DigiJED - 2

Report
from laboratory work No. 3
of the course "ICT Security"

Performed by:
Nizhivenko A. D.
Variant No. 9

Kharkiv
2023

Topic: "Protection of global networks"

Objective: Acquiring practical skills in securing global networks.

Initial data (Fig. 1):

First net:

2 switches are connected to each other (Switch 0, Switch 1), a server is connected to Switch 0 (Server 0), 2 computers are connected to Switch 1 (PC 0, PC 1), 2 access points (Access Point 1, Access Point 2) are connected to Switch 0, 4 laptops are connected to Access Point 1 (Laptop 0, Laptop 1, Laptop 2, Laptop 3), 2 laptops are connected to Access Point 2 (Laptop 4, Laptop 5), and a router is connected to Switch 0 (Router 1).

The second network:

switch (Switch 2), 3 computers connected to Switch 2 (PC 2, PC 3, PC 4), a server connected to Switch 2 (Server 1), a router connected to Switch 2 (Router 2).

The third network:

2 routers are connected to each other (Router 1, Router 2).

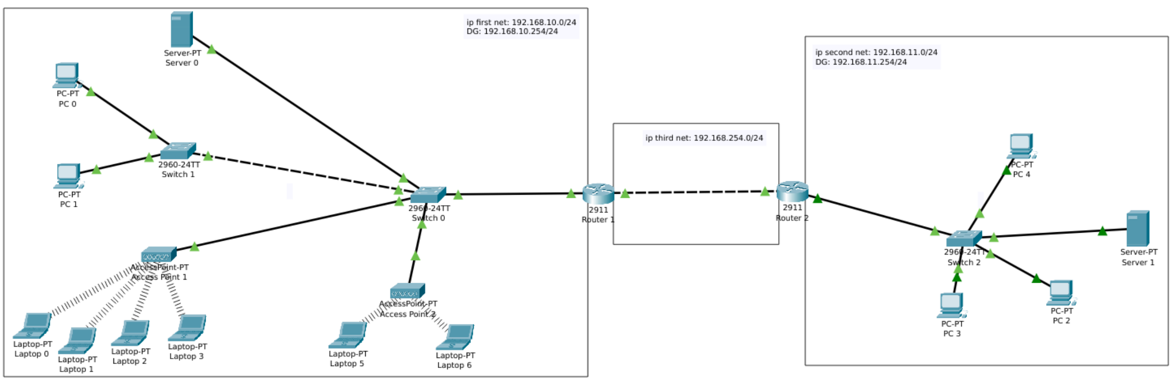

Figure 1. The initial data of the network

Work in progress

Step 1. Setting up and testing a remote secure access to the router using SSH

Remote secure access using SSH was configured on Router 1. To do this, we set the domain name Domai)n9 and created a 1024-bit RSA key (a key longer than 768 bits is a requirement for SSH version 2), enabled SSH version 2, and set the username User9 and password Pass9 (Fig. 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
```

Figure. 2. Setting up a remote secure access to the router using SSH

The settings made earlier were verified by creating an SSH connection to Router 1 from Laptop 5. During the test, it was found that access to the router via SSH is protected and requires a password to successfully access the command line interface (Fig. 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
```

Figure. 3. Checking the remote secure access to the router using SSH.

Step 2. Configuring the RIP routing protocol

1) Router Router 3 is added to the boundary of the first and third networks, and Switch 3 is added to the third network, through which all routers in the third network are now connected (Fig. 4).

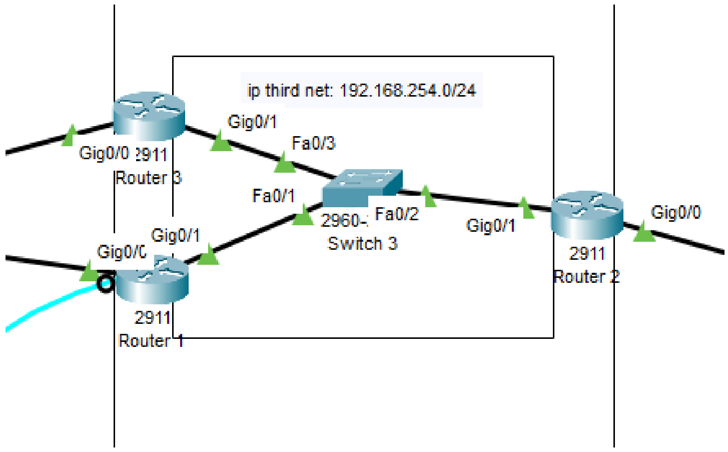

Figure 4. The new router and switch are connected to the network

2) All router interfaces have been enabled and IP addresses have been set to the correct ones for the subnets to which they belong (Fig. 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
```

a) For 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
```

b) For 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
```

c) For Router 3

Figure 5. Setting the IP address for router interfaces

3) On routers that used static routing, it was disabled (Fig. 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
```

a) For 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
```

b) For Router 2

Figure 6. Disabling static routing

4) The routers are configured with RIPv2 protocol and passive interfaces are specified to prevent the transmission of routing table updates through the router interface to devices that do not support the RIP protocol (Fig. 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
```

a) For 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
```

b) For 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
```

c) For Router 3

Figure 7. Configuring the RIPv2 protocol

5) Check the routing tables built by the RIP protocol (Fig. 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
```

a) For 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
```

b) For 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
```

c) For Router 3

Figure 8. Checking the tables built by the RIP protocol

Step 3. Configuring the HSRP fault tolerant routing protocol

1) The HSRP protocol is configured on the interfaces of routers Router 1 and Router 3. The standby group number is 9 (Fig. 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
```

a) For 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
```

b) For Router 3

Figure 9. Setting up the HSRP protocol

2) On the interfaces of the first subnet of routers Router 1 and Router 3, the priorities are set: for Router 1, the priority is 17, and for Router 3, the priority is 19. Also, on each of the interfaces of both routers, the preempt mode is enabled (Fig. 10).

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

a) For 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) For Router 3

Figure 10. Setting priorities and enabling preempt mode

3) Check the correctness of the settings (Fig. 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

Both routers are in the same group, which corresponds to group number 9. Router 1 is in the standby state, and Router 3 is the active router on this network. This is due to the difference in priority: Router 1's priority is 17, while Router 3's priority is higher and equal to 19. Accordingly, Router 3 is selected by HSRP as the active router.

Additionally, preempt mode is also enabled on both routers. This means that if Router 1 receives a higher priority, it can automatically take over as the active router even if Router 3, which is the current active router, is still running. This minimizes downtime and ensures a smooth disaster recovery process.

4) Check the functionality of the connection between PC 1 and PC 3 using the ping command (Fig. 12 a), also check the route of packets between these devices (Fig. 12 b) and check the contents of the ARP table on the sender's device (Fig. 12 c).

```
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
```

a) Checking the connection between PC 1 and 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.
```

b) Checking the route of packets between PC 1 and 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
```

c) Checking the ARP table on PC 1

Figure 12. Checking the performance

5) We simulated the failure of the active router in the network. To do this, a continuous sequence of ICMP packets was generated from PC 1 to PC 3 (Fig. 13). At the same time, the interface that is connected to the network from PC 1

was disabled on the active router Router 3, which simulates the situation of router failure (Fig. 14).

```
C:\>ping -t 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.11.10: bytes=32 time<1ms TTL=126
Reply from 192.168.11.10: bytes=32 time<1ms TTL=126
Reply from 192.168.11.10: bytes=32 time=23ms TTL=126
Reply from 192.168.11.10: bytes=32 time<1ms TTL=126
Request timed out.
Request timed out.
Reply from 192.168.11.10: bytes=32 time<1ms TTL=126
Reply from 192.168.11.10: bytes=32 time<1ms TTL=126
```

Figure 13. Continuous generation of ICMP packets from PC 1 to 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
```

a) Router status of 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
```

b) Router status of Router 3

Figure 14. Checking the status of routers

6) After the successful transmission of packets resumed, the previously disabled router interface is turned on and the status of ICMP packets transmitted by PC 1 to PC 3 is analyzed (Fig. 15).

```
Reply from 192.168.11.10: bytes=32 time=10ms TTL=126
Reply from 192.168.11.10: bytes=32 time=10ms TTL=126
Request timed out.
Reply from 192.168.10.252: Destination host unreachable.
Reply from 192.168.10.252: Destination host unreachable.
Reply from 192.168.10.252: Destination host unreachable.
Request timed out.
Request timed out.
Reply from 192.168.11.10: bytes=32 time<1ms TTL=126
Reply from 192.168.11.10: bytes=32 time=20ms TTL=126
```

Figure 15. Checking the status of ICMP packets transmitted from PC 1 to PC 3

During the simulation of the failure and recovery of the active router, packet loss was noticed twice.

The first packet loss occurred when the active router Router 3 failed, 2 packets were lost. This is due to the HSRP protocol, with the help of this protocol it was noticed that the active router Router 3 was not responding and therefore it was replaced by Router 1, which was in standby mode. During this time, it was not possible to transmit packets, so they were lost.

The second packet loss occurred after Router 3 resumed operation, and 6 packets were lost. This loss is due to a delay before the switches started working. When the link between Switch 0 and Router 3 became operational, Router 3 and Router 1 exchanged HSRP packets and determined that Router 3 had a higher priority and should become the active router on the network, which happened because preempt was enabled in the HSRP protocol. But when the packets were transmitted to Router 3, it could not forward them on because the Switch 3 and Router 3 had not yet established a link. This happened because a switch, unlike a router, takes some time after establishing a link to start servicing that link.

Section 4. Analysis of the security level of the HSRP protocol

1) On the border of the first and third networks, another Router Spy router was added (Fig. 16). All interfaces necessary for operation on this router have been enabled and IP addresses have been set to the correct ones for the subnets to which it belongs (Fig. 17).

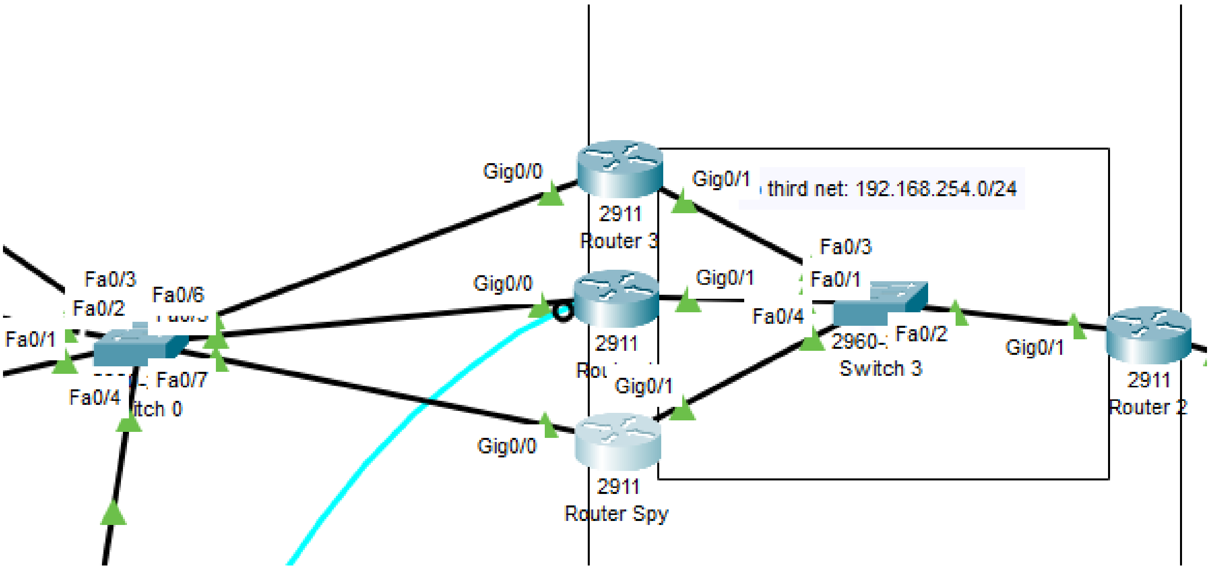

Figure 16. The malicious Router Spy router is connected to the network

```
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
```

Figure 17. Setting up a malicious Router Spy router

2) The Router Spy router is configured with the RIP and HSRP protocols. For the HSRP protocol, the interface connected to the first network has been configured, the group number is 9, the preempt mode has been enabled, and the priority has been set to 255 (Fig. 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
```

a) Configure the RIP protocol

```
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) Configuring the HSRP protocol

Figure 18. Configuring RIP and HSRP protocols on the Router Spy malicious router

3) Check the status of routers that create a single standby group (Fig. 19).

After analyzing the results, we can draw the following conclusions:

Router 3 is no longer the active router, it has entered standby mode and will take over for the active router in the event of a malfunction.

Router Spy became the active router because its priority is the highest among all other routers.

Router 1 has entered listening mode. This means that it is the backup router for 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
```

a) For 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
```

b) For 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
```

c) For Router Spy

Figure 19. Checking routers that create a single standby group

4) In order to prevent a situation where an attacker device takes over the functions of the active router, access control lists (ACLs) have been configured. To do this, an extended ACL rule was configured on the interfaces that are part of the same standby group of legitimate routers. The rule was configured to allow multicast updates to be received only from legitimate devices in its standby group and to deny multicast updates from any other devices that are

likely to be illegitimate, while all other traffic can be sent without restriction (Fig. 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
```

a) For 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
```

b) For Router 3

Figure 20. Creating an access control rule (ACL)

The configured access control lists are checked (Fig. 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
```

a) For 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) For Router 3

Figure 21. Checking the access control list settings

The configured access control list rule was enabled on the interfaces that are part of the same standby group of legitimate routers (Fig. 22).

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

a) For Router 1

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

b) For Router 3

Figure 22. Enabling the access control list rule

5) All ports on the Router Spy router have been disabled, and the function of the active router has been taken over by the legitimate router (Fig. 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
```

a) For 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
```

b) For Router 3

Figure 23. Checking the status of routers after Router Spy disconnects

The Router Spy router is reconnected to the network and the roles and status of the routers are checked after the access control lists are set (Fig. 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
```

a) For 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
```

b) For 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
```

c) For Router Spy

Figure 24. Checking the status of routers after reconnecting Router Spy

After the configuration, routers Router 1 and Router 3 began to drop HSRP packets sent to them from Router Spy. This means that the legitimate routers do not pay attention to the fact that Router Spy has a higher priority and decide among themselves which of them is active and which will be in standby mode. Thus, Router 3 becomes active and Router 1 goes into standby mode.

But unlike legitimate routers, Router Spy receives HSRP messages from both legitimate routers, so by comparing its priority with that of the legitimate routers, it realizes that it has the highest priority and becomes the active router.

And this is a serious problem, because there are two active routers in the network, and therefore the traffic that is transmitted to external networks goes through two routers at once, and is duplicated (Fig. 25). This leads to the fact that an attacker intercepts and analyzes all traffic and can use it to launch an attack on the network. Also, because packets are duplicated, it doubles the load on the network.

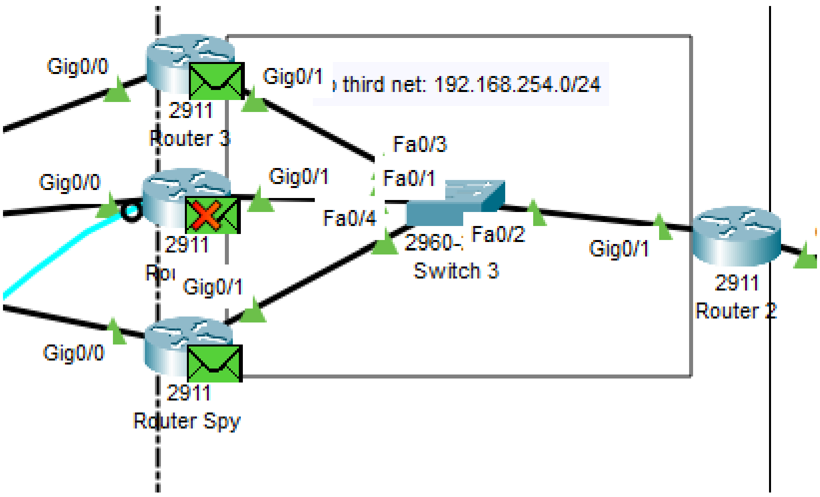

Figure 25. Duplicate packets

Conclusion:

In the course of the lab, various aspects of the network infrastructure were configured and tested, including remote secure access via SSH, configuration of the RIP routing protocol and the HSRP fault-tolerant routing protocol.

During the first stage of the laboratory work, it was found that the use of the SSH protocol provides a reliable and secure means of providing remote access to network equipment. Data encryption and effective authentication reduce the risk of unauthorized access to the system.

As a result of the second stage of configuration, the RIP protocol was successfully implemented, which led to an improvement in the speed of information exchange between routers. RIP implementation allows you to optimize routing and ensure efficient network operation.

It was found that during the transition from the active to the standby router, there may be a temporary loss of packets. However, the HSRP protocol demonstrates a high level of fault detection efficiency and reliable switching between routers.

In order to check the security level, Router Spy was added and access control lists (ACLs) were configured. This allows you to effectively control access to the HSRP protocol and protect against possible attacks. The results of the analysis emphasize the importance of properly configuring ACLs to ensure the security of the HSRP protocol and avoid potential threats.

The overall goal of the lab was to study and implement key aspects of networking technologies focused on security and fault tolerance. The skills acquired in the course of the tasks are an important reserve for effective management of local network security, as well as provide an opportunity to prevent potential threats to the infrastructure.