

La métrologie sur le site CNRS

Une métrologie, pourquoi ?

Objectifs fixés

pour la mise en oeuvre d'un outil spécifique

Méthode retenue

Evolution

Conclusions

Une métrologie, pourquoi ?

L'Internet, support universel pour tous type d'information

- > disponibilité nécessaire du réseau
- > en garder la maîtrise,
- > envisager son évolution.

Notre responsabilité en tant que Point d'accès Internet :

- .vis-à-vis de Renater (usages détournés)
- .vis-à-vis des utilisateurs (services non/mal rendus)

Un élément concourant à la sécurité.

Objectifs fixés pour mettre en oeuvre une métrologie

Un affichage clair, visualisant d'un seul coup d'oeil
l'usage instantané et *réel* du réseau,
par laboratoire, par Institut.

Afin de détecter :

- . un comportement inhabituel,
- . une anomalie,
- . éventuellement des signes d'attaque.

Permettant d'accéder à des détails sur un échange en cours.

Etre assurés que ce qui est affiché est vrai.

La méthode retenue

Règle No1: ne pas réinventer la roue :

- .MRTG : pas assez réactif

- .NetFlow : seulement sur routeurs

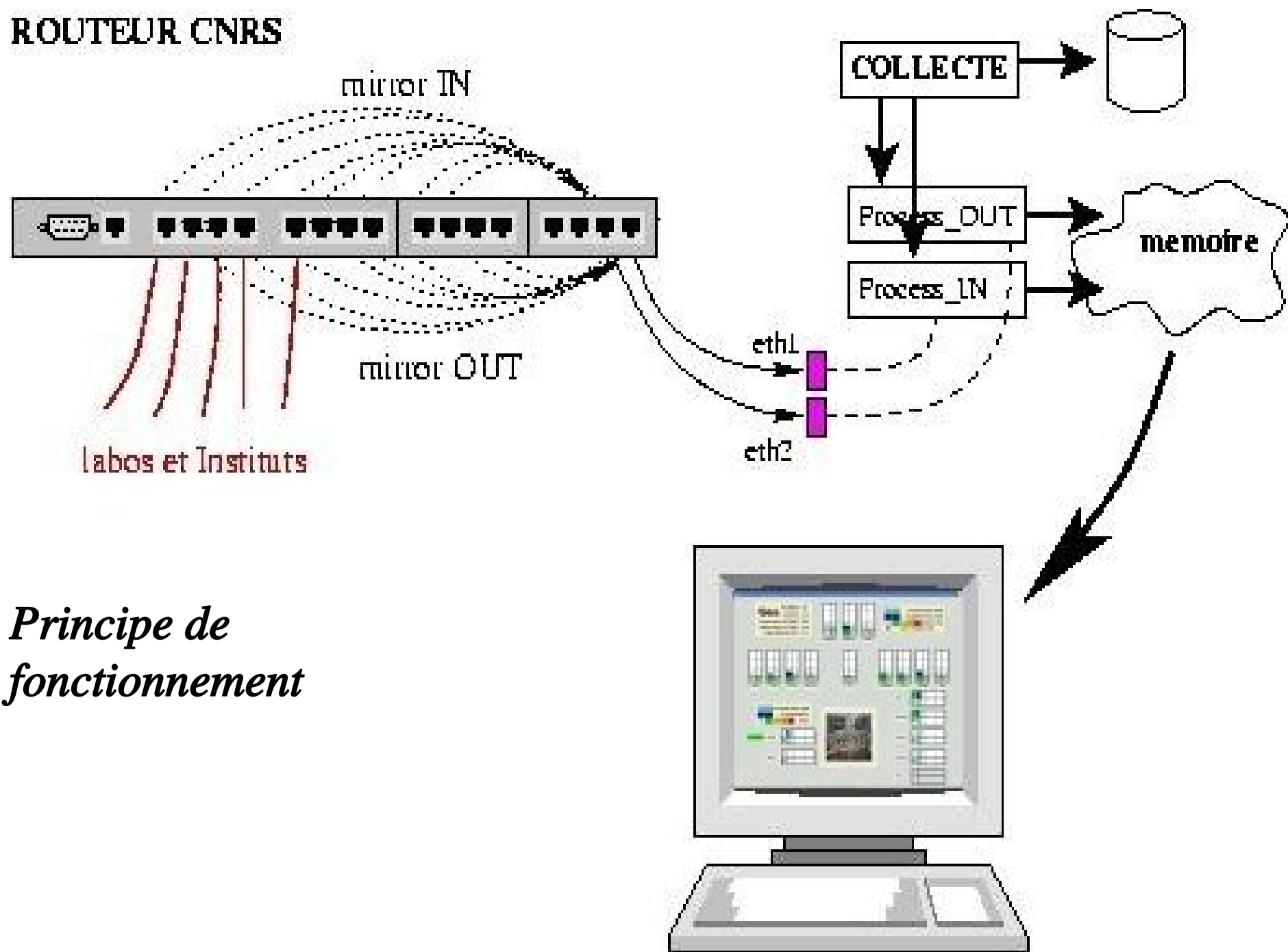
Scinder le projet en modules :

- . collecte

- . mise en base données

- . affichage

ROUTEUR CNRS



*Principe de
fonctionnement*

Principes de fonctionnement (suite)

- > **Paralléliser IN/OUT sur 2 cartes Gb.**
Mais sérialiser collecte, puis affichage
pour éviter toute saturation de CPU.
- > **Contre-vérification dynamique via SNMP**
(une seule requête : infos sur tous les ports :
 - .UP/DOWN,
 - .trafic unicast/Mcast IN/OUT,
 - .erreurs IN/OUT, etc.)
- > **Les avertissements audios**
évitent la surveillance continue de l'écran.

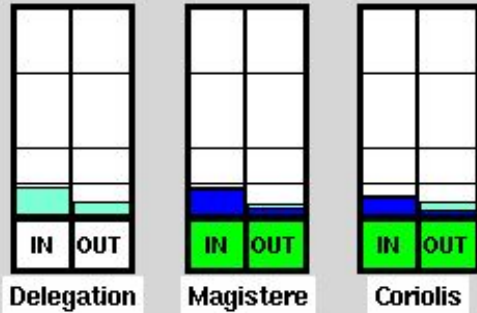
Mise en service
en sept 2002



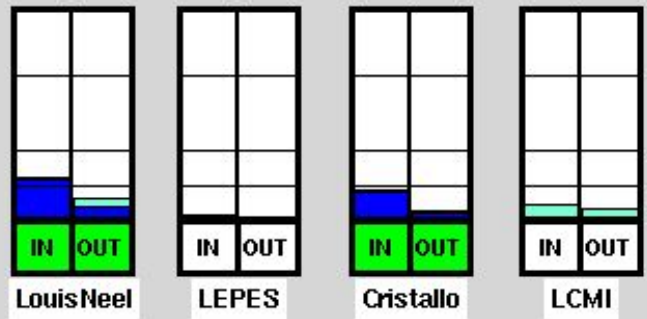
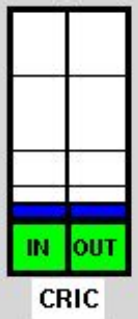
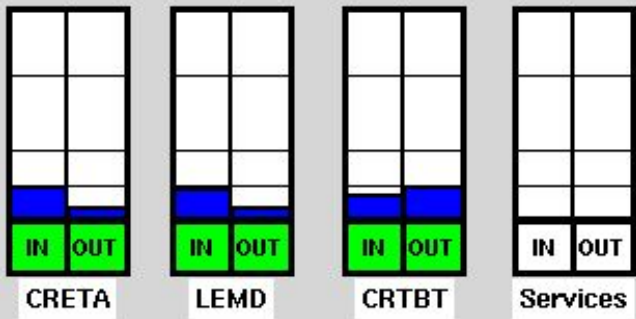
.2 cartes Gb
.double CPU
AMD 2800+
.2 Go RAM



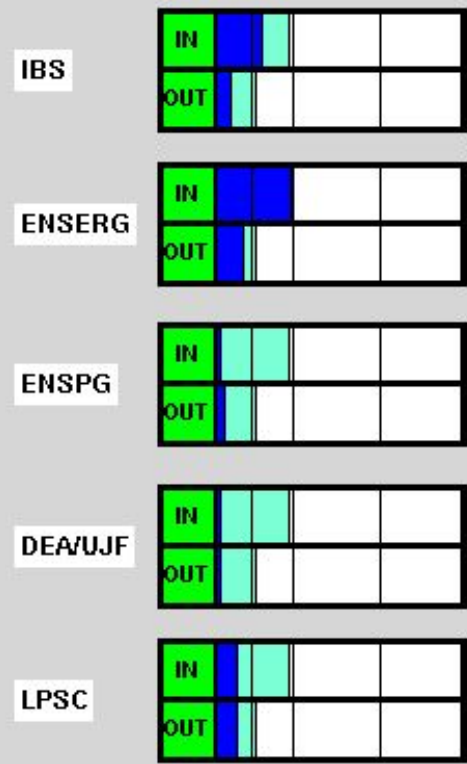
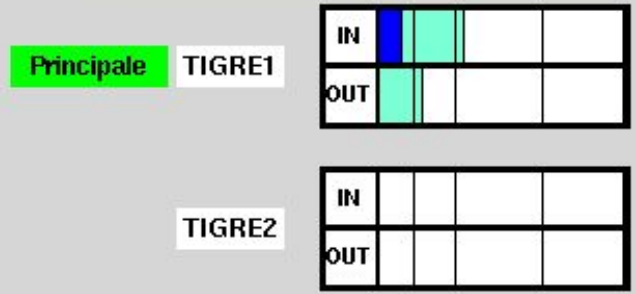
CPU Routeur : 10%
 CPU GEO : 0%
 Occup Var : 33%
 Paquets Perdus GEO SPAN1 : 0%%
 Paquets Perdus GEO SPAN2 : 0%%
 Temps Moyen d'un Cycle : 0.4 s



IN	OUT	Occupation Réseau SNMP
IN	OUT	
=0	<25	Occupation Réseau Calculé
	<50	Nombre de Flux
	>75	
 Seuil du Gyrophare a 60%		



IN	OUT	Occupation Réseau SNMP
IN	OUT	Occupation Multicast
=0	<25	Erreurs
	>75	



Cartouche d'informations générales



CPU Routeur : 7%

CPU GEO : 0%

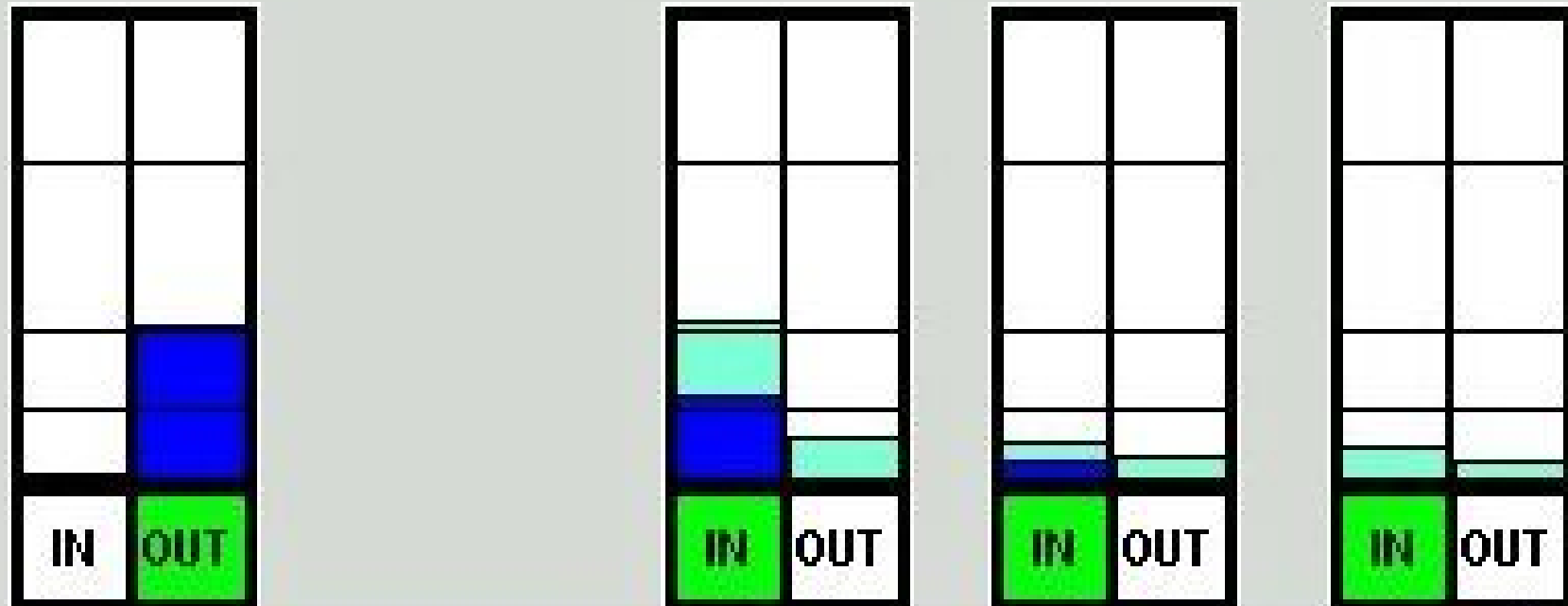
Occup /var : 13 %

Paquets Perdus GEO SPAN1 : 0%%

Paquets Perdus GEO SPAN2 : 0%%

Temps Moyen d'un Cycle : 0.1 s

Un échange entre 2 laboratoires




```
Debit : - (0) 0.0.0.0 -> 0.0.0.0 (0 bits)
Debit : TCP (22) 147.173.3.16 -> 147.173.69.2 (1752000 bits)
Flux : (Nombre : 0) 0.0.0.0 -> 0.0.0.0
Flux : (Nombre : 1) 147.173.1.26 -> 147.173.84.60
```

IN

OUT

Cartouche rappelant la signification des couleurs



The legend is contained within a light yellow rectangular box with a thin black border. It features a grid of colored boxes on the left and corresponding text labels on the right. The grid consists of three rows and five columns. The first row has two boxes labeled 'IN' and 'OUT' in cyan. The second row has two boxes labeled 'IN' and 'OUT' in blue. The third row has five boxes: a white box with '=0', a green box with '<25', a yellow box with '<50', an orange box with '<75', and a red box with '>75'. Below the first box of the third row is a small brown shield icon. To the right of the grid, the text labels are: 'Occupation Réseau SNMP' (aligned with the cyan boxes), 'Occupation Réseau Calculé' (aligned with the blue boxes), and 'Nombre de Flux' (aligned with the third row). At the bottom of the legend, the text 'Seuil du Gyrophare à 60%' is displayed.

IN	OUT				Occupation Réseau SNMP
IN	OUT				Occupation Réseau Calculé
=0	<25	<50	<75	>75	Nombre de Flux

Seuil du Gyrophare à 60%

Partie connexion au réseau MetroNet



Principale TIGRE1

IN	IN	OUT		
OUT	IN			

TIGRE2

IN				
OUT				

Evolution

Replication sur une autre machine dédiée,
qui compléterait GEO.

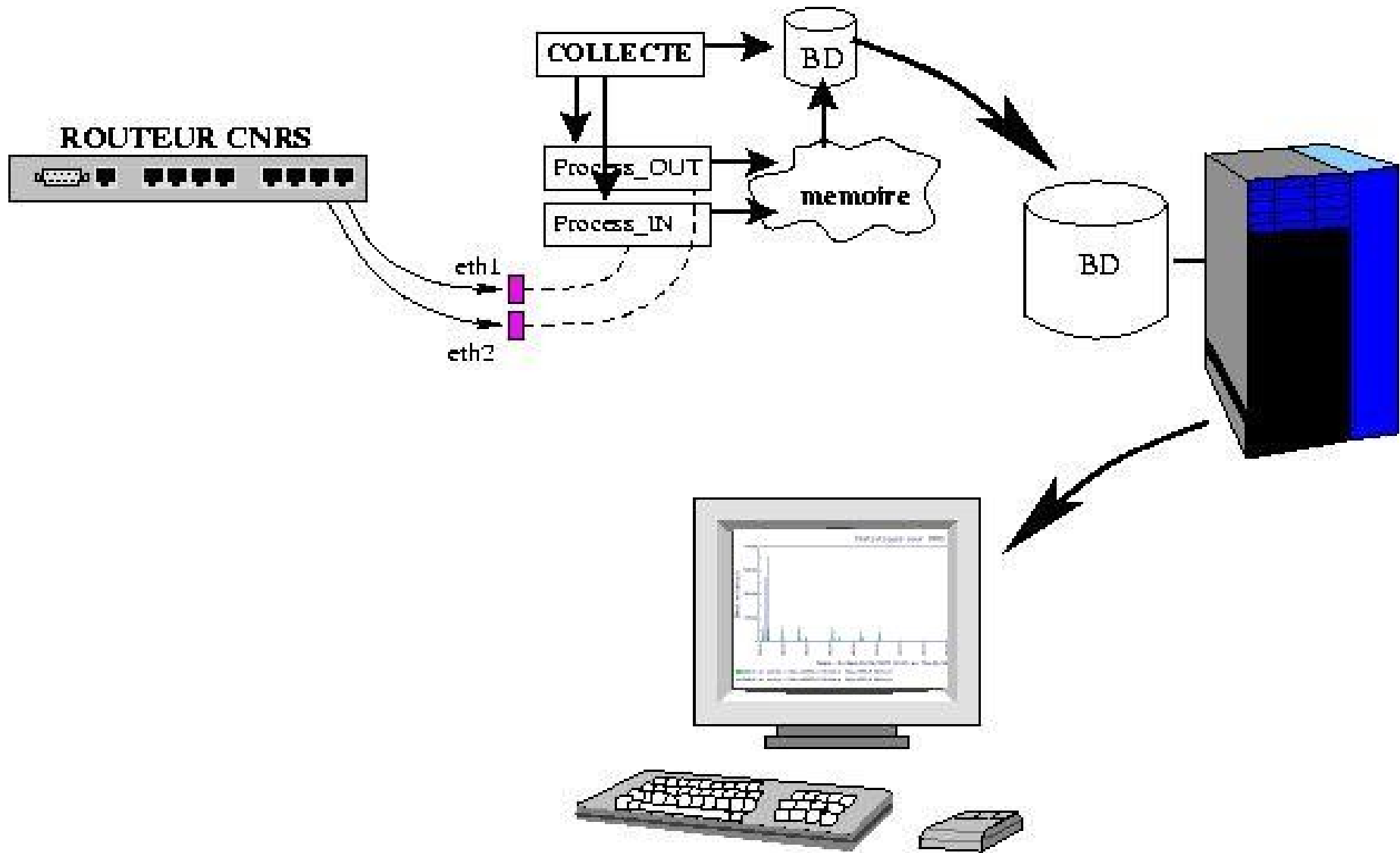
-> observation du trafic sur la durée

-> possibilité a posteriori :

.stats dynamiques (affichage)

.traces pour problèmes jour(s) précédent(s)

.détection P2P



Evolution: le projet "accounting"

Conclusions :

Bilan très positif :

.un coup d'oeil suffit

.l'audio appréciable aussi