The Survey Report on DNS Cache & Recursive Service in China Mainland

Wei WANG, Chinese Academy of Sciences

Zhiwei YAN, China Internet Network Information Center

Motivation

Improve the traditional recursive service model to adapt to new situations:

Recursive servers work as the only data provider for end users in the last mile, play an important role in decentralization, localization and scalability of DNS, and should bear more multiple and flexible functions to adapt to the evolution of internet techniques and market.

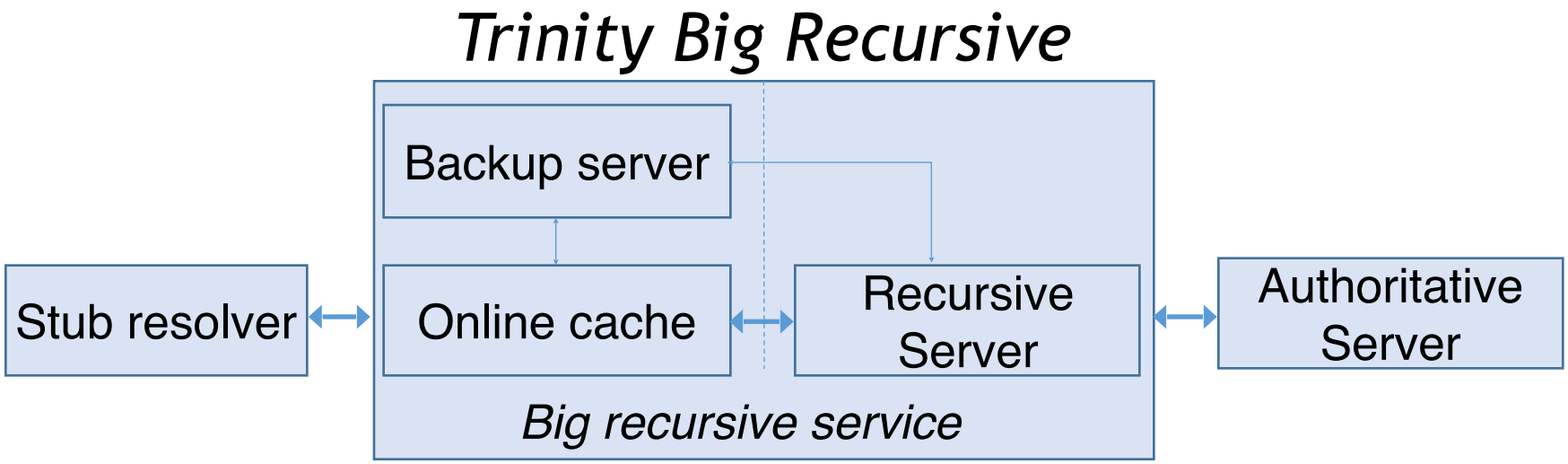
- Function extensions promoted by IETF, e.g.:
  - Recursive server loads root zonefile
    - draft-ietf-dnsop-root-loopback-01
  - Recursive server carries client subnet information
    - draft-ietf-dnsop-edns-client-subnet-00
  - Recursive server secures the signalings
    - draft-hoffman-dprive-dns-tls-alpn-00
- Function modifications driven by market
  - Many companies make use of recursive server to realize special management and business purpose like access control, service schedule, traffic2profit and etc., but regardless of the potential undermining to DNS ecosystem.

China Recursive Service Market

- Traditional recursive service providers
  - ISP: China Telecom, China Unicom, China Mobile
    - > 90% market share
    - Classical textbookish service model strictly follow RFCs

- New players and new architecture
  - Alibaba, 114DNS, Qihoo360
    - Compound system consisted of independent cache subsystem, recursive subsystem and backup subsystem.

The evolution of recursive service



- Cache: covering multiple regions (areas), decreasing latency and improving hit ratio by all means, such as
  - Actively initiate queries based on end user behavior estimation
- Recursive: degenerated into a weak and simple data fetching tool
- Backup: maintained mainly for emergency cases
  - Backups important zonefiles or TOP-N names beforehand
  - Imports data into Cache or directly works as recursive server in emergency

Merits of new architecture

- Performance
  - Increases the hit ratio by pre-detection and pre-store mechanism.
- Security
  - Spreads the risks by separating cache function from recursive.
    - Cache is not exposed to the public, only visible to given end users
- Emergency response
  - Provides a relatively alternative credible data source in case of emergency.
- DNSSEC
  - Provides an extra DNSSEC resolution path
    - Most stubs originates non-DNSSEC requests, but cache administrator would forward them in DNSSEC-enabled form for specified domain names, increasing the integrity of cached data.

Practice in China Telecom

- Global biggest DNS service provider
  - Cover 100M fixed network users and 200M mobile users
  - Daily DNS queries over 300B (average 3.5M QPS, peak 8M QPS)

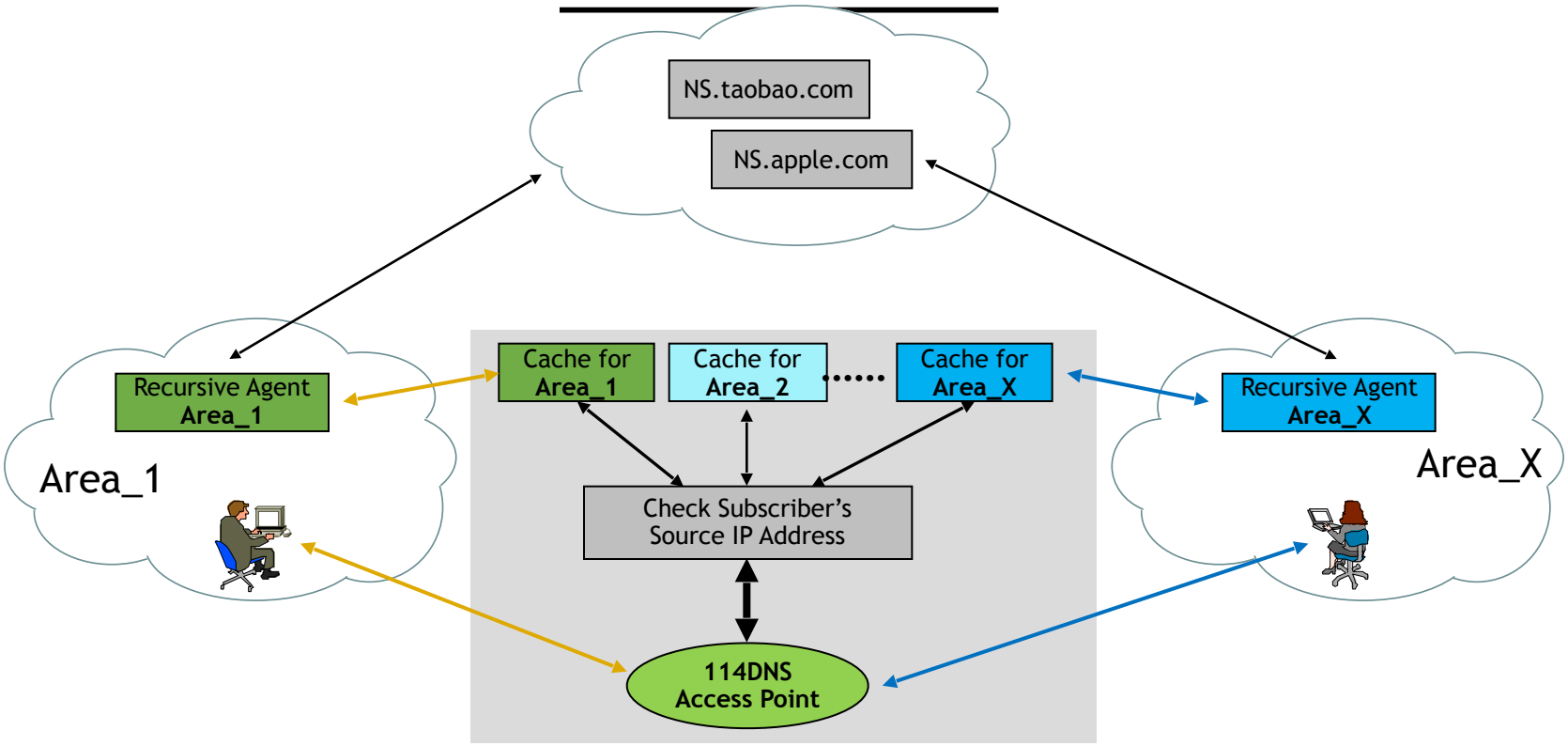
- 80 backbone DNS service nodes in China
  - 2-4 nodes per province with a standby backup server
  - Every node is consisted of 2 sub-systems:
    - Level1: cache-only system
    - Level2: recursive (forwarding) system

- Access point: 2-4 DNS servers each city
  - Resolve the queries directly.
  - Forward queries to cache system in the province-level.

Practice in AliDNS

- Fast growing DNS service provider
  - Cover 70M users in 1 year after published
  - Daily DNS queries over 20B (average 280k QPS, peak 600k QPS)
- multi-optimization
  - Friendly with CDN
    - deploying local forwarding recursive agent in different networks and regions
    - support edns-client-subnet
  - cache 10M DNS records
    - pre-fetch before TTL expires
- 4 Access points
  - 223.5.5.5 223.6.6.6
  - Anycasting

Practice in 114DNS (114.114.114.114)



3 access point, 56 DNS service areas all over China.
About 30,000,000 end users use 114DNS as their primary DNS.
Friendly with CDN by deploying local forwarding recursive agent in different networks and regions.

Negative impact to DNS ecosystem

The new architecture breaks the balance between stub, recursive and authoritative functions originally designed.

- Decreases the number of queries arriving at authoritative server.
  - More end users covered by on-line cache server, less queries reach authoritative server.
  - In extremis, the authoritative server get 6 queries during TTL period if all 6 recursive providers share the market.

- Distorts the query behavior and statistics at authoritative server
  - The packets reach recursive server are not all triggered by stub any more, a high percentage are initiated (forwarded or simulated) by cache administrator.

- Cut the authoritative queries number to ZERO in emergency
  - Usually activated by local administrator without notifying related authoritative servers.
  - For authoritative, the related area is black-hole from where all queries disappear.

Conclusions

- The role of recursive server is becoming more important and more complicated with the expansion of DNS tree as well as the whole internet.
- The market has made the choice. Modification on recursive system is becoming a mainstream solution.
- The current rough solution brings unexpected problems, undermines the foundation of DNS module.

- Cooperation mechanism and technical extension between recursive and authoritative is needed.

Some Suggestions

- Cache & Recursive query packets carry optional information to authoritative, like:
  - Query amount for a given domain name
  - Total number of local stubs
  - Cache initiated or stub initiated
- Backup server notify authoritative before and after emergency
  - Before: Take-over notification
  - After: Emergency processing statistics report
- Local shared backup service agent
  - Trusted by multiple recursive operators in a local area
  - High speed data synchronization with authoritative operators
    - IXFR or frequently AXFR

Thanks
Q&A

Wei WANG: wangwei@cnic.cn

Zhiwei YAN: yanzhiwei@cnnic.cn