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

Лабораторна робота №3

З дисципліни: **«Комп'ютерні мережі»**

На тему: **«Протокол DNS»**

Виконала:

Студентка III курсу

Групи КА-74

Горюшкіна К.Г.

Перевірив:

Кухарєв С.О.

Київ 2020

Рекомендується ознайомитися з такими концепціями:

- локальні сервери DNS;
- кешування DNS-записів і повідомлень;
- тип поля в записі DNS.

Надамо означення вказаним поняттям.

Локальний DNS-сервер - локальний сервер, що використовується для обслуговування DNS-клієнтів, які працюють на локальній машині. Фактично, це різновид кешувального DNS-сервера, сконфігурованого для обслуговування локальних додатків;

Кеш-сервер DNS — сервер, який обслуговує запити клієнтів, (отримує рекурсивний запит, виконує його за допомогою нерекурсивних запитів до авторитетних серверів, або передає рекурсивний запит DNS-серверу, що стоїть вище в ієрархії);

DNS-клієнт (від англ. Domain Name System-client) — програма або модуль в програмі, що забезпечує з'єднання із DNS-сервером для визначення IP-адреси по його доменному імені.

DNS-запит (англ. DNS query) — запит від клієнта (або сервера) до сервера. Запит може бути рекурсивним або нерекурсивний

Рекурсивна процедура:

1. DNS-клієнт запитує локальний DNS-сервер, який обслуговує піддомен, якому належить клієнт;
2. Далі, якщо локальний DNS-сервер відповідь знає, то повертає її клієнту, в протилежному випадку виконує ітеративні запити до кореневого сервера до тих пір, поки не отримає відповідь.

Нерекурсивна процедура:

1. DNS-клієнт звертається до кореневого DNS-сервера з вказівкою повного доменного імені;
2. DNS-сервер відповідає клієнту, вказуючи адресу наступного DNS-сервера, який виконує обслуговування домену верхнього рівня, заданого в наступній старшій частині імені;
3. DNS-клієнт виконує запит наступного DNS-сервера, який його надсилає до DNS-сервера потрібного піддомену і т. д., доти, доки не буде знайдено DNS-сервер, який повністю відповідає запитуваному імені IP-адреси. Сервер дає кінцеву відповідь клієнту.

Після отримання відповіді сервер передає її клієнту. Таким чином, при рекурсивній процедурі клієнт фактично передоручає роботу власному серверу. Для прискорення пошуку IP-адрес DNS-сервери часто застосовують кешування (на час від годин до декількох днів) відповідей, які проходять через них.

«Вебкеш» — інформаційна технологія для тимчасового зберігання вебдокументів і зображень задля зменшення серверних затримок. Система вебкешу зберігає копії документів, що проходять через неї; подальші запити можуть бути виконані з кешу за певних умов.

DNS-сервери часто встановлюються у мережі організацій для прискорення процесу трансляції імен **за допомогою кешування** раніше отриманих відповідей на запити.

Типи DNS-запитів

(Джерело: http://break-people.ru/cmsmade/index.php?page=unix_webmin_howto_dns_type_dns_records**)**

Address (A) - адресный тип записи. Этот тип ассоциирует IP адрес с hostname(имя хоста).

Name Server (NS) - тип записи определяющий имя сервера, отвечающего за обслуживание зоны. Каждая зона должна иметь хотя бы одну NS запись и кроме того, может иметь дополнительные NS записи для поддоменов этой зоны.

Name Alias (CNAME) - этот тип записи позволяет создавать алиасы(псевдонимы, ссылки, привязки) к уже существующим адресным(Address; тип A) и обратным адресным(Reverse Address, тип PTR) записям. Когда DNS клиент запрашивает IP адрес, этого типа(Name Alias), то он получает тот IP адрес, прописанный в той записи, к которой сделана привязка. Это может быть полезным, если вы хотите, чтобы некоторый хост был доступен под несколькими именами.

Mail Server (MX) - тип записи, который сообщает почтовым программам, вроде Sendmail или Qmail, где находится почтовый сервер(сервер к которому, нужно обратится, для доставки почты в этом домене).

Host Information (HINFO) - тип записи используемый для хранения информации об архитектуре и операционной системе некоторого хоста.

Text (TXT) - тип записи, который ассоциирует произвольную текстовую информацию с выбранной зоной(доменом).

Well Known Service (WKS) - тип записи, который ассоциирует hostname(имя хоста), порт и протокол некоторого сервиса(например, почта) с выбранной зоной. Это может быть, к примеру, использовано, для указания клиентам, какой хост является почтовым сервером.

Responsible Person (RP) - тип записи, который ассоциирует человека или группу людей ответственных за эту зону(домен).

Location (LOC) - тип записи, который используется для указания физического расположения хоста. В координатах широты и долготы.

Service Address (SRV) - тип записи, который ассоциирует доменное имя, имя сервиса и протокол с некоторым хостом. Другими словами, эта запись используется для указания расположения некоторого сервиса на некотором хосте.

Public Key (KEY) - тип записи, который ассоциирует «ключ» к некоторому хосту. Этот ключ используется для IPsec VPN.

Reverse Address (PTR) - тип записи, который ассоциирует hostname(имя хоста) с IP адресом в обратной зоне.

Name Server (NS) - тип записи NS в обратной зоне, предназначен для того же, что и в прямой - он сообщает другим DNS серверам, IP адрес или hostname(имя хоста) сервера обслуживающего некоторую зону(домен) или некоторый поддомен.

Name Alias (CNAME) - тип записи в обратной зоне, предназначен для того же, что и в прямой - алиас, ссылка, привязка к некоторой записи.

Хід роботи:

Очистка кеша DNS-записів: у терміналі команда

```
sudo killall -HUP mDNSResponder; sleep 2;
```

Контрольні запитання:

До dump1:

```
No.     Time           Source                Destination           Protocol Info
Length
      9 7.928083       192.168.1.117         192.168.1.1           DNS      Standard query
0x986a A frpxa.com                              69
Frame 9: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface en0, id 0
Ethernet II, Src: Apple_ef:19:a4 (48:bf:6b:ef:19:a4), Dst: ASUSTekC_92:2d:1a (c8:60:00:92:2d:
1a)
Internet Protocol Version 4, Src: 192.168.1.117, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 55078, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x986a
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 11]
```

```
No.     Time          Source              Destination         Protocol Info
Length
     11 7.939454      192.168.1.1         192.168.1.117       DNS      Standard query
response 0x986a A frpxa.com A 79.137.156.51 NS ns-803.awsdns-36.net NS ns-177.awsdns-22.com NS
ns-1930.awsdns-49.co.uk NS ns-1027.awsdns-00.org A 205.251.192.177 A 205.251.195.35 A
205.251.196.3 A 205.251.199.138 AAAA 2600:9000:5300:b100::1 AAAA 2600:9000:5303:2300::1 AAAA
2600:9000:5304:300::1 AAAA 2600:9000:5307:8a00::1 398
Frame 11: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits) on interface en0, id 0
Ethernet II, Src: ASUSTekC_92:2d:1a (c8:60:00:92:2d:1a), Dst: Apple_ef:19:a4 (48:bf:6b:ef:
19:a4)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.117
User Datagram Protocol, Src Port: 53, Dst Port: 55078
Domain Name System (response)
    Transaction ID: 0x986a
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
    Queries
    Answers
        frpxa.com: type A, class IN, addr 79.137.156.51
            Name: frpxa.com
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 10 (10 seconds)
            Data length: 4
            Address: 79.137.156.51
    Authoritative nameservers
        frpxa.com: type NS, class IN, ns ns-803.awsdns-36.net
            Name: frpxa.com
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 429 (7 minutes, 9 seconds)
            Data length: 22
            Name Server: ns-803.awsdns-36.net
        frpxa.com: type NS, class IN, ns ns-177.awsdns-22.com
            Name: frpxa.com
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 429 (7 minutes, 9 seconds)
            Data length: 19
            Name Server: ns-177.awsdns-22.com
        frpxa.com: type NS, class IN, ns ns-1930.awsdns-49.co.uk
            Name: frpxa.com
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 429 (7 minutes, 9 seconds)
            Data length: 25
            Name Server: ns-1930.awsdns-49.co.uk
        frpxa.com: type NS, class IN, ns ns-1027.awsdns-00.org
            Name: frpxa.com
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 429 (7 minutes, 9 seconds)
            Data length: 23
            Name Server: ns-1027.awsdns-00.org
    Additional records
        ns-177.awsdns-22.com: type A, class IN, addr 205.251.192.177
            Name: ns-177.awsdns-22.com
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 171995 (1 day, 23 hours, 46 minutes, 35 seconds)
            Data length: 4
            Address: 205.251.192.177
        ns-803.awsdns-36.net: type A, class IN, addr 205.251.195.35
```

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?

UDP

53

53

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?
192.168.1.1; Так
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
type A (class IN) - адресный тип записи. Этот тип ассоциирует IP адрес с hostname(имя хоста). Ні, не вміщує
4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?
6
name, type, class, addr, time to live, data length, name server, cname
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
6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?
Так

До dump2:

```
No.     Time           Source                Destination           Protocol Info
Length
     29 4.564708       192.168.1.117         192.168.1.1           DNS      Standard query
0xc1e1 A www.mit.edu                            71
Frame 29: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0
Ethernet II, Src: Apple_ef:19:a4 (48:bf:6b:ef:19:a4), Dst: ASUSTekC_92:2d:1a (c8:60:00:92:2d:
1a)
Internet Protocol Version 4, Src: 192.168.1.117, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 59967, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0xc1e1
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    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: 30]
```

```
No.     Time           Source                Destination           Protocol Info
Length
     30 4.609149       192.168.1.1           192.168.1.117         DNS      Standard query
response 0xc1e1 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A
23.63.130.176 160
Frame 30: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface en0, id 0
Ethernet II, Src: ASUSTekC_92:2d:1a (c8:60:00:92:2d:1a), Dst: Apple_ef:19:a4 (48:bf:6b:ef:
19:a4)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.117
User Datagram Protocol, Src Port: 53, Dst Port: 59967
Domain Name System (response)
    Transaction ID: 0xc1e1
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    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)
    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 23.63.130.176
    [Request In: 29]
    [Time: 0.044441000 seconds]
```

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

53

53

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

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

type A, ні

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

3

name, type, class, time to live, data length. cname

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

192.168.1.117; Hi

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

type A

Hi

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?
no servers could be reached
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?
18.0.72.3; Hi
www.aiit.or.kr
15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
type A; Hi
16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?
2
name, type, class, time to live, data length, cname