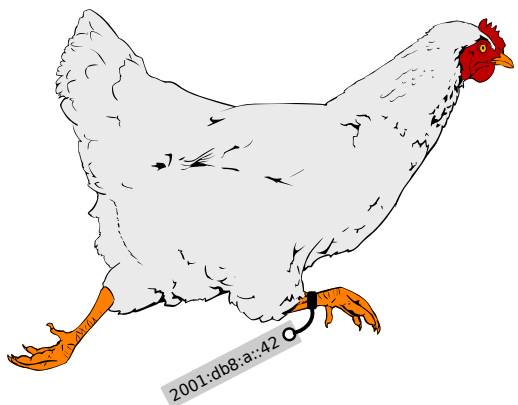
Lothaire Yarding

Julien VAUBOURG

Plan

Pourquoi IPv6 ?



Pourquoi IPv6 ?

Sans NAPT, tout est plus simple

- **VoIP** (vrai P2P)
- Visioconférences (**engorgements**)
- Accès aux **serveurs** (adresses publiques)
- **Chiffrement** (réécriture des paquets)
- **Journaux systèmes** (bannis)
- **Sécurité** des transactions (partage des IP)
- Etc.

Pourquoi IPv6 ?

Moins de conflits, moins de colisions

- Mise en place de **tunnels** (renumérotations)
- **Fusion** de deux sites (renumérotations)
- **Broadcast** intempestifs (colisions et boucles)
- Disparition de la **fragmentation** (*packet too big*)
- Etc.

Pourquoi IPv6 ?

Plein de nouveautés

- Nombre **illimité** d'adresses
- Adresses de lien local uniques (**zéroconf en mieux**)
- **Plus de broadcast** (fonctionnement plus léger avec multicast)
- **IPsec** disponible systématiquement
- Entêtes IP simplifiés (**plus de recalculs au routage !**)
- **Classement** par adresses multicast
- **Autoconfiguration** stateless
- **QoS facilitée** (+ flow label)
- Etc.

Le risque des CGN

- **Chevauchements** (RFC 1918 limitée)
- Connexions **P2P** (de quasi-impossible à impossible)
- **Réseaux limités** (max `10.0.0.0/8`)
- **Géolocalisation** impossible
- Protocoles limités aux standards (**plus d'innovation**)
- Nombre de **ports limités** (aucun standard, parfois critique)
- **Journaux systèmes** (moyens démesurés)
- **Sécurité** (IP partagées, connexions dures à retracer)
- Autohébergement / Neutralité du Net (**perte totale du modèle Internet**)
- Etc.

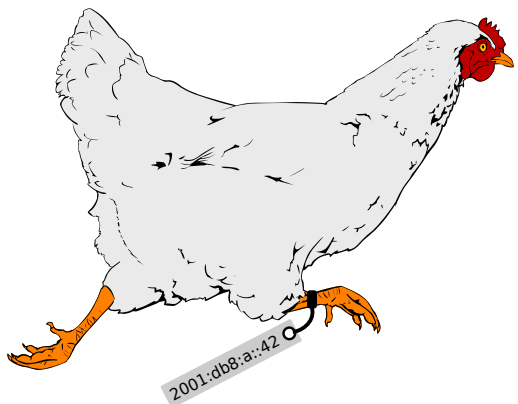
Pourquoi IPv6 ?

≪ **La non-migration vers IPv6 coûte très cher**, *notamment en* **temps passé** *à faire fonctionner les applications malgré le NAT, en* **complexité** *due à l'existence de deux domaines d'adressage [...], en* **temps passé** *à remplir des papiers pour [les] RIR [...], en* **lignes de code** *dans les applications SIP ou pair-à-pair pour arriver à contourner l'absence d'adresses globalement uniques.*

Le coût global de ces mesures est sans doute bien supérieur à celui d'une migration *vers IPv6.* ≫

Stéphane BORTZMEYER.

Diffusion du document



Diffusion du document

≪ **Y**et **A**nother **R**eference for **D**elivering **I**Pv6 to the **N**ext **G**eneration ≫

- Stage de **3 mois**
- **149 pages** (constante évolution)
- **48 schémas**

Diffusion du document

- **Historique** du protocole IP
- **Étude de son utilisation** actuelle
- **Études protocolaires**
- **Expérimentations** reproductibles

Diffusion du document

- Un jour et demi **en tête des dépêches LinuxFR**
- Plus de **100 commentaires et des feedbacks** par courriel
- **Un retour d'un expert** Cisco (via Sébastien)
- Plus de **3000 téléchargements**

Diffusion du document

- Relayé sur la **liste du G6** (chercheur TELECOM Bretagne)
- Mentionné sur **FRnOG** (thread NATv6)
- Publié par **Stéphane BORTZMEYER** (SeenThis)

Diffusion du document

Stéphane Bortzmeyer 3 weeks ago

L'état de l'art sur #IPv6 réalisé par un étudiant en stage au sein de l'équipe réseau #Lothaire (le réseau Éducation/Recherche de Lorraine). Très complet et très bien écrit.

En prime, j'y ai appris la différence entre « yarding » et « free range » pour l'élevage des poules :-)

julien.vaubourg.com/.../lothaire-yarding_ipv6....

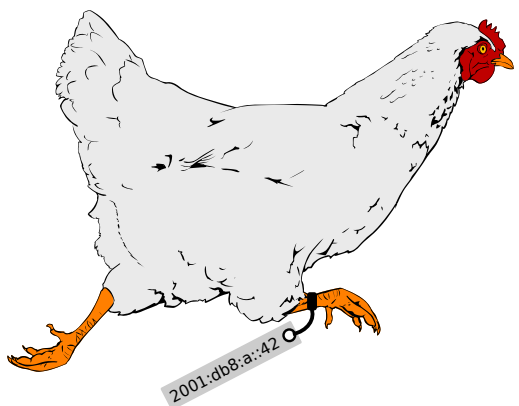
Intéressante et riche discussion sur LinuxFr à propos de ce rapport :

linuxfr.org/.../ipv6-des-poules-et-des-hommes [fr]

#Lorraine

@stephane CC BY-SA

Détermination des adresses



Portée des adresses

Adresses de lien local

- Préfixe `fe80::/10`
- Équivalent du préfixe `169.254/16`
- Non-routables

Adresses locales uniques

- Préfixe `fc00::/7`
- Routables uniquement en local (tunnels)
- Algorithme (RFC 4193) pour les rendre presque uniques
- Équivalent des plages privées IPv4

Portée des adresses

Adresses globales

- Toutes les autres adresses unicast (par RIR)
- Sauf `2001:db8::/32` (documentation et non APNIC)

Multiplicité des adresses

- Une adresse de lien local par interface
- *Multi-homage* (plusieurs FAI)
- Adresses temporaires (vie privée)
- Tunnels
- Double-pile IPv4/IPv6

Problématiques

Quelle adresse source pour sortir ?

Quelle adresse de destination pointer (AAAA, A) ?

Algorithmes

Source : une seule adresse déterminée (noyau / *connect()*)

Destination : liste ordonnée (*getaddrinfo()*)

Algorithmes

« *Default Address Selection for Internet Protocol version 6 (IPv6)* »

- **RFC 3484** (Yarding)
- **RFC 6724** (septembre 2012)

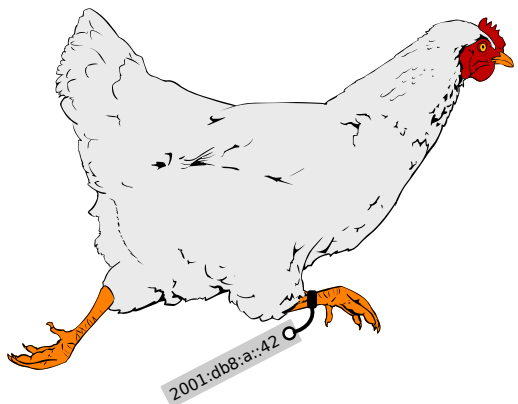
Couples source/destination (IPv6 prioritaire) :

1. Même portée
2. La portée la plus étroite possible
3. Adresses temporaires / masquées
4. Partagent le plus de bits de préfixe possible

Influencer / Contourner

- Au niveau applicatif (*BindAddress*)
- Table de politiques (*/etc/gai.conf*)
- Durée de validité des adresses

Adresses multicast



Adresses multicast

Le broadcast disparaît !

Nom	Adresse	Équiv. IPv4	Fonction
all-nodes	`ff02::1`	`224.0.0.1`	*Tout le monde*
all-routers	`ff02::2`	`224.0.0.2`	*Routeurs du lien*
all-dhcp	`ff02::1:2`	Aucun	*DHCP du lien*
solicited-node	`ff02::1:ff*`	Aucun	*Restreint*

Adresses multicast

```
user@debian$ cat /etc/hosts
# The following lines are desirable for IPv6 [...]
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Adresses multicast

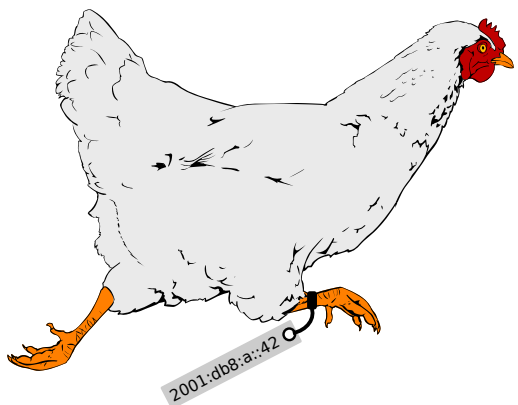
```
user@debian$ ip -6 maddress show dev eth0
2:      eth0
        inet6 ff02::fb
        inet6 ff02::202
        inet6 ff02::1:ffec:b49b users 2
        inet6 ff02::1
```

Adresses multicast

```
Router# show ipv6 interface fa 0/1

  IPv6 is enabled, link-local address is FE80::[...]
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:660:4503:105::2, subnet is 2001:660:4503:[...]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:2
    FF02::1:FF02:8DB9
```

Autoconfiguration



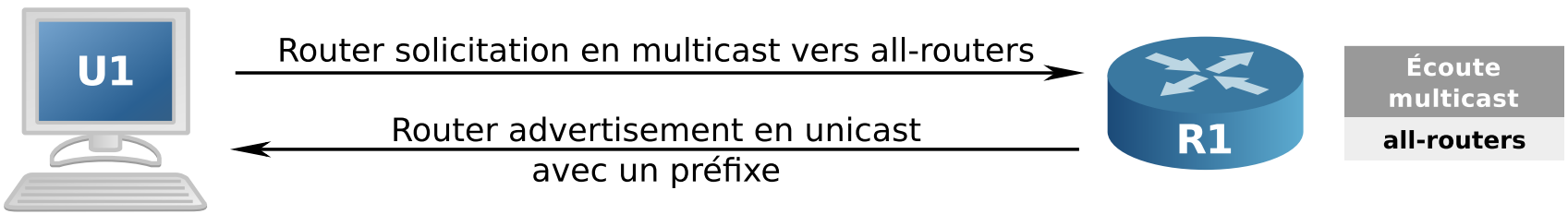
Stateless

- Nouveauté d'IPv6 ☺
- Aussi appelé SLAAC ou NDP
- Systématique en lien local (`fe80::/10`)

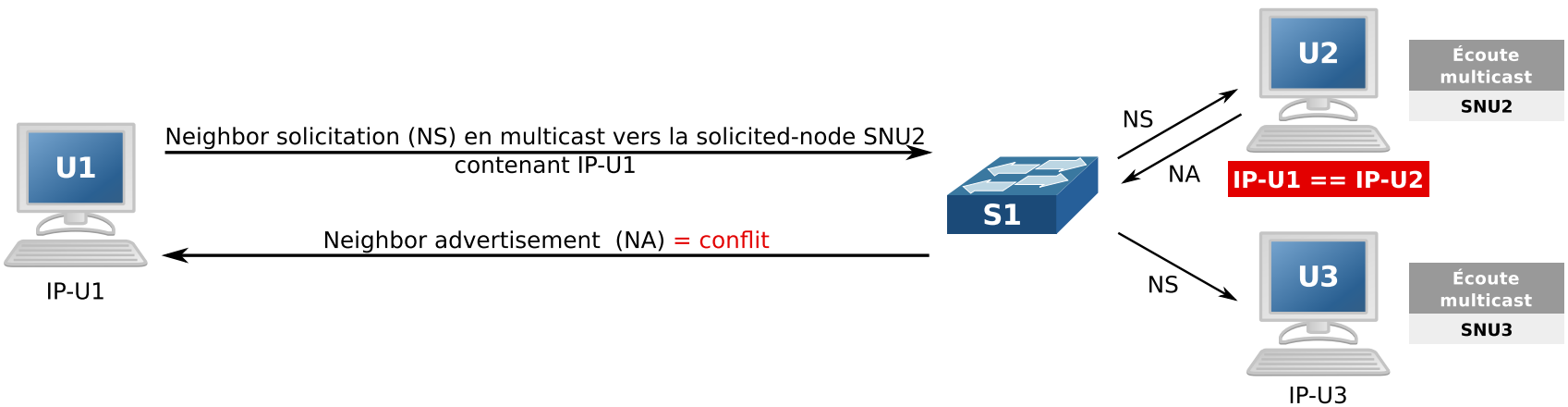
Stateless

1. Utilisation de l'adresse MAC
2. Légère transformation
3. Concaténation au(x) préfixe(s) diffusé(s)

Stateless


U1
Router solicitation en multicast vers all-routers
Router advertisement en unicast
avec un préfixe
R1
Écoute multicast
all-routers

Stateless


U1
IP-U1
Neighbor solicitation (NS) en multicast vers la solicited-node SNU2
contenant IP-U1
Neighbor advertisement (NA) = conflit
S1
NS
NA
NS
U2
Écoute multicast
SNU2
IP-U1 == IP-U2
U3
Écoute multicast
SNU3
IP-U3

Stateless

- Pas de serveurs d'attribution dédiés ☺
- Problèmes de vie privée à cause des MAC ☹
- DNS inverses (scripts) ☹

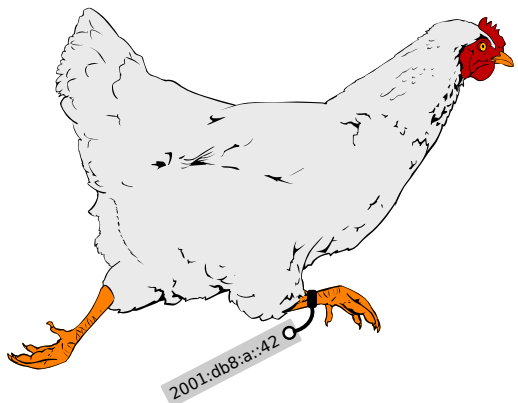
Stateless

- Diffusion des serveurs DNS (RDNSS & DNSSL) ☹
- Découverte du réseau (THC-IPv6) ☹
- Attaques diverses (DAD) ☹

Stateful

- Centralisé ☹
- DHCPv6 (diffusion IP et serveurs DNS) ☺
- DNS inverses (DDNS) ☺
- Répartition des tâches avec SLAAC ☺

Cohabitation IPv4/IPv6



Cohabitation IPv4/IPv6

- Beaucoup de solutions existantes
- **6to4/6rd inadaptés** à Lothaire
- **3 solutions** envisageables

Double-piles

- Double-piles activées par défaut ☺
- Aucun changement sur le réseau IPv4 ☺
- Double adressage ☹
- Double politique de sécurité ☹

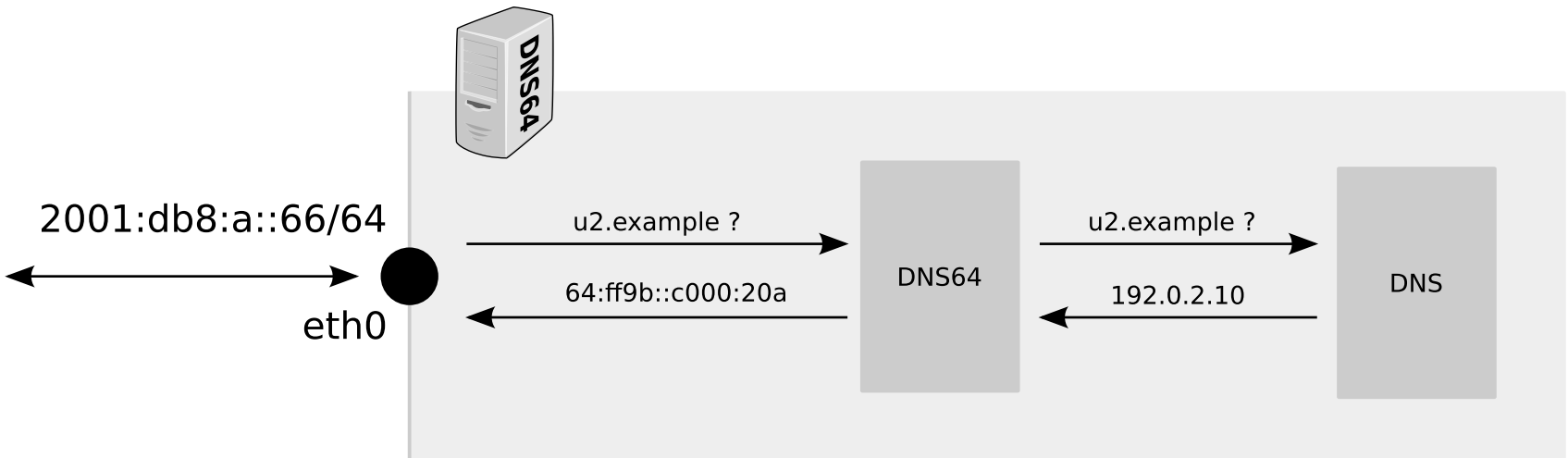
Proxies

- Réseau uniquement IPv6 ☺
- Un proxy par type de trafic ☹
- Configurations au niveau utilisateur ☹
- Goulots d'étranglement ☹

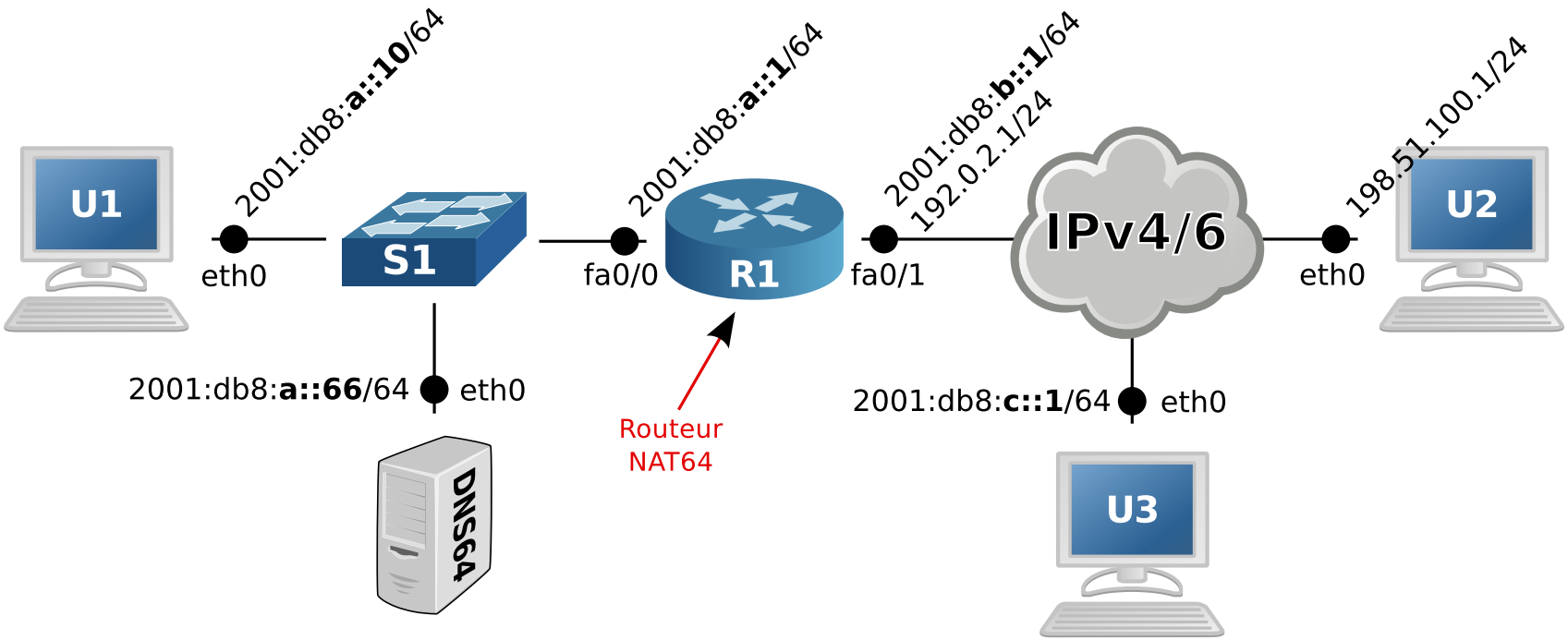
NAT64

- Réseau uniquement IPv6 ☺
- Configurations uniquement au niveau du réseau ☺
- Semble bien tenir la charge ☺
- Stateful / Stateless (**expérimentés**)

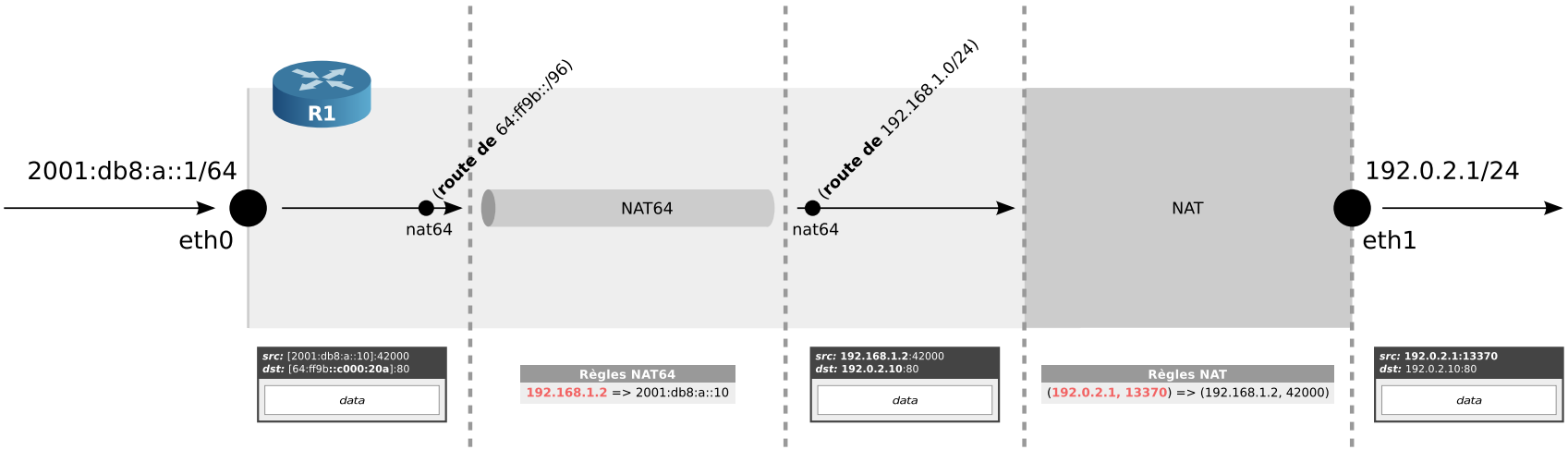
NAT64


DNS64
2001:db8:a::66/64
eth0
u2.example ?
64:ff9b::c000:20a
DNS64
u2.example ?
192.0.2.10
DNS

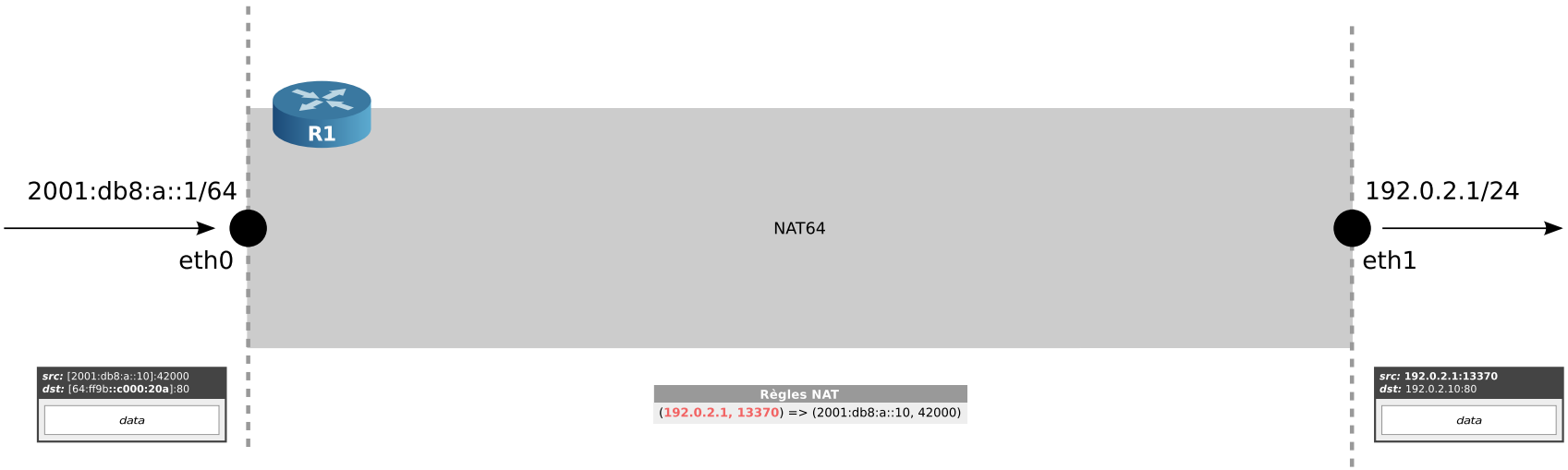
NAT64


U1
2001:db8:a::10/64
eth0
S1
2001:db8:a::1/64
fa0/0
R1
2001:db8:b::1/64
192.0.2.1/24
fa0/1
IPv4/6
198.51.100.1/24
eth0
U2
2001:db8:a::66/64
eth0
DNS64
Routeur
NAT64
2001:db8:c::1/64
eth0
U3

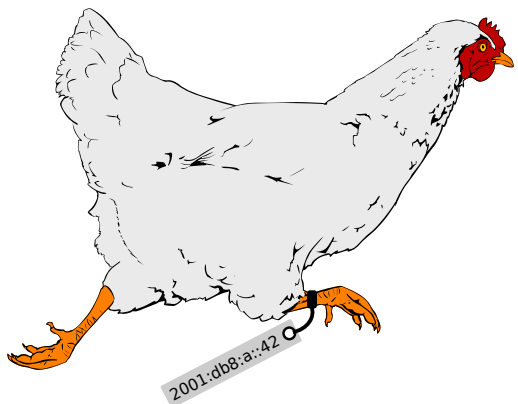
Mode stateless :



Mode stateful :



Commandes Cisco



Commandes Cisco

```
Routeur> en
Routeur# conf t
Routeur(config)# ipv6 unicast-routing
Routeur(config)# int fa 0/0
Routeur(config-if)# ipv6 addr 2001:db8:a::1/64
Routeur(config-if)# no shut
Routeur(config-if)# int fa 0/1
Routeur(config-if)# ipv6 addr 2001:db8:b::1/64
Routeur(config-if)# no shut
```

L'ARP disparaît !

```
Routeur# sh ipv6 neighbors
[...]
FE80::62FB:42FF:FEEF:E11A 0 60fb.42ef.e11a [...] Fa0/0
2001:DB8::42FF:FEEF:E11A  0 60fb.42ef.e11a [...] Fa0/0
```

Équivalent GNU/Linux :

```
# ip neigh
```

Commandes Cisco

```
Routeur(config)# ipv6 route 2001:db8:c::/64 2001:db8:a::1
Routeur(config)# ipv6 route ::/0 2001:db8:c::1
Routeur# sh ipv6 route
```

Équivalent GNU/Linux :

```
# ip route add 2001:db8:c::/64 2001:db8:a::1
# ip route add default via 2001:db8:c::1
# ip -6 route
```

Commandes Cisco

- Exemple de politique de sécurité dans Yarding (GNU/Linux) ☺
- Restrictive / Respectueuse des RFC / Utilisée en production ☺
- Pas de traduction disponible pour Cisco ☹