DNS

The Domain Name System (DNS) translates hostnames to IP addresses. As discussed in class, much can go on “under the covers,” invisible to the DNS clients, as the hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client’s DNS query. From the DNS client’s standpoint, however, the protocol is quite simple: a query is formulated to the local DNS server and a response is received from that server. We examine these interactions from the clients perspective in these exercises.

nslookup

The Linux/Unix nslookup tool allows the hosts to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result. You can type nslookup commands on in a terminal window on your Mac. For example, consider the following terminal session. The client host in my Mac located on Science Center, where the default local DNS server is Cheers. When running nslookup, if no DNS server is specified, then nslookup sends the query to the default DNS server. The first command nslookup www.smith.edu asks for the IP address of the host www.smith.edu. The response from this command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer (that would be server 149.130.10.16 who happens to be Cheers); and (2) the answer itself, which is the host name and IP address of www.smith.edu. Although the response came from the local DNS server at Polytechnic University, it is quite possible that this local DNS server iteratively contacted several other DNS servers to get the answer,

```
  rshulls-MacBook-Pro:~ rshull$ nslookup www.smith.edu
  Server: 149.130.10.16
  Address: 149.130.10.16#53

  Non-authoritative answer:
  www.smith.edu canonical name = websvr.smith.edu.
  Name: websvr.smith.edu
  Address: 131.229.64.19
```

```
  rshulls-MacBook-Pro:~ rshull$ nslookup -type=NS smith.edu
  Server: 149.130.10.16
  Address: 149.130.10.16#53

  Non-authoritative answer:
  smith.edu nameserver = ns3.umass.edu.
  smith.edu nameserver = babel.smith.edu.
  smith.edu nameserver = ns1.smith.edu.
  smith.edu nameserver = ns1.umass.edu.
  smith.edu nameserver = ns2.umass.edu.
```
Authoritative answers can be found from:
babel.smith.edu internet address = 131.229.64.2

rshulls-MacBook-Pro:~ rshull$ nslookup www.smith.edu babel.smith.edu
Server: babel.smith.edu
Address: 131.229.64.2#53

www.smith.edu canonical name = websvr.smith.edu.
Name: websvr.smith.edu
Address: 131.229.64.19

The second command, \texttt{nslookup -type=NS smith.edu}, provides the “-type=NS” option and the domain “smith.edu”. This causes \texttt{nslookup} to send a query for a type-NS record to the default local DNS server. In words, the query is saying, “please send me the host names of the authoritative DNS for smith.edu.” (When the \texttt{-type} option is not used, \texttt{nslookup} uses the default, which is to query for type A records.) The answer, displayed in the above transcript, first indicates the DNS server that is providing the answer (which is Cheers, our default local DNS server) along with three five smith.edu nameservers. Each of these servers might be an authoritative DNS server for the hosts on the Smith campus. However, \texttt{nslookup} also indicates that the answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative Smith DNS server. Finally, the answer also includes the IP addresses of the authoritative DNS servers at Smith. (Even though the type-NS query generated by \texttt{nslookup} did not explicitly ask for the IP addresses, the local DNS server returned this “for free” and \texttt{nslookup} displays the result.)

Finally consider the third command:

\texttt{nslookup www.smith.edu babel.smith.edu.}

In this example, we indicate that we want to the query sent to the DNS server \texttt{babel.smith.edu} rather than to the default DNS server. Thus, the query and reply transaction takes place directly between our querying host and \texttt{babel.smith.edu}. In this example, the DNS server \texttt{babel.smith.edu} provides the IP address of the host \texttt{www.smith.edu}.

Now that we have gone through a few illustrative examples, you are perhaps wondering about the general syntax of \texttt{nslookup} commands. The syntax is:

\texttt{nslookup -option1 -option2 host-to-find dns-server}

In general, \texttt{nslookup} can be run with zero, one, two or more options. And as we have seen in the above examples, the \texttt{dns-server} is optional as well; if it is not supplied, the query is sent to the default local DNS server.

1) Run \texttt{nslookup} to obtain the IP address of a Web server in Asia. What is the IP address of that server?
2) Run \texttt{nslookup} to determine the authoritative DNS servers for a university in Europe.