Project 2: DNS Resolver and Name Server

14 April 2015

Submitting your project

Requirements about the delivery of this project:

- Submit via Blackboard (http://blackboard.ru.nl);
- Upload one single .zip archive with the structure as described in the document.

Deadline: Monday, 30 May, 20:00 p.m. sharp! Late submissions are accepted with a corresponding penalty. Submissions delivered at most one day after the deadline elicit a 15% penalty, submissions delivered at most two days after the deadline elicit a 30% penalty. Submissions are not accepted more than 2 days after the deadline.

Organization: It is strongly encouraged that you work in pairs of two. You can also work individually. Pairs of more than two members are not allowed.

Marks: You can score a total of 100 points. The points are distributed as follows:

- 30 points for a non-caching DNS Resolver;
- 20 points for implementing caching and TTL;
- 30 points for implementing a DNS Name Server;
- 15 points for the set of tests;
- 10 points for documentation;
- 5 points for interface and structure.

Implementation: You can use the latest Python 2.7 version. A Python framework is provided which is compatible with this version. You are strongly encouraged to build your project on top of this framework. The framework is designed to simplify and streamline construction of the resolver functions, and also to give an example of how a test can be implemented.

We suggest you use versioning. In particular, we recommend Git. A good presentation on Git can be found on Giso Dal's page at: http://www.cs.ru.nl/~gdal/files/gittutorial.pdf. The faculty's own CnCZ is hosting a GitLab server, accessible with your science login, at https://gitlab.science.ru.nl/. For more information on it, see http://wiki.science.ru.nl/cncz/GitLab.

DNS Resolver and Name Server

This project consists of two parts. You first have to build a caching DNS Resolver capable of solving FQDNs (Fully Qualified Domain Names) to their IP address by accessing its cache, and eventually sending iterative queries to known name servers. You then have to embed the DNS Resolver within a Name Server, which has manages a zone file and can respond authoritatively to queries for names within its zone. Finally, you will have to implement a set of tests for common scenarios.

The DNS Resolver should roughly implement the algorithm in Section 5.3.3 of RFC 1034, while the Name Server should implement the algorithm in Section 4.3.2 of RFC 1034. The RFC documents that you will have to consider are RFC 1034 and RFC 1035. DNS query and reply messages comprise a header and 4 main sections. Among others, the header contains flags for determining whether the message is a query/reply, whether the replier is authoritative or whether recursion is enabled. Each section contains *Resource Records* where each *Resource Record* is a tuple made from a Type (A, CNAME...) a Class (IN) and *Resource Record*-specific information. In your implementation, your should concern yourselves only with *Resource Records* of Type A, CNAME and NS, with Class IN. Figure 1 gives an overview of DNS in the context of the full network stack.

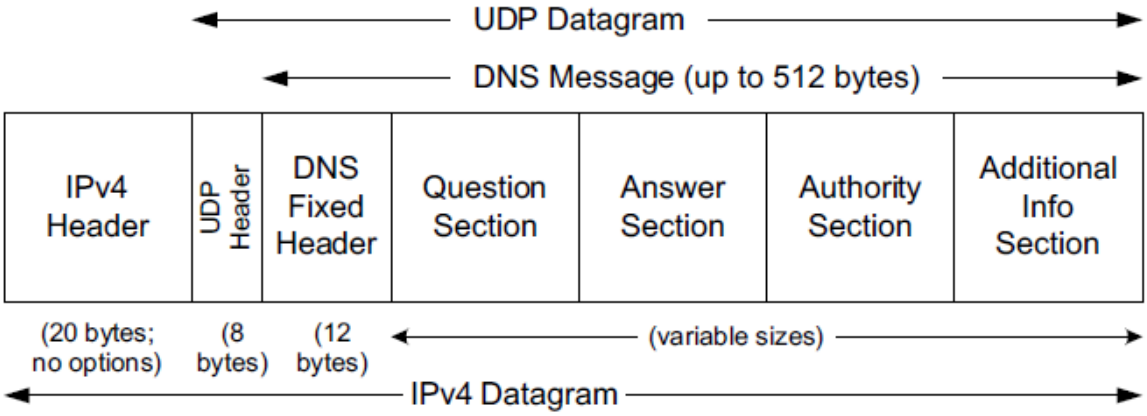

Figure 1: Stack with DNS (taken from 'TCP-IP Illustrated, Vol 1')

DNS Resolver

Your DNS Resolver given a FQDN string and a list of name server addresses (we will name them hints), will have to roughly (1) consult its cache and resolve the FQDN address immediately if response for the query is found (2) based on the FQDN, cache and the hints pick the best name server to query (3) build an **iterative** DNS query (4) send the query to the server over an UDP channel (5) process the response, if it is an answer for FQDN output and return, otherwise update the hints using answer and return to step (2).

Functionality: The DNS Resolver should resolve FQDNs to their corresponding addresses. A general overview of a resolver is given in Section 5 of RFC 1034. We first consider the case when there is no caching. Your resolver must send an **iterative** query for the FQDN to one of a list of given name servers (hints). As starting hints you should use the IPs of the root name servers found in the root hints. Hence, the resolver sends the query starting from one of these root name servers, continuing on with a TLD server and eventually with a sequence of authoritative name servers, until it receives an answer for the FQDN or it concludes the name cannot be resolved.

In case of a positive answer, the DNS Resolver generates an output, which is a tuple containing: (1) the FQDN; (2) the list of IP addresses found; and (3) the list of aliases for the FQDN. This matches the output interface of Python's gethostbyname_ex socket command.

This output has empty lists if the name could not be resolved or an error was encountered. The policy for selecting a name server out of a list of possibilities (hints) can be selecting the first in this list and removing it. If the name server is unreachable or responds with an error message/no answer, you could try the next name server in the list, and so on. If the FQDN can be resolved from the response (the response is a positive answer), resolve it and exit. Otherwise, the answer might contain referrals to better name servers, which you should add at the start of the hints list (so they are selected as you loop back). If you exhaust the list of hints, you should return an empty output.

At a technical level, the query sent has a corresponding *A-Resource Record* for the FQDN in the Question-Section. The answer received if positive will contain *A and CNAME-Resource Records* records in the Answer-Section from which the FQDN can be solved. Otherwise, the answer might refer to other name servers, referred by *A and NS-Resource Records*. You use these name servers further on in your resolution.

Caching: With caching, for every response received we cache all *A and CNAME-Resource Records*. The TTL of an entry in the cache is set to either a positive value given as parameter, or, in case no such value was given or the value given was negative, the TTL value of the record to be cached. The TTL value is measured in seconds.

Whenever the TTL of an entry expires, the records are removed. You are free to decide on how you manage and enforce TTL. For example, for each entry you may store a timestamp and check entry expiry against it. What is important is, once the TTL expires, the entry is no longer considered. The cache should be used not only as means of quickly resolving a FQDN, but also to minimize the number of iterative queries sent for a FQDN not solvable by the cache.

Caching should be made to a cache file in JSON format. The JSON entry for a cached record comprises 5 name value pairs, for `name`, `type`, `class`, `ttl` and `rdata` respectively. The cache file is loaded at start and updated. Note, this does not necessarily apply to real resolvers. Also note, you do not have to implement negative caching. (caching for negative responses)

DNS Name Server

The DNS Name Server manages a local zone file and uses it to answer A Type queries. It also utilizes the DNS Resolver described in . Your Name Server should follow the algorithm in Section 5.3.3 of RFC 1034, that is it should: (1) load the local zone file to memory, (2) listen to port 53 for incoming queries, (3) on receiving a query it consult its zone, and try to answer from its zone, if it cannot (4) it should use the DNS Resolver to answer the query and eventually (5) send the answer back to the originator of the query.

It is important to clarify that the zone is always consulted first. The interface differs from that of a DNS Resolver, as its inputs are now DNS queries instead of strings, while outputs are DNS replies sent over an UDP socket. In step (4), the Name Server accesses the Resolver by supplying it the FQDN from the query. It is not a problem that the Resolver will then have to rebuild this query (instead of receiving it directly from the Name Server).

The zone file (or master file) should be structured as described in Section 5 of RFC 1035. Your zone file can contain records of type NS, A and CNAMEs, and only for these records do you need to provide corresponding handling. An example of such a zone file is the root hints. A major simplification is that you don't have to consider zone maintenance and transfers, as described in Section 4.3.5 of RFC 1034. Moreover, there is no SOA record describing the zone. The zone file is loaded at the start and never updated. How to respond from zone information is described in the RFC 1034 algorithm.

The DNS Name Server is cognizant of DNS flags, namely it should use its DNS Resolver only if recursion is enabled in the query. Moreover, if it is authoritative over the requested FQDN in the query, it should then

send an authoritative response.

Concurrency: Your DNS Name Server should be able to handle multiple queries at the same time. To implement this feature, you should use the DNS Transaction ID to match responses to their corresponding queries.

Tests

Along with the DNS Resolver and Name Server, you should also supply a set of tests. We suggest you use FQDNs with relatively stable addresses in your tests, such as http://gaia.cs.umass.edu/.

For the DNS Resolver:

- with no caching:
  - ◇ solve a FQDN, output with corresponding IP/CNAME/authoritative status generated
  - ◇ look up a FQDN that does not exist, empty output generated
- with caching
  - ◇ solve an invalid cached FQDN (for example invalid_address.com), output corresponds to cache
  - ◇ start your server and wait configured TTL + 1 time for an invalid cached FQDN to expire, an empty output should be generated

For the DNS Name Server:

- ◇ solve a query for a FQDN for which your server has direct authority
- ◇ solve a query for a FQDN for which your server does not have direct authority, yet there is a name server within your zone which does
- ◇ solve a query for a FQDN which points outside your zone
- ◇ solve parallel requests for different FQDN, their servicing should be made in parallel and correct responses should be generated

To test your DNS Name Server you should use your DNS Resolver.

Structure and documentation

The project should be structured as follows:

```
proj2_sn1_sn2:
        dns_server.py
        dns_tests.py
        dns
        dns/resolver.py
        cache
        zone
        documentation.*
        (other support files)
```

Where:

- *sn1* and *sn2* are your student numbers (for example, s123456);

- *dns_server.py* is the python program implementing the DNS Name Server;
- *dns_tests.py* is the python program implementing the tests;
- *dns* is a folder where you store all support files
- *dns/resolver.py* contains the implementation of the resolver.
- *cache* is the cache file used by the DNS Resolver. It should be readable text;
- *zone* is the zone file used by the DNS Name Server. It too should be readable text;
- *documentation.** should explain the implementation;

Interface and Documentation

Your DNS Resolver should be implemented as a library class providing the `gethostbyname` function. This function receives a string and returns a tuple of form : (FQDN, list_of_IP_addresses, list_of_aliases). Your python programs should be run:

```
# running the DNS Server
python dns_server.py [-c|--caching][-t|--ttl time][-p|--port portNum]

# running the set of tests (in case you have implemented runnable tests)
python run_tests.py [-s|--server dns_server][-p|--port portNum]}
```

Where:

- *c* enables caching, by default it is disabled
- *t* sets the ttl that is applied to all cached entries
- *s* is the IP address in string format of the name server
- *p* is the port number at which the name server listens

You do not have to implement to long versions of these parameters (though with frameworks such as argparse it is easy to do). The framework provides *dns_client.py*, a wrapper program over a mock DNS Resolver, which you can use to test your Resolver. To test your Name Server you can use `dig` or `nslookup`.

You need to provide a brief documentation of the software provided. You should present a general flow of how the DNS Resolver and DNS Name Server operate mentioning the relevant flags for authority, query/reply and recursion. You should also describe how you crafted DNS messages (what libraries did you use), how you implemented concurrency, how you generate Transaction IDs, what format you use for storing the cache and what is the policy for removing expired entries from the cache. Also mention any problems you have encountered. Some of these questions can be answered directly by checking the framework provided. (should you use it)

Implementation guidance

As last time, you are provided a framework which implements a significant portion of the parsing message parsing, as required by RFC 1035. You are referred to RFC 1034 and RFC 1035, in particular the algorithms for the Resolver and Name Server. A very good high level overview on how DNS works is found on technet. You could start off with that, then dive into the RFC documents.