



**Лабораторные работы для курса
«Технологии коммутации и
маршрутизации современных
сетей Ethernet.
Базовый курс D-Link»**

(с применением коммутаторов DES-3810-28 и DES-3200-28 rev.C1)

Версия 3.2

Москва, 2014

Оглавление

Рекомендации по организации лабораторных работ.....	3
БАЗОВЫЙ НАБОР.....	4
Лабораторная работа №1. Основные команды коммутатора.....	4
Лабораторная работа №2. Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов.....	16
Лабораторная работа №3. Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы.....	20
Лабораторная работа №4. Настройка VLAN на основе стандарта IEEE 802.1Q.....	23
Лабораторная работа №5. Настройка протокола GVRP.....	28
Лабораторная работа №6. Настройка сегментации трафика без использования VLAN.....	31
Лабораторная работа №7. Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.....	33
Лабораторная работа №8. Настройка протоколов связующего дерева STP, RSTP, MSTP.....	37
Лабораторная работа №9. Настройка функции защиты от образования петель LoopBack Detection.....	50
Лабораторная работа №10. Агрегирование каналов.....	55
Лабораторная работа №11. Настройка QoS. Приоритизация трафика. Управление полосой пропускания.....	59
Лабораторная работа №12. Списки управления доступом (Access Control List).....	63
Лабораторная работа №13. Контроль над подключением узлов к портам коммутатора. Функция Port Security.....	69
Лабораторная работа №14. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding.....	74
Лабораторная работа №15. Функции анализа сетевого трафика.....	78
Лабораторная работа №16. Настройка протокола управления топологией сети LLDP.....	81
Лабораторная работа №17. Итоговая самостоятельная работа.....	85
РАСШИРЕННЫЙ НАБОР.....	89
Лабораторная работа №18. Настройка функции Q-in-Q (Double VLAN).....	89
Лабораторная работа №19. Настройка статической и динамической маршрутизации IPv4.....	93
Лабораторная работа №20. Установка и настройка протокола IPv6 на рабочей станции и коммутаторе D-Link.....	101
Лабораторная работа №21. Разрешение IPv6-адресов с помощью протокола Neighbor Discovery Protocol (NDP).....	106
Лабораторная работа №22. Настройка функции CPU Interface Filtering для IPv6.....	109
Лабораторная работа №23. Настройка маршрутизации IPv6 в пределах одного коммутатора.....	112
Лабораторная работа №24. Настройка статической и динамической маршрутизации IPv6.....	114

Рекомендации по организации лабораторных работ

Лабораторные работы по курсу умышленно разделены на базовый и расширенный функционал.

Базовый набор включает изучение и настройку функций 2-го уровня модели OSI. Для выполнения базового набора лабораторных работ рекомендуется следующий комплект оборудования, из расчёта на учебную группу, состоящую из 10 человек:

Коммутатор DES-3200-28 rev.C1	8 шт.
Коммутатор DES-3810-28	2 шт.
Коммутатор DES-1005A	5 шт.
Рабочая станция	20 шт.
Кабель Ethernet	35 шт.
Консольный кабель	10 шт.

Расширенный функционал предназначен для изучения 3-го уровня модели OSI, а именно основ маршрутизации и адресации IPv6. Расширенный набор лабораторных работ дополняет базовый и может выполняться факультативно. Для выполнения расширенного набора лабораторных работ рекомендуется следующий комплект оборудования, из расчёта на учебную группу, состоящую из 10 человек:

Коммутатор DES-3810-28	6 шт.
Коммутатор DES-3200-28 rev.C1	8 шт.
Коммутатор DES-1005A	5 шт.
Рабочая станция	20 шт.
Консольный кабель	14 шт.
Кабель Ethernet	35 шт.

Каждая лабораторная работа содержит схему установки с указанием количества рабочих мест, на которое она рассчитана.

Настройка коммутаторов осуществляется через интерфейс командной строки путём подключения управляющей рабочей станции к его консольному порту.

Команды в лабораторных работах приведены для коммутаторов со следующими версиями программного обеспечения:

Коммутатор DES-3810-28 – ПО v2.20.010.had или выше

Коммутатор DES-3200-28 rev.C1 – ПО v4.00.024.had или выше

Для проведения лабораторных работ потребуется ПО:

1. Генератор трафика *iperf* (<http://sourceforge.net/projects/iperf/>);
2. TFTP-сервер *Tftpd32* (<http://tftpd32.jounin.net>);
3. Анализатор трафика *Wireshark* (<http://www.wireshark.org>).
4. Программа эмуляции терминала *Putty* (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>)

БАЗОВЫЙ НАБОР

Лабораторная работа №1. Основные команды коммутатора

Для настройки различных функций коммутаторов при выполнении практических работ будет использоваться интерфейс командной строки (CLI), так как он обеспечивает более тонкую настройку устройства.

Все команды CLI являются чувствительными к регистру, поэтому прежде чем вводить команду, надо убедиться, что отключены все функции, которые могут привести к изменению регистра текста.

При работе в CLI можно вводить сокращённый вариант команды. Например, если ввести команду «sh sw», то коммутатор интерпретирует эту команду как «show switch».

Для описания ввода команд, ожидаемых значений и аргументов при настройке коммутатора через интерфейс командной строки (CLI) используются следующие символы:

Таблица 1

<угловые скобки >	
Назначение	Содержат ожидаемую переменную или значение, которое должно быть указано.
Синтаксис	config ipif <System> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable]}] bootp dhcp]
Описание	В приведённом примере синтаксиса, пользователь должен указать имя IP-интерфейса System, имя VLAN vlan_name длиной до 32 символов и сетевой адрес network_address . Сами угловые скобки вводить не надо.
Пример	config ipif System ipaddress 10.24.22.5/8 vlan Sales
[квадратные скобки]	
Назначение	Содержат требуемое значение или набор требуемых аргументов. Может быть указано одно значение или аргумент.
Синтаксис	create account [admin user] <username 15>
Описание	В приведённом примере синтаксиса, пользователь должен указать один из двух уровней привилегий (admin или user) для создаваемой учётной записи. Вводить квадратные скобки не надо.
Пример	create account admin user1
 вертикальная черта	
Назначение	Отделяет два или более взаимно исключающих пунктов из списка, один из которых должен быть введён/указан.
Синтаксис	create account [admin user] <username 15>
Описание	В приведённом примере синтаксиса, пользователь должен указать один из

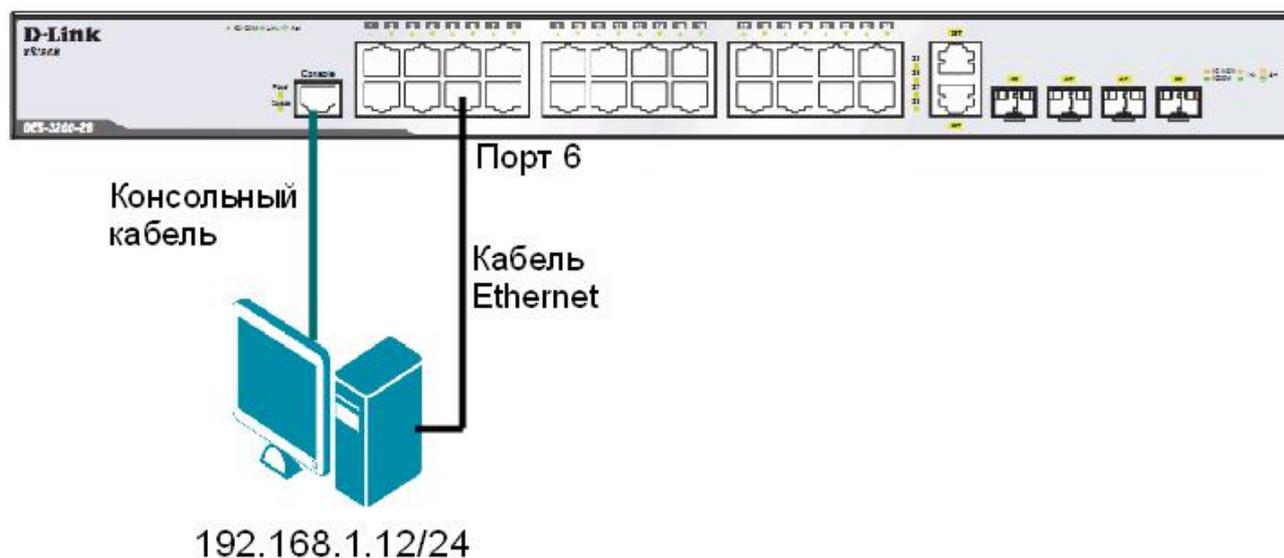
	двух уровней привилегий (admin или user) для создаваемой учётной записи. Вводить квадратные скобки не надо.
Пример	create account admin user1
{ фигурные скобки }	
Назначение	Содержит необязательное значение или набор необязательных аргументов.
Синтаксис	reset {[config system]} {force_agree}
Описание	В приведённом примере синтаксиса, пользователь может указать необязательное значение config или system. Его вводить необязательно, но результат выполнения команды будет зависеть от ввода дополнительного параметра.
Пример	reset config
(круглые скобки)	
Назначение	Показывает, что одно или более значений или аргументов, заключённых в фигурные скобки, должно быть введено.
Синтаксис	config dhcp_relay {hops <value 1-16> time <sec 0-65535>} (1)
Описание	В приведённом примере синтаксиса, от пользователя ожидается ввод одного или обоих необязательных параметров, заключённых в фигурные скобки. Параметр «(1)» показывает, что ожидается ввод, по крайней мере, одного из параметров или аргументов.
Пример	config dhcp_relay hops 3

Цель: познакомиться с основными командами настройки, поиска и устранения неполадок коммутаторов D-Link.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	1 шт.
Консольный кабель	1 шт.

Коммутатор
IP: 192.168.1.10/24



1.1 Вызов помощи по командам

Подключите компьютер к консольному порту коммутатора с помощью кабеля RS-232. После подключения к консольному порту коммутатора, на персональном компьютере запустите программу эмуляции терминала VT100 (например, *Putty* или программу *HyperTerminal* в Windows XP).

В программе *HyperTerminal* установите следующие параметры подключения:

Скорость (бит/с):	115200
Биты данных:	8
Чётность:	нет
Стоповые биты:	1
Управление потоком:	нет

В программе *Putty* установите следующие параметры подключения:

1. В категории *Session* выберите *Serial* и установите скорость 115200 (рис. 1.1);

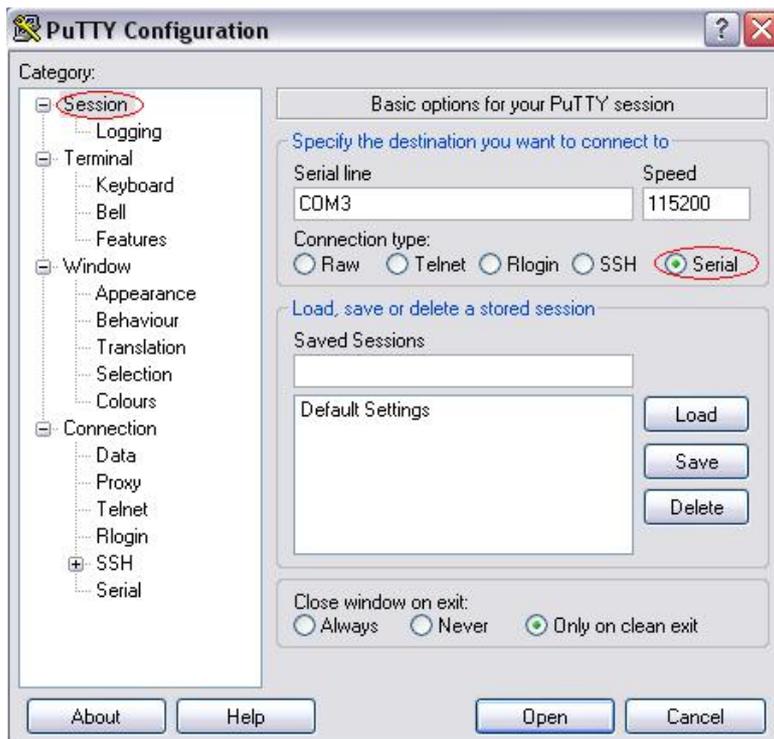


Рисунок 1.1 Окно программы Putty

2. В категории *Translation* установите *UTF-8* и нажмите *Open* (рис. 1.2);

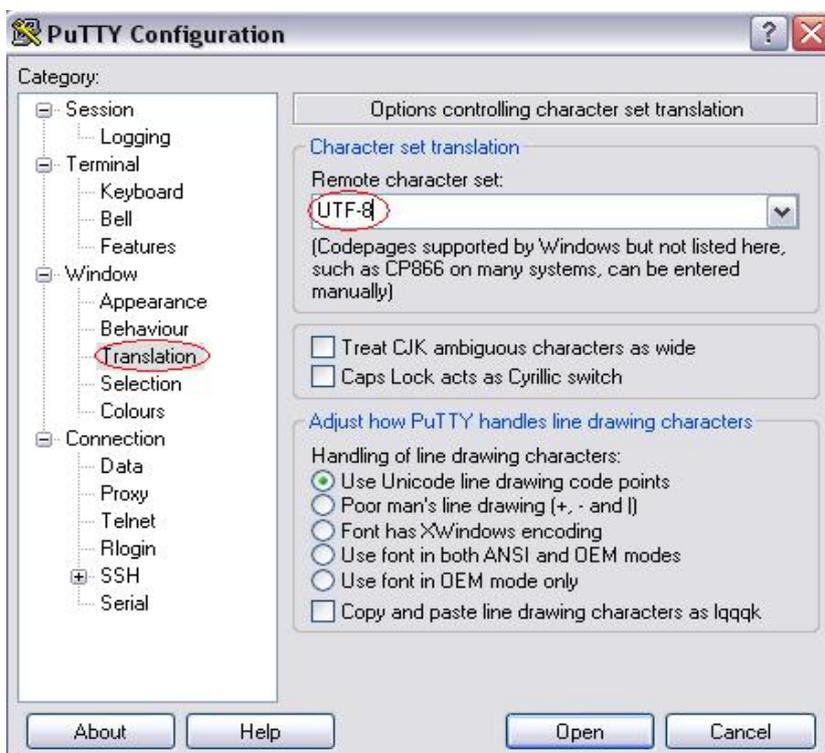


Рисунок 1.2 Окно программы Putty

3. В открывшемся окне нажмите клавишу *Enter* (рис. 1.3).

Примечание: по умолчанию на коммутаторе не определены *UserName* и *PassWord*, поэтому два раза нажмите клавишу *Enter*.

После этого появится приглашение для ввода команд:
DES-3200-28: #

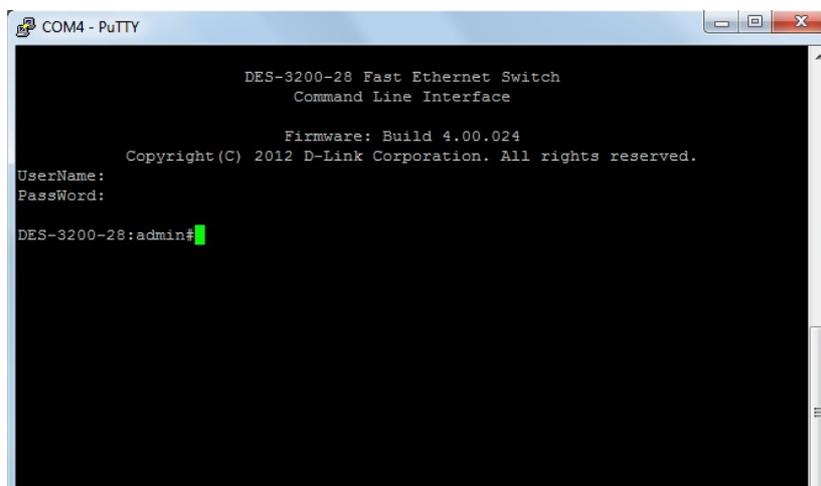


Рисунок 1.3 Окно эмуляции терминала VT100

В зависимости от версии ПО, может потребоваться установить скорость 9600 бит/с.

Внимание: при написании команд в CLI важно учитывать регистр. Для того чтобы ознакомиться с правильностью написания команд, последовательностью выполнения операций можно обращаться к встроенной помощи по командам!

Введите в консоли: ?

Введите в консоли: config

Введите в консоли: show

1.2. Изменение IP-адреса коммутатора

Посмотрите значение IP-адреса интерфейса управления коммутатора:
show ipif

Чему равен IP-адрес интерфейса управления коммутатора по умолчанию (вписать):

Измените IP-адрес интерфейса управления коммутатора:
config ipif System ipaddress 192.168.1.10/24

Настройте IP-адрес шлюза по умолчанию:
create iproute default 192.168.1.254

Примечание: IP-адрес шлюза по умолчанию должен быть назначен, если управление коммутатором будет осуществляться из других IP-подсетей.

Проверьте настройки коммутатора:
show switch

1.3. Настройка времени на коммутаторе

Проверьте время:

```
show time
```

Введите новую дату и время:

```
config time 01sep2013 15:45:30
```

Укажите текущую дату и время.

Установите часовой пояс Москва (GMT +4:00):

```
config time_zone operator + hour 4 min 0
```

Проверьте время:

```
show time
```

Примечание: установка времени необходима для правильного отображения информации в журналах регистрации коммутаторов (Log files), проведения аудита работы сети, мониторинга сети и т.п.

1.4. Управление учетными записями пользователей

Внимание: существует три основных уровня привилегий пользователей: *Admin* – максимальные права управления коммутатором, *Operator* – средние права управления (мониторинг сети, чтение системных параметров и конфигураций), *User* – минимальные права, в основном на чтение.

Длина имени пользователя должна быть от 1 до 15 символов, длина пароля от 0 до 15 символов, максимальное количество пользователей 8.

Никогда не сохраняйте настройки конфигурации после создания пользователей не проверив, можете ли вы зайти с созданной учётной записью в систему! В случае утраты сведений о Логине и Пароле, разблокировать коммутатор можно только в сервисном центре компании D-Link!

Создайте учётную запись администратора:

```
create account admin dlink
```

Укажите пароль и подтверждение пароля администратора: dlink

```
Enter a case-sensitive new password: dlink
```

```
Enter the new password again for confirmation: dlink
```

Для выхода из режима с текущими правами введите команду:

```
logout
```

Осуществить вход, введя параметры созданной учётной записи администратора:

```
Username: dlink
```

```
Password: dlink
```

```
DES-3200-28#
```

Создайте учётную запись пользователя:

```
create account user swuser
```

Укажите пароль и подтверждение пароля пользователя: dlink1
Enter a case-sensitive new password: dlink1
Enter the new password again for confirmation: dlink1

Проверьте настройки учётных записей пользователей:
show account

Измените пароль пользователя:
config account swuser

После ввода команды укажите старый пароль пользователя и 2 раза новый пароль.
Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****

Посмотрите список пользователей, подключенных к CLI коммутатора в настоящее время:
show session

Внимание: информация о паролях пользователей по умолчанию хранится в конфигурационном файле коммутатора в не зашифрованном виде. Для того чтобы избежать компрометации паролей, рекомендуется включать их шифрование на коммутаторе.

Активизируйте функцию шифрования паролей:
enable password encryption

Посмотрите текущую конфигурацию коммутатора, хранящуюся в RAM, и проверьте, зашифрованы ли пароли:
show config current_config

Отключите функцию шифрования паролей:
disable password encryption

Задайте пароль учётной записи пользователя, указав его использование без шифрования:
config account swuser encrypt plain_text dlink1

Убедитесь, что пароль учётной записи пользователя сохранён без шифрования:
show config current_config

Удалите учётную запись пользователя:
delete account swuser

Убедитесь в удалении учётной записи пользователя:
show account

1.5. Управление возможностью доступа к коммутатору через Web-интерфейс и Telnet

Для повышения безопасности сети, в том случае, если для доступа к коммутатору не используются Web-интерфейс или Telnet, рекомендуется их отключить (по умолчанию Web-интерфейс и Telnet на коммутаторе включены).

Отключите возможность подключения к коммутатору по Telnet:

```
disable telnet
```

Проверьте выполненные настройки:

```
show switch
```

Убедитесь, что доступ по Telnet отключён.

Выполните на рабочей станции ПК1 команду:

```
telnet <IP-адрес коммутатора>
```

Что вы наблюдаете? Запишите.

Включите функцию подключения к коммутатору по Telnet:

```
enable telnet
```

Проверьте выполненные настройки и убедитесь в возможности подключения к коммутатору по Telnet.

Протокол Telnet не предусматривает шифрование и не обеспечивает безопасность передаваемых данных. Протокол SSH обеспечивает безопасное соединение, путем шифрования передаваемых данных, включая пароли.

Включите возможность подключения к коммутатору по SSH:

```
enable ssh
```

Проверьте выполненные настройки:

```
show switch
```

Отключите возможность подключения к коммутатору по SSH:

```
disable ssh
```

Отключите возможность подключения к коммутатору через Web-интерфейс:

```
disable web
```

Проверьте выполненные настройки:

```
show switch
```

Убедитесь, что доступ к коммутатору через Web-интерфейс отключён.

Запустите на рабочей станции ПК1 браузер и введите в адресной строке IP-адрес коммутатора.

Что вы наблюдаете? Запишите.

Включите возможность подключения к коммутатору через Web-интерфейс и измените стандартный TSP-порт подключения на новый:

```
enable web 8008
```

Запустите на рабочей станции ПК1 браузер, введите в адресной строке IP-адрес коммутатора и укажите новый TSP-порт подключения:
http://192.168.1.10:8008

1.6. Настройка параметров баннера приветствия

С целью упрощения идентификации пользователями активного сетевого оборудования, или создания его уникальных логотипов, возможно изменение баннера приветствия, который появляется в момент загрузки коммутатора. Также возможно изменение приглашения Command Prompt в командной строке CLI.

Измените приглашение Command Prompt:

```
config command_prompt TEST_SWITCH
```

Установите приглашение по умолчанию:

```
config command_prompt default
```

Посмотрите баннер приветствия:

```
show greeting_message
```

Войдите в режим редактирования баннера приветствия:

```
config greeting_message
```

Для редактирования приветствия, используйте следующие команды:

<Function Key>	<Control Key>
Ctrl+C	Выйти без сохранения
Ctrl+W	Сохранить и выйти
left/right/up/down	Переместить курсор
Ctrl+D	Удалить линию
Ctrl+X	Стереть все настройки
Ctrl+L	Перезагрузить первоначальные настройки

Добавьте строку в приветствие:

```
SWITCH_TEST tel +7(495) 000-00-00
```

Сохраните изменения в приветствии и выйдите из режима редактирования:

```
Ctrl+W
```

Проверьте изменённый баннер приветствия:

```
show greeting_message
```

```
=====
DES-3200-28 Fast Ethernet Switch
Command Line Interface
SWITCH_TEST tel +7(495) 000-00-00
Firmware: Build 4.00.024
Copyright(C) 2012 D-Link Corporation. All rights reserved.
=====
```

Восстановите настройки баннера по умолчанию:

```
config greeting_message default
```

Проверьте баннер приветствия:

```
show greeting_message
```

1.7. Настройка основных параметров портов коммутатора

Посмотрите текущие настройки портов:

```
show ports
```

Измените скорость и режим работы портов 1-6:

```
config ports 1-6 speed 10_half
```

Проверьте выполненные настройки:

```
show ports
```

Что вы наблюдаете? Запишите.

Активизируйте функцию управления потоком на портах 1-6:

```
config ports 1-6 flow_control enable
```

Проверьте настройки:

```
show ports
```

Отключите работу портов 1-6:

```
config ports 1-6 state disable
```

Проверьте настройки:

```
show ports
```

Проверьте соединение между ПК1 и коммутатором. На ПК1 выполните команду:

```
ping 192.168.1.10
```

Что вы наблюдаете? Запишите.

Включите работу порта 6:

```
config ports 6 state enable
```

Проверьте соединение между ПК1 и коммутатором.

На ПК1 выполните команду:

```
ping 192.168.1.10
```

Что вы наблюдаете? Запишите.

Задайте описание порта 6:

```
config ports 6 description PC_PORT
```

Проверьте описание портов:

```
show ports description
```

1.8. Сохранение конфигурации в энергонезависимой памяти

Сохраните конфигурацию, хранимую в RAM, в первый слот для конфигурации в энергонезависимой памяти (NVRAM):

```
save config 1
```

или короче (сохранение сразу в активный слот конфигурации):

```
save
```

1.9. Команды мониторинга сети

Посмотрите статистику о пакетах, передаваемых и принимаемых портом 6 коммутатора:

```
show packet ports 6
```

Примечание: данная команда позволяет определять количественные характеристики передаваемых одноадресных, многоадресных и широковещательных пакетов. В случае возникновения в сети большого количества широковещательного трафика (более 15% от передаваемого), необходимо провести анализ сети на наличие DOS-атаки или неисправности.

Посмотрите статистику об ошибках передаваемых и принимаемых портом пакетов:

```
show error ports 6
```

Примечание: данная команда позволяет определять ошибки передаваемых данных и локализовать проблемы в коммутируемой сети.

Очистите счётчики статистики на порте:

```
clear counters ports 6
```

Примечание: в случае устранения выявленных ошибок или проверки отчёта загрузки портов, можно обнулить устаревшие данные.

Посмотрите загрузку ЦПУ коммутатора:

```
show utilization cpu
```

Внимание: в случае длительной загрузки CPU более 90%-100% необходимо проверить следующие характеристики:

1. Возможные атаки на коммутатор, неправильная настройка сети. Данная проблема может быть решена путём включения функции Safeguard Engine.

2. Неправильная настройка ACL или других функций коммутатора, влияющих на производительность и работу CPU.

3. Некорректная работа ПО (Firmware) коммутатора при работе некоторых функций. Данная проблема может быть решена путём обновления ПО коммутатора.

Посмотрите загрузку портов коммутатора:

```
show utilization ports
```

Примечание: с помощью данной команды можно посмотреть загрузку портов коммутатора и объем принимаемого и передаваемого ими трафика в секунду.

Посмотрите журнал работы коммутатора:

```
show log
```

Посмотрите журнал работы коммутатора с определенного индекса (ID):

```
show log index 5
```

Очистите журнал работы:

```
clear log
```

Протестируйте состояние медных кабелей, подключённых к портам коммутатора:

```
cable_diag ports all
```

Примечание: данная функция позволяет определить состояние пар, подключённого к порту коммутатора медного кабеля, а также его длину. Функция определяет следующие повреждения кабеля: разомкнутая цепь (*Open Circuit*) и короткое замыкание (*Short Circuit*).

1.10. Функция Factory Reset (сброс к заводским установкам)

Сбросьте текущие настройки коммутатора к настройкам по умолчанию командой:

```
reset
```

На коммутаторе восстановятся все заводские настройки по умолчанию, за исключением IP-адреса интерфейса управления, учётных записей пользователей и журнала регистраций. Коммутатор **не** произведёт сохранение сброшенных настроек в энергонезависимой памяти NVRAM и не перезагрузится.

Если указано ключевое слово **config**, на коммутаторе восстановятся все заводские настройки по умолчанию, включая IP-адрес интерфейса управления, учётные записи пользователей и журнал регистраций. Коммутатор **не** произведёт сохранение сброшенных настроек в энергонезависимой памяти NVRAM и не перезагрузится.

```
reset config
```

Если указано ключевое слово **system**, на коммутаторе восстановятся все заводские настройки по умолчанию в полном объеме. Коммутатор сохранит эти настройки в энергонезависимой памяти NVRAM и перезагрузится.

```
reset system
```

В случае необходимости, перезагрузить коммутатор можно командой:

```
reboot
```

Лабораторная работа №2. Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов

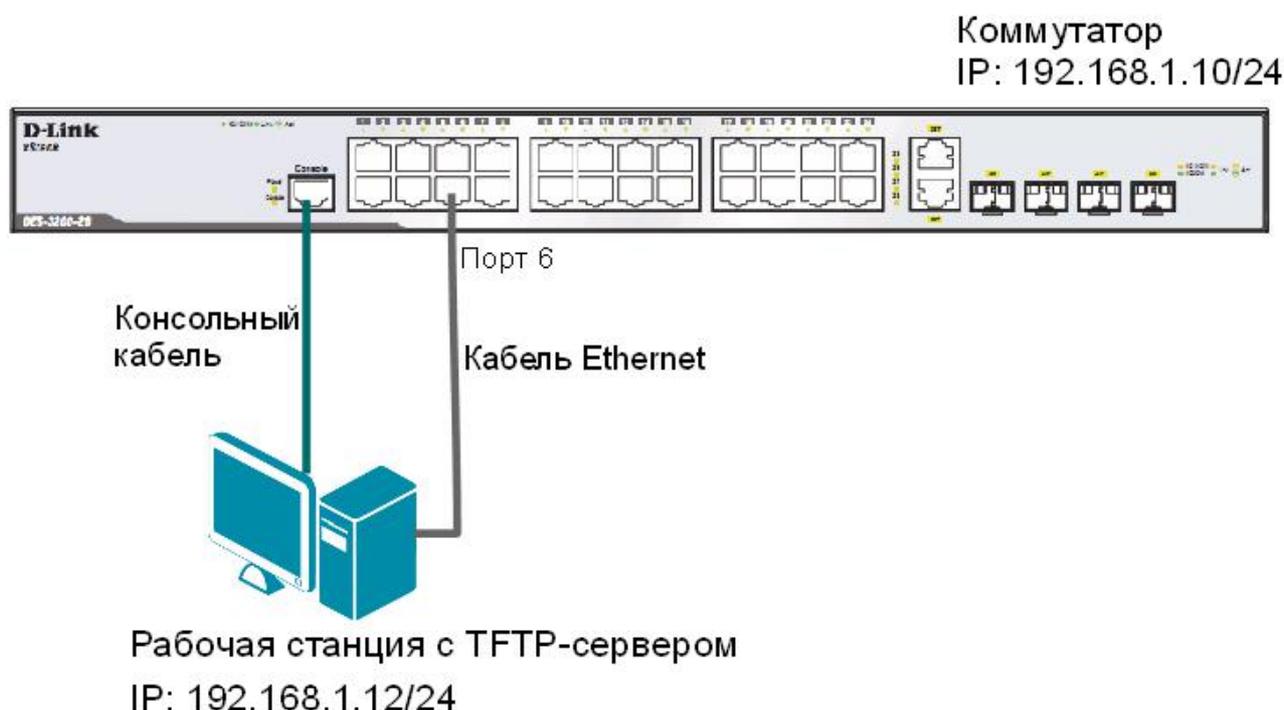
Обновление программного обеспечения (его иногда называют «прошивкой» коммутатора) может быть необходимо, когда доступна новая функциональность или требуется коррекция ошибок. Сохранять конфигурацию коммутатора необходимо при изменении его настроек, а также для упрощения восстановления функционирования коммутатора в результате сбоя его работы или поломки. Основным протоколом, применяемым для этих целей, служит протокол TFTP (Trivial File Transfer Protocol, простейший протокол передачи данных). Для передачи/загрузки программного обеспечения/конфигурации необходимо наличие в сети TFTP-сервера. Коммутаторы D-Link, поддерживают возможность хранения на коммутаторе двух версий программного обеспечения и конфигурации, причём любая из них может быть настроена как используемая при загрузке коммутатора. Это позволяет обеспечить отказоустойчивость оборудования при переходе на новое программное обеспечение или изменении конфигурации. Для изучения работы коммутатора, имеется возможность выгрузки через протокол TFTP журнала работы коммутатора.

Цель: изучить процесс обновления программного обеспечения и сохранения/восстановления конфигурации.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция с TFTP-сервером	1 шт.
Консольный кабель	1 шт.
Кабель Ethernet	1 шт.

Схема 2



2.1. Подготовка к режиму обновления и сохранения программного обеспечения коммутатора

Запустите на рабочей станции TFTP-сервер. В настройках программы выберите директорию приёма файлов:

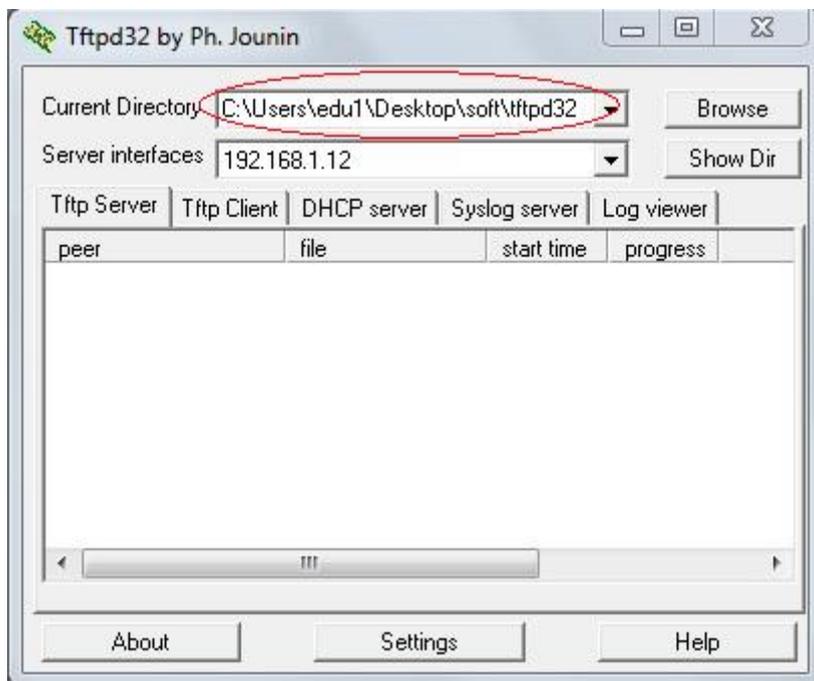


Рисунок 2.1 Выбор директории файлов

Подготовьте файл нового программного обеспечения коммутатора:

1. Найдите необходимый файл «прошивки» на сервере ftp://ftp.dlink.ru/;
2. Скачайте файл и перенесите его в директорию на TFTP-сервере;
3. Прочитайте файл сопровождения к «прошивке».

2.2. Загрузка файла программного обеспечения в память коммутатора

Все официальные версии ПО включают примечания, которые описывают новые функции и последние коррективы ошибок.

Внимание:

НЕ перезагружайте коммутатор во время обновления программного обеспечения.

Настройте IP-адрес интерфейса управления:

```
config ipif System ipaddress 192.168.1.10/24
```

Настройте TFTP-сервер:

Запустить TFTP-сервер, в настройках TFTP-сервера указать IP-адрес рабочей станции 192.168.1.12/24, указать директорию с прошивкой Current Directory.

Проверьте доступность TFTP-сервера с коммутатора:

```
ping 192.168.1.12
```

Проверьте информацию о текущем программном обеспечении коммутатора:

```
dir
```

Загрузите программное обеспечение на коммутатор (команда вводится в одну строку):

```
download firmware_fromTFTP 192.168.1.12 src_file DES-3200-26_28_C1_Run_v4.00.024.had dest_file DES_3200_runtime boot_up
```

Убедитесь, что программное обеспечение загружено:

```
dir
```

2.3. Настройка порядка загрузки программного обеспечения коммутатора

Задайте название файла программного обеспечения, которое будет загружаться при старте коммутатора:

```
config firmware image DES_3200_runtime boot_up
```

Сохраните изменения:

```
save
```

Обновлённая прошивка будет использована при следующей загрузке коммутатора.

Перезагрузите коммутатор:

```
reboot
```

После загрузки коммутатора проверьте информацию о программном обеспечении:

```
dir
```

Что вы наблюдаете?

2.4. Выгрузка и загрузка конфигурации

Посмотрите текущую версию конфигурации коммутатора (находящуюся в RAM):

```
show config current_config
```

Проверьте информацию об имеющихся в NVRAM конфигурациях коммутатора:

```
dir
```

Выгрузите конфигурацию №1 на TFTP-сервер:

```
upload cfg_toTFTP 192.168.1.12 dest_file config.txt
```

Откройте выгруженный конфигурационный файл любым текстовым редактором, например блокнотом, и просмотрите его структуру.

Замените IP-адрес 192.168.1.10/24 на 192.168.1.13/24:

```
# IP
```

```
config ipif System ipaddress 192.168.1.10/24  
disable autoconfig
```

Должно получиться так:

```
# IP
config ipif System ipaddress 192.168.1.13/24
disable autoconfig
```

Сохраните файл.

Загрузите изменённую конфигурацию на коммутатор в файл config_2:

```
download cfg_fromTFTP 192.168.1.12 src_file config.txt dest_file
config_2
```

Проверьте информацию об имеющихся в NVRAM конфигурациях коммутатора:

```
dir
```

Задайте номер конфигурации, которая будет загружаться при старте коммутатора:

```
config configuration config_2 boot_up
```

Чему будет равен IP-адрес после перезагрузки коммутатора? _____

Проверьте, изменился ли IP-адрес коммутатора:

```
show switch
```

Что вы наблюдаете?

2.5. Выгрузка log-файлов

Просмотрите журнал работы коммутатора:

```
show log
```

Выгрузите журнал работы на TFTP-сервер:

```
upload log_toTFTP 192.168.1.12 dest_file Logfiles.txt
```

Откройте выгруженный log-файл любым текстовым редактором, например блокнотом, и просмотрите его структуру.

Лабораторная работа №3. Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблица

Передача кадров коммутатором осуществляется на основе таблицы коммутации. Таблица коммутации может строиться коммутатором автоматически, на основе динамического изучения MAC-адресов источников поступающих на порты кадров, или создаваться вручную администратором сети. Коммутаторы третьего уровня также поддерживают таблицы коммутации IP-адресов, которые создаются динамически на основе изучения IP-адресов поступающих кадров.

ARP-таблица коммутатора хранит сопоставление IP- и MAC-адресов. ARP-таблица может строиться коммутатором динамически в процессе изучения ARP-запросов и ответов, передаваемых между устройствами подключёнными к его портам, или создаваться вручную администратором сети.

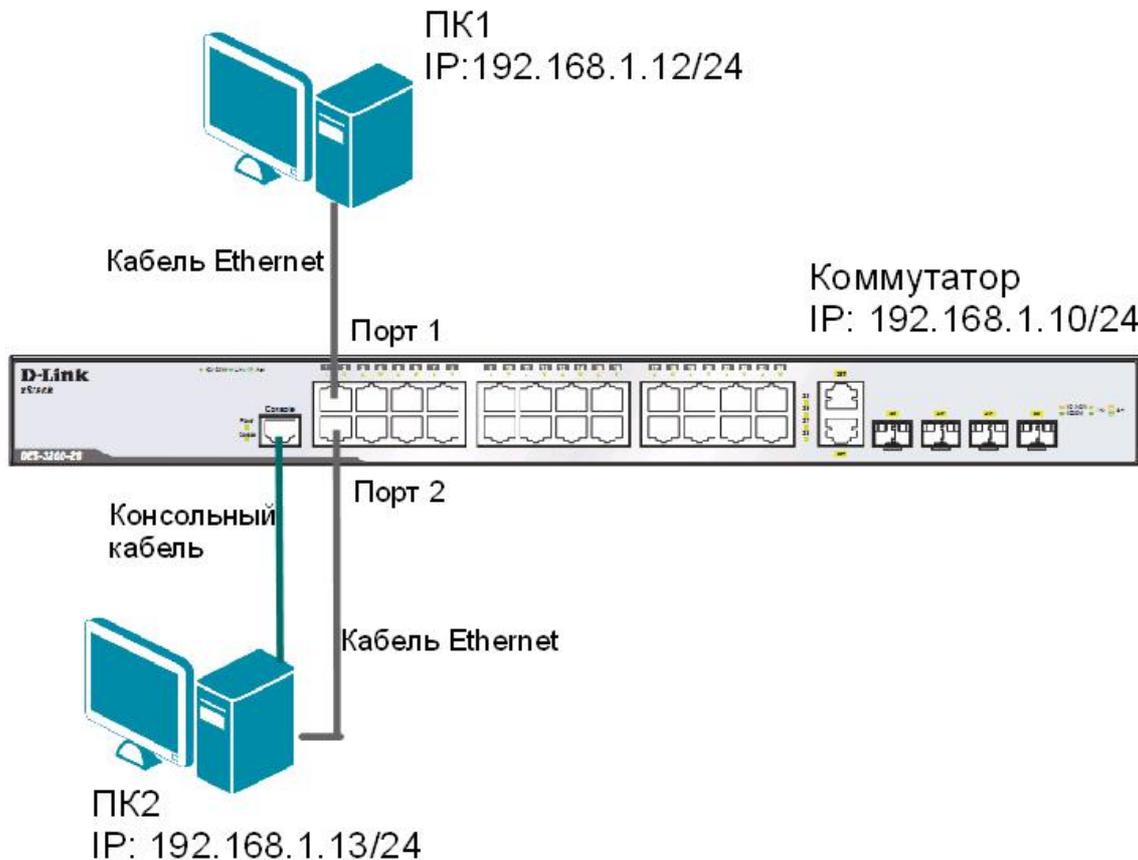
Умение работать с таблицами коммутации и ARP-таблицей позволяет диагностировать проблемы, возникающие в сети, например, атаки ARP Spoofing, а также отслеживать активность пользователей.

Цель: изучить процесс управления таблицей коммутации и ARP-таблицей.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	2 шт.
Консольный кабель	2 шт.
Кабель Ethernet	2 шт.

Схема 3



3.1. Команды управления таблицей коммутации

Просмотрите содержимое таблицы MAC-адресов:

```
show fdb
```

Определите порт коммутатора, к которому подключено устройство с известным MAC-адресом (в качестве MAC-адреса введите реальный MAC-адрес ПК1):

```
show fdb mac_address 00-03-47-BD-3F-57
```

Посмотрите список MAC-адресов устройств, принадлежащих VLAN по умолчанию (default VLAN):

```
show fdb vlan default
```

Посмотрите MAC-адреса устройств, изученные портом 2:

```
show fdb port 2
```

Просмотрите время нахождения записи в таблице MAC-адресов:

```
show fdb aging_time
```

Измените время нахождения MAC-адреса в таблице до 350 секунд:

```
config fdb aging_time 350
```

Удалите все динамически созданные записи из таблицы MAC-адресов:

```
clear fdb all
```

Создайте статическую запись в таблице MAC-адресов (в качестве MAC-адреса введите реальный MAC-адрес ПК2) на порте 2:

```
create fdb default 00-03-47-BD-01-11 port 2
```

Просмотрите статические записи в таблице MAC-адресов:

```
show fdb static
```

Просмотрите статические записи таблицы MAC-адресов на порте 2:

```
show fdb static port 2
```

Удалите статическую запись из таблицы MAC-адресов:

```
delete fdb default 00-03-47-BD-01-11
```

Просмотрите содержимое таблицы MAC-адресов:

```
show fdb
```

3.2. Команды управления ARP-таблицей

Просмотрите ARP-таблицу:

```
show arprentry
```

Найдите в ARP-таблице сопоставления IP-MAC по указанному IP-адресу:

```
show arprentry ipaddress 192.168.1.12
```

Просмотрите в ARP-таблице все сопоставления IP-MAC на интерфейсе System:

```
show arprentry ipif System
```

Удалите все динамически созданные записи из ARP-таблицы:

```
clear arptable
```

Убедитесь, что все динамические записи из таблицы удалены:

```
show arprentry
```

Создайте статическую запись в ARP-таблице (в качестве MAC-адреса укажите MAC-адрес ПК2):

```
create arprentry 192.168.1.12 00-50-BA-00-07-36
```

Просмотрите созданную статическую запись в ARP-таблице:

```
show arprentry static
```

Удалите статическую запись из ARP-таблицы:

```
delete arprentry 192.168.1.12
```

Проверьте, что запись удалена:

```
show arprentry static
```

Измените время нахождения записи в ARP-таблице до 30 минут (по умолчанию 20 минут):

```
config arp_aging time 30
```

Проверьте выполненные настройки:

```
show arprentry
```

Лабораторная работа №4. Настройка VLAN на основе стандарта IEEE 802.1Q

Виртуальная локальная сеть (Virtual Local Area Network, VLAN) представляет собой коммутируемый сегмент сети, который логически выделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического расположения пользователей. Виртуальные локальные сети обладают всеми свойствами физических локальных сетей, но рабочие станции можно группировать, даже если они физически расположены не в одном сегменте, т.к. любой порт любого коммутатора можно настроить на принадлежность определённой VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть. Кадры, предназначенные станциям не принадлежащим данной VLAN, должны передаваться через маршрутизирующее устройство (маршрутизатор или коммутатор 3-го уровня). Таким образом, с помощью виртуальных сетей решается проблема ограничений при передаче широковещательных кадров и вызываемых ими последствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Основные определения IEEE 802.1Q:

- *Tag* (Тег) – дополнительное поле данных длиной 4 байта, содержащее информацию о VLAN (идентификатор VLAN (12 бит), поле приоритета (3 бита), поле индикатора канонического формата (1 бит), добавляемое в кадр Ethernet;
- *Tagging* (Маркировка кадра) – процесс добавления информации (тега) о принадлежности к 802.1Q VLAN в заголовок кадра;
- *Untagging* (Удаление тега из кадра) – процесс извлечения информации 802.1Q VLAN из заголовка кадра;
- *Ingress port* (Входной порт) – порт коммутатора, на который поступают кадры, и принимается решение о принадлежности VLAN;
- *Egress port* (Выходной порт) – порт коммутатора, с которого кадры передаются на другие сетевые устройства (коммутаторы, рабочие станции) и на нем, соответственно, принимается решение о маркировке кадра.

Любой порт коммутатора может быть настроен как *tagged* (маркированный) или как *untagged* (немаркированный). Функция *untagging* позволяет работать с теми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать VLAN между несколькими коммутаторами, поддерживающими стандарт IEEE 802.1Q, подключать сетевые устройства, понимающие IEEE 802.1Q (например, серверы с сетевыми интерфейсами с поддержкой 802.1Q), обеспечивать возможность создания сложных сетевых инфраструктур.

Цель: понять технологию VLAN и её настройку на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

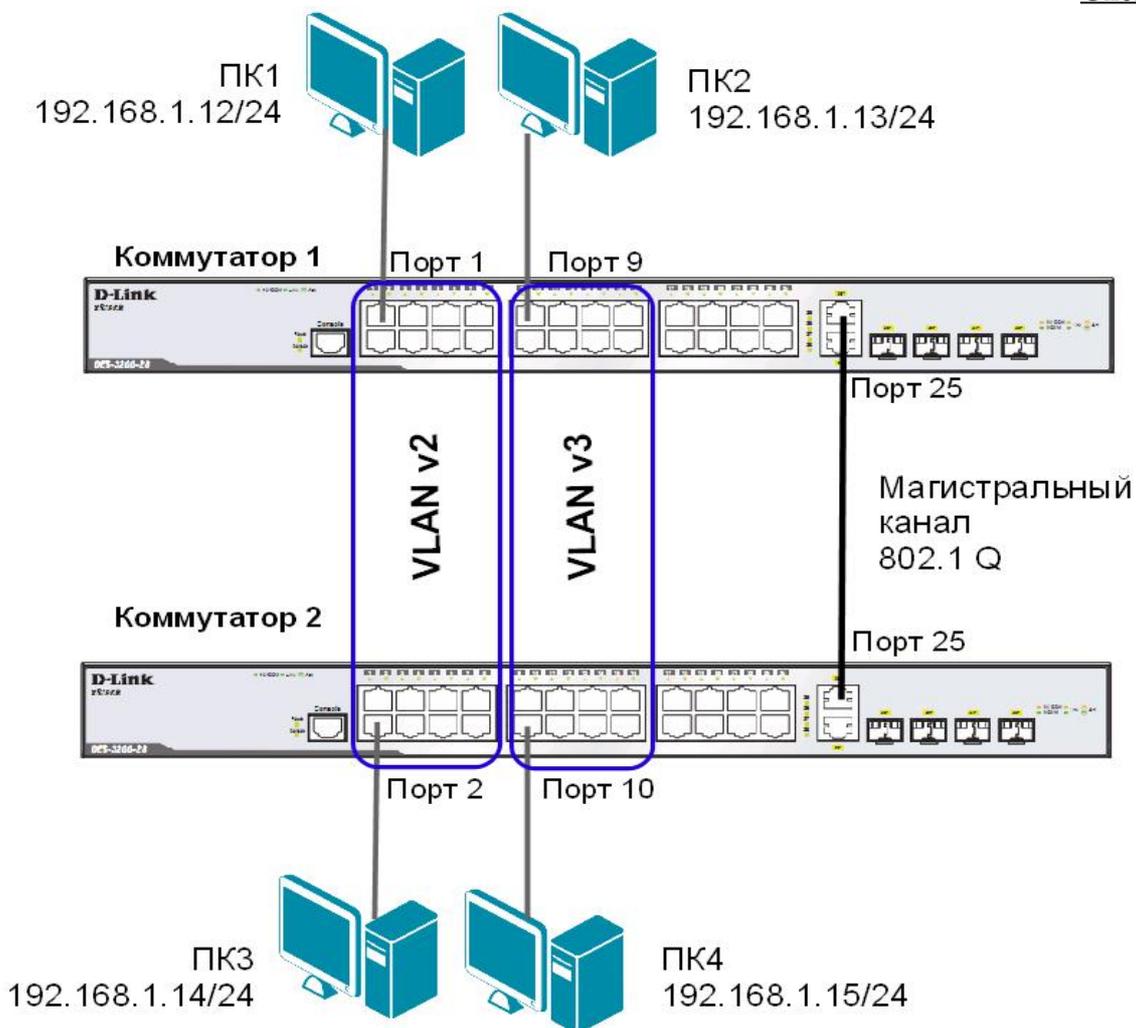
Коммутатор DES-3200-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

Перед выполнением лабораторной работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

4.1. Настройка VLAN на основе стандарта IEEE 802.1Q

Схема 4.1



Внимание: перед созданием новой VLAN, используемые в ней порты необходимо удалить из VLAN по умолчанию, т.к. в соответствии со стандартом IEEE 802.1Q, немаркированные порты не могут одновременно принадлежать нескольким VLAN.

Проверьте и запишите доступность соединения между рабочими станциями командой ping:
ping <IP-address>

~ от ПК1 к ПК 2, ПК 3 и ПК 4

~ от ПК2 к ПК 1, ПК 3 и ПК 4

Настройка коммутатора 1

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
config vlan default delete 1-16

Настройте порт 25 маркированным в vlan default:
config vlan default add tagged 25

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порт 25 маркированным:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-8
config vlan v2 add tagged 25
```

```
create vlan v3 tag 3
config vlan v3 add untagged 9-16
config vlan v3 add tagged 25
```

Проверьте настройки VLAN:

```
show vlan
```

Повторите процедуру настройки для коммутатора 2.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

```
~ от ПК1 к ПК 3           _____
~ от ПК2 к ПК4           _____
~ от ПК1 к ПК2 и ПК4     _____
~ от ПК2 к ПК1 и ПК3     _____
```

4.2. Настройка сегментации трафика внутри VLAN

Функция Traffic Segmentation (сегментация трафика) служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но имели доступ к разделяемым портам, используемым, например, для подключения серверов или магистральной сети. Функция сегментации трафика может использоваться с целью сокращения трафика внутри сетей VLAN 802.1Q, позволяя разбивать их на меньшие группы. При этом правила VLAN имеют более высокий приоритет при передаче трафика. Правила Traffic Segmentation применяются после них.

ЗАДАНИЕ

Используя функцию сегментации трафика, настроить порты 9-16 коммутатора 1, находящиеся в VLAN v3 таким образом, чтобы рабочие станции, подключённые к ним, не могли обмениваться данными между собой, но при этом могли передавать данные через магистральный канал.

Настройка коммутатора 1

Настройте сегментацию трафика:

```
config traffic_segmentation 9-16 forward_list 25
```

Проверьте выполненные настройки:

```
show traffic_segmentation
```

Подключите ПК1 к порту 9 коммутатора 1.

Проверьте доступность соединения между рабочими станциями командой ping:

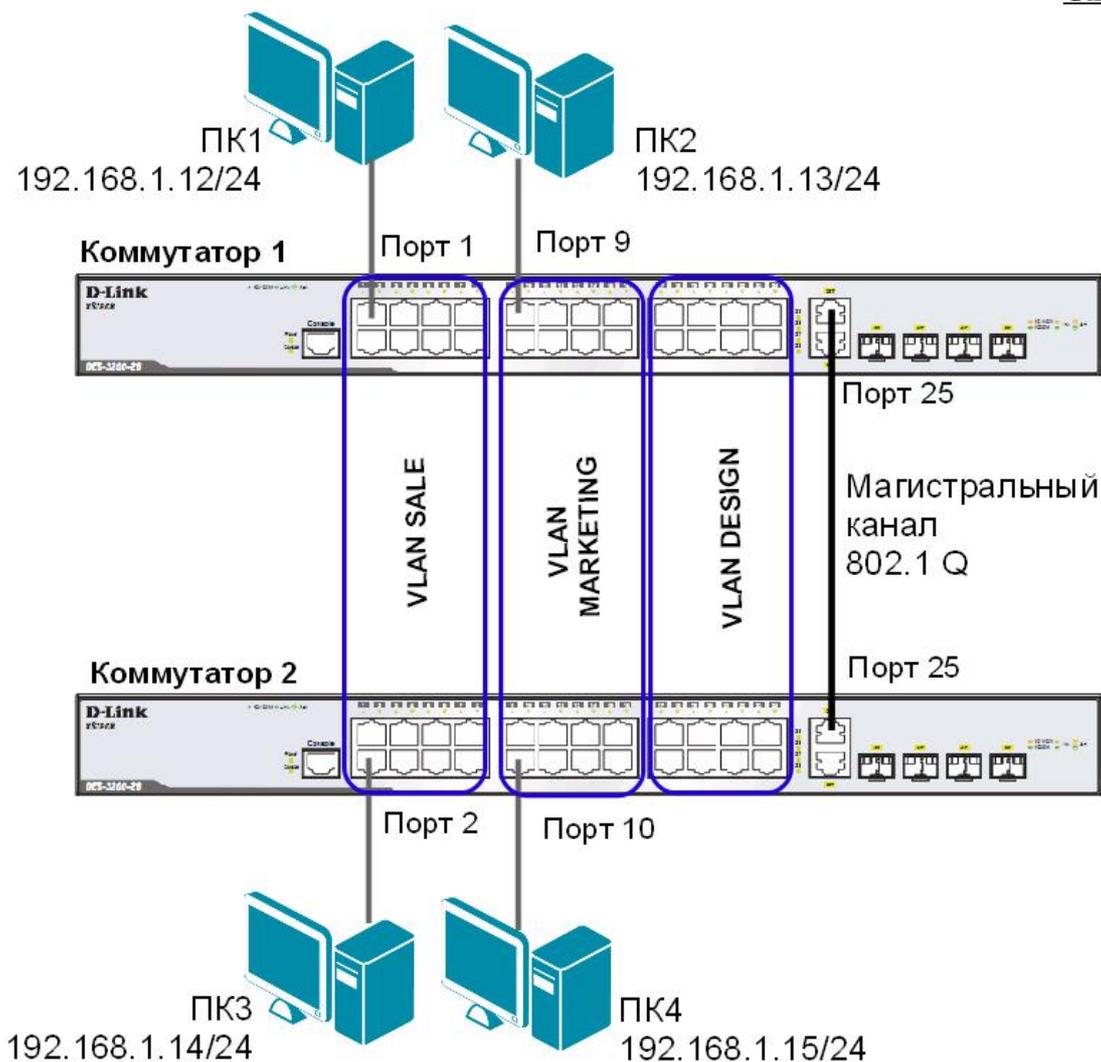
```
ping <IP-address>
```

- от ПК1 к ПК 2 _____
- от ПК1 к ПК4 _____

Что наблюдаете? Запишите.

4.3. Оптимизация настройки коммутаторов с большим количеством VLAN

Схема 4.2



Перед выполнением данной части лабораторной работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:
`reset config`

Настройка коммутатора 1

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
`config vlan default delete 1-24`

Создайте девять VLAN с тегами 2-10:
`create vlan vlanid 2-10`

Примечание: при создании VLAN без указания имени, имена присваиваются автоматически по шаблону (VLAN x, где x – тег создаваемой VLAN).

Измените имена в созданных VLAN и добавьте в них немаркированные порты:

```
config vlan vlanid 7 add untagged 1-8 name SALE
config vlan vlanid 8 add untagged 9-16 name MARKETING
config vlan vlanid 9 add untagged 17-24 name DESIGN
```

Добавьте маркированные порты сразу в несколько VLAN:

```
config vlan vlanid 2-10 add tagged 25-26
```

Проверьте настройки VLAN:

```
show vlan
```

Удалите порты из нескольких VLAN:

```
config vlan vlanid 2-10 delete 25-26
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте магистральный порт VLAN для передачи маркированных кадров с любыми VID:

```
config vlan_trunk ports 25 state enable
```

Активизируйте функционирование магистрального канала (выполнение коммутатором этой команды занимает некоторое время):

```
enable vlan_trunk
```

Проверьте выполненные настройки:

```
show vlan_trunk
```

Повторите процедуру настройки для коммутатора 2.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК 3 _____
- от ПК2 к ПК4 _____
- от ПК1 к ПК2 и ПК4 _____
- от ПК2 к ПК1 и ПК3 _____

Подключите ПК2 к порту 7 коммутатора 1, а ПК4 к порту 8 коммутатора 2.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК2 и ПК4 _____
- от ПК2 к ПК1 и ПК3 _____

Отключите магистральные каналы на обоих коммутаторах:

```
disable vlan_trunk
```

Лабораторная работа №5. Настройка протокола GVRP

Существуют два основных способа, позволяющих устанавливать членство в VLAN:

- статические VLAN;
- динамические VLAN.

В статических VLAN установление членства осуществляется вручную администратором сети. При изменении топологии сети или перемещении пользователя на другое рабочее место, администратору требуется вручную выполнять привязку порта к VLAN для каждого нового соединения.

Членство в динамических VLAN может устанавливаться динамически на основе протокола GVRP (GARP VLAN Registration Protocol). Протокол GVRP определяет способ, посредством которого коммутаторы обмениваются информацией о сети VLAN, чтобы автоматически зарегистрировать членов VLAN на портах во всей сети. Он позволяет динамически создавать и удалять VLAN стандарта IEEE 802.1Q на магистральных портах, автоматически регистрировать и исключать атрибуты VLAN (под регистрацией VLAN подразумевается включение порта в VLAN, под исключением – удаление порта из VLAN).

Протокол GVRP использует сообщения GVRP BPDU (GVRP Bridge Protocol Data Units), рассылаемые на многоадресный MAC-адрес 01-80-C2-00-00-21 для оповещения устройств-подписчиков о различных событиях.

Порт с поддержкой протокола GVRP подключается к сети VLAN только в том случае, если он непосредственно получает оповещение о ней. Если порт с поддержкой протокола GVRP передает оповещение, полученное от другого порта коммутатора, он не подключается к этой сети VLAN.

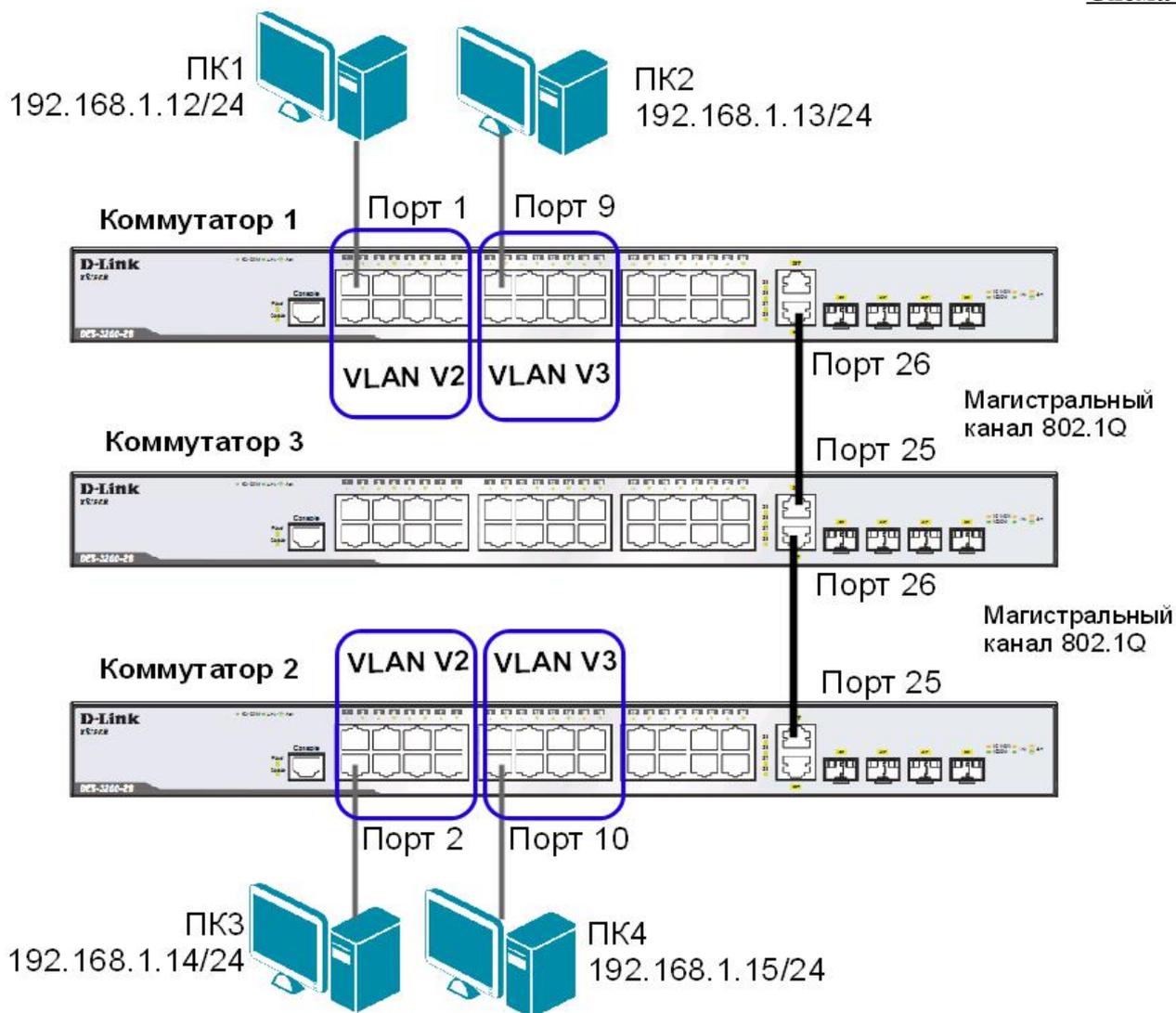
Главная цель протокола GVRP – позволить коммутаторам автоматически обнаруживать информацию о VLAN, которая иначе должна была бы быть вручную сконфигурирована на каждом коммутаторе. Наиболее рационально использовать протокол GVRP на магистральных коммутаторах для динамической передачи информации о статических VLAN на уровень доступа.

Примечание: при динамической передаче информации о VLAN через магистральные коммутаторы, рекомендуется передавать информацию только о пользовательских VLAN, а служебные VLAN и управляющие VLAN настраивать на магистральных коммутаторах статически.

Цель: изучить процесс динамического продвижения информации о VLAN в сети.

Оборудование (на 3 рабочих места):

Коммутатор DES-3200-28	3 шт.
Рабочая станция	4 шт.
Консольный кабель	3 шт.
Кабель Ethernet	6 шт.



Перед выполнением лабораторной работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:
`reset config`

Настройка коммутатора 1

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
`config vlan default delete 1-24`

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порты 25-26 маркированным:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-8
config vlan v2 add tagged 25-26
```

```
create vlan v3 tag 3
config vlan v3 add untagged 9-16
config vlan v3 add tagged 25-26
```

Проверьте настройки VLAN:

```
show vlan
```

Настройте объявление о VLAN v2 и v3:

```
config vlan v2 advertisement enable  
config vlan v3 advertisement enable
```

Включите работу протокола GVRP:

```
enable gvrp
```

Установите возможность приёма и отправки информации о VLAN через порты 25-26 коммутатора:

```
config port_vlan 25-26 gvrp_state enable
```

Повторите процедуру настройки для коммутатора 2.

Настройка коммутатора 3

Включите работу протокола GVRP:

```
enable gvrp
```

Установите возможность приема и отправки информации о VLAN через все порты коммутатора:

```
config port_vlan all gvrp_state enable
```

Проверьте настройки VLAN на коммутаторе 3:

```
show vlan
```

Проверьте состояние GVRP на портах коммутаторов 1, 2, 3:

```
show port_vlan
```

Запишите ваши наблюдения:

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК 3

- от ПК2 к ПК4

Лабораторная работа №6. Настройка сегментации трафика без использования VLAN

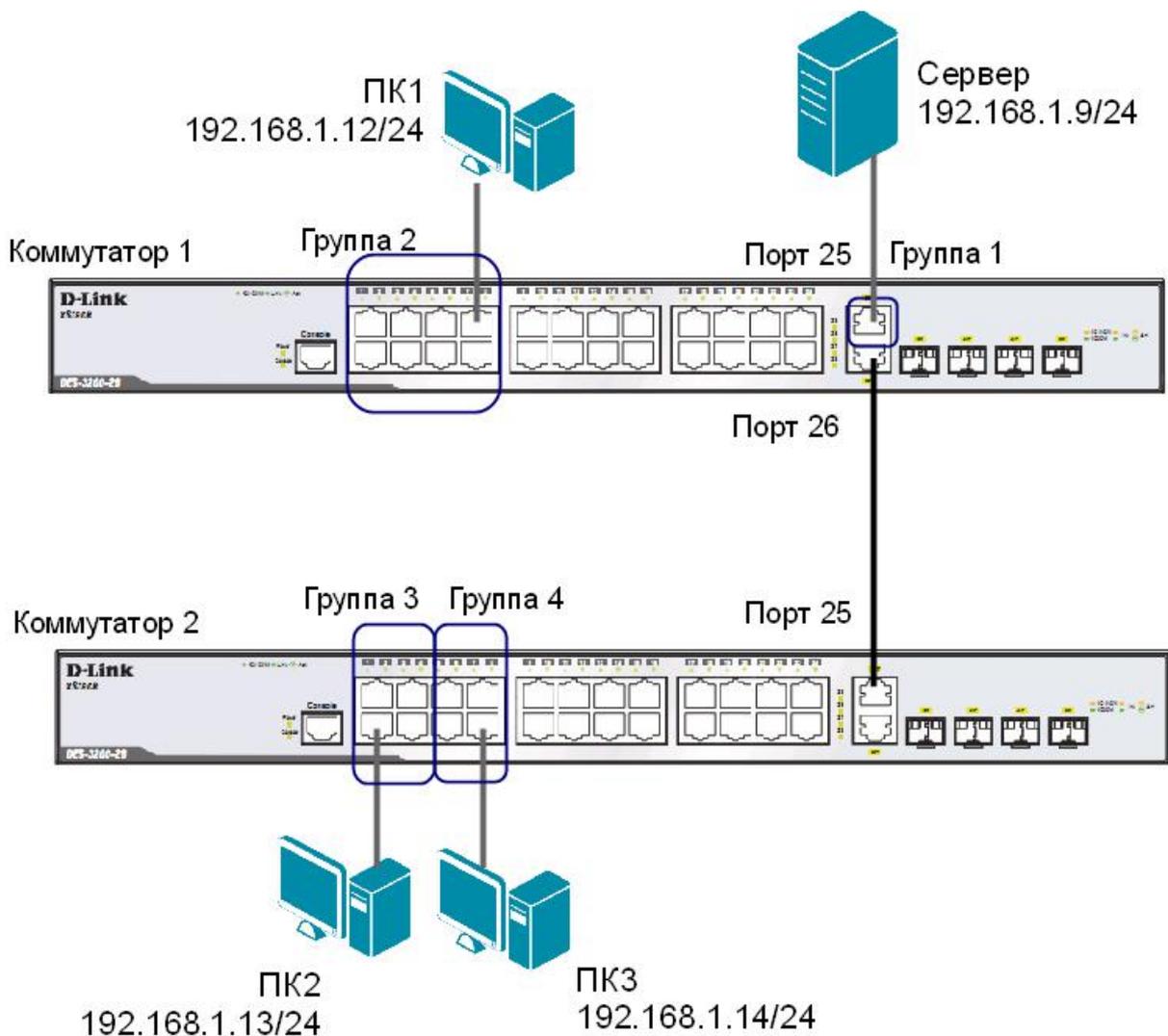
Функция Traffic Segmentation (сегментация трафика) служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов или магистрали сети.

Цель: научиться выполнять сегментацию трафика на канальном уровне без использования технологии VLAN.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

Схема 6



ЗАДАНИЕ

Используя функцию сегментации трафика, настройте коммутаторы таким образом, чтобы рабочие станции из разных групп получили доступ к совместно используемому серверу. При этом обмен данными между устройствами разных групп запрещён.

Сбросьте настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройте сегментацию трафика на коммутаторе 1:

```
config traffic_segmentation 1-8 forward_list 1-8,25
config traffic_segmentation 26 forward_list 25
config traffic_segmentation 25 forward_list 1-26
```

Настройте сегментацию трафика на коммутаторе 2:

```
config traffic_segmentation 1-4 forward_list 1-4,25
config traffic_segmentation 5-8 forward_list 5-8,25
config traffic_segmentation 25 forward_list 1-26
```

Проверьте настройки на обоих коммутаторах:

```
show traffic_segmentation
```

Проверьте доступность соединения между устройствами командой ping:

```
ping <IP-address>
```

- от ПК1 (Группа 2) к серверу (Группа 1)
- от ПК2 (Группа 3) к серверу (Группа 1)
- от ПК3 (Группа 4) к серверу (Группа 1)
- от ПК1 (Группа 2) к ПК2 (Группа 3)
- от ПК2 (Группа 3) к ПК3 (Группа 4)
- от ПК3 (Группа 4) к ПК1 (Группа 2)

Лабораторная работа №7. Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q

Цель: самостоятельно создать и настроить сеть на основе стандарта IEEE 802.1Q.

Оборудование (на 10 рабочих мест):

Коммутатор DES-3200-28	8 шт.
Коммутатор DES-3810-28	2 шт.
Рабочая станция	10 шт.
Консольный кабель	10 шт.
Кабель Ethernet	20 шт.

Перед выполнением данной лабораторной работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

ЗАДАНИЕ 1

Подключите устройства как показано на общей схеме сети 7. Задайте на всех ПК IP-адреса из подсети 192.168.1.0/24, в соответствии со схемой.

Проверьте соединение между рабочими станциями командой ping.

```
ping <IP-address>
```

В какой VLAN находятся ПК? Должна ли быть связь между всеми ПК и почему?

Проверьте на каждом коммутаторе состояние таблицы коммутации:

```
show fdb
```

Проверьте таблицу ARP каждого компьютера:

```
arp -a
```

Сколько записей вы наблюдаете в этих таблицах? Есть ли в них одинаковые MAC-адреса?

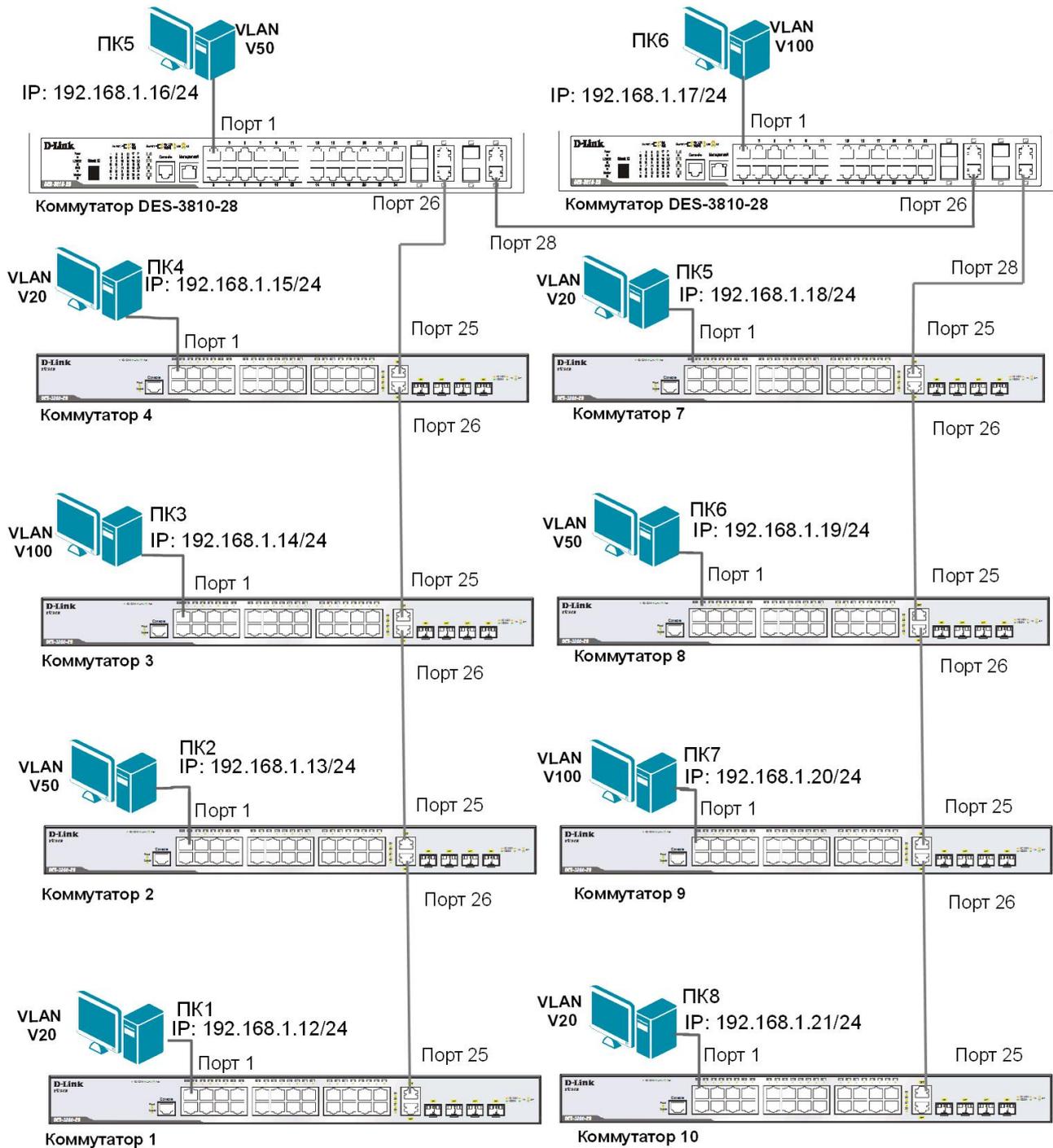
Если соединение до каких-либо ПК недоступно, необходимо выяснить причины и устранить их. Перейти к заданию 2 можно только после выявления и устранения причин отсутствия связи между ПК.

ЗАДАНИЕ 2

Создайте на каждом коммутаторе необходимые для работы сети VLAN.

Какие VLAN необходимо создать на каждом коммутаторе?

Схема 7 (общая схема сети)



Настройте магистральные порты коммутаторов как маркированные, а пользовательские порты как немаркированные, в соответствии со схемой 7.

Проверьте связь между всеми ПК командой ping.

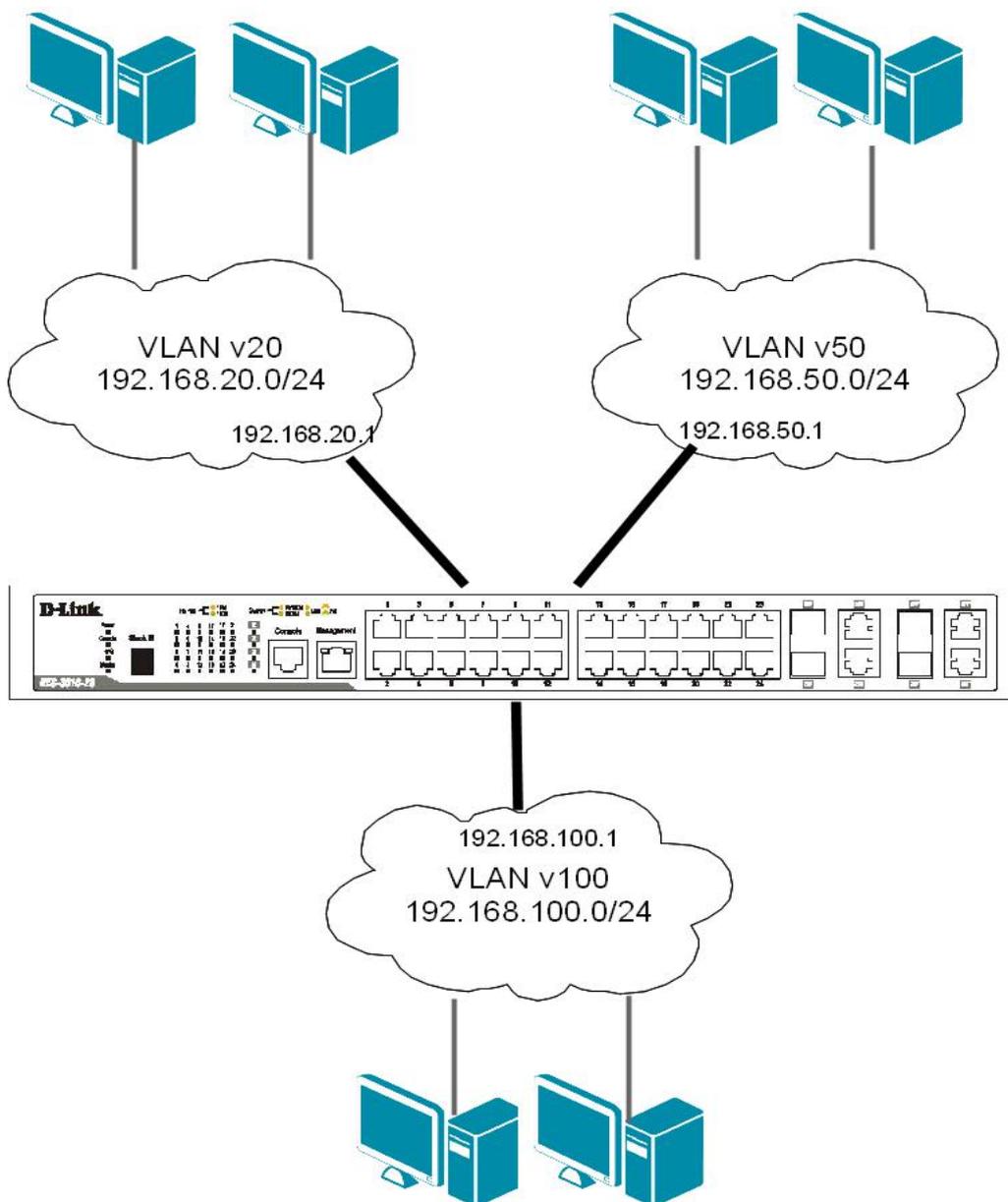
Какие ПК доступны с вашего рабочего места, а какие нет? Почему?

ЗАДАНИЕ 3

На коммутаторе DES-3810-28 (только на одном!) необходимо настроить маршрутизацию для объединения разных VLAN в общую сеть. Логическая схема сети с маршрутизацией показана на схеме 7.1.

Примечание: в пределах одного коммутатора 3-го уровня маршрутизация между VLAN включается автоматически при настройке IP-интерфейсов.

Схема 7.1



Перед настройкой маршрутизации на коммутаторе DES-3810-28 уже должны быть созданы необходимые VLAN v20, v50, v100.

Введите на коммутаторе DES-3810-28 следующие команды, чтобы создать IP-интерфейс для каждой VLAN:

```
create ipif IPIF20 192.168.20.1/24 v20 state enable
create ipif IPIF50 192.168.50.1/24 v50 state enable
create ipif IPIF100 192.168.100.1/24 v100 state enable
```

Примечание: в этом примере IPIF20, IPIF50, IPIF100 – имена создаваемых IP-интерфейсов, а v20, v50, v100 – имена ранее созданных на этом коммутаторе VLAN (если имена VLAN другие, необходимо отредактировать вводимые команды).

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif  
show iproute
```

Задайте на всех ПК, принадлежащих к одной VLAN, IP-адреса из той IP-сети, которая назначена данной VLAN (значения IP-адресов рабочих станций выберите самостоятельно). В качестве шлюза по умолчанию (default gateway) укажите адрес IP-интерфейса маршрутизирующего коммутатора соответствующей VLAN. Командой ping проверьте связь между всеми ПК.

В какой VLAN находятся ПК? Должна ли быть связь между всеми ПК и почему?

Проверьте на каждом коммутаторе состояние таблицы коммутации:

```
show fdb
```

Проверьте таблицу ARP каждого компьютера:

```
arp -a
```

Сколько записей вы наблюдаете в этих таблицах? Одинаковое ли количество записей в этих таблицах? Есть ли одинаковые MAC-адреса в них? Сравните с полученными результатами в задании 1.

Лабораторная работа №8. Настройка протоколов связующего дерева STP, RSTP, MSTP

Протокол Spanning Tree Protocol (STP).

Протокол связующего дерева Spanning Tree Protocol (STP) является протоколом 2 уровня модели OSI, который позволяет строить древовидные, свободные от петель, конфигурации связей между коммутаторами локальной сети. Конфигурация связующего дерева строится коммутаторами автоматически с использованием обмена служебными пакетами, называемыми Bridge Protocol Data Units (BPDU).

Для построения устойчивой активной топологии с помощью протокола STP необходимо с каждым коммутатором сети ассоциировать уникальный идентификатор моста (Bridge ID), с каждым портом коммутатора ассоциировать стоимость пути (Path Cost) и идентификатор порта (Port ID).

Процесс вычисления связующего дерева начинается с выбора корневого моста (Root Bridge), от которого будет строиться дерево. Вторым этапом работы STP – выбор корневых портов (Root Port). Третьим шагом работы STP – определение назначенных портов (Designated Port).

В процессе построения топологии сети каждый порт коммутатора проходит несколько стадий: Blocking (Блокировка), Listening (Прослушивание), Learning (Обучение), Forwarding (Продвижение), Disable (Отключен).

Протокол Rapid Spanning Tree Protocol (RSTP).

Протокол Rapid Spanning Tree Protocol (RSTP) является развитием протокола STP. Основные понятия и терминология протоколов STP и RSTP одинаковы. Существенным их отличием является способ перехода портов в состояние продвижения и то, каким образом этот переход влияет на роль порта в топологии. RSTP объединяет состояния Disabled, Blocking и Listening, используемые в STP, и создает единственное состояние Discarding («Отбрасывание»), при котором порт не активен. Выбор активной топологии завершается присвоением протоколом RSTP определённой роли каждому порту: корневой порт (Root Port), назначенный порт (Designated Port), альтернативный порт (Alternate Port), резервный порт (Backup Port).

Протокол RSTP предоставляет механизм предложений и соглашений, который обеспечивает быстрый переход корневых и назначенных портов в состояние Forwarding, а альтернативных и резервных портов в состояние Discarding. Для этого протокол RSTP вводит два новых понятия: граничный порт и тип соединения. *Граничным портом* (Edge Port) объявляется порт, непосредственно подключённый к сегменту сети, в котором не могут быть созданы петли. Граничный порт мгновенно переходит в состояние продвижения, минуя состояния прослушивания и обучения. Назначенный порт может выполнять быстрый переход в состояние продвижения в соединениях типа «точка — точка» (*Point-to-Point, P2P*), т.е. если он подключён только к одному коммутатору.

Администратор сети может вручную включать или выключать статусы Edge и P2P либо устанавливать их работу в автоматическом режиме, выполнив соответствующие настройки порта коммутатора.

Таблица 2

Стоимость пути в соответствии с протоколом RSTP

Скорость канала	Рекомендованное значение
<=100 Кбит/с	200 000 000
1 Мбит/с	20 000 000
10 Мбит/с	2 000 000
100 Мбит/с	200 000
1 Гбит/с	20 000
10 Гбит/с	2 000

* Коммутаторы, поддерживающие только стандарт STP должны использовать значения в соответствии со стандартом IEEE 802.1D-1998.

Протокол Multiple Spanning Tree Protocol (MSTP).

Протокол Multiple Spanning Tree Protocol (MSTP) является расширением протокола RSTP, который позволяет настраивать отдельное связующее дерево для любой VLAN или группы VLAN, создавая множество маршрутов передачи трафика и позволяя осуществлять балансировку нагрузки.

Протокол MSTP делит коммутируемую сеть на **регионы MST** (*Multiple Spanning Tree (MST) Region*), каждый из которых может содержать множество **копий связующих деревьев** (*Multiple Spanning Tree Instance, MSTI*) с независимой друг от друга топологией.

Для того чтобы два и более коммутатора принадлежали одному региону MST, они должны обладать одинаковой конфигурацией MST, которая включает: номер ревизии MSTP (*MSTP revision level number*), имя региона (*Region name*), карту привязки VLAN к копии связующего дерева (*VLAN-to-instance mapping*).

Внутри коммутируемой сети может быть создано множество MST-регионов.

Протокол MSTP определяет следующие типы связующих деревьев:

- **Internal Spanning Tree (IST)** — специальная копия связующего дерева, которая по умолчанию существует в каждом MST-регионе. IST присвоен номер 0 (Instance 0). Она может отправлять и получать кадры BPDU и служит для управления топологией внутри региона. Все VLAN, настроенные на коммутаторах данного MST-региона, по умолчанию привязаны к IST;

- **Common Spanning Tree (CST)** — единое связующее дерево, вычисленное с использованием протоколов STP, RSTP, MSTP и объединяющее все регионы MST и мосты SST;

- **Common and Internal Spanning Tree (CIST)** — единое связующее дерево, объединяющее CST и IST каждого MST-региона;

- **Single Spanning Tree (SST) Bridge** — это мост, поддерживающий только единственное связующее дерево, CST. Это единственное связующее дерево может поддерживать протокол STP или протокол RSTP.

Вычисления в MSTP

Процесс вычисления MSTP начинается с выбора **корневого моста CIST** (*CIST Root*) сети. В качестве CIST Root будет выбран коммутатор, обладающий наименьшим значением идентификатора моста среди всех коммутаторов сети.

Далее в каждом регионе выбирается **региональный корневой мост CIST** (*CIST Region Root*). Им становится коммутатор, обладающий наименьшей внешней стоимостью пути к корню CIST среди всех коммутаторов, принадлежащих данному региону.

При наличии в регионе отдельных связующих деревьев MSTI для каждой MSTI, независимо от остальных, выбирается **региональный корневой мост MSTI** (*MSTI Regional Root*). Им становится коммутатор, обладающий наименьшим значением идентификатора моста среди всех коммутаторов данной MSTI этого MST-региона.

При вычислении активной топологии CIST и MSTI используется тот же фундаментальный алгоритм, который описан в стандарте IEEE 802.1D-2004.

Роли портов

Протокол MSTP определяет роли портов, которые участвуют в процессе вычисления активной топологии CIST и MSTI аналогичные протоколам STP и RSTP. Дополнительно в MSTI используется ещё роль — мастер-порт (*Master Port*).

Счётчик переходов MSTP

При вычислении активной топологии связующего дерева IST и MSTI используется механизм счётчика переходов (Hop count), определяющий максимальное число переходов между устройствами внутри региона, прежде чем кадр BPDU будет отброшен. Значение счётчика переходов устанавливается региональным корневым мостом MSTI или CIST и уменьшается на 1 каждым портом коммутатора, получившим кадр BPDU. После того как значение счётчика станет равным 0, кадр BPDU будет отброшен и информация, хранящаяся портом, будет помечена как устаревшая.

Пользователь может установить значение счётчика переходов от 1 до 20. Значение по умолчанию — 20.

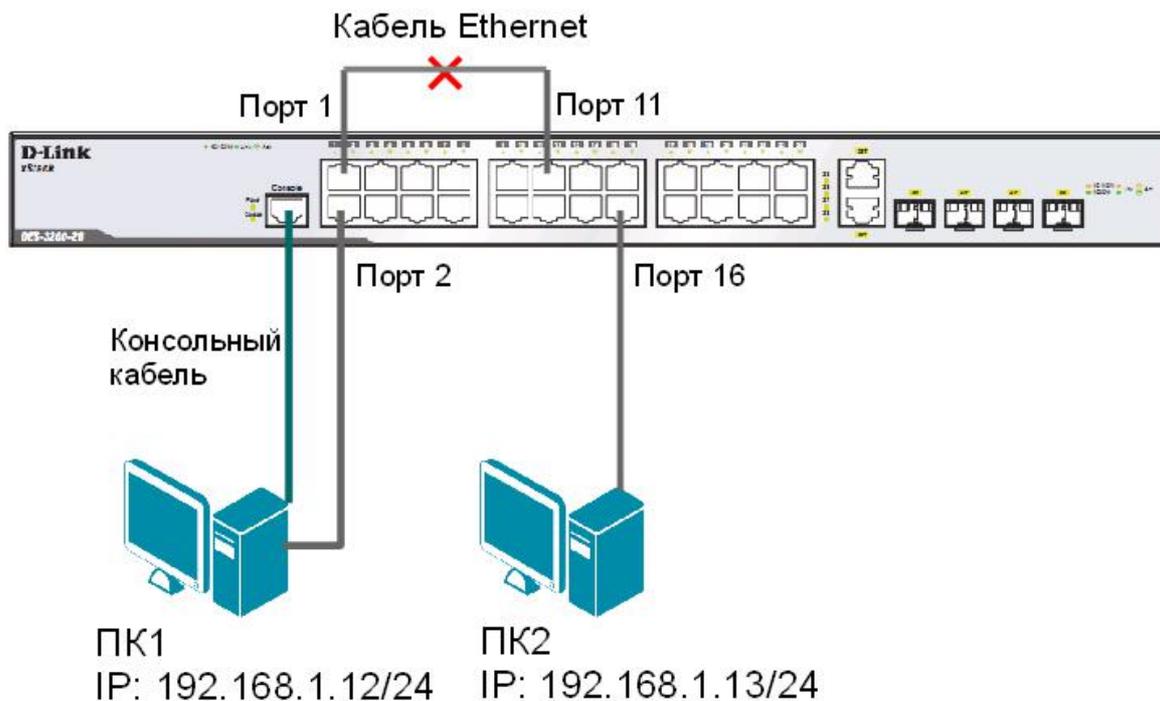
Цель: понять функционирование протоколов связующего дерева и изучить их настройку на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	8 шт.

8.1. Мониторинг и диагностика сети во время широковещательного шторма, вызванного наличием петли

Схема 8.1



Перед выполнением практического задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Просмотрите статистику о пакетах, передаваемых через порт 1:

```
show packet ports 1
```

Соберите схему и соедините кабелем Ethernet порты 1 и 11 коммутатора.

Выполните на рабочей станции ПК2 команду ping, и не останавливайте её до окончания выполнения задания 8.1:

```
ping 192.168.1.1 -t
```

Повторно просмотрите статистику о пакетах, передаваемых через порт 1:

```
show packet ports 1
```

Что вы наблюдаете? Возник широковещательный шторм? Почему?

Что происходит при работе ping с не используемым в схеме IP-адресом?

Посмотрите загрузку ЦПУ коммутатора (CPU):

```
show utilization cpu
```

Просмотрите загрузку портов коммутатора:

```
show utilization ports
```

Какая загрузка портов, используемых в схеме?

Порт 1 (%) _____

Порт 2 (%) _____

Порт 11 (%) _____

Порт 16 (%) _____

Просмотрите загрузку ЦПУ на ПК1 и ПК2.

Выполните на рабочей станции ПК 1 команду:

```
ping 192.168.1.13
```

Что вы наблюдаете? Объясните почему.

Отсоединив кабель от портов 1 и 11, удалите петлю.

Поместите порты 2 и 16 в новую VLAN:

```
config vlan default delete 2,16
```

```
create vlan v2 tag 2
```

```
config vlan v2 add untagged 2,16
```

Проверьте настройки VLAN:

```
show vlan
```

Просмотрите статистику о пакетах, передаваемых через порт 1:

```
show packet ports 1
```

Соедините кабелем порты 1 и 11 для повторного создания петли.

Просмотрите загрузку портов:

```
show utilization ports
```

Просмотрите загрузку ЦПУ на ПК1 и ПК2.

Что вы наблюдаете? Почему нет широковещательного шторма на портах 2 и 16?

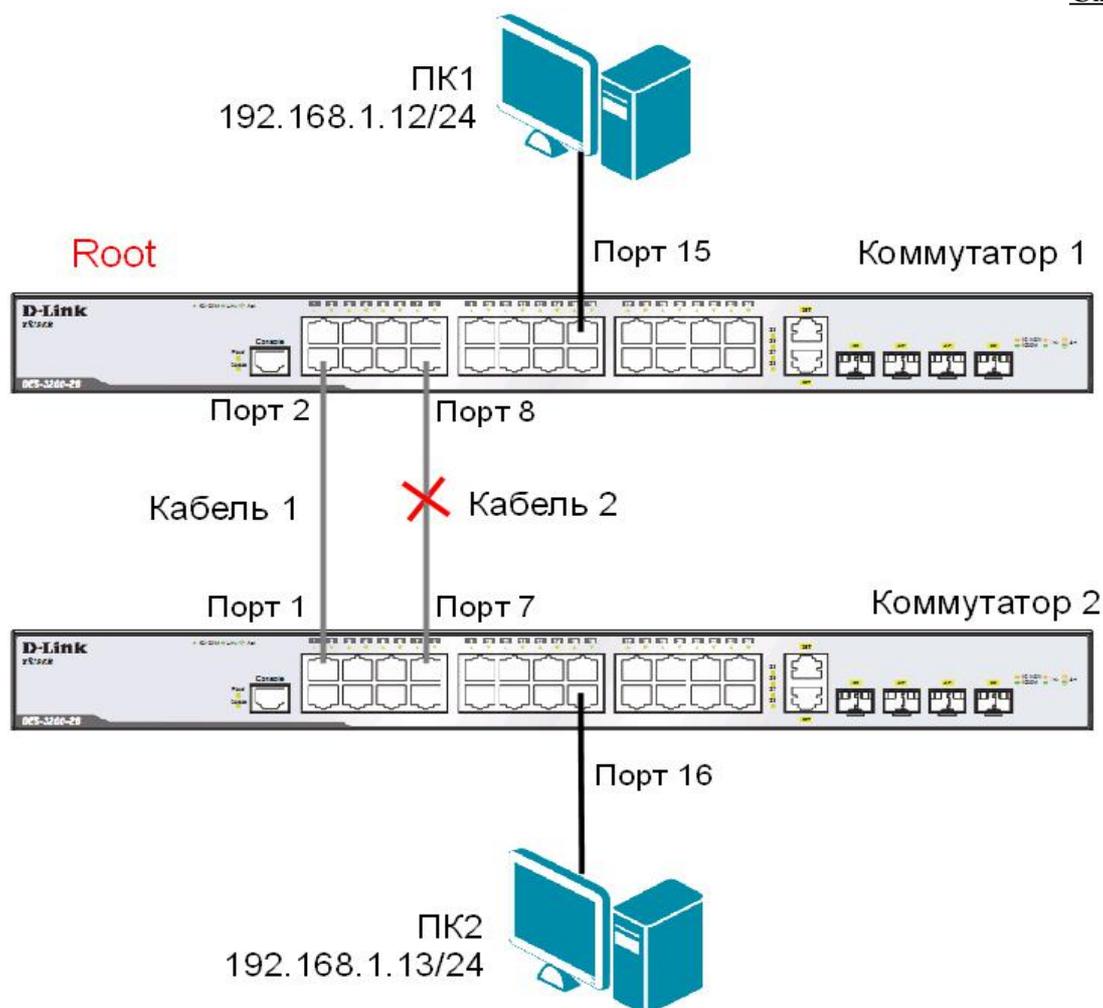
Выполните на рабочей станции ПК 1 команду:

```
ping 192.168.1.13
```

Что вы наблюдаете? Объясните почему.

8.2. Настройка протокола RSTP

Схема 8.2



Примечание: не соединяйте коммутаторы одновременно двумя кабелями во время настройки до особого указания.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1

Включите протокол связующего дерева на коммутаторе:

```
enable stp
```

Проверьте текущую конфигурацию протокола связующего дерева:

```
show stp
```

Протокол RSTP используется по умолчанию.

Если нет, активизируйте его:

```
config stp version rstp
```

Установите на коммутаторе меньшее значение приоритета, чтобы он был выбран корневым мостом:

```
config stp priority 8192 instance_id 0
```

Просмотрите выполненные изменения:

```
show stp instance 0
```

Назначьте порты 1-24 граничными портами:

```
config stp ports 1-24 edge true
```

Активизируйте протокол связующего дерева на портах:

```
config stp ports 1-24 state enable
```

Настройка коммутатора 2

Активизируйте функцию связующего дерева:

```
enable stp
```

Проверьте текущую конфигурацию протокола связующего дерева:

```
show stp
```

Протокол RSTP используется по умолчанию.

Если нет, включите его:

```
config stp version rstp
```

Назначьте порты 1-24 граничными портами:

```
config stp ports 1-24 edge true
```

Активизируйте протокол связующего дерева на портах:

```
config stp ports 1-24 state enable
```

Соедините между собой коммутаторы 1 и 2 с помощью двух кабелей, как показано на схеме 8.2.

Проверьте настройки RSTP, состояние портов и их роли у обоих коммутаторов:

```
show stp ports x, где x- номер порта
```

Какой коммутатор является корневым? _____

Какие порты являются заблокированными? _____

Какая роль у заблокированных портов? _____

Выполните от компьютера ПК1 до ПК2, и наоборот, команду ping, и не останавливайте её до окончания выполнения задания 8.2:

```
На ПК1: ping 192.168.1.13 -t
```

```
На ПК2: ping 192.168.1.12 -t
```

Отсоедините кабель от корневого порта.

Что происходит с тестом ping? _____

Превышен ли интервал ожидания для запроса? _____

Как долго пришлось ждать до появления ответа? _____

Проверьте состояние заблокированного порта, какая теперь у него роль?

Подключите обратно кабель.

Поменяйте версию протокола связующего дерева с RSTP на STP на обоих коммутаторах командой:

```
config stp version stp
```

Отсоедините кабель от корневого порта.

Что происходит с тестом ping? _____

Превышен ли интервал ожидания для запроса? _____

Как долго пришлось ждать до появления ответа? _____

8.3. Настройка защиты от несанкционированного подключения корневых коммутаторов

ЗАДАНИЕ

Настройте на коммутаторе 1 защиту от несанкционированного подключения корневых коммутаторов.

Отключите кабели, соединяющие коммутаторы.

Настройка коммутатора 1

Включите на портах 1-8 защиту от перевыборов корневого коммутатора, активизировав параметр `restricted_role`:

```
config stp ports 1-8 restricted_role true
```

Настройка коммутатора 2

Измените значение приоритета коммутатора 2, так чтобы оно стало ниже значения приоритета коммутатора 1:

```
config stp priority 4096 instance_id 0
```

Соедините порты обоих коммутаторов кабелем 1, как показано на схеме 8.2.

На коммутаторе 1 посмотрите log-файл.

```
show log
```

Что вы наблюдаете? Запишите.

Какой коммутатор является корневым? _____

Какая роль у порта 2 коммутатора 1? _____

На коммутаторе 1 переключите кабель из порта 2 в порт 9.

На коммутаторе 1 посмотрите log-файл.

```
show log
```

Что вы наблюдаете? Запишите.

Какой коммутатор является корневым? _____

Какая роль у порта 9 коммутатора 1? _____

8.4. Настройка защиты от получения ложных кадров об изменении топологии

ЗАДАНИЕ

Настройте на коммутаторе 1 защиту от получения ложных кадров об изменении топологии (TCN BPDU).

Отключите кабели, соединяющие коммутаторы.

Настройка коммутатора 1

Включите на портах 1-8 коммутатора функцию защиты от получения ложных TCN BPDU:

```
config stp ports 1-8 restricted_tcn true
```

Настройка коммутатора 2

Настройте на коммутаторе приоритет по умолчанию:

```
config stp priority 32768 instance_id 0
```

Проверьте выполненные настройки:

```
show stp instance 0
```

Соедините между собой коммутаторы 1 и 2 с помощью двух кабелей, как показано на схеме 8.2.

Соедините порт 10 и порт 12 коммутатора кабелем Ethernet.

На коммутаторе 1 посмотрите log-файл.

```
show log
```

Что вы наблюдаете? Запишите.

На коммутаторе 2 посмотрите log-файл.

```
show log
```

Что вы наблюдаете? Запишите.

Отключите на коммутаторе 1 функцию защиты от получения ложных TCN BPDU:

```
config stp ports 1-8 restricted_tcn false
```

Отключите кабель, соединяющий порты 10 и 12 коммутатора 2.

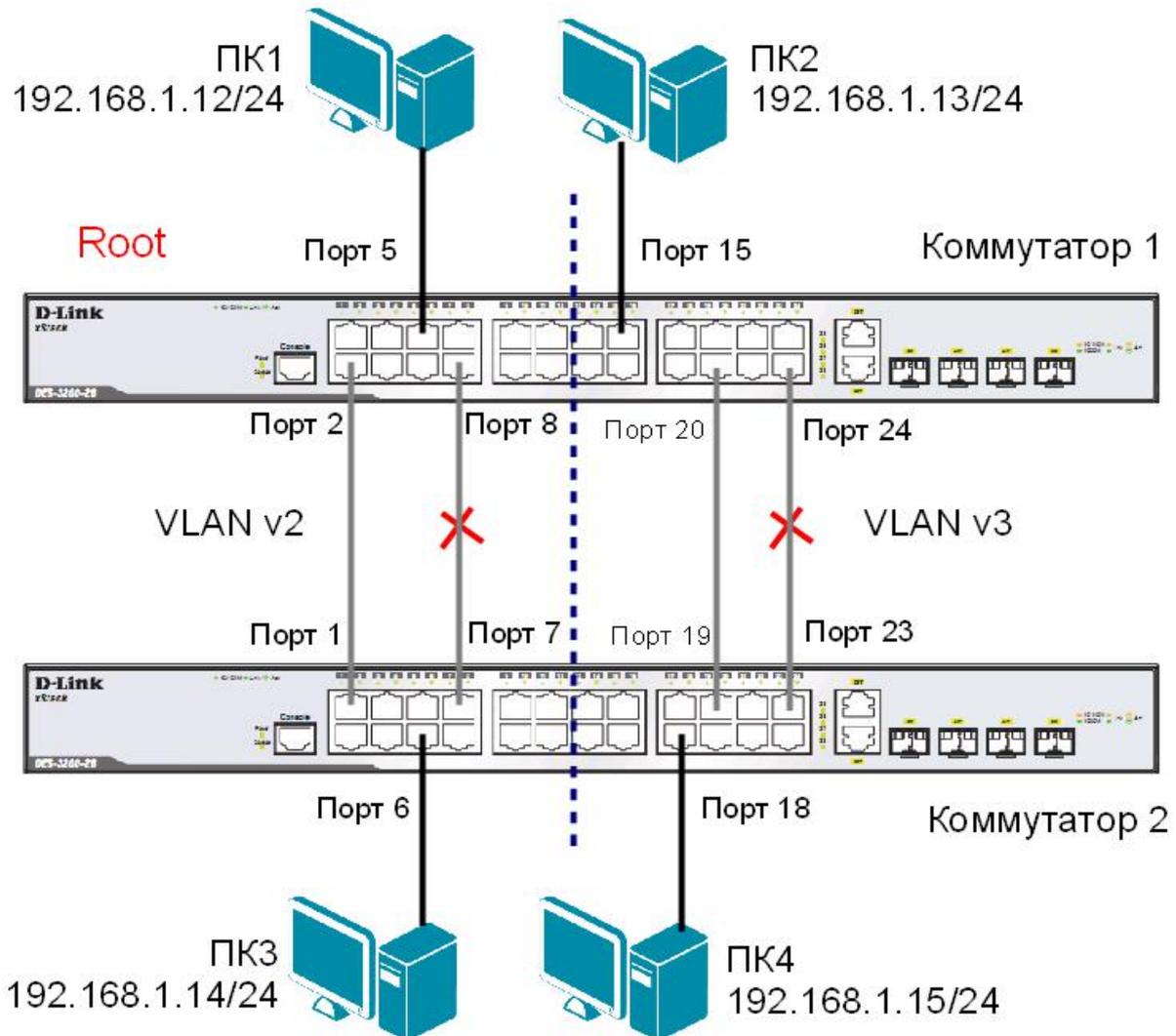
На коммутаторе 1 посмотрите log-файл.

```
show log
```

Что вы наблюдаете? Запишите.

8.5. Настройка протокола MSTP

Схема 8.3



Примечание: не соединяйте коммутаторы одновременно несколькими кабелями во время настройки до особого указания.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:
reset config

Настройка коммутатора 1

Удалите порты из VLAN по умолчанию для их использования в других VLAN:
config vlan default delete 1-24

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-24
```

Проверьте настройки VLAN:

```
show vlan
```

Включите протокол связующего дерева на коммутаторе:

```
enable stp
```

Проверьте текущую конфигурацию протокола связующего дерева на портах коммутатора:

```
show stp ports
```

Измените версию протокола связующего дерева на MSTP (по умолчанию используется RSTP):

```
config stp version mstp
```

Настройте имя MST-региона и ревизию:

```
config stp mst_config_id name abc  
config stp mst_config_id revision_level 1
```

Создайте MSTI и карту привязки VLAN к MSTI:

```
create stp instance_id 2  
config stp instance_id 2 add_vlan 2  
create stp instance_id 3  
config stp instance_id 3 add_vlan 3
```

Настройте приоритет STP так, чтобы коммутатор был выбран корневым мостом в MSTI 2:

```
config stp priority 4096 instance_id 2  
config stp priority 32768 instance_id 3
```

Настройте порты как граничные:

```
config stp ports 1-24 edge true
```

Активизируйте протокол связующего дерева на портах:

```
config stp ports 1-24 state enable
```

Настройка коммутатора 2

Удалите порты из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2  
config vlan v2 add untagged 1-12  
create vlan v3 tag 3  
config vlan v3 add untagged 13-24
```

Проверьте настройки VLAN:

```
show vlan
```

Включите протокол связующего дерева на коммутаторе:

```
enable stp
```

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК 3 _____
- от ПК2 к ПК4 _____

Что вы наблюдаете? Запишите.

Измените версию протокола связующего дерева на MSTP (по умолчанию используется RSTP):

```
config stp version mstp
```

Настройте имя MST-региона и ревизию:

```
config stp mst_config_id name abc
config stp mst_config_id revision_level 1
```

Создайте MSTI и карту привязки VLAN к MSTI:

```
create stp instance_id 2
config stp instance_id 2 add_vlan 2
create stp instance_id 3
config stp instance_id 3 add_vlan 3
```

Настройте приоритет STP так, чтобы коммутатор был выбран корневым мостом в MSTI 3:

```
config stp priority 32768 instance_id 2
config stp priority 4096 instance_id 3
```

Настройте порты как граничные:

```
config stp ports 1-24 edge true
```

Активизируйте протокол связующего дерева на портах:

```
config stp ports 1-24 state enable
```

Подключите коммутаторы как показано на схеме 8.3.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК 3 _____
- от ПК1 к ПК 2 _____
- от ПК1 к ПК 4 _____
- от ПК3 к ПК4 _____
- от ПК2 к ПК4 _____

Проверьте текущую конфигурацию протокола связующего дерева на портах коммутатора:

```
show stp ports
```

Какие порты являются корневым и альтернативным для VLAN v2? _____

Какие порты являются корневым и альтернативным для VLAN v3? _____

Какие порты являются назначенными для VLAN v2? _____

Какие порты являются назначенными для VLAN v3? _____

Лабораторная работа №9. Настройка функции защиты от образования петель LoopBack Detection

Функция LoopBack Detection (LBD) обеспечивает дополнительную защиту от образования петель на уровне 2 модели OSI. Существует две реализации этой функции:

- STP LoopBack Detection;
- LoopBack Detection Independent STP.

Коммутатор, на котором настроена функция STP LoopBack Detection, определяет наличие петли, когда отправленный им кадр BPDU вернулся назад на другой его порт. В этом случае порт-источник кадра BPDU и порт-приемник будут автоматически заблокированы, и администратору сети будет отправлен служебный пакет-уведомление. Порты будут находиться в заблокированном состоянии до истечения таймера LBD Recover Timer.

Функция LoopBack Detection Independent STP не требует настройки протокола STP на портах, на которых необходимо определять наличие петли. В этом случае наличие петли обнаруживается путем отправки портом специального служебного кадра ECTP (Ethernet Configuration Testing Protocol). При получении кадра ECTP этим же портом, он блокируется на указанное в таймере время. Существуют два режима работы этой функции: Port-Based и VLAN-Based (начиная с LBD версии v.4.00).

В режиме Port-Based при обнаружении петли происходит автоматическая блокировка порта, и никакой трафик через него не передается.

В режиме VLAN-Based порт будет заблокирован для передачи трафика только той VLAN, в которой обнаружена петля. Остальной трафик через этот порт будет передаваться.

Цель: понять принципы работы функции LoopBack Detection Independent STP в режимах Port-Based и VLAN-Based.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	2 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.
Неуправляемый коммутатор	1 шт.

9.1. Настройка функции LoopBack Detection Independent STP в режиме Port-Based

В данном задании рассматривается блокирование порта управляемого коммутатора при обнаружении петли в подключённом сегменте.

Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:
`reset config`

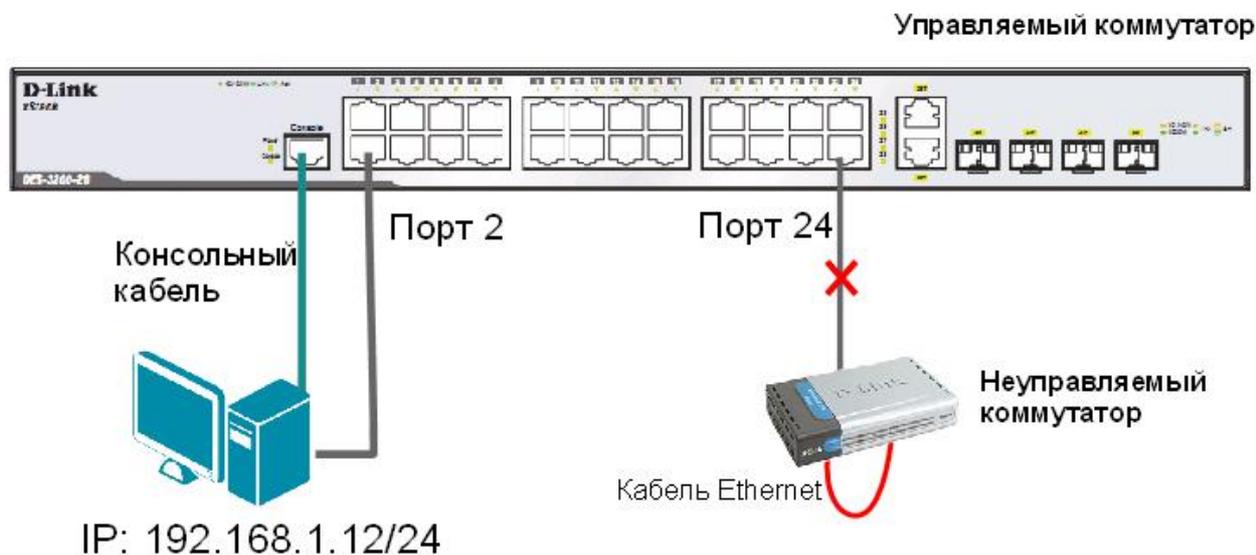
Включите функцию LBD глобально на коммутаторе:
`enable loopdetect`

Активизируйте функцию LBD на всех портах коммутатора:
`config loopdetect ports 1-24 state enabled`

Сконфигурируйте режим Port-Based, чтобы при обнаружении петли отключался порт:
`config loopdetect mode port-based`

Внимание: При отключении порта трафик передаваться не будет ни из одной VLAN. Порт будет заблокирован.

Схема 9.1



Проверьте текущую конфигурацию функции LBD:
`show loopdetect`

Подключите неуправляемый коммутатор с петлей к управляемому коммутатору, как показано на схеме 9.1.

Посмотрите, обнаружена ли петля на управляемом коммутаторе:
`show loopdetect ports`

Что вы наблюдаете? Запишите.

Проверьте log-файл:
`show log`

Что вы наблюдаете? Запишите.

Проверьте загрузку портов:
`show utilization ports`

Отключите неуправляемый коммутатор с петлей от управляемого коммутатора.

Отключите функцию LBD глобально на коммутаторе:
`disable loopdetect`

Проверьте загрузку портов:
show utilization ports

Подключите неуправляемый коммутатор с петлей к управляемому коммутатору.

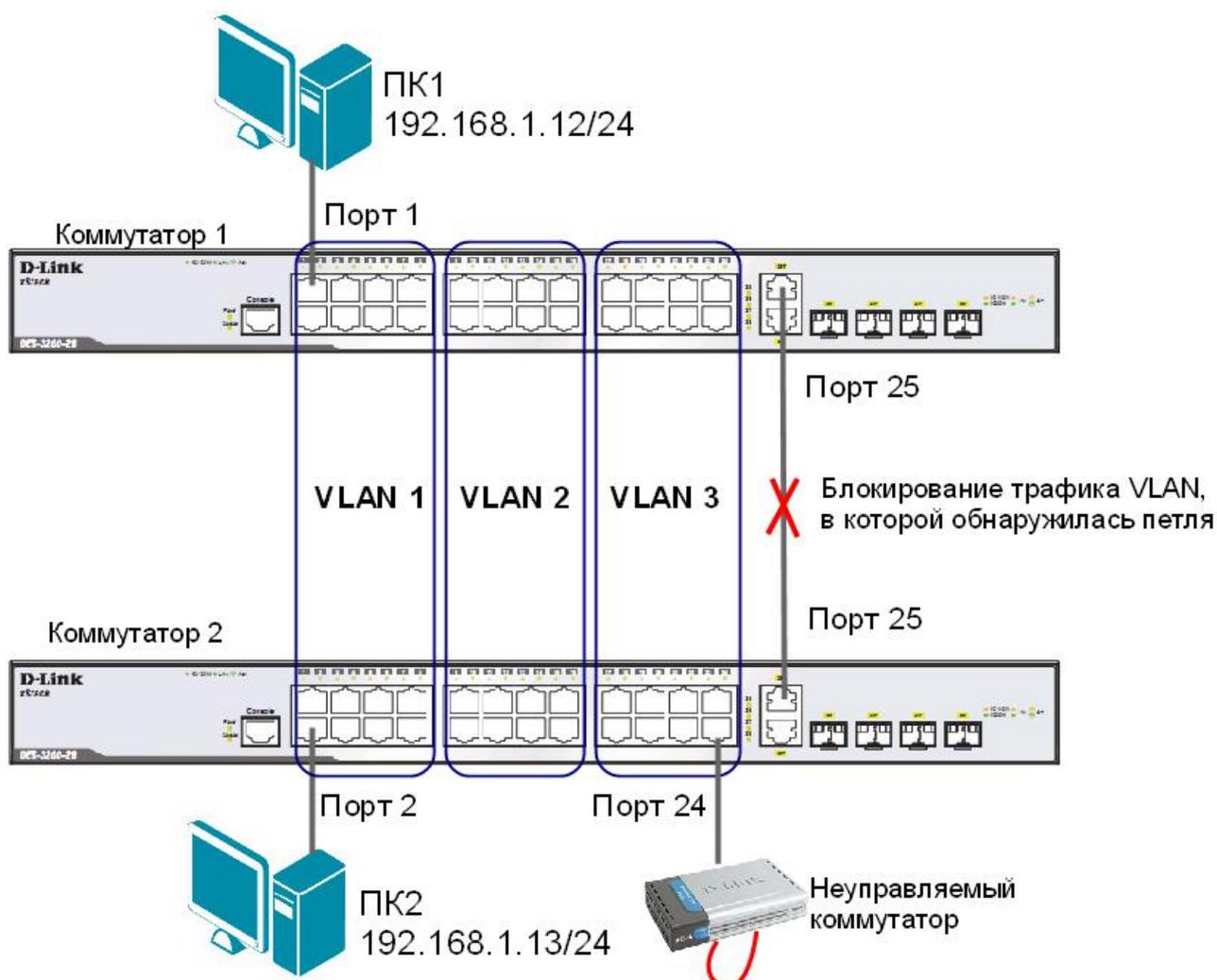
Что вы наблюдаете? Запишите.

Отключите неуправляемый коммутатор с петлей от управляемого коммутатора.

9.2. Настройка функции LoopBack Detection Independent STP в режиме VLAN-Based.

В данном задании рассматривается блокирование порта управляемого коммутатора для передачи трафика только той VLAN, в которой обнаружена петля. Остальной трафик будет передаваться через этот порт.

Схема 9.2



Примечание: если при передаче пакетов порт 25 коммутатора 1 получит ECTP-кадр, который отправлял сам, передача трафика в VLAN 3, из которой он пришёл, будет заблокирована.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам командой:

```
reset config
```

Настройка коммутатора 1

Удалите порты из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 9-24
```

Создайте VLAN vlan2 и vlan3:

```
create vlan vlan2 tag 2  
create vlan vlan3 tag 3
```

Добавьте в созданные VLAN v2 и v3 немаркированные порты. Добавьте порт 25 в VLAN default, v2 и v3 в качестве маркированного:

```
config vlan default add tagged 25  
config vlan vlan2 add untagged 9-16  
config vlan vlan2 add tagged 25  
config vlan vlan3 add untagged 17-24  
config vlan vlan3 add tagged 25
```

Проверьте настройки VLAN:

```
show vlan
```

Включите функцию LBD глобально на коммутаторе:

```
enable loopdetect
```

Активизируйте функцию LBD на всех портах коммутатора:

```
config loopdetect ports all state enabled
```

Сконфигурируйте режим VLAN-Based, в котором при обнаружении петли порт не сможет передавать трафик той VLAN, в которой обнаружена петля:

```
config loopdetect mode vlan-based
```

Настройка коммутатора 2

Удалите порты из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 9-24
```

Создайте VLAN vlan2 и vlan3:

```
create vlan vlan2 tag 2  
create vlan vlan3 tag 3
```

Добавьте в созданные VLAN v2 и v3 немаркированные порты. Добавьте порт 25 в VLAN default, v2 и v3 в качестве маркированного:

```
config vlan default add tagged 25  
config vlan vlan2 add untagged 9-16  
config vlan vlan2 add tagged 25  
config vlan vlan3 add untagged 17-24  
config vlan vlan3 add tagged 25
```

Проверьте настройки VLAN:

```
show vlan
```

Отключите функцию LBD глобально на коммутаторе:

```
disable loopdetect
```

Подключите неуправляемый коммутатор с петлей к коммутатору 2, как показано на схеме 9.2.

Посмотрите, обнаружена ли петля на коммутаторах 1 и 2:

```
show loopdetect ports 1-24
```

Что вы наблюдаете? Запишите.

Коммутатор 1 _____

Коммутатор 2 _____

Проверьте log-файл коммутаторов:

```
show log
```

Что вы наблюдаете, запишите?

Коммутатор 1 _____

Коммутатор 2 _____

Проверьте загрузку портов:

```
show utilization ports
```

Что вы наблюдаете? Запишите.

Коммутатор 1 _____

Коммутатор 2 _____

Отключите неуправляемый коммутатор с петлей от коммутатора 2.

Лабораторная работа №10. Агрегирование каналов

Агрегирование каналов связи (Link Aggregation) – это объединение нескольких физических портов в одну логическую магистраль на канальном уровне модели OSI с целью образования высокоскоростного канала передачи данных и повышения отказоустойчивости.

Все избыточные связи в одном агрегированном канале остаются в рабочем состоянии, а имеющийся трафик распределяется между ними для достижения балансировки нагрузки. При отказе одной из линий, входящих в такой логический канал, трафик распределяется между оставшимися линиями.

Включённые в агрегированный канал порты называются членами группы агрегирования (Link Aggregation Group). Один из портов в группе выступает в качестве мастера-порта (master port). Так как все порты агрегированной группы должны работать в одном режиме, конфигурация мастера-порта распространяется на все порты в группе.

Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Выбор порта для конкретного сеанса выполняется на основе выбранного алгоритма агрегирования портов, т.е. на основании некоторых признаков поступающих пакетов.

В коммутаторах D-Link по умолчанию используется алгоритм mac_source (MAC-адрес источника).

Программное обеспечение коммутаторов D-Link поддерживает два типа агрегирования каналов связи: статическое и динамическое, на основе стандарта IEEE 802.3ad (LACP).

При статическом агрегировании каналов (используется по умолчанию), все настройки на коммутаторах выполняются вручную, и они не допускают динамических изменений в агрегированной группе.

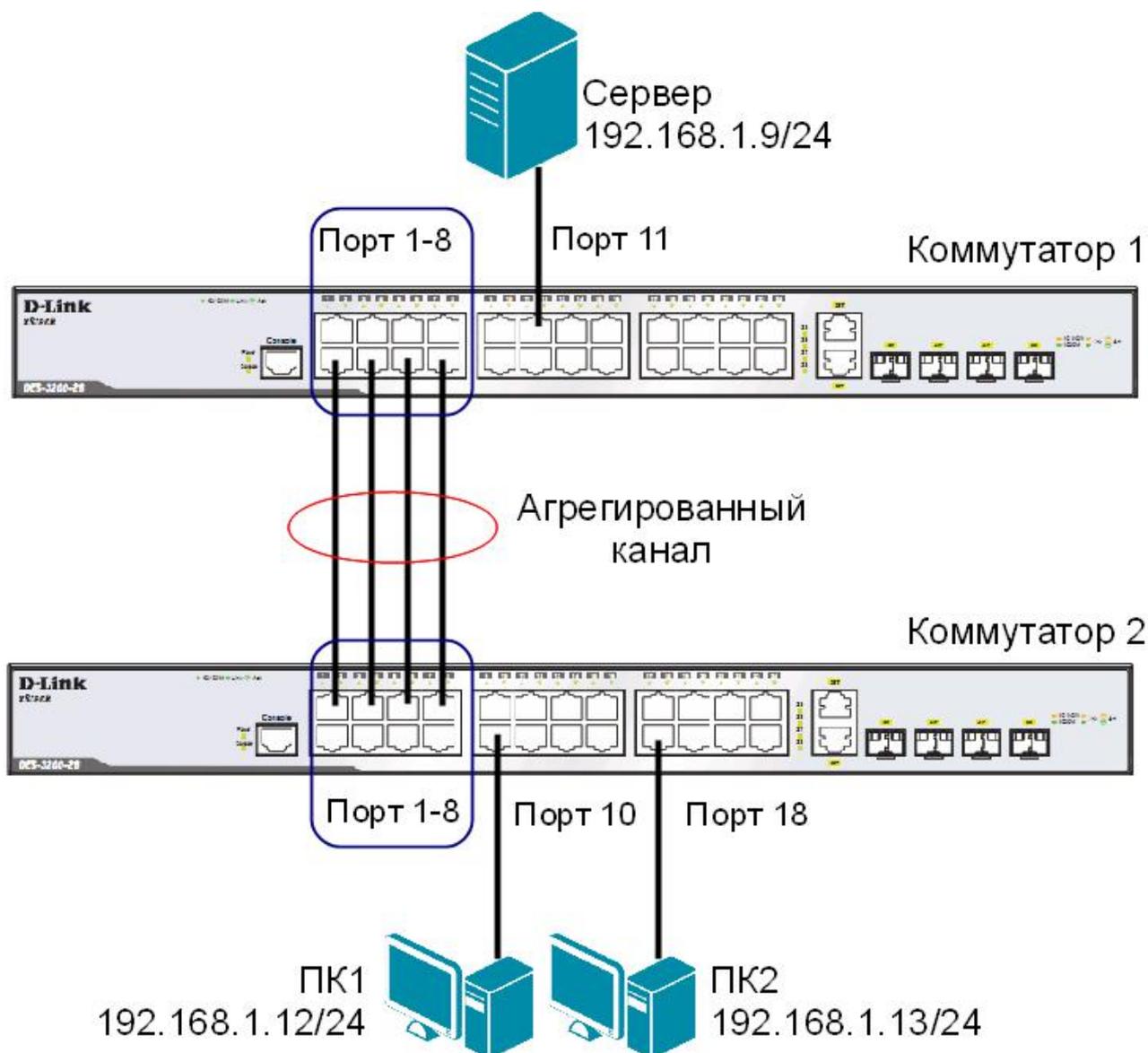
Для организации динамического агрегирования каналов между коммутаторами и другими сетевыми устройствами используется протокол управления агрегированным каналом – Link Aggregation Control Protocol (LACP). Протокол LACP определяет метод управления объединением нескольких физических портов в одну логическую группу и предоставляет сетевым устройствам возможность автосогласования каналов, путём отправки управляющих кадров протокола LACP непосредственно подключённым устройствам с поддержкой LACP. Порты, на которых активизирован протокол LACP, могут быть настроены для работы в одном из двух режимов: активном (active) или пассивном (passive). При работе в активном режиме порты выполняют обработку и рассылку управляющих кадров протокола LACP. При работе в пассивном режиме порты выполняют только обработку управляющих кадров LACP.

Для создания искусственной нагрузки на канал связи между коммутаторами, при выполнении лабораторной работы будет использоваться программа iperf.

Цель: изучить настройку динамического агрегирования каналов на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	3 шт.
Консольный кабель	2 шт.
Кабель Ethernet	7 шт.



Примечание: не соединяйте физически соответствующие порты коммутаторов до тех пор, пока не настроено агрегирование каналов, т.к. в коммутируемой сети может возникнуть петля.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:
`reset config`

Настройка коммутатора 1

Создайте группу агрегирования каналов:

```
create link_aggregation group_id 1 type lacp
```

Включите порты 1-8 в группу агрегирования каналов и выберите порт 1 в качестве мастера-порта:

```
config link_aggregation group_id 1 master_port 1 ports 1-8 state enabled
```

Настройте порты на работу в пассивном режиме:

```
config lacp_port 1-8 mode passive
```

Проверьте выполненные настройки:

```
show link_aggregation
```

Проверьте режим работы LACP на портах коммутаторов:

```
show lacp_port
```

Посмотрите текущий алгоритм агрегирования каналов:

```
show link_aggregation algorithm
```

Настройка коммутатора 2

Создайте группу агрегирования каналов:

```
create link_aggregation group_id 1 type lacp
```

Включите порты 1-8 в группу агрегирования каналов и выберите порт 1 в качестве мастера-порта:

```
config link_aggregation group_id 1 master_port 1 ports 1-8 state enabled
```

Настройте порты на работу в активном режиме:

```
config lacp_port 1-8 mode active
```

Проверьте выполненные настройки:

```
show link_aggregation
```

Проверьте режим работы LACP на портах коммутаторов:

```
show lacp_port
```

Подключите коммутаторы 4 кабелями, как показано на схеме 10. Из настроенной группы можно использовать любые порты.

Для создания искусственной нагрузки на канал связи между коммутаторами, используется утилита командной строки **iperf**. Iperf (для Windows) представляет собой небольшой исполняемый файл, который содержит клиентскую и серверную части. Программа не требует установки. Для запуска необходимо скопировать программу iperf на оба компьютера и запустить сначала серверную часть, а затем клиентскую.

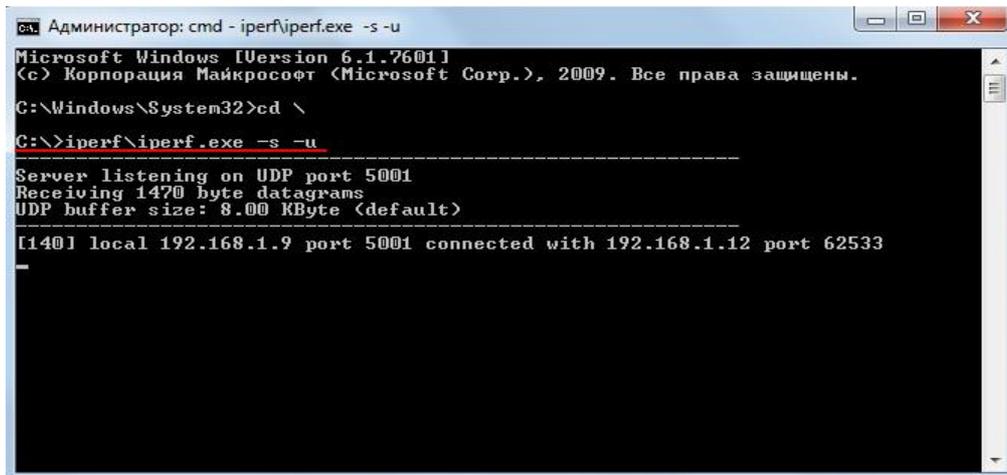
Ключи, используемые при запуске программы iperf:

- s – устанавливает режим сервера;
- c – устанавливает режим клиента и задает адрес сервера;
- i – задает интервал вывода отчета о скорости;
- t – время длительности теста в секундах;
- r – режим двустороннего тестирования;
- u – режим тестирования по протоколу UDP, а не TCP;
- b10M – задает полосу генерации трафика в 10 Мбит/с;
- P5 – запускает одновременно 5 тестовых потоков.

ЗАДАНИЕ

Запустите программу iperf на ПК, выполняющего роль сервера (запускается из командной строки, где указывается путь к программе и ключи):

```
iperf -s -u
```

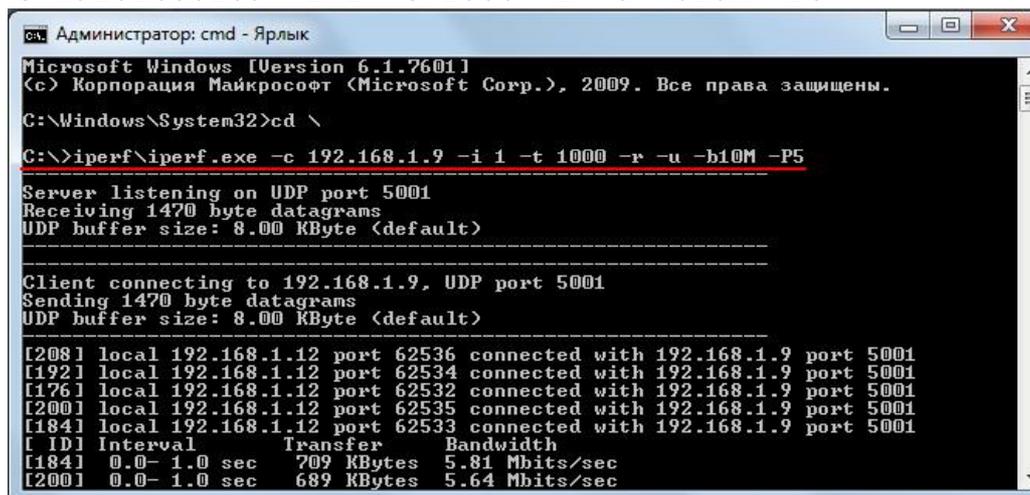


```
Администратор: cmd - iperf\iperf.exe -s -u
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Windows\System32>cd \
C:\>iperf\iperf.exe -s -u
-----
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
-----
[140] local 192.168.1.9 port 5001 connected with 192.168.1.12 port 62533
-
```

Рисунок 10.1 Запуск программы iperf на ПК, выполняющего роль сервера

Запустите программу iperf на ПК1 и ПК2:

```
iperf -c 192.168.1.9 -i 1 -t 1000 -r -u -b10M -P5
```



```
Администратор: cmd - Ярлык
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Windows\System32>cd \
C:\>iperf\iperf.exe -c 192.168.1.9 -i 1 -t 1000 -r -u -b10M -P5
-----
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
-----
Client connecting to 192.168.1.9, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
-----
[208] local 192.168.1.12 port 62536 connected with 192.168.1.9 port 5001
[192] local 192.168.1.12 port 62534 connected with 192.168.1.9 port 5001
[176] local 192.168.1.12 port 62532 connected with 192.168.1.9 port 5001
[200] local 192.168.1.12 port 62535 connected with 192.168.1.9 port 5001
[184] local 192.168.1.12 port 62533 connected with 192.168.1.9 port 5001
[ ID] Interval      Transfer      Bandwidth
[184] 0.0- 1.0 sec   709 KBytes    5.81 Mbits/sec
[200] 0.0- 1.0 sec   689 KBytes    5.64 Mbits/sec
```

Рисунок 10.2 Запуск программы iperf на ПК, выполняющего роль клиента

Во время теста проверьте загрузку портов на обоих коммутаторах:

```
show utilization ports
```

Что вы наблюдаете? Загрузка трафика перераспределяется между каналами? Сколько одновременно соединений участвует в передаче? Почему?

Лабораторная работа №11. Настройка QoS. Приоритизация трафика. Управление полосой пропускания

Сети с коммутацией пакетов на основе протокола IP не обеспечивают гарантированной пропускной способности, поскольку не обеспечивают гарантированной доставки.

Для приложений, где не важен порядок и интервал прихода пакетов, время задержек между отдельными пакетами не имеет решающего значения. Для приложений чувствительных к задержкам, в сети должны быть реализованы механизмы, обеспечивающие функции качества обслуживания (Quality of Service, QoS).

Функции качества обслуживания в современных сетях заключаются в обеспечении гарантированного и дифференцированного уровня обслуживания сетевого трафика, запрашиваемого теми или иными приложениями на основе различных механизмов распределения ресурсов, ограничения интенсивности трафика, обработки очередей и приоритизации.

Для обеспечения QoS на канальном уровне модели OSI коммутаторы поддерживают стандарт IEEE 802.1p. Стандарт IEEE 802.1p позволяет задать до 8 уровней приоритетов (от 0 до 7, где 7 – наивысший), определяющих способ обработки кадра, используя 3 бита поля приоритета тега IEEE 802.1Q.

В лабораторной работе рассматривается следующий пример: в сети, имеющей явное «узкое» место, на рабочих станциях ПК1 и ПК3 выполняется тест ping друг на друга. Этому трафику необходимо обеспечить высокий приоритет обработки по сравнению с приложениями остальных станций, которые создают искусственную нагрузку на канал связи между коммутаторами с помощью программы iperf.

Цель: изучить настройку приоритизации трафика, управление полосой пропускания на коммутаторах D-Link. Исследовать эффективность работы приоритизации.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1

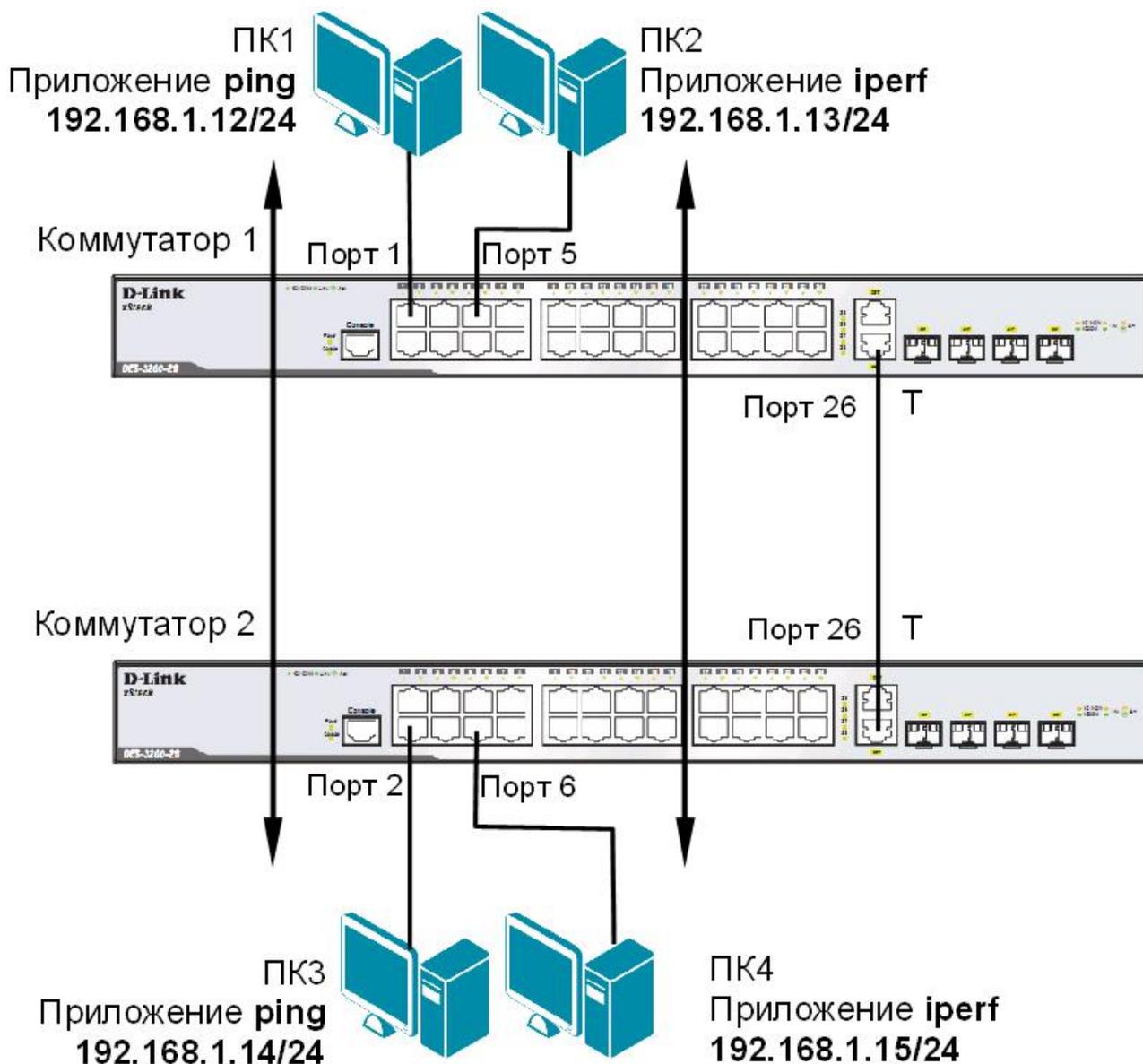
Для создания «узкого» места, настройте на порте 26 функцию bandwidth_control, ограничивающую приём и передачу данных скоростью 64 Кбит/с:

```
config bandwidth_control 26 rx_rate 64 tx_rate 64
```

Настройка коммутатора 2

Для создания «узкого» места, настройте на порте 26 функцию bandwidth_control, ограничивающую приём и передачу данных скоростью 64 Кбит/с:

```
config bandwidth_control 26 rx_rate 64 tx_rate 64
```



ЗАДАНИЕ 1

Назначьте на всех ПК IP-адреса из одной подсети. Запустите продолжительный тест ping между ПК1 и ПК3, а так же между ПК2 и ПК4.

Собрав в течение 20-30 секунд статистику, запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они существуют:

между ПК1 и ПК3 _____
 между ПК2 и ПК4 _____

ЗАДАНИЕ 2

Запустите продолжительный тест ping между ПК1 и ПК3, а так же между ПК2 и ПК4.

Для создания нагрузки на линию связи между коммутаторами, запустите программу iperf:

~ на ПК2 с ключом «-s» (в роли сервера):
`iperf -s -u`

~ на ПК4 с ключами «-с ip-сервера -i 1 -t 10000 -r -u -b10M -P5» (в роли клиента):
`iperf -c 192.168.1.13 -i 1 -t 10000 -r -u -b10M -P5`

НЕ ОСТАНАВЛИВАЙТЕ запущенные программы `ping` и `iperf`. Собранная с помощью них статистика понадобится для выполнения следующего задания.

Собрав в течение 20-30 секунд статистику, запишите примерную среднюю скорость, выводимую программой `iperf`:

- ПК2 _____
- ПК4 _____

Посмотрите на ПК1 и ПК3, ПК2 и ПК4 информацию и запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они есть:

от ПК1 к ПК3 _____
от ПК3 и ПК1 _____
от ПК2 и ПК4 _____
от ПК4 и ПК2 _____

Запишите ваши наблюдения, сравните их с результатами задания 1:

ЗАДАНИЕ 3

Настройте приоритизацию. Для этого поменяйте на порте 1, к которому подключена рабочая станция ПК1, значение приоритета по умолчанию на 7:

```
config 802.1p default_priority 1 7
```

Примечание: пользовательский приоритет и метод обработки остаются по умолчанию.

Поменяйте на порте 2, к которому подключена рабочая станция ПК3, значение приоритета по умолчанию на 7:

```
config 802.1p default_priority 2 7
```

Примечание: благодаря изменению значения приоритета портов, к которым подключены компьютеры с приоритетным трафиком на 7, все кадры, передаваемые ими, получат наивысший приоритет по сравнению с кадрами, поступающими от других компьютеров на остальные не приоритизированные порты обоих коммутаторов.

Посмотрите текущие настройки приоритета по умолчанию на портах коммутаторов 1 и 2:

```
show 802.1p default_priority
```

Какой приоритет назначен по умолчанию порту 3?

Посмотрите карту привязки пользовательских приоритетов 802.1p к очередям класса обслуживания:

```
show 802.1p user_priority
```

Запишите, что вы наблюдаете. Какому классу обслуживания соответствует приоритет по умолчанию = 0?

При включении приоритизации посмотрите, как изменились условия прохождения трафика. Изменились ли они, и насколько? Сравните результаты с заданием 2.

Сравните результаты с заданием 1. Удалось ли достичь в нагруженном канале с включённой приоритизацией таких же параметров, что и в не нагруженном канале для трафика между ПК 1 и ПК3? Объясните почему?

Лабораторная работа №12. Списки управления доступом (Access Control List)

Списки управления доступом (Access Control List, ACL) являются средством фильтрации потоков данных без потери производительности, так как проверка содержимого пакетов данных выполняется на аппаратном уровне. Фильтруя потоки данных, администратор может ограничить типы приложений, разрешённых для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS, путём классификации трафика и переопределения его приоритета.

ACL представляют собой последовательность условий проверки параметров пакетов данных. Когда сообщения поступают на входной интерфейс, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определёнными в ACL и выполняет над пакетами одно из действий: Permit (Разрешить) или Deny (Запретить).

Списки управления доступом состоят из профилей доступа (Access Profile) и правил (Rule). Профили доступа определяют типы критериев фильтрации, которые должны проверяться в пакете данных (MAC-адрес, IP-адрес, номер порта, VLAN и т.д.), а в правилах указываются непосредственные значения их параметров. Каждый профиль может состоять из множества правил.

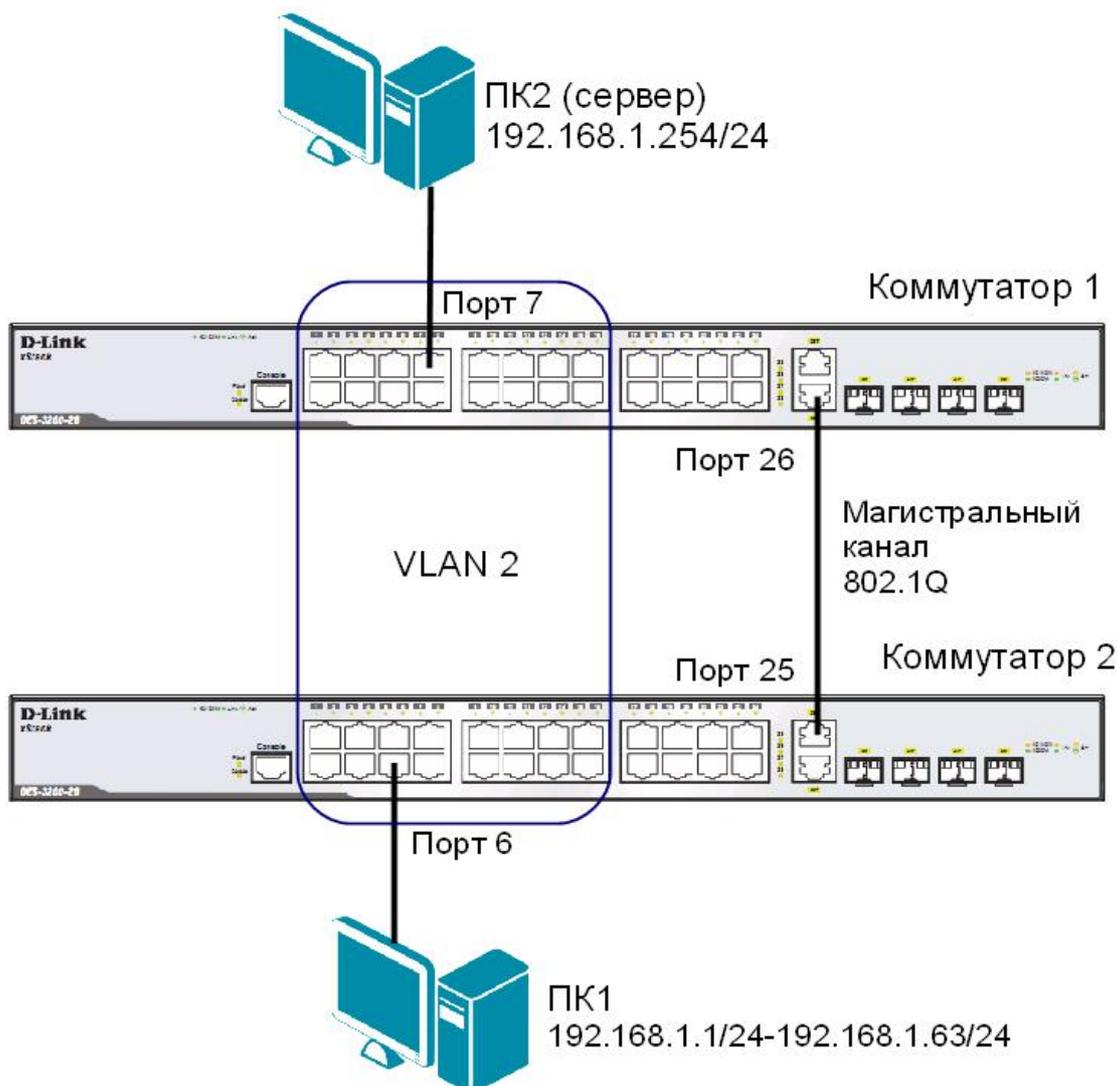
Цель: на коммутаторе D-Link настроить списки управления доступом, используя в качестве критериев фильтрации MAC и IP-адреса.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	2 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	3 шт.

12.1. Настройка ограничения доступа пользователей к серверу по IP-адресам

Схема 12.1



ЗАДАНИЕ

Разрешить доступ к серверу пользователям с IP-адресами с 192.168.1.1/24 по 192.168.1.63/24. Остальным пользователям сети 192.168.1.0/24, с адресами не входящими в разрешённый диапазон, доступ к серверу запретить.

Правила:

Правило 1:

Если IP-адрес источника = IP-адресам из диапазона с 192.168.1.1 по 192.168.1.63 (подсеть 192.168.1.0/26) — разрешить (permit);

Правило 2:

Если IP-адрес источника принадлежит сети 192.168.0.0/24, но не входит в разрешенный диапазон адресов — запретить (deny).

Правило 3:

Иначе, по умолчанию разрешить доступ всем узлам.

Примечание: максимальное количество профилей, которое поддерживает коммутатор DES-3200-28 равно 4.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам командой:
reset config

Настройка коммутатор 2

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
config vlan default delete 1-16

Создайте VLAN 2 и добавьте соответствующие порты, которые необходимо настроить немаркированными. Настройте порт 25 маркированным:
create vlan v2 tag 2
config vlan v2 add untagged 1-16
config vlan v2 add tagged 25

Проверьте настройки VLAN:
show vlan

Повторите процедуру настройки для коммутатора 1

Проверьте доступность соединения между ПК1 и ПК2 командой ping:
ping <IP-address>

от ПК1 к ПК2 _____

Настройка коммутатора 1

Создайте профиль доступа с номером 4, осуществляющий фильтрацию трафика по IP-адресам:
create access_profile profile_id 4 profile_name 4 ip
source_ip_mask 255.255.255.255

Правило 1.

Создайте правило для профиля доступа 4, разрешающее доступ для подсети 192.168.1.0/26 (узлам с 1 по 63):
config access_profile profile_id 4 add access_id 1 ip source_ip
192.168.1.0 mask 255.255.255.192 port 26 permit

Примечание: созданное правило разрешает прохождение трафика IP-подсети 192.168.1.0/26 через 26 порт.

Правило 2

Создайте правило для профиля доступа 4, запрещающее остальным станциям доступ к серверу:
config access_profile profile_id 4 add access_id 2 ip source_ip
192.168.1.0 mask 255.255.255.0 port 26 deny

Примечание: созданное правило запрещает прохождение через 26 порт трафика, который принадлежит сети 192.168.1.0/24, но не входит в разрешенный диапазон.

Правило 3

Разрешите все остальное:
Выполняется по умолчанию

Проверьте созданные профили:

```
show access_profile
```

Что вы наблюдаете? Сколько профилей создано, сколько в них правил?

Подключите рабочую станцию ПК1 как показано на схеме 12.1 (адрес из диапазона 192.168.1.1-192.168.1.63/24) к коммутатору 2.

Протестируйте командой ping соединение с сервером 192.168.1.254/24.

Что вы наблюдаете? Запишите.

Измените IP-адрес рабочей станции ПК1 (адрес из диапазона 192.168.1.64-192.168.1.254/24)

Протестируйте командой ping соединение с сервером 192.168.1.254/24.

Что вы наблюдаете? Запишите.

Удалите профиль ACL:

```
delete access_profile profile_id 4
```

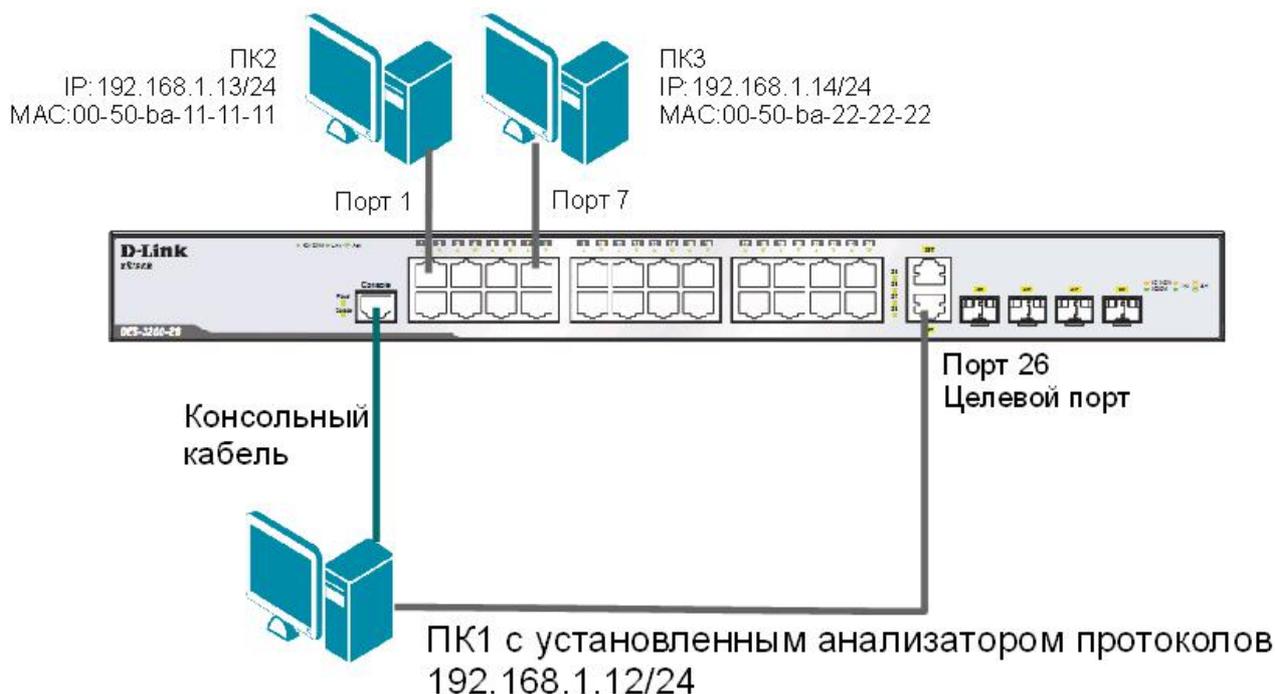
Проверьте соединение с сервером командой ping:

```
ping 192.168.1.254
```

Что вы наблюдаете? Запишите.

12.2. Настройка фильтрации кадров по MAC-адресам

Схема 12.2



ЗАДАНИЕ

Настроить профиль доступа так, чтобы кадры, принимаемые на любой порт коммутатора от ПК3 (с MAC-адресом 00-50-ba-22-22-22) зеркалировались (копировались) на целевой порт коммутатора, к которому подключено устройство мониторинга сети.

Правило:

Если MAC-адрес источника = MAC-адресу ПК3 (00-50-ba-22-22-22) — копировать кадры на целевой порт.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам командой:

```
reset config
```

Внимание! Замените указанные в командах MAC-адреса на реальные MAC-адреса рабочих станций.

Создайте профиль доступа 4:

```
create access_profile profile_id 4 profile_name 4 ethernet  
source_mac FF-FF-FF-FF-FF-FF
```

Создайте правило для профиля доступа 4, в результате выполнения которого кадры, принимаемые на любой порт коммутатора с ПК3 будут зеркалироваться на целевой порт:

```
config access_profile profile_id 4 add access_id 1 ethernet  
source_mac 00-50-ba-22-22-22 mask FF-FF-FF-FF-FF-FF port all  
mirror
```

Проверьте созданный профиль:

```
show access_profile
```

Включите функцию зеркалирования портов глобально на коммутаторе:
enable mirror

Укажите целевой порт:
config mirror port 26

Проверьте настройки функции:
show mirror

Подключите рабочие станции ПК2 и ПК3 как показано на схеме 12.2

Выполните тестирование соединения между ПК2 и ПК3 с помощью команды:
ping <IP address>

- от ПК2 к ПК3 _____
- от ПК3 к ПК2 _____

Запустите на рабочей станции ПК1 анализатор протоколов Wireshark (настройка программы описана в лабораторной работе №15).

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Что вы наблюдаете? Запишите.

Подключите рабочую станцию ПК3 к порту 10 коммутатора.

Выполните тестирование соединения между ПК2 и ПК3 и наоборот командой ping.

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Что вы наблюдаете? Что изменилось? Запишите.

Удалите все профили ACL:
delete access_profile all

Отключите функцию зеркалирования портов:
disable mirror

Лабораторная работа №13. Контроль над подключением узлов к портам коммутатора. Функция Port Security

Функция Port Security позволяет настроить какой-либо порт коммутатора так, чтобы доступ к сети через него мог осуществляться только определёнными устройствами. Устройства, которым разрешено подключаться к порту определяются по MAC-адресам. MAC-адреса могут быть изучены динамически или вручную настроены администратором сети. Помимо этого функция Port Security позволяет ограничивать количество изучаемых портом MAC-адресов, тем самым, ограничивая количество подключаемых к нему узлов.

Существует три режима работы функции Port Security:

- *Permanent* (Постоянный) – занесённые в таблицу коммутации MAC-адреса никогда не устаревают, даже если истекло время, установленное таймером Aging Time или коммутатор был перезагружен.
- *Delete on Timeout* (Удалить при истечении времени) – занесённые в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером Aging Time и будут удалены.

Если состояние канала связи на подключённом порте изменяется, MAC-адреса, изученные на нем, удаляются из таблицы коммутации, что аналогично выполнению действий при истечении времени, установленного таймером Aging Time.

- *Delete on Reset* (Удалить при сбросе) – занесённые в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

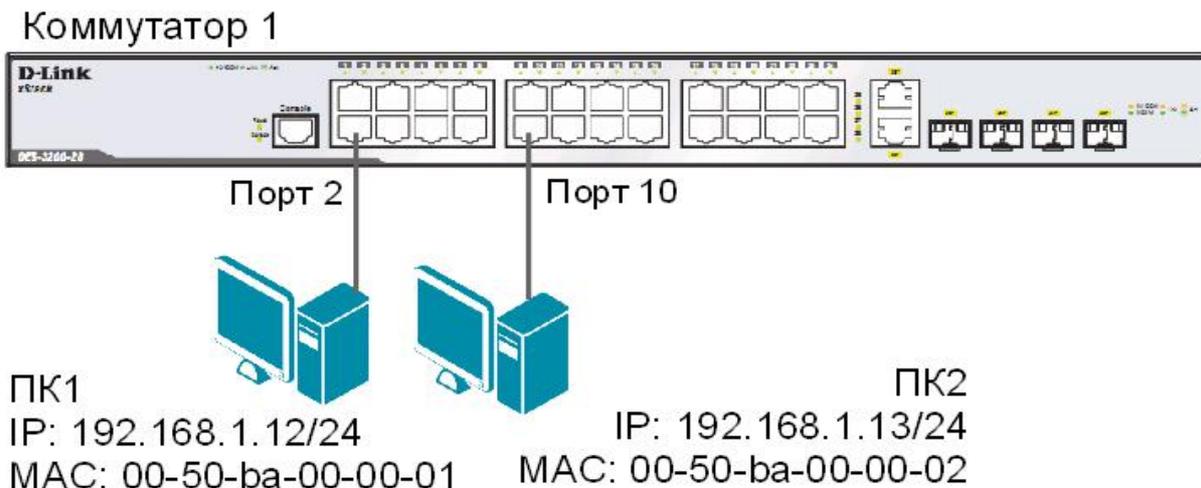
Функция Port Security оказывается весьма полезной при построении домашних сетей, сетей провайдеров Интернет и локальных сетей с повышенным требованием по безопасности, где требуется исключить доступ незарегистрированных рабочих станций к услугам сети.

Используя функцию Port Security можно полностью запретить динамическое изучение MAC-адресов указанными или всеми портами коммутатора. В этом случае доступ к сети получают только те пользователи, MAC-адреса которых указаны в статической таблице коммутации.

Цель: научиться управлять подключением узлов к портам коммутатора и изучить настройку функции Port Security на коммутаторах D-Link.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.



13.1. Управление количеством подключаемых к портам коммутатора пользователей, путём ограничения максимального количества изучаемых MAC-адресов

Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:
`reset config`

Проверьте информацию о настройках Port Security:
`show port_security`

Установите максимальное количество изучаемых каждым портом MAC-адресов равным 1, и включите функцию на всех портах:
`config port_security ports all admin_state enable`
`max_learning_addr 1`

Подключите ПК1 и ПК2 к портам 2 и 10 коммутатора соответственно.

Посмотрите MAC-адреса, которые стали известны портам 2 и 10:
`show fdb port 2`
`show fdb port 10`

Проверьте, соответствуют ли зарегистрированные адреса адресам рабочих станций: _____

Проверьте информацию о настройках Port Security на портах коммутатора:
`show port_security ports 1-24`

Включите запись в журнал работы коммутатора MAC-адресов, подключающихся к порту станций и отправку сообщений SNMP Trap:
`enable port_security trap_log`

Выполните тестирование доступности узлов командой `ping` от ПК1 к ПК2 и наоборот.

Подключите ПК1 к порту 10, а ПК2 к порту 1.

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте информацию в журнале работы коммутатора:

```
show log
```

Какой вы сделаете вывод? _____

Сохраните конфигурацию и перезагрузите коммутатор:

```
save  
reboot
```

Выполните тестирование соединения между рабочими станциями командой ping.

Какой вы сделаете вывод? Сохраняется ли информация о привязке MAC-порт?

Настройте на порте 2 работу функции Port Security в режиме Permanent и максимальное количество изучаемых адресов равное 1:

```
config port_security ports 2 admin_state enable max_learning_addr  
1 lock_address_mode permanent
```

Сохраните конфигурацию и перезагрузите коммутатор:

```
save  
reboot
```

Проверьте информацию о настройках Port Security на портах коммутатора:

```
show port_security ports 1-24
```

Какой вы сделаете вывод? Сохраняется ли информация о привязке MAC-порт?

Очистите информацию о привязке MAC-порт на порте 2:

```
clear port_security_entry port 2
```

Отключите работу функции Port Security на порте 2 и приведите настройки в исходное (по умолчанию) состояние:

```
config port_security ports 2 admin_state disable max_learning_addr  
1 lock_address_mode deleteonreset
```

Посмотрите время таймера блокирования (он соответствует времени жизни MAC-адреса в таблице коммутации):

```
show fdb aging_time
```

Изменить время действия таймера можно с помощью настройки времени жизни MAC-адреса в таблице коммутации (время указано в секундах):

```
config fdb aging_time 20
```

Измените режим работы функции Port Security на Delete on Timeout:

```
config port_security ports 2 admin_state enable max_learning_addr  
1 lock_address_mode deleteontimeout
```

Проверьте MAC-адреса, которые стали известны порту 2:

```
show fdb port 2
```

Проверьте информацию о настройках Port Security на портах коммутатора:

```
show port_security ports 1-24
```

Выполните тестирование соединения между ПК1 и ПК2 командой ping.

Какой вы сделаете вывод? Сохраняется информации о привязке MAC-порт?

Отключите работу функции Port Security на портах:

```
config port_security ports 1-24 admin_state disable
```

Отключите функцию записи в log-файл и отправки SNMP Trap:

```
disable port_security trap_log
```

Примечание: после выполнения обучения имеется возможность отключить функцию динамического изучения MAC-адресов, тогда в таблице коммутации сохранятся изученные адреса. Таким образом, текущая конфигурация сети будет сохранена, и дальнейшее подключение новых устройств без ведома администратора будет невозможно. Новые устройства можно добавить путём создания статических записей в таблице коммутации.

13.2. Настройка защиты от подключения к портам, основанной на статической таблице MAC-адресов

Сбросьте настройки коммутатора к заводским настройкам командой:

```
reset system
```

Активизируйте функцию Port Security на всех портах и запретите изучение MAC-адресов, установив параметр *max_learning_addr* равным 0 (команда вводится в одну строку):

```
config port_security ports 1-24 admin_state enable  
max_learning_addr 0
```

Проверьте состояние портов:

```
show ports
```

Проверьте соединение между ПК1 и ПК2 командой ping.

Проверьте состояние таблицы коммутации:

```
show fdb
```

Имеются ли там записи? _____

В таблице коммутации вручную создайте статические записи для MAC-адресов рабочих станций, подключённых к портам 2 и 10.

Внимание! Замените указанные в командах MAC-адреса на реальные адреса рабочих станций, подключаемых к коммутатору.

```
create fdb default 00-50-ba-00-00-01 port 2
create fdb default 00-50-ba-00-00-02 port 10
```

Проверьте созданные статические записи в таблице коммутации:
show fdb

Проверьте информацию о настройках Port Security на портах коммутатора:
show port_security ports 1-24

Проверьте соединение между ПК1 и ПК2 командой ping.

Подключите ПК1 к порту 8, а ПК2 к порту 2.

Повторите тестирование командой ping.

Какой вы сделаете вывод? _____

Удалите ранее созданную статическую запись из таблицы MAC-адресов на порте 2:
delete fdb default 00-50-ba-00-00-02 port 2

Лабораторная работа №14. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding

Функция IP-MAC-Port Binding (IMPВ), реализованная в коммутаторах D-Link, позволяет контролировать доступ компьютеров в сеть на основе их IP- и MAC-адресов, а также порта подключения. Администратор сети может создать записи («белый лист»), связывающие MAC- и IP-адреса компьютеров с портами подключения коммутатора. На основе этих записей, в случае совпадения всех составляющих, клиенты будут получать доступ к сети со своих компьютеров. В том случае, если при подключении клиента, связка IP-MAC-порт будет отличаться от параметров заранее сконфигурированной записи, то коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «чёрный лист».

Функция IP-MAC-Port Binding включает три режима работы: ARP mode (по умолчанию), ACL mode и DHCP Snooping mode.

ARP mode является режимом, используемым по умолчанию, при настройке функции IP-MAC-Port Binding на портах. При работе в режиме ARP коммутатор анализирует ARP-пакеты и сопоставляет параметры IP-MAC ARP-пакета с предустановленной администратором связкой IP-MAC. Если хотя бы один параметр не совпадает, то MAC-адрес узла будет занесён в таблицу коммутации с отметкой «Drop» (Отбрасывать). Если все параметры совпадают, MAC-адрес узла будет занесён в таблицу коммутации с отметкой «Allow» (Разрешён).

При функционировании в *ACL mode*, коммутатор на основе предустановленного администратором «белого листа» IMPВ создает правила ACL. Любой пакет, связка IP-MAC которого отсутствует в «белом листе», будет блокироваться ACL.

Режим *DHCP Snooping* используется коммутатором для динамического создания записей IP-MAC на основе анализа DHCP-пакетов и привязки их к портам с включённой функцией IMPВ (администратору не требуется создавать записи вручную). Таким образом, коммутатор автоматически создает «белый лист» IMPВ в таблице коммутации или аппаратной таблице ACL (при включении режима ACL). При этом для обеспечения корректной работы, сервер DHCP должен быть подключён к доверенному порту с выключенной функцией IMPВ. Администратор может ограничить максимальное количество создаваемых в процессе автоизучения записей IP-MAC на порт, следовательно, ограничить для каждого порта с активизированной функцией IMPВ количество узлов, которые могут получить IP-адрес с DHCP-сервера. При работе в режиме DHCP Snooping коммутатор не будет создавать записи IP-MAC для узлов с IP-адресом установленным вручную.

При активизации функции IMPВ на порте администратор должен указать режим его работы:

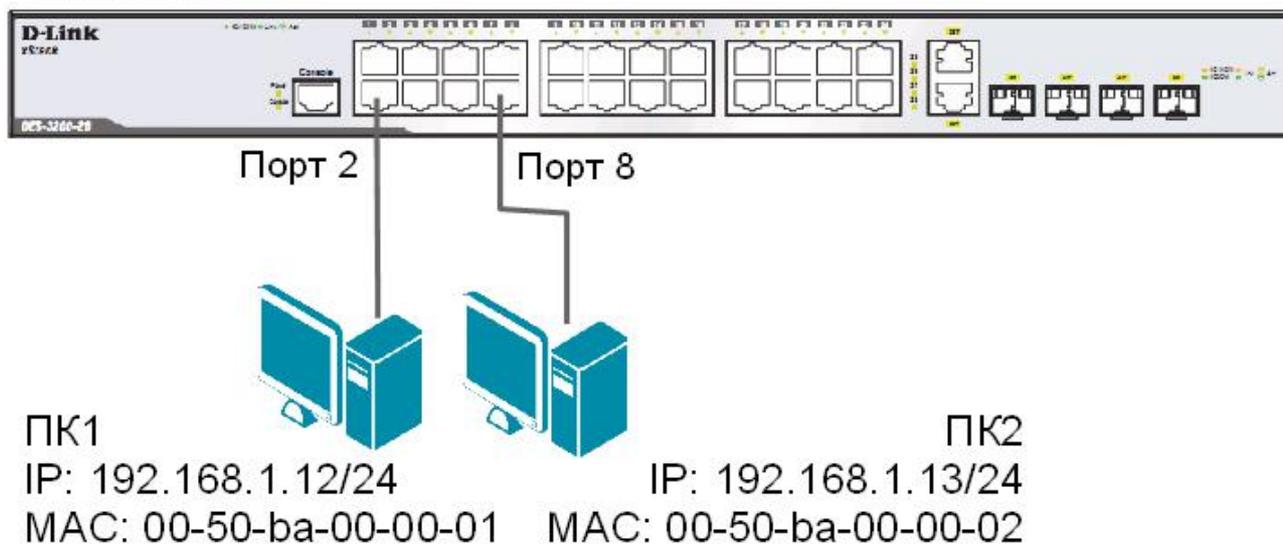
- **Strict Mode** – в этом режиме порт по умолчанию заблокирован.
- **Loose Mode** – в этом режиме порт по умолчанию открыт.

Цель: научиться управлять подключением узлов к портам коммутатора и изучить настройку функции IP-MAC-Port Binding на коммутаторах D-Link.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.

Коммутатор 1



14.1. Настройка работы функции IP-MAC-Port Binding в режиме ARP

Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:
`reset config`

Внимание! Замените указанные в командах MAC-адреса на реальные MAC-адреса рабочих станций, подключаемых к коммутатору.

Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес рабочей станции ПК1 с портом 2 (по умолчанию режим работы функции ARP):

```
create address_binding ip_mac ipaddress 192.168.1.12 mac_address
00-50-ba-00-00-01 ports 2
```

Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес рабочей станции ПК2 с портом 8:

```
create address_binding ip_mac ipaddress 192.168.1.13 mac_address
00-50-ba-00-00-02 ports 8
```

Активируйте функцию на портах 2 и 8 (по умолчанию режим работы портов strict):

```
config address_binding ip_mac ports 2,8 arp_inspection strict
```

Проверьте созданные записи IP-MAC-Port Binding:

```
show address_binding ip_mac all
```

Проверьте порты, на которых настроена функция и их режим работы:

```
show address_binding ports
```

Подключите рабочие станции ПК1 и ПК2 к коммутатору как показано на схеме 14.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

Включите запись в log-файл и отправку сообщений SNMP Trap в случае несоответствия ARP-пакета связке IP-МАС:

```
enable address_binding trap_log
```

Подключите ПК1 к порту 8, а ПК2 к порту 2.

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте заблокированные рабочие станции:

```
show address_binding blocked all
```

Проверьте наличие заблокированных станций в log-файле:

```
show log
```

Какой вы сделаете вывод? _____

Удалите адрес ПК1 из списка заблокированных адресов:

```
delete address_binding blocked vlan_name default mac_address 00-50-ba-00-00-01
```

Удалите адрес ПК2 из списка заблокированных адресов:

```
delete address_binding blocked vlan_name default mac_address 00-50-ba-00-00-02
```

Удалите запись IP-МАС-Port Binding:

```
delete address_binding ip_mac ipaddress 192.168.1.12 mac_address 00-50-ba-00-00-01
```

```
delete address_binding ip_mac ipaddress 192.168.1.13 mac_address 00-50-ba-00-00-02
```

Отключите функцию IP-МАС-Port Binding на портах 2 и 8:

```
config address_binding ip_mac ports 2,8 arp_inspection disable
```

14.2. Настройка работы функции IP-МАС-Port Binding в режиме ACL

Создайте запись IP-МАС-Port Binding, связывающую IP- и МАС-адрес станции ПК1 с портом 2:

```
create address_binding ip_mac ipaddress 192.168.1.12 mac_address 00-50-ba-00-00-01 ports 2
```

Создайте запись IP-МАС-Port Binding, связывающую IP- и МАС-адрес станции ПК2 с портом 8:

```
create address_binding ip_mac ipaddress 192.168.1.13 mac_address 00-50-ba-00-00-02 ports 8
```

Активизируйте функцию на портах 2 и 8 (по умолчанию режим работы портов Strict) и установите работу функции IMPV в режиме ACL:

```
config address_binding ip_mac ports 2,8 ip_inspection enable
```

Примечание: по умолчанию автоматически включается режим `allow_zeroip`, благодаря которому коммутатор не будет блокировать узлы, отправляющие ARP-пакеты с IP-адресом источника 0.0.0.0.

Проверьте созданные записи IP-MAC-Port Binding:

```
show address_binding ip_mac all
```

Проверьте порты, на которых настроена функция и их режим работы:

```
show address_binding ports
```

Проверьте, созданные профили доступа ACL:

```
show access_profile
```

Подключите рабочие станции ПК1 и ПК2 к коммутатору как показано на схеме 14.

Проверьте доступность соединения между рабочими станциями командой ping:

```
ping <IP-address>
```

Подключите ПК1 к порту 8, а ПК2 к порту 2.

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте заблокированные рабочие станции:

```
show address_binding blocked all
```

Какой вы сделаете вывод? _____

Удалите адрес из списка заблокированных адресов:

```
delete address_binding blocked vlan_name default mac_address 00-50-ba-00-00-01
```

Удалите все заблокированные адреса:

```
delete address_binding blocked all
```

Удалите все записи IP-MAC-Port Binding:

```
delete address_binding ip_mac ipaddress 192.168.1.12 mac_address 00-50-ba-00-00-01
```

```
delete address_binding ip_mac ipaddress 192.168.1.13 mac_address 00-50-ba-00-00-02
```

Отключите функцию IP-MAC-Port Binding на портах 2 и 8:

```
config address_binding ip_mac ports 2,8 ip_inspection disable
```

Какой можно сделать вывод о работе функции IP-MAC-Port Binding в режиме ACL?

Лабораторная работа №15. Функции анализа сетевого трафика

Коммутаторы улучшают производительность и надёжность сети, передавая трафик только на те порты, которым он предназначен. При этом анализ критичных данных – сложная задача, поскольку инструментальные средства сетевого анализа физически изолированы от анализируемого трафика.

В коммутаторах D-Link реализована поддержка функции Port Mirroring (Зеркалирование портов), которая полезна администраторам для мониторинга и поиска неисправностей в сети.

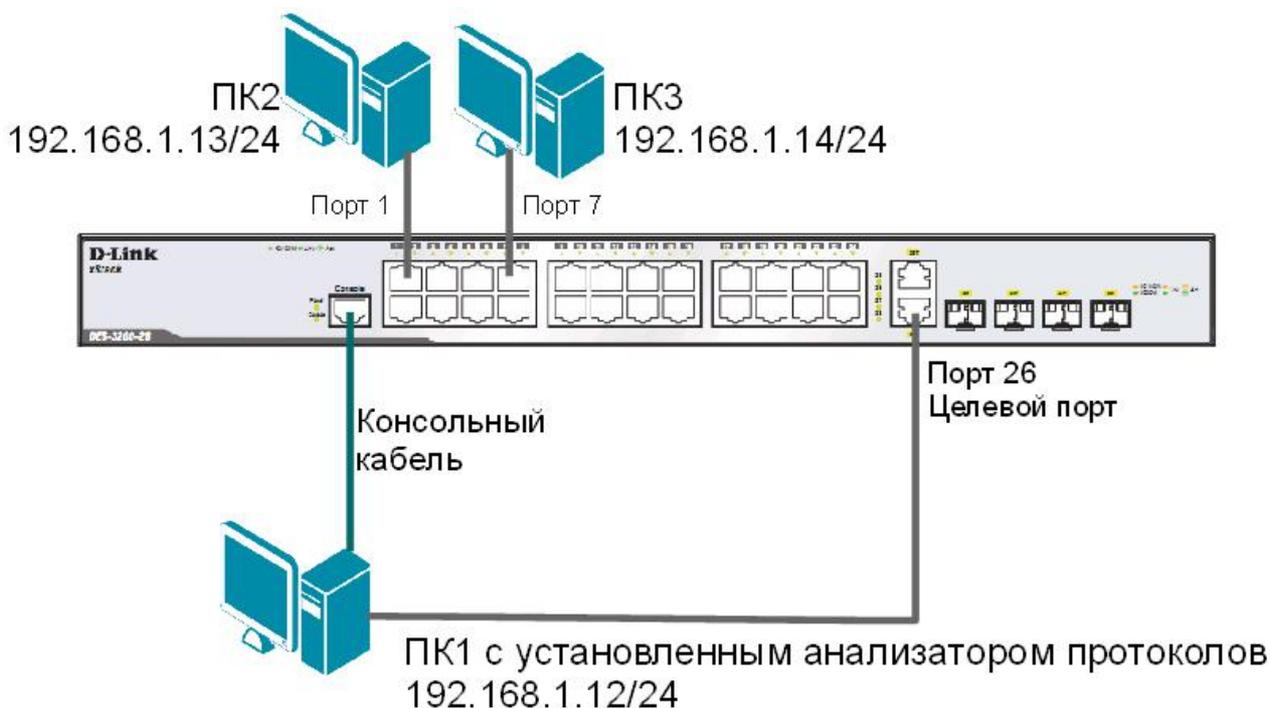
Функция Port Mirroring позволяет отображать (копировать) кадры, принимаемые в порт-источник (Source port) и отправляемые на целевой порт (Target port) коммутатора, к которому подключено устройство мониторинга с целью анализа проходящих через интересующий порт-источник пакетов.

Цель: изучить настройку функций зеркалирования портов и анализа сетевого трафика.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-28	1 шт.
Рабочая станция	3 шт.
Консольный кабель	1 шт.
Кабель Ethernet	3 шт.

Схема 15



Укажите порты, трафик которых будет пересылаться на целевой порт 26:
`config mirror port 26 add source ports 1,7 both`

Включите функцию зеркалирования портов глобально в коммутаторе:
`enable mirror`

Проверьте настройки функции:
show mirror

Внимание: целевой порт и порт-источник должны принадлежать одной VLAN и иметь одинаковую скорость работы. В том случае, если скорость порта-источника будет выше скорости целевого порта, то коммутатор снизит скорость порта-источника до скорости работы целевого порта. Также целевой порт не может быть членом группы агрегированных каналов.

Запустите на рабочей станции ПК1 анализатор протоколов Wireshark. Интерфейс программы представлен ниже.

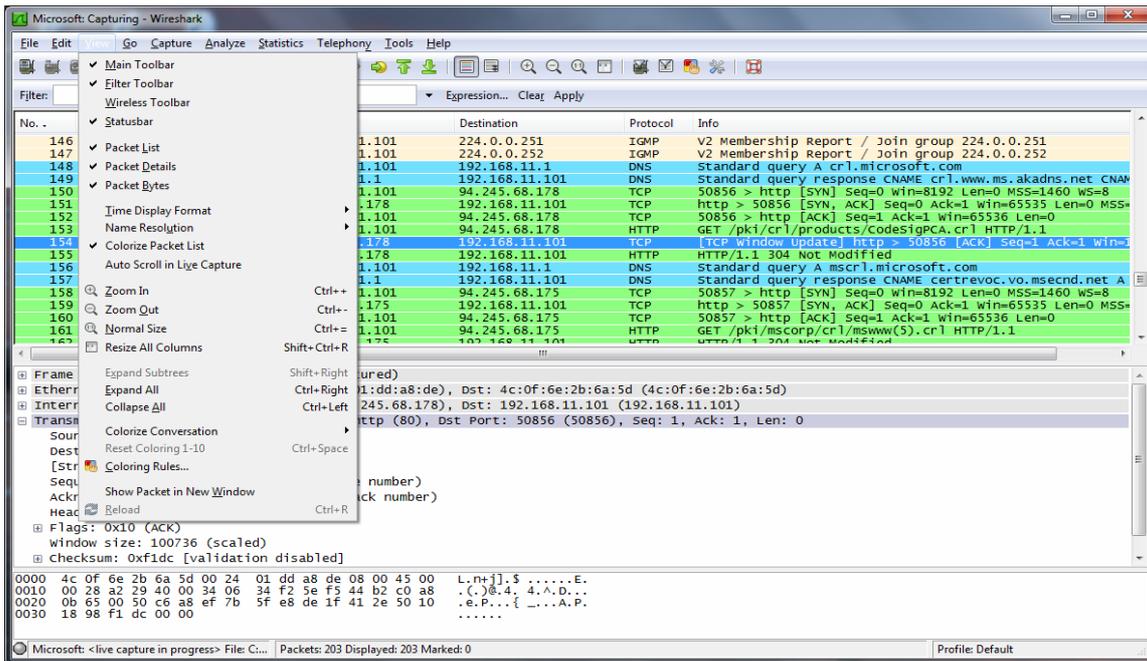


Рисунок 15. 1 Интерфейс программы Wireshark

Чтобы начать перехват трафика нужно выбрать правильный сетевой интерфейс. Чтобы выбрать сетевой адаптер, с которого будет выполняться перехват, необходимо нажать на кнопку **Interfaces** на тулбаре, либо меню **Capture > Interfaces**:

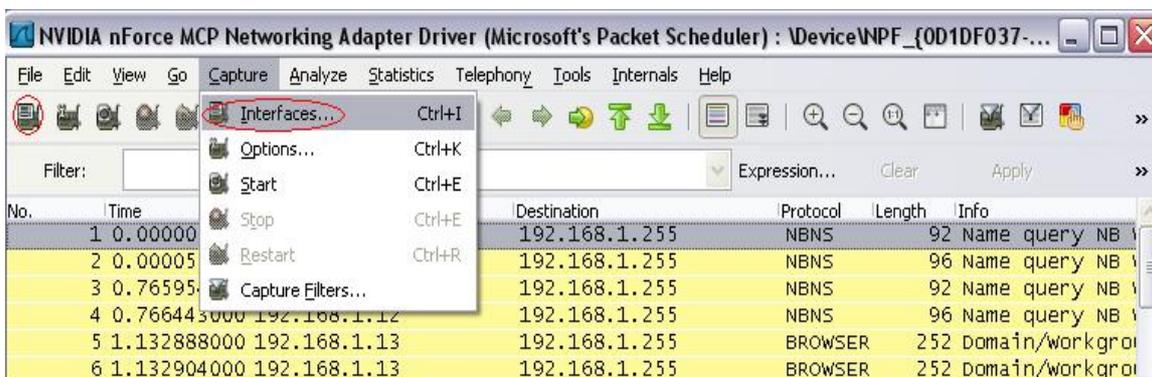


Рисунок 15. 2 Выбор интерфейса для перехвата трафика

После нажатия одной из этих кнопок появится окно со списком сетевых интерфейсов, доступных системе:



Рисунок 15. 3 Список сетевых интерфейсов

После нажатия кнопки **Start** начнется захват трафика.

ЗАДАНИЕ

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Выполните тестирование соединения между ПК2 и ПК3 и наоборот командой ping.

Наблюдаете ли вы трафик, передаваемый портами коммутатора? Какой еще трафик вы наблюдаете? _____

Отключите функцию зеркалирования портов:
`disable mirror`

Проверьте настройки функции:
`show mirror`

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Выполните тестирование соединения между ПК 2 и ПК 3 и наоборот командой ping.

Что вы наблюдаете теперь? Сравните с предыдущими результатами?

Лабораторная работа №16. Настройка протокола управления топологией сети LLDP

Согласованная работа различных узлов в локальной сети (LAN) требует корректной конфигурации протоколов и приложений, которые выполняются и поддерживаются ими. По мере того как число различных типов устройств в сети растет, сетевым администраторам все труднее становится отслеживать правильность конфигурации каждого из них, одновременно все большее количество времени затрачивается на то, чтобы обнаружить и устранить проблемы. Стандарт 802.1ab, или Link Layer Discovery Protocol (LLDP), обеспечивает решение проблем конфигурации, вызванных расширением LAN.

Link Layer Discovery Protocol (LLDP) – протокол канального уровня, позволяющий сетевому оборудованию (коммутаторам, маршрутизаторам, IP-телефонам, беспроводным точкам доступа, узлам и т.д.) оповещать локальную сеть о своем существовании и характеристиках, а также собирать такие же оповещения, поступающие от соседнего оборудования. Информация, собранная посредством LLDP накапливается в устройствах, и может быть запрошена с помощью протокола SNMP. Таким образом, топология сети, в которой используется LLDP, может быть получена с управляющего компьютера, посредством последовательного опроса каждого устройства, на предмет собранной им информации. При этом получаемая информация содержит следующие параметры:

- Имя устройства (System Name);
- Описание устройства (System Description);
- Идентификатор порта (Port ID);
- Описание порта (Port Description);
- Возможности устройства (System Capabilities);
- Управляющий адрес (Management Address) и т.д.

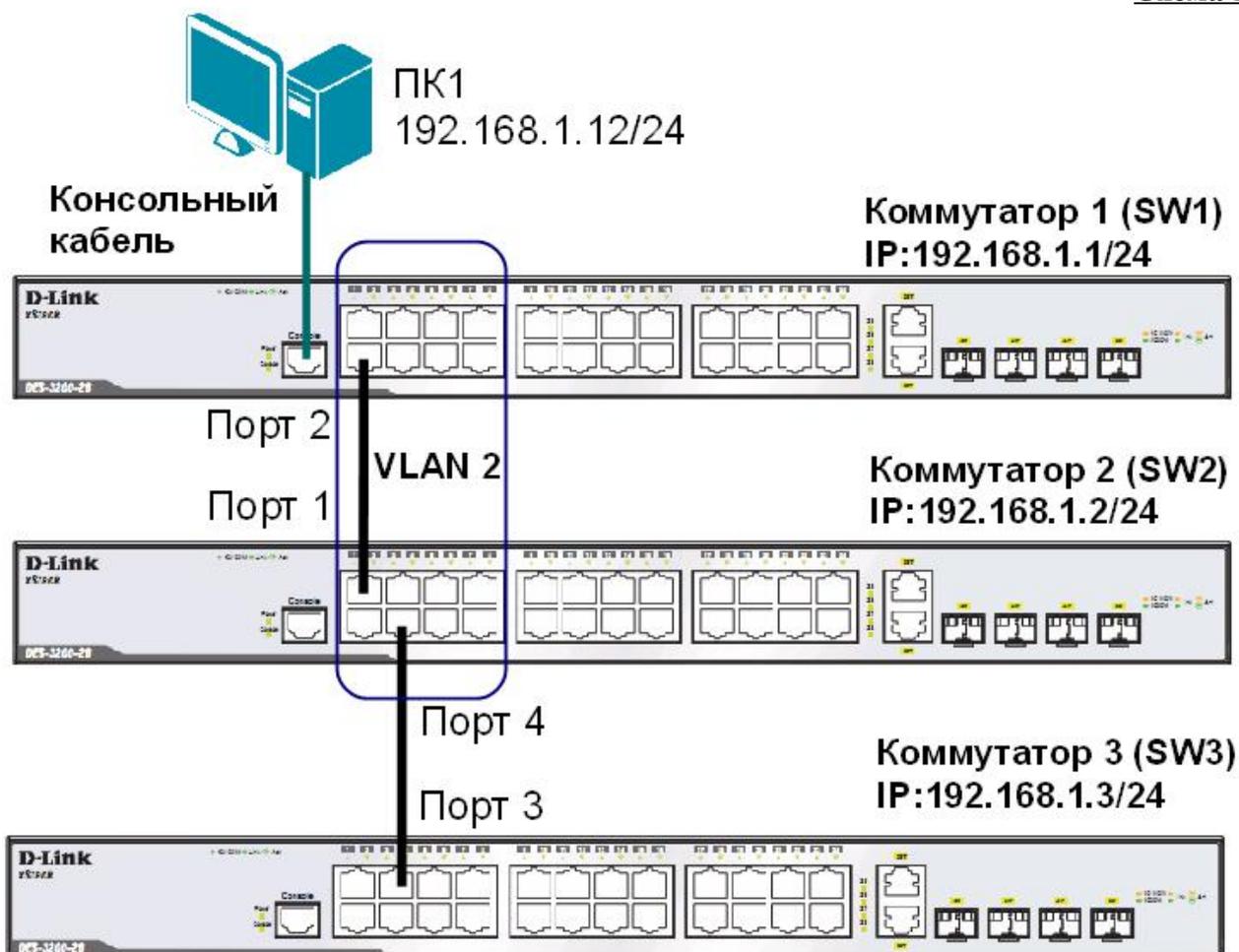
Протокол LLDP передает информацию в сообщениях, которые называются *LLDP Data Unit (LLDPDU)*. Протоколом предусматривается передача данных только в одном направлении, то есть LLDP-устройства не обмениваются информацией в режиме запрос-ответ, а так же не подтверждают ее получения.

Таким образом, сам по себе LLDP не управляет трафиком – он только распространяет информацию, относящуюся к конфигурации на канальном уровне. Данный протокол, поддерживается всеми основными производителями активного сетевого оборудования. Используя эту информацию, и опрашивая MIB базы данных обнаруженных устройств, системы управления могут динамически моделировать и отслеживать состояния локальных сетей передачи данных, а также строить их визуальные схемы для пользователей и администраторов.

Цель: понять функционирование протокола LLDP и изучить его настройку на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-28	3 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.



Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора 1 (SW1)

Настройте IP-адрес коммутатора:

```
config ipif System ipaddress 192.168.1.1/24
```

Настройте имя коммутатора:

```
config snmp system_name SW1
```

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-9
```

Создайте VLAN v2, добавьте в соответствующий VLAN порты, которые необходимо настроить немаркированными.

```
create vlan v2 tag 2
config vlan v2 add untagged 1-9
```

Проверьте настройки VLAN:

```
show vlan
```

Включите работу протокола LLDP глобально на коммутаторе:

```
enable lldp
```

Проверьте информацию о настройках LLDP:

```
show lldp
```

Включите продвижение пакетов LLDP:

```
config lldp forward_message enable
```

Настройте интервал передачи информационных пакетов LLDP:

```
config lldp message_tx_interval 20
```

Примечание: с помощью данной команды можно регулировать частоту отправки LLDP-сообщений соседним устройствам с активных портов коммутатора. По умолчанию интервал 30 секунд.

Настройте время переинициализации LLDP:

```
config lldp reinit_delay 3
```

Примечание: данная команда позволяет установить интервал времени ожидания, после которого повторно активизированные LLDP-порты начнут передачу пакетов LLDP. По умолчанию 2 секунды.

Проверьте информацию о настройках LLDP:

```
show lldp
```

Что вы наблюдаете? Запишите _____

Настройте на всех портах возможность приема и передачи LLDP пакетов:

```
config lldp ports all admin_status tx_and_rx
```

Включите передачу в оповещениях LLDP информации об IP-адресе управления коммутатора:

```
config lldp ports all mgt_addr ipv4 192.168.1.1 enable
```

Включите передачу в оповещениях основных информационных данных протокола LLDP:

```
config lldp ports all basic_tlvs all enable
```

Включите передачу в оповещениях LLDP информации о 802.1Q (VLAN):

```
config lldp ports all dot1_tlv_vlan_name vlan all enable
```

Проверьте настройку оповещений на портах:

```
show lldp ports 1-24
```

Что вы наблюдаете? Запишите _____

Повторите процедуру настройки для коммутатора 2 и коммутатора 3

На коммутаторе 2 (SW2):

Проверьте полную информацию о портах, используемых для отправки оповещений LLDP:

```
show lldp local_ports 1-24 mode detailed
```

Проверьте расширенную информацию о соседних устройствах:

```
show lldp remote_ports 1-24 mode detailed
```

Что вы наблюдаете? Запишите _____

Отключите кабель, соединяющий коммутатор 1 и коммутатор 2.

Проверьте расширенную информацию о соседних устройствах:

```
show lldp remote_ports 1-24 mode detailed
```

Что вы наблюдаете? Что изменилось? Запишите _____

Отключите протокол LLDP глобально на коммутаторе:

```
disable lldp
```

Проверьте информацию о настройках LLDP:

```
show lldp
```

Лабораторная работа №17. Итоговая самостоятельная работа

В предыдущих лабораторных работах была рассмотрена настройка и функционирование основных сетевых протоколов и функций, используемых в большинстве современных сетей. Данная лабораторная работа предполагает самостоятельное создание учебной сети, имитирующей локальную сеть реального предприятия и обеспечивающей решение широкого круга задач.

При выполнении работы, в учебной сети должен быть настроен один маршрутизирующий коммутатор.

Цель: самостоятельно разработать конфигурацию сложной сети. Собрать схему, настроить и исследовать совместное использование различных протоколов и функций.

Оборудование (на 10 рабочих мест):

Коммутатор DES-3200-28	8 шт.
Коммутатор DES-3810-28	1 шт.
Рабочая станция	10 шт.
Консольный кабель	10 шт.
Кабель Ethernet	31 шт.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

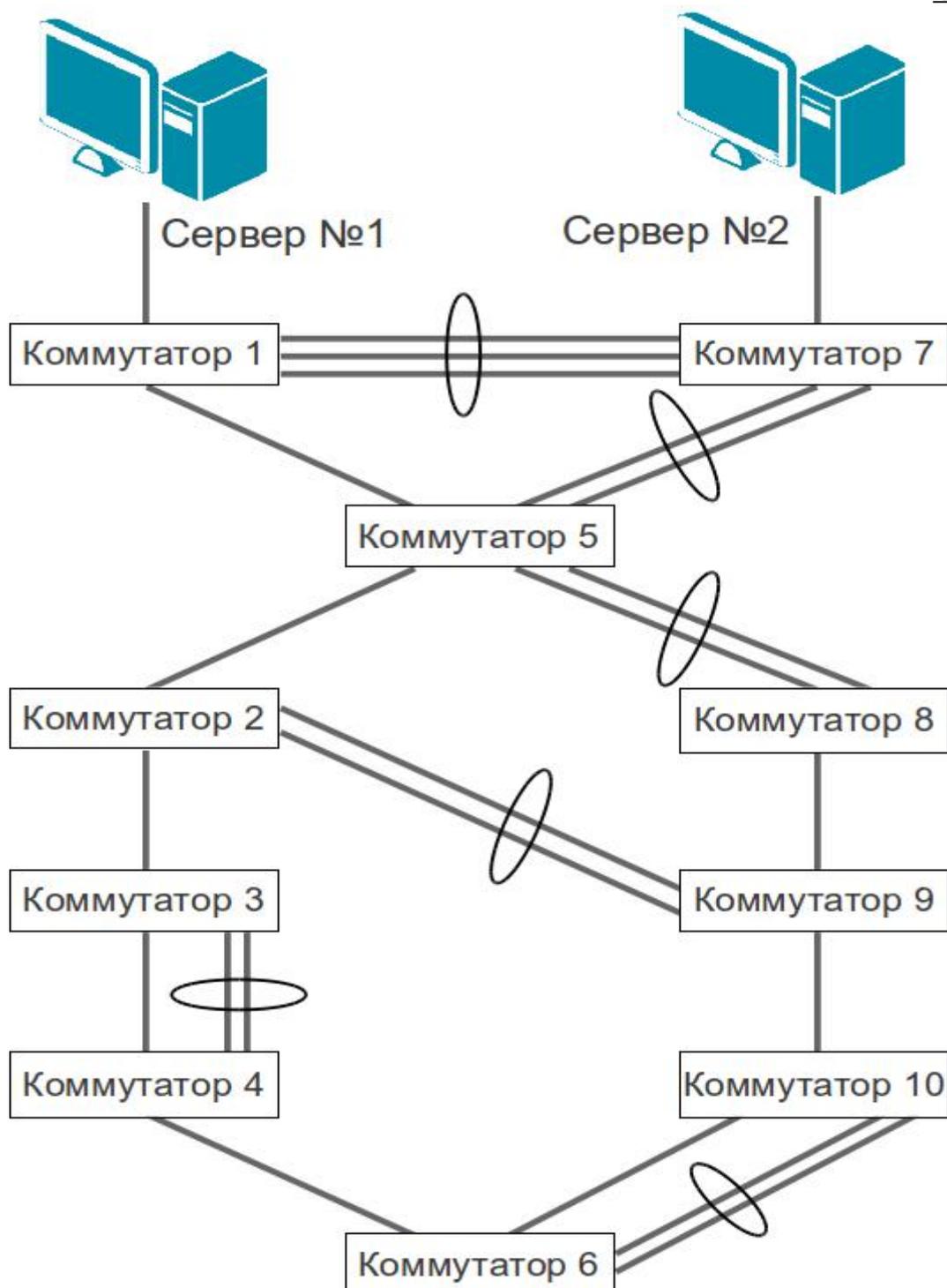
```
reset config
```

17.1 Подготовительная работа

В работе будут использованы следующие протоколы и функции:

- ◆ VLAN;
- ◆ маршрутизация между VLAN;
- ◆ LACP;
- ◆ RSTP;
- ◆ 802.1p;
- ◆ ACL;
- ◆ LBD;
- ◆ Safeguard Engine.

Прежде чем начать строительство сети, необходимо провести небольшое проектирование.



Модели коммутаторов умышленно не обозначены на схеме. Местоположение каждого коммутатора из используемых для выполнения работы необходимо определить самостоятельно. В роли серверов можно использовать две любые рабочие станции, например, ПК1 и ПК2.

Для повышения отказоустойчивости в топологии сети заложены избыточные каналы связи. Предполагается создание агрегированных каналов связи.

К каждому коммутатору необходимо подключить один ПК (порт подключения выбирается самостоятельно). Каждый применяемый в схеме ПК должен быть размещён в своём индивидуальном VLAN.

Устройства во всех VLAN должны иметь возможность обмениваться данными через маршрутизирующий коммутатор. Необходимо обеспечить приоритизацию входящих и исходящих пакетов на серверах №1 и №2.

Необходимо заблокировать любой трафик между ПК3-ПК6 и сервером №1, между ПК7-ПК10 и сервером №2.

В процессе проектирования и настройки сети предполагается совместная работа всех рабочих групп с целью согласования значений сетевых параметров, требуемых для организации связи между соседними коммутаторами. Укажите согласованные параметры на схеме сети.

Для дальнейшей работы необходимо:

1. Распределить имеющиеся коммутаторы по схеме так, чтобы получить сеть с максимальной пропускной способностью.
2. Выбрать номера портов коммутаторов для соединения друг с другом.
3. Выбрать номера портов коммутаторов для подключения ПК.
4. Определить очередность настройки протоколов и функций, очередность построения схемы.
5. Определить, какие порты, в каких VLAN должны быть настроены.
6. Разработать план IP-адресации для всех VLAN, выбрать адреса для IP-интерфейсов маршрутизирующего коммутатора.
7. Выбрать в качестве корневого моста для протокола RSTP такой коммутатор, который обеспечит построение топологии с максимальной производительностью сети.
8. Определить порты, на которых необходимо настроить приоритизацию.
9. Разработать ACL.
10. Выбрать порты, на которых будет включена функция LBD.
11. Определить пороговые значения для функции Safeguard Engine.

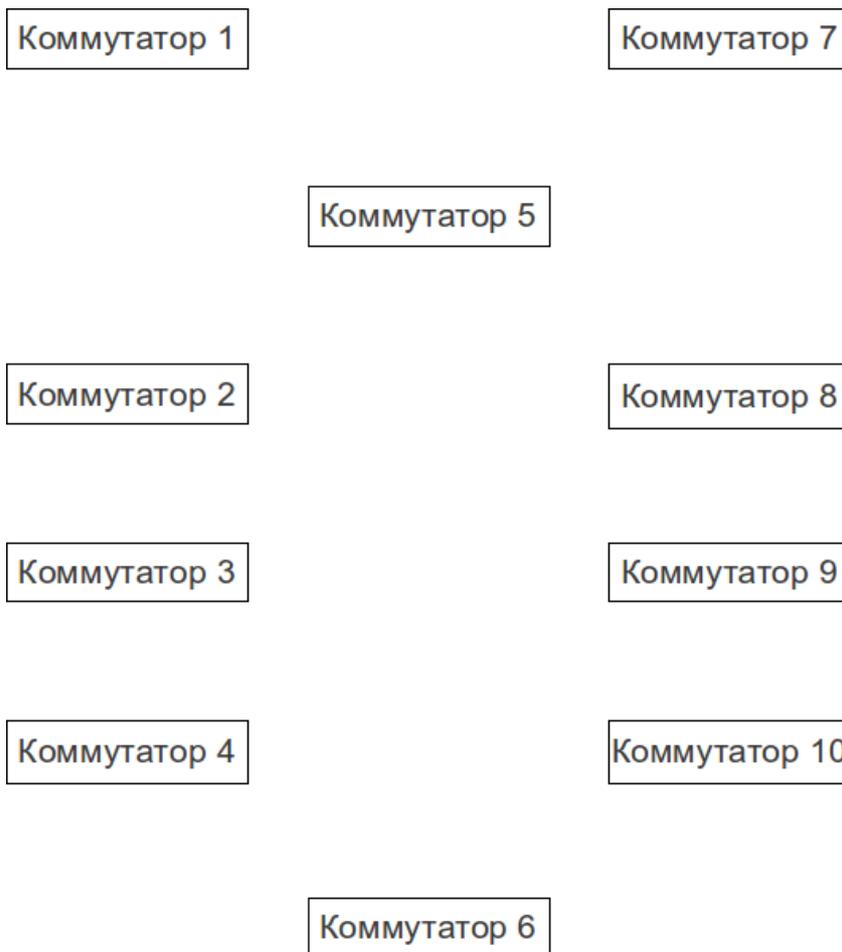
17.2 Выполнение работы

Ввиду сложности и объёмности работы, а так же зависимости результатов одной отдельной группы от результатов работы всех остальных групп, рекомендуется разделить лабораторную работу на этапы, согласовать очерёдность их выполнения и проведения промежуточных тестов. Это позволит своевременно обнаружить ошибки в проекте сети и выполненных конфигурациях.

17.3. Ожидаемый результат

1. Связь между всеми ПК и серверами должна быть только через маршрутизирующий коммутатор.
2. В созданной сети не должно быть активных коммутационных петель.
3. Любые коммутационные петли, появляющиеся в сети, должны автоматически блокироваться.
4. Корневой мост в RSTP должен быть назначен так, чтобы активная топология обеспечивала максимальную производительность сети.
5. Должны быть активизированы функции безопасности протокола RSTP и защиты от образования петель.
6. Настроенная приоритизация должна обеспечивать беспрепятственное прохождение определенных видов трафика через любые сетевые интерфейсы.
7. Запрещённый трафик не должен достигать получателей.

Зарисуйте получившуюся топологию RSTP, указав на ней корневой мост, все активные интерфейсы и их скорости:



Какой командой (командами) можно проверить, что данные между ПК и серверами передаются именно через маршрутизатор?

На каких устройствах, и какими командами можно проверить, что данные между ПК и серверами передаются именно через маршрутизирующий коммутатор?

Проверьте, блокируется ли запрещённый для передачи трафик. Как можно проверить, на каком именно коммутаторе происходит блокировка?

РАСШИРЕННЫЙ НАБОР

Лабораторная работа №18. Настройка функции Q-in-Q (Double VLAN)

Функция Q-in-Q, также известная как Double VLAN, соответствует стандарту IEEE 802.1ad, который является расширением стандарта IEEE 802.1Q. Она позволяет добавлять в маркированные кадры Ethernet второй тег IEEE 802.1Q.

Инкапсуляция кадра Ethernet вторым тегом происходит следующим образом: тег, содержащий идентификатор VLAN сети провайдера SP-VLAN ID (*внешний тег*) вставляется перед *внутренним тегом*, содержащим клиентский идентификатор VLAN – CVLAN ID. Передача кадров в сети провайдера осуществляется только на основе внешнего тега SP-VLAN ID, внутренний тег пользовательской сети CVLAN ID при этом скрыт.

Существует две реализации функции Q-in-Q: *Port-based Q-in-Q* и *Selective Q-in-Q*. Функция *Port-based Q-in-Q* по умолчанию присваивает любому кадру, поступившему на порт доступа граничного коммутатора провайдера идентификатор *SP-VLAN* равный идентификатору PVID порта. Порт маркирует кадр независимо от того, является он маркированным или немаркированным. При поступлении маркированного кадра в него добавляется второй тег с идентификатором равным *SP-VLAN*. Если на порт пришёл немаркированный кадр, в него добавляется только тег с *SP-VLAN* порта.

Роли портов в Port-based Q-in-Q

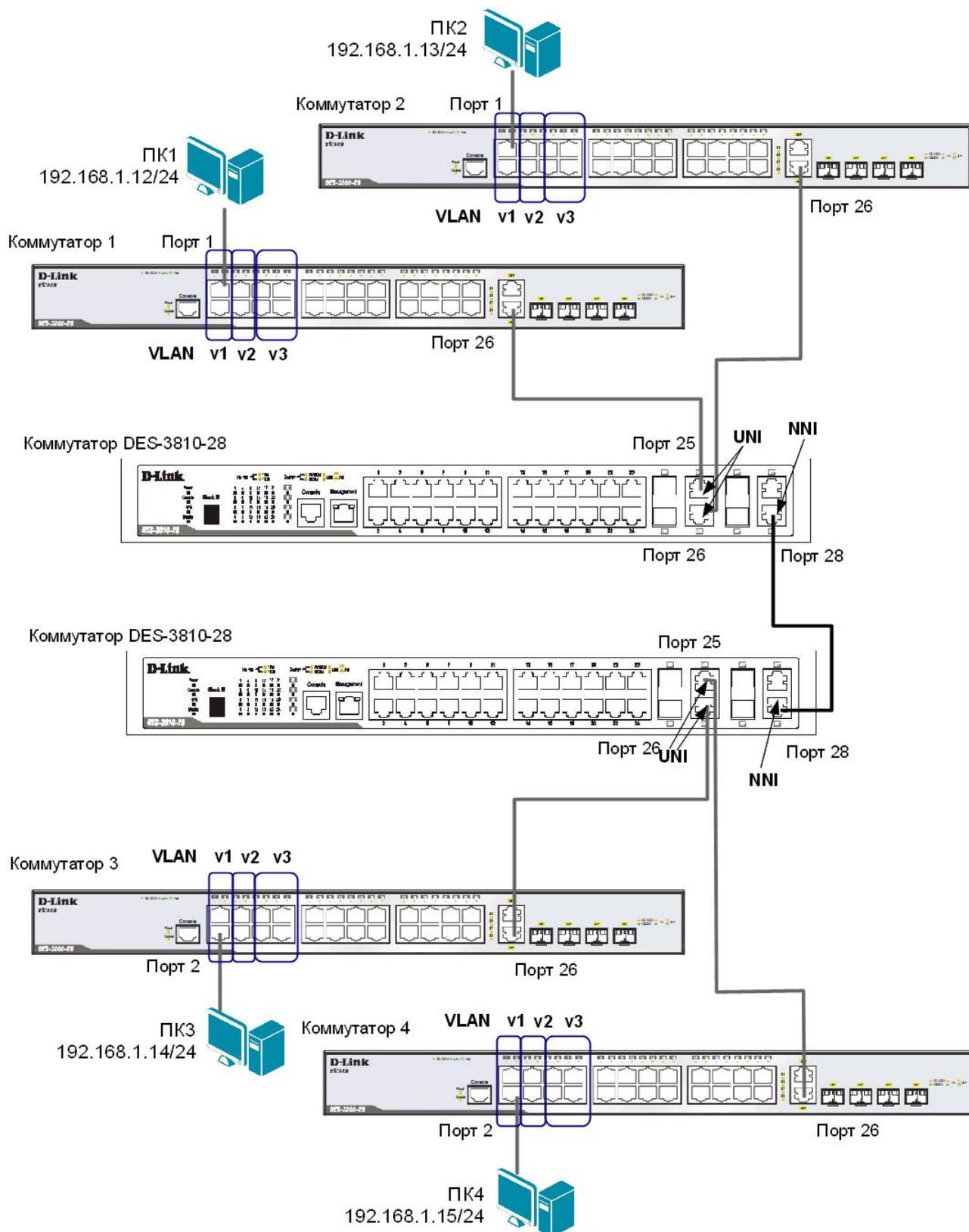
Все порты граничного коммутатора, на котором используется функция Port-based Q-in-Q, должны быть настроены как порты доступа (UNI) или Uplink-порты (NNI):

- UNI (User-to-Network Interface) – эта роль назначается портам, через которые будет осуществляться взаимодействие граничного коммутатора провайдера с клиентскими сетями.
- NNI (Network-to-Network Interface) – эта роль назначается портам, которые подключаются к внутренней сети провайдера или другим граничным коммутаторам.

Цель: изучить настройку функции Port-based Q-in-Q.

Оборудование (на 6 рабочих мест):

Коммутатор DES-3200-28	4 шт.
Коммутатор DES-3810-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	6 шт.
Кабель Ethernet	9 шт.



Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:
 reset config

Настройка коммутаторов 1, 2, 3, 4

Удалите все порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте VLAN v2, v3 и v4, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порты 26 маркированными:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-2
config vlan v2 add tagged 26
create vlan v3 tag 3
config vlan v3 add untagged 3-4
config vlan v3 add tagged 26
create vlan v4 tag 4
config vlan v4 add untagged 5-8
config vlan v4 add tagged 26
```

Проверьте настройки VLAN:

```
show vlan
```

Настройка коммутаторов DES-3810-28

Включите функцию Q-in-Q VLAN:

```
enable qinq
```

Удалите порты из Q-in-Q VLAN по умолчанию:

```
config vlan default delete 25-26
```

Создайте Q-in-Q VLAN с SP-VLAN ID равным d100 для первого клиента:

```
create vlan d100 tag 100
```

Создайте Q-in-Q VLAN с SP-VLAN ID равным d200 для второго клиента:

```
create vlan d200 tag 200
```

Настройте порты доступа в Q-in-Q VLAN d100:

```
config vlan d100 add untagged 25
```

Настройте порты доступа в Q-in-Q VLAN d200:

```
config vlan d200 add untagged 26
```

Настройте порт 28 как Uplink-порт в Q-in-Q VLAN d100 и d200:

```
config vlan d100 add tagged 28
config vlan d200 add tagged 28
```

Настроить роли портов доступа в Q-in-Q и отключить режим Missdrop на них.

```
config qinq ports 25-26 role uni missdrop disable
```

Проверьте настройку функции Q-in-Q VLAN:

```
show qinq ports
```

Запишите ваши наблюдения:

Проверьте доступность соединения между рабочими станциями командой ping:

ping <IP-address>

- от ПК1 к ПК 3 _____
- от ПК1 к ПК 2 _____
- от ПК3 к ПК4 _____
- от ПК2 к ПК4 _____

Проверьте таблицу ARP каждого компьютера и удостоверьтесь, что связь осуществляется в соответствии со схемой:

arp -a

Лабораторная работа №19. Настройка статической и динамической маршрутизации IPv4

Маршрутизация позволяет локальным сетям объединяться вместе, образуя огромные составные сети. Маршрутизация выполняется специальными устройствами, называемыми маршрутизаторами (коммутаторами 3 уровня), которые перенаправляют пакеты от сети к сети, позволяя устройству отправлять данные другому устройству, даже в том случае, если оно не имеет понятие, где находится пункт назначения.

Кратко маршрутизацию можно описать так — маршрутизаторы (коммутаторы 3 уровня) принимают решение о том, куда передавать пакет на основе его сетевого адреса назначения, который сравнивается с информацией, хранимой в специальных **таблицах маршрутизации**. Таблица маршрутизации содержит записи, представляющие собой список наилучших доступных маршрутов к соответствующим сетям. В том случае, если к пункту назначения имеется несколько маршрутов, в таблицу маршрутизации будет помещен маршрут, имеющий лучшие параметры, определяемые на основании загрузки, полосы пропускания, задержки, стоимости или надежности какого-либо канала связи.

Существуют 4 типа записей таблицы маршрутизации:

- *Статический маршрут (Static Route)* – задается вручную системным администратором.
- *Динамический маршрут (Dynamic Route)* – динамически создается в процессе обмена маршрутизаторами маршрутной информацией.
- *Маршрут по умолчанию (Default Route)* - задается вручную системным администратором в качестве пути, который используется, в том случае, если другой маршрут к пункту назначения неизвестен.
- *Локальный маршрут (Local Route)* – адреса непосредственно подключенных к интерфейсам маршрутизатора локальных сетей, задаются в процессе конфигурирования устройства.

Новые маршруты могут добавляться в таблицу маршрутизации с помощью:

- *статической маршрутизации*: записи о маршрутах вносятся и изменяются в таблицах маршрутизации вручную.
- *динамической маршрутизации*: записи о маршрутах заносятся и обновляются в таблицах с помощью *протоколов маршрутизации (например, RIP, OSPF)*.

Протокол RIP (Routing Information Protocol) является самым популярным протоколом маршрутизации стека протоколов TCP/IP. Он достаточно прост в понимании и настройке и поэтому наиболее распространен в небольших однородных сетях, т.е. имеющих одинаковые характеристики каналов связи.

В настоящее время существует 3 версии протокола RIP:

RIP version 1 (RIPv1) для протокола IPv4;

RIP version 2 (RIPv2) для поддержки бесклассовой адресации протокола IPv4;

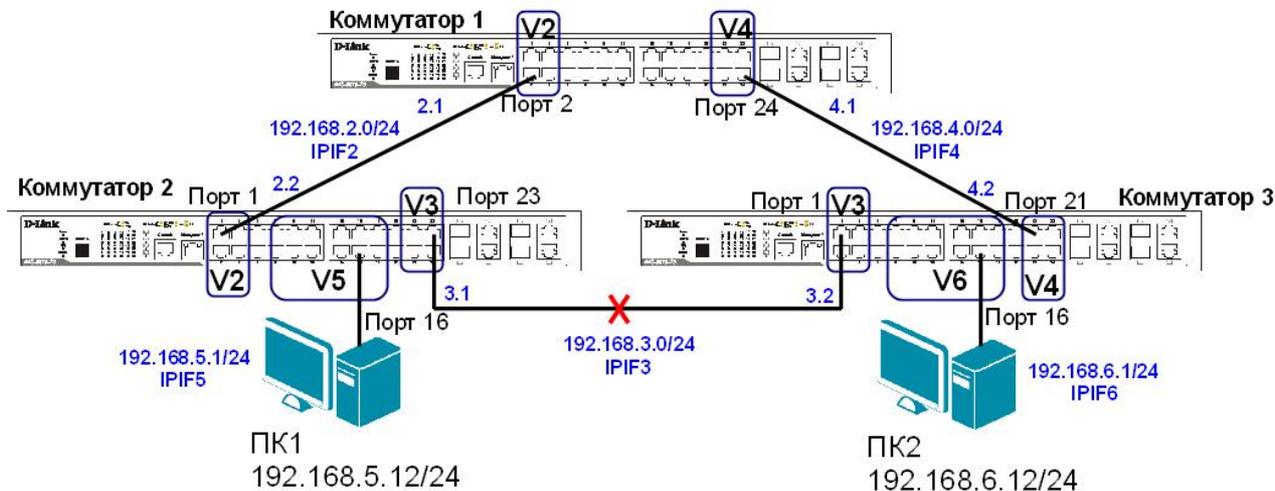
RIPng (next generation) для протокола IPv6.

Цель: изучить настройку статической и динамической маршрутизации на коммутаторах D-Link.

Оборудование (на 6 рабочих мест):

Коммутатор DES-3810-28	3 шт.
Рабочая станция	2 шт.
Консольный кабель	3 шт.
Кабель Ethernet	5 шт.

Схема 19



ЗАДАНИЕ 1

Настроить статическую маршрутизацию между VLAN V5 и VLAN V6.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Примечание: не соединяйте коммутаторы одновременно несколькими кабелями во время настройки до особого указания.

Настройка коммутатора 1

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
`config vlan default delete 1-24`

Создайте VLAN v2 и v4, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2  
config vlan v2 add tagged 1-4
```

```
create vlan v4 tag 4  
config vlan v4 add tagged 21-24
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте IP-интерфейс для VLAN v2 и v4 с именами IPIF2 и IPIF4 соответственно:

```
create ipif IPIF2 192.168.2.1/24 v2 state enable  
create ipif IPIF4 192.168.4.1/24 v4 state enable
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Настройка коммутатора 2

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте VLAN v2, v3 и v5 добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2  
config vlan v2 add tagged 1-4
```

```
create vlan v3 tag 3  
config vlan v3 add tagged 21-24
```

```
create vlan v5 tag 5  
config vlan v5 add untagged 7-18
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте IP-интерфейс для VLAN v2, v3 и v5 с именами IPIF2, IPIF3 и IPIF5 соответственно:

```
create ipif IPIF2 192.168.2.2/24 v2 state enable  
create ipif IPIF3 192.168.3.1/24 v3 state enable  
create ipif IPIF5 192.168.5.1/24 v5 state enable
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Настройка коммутатора 3

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте VLAN v3, v4 и v6 добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v3 tag 3  
config vlan v3 add tagged 1-4
```

```
create vlan v4 tag 4  
config vlan v4 add tagged 21-24
```

```
create vlan v6 tag 6  
config vlan v6 add untagged 7-18
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте IP-интерфейс для VLAN v3, v4 и v6 с именами IPIF3, IPIF4 и IPIF6 соответственно:

```
create ipif IPIF3 192.168.3.2/24 v3 state enable
create ipif IPIF4 192.168.4.2/24 v4 state enable
create ipif IPIF6 192.168.6.1/24 v6 state enable
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Соедините между собой коммутаторы 1, 2 и 3 с помощью Ethernet-кабелей, как показано на схеме 19.

Задайте рабочим станциям ПК1 и ПК2 IP-адреса в соответствии со схемой 19. В качестве шлюза по умолчанию (default gateway) укажите адрес IP-интерфейса маршрутизирующего коммутатора соответствующей VLAN.

Проверьте соединение между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК2 _____

- от ПК2 к ПК1 _____

Должна ли быть связь между всеми ПК? Объясните _____

Настройка коммутатора 1

Проверьте таблицу маршрутизации:

```
show iproute
```

Сколько записей в таблице маршрутизации вы наблюдаете? Запишите _____

Создайте статический маршрут к сети 192.168.5.0/24:

```
create iproute 192.168.5.0/24 192.168.2.2
```

Примечание: команда означает, что сеть 192.168.5.0/24 доступна через интерфейс 192.168.2.2 коммутатора 2.

Создайте статический маршрут к сети 192.168.6.0/24:

```
create iproute 192.168.6.0/24 192.168.4.2
```

Создайте статический маршрут к сети 192.168.3.0/24:

```
create iproute 192.168.3.0/24 192.168.2.2
```

Проверьте таблицу маршрутизации:

```
show iproute
```

Сколько записей в таблице маршрутизации вы наблюдаете? Сравните с предыдущими результатами _____

Настройка коммутатора 2

Проверьте таблицу маршрутизации:

```
show iproute
```

Сколько записей в таблице маршрутизации вы наблюдаете? Запишите _____

Создайте статический маршрут к сети 192.168.6.0/24:

```
create iproute 192.168.6.0/24 192.168.3.2
```

Создайте статический маршрут к сети 192.168.4.0/24:

```
create iproute 192.168.4.0/24 192.168.3.2
```

Проверьте таблицу маршрутизации:

```
show iproute
```

Сколько записей в таблице маршрутизации вы наблюдаете? Сравните с предыдущими результатами _____

Настройка коммутатора 3

Проверьте таблицу маршрутизации:

```
show iproute
```

Сколько записей в таблице маршрутизации вы наблюдаете? Запишите _____

Создайте статический маршрут к сети 192.168.2.0/24:

```
create iproute 192.168.2.0/24 192.168.4.1
```

Создайте статический маршрут к сети 192.168.5.0/24:

```
create iproute 192.168.5.0/24 192.168.3.1
```

Проверьте таблицу маршрутизации:

```
show iproute
```

Сколько записей в таблице маршрутизации вы наблюдаете? Сравните с предыдущими результатами _____

Проверьте соединение между рабочими станциями командой ping:

```
ping <IP-address>
```

- от ПК1 к ПК2 _____

- от ПК2 к ПК1 _____

Проверьте маршрут от ПК1 к ПК2 командой tracert. В командной строке ПК1 введите:

```
tracert 192.168.6.12
```

Какое количество переходов вы наблюдаете? _____

Проверьте маршрут от ПК2 к ПК1 командой tracer. В командной строке ПК2 введите:
tracert 192.168.5.12

Какое количество переходов вы наблюдаете? _____

Настройка коммутатора 1

Удалите статический маршрут:

```
delete iproute 192.168.5.0/24 192.168.2.2  
delete iproute 192.168.6.0/24 192.168.4.2  
delete iproute 192.168.3.0/24 192.168.2.2
```

Настройка коммутатора 2

Удалите статический маршрут:

```
delete iproute 192.168.6.0/24 192.168.3.2  
delete iproute 192.168.4.0/24 192.168.3.2
```

Настройка коммутатора 3

Удалите статический маршрут:

```
delete iproute 192.168.2.0/24 192.168.4.1  
delete iproute 192.168.5.0/24 192.168.3.1
```

ЗАДАНИЕ 2

Настроить маршрут по умолчанию в VLAN V5 и VLAN V6

Настройка коммутатора 1

Создайте маршрут по умолчанию:

```
create iproute default 192.168.4.2
```

Примечание: маршрут по умолчанию используется в том случае, если другой маршрут к сети назначения неизвестен.

Проверьте таблицу маршрутизации:

```
show iproute
```

Что вы наблюдаете? Запишите _____

Настройка коммутатора 2

Создайте маршрут по умолчанию:

```
create iproute default 192.168.2.1
```

Настройка коммутатора 3

Создайте маршрут по умолчанию:

```
create iproute default 192.168.3.1
```

Проверьте соединение между рабочими станциями командой ping:
ping <IP-address>

- от ПК1 к ПК2 _____
- от ПК2 к ПК1 _____

Проверьте маршрут от ПК1 к ПК2 командой tracert. В командной строке ПК1 введите:
tracert 192.168.6.12

Какое количество переходов вы наблюдаете? _____

Проверьте маршрут от ПК2 к ПК1 командой tracert. В командной строке ПК2 введите:
tracert 192.168.5.12

Какое количество переходов вы наблюдаете? _____

Настройка коммутатора 1

Удалите статический маршрут по умолчанию:
delete iproute default 192.168.4.2

Настройка коммутатора 2

Удалите статический маршрут по умолчанию:
delete iproute default 192.168.2.1

Настройка коммутатора 3

Удалите статический маршрут по умолчанию:
delete iproute default 192.168.3.1

ЗАДАНИЕ 3

Настроить протокол динамической маршрутизации RIP v2.

Настройка коммутатора 1

Включите работу протокола RIP глобально на коммутаторе:
enable rip

Настройте параметры протокола RIP для всех интерфейсов:
config rip all tx_mode v2_only rx_mode v2_only state enable

Повторите процедуру настройки для коммутатора 2 и коммутатора 3

Проверьте таблицу маршрутизации:
show iproute

Сколько записей в таблице маршрутизации вы наблюдаете? Запишите _____

Проверьте версию и статус протокола RIP:
show rip

Сколько записей вы наблюдаете? _____

Проверьте соединение между рабочими станциями командой ping:
ping <IP-address>

- от ПК1 к ПК2 _____
- от ПК2 к ПК1 _____

Проверьте маршрут от ПК1 к ПК2 командой tracert. В командной строке ПК1 введите:
tracert 192.168.6.12

Какое количество переходов вы наблюдаете? _____

Проверьте маршрут от ПК2 к ПК1 командой tracert. В командной строке ПК2 введите:
tracert 192.168.5.12

Какое количество переходов вы наблюдаете? _____

Отключите кабель Ethernet, соединяющий коммутатор 2 и коммутатор 3 (схема 19).

Проверьте таблицу маршрутизации:
show iproute

Сколько записей в таблице маршрутизации вы наблюдаете? Сравните с предыдущими результатами. Что изменилось? _____

Выключите работу протокола RIP глобально на коммутаторе:
disable rip

Лабораторная работа №20. Установка и настройка протокола IPv6 на рабочей станции и коммутаторе D-Link

Протокол IPv6 — новая версия протокола IP, которая разработана в качестве преемника IPv4 и призвана решить проблему исчерпания адресного пространства. Основным отличием IPv6 от IPv4 является:

- большое адресное пространство (2^{128} адресов);
- улучшенные механизмы по автоматической настройке узлов;
- упрощение маршрутизации;
- улучшенные механизмы обеспечения качества обслуживания (QoS);
- упрощенный заголовок пакета.

Адрес IPv6 имеет длину 128 бит и состоит из *префикса* и *идентификатора*. Отображается адрес как восемь групп по четыре шестнадцатеричные цифры, разделенные двоеточием. Например: ABCD:EF01:2345:6789:ABCD:EF01:2345:6789.

Префикс (64 бита) - это часть адреса, которая указывает количество фиксированных бит, отведенных под идентификатор сети/подсети (аналог адреса сети в IPv4).

Идентификатор (64 бита) - последние 64 бита адреса IPv6, используемые для идентификации интерфейса в сегменте сети (аналог адреса узла в IPv4), он должен быть уникальным внутри сети/подсети.

Идентификатор интерфейса может быть получен следующими способами:

- сформирован из 48-битного MAC-адреса путем конвертации в формат Modified EUI-64;
 - сгенерирован автоматически случайным образом;
 - настроен вручную;
 - назначен с помощью протокола DHCP.
- Существует три типа адресов IPv6:
- индивидуальный (unicast);
 - групповой (multicast);
 - альтернативный (anycast).

Индивидуальные адреса служат для идентификации одного интерфейса и разделяются на несколько видов:

- *Link-Local Unicast* - предназначены для коммуникаций в пределах одного сегмента сети или линии связи «точка-точка» и имеют значение только в пределах данной линии связи. Все адреса Link-Local начинаются с префикса FE80::/10;
- *Unique-Local Unicast* - предназначены для адресации внутри сети организации. Пакеты с адресами Unique-Local в качестве адреса источника или назначения не маршрутизируются через Интернет, они маршрутизируются только внутри сети организации (аналог частных адресов IPv4). Все адреса Unique-Local начинаются с префикса FC00::/7. Алгоритм для генерации уникального локального адреса можно найти в сети интернет <https://www.ultratools.com/tools/rangeGenerator>;
- *Global Unicast* — эти адреса выдаются локальными регистраторами и используются для идентификации узлов в глобальной сети (аналог глобальных адресов IPv4). В настоящее время назначаются адреса из диапазона 2000::/3.

В отличие от IPv4, где настройка параметров узла проводилась либо вручную, либо с помощью протокола DHCP, в IPv6 узел может практически самостоятельно сконфигурировать параметры своих интерфейсов. В IPv6 определены два механизма автоконфигурации:

- *Stateless autoconfiguration* - позволяет узлам генерировать свой собственный адрес на основе комбинации локально доступной информации и информации, объявляемой маршрутизаторами. Маршрутизаторы объявляют префиксы, идентифицирующие подсеть(и), а узлы генерируют идентификаторы интерфейсов. В отсутствие

маршрутизатора узлы могут автоматически генерировать канальный IPv6-адрес (Link-Local Unicast);

- *Stateful autoconfiguration* - узлы получают адрес интерфейса и/или конфигурационную информацию и параметры от сервера с помощью протокола DHCPv6.

Stateless и stateful autoconfiguration дополняют друг друга. Они могут использоваться одновременно.

Ручная настройка для конфигурации интерфейсов узлов может использоваться:

- в сети нет маршрутизаторов, которые рассылают объявления с информацией, требуемой для автоматической конфигурации;
- в случае обнаружения дублирования адресов при автоматической конфигурации узлов.

Цель: изучить настройку протокола IPv6 на рабочей станции и на коммутаторе D-Link.

Оборудование (на 1 рабочее место):

Коммутатор DES-3810-28	1 шт.
Рабочая станция	1 шт.
Консольный кабель	1 шт.
Кабель Ethernet	1 шт.

20.1 Установка и настройка протокола IPv6 на рабочей станции

ЗАДАНИЕ 1

Установите протокол IPv6 на рабочей станции.

Чтобы установить протокол IPv6 выполните следующие действия (для Windows 7):

1. Откройте Изменение параметров адаптера;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши на **Подключение по локальной сети** и выберите **Свойства**;

3. Нажмите кнопку **Установить**;

4. В диалоговом окне **Выбор сетевых компонентов** выберите строку **Протокол** и нажмите кнопку **Добавить**;

5. В диалоговом окне **Выбор сетевого протокола** выберите **Microsoft TCP/IP версия 6** и нажмите кнопку **ОК**.

Проверьте конфигурацию сетевого адаптера. В командной строке введите:

```
ipconfig
```

Что вы наблюдаете? К какому типу адресов IPv6 относится наблюдаемый адрес? Объясните

Примечание: Windows XP поддерживает протокол IPv6 в экспериментальном варианте.

ЗАДАНИЕ 2

Настройте статический IPv6-адрес на рабочей станции.

Чтобы настроить статический IPv6-адрес выполните следующие действия:

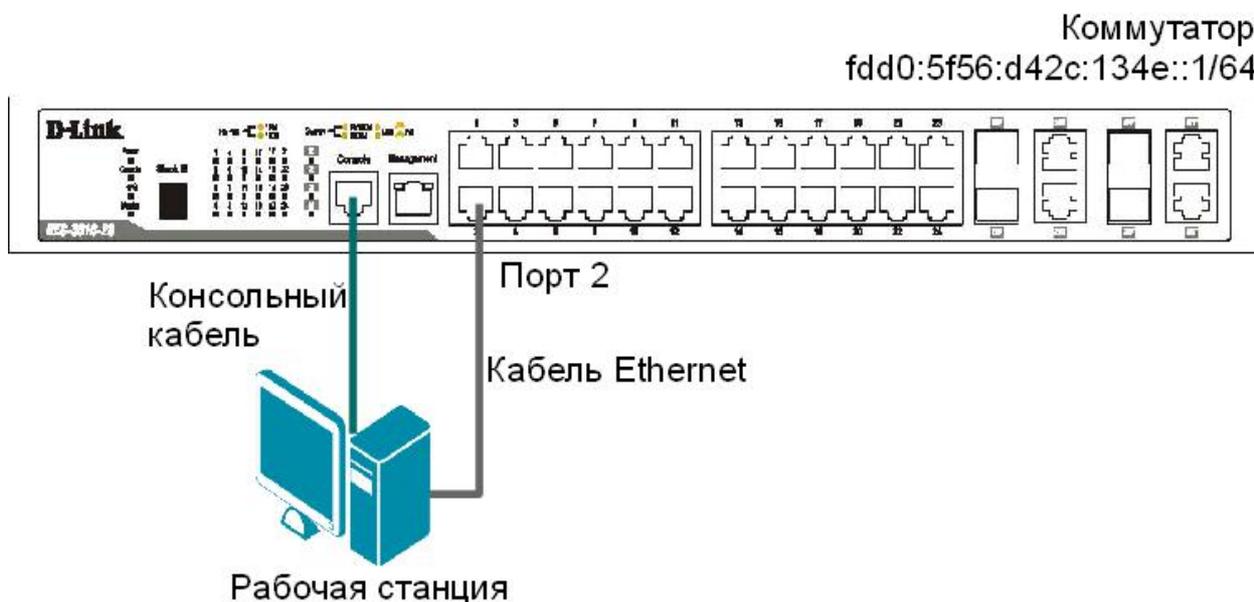
1. Откройте **Сетевые подключения**;
2. Щелкните правой кнопкой мыши на **Подключение по локальной сети**;
3. В диалоговом окне выберите **Протокол Интернета версии 6 (TCP/IPv6)** и нажмите **Свойства**;
4. Выберите **Использовать следующий IPv6-адрес**;
5. В поле **IPv6-адрес** введите: fdd0:5f56:d42c:134e::2
6. В поле **Длина префикса подсети** введите: 64
7. Нажмите **Ок**

Проверьте конфигурацию сетевого адаптера. В командной строке введите:
ipconfig

Что вы наблюдаете? К какому типу адресов IPv6 относится наблюдаемый адрес?

20.2 Настройка автоматической конфигурации (stateless autoconfiguration) адреса IPv6

Схема 20.2



Настройка коммутатора

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Настройте индивидуальный IPv6-адрес (Unique-Local) на интерфейсе System:

```
config ipif System ipv6 ipv6address fdd0:5f56:d42c:134e::1/64
```

Проверьте выполненные настройки:

```
show ipif
```

Включите автоматическую конфигурацию адреса на интерфейсе:

```
config ipv6 nd ra ipif System state enable
```

Настройте на рабочей станции автоматическое получение IPv6-адреса.

Проверьте конфигурацию сетевого адаптера рабочей станции. В командной строке введите:

```
ipconfig
```

Запишите IPv6-адрес. Какой IPv6-адрес шлюза по умолчанию (default gateway) вы наблюдаете?

Проверьте доступность соединения между рабочей станцией и коммутатором командой ping:

```
ping fdd0:5f56:d42c:134e::1
```

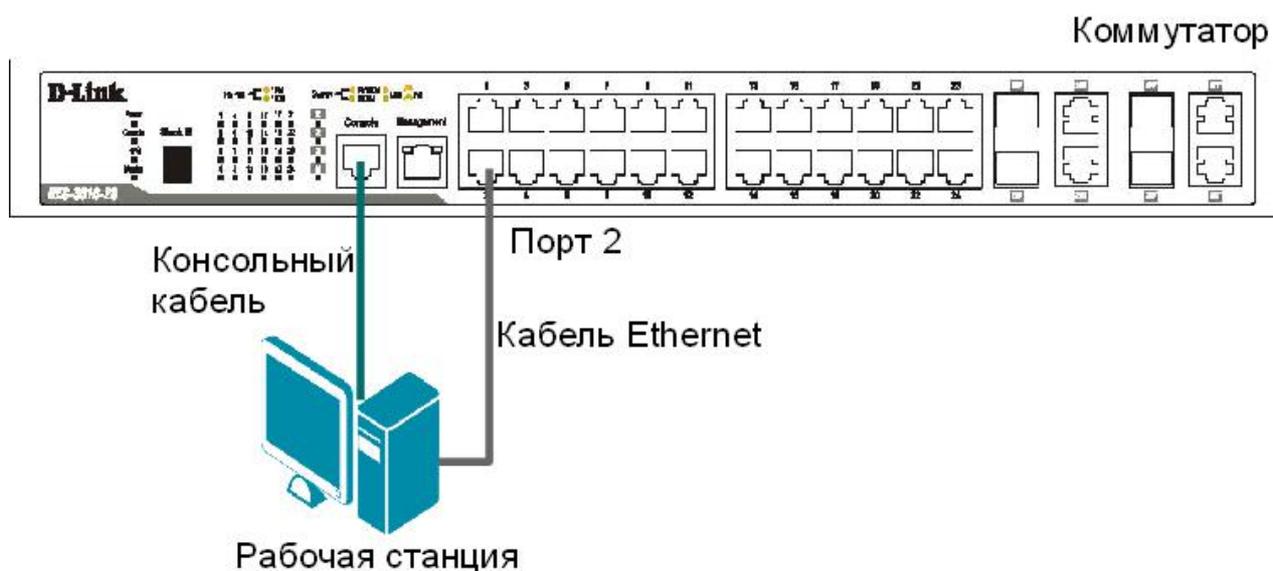
Проверьте доступность соединения между коммутатором и рабочей станцией. На коммутаторе введите команду:

```
ping <ipv6address>
```

Внимание: вместо *<ipv6address>* введите автоматически сконфигурированный адрес рабочей станции.

20.3 Подключение к коммутатору через Web-интерфейс с помощью адреса IPv6

Схема 20.3



Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Включите возможность подключения к коммутатору через Web-интерфейс и измените стандартный TSP-порт на новый:

```
enable web 8008
```

Проверьте выполненные настройки:

```
show switch
```

Проверьте настройки IP-интерфейсов:

```
show ipif
```

Что вы наблюдаете? Отображается ли IPv6-адрес? _____

Включите автоматическую конфигурацию адреса IPv6 Link-Local на интерфейсе System:

```
enable ipif_ipv6_link_local_auto System
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Что вы наблюдаете? Запишите IPv6-адрес интерфейса System _____

Настройте на рабочей станции автоматическое получение IPv6-адреса.

Запустите на рабочей станции браузер, введите в адресной строке IPv6-адрес коммутатора и укажите новый TSP-порт подключения:

```
http://[ipv6address]:8008
```

Внимание: вместо *<ipv6address>* введите автоматически сконфигурированный адрес Link-Local коммутатора.

Лабораторная работа №21. Разрешение IPv6-адресов с помощью протокола Neighbor Discovery Protocol (NDP)

Разработка протокола IPv6 привела к появлению совершенно нового протокола, обеспечивающего его поддержку. Он объединил ряд функций, относящихся к взаимодействию устройств в локальной сети, которые в IPv4 выполняются протоколами ARP и ICMP и добавил некоторые новые возможности. Новый протокол получил название *Neighbor Discovery Protocol* (NDP), протокол обнаружения соседей.

Понятие «сосед» используется в различных сетевых стандартах и технологиях для обозначения устройств, находящихся в одной локальной сети и которые могут непосредственно отправлять друг другу сообщения.

Протокол NDP, подобно протоколу ICMP является протоколом обмена сообщениями. Протокол NDP нельзя охарактеризовать словами, что он выполняет такую-то функцию. Он выполняет ряд операций путем обмена управляющими сообщениями.

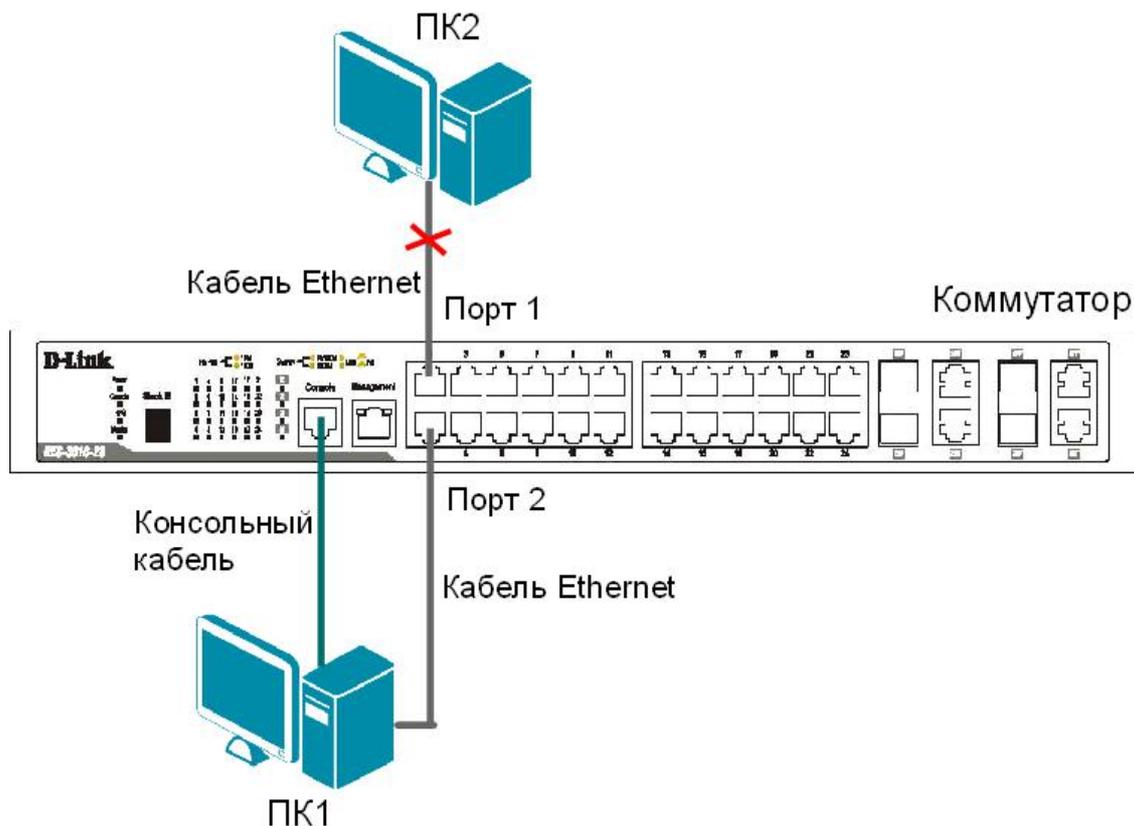
В протоколе IPv4 функцию разрешения адресов выполняет протокол ARP, а в протоколе IPv6 - NDP. Когда узел хочет узнать адрес канального уровня узла-назначения, он отправляет сообщение ICMPv6 Neighbor Solicitation (NS), содержащее IP-адрес того устройства, чей физический адрес надо узнать. Устройство назначения отвечает сообщением Neighbor Advertisement, которое содержит его физический адрес. При этом узел, запрашивающий физический адрес, отправляет сообщение не на широковещательный адрес, как в ARP, а на групповой адрес *Solicited-Node* целевого адреса IPv6.

Каждое устройство хранит в кэше (*neighbor cache*) информацию о соседнем устройстве локальной сети (узлах и маршрутизаторах).

Цель: изучить команды управления NDP-таблицей.

Оборудование (на 1 рабочее место):

Коммутатор DES-3810-28	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.



Подключите ПК1 к 2 порту коммутатора как указано на схеме 21.

Просмотрите информацию о соседних устройствах, подключенных к интерфейсу System:
`show ipv6 neighbor_cache ipif System all`

Подключите ПК2 как показано на схеме 21.

Просмотрите информацию о соседних устройствах, подключенных к интерфейсу System:
`show ipv6 neighbor_cache ipif System all`

Что вы наблюдаете? Запишите _____

Создайте статическую запись в NDP-таблице:
`create ipv6 neighbor_cache ipif System 3ffc::1 00:50:BA:00:07:36`

Просмотрите созданную статическую запись в NDP-таблице:
`show ipv6 neighbor_cache ipif System static`

Удалите статическую запись из NDP-таблицы:
`delete ipv6 neighbor_cache ipif System 3ffc::1`

Проверьте, что запись удалена:
`show ipv6 neighbor_cache ipif System static`

Просмотрите конфигурацию протокола Neighbor Discovery:

```
show ipv6 nd
```

Настройте время периодической отправки сообщений Neighbor Solicitation с интерфейса System:

```
config ipv6 nd ns ipif System retrans_time 400
```

Проверьте выполненные настройки:

```
show ipv6 nd
```

Лабораторная работа №22. Настройка функции CPU Interface Filtering для IPv6

Стандартные списки управления доступа выполняют фильтрацию входящего/исходящего через порты трафика на аппаратном уровне и не могут фильтровать потоки данных, предназначенные для ЦПУ, например при управлении коммутатором через Web-интерфейс.

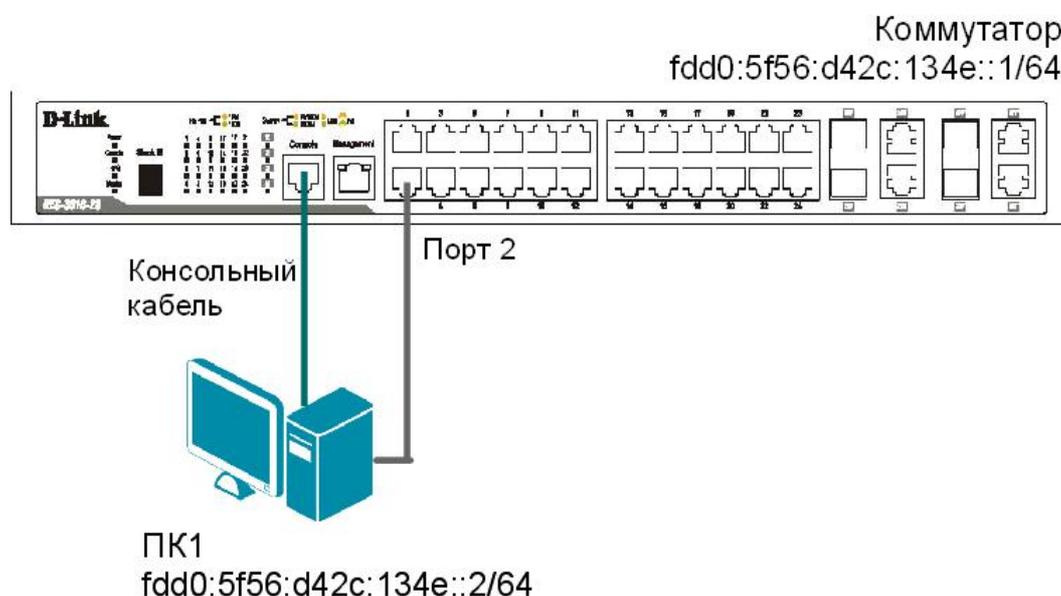
Функция CPU Interface Filtering, поддерживаемая на старших моделях коммутаторов D-Link, позволяет ограничить пакеты, поступающие для обработки на ЦПУ, путем фильтрации нежелательного трафика на программном уровне. Функция CPU Interface Filtering включает списки контроля доступа к управляющему интерфейсу коммутатора и обладает аналогичными стандартными ACL принципами работы и конфигурациями.

Цель: на коммутаторе D-Link настроить функцию CPU Interface Filtering для IPv6.

Оборудование (на 1 рабочее место):

Коммутатор DES-3810-28	1 шт.
Рабочая станция	1 шт.
Консольный кабель	1 шт.
Кабель Ethernet	1 шт.

Схема 22



ЗАДАНИЕ

Разрешить доступ ПК1 на Web-интерфейс коммутатора. Рабочим станциям, чей IPv6-адрес принадлежит сети fdd0:5f56:d42c:134e::/64, но не равен IP-адресу ПК1 доступ на Web-интерфейс запретить.

Правила:

Правило 1:

Если IP-адрес источника = IP-адресу ПК1 (fdd0:5f56:d42c:134e::2) и порт-назначения = 80 (по умолчанию для Web-интерфейса) — разрешить (permit);

Правило 2:

Если IP-адрес источника принадлежит сети fdd0:5f56:d42c:134e::/64, но не равен IP-адресу ПК1 — запретить (deny).

Правило 3:

Иначе, по умолчанию, разрешить доступ всем узлам.

Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора

Включите автоматическую конфигурацию IPv6-адреса (Link-Local) интерфейса управления:

```
enable ipif_ipv6_link_local_auto System
```

Настройте индивидуальный IPv6-адрес (Unique-Local) на интерфейсе System:

```
config ipif System ipv6 ipv6address fdd0:5f56:d42c:134e::1/64
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Создайте профиль доступа с номером 5, разрешающий доступ ПК1 на Web-интерфейс (порт 80) коммутатора (команда вводится в одну строку):

```
create cpu access_profile profile_id 5 ipv6 source_ipv6_mask  
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff tcp dst_port_mask 0xFFFF
```

Правило 1.

Создайте правило 1 для профиля доступа 5 (команду нужно вводить в одну строчку):

```
config cpu access_profile profile_id 5 add access_id 1 ipv6  
source_ipv6 fdd0:5f56:d42c:134e::2 mask  
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff tcp dst_port 80 mask  
0xFFFF port all permit
```

Примечание: созданное правило разрешает доступ ПК1 на Web-интерфейс через все порты коммутатора.

Правило 2.

Создайте правило 2 для профиля доступа 5 (команду нужно вводить в одну строчку):

```
config cpu access_profile profile_id 5 add access_id 2 ipv6  
source_ipv6 fdd0:5f56:d42c:134e:: mask ffff:ffff:ffff:ffff:: tcp  
dst_port 80 mask 0xFFFF port all deny
```

Примечание: созданное правило запрещает доступ на Web-интерфейс рабочим станциям, чей IP-адрес принадлежит сети fdd0:5f56:d42c:134e::/64, но не равен IP-адресу ПК1.

Правило 3.

Разрешить все остальное:

Выполняется по умолчанию

Проверьте созданные профили:

```
show cpu access_profile
```

Включите возможность подключения к коммутатору через Web-интерфейс:
enable web

Подключите рабочую станцию ПК1 как показано на схеме 22. Настройте на ПК1 IPv6-Unique-Local адрес fdd0:5f56:d42c:134e::2/64.

Запустите на рабочей станции ПК1 браузер, введите в адресной строке IPv6-адрес (Unique-Local) коммутатора и укажите TCP-порт подключения:
http://[fdd0:5f56:d42c:134e::1]:80

Что вы наблюдаете? _____

Настройте на рабочей станции ПК1 любой IPv6-адрес из подсети fdd0:5f56:d42c:134e::/64

Запустите на рабочей станции ПК1 браузер, введите в адресной строке IPv6-адрес (Unique-Local) коммутатора и укажите TCP-порт подключения:
http://[fdd0:5f56:d42c:134e::1]:80

Что вы наблюдаете? _____

Удалите профиль ACL (например профиль 5):
delete cpu access_profile profile_id 5

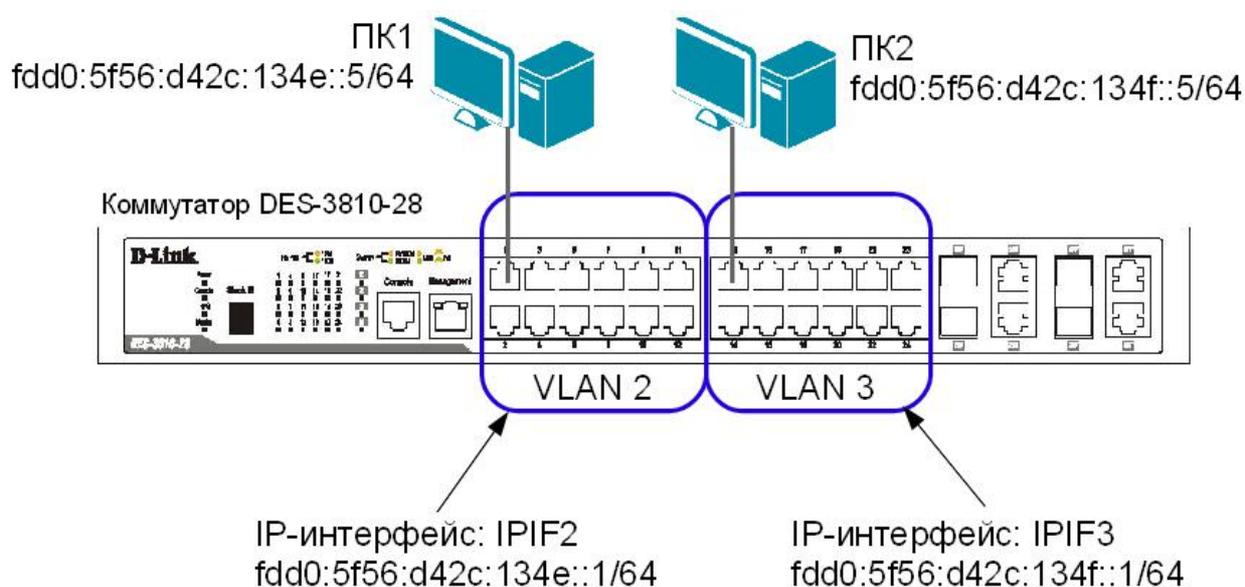
Лабораторная работа №23. Настройка маршрутизации IPv6 в пределах одного коммутатора

Цель: изучить настройку маршрутизации IPv6 между VLAN в пределах одного коммутатора.

Оборудование (на 1 рабочее место):

Коммутатор DES-3810-28	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.

Схема 23



Перед выполнением задания необходимо сбросить настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Настройка коммутатора

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2  
config vlan v2 add untagged 1-12
```

```
create vlan v3 tag 3  
config vlan v3 add untagged 13-24
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте IP-интерфейс для VLAN v2 и v3 с именами IPIF2 и IPIF3 соответственно:

```
create ipif IPIF2 v2 state enable  
create ipif IPIF3 v3 state enable
```

Настройте IPv6-адрес для интерфейсов IPIF2 и IPIF3:

```
config ipif IPIF2 ipv6 ipv6address fdd0:5f56:d42c:134e::1/64  
config ipif IPIF3 ipv6 ipv6address fdd0:5f56:d42c:134f::1/64
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Проверьте таблицу маршрутизации:

```
show ipv6route
```

Задайте рабочим станциям ПК1 и ПК2 IP-адреса в соответствии со схемой 23. В качестве шлюза по умолчанию (default gateway) укажите адрес IP-интерфейса маршрутизирующего коммутатора соответствующей VLAN.

Проверьте соединение между рабочими станциями командой ping6:

```
ping6 <ipv6address>
```

- от ПК1 к ПК2 _____
- от ПК2 к ПК1 _____

Должна ли быть связь между всеми ПК? Объясните _____

Лабораторная работа №24. Настройка статической и динамической маршрутизации IPv6

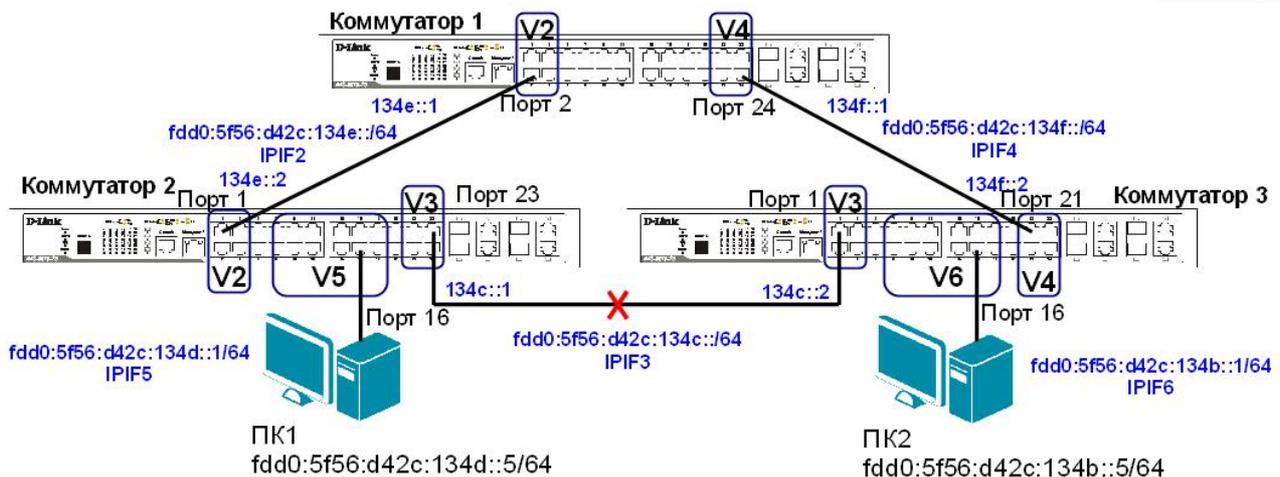
Примечание: протокол RIPv6 работает только на коммутаторах DES-3810-28 с образом программного обеспечения EI (Firmware Type). Чтобы проверить образ программного обеспечения на коммутаторе введите команду «show switch».

Цель: изучить настройку статической и динамической маршрутизации IPv6 на коммутаторах D-Link.

Оборудование (на 6 рабочих мест):

Коммутатор DES-3810-28	3 шт.
Рабочая станция	2 шт.
Консольный кабель	3 шт.
Кабель Ethernet	5 шт.

Схема 24



ЗАДАНИЕ 1

Настроить статическую маршрутизацию между VLAN V5 и VLAN V6.

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой:

```
reset config
```

Примечание: не соединяйте коммутаторы одновременно тремя кабелями во время настройки до особого указания.

Настройка коммутатора 1

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
config vlan default delete 1-24

Создайте VLAN v2 и v4, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2  
config vlan v2 add tagged 1-4
```

```
create vlan v4 tag 4
config vlan v4 add tagged 21-24
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте IP-интерфейс для VLAN v2 и v4 с именами IPIF2 и IPIF4 соответственно:

```
create ipif IPIF2 v2 state enable
create ipif IPIF3 v4 state enable
```

Настройте IPv6-адрес для интерфейсов IPIF2 и IPIF4:

```
config ipif IPIF2 ipv6 ipv6address fdd0:5f56:d42c:134e::1/64
config ipif IPIF4 ipv6 ipv6address fdd0:5f56:d42c:134f::1/64
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Настройка коммутатора 2

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

Создайте VLAN v2, v3 и v5 добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2
config vlan v2 add tagged 1-4
```

```
create vlan v3 tag 3
config vlan v3 add tagged 21-24
```

```
create vlan v5 tag 5
config vlan v5 add untagged 7-18
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте IP-интерфейс для VLAN v2, v3 и v5 с именами IPIF2, IPIF3 и IPIF5 соответственно:

```
create ipif IPIF2 v2 state enable
create ipif IPIF3 v3 state enable
create ipif IPIF5 v5 state enable
```

Настройте IPv6-адрес для интерфейсов IPIF2, IPIF3 и IPIF5:

```
config ipif IPIF2 ipv6 ipv6address fdd0:5f56:d42c:134e::2/64
config ipif IPIF3 ipv6 ipv6address fdd0:5f56:d42c:134c::1/64
config ipif IPIF5 ipv6 ipv6address fdd0:5f56:d42c:134d::1/64
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Настройка коммутатора 3

Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
config vlan default delete 1-24

Создайте VLAN v3, v4 и v6 добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v3 tag 3  
config vlan v3 add tagged 1-4
```

```
create vlan v4 tag 4  
config vlan v4 add tagged 21-24
```

```
create vlan v6 tag 6  
config vlan v6 add untagged 7-18
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте IP-интерфейс для VLAN v3, v4 и v6 с именами IPIF3, IPIF4 и IPIF6 соответственно:

```
create ipif IPIF3 v3 state enable  
create ipif IPIF4 v4 state enable  
create ipif IPIF6 v6 state enable
```

Настройте IPv6-адрес для интерфейсов IPIF3, IPIF4 и IPIF6:

```
config ipif IPIF3 ipv6 ipv6address fdd0:5f56:d42c:134c::2/64  
config ipif IPIF4 ipv6 ipv6address fdd0:5f56:d42c:134f::2/64  
config ipif IPIF6 ipv6 ipv6address fdd0:5f56:d42c:134b::1/64
```

Проверьте выполненные настройки IP-интерфейсов:

```
show ipif
```

Соедините между собой коммутаторы 1, 2 и 3 с помощью трех Ethernet-кабелей, как показано на схеме 24.

Задайте рабочим станциям ПК1 и ПК2 IP-адреса в соответствии со схемой 24. В качестве шлюза по умолчанию (default gateway) укажите адрес IP-интерфейса маршрутизирующего коммутатора соответствующей VLAN.

Проверьте соединение между рабочими станциями командой ping:

```
ping <IPv6-address>
```

- от ПК1 к ПК2 _____

- от ПК2 к ПК1 _____

Должна ли быть связь между всеми ПК? Объясните _____

Настройка коммутатора 1

Проверьте таблицу маршрутизации:
show ipv6route

Сколько записей в таблице маршрутизации вы наблюдаете? Запишите _____

Создайте статический маршрут к сети fdd0:5f56:d42c:134d::/64 (команда вводится в одну строку):

```
create ipv6route fdd0:5f56:d42c:134d::/64  
fdd0:5f56:d42c:134e::2
```

Примечание: команда означает, что сеть fdd0:5f56:d42c:134d::/64 доступна через интерфейс fdd0:5f56:d42c:134e::2 коммутатора 2.

Создайте статический маршрут к сети fdd0:5f56:d42c:134b::/64:

```
create ipv6route fdd0:5f56:d42c:134b::/64  
fdd0:5f56:d42c:134f::2
```

Создайте статический маршрут к сети fdd0:5f56:d42c:134c::/64:

```
create ipv6route fdd0:5f56:d42c:134c::/64  
fdd0:5f56:d42c:134e::2
```

Проверьте таблицу маршрутизации:
show ipv6route

Проверьте только статические записи в таблице маршрутизации:

```
show ipv6route static
```

Сколько записей в таблице маршрутизации вы наблюдаете? Сравните с предыдущими результатами _____

Настройка коммутатора 2

Проверьте таблицу маршрутизации:
show ipv6route

Сколько записей в таблице маршрутизации вы наблюдаете? Запишите _____

Создайте статический маршрут к сети fdd0:5f56:d42c:134b::/64:

```
create ipv6route fdd0:5f56:d42c:134b::/64  
fdd0:5f56:d42c:134c::2
```

Создайте статический маршрут к сети fdd0:5f56:d42c:134f::/64:

```
create ipv6route fdd0:5f56:d42c:134f::/64  
fdd0:5f56:d42c:134c::2/64
```

Проверьте таблицу маршрутизации:
show ipv6route

Сколько записей в таблице маршрутизации вы наблюдаете? Сравните с предыдущими результатами _____

Настройка коммутатора 3

Проверьте таблицу маршрутизации:

```
show ipv6route
```

Сколько записей в таблице маршрутизации вы наблюдаете? Запишите _____

Создайте статический маршрут к сети fdd0:5f56:d42c:134e::/64:

```
create ipv6route fdd0:5f56:d42c:134e::/64  
fdd0:5f56:d42c:134f::1
```

Создайте статический маршрут к сети fdd0:5f56:d42c:134d::/64:

```
create ipv6route fdd0:5f56:d42c:134d::/64  
fdd0:5f56:d42c:134c::1
```

Проверьте таблицу маршрутизации:

```
show ipv6route
```

Проверьте только статические записи в таблице маршрутизации:

```
show ipv6route static
```

Сколько записей в таблице маршрутизации вы наблюдаете? Сравните с предыдущими результатами _____

Проверьте соединение между рабочими станциями командой ping:

```
ping <IPv6-address>
```

- от ПК1 к ПК2 _____

- от ПК2 к ПК1 _____

Проверьте маршрут от ПК1 к ПК2 командой tracert. В командной строке ПК1 введите:

```
tracert fdd0:5f56:d42c:134b::5
```

Какое количество переходов вы наблюдаете? _____

Проверьте маршрут от ПК2 к ПК1 командой tracert. В командной строке ПК2 введите:

```
tracert fdd0:5f56:d42c:134d::5
```

Какое количество переходов вы наблюдаете? _____

Настройка коммутатора 1

Удалите статические маршруты (команда вводится в одну строку):

```
delete ipv6route fdd0:5f56:d42c:134d::/64  
fdd0:5f56:d42c:134e::2
```

```
delete ipv6route fdd0:5f56:d42c:134b::/64
```

```
fdd0:5f56:d42c:134f::2
```

```
delete ipv6route fdd0:5f56:d42c:134c::/64  
fdd0:5f56:d42c:134e::2
```

Настройка коммутатора 2

Удалите статический маршрут:

```
delete ipv6route fdd0:5f56:d42c:134b::/64  
fdd0:5f56:d42c:134c::2
```

```
delete ipv6route fdd0:5f56:d42c:134f::/64  
fdd0:5f56:d42c:134c::2/64
```

Настройка коммутатора 3

Удалите статический маршрут:

```
delete ipv6route fdd0:5f56:d42c:134e::/64  
fdd0:5f56:d42c:134f::1
```

```
delete ipv6route fdd0:5f56:d42c:134d::/64  
fdd0:5f56:d42c:134c::1
```

ЗАДАНИЕ 2

Настроить маршрут по умолчанию в VLAN V5 и VLAN V6

Настройка коммутатора 1

Создайте маршрут по умолчанию:

```
create ipv6route default fdd0:5f56:d42c:134f::2
```

Примечание: маршрут по умолчанию используется в том случае, если другой маршрут к сети назначения неизвестен.

Проверьте таблицу маршрутизации:

```
show ipv6route
```

Что вы наблюдаете? Запишите _____

Настройка коммутатора 2

Создайте маршрут по умолчанию:

```
create ipv6route default fdd0:5f56:d42c:134e::1
```

Настройка коммутатора 3

Создайте маршрут по умолчанию:

```
create ipv6route default fdd0:5f56:d42c:134c::1
```

Проверьте соединение между рабочими станциями командой ping:
ping <IPv6-address>

- от ПК1 к ПК2 _____
- от ПК2 к ПК1 _____

Проверьте маршрут от ПК1 к ПК2 командой tracert. В командной строке ПК1 введите:
tracert fdd0:5f56:d42c:134b::5

Какое количество переходов вы наблюдаете? Сравните с результатом задания 1 _____

Проверьте маршрут от ПК2 к ПК1 командой tracert. В командной строке ПК2 введите:
tracert fdd0:5f56:d42c:134d::5

Какое количество переходов вы наблюдаете? Сравните с результатом задания 1 _____

Настройка коммутатора 1

Удалите статический маршрут по умолчанию:
delete ipv6route default fdd0:5f56:d42c:134f::2

Настройка коммутатора 2

Удалите статический маршрут по умолчанию:
delete ipv6route default fdd0:5f56:d42c:134e::1

Настройка коммутатора 3

Удалите статический маршрут по умолчанию:
delete ipv6route default fdd0:5f56:d42c:134c::1

ЗАДАНИЕ 3

Настроить протокол динамической маршрутизации RIPng.

Настройка коммутатора 1

Включите работу протокола RIPng глобально на коммутаторе:
enable ripng

Активизируйте протокол RIPng на всех интерфейсах:
config ripng ipif all state enable

Настройте метод испорченного обратного маршрута (Poison reverse) для борьбы с петлями маршрутизации:
config ripng method poison_reverse

Измените интервал отправки обновлений таблицы маршрутизации (по умолчанию 30 секунд).

```
config ripng update 40
```

Настройте время старения записей в таблице маршрутизации (по умолчанию 180 секунд)

```
config ripng expire 190
```

Проверьте настройки протокола RIPng:

```
show ripng
```

Повторите процедуру настройки для коммутатора 2 и коммутатора 3

Настройка коммутаторов 1, 2, 3

Проверьте таблицу маршрутизации:

```
show ipv6route
```

Сколько записей в таблице маршрутизации вы наблюдаете? Запишите _____

Посмотрите таблицу маршрутизации протокола RIPng:

```
show ipv6route ripng
```

Проверьте версию и статус протокола RIP:

```
show ripng
```

Сколько записей вы наблюдаете? _____

Проверьте соединение между рабочими станциями командой ping:

```
ping <IPv6-address>
```

- от ПК1 к ПК2 _____
- от ПК2 к ПК1 _____

Проверьте маршрут от ПК1 к ПК2 командой `tracert`. В командной строке ПК1 введите:

```
tracert fdd0:5f56:d42c:134b::5
```

Какое количество переходов вы наблюдаете? _____

Проверьте маршрут от ПК2 к ПК1 командой `tracert`. В командной строке ПК2 введите:

```
tracert fdd0:5f56:d42c:134d::5
```

Какое количество переходов вы наблюдаете? _____

Отключите кабель Ethernet, соединяющий коммутатор 2 и коммутатор 3 (схема 24).

Проверьте таблицу маршрутизации:

```
show ipv6route
```

Сколько записей в таблице маршрутизации вы наблюдаете? Сравните с предыдущими результатами. Что изменилось? _____

Выключите работу протокола RIPv2 глобально на коммутаторе:
`disable ripng`