

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторний практикум № 3

Протокол DNS

З дисципліни:

Комп'ютерні мережі

Виконав:

Студент 3 курсу

Групи –ІС-зп92

Білозьор О.В.

Перевірив:

Кухарєв С.О.

Київ 2020

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?

Використовується протокол UDP.

User Datagram Protocol, Src Port: 54337, Dst Port: 53

341	27.803304	192.168.0.104	192.168.0.1	DNS	72	Standard query 0xe3c2 A www.ietf.org
342	27.834561	192.168.0.1	192.168.0.104	DNS	149	Standard query response 0xe3c2 A www.ietf.org CNAME www.ietf.org.cdn...
385	28.423020	192.168.0.104	192.168.0.1	DNS	77	Standard query 0x9344 A ocsp.digicert.com
386	28.430489	192.168.0.1	192.168.0.104	DNS	125	Standard query response 0x9344 A ocsp.digicert.com CNAME cs9.wac.ph...
688	29.940130	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x1a2a A analytics.ietf.org
1192	30.940836	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x1a2a A analytics.ietf.org

> Frame 341: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{C6EFBD58-01D6-4564-B1CF-C67A6F318DA3}, id 0
> Ethernet II, Src: ASUSTeK_c7:bb:18 (74:d0:2b:c7:bb:18), Dst: Tp-LinkT_93:aa:28 (c4:6e:1f:93:aa:28)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 54337, Dst Port: 53
v Domain Name System (query)
Transaction ID: 0xe3c2
> Flags: 0x0100 Standard query

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

Destination: 192.168.0.1

No.	Time	Source	Destination	Protocol	Length	Info
341	27.803304	192.168.0.104	192.168.0.1	DNS	72	Standard query 0xe3c2 A www.ietf.org
342	27.834561	192.168.0.1	192.168.0.104	DNS	149	Standard query response 0xe3c2 A www.ietf.org CNAME www.ietf.org.cdn...

Так, це адреса локального DNS-сервера.

IPv4-адрес: 192.168.0.104

DNS-сервери IPv4: 192.168.0.1

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

type A, містить посилання на рядок відповіді ([Response In: 342]).

No.	Time	Source	Destination	Protocol	Length	Info
341	27.803304	192.168.0.104	192.168.0.1	DNS	72	Standard query 0xe3c2 A www.ietf.org
342	27.834561	192.168.0.1	192.168.0.104	DNS	149	Standard query response 0xe3c2 A www.ietf.org CNAME

[Stream index: 0]
> [Timestamps]
v Domain Name System (query)
Transaction ID: 0xe3c2
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
> www.ietf.org: type A, class IN
[Response In: 342]

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

Отримано 3 відповіді.

```

v Queries
  > www.ietf.org: type A, class IN
v 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: 341]
[Time: 0.031257000 seconds]

```

Структура відповіді (на прикладі першої):

Name: www.ietf.org
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 221 (3 minutes, 41 seconds)
 Data length: 33
 CNAME: www.ietf.org.cdn.cloudflare.net

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?

Адреса співпадає.

No.	Time	Source	Destination	Protocol	Length	Info
344	27.851219	192.168.0.104	104.20.1.85	TCP	66	51446 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
345	27.851219	192.168.0.104	104.20.1.85	TCP	66	51445 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

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

Так, додатково було здійснено запити analytics.ietf.org: type A, class IN, ocsf.starfieldtech.com: type A, class IN тощо.

No.	Time	Source	Destination	Protocol	Length	Info
341	27.803304	192.168.0.104	192.168.0.1	DNS	72	Standard query 0xe3c2 A www.ietf.org
385	28.423020	192.168.0.104	192.168.0.1	DNS	77	Standard query 0x9344 A ocsf.starfieldtech.com
688	29.940130	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x1a2a A analytics.ietf.org
1192	30.940836	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x1a2a A analytics.ietf.org
1219	31.394974	192.168.0.104	192.168.0.1	DNS	82	Standard query 0x9831 A ocsf.starfieldtech.com
1272	32.024392	192.168.0.104	192.168.0.1	DNS	72	Standard query 0xa0a2 NS www.ietf.org
1283	33.023753	192.168.0.104	192.168.0.1	DNS	72	Standard query 0xa0a2 NS www.ietf.org

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

Src Port: 53, Dst Port: 51516

No.	Time	Source	Destination	Protocol	Length	Info
7	0.617592	192.168.0.104	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu
8	0.689810	192.168.0.1	192.168.0.104	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgek...

Identification: 0x37d8 (14296)
 > Flags: 0x0000
 Fragment offset: 0
 Time to live: 59
 Protocol: UDP (17)
 Header checksum: 0xc5c9 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.0.1
 Destination: 192.168.0.104

User Datagram Protocol, Src Port: 53, Dst Port: 51516
 Source Port: 53
 Destination Port: 51516
 Length: 126
 Checksum: 0xfc6d [unverified]
 [Checksum Status: Unverified]
 [Stream index: 1]
 > [Timestamps]

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

Destination: 192.168.0.1

No.	Time	Source	Destination	Protocol	Length	Info
7	0.617592	192.168.0.104	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu
8	0.689810	192.168.0.1	192.168.0.104	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgek...

Так, це адреса локального DNS-сервера.

IPv4-адрес: 192.168.0.104

DNS-сервери IPv4: 192.168.0.1

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

type A, містить посилання на рядок відповіді ([Response In: 8]).

No.	Time	Source	Destination	Protocol	Length	Info
7	0.617592	192.168.0.104	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu
8	0.689810	192.168.0.1	192.168.0.104	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgek...

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 57
 Identification: 0x1314 (4884)
 > Flags: 0x0000
 Fragment offset: 0
 Time to live: 128
 Protocol: UDP (17)
 Header checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.0.104
 Destination: 192.168.0.1

User Datagram Protocol, Src Port: 51516, Dst Port: 53
 Source Port: 51516
 Destination Port: 53
 Length: 37
 Checksum: 0x81f0 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 1]
 > [Timestamps]

Domain Name System (query)
 Transaction ID: 0x0002
 > 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: 8]

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

3 відповіді.

Структура (на прикладі першої):

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: 1800 (30 minutes)

Data length: 25

CNAME: www.mit.edu.edgekey.net

dns						
No.	Time	Source	Destination	Protocol	Length	Info
7	0.617592	192.168.0.104	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu
8	0.689810	192.168.0.1	192.168.0.104	DNS	160	Standard query response 0x0002 A www...
Answer RRs: 3						
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						
Name: www.mit.edu						
Type: CNAME (Canonical NAME for an alias) (5)						
Class: IN (0x0001)						
Time to live: 1800 (30 minutes)						
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 A, class IN, addr 23.61.218.91						
Name: e9566.dscb.akamaiedge.net						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 20 (20 seconds)						
Data length: 4						
Address: 23.61.218.91						
[Request In: 7]						
[Time: 0.072218000 seconds]						

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

Destination: 192.168.0.1

dns						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.009067	192.168.0.104	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
4	0.060721	192.168.0.1	192.168.0.104	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-173.akam.net NS asi...

Так, це адреса локального DNS-сервера.

IPv4-адрес: 192.168.0.104

DNS-сервери IPv4: 192.168.0.1

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

Це був запит типу NS, містить посилання на рядок відповіді ([Response In: 4]).

No.	Time	Source	Destination	Protocol	Length	Info
3	0.009067	192.168.0.104	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
4	0.060721	192.168.0.1	192.168.0.104	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-173.akam.net NS asi...

▼ User Datagram Protocol, Src Port: 61374, Dst Port: 53

Source Port: 61374

Destination Port: 53

Length: 33

Checksum: 0x81ec [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

> [Timestamps]

▼ Domain Name System (query)

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> mit.edu: type NS, class IN

[Response In: 4]

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 відповідей.

Запропоновані сервери (за допомогою доменного імені):

ns1-173.akam.net
asia2.akam.net
use5.akam.net
asia1.akam.net
usw2.akam.net
eur5.akam.net
use2.akam.net
ns1-37.akam.net

No.	Time	Source	Destination	Protocol	Length	Info
3	0.009067	192.168.0.104	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
4	0.060721	192.168.0.1	192.168.0.104	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-173.aka

[Stream index: 1]

> [Timestamps]

▼ Domain Name System (response)

Transaction ID: 0x0002

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 0

▼ Queries

> mit.edu: type NS, class IN

▼ Answers

> mit.edu: type NS, class IN, ns ns1-173.akam.net

> mit.edu: type NS, class IN, ns asia2.akam.net

> mit.edu: type NS, class IN, ns use5.akam.net

> mit.edu: type NS, class IN, ns asia1.akam.net

> mit.edu: type NS, class IN, ns usw2.akam.net

> mit.edu: type NS, class IN, ns eur5.akam.net

> mit.edu: type NS, class IN, ns use2.akam.net

> mit.edu: type NS, class IN, ns ns1-37.akam.net

[Request In: 3]

[Time: 0.051654000 seconds]

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?

Destination: 192.168.0.1

No.	Time	Source	Destination	Protocol	Length	Info
38	3.022444	192.168.0.104	192.168.0.1	DNS	73	Standard query 0x33d4 A bitsy.mit.edu
39	3.048535	192.168.0.104	192.168.0.1	DNS	73	Standard query 0x33d4 A bitsy.mit.edu
46	3.314989	192.168.0.1	192.168.0.104	DNS	89	Standard query response 0x33d4 A bitsy.mit.edu A 18.0.72.3

Так, це адреса локального DNS-сервера.

IPv4-адрес: 192.168.0.104

DNS-сервери IPv4: 192.168.0.1

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

type A, містить посилання на рядок відповіді ([Response In: 46]).

Domain Name System (query)
Transaction ID: 0x33d4
> 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: 46]

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

Одна відповідь.

Queries
> bitsy.mit.edu: type A, class IN
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: 38]
[Time: 0.292545000 seconds]

Структура відповіді:

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