

Intro aux enjeux techniques du cyberspace

Chapitre 1 Brève histoire des Internets Aperçu du fonctionnement des Internets



Pablo Rauzy <pr@up8.edu>
pablo.rauzy.name/teaching/ietc

Brève histoire des Internets

- ▶ Depuis fin 19ème : les réseaux téléphoniques *commutés*.
En France, un développement étonnamment décentralisé.

Les prémices

- ▶ Depuis fin 19ème : les réseaux téléphoniques *commutés*.
En France, un développement étonnamment décentralisé.
- ▶ En 1969, lancement du projet ARPANET (4 noeuds).

- ▶ Depuis fin 19ème : les réseaux téléphoniques *commutés*.
En France, un développement étonnamment décentralisé.
- ▶ En 1969, lancement du projet ARPANET (4 noeuds).
- ▶ En 1971, le premier virus, Creeper, se diffuse sur ARPANET.

- ▶ Depuis fin 19ème : les réseaux téléphoniques *commutés*. En France, un développement étonnamment décentralisé.
- ▶ En 1969, lancement du projet ARPANET (4 noeuds).
- ▶ En 1971, le premier virus, Creeper, se diffuse sur ARPANET.
- ▶ En 1976*, Whitfield Diffie et Martin Hellman inventent la cryptographie asymétrique.



Whitfield Diffie

Les prémices

- ▶ Depuis fin 19ème : les réseaux téléphoniques *commutés*. En France, un développement étonnamment décentralisé.
- ▶ En 1969, lancement du projet ARPANET (4 noeuds).
- ▶ En 1971, le premier virus, Creeper, se diffuse sur ARPANET.
- ▶ En 1976*, Whitfield Diffie et Martin Hellman inventent la cryptographie asymétrique.



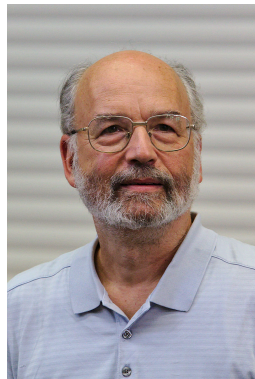
Martin Hellman

- ▶ Depuis fin 19ème : les réseaux téléphoniques *commutés*. En France, un développement étonnamment décentralisé.
- ▶ En 1969, lancement du projet ARPANET (4 noeuds).
- ▶ En 1971, le premier virus, Creeper, se diffuse sur ARPANET.
- ▶ En 1976*, Whitfield Diffie et Martin Hellman inventent la cryptographie asymétrique.
- ▶ En 1977*, Ronald Rivest, Adi Shamir, et Leonard Adleman présentent RSA et rendent la cryptographie asymétrique utilisable.



Ronald Rivest

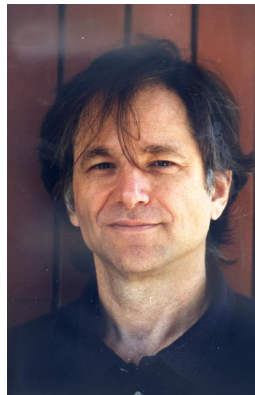
- ▶ Depuis fin 19ème : les réseaux téléphoniques *commutés*. En France, un développement étonnamment décentralisé.
- ▶ En 1969, lancement du projet ARPANET (4 noeuds).
- ▶ En 1971, le premier virus, Creeper, se diffuse sur ARPANET.
- ▶ En 1976*, Whitfield Diffie et Martin Hellman inventent la cryptographie asymétrique.
- ▶ En 1977*, Ronald Rivest, Adi Shamir, et Leonard Adleman présentent RSA et rendent la cryptographie asymétrique utilisable.



Adi Shamir

Les prémices

- ▶ Depuis fin 19ème : les réseaux téléphoniques *commutés*. En France, un développement étonnamment décentralisé.
- ▶ En 1969, lancement du projet ARPANET (4 noeuds).
- ▶ En 1971, le premier virus, Creeper, se diffuse sur ARPANET.
- ▶ En 1976*, Whitfield Diffie et Martin Hellman inventent la cryptographie asymétrique.
- ▶ En 1977*, Ronald Rivest, Adi Shamir, et Leonard Adleman présentent RSA et rendent la cryptographie asymétrique utilisable.



Leonard Adleman

L'apparition d'Internet

- ▶ Apparition des premiers ordinateurs personnels.

L'apparition d'Internet

- ▶ Apparition des premiers ordinateurs personnels.
- ▶ En 1984, Internet est né de la connexion TCP/IP entre ARPANET et NSFnet.

L'apparition d'Internet

- ▶ Apparition des premiers ordinateurs personnels.
- ▶ En 1984, Internet est né de la connexion TCP/IP entre ARPANET et NSFnet.
- ▶ En 1988, le premier vers, Morris worm, se diffuse largement sur Internet.



Robert Morris

L'apparition d'Internet

- ▶ Apparition des premiers ordinateurs personnels.
- ▶ En 1984, Internet est né de la connexion TCP/IP entre ARPANET et NSFnet.
- ▶ En 1988, le premier vers, Morris worm, se diffuse largement sur Internet.
- ▶ En 1989, les réseaux Internets nord américains et européens sont liés.

L'apparition d'Internet

- ▶ Apparition des premiers ordinateurs personnels.
- ▶ En 1984, Internet est né de la connexion TCP/IP entre ARPANET et NSFnet.
- ▶ En 1988, le premier vers, Morris worm, se diffuse largement sur Internet.
- ▶ En 1989, les réseaux Internets nord américains et européens sont liés.
- ▶ En 1989, Tim Berners-Lee développe au CERN le protocole HTTP et le World Wide Web.



Tim Berners-Lee

L'apparition d'Internet

- ▶ Apparition des premiers ordinateurs personnels.
- ▶ En 1984, Internet est né de la connexion TCP/IP entre ARPANET et NSFnet.
- ▶ En 1988, le premier vers, Morris worm, se diffuse largement sur Internet.
- ▶ En 1989, les réseaux Internets nord américains et européens sont liés.
- ▶ En 1989, Tim Berners-Lee développe au CERN le protocole HTTP et le World Wide Web.



Logo du WWW

années 1990

- ▶ En 1992, 1 millions d'ordinateurs sont reliés à Internet.

années 1990

- ▶ En 1992, 1 millions d'ordinateurs sont reliés à Internet.
- ▶ En 1993, le CERN autorise l'utilisation publique du WWW.

années 1990

- ▶ En 1992, 1 millions d'ordinateurs sont reliés à Internet.
- ▶ En 1993, le CERN autorise l'utilisation publique du WWW.
- ▶ En 1996, 10 millions d'ordinateurs sont reliés à Internet.

années 1990

- ▶ En 1992, 1 millions d'ordinateurs sont reliés à Internet.
- ▶ En 1993, le CERN autorise l'utilisation publique du WWW.
- ▶ En 1996, 10 millions d'ordinateurs sont reliés à Internet.
- ▶ En 1997, un programme informatique (Deep Blue) bat pour la première fois un grand maître d'échec (Garry Kasparov).



Deep Blue

années 1990

- ▶ En 1992, 1 millions d'ordinateurs sont reliés à Internet.
- ▶ En 1993, le CERN autorise l'utilisation publique du WWW.
- ▶ En 1996, 10 millions d'ordinateurs sont reliés à Internet.
- ▶ En 1997, un programme informatique (Deep Blue) bat pour la première fois un grand maître d'échec (Garry Kasparov).



Garry Kasparov

- ▶ En 2001, lancement de Wikipédia par Jimmy Wales.



Jimmy Wales

depuis 2000

- ▶ En 2001, lancement de Wikipédia par Jimmy Wales.



WIKIPÉDIA

L'encyclopédie libre

Wikipédia

depuis 2000

- ▶ En 2001, lancement de Wikipédia par Jimmy Wales.
- ▶ En 2004, sortie de la version 1.0 de Mozilla Firefox.



Firefox

- ▶ En 2001, lancement de Wikipédia par Jimmy Wales.
- ▶ En 2004, sortie de la version 1.0 de Mozilla Firefox.
- ▶ En 2013, le nombre d'utilisateurs connectés à Internet depuis un smartphone dépasse celui des utilisateurs connectés depuis un PC.

- ▶ En 2001, lancement de Wikipédia par Jimmy Wales.
- ▶ En 2004, sortie de la version 1.0 de Mozilla Firefox.
- ▶ En 2013, le nombre d'utilisateurs connectés à Internet depuis un smartphone dépasse celui des utilisateurs connectés depuis un PC.
- ▶ En 2014, le nombre de sites web dans le monde dépasse le milliard.

Aperçu du fonctionnement des Internets

- ▶ Internet est organisé hiérarchiquement :
 - au niveau de son infrastructure matérielle, et
 - au niveau des protocoles qui régissent le trafic sur le réseau.
- ▶ Pourtant, son fonctionnement reste très décentralisé.

- ▶ Chaque machine sur le réseau est identifiée par une *adresse IP*.
- ▶ Les données qui transitent sur le réseau sont découpées en *paquets*.
 - Chaque paquet a une IP *source* et une IP *destination*.
- ▶ La *route* de chaque paquet de machine en machine est indépendante.
 - Elle est décidée au fur et à mesure de manière complètement décentralisée.

- Sur un réseau local, il y a essentiellement deux types de machines :
- les machines hôtes, et
 - les routeurs.

Machine hôte

- ▶ Sur une machine *hôte*, le trafic est dirigé en fonction d'une *table de routage*.
- ▶ Cette table définit à qui envoyer un paquet en fonction de sa destination :
 - soit à elle même si elle est la destination,
 - soit l'adresser directement à la machine destination si elle est sur le réseau local.
 - soit l'envoyer à une adresse par défaut (le *routeur*).

Routeur

- ▶ Un *routeur* est simplement une machine connectée à plusieurs réseaux.
 - Elle dispose aussi d'une table de routage qui permet de faire passer les paquets d'un réseau à l'autre quand c'est nécessaire.
- ▶ Quand les deux réseaux sont de nature différente, on l'appelle *passerelle*.
 - Votre modem-routeur ("box") est typiquement une passerelle entre votre réseau local et Internet. En pratique, entre votre réseau local et votre fournisseur d'accès.

Systèmes autonomes (AS)

- ▶ Un *système autonome* est un ensemble de réseaux dont le routage interne est cohérent.
 - Exemple typique d'AS : un fournisseur d'accès à Internet (FAI).
- ▶ Un protocole de routage interne calcule tous les plus courts chemins dans l'AS.
- ▶ Les paquets qui ont une destination externe à l'AS sont :
 - soit envoyés à une passerelle en “bordure” de l'AS (*peering*),
 - soit remontés vers une route par défaut à un FAI de niveau supérieur (*transit*).

Appairage (peering)

- ▶ Un AS peut avoir des accords d'*appairage* avec d'autres AS :
 - Il peut s'agir d'un lien physique avec un autre AS (peering privé), ou
 - de la participation à un *point d'échange Internet* (peering public).
- ▶ Le protocole BGP permet d'échanger des informations de routage entre AS :
 - par exemple "je sais aller très rapidement à toutes mes destinations internes",
 - ou encore "j'ai un accord de peering me permettant d'aller à telle destination à telle vitesse",

Appairage (peering)

- ▶ Un AS peut avoir des accords d'*appairage* avec d'autres AS :
 - Il peut s'agir d'un lien physique avec un autre AS (peering privé), ou
 - de la participation à un *point d'échange Internet* (peering public).
- ▶ Le protocole BGP permet d'échanger des informations de routage entre AS :
 - par exemple "je sais aller très rapidement à toutes mes destinations internes",
 - ou encore "j'ai un accord de peering me permettant d'aller à telle destination à telle vitesse",
 - ou même "Je suis YouTube promis juré !"...
 - BGP est capable de s'auto-réparer en propageant les informations concernant les routes cassées, mais ça peut prendre du temps.

Points d'échanges Internet (IXP)

- ▶ Un *point d'échange Internet* relie plusieurs systèmes autonomes.
- ▶ Cela permet à ces AS de s'échanger du trafic directement, sans passer par un FAI :
 - optimisation du coût,
 - optimisation de la vitesse du trafic.

Trois niveaux d'opérateurs Internet

- ▶ Opérateurs *tier 3* : pas d'accord de peering, dépendent entièrement d'une offre de transit.
- ▶ Opérateurs *tier 2* : ont des accords de peering, nécessitent une offre de transit.
- ▶ Opérateurs *tier 1* : voient tout le réseau par peering, n'ont pas besoin de transit.
 - La *default-free zone* est l'ensemble des routeurs qui n'utilisent pas de route par défaut.

- ▶ Concernant le routage, la gouvernance d'Internet est assez décentralisée :
 - une table de routage à n'importe quel niveau peut être configurée manuellement ;
 - bien sûr, il reste un aspect hiérarchique fort dans la structure du réseau.
- ▶ En revanche, même si “code is law”, la gouvernance de certaines ressources est relativement centralisée.

- ▶ L'*Internet Corporation for Assigned Names and Numbers* est l'autorité suprême :
 - elle gère les racines du système des noms de domaines,
 - elle attribue les numéros d'AS et les adresses IP (déléguées depuis le début des années 90 aux *registres Internet régionaux*).
- ▶ L'ICANN n'est indépendante du gouvernement américain que depuis 2016...
 - Cela a évidemment fait l'objet de nombreuses controverses (privatisation au profit des GAFAM ?).
- ▶ La gouvernance de l'ICANN elle même est assez complexe, je vous laisse découvrir ça :
<https://www.icann.org/resources/pages/newcomers-2015-04-01-fr>