

Методические указания



Форма
Ф СО ПГУ 7.18.2/05

Министерство образования и науки Республики Казахстан
Павлодарский государственный университет им. С. Торайгырова
Кафедра информатики и информационных систем

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к лабораторным работам

по дисциплине Компьютерные сети

для студентов специальности 050602 –Информатика

Павлодар

Лист утверждения к
методическим указаниям



Форма
Ф СО ПГУ 7.18.1/05

УТВЕРЖДАЮ
Декан ФФМиИТ
_____ С.К. Глеуменов
«__» _____ 200_ г.

Составитель: ст. преподаватель Токкожина М.А.
(должность, уч. степень, звание, подпись)

Кафедра Информатика и информационные системы

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к лабораторным работам

по дисциплине Компьютерные сети

для студентов специальности 050602 – Информатика

Рекомендовано на заседании кафедры от «__» _____ 200_ г.

Протокол № _____

Заведующий кафедрой _____ Нурбекова Ж.К.
(подпись)

Одобрена методическим советом факультета ФФМиИТ

«__» _____ 200_ г. Протокол № _____

Председатель МС _____ Кишубаева А.Т.
(подпись)

Лабораторная работа №1

Совместное использование ресурсов сети. Идентификация компьютера в сети. Смена имени компьютера. Просмотр и поиск компьютеров в сети, и доступ к их ресурсам. Подключение сетевых дисков. Назначение компьютера координатором в сети. Контроль доступа к ресурсам пользователя инспектором сети Microsoft. Просмотр сетевых ресурсов Microsoft и подключение к сетевым дискам из командной строки

Цель работы: Создание различных видов сетей

Теоретические сведения

Данная топология относится к наиболее простым и широко распространенным топологиям. В ней используется одна сетевая кабель, именуемый *магистралью* или *сегментом*, вдоль которого подключены все РС сети (рис. 3.1).

1. При передаче пакетов данных каждый компьютер адресует его конкретному компьютеру ЛВС (PC_k), передавая его по сетевому кабелю в виде электрических сигналов.

2. Пакет в виде электрических сигналов передается по шине в обоих направлениях всем компьютерам сети.

3. Однако, информацию принимает только тот адрес, который соответствует адресу получателя, указанному в заголовке пакета. Так как в каждый момент времени в сети может вести передачу только одна РС, то производительности ЛВС зависит от количества РС, подключенных к шине. Чем их больше, тем больше ожидающих передачи данных, тем ниже производительности сети. Однако, нельзя указать прямую зависимость пропускной способности сети от количества РС, так как на нее также влияет:

- характеристики аппаратного обеспечения РС сети;
- частота, с которой передают сообщения РС;
- тип работающих сетевых приложений;
- тип кабеля и расстояние между РС в сети

Шина – пассивная топология. Это значит, что компьютеры только «слушают» передаваемые по сети данные, но не перемещают их от отправителя к получателю. Поэтому, если один из компьютеров выйдет из строя, это не скажется на работе всей сети (!).

4. Данные в виде электрических сигналов распространяются по всей сети от одного конца кабеля к другому, и, достигая конца кабеля, будут отражаться и занимать шину, что не позволит другим компьютерам осуществлять передачу.

5. Чтобы предотвратить отражение электрических сигналов, на каждом конце кабеля устанавливаются терминаторы (Т), поглощающие сигналы, прошедшие по шине.

6. При значительном расстоянии между РС (например, 180 м для тонкого коаксиального кабеля) в сегменте шины может наблюдаться ослабление электрического сигнала, что может привести к искажению или

потере передаваемого пакета данных. В этом случае исходный сегмент следует разделить на два, установив между ними дополнительное устройство – *репитер (повторитель)*, который усиливает принятый сигнал перед тем, как послать его дальше .

Правильно размещенные на длине сети повторители позволяют увеличить длину обслуживаемой сети и расстояние между соседними компьютерами. Следует помнить, что все концы сетевого кабеля должны быть к чему-либо подключены: к РС, терминатору или повторителю.

Разрыв сетевого кабеля или отсоединение одного из его концов приводит к прекращению функционирования сети. Сеть «падает». Сами РС сети остаются полностью работоспособными, но не могут взаимодействовать друг с другом. Если ЛВС на основе сервера, где большая часть программных и информационных ресурсов хранится на сервере, то РС, хотя и остаются работоспособными, но для практической работы малопригодны.

Топология типа «звезда»

При топологии «звезда» все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту – концентратору (Hub)

Пакеты данных от каждого компьютера направляются к центральному концентратору. Он, в свою очередь, перенаправляет пакеты к месту назначения. Основное достоинство этой топологии в том, что если повреждена какая-либо РС или отдельное соединение между РС и концентратором, вся сеть остается работоспособной. Положительным является и то, что подключение кабеля и управление конфигурацией сети централизовано, а также просто конфигурировать сеть при добавлении новых РС. Как недостатки организации такой топологии следует отметить следующее:

- Так как все РС подключены к центральной точке, то для больших ЛВС значительно увеличивается расход кабеля.
- Если поврежденным оказался сам концентратор, то нарушится и работа всей сети, хотя РС останутся работоспособными.

Концентраторы являются центральным узлом в топологии «звезда». Однако в настоящее время они становятся одним из стандартных компонентов большинства ЛВС.

Среди концентраторов выделяют активные и пассивные. *Активные* концентраторы регенерируют и передают сигналы, также как это делают репитеры. Иногда их называют еще *многопортовыми репитерами*. Они имеют от 8 до 12 портов для подключения компьютеров.

Пассивные концентраторы – это монтажные панели или коммутирующие блоки. Они просто пропускают через себя сигнал, не усиливая и не восстанавливая его. Пассивные, в отличие от активных, не надо подключать к источнику питания. *Гибридными* называют конденсаторы, к которым можно подключить кабели различных типов.

Концентраторы можно соединить между собой. При такой топологии

разрыв кабеля, подключенного к концентратору, нарушит работу только одного конкретного сегмента сети .

Топология типа «кольцо»

При этой топологии сеть замкнута, образуя неразрывное кольцо (рис. 3.5). Поэтому у кабеля просто не может быть свободного конца, к которому надо подключить терминатор. Начав движение в какой-либо точке кольца (PC₁), пакет данных в конце концов попадает в его начало. Из-за такой особенности данные в кольце движутся всегда в одном направлении.

В отличие от пассивной топологии «шина», здесь каждый компьютер выступает в роли репитера, усиливая сигналы и передавая их следующему компьютеру. В отличие от «звезды» «кольцу» необходим неразрывный путь между всеми сетевыми PC. Поэтому при выходе из строя какой-либо одной PC сеть прекращает функционировать.

Другое слабое место «кольца» состоит в том, что данные проходят через каждый сетевой компьютер, давая возможность "не очень хорошим" людям заниматься перехватом информации, не предназначенной посторонним. Кроме того, изменение конфигурации сети или подключение новой PC требует остановки всей сети.

Задание

Имитационная модель создается на языке программирования высокого уровня «Pascal 7.0» или «Delphi». Модель должна:

- нарисовать на экране детальную иллюстрацию заданной топологии;
- подробно промоделировать (путем динамизации изображения) на экране заданный процесс передачи данных с одного компьютера на другой;
- быть быстрой и красивой, компактной, с подробными комментариями.

1 Шина

2 Звезда

3 Кольцо

4 Шина с репитером

5 Кольцо с хабом

Лабораторная работа №2

Типы сетей. Одноранговая, двухранговая, комбинированная, гетерогенная сеть Microsoft и NetWare. Регистрация входа в сеть. Установка клиента Microsoft.

Цели занятия: получить представление об основных типах сетей. Изучить одноранговые, двухранговые и комбинированные сети.

Теоретическая часть

Комбинированные топологии

В настоящее время используются топологии ЛВС, которые комбинируют компоновку сети по принципу шины, звезды и кольца. При этом широкое применение находят концентраторы, использование которых дает ряд существенных преимуществ:

- простота изменения или расширения сети, так как достаточно просто подключить еще один компьютер или концентратор;
- возможность подключения кабелей различных типов;
- централизованный контроль за работой сети и сетевым трафиком, так как во многих сетях активные концентраторы наделены диагностическими возможностями, позволяющими определить работоспособность соединения.

Звезда –шина (star-bus) – это комбинация топологий «шина» и «звезда». Чаще всего это выглядит так: несколько сетей с топологией «звезда» объединяются при помощи магистральной шины.

В этом случае выход из строя одного компьютера не окажет никакого влияния на сеть. Остальные компьютеры по-прежнему взаимодействуют друг с другом. Выход из строя концентратора повлечет за собой остановку подключенных только к нему компьютеров и концентраторов. Такая топология очень удобна даже для небольших офисов, когда компьютеры в одном помещении подключаются к собственным концентраторам с помощью витой пары, а помещения (концентраторы) между собой соединяются только одним сетевым кабелем (витой парой, коаксиальным или оптическим кабелем).

Звезда-кольцо (star-ring) – кажется похожей на звезду-шину. И в том, и в другом случае компьютеры подключены к концентратору, который фактически формирует кольцо или шину.

Сравнительные характеристики топологий.

Существует множество факторов, которые необходимо учитывать при выборе подходящей топологии. Однако многие из этих факторов противоречивы. В приведенной ниже табл. 3.1 собраны основные достоинства и недостатки каждой из топологий..

Таблица 3.1

Сравнительные характеристики рассмотренных топологий.

Топология	Преимущества	Недостатки
Шина	<ul style="list-style-type: none"> - экономный расход кабеля; - недорогая и несложная в использовании среда передачи; - простота и надежность; - легкая расширяемость. 	<ul style="list-style-type: none"> - при значительных объемах трафика уменьшается пропускная способность; - трудная локализация проблем; - выход из строя кабеля остановит работу пользователей.
Кольцо	<ul style="list-style-type: none"> - все РС имеют равный доступ; - количество пользователей не сказывается на производительности. 	<ul style="list-style-type: none"> - выход из строя одной РС выводит из строя всю сеть; - трудно локализовать проблемы; - изменение конфигурации сети требует остановки всей сети.
Звезда	<ul style="list-style-type: none"> - легко модифицировать сеть, добавляя новые РС; - централизованный контроль и управление; - выход из строя РС не влияет на работу сети. 	<p>Выход из строя центрального концентратора выводит из строя всю сеть.</p>

Задание:

1. Внимательно прочитайте теоретический материал изложенный в данной лабораторной работе.
2. Составить сравнительную характеристику выше описанных типов сетей.
3. Сделайте вывод:какая сеть лучше, какая хуже, почему.
4. Ответьте на контрольные вопросы.

Контрольные вопросы

1. Какие виды сетей вы знаете
2. Какие выводы вы сделали для себя

Лабораторная работа №3

Профили пользователей. Профили пользователей Windows 9x/ME. Сеть Novell NetWare. Регистрация в WindowsNT. Учетные записи пользователей WindowsNT. Учетные записи групп.

Цели занятия: получить представление об основных профилях пользователей Windows 9x/ME. Сеть Novell NetWare. Регистрация в WindowsNT.

Теоретическая часть

Каждый сетевой уровень подчиняется определенному сетевому протоколу, определяющему набор сетевых служб, присущих данному уровню. Короче говоря, *сетевая служба* – это набор функций, которые уровень выполняет для вышележащего уровня (например, коррекция ошибок).

С другой стороны, *протокол* – это правила, которым должен следовать уровень, чтобы реализовать сетевую службу.

Пример. Чтобы отправить кому-либо письмо, мы пишем адрес на конверте. Таким образом, функция адреса заключается в обеспечении правильной доставки. Формат, в котором пишется адрес, строго определен:

- 1-я строка – город,
- 2-я строка – улица, дом,
- 3-я строка – кому.

Почтовые работники ожидают, что на второй строке будет указана улица, а за ней – номер дома. Формат адреса на конверте следует определенному протоколу. Сетевая служба таким же образом определяет выполнение какой-либо функции или задачи (определение ошибки или доставки сообщения).

Сетевой протокол описывает формат данных или пакетов данных, т. е. правила оформления, которым данные должны подчиняться, чтобы программное обеспечение выполняло ту или иную функцию или сетевую службу (для случая коррекции ошибок протокол описывает, какие ошибки сетевая служба должна исправлять).

Набор свойств и функций, которым обладает определенный сетевой уровень, называется *сетевой службой*. Каждый сетевой уровень запрашивает определенную сетевую службу от нижележащего уровня. Протокол уровня определяет структуру данных и формат пакета для выполнения запрашиваемой сетевой службы.

Привязка протоколов

Процесс, который называется привязкой, позволяет с достаточной гибкостью настраивать сеть, т. е. сочетать протоколы и платы сетевых адаптеров, как того требует ситуация.

Так, например, Ваш компьютер является членом рабочей группы одноранговой сети на базе Windows 95, и обмен данными осуществляется по протоколу NetBEUI. Если помимо этого Вам необходим доступ на сервер

Вашей организации, работающей под управлением Novell NetWare, то первое, что необходимо сделать – установить на Вашем компьютере соответствующий протокол – IPX/SPX.

Таким образом, два стека протоколов должны быть привязаны к одной плате сетевого адаптера – NetBEUI и IPX / SPX. При подключении к глобальной сети Интернет на Вашем компьютере дополнительно должен быть установлен еще один протокол TCP / IP.

Задание:

1. Внимательно прочитайте теоретический материал изложенный в данной лабораторной работе.
2. Составить сравнительную характеристику выше описанных понятий.
3. Ответьте на контрольные вопросы.

Контрольные вопросы

1. Что такое протокол?
2. Виды протоколов
3. Сравнительный протоколов.

Лабораторная работа №4

Защита сетевых ресурсов Windows9x. Реестр Windows 98/ME. Домены WindowsNT. Настройка среды WindowsNT. Защита сетевых ресурсов с помощью прав доступа к общим папкам. Защита сетевых ресурсов разрешениями NTFS. Сетевая печать. Установка и настройка сетевого принтера.

Цели занятия: получить представление об основных защитах сетевых ресурсов

Теоретическая часть

ЛВС имеют свойство перерастать начальные проекты. С ростом компаний растут и ЛВС. Изменение профиля деятельности или организации работы компании могут потребовать переконфигурации сети. Это становится очевидным, когда:

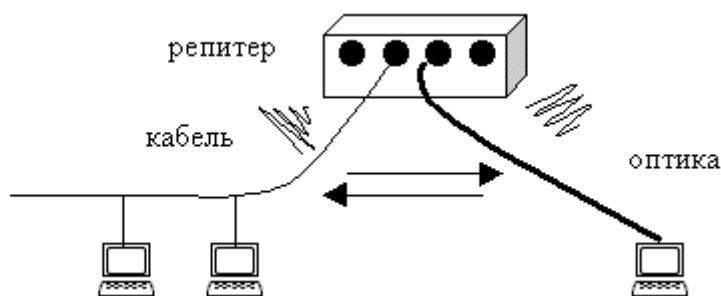
- недопустимо долго документы стоят в очереди на сетевой принтер;
- увеличилось время запроса к БД;
- изменились требования по защите информации и т. д.

Сети не могут расширяться за счет простого добавления рабочих станций и прокладки кабеля. Любая топология или архитектура имеет свои ограничения. Однако существуют устройства, которые могут:

- сегментировать ЛВС так, что каждый сегмент станет самостоятельной ЛВС;
- объединять две ЛВС в одну;
- подключать ЛВС к другим сетям для объединения их в интернет.

К таким устройствам относятся: репитеры, мосты, маршрутизаторы, мосты-маршрутизаторы и шлюзы.

Репитеры



Это устройства, которые принимают затухающий сигнал из одного сегмента сети, восстанавливают его и передают в следующий сегмент, чем повышают дальность передачи сигналов между отдельными узлами сети. Репитеры передают весь трафик в обоих направлениях и работают на физическом уровне модели OSI. Это означает, что каждый сегмент должен использовать одинаковые: форматы пакетов, протоколы и методы доступа. То есть, с помощью репитера можно объединить в единую сеть два сегмента Ethernet и невозможно Ethernet и Token Ring.

Однако репитеры позволяют соединять два сегмента, которые используют различные физические среды передачи сигналов (кабель – оптика, кабель – пара и т. д.). Некоторые многопортовые репитеры работают как многопортовые концентраторы, соединяющие разные типы кабелей.

Применение репитеров оправдано в тех случаях, когда требуется преодолеть ограничение по длине сегмента или по количеству РС. Причем ни один из сегментов сети не генерирует повышенного трафика, а стоимость ЛВС – главный фактор. Связано это с тем, что репитеры не выполняют функций: изоляции и фильтрации.

Так передавая из сегмента в сегмент каждый бит данных, они будут передавать и искаженные пакеты, и пакеты, не предназначенные этому сегменту. В результате проблемы одного сегмента скажутся и на других. Т.е. применение репитеров не обеспечивает функцию изоляции сегментов.

Кроме того, репитеры будут распространять по сети все широковещательные пакеты. И если устройство не отвечает на все пакеты или пакеты постоянно пытаются достичь устройств, которые никогда не отзываются, то производительность сети падает, т. е. репитеры не осуществляют фильтрацию сигналов.

Мосты

Мост – это устройство комплексирования ЛВС. Эти устройства, как и репитеры, могут

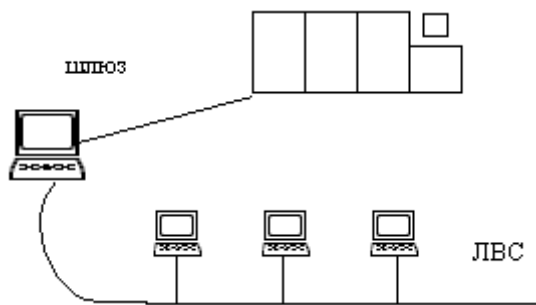
- увеличивать размер сети и количество РС в ней;
- соединять разнородные сетевые кабели.

Однако принципиальным их отличием является то, что они работают на *канальном* уровне модели OSI, т. е. на более высоком, чем репитеры и учитывают больше особенностей передаваемых данных, позволяя:

- восстанавливать форму сигналов, но делая это на уровне пакетов;
- соединять разнородные сегменты сети (например, Ethernet и Token Ring) и переносить между ними пакеты;
- повысить производительность, эффективность, безопасность и надежность сетей (что будет рассмотрено ниже).

Принципы работы мостов

Работа моста основана на принципе, согласно которому все узлы сети имеют уникальные сетевые адреса, и мост передает пакеты исходя из адреса узла назначения



Управляя доступом к сети, мост:

- слушает весь трафик;
- проверяет адрес источника и получателя пакета;
- строит таблицу маршрутизации;
- передает пакеты на основе адреса узла назначения.

Мост обладает некоторым «интеллектом», поскольку изучает, куда направить данные. Когда пакеты передаются через мост, адреса передатчиков сохраняются в памяти моста, и на их основе создается таблица маршрутизации.

В начале работы таблица пуста. Затем, когда узлы передают пакеты, их адреса копируются в таблицу. Имея эти данные, мост изучает расположение компьютеров в сегментах сети.

Прослушивая трафик всех сегментов, и принимая пакет, мост ищет адрес передатчика в таблице маршрутизации. Если адрес источника не найден, он добавляет его в таблицу. Затем сравнивает адрес получателя с БД таблицы маршрутизации.

- Если адрес получателя есть в таблице и адресат находится в одном сегменте с источником, пакет отбрасывается. Эта фильтрация уменьшает сетевой трафик и изолирует сегменты сети.
- Если адрес получателя есть в таблице, но адресат и источник находятся в разных сегментах, мост передает пакет через соответствующий порт в нужный сегмент.
- Если адреса нет в таблице, пакет ретранслируется во все сегменты, исключая тот, откуда был принят.

Короче говоря, если мост знает о местоположении узла – адресата, он передает пакет ему. В противном случае – транслирует пакет во все сегменты.

Рассмотренный вариант соответствует наиболее простым, так называемым прозрачным мостам. В настоящее время находят применение мосты с алгоритмом остоного дерева, мосты с маршрутизацией от источника и др.

Назначение мостов

1. Мосты позволяют увеличить *дальность* охвата сети, работая в качестве повторителей. При этом допускается каскадное соединение ЛВС через мосты. Причем эти ЛВС могут быть разнородны.

2. Использование мостов повышает *производительность* сети вследствие возможности ее *сегментации*. Т. к. мосты способны фильтровать пакеты согласно некоторым критериям, то большая сеть делится на несколько сегментов, соединенных мостами. Два небольших сегмента будут работать быстрее, чем один большой, т. к. трафик локализуется в пределах каждого сегмента.

3. Применение мостов повышает *эффективность* работы сети, т. к. для каждой подсети (сегмента) можно использовать разные топологии и среды передачи, а затем их объединять мостами.

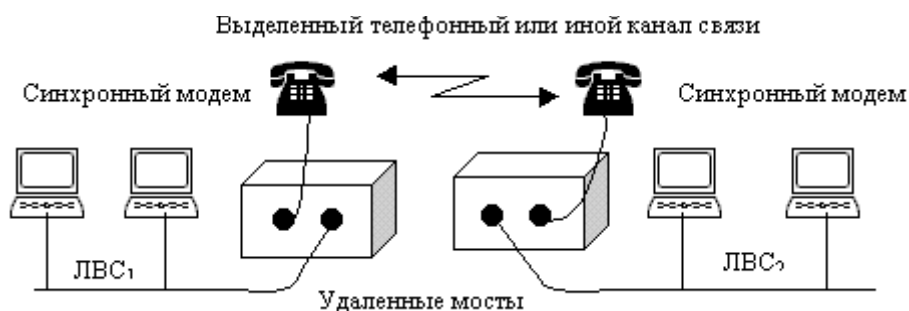
Так, например, если в отдельных отделах ПК соединены витыми парами, то мостом эти подсети можно соединить с корпоративной ЛВС оптической магистралью. Т. к. витые пары стоят дешево, то это сэкономит средства, а в базовой магистрали (на которую приходится большая часть трафика) будет использована среда высокой пропускной способности.

4. Мосты позволяют увеличить безопасность (защиту) данных за счет того, что их можно программировать на передачу только тех пакетов, которые содержат адреса определенных отправителей и получателей. Это позволяет ограничить круг РС, способных посылать и принимать информацию из другой подсети.

Например, в сети, обслуживающей бухгалтер можно поставить мост, который позволит принимать информацию лишь некоторым внешним станциям.

5. Мосты увеличивают надежность и отказоустойчивость сети. При сегментировании сети отказ какой-либо подсети не приведет к остановке всех других. Кроме этого, когда выходит из строя единственный файл-сервер, прекращает работу вся сеть. Если с помощью внутренних мостов связать два файл-сервера, страхующих друг друга, то:

- возрастет отказоустойчивость сети;
- снизится уровень трафика.



Различают локальные и удаленные мосты. *Удаленные мосты* используются в больших сетях, когда ее отдельные сегменты связываются телефонными (или иными) каналами связи.

Однако если для соединения двух кабельных сегментов ЛВС используют только один локальный мост, то в крупных сетях приходится использовать два удаленных моста, подключенных через синхронные модемы к выделенному каналу связи

Когда компьютеры находятся далеко друг от друга и их невозможно соединить сетевым кабелем, то встает задача обеспечения удаленного доступа. До сих пор для удаленной связи ПК с ЛВС или ЛВС с остальным миром используются в основном не дорогостоящие цифровые каналы связи, а обычные телефонные линии, которые служат для передачи аналоговых сигналов.

Модем (МОдулятор – ДЕМОдулятор) – это устройство связи, позволяющее компьютеру передавать данные по обычной телефонной линии. Он выполняет модуляцию аналогового сигнала телефонной линии в соответствии с поступающими от компьютера цифровыми данными. При приеме сообщений модем преобразует аналоговые сигналы в цифровые

Модем – оборудование для передачи данных – имеет два стандартных физических интерфейса: - последовательный интерфейс передачи данных (RS–232); - интерфейс с телефонной линией RJ–11 (четырёхконтактный разъем). Существуют *внутренние* и *внешние* модемы. Внутренние устанавливаются в слоты расширения системной платы, внешние выполняются в виде отдельного блока.

Основной характеристикой модема является его производительность, измеряемая количеством битов, переданных за 1 секунду. Изначально скорость модема измерялась в бодах (1бод = 1 бит/с). Однако бод используется в технике связи и относится к частоте изменений аналогового сигнала, переносящей биты данных по телефонной линии.

В 80-х годах скорость бодов равнялась скорости передачи модемов (300 бод было эквивалентно 300 бит/с). Затем инженеры связи разработали методы сжатия и кодирования данных. В результате каждая модуляция аналогового сигнала могла переносить больше одного бита информации. Это означает, что скорость в бит/с больше скорости в бод. Так модем со скоростью модуляции 28800 бод может в действительности передать до 115200 бит/с.

Международные стандарты, определяющие скорость модема, используемые методы кодирования и сжатия, определяют совместимость модемов от разных производителей (таблица 9.1).

Таблица 9.1

Стандарт модемов	Скорость передачи	Функции
V. 32bis	14400 бит/с	Передача
V.34	28800 бит/с	Передача
V.42	57600бит/с	Контроль ошибки
V.42bis / MNP5	27600 – 75800 бит/с	Сжатие

В различных линиях передачи данных используются различные методы передачи: асинхронные и синхронные. Тип модема зависит от метода передачи и назначения сети.

Асинхронные модемы

Стандартные телефонные линии наиболее часто используют асинхронную связь, при которой данные передаются последовательным потоком.

При старт-стопной передаче отсутствует синхронизация между приемником и передатчиком. Передающий модем просто шлет данные, а принимающий – принимает, а затем проверяет, что они приняты без ошибок. Для обнаружения ошибок выделяется дополнительный бит – бит четности. Если информационные биты имеют нечетное число «1», то в бит четности заносится «1», если четное – «0». При приеме осуществляется контроль четности. Если в процессе передачи произошло искажение какого-либо разряда («1» → «0» или «0» → «1»), то будет получено нечетное количество «1» и обнаружена ошибка.

Стандарт модемов V.32 не предусматривает аппаратного контроля ошибок, и он возлагается на специальное программное обеспечение, работающее с модемом. Модемы V.42 используют аппаратную коррекцию ошибок (и поддерживают MNP4). Недостатком асинхронной связи является то, что $\approx 25\%$ трафика данных состоит из управляющей и контролирующей информации.

Сжатие уменьшает время, необходимое для передачи данных (за счет удаления избыточных элементов или пустых участков). Наиболее распространенными стандартами сжатия являются V.42bis и MNP5 (Microsoft Network Protocol class 5). Различные стандарты определяют различные аспекты работы модема. Поэтому один и тот же модем, чтобы увеличить производительность, иногда использует комбинацию протоколов передачи данных и контроля ошибок.

Например, при использовании модемов на асинхронном аналоговом канале связи между ЛВС хорошие результаты может дать следующая комбинация: V.32bis – передача; V.42 – контроль ошибок; V.42bis – сжатие. Однако необходимо, чтобы модемы на обеих сторонах поддерживали одни и те же протоколы. Асинхронные или последовательные модемы дешевле синхронных, поскольку не нуждаются в схемах и компонентах для управления синхронизацией.

Синхронные модемы

Синхронная связь основана на согласованной работе двух устройств. Ее цель – выделить биты из группы при передаче их блоками. Эти блоки называют *кадрами*. Для установки синхронизации и периодической проверки ее правильности используются специальные символы.

Поскольку биты передаются в синхронном режиме, стартовые и стоповые биты не нужны (рис. 9.3). Передача завершается в конце одного кадра и начинается вновь на следующем кадре. Этот метод более эффективнее, чем асинхронная передача, т. к. доля передаваемой полезной информации может превышать 95% (в то время как при асинхронной передаче не более 75 – 80%).

В случае обнаружения ошибки синхронная схема распознавания и

коррекции ошибок просто повторяет передачу кадра. Синхронные протоколы:

- разбивают данные на блоки;
- добавляют управляющую информацию;
- устанавливают соединение;
- проверяют данные на наличие ошибок.
- Основные протоколы синхронной связи: SDLC – протокол синхронного управления каналом (Synchronous Data Link Control); HDLC – высокоуровневый протокол управления каналом (High Data Link Control); BISYNC – протокол двоичной синхронной связи (Binary Synchronous Communication protocol).

Синхронная связь используется практически во всех цифровых системах связи. Если для соединения удаленных ПК используются цифровые линии, то необходимо устанавливать синхронный модем. Следует отметить, что из-за высокой стоимости и сложности синхронные модемы для домашних условий и небольших ЛВС, как правило, не предлагаются.

Линии связи, используемые модемами

Связь с помощью модемов всегда осуществляется по какой-либо коммуникационной линии. Использование той или иной линии определяется такими факторами, как:

- пропускная способность;
- расстояние;
- стоимость.

Существует два типа телефонных линий, по которым может осуществляться модемная связь: каналы общедоступной коммутируемой телефонной сети (коммутируемые линии), арендуемые (выделенные) линии.

Коммутируемые – это обычные телефонные линии. Они требуют установления соединения для каждого сеанса связи. Медленны и не очень надежны при передаче данных. (Диапазон частот от 0,3 – 3,4 кГц, несущая – 1,8 кГц). Однако некоторые компании используют их для передачи файлов или обновления БД, ежедневно на некоторое время устанавливая связь. Это практически единственные линии для связи с фирмами сотрудников из дома, поездок или командировок.

Телефонные компании постоянно улучшают качество предоставляемых коммутируемых товаров. На некоторых цифровых линиях достигается скорость до 56 Кбит/с (при использовании стандартов V.90). Однако на длинных каналах, например, между странами, качество каналов может резко изменяться от сеанса к сеансу.

Арендуемые линии обеспечивают круглосуточно связь, при которой чтобы установить соединение, последовательность коммутаторов не нужна. Качество выделенных линий обычно выше, чем телефонных, которые были созданы только для передачи речи. Типичный диапазон скоростей – от 56 Кбит/с до 45 Мбит/с. Являясь более надежными и быстродействующими, арендуемые линии дороже, т. к. коммуникационная компания выделяет ресурсы этому каналу вне зависимости от того, используется линия или нет. Поставщики коммуникационных услуг предлагают линии различных типов и

качества (табл.9.2).

Таблица 9.2

Тип линии	Передача	Тип линии	Передача
1	Речи	6	Речи и данных по магистралям
2	Речи с контролем качества	7	Речи и данных по частным линиям
3	Речи/радио с подавлением помех	8	Речи и данных по магистралям между компьютерами
4	Данных со скоростью до 1200 бит/с	9	Речи и видео
5	Данных (основной тип)	10	Ретрансляция приложений

Методы удаленного доступа

Существует три метода подключения удаленного пользователя или отделения фирмы к ЛВС компании.

Эмуляция терминала – это метод, при котором пользователь удаленного терминала с помощью специального программного обеспечения подключается по глобальной сети к другому компьютеру, как локальный узел. Этот способ часто используется на мейнфреймах и мини-компьютерах, но мало распространен в ЛВС.

Удаленной управление (remote control) – это метод, который позволяет удаленному пользователю получить контроль над локальными ПК в ЛВС корпорации (т. е. управлять одним из ПК в ЛВС). Скорость проведения сеанса и его возможности зависят от характеристик управляемого ПК, т. к. именно на нем выполняется обработка всех сетевых команд. Коды клавиш, нажимаемых на удаленном ПК, посылаются в управляемый ПК, а все изменения на экране управляемого выводятся на экран удаленного ПК

Используемые файлы и прикладные программы не загружаются в удаленный ПК. Передача через модем со скоростью 2400 – 57600 бит/с. Недостаток метода: для выполнения одной работы задействованы два ПК.

Метод удаленного узла (remote node) основан на использовании сервера удаленного доступа, который служит своего рода «регулирующим» и позволяет отдельному удаленному ПК или ЛВС связываться с центральной ЛВС. Программное обеспечение удаленного ПК, реализующее функции удаленного узла, позволяет ему функционировать как полноценному пользователю ЛВС. Таким программным обеспечением может быть Windows 98, NT WorkStation.

Как только связь установлена, телефонные линии становятся «прозрачными» и пользователь может работать со всеми ресурсами сети, как будто он сидит за ПК, непосредственно подключенным к ЛВС. Сервер удаленного доступа может быть реализован:

- в виде модема со встроенным специальным ПО;
- либо быть сервером ЛВС, на котором выполняются программы удаленного узла.

Желательно, чтобы на удаленном ПК помимо сетевого системного ПО находилось все прикладное ПО, необходимое для сеанса связи: все

выполняемые (*.exe) файлы; необходимые Windows-приложения. В противном случае их необходимо будет передавать с сетевого сервера на канал связи. Т. к. они имеют, как правило, большие объемы данных, то это потребует значительных затрат времени.

Как каждый полноценный пользователь ЛВС, удаленный узел имеет свой сетевой адрес. Сетевая операционная система преобразует сетевые пакеты, которые нужно передать через модем, из формата протокола IP или IPX в формат, совместимый со стандартом последовательной передачи. С появлением все большего количества программ, поддерживающих архитектуру «клиент - сервер», усиливается тенденция на программное обеспечение для удаленных узлов, т. к. такие программы позволяют обрабатывать большие файлы данных на серверах ЛВС, а на удаленный ПК передать только результаты обработки.

Поскольку очень немногие пользователи загружают свои модемы на 100%, то, как с технической, так и с экономической точки зрения, выгодно объединить модемы, работающие в ЛВС предприятия, в группы для коллективного использования.

Кроме того, многие удаленные офисы являются отделениями банков или фирм, их отделами продаж. Естественно, их сотрудники должны иметь возможность связываться со штаб-квартирой. В общем объеме удаленной связи большая часть приходится на контакты сотрудников с офисами из дома или командировок. Чтобы обеспечить эти потребности, требуется:

- коммуникационный сервер;
- многопортовый адаптер – плата, подключаемая к системной шине сервера, обеспечивающая несколько выходных последовательных портов;
- модемный пул – группа модемов, каждый из которых подключается к соответствующему последовательному порту многопортового адаптера;
- дополнительное серверное и клиентское ПО.

При выборе архитектуры построения таких систем и поддерживающих их ПО необходимо обратить внимание на возможность:

- поддержки Windows и конфигурации Windows/NetWare;
- интеграции средств защиты сервера и аутентификации в среде предприятия;
- способность отсеивания пользователей на уровне портов;
- возможность подробной регистрации статистической информации и выполняемых операций.

Задание 1. Установка драйвера платы сетевого адаптера.

1. В программной группе Activity дважды щелкните значок Lab.
2. В главной программной группе Main дважды щелкните значок Control Panel. На экране появится окно Control Panel.
3. Дважды щелкните значок Network. На экране появится окно Network Settings. Обратите внимание: поле ввода Installed Adapter Cards пустое.
4. Щелкните кнопку Add Adapter. На экране появится окно Add

Network Adapter.

5. Убедитесь, что поле Network Adapter Card содержит запись «3Com EtherLink II[□] Adapter». Щелкните кнопку Continue.

6. В этом примере используются следующие установки:

Параметр	Значение
IRQ level	3
I/O Port Address	0x300
Transceiver Type	OnBoard
Memory Mapped	No

7. Выбрав правильные параметры, щелкните ОК. На этом заканчивается установка программного обеспечения, и на экране раскрывается окно Network Settings. Обратите внимание: плата 3Com EtherLink II Adapter появилась в поле Installed Adapter Cards.

8. Добавьте адаптер Intel EtherExpress[™] 16 LAN Adapter со следующими установкам:

Параметр	Значение
Interrupt Number	5
I/O Port Address	0x300
I/O Channel Ready	Late
Transceiver Type	Twisted-Pair (TPE)

Обратите внимание: в списке Installed Adapter Cards присутствуют две платы – 3Com EtherLink II Adapter и Intel EtherExpress 16 LAN Adapter.

Лабораторная работа №5

Администрирование серверов MS Windows 2000

Цель работы: познакомиться с тремя типами беспроводных сетей и их применением, и с четырьмя способами передачи данных в беспроводных сетях.

Теоретическая часть

Словосочетание «беспроводная среда» не означает полного отсутствия проводов в сети. Обычно беспроводные компоненты взаимодействуют с сетью, в которой – как среда передачи – используется кабель. Такая сеть со смешанными компонентами называется гибридной.

Компоненты беспроводной среды:

- обеспечивают временное подключение к существующей кабельной сети;
- помогают организовать резервное копирование в существующую кабельную сеть;
- гарантируют определенный уровень мобильности;
- позволяют снять ограничения на максимальную протяженность сети, накладываемые медными или даже оптоволоконными кабелями.

Трудность установки кабеля – это фактор, который дает беспроводной среде неоспоримое преимущество. Она может оказаться особенно полезной в следующих ситуациях:

- в помещениях, заполненных людьми (например, в прихожей или приемной);
- для людей, которые не работают на одном месте (например, для врачей или медсестер);
- в изолированных помещениях и зданиях;
- в помещениях, планировка которых часто меняется;
- в строениях (например, памятниках истории или архитектуры), где прокладывать кабель непозволительно.

Типы беспроводных сетей

В зависимости от технологии беспроводные сети можно разделить на три типа:

- локальные вычислительные сети;
- расширенные локальные вычислительные сети;
- мобильные сети (переносные компьютеры).

Основные различия между этими типами сетей – параметры передачи. Локальные и расширенные локальные вычислительные сети используют передатчики и приемники, принадлежащие той организации, в которой функционирует сеть. Для переносных компьютеров в качестве среды передачи сигналов выступают АТ&Т, МСI, местные телефонные компании и их общедоступные службы.

Локальные вычислительные сети

Типичная беспроводная сеть выглядит и функционирует практически так же, как и обычная, за исключением среды передачи. Беспроводной сетевой адаптер с трансивером установлен в каждом компьютере, и пользователи работают так, будто их компьютеры соединены кабелем.

Трансивер, называемый иногда точкой доступа (access point), обеспечивает обмен сигналами между компьютерами с беспроводным подключением и остальной сетью (рис. 16).

В беспроводных ЛВС используются небольшие настенные трансиверы. Они устанавливают радиокontakt между переносными устройствами. Такую сеть нельзя назвать полностью беспроводной именно из-за использования этих трансиверов.

Беспроводные локальные сети используют четыре способа передачи данных:

- инфракрасное излучение;
- лазер;
- радиопередачу в узком спектре (одночастотная передача);
- радиопередачу в рассеянном спектре.

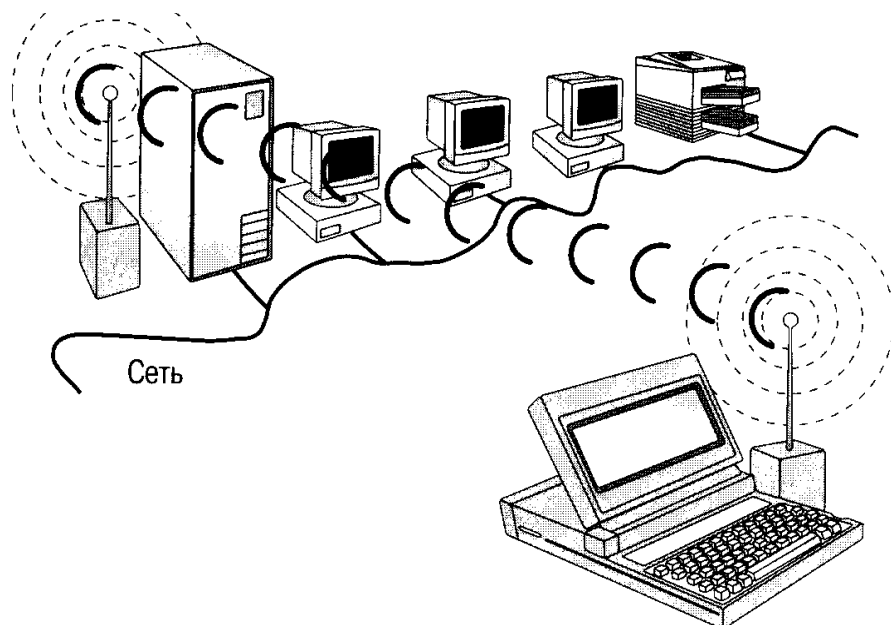


Рис. 16. Беспроводной переносной компьютер подключается к точке доступа

Инфракрасное излучение

Все инфракрасные беспроводные сети используют для передачи данных инфракрасные лучи. В подобных системах необходимо генерировать очень сильный сигнал, так как в противном случае значительное влияние будут оказывать другие источники, например окна.

Этот способ позволяет передавать сигналы с большой скоростью, поскольку инфракрасный свет имеет широкий диапазон частот. Инфракрасные сети способны нормально функционировать на скорости 10 Мбит/с. Существует четыре типа инфракрасных сетей.

- Сети прямой видимости. В таких сетях передача возможна лишь в случае прямой видимости между передатчиком и приемником.

- Сети на рассеянном инфракрасном излучении. При этой технологии сигналы, отражаясь от стен и потолка, в конце концов достигают приемника. Эффективная область ограничивается примерно 30 м (100 футами), и скорость передачи невелика (так как все сигналы отраженные).

- Сети на отраженном инфракрасном излучении. В этих сетях оптические трансиверы, расположенные рядом с компьютером, передают сигналы в определенное место, из которого они переадресуются соответствующему компьютеру.

□ Широкополосные оптические сети. Эти инфракрасные беспроводные сети предоставляют широкополосные услуги. Они соответствуют жестким требованиям мультимедийной среды и практически не уступают кабельным сетям.

Хотя скорость и удобство использования инфракрасных сетей очень привлекательны, возникают трудности при передаче сигналов на расстояние более 30 м (100 футов). К тому же такие сети подвержены помехам со стороны сильных источников света, которые есть в большинстве организаций.

Лазер

Лазерная технология похожа на инфракрасную. Она требует прямой видимости между передатчиком и приемником. Если по каким-либо причинам луч будет прерван, это прервет и передачу.

Радиопередача в узком спектре (одночастотная передача)

Этот способ напоминает вещание обыкновенной радиостанции. Пользователи настраивают передатчики и приемники на определенную частоту. При этом прямая видимость необязательна, площадь вещания составляет около 46500 м² (500 000 квадратных футов). Используемый сигнал высокой частоты не проникает через металлические или железобетонные преграды.

Доступ к такому способу связи осуществляется через поставщика услуг. Связь относительно медленная (около 4,8 Мбит/с).

При этом способе сигналы передаются в некоторой полосе частот, что позволяет избежать проблем связи, присущих одночастотной передаче.

Доступные частоты разделены на каналы, или интервалы. Адаптеры в течение предопределенного промежутка времени настроены на установленный интервал, после чего переключаются на другой интервал. Переключение всех компьютеров в сети происходит синхронно.

Чтобы защитить данные от несанкционированного доступа, применяют кодирование.

Скорость передачи в 250 Кбит/с относит данный способ к разряду самых медленных. Но есть сети, построенные на его основе, которые передают данные со скоростью до 2 Мбит/с на расстояние до 3,2 км – на открытом пространстве и до 120 м – внутри здания.

Это по-настоящему беспроводная сеть. Например, два (или более) компьютера, оснащенные адаптерами Xircom CreditCard Netware с операционными системами типа Microsoft Windows 95 или Microsoft Windows NT, могут без кабеля функционировать как одноранговая сеть. В то же время, если сеть на основе Windows NT Server уже работает. Вы можете связать эти сети, добавив к одному из компьютеров Windows NT-сети устройство Netware Access Point.

Некоторые типы беспроводных компонентов способны функционировать в расширенных локальных вычислительных сетях так же, как их аналоги – в кабельных сетях. Беспроводной мост, например, соединяет сети, находящиеся друг от друга на расстоянии до трех миль (рис. 18).

Компонент, называемый беспроводным мостом (wireless bridge), помогает установить связь между зданиями без участия кабеля. Как обычный мост служит людям для перехода с одного берега реки на другой, так и беспроводной мост прокладывает для данных путь между двумя зданиями. Мост AIRLAN/Bridge Plus, например, использует технологию радиопередачи в рассеянном спектре для создания магистрали, соединяющей ЛВС. Расстояние между ними, в зависимости от условий, может достигать 5 км. Стоимость эксплуатации такого устройства не покажется чрезмерной, поскольку отпадет необходимость арендовать линии связи.

Если расстояние, которое «покрывает» беспроводной мост, недостаточно, можно установить мост дальнего действия. Для работы с сетями Ethernet и Token Ring расстояние до 40 км он также использует технологию радиопередачи в рассеянном спектре. Его стоимость (как и обыкновенного беспроводного моста) может оказаться вполне удовлетворительной, так как отпадут затраты на аренду микроволновых каналов или линий T1. Линия T1 – это стандартная цифровая линия, предназначенная для передачи данных со скоростью до 1,544 Мбит/с. По ней можно передавать и речь, и данные.

Мобильные сети

В беспроводных мобильных сетях в качестве среды передачи выступают телефонные системы и общественные службы. При этом используются:

- пакетное радиосоединение;
- сотовые сети;
- спутниковые станции.

Работники, которые постоянно находятся в разъездах, могут воспользоваться этой технологией: имея при себе переносные компьютеры или PDA (Personal Digital Assistants), они будут обмениваться электронной почтой, файлами и другой информацией.

Такая форма связи удобна, но довольно медленна. Скорость передачи – от 8 Кбит/с до 28,8 Кбит/с. А если запущена система коррекции ошибок, скорость становится еще меньше.

Для подключения переносных компьютеров к основной сети применяют беспроводные адаптеры, использующие технологию сотовой связи. Небольшие антенны, установленные на переносных компьютерах, связывают их с окружают радиоретрансляторами.

Пакетное радиосоединение

При пакетном радиосоединении данные разбиваются на пакеты (подобные сетевым пакетам), в которых содержится следующая информация:

- адрес источника;
- адрес приемника;
- информация для коррекции ошибок.

Пакеты передаются на спутник, который транслирует их в широкоэмитальном режиме. Затем устройства с соответствующим адресом принимают эти пакеты.

Сотовые сети

Сотовые цифровые пакеты данных (Cellular Digital Packet Data - CDPD) используют ту же технологию, что и сотовые телефоны. Они передают данные по существующим для передачи речи сетям в те моменты, когда эти сети не заняты. Это очень быстрая технология связи с задержкой в доли секунды, что делает ее вполне приемлемой для передачи в реальном масштабе времени.

В сотовых сетях, как и в других беспроводных сетях, необходимо найти способ, который позволит подключиться к существующей кабельной сети. Nortel out of Mississauga (Онтарио, Канада) – компания, которая производит интерфейсный блок Ethernet (Ethernet Interface Unit – EIU), предназначенный для этой цели.

Задание №1:

1. Внимательно прочитайте теоретический материал изложенный в данной лабораторной работе.
2. Составить сравнительную характеристику выше описанных видов сетей.
3. Ответьте на контрольные вопросы.

Контрольные вопросы

1. Беспроводные сети. Применение беспроводных сред. Типы беспроводных сетей.
2. Локальные вычислительные сети. Используемые способы передачи данных.
3. Локальные вычислительные сети. Инфракрасное излучение. Типы инфракрасных сетей. Лазер.
4. Локальные вычислительные сети. Радиопередача в узком спектре и рассеянном спектре.
5. Расширенные локальные сети. Беспроводные мосты.
6. Мобильные сети (пакетное радиосоединение, сотовые сети, микроволновые системы).

Лабораторная работа №6

Маршрутизация в сети

Цель работы: изучить основные понятия маршрутизаторов, мостов, репитеров

Теоретические сведения

Маршрутизатор – это устройство для соединения сетей, использующих различные архитектуры и протоколы. Работая на сетевом уровне модели OSI, они могут:

- коммутировать и направлять пакеты через несколько сетей;
- определять наилучший путь для их передачи;
- обходить медленные и неисправные каналы;

- отфильтровывать широковещательные сообщения;
- действовать как барьер безопасности между сетями.

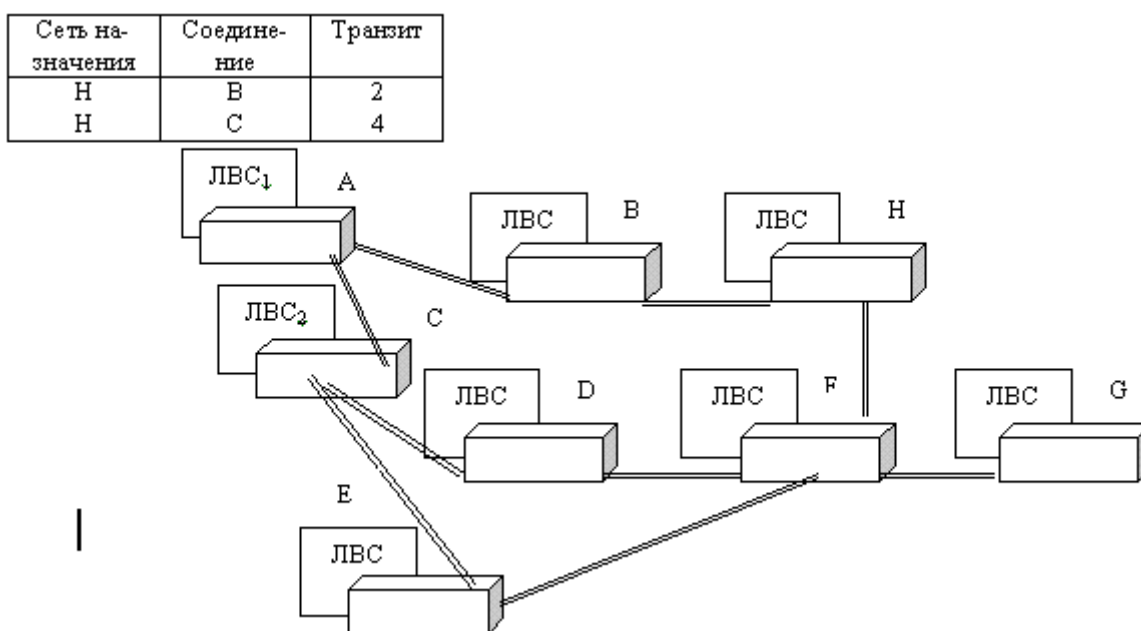
Маршрутизатор в отличие от моста имеет свой адрес и используется как промежуточный пункт назначения.

Принцип работы маршрутизатора

Работа маршрутизатора основывается на хранимой в его памяти таблице. Однако, эта таблица существенно отличается от таблиц мостов тем, что она содержит не адреса узлов, а *адреса сетей* (рис.8.4). Для каждого протокола, используемого в сети, строится своя таблица, которая включает:

- все известные адреса сетей;
- способы связи с другими сетями;
- возможные пути маршрутизации;
- стоимости передачи данных по этим путям.

Маршрутизаторы, принимая пакеты, не проверяют адрес узла назначения, а выделяют только адрес сети. Они пропускают пакет, если адрес сети известен, передавая его маршрутизатору, который обслуживает сеть назначения.



.Пример соединения ЛВС с использованием маршрутизаторов

Воспринимая только адресованные сетевые пакеты, они препятствуют проникновению в сеть некорректных и широковещательных пакетов, уменьшая тем самым нагрузку на сеть.

Маршрутизатор может «прослушивать» сеть и определять, какие ее части сильнее загружены. Он устанавливает количество транзитов между ЛВС. Используя эту информацию, маршрутизатор выбирает маршрут передачи. Если один перегружен, он укажет другой. Используются различные алгоритмы маршрутизации:

- на основе состояния канала (в IPX);
- дистанционно-векторные (в TCP/IP);

- открытый протокол предпочтения кратчайшего пути (OSPF и TCP/IP), который вычисляет маршрут с учетом количества транзитов, скорости линии, трафика и стоимости.

Типы маршрутизаторов и их отличие от мостов

Так же как и мосты, маршрутизаторы бывают локальными и удаленными. По типу работы выделяют статические и динамические маршрутизаторы:

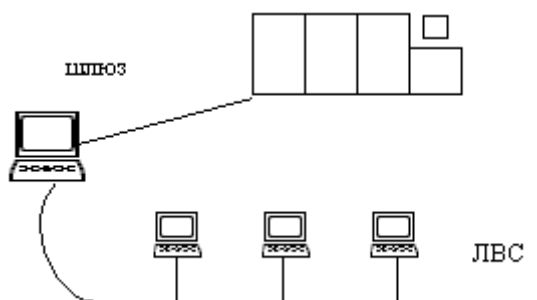
- *статические* требуют, чтобы администратор сети вручную создавал и конфигурировал таблицу маршрутизации, а также указал каждый маршрут;
- *динамические* автоматически определяют маршруты и поэтому требуют минимальной настройки и конфигурации. Они сложнее и дороже, т. к. принимают отдельное решение по каждому пакету.

Отличие мостов и маршрутизаторов в том, что:

- Мост работает на *канальном уровне* и «видит» только адрес узла; распознавая его, передает в нужный сегмент сети; не определив адрес, пересылает во все сегменты;
- Маршрутизатор работает на *сетевом уровне*, определяя и то, что нужно передать, и то, куда нужно; т. е. он распознает не только адрес (но уже сети!), но и тип протокола; кроме этого маршрутизатор может установить адреса других маршрутизаторов и решить, какие пакеты каким маршрутизаторам переадресовать.

Мост может распознать только один путь между сетями, а маршрутизатор из многих находит лучший. В настоящее время стали использоваться *мосты – маршрутизаторы* – устройства, которые соединили в себе лучшие свойства мостов и маршрутизаторов: для одних протоколов они действуют как мосты; для других – как маршрутизаторы.

Шлюзы



Шлюзы – это устройства, которые обеспечивают связь между различными архитектурами и средами. Главное их назначение – осуществить связь между ПК и средой мини-компьютеров или мейнфреймов (рис. 8.5).

Обычно роль шлюзов в ЛВС выполняют выделенные сервера, а все остальные рабочие станции ЛВС работают с мейнфреймом также просто, как со своими ресурсами.

Шлюз связывает две системы, которые используют разные:

- коммуникационные протоколы;

- структуры и форматы данных;
- языки и архитектуры.

Шлюзы принимают данные из одной среды, удаляют протокольный стек и переупаковывают их в протокольный стек системы назначения (рис. 8.6). Обработывая данные, шлюз выполняет следующие операции:

- 1) извлекает данные из входящих пакетов, пропуская их снизу вверх через полный стек протоколов передающей среды;
- 2) заново упаковывает полученные данные, пропуская их сверху вниз через стек протоколов сети назначения.

Задание

- 1 Описать методы маршрутизации
- 2 Дать определение шлюзам и мостам
- 3 Дать сравнительную характеристику
- 4 Сдать в виде отчета

Лабораторная работа №7

Программирование задач типа «клиент-сервер». Освоение методики программирования услуг коммуникаций на базе протокола ТСР/IP

Цель работы: изучить основные понятия маршрутизаторов, мостов, репитеров

Теоретические сведения

Работа протоколов

Протоколы реализуются через заголовки, которые добавляются к пакетам по мере того, как они передаются по уровням. Каждый заголовок связывается с конкретным уровнем и в каждом последующем уровне воспринимается как часть пакета .

При поступлении пакета в принимающий узел, заголовки соответствующих уровней используются для вызова заданной функции в принимающем узле. При передаче пакета выше этот заголовок изымается. И компьютер-отправитель, и компьютер-получатель должны выполнять каждое действие одинаковым способом с тем, чтобы пришедшие по сети данные совпали с отправленными.

Если, например, два протокола будут по-разному разбивать данные на пакеты или по-разному добавлять данные (о последовательности пакетов, синхронизации и т. д.), то тогда компьютер, использующий один из протоколов, не сможет связаться с компьютером, на котором работает другой протокол.

На работу протоколов ряда уровней оказывает влияние, является ли сеть с коммутацией соединений или с коммутацией пакетов. Широкое развитие межсетевых объединений («интернет»), компонентами которых являются ЛВС, привело к тому, что данные из одной ЛВС в другую могут передаваться по одному из возможных маршрутов. Протоколы, которые поддерживают такую передачу, называются *маршрутизируемыми протоколами*. И их роль постоянно возрастает.

Существует несколько стандартных стеков протоколов, разработанных разными фирмами. Протоколы этих стеков выполняют работу, специальную для своего уровня. Однако коммуникационные задачи, которые возложены на сеть, приводят к разделению протоколов на три типа : прикладные протоколы; транспортные протоколы и сетевые протоколы.

Прикладные протоколы работают на верхнем уровне модели OSI и обеспечивают взаимодействие приложений и обмен данными между ними.

Транспортные протоколы поддерживают сеансы связи между компьютерами и гарантируют надежный обмен данными между ними.

Сетевые протоколы обеспечивают услуги связи. Эти протоколы управляют: адресацией, маршрутизацией, проверкой ошибок и запросами на повторную передачу.

Наиболее популярными в настоящее время являются стеки протоколов: TCP/IP разработанный более 20 лет назад по заказу МО США; IPX/SPX фирмы Novell и NETBEUI / NetBIOS фирмы IBM.

1. Стек TCP/IP включает в себя два основных протокола:

- TCP (Transmission Control Protocol) – протокол для гарантированной доставки данных, разбитых на последовательность фрагментов. Соответствует транспортному уровню.
- IP (Internet Protocol) – протокол для передачи пакетов, относится к разряду сетевых протоколов.

Стек TCP/IP является промышленным стандартным набором протоколов, которые обеспечивают связь в неоднородной среде, т. е. обеспечивают совместимость между компьютерами разных типов. Кроме того, TCP/IP:

- представляет доступ к ресурсам Интернет;
- поддерживает маршрутизацию и обычно используется в качестве межсетевого протокола.

Благодаря своей популярности TCP/IP стал стандартом де-факто для межсетевого взаимодействия. К другим специально созданным для стека TCP/IP протоколам относятся: SMTP (Simple Mail Protocol) – электронная почта; FTP (File Transfer Protocol) – обмен файлами между ЭВМ и др. Эти протоколы относятся к разряду прикладных протоколов.

Задание

С помощью утилиты ping определите IP адреса интернет-узлов для всех DNS-имён (доменов) из вашего варианта. По IP адресам с помощью обратного DNS-запроса определите имена интернет-узлов, зарегистрированных для данных IP адресов (используйте ключ -a утилиты ping). Сравните имена и сделайте вывод о том, является ли домен основным для данного интернет-узла. Если возможно, укажите хостинг-провайдера или название организации, которая обеспечивает работу указанного домена. В отчете также приведите один screenshot (копию экрана), полученный во время выполнения этого пункта.

ЛИТЕРАТУРА

ОСНОВНАЯ

- 1 Самоучитель по работе с компьютерной сетью. ПК с нуля. Пособие для начинающих опытных пользователей ПК. Москва «Альянс-Пресс», 2003г.
- 2 А.П. Пятибратов, Л.П.Гудыно, А.А.Кириченко Вычислительные системы, сети и телекоммуникации. Москва, «Финансы и статистика» 2002г.
- 3 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. - СПб: Питер, 2001г.
- 4 Windows 2000 Server в подлиннике Санкт-Петербург. «БХВ -Петербург» 2003г.
- 5 Э.Таненбаум Компьютерные сети. Санкт-Петербург. «Питер» 2003г.
- 6 Компьютерные сети. Учебный курс/Пер, с англ. - М.:Издательский отдел "Русская редакция" ТОО "Channel Trading Ltd".-1997г.
- 7 Джамса К., Коул К. Программирование для Internet в среде Windows/ Пер.с англ.-СПб Питер, 1996г.
- 8 Барфилд Э. Программирование "клиент/сервер" в ЛВС/ Пер. с англ. М.: Филинь, 1997г.
- 9 Гук М. Аппаратные средства локальных сетей. Энциклопедия СПб.:Питер, 2000г.
- 10 Фролов В. и др. Глобальные сети компьютеров: Практическое введение в Internet, E-mail, FTP WWW и программирование для Windows Sockets. МЛ: Диалог-МИФИ, 1996г.
- 11 Зимянин Л.Ф. Основы семейства протоколов TCP/IP. Учебное пособие.- Мн.:Белгосуниверситет, 1996г.
- 12 Вишневский А. Сетевые технологии Windows 2000 для профессионалов. -СПб: Питер, 2000г.

ДОПОЛНИТЕЛЬНАЯ

- 1 Ларионов А.М., Майоров С.А., Новиков Г.И. Вычислительные комплексы, системы, сети. Л., Энергоатомиздат, 1987г.
- 2 Шербо В.К., Киреичев В.М., Самойленко СИ. Стандарты по локальным вычислительным сетям: Справочник. -М.: Радио и связь. -1990г.
- 3 Золотев С. Протоколы Internet ВН, 1998г.
- 4 Стерн, Монти Сети предприятий на основе WINDOWS NT для профессионалов; перев. С англ. - СПб: Питер, 1999г.
- 5 Челлис Дж., Перкинс Ч. Стриб М. Основы построения сетей. Учебное руководство для специалистов МС8Е. - Лори, 1997г.
- 6 Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 1999г. Компьютерные сети. Учебный курс. MicrosoftPress, - Русская редакция, 1998г.
- 7 Ю.Анин Б. Защита компьютерной информации. - СПб.: ВHV- Санкт-Петербург, 2000г.