ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2014

EFFICIENT ORIENTED DOMAIN NAME SYSTEM CACHE UPDATE PROTOCOL

DR.R.UDAYAKUMAR[1]

Associate Professor, Department Of IT, Bharath University, Chennai, India[1]

ABSTRACT: With the deployment of caches, cache consistency has become a serious concern. Strong cache consistency is defined as the model in which no stale copy of a modified original will be returned to clients, whereas weak cache consistency is the model in which a stale copy might be returned to clients. Currently, DNS only supports weak cache consistency by using the Time-to-Live (TTL) mechanism we propose a proactive DNS cache update protocol (DNScup), working as middleware to maintain strong cache consistency among DNS name servers and improve the responsiveness of DNS-based service redirection.

I. INTRODUCTION

The Domain Name System is a general-purpose database for managing host information on the Internet. It supports any kind of data, including network address, ownership, and service configuration, to be associated with hierarchically structured names. It is primarily used to translate human-readable names of internet resources to their corresponding IP addresses. One concrete way to estimate the effectiveness of DNS caching is to observe the amount of DNS traffic in the wide area Internet. DNS cache implementations employ different approaches in query load balancing at the upper levels. DNS only supports weak cache consistency by using the Time-To-Live (TTL) mechanism. The majority of TTLs of DNS resource records range from one hour to one day. Most of the domain-name-to-IP address mappings are infrequently changed; the TTL approach to coping with an expected mapping change is still cumbersome. The propagation of the mapping change may take much longer than expected. Some local DNS name servers that do not follow the TTL expiration rule and violate it by a large amount of time induce this pathology.

The proposed system offers the proactive DNS cache update protocol, achieves strong cache consistency of DNS and significantly improves its performance and scalability. DNScup working as middleware to maintain strong cache consistency among DNS name servers and improve the responsiveness of DNS-based service redirection.

The core of DNScup uses a dynamic lease technique to keep track of the local DNS name servers whose clients are tightly coupled with an Internet server. Upon a DN2IP mapping change of the corresponding Internet server, its authoritative DNS name server proactively notifies these local DNS name servers still holding valid leases.

Although the User Data gram Protocol carries the notification messages, dynamic lease also minimizes storage overhead and communication overhead, making DNScup a lightweight and scalable solution. The proposed DNS cache update mechanism can be viewed as an external extension to the DNS Dynamic Update protocol, which makes the implementation and deployment of DNScup much easier. The required modifications and additions to the current DNS implementation are minimized.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2014

II. SYSTEM ARCHITECTURE

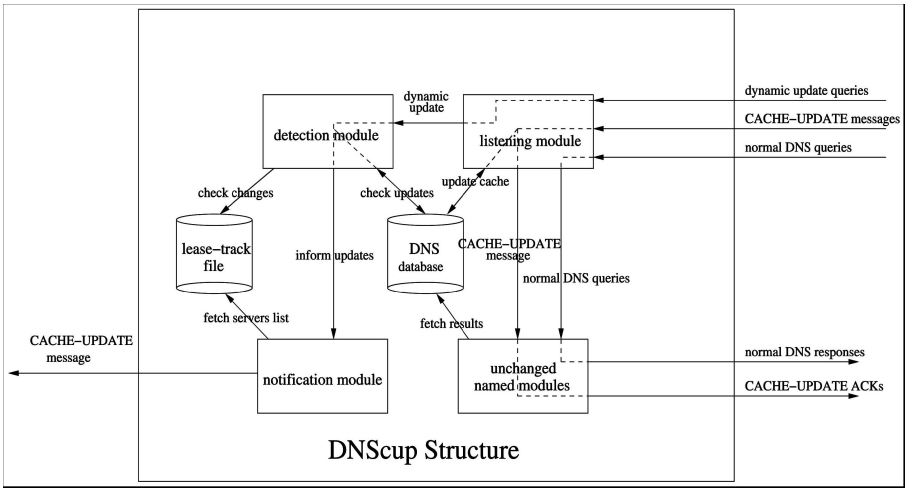

FIG1.SYSTEMARCHITECTURE

LIST OF MODULES

1. DNS Server
2. DNScup listener & detection
3. DNScup notification
4. Dynamic lease algorithms
5. DNS cache
6. Client

DNS SERVER

The DNS name space is hierarchically organized so that sub domains can be locally administered. The root of the hierarchy is centrally administered and served from a collection of root servers. Sub-domains are delegated to other servers that are authoritative for their portion of the name space. This process may be repeated recursively. The root name servers know the names and addresses of the name servers for each of the top-level domains. In the absence of any other information, DNS query resolution has to start at the root name servers, which makes the root name servers the hotspot of DNS operation.

DNS CUP LISTENER & DETECTION

The listening module monitors incoming DNS queries and updates the track file when necessary. The detection module detects a DNS record change. The mapping change detection module is straightforward to implement, since only the authoritative DNS name server has the privilege to change a DNS resource record. There are two ways for an authoritative DNS name server to change a DNS resource record: one is through manual reconfiguration and the other is through the DNS dynamic update command such as name server update.

DNS CUP NOTIFICATION

The notification module propagates DNS cache update messages. To reduce communication overhead and latency, we choose UDP as the primary transport carrier for update propagation. Transmission control protocol is used only when a firewall is set on the path from the authoritative DNS name server to a DNS cache.

DYNAMIC LEASE ALGORITHMS

Dynamic lease algorithm, one minimizes the communication overhead, given a constraint on storage budget, and the other minimizes the storage overhead, given a constraint on communication traffic. Whether or not a lease is signed between the DNS name server and a DNS cache is based on the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2014

DNS cache's query rate, whereas the length of a lease is determined by the DN2IP mapping change rate at the DNS name server.

DNS CACHE:

DNS makes extensive use of caching to reduce server load and client latency. It is believed that caches work well because DNS data changes slowly and a small amount of staleness is tolerable. On this premise, many servers are not authoritative for most data they serve, but merely cache responses and serve as local proxies for resolvers. Such proxy servers may conduct further queries on behalf of a resolver to complete a query recursively. Clients that make recursive queries are known as stub resolvers in the DNS specification. On the other hand, a query that requests only what the server knows authoritatively or out of cache is called an iterative query.

CLIENT:

Clients create queries and send them across the network to name servers. In most cases, network applications such as web browsers and mail transfer agents have integral DNS resolver clients. DNS servers, on the other hand, are typically dedicated applications.

III. FUTURE ENHANCEMENT

In this project, we transmit DNS messages in plaintext for simplicity and efficiency. However, to protect DNS caches against poisoned CACHE-UPDATE.

Messages originated from a compromised DNS name server, we need a secure communication channel for cache update. DNS Security Extensions (DNSSEC) and the secure DNS Dynamic Update protocols have been proposed. Coupled with the proposed secure DNS mechanisms, DNScup can achieve a secure cache update without much difficulty.

IV. CONCLUSION

In this project, we have proposed DNScup, working as middleware to maintain strong consistency in DNS caches. We conclude that maintaining strong cache consistency is essential to prevent potential losses of service availability.

The major components of the DNScup prototype include the detection module, the listening module, the notification module, and the lease-track file. Our trace-driven simulation and prototype implementation demonstrate that DNScup achieves the strong cache consistency in DNS and significantly improves its availability, performance, and scalability.

REFERENCES

1. Content Delivery and Distribution Networks, http://www.webcaching.com/cdns.html, 2008.
2. Dynamic DNS Provider List, http://www.technopagan.org/2008
3. Internet Systems Consortium, http://www.isc.org, 2007.
4. IRcache home page, http://www.ircache.net/, 2006.