Hands-on-3: Domain Name Service

Complete the following hands-on assignment. Do the activities described, and submit your solutions for following questions to your TA. Please submit a doc or a pdf with title like studentID.pdf. You are free to use either Chinese or English. Due time is 2018-10-8 00:00.

This hands-on exercise is designed to help you know more about the Internet's Domain Name System (DNS) and introduce you to a good tool for exploring DNS, Domain Information Groper (dig).

Introduction

Dig is similar with nslookup, which is a useful tool for querying information of domain name. If using windows now, you can type "nslookup www.baidu.com" in command line. Dig is even more powerful than it. You can install dig both in windows or linux(% sudo apt-get install dnsutils).

Question 1: Please briefly answer the role of DNS in your own words.

DNS is actually a general-purpose name management and name resolution system that hierarchically distributes the management of names among different naming authorities and also hierarchically distributes the job of resolving names to different name servers. Its design allows it to respond rapidly to requests for name resolution and to scale up to extremely large numbers of stored records and numbers of requests.

Getting started Here is an simple example use of dig:

```
cse@cse-lab:~$ dig www.sina.com

; <<>> DiG 9.7.3 <<>> www.sina.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56515
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;www.sina.com.                  IN      A

;; ANSWER SECTION:
www.sina.com.           5       IN      CNAME   us.sina.com.cn.
us.sina.com.cn.         5       IN      CNAME   news.sina.com.cn.
news.sina.com.cn.       5       IN      CNAME   jupiter.sina.com.cn.
jupiter.sina.com.cn.    5       IN      CNAME   auriga.sina.com.cn.
auriga.sina.com.cn.     5       IN      A       61.172.201.239
auriga.sina.com.cn.     5       IN      A       61.172.201.194
auriga.sina.com.cn.     5       IN      A       61.172.201.195
auriga.sina.com.cn.     5       IN      A       61.172.201.237

;; AUTHORITY SECTION:
```

```
sina.com.cn.            5       IN      NS      ns3.sina.com.cn.
sina.com.cn.            5       IN      NS      ns4.sina.com.cn.
sina.com.cn.            5       IN      NS      ns1.sina.com.cn.
sina.com.cn.            5       IN      NS      ns2.sina.com.cn.

;; ADDITIONAL SECTION:
ns1.sina.com.cn.        5       IN      A       202.106.184.166
ns2.sina.com.cn.        5       IN      A       61.172.201.254
ns3.sina.com.cn.        5       IN      A       123.125.29.99
ns4.sina.com.cn.        5       IN      A       121.14.1.22

;; Query time: 5 msec
;; SERVER: 192.168.110.2#53(192.168.110.2)
;; WHEN: Thu Mar  5 22:56:38 2015
;; MSG SIZE  rcvd: 320
```

Most of the information we are interested in is in the ANSWER section, colored in red. The five field of this section are name, expire time, class, type, data. You can ignore the "class" field because this is nearly always IN for Internet.The AUTHORITY section contains records of type NS, indicating the names of DNS servers that have name records for a particular domain. Here, we can see that four DNS servers are responsible for answering requests for names in the www.sina.com domain. The other sections are easy to understand.

Question 2: The type field have a few different values to indicate the kind of this record. What do "A", "NS" and "CNAME" mean?

A (the IP address),
CNAME(Canonical name record),
TXT (text annotations),
MX (mail exchanges), and
NS (nameservers).

More Options

When just wanting a simple result for a domain, we can add "+short" in the command. (Try %dig +short www.sina.com)

When you want to find the domain name of some ip, try adding "-x" in the command. (Try %dig -x 173.194.127.80)

There are many interesting options like -f, +domain and +trace. Read the man page of dig yourself.

Question 3: How can we ask a specific dns server (instead of the default) for information about a domain name? When I use "dig www.baidu.com",the DNS server is 192.168.110.2. However if this server crashed and I have to ask the server 8.8.8.8, what command should I use?

通过dig -x查找该ip对应的DNS服务器

$ dig -x 8.8.8.8 +short
google-public-dns-a.google.com.
8.8.8.8是google的一个公共DNS服务器

Understanding hierarchy

Dig only prints the final result of the recursive search. You can mimic the individual steps of a recursive search by sending a request to a particular DNS server and asking for no recursion, using the +norecurs flag. For example, to send a non-recursive query to one of the root servers:

```
%dig @a.root-servers.net www.sina.com +norecurs
```

As you can see, the server does not know the answer and instead provides information about the servers most likely to be able to provide authoritative information. In this case, the best the root server knows is the identities of the servers for the com. domain.

Question 4: Do you know the process of solving domain name "lirone.csail.mit.edu"? You need to go through the steps of resolving a particular hostname, mimicing a standard recursive query. Assuming it knows nothing else about a name, a DNS resolver will ask a well-known root server. The root servers on the Internet are in the domain root-servers.net. You can use "%dig . ns" to get the list of 13 root servers.You can show us the result of each step or briefly introduce your idea.[Hint: you should start from "edu"]

Something interesting

Type the command "%dig www.twitter.com +trace" and "dig www.baidu.com +trace".Do you find some difference between the two outputs? Type the command "%dig www.twitter.com @1.0.0.0" and "dig www.baidu.com @1.0.0.0". Do you find some difference between the two outputs?(Does 1.0.0.0 exits？ You can try "%ping 1.0.0.0".)

Repeat typing the command "%dig www.twitter.com +trace" for a few times. Do you think the results are weird?

www.twitter.com. received bytes directly from one of root-servers,
www.twitter.com. doen't have name server.
You can check physical location of these results(ip).
compared with www.baidu.com. from one of name-servers which is a descendant from the root-servers.

Question 5: Please explain the above phenomenon. Have a guess!

Type the command "%dig www.google.com", mostly you cannot connect to google using the ip you get or the domain name "www.google.com". However you can connect to google with some ips like 61.219.131.99 or 74.125.224.18.

Question 6: The ips which dig returns to you belong to google indeed. Give the reason for the above phenomenon.

【optional】 Iodine

This is a piece of software that lets you tunnel IPv4 data through a DNS server. This can be usable in different situations where internet access is firewalled, but DNS queries are

allowed. Here is link： https://github.com/yarrick/iodine If you are interested in this, have a try.