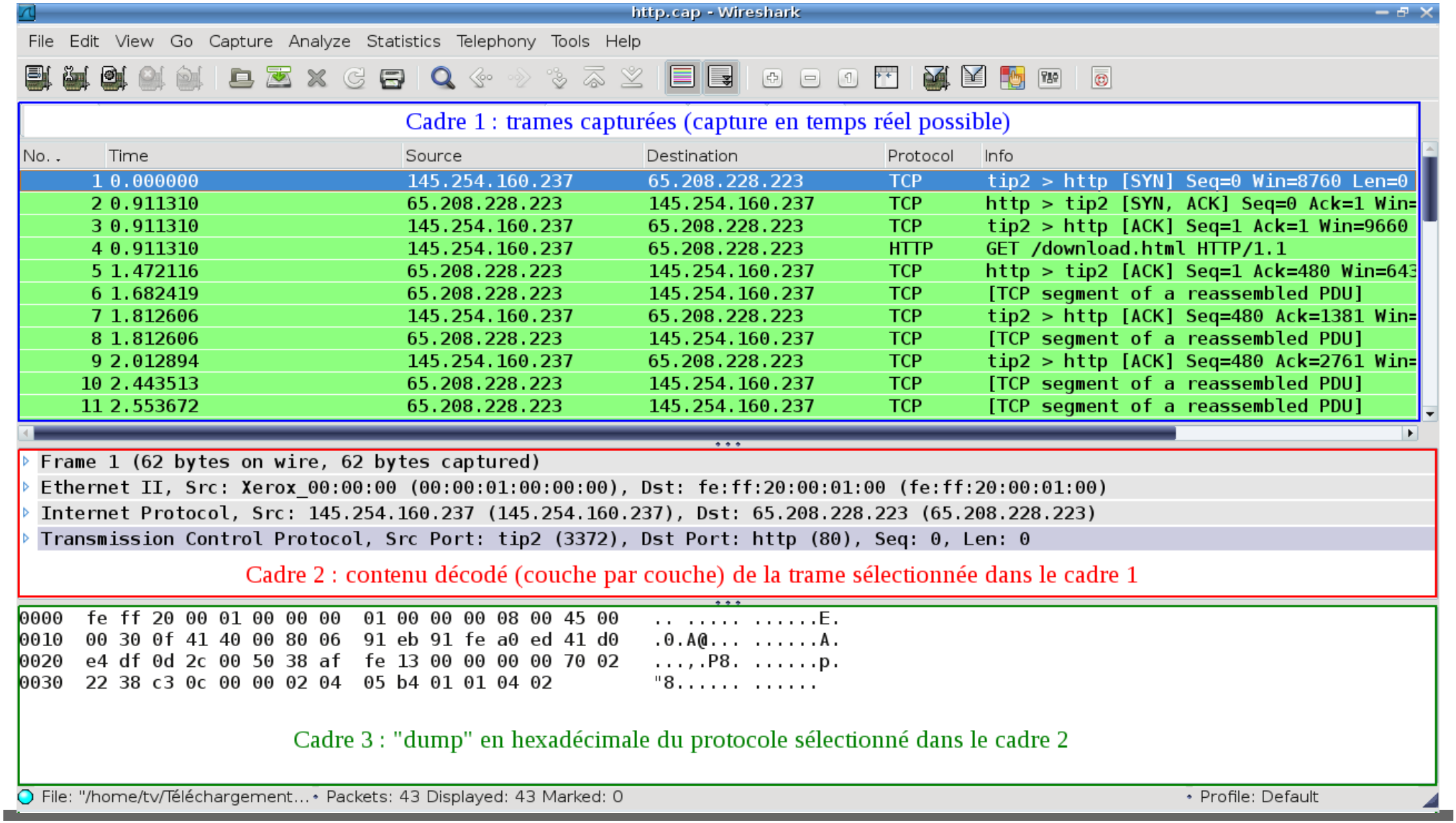
Fichier	*Description*
Mandriva : `/etc/sysconfig/network-scripts/ifcfg-eth0` **Ubuntu : `/etc/network/interfaces`**	Configuration des interfaces
`/etc/host.conf`	Configuration de la résolution de noms
`/etc/hosts`	Correspondances statiques de noms d'hôtes
`/etc/ethers`	Base de données adresses Ethernet - adresses IP
`/etc/resolv.conf`	Fichier de configuration de la résolution de noms
`/etc/protocols`	Fichier de définition des protocoles internet
`/etc/services`	Liste des services internet

Analyseur de protocole

- tcpdump est un « packet sniffer » en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau. C'est un outil de mise au point apprécié pour sa puissance. Site officiel : http://www.tcpdump.org/

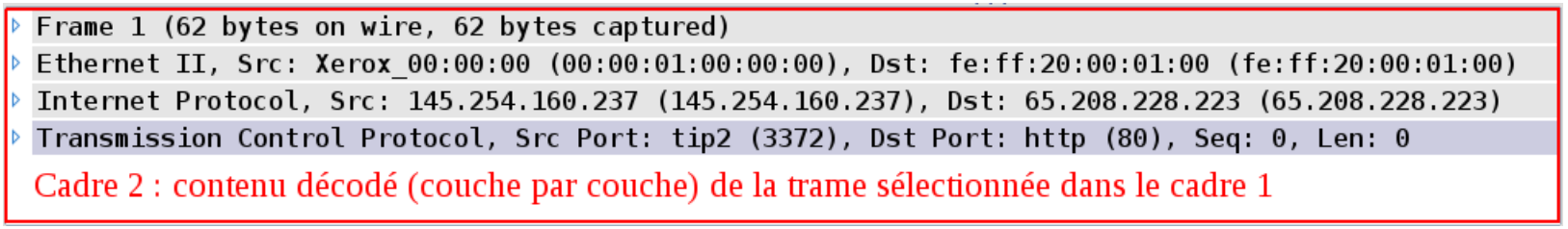
- Wireshark (anciennement Ethereal) est un logiciel libre d'analyse de protocole, ou « packet sniffer », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage. Wireshark est multi-plates-formes, il fonctionne sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD. Wireshark reconnait 759 protocoles. Site officiel : http://www.wireshark.org/

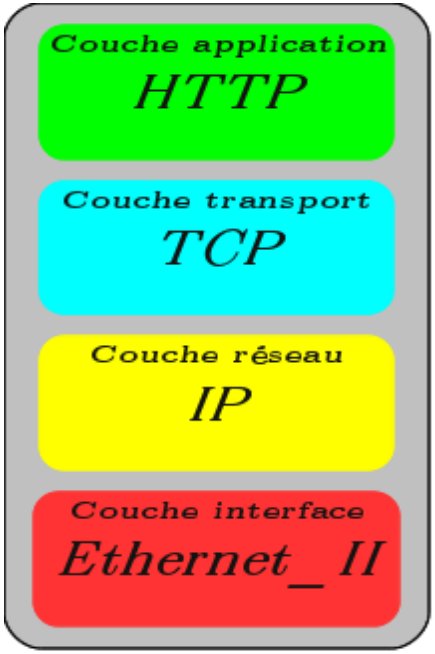
wireshark


http.cap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Cadre 1 : trames capturées (capture en temps réel possible)
No. Time Source Destination Protocol Info
1 0.000000 145.254.160.237 65.208.228.223 TCP tip2 > http [SYN] Seq=0 Win=8760 Len=0
2 0.911310 65.208.228.223 145.254.160.237 TCP http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=
3 0.911310 145.254.160.237 65.208.228.223 TCP tip2 > http [ACK] Seq=1 Ack=1 Win=9660
4 0.911310 145.254.160.237 65.208.228.223 HTTP GET /download.html HTTP/1.1
5 1.472116 65.208.228.223 145.254.160.237 TCP http > tip2 [ACK] Seq=1 Ack=480 Win=643
6 1.682419 65.208.228.223 145.254.160.237 TCP [TCP segment of a reassembled PDU]
7 1.812606 145.254.160.237 65.208.228.223 TCP tip2 > http [ACK] Seq=480 Ack=1381 Win=
8 1.812606 65.208.228.223 145.254.160.237 TCP [TCP segment of a reassembled PDU]
9 2.012894 145.254.160.237 65.208.228.223 TCP tip2 > http [ACK] Seq=480 Ack=2761 Win=
10 2.443513 65.208.228.223 145.254.160.237 TCP [TCP segment of a reassembled PDU]
11 2.553672 65.208.228.223 145.254.160.237 TCP [TCP segment of a reassembled PDU]
Frame 1 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Internet Protocol, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
Cadre 2 : contenu décodé (couche par couche) de la trame sélectionnée dans le cadre 1
0000 fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45 00 .. ..E.
0010 00 30 0f 41 40 00 80 06 91 eb 91 fe a0 ed 41 d0 .0.A@... ......A.
0020 e4 df 0d 2c 00 50 38 af fe 13 00 00 00 00 70 02 ...,.P8. ......p.
0030 22 38 c3 0c 00 00 02 04 05 b4 01 01 04 02 "8..... ......
Cadre 3 : "dump" en hexadécimale du protocole sélectionné dans le cadre 2
File: "/home/tv/Téléchargement... Packets: 43 Displayed: 43 Marked: 0 Profile: Default

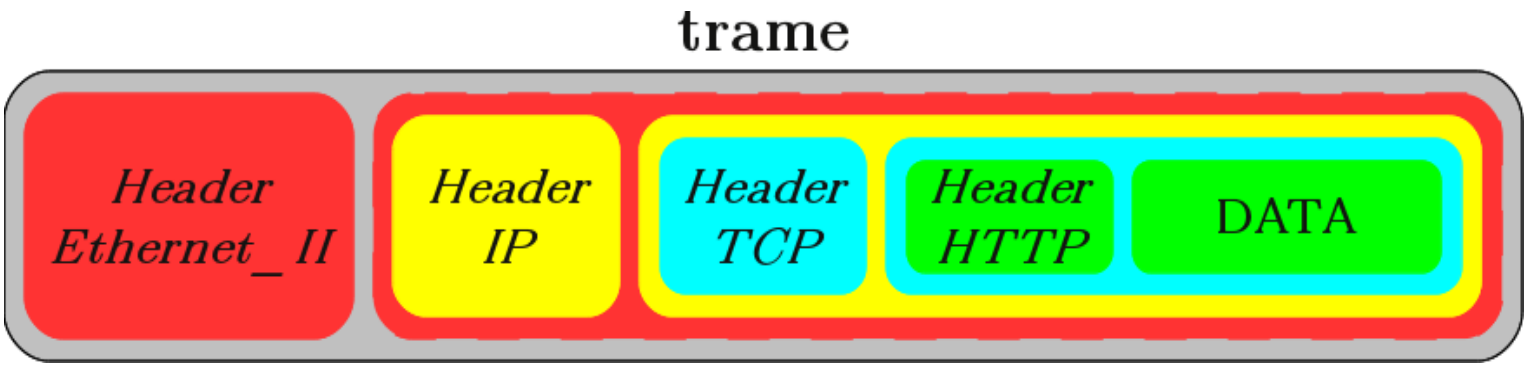
Encapsulation

- Le cadre 2 de wireshark illustre le principe de l'encapsulation des protocoles utilisées dans l'échange d'une trame.



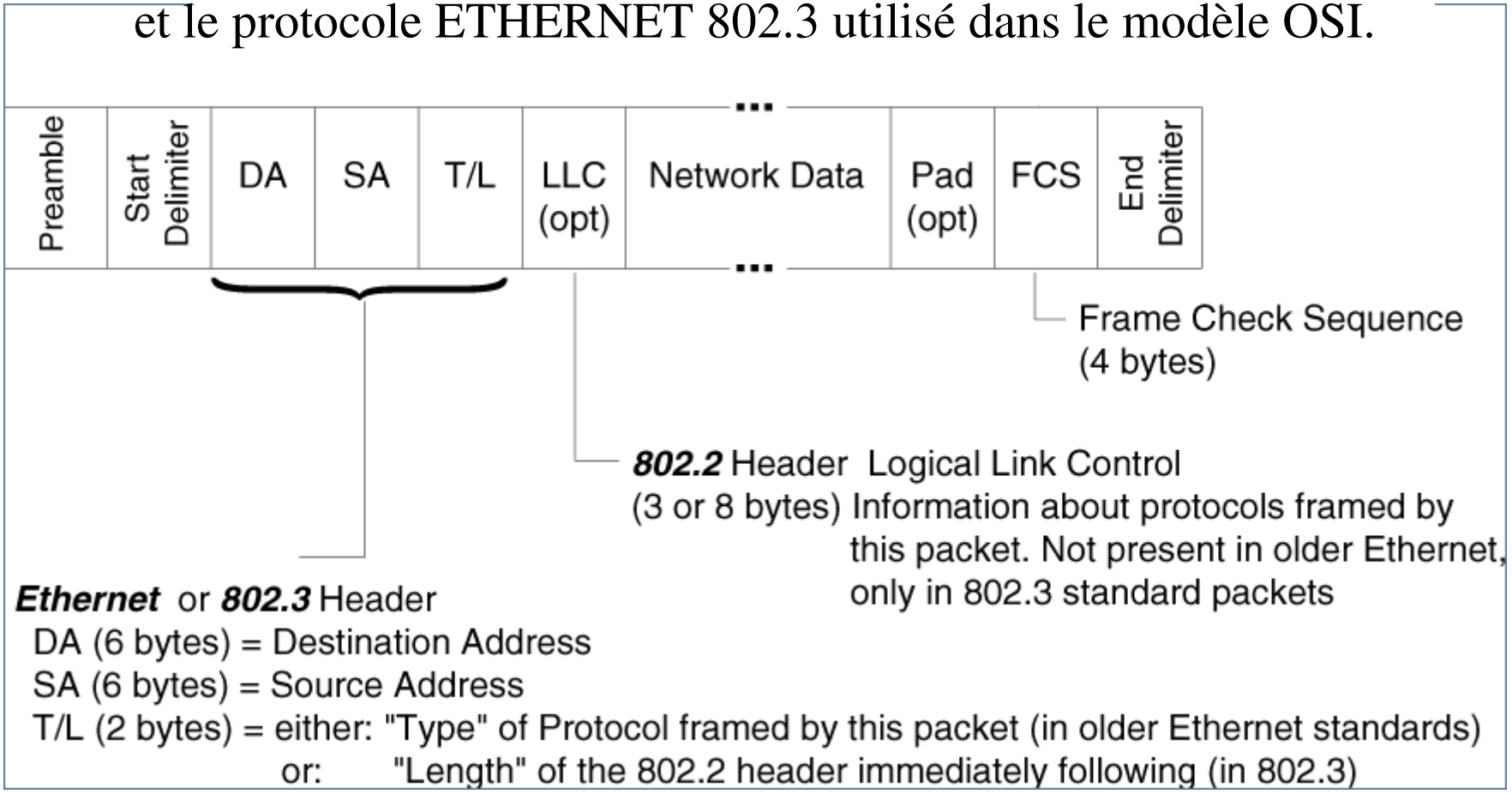


Modèle DoD



Trames Ethernet

- On distinguera deux protocoles pour les trames Ethernet :
  le protocole ETHERNET_II, plus ancien et utilisé dans le modèle TCP/IP
  et le protocole ETHERNET 802.3 utilisé dans le modèle OSI.



Tracer la route

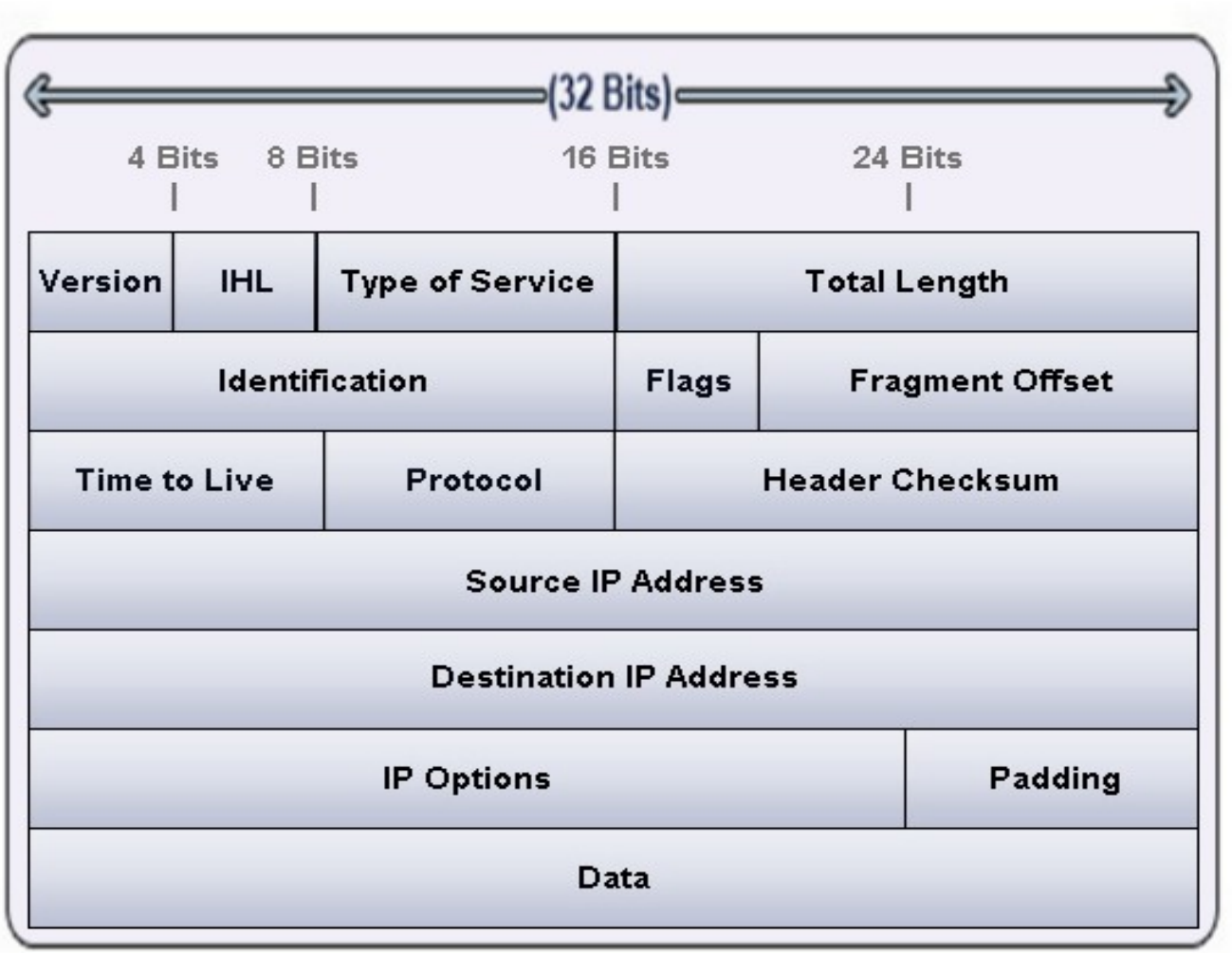
- traceroute est un programme utilitaire qui permet de suivre le chemin qu'un paquet de données (paquet IP) va prendre pour aller de la machine locale à une autre machine connectée au réseau. En exploitant le champ TTL de l'en-tête IP, il découvre ainsi les routeurs de proche en proche.


```
# traceroute -nI www.google.fr
traceroute to www.google.fr (209.85.227.104), 30 hops max, 60 byte packets
 1  192.168.52.1  0.935 ms  1.185 ms  1.449 ms
 2  90.36.253.1  118.547 ms  119.879 ms  122.841 ms
 3  10.125.49.14  124.873 ms  124.961 ms  125.348 ms
 4  193.253.86.234  126.607 ms  127.735 ms  130.226 ms
 5  193.252.101.86  138.891 ms  140.009 ms  141.475 ms
 6  193.252.161.182  149.277 ms  149.219 ms  150.707 ms
 7  193.251.128.226  152.001 ms 193.251.128.230  176.682 ms 193.251.129.57  176.654 ms
 8  193.251.249.46  175.432 ms  177.436 ms  177.426 ms
 9  209.85.250.142  203.125 ms  202.047 ms  201.006 ms
10  216.239.43.233  188.632 ms  181.575 ms  186.189 ms
11  209.85.252.83  181.654 ms  177.028 ms 216.239.49.45  176.469 ms
12  209.85.243.93  186.766 ms 209.85.243.97  175.459 ms 209.85.243.93  208.022 ms
13  209.85.227.104  196.754 ms  195.144 ms  191.072 ms
```

Protocole IPv4

IP (*Internet Protocol*) représente le protocole réseau le plus répandu. Il permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée.

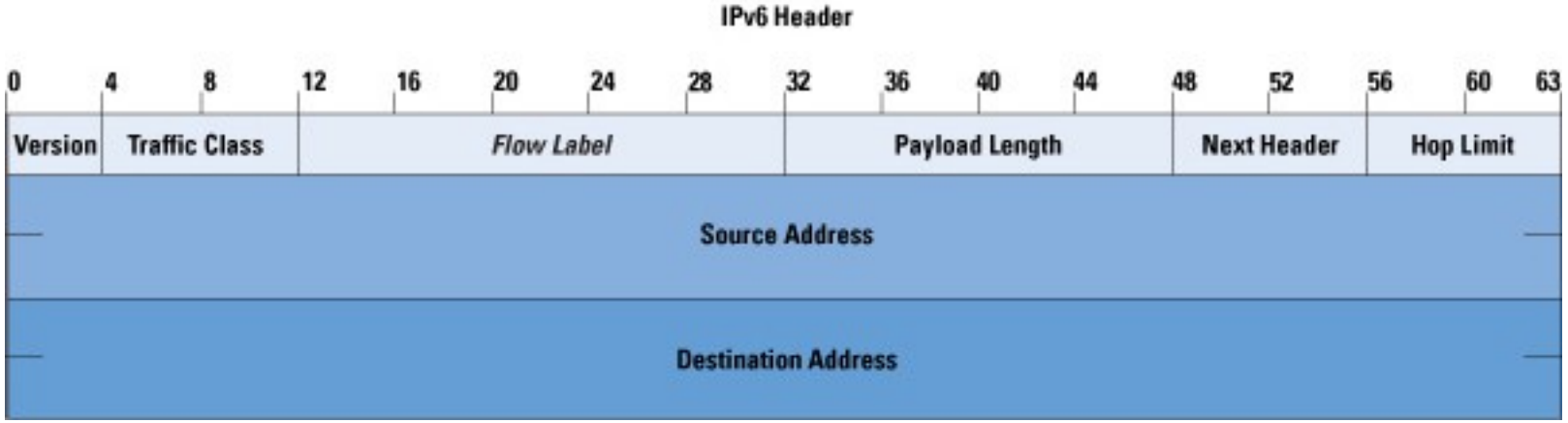
Ce protocole utilise ainsi la technique dite de commutation de paquets. Les détails du protocole IP sont spécifiés dans la RFC791.



Protocole IPv6

- Les différences avec IPv4 :
  - Les champs *Traffic Class* et *Flow Label* ont un rôle équivalent à TOS
  - Le champ *Hop Limit* remplace le champ TTL (64 par défaut)
  - Le champ *Next Header* permet un chaînage des options
  - Les adresses IP sources et destination sont codées sur 128 bits (soit 16 octets)

Le champ *Next Header* (NH) :
0 : option "Hop-by-Hop"
4 : IPv4
6 : TCP
17 : UDP
43 : option "Routing Header"
44 : option "Fragment Header"
45 : Interdomain Routing Protocol
46 : RSVP
50 : option "Encapsulation Security Payload" (IPsec)
51 : option "Authentification Header" (IPsec)
58 : ICMP
59 : No next header
60 : option "Destination Options Header"



Tester l'état de la connexion (*ping*)

- En utilisant le protocole ICMP, la commande **ping** permet d'obtenir des informations (en particulier le temps de réponse de la machine à travers le réseau) et aussi quel est l'état de la communication avec cette machine.

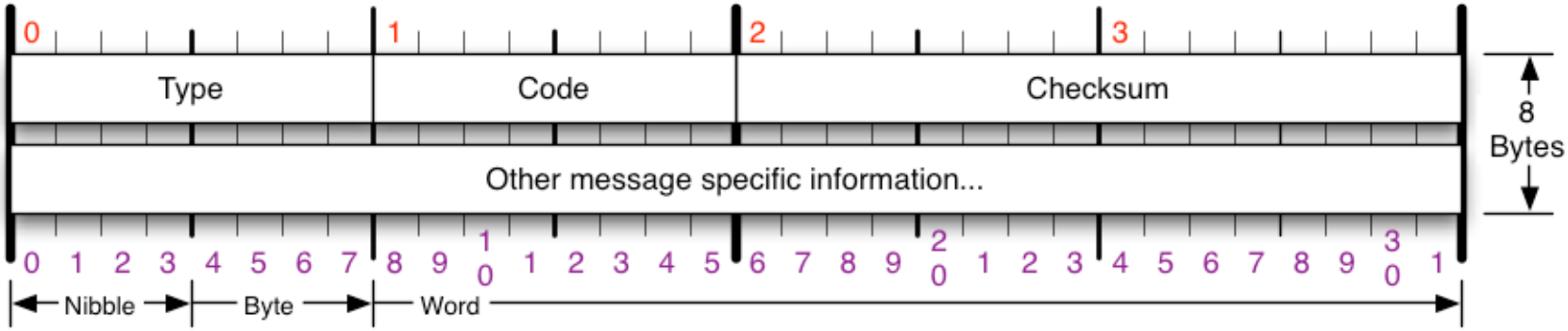
```
# ping -c 1 -t 12 209.85.227.104
PING 209.85.227.104 (209.85.227.104) 56(84) bytes of data.
From 209.85.243.101 icmp_seq=1 Time to live exceeded

# ping -c 1 -t 13 209.85.227.104
PING 209.85.227.104 (209.85.227.104) 56(84) bytes of data.
64 bytes from 209.85.227.104: icmp_seq=1 ttl=52 time=149 ms

rtt min/avg/max/mdev = 149.220/149.220/149.220/0.000 ms
```

Protocole ICMP

- ICMP (*Internet Control Message Protocol*) est un protocole de la couche Réseau qui transmet des message de contrôle et d'erreurs (RFC 792). Um message ICMP est encapsulé dans un paquet IP.



L'utilisation la plus connue du protocole ICMP est celle de la commande **ping** qui permet d'obtenir des informations (en particulier le temps de réponse de la machine à travers le réseau) et aussi quel est l'état de la communication avec cette machine.

ICMP Message Types

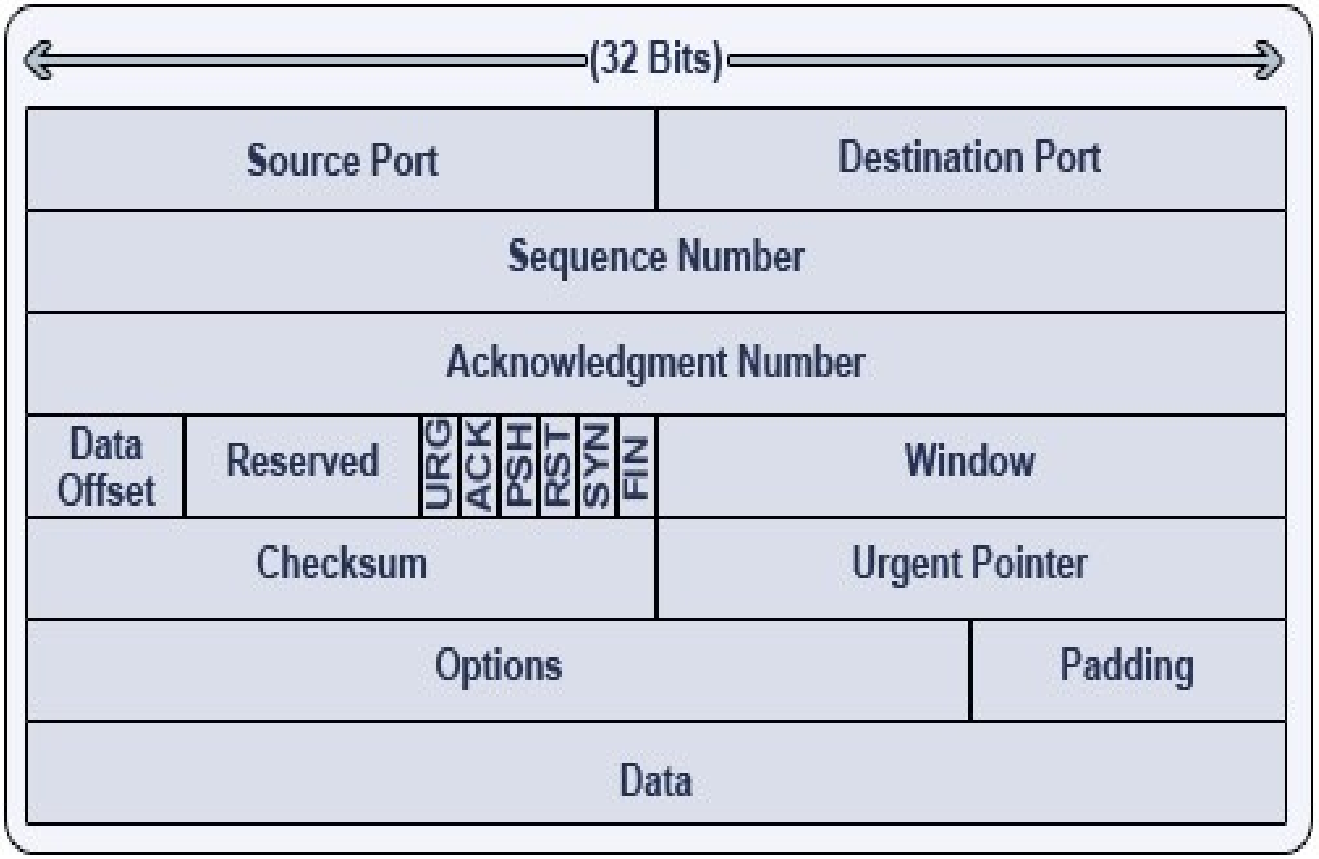
Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS

Type	Code/Name
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection

Type	Code/Name
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Protocole TCP

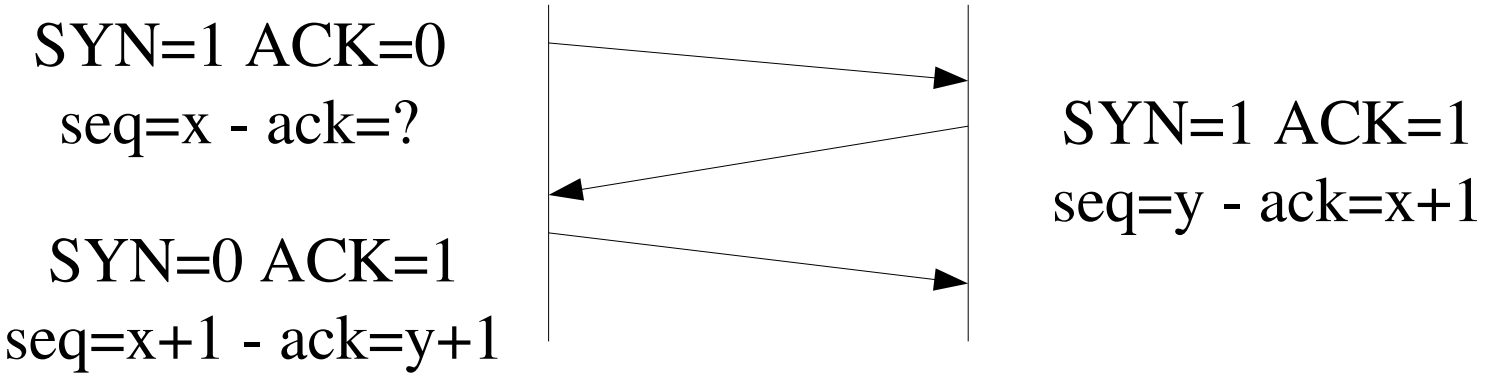
TCP (*Transmission Control Protocol*) est un protocole de transport fiable, en mode connecté (RFC 793) qui assure la transmission des données de bout en bout (d'un processus à un autre processus).



Modes de communication

- De manière générale, on distingue deux techniques possibles pour assurer une communication ou pour caractériser un protocole :
  - Le mode connecté : ce mode se déroule en trois phases (établissement de la liaison, transmission et libération). Exemples : le protocole TCP, le téléphone, …

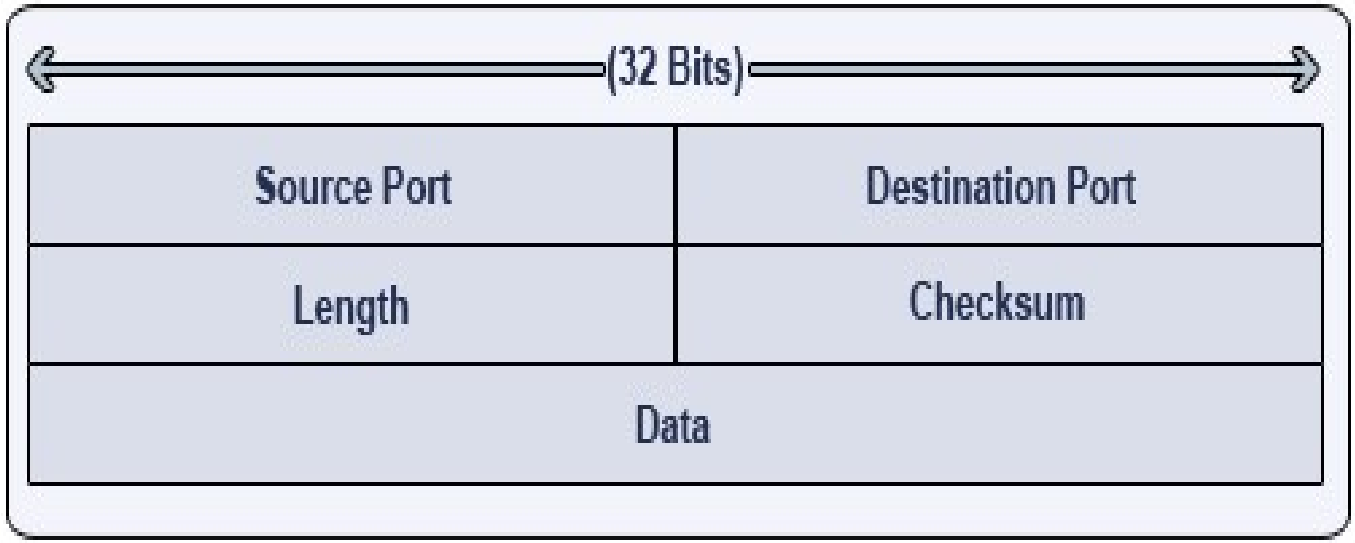
Exemple d'une connexion TCP en trois temps (*Three Way Handshake*)



  - Le mode non connecté : ce mode ne nécessite pas de phase de connexion (et donc de libération). On transmet directement. Le mode non connecté est décrit de manière générale comme moins fiable mais plus rapide que le mode connecté. Exemple : les protocoles IP et UDP, la diffusion télévision hertzienne ou satellite, ...

Protocole UDP

UDP (*User Datagram Protocol*) est un protocole souvent décrit comme étant non-fiable, en mode non-connecté (RFC 768), mais plus rapide que TCP.



Protocole HTTP

- Le Protocole HTTP (*HyperText Transfert Protocol*) sert notamment au dialogue entre un client web (navigateur par exemple) et un serveur (apache par exemple).
- Comme la plupart des protocoles de la couche Application, c'est un **protocole orienté texte (ASCII),** basé sur TCP. Il existe deux spécifications la 1.0 et la 1.1 (RFC 1945).

Requête HTTP

```
GET /index.html HTTP/1.1\r\n
Host: www.btsiris.net\r\n
\r\n
```

→ Ligne vide = fin de l'en-tête HTTP

En-tête

Le corps est vide

Corps

Réponse HTTP

```
HTTP/1.1 200 OK
Date: Wed, 10 Mar 2010 09:58:08 GMT
Server: Apache/2.2.11 (Mandriva
Linux/PREFORK-10.7mdv2009.1)
Content-Length: 215
Connection: close
Content-Type: text/html
```

→ Ligne de statut

→ Ligne vide = fin de l'en-tête HTTP

En-tête

```
<html>
<body>
<h1>It works!</h1>
</body>
</html>
```

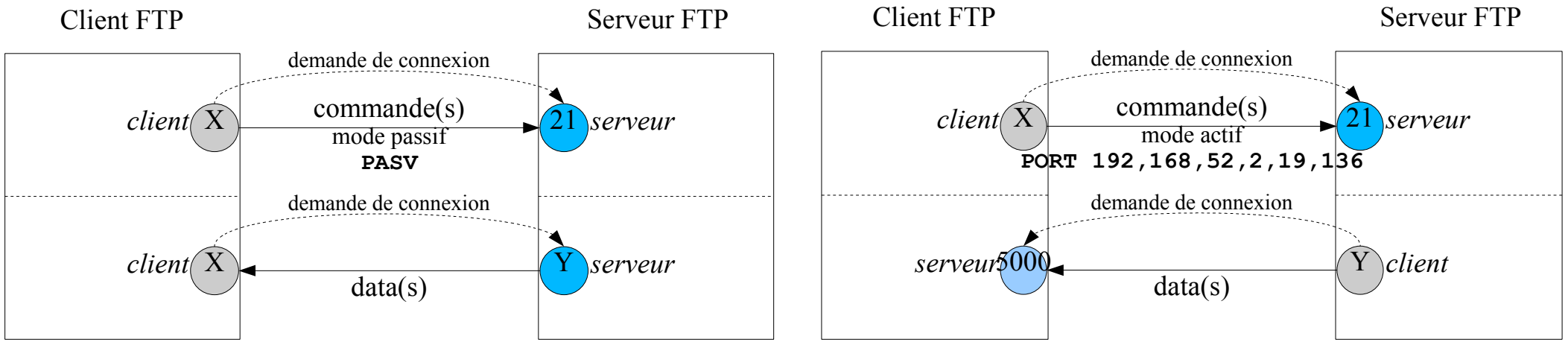
Le corps de la réponse contient le contenu du fichier index.html demandé dans la requête

Corps

Protocole FTP

- Le protocole FTP (*File Transfer Protocol*) est un protocole de transfert de fichier (R-FC959). Le protocole FTP s'utilise de façon standard sur le **port 21 du serveur en mode TCP**. Par contre le **FTP ne fonctionne que sur du TCP**. Il existe un protocole TFTP (*Trivial FTP*) qui est basé sur UDP.

- Lors d'une connexion FTP, deux canaux de transmission sont ouverts :
  - Un canal pour les commandes (canal de contrôle) : USER, PASS, LIST, RETR, STOR, ...
  - Un canal pour les données



Protocoles : historique

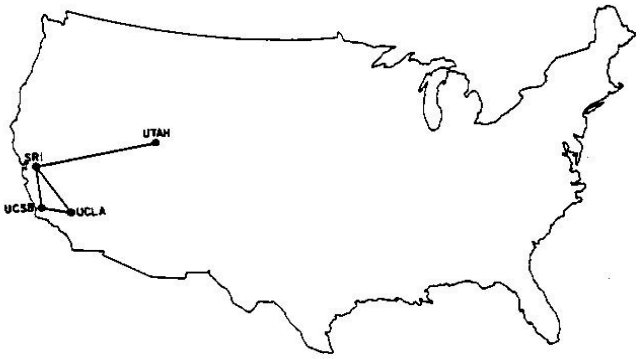
- 1970 : NCP (Network Control Program)
- 1971 : FTP (1980), Telnet (1983)
- 1972 : Courriel - email
- 1973 : Ethernet (1976)
- 1974 : TCP/IP
- 1979 : Usenet
- 1980 : IPv4, TCP, UDP, FTP
- 1981 : ICMP
- 1982 : SMTP
- 1983 : Telnet, DNS
- 1985 : NTP
- 1985 : BOOTP
- 1989 : WWW
- 1990 : HTTP
- 1988 : IRC
- 1993 : DHCP
- 1995 : SSH
- 1996 : HTTP 1.0, POP3, RTP, ICQ
- 1998 : IPv6, Jabber (XMPP)
- 1999 : MSN (Microsoft)
- 2002 : BitTorrent

Internet (I) : historique

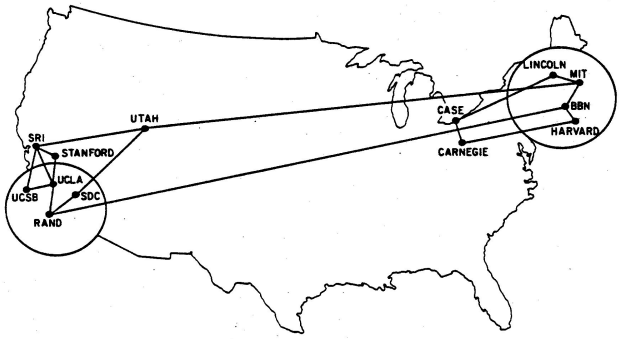
- 1958 : La BELL crée le premier Modem permettant de transmettre des données binaires sur une simple ligne téléphonique
- 1961 : Leonard Kleinrock du MIT publie une première théorie sur l'utilisation de la commutation de paquets pour transférer des données
- 1962 : Début de la recherche par ARPA, une agence du ministère de la Défense américain
- 1964 : Leonard Kleinrock du MIT publie un livre sur la communication par commutation de paquets pour réaliser un réseau
- 1969 : Connexion des premiers ordinateurs sur l'ARPANET
- 1979 : Création des NewsGroups (forums de discussion) par des étudiants américains
- 1982 : Définition du protocole TCP/IP et du mot « Internet »
- 1983 : Premier serveur de noms de sites (DNS)
- 1988 : Première connexion Internet en France
- 1991 : Annonce publique du *World Wide Web* qui est basé sur trois inventions, le protocole de communication client/serveur HTTP (*Hypertext Transfer Protocol*), les adresses web (URI/URL) et le langage HTML (*HyperText Markup Language*).
- 1994 : Premier moteur de recherche

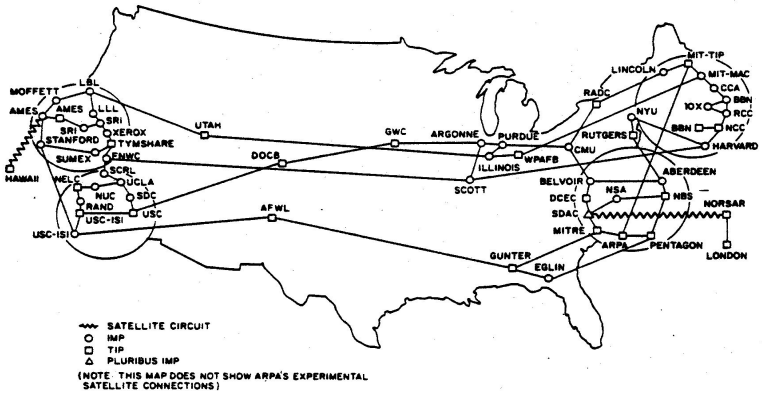
Internet (III) : évolution

- Depuis 2006, il y a plus d'un milliard d'ordinateurs connectés à Internet ...



Il y a seulement 4 noeuds à la création du réseau ARPAnet fin 1969.





Un an plus tard, fin 1970, il y a 13 noeuds d'interconnectés, le réseau maillé se construit ...

Il y aura plus de 100 000 noeuds à la fin des années 80

L'équipe de Christian HUITEMA à l'INRIA Sophia Antipolis réalise la première connexion Internet en France en juillet 1988.

Internet (IV) : réseau mondial

- Source : http://www.telegeography.com/ee/free_resources/