

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт цифровых технологий, электроники и физики (ИЦТЭФ)
Кафедра вычислительной техники и электроники (ВТиЭ)

Лабораторная работа № 03
Коммутаторы третьего уровня.

Выполнили: студенты 595 гр.

_____ А.В. Осипов

_____ А.В. Лаптев

_____ А.Е. Половинкин

Проверил: доцент кафедры ВТиЭ

_____ А.В. Калачёв

Лабораторная работа защищена

«__»__сентября____2022 г.

Оценка _____

Барнаул 2022

Цель работы: Изучить основы работы с коммутаторами третьего уровня, произвести настройку коммутатора через консольный порт и через Ethernet, научиться работать с коммутатором посредством консольных команд и через web-интерфейс.

Задачи работы:

1. Теоретическая часть

Типичная сеть состоит из узлов (компьютеров), соединенных средой передачи данных (кабельной или беспроводной) и специализированным сетевым оборудованием, таким как маршрутизаторы, концентраторы или коммутаторы. Все эти компоненты сети, работая вместе, позволяют пользователям пересылать данные с одного компьютера на другой, возможно даже в другую часть света.

Коммутаторы – фундаментальная часть большинства современных сетей. Используя *микросегментацию*, они дают возможность одновременно посылать по сети информацию множеству пользователей. Микросегментация позволяет создать частные или выделенные сегменты – по одной рабочей станции на сегмент (к порту коммутатора подключается не сегмент, а только рабочая станция). Каждая рабочая станция, при этом, получает доступ сразу ко всей полосе пропускания, и ей не приходится конкурировать с другими станциями. Если оборудование работает в дуплексном режиме, то исключаются коллизии.

Существует множество различных типов коммутаторов и сетей. Коммутаторы, которые обеспечивают выделенное соединение для каждого узла внутренней сети компании, называются *коммутаторами локальных сетей (LAN Switches)*.

Коммутация 3-го уровня

Коммутация 3-го уровня – это аппаратная маршрутизация, где передача пакетов обрабатывается контроллерами ASIC. В отличие от коммутаторов 2-го уровня, коммутаторы 3-го уровня принимают решения на основе информации сетевого уровня, а не на основе MAC-адресов. Основная цель коммутации 3-го уровня – получить скорость коммутации 2-го уровня и масштабируемость

маршрутизации. Обработку пакетов коммутатор 3-го уровня выполняет таким же образом, как и маршрутизатор:

- на основе информации 3-го уровня (сетевых адресов) определяет путь к месту назначения пакета
- проверяет целостность заголовка 3-го уровня, вычисляя контрольную сумму
- проверяет время жизни пакета
- обрабатывает и отвечает на любую дополнительную информацию
- обновляет статистику в Информационной базе управления (Management Information Base-MIB)
- обеспечивает управление безопасностью (если необходимо)
- обеспечивает необходимое качество сервиса (QoS) для мультимедийных приложений чувствительных к задержкам передачи

Основное отличие между маршрутизаторами и коммутаторами 3-го уровня заключается в том, что в основе коммутации 3-го уровня лежит аппаратная реализация. В маршрутизаторах общего назначения коммутация пакетов обычно выполняется программным образом. Т.к. коммутаторы 3-го уровня обычно быстрее и дешевле маршрутизаторов, то их использование в локальных сетях очень привлекательно. В качестве примеров коммутаторов 3-го уровня можно привести D-Link DES-3326S и DES-3326SR, DES-3350SR, DES-6300, DES-6500.

2. Выполнение работы

Базовая конфигурация коммутатора

Изначальной задачей при создании конфигурации коммутатора является обеспечение его защиты от доступа неавторизованных пользователей. Для этих целей самым простым вариантом является создание учетных записей пользователей с соответствующими правами. При этом для новой учетной записи можно выбрать один из следующих уровней привилегий: Admin, User.

Процесс создания пользователя с привилегиями Admin представлен на рис. 1.

```

qqq - HyperTerminal
Файл  Правка  Вид  Вызов  Передача  Справка

DES-3800:admin#create account admin mgknn
Command: create account admin mgknn

Enter a case-sensitive new password:***
Enter the new password again for confirmation:***
Success.

DES-3800:admin#show account
Command: show account

Current Accounts:
Username      Access Level
-----
mgknn         Admin

Total Entries : 1

DES-3800:admin#

```

Рис. 1. Создание новой учетной записи пользователя.

Настройка IP-адреса

Для того, чтобы можно было осуществлять управление коммутатором удаленно — через web-интерфейс или telnet, необходимо назначить ему IP-адрес из адресного пространства сети, в которой он будет использоваться. В данной ситуации IP-адрес задавался статически, с помощью команд CLI.

Процесс задания IP-адреса показан на рис. 2.

```

qqq - HyperTerminal
Файл  Правка  Вид  Вызов  Передача  Справка

DES-3800:admin#show ipif
Command: show ipif

IP Interface Settings
Interface Name : System
IP Address     : 192.168.0.1      (MANUAL)
Secondary      : FALSE
Subnet Mask    : 255.255.255.0
VLAN Name      : default
Admin. State   : Enabled
Proxy ARP      : Disabled
Link Status    : Link UP |
Member Ports   : 5-28

Total Entries : 1

DES-3800:admin#

```

Рис. 2. Настройка IP-адреса для коммутатора.

Настройка параметров портов коммутатора

Все порты коммутаторов D-Link поддерживают автоматическое определение скорости и режима работы. Но на случай некорректного автоопределения потребуется ручная настройка скорости и режима работы. Для ручной настройки этих параметров портов можно воспользоваться командой **config ports**.

Работа с данной командой проиллюстрирована на рис. 3.

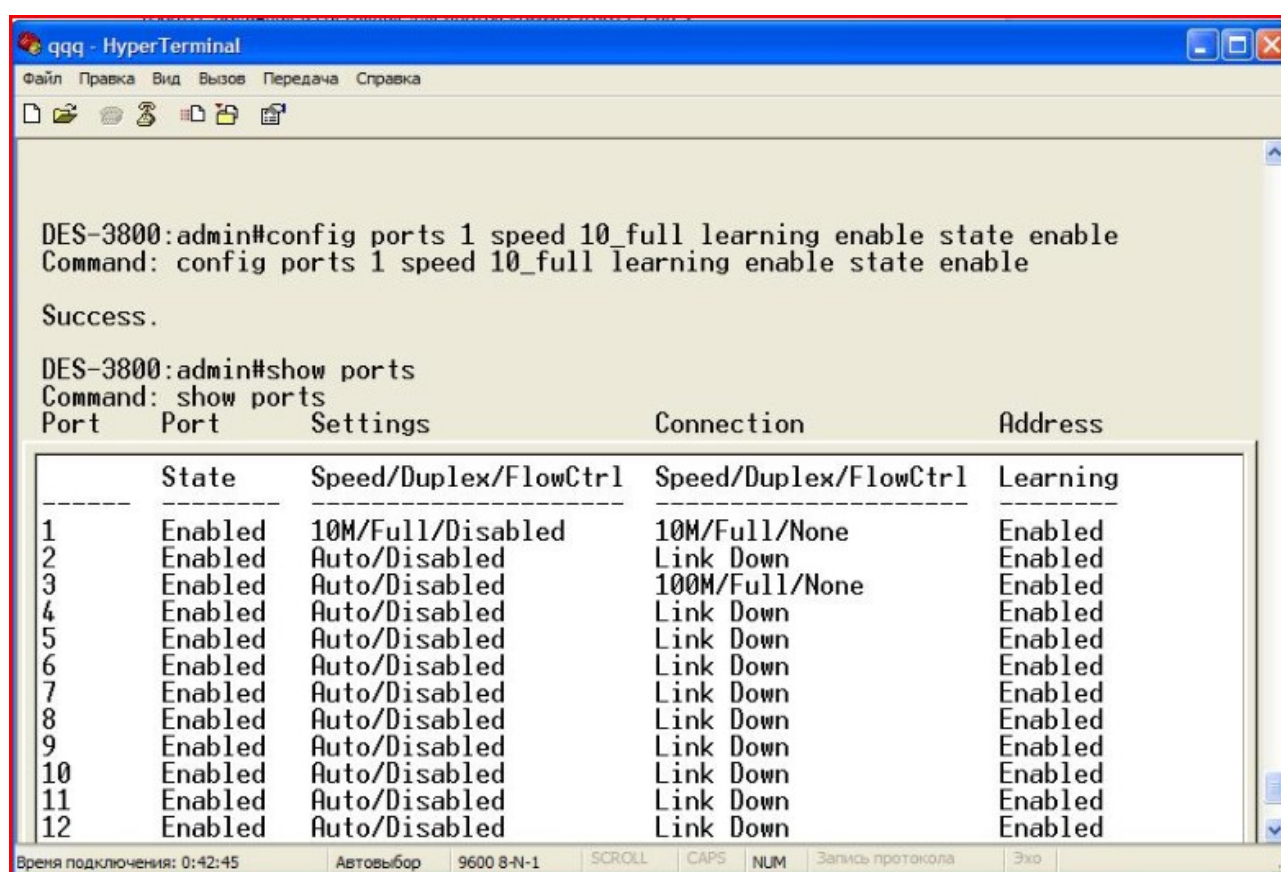


Рис. 3. Настройка параметров портов вручную.

Также, с помощью команды **show ports** можно вывести на экран информацию о настройке портов коммутатора.

Сохранение текущей конфигурации коммутатора в энергонезависимую память NVRAM

Для выполнения данного действия выполняем команду **save**.

Перезагрузка коммутатора

Для перезагрузки коммутатора используется команда **reboot**.

Результат работы данной команды демонстрирует рис. 4.

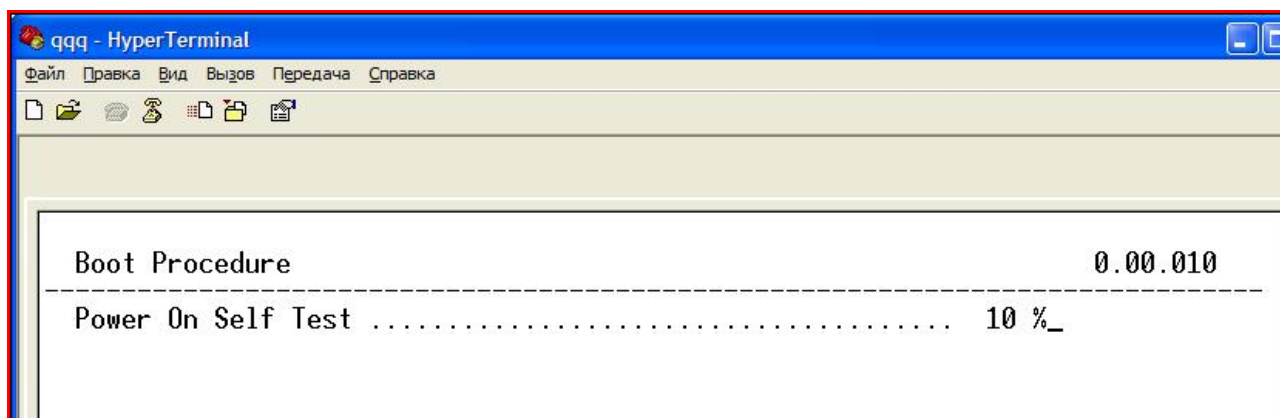


Рис. 4. Перезагрузка коммутатора.

Перезагрузка коммутатора осуществлялась после сохранения текущей конфигурации для того, чтобы проверить факт сохранения настроек. На рис. 5 видно, что все настройки были сохранены после перезагрузки.

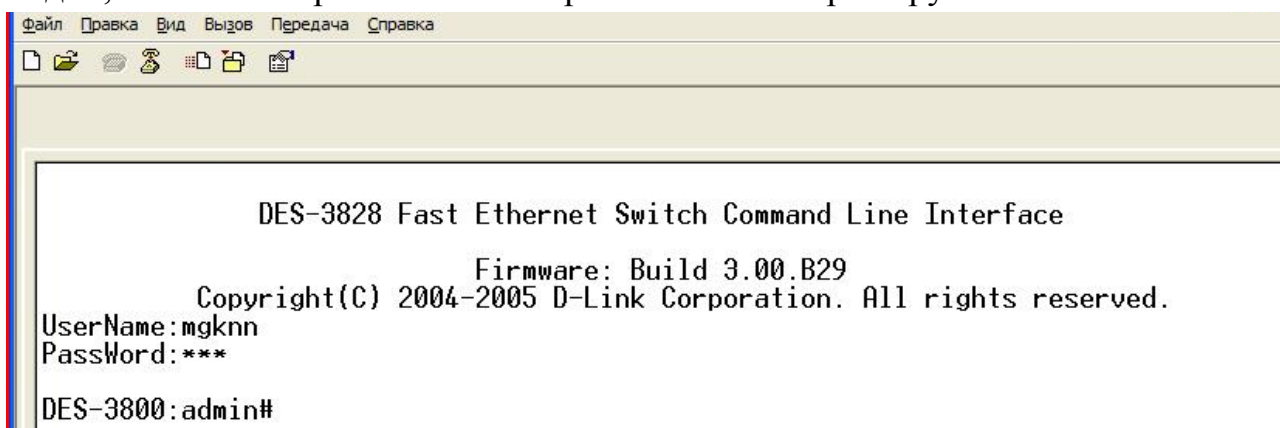


Рис. 5. Последствия перезагрузки коммутатора.

Просмотр конфигурации коммутатора

Для просмотра текущей конфигурации коммутатора достаточно выполнить команду **show switch**.

Результат выполнения описанной выше команды представлен на рис. 6

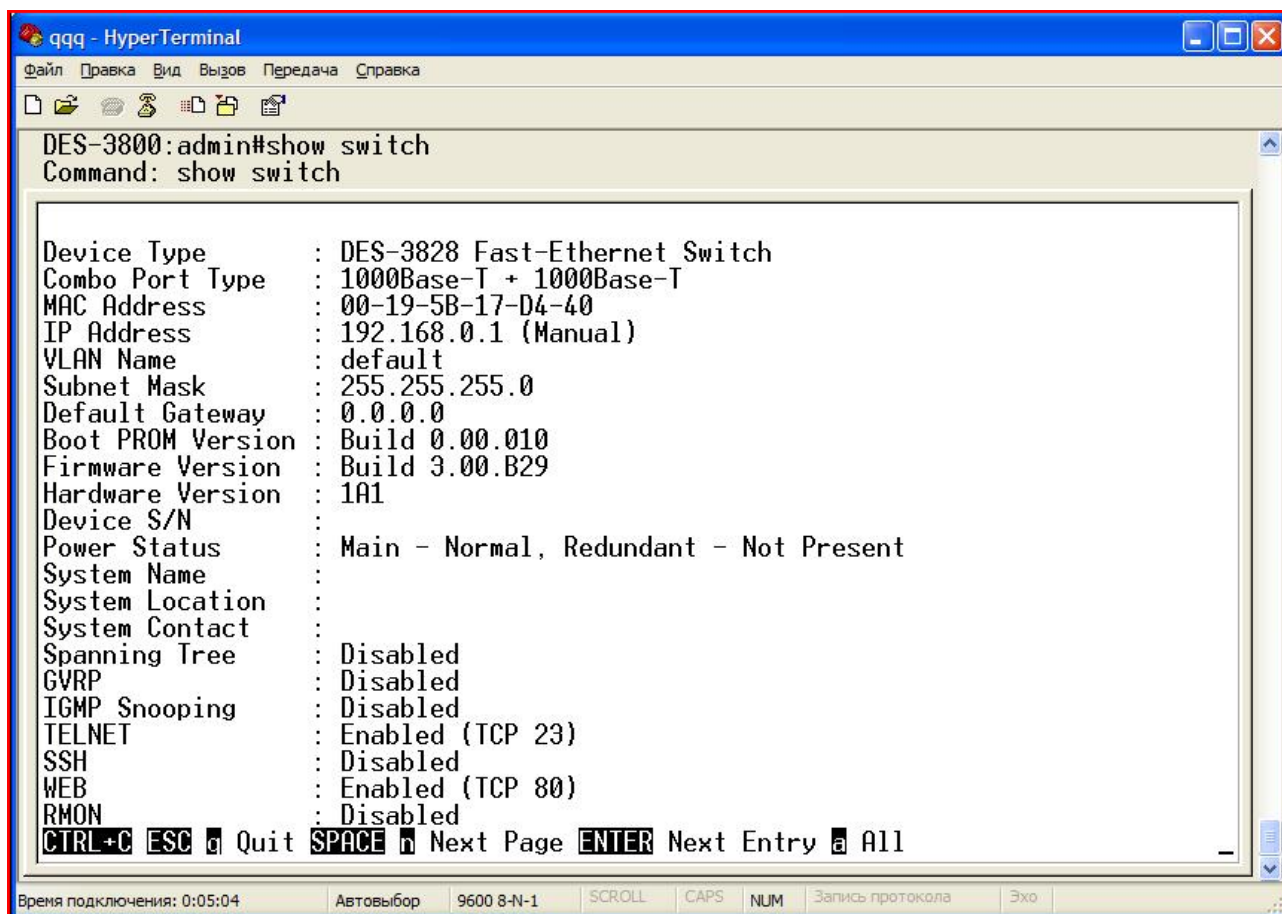


Рис. 6. Просмотр текущей конфигурации коммутатора.

Подключение к Web-интерфейсу управления коммутатора

Настройка коммутатора может осуществляться через Web-интерфейс управления, который состоит из графического пользовательского интерфейса, который запускается на клиенте, а также, HTTP-сервера, который запускается на коммутаторе. Такой подход является альтернативным относительно использования командной строки и обеспечивает графическое представление коммутатора в режиме реального времени и подробную информацию о состоянии портов, модулей, их типе и т. д.

Для налаживания связи между клиентом и сервером используется TCP/IP соединение с портом 80 (номер порта HTTP).

Для того, чтобы подключиться к HTTP серверу на коммутаторе надо выполнить следующее:

1. Назначить коммутатору IP-адрес из диапазона адресов сети (выполнено ранее).
2. Проверить правильность настройки IP-адреса.

3. На рабочей станции в Web-браузере набрать IP-адрес коммутатора в поисковой строке.

Web-интерфейс управления представлен на рис. 7.

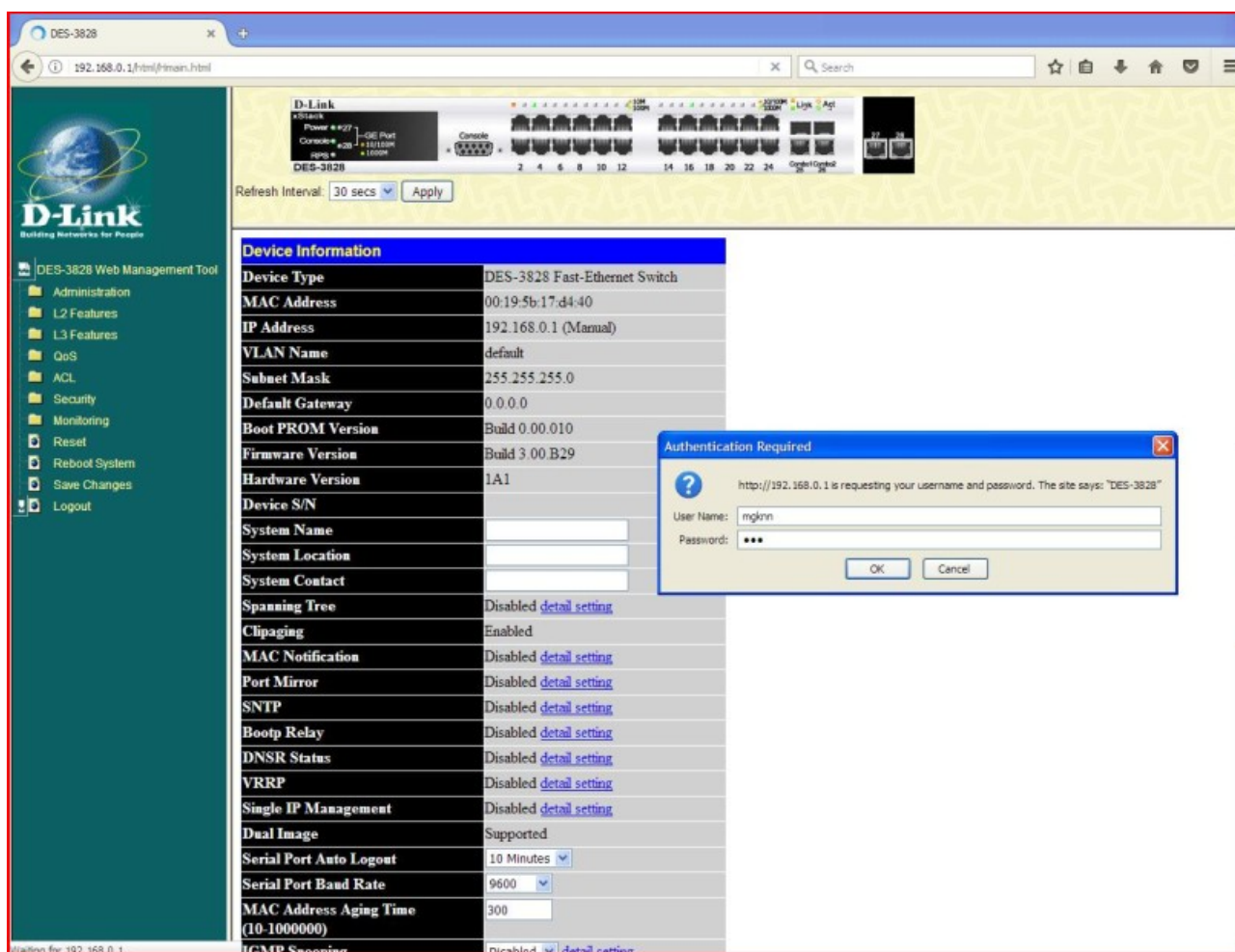


Рис. 7. Интерфейс управления коммутатора.

Выполнение практических заданий

1. Подключить консольный порт коммутатора к компьютеру. Произвести настройки IP-адреса коммутатора таким образом, чтобы он находился в одном адресном пространстве с компьютерами класса.

Выполнение данного пункта описано выше.

2. Написать скрипт, удаляющий все существующие VLAN и создающий 4 VLAN на основе портов со следующим количеством компьютеров в VLAN и сохранить скрипт:

- VLAN1 – 4
- VLAN2 – 6
- VLAN3 – 12

- VLAN4 – 5

Для удаления всех существующих VLAN воспользуемся командой **config vlan default delete 1–24**. После чего можем посмотреть список VLAN при помощи команды **show vlan**

Скрипт с результатами выполнения команд представлен ниже:

```
DES-3800:admin#config vlan default delete 1-24
Command: config vlan default delete 1-24
DES-3800:admin#show vlan
Command: show vlan
VID          : 1          VLAN Name    : default
VLAN TYPE    : static    Advertisement : Enabled
Member ports : 5-28
Static ports  : 5-28
Current Tagged ports :
Current Untagged ports : 5-28
Static Tagged ports :
Static Untagged ports : 5-28
Forbidden ports :
Total Entries : 1
```

Для того, чтобы создать новый VLAN используется команда **create vlan** с указанием имени и тега. После чего конфигурируем созданный VLAN при помощи команды **config vlan** с указанием названия VLAN на добавление указанного в задании количества компьютеров без тега (например, **add untagged 1-4**).

Полный скрипт для создания и конфигурации VLAN на основе портов приведен ниже:

```
DES-3800:admin#create vlan VLAN1 tag 11
Command: create vlan VLAN1 tag 11
Success.
Command: config vlan VLAN1 add untagged 1-4
Success.
```

DES-3800:admin#create vlan VLAN2 tag 22

Command: create vlan VLAN2 tag 22

Success.

DES-3800:admin#config vlan VLAN2 add untagged 5-10

Command: config vlan VLAN2 add untagged 5-10

Success.

DES-3800:admin#create vlan VLAN3 tag 33

Command: create vlan VLAN3 tag 33

Success.

DES-3800:admin#config vlan VLAN3 add untagged 11-18

Command: config vlan VLAN3 add untagged 11-18

Success.

DES-3800:admin#create vlan VLAN4 tag 44

Command: create vlan VLAN4 tag 44

Success.

DES-3800:admin#config vlan VLAN4 add untagged 19-23

Command: config vlan VLAN4 add untagged 19-23

Success.

После создания всех VLAN снова выводим всю информацию о существующих VLAN при помощи команды **show vlan**:

DES-3800:admin#show vlan

Command: show vlan

VID : 1 VLAN Name : default

VLAN TYPE : static Advertisement : Enabled

Member ports : 25-28

Static ports : 25-28

Current Tagged ports :

Current Untagged ports : 25-28

Static Tagged ports :

Static Untagged ports : 25-28

Forbidden ports :

VID : 11 VLAN Name : VLAN1
VLAN TYPE : static Advertisement : Disabled
Member ports : 1-4
Static ports : 1-4
Current Tagged ports :
Current Untagged ports : 1-4
Static Tagged ports :
Static Untagged ports : 1-4
Forbidden ports :
VID : 22 VLAN Name : VLAN2
VLAN TYPE : static Advertisement : Disabled
Member ports : 5-10
Static ports : 5-10
Current Tagged ports :
Current Untagged ports : 5-10
Static Tagged ports :
Static Untagged ports : 5-10
Forbidden ports :
VID : 33 VLAN Name : VLAN3
VLAN TYPE : static Advertisement : Disabled
Member ports : 11-18
Static ports : 11-18
Current Tagged ports :
Current Untagged ports : 11-18
Static Tagged ports :
Static Untagged ports : 11-18
Forbidden ports :
VID : 44 VLAN Name : VLAN4
VLAN TYPE : static Advertisement : Disabled
Member ports : 19-23
Static ports : 19-23

Current Tagged ports :
 Current Untagged ports : 19-23
 Static Tagged ports :
 Static Untagged ports : 19-23
 Forbidden ports :
 Total Entries : 5

3. Проверить работу созданных виртуальных сетей, определить временные задержки передачи трафика. Проверить возможность передачи трафика между сетями.

Проверка работы созданных виртуальных сетей производилась с помощью отправки тестовых пакетов по указанному IP-адресу. Пример выполнения тако проверки с использованием **ping** из командной строки показан на рис. 8.

```

Командная строка
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 2007. Все права защищены.

C:\Пользователи\user>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 32 байт:

Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Пользователи\user>_
  
```

Рис. 8. Проверка работы виртуальных сетей.

Далее было необходимо проверить возможность передачи трафика между сетями. Для этого также использовалась команда **ping**, но, в данном случае, как видно на рис. 9, передача не удалась.

```

Командная строка - ping 192.168.1.1

C:\Пользователи\user>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 32 байт:

Превышен интервал ожидания для запроса.
  
```

Рис. 9. Проверка передачи трафика между сетями.

- Удалить созданные виртуальные сети. Прodelать пункт 1 при помощи web-интерфейса.

Настройка IP-адреса производится на вкладке Administration->IP Address.

Процесс настройки изображен на рис. 10.

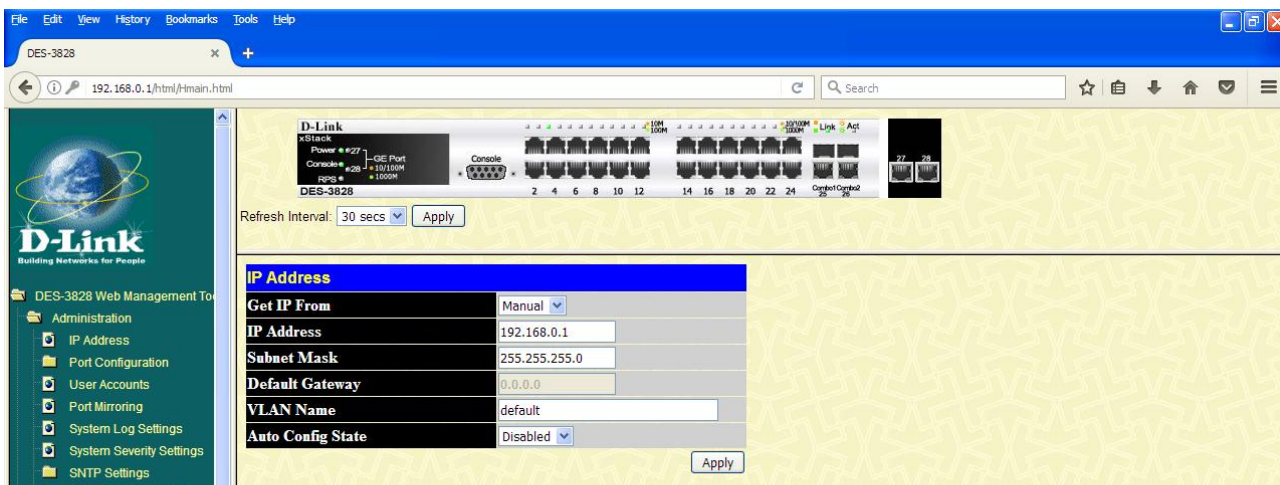


Рис. 10. Настройка статического IP-адреса.

Удаление виртуальных сетей происходит также, как в Задании 2, с помощью команды **config vlan default delete 1–24**.

После этого в Web-версии переходим во вкладку L2 Features->VLAN->Static VLAN Entry. Откроется окно, в котором можно создать новую сеть. Процесс создания сети показан на рис. 11.

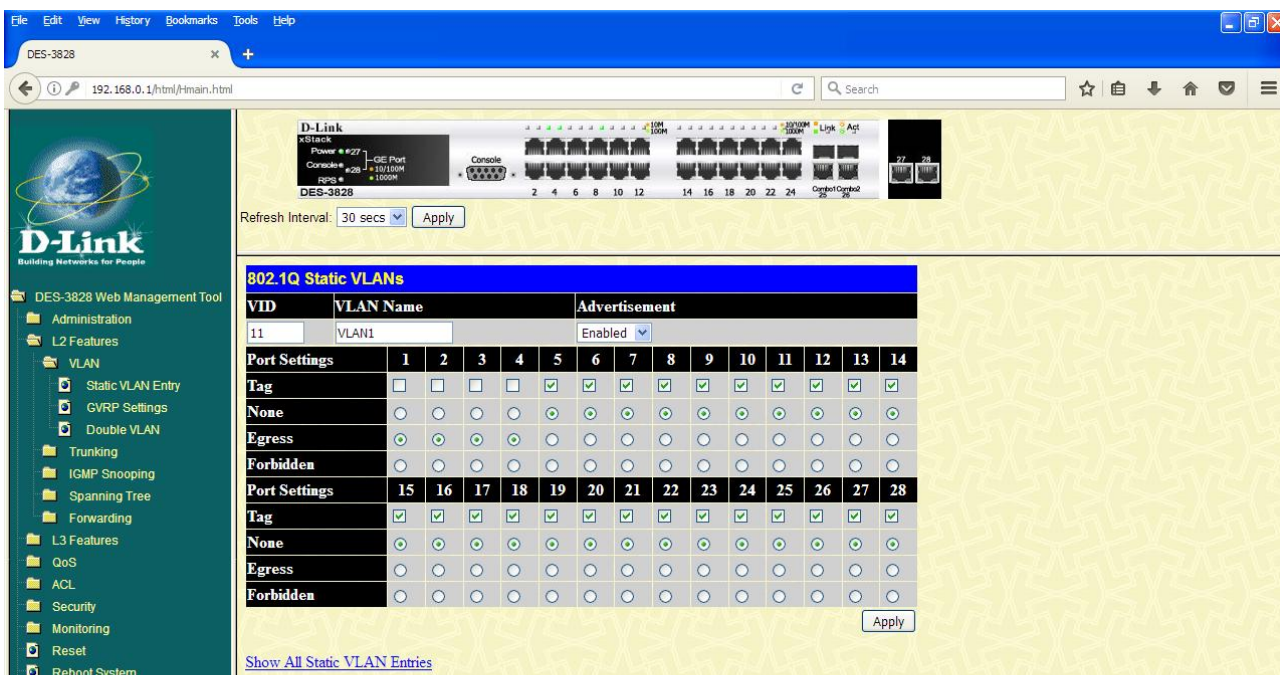


Рис. 11. Создание нового VLAN.

После создания VLAN также можно просмотреть их полный список, нажав на ссылку внизу (на рис. 12 показан список всех созданных VLAN):

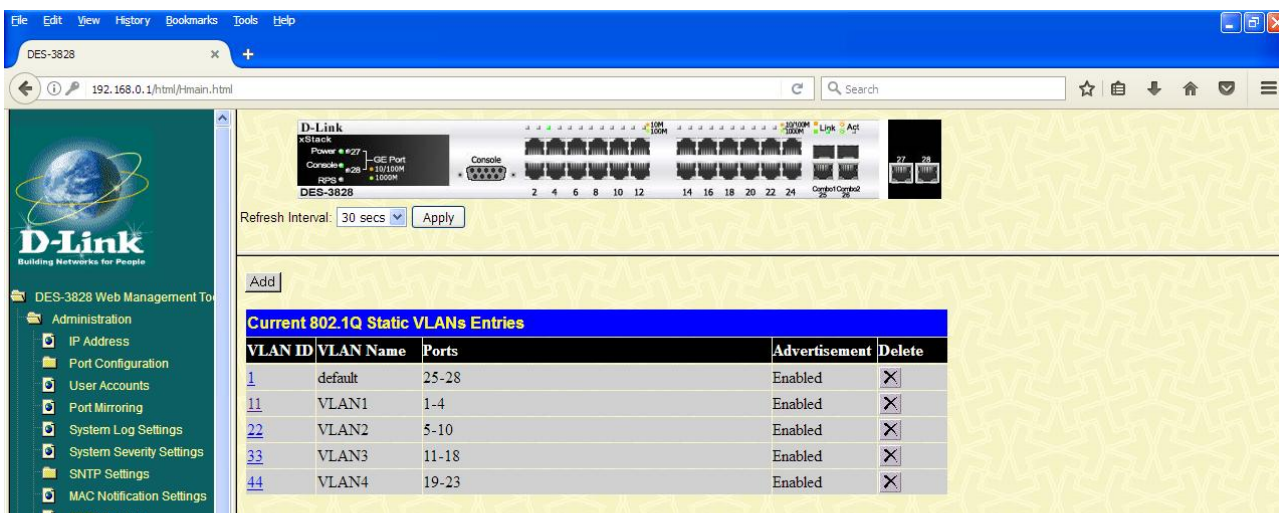


Рис. 12. Список созданных VLAN.

5. Подключить маршрутизатор cli-804 к коммутатору для обеспечения связи между VLAN. Объяснить то, каким образом осуществляется трансляция пакетов в таком случае. Замерить временные задержки при передаче трафика, провести трассировку маршрута. Провести подключение компьютера одной VLAN к порту другой. Пояснить, что произошло при этом.

После подключения маршрутизатора проверяем связь между VLAN путем отправки тестовых пакетов. Производим эту операцию при помощи команды **ping**. Проверка связи приведена на рис. 13.

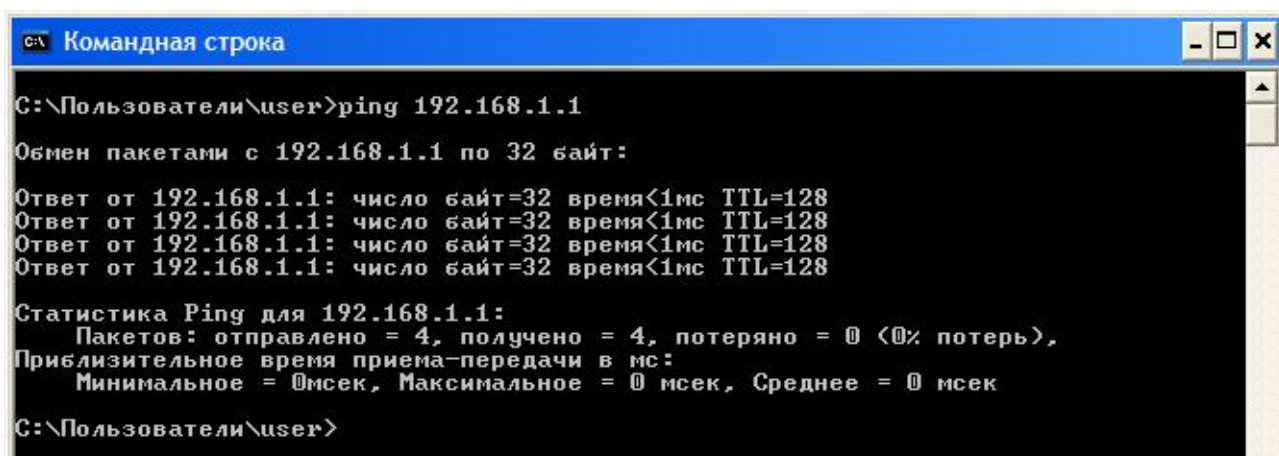


Рис. 13. Проверка наличия связи.

Далее производим трассировку маршрута через маршрутизатор. Для этих целей используем команду **tracert**, результат выполнения которой продемонстрирован на рис. 14.

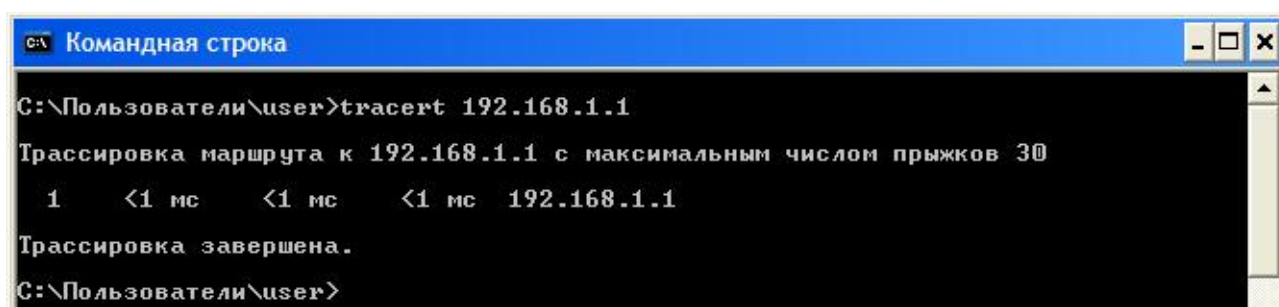


Рис. 14. Трассировка маршрута, проходящего через маршрутизатор.

6. Написать скрипт, удаляющий на коммутаторе все существующие VLAN, создающий 3 VLAN на основе стандарта IEEE 802.1q. Количество узлов в VLAN:

VLAN1 --- 2
 VLAN2 --- 4
 VLAN3 --- 2

Command: create vlan VLAN1 tag 11

Command: config vlan VLAN1 add untagged 1-1

Command: config vlan VLAN1 add tagged 2

Command: create vlan VLAN2 tag 22

Command: config vlan VLAN2 add untagged 3-5

Command: config vlan VLAN2 add tagged 6

Command: create vlan VLAN3 tag 33

Command: config vlan VLAN3 add untagged 7-7

Command: config vlan VLAN3 add tagged 8

7. Поможет ли в данном случае использование маршрутизатора для обеспечения связи между VLAN.

Нет, не поможет. С помощью маршрутизатора соединим VLAN1 и VLAN2 через порты 2 и 6 соответственно. После этого, используя команду **ping** проверим возможность доставки пакетов между компьютерами из разных сетей VLAN . Доставка невозможна, поскольку пакет содержал информацию,

предназначенную для другой VLAN, потому и был отброшен принимаемым портом.

8. К двум из портов коммутатора подключены серверные станции. Необходимо разбить оставшиеся порты на 3 VLAN, настроить сегментацию и ограничения пропускной способности трафика, таким образом, что допустимый трафик на серверные станции между сетями трафик поделен в пропорции 2/4/8.

Для разбиения портов на 3 VLAN воспользуемся web-интерфейсом. Шаги по созданию новых VLAN дублируют пункт 4. Список всех созданных VLAN показан на рис. 15.

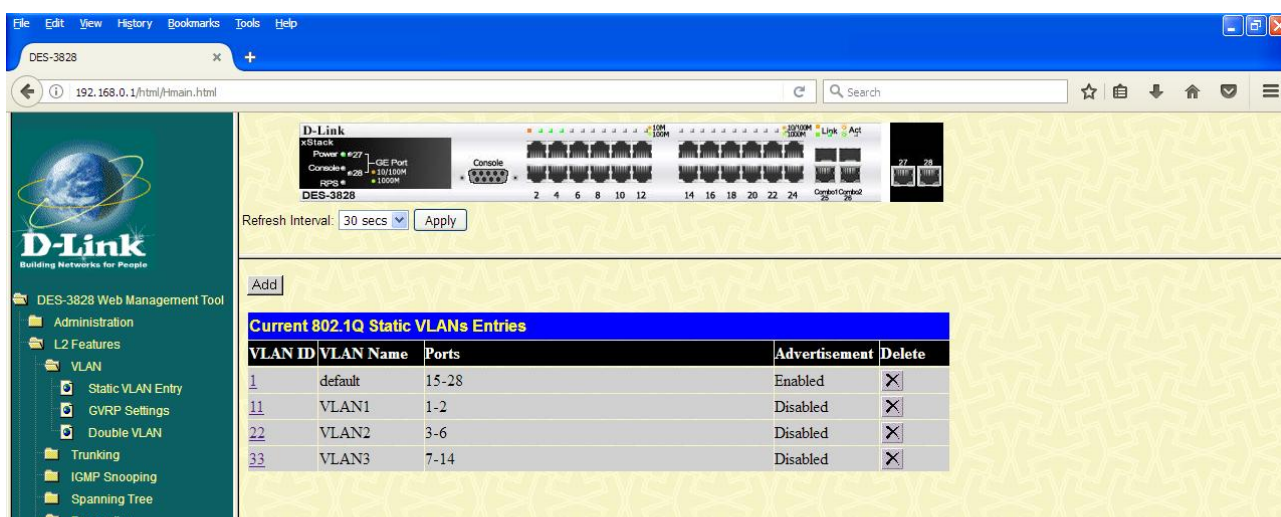


Рис. 15. Разбиение портов в пропорции 2/4/8 на 3 VLAN.

Следующим шагом является настройка сегментации трафика и ограничение его пропускной способности. Для этих целей используются команды **config traffic_segmentation** и **config bandwidth_control**.

Сначала в команде указываются порты, которые будут передавать кадры, а после ключевого слова **forward** указываются порты, которым будут передаваться кадры. Процесс выполнения данных команд представлен на рис. 16.

```

DES-3800:admin#config traffic_segmentation 1-2 forward_list 26-27
Command: config traffic_segmentation 1-2 forward_list 26-27

Success.

DES-3800:admin#config traffic_segmentation 3-6 forward_list 26-27
Command: config traffic_segmentation 3-6 forward_list 26-27

Success.

DES-3800:admin#config traffic_segmentation 7-14 forward_list 26-27
Command: config traffic_segmentation 7-14 forward_list 26-27

Success.

DES-3800:admin#show traffic_segmentation
Command: show traffic_segmentation

```

Traffic Segmentation Table

Время подключения: 2:08:33 Автовыбор 9600 8-N-1 SCROLL CAPS NUM Запись протокола Эхо

Рис. 16. Настройка сегментации и пропускной способности трафика.

Чтобы посмотреть лист сегментации вводим команду **show traffic_segmentation**. Результат выполнения данной команды представлен на рис. 17.

```

qqq - HyperTerminal
Файл Правка Вид Вызов Передача Справка
DES-3800:admin#show traffic_segmentation
Command: show traffic_segmentation

```

Port	Forward Portlist
1	26-27
2	26-27
3	26-27
4	26-27
5	26-27
6	26-27
7	26-27
8	26-27
9	26-27
10	26-27
11	26-27
12	26-27
13	26-27
14	26-27
15	1-28
16	1-28
17	1-28
18	1-28

CTRL+C ESC Quit SPACE Next Page ENTER Next Entry All

Время подключения: 2:08:00 Автовыбор 9600 8-N-1 SCROLL CAPS NUM Запись протокола Эхо

Рис. 17. Таблица сегментации трафика.

Для ограничения пропускной способности с помощью команды **config bandwidth_control** в параметрах команды указываем порты, для которых настраиваем скорость передачи, а после ключевого слова **tx_rate** непосредственно скорость передачи в Мбит/с.

```

DES-3800:admin#config bandwidth_control 1-2 tx_rate 10
Command: config bandwidth_control 1-2 tx_rate

Next possible completions:
no_limit          <value 64-1000000>

DES-3800:admin#config bandwidth_control 1-2 tx_rate 1000
Command: config bandwidth_control 1-2 tx_rate 1000

The TX setting value is not a multiple of 64, closest value 960 is choosed.
Success.

DES-3800:admin#config bandwidth_control 3-6 tx_rate 1920
Command: config bandwidth_control 3-6 tx_rate 1920

Success.

DES-3800:admin#config bandwidth_control 7-14 tx_rate 3840
Command: config bandwidth_control 7-14 tx_rate 3840

Success.

```

Рис. 18. Ограничение пропускной способности трафика.

9. К двум из портов коммутатора подключены серверные станции. Запретить доступ к ним для 2-х выбранных компьютеров класса.

Описанные ниже действия по запрещению доступа проводились на примере одного компьютера.

Используя web-интерфейс создаем запись доступа **Access Profile Table** для Ethernet. Созданная запись доступа продемонстрирована на рис. 19.

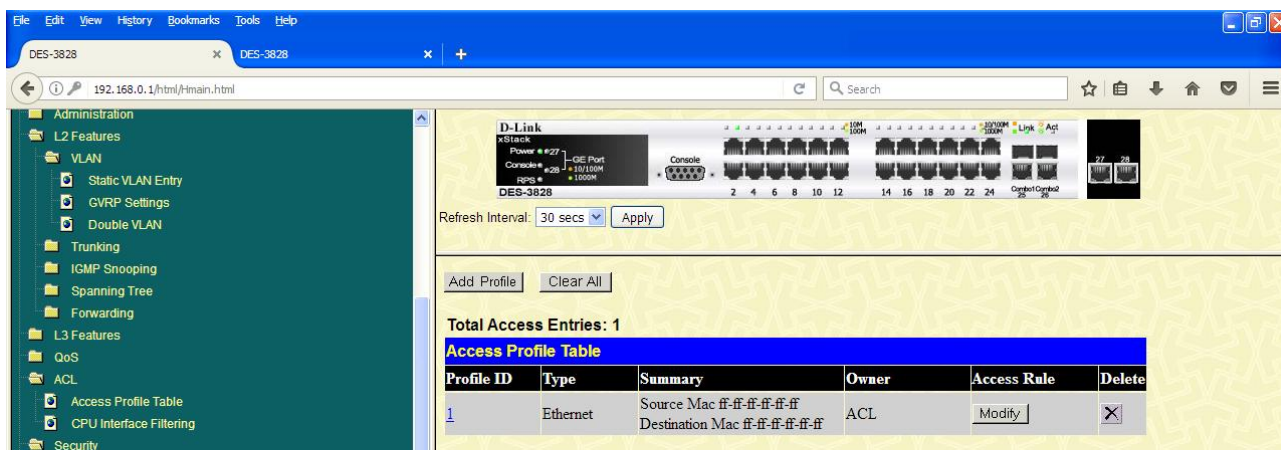


Рис. 19. Запись доступа в Access Profile Table.

После этого, требуется настроить правила доступа **Access Profile Rules**, связанные с маской. Правила доступа будут касаться ограничений для MAC-адреса определенного компьютера. Ниже, на рис. 20, приведен пример создания таких правил: требуется указать тип профиля доступа, а также MAC-адрес отправителя пакетов и MAC-адрес получателя пакетов, кроме того, указываем номер порта, через который будет блокироваться передача.

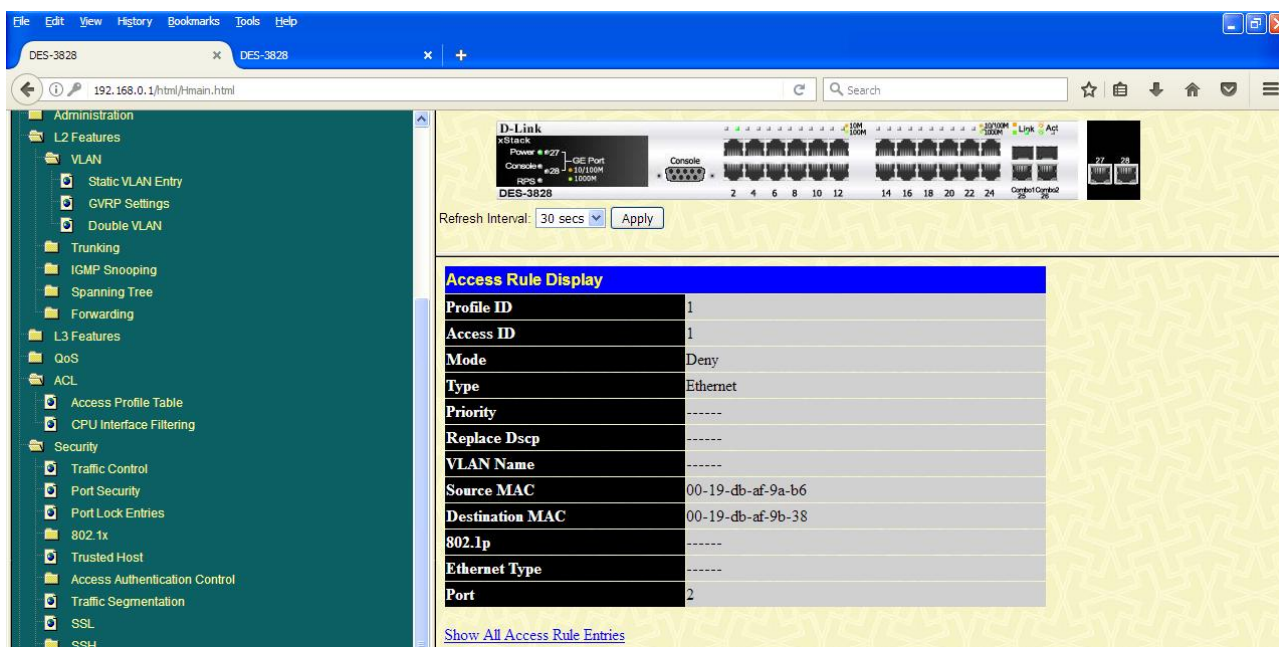


Рис. 20. Создание правил доступа Access Profile Rules.

3. Вывод

В ходе выполнения лабораторной работы были изучены основы работы с коммутаторами третьего уровня, была произведена настройка коммутатора как через консольный порт, так и через Ethernet, освоены навыки работы с коммутатором посредством консольных команд и через web-интерфейс.