Application-centric DNS for the Morden Internet

Yong Ma
Principal engineer
mayong.my@alibaba-inc.com

Davey Song
DNS architect
linjian.slj@alibaba-inc.com

2021 ICANN IDS
Content

- Modern DNS as a online service
- What we do in DNS
- Conclusion
An analogy: The Skyscraper and the base

A solid and stable base is a matter most for the building
The details of the base...

Complicated structures and reinforced concrete with steel bars
Internet evolving with DNS

Birth
- Start from ARPANET
- Map name to address with HOST.TXT
- 4 machines

1969

Growth
- TCP/IP enable the network to scale to thousands of machines
- DNS invented to manage the naming
- Rapid growth: thousands of machines

1980s

Internet Popularity
- PC, website and Internet
- WWW, HTTP, Web service, domain business popularity
- Explosion: millions machines, huge connections

1990s

Internet of everything
- 5G, IoT, IPv6, M2M
- Everything connected, trillion of connections

2000s

Mobile Internet and Cloud
- 4G, Smart Phone, APP, H5, cloud
- Millions of domains and Apps
- Billions of mobile devices, dynamic resources and ten billions of connections

Future

Connection-centric, Domain/IP/RR database

Application-centric, Intelligent Brain
The hot topics in modern DNS

Combined with Cloud technologies

- **Cloud-Based DNS** (resilience, Rapid Deployment, Easy operation)
- **Hybrid DNS Cloud** (One DNS for ADNS and RDNS, private and public domain)
- **Cloud-Native DNS** (Cloud native design: CoreDNS)

Fine-grained Intelligence

- Fine-grained users separation
- Rich scheduling policies

Application-Centric DNS

- Native APP DNS: HTTPDNS/SDK
- HTTPS/SVCB

Privacy and Security

- DoH/DoT (Android, iOS, Windows, Firefox, Chrome)
- DNS Firewall (PassiveDNS, DNS filtering)
What we do DNS in Alibaba Cloud

Serve ~1 billion users, 1 Trillion queries per day (IDC, Public DNS, ADNS etc), serve 20 regions and Millions VMs

Alibaba DNS has a series of products that covers the **Alibaba Cloud DNS**, Alibaba Cloud PrivateZone, Alibaba Cloud Public DNS, Apsara Stack DNS, and Global Traffic Manager, Cached Public Zone.
More Capacities

Alibaba Cloud DNS developed the advance services based on customers’ requirements

- IPv6
- DNSSEC
- DNS TCP
- DoH/DoT

Authoritative DNS in June 2018
Public DNS in Oct 2019
Alibaba Public DNS

Online in Jan 2020
For DNS data integrity

Supporter of DNS Flag Day

Public DoH/DoT in April 2020
Consideration on Data privacy and security
Alibaba Public DNS: www.alidns.com
The Major challenges – Stability and security

It is a big challenge to operate a large-scale DNS system

- DDoS attack on ADNS
- DNS water torture attack on RDNS
- Anycast network operation/scheduling
- Hung server issue
- Data consistency in large system
- Bugs on DNS software
- DNS Hijacking between stub and resolvers
- External/Third-part interference (Stale DNS data)
- ...

There are always uncertainties and risks in current DNS architecture
Case: Mitigation of DDoS on Live signing

Alibaba Cloud DNS uses sign-on-the-fly in DNSSEC

Why
- Huge zones and domains
- Multiple dynamic resolution policy
- Large global distributed system

Extra pay
- Security challenge in key distribute
- Significant increase CPU load

Mitigation solution on DDOS

Overall performance has increased by **50 times** than without DNSSEC cache
The Major challenges: fine grained control in time

To meet the requirement of Application-centric DNS in Mobile Internet

• Multiple policy, fine-grained scheduling and control
  To achieve precise GrayRelease for example.

• End-to-End Propagation time (in seconds or less)
  To achieve fast Failover for example
Traffic scheduling scenarios of Alibaba Cloud DNS

Intelligent traffic scheduling base on Geo-location and App-specific tag

General public network resolution scenarios

Application-level DNS for Mobile Internet
Hybrid DNS solution for Failover scenarios

For the situation that Internet online services are not available due to attack or system failures, Alibaba Public DNS + Alibaba Cloud DNS + GTM collocation can be used to improve the overall protection capability.

Advantages

- **No Hijacking:** Bypass the middle box to avoid domain name hijacking.
- **Accelerated access:** Access to direct requests without layers of recursion by pushing authoritative data to recursive.
- **Security and privacy:** Support DoT/DoH access to ensure users’ privacy.
- **One-stop resolution:** To achieve domain name change and propagation in seconds through the sync between recursive and authoritative DNS.
- **Intelligent resolution:** Carry app-specific info via HTTP or EDNS0 Tag from end client to DNS server, with more intelligent traffic scheduling.
Conclusion and thoughts

- DNS is the base of the whole Internet evolving to next stage
- Different from Connection-Centric DB, Application Centric DNS provides:
  - Multiple policies, fine-grained scheduling and control
  - End-to-End Propagation time (in seconds or less)
  - and more features of resilience, security, and stability

- Alibaba Cloud DNS provide Application-Centric DNS solution
  - Now it is proprietary solution with Alibaba Cloud’s ADNS, Public DNS, GTM, CDN, DDoS protection, HTTPDNS/SDK...

- It is a promising field to define some use cases of Application-Centric DNS with multiple vendors
  - EDNS0 Tag (draft-bellis-dnsop-edns-tags) is one example for firewall application