

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

**Інститут прикладного системного аналізу
Кафедра математичних методів системного аналізу**

Дисципліна: “Комп’ютерні мережі”

Лабораторна робота № 3

Тема роботи: “ Протокол DNS”

Виконала: студентка
3 курсу групи КА-77
Деменкова В.В.

Прийняв: к.т.н. Кухарев С.О.

Київ – 2020

Лабораторна робота № 3. Протокол DNS

Мета роботи: Аналіз деталей роботи протоколу DNS.

Отримані результати:

```
No.      Time      Source      Destination      Protocol Length Info
 101 6.476531 192.168.1.109 8.8.8.8          DNS           72      Standard query 0x0454 A www.ietf.org
Frame 101: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{A1BA2240-64F3-4F12-995F-D42D06B55803}, id 0
Ethernet II, Src: HonHaiPr_b9:36:4d (a4:17:31:b9:36:4d), Dst: Tp-LinkT_de:11:f8 (b0:48:7a:de:11:f8)
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 57904, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x0454
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
  [Response In: 106]
```

```
No.      Time      Source      Destination      Protocol Length Info
 106 6.506624 8.8.8.8      192.168.1.109    DNS           149     Standard query response 0x0454 A www
www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
Frame 106: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{A1BA2240-64F3-4F12-995F-D42D06B55803}, id 0
Ethernet II, Src: Tp-LinkT_de:11:f8 (b0:48:7a:de:11:f8), Dst: HonHaiPr_b9:36:4d (a4:17:31:b9:36:4d)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.109
User Datagram Protocol, Src Port: 53, Dst Port: 57904
Domain Name System (response)
  Transaction ID: 0x0454
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
  [Request In: 101]
  [Time: 0.030093000 seconds]
```

Контрольні питання:

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP?

UDP

```
User Datagram Protocol, Src Port: 55508, Dst Port: 53
  Source Port: 55508
  Destination Port: 53
  Length: 55
  Checksum: 0xf77a [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  > [Timestamps]
```

Який номер цільового порта запиту DNS?

Який номер вихідного порта відповіді DNS?

```
User Datagram Protocol, Src Port: 57904, Dst Port: 53
  Source Port: 57904
  Destination Port: 53
```

2. На який адрес IP був відправлений запит DNS? 8.8.8.8

Чи є цей адрес адресом локального сервера DNS?

Ні, це зовнішня адреса. Локальні адреси починаються з

- 10.0.0.0 — 10.255.255.255 (маска підсети для бесклассовой (CIDR) адресации: 255.0.0.0 или /8)
- 100.64.0.0 — 100.127.255.255 (маска підсети 255.192.0.0 или /10) - Данная подсеть рекомендована согласно RFC 6598 для использования в качестве адресов для CGN (Carrier-Grade NAT).
- 172.16.0.0 — 172.31.255.255 (маска підсети: 255.240.0.0 или /12)
- 192.168.0.0 — 192.168.255.255 (маска підсети: 255.255.0.0 или /16)

3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? А

```
▼ Queries
  > www.google.com: type A, class IN
▼ Answers
  > www.google.com: type A, class IN, addr 216.58.215.100
```

Чи вміщує цей запит деякі можливі компоненти «відповіді»?

```
▼ Queries
  > www.google.com: type A, class IN
  [Response In: 68]
```

4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? 3

Що вміщує кожна з цих відповідей?

▼ Answers

```
> www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
[Request In: 101]
[Time: 0.030093000 seconds]
```

5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS? Так, співпадає.

101	6.476531	192.168.1.109	8.8.8.8	DNS	72 Standard query 0x0454 A www.ietf.org
102	6.488507	34.247.224.162	192.168.1.109	TLSv1.2	387 Application Data
103	6.495177	192.168.1.109	34.247.224.162	TCP	1514 50933 → 443 [ACK] Seq=1 Ack=334 Win=511 Len=1460 [T
104	6.495179	192.168.1.109	34.247.224.162	TLSv1.2	282 Application Data
105	6.496591	216.58.215.100	192.168.1.109	TCP	54 443 → 50941 [ACK] Seq=1719 Ack=1975 Win=64256 Len=0
106	6.506624	8.8.8.8	192.168.1.109	DNS	149 Standard query response 0x0454 A www.ietf.org CNAME
107	6.508324	192.168.1.109	104.20.1.85	TCP	66 50943 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=

6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер? Так

DNS	72 Standard query 0x0454 A www.ietf.org
DNS	149 Standard query response 0x0454 A www.ietf.org CNAME www.ietf.org.c
DNS	76 Standard query 0x7d7a A drive.google.com
DNS	92 Standard query response 0x7d7a A drive.google.com A 216.58.215.110
DNS	78 Standard query 0x816c A analytics.ietf.org
DNS	108 Standard query response 0x816c A analytics.ietf.org CNAME ietf.org
DNS	75 Standard query 0x2d90 A play.google.com
DNS	91 Standard query response 0x2d90 A play.google.com A 172.217.16.14
DNS	70 Standard query 0x1b5f A analytics.google.com

7. Яким був цільовий порт повідомлення із запитом DNS?

Яким був вихідний порт повідомлення із відповіддю DNS?

```
User Datagram Protocol, Src Port: 57220, Dst Port: 53
Source Port: 57220
Destination Port: 53
```

8. На яку IP-адресу був направлений запит DNS?

351	19.487775	192.168.1.109	8.8.8.8	DNS	71 S
-----	-----------	---------------	---------	-----	------

8.8.8.8

Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Так

Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	8 . 8 . 4 . 4

```
C:\Users\Doris>nslookup www.mit.edu
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d8:490::255e
           2a02:26f0:d8:4a5::255e
           92.123.7.194
Aliases:  www.mit.edu
           www.mit.edu.edgekey.net
```

8.8.8.8 (публічний DNS-сервер Google)

9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? А

351	19.487775	192.168.1.109	8.8.8.8	DNS	71 Standard qu
354	19.519701	192.168.1.109	8.8.4.4	DNS	71 Standard qu
355	19.522153	8.8.8.8	192.168.1.109	DNS	160 Standard qu
360	19.586998	8.8.4.4	192.168.1.109	DNS	160 Standard qu
447	19.944224	192.168.1.109	8.8.8.8	DNS	76 Standard qu
448	19.944320	192.168.1.109	8.8.8.8	DNS	72 Standard qu

Domain Name System (query)

Transaction ID: 0x3ba0

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> www.mit.edu: type A, class IN

[\[Response In: 355\]](#)

Тип	Расшифровка названия (англ.)	Код	Описание
A	Address	1	Адресная запись, соответствие между именем и IP-адресом

Чи вміщує цей запит деякі можливі компоненти «відповіді»?

[Response In: 355]

10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером?

З чого складається кожна із цих відповідей?

355	19.522153	8.8.8.8	192.168.1.109	DNS	160 Standard qu
360	19.586998	8.8.4.4	192.168.1.109	DNS	160 Standard qu
447	19.944224	192.168.1.109	8.8.8.8	DNS	76 Standard qu
448	19.944320	192.168.1.109	8.8.8.8	DNS	72 Standard qu

Authority RRs: 0
Additional RRs: 0

Queries

- > www.mit.edu: type A, class IN

Answers

- > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
- > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
- > e9566.dscb.akamaiedge.net: type A, class IN, addr 104.125.25.61

[\[Request In: 351\]](#)
[Time: 0.034378000 seconds]

11. На яку IP-адресу був направлений запит DNS?

177	20.235323	192.168.1.109	8.8.8.8	DNS	71 St
178	20.266693	192.168.1.109	8.8.4.4	DNS	71 St
180	20.286480	8.8.8.8	192.168.1.109	DNS	160 St

Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Так, за замовчуванням 8.8.8.8

```

C:\Users\Doris>nslookup www.mit.edu
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d8:490::255e
           2a02:26f0:d8:4a5::255e
           92.123.7.194
Aliases:  www.mit.edu
           www.mit.edu.edgekey.net

```

12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? А Чи вміщує цей запит деякі можливі компоненти «відповіді»?

178	20.266693	192.168.1.109	8.8.4.4	DNS	71 Standard qu
180	20.286480	8.8.8.8	192.168.1.109	DNS	160 Standard qu
182	20.299667	8.8.4.4	192.168.1.109	DNS	160 Standard qu
197	20.396432	192.168.1.109	8.8.8.8	DNS	84 Standard qu
198	20.428580	192.168.1.109	8.8.4.4	DNS	84 Standard qu

< >

Domain Name System (query)

Transaction ID: 0x15d8

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

> www.mit.edu: type A, class IN

[Response In: 182]

13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером?

180	20.286480	8.8.8.8	192.168.1.109	DNS	160 Standard qu
182	20.299667	8.8.4.4	192.168.1.109	DNS	160 Standard qu
197	20.396432	192.168.1.109	8.8.8.8	DNS	84 Standard qu
198	20.428580	192.168.1.109	8.8.4.4	DNS	84 Standard qu

< >

Authority RRs: 0

Additional RRs: 0

Queries

> www.mit.edu: type A, class IN

Answers

> www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

> www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

> e9566.dscb.akamaiedge.net: type A, class IN, addr 92.123.7.194

[Request In: 177]

[Time: 0.051157000 seconds]

Які сервери DNS були запропоновані у відповіді?

```
C:\Users\Doris>nslookup -type=NS mit.edu
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-173.akam.net
```

Які сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого? Лише за допомогою доменного імені.

```
C:\Users\Doris>nslookup -type=NS mit.edu
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-173.akam.net
```

14. На яку IP-адресу був направлений запит DNS? 8.8.8.8

Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Якщо ні, то якому доменному імені відповідає ця IP-адреса?


```

C:\Users\Doris>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

```

15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

142	9.939308	192.168.1.109	8.8.8.8	DNS	73 Standard qu
143	9.955204	8.8.8.8	192.168.1.109	DNS	89 Standard qu

>

Frame 142: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF{...}

>

Ethernet II, Src: HonHaiPr_b9:36:4d (a4:17:31:b9:36:4d), Dst: Tp-LinkT_de:11:f8 (b0:48:00:11:f8:00)

>

Internet Protocol Version 4, Src: 192.168.1.109, Dst: 8.8.8.8

>

User Datagram Protocol, Src Port: 56990, Dst Port: 53

▼

Domain Name System (query)

>

Transaction ID: 0x4a64

>

Flags: 0x0100 Standard query

>

Questions: 1

>

Answer RRs: 0

>

Authority RRs: 0

>

Additional RRs: 0

▼

Queries

>

bitsy.mit.edu: type A, class IN

>

[\[Response In: 143\]](#)

16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?

142	9.939308	192.168.1.109	8.8.8.8	DNS	73 Standard qu
143	9.955204	8.8.8.8	192.168.1.109	DNS	89 Standard qu

<

>

> Frame 143: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device

> Ethernet II, Src: Tp-LinkT_de:11:f8 (b0:48:7a:de:11:f8), Dst: HonHaiPr_b9:36:4d (a4:17::

> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.109

> User Datagram Protocol, Src Port: 53, Dst Port: 56990

> Domain Name System (response)

Transaction ID: 0x4a64

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

> Queries

bitsy.mit.edu: type A, class IN

> Answers

bitsy.mit.edu: type A, class IN, addr 18.0.72.3

[\[Request In: 142\]](#)

[Time: 0.015896000 seconds]

Висновок: В данній лабораторій роботі було проаналізовано деталі роботи з протоколом DNS. Розглянуто повідомлення із запитом та відповіддю DNS, досліджено деталі повідомлення. Проаналізовано повідомлення TCP SYN, перевірено співпадіння цільової IP адреси повідомлень з відповідями сервера DNS та перераховано кількість записів із відповідями, які були перераховані сервером.