Informatique scientifique à l’Institut Pasteur

Du matériel :

- un réseau de structure simple
- des machines : une cinquantaine.

Des logiciels :

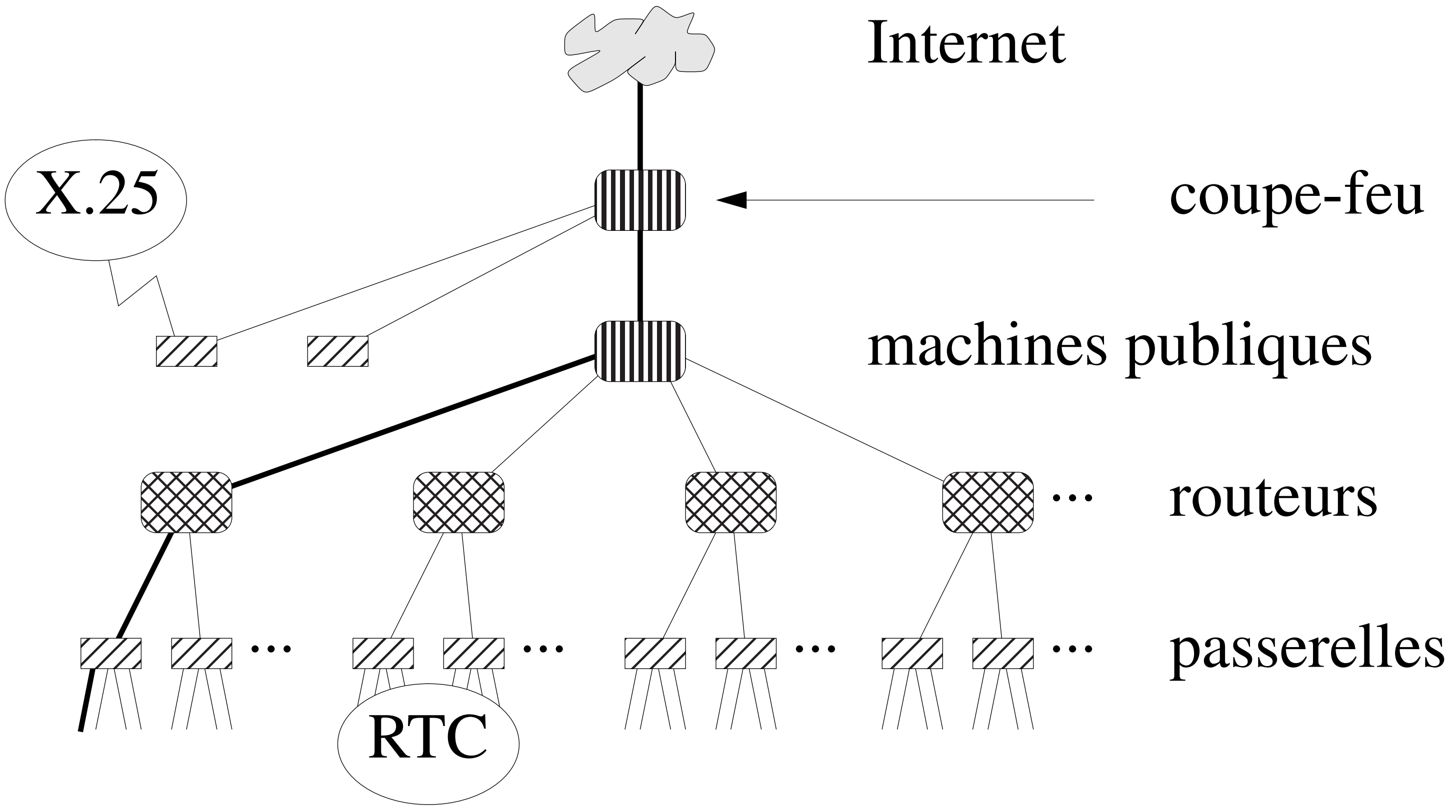
- GUI, Mail, News, serveurs d’information
- biologiques.

Objectifs :

- faire marcher tout ça,
- formation des utilisateurs à l’informatique,
- développement.

Réseau

Topologie logique hiérarchique à 3 niveaux



Réseau

Construction physique :

- mi 92 $\rightarrow$ mi 93,
- 4 km de fibre optique, 150 km de câble métallique,
- 34 baies, équipée chacune d'un routeur Cisco, et de jusqu'à 2 passerelles,
- 2200 points de connexion sur lesquels on peut brancher 2 prises,
- coût total 8MF (+ 4MF de donation de DEC), < 2000F/prise,
- accès Renater à 2Mbit/s.

Machines «publiques»

Serveur d’accès, de courier, NFS, de logiciels :

Sun 4/670 MP sous SunOS 4.1.3

- 128 Moctets de mémoire centrale,
- 15 Goctets de disque.

Serveur de calcul : Convex C 3420 sous ConvexOS v10.1

- 512 Moctets de mémoire centrale,
- 7 Goctets de disque.

Serveur FTP, de News, w3 :

DEC alpha 5000 sous OSF/1 v2.0

- 128 Moctets de mémoire centrale
- 13 Goctets de disque.

Moyens d’accès

Internet

- routage, filtrage ;

X.25

- accès limité au serveur d’accès,
  se ramène donc à un problème de qualité d’authentification sur ce serveur ;

RTC :

- géré par le service, et contrôlé,
- «sauvage» non forcément détectable. Solutions ?
  Publicité sur la présomption de responsabilité ?
  Engagement contractuel de responsabilité ? ….

Physique.

Routeurs

Routage statique.

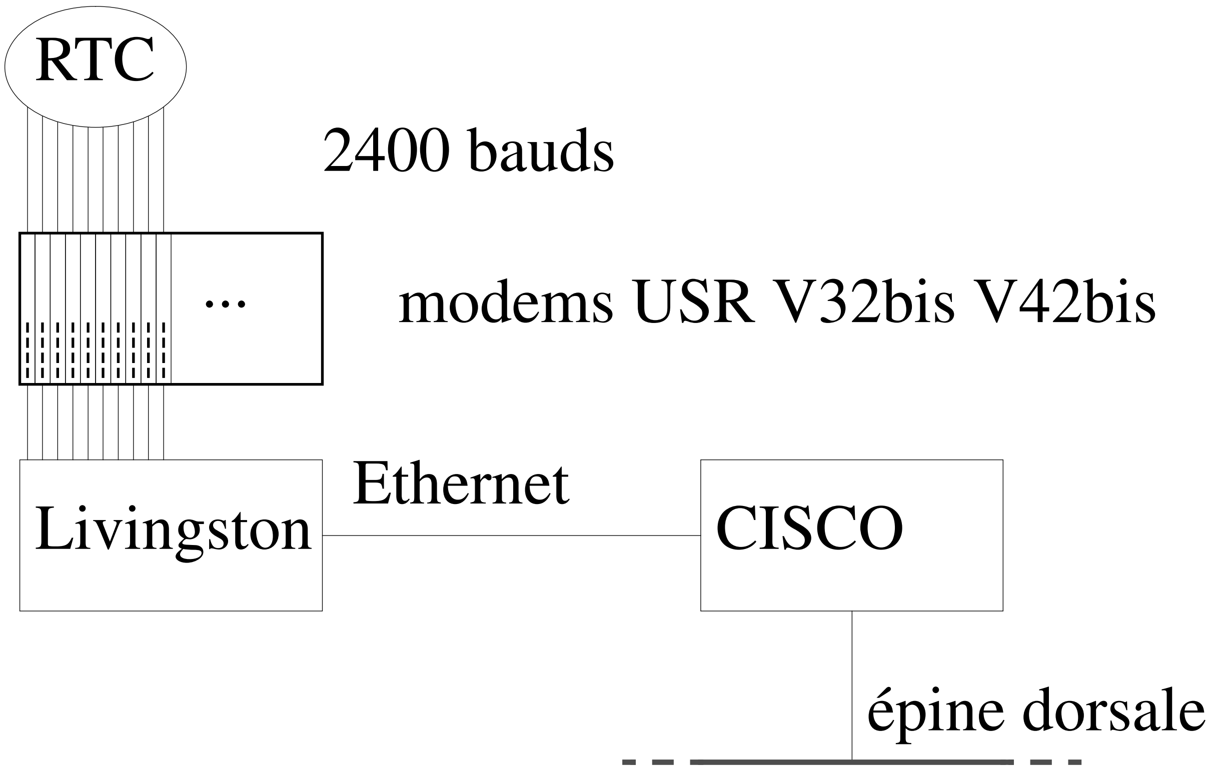
Filtrage d'accès à tous les routeurs :

- connexion limitée aux machines d'administration «internes»,
- aucun filtrage entre sous-réseaux.

Coupe-feu :

- accès aux machines «publiques» ouvert,
- accès aux autres machines limité aux services utilisant des ports non privilégiés (>1023) : essentiellement X.

Accès RTC géré par le Service



Types d'accès RTC gérés

Accès asynchrone :

→ rlogin / serveur d'accès ;

Accès réseau (SL/IP ou PPP) anonyme :

→ limité aux machines publiques par protocoles telnet, ftp, gopher, http ;

→ adresse assignée dynamiquement dans le réseau «externe» :
[64 ; 254].

Accès réseau authentifié par rappel :

→ ouvert,

→ adresse fixe dans le réseau «externe» :
[16 ; 63].

Serveur d'accès

tcp_wrappers : trace des accès par 'syslog';

shadow_login : trace des accès refusés, trace des connexions X.25 et RTC par 'syslog'.

Vérification régulière de la qualité des mots de passe :
elle est toujours aussi bonne :o).
Solutions ?
Engagement de responsabilité lors de la demande d'ouverture d'un compte ?

Formation des utilisateurs à UNIX :

`umask(1)`, `chmod(1)`, `rhosts(4)`, `xhost(1)`, `xauth(1)`, ...

Vérification régulière d'intégrité par mirroir asynchrone de '`/`' et '`/usr`', ...

Projets

Mise en place d'un mouchard sur Ethernet en amont de notre coupe-feu.

Surveillance automatique de l'ARP.

Mise en place d'un relai dans le réseau «public» pour les protocoles filtrés par notre coupe-feu.

Automatiser la surveillance de la qualité des mots de passe, et de l'intégrité des systèmes «publics».

Automatiser la surveillance de l'intégrité de la configuration de tous les équipements «sensibles» : routeurs, passerelles, machines d'administration «internes».

….