Oscar Petersson, Matteus Laurent
oscpe262, matla782

TDDI41 Lab report

Högskoleingenjörsutbildning i datateknik, 180 hp

Laboration report - December 15, 2016
System Administration
TDDI41, Linköpings universitet

Assistant:
Jon Dybeck
IDA

DNS

Exercise 1: Review and preparation

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.

A name server which answers queries about names in a zone.

b) What is the difference between a domain and a zone.

A domain is a subtree of the namespace, and a zone is a part of the namespace of which a NS is authoritative. Zone $\subseteq$ Domain

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

A recursive query will not return until it has a complete answer, whereas the non-recursive can return a "partial" answer—i.e. "I don't know, but ask this other guy ...".

Recursive resolving should foremost be used to focus the caching to specific machines rather than having entire subnets' hosts handle their own caching.

Iterative resolving is always found on authorative name servers.

d) What is the purpose of delegation in DNS.

The purpose of delegation is to delegate administration of DNS zones, effectively limiting the branching factor for each NS.

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

An RR consists of node name (NAME), record type (TYPE), class code (CLASS), TTL, length of the RDATA field (RDLENGTH), and data of type-specific relevance (RDATA) such as IP address and hostname.

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

"Answer" lists the answer to the query (Address record, Canonical name record).

"Authority" lists the authorities for the query.

"Additional" lists other relevant info related to the query, such as addresses of the name servers.

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.

In the header:

Authorative name server answer: [AA]
Recursive query: [RD]

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

Glue records are [A] records, held higher in the tree, for delegated zone name servers.

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.

PTR records corresponding to IP addresses in the network 10.131.24.64/27 are contained in `[24.131.10.in-addr.arpa.]`. Another network that have PTR records in the same zone would be 10.131.24.96/27, and so would 10.131.24.128/28.

The problem with delegating authority over the DNS records corresponding only to 10.131.24.64/27 is that we don't delegate PTR records, but zones. The most specific zone we can delegate is 24.131.10.in-addr.arpa. unless *1-4*.

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

Classless in-addr.arpa delegation allows for narrower delegation of zones within an IP-range, not limiting us to 256 address blocks. Using the RFC 2317 an authority uses CNAMEs to insert subdomains that can then be delegated. For instance, the subnet 172.20.24.8/29 could be delegated as 8-15.24.20.172.in-addr.arpa, with logical CNAMEs such as 8.8-15.24.20.172.in-addr.arpa, 9.8-15.24.20.172.in-addr.arpa, and so on.

2-1

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.

informatix.ida.liu.se has address 130.236.177.26

b) What is the address of www.ida.liu.se.

www.ida.liu.se is an alias for informatix.ida.liu.se, i.e. 130.236.177.26

c) What is the address of liu.se.

liu.se has address 130.236.5.6

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.

a/b) www.ida is not within the zone for ns3, but within the domain for dns.liu.se.

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.

```
$ host -a adlibris.se a.ns.se

;; AUTHORITY SECTION:
adlibris.se. 86400 IN NS c.ns.ip-only.net.
adlibris.se. 86400 IN NS b.ns.ip-only.net.
adlibris.se. 86400 IN NS a.ns.ip-only.net.
```

*Which organization(s) operate them?*ip-only.net

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.

```
$ host -l sysinst.ida.liu.se ns.ida.liu.se | sed '1,/^$/d' | wc -l
125
```

3-3

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.

```
$ host -a ida.liu.se $(host -av ida.liu.se | grep SOA \
| sed 's/.*SOA//g ; s/\.\ .*//g ; s/\t//g')
```

We found the records (A,AAAA,MX,SOA,NS) regarding the zone, and glue records for the name servers.

This is all the information available as the ida.liu.se domain is wholly delegated to the ida.liu.se zone, which subsequently only delegates **sub**-domains if such exists.

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.

```
$ dig ida-gw.sysinst.ida.liu.se
[...]
;; ANSWER SECTION:
ida-gw.sysinst.ida.liu.se. 300 IN A 130.236.178.1
```

b) Which nameservers have authoritative information for sysinst.ida.liu.se.

```
$ dig ida-gw.sysinst.ida.liu.se SOA
[...]
;; QUESTION SECTION:
;ida-gw.sysinst.ida.liu.se. IN SOA

;; AUTHORITY SECTION:
sysinst.ida.liu.se. 300 IN SOA sysinst-gw.ida.liu.se. david.byers.liu.se. 2016110901 3600 18
```

c) Which name corresponds to the IPv4 address 130.236.189.1.

```
  $ dig -x 130.236.189.1
[...]
```

```
;; QUESTION SECTION:
;1.189.236.130.in-addr.arpa. IN PTR

;; ANSWER SECTION:
1.189.236.130.in-addr.arpa. 3564 IN PTR idagw-189.ida.liu.se.
```

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.

```
  $ dig www.ida.liu.se A +trace | grep Received
;; Received 525 bytes from 130.236.1.9#53(130.236.1.9) in 1 ms
;; Received 865 bytes from 192.203.230.10#53(e.root-servers.net) in 30 ms
;; Received 483 bytes from 130.239.5.114#53(g.ns.se) in 11 ms
;; Received 1188 bytes from 192.36.125.2#53(sunic.sunet.se) in 4 ms
;; Received 958 bytes from 130.236.146.68#53(ns2.liu.se) in 2 ms
```

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.

```
dig update.microsoft.com +trace | grep Received

;; Received 525 bytes from 130.236.1.9#53(130.236.1.9) in 58 ms
;; Received 872 bytes from 192.36.148.17#53(i.root-servers.net) in 5 ms
;; Received 790 bytes from 192.54.112.30#53(h.gtld-servers.net) in 21 ms
;; Received 61 bytes from 208.84.2.53#53(ns2.msft.net) in 61 ms

$ dig update.microsoft.com @ns2.msft.net +trace | grep Received
;; Received 40 bytes from 208.84.2.53#53(ns2.msft.net) in 22 ms
```