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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

ПМ. 02. РАЗРАБОТКА И АДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ
МДК.02.01 Инфокоммуникационные системы и сети
Тема 1.1. Компьютерные сети
для студентов специальности
09.02.03 Программирование в компьютерных системах
(базовой подготовки)

Магнитогорск, 2017

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

Протокол № 7 от 14 марта 2017

Методической комиссией МпК
Протокол №4 от «23» марта 2017г

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

Методические указания по выполнению практических занятий разработаны на основе рабочей программы ПМ. 02. Разработка и администрирование баз данных.

Содержание практических работ ориентировано на формирование общих и профессиональных компетенций по основной профессиональной образовательной программе по специальности 09.02.03 Программирование в компьютерных системах МДК.02.01, Темы 1. Компьютерные сети.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 5

2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ 7

Практическая работа № 1 7

Практическая работа № 2 11

Практическая работа № 3 17

Практическая работа № 4 22

Практическая работа № 5 30

Практическая работа № 6 33

Практическая работа № 7 36

Практическая работа № 8 37

Практическая работа № 9 40

Практическая работа № 10 44

Практическая работа № 11 51

Практическая работа № 12 54

Практическая работа № 13 57

Практическая работа № 14 61

Практическая работа № 15 63

Практическая работа № 16 66

Практическая работа № 17 70

Практическая работа № 18 74

Практическая работа № 19 78

Практическая работа № 20 83

Практическая работа № 21 84

Практическая работа № 22 88
Практическая работа № 23,24 96

1 ВВЕДЕНИЕ

Важную часть теоретической и профессиональной практической подготовки студентов составляют практические занятия.

Состав и содержание практических работ направлены на реализацию действующего федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах.

Ведущей дидактической целью практических занятий является формирование практических умений - профессиональных (умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности), необходимых в последующей учебной деятельности по профессиональным модулям.

В соответствии с рабочей программой ПМ. 02. Разработка и администрирование баз данных, МДК.02.01 Инфокоммуникационные системы и сети, Темой 1. Компьютерные сети предусмотрено проведение практических работ.

В результате их выполнения, обучающийся должен:

уметь:

- проводить контроль, диагностику и восстановление работоспособности компьютерных систем и комплексов;
- проводить системотехническое обслуживание компьютерных систем и комплексов;
- проводить технические испытания компьютерных систем и комплексов, инсталляции, конфигурирование и настройку операционной системы, драйверов, резидентных программ.

Содержание практических занятий ориентировано на формирование общих компетенций по профессиональному модулю основной профессиональной образовательной программы по специальности:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

И овладению профессиональными компетенциями:

ПК 2.3. Решать вопросы администрирования базы данных.

ПК 2.4. Реализовывать методы и технологии защиты информации в базах данных.

Выполнение студентами практических работ по ПМ. 02. Разработка и администрирование баз данных, МДК.03.01 Техническое обслуживание и ремонт компьютерных систем и комплексов, Теме 4. Компьютерные сети и телекоммуникации направлено на:

- 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 для проведения опытов;
- 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.

Продолжительность выполнения практической работы составляет не менее двух академических часов и проводится после соответствующего занятия, которое обеспечивает наличие знаний, необходимых для ее выполнения.

2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Тема 1.1. Компьютерные сети

Практическая работа № 1

Построение схемы компьютерной сети в среде FPinger

Цель работы: знакомство с программой FPinger и построение схемы компьютерной сети.

Выполнив работу, Вы будете:

уметь:

- визуализировать компьютерную сеть;
- отследить включенные компьютеры;

Материальное обеспечение:

учебно-лабораторный комплекс «Локальные компьютерные сети»

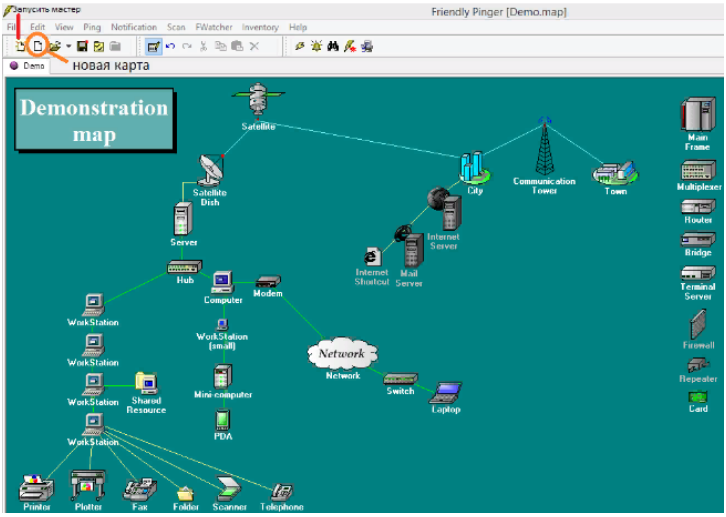
Порядок выполнения работы:

Friendly Pinger - это бесплатное приложение для администрирования, мониторинга и инвентаризации компьютерных сетей, позволяет выполнять:

- Визуализацию компьютерной сети в 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 "просматривает информацию" в Вашем компьютере и какие файлы скачивает;
- 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.

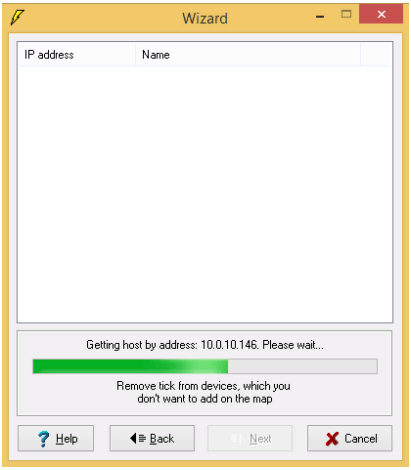
После установки, потребуется запустить fpinger. Далее вам предлагается посмотреть на задачу по мониторингу с именем Demo. Это

гипотетическая (вымышленная) сеть для демонстрации графической возможности этой программы.



После просмотра карты Demo, создайте новую чистую задачу по мониторингу своей сети и запустите Мастера для первоначальной настройки. Далее вам предложат указать диапазон адресов локальной сети, например 192.168.1.0-200, который требуется мониторить. Этим мы указали для Fpinger, чтобы он проверил заданный диапазон. Нажав далее, Fpinger начинает пинговать хосты.

Найденные устройства отображаются в этом окне. Не волнуйтесь если Fpinger не нашел вашего устройства, добавлять новые объекты мониторинга можно в ручную, не надеясь на мастера настроек.



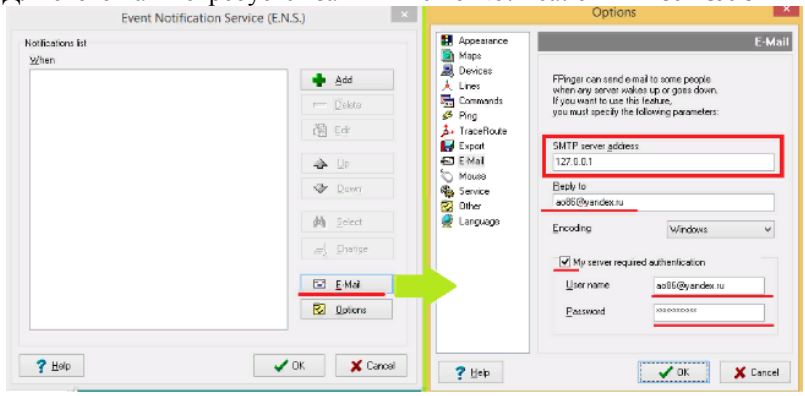
После добавления устройств, надо обязательно настроить уведомления по почте и/или СМС, в случае не работы одного из устройств вашей сети.

Настройка уведомлений

Допустим есть два сервера Asterisk и 1С.

Мы хотим чтобы при падении любого из серверов, высылался отчет на почтовый ящик от yandex.ru.

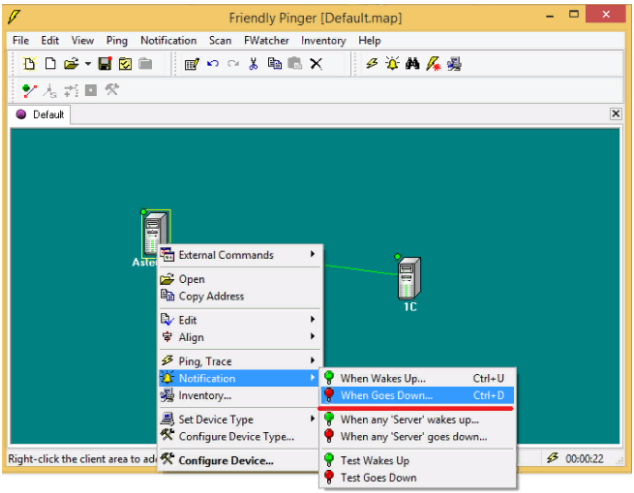
Для этого нам потребуется зайти в меню Notification -> Notification



В окне Options -> E-Mail, пишем свой e-mail и пароль, SMTP сервер указываем как **127.0.0.1** (заметьте не smtp.yandex.ru).

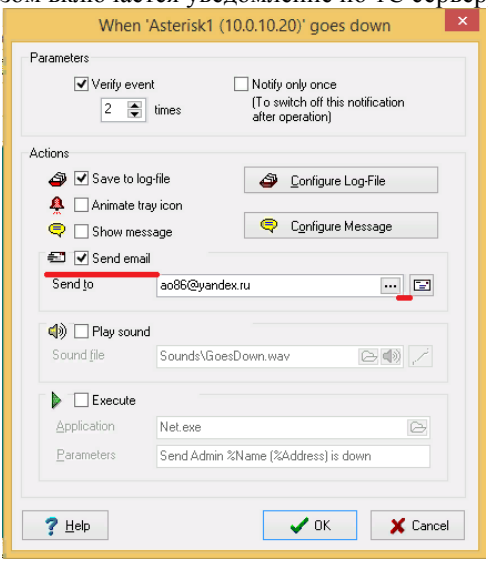
Так как Fpinger не поддерживает SSL (465) по email, мы сделаем проброс через stunnel.

Теперь мы должны на каждом сервере включить уведомления.



Сначала надо сохранить карту File -> Save.

Когда пропадает пинг, будет высылаться отчет на email. Аналогичным образом включается уведомление по 1С серверу.



Теперь надо настроить stunnel:

1. Скачиваем stunnel с официального сайта https://www.stunnel.org/downloads/stunnel-5.30-installer.exe

2. Устанавливаем

3. Редактируем его конфигурационный файл **C:\Users\Almas\AppData\Local\stunnel\config\stunnel.conf**

Теперь надо чтобы stunnel прописался в службах:

C:\Users\Almas\AppData\Local\stunnel\bin\stunnel.exe -install

Запустим stunnel:

C:\> net start stunnel

И проверяем как приходят отчеты.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 2
Построение одноранговой сети

Цель работы: научиться создавать одноранговые сети при использовании топологии сети с шиной типа «звезда».

Выполнив работу, Вы будете:

уметь:

- выбирать аппаратное и программное обеспечение, необходимое для создания одноранговых сетей;
-создавать одноранговую сеть;
-выполнять тестирование одноранговых сетей;

Материальное обеспечение:

учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

1. Для всех компьютеров присоедините сетевые адаптеры рабочих станций, входящих в рабочую группу, к хабу рабочей группы, используя кабель пятой категории с RJ-45 коннекторами.

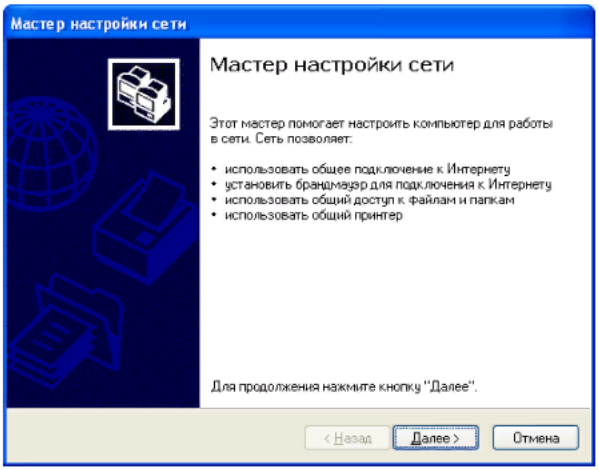
2. Запустите те компьютеры, которые будут объединены в индивидуальные рабочие группы.

Для того, чтобы начать создание одноранговой сети для рабочей группы, запустите «**Мастер настройки сети**», выполните следующие действия на одном компьютере каждой сети:

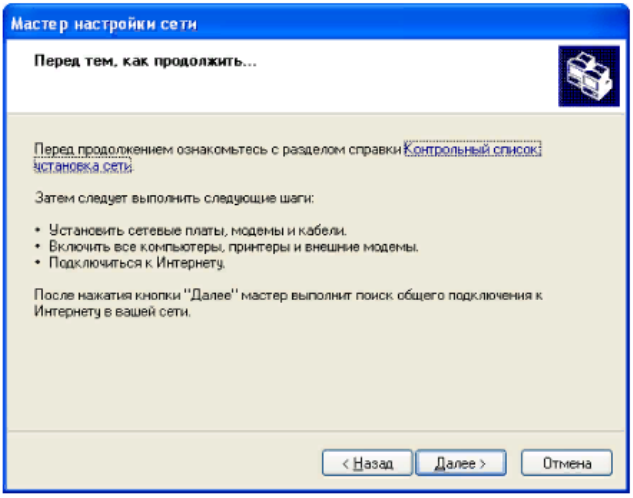
3. Нажмите **Пуск**, затем щелкните **Панель управления**.

4. Щелкните **Сетевые подключения**, а затем на правой панели щелкните **Установить домашнюю сеть или сеть малого офиса**.

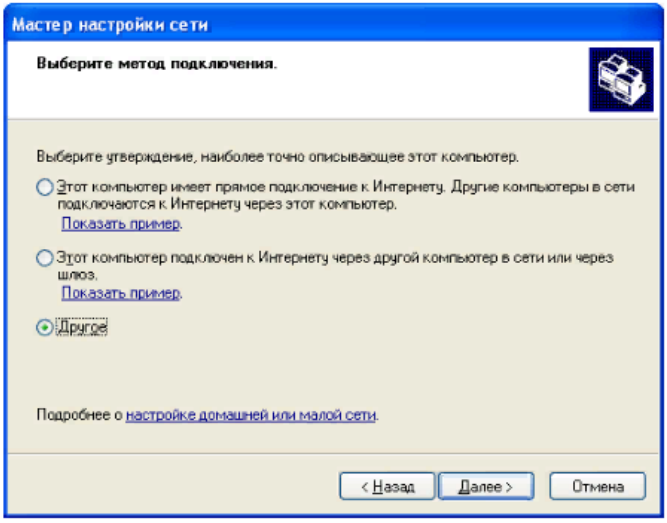
5. На странице **Мастер настройки сети** нажмите **Далее**.



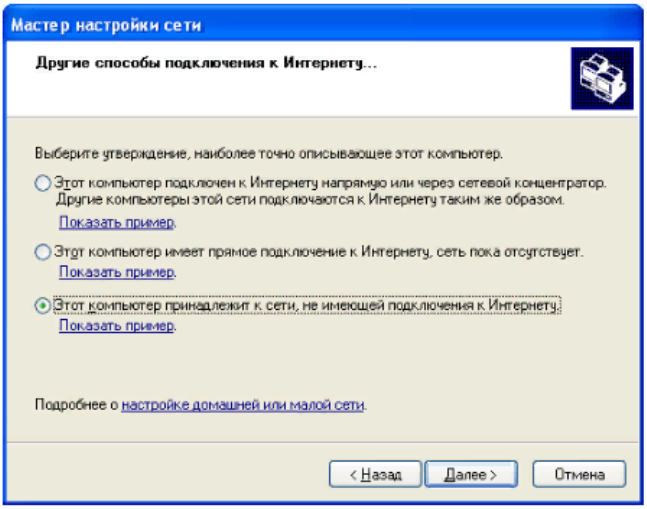
6. На следующей странице просмотрите требования и, убедившись, что все соответствует, нажмите **Далее**.



7. На странице **Выберите метод подключения** выберете **Другое** и затем нажмите **Далее**.



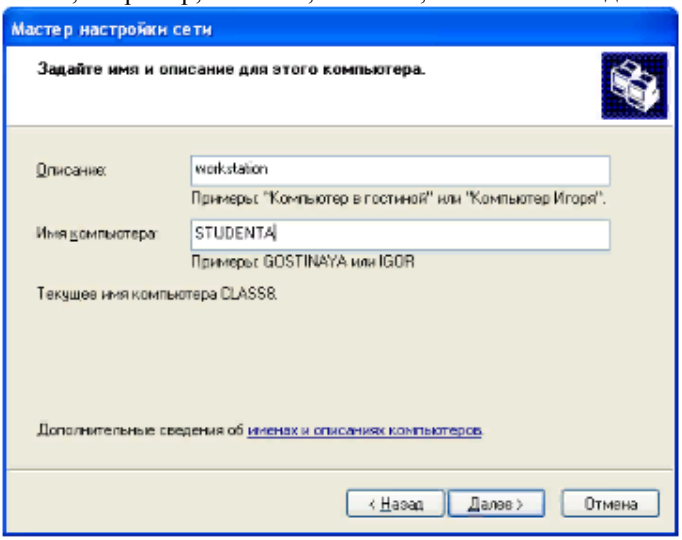
8. На странице **Другие способы подключения к Интернету** выберете **Этот компьютер принадлежит к сети, не имеющей подключения к Интернету**, затем щелкните Далее.



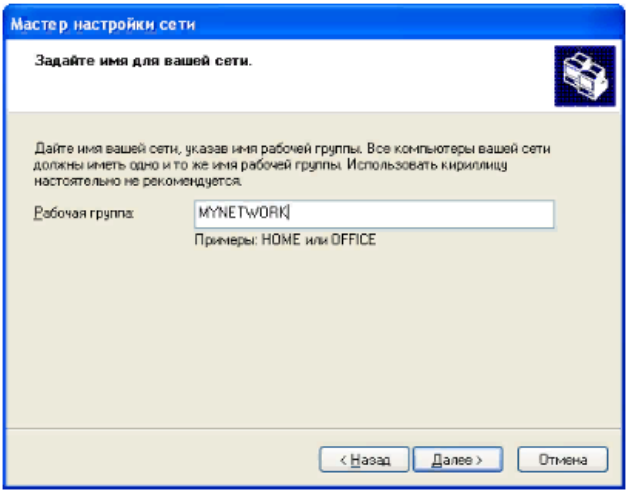
9. В текстовое поле Описание введите **workstation.**

10. В текстовое поле Имя компьютера введите уникальное имя (например: STUDENTA), называя тем самым свою рабочую станцию в сети, а затем щелкните **Далее.**

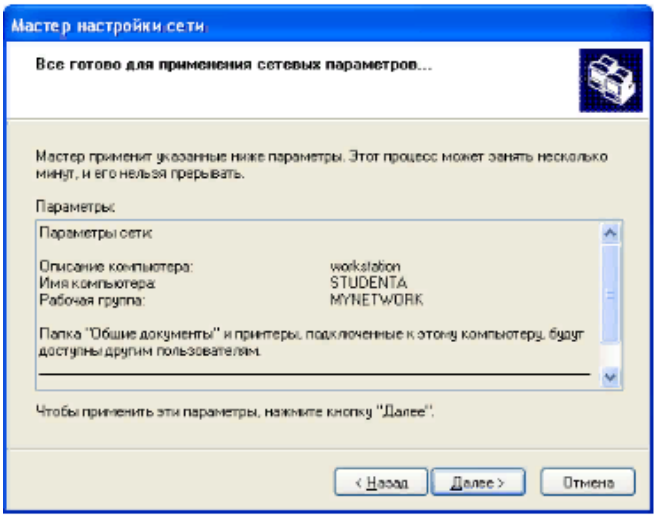
Замечание: Когда вы даете имя своему компьютеру, убедитесь, что это имя уникально в данной рабочей группе. Именуйте компьютеры последовательно, например, StudentB, StudentC, StudentD и так далее.



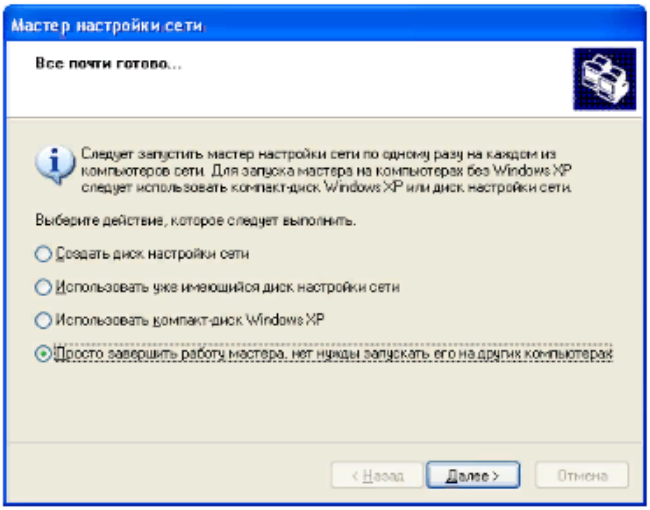
11. На странице **Задайте имя для вашей сети** смените стандартное имя Рабочей группы на **MYNETWORK**.



12. На странице **Все готово для применения сетевых параметров** проверьте установки и затем щелкните **Далее** для того, чтобы начать процесс создания сетевого соединения.



13. На следующей странице щелкните **Просто завершить работу мастера**, а затем щелкните **Далее.**



14. На странице **Завершение работы мастера настройки сети** щелкните **Готово.**

15. Если вам будет предложено перезагрузить ваш компьютер, то щелкните **Да.**

16. Начните работу на своем компьютере.

17. Запустите «**Мастер настройки сети**» (шаги с 3 по 13) на остальных компьютерах в каждой сети, чтобы подключить их к рабочей группе MYNETWORK

Для проверки работы одноранговой сети создайте папку для совместного использования на каждом компьютере. Выполните следующие действия на каждом компьютере.

18. Щелкните **Пуск**, отметьте **Все программы**, щелкните **Стандартные**, и затем щелкните **Проводник.**

19. На левой панели щелкните **Мои документы** в открывшемся окне выберете **Файл**, затем отметьте **Создать**, и щелкните **Папка.**

21. Введите Имя папки, которое состоит из вашего имени и слова Папка (например: Папка Глеба), и нажмите **Enter.**

22. В окне **Мои документы** щелкните правой кнопкой мыши по только что созданной папке и выберите пункт меню **Общий доступ и безопасность.**

23. Во вкладке **Доступ** щелкните **Открыть общий доступ к этой папке-ОК**.

24. В правой половине открывшегося окна дважды щелкните по только что созданной папке.

25. В открывшемся окне щелкните **Файл**, отметьте **Создать** и щелкните **Текстовый документ.**

26. Введите имя документа (используйте ваше имя для названия файла) и нажмите **Enter.**

27. Дождитесь, пока остальные студенты создадут файлы в директории для совместного использования.

Для доступа учащихся к совместно используемым файлам, созданным на других компьютерах, необходимо следовать указаниям:

28. Щелкните **Пуск**, отметьте **Все программы**, щелкните **Стандартные**, а затем щелкните на **Проводник.**

29. На левой панели щелкните **Сетевое окружение**, а затем щелкните **Отобразить** компьютеры рабочей группы.

Замечание: теперь вы можете увидеть список компьютеров рабочей группы сети MYNETWORK.

30. На правой панели дважды щелкните по какому-либо компьютеру (не своему) для того, чтобы найти файлы, созданные другими учащимися для совместного пользования.

31. На правой панели дважды щелкните по одной из созданных папок для получения доступа к файлам, созданным другими учащимися.

32. На правой панели дважды щелкните по имени файла, чтобы открыть его. Итак, ,вы получили удаленный доступ к файлам на другом компьютере.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 3
Обжим и монтаж кабельных систем ЛВС

Цель работы: Получить навыки по подключению отдельного ПК к ЛВС, исследованию топологии и организации ЛВС небольшого подразделения. Изучить простейшие приемы работы в сетевой среде и команды ОС, используемые для этого.

Выполнив работу, Вы будете:

уметь:
- выполнять обжим и монтаж кабельных систем ЛВС;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Основные правила, которые необходимо соблюдать при монтаже кабельной системы:

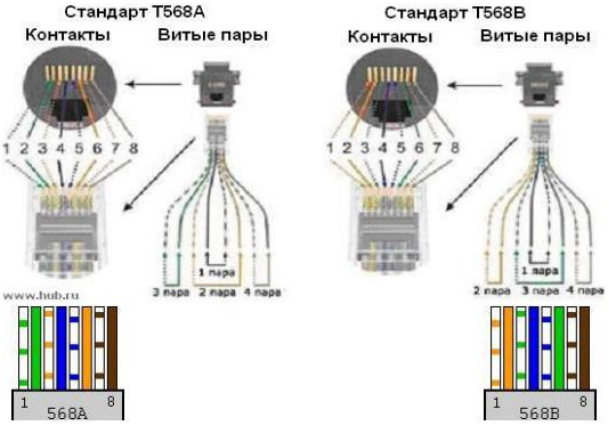
– Не допускайте растяжения кабеля во время монтажных работ.

– Радиус изгиба кабеля должен быть не меньше 10 внешних диаметров кабеля.

– Удалять оболочку кабеля следует лишь настолько, сколько требуется для монтажа. Сохраняйте целостность скручивания пар как можно ближе к месту монтажа, что обеспечивает минимальное влияние сигналов различных пар друг на друга. Раскрученные во время монтажа кабельные пары не следует скручивать снова, т.к. неправильное скручивание отрицательно влияет на рабочие характеристики.

– Кабели ЛВС не должны располагаться рядом с силовыми проводами (220в), флуоресцентными лампами, силовыми трансформаторами и другими устройствами, мощные электромагнитные поля которых, создают помехи и оказывают отрицательное воздействие на качество передачи сигнала.

Вилка RJ-45 монтируется обжимным способом с помощью специального обжимного инструмента в соответствии с одним из стандартов T568A или T568B.



Для разделки витых пар используют специальное устройство, которое имеет три рабочие области и соответственно выполняет три функции.

1. Ближе всего к рукояткам устройства располагается область, в которой установлен нож для обрезания проводников витой пары.

2. В центре находится гнездо для обжима разъема.

3. В верхней части устройства- область для зачистки наружной изоляции витой пары (внутренняя изоляция проводников не зачищается, а как уже было сказано прорезается контактами разъема).

Последовательность операций при разделке разъема витой пары:

1. Вначале проводят зачистку наружной изоляции кабеля. При зачистке плоского кабеля его упирают в специальный выступ на устройстве, расположенный в области зачистки, чтобы получить глубину зачистки под стандартный разъем, зажимают кабель и рывком производят зачистку. Немного более сложным выглядит процесс зачистки круглых кабелей витых пар. Наружную изоляцию круглого кабеля лучше только слегка надрезать, осторожно поворачивая его в области зачистки, а затем снять кусочек изоляции по кольцевому надрезу вручную.

2. После зачистки разводят провода витой пары в одной плоскости в определенном порядке, выравнивают длину всех проводов и еще раз ровно подрезают. Порядок разводки проводов для разъемов RJ-45 определяется стандартом EIA/TIA568B. Цифрами на рисунке обозначены номера контактов для витой пары с восьмью и четырьмя жилами .

3. Затем производят заправку проводников в разъем и их опрессовку. Рекомендуется по возможности использовать разъемы без вставки, так как процесс заправки проводников в корпус такого разъема выполняется проще.

3а. Если конструктивно разъем выполнен без вставки, то проводники аккуратно заправляются в его корпус до упора в торец разъема. Затем вставляют разъем в гнездо обжимного устройства и надавливают до тех пор пока устройство полностью не закроется.

3б. Если в конструкцию разъема входит вставка, то сначала на проводники витой пары надевается вставка.

Вставка имеет форму крышки спичечного коробка, на одной из поверхностей которого имеются прорези по количеству проводников в витой паре. Вставку надевают на проводники таким образом: чтобы прорези были обращены к корпусу разъема. После насаживания вставки проводники витой пары еще раз подрезают и выравнивают срез с краем вставки.

Для закрепления вставки в этом положении полезно у противоположного ее конца обжать проводники пальцами, чтобы вставка не смещалась.

Затем вставку с проводниками вставляют в корпус разъема до тех пор пока она не упрется в торец разъема и обжимают разъем также как в случае разъема без вставки.

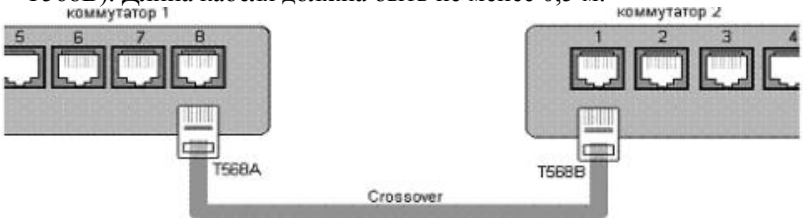
Правила монтажа определяются типом предполагаемого соединения. Возможны два варианта:

– Компьютер соединяется с сетевым концентратором (hub) или коммутатором (switch) используя «прямую» разводку кабеля (стандарт T568B);

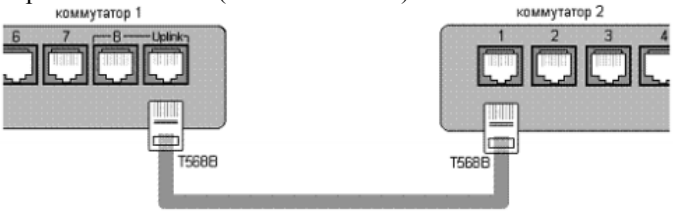
– Соединение между коммутаторами или концентраторами, такие как “hub – hub”, “switch – switch”, “hub – switch” производятся с помощью кабеля с «перевернутой» разводкой (Uplink или Crossover). С одной стороны кабель разводится по стандарту T568A, а с другой по стандарту T568B.

Подключение сетевого оборудования.

Коммутаторы и концентраторы подключаются к локальной сети одинаково. Если используется несколько коммутаторов, то они объединяются между собой кабелем UTP с «перевернутой» разводкой (T568A – T568B). Длина кабеля должна быть не менее 0,5 м.



Во многих моделях коммутаторов наряду с простыми портами используется дополнительный порт “Uplink”. Он совмещен с одним из простых портов и имеет «перевернутую» разводку в соответствии со стандартом T568A. Используя этот порт можно подключать второй коммутатор простым кабелем (T568B – T568B).

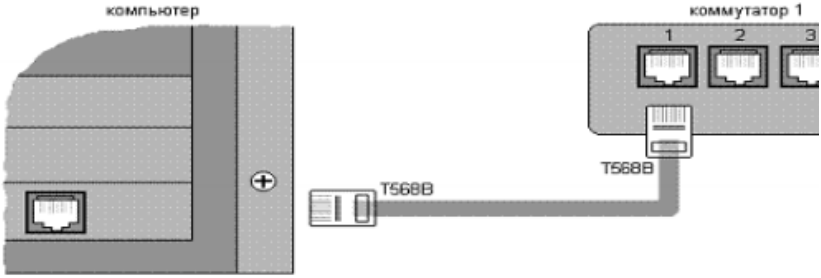


На рисунке показано применение дополнительного порта “Uplink” совмещенного с портом №8. При этом сам порт №8 должен оставаться пустым.

В современных коммутаторах реализована функция автоматического определения типа кабеля. Каждый порт коммутатора может сам определить стандарт подключенного к нему кабеля и порт сам определяет, в каком режиме ему работать. Функция автоматического определения типа кабеля значительно облегчает работу администратора сети. Для подключения ПК к ЛВС необходимо:

– установить сетевой адаптер, поддерживающий сетевую технологию Ethernet

– осуществить физическое подключение к сетевому оборудованию с помощью кабеля



Для соединения двух ПК между собой с использованием только сетевых адаптеров используют кабель с «перевернутой» разводкой (Uplink или Crossover) по стандарту T568A – T568B.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 4
Работа с диагностическими утилитами протокола TCP/IP

Цель работы: Познакомиться со средствами диагностики сети и поиска неисправностей стека TCP/IP.

Выполнив работу, Вы будете:
уметь:
- применять диагностические утилиты для исследования сети и поиска неисправностей в настройке TCP/IP;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Диагностические утилиты TCP/IP.

Целью устранения неисправностей в настройке TCP/IP является восстановление нормальной работы сети. Для поиска неисправностей можно использовать специальные диагностические утилиты, предназначенные для проверки конфигурации стека TCP/IP и тестирования сетевого соединения. Список некоторых утилит приведен в таблице

Утилита	Применение
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу).
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.

netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

Проверка правильности конфигурации TCP/IP.

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

Параметры:

all выдает весь список параметров. Без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

renew[adapter] обновляет параметры конфигурации DHCP для указанного сетевого адаптера;

release[adapter] освобождает выделенный DHCP IP-адрес;

adapter – имя сетевого адаптера;

displaydns выводит информацию о содержимом локального кэша клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

- если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;
- если IP-адреса дублируются, то маска сети будет 0.0.0.0;
- если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0 .

3. **Тестирование связи с использованием утилиты ping.**

Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование указанного узла и позволяет измерить время прохождения пакетов от данного узла до любого другого узла сети. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. (Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.)

Команда ping проверяет соединение с удаленным хостом, посылая к этому хосту несколько IP-пакетов и ожидая ответы на них. При этом она измеряет интервал времени, в течение которого пакет вернулся, а также показывает соотношение количества отосланных пакетов к количеству принятых, то может служить субъективной оценкой «качества связи» между узлами. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

Утилита использует протокол ICMP. Посылаемые и получаемые IP-пакеты – это эхо-запросы и эхо-ответы протокола ICMP.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение «Request time out» (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа –w.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Утилита ping используется следующими способами:

1) Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address): ping 127.0.0.1

Если тест успешно пройден, то вы получите следующий ответ:

Reply from 127.0.0.1

Reply from 127.0.0.1

Reply from 127.0.0.1

Reply from 127.0.0.1

2) Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера:

ping IP-адрес_локального_хоста

3) Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping IP-адрес_шлюза

4) Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

ping IP-адрес_удаленного хоста

Синтаксис утилиты ping:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] |

[-k host-list]] [-w timeout] destination-list

Параметры:

-t выполняет команду ping до прерывания. Control-Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

-a позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count посылает количество пакетов ECHO, указанное параметром count;

-l length посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos устанавливает тип поля «сервис» в величину tos;

-r count записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;

-s count позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая

маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;

-w timeout указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);

-destination-list указывает удаленный хост, к которому надо направить пакеты ping.

Изучение маршрута между сетевыми соединениями с помощью утилиты tracert.

Tracert - это утилита трассировки маршрута. Она позволяет проследить путь от данного узла до любого другого узла сети Internet. Хост за хостом показывается прохождение IP-пакетов, при этом выводится название и IP-адрес каждого пройденного хота, а также значение интервала времени, в течение которого был получен ответ.

Утилита использует поле TTL (time-to-live, время жизни) из заголовка IP-пакета и сообщения об ошибках протокола ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP “Time Exeeded” (Время истекло). Маршрут исследуется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет

достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста

Параметры:

-d указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops указывает максимальное число хопов для того, чтобы искать цель;

-j host-list указывает нежесткую статическую маршрутизацию в соответствии с host-list;

-w timeout указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

Утилита ARP.

Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Утилита arp выводит для просмотра и изменения таблицу трансляции адресов.

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметры:

-s занесение в кэш статических записей;

-d удаление из кэша записи для определенного IP-адреса;

-a просмотр содержимого кэша для всех сетевых адаптеров локального компьютера;

inet_addr - IP-адрес;

eth_addr - MAC-адрес.

Утилита netstat.

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

Параметры:

-a выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n выводит информацию по всем активным соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;

-s выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет просмотреть информацию постранично;

-r выводит содержимое таблицы маршрутизации.

Упражнение 1. Получение справочной информации по командам

Вывести на экран справочную информацию по утилитам ipconfig, ping, tracert, hostname. Для этого в командной строке ввести имя утилиты без параметров или с /?. Изучить ключи, используемые при запуске утилит.

Упражнение 2. Получение имени хоста

Вывести на экран имя локального хоста с помощью команды hostname.

Упражнение 3. Изучение утилиты ipconfig

Проверить конфигурацию TCP/IP локального хоста с помощью утилиты ipconfig. Заполнить таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	

Адрес WINS-сервера	

Упражнение 4. Тестирование связи с помощью утилиты ping

1. Проверить правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверить, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.
3. Проверить функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта.
4. Проверить с помощью ping, можете ли вы обратиться к компьютерам в своей локальной сети. Сравнить результаты выполнения программы ping с указанием адреса компьютера, который отключен, и несуществующего адреса. Отличаются ли эти результаты?
5. Проверить возможность установления соединения с различными удаленными хостами, используя DNS-имена. Определите IP-адреса этих узлов. Отметить время отклика (время кругового обращения пакета). Попробовать увеличить время отклика. Как влияет размер пакета на время кругового обращения?

Упражнение 5. Определение пути IP-пакета

1. Воспользоваться командой tracert для определения числа участков маршрута от вашего компьютера к различным хостам (локальному хосту, шлюзу по умолчанию, удаленному хосту). Отметьте, через какие промежуточные узлы проходят эхо-пакеты.
2. Сравнить значения времени кругового обращения, полученные при выполнении программы ping, с числом участков маршрута, полученным при выполнении программы tracert, для ряда адресов назначения. Существует ли зависимость между продолжительностью задержки и числом участков маршрута?

Упражнение 6: Просмотр ARP-кэша

С помощью утилиты arp просмотреть ARP-таблицу локального узла.

Упражнение 7. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

1. С помощью утилиты netstat вывести перечень сетевых соединений и прослушиваемых портов локального узла.
2. Получить статистическую информацию для протоколов UDP, TCP, ICMP, IP.
3. Вывести на экран локальную таблицу маршрутизации. Изучить ее содержимое.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 5
Основные команды коммутатора. Управление коммутаторами

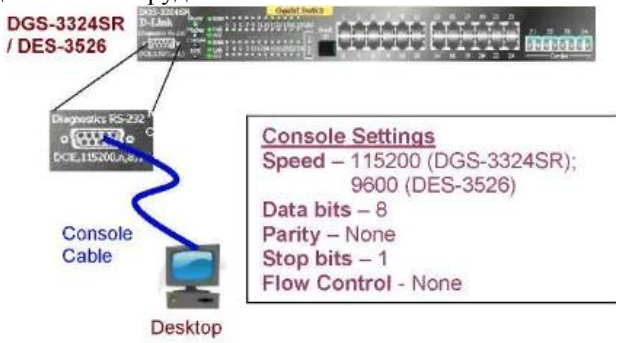
Цель работы: ознакомиться с основными командами для настройки, контроля и устранения неполадок коммутаторов D-Link

Выполнив работу, Вы будете:
уметь:
- применять основные командамы для настройки, контроля и устранения неполадок коммутаторов D-Link;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Подключите оборудование согласно схеме



Настройка DES-3828/DES-3526
1 Вызов помощи по командам
Напишите в консоли ?

Напишите в консоли *config ?*

Напишите в консоли *show ?*

2 Изменение IP-адреса коммутатора

IP-адрес по умолчанию 10.90.90.90/8

Измените IP-адрес *config ipif System vlan default ipaddress 10.1.1.10/8*

Настройка IP шлюза по умолчанию*create iproute default 10.1.1.254 1*

Замечание. IP шлюз по умолчанию назначается, если управление коммутатором осуществляется из других IP подсетей.

Проверьте настройки *show switch*

3 Управление учетными записями пользователей

Заводим учетную запись администратора *Create account admin dlink*

Указываем пароль и подтверждение пароля администратора: dlink

Enter a case-sensitive new password: dlink

Enter the new password again for confirmation: dlink

Заводим учетную запись пользователя *Create account user swuser*

Указываем пароль и подтверждение пароля пользователя:dlink1

Enter a case-sensitive new password:dlink1

Enter the new password again for confirmation:dlink1

Проверьте настройки учетных записей пользователей

show account

Отключение от режима администрирования*Logout*

Войдите в режим управления login *Username: dlink*

Password: dlink

DES-3526:4#

Изменение пароля пользователя

После ввода команды указываем старый пароль пользователя и 2 раза новый пароль. *Config account swuser*

*Enter a old password:*****

*Enter a case-sensitive new password:*****

*Enter the new password again for confirmation:*****

Удаление учетной записи *delete account swuser*

Проверьте удаление учетной записи пользователя *show account*

Внимание: Длина имени пользователя от 1-15 символов, длина пароля от 0-15 символов, максимальное количество пользователей 8.

Никогда не сохраняйте настроек конфигурации после создания пользователей не проверив, можете ли вы зайти в систему! В случае утраты сведений о Логине и Пароле, разблокировать коммутатор можно

только в сервисном центре компании Длинк! (Для старых версий firmware)

4 Настройка параметров идентификации коммутатора

Настроим имя коммутатора *config snmp system_name HQ-SW01*

Настроимместорасположение(локализацию) *config snmp system_location HQ 5F*

Настроимответственный контакт *config snmp system_contact HQ IT Department*

Проверьте внесенные параметры *show switch*

Внимание: Длина параметров идентификации коммутаторов от 0 до 255 символов.

0 символов подразумевает, что информация отсутствует

5 Настройка времени на коммутаторе

Введите команду *config time 30102007 15:45:30*

Установка часового пояса

Москва (GMT +3:00) *config time_zone operator + hour 3 min 0*

Проверьте время *show time*

Примечание: Установка времени необходима для правильного отображения информации в журналах коммутаторов (Log files)

6 Конфигурирование основных настроек портов коммутатора

Конфигурирование скорости и режима работы порта *config ports 1-5 speed 10_half*

Просмотр режима работы портов *show ports*

Подключите компьютер к порту 2 коммутатора *Что вы наблюдаете?*

Отключение работы порта *config ports 1-5 state disable*

Включение работы порта *config ports 5 state enable*

Именование порта *config ports 5 description Magistral_port_Mipk*

Проверим descriptions портов *show ports description*

Внимание! Все параметры конфигурирования порта можно сделать одновременно в одной команде.

7 Функция Factory Reset (сброс к заводским установкам)

Сбросьте в настройки по умолчанию *reset config*

Все заводские настройки по умолчанию восстановятся на коммутаторе включая IP-адрес, учетные записи пользователей и журнал историй. Коммутатор не сохранит настройки и не перегрузится.

Или *reset system*

Все заводские настройки по умолчанию восстановятся на коммутаторе исключая IP-адрес, учетные записи пользователей и журнал историй. Коммутатор не сохранит настройки и не перегрузится.

Сохраните изменения в энергонезависимую память *Save*

Перезагрузите коммутатор *Reboot*

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 6
Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов

Цель работы: изучить процесс обновления прошивки и загрузчика.

Выполнив работу, Вы будете:

уметь:

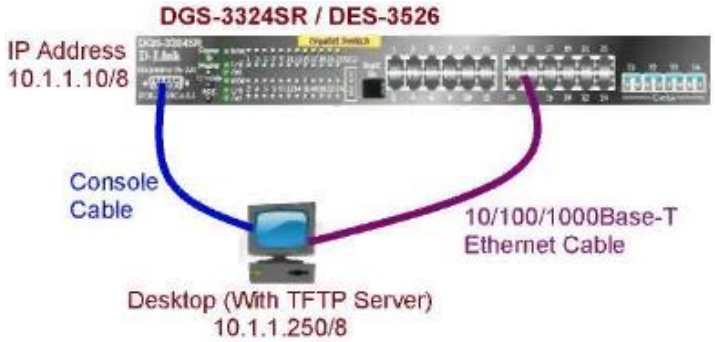
- применять команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов;

Материальное обеспечение:

учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Подключите оборудование согласно схеме



1 Подготовка к режиму обновления и сохранения прошивок коммутатора.

Настройка TFTP –сервера (на примере Tftpd32 by Ph.Jounin)

1.В настройках необходимо установить директорию приема файлов

2. Отключить все другие сервисы кроме TFTP server

Подготовка файла обновления

1. Поиск необходимого файла обновления прошивки на сайте http://www.dlink.ru (или http://www.dlink.com)

2. Выкачивание файла и перенос в директорию указанную в tftp сервере.

3. Прочитайте файл сопровождения к прошивке.

2 Загрузка файла прошивки в память коммутатора

Настройка IP-адреса *config ipif System vlan default ipaddress 10.1.1.10/8*

Настроить TFTP сервер Выбрать прошивку для загрузки (10.1.1.250/8).

Проверка доступностиTFTP сервера *Ping 10.1.1.250*

Проверка текущих прошивок firmware *show firmware information*

Загрузить прошивку на коммутатор *download firmware 10.1.1.250 xStack400B13.had image_id 2*

Официальная версия прошивки Все официальные версии прошивки включают примечания, которые описывают новые функции и последние коррекции ошибок.

Внимание: НЕ перезагружайте коммутатор во время загрузки прошивки

Выполнение команды без ключа image_id приводит к перезаписи текущей firmware!

3. Конфигурирование загрузки firmware коммутатора

Смена прошивки с которой загружается коммутатор*config firmware image_id 2 boot_up*

Сохраните изменения *Save*

Перезагрузите коммутатор Обновленная прошивка вступит в силу только после перезагрузки.

Проверьте информацию прошивки *show firmware information*

Что вы наблюдаете? Запишите в отчете

2.4 Управление изменениями конфигураций

Просмотр текущей версии коммутатора (в RAM) *show config current_config*

Просмотр конфигурации загрузки (из NVRAM) *show config config_in_nvram*

Выгрузка конфигурации на TFTP сервер *upload configuration 10.1.1.250 config.txt*

Измените в выгруженной конфигурации в разделе management имя коммутатра с HQ-SW01 на HQ-SW02 *# MANAGEMENT*

enable snmp traps

enable snmp authenticate traps

config snmp system_name HQ-SW02

disable rmon

Загрузим измененную конфигурацию *Download configuration 10.1.1.250 config.txt*

Проверим изменилось ли имя коммутатора *show switch*

Что вы наблюдаете? Запишите в отчете

5 Выгрузка Log файлов

Выгрузим Log на TFTP сервер *upload log 10.1.1.250 logfiles.txt*

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 7
Преобразование форматов IP-адресов

Цель работы: обобщение и систематизация знаний по теме Передача данных по сети, научиться определять идентификаторы сетей.

Выполнив работу, Вы будете:
уметь:
-преобразовывать форматы IP-адресов;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

В двоичном формате каждому биту в октете сопоставлено определенное десятичное число. Максимальное десятичное значение октета равно 255(участвует каждый бит). Каждый октет преобразуется в число отдельно от других.

Бит, установленный в 0, всегда соответствует нулевому значению. Бит, установленный в 1, может быть преобразован в десятичное число. Младший бит октета представляет десятичное число 1, а старший - 128. Максимальное значение октета (255) достигается, когда каждый его бит равен 1.

Каждый класс IP-адресов определяет, какая часть адреса отводится под идентификатор сети, а какая - под идентификатор узла.

Протокол TCP/IP поддерживает адреса классов A, B и C. Класс адреса определяет, какие биты относятся к идентификатору сети, а какие - к идентификатору узла. Также он определяет максимально возможное количество узлов в сети.

Класс IP-адреса идентифицируют по значению его первого октета, 32-разрядные IP-адреса могут быть присвоены в общей совокупности 3720314628 узлам. Ниже показано, как определяются поля в IP-адресах разных классов.

Класс A:Адреса класса A назначаются узлам очень большой сети. Старший бит в адресах этого класса всегда равен нулю. Следующие семь бит первого октета представляют идентификатор сети. Оставшиеся 24 бита (три октета) содержат идентификатор узла. Это позволяет иметь 126 сетей с числом узлов до 17 миллионов в каждой.

Класс B: Адреса класса B назначаются узлам в больших и средних по размеру в сетях. В двух старших битах IP-адреса класса B записывается двоичное значение 10. Следующие 14 бит содержат идентификатор сети (два первых октета). Оставшиеся 16 бит (два октета)

представляют идентификатор узла. Таким образом возможно существование 16384 сетей класса B, в каждой из которых около 65000 узлов.

Класс C: Ареса класса C применяются в небольших сетях. Три старших бита IP-адреса этого класса содержат двоичное значение 110. Следующие 21 бит составляет идентификатор сети (первые три октета). Оставшиеся 8 бит (последний октет) отводится под идентификатор узла. Всего возможно около 2000000 сетей класса C, содержащих до 254 узлов.

Для заданных IP-адресов классов A, B и C и предложенных масок определить:

- класс адреса;
- максимально возможное количество подсетей;
- диапазон изменения адресов подсетей;
- максимальное число узлов в подсетях.

Адрес	Маска
135.209.23.246	11111111.11111111.11111111.11000000
200.131.197.27	11111111.11111111.11111111.11111000
214.147.120.38	11111111.11111111.11111111.11110000
176.72.82.62	11111111.11111111.11111111.10000000
82.67.174.114	11111111.11000000.00000000.00000000

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 8
Расчет IP-адреса и маски подсети

Цель работы: обобщение и систематизация знаний по теме Передача данных по сети, научиться рассчитывать IP-адрес и маску подсети.

Выполнив работу, Вы будете:
уметь:
- рассчитывать IP-адрес и маску подсети;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Маска подсети всегда представляет собой последовательное количество вначале единиц, а затем – нулей. Маски вида 11011111.11111111.11111111.1100000 быть не может.

Маска подсети	CIDR префикс	Всего IP адресов	Используемых IP адресов	Число /24 сетей
255.255.255.255	/32	1	1	1/256
255.255.255.254	/31	2	0	1/128
255.255.255.252	/30	4	2	1/64
255.255.255.248	/29	8	6	1/32
255.255.255.240	/28	16	14	1/16
255.255.255.224	/27	32	30	1/8
255.255.255.192	/26	64	62	1/4
255.255.255.128	/25	128	126	1/2
255.255.255.0	/24	256	254	1

Стоить учесть, что для любой подсети работает правило вычисление количества хостов:

232-n -2, где n – длина подсети. 232-24 -2 = 254 для маски 255.255.255.0.

Откуда берется -2?

Это первый и последний адреса сети: первый – адрес самой сети, последний – адрес широковещательных рассылок.

Еще для наглядности. Рассмотрим, как разделить сеть 192.168.1.0 /24 на две на подсети с помощью маски. Для этого заберем один бит хостовой части в пользу сетевой, получаем 11111111.11111111.11111111.10000000. На выходе у нас две подсети – 192.168.1.0 /25 и 192.168.1.128 /25. (0 и 128 – значения, которые может принять первый бит четвертого октета, 0 и 1 соответственно).

Теперь рассмотрим, как разделить первоначальную сеть на четыре подсети. Для этого отдаем первые два бита из последнего октета в пользу сети:

11111111.11111111.11111111.00000000 = 192.168.1.0
11111111.11111111.11111111.01000000 = 192.168.1.64
11111111.11111111.11111111.10000000 = 192.168.1.128
11111111.11111111.11111111.11000000 = 192.168.1.192

Деление больших сетей на маленькие используется администраторами для упрощения работы с сетевой инфраструктурой. Использование ограничений для различных департаментов компании

удобно реализовывать на группу ПК, нежели отдельно на каждую машину. Кроме того, наличие подсетей уменьшает домены широковещательных рассылок, снижая нагрузку на коммутаторы.

Если два устройства относятся к одной подсети, то общение между ними будет осуществляться напрямую, минуя маршрутизатор. Для того, что бы отправить пакет в другую подсеть, устройство направляет его на свой шлюз по умолчанию, которым является физический или виртуальный интерфейс устройства третьего уровня (L3). Там сверяется адрес получателя с таблицей маршрутизации, и пакет направляется дальше.

Когда на маршрутизатор попадает очередной пакет, он проверяет сеть получателя, чтобы найти совпадение в своей таблице маршрутизации. Если совпадение есть, то пакет перенаправляется в нужный интерфейс, если совпадение отсутствует, то используется маршрут по умолчанию. В случае, когда поддержка бесклассовой маршрутизации не настроена, а пакет не относится к какой-либо сети в таблице маршрутизации, то он будет отброшен.

Например, пакет из сети 192.168.10.0 попадает на роутер, в таблице маршрутизации имеется два маршрута: к сетям 192.168.1.0 и 192.168.2.0, а так же маршрут по умолчанию 0.0.0.0 0.0.0.0. В такой ситуации пакет будет отброшен, так как сеть 192.168.10.0 относится к классу С, а маршрут к такой сети в таблице не существует.

В случае, когда используется бесклассовая маршрутизация, пакет будет отправлен на шлюз по умолчанию – 0.0.0.0 0.0.0.0.

Стоит учесть, что при использовании бесклассовой адресации само понятие «класс» пропадает. Нельзя сказать, что адрес 192.168.1.1 /24 относится к классу С или адрес 10.1.1.1 /24 относится к классу А. Классы были нужны для определения границ сети до тех пор, пока не использовалась маска сети.

По заданным классу (A, B или C), количеству подсетей N и максимальному количеству компьютеров M1…MN в каждой подсети определить маску для разбиения на подсети. Сделать вывод о возможности такого разбиения. Если разбиение невозможно, то сформулируйте рекомендации по изменению каких-либо исходных данных для обеспечения возможности разбиения.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 9
Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы

Цель работы: обобщение и систематизация знаний по теме Передача данных по сети, изучить процесс управления таблицей коммутации и ARP-таблицей.

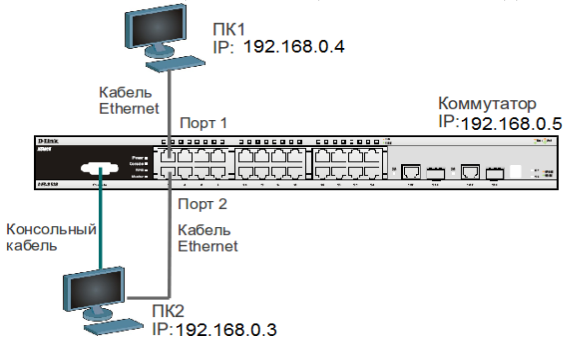
Выполнив работу, Вы будете:
уметь:
- управлять таблицей коммутации и ARP-таблицей;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»
Порядок выполнения работы:

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 о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 10
Управление сетью с помощью технологии SIM

Цель работы: обобщение и систематизация знаний по теме Сетевые архитектуры, научиться управлять сетью с помощью технологии SIM.

Выполнив работу, Вы будете:
уметь:
управлять сетью с помощью технологии SIM;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Технология Single IP Management (SIM) является простым и удобным способом сетевого управления. Она разработана для управления группой коммутаторов, называемых SIM-группой, как единым устройством. При этом для управления SIM-группой требуется только один IP-адрес, который назначается выделенному коммутатору группы (Commander switch).

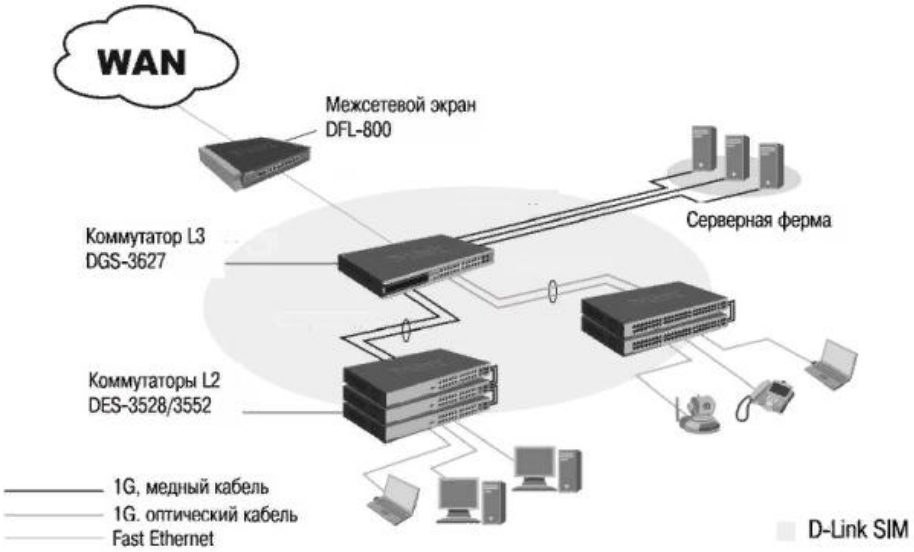
Технология SIM позволяет:

- устранить ограничения на модели коммутаторов, объединяемых в стек;
- уменьшить количество управляющих IP-адресов в сети;
- устранить необходимость использования специализированных модулей и кабелей, предназначенных для стекирования; преодолеть ограничения, связанные с длиной кабелей в стеке.

В отличие от стеков, построенных с использованием традиционных методов стекирования, виртуальный стек на основе технологии SIM не ограничивается 6-ю или 12-ю коммутаторами. В SIM-группу может входить до 32-х коммутаторов любых моделей, поддерживающих функции Single IP Management. Это означает, что виртуальный стек может включать коммутаторы разного типа, от недорогих коммутаторов 2-го уровня до высокопроизводительных коммутаторов на основе шасси (для ядра сети).

Объединение коммутаторов в SIM-группу не требует использования специальных соединительных кабелей. Трафик, передаваемый между устройствами стека, проходит через интерфейсы Fast Ethernet, Gigabit Ethernet или 10 Gigabit Ethernet по обычным медным или оптическим кабелям. Отказ от использования специализированных

стекирующих кабелей позволяет преодолеть ограничения, связанные с их длиной. Устройства SIM-группы могут быть подключены друг к другу через промежуточные устройства, не поддерживающие технологию SIM. Объединение коммутаторов в SIM-группу не влияет на их нормальное функционирование.



Внимание: SIM является дополнительной функцией коммутаторов и может быть активизирована или отключена через Web-интерфейс или *CLI*. По умолчанию эта функция на коммутаторе отключена.

Технология SIM предусматривает три роли, которые могут быть назначены коммутаторам группы:

1. **Commander Switch (CS)** — это коммутатор, который вручную настраивается администратором сети как *управляющее устройство* SIM-группы. В SIM-группе может быть только один Commander Switch. CS обладает следующими характеристиками:
    - ему присвоен IP-адрес;
    - он не является Commander Switch или Member Switch другой SIM-группы;
    - он подключен к коммутаторам Member Switch через управляющую VLAN (VLAN, к которой привязан *управляющий интерфейс* коммутатора System. По умолчанию управляющей VLAN является default VLAN);

2. **Member Switch (MS)** — коммутатор, который вступил в SIM-груп-пу и доступен через Commander Switch. Member Switch обладает следующими характеристиками:
    - он не является Commander Switch или Member Switch другой SIM-группы;
    - он подключен к Commander Switch через управляющую VLAN;
3. **Candidate Switch (CaS)** — это коммутатор, который готов вступить в SIM-группу (стать Member Switch), используя либо автоматический метод, либо ручную настройку. Коммутатор, настроенный как Candidate Switch, не является членом SIM-группы. Он обладает следующими характеристиками:
    - он не является Commander Switch или Member Switch другой SIM-группы;
    - он подключен к Commander Switch через управляющую VLAN.

Все коммутаторы, объединенные в одну SIM-группу, должны принадлежать одной IP-подсети (широковещательному домену). В пределах одной подсети может быть создано несколько SIM-групп, но при этом каждый коммутатор должен принадлежать только одной SIM-группе. Каждая группа может содержать до 32 коммутаторов (от 0 до 31), включая Commander Switch (его номер 0). Если в сети настроено несколько VLAN, SIM-группа будет использовать только управляющую VLAN любого коммутатора.

По умолчанию после активизации функции SIM всем коммутаторам присваивается роль "Candidate Switch". Это означает, что они смогут стать членами SIM-группы (Member Switch), как только получат запрос от Commander Switch.

После того, как одному из коммутаторов группы была присвоена роль "Commander Switch", он начинает формировать SIM-группу, добавляя в нее новых членов. Для этого Commander Switch просматривает список кандидатов (Candidate Switch) и отправляет им периодические запросы. Кандидат отправляет Commander Switch ответ, содержащий информацию о нем, что позволяет ему стать членом SIM-группы. Если коммутатор-кандидат имел ранее сконфигурированный пароль, он не сможет стать членом группы до тех пор, пока не будут введены его *аутентификационные данные*.

Можно добавлять членов группы, используя Web-интерфейс. Функционал SIM встроен в Web-интерфейс управления коммутаторов и не требует установки дополнительного ПО.

Изменение топологии стека

В случае добавления или удаления коммутатора(-ов) из стека или изменения топологии протокол стекирования, реализованный в устройствах, быстро обнаружит изменения и синхронизирует информацию о новой топологии стека.

Когда новый коммутатор добавляется в работающий стек, ему присваивается роль ведомого или резервного мастера, в зависимости от значений приоритета и MAC-адреса.

Если в стек добавляется только одно устройство, то процесс выбора основного мастера не запускается.

При удалении одного или нескольких коммутаторов из работающего стека оставшиеся коммутаторы удаляют информацию о выбывших устройствах из своих баз данных топологии стека.

При удалении резервного мастера запускается процесс выборов нового резервного мастера. Этот процесс также запускается при удалении или выходе из строя основного мастера, т.к. резервный мастер становится в этом случае основным. При этом для минимизации нарушения работы сети новому основному мастеру присваивается тот же IP-адрес, который был у предыдущего (Box ID не меняется).

При удалении обоих мастеров (основного и резервного) мгновенно инициируется процесс выбора нового основного и резервного мастеров из оставшихся коммутаторов стека.

Когда происходит изменение топологии стека — с линейной на кольцевую или наоборот, состояние устройств не изменяется.

Пример настройки стекирования

В качестве примера приведем настройку двух коммутаторов, объединенных в физический стек.

Настройка коммутатора 1

config stacking mode enable

config box_priority current_box_id 1 priority 1

Настройка коммутатора 2

config stacking mode enable

config box_priority current_box_id 1 new_box_id 2

config box_priority current_box_id 2 priority 2

Виртуальный стек. Технология Single IP Management (SIM)

Технология **Single IP Management (SIM)** является простым и удобным способом сетевого управления. Она разработана для управления группой коммутаторов, называемых *SIM-группой*, как единым устройством. При этом для управления SIM-группой требуется только один IP-адрес, который назначается выделенному коммутатору группы (Commander switch).

Технология SIM позволяет:

- устранить ограничения на модели коммутаторов, объединяемых в стек;
- уменьшить количество управляющих IP-адресов в сети;
- устранить необходимость использования специализированных модулей и кабелей, предназначенных для стекирования; преодолеть ограничения, связанные с длиной кабелей в стеке.

В отличие от стеков, построенных с использованием традиционных методов стекирования, виртуальный стек на основе технологии SIM не ограничивается 6-ю или 12-ю коммутаторами. В SIM-группу может входить до 32-х коммутаторов любых моделей, поддерживающих функции Single *IP Management*. Это означает, что виртуальный стек может включать коммутаторы разного типа, от недорогих коммутаторов 2-го уровня до высокопроизводительных коммутаторов на основе *шасси* (для ядра сети).

Объединение коммутаторов в SIM-группу не требует использования специальных соединительных кабелей. Трафик, передаваемый между устройствами стека, проходит через интерфейсы Fast Ethernet, Gigabit Ethernet или 10 Gigabit Ethernet по обычным медным или оптическим кабелям. Отказ от использования специализированных стекирующих кабелей позволяет преодолеть ограничения, связанные с их длиной. Устройства SIM-группы могут быть подключены друг к другу через промежуточные устройства, не поддерживающие технологию SIM. Объединение коммутаторов в SIM-группу не влияет на их нормальное функционирование.

Внимание: SIM является дополнительной функцией коммутаторов и может быть активизирована или отключена через Web-интерфейс или *CLI*. По умолчанию эта функция на коммутаторе отключена.

Технология SIM предусматривает три роли, которые могут быть назначены коммутаторам группы:

1. **Commander Switch (CS)** — это коммутатор, который вручную настраивается администратором сети как *управляющее устройство* SIM-группы. В SIM-группе может быть только один Commander Switch. CS обладает следующими характеристиками:
    - ему присвоен IP-адрес;
    - он не является Commander Switch или Member Switch другой SIM-группы;
    - он подключен к коммутаторам Member Switch через управляющую VLAN (VLAN, к которой привязан *управляющий интерфейс* коммутатора System. По умолчанию управляющей VLAN является default VLAN);

2. **Member Switch (MS)** — коммутатор, который вступил в SIM-груп-пу и доступен через Commander Switch. Member Switch обладает следующими характеристиками:
    - он не является Commander Switch или Member Switch другой SIM-группы;
    - он подключен к Commander Switch через управляющую VLAN;
3. **Candidate Switch (CaS)** — это коммутатор, который готов вступить в SIM-группу (стать Member Switch), используя либо автоматический метод, либо ручную настройку. Коммутатор, настроенный как Candidate Switch, не является членом SIM-группы. Он обладает следующими характеристиками:
    - он не является Commander Switch или Member Switch другой SIM-группы;
    - он подключен к Commander Switch через управляющую VLAN.

Все коммутаторы, объединенные в одну SIM-группу, должны принадлежать одной IP-подсети (широковещательному домену). В пределах одной подсети может быть создано несколько SIM-групп, но при этом каждый коммутатор должен принадлежать только одной SIM-группе. Каждая группа может содержать до 32 коммутаторов (от 0 до 31), включая Commander Switch (его номер 0). Если в сети настроено несколько VLAN, SIM-группа будет использовать только управляющую VLAN любого коммутатора.

По умолчанию после активизации функции SIM всем коммутаторам присваивается роль "Candidate Switch". Это означает, что они смогут стать членами SIM-группы (Member Switch), как только получат запрос от Commander Switch.

После того, как одному из коммутаторов группы была присвоена роль "Commander Switch", он начинает формировать SIM-группу, добавляя в нее новых членов. Для этого Commander Switch просматривает список кандидатов (Candidate Switch) и отправляет им периодические запросы. Кандидат отправляет Commander Switch ответ, содержащий информацию о нем, что позволяет ему стать членом SIM-группы. Если коммутатор-кандидат имел ранее сконфигурированный пароль, он не сможет стать членом группы до тех пор, пока не будут введены его *аутентификационные данные*.

Можно добавлять членов группы, используя Web-интерфейс. Функционал SIM встроен в Web-интерфейс управления коммутаторов и не требует установки дополнительного ПО.

После настройки Commander Switch в папке Single *IP Management* Web-интерфейса станет доступна опция *Topology*. Эта опция

позволяет настраивать коммутаторы и управлять ими внутри SIM-группы. При выборе пункта View окна *Topology* появится топологическая карта, показывающая, как подключены устройства внутри SIM-группы. Топологическая карта автоматически обновляется каждые 20 секунд.

Используя топологическую карту, администратор может получать детальную информацию о группе, просматривать краткую информацию о каждом коммутаторе SIM-группы, настраивать его, добавлять и удалять устройства из SIM-группы.

В топологической карте используются следующие иконки для обозначения Commander Switch, Member Switch и Candidate Switch.

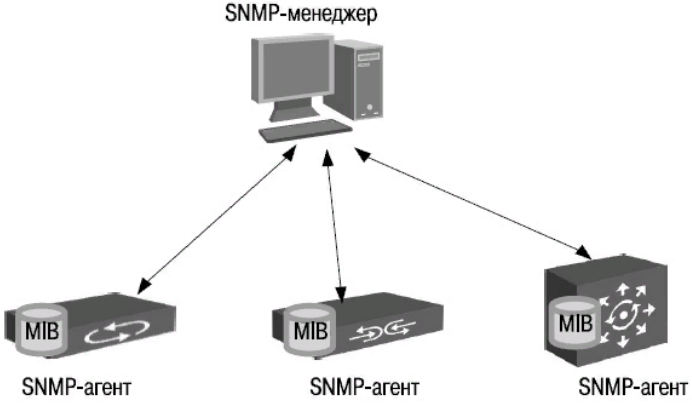
Протокол SNMP

Протокол *SNMP* (Simple *Network Management Protocol*) является протоколом 7 уровня модели *OSI*, который специально разработан для управления и мониторинга сетевых устройств. Протокол *SNMP* входит в *стек* протоколов *TCP/IP* и позволяет администраторам сетей получать информацию о состоянии устройств сети, обнаруживать и исправлять неисправности и планировать развитие сети.

В настоящее время существует три версии протокола *SNMP*: *SNMP* v1 (*RFC* 1157), *SNMP* v2c (*RFC* 1901-1908) и *SNMP* v3 (*RFC* 3411-3418). Эти версии отличаются предоставляемым уровнем безопасности при обмене данными между менеджером и агентом *SNMP*. Коммутаторы D-Link поддерживают все три версии протокола.

Компоненты SNMP

Сеть, управляемая по протоколу SNMP, основывается на архитектуре "клиент/сервер" и состоит из трех основных компонентов: менеджера SNMP, агента SNMP, базы управляющей информации.



Менеджер SNMP (SNMP Manager) — это программное обеспечение, установленное на рабочей станции управления, наблюдающее за сетевыми устройствами и управляющее ими.

Агент SNMP (SNMP Agent) — это программный модуль для управления сетью, который находится на управляемом сетевом устройстве (маршрутизаторе, коммутаторе, точке доступа, Интернет-шлюзе, принтере и т.д.). Агент обслуживает базу управляющей информации и отвечает на запросы менеджера SNMP.

База управляющей информации (Management Information Base, *MIB*) — это совокупность иерархически организованной информации, доступ к которой осуществляется посредством протокола управления сетью.

Менеджер взаимодействует с агентами при помощи протокола SNMP с целью обмена управляющей информацией. В основном это взаимодействие реализуется в виде периодического опроса менеджером множества агентов, которые предоставляют доступ к информации.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 11
Управление полосой пропускания

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

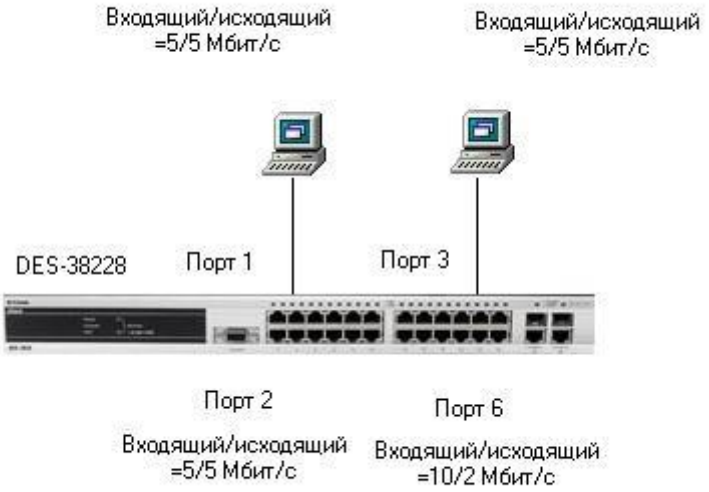
Выполнив работу, Вы будете:
уметь:
- настраивать ограничение полосы пропускания на коммутаторе.

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 о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 12
Настройка статического агрегирования каналов

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

Выполнив работу, Вы будете:

уметь:

-выполнять настройку статического агрегирования каналов на коммутаторах D-Link;

Материальное обеспечение:

учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

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.

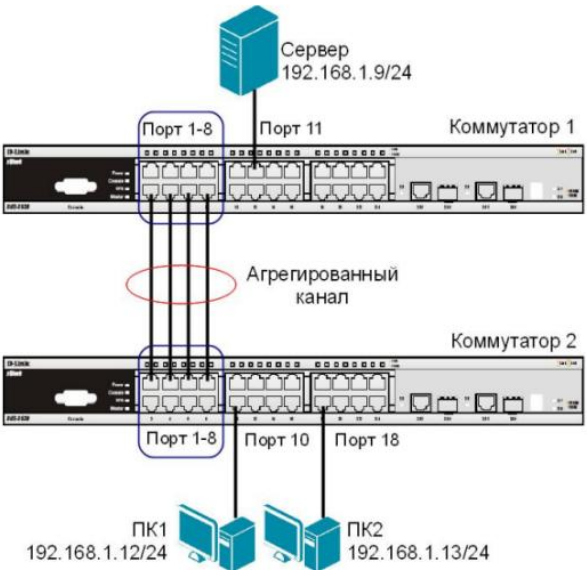
Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Выбор порта для конкретного сеанса выполняется на основе выбранного алгоритма агрегирования портов, т.е. на основании некоторых признаков поступающих пакетов.

В коммутаторах D-Link по умолчанию используется алгоритм mac_source (MACадрес 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.



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

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

Настройка коммутатора 1

Создайте группу агрегирования каналов: create link_aggregation group_id 1 type lacp

Включите порты 1-8 в группу агрегирования каналов и выберите порт 1 в качестве мастера порта: config link_aggregation group_id 1 master_port 1 ports 1-8 state enabled

Настройте порты на работу в пассивном режиме: config lacp_port 1-8 mode passive

Проверьте выполненные настройки: show link_aggregation

Проверьте режим работы LACP на портах коммутаторов: show lacp_port

Посмотрите текущий алгоритм агрегирования каналов: show link_aggregation algorithm

Настройка коммутатора 2

Создайте группу агрегирования каналов:

create link_aggregation group_id 1 type lacp

Включите порты 1-8 в группу агрегирования каналов и выберите порт 1 в качестве мастера порта: config link_aggregation group_id 1 master_port 1 ports 1-8 state enabled

Настройте порты на работу в активном режиме: config lacp_port 1-8 mode active

Проверьте выполненные настройки: show link_aggregation Проверьте режим работы LACP на портах коммутаторов: show lacp_port

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

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

Ключи, используемые при запуске программы iperf:

-s – устанавливает режим сервера;

-c -устанавливает режим клиента и задает адрес сервера;

-i -задает интервал вывода отчета о скорости;

-t -время длительности теста в секундах;

-r -режим двустороннего тестирования;

-u -режим тестирования по протоколу UDP, а не TCP;

-b10M -задает полосу генерации трафика в 10 Мбит/с;

-P5 -запускает одновременно 5 тестовых потоков.
Запустите программу iperf на ПК, выполняющего роль сервера (запускается из командной строки, где указывается путь к программе и ключи): iperf-s-u
Запустите программу iperf на ПК1 и ПК2: iperf -c 192.168.1.9 -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 о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Практическая работа № 13
Настройка динамического агрегирования каналов

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

Выполнив работу, Вы будете:
уметь:
-выполнять настройку динамического агрегирования каналов на коммутаторах D-Link;
Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:
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.

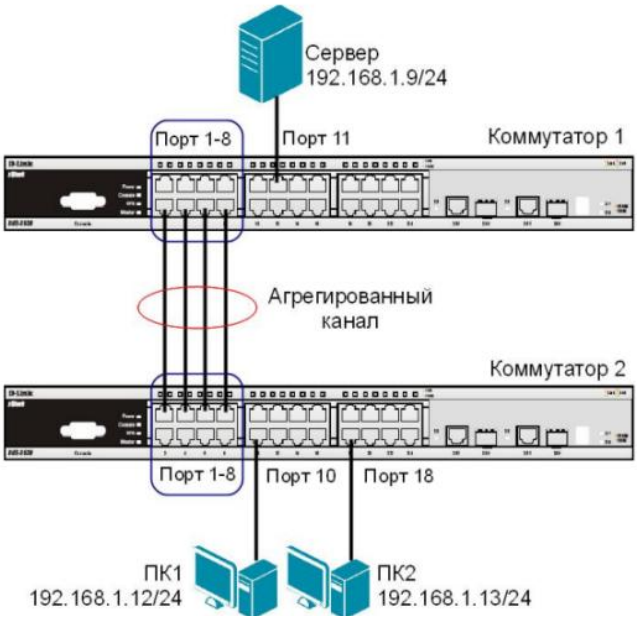
Важным моментом при реализации объединения портов в агрегированный канал является распределение трафика по ним. Выбор порта для конкретного сеанса выполняется на основе выбранного алгоритма агрегирования портов, т.е. на основании некоторых признаков поступающих пакетов.

В коммутаторах D-Link по умолчанию используется алгоритм mac_source (MACадрес 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.



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

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

Настройка коммутатора 1

Создайте группу агрегирования каналов: create link_aggregation group_id 1 type lacp

Включите порты 1-8 в группу агрегирования каналов и выберите порт 1 в качестве мастера порта: config link_aggregation group_id 1 master_port 1 ports 1-8 state enabled

Настройте порты на работу в пассивном режиме: config lacp_port 1-8 mode passive

Проверьте выполненные настройки: show link_aggregation

Проверьте режим работы LACP на портах коммутаторов: show lacp_port

Посмотрите текущий алгоритм агрегирования каналов: show link_aggregation algorithm

Настройка коммутатора 2

Создайте группу агрегирования каналов:

create link_aggregation group_id 1 type lacp

Включите порты 1-8 в группу агрегирования каналов и выберите порт 1 в качестве мастера порта: config link_aggregation group_id 1 master_port 1 ports 1-8 state enabled

Настройте порты на работу в активном режиме: config lacp_port 1-8 mode active

Проверьте выполненные настройки: show link_aggregation Проверьте режим работы LACP на портах коммутаторов: show lacp_port

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

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

Ключи, используемые при запуске программы iperf:

-s – устанавливает режим сервера;

-c -устанавливает режим клиента и задает адрес сервера;

-i -задает интервал вывода отчета о скорости;

-t -время длительности теста в секундах;

-r -режим двустороннего тестирования;

-u -режим тестирования по протоколу UDP, а не TCP;

-b10M -задает полосу генерации трафика в 10 Мбит/с;

-P5 -запускает одновременно 5 тестовых потоков.

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

Запустите программу iperf на ПК1 и ПК2: iperf -c 192.168.1.9 -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 о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 14
Настройка VLAN на основе портов

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

Выполнив работу, Вы будете:
уметь:
-выполнять настройку на коммутаторах D-Link;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

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

Настройка коммутатора 1

Удалите все порты коммутатора из VLAN по умолчанию для их использования в других VLAN: config vlan default delete 1-10

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

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

Измените имя нескольких VLAN и добавьте в них немаркированные порты:

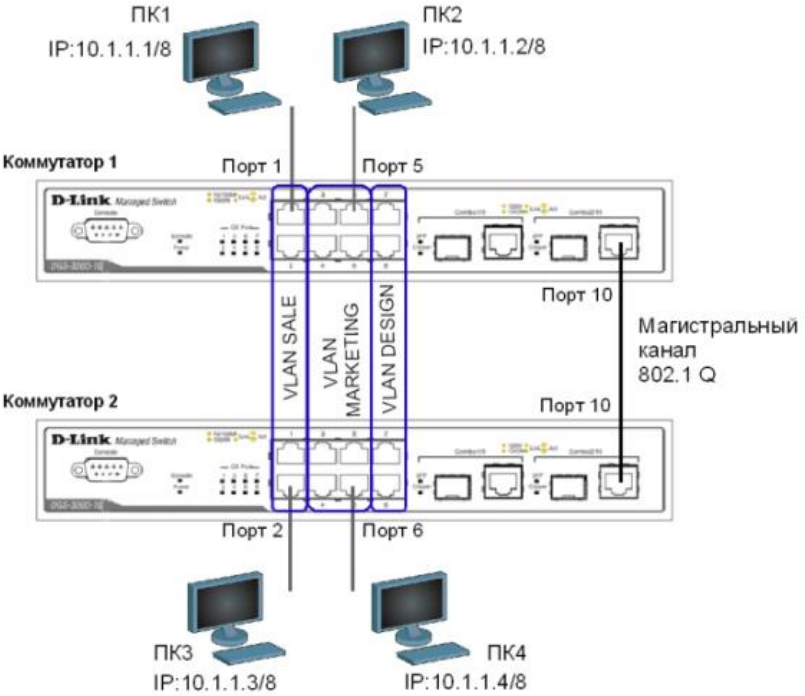
config vlan vlanid 7 name SALE add untagged 1-2
config vlan vlanid 8 name MARKETING add untagged 3-6
config vlan vlanid 9 name DESIGN add untagged 7-8

Добавьте маркированные порты в несколько VLAN:
config vlan vlanid 2-10 add tagged 9-10

Проверьте настройки VLAN: show vlan

Удалите порты из нескольких VLAN: config vlan vlanid 2-10 delete 9-10

Проверьте настройки VLAN: show vlan



Создайте магистральный порт VLAN для передачи маркированных кадров: config vlan_trunk ports 10 state enable

Активизируйте функционирование магистрального канала: enable vlan_trunk

Проверьте выполненные настройки: show vlan_trunk

Повторите процедуру настройки для коммутатора 2.

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

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

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

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

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

Отключите магистральные каналы на обоих коммутаторах: disable vlan_trunk

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Практическая работа № 15
Настройка VLAN на основе стандарта IEEE 802.1Q

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

Выполнив работу, Вы будете:
уметь:
-выполнять настройку на коммутаторах D-Link;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

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

проблема ограничений при передаче широковещательных кадров и вызываемых ими последствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Основные определения IEEE 802.1Q:

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

• Tagging (Маркировка кадра) – процесс добавления информации (тега) о принадлежности к 802.1Q VLAN в заголовок кадра;

• Untagging (Удаление тега из кадра) – процесс извлечения информации 802.1Q VLAN из заголовка кадра;

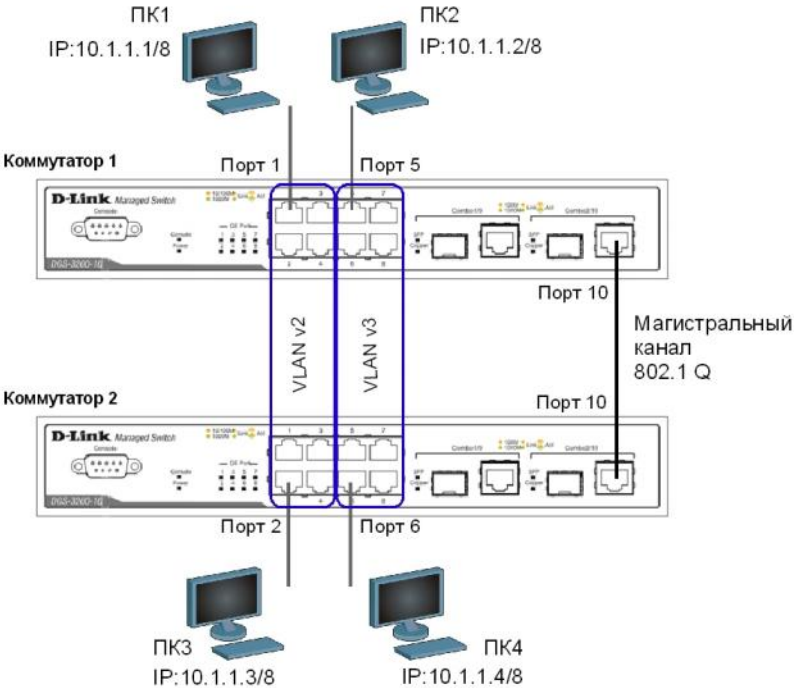
• Ingress port (Входной порт) – порт коммутатора, на который поступают кадры, и принимается решение о принадлежности VLAN;

• Egress port (Выходной порт) – порт коммутатора, с которого кадры передаются на другие сетевые устройства (коммутаторы, рабочие станции) и на нем, соответственно, принимается решение о маркировке кадра.

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

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

Настройка VLAN на основе стандарта IEEE 802.1Q



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

Настройка коммутатора 1

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

config vlan default delete 1-10

config vlan default add tagged 10

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

create vlan v2 tag 2

config vlan v2 add untagged 1-4

config vlan v2 add tagged 10

create vlan v3 tag 3

config vlan v3 add untagged 5-8

config vlan v3 add tagged 10

Проверьте настройки VLAN:

show vlan

Повторите процедуру настройки для коммутатора 2.

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

- от ПК1 к ПК 3 _____
- от ПК2 к ПК4 _____
- от ПК1 к ПК2 и ПК4 _____
- от ПК2 к ПК1 и ПК3_____

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 16
Команды протокола GVRP

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

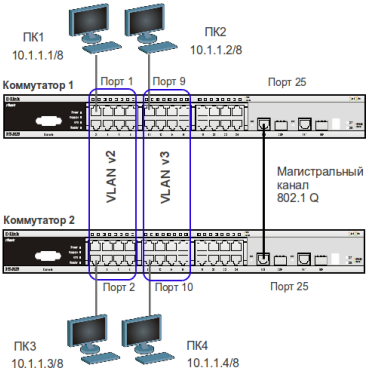
Выполнив работу, Вы будете:
уметь:
-выполнять настройку на коммутаторах D-Link;

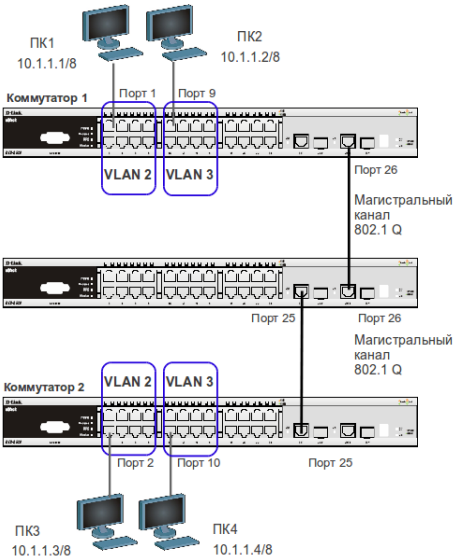
Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

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 о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 17
Настройка протоколов связующего дерева STP, RSTP

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

Выполнив работу, Вы будете:
уметь:
-выполнять настройку коммутаторов D-Link с использованием протоколов связующего дерева;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Протокол Spanning Tree Protocol (STP).

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

Для построения устойчивой активной топологии с помощью протокола STP необходимо с каждым коммутатором сети ассоциировать уникальный идентификатор моста (Bridge ID), с каждым портом

коммутатора ассоциировать стоимость пути (Path Cost) и идентификатор порта (Port ID).

Процесс вычисления связующего дерева начинается с выбора корневого моста (Root Bridge), от которого будет строиться дерево. Второй этап работы STP – выбор корневых портов (Root Port). Третий шаг работы STP – определение назначенных портов (Designated Port).

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

Протокол Rapid Spanning Tree Protocol (RSTP).

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

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

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

Протокол Multiple Spanning Tree Protocol (MSTP).

Протокол Multiple Spanning Tree Protocol (MSTP) является расширением протокола RSTP, который позволяет настраивать отдельное связующее дерево для любой VLAN или группы VLAN, создавая

множество маршрутов передачи трафика и позволяя осуществлять балансировку нагрузки.

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

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

Внутри коммутируемой сети может быть создано множество MST-регионов.

Протокол MSTP определяет следующие типы связующих деревьев:

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

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

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

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

Вычисления в MSTP

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

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

При наличии в регионе отдельных связующих деревьев MSTI для каждой MSTI, независимо от остальных, выбирается региональный корневой мост MSTI (MSTI Regional Root). Им становится коммутатор,

обладающий наименьшим значением идентификатора моста среди всех коммутаторов данной MSTI этого MST-региона.

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

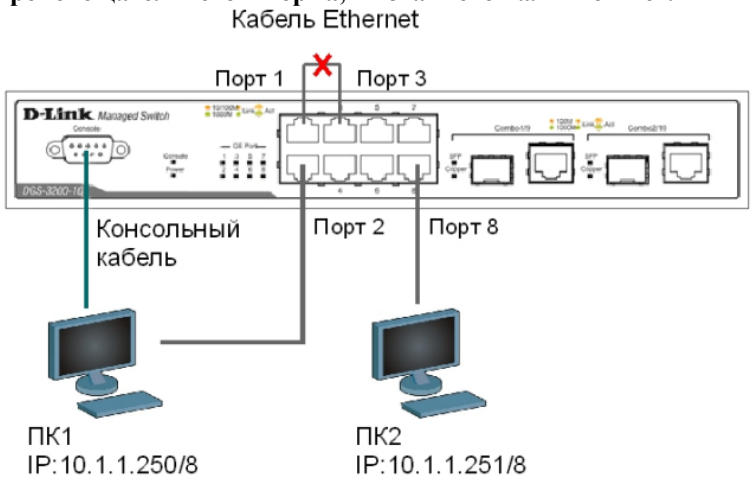
Роли портов

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

Счетчик переходов MSTP

При вычислении активной топологии связующего дерева IST и MSTI используется механизм счетчика переходов (Hop count), определяющий максимальное число переходов между устройствами внутри региона, прежде чем кадр BPDU будет отброшен. Значение счетчика переходов устанавливается региональным корневым мостом MSTI или CIST и уменьшается на 1 каждым портом коммутатора, получившим кадр BPDU. После того как значение счетчика станет равным 0, кадр BPDU будет отброшен и информация, хранимая портом, будет помечена как устаревшая. Пользователь может установить значение счетчика переходов от 1 до 20. Значение по умолчанию — 20.

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



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

Соедините кабелем Ethernet порты 1 и 3 коммутатора.

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

Что вы наблюдаете? Возник широковещательный шторм? Почему?

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

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

Что вы наблюдаете? Объясните почему.

Посмотрите загрузку ЦПУ (CPU): show utilization cpu

Просмотрите загрузку порта: show utilization ports

Отсоедините кабель от портов 1 и 3, удалите петлю.

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

config vlan default delete 2,4,6,8

create vlan v2 tag 2

config vlan v2 add untagged 2,4,6,8

Проверьте настройки VLAN: show vlan

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

Соедините кабелем порты 1 и 3. Что вы наблюдаете? Почему нет широковещательного шторма?

Выполните на рабочей станции ПК 1 команду: ping 10.1.1.251

Что вы наблюдаете? Объясните почему.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 18

Функция предотвращения петлеобразования (LoopBackDetection)

Цель работы: Понять способы работы LBD-алгоритма в различных режимах функционирования.

Выполнив работу, Вы будете:

уметь:

- обеспечивать дополнительную защиту от образования петель;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

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

- STP LoopBack Detection;
- LoopBack Detection Independent STP.

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

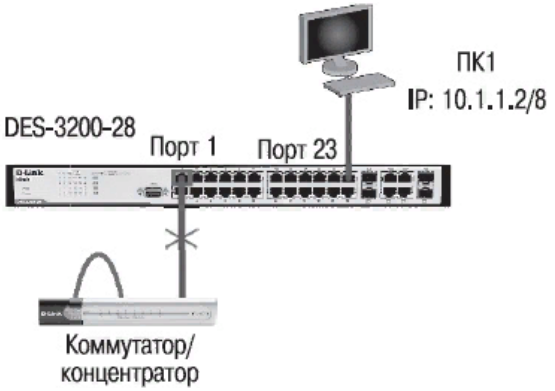
Функция LoopBack Detection Independent STP не требует настройки протокола STP на портах, на которых необходимо определять наличие петли. В этом случае наличие петли обнаруживается путем отправки портом специального служебного кадра ECTP (EthernetConfiguration Testing Protocol). При получении кадра ECTP этим же портом он блокируется на указанное в таймере время. Начиная с LBD версии 4.03, функция LoopBack Detection Independent STP также может определять петли, возникающие между портами одного коммутатора. Существуют два режима работы этой функции: Port-Based и VLAN-Based (начиная с LBD версии v.4.00).

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

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

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

Настройка LoopBack Detection Independent STP в режиме Port-Based



Настройка DES-3200-28

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

Включите функцию LBD глобально на коммутаторе

enable loopdetect

Активизируйте функцию LBD на всех портах коммутатора

config loopdetect ports 1-28 state enabled

Сконфигурируйте режим Port-Based, чтобы при обнаружении петли отключался порт

config loopdetect mode port-based

Внимание! При блокировании порта трафик не будет передаваться ни из одной VLAN.

Упражнения

Подключите неуправляемый коммутатор с петлей к DES-3200-28, как показано на схеме 1 .Проверьте текущую конфигурацию функции LBD

show loopdetect

Что вы наблюдаете, запишите:

Посмотрите, обнаружена ли петля на коммутаторе

show loopdetect ports all

Что вы наблюдаете, запишите:

Проверьте, выполнил ли коммутатор блокировку порта

show ports

Отключите неуправляемый коммутатор с петлей от коммутатора DES-3200-28.

Настройка функции LoopBack Detection Independent STP в режиме VLAN-Based (для версии LBD 4.0)

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

Настройка DES-3200-28_A и DES- 3200-28_B

Сбросьте настройки коммутатора к заводским настройкам по умолчанию

reset config

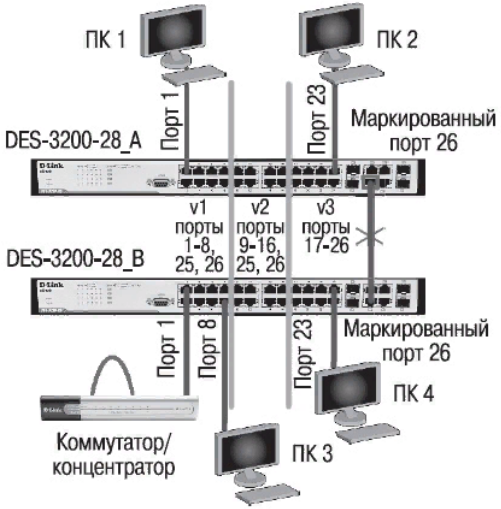
Удалите порты из VLAN по умолчанию для использования в других VLAN

config vlan default delete 8-26

Создайте VLAN v2 и v3

create vlan v2 tag 2

create vlan v3 tag 3



Добавьте в созданные VLAN немаркированные порты. Добавьте порты 25-26 как маркированные в созданные VLAN и VLAN по умолчанию

config vlan default add tagged 25-26

config vlan v2 add untagged 9-16

config vlan v2 add tagged 25-26

config vlan v3 add untagged 17-24

config vlan v3 add tagged 25-26

Настройка DES-3200-28_A

Включите функцию LBD глобально на коммутаторе

enable loopdetect

Активизируйте функцию LBD на всех портах коммутатора

config loopdetect ports 1-28 state enabled
Сконфигурируйте режим VLAN-Based LBD
config loopdetect mode vlan-based

Внимание! При обнаружении петли порт не будет передавать трафик только той VLAN, в которой обнаружена петля.

Упражнения

Подключите неуправляемый коммутатор с петлей к DES-3200-28_B, как показано на схеме 2 .

Что вы наблюдаете, запишите:
Проверьте текущую конфигурацию функции LBD
show loopdetect
Что вы наблюдаете, запишите:
Посмотрите, обнаружена ли петля на коммутаторе
show loopdetect ports all
Что вы наблюдаете, запишите:
Проверьте, выполнил ли коммутатор блокировку порта
show ports
Проверьте состояние подключения и причину блокировки портов
show ports err_disabled

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 19

Ограничение административного доступа к управлению коммутатором.

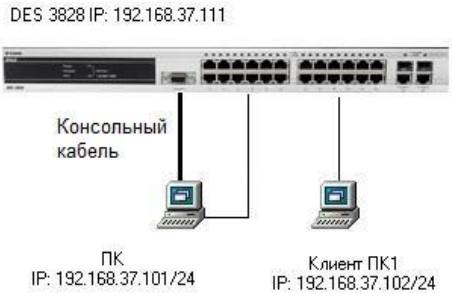
Цель работы: Изучить механизмы ограничения административного доступа к управлению коммутатором.

Выполнив работу, Вы будете:

Уметь: использовать механизмы ограничения административного доступа к управлению коммутатором.

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

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

1. Создайте учетную запись пользователя *swadmin* **create account admin swadmin**
2. Посмотрите созданную учетную запись **show account**
3. Посмотрите информацию и способ хранения паролей в конфигурационном файле
   show config current_config
4. Включите хранение пароей в зашифрованном виде **enable password encryption**
5. Посмотрите тнформацию и способ хранения паролей в конфигурационном файле
   show config current_config
6. Отключите режим шифрования паролей
   disable password encryption
7. Дешифруйте пароль учетной записи swadmin в конфигурационном файле
   config account swadmin encrypt plain_text dlink
8. Посмотрите выполнение дешифрования
   show config current_config
9. Запишите, что вы наблюдаете
   _____

3. Настройка Web-консоли (по протоколу SSL)

1. Включите режим SSL (при этом автоматически будет отключен режим Web) **enable ssl**
2. Попробуйте зайти на сайт через консоль SSL
   https://192.168.37.111
3. Какой вы сделаете вывод?
   Запишите_____

4. Настройка Secure Console (SSH)

1. Включите функцию SSH **enable ssh**
2. Проверьте включение встроенного сервера SSH **show ssh server**
3. Измените период времени смены ключей SSH (по умолчанию

ключи никогда не изменяются)

config ssh server rekey 10min

4. Сконфигурируйте настройки пользователя SSH (учетная запись пользователя уже должна быть создана)

config ssh user dlink authmode password

5. 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 о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 20
Зеркалирование портов (PortMirroring)

Цель работы: изучить настройку функции зеркалирования портов.

Выполнив работу, Вы будете:
уметь:
-применять зеркалирование портов для мониторинга и поиска неисправностей в сети;

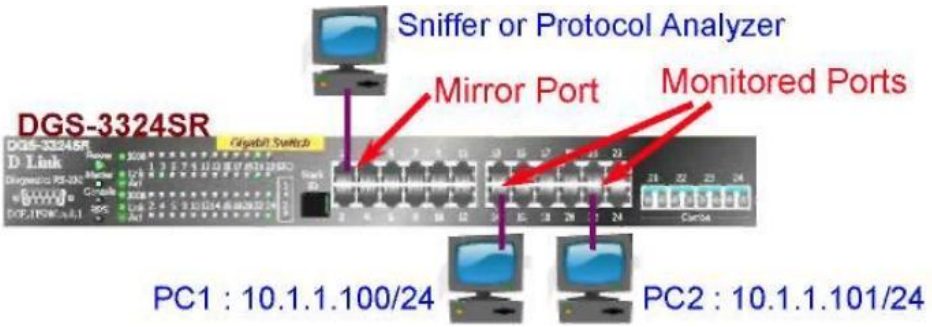
Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

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

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

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



Настроим список портов отображения config mirror port 1 add source ports 13-24 both

Включаем отображение (зеркалирование) enable mirror

Выполните ping тест от PC1 к PC2 и наоборот. Запустите Ethereal и захватите и проанализируйте трафик. Вы видите пакеты от и к рабочим станциям?

Отключите отображение портов *disable mirror*

Выполните ping тест от PC1 к PC2 и наоборот. Запустите Ethereal опять. Что вы наблюдаете теперь? Зафиксируйте выводы в отчете.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 21
Команды мониторинга

Цель работы: Изучить принципы работы простейших средств мониторинга сети, получить навыки решения задач, связанных с мониторингом сети.

Выполнив работу, Вы будете:
уметь:
-выполнять мониторинг сетевых соединений;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Протокол ICMP

Протокол ICMP (Интернет-протокол контрольных сообщений) стека протоколов TCP/IP предназначен для передачи между сетевыми устройствами сообщений об ошибках и контрольных сообщений при помощи IP-пакетов.

В протоколе ICMP определены несколько типов сообщений, в том числе:

- Destination Unreachable
- Time to Live Exceeded
- Parameter Problem
- Source Quench
- Redirect
- Echo
- Echo Reply
- Timestamp
- Timestamp Reply
- Information Request
- Information Reply
- Address Request
- Address Reply

Например, если маршрутизатор получает пакет, который он не может доставить по указанному в нем адресу, отправителю передается ICMP-сообщение о недостижимости адреса (Destination Unreachable).

PING: Проверка соединения с определенным интерфейсом.

Программа ping использует протокол ICMP.

Эта команда посылает пакет эхо-запроса на другой IP-адрес и ожидает ответа. Она чаще всего используется для того, чтобы посмотреть, «жив ли» другой компьютер. Ответ на запрос содержит также данные о том, как долго пакет путешествовал до адресата. Можно использовать команду ping с различными опциями: число посланных пакетов (от 1 до 10), время жизни пакета (time to live –TTL, от 1 до 255ms), размер пакета (от 16 до 8192 байт), время ожидания (timeout, до 9999 ms) и разрешать или нет фрагментацию каждого пакета.

Формат команды в ОС Windows:

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list

Options:

-t Выполнение команды до прерывания (Ctrl+C)
-a Разрешать адреса в имена
-n count Число отправляемых пакетов.
-l size Размер буфера отправки
-f Установить флаг "Не фрагментировать".
-i TTL Установить время жизни.
-w timeout Время ожидания ответа в мс.
-v TOS Задание типа службы (поле "Type Of Service").

-r count Запись маршрута для указанного числа переходов.

-s count Штамп времени для указанного числа переходов.

-j host-list Свободный выбор маршрута по списку узлов.

-k host-list Жесткий выбор маршрута по списку узлов.

destination-list Список рассылки.

3. Программа tracert. Определение промежуточных сетевых интерфейсов между хостами. Трассировка маршрута

Программа трассировки маршрута использует протокол ICMP.

Эта утилита очень похожа на Ping, за исключением того, что она показывает все другие IP-адреса (интерфейсы), которые пакет проходит до своего места назначения. Дополнительно можно изменять различные опции, ассоциированные с Trace Route: максимальное число дозволяемых промежуточных узлов (maximum hops, от 1 до 255) и timeout (до 9999 ms).

Формат команды в ОС Windows:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:

-d Не разрешать адреса в имена.

-h maximum_hops Наибольшее число промежуточных узлов.

-j host-list Трассировка через определенный список хостов

-w timeout Время ожидания каждого ответа в мс.

4. Программа netstat. Сетевая статистика.

Программа netstat используется для просмотра активных соединений каждого протокола, таблиц маршрутизации, а так же детализирует статистику передачи данных.

Формат команды в ОС Windows:

netstat [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]

-a Отображение всех подключений и ожидающих портов.

(Подключения со стороны сервера обычно не отображаются).

-e Отображение статистики Ethernet. Этот ключ может применяться вместе с ключом -s.

-n Отображение адресов и номеров портов в числовом формате.

-p имя Отображение подключений для протокола "имя": tcp или udp. Используется вместе с ключом -s для отображения статистики по протоколам. Допустимые значения "имя": tcp, udp или ip.

-r Отображение содержимого таблицы маршрутов.

-s Отображение статистики по протоколам. По умолчанию выводятся данные для TCP, UDP и IP. Ключ -p позволяет указать подмножество выводящихся данных.

Повторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши

CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.

1 Выполните команду ping в командной строке с различными значениями параметров -t, -n, -l, -i,-w. Какие наблюдения и выводы вы сделали?

ping www.seun.ru
ping www.sgu.ru
ping www.microsoft.com
ping www.sun.com
ping212.193.38.83

2 Выполните ping к тем же хостам с параметром –f, увеличивая параметр -l size. При каком значении размера перестают получаться ответы?

3 Выполните команду tracert в командной строке с различными значениями параметров. Какие наблюдения и выводы вы сделали?

Используйте, например,
tracertwww.seun.ru
tracert www.sgu.ru
tracert www.microsoft.com
tracert www.sun.com
tracert 212.193.38.83

4 Определите, кому принадлежат сети 194.85.33.0, 217.23.64.0, 212.193.38.0. Для этого используйте поисковые аппараты http://www.ripe.net/db/whois/whois.html и http://www.ripn.net:8080/nic/whois/index.html.

Пользуясь данными этих информационных систем, попробуйте определите географическое расположение сетей. Попробуйте изобразить топологическую схему соединения этих сетей.

5 Приведите сравнительные результаты выполнения команд ping по адресам 194.85.33.29, 194.85.33.30, 217.23.64.2, 212.193.38.248, 212.193.35.10 по параметрам «время отклика», TTL в форме таблицы. Объясните полученные различия.

6 Соберите средние времена прохождения 10 пакетов на указанные адреса. Сравните с р4езультатами, полученными при использовании сервиса ping в интерфейсе Looking Glass на сайте http://noc.runnet.ru. Объясните полученные различия.

7 Соберите усредненные времена прохождения 10 пакетов увеличивающегося размера по указанным адресам. Начните с 64 байт и каждый раз удваивайте размер пакета. При каком размере пакета потери превышают 50 %. Как влияет время ожидания отклика на процент прохождения пакетов этого размера. При каком времени ожидания отклика потери для пакетов зафиксированного размера не возникают?

Представьте результаты измерений в форме таблиц, наилучшим образом проявляющим, по вашему мнению, обнаруженные зависимости.

8 Используя программу ping, оцените вклад разных сетевых участков, по которым проходит эхо-пакет между вашей рабочей станцией и интерфейсом 194.85.33.29.

9 Приведите сравнительные результаты выполнения команд tracert по адресам 194.85.33.29, 194.85.33.30, 217.23.64.2, 212.193.38.248, 212.193.35.10. Объясните полученные различия.

10 Выполните трассировку к адресу 212.193.38.248 и к адресу 217.23.64.2 со стороны сайта http://noc.runnet.ru. Приведите полученные результаты.

11 Используя данные, полученные в результате выполнения трассировки и отправки эхо-пакетов между интерфейсами 212.193.38.248 и 194.85.35.100, оцените вклад разных участков сетей, соединяющих эти интерфейсы, в среднее время прохождения пакетов между ними.

12 Используя полученную в ходе выполнения всех заданий информацию, уточните схему задания 1, изобразите на ней обнаруженные вами промежуточные интерфейсы и линки сети, объединяющей подсети 194.85.33.0, 217.23.64.0, 212.193.38.0.

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети
Практическая работа № 22
Настройка маршрутизации

Цель работы: Изучить принципы маршрутизации в IP-сетях, получить практические навыки настройки программных маршрутизаторов на базе операционной системы (ОС) Linux с применением маршрутизации интерфейсов и маршрутизации виртуальных локальных сетей (VLAN).

Выполнив работу, Вы будете:

уметь:

-выполнять настройку программных маршрутизаторов;

Материальное обеспечение:
учебно-лабораторный комплекс «Локальные компьютерные сети»

Порядок выполнения работы:

Маршрутизация включает в себя следующие частные задачи:

1. Обмен информацией о топологии сети. Реализуется протоколами маршрутизации.
2. Определение оптимальных маршрутов и построение таблиц маршрутизации.
3. Продвижение пакета маршрутизаторами на основании таблиц маршрутизации.

Информация об оптимальных маршрутах представляется в маршрутизаторе в виде таблицы маршрутизации. В случае адресации без масок таблица маршрутизации имеет вид:

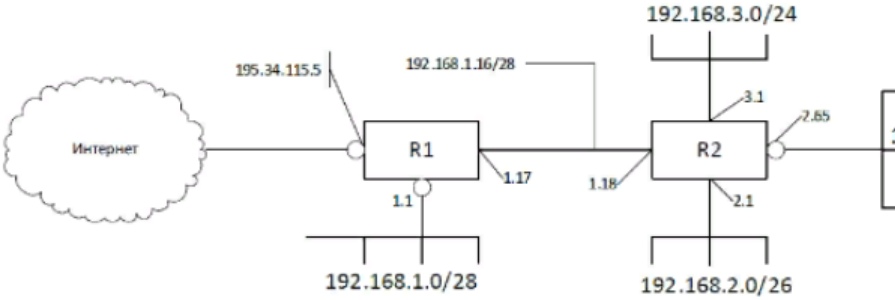
Адрес назначения	Маска	Адрес след. маршр.	Интерфейс	Метрика

В таблице:

- Адрес назначения – это IP-адрес сети или конкретного узла.
- IP следующего маршрутизатора – адрес следующего транзитного маршрутизатора на пути к адресу назначения.
- Интерфейс – это идентификатор сетевого интерфейса маршрутизатора, через который нужно передавать данные следующему маршрутизатору.
- Метрика – абстрактная характеристика качества маршрута. В качестве метрики может выступать количество транзитных узлов («хопов»), пропускная способность и т.п. Меньшее значение метрики всегда соответствует лучшему маршруту.

При поиске маршрута для продвижения IP-пакета предпочтение отдается специфическим маршрутам (то есть маршрутам до конкретного узла, а не сети), даже в том случае, если метрика этого маршрута хуже.

При использовании масок алгоритм работы маршрутизатора при продвижении пакета несколько усложняется. В таблицу маршрутизации добавляется колонка с маской, соответствующей адресу назначения. Рассмотрим пример:



Для данного примера в таблице маршрутизации R2 могут быть следующие записи:

Пример таблицы маршрутизации с масками

Адрес назначения	Маска	Адрес след. маршр.	Интерфейс	Метрика
192.168.1.16	255.255.255.240	-	192.168.1.18	0
192.168.3.0	255.255.255.0	-	192.168.3.1	0
192.168.2.0	255.255.255.192	-	192.168.2.1	0
192.168.2.64	255.255.255.192	-	192.168.2.65	0
192.168.1.0	255.255.255.240	192.168.1.17	192.168.1.18	1
Default	0.0.0.0	192.168.1.17	192.168.1.18	16

Продвижение пакета основывается на следующем алгоритме:

1. Маршрутизатор извлекает из пакета IP-адрес назначения.
2. Поиск специфического маршрута, то есть записи, в которой адрес назначения равен целевому IP-адресу. Если запись найдена, то используется этот маршрут, иначе на шаг 3.
3. Поиск неспецифического маршрута. Включает следующие шаги:

- для каждой записи таблицы маршрутизации выполняется операция IPd & M, где IPd – целевой адрес из пакета, M - маска из записи таблицы маршрутизации;
- если результат равен адресу назначения IP, запись отмечается подходящей.

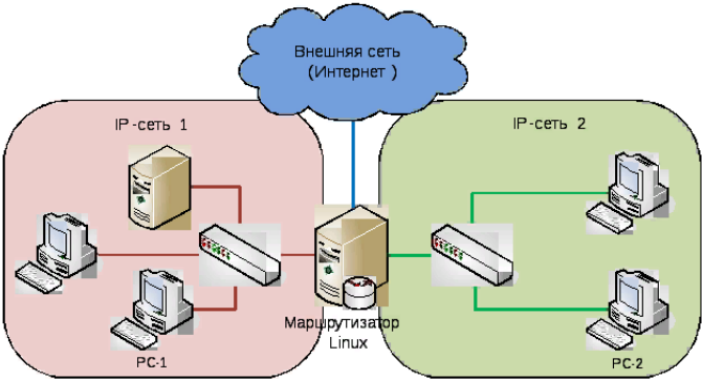
Из всех подходящих маршрутов выбирается наиболее специфический. Такой маршрут содержится в записи с наиболее длинной маской.

Среди подходящих маршрутов, обладающих одинаковой "специфичностью", выбирается маршрут с меньшей метрикой.

Задание

Настроить взаимодействие двух IP-сетей между собой и с внешней сетью средствами программного маршрутизатора на базе ОС Linux.

Настроить простейшие правила фильтрации трафика средствами ОС Linux.



Ситуация 1. Сети изолированы друг от друга физически, т.е. построены на различных коммутаторах, не связанных друг с другом непосредственно.

Ситуация 2. Изоляция сетей обеспечивается за счет применения технологии виртуальных локальных сетей.

Проверить настройку маршрутизации и фильтров на примере взаимодействия рабочих станций PC-1 и PC-2, принадлежащих различным сетям.

Перед выполнением лабораторной работы необходимо:

1. Подготовить схемы сети с указанием ip-адресов в соответствии с вариантом.
2. Подготовить виртуальные машины PC-1, PC-2, на которых может быть установлена любая сетевая операционная система, например Microsoft Windows XP или Linux.
3. Подготовить виртуальную машину, которая будет выполнять роль маршрутизатора. Рекомендуется использовать дистрибутив Debian GNU/Linux. Для данной виртуальной машины использовать сетевые адаптеры ***«PCnet»***, обеспечивающие передачу тэгированных кадров VLAN.

В установленной ОС Linux должна быть включена поддержка VLAN. В Debian необходимо установить соответствующий пакет командой

apt-get install vlan

Рекомендуется также установить графическую версию текстового редактора vi. В Debian соответствующий пакет устанавливается командой

apt-get install vi-gnome

Только для Debian! В случае, если образ ОС Debian Linux копируется/клонируется, необходимо отключить контроль MAC-адресов интерфейсов в файле «/etc/udev/rules.d/75-persistent-net-generator.rules» (изменять файл можно только с правами администратора). Для этого внести в приведенный ниже раздел строку с маской сетевых адаптеров VirtualBox и перезагрузить операционную систему.

```
# ignore interfaces with locally administered or null MAC addresses
# and VMWare virtual interfaces
ENV{MATCHADDR}=="?[2367abef]:*", ENV{MATCHADDR}=""
ENV{MATCHADDR}=="00:00:00:00:00:00",
ENV{MATCHADDR}=""
ENV{MATCHADDR}=="00:0c:29:*|00:50:56:*",
ENV{MATCHADDR}=""
```

ENV{MATCHADDR}=="08:00:27:*", ENV{MATCHADDR}=""

4. Подготовить коммутаторы 3COM Switch 1100 (SW-1, SW-2) для моделирования ситуаций 1, 2 задания (при подключении к коммутаторам использовать имя «manager», пароль – «superuser»). Для этого настроить:

- порты 1-2 коммутаторов SW-1, SW-2 для работы в VLAN-2 без тегирования;
- порты 3, 4 коммутатора SW-1 для работы в VLAN-3 без тегирования;
- порты 3, 4 коммутатора SW-2 для работы в VLAN-4 без тегирования;
- порты 5, 6 коммутаторов SW-1, SW-2 для работы в VLAN-2/3/4 с тегированием.

Выполнение лабораторной работы включает следующие этапы:

– Подключение и запуск рабочих станций pc-1, pc-2

Цель данного этапа состоит в подготовке моделей IP-сетей, взаимодействие между которыми будет настраиваться в лабораторной работе.

1. Подключить образ виртуальной машины в системе VirtualBox на одном из компьютеров лаборатории. В настройках виртуальной машины в разделе «Сеть» включить 1 сетевой адаптер, для которого указать тип подключения «Сетевой мост» и сетевой адаптер «Realtek 8029» или «3COM» (в зависимости от компьютера).
2. Запустить виртуальную машину.
3. Настроить IP-адрес сетевого интерфейса виртуальной машины в соответствии с вариантом.

4. Подключить компьютер через соответствующий разъем патч-панели «B-0x» на порт коммутатора 1 или 2 (для 1-й ситуации из задания).
5. Повторить шаги 1-5 для 2-й виртуальной машины (на другом компьютере).

– Подключение и настройка маршрутизации. Ситуация 1

Цель данного этапа состоит в настройке маршрутизации средствами ОС Linux для ситуации, когда на маршрутизаторе установлено 3 сетевых интерфейса. Фильтры на данном этапе не настраиваются. Выход во внешнюю сеть обеспечивается через VirtualBox Host-Only Network (адрес сети 192.168.13x.0/24) и маршрутизируется хост-компьютером.

1. Подключить хост-компьютеры в сеть в соответствии с физической схемой для ситуации 1. Использовать порты 1, 2 коммутаторов.
2. Подключить образ виртуальной машины под управлением ОС Linux в системе VirtualBox на одном из компьютеров лаборатории. В настройках виртуальной машины в разделе «Сеть» включить 3 сетевых адаптера и настроить следующим образом:

- адаптер 1: тип подключения «Сетевой мост» и сетевой адаптер «Realtek 8029» или «3COM» (в зависимости от компьютера);
- адаптер 2: тип подключения «Сетевой мост» и сетевой адаптер «D-Link DGE-528»;
- адаптер 3: тип подключения «Виртуальный адаптер хоста» и сетевой адаптер «VirtualBox Host-Only Ethernet Adapter».

3. Запустить ОС Linux на виртуальной машине, запустить консоль с правами администратора.
4. Выключить сетевые интерфейсы командой
   ifdown --all
5. Настроить статические адреса сетевых интерфейсов маршрутизатора. Для этого в файле /etc/network/interfaces для каждого сетевого интерфейса (eth0, eth1, eth2) задать ip-адрес, маску подсети и шлюз:
   auto eth0
   iface eth0 inet static
   address x.x.x.x
   netmask x.x.x.x
   gateway x.x.x.x
6. Включить сетевые интерфейсы с заданными настройками:
   ifup --all

7. Проверить с помощью команды ifconfig, что требуемые настройки сетевых интерфейсов установлены.
8. Включить перенаправление пакетов с использованием команды:
   echo 1 > /proc/sys/net/ipv4/ip_forward
9. С использованием утилиты ping проверить возможность сетевого взаимодействия виртуальных рабочих станций PC-1, PC-2 с сервером и между собой (проверять по ip-адресам!). Проверить возможность доступа с сервера Linux к серверу кафедры Asuserv (для доступа к Asuserv с PC-1, PC-2 потребуется выполнить настройку NAT, см. п. 4).

– Подключение и настройка маршрутизации. Ситуация 2

Цель данного этапа состоит в настройке маршрутизации средствами ОС Linux для ситуации, когда на маршрутизаторе установлен 1 сетевой интерфейс, а сегменты сети разделены за счет использования VLAN. Фильтры на данном этапе не настраиваются. Выход во внешнюю сеть обеспечивается через сеть 192.168.14x.0/24 и маршрутизируется хост-компьютером.

1. Подключить хост-компьютеры в сеть в соответствии с физической схемой для ситуации 2:

- ПК-1 (PC-1) включить в VLAN-3;
- ПК-4 (PC-2) включить в VLAN-4;
- ПК-2 (Router Linux): сетевой интерфейс 1 («Realtek 8029» или «3COM») через разъем B-0x включить в VLAN-2; сетевой интерфейс 2 (адаптер «D-Link DGE-528») через разъем C-0x включить в порт коммутатора, настроенный для передачи тегированных кадров 802.1Q (VLAN-2/3/4);
- коммутаторы соединить друг с другом через порты, настроенные для передачи тегированных кадров 802.1Q (VLAN-2/3/4).

2. Подключить образ виртуальной машины под управлением ОС Linux в системе VirtualBox на одном из компьютеров лаборатории. В настройках виртуальной машины в разделе «Сеть» включить 1-й виртуальный сетевой адаптер и настроить его на работу в режиме «Сетевой мост» через физический адаптер «D-Link DGE-528». Другие виртуальные сетевые адаптеры выключить.
3. Запустить ОС Linux на виртуальной машине, запустить консоль с правами администратора.
4. Создать виртуальные интерфейсы для каждой VLAN с использованием команды:

```
//добавление виртуального интерфейса для VLAN-2 на физический интерфейс eth0
vconfig add eth0 2
```

5. Настроить способ формирования имен виртуальных интерфейсов в виде eth0.x, где x – идентификатор VLAN:
   vconfig set_name_type DEV_PLUS_VID_NO_PAD
6. Выключить сетевые интерфейсы командой
   ifdown --all
7. Настроить статические адреса виртуальных интерфейсов маршрутизатора. Для этого в файле /etc/network/interfaces для каждого виртуального интерфейса (eth0.x) задать ip-адрес, маску подсети и шлюз. При этом на сам физический интерфейс адрес не назначать:
   auto eth0
   iface eth0 inet static
   address 0.0.0.0
   netmask 0.0.0.0
   auto eth0.2
   iface eth0.2 inet static
   address x.x.x.x
   netmask x.x.x.*x*
8. Включить сетевые интерфейсы с заданными настройками:
   ifup -all
9. Проверить с помощью команды ifconfig, что требуемые настройки сетевых интерфейсов установлены.
10. Включить перенаправление пакетов с использованием команды:
    echo 1 > /proc/sys/net/ipv4/ip_forward
11. С использованием утилиты ping проверить возможность сетевого взаимодействия виртуальных рабочих станций PC-1, PC-2 с сервером и между собой (проверять по ip-адресам!). Проверить возможность доступа с сервера Linux к серверу кафедры Asuserv (для доступа к Asuserv с PC-1, PC-2 потребуется выполнить настройку NAT, см. п. 4).

Форма представления результата: Отчет о проделанной работе, выполненная работа.

Критерии оценки:

Оценка «отлично» ставится, если задание выполнено верно.

Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.

Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.

Оценка «неудовлетворительно» ставится, если задание не выполнено.

Тема 1.1. Компьютерные сети

Практическая работа № 23,24

Списки управления доступом (AccessControlList)

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.

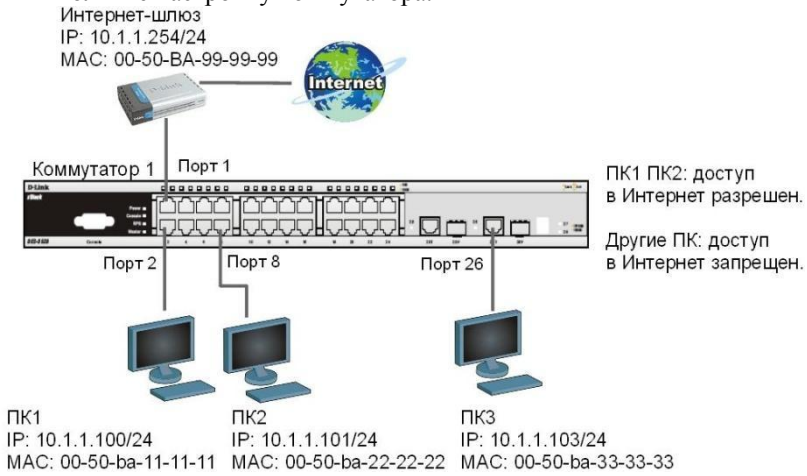
Материальное обеспечение:

учебно-лабораторный комплекс «Локальные компьютерные сети»

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 destination_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 destination_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 о проделанной работе, выполненная работа.

Критерии оценки:
Оценка «отлично» ставится, если задание выполнено верно.
Оценка «хорошо» ставится, если ход выполнения задания верный, но была допущена одна или две ошибки, приведшие к неправильному ответу.
Оценка «удовлетворительно» ставится, если в работе не получен ответ и приведено неполное выполнение задания, но ход выполнения задания.
Оценка «неудовлетворительно» ставится, если задание не выполнено.