



# **Du fonctionnement d'Internet**

---

**Ronan Keryell**

`rk@enstb.org`

**Département Informatique, ENSTBr**

**24 janvier 2006**

**F2B402A Ingénierie des réseaux**

**Version 1.5**

- Copyright (c) 1986–2037 by Ronan.Keryell@enstb.org.  
This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, v1.0 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).
- Si vous améliorez ces cours, merci de m'envoyer vos modifications ! ☺
- Transparents 100 % à base de logiciels libres (LaTeX,...)



- Révolution : télégraphe, téléphone, télévision,... Internet
- Internet : LE réseau DES réseaux, ébauche des autoroutes de l'information
- $10^7$  (1997) utilisateurs  $\nearrow \rightsquigarrow 10^9$  (2006)
- Outil de travail utile
- Importance stratégique  $\nearrow$
- Opportunités de télétravail, dématérialisation...
- Fonctionnement peu connu chez les utilisateurs
- ...ni les professionnels du domaine !
- Constatation que les élèves connaissaient bien les trames Ethernet et Corba ou SOAP mais pas trop entre les 2 ☺  $\rightsquigarrow$  ressorti cours de 1997 aux Mines



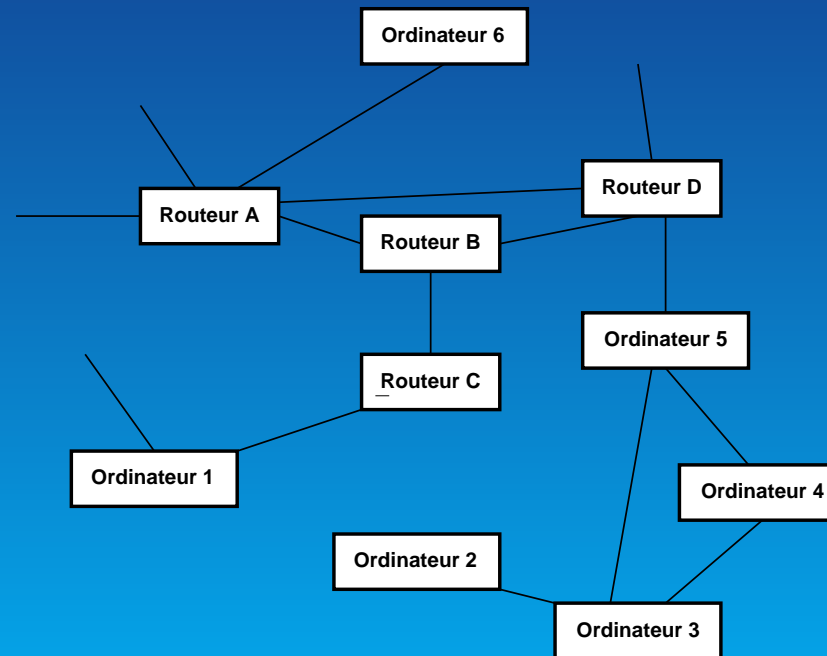
- Utile pour utilisation correcte et résoudre les problèmes



- Histoire et réseaux
- Protocoles & services
- Futur



- Interconnexion de machines (ordinateurs)
- Graphe : nœuds (ordinateurs, routeurs) et arcs (liaisons transportant de l'information)



- Faire communiquer les machines entre elles
- Local (LAN) : Ethernet (10 Mbit/s–10 Gbit/s, ATM)



155+Mbit/s)

- Distant (WAN) : liaisons spécialisées (64 Kbit/s–10 Gbit/s), satellite, ATM (155 Mbit/s, 622 Mbit/s, 2,5 Gbit/s...)
- Multiplexage en longueur d'onde sur fibre optique (DWDM) : ↗ ↗ débit





- 1957** : Création de l'*Advanced Research Project Agency* par le DoD américain (guerre froide...)
- 1961** : Article de KLEINROCK vantant la commutation de paquets  $\neq$  téléphone
- 1962** : Étude pour l'US Air Force d'un réseau très décentralisé et maillé : pas de point central  $\rightsquigarrow$  résiste à une destruction partielle
- 1968** : Réseau à commutation de paquets au *National Physical Laboratories*, UK
- 1969** : Premier échange sur ARPANET entre ordinateur à UCLA and SRI. Création de la documentation, *Request For Comments* (RFC)
- 1970** : Définition du *Network Control Protocol*



**1972** : Création de *InterNetwork Working Group* pour concevoir des protocoles de communication communs avec tolérance aux pannes et aux pertes. Définition d'une architecture : réseaux autonomes interconnectés par des passerelles. ARPANET. *E-mail*

**1972** Projet Cyclades au CNET de réseau à commutation de paquets avec Louis POUZIN

**1972–1974** : protocoles *telnet*, FTP, TCP

**1976** : protocole UUCP pour échanger des données entre machines UNIX

**1977** : Format des messages électroniques. Création de *TheoryNet* basé sur UUCP



- 1979** : ARPA crée *Internet Configuration Control Board* pour gérer l'évolution. Usenet (échange des *News*) basé sur UUCP. Création de CompuServe (messagerie, fora, échanges de fichiers)
- 1980** : Protocole IP mis dans le domaine public → interconnexion TheoryNet avec ARPANET. Téletel en France avec des terminaux vidéotex
- 1981** : Création de *Because It's Time NETwork* (BITNET), 4000 listes de discussions (*listserv*). Culture plus conservatrice que sur Usenet
- 1983** : Changement NCP → IP sur ARPANET
- 1986** : Optimisation d'Usenet avec NNTP. Création des groupes *alt.* pour échapper à la censure. Création de



FidoNet regroupant des serveurs de BBS (messagerie, échange de fichiers)

**1987** : Intelmatique pour utilisation du Minitel via Internet

**1989** : *World-Wide-Web* développé au CERN pour accéder à des informations hypertextuelles délocalisées



Internet n'appartient à personne mais...

**Internet Society (ISOC)** : organisation destinée à promouvoir l'interconnexion ouverte des systèmes et Internet. *Board of Trustees* élus par les membres de l'ISOC dirige plusieurs comités

**Internet Architecture Board (IAB)** : évolution des protocoles de communication

**Internet Assigned Number Authority (IANA)** : gère tous les numéros et codes qui doivent être uniques dans Internet. Délègue à InterNIC/RIPE/NIC France l'allocation des adresses IP

**Internet Engineering Task Force (IETF)** : fédère groupes développant les nouvelles technologies. Dirigé



par l'Internet Engineering Steering Group (IESG)

**Internet Research Task Force (IRTF)** : fédère groupes de recherche à long terme. Dirigé par l'Internet Research Steering Group (IRSG)

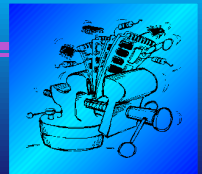
Système de développement des standards plus souple et plus rapide qu'ISO & ITU

- Standards disponibles gratuitement sur Internet : Requests For Comments (RFC)
- Spécifications ISO : payantes...
- UNIX arrivait avec IP gratuitement...

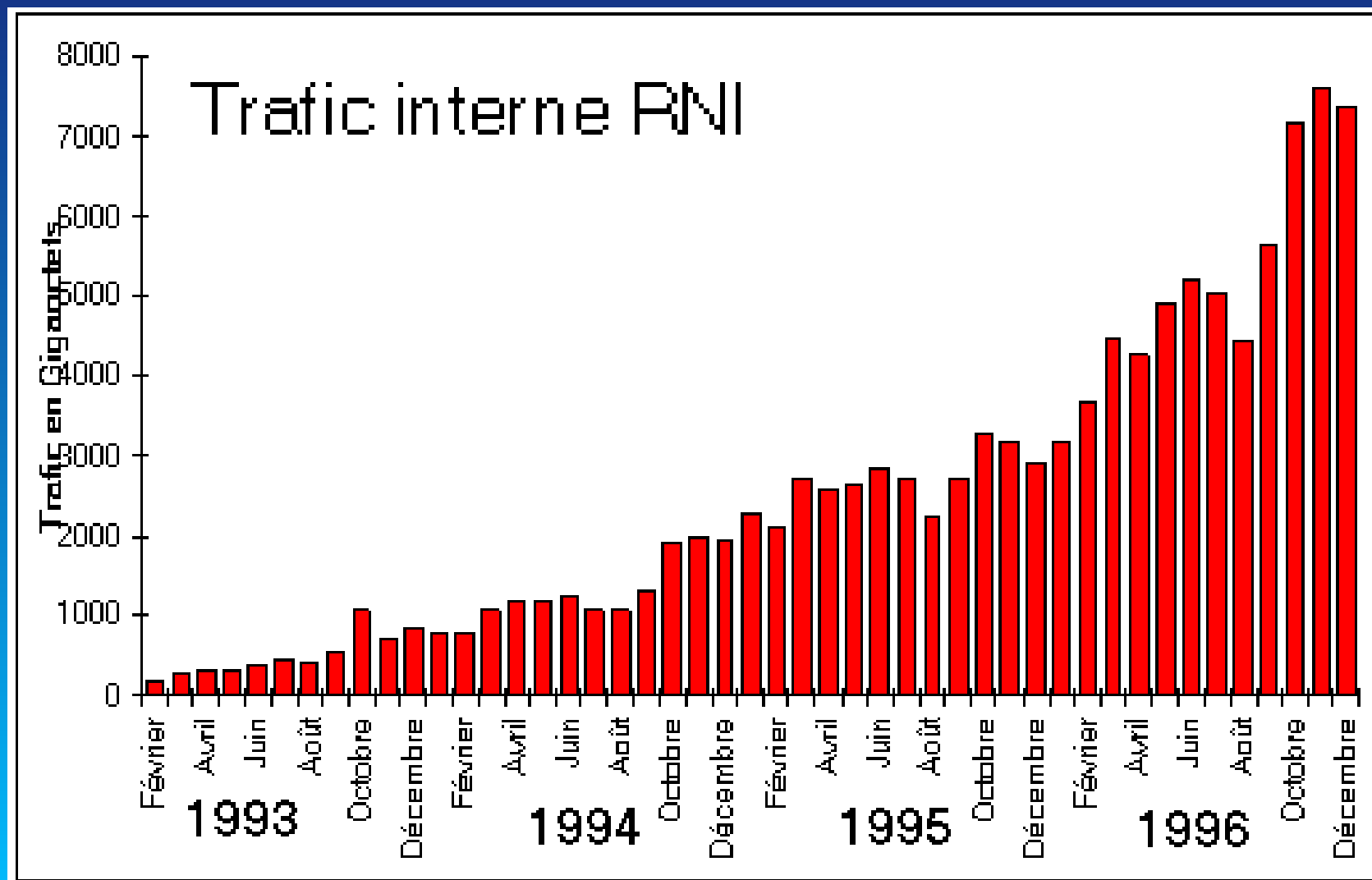


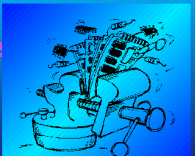
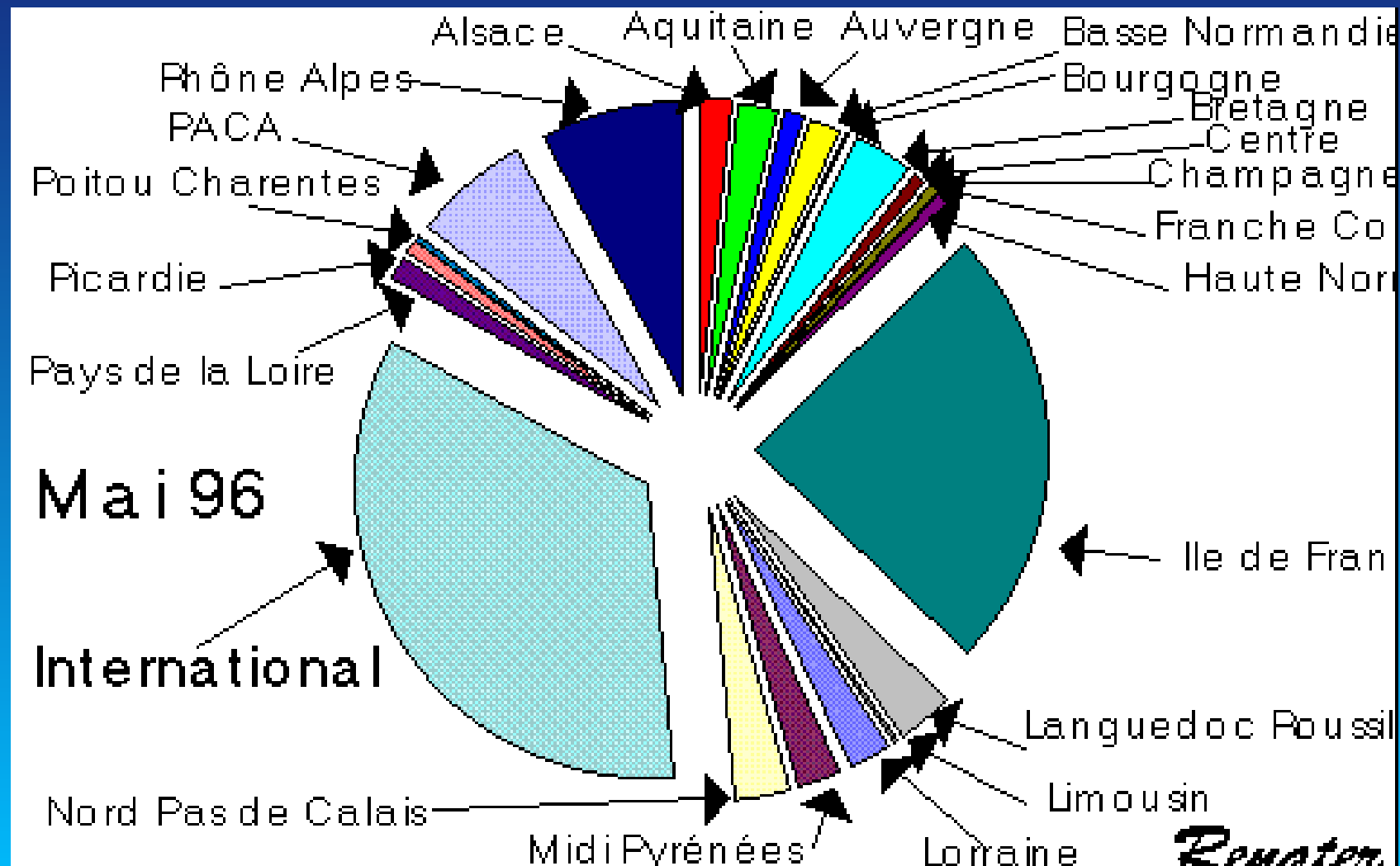
RÉseau NATional de l'Enseignement et de la Recherche  
[http ://www.renater.fr](http://www.renater.fr)



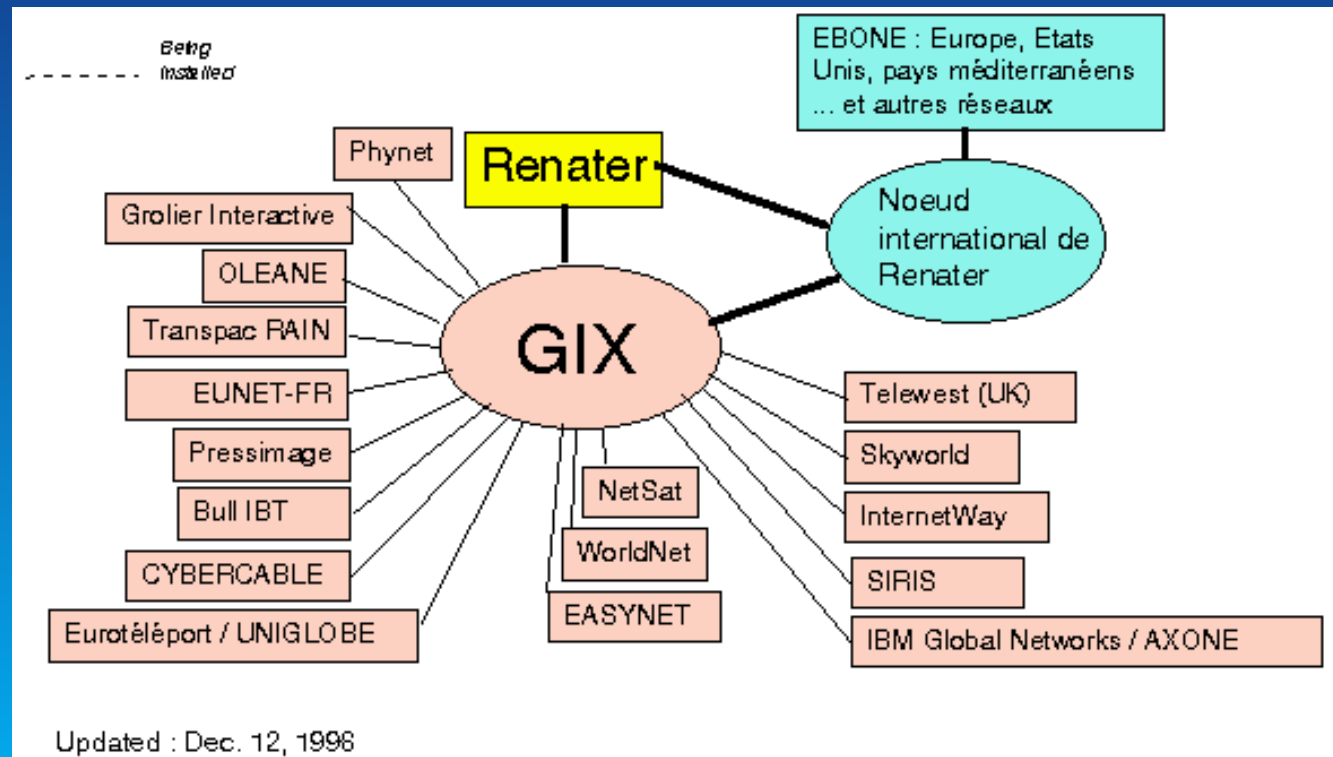




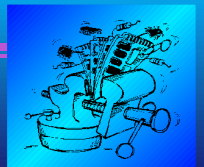




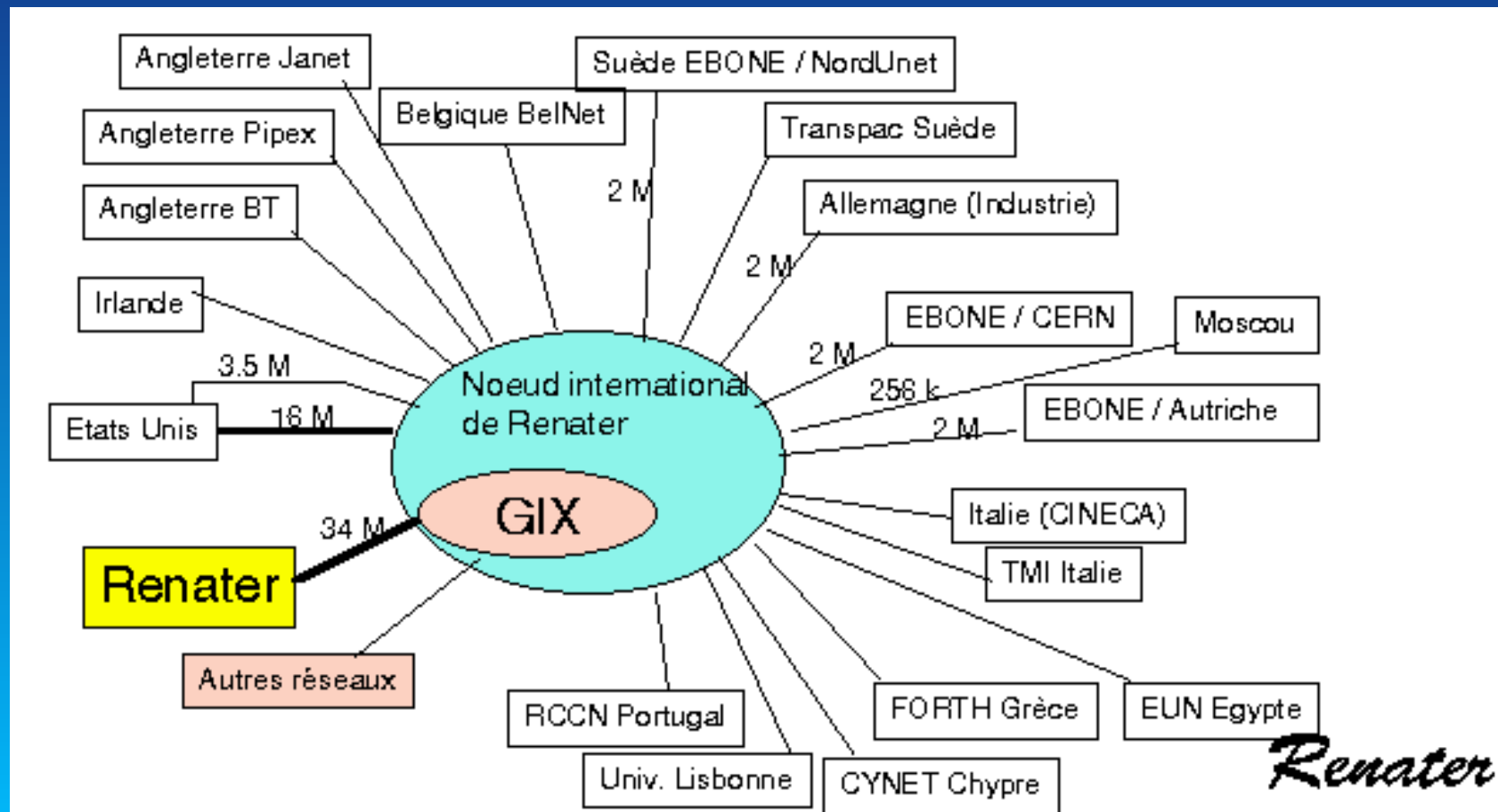
RENATER  $\neq$  Internet en France  $\rightsquigarrow$  politique de communication entre les réseaux français

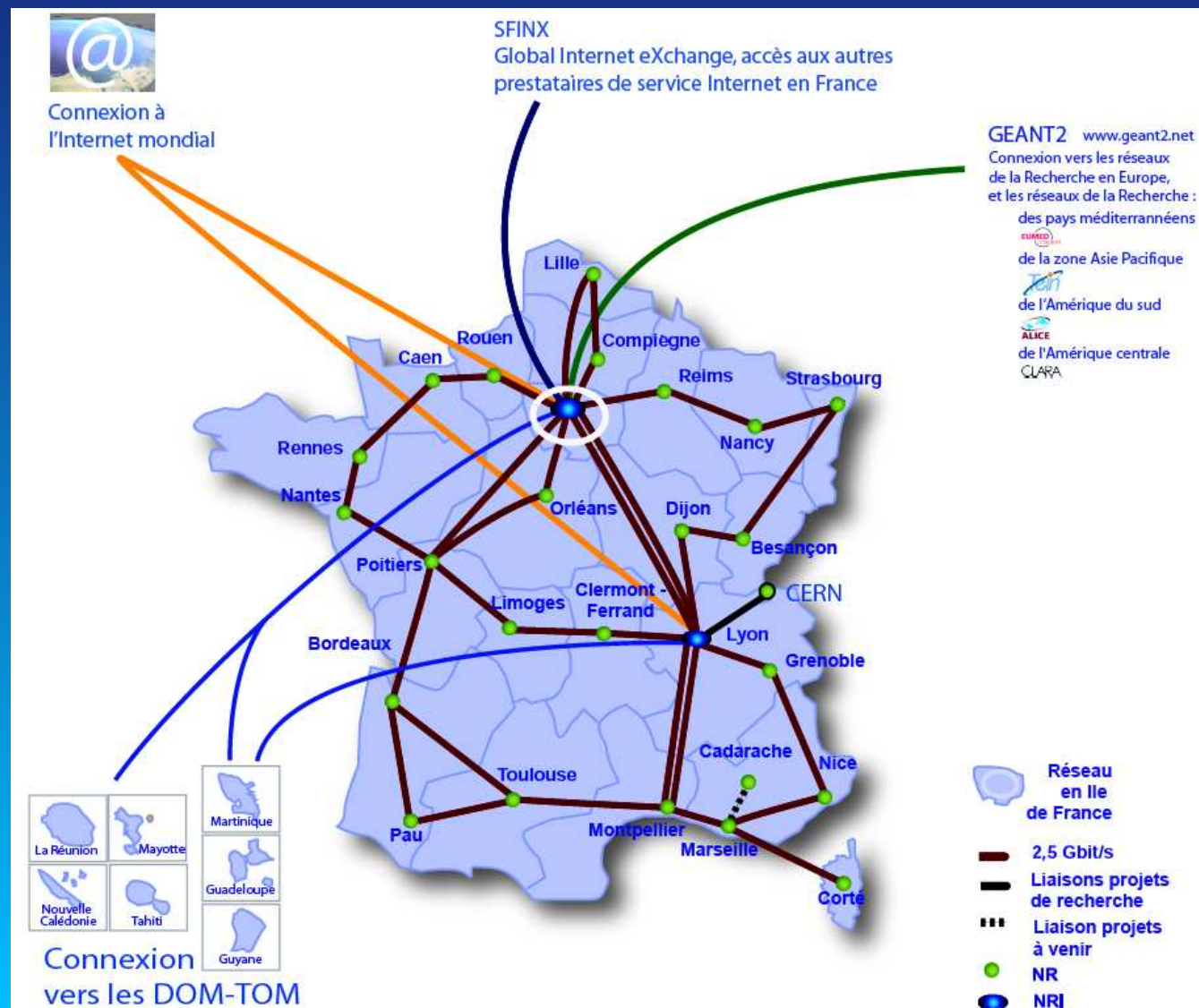


SFINX : service payant d'interconnexion (85kF/an connexion Ethernet + LS)



[http ://www.renater.fr/international/interaccueil.html](http://www.renater.fr/international/interaccueil.html)





- *Sockets* UNIX : tuyau ( $\approx$  *file descriptor*) sur lequel on peut envoyer et recevoir une suite d'octets
- `socket()` crée un tuyau. IP si domaine `PF_INET`. Type `SOCK_STREAM`, `SOCK_DGRAM`, `SOCK_RAW`,...
- `connect()` connecte une socket à une autre machine (appel)
- `bind()` associe une adresse à une socket (pour permettre à quelqu'un d'autre de la nommer)
- `listen()` déclare une socket comme attendant des connexions
- `accept()` traite une connexion en attente
- `getpeername()` donne l'adresse du connecté à l'autre bout



- `read()`, `write()`, `send()`, `recv()`,...



- Internet Protocol
- Niveaux 3 (réseau) dans le monde OSI (ultérieur)
- Assure le routage de datagrammes (petits paquets de données)
- Contient adresse de source (envoyeur) et de destination
- Type de protocole
- Longueur
- Gestion de la fragmentation des paquets en morceaux
- Durée de vie
- Somme de vérification
- Pas de garantie de l'ordre d'arrivée, du chemin, ni de... l'arrivée !





- Rangement des octets : grand indien



Numéros de machines sur 32 bits séparés en classes, les « réseaux », de différente importance

Classe A	0	Réseau (7 bits)		Machine (24 bits)		
Classe B	1	0	Réseau (14 bits)		Machine (16 bits)	
Classe C	1	1	0	Réseau (21 bits)		Machine (8 bits)
Classe D	1	1	1	0	Multicast (28 bits)	

Classe E 11111 pour extensions futures

Surcharge du réseau →

- ▶ Apparition du CIDR (*Classless Inter-Domain Routing*)
- ▶ Notion de numéros locaux (privés) style 10.x.y.z
- ▶ Fontainebleau : 2 classes C sur le même support physique  
192.54.148 & 192.54.172



- Niveau OSI 4 : transport
- Transmission de datagrammes
- Pas de connexion
- IP + port d'émission & port de réception pour avoir plusieurs services + somme de vérification : protocole 17
- Pas de gestion d'erreur...
- Certains numéros de port sont standardisés par IANA pour des services précis
- Pour des raisons de sécurité l'ouverture des ports  $< 1024$  nécessitent d'être `root`



- Niveau OSI 4 : transport
- Transmission + robuste de données (retransmission si nécessaire)
- Notion de connexion
- UDP + numéro de séquence + accusé de réception + taille de fenêtre + urgence... : protocole 6
- Numéro de séquence pour remettre les octets dans l'ordre (sécurité : numéro de séquence initial choisi au hasard à la connexion)
- Fenêtre d'accusé de réception pour pipeliner le temps de transfert (autorise l'émetteur à prendre de l'avance)
- Protocole d'établissement, de resynchronisation et de fin de connexion



- Utilisation des ports semblable à UDP (/etc/services)



Notions de service :


- Fonctionnement asymétrique
- Demande une page WWW
- Demander un affichage à l'écran
- Recherche dans une base de donnée
- Se connecter à distance
- Écrire sur un serveur disque NFS



- Besoin humain d'un annuaire nom de machine  $\leftrightarrow$  numéro IP
- Trop de machines  $\rightsquigarrow$  hiérarchisation des noms et délégation :
  - ▶ Serveur racine (.)
  - ▶ Serveurs pour zones .fr, .edu, .com, .org, .gov, .net,... Problème : des millions d'entrées dans .com!
  - ▶ Délégation : envoyer vers un autre serveur qui sert une zone
  - ▶ Serveurs pour .enst-bretagne.fr, .ensmp.fr, .univ-rennes1.fr, .gouv.fr, .asso.fr,...
- Traduction de numéros vers noms : faux domaine hiérarchique sur les numéros inversés in-addr.arpa :



200.172.54.192.in-addr.arpa      name = chailly.ensmp.fr

-  Décorrélation entre hiérarchie des noms et des numéros
- Échange d'information sur le port `domain` (53, TCP ou UDP)
- Serveur primaire secondé par des serveurs secondaires
- Système de cache : garder dans un coin les informations récentes
- Système de cache de non-existence aussi (cache négatif) : répondre à des erreurs de configuration
- Géré en UNIX souvent par `named` (BIND)





- Informations SOA (description de la zone), NS (serveur de nom pour délégation), A (adresse), PTR (nom), CNAME (donne un alias), MX (échangeur de mail),...
- Problèmes de saturation et de marques déposées...
- Déclaration des noms auprès des responsables : NIC France pour .fr

dig pour demander des informations :

```
dig enstb.org any
```

```
enstb.org.      3600    IN      MX      1 minou.info.enstb.org.
enstb.org.      3600    IN      A        193.50.97.146
enstb.org.      3600    IN      AAAA     2001:660:7302:e771:201:2ff:fefa:64ee
enstb.org.      3600    IN      A6       0 2001:660:7302:e771:201:2ff:fefa:64ee
enstb.org.      3600    IN      SOA      dns2.enstb.org. keryell.cri.ensmp.fr. 2006011300 7200 3600 6048
enstb.org.      3600    IN      NS       dns-cri.ensmp.fr.
enstb.org.      3600    IN      NS       rsm.rennes.enst-bretagne.fr.
enstb.org.      3600    IN      NS       dns2.enstb.org.
enstb.org.      3600    IN      NS       dns3.enstb.org.
```



```
;; ADDITIONAL SECTION:
minou.info.enstb.org. 3600 IN A 193.50.97.146
minou.info.enstb.org. 3600 IN AAAA 2001:660:7302:e771:201:2ff:fefa:64ee
rsm.rennes.enst-bretagne.fr. 3475 IN A 192.44.77.1
dns2.enstb.org. 3600 IN A 193.50.97.146
dns2.enstb.org. 3600 IN AAAA 2001:660:7302:e771:201:2ff:fefa:64ee
dns3.enstb.org. 3600 IN A 193.50.97.139
dns-cri.ensmp.fr. 102673 IN A 193.48.171.215
```

- Service extrêmement sensible
  - ▶ Si comportement faux : détournements de services ☹
  - ▶ Cible d'attaques, de dénis de service
- 🌐 DNSSEC sécurisé avec cryptographie à clé publique




- Le succès d'Internet  $\rightsquigarrow$  confusion... ☹
- TCP port 80
- « Document » référencé par *Universal Resource Locator* (URL)  
`proto://nom@machine:port/CheminFichier#fragment`
- HTTP gère le transport (GET demande une page, HEAD méta-information, POST envoie une requête, PUT envoie une page ,...)
- HTML décrit la structure des documents. Langage de marquage ( $\approx$   $\text{\LaTeX}$ ) avec des balises SGML/XML
- Possibilité de lancer d'autres applications (*plug-in*) via MIME




- ECMAScript/JavaScript rajoute de la programmation côté navigateur (AJAX avec du XML RPC)
- Langage JAVA permettant de télécharger et d'exécuter des applications



- Accéder à des machines puissantes (supercalculateurs...)
- Émulation de terminal
- Protocoles de connexion indépendant du système
- Pas de graphisme
- `telnet` TCP port 23, Émulation VT-100 et IBM 3270
  - ▶ Mot de passe en clair sur le réseau... 
  - ▶ `telnet` accepte un numéro de port : utile pour tester d'autres ports TCP/IP
    - Debug de serveur de mail
- ▶ ∃ Version sécurisée avec Kerberos et TLS

```
telnet enstb.org 25
```





- `rlogin` TCP port 513
  - ▶ Terminal plus complet (passe la taille du terminal local)
  - ▶  Mot de passe en clair aussi mais `.rhosts` & `/etc/hosts.equiv` préférable...
  - ▶  $\exists$  Version sécurisée avec Kerberos et TLS
- `ssh`
  - ▶ Utilisation cryptographie forte
  - ▶ Chiffrement des communications et authentifications
  - ▶ Authentification par mot de passe ou clé publique
  - ▶ Agent d'authentification pour éviter de retaper sans arrêt des mots de passe



- ▶ Téléportation de ports TCP : tunnels dans Intranet...
- ▶ Permet aussi de recopier des fichiers à distance ou lancer des commandes à distance
- ▶ ~~~> Solution moderne conseillée




- Lancer des commandes à distance
- Autorisation avec `.rhosts` & `/etc/hosts.equiv`
- `rsh nom@machine TCP port 514`
- `on TCP port 512`. Passe l'environnement et le répertoire courant. Problèmes de sécurité connus... 
-  Utiliser encore `ssh` !






## *File Transfer Protocol (FTP)*

- Ancêtre des protocoles  $\rightsquigarrow$  concepts repris souvent par d'autres protocoles
  - ▶ Commandes courtes + arguments textuels
  - ▶ Réponse à 3 chiffres + commentaires textuels pour humains
- FTP `anonymous` pour transférer des fichiers dans `~ftp` sans avoir besoin de compte
- FTP `guest` idem mais avec mot de passe
- $\exists$  Versions sécurisées, mais pourquoi pas `ssh` plutôt ?
- Trivial FTP `tftp` : simplifié, pas de mot de passe. Utilisé pour initialiser des machines et terminaux X sur le réseau.
-  à bien restreindre l'accessibilité des fichiers avec `-s`



- Échange asynchrone de messages entre plusieurs utilisateurs
- Simple Mail Transfer Protocol, proche de FTP
- `nom@machine`, `nom%machine3%machine2@machine` (test)
-  Spam (pourriel)...
- Entêtes standard : From:, To:, Subject:,...
- Démon `sendmail` TCP port 25
- Algorithme : envoyer à l'échangeur de mail de la destination sauf si c'est soi-même (distribué en local).  
Plein de paramétrages...
- Déclaration des échangeurs de mail : MX dans le DNS



- Problèmes d'authentification (faux mails faciles à faire).  
Regarder de près les entêtes...
- Confidentialité faible si pas de chiffrement (root...)
- Métaprotocole : les *smileys* :- ) ☺

Accès par des machines qui n'ont pas de démon SMTP

- ▶ Démons POP3 (TCP port 110) & IMAP4 (plus récent) qui tournent sur le serveur
- ▶ Possibilité de télécharger des messages sur un poste, gérer des dossiers...



- Protocole qui décrit le codage et le type de document

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 8bit

Content-Length: 104411

- Son, images, texte enrichi
- Gestion de plusieurs parties
- Problème si le récepteur ne comprend pas MIME  
=?ISO-8859-1?Q?Re:\_e-038\_-\_...
- Utilisé pour le mail, les news, WWW,...



- Diffusion de messages sur toute la planète, classés par *newsgroup*
- Network News Transfer Protocol, TCP port 119
- Démons qui parlent entre eux
- Path: contient la liste des machines traversées et est utilisé pour empêcher de repasser par une machine
- Mode serveur interrogé par les interfaces utilisateurs des news
- Souvent `inn` sous UNIX




- Exécuter des procédures à distance (mode client/serveur)
- `rpcbind/portmap` UDP/TCP port 111 transforme un service en un port temporaire vers le serveur.  $\approx$  annuaire
- `rpcinfo -p` donne la liste des services disponibles
- Services : NFS, `bootparam`, `rstatd`, `walld`, `sprayd`,...



- Network File System 2, 3 & 4
- Utilisation transparente d'un fichier résidant sur le disque d'une autre machine
- Utilise les RPC
- mountd sert les demandes de montage
- nfsd sert les transferts de données
- Dans NFS 2 écritures synchrones seulement.  
Performances ↘
- Version 4 : modèle plus asynchrone, sécurité plus fine des sessions


Autres systèmes : DCE DFS, CIFS (Samba met protocole MicroSoft dans UNIX), Coda, AFS,...



- Affichage à distance
- Extensions graphiques génériques
- Contrôle la souris, le clavier, le fond d'écran, etc.
- TCP port  $6000 + d$
- Protocole LBX comprimant les ordres graphiques si limité en bande passante
- Authentification
  - ▶ Par machine via `xhost`
    -  Toutes les personnes d'une machine peuvent se connecter !
  - ▶ Par fichier de secret (MIT-MAGIC-COOKIE)





- Connexion autorisée si le client et le serveur arrivent à lire le même fichier
- Protégé en lecture des regards indiscrets 




- Nécessaire de synchroniser les machines (NFS, makefile, corrélation d'événements (logs)...)
- rdate resynchronise sur un serveur. Problème du temps de propagation...
- Network Time Protocol : resynchronise sur un serveur en corrigeant avec des statistiques sur le temps de réponse

```
chailly-keryell > ntpq -p
```

remote	refid	st	t	when	poll	reach	delay	offset	disp
=====									
+resone.univ-ren	.PPS.	1	u	80	1024	377	32.94	9.737	4.32
+canon.inria.fr	.TDF.	1	u	25	1024	377	23.82	9.917	26.87
*yseult.sis.past	.TDF.	1	u	868	1024	377	481.43	59.655	52.12



- De plus en plus de systèmes sur Internet ~> contrôle à distance
- Définition d'un protocole de commande standard : Simple Network Management Protocol
- Contrôle de routeurs, imprimantes, ordinateurs,...  

```
chailly-keryell > hpnpadmin -v strasbourg  
strasbourg is a network peripheral  
ready to print  
chailly is allowed access to strasbourg  
Frontpanel message : 00 PRET
```
-  Protéger les accès...



- Connexion entre ordinateurs par liaisons séries ou ADSL (PPPoE, PPTP)
- Coder IP pour le faire passer
- Point to Point Protocol (PPP)
- Multiprotocoles (IP cas particulier)
- Compression des entêtes et du contenu
- Typiquement accès à la maison
- Possibilité de lancer PPP dans une fenêtre de login...
- Authentification par PAP (envoi d'un mot de passe) ou CHAP (échange de preuves de secret)
- Utilisation aussi pour tunnels



**Identification Protocol** : identification de l'utilisateur au bout d'une socket. Information à titre informatif sur utilisateur de WWW

**talk** : Discussion à 2



- Interdit à l'exportation aux USA au départ
- Usage cryptographie forte interdit en France pendant longtemps (arme de guerre)
- PGP *Pretty Good Privacy*/GnuPG : chiffrement à clé publique
  - ▶ Exploite relation chiffrement par une clé TRÈS secrète et déchiffrement par une clé publique ou réciproque
  - ▶ Signature : chiffrement par clé privée & tout destinataire peut déchiffrer en utilisant la clé publique de l'envoyeur
  - ▶ Chiffrement : chiffrement par clé publique du destinataire & décodage par la clé secrète du destinataire



- ▶ Combinaison des 2
- ▶ Combinaison avec algorithmes symétriques pour aller plus vite
  - Chiffre avec algorithme symétrique rapide
  - Joint la clé de session chiffrée avec algorithme à clé publique



- Niveau liaison
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- Paquet Ethernet avec source et destination (adresses Ethernet)
- Encapsulation d'un paquet IP dans un paquet Ethernet (`tcpdump -e`)
- Nécessité de traduire les adresses IP en adresse Ethernet avant de pouvoir envoyer un paquet IP : ARP





- Address Resolution Protocol
- Traduit une adresse IP en adresse Ethernet
- Envoie un message de diffusion demandant la traduction
- Quelqu'un (en principe la machine destination) répond la traduction
- tcpdump arp :  
05:26:44.046284 arp who-has node07 tell node06  
05:28:07.252011 arp who-has akanthos tell cmm02




- Machines sans disque : pas de quoi stocker leur numéro IP lors du démarrage...
- Nécessiter de le retrouver à partir du numéro Ethernet (qui est unique, assigné par le constructeur)
- Reverse Address Resolution Protocol
- `rarpd` sur un serveur avec `/etc/ethers`
- Lorsque la machine a son adresse IP, envoie d'une demande de chargeur de noyau pour son adresse IP a tous les serveurs TFTP
- `tcpdump rarp`  
`05:34:38.479046 rarp who-is 0:0:c9:10:c3:ef tell 0:0:c9:10:c3:ef`
- Plutôt remplacé par DHCP plus complet



- *Dynamic Host Configuration Protocol* étend protocole BOOTP plus ancien sur même protocole vers UDP 67 (requêtes) et 68 (réponses)
- Permet d'attribuer automatiquement paramètres réseau pour simplifier administration/configuration
  - ▶ Statique
  - ▶ Dynamique (visiteurs, réseaux WiFi publics...)
- Paramètres
  - ▶ Netmask
  - ▶ Adresse
  - ▶ Routeur
  - ▶ Serveurs DNS



- ▶ Nom de domaine et liste de domaines à essayer
- ▶ Serveurs d'impression
- ▶ Serveurs de journaux de fonctionnement (*log*)
- ▶ Serveur de boot et fichier d'image, fichier de swap
- ▶ ...
-  Pas (encore) sécurisé → difficile de faire une installation système automatisée et sécurisée...



- Protocoles utilisés pour mettre en place un réseau local privé
  - ▶ En IPv4 beaucoup moins d'adresses privées que de MAC  $\rightsquigarrow$  besoin d'allouer des adresses IPv4 aux dispositifs ☹
  - ▶ Sans infrastructure particulière (serveur DHCP...)
  - ▶ Ressources limitées (téléviseur, réveil, cafetière...)
  - ▶ En IPv6, contraire  $\rightsquigarrow$  possible de générer adresse privée unique à partir adresse MAC  $\rightsquigarrow$  pas de problème ☺
- RFC 3927



- Comment faire transiter des paquets d'un bout à l'autre de la planète ?
- Utiliser des routes de destination : « pour aller là-bas, passer par là »...

- Comment trouver les routes ?

► Déclarées statiquement :

```
roazhon-keryell > netstat -r  
Routing tables
```

Destination	Gateway	Flags	Refcnt	Use	Interf
localhost	localhost	UH	3	488704	lo0
ecuelles	roazhon	UH	3	17090	ppp0
default	routeur-172	UG	2	37036	le0
ensmp-private	roazhon	U	0	0	le0
ensmp-fbleau2	roazhon	U	106	7848007	le0

► Utiliser un protocole de routage qui va les calculer



- Internet Control Message Protocol, IP protocole 1
- Écho (base de ping)
- Messages d'erreur : destination non atteignable
- Suspension de la transmission
- Message de redirection : rajoute une route vers la machine destination
- Distribution de route



- Durée de vie excédée : base de traceroute (envoi de paquets avec des TTL croissants à partir de 0)

```
roazhon-keryell > traceroute cactus.insead.fr
```

```
traceroute to cactus.insead.fr (193.105.56.2), 30 hops max, 40 byte packets
```

```
1  chailly-qe0 (192.54.172.201)  1 ms  1 ms  1 ms
2  routeur-148 (192.54.148.101)  4 ms  4 ms  5 ms
3  194.214.157.1 (194.214.157.1)  6 ms  4 ms  4 ms
4  evry.rerif.ft.net (193.48.56.9)  15 ms  20 ms  18 ms
5  insead-fontainebleau.rerif.ft.net (193.48.56.50)  39 ms  39 ms  73 ms
6  194.57.233.1 (194.57.233.1)  41 ms  39 ms  41 ms
7  insead.fr (193.105.56.2)  40 ms  53 ms  40 ms
```





- Simplification du routage sur les machines  $\lambda$
- Si on ne sait pas : on envoie à la route par défaut, censée tomber sur un routeur intelligent...
- Définition des machines (non) locales par un netmask
- Adresse  $a$  locale si  $a \wedge \text{netmask} = \lambda \wedge \text{netmask}$
- Dans notre cas, si numéro commence par 192.54.172

```
roazhon-keryell > ifconfig -a
```

```
le0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING>
```

```
inet 192.54.172.226 netmask fffffff0 broadcast 192.54.172.0
```



Nécessité d'envoyer des messages à tout le monde (questions, charge, routage,...)  $\rightsquigarrow$  utilisation d'adresses spéciales :

**255.255.255.255** : diffusion limitée, ne passe pas les routeurs

**réseau.255** : envoie à toutes les machines du réseau

**réseau.x.255** : à tout un sous réseau contrôlé par netmask (ici 255.255.255.0)

**réseau.255.255** : tous les sous-réseaux contrôlés par netmask (ici 255.255.255.0)



- Internet : plusieurs réseaux, plusieurs entités avec des politiques de routages (Autonomous System, AS)
- Au sein d'une même entité (École des Mines)
- Par exemple Routing Information Protocol (RIP), RFC 1058, démon routed, gated, xorp, quagga...
- Messages de diffusion des routes disponibles par chaque routeur avec métrique
- Construction d'une table de destination à partir des messages reçus des autres routeurs
- Choix de la route de destination avec plus petite métrique



- Connexion de plusieurs AS entre eux
- Rôle de médiateur
- Exemple du Border Gateway Protocol (BGP 4) RFC 1467, gated
- Échange information sur la connectivité avec les autres systèmes BGP avec les chemins d'AS à traverser pour atteindre ces réseaux
- Construction d'une carte de connexion
- Politique : notion d'AS qui ne fait que du transfert local, connecté à d'autres AS mais avec transit interdit ou transit autorisé ~→ définition des connectivités entre fournisseurs, pays, etc...



- Recalcule l'état en fonction des routeurs en panne
- Classless Inter-Domain Routing permet de diminuer le nombre de routes : agrégation



- Besoin de diffuser de l'information au lieu d'envoyer  $n$  copies  $\rightsquigarrow$  meilleure utilisation de la bande passante
- Pas prévu dans IP de base, ni dans les routeurs
- $\approx$  extensions des News (application) vers niveau paquet IP (transport)
- $\rightsquigarrow$  Multidifusion au dessus d'Internet entre `mroute`s
- Encapsulation dans du protocole standard (IP dans IP, RFC)
- 1988 entre BBN & Stanford, « répandu » à partir de 1992
- Pas encore accessible au grand public ☹
- Choix d'une topologie efficace pour éviter de saturer des liens physiques



[http ://www.univ-rennes1.fr/CRU/Multicast/presentation\\_mcast\\_mbone.ar](http://www.univ-rennes1.fr/CRU/Multicast/presentation_mcast_mbone.ar)



- Diffusion de son et d'images (navette spatiale)
- Téléconférence & télé-enseignement (thèses, conférences)
- Tableau blanc distribué avec distribution de transparents
- Éditeur de texte distribué
- Extension du WWW commandé à distance
- Magnétoscopes virtuels

Outil d'annonce d'application : sdr





- Consultation avec calendrier des événements (sdr)
- Lancement des applications nécessaires
- Création et annonce de ses propres événements
- Envoie chaque annonce SAP toutes les 8 minutes via...  
MBone ! Gestion distribuée
- Restriction de certaines sessions par chiffrement
- Protocoles à la base de la téléphonie sur IP et autres  
visio-conférences (SAP, SDP, RTP...)



- RFC 1112
- Utilisation d'une plage d'adresse plutôt que d'ajouter directement un protocole
- Adresses 1110 224.0.0.0 à 239.255.255.255 :  $2^{28}$  adresses de groupes avec protocole spécial
- Extension des sockets : paquet diffusé vers toutes les autres sur le même adresse/port
- Fonction joindre et quitter groupe
- Utilisation du TTL pour restreindre la diffusion : 31 site, 127 l'univers
- 224.0.0.1 : machines du réseau local



- Internet Group Management Protocol (protocole IP numéro 2)
- Gestion du transit dans MBone
- Messages d'abonnement et de désabonnement à un groupe
- Envoie information aux routeurs du voisinage pour savoir si intéressé par un groupe
- Demande si participation à un groupe



- Utilisation du broadcast d'Ethernet
- Adresse IP D (28 bits)  $\rightsquigarrow$  Ethernet 01-00-5E-xy-zt-uv (23 bits), recouvrement non gênant
- Messages IGMP pour joindre/quitter envoyés en local



- Comment atteindre les membres d'un groupe sur tout Internet ?
  - Comment économiser la bande passante ? Ne transmettre que si des abonnés
  - Optimisation des échanges entre routeurs : dire ce qu'on veut recevoir ou au contraire ce qu'on ne veut pas recevoir ?
- 
- ▶ Mode dense : suppose plein de machines intéressées & absence de membre = exception (DVMRP, PIM-DM)
  - ▶ Mode clairsemé : suppose peu de machines intéressées & absence de membre = règle (PIM-SM). Mécanisme de rendez-vous



PIM (Protocol Independent Multicast) développé par CISCO



- RFC 1075, implémentation sous UNIX `mrouted`, IGMP type 3
- Version multicast de RIP
- Réseau virtuel de tunnels IP-IP entre routeurs
- Adresses 224.0.0.0 à 224.0.0.255 réservées pour protocoles de routage
- Métrique : « distance » pour prendre le plus court chemin
- Barrières de TTL pour délimiter des zones de propagation
- TTL décrémenté de 1 à chaque routeur
- Limitations possible du débit réservé à MBone
- Propagation de routes avec métriques



- Choix des routes avec métrique minimale
- Élagage sur les transmissions inutiles (*prunning*)





- Internet basé sur la confiance (1960...)
- Beaucoup de changements avec le commerce
- Faire confiance aux machines
- Création du *Computer Emergency Response Team* (CERT) en 1988
- Listes de points faibles qui traînent sur le réseau. À double tranchant...
- Logiciels qui testent des points de sécurité (SATAN, ISS, Crack,...)



- Restriction des possibilités dangereuses par logiciel et/ou matériel
- Interdiction de certains protocoles (`rlogin` depuis l'extérieur, connexion `X11` depuis l'extérieur) depuis certaines machines/réseaux
- N'empêche pas les chevaux de Troie (virus apporté par un utilisateur interne ou récupéré sur le réseau)



- L'Expérience...
- Approche haut  $\rightsquigarrow$  bas :
  1. Niveau application (`ps`)
  2. Niveau système (`ps`)
  3. Niveau routage (`netstat -r`)
  4. Niveau transport (`tcpdump`)
  5. Niveau matériel (analyseur réseau)



- Acheter un PC sans produit MicroSoft
- Acheter des modems
- Installer un UNIX du domaine publique
- Gérer les modems avec PPP
- Prendre un accès IP auprès d'un gros fournisseur avec un liaison spécialisé rapide
- Gérer le routage avec gated



- Croissance anarchique du réseau
- Pénurie d'adresses IP (comme le téléphone en France...)  
    ~> IPv6
- Renumérotation en attendant pour simplifier les tables de routage
- Baisse des performances : évolution du nombre d'utilisateurs trop rapide
- Nécessité d'injecter des capitaux privés ~> autoroutes de l'information (1997 ☺)
- Serveurs miroirs, compression, caches WWW
- Augmentation du bruit par les nouveaux « qui ne savent pas », spam...



- Sécurité basée d'abord sur la confiance...
- Nécessité d'avoir des protocoles sécurisés (télépaiement...)



- Adresses sur 128 bits, place pour plus de hiérarchie
- Réservation des ressources possibles (téléconférence)
- Prend en compte des contraintes de temps réel
- Chiffrement et authentification
- Multidiffusion plus hiérarchisée
- Optimisation des entêtes (plus de sommes de contrôles superflues)
- Pas de fragmentation dans les routeurs
- Entêtes d'extension
- Étiquette de flot sur 24 bits (simplifie le routage)



- Comprendre comment cela fonctionne
- Beaucoup de mécanismes « transparents » peuvent ralentir le réseau s'ils sont mal utilisés
- Résoudre les problèmes quand il n'y a personne pour les résoudre...
- Faire des choix techniques (applications, fournisseurs)
- Gagner des sous, télétravail, téléconférence
- Transférer expérience Minitel française dans Internet ? (1997 ☺)
- Importance socio-économico-politique capitale : disparition des frontières physiques et culturelles...





1	Titre . . . . .	0	12	Interface programmeur . . . . .	20
2	Copyright (c) . . . . .	1	11	<b>Protocole</b> . . . . .	19
3	Introduction . . . . .	2	13	Protocole IP . . . . .	22
2	<b>Introduction</b> . . . . .	1	14	Espace d'adressage . . . . .	24
4	Plan . . . . .	4	15	User Datagramm Protocol (UDP) . . . . .	25
5	Réseau ? . . . . .	5	16	Transmission Control Protocol (TCP) . . . . .	26
4	<b>Histoire</b> . . . . .	4	17	Clients & serveurs . . . . .	28
6	Origine . . . . .	7	18	Service de nom . . . . .	29
7	Organisation . . . . .	11	19	World Wide Web . . . . .	33
8	RENATER (1997) . . . . .	13	20	Connexion à distance . . . . .	35
7	<b>France</b> . . . . .	12	21	Exécution à distance . . . . .	38
7	<b>RENATER</b> . . . . .	12	22	Transferts de fichier . . . . .	39
9	GIX RENATER (1997) . . . . .	17	23	Messagerie électronique . . . . .	40
10	Connexion internationale (1997) . . . . .	18	24	MIME . . . . .	42
11	RENATER 4 (2006) . . . . .	19	25	Nouvelles . . . . .	43



26	Remote Procedure Call . . . . .	44
27	Partage de fichiers . . . . .	45
28	XWindow System 11 . . . . .	46
29	Distribution du temps . . . . .	48
30	Contrôle SNMP . . . . .	49
31	Encapsulation pour accès modem . . . . .	50
32	Divers . . . . .	51
33	Chiffrement . . . . .	52
34	Ethernet . . . . .	54
33	<b>Niveau physique – MAC</b> . . . . .	53
35	Protocole ARP . . . . .	55
36	Protocole RARP . . . . .	56
37	DHCP . . . . .	57
38	Zeroconf . . . . .	59
39	Le routage . . . . .	60

38	<b>Routage</b> . . . . .	59
40	Protocole ICMP . . . . .	61
41	Route par défaut . . . . .	63
42	Diffusion . . . . .	64
43	Routage interne . . . . .	65
44	Routage externe . . . . .	66
45	MBone . . . . .	68
44	<b>Multi-diffusion</b> . . . . .	67
46	Application de MBone . . . . .	70
47	Annonce des sessions . . . . .	71
48	Espace d'adressage de MBone . . . . .	72
49	Protocole IGMP . . . . .	73
50	MBone sur Ethernet . . . . .	74
51	Routage sur MBone . . . . .	75
52	DVMRP . . . . .	77
53	Problèmes de sécurité . . . . .	79



52	<b>Sécurité</b> . . . . .	78
54	Pare-feu . . . . .	80
55	Résoudre les problèmes . . . . .	81
54	<b>Production</b> . . . . .	80
56	Faites votre fournisseur Internet . . . . .	82
55	<b>Futur</b> . . . . .	81

57	Problèmes . . . . .	83
58	IPv6 . . . . .	85
57	<b>Futur</b> . . . . .	84
59	Conclusion . . . . .	86
58	<b>Conclusion</b> . . . . .	85
60	Table des matières . . . . .	87

