Computer Networking Lab DNS

Please capture some related screenshots to support your answer.

As described in 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 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 the textbook. 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.

Part 1. Using ipconfig

ipconfig (for Windows) and ifconfig (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we'll only describe ipconfig, although the Linux/Unix ifconfig is very similar. ipconfig can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on.

Do the following steps:

- Select Run from the Start Menu of your computer, type cmd and press OK.
- In the command screen window type "ipconfig /all" and press enter. The current TCP/IP settings of your network are displayed.

Answer the following questions:

1. What is the host name?
2. What is the physical (data-link) address?
3. What is the IP address?
4. What is the IP address of the default gateway?

Part 2. Tracing DNS with Wireshark

ipconfig is also very useful for managing the DNS information stored in your host. We learned that a host can cache DNS records it recently obtained. To see these cached records, after the prompt C:\> provide the following command: "ipconfig /displaydns"

Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter: "ipconfig /flushdns"
Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

Do the following steps:

- Use ipconfig to empty the NDS cache in your host.
- Open your browser and empty your browser cache.
  (For example, you may try to do this under Firefox, select Tools->Clear Recent History and check the Cache box, or for Internet Explorer, select Tools->Internet Options->Delete File; these actions will remove cached files from your browser's cache.)
- Start packet capture in Wireshark.
- With your browser, visit the Web page: www.ntut.edu.tw
- Stop packet capture
- Enter "ip.addr == your_IP_address" into the filter

Answer the following questions:

5. Locate the DNS query and response messages for the Web page:www.ntut.edu.tw. Are they sent over UDP or TCP?
6. What is the destination port for the DNS query message? What is the source port of DNS response message?
7. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?