

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ  
УНИВЕРСИТЕТ “МИФИ”»**

Институт Интеллектуальных Кибернетических Систем  
Кафедра №42 "Криптология и кибербезопасность"

Дисциплина «Компьютерные сети»

Отчет к лабораторной работе № 4  
«Настройка управляемого коммутатора»

Выполнили студенты группы Б22-505:  
Глушко Глеб  
Панкратов Дмитрий  
Титов Дмитрий  
Черепанова Ульяна

Москва  
2025 год

Введение.....	3
Ход работы.....	4
1. Подключение к коммутатору через com порт и настройка подключения по ssh.....	4
2. Настройка ACL.....	7
3. Настройка Port Security.....	9
4. Настройка IP-MAC-PORT binding.....	11
ЗАКЛЮЧЕНИЕ.....	13

# Введение

В современных локальных сетях управляемые коммутаторы играют ключевую роль в обеспечении безопасности, гибкости и управляемости трафика. Целью данной лабораторной работы является освоение практических навыков настройки коммутатора уровня L2+ для реализации защищенного доступа и контроля потоков данных. В рамках работы были последовательно выполнены следующие задачи:

1. Установка защищенного удаленного доступа по SSH для защищенного управления устройством.
2. Конфигурирование списков контроля доступа (ACL) для фильтрации нежелательного трафика.
3. Включение и проверка механизмов Port Security для ограничения доступа клиентов по MAC-адресам.
4. Настройка привязки IP-MAC-PORT (IP-MAC-PORT binding) для защиты от спуфинга.

В процессе выполнения работы использовались как CLI-команды, так и встроенный веб-интерфейс коммутатора, что позволило отследить результаты настроек в реальном времени.

## Ход работы

### 1. Подключение к коммутатору через com порт и настройка подключения по ssh

Для начала через COM-порт был установлен базовый консольный доступ к устройству. На рис. 1.1 показаны параметры соединения (скорость 9600 бод, 8N1). Далее произведена авторизация и создана учетная запись администратора (рис. 1.2), после чего активирован SSH-сервер и загружен криптографический ключ (рис. 1.3). Успешное подключение по защищенному протоколу подтверждает рис. 1.4.

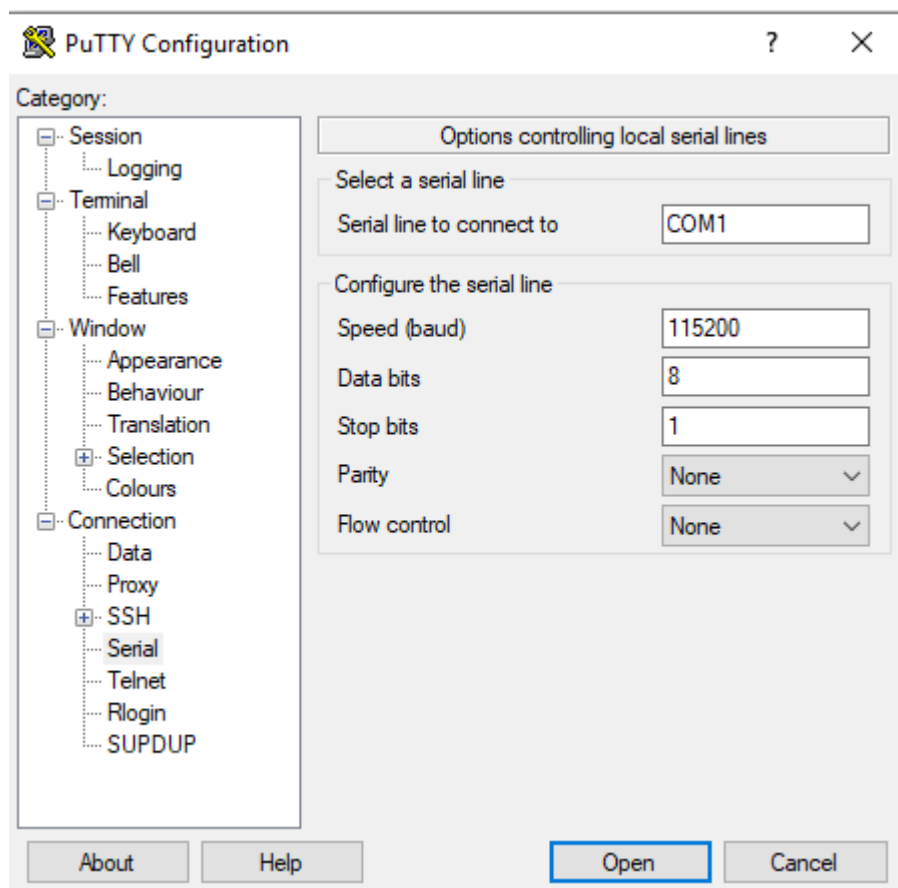
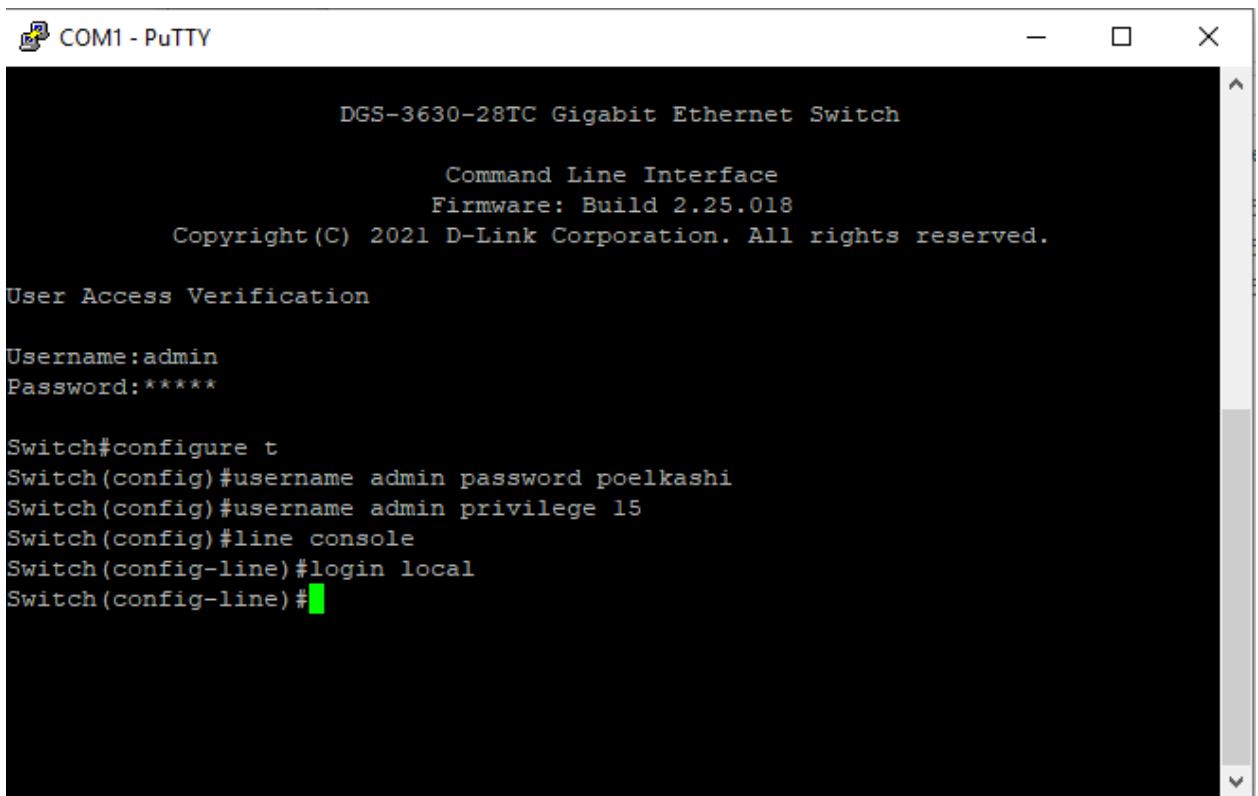


Рис 1.1 – Параметры подключение по ком-порту



```
COM1 - PuTTY

DGS-3630-28TC Gigabit Ethernet Switch

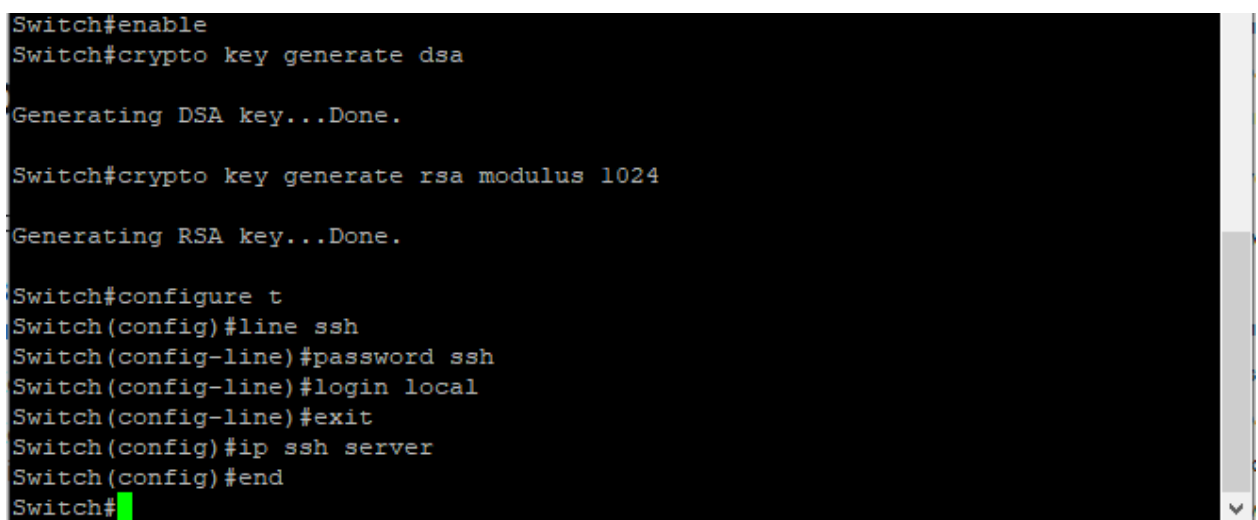
Command Line Interface
Firmware: Build 2.25.018
Copyright(C) 2021 D-Link Corporation. All rights reserved.

User Access Verification

Username:admin
Password:*****

Switch#configure t
Switch(config)#username admin password poelkashi
Switch(config)#username admin privilege 15
Switch(config)#line console
Switch(config-line)#login local
Switch(config-line)#
```

Рис 1.2 – авторизация и создание пользователя admin

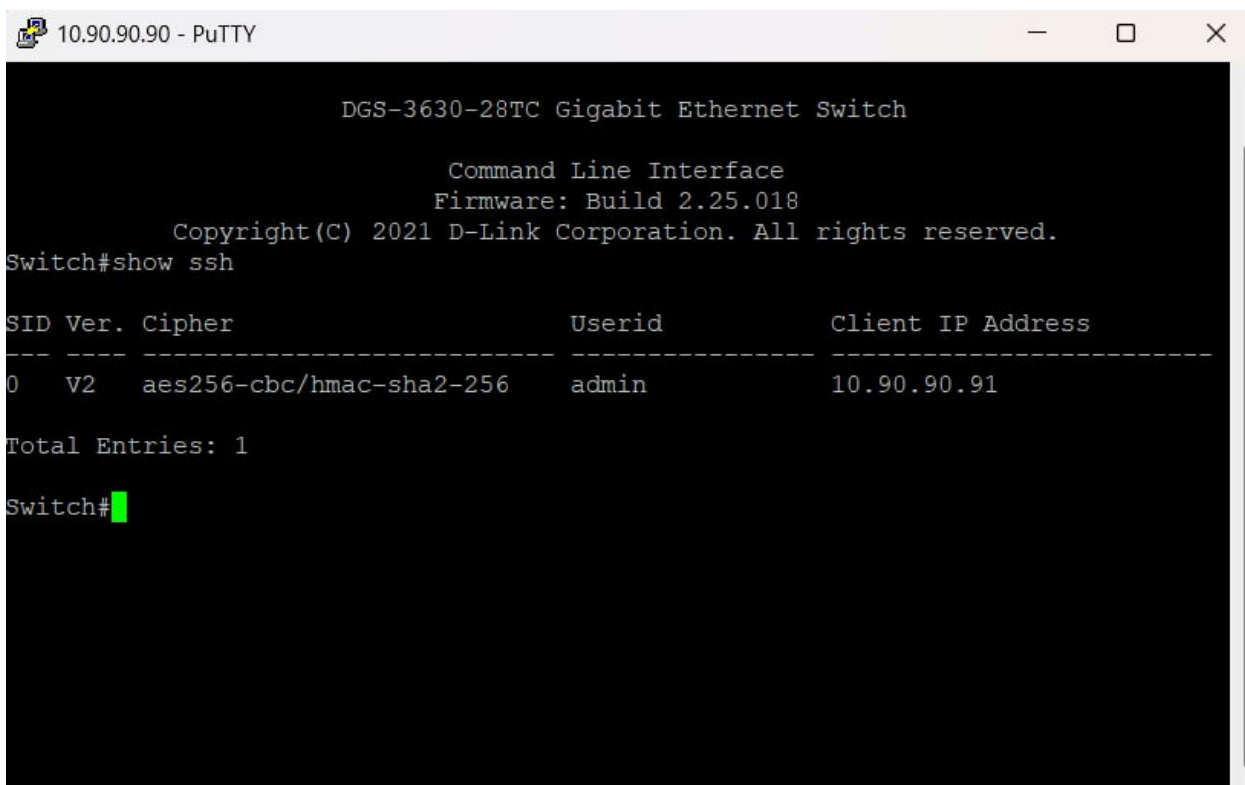


```
Switch#enable
Switch#crypto key generate dsa
Generating DSA key...Done.

Switch#crypto key generate rsa modulus 1024
Generating RSA key...Done.

Switch#configure t
Switch(config)#line ssh
Switch(config-line)#password ssh
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#ip ssh server
Switch(config)#end
Switch#
```

Рис 1.3 – настройка ssh



```
10.90.90.90 - PuTTY

DGS-3630-28TC Gigabit Ethernet Switch

Command Line Interface
Firmware: Build 2.25.018
Copyright(C) 2021 D-Link Corporation. All rights reserved.
Switch#show ssh

SID Ver. Cipher Userid Client IP Address
-----
0 V2 aes256-cbc/hmac-sha2-256 admin 10.90.90.91

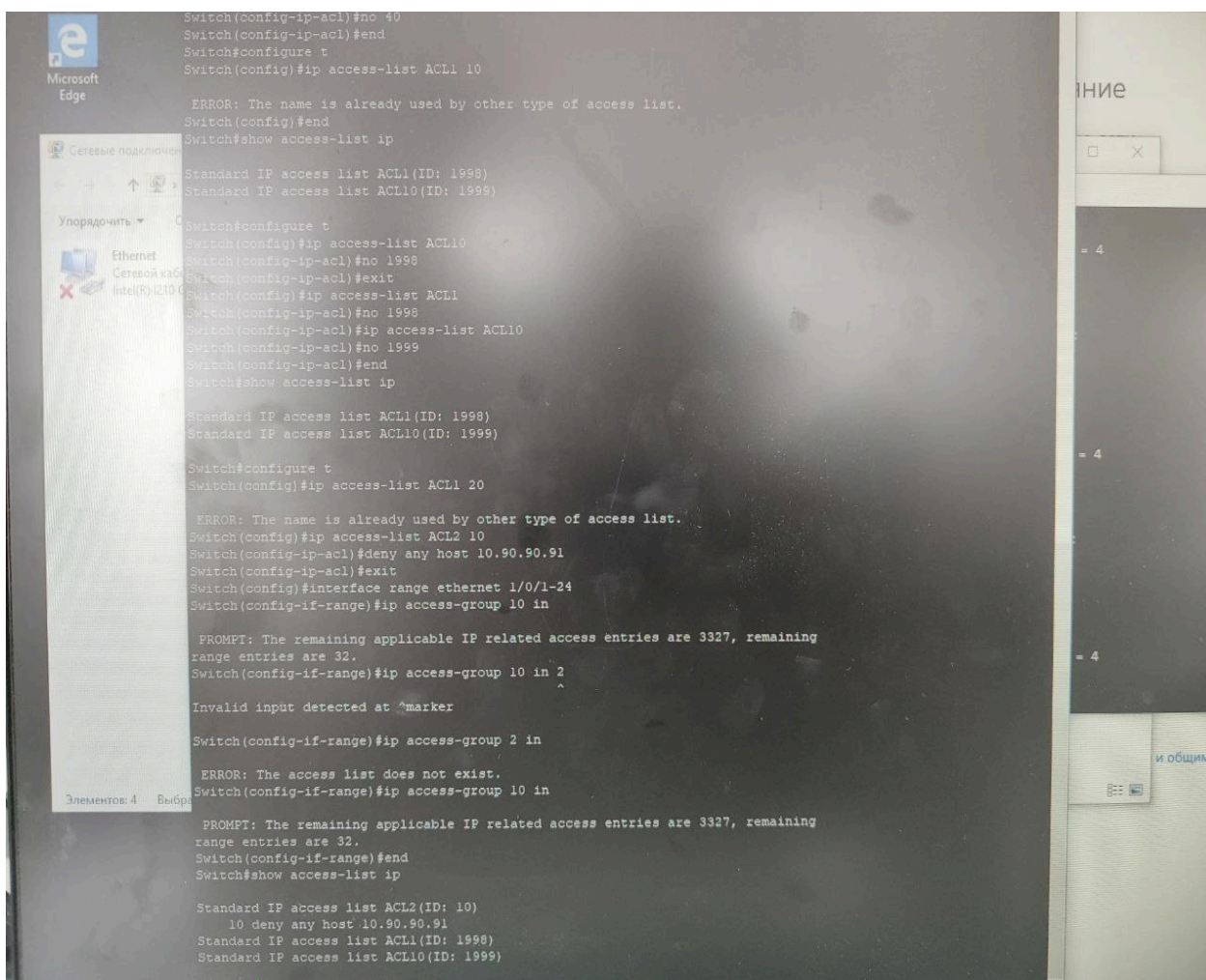
Total Entries: 1

Switch#
```

Рис 1.4 – подключение по SSH

## 2. Настройка ACL

С помощью CLI были заданы правила ACL для блокировки несанкционированного доступа к служебным VLAN и разрешения только необходимого трафика. На рис. 2.1 приведена конфигурация, а на рис. 2.2 продемонстрирована проверка — пакеты, не соответствующие правилам, отброшены.



```
Switch(config-ip-acl)#no 40
Switch(config-ip-acl)#end
Switch#configure t
Switch(config)#ip access-list ACL1 10

ERROR: The name is already used by other type of access list.
Switch(config)#end
Switch#show access-list ip

Standard IP access list ACL1(ID: 1998)
Standard IP access list ACL10(ID: 1998)

Switch#configure t
Switch(config)#ip access-list ACL10
Switch(config-ip-acl)#no 1998
Switch(config-ip-acl)#exit
Switch(config)#ip access-list ACL1
Switch(config-ip-acl)#no 1998
Switch(config-ip-acl)#ip access-list ACL10
Switch(config-ip-acl)#no 1999
Switch(config-ip-acl)#end
Switch#show access-list ip

Standard IP access list ACL1(ID: 1998)
Standard IP access list ACL10(ID: 1999)

Switch#configure t
Switch(config)#ip access-list ACL1 20

ERROR: The name is already used by other type of access list.
Switch(config)#ip access-list ACL2 10
Switch(config-ip-acl)#deny any host 10.90.90.91
Switch(config-ip-acl)#exit
Switch(config)#interface range ethernet 1/0/1-24
Switch(config-if-range)#ip access-group 10 in

PROMPT: The remaining applicable IP related access entries are 3327, remaining
range entries are 32.
Switch(config-if-range)#ip access-group 10 in 2

Invalid input detected at ^marker

Switch(config-if-range)#ip access-group 2 in

ERROR: The access list does not exist.
Switch(config-if-range)#ip access-group 10 in

PROMPT: The remaining applicable IP related access entries are 3327, remaining
range entries are 32.
Switch(config-if-range)#end
Switch#show access-list ip

Standard IP access list ACL2(ID: 10)
10 deny any host 10.90.90.91
Standard IP access list ACL1(ID: 1998)
Standard IP access list ACL10(ID: 1999)
```

Рис 2.1 – настройка асl при помощи cli

```
Командная строка
Приблизительное время приема-передачи в мс:
  Минимальное = 2мсек, Максимальное = 3 мсек, Среднее = 2 мсек

C:\Users\DMI>ping 10.90.90.90

Обмен пакетами с 10.90.90.90 по с 32 байтами данных:
Ответ от 10.90.90.90: число байт=32 время=3мс TTL=255
Ответ от 10.90.90.90: число байт=32 время=3мс TTL=255
Ответ от 10.90.90.90: число байт=32 время=2мс TTL=255
Ответ от 10.90.90.90: число байт=32 время=2мс TTL=255

Статистика Ping для 10.90.90.90:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 2мсек, Максимальное = 3 мсек, Среднее = 2 мсек

C:\Users\DMI>ping 10.90.90.91

Обмен пакетами с 10.90.90.91 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 10.90.90.91:
  Пакетов: отправлено = 4, получено = 0, потеряно = 4
  (100% потерь)

C:\Users\DMI>
```

Рис2.2 – демонстрация работы asl



### 3. Настройка Port Security

В веб-интерфейсе (рис. 3.1) активирована функция Port Security на портах доступа. На рис. 3.2 указаны ограничения: максимальное число MAC-адресов = 2, режим защитного действия — shutdown. Рис. 3.3 иллюстрирует ситуацию превышения лимита и автоматическую блокировку порта.

Порт	Максимум	Текущий номер	Действие при нарушении ограничения	Количество нарушений	Режим безопасности	Статус администрирования	Текущее состояние	Время устаревания (Aging Time)	Тип aging
eth1/0/1	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/2	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/3	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/4	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/5	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/6	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/7	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/8	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/9	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/10	32	1	Защитить	-	Постоянный (Permanent)	Включен	Перенаправление	0	Абсолютный
eth1/0/11	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/12	0	0	Защитить	-	Постоянный (Permanent)	Включен	Перенаправление	0	Абсолютный
eth1/0/13	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/14	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный
eth1/0/15	32	0	Защитить	-	Удалить по истечении времени	Выключен	-	0	Абсолютный

Рис 3.1 – окно настройки port security

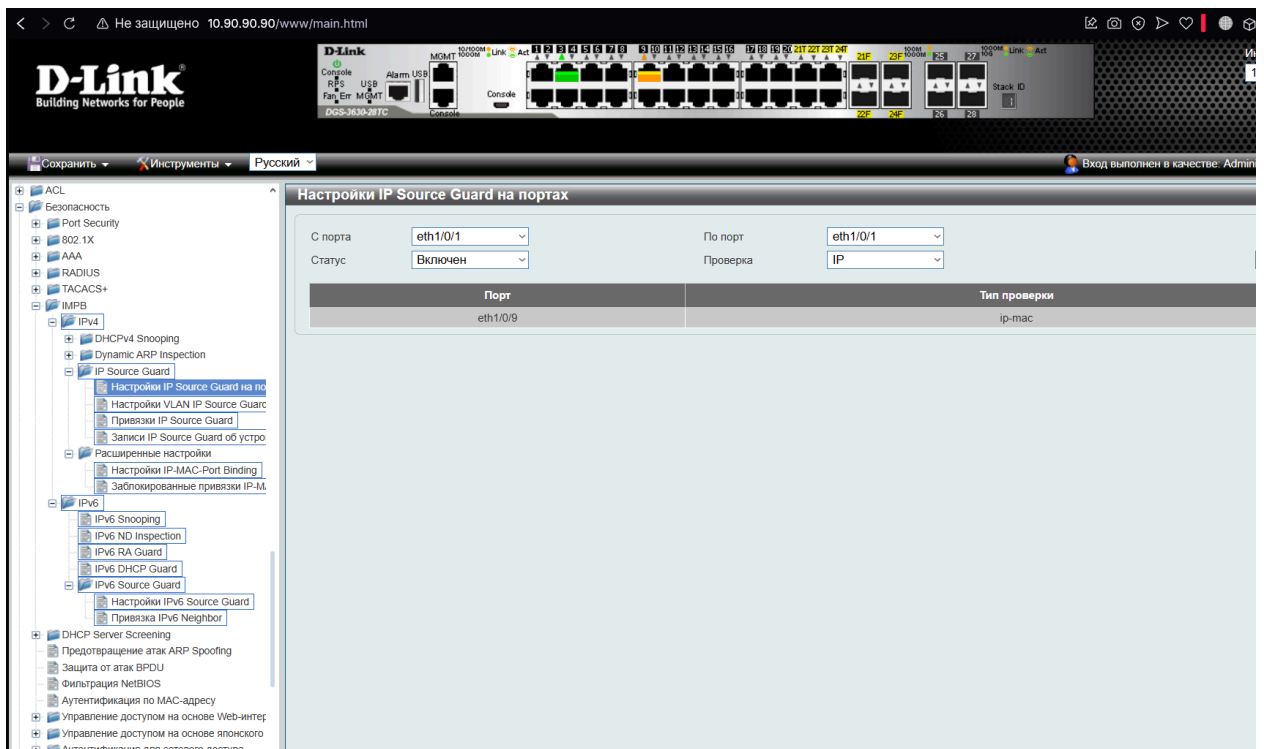


Рис 3.2 – настройка port security

```
C:\Users\DMI>ping 10.90.90.90

Обмен пакетами с 10.90.90.90 по 32 байтами данных:
Ответ от 10.90.90.90: число байт=32 время=2мс TTL=255
Ответ от 10.90.90.90: число байт=32 время=3мс TTL=255
Ответ от 10.90.90.90: число байт=32 время=3мс TTL=255
Ответ от 10.90.90.90: число байт=32 время=5мс TTL=255

Статистика Ping для 10.90.90.90:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 5 мсек, Среднее = 3 мсек

C:\Users\DMI>ping 10.90.90.90

Обмен пакетами с 10.90.90.90 по 32 байтами данных:
Ответ от 10.90.90.97: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 10.90.90.90:
    Пакетов: отправлено = 4, получено = 1, потеряно = 3
    (75% потерь)
```

Рис 3.3 – демонстрация работы port security

## 4. Настройка IP-MAC-PORT binding

Для каждой коммутационной линии была произведена статическая привязка IP-адреса к MAC и порту (рис. 4.1). Тестирование (рис. 4.2) подтвердило, что при попытке подмены MAC или IP трафик блокируется, что исключает ARP-спуфинг.

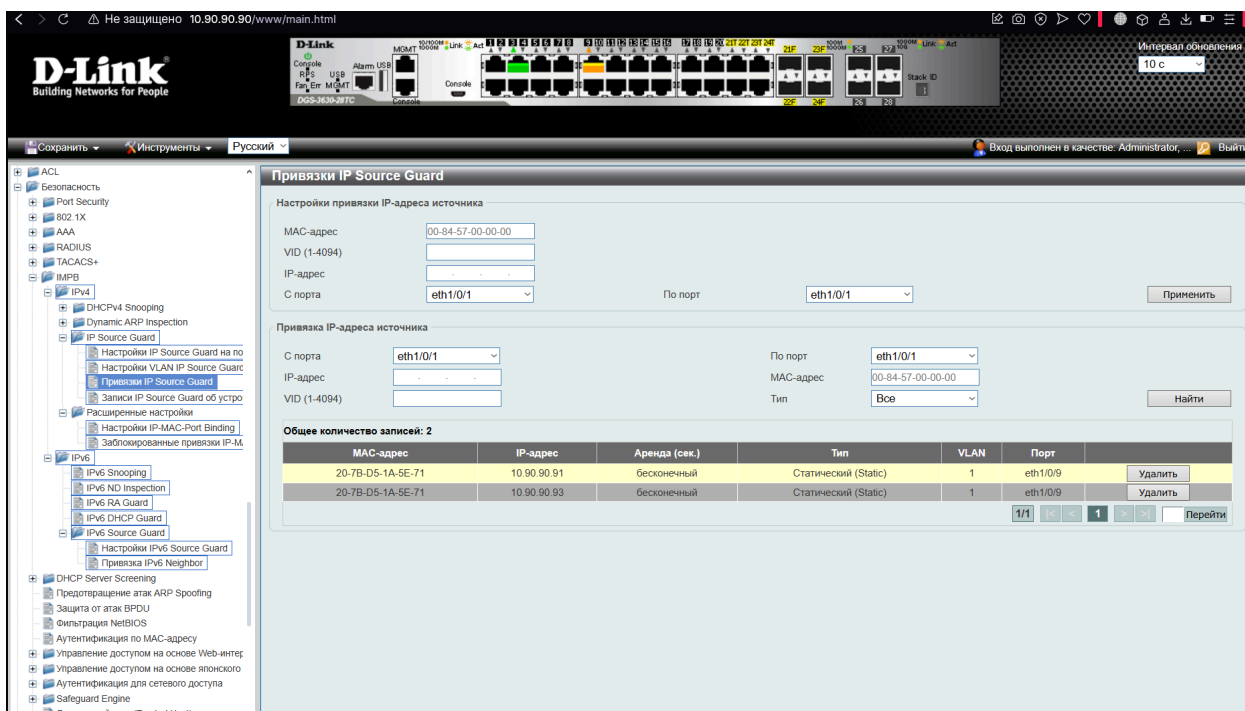


Рис 4.1 – настройка ip-mac-port binding

```
C:\Users\DMI>ping 10.90.90.90
```

```
Обмен пакетами с 10.90.90.90 по с 32 байтами данных:  
Ответ от 10.90.90.90: число байт=32 время=3мс TTL=255  
Ответ от 10.90.90.90: число байт=32 время=3мс TTL=255  
Ответ от 10.90.90.90: число байт=32 время=3мс TTL=255  
Ответ от 10.90.90.90: число байт=32 время=3мс TTL=255
```

```
Статистика Ping для 10.90.90.90:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0  
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 3мсек, Максимальное = 3 мсек, Среднее = 3 мсек
```

```
C:\Users\DMI>ping 10.90.90.90
```

```
Обмен пакетами с 10.90.90.90 по с 32 байтами данных:
```

```
Превышен интервал ожидания для запроса.
```

```
Превышен интервал ожидания для запроса.
```

```
Превышен интервал ожидания для запроса.
```

```
Превышен интервал ожидания для запроса.
```

```
Статистика Ping для 10.90.90.90:
```

```
Пакетов: отправлено = 4, получено = 0, потеряно = 4  
(100% потерь)
```

```
C:\Users\DMI>|
```

Рис 4.2 – демонстрация работы ip-mac-port binding

# ЗАКЛЮЧЕНИЕ

В результате выполнения лабораторной работы студенты закрепили практические навыки настройки управляемого L2+ коммутатора. Были успешно реализованы и протестированы ключевые функции безопасности:

- Защищенный доступ по SSH
- Фильтрация трафика с помощью ACL
- Ограничение доступа клиентов через Port Security
- Защита от ARP-спуфинга при помощи IP-MAC-PORT binding

Достигнутые результаты показывают, что применение комплексных мер безопасности на уровне коммутатора существенно повышает защищенность локальной сети и снижает риски несанкционированного доступа и атак.