МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Автоматизированные системы управления»

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Методические рекомендации к лабораторным работам для студентов направлений подготовки 09.03.01 «Информатика и вычислительная техника» и 09.03.04 «Программная инженерия» очной формы обучения

Могилев 2022

УДК 004.7
ББК 32.973.202
С33

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Автоматизированные системы управления» «13» сентября 2022 г., протокол № 2

Составитель канд. физ.-мат. наук, доц. Ю. Д. Столяров

Рецензент канд. техн. наук. доц. С. К. Крутолевич

Методические рекомендации к выполнению лабораторных работ по дисциплине «Сети и телекоммуникации» для студентов направлений подготовки 09.03.01 «Информатика и вычислительная техника» и 09.03.04 «Программная инженерия» очной формы обучения.

Учебно-методическое издание

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Ответственный за выпуск	А. И. Якимов
Корректор	А. А. Подошевко
Компьютерная верстка	М. М. Дударева

Подписано в печать 09.12.2022 . Формат 60×84/16. Бумага офсетная. Гарнитура Таймс. Печать трафаретная. Усл. печ. л. 2,33. Уч.-изд. л. 2,38. Тираж 31 экз. Заказ № 1162.

Издатель и полиграфическое исполнение:
Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/156 от 07.03.2019.
Пр-т Мира, 43, 212022, г. Могилев.

© Белорусско-Российский
университет, 2022

Содержание

Введение

Целью преподавания дисциплины «Сети и телекоммуникации» является ознакомление студентов с основными принципами построения компьютерных сетей, методами функционального анализа, проектирования и эксплуатации систем телеобработки данных в составе автоматизированных систем обработки информации и управления, получение знаний о вычислительных сетях, о принципах построения и функционирования современных сетей, об алгоритмах, протоколах и стандартах вычислительных сетей и интегрированных сетей обработки данных, а также о перспективных направлениях в развитии современных сетевых технологий.

В отчете отобразить структуру сети, необходимые таблицы и выводы по работе.

1 Лабораторная работа № 1. Изучение работы в качестве клиента в локальной сети

Цель работы: изучение работы в качестве клиента в локальной сети.

Основные теоретические положения

Для работы в сети помимо аппаратного обеспечения требуются сетевые операционные системы (ОС), с помощью которых пользователи смогут обмениваться информацией друг с другом, совместно работать с данными, использовать общие ресурсы и т. д.

Под сервером в разных случаях может пониматься как собственно компьютер, так и установленное на нем специализированное программное обеспечение, либо весь этот программно-аппаратный комплекс в целом.

Контроллеры домена обеспечивают в сетях Microsoft работу служб *Активного каталога* (*Active Directory*) и поддерживают базу данных всех зарегистрированных в *домене* пользователей, компьютеров, групп и ресурсов. Наличие такой базы данных позволяет администраторам централизованно управлять всеми сетевыми объектами и ресурсами. Пользователи же получают возможность входить в сеть с любого принадлежащего домену компьютера, подключаться к другим компьютерам и работать с их ресурсами.

Домен – это логическая группировка компьютеров, объединенных *общей базой данных пользователей и компьютеров, политикой безопасности и управления*.

Рабочая группа – это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети.

Порядок выполнения работы

1 Изучить теоретические сведения.
2 Получить задание у преподавателя.
3 Реализовать задание.
4 Сделать выводы по результатам исследований.
5 Оформить отчет.

Контрольные вопросы

1 Для чего нужны сетевые операционные системы? Чем они отличаются от «несетевых»? Какие возможны типы сетевых операционных систем?
2 Чем различаются клиентские и серверные сетевые операционные системы?
3 Какие сетевые сервисы и службы предоставляются в Windows 7/10?
4 Какие возможны виды серверов? Каково их назначение?
5 В чем заключается проблема безопасности при работе в сети?
6 Как организована работа пользователей в защищенных ОС?
7 В чем заключается авторизация пользователей? Как она реализуется?
8 Какие возможны виды учетных записей? Какая информация входит в учетную запись? Какие права доступа могут обеспечиваться для пользователя

учетной записи в ОС Windows?

9 Что такое рабочая группа? Что такое домен? В чем заключается их основное различие?

2 Лабораторная работа № 2. Проектирование локальной сети

Цель работы: изучить основные виды, преимущества и недостатки сетевых топологий, их наиболее распространенные типы сетей, виды и методы доступа к среде передачи данных, сетевые архитектуры.

Основные теоретические положения

При организации компьютерной сети исключительно важным является выбор *топологии*, т. е. *компоновки сетевых устройств и кабельной инфраструктуры*. Нужно выбрать такую топологию, которая обеспечила бы надежную и эффективную работу сети, удобное управление потоками сетевых данных. В топологии **Шина (Bus)** все компьютеры соединяются друг с другом *одним кабелем.* Посланные в такую сеть данные передаются *всем компьютерам*, но обрабатывает их только тот компьютер, аппаратный адрес сетевого адаптера которого записан в кадре как адрес получателя. В топологии **Кольцо (Ring)** каждый из компьютеров соединяется с двумя другими так, чтобы от одного он получал информацию, а второму – передавал ее. Последний компьютер подключается к первому и кольцо *замыкается*. В конфигурации **Звезда (Active Star)** все потоки данных идут исключительно через центральный компьютер; он же полностью отвечает за управление информационным обменом между всеми участниками сети.

Звезда – Шина (**Star Bus**), или **«пассивная звезда».** Здесь периферийные компьютеры подключаются не к центральному компьютеру, а к пассивному *концентратору*, или *хабу* (*hub*). Последний, в отличие от центрального компьютера, никак не отвечает за управление обменом данными, а выполняет те же функции, что и повторитель, т. е. восстанавливает приходящие сигналы и пересылает их всем остальным подключенным к нему компьютерам и устройствам. Именно поэтому данная топология, хотя физически и выглядит как «звезда», логически является топологией «шина».

Однако особо следует выделить топологию **Дерево (tree)**, которую можно рассматривать, как объединение нескольких «звезд». Именно эта топология сегодня является наиболее популярной при построении локальных сетей. Наконец, следует упомянуть о **сетчатой**, или **сеточной (mesh) т**опологии, в которой все либо многие компьютеры и другие устройства соединены друг с другом напрямую.

Чтобы компьютеры могли взаимодействовать, необходима какая-либо среда, обеспечивающая возможность передачи сигналов на физическом уровне.

Наиболее часто в компьютерных сетях применяются кабельные соединения, выступающие в качестве среды передачи электрических или оптических

сигналов между компьютерами и другими сетевыми устройствами. При этом используются следующие типы кабеля:

– коаксиальный кабель (coaxial cable);

– витая пара (twisted pair): неэкранированная (unshielded, UTP) и экранированная (shielded);

– волоконно-оптический, или оптоволоконный кабель (fiber optic).

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Контрольные вопросы

1 В чем заключается различие между физическими и логическими связями?

2 Каковы преимущества и недостатки конфигурации «звезда»? В каких локальных сетях она применяется?

3 Каковы преимущества и недостатки топологии «кольцо»? В каких локальных сетях она применяется?

4 Каковы преимущества и недостатки конфигурации «шина»? В каких локальных сетях она применяется?

5 Какие гибридные топологии вам известны?

6 Какие факторы необходимо учитывать при планировании сети?

7 К какой категории относится кабель из неэкранированной витой пары, способный передавать данные со скоростью до 10 Мбит/с?

8 Какие именно проводники используются в коаксиальном кабеле?

9 Зачем в кабеле «витая пара» используется несколько пар проводников?

10 Какой разъем используется для подключения кабеля «витая пара» к компьютерам?

11 Какие вы знаете разновидности архитектуры Ethernet? Чем они различаются?

3 Лабораторная работа № 3. Установка Windows Server

Цель работы: ознакомление с редакциями, набором сетевых служб, процессом установки и начальной настройки операционных систем семейства Windows Server.

Основные теоретические положения

Операционные системы семейства Windows Server 2008/7/10 являются универсальной платформой, на которой реализованы практически все сетевые службы – служба каталогов Active Directory, службы сетевой инфраструктуры (DNS, DHCP, WINS, маршрутизация и удаленный доступ), службы файлов

и печати, службы веб-публикаций и т. д. Установка, настройка и использование системы Windows Server зависит от тех задач, которые должна выполнять конкретная инсталляция. Типовые задачи системы корпорация Microsoft объединила в виде т. н. «ролей» сервера. Все роли можно увидеть при запуске мастеров «Мастер настройки сервера» или «Управление данным сервером». Active Directory – расширяемая и масштабируемая служба каталогов, в которой используется пространство имен, основанное на стандартной интернет-службе именования доменов (Domain Name System, DNS). IntelliMirror – средства конфигурирования, поддерживающие зеркальное отображение пользовательских данных и параметров среды, а также центральное администрирование установки и обслуживания программного обеспечения. Terminal Services – службы терминалов, обеспечивающие удаленный вход в систему и управление другими системами Windows Server. Windows Script Host – сервер сценариев Windows для автоматизации таких распространенных задач администрирования, как создание учетных записей пользователей и отчетов по журналам событий.

При планировании приобретения и установки сервера (или нескольких серверов) службе ИТ любой компании или организации необходимо решить целый комплекс задач:

– определить набор задач, возлагаемых на каждый сервер (сервер сетевой инфраструктуры, сервер службы каталогов, сервер файлов/печати, сервер удаленного доступа, сервер электронной почты, сервер баз данных и т. д.);

– определить предполагаемую нагрузку на сервер, исходя из выполняемых им ролей и количества пользователей и компьютеров в сети;

– исходя из полученной информации, определить аппаратную конфигурацию сервера (тип и количество процессоров, объем оперативной памяти, параметры дисковой подсистемы, сетевые адаптеры и пр.) и редакцию операционной системы (Standard, Enterprise, Datacenter, Web);

– спланировать процедуру установки и параметры системы (будет ли производиться модернизация системы с предыдущей версии или новая установка, как сконфигурировать дисковую подсистему, определить сетевые параметры и т. д.). После того как определены роли, выполняемые сервером, его аппаратная конфигурация, редакция системы, можно приступить к установке операционной системы на сервере.

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Контрольные вопросы

1 Какие редакции систем входят в семейство Windows Server?

2 Функциональные возможности различных редакций системы Windows Server.

3 Какие сетевые службы функционируют в операционных системах семейства Windows Server?

4 Лабораторная работа № 4. Планирование клиентов и групп в сетях Windows

Цель работы: изучить базовые структурные единицы – объекты Active Directory, такие как клиенты Windows Server (пользователи и компьютеры), группы пользователей, организационные единицы (OU); научиться создавать учетные записи пользователей, различные группы безопасности пользователей; настраивать параметры и свойства клиентов пользователей и компьютеров сети.

Основные теоретические положения

При планирование доменной сети Windows необходимым условием является, наличие контроллера домена на одном из серверов, в котором установлена и развернута роль Active Directory. Active Directory («Активный каталог», AD) – службы каталогов корпорации Microsoft позволяет администраторам создавать иерархическую структуру объектов, а именно клиентов (пользователи, компьютеры), объединять их в организационные единицы и группы безопасности.

Организационные единицы (organizational unit – OU подразделение) – контейнер, способствующий систематизации объектов домена в рамках логических административных групп. Подразделения OU можно использовать для организации объектов каталога AD в соответствии с их географическим расположением или с принадлежностью к некоторому структурному подразделению предприятия. Например, реализовав вычислительную сеть университета в виде домена, можно создать для каждого факультета свое подразделение. Для кафедр, имеющихся на каждом факультете, можно также создать свои подразделения. В каждом подразделении OU администратор создает такие объекты, как пользователи-клиенты, компьютеры-клиенты, различные группы безопасности, принтеры, приложения, общие папки, а также другие вложенные подразделения, относящиеся к локальному домену. Графически подразделения обозначаются пиктограммой папки с книгой. Объекты, ассоциированные с пользователями, компьютерами и контактной информацией, могут быть объединены в специальные группы (groups).

При создании группы в Active Directory системный администратор выбирает:

– области действия группы (локальная доменная, глобальная или универсальная область действия);

– тип группы (группа безопасности или группа распространения).

Группы безопасности используются для назначения разрешений на доступ к ресурсам определенной совокупности пользователей, например отдел кадров имеет право на формирование, редактирование базы данных работников предприятия.

Группы распространения (distribution groups) используются как списки рассылки электронной почты, не имеют дескрипторов безопасности и опреде-

ляются в доменах посредством консоли Active Directory – пользователи и компьютеры (Active Directory Users and Computers).

По области действия группы безопасности делятся на следующие категории:

– локальные группы компьютера;

– локальные группы домена;

– глобальные группы;

– универсальные группы.

Локальные группы компьютера могут быть использованы для назначения разрешений доступа к ресурсам, но только для локального компьютера. **Локальные группы AD домена** являются локальными в том смысле, что их можно использовать для назначения разрешений на доступ к ресурсам, которые являются локальными с точки зрения домена.

Глобальные группы AD могут содержать объекты следующих типов:

– учетные записи пользователей;

– другие глобальные группы из того же домена Active Directory.

Глобальные группы можно использовать для назначения разрешений на доступ к ресурсам, находящимся в любом домене леса.

Универсальные группы могут содержать объекты из любого доверенного домена и могут использоваться для назначения разрешений доступа к любому ресурсу в лесу Active Directory. Универсальные группы при наполнении и редактировании создают дополнительный трафик репликации, поэтому их нужно использовать с осторожностью. При планировании клиентов (пользователей) и групп рекомендуется использовать при обозначении имен групп следующее правило: имена глобальных групп должны начинаться с буквы G, а локальных в домене со как DL и вообще весь процесс создания пользователей и включая их в группы можно описать следующим образом: **A > G > DL < P.** Это означает, что учётные записи пользователей (**A** – Accounts) являются членами глобальной группы (**G**), которая включается в локальную группу того или иного домена (**DL**), а для локальной доменной группы настроены права доступа к ресурсу (например, к папке с файлами) – **P**. Чтобы пользователи получили доступ к этому ресурсу, остаётся сделать только одно – включить глобальную группу в локальную доменную группу.

Порядок выполнения работы

1 Создать подразделение типа (organizational unit, OU) в домене study.local подразделение FIO_Company (FIO – первые буквы ФИО студента).

2 Создать три подразделения в подразделении FIO_Company: Администрация – общий отдел – OU_ DirectGener ; Бухгалтерия OU _Buhgalter; Коммерческий Отдел – OU_Commercial.

3 Создать в каждом подразделении по два-три пользователя (согласовать с преподавателем).

4 Создать глобальные группы безопасности исходя из данной структуры нашей организации SIV_Company, т. е. тоже три глобальных групп: G_DirectGener, G_Buhgalter и G_Commercial. Для доступа к определенным ре-

сурсам каждого подразделения создать по две локальные группы безопасности для каждой OU – первая для пользователей с полным доступом к ресурсам, а вторая только для чтения. DL_DirectFull, DL_DirectRead, DL_BuhFull, DL_BuhRead и DL_ComrcFull, DL_ComrcRead.

5 Создать для подразделений необходимые ресурсы, папки, вложенные папки и файлы-документы. Используя свойства папок, назначить права доступа (Полный доступ, изменение, чтение) для соответствующих групп DL.

6 Вложить в созданные локальные группы DL сконфигурированные глобальные группы G_DirectGener, G_Buhgalter и G_Commercial. Перезагрузить сервер и проверить права доступа.

Контрольные вопросы

1 Дать определение таким понятиям, как глобальная, локальная группа безопасности.

2 Как лучше назначить «Общий доступ» к папке в сети?

3 Что означает стратегия A > G > DL < P и почему лучше пользователей размещать в глобальной группе, а доступ к ресурсам – в локальных группах?

4 Какие права предоставляются Администраторам сервера и домена?

5 Какие разрешения существуют на сетевом уровне и какие на уровне NTFS?

6 Какой доступ будет обеспечен пользователю к папке, если на сетевом уровне установлен доступ «Полный доступ», а для ОС сервера NTFS этой же папке «Обзор папки /Выполнение файлов»?

7 Как во вложенной папке лучше назначить новые разрешения, чтобы они не соответствовали разрешениям родительской папки?

8 Как произвести проверку существующих разрешений к ресурсам сервера и сети?

5 Лабораторная работа № 5. Изучение протоколов доступа к среде передачи

Цель работы: изучение принципов организации работы в сети: сетевых служб, клиентов, серверов, ресурсов, защиты при работе в сети.

Основные теоретические положения

Ethernet – это самый распространенный на сегодняшний день стандарт локальных сетей. Когда говорят Ethernet, то под этим обычно понимают любой из вариантов этой технологии. В более узком смысле Ethernet – это сетевой стандарт, основанный на экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 г. Метод доступа был опробован еще раньше: во второй половине 1960-х гг. в радиосети Гавайского университета использовались различные варианты случайного доступа к общей радиосреде, получившие общее название Aloha. В 1980 г. фирмы DEC, Intel и Xerox сов-

местно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля, который стал последней версией фирменного стандарта Ethernet. Поэтому фирменную версию стандарта Ethernet называют стандартом Ethernet DIX или Ethernet II.

На основе стандарта Ethernet DIX был разработан стандарт IEEE 802.3, который во многом совпадает со своим предшественником, но некоторые различия все же имеются. В то время как в стандарте IEEE 802.3 различаются уровни MAC и LLC, в оригинальном Ethernet оба эти уровня объединены в единый канальный уровень. В Ethernet DIX определяется протокол тестирования конфигурации (Ethernet Configuration Test Protocol), который отсутствует в IEEE 802.3. Несколько отличается и формат кадра, хотя минимальные и максимальные размеры кадров в этих стандартах совпадают. Часто для того, чтобы отличить Ethernet, определенный стандартом IEEE, и фирменный Ethernet DIX, первый называют технологией 802.3, а за фирменным оставляют название Ethernet без дополнительных обозначений. Все виды стандартов Ethernet (в том числе Fast Ethernet и Gigabit Ethernet) используют один и тот же метод разделения среды передачи данных – метод CSMA/CD.

Контрольные вопросы

1 В каком году и какие фирмы совместно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля?

2 На основе какого стандарта Ethernet был разработан стандарт IEEE 802.3?

3 Какой метод разделения среды передачи данных используют все виды стандартов Ethernet (в том числе Fast Ethernet и Gigabit Ethernet)?

4 Дайте определение метода управления обменом CSMA/CD.

5 Опишите алгоритм доступа к сети в соответствии с методом CSMA/CD для одного из абонентов, имеющих данные (кадры) для передачи.

6 Что такое коллизия?

7 Кем практически обнаруживаются коллизии?

6 Лабораторная работа № 6. Изучение протокола сетевого уровня IP

Цель работы: изучить правила адресации сетевого уровня; научиться распределять адреса между участниками сети передачи данных.

Основные теоретические положения

Стеком протоколов TCP/IP называют набор сетевых протоколов, используемых в интернете.

В стеке TCP/IP различают два уровня, согласно модели OSI это третий (IP-протокол) уровень и четвертый – TCP- и UDP-протоколы. Протоколы высокого уровня всегда базируются на протоколах более низких уровней. Протокол IP использует функциональность протоколов второго канального уровня. Например, технологию второго уровня модели OSI – Ethernet, описывающую

передачу данных по коаксиальному кабелю, витой паре или оптоволоконному кабелю. Протоколы этих уровней обычно реализуются на уровне «железа», например в сетевой карте компьютера. На верхних уровнях OSI (с 5-го по 7-й) находится множество протоколов прикладного уровня, выполняющих конкретные прикладные задачи. Обычно они программируются в отдельных приложениях. IP-протокол, лежащий в основе интернета, его название так и расшифровывается: Internet Protocol. В настоящее время используются следующие две версии протокола IP. IPv6 – сравнительно новая (текущая версия спецификации опубликована в декабре 1998 г.); IP-адрес имеет разрядность 128 бит и записывается в виде восьми 16-битных полей, с использованием шестнадцатеричной системы счисления и с возможностью сокращения двух и более последовательных нулевых полей; пример: 2001: db8:42::1337: cafe. IPv4-адрес имеет разрядность 32 бита и записывается в виде четырех десятичных чисел в диапазоне 0…255 через точку; пример: 192.0.2.34. Каждый узел может напрямую связаться только с узлами своей сети (например, подключенными к одному из сегментов Ethernet), для определения которых используется адрес сети – часть IP-адреса, определяемая маской сети. Связь с узлами других сетей осуществляется через промежуточные узлы – маршрутизаторы. Просмотреть маршрут пакета от вашего компьютера к другим узлам можно с помощью команды traceroute (в Linux) или tracert (в Windows).

IP-протокол отвечает за адресацию и маршрутизацию между компьютерами, TCP и UDP связывают два приложения на разных компьютерах в сети, используя для этого идентификаторы запущенных процессов – порты процессов.

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Контрольные вопросы

1 Назначение и принцип работы сетевого уровня.

2 Что такое сеть передачи данных?

3 Какие требования предъявляются к сетевой адресации?

4 Можно ли использовать в качестве сетевого MAC-адрес?

5 Что такое маска подсети?

6 Какова структура IP-адреса?

7 Чем определяется размер подсети?

8 Как определить диапазон адресов в подсети?

9 Как определить размер подсети?

7 Лабораторная работа № 7. Изучение маршрутизации IP

Цель работы: изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети.

Основные теоретические положения

Основное предназначение протокола IP – это объединение отдельных разнородных пакетных подсетей канального уровня (Ethernet, Token Ring, FDDI, Frame Relay) в составную сеть. В любой из разнородных подсетей пакет информации (данные с соответствующим сетевым заголовком) может быть доставлен по указанному адресу в этой конкретной подсети с использованием механизмов и свойств технологий канального уровня. Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами. Когда необходимо передать пакет между машинами, подключенными к разным подсетям, то машина-отправитель посылает пакет в соответствующий шлюз (шлюз подключен к подсети также как обычный узел). **ШЛЮЗ (GATEWAY)** – любое сетевое оборудование с несколькими сетевыми интерфейсами, осуществляющее продвижение пакетов между сетями на уровне протоколов сетевого уровня.

Из шлюза пакет направляется по определенному маршруту через систему шлюзов и подсетей, пока не достигнет шлюза, подключенного к той же подсети, что и машина-получатель; там пакет направляется к получателю.

Таким образом, шлюз выполняет **маршрутизацию** – процедуру нахождения в структуре сети пути достижения получателя (построение пути доставки пакетов). Для продвижения пакетов по тому или иному маршруту, **ШЛЮЗ** использует таблицу **маршрутизации,** состоящую из отдельных записей – правил маршрутизации. Правила маршрутизации определяют куда и как должны посылаться пакеты для разных сетей.

Каждое правило состоит из следующих компонентов.

НАЧАЛЬНЫЙ АДРЕС ПОДСЕТИ – порядок достижения которой описывает правило.

МАСКА подсети, которую описывает правило.

ШЛЮЗ – показывает, на какой адрес будут посланы пакеты, идущие в сеть назначения. Если пакеты будут идти напрямую, то указывается собственный адрес (точнее адрес того канала, через который будут передаваться пакеты),

ИНТЕРФЕЙС – показывает, через какой сетевой адаптер (его номер или IP-адрес) должен посылаться пакет в заданную сеть.

МЕТРИКА – показывает время, за которое пакет может достигнуть сети получателя (величина условная и может быть изменена при маршрутизации). Если имеется несколько правил достижения одной сети, пакеты посылаются по правилу с наименьшей метрикой.

Применение правила заключается в определении какой подсети (сети) принадлежит хост назначения, указанный в принимаемом пакете. Далее, со-

гласно правилу в таблице маршрутизации, направить пакет на адрес шлюза через соответствующий интерфейс.

Правила маршрутизации сведены в таблицу маршрутизации (где расположены по степени уменьшения маски), которую можно посмотреть с помощью команды **ROUTE PRINT**.

Контрольные вопросы

1 Сколько адресов может иметь хост?

2 Может ли у хоста быть прописано несколько шлюзов и почему?

3 Может ли у хоста быть прописано несколько шлюзов по умолчанию и почему?

4 Чем отличаются таблицы у разных классов сетевых устройств и почему?

5 Почему начальный адрес подсети должен быть кратен ее размеру?

6 Чем Вы руководствовались при выборе шлюзов по умолчанию?

7 Может ли физический сегмент сети содержать несколько сетевых подсетей?

8 Лабораторная работа № 8. Изучение сетевых утилит Windows

Цель работы: изучение основных утилит командной строки Windows, предназначенных для контроля и мониторинга сетей, построенных на базе стека протоколов TCP/IP.

Основные теоретические положения

Утилита – вспомогательная компьютерная программа в составе общего программного обеспечения для выполнения специализированных типовых задач, связанных с работой оборудования и операционной системы (ОС).

Утилиты предоставляют доступ к различным параметрам ОС, свойствам настройкам устройств компьютера, которые недоступны без их применения, либо делают процесс изменения некоторых параметров проще либо автоматизируют его. По функциям различают утилиты сетевые, системные, файловые и др. В данном случае рассматриваются сетевые утилиты.

Сетевые утилиты можно разделить на две категории – утилиты командной строки и утилиты с графическим интерфейсом.

В этой лабораторной работе рассмотрим утилиты – наиболее известные и часто применяемые системными администраторами. Сетевая операционная система Windows содержит набор утилит, полезных при диагностике, мониторинге сети и конфигурации узлов сети. Основными задачами этих программ является:

– определение работоспособности сети;

– определение параметров и характеристик сети;

– в случае неправильного функционирования сети – локализация службы или сервиса, вызывающих неисправность.

Главными параметрами сетевых подключений являются их канальные и сетевые адреса и параметры, влияющие на работу сетевого уровня.

Большинство рассматриваемых сетевых утилит для полноценной работы требуют наличия административных привилегий. Для операционных систем семейства Windows 2000/XP достаточно того, чтобы пользователь работал под учетной записью члена группы администраторов. Интерпретатор командной строки **cmd.exe** можно запустить с использованием меню Пуск – Выполнить – **cmd.exe**. В среде операционных систем Widows Vista/Windows 7 интерпретатор **cmd.exe** должен быть запущен для выполнения с использованием пункта контекстного меню «***Запустить от имени администратора*».** Командные файлы, в которых используются сетевые утилиты, также должны выполняться в контексте учетной записи с привилегиями администратора.

Единственным параметром канального уровня, который может быть просмотрен, являются MAC-адреса сетевых адаптеров. Для их просмотра можно воспользоваться утилитой GETMAC, широко известной утилитой IPCONFIG, которая покажет MAC-адреса для каждого адаптера, а также, начиная с Windows XP, с помощью ROUTE PRINT. Для изменения MAC- адресов следует воспользоваться драйверами соответствующих сетевых адаптеров, если конечно они допускают подобную операцию.

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Контрольные вопросы

1 В каких случаях применяется MAC-адрес? Дать определение и особенности MAC-адресов.

2 Для чего необходим протокол ARP? Особенности применения утилиты ARP с различными ключами.

3 Назначение протокола и сервера DHCP?

4 Протокол ICMP. Назначение. В каких утилитах он применяется, к какому стеку протоколов относится?

5 Что такое петля маршрутизации и как её устранить?

6 Утилита ping с различными ключами. Назначение и применение утилиты с различными ключами.

7 Правила маршрутизации на хостах. Объяснить каждое правило.

9 Лабораторная работа № 9. Изучение протоколов высших уровней

Цель работы: ознакомиться с принципами работы текстовых протоколов высших уровней на примере протоколов электронной почты.

Основные теоретические положения

Большинство стандартных сетевых протоколов высших уровней – **текстовые** – запросы и ответы передаются в виде текста, т. е. в запросах и ответах могут присутствовать только печатные символы.

Во многих протоколах ответы начинаются со специальной строки, состоящей из трехзначного числа и, возможно, текстового описания типа ответа. Трехзначное число разделяется на две части: первый символ рассматривается как код класса сообщения; два последние – как тип сообщения данной важности.

Коды классов следующие:

1) **информационное сообщение**. Обычно игнорируется программными клиентами;

2) **удачное завершение запроса**. Рассматривается программами-клиентами как успех обработки запроса ПО клиента.

Часто программы-серверы не различают сообщения первого и второго типа, т. е. информационное сообщение проходит по второй категории;

3) сообщение об удачной обработке запроса, но требующее **дополнительных действий** клиента;

4) **ошибка со стороны клиента**, т. е. клиент послал запрос, который не может обработать сервер вследствие ошибочности или недостаточности данных;

5) **ошибка со стороны сервера**. Клиент послал правильный запрос, но сервер не смог его выполнить в силу каких-то причин.

Трехзначные коды ответов очень удобны для программного распознавания, нет необходимости распознавать текст ответа, который, в общем случае, может прийти на разных языках, достаточно распознать только три цифры и программное обеспечение клиента выполнит соответствующее действие.

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Контрольные вопросы

1 Почему протоколы называются протоколами высших уровней?

2 Почему прием и передача электронной почты производятся по разным протоколам?

3 Почему POP3 требует обязательной аутентификации, а SMTP нет?

4 Как определить окончание письма?

5 Почему для проверки наличия писем удобнее использовать list 1 по сравнению с list без параметра?

6 Для чего предназначен данный вам сервер?

7 Является ли его протокол текст-ориентированным?

8 Поддерживает ли он трехсимвольные коды ответов?

9 Почему для работы со стандартными протоколами используют специальные программы?

10 Лабораторная работа № 10. Изучение пользовательских протоколов

Цель работы: изучение принципов анализа пользовательского сетевого трафика с помощью сетевых анализаторов; получение навыков в использовании сетевых анализаторов (снифферов); научиться анализировать и оценивать сетевой трафик на примере протоколов ARP, IP и ICMP, используя сетевой анализатор (сниффер Wireshark).

Основные теоретические положения

Sniffer (от англ. to sniff – нюхать) – это сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Перехват трафика может осуществляться:

– подключением сниффера в разрыв канала;

– обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свичей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);

– ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер;

– через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;

– через атаку на канальном (2-м) или сетевом (3-м) уровне, приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

В начале 1990-х гг. широко применялся хакерами для захвата пользовательских логинов и паролей. Широкое распространение хабов позволяло захватывать трафик без больших усилий в больших сегментах сети.

Снифферы применяются как в благих, так и в деструктивных целях. Анализ прошедшего через сниффер трафика, позволяет:

– отслеживать сетевую активность приложений;

– отлаживать протоколы сетевых приложений;

– локализовать неисправность или ошибку конфигурации;

– обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает нагрузку сетевого оборудования и каналов связи;

– выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие;

– перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью узнавания паролей и другой информации.

Постепенно из инструментов, предназначенных только для диагностики, снифферы превратились в средства для исследований и обучения. Например, они постоянно используются для изучения динамики и взаимодействий в сетях. В частности, они позволяют легко и наглядно изучать тонкости сетевых протоколов. Наблюдая за данными, которые посылает протокол, вы можете глубже понять его функционирование на практике, а заодно увидеть, когда некоторая конкретная реализация работает не в соответствии со спецификацией.

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Контрольные вопросы

1 Каковы основные цели мониторинга сетевого трафика?

2 Чем отличается мониторинг трафика от фильтрации?

3 Каково назначении класса программ-снифферов?

4 Какие основные функции выполняют снифферы?

5 Зачем используются фильтры отображения и фильтры захвата сниффера Wireshark? В чем их отличие?

6 Какие базовые функции статистической обработки захваченных пакетов имеет сниффер Wireshark?

7 Какие задачи рассчитан решать протокол ARP?

11 Лабораторная работа № 11. Изучение веб-технологий

Цель работы: овладение технологией создания гипертекстовых документов – создания и оформления гипертекстовых документов в HTML-формате средствами Word, создания внешних и внутренних гиперссылок, просмотра HTML-документов средствами браузера, программирования фреймов с элементами языка HTML.

Основные теоретические положения

Веб-узел – это специальная папка, в которой размещены файлы, содержащие текстовую информацию по какой-либо теме, а также информацию в виде рисунков, графиков, фотографий, анимационных изображений, звуковых эффектов. В этих файлах содержатся описания веб-страниц на одном из языков разметки гипертекста – HTML (Hyper Text Markup Language) или XML (Extensible Markup Language). Они имеют одно из следующих расширений: html, htm, xml. Все, что содержит веб-узел, далее будем называть веб-проектом. Существуют три типа веб-узлов: создаваемые на веб-сервере поставщика услуг интернета; создаваемые в интрасети как веб-узлы группы, виртуальный веб-узел, создаваемый на жестком диске автономного компьютера, не подключенного к какой-либо сети.

Веб-страница представляет собой документ, содержащий описание ее структуры и содержания, создаваемого посредством команд, сформированных на языке HTML.Эти команды выполняются программой-браузером, таким, например, как Microsoft Internet Explorer. Интерпретируя команды HTML, браузер создает визуальное изображение документа, собирая его из отдельных объектов. Таким образом, *веб-документ* – это изображение в окне браузера, которое он создает, выполняя команды языка HTML. Фактически веб-мастер создает не сам документ, а лишь описывает его структуру на языке гипертекстовой разметки. Сам документ создается браузером, интерпретирующим команды языка HTML. Таким образом, для каждой веб-страницы на узле должен быть помещен файл, содержащий документ HTML с ее описанием. Язык HTML не является языком программирования, он обеспечивает только описание структуры HTML-документа. Для создания интерактивных веб-страниц, кроме языка HTML, служат так называемые сценарии, представляющие собой программы, которые создаются на языках программирования, обеспечивающих их интерпретацию и выполнение браузером. Существуют две разновидности таких языков – Java Script и VB Script. Поэтому для того чтобы создавать интерактивные веб-страницы, необходимо использовать язык HTML и один из приведенных языков программирования. Документы HTML могут иметь различную структуру, включающую множество элементов, но все они должны содержать два таких элемента, как раздел заголовка страницы – HEAD и тело документа (страницы) – BODY.

Раздел заголовка служит для описания общих свойств страницы, таких как заголовок (имя) страницы, который будет отображаться в строке имени окна браузера, META-указаний и описания таблиц стилей. META-указания служат для задания параметров, которые необходимы для поисковых систем. Этот раз-

дел формируется с помощью парного дескриптора <HEAD>. Внутри контейнера <HEAD> могут помещаться дескрипторная пара <TITLE>, содержащая внутри себя информацию, которая должна быть помещена в строку заголовка окна браузера, и одиночный дескриптор <META>, который предназначен для записи информации, необходимой для поисковых систем.

Порядок выполнения работы

1 Создайте HTML-документы средствами Word.

2 Оформите каждый документ в соответствии с его содержанием и целью работы.

3 Создайте ссылки между главной страницей и остальными страницами.

4 Запустите созданные документы с помощью Internet Explorer.

5 Оформите отчет.

Контрольные вопросы

1 Что такое веб-узел?

2 Какие существуют типы веб-узлов?

3 По какому принципу организуется связь информационных страниц в веб-узле?

4 Как создаются сайты?

5 Что такое HTML?

6 Что такое дескриптор (тег) языка HTML?

7 Какова структура HTML-документа?

8 Назовите инструментальные средства для ввода и редактирования HTML-документов.

9 Что такое гипертекст?

10 Какова структура гипертекста?

11 Что такое гиперссылки?

12 Что такое внутренние гиперссылки?

13 Как создать внутреннюю гиперссылку?

14 Что такое внешние гиперссылки? Как их создать?

12 Лабораторная работа № 12. Изучение технологий распределенных вычислений

Цель работы: изучение технологий создания распределенных вычислений на основе классов TcpClient и TcpListener.

Основные теоретические положения

Под распределенными вычислениями будем понимать такой способ решения трудоемких вычислительных задач, при котором используется сразу несколько компьютеров, объединенных в общую сеть. Мощность таких систем можно наращивать почти не ограниченно. При этом задачи, которые такая сеть решает, должны быть хорошо распараллеливаемыми. Иначе ком-

пьютеры будут простаивать. В качестве примера рассмотрим простую задачу: умножение матриц. В больших матрицах достаточно объемные вычисления и задача полностью распараллеливается. Компьютер в нашей сети будет брать одну строку из матрицы A, умножать ее на матрицу B и получать строку матрицы C. Сложив полученные строки, мы получим элемент итоговой матрицы C. В сети будет главный компьютер, который выдает задания остальным, принимает от них результат и формирует матрицу C. Остальные компьютеры будут ему подчиняться. Обычно для такого взаимодействия используют передачу сообщений. Сообщение – это некий контейнер, в котором есть определенные поля, например, структура или класс. В полях должен быть указан получатель. Для рассматриваемого примера выберем следующие поля:

– целочисленный тип сообщения (запрос на выдачу нового задания; выдача нового задания, сообщение с результатом; работа завершена);

– одномерный массив для строки матрицы A или строки матрицы C;

– двухмерный массив для матрицы B.

Организовать взаимодействие по сети можно разными способами. Самым простым является использование классов TcpClient и TcpListener, которые включены в .Net Framework.

Порядок выполнения работы

1 Найдите интеграл на интервале.
2 Рассчитайте энергию сигнала скользящим окном.
3 Усредните сигнал скользящим окном.
4 Рассчитайте определители всех порядков у матрицы.
5 Подсчитайте количество буквы «И» в текстовом файле.
6 Зашифруйте текстовый файл.

Контрольные вопросы

1 Что такое распределенные вычисления ?
2 Что такое сообщение ?
3 Какими способами можно организовать взаимодействие в сети ?

13 Лабораторная работа № 13. Маршрутизатор. Статическая маршрутизация

Цель работы: для статической маршрутизации научиться составлять таблицы маршрутизации, настроить связь двух сетей через маршрутизатор и протестировать их работу.

Основные теоретические положения

Таблица маршрутизации может составляться двумя способами: статично и динамично. В случае статической маршрутизации записи в таблице вводятся и изменяются вручную. Такой способ требует вмешательства администратора

каждый раз, когда происходят изменения в топологии сети. С другой стороны, он является наиболее стабильным и требующим минимума аппаратных ресурсов маршрутизатора для обслуживания таблицы. Статическая маршрутизация – вид маршрутизации, при котором информация о маршрутах заносится в таблицы маршрутизации каждого маршрутизатора вручную администратором сети. Отсюда сразу же вытекает ряд недостатков. Прежде всего это очень плохая масштабируемость сетей, т. к. при добавлении N+1 сети потребуется сделать 2(N+1) записей о маршрутах. Но, при использовании статических записей процессору маршрутизатора не требуется производить никаких расчетов, связанных с определением маршрутов – это плюс. Статическая маршрутизация успешно используется при организации работы компьютерных сетей небольшого размера (один-два маршрутизатора), в силу легкости конфигурации и отсутствии дополнительной нагрузки на сеть в виде широковещательного служебного трафика, характерного для динамических протоколов маршрутизации. Также статическая маршрутизация используется на компьютерах внутри сети. В таком случае обычно задается маршрут шлюза по умолчанию. Маршрутизатором (шлюзом) называется узел сети с несколькими IP-интерфейсами (содержащими свой MAC-адрес и IP-адрес), подключенными к разным IP-сетям, осуществляющий на основе решения задачи маршрутизации перенаправление дейтаграмм из одной сети в другую для доставки от отправителя к получателю. Динамическая маршрутизация – это процесс протокола маршрутизации, определяющий взаимодействие устройства с соседними маршрутизаторами. Маршрутизатор будет обновлять сведения о каждой подключенной к нему сети. Если в сети произойдет изменение, протокол динамической маршрутизации автоматически информирует об изменении все маршрутизаторы. Если же используется статическая маршрутизация, обновить таблицы маршрутизации на всех устройствах придется системному администратору. Статическая маршрутизация позволяет сократить объем таблиц маршрутизации в конечных узлах и маршрутизаторах за счет использования в качестве номера сети назначения т. н. маршрута по умолчанию – default (0.0.0.0), который обычно занимает в таблице маршрутизации последнюю строку. Если в таблице маршрутизации есть такая запись, то все пакеты с номерами сетей, которые отсутствуют в таблице маршрутизации, передаются маршрутизатору, указанному в строке default. Шлюз по умолчанию (defaultgateway) – адрес маршрутизатора, на который отправляется трафик, для которого не нашлось отдельных записей в таблице маршрутизации. Для устройств, подключенных к одному маршрутизатору (как правило, это рабочие станции) использование шлюза по умолчанию – единственная форма маршрутизации. Доступность компьютера проверяется при помощи посылки контрольного диагностического сообщения по протоколу ICMP (Internet Control Message Protocol), по которому любая оконечная станция должна выдать эхо-

ответ узлу, отправившему такое сообщение. В сетях на основе TCP/IP для проверки соединений обычно используется утилита ping. Эта программа отправляет запросы (ICMP Echo-Request) протокола ICMP узлу сети с указанным IP-адресом. Получив этот запрос, исследуемый узел должен послать пакет с ответом (ICMP Echo-Reply). Первый узел фиксирует поступающие ответы. Время между отправкой запроса и получением ответа (RTT, от англ. Round Trip Time) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, т. е. косвенно определить загруженность каналов передачи данных и промежуточных устройств. Метрика – числовой коэффициент, влияющий на выбор маршрута в компьютерных сетях. Как правило, определяется количеством «хопов» (ретрансляционных переходов) до сети назначения или параметрами канала связи. Чем метрика меньше, тем маршрут приоритетнее. Петля маршрутизации – явление, возникающее, когда маршрутизатор отсылает пакет на неверный адрес назначения. Получивший такой пакет маршрутизатор возвращает его обратно. Таким образом, получается петля. Для борьбы с подобными петлями в TCP/IP предусмотрен механизм TTL. Протоколы маршрутизации также предлагают свои способы.

Порядок выполнения работы

Настраиваем связь двух сетей через маршрутизатор.
Построим такую сеть (рисунок 13.1).

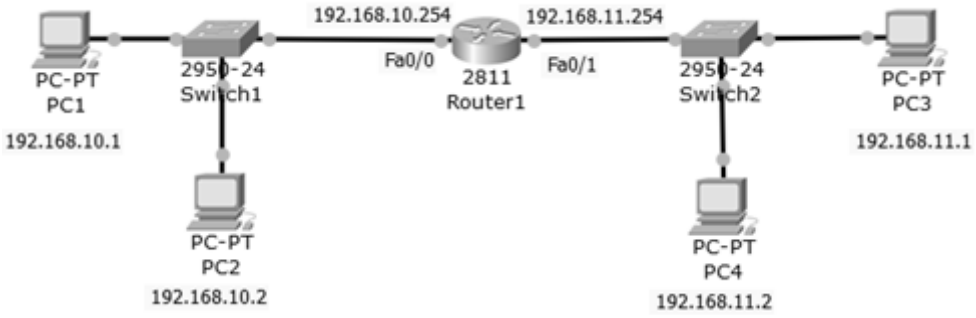

Рисунок 13.1 – Постановка задачи

Наша цель – настроить связь двух сетей через маршрутизатор (роутер). Настраиваем компьютеры подсети 192.168.10.0 и подсети 192.168.11.0. согласно постановке задачи. Настраиваем роутер (маршрутизатор) как шлюз 192.168.10.254 для первой сети на интерфейсе Fa0/0. Аналогично настраиваем роутер как шлюз 192.168.11.254 для второй сети на интерфейсе Fa0/1. Проверяем таблицу маршрутизации командой **show ip oute.** Проверяем связь роутера 1 и ПК и связь через роутеры с ПК двух сетей.

Контрольные вопросы

1 Что такое таблица маршрутов?
2 Чем статическая маршрутизация отличается от динамической?
3 Какие две формы задания статической маршрутизации вы знаете?
4 Как в команде маршрутизации определяется сеть назначения?
5 Объясните значения полей в командах маршрутизации.
6 Почему в качестве поля Адрес рекомендуют использовать адрес следующего хопа по пути к сети назначения?
7 Когда используется маршрутизация по умолчанию?

14 Лабораторная работа № 14. Протокол DHCP

Цель работы: изучение особенностей установки и управления DHCP-сервером в сетях Windows.

Основные теоретические положения

DHCP (Dynamic Host Configuration Protocol) – это протокол, позволяющий компьютерам динамически получать IP- адреса и другие сетевые параметры. Для работы протокола DHCP требуется сервер и клиент.

DHCP-сервер – это сервер, который раздает IP-адреса и параметры компьютерам в сети, соответственно, на нем и задаются настройки раздачи IP-адресов и сетевых параметров. **DHCP-клиент** – это приложение, установленное на клиентских компьютерах, которое обращается к DHCP-серверу для получения IP-адреса и соответствующих параметров. Во всех операционных системах по умолчанию установлен клиент DHCP, например, в Windows он выглядит в виде службы с логичным названием DHCP-клиент. DHCP доступен как для IPv4 (DHCPv4) (версии 4), так и для IPv6 (DHCPv6) (версии 6). Каждому устройству, подключенному к сети, нужен уникальный IP-адрес. Сетевые администраторы назначают статические IP-адреса маршрутизаторам, серверам, принтерам и другим сетевым устройствам, местоположение которых (физическое и логическое) вряд ли изменится. Обычно это устройства, предоставляющие услуги пользователям и устройствам в сети, поэтому назначенные им адреса должны оставаться постоянными. Кроме того, статические адреса позволяют администраторам удаленно управлять этими устройствами – до них проще получить доступ к устройству, когда они могут легко определить его IP-адрес. Использование DHCP в локальной сети упрощает назначение IP-адресов как на настольных, так и на мобильных устройствах. Использование централизованного DHCP-сервера позволяет администрировать все назначения динамических IP-адресов с одного сервера. Эта практика делает управление IP-адресами более эффективным и обеспечивает согласованность внутри организации, включая филиалы. DHCPv4 динамически назначает адреса IPv4 и другую информацию о конфигурации сети. Отдельный сервер DHCPv4 является масштабируемым и относительно простым в управлении. Однако в небольшом офисе маршрутиза-

тор может быть настроен для предоставления услуг DHCP без необходимости выделенного сервера. Для подключения компьютера к интернету через сеть TCP/IP предварительно необходимо настроить сетевой протокол DHCP. Именно он отвечает за то, чтобы ПК автоматически получил IP-адрес и прочие необходимые параметры для полноценного пользования интернетом. По умолчанию такой протокол в системе Windows активизируется автоматически. Правда срабатывает он не всегда. В этом случае приходится думать над тем, как вручную включить DHCP в ОС Windows 7. А сделать это на самом деле несложно.

Порядок выполнения работы

В практической части необходимо выполнить установку и настройку DHCP-сервера способом – через опцию «Службы». Отталкиваясь от модели действия DHCP «клиент – сервер», включить этот сетевой протокол в Windows 7 можно через сервис «Службы». Используется следующий порядок: необходимо войти в меню «Пуск», перейти в раздел «Панель управления», а в нем выбрать вкладку «Администрирование»: Панель управления – Администрирование. Далее в открывшемся списке находим и кликаем пункт «Службы», чтобы появилось окошко соответствующего сервиса (рисунок 14.1).

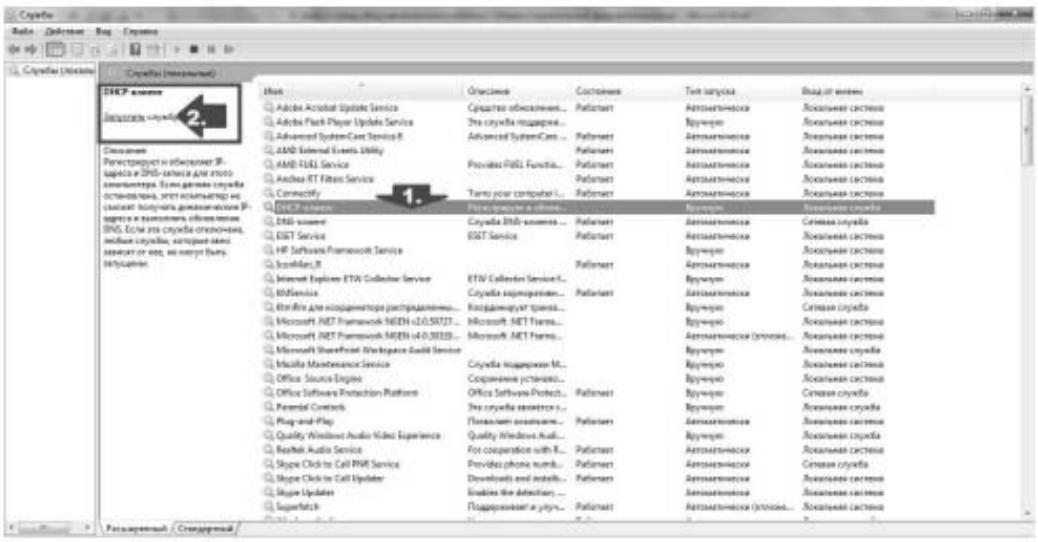

Рисунок 14.1 – Запуск DHCP-клиента

После того как оно открылось, ищем в нем службу DHCP-клиент и запускаем ее нажатием соответствующей кнопки в меню Запуск DHCP-клиента, проверяем тип запуска службы. В идеале запускаться она должна автоматически. Если это не так, кликаем правой кнопкой мыши по пункту DHCP-клиент, выбираем в появившемся меню вкладку «Свойства», выставляем автоматический тип запуска и сохраняем настройки нажатием кнопки OK. В результате таких действий сетевой протокол в OS Windows 7 будет срабатывать автоматически, не требуя дополнительных настроек.

Контрольные вопросы

1 Дайте определение DHCP.
2 Что собой представляет DHCP-сервер, в чем его функции?
3 Дайте определение DHCP-клиента.
4 В чем преимущества использования DHCP?
5 Для чего необходима настройка DHCP в сети?

15 Лабораторная работа № 15. Динамическая маршрутизация (протокол OSPF)

Цель работы: настроить автоматическое построение таблиц маршрутизации в составной сети по протоколу OSPF.

Основные теоретические положения

Работа протокола OSPF строится по следующему алгоритму.

Маршрутизаторы производят обмен малыми пакетами HELLO. После выполнения обмена между ними устанавливаются соседства. Каждый из маршрутизаторов добавляет в специальную локальную таблицу соседей. Маршрутизаторы выполняют сбор состояний своих связей с соседями (линков). Линки включают id самого маршрутизатора и соседа, сеть и префикс, тип сети и метрику (стоимость линка). После сбора состояний маршрутизатор формирует пакет LSA (Link State Advertisement). LSA рассылается каждому соседу, который передает пакет дальше по сети. После получения пакета LSA каждый маршрутизатор добавляет содержащуюся в нем информацию в локальную таблицу LSDB (Link State Database). В таблице LSDB накапливаются данные обо всех парах маршрутизаторов в пределах сети. На основании накопленных данных выстраивается полная карта сети, которая включает все действующие маршрутизаторы и образованные между ними связи. Используя карту, каждый маршрутизатор выполняет поиск самых коротких маршрутов во все сети и формирует из них таблицу маршрутизации. Пакет OSPF помещается в пакет IP с мультикастовым адресом получателя. Отправителю же в нем соответствует адрес маршрутизатора. Пакет помещается в мультикастовый фрейм, например в Ethernet. При формировании списков контроля доступа нужно учитывать, что OSPF инкапсулируется непосредственно в IP, а не в UDP или TCP. Hello-пакеты отправляются с установленной периодичностью. По умолчанию она составляет один раз в 10 с для сетей BMA и point-to-point и один раз в 40 с для сетей NBMA. Также существует понятие Dead-интервала, который по умолчанию равняется четырем Hello-интервалам. Если в течение этого периода маршрутизатор не получает ни одного пакета, то он считает, что сосед отключился. За этим следует пересчет и обновление таблицы маршрутизатора. Открытый протокол маршрутизации не устанавливает отдельных требований к расчету метрики и оценки маршрутов.

Порядок выполнения работы

1 Соберите схему, изображенную на рисунке 15.1.

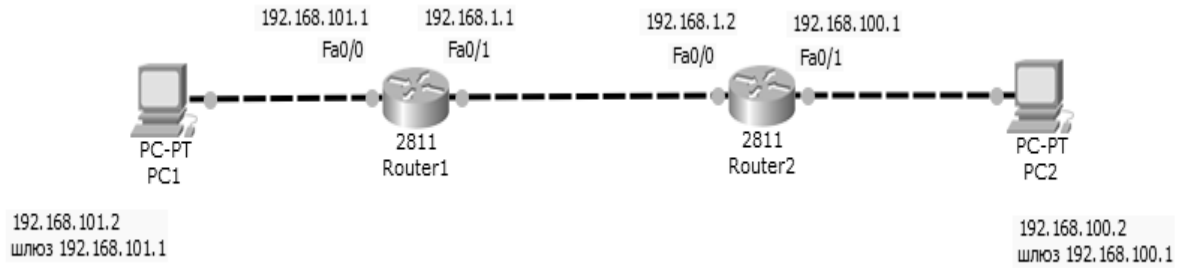

Рисунок 15.1 – Схема для конфигурации протокола OSPF

2 Выполним конфигурирование Router1 (рисунок 15.2).

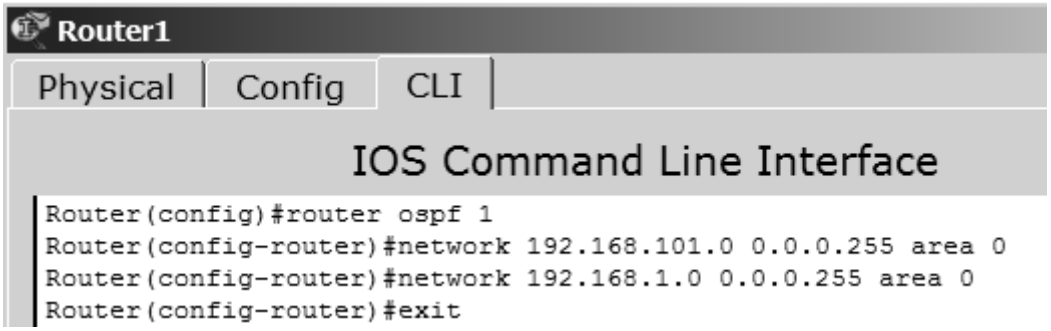

Рисунок 15.2 – Настройка Router1

3 Выполним настройки R2 (рисунок 15.3).

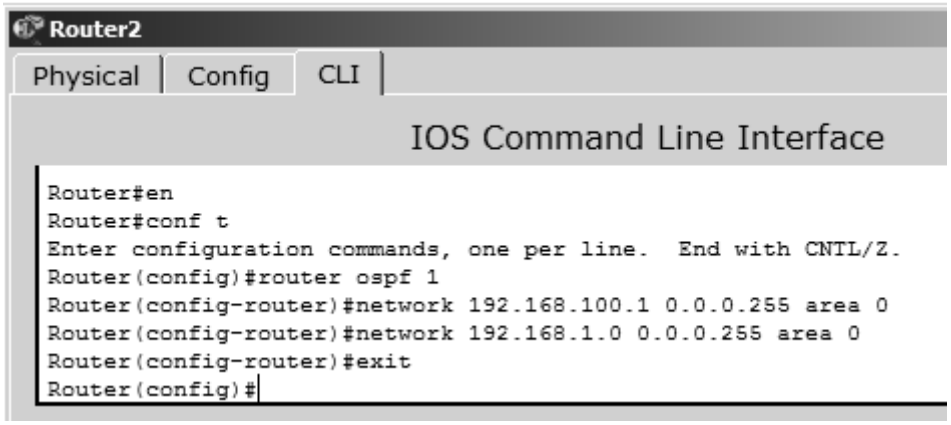

Рисунок 15.3 – Настройка R2

4 Для проверки маршрутизации пропингуем ПК из разных сетей.

Контрольные вопросы

1 Что такое динамическая маршрутизация? Какие этапы в ней присутствуют?

2 Чем отличаются векторные алгоритмы маршрутизации от алгоритмов на основе состояний каналов связей?

3 Что такое метрика маршрута? Зачем она используется?

4 Может ли в таблице маршрутизации быть несколько строк, описывающих путь до одной и той же сети?

5 Что такое технология «расщепления горизонта»?

6 За счет чего сокращается объем передаваемой по сети служебной информации при использовании протокола OSPF?

16 Лабораторная работа № 16. Динамическая маршрутизация (протокол EIGRP)

Цель работы: настроить автоматическое построение таблиц маршрутизации в составной сети по протоколу EIGRP.

Основные теоретические положения

EIGRP – это «продвинутый протокол маршрутизации вектора расстояния». Рассмотрим фундаментальную характеристику протокола маршрутизации состояния канала, которая заключается в том, что маршрутизаторы поддерживают таблицу топологии, указывающую, как маршрутизаторы связаны между собой. Эти маршрутизаторы (говоря о протоколах маршрутизации, таких как OSPF и IS-IS) затем запускают алгоритм Дейкстры на этой топологии, чтобы определить «кратчайший» путь к целевой сети с точки зрения конкретного маршрутизатора. EIGRP не поддерживает представление о топологии сети и не выполняет алгоритм Дейкстры. Скорее всего, таблица топологии EIGRP содержит список доступных сетей, а также информацию о «расстоянии» до этих сетей.

Порядок выполнения работы

Настройка EIGRP. Заходим в режим конфигурирования роутера router eigrp 1. Указываем все сети, которые подключены к рассматриваемому роутеру, с помощью команд network 192.168.1.0 0.0.0.255, network 10.10.10.0 0.0.0.3. Аналогично укажите для оставшейся сети. Отключим суммирование маршрутов с помощью команды no auto-summary; Аналогично настроим роутер Router2. Проверим настройки и таблицы маршрутизации. Проверим ping с компьютера.

Проверим реализацию отказоустойчивость системы. Распространим дефолтный маршрут на другие маршрутизаторы, чтобы не прописывать их статически: 8.1. Пусть Router2 имеет дефолтный маршрут ip route 0.0.0.0 0.0.0.0 192.168.3.2; 8.2. Зайдем в настройку EIGRP router eigrp 1 и распространим информацию о дефолтном маршруте с помощью команды redistribute static. Проверим, например на Router1, таблицу маршрутизации.

Контрольные вопросы

1 Что такое протокол EIGRP?
2 Какую топологию поддерживает протокол EIGRP?
3 Что содержит таблица топологии?
4 Что такое дефолтный маршрут?

17 Лабораторная работа № 17. Виртуальные сети VLAN

Цель работы: изучить структуру и особенности применения виртуальных локальных компьютерных сетей.

Основные теоретические положения

VLAN (Virtual Local Area Network) – виртуальная локальная компьютерная сеть из группы хостов с общим набором требований. VLAN позволяют хостам группироваться или дистанцироваться между собой. Устройства, в пределах одной VLAN могут общаться, а узлы, находящиеся в разных VLAN невидимы друг для друга. Они взаимодействуют так, как если бы они были подключены к широковещательному домену независимо от их физического местонахождения. Проектирование локальных сетей кампуса с использованием большего количества VLAN, в каждом из которых используется минимальное количество коммутационного оборудования, часто помогает улучшить локальную сеть во многих отношениях. Например, широковещательная передача, отправленная одним узлом во VLAN1, будет приниматься и обрабатываться всеми другими узлами этого VLAN1, но не узлами из другого VLAN. Чем меньше посторонних узлов в сети получают широковещательные кадры, тем выше безопасность локальной сети.

В следующем списке перечислены наиболее распространенные причины, по которым следует создавать VLAN: чтобы уменьшить нагрузку на процессор на каждом устройстве; повышение производительности узла путем уменьшения числа устройств, которые принимают каждый широковещательный кадр; повышение безопасности хостов за счет применения различных политик безопасности для каждого VLAN; создание подразделений, группирующих пользователей по отделам или группам, которые работают вместе, а не по физическому местоположению; уменьшение нагрузки для протокола связующего дерева (STP) путем ограничения VLAN одним коммутатором доступа.

Порядок выполнения работы

Используя два VLAN, организовать две сети, что изображены на рисунке 17.1 создать два широковещательных домена с помощью одного коммутатора. С VLAN коммутатор может настроить некоторые интерфейсы в один широковещательный домен, а некоторые в другой, создавая несколько широковещательных доменов. Эти отдельные широковещательные домены, созданные коммутатором, называются виртуальными локальными сетями (VLAN).

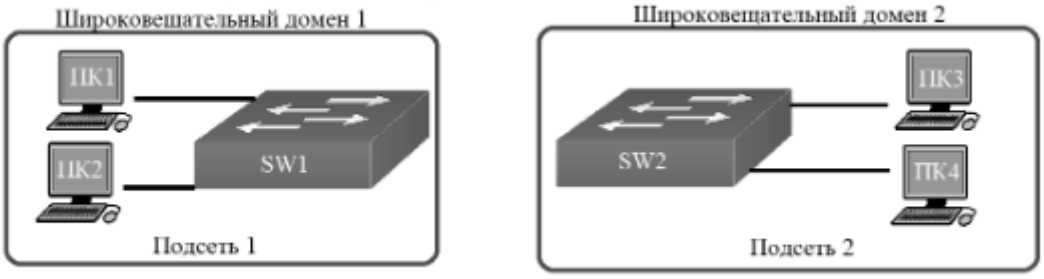

Рисунок 17.1 – Две VLAN-сети

Использовать один коммутатор для нескольких широковещательных доменов (рисунок 17.2). Из широковещательного домена 1 (подсеть 1) две системы ПК1 и ПК2 подключены к коммутатору SW1. Из широковещательного домена 2 (подсеть 2) к коммутатору SW1 подключены две системы ПК3 и ПК4. Из широковещательного домена 1 (подсеть 1) две системы ПК1 и ПК2 подключены к коммутатору SW1. Из широковещательного домена 2 (подсеть 2) к коммутатору SW1 подключены две системы ПК3 и ПК4.

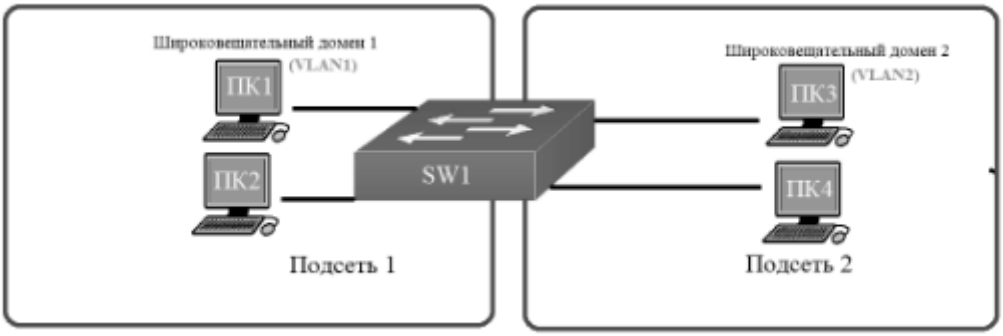

Рисунок 17.2 – Две VLAN-сети с одним коммутатором

Контрольные вопросы

1 Что такое VLAN?
2 Преимущества VLAN.
3 Свойства VLAN.

18 Лабораторная работа № 18. Списки доступа

Цель работы: изучить настройку стандартного списков доступа на маршрутизаторе.

Основные теоретические положения

Списки доступа (access-lists) используются в целом ряде случаев и являются механизмом задания условий, которые роутер проверяет перед выполнением каких-либо действий. Маршрутизатор проверяет каждый пакет и на основании

вышеперечисленных критериев, указанных в ACL определяет, что нужно сделать с пакетом, пропустить или отбросить. Типичными критериями являются адреса отправителя и получателя пакета, тип протокола. Каждый критерий в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор строк с критериями, имеющих один и тот же номер (или имя). Порядок задания критериев в списке существенен. Проверка пакета на соответствие списку производится последовательным применением критериев из данного списка (в том порядке, в котором они были введены). Пакет, который не соответствует ни одному из введенных критериев будет отвергнут. Для каждого протокола на интерфейс может быть назначен только один список доступа. писки доступа либо нумеруются, либо именуются. Использование нумерованных, либо именованных списков доступа определяется их применением (некоторые протоколы требуют использования только нумерованных списков, некоторые допускают как именованные, так и нумерованные списки).

Если используются нумерованные списки, то номера их должны лежать в определенных диапазонах, в зависимости от области применения списка. Некоторые наиболее часто применяемые диапазоны, приведены в таблице 18.1.

Таблица 18.1 – Диапазоны списков доступа

Протокол	Диапазон номеров
Стандартный список IP	1 to 99
Расширенный список IP	100 to 199
MAC Ethernet address	700 to 799
IPX	800 to 899
Extended IPX	900 to 999
IPX SAP	1000 to 1099

Списки доступа определяют критерии, на соответствие которым проверяется каждый пакет, обрабатываемый маршрутизатором в точке списка доступа. Типичными критериями являются адреса отправителя и получателя пакета, тип протокола. Однако для каждого конкретного протокола существует свой собственный набор критериев, которые можно задавать в списках доступа. Каждый критерий в списке доступа записывается отдельной строкой. Список доступа в целом представляет собой набор строк с критериями, имеющих один и тот же номер (или имя). Есть только возможность стереть весь список целиком. Порядок задания критериев в списке существенен. Проверка пакета на соответствие списку производится последовательным применением критериев из данного списка (в том порядке, в котором они были введены). Если пакет удовлетворяет какому-либо критерию, то дальнейшие проверки его на соответствие следующим критериям в списке – *не производятся*. В конце каждого списка системой

добавляется неявное правило. Таким образом, пакет, который не соответствует ни одному из введенных критериев, будет отвергнут.

Порядок выполнения работы

Изучить примеры составления списков. Поскольку порядок строк в списке доступа очень важен, а также поскольку невозможно изменить этот порядок или исключить какие-либо строки из существующего списка доступа, рекомендуется создавать списки доступа на tftp-сервере и загружать их целиком в маршрутизатор, а не пытаться редактировать их на маршрутизаторе.

Назначение списков доступа на интерфейсы.

Для каждого протокола на интерфейс может быть назначен только один список доступа. Для большинства протоколов можно задать раздельные списки для разных направлений трафика. Если список доступа назначен на входящий через интерфейс трафик, то при получении пакета, маршрутизатор проверяет критерии, заданные в списке. Если пакет разрешен данным списком, то он передается для дальнейшей обработки. Если пакет запрещен, то он отбрасывается. Если список доступа назначен на выходящий через интерфейс трафик, то после принятия решения о передаче пакета через данный интерфейс маршрутизатор проверяет критерии, заданные в списке. Если пакет разрешен данным списком, то он передается в интерфейс. Если пакет запрещен, то он отбрасывается. В конце каждого списка стоит неявное правило «deny all», поэтому при назначении списков на интерфейс нужно следить, чтобы явно разрешить все виды необходимого трафика через интерфейс (не только пользовательского, но и служебного, например, обмен информацией по протоколам динамической маршрутизации).

Списки доступа для протокола IP.

Стандартные и расширенные нумерованные списки доступа.

Поддерживаются следующие виды списков доступа для IP:

– стандартные списки доступа (проверяют адрес отправителя пакета);

– расширенные списки доступа (проверяют адрес отправителя, адрес получателя и другие параметры пакета);

– динамические расширенные списки доступа.

Каждый вид ACL необходимо размещать там, где он будет наиболее эффективно отрабатывать.

– стандартный ACL размещают как можно ближе к адресату;

– расширенный ACL размещают как можно ближе к источнику блокируемого трафика.

Создание стандартного списка доступа:

access-list 1 deny 192.168.1.0 0.0.0.255

access-list 1 permit 192.168.0.0 0.0.255.255

Разрешается прохождение пакетов с адресов в блоке 192.168.0.0/16 за исключением адресов 192.168.1.0/24.Часто используемое описание фильтра, ко-

торому удовлетворяет любой адрес 0.0.0.0 255.255.255.255 имеет специальное обозначение «any».

access-list *access-list-number* **{deny | permit} any**

Создание расширенного списка доступа

Критерии расширенного списка доступа записываются в следующем формате:

access-list *access-list-number* **{deny | permit}** *protocol source [source-wildcard]* **[operastor** *operand*] [**port** *port-number or name*] *destination [destination-wildcard]* **[operastor** *operand*] [**port** *port-number or name*] **[established] [log]**

access-list *access-list-number* **{deny | permit}** *protocol* **any any**

access-list *access-list-number* **{deny | permit}** *protocol host source host destination*

Ключевое слово «log» вызывает выдачу записи о совпадении пакета с данным критерием на консоль и в системный лог-файл.

Если в качестве протокола указано «tcp» или «udp», то описания source- и destination-wildcard могут включать номера портов для данных протоколов с ключевыми словами «eq», «lt», «gt», «range». Для протокола «tcp», возможно также применение слова «established» для выделения только установленных tcp-сессий.

Ключевое слово «host source» – эквивалентно записи: «source 0.0.0.0»

Создание стандартного именованного списка доступа.

Шаг 1. Задание имени и переход в режим формирования списка:

*Router(config)#**ip access-list standard** name*

Шаг 2. Задание критериев в порядке, в котором они должны применяться в списке:

*Router(config-std-nacl)#**deny** {source [source-wildcard]| **any**}*

или

*Router(config-std-nacl)#**permit** {source [source-wildcard]| **any**}*

Шаг 3. Выход из режима формирования списка:

*Router(config-std-nacl)#**exit***

Расширенный именованный список доступа создается аналогично.

В режиме конфигурировании терминальной линии выполните команду:

access-class** access-list-number **{in | out}

В режиме конфигурирования интерфейса выполните команду:

ip access-group** {access-list-number | name} **{in | out}

Примеры расширенных списков доступа.

Первый критерий разрешает любые входящие TCP-соединения на порты с номерами больше 1023. Второй критерий разрешает входящие SMTP-соединения на адрес 128.88.1.2. Следующий критерий разрешает прохождение ICMP-сообщений.

Все остальные пакеты, входящие с интерфейса Ethernet0, будут *отброшены.*

!

access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 gt 1023

access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25

```
access-list 102 permit icmp 0.0.0.0 255.255.255.255 128.88.0.0 255.255.255.255
!
interface ethernet 0
ip access-group 102 in
!
```

Контрольные вопросы

1 Создание именованных списков доступа.
2 Создание расширенного списка доступа.
3 Назначение списка доступа на интерфейс.
4 Списки доступа для протокола IP.

19 Лабораторная работа № 19. Протокол TFTP

Цель работы: ознакомиться с возможностью передачи файлов по протоколу TFTP.

Основные теоретические положения

Протокол telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленной ЭВМ. В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Приложения, которым не требуются все возможности FTP, могут использовать другой, более экономичный протокол – простейший протокол пересылки файлов TFTP (Trivial File Transfer Protocol). Этот протокол реализует только передачу файлов, причем в качестве транспорта используется более простой, чем TCP, протокол без установления соединения – UDP. В силу своей простоты протокол tftp используется не только для передачи файлов, но и для загрузки X-терминалов, процедура загрузки которых предполагает использование протоколов RARP, TFTP и BOOTP. Администраторам сети часто приходится сохранять файлы конфигурации, системное программное обеспечение (IOS) или восстанавливать их на коммуникационное оборудование. Возможно два способа копирования образа IOS во флеш-память: через консоль по протоколу Xmodem или через порт Ethernet по протоколу TFTP. Первый способ характеризуется огромным временем выполнения операции (часы). Второй способ предполагает наличие TFTP-сервера. Встроенная поддержка TCP/IP MS Windows позволяет использовать протокол TFTP в цифровых сетях для передачи файлов между устройствами. Созданный в процессе лабораторной работы некоторый файл конфигурации может быть сохранен студентами на TFTP-серверы для последующего анализа или повторного использования.

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Контрольные вопросы

1 Для чего предназначен FTP-протокол и как происходит в нем обмен данными?

2 Опишите простейшую модель работы протокола FTP.

3 Опишите алгоритм работы протокола FTP.

4 Опишите алгоритм работы при соединении двух FTP-серверов.

5 Опишите схему организации передачи данных между двумя FTP-серверами.

6 В каких случаях FTP-сервер должен самостоятельно закрыть канал передачи данных?

7 Опишите команды FTP для управления доступом к системе.

8 Опишите команды FTP для управления потоком данных.

9 Опишите команды FTP-сервиса.

20 Лабораторная работа № 20. WIFI

Цель работы: настроить беспроводной доступ доверенных конечных устройств в локальную сеть.

Порядок выполнения работы

Рассмотрим схему на рисунке 20.1.

Рисунок 20.1 – Пример для организации WiFi роутера

Рассмотрим пример WiFi роутера (см. рисунок 20.1):

1 На интерфейсе Router3 настройте IP-адрес 210.210. 0.1.

2 Настроим WiFi Router1.

2.1 Во вкладке GUI настроем IP-адрес, используя Static IP 210.210.0.2, 255.255.255.255.252, маршрутом будет 210.210.0.1.

2.2 Во вкладке Wireless можно выбрать настройки WiFi.

2.3 Во вкладке Wireless Security можно выбрать режим, выбрать режим шифрования и задать ключевое слово.

3 Настроим ноутбук. Wireless, вкладка Desktop, вкладка Connect, где видим доступные сети. Подключитесь к созданному нами WiFi и введите пароль. На рисунке 20.1 видно, что подключение успешное (пунктирная линия). Проверьте выход в интернет.

4 В настройках компьютера проверьте IP-адрес, выход в интернет и доступность ноутбука.

Рассмотрим пример WiFi точки доступа (рисунок 20.2).

1 Настройте порты на коммутаторе Switch0 в соответствующие VLAN.

2 На Router1 настройте интерфейс на подключение к интернет провайдеру, настройте sub-интерфейсы, которые соответствуют VLAN 2 и 3, настройте NAT.

3 Проверьте сеть.

4 Настроим точку доступа, вкладка Config, вкладка Port 1, задайте идентификатор сети, тип аутентификации и задайте пароль.

5 Пусть WiFi сегмент будет во VLAN 4. Создайте VLAN 4 и настройте интерфейс в Switch0.

6 Создайте sub-интерфейсы на Router1 и добавьте IP-адрес 192.168.4.1 255.255.255.0.

7 Настроим раздачу IP-адресов пользователям на Router1.

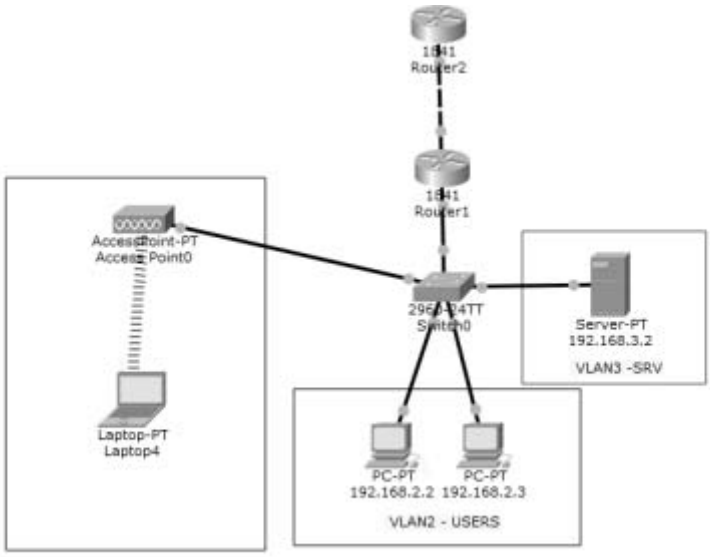

Рисунок 20.2 – Пример для организации WiFi точки доступа

7.1 Создадим ip dhcp pool WiFi-pool, network 192.168.4.0. 255.255.255.0, default router 192.168.4.1.

7.2 Необходимо исключить IP-адрес маршрутизатора из DHCP с помощью команды ip dhsp excluded-addresses 192.168.4.1; 61.

7.3 Настроим NAT, отредактировав созданный access list – ip accesslist standard FOR-NAT, permit 192.168.4.0 0.0.0.255.

7.4 В нашем случае fa0/1.4 определим как ip nat inside. Сохраните.

8 Настроим ноутбук аналогично предыдущей схеме (см. рисунок 20.2) и определим точку доступа в VLAN 4 на маршрутизаторе с помощью команд swichport mode access, switchport access vlan 4 description WiFi-AP. 9. Проверьте работоспособность сети.

Список литературы

1 **Кенин, А**. Самоучитель системного администратора / А. Кенин. – Санкт-Петербург : БХВ-Петербург, 2012. – 512 с.

2 Microsoft Windows Server 2012. Полное руководство / Р. Моримото [и др.]. – Москва : Вильямс, 2013. – 1456 с.

3 **Поляк-Брагинский, А**. Администрирование сети на примерах / А. Поляк-Брагинский. – Санкт-Петербург : БХВ-Петербург, 2012. – 432 с.

4 **Олифер, В. Г.** Компьютерные сети. Принципы, технологии, протоколы : учебное пособие / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – Санкт-Петербург : Питер, 2013. – 944 с. : ил.

5 **Новиков, В. А.** Информационные системы и сети : учебное пособие / В. А. Новиков, А. В. Новиков, В. В. Матвеенко. – Минск : Изд-во Гревцова, 2014. – 448 с.

6 **Бройдо, О. П.** Вычислительные системы, сети и телекоммуникации : учебник / О. П. Бройдо, В. Л. Бройдо, О. П. Ильина. – 4-е изд. – Санкт-Петербург : Питер, 2011. – 560 с.