DNS Fundamentals

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

REVISION: 1.4 [2008-08-05]

Table of Contents

PRELAB

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 using RFCs 1032, 1033, 1034 and 1035:

(a) What is an authoritative name server?

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

(c) What does delegation mean?

(d) What is a resource record?

(e) How does the DNS protocol indicate if an answer comes from an authoritative name server or not?

(f) Describe the answer, authority and additional sections of the DNS protocol.

(g) How can a name server tell if a client wants a recursive query or not?

(h) What resource records are required to do delegation?

1-3 Read the man page for `dig` and `host`, and answer the following questions:

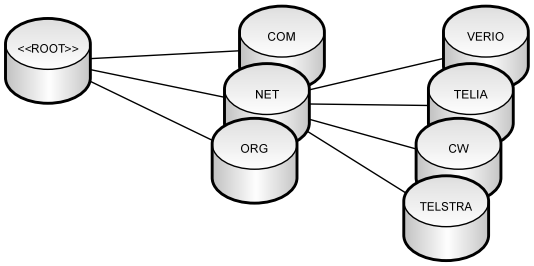
(a) How do you send a query to a specific name server using `host`?

(b) How do you send a query to a specific name server using `dig`?

(c) What does the `+trace` option to `dig` do?

Report: Answers to the questions above.

MAIN LAB



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 (which gives you `dig` from BIND 9 and host from BIND 8).

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.

`host` *`name`*

Query the default nameserver for the address corresponding to *name*. The default name server is usually given by the file /etc/resolv.conf

`host` *`name nameserver`*

Query *nameserver* for the address corresponding to *name*. Whenever possible, us an IP

address, not a name, for *nameserver*.

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 udns1.ultradns.com` 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:

`-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.

`-d`, `-dd`

Display additional debugging information, such as the exact DNS queries sent.

`-Z`

Output in full zone file format. This includes, among other things, the TTL field.

Exercise 3: Other queries using host

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

3-2 Use `host` to find out how long records in the .com zone should be cached. How long should they be cached?

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

3-4 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?

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.

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.

`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) What 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!

Report: Answers to all the questions above, including the commands used and their output.

Part 2: Nameserver configuration

Your network needs a name server. Please consult the course home page to determine what 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 piece of nameserver software out there, but it gets the job done and has proven fairly straightforward to work with, even for inexperienced users.

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 forward 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 consider using `dig` for testing, since dig 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 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 to recursive queries for any name from your hosts.

(b) It must *not* respond to recursive queries for any name from any outside host.

(c) It must respond authoritatively to iterative queries for your zone(s) from any host.

(d) It must contain valid zone data for your zone(s).

(e) The cache parameters must be chosen sensibly.

(f) It must not be susceptible to the latest cache poisoning attacks (or any old ones). 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 the forward zone.

Report: Test protocols that demonstrate that your DNS service is functioning properly for the zones installed so far. You will need several test cases – one per specific requirement is probably a minimum.

Delegation of the forward zone

After basic configuration you need to have the forward 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 the forward 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 forward zone delegated to your name server and give to your lab assistant.

Report: Test protocols that demonstrate that delegation of the forward zone works. This will probably only require one or two test cases.

Configuration and delegation of the reverse zone

The reverse zone 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 sub-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 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: Test protocols that demonstrate that your DNS service is functioning properly for the zones installed so far. These test cases are probably similar to those you wrote for exercise 5. Test protocols that demonstrate that delegation of the reverse zone works. These will be similar to those for exercise 6.

FEEDBACK FORM DNS

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)?

	Difficulty	Learning	Interest	Time (minutes)
Prelab				
Part 1: Using host and dig				
Part 2: Nameserver configuration				
Overall				

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.

FEEDBACK FORM DNS

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)?

	Difficulty	Learning	Interest	Time (minutes)
Prelab				
Part 1: Using host and dig				
Part 2: Nameserver configuration				
Overall				

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.

FEEDBACK FORM DNS

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)?

	Difficulty	Learning	Interest	Time (minutes)
Prelab				
Part 1: Using host and dig				
Part 2: Nameserver configuration				
Overall				

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.