



Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут ім. І. Сікорського»
Інститут Прикладного Системного Аналізу

Лабораторна робота №3
з дисципліни Комп'ютерні мережі

Виконала
студентка групи КА-77
Кулина Анісія

Прийняв Кухарєв С.О.

Київ 2020

Тема. Протокол DNS

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід роботи:

```
Командная строка
Microsoft Windows [Version 10.0.18362.836]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\Users\Админ>ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.

C:\Users\Админ>
```

```
Командная строка
Microsoft Windows [Version 10.0.18362.836]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\Users\Админ>nslookup www.mit.edu
Server: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
Server: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d200:19e::255e
           2a02:26f0:d200:191::255e
           23.7.200.176
Aliases:   www.mit.edu
           www.mit.edu.edgekey.net

C:\Users\Админ>
```

```
C:\Users\Админ>nslookup -type=NS mit.edu
Server: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net

eur5.akam.net internet address = 23.74.25.64
use2.akam.net internet address = 96.7.49.64
use5.akam.net internet address = 2.16.40.64
use5.akam.net AAAA IPv6 address = 2600:1403:a::40
usw2.akam.net internet address = 184.26.161.64
asia1.akam.net internet address = 95.100.175.64
asia2.akam.net internet address = 95.101.36.64
ns1-37.akam.net internet address = 193.108.91.37
ns1-173.akam.net internet address = 193.108.91.173
ns1-173.akam.net AAAA IPv6 address = 2600:1401:2::ad
```

```

Microsoft Windows [Version 10.0.18362.836]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\Users\Админ>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
*~x~x~x~: 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.
*** Превышено время ожидания запроса UnKnown

```

Контрольні запитання:

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

І запит і відповідь використовують протокол UDP.

Protocol: UDP (17)

Номер цільового порта (destination) запиту DNS: 53

✓ User Datagram Protocol, Src Port: 1025, Dst Port: 53
Source Port: 1025
Destination Port: 53

Номер вихідного порта (source) відповіді DNS: 53

Source Port: 53
Destination Port: 1025

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?

Запит був направлений на наступну IP-адресу: 192.168.0.1. Так, ця адреса співпадає з адресою локального сервера DNS.

Source: 192.168.0.107
Destination: 192.168.0.1

3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Запит містить запис типу A. Із можливих компонентів відповіді запит містить ім'я класу.

```

Queries
  www.ietf.org: type A, class IN
    Name: www.ietf.org
    [Name Length: 12]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
[Response In: 8]

```

4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

Було запропоновано сервером 3 записи із відповідями. Кожна із цих відповідей складається із наступних пунктів: ім'я, тип, клас, час життя, довжина даних, канонічне ім'я або адреса.

```

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 104.20.0.85
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1638 (27 minutes, 18 seconds)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 138 (2 minutes, 18 seconds)
    Data length: 4
    Address: 104.20.0.85
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 138 (2 minutes, 18 seconds)
    Data length: 4
    Address: 104.20.1.85

```

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?

7 2.387810	192.168.0.107	192.168.0.1	DNS	72 Standard query 0x1a28 A www.ietf.org
8 2.390351	192.168.0.1	192.168.0.107	DNS	459 Standard query response 0x1a28 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85 NS ns2.cloudflare.net
9 2.391705	192.168.0.107	104.20.0.85	TCP	74 [6481 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=433757430 TSecr=0
10 2.392197	192.168.0.107	104.20.0.85	TCP	74 [6482 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=433757430 TSecr=0
11 2.407620	104.20.0.85	192.168.0.107	TCP	66 443 → 16481 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
12 2.407621	104.20.0.85	192.168.0.107	TCP	66 443 → 16482 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024

Ні. Не співпадає.

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

Так, виконує.

No.	Time	Source	Destination	Protocol	Length	Info
7	2.387010	192.168.0.107	192.168.0.1	DNS	72	Standard query 0x1a28 A www.ietf.org
8	2.390351	192.168.0.1	192.168.0.107	DNS	459	Standard query response 0x1a28 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85 NS ns2.cloudflare.net
894	2.804259	192.168.0.107	192.168.0.1	DNS	78	Standard query 0xdcca A analytics.ietf.org
908	2.807594	192.168.0.1	192.168.0.107	DNS	389	Standard query response 0xdcca A analytics.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.hkg1.afilias-nst.info NS ns0.ams1.com NS ns1

7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

цільовий порт повідомлення із запитом DNS: 53

✓ User Datagram Protocol, Src Port: 6053, Dst Port: 53
Source Port: 6053
Destination Port: 53

вихідний порт повідомлення із відповіддю DNS: 53

✓ User Datagram Protocol, Src Port: 53, Dst Port: 6053
Source Port: 53
Destination Port: 6053

8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Запит був направлений на наступну IP-адресу: 192.168.0.1. Так, ця адреса є адресою локального сервера DNS.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.560392	192.168.0.107	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu

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

Запит містить запис типу A. Із можливих компонентів відповіді запит містить ім'я класу.

✓ Queries
 ✓ www.mit.edu: type A, class IN
 Name: www.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 5]

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

Було запропоновано сервером 4 записи із відповідями. Кожна із цих відповідей складається із наступних пунктів: ім'я, тип, клас, час життя, довжина даних, канонічне ім'я або адресу.

```

  Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1308 (21 minutes, 48 seconds)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:19e::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 16
    AAAA Address: 2a02:26f0:d200:19e::255e
  e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:191::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 16
    AAAA Address: 2a02:26f0:d200:191::255e
  Authoritative name servers

```

11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Запит був направлений на наступну IP-адресу: 192.168.0.1. Так, ця адреса співпадає з адресою локального сервера DNS.

9	6.621839	192.168.0.107	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
---	----------	---------------	-------------	-----	----	----------------------------------

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

Запит містить запис типу IN. Із можливих компонентів відповіді запит містить ім'я класу.

```

  Queries
  mit.edu: type NS, class IN
    Name: mit.edu
    [Name Length: 7]
    [Label Count: 2]
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    [Response In: 10]

```

13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді?

Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

Було запропоновано сервером 8 записів із відповідями.

У відповіді були запропоновані сервери з наступними іменами: use5.akam.net, ns1-173.akam.net, use2.akam.net, asia1.akam.net, eur5.akam.net, ns1-37.akam.net, usw2.akam.net, asia2.akam.net.

Сервери були запропоновані за допомогою доменного імені.

```

▼ Answers
  ▼ mit.edu: type NS, class IN, ns use5.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 15
    Name Server: use5.akam.net
  ▼ mit.edu: type NS, class IN, ns ns1-173.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 10
    Name Server: ns1-173.akam.net
  ▼ mit.edu: type NS, class IN, ns use2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 7
    Name Server: use2.akam.net
  ▼ mit.edu: type NS, class IN, ns asia1.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 8
    Name Server: asia1.akam.net

  ▼ mit.edu: type NS, class IN, ns eur5.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 7
    Name Server: eur5.akam.net
  ▼ mit.edu: type NS, class IN, ns ns1-37.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 9
    Name Server: ns1-37.akam.net
  ▼ mit.edu: type NS, class IN, ns usw2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 7
    Name Server: usw2.akam.net
  ▼ mit.edu: type NS, class IN, ns asia2.akam.net
    Name: mit.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 8
    Name Server: asia2.akam.net
```

14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

Запит був направлений на наступну IP-адресу: 18.0.72.3

Ні, ця адреса не є адресою локального сервера DNS за замовчанням. Це IP-адреса доменного імені bitsy.mit.edu

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

Запити містять записи типу A, AAAA та PTR. Із можливих компонентів відповіді запит містить ім'я класу IN.

```

  ▾ Queries
    ▾ 3.72.0.18.in-addr.arpa: type PTR, class IN
      Name: 3.72.0.18.in-addr.arpa
      [Name Length: 22]
      [Label Count: 6]
      Type: PTR (domain name Pointer) (12)
      Class: IN (0x0001)

      Additional RRs: 0
    ▾ Queries
      ▾ www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)

  -----
  ▾ Queries
    ▾ www.aiit.or.kr: type AAAA, class IN
      Name: www.aiit.or.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)

```

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

Відповідь не надішла.

Висновок: у ході виконання третьої лабораторної роботи було виконано аналіз деталей роботи протоколу DNS та покращено навички роботи з Wireshark.