Linux or Mac/Windows Based DNS Lab with Wireshark
2015

Instructions

As described in Section 2.5 of the textbook, the Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a query to its local DNS server, and receives a response back. As shown in Figures 2.21 and 2.22 in the textbook, 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.

Before beginning this lab, you'll probably want to review DNS by reading Section 2.5 of the text. In particular, you may want to review the material on local DNS servers, DNS caching, DNS records and messages, and the TYPE field in the DNS record.

1. Using host and Nslookup to find DNS records

Record the responses from the following commands.
Instead of using nslookup for looking up DNS records, we will use the host command.

To see how it works, type: **$ host www.mit.edu**

To set the nameservers for mit.edu, use the following command.

$ host -t NS mit.edu

The above command gives us the authoritative nameservers for doman, mit.edu.
1a. Write them down.

Run the man page on host to see more options, type: $ man host
If you are at home on a Windows system, host will not work, just use nslookup below

You can do the same thing with Nslookup, type: **$ nslookup mit.edu**
Note the non-authoritative reponse.

Now, to see the authoritative nameservers, type: **$ nslookup -type=NS mit.edu**
So, now use one of the nameservers to get an authoritative response.
Type: **$ nslookup**
> server {one of dns servers from mit.edu}
> mit.edu

Do the following (and write down the results) Google is your friend:

1. Run host or nslookup to obtain the IP address of a Web server in Asia.
2. Run host or nslookup to determine the authoritative DNS servers for a university in Europe.
3. Run host or nslookup to obtain the the mail servers for Yahoo.com.
   Hint - Run nslookup -type=MX yahoo.com

2. Tracing DNS with Wireshark

Now that we are familiar with host, we're ready to get down to some serious business. Let's first capture the DNS packets that are generated by ordinary Web- surfing activity.

- Download a wireshark capture file: http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip
  Save it and extract the trace: dns1-ethereal-trace-1

- Open the trace file in wireshark.

Answer the following questions:

4. Locate the DNS query and response messages. Are they sent over UDP or TCP?
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
6. To what IP address is the DNS query message sent?
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
8. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
9. This web page contains images. Before retrieving each image, does the host in the trace file issue new DNS queries?