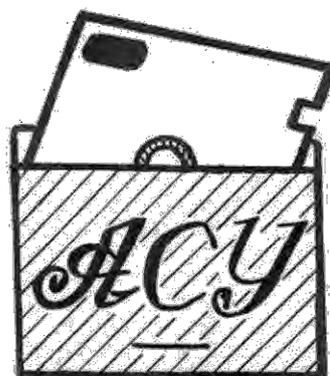


ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Автоматизированные системы управления»

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

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



Могилев 2018

УДК 004.7
ББК 32.973.202
С 33

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Автоматизированные системы управления»
«04» сентября 2018 г., протокол № 2

Составители: доц. А. И. Якимов;
ст. преподаватель В. Т. Садовский

Рецензент О. В. Леоненко

Методические рекомендации предназначены для студентов направлений
подготовки 09.03.04 «Программная инженерия» и 09.03.01 «Информатика и
вычислительная техника» дневной формы обучения.

Учебно-методическое издание

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Ответственный за выпуск	А. И. Якимов
Технический редактор	С. Н. Красовская
Компьютерная верстка	Е. С. Лустенкова

Подписано в печать . Формат 60×84/16. Бумага офсетная. Гарнитура Таймс.
Печать трафаретная. Усл. печ. л. . Уч.-изд. л. . Тираж 16 экз. Заказ №

Издатель и полиграфическое исполнение:
Государственное учреждение высшего профессионального образования
«Белорусско-Российский университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/156 от 24.01.2014.
Пр. Мира, 43, 212000, Могилев.

© ГУ ВПО «Белорусско-Российский
университет», 2018



Содержание

Введение.....	4
Лабораторная работа № 1. Изучение работы в качестве клиента в локальной сети.....	5
Лабораторная работа № 2. Проектирование локальной сети. Изучение протоколов доступа к среде передачи.....	7
Лабораторная работа № 3. Установка Windows Server.....	9
Лабораторная работа № 4 Планирование клиентов и групп в сетях Windows.....	12
Лабораторная работа № 5. Изучение протоколов доступа к среде передачи.....	15
Лабораторная работа № 6. Изучение протокола сетевого уровня IP.....	16
Лабораторная работа № 7. Изучение маршрутизации IP.....	19
Лабораторная работа № 8. Изучение сетевых утилит Windows.....	21
Лабораторная работа № 9. Изучение протоколов высших уровней.....	24
Лабораторная работа № 10. Изучение пользовательских протоколов.....	26
Лабораторная работа № 11. Изучение Web-технологий.....	28
Лабораторная работа № 12. Изучение технологий распределенных вычислений.....	30
Список литературы.....	32



Введение

Целями преподавания дисциплины «Сети и телекоммуникации» являются 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.

Даны методические рекомендации по выполнению лабораторных работ по дисциплине «Сети и телекоммуникации», а также приведены задания к ним и список литературы для подготовки.

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

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

Порядок выполнения работы

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

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты задания.
- 4 Выводы.

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.

Задание

- 1 Используя системную папку **Сетевое окружение**, составить список доступных ресурсов локальной сети университета.
- 2 Просмотреть список сетевых подключений вашего компьютера.
- 3 Составить список компонентов подключения к локальной сети и записать их конфигурационные параметры.
- 4 Загрузить виртуальную машину, используя указанный преподавателем образ, и выполнить настройку компонентов сетевых подключений для работы в Вашей сети.
- 5 Для проверки правильности настройки параметров сетевого подключения убедиться в том, что перечень ресурсов сети, доступных с виртуальной машины, совпадает с ранее составленным списком.
- 6 На виртуальной машине подключить сетевой принтер и сетевой диск.

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 2000/XP?
- 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?
- 10 Каковы основные угрозы при работе в сети? Каковы, по Вашему мнению, основные причины (мотивы), побуждающие злоумышленников осуществлять подобные действия?
- 11 Каковы основные правила (меры) безопасности при работе в сети?
- 12 Какие меры безопасности применяются в сети университета?

Лабораторная работа № 2. Проектирование локальной сети. Изучение протоколов доступа к среде передачи

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.

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.

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

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.

«Шина» (Bus). В этой топологии 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.

«Кольцо» (Ring). В данной топологии 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.

Активная топология «звезда» (Active Star). В этой топологии компьютеры клиенты-абоненты сети подключаются к более мощному центральному компьютеру. В такой конфигурации 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 проходящие 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) топологии**, 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).

Контрольные вопросы

- 1 В чем 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 Передача электрического сигнала требует наличия двух проводников. Какие именно проводники используются в коаксиальном кабеле?
- 9 Зачем в кабеле «витая пара» используется несколько пар проводников (2 или 4)?
- 10 Какой разъем используется для подключения кабеля «витая пара» к компьютерам?
- 11 Что может создать помехи работе беспроводной сети, если в ней используется радиосвязь? Что может создать помехи работе беспроводной сети, основанной на использовании инфракрасного излучения?
- 12 Какие Вы знаете разновидности архитектуры Ethernet? Чем они различаются?
- 13 Какие Вы знаете беспроводные сетевые технологии?



Лабораторная работа № 3. Установка Windows Server

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

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.

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

Основные теоретические положения

Операционные системы семейства Windows Server 2000/2003/2008 являются универсальной платформой, на которой реализованы почти 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»:

а) Active Directory – расширяемая и масштабируемая служба каталогов, в которой используется пространство имен, основанное на стандартной Интернет-службе именованного доменов (Domain Name System, DNS);

б) IntelliMirror – средства конфигурирования, поддерживающие зеркальное отображение пользовательских данных и параметров среды, а также центральное администрирование установки и обслуживания программного обеспечения;

в) Terminal Services – службы терминалов, обеспечивающие удаленный вход в систему и управление другими системами Windows Server;

г) 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.

Задание

1 Выполнить установку операционной системы Windows Server.

1.1 Запустить установку. Вариант 1: вставить в CD-дисковод установочный CD, загрузить компьютер с компакт-диска, выбрать нужную редакцию системы. Вариант 2: вставить в CD-дисковод установочный CD, автоматически загружается программа установки системы, выбрать пункт «Установить систему». Вариант 3: кнопка «Пуск» – «Выполнить» – «Обзор», найти и открыть папку i386 на дистрибутиве операционной системы, найти файл с именем winnt32.exe, запустить данный файл. Продолжить установку.

1.2 Установка в текстовом режиме.

1.2.1 Выбор действий. «Чтобы приступить к установке Windows», нажмите «Ввод».

1.2.2 Лицензионное соглашение. Нажмите клавишу F8 – «Принимаю лицензионное соглашение».

1.2.3 Разметка жесткого диска и выбор раздела для установки. Пример: Неразмеченная область – 14345 МБ. Нажать клавишу C – «Создать раздел» (или выбрать существующий). Создать раздел размером 5000 МБ. Нажать клавишу Ввод – «Установить». Выбрать «Форматировать раздел в системе NTFS (Быстрое)».

1.3 Установка в графическом режиме.

1.3.1 Язык и региональные стандарты: Язык ввода по умолчанию – Русский.

1.3.2 Имя: Организации;

1.3.3 Ключ продукта: Введите ключ для установки системы.

1.3.4 Имя компьютера и пароль администратора: Введите имя компьютера и пароль администратора сервера.

1.3.5 Настройка времени и даты: Установите нужную дату и время.

1.3.6 Установка поддержки сети.



1.3.7 Сетевые параметры: «Особые параметры» – Свойства TCP/IP – задайте параметры протокола TCP/IP.

1.3.8 Рабочая группа или домен. Оставьте по умолчанию рабочую группу WORKGROUP.

1.3.9 Завершающие действия по установке системы (настройка Главного меню, регистрация компонентов, сохранение настроек и т. д.).

1.4 Специфические моменты.

1.4.1 Драйверы устройств. В процессе установки могут потребоваться драйверы для устройств, для которых в БД драйверов системы нет соответствующего драйвера. Если Вы занимаетесь в группе под руководством преподавателя, то он предоставит все необходимые драйверы. Если Вы занимаетесь индивидуально, то сами позаботьтесь о необходимых драйверах для Ваших компьютеров.

1.4.2 Ввод сведений о пользователе. В полях «Пользователь» и «Организация» введите любую текстовую информацию.

1.4.3 Настройка сетевых подключений. Протокол TCP/IP. Значение IP-адреса и маски подсети необходимо взять из таблицы распределения IP-адресов и имен компьютеров – введите параметры того компьютера, который назначен для Вас преподавателем; значения остальных параметров протокола TCP/IP оставьте пустыми.

1.4.4 Выбор имени компьютера. Выберите имя компьютера из таблицы распределения IP – адресов и имен компьютеров – введите то имя, которое назначено для Вас преподавателем.

1.5 Завершение установки.

1.5.1 Региональные настройки. Завершить настройку региональных параметров.

1.5.2 Настройка стандартного профиля пользователя. Зарегистрируйтесь в системе с учетной записью администратора компьютера. Настройте следующие параметры профиля:

- вид рабочего стола;
- просмотр папок: показ полного пути, показ скрытых файлов и папок, показ содержимого системных папок, показ защищенных системных файлов, показ расширений файлов; показ сжатых и зашифрованных файлов другим цветом, отмена запоминания вида каждой отдельной папки;
- применить данный способ: просмотр для всех папок, свойства кнопки «Пуск» и «Главного меню» программ, нажав кнопку «Ок»;
- сделайте профиль администратора, профилем по умолчанию.

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?



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, а также настраивать параметры и свойства клиентов пользователей и компьютеров сети.

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.

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

Основные теоретические положения

При планировании доменной сети Windows необходимым условием является наличие контроллера домена на одном из серверов, в котором установлена и развернута роль Active Directory. Active Directory (AD – «Активный каталог») – служба 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, имеющих 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:

- первое – области действия группы (локальная доменная, глобальная или универсальная область действия);
- второе – 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 определяются в доменах посредством консоли Active Directory – пользователи и компьютеры (Active Directory Users and Computers).

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 для обозначения имен групп, рекомендуется использовать следующее правило: имена глобальных групп должны начинаться с буквы G, а локальных в домене, с букв DL. Весь процесс создание пользователей, включая их в группы можно описать следующим образом: **A > G > DL < P**. Это означает, что учётные записи поль-



зователей (**A**-Accounts), являются членами глобальной группы **G**, которая включается в локальную группу 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.

Задание

Создать подразделение типа OU в домене «**study.local**» подразделение «FIO_Company»; (FIO – Первые буквы ФИО студента).

В подразделении «FIO_Company» создать три подразделения:

- администрация – общий отдел – «OU_DirectGener»;
- бухгалтерия «OU_Buhgalter»;
- коммерческий Отдел - «OU_Commercial».

В каждом подразделении создать по два – три пользователя (согласовать с преподавателем).

Создать три глобальные группы безопасности исходя из данной структуры нашей организации SIV_Company: G_DirectGener, G_Buhgalter и G_Commercial.

Включить созданных пользователей в соответствующие группы.

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

С помощью локальных групп в домене будем разграничивать доступ к определенным ресурсам каждого подразделения.

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.

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?

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.

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.

Требования к отчету

- 1 Цель работы;
- 2 Постановка задачи;
- 3 Результаты исследования;
- 4 Выводы.

Основные теоретические положения

Стандарт 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 Херох разработала и реализовала в 1975 г. Метод доступа был опробован еще раньше: во второй половине 60-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 Херох совместно 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 протокол присутствует в Ethernet DIX и отсутствует в IEEE 802.3?
- 4 Какой метод разделения среды передачи данных используют все виды стандартов Ethernet (в том числе Fast Ethernet и Gigabit Ethernet)?
- 5 Дайте определение метода управления обменом CSMA/CD.
- 6 Что такое IPG (interpacket gap, межпакетная щель), BT (Bit Time, время бита), PDV (Path Delay Value, значение задержки в пути), Collision window (окно коллизий), Collision domain (область коллизий, зона конфликта, Slot time (время канала)?
- 7 Что такое minimum frame size, maximum frame size и чему они равны?
- 8 Что такое truncated binary exponential back off (усеченная двоичная экспоненциальная отсрочка) и как она вычисляется?
- 9 Опишите алгоритм доступа к сети в соответствии с методом CSMA/CD для одного из абонентов, имеющих данные (кадры) для передачи.
- 10 Что такое коллизия?
- 11 Кем практически обнаруживаются коллизии?
- 12 Какое соотношение должно выполняться для надежного распознавания коллизий?

Лабораторная работа № 6. Изучение протокола сетевого уровня IP

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

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.



Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

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 уровень (IP- протокол) 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 пятого по седьмой) находится множество протоколов прикладного уровня, выполняющих конкретные прикладные задачи.

IP – протокол, лежит в основе Интернета, его название так и расшифровывается: Internet Protocol.

В настоящее время используются следующие две версии протокола IP:

1) IPv6 – сравнительно новая (текущая версия спецификации опубликована в декабре 1998); IP-адрес имеет разрядность 128 бит и записывается в виде восьми шестнадцатитрибитных полей, с использованием цифр в шестнадцатеричной системе исчисления. Если в адресе имеется длинная последовательность нулей, то запись адреса можно сократить, вместо нулей пишется «:».

2) IPv4 – «классическая» (1981); IP-адрес имеет разрядность 32 бита и записывается в виде четырех десятичных чисел в диапазоне 0 ... 255 через точку, например: 192.0.2.34.

Каждый узел может напрямую связаться только с узлами своей сети (например: подключенными к одному из сегментов Ethernet). Компьютеры – узлы одной сети должны иметь единый адрес сети, который определяется с помощью маски сети. Связь с узлами других сетей осуществляется через промежуточные узлы – маршрутизаторы.

Посмотреть маршрут движения пакета IP 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, а TCP и UDP связывают два приложения на разных компьютерах в сети, используя для этого идентификаторы запущенных процессов – порты процессов.

Задания

1 Какие адреса из приведенного ниже списка являются допустимыми адресами хостов и почему:

0.10.10.10
 10.10.0.10
 10.10.10.10
 127.0.127.127
 127.0.127.0
 255.0.200.1
 1.255.0.0.

2 Укажите все допустимые маски. По какому принципу они получаются?

3 Определите диапазоны адресов подсетей (даны адрес хоста и маска подсети):

10.212.157.12/24
 27.31.12.254/31
 192.168.0.217/28
 10.7.14.14/16

4 Какие из ниже перечисленных адресов будут достигнуты напрямую с хоста 242.254.169.212/21:

241.253.169.212
 243.253.169.212
 242.252.169.212
 242.254.169.212
 242.253.170.212
 242.253.169.211

5 Определите диапазон адресов подсети этого хоста: 242.254.169.212/21.

С помощью команды ipconfig определите параметры IP на своем компьютере: IP-адрес, диапазон адресов, размер подсети. Объяснить, почему выбраны такие сетевые параметры и какие сетевые параметры выбрали бы Вы.

Напишите компьютерную программу со следующими функциями:

- чтение IP-адреса в точно десятичном формате и преобразование в 32-битовое число;
- обратное преобразование 32-битовых чисел в точное десятичное представление;
- определение к какому классу А, В, С, D, Е относится введенный IP-адрес;
- определение и отдельное отображение адреса сети и адреса хоста по введенному IP-адресу и маски сети (автоматическое определение корректности введенных значений);
- прямое и обратное преобразования из системы обозначений CIDR с косой чертой в эквивалентное точное десятичное представление;
- определение ограниченного и направленного, широковещательных адресов для введенных IP-адреса и маски подсети в данной подсети; (использовать адреса для «частного применения – частных LAN»)



Контрольные вопросы

- 1 Назначение и принцип работы сетевого уровня?
- 2 Какие требования предъявляются к сетевой адресации?
- 3 Можно ли использовать в качестве сетевого адреса MAC-адрес?
- 4 Что такое маска подсети?
- 5 Какова структура IP-адреса?
- 6 Чем определяется размер подсети?
- 7 Как определить диапазон адресов в подсети?
- 8 Как определить размер подсети?

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.

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.

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

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.

1 **НАЧАЛЬНЫЙ АДРЕС ПОДСЕТИ**, порядок достижения которого описывает правило.

2 **МАСКА ПОДСЕТИ**, которую описывает правило.

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

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

5 **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, согласно 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**.

Задания

1 С помощью программы route print посмотрите таблицу маршрутизации Вашего компьютера. Объясните все правила.

2 Посмотрите таблицу маршрутизации хоста, имеющего несколько каналов. Объясните все правила.

3 Посмотрите таблицу маршрутизации маршрутизатора. Объясните все правила.

4 Добавьте новое правило в таблицу маршрутизации для сети 192.168.0.0/24 через шлюз в Вашей сети с последним байтом в адресе 125 и

метрикой 12.

5 Удалите это правило.

6 В соответствии с таблицей и схемами выполните задание на распределение адресов по подсетям (согласно варианта). Постройте таблицы маршрутизации для всех шлюзов и для одного хоста для каждого сегмента.

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?

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.

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.

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

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 и



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 наиболее известные и часто применяемые системными администраторами утилиты командной строки. Сетевая операционная система Windows содержит набор утилит, полезных при диагностике, мониторинге сети и конфигурации узлов сети. Основными задачами этих программ являются:

- 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 Windows 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.

Задания

1 Используя утилиту **GETMAC**, получить MAC-адреса на локальном компьютере в формате CSV и удаленном (используя физическую рабочую станцию в классе или виртуальные машины), попробуйте разные ключи, сравните результаты.

2 С помощью утилиты IPCONFIG получите текущие настройки протокола TCP/IP на физических машинах учебного класса со статическими IP-адресами без сервера DHCP. Выполните команду IPCONFIG на виртуальных машинах с сервером DHCP, для этого необходимо:

- запустить сервер DHCP на виртуальной машине в среде ESXI (запускает



преподаватель);

- на виртуальном сервере удаляются учетные записи виртуальных рабочих станций;
- на физических машинах учебного класса запускаются виртуальные рабочие станции;
- на виртуальных рабочих станциях удаляются IP-адреса, маска и DNS, виртуальные машины перезапускаются;
- командой PING VirtMailSrvr (или PING 192.168.10.200) проверяется доступность сервера;
- и наконец, с помощью команды IPCONFIG получаем новые настройки;
- представить screenshot's.

3 Используя утилиту PING, определить пропускную способность сети к узлам с IP-адресами: 10.7.0.120, 10.219.0.1, 10.239.1.1 и 10.7.15.15. Объясните разницу в результатах.

4 С помощью утилиты PING определите максимальный размер пакетов MSS/MTU.

5 Примените утилиту PING с разными ключами.

6 Используя утилиту TRACERT и таблицу маршрутизации шлюза (используйте файл «APOS–LR#04–router2», а точнее адреса шлюзов), постройте схему сети университета.

7 Передайте пакеты участникам сети напрямую и через шлюз. Объясните полученные записи в таблице ARP.

8 Определите IP-адреса www.microsoft.com, www.hp.com, www.tut.by, ftp.cdrom.ru при помощи утилиты NSLOOKUP.

9 Повторить назначение, синтаксис утилиты ROUTE со всеми ключами (лабораторная работа № 10 «Изучение маршрутизации IP»). Применить данную команду на виртуальной и физической машинах. Добавить и удалить правило маршрутизации для виртуальной машины (IP-адрес согласовать с преподавателем).

10 Перечислить все вышеописанные утилиты, их назначение, привести примеры и скриншоты.

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 Каково 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.



Лабораторная работа № 9. Изучение протоколов высших уровней

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

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;

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

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: первая часть – цифра рассматривается как код класса сообщения; вторая часть – две последних цифры – 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 типов, 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.

Задания

Во всех заданиях адрес сервера: 10.203.0.201.

Где необходимо, требуется пояснить трехсимвольные коды ответов, например, при первом появлении такого кода.

В пятом и шестом заданиях, после аутентификации (если она необходима) рекомендуется в первую очередь вызвать помощь в командной строке `help` и посмотреть информацию о других командах, поддерживаемых данным протоколом.

1 Получить у преподавателя IP-адрес сервера электронной почты, имена и пароли пользователей. Отправить и получить почту без использования почтового клиента (для аутентификации использовать имя пользователя типа: `user№`, тогда паролем будет `№`, в качестве номера `№` использовать номер Вашей подгруппы и номер в журнале посещаемости).

2 Поработать с POP3 без аутентификации. Сделать соответствующие выводы.

3 Определить, является ли протокол FTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.

4 Подключиться к HTTP серверу и определить, является ли протокол HTTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.

5 Получить у преподавателя адрес и порт неизвестного для Вас протокола и сервера. Получите список его команд, объясните, что делает каждая команда; Попробовать некоторые из них и проанализировать результаты (использовать 1000-ый порт, при аутентификации имя пользователя и пароль: `admin`).

6 Поработайте с FTP-сервером с помощью TELNET и программы FTP. Объясните и подтвердите на конкретном примере разницу между ними (при аутентификации имя пользователя: `anonymous` и пароль: `any`), для запуска программы FTP в командной строке вызвать `ftp>open (узел) 10.203.0.201`).

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?

Лабораторная работа № 10. Изучение пользовательских протоколов

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

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.

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

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 или сетевом уровне, приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последу-



ющим возвращением трафика в надлежащий адрес.

В начале 1990 гг. перехват 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;
- локализовывать неисправность или ошибку конфигурации;
- обнаруживать паразитный, вирусный и закольцованный трафик, наличие которого увеличивает нагрузку сетевого оборудования и каналов связи;
- выявлять в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей;
- перехватывать 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.

Задание

1 Изучить интерфейс программы Wireshark (\\corp.mgkit.ru\dfs\work\wireshark).

2 Захватить 100 произвольных пакетов. Определить статистические данные:

- процентное соотношение трафика разных протоколов TCP/IP в сети;
- среднюю скорость кадров в секунду;
- среднюю скорость байт в секунду;
- минимальный, максимальный и средний размеры пакета;
- степень использования полосы пропускания канала (загрузка сети).

3 Выполнить анализ ARP-протокола.

4 На примере любого IP-пакета указать структуры протоколов Ethernet и IP, отметить поля заголовков и описать их.

5 Проанализировать и описать принцип работы утилиты PING.

При этом описать все протоколы, используемые утилитой. Составить диаграмму взаимодействия машин при работе утилиты PING.

Контрольные вопросы

- 1 Каковы основные цели мониторинга сетевого трафика?
- 2 Чем отличается мониторинг трафика от фильтрации?
- 3 Каково назначение 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?

Лабораторная работа № 11. Изучение Web-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.

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.

Требования к отчету

1 Цель работы.

2 Постановка задачи.

3 Результаты исследования.

4 Выводы.

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:

1) создаваемые на веб-сервере поставщика услуг Интернета;

2) создаваемые в интрасети как веб-узлы группы;

3) виртуальный веб-узел, создаваемый на жестком диске автономного компьютера, не подключенного к какой-либо сети.

Веб-документ – это веб-страница, содержащая описание структуры и содержания гипертекстового документа, создаваемого посредством команд, сформированных на языке HTML. Эти команды выполняются программой-браузером,



такими, например, как Microsoft Internet Explorer, Opera, Chrome и др.

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. 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 – JavaScript и VB Script. Поэтому для того чтобы создавать интерактивные веб-страницы, необходимо использовать язык HTML и один из приведенных языков программирования.

Структура HTML-документа. Документы HTML могут иметь различную структуру, включающую множество элементов, но все они должны содержать два таких элемента, как:

- раздел заголовка страницы – HEAD;
- 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 раздел 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.

Задание

- 1 Создайте HTML документы средствами Word.
- 2 Оформите каждый документ в соответствии с его содержанием и целью.
- 3 Создайте ссылки между главной страницей и остальными страницами.
- 4 Запустите созданные документы с помощью Internet Explorer.

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 (тэг) 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 создать внешнюю гиперссылку?

Лабораторная работа № 12. Изучение технологий распределенных вычислений

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

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.

Требования к отчету

- 1 Цель работы.
- 2 Постановка задачи.
- 3 Результаты исследования.
- 4 Выводы.

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 ограничено. При этом задачи, которые такая сеть решает, должны быть хорошо распараллеливаемыми. Иначе компьютеры 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`.

Контрольные вопросы

- 1 Что обозначает аббревиатура TCP?
- 2 К какому уровню модели OSI относится протокол TCP?
- 3 Назовите основные поля заголовка сообщения/пакета TCP.
- 4 Какое поле фиксирует идентификатор процесса, выполняемой задачи на удаленном сетевом ресурсе?
- 5 Принцип алгоритма «скользящего окна», его назначение и особенности.
- 6 Назовите единицу информации, с которой оперирует протокол TCP? (так на физическом уровне это бит, на канальном – кадр, на сетевом – пакет).
- 7 Какой модуль сетевого программного обеспечения протокола TCP является инициатором сеанса связи `TcpClient` или `TcpServer`?
- 8 Что такое порт в концепции протокола TCP?
- 9 Что такое сокет TCP и какие параметры являются обязательными при инициализации сокета TCP?

Задание

- 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.



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. Матвеев. – 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.

