

Du fonctionnement d'Internet

Ronan KERYELL@cri.ensmp.fr

—
IAR2M
—

Centre de Recherche en Informatique de
l'École des Mines de Paris

6 décembre 1999

Introduction

1

- Révolution : télégraphe, téléphone, télévision,... Internet
- Internet : LE réseau DES réseaux, ébauche des autoroutes de l'information
- $x.10^8$ utilisateurs ↗
- Outil de travail utile
- Importance stratégique ↗
- Fonctionnement peu connu chez les utilisateurs
- ... et pas toujours par les professionnels du domaine !
- Utile pour utilisation correcte et résoudre les problèmes
- Opportunités de télétravail...



Donner une vision globale rapide sur Internet

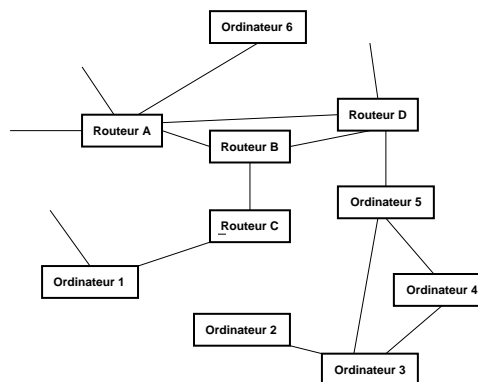
- Histoire et réseaux
- Protocoles & services
- Futur



Réseau ?

3

- Interconnexion de machines (ordinateurs)
<http://www.leb.net/hzo/ioscount>
- Graphe : nœuds (ordinateurs, routeurs) et arcs (liaisons transportant de l'information)



- Faire communiquer les machines entre elles



- Local (LAN : *Local Area Networks*)
 - ▶ Ethernet : 10–100 Mbit/s, 1 Gbit/s
 - ▶ ATM : 155 Mbit/s,...
 - ▶ i SCSI ! 80 Mo/s
- Distant (WAN : *Wide Area Networks*)
 - ▶ RTC : V90 = 56 kbit/s descendant et 33,6 kbit/s (V34) remontant
 - ▶ Liaisons spécialisées et RNIS : 64 Kbit/s–34 Mbit/s
 - ▶ Câble x Mbit/s, souvent asymétrique
 - ▶ x DSL sur ligne téléphonique y Mbit/s, souvent asymétrique (ADSL)
 - ▶ Satellite (souvent sens descendant)
 - ▶ ATM : 155 Mbit/s, 622 Mbit/s, 2,4 Gbit/s,...



- ▶ WDM natif : 1022 longueurs d'onde sur 1 fibre en 1999...
- Portables : GSM (9600 bit/s), UMTS,...
- Protocole : méta-langage pour s'y retrouver et transmettre correctement des informations



- 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, <ftp://ftp.imag.fr/IETF>)
- 1970** : Définition du *Network Control Protocol*
- 1972** : Création de *InterNetwork Working Group* pour concevoir des



Origine

7

protocoles de communication communs avec tolérance aux pannes et aux pertes. Définition d'une architecture : réseaux autonomes interconnectés par des passerelles. ARPANET.
E-mail

- 1972–1974** : 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 (messaging, fora, échanges de fichiers)



- 1980** : Protocole IP mis dans le domaine public ↔ interconnexion TheoryNet avec ARPANET. Télétel 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)



Organisation

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

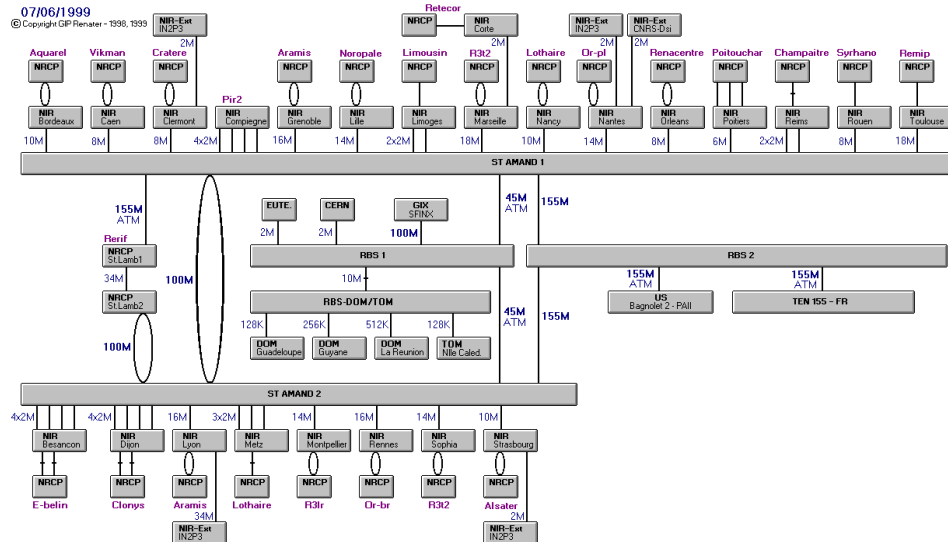
Système de développement des standards plus souple et plus rapide qu'ISO & ITU

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





En 1999 :

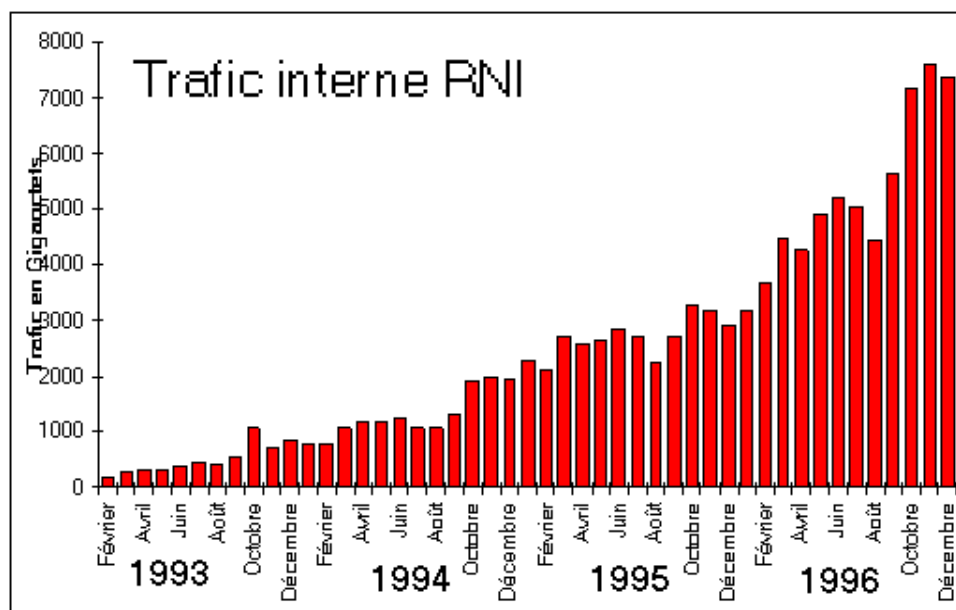


Volume en 1996 sur le Réseau National d'Interconnexion :



Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—France—

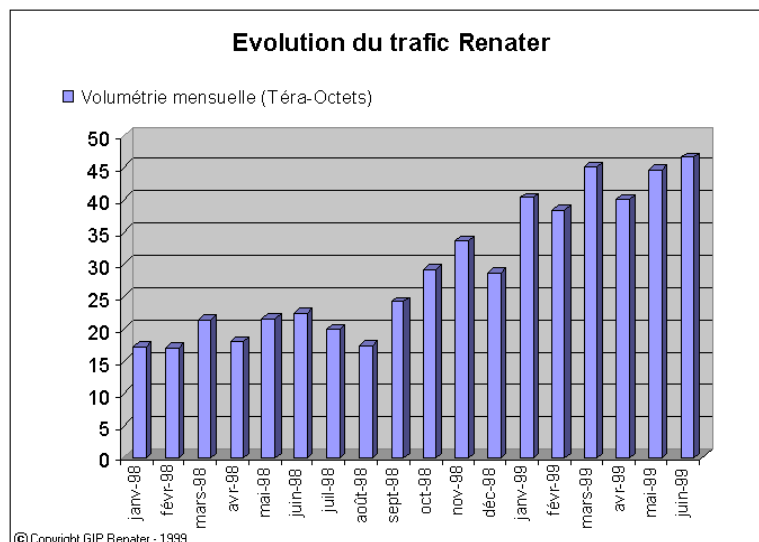


Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—France—



Volume en 1999 (croissance de 150 % par an...) :

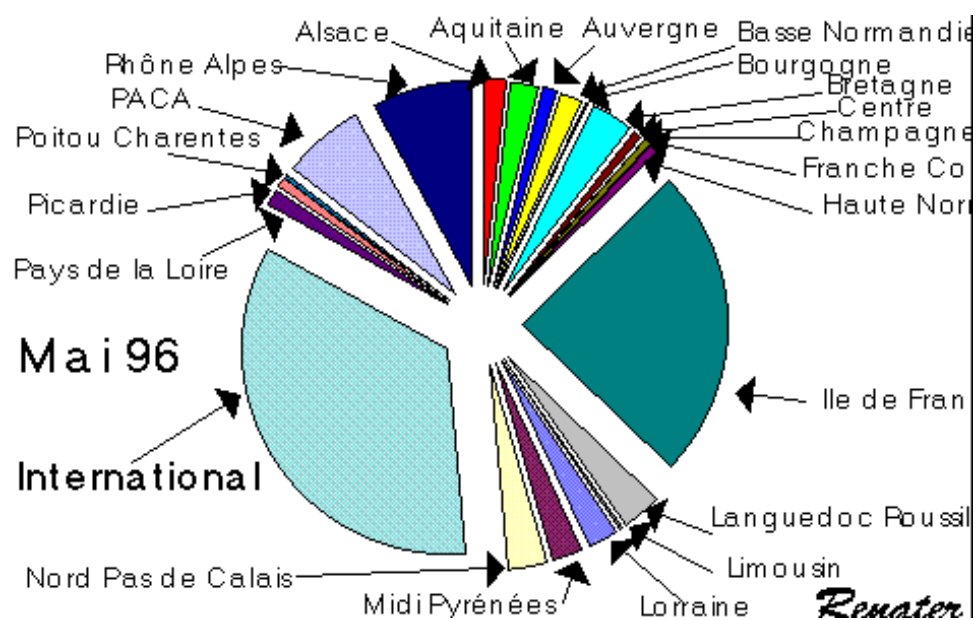


Partition du trafic en 1996 :



Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—France—

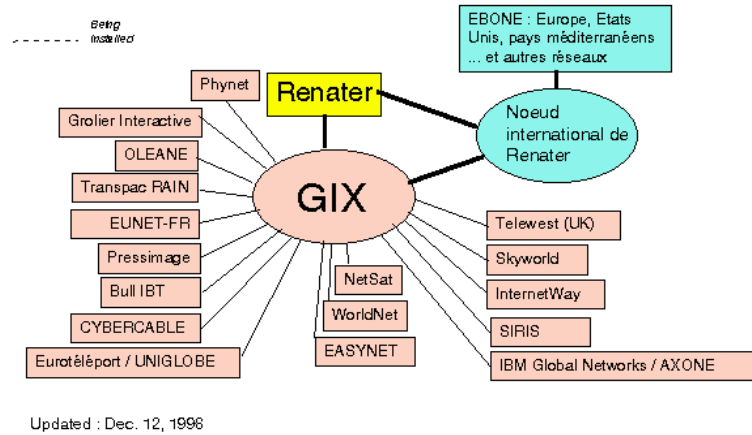


Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—France—



RENATER \neq Internet en France \rightsquigarrow politique de communication entre les réseaux français (matrice de *peering*)



SFINX : service payant d'interconnexion (85kF/an connexion Ethernet + LS en 1998)



Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—France—

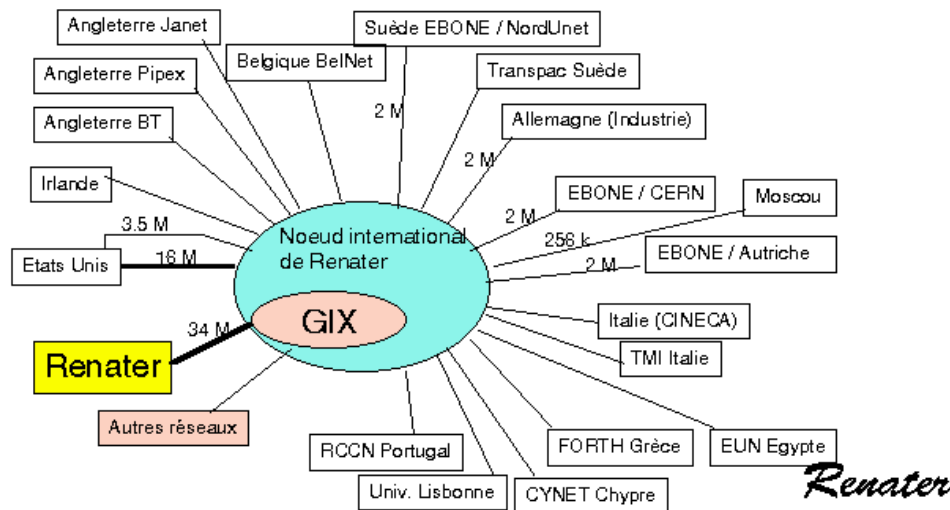


Connexion internationale

19

<http://www.renater.fr/International>

En 1996–1998 :

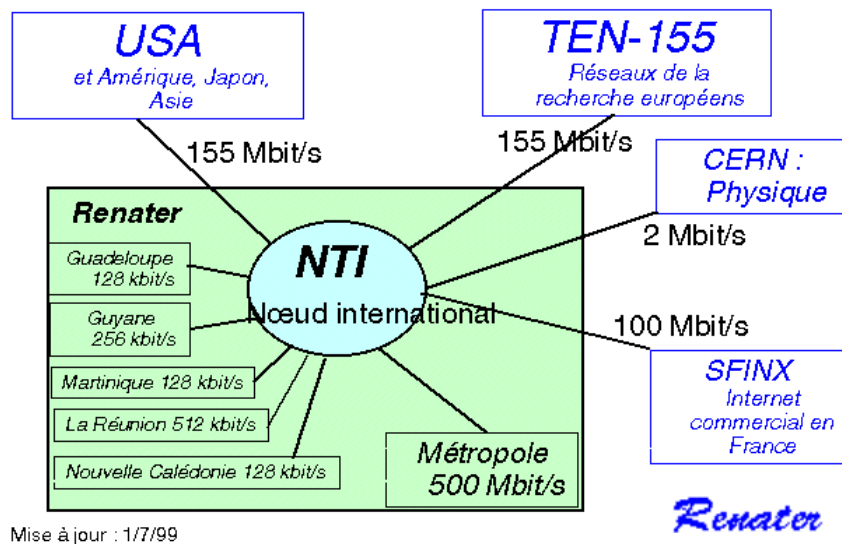


Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—France—



En 1999 :



Avec les USA : <http://www.renater.fr/International/US.htm>



Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

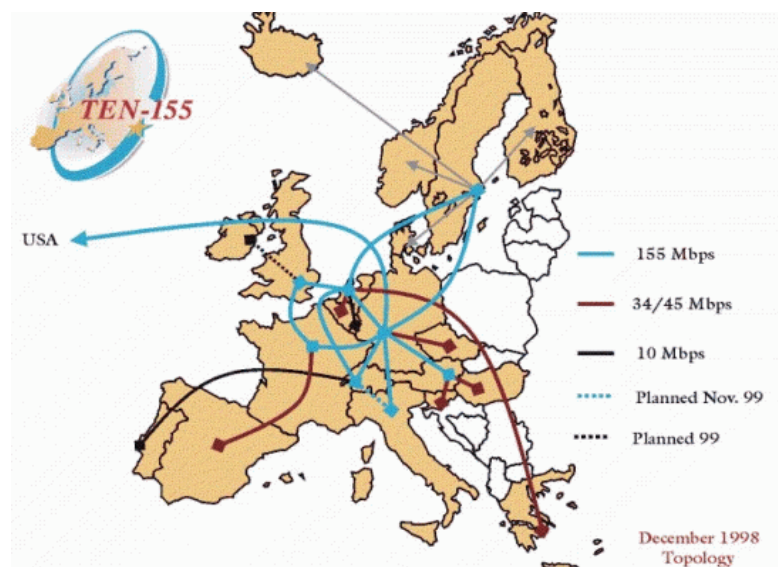
—France—



Connexion européenne : TEN-155

21

<http://www.renater.fr/International/Europe.htm>. En 1999 :



Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—France—



- `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()`,...



Protocole IP

23

- Internet Protocol
- Niveaux 3 (réseau) dans le monde OSI (ultérieur)
- Assure le routage de datagrammes (petits paquets de données)
- Contient adresse de source (expéditeur) 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 <http://www.ipindex.net>

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 10.x.y.z
- Fontainebleau : 2 classes C sur le même support physique
192.54.148 & 192.54.172



User Datagramm Protocol (UDP)

25

- 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



Transmission Control Protocol (TCP)

27

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




Notion 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



Service de nom

29

- Besoin humain d'un annuaire nom de machine ↔ numéro IP
- Trop de machines ~> hiérarchisation des noms et délégation :
 - ▶ Serveur `root (.)`
 - ▶ Serveurs pour `.fr`, `.edu`, `.com`, `.org`, `.gov`, `.net`,... Problème : +700 000 entrées dans `.com` vers 1998 !
 - ▶ Serveurs pour `.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
- Géré en UNIX par `named` (BIND)
- Informations SOA (description de la zone), NS (serveur de nom), 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`

`nslookup` pour demander des informations:

```
> ensmp.fr
Server: chailly.ensmp.fr
Address: 192.54.172.200

ensmp.fr
origin = fontainebleau.ensmp.fr
```



Service de nom

31

```
mail addr = khaled.fontainebleau.ensmp.fr
serial = 1997021900
refresh = 21600 (6 hours)
retry = 3600 (1 hour)
expire = 3600000 (41 days 16 hours)
minimum ttl = 172800 (2 dans)

ensmp.fr      nameserver = fontainebleau.ensmp.fr
ensmp.fr      nameserver = paris.ensmp.fr
ensmp.fr      nameserver = baloo.ensmp.fr
ensmp.fr      nameserver = chailly.ensmp.fr
ensmp.fr      nameserver = calloway.ensmp.fr
ensmp.fr      preference = 1, mail exchanger = fontainebleau.ensmp.fr
ensmp.fr      preference = 2, mail exchanger = paris.ensmp.fr
ensmp.fr      preference = 3, mail exchanger = baloo.ensmp.fr
ensmp.fr      preference = 4, mail exchanger = chailly.ensmp.fr
ensmp.fr      internet address = 192.54.148.100
fontainebleau.ensmp.fr internet address = 192.54.148.100
paris.ensmp.fr internet address = 192.54.165.200
baloo.ensmp.fr internet address = 192.54.173.101
chailly.ensmp.fr internet address = 192.54.172.200
calloway.ensmp.fr internet address = 192.54.165.171
```

Plus d'information dans le cours sur le **DNS**



- TCP port 80
- *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 \LaTeX) avec des balises SGML
- Possibilité de lancer d'autres applications (*plug-in*) via MIME
- Langage JAVA permettant de télécharger et d'exécuter des applications



Connexion à distance

33

- Accéder à des machines puissantes (SP2...)
- Émulation de terminal
- Protocoles de connexion indépendant du système
- Pas de graphisme
- telnet TCP port 23, VT-100. Mot de passe en clair sur le réseau... telnet accepte un numéro de port : utile pour tester d'autres ports TCP/IP
- tn3270 version émulant un IBM3270
- 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...
- Pour plus de sécurité utiliser des outils style ssh (cf. **cours de sécurité**)



- 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...



Transferts de fichier

35

File Transfer Protocole (FTP)

- FTP `anonymous` pour transférer des fichiers dans `~ftp` sans avoir besoin de compte
- FTP `guest` idem mais avec mot de passe
- 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 mais attention au relai de *spam*)
- 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...
- Problèmes d'authentification (faux mails faciles à faire). Regarder de près les entêtes...
- Confidentialité faible si pas de cryptage (`root...`)
- Métaprotocole : les *smileys* : -)



Messagerie électronique

37

Voir cours sur [sendmail](#) Accès par des machines qui n'ont pas de démon SMTP

- ▶ Démons POP (TCP port 110) & IMAP4 (plus récent) qui tournent sur le serveur
- ▶ Possibilité de télécharger des messages sur un poste PC



- 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,...



Nouvelles

39

- Diffusion de messages sur toute la planète, classés par *newsgroup*
- Network News Transfer Protocol, TCP port 119
- Démons *inn* 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



- 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,...



Partage de fichiers

41

- Network File System 2 & 3
- 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 ↘

Autres systèmes : DCE DFS, Samba (met un protocole MicroSoft dans Unix)



- 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 (`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)




Distribution du temps

43

- Nécessaire de synchroniser les machines (NFS, makefile,...)
- `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,...
-  Pas de cryptographie

```
chailly-keryell > hnpadmin -v strasbourg
strasbourg is a network peripheral
ready to print
chailly is allowed access to strasbourg
Frontpanel message : 00 PRET
```



Encapsulation pour accès modem

45

- Connexion entre ordinateurs par liaisons séries
- 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)

Voir cours sur **PPP**



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



Problème des administrateurs incompetents qui croient à une attaque ou blague dans avertissement ICMP

BOOTP : Renvoie une configuration pour un numéro Ethernet particulier (initialisation)

DHCP : Dynamic Host Configuration Protocol. Configure automatiquement un PC au démarrage (interface réseau, etc)



Cryptage

47

- Interdit à l'exportation aux USA
- Usage en pratique interdit en France sauf avec des clés assez petites (arme de guerre)
- PGP *Pretty Good Privacy* : cryptage à clé publique
 - ▶ Cryptage par une clé TRÈS secrète
 - ▶ Décryptage par une clé publique
 - ▶ Signature : encryptage par clé privée & tout destinataire peut déchiffrer en utilisant la clé publique de l'envoyeur
 - ▶ Chiffrement : encryptage par clé publique du destinataire & décodage par la clé secrète du destinataire
 - ▶ Combinaison des 2

Voir [cours de sécurité](#)



- Niveau liaison physique
 - ▶ Cable coaxial (bus) à 10 Mbits/s
 - ▶ Paire torsadée à 10,100 Mbits/s et 1 Gbits/s
 - ▶ Fibre optique à 10,100 Mbits/s et 1 Gbits/s
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) \rightsquigarrow non déterministe à la base
- ...mais une liaison point à point est déterministe !
- 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



Protocole ARP

49

- 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 de l'adresse 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`



Modems

51

- Transmet des signaux numériques sur un support analogique
- Convertisseurs numériques/analogiques à chaque bout
- Transcodage : transmet des « symboles » (Baud)
- V34 : 33600 bits/s (3429 baud)
- Les gros fournisseurs d'accès ont un accès numérique (MIC) \rightsquigarrow économise le modem analogique côté fournisseur
- \rightsquigarrow V90 = V34 montant + 56000 bits/s dans le sens descendant avec un « modem » numérique économisant la conversion côté fournisseur et permettant une modulation plus fine



- 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      Interface
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



Protocole ICMP

53

- 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
```



Route par défaut

55

- Simplification du routage sur les machines λ
- Si on ne sait pas : on envoie à la route par défaut, censée tomber sur un routeur moins à la rue...
- Simplification avec la notion de machines locale définies 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 : envoi 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)



Routage interne

57

- Internet : plusieurs réseaux, plusieurs entités avec des politiques de routages internes propres (Autonomous System, AS)
- Au sein d'une même entité (École des Mines)
- Par exemple Routing Information Protocol (RIP), [RFC 1058](#), démon `routed` ou `gated`
- 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



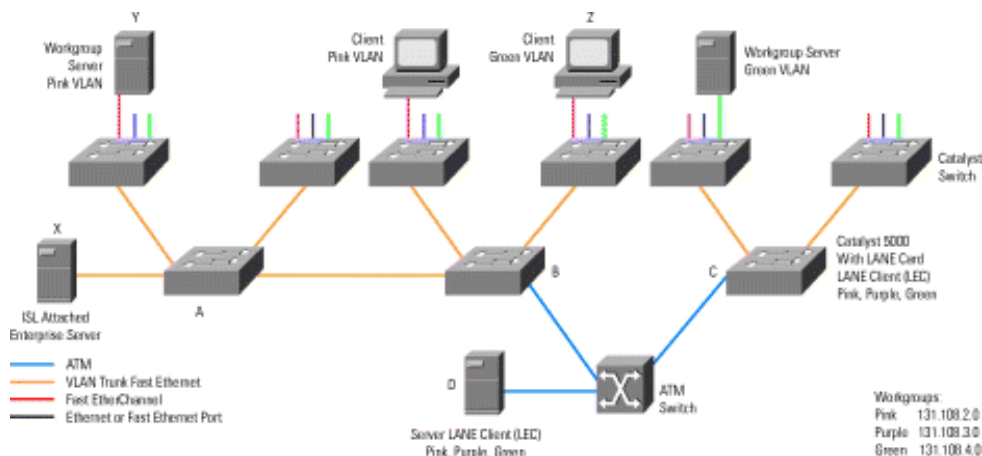
- Connexion de plusieurs AS entre eux
- Rôle de médiateur
- Exemple du Border Gateway Protocol (BGP 4) RFC 1467, gated
- Échange information sur la connectivité avec les autres systèmes BGP avec les chemins d'AS à traverser pour atteindre ces réseaux
- Construction d'une carte de connexion
- Politique : 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



VLAN niveau 2

59

Virtual Local Area Network



- Réseau virtuel au niveau couche basse (niveau 2, Ethernet)



- Relie des machines distantes comme si elles étaient sur le même réseau local (modulo le débit et la latence...)
- Étanchéité des différents VLAN (service comptabilité, production,...)
- Transporte naturellement tous les protocoles au dessus (transport : IP, DEC, NetBIOS, EtherTalk,...)
- Données transitent dans des « tunnels » à travers différents réseaux possibles
- Étanchéité vis-à-vis du transport (Internet) pour la sécurité
- Rajout d'étiquettes identifiant son VLAN à chaque paquet pour faciliter le transport (protocoles ISL, IEEE 802.10 ou 802.1q)
- Peut servir de baie de connexion programmable dans une salle machine...



Voir aussi les VPN

http://www.cisco.com/warp/public/cc/sol/mkt/ent/ndsgn/highd_wp.htm



- *Virtual Private Network*
- Réseau virtuel au niveau réseau
- Doit gérer les protocoles réseau cas par cas (IP, DEC, NetBIOS, EtherTalk,...)
- Relie des machines distantes comme si elles étaient dans un espace de nommage IP unifié
- Données transitent dans des « tunnels » (typiquement encapsulation PPP) à travers différents réseaux possibles
- Étanchéité vis-à-vis du transport (Internet) pour la sécurité
- Permet par exemple de relier des numéros en 10.x.y.z
 - ▶ 10.1.centre.z : Mines de Paris site d'Évry
 - ▶ 10.2.centre.z : Mines de Paris site de Fontainebleau
 - ▶ 10.3.centre.z : Mines de Paris site de Paris



- ▶ 10.4.y.z : Mines de Paris matériel d'interconnexion
- Possibilité de monter en niveau 4 (ports UDP, TCP,...) pour spécialiser le transport de certains flux (vidéo sur un réseau sans qualité de service mais voix sur un réseau avec une meilleure qualité)



- 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 Multidiffusion au dessus d'Internet entre `m`routeurs
- Encapsulation dans du protocole standard (IP dans IP, RFC)
- 1988 entre BBN & Stanford, répandu à partir de 1992
- Choix d'une topologie efficace pour éviter de saturer des liens physiques

<http://www.urec.cnrs.fr/fmbone/>



Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—Multi-diffusion—



Application de MBone

65

- 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`



Fonctionnement d'Internet
DÉPARTEMENT INFORMATIQUE — ENST Bretagne

—Multi-diffusion—



- Consultation avec calendrier des événements
- Lancement des applications nécessaires
- Création et annonce de ses propres événements
- Envoie chaque annonce toutes les 8 minutes via... MBone !
Gestion distribuée
- Ce cours sur MBone ?...

Restriction de certaines sessions par cryptage



Espace d'adressage de MBone

67

- 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



MBone sur Ethernet

69

- Utilisation du broadcast d'Ethernet
- Adresse IP D (28 bits) \rightsquigarrow Ethernet 01-00-5E-xy-zt-uv (23 bits), recouvrement non gênant et permet un préfiltrage au niveau carte Ethernet
- 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) de CISCO



DVMRP

71

- **RFC 1075**, implémentation sous UNIX `mrouterd`, 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,...)



Coupes feu

73

- 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)

Voir [cours de sécurité](#)



- Internet basé sur la confiance mutuelle
- Essaye de faire au mieux dans le transport
- IP protocole unificateur utilisé à toutes les sauces : interactif (rlogin), WWW, multimédia, téléphone, télévision,...
- « Légers » problèmes a priori :
 - ▶ Pas de garantie de débit
 - ▶ Pas de garantie d'arrivée
 - ▶ Jigue incontrôlée
 - ▶ Pas de temps réel
 - ▶ Pas de réservation de bande passante
 - ▶ Pas de gestion de la qualité de service

Gageure ?



Qualité de service

75

- Réseau \equiv Service
- Qualité de service (débit, jigue, taux de pertes/erreurs,...)
nécessaire pour une application
- Mesure
 - ▶ Absolue : qualité de service (QoS)
 - ▶ Relative : classe de service (CoS) favorisant un flot



- Réserve de ressources par flot
 - Implique tous les routeurs
 - Tables d'état des flots dans les routeurs
 - Types de service :
 - ▶ Garantie du délai et débit : applications temps réel
 - ▶ Meilleur effort : Internet classique
 - ▶ Charge contrôlée : intermédiaire (comme sur un réseau peu chargé) pour les applications adaptatives (vidéo)
- RFC 1633



RSVP

77

- Protocole pour dépasser la réservation statique de ressources
- Resource reSerVation Protocol
- Réserve faite par flot (source → destination)
- Nécessite de « rafraîchir » régulièrement la demande
- Adapté aussi au multipoint



- Limiter le nombre de réservations et la taille des tables
 - Étiquetage des paquets à l'entrée du réseau dans le champ IP optionnel DS (6 bits)
 - Routeurs gèrent le trafic en fonction des étiquettes
 - Tables d'étiquettes au lieu de flots
 - Plus simple qu'un routeur IntServ, mieux adapté aux grands réseaux distants
- RFC 2475



Qualité de service sur réseau local

79

- Nécessité de transposer la qualité de service IP sur le réseau local et vers d'autres réseaux
- Ethernet IEEE 802.1p et 802.1q
 - ▶ 8 types de service
 - ▶ Correspondances avec des priorités IntServ et DiffServ
- ATM
 - ▶ CBR, VBR, UBR
 - ▶ Même système de correspondance



- Comment facturer ?
- Qui a le droit de réserver de la qualité ?
- Comment gérer toutes ces demandes de réservation ?
- Courtiers de réservation entre domaines...

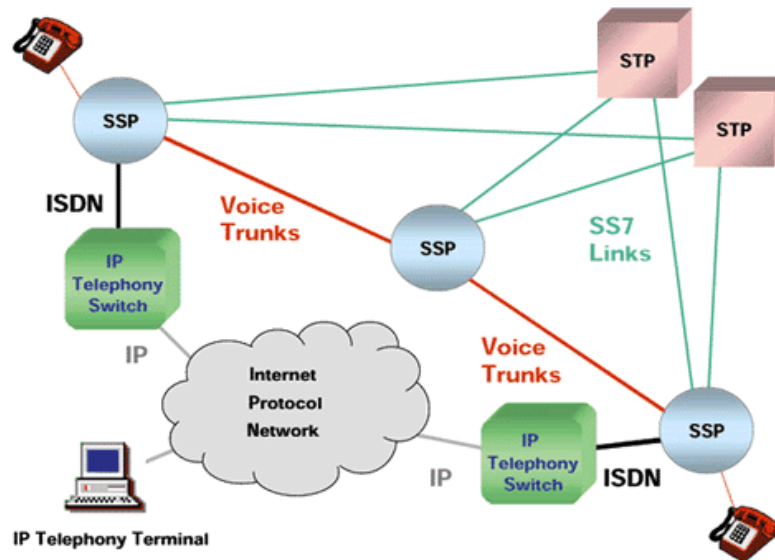


Le Téléphone sur IP

81

- Internet à la mode ~> mettre le téléphone sur IP
 - ▶ Commutation de paquets : optimisation de la bande passante
 - ▶ Compression de la voix
 - ▶ Utilisation d'Internet pas chère (forfait)
 - ▶ Problèmes de perte des paquets, de délais, de gigue,...
- Le GSM habitue le grand public à la mauvaise qualité sonore !
- De toute manière compression en cours de déploiement dans le Réseau Téléphonique Commuté Publique...
- Essayer tout de même d'avoir de la qualité





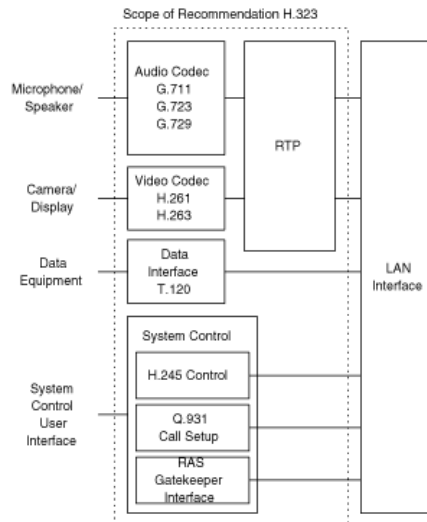
Téléphone H.323

83

- Standard UIT-T
- Téléphones multimédia : voix, vidéo, données,...
- Extension d'un protocole RNIS \rightsquigarrow IP
- Protocole encodé en binaire
- Architecture :
 - ▶ Terminaux de communication
 - ▶ Passerelles (*gateways*) vers le réseau téléphonique classique RNIS ou RTCP
 - ▶ Garde-barrières (*gatekeepers*), points d'entrée, qui font traductions d'adresses/alias, re-routage, autorisation, contrôle de bande passante,...

<http://www.databeam.com/h323/h323primer.html>





Téléphone SIP

85

- Session Initiation Protocol
- Standard IETF
- URL SIP pour appeler en cliquant :
sip:patrik@example.com
- Protocole textuel (ISO-10646) : utilise des entêtes style mail ~>
debug simple
- Utilise protocole SDP (Session Description Protocol comme sdr
pour MBone) pour décrire la session multimédia

```

INVITE sip:pgn@example.se SIP/2.0
Via: SIP/2.0/UDP science.fiction.com
From: Fingal <sip:fll@fiction.com>
To: Patrik <sip:pgn@example.se>
Call-ID: 1234567890@science.fiction.com

```



CSeq: 1 INVITE
 Subject: lunch at La Empenada?
 Content-Type: application/sdp
 Content-Length: ...

v=0
 o=ffl 53655765 2353687637 IN IP4 123.4.5.6
 s=Chorizo
 c=IN IP4 science.fiction.com
 m=audio 5004 RTP/AVP 0 3 5

<http://computer.org/Internet/telephony/w3schrosen.htm>

<http://www.cs.columbia.edu/hgs/sip/sip.html>

http://www.cs.columbia.edu/hgs/sip/drafts/Fing9902_SIP.pdf



Quel téléphone sur IP ?

87

- Guerre H.323 contre SIP/SDP
- H.323, religion UIT, les « commutants »
 - ▶ Complet
 - ▶ Fonctionne
 - ▶ Trop complexe
 - ▶ Fermé
- SIP/SDP, religion IETF, les informaticiens
 - ▶ Souple
 - ▶ Plus simple
 - ▶ Ouvert
 - ▶ Pas encore mature
- Suspense...



- Le téléphone actuel marche bien et est simple d'utilisation...



Résoudre les problèmes

89

- *L'Expérience...*
- Approche haut \rightsquigarrow bas :
 1. Niveau application (messages d'erreur, ps, truss/strace)
 2. Niveau système (ps, truss/strace, messages de log dans /var/log/syslog, /var/adm/messages)
 3. Niveau routage (netstat -rn, netstat -in,...)
 4. Niveau transport (ifconfig, snoop, tcpdump)
 5. Niveau matériel (analyseur réseau, testeur de câbles)



- Acheter un PC sans produit MicroSoft
- Acheter des modems ou sous-traiter à un opérateur (modems, xDSL)
- Installer un UNIX du domaine libre
- Gérer les modems avec PPP
- Prendre un accès IP auprès d'un gros fournisseur avec un liaison spécialisé rapide
- Gérer le routage avec gated

Voir par exemple <http://www.free.fr/free/philo.html>



Problèmes

91

- Croissance anarchique du réseau
- Pénurie d'adresses IP (comme le téléphone en France...) ~> IPv6 et translation d'adresse en attendant
- 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
- Serveurs miroirs, compression, caches WWW
- Augmentation du bruit par les nouveaux « qui ne savent pas » et les effets de bord du commerce
- Sécurité basée d'abord sur la confiance...



- Nécessité d'avoir des protocoles sécurisés (télépaiement...)



IPv6

93

- Adresses sur 128 bits, place pour plus de hiérarchie
- Réservation des ressources possibles (téléconférence) (mais DiffServ et autres aussi en IPv4...)
- Prend en compte des contraintes de temps réel
- Cryptage et authentification (mais IPsec aussi en IPv4...)
- 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
- Indispensable pour résoudre les problèmes
- Faire des choix techniques (applications, fournisseurs)
- Beaucoup de mécanismes « transparents » peuvent ralentir le réseau s'ils sont mal utilisés
- Gagner des sous, télétravail, téléconférence
- Transférer expérience Minitel française dans Internet ?
- Importance socio-économico-politique capitale : disparition des frontières physiques et culturelles...



List of Slides

- | | |
|--|-----------------------------------|
| 1 Introduction | 33 Connexion à distance |
| 2 Plan | 34 Exécution à distance |
| 3 Réseau ? | 35 Transferts de fichier |
| 6 Origine | 36 Messagerie électronique |
| 10 Organisation | 38 MIME |
| 12 RENATER | 39 Nouvelles |
| 18 GIX RENATER | 40 Remote Procedure Call |
| 19 Connexion internationale | 41 Partage de fichiers |
| 21 Connexion européenne : TEN-155 | 42 XWindow System 11 |
| 22 Interface programmeur | 43 Distribution du temps |
| 23 Protocole IP | 44 Contrôle SNMP |
| 24 Espace d'adressage | 45 Encapsulation pour accès modem |
| 25 User Datagram Protocol (UDP) | 46 Divers |
| 26 Transmission Control Protocol (TCP) | 47 Cryptage |
| 28 Clients & serveurs | 48 Ethernet |
| 29 Service de nom | 49 Protocole ARP |
| 32 World Wide Web | 50 Protocole RARP |
| | 51 Modems |
| | 52 Le routage |



53	Protocole ICMP	74	Politique du meilleur effort
55	Route par défaut	75	Qualité de service
56	Diffusion	76	IntServ
57	Routage interne	77	RSVP
58	Routage externe	78	DiffServ
59	VLAN niveau 2	79	Qualité de service sur réseau local
62	VPN niveau 3	80	Problèmes liés à la QoS
64	MBone	81	Le Téléphone sur IP
65	Application de MBone	83	Téléphone H.323
66	Annonce des sessions	85	Téléphone SIP
67	Espace d'adressage de MBone	87	Quel téléphone sur IP ?
68	Protocole IGMP	89	Résoudre les problèmes
69	MBone sur Ethernet	90	Faites votre fournisseur Internet
70	Routage sur MBone	91	Problèmes
71	DVMRP	93	IPv6
72	Problèmes de sécurité	94	Conclusion
73	Coupes feu	95	Table des matières

