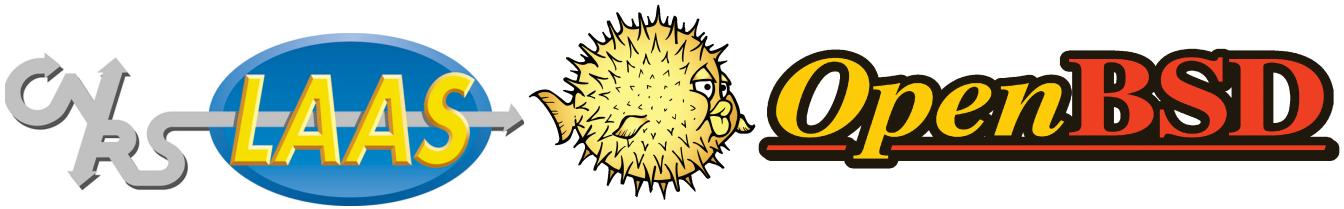
Haute disponibilité avec OpenBSD

Matthieu Herrb



Capitoul, 16 Octobre 2008

http://www.laas.fr/~matthieu/talks/obsd-ha.pdf

Plan

1 Introduction

2 CARP + pfsync

3 relayd

4 Autres services

5 Conclusion

Agenda

1 Introduction

2 CARP + pfsync

3 relayd

4 Autres services

5 Conclusion

Introduction

Haute disponibilité :

- robustifier les implémentations des services existants
  - améliorer la qualité du code
  - protéger contre les attaques/bugs
- assurer la redondance avec plusieurs serveurs

OpenBSD intègre de nombreux outils adaptés :

- Tables dans PF
- CARP / pfsync
- relayd
- etc.

Agenda

1 Introduction

2 CARP + pfsync

3 relayd

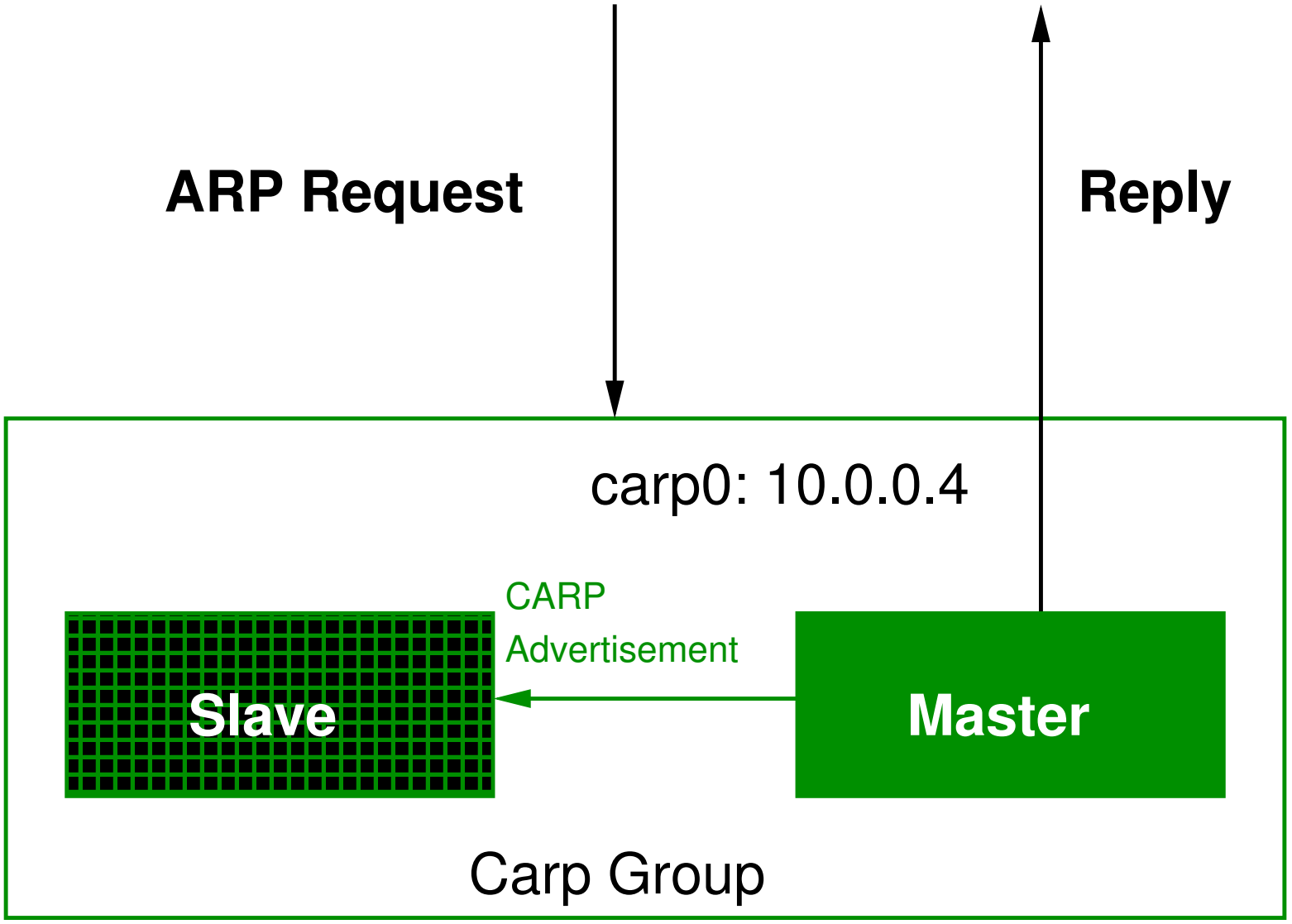
4 Autres services

5 Conclusion

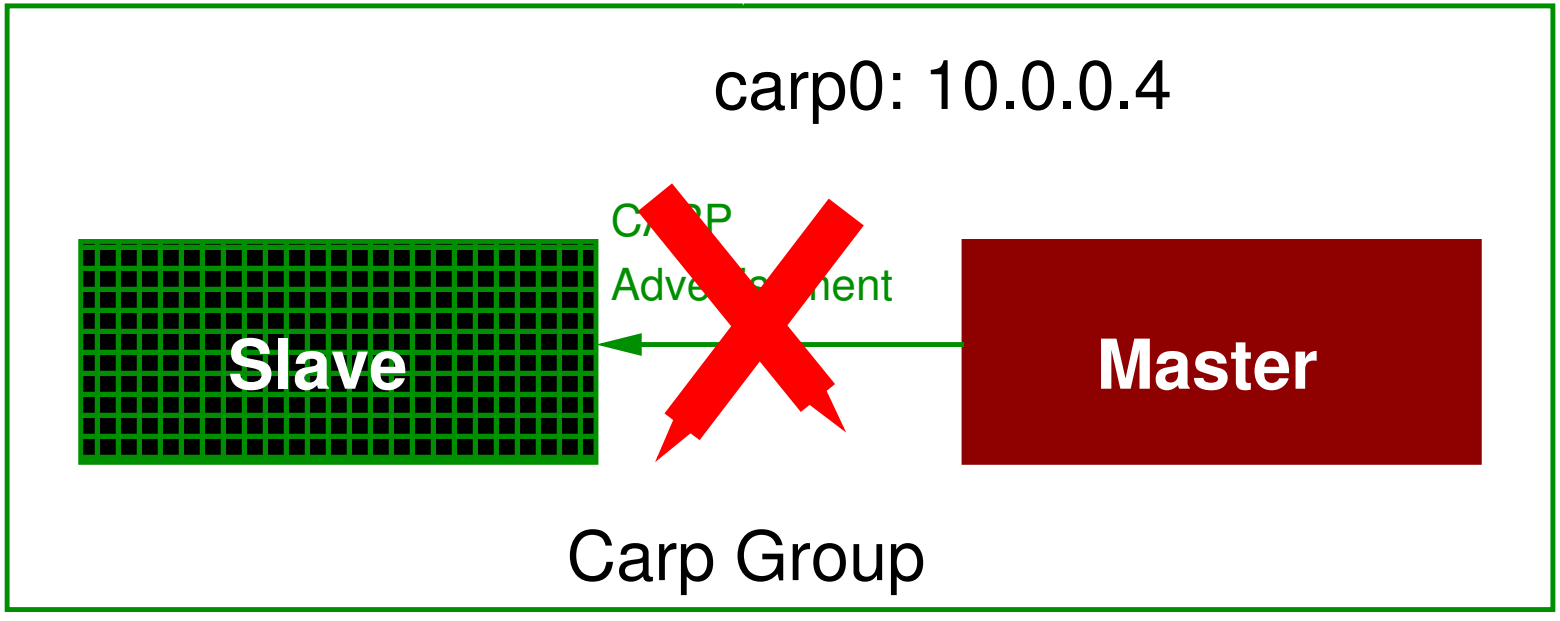
Principe

- CARP gère la redondance à la frontière des niveaux 2 et 3.
- **groupe CARP :** une adresse MAC et une adresse IP
- répond aux requetes ARP pour l'adresse IP
- utilise l'adresse MAC du groupe
  $\longrightarrow$ mise à jour des tables MAC des switches.
- Le maître envoie périodiquement des *CARP advertisements* (multicast)
  $\longrightarrow$ indique qu'il est vivant
- Si plus d'advertisments, autres membres envoient des advertisements, puis élection d'un nouveau maître.

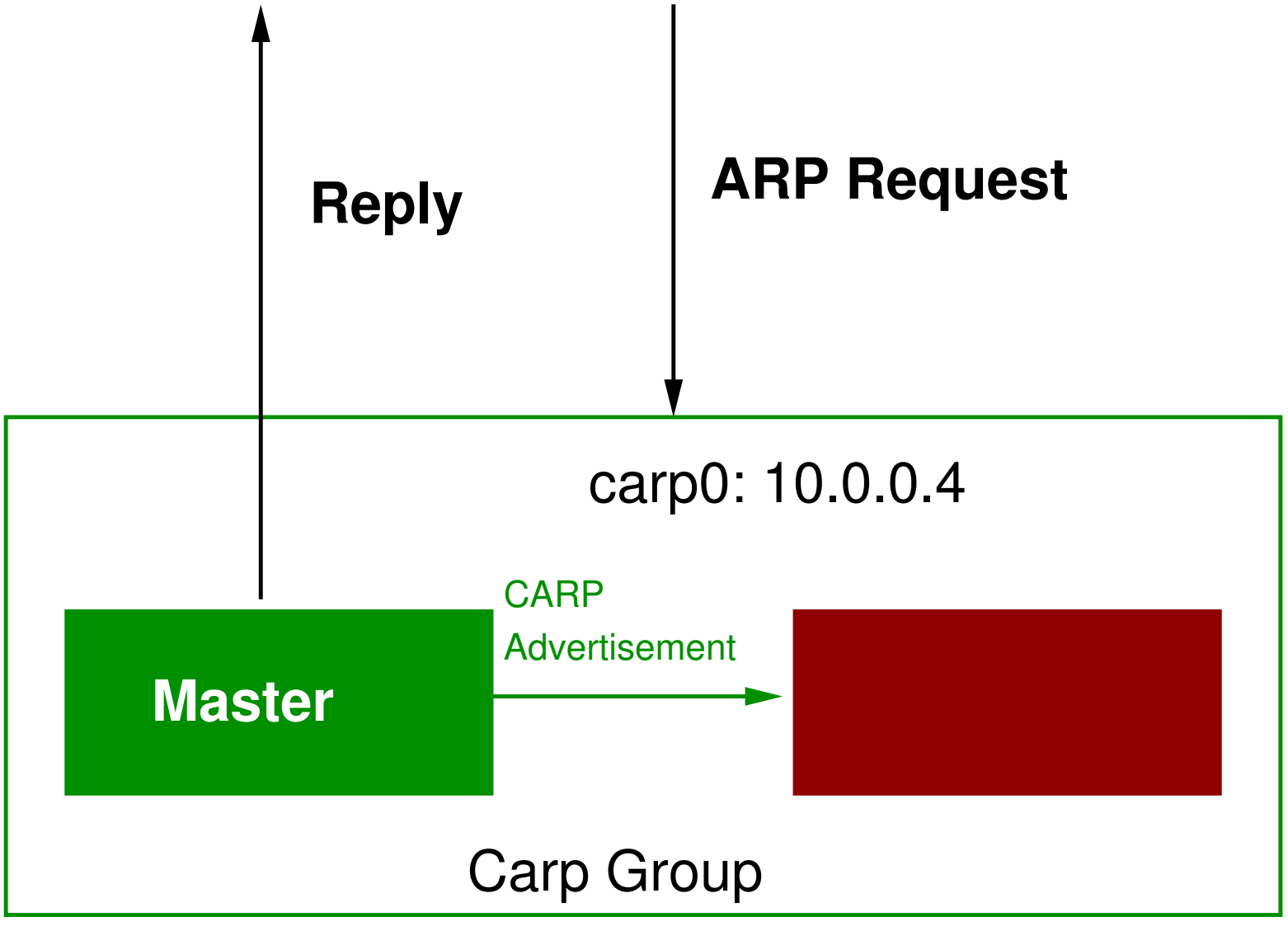
CARP : illustration



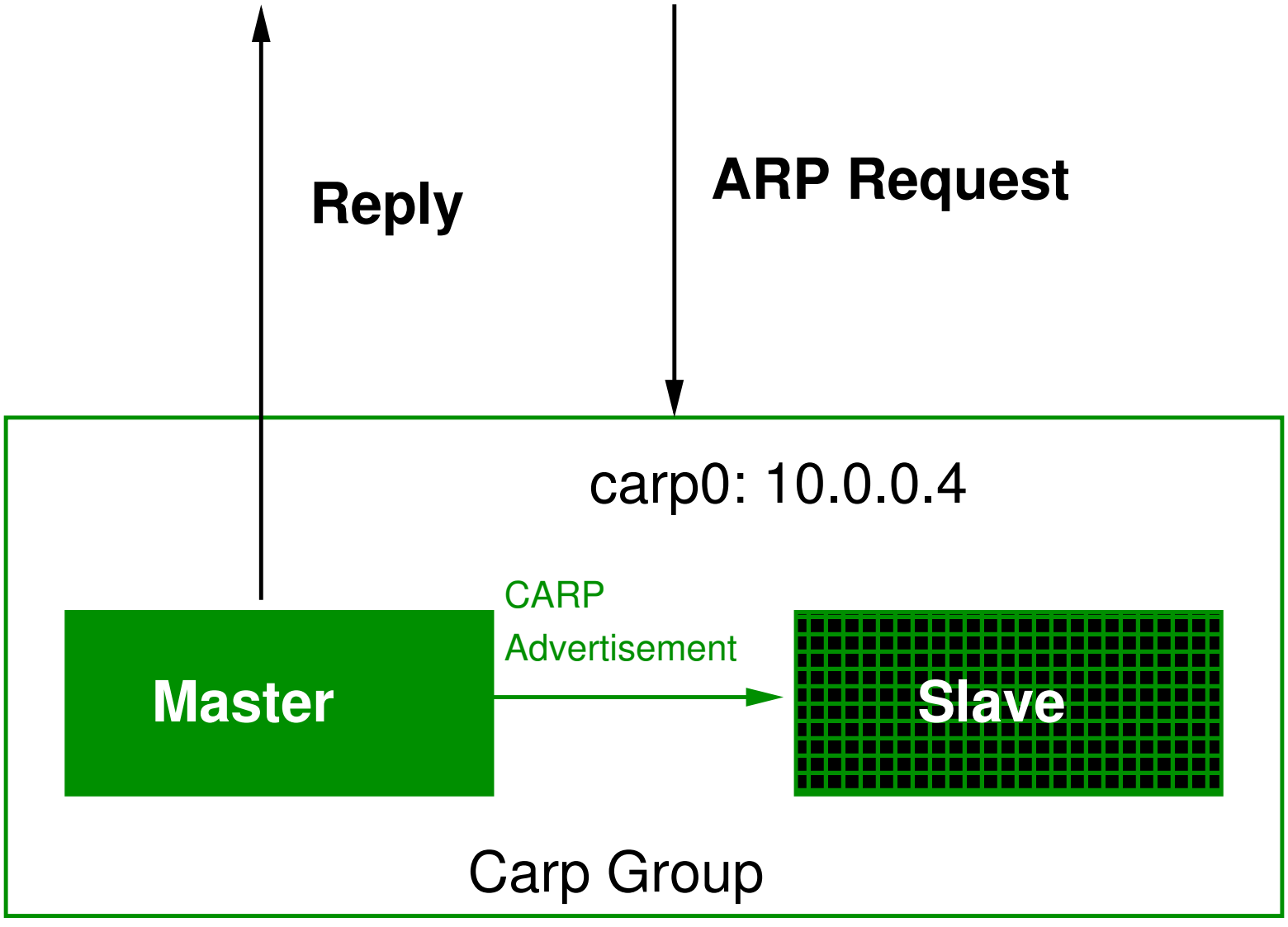
CARP : illustration



CARP : illustration



CARP : illustration



Préemption

Permet de définir des priorités entre les membres d'un groupe

- celui qui a la plus haute priorité (re)devient le maître
- répartition de charge à partir des priorités
  - au niveau ARP
  - au niveau IP

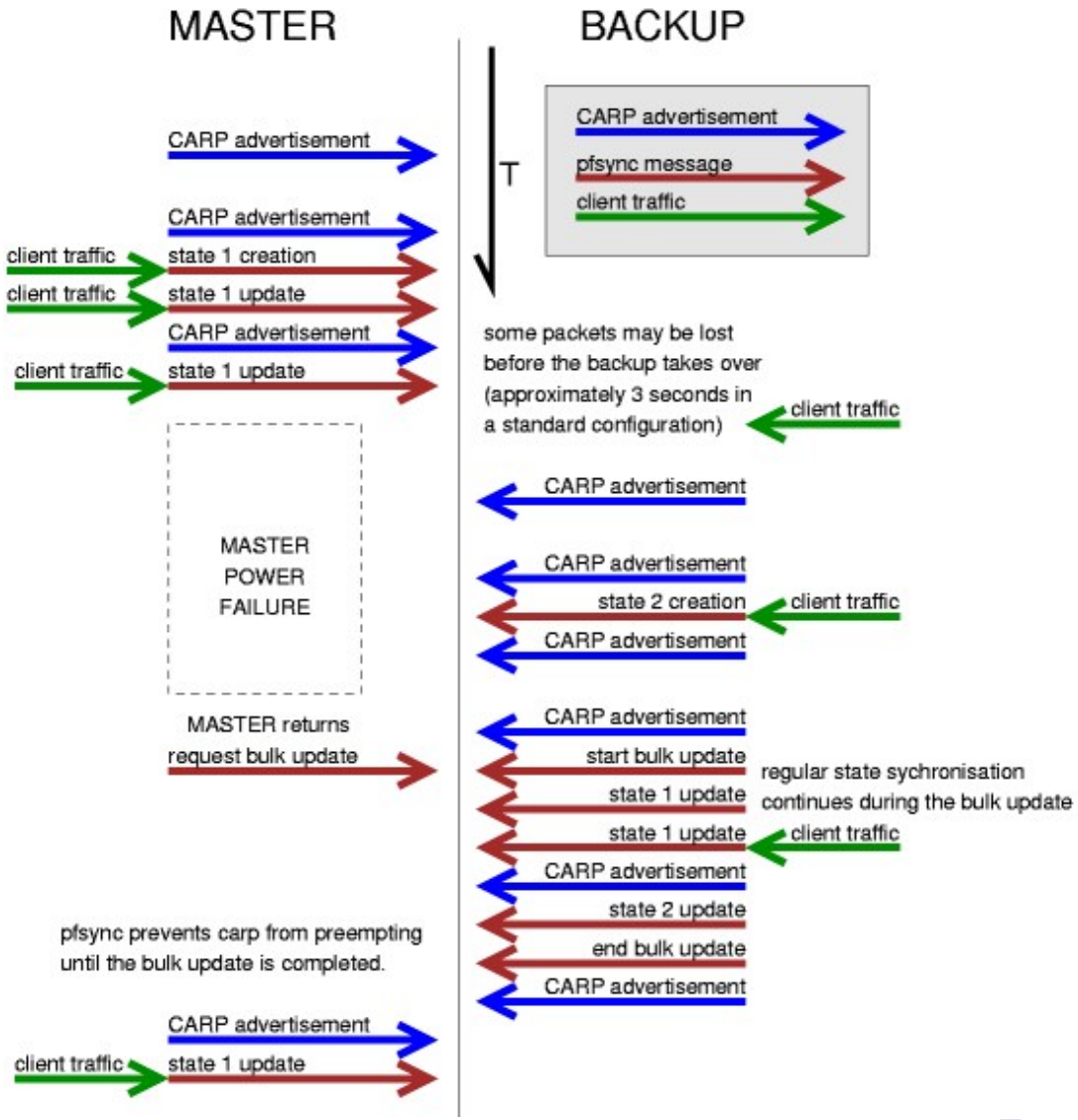
pfsync

PF : filtre de paquets à états (*stateful*)
$\longrightarrow$ synchroniser les états entre les pare-feu.

pfsync

- multicast protocole 240
- diffuse les créations, mises à jour et destructions d'états
- écoute les mise à jour des voisins
- met à jour la table d'états

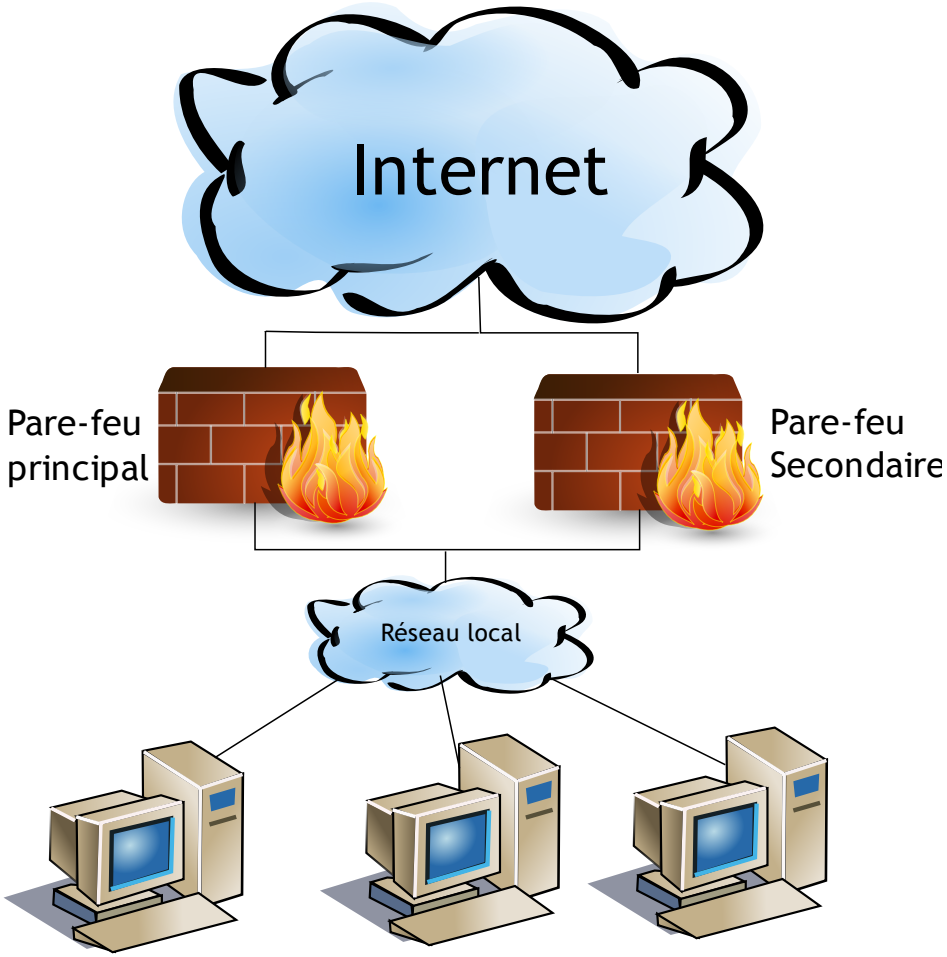
Chronogramme CARP + pfsync

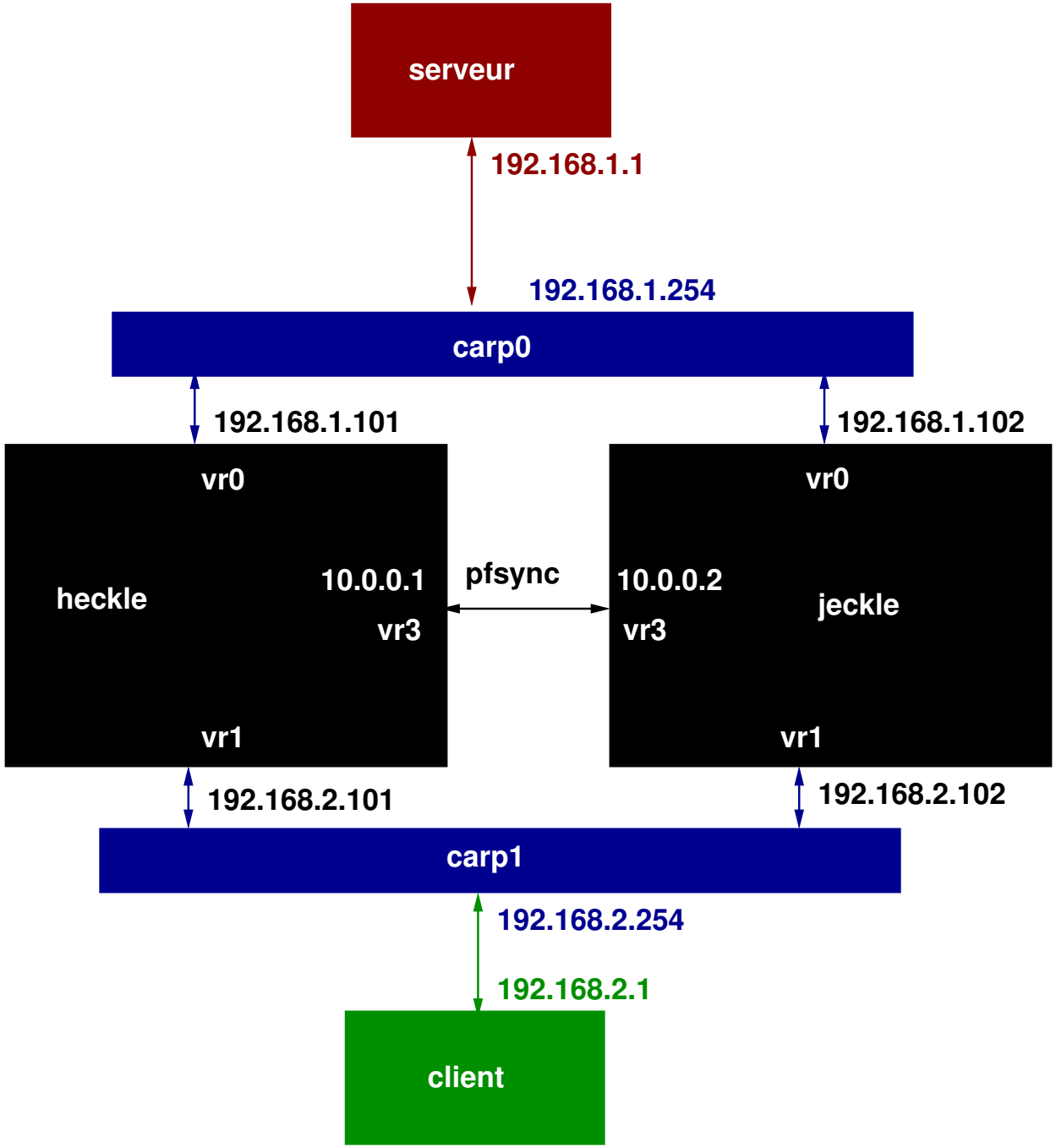


Spécificités par rapport à VRRP

- indépendant de la version du protocole.
  Supporte IPv4 et IPv6
- fonction *arp balance* pour faire du partage de charge.
- protection des advertisements par HMAC SHA-1

Configuration Simple




serveur
192.168.1.1
192.168.1.254
carp0
192.168.1.101
192.168.1.102
vr0
vr0
heckle
10.0.0.1
vr3
pfsync
10.0.0.2
vr3
jeckle
vr1
vr1
192.168.2.101
192.168.2.102
carp1
192.168.2.254
192.168.2.1
client

configuration maître

/etc/hostname.carp0

```
inet 192.168.1.254 255.255.255.0 192.168.1.255 vhid 1
pass secret1
```

/etc/hostname.carp1

```
inet 192.168.2.254 255.255.255.0 192.168.2.255 vhid 2
pass secret2
```

/etc/hostname.pfsync0

```
up syncif vr3
```

configuration esclave

/etc/hostname.carp0

```
inet 192.168.1.254 255.255.255.0 192.168.1.255 vhid 1
advskew 100 pass secret1
```

/etc/hostname.carp1

```
inet 192.168.2.254 255.255.255.0 192.168.2.255 vhid 2
advskew 100 pass secret2
```

/etc/hostname.pfsync0

```
up syncif vr3
```

Configuration pf

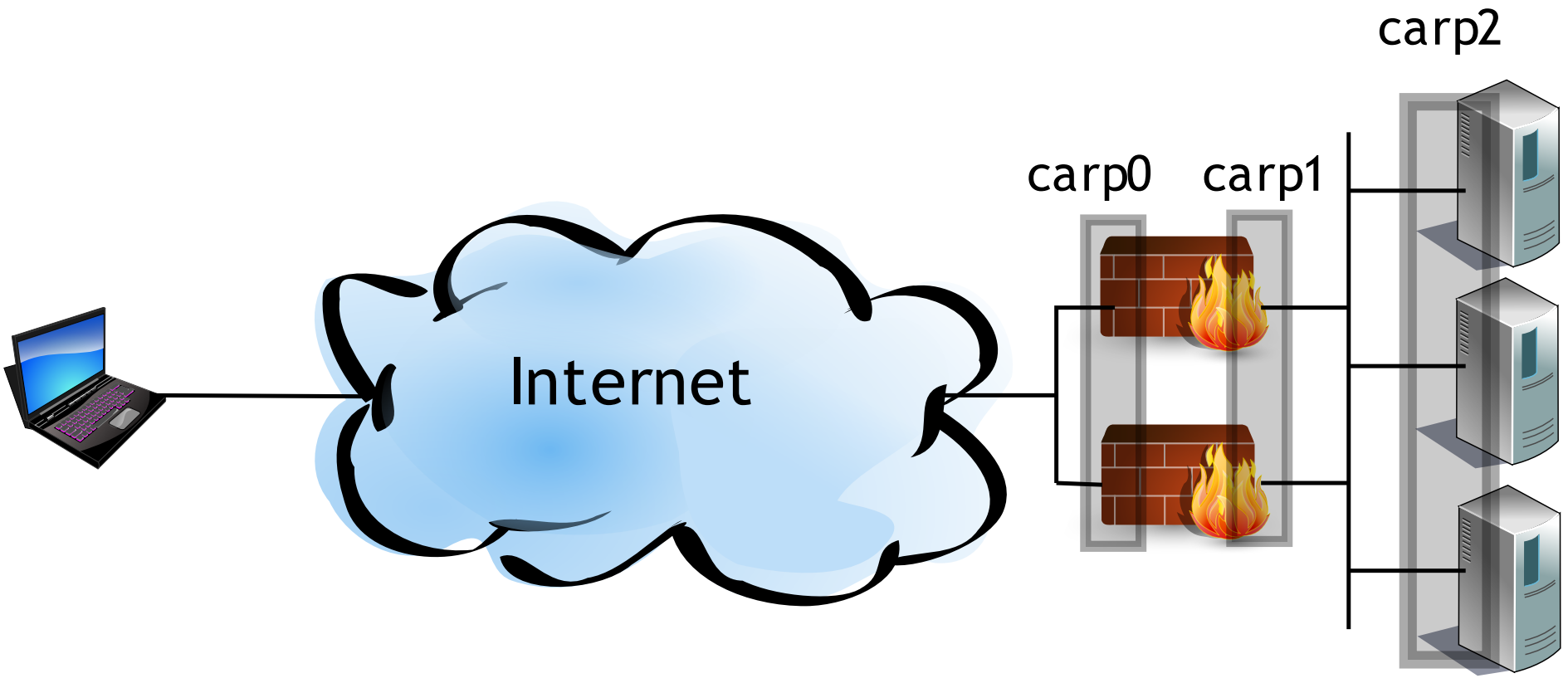
/etc/pf.conf

```
block in log
block out log

pass on $carpdevs proto carp
pass on $syncdev proto pfsync keep-state (no-sync)
```

Démonstration

Exemple complexe



Agenda

1 Introduction

2 CARP + pfsync

3 relayd

4 Autres services

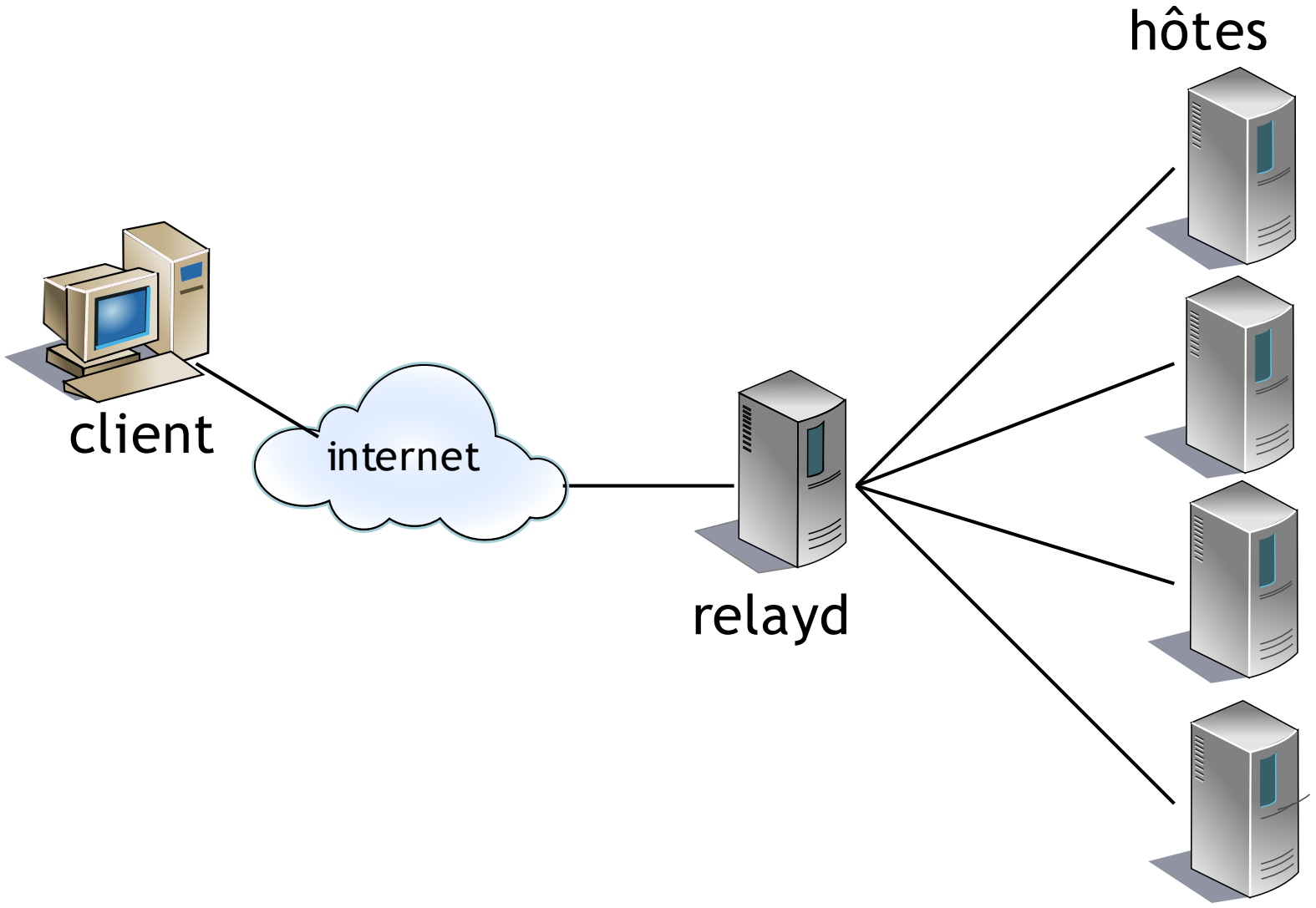
5 Conclusion

Principe

Répartition de charge :
Utiliser PF et ses mécanismes de redirection
pour répartir la charge vers plusieurs serveurs .
Niveau 3 ou niveau 7
Composants :

- *Config Parser :* lit le fichier de configuration, crée les règles.
- *Host Checking Engine :* sondes pour mesurer la disponibilité
- *PF Engine :* modifie dynamiquement les règles de PF
- *Relay Engine :* crée les sockets et traite les données avant redirection

Exemple



Éléments de configuration

- hôtes : fournisseurs de service
- tables : groupes d'hôtes fournissant le même service
- services : déclarations de partage de niveau 3
- protocoles : paramètres spécifiques pour les relais applicatifs
- relais : déclaration de partage de nivieau 7

Exemple : configuration simple niveau 3

- une adresse visible sur internet
- deux machines fournissant un service web statique

/etc/pf.conf

```
rdr anchor "relayd/*"
```

/etc/relayd.conf

```
public_addr=195.83.132.161
webhost1=10.1.1.100
webhost2=10.1.1.101


table <webhosts> { $webhost1 $webhost2 }


redirect www {
    listen on $public_addr port http interface trunk0
    forward to <webhosts> check http "/" code 200
}
```

relayctl

Commande de contrôle de `relayd`

- visualiser l'état des services
- activer/désactiver des hôtes
- activer/désactiver des services

Agenda

1 Introduction

2 CARP + pfsync

3 relayd

4 Autres services

5 Conclusion

DHCP

Le démon dhcpd d'OpenBSD supporte la synchronisation de la table des baux entre plusieurs serveurs.

- procotole multicast
- sécurisé via SHA-1 HMAC

$\longrightarrow$ permet d'avoir une redondance pour les serveurs DHCP

Exemple :

```
# dd if=/dev/arandom of=/var/db/dhcpd.key bs=2048 count=1
# /usr/sbin/dhcpd -y vr3 -Y vr3
```

IPSec : sasyncd

sasyncd synchronise les données d'un flux IPsec entre plusieurs routeurs.

Avec CARP et `isakmpd(8)` permet de construire un serveur de VPN IPsec redondant,
$\longrightarrow$ sessions non interrompues en cas d'arrêt d'un routeur.

Agenda

1 Introduction

2 CARP + pfsync

3 relayd

4 Autres services

5 Conclusion

Limites

Pourquoi pas plus de services avec support haute disponibilité ?

- difficile de synchroniser de l'état d'un service complexe (ex. : NFS, IMAP)
- problèmes de robustesse face à un état incohérent

Solutions complémentaires : virtualisation du stockage...

Conclusion

- Mécanismes de base pour la haute disponibilité au niveau logiciel.
- Permettent de construire des architectures sur mesure
- Attention : ne pas oublier la redondance matérielle.
- Rend la haute-disponibilité accessible.
- Complémentaire d’autres technologies.

Bibliographie

- *The Book of PF - A No-Nonsense Guide to the OpenBSD Firewall*, Peter N. M. Hansteen, ISBN-13 : 978-1593271657 December 2007, 184 pp.
- *Firewall Failover with pfsync and CARP*, Ryan Mc Bride, `http://www.countersiege.com/doc/pfsync-carp/`.
- *Load-Balancing using HostStated*, Pierre-Yves Ritschard, EuroBSDCon 2007, `http://www.openbsd.org/papers/eurobsdcon07/pyr-loadbalancing/`

Questions ?