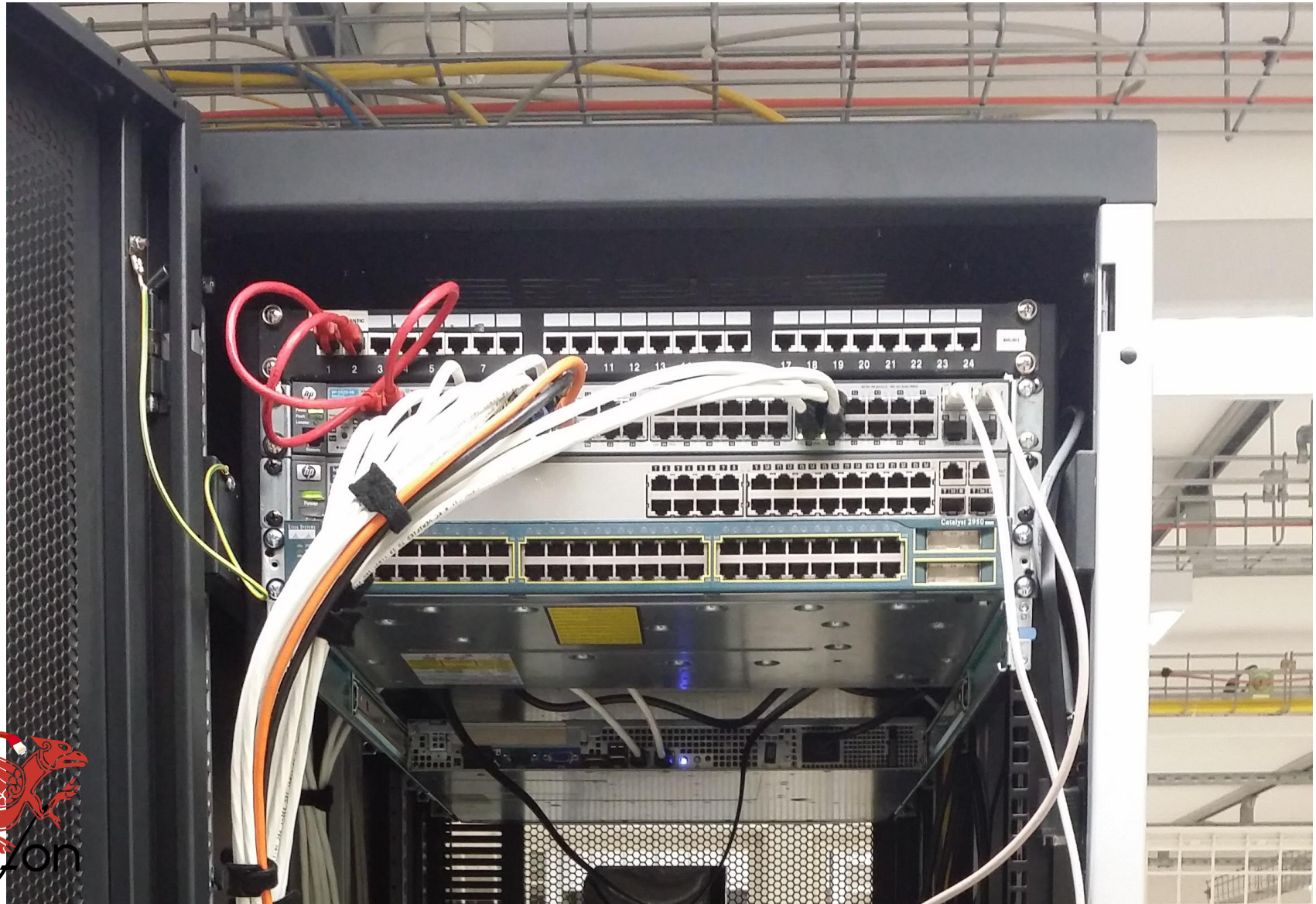
Routeur FreeBSD : redondance et sécurité

Alarig Le Lay <alarig@grifon.fr>

Meetup BSD – 26 juin 2017

Grifon, `89.234.186.0/24` – `2a00:5884::/32` – `AS204092`

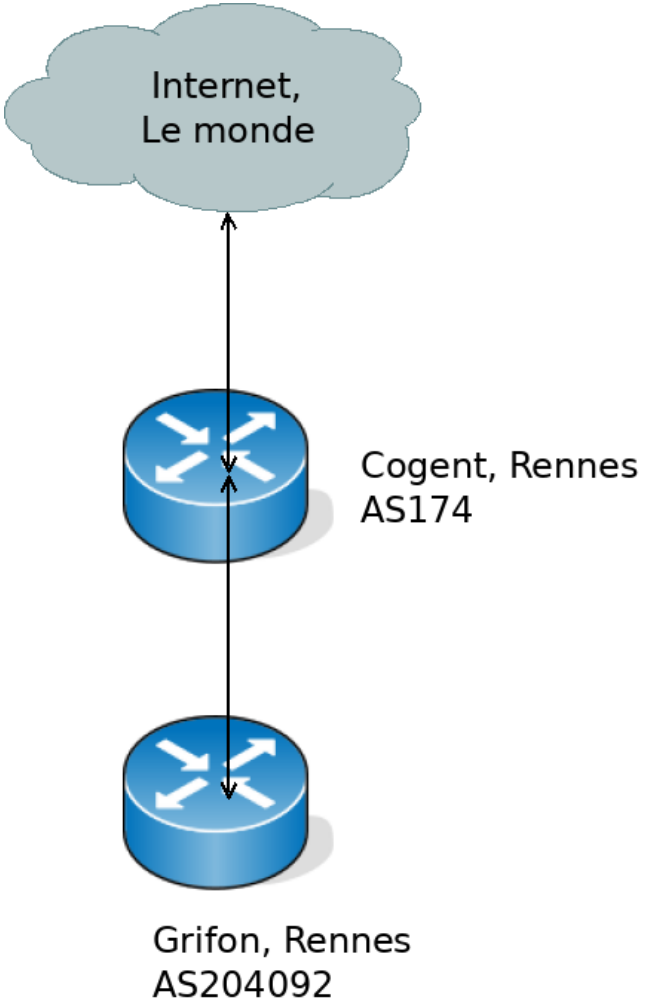
L’asso grifon



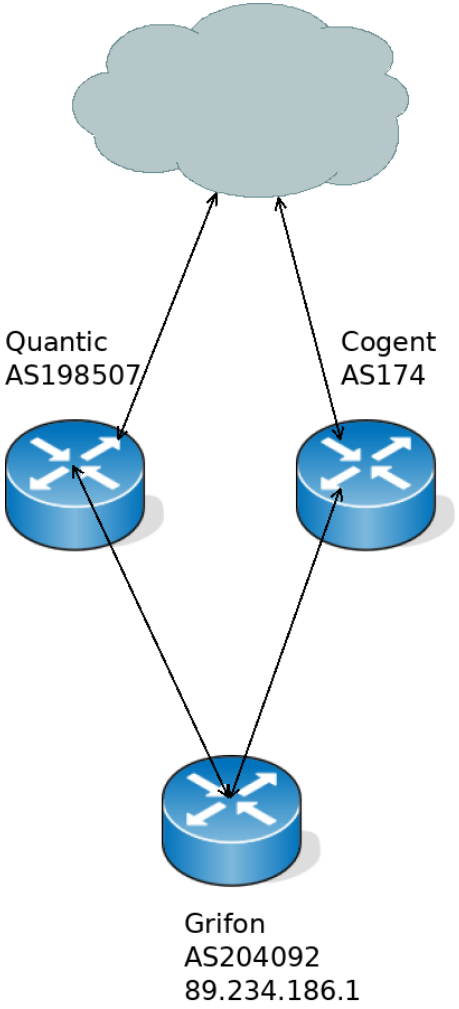
Comment avoir de la haute disponibilité réseau ?

1. Comment ne pas dépendre d'un seul transitaire ?
2. Comment ne pas dépendre d'un seul routeur ?

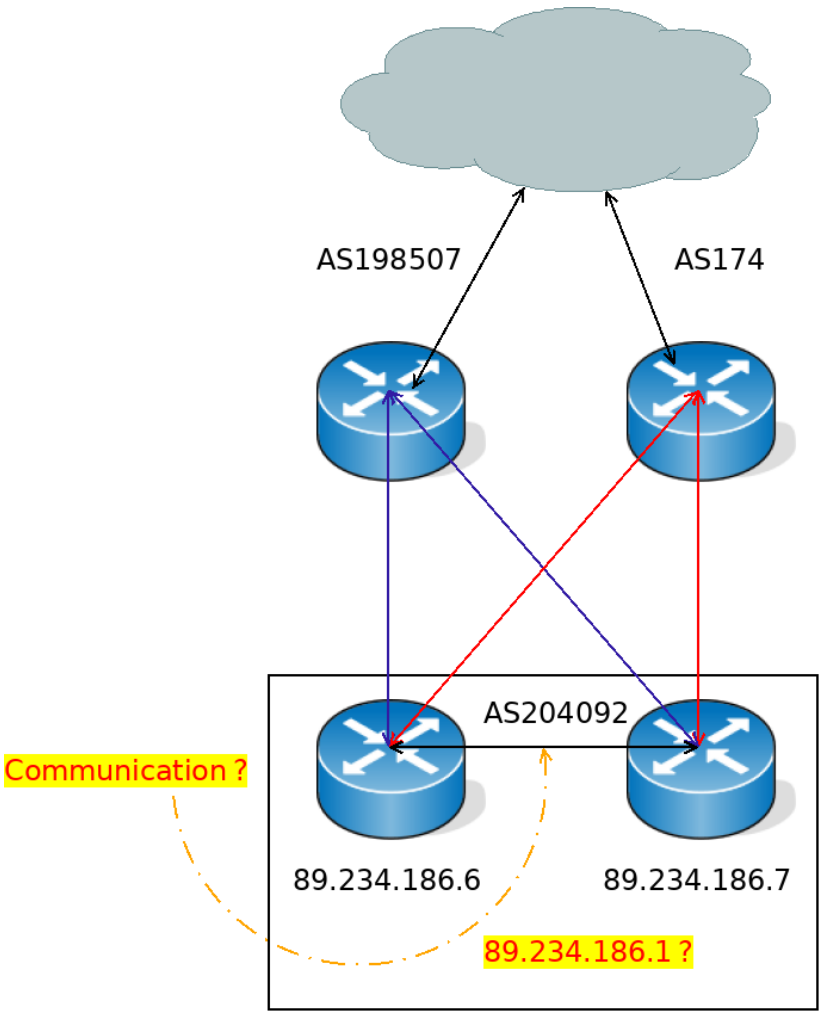
Au commencement, un seul transitaire



Deux transitaires, c'est bien mais pas top



C'est déjà mieux, mais pas encore tout à fait



Problème numéro 1 : la communication entre les routeurs

Comment continuer à recevoir la fullview si les interconnexion avec l'extérieur tombe ?

iBGP !

Problème numéro 1 : la communication entre les routeurs

```
protocol bgp ibgp_nominoe {
    local as 204092;
    description "fullmesh iBGP";
    neighbor 89.234.186.7 as 204092;
    source address 89.234.186.6;
    import keep filtered;
    export all;
    receive limit 680000 action block;
    next hop self;
}
```

Grizon

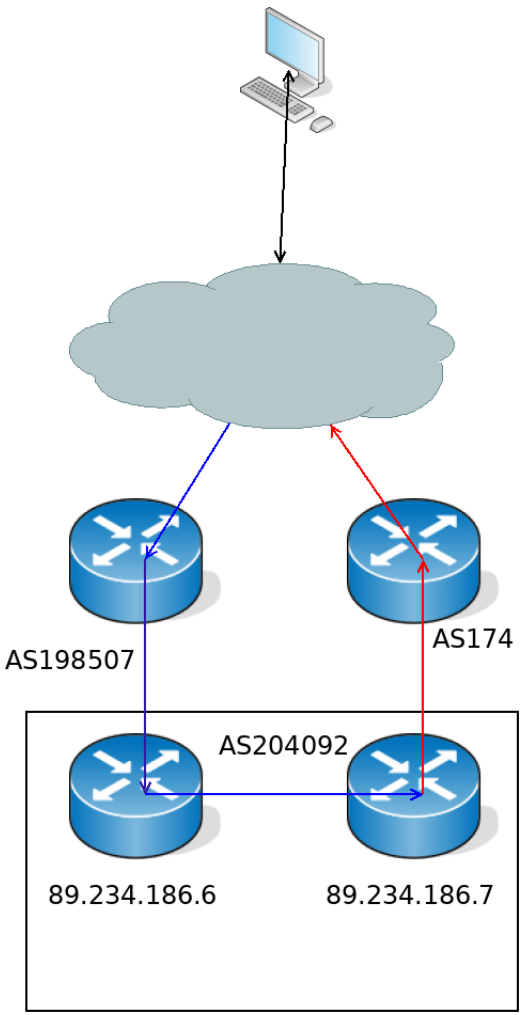
Problème numéro 1 bis : ne pas fâcher BCP38

Que ce passe-t-il quand on veut se connecter à un routeur alors que le routage n'est pas symétrique ?

Ça ne marche pas, donc on modifie notre configuration de firewall.

Grizon

Problème numéro 1 bis : ne pas fâcher BCP38

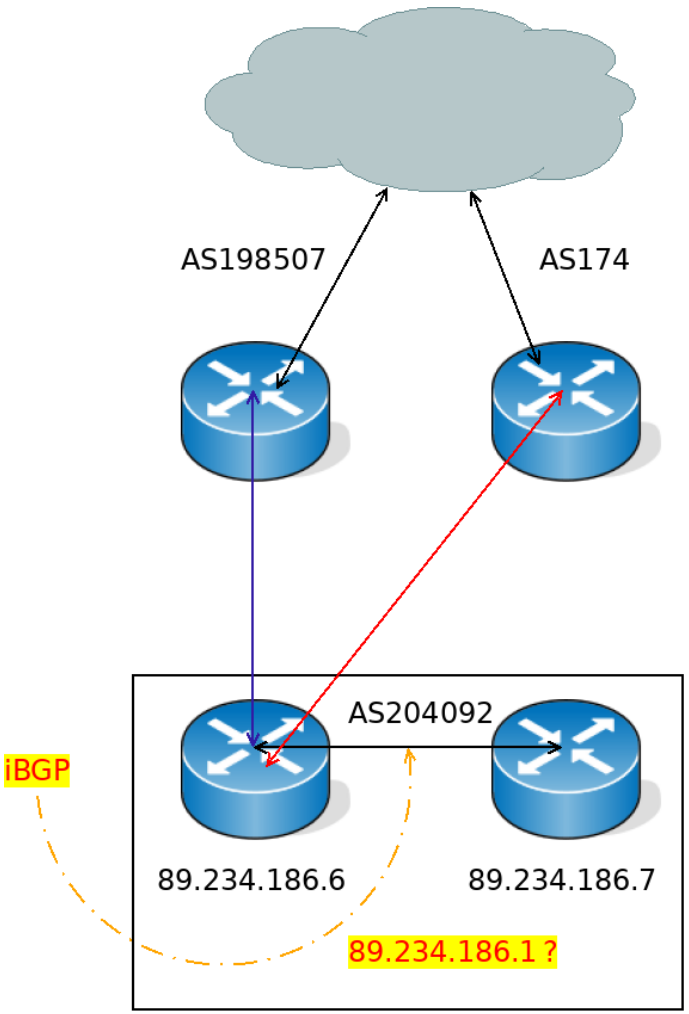


Problème numéro 1 bis : ne pas fâcher BCP38

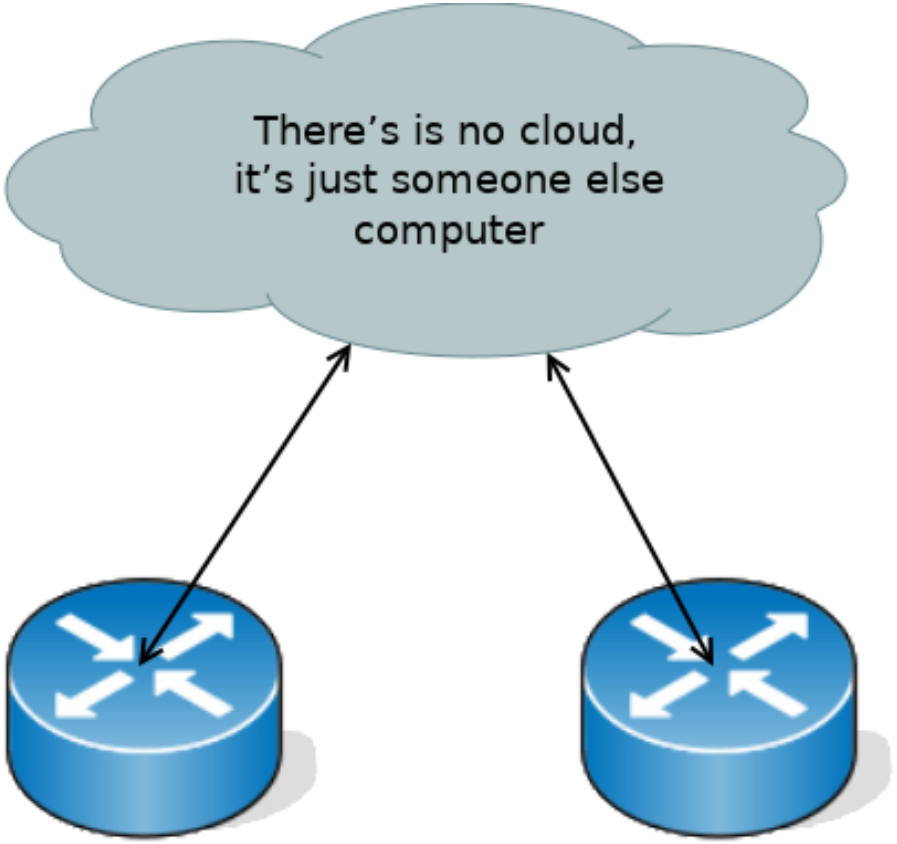
```
loopback_addr4 = "89.234.186.7/32"
loopback_addr6 = "2a00:5884::1/128"

block in quick on $int_if from urpf-failed to \
        ! $loopback_addr4 label uRPF
block in quick on $int_if from urpf-failed to \
        ! $loopback_addr6 label uRPF
```

Grizon

Problème numéro 1 : la communication entre les routeurs



Problème numéro 2 : la communication clients/routeurs



00:15:17:39:f0:1b
89.234.186.1

00:0d:b9:3a:24:b9
89.234.186.1

Problème numéro 2 : la communication clients/routeurs

1. Fonctionnalités similaires à VRRP ou HSRP
2. 1990 : travaux de l'IETF sur la redondance réseau
3. 1997 : Cisco vient mettre son grain de sel
4. Cisco informe OpenBSD de leur brevet pour empêcher une implémentaton libre
5. Création de CARP par OpenBSD
6. Intégration native dans FreeBSD

Grizon

Problème numéro 2 : la communication clients/routeurs

Configuration IPv4

/etc/rc.conf

```
ifconfig_re1="inet 89.234.186.6 netmask 255.255.255.128"
ifconfig_re1_alias0="inet vhid 1 advskew 10 pass password \
        alias 89.234.186.1/32"
```

Problème numéro 2 : la communication clients/routeurs

Configuration IPv6 intuitive

/etc/rc.conf

```
ifconfig_re1="inet 89.234.186.6 netmask 255.255.255.128"
ifconfig_re1_ipv6="inet6 2a00:5884::6/64"

ifconfig_re1_alias0="inet vhid 1 advskew 10 pass password \
        alias 89.234.186.1/32"
ifconfig_re1_alias0_ipv6="inet6 vhid 1 advskew 10 pass \
        password alias fe80::204:092:100:1/64"
```

BOOM

Problème numéro 2 : la communication clients/routeurs

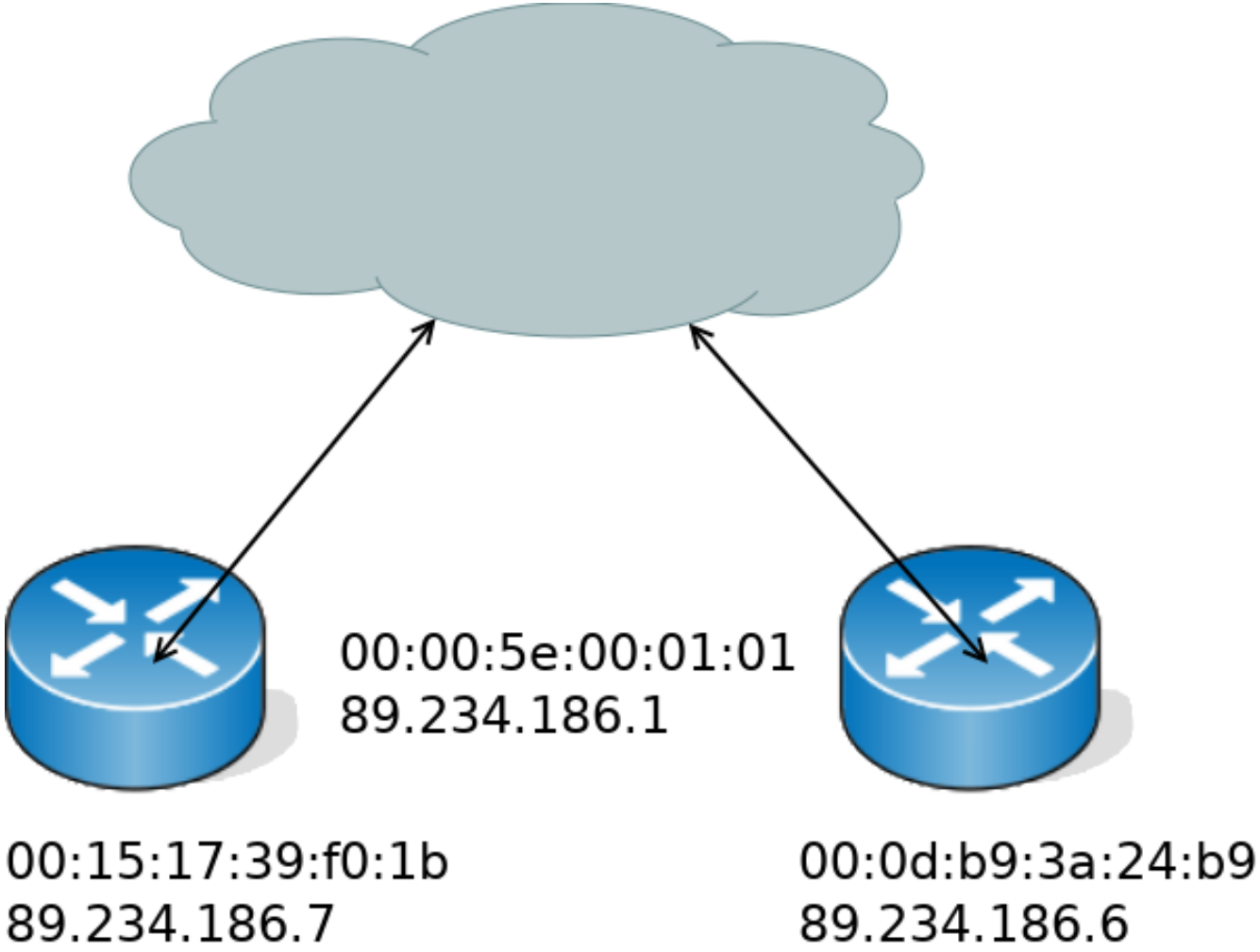
Configuration IPv6 fonctionnelle

/etc/rc.conf

```
ifconfig_re1="inet 89.234.186.6 netmask 255.255.255.128"
ifconfig_re1_ipv6="inet6 2a00:5884::6/64"

ifconfig_re1_alias0="inet6 fe80::204:092:100:1/64 vhid 2 \
        advskew 10 pass passwordv6"
ifconfig_re1_alias1="inet vhid 1 advskew 10 pass password \
        alias 89.234.186.1/32"
```

Pas boom.

Problème numéro 2 : la communication clients/routeurs



Conclusion

- Partie WAN : eBGP (plus de transitaires) + iBGP (discussion entre routeurs) + pf (BCP38)
- Partie LAN : CARP

Question ?