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

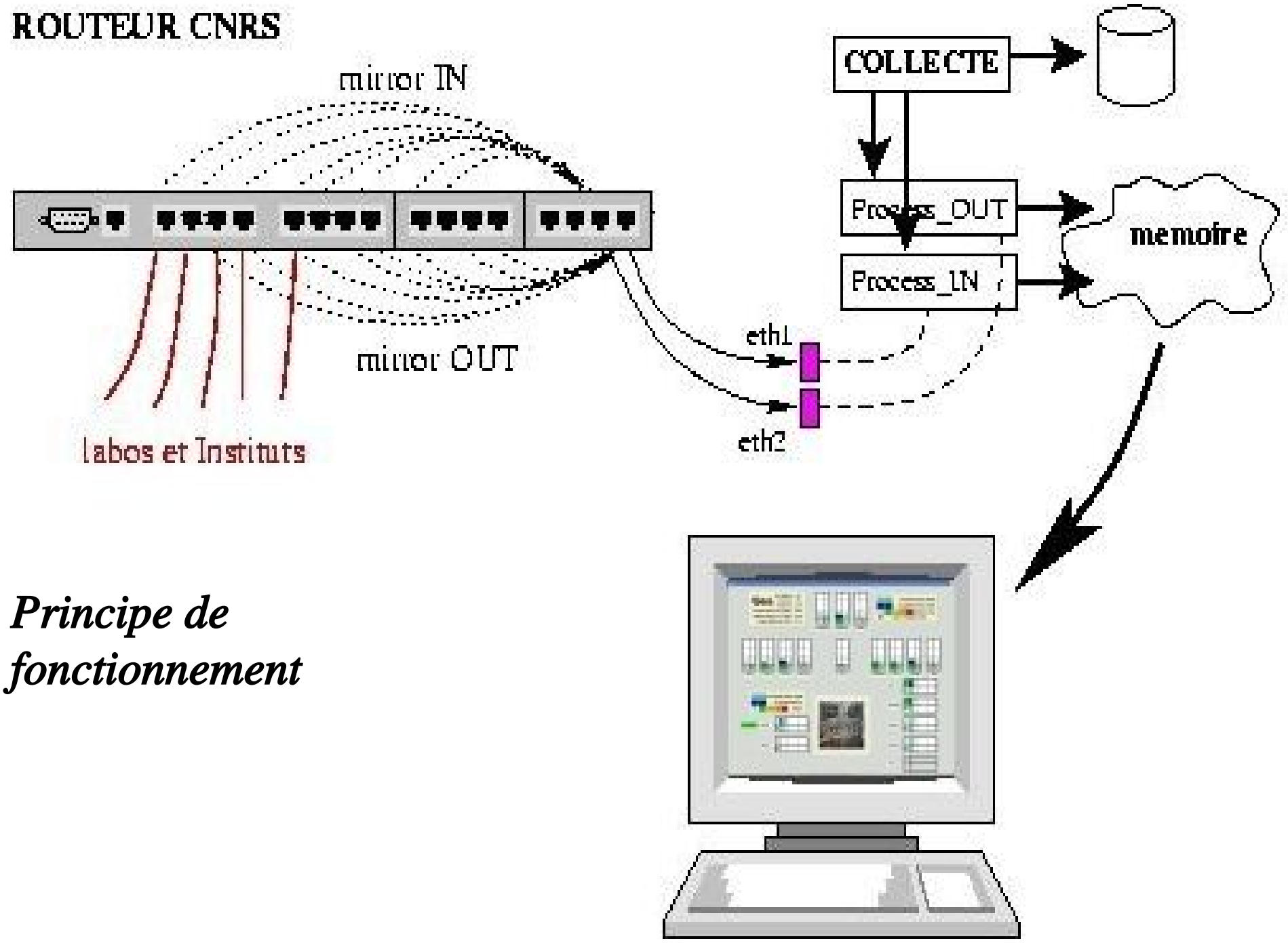
.NetFlow : seulement sur routeurs

Scinder le projet en modules :

. collecte

. mise en base données

. affichage



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 suveillance continue de l'écran.

Mise en service
en sept 2002

.2 cartes Gb

.double CPU
AMD 2800+

.2 Go RAM

GEO2

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

IN OUT Delegation
IN OUT Magistere
IN OUT Coriolis

IN OUT CRETA
IN OUT LEMD
IN OUT CRTBT
IN OUT Services
IN OUT CRIC
IN OUT LouisNeel
IN OUT LEPES
IN OUT Cristallo
IN OUT LCMI

IN OUT Occupation Réseau SNMP
IN OUT Occupation Multicast
=0 <25 <50 <75 >75 Erreurs

Principale TIGRE1
IN OUT

TIGRE2
IN OUT

IBS
IN OUT

ENSERG
IN OUT

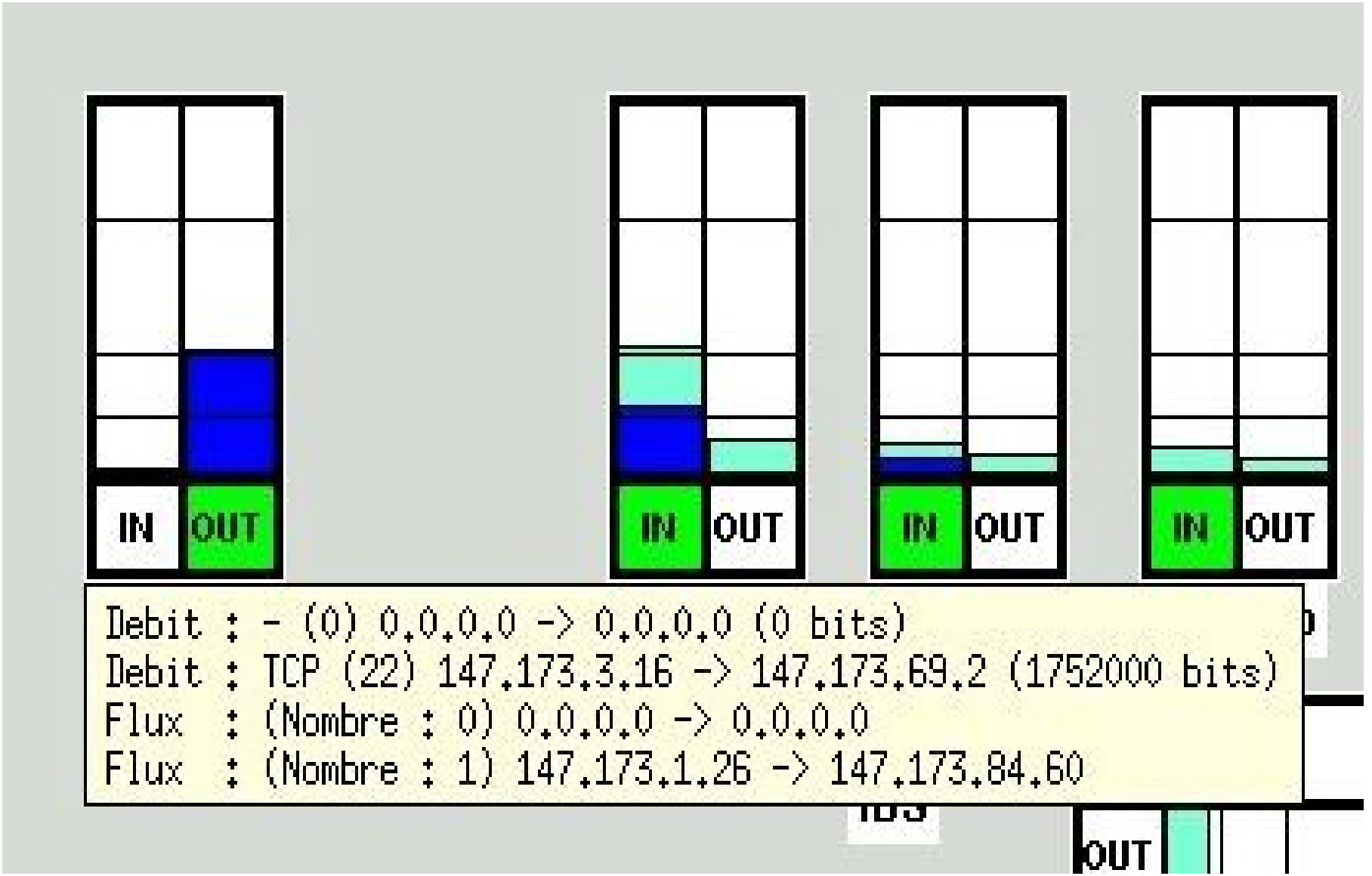
ENSPG
IN OUT

DEA/UJF
IN OUT

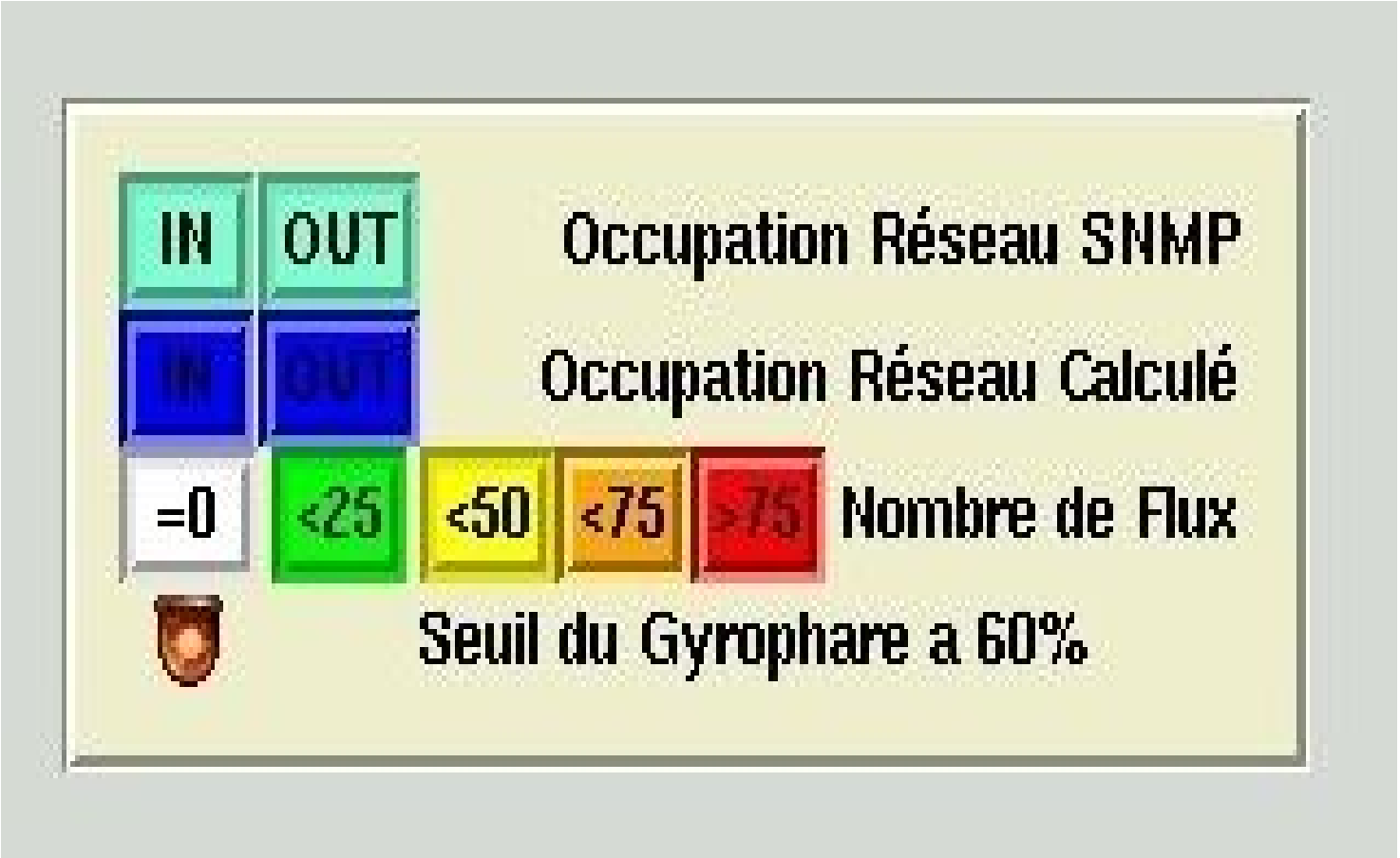
LPSC
IN OUT

Cartouche d'informations générales

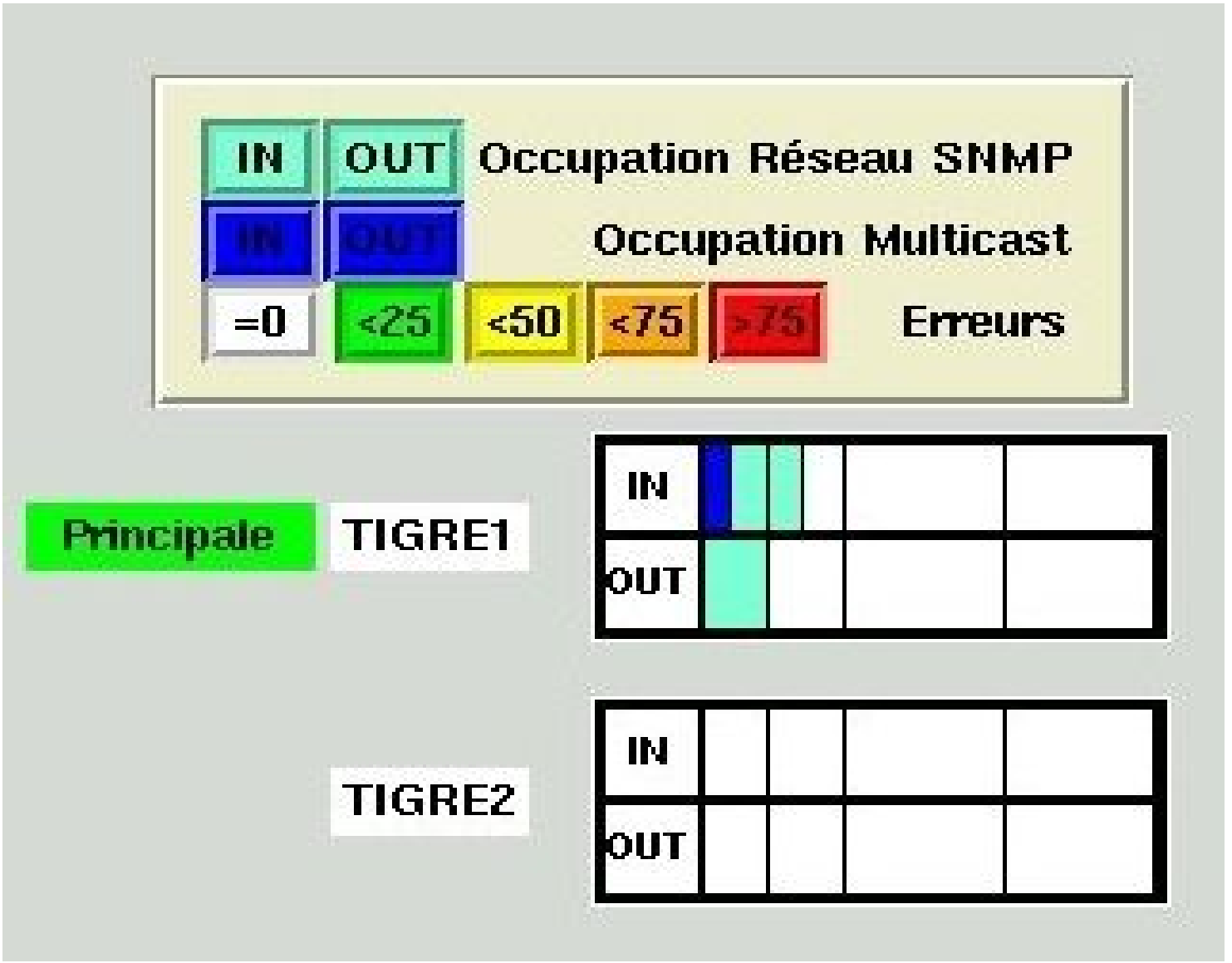
Un échange entre 2 laboratoires



Cartouche rappelant la signification des couleurs



Partie connexion au réseau MétroNet



Evolution

Replication sur une autre machine dédiée,
qui complèterait GEO.

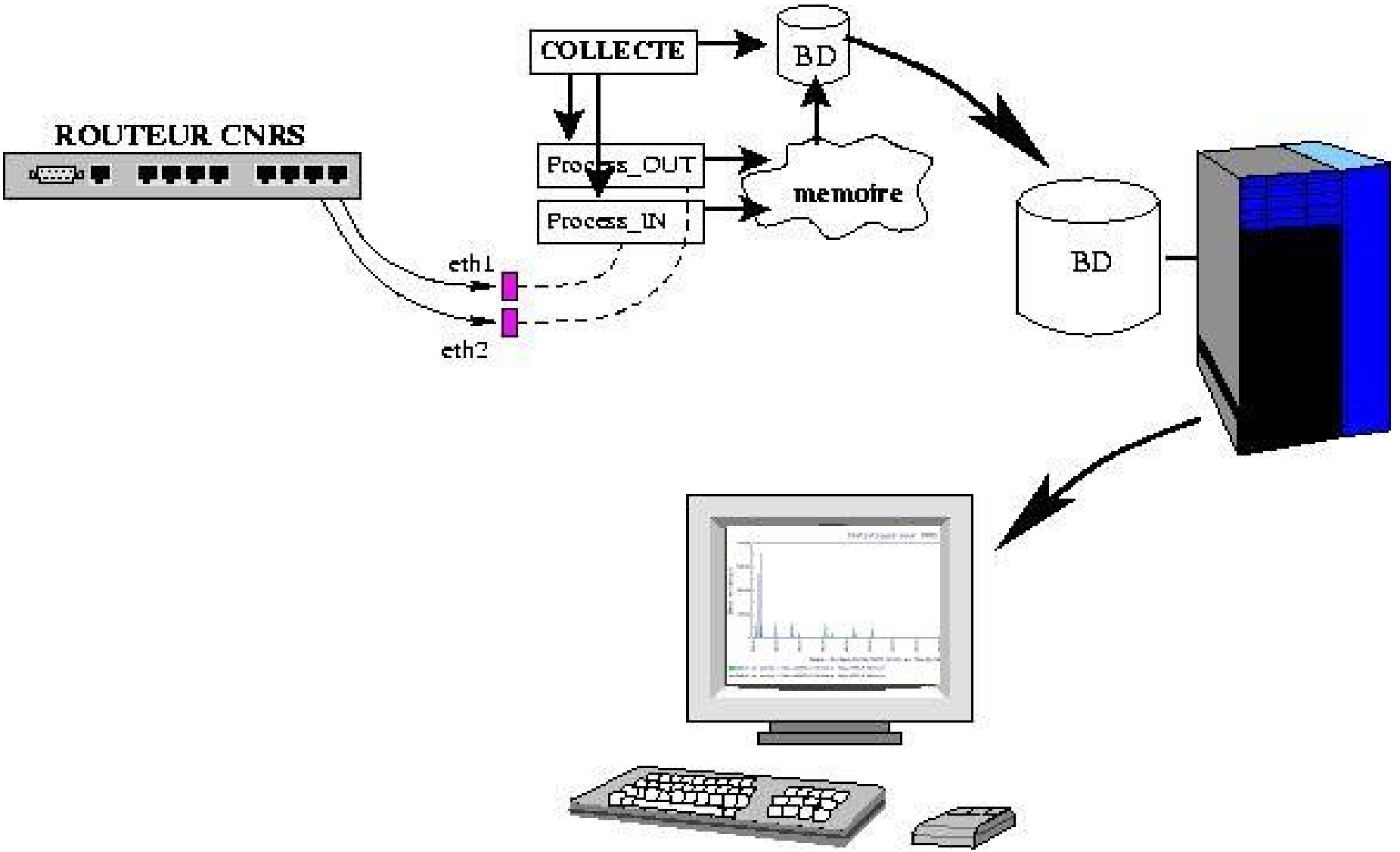
-> observation du trafic sur la durée

-> 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