ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Автоматизированные системы управления»

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Методические рекомендации к лабораторным работам для студентов направления подготовки 09.03.01 «Информатика и вычислительная техника» дневной формы обучения

Могилев 2017

УДК 004.7
ББК 32.973
С 33

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Автоматизированные системы управления» «07» февраля 2017 г., протокол № 9

Составитель канд. техн. наук, доц. И. А. Евсеенко

Рецензент канд. техн. наук, доц. И. В. Лесковец

Методические рекомендации предназначены к выполнению студентами лабораторных работ по темам согласно рабочей программе, содержат введение, краткие теоретические сведения, задания по вариантам, общие требования к отчету, список литературы.

Учебно-методическое издание

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Ответственный за выпуск	С. К. Крутолевич
Технический редактор	А. А. Подошевко
Компьютерная верстка	Н. П. Полевничая

Подписано в печать . Формат 60×84/16. Бумага офсетная. Гарнитура Таймс.
Печать трафаретная. Усл. печ. л. . Уч.-изд. л. . Тираж 56 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 г. Могилев

Содержание

Введение

Основной материал в приведенных методических рекомендациях посвящен операционным системам Microsoft Windows, технологии программирования Asp.net MVC5 с использованием языка программирования C#.

Целью методических рекомендаций является предоставление возможности самостоятельного освоения студентами основных методов функционального анализа, проектирования и эксплуатации компьютерных сетей, получения знаний, умений и навыков администрирования, а также изучения перспективных направлений в развитии современных сетевых технологий.

Целью дисциплины является изучение проблем проектирования и моделирования компьютерных сетей, классификации и применяемого оборудования в компьютерных сетях, выбора маски сети и назначения IP-адресов, основных стандартов в области инфокоммуникационных систем и технологий, теоретических основ архитектурной и системотехнической организации вычислительных сетей, построения сетевых протоколов, основ интернет-технологий.

При освоении данной дисциплины студент приобретает практические навыки работы с маршрутизаторами, создания клиент-серверных приложений, выбора и эксплуатации программно-аппаратных средств в создаваемых вычислительных системах и сетевых структурах, диагностирования и устранения неполадок в сетях, инсталлирования, тестирования, испытания и использования программно-аппаратных средств вычислительных и информационных систем, настройки конкретных конфигураций операционных систем, работы с различными операционными системами и их администрирования, конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств.

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

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

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.

Сетевые ОС можно разделить на *клиентские*, такие как Windows 8, 10 Professional, и *серверные*, например Windows Server 2016.

Основная функция клиентской сетевой ОС – предоставить пользователю удобный интерфейс для работы с сетевыми приложениями и службами, обеспечив при этом максимальную защиту компьютера и безопасность при доступе к данным и ресурсам. Серверы же выполняют сервисные функции, предоставляя свои данные и ресурсы для совместного использования, а также обслуживая различные клиентские запросы.

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.

Серверы, обеспечивающие работу в сети TCP/IP, или серверы сетевой инфраструктуры. К ним относятся DHCP-, DNS- и WINS-серверы; обычно настройку работы в крупной сети начинают именно с них.

DHCP-серверы нужны, чтобы по запросу *DHCP-клиента* (компьютера, у которого в настройках протокола TCP/IP включен режим автоматического получения IP-адреса) выдать ему такие параметры, как уникальный IP-адрес и маску подсети. Кроме них, клиент может получать от DHCP-сервера ряд дополнительных параметров, важных для взаимодействия с другими сетями и удобной работы в сети: адрес основного шлюза, адреса DNS- и WINS-серверов, название домена, в который входит этот компьютер, и некоторые другие.

DNS-серверы выполняют очень важную функцию *преобразования (разрешения) имен узлов (host names) в соответствующие им IP-адреса*. DNS (Domain Name System) расшифровывается как «система (служба) доменных имен». Служба DNS была реализована в Интернете в 1981 г., а с 2000 г. она стала основной службой преобразования имен в сетях Microsoft.

Серверы файлов (файл-серверы) нужны для хранения больших объемов данных и предоставления к ним доступа пользователей. Один файловый сервер может поддерживать одновременную работу сотен и даже тысяч пользователей. Чтобы обеспечить сохранность информации, файл-серверы, как правило, оснащены отказоустойчивыми наборами (массивами) жестких дисков и системами резервного копирования на магнитную

ленту или другой носитель.

Серверы приложений выполняют задачи обслуживания запросов пользователей на выборку или обработку какой-либо информации; их часто объединяют с **серверами баз данных**. Важно, что с серверами приложений и баз данных одновременно может работать большое число пользователей, причем выполнение клиентских запросов на специализированном многопроцессорном сервере производится намного быстрее, чем на компьютерах пользователей.

Серверы удаленного доступа и **серверы VPN** (Virtual Private Network – «виртуальная частная сеть») обеспечивают удаленное подключение к локальной сети по модему или через Интернет. Это дает пользователям возможность работать с ресурсами локальной сети предприятия, офиса или учебного заведения из дома или из любого места, где есть подключение к Интернету, например из Интернет-кафе.

Терминальные серверы предоставляют возможность работы с другими серверами через специальные программы – *терминальные клиенты*. С помощью этих программ администраторы, находясь вдалеке от локальной сети, оказываются как будто за консолью сервера и могут полностью управлять им, а пользователи могут удаленно работать с установленными на сервере приложениями.

Брандмауэры (межсетевые экраны) используются при подключении к Интернету для защиты внутренней сети от проникновения или атаки злоумышленников на корпоративные серверы. **Прокси-серверы (серверы-посредники)** выполняют функции контроля доступа пользователей в Интернет и кеширования часто запрашиваемых веб-страниц (что позволяет снизить расходы на пользование Интернетом). Поскольку оба этих сервера предназначены для установки на компьютер, связывающий локальную сеть с Интернетом, их часто объединяют в единую программно-аппаратную систему.

Серверы электронной почты (почтовые серверы, mail-серверы) обслуживают почтовые ящики пользователей в данной организации, обеспечивая подключения к ним *почтовых клиентов*, а также обрабатывают все входящие и исходящие сообщения. Их также можно использовать для ведения адресных книг, общих папок и систем электронного документооборота.

Веб- и FTP-серверы предоставляют для внешних (а часто – и для внутренних) пользователей доступ к веб- и FTP-ресурсам, размещенным в данной сети.

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, а затем «прозрачно» (без ввода имени и пароля) подключаться к другим компьютерам и работать с их ресурсами.

Рабочая группа – это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети. Принципиально важно, что каждый компьютер в рабочей группе *равноправен* (т. е. сеть получается одноранговой) и *поддерживает собственную локальную базу данных учетных записей пользователей* (*Security Accounts Manager*, *SAM*).

Отсюда вытекает основная проблема, которая не позволяет использовать рабочие группы в крупных корпоративных сетях. Для обеспечения «прозрачного» взаимодействия в рабочей группе нужно *создавать одинаковые учетные записи с одинаковыми паролями на всех компьютерах*, где работают пользователи и расположены ресурсы.

Понятно, что управлять учетными записями и ресурсами в рабочей группе можно только при небольшом количестве компьютеров и пользователей. В крупных сетях следует применять домены.

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

Домены создаются на основе сетевых ОС Windows, а база данных поддерживается *контроллерами домена*. Важным в доменах является то, что все компьютеры здесь не сами осуществляют проверку пользователей при входе, а передоверяют эту процедуру контроллерам. Такая организация доступа позволяет легко осуществить однократную проверку пользователя при входе в сеть, а затем уже без проверки предоставлять ему доступ к ресурсам всех компьютеров домена.

Задание

1 Используя системную папку Сетевое окружение, составьте список доступных ресурсов локальной сети университета.

2 Просмотрите список сетевых подключений компьютера.

3 Составьте список компонентов подключения к локальной сети и запишите их конфигурационные параметры.

4 Загрузите виртуальную машину, используя указанный преподавателем образ, и выполните настройку компонентов сетевых подключений для работы в сети.

5 Для проверки правильности настройки параметров сетевого подключения убедитесь в том, что перечень ресурсов сети, доступных с виртуальной машины, совпадает с ранее составленным списком.

6 На виртуальной машине подключите сетевой принтер и сетевой диск.

7 Установите две клиентские операционные системы Windows 10.

2 Лабораторная работа № 2. Проектирование локальной сети

***Цель работы*:** изучение основных видов, преимуществ и недостатков сетевых топологий, наиболее распространенных типов сетей, видов и методов доступа к среде передачи данных, сетевых архитектур.

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. По возможности, сеть по стоимости создания и сопровождения должна быть недорогой, но в то же время оставались возможности для ее дальнейшего расширения и для перехода к более высокоскоростным технологиям связи. При этом следует различать понятия *физической топологии*, т. е. способа размещения компьютеров, сетевого оборудования и их соединения с помощью кабельной инфраструктуры, и *логической топологии* – структуры взаимодействия компьютеров и характера распространения сигналов по сети. Существуют три базовые топологии, на основе которых строится большинство сетей.

«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.

Эта топология исключительно проста в реализации и дешева (требует меньше всего кабеля), однако имеет ряд существенных недостатков:

– такие сети трудно *расширять* (увеличивать число компьютеров в сети и количество *сегментов* – отдельных отрезков кабеля, их соединяющих);

– поскольку шина используется совместно, в каждый момент времени передачу может вести *только один из компьютеров*. Если передачу одновременно начинают два или больше компьютеров, возникает искажение сигнала (*столкновение*, или *коллизия*), приводящее к повреждению всех кадров. Тогда компьютеры вынуждены приостанавливать передачу, а затем по очереди ретранслировать данные. Влияние столкновений тем заметнее, чем выше объем передаваемой по сети информации и чем больше компьютеров подключено к шине;

– надежность сети с топологией «шина» невысока. Когда электрический сигнал достигает конца кабеля, он (если не приняты специальные меры) *отражается*, нарушая работу всего сегмента сети. Чтобы предотвратить такое отражение сигналов, на концах кабеля устанавливаются специальные *резисторы* (*терминаторы*), поглощающие сигналы. Если же в любом месте кабеля возникает обрыв (например, при нарушении целостности кабеля или просто при отсоединении коннектора), то

возникают два незатерминированных сегмента, на концах которых сигналы начинают отражаться, и вся сеть перестает работать.

«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*.

Преимущества сетей с топологией «кольцо»:

– поскольку у кабелей в этой сети нет свободных концов, терминаторы здесь не нужны;

– каждый из компьютеров выступает в роли *повторителя*, усиливая сигнал, что позволяет строить сети большой протяженности;

– из-за отсутствия *столкновений* топология обладает высокой устойчивостью к перегрузкам, обеспечивая эффективную работу с большими потоками передаваемой по сети информации.

Недостатки сетей с топологией «кольцо»:

– сигнал в «кольце» должен пройти последовательно (и только в одном направлении) через все компьютеры, каждый из которых проверяет, не ему ли адресована информация, поэтому время передачи может быть достаточно большим;

– подключение к сети нового компьютера часто требует ее остановки, что нарушает работу всех других компьютеров;

– выход из строя хотя бы одного из компьютеров или устройств нарушает работу всей сети;

– обрыв или короткое замыкание в любом из кабелей кольца делает работу всей сети невозможной;

– чтобы избежать остановки работы сети при отказе компьютеров или обрыве кабеля, прокладывают два кольца, что существенно удорожает сеть.

Активная топология «звезда» (Active Star). В такой конфигурации все потоки данных шли исключительно через центральный компьютер; он же полностью отвечал за управление информационным обменом между всеми участниками сети. Сейчас такие сети встречаются довольно редко. Гораздо более распространенной сегодня топологией является похожий вариант – **«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» (что и отражено в ее названии).

Несмотря на больший расход кабеля, характерный для сетей типа

«звезда», эта топология имеет существенные преимущества перед остальными, что и обусловило ее широчайшее применение в современных сетях.

Преимущества сетей типа «звезда-шина»:

– *надежность* – подключение к центральному концентратору и отключение компьютеров от него никак не отражается на работе остальной сети; обрывы кабеля влияют только на единичные компьютеры;

– *защищенность* – концентрация точек подключения в одном месте позволяет легко ограничить доступ к жизненно важным объектам сети;

– *легкость при обслуживании и устранении проблем* – все компьютеры и сетевые устройства подключаются к центральному соединительному устройству, что существенно упрощает обслуживание и ремонт сети.

При использовании вместо концентраторов более «интеллектуальных» сетевых устройств (*мостов, коммутаторов* и *маршрутизаторов*) получается «промежуточный» тип топологии между активной и пассивной звездой. В этом случае устройство связи не только ретранслирует поступающие сигналы, но и производит управление их обменом.

Реальные компьютерные сети постоянно расширяются и модернизируются. Поэтому почти всегда такая сеть является *гибридной*, т. е. ее топология представляет собой комбинацию нескольких базовых топологий. Легко представить себе гибридные топологии, являющиеся комбинацией «звезды» и «шины» либо «кольца» и «звезды».

Однако особо следует выделить **топологию «дерево»**, 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, топологии** в которой все либо многие компьютеры и другие устройства соединены друг с другом напрямую. Такая топология исключительно надежна – при обрыве любого канала передача данных не прекращается, поскольку возможно *несколько маршрутов доставки информации*. Сеточные топологии (чаще всего не полные, а частичные) используются там, где требуется обеспечить *максимальную отказоустойчивость* сети, например при объединении нескольких участков сети крупного предприятия. При этом существенно увеличивается расход кабеля, усложняется сетевое оборудование и его настройка.

Задание

Вам поручено установить сеть для небольшой, но развивающейся компании, занимающей половину этажа. В состав компании входят директор, управляющий, администратор и пять сотрудников. Планируется взять на работу еще двух сотрудников. У каждого сотрудника компании есть компьютер. Цветной лазерный принтер находится у администратора. У каждого сотрудника имеется отдельный монохромный лазерный принтер (рисунок 1).

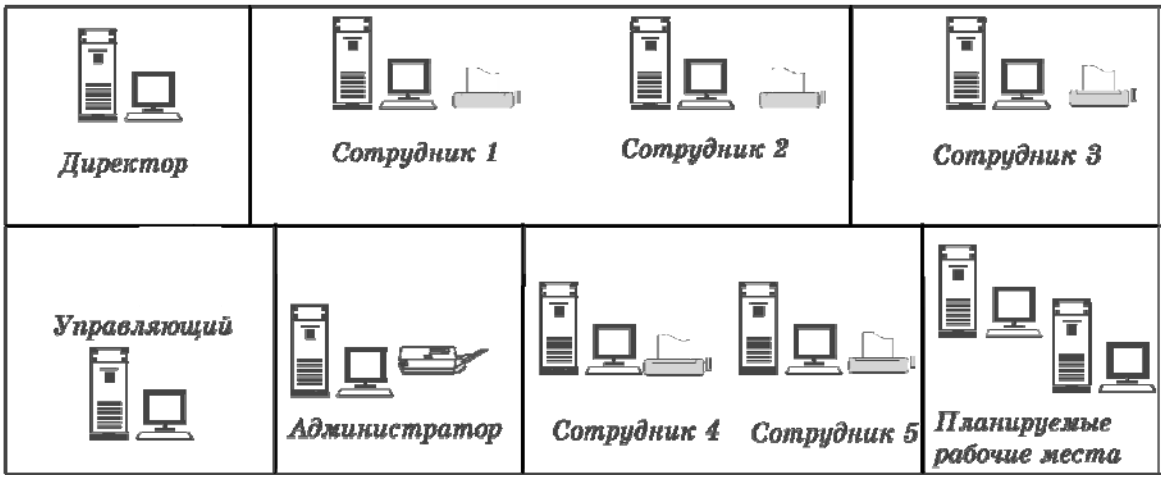


Рисунок 1 – Схема размещения рабочих мест

Предложите несколько вариантов топологии сети для этой компании, а также оцените суммарную длину кабеля, требуемого для прокладки сети, в каждом из предложенных вариантов и выберите из них наиболее оптимальный.

Составьте проект прокладки кабеля «витая пара» пятой категории в кабельных каналах согласно выбранной Вами топологии.

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.

Операционные системы семейства Windows Server 2003/2008/ 2012/2016 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». Перечислим эти роли: файловый сервер (сервер, предоставляющий доступ к файлам и управляющий им; выбор этой роли позволит быстро настроить параметры квотирования и индексирования); сервер печати (сервер, организующий доступ к сетевым принтерам и управляющий очередями печати и драйверами принтеров; выбор этой роли позволит быстро настроить параметры принтеров и драйверов); сервер приложений (сервер, на котором выпол-

няются Web-службы XML, Web-приложения и распределенные приложения; при назначении серверу этой роли на нем автоматически устанавливаются IIS, COM+ и Microsoft .NET Framework; при желании можно добавить к ним серверные расширения Microsoft FrontPage, а также включить или выключить ASP.NET); почтовый сервер (сервер, на котором работают основные почтовые службы POP3 (Post Office Protocol 3) и SMTP (Simple Mail Transfer Protocol), благодаря чему почтовые POP3-клиенты домена могут отправлять и получать электронную почту; выбрав эту роль, можно определить домен по умолчанию для обмена почтой и создать почтовые ящики); сервер терминалов (сервер, выполняющий задачи для клиентских компьютеров, которые работают в режиме терминальной службы; выбор этой роли приводит к установке служб терминалов, работающих в режиме сервера приложений); сервер удаленного доступа/сервер виртуальной частной сети (сервер, осуществляющий маршрутизацию сетевого трафика и управляющий телефонными соединениями и соединениями через виртуальные частные сети (virtual private network, VPN); эта роль позволяет запустить Мастер настройки сервера маршрутизации и удаленного доступа (Routing and Remote Access Server Setup Wizard); с помощью параметров маршрутизации и удаленного доступа можно разрешить только исходящие подключения, входящие и исходящие подключения или полностью запретить доступ извне); служба каталогов (контроллер домена Active Directory – сервер, на котором работают службы каталогов и располагается хранилище данных каталога; контроллеры домена также отвечают за вход в сеть и поиск в каталоге; при выборе этой роли на сервере будут установлены DNS и Active Directory); система доменных имен (сервер, на котором запущена служба DNS, разрешающая имена компьютеров в IP-адреса и наоборот; при выборе этой роли на сервере будет установлена DNS и запущен Мастер настройки DNS-сервера); сервер протокола динамической настройки узлов (сервер, на котором запущен служба DHCP (Dynamic Hose Configuration Protocol), позволяющая автоматизировать назначение IP-адресов узлам сети; при выборе этой роли на сервере будет установлена служба DHCP и запущен Мастер создания области); сервер Windows Internet Naming Service (сервер, на котором запущена служба WINS (Windows Internet Name Service), разрешающая имена NetBIOS в IP-адреса и наоборот; выбор этой роли приводит к установке службы WINS); сервер потокового мультимедиавещания (сервер, предоставляющий мультимедийные потоки другим системам сети или Интернета; выбор этой роли приводит к установке служб Windows Media; эта роль поддерживается только в версиях Standard Edition и Enterprise Edition).

Со способами решения административных задач теснейшим образом связана и архитектура системы безопасности Windows Server. Active Directory и административные шаблоны позволяют применять параметры

безопасности ко всем рабочим станциям и серверам компании. Иными словами, настраивается защита данных не каждого конкретного компьютера, а всего предприятия в целом.

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

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

2) определить предполагаемую нагрузку на сервер, исходя из выполняемых им ролей и количества пользователей, которые будут работать с сервером;

3) 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);

4) 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

Выполните установку операционной системы Windows Server 2016.

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

***Цель работы*:** изучение базовых понятий, настройки параметров протокола TCP/IP, процесса установки службы DNS, создания зон прямого просмотра, настройки параметров регистрации узлов на сервере DNS, приобретение навыков применения диагностических утилит для поиска неисправностей и неверных конфигураций протокола TCP/IP и службы DNS.

Физический адрес узла (MAC-адрес сетевого адаптера или порта маршрутизатора назначается производителями сетевого оборудования.

IP-адрес узла (например, 192.168.0.1) и символьное имя (например, www.microsoft.com) назначаются сетевыми администраторами или интернет-провайдерами.

Для более эффективного использования пространства адресов IP-сети с помощью маски подсети могут быть разбиты на более мелкие

подсети (subnetting) или объединены в более крупные сети (supernetting).

Рассмотрим на примере разбиение сети 192.168.1.0/24 (сеть класса C) на более мелкие подсети. В исходной сети в IP-адресе 24 бита относятся к идентификатору сети и 8 бит – к идентификатору узла. Используем маску подсети из 27 бит, или, в десятичном обозначении 255.255.255.224, в двоичном обозначении – 11111111 11111111 11111111 11100000. Получим следующее разбиение на подсети (таблица 1).

Таблица 1 – Пример разбиения на подсети

Подсеть	Диапазон IP-адресов	Широковещательный адрес в подсети
192.168.1.0/27	192.168.1.1–192.168.1.30	192.168.1.31
192.168.1.32/27	192.168.1.33–192.168.1.62	192.168.1.63
192.168.1.64/27	192.168.1.65–192.168.1.94	192.168.1.95
192.168.1.96/27	192.168.1.97–192.168.1.126	192.168.1.127
192.168.1.128/27	192.168.1.129–192.168.1.158	192.168.1.159
192.168.1.160/27	192.168.1.161–192.168.1.190	192.168.1.191
192.168.1.192/27	192.168.1.193–192.168.1.222	192.168.1.223
192.168.1.224/27	192.168.1.225–192.168.1.254	192.168.1.255

Таким образом, получено восемь подсетей, в каждой из которых может быть до 30 узлов. Идентификатор узла, состоящий из нулей, обозначает всю подсеть, а идентификатор узла, состоящий из одних единиц, означает широковещательный адрес (пакет, отправленный на такой адрес, будет доставлен всем узлам подсети).

Отметим очень важный момент. Узлы с такими IP-адресами, как 192.168.1.48/27 и 192.168.1.72/27, находятся в различных подсетях, и для взаимодействия данных узлов необходимы маршрутизаторы, пересылающие пакеты между подсетями 192.168.1.32/27 и 192.168.1.64/27.

Согласно стандартам протокола TCP/IP для данного примера не должно существовать подсетей 192.168.1.0/27 и 192.168.1.224/27 (т. е. первая и последняя подсети). На практике большинство операционных систем (в т. ч. системы семейства Microsoft Windows) и маршрутизаторов поддерживают работу с такими сетями.

Аналогично можно с помощью маски подсети объединить мелкие сети в более крупные.

Преимущества подсетей внутри частной сети: разбиение больших IP-сетей на подсети (subnetting) позволяет снизить объем широковещательного трафика (маршрутизаторы не пропускают широковещательные пакеты); объединение небольших сетей в более крупные сети (supernetting) дает возможность увеличить адресное пространство с помощью сетей более низкого класса; изменение топологии частной сети

не влияет на таблицы маршрутизации в сети Интернет (хранят только маршрут с общим номером сети); размер глобальных таблиц маршрутизации в сети Интернет не растет; администратор может создавать новые подсети без необходимости получения новых номеров сетей.

Задание

1 *Настройка параметров TCP/IP*. Значение IP-адреса и маски подсети необходимо взять из таблицы распределения IP-адресов и имен компьютеров.

2 *Проверка с помощью команды ping коммуникаций по IP-адресам*. Выполните команду ping в таких вариантах:

ping <IP-адрес Вашего компьютера>

ping <IP-адрес компьютера партнера в Вашем домене>

3 *Проверка с помощью команды ping коммуникаций по коротким именам компьютеров (NetBIOS-имена)*. Выполните команду ping в таких вариантах:

ping <имя Вашего компьютера>

ping <имя компьютера партнера в Вашем домене>

4 *Проверка с помощью команды ping коммуникаций по полным именам компьютеров (FQDN-имена)*. Выполните команду ping в таких вариантах:

ping <имя Вашего компьютера>

ping <имя компьютера партнера в Вашем домене>

5 *Установка службы DNS на сервере*. *Создание основной зоны прямого просмотра*. Данное задание выполняется на первом компьютере в Вашей паре.

6 *Настройка параметров TCP/IP для динамической регистрации узлов на сервере DNS*.

6.1 Откройте свойства протокола TCP/IP Вашего сервера.

6.2 Укажите в качестве «Предпочитаемого сервера DNS» IP-адрес первого сервера в Вашей паре.

6.3 Назначьте в качестве суффикса полного имени Вашего сервера имя назначенного Вашей паре домена.

6.4 Проверьте, что оба сервера в Вашей паре зарегистрировались в соответствующей зоне сервера DNS на первом сервере. Если серверы не зарегистрировались в процессе перезагрузки, сделайте принудительную регистрацию с помощью команды ipconfig /registerdns.

6.5 Проверьте, что на втором сервере произошла корректная передача зоны для Вашего домена. Если автоматическая передача зоны не произошла, то сделайте это вручную в консоли DNS (консоль DNS – выбрать Вашу зону, щелчок правой кнопки мыши – выбрать «Все задачи» – выбрать «Передать зону с основного сервера»).

7 *Проверка коммуникаций.*

7.1 Проверка с помощью команды ping коммуникаций по коротким именам компьютеров (NetBIOS-имена). Выполните команду ping в таких вариантах:

ping <имя Вашего компьютера>

ping <имя компьютера партнера в Вашем домене>

ping <имена компьютеров в других доменах>

Обратите внимание на результаты работы команды ping, когда Вы проверяете коммуникации в «своем» домене.

7.2 Проверка с помощью команды ping коммуникаций по полным именам компьютеров (FQDN-имена). Выполните команду ping в таких вариантах:

ping <имя Вашего компьютера>

ping <имя компьютера партнера в Вашем домене>

ping <имена компьютеров в других доменах>

8 *Диагностические утилиты для протокола TCP/IP: ipconfig, arp, ping, netstat, nbtstat, traced, pathping*. Изучите результаты работы следующих команд.

8.1 Команда *ipconfig*. Выполните команду ipconfig с параметрами:

/flushdns; /registerdns; /displaydns/

8.2 Команда *arp*. Выполните команду arp с параметром: *-a*.

8.3 Команда *ping*. Выполните команду ping с параметрами:

-t; -a; -n count;-l size;-w timeout.

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

***Цель работы*:** изучение способов и протоколов доступа к среде передачи.

С сетевой топологией тесно связано понятие *способа доступа к среде передачи*, под которым понимается набор правил, определяющих, как именно компьютеры должны отправлять и принимать данные по сети.

Основные способы доступа к среде передачи:

– множественный доступ с контролем несущей и обнаружением столкновений;

– множественный доступ с контролем несущей и предотвращением столкновений;

– передача маркера.

При **множественном доступе с контролем несущей и обнаружением столкновений** (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) все компьютеры (*множественный доступ*) «слушают» кабель (*контроль несущей*), чтобы определить, передаются по

нему данные или нет. Если кабель свободен, любой компьютер может начать передачу; тогда все остальные компьютеры должны ждать, пока кабель не освободится. Если компьютеры начали передачу одновременно и возникло столкновение, все они приостанавливают передачу (*обнаружение столкновений*), каждый – на разные промежутки времени, после чего ретранслируют данные.

Серьезным недостатком этого способа доступа является то, что при большом количестве компьютеров и высокой нагрузке на сеть число столкновений возрастает, а пропускная способность падает, иногда очень существенно.

Однако этот метод очень прост в технической реализации, поэтому именно он используется в наиболее популярной сегодня *технологии Ethernet*. А чтобы уменьшить количество столкновений, в современных сетях применяются такие устройства, как мосты, коммутаторы и маршрутизаторы.

Метод **множественного доступа с контролем несущей и предотвращением столкновений** (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) отличается от предыдущего тем, что перед передачей данных компьютер посылает в сеть специальный небольшой пакет, сообщая остальным компьютерам о своем намерении начать трансляцию. Так, другие компьютеры «узнают» о готовящейся передаче, что позволяет избежать столкновений. Конечно, эти уведомления увеличивают общую нагрузку на сеть и снижают ее пропускную способность (из-за чего метод CSMA/CA работает медленнее, чем CSMA/CD), однако они, безусловно, необходимы для работы, например, беспроводных сетей.

В сетях **с передачей маркера** (Token Passing) от одного компьютера к другому по кольцу постоянно курсирует небольшой блок данных, называемый *маркером*. Если у компьютера, получившего маркер, нет информации для передачи, он просто пересылает его следующему компьютеру. Если же такая информация имеется, компьютер «*захватывает*» *маркер*, дополняет его данными и отсылает все это следующему компьютеру по кругу. Такой информационный пакет передается от компьютера к компьютеру, пока не достигает станции назначения. Поскольку в момент передачи данных маркер в сети отсутствует, другие компьютеры уже не могут ничего передавать. Поэтому в сетях с передачей маркера невозможны ни столкновения, ни временные задержки, что делает их весьма привлекательными для использования в системах автоматизации работы предприятий.

При выборе компьютерной сети следует учитывать:

– уже имеющуюся кабельную систему и оборудование – есть ли в Вашем доме, школе, офисе сеть, которую нужно просто расширить, или у Вас имеются только отдельные компьютеры;

– физическое месторасположение – важно учитывать, как расположены компьютеры и где Вы собираетесь разместить сетевое оборудование. Объединить компьютеры в одной комнате довольно просто, однако если Ваши компьютеры располагаются на разных этажах здания или даже в нескольких зданиях, наилучшую конфигурацию сети и ее топологию следует тщательно продумать;

– размеры планируемой сети – если у Вас имеется лишь несколько компьютеров, структура сети будет довольно простой; если же компьютеров сотни или тысячи, то, скорее всего, придется остановить свой выбор на сложной гибридной топологии;

– объем и тип информации для совместного использования – эти параметры должны обязательно учитываться при выборе типа сети: если между компьютерами передаются большие файлы – музыкальные, видео- или графические, то Вам потребуется высокоскоростная сеть, позволяющая быстро и без задержек передавать такие объемы информации.

Подавляющее большинство современных сетей используют топологию «звезда» или гибридную топологию, представляющую собой объединение нескольких «звезд» (например, топологию типа «дерево»), и метод доступа к среде передачи CSMA/CD (множественный доступ с контролем несущей и обнаружением столкновений).

Задание

Спроектируйте (в виде структурной схемы) сеть крупной фирмы, состоящей из трех подразделений:

– офис администрации (отдельный этаж здания в центре Минска, десять рабочих мест) (см. рисунок 1);

– склад (отдельное здание за пределами МКАД), оснащен пятью стационарными рабочими станциями;

– торговый центр (рынок стройматериалов большой площади плюс автостоянки для покупателей), персонал которого при работе с клиентами использует КПК, свободно перемещаясь по территории торгового центра и стоянок на расстояния до 1,5–2 км.

При этом в пределах офиса и склада подсети должны иметь звездообразную структуру, для офиса администрации необходимо обеспечить возможность выхода в Интернет по каналу ADSL, а связь между подразделениями фирмы осуществляется при помощи оптоволоконного кабеля. Считать определяющими параметры скорости и надежности работы сети, пренебрегая ее стоимостью.

6 Лабораторная работа № 6. Изучение протокола IP

***Цель работы*:** изучение правил адресации сетевого уровня, получение навыков распределять адреса между узлами сети передачи данных.

Архитектуру сетевого уровня удобно рассматривать на примере сетевого протокола IP – самого распространенного в настоящее время, основного протокола сети Интернет. Термин «стек протоколов TCP/IP» означает «набор протоколов, связанных с IP и TCP (протоколом транспортного уровня)».

IP-протокол создан для использования в объединенных системах компьютерных коммуникационных сетей с коммутацией пакетов. Протокол IP обеспечивает передачу блоков данных, называемых датаграммами, от отправителя к получателям, где отправители и получатели являются узлами, идентифицируемыми адресами фиксированной длины. IP-протокол обеспечивает при необходимости также фрагментацию и сборку датаграмм для передачи данных через сети с малым размером пакетов.

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом маршрутизаторами (шлюзами) отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети.

В технологии TCP/IP сетевой адрес называют IP-адрес.

Таким образом, адрес получателя должен содержать в себе:

– номер (адрес) подсети;

– номер (адрес) участника (хоста) внутри подсети.

IP-адреса представляют собой 32-разрядные двоичные числа. Для удобства их записывают в виде четырех десятичных чисел, разделенных точками. Каждое число является десятичным эквивалентом соответствующего байта адреса.

192.168.200.47 является десятичным эквивалентом двоичного адреса

11000000.10101000.11001000.00101111 (точки оставлены для удобства).

Пример перевода чисел из двоичной системы в десятичную представлен в таблице 2.

IP-адрес содержит информацию адреса подсети и адреса узла в ней.

Запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла, но необходимость в этом несомненно есть. Для решения этой проблемы используются несколько вариантов.

Таблица 2 – Перевод чисел из двоичной системы счисления в десятичную и обратно

Двоичная система	Десятичная система
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Первоначально использовался простой способ, а именно: адрес фиксированно, жестко разбивался на две части (RFC 760). Очевидно, что такой жесткий подход не позволяет дифференцированно удовлетворять потребности отдельных предприятий и организаций. Он не нашел широкого применения.

Второй подход заключается в использовании классов адресов (RFC 791). Вводится пять классов адресов: A, B, C, D, E. Три из них – A, B и C – используются для адресации сетей, а два – D и E – имеют специальное назначение. Для каждого класса сетевых адресов определено собственное положение границы между номером сети и номером узла.

Третий способ (RFC 950, RFC 1518) основан на использовании маски, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла. При таком подходе адресное пространство можно использовать для создания множества сетей разного размера. Для этих целей, наряду с IP-адресом, введено такое понятие, как маска.

Практический интерес представляют два последних способа построения адреса IP.

Признаком, на основании которого IP-адрес относится к тому или иному классу, являются значения нескольких первых битов адреса (таблица 3).

Таблица 3 – Классы номеров IP

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0 (0 – не используется)	126.0.0.0 (127 – зарезервирован)	Поле 3 байта
B	10	128.0.0.0	191.255.0.0	Поле 2 байта
C	110	192.0.0.0	223.255.255.0	Поле 1 байт
D	1110	224.0.0.0	239.255.255.255	Групповые адреса
E	11110	240.0.0.0	247.255.255.255	Зарезервировано

Адреса класса A назначаются узлам очень большой сети. Старший бит в адресах этого класса всегда равен нулю. Следующие 7 бит первого октета представляют идентификатор сети. Оставшиеся 24 бита (три октета) содержат идентификатор узла. Адреса сетей могут принимать значения от 1 (00000001) до 126 (01111110). Из-за ограничений значение 0 (00000000) первого байта не используется, а значение 127 (01111111) зарезервировано для «внутренней петли».

К классу B относятся все адреса, старшие два бита которых имеют значение 10. В адресах класса B под номер сети и под номер узла отводится по два байта. Сети, значения первых двух байтов адресов которых находятся в диапазоне от 128.0. (1000000000000000) до 191.255 (10111111 11111111), называются сетями класса B. Ясно, что сетей класса B больше, чем сетей класса A, а размеры их меньше. Максимальное количество узлов в сетях класса B составляет 216 = (65 536).

К классу C относятся все адреса, старшие три бита которых имеют значение 110. В адресах класса C под номер сети отводится 3 байта, а под номер узла 1 байт. Сети, старшие три байта которых находятся в диапазоне от 192.0.0 (11000000 00000000 00000000) до 223.255 (11011111 11111111 11111111), называются сетями класса C. Сети класса C наиболее распространены и имеют наименьшее максимальное число узлов – 2^8 степени (256).

Определение диапазона адресов подсети можно произвести из определения понятия маски:

– те разряды, которые относятся к адресу подсети, у всех хостов подсети должны быть одинаковы;

– адреса хостов в подсети могут быть любыми.

То есть, если адрес 192.168.200.47 и маска равна /20, то диапазон можно посчитать как

11000000.10101000.11001000.00101111 – адрес;

11111111.11111111.11110000.00000000 – маска;

11000000.10101000.1100XXXX.XXXXXXXX – диапазон адресов, где 0, 1 – определенные значения разрядов, X – любое значение,

что приводит к диапазону адресов

от 11000000.10101000.11000000.00000000 (192.168.192.0)

до 11000000.10101000.11001111.11111111 (192.168.207.255)

Следует учитывать, что некоторые адреса являются запрещенными или служебными и их нельзя использовать для адресов хостов или подсетей. Это адреса, содержащие:

0 в первом или последнем байте;

255 в любом байте (это широковещательные адреса);

127 в первом байте (внутренняя петля – этот адрес имеется в каждом хосте и служит для связывания компонентов сетевого уровня).

Поэтому доступный диапазон адресов будет несколько меньше.

Диапазон адресов:

10.X.X.X – для огромных локальных сетей;

172.16.X.X – для больших локальных сетей;

192.168.X.X – для маленьких (небольших) локальных сетей, не может быть использован в сети Интернет, т. к. отдан для использования в сетях непосредственно не подключенных к глобальной сети.

Для небольшой автономной IP-сети условие уникальности номеров сетей и узлов может быть выполнено силами сетевого администратора.

В этом случае в распоряжении администратора имеется все адресное пространство, т. к. совпадение IP-адресов в не связанных между собой сетях не вызовет никаких отрицательных последствий, администратор может выбирать адреса произвольным образом, соблюдая лишь синтаксические правила и учитывая ограничения на особые адреса.

Для того чтобы избежать совпадения с внешними адресами глобальной сети Интернет, в стандартах Интернета определено несколько так называемых частных адресов, рекомендуемых для автономного использования в частных (корпоративных) LAN :

- в классе A – сеть 10.0.0.0;
- в классе B – диапазон из 16 номеров сетей 172.16.0.0-172.31.0.0;
- в классе C – диапазон из 255 сетей 192.168.0.0-192.168.255.0.

Эти адреса, исключенные из множества централизованно распределяемых, составляют огромное адресное пространство, достаточное для нумерации узлов автономных сетей почти любых размеров. Следует отметить также, что частные адреса, как и при произвольном выборе адресов, в разных автономных сетях могут совпадать. В то же время использование частных адресов для адресации автономных сетей делает возможным корректное подключение их к Интернету. Применяемые при этом специальные технологии подключения исключают коллизии адресов.

Задание

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

0.10.10.10
10.0.10.10
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 Перечислите 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 адресов

241.253.169.212
243.253.169.212
242.252.169.212
242.254.169.212
242.253.168.212
242.253.170.212
242.253.169.211
242.253.169.213

будут достигнуты напрямую с хоста 242.254.169.212/21 ?

Определите диапазон адресов в его подсети.

5 Посмотрите параметры IP на своем компьютере с помощью команды ipconfig. Определите диапазон адресов и размер подсети, в которой Вы находитесь. Попробуйте объяснить, почему выбраны такие сетевые параметры и какие сетевые параметры выбрали бы Вы.

7 Лабораторная работа № 7. Изучение маршрутизации IP

***Цель работы*:** изучение правил адресации сетевого уровня, получение навыков распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети.

Сетевой узел (node) – любое сетевое устройство с протоколом TCP/IP; хост (host) – сетевой узел, не обладающий возможностями маршрутизации пакетов; маршрутизатор (router) – сетевой узел, обладающий возможностями маршрутизации пакетов.

Когда один узел IP-сети отправляет пакет другому узлу, в заголовке IP-пакета указываются IP-адрес узла отправителя и IP-адрес узла-получателя. Отправка пакета происходит следующим образом.

Узел-отправитель определяет, находится ли узел-получатель в той же самой IP-сети, что и отправитель (в локальной сети), или в другой IP-сети (в удаленной сети). Для этого узел-отправитель производит поразрядное логическое умножение своего IP-адреса на маску подсети, затем поразрядное логическое умножение IP-адреса узла получателя также на свою маску подсети. Если результаты совпадают, значит, оба узла находятся в одной подсети. Если результаты различны, то узлы находятся в разных подсетях.

Если оба сетевых узла расположены в одной IP-сети, то узел-отправитель сначала проверяет ARP-кеш на наличие в ARP-таблице MAC-адреса узла-получателя. Если нужная запись в таблице имеется, то дальше отправка пакетов производится напрямую узлу-получателю на канальном уровне. Если же в ARP-таблице нужной записи нет, то узел-отправитель посылает ARP-запрос для IP-адреса узла-получателя, ответ помещает в ARP-таблицу и после этого передача пакета также производится на канальном уровне (между сетевыми адаптерами компьютеров).

Если узел-отправитель и узел-получатель расположены в разных IP-сетях, то узел-отправитель посылает данный пакет сетевому узлу, который в конфигурации отправителя указан как «основной шлюз» (default gateway). Основной шлюз всегда находится в той же IP-сети, что и узел-отправитель, поэтому взаимодействие происходит на канальном уровне (после выполнения ARP-запроса). Основной шлюз – это маршрутизатор, который отвечает за отправку пакетов в другие подсети (либо напрямую, либо через другие маршрутизаторы).

Рассмотрим пример, изображенный на рисунке 2.

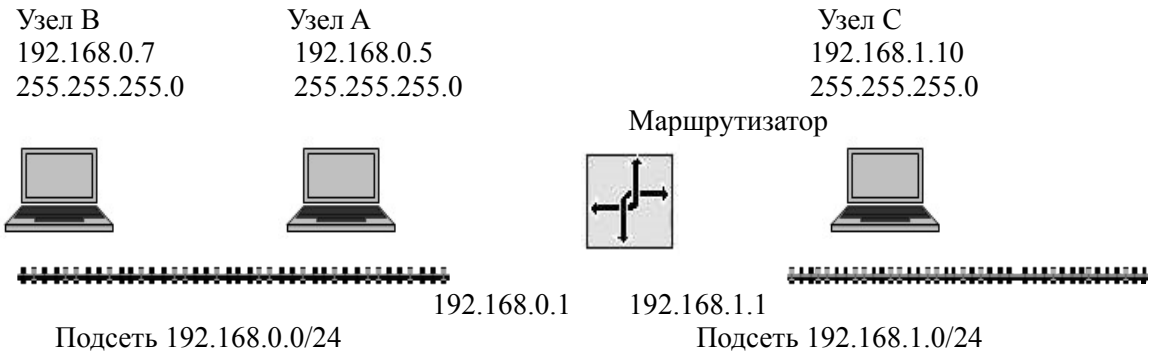


Рисунок 2 – Пример маршрутизации в сети

В данном примере две подсети: 192.168.0.0/24 и 192.168.1.0/24. Подсети объединены в одну сеть маршрутизатором. Интерфейс маршрутизатора в первой подсети имеет IP-адрес 192.168.0.1, во второй подсети – 192.168.1.1. В первой подсети имеются два узла: узел A (192.168.0.5) и узел B (192.168.0.7). Во второй подсети имеется узел C с IP-адресом 192.168.1.10.

Если узел A будет отправлять пакет узлу B, то сначала он вычислит, что узел B находится в той же подсети, что и узел A (т. е. в локальной подсети), затем узел A выполнит ARP-запрос для IP-адреса 192.168.0.7. После этого содержимое IP-пакета будет передано на канальный уровень, а информация будет передана сетевым адаптером узла A сетевому адаптеру узла B. Это пример прямой доставки данных (или прямой маршрутизации, direct delivery).

Если узел A будет отправлять пакет узлу C, то сначала он вычислит,

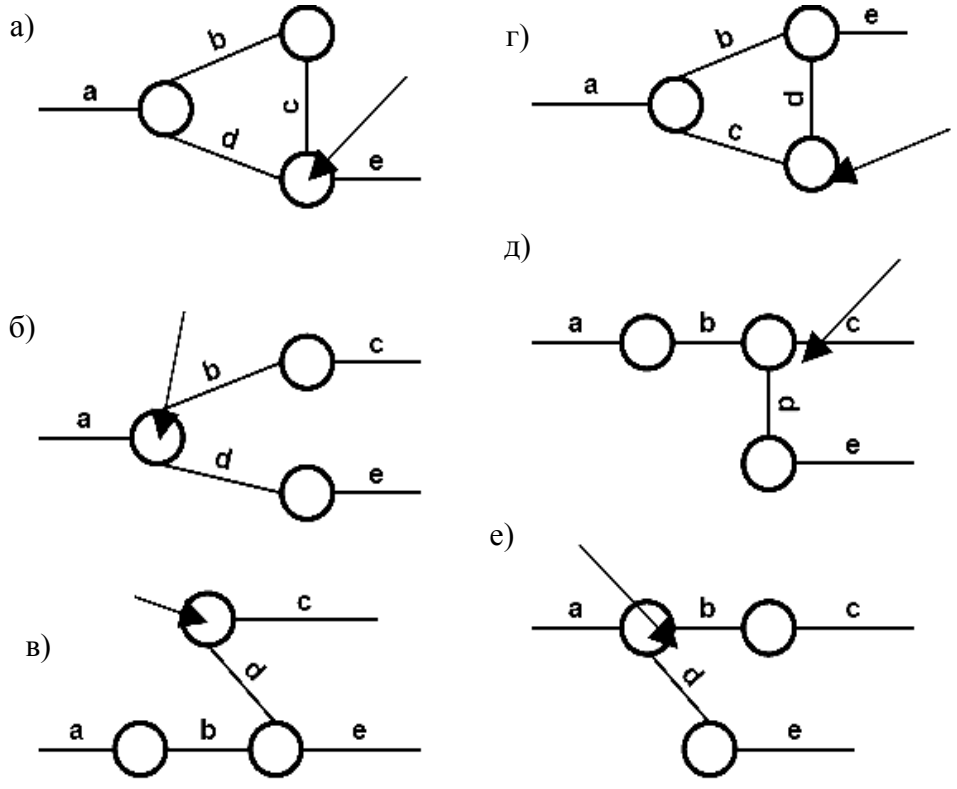
что узел С находится в другой подсети (т. е. в удаленной подсети). После этого узел А отправит пакет узлу, который в его конфигурации указан в качестве основного шлюза (в данном случае это интерфейс маршрутизатора с IP-адресом 192.168.0.1). Затем маршрутизатор с интерфейса 192.168.1.1 выполнит прямую доставку узлу С. Это пример непрямой доставки (или косвенной маршрутизации, indirect delivery) пакета от узла А узлу С. В данном случае процесс косвенной маршрутизации состоит из двух операций прямой маршрутизации.

В целом процесс IP-маршрутизации представляет собой серии отдельных операций прямой или косвенной маршрутизации пакетов.

Каждый сетевой узел принимает решение о маршрутизации пакета на основе таблицы маршрутизации, которая хранится в оперативной памяти данного узла. Таблицы маршрутизации существуют не только у маршрутизаторов с несколькими интерфейсами, но и у рабочих станций, подключаемых к сети через сетевой адаптер. Таблицу маршрутизации в системе Windows можно посмотреть по команде route print. Каждая таблица маршрутизации содержит набор записей. Записи могут формироваться различными способами.

Задание

В соответствии с таблицей 4 и схемами (рисунок 3) выполните задание на распределение адресов по подсетям (согласно варианту).



Стрелками показан шлюз по умолчанию

Рисунок 3 – Схемы разбиения на подсети (согласно варианту)

Таблица 4 – Исходные данные для разбиения на подсети

Номер варианта	Количество хостов в подсети					Диапазон адресов	
	A	B	C	D	E	от	до
1	5	10	20	15	50	10.0.20.0	10.0.20.255
2	20	15	6	70	25	192.168.0.0	192.168.0.255
3	15	25	5	40	5	112.38.25.128	112.38.25.255
4	24	32	8	10	2	196.13.49.0	196.13.49.128
5	50	16	64	20	15	68.76.115.0	68.76.115.255
6	40	6	10	12	5	211.3.45.0	211.3.45.128
7	5	10	20	15	50	10.0.20.0	10.0.20.255
8	16	12	8	60	20	92.190.0.0	92.190.0.255
9	16	12	8	60	20	92.190.0.0	92.190.0.255

8 Лабораторная работа № 8. Изучение сетевых утилит Windows

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

Любая операционная система имеет набор диагностических утилит для тестирования сетевых настроек и функционирования коммуникаций.

В таблице 5 перечислены утилиты командной строки, являющиеся инструментами первой необходимости для проверки настроек протокола TCP/IP и работы сетей и коммуникаций, а также указаны основные и наиболее часто используемые параметры этих команд и дано их краткое описание. Подробное описание данных утилит содержится в системе интерактивной помощи Windows.

Таблица 5 – Диагностические утилиты TCP/IP и DNS.

Название утилиты	Параметры	Комментарий
ipconfig	/? – отобразить справку по команде /all – отобразить полную информацию о настройке параметров всех адаптеров /release – освободить динамическую IP-конфигурацию /renew – обновить динамическую IP-конфигурацию с DHCP-сервера /flushdns – очистить кеш разрешений DNS /registerdns – обновить регистрацию на DNS-сервере	Служит для отображения всех текущих параметров сети TCP/IP и обновления параметров DHCP и DNS. При вызове команды ipconfig без параметров выводятся IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера

Окончание таблицы 5

Название утилиты	Параметры	Комментарий
arp	a – отображает текущие ARP-записи	Отображение и изменение ARP-таблиц
ping	Формат команды: «ping <сетевой узел> параметры» Параметры: t – бесконечная (до нажатия клавиш <Ctrl> + <Break>) отправка пакетов на указанный узел a – определение имени узла по IP-адресу n <число> – число отправляемых запросов l <размер> – размер буфера отправки w <тайм-аут> – тайм-аут ожидания каждого ответа в миллисекундах	Команда ping позволяет проверить: работоспособность IP-соединения; правильность настройки протокола TCP/IP на узле; работоспособность маршрутизаторов; доступность и работоспособность какого-либо сетевого ресурса
tracert	d – без разрешения IP-адресов в имена узлов h <макс число> – максимальное число прыжков при поиске узла w <тайм-аут> – тайм-аут каждого ответа в миллисекундах	Служебная программа для трассировки маршрутов, используемая для определения пути, по которому IP-дейтаграмма доставляется по месту назначения
pathping	n – без разрешения IP-адресов в имена узлов h макс число – максимальное число прыжков при поиске узла q <число_запросов> – число запросов при каждом прыжке w <тайм-аут> – тайм-аут каждого ответа в миллисекундах	Средство трассировки маршрута, сочетающее функции программ ping и tracert и обладающее дополнительными возможностями. Эта команда показывает степень потери пакетов на любом маршрутизаторе
netstat	a – отображение всех подключений и ожидающих (слушающих) портов n – отображение адресов и номеров портов в числовом формате o – отображение кода (ID) процесса каждого подключения r – отображение содержимого локальной таблицы маршрутов	Используется для отображения статистики протокола и текущих TCP/IP-соединений
nbtstat	n – выводит имена пространства имен NetBIOS, зарегистрированные локальными процессами c – отображает кеш имен NetBIOS (разрешение NetBIOS-имен в IP-адреса)	Средство диагностики разрешения имен NetBIOS

Задание

Примените все утилиты, представленные в таблице 5 с использованием различных параметров.

9 Лабораторная работа № 9. Изучение протоколов высших уровней

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

Большинство 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:

– информационное сообщение. Обычно игнорируется программными клиентами;

– удачное завершение запроса. Рассматривается программами-клиентами как успех обработки запроса и обычно игнорируется.

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

– сообщение об удачной обработке запроса, но требующее дополнительных действий клиента;

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

– 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.

Программа TELNET. Для работы с текстовыми протоколами воспользуемся программой TELNET, входящей в состав Windows. Эта программа предназначена для работы с протоколом TELNET, задачей которого является обмен информацией между клиентом и сервером без каких-либо преобразований, т. е. организация прозрачного канала между клиентом и сервером.

Протокол FTP (File Transfer Protocol) – протокол передачи файлов. Этот протокол содержит встроенные средства идентификации клиента. Все распознаваемые им команды состоят из трех или четырех символов, являющихся сокращениями или аббревиатурами выполняемых действий.

Протокол HTTP (Hyper Text Transfer Protocol) – протокол передачи

гипертекста, т. е. данных разного представления (текст, изображения, видео, звук). Обычно этот протокол работает на 80-м порту. Он содержит средства идентификации и перекодирования передаваемой информации.

Задание

1 Получите у преподавателя адрес сервера электронной почты, имена и пароли пользователей. Отправьте и получите почту без использования почтового клиента (для аутентификации использовать имя пользователя типа: user№, тогда паролем будет №, в качестве номера № использовать номер Вашей подгруппы).

2 Примените POP3 без аутентификации. Сделайте соответствующие выводы.

3 Определите, является ли протокол FTP текстоориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердите и объясните полученные результаты.

4 Подключитесь к HTTP-серверу и определите, является ли протокол HTTP текстоориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердите и объясните полученные результаты.

5 Получите у преподавателя адрес и порт неизвестного для Вас протокола и сервера. Получите список его команд, объясните, что делает каждая команда.

10 Лабораторная работа № 10. Изучение пользовательских протоколов

Цель работы: изучение принципов анализа сетевого трафика, получение умений использовать сетевой анализатор (сниффер) и оценивать сетевой трафик на примере протоколов ARP, IP и ICMP.

Sniffer – это сетевой анализатор трафика, программа или программно-аппаратное устройство для перехвата и последующего анализа либо только анализа сетевого трафика для других узлов.

Перехват трафика может осуществляться:

– 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);

– подключением сниффера в разрыв канала;

– 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 (второй) или сетевом (третий) уровне, приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

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.

Задание

Изучите интерфейс программы сниффер. Захватите 100 произвольных пакетов. Определите статистические данные: процентное соотношение трафика разных протоколов в сети; среднюю скорость кадров/с; среднюю скорость байт/с; минимальный, максимальный и средний размеры пакета; степень использования полосы пропускания канала (загрузку сети). Зафиксируйте 20 IP-пакетов. Определите статистические данные: процентное соотношение трафика разных протоколов стека tcp/ip в сети; средний, минимальный, максимальный размеры пакета. Выполните анализ ARP-протокола. На примере любого IP-пакета укажите структуры протоколов Ethernet и IP. Отметьте поля заголовков и опишите их.

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.

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 и звуковых эффектов. В этих файлах содержатся описания веб-страниц на одном из языков разметки гипертекста – HTML (HyperText Markup

Language) или XML (Extensible Markup Language). Они имеют одно из следующих расширений: html, htm, xml.

Родовые отношения обеспечивают удобство при просмотре содержимого веб-узла от общего к частному. Сетевые отношения создаются в тех случаях, когда целесообразно иметь возможность перехода с одних на другие страницы для получения справочной либо уточняющей информации.

Каждая веб-страница хранится в отдельном файле. Связь между веб-страницами (файлами), обеспечивающая быстрый переход с одной страницы на другую и эффективный поиск нужной информации, устанавливается с помощью гиперссылок.

Одна из страниц выполняет роль главной страницы. В ней должна содержаться информация о тематической направленности проекта, а также элементы, обеспечивающие навигацию по страницам и поиск нужной информации. Именно эта страница будет отображаться первой на экране посетителя. Так, если в адресную строку браузера ввести, например, DNS-адрес http://www.fa.ru, то на самом деле будет сформирован URL-адрес HTTP://www.fa.ru/index.htm и будет выполнена попытка найти и загрузить веб-страницу именно с таким URL-адресом.

Поэтому файл, в котором хранится первая веб-страница, с которой посетитель начнет движение по страницам узла, используя гиперссылки, должен иметь имя «index.htm».

Папка веб-узла внутри себя должна содержать еще одну папку. Эта папка служит для хранения файлов с графическими изображениями, которые предполагается отображать на веб-страницах.

Задание

1 Спроектируйте гипертекстовый документ, преобразовав текст задания Вашего варианта из линейной формы в гипертекстовую (сетевую) и постройте графическую модель (схему ссылок). Для этого:

– разделите текст на страницы;

– каждой странице присвойте имя файла;

– выделите ключевые слова связи страниц.

2 Предусмотрите в каждой странице ключевое слово возврата на главную страницу.

3 Создайте HTML документы средствами Word.

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

5 Создайте ссылки между главной страницей и остальными страницами. Запустите созданные документы с помощью Internet Explorer.

6 Создайте фреймовый HTML-документ с помощью тегов языка HTML.

12 Лабораторная работа № 12. Изучение технологий распределенных вычислений

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

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 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.

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.

13 Требования к отчетам и защите лабораторных работ

Лабораторная работа направляется на доработку, если количество ошибок и погрешностей позволяет отнести её к низкому уровню соответствия. Допустимые погрешности и ошибки при определении учебных достижений представлены в таблице 6.

Таблица 6 – Допустимые погрешности и ошибки при определении учебных достижений студентов

Шкала соответствия	Уровень соответствия	Балл	Количество ошибок, погрешности / несущественные / существенные
Соответствие	Высокий	5	3/2/0
	Средний	4	6/3/2
	Минимально необходимый	3	7/4/3
Несоответствие	Низкий	2	8/5/4

Погрешностями при определении учебных достижений считаются:

– неточные выражения в отчете по лабораторной работе;

– нерациональные, но правильные приемы, используемые для решения поставленных задач;

– незначительные погрешности при определении параметров.

К несущественным ошибкам относятся:

– неточности определения характеристик и параметров;

– неточности при проектировании сети;

– нерациональный способ решения задачи или план ответа (нарушение логики изложения материала, подмена основных понятий второстепенными);

– несоблюдение требований ГОСТа и небрежное оформление отчета по лабораторной работе и графического материала.

К существенным ошибкам относятся:

– подмена понятий в изложении основных понятий;

– незнание фундаментальных понятий вычислительных сетей;

– неумение администрировать и диагностировать вычислительные сети;

– неумение в ответе объяснить материал, делать выводы и обобщения, неумение письменно оформить материал;

– неумение применять теоретические знания для построения СКС;

– незнание логических и физических топологий вычислительных сетей;

– отсутствие необходимых математических моделей.

Оформление отчета по лабораторным работам должно соответствовать требованиям ГОСТ 2.105–95. Текстовая часть отчета выполняется либо чертежным шрифтом по ГОСТ 2304–81 с высотой букв не менее 5 мм либо машинным способом шрифтом Times с высотой букв 14 пунктов

через одинарный интервал.

Формулы, иллюстрации и таблицы нумеруются в пределах отчета. Обозначения переменных и параметров, принятых в формулах, должны быть расшифрованы сразу после написания формулы. При этом указываются единицы измерения переменных и параметров.

Рисунки, графики и таблицы сопровождаются наименованиями, отображающими их содержание (например, Рисунок 1 – Физическая топология компьютерной сети). Если на одном рисунке изображено несколько графиков различных процессов, то каждый график должен иметь отдельное обозначение, которое необходимо расшифровать в поясняющих данных к рисунку. Поясняющие данные помещаются под рисунком перед его наименованием.

Общие требования к содержанию отчета

1 Тема, цель работы.
2 Постановка задачи.
3 Вариант задания с исходными данными.
4 Выполненное задание согласно варианту: алгоритм решения поставленной задачи; листинг программы, реализующий данный алгоритм (в распечатанном виде); результаты выполненного задания.
5 Результаты тестирования задания.
6 Выводы по теме лабораторной работы.

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.