

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

Лабораторна робота №5
з дисципліни «Комп'ютерні мережі»

«Доменна служба імен. Утиліти nslookup та dig»

Виконала студентка групи: КВ-11

ПІБ: Михайліченко Софія Віталіївна

Перевірив: _____

Мета роботи:

Поглиблене самостійне вивчення спеціальних питань, присвячених організації та конфігуруванню сервера доменних імен.

План виконання лабораторної роботи:

1. Ознайомитися та засвоїти теоретичні відомості, викладені в методичному посібнику до лабораторної роботи.
2. Виконати завдання до лабораторної роботи.

Завдання:

1. Виконати пряме перетворення для вказаного викладачем доменного імені. Звернути увагу на наявність канонічного доменного імені і псевдоніма (alias). Виконати зворотне перетворення для отриманої IP-адреси. Перетворення виконувати шляхом посилки ітеративних запитів, не забудьте вказати абсолютні доменні імена. Виконати пряме і зворотне перетворення для scs.kpi.ua.
2. Налаштувати хост так, щоб він звертався до іншого DNS-серверу своєї зони. Список серверів своєї зони знайти.
3. Для вказаного викладачем хосту знайти зону DNS, до якої він належить; сервери DNS, які її обслуговують; тимчасові характеристики взаємодії первинного і вторинного серверів для цієї зони; можливі псевдоніми даного хосту. Одержувати тільки авторитетні відповіді.

Короткі теоретичні відомості:

Система доменних імен (DNS) є критично важливою частиною інфраструктури Інтернету, що забезпечує перетворення зручних для користувачів доменних імен у IP-адреси, які використовуються для маршрутизації даних. Основна мета DNS полягає в спрощенні доступу до ресурсів мережі, дозволяючи користувачам вводити зрозумілі імена замість числових адрес.

Пряме перетворення полягає у визначенні IP-адреси для заданого доменного імені. Це здійснюється шляхом надсилання запиту до DNS-сервера, який обробляє запити, використовуючи ітеративний або рекурсивний підходи. Ітеративний запит передбачає, що сервер повертає або IP-адресу, або посилання на інший сервер, якщо не має необхідної інформації. Важливо зазначити, що під час виконання запиту слід використовувати абсолютні доменні імена, що включають кореневий домен (наприклад, `scs.kpi.ua.`).

Канонічне доменне ім'я (CNAME) є альтернативним іменем для вже існуючого доменного імені, що дозволяє використовувати декілька імен для одного ресурсу. Псевдонім (alias) вказує на те, що дане ім'я є синонімом для іншого доменного імені. Зворотне перетворення, в свою чергу, полягає у визначенні доменного імені за відомою IP-адресою, що також виконується через запити до DNS-сервера.

Зона DNS є частиною простору імен, за яку відповідає певний DNS-сервер. Для визначення зони, до якої належить вказаний хост, необхідно виконати запит до авторитетного сервера, який надасть інформацію про сервери, що обслуговують цю зону, а також про тимчасові характеристики взаємодії між первинним і вторинним серверами. Ці характеристики включають параметри, такі як час оновлення (refresh), час повторної спроби (retry) та час життя (expire) записів.

Отримання авторитетних відповідей є важливим аспектом, оскільки вони забезпечують точність і достовірність інформації, що надається. Це дозволяє уникнути помилок, пов'язаних з кешованими даними, які можуть бути застарілими або некоректними.

Порядок виконання роботи:

Для виконання завдання 1 спочатку нам потрібно обрати глобальний DNS сервер. Дані в яких завжди доступні і здатні швидко відповідати на запити з усього світу і регулярно оновлюються.

Обраний нами сервер Cloudflare DNS server – 1.1.1.1

Також відповідно до завдання перетворення потрібно виконувати шляхом посилки ітеративних запитів, для чого використаємо `-norecurse`. У той час для отримання інформації про сервери, що обслуговують потрібний нам домен `-type=ns`.

Результат отримання списку корневих DNS-серверів:

```
C:\Users\sofia>nslookup -norecurse -type=ns . 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
(root)  nameserver = a.root-servers.net
(root)  nameserver = b.root-servers.net
(root)  nameserver = c.root-servers.net
(root)  nameserver = d.root-servers.net
(root)  nameserver = e.root-servers.net
(root)  nameserver = f.root-servers.net
(root)  nameserver = g.root-servers.net
(root)  nameserver = h.root-servers.net
(root)  nameserver = i.root-servers.net
(root)  nameserver = j.root-servers.net
(root)  nameserver = k.root-servers.net
(root)  nameserver = l.root-servers.net
(root)  nameserver = m.root-servers.net

C:\Users\sofia>
```

Далі отримаємо IP-адреси DNS-сервера a.root-servers.net:

```
C:\Users\sofia>nslookup -norecurse a.root-servers.net 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    a.root-servers.net
Addresses: 2001:503:ba3e::2:30
          198.41.0.4
```

Виконаємо запит до кореневого DNS-сервера для отримання інформації про DNS-сервери, які обслуговують доменну зону scs.kpi.ua:

```
C:\Users\sofia>nslookup -norecurse -type=ns scs.kpi.ua 198.41.0.4
in-addr.arpa    nameserver = f.in-addr-servers.arpa
in-addr.arpa    nameserver = b.in-addr-servers.arpa
in-addr.arpa    nameserver = d.in-addr-servers.arpa
in-addr.arpa    nameserver = a.in-addr-servers.arpa
in-addr.arpa    nameserver = c.in-addr-servers.arpa
in-addr.arpa    nameserver = e.in-addr-servers.arpa
f.in-addr-servers.arpa internet address = 193.0.9.1
f.in-addr-servers.arpa AAAA IPv6 address = 2001:67c:e0::1
b.in-addr-servers.arpa internet address = 199.253.183.183
b.in-addr-servers.arpa AAAA IPv6 address = 2001:500:87::87
d.in-addr-servers.arpa internet address = 200.10.60.53
d.in-addr-servers.arpa AAAA IPv6 address = 2001:13c7:7010::53
a.in-addr-servers.arpa internet address = 199.180.182.53
a.in-addr-servers.arpa AAAA IPv6 address = 2620:37:e000::53
c.in-addr-servers.arpa internet address = 196.216.169.10
c.in-addr-servers.arpa AAAA IPv6 address = 2001:43f8:110::10
e.in-addr-servers.arpa internet address = 203.119.86.101
e.in-addr-servers.arpa AAAA IPv6 address = 2001:dd8:6::101
Server:  UnKnown
Address:  198.41.0.4

ua          nameserver = bg.ns.ua
ua          nameserver = nn.ns.ua
ua          nameserver = rcz.ns.ua
ua          nameserver = in1.ns.ua
ua          nameserver = cz.ns.ua
ua          nameserver = ho1.ns.ua
ua          nameserver = pch.ns.ua
bg.ns.ua    internet address = 185.136.97.185
bg.ns.ua    internet address = 185.136.96.185
bg.ns.ua    AAAA IPv6 address = 2a06:fb00:1::2:185
bg.ns.ua    AAAA IPv6 address = 2a06:fb00:1::4:185
nn.ns.ua    internet address = 194.58.197.4
nn.ns.ua    AAAA IPv6 address = 2a01:3f1:c001::53
rcz.ns.ua   internet address = 193.46.128.10
rcz.ns.ua   AAAA IPv6 address = 2a02:850:ffe0::10
in1.ns.ua   internet address = 74.123.224.40
in1.ns.ua   AAAA IPv6 address = 2604:ee00:0:101::40
cz.ns.ua    internet address = 185.43.134.15
cz.ns.ua    AAAA IPv6 address = 2001:148f:fffd::15
ho1.ns.ua   internet address = 195.47.253.1
ho1.ns.ua   AAAA IPv6 address = 2001:67c:258::1
pch.ns.ua   internet address = 204.61.216.12
pch.ns.ua   AAAA IPv6 address = 2001:500:14:6012:ad::1
```

Згідно із завданням отримаємо інформацію про сервери імен для домену scs.kpi.ua:

```
C:\Users\sofia>nslookup -norecurse -type=ns scs.kpi.ua 185.136.96.185
Server: UnKnown
Address: 185.136.96.185

kpi.ua nameserver = robotns3.second-ns.com
kpi.ua nameserver = robotns2.second-ns.de
kpi.ua nameserver = ns1.first-ns.de
kpi.ua nameserver = ns.kpi.ua
ns.kpi.ua internet address = 77.47.128.130
C:\Users\sofia>
```

Отримання IP-адреси домену scs.kpi.ua:

```
C:\Users\sofia>nslookup -norecurse scs.kpi.ua 77.47.128.130
Server: ns.kpi.ua
Address: 77.47.128.130

Name: scs.kpi.ua
Address: 77.47.131.42
```

Виконаємо рекурсивний запит для перевірки:

```
C:\Users\sofia>nslookup scs.kpi.ua
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: scs.kpi.ua
Address: 77.47.131.42
```

Порівнюючи бачимо, що адреси збігаються 77.47.131.42, можемо зробити висновок про правильність виконаних перетворень.

Також нам потрібно звернути увагу на наявність канонічного доменного імені і псевдоніма (alias).

```
C:\Users\sofia>nslookup -type=cname www.scs.kpi.ua
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
www.scs.kpi.ua canonical name = scs.kpi.ua
```

Доменне ім'я www.scs.kpi.ua є псевдонімом для канонічного домену scs.kpi.ua. Це означає, що запит на www.scs.kpi.ua буде перенаправлено на адресу scs.kpi.ua.

Виконаємо зворотнє перетворення:

```
C:\Users\sofia>nslookup 77.47.131.42
Server: UnKnown
Address: 192.168.1.1

Name:     scs.kpi.ua
Address:  77.47.131.42
```

Для виконання завдання 2, нам потрібно налаштувати хост так, щоб він звертався до іншого DNS-серверу своєї зони, потрібно для початку знайти список серверів цієї зони.

Отримання інформації про сервери імен для домену scs.kpi.ua:

```
C:\Users\sofia>nslookup -type=ns scs.kpi.ua
Server: UnKnown
Address: 192.168.1.1

kpi.ua
primary name server = ns.kpi.ua
responsible mail addr = domainmaster.kpi.ua
serial = 2024112201
refresh = 14400 (4 hours)
retry = 3600 (1 hour)
expire = 1209600 (14 days)
default TTL = 86400 (1 day)

C:\Users\sofia>
```

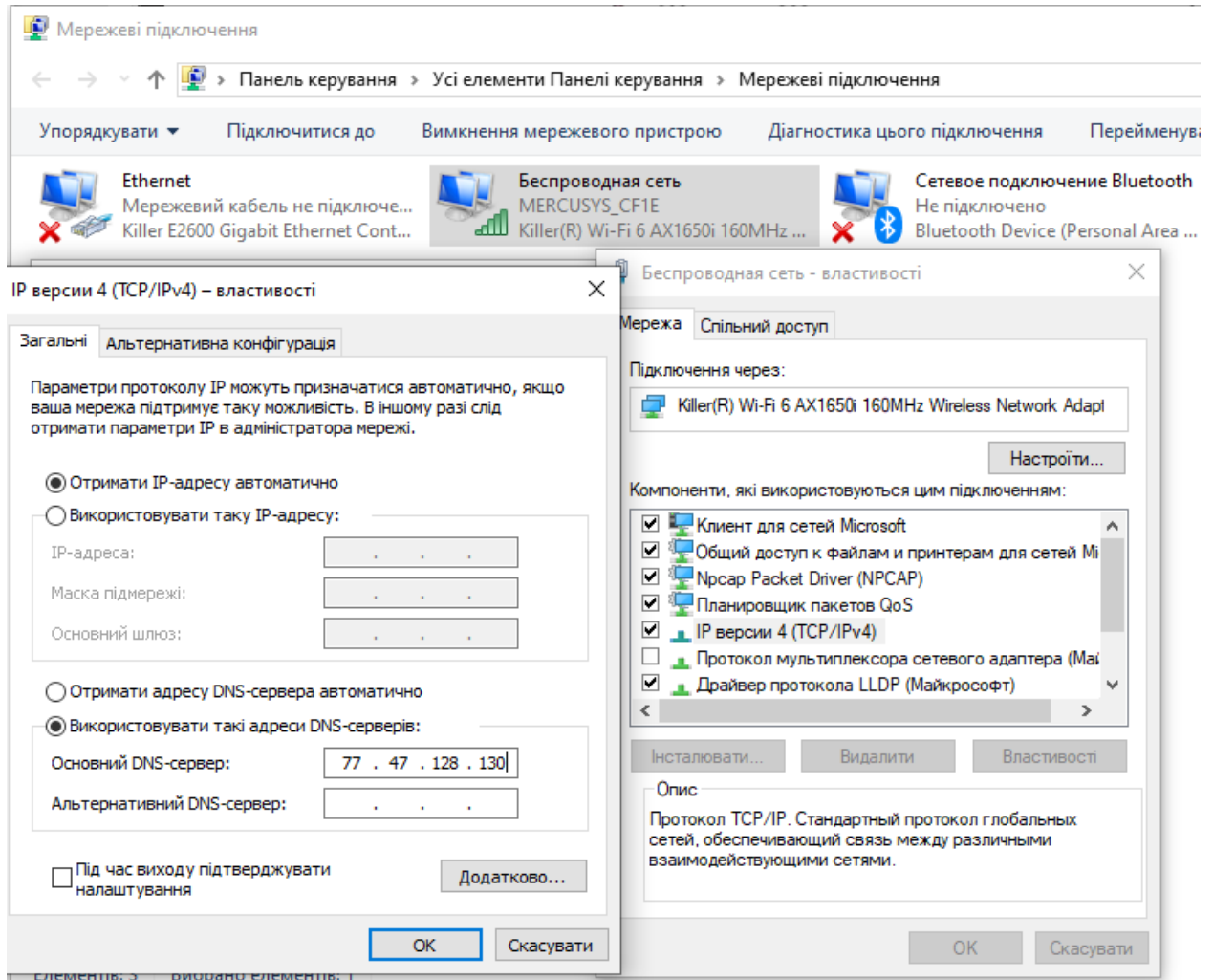
Запит підтвердив, що основний сервер для зони kpi.ua — це **ns.kpi.ua**, і всі записи цієї зони, включаючи scs.kpi.ua, обслуговуються відповідно до вказаних тимчасових параметрів.

Отримання IP-адреси ns.kpi.ua:

```
C:\Users\sofia>nslookup ns.kpi.ua
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name:     ns.kpi.ua
Address:  77.47.128.130
```

Далі для зміни налаштувань DNS-сервера відкриємо мережеві налаштування:



Результат запиту після зміни сервера:

```
C:\Users\sofia>nslookup scs.kpi.ua
Server: ns.kpi.ua
Address: 77.47.128.130

Name: scs.kpi.ua
Address: 77.47.131.42
```


Для виконання завдання 3 нам потрібно отримати Тимчасові характеристики взаємодії первинного і вторинного серверів для цієї зони:

```
C:\Users\sofia>nslookup
Default Server:  ns.kpi.ua
Address:  77.47.128.130

> set type=soa
> www.kpi.ua ns.kpi.ua
Server:  ns.kpi.ua
Address:  77.47.128.130

www.kpi.ua      canonical name = kpi.ua
kpi.ua
        primary name server = ns.kpi.ua
        responsible mail addr = domainmaster.kpi.ua
        serial = 2024112201
        refresh = 14400 (4 hours)
        retry = 3600 (1 hour)
        expire = 1209600 (14 days)
        default TTL = 86400 (1 day)
kpi.ua  nameserver = robotns3.second-ns.com
kpi.ua  nameserver = robotns2.second-ns.de
kpi.ua  nameserver = ns1.first-ns.de
kpi.ua  nameserver = ns.kpi.ua
ns.kpi.ua      internet address = 77.47.128.130
> server ns.kpi.ua
Default Server:  ns.kpi.ua
Address:  77.47.128.130
```

```
> set type=any
> kpi.ua
Server:  ns.kpi.ua
Address:  77.47.128.130

kpi.ua
        primary name server = ns.kpi.ua
        responsible mail addr = domainmaster.kpi.ua
        serial = 2024112201
        refresh = 14400 (4 hours)
        retry = 3600 (1 hour)
        expire = 1209600 (14 days)
        default TTL = 86400 (1 day)
kpi.ua  nameserver = ns1.first-ns.de
kpi.ua  nameserver = robotns2.second-ns.de
kpi.ua  nameserver = robotns3.second-ns.com
kpi.ua  nameserver = ns.kpi.ua
kpi.ua  internet address = 80.91.164.19
kpi.ua  MX preference = 10, mail exchanger = mx-gw1.kpi.ua
kpi.ua  MX preference = 11, mail exchanger = mx-gw2.kpi.ua
kpi.ua  text =

        "v=spf1 redirect=_spf.kpi.ua"
kpi.ua  text =

        "MS=D1089BC569920E3185FF812D85F63F171F8DE51D"
kpi.ua  text =

        "google-site-verification=AhOSPr7LFcgWK0o01AhuKccz6Mi73MGARduYJTVkQzk"
kpi.ua  text =

        "google-site-verification=UdsMKVZhK2Vf1_xgeVHCu7vZbnpPtdoOgeUtIXnIeBA"
kpi.ua  text =

        "atlassian-domain-verification=ijtfCz1ndHjAhpMh8ZlKIEuQorBS0yN/CpWNwnEJa5MF0piWIJhpFDH4Lr7B1rz0"
kpi.ua  text =

        "MS=ms73409330"
ns.kpi.ua      internet address = 77.47.128.130
mx-gw1.kpi.ua  internet address = 77.47.128.185
mx-gw1.kpi.ua  AAAA IPv6 address = 2a02:db0:0:798::185
mx-gw2.kpi.ua  internet address = 77.47.128.186
mx-gw2.kpi.ua  AAAA IPv6 address = 2a02:db0:0:798::186
```

Висновок:

Лабораторна робота дала змогу поглиблено вивчити принципи роботи системи доменних імен (DNS), які є основою для коректної та стабільної роботи Інтернету. Вивчення інструментів, таких як nslookup і dig, дозволило на практиці зрозуміти, як здійснюються запити для перетворення доменних імен в IP-адреси та навпаки. Особливу увагу було приділено аналізу канонічних доменних імен та псевдонімів, що є важливими аспектами організації DNS.

Завдання, що стосувались налаштування хоста для використання іншого DNS-сервера, продемонстрували важливість точного управління зонами та забезпечення коректної роботи мережевої інфраструктури. Завдяки аналізу тимчасових характеристик взаємодії первинного і вторинного серверів, вдалося зрозуміти принципи синхронізації та оновлення даних у DNS-системі. Отримані знання та навички є важливими для адміністрування мереж та налаштування серверів імен, що має велике значення для забезпечення надійності та безпеки мережевих ресурсів. Цей досвід стане основою для подальшого вдосконалення в галузі комп'ютерних мереж.