Communication Systems Lab

Exercise 4

October 11, 2022

Group2: Songyi Han and Mohamed Zahir Mohamed Wazeer

1. First, disable your dhcp server. Also, make sure to flush your iptables and accept all inbound and outbound traffic. Now, reboot your machines.

`sudo systemctl disable isc-dhcp-server`
`sudo iptables -F INPUT`

2. Make sure both machines are connected to the Internet. Make sure you connect both machines to the wall to get an uplink for both machines. Additionally, configure a static point-to-point link between them.

connect to the internet (both PC) : `sudo dhclient enp4s0`
point-to-point link for PC1 : `sudo ip address add dev enp5s0 10.0.0.1/24`
point-to-point link for PC2 : `sudo ip address add dev enp5s0 10.0.0.2/24`
Test from PC2 : `ping 10.0.0.1`

4. On PC1, change files /etc/bind/named.conf.options such that your DNS server forwards all queries to the lab DNS server with IP: 192.168.3.1 (hint: use “forwarders”).
• Disable DNSSEC features by removing the line “dnssec-validation auto;”
• And adding the lines: “dnssec-enable no; dnssec-validation no;” Then, restart your DNS server by executing: sudo systemctl restart bind9;

5. Configure your PC2 with exactly the same as PC1, but add PC1 as forwarder. Test the configuration by executing a query with dig on PC2. If PC1 does not respond, the configuration is wrong.

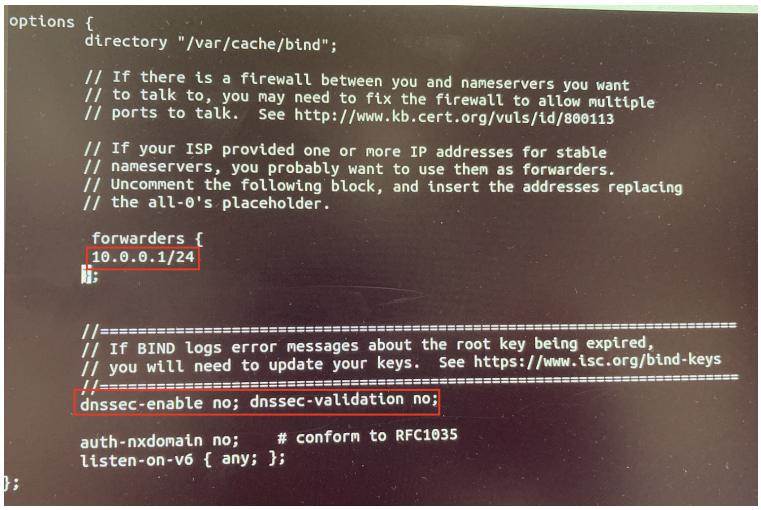

Fig1. /etc/bind/named.conf.options on PC2

```
pc-2-2@pc-2-2:~$ dig google.com

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32430
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             101     IN      A       172.217.168.14

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Oct 11 15:00:22 CEST 2022
;; MSG SIZE  rcvd: 55
```

Fig2. Test result by executing a query with dig on PC2

6. Run Wireshark on PC1 to inspect the DNS forwarding from the client (PC1) to the server (PC2) to view the packet trace of a new DNS query. What traffic can you observe? What happens when the same query is repeated?

- What traffic can you observe?

  Traffic forwarded from PC1 to PC2 and the corresponding DNS acknowledgement messages are shown on wireshark where bypassed executions via the lab network are not demonstrated on wireshark. When the query is repeated, it just adds up. But nothing happens especially than the accumulation. The cache is increased and the action would be reflected on wireshark unless a different domain name to the concurrent is executed.

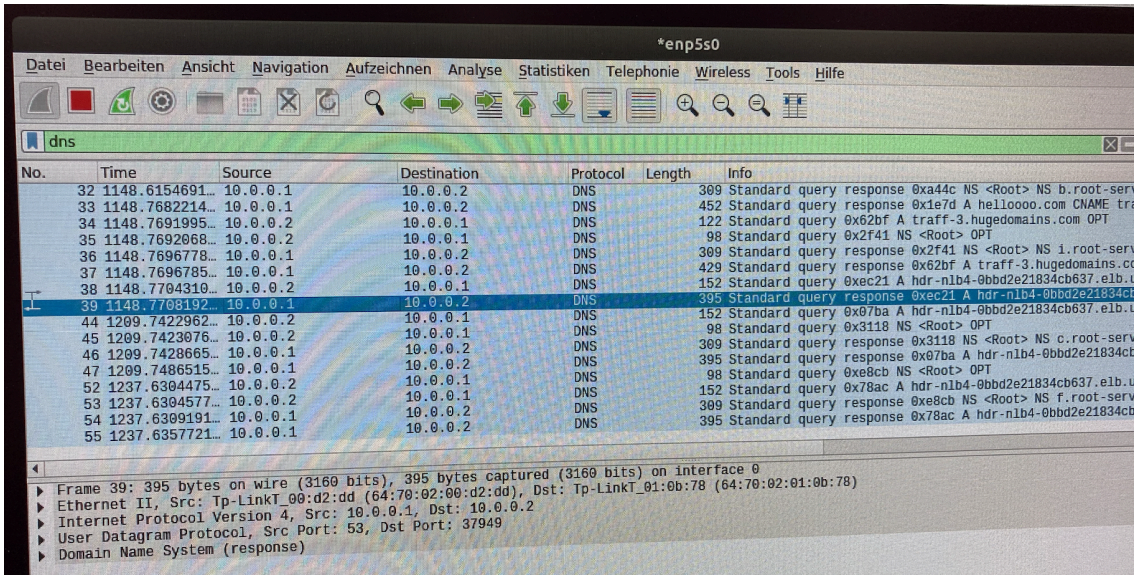

Fig3. Network traffic of PC1

- What happens when the same query is repeated?
  it is cashed and does not create new packet

7. Now, create a new file /etc/bind/db.groupXX.comsys.org. in server. Include the file in /etc/bind/named.conf.default-zones. Configure your own zone on your DNS server as master.

```
;
;
$TTL      604800
@ IN SOA group2.comsys.org. root.comsys.org. (
             2       ; Serial
        604800       ; Refresh
         86400       ; Retry
       2419200       ; Expire
        604800 )       ; Negative Cache TTL
;

@    IN NS ns.group2.comsys.org.
ns   IN A  10.0.0.1
pc21 IN A  10.0.0.1
pc22 IN A  10.0.0.2

mail IN CNAME pc21
www IN CNAME pc21
```

Fig4. database for pc1

```
;
;
$TTL      604800
@ IN SOA group2.comsys.org. root.comsys.org. (
              2 ;     Serial
         604800 ;     Refresh
          86400 ;     Retry
        2419200 ;     Expire
         604800 ) ;     Negative Cache TTL
;

@    IN NS ns.group2.comsys.org.
ns   IN A  10.0.0.2
pc21 IN A  10.0.0.1
pc22 IN A  10.0.0.2

mail IN CNAME pc22
www IN CNAME pc22
```

Fig5. database for pc1

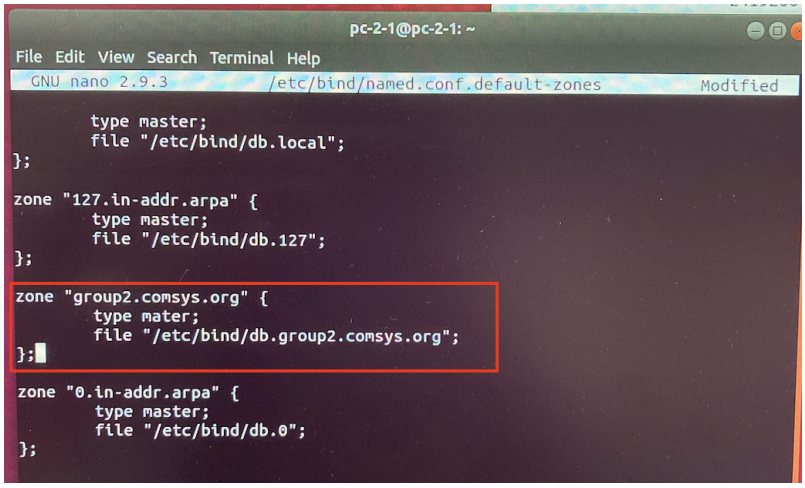

Fig6. configuration /etc/bind/named.conf.default-zones

9. Test your server by executing queries for your domain with dig from both PC1 and PC2.

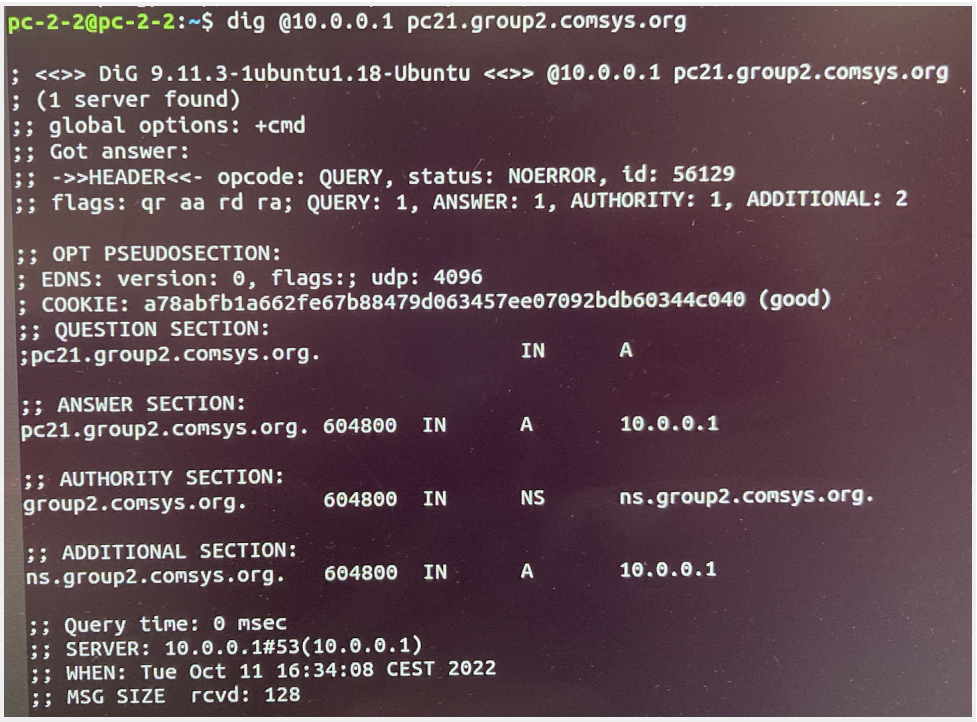

Fig7. Test dig from PC2

Questions

1. What purpose serves the DNS protocol?

=> DNS protocol translates human readable domain names to machine readable IP addresses hence it converts IP addresses.

2. What is a DNS TLD?

=> TLD or top level domain name refers to the last segment of a domain name or the part that immediately follows after the dot. As an example, .org, .com, etc. which is the highest level of hierarchical domain name system after the root domain.

3. What is a DNS Root Server?

=> DNS root servers are DNS name servers which operates in the root zone. These servers can directly answer queries for records stored or cached within the root zone, and they can also refer other requests to the appropriate Top Level Domain (TLD) server. A DNS look up starts at the root server.

4. Why do DNS entries need a TTL field?

=> DNS TTL serves to tell the recursive server or local resolver how long it should keep said record in its cache hence the server setting that tells a cache how long to store DNS records before refreshing the search to get an answer again from a name server hence determines the discarding time of the resolver.

5. Why is it advantageous for web servers to have a static IP address?

=> Prime benefit would be the provision to have a better DNS support hence provides better name resolution across internet and provides a high level of protection against threats. Similarly a static IP can provide reduced lapses during connection with a higher download and upload speed. Correspondingly, it's easier to locate shared devices. Remote accessibility is another advantage of having a static IP.

6. Which transport layer protocol is used by DNS, why?

=> DNS uses UDP or User Datagram Protocol on port 53 for DNS queries.
DNS requests are generally very small and fit well within UDP segments. UDP is much faster. TCP is slow as it requires a 3-way handshake. The load on DNS servers is also an important factor. DNS servers (since they use UDP) don't have to keep connections.

7. Name three different resource record types.

=> There are a large number of types and out of them the following are a few.

- A – Address Record
- AAAA – Ipv6 address record
- APL – Address Prefix List
- SIG – Signature

8. What do zone files consist of?

=> The zone file contains the IP name and data, MX records and other service records. It also contains glue data which connects them to the DNS servers. Hence it contains mapping between domains, IP addresses and other resources.