**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**»

**Выполнил:**

Молитвин Илья Алексеевич, студент группы N3Изображение выглядит как текст, соединитель

Контент, сгенерированный ИИ, может содержать ошибки.345

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Бучаев Абдулхамид Яхьяевич

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Содержание**

[1 БЕЗОПАСНОСТЬ КАНАЛЬНОГО УРОВНЯ 4](#_30j0zll)

[1.1 Ход работы 4](#_1fob9te)

[1.1.1 Создание лабораторного стенда 4](#_3znysh7)

[1.1.2 Создание VLAN 4](#_2et92p0)

[1.1.3 Настройка портов на коммутаторах и роутере 5](#_uh6smaxfica8)

[1.1.4 Создание сабинтерфейсов 7](#_foh8bz2nelwb)

[1.1.5 Работа с DHCP 8](#_vo72fq6vaxy8)

[1.1.6 Port Security 11](#_3dy6vkm)

[1.1.7 DHCP Snooping 12](#_1t3h5sf)

**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:

− настроить лабораторный стенд в среде GNS3 согласно сетевой схеме;

− на коммутаторах создать необходимые VLAN (по схеме, выданной

преподавателем);

− на каждом коммутаторе необходимо выставить режимы портов и задать

VLAN (access и trunk) порты в соответствии с заданной схемой;

− между коммутатором и роутером настроить порты и переключить их в режим

транка;

− на роутере, на интерфейсе, подключенном к коммутатору создать

сабинтерфейсы, соответствующие созданным VLAN, назначить адрес для каждого

сабинтерфейса в виде 192.168.х.1, где х-номер VLAN;

− настроить DHCP сервер для каждого VLAN c диапазоном адресов в

соответствии с IP адресацией каждого VLAN;

− настроить Port Security c политикой реагирования (по заданию

преподавателя);

− настроить DHCP Snooping на каждом коммутаторе, протестировать

подключение DHCP сервера к недоверенному порту;

− результаты выполнения работы оформить в виде отчета.

# **БЕЗОПАСНОСТЬ КАНАЛЬНОГО УРОВНЯ**

## **Ход работы**

Моделирование сетевой схемы в ПО GNS3 с использованием базовых инструментов для обеспечения безопасности канального уровня.

### **Создание лабораторного стенда**

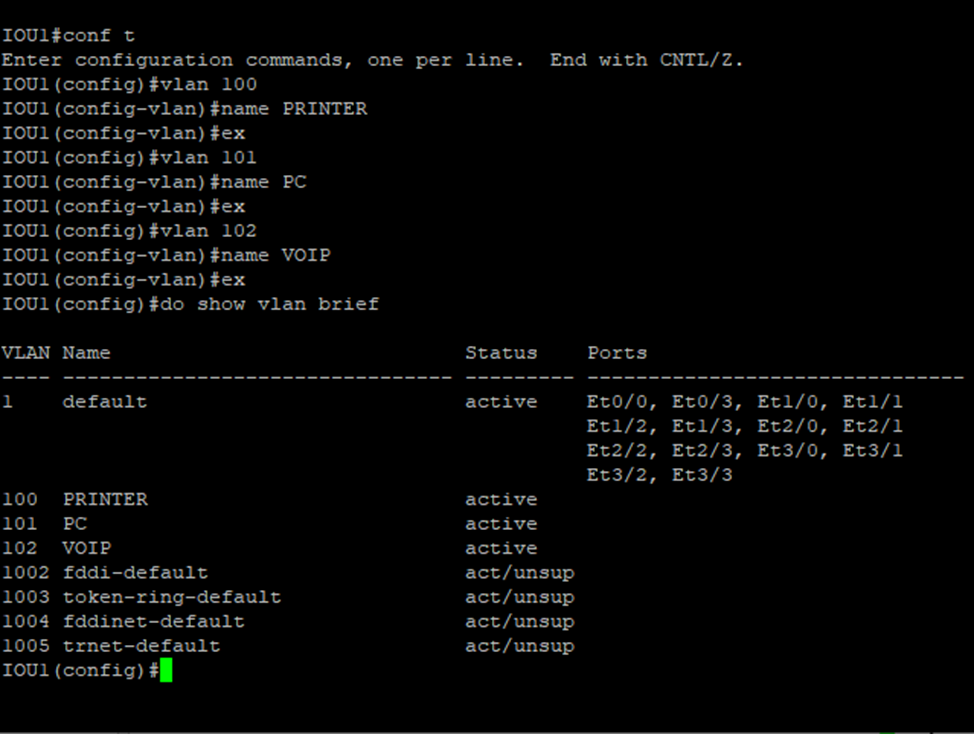
Создадим лабораторный стенд согласно сетевой схеме (рисунок 1). Изображение выглядит как диаграмма, текст, снимок экрана, дизайн

Контент, сгенерированный ИИ, может содержать ошибки.

1. Лабораторный стенд

### **Создание VLAN**

Теперь на коммутаторах создадим 3 VLAN, с помощью команды *vlan номер*, затем ведем show vlan brief, чтобы увидеть информацию о созданных VLAN.



1. Создание VLAN

### **Настройка портов на коммутаторах и роутере**

Схема назначения портов

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **IOU1** | **IOU2** | **IOU3** |
| e0/0 | Trunk to R1 | Trunk to IOU1 | Trunk to IOU1 |
| e0/1 | Trunk to IOU2 | Access (100) | Access (101) |
| e0/2 | Trunk to IOU3 | Access (100) | Access (102) |
| e0/3 |  |  | Access (102) |
| **…** |  |  |  |

Таблица 1

По умолчанию все порты настроены как Access. Чтобы поменять режим на Trunk,

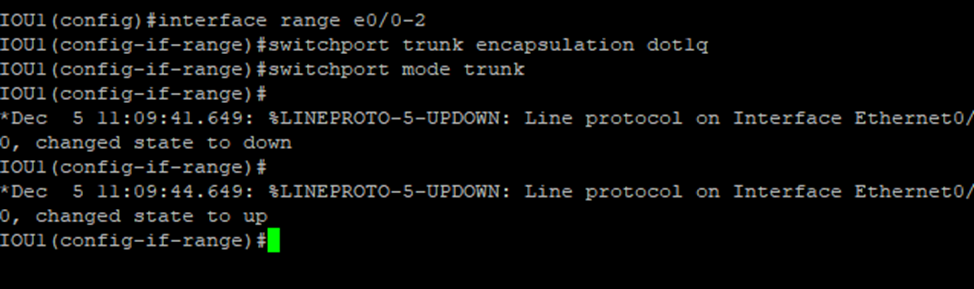
необходимо выбрать интерфейс порта, на который мы ставим данный режим, с помощью

команды interface выбранный порт (для удобства можно указать несколько портов с

помощью interface range выбранные порты). Далее явно указываем тип инкапсуляции для

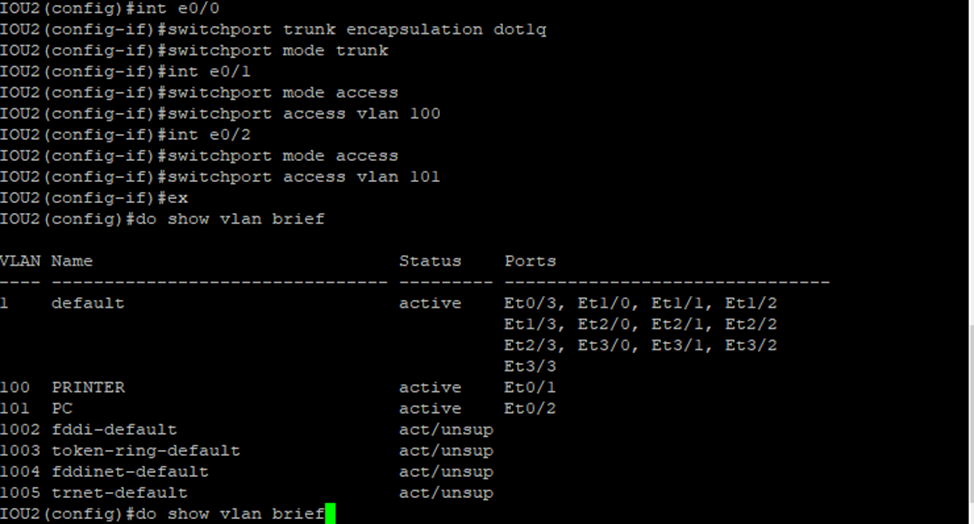
конкретного интерфейса, путем ввода switchport trunk encapsulation dot1q. И наконец

переведем интерфейс в режим trunk командой switchport mode trunk (рисунок 3).

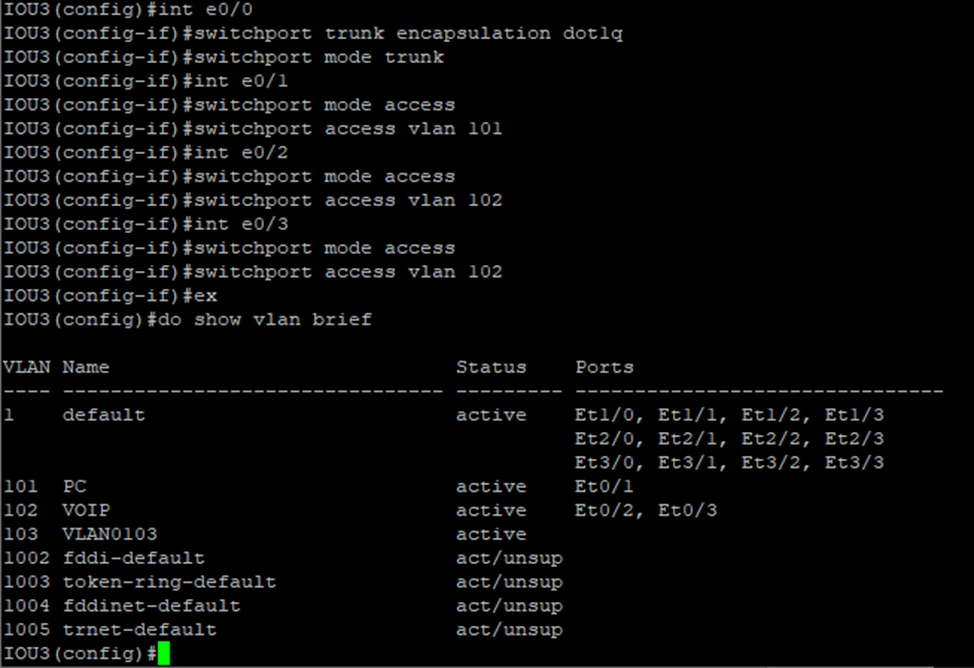


1. Настройка Trunk на IOU1

На коммутаторах IOU2 (рисунок 4) и IOU3 (рисунок 5) помимо trunk-портов также назначаем access-порты. Выбрав нужный интерфейс, вводим switchport mode access и потом switchport access vlan номер\_VLAN. Команда show vlan brief помогает убедиться, что порты назначены верно.



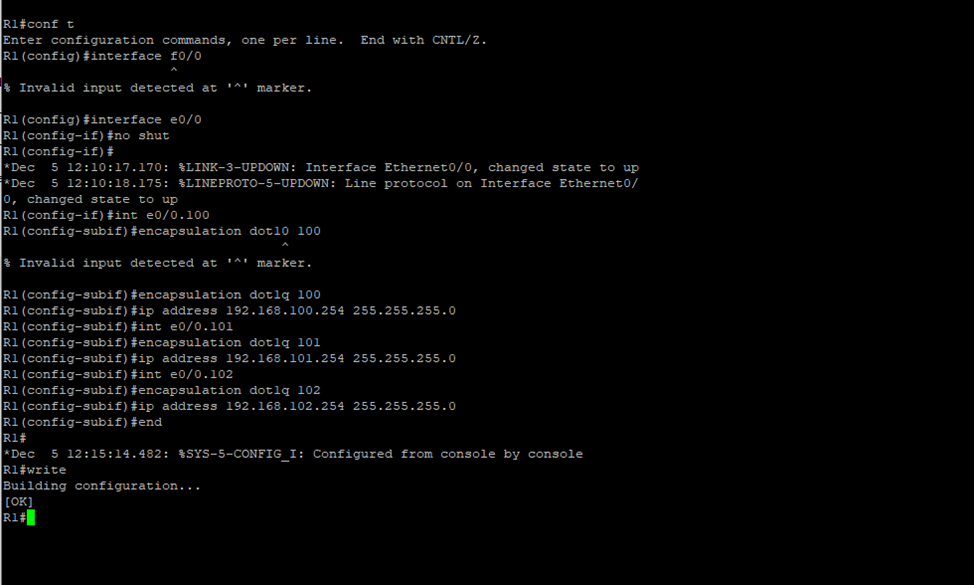
1. *Настройка портов на IOU2*

**

1. *Настройка портов на IOU3*

### **Создание сабинтерфейсов**

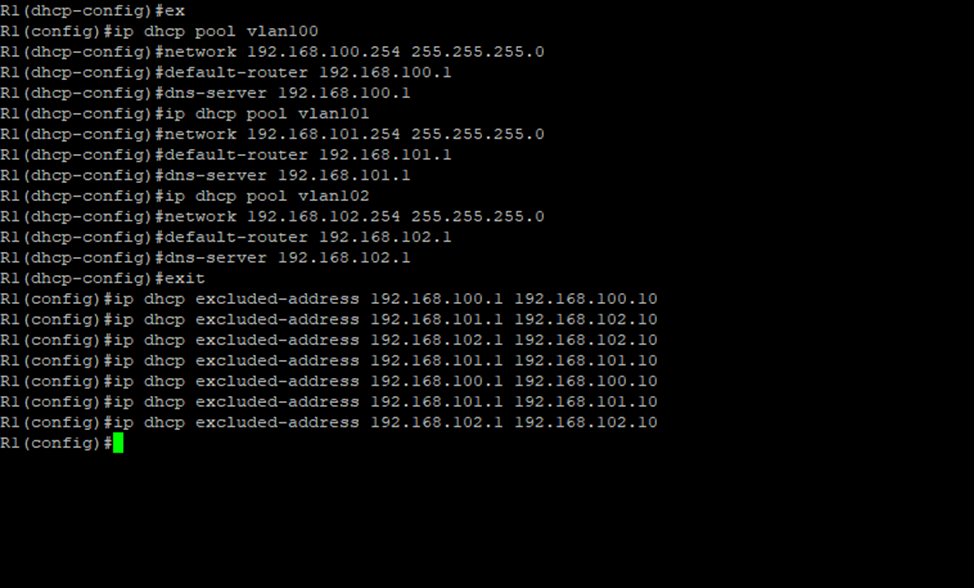
На роутере R1, на интерфейсе, подключенном к коммутатору IOU1 (в нашем случае e0/1), создаем и настраиваем сабинтерфейсы (e0/1.101, e0/1.102 и e0/1.103) с соответствующими IP-адресами (в виде 192.168.х.1, где х-номер VLAN) для каждого VLAN (рисунок 6).

**

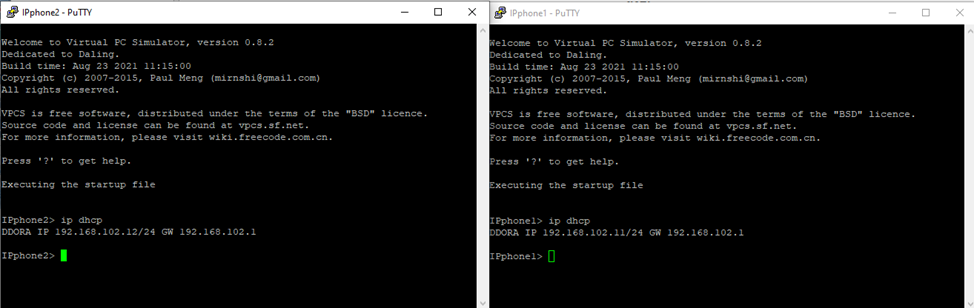
1. *Создание сабинтерфейсов*

### **Работа с DHCP**

В нашей сети мы настроим DHCP сервер для каждого VLAN. Создадим пул адресов для каждого VLAN. Введем ip dhcp pool vlanномер. Далее указываем network, default-router и dns-server (адрес 192.168.x.1, где x – номер VLAN). Чтобы ограничить диапазон адресов введем ip dhcp excluded-address диапозон\_адресов (рисунок 7).

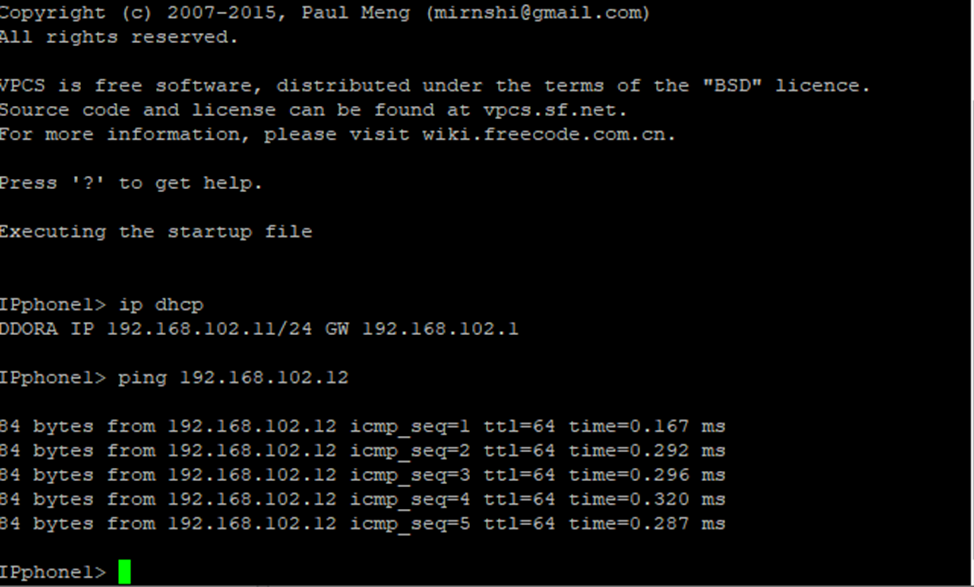
**

1. *Настройка DHCP-пулов*

**

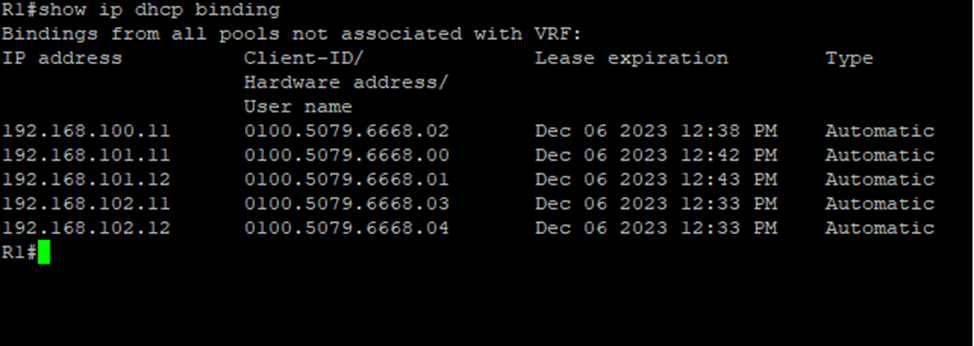
1. *IPphone1 и IPphone2 видят DHCP-сервер*

Используем команду ping, чтобы «достучаться» с одного VOIP до другого. Все работает корректно (рисунок 9).

**

1. *Команда ping между VOIP IPphone1 и IPphone2*

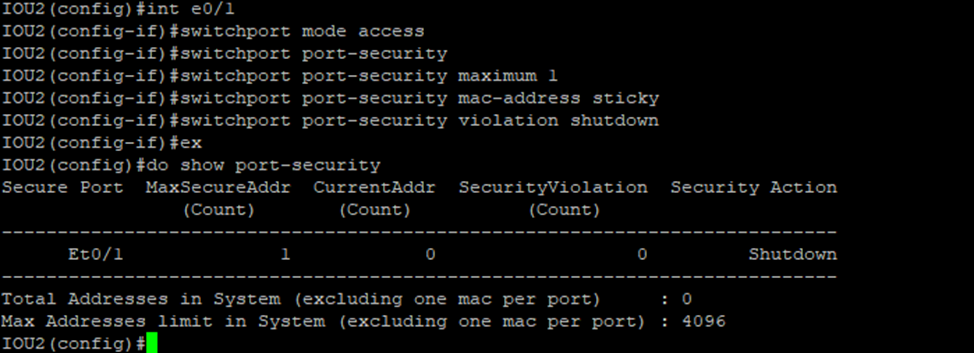
Откроем консоль у роутера R1 и введем команду show ip dhcp binding. Она показывает список созданных связей, используемых для распространения пакетов протокола DHCP (рисунок 10).

**

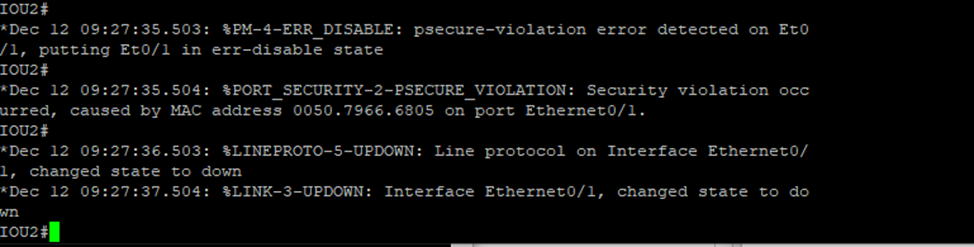
1. *Команда ping между VOIP IPphone1 и IPphone2*

### **Port Security**

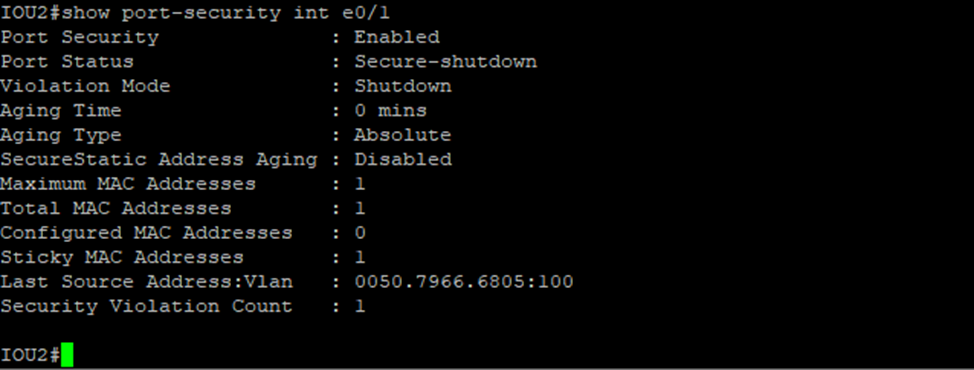
Настроим Port security (безопасность канального уровня) на коммутаторе IOU2 (рисунок 11). Сначала укажем лимит разрешенных адресов для конкретного интерфейса через switchport port-security maximum число. В нашем случае лимит равен единице. Опция sticky для MAC-адреса закрепляет за портом тот адрес, который в данный момент работает на порту.



1. *Настройка Port Security*

**

1. *Работа Port Security*

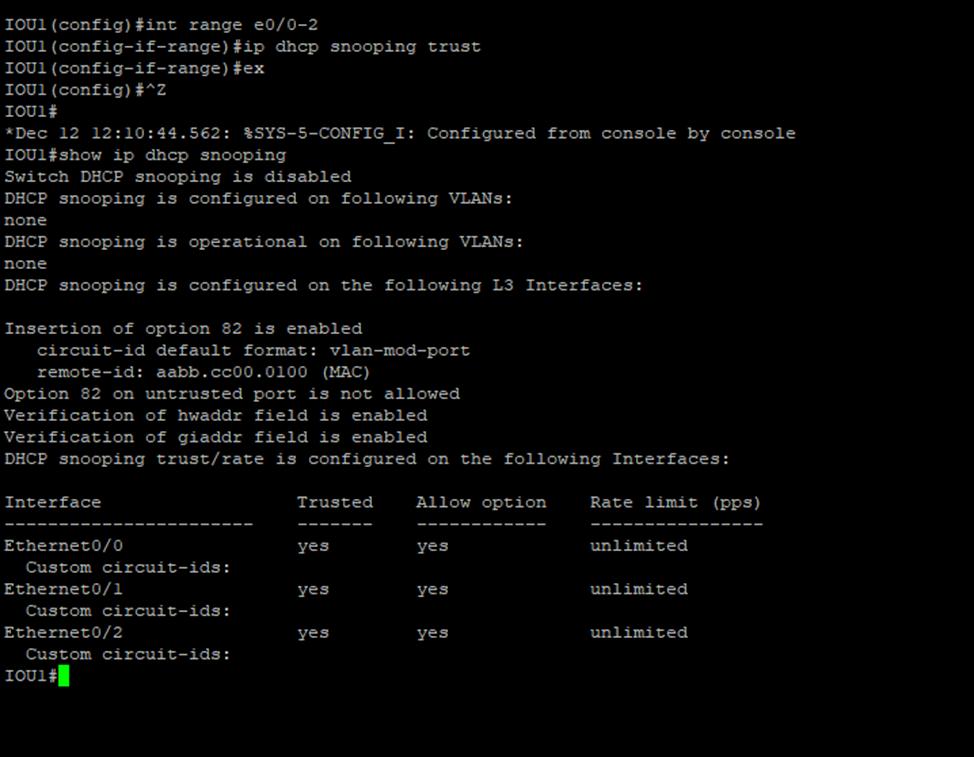
**

1. *Работающий Port Security*

### **DHCP Snooping**

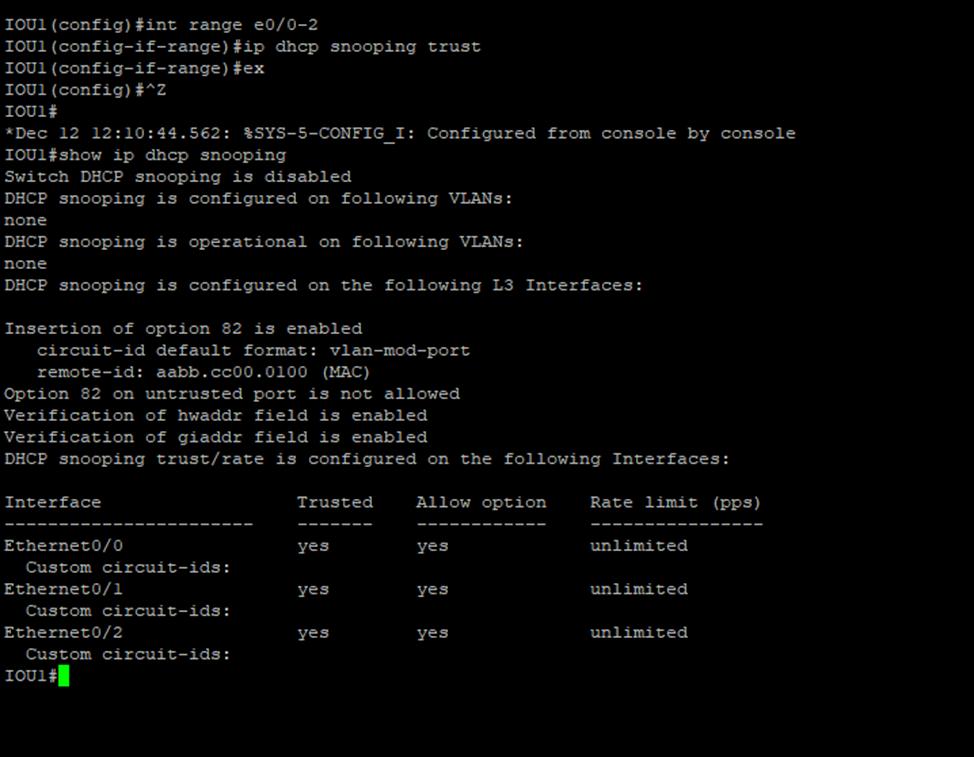
Настроим DHCP snooping на каждом коммутаторе, затем протестируем подключение DHCP сервера к недоверенному порт (рисунок 14).

Настроим коммутатор IOU1 для установки доверия определенным портам. Злоумышленник не сможет выдать себя за DHCP сервер, т. к. порт, к которому он подключится, не будет доверенным.



1. Настройка DHCP snooping

Проверим, правильно ли мы настроили DHCP snooping для коммутатора IOU1. Настройки корректны, т. к. доверены только определенные порты.



1. Результаты настройки DHCP snooping

**Заключение**

В данной лабораторной работе мы научились работать со средой GNS3, выставлять режимы портов и задавать VLAN-порты, настраивать DHCP-сервер, а также настраивать DHCP Snooping и Port Security.

Это позволило нам получить представление об основных угрозах сетевой безопасности на канальном уровне, а также изучить базовые инструменты безопасности, используемые на коммутаторах.