Goals of this lab:

- Learn how the domain name system works
- Learn about tools to test and troubleshoot DNS
- Learn how to deploy a basic DNS service

Prerequisites: LXB, NET
## Table of Contents

**PREPARATION** ......................................................................................................................................................... 1
  Exercise 1: Review and preparation .................................................................................................................. 1

**MAIN LAB** ................................................................................................................................................................ 3
  Part 1: Using host and dig ................................................................................................................................... 3
  Simple queries with host ........................................................................................................................................ 3
  Exercise 2: Address queries with host ............................................................................................................. 4
  Exercise 3: Other queries using host ................................................................................................................ 4
  Simple queries with dig ........................................................................................................................................ 4
  Exercise 4: Queries with dig .............................................................................................................................. 5
  Part 2: Nameserver configuration ..................................................................................................................... 5
  Exercise 5: Basic DNS server installation and configuration ...................................................................... 6
  Delegation of your `group.sysinst.ida.liu.se` zone ............................................................................................ 6
  Exercise 6: Delegation of your `group.sysinst.ida.liu.se` zone ....................................................................... 6
  Configuration and delegation of your `in-addr.arpa` (reverse) zone .............................................................. 6
  Exercise 7: Delegating the reverse zone .......................................................................................................... 7
PREPARATION

Do these exercises before proceeding with the main lab. On-line documentation, RFCs and man pages should be sufficient to answer the questions.

Exercise 1: Review and preparation

1-1 Review the section on DNS from the basic network course.

1-2 Answer the following questions (the information can be found in e.g. the RFCs that describe DNS):

(a) What is an authoritative name server? What is its role in DNS?

(b) What is the difference between a domain and a zone?

(c) What is the difference between a recursive and a non-recursive query in DNS? When is each type of query used?

(d) What is the purpose of delegation in DNS?

(e) What is a resource record? What does a resource record consist of?

(f) DNS messages contain answer, authority and additional sections. What is the purpose of each section?

(g) How does the DNS protocol indicate if an answer comes from an authoritative name server or not? How does the DNS protocol indicate whether a query is recursive or not?

(h) Explain what glue records are and when they are necessary.

1-3 Which zone in DNS contains PTR records corresponding to IP addresses in the network 10.131.24.64/27? Name some other networks that have PTR records in the same zone. What is the problem with delegating authority over the DNS records corresponding only to 10.131.24.64/27?

1-4 Explain the purpose of classless in-addr.arpa delegation. Explain how it works.

Report: Answers to the questions above.
The domain name system (DNS) is a critical part of the Internet infrastructure. In this lab you will experiment with DNS-related tools and set up a basic DNS service for your network. It is important that you understand the concepts of DNS. If you don’t, the exercises will be very difficult to complete in a timely fashion.

**Time taken 2005:** 1-17 hours, average 10 hours (no accurate data available for 2006)

**Past problems:** Most problems encountered in this lab have been due to the group not fully understanding what they are doing and how the configuration files work (resulting in strange configurations); not understanding key concepts, such as “zone” in DNS (resulting in strange configurations and bad test cases); unstructured work methods (resulting in a lot of duplicated and wasted effort); and lack of attention to detail (resulting in bad test cases, small but significant configuration errors and a lot of wasted effort).

### Part 1: Using host and dig

The two tools most commonly used when working the DNS are **host** and **dig**. Both are pure DNS tools—they will not query any other information source—and both allow you to manipulate DNS queries at a fairly low level. The **host** utility is convenient to run simple queries. The **dig** utility allows more detailed manipulation of DNS queries, and essentially allows the user to manipulate any part of the protocol.

You may find documents that refer to a tool named **nslookup**. In theory, **nslookup** is an alternative to **host**, but **nslookup** is so insistent on presenting the user with some kind of answer, that it may mask actual problems or behaviors in DNS. Do not use **nslookup** unless it is the only option or if you don’t care if the answer is 100% accurate. If you do use **nslookup** ensure that you understand all its output.

There are several versions of **host** and **dig** available. These labs assume the Debian packages **dnsutils** and **host** are installed.

#### Simple queries with host

The simplest query possible with **host** is to request the address corresponding to a particular name. It is possible to direct queries to a particular name server. This is particularly useful when troubleshooting cache problems, where two name servers might have contradictory information about the same name.

<table>
<thead>
<tr>
<th><strong>host name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Query the default nameserver for the address corresponding to <strong>name</strong>. The default name server is usually given by the file /etc/resolv.conf</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>host name nameserver</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Query <strong>nameserver</strong> for the address corresponding to <strong>name</strong>. Whenever possible, use an IP address, not a name, for <strong>nameserver</strong>, or DNS is involved in finding the nameserver as well – not what you</td>
</tr>
</tbody>
</table>
Exercise 2: Address queries with host

2-1 Use the host tool to answer the following questions:
(a) What is the address of informatix.ida.liu.se?
(b) What is the address of www.ida.liu.se?
(c) What is the address of liu.se?

2-2 Compare the output of `host www.ida.liu.se ns3.liu.se` and `host www.ida.liu.se dns.liu.se` and answer the following questions:
(a) Why is there no answer in the first query but in the second query?
(b) Both answers are correct, even though they differ. Explain why.

Report: Answers to the questions above.

With additional command line options, `host` can be used to extract other information from the domain name system. The full details are in the man page for `host`. The following are some of the more common and useful options (these apply to the BIND 9 version of `host`; earlier versions have slightly different options:

- `t querytype`
  Query for resource records of type `querytype`.
- `a`
  Query for any resource record.
- `l zone`
  List the entire contents of `zone`. This option attempts to initiate a zone transfer, which may not be permitted by the queried name server.
- `v`
  Display additional debugging information, such as the exact DNS queries sent.

Exercise 3: Other queries using host

3-1 Use `host` to find out which name servers are authoritative for the zone adlibris.se. Which organization(s) operate them?

3-2 Use `host` to list all records in the sysinst.ida.liu.se zone and `wc` to count them. How many records are there?

3-3 Use `host` to find out all information you can about the name ida.liu.se (i.e. the name itself, not the contents of the zone). What did you find out? How can you be sure that is all the information that is available?

Report: The commands used above and answers to the questions.

Simple queries with `dig`

The `host` utility is ideal for looking up information in DNS, but its use as a diagnostic tool is limited. For diagnostic use, the `dig` utility is better since it allows the user to manipulate almost every aspect of the query, and displays all information available about the response. The problem that many beginners encounter with `dig` is that it doesn’t try to guess what the user wants. For example, whereas `host` will automatically detect that the user has entered an IPv4 address, and infer that the user probably wants
to look up the corresponding PTR record in the in-addr.arpa zone, dig will merrily attempt to locate an A record for that address.

**Output from dig**

The output of `dig` is more complex than the output of `host`. Note that almost all sections of the output can be suppressed (and additional output is available for those who need it) using command-line options. Essentially, the output is a protocol dump of the response packet. Here are some common (and simple) ways to use `dig`:

- **dig name**
  Send a recursive query to the default name server (determined by ` /etc/resolv.conf`) for the A record corresponding to `name`.

- **dig –x address**
  Send a recursive query to the default name server for the PTR record corresponding to IPv4 address `address`. Essentially, the `-x` option changes the default query type to PTR, reverses the order of components in its argument and appends in-addr.arpa.

- **dig query nameserver**
  Query `nameserver` instead of the default name server.

**Exercise 4: Queries with dig**

4-1 Use `dig` to answer the following questions:

(a) What is the address of ida-gw.sysinst.ida.liu.se?
(b) Which nameservers have authoritative information for sysinst.ida.liu.se?
(c) Which name corresponds to the IPv4 address 130.236.189.1?

4-2 Use the trace feature of `dig` to answer the following questions:

(a) What nameservers are consulted in a query for the A record of www.ida.liu.se?
(b) What nameservers are consulted when determining the address of update.microsoft.com? Note that the presence of a CNAME record makes this question different from the previous one: you will need to run `dig` more than once to get the answer!

**Report:** Answers to all the questions above, including the commands used.

**Part 2: Nameserver configuration**

Your network needs a name server. Please consult the course home page to determine which names and addresses your hosts should have (you should already have done this).

Although you may use any DNS software you want for this task, BIND is recommended. BIND may not be the hottest nameserver software out there, but it gets the job done and has proven fairly straightforward to work with, even for inexperienced users. The most comprehensive documentation available is the BIND 9 Administrator Reference Manual (also known as Bv9ARM), currently available from www.bind9.net. This is a reference manual, so it will be fairly useless unless you understand how DNS works and what you want to do.

DNS service is a critical part of the network infrastructure, and you will be required to do a quality implementation of the service. Your DNS service will be authoritative for two zones (it will be the master server): your normal zone (e.g. a1.sysinst.ida.liu.se) and your reverse zone (where PTR records are stored).
Before you start you should make sure you have everything planned out in detail. You need to be particularly careful with TTL and other cache parameters. Badly chosen cache parameters can seriously harm your ability to complete this exercise (and hence all that require DNS functioning).

Testing tip: since the DNS is a distributed system, name resolution problems can be due to a number of different issues. Your tests should address each possible issue in isolation. Your first set of test cases should query your nameserver directly to see that it behaves as expected. That way, once you’ve set up delegation you know that the basic functions are present, and any new problems are related to delegation. You should use dig for testing, since it shows you the entire response, not just the answer section.

Exercise 5: Basic DNS server installation and configuration

Your DNS server is to be installed on your server, not on your router. No normal router includes a full-featured DNS server (although some consumer grade broadband routers have some limited DNS serving or DNS forwarding features).

5-1 Install a DNS server on your server and configure it to meet the following requirements:
(a) It must respond authoritatively to all non-recursive queries for names in the zones you are authoritative for.
(b) It must respond to all recursive queries from the hosts on your own network.
(c) It must not respond to any recursive queries from any outside host (i.e. host not on your own network).
(d) Apart from the queries in (a), it should not respond to any queries from any outside host.
(e) It must contain valid zone data for your zone(s).
(f) The cache parameters must be chosen sensibly (i.e. you are expected to be able to motivate your choice).
(g) It must not be susceptible to the standard cache poisoning attacks. See http://www.kb.cert.org/vuls/id/800113 for details. Test your DNS server using porttest.dns-oarc.net (see http://www.dns-oarc.net/oarc/services/porttest).

5-2 Install zone data for your normal zone.

Report: Automated test cases that verify that your system meets the requirements.

Delegation of your group.sysinst.ida.liu.se zone

After basic configuration you need to have the group.sysinst.ida.liu.se zone delegated from the sysinst.ida.liu.se nameserver. Since that server is under external control, you cannot install the zone file data yourself.

Plan delegation carefully. There will be a delay from the time you present your lab assistant with a request for delegation to the time when it is operative. Every error you make will cost a significant amount of time.

Exercise 6: Delegation of your group.sysinst.ida.liu.se zone

6-1 List the exact resource records that you want installed in the sysinst.ida.liu.se zone (fully qualified name, record type and record data) in order to have your group.sysinst.ida.liu.se zone delegated to your name server and give to your lab assistant.

Report: Automated test cases that verify that your system meets the requirements.

Configuration and delegation of your in-addr.arpa (reverse) zone

The in-addr.arpa (a.k.a. reverse) zone, that enables translation of IP addresses to host names, is a bit tricky. Each dot in a domain name indicates a point where delegation can take place. For example, if the
domain name is 1.189.236.130.in-addr.arpa, delegation can take place at 189.236.130.in-addr.arpa, 236.130.in-addr.arpa, 130.in-addr.arpa, in-addr.arpa and arpa. In the context of this course, we need to delegate very small zones that will hold PTR records for only a few addresses. The zone 189.236.130.in-addr.arpa has been delegated to the course name server, and it would be ideal to further delegate parts of that zone to student servers. The problem is that there are no more dots left in the names, so no more delegation can take place.

There are two common ways of dealing with this: by using CNAME records (preferred by BIND users) or by delegating each name as a separate zone (preferred by e.g. djbdns users).

The use of CNAME records is called “classless in-addr.arpa delegation, and works by placing CNAME records in the delegating name server (in our case the course name server) that point to names in a zone that can be delegated (i.e. a subdomain of sysinst.ida.liu.se or 189.236.130.in-addr.arpa), and delegating that zone.

An alternative to classless in-addr.arpa delegation is to delegate each name in the reverse zone separately (in other words, you will end up with one zone per address you want to be able to look up). If you run djbdns this method is preferred. If you are using BIND, delegating each name separately will result in a much larger configuration file than classless in-addr.arpa delegation does. You may use either method.

An important part of this exercise is reading and understanding the relevant documentation on the topic.

Exercise 7: Delegating the reverse zone

7-1 Install the reverse zone on your name server and check that it works.

7-2 List the exact resource records (fully qualified name, record type and record data) that you need installed in the sysinst.ida.liu.se zone (fully qualified name, record type and record data) in order to implement classless in-addr.arpa delegation for your reverse zone, and hand the list to your lab assistant.

Report: Automated test cases that verify that your system meets the requirements.
Complete this feedback form individually at the end of the lab and hand it to the lab assistant when you finish. Your feedback is essential for improving the labs. Each student should hand in a feedback form. Do not cooperate on completing the form.

You do not need to put your name on the feedback form. Your feedback will be evaluated the same way regardless of whether your name is on it or not. Your name is valuable to us in case you have made and comments in the last section that need clarifications or otherwise warrant a follow-up.

For each section, please rate the following (range 1 to 5 in all cases).

- **Difficulty**: Rate the degree of difficulty (1=too easy, 5=too difficult)
- **Learning**: Rate your learning experience (1=learned nothing, 5=learned a lot).
- **Interest**: Rate your interest level after completing the part (1=no interest, 5=high interest).
- **Time**: How long did the part take to complete (in minutes)?

<table>
<thead>
<tr>
<th></th>
<th>Difficulty</th>
<th>Learning</th>
<th>Interest</th>
<th>Time (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part 1: Using host and dig</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part 2: Nameserver configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please answer the following questions:

- What did you like about this lab?
- What did you dislike about this lab?
- Make a suggestion to improve this lab.
Complete this feedback form **individually** at the end of the lab and hand it to the lab assistant when you finish. Your feedback is essential for improving the labs. Each student should hand in a feedback form. Do not cooperate on completing the form.

You do not need to put your name on the feedback form. Your feedback will be evaluated the same way regardless of whether your name is on it or not. Your name is valuable to us in case you have made and comments in the last section that need clarifications or otherwise warrant a follow-up.

For each section, please rate the following (range 1 to 5 in all cases).

- **Difficulty**: Rate the degree of difficulty (1=too easy, 5=too difficult)
- **Learning**: Rate your learning experience (1=learned nothing, 5=learned a lot).
- **Interest**: Rate your interest level after completing the part (1=no interest, 5=high interest).
- **Time**: How long did the part take to complete (in minutes)?

<table>
<thead>
<tr>
<th>Difficulty</th>
<th>Learning</th>
<th>Interest</th>
<th>Time (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part 1: Using host and dig</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part 2: Nameserver configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please answer the following questions:

- What did you like about this lab?

- What did you dislike about this lab?

- Make a suggestion to improve this lab.