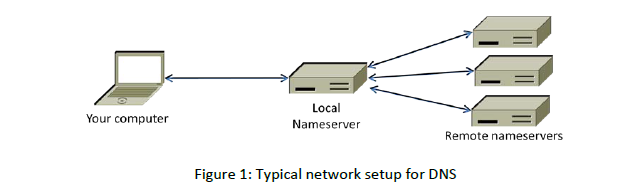
Lab Exercise – DNS

**Objective**

DNS (Domain Name System) is the system and protocol that translates domain names to IP addresses and more. DNS is covered in §7.1 of your text. Review that section before doing this lab.

**Network Setup**

In a typical network, your computer contacts a local DNS nameserver to resolve domain names to IP ad-dresses. The local nameserver may be another computer in your company network, a computer at your ISP, or your wireless AP. It exchanges a series of messages with remote DNS nameservers all over the Internet to perform the resolution. The setup is as shown in the figure below.



We assume this setup for the lab, and it has an important implication: the trace we gather at our com-puter will see the exchanges between our computer and the local nameserver, but not between the lo-cal nameserver and the remote nameservers.

**Step 3: Inspect the Trace**

*To explore the details of DNS packets, select a DNS query expand its Domain Name System block (by us-ing the “+” expander or icon).* Your display should be similar to the one shown in our figure, with a series of packets with protocol DNS. The first packets should correspond to your dig commands, followed by DNS traffic produced by your browser. We have selected the first DNS message.



Figure 3: Trace of DNS traffic showing the details of the DNS header

*Look for the following details:*

• The DNS block follows the IP and UDP blocks. This is because DNS messages are carried in UDP segments within IP packets. You will see that the UDP port used by a nameserver is 53.

• The DNS header starts with a Transaction ID that is used to link a request and the corresponding reply – they both carry the same Transaction ID.

• Next come a set of flags that you can expand. They indicate whether the DNS message is a query or response, amongst other details.

• Then come the number of query, answer, authority and additional records. These fields con-clude the header.

• After the DNS header, the remainder of the message consists of the indicated number of query, answer, authority and additional records. Often there will be only one query – for the IP address of the domain name we are seeking – but there may be many of the other records. These records are grouped in sections, such as the Authority section for all of the authority records. Each query has a Type code that indicates the kind of record sought, whether an IP address or other-wise. Each of the other records also has a Type code that indicates whether it carries an IP ad-dress of a host, the name of a nameserver, or something else. The format of an individual record depends on its type. The entire DNS message is designed to fit within one UDP message.

• Wireshark may show other information, such as the number of the packet that carries the response to this request or the response time for the DNS exchange, but this is derived information. It is not actually carried on any packet.

*Repeat the above to look at a DNS response.* You should see a larger set of records in this message; while DNS queries mostly serve to carry the query, DNS responses often return a set of useful information.

**Step 4: Details of DNS Messages**

*Select the first DNS query that corresponds to your* dig *commands and expand its DNS block.* Likely this query is the first packet in your trace, with the first several packets corresponding to your dig commands, followed by other DNS traffic produced by your browser. To check, see if there are several queries that list the domain you chose in the Info column, each followed by a response. We will use these DNS messages to study the details of the DNS protocol. Sometimes there may be other DNS traffic interspersed with these queries due to background activity; you should ignore these extraneous packets.

*Look at the DNS header, and answer the following questions:*

1. *How many bits long is the Transaction ID? Based on this length, take your best guess as to how likely it is that concurrent transactions will use the same transaction ID.*

Transaction ID = 2 bytes long = 16 bits long

Yes?

2. *Which flag bit and what values signifies whether the DNS message is a query or response?*

Flag = 0x0120 standard query

0... .... .... .... = Response: Message is a query

.000 0... .... .... = Opcode: Standard query (0)

3. *How many bytes long is the entire DNS header?* Use information in the bottom status line when you select parts of the packet and the bottom panel to help you work this out.

DNS header =12 bytes long

*Now examine the responses to the* dig *DNS queries you made.* The initial response should have provided another nameserver one step closer to the nameserver, but not the final answer. You should find that it includes the original query in its Query section. It will also include records with both the name of the nameservers to contact next, and the IP addresses of those nameservers. The final response in this series will include the IP address of the domain name – this is the answer to the query.

*Look at the body of the DNS response messages, and answer the following questions:*

4. *For the initial response, in what section are the names of the nameservers carried? What is the Type of the records that carry nameserver names?*

Authoritative nameservers

Type of records? The records themselves are text items. The entry says type NS. Not sure which of the 2 is being asked.

5. *Similarly, in what section are the IP addresses of the nameservers carried, and what is the Type of the records that carry the IP addresses?*

Additional records

Also text items, type A or AAAA

6. *For the final response, in what section is the IP address of the domain name carried?*

Answers