Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет
им. Г.И. Носова»
Многопрофильный колледж

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ РАБОТ

По учебной дисциплине
ОПЦ.11 Компьютерные сети
программы подготовки специалистов среднего звена
специальности 09.02.07 Информационные системы и программирование
Квалификация: Разработчик веб и мультимедийных приложений

Магнитогорск, 2020

ОДОБРЕНО:
Предметно-цикловой комиссией
Информатики и вычислительной техники
Председатель И.Г. Зорина

Протокол №7 от 17.02.2020

Методической комиссией МпК
Протокол №3 от «26» февраля 2020г

Составитель:
преподаватель ФГБОУ ВП МГТУ МпК Н.А. Криворучко

Методические указания по выполнению практических и лабораторных работ разработаны на основе рабочей программы ОПЦ 11 Компьютерные сети.
Содержание практических и лабораторных работ ориентировано на подготовку обучающихся к освоению профессиональных модулей программы подготовки специалистов среднего звена по специальности 09.02.07 Информационные системы и программирование Квалификация:: Разработчик веб и мультимедийных приложений и овладению общими компетенциями.

СОДЕРЖАНИЕ

1 Пояснительная записка

Состав и содержание практических и лабораторных занятий направлены на реализацию Федерального государственного образовательного стандарта среднего профессионального образования.

Ведущей дидактической целью практических занятий является формирование профессиональных практических умений (умений выполнять определенные действия, операции, необходимые в последующем в профессиональной и учебной деятельности).

Ведущей дидактической целью лабораторных занятий является экспериментальное подтверждение и проверка существенных теоретических положений (законов, зависимостей).

В соответствии с рабочей программой учебной дисциплины «Компьютерные сети» предусмотрено проведение практических и лабораторных занятий. В рамках практического/лабораторного занятия обучающиеся могут выполнять одну или несколько практических/лабораторных работ.

В результате их выполнения, обучающийся должен:

уметь:

У.1 Организовывать и конфигурировать компьютерные сети;
У.2 Строить и анализировать модели компьютерных сетей;
У.3 Эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач;

- У.4 Выполнять схемы и чертежи по специальности с использованием прикладных программных средств
- У.5 Работать с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP, IPX/SPX);
- У.6 Устанавливать и настраивать параметры протоколов;
- У.7 Обнаруживать и устранять ошибки при передаче данных;
- У 01.1 распознавать задачу и/или проблему в профессиональном и/или социальном контексте;
- У 01.2 анализировать задачу и/или проблему и выделять её составные части;
- У 01.3 определять этапы решения задачи;
- У 01.4 выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;
- У 01.5 составлять план действия;
- У 01.6 определять необходимые ресурсы;
- У 02.1 определять задачи поиска информации
- У 02.6 оценивать практическую значимость результатов поиска;
- У 04.2 взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
- У05.3 излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке;
- У 09.2 использовать современное программное обеспечение
- У 10.1 понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые);

Содержание практических и лабораторных занятий ориентировано на подготовку обучающихся к освоению профессионального модуля программы подготовки специалистов среднего звена по специальности и овладению ***профессиональными компетенциями:***

ПК 5.3 - Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

ПК 9.4 - Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием.

ПК 9.6 - Размещать веб-приложения в сети в соответствии с техническим заданием.

ПК.9.10 - Реализовывать мероприятия по продвижению веб-приложений в информационно-телекоммуникационной сети "Интернет".

А также формированию ***общих компетенций***:

ОК ОК 0.1 - Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 0.2 - Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 0.4 - Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 0.5 - Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 0.9 - Использовать информационные технологии в профессиональной деятельности.

ОК 10 - Пользоваться профессиональной документацией на государственном и иностранном языке.

Выполнение обучающихся практических и лабораторных работ по учебной дисциплине «Компьютерные сети» направлено на:

- обобщение, систематизацию, углубление, закрепление, развитие и детализацию полученных теоретических знаний по конкретным темам учебной дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- формирование и развитие умений: наблюдать, сравнивать, сопоставлять, анализировать, делать выводы и обобщения, самостоятельно вести исследования, пользоваться различными приемами измерений, оформлять результаты в виде таблиц, схем, графиков;
- приобретение навыков работы с различными приборами, аппаратурой, установками и другими техническими средствами;
- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач профессионально значимых качеств, таких как самостоятельность, ответственность, точность, творческая инициатива.

Практические и лабораторные занятия проводятся после соответствующей темы, которая обеспечивает наличие знаний, необходимых для ее выполнения.

2 Перечень практических и лабораторных занятий

Разделы/темы	Темы практических/лабораторных занятий	Количество часов	Требования ФГОС СПО (уметь)
РАЗДЕЛ 1 КОМПЬЮТЕРНЫЕ СЕТИ И ИХ АППАРАТНЫЕ КОМПАНЕНТЫ		**18**	
Тема 1.1 Общие сведения о компьютерной сети	Практическая работа 1 Проектирование сетей различных типов в среде FPinger	4	**У1, У2, У3, У4, У7.** У 01.1 У 01.2 У 01.3 У 01.4 У 01.5 У 01.6 У 02.1 У 02.6 У 04.2 У05.
Тема 2.1 Передача данных по сети	Лабораторная работа 1 Обжим и монтаж кабельных систем ЛВС	2	
	Лабораторная работа 2 Работа с диагностическими утилитами протокола TCP/IP	2	
	Лабораторная работа 3 Основные команды коммутатора. Управление коммутаторами	2	
	Лабораторная работа 4 обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	2	
	Лабораторная работа 5 Конфигурирование портов коммутатора	2	
	Лабораторная работа 6 Контроль над подключением узлов к портам коммутатара. Функция Port Security	2	
	Лабораторная работа 7 Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	2	
РАЗДЕЛ 2 ПРОТОКОЛЫ ПЕРЕДАЧИ ДАННЫХ		14	
Тема 2.1 Передача данных по сети	Лабораторная работа 8 Управление сетью с использованием технологии Single IP Management	2	**У1, У2, У3, У4, У5, У6, У7.** У 01.1 У 01.2 У 01.3 У 01.4 У 01.5 У 01.6 У 02.1 У 02.6 У 04.2 У05.
	Лабораторная работа 9 Управление полосой пропускания	2	
	Лабораторная работа 10 Агрегирование каналов	2	
	Лабораторная работа 11 Настройка VLAN на основе стандарта IEEE 802.1Q Команды протокола GVRP	2	
	Лабораторная работа 12 Ограничение административного доступа к управлению коммутатором	2	
Тема 2.2 Сетевые архитектуры	Лабораторная работа 13 Команды мониторинга	2	
	Лабораторная работа 14 Списки управления доступом	2	
ИТОГО		**32**	

3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

РАЗДЕЛ 1 КОМПЬЮТЕРНЫЕ СЕТИ И ИХ АППАРАТНЫЕ КОМПАНЕНТЫ

Тема 1.1 Общие сведения о компьютерной сети

Практическая работа № 1

Проектирование сетей различных типов в среде FPinger

Цель работы: научиться проектировать различные типы сетей **в** среде FPinger.

Выполнив работу, Вы будете:

уметь:

- администрировать, производить мониторинг и инвентаризацию компьютерных сетей.

Материальное обеспечение:

Friendly Pinger 5.0.1

Задание:

1 Построить топологию сети по заданию преподавателя.

Краткие теоретические сведения:

Программа Friendly Pinger позволяет:

Визуализация компьютерной сети в красивой анимационной форме;

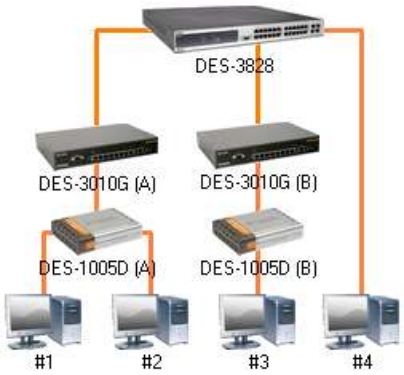
- Отображение, какие компьютеры включены, а какие нет;
- Пингование всех устройств за раз;
- Оповещение в случае остановки/запуска серверов;
- Инвентаризация программного и аппаратного обеспечения всех компьютеров в сети;
- Слежение, кто "лазает" по Вашему компьютеру и какие файлы качает;
- Назначение внешних команд (например, telnet, tracert, net.exe) устройствам;
- Поиск HTTP, FTP, e-mail и других сетевых служб;
- Отображение состояния сети на рабочем столе или Web странице;
- Графический TraceRoute;
- Открытие компьютеров в проводнике, в Total Commander'e или в FAR'e;
- Функция "Создать дистрибутив" позволяет создать облегченную версию с Вашими картами и настройками.

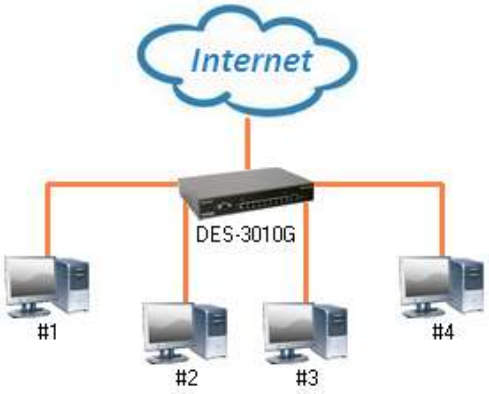
Порядок выполнения работы:

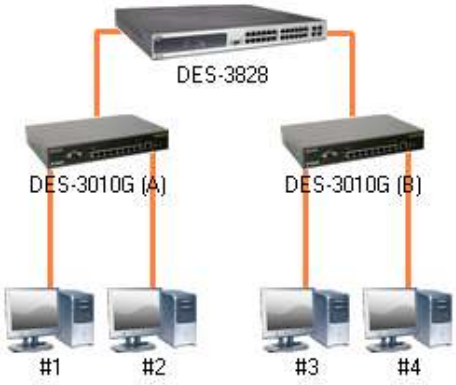
1 Запустить программу.

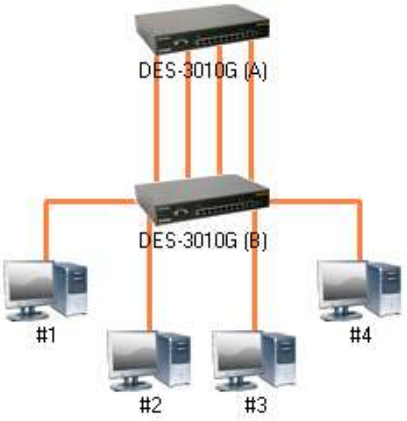
2 Ознакомиться с интерфейсом программы.

3 Построить топологию по заданию преподавателя.









Форма представления результата: файл **с** топологией сети.

Критерии оценки:

«5» - практическая работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - практическая работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - практическая работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - практическая работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 1

Обжим и монтаж кабельных систем ЛВС

Цель работы: Научиться производить обжим кабеля категории cat 5.

Выполнив работу, Вы будете:

уметь:

- обжимать кабель категории cat 5;
- проверять работоспособность кабеля категории cat 5.

Материальное обеспечение:

Кабель витая пара категории cat 5, обжимной инструмент, коннекторы RJ 45, тестер, фильм «Обжим кабеля»

Задание:

1 Обжать кабель и проверить его работоспособность.

Порядок выполнения работы:

1 Просмотреть фильм «Обжим кабеля»;
2 Выполнить обжатие кабеля;
3 Проверить работоспособность кабеля.

Форма представления результата: рабочий обжатый кабель

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 2

Работа с диагностическими утилитами протокола TCP/IP

Цель работы: Научиться производить мониторинг сети с помощью утилит.

Выполнив работу, Вы будете:

уметь:

- производить мониторинг сети с помощью утилит.

Материальное обеспечение:

Учебно-лабораторный комплекс «Локальные компьютерные сети»

Задание:

1 Используя утилиты мониторинга сети определить сетевые параметры всех узлов.

Краткие теоретические сведения:

Ping – проверка связи с удаленным узлом.

Ifconfig – определение сетевых параметров узла таких как IP-адрес, Mac-адрес.

ARP – вывод arp-таблиц на соответствие IP-адреса и Mac-адреса.

Порядок выполнения работы:

1 Изучить теоретические сведения.

2 Собрать топологию сети.

3 Определить сетевые параметры всех узлов и заполнить таблицу

Узел	Интерфейс	IP-адрес	Mac-адрес
ПК1	**eth 0**		
	eth 1		
	eth 2		
ПК2	**eth 0**		
	eth 1		
	eth 2		
ПК3	**eth 0**		
	eth 1		
	eth 2		
ПК4	**eth 0**		
	eth 1		
	eth 2		
DES 3828			
DES 3010 G			
DES 3010 G			

Форма представления результата: заполненная таблица

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 3

Основные команды коммутатора. Управление коммутаторами

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

Выполнив работу, Вы будете:

уметь:

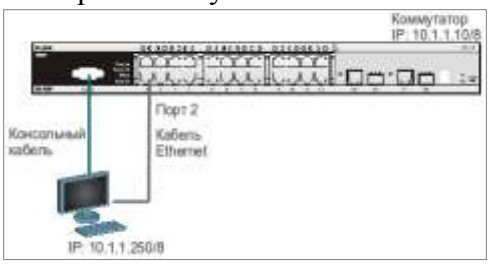
- осуществлять вызов помощи по командам;
- осуществлять изменение IP-адреса коммутатора;
- производить настройку времени на коммутаторе;
- управлять учетными записями пользователей;
- управлять возможностью доступа к коммутатору через Web-интерфейс и Telnet;
- настраивать параметры баннера приветствия.

Материальное обеспечение:

Коммутатор DES-3528 или DES-3810-28	1 шт.
Рабочая станция	1 шт.
Консольный кабель	1 шт

Задание:

1 Собрать схему



Краткие теоретические сведения:

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

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

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

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

Таблица 1

<угловые скобки >	
Назначение	Содержат ожидаемую переменную или значение, которое должно быть указано.
Синтаксис	**config ipif <System> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable}] | bootp | dhcp]**
Описание	В привёденном примере синтаксиса, пользователь должен указать имя IP-интерфейса System, имя VLAN vlan_name длиной до 32 символов и сетевой

	адрес network_address . Сами угловые скобки вводить не надо.
Пример	**config ipif System ipaddress 10.24.22.5/8 vlan Sales**
[квадратные скобки]	
Назначение	Содержат требуемое значение или набор требуемых аргументов. Может быть указано одно значение или аргумент.
Синтаксис	**create account [admin | user] <username 15>**
Описание	В приведённом примере синтаксиса, пользователь должен указать один из двух уровней привилегий (admin или user) для создаваемой учётной записи. Вводить квадратные скобки не надо.
Пример	**create account admin user1**
| вертикальная черта	
Назначение	Отделяет два или более взаимно исключающих пунктов из списка, один из которых должен быть введён/указан.
Синтаксис	**create account [admin | user] <username 15>**
Описание	В приведённом примере синтаксиса, пользователь должен указать один из двух уровней привилегий (admin или user) для создаваемой учётной записи. Вводить квадратные скобки не надо.
Пример	**create account admin user1**
{ фигурные скобки }	
Назначение	Содержит необязательное значение или набор необязательных аргументов.
Синтаксис	**reset {[config | system]} {force_agree}**
Описание	В приведённом примере синтаксиса, пользователь может указать необязательное значение config или system. Его вводить необязательно, но результат выполнения команды будет зависеть от ввода дополнительного параметра.
Пример	**reset config**
(круглые скобки)	
Назначение	Показывает, что одно или более значений или аргументов, заключённых в фигурные скобки, должно быть введено.
Синтаксис	**config dhcp_relay {hops <value 1-16> | time <sec 0-65535>}(1)**
Описание	В приведённом примере синтаксиса, от пользователя ожидается ввод одного или обоих необязательных параметров, заключённых в фигурные скобки. Параметр «(1)» показывает, что ожидается ввод, по крайней мере, одного из параметров или аргументов.
Пример	**config dhcp_relay hops 3**

Порядок выполнения работы:

1 Вызов помощи по командам.
2 Изменение IP-адреса коммутатора.
3 Настройка времени на коммутаторе
4 Управление учетными записями пользователей
5 Управление возможностью доступа к коммутатору через Web-интерфейс и Telnet
6 Настройка параметров баннера приветствия

Ход работы:

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, Putty или программу

HyperTerminal в Windows). В программе следует установить следующие параметры подключения:

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

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

1. Введите в консоли: **?**
2. Введите в консоли: **config**
3. Введите в консоли: **show**

2. Настройка времени на коммутаторе

1. Проверьте время: **show time**
2. Установите часовой пояс Москва (GMT +6:00) (Для Екатеринбурга):

config time_zone operator + hour 6 min 0

3. Введите новую дату и время: **config time 26jan2011 15:45:30**
4. Проверьте время: **show time**
5. Укажите текущую дату и время**.**
6. Проверьте время.

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

3. 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).

1. тключите возможность подключения к коммутатору по Telnet: **disable telnet**
2. Проверьте выполненные настройки: **show switch**
3. Убедитесь, что доступ по Telnet отключён.
4. Выполните на рабочей станции команду: **telnet <IP-адрес коммутатора>**
5. Что вы наблюдаете? Запишите.

   _____
6. Включите функцию подключения к коммутатору по Telnet:**enable telnet**
7. Проверьте выполненные настройки и убедитесь в возможности подключения к коммутатору по Telnet.
8. Отключите возможность подключения к коммутатору через Web-интерфейс: **disable web**
9. Проверьте выполненные настройки: **show switch**
10. Убедитесь, что доступ к коммутатору через Web-интерфейс отключён? Для этого запустите на рабочей станции браузер и введите в адресной строке IP-адрес коммутатора. Что вы наблюдаете?
    Запишите_____

4. Настройка параметров баннера приветствия

С целью упрощения идентификации пользователями активного сетевого оборудования, или создания его уникальных логотипов, возможно изменение баннера приветствия, который

появляется в момент загрузки коммутатора. Также возможно изменение приглашения Command Prompt в командной строке CLI.

1. Измените приглашение Command Prompt:

config command_prompt TEST_SWITCH

2. Установите приглашение по умолчанию:

config command_prompt default

3. Посмотрите текущий баннер приветствия:

show greeting_message

4. Войдите в режим редактирования 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

5. Добавьте строчку в приветствие:

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

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

7. Проверьте изменённый баннер приветствия:

show greeting_message

```
============================================================

              DES-3528 Fast Ethernet Switch
                Command Line Interface
            SWITCH_TEST  tel +7(495) 000-00-00
               Firmware: Build 2.80.B042
  Copyright(C) 2010 D-Link Corporation. All rights reserved.
============================================================
```

8. Представьте результаты работы преподавателю.

9. Восстановите настройки баннера по умолчанию:

config greeting_message default

10. Проверьте баннер приветствия:

show greeting_message

5. Настройка основных параметров портов коммутатора

1. Посмотрите текущие настройки портов: **show ports**

2. Измените скорость и режим работы портов 1-5:

config ports 1-5 speed 10_half

3. Проверьте выполненные настройки: show ports

Что вы наблюдаете? Запишите.

_____

4. Активизируйте функцию управления потоком на портах 1-5:

config ports 1-5 flow_control enable

5. Проверьте настройки: show ports

6. Отключите работу портов 1-5:

config ports 1-5 state disable

7. Проверьте настройки: show ports

8. Проверьте соединение между компьютером и коммутатором. На ПК выполните команду:

ping 195.168.0.5

Что вы наблюдаете? Запишите.

_____

9. Включите работу порта 2:

config ports 2 state enable

10. Проверьте соединение между ПК и коммутатором.

На ПК выполните команду: **ping 195.168.0.5**

Что вы наблюдаете? Запишите._____

11. Задайте описание порта 2: **config ports 2 description PC_PORT**

12. Проверьте описание портов: **show ports description**

1.6. Изменение IP-адреса интерфейса управления коммутатора

1. Посмотрите значение IP- адреса интерфейса управления коммутатора:

show ipif

2. Чему равен IP-адрес интерфейса управления коммутатора по умолчанию (записать в тетрадь): _____

3. Измените IP-адрес интерфейса управления коммутатора:

config ipif System ipaddress 10.1.1.10/8

4. Настройте IP-адрес шлюза по умолчанию:

create iproute default 10.1.1.254

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

5. Проверьте настройки коммутатора: **show switch**

1.7. Функция Factory Reset (сброс к заводским установкам)

1. Сбросьте текущие настройки коммутатора к настройкам по умолчанию командой:

reset

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

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

reset config

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

reset system

В случае необходимости, перезагрузить коммутатор можно командой:

Reboot

Заполните в тетради таблицу.

Команда	Назначение	Команда	Назначение
show ipif		config greeting_message default	
config ipif System ipaddress		show ports	
create iproute default		config ports speed	
show switch		config ports flow_control	

		enable	
show time		config ports state disable / enable	
config time_zone operator + hour 6 min 0		config ports description	
config time		show ports description	
disable / enable telnet		Reset	
disable / enable web		reset config	
config command_prompt		reset system	
config command_prompt default		reboot	
show greeting_message			
config greeting_message			

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

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

Отключите возможность подключения к коммутатору по Telnet:
disable telnet

Проверьте выполненные настройки:
show switch

Убедитесь, что доступ по Telnet отключён.

Выполните на рабочей станции ПК1 команду:
telnet <IP-адрес коммутатора>

Что вы наблюдаете? При попытке подключиться: “Запишите. Подключение к 10.1.1.10...Не удалось открыть подключение к этому узлу, на порт 23: Сбой подключения”.
Не смотря на доступность по протоколу ICMP:
Ответ от 10.1.1.10: число байт=32 время=1мс TTL=255
Ответ от 10.1.1.10: число байт=32 время=1мс TTL=255
Ответ от 10.1.1.10: число байт=32 время=1мс TTL=255
Ответ от 10.1.1.10: число байт=32 время=1мс TTL=255

Статистика Ping для 10.1.1.10:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек

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 отключён.

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

Что вы наблюдаете? Запишите. _____
Включите возможность подключения к коммутатору через Web-интерфейс и измените стандартный 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:
_____

6. Настройка параметров баннера приветствия

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

Измените приглашение Command Prompt:
config command_prompt TEST_SWITCH

Установите приглашение по умолчанию:
config command_prompt default

Посмотрите баннер приветствия:
show greeting_message

Войдите в режим редактирования баннера приветствия:
config greeting_message

Для редактирования приветствия, используйте следующие команды:

<Function Key>		<Control Key>	
Ctrl+C	Выйти без сохранения	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 изменённый баннер приветствия:
show greeting_message

==========

DES-3528 Fast Ethernet Switch

Command Line Interface
SWITCH_TEST tel +7(495) 000-00-00
Firmware: Build 2.80.B042
Copyright(C) 2010 D-Link Corporation. All rights reserved.
==========

Восстановите настройки баннера по умолчанию:
config greeting_message default

Проверьте баннер приветствия:
show greeting_message

Форма представления результата: отчет

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 4

Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов

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

Выполнив работу, Вы будете:

уметь:

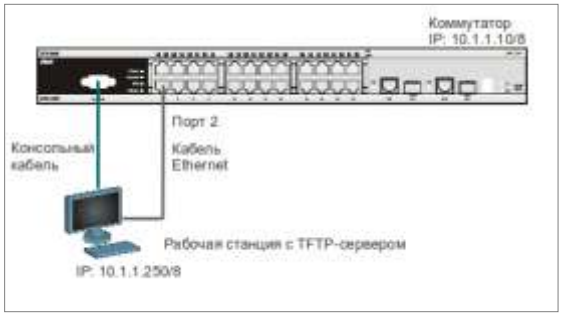
- Подготавливать к режиму обновления и сохранения программного обеспечения коммутатор.
- Загружать файл программного обеспечения в память коммутатора.
- Настраивать порядок загрузки программного обеспечения коммутатора.
- Выгружать и загружать конфигурации.
- Выгружать log-файлы.

Материальное обеспечение (на одно рабочее место):

Коммутатор DES-3528 или DES-3810-28	1 шт.
Рабочая станция с TFTP-сервером	1 шт.
Консольный кабель	1 шт.
Кабель Ethernet	1 шт.

Задание:

1 Собрать схему.



2. Изучить и выполнить команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов.

Краткие теоретические сведения:

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

Порядок выполнения работы:

1 Подготовить к режиму обновления и сохранения программного обеспечения коммутатор.

2 Загрузить файл программного обеспечения в память коммутатора

3 Настроить порядок загрузки программного обеспечения коммутатора.

4 Выгрузить и загрузить конфигурации

5 Выгрузить log-файлы

Ход работы:

1. Подготовка к режиму обновления и сохранения программного обеспечения коммутатора

Настройте TFTP-сервер.В настройках программы необходимо:

1. установить директорию приёма файлов;
2. отключить все другие сервисы, кроме TFTP server.

Подготовьте файл нового программного обеспечения коммутатора:

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

2.2. Загрузка файла программного обеспечения в память коммутатора

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

Настройте IP-адрес интерфейса управления:
config ipif System ipaddress 10.1.1.10/8

Настройте TFTP-сервер:
Запустить TFTP-сервер, в настройках TFTP-сервера указать IP-адрес рабочей станции 10.1.1.250/8, указать директорию с прошивкой Current Directory.

Проверьте доступность TFTP-сервера с коммутатора:
ping 10.1.1.250

Проверьте информацию о текущем программном обеспечении коммутатора:
show firmware information
Проверьте, что вы загружены с прошивки 2.80 из слота 2

Загрузите программное обеспечение на коммутатор в первый слот (команда вводится в одну строку):
download firmware_fromTFTP 10.1.1.250 src_file DES-3528_Series_FW_v2.01.B042.had image_id 1

Убедитесь, что программное обеспечение загружено:
show firmware information

2.3. Настройка порядка загрузки программного обеспечения коммутатора

Задайте номер слота программного обеспечения, которое будет загружаться при старте коммутатора:
config firmware image_id 1 boot_up

Сохраните изменения:
save

Обновлённая прошивка будет использована при следующей загрузке коммутатора.
Перезагрузите коммутатор:
reboot

После загрузки коммутатора проверьте информацию о программном обеспечении:

show firmware information

Что вы наблюдаете?
show firmware information
Command: show firmware information

ID	Version	Size(B)	Update Time	From	User
*1	2.01.B042	2740273	0 days 00:00:00	Serial Port(Prom)	Unknown
2	2.80.B045	3849399	0 days 00:00:00	Serial Port(Prom)	Unknown

'*' means boot up firmware
(R) means firmware update through Serial Port(RS232)
(T) means firmware update through TELNET
(S) means firmware update through SNMP
(W) means firmware update through WEB
(SSH) means firmware update through SSH
(SIM) means firmware update through Single IP Management

Снова загрузитесь со второго слота (прошивка 2.80). Затем обновите прошивку в первом слоте с 2.01 на прошивку 2.60.

После всех операций вы должны быть загружены со второго слота и список прошивок должен быть: 1 слот – прошивка 2.60, 2 слот – прошивка 2.80.

2.4. Выгрузка и загрузка конфигурации

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

Проверьте информацию об имеющихся в NVRAM конфигурациях коммутатора:
show config information

Посмотрите конфигурацию коммутатора №1, сохранённую в NVRAM:
show config config_in_nvram 1

Выгрузите конфигурацию №1 на TFTP-сервер:
upload cfg_toTFTP 10.1.1.250 dest_file config.txt 1

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

Должно получиться так:
IP
config ipif System ipaddress 10.1.1.**8**/8 vlan default state enable
disable autoconfig

Сохраните файл.

Загрузите изменённую конфигурацию на коммутатор в слот для конфигурации №2:
download cfg_fromTFTP 10.1.1.250 src_file config.txt 2

Проверьте, изменился ли IP-адрес коммутатора:
show switch

Что вы наблюдаете?
Задайте номер конфигурации, которая будет загружаться при старте коммутатора:
Device Type : DES-3528 Fast Ethernet Switch
MAC Address : 1C-BD-B9-36-65-90
IP Address : 10.1.1.10 (Manual)
VLAN Name : default
Subnet Mask : 255.0.0.0
Default Gateway : 0.0.0.0
Boot PROM Version : Build 1.00.B008
Firmware Version : Build 2.80.B045
Hardware Version : A3
Serial Number : PVIH1A7003065
System Name :
System Location :
System Uptime : 0 days, 0 hours, 6 minutes, 50 seconds
System Contact :
Spanning Tree : Disabled
GVRP : Disabled
IGMP Snooping : Disabled
MLD Snooping : Disabled
VLAN Trunk : Disabled
Telnet : Enabled (TCP 23)
Web : Enabled (TCP 80)
SNMP : Disabled
SSL Status : Disabled
SSH Status : Disabled
802.1x : Disabled
Jumbo Frame : Off
CLI Paging : Enabled
MAC Notification : Disabled
Port Mirror : Disabled
SNTP : Disabled
HOL Prevention State : Enabled
Syslog Global State : Disabled
Single IP Management : Disabled
Dual Image : Supported

Password Encryption Status : Disabled

config configuration 2 boot_up

Чему будет равен IP-адрес после перезагрузки коммутатора?
Command: show ipif

IP Interface : System
VLAN Name : default
Interface Admin State : Enabled
DHCPv6 Client State : Disabled
Link Status : LinkUp
IPv4 Address : 10.1.1.8/8 (Manual) Primary
Proxy ARP : Disabled (Local : Disabled)
IPv4 State : Enabled
IPv6 State : Enabled
DHCP Option12 State : Disabled
DHCP Option12 Host Name :

Total Entries: 1

2.5. Выгрузка log-файлов

Просмотрите журнал работы коммутатора:
show log

Выгрузите журнал работы на TFTP-сервер:
upload log_toTFTP 10.1.1.250 dest_file Logfiles.txt

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

Форма представления результата: отчет
Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 5

Конфигурирование портов коммутатора

Цель работы: Получение навыков настройки портов коммутатора D-Link DES 3010G

Выполнив работу, Вы будете:

уметь:

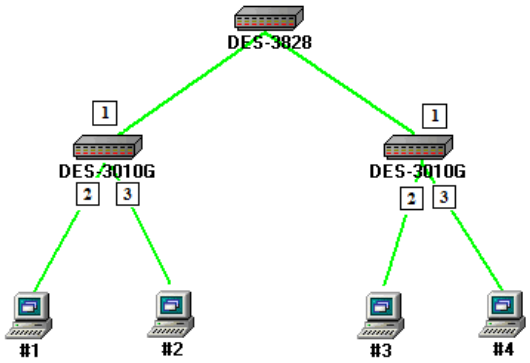
- установите пропускную способность портов коммутатора.

Материальное обеспечение:

Коммутатор DES-3828	1 шт.
Коммутатор DES-3010G	2 шт.
Рабочая станция	4 шт.
Кабель Ethernet	

Задание:

1 Постройте топологию сети.



2 Выполнить задание по настройке портов коммутатора.

Краткие теоретические сведения:

Раздел «Администрирование» меню «Конфигурирование портов»

Port Configuration

From	To	State	MDIX	Speed/Duplex	Flow Control	Apply
Port 1	Port 1	Enabled	Auto	Auto	Disabled	Apply

The Port Information Table

Port	State	MDIX	Speed/Duplex	Flow Control	Connection/Duplex/FlowCtrl	Learning
1	Enabled	Auto	Auto	Disabled	100M/Full/None	Enabled
2	Enabled	Auto	Auto	Disabled	100M/Full/None	Enabled
3	Enabled	Auto	Auto	Disabled	100M/Full/None	Enabled
4	Enabled	Auto	Auto	Disabled	LinkDown	Enabled
5	Enabled	Auto	Auto	Disabled	LinkDown	Enabled
6	Enabled	Auto	Auto	Disabled	LinkDown	Enabled
7	Enabled	Auto	Auto	Disabled	LinkDown	Enabled
8	Enabled	Auto	Auto	Disabled	LinkDown	Enabled
9	Enabled	Auto	Auto	Disabled	LinkDown	Enabled
10	Enabled	Auto	Auto	Disabled	LinkDown	Enabled

Меню «**From», «To».** Позволяет задать порт или последовательность портов для которых необходимо сконфигурировать следующие параметры:

- **State (Состояние)**. Может принимать значение Enabled (Включен) или Disabled (Выключен).
- **Speed/Duplex (Скорость/Дуплекс).** Позволяет задать скорость и режим работы порта. Может принимать следующие значения:

Auto. Автоматически согласует скорость и режим работы порта, выбирая лучшие значения (10 Мб/с или 100 Мб/с, полудуплекс или дуплекс).
10M/Hatf
10M/Full
10OM/Half
100M/Full
1000M/Full
1000M/Full_M
1000M/Full_S

- **Flow Control (Контроль потока данных).** Отображает схему управления потоком данных, использующуюся при конфигурировании портов. Порты в полнодуплексном режиме используют схему 802.3x. Порты в полудуплексном режиме используют схему backpressure Порты в автоматическом режиме используют одну из указанных схем. По умолчанию управление потоком отключено.

Кнопка «**Apply**» для установки новых настроек.

Ход работы:

1. У всех портов установите пропускную способность 100 Мбит/с.

2. Выключите один из портов коммутатора, к которому подключен один из компьютеров. Попробуйте осуществить взаимодействие компьютеров. Сделайте выводы на основе полученного результата.

3. Установите пропускную способность портов коммутатора DES-3010G, к которому подключены машины 3 и 4, равной 10 Мбит/с.

4. «Пингуйте» одновременно машину 2 с машин 3 и 4

5. Запустите на машинах 1 и 2 утилиту tcpdump. Сравните результаты работы на обеих машинах.

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 6

Контроль над подключением узлов к портам коммутатора. Функция Port Security

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

Выполнив работу, Вы будете:

уметь:

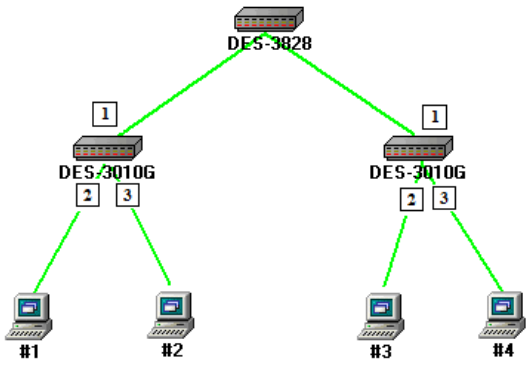
- управлять подключением узлов к портам коммутатора.

Материальное обеспечение:

Коммутатор DES-3828	1 шт.
Рабочая станция	2 шт.
Кабель Ethernet	2 шт.
Консольный кабель	1 шт.

Задание:

1 Постройте топологию сети.



2 Выполнить задание по настройке портов коммутатора.

Краткие теоретические сведения:

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

Существует три режима работы функции Port Security:

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

  Если состояние канала связи на подключённом порте изменяется, MAC-адреса, изученные на нем, удаляются из таблицы коммутации, что аналогично выполнению действий при истечении времени, установленного таймером Aging Time.
- *Delete on Reset* (Удалить при сбросе) – занесённые в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора (этот режим используется по умолчанию).

Функция Port Security оказывается весьма полезной при построении 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.

Ход работы:

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

Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:

```
reset config
```

Проверьте информацию о настройках Port Security:

```
show port_security
```

Установите максимальное количество изучаемых каждым портом MAC-адресов равным 1, и включите функцию на всех портах:

```
config port_security ports all admin_state enable max_learning_addr
1
```

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

Посмотрите MAC-адреса, которые стали известны портам 2 и 10:

```
show fdb port 2
show fdb port 10
```

Проверьте, соответствуют ли зарегистрированные адреса адресам рабочих станций
да

Проверьте информацию о настройках Port Security на портах коммутатора:

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

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

```
enable port_security trap_Log
```

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

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

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте информацию в журнале работы коммутатора:

```
show log
```

Какой вы сделаете вывод
К портам привезались мак адреса. Другие не могут подключиться к этому порту

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 1-24
```

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

Очистите информацию о привязке MAC-порт на порте 2:
```
clear port_security_entry port 2
```

Отключите работу функции Port Security на порте 2 и приведите настройки в исходное (по умолчанию) состояние:
`config port_security ports 2 admin_state disable max_learning_addr 1 lock_address_mode deleteonreset`

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

Изменить время действия таймера можно с помощью настройки времени жизни MAC-адреса в таблице коммутации (время указано в секундах):
```
config fdb aging_time 20
```

Измените режим работы функции Port Security на Delete on Timeout:
```
config port_security ports 2 admin_state enable max_learning_addr 1
lock_address_mode deleteontimeout
```

Проверьте MAC-адреса, которые стали известны порту 2:
```
show fdb port 2
```

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

Выполните тестирование соединения между ПК1 и ПК2 командой ping.

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

Отключите работу функции Port Security на портах:
```
config port_security ports 1-24 admin_state disable
```

Отключите функцию записи в log-файл и отправки SNMP Trap:
```
disable port_security trap_Log
```

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

1.2. 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, установив параметр *max_learning_addr* равным 0 (команда вводится в одну строку):
```
config port_security ports 1-24 admin_state enable max_learning_addr
0
```

Проверьте состояние портов:
```
show ports
```

Проверьте соединение между ПК1 и ПК2 командой ping.

Проверьте состояние таблицы коммутации:
```
show fdb
```

Имеются ли там записи? Есть одна запись

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

Внимание! Замените указанные в командах MAC-адреса на реальные адреса рабочих станций, подключаемых к коммутатору.
```
create fdb default 00-50-ba-00-00-01 port 2
create fdb default 00-50-ba-00-00-02 port 10
```
Проверьте созданные статические записи в таблице коммутации:
```
show fdb
```
Проверьте информацию о настройках Port Security на портах коммутатора:
```
show port_security ports 1-24
```
Проверьте соединение между ПК1 и ПК2 командой ping.

Подключите ПК1 к порту 8, а ПК2 к порту 2.
Повторите тестирование командой ping.
Какой вы сделаете вывод

Пинга нет, так как включены в другие порты

Удалите ранее созданную статическую запись из таблицы MAC-адресов на порте 2:

```
delete fdb default 00-50-ba-00-00-02 port 2
```

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 7

Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы

Цель работы: Изучить процесс управления таблицами MAC, IP и ARP.

Выполнив работу, Вы будете:

уметь:

- работать с таблицами коммутации и ARP- таблицей.

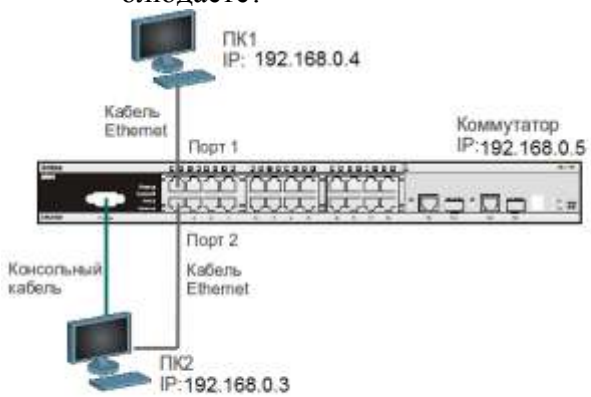
Материальное обеспечение:

Коммутатор DES-3828	1 шт.
Рабочая станция	2 шт.
Кабель Ethernet	2 шт.
Консольный кабель	1 шт.

Задание:

1 Подключите станции к коммутатору, как показано на схеме.

2 Попробуйте найти соответствие адресов подключенной станции в таблице. Что вы наблюдаете?



3 Запишите теорию в тетрадь и заполните таблицу:

Команда	Назначение
show fdb	
show fdb mac_address 00-03-47-BD-3F-57	
show fdb vlan default	
show fdb port 2	
show fdb aging_time	
config fdb aging_time	
clear fdb all	
	Создание статической записи в таблице MAC-адресов
	Просмотр статических записей в таблице MAC-адресов
	Просмотр статической записи таблицы MAC-адресов на заданном порте
	Удалить статическую запись из таблицы MAC-адресов

show ipfdb	
show ipfdb ip_address	
	Просмотр ARP-таблицы
	Найдти в ARP-таблице сопоставления IP-MAC по указанному IP-адресу:
	Просмотрите в ARP-таблице все сопоставления IP-MAC на интерфейсе System
clear arptable	
create arpentry 192.168.0.3 00-50-BA-00-07-36	
show arpentry static	
	Удалить статическую запись из ARP-таблицы
show arpentry static	

Краткие теоретические сведения:

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

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

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

Ход работы:

1. Просмотрите содержимое таблицы MAC-адресов:

show fdb

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

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

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

show fdb vlan default

4. Посмотрите MAC-адреса устройств, изученные портом 2:

show fdb port 2

5. Просмотрите время нахождения записи в таблице MAC-адресов:

show fdb aging_time

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

config fdb aging_time 350

7. Удалите все динамически созданные записи из таблицы MAC-адресов: **clear fdb all**

8. 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

9. Просмотрите статические записи в таблице MAC-адресов:

show fdb static
10. Просмотрите статические записи таблицы MAC-адресов на порте 2:
show fdb static port 2
11. Удалите статическую запись из таблицы MAC-адресов:
delete fdb default 00-03-47-BD-01-11
12. Просмотрите содержимое таблицы MAC-адресов:
show fdb
13. Просмотрите таблицу коммутации IP-адресов:
show ipfdb
14. Найдите порт коммутатора, к которому подключено устройство с определенным IP-адресом
show ipfdb ip_address 192.168.0.4
15. Просмотрите ARP-таблицу:
show arpentry
16. Найдите в ARP-таблице сопоставления IP-MAC по указанному IP-адресу:
show arpentry ipaddress 192.168.0.3
17. Просмотрите в ARP-таблице все сопоставления IP-MAC на интерфейсе System:
show arpentry ipif System
18. Удалите все динамически созданные записи из ARP-таблицы:
clear arptable
19. Убедитесь, что все динамические записи из таблицы удалены:
show arpentry
20. Создайте статическую запись в ARP-таблице (в качестве MAC-адреса укажите MAC-адрес ПК2):
create arpentry 192.168.0.3 00-50-BA-00-07-36
21. Просмотрите созданную статическую запись в ARP-таблице:
show arpentry static
22. Удалите статическую запись из ARP-таблицы:
delete arpentry 192.168.0.3
23. Проверьте, что запись удалена:
show arpentry static
24. Измените время нахождения записи в ARP-таблице до 30 минут (по умолчанию 20 минут):
config arp_aging time 30
25. Проверьте выполненные настройки:
show arpentry

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

РАЗДЕЛ 2 ПРОТОКОЛЫ ПЕРЕДАЧИ ДАННЫХ

Тема 2.1 Передача данных по сети

Лабораторная работа № 8

Управление сетью с использованием технологии Single IP Management

Цель работы: научиться управлять сетью с использованием технологии Single IP Management.

Выполнив работу, Вы будете:

уметь:

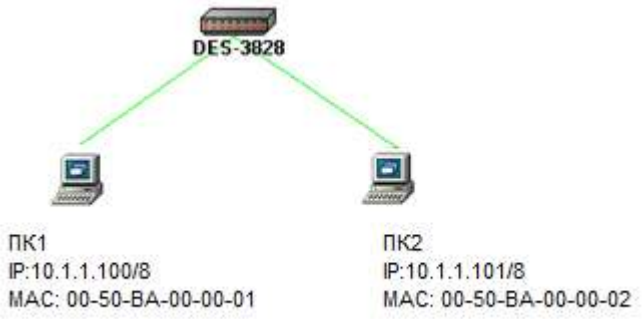
- управлять сетью с использованием технологии Single IP Management.

Материальное обеспечение:

Коммутатор DES-3828	1 шт.
Коммутатор DES-3010G	2 шт.
Рабочая станция	2 шт.
Кабель Ethernet	

Задание:

1 Постройте топологию сети



2 Выполните настройку коммутатора.

Ход работы:

1. Постройте топологию сети, показанную на рисунке.
2. Настройте коммутатор DES-3828 как командный коммутатор виртуального стека, а коммутаторы DES-3010G как коммутаторы-кандидаты.
3. Используя веб-интерфейс управления DES-3828, выведите карту сети, построенную коммутатором.
4. Зарисуйте карту сети, построенную коммутатором и ответьте на следующие вопросы:

- ✓ Почему на топологии сети не отображаются компьютеры?
- ✓ Какова пропускная способность всех линий связи?
- ✓ Мас-адрес коммутатора DES-3828

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 9

Управление полосой пропускания

Цель работы: Настроить ограничение полосы пропускания на коммутаторе D-Link.

Выполнив работу, Вы будете:

уметь:

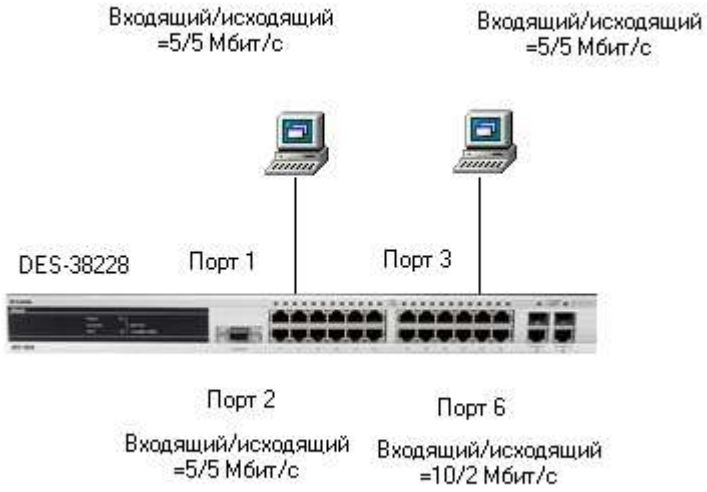
- настраивать ограничение полосы пропускания на коммутаторе.

Материальное обеспечение:

Коммутатор DES-3828	1 шт.
Рабочая станция	2 шт.
Кабель Ethernet	2 шт.

Задание:

1 Постройте топологию сети.



2 Выполнить задание по настройке ограничения полосы пропускания

Краткие теоретические сведения:

Современные коммутаторы позволяют регулировать интенсивность трафика на своих портах с целью обеспечения функций качества обслуживания.

Для управления полосой пропускания входящего и исходящего трафика на портах Ethernet коммутаторы D-Link поддерживают функцию Bandwidth Control, которая использует механизм Traffic Policing. Администратор может вручную устанавливать требуемую скорость соединения на порте в диапазоне от 64 Кбит/с до максимально поддерживаемой скорости интерфейса с шагом 64 Кбит/с.

Ход работы:

1. Настройте полосу пропускания на портах 1-4 равной 5Мбит/с для входящего и исходящего трафика

config bandwidth_control 1-4 rx_rate 5120 tx_rate 5120

2. Настройте полосу пропускания на порте 6 равной 10 Мбит/с для входящего и 2 Мбит/с для исходящего трафика

config bandwidth_control 6 rx_rate 10240 tx_rate 2048

3. Проверьте выполненные настройки

Show bandwidth_control 1-10

4. Подключите станции ПК1 и ПК2 к портам 8 и 10 и скачайте файл размером 50 Мб со станции ПК1 на станцию ПК 2 и обратно. Запишите время передачи файла (в секундах)_____

5. Подключите станцию ПК1 к порту 1, повторите скачивание. Запишите время передачи файла (в секундах) _____

6. Подключите станцию ПК1 к порту 6, повторите скачивание. Запишите время передачи файла (в секундах) _____. Что вы наблюдаете?

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 10

Агрегирование каналов

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

Выполнив работу, Вы будете:

уметь:

- выполнять настройку динамического агрегирования каналов.

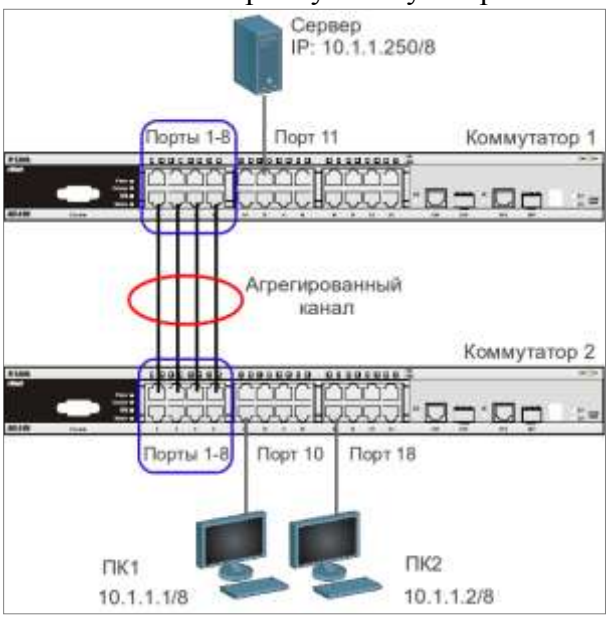
Материальное обеспечение:

Коммутатор DES-3528 или DES-3810-28	2 шт.
Рабочая станция	3 шт.
Консольный кабель	2 шт.
Кабель Ethernet	7 шт.

Задание:

1 Постройте топологию сети.

2 Выполните настройку коммутатора.



Краткие теоретические сведения:

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

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

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

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

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

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

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

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

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

Порядок выполнения работы:

Настройка коммутатора 1

Создайте группу агрегирования каналов:

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

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

```
config link_aggregation group_id 1 master_port 1 ports 1-8 state en-
abled
```

Настройте порты на работу в пассивном режиме:

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

Проверьте выполненные настройки:

```
show link_aggregation
```

Проверьте режим работы LACP на портах коммутаторов:

```
show lacp_port
```

Посмотрите текущий алгоритм агрегирования каналов:

```
show link_aggregation algorithm
```

Настройка коммутатора 2

Создайте группу агрегирования каналов:

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

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

```
config link_aggregation group_id 1 master_port 1 ports 1-8 state en-
abled
```

Настройте порты на работу в активном режиме:

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

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

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

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

Запустите программу iperf на ПК, выполняющего роль сервера:
```
iperf –s -u
```

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

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?

_____
_____
_____

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 11

Настройка VLAN на основе стандарта IEEE 802.1Q. Команды протокола GVRP

Цель работы: изучить технологию VLAN и её настройку на коммутаторах D-Link, изучить процесс динамического продвижения информации о VLAN в сети.

Выполнив работу, Вы будете:

уметь:

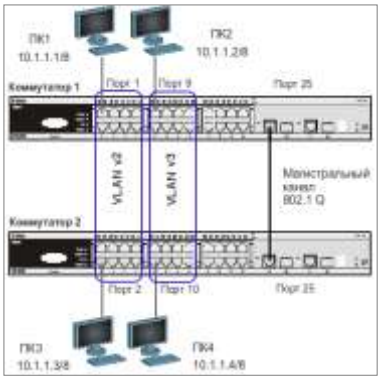
- выполнять настройку VLAN на коммутаторах D-Link;
- настраивать протокол GVRP.

Материальное обеспечение:

Коммутатор DES-3528 или DES-3810-28	2 шт.
Рабочая станция	4 шт.
Консольный кабель	2 шт.
Кабель Ethernet	5 шт.

Задание:

1 Постройте топологию сети.



2 Выполните настройку коммутатора.

Краткие теоретические сведения: 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 любого коммутатора можно настроить на принадлежность определённой VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть. Кадры, предназначенные станциям не принадлежащим данной VLAN, должны передаваться через маршрутизирующее устройство (маршрутизатор или коммутатор 3-го уровня). Таким образом, с помощью виртуальных сетей решается проблема ограничений при передаче широковещательных кадров и вызываемых ими последствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Основные определения IEEE 802.1Q:

- *Tag* (Тег) – дополнительное поле данных длиной 4 байта, содержащее информацию о VLAN (идентификатор VLAN (12 бит), поле приоритета (3 бита), поле индикатора канонического формата (1 бит)), добавляемое в кадр Ethernet;

- *Tagging* (Маркировка кадра) – процесс добавления информации (тега) о принадлежности к 802.1Q VLAN в заголовок кадра;
- *Untagging* (Удаление тега из кадра) – процесс извлечения информации 802.1Q VLAN из заголовка кадра;
- *Ingress port* (Входной порт) – порт коммутатора, на который поступают кадры, и принимается решение о принадлежности VLAN;
- *Egress port* (Выходной порт) – порт коммутатора, с которого кадры передаются на другие сетевые устройства (коммутаторы, рабочие станции) и на нем, соответственно, принимается решение о маркировке кадра.

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

Порядок выполнения работы:

Проверьте и запишите доступность соединения между рабочими станциями командой ping:

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

- от ПК1 к ПК 2, ПК 3 и ПК 4 _____
- от ПК2 к ПК 1, ПК 3 и ПК 4 _____

Настройка коммутатора 1

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

```
config vlan default delete 1-16
```

Настройте порт 25 маркированным в vlan default:

```
config vlan default add tagged 25
```

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

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

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

Проверьте настройки VLAN:

```
show vlan
```

Повторите процедуру настройки для коммутатора 2.

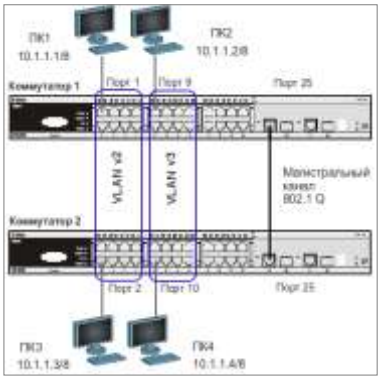
Проверьте доступность соединения между рабочими станциями командой ping:
ping <IP-address>

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

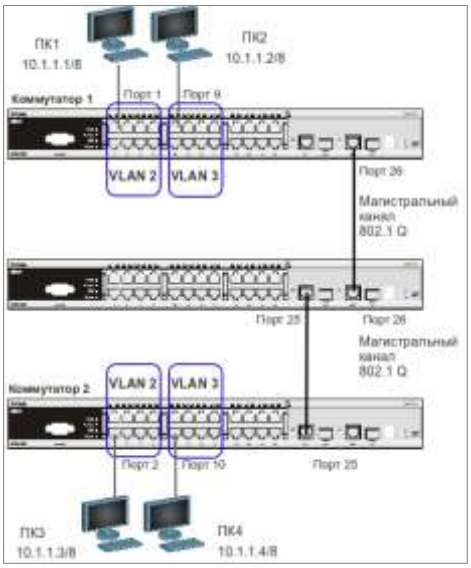
– от ПК1 к ПК2 и ПК4 Не доступен
– от ПК2 к ПК1 и ПК3 Не доступен

Задание:

1 Постройте топологию сети.



2 Выполните настройку коммутатора.



Краткие теоретические сведения:

Существуют два основных способа, позволяющих устанавливать членство в VLAN:

статические VLAN;

динамические VLAN.

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

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

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

Порт с поддержкой протокола GVRP подключается к сети VLAN только в том случае, если он непосредственно получает оповещение о ней. Если порт с поддержкой протокола 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.

Порядок выполнения работы:

Настройка коммутатора 1

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

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

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

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

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

Проверьте настройки VLAN:

```
show vlan
```

Настройте объявление о VLAN v2 и v3:

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

Включите работу протокола GVRP:

```
enable gvrp
```

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

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

Повторите процедуру настройки для коммутатора 2.

Настройка коммутатора 3

Включите работу протокола GVRP:

```
enable gvrp
```

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

```
config port_vlan all gvrp_state enable
```

Проверьте настройки VLAN на коммутаторе 3:

```
show vlan
```

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

```
show port_vlan
```

Запишите ваши наблюдения: *На коммутаторе №3 вланы v2, v3 создались динамически, и добавились в тегированном виде на порты 25,26.*

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

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

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.1 Передача данных по сети

Лабораторная работа № 12

Ограничение административного доступа к управлению коммутатором.

Формируемая(-ые) компетенция(-и):

Цель работы: Изучить механизмы ограничения административного доступа к управлению коммутатором.

Выполнив работу, Вы будете:

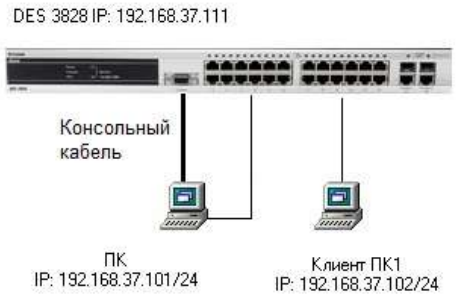
Уметь: использовать механизмы ограничения административного доступа к управлению коммутатором.

Материальное обеспечение:

Коммутатор DES-3828	1 шт.
Рабочая станция	2 шт.
Кабель Ethernet	2 шт.
Консольный кабель	1 шт.

Задание:

1 Постройте топологию сети



2 Выполните настройку коммутатора.

Краткие теоретические сведения:

В современных сетях, особенно в сетях провайдеров услуг, необходимо осуществлять не только защиту периметра сети и ограничения передачи трафика, но и контроль над консолями управления активным оборудованием, минимизировать доступ к средствам управления, учетным административным записям коммутатора.

- SSL (Secure Sockets layer, уровень защищенных сокетов) – криптокрафический протокол, обеспечивающий безопасную передачу данных по сети Интернет. При его использовании создается защищенное соединение между клиентом и сервером. Используется шифрование с открытым ключом для подтверждения подлинности отправителя и получателя.

Для доступа к Web-страницам, защищенным протоколом SSL, в адресной строке браузера вместо обычного префикса http, применяется префикс https, указывающий на то, что будет использоваться SSL-соединение. Стандартный TCP-порт для соединения по протоколу https – 443. Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат.

- SHH (Secure Shell, «безопасная оболочка») – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой. Сходен по функциональности с протоколом Telnet, но. В отличие от него, шифрует весь трафик, включая и передаваемые пароли. SHH допускает

выбор различных алгоритмов шифрования. SHH позволяет безопасно передавать в незащищенной среде практически любой другой сетевой прокол.

Порядок выполнения работы:

Настройка «доверенного узла» (Trusted Host)на DES 3828

1. Настройте IP-адрес интерфейса управления коммутатора:
   config ipif System ipaddress 192.168.37.111/24
2. Создайте доверенную рабочую станцию, с которой разрешено управление коммутатором
   create trusted_host 192.168.37.101
3. Посмотрите список доверенных узлов сети **show trusted_host**
4. Проверьте возможность управления коммутатором со станций ПК И ПК1
   telnet 192.168.37.111
5. Запишите, что вы наблюдаете
   _____.
6. Удалите доверенную станцию управления **delete trusted_host ipaddr 192.168.37.101**
7. Создайте сеть, из которой разрешено управление коммутатором
   create trusted_host network 192.168.37.0/24
8. Проверьте возможность управления коммутатором со станций ПК И ПК1
   telnet 192.168.37.111
9. Запишите, что вы наблюдаете
   _____.
10. Удалите сеть, из которой разрешено управление коммутатором
    delete trusted_host network 192.168.37.0/24

Внимание! После создания IP-адресов доверенных станций или сетей управления управление коммутатором через Web-интерфейцс или через Telnet будет доступно только с этих станций или сетей. Максимальное количество объектов управления – 10.

2. Включение режима шифрования паролей учетных записей в конфигурационных формах

11. Создайте учетную запись пользователя *swadmin* **create account admin swadmin**
12. Посмотрите созданную учетную запись **show account**
13. Посмотрите информацию и способ хранения паролей в конфигурационном файле
    show config current_config
14. Включите хранение пароей в зашифрованном виде **enable password encryption**
15. Посмотрите тнформацию и способ хранения паролей в конфигурационном файле
    show config current_config
16. Отключите режим шифрования паролей **disable password encryption**
17. Дешифруйте пароль учетной записи swadmin в конфигурационном файле
    config account swadmin encrypt plain_text dlink
18. Посмотрите выполнение дешифрования
    show config current_config
19. Запишите, что вы наблюдаете
    _____

3. Настройка Web-консоли (по протоколу SSL)

13. Включите режим SSL (при этом автоматически будет отключен режим Web) **enable ssl**
14. Попробуйте зайти на сайт через консоль SSL **https://192.168.37.111**

15. Какой вы сделаете вывод?
Запишите_____

4. Настройка Secure Console (SSH)

6. Включите функцию SSH **enable ssh**
7. Проверьте включение встроенного сервера SSH **show ssh server**
8. Измените период времени смены ключей SSH (по умолчанию ключи никогда не изменяются) **config ssh server rekey 10min**
9. Сконфигурируйте настройки пользователя SSH (учетная запись пользователя уже должна быть создана) **config ssh user dlink authmode password**
10. Проверьте возможность управления коммутатором через SSH-консоль.

Заполните в тетради таблицу.

Команда	Назначение
create trusted_host	
show trusted_host	
delete trusted_host ipaddr	
create trusted_host network	
delete trusted_host network	
create account	
show account	
show config current_config	
disable password encryption	
enable ssl	
enable ssh	
show ssh server	
config ssh server rekey 10min	

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.2 Сетевые архитектуры

Лабораторная работа № 13

Команды мониторинга

Цель работы: изучить основные команды мониторинга работы коммутаторов D-Link.

Выполнив работу, Вы будете:

уметь:

-применять основные команды мониторинга компьютерной сети.

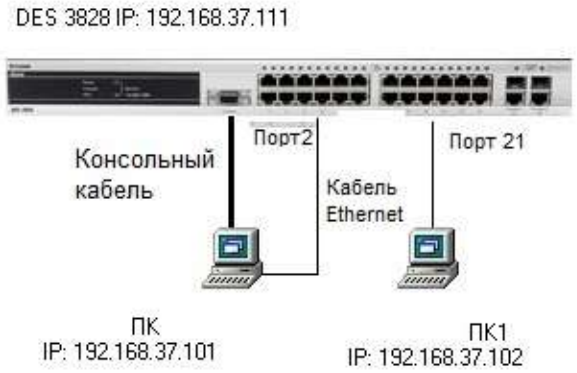
Материальное обеспечение:

Коммутатор DES-3828	1 шт.
Рабочая станция	2 шт.
Консольный кабель	1 шт.
Кабель Ethernet	2 шт.

Задание:

1 Постройте топологию сети.

2 Выполните настройку коммутатора.



Краткие теоретические сведения:

Мониторинг работоспособности компьютерной сети является очень важным элементом управления сетью. Он позволяет быстро локализовать проблему, найти источник сбоя. Посмотреть загрузку сети, оценить возможность масштабирования сети.

Порядок выполнения работы:

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-атаки 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 счётчики статистики на порте:
clear counters ports 2

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

Посмотрите загрузку ЦПУ коммутатора:
show utilization cpu

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

1. Возможные атаки на коммутатор, неправильная настройка сети. Данная проблема может быть решена путём включения функции Safeguard Engine.
2. Неправильная настройка ACL или других функций коммутатора, влияющих на производительность и работу CPU.
3. Некорректная работа ПО (Firmware) коммутатора при работе некоторых функций. Данная проблема может быть решена путём обновления ПО коммутатора.

Посмотрите загрузку портов коммутатора:
show utilization ports

Примечание: с помощью данной команды можно посмотреть загрузку портов коммутатора и объем принимаемого и передаваемого ими трафика в секунду.
Посмотрите журнал работы коммутатора:
show log
Посмотрите журнал работы коммутатора с определенного **индекса (ID):**
show log index 5

Очистите журнал работы:
clear log

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

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

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.

Тема 2.2 Сетевые архитектуры

Лабораторная работа № 14

Списки управления доступом

Цель работы: на коммутаторе D-Link настроить списки управления доступом, используя в качестве критериев фильтрации MAC- адрес.

Выполнив работу, Вы будете:

уметь:

-настраивать списки управления доступом, используя в качестве критериев фильтрации MAC- адрес.

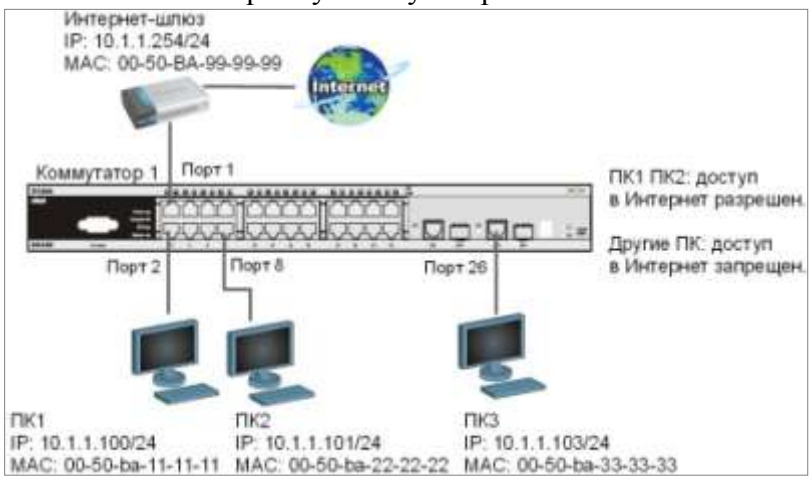
Материальное обеспечение:

Коммутатор DES-3528	1 шт.
Рабочая станция	3 шт.
Консольный кабель	1 шт.
Кабель Ethernet	3 шт.
Интернет-шлюз	1 шт.

Задание:

1 Постройте топологию сети.

2 Выполните настройку коммутатора.



Краткие теоретические сведения:

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, разрешённых для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS, путём классификации трафика и переопределения его приоритета.

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

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

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

Порядок выполнения работы:

Разрешить пользователям ПК1 и ПК2 доступ в Интернет, остальным пользователям доступ в Интернет 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.

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 profile_id 10 profile_name 10 ethernet
source_mac FF-FF-FF-FF-FF-FF destination_mac FF-FF-FF-FF-FF-FF
```

Создайте правило для профиля 10, разрешающее доступ ПК1, подключённого 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 profile_id 11 profile_name 20 ethernet desti-
nation_mac FF-FF-FF-FF-FF-FF
```

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

```
config access_profile profile_id 11 add access_id 21 ethernet desti-
nation_mac 00-50-ba-99-99-99 port 1-10 deny
```

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
Протестируйте соединение до Интернет-шлюза командой ping.
Что вы наблюдаете?

_____

Подключите ещё 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
```

Удалите все профили ACL:
```
delete access_profile all
```

Форма представления результата: отчет в тетради

Критерии оценки:

«5» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь, студент отвечает на все вопросы преподавателя по теме работы.

«4» - лабораторная работа выполнена полностью, этапы выполнения работы, алгоритмы и теоретический материал не полностью записаны в тетрадь, студент затрудняется отвечать на вопросы преподавателя по теме работы.

«3» - лабораторная работа выполнена на 70% и более, этапы выполнения работы, алгоритмы и теоретический материал записаны в тетрадь не в полном объеме, студент не отвечает на все вопросы преподавателя по теме работы.

«2» - лабораторная работа выполнена мене 70%.