Outils de collecte pour réseaux gigabit

DR

Une alternative à la technologie Cisco Netflow

david.rideau AT grenet.fr

De quoi va-t-on discuter ?

D'une "beta" Sonde

OpenSource

Pour réseaux haut-débit

Indépendante du matériel actif

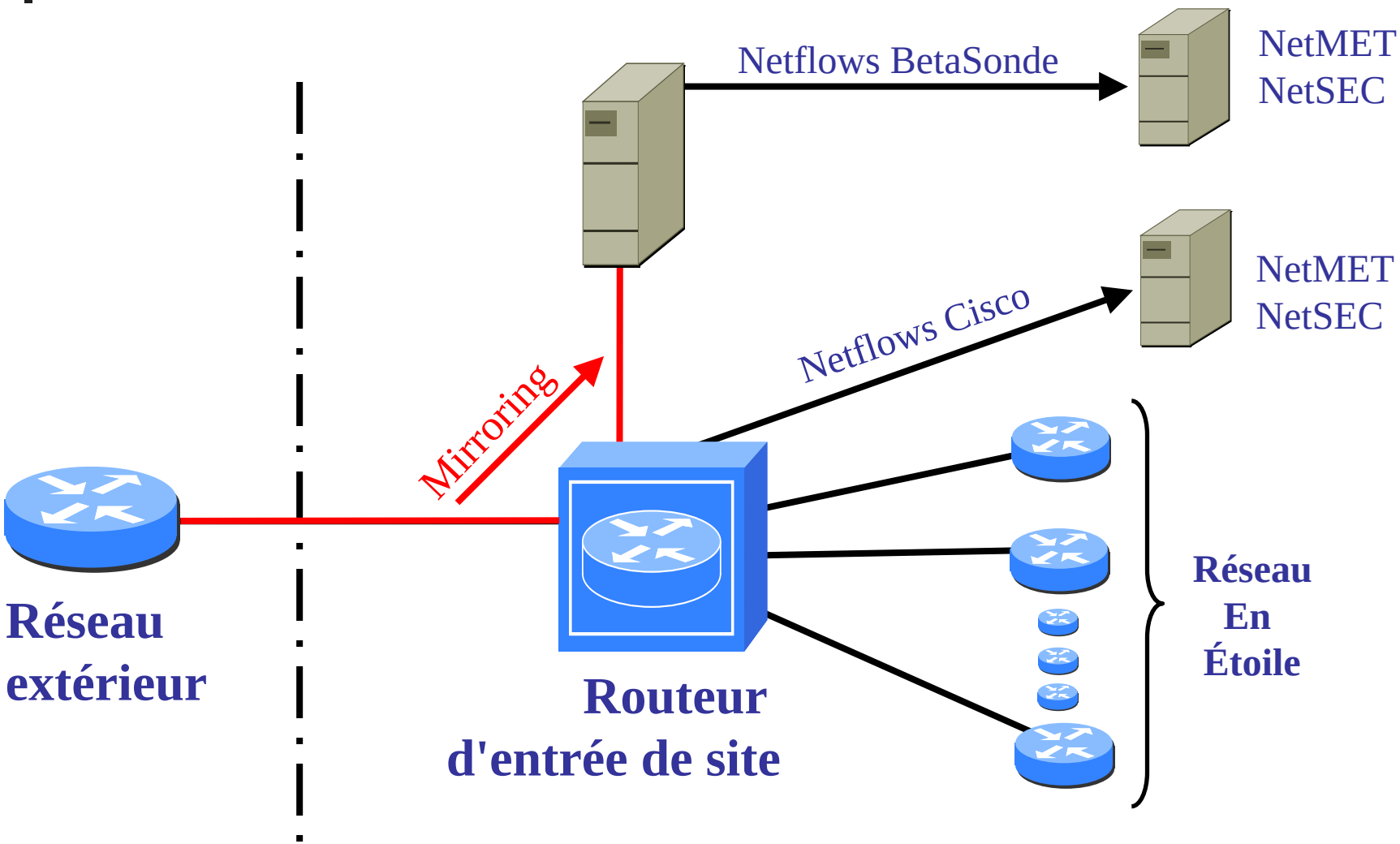
Qui génère des Netflows Cisco

Compatible avec NetMET et NetSEC

Dont le concept de "flows" pourra être exploité…

…Pour essayer de se faire pirater un peu moins :-()

Dans quel contexte ?

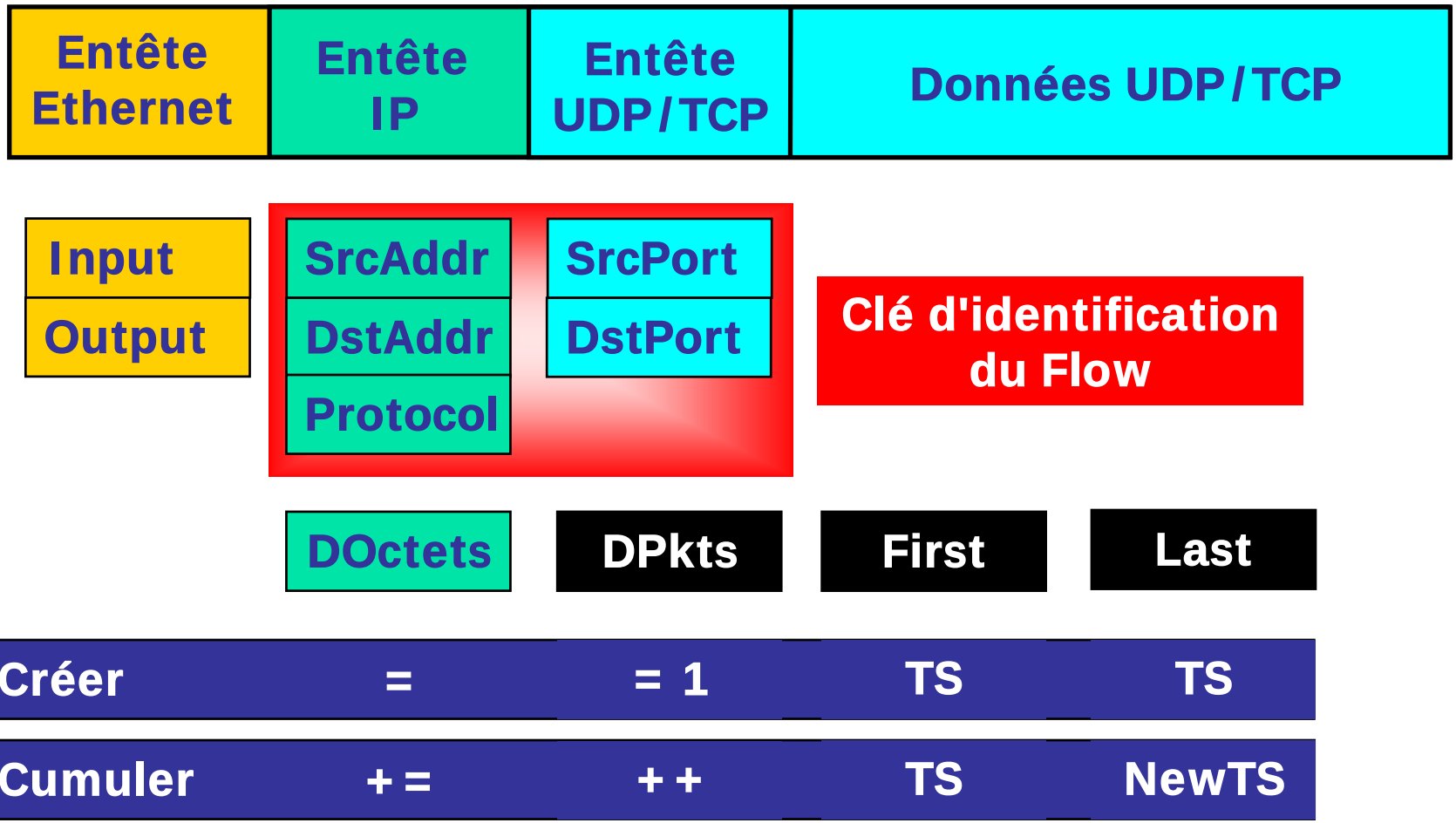


Commençons par le moins drôle...

DR

Théorèmes et Définitions

Qu'est-ce qu'un Flow ?



Qu'est-ce qu'un Netflow V5 ?

Un Netflow est un datagramme UDP

Entête de Netflow V5 = 24 octets

Version	Count	SysUptime	UnixSecs	UnixNSecs
FlowSequence		Reserved		

30 flows de 48 octets dans le corps du Netflow

SrcAddr		DstAddr			NextHop		Input	Output		
DPkts		DOctets			First		Last			
SrcPort	DstPort	pad1	flag	Prot	Tos	SrcAS	DstAS	Src mask	Dst mask	Pad2

24 + 30 x 48 = 1464 octets de données

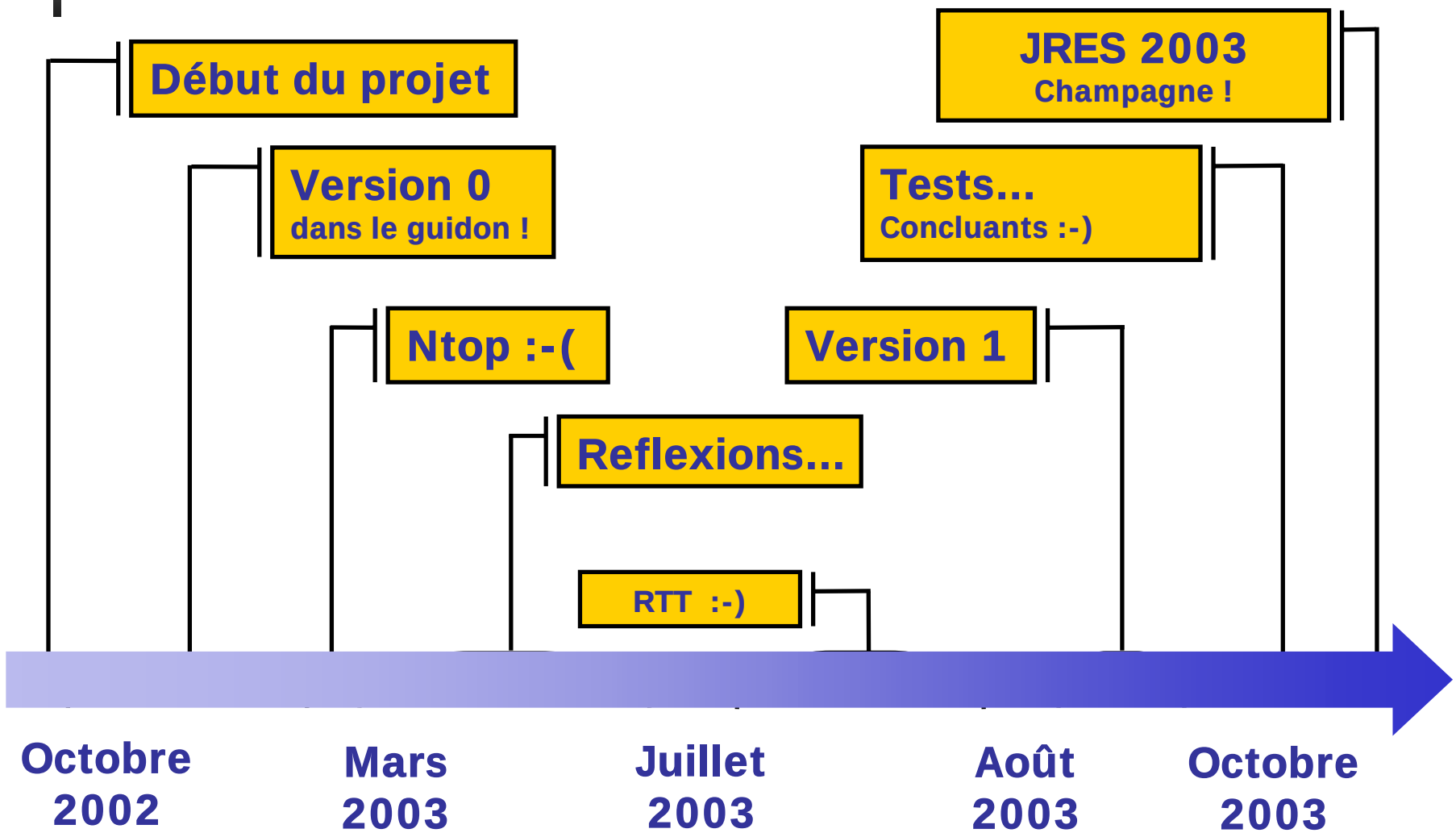
+ 8 (entête UDP)

+ 20 (entête IP)

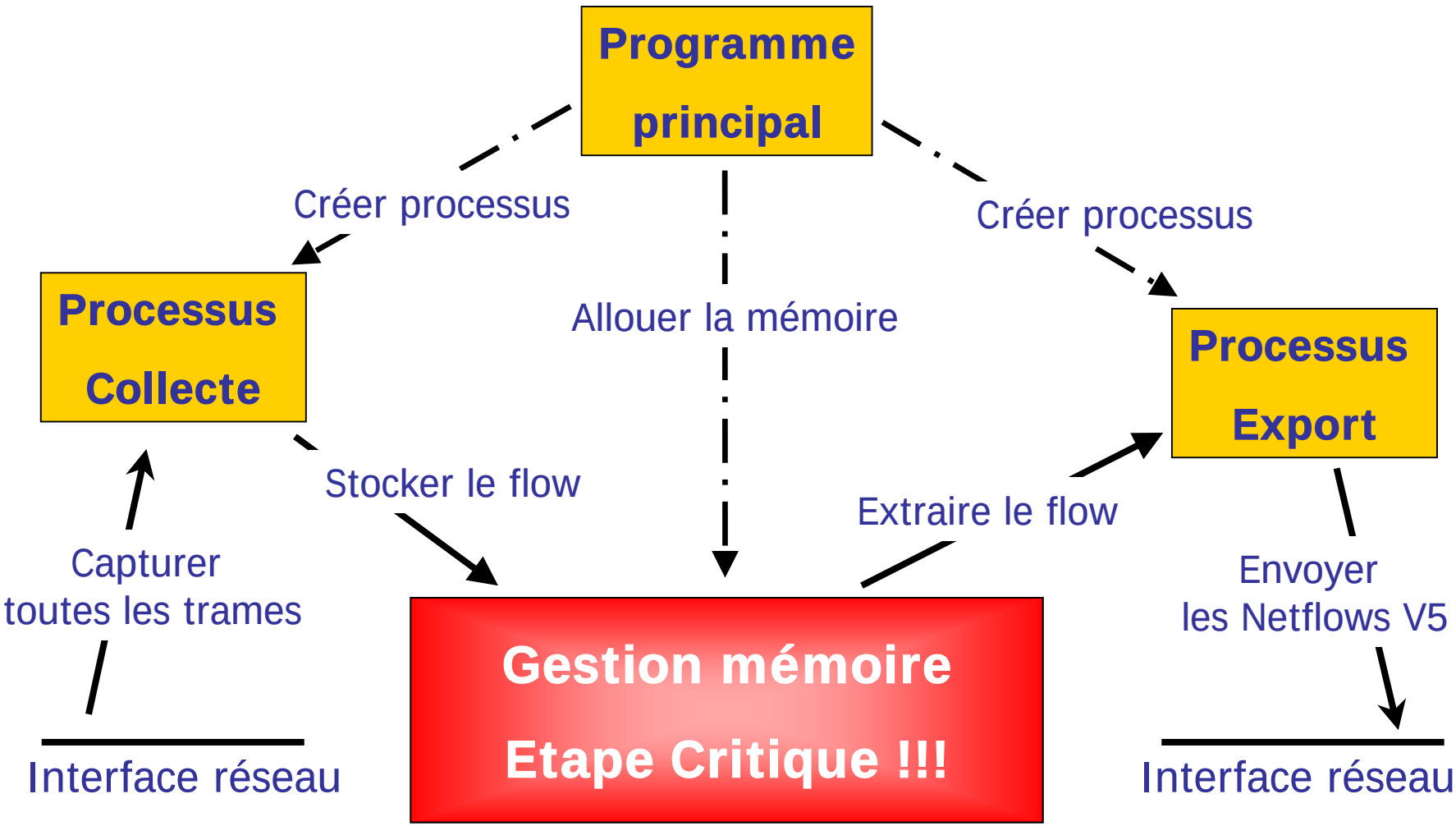
= 1492 octets inférieur à 1500 (MTU ethernet)

c'est l'Amérique :-)

Du concept à la Version "beta"

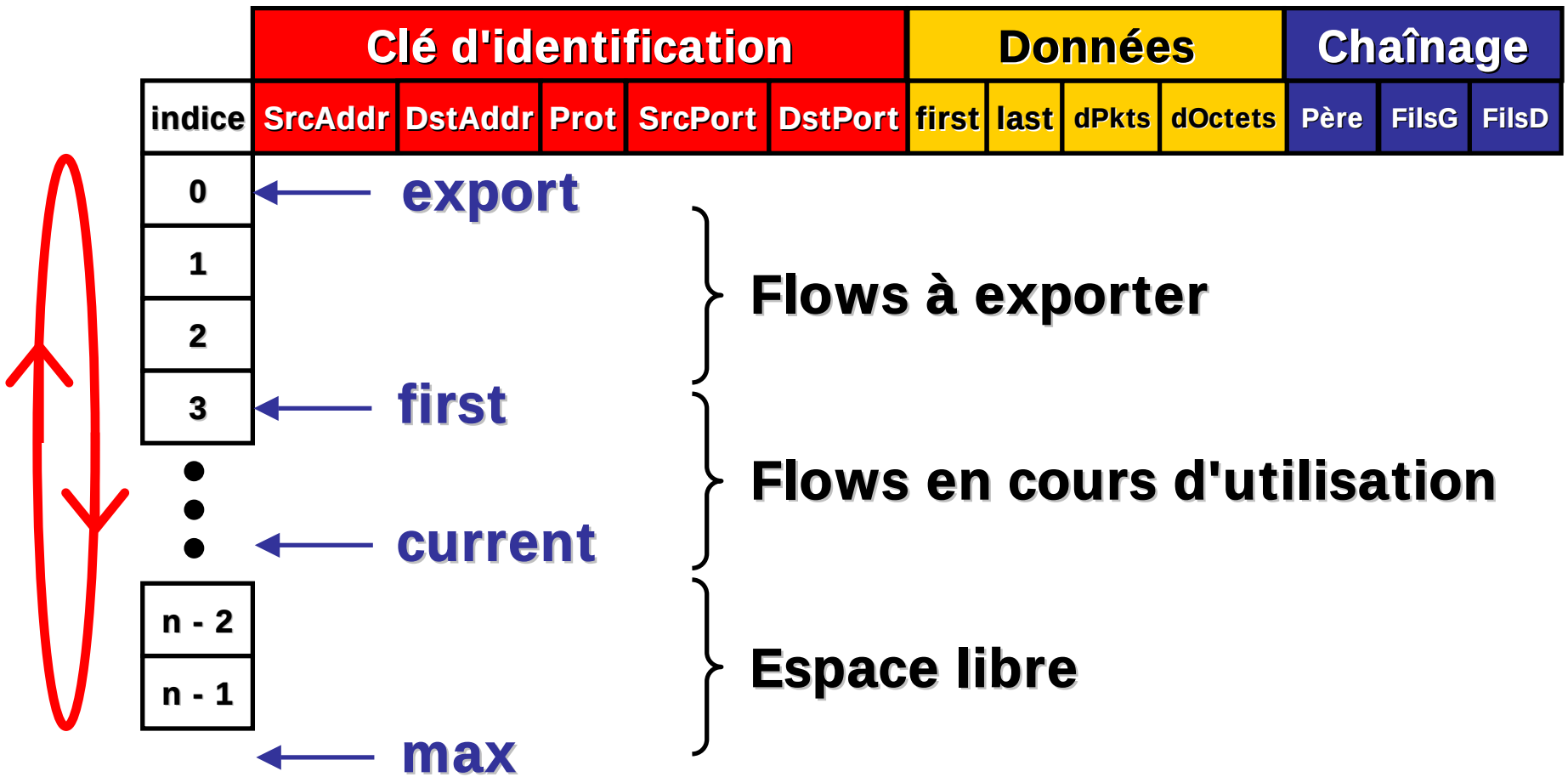


La Version beta

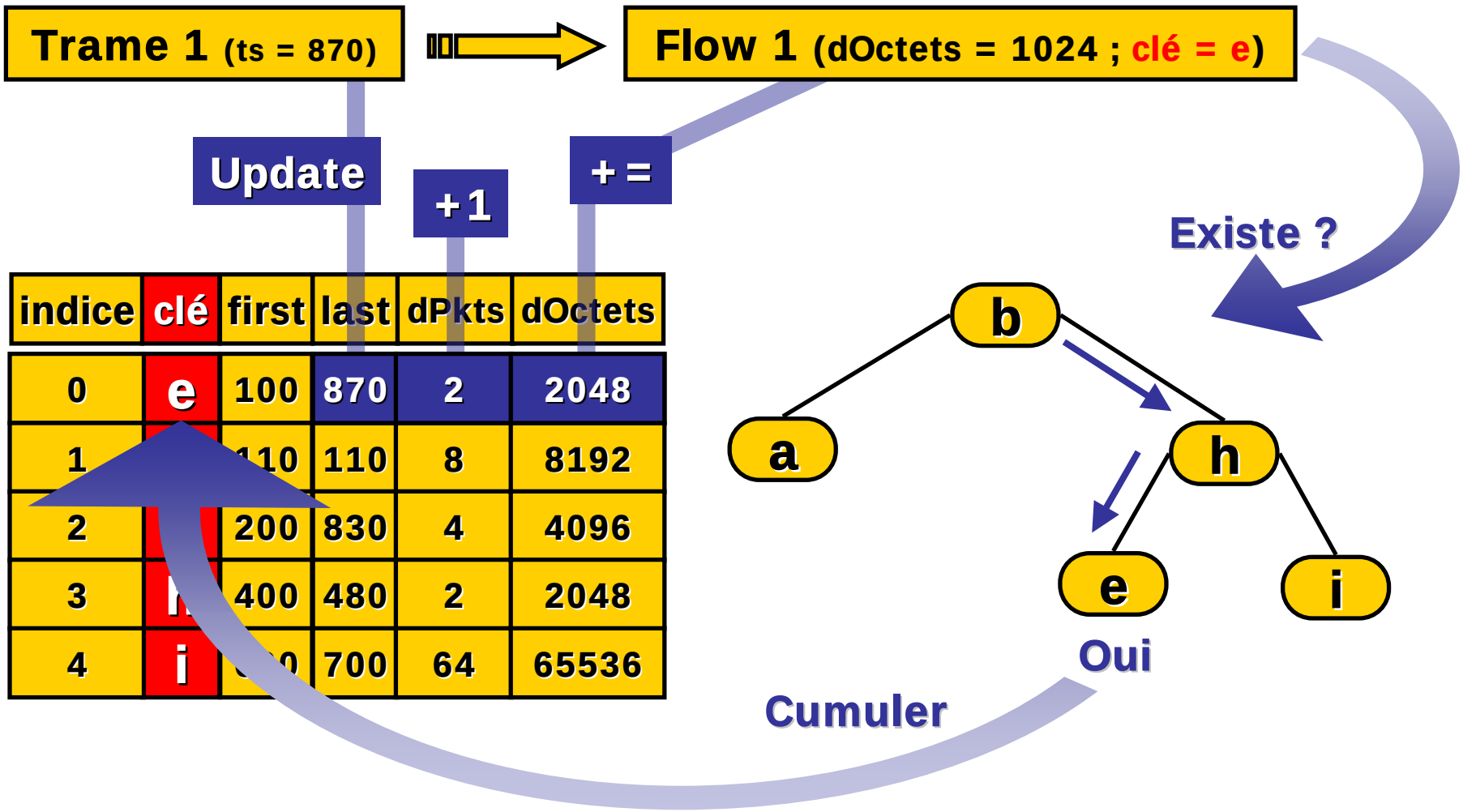


Le mot d'ordre : efficacité

Allocation dynamique en une seule étape pour N flows



Cumuler dans un flow existant

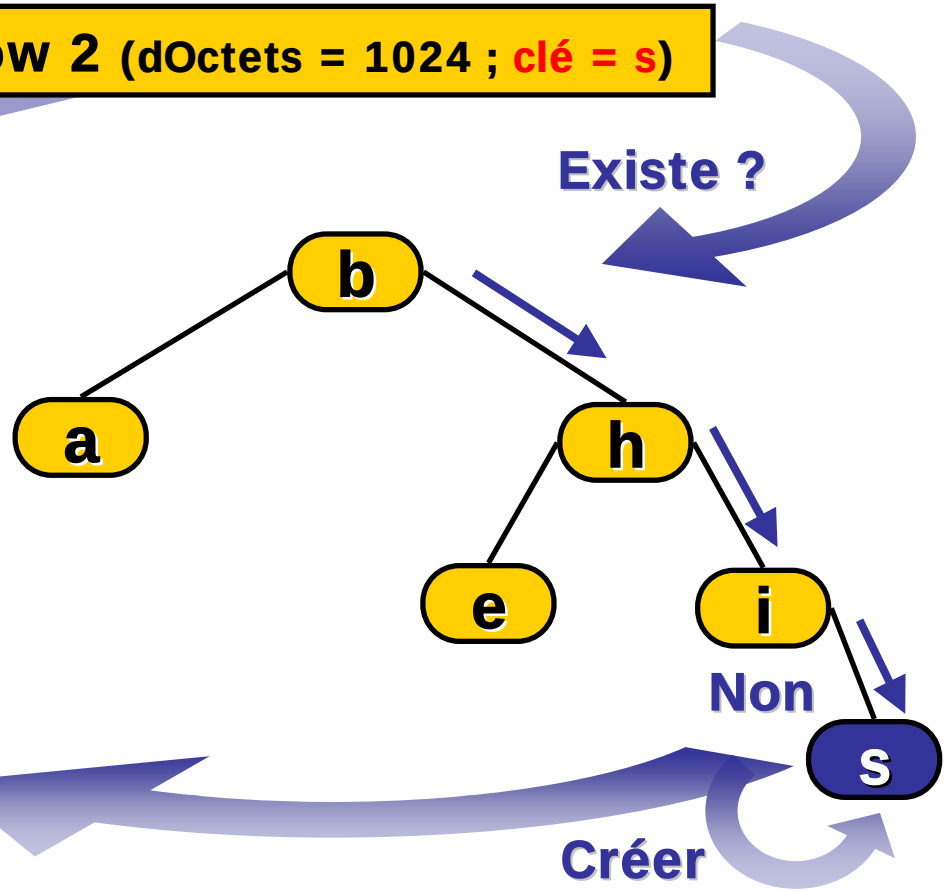


Créer un nouveau flow

Trame 1 (ts = 870) → **Flow 1** (dOctets = 1024 ; clé = e)

Trame 2 (ts = 900) → **Flow 2** (dOctets = 1024 ; clé = s)

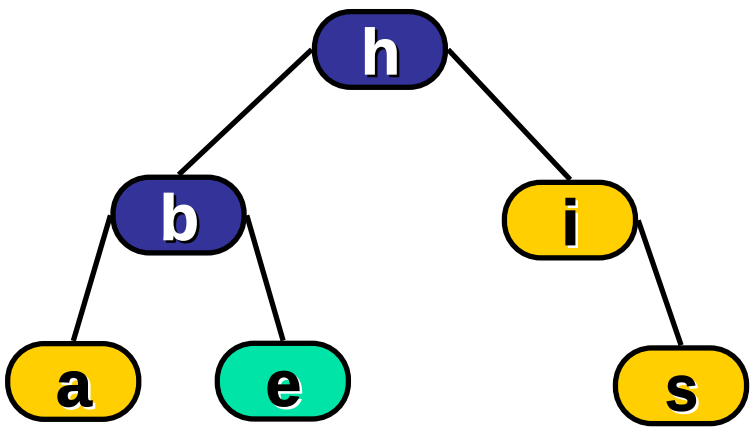
	=		=1	=	
indice	clé	first	last	dPkts	dOctets
0	e	100	870	2	2048
1	b	110	110	8	8192
2	a	200	830	4	4096
3	h	400	480	2	2048
4	i	600	700	64	65536
5	s	900	900	1	1024



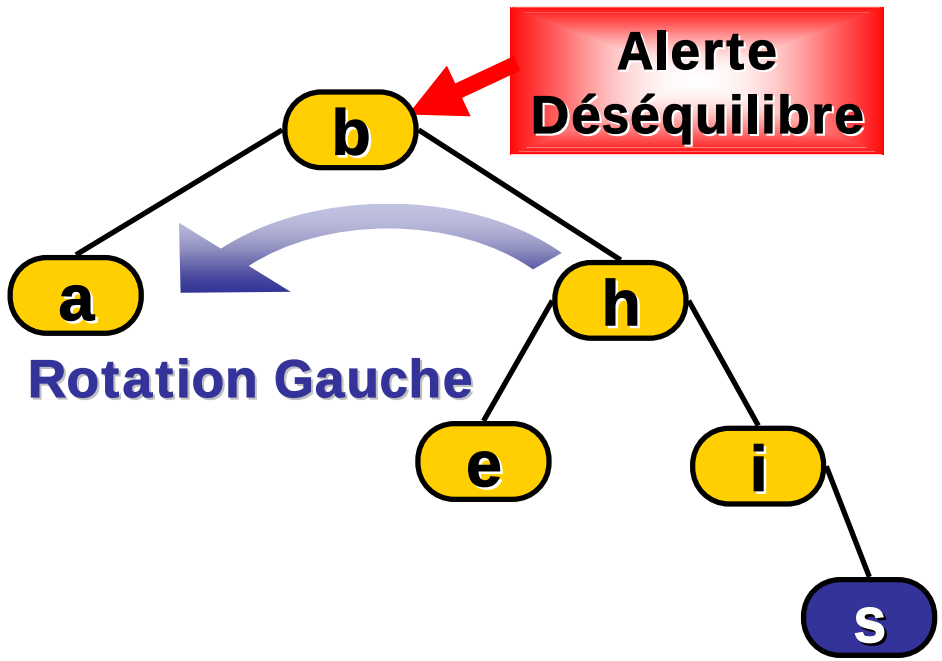
Equilibrer l'arbre binaire

Trame 1 (ts = 870) → **Flow 1** (dOctets = 1024 ; clé = e)

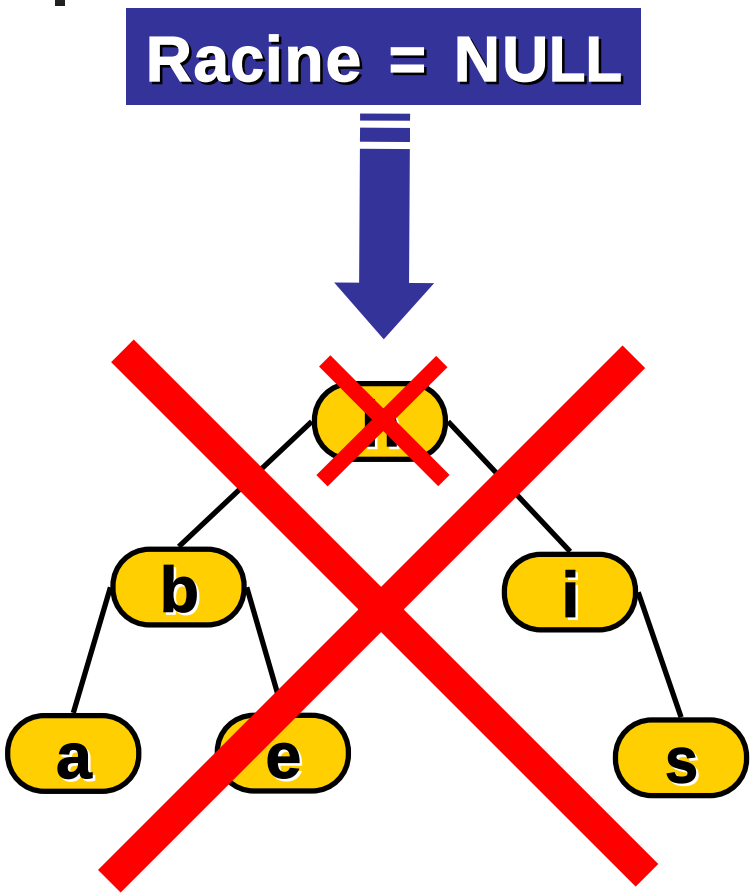
Trame 2 (ts = 900) → **Flow 2** (dOctets = 1024 ; clé = s)



Arbre ré-équilibré



Exporter les flows



indice	clé	first	last	dPkts	dOctets
0	e	100	870	2	2048
1	b	110	110	8	8192
2	a	200	830	4	4096
3	h	400	480	2	2048
4	i	600	700	64	65536
5	s	900	900	1	1024
.	.	.	.	.	.
.	.	.	.	.	.

Créer nouveaux Flows ici

EXPORT

Quels résultats obtenus ?

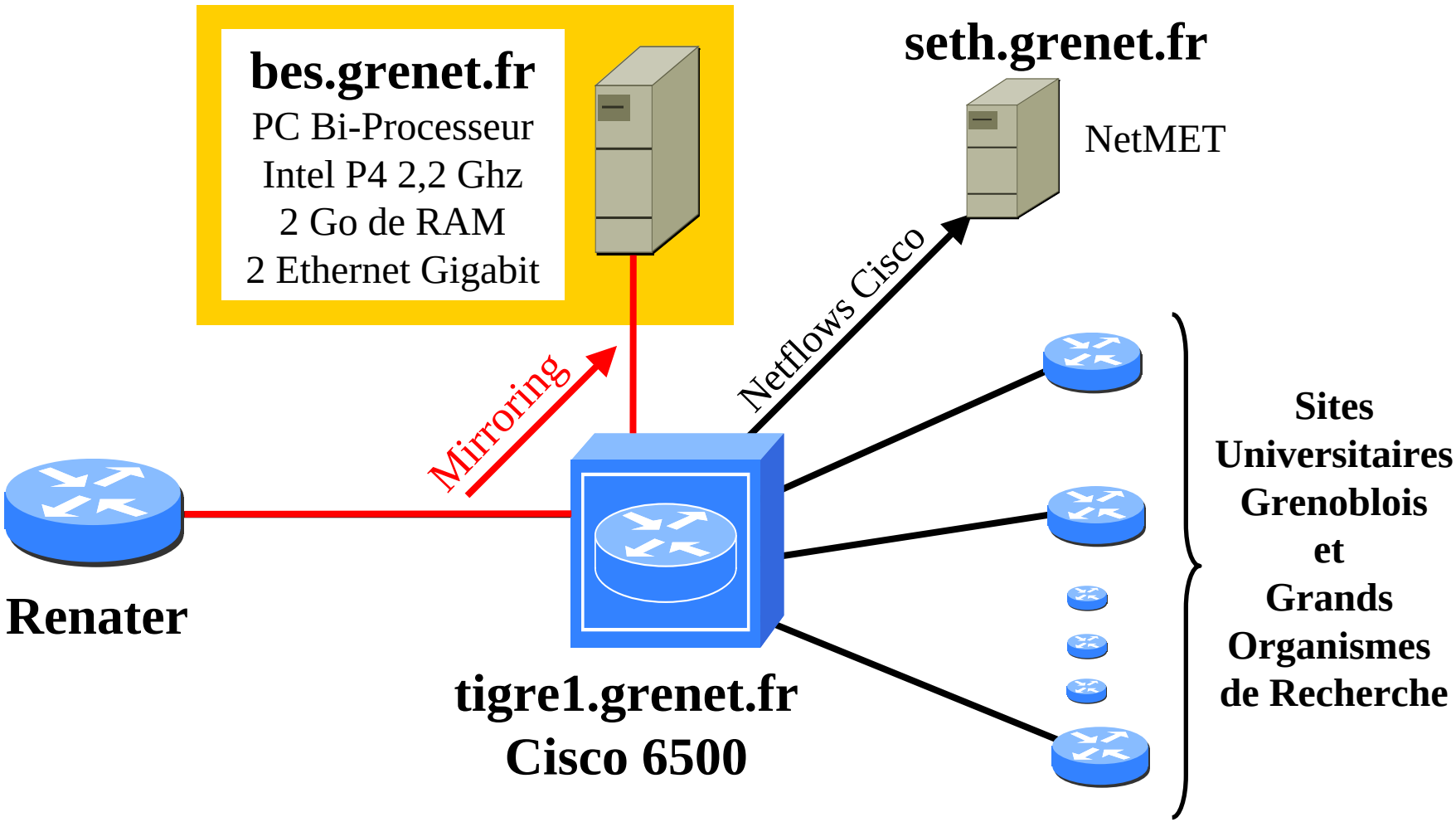
DR

Une plateforme adaptée

Quelques chiffres

Quelques graphes

Plateforme de test



Quelques chiffres sur 3 semaines

15,2 milliards de paquets traités

Dont

Soit 416 Go de moyenne par jour

2,3 milliards de flows distincts

Pour

1 Pour 29,948

76,8 millions de netflows générés

Quelques chiffres... 2/2

Débit moyen

Environ 4,6 Mo par seconde

Pic de trafic le 23/10 à 13:31:17

48774 paquets reçus, dont 47271 traités

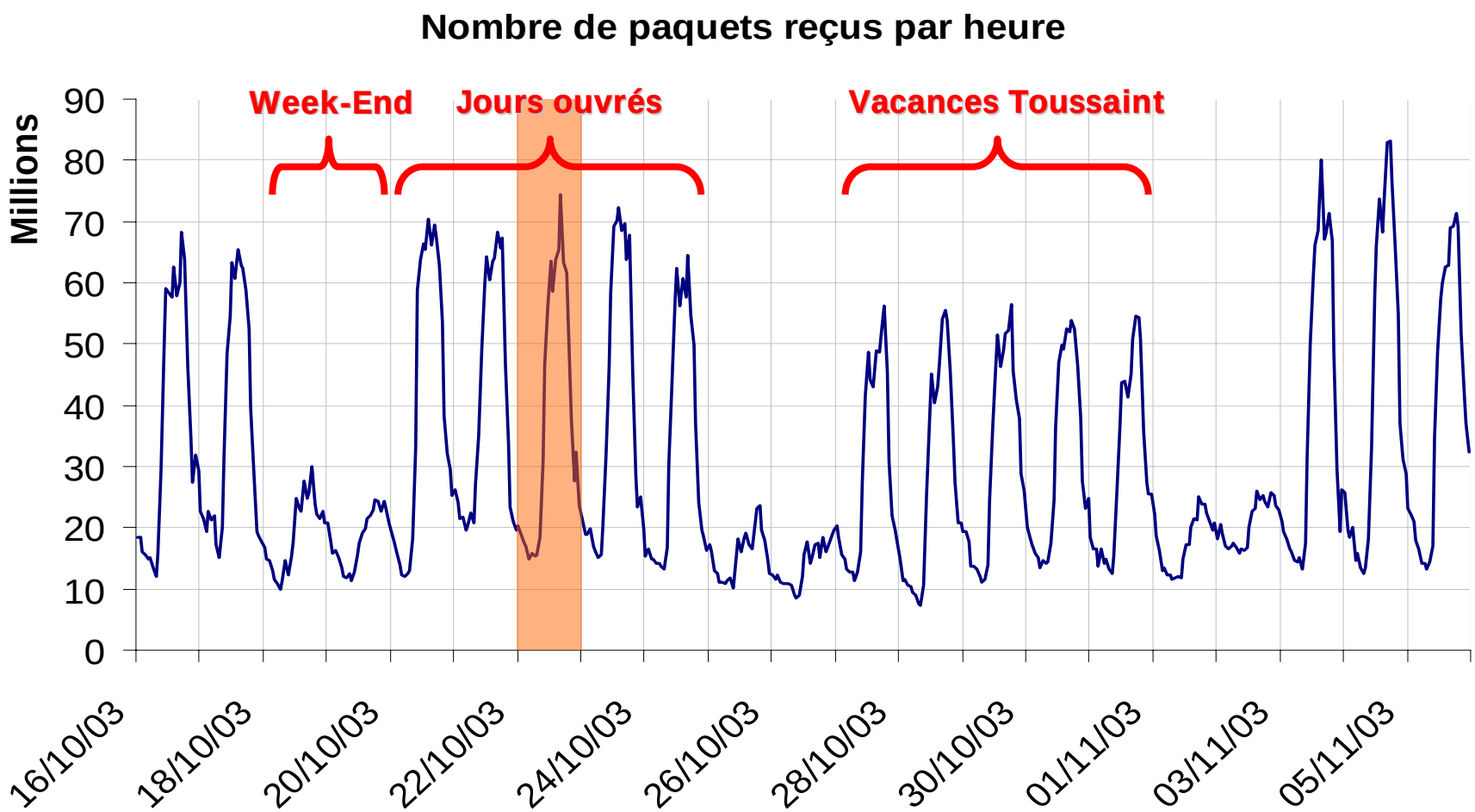
soit 29 298 589 octets en une seconde

Taux de compression

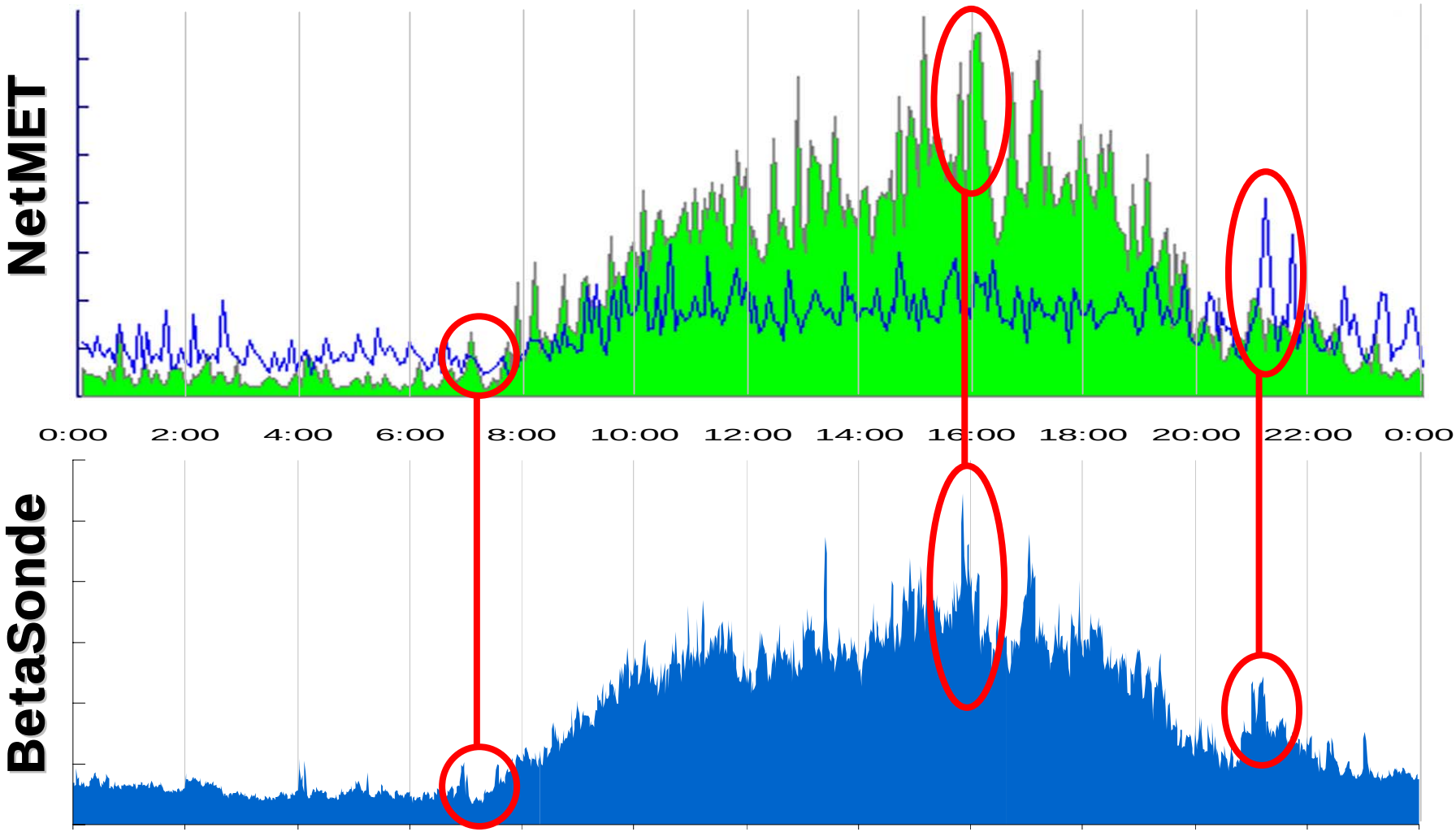
1 netflow pour 200 paquets traités

1 octet généré pour 80 traités

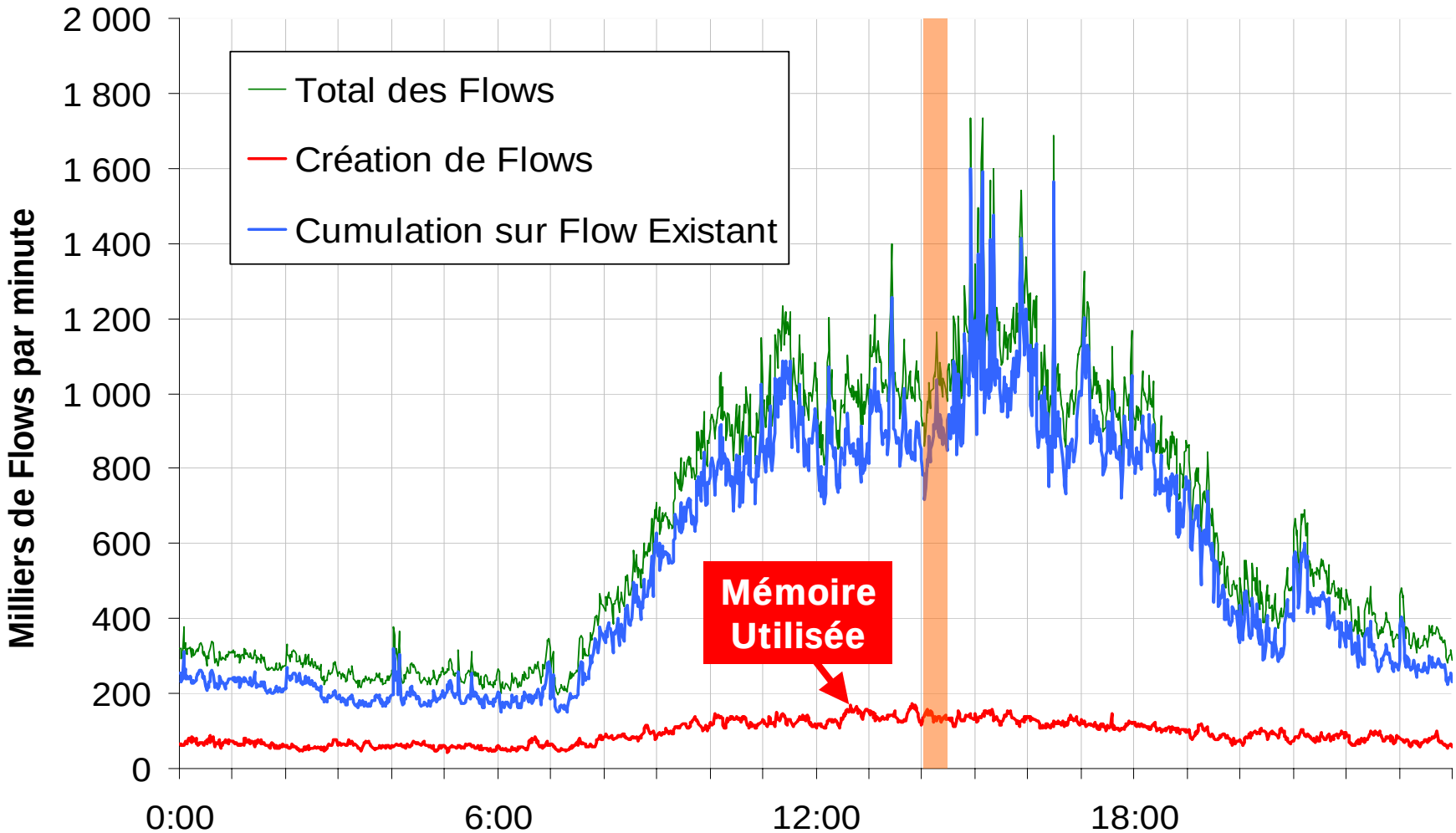
Trois semaines, 0 paquet perdu



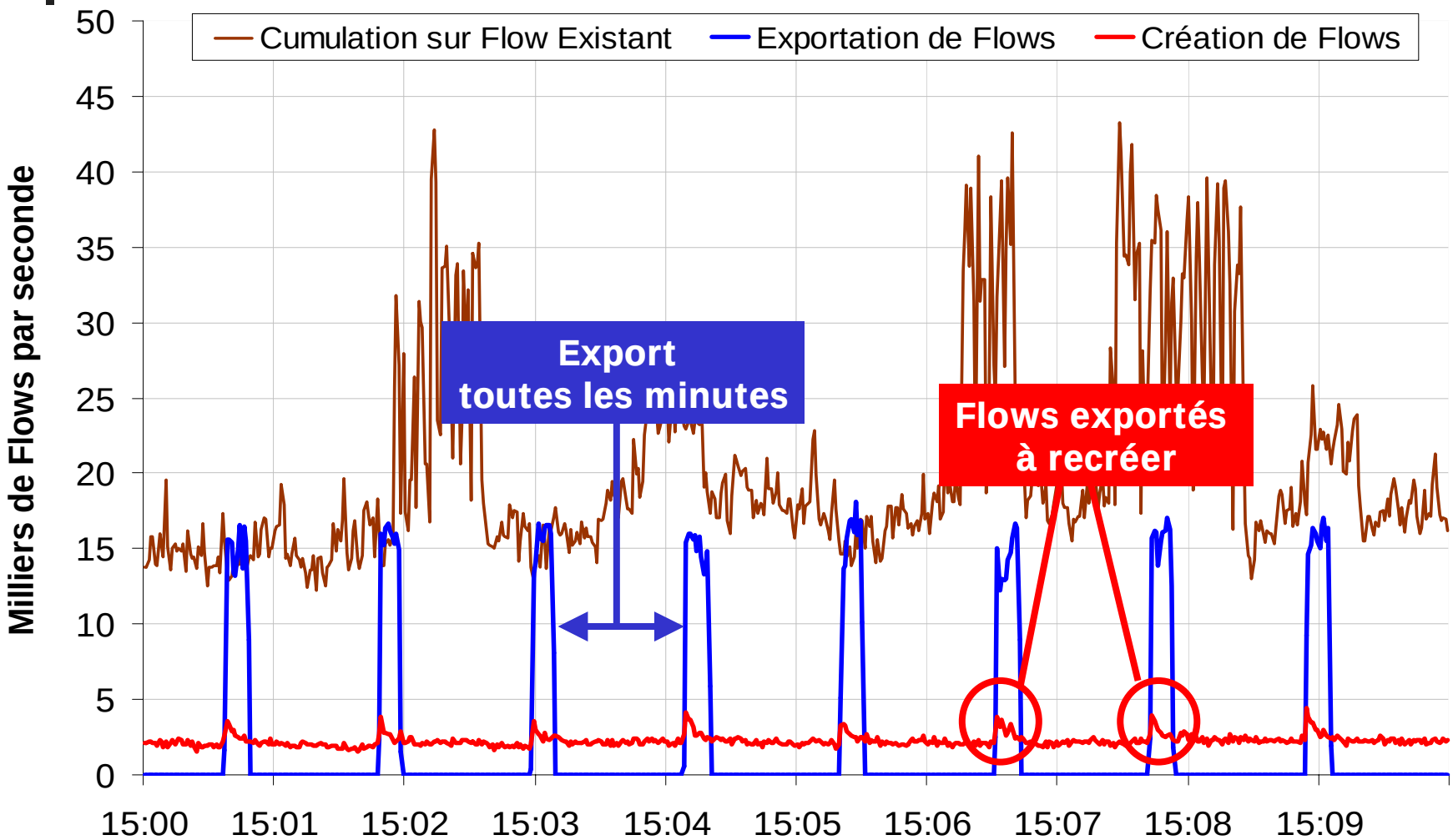
NetMET, le 22 octobre 2003



Ressources mémoires



Deux Processus asynchrones



Pour finir...

DR

Points forts, faibles

Evolutions

Détection de scan

Quels avantages ?

- **Métrologie indépendante**
- **Économie de CPU du routeur**
- **Sélection du trafic (libpcap)**
- **Packaging avec NetSEC sans netflow**

Quels inconvénients ?

- **Besoin d'un commutateur (mirroring)**
- **Qualification des flows TCP**

Demain

- **Paramétrage du programme**
- **Évolution de protocoles**
- **Interface Homme-Machine**
- **Filtrage libpcap**
- **Spécification modulaire**

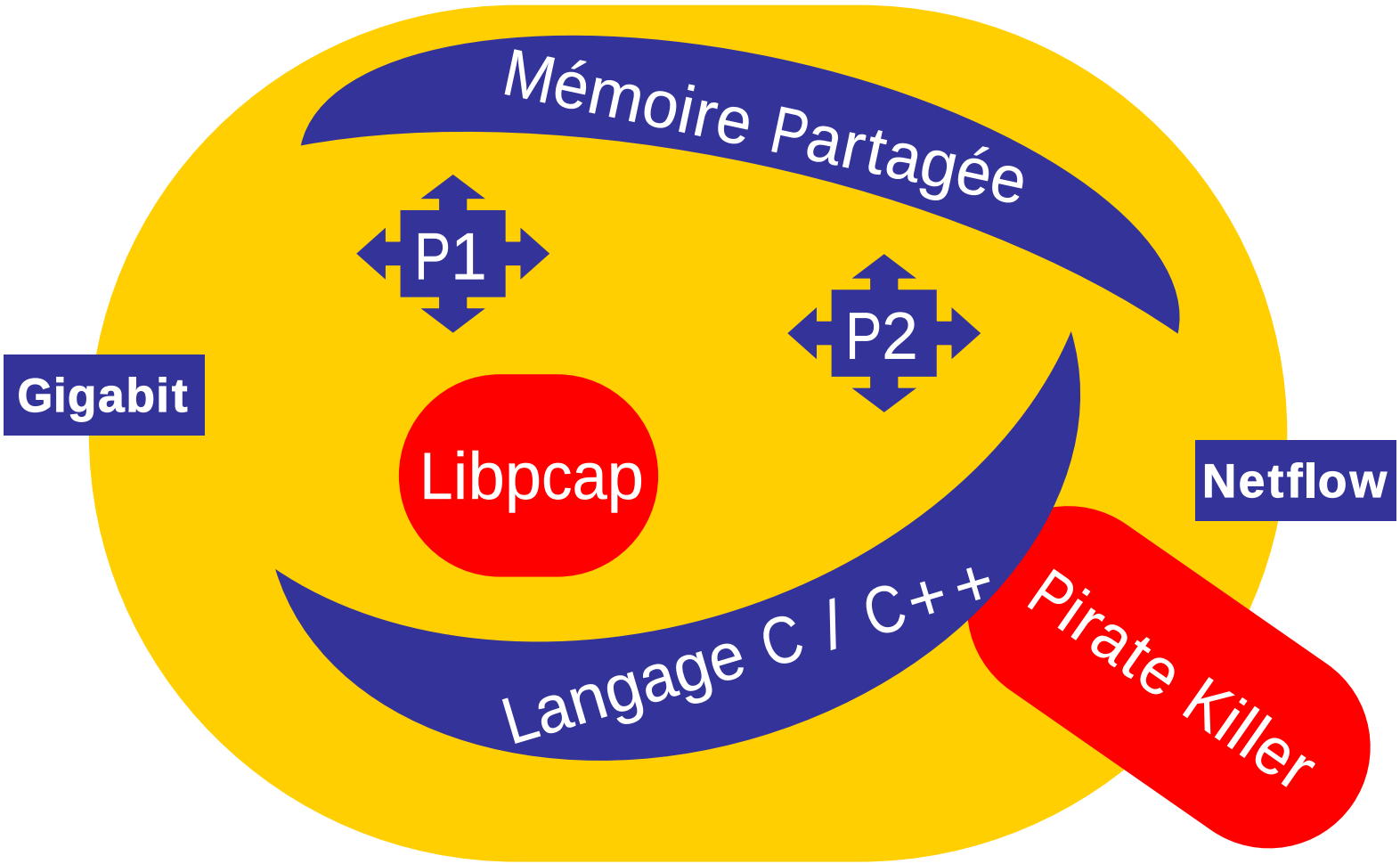
Détecter un scan : facile !

- **Des flows triés par adresse IP**
- **Isoler une provenance commune**
- **Fixer un seuil d'alerte**
- **Conserver les flux suffisamment longtemps (scans lents)**

Bloquer un scan : plus difficile ?

- **Alerter l'administrateur réseau**
- **Agir sur le routeur d'entrée de site**
- **Temps de réaction**
- **Bloquer l'attaque à venir**

Plateforme Linux OpenSource



Questions

Outils de collecte pour réseaux gigabit

DR

Une alternative à la technologie Cisco Netflow

david.rideau@grenet.fr