DigiJED - 2

Звіт
з лабораторної роботи № 3
з курсу “ICT Security”

Виконав:
Ніживенко А. Д.
Варіант № 9

Харків
2023

Тема: “Захист глобальних мереж”

Мета: Набуття практичних навичок щодо захисту глобальних мереж.

Вихідні дані (рис. 1):

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).

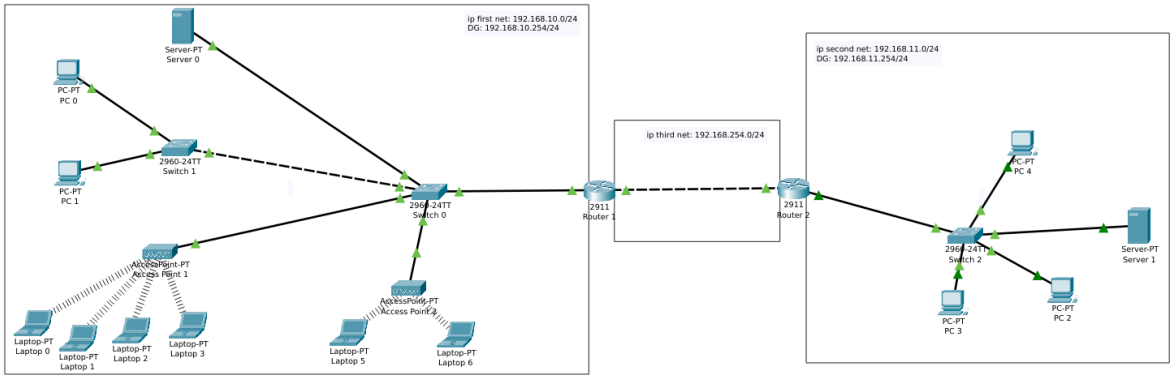

Рис. 1. Вихідні дані мережі

Хід роботи

Пункт 1. Налаштування та перевірка віддаленого безпечного доступу до маршрутизатора за допомогою SSH

1 На маршрутизаторі Router 1 було налаштовано віддалений безпечний доступ за допомогою SSH. Для цього було задане доменне ім’я Domai)n9 і створено RSA ключ довжиною 1024 бітів (ключ довжиною більше 768 бітів є вимогою для SSH другої версії), також увімкнуто другу версію SSH і встановлено ім’я користувача User9 та пароль Pass9 (рис. 2).

```
User Access Verification

Password:

Router9>enable
Password:
Router9#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router9(config)#ip domain name Domain9
Router9(config)#crypto key generate rsa
The name for the keys will be: Router9.Domain9
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router9(config)#ip ssh version 2
*Mar 1 0:42:32.472: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router9(config)#username User9 password Pass9
Router9(config)#line vty 0 15
Router9(config-line)#transport input all
Router9(config-line)#login local
Router9(config-line)#exit
```

Рис. 2. Налаштування віддаленого безпечного доступу до маршрутизатора за допомогою SSH

Налаштування проведені раніше було перевірено за допомогою створення підключення через SSH до Router 1 з пристрою Laptop 5. Під час проведення перевірки встановлено, що доступ до маршрутизатора через SSH захищений і потребує введення пароля для успішного отримання доступу до інтерфейсу командного рядку (рис. 3).

```
C:\>ssh -l User9 192.168.10.254

Password:



Router9>enable
Password:
Router9#show running-config
Building configuration...

Current configuration : 1045 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router9
!
!
!
enable secret 5 $1$mERr$4oCf3EpMOFDvBTFl4xJ0//
!
!
!
!
!
!
ip cef
no ipv6 cef
```

Рис. 3. Перевірка віддаленого безпечного
доступу до маршрутизатора за допомогою SSH.

Пункт 2. Налаштування протоколу маршрутизації RIP

1) На межі першої і третьої мережі додано маршрутизатор Router 3, також в третю мережу додано комутатор Switch 3 через який тепер під'єднані всі маршрутизатори в третій мережі (рис. 4).

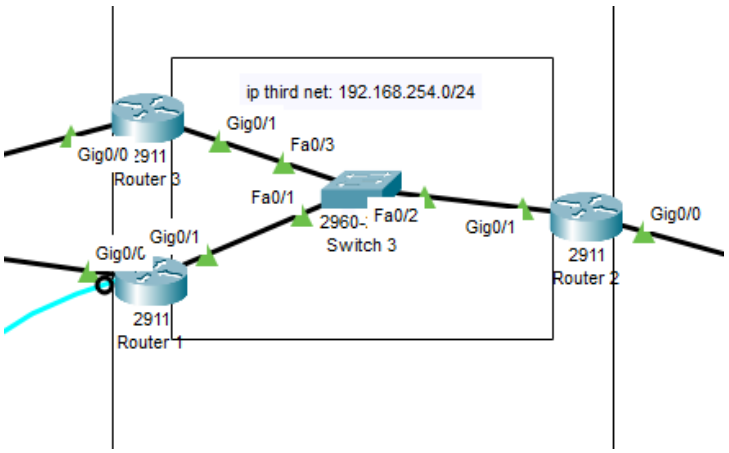

Рис. 4. Новий маршрутизатор і комутатор під'єднані до мережі

2) Всі інтерфейси маршрутизаторів були увімкнуті і встановлено IP адреси, що є коректними для підмереж, до яких вони належать (рис. 5).

```
Router9(config)#interface GigabitEthernet0/0
Router9(config-if)#ip address 192.168.10.253 255.255.255.0
Router9(config-if)#no shutdown
Router9(config-if)#interface GigabitEthernet0/1
Router9(config-if)#ip address 192.168.254.1 255.255.255.0
Router9(config-if)#no shutdown
Router9(config-if)#exit
```

а) Для Router 1

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.11.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.254.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

б) Для Router 2

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.10.252 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.254.3 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

в) Для Router 3

Рис. 5. Встановлення IP адреси для інтерфейсів маршрутизаторів

3) На маршрутизаторах, які використовували статичну маршрутизацію, її було вимкнуто (рис. 6).

```
Router9(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.253/32 is directly connected, GigabitEthernet0/0
S    192.168.11.0/24 [1/0] via 192.168.254.2
     192.168.254.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.254.0/24 is directly connected, GigabitEthernet0/1
L       192.168.254.1/32 is directly connected, GigabitEthernet0/1

Router9(config)#no ip route 192.168.11.0 255.255.255.0
```

а) Для Router 1

```
Router(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.10.0/24 [1/0] via 192.168.254.1
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/0
L       192.168.11.254/32 is directly connected, GigabitEthernet0/0
     192.168.254.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.254.0/24 is directly connected, GigabitEthernet0/1
L       192.168.254.2/32 is directly connected, GigabitEthernet0/1

Router(config)#no ip route 192.168.10.0 255.255.255.0
```

б) Для Router 2

Рис. 6. Вимкнення статичної маршрутизації

4) На маршрутизаторах налаштовано протокол RIPv2 і вказано пасивні інтерфейси, щоб заборонити передачу оновлень маршрутних таблиць через інтерфейс маршрутизатора до пристроїв, які не підтримують протокол RIP (рис. 7).

```
Router9(config)#router rip
Router9(config-router)#version 2
Router9(config-router)#network 192.168.10.0
Router9(config-router)#network 192.168.254.0
Router9(config-router)#passive-interface GigabitEthernet0/0
Router9(config-router)#exit
```

а) Для Router 1

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.11.0
Router(config-router)#network 192.168.254.0
Router(config-router)#passive-interface GigabitEthernet0/0
Router(config-router)#exit
```

б) Для Router 2

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.254.0
Router(config-router)#passive-interface GigabitEthernet0/0
Router(config-router)#exit
```

в) Для Router 3

Рис. 7. Налаштування протоколу RIPv2

5) Перевірено таблиці маршрутизації, побудовані протоколом RIP (рис. 8).

```
Router9#show ip route rip
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.11.0/24 [120/1] via 192.168.254.2, 00:00:02, GigabitEthernet0/1
```

а) Для Router 1

```
Router#show ip route rip
R    192.168.10.0/24 [120/1] via 192.168.254.1, 00:00:10, GigabitEthernet0/1
                     [120/1] via 192.168.254.3, 00:00:04, GigabitEthernet0/1
```

б) Для Router 2

```
Router#show ip route rip
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.11.0/24 [120/1] via 192.168.254.2, 00:00:25, GigabitEthernet0/1
```

в) Для Router 3

Рис. 8. Перевірка таблиць побудованих протоколом RIP

Пункт 3. Налаштування протоколу відмовостійкої маршрутизації HSRP

1) Налаштовано на інтерфейсах маршрутизаторів Router 1 та Router 3 протокол HSRP. Номер standby групи є рівним 9 (рис. 9).

```
Router9(config)#interface GigabitEthernet0/0
Router9(config-if)#standby version 2
Router9(config-if)#standby 9 ip 192.168.10.254
Router9(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 9 state Init -> Init

%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 9 state Speak -> Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 9 state Standby -> Active
```

а) Для Router 1

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#standby version 2
Router(config-if)#standby 9 ip 192.168.10.254
Router(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 9 state Init -> Init

%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 9 state Speak -> Standby
```

б) Для Router 3

Рис. 9. Налаштування протоколу HSRP

2) На інтерфейсах першої підмережі маршрутизаторів Router 1 та Router 3 встановлено пріоритети: для маршрутизатора Router 1 пріоритет становить 17, а для маршрутизатора Router 3 пріоритет становить 19. Також на кожному з інтерфейсів обох маршрутизаторів увімкнено режим preempt (рис. 10).

```
Router9(config-if)#standby 9 priority 17
Router9(config-if)#standby 9 preempt
```

а) Для Router 1

```
Router(config-if)#standby 9 priority 19
Router(config-if)#standby 9 preempt
Router(config-if)#
Router(config-if)#
 %HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 9 state Standby -> Active
```

б) Для Router 3

Рис. 10. Налаштування пріоритетів і увімкнення режиму preempt

3) Перевірено правильність проведених налаштування (рис. 11).

```
Router9#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Standby
    10 state changes, last state change 03:11:43
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.459 secs
  Preemption enabled
  Active router is 192.168.10.252, priority 19 (expires in 8 sec)
    MAC address is 0000.0C9F.F009
  Standby router is local
  Priority 17 (configured 17)
  Group name is hsrp-Gig0/0-9 (default)
Router9#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    17  P Standby  192.168.10.252  local           192.168.10.254
```

а) Для Router 1

```
Router#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Active
    6 state changes, last state change 01:24:03
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.056 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.253, priority 17 (expires in 6 sec)
  Priority 19 (configured 19)
  Group name is hsrp-Gig0/0-9 (default)
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    19  P Active   local           192.168.10.253  192.168.10.254
```

б) Для Router 3

Рис. 11. Перевірка налаштування standby

Обидва маршрутизатори знаходяться в одній групі, яка відповідає номеру 9. Маршрутизатор Router 1 знаходиться у стані очікування (standby), а маршрутизатор Router 3 є активним (active) маршрутизатором цієї мережі. Це обумовлено різницею у пріоритетах: пріоритет Router 1 становить 17, в той час як пріоритет Router 3 вищий і дорівнює 19. Відповідно, Router 3 обраний протоколом HSRP як активний.

Додатково, режим пріоритетного перевибору (preempt) також увімкнутий на обох маршрутизаторах. Це означає, що якщо Router 1 отримає більшу пріоритетність він може автоматично перейти до ролі активного маршрутизатора, навіть якщо Router 3, який є поточним активним маршрутизатором, все ще працює. Це мінімізує час простою та гарантує безперебійність процесу відновлення після відмови.

4) Перевірено працездатність з'єднання між пристроями PC 1 та PC 3 за допомогою команди ping (рис. 12 а), також перевірено маршрут проходження пакетів між цими пристроями (рис. 12 б) і перевірено зміст ARP-таблиці на пристрої відправника (рис. 12 в).

```
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.11.10: bytes=32 time=11ms TTL=126
Reply from 192.168.11.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms
```

а) Перевірка працездатності з'єднання між PC 1 і PC 3

```
C:\>tracert 192.168.11.10

Tracing route to 192.168.11.10 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.10.252
  2    0 ms      0 ms      0 ms      192.168.254.2
  3    0 ms      0 ms      0 ms      192.168.11.10

Trace complete.
```

б) Перевірка маршруту проходження пакетів між PC 1 і PC 3

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.10.253        0009.7c80.2d01        dynamic
  192.168.10.254        0000.0c9f.f009        dynamic
```

в) Перевірка ARP-таблиці на PC 1

Рис. 12. Перевірка працездатності

5) Змодельовано відмову активного маршрутизатора у мережі. Для цього з PC 1 було згенеровано безперервну послідовність ICMP-пакетів на PC 3 (рис. 13). Під час цього на активному маршрутизаторі Router 3 було вимкнуто інтерфейс, який під'єднаний до мережі з PC 1, це моделює ситуацію виходу з ладу маршрутизатора (рис. 14).

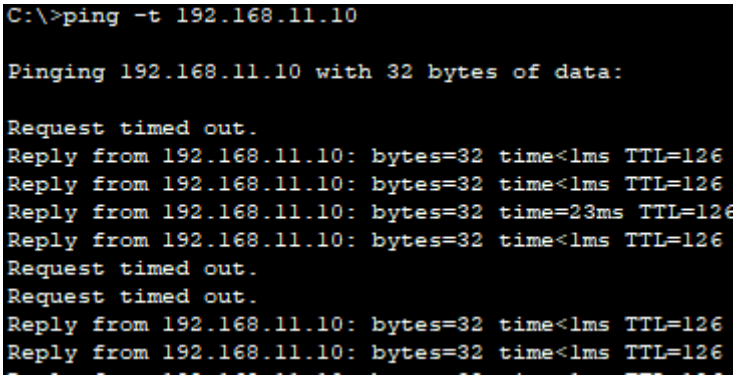

Рис. 13. Безперервна генерація ICMP пакетів з PC 1 на PC 3

```
Router9#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Active
    11 state changes, last state change 00:12:37
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.349 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 17 (configured 17)
  Group name is hsrp-Gig0/0-9 (default)
Router9#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    17  P Active   local           unknown         192.168.10.254
```

а) Стан маршрутизатора Router 1

```
Router#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Init (interface down)
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.180 secs
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 19 (configured 19)
  Group name is hsrp-Gig0/0-9 (default)
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    19  P Init     unknown         unknown         192.168.10.254
```

б) Стан маршрутизатора Router 3

Рис. 14. Перевірка стану маршрутизаторів

6) Після поновлення успішного передавання пакетів раніше вимкнутий інтерфейс маршрутизатора увімкнуто та проаналізовано стан ICMP-пакетів передаваємі PC 1 на PC 3 (рис. 15).

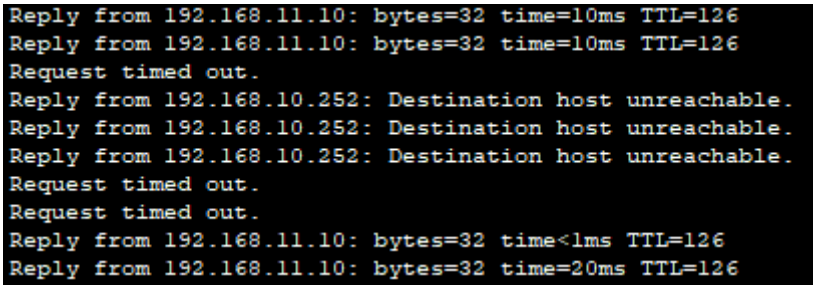

Рис. 15. Перевірка стану ICMP-пакетів передаваємі з PC 1 на PC 3

Під час моделювання ситуації відмови і поновлення активного маршрутизатора двічі було помічено втрату пакетів.

Перша втрата пакетів сталась під час відмови активного маршрутизатора Router 3, було втрачено 2 пакети. Це пов’язано з протоколом HSRP, за допомогою цього протоколу було помічено, що активний маршрутизатор Router 3 не відповідає і тому він був замінений на маршрутизатор Router 1, який знаходився в режимі очікування . Під час цього не було можливості передавати пакети, тому вони були втрачені.

Друга втрата пакетів сталась після поновлення роботи маршрутизатора Router 3, було втрачено 6 пакетів. Ця втрата пов’язана з затримкою перед початком роботи на комутаторах. Коли канал між комутатором Switch 0 і маршрутизатором Router 3 почав працювати, маршрутизатори Router 3 і Router 1 обмінялись HSRP пакетами і визначили, що маршрутизатор Router 3 має більшу пріоритетність, тому він повинен стати активним маршрутизатором у цій мережі, це сталось, бо у протоколі HSRP був увімкнений режим пріоритетного перевибору (preempt). Але коли пакети передавались на маршрутизатор Router 3, він не міг їх передати далі, бо комутатор Swtich 3 і маршрутизатор Router 3 ще не встановили канал

з’єднання. Це сталось, бо комутатору, на відміну від маршрутизатора, після встановлення каналу зв’язку потрібен деякий час для початку обслуговування цього каналу.

Пункт 4. Аналіз рівня безпеки протоколу HSRP

1) На межі першої і третьої мережі додано ще один маршрутизатор Router Spy (рис. 16). Всі необхідні для роботи інтерфейси на цьому маршрутизаторі були увімкнені і встановлено IP адреси, що є коректними для підмереж, до яких він належать (рис. 17).

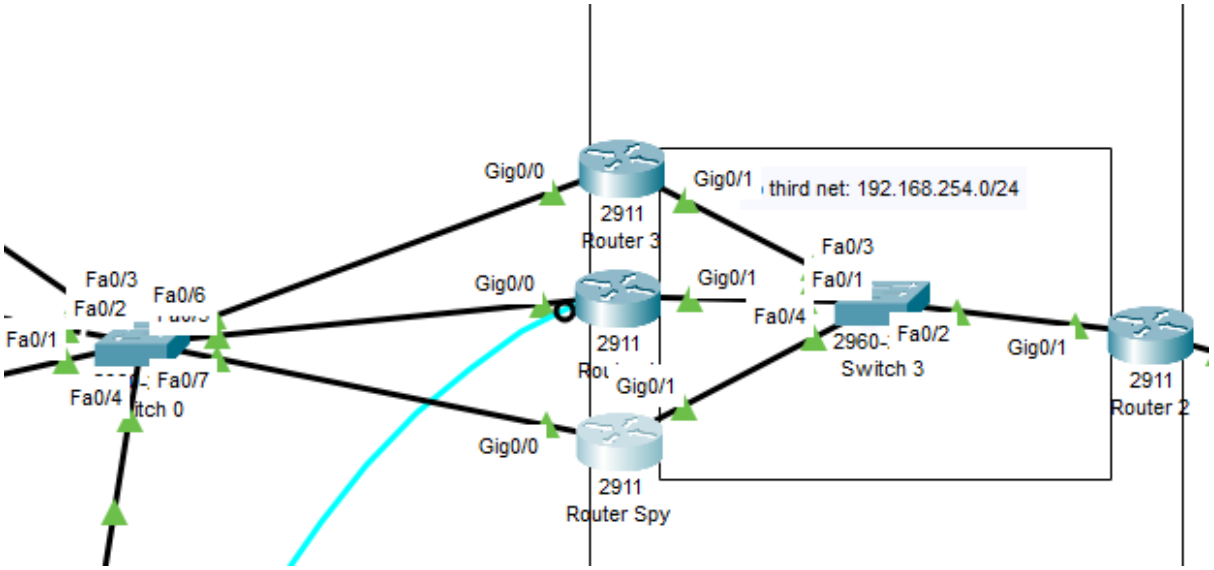

Рис. 16. Зловмисний маршрутизатор Router Spy під’єднаний до мережі

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.10.251 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.254.4 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Рис. 17. Налаштування зловмисного маршрутизатора Router Spy

2) На маршрутизаторі Router Spy налаштовано протоколи RIP та HSRP. Для протоколу HSRP були налаштовані інтерфейс, який з’єднаний з першою мережею, номер групи відповідає 9, також був увімкнений режим пріоритетного перевибору

(preempt) і встановлена пріоритетність, яка становить 255 (рис. 18).

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.254.0
Router(config-router)#exit
```

а) Налаштування протоколу RIP

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#standby version 2
Router(config-if)#standby 9 ip 192.168.10.254
Router(config-if)#standby 9 priority 255
Router(config-if)#standby 9 preempt
```

б) Налаштування протоколу HSRP

Рис. 18. Налаштування протоколів RIP і HSRP на зловмисному маршрутизаторі Router Spy

3) Перевірено стан маршрутизаторів, які створюють одну standby-групу (рис. 19).

Проаналізувавши отримані результати можна зробити такі висновки:

Маршрутизатор Router 3 більше не є активним маршрутизатором, він перейшов до режиму очікування, і у випадку несправності стане на заміну активному маршрутизатору.

Маршрутизатор Router Spy став активним маршрутизатором, тому що його пріоритет найбільший серед всіх інших маршрутизаторів.

Маршрутизатор Router 1 перейшов у режим прослуховування. Це означає, що він є запасним маршрутизатором для маршрутизатора Router 3.

```
Router9#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Listen
    81 state changes, last state change 03:56:39
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0 secs
  Preemption enabled
  Active router is 192.168.10.251
  Standby router is 192.168.10.253
  Priority 17 (configured 17)
  Group name is hsrp-Gig0/0-9 (default)
Router9#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    17  P Listen   192.168.10.251  192.168.10.253  192.168.10.254
```

а) для Router 1

```
Router#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Standby
    148 state changes, last state change 03:56:39
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.041 secs
  Preemption enabled
  Active router is 192.168.10.251, priority 255 (expires in 8 sec)
    MAC address is 0000.0C9F.F009
  Standby router is local
  Priority 19 (configured 19)
  Group name is hsrp-Gig0/0-9 (default)
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    19  P Standby  192.168.10.251  local           192.168.10.254
```

б) для Router 3

```
Router#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Active
    6 state changes, last state change 00:48:17
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.739 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.252, priority 19 (expires in 9 sec)
  Priority 255 (configured 255)
  Group name is hsrp-Gig0/0-9 (default)
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    255 P Active   local           192.168.10.252  192.168.10.254
```

в) для Router Spy

Рис. 19. Перевірка маршрутизаторів, створюють одну standby-групу

4) З метою упередження такої ситуації, коли пристрій зловмисника захоплює собі функції активного маршрутизатора, було налаштовано списки контролю доступу (ACL). Для цього на інтерфейсах, які входять до однієї standby групи легітимних маршрутизаторів налаштовані розширене правило списку контролю доступу (ACL). Правило було налаштоваеі таким чином, щоб дозволити прийом багатоадресних оновлень лише з легітимних пристроїв своєї standby-групи і заборонити прийом багатоадресних оновлень від будь-яких інших пристроїв, які скоріш за все є нелегітимними, весь інший трафік може відправлятись без обмежень (рис. 19).

```
Router9(config)#access-list 109 permit ip host 192.168.10.252 host 224.0.0.102
Router9(config)#access-list 109 deny ip any host 224.0.0.102
Router9(config)#access-list 109 permit ip any any
```

а) для Router 1

```
Router(config)#access-list 109 permit ip host 192.168.10.253 host 224.0.0.102
Router(config)#access-list 109 deny ip any host 224.0.0.102
Router(config)#access-list 109 permit ip any any
```

б) для Router 3

Рис. 20. Створення правила контролю доступу (ACL)

Перевірено налаштовані списку контролю доступу (рис. 21).

```
Router9#show access-lists
Extended IP access list 109
    10 permit ip host 192.168.10.252 host 224.0.0.102 (7 match(es))
    20 deny ip any host 224.0.0.102
    30 permit ip any any
```

а) для Router 1

```
Router#show access-lists
Extended IP access list 109
    10 permit ip host 192.168.10.253 host 224.0.0.102 (3 match(es))
    20 deny ip any host 224.0.0.102
    30 permit ip any any
```

б) для Router 3

Рис. 21. Перевірка налаштування списку контролю доступу

Налаштоване правило списку контролю доступу було ввімкнено на інтерфейсах, які входять до однієї standby групи легітимних маршрутизаторів (рис. 22).

```
Router9(config)#interface gigabitEthernet 0/0
Router9(config-if)#ip access-group 109 in
```

а) для Router 1

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 109 in
```

б) для Router 3

Рис. 22. Увімкнення правила списку контролю доступу

5) На маршрутизаторі Router Spy були вимкнені всі порти, і функція активного маршрутизатора перейшла до легітимного маршрутизатора (рис. 23).

```
Router9#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Standby
    13 state changes, last state change 00:06:29
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.979 secs
  Preemption enabled
  Active router is 192.168.10.252, priority 19 (expires in 8 sec)
    MAC address is 0000.0C9F.F009
  Standby router is local
  Priority 17 (configured 17)
  Group name is hsrp-Gig0/0-9 (default)
Router9#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    17  P Standby  192.168.10.252  local           192.168.10.254
```

а) для Router 1

```
Router#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Active
    6 state changes, last state change 00:00:17
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.724 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.253, priority 17 (expires in 6 sec)
  Priority 19 (configured 19)
  Group name is hsrp-Gig0/0-9 (default)
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    19  P Active   local           192.168.10.253  192.168.10.254
```

б) для Router 3

Рис. 23. Перевірка стану маршрутизаторів після від'єднання Router Spy

Маршрутизатор Router Spy знову під'єднано до мережі і перевірено ролі і статус маршрутизаторів, після встановлення списків контролю доступу (рис. 24).

```
Router9#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Standby
    24 state changes, last state change 00:30:51
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.504 secs
  Preemption enabled
  Active router is 192.168.10.252, priority 19 (expires in 7 sec)
    MAC address is 0000.0C9F.F009
  Standby router is local
  Priority 17 (configured 17)
  Group name is hsrp-Gig0/0-9 (default)
Router9#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    17  P Standby  192.168.10.252  local           192.168.10.254
```

а) для Router 1

```
Router#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Active
    25 state changes, last state change 00:30:28
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.385 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.253, priority 17 (expires in 6 sec)
  Priority 19 (configured 19)
  Group name is hsrp-Gig0/0-9 (default)
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    19  P Active   local           192.168.10.253  192.168.10.254
```

б) для Router 3

```
Router#show standby
GigabitEthernet0/0 - Group 9 (version 2)
  State is Active
    21 state changes, last state change 00:32:23
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C9F.F009
    Local virtual MAC address is 0000.0C9F.F009 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.558 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.253, priority 19 (expires in 8 sec)
  Priority 255 (configured 255)
  Group name is hsrp-Gig0/0-9 (default)
Router#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      9    255 P Active   local           192.168.10.253  192.168.10.254
```

в) для Router Spy

Рис. 24. Перевірка стану маршрутизаторів після повторного підключення Router Spy

Після проведених налаштувань маршрутизатори Router 1 і Router 3 почали відкидати HSRP пакети, які відправлялись до них від маршрутизатора Router Spy. Це означає, що легітимні маршрутизатори не звертають увагу на те, що Router Spy має більший пріоритет і вирішують між собою хто з них активний, а хто буде у режимі очікування. Таким чином Router 3 стає активним, а Router 1 переходить в режим очікування.

Але на відміну від легітимних маршрутизаторів, маршрутизатор Router Spy отримує HSRP повідомлення від обох легітимних маршрутизаторів, тому порівнюючи свій пріоритет і пріоритет легітимних маршрутизаторів, він розуміє, що він має найбільший пріоритет і стає активним маршрутизатором.

І це є серйозною проблемою, в мережі з'являється два активних маршрутизатори і тому трафік, який передається в зовнішні мережі йде відразу через два маршрутизатори, причому дублюючись (рис. 25). Це призводить до того, що зловмисник перехоплює і аналізує весь трафік і може це використати для реалізації атаки на мережу. Також через те що пакети дублюються це вдвічі збільшує навантаження на мережу.

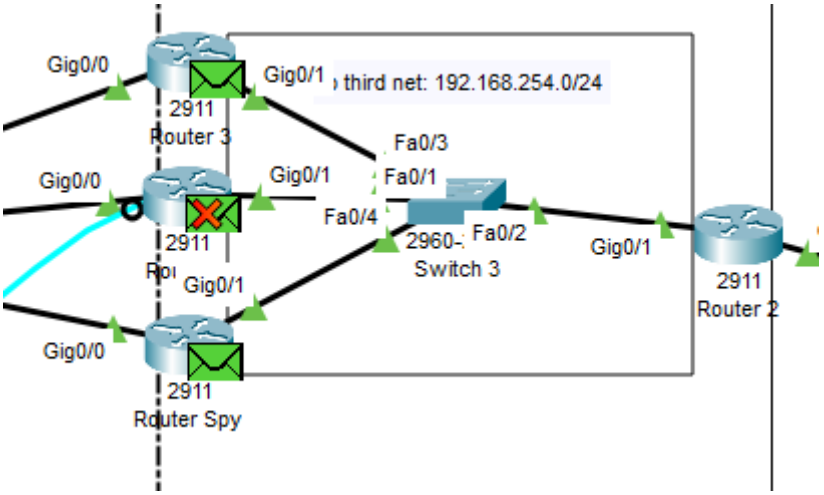

Рис. 25. Дублювання пакетів

Висновок:

У ході проведеної лабораторної роботи було налаштовано та перерено різноманітні аспекти мережевої інфраструктури, включаючи віддалений безпечний доступ через протокол SSH, налаштування протоколу маршрутизації RIP та відмовостійкого протоколу маршрутизації HSRP.

Під час виконання першого етапу лабораторної роботи було встановлено, що використання протоколу SSH надає надійний та безпечний засіб для забезпечення віддаленого доступу до мережевого обладнання. Шифрування даних та ефективна аутентифікація зменшують ризик несанкціонованого доступу до системи.

У результаті виконання другого етапу налаштування успішно впроваджено протокол RIP, що призвело до покращення швидкості обміну інформацією між маршрутизаторами. Реалізація RIP дозволяє оптимізувати маршрутизацію та забезпечити ефективну роботу мережі.

Виявлено, що під час переходу від активного до резервного маршрутизатора може виникати тимчасова втрата пакетів. Проте, протокол HSRP демонструє високий рівень ефективності виявлення відмов та надійного переключення між маршрутизаторами.

З метою перевірка рівня безпеки був внесений маршрутизатор Router Spy, і налаштовані списки контролю доступу (ACL). Це дозволяє ефективно управляти доступом до протоколу HSRP та захищати від можливих атак. Результати аналізу підкреслюють важливість правильного конфігурування ACL для забезпечення безпеки протоколу HSRP та уникнення потенційних загроз.

Загальною метою проведеної лабораторної роботи було вивчення та практичне впровадження ключових аспектів мережевих технологій, зосереджених на безпеці та відмовостійкості. Отримані в ході виконання завдань навички є важливим резервом для ефективного управління безпекою локальної мережі, а також надають можливість запобігати потенційним загрозам інфрастру