Networking Lab Day 8

Kevin Neumann, Alain C. Mendy

June 22, 2014, Goettingen

1 Part 2: Static mapping of names to IP addresses via the /etc/hosts file

1.1 What happens if the same name is assigned to different IP addresses in /etc/hosts?

The first entry is chosen per default, the second will never be reached.

2 Part 3: Configure a DNS server on a Linux PC, Configuring a DNS resolver, Running a DNS name server and Modifying the name server

2.1 Explain the role of each resource record in file db.mylab.com shown in Figure 8.2. Explain the line $TTL86400$.

mylab.com. IN SOA PC4.mylab.com. hostmaster.mylab.com. (1 ; serial 28800 ; refresh 7200 ; retry 604800 ; expire 86400 ; ttl);

Start of authority entry. Shows, that this nameserver is the best source of informatuion for this DNS-domain. Contains host, on which the file was generated, serial number (should be increased by one each time the file is changed so that secondary DNS servers get the changes), refresh time (time secondary DNS-servers waits before asking the SOA entry for changes), retry time (time a secondary server waits before retrying failed zone information exchange), expiration time (time a secondary server tries again to perform a zone convertion. If the time expires before a successful attempt, the secondary server will crush its zone file. This means that the secondary server will no longer answer to queries, because it assumes its data is too old), and time to live (The minimum value of valid ressource entries. It is included in all answers to queries and tells different servers for how long to keep information in their cache).

mylab.com. IN NS PC4.mylab.com.

Domain mylab.com in Internet namespace (IN) using namespace (NS) for PC4.

localhost A 127.0.0.1,PC4.mylab.com. A 10.0.1.41,PC3.mylab.com. A 10.0.1.31,PC2.mylab.com. A 10.0.1.21,PC1.mylab.com. A 10.0.1.11

Assigning different ipv4-addresses (A) to different hostnames in the domain.

2.2 Include the output on PC4 from commands host -v PC3.mylab.com and host -v 10.0.1.21 and provide an interpretation of the output.

;; QUESTION SECTION: ;PC3.mylab.com. IN A

Trying to find out information about requested hostname in ipv4.

;; ANSWER SECTION: PC3.mylab.com. 86400 IN A 10.0.1.31
Answer to query showing TTL and ip-address of PC3.
;; AUTHORITY SECTION: mylab.com. 86400 IN NS PC4.mylab.com.
Showing authority section. Includes domain and DNS server.
;; ADDITIONAL SECTION: PC4.mylab.com. 86400 IN A 10.0.1.41
Information about the nameserver.
;; QUESTION SECTION: ;PC3.mylab.com. IN AAAA
Trying to get information of PC3's ipv6 address.
;; AUTHORITY SECTION: mylab.com. 86400 IN SOA PC4.mylab.com. hostmaster.mylab.com. 1 28800 7200 604800 86400
Returns SOA, no information found.
;; QUESTION SECTION: ;PC3.mylab.com. IN MX
Trying to get information about PC3's mail exchanger record. None there.
;; QUESTION SECTION: ;21.1.0.10.in-addr.arpa. IN PTR
Trying to resolve hostname for ip address 10.0.1.21 by reverse search.
;; ANSWER SECTION: 21.1.0.10.in-addr.arpa. 86400 IN PTR PC2.mylab.com.
Entry found, points to PC2.
;; AUTHORITY SECTION: 1.0.10.in-addr.arpa. 86400 IN NS PC4.mylab.com.
Authority section containing information.
;; ADDITIONAL SECTION: PC4.mylab.com. 86400 IN A 10.0.1.41
Nameserver information.

3 Part 4: Observe traffic of DNS queries

3.1 Does the DNS server generate traffic when there are no DNS requests?

Nope, no traffic was observed.

3.2 Do all commands generate a DNS message?

No, for the unknown host/domain tcpip-lab.net there is no information available and thus no DNS traffic is generated.

3.3 Determine how domain names and IP addresses are encoded in DNS messages.

There is a Domain Name System (response) section, which itself contains sections queries, answers, authorities and additional information (similar to the host -v command). In these sections all available information about queried host and nameserver can be found.

3.4 What happens if a DNS query that cannot be resolved is issued?

A reply containing the message 'server failure' is returned to the issuer.

3.5 If you repeat one of the commands, does PC1 issue another request or does PC1 cache the previous response?

No, the request is sent out again.

3.6 DNS queries are either recursive or iterative. Use the data captured by Wireshark to determine if DNS queries are generated by issuing the ping commands.

The recursive flag is set, so recursive mode is activated.

3.7 Select a single DNS query or response, and explain all fields in the flags field.

Flags: 0x8182 (Standard query response, Server failure)
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
.... 0010 = Reply code: Server failure (2)

4 Part 5: Running a caching only DNS server

4.1 Which commands generate a DNS message?

The first and third ping command generate a DNS message.

4.2 Are any DNS queries issued when you repeat the query to resolve PC3.mylab.com?

No there are not. The previous result was cached.

4.3 Do you observeany difference with the queries captured in Part 4? Specifically, if you run ping -c 3 PC3.mylab.com on PC1(which runs a DNS resolver, but no caching-only DNS server) and PC2(which runs a caching-only DNS server) do you observe any difference in the outgoing DNS messages?

The difference is that from PC1, each time a DNS query is issued, whereas on PC2 the results are cached and no further queries are made until cache is alive or query fails.

5 Part 6: Resolution of DNS queries in a hierarchical system of DNS servers.

5.1 Compare the file /var/named/part6/db.cache on the PCs and describe the differences. What is the difference of the file db.cache to the file db.cache used earlier(shown in Figures 8.6 and 8.7)

The major difference is that there is more than one authority section. PC1 for example knows all different subservers and delegates queries to them. Formerly, there was only one root server being the authority for every query.

5.2 Compare the entry for zone . in file /etc/named.conf at PC1 (the root server) and the other PCs. Explain the differences.

The type differs. PC1 is the master server, the other ones are of type hint. This means that A DNS Caching Server (frrequently called a Resolver) obtains information from another server (a Zone Master) in response to a host query and then saves (caches) the data locally. On a second or subsequent request for the same data the Caching Server (Resolver) will respond with its locally stored data (the cache) until the time-to-live (TTL) value of the response expires, at which time the server will refresh the data from the zone master.

5.3 In the DNS hierarchy, the root server has resource records in the zone data file so that it can delegate DNS queries to the servers of the .com and the .net zone. Likewise, the server for .com has resource records that delegate DNS queries to the server for mylab.com. These resource records are called glue records. Identify the glue records at the DNS servers for zones ., .com, and .net. Are there any other glue records?

PC1: net. IN NS PC3.mylab.com.
PC3.mylab.com. IN A 10.0.1.31;
com. IN NS PC2.mylab.com.
PC2.mylab.com. IN A 10.0.1.21
PC2: mylab.com. IN NS PC4.mylab.com.
PC4.mylab.com. IN A 10.0.1.41
PC3: lab8.net. IN NS PC3.mylab.com.
PC3.mylab.com. IN A 10.0.1.31
PC4 has none.