Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича

Лицей при СПбГУТ

А.В. Красов, Д.В. Кушнир

Основы построения сетей

методическое пособие по курсу

Санкт-Петербург
2001 г.

УДК 621.399

А.В. Красов, Д.В. Кушнир. Методическое пособие по курсу “Основы построения сетей”. СПб.: Лицей СПбГУТ 2001, - 59 с.

В пособии рассмотрены вопросы организации сетей. Материал излагается на основе курса фирмы Microsoft.

Пособие предназначено для школьников базовых школ университета, учащихся Лицея, поэтому из него исключены вопросы, связанные с видами модуляциями и другими техническими подробностями, для освоения которых требуется знания, выходящие за рамки школьной программы.

Пособие может быть полезно для всех тех, кто интересуется информатикой.

Сведения об авторах:

А.В. Красов - ведущий инженер-программист учебно-исследовательского центра информационных и телекоммуникационных технологий, ведущий преподаватель Лицея и Малого факультета СПбГУТ с 1989 г., автор комплекса учебно-методических пособий по курсу информатики, читаемого в СПбГУТ.

Д.В. Кушнир - доцент кафедры информационной безопасности телекоммуникационных систем.

Подробную информацию о наших разработках можно получить на:

http://fem.sut.ru/~Krasov или www.uicitt-sut.spb.ru/Krasov

Вопросы, предложения о контактах можно послать по адресу:

krasov@mail.wplus.net или krasov@fem.sut.ru

Пособие предназначено для учащихся базовых школ университета. Изложенный материал соответствует стандарту и учебному плану по данной дисциплине. Пособие представляет большую учебно-методическую ценность, поскольку данный раздел курса слабо освещен в специализированной литературе, предназначенной для школьников.

Рецензент - методист адмиралтейского района Н.И. Жиганова

Введение

Миллионы компьютеров во всем мире объединяются в сети. От самых простых локальных сетей маленьких фирм, школ, отдельных групп пользователей до единой глобальной сети Internet. Этот процесс стремительно развивается прямо на наших глазах и предоставляет качественно новые возможности. Поэтому знания в этой новой области крайне важны и актуальны. В качестве основной задачи начальной стадии образования президентом США Бил Клинтоном, ставится задача чтобы к 12 годам каждый американец свободно владел сетью Internet, на эти целевые установки ориентируются и большинство остальных прогрессивных стран мира, в том числе и наше государство. Наша страна заметно отстает в этой области, но возможность познакомиться с этой темой есть и у нас. Кроме того, в стандарт школьного образования включен целый раздел, посвященный сетям и сетевым технологиям, эти вопросы входят в перечень обязательного минимума для среднего образования.

Данная тема является крайне своевременной и необходимой, в связи с переходом от индустриального общества к информационному, в котором большая часть населения занята процессом обработки информации, а не материальным производством. Этот процесс невозможен без широкого использования сетевых ресурсов и современных средств телекоммуникации. По многим прогнозам к 2020 году сеть Internet вытеснит очень многие сегодняшние понятия не только почту, телевидение, газеты, но и как прогнозируют - правительство.

Уже сейчас на западе консультации по многим вопросам, в том числе и по медицинским проблемам, телеконференции, заключение контрактов проходит с использованием компьютерных сетей, и неважно, где расположен Ваш партнер, в соседней комнате или на противоположной стороне планеты. В настоящее время в западной системе образования широко используется получение различных учебных материалов по сетям, используется дистанционное обучение. Живое общение сразу многих пользователей открывает качественно новые возможности по организации конференций по сети Internet, в том числе с использованием видеоматериалов. Во многих странах широко применяются системы электронных платежей, позволяющие производить покупку товаров, не выходя из дома.

Тем самым сети, (и в первую очередь глобальная сеть Internet) становятся неотъемлемой частью нашей жизни, это справедливо не

только для людей, связанных с компьютерами, но для всех слоев общества.

1. Введение в компьютерные сети

1.1. Назначение и возможности

Сеть - в простейшем случае это объединение нескольких компьютеров (не менее двух), обменивающихся между собой информацией по каналу связи. Это позволяет передавать огромные объемы информации между пользователями сети. Этот процесс занимает во много раз меньшее количество времени, чем ручной способ передачи информации, совместно использовать некоторые ресурсы например принтеры и диски.

Локальная сеть - несколько компьютеров, соединенных между собой кабелем. Возможности - до 30 (100) компьютеров, максимальная длина соединительного кабеля до 180 м.

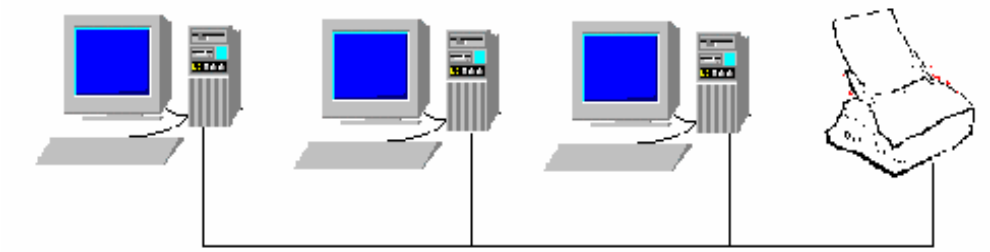


Рис. 1.1.

Локальная сеть позволяет организовать совместное использование общей для всех пользователей информации или аппаратных средств, например, принтера, как представлено на рис. 1.1.

Глобальные сети - совокупность локальных сетей, связанных каналами связи, например, выделенными линиями, телефонными, волоконно-оптическим кабелем, спутниковыми каналами связи и по радиоканалу. Это более дорогой способ передачи информации, скорости на порядки ниже чем в локальной сети. По этому глобальная сеть используется, в первую очередь, не для предоставления ресурсов в совместное пользование, а для пересылки сообщений, например, по электронной почте.

Пример фрагмента глобальной сети приведен на рис. 1.2.

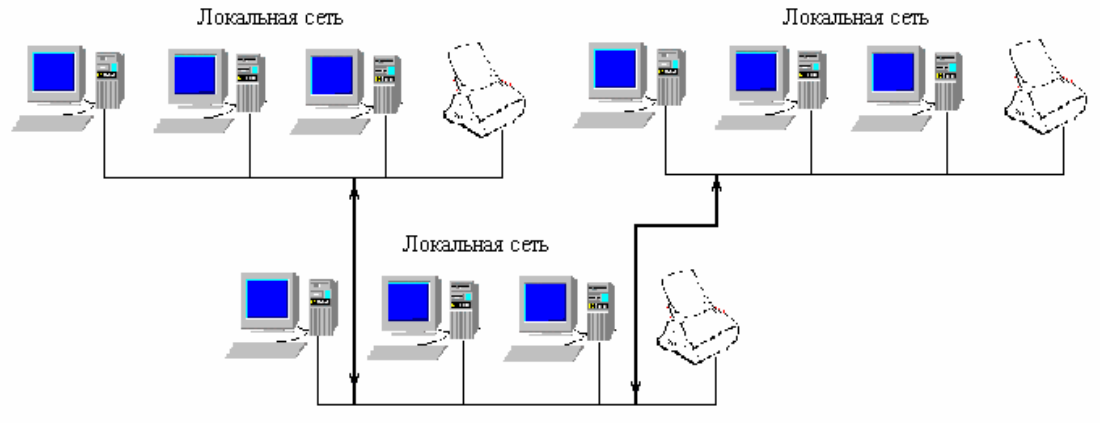


Рис. 1.2.

1.2. Одноранговые сети

Одноранговые сети являются простейшим способом организации локальной сети. Пример такой сети приведен на рис. 1.1, все компьютеры в такой сети равноправны, нет выделенных машин - серверов. Для одноранговой сети характерно отсутствие централизованного управления, каждый пользователь имеет право передавать сои ресурсы в общее пользование, возможно по паролю. Предусматриваются два типа паролей с правим на чтение и на запись. Пароль можно установить на каждый предоставляемый ресурс, например, диск или принтер. Количество пользователей одновременно подключающихся к ресурсу, ограниченно, кроме того, такое подключение снижает производительность компьютера, к которому происходит подключение.

Использование одноранговых сетей целесообразно для сравнительно малых фирм, которые не могут себе позволить дополнительные расходы на выделение отдельного компьютера для обслуживания сети и на специализированное сетевое оборудование.

Группа - объединение пользователей одноранговой сети.

Преимущества одноранговых сетей:

1. Не требует выделенных серверов.
2. Не требуют специализированного программного обеспечения.
3. Позволяют каждому пользователю самостоятельно управлять своими ресурсами.
4. Каждая машина может работать автономно и не зависит от исправности сетевого оборудования.
5. Наиболее дешевое решение.
6. Не требуют введения поста сетевого администратора.

Недостатки одноранговых сетей:

1. Снижение скорости работы компьютеров, предоставляющих доступ к своим ресурсам.
2. Малое количество соединений.
3. Анархия пользователей, самостоятельно и неединообразно администрирующих свои машины.
4. Практически отсутствующая система защиты. Компьютер не имеет информации о том, какой конкретно пользователь подключается к его ресурсам. Все подключающиеся пользователи равноправны.

1.3. Серверные сети

Отличие серверных сетей - наличие в них одного или нескольких серверов.

Сервер - выделенный компьютер, предоставляющий свои ресурсы всем машинам сети.

Домен - логическая организация (объединение) компьютеров и серверов, имеющих единую базу учетных записей и средств защиты. Домен - основной способ организации серверных сетей в Windows NT.

Преимущества серверных сетей:

1. Централизованная защита информации. Организация пользователей с различным уровнем доступа.
2. Хранение в одном месте файлов, предоставляемых всем пользователям. Это заметно упрощает обслуживание и резервное копирование.
3. Совместное использование программного обеспечения - одна копия вместо многих.
4. Совместное использование аппаратных средств - принтеров, CD дисков и т.д.
5. Более быстрый доступ по сравнению с одноранговой сетью.
6. Освобождение пользователя от управления процессом предоставления прав на ресурс своего компьютера.
7. Более простая и централизованная управляемость сети.
8. Возможность построения сложных сетей с иерархической структурой, решающих задачи различного типа.

Недостатки серверных сетей:

1. Выделение специальной машины под сервер.
2. Необходимость, для их работы, специального программного обеспечения.
3. Необходимость иметь в фирме администратора сети, выделенного сотрудника, занимающегося, как правило, только этой работой.

1.4. Гибридные сети

Данный тип сетей позволяет сочетать оба предыдущих типа. В сети существуют выделенные серверы, но также существует возможность пользователей предоставлять ресурсы своих локальных машин другим пользователям группы.

1.5. Типы серверов

В сети могут существовать следующие типы серверов:

1. Файловые серверы - функции обслуживания и хранения файлов.
2. Серверы печати - управление печатью документов всех пользователей.
3. Серверы баз данных - специализированные файловые серверы.
4. Почтовые серверы - управление системой электронной почты, защита от проникновения в сеть по этим каналам незаконных пользователей.
5. Сервер приложений - сервер, предназначенный для обслуживания только одного приложения (программы или пакета программ), представляющего большую важность для организации.

На практике один сервер может выполнять сразу все эти функции.

1.6. Контрольные вопросы

Вопрос 1:
Какие из следующих устройств могут быть предоставлены в совместное использование в сети ?
1. Модемы.
2. Жесткие диски.

3. Дисководы для компакт дисков.
4. Накопители на магнитной ленте.
5. Блоки бесперебойного питания.

Вопрос 2:
Что из нижеприведенного верно для серверных сетей?
1. Централизованное управление сетевыми ресурсами.
2. Все компьютеры равноправны.
3. Безопасность информации выше, чем при одиночном использовании этих же компьютеров.
4. Рост числа компьютеров в сети ничем не ограничен.

Вопрос 3:
Что из нижеприведенного описывает преимущества крупномасштабной сети с выделенным сервером?
1. Легкость администрирования.
2. Централизованное резервное копирование сетевых данных.
3. Невысокая стоимость реализации.
4. Повышенная производительность.

Вопрос 4:
Что из нижеприведенного описывает недостатки одноранговой сети?
1. Неисправность сервера может сделать сеть неработоспособной.
2. Стоимость сети возрастает вследствие выделенного оборудования и специализированного программного обеспечения.
3. Когда вы предоставляете доступ к своим ресурсам, скорость работы Вашего компьютера заметно снижается.
4. Для управления сложным специализированным программным обеспечением требуется квалифицированный персонал.

Вопрос 5:
Что из нижеприведенного описывает локальную сеть?
1. Соединяет сети по всему миру.
2. Компьютеры, соединенные в сеть, расположены близко друг от друга.
3. Требует использования выделенных коммуникационных линий для поддержки соединений, например, телефонных линий.
4. Использует технологии глобальных сетей внутри конкретного географического региона.

2.Топология сетей

2.1. Шинная топология

Шинная организация локальной сети является самой простой и дешевой в исполнении.

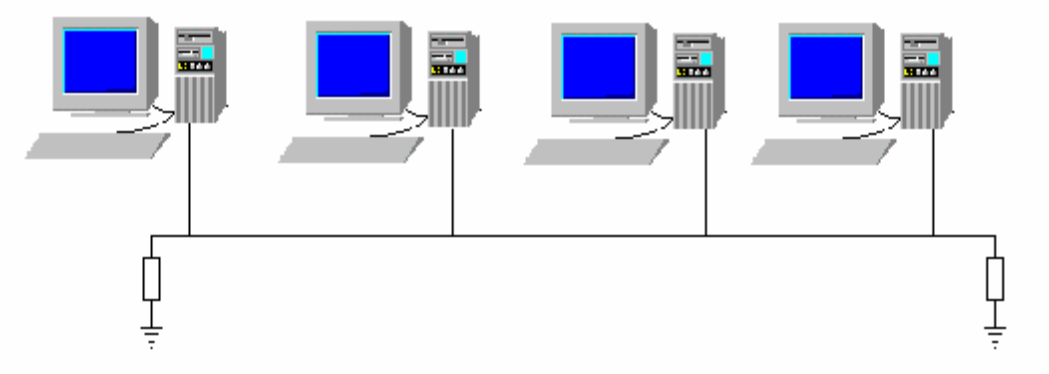


Рис. 2.1.

Все компьютеры соединяются коаксиальным кабелем, подключающимся к сетевой карте посредством Т-образного разъема, имеющего 2 выхода. Информационный пакет от передающего компьютера передается всем компьютерам, объединенным этой сетью. Тот компьютер, сетевой адрес которого совпадает с адресом получателя, обрабатывает этот пакет, остальные пропускают его мимо “ушей”. Это приводит к тому, что в сети, в каждый момент времени, находится только один информационный пакет, а остальные компьютеры ждут своей очереди. С ростом числа машин это заметно снижает скорость передачи данных.

Кроме этого, каждое подключение нового компьютера приводит к дополнительному затуханию информационного сигнала. На концах кабеля необходимо ставить специальные устройства - называемые терминаторами, предотвращающими отражение и повторное попадание сигнала в соединительный кабель, эффекта “эхо”, от старого сигнала, приводящего к ошибкам при приеме информации. Для коаксиального кабеля в качестве терминатора используют резисторы по 50 Ом, замкнутые на заземленную экранирующую оплетку кабеля.

Достоинства шинной топологии:

1. Надежно работает в маленьких сетях, проста и понятна.
2. Требует меньше соединительного кабеля, к тому же он дешевле, чем используемый в других типах соединений.
3. Легкая возможность расширения сети. Для этого не требуется тащить отдельный кабель, а можно добавить еще один фрагмент и переставить терминатор на следующую машину.

Недостатки шинной топологии:

1. Наличие, в каждый момент времени, только одного пакета в сети значительно снижает производительность сети.

2. Ослабление сигнала вследствие большого количества подключенных компьютеров, что может привести к их неправильному приему.
3. Разрыв кабеля или некоторые неисправности сетевой карты одной из машин приводят к полной неработоспособности сети.
4. Невозможно диагностировать повреждения кабеля. Необходимо последовательно просматривать все соединения до обнаружения повреждения, как это было на заре телефонии.
5. Общая длина сети, построенной на шинной топологии, не может превышать 180 м.

2.2. Звездообразная топология

В топологи типа “звезда” используется специальный концентратор - Hub, соединяющий все машины, как показано на рис. 2.2.

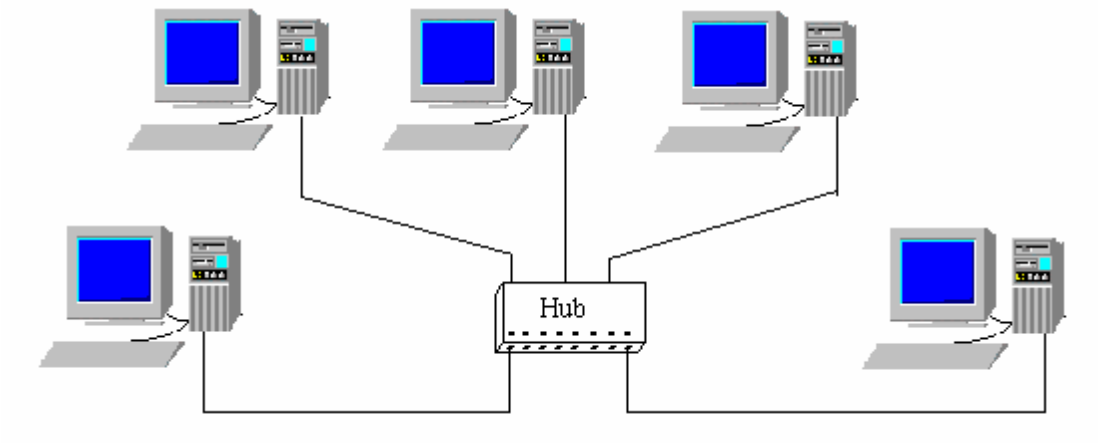


Рис. 2.2.

Звездообразная топология применима в сетях с сильно сосредоточенными компонентами. В коммутированной звездообразной сети пакеты передаются только от отправителя получателю, это не мешает обмену сообщениями между остальными компьютерами, подключенными к сети.

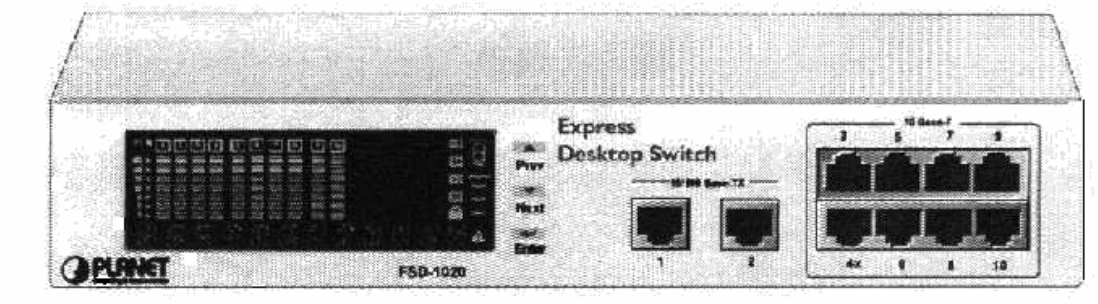


Рис. 2.3. Сетевой концентратор FSD 1020

На рис. 2.3. приведен внешний вид сетевого концентратора. В левой части располагается индикаторная панель, показывающая режим, в котором работает каждый из выходов концентратора; два выхода в центре предназначены для соединения концентраторов между собой, так называемый прямой и инверсный выходы; в правой части расположены обычные выходы. Внешний вид сетевых концентраторов может различаться.

Активный концентратор позволяет усилить сигнал в линии и предавать его на значительно большие расстояния, чем в шинной топологии, до 500 м. Усложнением звездообразной сети является гибридная звездообразная сеть, когда сеть расширяется с помощью дополнительных концентраторов, включаемых вместо одной из машин в первый концентратор, создавая сколь угодно сложные структуры. Пример такой структуры представлен на рис. 2.4.

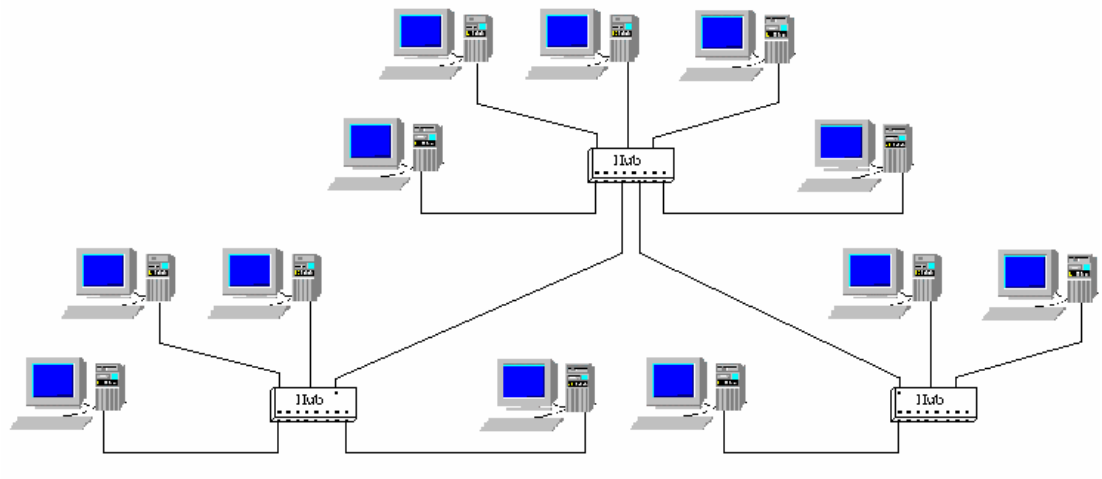


Рис. 2.4.

Используя сетевые концентраторы с выходами, поддерживающими различные скорости обмена, можно организовывать сложные топологии с более оптимальным трафиком - загрузкой линий. Это очень актуально для сервера, к которому обращаются сразу большое число компьютеров, как показано на рис. 2.5. Сервер передает информацию концентратору со скоростью 100 Мбит в секунду (конечно, для этого на нем должна быть соответствующая сетевая карта, такую скорость должен поддерживать концентратор и соединительные линии), а рабочие станции принимают ее со скоростью 10 Мбит в секунду. В данном примере сервер может успевать отвечать 10 рабочим станциям без задержек со своей стороны.

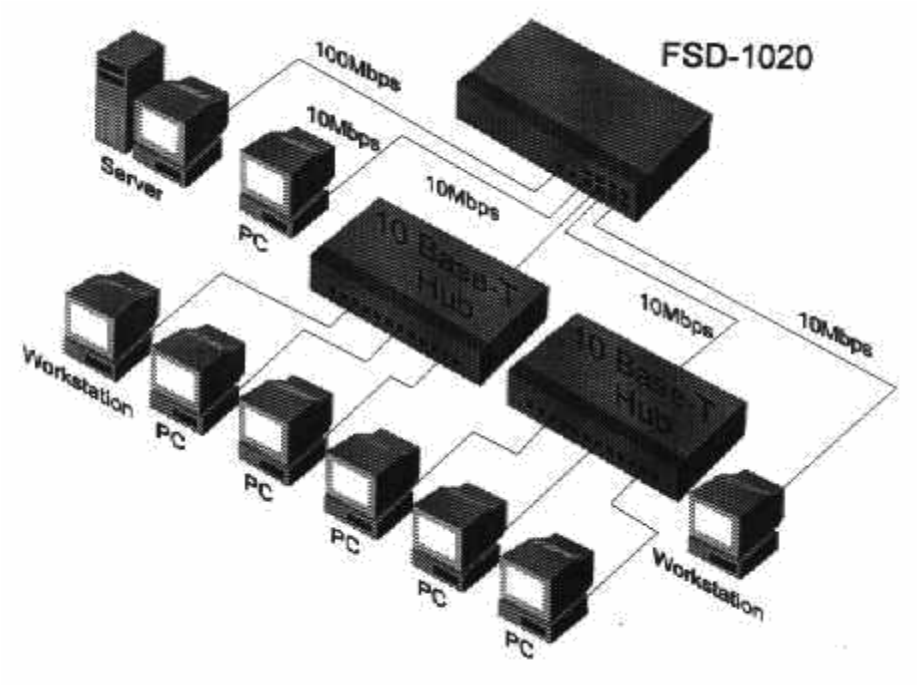


Рис. 2.5.

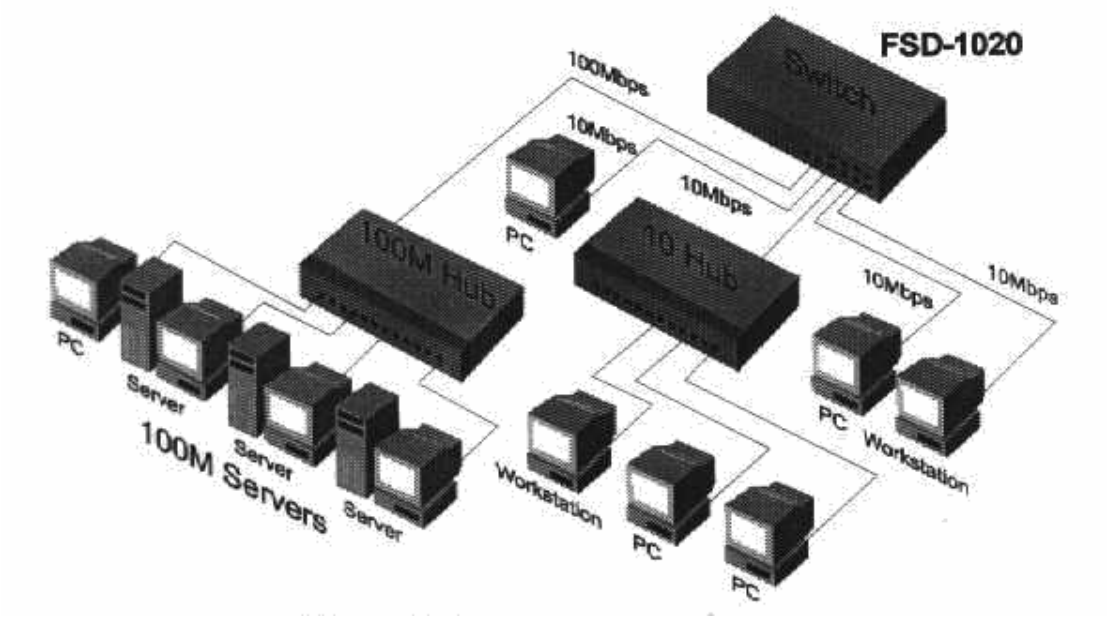


Рис. 2.6.

На рис. 2.6, через высокоскоростной сетевой концентратор подключена целая группа серверов. Для большой организации такое решение может быть очень оправданно и позволит вынести все сервера в удаленное и хорошо защищенное помещение, что уменьшает риск вывода из строя или кражи сетевого оборудования и информации, на нем хранящейся.

Достоинства звездообразной топологии сети:

1. Простое добавление новых компьютеров к сети, большие возможности для расширения ее.
2. Быстрая возможность диагностирования соединений сети по индикаторам на концентраторах.

3. Сбои или обрыв связи с одной из машин не сбивает работу остальных машин сети.
4. Большие возможности для защиты информации от несанкционированного доступа.
5. Усиление концентраторами сигналов, увеличение длины связей.
6. Обмен между конкретными парами компьютеров обычно не мешает связям между остальными машинами и значительно повышает скорость обмена по сети.

Недостатки сети звездообразного типа:

1. Значительное увеличение расхода соединительного кабеля.
2. Выход из строя концентратора исключает из сети сразу все подключенные к нему машины.

2.3. Кольцевая топология

Сети с кольцевой топологией используют последовательную передачу сообщения от одной машины другой, по кругу, пока сообщение не достигнет адресата.

Примером организации сети такого типа является сетевой класс УКНЦ, ранее широко распространяемый в нашей стране для обучения информатики школьников. Кроме этого, данный тип сетей применяется в сетях FDDI и Token Ring, построенных на волоконно-оптических линиях. Однонаправленность этих кабелей хорошо сочетается с кольцевой архитектурой сети, в других топологиях вынуждены применять волоконно-оптическую пару, для двух направлений.

Благодаря постоянной ретрансляции сигнала в сети такого типа, значительно менее остро стоит проблема расстояния и количества пользователей.

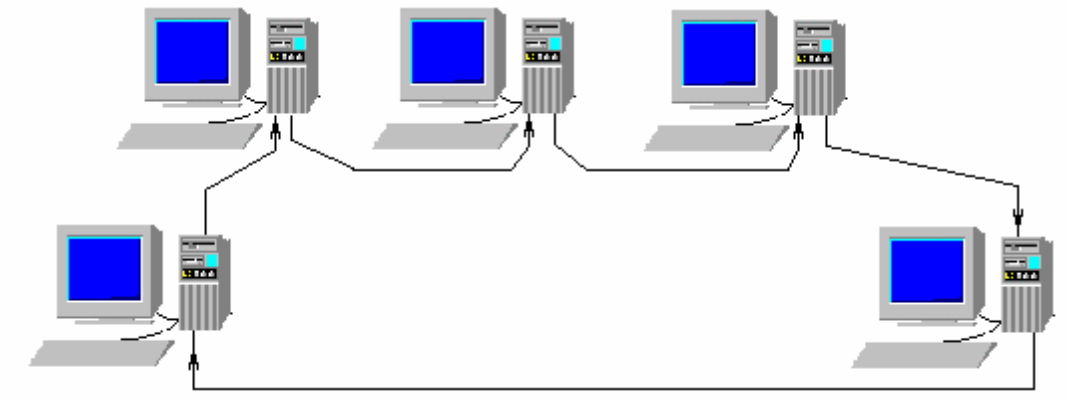


Рис. 2.7.

Достоинства сети с кольцевой топологией:

1. В архитектуре сети заложены равные права всех компьютеров, подключенных к сети. Это делает очень затруднительным монопольный захват всех ресурсов сети.
2. Увеличение числа пользователей приведет к снижению скорости обмена по сети, но не остановит этот обмен, в отличие от сети с шинной топологией.

Недостатки сети с кольцевой топологией:

1. Разрыв кабеля или отказ одного из компьютеров приводит к обрыву процесса обмена сообщениями.
2. Для реализации этой сети, широко встречавшейся в нашей стране - классе УКНЦ, которым комплектовались средние и профессиональные учебные заведения был характерен следующий недостаток. Система выключения компьютера из сети при выключенном питании, для пропуска сообщений следующему компьютеру, реализовывалась механическим способом, что заметно снижает надежность и временной ресурс эксплуатации сети.

2.4. Комбинированные топологии

На практике встречаются различные комбинации выше перечисленных сетей.

Звездообразно - шинная- топология - шина связывает несколько концентраторов, на которых собраны локальные сети типа “звезда”.

Звездообразно-кольцевая топология - кольцеобразная сеть объединяет концентраторы с организованными на их основе локальными сетями звездообразной топологии.

Шинно-звездообразная топология - центральная сеть звездообразной топологии объединяет концентраторы, к которым подключены сети, основанные на шинной топологи. Многие концентраторы, например EH-802, имеют каждый по два выхода на коаксиальный кабель.

2.5. Сотовая топология

Для сетей с повышенной надежностью, как правило, предусматривается сотовая топология. Данный тип предусматривает соединение каждого компьютера с каждым. Возможности размещение многих сетевых карт в одном компьютере ограниченна.

В стандартную системную плату их можно вставить не более 5 шт., можно, конечно, вставить платы расширения слотов компьютера, но это все равно не позволит построить большую сеть. К тому же с ростом числа узлов быстро растет стоимость такой сети. Все это делает такой тип сетей мало реализуемым на практике. Как правило, вместо них используются сети с гибридной топологией. Пример сети с сотовой топологией представлен на рис. 2.8.

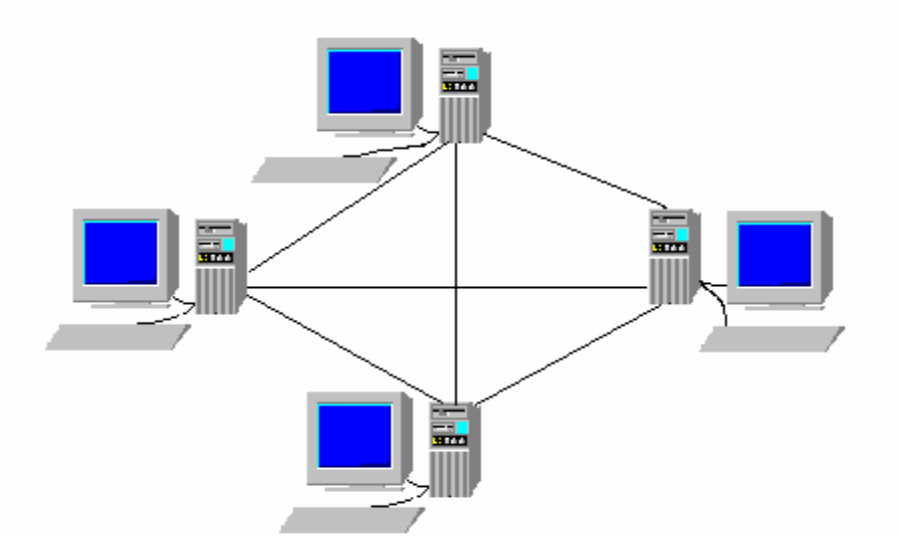


Рис. 2.8.

2.6. Гибридная топология

Для топологий этого типа характерно резервирование связей между основными серверами, выделенными на рис. 2.9, более крупными компьютерами без мониторов. Даже при выходе из строя некоторых линий связи это не выведет из строя всю сеть, наиболее важные узлы сети получат информацию, пришедшую обходными путями. Практически все важные сети государственных организаций построены по этому принципу.

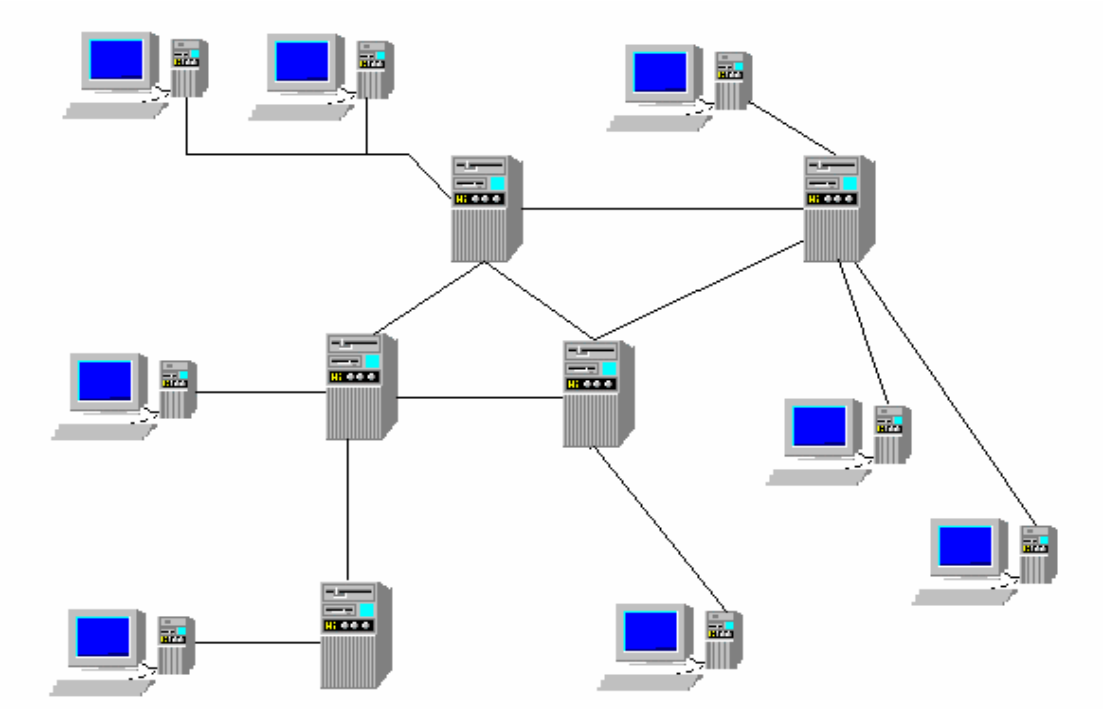


Рис. 2.9.

Наиболее яркий пример такой сети - всемирная паутина - Internet. Пример сети построенной по этому принципу, приведен на рис. 2.9.

2.7. Контрольные вопросы

Выберите правильный ответ и обоснуйте его.

Вопрос 1:

Какая сетевая топология самая дешевая в исполнении?

1. Топология типа “звезда”.
2. Топология типа “шина”.
3. Гибридная топология.
4. Кольцевая топология.

Вопрос 2:

Какая топология обеспечивает максимально быстрое получение информации компьютером с трех других компьютеров?

1. Топология типа “звезда”.
2. Топология типа “шина”.
3. Гибридная топология.
4. Кольцевая топология.
5. Сотовая топология.

Вопрос 3:

Какая топология допускает значительное наращивание числа компьютеров в сети?
1. Топология типа “простая звезда”.
2. Топология типа “шина”.
3. Кольцевая топология.
4. Сотовая топология.

Вопрос 4:
Какая топология обеспечивает максимально возможное по надежности соединение 10 компьютеров типа P5, в локальную сеть?
1. Топология типа “звезда”.
2. Топология типа “шина”.
3. Гибридная топология.
4. Кольцевая топология.
5. Сотовая топология.

Вопрос 5:
В комнате “А” располагается сервер и 6 компьютеров, в комнатах “Б” и “С” располагается по 8 компьютеров. Расстояние между всеми комнатами 30 м., все компьютеры запускают много программ с сервера, и на право доступа к нему постоянно есть очередь. По финансовым соображениям Вы можете приобрести только два сетевых концентратора, а сеть в третьей комнате приходится делать на шинной тополоти. Как обеспечить максимально равный приоритет по доступу к серверу?
1. Установить шинную топологию в комнате “А” и подключить к ней сетевые концентраторы комнат “В” и “С”.
2. Установить шинную топологию в комнате “С” и подключить ее к сетевому концентратору комнаты “А”, к которому также подключен сетевой концентратор комнаты “В”.
3. Установить шинную топологию в комнате “С” и подключить ее к сетевому концентратору комнаты “В”, подключенному к сетевому концентратору комнаты “А”.
4. Установить шинную топологию в комнате “В” и подключить ее к сетевому концентратору комнаты “А” и комнаты “С”.

3. Сетевые компоненты

3.1. Коаксиальный кабель

Коаксиальный кабель - это два проводника, один из которых расположен внутри другого, являющегося экраном. Внешне этот тип

кабеля аналогичен телевизионному кабелю используемому в подключении к антеннам.

Достоинства коаксиального кабеля:

1. Низкая стоимость.
2. Простое подключение к разъему, которое трудно перепутать.
3. Возможность наращивания узлов подключением к узлу одного из компьютеров.
4. Экранирование обеспечивает высокую помехозащищенность.

Недостатки коаксиального кабеля:

1. Кабель остается подвержен электромагнитным помехам.
2. Возможен свободный перехват сообщений, передаваемых по этому типу кабеля, злоумышленником.

Пропускная способность такого кабеля 10 Мбит/с. Максимальное число узлов для кабеля типа RG-58 - 30 узлов, для RG-8 и RG-11 - 100 узлов, максимальная длина кабеля - 185 м.

3.2. Витая пара

Витая пара объединяет 4 пары проводников, скрученных друг относительно друга. Это позволяет значительно снизить паразитные наводки и взаимовлияние друг на друга. Внешний вид витой приведен на рис. 3.1.

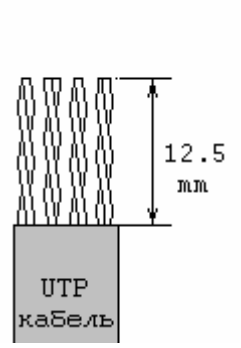


Рис. 3.1.

Скорость передачи по этому типу соединений от 1 до 155 Мбит/с., в среднем эта величена равна 10-16 Мбит/с. Максимальная длина участка до 200 м.

Категории кабелей, UTP - неэкранированная витая пара:

Категория	Характеристика
1-2	Речевые сигналы, или данные с низкой скоростью передачи.
3	Используется в большинстве компьютерных сетей. Скорость передачи до 10Мбит/с.
4	Повышенная скорость передачи до 20Мбит/с.

5 Аналогичен кабелю 3 категории, но с более высокими потребительскими качествами, прочностью, долговечностью и т.п. Профессиональная категория для сетей. Скорость передачи до 100Мбит/с.

Подключение кабеля к разъему невозможно без специального инструмента и требует определенных технических навыков и практического опыта при выполнении подобной операции. В первый раз Вас скорее всего постигнет неудача. Однако, во многих магазинах этот тип кабеля может быть приобретен уже с установленными разъемами. В качестве разъемов для кабелей этого типа используется разъем RJ-45.

Достоинством этого типа кабеля является его низкая стоимость.

Улучшением данного типа кабеля является витая пара с экранированием - тип STP. Характеристики STP в целом аналогичны кабелю UTP.

Кабели типа UTP, и несколько менее STP, остаются подвержены электромагнитным помехам. Возможен также перехват сообщений, передаваемых по этим типам кабелей за счет их паразитного электромагнитного излучения.

3.3. Волокно - оптический кабель

Достоинством стекловолокна как среды передачи информации- это самая высокая скорость, до 2Гбит/с., максимально возможная на современном уровне развития технологий. Очень низкие потери в канале, позволяющие передавать сообщения на большие расстояния, сотни километров. Кроме того, волоконный кабель обладает очень высокой надежностью, прочностью, долговечностью. Кроме того, стекловолокно позволяет избежать проблем с перехватом передаваемых сообщений злоумышленниками, и не подвержен помехам.

Стекловолокно является самым перспективным видом связи, но остающимся пока достаточно дорогим. Особой проблемой является сварка волоконно-оптического кабеля и подключение кабеля к разъему.

3.4. Телефонные каналы

Подключение удаленного компьютера с помощью телефона является основным способом подключения частных пользователей к сети Internet во всем мире. Информация хранится и обрабатывается в ПЭВМ в цифровом виде и не может непосредственно передаваться по телефонным линиям предназначенных для пропускания аналоговых сигналов. Для передачи цифровой информации по таким линиям требуется специальное устройство - модем, преобразующий цифровую информацию в аналоговые сигналы и обратно. Скорость передачи определяется пропускной способностью телефонных линий и станций. На сегодняшний день она составляет 33600 бит/сек. Новые протоколы позволяют работать со скоростью до 56000 бит/сек.

Первые модемы и подключение к сети с использованием телефонного аппарата используются уже с начала 60-х годов.

3.5. Радиоканал

Передача информации по радиоканалу позволяет организовать удаленное подключение компьютера, расположенного на большом удалении или даже возможно перемещаемого, к сети. Таким образом, организуется связь с сетью Internet журналистов находящихся в различных уголках мира.

Кроме того, с использованием радиоканала строятся специализированные радио сети, например, такая как “Теллур”, созданная в нашем университете с участием одного из авторов данной работы.

В отдельный класс радиосетей необходимо выделить спутниковые системы телекоммуникации, в которых передача радиосигнала от одного абонента к другому проходит через спутник.

3.6. Инфракрасные лучи

Достоинством передачи информации с помощью излучателей в инфракрасном диапазоне является отсутствие необходимости прокладки соединительных кабелей или получения разрешений на использование радиочастоты.

Наибольшая эффективность в использовании этого способа соединения может быть достигнута во временной сети, или в случае, если прямое подключение, с помощью соединительного кабеля,

затруднительно или невозможно. Например, один из компьютеров расположен в здании напротив, узкий переулок, прокладка кабеля в этом случае вызовет большие затруднения, а поставить два узконаправленных передатчика, будет наиболее правильным решением.

Недостатками этого типа связи является необходимость в четком ориентировании направления приема и передачи и наличие прямой видимости на небольшом расстоянии.

3.7. Стандарты на сети

Во всем мире приняты общие стандарты на соединения компьютеров, описанные в форме протоколов. ***Протокол*** - точно определенный порядок обмена информацией между устройствами.

Протокол может реализовываться аппаратно или программно, возможны и сочетания этих двух способов. Используемые в сетях протоколы будут рассмотрены далее.

Стандарты на физические сети:

10Base5 (Толстый Ethernet)	Толстый коаксиальный кабель. Максимальная длина - 500 м. Максимальная скорость - 10Мбит/с.
10Base2 (Тонкий Ethernet)	Тонкий коаксиальный кабель. Максимальная длина - 185 м. Максимальная скорость - 10Мбит/с.
10BaseT	Витая пара. Максимальная длина - 100 м. Максимальная скорость - 10Мбит/с.
10BaseFL	Волоконно-оптическая линия. Максимальная длина - 2000 м. Максимальная скорость - 10Мбит/с.
100VG-AnyLAN	Максимальная скорость - 100Мбит/с.
100BaseT	Максимальная скорость - 100Мбит/с.

Стандарты на сетевые технологии:

802.2	поддержка двух подуровней, логической связи и управления доступом.
802.3	Организация множественного доступа и проверки конфликтов.
802.5	Стандарты для сетей Token Ring (кольцо на оптических линиях).

3.8. Сетевые карты

Сетевая карта - интерфейсная плата, вставляющаяся в слот материнской платы компьютера и обеспечивающая посылку и прием сообщений из сети, при этом обеспечивается проверка целостности и достоверности переданной информации.

Кроме сетевой карты, в компьютере должно быть установлено соответствующее программное обеспечение: драйвер сетевой карты, протокол, клиент, для соответствующего типа сети. В системном окружении компьютера, за этими драйверами, должны быть зарезервированы соответствующие прерывания и базовые адреса буферов.

3.9. Мост

Мостом называют компьютер или иное устройство, с установленными в нем двумя или более сетевыми картами, подключенными к разным локальным сетям. В отличие от соединения с помощью сетевого концентратора, при таком способе подключения можно организовать фильтрацию и отслеживание пакетов, передаваемых по сети. Например, Вы можете поставить такой компьютер на входе Вашей сети и пропускать запросы от пользователей только из перечисленного списка или по паролю. Тем самым Вы закрываете внутреннюю сеть от проникновения злоумышленников или просто нежелательных пользователей, т.е. повышается безопасность Вашей локальной сети.

Дополнительным достоинством моста является то, что он может соединять сети различного типа. Кроме того, мост может выполнять функции маршрутизатора, с помощью специальных таблиц, направляющего информацию к указанному адресу кратчайшим путем.

3.10. Бездисковые станции

Бездисковые станции не имеют в своем составе жестких дисков. Загрузка операционной системы и всех необходимых для работы файлов происходит с сервера через локальную сеть.

Для выполнения этой операции в сетевую карту такого компьютера вставляется специальная микросхема ПЗУ, с прошитой в ней программой, эмулирующей на этапе загрузки системную

дискету, содержимое которой получается с сервера по локальной сети.

Бездисковая станция является очень хорошим решением, к достоинством его можно отнести:

1. Экономию денег, за счет отсутствия дисководов и винчестеров.
2. При загрузке с сервера возможно сделать различные варианты загрузки, в том числе различных операционных систем. Это было бы невозможно при загрузке с жесткого диска. Это позволяет удовлетворять на одной машине потребности самых различных пользователей.
3. Отсутствие дисководов исключают возможности записи пользователями посторонних программ, с которыми как правило, и приходят вирусы, или выноса служебной информации за пределы организации, все данные и программы хранятся централизованно, что упрощает вопросы обеспечения безопасности информации. Кража рабочей станции дает в руки грабителей только машину без записанной на ней информации.

Бездисковые станции - очень удачное решение для организаций с сильной централизацией, учебных организаций.

3.11. Контрольные вопросы

Выберите правильный ответ и обоснуйте его.
Вопрос 1:
Какой тип кабеля необходимо использовать для соединения компьютеров, расположенных на расстоянии 700 м. друг от друга?
1. Коаксиальный кабель.
2. Витая пара.
3. Волоконно-оптическая линия.

Вопрос 2:
Какой тип кабеля необходимо применить для организации сети с топологией типа “звезда”.
1. Коаксиальный кабель.
2. Витая пара.
3. Волоконно-оптическая линия.

Вопрос 3:

Необходимо организовать компьютерную связь между двумя зданиями, расположенными в пределах прямой видимости. Какой тип соединения Вы рекомендуете?

1. Соединение по радиоканалу.
2. Соединение на инфракрасных лучах.
3. Проложить волоконно-оптическую линию.

Вопрос 4:

Какие дополнительные требования к сети вызывает применение для работы в сети бездисковых рабочих станций?

1. Делает невозможным использование шинной топологии.
2. Требует обеспечение более высокой скорости передачи информации по сети.
3. Делает бессмысленным применение одноранговых сетей.

Вопрос 5:

Какие еще устройства, кроме сетевой карты, позволяют организовать сеть?

1. Модем.
2. COM порт.
3. Порт принтера.
4. Звуковая карта.

Вопрос 6:

В Вашей сети один из сегментов превышает 200 метров. Какой тип устройства поможет предотвратить затухание сигнала ?

1. Тюнер.
2. Приемник.
3. Усилитель.
4. Повторитель.

4. Проектирование сети

4.1. Выбор типа сети

При создании сети первый вопрос, на который необходимо ответить - это выбор типа сети: серверной или одноранговой сети.

Одноранговая сеть	Серверная сеть
1. В сети объединяются менее 10 компьютеров. 2. Сотрудники, работающие в данной сети, обладают хорошим уровнем компьютерной подготовки. 3. Проблема защиты информации не является актуальной. 4. Все пользователи являются равноправными. 5. Финансовое состояние не позволяет приобрести сервер с необходимым обеспечением. 6. Проблема резервирования данных успешно решается самими пользователями. 7. Специализированные серверы не требуются (почтовые).	1. Сеть состоит из более 10 компьютеров. 2. Уровень квалификации пользователей различен. 3. Ряд файлов с информацией, программных средств находится в общем использовании всеми пользователями. 4. Необходимо разделять пользователей по уровням доступа к информации, правам на ее использование. 5. В фирме существует единая политика в области использования компьютеров.

4.2. Выбор сервера

В настоящее время наиболее распространенными серверными типами сетей являются сети, построенные на базе Novell NetWare и WindowsNT Server.

Достоинством сетей на базе Novel NetWare является:

1. Высокая скорость работы
2. Высокая надежность
3. Возможность разбиения пользователей на группы. Предоставление различных прав доступа различным группам пользователей.

Недостатки:

1. Выделение отдельной машины для организации сервера и периодическом отвлечении рабочей машины на задачи администрирования сети.

Достоинством сетей с сервером WindowsNT является:

1. Хорошая совместимость с наиболее распространенной операционной системой для персональных компьютеров Windows95.
2. Взаимодействие с глобальной сетью Internet Возможность организации WEB сервера одновременно с файл сервером.
3. Позволяет использовать сам сервер для выполнения различных операций, например, служебных действий по администрированию сети.
4. Операционная система WindowNT Server удовлетворяет классу защищенности С2 и сертифицирована для использования в министерстве обороны США.

Недостатки:

1. Содержит достаточно большое количество ошибок, что требует периодического внесения исправлений в работающую операционную систему и отслеживания появления этих исправлений.
2. Закрытость кода.
3. В связи с закрытостью исходного кода отсутствуют надстройки, обеспечивающие защиту данных от несанкционированного доступа на уровне системных функций.
4. Требует большего количества ресурсов для выполнения аналогичных задач по сравнению с NetWare.

Для специализированных почтовых, WEB серверов часто применяются различные модификации сетевой операционной системы UNIX.

Достоинства:

1. Высокая надежность.
2. Его родные протоколы используются в Internet.
3. Написан на языке Си, исходные тексты полностью доступны и документированы.

4. Язык Си встроен как основной элемент операционной системы, что позволяет гибко модифицировать элементы операционной системы под задачи конкретных пользователей.

Недостатки:

1. Несовместимость с наиболее распространенной операционной системой для рабочих станций Windows.

4.3. Выбор среды передачи информации

Вопрос выбора среды передачи зависит от выбранной топологии, задач создаваемой сети и удаленность друг от друга отдельных компьютеров, которые предполагается объединить в сеть.

Наиболее дешевым является использование кабельных соединений. Радиомодемы по стоимости соизмеримы со стоимостью целого компьютера. Обычные модемы, инфракрасные излучатели несколько дешевле, но тоже требуют значительную сумму. Применение этих средств связи должно быть обосновано.

4.5. Выбор топологии

При выборе топологи сети первый вопрос о выборе между шинной или звездообразной сетью. Кольцевые сети сейчас используются сравнительно редко, реализация сотовой топологии является очень тяжело реализуемой. Поэтому выбор стоит в первую очередь между звездообразной и шинной топологиях. Если этого не достаточно можно использовать их комбинацию или гибридную топологию.

Можно привесит следующие рекомендации этого выбора.

Шинная топология	Звездообразная топология
1. В сеть требуется объединить небольшое число компьютеров. 2. Требуется максимально дешевое решение.	1. Сеть объединяет большое количество компьютеров. 2. Необходимо иметь легкий способ наращивания числа компьютеров в сети. 3. Необходимо проводить

	диагностику в сети. 4. Скорость в сети является актуальной проблемой.

4.6. Контрольные вопросы

Вопрос 1:

Вам необходим сервер для 10 рабочих станций, работающих под управлением Ms Windows95, кроме этого на этом же сервере должна поддерживаться Web - страница этого подразделения. Какой тип сервера Вы используете?

1. Novell Netware.
2. WindowsNT.
3. UNIX.

Вопрос 2:

Вам необходим тип сервера, отвечающий международным требованиям по безопасности сети. Какой тип сервера Вы используете?

1. Novell Netware.
2. WindowsNT.
3. UNIX.

Вопрос 3:

Вам необходим тип сервера с максимальной скоростью обслуживания рабочих станций, работающих под управлением Windows 95?

1. Novell Netware.
2. WindowsNT.
3. UNIX.

Вопрос 4:

Какое решение будет оптимальным для сети из 10 рабочих бездисковых станций, с удаленной загрузкой Windows 95?

1. Сервер Novell Netware с шинной топологией сети.
2. Сервер WindowsNT с топологией сети типа “звезда”.
3. Сервер WindowsNT с шинной топологией сети.
4. Сервер UNIX с топологией сети типа “звезда”.

5. Администрирование сети

Основная задача администратора сети - управление и поддержание работоспособности сети. Как правило, предварительно сеть требуется создать и инсталлировать.

5.1. Пользователь

Основным логическим элементом сети является пользователь. Пользователи распознаются по именам. За каждым из них может быть закреплен свой пароль и присвоены права доступа к тем или иным ресурсам. Для каждого пользователя возможно создание своих домашних каталогов, все права на них (чтение, запись) предоставляются автоматически. Права на дополнительные разделы необходимо предоставлять отдельно при конфигурировании каждого пользователя.

Кроме того, каждому пользователю можно прописать свои учетные записи и стартовые файлы, конфигурирующие и определяющие его работу на компьютере, например, время работы в сети, имена отображаемых ему каталогов в качестве дисков, количество одновременных входов в сеть под его именем, пароли, их срок действия. Чтобы не прописывать всю эту информацию для каждого пользователя, ее можно прописать для всей группы, объединяющей выбранных пользователей.

5.2. Группа

Как правило, для упрощения предоставления прав, пользователей объединяют в группы и предоставляют права сразу всем членам группы. Это позволяет избежать много рутинных операций и снижает вероятность ошибок.

Как правило, большинство серверных операционных систем предлагают по умолчанию создание трех групп - GUEST (вход в сеть с минимальными правами, USERS (по умолчанию, вход в сеть с полными правами на свои домашние каталоги) и ADMIN (полные права для всех операций в сети). В зависимости от сложности иерархии пользователей Вам может понадобиться создание и других групп пользователей, например, разбив их по классам, создать группу менеджеров над отдельными пользователями и целыми группами.

5.3. Права

Основными предоставляемыми правами является доступ к диску, отдельным каталогам или файлам. Возможно представление следующих комбинаций прав:

Права на чтение	Есть права только просматривать данные и запускать программы. Записать любые изменения невозможно.
Права на запись	Допустимо создавать и записывать файлы.
Права на выполнение	Возможность только выполнять файлы, без права их просмотра, копирования, удаления и изменения.
Право на удаление	Права на удаление файлов. (Возможен вариант, что пользователь имеет право только читать и редактировать файлы, но не может их удалить)
Передача прав на свои разделы.	Возможность передачи прав, на свой каталог или целый раздел, другому пользователю.

Возможна любая комбинация прав, предоставляемых как отдельным пользователям, так и целым группам, в этом случае тоже происходит их комбинация.

5.4. Администрирование в сетях Novell Netware

Администрирование сетей Novell Netware осуществляется с помощью программы NwAdmin. После запуска программы у Вас открывается окно со следующей информацией.

Логическая структура сети - дерево сети - представлено в дочернем окне программы NetAdmin. Дерево является способом логической организации сети на сервере Novell, остальные сетевые операционные системы имеют аналогичные понятия, например, домен в сервере WindowsNT.

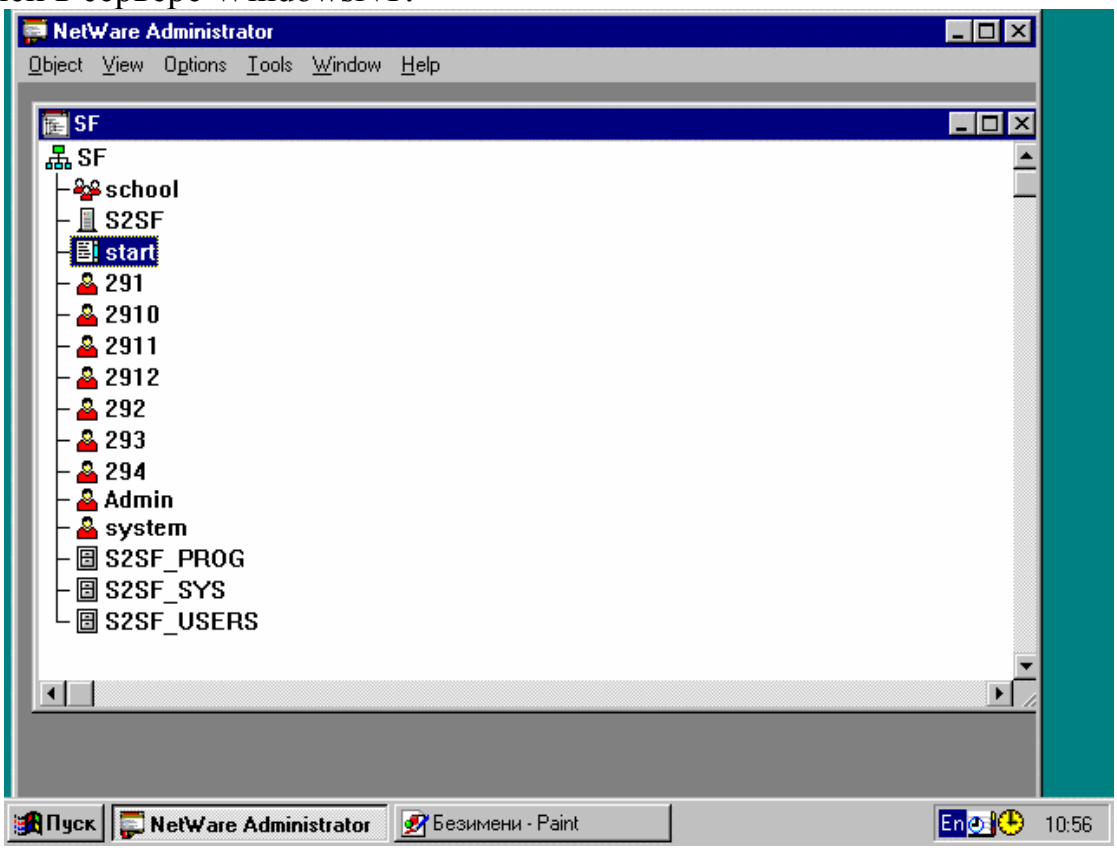
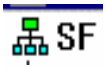
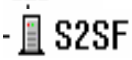


Рис. 5.1. Окно программы NwAdmin

В приведенном примере элементами дерева являются:

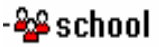


Обозначение самого дерева сети



Сервер S2SF (в дереве может присутствовать несколько серверов)

Пользователь. Если перейти в данный раздел, то откроется окно со всеми его учетными данными именем, паролем, правами доступа и т.д.



Группа пользователей. При переходе во внутрь данного раздела предоставляется возможность

добавлять или удалять членов группы; назначать права доступа сразу всем членам группы.

Раздел сервера (логический диск).

Стартовый файл для пользователя. Используя глобальные имена, можно создать универсальные стартовые файлы сразу для всей группы пользователей.

Стартовый файл аналогичен по функциям файлу autoexec.bat, но содержит ряд дополнительных команд по мапированию (назначению) дисков для конкретных пользователей. Каталоги разделов сервера назначаются администратором, для конкретных пользователей, как сетевые логические диски.

Кроме перечисленных, элементами дерева могут являться: устройства, находящиеся в совместном использовании, например, принтеры, модемы, CDROM и т.д. Кроме того, могут присутствовать элементы объединения сетей - шлюзы, мосты.

Добавление новых элементов дерева осуществляется нажатием клавиши insert, удаление нажатием клавиши del на подсвеченном элементе.

Выполнение администрирования сети и просто запуск программы NwAdmin требуют прав системного администратора.

5.5. Проектирование сети

При составлении проекта администрирования сети Вам необходимо решить задачу предоставления прав различным пользователям на доступ к дискам, каталогам, файлам, принтерам, создания групп пользователей, размещение общих программ на сетевых дисках и т.д.

При этом следует руководствоваться принципом минимальной достаточности выделяемых прав для выполнения поставленных ему задач.

5.6. Контрольные вопросы

Выберите правильный ответ и обоснуйте его.

Вопрос 1:

Какие права в сети должен иметь директор фирмы?

1. Все права на все, разделы сервера.
2. Права только на свои разделы.
3. Права сетевого администратора.
4. Право на передачу своих прав на свои разделы другим сотрудникам фирмы.

Вопрос 2:

Какая комбинация прав на раздел должна быть у пользователя для работы с документами в Ms Word?

1. Права на чтение.
2. Права на чтение и права на выполнение.
3. Права на чтение, права на выполнение, право на удаление.
4. Права на чтение, права на выполнение, право на удаление и право на запись.

Вопрос 3:

Какие устройства будут фигурировать в дереве сервера Novell?

1. Пользователь.
2. Звуковая карта.
3. Принтер.
4. UPS.

Вопрос 4:

Какие права необходимо иметь для редактирования файла с заранее известным полным именем?

1. Права администратора.
2. Право на запись и чтение.
3. Право на запись.
4. Право на удаление.

6. Безопасность

Вопросы безопасности сети становятся с каждым днем все более и более актуальными.

К вопросом обеспечения безопасности следует отнести целый ряд мероприятий по обеспечению сохранности и целостности информации и ее носителей (компьютеров, дискет); защиты от проникновения посторонних лиц и перехвата ими закрытой информации.

6.1. Виды угроз

Угрозы информации можно разделить на следующие категории:

1. Неумышленное повреждение.
2. Сбои в работе оборудования.
3. Умышленное повреждение.
4. Несанкционированное подключение.
5. Перехват информации по побочным каналам.
6. Кража информации, имеющий конфиденциальный характер.

6.2. Ограничение доступа

При проектировании сети необходимо придерживаться принципа предоставления минимально достаточных прав доступа к служебной информации и техники.

6.3. Вирусы

Наиболее вероятным видом угроз, с которыми встречались и встречаются практически все пользователи - это компьютерные вирусы.

Увлекательная игра системных программистов по написанию системных программ, разделяющих между собой ресурсы компьютера, переросла в мощный инструмент атаки и защиты информации, доказательство своего уровня как программиста. Написать собственный вирус является показателем высшего уровня

системного программирования, требующего высокого уровня знаний аппаратно - программного устройства компьютера.

Большинство вирусов, разрабатываемых в целях самоутверждения, безвредны, хотя есть и исключения из этого правила.

Ряд вирусов специально разрабатывался для защиты и контроля распространения авторского программного обеспечения. Здесь можно приводить пример Лозинского, автора широко распространенных в нашей стране антивирусных программ и написавшего специальный вирус для контроля их незаконного копирования. Далеко не все авторы незаконно копируемых программ ограничиваются только контролем, но и принимают меры против незаконных пользователей.

Одним словом вирусы являются очень серьезной проблемой. Все программы, относимые к вирусам можно разделить на четыре основных класса:

1. Собственно вирусы. Программы, которые делают копии самих себя, прицепляясь к исполнимым файлам *(файловые вирусы*) или загрузочным областям дисков (*дисковые вирусы*).
2. Самокопирующиеся файлы. Эти программы размножаются по компьютерам, не прикрепляясь к файлам.
3. Троянские кони – программы, истинный смысл которых Вы узнаете только при их исполнении, остановить которое возможно далеко не всегда. Их деструктивные действия могут проявиться в произвольный момент, известный только автору троянской программы. Так как обычно троянские программы не обладают возможностью самовоспроизведения, то часто их к вирусам не относят, а выделяют в особый класс.
4. Макровирусы, вирусы написанные на макроязыках многих интегрированных пакетов, например MsWord, и меняющие функции его действий. Они существуют только в этих пакетах, но тоже представляют серьезную опасность, представьте себе ситуацию, когда в один прекрасный момент все Ваши текстовые документы окажутся испорченными.

Наиболее вероятным источником появления вирусов является копирование всяческих нелицензионно чистых программ, например, игрушек, которые в нашей стране мало кто покупает, либо посещение знакомых, которые этим увлекаются.

Борьба с вирусами сводится к следующим мероприятиям:

1. Ограничение загрузки программного обеспечения.
2. Его предварительную проверку на предмет наличия вирусов.

3. Периодическую проверку всех дисков компьютеров на наличие вирусов.

Активной мерой борьбы с вирусами являются резидентные антивирусы и аппаратный антивирус, встроенный в ПЗУ всех современных компьютеров. Они постоянно контролируют процессы, протекающие в компьютере, на наличие эффектов подозрительных на действие вирусов. Но полностью надеяться только на них очень опасно, количество вирусов постоянно увеличивается и средства борьбы с ними далеко не всегда поспевают за этими процессами.

6.4. UPS

Устройство UPS (источник бесперебойного питания) предназначено для поддержания электропитания, подключенного к нему устройства, при пропадании электропитания в сети.

Сервер является ключевым элементом любой сети и внезапное отключение его или нестабильная работа могут привести к потери значительной части информации, обрабатываемой в сети.

Сетевые операционные системы при работе открывают огромное количество файлов, частично храня их содержимое в оперативной памяти. При отключении электропитания содержимое незакрытых файлов может быть потеряно, а также возможно нарушение структуры каталогов и файлов. Это может привести к безвозвратной потери информации и выходу из строя программного обеспечения сетевой операционной системы.

UPS позволяет защитить сервер (рабочую станцию) от:

1. Бросков напряжения в сети.
2. Кратковременного пропадания напряжения в сети (от минуты до получаса, в зависимости от мощности и нагрузки).
3. Колебаний в уровне напряжения в сети.

В случае долговременного отсутствия питания в сети, UPS позволяет корректно завершить работу сетевой операционной системы или рабочей станции.

6.5. Резервное копирование

Одним из наиболее важных элементов обеспечения информационной безопасности в локальной сети является резервное

копирование системных и пользовательских разделов. Это главное правило при работе с компьютером.

В качестве средства для резервного копирования чаще всего используются накопители на магнитной ленте, редко меняющуюся информацию, например, свои рабочие архивы часто записывают на CD диски; если эти возможности недоступны, приходится обращаться к обычным магнитным дискам.

В зависимости от размеров (потребностей) Ваших или Вашей организации, Вам необходимо выбрать период для резервного копирования. Записанные резервные архивы рекомендуется хранить в другом безопасном месте (в другом офисе). Это будет хорошей стратегией при несчастном случае (например пожаре), если компьютер с информацией и Ваш офис будет поврежден или не доступен.

Встроенным в сетевые операционные системы средством резервного копирования является зеркальное отображение серверных дисков, информация в этом случае заносится одновременно на два разных физических диска.

6.6. Информационная безопасность

Современная информационная система крупной организации все больше становится ядром ее нормального функционирования. Все чаще и чаще компьютерам доверяют наиболее секретную и жизненно важную информацию. В то же время информационная система крупной организации является настолько сложным механизмом, что никто не сможет гарантировать доступность информации тем и только тем, кто обладает соответствующими правами. Причинами нарушения установленных прав доступа может быть халатность персонала, сбои в работе аппаратуры и, наконец, различные программные ошибки, наличием которых могут воспользоваться злоумышленники, желающие проникнуть в секреты организации, и компьютерные хулиганы, вскрывающие системы защиты из чисто спортивного интереса.

Большинство экспертов по безопасности рекомендуют многоуровневый подход к защите сетевых ресурсов, включая шифрование и аутентификацию.

Ни одна компьютерная система защиты информации не является абсолютно безопасной. Ключевым элементом в системе безопасности является администратор системы.

Существующие сетевые операционные системы в большинстве случаев в сочетании с некоторыми административно-техническими мероприятиями обладают достаточными встроенными средствами для защиты информации. Например, ОС WindowsNT сертифицирована Министерством обороны США по уровню С2.

Требования к операционной системе для получения сертификации по рейтингу С2.

1. Каждый пользователь должен быть уникальным образом идентифицирован в системе.

2. Система должна предоставлять средства идентификации и контроля за действиями пользователя в соответствии с определенными ему правами.

3. Владелец ресурса должен иметь возможность определения прав доступа к ресурсу и контроля за их выполнением.

4. Операционная система должна защищать находящиеся в памяти компьютера и принадлежащие одному процессу данные от их использования другими процессами.

5. После удаления файла с диска пользователи не должны иметь доступа к его данным, даже если дисковое пространство, ранее занятое удаленным файлом, выделяется для использования новым файлом.

6. Администратор системы должен иметь возможность аудита всех событий, связанных с защитой системы, а также действий отдельных пользователей. Правами доступа к данным аудита должен обладать ограниченный круг администраторов.

7. Система должна защищать себя от вмешательства, такого как модификация работающей системы или файлов, хранящихся на диске.

Требования уровня защиты С2 определены в издании Национального центра защиты компьютеров (National Computer Security Center NCSC) Министерства обороны США — Trusted Computer System Evaluation Criteria, известном также как “Оранжевая книга” (Orangebook). Независимо от того, предназначены ли операционные системы для использования в сети или автономно, для доступа в государственный сектор США, они должны быть сертифицированы согласно требованиям, описанным в “Оранжевой книге”.

Очевидно, что этот перечень не является полным: есть дополнительные требования, жизненно необходимые для эффективного управления средствами защиты средних и крупных сетей, а особенно — территориально распределенных. Среди них:

1. возможность централизованного контроля со стороны администратора за тем, какие и кем используются ресурсы — аудита использования ресурсов;

2. возможность централизованного управления привилегиями и правами;

3. возможность включения пользователей в группы,

4. возможность установления допустимого времени работы,

5. блокировка бюджетов при неверной регистрации,

6. возможность оперативного оповещения администратора о попытке несанкционированного проникновения в сеть,

7. установление временных ограничений на использование одной и той же учетной записи и ведение истории изменения параметров регистрации.

Windows NT Server отвечает всем этим требованиям, предоставляя возможность централизованного управления правами пользователей, применения средств защиты и аудита, в том числе и в географически распределенных сетях. Таким образом, администратор корпоративной сети может отслеживать соответствие действий пользователей выбранной политике безопасности и оперативно решать возникающие вопросы.

Пример более глубокого использования защиты в Windows NT Server — способность системы защищать данные, находящиеся в физической памяти компьютера. Windows NT Server предоставляет доступ к таким данным только программам, имеющим на это право. Если данные больше не содержатся на диске, система предотвращает несанкционированный доступ к той области диска, где они содержались, и никакая программа не получит доступа к данным, которыми оперирует в данный момент другое приложение в физической памяти машины.

Способы несанкционированного доступа к программам и данным в условиях компьютерной сети более многообразны, чем в автономных системах.

Основные пути получения несанкционированной информации это:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- применение подслушивающих устройств;
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- хищение носителей информации и производственных отходов;
- считывание данных в массивах других пользователей;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;

- мистификация (маскировка под запросы системы);
- использование программных ловушек;
- использование недостатков языков программирования и операционных систем;
- включение в библиотеки программ специальных блоков типа “троянский конь”;
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- внедрение и использование компьютерных вирусов.

Разъясните важность хранения параметров регистрации пользователей в тайне. Внутренний идентификатор пользователя и его идентификатор в сети не должны совпадать. Необходимо ввести в штат отдела информатизации аналитика по информационной безопасности. Каждый сотрудник организации должен быть лично знаком со специалистом по информационной безопасности. Рекомендуется ввести в штатное расписание одного аналитика на 60 сотрудников. В функции аналитика входит формирование политики обеспечения информационной безопасности и контроль за ее исполнением пользователями. Пользователи обязаны немедленно связаться с аналитиком в случае подозрения на взлом информационной системы.

Необходимо проводить независимую экспертизу для оценки выработанной политики безопасности.

Если есть сомнение, что разработанная политика безопасности неадекватно защитит корпоративную сеть, то лучше обратиться к сторонним специалистам, способным оценить как техническую, так и организационную сторону стратегии обеспечения безопасности.
Все эти меры являются эффективными в сочетании с надежной организацией защиты, предоставляемой самой операционной системой (Windows NT, UNIX, Net Ware ...).

6.7. Встроенные средства анализа работы сети в Windows

В состав Windows входит программа “инспектор сети”, которая позволяет Вам проследить подключение к Вашему компьютеру других пользователей, совместное использование файлов и каталогов.

Для запуска программы Вам необходимо: нажать кнопку “Пуск”, выбрать пункт “программы”, “стандартные”, “служебные программы”, “инспектор сети”. После запуска на рабочем столе откроется окно со следующим содержанием:

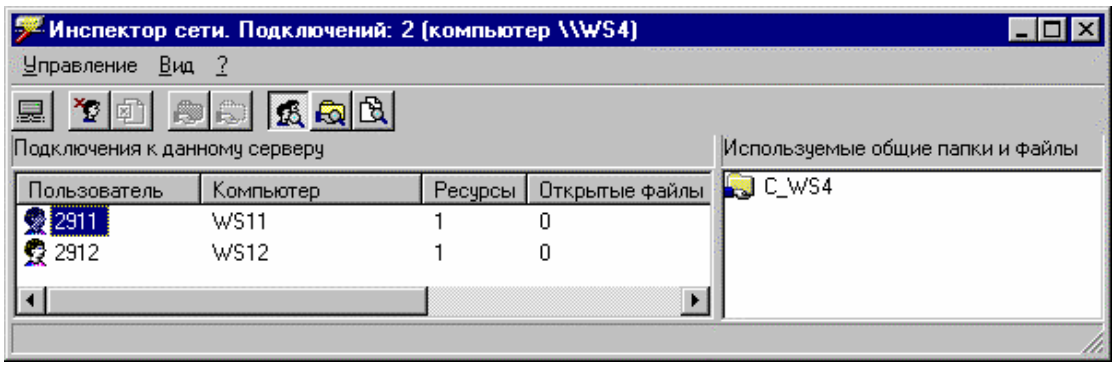


Рис. 5.2. Окно программы Инспектора сети

В данный момент мы видим, что к Вам подключились два пользователя 2911 и 2912.

Подсветив конкретного пользователя и нажав клавишу Del или выбрав соответствующую команду в меню, Вы отключите его от своей машины.

Вывод информации о подключении пользователя к компьютеру несколько отстает от момента подключения, поэтому программа позволяет только констатировать факт подключения.

6.8. Контрольные вопросы

Выберите правильный ответ и обоснуйте его.

Вопрос 1:

Что из приведенных мер обеспечивает безопасность данных в локальной сети от кражи?

1. UPS.
2. Резервное копирование.
3. Шифрование.
4. Ежедневный запуск антивирусных программ.

Вопрос 2:

Укажите самый бесполезный способ защиты информации?

1. Криптографические методы.
2. Установить пароль на загрузку компьютера.
3. Закрыть компьютер на замок.
4. Установить пароль на каждый документ, например, средствами MsWord.

Вопрос 3:

Как защитить программу от незаконного копирования?

1. Не допускать никого к своему компьютеру.
2. Написать собственную систему защиты.
3. Написать собственный вирус и встроить его в защищаемую программу.

4. Воспользоваться электронным ключом.

Вопрос 4:
Что даст Вам уверенность в информационной безопасности Ваших данных?

1. Знание математических основ, положенных в основу работы криптографической системы, которую Вы применили.
2. Пройти обучение по соответствующей специальности, например “информационная безопасность телекоммуникационных систем” СПбГУТ?
3. Самому разработать систему защиты, на одном из языков программирования.
4. Прочитать рекламу или научно-популярную статью о работе данной системы.

Вопрос 5:
Какие знания необходимо иметь для организации квалифицированной системы защиты информации?

1. Знание криптографии.
2. Знание языков программирования и особенностей организации компьютера.
3. Знание математики.
4. Знание иностранных языков.

6.9. Практическое задание

1. Практическое задание строится как сетевая игра, в которой участникам приходится выступать сразу в двух ролях: и защищать свою информацию, и пытаться произвести несанкционированное получение информации других участников игры.
2. Для проведения игры Вам необходима одноранговая локальная сеть, пароль на доступ по чтению дисков всех машин известен всем игрокам.
3. В установке Windows должна быть инсталлирована программа “инспектора сети”, возможности которой описаны в предыдущем разделе.

Порядок игры:

4. На компьютере необходимо создать файл с именем пользователя и расширением txt, например, WS1.txt. В этом файле необходимо разместить информацию о себе.
5. Спрятать этот файл в одном из каталогов жесткого диска компьютера.

6. Открыть доступ к дискам Вашего компьютера по чтению всем машинам сети и установит известный всем пароль, например all.
7. Запустить инспектор сети.
8. Через сетевое окружение пытаться войти в другие компьютеры участников игры, найти и скопировать их файлы (ws2.txt, ws3.txt и т.д.) в каталог своей школы, но при этом не дать скопировать свой файл. Как только в окне “инспектора сети”, заметите подключение к Вашей машине другого пользователя необходимо быстро его отключить, до того как он успеет найти и скопировать Ваш файл.
9. Выигрывает тот участник игры, кто скопирует больше всех файлов, а его файл скопируют наименьшее число раз.

7. Удаленный доступ

7.1. Модемы

Первые устройства для передачи сигналов от компьютеров по телефонным каналам применялись еще с 60-х годов.

Подключение к сети с помощью модема является простейшим способом связи практически с любым компьютером, оборудованным аналогичным или совместимым модемом. Модем преобразует компьютерные (цифровые) сигналы в аналоговые и обратно.

Модемы делятся на два типа: внешний и внутренний. Также модемы делятся по скорости работы. Максимальная скорость работы через модем по телефонным линиям 33600 бит/сек., такая скорость достигается только в том случае, если Вы подключены к новой (цифровой) АТС, и на пути сигнала от вашего модема было только одно преобразование. Внешний модем подключается к компьютеру через COM порт, внутренний модем вставляется в компьютер в слот материнской платы.

Достоинства внешнего модема:

1. Наличие индикаторных лампочек, позволяющих контролировать его работу.
2. Внешний модем это - отдельное устройство, его зависание не приводит к зависанию компьютера, достаточно включить/выключить модем.
3. Большинство внешних модемов оснащены спикером, позволяющим слышать абонента, если Вы по ошибке попали на обычный телефон.

Недостатки внешнего модема:

1. Более высокая стоимость по сравнению со встроенными модемами.
2. Требуется задействовать один из COM портов только для этой работы.

Достоинства внутреннего модема:

1. Стоимость внутреннего модема ниже стоимости внешнего модема.

Недостатки внутреннего модема:

1. Нет возможности контролировать процесс передачи информации.
2. Зависание модема, как правило, приводит к зависанию всего компьютера, и его придется перегружать.

7.2. Удаленное соединение в Windows 95

Для настройки удаленного подключения к Internet в Windows 95 Вам необходимо настроить протокол TCP/IP. Для этого необходимо выполнить следующие действия:

1. Установить модем и его обеспечение поставляемое в его комплекте. Проверить, что модем нормально виден из под Windows.
2. Добавить “Удаленный доступ к сети” (раздел “Связь” в “установке и удаление программ / Установка Windows”).
3. В разделе “Сеть” добавить клиента (Microsoft - клиент для сетей Microsoft), сетевую плату (Microsoft - Контроллер удаленного доступа) и протокол (Microsoft - TCP/IP).
4. В свойствах TCP/IP установить Адрес IP: Получить автоматически; Конфигурация Wins - отключить распознавание Wins, Шлюз - добавить шлюз XXX.X.XXX.XX, (номер Вашего шлюза, предоставленный Вашем провайдером). Конфигурация DNS - включить DNS, указать название главного компьютера, домена и порядка просмотра серверов DNS.
5. Закрыть раздел “сеть” с подтверждением изменений.

В настройках “Удаленного доступа к сети” Вам необходимо выполнить следующие действия:

1. Создать новое соединение. Для этого Вы должны щелкнуть мышкой на значке “Новое соединение” в папке “Мой компьютер”, “Удаленный доступ к сети”. Вводим номер телефона, к которому производится подключение.
2. В свойствах, раздел “Тип сервера” Вам необходимо включить режим программного сжатия данных.
3. Дважды щелкнуть на созданном Вами соединении, в открывшемся окне заполнить поле “Имя пользователя” и ввести пароль.
4. Для домашнего компьютера имеет смысл установить флаг “Сохранить пароль”.

Обычно порядок действий, необходимых для создания удаленного соединения в наиболее распространенных программных продуктах, указывается в инструкции которая Вам предлагается при покупке адреса и услуг провайдера сети Internet. Кроме того, Вам должны указать телефон по которому осуществляется подключение, пароль, и должны зарегистрировать Ваше имя в сети.

7.3. Контрольные вопросы

Выберите правильный ответ и обоснуйте его.
Вопрос 1:
Возможно ли реализовать удаленный запуск Windows 95 на бездисковой станции с помощью модема?
1. Возможно, если прошить в ПЗУ модема BOOTROM.
2. Невозможно.
3. Если и возможно, то займет очень много времени.
4. Возможно, но без запуска графической оболочки.

Вопрос 2:
Имеет ли смысл, на ПЭВМ, подключенной к локальной сети с помощью модема, удаленно запускать на своем компьютере Ms Word с сервера?
1. Это оправдано и позволит Вам сэкономить место на жестком диске своего компьютера.
2. Возможно, ради использования общих настроек и редактируемых файлов.

3. Будет затруднительно, в связи с низкой скоростью передачи информации.
4. Невозможно в принципе.

Вопрос 3:

Возможен ли одновременный разговор и передача данных по модему между пользователями двух удаленных компьютеров.

1. Невозможно.
2. Данные и разговор будут проходить, но при этом искажать друг друга.
3. Возможно, если использовать уплотнение канала и арендовать у телефонной станции дополнительный телефонный номер.
4. Возможно, если использовать новый модем со стандартом передачи информации со скоростью 56к, так как при разговоре используется скорость только до 33,6 кб.

Вопрос 4:

Можно ли организовать полноценную компьютерную сеть на основе модемного соединения компьютеров между собой и сервером?

1. Можно, если использовать шинную топологию сети.
2. Можно, если применить шинную топологию сети.
3. Невозможно из-за низкой пропускной способности модемного соединения.
4. Невозможно одновременное подключение большого числа модемов к одному компьютеру.

7.5. Практическое задание

Создайте удаленное соединение с Web сервером УИЦ ИТТ, или указанным Вам тестовым адресом. Web сервер УИЦ ИТТ обслуживает это соединение только во время Вашего учебного занятия. Сразу после конца занятия данный вход будет уничтожен, телефон отключен от дополнительной линии, так что просьба: не занимать зря телефонную станцию. Имя пользователя и пароль, и номер телефона, включенного на момент занятия, будет Вам предоставлен в задании.

8. Протоколы

Протоколы делятся на три основных типа: сетевые протоколы, транспортные протоколы, прикладные протоколы.

Сетевые протоколы предназначены для передачи информации по сети, адресации и маршрутизации пакетов.

Транспортные протоколы предназначены для передачи данных между компьютерами.

Прикладные протоколы предназначены для организации взаимодействия приложений.

Рассмотренные ниже протоколы являются комбинациями указанных протоколов. Например, в протокол TCP/IP входит сетевой протокол IP, транспортный протокол TCP, протоколы приложений FTP (передача файлов), SMTP (почтовый протокол), SNMP (протокол управления сетью). Остальные рассмотренные протоколы также включают, как составные части, аналогичные по функциям транспортные, сетевые и прикладные протоколы.

8.1. IPX

Протокол IPX (межсетевой обмен пакетами) является основным протоколом для сетей типа Novell NetWare, протокол поддерживается также фирмой Microsoft.

Достоинства протокола:

1. Может использоваться совместно с другими протоколами, что обеспечивает легкий переход с одной сети на другую. Например, в сети построенной на сервере Novell NetWare, кроме серверной сети, можно одновременно пользоваться одноранговой сетью, построенной на другом протоколе, например TCP/IP.
2. Прост в инсталляции и настройке.
3. Поддерживает маршрутизацию между сетями.
4. Самый быстрый протокол для сетей со сложной конфигурацией.

Недостатки протокола:

1. Отсутствие централизованной службы выделения адресов может привести к путанице в сети.

8.2. TCP/IP

Разработан в 1969 году, по заказу министерства обороны США. Основное назначение протокола в настоящее время - глобальная сеть Internet и организация межсетевого взаимодействия.

Достоинства протокола:

1. Пригоден для всех типов компьютеров и серверов.
2. Поддерживается всеми типами операционных систем.
3. Обеспечивает работу с Internet.
4. Максимальный уровень маршрутизации сообщений.
5. Обеспечивает динамическое распределение сетевых адресов.
6. Поддержка специализированных протоколов глобальной сети Internet.
7. Максимальный уровень контроля ошибок

Недостатки протокола:

1. Проблема регистрации центральных доменов и их уникальных номеров (в следствие широкого распространения глобальной сети Internet).
2. Более сложная инсталляция протокола, по сравнению с другими.
3. Скорость работы ниже, чем у IPX или NetBIOS. TCP/IP - самый медленный из протоколов, поддерживаемых Windows.
4. В связи с тем, что протокол изначально не разрабатывался с учетом требований безопасности, то всегда существует угроза использования отдельных особенностей протокола для нарушения безопасности использующих этот протокол компьютеров и сетей.

8.3. NetBIOS

Протокол NetBIOS предназначен для небольших сетей с одним сервером. Протокол разработан в середине 80-х годов фирмой IBM.

Достоинства протокола:

1. Высокая скорость работы в небольших сетях.
2. Самонастройка.
3. Высокий уровень защиты от ошибок.
4. Минимум ресурсов.

Недостатки протокола:

1. Отсутствуют средства маршрутизации пакетов.
2. Чрезвычайно мало средств диагностики и анализа работы сети.
3. Могут возникать проблемы со связями, с сетями, использующими другой протокол.

В настоящее время данный протокол используется сравнительно редко.

8.4. Контрольные вопросы

Выберите правильный ответ и обоснуйте его.

Вопрос 1:

Какой протокол необходимо установить на Вашей машине для работы в одноранговой сети, реализованной средствами Windows95?

1. NetBIOS.
2. IPX.
3. TCP/IP.

Вопрос 2:

Какой протокол обеспечит максимальную скорость передачи информации по сети?

1. NetBIOS.
2. IPX.
3. TCP/IP.

Вопрос 3:

Какой протокол обеспечит максимальную скорость передачи информации по сети со сложной гибридной топологией и наличием маршрутизаторов?

1. NetBIOS.
2. IPX.
3. TCP/IP.

Вопрос 4:

Какие протоколы могут работать совместно в одной сети?

1. NetBIOS.
2. IPX.
3. TCP/IP.

9. Глобальные сети

9.1.Глобальные сети

В настоящее время все сети объединяются в единую глобальную сеть. Для объединения локальных сетей в глобальную сеть используются высокоскоростные глобальные связи.

Используются следующие типы соединений:

1. Аналоговые соединения - соединения с помощью телефонных линий, посредством модемов.
2. Цифровые соединения - используются цифровые технологии на всем протяжении. Могут использоваться цифровые телефонные линии или выделенные линии.
3. Коммутированные соединения - используется коммутация и последовательная передача пакетов.

9.2. Шлюзы, маршрутизаторы

Шлюз – устройство, позволяющее организовать обмен данными между двумя сетями, использующими различные протоколы взаимодействия. С помощью шлюзов организуется подключение пользователей локальной сети организации к глобальной, например, к Internet.

Маршрутизатор– устройство, позволяющее оптимизировать направление передачи информации от одного пользователя другому. Кроме того маршрутизатор выполняет функции фильтрации сообщений, направляя в каждую сеть только ту информацию, которая ей адресована.

9.3. Мосты

Мост – устройство, соединяющее две сети, использующие Самый простой способ объединения – это отдельный компьютер с несколькими сетевыми картами и специальным программным обеспечением. Мост может соединять сети различных топологий, но работающие под управлением однотипных сетевых операционных систем.

Различают следующие разновидности мостов:

Локальный мост - соединяет локальные сети.

Внутренний локальной мост – выполняет логического организации сети, физически сеть остается одна. Реализуется чисто программным путем.

Удаленный мост – соединяет, территориально разнесенные, сети с помощью модемов или других каналов связи.

9.3. Глобальная сеть Internet

Internet - это всемирная сеть, используемая на сегодняшний день всеми: от правительства до образовательных учреждений и частных лиц. Эта сеть не имеет конкретного владельца, и доступ к ней может получить любой, основная часть расходов сети оплачивается правительством США, которая рассматривает Internet как важнейший элемент распространения своего влияния и образа мысли.

Уже сейчас пользователями сети Internet являются более 50 миллионов человек, во всех уголках Земного шара.

Основными услугами предлагаемыми в сети Internet являются: электронная почта, система новостей, информационные страницы, система поиска информации.

Каждая станция (хост) в сети Internet имеет уникальный цифровой адрес. Запоминать его довольно трудно, поэтому чаще используются его символьная запись выполненная в определенном соглашении об именах.

Доменная система имен имеет иерархическую структуру, разделителем выступает символ “точка”:

<Имя сервера>.<название сегмента сети>.<Имя домена>,

например: fem.sut.ru, сервер факультета экономики и управления СПбГУТ, по имени сразу видно что данный сервер расположен в

России (ru), главная организация СПб университет телекоммуникаций (sut), и наконец название сервера - fem.

Кроме этого у пользователей, групп пользователей, или даже небольших организаций могут быть собственные домашние страницы. Имя формируется следующим образом - <Полное имя сервера>/~<Имя пользователя>.

Например: fem.sut.ru/~Krasov - сраниуа группы ИКТО, расположенная на сервере ФЭУ СПбГУТ. Признак домашней страницы символы "/~" со следующим за ним именем пользователя.

Кроме домашней страницы, у пользователя обычно есть адрес электронной почты, строящейся по аналогичному принципу - <Имя пользователя>@<Полное имя сервера>. Пример: Krasov@fem.sut.ru.

Подробнее о работе с сетью Internet можно прочитать в следующих методических пособиях для этого курса [3-4].

9.4. Контрольные вопросы

Выберите правильный ответ и обоснуйте его.

Вопрос 1:

Необходим ли мост для соединения дух компьютерных классов, построенных на шинной топологии?

1. Без него соединение двух сетей будет невозможно.
2. В данной задаче установка моста не требуется.
3. Установка моста будет необходимо если в сетях работают сервера с различными сетевыми операционным системами, например, Novell и WindowsNT.
4. Установка моста между этими сетями только замедлит обмен сообщениями.

Вопрос 2:

Что позволит снизит время пересылки файлов в очень большой организации с сложной гибридной топологией сети?

1. Подключение локальных сетей отделов только через шлюзы.
2. Установка маршрутизатров в наиболее важных узлах сети.

Вопрос 3:

Укажите правильные имена серверов сети Internet?

1. sut.fem.krasov.
2. error.ru

3. inform@sut.ru
4. test~/fem.sut.ru

Вопрос 4:
Не богатой организации требуется представить себя в сети Internet.
1. Необходимо создавать и регистрировать собственный Web сервер.
2. Необходимо создать собственный Web сервер но не регистрировать его имя, а ограничиться цифровым именем.
3. Необходимо создать домашнюю страницу на одном из Web серверов.
4. Необходимо ограничится адресом электронной почты.

Вопрос 5:
Укажите правильный адрес электронной почты?
1. ddd.ru/Andrey
2. ddd.ru/~Andrey
3. Andrey@ddd.ru
4. Andrey.ddd.ru

10. Итоговая работа по курсу

10.1. Постановка задачи

Итоговая работа по курсу “Основы построения сетей” представляет собой квалификационную работу. Работа выполняется по бригадой из двух трех учащихся, защита работы проходит индивидуально.

В качестве задания на итоговую работу предлагается составить проект локальный сети, для гипотипической организации (подразделения) и написать пояснительную записку объемом 5-10 страниц с его обоснованием.

Данная пояснительная записка сдается в электронном и, по возможности, в бумажном виде. Используется редактор MS Word. При оформлении необходимо придерживаться предложенных требований по оформлению работы, так как данный отчет является квалификационной работой и по работе с MS Word.

10.2. Составление проекта

При составлении проекта целесообразно придерживаться следующего порядка действий:

1. По поставленной задачи четко выписать требования к проектируемой сети.
2. Выбор типа сети: серверная и ли одноранговая.
3. С учетом размещения компьютеров, выбор топологии сети.
4. Выбор типа сервера.
5. Составление проекта, размещения компьютеров, прокладки кабелей.
6. Администрирование сети: какие пользователи и с какими правами должны работать в сети, выделение групп пользователей.
7. Меры по обеспечению безопасности сети.
8. Смета расходов на приобретение оборудования.
9. Заключение, оценка выполнения проекта.

Заключение

Значение сетевых технологий возрастает год от года. Одиночный компьютер больше не способен обрабатывать все возрастающие объемы непрерывно поступающей информации. В этой связи возрастает роль коллективной обработки потоков информации, разработки коллективный проектов. Объединение их в готовый продукт невозможно без применения сетевых технологий. Сеть снимает территориальные проблемы, обмен информацией можно производить не сходя со своего рабочего места.

Знания сетевых технологий кране необходимы современному специалисту. Предложено Вашему вниманию пособие не может и не ставит перед собой цель заменить серьезные книги по этому вопросу. Материл рассматриваемый в пособии и входящий в стандарт школьного курса информатики, призван осветить круг решаемых задач, основные возможности и преимущества применения сетевых технологий.

Литература

1. Дж. Челлис, Ч. Перкинс, М. Стриб. Основы построения сетей. М.Лори, 1997, - 320 с.
2. Э. Титтел, К. Хадсон, Дж. Стюард. Networking Essentials. Сертификационный экзамен - экстерном (экзамен 70-058). СПб.: Питер Ком, 1999, -384 с.
3. А.В. Красов. Сеть Internet. В стадии разработки.
4. А.В. Красов. Разработка Web страниц. В стадии разработки.

Оглавление