

**Звіт**  
**з дисципліни Телекомунікаційні**  
**Інформаційні Мережі**  
**Лабораторна робота №2**  
**на тему: «Діагностика стану мережі на основі TCP/IP»»**

Виконав: студент групи ІПЗ-3.04

Бухта М.М

---

Перевірів: Шулакова К.С.

---

Одеса 2023

## МЕТА РОБОТИ

Ознайомитися з мережними командами та навчитися використовувати їх при тестуванні комп'ютерних мереж різного призначення та архітектури.

## КЛЮЧОВІ ПИТАННЯ

1. Укажіть призначення й основні параметри утиліти `ipconfig`.

Утиліта `ipconfig` використовується для відображення всіх поточних параметрів мережі TCP/IP та оновлення параметрів DHCP і DNS. За замовчуванням виводиться лише IP-адреса, маска підмережі і основний шлюз для кожного мережного адаптера. Основні параметри утиліти:

- a. `/all` = виведення повної конфігурації TCP/IP для всіх адаптерів.
- b. `/renew [адаптер]` – оновлення конфігурації DHCP для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера.
- c. `/release [адаптер]` – відправка повідомлення DHCPRELEASE серверу DHCP для звільнення поточної конфігурації DHCP і видалення конфігурації IP-адрес для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера.
- d. `/flushdns` – скидання та очищення вмісту кеша порівняння імен DNS.
- e. `/displaydns` – відображення вмісту кеша порівняння імен DNS, включає записи, попередньо завантажені з локального файлу `Hosts`, а також останні отримані записи ресурсів для запитів на порівняння імен.
- f. `/registerdns` – динамічна реєстрація вручну імен DNS на IP-адрес, налаштованих на комп'ютері.
- g. `/showclassid` (або `/allcompartments`) адаптер – відображення коду класу DHCP для зазначеного адаптера.
- h. `/setclassid адаптер [код класу]` – присвоєння коду класу DHCP для зазначеного адаптера.
- i. `/?` = відображення довідки в командному рядку.

2. Укажіть призначення й основні параметри утиліти `arp`.

Утиліта `arp` використовується для виводу і зміни записів кеша протоколу ARP, який містить одну або декілька таблиць, які використовуються для зберігання IP-адрес та відповідних їм фізичних адрес Ethernet або Token Ring. Запущена без параметрів, команда `arp` виводить довідку. Основні параметри утиліти:

- a. `-a [інет_адрес] [-N ін_адрес]` – виведення таблиць поточного протоколу ARP для всіх інтерфейсів
- b. `-g [інет_адрес] [-N ін_адрес]` – збігається з `-a`.
- c. `-d інет_адрес [ін_адрес]` – видалення запису з певною IP адресою, де `інет_адрес` – це IP-адреса.
- d. `-s інет_адрес е_адрес [ін_адрес]` – додавання статичного запису, який співставляє IP-адресу з `інет_адрес` з фізичною адресою `е_адрес`, в кеші ARP.

3. Укажіть призначення утиліти `nslookup`.

Утиліта `nslookup` призначена для діагностики інфраструктури DNS.

4. Для чого використовується утиліта `netstat`?

Утиліта `netstat` використовується для того, щоб виводити статистику про поточні IP-з'єднання, стані портів, таблиці маршрутизації, стані активних TCP з'єднань і ін.

5. Який протокол необхідний для роботи з утилітами?

TCP/IP

6. Який результат видасть утиліта `netstat` з параметрами `-a`, `-s` та `-r`?

Параметр `-a` буде виводити у живому режимі всі підключення та порт, на котрі комп'ютер очікує з'єднання.

Параметр `-s` буде виводити статичні дані по протоколам.

Параметр `-r` буде виводити таблицю маршрутизації.

7. Як можна за допомогою утиліти оновити IP-адресу?

`ipconfig /release` – виводить IP-адресу з мережевого адаптера.  
`ipconfig /renew` – надає запит на оновлення IP-адреси від DHCP-сервера

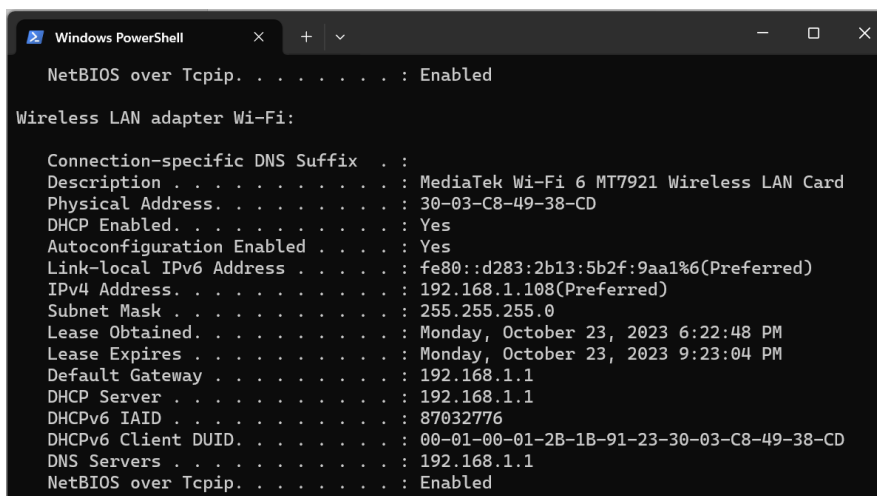
# ЗАВДАННЯ 1

## Опис завдання:

- Запишіть основні параметри мережної конфігурації PC, а саме фізичну адресу, IP-адресу, маску підмережі, основний шлюз та DHCP-сервер.
- Для оновлення конфігурації IP-адреси, яка визначена DHCP-сервером, тільки для адаптера «Підключення по локальній мережі», введіть: `ipconfig /renew`.
- Для того, щоб скинути кеш порівняння імен DNS за наявності несправностей у порівнянні імен, введіть `ipconfig /flushdns`;
- Для того, щоб ввести код класу DHCP для всіх адаптерів, які починаються зі слова Подключение, введіть `/allcompartments`.

## Виконання:

Для того, щоб дізнатися конфігурацію PC, треба використати команду `ipconfig /all`. Ця команда виводить детальну інформацію о всіх мережевих адаптерів. Для мого випадку, я буду шукати адаптер Wi-Fi, так як він використовується повсякденно. Результат виконання програми можна побачити на рисунку 1.1. Мак адрес цього мережевого адаптера 30-03-C8-49-38-CD, IP-адреса 192.168.1.108 з маскою 255.255.255.0. Також є інформація про шлюз та про DHCP сервер, що у даному випадку є один та теж самий пристрій з IP-адресою 192.168.1.1.



```
Windows PowerShell
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Description . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Physical Address. . . . . : 30-03-C8-49-38-CD
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d283:2b13:5b2f:9aa1%6(Preferred)
IPv4 Address. . . . . : 192.168.1.108(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, October 23, 2023 6:22:48 PM
Lease Expires . . . . . : Monday, October 23, 2023 9:23:04 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 87032776
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-1B-91-23-30-03-C8-49-38-CD
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

Рисунок 1.1 – інформація LAN адаптера.

Після оновлюємо конфігурацію через команду `ipconfig /renew` (рис 1.2), але, судячи по результату виконання, ніяких змін фактично не відбулося.



```
PS C:\Users\Nikita> ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::522b:dea:d9a8:147b%25
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6649:8b9e:f689:4edb%5
    IPv4 Address. . . . . : 192.168.245.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::799:ed2e:88d0:99ac%14
    IPv4 Address. . . . . : 192.168.119.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

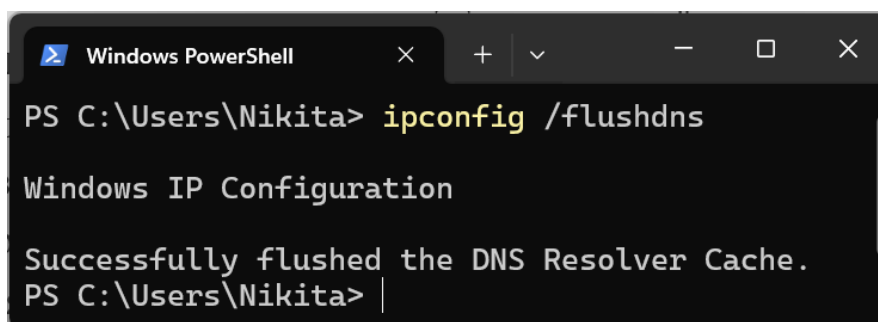
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d283:2b13:5b2f:9aa1%6
    IPv4 Address. . . . . : 192.168.1.108
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter vEthernet (Default Switch):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bff:fb46:635c:71e9%27
    IPv4 Address. . . . . : 172.30.32.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 
PS C:\Users\Nikita>
```

Рисунок 1.2 – результат виконання команди `ipconfig /renew`.

Скинемо кеш порівняння імен DNS через команду `ipconfig /flushdns` (рис 1.3)



```
PS C:\Users\Nikita> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\Users\Nikita>
```

Рисунок 1.3 – результат виконання команди `ipconfig /flushdns`.

Введемо код класу DHCP для всіх адаптерів, які починаються зі слова Подключение, введіть /allcompartments (рис 1.4)

```
Windows PowerShell
PS C:\Users\Nikita> ipconfig /allcompartments

Windows IP Configuration

=====
Network Information for Compartment 1 (ACTIVE)
=====

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::522b:dea:d9a8:147b%25
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6649:8b9e:f689:4edb%5
    IPv4 Address. . . . . : 192.168.245.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::799:ed2e:88d0:99ac%14
    IPv4 Address. . . . . : 192.168.119.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d283:2b13:5b2f:9aa1%6
    IPv4 Address. . . . . : 192.168.1.108
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter vEthernet (Default Switch):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bff:fb46:635c:71e9%27
    IPv4 Address. . . . . : 172.30.32.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 

PS C:\Users\Nikita>
```

Рисунок 1.4 – результат виконання команди ipconfig /allcompartments.

## ЗАВДАННЯ 2

### Опис завдання:

- Для виведення таблиці кеша ARP для усіх інтерфейсів, введіть: arp -a;

- Для того, щоб вивести таблицю кеша ARP для інтерфейсу, якому призначена IP-адреса 10.0.9.51, введіть: `arp -a -N 10.0.9.51`
- Додайте статичний запис кешу ARP, який порівнює IP-адресу 10.0.0.80 з фізичною адресою 00-AA-00-4F-2A-9C.

## Виконання:

Введемо команду `arp -a` щоб дізнатися кеш arp (рис 2.1).

```

PS C:\Users\Nikita> arp -a

Interface: 192.168.245.1 --- 0x5
Internet Address      Physical Address      Type
192.168.245.255       ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.1.187           01-00-5e-00-01-bb    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 192.168.1.108 --- 0x6
Internet Address      Physical Address      Type
192.168.1.1           9c-53-22-7f-6e-e7    dynamic
192.168.1.102         f8-b9-5a-48-30-e2    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.1.187           01-00-5e-00-01-bb    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.119.1 --- 0xe
Internet Address      Physical Address      Type
192.168.119.255       ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.1.187           01-00-5e-00-01-bb    static
239.255.255.250       01-00-5e-7f-ff-fa    static

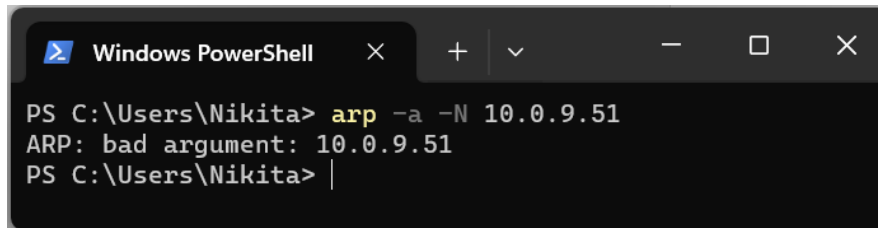
Interface: 192.168.56.1 --- 0x19
Internet Address      Physical Address      Type
192.168.56.255       ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.1.187           01-00-5e-00-01-bb    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 172.30.32.1 --- 0x1b
Internet Address      Physical Address      Type
172.30.47.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.1.187           01-00-5e-00-01-bb    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
PS C:\Users\Nikita>

```

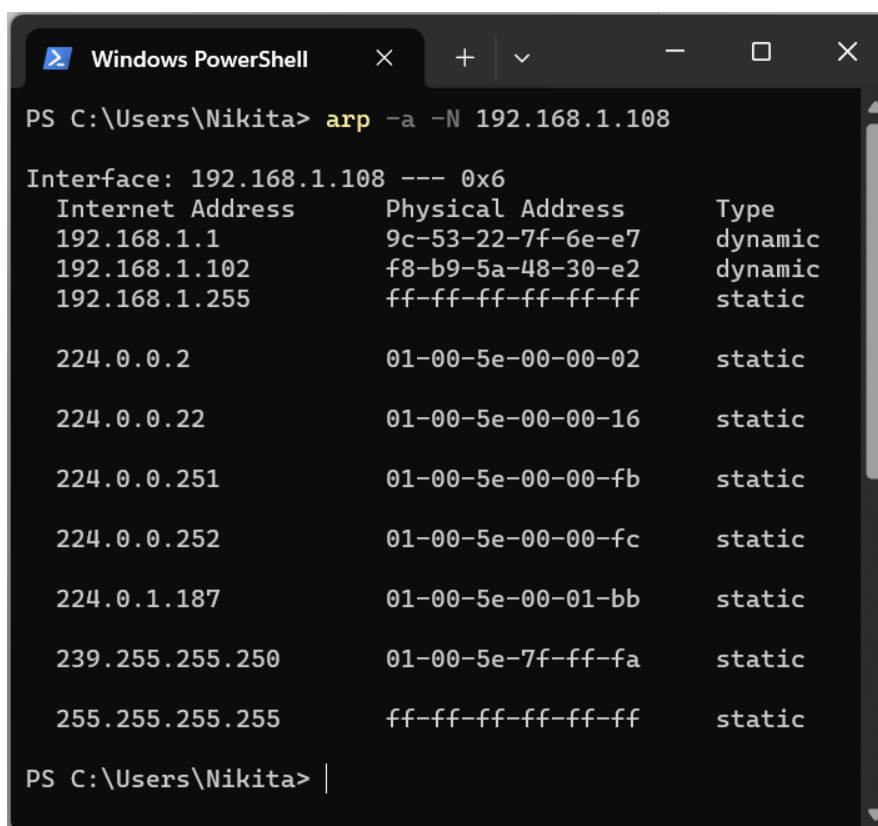
Рисунок 2.1 – список arp таблиц кожного інтерфейсу.

Далі по завданню на м потрібно знайти arp таблицю неіснуючого на даній машині інтерфейсу 10.0.9.51. Як результат, ми получили повідомлення о помилці, яке можна побачити на рис 2.2. Тому використаєм один з інтерфейсів, що вже існує. Результат виконання зображен на рис 2.3.



```
Windows PowerShell
PS C:\Users\Nikita> arp -a -N 10.0.9.51
ARP: bad argument: 10.0.9.51
PS C:\Users\Nikita> |
```

Рисунок 2.2 – пошук arp таблиці інтерфейса 10.0.9.51.



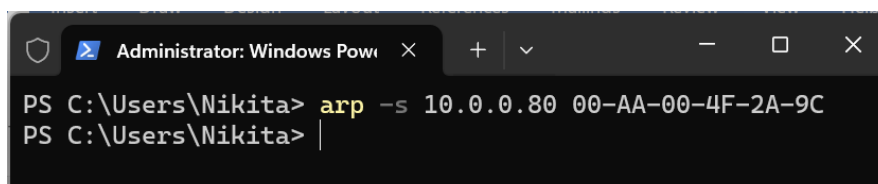
```
Windows PowerShell
PS C:\Users\Nikita> arp -a -N 192.168.1.108

Interface: 192.168.1.108 --- 0x6
Internet Address      Physical Address      Type
192.168.1.1           9c-53-22-7f-6e-e7     dynamic
192.168.1.102         f8-b9-5a-48-30-e2     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static

224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
224.0.1.187           01-00-5e-00-01-bb     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

PS C:\Users\Nikita> |
```

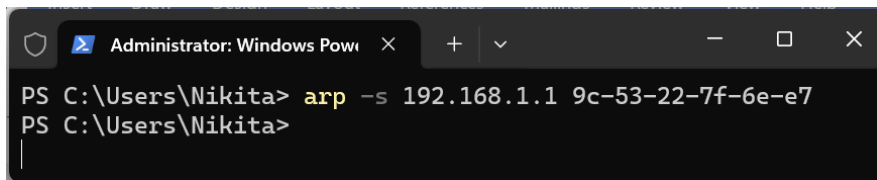
Рисунок 2.3 – пошук arp таблиці інтерфейса 192.168.1.108.



```
Administrator: Windows PowerShell
PS C:\Users\Nikita> arp -s 10.0.0.80 00-AA-00-4F-2A-9C
PS C:\Users\Nikita> |
```

Рисунок 2.4 – порівняння неіснуючої IP адреси в arp таблиці з мак адресом.





```
Administrator: Windows PowerShell
PS C:\Users\Nikita> arp -s 192.168.1.1 9c-53-22-7f-6e-e7
PS C:\Users\Nikita>
```

Рисунок 2.5 – порівняння неіснуючої IP адреси в arp таблиці з мак адресом.

Порівняння IP-адреси з мак адресою можна побачити на рис 2.4 та 2.5. На рисунку 2.4 дані, які дали по завданню, а в 2.5 дані взяті з arp таблиці. Як можна побачити, в обох випадках результат виконання чомусь пустий.

## ЗАВДАННЯ 3

### Опис завдання:

- Для відображення статистики Ethernet та статистики по всіх протоколах введіть наступну команду: `netstat -e -s`;
- Для відображення статистики лише за протоколами TCP і UDP введіть наступні команди: `netstat -s -p tcp`, або `netstat -s -p udp`;
- Для відображення активних підключень TCP та кодів процесів з використанням числового формату введіть наступну команду: `netstat -n -o`.

### Виконання:

На рисунку 3.1 зображена статистика Ethernet та статистики по всіх протоколах, використовуючи команду `netstat -e -s`.

На рисунку 3.2 зображені статистики TCP та UDP, використовуючи команди : `netstat -s -p tcp`, та `netstat -s -p udp`.

На рисунку 3.3 зображено відображення активних підключень TCP та усі коди процесів., використовуючи команду `netstat -n -o`.

PS C:\Users\Nikita> netstat -e -s			Address Masks			0	0
Interface Statistics			Address Mask Replies			0	0
	Received	Sent	Router Solicitations			0	0
Bytes	2823356448	162509970	Router Advertisements			0	0
Unicast packets	2564320	834912	ICMPv6 Statistics				
Non-unicast packets	75128	23496		Received	Sent		
Discards	0	0	Messages	0	45		
Errors	0	0	Errors	0	0		
Unknown protocols	0		Destination Unreachable	0	0		
IPv4 Statistics			Packet Too Big	0	0		
			Time Exceeded	0	0		
Packets Received	= 313444		Parameter Problems	0	0		
Received Header Errors	= 16		Echos	0	0		
Received Address Errors	= 228		Echo Replies	0	0		
Datagrams Forwarded	= 0		MLD Queries	0	0		
Unknown Protocols Received	= 0		MLD Reports	0	0		
Received Packets Discarded	= 4692		MLD Dones	0	0		
Received Packets Delivered	= 333825		Router Solicitations	0	27		
Output Requests	= 131079		Router Advertisements	0	0		
Routing Discards	= 0		Neighbor Solicitations	0	9		
Discarded Output Packets	= 0		Neighbor Advertisements	0	9		
Output Packet No Route	= 29		Redirects	0	0		
Reassembly Required	= 0		Router Renumberings	0	0		
Reassembly Successful	= 0		TCP Statistics for IPv4				
Reassembly Failures	= 0		Active Opens	= 6724			
Datagrams Successfully Fragmented	= 0		Passive Opens	= 32			
Datagrams Failing Fragmentation	= 0		Failed Connection Attempts	= 3878			
Fragments Created	= 0		Reset Connections	= 239			
IPv6 Statistics			Current Connections	= 20			
			Segments Received	= 74818			
Packets Received	= 39		Segments Sent	= 59884			
Received Header Errors	= 0		Segments Retransmitted	= 15454			
Received Address Errors	= 30		TCP Statistics for IPv6				
Datagrams Forwarded	= 0		Active Opens	= 19			
Unknown Protocols Received	= 0		Passive Opens	= 1			
Received Packets Discarded	= 0		Failed Connection Attempts	= 18			
Received Packets Delivered	= 1204		Reset Connections	= 2			
Output Requests	= 1771		Current Connections	= 0			
Routing Discards	= 0		Segments Received	= 339			
Discarded Output Packets	= 0		Segments Sent	= 327			
Output Packet No Route	= 0		Segments Retransmitted	= 12			
Reassembly Required	= 0		UDP Statistics for IPv4				
Reassembly Successful	= 0		Datagrams Received	= 278855			
Reassembly Failures	= 0		No Ports	= 3152			
Datagrams Successfully Fragmented	= 0		Receive Errors	= 0			
Datagrams Failing Fragmentation	= 0		Datagrams Sent	= 75643			
Fragments Created	= 0		UDP Statistics for IPv6				
ICMPv4 Statistics			Datagrams Received	= 1367			
	Received	Sent	No Ports	= 0			
Messages	412	440	Receive Errors	= 0			
Errors	0	0	Datagrams Sent	= 1268			
Destination Unreachable	411	439	PS C:\Users\Nikita>				
Time Exceeded	0	0					
Parameter Problems	0	0					
Source Quenches	0	0					
Redirects	0	0					

Рисунок 3.1 – статистика Ethernet та інших протоколів.

Administrator: Win

PS C:\Users\Nikita> netstat -s -p tcp

TCP Statistics for IPv4

Active Opens = 6822

Passive Opens = 32

Failed Connection Attempts = 3945

Reset Connections = 239

Current Connections = 20

Segments Received = 75747

Segments Sent = 60570

Segments Retransmitted = 15721

Active Connections

Proto Local Address Foreign Address State

TCP 127.0.0.1:4573 DESKTOP-EGAMP25:50268 ESTABLISHED

ABLISHED

TCP 127.0.0.1:9010 DESKTOP-EGAMP25:55670 ESTABLISHED

ABLISHED

TCP 127.0.0.1:9100 DESKTOP-EGAMP25:55674 ESTABLISHED

ABLISHED

TCP 127.0.0.1:50268 DESKTOP-EGAMP25:4573 ESTABLISHED

ABLISHED

TCP 127.0.0.1:50277 DESKTOP-EGAMP25:65001 ESTABLISHED

ABLISHED

TCP 127.0.0.1:50279 DESKTOP-EGAMP25:50903 ESTABLISHED

ABLISHED

TCP 127.0.0.1:50903 DESKTOP-EGAMP25:50279 ESTABLISHED

ABLISHED

TCP 127.0.0.1:55670 DESKTOP-EGAMP25:9010 ESTABLISHED

ABLISHED

TCP 127.0.0.1:55674 DESKTOP-EGAMP25:9100 ESTABLISHED

ABLISHED

TCP 127.0.0.1:65001 DESKTOP-EGAMP25:50277 ESTABLISHED

ABLISHED

TCP 192.168.1.108:49409 20.199.120.85:https ESTABLISHED

ABLISHED

TCP 192.168.1.108:55563 149.154.167.41:https ESTABLISHED

ABLISHED

Administrator: Win

PS C:\Users\Nikita> netstat -s -p udp

UDP Statistics for IPv4

Datagrams Received = 285593

No Ports = 3253

Receive Errors = 0

Datagrams Sent = 77418

Active Connections

Proto Local Address Foreign Address State

PS C:\Users\Nikita> |

Рисунок 3.2 – статистика TCP та UDP.

Administrator: Windows Powe

PS C:\Users\Nikita> netstat -n -o

Active Connections

Proto Local Address Foreign Address State PID

TCP 127.0.0.1:4573 127.0.0.1:50268 ESTABLISHED 5428

TCP 127.0.0.1:9010 127.0.0.1:55670 ESTABLISHED 13384

TCP 127.0.0.1:9100 127.0.0.1:55674 ESTABLISHED 5400

TCP 127.0.0.1:50268 127.0.0.1:4573 ESTABLISHED 9624

TCP 127.0.0.1:50277 127.0.0.1:65001 ESTABLISHED 5636

TCP 127.0.0.1:50279 127.0.0.1:50903 ESTABLISHED 9188

TCP 127.0.0.1:50903 127.0.0.1:50279 ESTABLISHED 15432

TCP 127.0.0.1:55670 127.0.0.1:9010 ESTABLISHED 10880

TCP 127.0.0.1:55674 127.0.0.1:9100 ESTABLISHED 13384

TCP 127.0.0.1:65001 127.0.0.1:50277 ESTABLISHED 5636

TCP 192.168.1.108:49409 20.199.120.85:443 ESTABLISHED 6132

TCP 192.168.1.108:55563 149.154.167.41:443 ESTABLISHED 3844

TCP 192.168.1.108:55566 149.154.167.41:443 ESTABLISHED 3844

TCP 192.168.1.108:58777 140.82.114.26:443 ESTABLISHED 4392

TCP 192.168.1.108:58809 23.64.12.59:443 CLOSE\_WAIT 9900

TCP 192.168.1.108:58810 23.64.12.59:443 CLOSE\_WAIT 9900

TCP 192.168.1.108:58811 23.64.12.59:443 CLOSE\_WAIT 9900

TCP 192.168.1.108:58813 23.64.12.59:443 CLOSE\_WAIT 9900

TCP 192.168.1.108:58822 152.199.21.118:443 CLOSE\_WAIT 9900

TCP 192.168.1.108:59033 23.45.138.32:80 TIME\_WAIT 0

TCP 192.168.1.108:59035 23.192.94.59:80 TIME\_WAIT 0

TCP 192.168.1.108:59036 209.197.3.8:80 TIME\_WAIT 0

TCP 192.168.1.108:59066 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59067 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59072 52.109.32.7:443 TIME\_WAIT 0

TCP 192.168.1.108:59073 52.109.32.7:443 TIME\_WAIT 0

TCP 192.168.1.108:59075 38.106.231.204:443 TIME\_WAIT 0

TCP 192.168.1.108:59081 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59082 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59090 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59091 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59098 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59099 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59103 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59104 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59105 192.168.1.1:53 TIME\_WAIT 0

TCP 192.168.1.108:59106 192.168.1.1:53 TIME\_WAIT 0

PS C:\Users\Nikita> |

Рисунок 3.3 – активні підключення TCP.

## ЗАВДАННЯ 4

### Опис завдання:

- Дізнайтеся ір-адреси вузлів: facebook.com, youtube.com, ukr.net;
- Отримайте DNS-інформацію за допомогою команди nslookup -type=ns google.com, дізнайтесь назви серверів та дізнайтесь їх адресу.

### Виконання:

На рисунках 4.1 – 4.3 можна побачити результат виконання команди nslookup. У перших двох строках виводу можна побачити інформацію про маршрутизатор, а вже знизу домене ім'я та IP-адреса серверу (IPv4 та IPv6). Інформація про сервера зображена на табл 4.1.

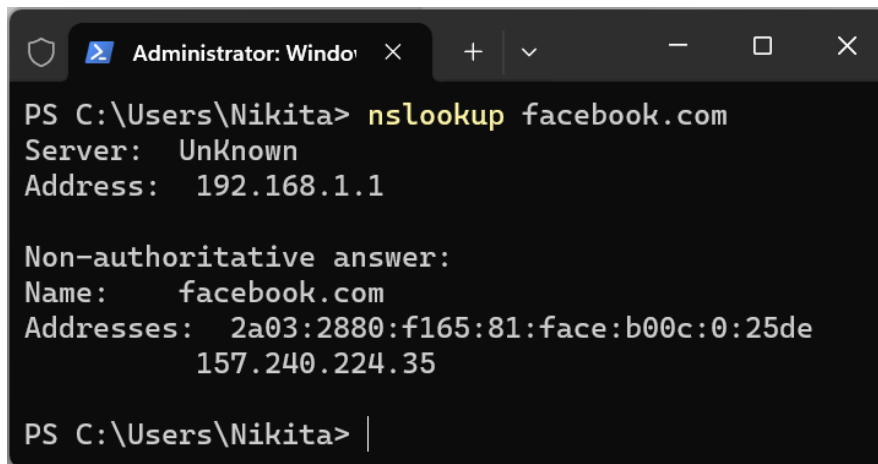
Домен	IPv4	IPv6
facebook.com	157.240.224.35	2a03:2880:f165:81:face:b00c:0:25de
youtube.com	216.58.209.14	2a00:1450:401b:808:200e
ukr.net	104.18.9.128	-

Таблиця 4.1 – IP-адреси серверів.

Далі треба дізнатися IP-адресу серверів google.com. Для цього ми використовуємо команду nslookup -type=ns google.com. Ми отримуємо 4 сервери з іменами ns4.google.com, ns3.google.com, ns2.google.com, ns1.google.com (рис 4.4). Тепер, знаючи цю інформацію ми можемо дізнатись їх IP-адреси. Сам процес зображений на рис 4.5 – 4.8, а скомпанований вивод можна побачити на табл 4.2.

Домен	IPv4	IPv6
ns4.google.com	216.239.38.10	2001:4860:4802:38::a
ns3.google.com	216.239.36.10	2001:4860:4802:36::a
ns2.google.com	216.239.34.10	2001:4860:4802:34::a
ns1.google.com	216.239.32.10	2001:4860:4802:32::a

Таблиця 4.2 – IP-адреси серверів google.com

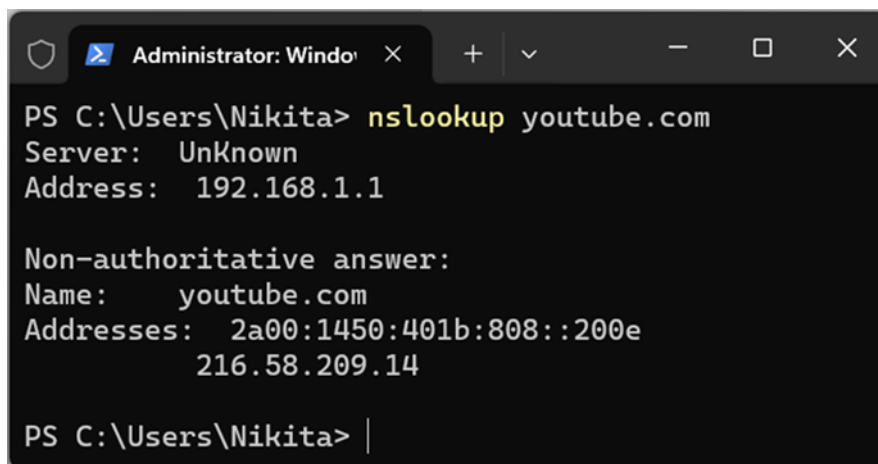


```
Administrator: Windows Command Prompt
PS C:\Users\Nikita> nslookup facebook.com
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: facebook.com
Addresses: 2a03:2880:f165:81:face:b00c:0:25de
          157.240.224.35

PS C:\Users\Nikita> |
```

Рисунок 4.1 – виконання команди nslookup facebook.com.

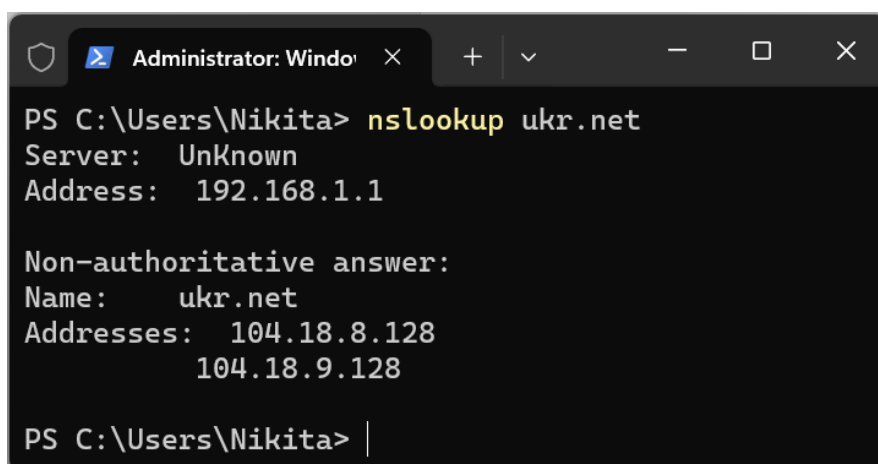


```
Administrator: Windows Command Prompt
PS C:\Users\Nikita> nslookup youtube.com
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: youtube.com
Addresses: 2a00:1450:401b:808::200e
          216.58.209.14

PS C:\Users\Nikita> |
```

Рисунок 4.2 – виконання команди nslookup youtube.com.

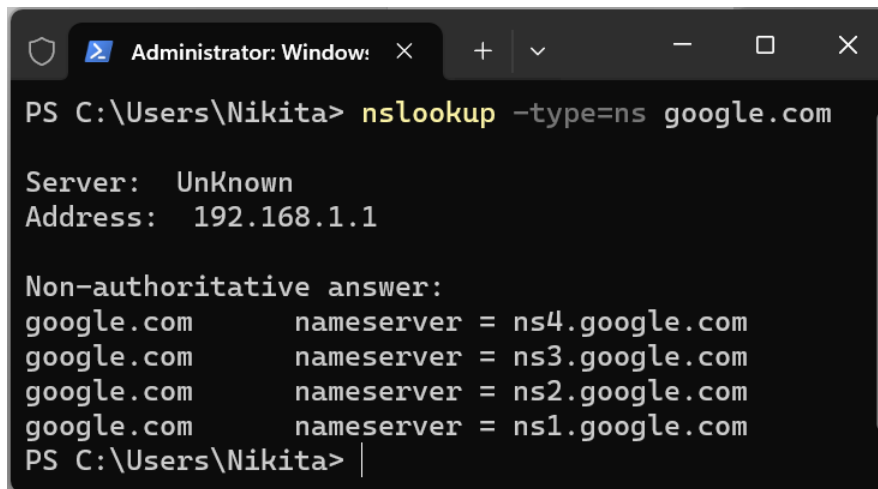


```
Administrator: Windows Command Prompt
PS C:\Users\Nikita> nslookup ukr.net
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: ukr.net
Addresses: 104.18.8.128
          104.18.9.128

PS C:\Users\Nikita> |
```

Рисунок 4.3 – виконання команди nslookup ukr.net.

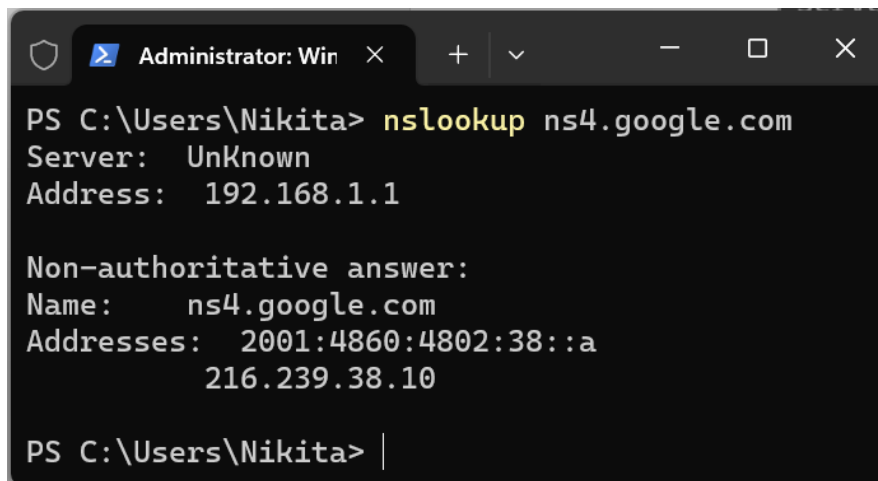


```
PS C:\Users\Nikita> nslookup -type=ns google.com

Server:      UnKnown
Address:     192.168.1.1

Non-authoritative answer:
google.com   nameserver = ns4.google.com
google.com   nameserver = ns3.google.com
google.com   nameserver = ns2.google.com
google.com   nameserver = ns1.google.com
PS C:\Users\Nikita> |
```

Рисунок 4.4 – виконання команди nslookup -type=ns google.com.

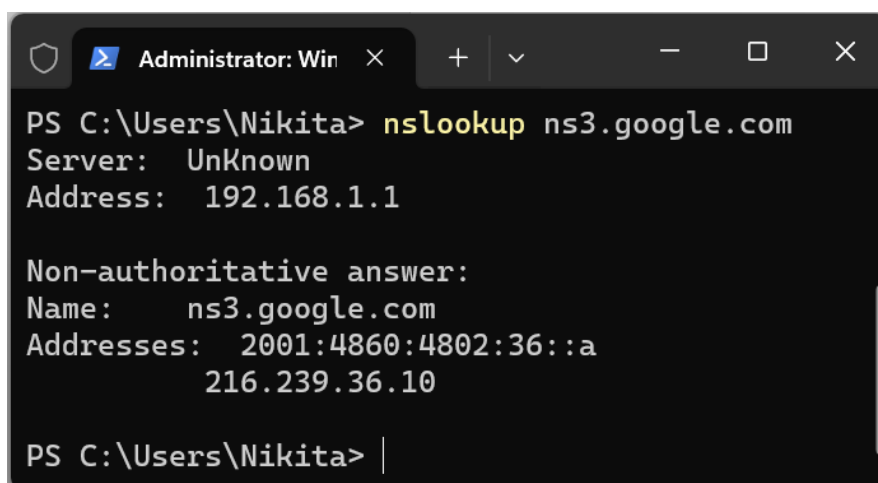


```
PS C:\Users\Nikita> nslookup ns4.google.com
Server:      UnKnown
Address:     192.168.1.1

Non-authoritative answer:
Name:        ns4.google.com
Addresses:   2001:4860:4802:38::a
             216.239.38.10

PS C:\Users\Nikita> |
```

Рисунок 4.5 – виконання команди nslookup ns4.google.com

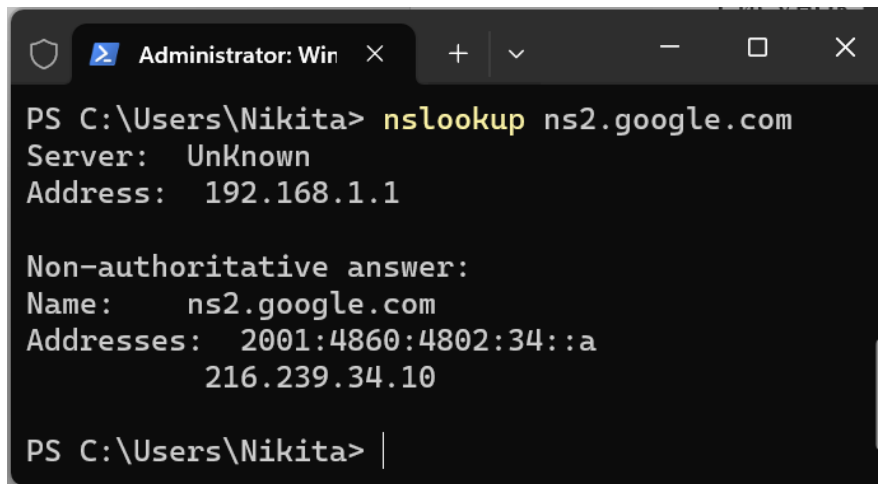


```
PS C:\Users\Nikita> nslookup ns3.google.com
Server:      UnKnown
Address:     192.168.1.1

Non-authoritative answer:
Name:        ns3.google.com
Addresses:   2001:4860:4802:36::a
             216.239.36.10

PS C:\Users\Nikita> |
```

Рисунок 4.6 – виконання команди nslookup ns3.google.com

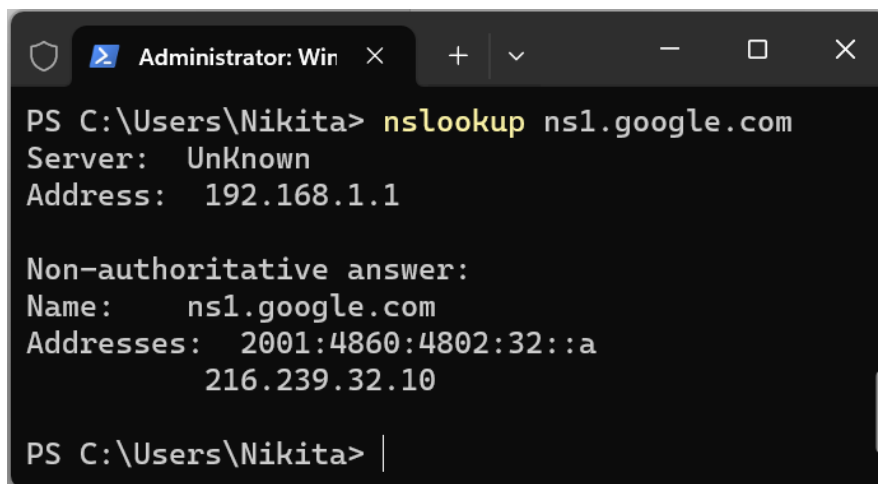


```
PS C:\Users\Nikita> nslookup ns2.google.com
Server:      UnKnown
Address:     192.168.1.1

Non-authoritative answer:
Name:        ns2.google.com
Addresses:   2001:4860:4802:34::a
             216.239.34.10

PS C:\Users\Nikita> |
```

Рисунок 4.7 – виконання команди nslookup ns2.google.com



```
PS C:\Users\Nikita> nslookup ns1.google.com
Server:      UnKnown
Address:     192.168.1.1

Non-authoritative answer:
Name:        ns1.google.com
Addresses:   2001:4860:4802:32::a
             216.239.32.10

PS C:\Users\Nikita> |
```

Рисунок 4.8– виконання команди nslookup ns1.google.com

## ВИСНОВОК

Виконуючи цю лабораторну роботу, я навчався важливим навичкам у сфері мережних команд та їх застосуванню для тестування різних типів комп'ютерних мереж. Ці навички дозволяють мені здобути розширене розуміння функціонування мереж, підвищити ефективність діагностики мережових проблем, та готують до подальшого професійного розвитку в сфері інформаційних технологій.