CSE 6032 Computer Networks
2021/22 Spring Term

Project: 2 – Part 1
Topic: DNS Service and Protocol
Date: 03.03.2022 – 12.03.2022

Objectives:

- to test DNS services with **nslookup** tool
- to analyze DNS services and protocol with **Wireshark**

References

- **IANA DNS Parameters** https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml
- **IANA Top Domains** List http://data.iana.org/TLD/tlds-alpha-by-domain.txt
- **Root Servers List** http://www.root-servers.org

Project Definition and Testbed De[loyment

The project aims at deploying the **DNS server** "**mydns**" to be the primary **Authoritative DNS server** for the private domain "**cen.net.**" you will create on the virtualization platform**.** Project is organized in two parts:

- ✓ **Part-1** focuses on how DNS services are organized globally on the Internet and how our workstation access these services, how users can explore/debug these services with the "nslookup" tool.
- ✓ **Part-2** is dedicated to the deployment of a local DNS service on a **VM** running **Windows Server2012 R2.**

Although you don't need the DNS server appliance in the first part, you are advised to download **"WS2012-Ref.ova"**

- ✓ either, from University **ftp server** using the procedures outlined in **Project-1 Part -1 Section A**;
- ✓ or, from the google repository accessible from following link:
  https://drive.google.com/file/d/1gUDWmmN4Dish5gTSmk3qBI3nOued5Z0x/view?usp=sharing

→ You may proceed with Part-1 of this project without waiting for the termination of download operation. But once the appliance is there, you are advised to import it in your VirtualBox platform under the name "MyDNS" using the procedures outlined in **Project-1 Part -1 Section D.3**

→ You may verify that the "MyDNS" is operational by starting it after connecting it's adapter to the Host-only Network. Since the "**ctrl-alt-del**" key combination is dedicated to the Host; **VirtualBox** defined the "**right ctrl + del**" key combination as the alternative setting. Log in as '**Administrator'** using the password "**Qwer1234**"; then power it off.

Section A. Exploring DNS Service with "nslookup" Tool

A.1 Invoking "nslookup"

'**nslookup**' is a versatile tool that helps to retrieve any type of **DNS Resource Record (RR)** from any server in the DNS server hierarchy: **root**, **TLD**, **SLD** (**Authoritative)**, or local.

Retrieved **DNS RRs** are used:

- ✓ to map FQDNs to corresponding IP@, and vice-et-versa;
- ✓ to obtain the list of Internet services (mail, dns etc.) available at a domain;
- ✓ to debug the configuration and operation of **DNS Servers**.

On Windows systems **nslookup** runs from the **command line interface** using the following syntax:

nslookup { -option }* { record-to-query } { name or IP@ of the dns-server to use }

Braces indicate that all of the command line parameters are optional; they are mainly used in stored scripts. Invoked without parameter, **nslookup** runs in interactive mode and processes the directives entered from command line console.

→ **Note that**, '**nslookup**' contacts directly a DNS server, bypassing **OS**'s **DNS client**, thus local DNS **cache** is not used!

A.2 Exploring "nslookup"

In this project you will use **nslookup** in interactive mode. The tool will direct your queries to the default **DNS server**. Identify **local DNS server** with "**ipconfig /all**"; then perform the following.

i) Run **nslookup** from the command line; it should print an output similar to the one on the right, displaying:
   - ✓ **server's FQDN** (if available); or the "**UnKnown**" label;
   - ✓ **server's IP @** (*should be the one you identified with ipconfig*).

```
Command Prompt - nslookup

C:\>nslookup
Default Server:  UnKnown
Address:  46.197.15.60

> ?
```

ii) Enter the "**?**" character to display the list of **nslookup** directives; out of which will mainly use:
   - ✓ "**set option**" - to control the behavior of the tool;
   - ✓ "**server NAME**" - to change the current DNS server resolving you queries; and "**exit**" to terminate.

iii) Query the FQDN "cnn.com." (note the dot at the end to completing FQDN); an output like on the right will be displayed and include:
   - + the name and the address of the server that resolved FQDN;
   - + the answer is qualified "**Non-authoritative**" as it has been resolved by your local server, from its cache;
   - + list of IPv.6@ associated with the FQDN;
   - + followed by the list of IPv.4@ defined for it.

```
> cnn.com.
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
Name:    cnn.com
Addresses:  2a04:4e42:200::323
          2a04:4e42:600::323
          2a04:4e42:400::323
          2a04:4e42::323
          151.101.129.67
          151.101.193.67
          151.101.1.67
          151.101.65.67
```

iv) Verify that **nslookup** has **displayed** the information defined by its current (default) settings; check it with "**set all**". Among listed options identify the following parameters.
   - ✓ The **query** "type" was set to "A+AAAA" (where A stands for the IPv.4@ and AAAA for the IPv.6@), thus **nslookup** issued two queries one to retrieve the IPv.6@ and the other IPv.4@
     You will observe this fact at next step by capturing **DNS** protocol traffic with **Wireshark**.
   - ✓ Query **time-out** is set to **2 seconds** - *acceptable for a local server but may need to be increased to contact remote DNS servers, especially when the Internet connection is slow-*.
   - ✓ **Retry** number is set to **1** -*acceptable for a local server but may be increased* for remote servers-.
   - ✓ Default **root** server is set to "**A.ROOT-SERVERS.NET.**" –*your queries will not use it for now-*

A.3 Capturing DNS Traffic & Matching it with nslookup Messages

On the Host perform the procedures outlined here after to capture **DNS** protocol traffic between your workstation and the local **DNS** server, and analyze them.

i) Start **Wireshark** and customize its **address resolution** options as defined in **section B.3** of the Project 1 Part 2.

ii) Run **nslookup**; and set it to debug mode using the "**set debug**" directive.

iii) Start capturing Home Network traffic.

iv) Resolve again the FQDN "**cnn.com.**"; locate the 2 replies returned:
   - ✓ one in response to the query of type A (note that the query is embedded in the reply); and
   - ✓ the other of type AAAA.

```
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 4,  authority records = 0,  additional = 0

    QUESTIONS:
        cnn.com, type = A, class = IN
    ANSWERS:
    ->  cnn.com
        internet address = 151.101.129.67
        ttl = 60 (1 min)
    ->  cnn.com
        internet address = 151.101.65.67
        ttl = 60 (1 min)
    ->  cnn.com
        internet address = 151.101.1.67
        ttl = 60 (1 min)
    ->  cnn.com
        internet address = 151.101.193.67
        ttl = 60 (1 min)
```

```
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 4,  authority records = 0,  additional = 0

    QUESTIONS:
        cnn.com, type = AAAA, class = IN
    ANSWERS:
    ->  cnn.com
        AAAA IPv6 address = 2a04:4e42::323
        ttl = 300 (5 mins)
    ->  cnn.com
        AAAA IPv6 address = 2a04:4e42:400::323
        ttl = 300 (5 mins)
    ->  cnn.com
        AAAA IPv6 address = 2a04:4e42:200::323
        ttl = 300 (5 mins)
    ->  cnn.com
        AAAA IPv6 address = 2a04:4e42:600::323
        ttl = 300 (5 mins)
```

v) Exit debugging mode with "**set nodebug**" directive; then enter the "**set type=A**" to query just **IPv.4@** set.

vi) Query the FQDN "**cnn.com.**" again; now the list should contain only the IPv.4@ of the domain.

vii) Repeat the query **2 more times** and note that returned IPv.4@ list rotates each time; network applications use the IPv.4@ provided on top of the list, access the rest if the first one does not reply .

viii) Stop **Wireshark** capturing; save it as the "a3.pcapng" file *-you will use it to write the project report-*.

ix) Filter displayed **L2** frames with "**dns && (ip.addr==x.y.z.t)**" to keep just the **DNS** traffic generated by your queries.

x) Identify and mark all **DNS** frames corresponding to the queries in (iv), (vi) and (vii).
L2 frame list should be similar to the screen shut here after except the **IPv4 addresses**. Match them versus displayed **nslookup** messages.

dns && (ip.addr==192.168.0.14)

No.	Source	Destination	Protocol	Length	Info
17	192.168.0.14	46.197.15.60	DNS	67	Standard query 0x0002 A cnn.com
18	46.197.15.60	192.168.0.14	DNS	131	Standard query response 0x0002 A cnn.com A 151.101.129.67 A 151.101.65.67 A 151.101.1.67 A 151.101.193.67
19	192.168.0.14	46.197.15.60	DNS	67	Standard query 0x0003 AAAA cnn.com
20	46.197.15.60	192.168.0.14	DNS	179	Standard query response 0x0003 AAAA cnn.com AAAA 2a04:4e42::323 AAAA 2a04:4e42:400::323 AAAA 2a04:4e42:200:
70	192.168.0.14	46.197.15.60	DNS	67	Standard query 0x0004 A cnn.com
71	46.197.15.60	192.168.0.14	DNS	131	Standard query response 0x0004 A cnn.com A 151.101.129.67 A 151.101.1.67 A 151.101.193.67 A 151.101.65.67
72	192.168.0.14	46.197.15.60	DNS	67	Standard query 0x0005 A cnn.com
73	46.197.15.60	192.168.0.14	DNS	131	Standard query response 0x0005 A cnn.com A 151.101.1.67 A 151.101.193.67 A 151.101.65.67 A 151.101.129.67
76	192.168.0.14	46.197.15.60	DNS	67	Standard query 0x0006 A cnn.com
77	46.197.15.60	192.168.0.14	DNS	131	Standard query response 0x0006 A cnn.com A 151.101.193.67 A 151.101.65.67 A 151.101.129.67 A 151.101.1.67

xi) Prepare **Packet Summary Report** of selected frames as defined in **section B.4/iii** of the Project 1 Part 2, and save it as the "a3.txt" file.

xii) Verify that the contents of "a3.txt" comply with the format defined in **section B.4/iv**.

A.4 Resolving Domain Name using an Authoritative DNS Server

To resolve queries for the FQDN "iku.edu.tr." using an **authoritative** server, we need to set the **default DNS resolver** to the one registered for this domain.
Mind that organizations do not allow outsiders to use **all** of their DNS servers obviously for performance, security, and privacy concerns. Yet the authoritative servers have to be publicly accessible.

To identify "iku.edu.tr." domain's **authoritative** server and to set it as **nslookup** resolver perform the following steps.

i) Set the query type with "**set type=ns**" to retrieve **DNS** RRs (left screen shut here after).

ii) Query "iku.edu.tr." domain; the answer should display at least 2 **DNS** FQDNs *-they are likely defined under the SOA header of the domain; refer to lecture notes and to **Section A.6** -*.

iii) Change your resolver to one of them e.g. "**ns02**" with the "**server ns02.iku.edu.tr**" directive.
Note that **nslokup** displays the FQDN and IPv4@ of the new DNS resolver.

iv) Test the operations of the selected **DNS server** by querying the IPv.4@ of domain entities (right screen shut).
- ✓ Set query type using the "**set type=A**" directive.
- ✓ Query "www.iku.edu.tr." to acquire the IPv.4@ of University's web server.
- ✓ Query "ns01.iku.edu.tr." to acquire the IPv.4@ of University's other authoritative DNS server.

```
> set type=ns
> iku.edu.tr
Server:  UnKnown
Address:  46.197.15.60

Non-authoritative answer:
iku.edu.tr      nameserver = ns02.iku.edu.tr
iku.edu.tr      nameserver = ns01.iku.edu.tr
> server ns02.iku.edu.tr
Default Server:  ns02.iku.edu.tr
Address:  154.52.100.17
```

```
> set type=A
> www.iku.edu.tr
Server:  ns02.iku.edu.tr
Address:  154.52.100.17

Name:    www.iku.edu.tr
Address:  154.52.100.15

> ns01.iku.edu.tr
Server:  ns02.iku.edu.tr
Address:  154.52.100.17

Name:    ns01.iku.edu.tr
Address:  194.27.151.1
```

v) Query University's mail service information (screen shut here after).

- ✓ **Set** query type using the "**set type=MX**" directive.
- ✓ Query "iku.edu.tr." domain to acquire mailer's IPv.4@ , FQDN, and associated information.

```
> set type=MX
> iku.edu.tr
Server:  ns02.iku.edu.tr
Address:  154.52.100.17

iku.edu.tr      MX preference = 4, mail exchanger = mail.iku.edu.tr
mail.iku.edu.tr internet address = 154.52.100.16
```

A.5 Querying the Reverse Domain

To retrieve the FQDN associated with a given **IPv4.@** we have to query the **Reverse Domain** "**in-addr**" located under the **TLD "arpa."**.

Perform the following to query the name associated with **IKU**'s **DNS server** "**194.27.151.1**".

- ✓ Set **query type** to reverse address resolution using the "**set type=ptr**" directive.
- ✓ Query the **Reverse Domain IP @** of the **DNS** server expressed in **reversed dotted decimal order** and terminated with the suffix "in-addr.arpa." as shown here after.

```
> set type=ptr
> 1.151.27.194.in-addr.arpa.
Server:  ns02.iku.edu.tr
Address:  154.52.100.17

1.151.27.194.in-addr.arpa       name = ns01.iku.edu.tr
```

→ **Note that**, not all the **IPv4@** definitions with A type RRs (referred as the **"DNS Forward Zone"** records) have their corresponding **Reverse Domain** definition. As such reverse domain queries may often fail for most of the systems and services. Only **essential entities** such as name servers have both!

A.6 Querying all the RRs of a Domain

Perform the following steps to retrieve all of the **RR**s for a given **domain of control** (authority zone in DNS terminology).

- ✓ Set the query type with "**set type=any**".
- ✓ Define one of IKU's DNS servers to be your resolver e.g. using the "**server ns02.iku.edu.tr**" directive.
- ✓ Query the domain name "iku.edu.tr."

```
> set type=any
> iku.edu.tr
Server:  ns02.iku.edu.tr
Address:  154.52.100.17

iku.edu.tr      internet address = 154.52.100.15
iku.edu.tr      nameserver = ns02.iku.edu.tr
iku.edu.tr      nameserver = ns01.iku.edu.tr
iku.edu.tr
        primary name server = ns01.iku.edu.tr
        responsible mail addr = hostmaster.iku.edu.tr
        serial  = 2017022400
        refresh = 3600 (1 hour)
        retry   = 600 (10 mins)
        expire  = 1814400 (21 days)
        default TTL = 3600 (1 hour)
```

→ **Note that**, the query also retrieved the Zone Definition SOA (**Start of Authority**) record. It shows:

- ✓ the FQDN of the **primary authoritative** DNS server of the domain;
- ✓ email of the person in charge;
- ✓ TTL and expire time that are associated with the RRs returned for each query.

Refer to lecture notes and **IANA DNS Parameters** reference to inspect the information they provide.

Section B. Exploring DNS Client - Local DNS Server Cooperation

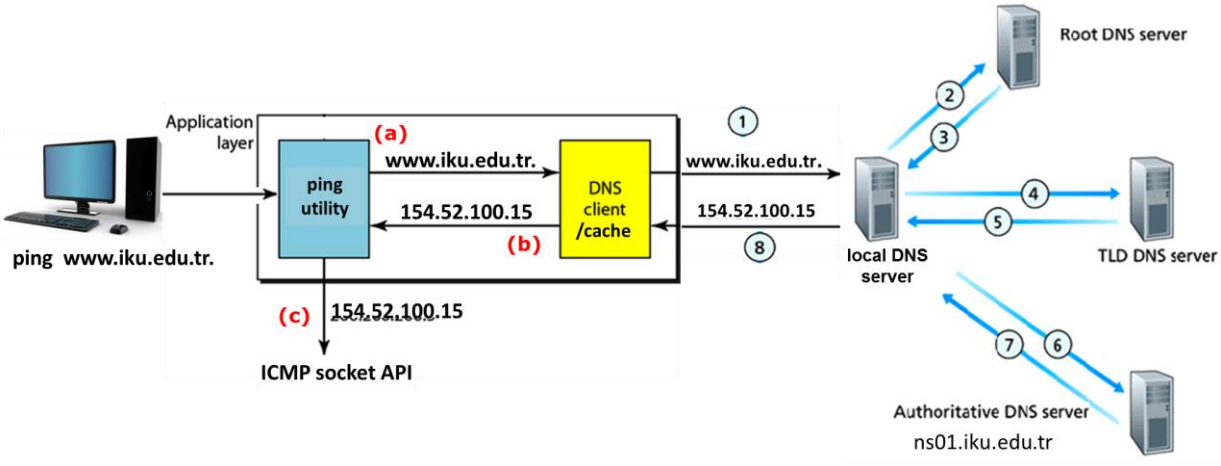
Almost all network applications e.g. *browsers, mail and ftp agents, A/V application* resolve the FQDN of systems they communicate with using a local **DNS server** defined by the institution or the ISP. However, these network applications use the **OS** service **DNS Client/Cache** to access the local **DNS server**.

The figure here after depicts the communication flow when a client entered the "**ping www.iku.edu.tr.**" command.

a) "ping" utility asks the **OS** service **DNS Client/Cache to** resolve the FQDN "www.iku.edu.tr.";

b) **DNS Client/Cache** returns the IPv4@ "**154.52.100.15**" for the FQDN.

c) "ping" utility passes then its "echo **154.52.100.15**" request to an ICMP socket API/



The **DNS Client/Cache** and the local **DNS server** maintain both their cache to **reduce query response times** and the amount of **network traffic**.

> If application's query matches a **cached** RR, the **answer** is returned without querying the "Authoritative Server" of the domain. The reply is tagged as "**Non-authoritative answer**".

> If not, local DNS server queries iteratively the **DNS** servers' hierarchy (steps 1-5); then the authoritative server "iku.edu.tr." domain which resolves the query and replies with the IPv4@ (steps 6-7).
>
> The local DNS server and the OS **DNS Client/Cache** service update their respective cache).

B.1 Observing DNS Client Cache and Local DNS Server Traffic

On your Host perform the following procedures to observing **DNS Client cache** contents and the L2 frame traffic generated with the **local DNS Server**.

i) Display the **DNS-client** cache using the "**ipconfig /displaydns**" command.
The output should contain not only FQDNs of the sites you have accessed earlier but also a plea of references accessed by the applications running on your system.

ii) Clear **DNS-client cache** with the "**ipconfig /flushdns**" command; and display its contents again; the list should be very short; try to identify them.

iii) Start **Wireshark;** reset its "**Address Resolution**" options as defined earlier.

iv) Start capturing Home Network traffic;

v) Ping only 2 times "www.iku.edu.tr."

vi) Display **DNS-client** cache and identify the "www.iku.edu.tr." RR; if it is not there restart at step (i).

vii) Ping only 2 times "www.iku.edu.tr." again.

viii) Stop **Wireshark** capture; and save the frames in the "b1.pcapng" file.

ix) Search captured frames and verify that your second "ping" command **did not generate** additional DNS query and reply messages to resolve "**www.iku.edu.tr.**"; if not restart at step (i).

B.2 Analyzing Network Traffic

i) Analyze the network traffic you have captured in section **B.1** identify and filter the frames/messages listed here after.
   - ✓ DNS **query** and **reply** frames that resolved the FQDN "www.iku.edu.tr.".
   - ✓ Ping related frames (ICMP).

ii) Prepare the **'packet summary report'** and save it as the "b1.txt" file (verify its format!).

Section C. Project Report

Use the information you gathered in sections **A** and **B** to prepare the project report "**Prj2-Part1- Report.docx**" stored at CATS course portal under the Resources/Project Appendices folder.

Compress the files listed here after using the **Compress Project Reports** stored under **Resources/How to?** folder.

- ✓ Prj2-Part1- Report.docx
- ✓ a3.pcapng and a3.txt
- ✓ b1.pcapng and b1.txt

Store compressed report in the **Prj2-Part1** folder located under **Assignments** heading at the course portal CATS **CSE6032-SectionX**; where "X" stands for (1.2.3.4), the laboratory session group you are registered in.

Collaboration Rules: What is Allowed What is NOT

Collaboration is a great way to learn. Students are encouraged to **discuss** project concepts and confer on **implementation** procedures with their peers. The key is to **use collaboration** as a way **to enhance learning**, **not** as a way of sharing answers without understanding

To avoid **plagiarism** all prose and code that you write for projects must be your own original work. Any other source you use must clearly identify and accurately cited.

Submitted work should be exclusively yours; **copying** or **getting help** from a third party is prohibited. Your submissions should be kept **confidential**, **sharing** them is **cheating**. No distinction will be made between those who cheat and who facilitate cheating by revealing their submissions.