Hyperlocal Root Zone

A Collective Term for Using the Root Zone Locally

Roy Arends
Principal Research Scientist, ICANN's Office of the CTO

25 October 2021

Hyperlocal

“relating to or focusing on matters concerning a small community or geographical area.” *(Oxford English Dictionary*)

- Used in the context of local news and weather forecast provisioning
- Now more generally used in the context of provisioning data pertaining to locally used applications.
  - weather apps, local maps, local services, etc.
- Hyperlocal root zone: resolver uses a locally available root zone instead of root-servers

Hyperlocal

- Concept is not new
- Not invented by ICANN
- Suggested by Paul Mockapetris in 2003
  - Suggested by many since
- Researched in 2004 by David Malone: “Hints or Slaves”
- Many “user-group” questions throughout the last 10 years on how to do this
- Operators already do this
- Time for a technical analysis

Hyperlocal Impacts the Resolver in Various Ways

- Query privacy
- Root zone integrity
- Query latency
- Telemetry
- Operational complexity

Query Privacy

- DNS servers are observers (RFC6973)
  - an entity that can observe and collect information from communications, potentially posing privacy threats
  - DNS data is collected passively at observation points (passive DNS)
  - DNS data is kept for a long time and distributed to third parties
  - No transparency how DNS query data is collected, stored, processed, analyzed, used, shared, and sold
  - Query minimization and aggressive negative caching helps to preserve privacy
- A hyperlocal root zone avoids the need to send queries to root-servers
- A query not sent is a query that can’t be collected

Root Zone Integrity

- The bulk of records in the root zone are not DNSSEC signed
  - None of the delegation point NS records and glue records have signatures
- There is no transport security between root-servers and resolvers
- A hyperlocal root zone provides better integrity than individual responses coming from root servers.
  - Provided that the root zone is securely retrieved or securely checked
  - Currently with HTTPS, PGP signatures or TSIG (via LocalRoot)
  - Future: DNSSEC validated ZONEMD records

Query Latency

- A query to the root zone is often a resolver's first query in a series, blocking the rest of the series
  - This only happens sporadically though, when the information is not available in cache
- About 68% of queries to the root return NXDOMAIN
  - Chrome browsers send a large amount of nonce-labels, which causes a lot of processing
  - Responses will be cached, causing memory consumption in caching resolvers
  - Root-servers spend a lot of time answering these queries.
  - Google is working to fix this
- Hyperlocal root zone lowers latency, causing better throughput for all queries.

Reduced Telemetry

- DITL data provides a lot of fertile ground for DNS research
- Some interesting telemetry data, such as deployment of new features, v4/v6, UDP/TCP ratios will be lost
  - However, they could be observed elsewhere

Elements of Deployment

- Availability, or “Where am I going to get it?”
  - Root Server Operators? IANA? Root Zone Maintainer?
- Transport , or “How am I going to get it?”
  - FTP, HTTPS, AXFR?
- Integrity, or “How do I know it is correct?”
  - ZONEMD+DNSSEC, PGP, TLS…
- Timely Updates, or “How do I make sure that I use the latest”
  - Notify is handy, but I should check anyway
- Fallback Mechanism, or “What do I do when it fails?”
  - Make sure to use them root hints again.

Operational Complexity

- Current security provisioning is cumbersome
  - LocalRoot offers TSIG, but a shared secret doesn't scale well
- TLS certificates are guaranteed by Certicom, not IANA
  - Internic.net uses HTTPS
- PGP is cumbersome in an automated environment
  - How to roll the PGP key…
- Local disk management, simple file write rights, cronjob management
  - For hand-rolled deployments
- Some of this is addressed by modern implementations
  - Each implementation has its own method
- Cryptographic zone file integrity check remains an issue
  - . . . until ZONEMD is deployed

Hyperlocal Deployment Methods

- Resolver serves authoritative data
  - Clients may not see AD bit on root zone content from the resolver
  - LocalRoot ships this configuration
- Resolver uses a local authoritative server for the root zone
  - On the network, on loopback, or as an internal “mirror zone”
  - RFC8806 has this configuration. Bind uses “mirror zone”
- Resolver primes the cache with the root zone
  - Times out nicely, re-prime once a day
  - Knot resolver does this

Conclusion

- Hyperlocal root zone is not new, and has been deployed for years
- Recent software makes a hyperlocal root zone deployment easier
- There are benefits, such as better integrity, privacy, and latency
- There are drawbacks
  - such as less telemetry at observation points
  - additional operational complexity
- There is work to be done to make a hyperlocal root zone
  - Deployment more secure (ZONEMD)
  - More available (maybe via a pool of root-zone publishers)
- Full paper at https://www.icann.org/octo-027-en.pdf

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**


@icann


facebook.com/icannorg

youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


soundcloud/icann


instagram.com/icannorg