МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №3

з курсу «Комп’ютерні мережі»

тема: «Протокол DNS»

Виконав: студент 3 курсу

групи КА-77

Науменко В.Є.

Прийняв: Кухарєв С.О.

Київ – 2020р.

Пакети для відповідей 1-6

No. Time Source Destination Protocol Length Info
5 0.461056 192.168.1.106 192.168.1.1 DNS 72 Standard query 0x44b0 A www.ietf.org

Frame 5: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0
Ethernet II, Src: CloudNet_2a:d4:77 (48:5f:99:2a:d4:77), Dst: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18)
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 18755 (18755), Dst Port: domain (53)
Domain Name System (query)
Transaction ID: 0x44b0
Flags: 0x0100 Standard query
0..... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... ..0. = Truncated: Message is not truncated
....1 = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
[Response In: 6]

No. Time Source Destination Protocol Length Info
6 0.476754 192.168.1.1 192.168.1.106 DNS 149 Standard query response 0x44b0 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

Frame 6: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0
Ethernet II, Src: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18), Dst: CloudNet_2a:d4:77 (48:5f:99:2a:d4:77)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.106
User Datagram Protocol, Src Port: domain (53), Dst Port: 18755 (18755)
Domain Name System (response)
Transaction ID: 0x44b0
Flags: 0x8180 Standard query response, No error
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

....0.....= Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
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)
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: 335 (5 minutes, 35 seconds)
Data length: 33
CNAME: www.ietf.org.cdn.cloudflare.net
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: 107 (1 minute, 47 seconds)
Data length: 4
Address: 104.20.1.85
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: 107 (1 minute, 47 seconds)
Data length: 4
Address: 104.20.0.85
[Request In: 5]
[Time: 0.015698000 seconds]

Пакети для відповідей 7-10

No.	Time	Source	Destination	Protocol	Length	Info
6	0.163935	192.168.1.106	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu

Frame 6: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0
Ethernet II, Src: CloudNet_2a:d4:77 (48:5f:99:2a:d4:77), Dst: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18)
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 14889 (14889), Dst Port: domain (53)
Domain Name System (query)
Transaction ID: 0x0003
Flags: 0x0100 Standard query

0..... = Response: Message is a query
.000 0..... = Opcode: Standard query (0)
.... ..0. ..... = Truncated: Message is not truncated
....1 ..... = Recursion desired: Do query recursively
.... .0. ..... = Z: reserved (0)
....0 ..... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.mit.edu: type AAAA, class IN
Name: www.mit.edu
[Name Length: 11]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 7]

No. Time Source Destination Protocol Length Info
7 0.199471 192.168.1.1 192.168.1.106 DNS 200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:10e:197::255e AAAA 2a02:26f0:10e:1a2::255e

Frame 7: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0
Ethernet II, Src: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18), Dst: CloudNet_2a:d4:77 (48:5f:99:2a:d4:77)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.106
User Datagram Protocol, Src Port: domain (53), Dst Port: 14889 (14889)
Domain Name System (response)
Transaction ID: 0x0003
Flags: 0x8180 Standard query response, No error
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
....0 ..... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 4
Authority RRs: 0
Additional RRs: 0
Queries
www.mit.edu: type AAAA, class IN
Name: www.mit.edu
[Name Length: 11]

[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
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: 1765 (29 minutes, 25 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: 25 (25 seconds)
Data length: 24
CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:10e:197::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: 2a02:26f0:10e:197::255e
e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:10e:1a2::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: 2a02:26f0:10e:1a2::255e
[Request In: 6]
[Time: 0.035536000 seconds]

Пакети для відповідей 11-13

No. Time Source Destination Protocol Length Info
5 0.155720 192.168.1.106 192.168.1.1 DNS 67 Standard query 0x0002 NS mit.edu

Frame 5: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0
Ethernet II, Src: CloudNet_2a:d4:77 (48:5f:99:2a:d4:77), Dst: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18)
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 19074 (19074), Dst Port: domain (53)
Source Port: 19074 (19074)
Destination Port: domain (53)
Length: 33
Checksum: 0x587a [unverified]
[Checksum Status: Unverified]
[Stream index: 1]

```
    [Timestamps]
Domain Name System (query)
    Transaction ID: 0x0002
    Flags: 0x0100 Standard query
        0...............= Response: Message is a query
        .000 0..........= Opcode: Standard query (0)
        .... ..0.......= Truncated: Message is not truncated
        .... ...1......= Recursion desired: Do query recursively
        .... .... .0....= Z: reserved (0)
        .... .... ...0 ....= Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    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: 8]

No.     Time           Source                Destination           Protocol Length Info
      8 0.221839       192.168.1.1           192.168.1.106         DNS      234    Standard query
response 0x0002 NS mit.edu NS asia2.akam.net NS usw2.akam.net NS use5.akam.net NS ns1-
173.akam.net NS ns1-37.akam.net NS eur5.akam.net NS asia1.akam.net NS use2.akam.net

Frame 8: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface
\Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0
Ethernet II, Src: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18), Dst: CloudNet_2a:d4:77
(48:5f:99:2a:d4:77)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.106
User Datagram Protocol, Src Port: domain (53), Dst Port: 19074 (19074)
    Source Port: domain (53)
    Destination Port: 19074 (19074)
    Length: 200
    Checksum: 0x7301 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    [Timestamps]
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
        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
....0 .....= Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 8
Authority RRs: 0
Additional RRs: 0
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)
Answers
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: 16
Name Server: asia2.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 use5.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: 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 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 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 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 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
[Request In: 5]
[Time: 0.066119000 seconds]

Пакети для відповідей 14-16

No.	Time	Source	Destination	Protocol	Length	Info
2	0.024799	192.168.1.106	192.168.1.1	DNS	73	Standard query 0x1841 A bitsy.mit.edu

Frame 2: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0
Ethernet II, Src: CloudNet_2a:d4:77 (48:5f:99:2a:d4:77), Dst: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18)
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
User Datagram Protocol, Src Port: blackjack (1025), Dst Port: domain (53)
Source Port: blackjack (1025)
Destination Port: domain (53)
Length: 39
Checksum: 0xa560 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
Domain Name System (query)
Transaction ID: 0x1841
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0

```
    Authority RRs: 0
    Additional RRs: 0
    Queries
        bitsy.mit.edu: type A, class IN
            Name: bitsy.mit.edu
            [Name Length: 13]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    [Retransmitted request. Original request in: 1]
    [Retransmission: True]

No.     Time           Source                Destination           Protocol Length Info
      3 0.057917       192.168.1.1           192.168.1.106         DNS      89     Standard query response
0x1841 A bitsy.mit.edu A 18.0.72.3

Frame 3: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface
\Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0
Ethernet II, Src: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18), Dst: CloudNet_2a:d4:77
(48:5f:99:2a:d4:77)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.106
User Datagram Protocol, Src Port: domain (53), Dst Port: blackjack (1025)
    Source Port: domain (53)
    Destination Port: blackjack (1025)
    Length: 55
    Checksum: 0x069e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
Domain Name System (response)
    Transaction ID: 0x1841
    Flags: 0x8180 Standard query response, No error
        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
        .... .... ...0..= Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        bitsy.mit.edu: type A, class IN
            Name: bitsy.mit.edu
            [Name Length: 13]
            [Label Count: 3]
```

Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
bitsy.mit.edu: type A, class IN, addr 18.0.72.3
Name: bitsy.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 4
Address: 18.0.72.3
[Request In: 1]
[Time: 0.057917000 seconds]

Контрольні питання

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?

UPD (17), номер цільового порту запиту DNS – domain (53), номер вихідного порту відповіді DNS – 18755.

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

На 192.168.1.1. Так, є.

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

Типу «A» (Host Address), ні.

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

3 відповіді. Name, Type, Class, Time to live, Data length, CNAME(1 відповідь)/Adress(2-3 відповіді).

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?

Ні.

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

Так.

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

Номер цільового порту запиту DNS – domain (53), номер вихідного порту відповіді DNS – 14889 (14889).?

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

192.168.1.1, так, є.

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

Типу «AAAA (IPv6 Address» (Host address), ні.

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

4 записи із відповідями. Кожна відповідь складається з: Name, Type, Class, Time to live, Data length, CNAME(перші дві)/AAAA Adress(дві останні).

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

192.168.1.1, так, є.

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

Типу «NS» (authoritative Name Server), ні.

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?

8 записів із відповідями. mit.edu, asia2.akam.net, usw2.akam.net, use5.akam.net, ns1-73.akam.net, ns1-37.akam.net, eur5.akam.net, asia1.akam.net, use2.akam.net
. Сервери були запропоновані за домогою доменного імені.

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?

192.168.1.1. Так, це адреса локального сервера.

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

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

Одна відповідь від першого сервера, жодної від другого. Відповідь складається з Name, Type, Class, Time to live, Data length, Adress.

Висновки

Проаналізували деталі роботи протоколу DNS.