

Fiabilisation d'une architecture DNS

Philippe PEGON

Philippe.Pegon@crc.u-strasbg.fr

Centre Réseau Communication



1. Introduction

2. Pourquoi faire évoluer l'architecture DNS ?

3. Principe de la nouvelle architecture DNS

4. VRRP

5. Mise en œuvre

6. Conclusion

Introduction (1)

- Le réseau Osiris en quelques chiffres
 - créé en 1989
 - 15 établissements
 - près de 60 000 utilisateurs
 - plus de 120 bâtiments
- 2 équipes
 - équipe réseau (6 ingénieurs, 3 techniciens)
 - équipe téléphone (3 techniciens, 6 standardistes)
 - + 1 directeur et 1 secrétaire

Introduction (2)

- Applications de plus en plus dépendantes du réseau
- Objectif politique pour Osiris
 - 99,9 % de disponibilité réseau
 - soit environ 4 heures d'indisponibilité par an
- ⇒ Osiris 2
 - redondance optique
 - sécurisation environnementale
 - renouvellement des serveurs et équipements actifs
 - évolution des services et de ***l'architecture DNS***

1. Introduction
2. Pourquoi faire évoluer l'architecture DNS ?
3. Principe de la nouvelle architecture DNS
4. VRRP
5. Mise en œuvre
6. Conclusion

Pourquoi faire évoluer l'archi DNS ?

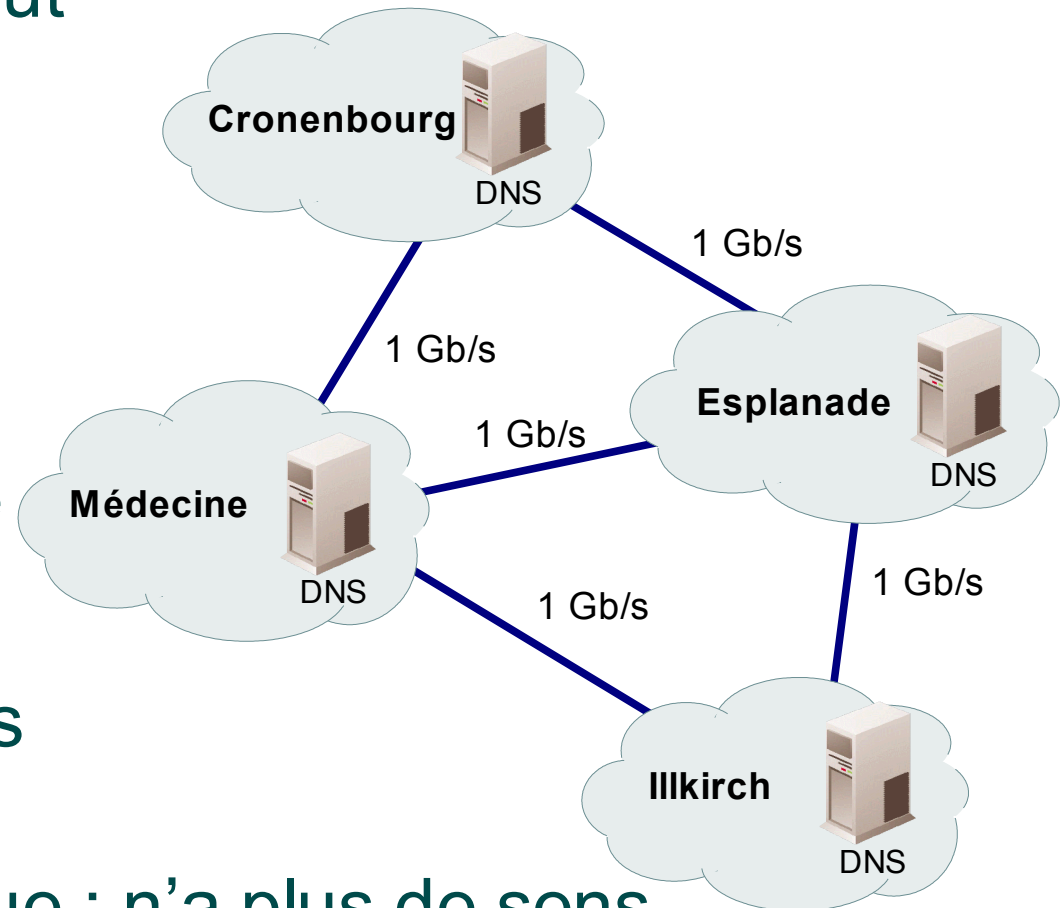
- Service DNS :
 - crucial
- Exemple
 - le réseau fonctionne
 - le serveur DNS ne fonctionne pas



« Le réseau est cassé » !

Architecture Osiris

- Basée sur des LS début des années 90
 - Architecture DNS distribuée
 - 1 serveur par grand campus
 - Proximité géographique
 - Liens Giga en 2003
 - Liens Giga redondants en 2003/2004
- ⇒ proximité géographique : n'a plus de sens



1. Introduction
2. Pourquoi faire évoluer l'architecture DNS ?
3. Principe de la nouvelle architecture DNS
4. VRRP
5. Mise en œuvre
6. Conclusion

Nouvelle architecture DNS (1)

- Configuration de plusieurs DNS dans les résolveurs non satisfaisante
 - timeout de 4 secondes sous FreeBSD
 - timeout de 2 secondes sous Windows
 - beaucoup d'utilisateurs ne mettent pas de deuxième DNS dans leur configuration
- Fiabilisation d'*un* serveur DNS
 - deux serveurs redondants répartis sur Osiris
 - vus comme un seul
- Une seule adresse IP pour tout Osiris
 - Simplification de la configuration des postes clients

Nouvelle architecture DNS (2)

- 2 solutions étudiées :
- Utilisation d'un protocole de routage
 - 2 annonces pour la même adresse IP
 - comparable à l'anycast IPv6
 - les machines doivent participer au protocole de routage
 - ⇒ risque de fragilisation du réseau
- Utilisation de VRRP
 - indépendance vis-à-vis du protocole de routage
 - 2 serveurs dans un même VLAN
 - rapidité de convergence : **inférieure à 4 secondes**

1. Introduction
2. Pourquoi faire évoluer l'architecture DNS ?
3. Principe de la nouvelle architecture DNS
4. VRRP
5. Mise en œuvre
6. Conclusion

VRRP (1)

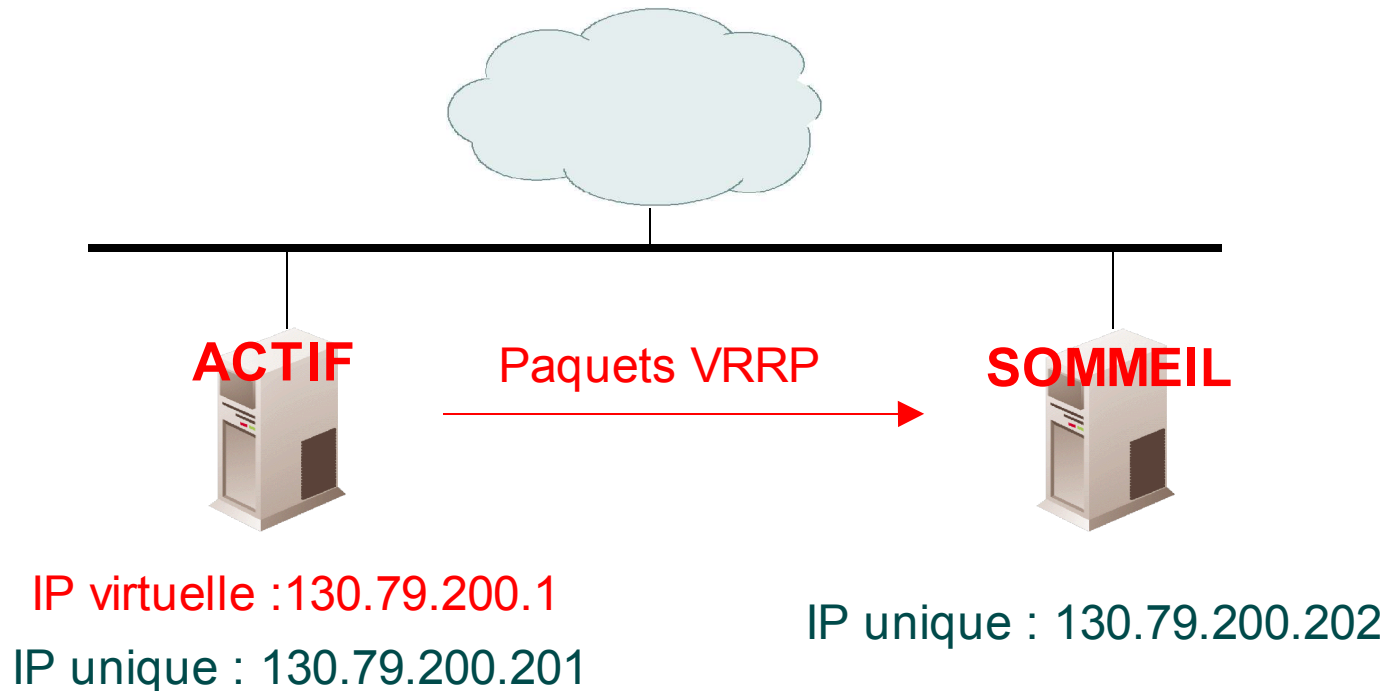
- VRRP : Virtual Router Redundancy Protocol
- Protocole issu du « monde réseau »
 - RFC 2338
- Créé à l'origine pour les routeurs
 - s'applique également à des serveurs

VRRP (2)

- Plusieurs systèmes participent à une instance
 - un **VRID**
- Chaque système possède une adresse IP unique
- Chacun partage
 - une même adresse IP dite virtuelle
 - une même adresse MAC (00:00:5E:00:01:<VRID>)
- Chaque machine a un identifiant
 - compris entre 0 et 255
 - configuré manuellement
 - le plus élevé s'approprie l'adresse IP virtuelle
- Paquets de contrôle : IP multicast

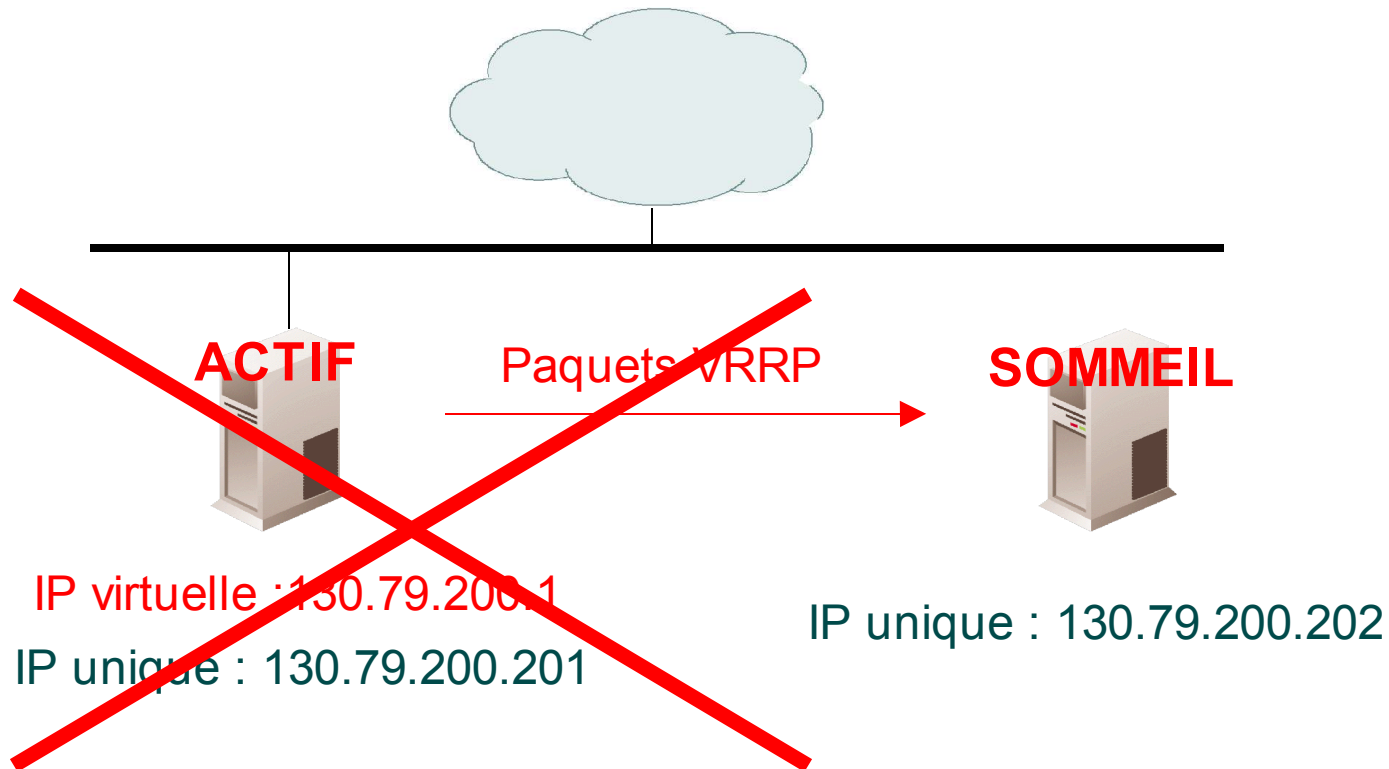
VRRP : principe (1)

- Un serveur actif (identifiant le plus élevé)
- Émission de paquet multicast : 224.0.0.18



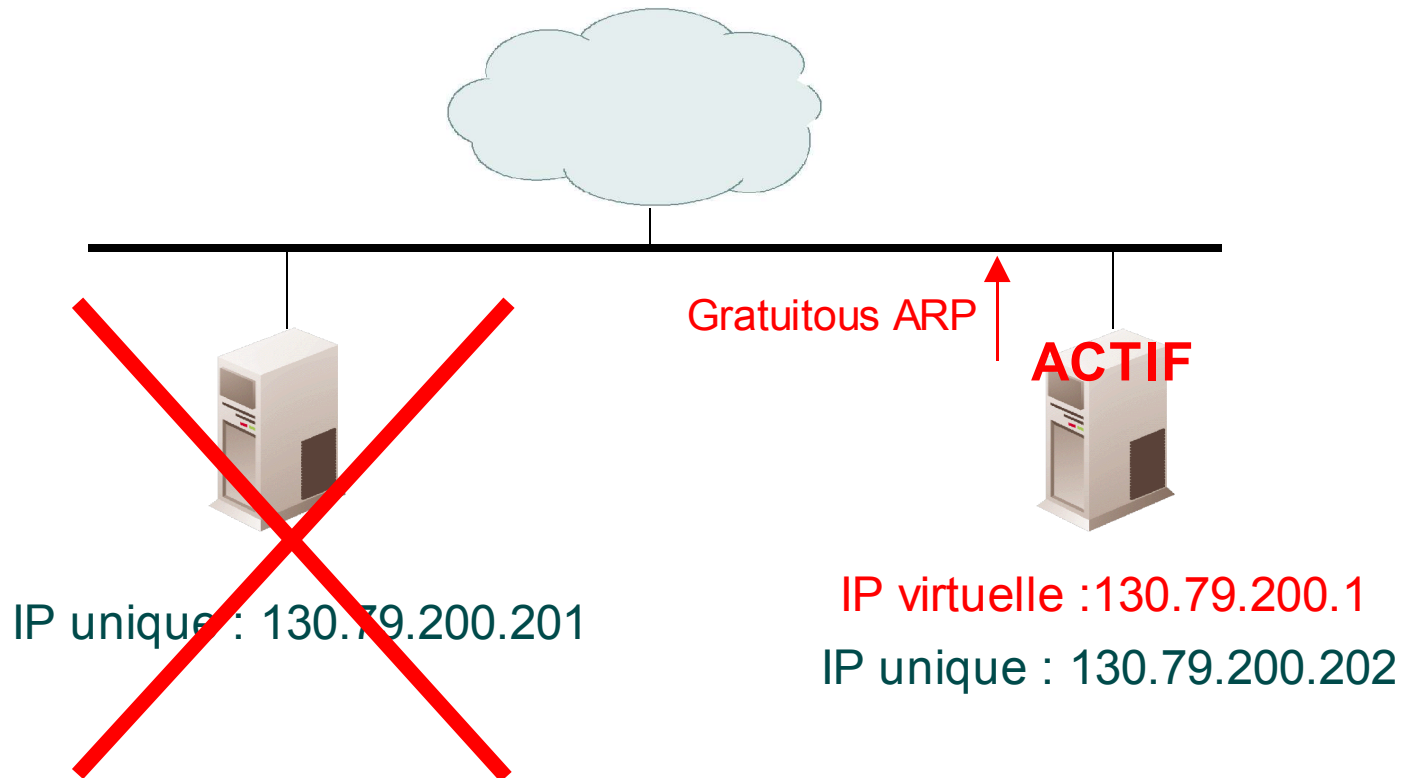
VRRP : principe (2)

- Plus de paquets émis par la machine active



VRRP : principe (3)

- Appropriation de l'adresse IP virtuelle par la deuxième machine ayant l'identifiant le plus élevé
- Émission d'un « gratuitous arp » sur le réseau



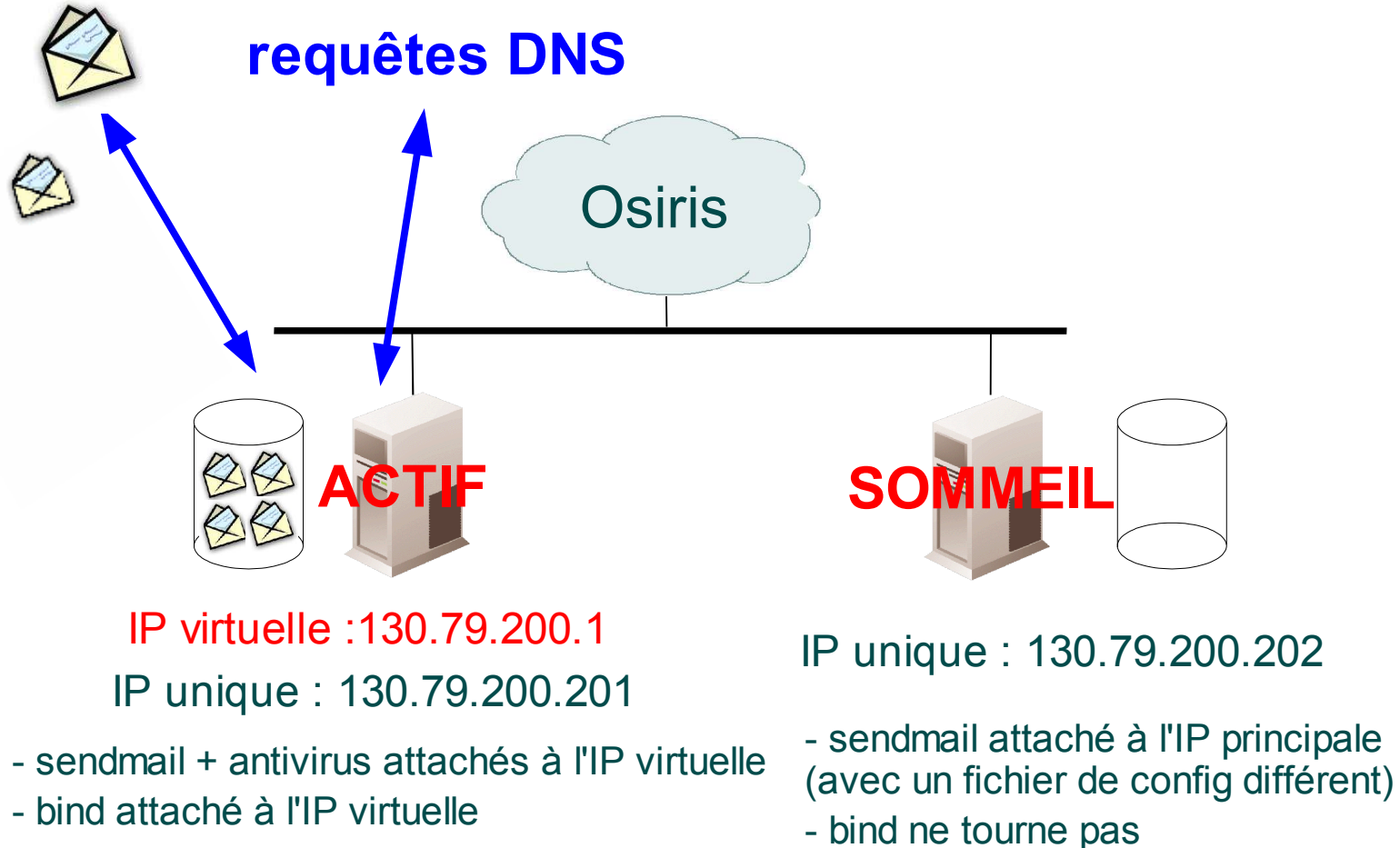
1. Introduction
2. Pourquoi faire évoluer l'architecture DNS ?
3. Principe de la nouvelle architecture DNS
4. VRRP
5. Mise en œuvre
6. Conclusion

Mise en œuvre

- Serveurs sous FreeBSD
- Utilisation de freevrrpd dans les ports
- Plusieurs services hébergés
 - DNS
 - Relayage de messagerie
- Configuration pointue
 - BIND
 - Sendmail
 - Divers scripts (synchronisation, changement d'états)

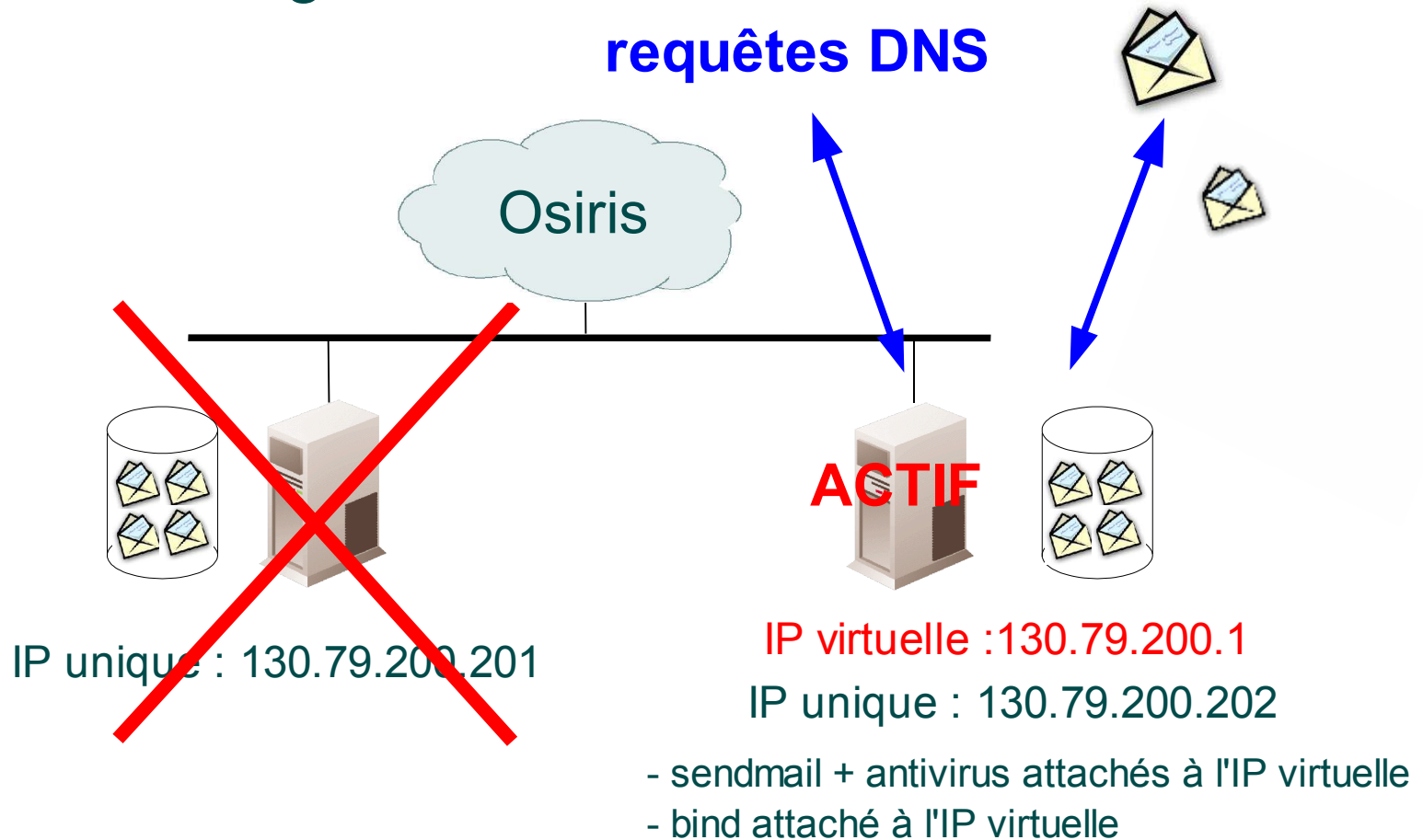
Comportement applicatif (1)

- Situation normale



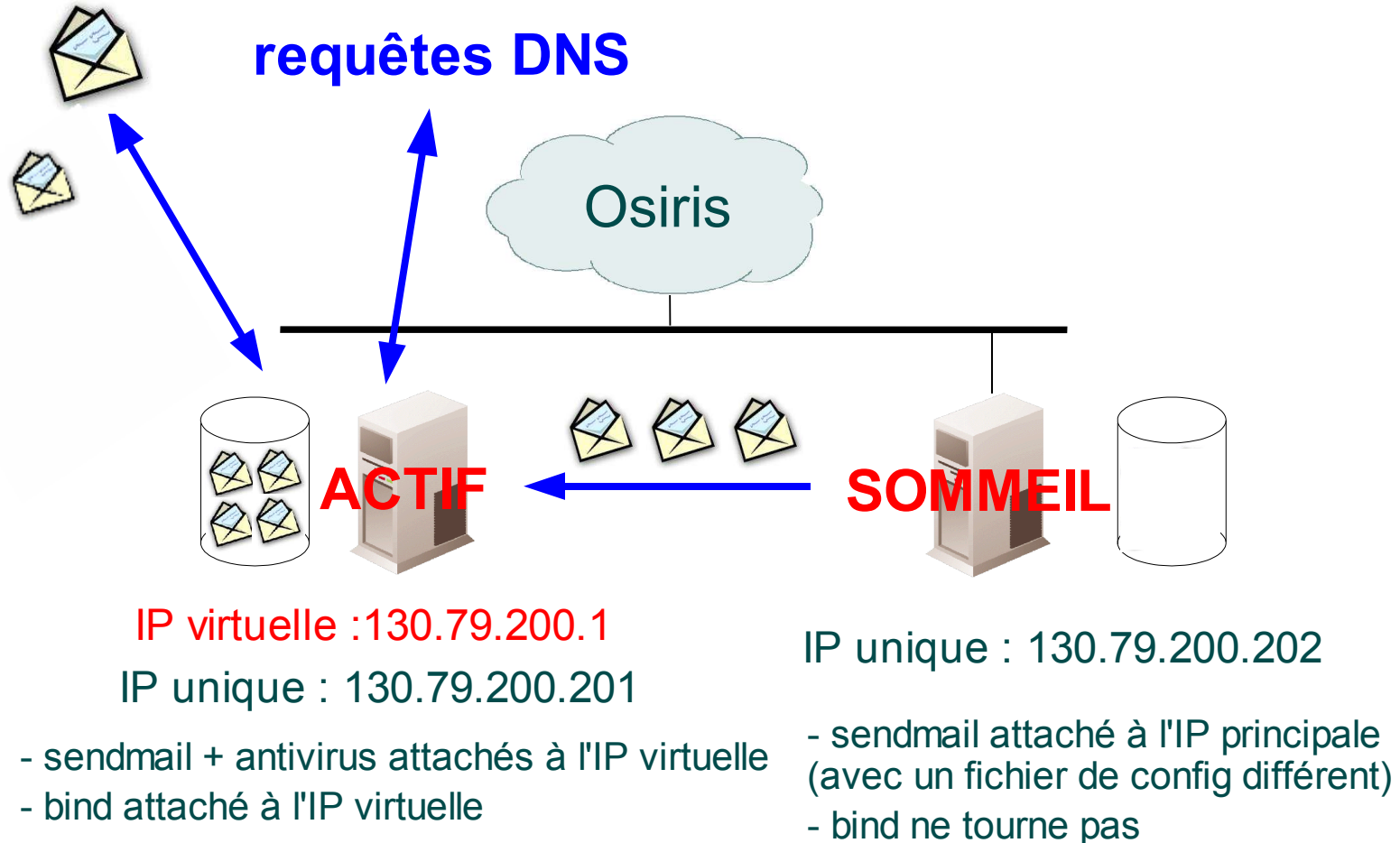
Comportement applicatif (2)

- Situation dégradée



Comportement applicatif (3)

- Retour à l'état normal



- **Configuration freevrrpd :**

```
[VRID]
```

```
serverid = 1
```

```
priority = 1
```

```
addr = 130.79.200.1
```

```
password = XXXX
```

```
masterscript = "/local/freevrrpd/master.sh"
```

```
backupscrip = "/local/freevrrpd/slave.sh"
```

- **Modification sendmail.cf du master**

```
O ClientPortOptions=Addr=130.79.200.1
```

- **Modifications named.conf**

```
query-source address 130.79.200.1 ;
```

```
transfer-source 130.79.200.1 ;
```

Mise en exploitation opérationnelle

- Maquettage préalable
- Migration en 2 étapes (30/04 et 12/05/2003)
 - Changement de l'adresse primaire du DNS principal
 - Mise en place du second serveur et de freevrrpd
- Interruption totale inférieure à 6 minutes
- Mise en place définitive le 12 mai 2003

1. Introduction
2. Pourquoi faire évoluer l'architecture DNS ?
3. Principe de la nouvelle architecture DNS
4. VRRP
5. Mise en œuvre
6. Conclusion

Conclusion

- Objectif de disponibilité atteint
- 99,99997 % de disponibilité du DNS durant les 5 derniers mois
- Facilité de mise à jour des systèmes d'exploitation
- Disparition des anciens DNS fin septembre 2004

- Pas encore de vérification applicative
- Pas encore de support IPv6