TechNote #4

Domain Name System

Pierre-Olivier Mercier

les bases

```
$ netcat [2a01:e35:8bb7:3c60:d263:d4ff:fe00:8332] 80
```

vs.

Les noms de domaines ?

```
$ netcat [2a01:e35:8bb7:3c60:d263:d4ff:fe00:8332] 80
```

vs.

```
$ netcat you.p0m.fr 80
```

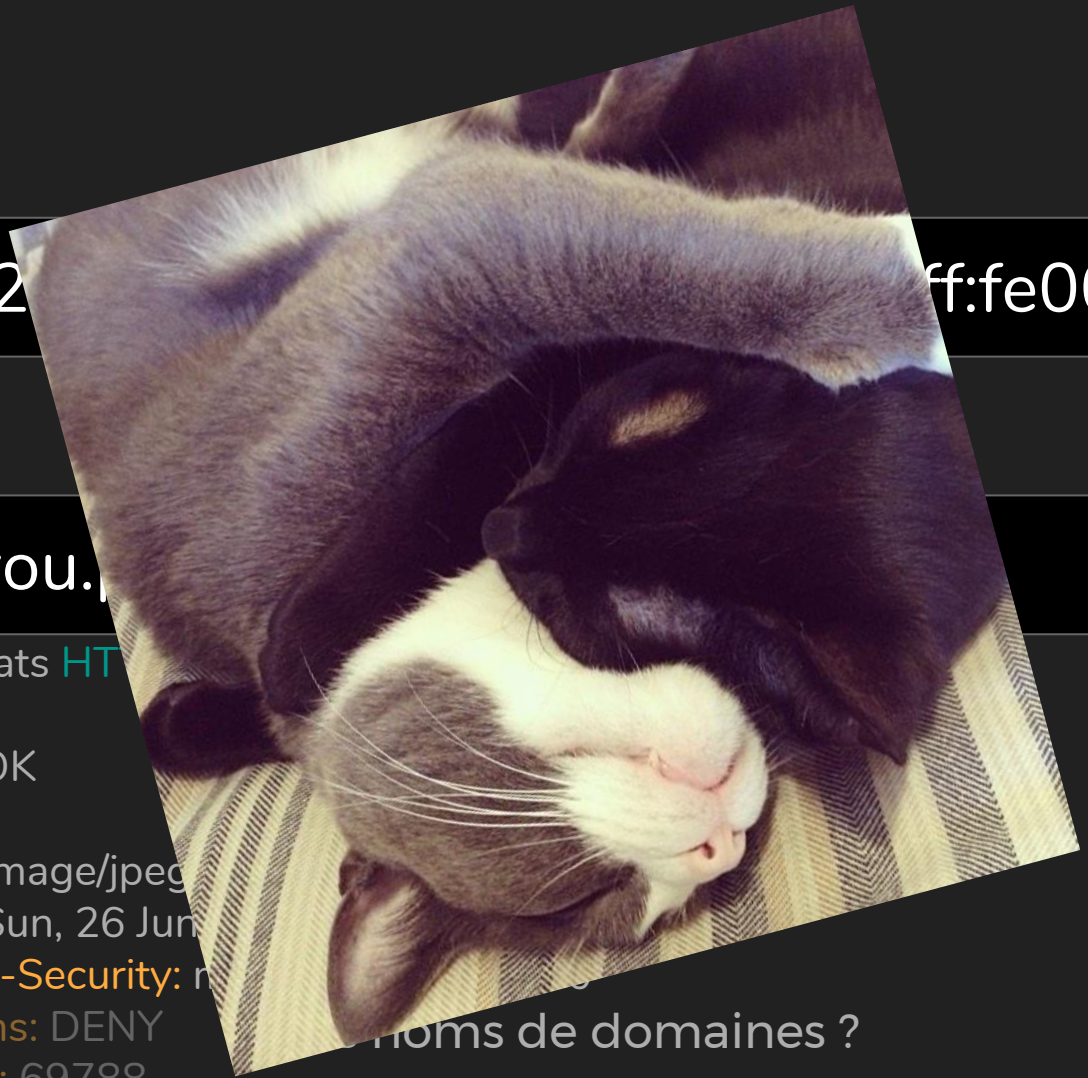
Les noms de domaines ?

$ netcat [2 ff:fe00:8332] 80

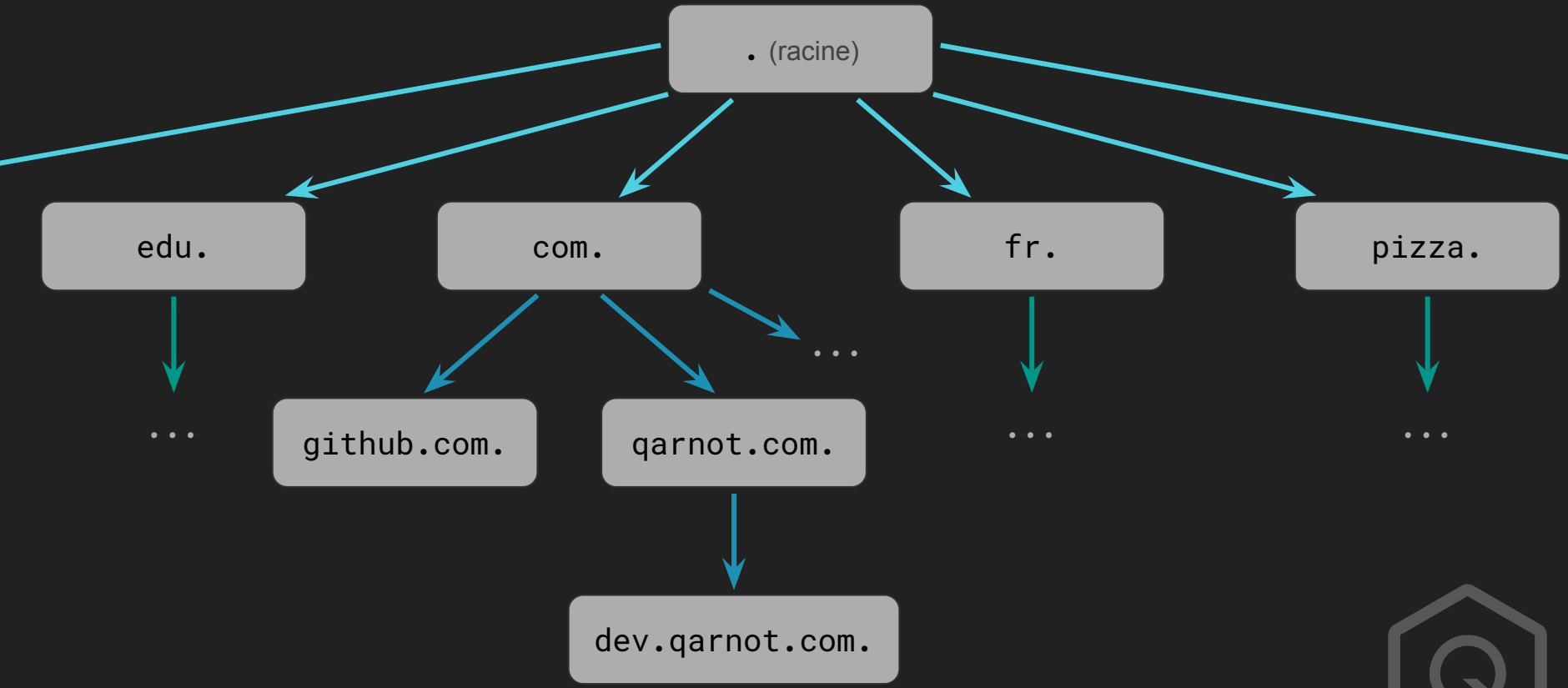
$ netcat you.

GET /images/chats HT

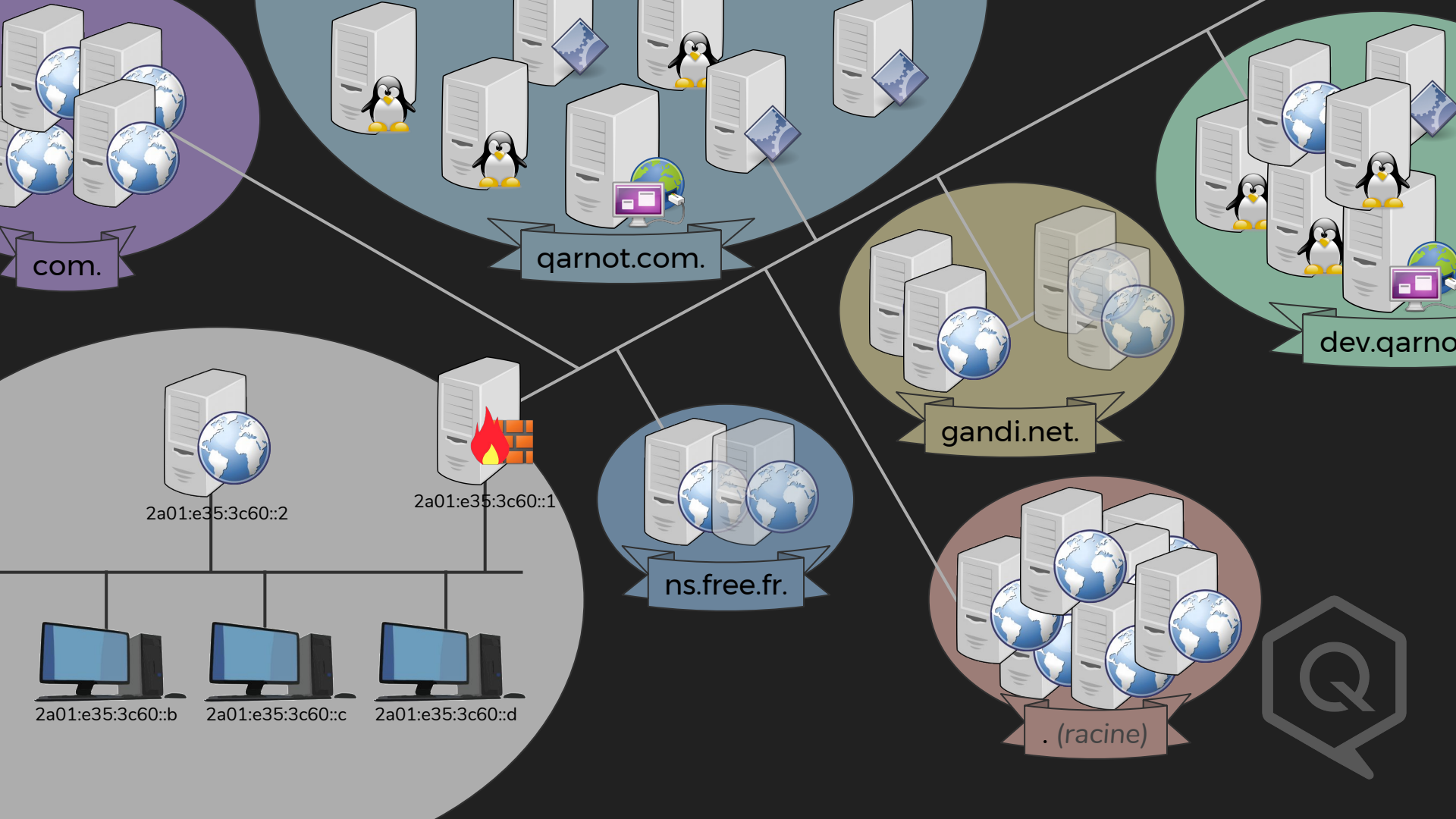
HTTP/1.0 200 OK
Server: nginx
Content-Type: image/jpeg
Last-Modified: Sun, 26 Jun
Strict-Transport-Security: m
X-Frame-Options: DENY
Content-Length: 69788

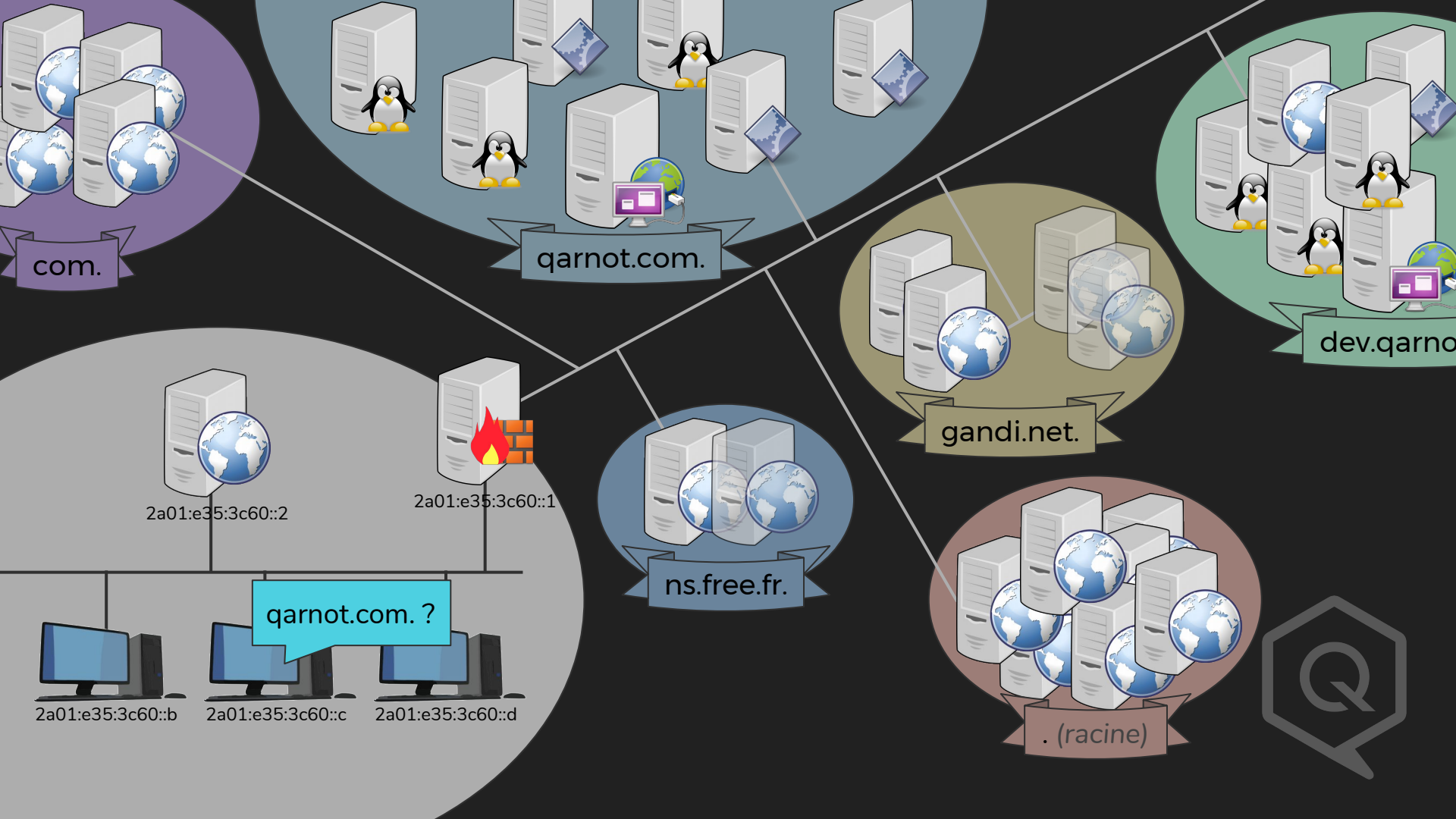


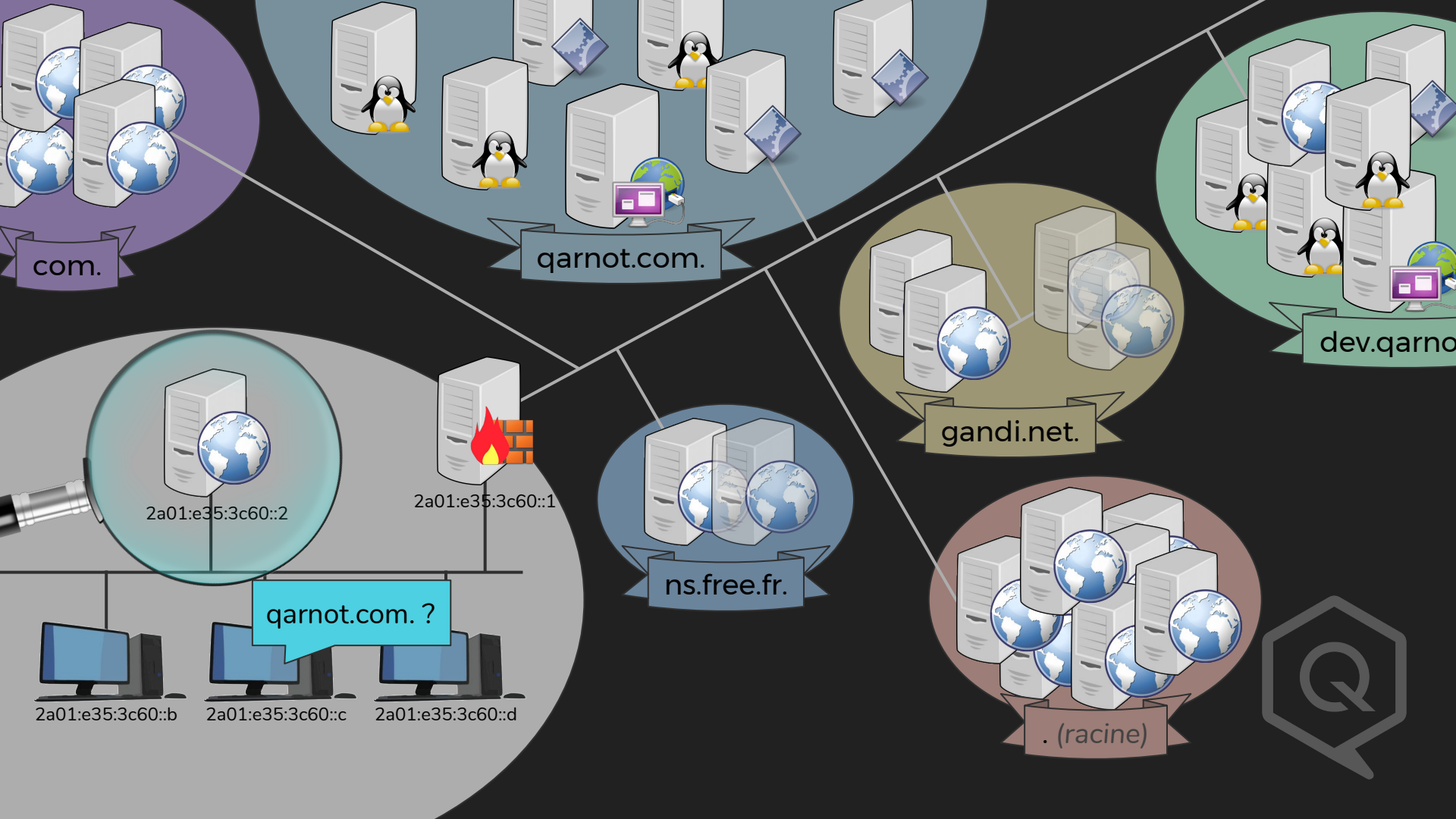
noms de domaines ?

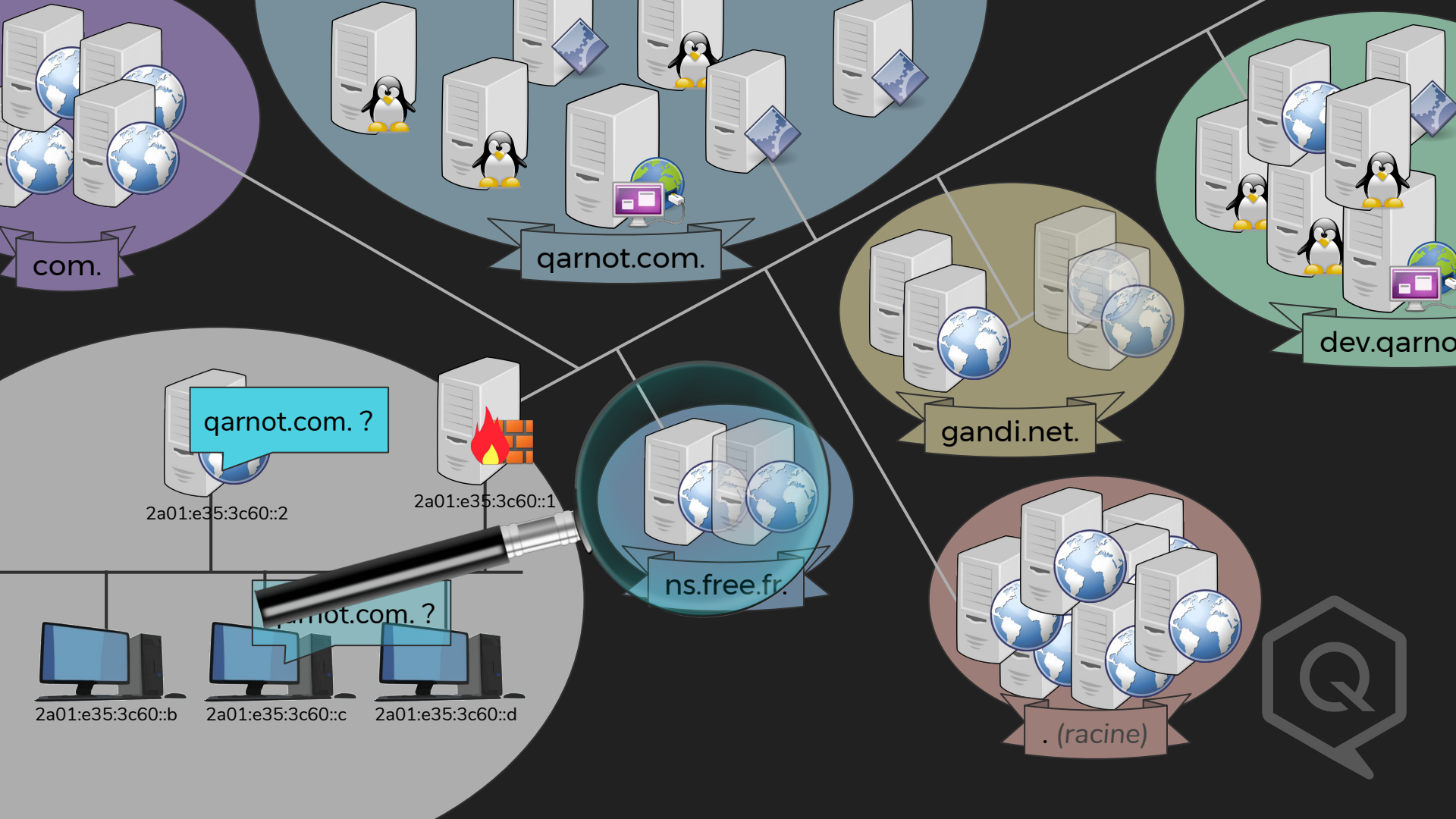


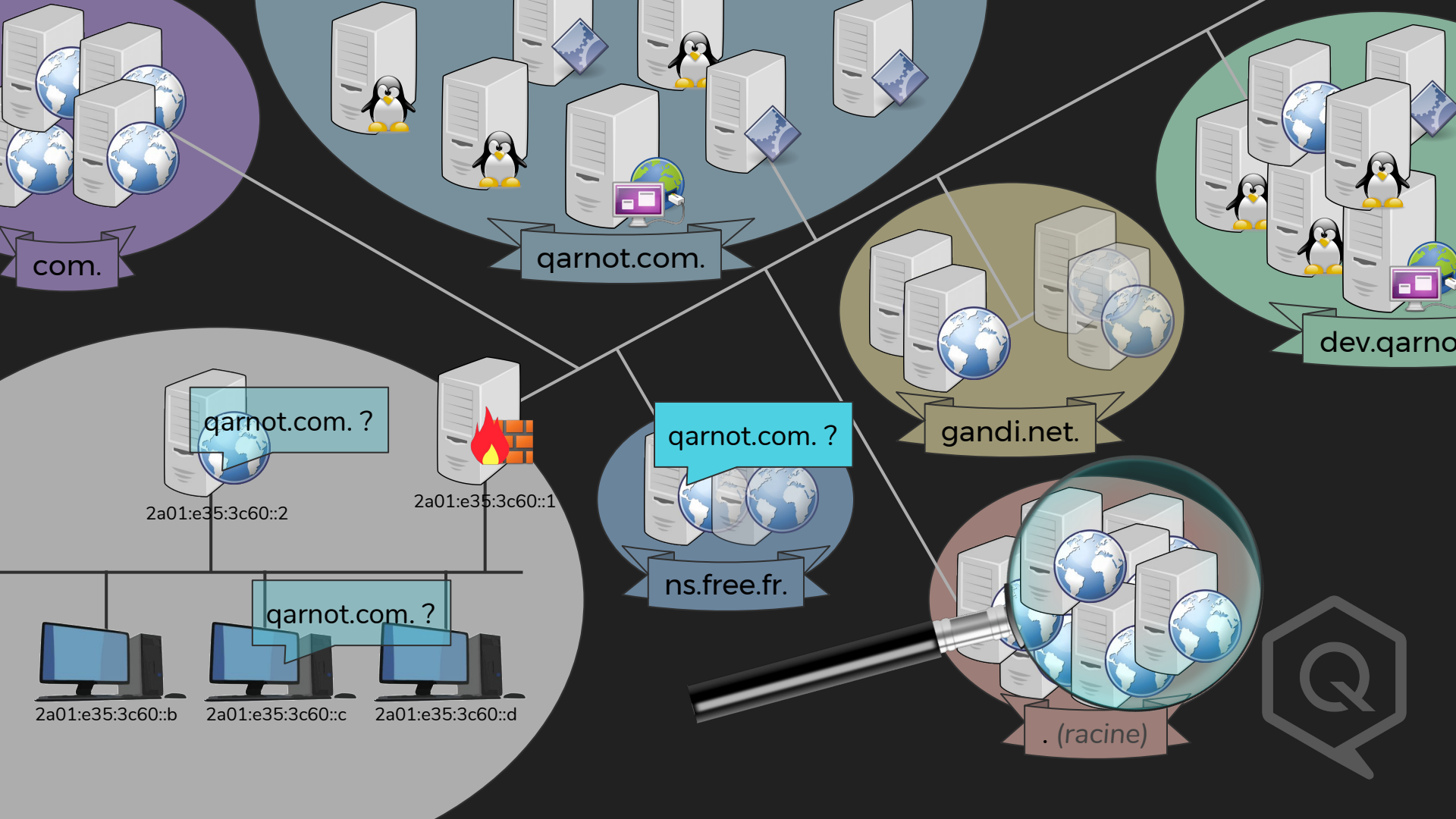
L’arbre du DNS

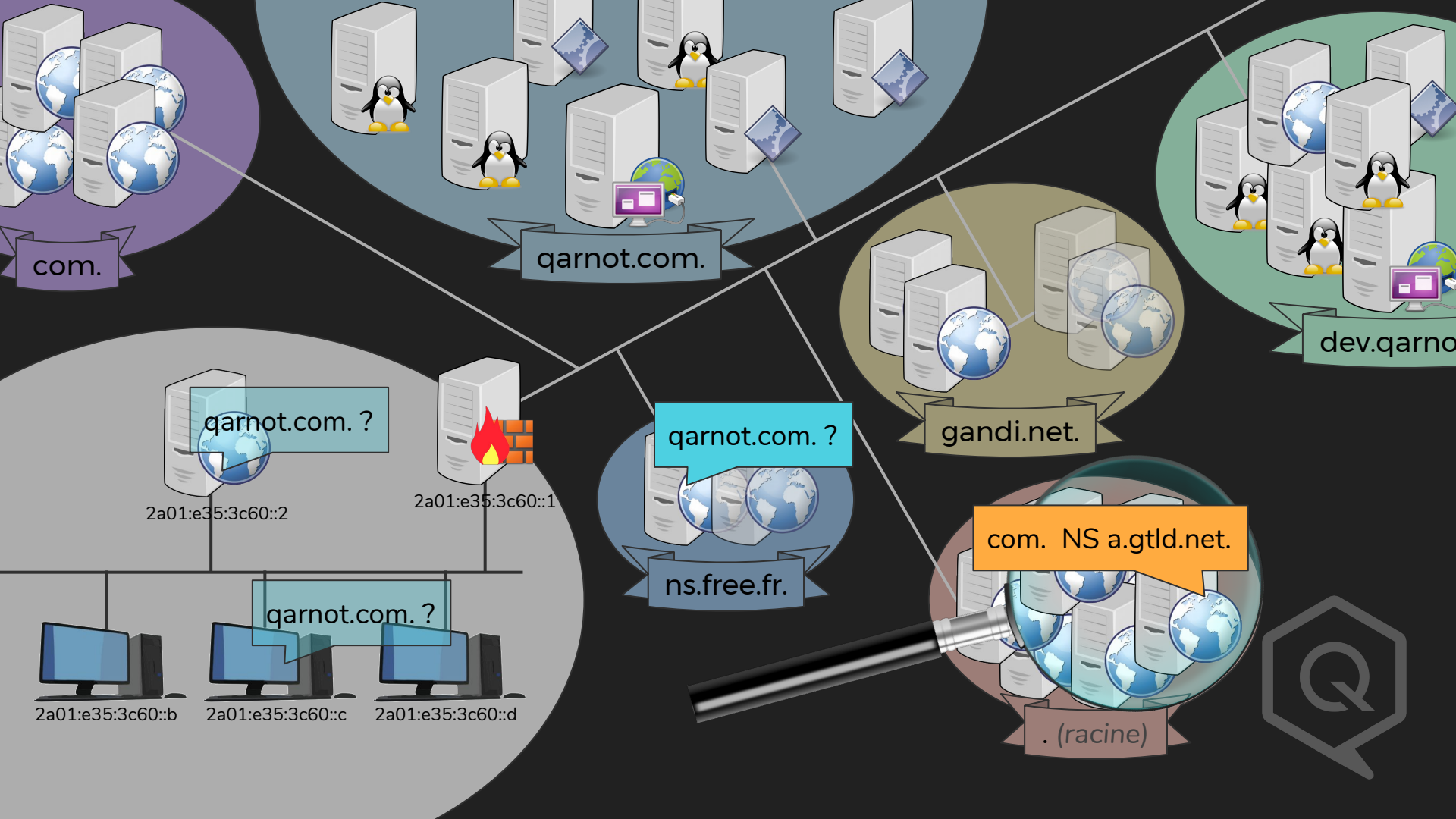

com.
qarnot.com.
dev.qarno
gandi.net.
ns.free.fr.
. (racine)
2a01:e35:3c60::2
2a01:e35:3c60::1
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d

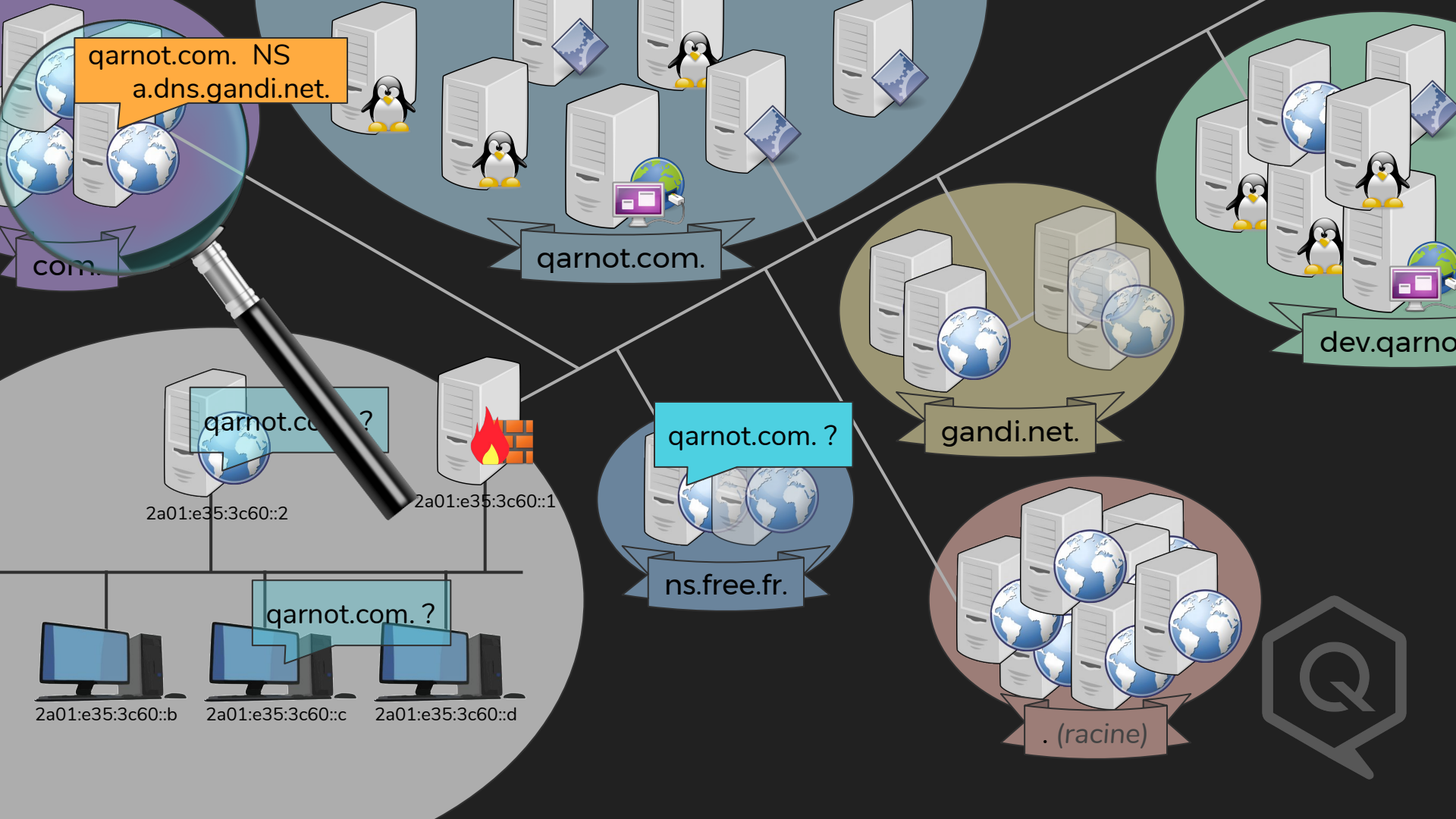

com.
qarnot.com.
dev.qarno
gandi.net.
ns.free.fr.
. (racine)
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d

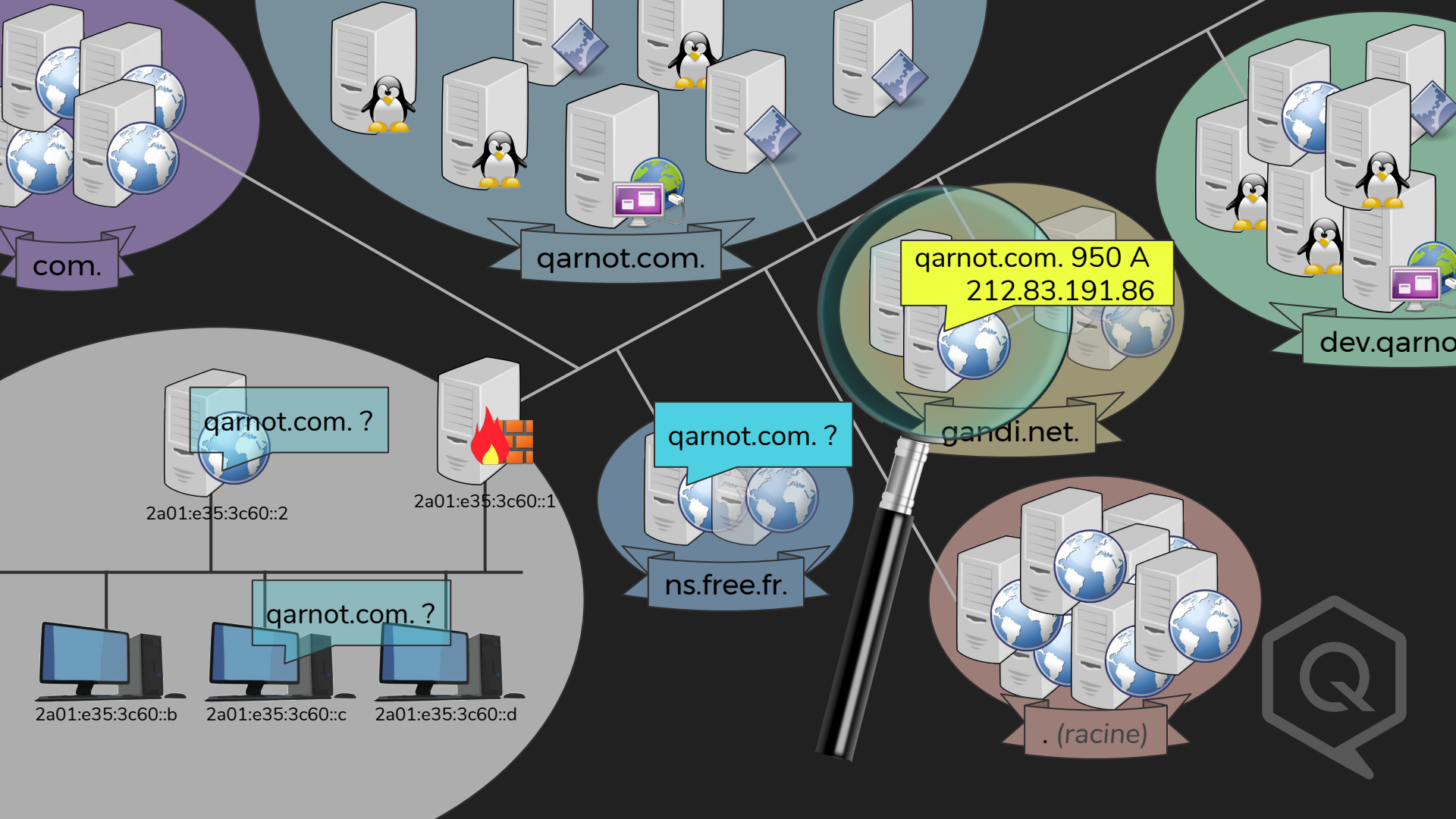

com.
qarnot.com.
dev.qarno
gandi.net.
ns.free.fr.
. (racine)
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d

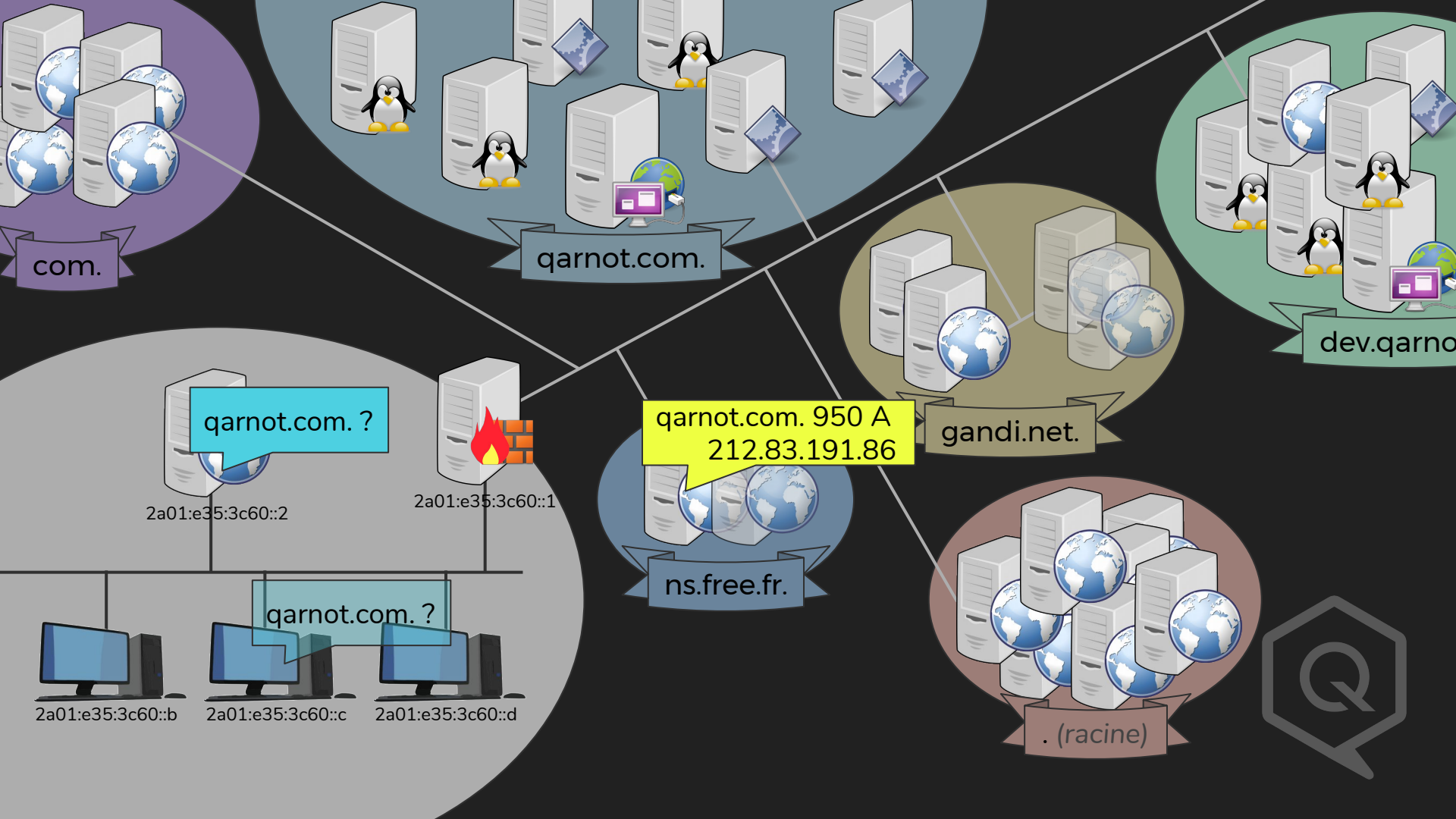

com.
qarnot.com.
dev.qarno
gandi.net.
qarnot.com. ?
2a01:e35:3c60::2
2a01:e35:3c60::1
ns.free.fr.
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

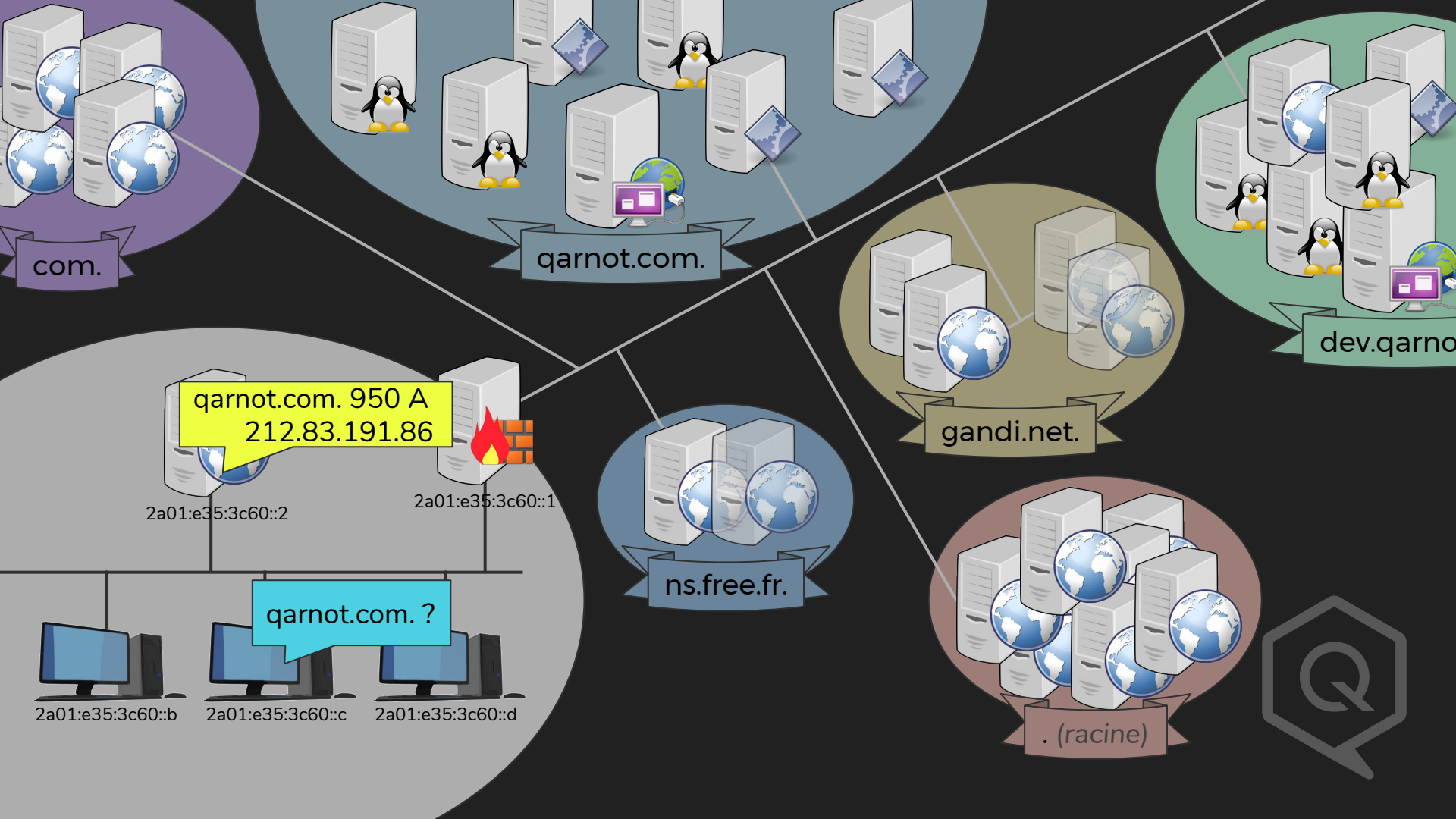

com.
qarnot.com.
gandi.net.
dev.qarno
qarnot.com. ?
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. ?
ns.free.fr.
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

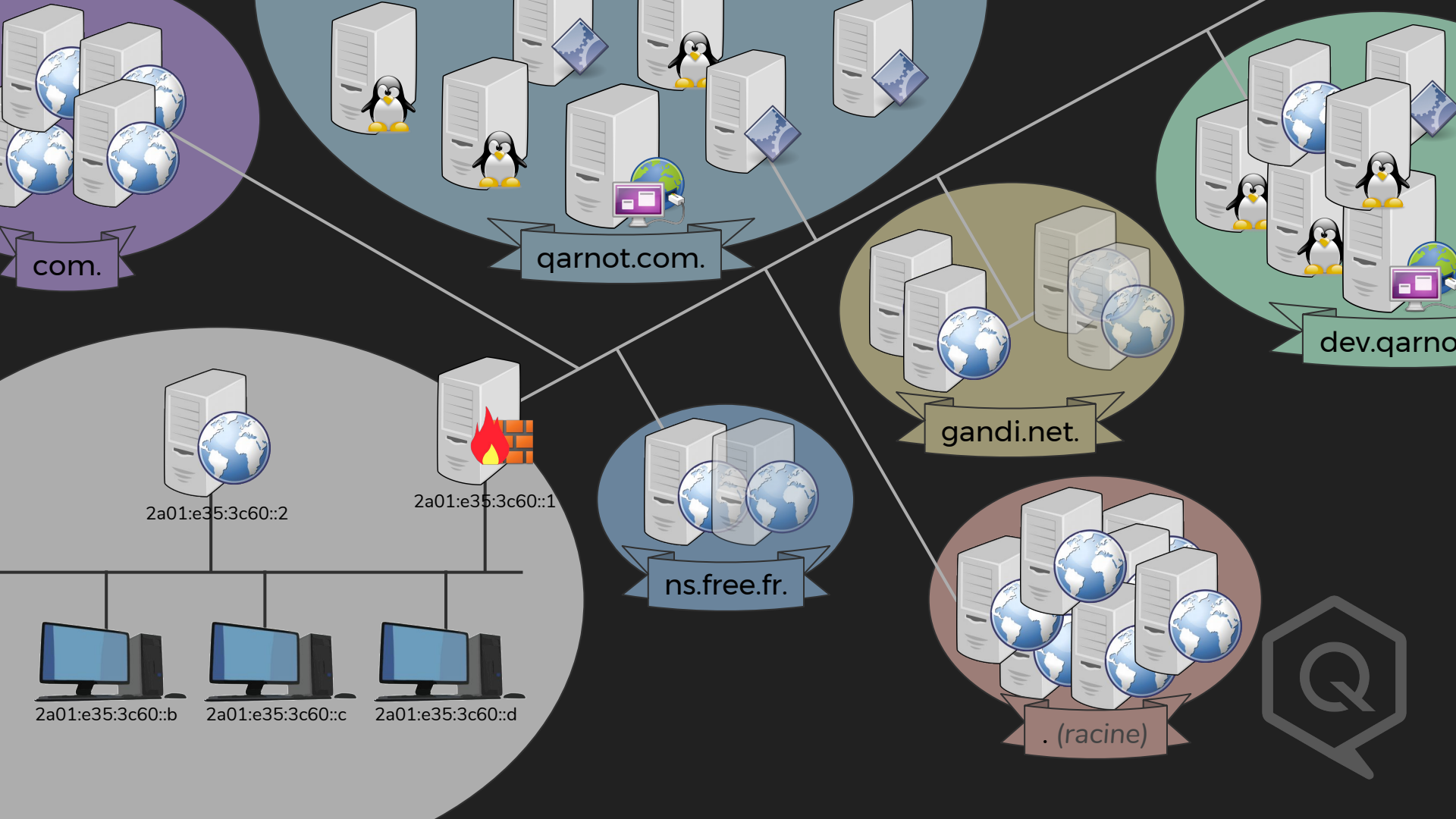

com.
qarnot.com.
gandi.net.
dev.qarno
qarnot.com. ?
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. ?
ns.free.fr.
com. NS a.gtld.net.
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

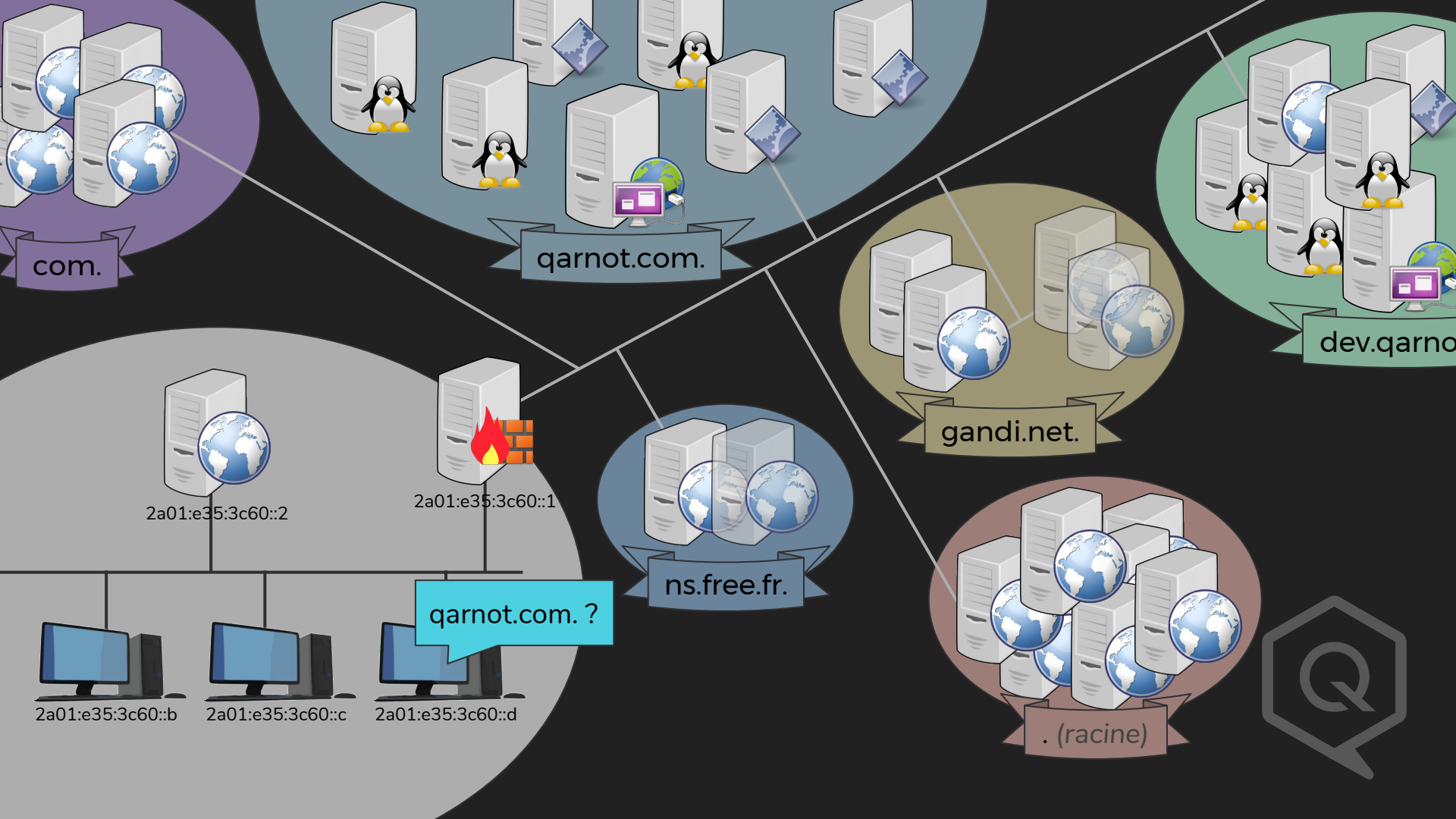

qarnot.com. NS
a.dns.gandi.net.
com.
qarnot.com.
dev.qarno
gandi.net.
qarnot.com. ?
ns.free.fr.
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

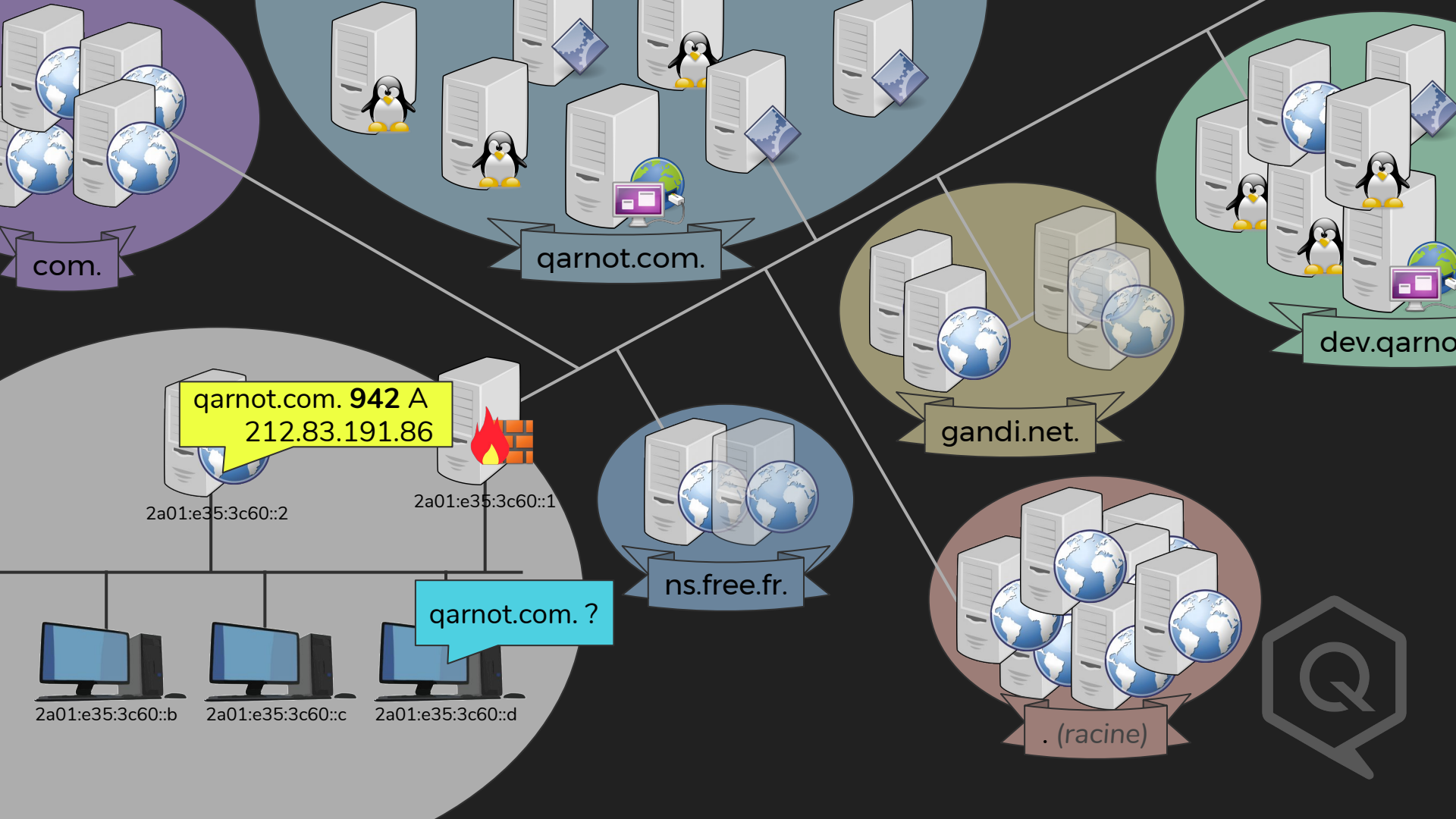

com.
qarnot.com.
qarnot.com. 950 A
212.83.191.86
gandi.net.
dev.qarno
qarnot.com. ?
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. ?
ns.free.fr.
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

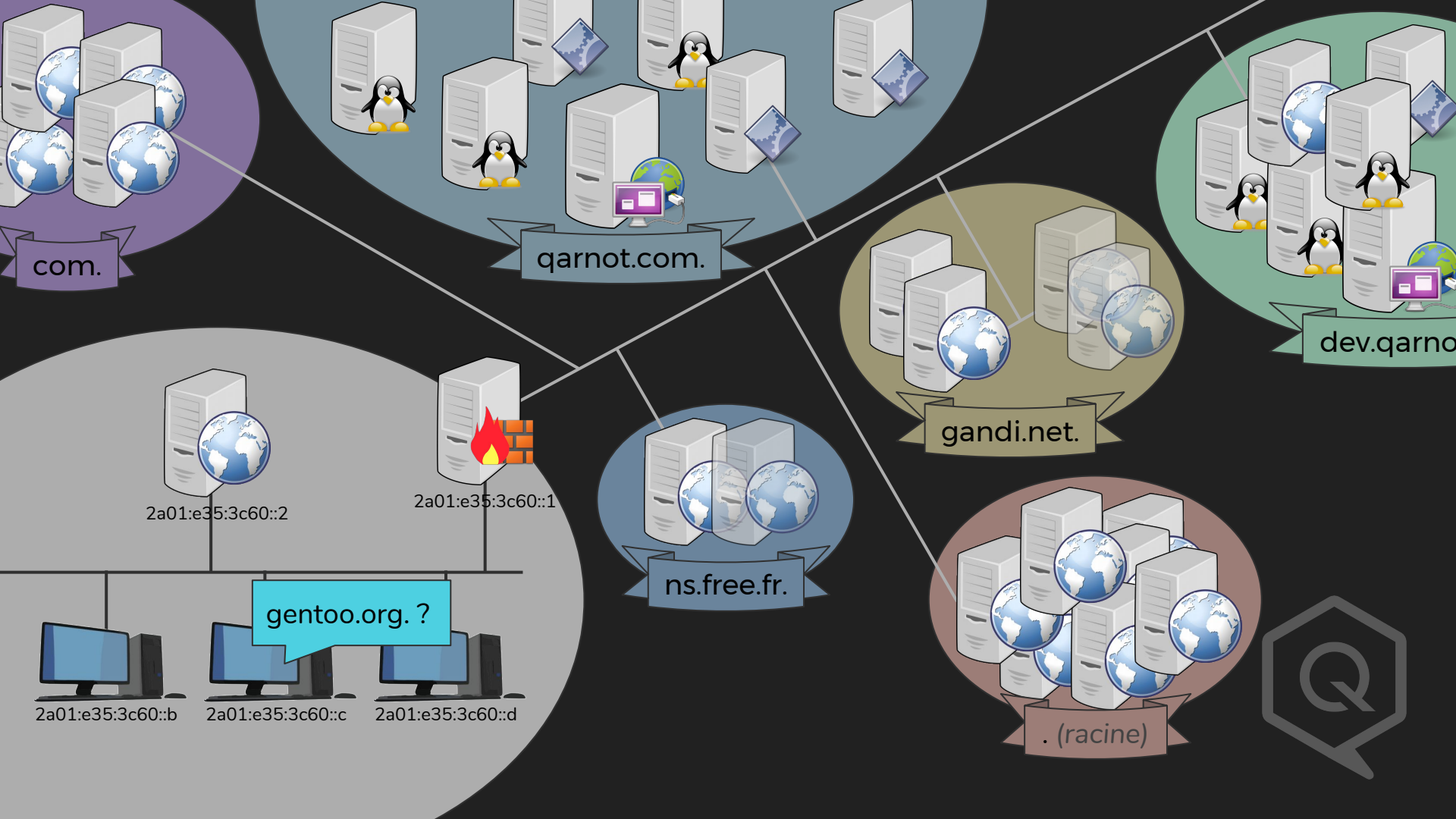

com.
qarnot.com.
dev.qarno
gandi.net.
qarnot.com. ?
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. 950 A
212.83.191.86
ns.free.fr.
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

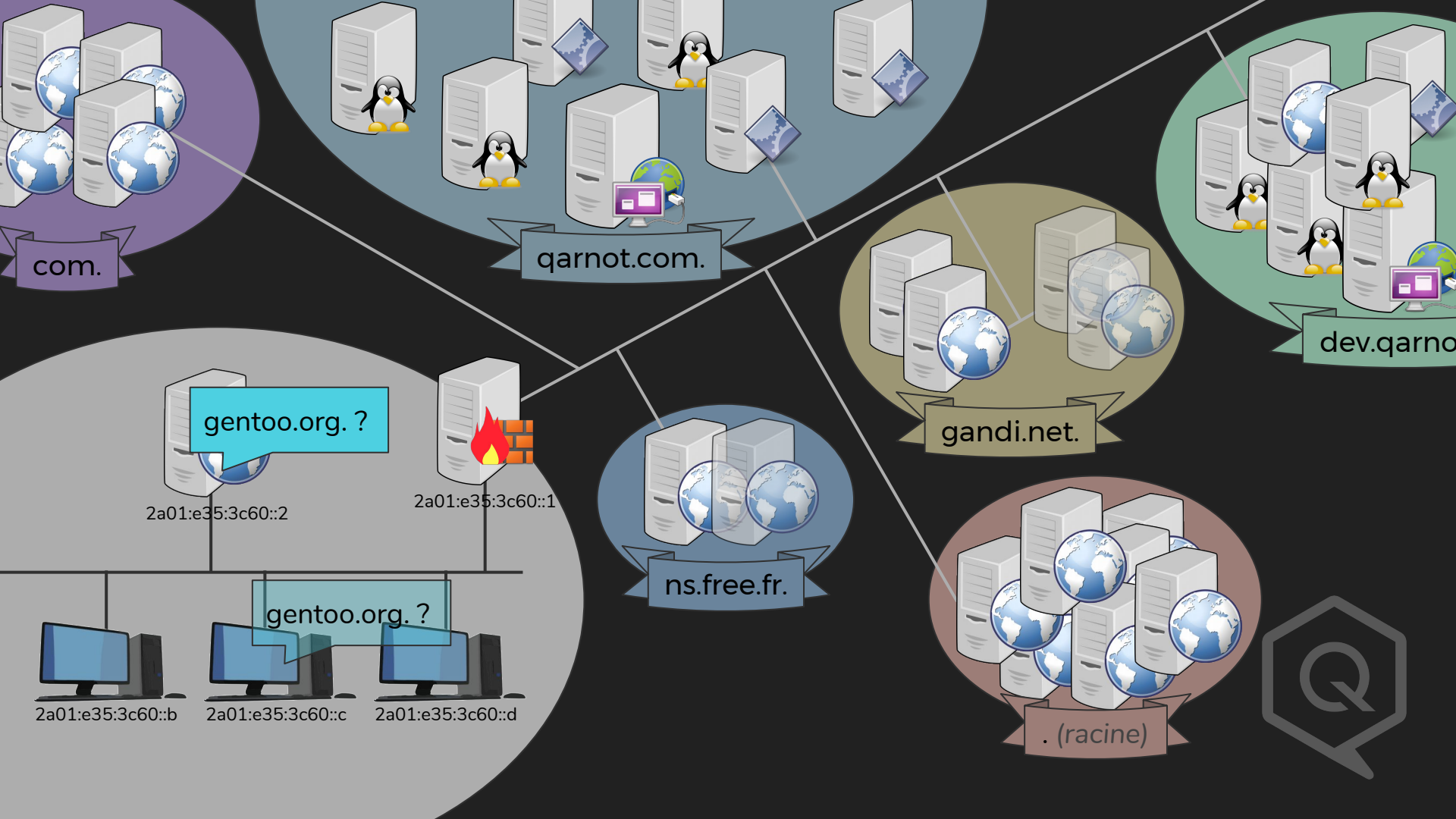

com.
qarnot.com.
dev.qarno
gandi.net.
ns.free.fr.
. (racine)
qarnot.com. 950 A
212.83.191.86
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d

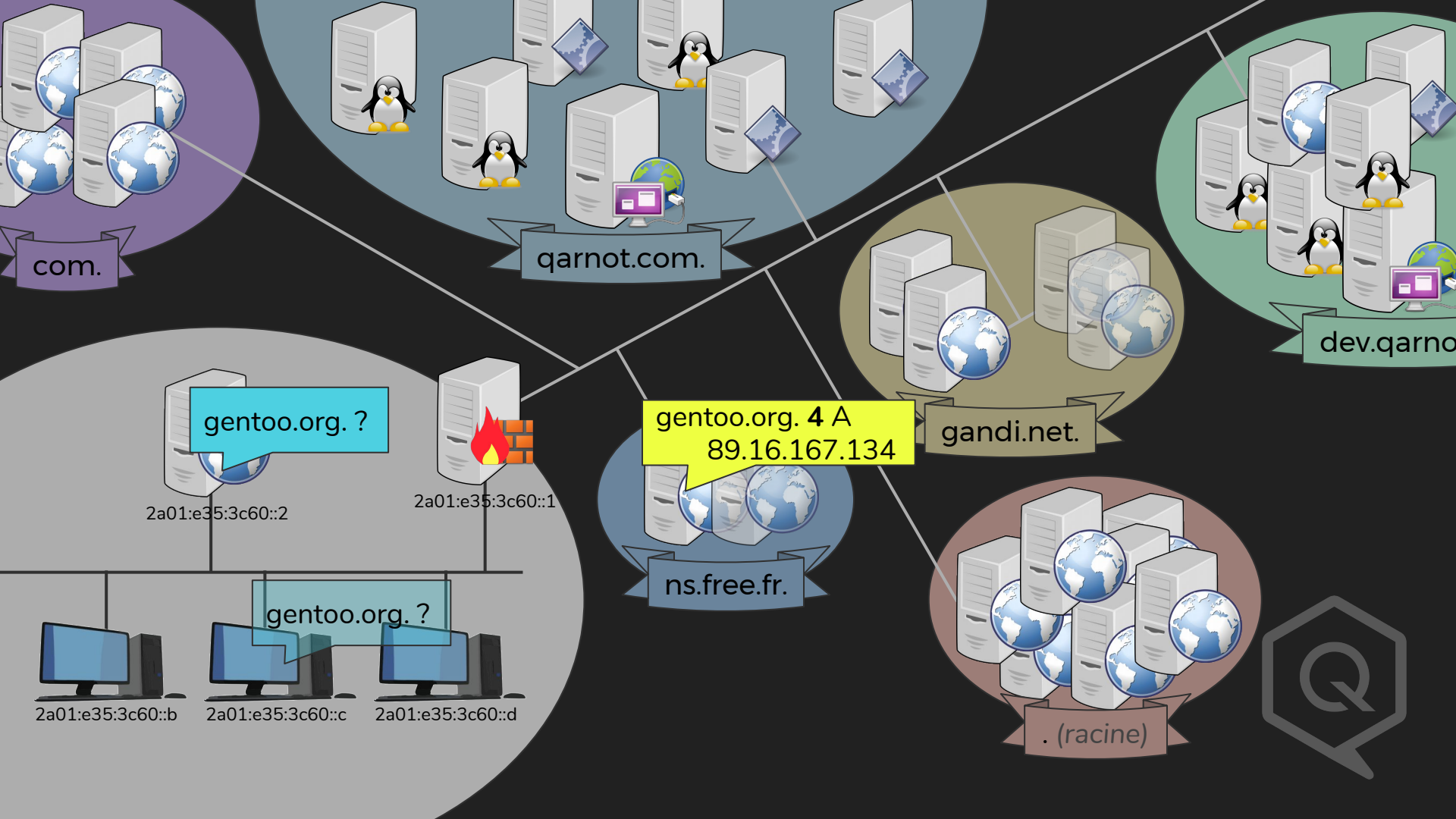

com.
qarnot.com.
dev.qarno
gandi.net.
ns.free.fr.
. (racine)
2a01:e35:3c60::2
2a01:e35:3c60::1
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d

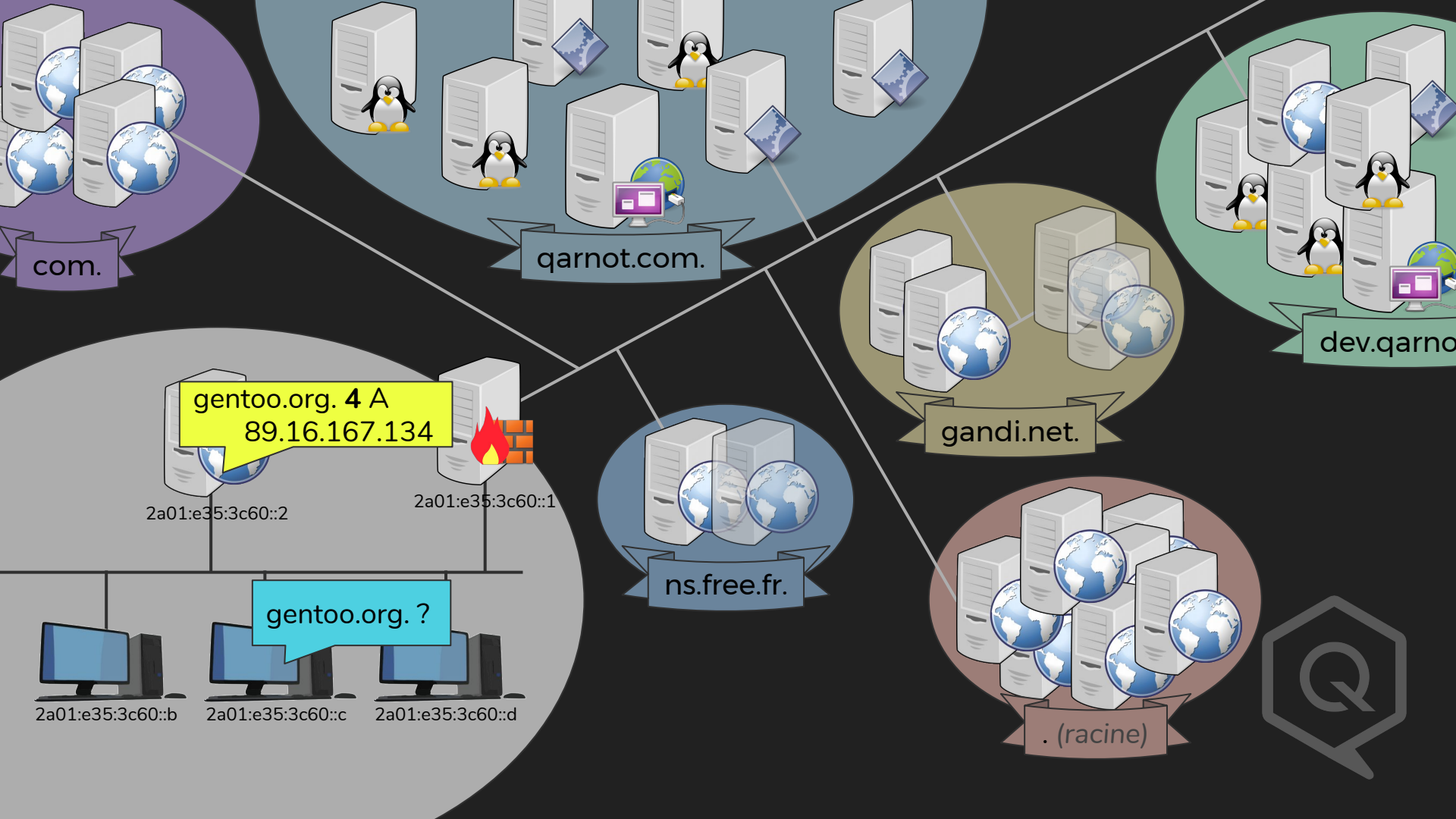

com.
qarnot.com.
dev.qarno
gandi.net.
ns.free.fr.
. (racine)
2a01:e35:3c60::2
2a01:e35:3c60::1
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d

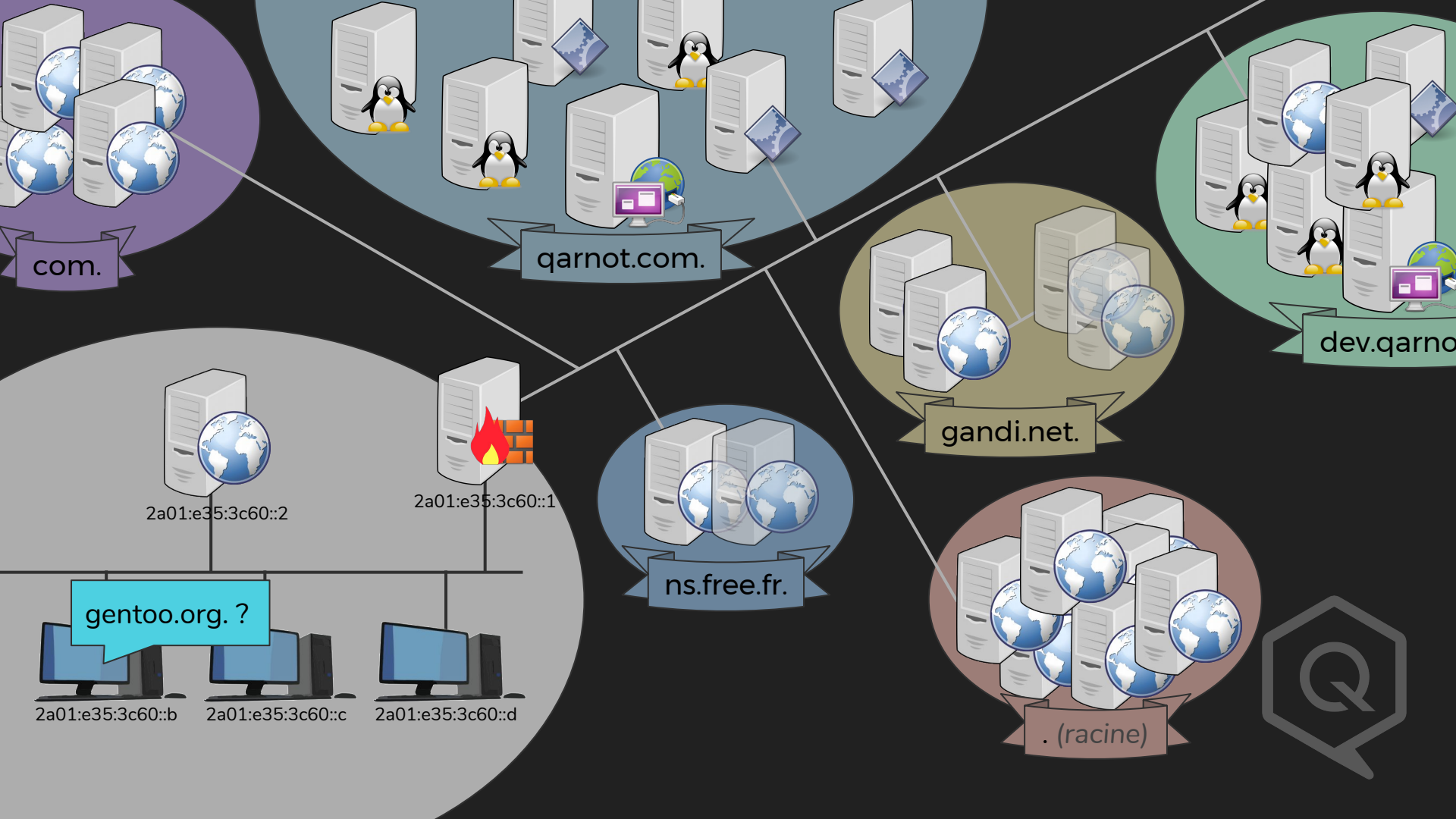

com.
qarnot.com.
dev.qarno
gandi.net.
qarnot.com. 942 A
212.83.191.86
2a01:e35:3c60::2
2a01:e35:3c60::1
ns.free.fr.
qarnot.com. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

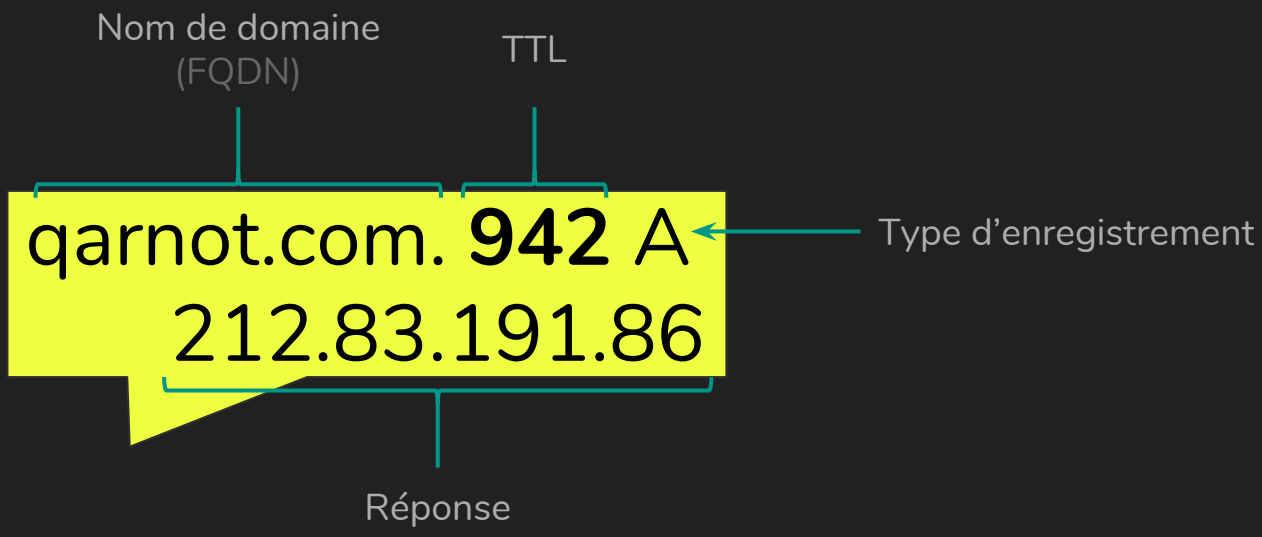

com.
qarnot.com.
dev.qarno
gandi.net.
ns.free.fr.
. (racine)
2a01:e35:3c60::2
2a01:e35:3c60::1
gentoo.org. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d


com.
qarnot.com.
dev.qarno
gandi.net.
gentoo.org. ?
2a01:e35:3c60::2
2a01:e35:3c60::1
ns.free.fr.
gentoo.org. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

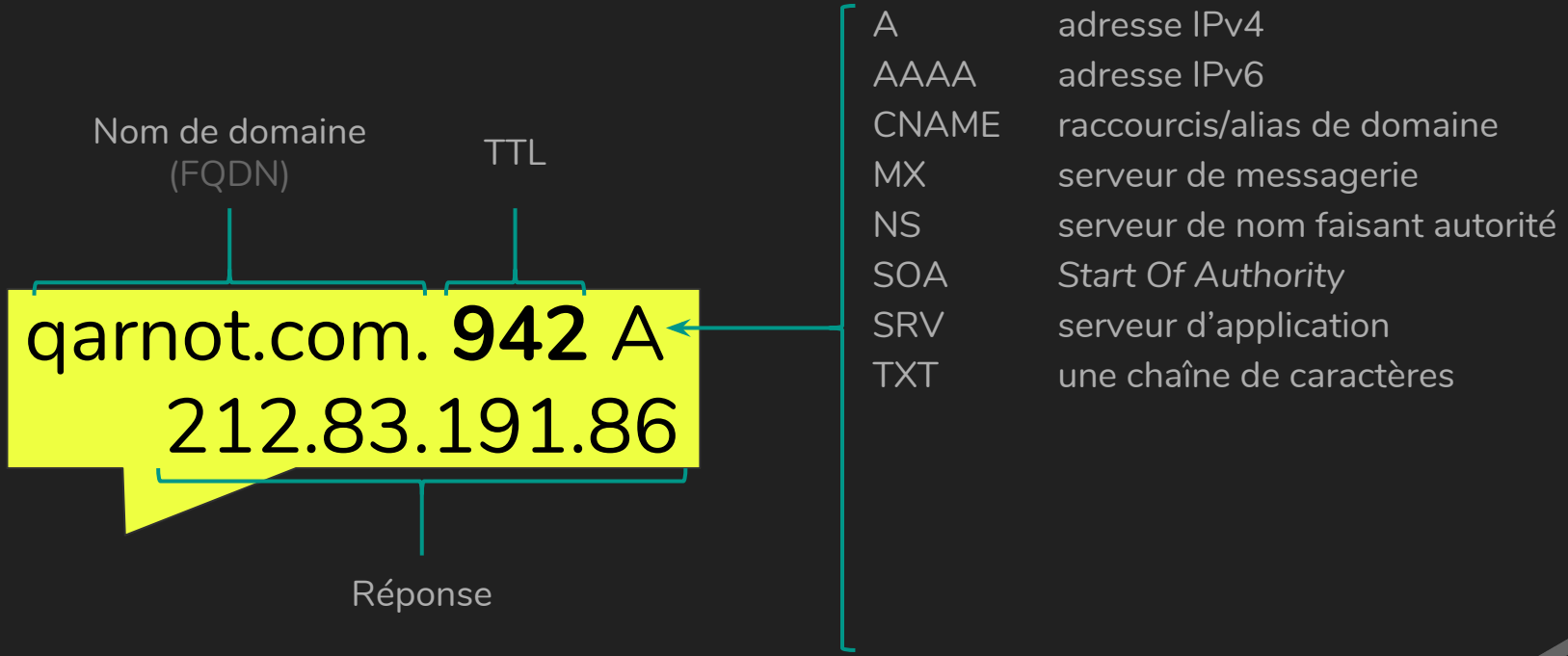

com.
qarnot.com.
dev.qarno
gandi.net.
gentoo.org. ?
2a01:e35:3c60::2
2a01:e35:3c60::1
gentoo.org. 4 A
89.16.167.134
ns.free.fr.
gentoo.org. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)


com.
qarnot.com.
dev.qarno
gandi.net.
gentoo.org. 4 A
89.16.167.134
2a01:e35:3c60::2
2a01:e35:3c60::1
ns.free.fr.
gentoo.org. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d
. (racine)

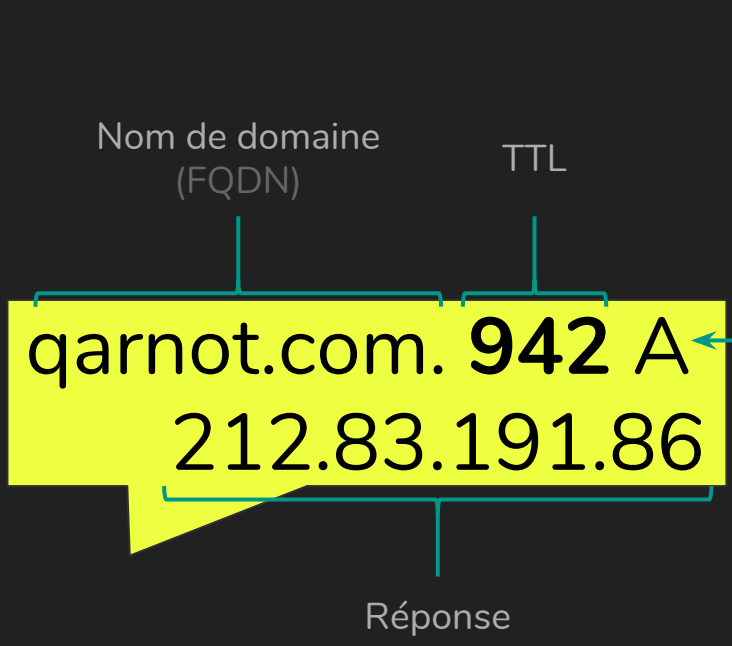

com.
qarnot.com.
dev.qarno
gandi.net.
ns.free.fr.
. (racine)
2a01:e35:3c60::2
2a01:e35:3c60::1
gentoo.org. ?
2a01:e35:3c60::b
2a01:e35:3c60::c
2a01:e35:3c60::d


Nom de domaine
(FQDN)
TTL
qarnot.com. 942 A
212.83.191.86
Type d'enregistrement
Réponse

Réponse DNS


Nom de domaine
(FQDN)
TTL
qarnot.com. 942 A
212.83.191.86
Réponse
A adresse IPv4
AAAA adresse IPv6
CNAME raccourcis/alias de domaine
MX serveur de messagerie
NS serveur de nom faisant autorité
SOA Start Of Authority
SRV serveur d'application
TXT une chaîne de caractères

Réponse DNS

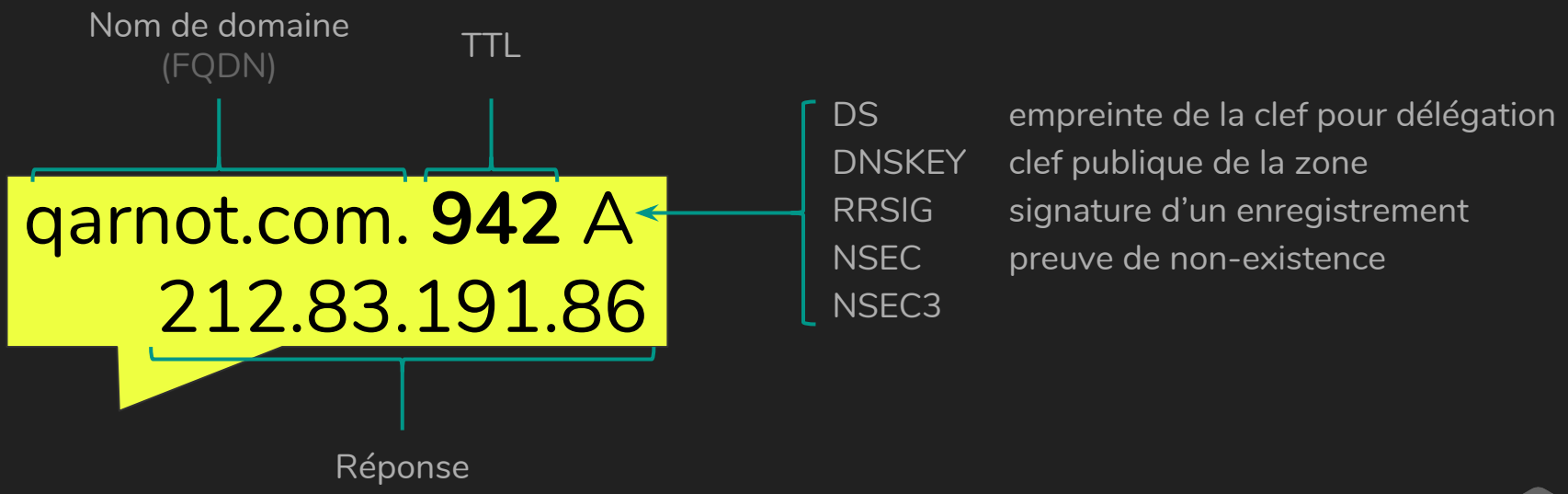


A	adresse IPv4
AAAA	adresse IPv6
CNAME	raccourcis/alias de domaine
MX	serveur de messagerie
NS	serveur de nom faisant autorité
SOA	*Start Of Authority*
SRV	serveur d'application
TXT	une chaîne de caractères

DANE

CAA	autorisation d'autorité de certification
SSHFP	empreinte clef publique SSH
TLSA	empreinte certificat X.509
OPENPGPKEY	clef publique PGP

Réponse DNS


Nom de domaine
(FQDN)
TTL
qarnot.com. 942 A
212.83.191.86
Réponse
DS empreinte de la clef pour délégation
DNSKEY clef publique de la zone
RRSIG signature d'un enregistrement
NSEC preuve de non-existence
NSEC3

Réponse DNS

Exercices

Exercices

qarnot.com. MX?

Exercice

qarnot.com. MX?

qarnot.com. 28800 MX 1 ASPMX.L.GOOGLE.COM.
qarnot.com. 28800 MX 3 ALT1.ASPMX.L.GOOGLE.COM.
qarnot.com. 28800 MX 3 ALT2.ASPMX.L.GOOGLE.COM.
qarnot.com. 28800 MX 5 ASPMX2.GOOGLEMAIL.COM.
qarnot.com. 28800 MX 5 ASPMX3.GOOGLEMAIL.COM.

qarnot.com. MX?

qarnot.com. 28800 MX **1** ASPMX.L.GOOGLE.COM.
qarnot.com. 28800 MX **3** ALT1.ASPMX.L.GOOGLE.COM.
qarnot.com. 28800 MX **3** ALT2.ASPMX.L.GOOGLE.COM.
qarnot.com. 28800 MX **5** ASPMX2.GOOGLEMAIL.COM.
qarnot.com. 28800 MX **5** ASPMX3.GOOGLEMAIL.COM.

_qaiot._tcp.frigg.dev.qarnot.com. SRV?

Exercice

DNS-Based Service Discovery

RFC 6763

_qaiot._tcp.frigg.dev.qarnot.com. SRV?

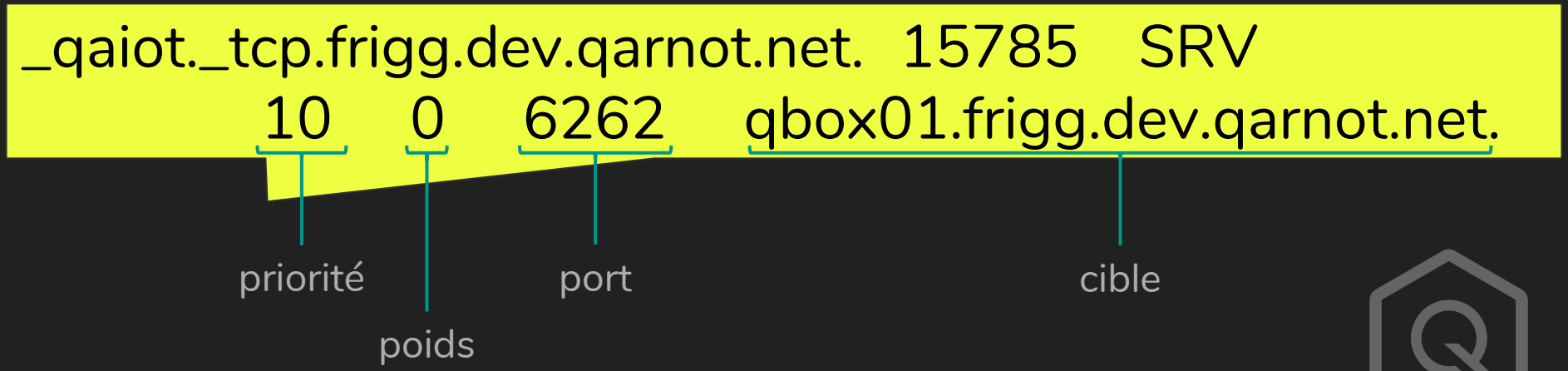
Exercice

_qaiot._tcp.frigg.dev.qarnot.com. SRV?

```
_qaiot._tcp.frigg.dev.qarnot.net.  15785  SRV
        10  0  6262  qbox01.frigg.dev.qarnot.net.
```

Exercice

_qaiot._tcp.frigg.dev.qarnot.com. SRV?



```
@  3600 IN  SOA   a.dns.gandi.net. hostmaster.gandi.net. (
                  2017072400     ; Serial
                  10800          ; Refresh
                  3600           ; Retry
                  604800         ; Expiry
                  10800 )        ; Negative Cache TTL

@  86400   IN  NS    a.dns.gandi.net.
   86400   IN  NS    b.dns.gandi.net.

www 900    IN  A     212.83.191.86
```

Notions avancées

Zone

```
@ 10800 IN SOA a.dns.gandi.net.
      hostmaster.gandi.net. 2017071700
      10800 3600 604800 10800
@ 10800 IN NS a.dns.gandi.net.
@ 10800 IN NS b.dns.gandi.net.
@ 3600 IN A 212.83.190.173
@ 3600 IN A 212.83.191.86
blender 3600 IN A 212.129.29.215
compute 10800 IN CNAME computing
computing 3600 IN CNAME www
console 3600 IN CNAME www
credits 3600 IN CNAME www
developer 3600 IN CNAME www
login 10800 IN CNAME sso-front01
storage 10800 IN A 87.98.180.1
storage 10800 IN A 92.222.155.233
sso-front01 3600 IN A 212.129.18.149
sso-back01 10800 IN CNAME sso-back
workers 3600 IN A 217.182.239.19
www  3600 IN A 163.172.121.37
...
```

Enregistrement

Resource Record (RR)

```
qarnot.com.   3600 IN A 212.83.190.173
              3600 IN A 212.83.191.86
```

Entrée

```
qarnot.com.   3600 IN A 212.83.190.173
```

Vocabulaire

qarnot.com. ANY ?

Exercice

qarnot.com. ANY ?

```
qarnot.com.  3600     A    212.83.190.173
qarnot.com.  3600     A    212.83.191.86
qarnot.com.  28800    MX 1 ASPMX.L.GOOGLE.COM.
qarnot.com.  28800    MX 3 ALT1.ASPMX.L.GOOGLE.COM.
qarnot.com.  28800    MX 3 ALT2.ASPMX.L.GOOGLE.COM.
qarnot.com.  28800    MX 5 ASPMX2.GOOGLEMAIL.COM.
qarnot.com.  28800    MX 5 ASPMX3.GOOGLEMAIL.COM.
qarnot.com.  10800    NS  a.dns.gandi.net.
qarnot.com.  10800    NS  b.dns.gandi.net.
qarnot.com.  10800    NS  c.dns.gandi.net.
```

heat.qarnot.com. A ?

Exercice

heat.qarnot.com. A ?

heat.qarnot.com. 1800 CNAME www.qarnot.com.

Exercice

heat.qarnot.com. A ?

heat.qarnot.com. 1800 CNAME www.qarnot.com.

www.qarnot.com. 3600 A 212.83.190.173

Exercice

wikimedia.org. NS ?

Exercice

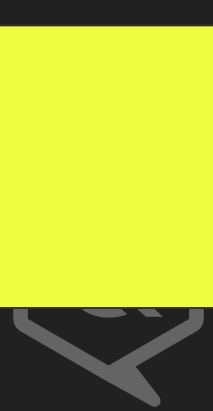
wikimedia.org. NS ?

```
wikimedia.org. 86400    NS    ns0.wikimedia.org.
wikimedia.org. 86400    NS    ns1.wikimedia.org.
wikimedia.org. 86400    NS    ns2.wikimedia.org.
```

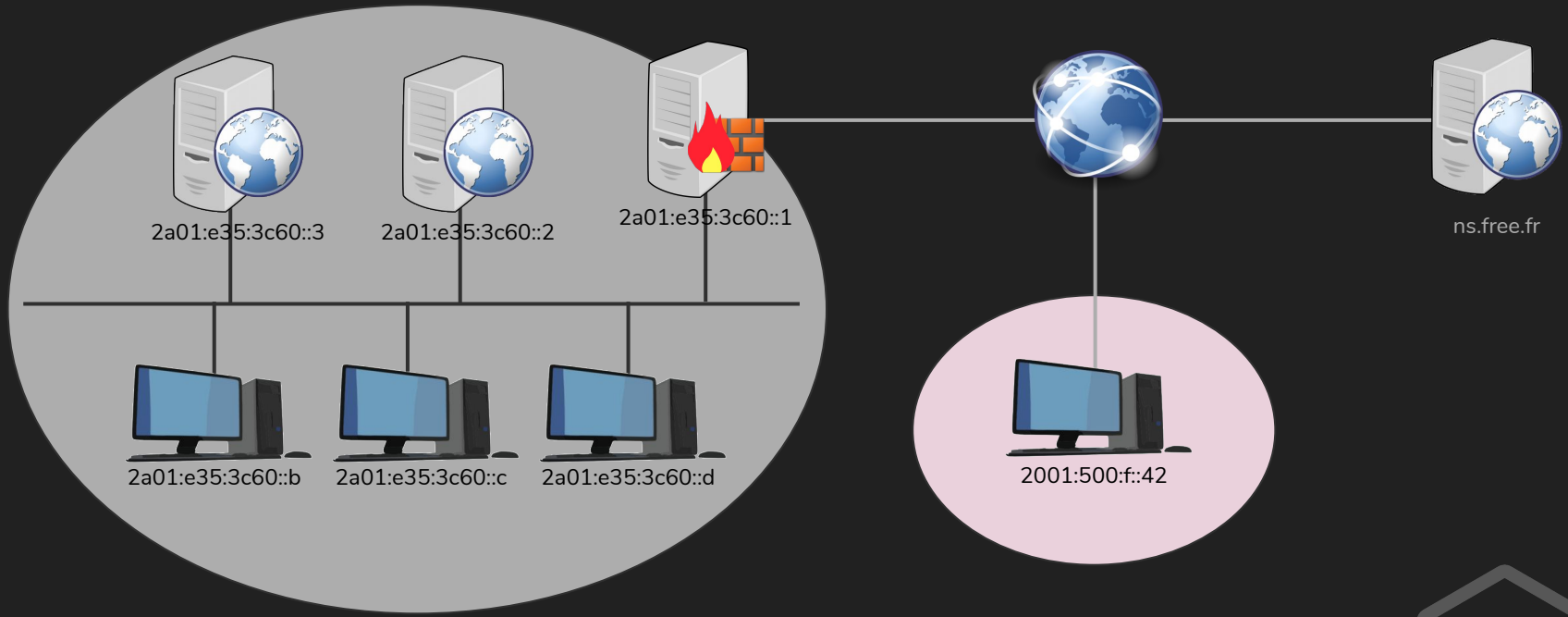
wikimedia.org. NS ?

```
wikimedia.org. 86400    NS     ns0.wikimedia.org.
wikimedia.org. 86400    NS     ns1.wikimedia.org.
wikimedia.org. 86400    NS     ns2.wikimedia.org.
```

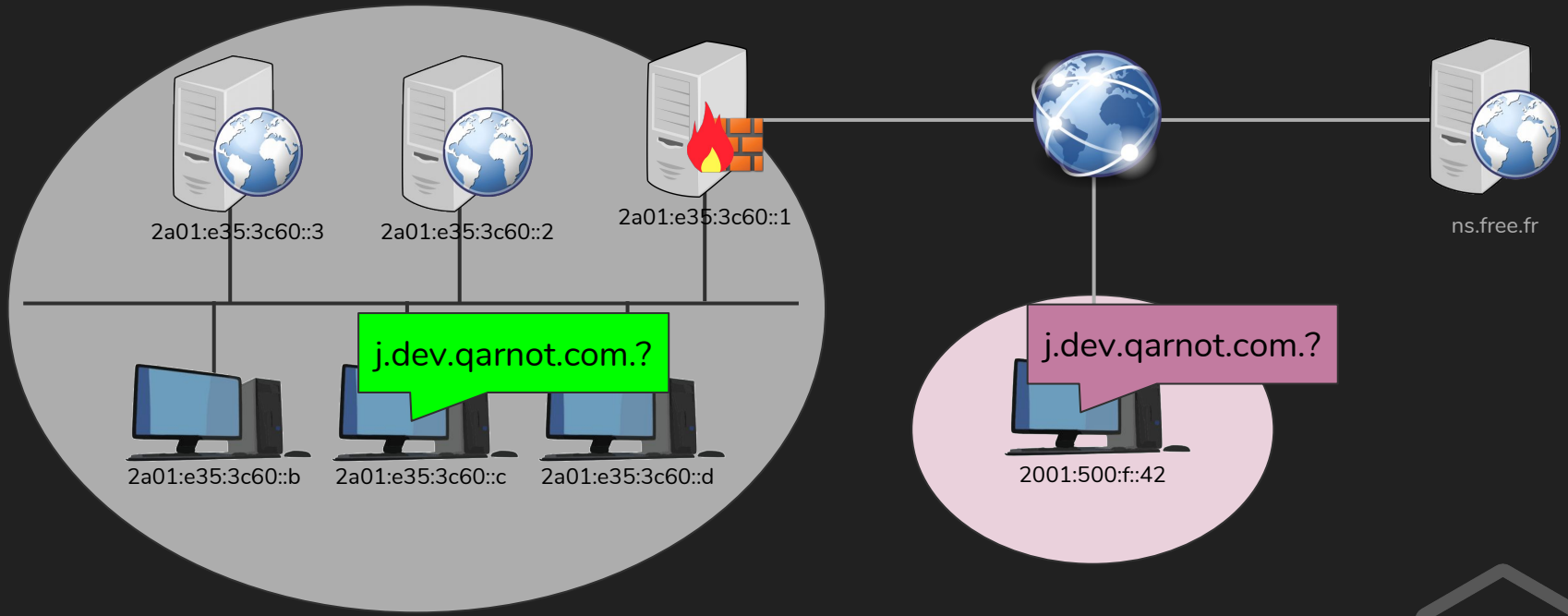
```
ns0.wikimedia.org.    3600 IN A  208.80.154.238
ns1.wikimedia.org.    3600 IN A  208.80.153.231
ns2.wikimedia.org.    3600 IN A  91.198.174.239
```



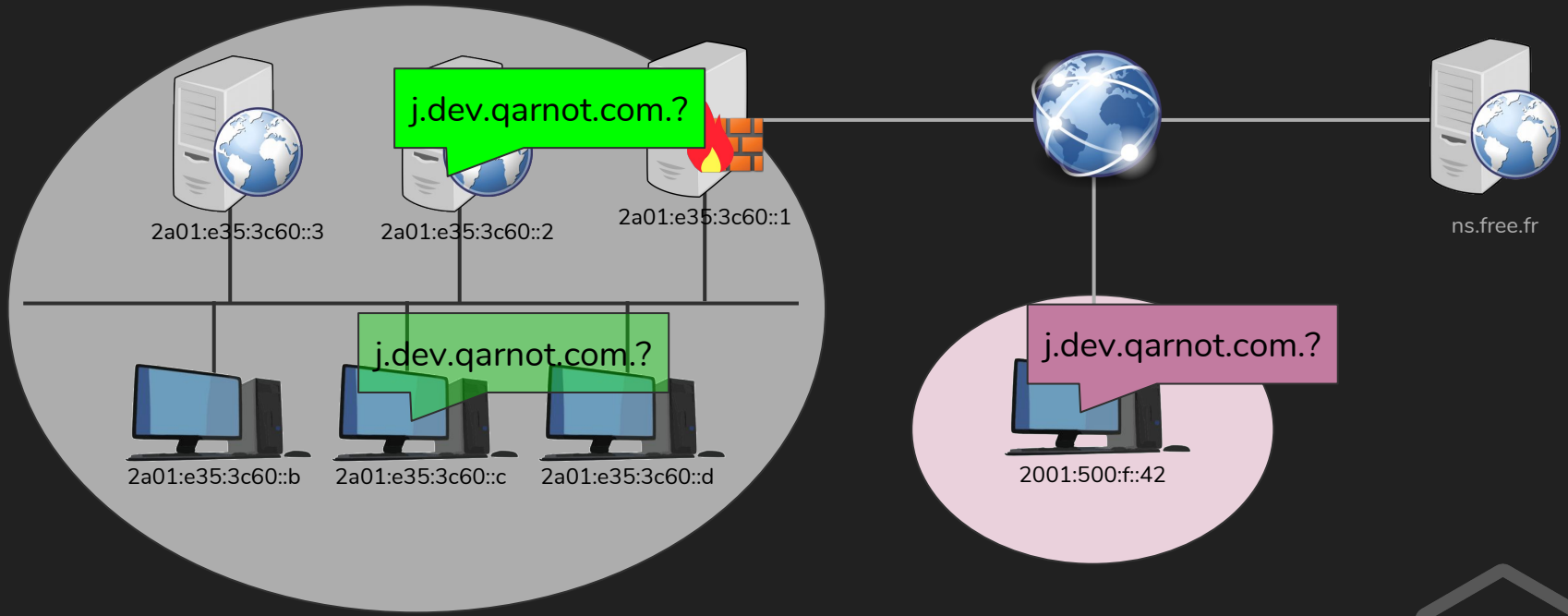

Split Horizon



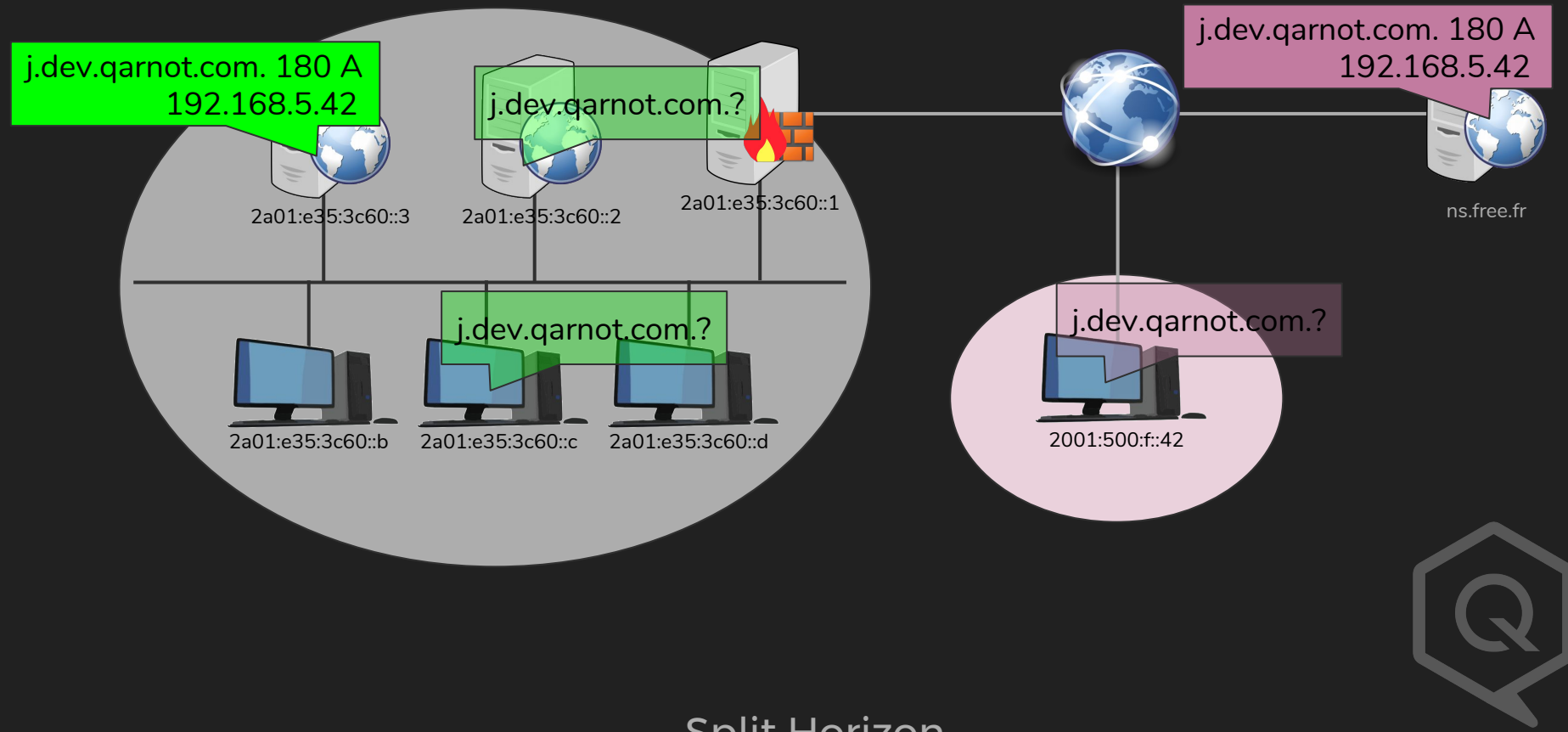
Split Horizon



Split Horizon



Split Horizon



Split Horizon


Édition de zone

```
$TTL 3h
@       IN  SOA     a.dns.gandi.net. hostmaster.gandi.net. (
                    2017072400      ; Serial
                    3h              ; Refresh
                    1h              ; Retry
                    10d             ; Expire
                    3h )            ; Negative Cache TTL

@       IN  NS      a.dns.gandi.net.
        IN  NS      b.dns.gandi.net.

www     IN  A       212.83.191.86
```

Un fichier de zone *RFC 1035*


QUESTION SECTION
? ?


DiG
obal options:
ot answer:
>>HEADER<<- opcode: QUERY,
flags: qr rd ra ad; QUERY: 1, ANSWER:
OPT PSEUDOSECTION:
EDNS: version: 0, flags: do; udp: 4096
; QUESTION SECTION:
;nemunai.re.
;; ANSWER SECTION:
nemunai.re.
nemunai.re.
IMYoe4GS/h0kG1NamQ2vevNKxg/1lvao8rfXwfyiR5Z
Ath8kDb186Y 5tTBCUG9/qNHhs0TJwCMGggiV
motIQLANNohM4P00vP1euNfYcxL
1R+awsdcqpEK18YwFHexqk
R4Up1TBuAmAzbML
katnk0J
IN SOA
345600 IN SOA
345600 IN RRSIG
nou
SO

webographie

- http://www.bortzmeyer.org/ Blog de Stéphane Bortzmeyer, ingénieur à l'AFNIC
- http://www.zytrax.com/books/dns/ Bases du livre *Pro DNS and BIND*, une lecture incontournable

- https://www.zonemaster.net/ Testeur de zone (partenariat ISS et AFNIC)
- http://dnsviz.net/ Visualisation des délégations et débogage DNSSEC

Next episode...

DNSSEC
Hidden master
Serveurs esclaves
Transfert de zone (AXFR/IXFR)
Délégation de domaine
Wildcard (`*.dev.qarnot.com`)
Zones dynamiques
DNSBL/DNSRBL

EDNS
Format binaire
Flags des paquets
Codes de retours
Noms de domaines internationaux
mDNS
...