

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет безопасности информационных технологий

Дисциплина:

«Вычислительные сети и контроль безопасности в компьютерных сетях»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

«Безопасность канального уровня»

Выполнили:

Чу Ван Доан, студент группы N3347



(подпись)

Чан Бао Линь, студентка группы N3346



(подпись)

Проверил:

Савков Сергей Витальевич, инженер факультета БИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

СОДЕРЖАНИЕ

Содержание.....	2
Введение.....	3
1. Задание.....	4
2. Ход работы.....	4
2.1. Настройка лабораторного стенда в среде GNS3 согласно сетевой схеме.....	4
2.2. Создание необходимых VLAN на коммутаторах.....	4
2.3. Настройка режимов портов и привязка VLAN (access и trunk) на каждом коммутаторе в соответствии с заданной схемой. Настройка портов между коммутатором и роутером и перевод их в режим trunk.....	7
2.3.1. Настройка Trunk на IOU1.....	7
2.3.2. Настройка Trunk на IOU2.....	9
2.3.3. Настройка Trunk на IOU3.....	11
2.3.4. Настройка Access на IOU2.....	12
2.3.5. Настройка Access на IOU3.....	13
2.4. Создание сабинтерфейсов на роутере для каждой VLAN, назначение IP-адресов в формате 192.168.x.254, где x – номер VLAN.....	15
2.5. Настройка DHCP-сервера для каждой VLAN с диапазоном адресов от 10 до 100 в соответствии с IP-адресацией каждой VLAN.....	17
2.5.1. Настройка DHCP на маршрутизаторе R1.....	17
2.5.2. Запрос DHCP на устройствах.....	19
2.5.3. Проверка доступа.....	22
2.6. Настройка port security.....	23
2.6.1. Настройка port security на IOU3:.....	23
2.6.1.1. Настройка на порту Ethernet0/1 (Подключение PC3 - VLAN 120).....	23
2.6.1.2. Настройка на портах Ethernet0/2 и Ethernet0/3 (Подключение PC4, PC5 - VLAN 130).....	25
2.6.2. Проверка работы Port Security.....	26
2.7. Настройка DHCP snooping.....	27
2.7.1. Настройка DHCP snooping на IOU1.....	27
2.7.2. Настройка DHCP snooping на IOU2.....	29
2.7.3. Настройка DHCP snooping на IOU3.....	31
2.7.4. Проверка DHCP-запроса.....	33

ВВЕДЕНИЕ

Цель работы – Получить представление об основных угрозах сетевой безопасности на канальном уровне. Изучить базовые инструменты безопасности, используемые на коммутаторах.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Настроить лабораторный стенд в среде GNS3 согласно сетевой схеме;
2. На коммутаторах создать необходимые VLAN (по схеме, выданной преподавателем).
3. На каждом коммутаторе необходимо выставить режимы портов и задать VLAN (access и trunk) порты в соответствии с заданной схемой
4. Между коммутатором и роутером настроить порты и переключить их в режим транка
5. На роутере, на интерфейсе, подключенном к коммутатору - создать сабинтерфейсы, соответствующие созданным VLAN, назначить адрес для каждого сабинтерфейса в виде 192.168.x.254, где x-номер VLAN.
6. Настроить DHCP сервер для каждого VLAN с диапазоном адресов с 10 по 100 в соответствии с IP адресацией каждого VLAN
7. Настроить Port security с политикой реагирования (по заданию преподавателя)
8. Настроить DHCP snooping на каждом коммутаторе, протестировать подключение DHCP сервера к недоверенному порту.

1. Задание

- Вариант 1
- VLAN-ы: 110, 120, 130. Адресация по типу 10.1.130.0/25 (где 130 номер VLAN). Port security - на 3 коммутаторе, режим restrict

2. Ход работы

2.1. Настройка лабораторного стенда в среде GNS3 согласно сетевой схеме.

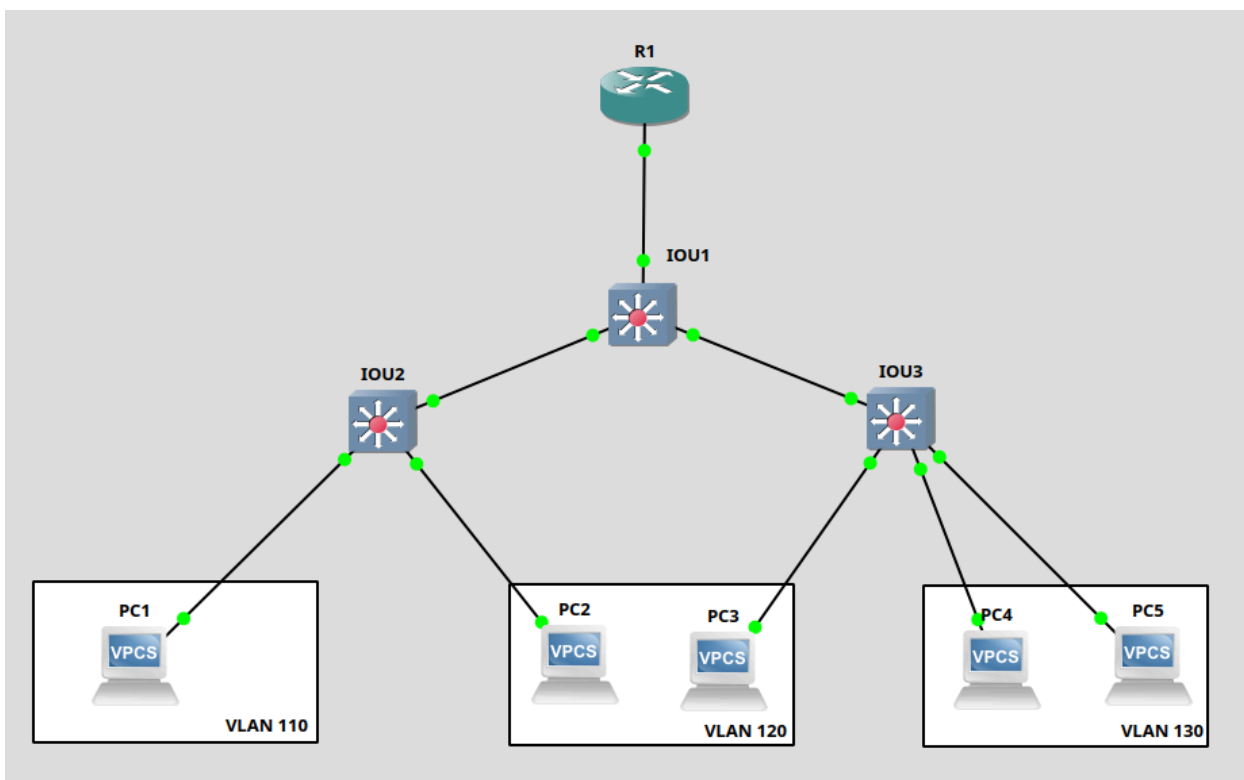


Рисунок 1 – Топология в GNS3

2.2. Создание необходимых VLAN на коммутаторах.

- Создание VLAN на IOU1:

```
enable
configure terminal
vlan 110
name Printer
vlan 120
name Computers
```

```

vlan 130

name Phones

exit

```

```

IOU1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#vlan 110
IOU1(config-vlan)#name Printer
IOU1(config-vlan)#vlan 120
IOU1(config-vlan)#name Computers
IOU1(config-vlan)#vlan 130
IOU1(config-vlan)#name Phones
IOU1(config-vlan)#exit
IOU1(config)#exit
IOU1#
*Mar 13 15:22:43.470: %SYS-5-CONFIG_I: Configured from console by console
IOU1#show vl
IOU1#show vlan b
IOU1#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Et0/0, Et0/1, Et0/2, Et0/3 Et1/0, Et1/1, Et1/2, Et1/3 Et2/0, Et2/1, Et2/2, Et2/3 Et3/0, Et3/1, Et3/2, Et3/3
110	Printer	active	
120	Computers	active	
130	Phones	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Рисунок 2 - Создание VLAN на IOU1.

- Создание VLAN на IOU2:

```

configure terminal

vlan 110

name Printer

vlan 120

name Computers

exit

```

```

IOU2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU2(config)#vlan 110
IOU2(config-vlan)#name Printer
IOU2(config-vlan)#vlan 120
IOU2(config-vlan)#name Computers
IOU2(config-vlan)#exit
IOU2(config)#exit
IOU2#
*Mar 13 15:23:49.221: %SYS-5-CONFIG_I: Configured from console by console
IOU2#show vlan br
IOU2#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Et0/0, Et0/1, Et0/2, Et0/3 Et1/0, Et1/1, Et1/2, Et1/3 Et2/0, Et2/1, Et2/2, Et2/3 Et3/0, Et3/1, Et3/2, Et3/3
110	Printer	active	
120	Computers	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Рисунок 3 - Создание VLAN на IOU2.

- Создание VLAN на IOU3:

```

configure terminal

vlan 120

name Computers

vlan 130

name Phones

exit

```

```

IOU3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU3(config)#vlan 120
IOU3(config-vlan)#name Computers
IOU3(config-vlan)#vlan 130
IOU3(config-vlan)#name Phones
IOU3(config-vlan)#exit
IOU3(config)#exit
IOU3#
IOU3#
IOU3#
*Mar 13 15:24:55.471: %SYS-5-CONFIG_I: Configured from console by console
IOU3#show vl
IOU3#show vlan b
IOU3#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Et0/0, Et0/1, Et0/2, Et0/3 Et1/0, Et1/1, Et1/2, Et1/3 Et2/0, Et2/1, Et2/2, Et2/3 Et3/0, Et3/1, Et3/2, Et3/3
120	Computers	active	
130	Phones	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Рисунок 4 - Создание VLAN на IOU3.

2.3. Настройка режимов портов и привязка VLAN (access и trunk) на каждом коммутаторе в соответствии с заданной схемой. Настройка портов между коммутатором и роутером и перевод их в режим trunk.

2.3.1. Настройка Trunk на IOU1.

- Позволяет передавать несколько VLAN через одно соединение
 - Порты Ethernet0/0, Ethernet0/1, Ethernet0/2 работают в режиме trunk, что позволяет IOU1 передавать несколько VLAN без необходимости в нескольких физических соединениях.
- Соединение и передача VLAN между сетевыми устройствами
 - Ethernet0/0: Trunk-подключение к IOU2, передача VLAN между IOU1 и IOU2.
 - Ethernet0/1: Trunk-подключение к IOU3, передача VLAN между IOU1 и IOU3.

- Ethernet0/2: Trunk-подключение к маршрутизатору R1, что позволяет маршрутизатору выполнять маршрутизацию между VLAN (Inter-VLAN Routing).
- Использование протокола 802.1Q (dot1q) для маркировки VLAN
 - Команда `switchport trunk encapsulation dot1q` позволяет IOS использовать стандарт IEEE 802.1Q, обеспечивая совместимость с другими сетевыми устройствами.
Поддержка связи между VLAN через маршрутизатор R1
 - Благодаря trunk-подключению к маршрутизатору R1, устройства из разных VLAN могут обмениваться данными через подинтерфейсы маршрутизатора (Router-on-a-stick).

```
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

```
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

```
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```



```

IOU1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#interface Ethernet0/0
IOU1(config-if)#switchport trunk encapsulation dot1q
IOU1(config-if)#switchport mode trunk
IOU1(config-if)#exit
IOU1(config)#interface Ethernet0/1
IOU1(config-if)#switchport trunk encapsulation dot1q
IOU1(config-if)#switchport mode trunk
IOU1(config-if)#exit
IOU1(config)#interface Ethernet0/2
IOU1(config-if)#switchport trunk encapsulation dot1q
IOU1(config-if)#switchport mode trunk
IOU1(config-if)#exit
IOU1(config)#exit
IOU1#
*Mar 13 15:55:29.283: %SYS-5-CONFIG_I: Configured from console by console
IOU1#show interfaces trunk

Port                Mode                Encapsulation    Status        Native vlan
Et0/0                on                  802.1q           trunking      1
Et0/1                on                  802.1q           trunking      1
Et0/2                on                  802.1q           trunking      1

Port                Vlans allowed on trunk
Et0/0                110,120,130
Et0/1                110,120,130
Et0/2                110,120,130

Port                Vlans allowed and active in management domain
Et0/0                110,120,130
Et0/1                110,120,130
Et0/2                110,120,130

Port                Vlans in spanning tree forwarding state and not pruned
Et0/0                110,120,130
Et0/1                110,120,130
Et0/2                110,120,130
IOU1#

```

Рисунок 5 - Настройка Trunk на IOU1.

2.3.2. Настройка Trunk на IOU2.

- Позволяет передавать несколько VLAN через одно соединение
 - Порт Ethernet0/0 настроен в режиме trunk, что позволяет IOU2 передавать данные нескольких VLAN через IOU1, вместо использования отдельных соединений для каждой VLAN.
- Соединение между IOU2 и IOU1 для работы VLAN

- Данные от PC1 (VLAN 110) и PC2 (VLAN 120) на IOU2 передаются в IOU1 через Trunk, что гарантирует возможность их взаимодействия с устройствами соответствующих VLAN в сети.
- Использование протокола 802.1Q (dot1q) для маркировки VLAN
 - switchport trunk encapsulation dot1q позволяет IOU2 использовать стандарт IEEE 802.1Q, обеспечивая правильную маркировку данных VLAN при передаче через IOU1.
- Поддержка связи между VLAN через маршрутизатор R1
 - Благодаря trunk-соединению с IOU1, устройства VLAN на IOU2 могут маршрутизироваться через маршрутизатор R1 для взаимодействия с другими VLAN.

```
configure terminal
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

```
IOU2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU2(config)#interface Ethernet0/0
IOU2(config-if)#switchport trunk encapsulation dot1q
IOU2(config-if)#switchport mode trunk
IOU2(config-if)#exit
IOU2(config)#exit
IOU2#
*Mar 13 15:59:56.630: %SYS-5-CONFIG_I: Configured from console by console
IOU2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	on	802.1q	trunking	1

```
Port      Vlans allowed on trunk
Et0/0     1-4094

Port      Vlans allowed and active in management domain
Et0/0     1,110,120

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     1,110,120
IOU2#
```

Рисунок 6 - Настройка Trunk на IOU2.

2.3.3. Настройка Trunk на IOU3

- Позволяет передавать несколько VLAN через одно соединение
 - Порт Ethernet0/0 настроен в режиме trunk, что позволяет IOU3 передавать данные нескольких VLAN через IOU1, вместо использования отдельных портов для каждой VLAN.
- Соединение IOU3 с IOU1 для корректной работы VLAN
 - Данные от PC3 (VLAN 120), PC4 и PC5 (VLAN 130) на IOU3 передаются через Trunk в IOU1, что обеспечивает их взаимодействие с устройствами соответствующих VLAN в сети.
- Использование протокола 802.1Q (dot1q) для маркировки VLAN
 - switchport trunk encapsulation dot1q позволяет IOU3 использовать стандарт IEEE 802.1Q, обеспечивая правильную маркировку данных VLAN при передаче через IOU1.
- Поддержка связи между VLAN через маршрутизатор R1
 - Благодаря trunk-соединению с IOU1, устройства VLAN на IOU3 могут маршрутизироваться через маршрутизатор R1 для взаимодействия с другими VLAN.

```
configure terminal
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

```

IOU3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU3(config)#interface Ethernet0/0
IOU3(config-if)#switchport trunk encapsulation dot1q
IOU3(config-if)#switchport mode trunk
IOU3(config-if)#exit
IOU3(config)#exit
IOU3#
*Mar 13 16:02:54.876: %SYS-5-CONFIG_I: Configured from console by console
IOU3#show interfaces trunk

Port      Mode           Encapsulation  Status        Native vlan
Et0/0     on             802.1q         trunking      1

Port      Vlans allowed on trunk
Et0/0     1-4094

Port      Vlans allowed and active in management domain
Et0/0     1,120,130

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     1,120,130
IOU3#

```

Рисунок 7 - Настройка Trunk на IOU3.

2.3.4. Настройка Access на IOU2

- Назначение VLAN для каждого порта на IOU2
 - Ethernet0/1 настроен в режиме Access VLAN 110, подключая PC1 к VLAN 110.
 - Ethernet0/2 настроен в режиме Access VLAN 120, подключая PC2 к VLAN 120.
- Позволяет ПК в одной VLAN взаимодействовать друг с другом
 - PC1 (VLAN 110) может общаться только с устройствами в VLAN 110.
 - PC2 (VLAN 120) может общаться только с устройствами в VLAN 120.
- Ограничение несанкционированного доступа между VLAN
 - Устройства в разных VLAN не могут взаимодействовать напрямую, что предотвращает конфликты и повышает безопасность сети.
- Поддержка связи между VLAN через маршрутизатор R1
 - Если PC1 (VLAN 110) хочет взаимодействовать с PC2 (VLAN 120), маршрутизация должна выполняться через R1 (Inter-VLAN Routing).

```

configure terminal
interface Ethernet0/1
switchport mode access
switchport access vlan 110
exit

interface Ethernet0/2
switchport mode access
switchport access vlan 120
exit

```

```

IOU2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU2(config)#interface Ethernet0/1
IOU2(config-if)#switchport mode access
IOU2(config-if)#switchport access vlan 110
IOU2(config-if)#exit
IOU2(config)#interface Ethernet0/2
IOU2(config-if)#switchport mode access
IOU2(config-if)#switchport access vlan 120
IOU2(config-if)#exit
IOU2(config)#exit
IOU2#
*Mar 13 16:21:37.481: %SYS-5-CONFIG_I: Configured from console by console
IOU2#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Et0/3, Et1/0, Et1/1, Et1/2 Et1/3, Et2/0, Et2/1, Et2/2 Et2/3, Et3/0, Et3/1, Et3/2 Et3/3
110	Printer	active	Et0/1
120	Computers	active	Et0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```

IOU2#

```

Рисунок 8 - Настройка Access на IOU2.

2.3.5. Настройка Access на IOU3

- Назначение VLAN для каждого порта на IOU3
 - Ethernet0/1 настроен как Access VLAN 120, подключая PC3 к VLAN 120.
 - Ethernet0/2-3 настроены как Access VLAN 130, подключая PC4 и PC5 к VLAN 130.
- Обеспечение правильного присвоения VLAN для устройств
 - PC3 может взаимодействовать только с устройствами в VLAN 120.

- PC4 и PC5 могут взаимодействовать только с устройствами в VLAN 130.
- Ограничение несанкционированного доступа между VLAN
 - Так как порты работают в режиме Access, устройства могут работать только в назначенной VLAN и не могут взаимодействовать напрямую с другими VLAN.
- Поддержка связи между VLAN через маршрутизатор R1
 - Если PC3 (VLAN 120) хочет взаимодействовать с PC4 или PC5 (VLAN 130), данные должны маршрутизироваться через R1 (Inter-VLAN Routing).

```
configure terminal
interface Ethernet0/1
switchport mode access
switchport access vlan 120
exit

interface range Ethernet0/2-3
switchport mode access
switchport access vlan 130
exit
```

```
IOU3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU3(config)#interface Ethernet0/1
IOU3(config-if)#switchport mode access
IOU3(config-if)#switchport access vlan 120
IOU3(config-if)#exit
IOU3(config)#interface range Ethernet0/2-3
IOU3(config-if-range)#switchport mode access
IOU3(config-if-range)#switchport access vlan 130
IOU3(config-if-range)#exit
IOU3(config)#exit
IOU3#
*Mar 13 16:33:35.111: %SYS-5-CONFIG_I: Configured from console by console
IOU3#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et1/0, Et1/1, Et1/2, Et1/3 Et2/0, Et2/1, Et2/2, Et2/3 Et3/0, Et3/1, Et3/2, Et3/3
120	Computers	active	Et0/1
130	Phones	active	Et0/2, Et0/3
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
IOU3#
```

Рисунок 9 - Настройка Access на IOU3.

2.4. Создание сабинтерфейсов на роутере для каждой VLAN, назначение IP-адресов в формате 192.168.x.254, где x – номер VLAN.

Значение создания подинтерфейсов на R1:

- Обеспечение связи между VLAN (Inter-VLAN Routing)
 - Так как коммутаторы передают данные только внутри одной VLAN, необходим маршрутизатор для маршрутизации между VLAN.
 - Созданные подинтерфейсы на Ethernet0/0 позволяют каждой VLAN иметь свой виртуальный интерфейс на маршрутизаторе.
- Использование протокола 802.1Q для маркировки VLAN
 - encapsulation dot1Q X → Назначает VLAN X для подинтерфейса.
 - При передаче трафика через маршрутизатор данные маркируются (tagged) по стандарту IEEE 802.1Q, чтобы маршрутизатор мог правильно идентифицировать VLAN.
- Назначение IP-адресов для каждой VLAN
 - ip address 192.168.X.254 255.255.255.0 → Каждая VLAN получает адрес шлюза по умолчанию (Default Gateway) для выхода за пределы своей VLAN.
 - Например:
 - VLAN 110: Gateway 192.168.110.254
 - VLAN 120: Gateway 192.168.120.254
 - VLAN 130: Gateway 192.168.130.254
- Обеспечение связи между устройствами в разных VLAN
 - Если PC1 (VLAN 110) хочет взаимодействовать с PC3 (VLAN 120), данные должны пройти через маршрутизатор R1, так как они находятся в разных VLAN.

```
enable
```

```
configure terminal
```

```
interface Ethernet0/0
```

```
no shutdown
```

```
exit
```

```
interface Ethernet0/0.110
```

```
encapsulation dot1Q 110
```

```
ip address 192.168.110.254 255.255.255.0
```

```
exit
```

```

interface Ethernet0/0.120
encapsulation dot1Q 120
ip address 192.168.120.254 255.255.255.0
exit

interface Ethernet0/0.130
encapsulation dot1Q 130
ip address 192.168.130.254 255.255.255.0
exit

```

```

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Ethernet0/0
R1(config-if)#no shutdown
R1(config-if)#
*Mar 13 16:46:14.899: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Mar 13 16:46:15.905: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R1(config-if)#exit
R1(config)#interface Ethernet0/0.110
R1(config-subif)#encapsulation dot1Q 110
R1(config-subif)#ip address 192.168.110.254 255.255.255.0
R1(config-subif)#exit
R1(config)#interface Ethernet0/0.120
R1(config-subif)#encapsulation dot1Q 120
R1(config-subif)#ip address 192.168.120.254 255.255.255.0
R1(config-subif)#exit
R1(config)#interface Ethernet0/0.130
R1(config-subif)#encapsulation dot1Q 130
R1(config-subif)#ip address 192.168.130.254 255.255.255.0
R1(config-subif)#exit
R1(config)#exit
R1#
*Mar 13 16:47:12.996: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip interfaces brief
      ^
% Invalid input detected at '^' marker.

R1#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	NVRAM	up	up
Ethernet0/0.110	192.168.110.254	YES	manual	up	up
Ethernet0/0.120	192.168.120.254	YES	manual	up	up
Ethernet0/0.130	192.168.130.254	YES	manual	up	up
Ethernet0/1	unassigned	YES	NVRAM	administratively down	down
Ethernet0/2	unassigned	YES	NVRAM	administratively down	down
Ethernet0/3	unassigned	YES	NVRAM	administratively down	down
Ethernet1/0	unassigned	YES	NVRAM	administratively down	down
Ethernet1/1	unassigned	YES	NVRAM	administratively down	down
Ethernet1/2	unassigned	YES	NVRAM	administratively down	down
Ethernet1/3	unassigned	YES	NVRAM	administratively down	down
Serial2/0	unassigned	YES	NVRAM	administratively down	down
Serial2/1	unassigned	YES	NVRAM	administratively down	down
Serial2/2	unassigned	YES	NVRAM	administratively down	down
Serial2/3	unassigned	YES	NVRAM	administratively down	down
Serial3/0	unassigned	YES	NVRAM	administratively down	down
Serial3/1	unassigned	YES	NVRAM	administratively down	down
Serial3/2	unassigned	YES	NVRAM	administratively down	down
Serial3/3	unassigned	YES	NVRAM	administratively down	down

Рисунок 8 - Настройка подинтерфейсов на маршрутизаторе R1.

2.5. Настройка DHCP-сервера для каждой VLAN с диапазоном адресов от 10 до 100 в соответствии с IP-адресацией каждой VLAN.

2.5.1. Настройка DHCP на маршрутизаторе R1

- DHCP (Dynamic Host Configuration Protocol) на маршрутизаторе используется для автоматической выдачи IP-адресов устройствам в сети. Вместо того чтобы назначать IP-адреса вручную для каждого устройства, DHCP позволяет управлять и распределять IP-адреса автоматически, быстро и эффективно.
- Исключение диапазона IP-адресов из выдачи (ip dhcp excluded-address)
 - ip dhcp excluded-address 192.168.X.1 192.168.X.10 → Исключает IP-адреса от .1 до .10, которые обычно предназначены для ключевых устройств (маршрутизатор, коммутаторы, серверы).
 - Предотвращает конфликты IP между DHCP и устройствами с ручной настройкой.
- Создание отдельных DHCP-пулов для разных типов устройств (ip dhcp pool)
 - Pool "Printer" (VLAN 110): Выдача IP для принтеров.
 - Pool "Computers" (VLAN 120): Выдача IP для компьютеров.
 - Pool "Phones" (VLAN 130): Выдача IP для IP-телефонов.
- Автоматическая выдача IP-адресов в заданном диапазоне
 - network 192.168.X.0 255.255.255.0 → Определяет диапазон IP-адресов, которые может выдавать DHCP.
 - Устройства получают IP автоматически, без необходимости ручной настройки.
- Настройка шлюза по умолчанию (default-router)
 - default-router 192.168.X.254 → Указывает шлюз по умолчанию для выхода за пределы VLAN.
- Настройка DNS-сервера (dns-server)
 - dns-server 8.8.8.8 → Назначает Google DNS для доступа к интернету.
- Время аренды IP-адреса (lease)
 - lease 7 → IP-адрес выделяется на 7 дней, после чего устройство может продлить аренду или запросить новый IP.

enable

configure terminal

ip dhcp excluded-address 192.168.110.1 192.168.110.10

```
ip dhcp pool Printer
network 192.168.110.0 255.255.255.0
default-router 192.168.110.254
dns-server 8.8.8.8
lease 7
exit
```

```
ip dhcp excluded-address 192.168.120.1 192.168.120.10
ip dhcp pool Computers
network 192.168.120.0 255.255.255.0
default-router 192.168.120.254
dns-server 8.8.8.8
lease 7
exit
```

```
ip dhcp excluded-address 192.168.130.1 192.168.130.10
ip dhcp pool Phones
network 192.168.130.0 255.255.255.0
default-router 192.168.130.254
dns-server 8.8.8.8
lease 7
exit
```

```

R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.110.1 192.168.110.10
R1(config)#ip dhcp pool Printer
R1(dhcp-config)#network 192.168.110.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.110.254
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#lease 7
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.120.1 192.168.120.10
R1(config)#ip dhcp pool Computers
R1(dhcp-config)#network 192.168.120.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.120.254
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#lease 7
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.130.1 192.168.130.10
R1(config)#ip dhcp pool Phones
R1(dhcp-config)#network 192.168.130.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.130.254
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#lease 7
R1(dhcp-config)#exit
R1(config)#exit
R1#
*Mar 13 17:05:06.747: %SYS-5-CONFIG_I: Configured from console by console

```

Рисунок 9 - Настройка DHCP на маршрутизаторе R1.

2.5.2. Запрос DHCP на устройствах.

```

PC1> dhcp
DDORA IP 192.168.110.11/24 GW 192.168.110.254

PC1> show ip

NAME           : PC1[1]
IP/MASK        : 192.168.110.11/24
GATEWAY        : 192.168.110.254
DNS            : 8.8.8.8
DHCP SERVER    : 192.168.110.254
DHCP LEASE     : 604781, 604800/302400/529200
MAC            : 00:50:79:66:68:00
LPORT          : 20016
RHOST:PORT     : 127.0.0.1:20017
MTU            : 1500

```

Рисунок 10 - Запрос DHCP на PC1

```
PC2> dhcp
DDORA IP 192.168.120.11/24 GW 192.168.120.254

PC2> show ip

NAME           : PC2[1]
IP/MASK        : 192.168.120.11/24
GATEWAY        : 192.168.120.254
DNS            : 8.8.8.8
DHCP SERVER    : 192.168.120.254
DHCP LEASE     : 604756, 604800/302400/529200
MAC            : 00:50:79:66:68:01
LPORT          : 20018
RHOST:PORT     : 127.0.0.1:20019
MTU            : 1500
```

Рисунок 11 - Запрос DHCP на PC2

```
PC3> dhcp
DDORA IP 192.168.120.12/24 GW 192.168.120.254

PC3> show ip

NAME           : PC3[1]
IP/MASK        : 192.168.120.12/24
GATEWAY        : 192.168.120.254
DNS            : 8.8.8.8
DHCP SERVER    : 192.168.120.254
DHCP LEASE     : 604776, 604800/302400/529200
MAC            : 00:50:79:66:68:02
LPORT          : 20020
RHOST:PORT     : 127.0.0.1:20021
MTU            : 1500
```

Рисунок 12 - Запрос DHCP на PC3

```
PC4> dhcp
DDORA IP 192.168.130.11/24 GW 192.168.130.254

PC4> show ip

NAME           : PC4[1]
IP/MASK        : 192.168.130.11/24
GATEWAY        : 192.168.130.254
DNS            : 8.8.8.8
DHCP SERVER    : 192.168.130.254
DHCP LEASE     : 604776, 604800/302400/529200
MAC            : 00:50:79:66:68:03
LPORT          : 20022
RHOST:PORT     : 127.0.0.1:20023
MTU            : 1500
```

Рисунок 13 - Запрос DHCP на PC4

```
PC5> dhcp
DDORA IP 192.168.130.12/24 GW 192.168.130.254

PC5> show ip

NAME           : PC5[1]
IP/MASK        : 192.168.130.12/24
GATEWAY        : 192.168.130.254
DNS            : 8.8.8.8
DHCP SERVER    : 192.168.130.254
DHCP LEASE     : 604775, 604800/302400/529200
MAC            : 00:50:79:66:68:04
LPORT          : 20024
RHOST:PORT     : 127.0.0.1:20025
MTU            : 1500
```

Рисунок 14 - Запрос DHCP на PC5

2.5.3. Проверка доступа

```
PC1> ping 192.168.120.254

84 bytes from 192.168.120.254 icmp_seq=1 ttl=255 time=5.419 ms
84 bytes from 192.168.120.254 icmp_seq=2 ttl=255 time=4.156 ms
84 bytes from 192.168.120.254 icmp_seq=3 ttl=255 time=4.164 ms
84 bytes from 192.168.120.254 icmp_seq=4 ttl=255 time=0.869 ms
84 bytes from 192.168.120.254 icmp_seq=5 ttl=255 time=2.541 ms

PC1>
PC1> ping 192.168.130.254

84 bytes from 192.168.130.254 icmp_seq=1 ttl=255 time=4.155 ms
84 bytes from 192.168.130.254 icmp_seq=2 ttl=255 time=2.909 ms
84 bytes from 192.168.130.254 icmp_seq=3 ttl=255 time=3.178 ms
84 bytes from 192.168.130.254 icmp_seq=4 ttl=255 time=3.097 ms
84 bytes from 192.168.130.254 icmp_seq=5 ttl=255 time=2.324 ms
^C
```

Рисунок 15 - Проверка доступа между разными VLAN с PC1

```
PC3> ping 192.168.110.11

84 bytes from 192.168.110.11 icmp_seq=1 ttl=63 time=3.402 ms
84 bytes from 192.168.110.11 icmp_seq=2 ttl=63 time=3.948 ms
84 bytes from 192.168.110.11 icmp_seq=3 ttl=63 time=5.742 ms
84 bytes from 192.168.110.11 icmp_seq=4 ttl=63 time=7.466 ms
84 bytes from 192.168.110.11 icmp_seq=5 ttl=63 time=2.649 ms
^C
PC3> ping 192.168.130.11

84 bytes from 192.168.130.11 icmp_seq=1 ttl=63 time=5.078 ms
84 bytes from 192.168.130.11 icmp_seq=2 ttl=63 time=8.200 ms
84 bytes from 192.168.130.11 icmp_seq=3 ttl=63 time=3.266 ms
84 bytes from 192.168.130.11 icmp_seq=4 ttl=63 time=5.535 ms
84 bytes from 192.168.130.11 icmp_seq=5 ttl=63 time=8.759 ms
^C
```

Рисунок 16 - Проверка доступа между разными VLAN с PC3

```

PC5> ping 192.168.110.11

84 bytes from 192.168.110.11 icmp_seq=1 ttl=63 time=7.959 ms
84 bytes from 192.168.110.11 icmp_seq=2 ttl=63 time=8.267 ms
84 bytes from 192.168.110.11 icmp_seq=3 ttl=63 time=8.419 ms
84 bytes from 192.168.110.11 icmp_seq=4 ttl=63 time=1.662 ms
84 bytes from 192.168.110.11 icmp_seq=5 ttl=63 time=8.829 ms
^C
PC5> ping 192.168.120.12

84 bytes from 192.168.120.12 icmp_seq=1 ttl=63 time=10.297 ms
84 bytes from 192.168.120.12 icmp_seq=2 ttl=63 time=5.077 ms
84 bytes from 192.168.120.12 icmp_seq=3 ttl=63 time=8.946 ms
84 bytes from 192.168.120.12 icmp_seq=4 ttl=63 time=8.404 ms
^C

```

Рисунок 17 - Проверка доступа между разными VLAN с PC5

2.6. Настройка port security

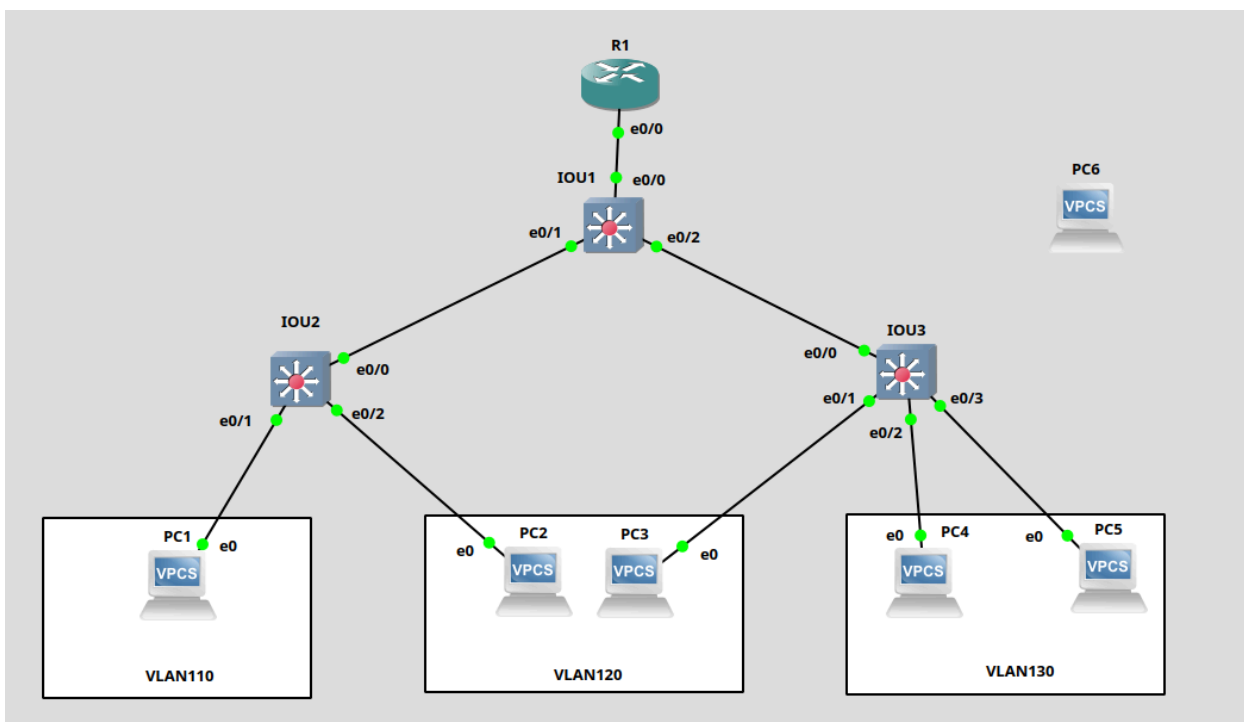


Рисунок 18 - Добавление PC6 в лабораторный стенд

2.6.1. Настройка port security на IOU3:

2.6.1.1. Настройка на порту Ethernet0/1 (Подключение PC3 - VLAN 120).

- Настройка порта Access для VLAN 120, разрешение подключения только для PC3.

- Ограничение до одного MAC-адреса, чтобы только PC3 мог использовать этот порт.
- Режим Restrict: при обнаружении неизвестного MAC-адреса порт не выключается (не уходит в shutdown), но пакеты блокируются, а событие фиксируется в логах.
- Режим Sticky: автоматическое обучение и сохранение первого MAC-адреса, подключенного к порту.

```

configure terminal
interface Ethernet0/1
switchport mode access
switchport access vlan 120
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security mac-address sticky
no shutdown
exit

```

```

IOU3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU3(config)#interface Ethernet0/1
IOU3(config-if)#switchport mode access
IOU3(config-if)#switchport access vlan 120
IOU3(config-if)#switchport port-security
IOU3(config-if)#switchport port-security maximum 1
IOU3(config-if)#switchport port-security violation restrict
IOU3(config-if)#switchport port-security mac-address sticky
IOU3(config-if)#no shutdown
IOU3(config-if)#exit
IOU3(config)#exit
IOU3#
*Mar 13 17:52:53.265: %SYS-5-CONFIG_I: Configured from console by console
IOU3#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Et0/1                1                0                0                Restrict
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096

```

Рисунок 19 - Настройка на порту Ethernet0/1

2.6.1.2. Настройка на портах Ethernet0/2 и Ethernet0/3 (Подключение PC4, PC5 - VLAN 130)

- Настройка портов Access для VLAN 130, разрешение подключения только для PC4 и PC5.
- Ограничение до одного MAC-адреса на каждый порт, чтобы только PC4 или PC5 могли подключаться.
- Режим Restrict: если будет подключено неизвестное устройство, порт останется активным, но пакеты будут блокироваться, а событие фиксироваться в логах.
- Режим Sticky: коммутатор автоматически запоминает первый корректный MAC-адрес, подключенный к порту.

```
configure terminal
interface range Ethernet0/2-3
switchport mode access
switchport access vlan 130
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security mac-address sticky
no shutdown
exit
```

```
IOU3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU3(config)#interface range Ethernet0/2-3
IOU3(config-if-range)#switchport mode access
IOU3(config-if-range)#switchport access vlan 130
IOU3(config-if-range)#switchport port-security
IOU3(config-if-range)#switchport port-security maximum 1
IOU3(config-if-range)#switchport port-security violation restrict
IOU3(config-if-range)#switchport port-security mac-address sticky
IOU3(config-if-range)#no shutdown
IOU3(config-if-range)#exit
IOU3(config)#exit
IOU3#
*Mar 13 18:00:53.535: %SYS-5-CONFIG_I: Configured from console by console
IOU3#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)           (Count)           (Count)
-----
    Et0/1         1             0              0              Restrict
    Et0/2         1             0              0              Restrict
    Et0/3         1             0              0              Restrict
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Рисунок 20 - Настройка на порту Ethernet0/2-3

2.6.2. Проверка работы Port Security

```
PC3> ping 192.168.120.11
84 bytes from 192.168.120.11 icmp_seq=1 ttl=64 time=4.069 ms
84 bytes from 192.168.120.11 icmp_seq=2 ttl=64 time=5.893 ms
84 bytes from 192.168.120.11 icmp_seq=3 ttl=64 time=5.406 ms
84 bytes from 192.168.120.11 icmp_seq=4 ttl=64 time=2.028 ms
84 bytes from 192.168.120.11 icmp_seq=5 ttl=64 time=3.515 ms
^C
```

Рисунок 21 - PC3 — третье устройство, подключенное к IOU3.

```
IOU3#show port-security interface Ethernet0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0050.7966.6802:120
Security Violation Count : 0
```

Рисунок 22 - Проверьте настройки

- Мы подключаем PC6 к IOU3 и проводим проверку.

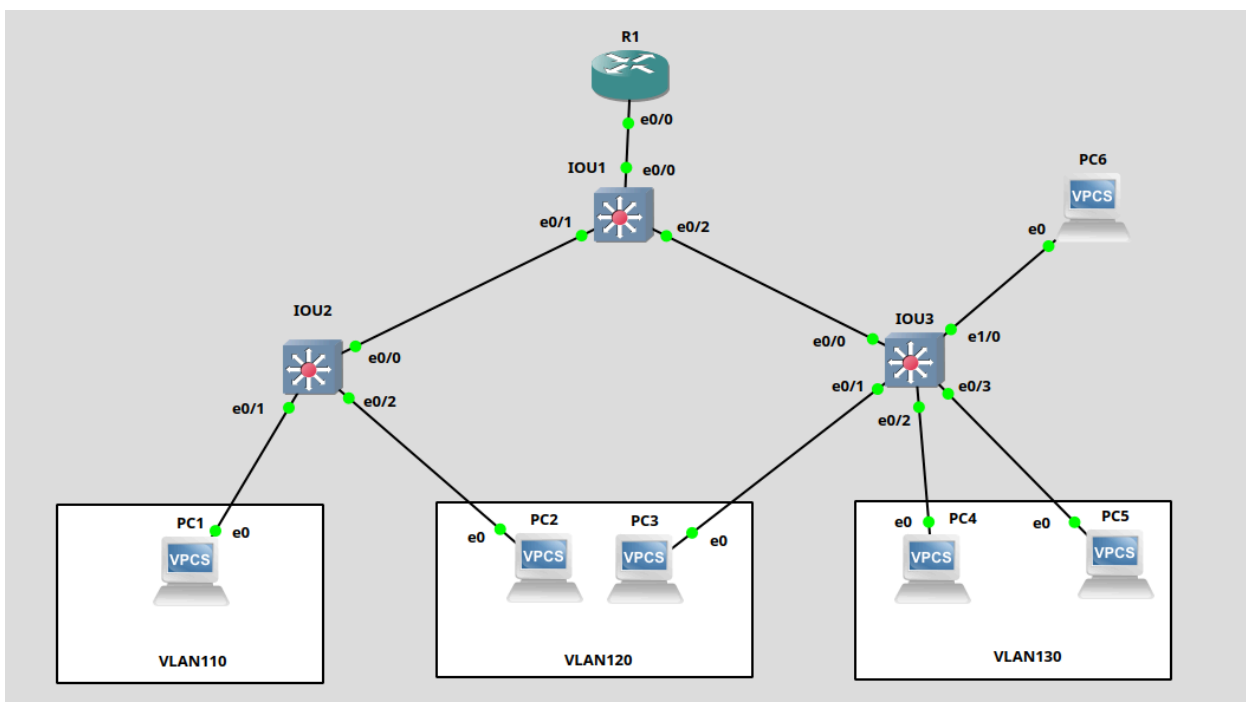


Рисунок 23 - PC6

```
PC6> dhcp
DDD
Can't find dhcp server

PC6> ping 192.168.120.12

host (192.168.120.12) not reachable

PC6> ping 192.168.120.254

host (192.168.120.254) not reachable
```

Рисунок 24 - Проверка работоспособности port security

2.7. Настройка DHCP snooping

2.7.1. Настройка DHCP snooping на IOU1

- Включите DHCP Snooping для защиты сети от поддельных DHCP-серверов.
- Применяйте только для VLAN 110, 120, 130, чтобы контролировать выдачу IP-адресов в необходимых VLAN.
- Назначьте порт e0/0 как доверенный (trusted), так как он соединен с R1 (настоящий DHCP-сервер), позволяя передачу DHCP Offer и DHCP ACK.

- Назначьте порты e0/1 и e0/2 как доверенные (trusted), чтобы разрешить передачу DHCP между коммутаторами (IOU1, IOU2, IOU3).
- Остальные порты по умолчанию недоверенные (untrusted), блокируют DHCP Offer от несанкционированных устройств, предотвращая DHCP Spoofing.

```
configure terminal
ip dhcp snooping
ip dhcp snooping vlan 110,120,130
```

```
interface Ethernet0/0
ip dhcp snooping trust
exit
```

```
interface Ethernet0/1
ip dhcp snooping trust
exit
```

```
interface Ethernet0/2
ip dhcp snooping trust
exit
```

```

IOU1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#ip dhcp snooping
IOU1(config)#ip dhcp snooping vlan 110,120,130
IOU1(config)#interface Ethernet0/0
IOU1(config-if)# ip dhcp snooping trust
IOU1(config-if)#exit
IOU1(config)#interface Ethernet0/1
IOU1(config-if)# ip dhcp snooping trust
IOU1(config-if)#exit
IOU1(config)#interface Ethernet0/2
IOU1(config-if)# ip dhcp snooping trust
IOU1(config-if)#exit
IOU1(config)#exit
IOU1#
*Mar 13 18:38:50.580: %SYS-5-CONFIG_I: Configured from console by console
IOU1#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
110,120,130
DHCP snooping is operational on following VLANs:
110,120,130
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0200 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0              yes       yes             unlimited
  Custom circuit-ids:
Ethernet0/1              yes       yes             unlimited
  Custom circuit-ids:
Ethernet0/2              yes       yes             unlimited
  Custom circuit-ids:
IOU1#

```

Рисунок 25 - Настройка DHCP snooping на IOU1

2.7.2. Настройка DHCP snooping на IOU2.

- Включите DHCP Snooping для защиты VLAN 110, 120, 130 от поддельных DHCP-серверов.
- Применяйте только для VLAN 110, 120, 130, чтобы контролировать выдачу IP-адресов в необходимых VLAN.

- Назначьте порт e0/0 как доверенный (trusted), так как он соединен с IOU1 (центральный коммутатор, подключенный к DHCP-серверу R1), позволяя передачу DHCP.
- Порты e0/1 и e0/2 являются недоверенными (untrusted), так как они подключены к PC1 и PC2, предотвращая подмену устройств в качестве DHCP-сервера.

```
configure terminal
ip dhcp snooping
ip dhcp snooping vlan 110,120,130
interface Ethernet0/0
ip dhcp snooping trust
exit
interface Ethernet0/1
no ip dhcp snooping trust
exit
interface Ethernet0/2
no ip dhcp snooping trust
exit
```

```

IOU2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU2(config)#ip dhcp snooping
IOU2(config)#ip dhcp snooping vlan 110,120,130
IOU2(config)#interface Ethernet0/0
IOU2(config-if)#ip dhcp snooping trust
IOU2(config-if)#exit
IOU2(config)#interface Ethernet0/1
IOU2(config-if)#no ip dhcp snooping trust
IOU2(config-if)#exit
IOU2(config)#interface Ethernet0/2
IOU2(config-if)#no ip dhcp snooping trust
IOU2(config-if)#exit
IOU2(config)#exit
IOU2#
*Mar 13 18:58:29.254: %SYS-5-CONFIG_I: Configured from console by console
IOU2#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleanig is disabled
DHCP snooping is configured on following VLANs:
110,120,130
DHCP snooping is operational on following VLANs:
110,120,130
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0300 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0              yes        yes              unlimited
  Custom circuit-ids:
IOU2#

```

Рисунок 26 - Настройка DHCP snooping на IOU2

2.7.3. Настройка DHCP snooping на IOU3

- Включен DHCP Snooping, но ни один порт не блокируется.
 - DHCP Snooping активирован для VLAN 110, 120, 130.
 - Однако все порты являются доверенными (trusted), то есть коммутатор не фильтрует DHCP Offer ни от одного источника.
- Разрешена передача DHCP-пакетов на всех портах.
 - Поскольку все порты (Ethernet0/0, Ethernet0/1, Ethernet0/2, Ethernet0/3, Ethernet1/0) настроены как trusted, коммутатор не блокирует DHCP Offer или DHCP ACK для любых устройств.
- Отсутствует защита от DHCP Spoofing на IOU3.

- Злоумышленник с поддельным DHCP-сервером может отправлять DHCP Offer без ограничений.
- Это может привести к тому, что ПК получают некорректные IP-адреса от несанкционированного DHCP-сервера в сети.

```
configure terminal
ip dhcp snooping
ip dhcp snooping vlan 110,120,130
interface Ethernet0/0
ip dhcp snooping trust
exit
interface Ethernet0/1
ip dhcp snooping trust
exit
interface Ethernet0/2
ip dhcp snooping trust
exit
interface Ethernet0/3
ip dhcp snooping trust
exit
interface Ethernet1/0
ip dhcp snooping trust
exit
```



```

IOU3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU3(config)#ip dhcp snooping
IOU3(config)#ip dhcp snooping vlan 110,120,130
IOU3(config)#interface Ethernet0/0
IOU3(config-if)#ip dhcp snooping trust
IOU3(config-if)#exit
IOU3(config)#interface Ethernet0/1
IOU3(config-if)#ip dhcp snooping trust
IOU3(config-if)#exit
IOU3(config)#interface Ethernet0/2
IOU3(config-if)#ip dhcp snooping trust
IOU3(config-if)#exit
IOU3(config)#interface Ethernet0/3
IOU3(config-if)#exit
IOU3(config)#exit
IOU3#
*Mar 13 19:07:07.834: %SYS-5-CONFIG_I: Configured from console by console
IOU3#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleanig is disabled
DHCP snooping is configured on following VLANs:
110,120,130
DHCPsnooping is operational on following VLANs:
110,120,130
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0400 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

```

Interface	Trusted	Allow option	Rate limit (pps)
Ethernet0/0	yes	yes	unlimited
Custom circuit-ids:			
Ethernet0/1	yes	yes	unlimited
Custom circuit-ids:			
Ethernet0/2	yes	yes	unlimited
Custom circuit-ids:			

```

IOU3#
IOU3#

```

Рисунок 27 - Настройка DHCP snooping на IOU2

2.7.4. Проверка DHCP-запроса

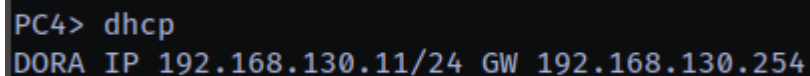
```

PC1> dhcp
DDD
Can't find dhcp server

```

Рисунок 28 - PC1 не может получить IP-адрес от DHCP-сервера.

- Порт Ethernet0/0 на IOU2 является доверенным (trusted), что позволяет ему получать и передавать DHCP-пакеты от IOU1.
- Порты Ethernet0/1, Ethernet0/2 (подключенные к PC1, PC2) являются недоверенными (untrusted), поэтому:
 - Блокируют DHCP Offer от R1 для PC1 и PC2.
 - PC1 и PC2 не могут получить IP-адрес от DHCP-сервера.
 - Если PC1 или PC2 попытаются запустить поддельный DHCP-сервер, их DHCP-пакеты будут отфильтрованы и удалены.



```
PC4> dhcp
DORA IP 192.168.130.11/24 GW 192.168.130.254
```

Рисунок 28 - PC4 получил правильный IP-адрес от DHCP-сервера (так как порт является доверенным).

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы были решены следующие задачи:

- настройка лабораторной среды в GNS3 в соответствии с предоставленной сетевой схемой.
- создание необходимых VLAN на коммутаторах в соответствии со схемой, предоставленной преподавателем.
- настройка режимов портов на каждом коммутаторе и задание VLAN (access и trunk) портов в соответствии с схемой.
- конфигурация портов между коммутаторами и маршрутизатором, перевод их в режим транка.
- создание сабинтерфейсов на роутере для каждого VLAN с адресацией 192.168.x.254, где x - номер VLAN.
- настройка DHCP-сервера для каждого VLAN с диапазоном адресов от 10 до 100 в соответствии с IP-адресацией каждого VLAN.
- настройка Port Security с учетом политики реагирования, установленной преподавателем.
- настройка DHCP Snooping на каждом коммутаторе, с последующим тестированием подключения DHCP-сервера к недоверенному порту.

Таким образом, все поставленные задачи успешно выполнены, и цель лабораторной работы достигнута.