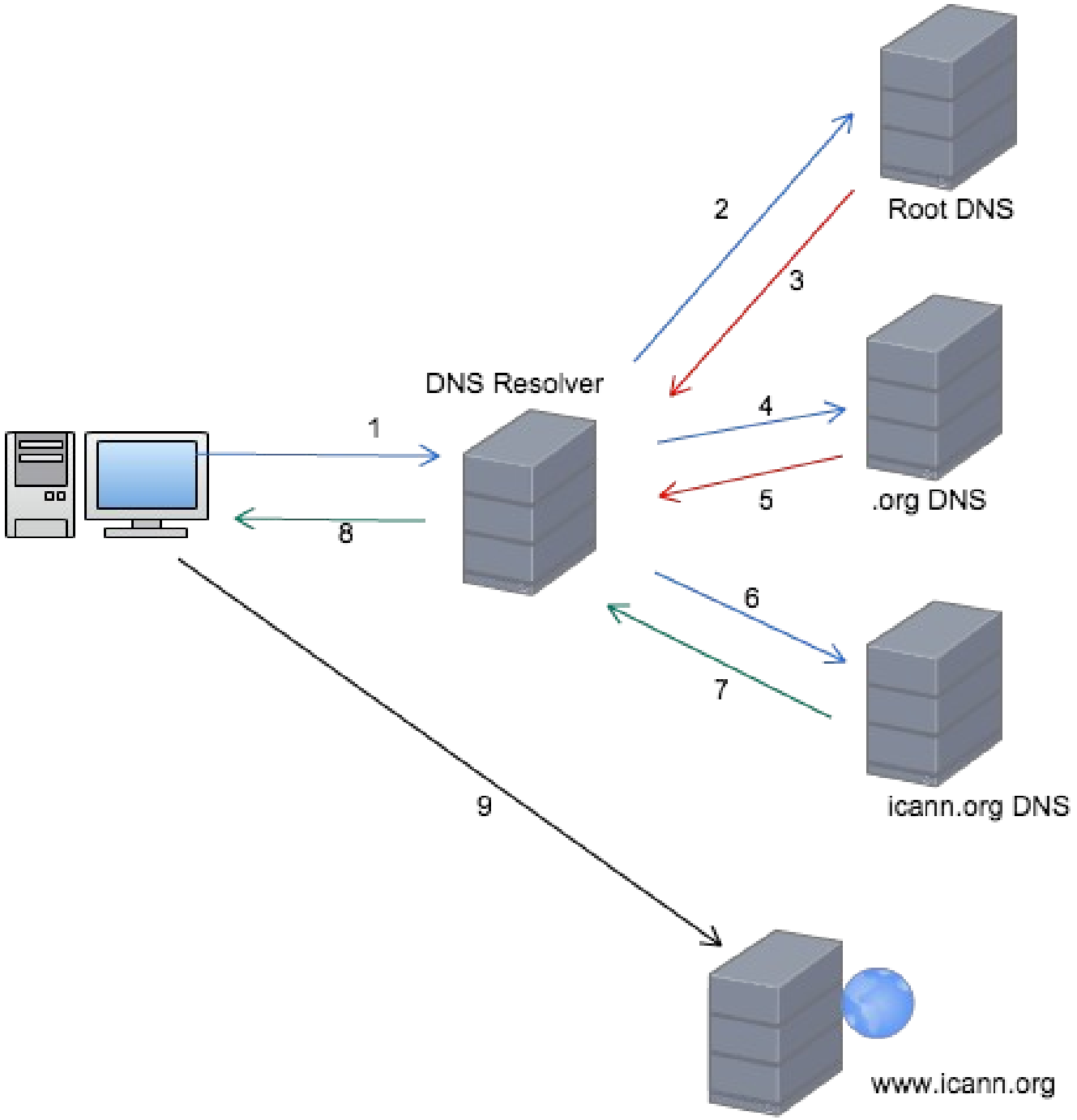
DNS- based Internet filtering

DNS Concepts

- Translates names to the numerical IP addresses
- Structuring the information hierarchically
- the use of multiple server replicas
- the caching of the responses obtained : In order to avoid overloading the DNS architecture.
- Improved routing for Email.
- A protocol for exchanging naming information.


Root DNS
2
3
DNS Resolver
4
1
5
.org DNS
8
6
7
icann.org DNS
9
www.icann.org

Blocking domain names and IP mapping

- At the level of the **registry** by no longer publishing information which will therefore gradually disappear from caches,
- At the level of the **resolvers**.
  - Black Lists provided by governmental or judicial authorities.
  - Modifying the normal resolution of a name on a server to an IP address.
  - Blocking the response.
  - Returning the address of another server indicating that access to the website is prohibited.

Turkish Government Censorship

- March 2014
- the Turkish government ordered the censorship of Twitter and YouTube.
- IAP (Internet Access Providers), who typically provide a recursive DNS service to their users, configures these recursors to lie !!
- Providing false answers when queried about censored names of twitter and YouTube.

People reaction

Counter reaction

- Turkish Internet service providers (ISPs) hijacking the routes to public DNS servers such as those operated by **Google** or **OpenDNS**
- The Turkish routers are lying about how to get to the Google Public DNS service, and taking all the traffic to a different destination.

Youtube.com lookup at Google's 8.8.8.8 DNS server 8.8.8.8 from Turk Telekom

```
;; ANSWER SECTION (1 record)
youtube.com.     86064    IN       A     195.175.254.2
                                          ^^^^^^^^^^^^^^^^
                                  Not a real Youtube IP address
```

Youtube.com lookup at Google's 8.8.8.8 DNS server from The Netherlands

```
;; ANSWER SECTION:
youtube.com.          299    IN A   74.125.136.93
youtube.com.          299    IN A   74.125.136.91
youtube.com.          299    IN A   74.125.136.136
youtube.com.          299    IN A   74.125.136.190
                                     ^^^^^^^^^^^^^^^^^
                                  Normal Youtube IP addresses
```


DNS lookup at 8.8.8.8 using RIPE Atlas

Conclusion

- The DNS was not designed to filter content !!
- DNS Filtering is ineffective :
  - Use of public resolver
  - Use of VPN.
  - Use of anonymous proxy.
- Blocking expose the users to new threats.

References

- http://www.bortzmeyer.org/dns-routing-hijack-turkey.html
-
- http://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/
-
- https://labs.ripe.net/Members/emileaben/a-ripe-atlas-view-of-internet-meddling-in-turkey/
-
- http://www.internetsociety.org/deploy360/blog/2014/04/turkish-hijacking-of-dns-providers-shows-clear-need-for-deploying-bgp-and-dns-security/
-
- http://www.afnic.fr/medias/documents/conseilscientifique/SC-consequences-of-DNS-based-Internet-filtering.pdf