

# Лабораторна робота № 1

## Діагностичні утиліти стеку протоколів TCP/IP

1. Підготовка до роботи.

1.1. Переглянути основні теоретичні відомості з протоколів: IP, TCP, UDP, ICMP, ARP, їх призначення та заголовки.

1.2. Переглянути довідку та приклади використання діагностичних утиліт.

1.2.1. ping

1.2.2. traceroute

1.2.3. nslookup

1.2.4. dig

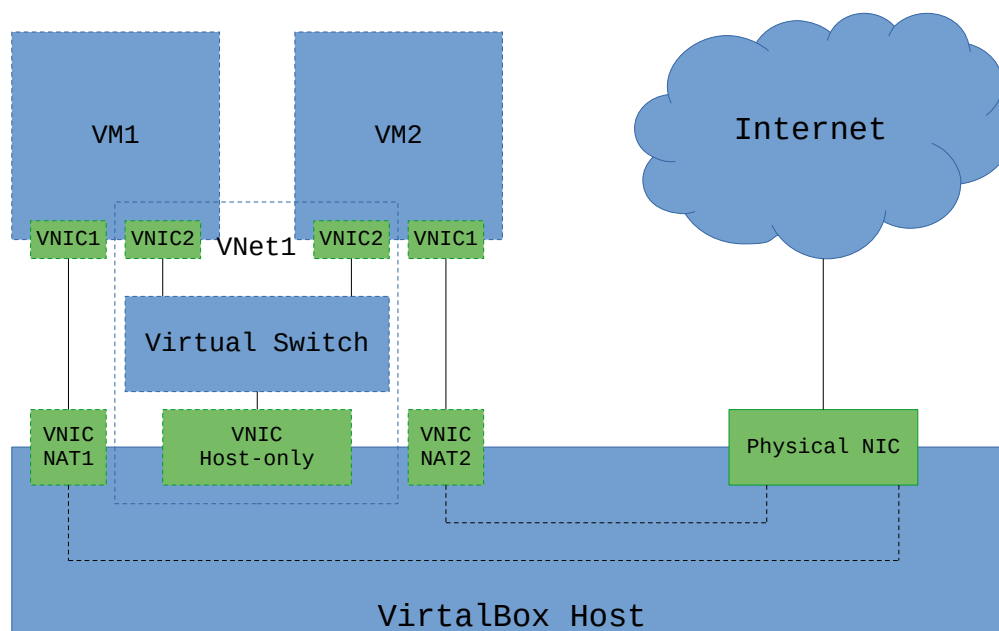
1.2.5. netstat

1.3. Переглянути приклади використання telnet та nc для роботи з текстовими протоколами.

1.4. Переглянути довідку та приклади використання утиліти tcpdump для перехоплення мережного трафіку.

2. Завдання на роботу.

Створити віртуальну лабораторію, схема якої наведена на малюнку 1.



Малюнок .1

2.1. Встановити систему віртуалізації VirtualBox, завантаживши дистрибутив з <https://www.virtualbox.org/wiki/Downloads>.

2.1.1. Створити віртуальну мережу VNet1 (“Host-only Network”) та вимкнути для неї вбудований сервіс DHCP.

2.1.2. Виконати конфігурацію віртуального мережного інтерфейсу хост-системи у відповідності до варіанту.

2.1.3. За необхідності додати правило в фаєрвол хост-системи, що дозволяє будь-який трафік із створеної віртуальної мережі.

2.2. Створити віртуальну машину VM1 з операційною системою Debian.

2.2.1. Виконати встановлення операційної системи Debian, завантаживши iso-образ з <https://www.debian.org/download>.

2.2.2. За необхідності встановити пакети tcpdump та net-tools.

2.2.3. Додати другий мережний адаптер VNIC2 до віртуальної машини, встановити тип підключення “Host-only Adapter” та під'єднати його до віртуальної мережі VNet1.

2.2.4. Виконати конфігурацію VNIC2 у відповідності до варіанту (має бути встановлена статична IP-адреса).

2.3. Створити віртуальну машину VM2 з операційною системою Debian.

2.3.1. Створити клон віртуальної машини VM1.

2.3.2. Виконати конфігурацію другого мережного інтерфейсу VNIC2 у відповідності до варіанту (має бути встановлена статична IP-адреса).

2.4. На віртуальній машині VM2 виконати наступні дії.

2.4.1. Встановити додаткову IP-адресу на інтерфейсі VNIC2 у відповідності до варіанту.

2.5. На віртуальній машині VM1 виконати наступні дії.

2.5.1. Встановити додаткову IP-адресу на інтерфейсі VNIC2 у відповідності до варіанту.

2.5.2. Змінити значення MTU на інтерфейсі VNIC2 у відповідності до варіанту (Таблиця 2).

2.5.3. Використовуючи утиліту ping, перевірити доступність хост-системи та віртуальної машини VM2. При цьому кількість пакетів, що відправляються, повинна дорівнювати номеру варіанту, а розмір пакетів – подвоєному значенню MTU.

2.5.4. Встановити значення MTU на інтерфейсі VNIC2 в 1500.

2.5.5. Вивести таблицю ARP.

2.5.6. Додати MAC-адресу в таблицю ARP для IP-адреси хост-системи у відповідності до варіанту (Таблиця 2).

2.5.7. Перевірити доступність хост-системи.

2.5.8. Видалити із таблиці ARP запис, створений у п. 2.5.6.

2.5.9. Перевірити доступність хост-системи.

2.5.10. Вивести таблицю маршрутизації.

2.5.11. Перевірити доступність додаткової IP-адреси VNIC2 віртуальної машини VM2.

2.5.12. Додати запис до таблиці маршрутизації до мережі, якій належить додаткова IP-адреса VNIC2 віртуальної машини VM2.

2.5.13. Перевірити доступність додаткової IP-адреси VNIC2 віртуальної машини VM2.

2.5.14. Визначити IP-адресу вузла comsys.kpi.ua.

2.5.15. За допомогою утиліти traceroute (з використанням протоколу ICMP) визначити проміжні маршрутизатори на шляху до вузла 8.8.8.8.

2.5.16. За допомогою утиліти netstat вивести статистику роботи протоколів TCP, UDP, ICMP, IP.

2.5.17. Згідно варіанту (Таблиця 3) налаштувати фільтр для утиліти tcpdump для виведення необхідного трафіку на екран. Для перевірки роботи фільтру необхідно використовувати засоби генерації трафіку для відповідних протоколів.

### 3. Варіанти завдання.

X — номер варіанту від 1 до 15.

Таблиця 1.

IP-адреса віртуальної мережі	192.168.(100+X).0/24
IP-адреса хост-системи	192.168.(100+X).1/24
Основна IP-адреса VNIC2 віртуальної машини VM1	192.168.(100+X).10/24
Додаткова IP-адреса VNIC2 віртуальної машини VM1	172.17.(100+X).10/24
Основна IP-адреса VNIC2 віртуальної машини VM2	192.168.(100+X).20/24
Додаткова IP-адреса VNIC2 віртуальної машини VM2	172.17.(200+X).20/24

Таблиця 2.

Варіант	MAC-адреса	MTU
1	00:11:22:33:44:55	1000
2	00:11:00:11:00:11	900
3	00:11:22:11:22:11	850
4	00:55:44:33:22:11	1100
5	00:11:11:11:22:22	750
6	00:66:77:88:99:AA	650
7	00:AA:99:88:77:66	1050
8	00:55:00:55:00:55	1200
9	00:99:11:99:11:99	950
10	00:33:44:55:66:77	800
11	00:88:77:66:55:44	1150
12	00:12:34:56:78:9A	600
13	00:A9:87:65:43:21	1250
14	00:01:10:01:10:01	700
15	00:01:23:44:32:10	950

Таблиця 3.

Варіант	Вхідний трафік	Вихідний трафік
1	ICMP, TCP з 21 порту з мережі VNet1	UDP на 53 порт
2	Широкомовний трафік, UDP з 53 порту	TCP на 22 порт до вузла VM2
3	ARP, UDP, з вузла VM2	ICMP, TCP в мережу VNet1
4	TCP з мережі VNet1, ICMP echo reply	ARP, UDP
5	TCP syn, UDP з мережі VNet1	ICMP в мережу VNet1
6	TCP з 22 порту з вузла VM2, ICMP	TCP на 22 порт, TCP на 80
7	UDP, з вузла VM2	ARP, ICMP до вузла VM2
8	TCP з 80 порту, ICMP з вузла VM2	TCP, UDP до вузла VM2
9	ICMP, TCP з 25 порту з мережі VNet1	ARP, ICMP до вузла VM2
10	ARP, UDP, з вузла VM2	ICMP в мережу VNet1
11	TCP, UDP з мережі VNet1	ICMP, TCP в мережу VNet1
12	UDP, з вузла VM2	TCP на 21 порт до вузла VM2
13	TCP з 21 порту з вузла VM2, ICMP	UDP на 53 порт
14	TCP з мережі VNet1, ICMP echo reply	ARP, UDP
15	Широкомовний трафік, UDP з 53 порту	TCP на 21 порт, TCP на 22

#### 4. Контрольні запитання.

- 4.1. Як можна визначити номер порту, який використовує мережний сервіс?
- 4.2. Що означає promiscuous mode мережного інтерфейсу?
- 4.3. Яким чином утиліта traceroute визначає маршрут просування пакету?
- 4.4. Які функції виконує утиліта ping?
- 4.5. Рівні стека протоколів TCP/IP і їх функції.
- 4.6. З якою метою може використовуватися утиліта tcpdump?

#### 5. Література.

RFC768 <https://tools.ietf.org/html/rfc768>  
 RFC791 <https://tools.ietf.org/html/rfc791>  
 RFC792 <https://tools.ietf.org/html/rfc792>  
 RFC793 <https://tools.ietf.org/html/rfc793>  
 RFC826 <https://tools.ietf.org/html/rfc826>