Rainbow™
www.openrainbow.com

Alcatel-Lucent Rainbow

Alcatel-Lucent Rainbow™ is using DNS to steer the traffic to the closest location to end users and guarantee best possible response times. This technique is commonly called GeoDNS or latency-based routing.

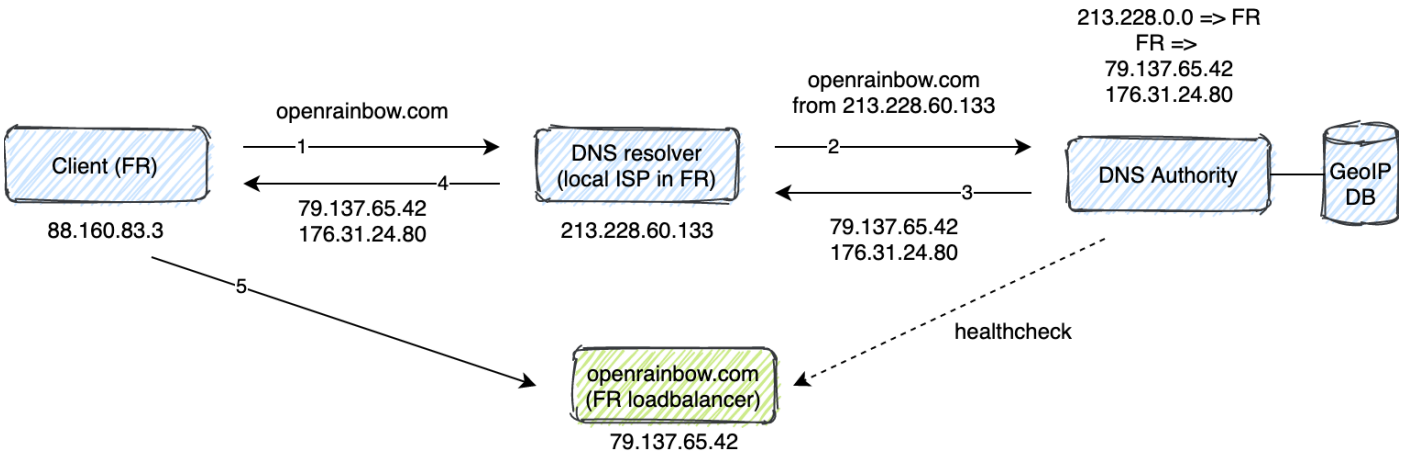

Fig 1: DNS Geo IP resolution using your local ISP

DNS steering works on the premise that DNS resolvers are provided by ISPs, and thus live on the same network within close location of the user. However, the increasing number of public DNS services that are less likely to be a good approximation for end-user location compared to ISP-provided resolvers results in an increase in suboptimal selection of the Rainbow load balancer the traffic will be sent to. Additionally, some ISPs may have temporary routing or peering issues, making their DNS resolver appear in other countries (as illustrated in Figure 2).

According to rainbow metrics, a very small part of our clients is experiencing slowness when using Rainbow due to a wrong geo-DNS resolution.

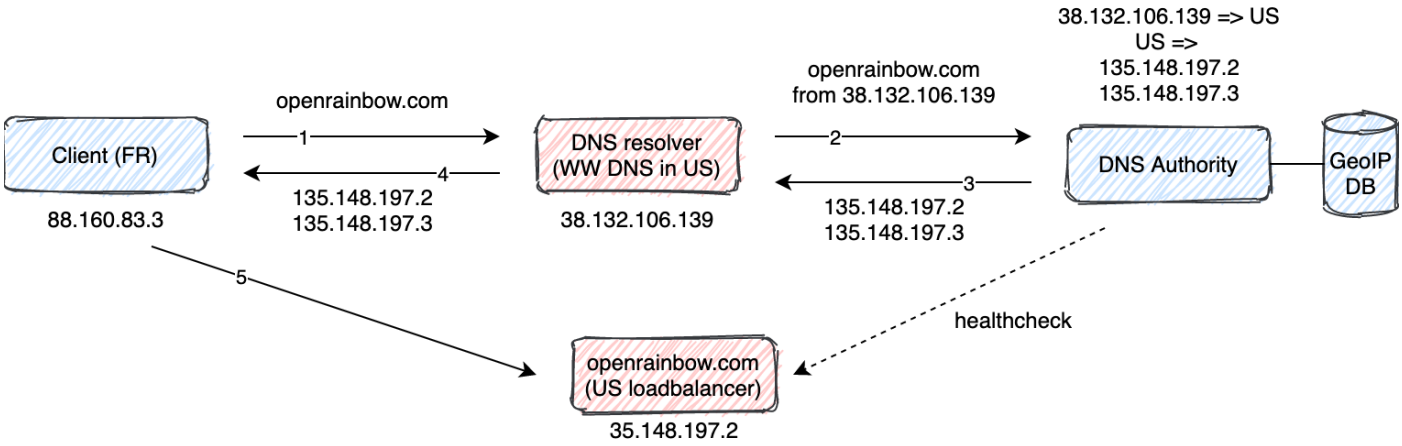

Fig 2: DNS Geo IP failure due to basic worldwide DNS resolvers

How to know if I'm affected?

First, you can check which country is currently serving your Rainbow requests by opening the following links in your favorite browser:

https://openrainbow.com/debug

The page will show you the country in which the load balancer is installed. The country should be the nearest one to you among following countries: France, Germany, Brazil, USA, Singapore, Australia.

If you see different countries from time to time or always a far away country, Your DNS provider may be affected.

What is the solution?

To work around this issue, EDNS0 Client Subnet (ECS: rfc7871) was invented. This extension to the DNS protocol provides a way for the DNS resolver to release information about the client IP requesting the domain to the authoritative DNS. The full client IP is not transmitted, only a part of it called a subnet, and thus preserves end users' privacy.

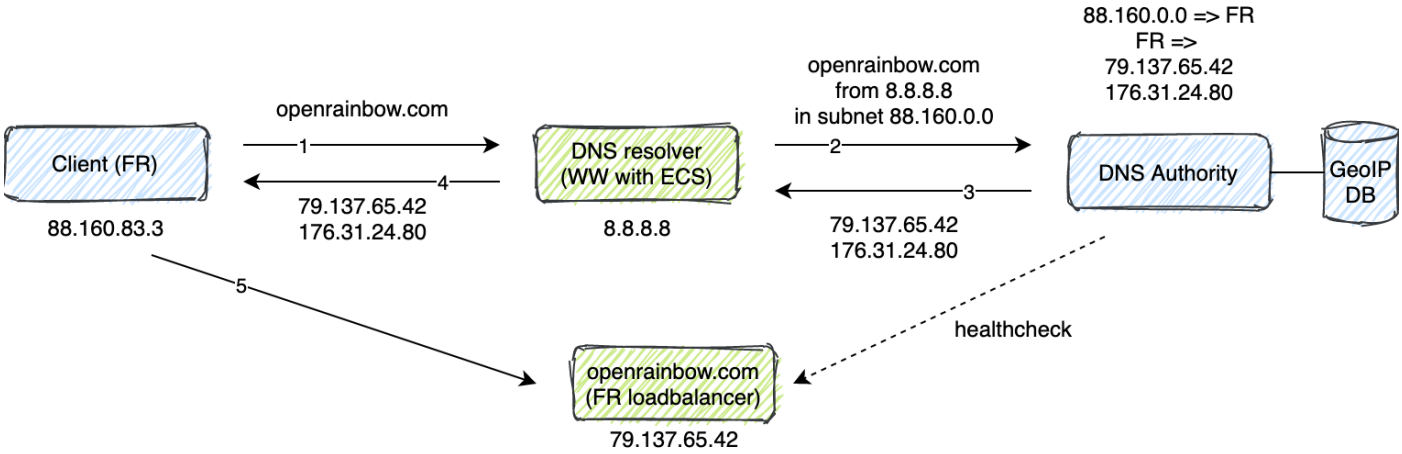

Fig 3: DNS Geo IP valid resolution using DNS resolves with EDNS0 Client Subnet extension

Thus, if you are encountering this DNS issue, affecting Rainbow as well as other global worldwide services, you should report the issue to your ISP or opt for another DNS provider who is known to support EDNS0 extensions (see list in Figure 4). Ideally, you may want to choose a primary server on one provider and a backup server on another one.

Provider	Primary DNS	Secondary DNS
Google Public DNS (US)	8.8.8.8	8.8.4.4
Cisco OpenDNS (US)	208.67.222.222	208.67.220.220
Cloudflare (US)	1.1.1.1	1.0.0.1
Quad9 (Switzerland)	9.9.9.9	149.112.112.112
NextDNS (France)	45.90.28.190	45.90.30.190
VeriSign Public DNS	64.6.64.6	64.6.65.6
DNS.watch	84.200.69.80	84.200.70.40

Fig 4: Alternate free, up-to-date and secured DNS providers

This DNS configuration can be changed in different locations:

- By the company's **network administrator** through using DHCP propagation or reconfiguring the central company DNS server
- By the end user by customizing the **OS** DNS resolution directly. There are numerous tutorials on Internet specific to your environment.
- For web application, the most modern **browsers** allow the user to override the OS settings and "secured DNS server":
    - In Firefox settings, search for "Activate DNS over HTTPS"
    - In chrome settings, security, "use secured DNS"