**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**

**Выполнили:**

Ахраров Али, студент группы N3350

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

(подпись)

**Проверил:**

Бучаев Абдулхамид Яхъяевич

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

(отметка о выполнении)

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

(подпись)

Содержание

[1 ВВЕДЕНИЕ 4](#_Toc191140576)

[1.1. Цель работы 4](#_Toc191140577)

[1.2. Задачи работы 4](#_Toc191140578)

[2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ 5](#_Toc191140579)

[2.1. Сегментация сети и VLAN 5](#_Toc191140580)

[2.2. Режимы портов (Access, Trunk) 5](#_Toc191140581)

[2.3. Сабинтерфейсы на маршрутизаторе 5](#_Toc191140582)

[2.4. DHCP-сервер 5](#_Toc191140583)

[2.5. Port Security 5](#_Toc191140584)

[2.6. DHCP Snooping 5](#_Toc191140585)

[2.7. Dynamic ARP Inspection (DAI) 6](#_Toc191140586)

[3 СХЕМА СЕТИ И ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА 7](#_Toc191140587)

[3.1. Топология сети 7](#_Toc191140588)

[3.2. Состав оборудования и версии 7](#_Toc191140589)

[3.3. Привязка VLAN и портов 7](#_Toc191140590)

[4 ХОД РАБОТЫ 8](#_Toc191140591)

[4.1. Первичная настройка коммутаторов 8](#_Toc191140592)

[4.2. Настройка роутера (IOU1) – сабинтерфейсы 8](#_Toc191140593)

[4.3. DHCP-сервер 8](#_Toc191140594)

[4.4. Проверка соединения 9](#_Toc191140595)

[4.5. Настройка Port Security 9](#_Toc191140596)

[4.6. Настройка DHCP Snooping 9](#_Toc191140597)

[4.7. Dynamic ARP Inspection 9](#_Toc191140598)

[5 РЕЗУЛЬТАТЫ 10](#_Toc191140599)

[5.1. Вывод команд (Show) и скриншоты 10](#_Toc191140600)

[5.2. Анализ полученных результатов 10](#_Toc191140601)

[6 ВЫВОДЫ 11](#_Toc191140602)

[7 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 12](#_Toc191140603)

# ВВЕДЕНИЕ

### 1.1. Цель работы

Цель данной лабораторной работы – получить представление об основных механизмах безопасности канального уровня (Layer 2), применяемых в корпоративных сетях, а также научиться настраивать базовые средства защиты на коммутаторах (VLAN, Port Security, DHCP Snooping, DAI и т. д.).

### 1.2. Задачи работы

1. Настроить топологию сети согласно заданной схеме (4 коммутатора/IOU, 4 рабочие станции, 1 маршрутизатор).
2. Создать и назначить VLAN на портах коммутаторов (Access и Trunk).
3. На маршрутизаторе создать сабинтерфейсы для взаимодействия с несколькими VLAN (Inter-VLAN Routing).
4. Настроить DHCP-сервер на маршрутизаторе для каждого VLAN.
5. Включить Port Security на коммутаторах с заданной политикой реагирования.
6. Включить и проверить DHCP Snooping, продемонстрировать работу механизма.
7. (Дополнительно) Настроить и проверить Dynamic ARP Inspection (или IP Source Guard).

# **КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

### 2.1. Сегментация сети и VLAN

Виртуальные локальные сети (VLAN) позволяют логически сегментировать коммутаторы на несколько широковещательных доменов. Это повышает безопасность и управляемость, поскольку каждое подразделение/группа пользователей может работать в отдельном VLAN.

### 2.2. Режимы портов (Access, Trunk)

* **Access** – порт, принадлежащий одному VLAN. Обычно для подключения конечных устройств (ПК, принтеры и т. д.).
* **Trunk** – порт, передающий трафик сразу нескольких VLAN (с тегами 802.1Q). Используется для связи между коммутаторами или коммутатором и маршрутизатором (Router-on-a-stick).

### 2.3. Сабинтерфейсы на маршрутизаторе

На физическом интерфейсе маршрутизатора создаются несколько логических сабинтерфейсов (например, Ethernet0/0.101, Ethernet0/0.102), каждый из которых связывается с определённым VLAN (через тег 802.1Q). У каждого сабинтерфейса собственный IP-адрес, используемый как шлюз по умолчанию в соответствующем VLAN.

### 2.4. DHCP-сервер

Для автоматической выдачи IP-адресов, маски, шлюза и пр. на маршрутизаторе настраивается DHCP-сервер. В конфигурации создаются DHCP-пулы для каждого VLAN, указываются сети и default-router.

### 2.5. Port Security

Механизм Port Security ограничивает число допустимых MAC-адресов на одном порту (или фиксирует MAC-адрес), что позволяет предотвратить подключение несанкционированных устройств.

### 2.6. DHCP Snooping

DHCP Snooping защищает от ложных DHCP-серверов, определяя «доверенные» порты (где действительно может находиться DHCP-сервер) и «недоверенные» (где такой трафик фильтруется).

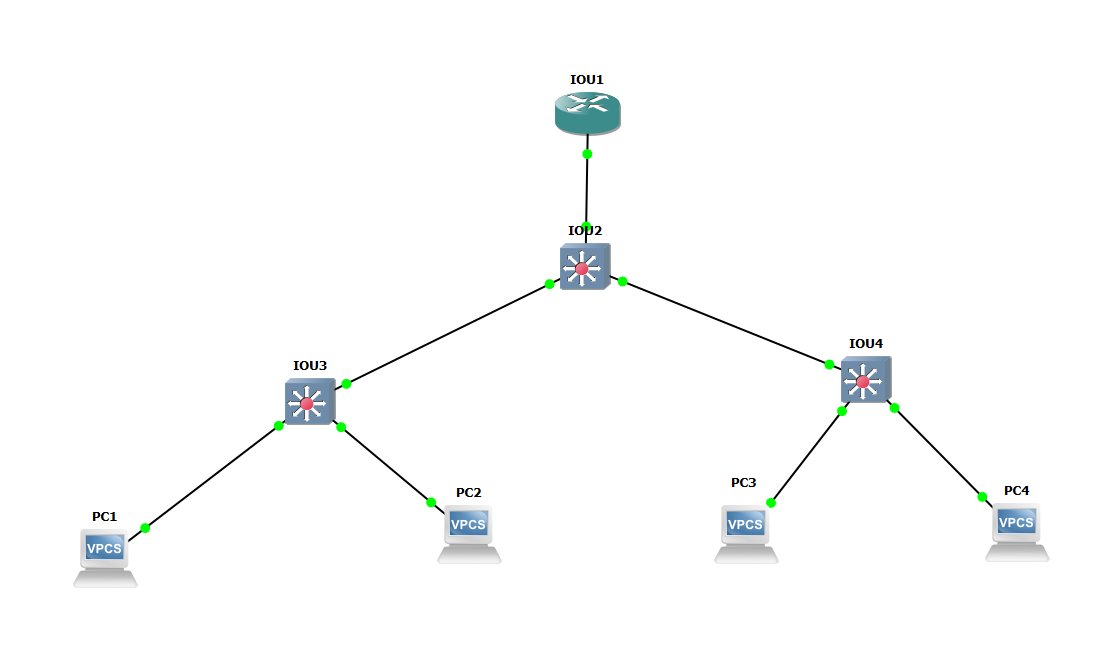
### 2.7. Dynamic ARP Inspection (DAI)

DAI защищает от ARP-spoofing, сверяя ARP-запросы/ответы с таблицей DHCP Snooping Binding (где хранятся IP-MAC-VLAN-Interface). Если пакет не соответствует, он отбрасывается.

# СХЕМА СЕТИ И ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

### 3.1. Топология сети

Ниже приведён скриншот топологии (Рисунок 1):

  
Рисунок 1 – топология сети

Состав:

* **IOU1** (маршрутизатор L3 или отдельный Router + L2 switch),
* **IOU2**, **IOU3**, **IOU4** – коммутаторы L2,
* **PC1, PC2, PC3, PC4** – рабочие станции (VPCS).

### 3.2. Состав оборудования и версии

* GNS3 v2.2.26
* IOU (Cisco IOS on Unix) – L2 (i86bi\_linux\_l2) и L3 (i86bi\_linux\_l3)
* VPCS (минимальный эмулятор ПК)

### 3.3. Привязка VLAN и портов

Пример (согласно заданию):

* VLAN 101 – Executive office, IP 192.168.101.0/24, шлюз 192.168.101.254
* VLAN 102 – Finances, IP 192.168.102.0/24, шлюз 192.168.102.254

На IOU2/IOU3/IOU4 назначены порты:

* **Ethernet0/0** и **Ethernet0/1** в Access (для PC)
* **Ethernet1/0** в Trunk (для связи с центральным коммутатором IOU2)

# ХОД РАБОТЫ

### 4.1. Первичная настройка коммутаторов

На каждом коммутаторе:

1. Создали VLAN 101 и 102 (командой vlan 101, vlan 102), присвоили им имена (опционально).
2. Перевели нужные порты в режим Access для соответствующего VLAN, например:

interface Ethernet0/0

switchport mode access

switchport access vlan 101

1. Перевели порты между коммутаторами в Trunk:

interface Ethernet1/0

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 101,102

### 4.2. Настройка роутера (IOU1) – сабинтерфейсы

На интерфейсе Ethernet0/0 создаются сабинтерфейсы:

interface Ethernet0/0

no shutdown

!

interface Ethernet0/0.101

encapsulation dot1Q 101

ip address 192.168.101.254 255.255.255.0

!

interface Ethernet0/0.102

encapsulation dot1Q 102

ip address 192.168.102.254 255.255.255.0

### 4.3. DHCP-сервер

На том же роутере IOU1:

ip dhcp pool vlan101

network 192.168.101.0 255.255.255.0

default-router 192.168.101.254

ip dhcp pool vlan102

network 192.168.102.0 255.255.255.0

default-router 192.168.102.254

### 4.4. Проверка соединения

* На PC1 и PC2 (подключённых к VLAN 101) выполняем ip dhcp. Убеждаемся, что адрес получен из пула 192.168.101.x.
* На PC3 и PC4 (VLAN 102) аналогично выполняем ip dhcp.
* Проверяем пинг ping 192.168.101.254 (шлюз), ping 192.168.102.254.

### 4.5. Настройка Port Security

На портах, где подключены ПК:

interface Ethernet0/0

switchport mode access

switchport access vlan 101

switchport port-security

switchport port-security maximum 2

switchport port-security mac-address sticky

### 4.6. Настройка DHCP Snooping

Включаем DHCP Snooping на коммутаторе (например, IOU3):

ip dhcp snooping

ip dhcp snooping vlan 101,102

interface Ethernet1/0

ip dhcp snooping trust

(Где Ethernet1/0 – trunk-порт, ведущий к IOU1 или к «центральному» коммутатору, где DHCP-сервер доступен.)

### 4.7. Dynamic ARP Inspection

ip arp inspection vlan 101,102

! Доверяем trunk-порту:

interface Ethernet1/0

ip arp inspection trust

Проверяем, что при попытке «подделать» ARP, пакеты отбрасываются (видно в логах).

# РЕЗУЛЬТАТЫ

### 5.1. Вывод команд (Show) и скриншоты

Ниже примеры основных команд и результаты (см. также скриншоты в приложении):

* **show ip interface brief** – убеждаемся, что сабинтерфейсы подняты.
* **show vlan brief** – видим VLAN 101 и 102.
* **show interfaces trunk** – проверяем, что trunk-порты активны и передают нужные VLAN.
* **show ip dhcp binding** (на роутере) – видим, что PC1, PC2, PC3, PC4 получили IP.
* **show port-security** – показывается текущее состояние, кол-во MAC.
* **show ip dhcp snooping binding** – проверяем записи snooping (IP-MAC).
* **show ip arp inspection statistics** – смотрим, есть ли отбрасывания пакетов.

### 5.2. Анализ полученных результатов

* DHCP успешно выдаёт IP-адреса в обоих VLAN (101 и 102).
* При включении DHCP Snooping недоверенные порты блокируют ложный DHCP-трафик.
* Dynamic ARP Inspection позволяет отсекать ARP-spoofing.
* Port Security успешно ограничивает MAC-адреса.

# ВЫВОДЫ

В ходе лабораторной работы:

1. Настроили VLAN 101 и 102, разделив пользователей на две сети.
2. Реализовали сабинтерфейсы на роутере, обеспечив межвлановую маршрутизацию.
3. Настроили DHCP-сервер на маршрутизаторе IOU1, проверили автоматическую выдачу адресов.
4. Включили Port Security, ограничив MAC-адреса на портах.
5. Настроили DHCP Snooping, назначили «доверенные» порты, убедились в защите от поддельных DHCP-серверов.
6. Дополнительно включили ARP Inspection, проверили логи отбрасывания некорректных ARP.

Таким образом, были отработаны базовые механизмы безопасности на уровне 2 (L2), повысившие защищённость сети от ряда распространённых атак (MAC-flooding, ARP-spoofing, rogue DHCP server и т. д.).

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Cisco Systems. [Документация по DHCP Snooping](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst...)
2. Cisco Systems. [Port Security Configuration Guide](https://www.cisco.com/c/en/us/td/docs/switches...)
3. Официальная документация GNS3 (<https://docs.gns3.com/>).