

DigiJED - 2

Звіт  
з лабораторної роботи № 2  
з курсу “ICT Security”

Виконав:  
Ніживенко А. Д.  
Варіант № 9

Харків  
2023

## Тема: “Захист локальних мереж”

**Мета:** Набуття практичних навичок щодо захисту локальних мереж.

**Вихідні дані:**

### Перша мережа (first net):

2 комутатори з'єднані між собою (Switch 0, Switch 1), сервер під'єднаний до комутатора Switch 0 (Server 0), 2 комп'ютери під'єднані до Switch 1 (PC 0, PC 1), 2 точки доступу (Access Point 1, Access Point 2) під'єднані до Switch 0, 4 ноутбуки під'єднані до Access Point 1 (Laptop 0, Laptop 1, Laptop 2, Laptop 3), 2 ноутбуки під'єднані до Access Point 2 (Laptop 4, Laptop 5), маршрутизатор під'єднаний до Switch 0 (Router 1).

### Друга мережа (second net):

комутатор (Switch 2), 3 комп'ютери під'єднані до Switch 2 (PC 2, PC 3, PC 4), сервер під'єднаний до Switch 2 (Server 1), маршрутизатор під'єднаний до Switch 2 (Router 2).

### Третя мережа (third net):

2 роутери з'єднані між собою (Router 1, Router 2).

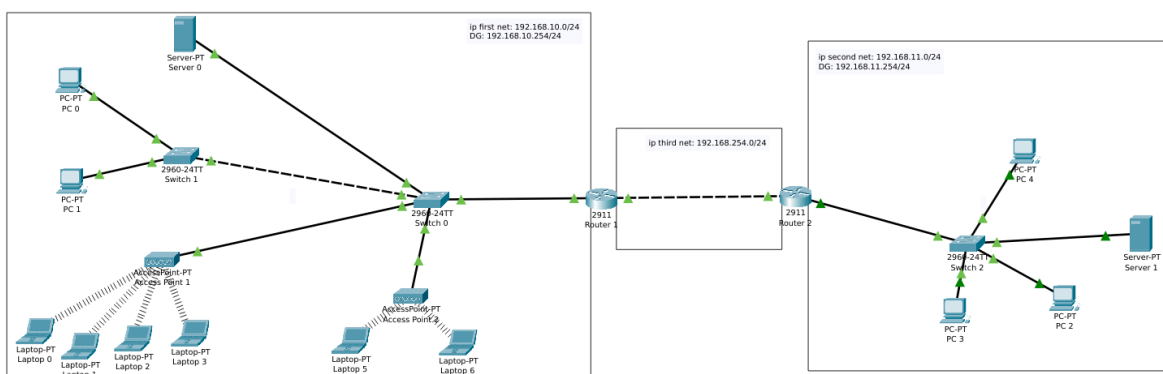


Рис. 1. Вихідні дані мережі

## Хід роботи

**Пункт 1.** Дослідження засобів захисту CAM-таблиць на комутаторі мережі.

1) Для захисту CAM-таблиць на комутаторі Switch 0 використано функціонал захисту порту (Port Security), для порту FastEthernet 0/1, який з'єднує Switch 0 з Access Point 1.

Використовуючи функціонал захисту порту (Port Security), було обмежено максимальну кількість підключених кінцевих пристроїв до порту FastEthernet 0/1. Максимальна кількість підключених кінцевих пристроїв становить 4 (рис. 2).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security maximum 4
Switch(config-if)#switchport port-security
Switch(config-if)#
```

Рис. 2. Налаштування захисту порту на комутаторі Switch 0

Результат налаштування перевірено командою *show port-security* (рис. 3).

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/1      4              4              0      Shutdown
-----
```

Рис. 3. Перевірка налаштування захисту порту на комутаторі Switch 0

2) Змодельовано перший можливий варіант порушення рівня безпеки локальної мережі: до Access Point 1 під'єднано новий нелегітимний пристрій (Laptop Enemy) (рис. 4).

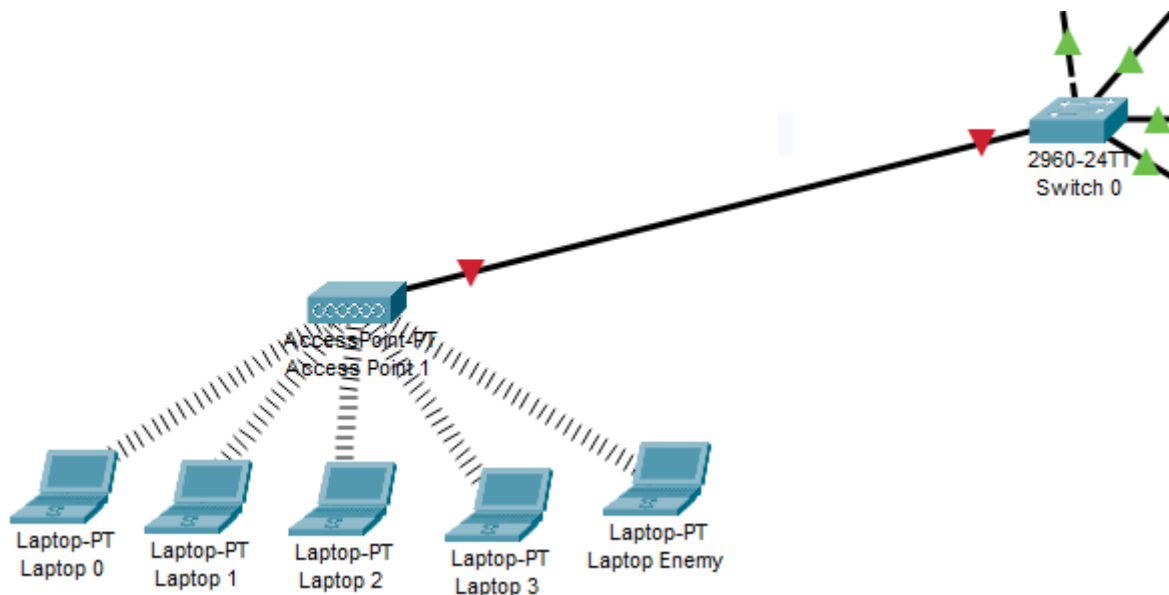


Рис. 4. Новий пристрій під'єднаний до Access Point 1

Проаналізовано стан каналу, який з'єднує комутатор Switch 0 та точку доступу Access Point 1 (рис. 5).

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

а) Службове повідомлення в CLI

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/1      4                0                1      Shutdown
-----
```

б) Перевірка за допомогою команди *show port-security*

Рис. 5. Перевірка стану каналу після моделювання першого випадку порушення безпеки

Канал, який з'єднує комутатор Switch 0 та точку доступу Access Point 1, відключений за допомогою функціоналу захисту порту (Port Security).

Комутатор отримав інформацію про те, що було підключено новий кінцевий пристрій до Access Point 1, це означає, що до Access Point 1 підключено 5 пристроїв, що перевищує

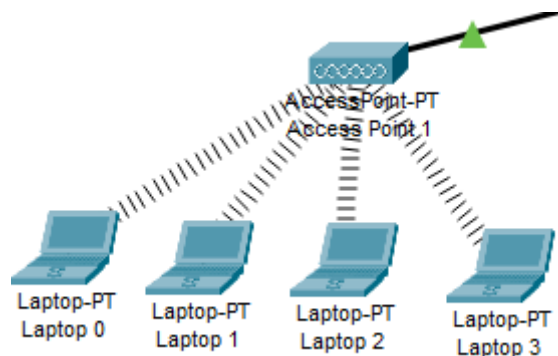
максимальну кількість пристроїв, які можуть бути підключені до комутатора Switch 0 згідно з конфігурацією заданої в пункті 1. Це розглядається як порушення політики безпеки, внаслідок чого комутатор вимикає порт FastEthernet 0/1, який з'єднує Switch 0 з Access Point 1.

3) Повернено попередній стан мережі, видаливши Laptop Enemy і змінивши стан порту FastEthernet 0/1 на комутаторі Switch 0 на активний (рис. 6). Також було перевірено стан захисту порту (Port Security) на порті FastEthernet 0/1 (рис. 7).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
Switch(config-if)#no shutdown
```

а) Увімкнення порту FastEthernet 0/1



б) Результат повернення мережі до попереднього стану

Рис. 6. Повернення попереднього стану мережі

```
show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	4	4	0	Shutdown

Рис. 7. Перевірка стану захисту порту на Switch 0

4) Змодельовано другий можливий варіант порушення рівня безпеки локальної мережі: на пристрої Laptop 0 було змінено MAC-адресу (рис. 8).

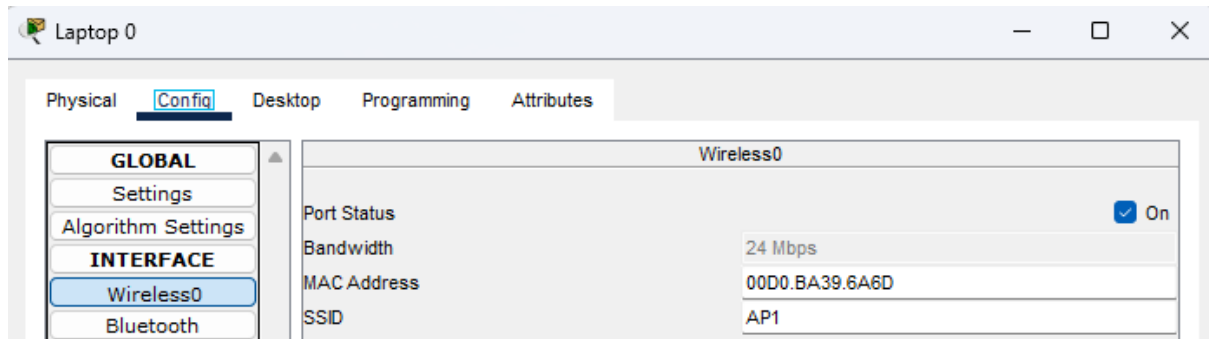
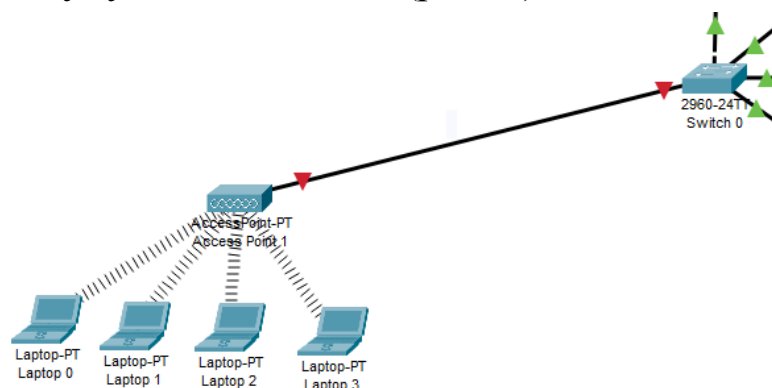


Рис. 8. Змінення MAC-адреси Laptop 0

Проаналізовано стан каналу, який з'єднує комутатор Switch 0 та точку доступу Access Point 1 (рис. 9).



а) Стан каналу з'єднання

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

б) Службове повідомлення в CLI комутатора Switch 0

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/1      4              0              1      Shutdown
-----
```

в) Перевірка за допомогою команди *show port-security*

Рис. 9. Перевірка стану каналу після моделювання другого випадку порушення безпеки

Канал, який з'єднує комутатор Switch 0 та точку доступу Access Point 1, відключений за допомогою функціоналу захисту порту (Port Security).

Комутатор отримав інформацію про, те що до мережі підключено пристрій з новою MAC-адресою, комутатор вважає цю MAC-адресу сторонньою, тому що ця MAC-адреса не відповідає жодній з допущених MAC-адрес для цього порту. Це розглядається як порушення політики безпеки, внаслідок чого комутатор вимикає порт FastEthernet 0/1, який з'єднує Switch 0 з Access Point 1.

## Пункт 2. Дослідження засобів захисту сервісу DHCP

1) Додано у налаштування легітимного DHCP-серверу IP-адресу DNS-серверу 8.8.8.8 (рис. 10).

DHCP

Interface	FastEthernet0	Service	<input checked="" type="radio"/> On <input type="radio"/> Off
Pool Name	serverPool		
Default Gateway	192.168.10.254		
DNS Server	8.8.8.8		

Рис. 10. Налаштування легітимного DHCP-серверу

2) Додано у мережу нелегітимний DHCP-сервер (Server Enemy), який підключено до комутатора Switch 1 (рис. 11).

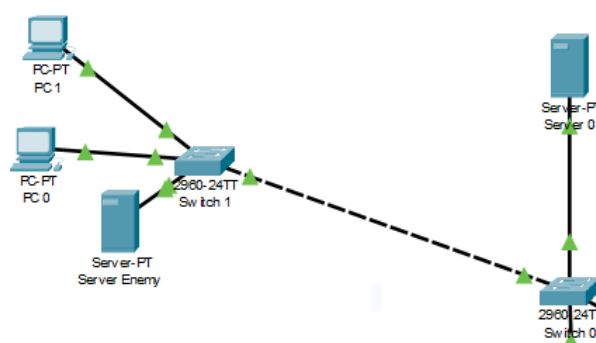


Рис. 11. Новий нелегітимний DHCP-сервер під'єднаний до мережі

Нелегітимний DHCP-сервер (Server Enemy) налаштовано для видачі адреси на нелегітимний DNS 7.7.7.7 (рис. 12).

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.10.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.254

DNS Server: 0.0.0.0

а) Налаштування IP конфігурації

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.10.254

DNS Server: 7.7.7.7

Start IP Address: 192 168 10 100

Subnet Mask: 255 255 255 0

Maximum Number of Users: 10

б) Налаштування сервісу DHCP

Рис. 12. Налаштування нелегітимного DHCP-серверу

3) На пристроях PC 0, PC 1, Laptop 4, Laptop 5 відправлено перезапит (DHCPDISCOVER) на оновлення IP-адрес від DHCP-серверу.

Для PC 0 IP-адресу і маску підмережі було отримано від легітимного сервера (Server 0), а шлюз за замовчуванням і DNS сервер від нелегітимного сервера (Server Enemy) (рис. 13).

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 192.168.10.3

Subnet Mask: 255.255.255.0

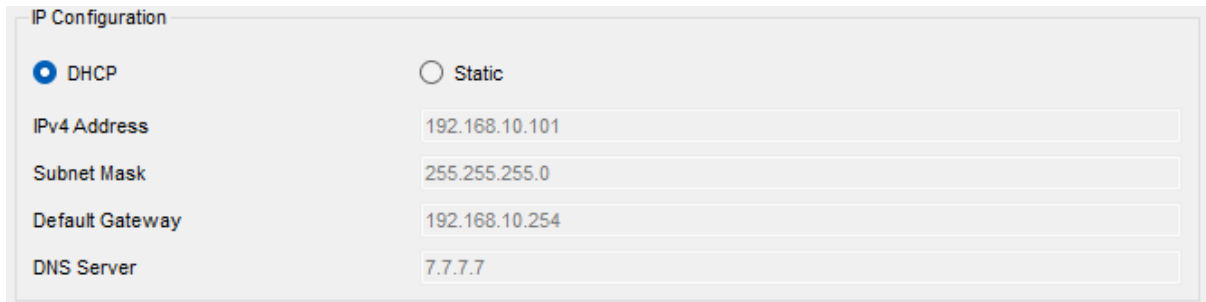
Default Gateway: 192.168.10.254

DNS Server: 7.7.7.7

Рис. 13. Налаштування отримані за допомогою DHCP для PC 0



Для PC 1 вся конфігурація отримана від нелегітимного сервера (Server Enemy) (рис. 14).

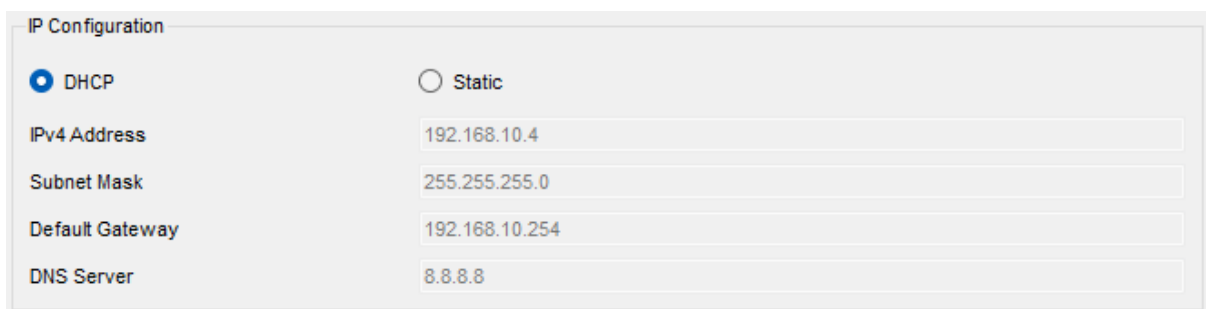


The screenshot shows the 'IP Configuration' window for PC 1. The 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are populated with the following values:

Field	Value
IPv4 Address	192.168.10.101
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.254
DNS Server	7.7.7.7

Рис. 14. Налаштування отримані за допомогою DHCP для PC 1

Для Laptop 4 вся конфігурація отримана від легітимного сервера (Server 0) (рис. 15).

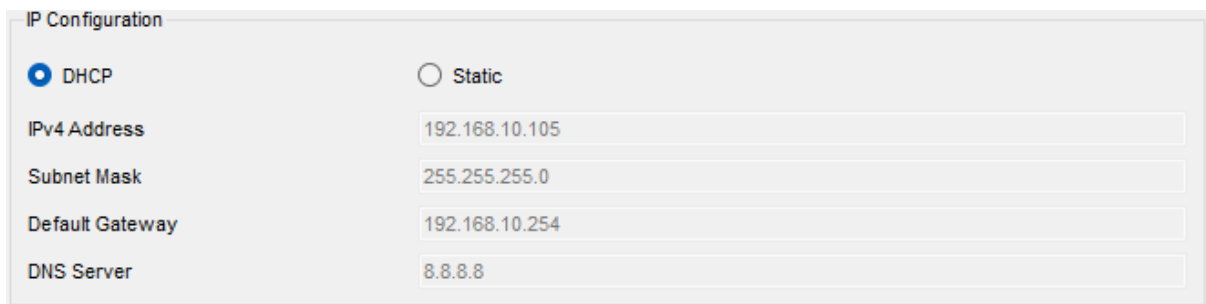


The screenshot shows the 'IP Configuration' window for Laptop 4. The 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are populated with the following values:

Field	Value
IPv4 Address	192.168.10.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.254
DNS Server	8.8.8.8

Рис. 15. Налаштування отримані за допомогою DHCP для Laptop 4

Для Laptop 5 IP-адресу і маску підмережі було отримано від нелегітимного сервера (Server Enemy), а шлюз за замовчуванням і DNS сервер від легітимного сервера (Server 0) (рис. 16).



The screenshot shows the 'IP Configuration' window for Laptop 5. The 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are populated with the following values:

Field	Value
IPv4 Address	192.168.10.105
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.254
DNS Server	8.8.8.8

Рис. 16. Налаштування отримані за допомогою DHCP для Laptop 5

Пристрій отримує налаштування того DHCP-сервера, який відповідь швидше на запит пристрою. Прикладом цього є Laptop 4 і PC 1.

PC 1 знаходиться ближче до Server Enemy, тому отримав всю конфігурацію від цього серверу, в свою чергу Laptop 4 знаходиться ближче до Server 0, тому вся конфігурація отримана з нього.

Також може статися таке, що половину конфігурації пристрій отримує від Server 0, а іншу половину він отримує з Server Enemy, або навпаки. Прикладом цього є Laptop 5 і PC 0. Це стається тому, що сервери надсилають конфігурацію декількома пакетами і пристрої можуть отримувати конфігурацію з різних пакетів, де один пакет відправлений від першого сервера, а другий пакет відправлений від другого сервера.

4) На комутаторах Switch 0 і Switch 1 активовано DHCP Snooping та порти FastEthernet 0/2, FastEthernet 0/3 на Switch 0 та порт FastEthernet 0/3 на Switch 1 налаштовані як довірчі (trust) порти (рис. 17).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#interface range fastEthernet 0/2 - 3
Switch(config-if-range)#ip dhcp snooping trust
```

а) Конфігурація на Switch 0

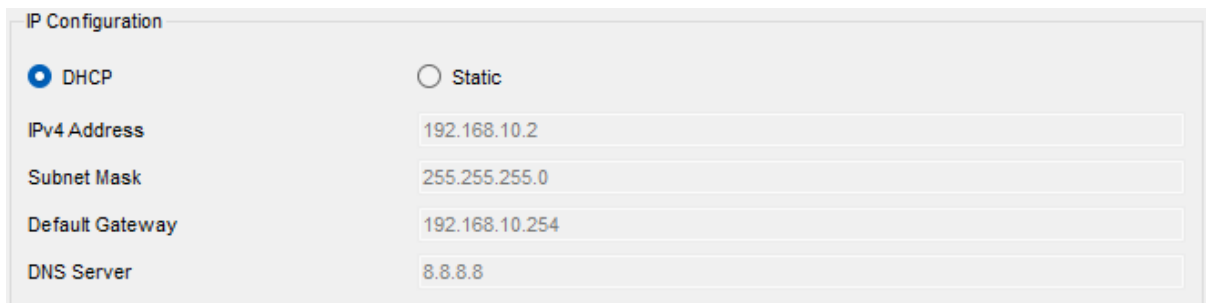
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#ip dhcp snooping trust
```

б) Конфігурація на Switch 1

Рис. 17. Конфігурація DHCP Snooping і довірчих портів на комутаторах

5) Перевірено порядок IP-адресації на кінцевих пристроях, на яких раніше налаштування здійснювалось з нелегітимного DHCP-серверу.

Всі кінцеві пристрої отримали конфігурацію від легітимного сервера (Server 0) (рис. 18).



IP Configuration

☒ DHCP ☐ Static

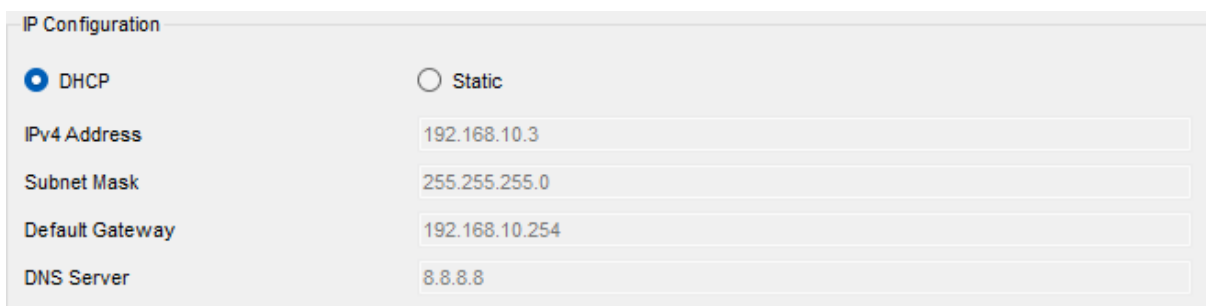
IPv4 Address: 192.168.10.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.254

DNS Server: 8.8.8.8

а) Налаштування на PC 0



IP Configuration

☒ DHCP ☐ Static

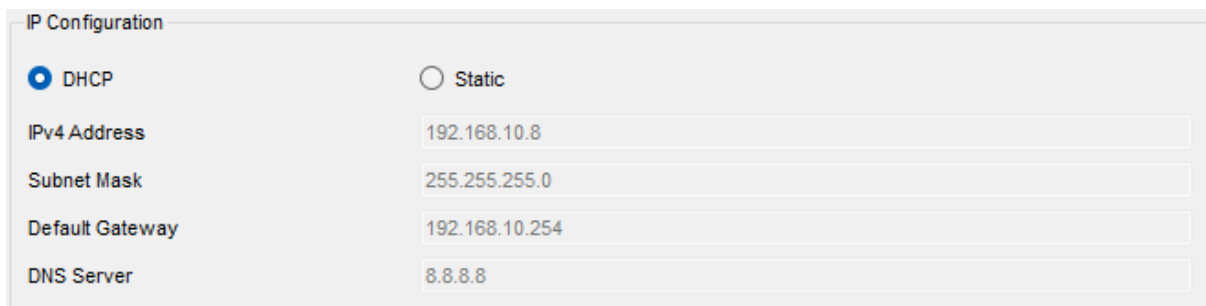
IPv4 Address: 192.168.10.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.254

DNS Server: 8.8.8.8

б) Налаштування на PC 1



IP Configuration

☒ DHCP ☐ Static

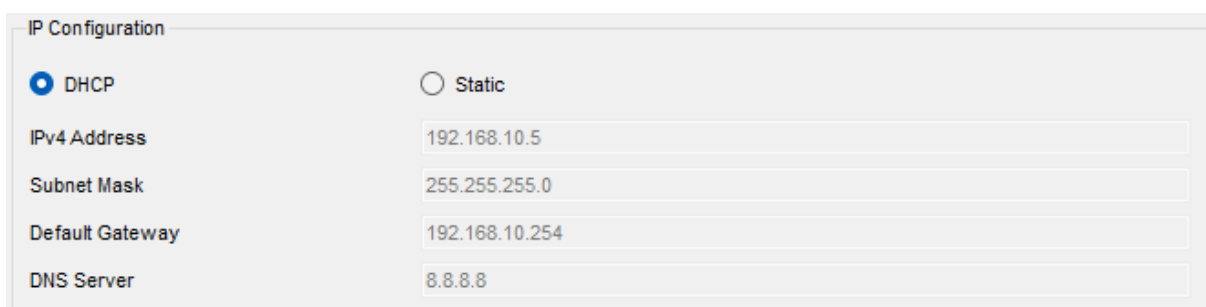
IPv4 Address: 192.168.10.8

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.254

DNS Server: 8.8.8.8

в) Налаштування на Laptop 4



IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 192.168.10.5

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.254

DNS Server: 8.8.8.8

г) Налаштування на Laptop 5

Рис. 18. Налаштування отримані за допомогою DHCP для PC 0, PC 1, Laptop 4, Laptop 5

6) Виконано відключення всіх портів, які не використовуються на Switch 0 та Switch 1 (рис. 19).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/6 - 24, gigabitEthernet 0/1 - 2
Switch(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
```

#### а) Відключення портів на Switch 0

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/5 - 24, gigabitEthernet 0/1 - 2
Switch(config-if-range)#shutdown
```

#### б) Відключення портів на Switch 1

Рис. 19. Відключення всіх портів, які не використовуються на комутаторах

Це було зроблено для запобігання підключення зломисника через ці порти.

7) Встановлено обмеження швидкості на всіх ненадійних портах комутаторів Switch 0 та Switch 1. Швидкість обмеження становить 90 (рис. 20).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1 , fastEthernet 0/4 - 5
Switch(config-if-range)#ip dhcp snooping limit rate 90
```

а) Обмеження швидкості на Switch 0

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1 - 2, fastEthernet 0/4
Switch(config-if-range)#ip dhcp snooping limit rate 90
```

б) Обмеження швидкості на Switch 1

Рис. 20. Встановлення обмеження швидкості на комутаторах  
Це було зроблено для запобігання атак DHCP Flood і Starvation.

8) Перевірено налаштування DHCP Snooping (рис. 21).

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet0/1          no          90
FastEthernet0/2          yes         unlimited
FastEthernet0/3          yes         unlimited
FastEthernet0/4          no          90
FastEthernet0/5          no          90
```

а) Перевірка для Switch 0

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet0/1          no          90
FastEthernet0/3          yes         unlimited
FastEthernet0/2          no          90
FastEthernet0/4          no          90
```

б) Перевірка для Switch 1

Рис. 21. Перевірка налаштування DHCP Snooping на комутаторах

**Висновок:**

У ході виконання лабораторної роботи були вивчені та успішно застосовані інструменти забезпечення безпеки в локальних мережах.

В першому завданні було налаштовано функціонал захисту порту (Port Security) на комутаторі Switch 0. В результаті встановлено обмеження на максимальну кількість підключених пристроїв до певного порту, що дозволяє ефективно контролювати доступ до мережі. Моделювання двох можливих випадків порушення безпеки дозволило перевірити працездатність та ефективність застосованих заходів.

У другому завданні досліджувалося застосування засобів захисту сервісу DHCP. Налаштовано легітимний та нелегітимний DHCP-сервери, а також використано DHCP Snooping для заборони нелегітимних DHCP-серверів у мережі. Встановлено довірчі порти та обмежено швидкість на ненадійних портах комутаторів, що підвищує рівень безпеки мережі.

Загальною метою лабораторної роботи було ознайомлення з основними засобами захисту локальних мереж та навичками їх практичного застосування. Отримані навички дозволять ефективно управляти безпекою мережі та запобігати можливим загрозам.