computing
conference 2022

Measuring the Resolution Resiliency of Domain Name

Lanlan Pan (潘蓝兰)

abbypan@gmail.com

What is the problem?

Domain name system (DNS) is critical.

DNS resolution failure can result in disruptions at prominent internet service such as Facebook, Twitter, and Weibo.

There are many factors can cause DNS resolution failure, including DDoS attack, BGP operation, DNS server operation, domain name registrar phishing, etc.

Conclusion

It is important to measure the DNS resiliency to serve the internet service better.

Our Solution

We analyze some typical DNS Resolution Failure cases, and…

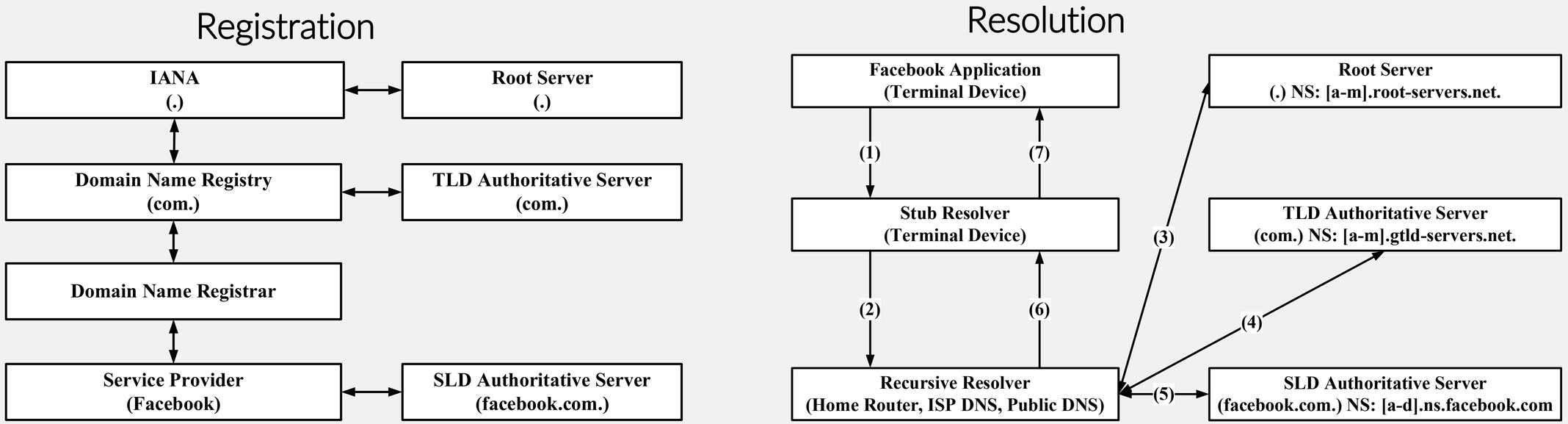
Discuss the metrics to measure resolution resiliency of second-level domain name.

Do the resiliency measurement on some famous internet service.

Describe a stub resolver cache proposal to mitigate the domain resolution failure, defense against DDoS attack.

Typical DNS Resolution Failure Cases

Typical DNS resolution failure cases are related with the registration chain and the resolution path.



Date	Failure Case	Failure Factor	Failure DNS Component
2021-10-04	Facebook outage [4]	False BGP operation	SLD authoritative server
2016-10-21	DYN DDoS [5] [6]	DDoS attack	SLD authoritative server
2013-08-25	CN TLD DDoS [7] [8]	DDoS attack	TLD authoritative server
2011-05-30	www.qq.com outage [9]	False DNS operation	SLD authoritative server
2010-01-12	Baidu NS hijack [10]	Tamper SLD's NS record	Domain name registrar
2009-05-18	Baofeng DDoS [11]	DDoS attack	ISP Recursive resolver

Resolution Resiliency Measurement: Domain Status Code Metrics

The domain status code lock can help to defense against the Jan 2010 Baidu NS hijack.

Metric	Description
clientDeleteProhibited	prevents domain from being deleted without registrar credit.
clientTransferProhibited	prevents domain from being transferred without registrar credit.
clientUpdateProhibited	prevents domain from being updated without registrar credit.
serverDeleteProhibited	prevents domain from being deleted without registry credit.
serverTransferProhibited	prevents domain from being transferred without registry credit.
serverUpdateProhibited	prevents domain from being updated without registry credit.

Whois information of facebook.com

Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2021-10-18T18:07:40Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2031-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited

Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM

DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

Resolution Resiliency Measurement: NS Diversity Metrics

Consider about the DNS resolution incidents (Facebook outage, DYN DDoS, CN TLD DDoS, www.qq.com outage) ,

the resolution resiliency is heavily dependent on the NS diversity and anycast deployment.

To avoid single point of failure, the domain owner is better to make distributed deployment for NS.

Metric	Description
NS Count	the count of domain's NS.
NS IP Count	the IP count of domain's NS.
NS IP AS Count	the IP AS count of domain's NS.
NS IP Country Count	the IP Country count of domain's NS.
NS IP Anycast Count	the count of domain's anycast NS IP.

Resolution Resiliency Measurement: TTL Configuration Metrics

TTL configuration is critical to domain name's resource record (RR).

There are 6 types of TTL, belong to authoritative service, email service, and web service.

Metric	Description
NS TTL	The maximum TTL of domain's NS RR.
NS IP TTL	The maximum A/AAAA TTL of domain's NS RR.
MX TTL	The maximum TTL of domain's MX RR.
MX IP TTL	The maximum A/AAAA TTL of domain's MX RR.
www CNAME TTL	The minimum TTL of "www" subdomain's CNAME RR.
www IP TTL	The minimum TTL of "www" subdomain's A/AAAA RR.

From the DNS authority view, recursive resolvers should overwrite the glue record from TLD authoritative servers with the answer from SLD authoritative servers.

In other words, if follow the DNS hierarchy authoritative design strictly, recursive resolvers should cache the IP of "ns1.qq.com" for 3600 seconds, and cache the IP of ns[2-4].qq.com for 600 seconds, but not 172800 seconds.

Therefore, it will reduce the resolution resiliency of "qq.com" if recursive resolvers couldn't get glue record from "com" TLD in every 3600 seconds.

Authoritative Server	NS	TTL Type	TTL Configuration	Response Section	Description
[a-m].gtld-servers.net	ns[1-4].qq.com	NS TTL	172800	AUTHORITY	"qq.com" NS record on "com" TLD
	ns[1-4].qq.com	NS IP A TTL	172800	ADDITIONAL	"qq.com" NS IP glue record on "com" TLD
	ns[1-2].qq.com	NS IP AAAA TTL			
ns[1-4].qq.com	ns[1-4].qq.com	NS TTL	86400	AUTHORITY	zone data on "qq.com" SLD
	ns1.qq.com	NS IP A TTL	3600	ANSWER	
	ns[2-4].qq.com	NS IP A TTL	600		
	ns[1-2].qq.com	NS IP AAAA TTL	600		

Measure Resolution Resiliency

To measure resolution resiliency, we define a risk threshold for each resolution resiliency metric.

Method: measurement = measure_resolution_resiliency(qd, qt)

```
qd: domain name to query
qt: RR type to query

measurement = 0

foreach domain name d on the resolution path of <qd, qt>
do
   foreach metric m in [NS Diversity Metrics, TTL Configuration Metrics]
   do
      risk = 0
      skip if find duplicate check on metric <domain: d, metric: m>.
 check the value of metric <domain: d, metric: m>, set risk = 1 if risk.
 measurement = measurement + risk
      end
end

if qd is second-level domain
foreach metric m in [Domain Status Code Metrics]
do
      risk = 0
      skip if find duplicate check on metric <domain: d, metric: m>.
  check the value of metric <domain: qd, metric: m>, set risk = 1 if risk.
  measurement = measurement + risk
 end
endif

return measurement
```

Method: measurement = measure_SLD_resolution_resiliency(qsld)

```
qsld: second-level domain name to query.
qsld_www: the www subdomain of qsld.

measurement = 0

foreach qt in [ NS, MX ]
do
   measurement = measurement + measure_resolution_resiliency(qsld, qt)
end

foreach qt in [ A, AAAA ]
do
   measurement = measurement + measure_resolution_resiliency(qsld_www, qt)
end

return measurement
```

Our Resolution Resiliency Measurement on Some Famous Internet Service

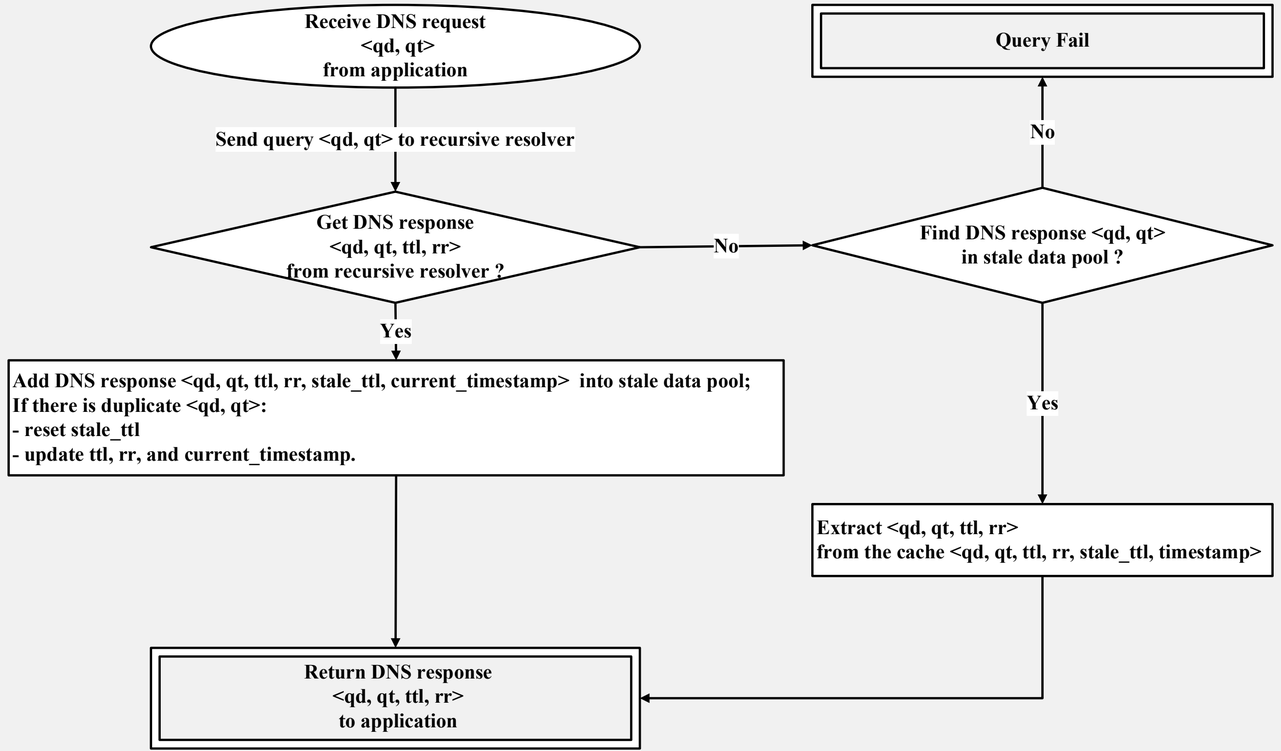
- “twitter.com” doesn’t configure clientDeleteProhibited and clientUpdateProhibited.
- “twitter.com” and “weibo.cn” make a better NS IP AS deployment.
- “weibo.cn” doesn’t make anycast NS, and NS servers are only deployed in China.
- “qq.com” and “amazon.com” configure different TTL for NS or NS IP, which may cause TTL overwrite of NS on recursive resolvers.
- “google.com” has a better MX configuration.
- Akamai edge CDN service configures very short IP TTL (20 seconds) for “www.qq.com” and “www.amazon.com”.

Note that the measurement may be different from different probe node, if the SLD’s authoritative server with Geo-Location based traffic management.

Resolution Resiliency Improvement

We propose that a stub resolver cache proposal for terminal device, such as PC, Mobile Phone.

- Stub resolver just maintains a stale data pool for cache, no other complex recursive resolver selection policies.
- It can address the typical DNS resolution failure as we metioned.
- It can persist the application visit the working internet server, even when the SLD authoritative server is breakdown, or the recursive resolver is out of order.
- It can distribute the cache burden to terminal service, mitigate the random subdomain DDoS risk to recursive resolver which support stale data cache.



Thank You