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

Версия 1.3

Москва, 2011

Оглавление

Рекомендации по организации лабораторных работ

Для выполнения настоящих лабораторных работ, рекомендуется следующий комплект оборудования:

Коммутатор DGS-3612	2 шт.
Коммутатор DES-3200-10 или DGS-3200-10	8 шт.
Коммутатор DES-1005A	5 шт.
Рабочая станция	20 шт.
Кабель Ethernet	35 шт.
Консольный кабель	10 шт.

Данный комплект оборудования рассчитан на учебную группу, состоящую из 10 человек.

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

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

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

Коммутатор DGS-3612 – ПО версии 2.80.B35 и выше
Коммутатор DES-3200-10 – ПО версии 1.50.B002 и выше
Коммутатор DGS-3200-10 – ПО версии 1.62.B020 и выше

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 сокращенный 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 приведенном примере синтаксиса, пользователь должен указать имя IP-интерфейса System, имя VLAN vlan_name 32 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 приведенном примере синтаксиса, пользователь должен указать один из двух уровней привилегий (admin или user) для создаваемой учетной 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 введен/указан.
Синтаксис	**create account [admin | user] <username 15>**
Описание	В приведенном примере синтаксиса, пользователь должен указать один из

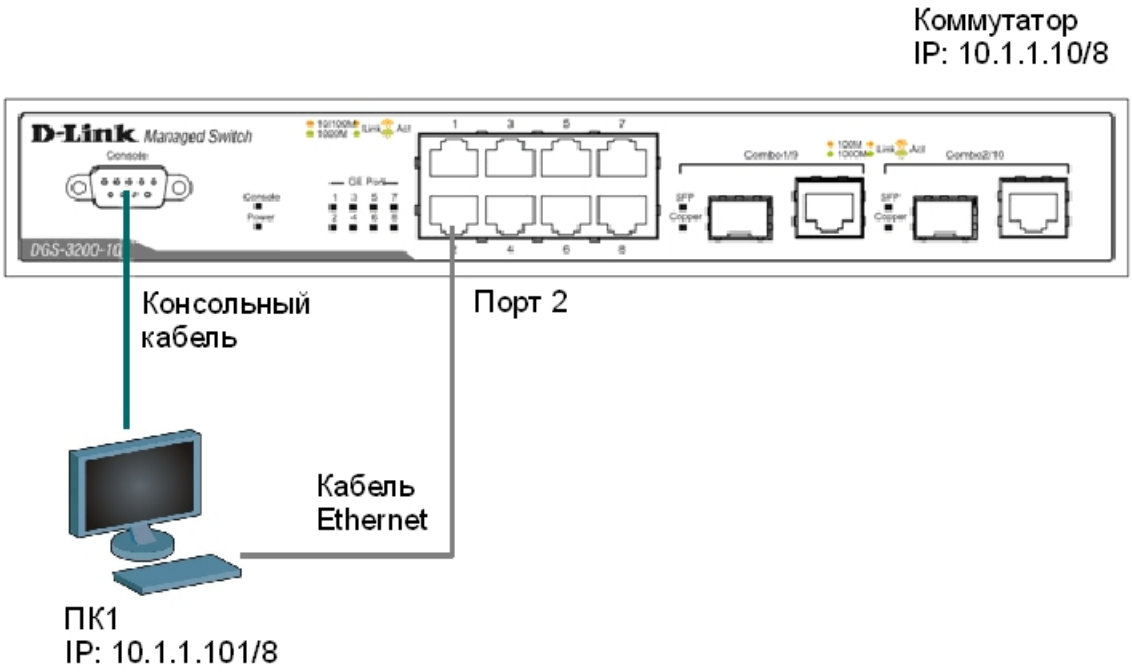
	двух уровней привилегий (admin или user) для создаваемой учетной записи. Вводить квадратные скобки не надо.
Пример	**create account admin user1**
{ фигурные скобки }	
Назначение	Содержит необязательное значение или набор необязательных аргументов.
Синтаксис	**reset {[config | system]} {force_agree}**
Описание	В приведенном 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, заключенных в фигурные скобки, должно быть введено.
Синтаксис	**config dhcp_relay {hops <value 1-16> | time <sec 0-65535>}(1)**
Описание	В приведенном примере синтаксиса, от пользователя ожидается ввод одного или обоих необязательных параметров, заключенных в фигурные скобки. Параметр «(1)» показывает, что ожидается ввод, по крайней мере, одного из параметров или аргументов.
Пример	**config dhcp_relay hops 3**

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

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-10 или DGS-3200-10 1 шт.
Рабочая станция 1 шт.
Консольный кабель 1 шт.

Схема 1:



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 необходимо запустить программу эмуляции терминала VT100 (например, программу HyperTerminal в Windows). В программе следует установить следующие параметры подключения:

Скорость (бит/с):	115200 (DGS-3200-10) или 9600 (DES-3200-10)
Биты данных:	8
Четность:	нет
Стоповые биты:	1
Управление потоком:	нет

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!

Напишите в консоли: `?`
Напишите в консоли: `dir`
Напишите в консоли: `config`
Напишите 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 10.1.1.10/8
```

Настройте IP-адрес шлюза по умолчанию:
```
create iproute default 10.1.1.254
```

Примечание: IP-адрес шлюза по умолчанию назначается, если управление коммутатором осуществляется из других IP-подсетей.

Проверьте настройки коммутатора:
```
show switch
```

(MAC-адрес, IP-адрес интерфейса управления, IP-адрес шлюза по умолчанию, версия программного обеспечения, серийный номер, имя коммутатора, доступные консоли управления).

1.3. Настройка времени на коммутаторе

Проверьте время:
```
show time
```

Введите новую дату и время:
```
config time 10022011 15:45:30
```

Укажите текущую дату и время.

Установите часовой пояс Москва (GMT +3:00):
```
config time_zone operator + hour 3 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 до15 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 в систему! В случае утраты сведений о Логине и Пароле, разблокировать коммутатор можно только в сервисном центре компании D-Link! (Для старых версий ПО)

Создайте учетную 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 учетной записи администратора:
Username: dlink

```
Password: dlink
DES-3200-10#
```

Создайте учетную 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 учетных 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 незашифрованном 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
```

Дешифруйте пароль учетной записи пользователя:

```
config account swuser encrypt plain_text dlink1
```

Убедитесь, что пароль учетной записи пользователя дешифрован:

```
show config current_config
```

Удалите учетную запись пользователя:
```
delete account swuser
```

Убедитесь в удалении учетной 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 отключен.

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.

Отключите возможность подключения к коммутатору через Web-интерфейс:
```
disable web
```

Проверьте выполненные настройки:
```
show switch
```

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

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 TCP-порт подключения на новый:

```
enable web 8008
```

Запустите на рабочей станции ПК1 браузер, введите в адресной строке IP-адрес коммутатора и укажите новый TCP-порт подключения:
```
http://10.1.1.10:8008
```

1.6. Настройка параметров баннеров 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 конфигурирования баннера приветствия:
```
config greeting_message
```

Для редактирования приветствия, используйте следующие команды:

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

Добавьте строчку в приветствие:
```
SWITCH_TEST  tel +7(495) 000-00-00
```

Сохраните изменения в приветствии и выйдите из режима редактирования:
Ctrl+W

Проверьте баннер приветствия:
```
show greeting_message
```

```
 = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
DES-3200-28 Fast Ethernet Switch
Command Line Interface
SWITCH_TEST  tel +7(495) 000-00-00
Firmware: Build 1.50.B002
Copyright(C) 2008 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 1-5:
```
config ports 1-5 speed 10_half
```

Проверьте выполненные настройки:
```
show ports
```

Что вы наблюдаете? Запишите.

_____

_____

Активизируйте функцию управления потоком на портах 1-5:
```
config ports 1-5 flow_control enable
```

Проверьте настройки:
```
show ports
```

Отключите работу портов 1-5:
```
config ports 1-5 state disable
```

Проверьте настройки:
```
show ports
```

Проверьте соединение между ПК1 и коммутатором. На ПК1 выполните команду:
```
ping 10.1.1.10
```

Что вы наблюдаете? Запишите.

_____

_____

Включите работу порта 2:
```
config ports 2 state enable
```

Проверьте соединение между ПК1 и коммутатором.
На ПК1 выполните команду:
```
ping 10.1.1.10
```

Что вы наблюдаете? Запишите.

_____

_____

Задайте описание порта 2:
```
config ports 2 description PC_PORT
```

Проверьте описание портов:
```
show ports description
```

1.8. Сохранение конфигурации в энергонезависимой памяти

Сохраните конфигурацию, хранимую в RAM, в энергонезависимую память (NVRAM):
```
save
```

Посмотрите конфигурацию коммутатора, сохраненную в NVRAM:
```
show config config_in_nvram
```

1.9. Команды мониторинга сети

Посмотрите статистику о пакетах, передаваемых и принимаемых портом 2 коммутатора:
```
show packet ports 2
```

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-атак или неисправности.

Посмотрите статистику об ошибках передаваемых и принимаемых портом пакетов:
```
show error ports 2
```

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

Очистите счетчики статистики на порте:
```
clear counters ports 2
```

Примечание: в случае устранения выявленных ошибок или проверки отчета 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 путем 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 путем замены 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.

Посмотрите log-файл коммутатора:
```
show log
```

Посмотрите log-файл коммутатора с определенного индекса (ID):
```
show log index 25
```

Очистите log-файл:
```
clear log
```

Протестируйте состояние медных кабелей, подключенных к портам коммутатора:
```
cable_diag ports all
```

Примечание: данная функция позволяет определить состояние пар, подключенного 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, учетных записей пользователей и журнала регистраций. Коммутатор не сохранит настройки в энергонезависимой памяти NVRAM и не перегрузится.

Если указано ключевое слово **config**, на коммутаторе восстановятся все заводские настройки по умолчанию, включая IP-адрес интерфейса управления, учетные записи пользователей и журнал регистраций. Коммутатор не сохранит настройки 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, причем любая из них может быть настроена в качестве основной, т.е. используемой 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 log-файла оборудования.

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

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-10 или DGS-3200-10	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

Настройте TFTP-сервер (пример, Tftpd32 by Ph.Jounin для Windows, доступный по адресу http://tftpd32.jounin.net).

1. В настройках необходимо установить директорию приема файлов.
2. Отключить все другие сервисы кроме TFTP server.

Подготовьте файл нового программного обеспечения коммутатора.

1. Найдите необходимый файл «прошивки» на сайте 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 коррекции ошибок.

Внимание: **НЕ** перезагружайте коммутатор во время загрузки программного обеспечения. Выполнение команды без ключа image_id приводит к перезаписи текущего ПО!

Настройте IP-адрес интерфейса управления:

```
config ipif System ipaddress 10.1.1.10/8
```

Настройте TFTP-сервер:

```
Указать IP-адрес рабочей станции 10.1.1.250/8
Запустить TFTP-сервер, указать директорию с прошивкой Current
Directory.
```

Проверьте доступность TFTP-сервера:

```
ping 10.1.1.250
```

Проверьте информацию о текущем программном обеспечении:

```
show firmware information
```

Загрузите программное обеспечение на коммутатор:

```
download firmware_fromTFTP 10.1.1.250 DGS3200_Run_1_62_B020.had
image_id 2
```

Убедитесь, что программное обеспечение загружено:

```
show firmware information
```

2.3. Настройка порядка загрузки программного обеспечения коммутатора

Измените программное обеспечение, которое будет загружаться при старте коммутатора:

```
config firmware image_id 2 boot_up
```

Сохраните изменения:

```
save
```

Перезагрузите коммутатор:
```
reboot
```

Обновленная прошивка вступит в силу только после перезагрузки.

Проверьте информацию о программном обеспечении:
```
show firmware information
```

Что вы наблюдаете?

_____
_____
_____
_____
_____

2.4. Выгрузка и загрузка конфигурации

Посмотрите текущую версию конфигурации коммутатора (находящуюся в RAM):
```
show config current_config
```

Посмотрите конфигурацию коммутатора, сохраненную в NVRAM:
```
show config config_in_nvram 1
```

Выгрузите конфигурацию на TFTP-сервер:
```
upload cfg_toTFTP 10.1.1.250 config.txt
```

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

Замените IP-адрес 10.1.1.**10**/8 на 10.1.1.**8**/8
```
# IP
config ipif System ipaddress 10.1.1.10/8 vlan default state enable
disable autoconfig

# IP
config ipif System ipaddress 10.1.1.8/8 vlan default state enable
disable autoconfig
```

Сохраните файл.

Загрузите измененную конфигурацию на коммутатор:
```
download cfg_fromTFTP 10.1.1.250 config.txt
```

Проверьте, изменился ли IP-адрес коммутатора:
```
show switch
```

Что вы наблюдаете?

_____
_____
_____
_____

Чему будет равен IP-адрес после перезагрузки коммутатора? _____

2.5. Выгрузка log-файлов

Просмотрите log-файл коммутатора:

```
show log
```

Выгрузите log-файл на TFTP-сервер:

```
upload log_toTFTP 10.1.1.250 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-таблицами

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-таблицы коммутаторов хранят сопоставления IP- и MAC-адресов. ARP-таблица может строиться коммутатором динамически в процессе изучения ARP-запросов и ответов, передаваемых между устройствами подключенными к его портам, или создаваться вручную администратором сети.

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

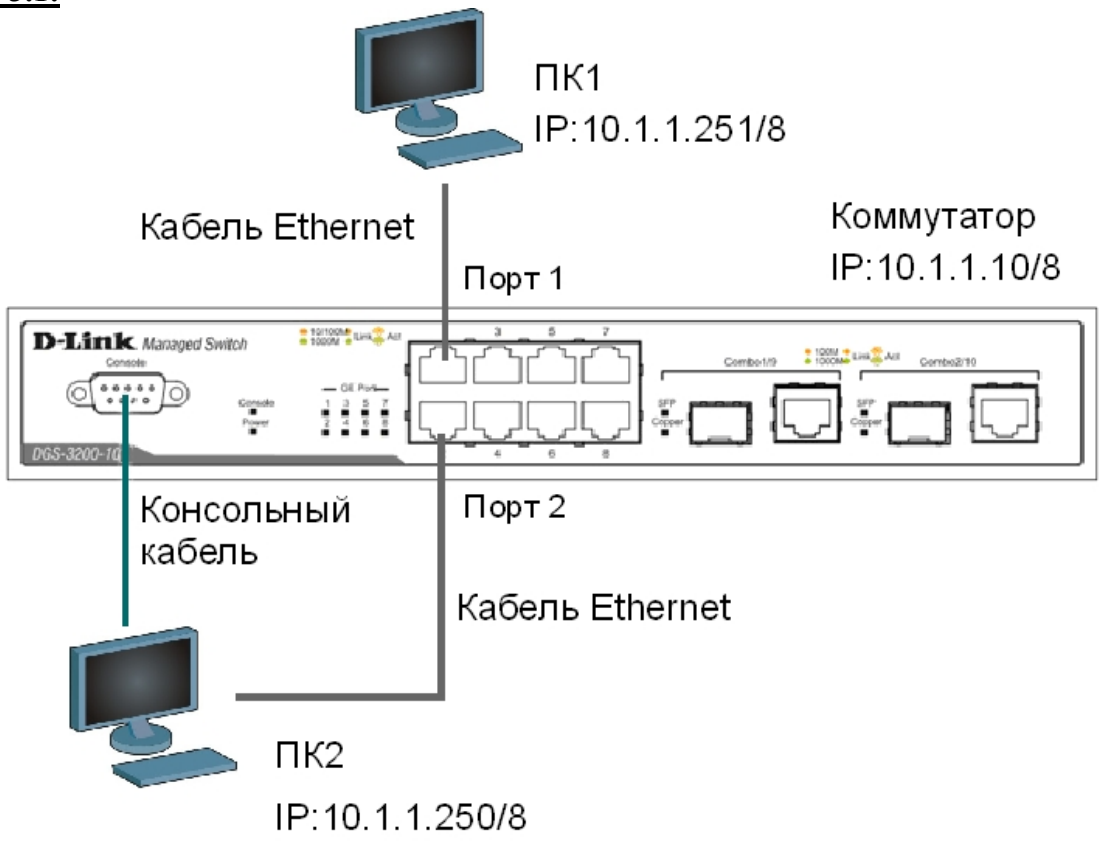
Цель: изучить процесс управления таблицами коммутации и ARP-таблицами.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-10 или DGS-3200-10	1 шт.
Коммутатор DGS-3612	1 шт.
Рабочая станция	2 шт.
Консольный кабель	2 шт.
Кабель Ethernet	2 шт.

3.1. Команды управление таблицей коммутации

Схема 3.1:



Просмотрите содержимое таблицы MAC-адресов:
```
show fdb
```

Определите порт коммутатора, к которому подключено устройство с определенным 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 управление ARP-таблицей

Просмотрите ARP-таблицу:
```
show arpentry
```

Найдите в ARP-таблице сопоставления IP-MAC по указанному IP-адресу:
```
show arpentry ipaddress 10.1.1.250
```

Просмотрите в ARP-таблице все сопоставления IP-MAC на интерфейсе System:
```
show arpentry ipif System
```

Удалите все динамически созданные записи из ARP-таблицы:
```
clear arptable
```

Убедитесь, что все динамические записи из таблицы удалены:
```
show arpentry
```

Создайте статическую запись в ARP-таблице (в качестве MAC-адреса укажите MAC-адрес ПК2):
```
create arpentry 10.1.1.250 00-50-BA-00-07-36
```

Просмотрите созданную статическую запись в ARP-таблице:
```
show arpentry static
```

Удалите статическую запись из ARP-таблицы:
```
delete arpentry 10.1.1.250
```

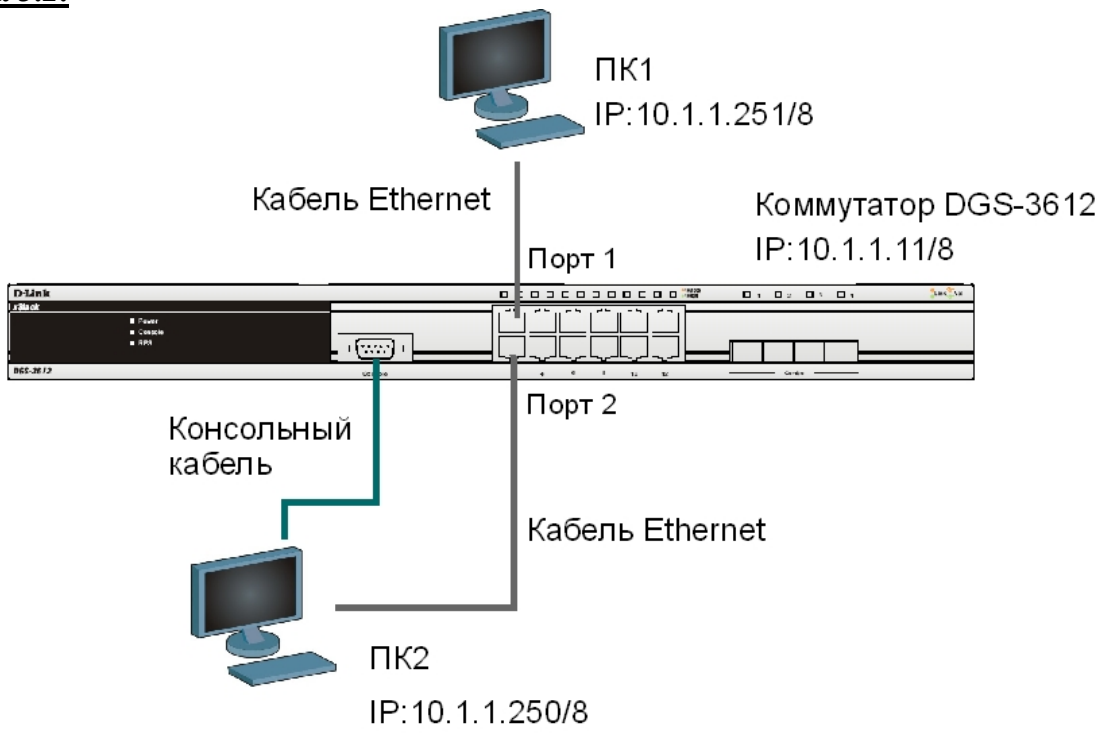
Проверьте, что запись удалена:
```
show arpentry static
```

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

Проверьте выполненные настройки:
```
show arpentry
```

3.3. Команды просмотра таблицы коммутации уровня 3

Схема 3.2:



Посмотрите таблицу коммутации 3-го уровня:
```
show ipfdb
```

Определите порт коммутатора, к которому подключено устройство с определенным IP-адресом:
```
show ipfdb 10.1.1.250
```

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

Виртуальная локальная сеть (Virtual Local Area Netwrok, 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 коммутатора можно настроить на принадлежность определенной VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть, т.е. кадры, предназначенные станциям, которые не принадлежат 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 ее настройку на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

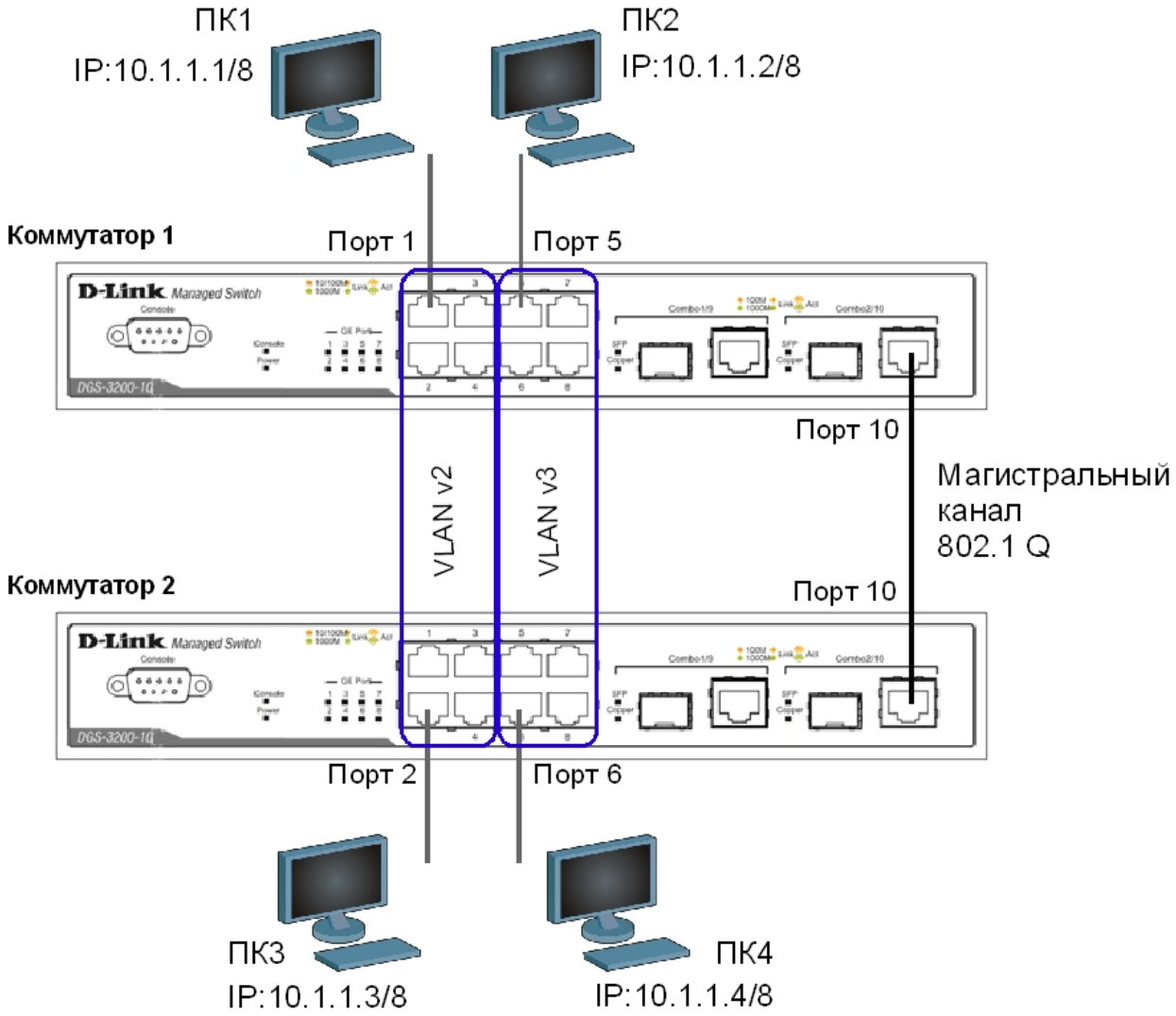
Коммутатор DES-3200-10 или DGS-3200-10	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

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.

Настройка коммутатора 1

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

```
config vlan default delete 1-10
config vlan default add tagged 10
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порт 10 маркированным:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-4
config vlan v2 add tagged 10
```

```
create vlan v3 tag 3
config vlan v3 add untagged 5-8
config vlan v3 add tagged 10
```

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 в то же время имели доступ к разделяемым портам, используемым, например, для подключения серверов или магистрали 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 5-8 коммутатора 1, находящиеся в VLAN v3 таким образом, чтобы рабочие станции, подключенные к ним, не могли обмениваться данными, но при этом могли передавать данные через магистральный канал.

Настройка коммутатора 1

Настройте сегментацию трафика:
```
config traffic_segmentation 5 forward_list 10
config traffic_segmentation 6 forward_list 10
config traffic_segmentation 7 forward_list 10
config traffic_segmentation 8 forward_list 10
```

Проверьте выполненные настройки:
```
show traffic_segmentation
```

Подключите ПК1 к порту 6 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.

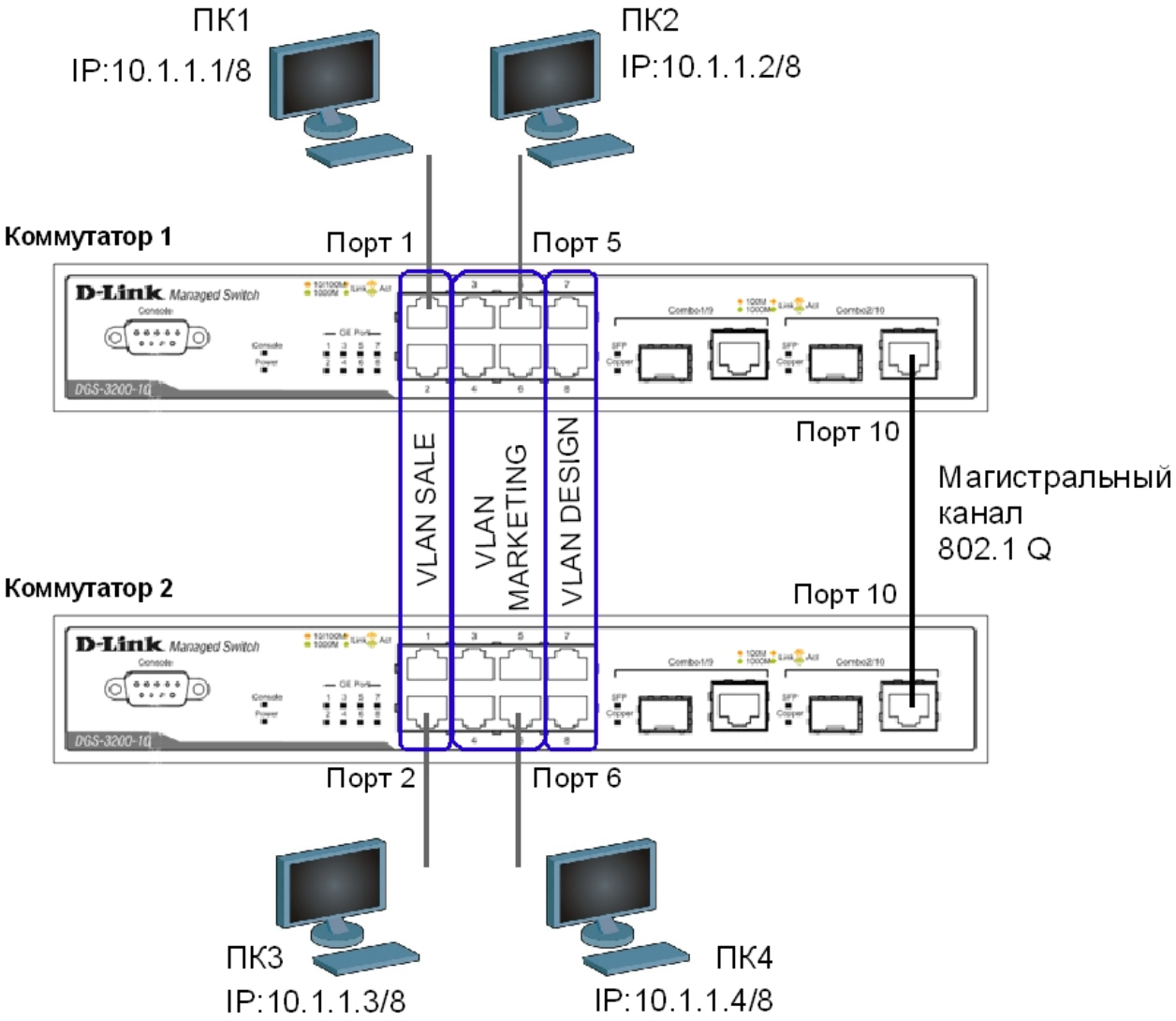
_____

_____

_____

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

```
config vlan default delete 1-10
```

Создайте девять VLAN с тегами 2-10:

```
create vlan vlanid 2-10
```

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

Измените имя нескольких VLAN и добавьте в них немаркированные порты:

```
config vlan vlanid 7 name SALE add untagged 1-2
config vlan vlanid 8 name MARKETING add untagged 3-6
config vlan vlanid 9 name DESIGN add untagged 7-8
```

Добавьте маркированные порты в несколько VLAN:

```
config vlan vlanid 2-10 add tagged 9-10
```

Проверьте настройки VLAN:

```
show vlan
```

Удалите порты из нескольких VLAN:

```
config vlan vlanid 2-10 delete 9-10
```

Проверьте настройки VLAN:

```
show vlan
```

Создайте магистральный порт VLAN для передачи маркированных кадров:

```
config vlan_trunk ports 10 state enable
```

Активизируйте функционирование магистрального канала:

```
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 порт-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 GVPR 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.

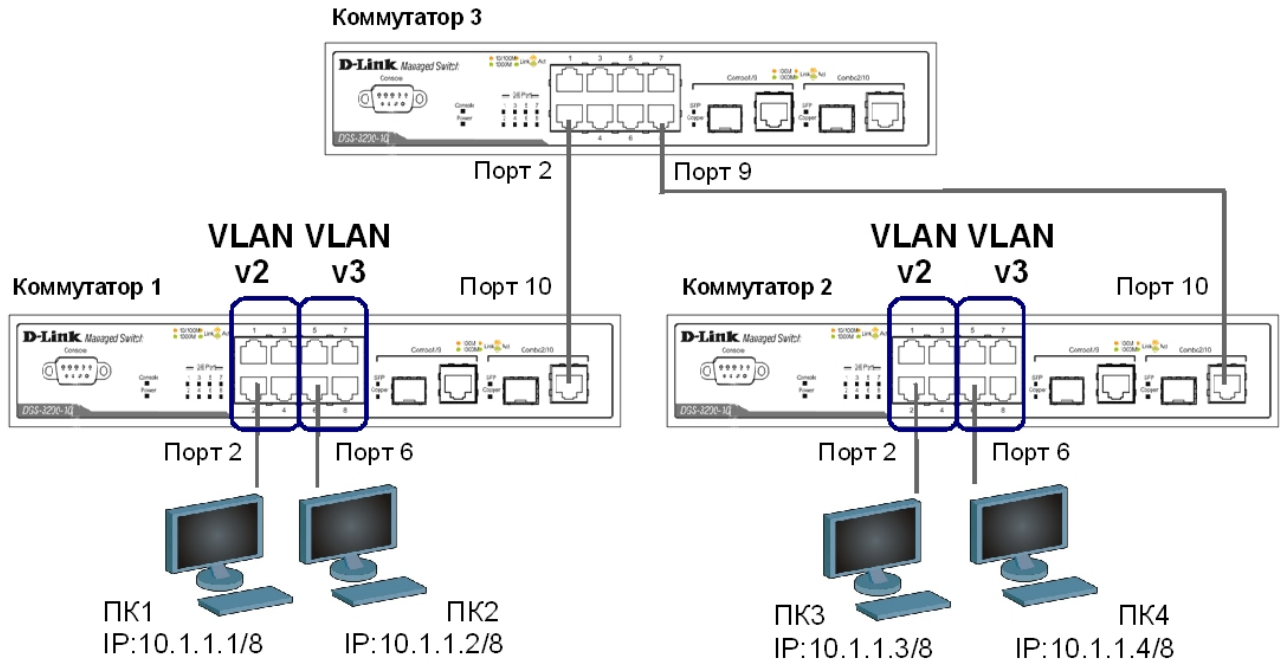
Примечание: при динамической передаче информации о VLAN через магистральные коммутаторы, рекомендуется передавать информацию только о пользовательских VLAN, а служебные VLAN и управляющие VLAN настраивать на магистральных коммутаторах статически.

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

Оборудование (на 3 рабочих места):

Коммутатор DES-3200-10 или DGS-3200-10	3 шт.
Рабочая станция	4 шт.
Консольный кабель	3 шт.
Кабель Ethernet	6 шт.

Схема 5:



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

```
reset config
```

Настройка коммутатора 1

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

```
config vlan default delete 1-10
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порт 10 маркированным:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-4
config vlan v2 add tagged 10

create vlan v3 tag 3
config vlan v3 add untagged 5-8
config vlan v3 add tagged 10
```

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 приема и отправки информации о VLAN через порт 10 коммутатора:

```
config gvrp 10 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 gvrp all state enable
```

Проверьте настройки VLAN на коммутаторе 3:

```
show vlan
```

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

```
show gvrp
```

Запишите ваши наблюдения:

_____
_____
_____
_____

Проверьте доступность соединения между рабочими станциями командой ping:

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

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

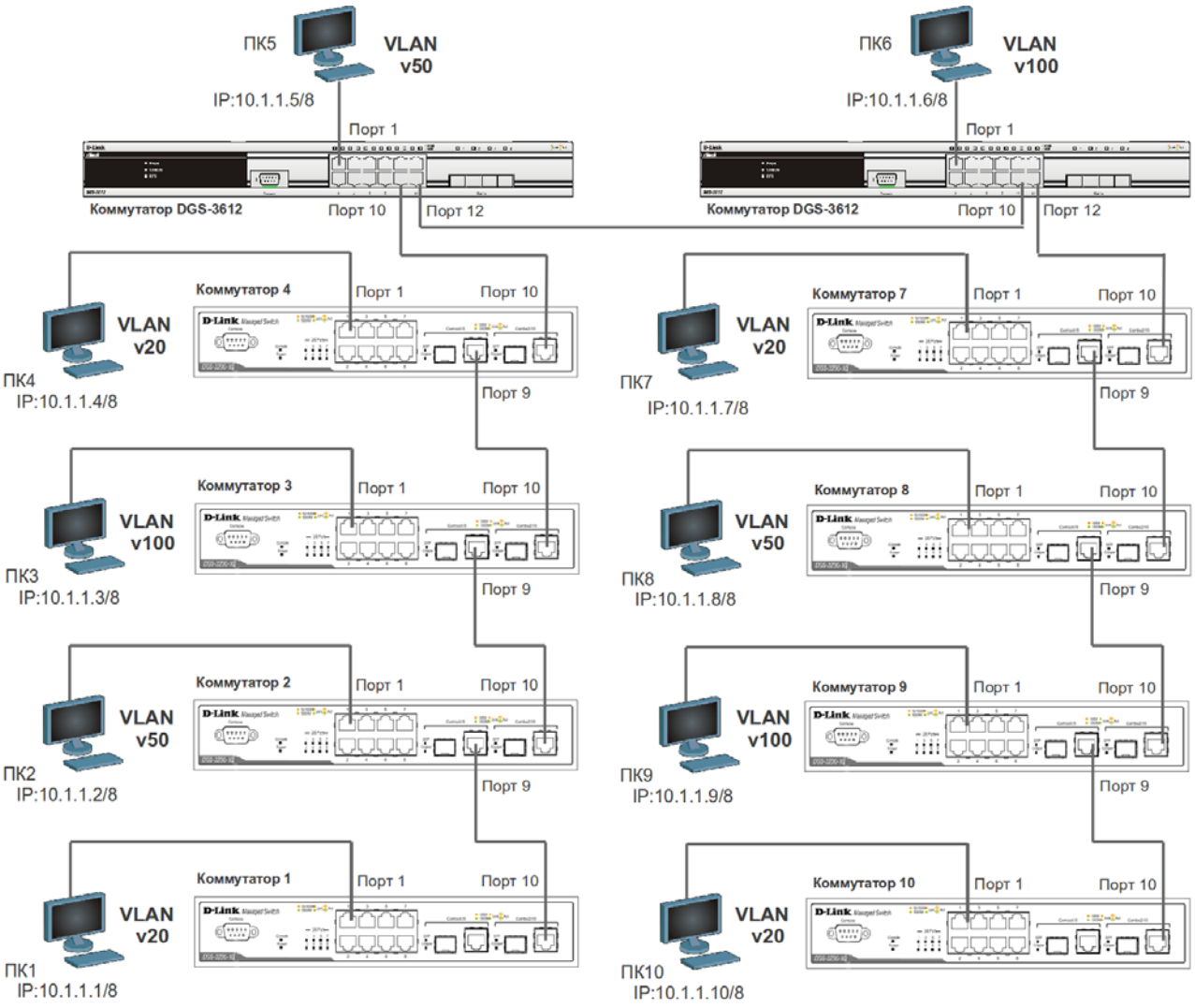
Лабораторная работа №6. Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q

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

Оборудование (на 10 рабочих мест):

Коммутатор DES-3200-10 или DGS-3200-10	8 шт.
Коммутатор DGS-3612	2 шт.
Рабочая станция	10 шт.
Консольный кабель	10 шт.
Кабель Ethernet	20 шт.

Схема 6 (общая схема сети):



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

```
reset config
```

ЗАДАНИЕ 1

Подключите устройства как показано на схеме 6. Задайте на всех ПК IP-адреса из подсети 10.1.1.0/8.

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 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?

_____
_____
_____

Настройте магистральные порты коммутаторов как маркированные, а пользовательские порты как немаркированные, в соответствии со схемой 6.

Проверьте связь между всеми ПК командой ping.

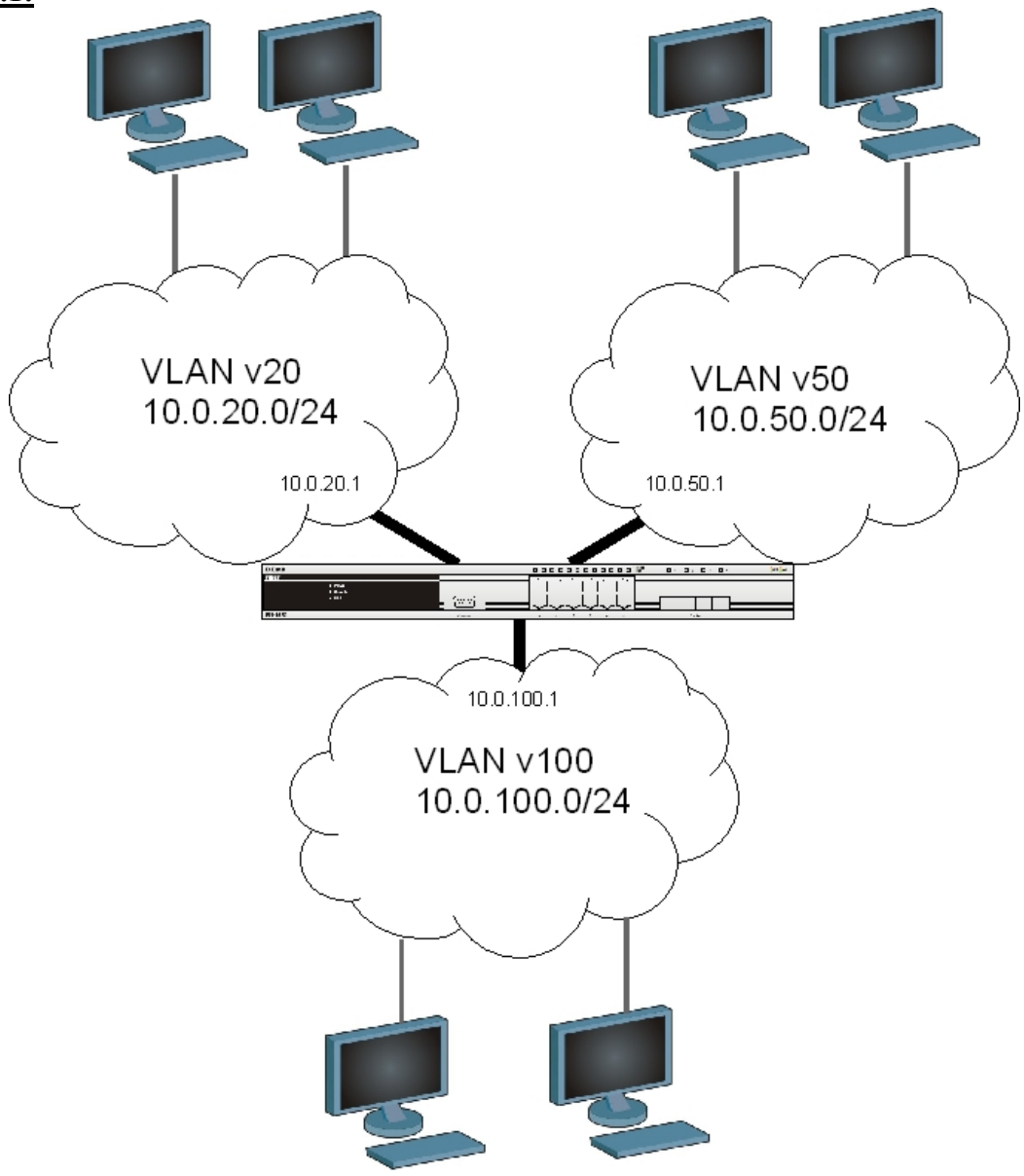
Какие ПК доступны с вашего рабочего места, а какие нет? Почему?

_____
_____
_____

ЗАДАНИЕ 3

На одном из коммутаторов DGS-3612 необходимо настроить маршрутизацию для объединения разных VLAN в общую сеть. Логическая схема сети с маршрутизацией показана на схеме 6.1.

Схема 6.1:



Перед настройкой маршрутизации на коммутаторе DGS-3612 в задании 2 уже должны быть созданы необходимые VLAN v20, v50, v100.

Введите на коммутаторе DGS-3612 следующие команды, чтобы создать IP-интерфейс для каждой VLAN:

```
create ipif IPIF20 10.0.20.1/24 v20 state enable
create ipif IPIF50 10.0.50.1/24 v50 state enable
create ipif IPIF100 10.0.100.1/24 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 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 здании 1.

_____
_____
_____
_____
_____

Лабораторная работа №7. 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. Второй этап работы STP – выбор корневых портов (Root Port). Третий шаг 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 определенной 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 подключенный 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 подключен 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 1 Мбит/с 10 Мбит/с 100 Мбит/с	200 000 000* 20 000 000* 2 000 000* 200 000*
1 Гбит/с 10 Гбит/с	20 000 2 000

* Коммутаторы, поддерживающие только стандарт IEEE 802.1D-1998 (STP) для этих скоростей канала должны использовать значение 65 535.

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 еще роль — мастер-порт (*Master Port*).

Счетчик переходов MSTP

При вычислении активной топологии связующего дерева IST и MSTI используется механизм счетчика переходов (Hop count), определяющий максимальное число переходов между устройствами внутри региона, прежде чем кадр BPDU будет отброшен. Значение

счетчика переходов устанавливается региональным корневым мостом MSTI или CIST и уменьшается на 1 каждым портом коммутатора, получившим кадр BPDU. После того как значение счетчика станет равным 0, кадр BPDU будет отброшен и информация, хранимая портом, будет помечена как устаревшая.
Пользователь может установить значение счетчика переходов от 1 до 20. Значение по умолчанию — 20.

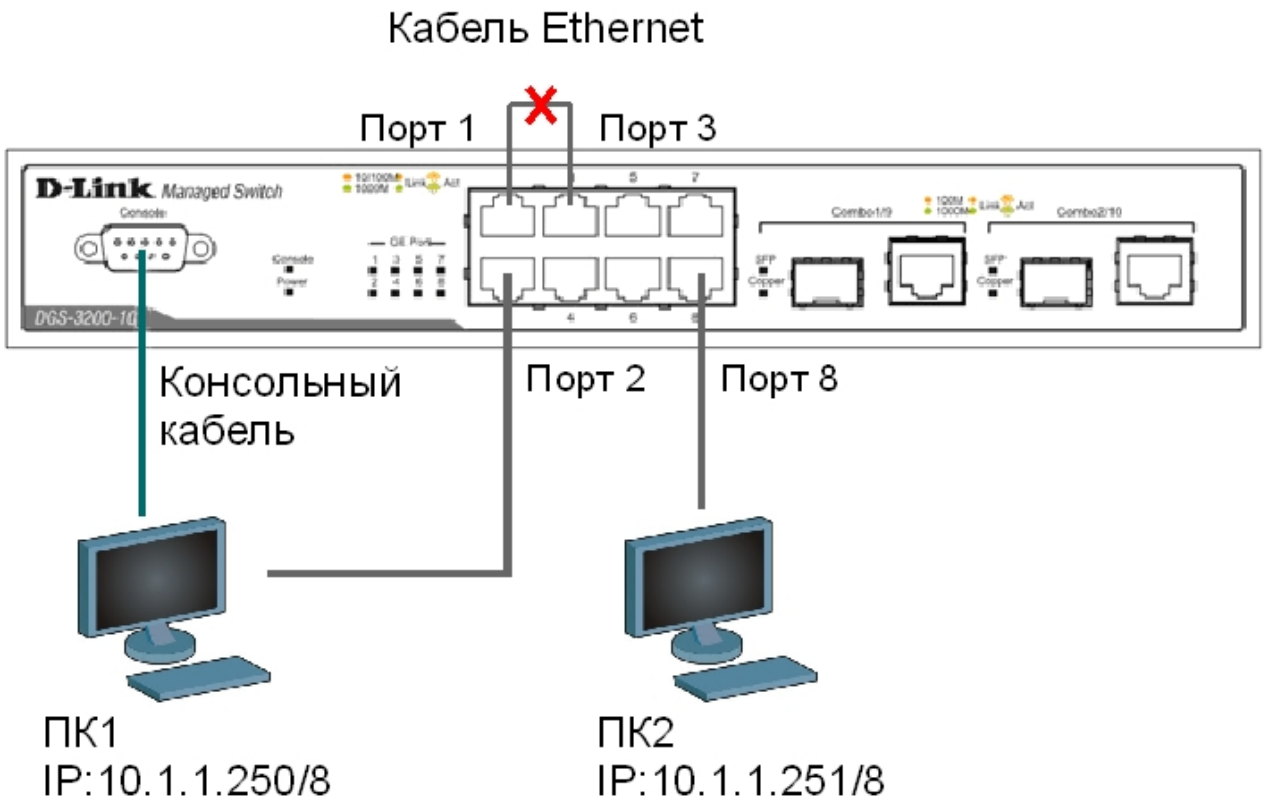
Цель: понять функционирование протоколов связующего дерева и изучить их настройку на коммутаторах D-Link.

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-10 или DGS-3200-10	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	8 шт.

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

Схема 7.1:



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

```
reset config
```

Соедините кабелем Ethernet порты 1 и 3 коммутатора.

Просмотрите статистику о пакетах, передаваемых через порт 1:

```
show packet ports 1
```

Что вы наблюдаете? Возник широковещательный шторм? Почему?

_____
_____
_____

Выполните на рабочей станции ПК 1 команду:
```
ping 10.1.1.251 -t
```

Выполните на рабочей станции ПК 2 команду:
```
ping 10.1.1.250 -t
```

Что вы наблюдаете? Объясните почему.

_____
_____
_____

Посмотрите загрузку ЦПУ (CPU):
```
show utilization cpu
```

Просмотрите загрузку порта:
```
show utilization ports
```

Отсоедините кабель от портов 1 и 3, удалите петлю.

Оставте порты 1,3,5,9 в default VLAN, а порты 2,4,6,8 поместите в новую VLAN:
```
config vlan default delete 2,4,6,8

create vlan v2 tag 2
config vlan v2 add untagged 2,4,6,8
```

Проверьте настройки VLAN:
```
show vlan
```

Просмотрите статистику о пакетах, передаваемых через порт 1:
```
show packet ports 1
```

Соедините кабелем порты 1 и 3.

Что вы наблюдаете? Почему нет широковещательного шторма?

_____
_____

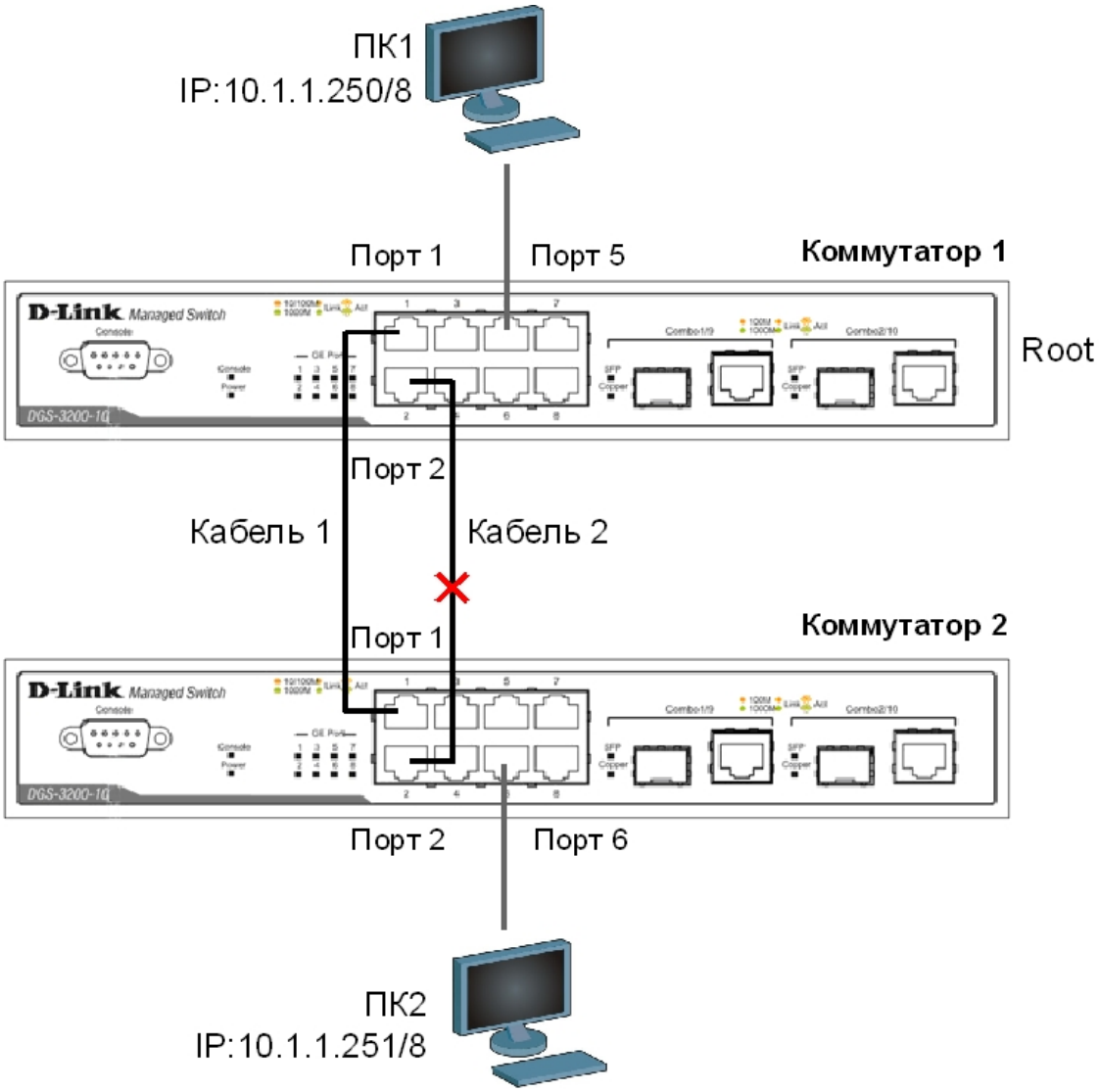
Выполните на рабочей станции ПК 1 команду:
```
ping 10.1.1.251
```

Что вы наблюдаете? Объясните почему.

_____
_____
_____

7.2. Настройка протокола RSTP

Схема 7.2:



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

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 наименьшее значение приоритета, чтобы он мог быть выбран корневым мостом (приоритет по умолчанию = 32768):
```
config stp priority 8192 instance_id 0
```

Просмотрите выполненные изменения:
```
show stp instance 0
```

Назначьте порты 3-10 граничными портами:
```
config stp ports 3-10 edge true
```

Активизируйте протокол связующего дерева на портах:
```
config stp ports 1-10 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 3-10 граничными портами:
```
config stp ports 3-10 edge true
```

Активизируйте протокол связующего дерева на портах:
```
config stp ports 1-10 state enable
```

Соедините между собой порты 1 и порты 2 коммутаторов 1 и 2 с помощью кабелей, как показано на схеме 7.2.

Проверьте настройки RSTP, состояние портов и их роли у обоих коммутаторов:
`show stp ports x, где x- номер порта`

Вопросы:
Какой коммутатор является корневым? _____
Какие порты являются заблокированными? _____
Какая роль у заблокированных портов? _____
_____

Выполните продолжительный тест ping от компьютера ПК1 до ПК2 и наоборот:
```
На ПК1, ping 10.1.1.250 –t
На ПК2, ping 10.1.1.251 –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
```

Выполните продолжительный ping от компьютера ПК1 до ПК2 и наоборот:

```
На ПК1, ping 10.1.1.250 –t
На ПК2,ping 10.1.1.251 –t
```

Отсоедините кабель от корневого порта.

Что происходит с тестом ping? _____

Превышен ли интервал ожидания для запроса?_____

Как долго пришлось ждать до появления ответа? _____

7.3. Настройка защиты от подключения несанкционированных корневых коммутаторов

ЗАДАНИЕ

Настройте на коммутаторе 1 защиту от подключения несанкционированных корневых коммутаторов.

Отключите кабели, соединяющие коммутаторы.

Настройка коммутатора 1

Включите на портах 1-4 коммутатора защиту от перевыборов корневого коммутатора, активизировав параметр restricted_role:

```
config stp ports 1-4 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 1 обоих коммутаторов кабелем Ethernet.

На коммутаторе 1 посмотрите log-файл.

```
show log
```

Что вы наблюдаете? Запишите.

_____

_____

Какой коммутатор является корневым?_____
Какая роль у порта 1 коммутатора 1?_____

На коммутаторе 1 переключите кабель из порта 1 в порт 5.

На коммутаторе 1 посмотрите log-файл.
```
show log
```

Что вы наблюдаете? Запишите.

_____
_____

Какой коммутатор является корневым?_____
Какая роль у порта 5 коммутатора 1? _____

7.4. Настройка защиты от получения ложных пакетов об изменении топологии

ЗАДАНИЕ

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

Отключите кабели, соединяющие коммутаторы.

Настройка коммутатора 1
Включите на портах 1-2 коммутатора функцию защиты от получения ложных TCN BPDU:
```
config stp ports 1-2 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 порты 1 и порты 2 коммутаторов 1 и 2 с помощью кабелей, как показано на схеме 7.2.

Соедините порт 5 и порт 7 коммутатора 2 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 1-2 restricted_tcn false
```

Отключите кабель, соединяющий порты 5 и 7 коммутатора 2.

На коммутаторе 1 посмотрите log-файл.

```
show log
```

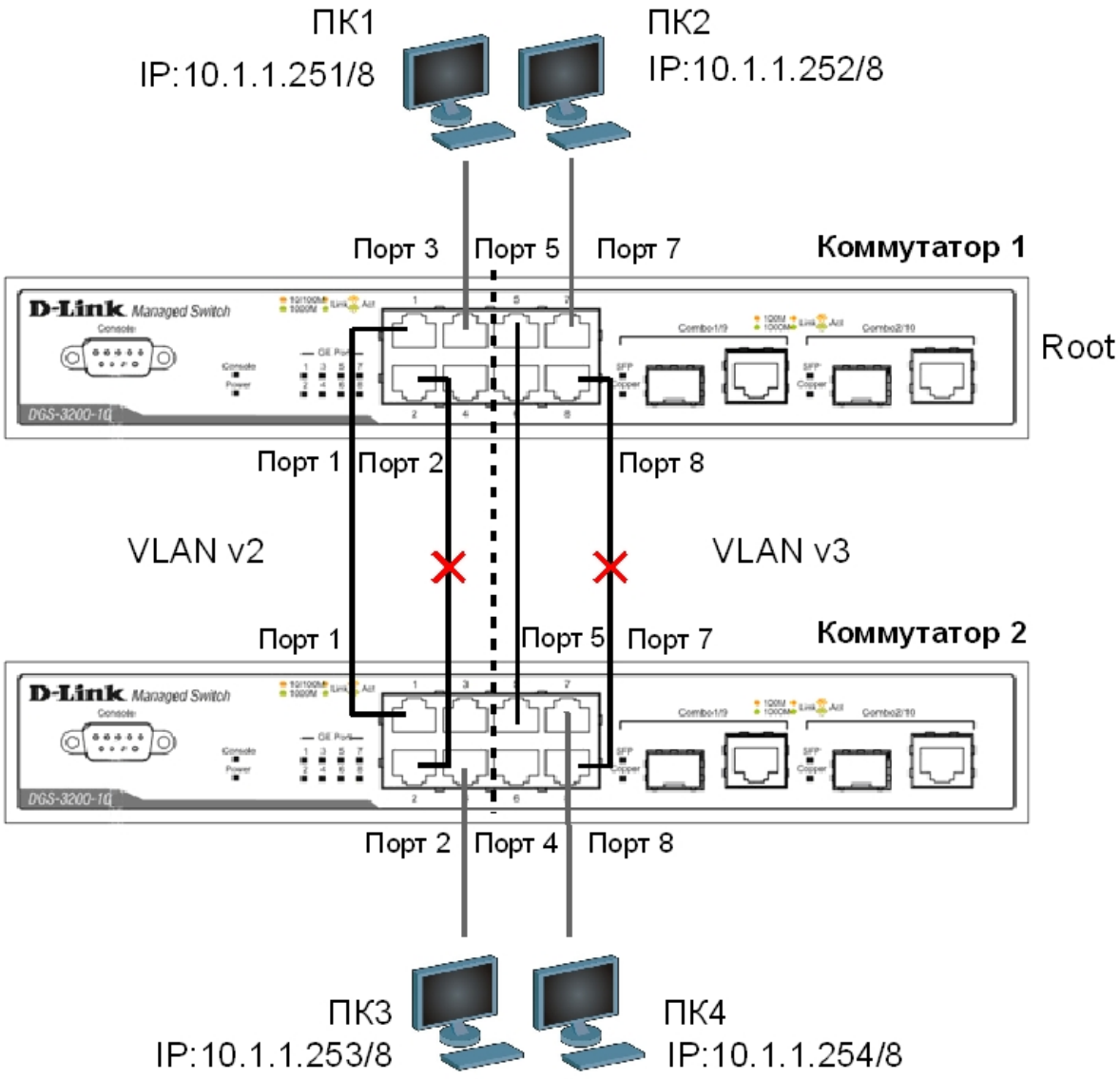
Что вы наблюдаете? Запишите.

_____

_____

7.5. Настройка протокола MSTP

Схема 7.3:



Примечание: не соединяйте коммутаторы одновременно всеми кабелями во время настройки.

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 1-8
```

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

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

Проверьте настройки VLAN:

```
show vlan
```

Включите протокол связующего дерева на коммутаторе:

```
enable stp
```

Проверьте текущую конфигурацию протокола связующего дерева:

```
show 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 1-4 и 5-8 как граничные порты:

```
config stp ports 1-4 edge true
config stp ports 5-8 edge true
```

Активизируйте протокол связующего дерева на портах:

```
config stp ports 1-8 state enable
```

Настройка коммутатора 2

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

```
config vlan default delete 1-8
```

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

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

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.

_____
_____
_____

Проверьте текущую конфигурацию протокола связующего дерева:

```
show stp
```

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 1-4 и 5-8 как граничные порты:

```
config stp ports 1-4 edge true
config stp ports 5-8 edge true
```

Активизируйте протокол связующего дерева на портах:
`config stp ports 1-8 state enable`

Подключите коммутаторы как показано на схеме 7.3.

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 №8. 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.

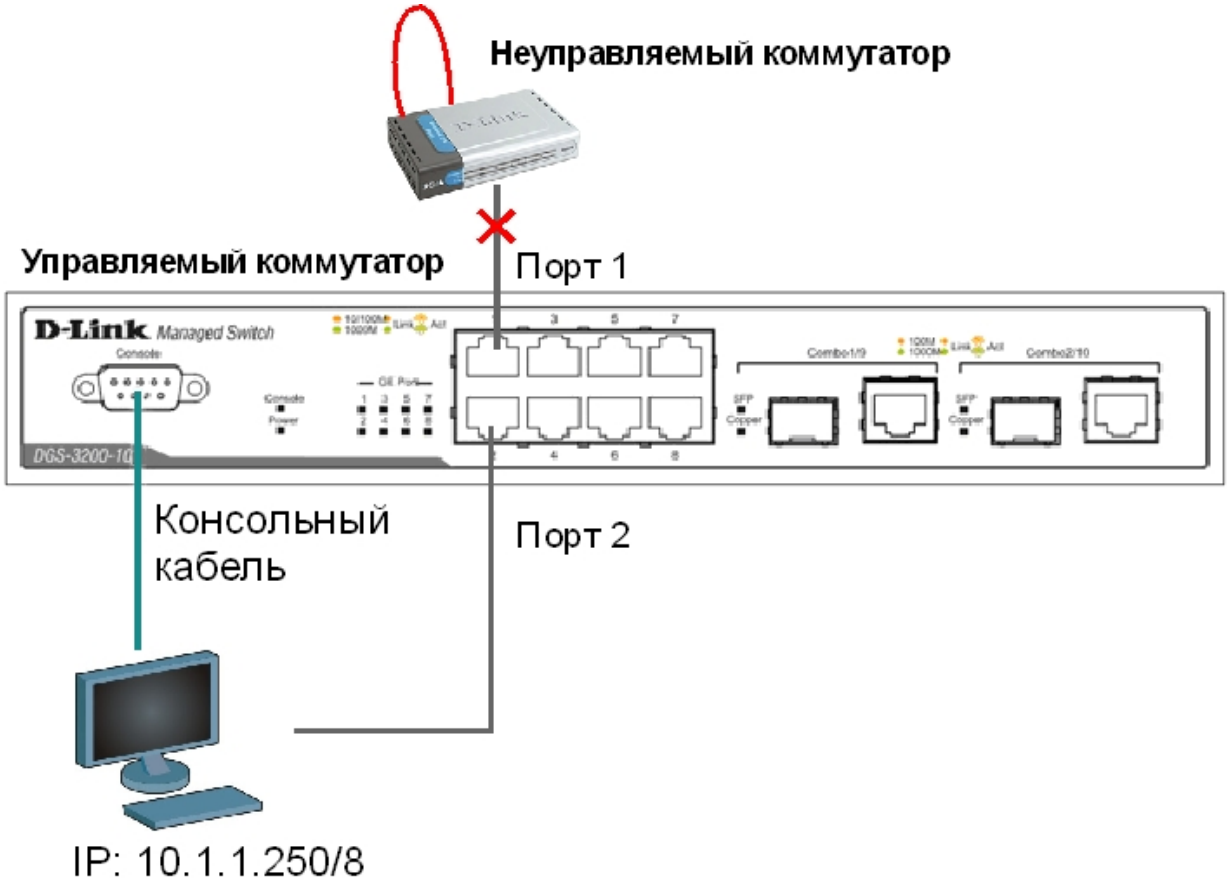
Оборудование (на 2 рабочих места):

Коммутатор DES-3200-10 или DGS-3200-10	2 шт.
Рабочая станция	2 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.
Неуправляемый коммутатор	1 шт.

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

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

Схема 8.1:



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 1-10 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.

Проверьте текущую конфигурацию функции LBD:

```
show loopdetect
```

Подключите неуправляемый коммутатор с петлей к управляемому коммутатору, как показано на схеме 8.1.

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

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.

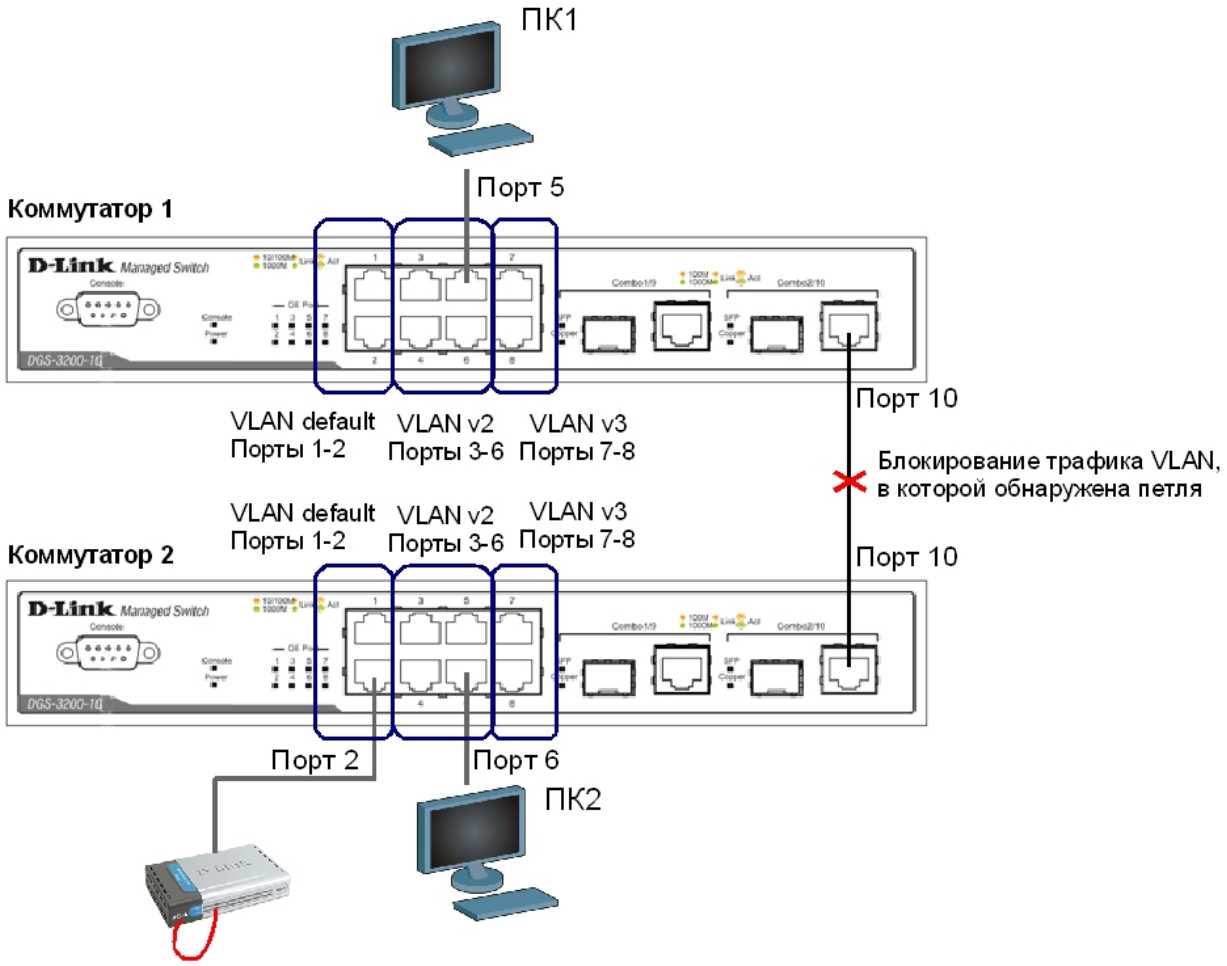
_____
_____

Отключите неуправляемый коммутатор с петлей от управляемого коммутатора.

8.2. Настройка функции LoopBack Detection Independent STP в режиме VLAN-Based (для версии LBD 4.00).

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 8.2:



Примечание: если при передаче пакетов порт 10 коммутатора получит ECTP-пакет, который отправлял сам, передача трафика в VLAN default, из которой он пришел, 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 3-10
```

Создайте VLAN v2 и v3:

```
create vlan v2 tag 2
create vlan v3 tag 3
```

Добавьте в созданные VLAN v2 и v3 немаркированные порты. Добавьте порт 10 в VLAN default, v2 и v3 в качестве маркированного:

```
config vlan default add tagged 10
config vlan v2 add untagged 3-6
config vlan v2 add tagged 10
config vlan v3 add untagged 7-8
config vlan v3 add tagged 10
```

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
```

Повторите настройку для коммутатора 2.

Проверьте текущую конфигурацию функции LBD:

```
show loopdetect
```

Подключите неуправляемый коммутатор с петлей к коммутатору 2, как показано на схеме 8.2.

Посмотрите, обнаружена ли петля на коммутаторах 1 и 2:

```
show loopdetect ports all
```

Что вы наблюдаете? Запишите.
Коммутатор 1 _____
Коммутатор 2 _____

Проверьте log-файл:

```
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 №9. 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.

Включенные 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 (установлено 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, путем отправки управляющих кадров протокола LACP непосредственно подключенным 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.

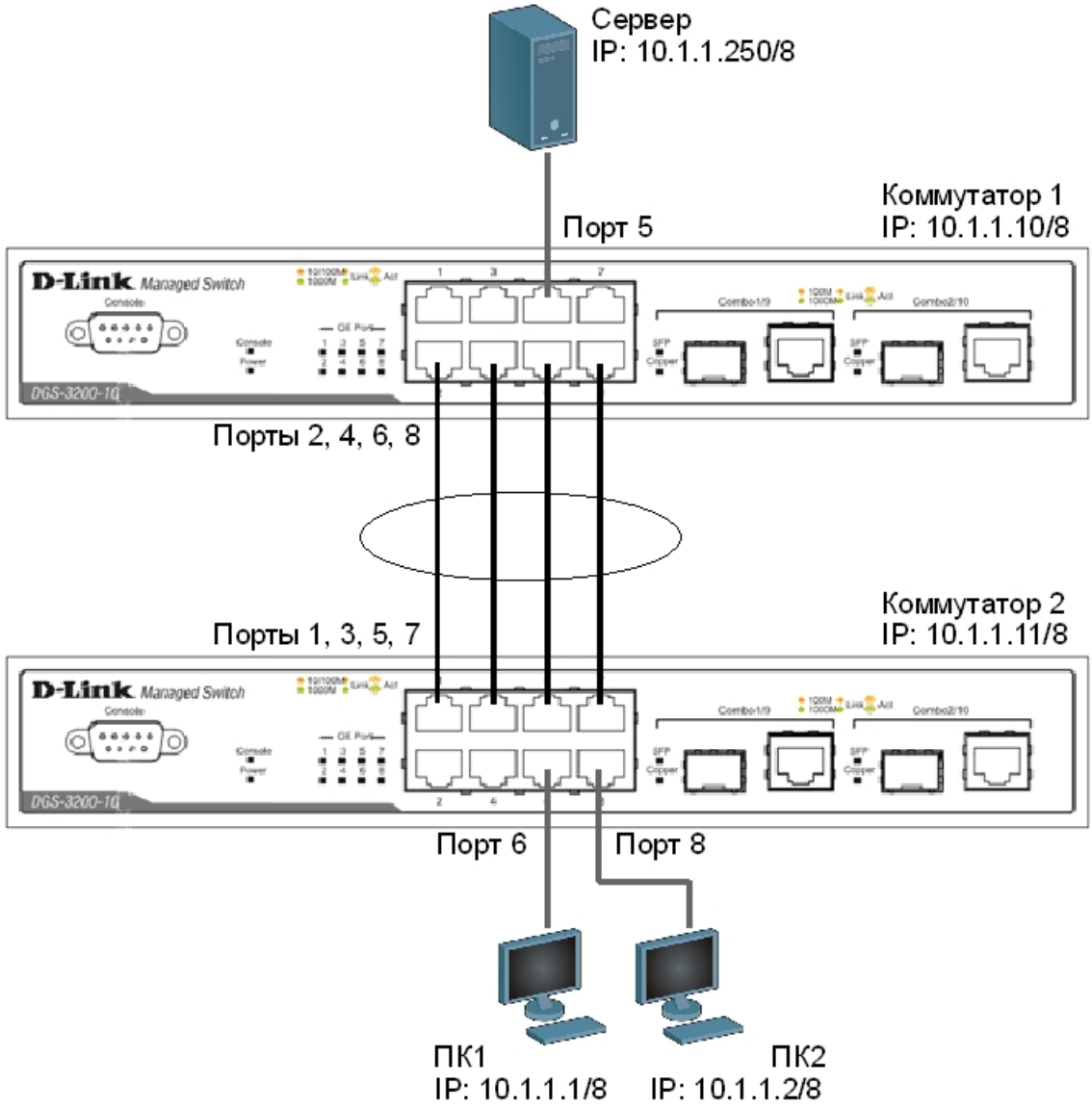
Для создания искусственной нагрузки на канал связи между коммутаторами, при выполнении лабораторной работы будет использоваться программа iperf. Версия для ОС Windows доступна по адресу ftp://ftp.dlink.ru/pub/Trainings/, исходные коды версии для Unix-подобных ОС доступны по адресу http://sourceforge.net/projects/iperf.

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

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-10 или DGS-3200-10	2 шт.
Рабочая станция	3 шт.
Консольный кабель	2 шт.
Кабель Ethernet	7 шт.

Схема 9:



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 2, 4, 6, 8 в группу агрегирования каналов и выберите порт 2 в качестве мастера-порта:

```
config link_aggregation group_id 1 master_port 2 ports 2,4,6,8
state enabled
```

Настройте порты на работу в пассивном режиме:

```
config lacp_port 2,4,6,8 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, 3, 5, 7 в группу агрегирования каналов и выберите порт 1 в качестве мастера-порта:
```
config link_aggregation group_id 1 master_port 1 ports 1,3,5,7
state enabled
```

Настройте порты на работу в активном режиме:
```
config lacp_port 1,3,5,7 mode active
```

Проверьте выполненные настройки:
```
show link_aggregation
```

Проверьте режим работы LACP на портах коммутаторов:
```
show lacp_port
```

Запустите на ПК1 и ПК2 программу iperf:
```
iperf -c 10.1.1.250 -i 1 -t 1000 -r -u -b10M -P5
```

Запустите на сервере: `iperf –s -u`

Ключ «-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 UDP трафиком; «-b10M» задает полосу генерации трафика в 10 Мбит/с; «-P5» запускает одновременно 5 тестовых потоков.

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 №10. Списки управления доступом (Access Control List)

Списки управления доступом (Access Control List, ACL) являются средством фильтрации потоков данных без потери производительности, т.к. проверка содержимого пакетов данных выполняется на аппаратном уровне. Фильтруя потоки данных, администратор может ограничить типы приложений, разрешенных 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, путем 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, определенными 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.

В коммутаторах D-Link существует три типа профилей доступа: Ethernet, IP и Packet Content Filtering (фильтрация по содержимому пакета).

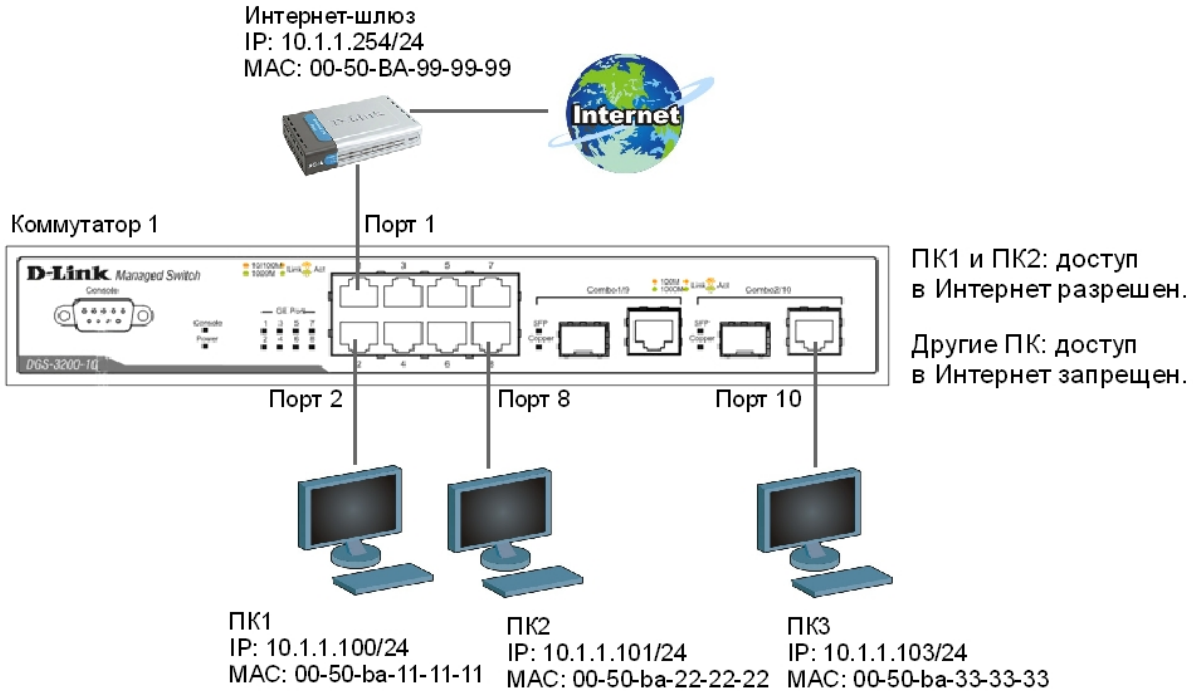
Цель: на коммутаторе D-Link настроить списки управления доступом, использую в качестве критериев фильтрации MAC- и IP- адреса.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-10 или DGS-3200-10	1 шт.
Рабочая станция	3 шт.
Консольный кабель	1 шт.
Кабель Ethernet	3 шт.
Интернет-шлюз	1 шт.

10.1.Настройка ограничения доступа пользователей в Интернет по MAC-адресу

Схема 10.1:



ЗАДАНИЕ

Разрешить пользователям ПК1 и ПК2 доступ в Интернет, остальным пользователям – запретить. Пользователи идентифицируются по MAC-адресам их компьютеров.

Правила:
Правило 1:
Если MAC-адрес назначения = MAC-адресу Интернет-шлюза и MAC-адрес источника = ПК1, разрешить;
Если MAC-адрес назначения = MAC-адресу Интернет-шлюза и MAC-адрес источника = ПК2, разрешить;
Правило 2:
Если MAC-адрес назначения = MAC-адресу Интернет-шлюза, запретить;
Правило 3:
Иначе, по умолчанию разрешить доступ всем узлам.

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 и Интернет-шлюза.

Правило 1
Создайте профиль доступа 10:

```
create access_profile ethernet source_mac FF-FF-FF-FF-FF-FF
destination_mac FF-FF-FF-FF-FF-FF profile_id 10
```

Создайте правило для профиля 10, разрешающее доступ ПК1, подключенного к порту 2, в Интернет:

```
config access_profile profile_id 10 add access_id 11 ethernet
source_mac 00-50-ba-11-11-11 destination_mac 00-50-ba-99-99-99
port 2 permit
```

Создайте правило для профиля 10, разрешающее доступ ПК2, подключенного к порту 8, в Интернет:

```
config access_profile profile_id 10 add access_id 12 ethernet
source_mac 00-50-ba-22-22-22 destination_mac 00-50-ba-99-99-99
port 8  permit
```

Правило 2

Создайте профиль доступа 20:

```
create access_profile ethernet destination_mac FF-FF-FF-FF-FF-FF
profile_id 20
```

Создайте правило для профиля 20, запрещающее доступ остальным пользователям в Интернет:

```
config access_profile profile_id 20 add access_id 21 ethernet
destination_mac 00-50-ba-99-99-99 port 1-10 deny
```

Примечание: созданное правило запретит прохождение кадров, содержащих MAC-адрес назначения равный MAC-адресу Интернет-шлюза на всех портах коммутатора. Если данное правило необходимо применить на одном из портов, в конфигурации указывается определенный порт, к которому подключена станция, трафик которой необходимо блокировать.

Правило 3

Разрешите все остальное:

Выполняется по умолчанию

Проверьте созданные профили ACL:

```
show access_profile
```

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

_____

Подключите станции ПК1 и ПК2, как показано на схеме 10.1.

Протестируйте соединение до Интернет-шлюза командой ping.

Что вы наблюдаете?

_____

_____

Подключите еще одну рабочую станцию, или подключите ПК1 и ПК2 к другим портам и попробуйте получить доступ к Интернет-шлюзу.

Что вы наблюдаете? Запишите, почему так происходит?

_____

_____

_____

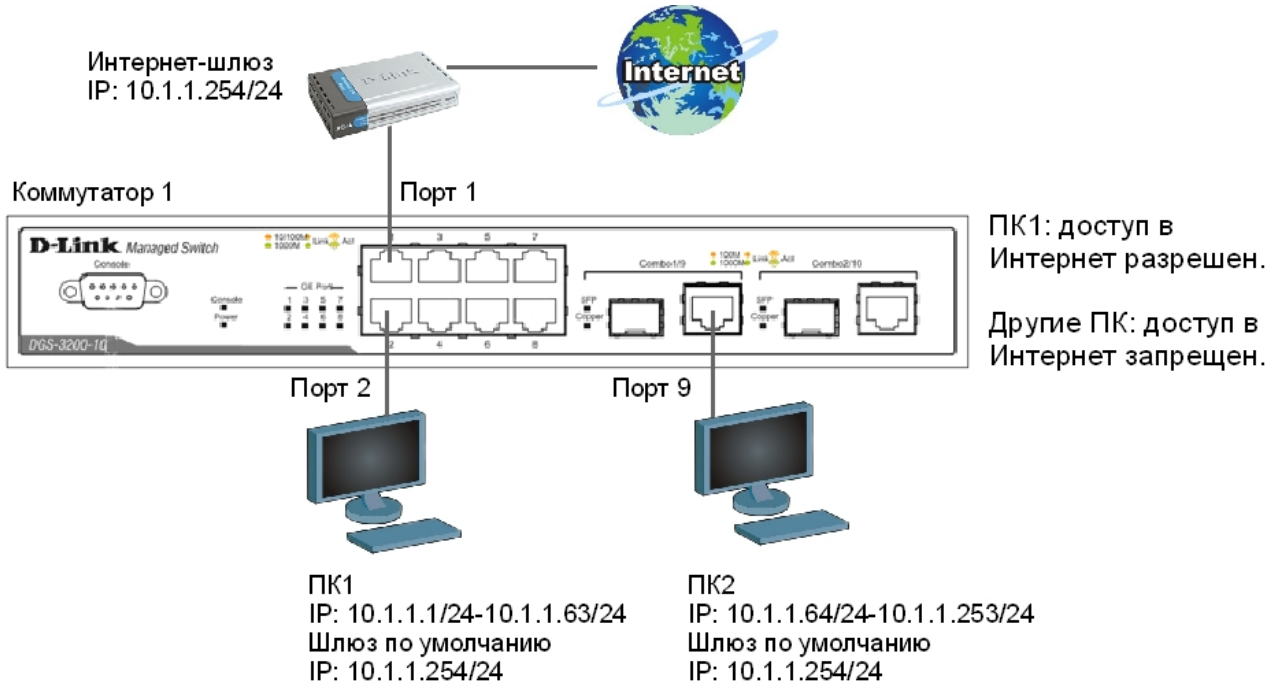
_____

Удалите правило из профиля (например, для отключения ПК2 от Интернет):
```
config access_profile profile_id 10 delete access_id 12
```

Удалите профиль ACL (например, разрешающий доступ в Интернет станциям ПК1 и ПК2):
```
delete access_profile profile_id 10
```

10.2. Настройка ограничения доступа пользователей в Интернет по IP-адресам

Схема 10.2:



ЗАДАНИЕ

Разрешить доступ в Интернет пользователям с IP-адресами с 10.1.1.1/24 по 10.1.1.63/24. Остальным пользователем сети 10.1.1.0/24, с адресами не входящими в разрешенный диапазон, доступ в Интернет запретить.

Правила:
Правило 1:
Если IP-адрес источника = IP-адресам из диапазона с 10.1.1.1 по 10.1.1.63 (подсеть 10.1.1.1/26), разрешить;
Правило 2:
Если MAC-адрес назначения = MAC-адресу Интернет-шлюза, запретить;
Правило 3:
Иначе, по умолчанию разрешить доступ всем узлам.

Перед выполнением задания удалите последний профиль из предыдущего задания:
```
delete access_profile profile_id 20
```

Убедитесь, что больше не осталось профилей:
```
show access_profile
```

Правило 1.
Создайте профиль доступа с номером 10, разрешающий доступ для подсети 10.1.1.0/26 (узлам с 1 по 63):

```
create access_profile ip source_ip_mask 255.255.255.192 profile_id 10
```

Создайте правило для профиля доступа 10:

```
config access_profile profile_id 10 add access_id 11 ip source_ip 10.1.1.0 port 1-10 permit
```

Примечание: созданное правило разрешает прохождение трафика IP-подсети 10.1.1.0/26 на всех портах коммутатора. Если данное правило необходимо применить на одном из портов, в конфигурации указывается определенный порт, к которому подключена станция, чей трафик необходимо разрешить.

Правило 2
Создайте профиль доступа 40:

```
create access_profile ethernet destination_mac FF-FF-FF-FF-FF-FF profile_id 40
```

Внимание! Замените указанный в команде MAC-адрес на реальный MAC-адрес Интернет-шлюза.

Создайте правило для профиля доступа 40, запрещающее остальным станциям подключаться к Интернет-шлюзу:

```
config access_profile profile_id 40 add access_id 41 ethernet destination_mac 00-50-ba-99-99-99 port 1-10 deny
```

Правило 3
Разрешите все остальное:
Выполняется по умолчанию

Проверьте созданные профили:

```
show access_profile
```

Подключите рабочие станции ПК1 (адрес из диапазона 10.1.1.1-63/24) и ПК2 (адрес из диапазона 10.1.1.64-253/24) к коммутатору.

Протестируйте командой ping соединение до Интернет-шлюза 10.1.1.254/24.

Что вы наблюдаете? Запишите.

_____

_____

Удалите профиль ACL (например, профиль 10).

```
delete access_profile profile_id 10
```

Проверьте соединение до Интернет-шлюза командой:

```
ping 10.1.1.254
```

Что вы наблюдаете? Запишите.

_____

_____

Лабораторная работа №11. 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 определенными 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) – занесенные 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) – занесенные в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером Aging Time и будут удалены.

  Если состояние канала связи на подключенном 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) – занесенные в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

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

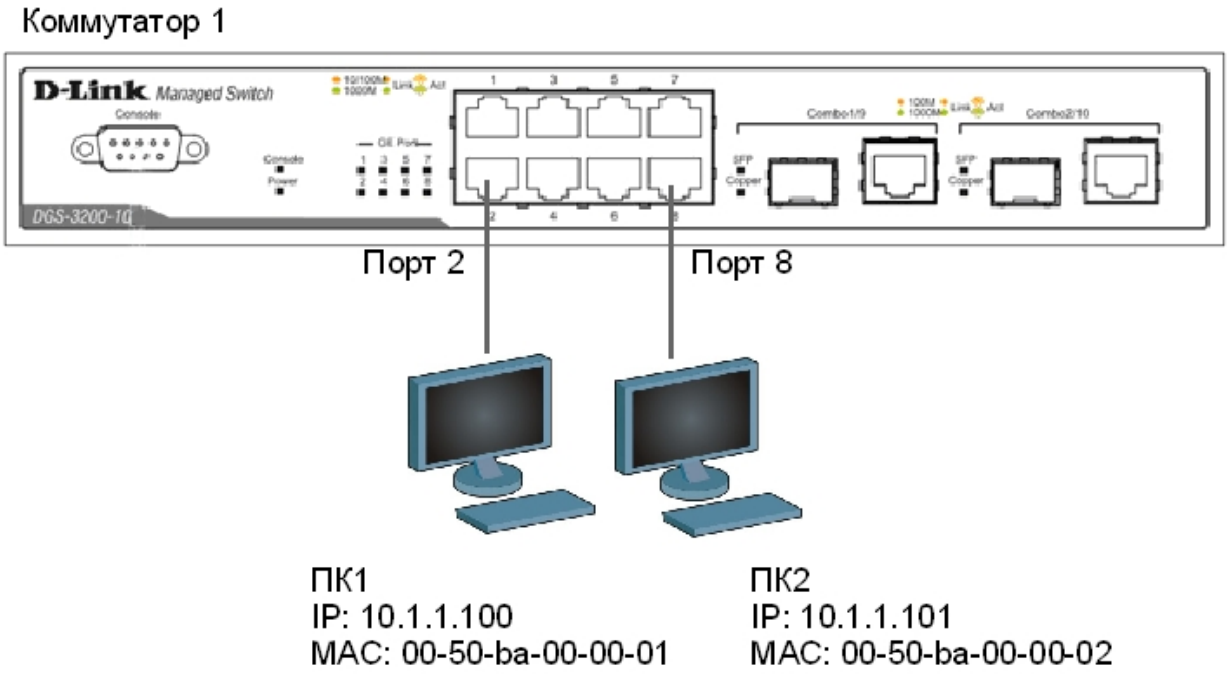
Используя функцию Port Security можно полностью запретить динамическое изучение MAC-адресов указанными или всеми портами коммутатора. В этом случае доступ к сети получат только те пользователи, MAC-адреса которых указаны в статической таблице коммутации.

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-3200-10 или DGS-3200-10	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.

Схема 11:



11.1. Управление количеством подключаемых к портам коммутатора пользователей, путем 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 всеми портами 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 8 коммутатора соответственно.

Посмотрите MAC-адреса, которые стали известны портам 2 и 8:

```
show fdb port 2
show fdb port 8
```

Проверьте, соответствуют ли зарегистрированные адреса адресам рабочих станций:_____

Проверьте информацию о настройках Port Security на портах коммутатора:

```
show port_security ports 1-10
```

Настройте запись в log-файл 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 8, а ПК2 к порту 2.

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте информацию в log-файле 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-port?
_____
_____

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 1-10
```

Какой вы сделаете вывод? Сохраняется информации 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 disable 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 1-10
```

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 1-10 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 путем создания статических записей в таблице коммутации.

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

Отключите рабочие станции от коммутатора.

Сбросьте настройки коммутатора к заводским настройкам командой:

```
reset system
```

Активизируйте функцию Port Security на всех портах и запретите изучение MAC-адресов (параметр *max_learning_addr* установить равным 0):

```
config port_security ports 1-10 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, подключенных к портам 2 и 8.

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 8
```

Проверьте созданные статические записи в таблице коммутации:
```
show fdb
```

Проверьте информацию о настройках Port Security на портах коммутатора:
```
show port_security ports 1-10
```

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 №12. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding

Функция IP-MAC-Port Binding (IMPB), 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 MAC-IP-порт будет отличаться от параметров заранее сконфигурированной записи, то коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «черный 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 занесен в таблицу коммутации с отметкой «Drop» (Отбрасывать). Если все параметры совпадают, MAC-адрес узла будет занесен в таблицу коммутации с отметкой «Allow» (Разрешен).

При функционировании в *ACL mode*, коммутатор на основе предустановленного администратором «белого листа» IMPB 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 включенной функцией IMPB (администратору не требуется создавать записи вручную). Таким образом, коммутатор автоматически создает «белый лист» IMPB в таблице коммутации или аппаратной таблице ACL (если режим ACL включен). При этом для обеспечения корректной работы, сервер DHCP должен быть подключен к доверенному порту с выключенной функцией IMPB. Администратор может ограничить максимальное количество создаваемых в процессе автоизучения записей IP-MAC на порт, т.е. ограничить для каждого порта с активизированной функцией IMPB 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 IMPB на порте администратор должен указать режим его работы:

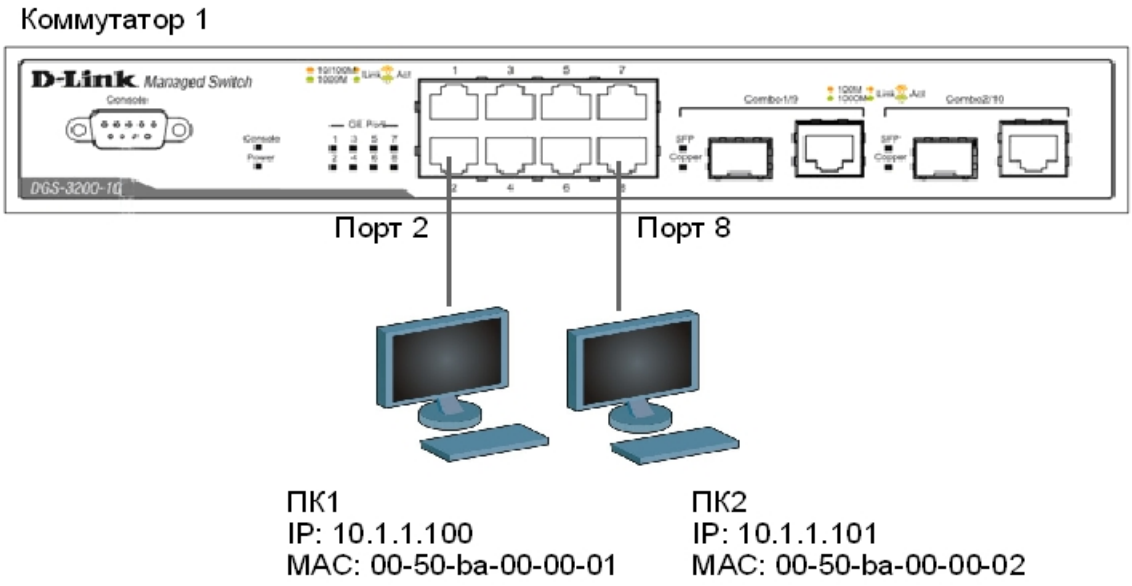
- **Strict Mode** – в этом режиме порт по умолчанию заблокирован.
- **Loose Mode** – в этом режиме порт по умолчанию открыт.

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-3200-10 или DGS-3200-10	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.

Схема 12:



12.1. 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-MAC-адрес рабочей станции ПК1 с портом 2 (по умолчанию режим работы функции ARP):

```
create address_binding ip_mac ipaddress 10.1.1.100 mac_address 00-50-ba-00-00-01 ports 2
```

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

```
create address_binding ip_mac ipaddress 10.1.1.101 mac_address 00-50-ba-00-00-02 ports 8
```

Активизируйте функцию на портах 2 и 8 (по умолчанию режим работы портов Strict):

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

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 12.

Проверьте доступность соединения между рабочими станциями командой ping:

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

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

```
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 из списка заблокированных адресов:

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

Удалите запись IP-MAC-Port Binding:

```
delete address_binding ip_mac ipaddress 10.1.1.100 mac_address 00-
50-ba-00-00-01
```

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

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

12.2. Настройка работы функции IP-MAC-Port Binding в режиме ACL

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

```
create address_binding ip_mac ipaddress 10.1.1.100 mac_address 00-
50-ba-00-00-01 ports 2
```

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

```
create address_binding ip_mac ipaddress 10.1.1.101 mac_address 00-
50-ba-00-00-02 ports 8
```

Активизируйте функцию на портах 2 и 8 (по умолчанию режим работы портов Strict), включите режим *allow_zeroip*, благодаря которому коммутатор не будет блокировать узлы, отправляющие ARP-пакеты с IP-адресом источника 0.0.0.0, и установите работу функции IMPB в режиме ACL:

```
config address_binding ip_mac ports 2,8 state enable allow_zeroip
enable mode acl
```

Проверьте созданные записи IP-MAC-Port Binding:

```
show address_binding ip_mac
```

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 12.

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 System 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 10.1.1.100 mac_address 00-50-ba-00-00-01

delete address_binding ip_mac ipaddress 10.1.1.101 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 state disable
```

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

Лабораторная работа №13. 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 приложения 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.

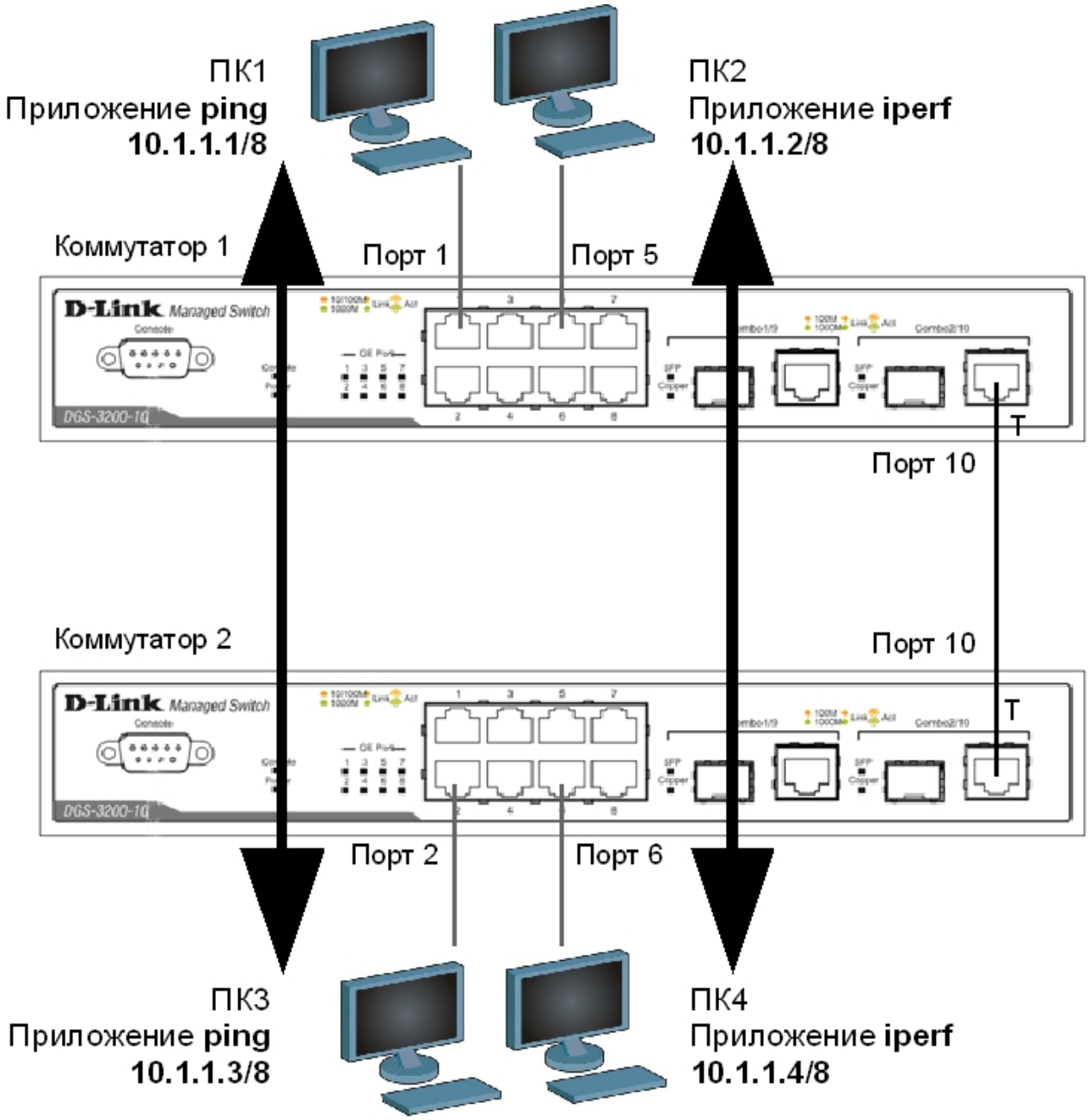
В лабораторной работе рассматривается следующий пример: в сети, имеющей явное «узкое» место, на рабочих станциях ПК1 и ПК3 выполняется тест ping друг на друга. Этому трафику необходимо обеспечить высокий приоритет обработки по сравнению с приложениями остальных станций, которые создают искусственную нагрузку на канал связи между коммутаторами с помощью программы iperf. Версия для ОС Windows доступна по адресу ftp://ftp.dlink.ru/pub/Trainings/, исходные коды версии для Unix-подобных ОС доступны по адресу http://sourceforge.net/projects/iperf.

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

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-10 или DGS-3200-10	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

Схема 13:



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 10 функцию bandwidth_control, ограничивающую прием и передачу данных скоростью 64 Кбит/с:

```
config bandwidth_control 10 rx_rate 64 tx_rate 64
```

Настройка коммутатора 2

Для создания «узкого» места, настройте на порте 10 функцию bandwidth_control, ограничивающую прием и передачу данных скоростью 64 Кбит/с:

```
config bandwidth_control 10 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:

_____
_____
_____

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 «-c ip-сервера -i 1 -t 1000 -r -u -b10M -P5» (в роли клиента):

```
iperf -c 10.1.1.2 -i 1 -t 1000 -r -u -b10M -P5
```

Ключ «-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 UDP трафиком; «-b10M» задает полосу генерации трафика в 10 Мбит/с; «-P5» запускает одновременно 5 тестовых потоков.

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

Собрав в течение 20-30 секунд статистику, посмотрите на ПК1 и ПК3, ПК2 и ПК4 информацию и запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они есть:

_____
_____
_____

Запишите примерную среднюю скорость, выводимую программой iperf на ПК4:

_____
_____
_____

Запишите ваши наблюдения, сравните их с результатами задания 1:

_____
_____
_____

ЗАДАНИЕ 3

Включите 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 неприоритизированные порты обоих коммутаторов.

Посмотрите текущие настройки приоритета по умолчанию на всех 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 добиться в нагруженном канале с включенной приоритизацией таких же параметров, что и в ненагруженном канале? Объясните почему?

_____
_____
_____

Лабораторная работа №14. Зеркалирование портов (Port Mirroring)

Коммутаторы улучшают производительность и надежность 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.

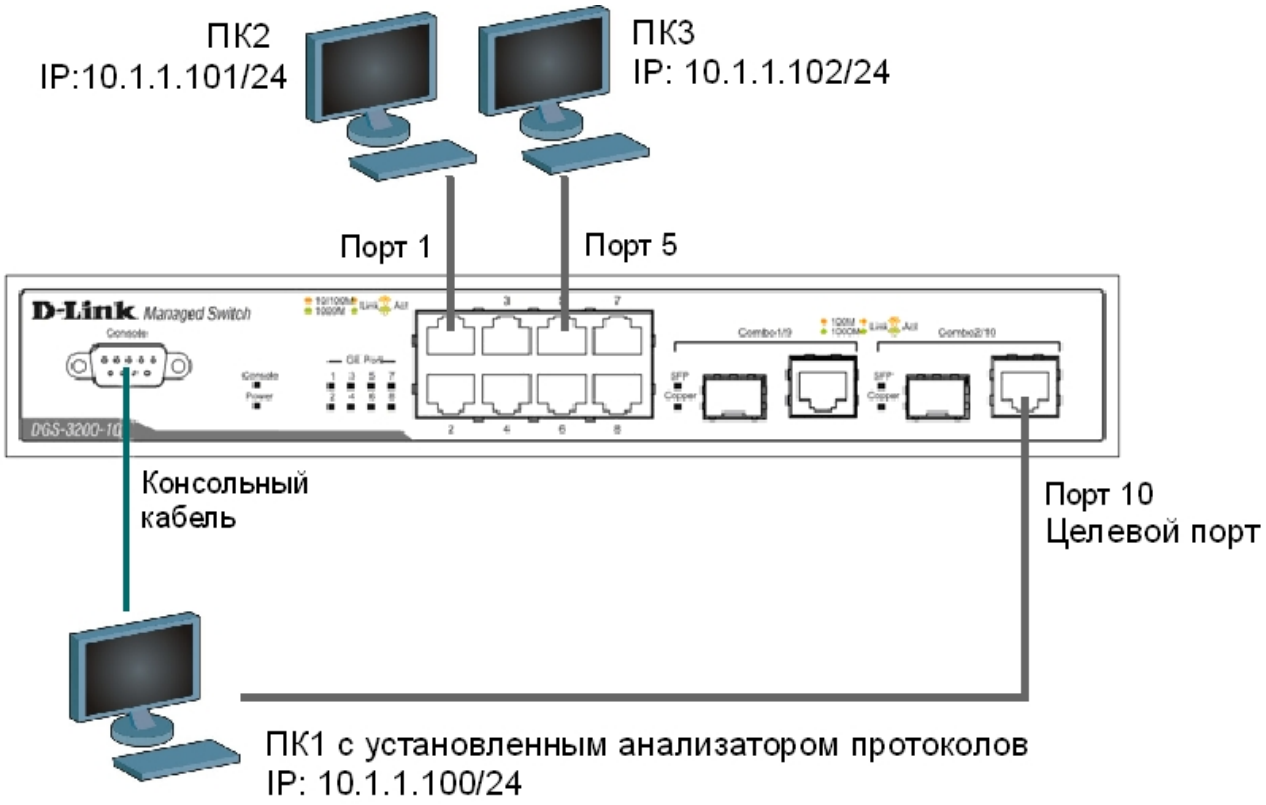
Функция Port Mirroring позволяет отображать (копировать) кадры, принимаемые и отправляемые портом-источником (Source port) на целевой порт (Target port) коммутатора, к которому подключено устройство мониторинга с целью анализа проходящих через интересующий порт пакетов.

Цель: изучить настройку функции зеркалирования портов.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-10 или DGS-3200-10	1 шт.
Рабочая станция	3 шт.
Консольный кабель	1 шт.
Кабель Ethernet	3 шт.

Схема 14:



Укажите порты, трафик которых будет пересылаться на целевой порт 10:

```
config mirror port 10 add source ports 1,5 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 (например,Wireshark).
www.wireshark.org — официальный сайт Wireshark.

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

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Что вы наблюдаете? Запишите.

_____
_____

Отключите функцию зеркалирования портов:
```
disable mirror
```

Проверьте настройки функции:
```
show mirror
```

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

Захватите и проанализируйте пакеты с помощью анализатора протоколов.

Что вы наблюдаете теперь? Объясните, почему так происходит?

_____
_____
_____
_____

Лабораторная работа №15. 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-3200-10 или DGS-3200-10	8 шт.
Коммутатор DGS-3612	2 шт.
Рабочая станция	10 шт.
Консольный кабель	10 шт.
Кабель Ethernet	25 шт.

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

```
reset config
```

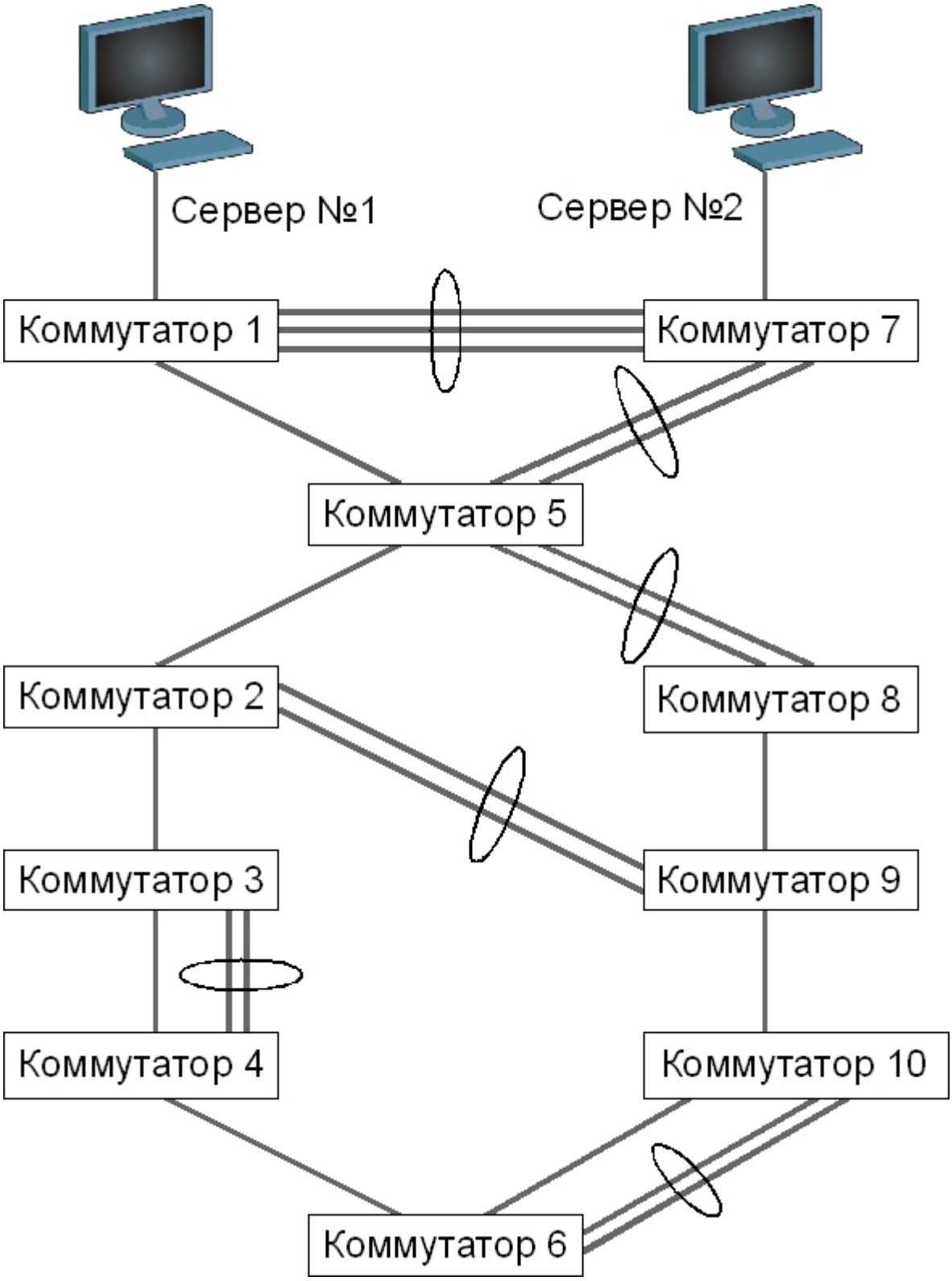
15.1 Подготовительная работа

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.

Схема 15:



Модели коммутаторов умышленно не обозначены на схеме. Местоположение каждого коммутатора необходимо определить самостоятельно. В роли серверов можно использовать две рабочие станции – 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). Все применяемые в схеме ПК должны быть размещены в индивидуальных VLAN.

Устройства всех VLAN должны иметь возможность обмениваться данными через маршрутизирующий коммутатор. Необходимо обеспечить приоритезацию 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.

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 интерфейсов маршрутизирующего коммутатора.
7. Выбрать в качестве корневого моста для протокола RSTP такой коммутатор, который обеспечит максимальную производительность сети.
8. Определить порты, на которых необходимо настроить приоритезацию.
9. Разработать ACL.
10. Выбрать порты, на которых будет включена функция LBD.
11. Определить пороговые значения для функции Safeguard Engine.

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.

15.2 Выполнение работы

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

15.3. 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 приоритезация должна обеспечивать беспрепятственное прохождение определенных видов трафика через любые сетевые интерфейсы.
7. Запрещенный 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 запрещенный для передачи трафик. Как можно проверить, на каком именно коммутаторе происходит блокировка?

_____
_____
_____

ЛАБОРАТОРНЫЕ РАБОТЫ, ВЫПОЛНЯЕМЫЕ ФАКУЛЬТАТИВНО

Лабораторная работа №16. Настройка ассиметричных VLAN

Основной целью асимметричных VLAN является более эффективное использование разделяемых ресурсов, таких как серверы или Интернет-шлюзы, в коммутируемых сетях. Данная функция реализована в программном обеспечении коммутаторов 2-го уровня D-Link. Асимметричные виртуальные локальные сети позволяют клиентам, принадлежащим разным VLAN и не поддерживающим тегирование 802.1Q взаимодействовать с сервером (или несколькими серверами) через один физический канал связи с коммутатором, не требуя использования внешнего маршрутизатора. Активизация функции Asymmetric VLAN в коммутаторе 2-го уровня позволяет сделать его немаркированные порты членами нескольких виртуальных локальных сетей. При этом рабочие станции остаются полностью изолированными друг от друга.

При активизации асимметричных VLAN, каждому порту коммутатора назначается уникальный PVID в соответствии с идентификатором VLAN, членом которой он является. При этом каждый порт, может получать кадры от VLAN по умолчанию.

Функция Asymmetric VLAN не поддерживается коммутаторами 3-го уровня. Организация обмена данными между устройствами различных VLAN не поддерживающих тегирование реализуется в таких коммутаторах с помощью маршрутизации и списков управления доступом (ACL), ограничивающих доступ устройств к сети.

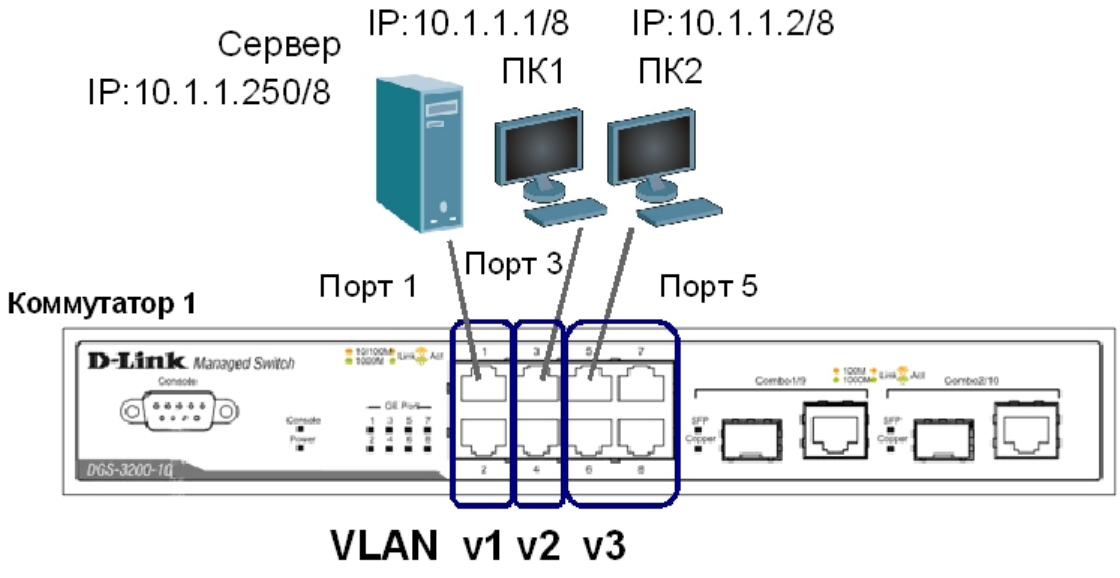
При использовании асимметричных VLAN не поддерживается IGMP Snooping.

Цель: изучить настройку асимметричных VLAN.

Оборудование (на 1 рабочее место):

Коммутатор DES-3200-10 или DGS-3200-10	1 шт.
Рабочая станция	3 шт.
Консольный кабель	1 шт.
Кабель Ethernet	3 шт.

Схема 16:



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

Включите функцию асимметричных VLAN:
```
enable asymmetric_vlan
```

Проверьте, все ли порты находятся в VLAN по умолчанию:
```
show vlan
```

Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными:
```
create vlan v2 tag 2
config vlan v2 add untagged 1-4

create vlan v3 tag 3
config vlan v3 add untagged 1-2, 5-8
```

Назначьте PVID немаркированным портам, созданных VLAN:
```
config gvrp 1-2 pvid 1
config gvrp 3-4 pvid 2
config gvrp 5-8 pvid 3
```

Проверьте доступность соединения между устройствами командой ping:
```
ping <IP-address>
```

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

Проверьте состояние PVID на всех портах коммутатора:
```
show gvrp
```

Лабораторная работа №17. Настройка сегментации трафика

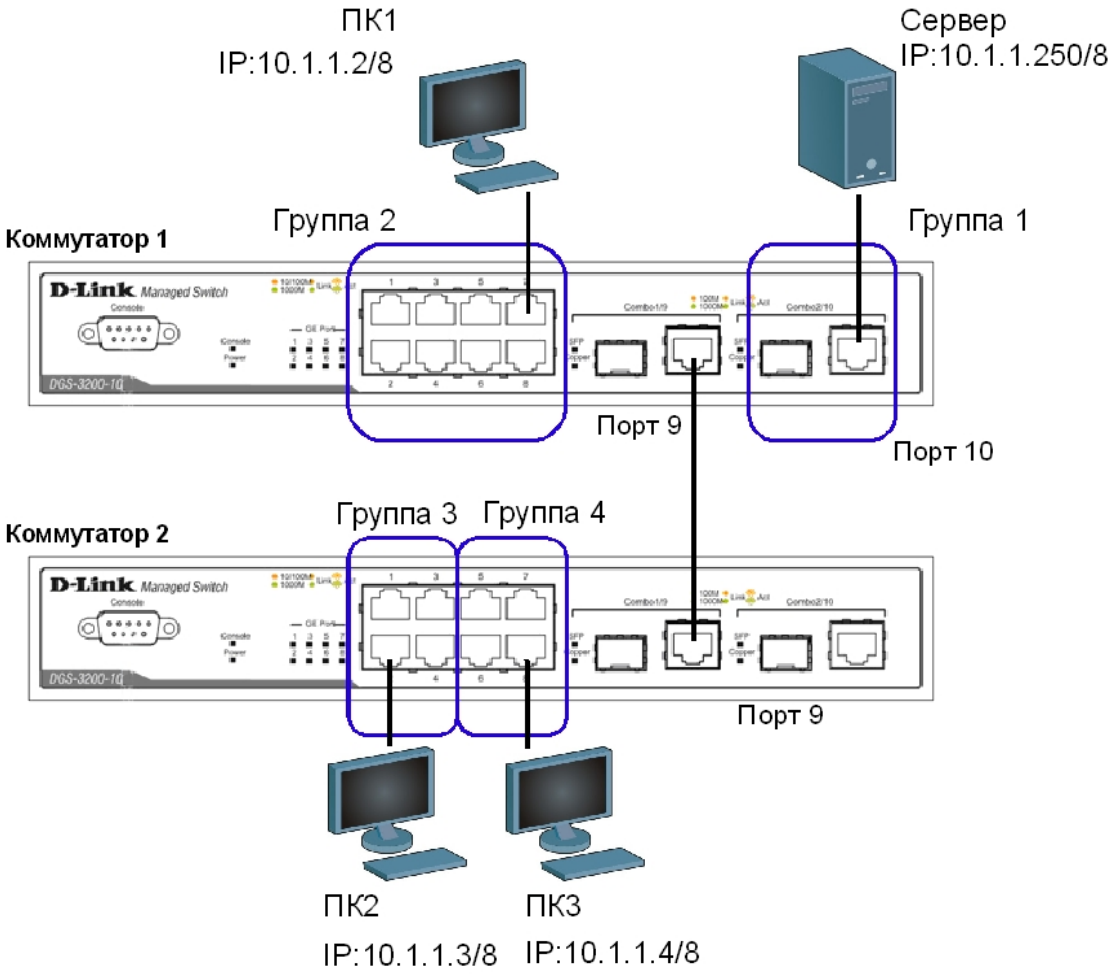
Функция Traffic Segmentation (сегментация трафика) служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для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

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

Оборудование (на 2 рабочих места):

Коммутатор DES-3200-10 или DGS-3200-10	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

Схема 17:



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 запрещен.

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

Настройте сегментацию трафика на коммутаторе 1:
```
config traffic_segmentation 1-8 forward_list 1-8,10
config traffic_segmentation 9 forward_list 10
config traffic_segmentation 10 forward_list 1-10
```

Настройте сегментацию трафика на коммутаторе 2:
```
config traffic_segmentation 1-4 forward_list 1-4,9
config traffic_segmentation 5-8 forward_list 5-8,9
config traffic_segmentation 9 forward_list 1-9
```

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 №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.

Функция Q-in-Q позволяет расширить доступное пространство идентификаторов и использовать до 4094 x 4094 = 16 760 836 уникальных виртуальных локальных сетей.

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 пришел 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):

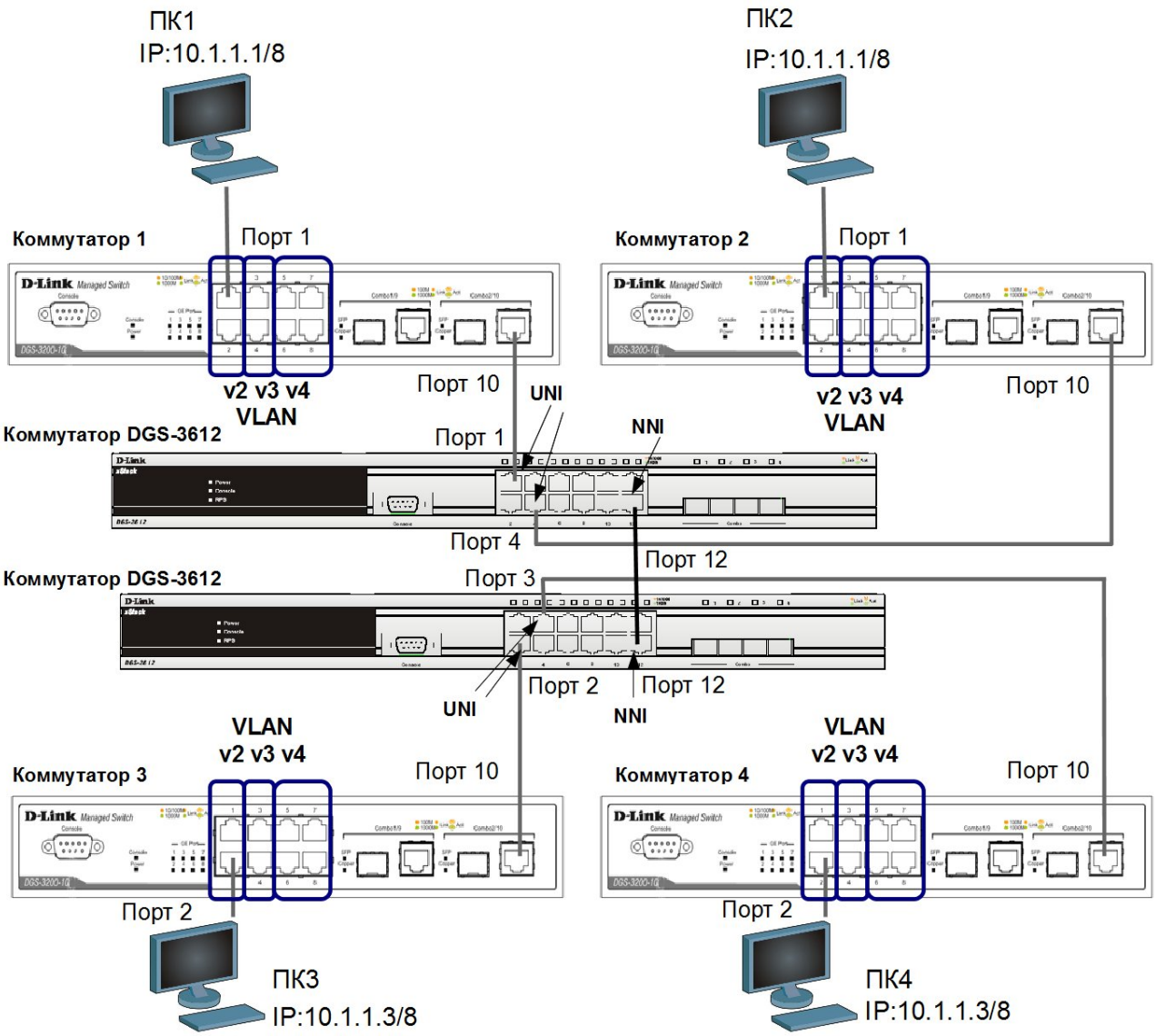
- UNI (User-to-Network Interface) – эта роль назначается портам, через которые будет осуществляться взаимодействие граничного коммутатора провайдера с клиентскими сетями.
- NNI (Network-to-Network Interface) – эта роль назначается портам, которые подключаются к внутренней сети провайдера или другим граничным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

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

Оборудование (на 6 рабочих мест):

Коммутатор DES-3200-10 или DGS-3200-10	4 шт.
Коммутатор DGS-3612	2 шт.
Рабочая станция	4 шт.
Консольный кабель	4 шт.
Кабель Ethernet	9 шт.

Схема 18:



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 1-10
```

Создайте VLAN v2, v3 и v4, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порты 9 и 10 маркированными:

```
create vlan v2 tag 2
config vlan v2 add untagged 1-2
config vlan v2 add tagged 9-10
create vlan v3 tag 3
config vlan v3 add untagged 3-4
config vlan v3 add tagged 9-10
```

```
create vlan v4 tag 4
config vlan v4 add untagged 5-8
config vlan v4 add tagged 9-10
```

Проверьте настройки VLAN:
```
show vlan
```

Настройка коммутаторов DGS-3612
Включите функцию Q-in-Q VLAN:
```
enable qinq
```

Удалите порты из Q-in-Q VLAN по умолчанию:
```
config vlan default delete 1-12
```

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 1-2
```

Настройте порты доступа в Q-in-Q VLAN d200:
```
config vlan d200 add untagged 3-4
```

Настройте порт 12 как Uplink-порт в Q-in-Q VLAN d100 и d200:
```
config vlan d100 add tagged 12
config vlan d200 add tagged 12
```

Настроить роли портов доступа в Q-in-Q и отключить режим Missdrop на них.
```
config qinq ports 1-4 role uni missdrop disable
```

Проверьте настройку функции Q-in-Q VLAN:
```
show qinq ports all
```

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 _____