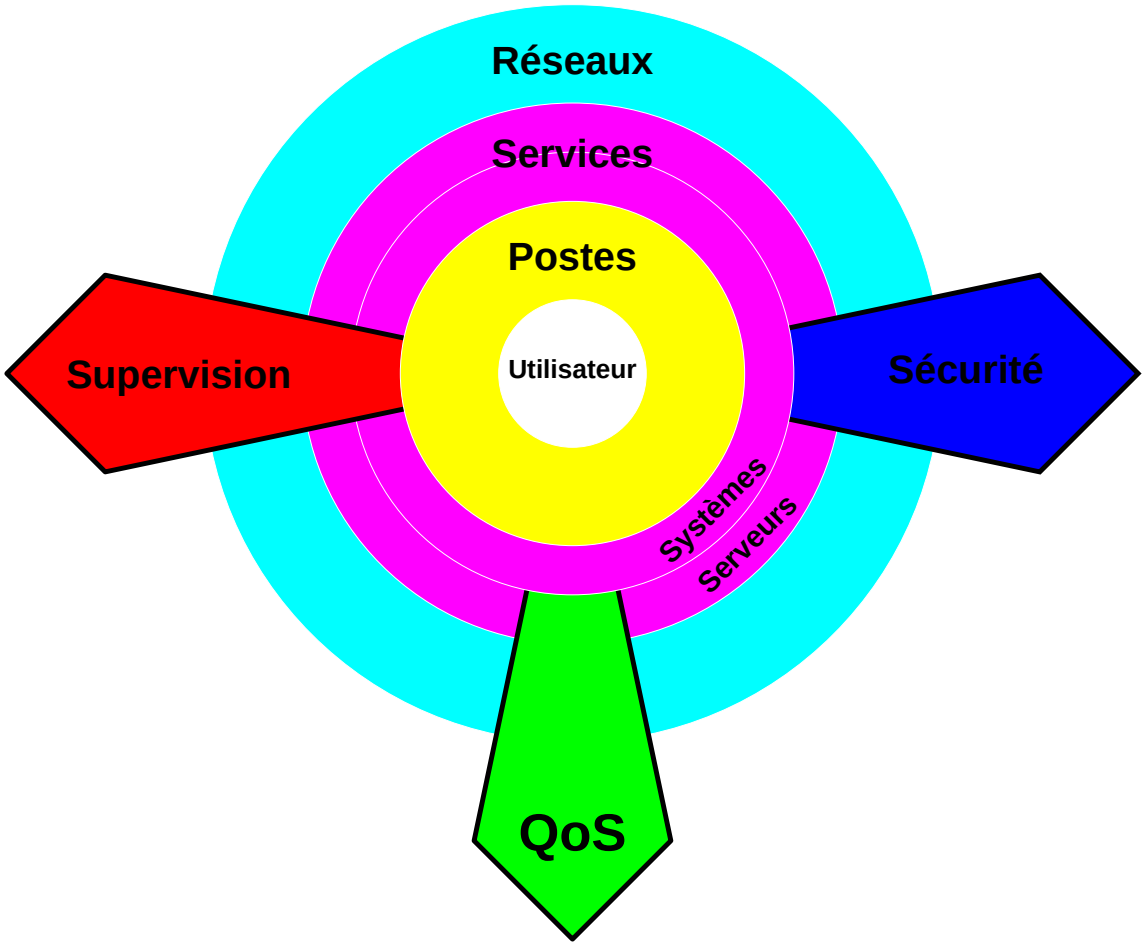
De l'intérêt d'une même plate-forme système sur un campus en général...

... au radical déploiement de GNU/Linux sur l'ENS-Cachan en particulier

Emmanuel Quémener, Pascal Soullard, Pascal Varoqui

CRI – Ecole Normale Supérieure de Cachan

L'utilisateur au centre du dispositif informatique



GNU/Linux à l'ENS-Cachan avant le JRES 1999

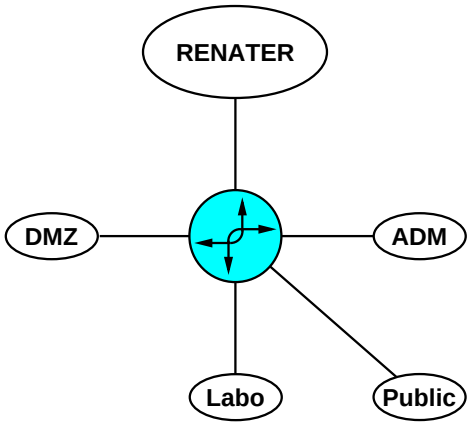
- **Réseaux**
  - Routeur AppleTalk/IP de la direction : GNU/Linux sous Slackware
  - Passerelle PPP : GNU/Linux sous Slackware
- **Services**
  - Serveur de courriel : SendMail sous Solaris 2.6 sur Sparc 4 et Sparc 1+
  - Serveur WWW : Apache sous Solaris 2.6 sur Sparc 4
  - Serveur de cache WWW : Squid sous Solaris 2.6 sur Sparc 4
  - Serveur de Forums de Discussion : INN sous Debian sur i386
- **Postes de Travail**
  - Administration : aucun, à l'exception de TeraTerm...
  - Salles publiques : outils de développement GNU
  - Laboratoires CNRS et départements de recherches (culture UNIX) :
    - LURPA : Slackware sur i386
    - LMT : SuSE sur i386
    - LSV : RedHat sur i386

Choix de Debian GNU/Linux sur i386

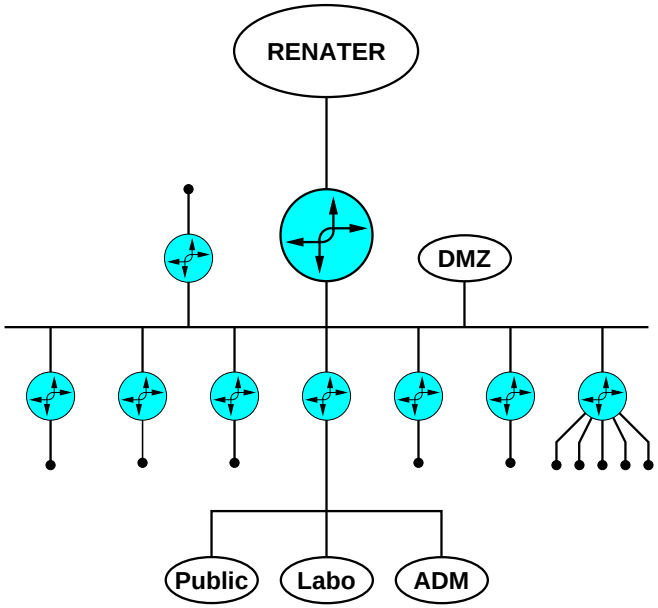
Réseaux

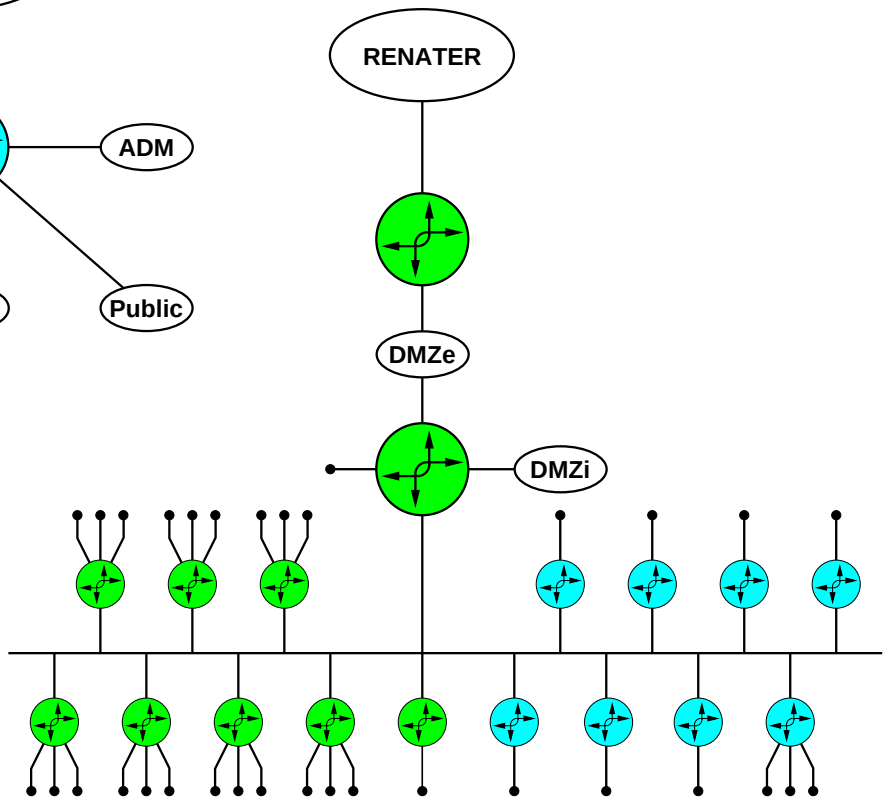
Evolution d'un réseau local de 1999 à 2001

Projet



JRES 1999





JRES 2001

Réseaux

Solution : PC générique équipé de 4 cartes FastEthernet

Partie Matérielle

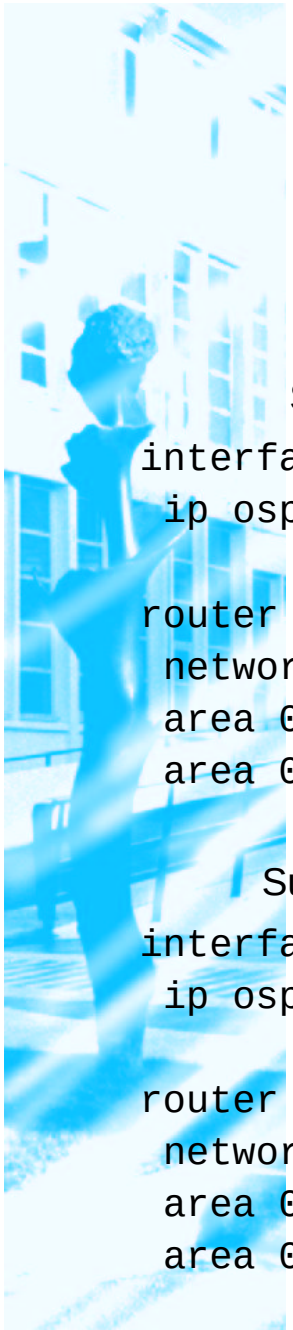
- Carte mère Pentium
- Boîtier Desktop
- PC Pentium 133 MHz à 225 MHz
- Mémoire de 32 Mo à 96 Mo
- HD en rack amovible
- 4 carte PCI 3com 3c905
- 1 video ISA
- 1 carte PCI ATM ForeRunnerLE

Partie Logicielle

- Routage OSPF : Zebra & GaTeD
- Routage DVMRP : Mrouted
- Routage AppleTalk : UAR
- Serveur SNMP : UCD SNMPd
- «Traçage» : NetAcct
- Filtrage avancé : NetFilter + IPtables
- Interopérabilité : respect RFCs !
- Services : NTPd, SSHd, DHCPd

Remarques

- Capacités de routage : > à 80 Mb/s ;
- Capacités de filtrage : > à 70 Mb/s ;
- Disponibilité immédiate de 3 routeurs ;



Réseaux

Routage dynamique : OSPF & BGP

Routage OSPF

Sur un routeur «standard» sous IOS :

```
interface Ethernet0/1
 ip ospf authentication-key COOLZEBRA

router ospf 31415
 network 138.231.0.0 0.0.255.255 area 0
 area 0 authentication
 area 0 range 138.231.0.0 255.255.0.0
```

Sur un routeur «générique» sous Zebra :

```
interface eth0
 ip ospf authentication-key COOLZEBRA

router ospf
 network 138.231.0.0/16 area 0
 area 0 authentication
 area 0 range 138.231.0.0/16
```

Routage BGP

Sur un routeur «standard» sous IOS :

```
router bgp 65014
 network 138.231.0.0 mask 255.255.128.0
 network 138.231.128.0 mask 255.255.128.0
 neighbor 193.51.12.69 remote-as 2200
 neighbor 193.51.12.69 ebgp-multihop 2
 neighbor 193.51.12.69 update-source Loopback1
 neighbor 193.51.12.69 version 4
```

Sur un routeur «générique» sous Zebra :

```
router bgp 65014
 bgp router-id 193.51.12.70
 network 138.231.0.0/17
 network 138.231.128.0/17
 neighbor 193.51.12.69 remote-as 2200
 neighbor 193.51.12.69 update-source eth0:1
 neighbor 193.51.12.69 ebgp-multihop 2
```

Réseaux

Routage Macintosh

- Premier routeur GNU/Linux à l'ENS-Cachan : 1995
- Placement d'un «dispositif AppleTalk» dans zone spécifique :
  - séparation automatique des domaines (équivalent sous-domaine DNS),
  - dispositif AppleTalk : Macintosh, imprimante,
  - routage AppleTalk à travers RENATER (tunnel IP) ;
- Logiciel utilisé : UAR (Unix Appletalk Router).

Serveur d'accès distant

- avec carte multi-séries Cyclade :
  - 8 modems 28800 bauds,
  - mise en service en 1997, 150000 connexions ;
- avec carte RTC/RNIS Digi Datafire RAS B4ST :
  - 8 entrées V90/Numéris,
  - mise en service en 2001.

Services

Convergence vers un serveur générique

Etat des serveurs fin 2000 :

– DNS, SendMail, Proxy, WWW : Sparc 4 64 Mo de RAM,
– SendMail vers clients : 2 Sparc 1+ 32 Mo de RAM,
– Comptes UNIX des élèves : Ultra 5 128 Mo de RAM,
– UseNet : Pentium 200 MHz 128 Mo ;

Utilisation de Postes Ultra 5 : **essais peu concluants**

– puissance d'équivalence K6 233 Mhz,
– mémoire spécifique de prix inabordable,
– contrôleur et disque IDE indignes, PCI non standard,
– (clavier+souris) spécifiques ;

Nouveaux Postes de salle élève = Nouveaux Serveurs

– processeur Athlon, 256 Mo de RAM minimum,
– carte 3ware en RAID 1, 2 disques 45 Go.

Migration : uniquement vers Debian (services en LL)

Services

Authentification globale Windows/(Linux+Solaris)

Premier jet :

– Samba pour authentification/partage sous Windows
– NIS+/NFS pour authentification/partage sous Solaris+Linux
– Difficultés : synchronisation entre Samba et NIS+ (Expect...)

Solution déployée :

– Samba pour authentification et partage sous Windows,
– PAM_SMB/NFS pour authentification et partage sous Solaris+Linux,
– modification dans `/etc/pam.d/<application>` :
remplacement de `auth required pam_unix.so`
par `auth required pam_smb_auth.so`,
– Difficultés : nécessité des identifiants dans `/etc/passwd`,
– Futur : nouvelles fonctionnalités de Samba 2.2.

Postes de Travail

L'angoisse des Mise-à-Jour

Arrivée de 3 salles sous PC : double démarrage Linux / Windows NT

- première étape : création d'une «matrice» ;
- deuxième étape : déploiement ;
  - par un `dd if=/dev/hda of=/dev/hdb`,
  - par Ghost : Ok pour Windows, moins clair pour Linux,
  - par Replicator : fonctionnel moyennant quelques améliorations,
    - Démarrage en réseau d'un NFSroot,
    - Partitionnement et formatage,
    - RSync entre la matrice et son clone,
- dernière étape : ultimes réglages avant redémarrage...

Replicator : Sébastien Chaumat, cet après-midi à 14h30

FAI : `http ://www.informatik.uni-koeln.de/fai`

Supervision

Sauvez les Logs !

Et plus si possible...

- **Stockage** :
  - Logs de syslog ;
  - Données de NetAcct ;
  - Configuration des routeurs/serveurs/(postes de travail).
- **Traitement** :
  - Syslog : statistiques et détection de malignité (`detescan.pl`) ;
  - NetAcct : métrologie pour refacturation et statistiques de consommation ;
  - Configuration : extraction des fichiers importants pour reconstruction rapide.
- **Supervision** :

  détection d'activités sur équipements réseau, serveurs et services.

Supervision

Matériels

Bi-Pentium III 1 Ghz avec 768 Mo de RAM, 2×75 Go de HD

Logiciels

- **Supervision :**
  - `Autostatus` : signalisation et expédition de messages
  - `Checkservice` : signalisation sur les services, statistiques et expédition de messages
- **Métrologie : `MRTG`**
  - en standard, accès aux interfaces : routeurs, commutateurs, serveurs, postes ;
  - appel d'une MIB particulière : charge processeur, charge mémoire ;
  - appel de script + `SNMPd` personnalisé sur équipement :
    - `LM-sensors` : température & vitesse de ventilateur ;
    - Nombre de connexions et celles établies sur un routeur ;
    - Nombre de messages dans la queue du `SendMail`
- **Statistiques : `Webalizer, Analog, FWLogWatch`**

Sécurité

De l'utilisateur au réseau

Sensibilisation CNRS : jusqu'à l'utilisateur...

- **Utilisateur :**
  - FORMATION !
- **Postes de Travail :**
  - outils universels sécurisés : Mozilla
  - installation d'un antivirus (pas de libre)
- **Services :**
  - Serveurs : authentification globale et systématique...
  - Systèmes : sécurisation pour utilisation restreinte
    TCP wrappers et expédition de Courriel à chaque connexion
- **Réseaux :**
  - Là où on est intervenu massivement (au niveau des routeurs)...

Sécurité

Le Couple Infernal : NetFilter & IPtables

- **Historique :** IPfwadm (noyaux 2.0.x), IPchains (2.2.x)
- **Contexte :**
  - réécriture pile IP noyau 2.4.x
  - rationnalisation de fonctionnalités (*Masquerading*, *Transparent Proxy*)
- **Filtrage classique :** (SRC:SPT), (DST:DPT), drapeau SYN, NOT sur tout paramètre
- **Modularisation :**
  - définition de jusqu'à 15 ports par ligne de filtrage — `ipt_multiport`
  - filtrage par drapeaux TCP étendu (SYN, ALL, FIN, RST, URG, PSH)
  - limitation sur un port donné en moyenne et impulsionnel — `ipt_limit`
  - filtrage par adresse MAC (pour association IP/MAC) — `ipt_mac`
  - modification à la volée des drapeaux TCP de ToS — `ipt_TOS`
  - translation d'adresses en source et en destination — `iptable_nat, ipt_MASQUERADE, ipt_REDIRECT`
  - marquage par drapeaux pour traitement par QoS — `ipt_MARK`
  - **filtrage orienté connexion** — **`ip_conntrack, ip_conntrack_ftp`**
  - fonctionnalités en perpétuelle croissance — `http://netfilter.samba.org`

NetFilter : modules du noyau

IPtables : utilitaire de configuration

Sécurité

Filtrage Orienté Connexion dans un routeur GNU/Linux

A la base : n'autorisez que les connexions initiées de l'intérieur

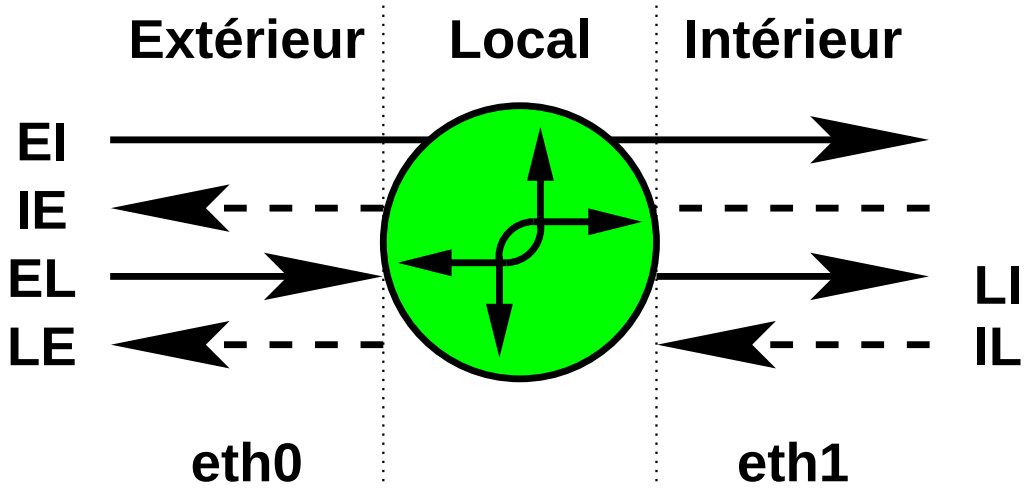
```
iptables -A FORWARD -i eth0 -o eth1 -j EI
iptables -A FORWARD -i eth1 -o eth0 -j IE
iptables -A EI -m state -state ESTABLISHED,RELATED -j ACCEPT
iptables -A IE -j ACCEPT
```

D'extérieur vers intérieur (EI)

- **EI** anti-IP spoofing
- **EI** anti-broadcast
- **EI** ICMP limités (0,3,4,5,8,11,12)
- **EI** traceroute
- **EI** services internes
- **EI** réponses aux requêtes

D'intérieur vers extérieur (IE)

- **IE** anti-IP spoofing
- **IE** anti-broadcast
- **IE** association MAC/IP
- **IE** tout !



Classes de Services

Lissage de trafic différentiel

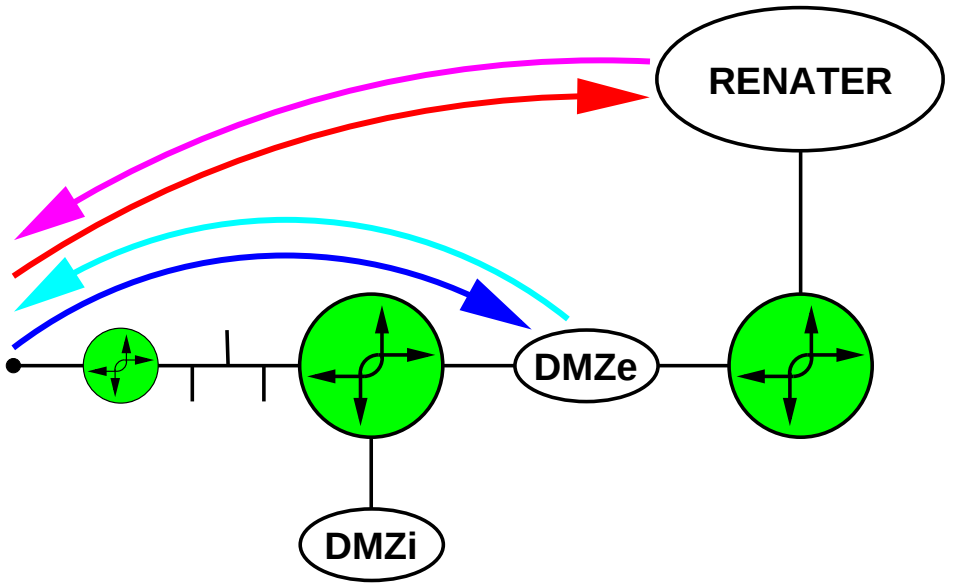
Utilisation de tc (IProute2)

- définition d'une classe par lissage : bande passante maximale
- affectation d'une méthode à la classe : CBQ, CSZ, RED, SFQ, ...
- application par un filtre de cette classe : Adresses source ou destination

Problématique : accès Internet «partagé» avec CR@NS et Lycées du domaine

4 niveaux de lissage

- CR@NS vers ENS-Cachan
- CR@NS vers RENATER
- ENS-Cachan vers CR@NS
- RENATER vers CR@NS



Bilan Financier

Evolution à base de GNU/Linux

- Matériel :
  - Routeur générique Pentium : 300€ (500€ si ATM) 3000€
  - Routeur «musclé» Athlon : 750€ 1500€
  - Serveur «générique» : 1500€ 15000€
- Licences logicielles : rien !
- Maintenance matérielle : rien !
- Maintenance logicielle : rien !

Bilan Humain

De l'intérêt d'une même plate-forme système

- **Avant JRES 1999** : fonctions exclusives des personnels du CRI
  - réseau général, réseau AppleTalk,
  - systèmes, services,
  - postes de travail ;
- **Après JRES 2001** : la recherche d'une polyvalence systématique
  - fonctions doublées : spécialité + 1 ou 2 sous-spécialités,
  - plate-forme unique pour le réseau & les serveurs (ingénieurs & PRAG),
  - formation progressive de deux assistants ingénieurs ;
- Polyvalence du personnel du CRI (RTT...) : routeurs, serveurs (non-administratifs).

Développements à venir

Gros travail à poursuivre sur les postes utilisateurs :

- bornes d'accès à l'Intranet & sites ministériels ;
- standardisation des postes bureautiques.

Travail sur les services :

- Annuaire LDAP : OpenLDAP (cf *«annuaire intégré de l'INP»*) ;
- Infrastructure de gestion de clés : IdealX PKI ;
- Sécurisation des services : contre-mesures DoS, remontées de requêtes suspectes.

Travail sur les réseaux :

- Gestion des zones publiques ;
- Généralisation DHCPd + filtrage par adresse MAC ;
- Meilleure intégration filtrage & QoS (marquage des paquets).

Remerciements

- Pierre Bazart (DRI de l'ENS-Cachan) — confiance
- Utilisateurs de l'ENS-Cachan — indulgence
- Développeurs de GNU/Linux — qualité des réalisations
- Traducteurs — efforts de vulgarisation

Annexes

- ATM sous Linux
- Quelle définition pour la sécurité ?
- Optimisation & réorientation du trafic

Réseaux

ATM sous Linux

- Œuvre de W. Almesberger (comme `LiLo` et `TC`) ;
- Quelques dates :
  - 1995 : démarrage du support d'ATM sous Linux
  - 2000 : intégration au noyau 2.4
  - 2001 : migration vers SourceForge (`http ://linux-atm.sourceforge.org`)
- Deux parties :
  - Modules noyau : CLIP, LANE, MPOA + modules matériels (interfaces réseau) ;
  - Utilitaires de configuration et de contrôle ;
- Au CRI de l'ENS-Cachan :
  - Expérimenté dès Janvier 2000
  - Déployé en test sur un serveur FTP de mars à décembre 2000
  - Utilisé en «production» sur un routeur depuis avril 2001
  - Expérimentations en cours pour en faire des LES et LECS

Sécurité

Quelle définition pour la sécurité

Assurer l'intégrité du système informatique quoiqu'il arrive...

- **Alimentation** : prise, onduleur, grosse coupure ;
- **Matériel** : ventilateur, HD, alimentation, mémoire ;
- **Système d'exploitation** : plantage intempestif en charge ;
- **Système de fichiers** : journalisation ;
- **Sauvegarde** : augmentation des capacités de HD ;
- **Personnel** : polyvalence parfaite en cas de nécessité ?

Et puis tout le reste...

Classes de Services

Optimisation et réorientation de trafic

Changements à la volée des champs ToS :

- Minimize-Delay : Telnet, SSH
- Maximize-Throughput : FTP, WWW
- Maximize-Reliability :
- Minimize-Cost : SMTP, NNTP
- Normal-Service : les autres ?

⇒ Grosse dépendance aux serveurs & clients...

Redirection de requêtes HTTP vers Proxy :

- une ligne dans le routeur vers la DMZ ;
- 4 # décommentés dans le `/etc/squid.conf`

⇒ Première expérience mitigée :

- Sites authentifiant par IP source...
- Efficacité 50%