DigiJED - 2

# Report
from laboratory work No. 2
of the course "ICT Security"

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

Kharkiv
2023

Topic: "Protection of local networks"

Objective: Acquiring practical skills in securing local networks.

Initial data:

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), the router is connected to Switch 0 (Router 1).

Second net:

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

Third net:

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

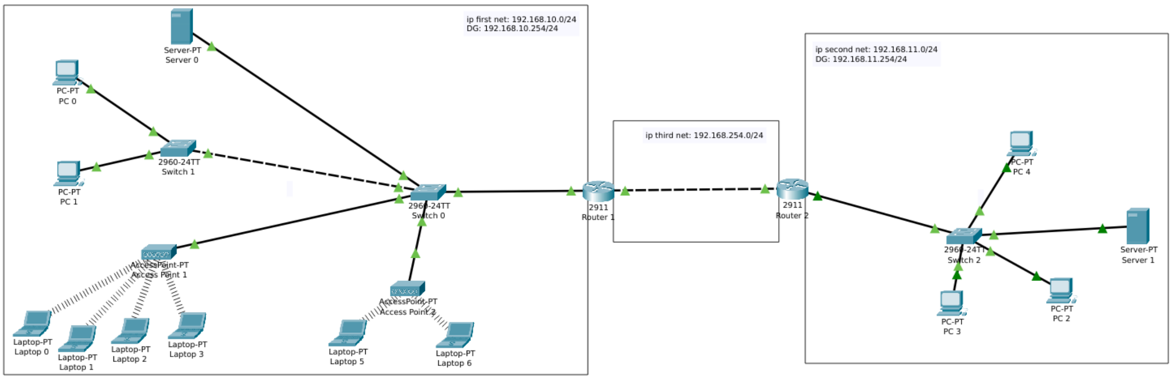


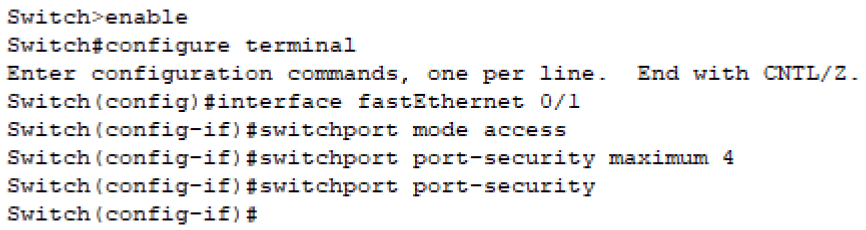
Figure 1. The initial data of the network

Work in progress

Para. 1. Research means of protection CAM tables on the network switch.

1) To protect the SAM tables on Switch 0, Port Security is used on FastEthernet port 0/1, which connects Switch 0 to Access Point 1.

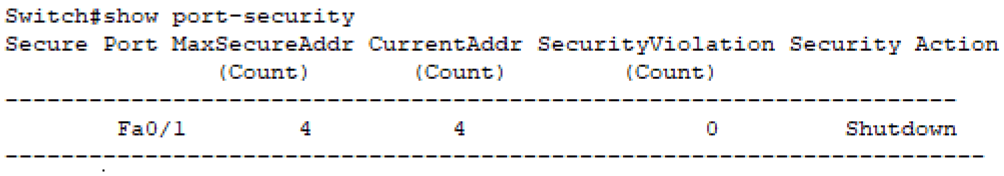
Using the Port Security functionality, the maximum number of connected end devices to FastEthernet port 0/1 was limited. The maximum number of connected end devices is 4 (Fig. 2).



```
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)#
```

Figure 2. Configuring Port Security on Switch 0

The result of the configuration was checked with the *show port-security command* (Fig. 3).



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

Figure 3. Verifying the port security settings on Switch 0

2) Modeled the first possible scenario of a local network security breach: a new illegitimate device (Laptop Enemy) is connected to Access Point 1 (Fig. 4).

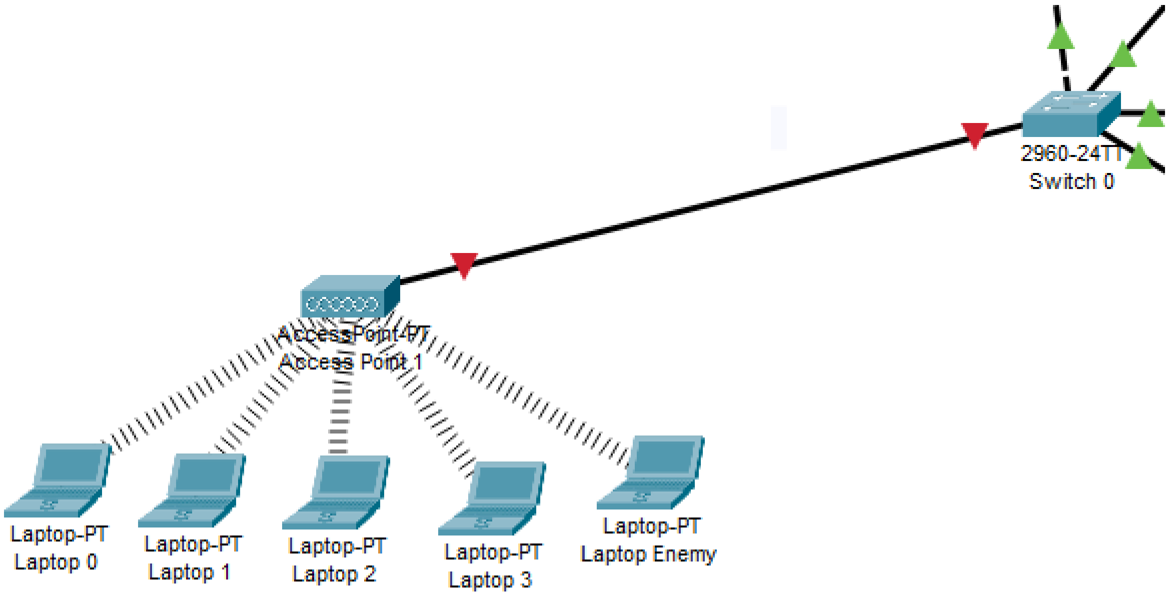
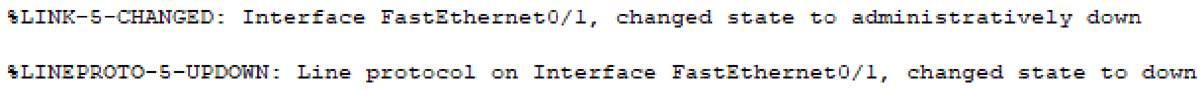


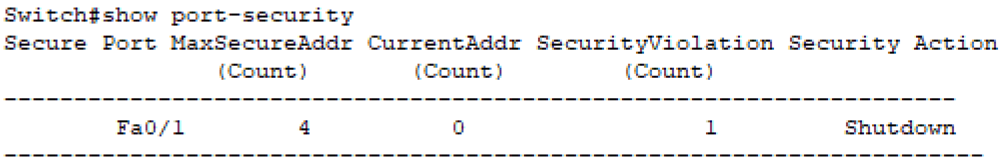
Figure 4. The new device is connected to Access Point 1

Analyze the state of the channel that connects Switch 0 and Access Point 1 (Fig. 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
```

a) Service message in the CLI



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

b) Checking with the *show port-security* command

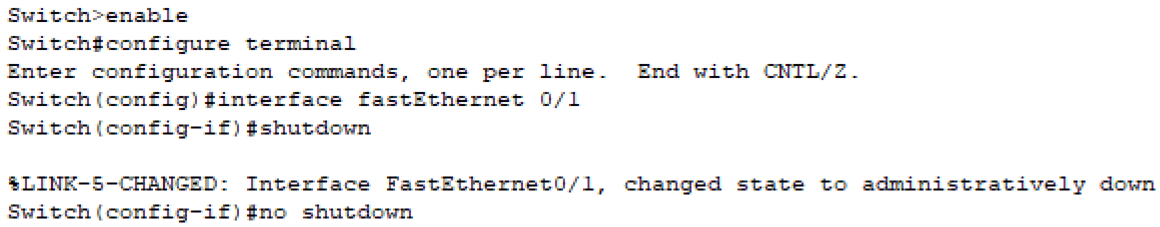
Figure 5. Checking the channel status after simulating the first security breach

The link connecting Switch 0 to Access Point 1 is disabled by Port Security.

The switch has received information that a new endpoint device has been connected to Access Point 1, which means that there are 5 devices connected to

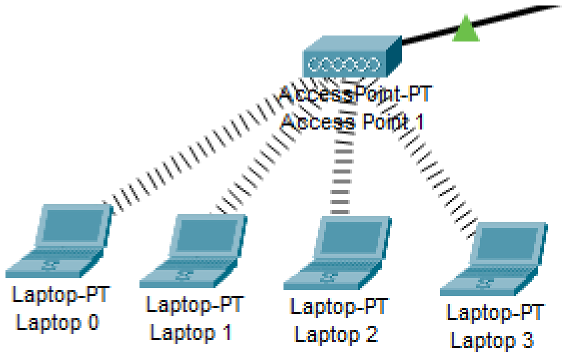
Access Point 1, which exceeds the maximum number of devices that can be connected to Switch 0 according to the configuration specified in step 1. This is considered a security policy violation and causes the switch to disable FastEthernet port 0/1, which connects Switch 0 to Access Point 1

3) The network was restored to its previous state by removing Laptop Enemy and changing the state of FastEthernet port 0/1 on Switch 0 to active (Fig. 6). The Port Security status on FastEthernet 0/1 was also checked (Fig. 7).



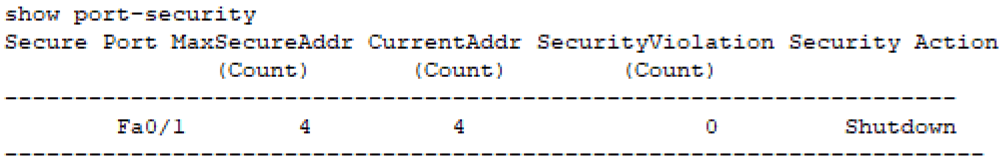
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#shutdown

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

a) Enable FastEthernet port 0/



b) The result of returning the network to its previous state

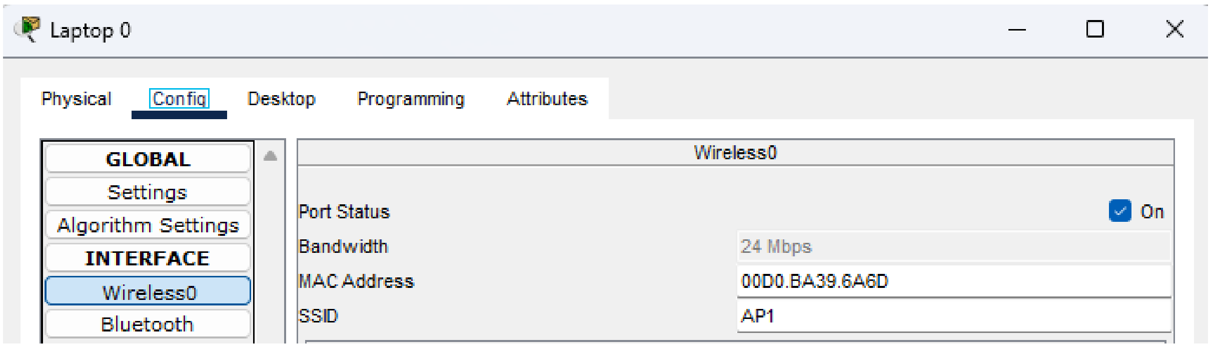
Figure 6. Returning the previous state of the network



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

Figure 7. Checking the port security status on Switch 0

4) Modeled the second possible scenario of a local network security breach: the MAC address of Laptop 0 was changed (Fig. 8).



Wireless0

Port Status ☑ On

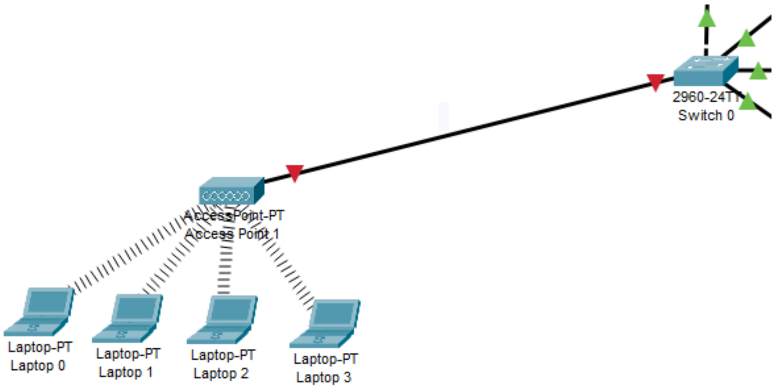
Bandwidth 24 Mbps

MAC Address 00D0.BA39.6A6D

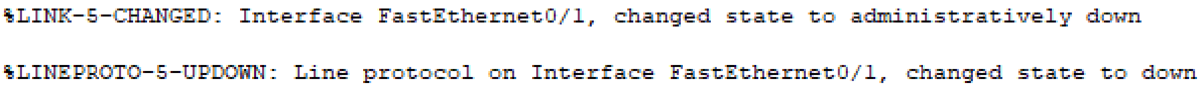
SSID AP1

Figure 8. Changing the MAC address of Laptop

Analyzing the status of the link connecting the Switch 0 and Access Point 1 (Fig. 9).

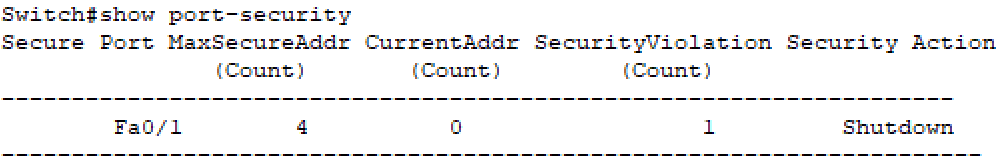


a) Status of the connection channel



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

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

b) Service message in the CLI of Switch 0



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

c) Checking with the *show port-security* command

Figure 9. Checking the channel state after simulating the second security breach

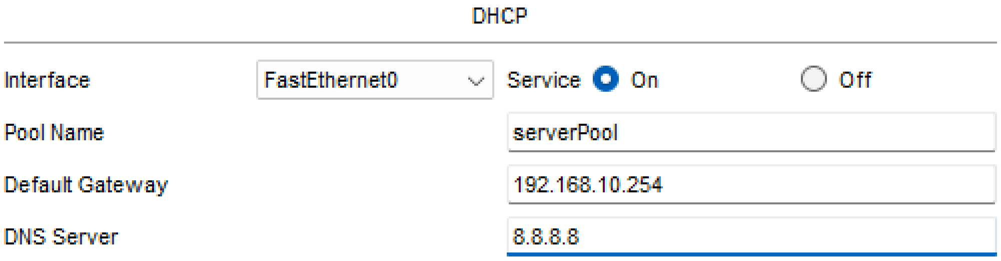
7

The link connecting Switch 0 to Access Point 1 is disabled by Port Security.

The switch receives information that a device with a new MAC address is connected to the network, and the switch considers the MAC address to be an outsider because the MAC address does not match any of the valid MAC addresses for that port. This is treated as a security policy violation, and the switch shuts down the FastEthernet 0/1 port that connects Switch 0 to Access Point 1.

Objective 2. Study of DHCP service security features

1) Added y setting legitimate DHCP server settings, the IP address of the DNS server is 8.8.8.8 (Fig. 10).



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name serverPool

Default Gateway 192.168.10.254

DNS Server 8.8.8.8

Figure 10. Setting up a legitimate DHCP server

2) An illegitimate DHCP server (Server Enemy) has been added to the network and is connected to Switch 1 (Fig. 11).

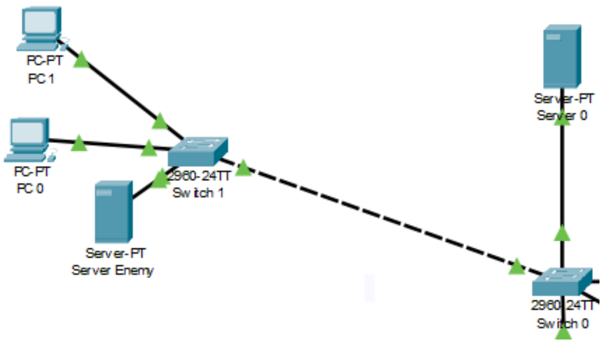
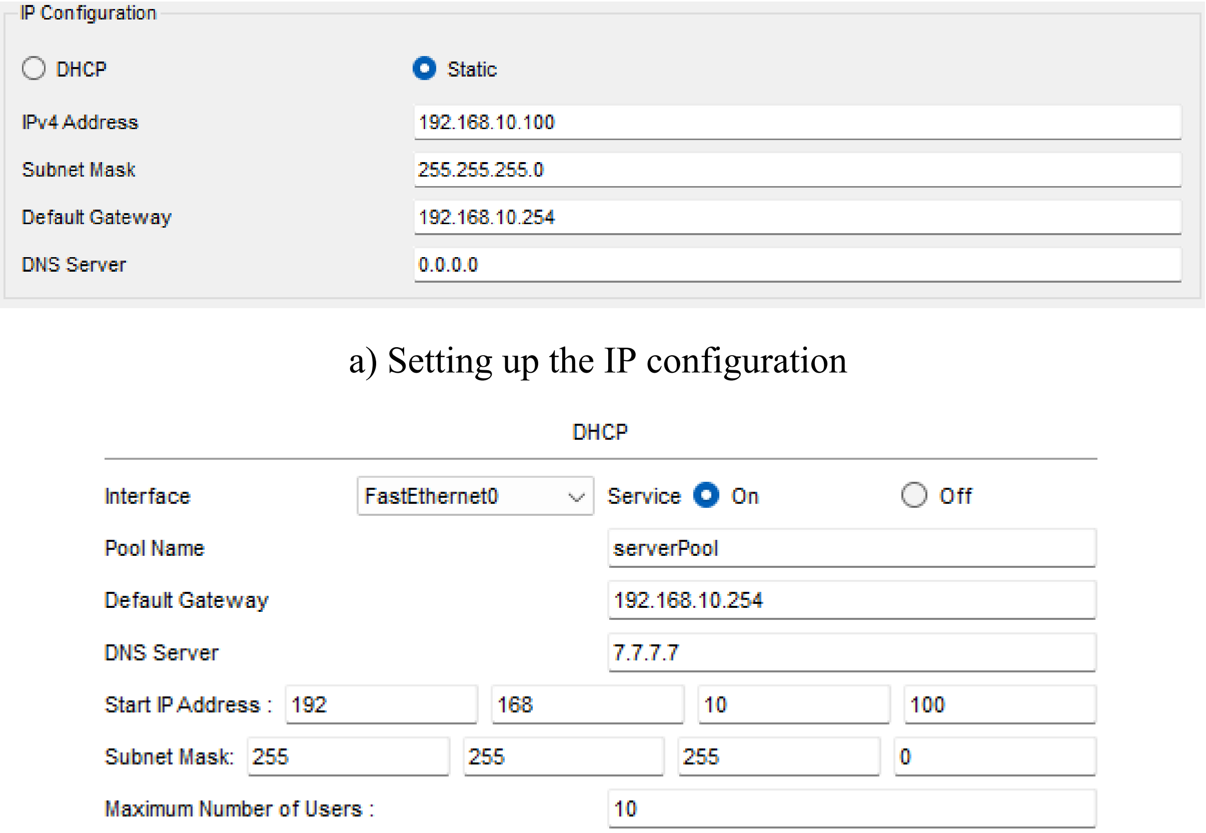


Figure 11. A new rogue DHCP server is connected to the network

The illegitimate DHCP server (Server Enemy) is configured to issue an address to the illegitimate DNS 7.7.7.7 (Fig. 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

a) Setting up the IP configuration

DHCP

Interface FastEthernet0 Service ● On ○ Off

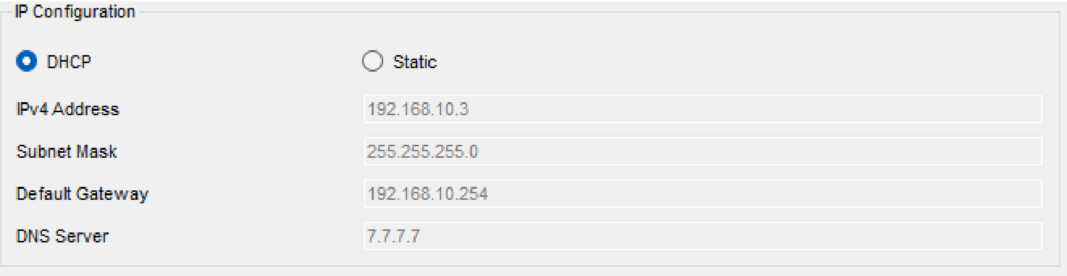
Pool Name	serverPool			
Default Gateway	192.168.10.254			
DNS Server	7.7.7.7			
Start IP Address :	192	168	10	100
Subnet Mask:	255	255	255	0
Maximum Number of Users :	10			

b) Setting up the DHCP service

Figure 12. Setting up an illegitimate DHCP server

3) DHCPDISCOVER request was sent to devices PC 0, PC 1, Laptop 4, Laptop 5 to update IP addresses from the DHCP server.

For PC 0, the IP address and subnet mask were obtained from a legitimate server (Server 0), and the default gateway and DNS server from an illegitimate server (Server Enemy) (Figure 13).



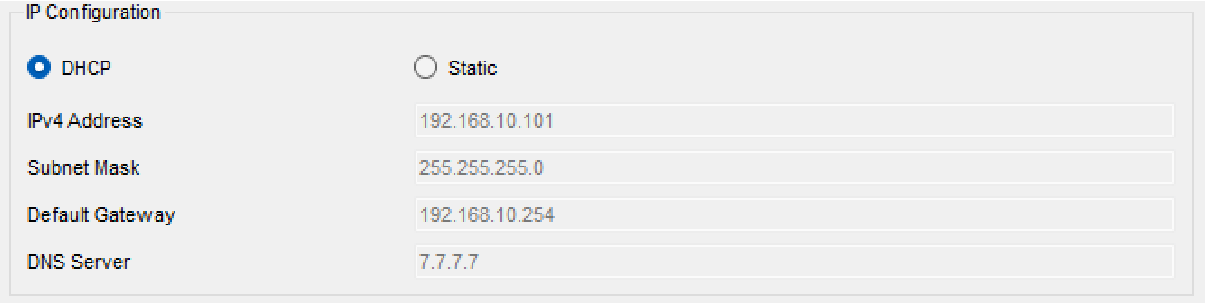
IP Configuration

● 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

Figure 13. Settings obtained using DHCP for PC 0

For PC 1, the entire configuration was obtained from an illegitimate server (Server Enemy) (Fig. 14).



IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.10.101

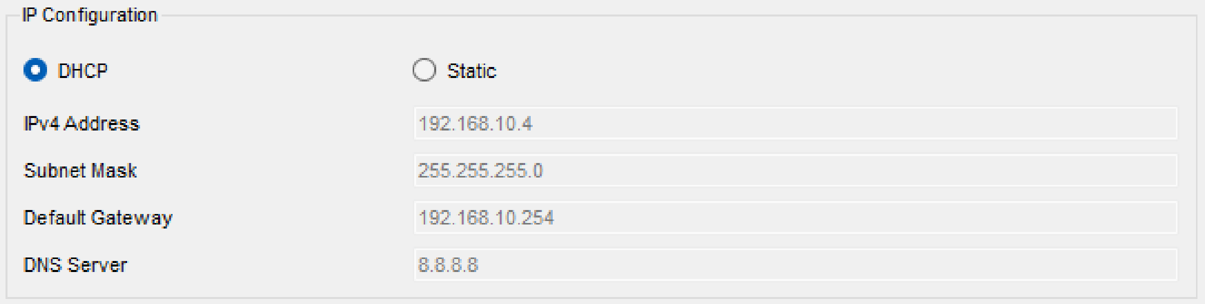
Subnet Mask 255.255.255.0

Default Gateway 192.168.10.254

DNS Server 7.7.7.7

Figure 14. Settings obtained using DHCP for PC 1

For Laptop 4, the entire configuration is obtained from a legitimate server (Server 0) (Fig. 15).



IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.10.4

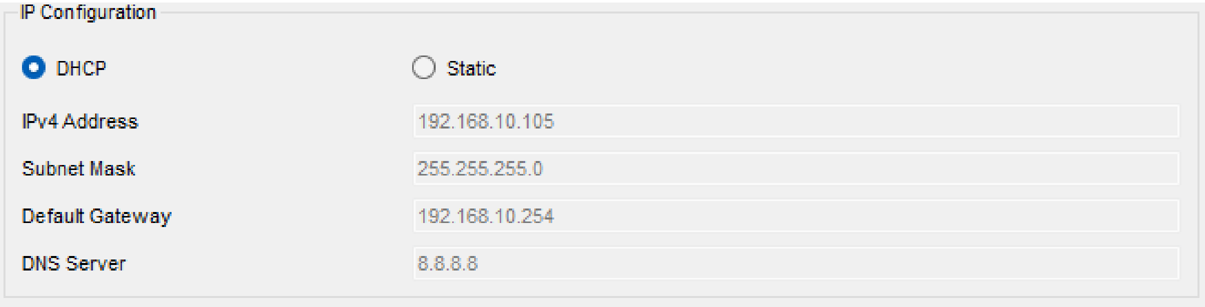
Subnet Mask 255.255.255.0

Default Gateway 192.168.10.254

DNS Server 8.8.8.8

Figure 15. Settings obtained using DHCP for Laptop 4

For Laptop 5, the IP address and subnet mask were obtained from an illegitimate server (Server Enemy), and the default gateway and DNS server were obtained from a legitimate server (Server 0) (Fig. 16).



IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.10.105

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.254

DNS Server 8.8.8.8

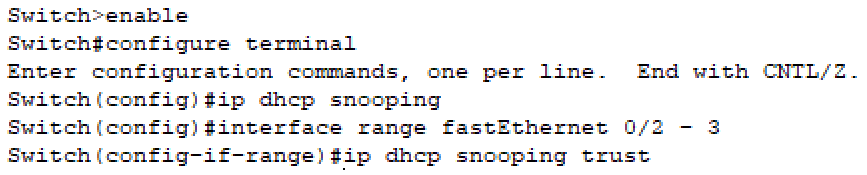
Figure 16. Settings obtained using DHCP for Laptop 5

The device receives the settings of the DHCP server that responds faster to the device's request. An example of this is Laptop 4 and PC 1.

PC 1 is closer to Server Enemy, so it received the entire configuration from this server, while Laptop 4 is closer to Server 0, so it received the entire configuration from it.

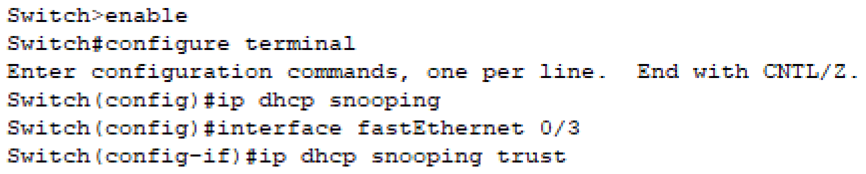
It is also possible that a device receives half of its configuration from Server 0 and the other half from Server Enemy, or vice versa. An example of this is Laptop 5 and PC 0. This happens because the servers send the configuration in multiple packets and the devices can receive the configuration from different packets, where one packet is sent from the first server and the second packet is sent from the second server.

4) DHCP Snooping is enabled on Switch 0 and Switch 1, and FastEthernet ports 0/2, FastEthernet port 0/3 on Switch 0 and FastEthernet port 0/3 on Switch 1 are configured as trust ports (Fig.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
```

a) Configuration on Switch 0

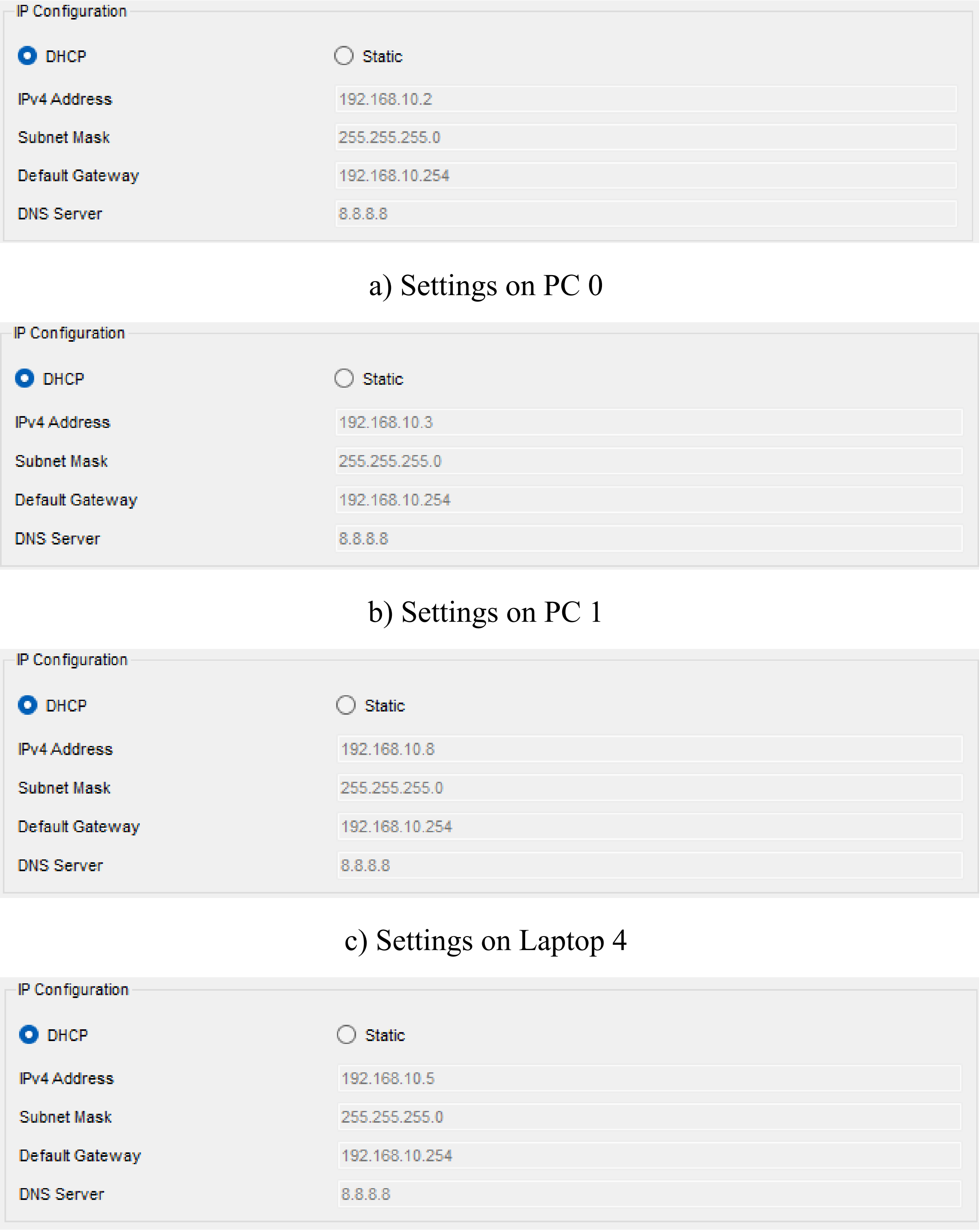


```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#ip dhcp snooping trust
```

b) Configuration on Switch 1

Figure 17. Configuring DHCP Snooping and Trust Ports on Switches

5) Checked the IP addressing order on endpoints that were previously configured from an illegitimate DHCP server. All terminal devices have received configuration from a legitimate server (Server 0) (Fig. 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

a) Settings on 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

b) Settings on 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

c) Settings on Laptop 4

IP Configuration

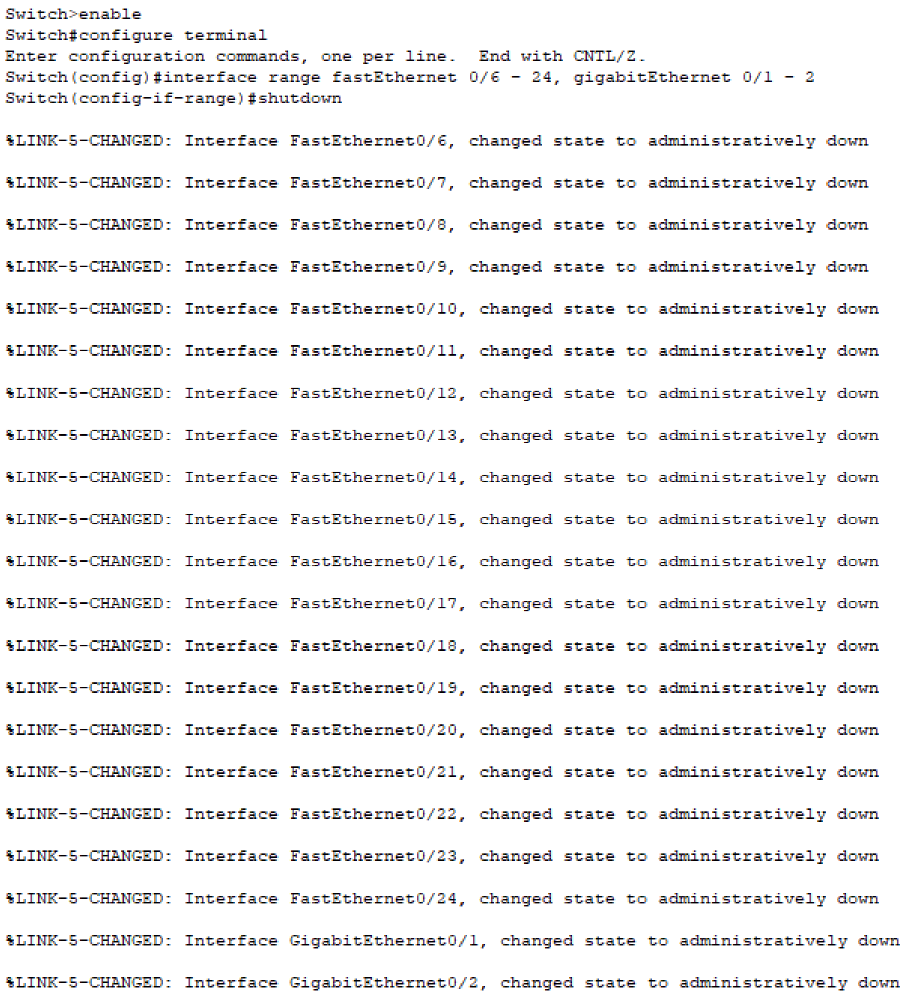
● DHCP ○ Static

IPv4 Address	192.168.10.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.254
DNS Server	8.8.8.8

d) Settings on Laptop 5

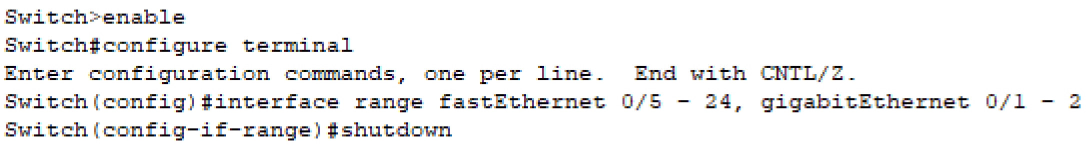
Figure 18. Settings received via DHCP for PC 0, PC 1, Laptop 4, Laptop 5

6) Done disconnection of all ports, that are not not used on Switch 0 and Switch 1 (Fig. 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
```

a) Disabling ports on Switch 0



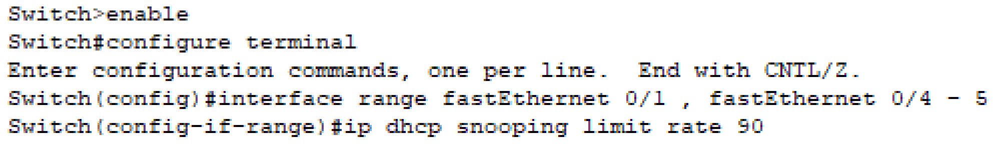
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/5 - 24, gigabitEthernet 0/1 - 2
Switch(config-if-range)#shutdown
```

б) Disabling ports on Switch 1

Figure 19. Disabling all ports that are not used on the switches

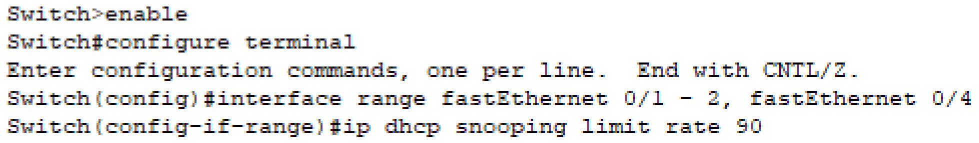
This was done to prevent an attacker from connecting through these ports.

7) Set the rate limiting on all untrusted ports on switches Switch 0 and Switch 1. The rate limit is 90 (Fig. 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
```

a) Speed limit on Switch 0



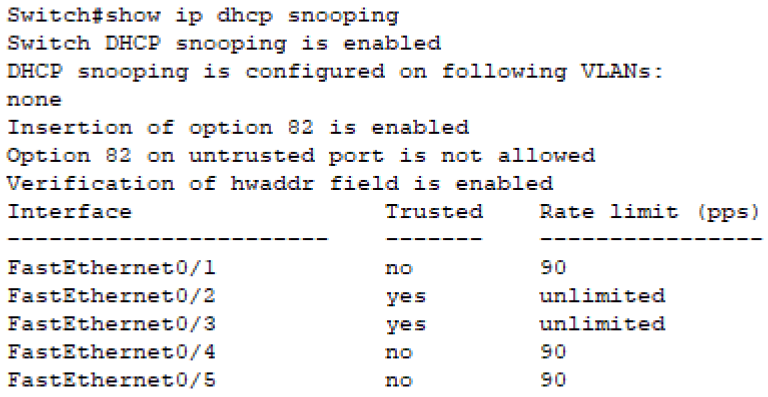
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1 - 2, fastEthernet 0/4
Switch(config-if-range)#ip dhcp snooping limit rate 90
```

b) Speed limit on Switch 1

Figure 20. Setting the speed limit on switches

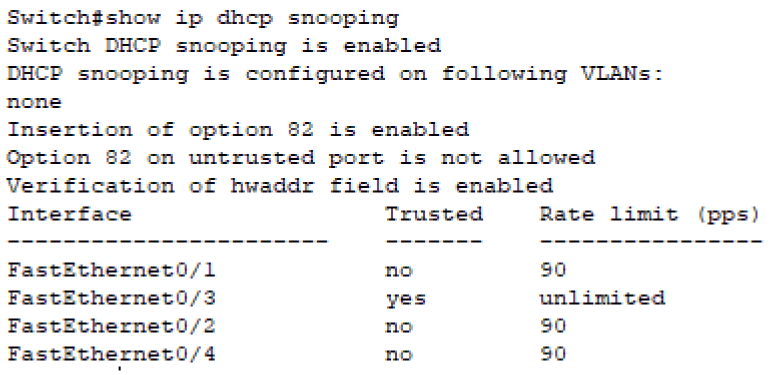
This was done to prevent DHCP Flood and Starvation attacks

8) The DHCP Snooping settings are checked (Fig. 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
```

a) Check for 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) Check for Switch 1

Figure 21. Checking the DHCP Snooping configuration on the switches

Conclusion:

In the course of the laboratory work, security tools for local networks were studied and successfully applied. In the first task, we configured Port Security on Switch 0. As a result, we set a limit on the maximum number of devices connected to a particular port, which allows us to effectively control access to the network. Modeling two possible cases of security breaches allowed us to check the efficiency and effectiveness of the applied measures.

The second task investigated the use of DHCP service protection. Legitimate and illegitimate DHCP servers were configured, and DHCP Snooping was used to ban illegitimate DHCP servers from the network. Trust ports are set up and speeds are limited on untrusted switch ports, which increases network security.

The overall goal of the lab was to familiarize students with the basic means of protecting local networks and the skills of their practical application. The acquired skills will allow you to effectively manage network security and prevent possible threats.