МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ

БУХАРСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ

ПИЩЕВОЙ И ЛЕГКОЙ ПРОМЫШЛЕННОСТИ

СБОРНИК ЛЕКЦИИ

ПО ПРЕДМЕТУ:

«КОМПЬЮТЕРНЫЕ СЕТИ И АРХИТЕКТУРА РЕСУРСОВ.

»

Кафедра «Информационные технологии»

БУХАРА – 2004

Составитель : к.т.н. Убайдуллаева Ш.Р.

Рецензенты: доц. кафедры «Вычислительная математика и информатика» БГУ Жумаев Ж.Ж., зав. кафедрой «Информатика»
БухТИП иЛП доц. Абидов К.З.

Рекомендовано и утверждено на заседании кафедры «ИТ»

(протокол №____ от 29 августь 2003 г.)

Рекомендовано к печати по решению Учебно- методического

Совета института (протокол №2 от 12 декабрь 2003 г.)

А Н Н О Т А Ц И Я

Курс предмета «Компьютерные сети и архитектура ресурсов» является одной из специальных дисциплин, читаемых для студентов специальности «Информатика и информационные технологии».

В предлагаемый сборник вошли лекции, посвященные изучению основ компьютерных сетей:

- понятие о компьютерной сети, два типа сетей;
- различные сетевые топологии;
- сетевые кабели;
- беспроводные сети;
- платы сетевого адаптера;
- драйверы;
- сетевые модели;
- протоколы;
- передача данных по кабелю и т.д.

Сборник лекций полностью соответствует программе курса «Компьютерные сети и архитектура ресурсов».

В В Е Д Е Н И Е

Потребность в вычислениях возникла у людей на самых ранних стадиях развития человеческого общества. Причем с самого начала для облегчения счета люди использовали различные приспособления. Многие из них были весьма интересными и остроумными по принципу действия, но все они требовали, чтобы в процессе вычислений активно участвовал человек.

Качественно новый этап наступил с созданием компьютеров и внедрением информационных технологий во многие сферы жизнедеятельности человека. Компьютеры вторгаются в область умственного людей, выполняют те функции, которые раннее были доступны только человеку.

В компьютерах числа представлены в виде последовательности цифр, переменные в виде последовательности множества значений . Для представления любой цифры используется какой- либо элемент, который может находиться в одном из нескольких устойчивых (четко разграниченных между собой) состояний.

Современным компьютерам присущи все свойства, необходимые для решения математических задач:

а) выполнение всех элементарных арифметических и логических операций в произвольной последовательности;

б) запоминание большого числа промежуточных результатов и исходных данных;

в) автоматическое изменение направления вычислительного процесса в зависимости от результатов отдельных операций.

В современных компьютерах для запоминания чисел и выполнения действий с ними используется двоичная система счисления. Это обусловлено, главным образом, наличием двоичных элементов и функциональных узлов, которые оказались удобными для этих целей.

Лекция № 1.

Понятие о компьютерной сети. Два типа сетей. Интеграция компьютеров в локальную вычислительную сеть (ЛВС)

План:

Концепции построения сети

Локальные вычислительные сети.

Расширение компьютерных сетей.

Назначение компьютерной сети.

Принтеры и другие периферийные устройства.

Данные.

Приложения.

Резюме.

Концепции построения сети

Самая простая сеть (networ) состоит как минимум из двух комп ютеров, объединенных друг с другом кабелем.Это позваляет им использо вать данные совместно.Все сети основываются именно на этом простом принципе. Хотя соединения компьютеров с помощью кабеля не кажетсянам особо выдающейся,в свое время она явилась значительным достижением в области коммуникаций.

Рождение компьютерных сетей было вызвано практической потребностью иметь возможность для совместного использования данных. Персональный компьютер прекрасный инструмент для создания докумен та,подготовки таблици других видов информации, но при этом вы не можете быстро поделится своей информацией с другими. Когда не было сетей, приходилось распечатовать каждый документ, чтобы другие пользователи могли работать с ним или в следующем случае - копировать информацию на дискеты. Одновременная обработка документа

несколькими пользователями исключалась. Подобная схема называется работой в автономной среде.

Сетью называется группа соединенных компьютеров и других устройств. Аконцепция соединенных и совместно использующих ресурсыкомпьютеров носит название сетевого взаимодействия. Компьютеры, входящие в сеть, могут совместно использовать:

- данные;
- принтеры;
- факсимильные аппараты;
- Модемы;
- другие устройства

Данный список постоянно пополняется, так как возникают новые способы совместного использования ресурсов.

Локальные вычислителиные сети

Первоначально компьютерные сети били небольшими и объединяли додесяти компьютеров и один принтер. Технология ограничивала размеры сети, в том числе количество компьютеров в сети и ее физическую длину. В начале 1980-х годов наиболее популярный тип сетей состоял не более чем из 30 компьютеров, а длина ее кабеля не привышала 185м (600 футов). Такие сети легко располагались в пределах одного этажа здания. Эти сети называются локальными вычислительными сетями [ЛВС(LAN)].

Расширение компьютерных сетей

Самые первые типы локальных сетей не могли соответствовать потребностям крупных предприятий, офисы которых расположены в различных местах. Но как только преимущества компьютерных сетей стали неоспоримыми и сетевые программные продукты начали заполнять рынок, перед корпорациями для сохранения конкурентоспособности - встала задача расширения сетей. Сегодня, когда географические рамки сетей раздвигаются, чтобы соединить пользователей из разных из разных

городов и государств, ЛВС превращаются в глобальную вычислительную сеть [ГВС(WAN)], а количество компьютеров в сети уже может варьироваться от десятка до нескольких тысяч лет.

Назначение компьютерной сети

Основное назначение компьютерных сетей - совместное использование ресурсов осуществление интерактивной связи как внутри одной фирмы, так и за ее пределами. Ресурсы - это данные, приложения и перифирийные устройства. Понятие интерактивной связи компьютеров подразумевается обмен сообщениями в реальном режиме времени

Принтеры и другие перефирийные устройства

До появления компьютерных сетей каждый пользователь должен был иметь свой принтер, плоттер и другие перефирийные устройства. Чтобы совместно использовать принтер, существовал единственный способ - пересесть за компьютер, подключенный к этому принтеру. Теперь сети позволяют целому ряду пользователей одновременно "владеть" данными и периферийными устройствами. Если нескольким пользователем надо распечатать документ, все они могут обратится ксетевому принтеру.

Данные

До появления компьютерных сетей люди обменивались информацией примерно так:

- передавали информацию устно;
- писали записки или письма;
- записывали информацию на дискету, несли дискету к другому компьютеру и копировали в него данные. Компьютерные сети упрощают этот процесс, предоставляя пользователям доступ почти к любым типам данных.

Приложения

Сети создают отличные условия для унификации приложений. Это значит, что на всех компьютерах в сети выполняются приложения одного типа и одной версии. Использование единного приложения может упростить поддержку всей сети. Удобнее также иметь дело с одной версией приложения и настраивать компьютеры одинаковым образом. Другая привлекательная сторона сетей - наличие программ электронной почты и планирования рабочего дня. Благгодаря им управляющие крупных предприятий быстро и эффективно взаимодействуют с многочисленным штатом своих сотрудников или партнеров по бизнессу, а планирование и корректировка деятельности всей компании осуществляется с гораздо меньшими усилиями, чем прежде.

Резюме

Локальная вычислительная сеть (ЛВС) состоит из нескольких компьютеров и периферийных устройств, соединеных кабелем в пределах ограниченой территории. Сеть позволяет совместно использовать ресурсы, а так же работать с интерактивными приложениями.

Использование компьютерных сетей сулит множество преимуществ:

- снижение затрат благодаря совместному использованию данных и периферийных устройств;
- стандартизация приложений;
- современное получение данных;
- более эффективное взаимодействие и планирование рабочего времени.

В настоящее время компьютерные сети выходят за пределы ЛВС и вырастают в глобальные компьютерные сети (ГВС), охватывая целые страны и континенты.

Два типа сетей

Главные характтеристики и приимущества каждого типа сетей. Идет заложенные в реализацию одноранговой сетевой среды и сетевой среды на основе сервера.

Все сети имеют некторые общие компоненты, функции и характеристики

В их числе:

серверы (server)-компьютеры, предоставляющие свои ресурсы пользователям;

клиенты (client)-компьютеры, осуществляющие доступ к сетевым ресурсам, представляемым сервером;

среда (media)-способ соединения компьютеров совместно используемые данные файлы, представляемые серверами по сети;

совместно используемые периферинны еустройства, например, принтеры, библиотеки СД-ROM и т.д., ресурсы, предоставленные серверками;

ресурсы-файлы, принтеры и другие элементв, используемые в сети. Несмотря на определенные сходства, сетии разделяются на 2 типа:

одноранговые (peer to peer)

на основе сервиса (server based)

Одноранговые сетии

В одноронговые сети все компьютеры равноправны: нет иерархии среди компьютеров и нет выделенного сервера. Каждый компьютер функционирует и как клиент, и как сервер, иначе говоря, нет отдельного компьютера, ответственного за администрирование всей сети.

Все пользователи самостаятельно решают, какие данные на своём компьютер сделать общедоступными по сети. В одноранговой сети все компьютеры выступают и как клиенты, и как серверы.

Размеры

Одноранговые сети называют также рабочими группами. Рабочая группа -это небольшой коллектив, поэтому в одноранговых сетех чаще всего не более 10 компьютеров.

Стоимость

Одногранговые сети относительно просты. Они обычно дешевле сетей на основе сервера, но требуют более мощных (и боленедорогих) компьютеров. Операционные системы в одноранговых сетях требования к производительности и куровню защиты для сетевого программного обеспечения ниже чем всетях с выделенным сервером.

В такие ОС, как Mictosoft Windows NT, Mictosoft Windows-95, Mictosoft Windows for Workgroups встроена поддержкаодноранговых сетей. Поэтому, чтобы установить сеть, дополнительного програмного обеспечения не требует.

Реализация.

ОР сеть характеризуется рядом стандартных ришений:

- компьютеры расположены на рабочих столах пользователей;
- пользователи сами выступают в роли администраторов и бпеспечивают защиту информации;

Для обьединения компьютеров в сеть прменяется простая кабельная система.

Целесообразность применения

одноранговая сеть вполне подходит там, где количество пользователей не превышает 10 человек;

- пользователи расположены компактно;
- вопросы защиты данных не принципиальны;

Администрирование

Сетевое администрирование решает ряд задач, в том числе:

- управление работой пользователей и защитой данных;
- обеспечение доступа к ресурсам;

- установка прикладного программного обеспечения.

В одноранговой сети администратор не выделяется. Каждый пользователь сам администрирует свой компьютер.

Разделяемые ресурсы

В одноранговой сети пользователи могут "поделиться" своими ресурсами с другими. К совместно исполььзуемым ресурсам относятся каталоги, файлы, принтеры, факс-модемы и т.п.

Сети на основе сервера.

Если к сети подключено более 10 пользователей, то одноранговая сетьможет оказаться недостаточно производительной. Поэтому в большинстве случаях используются сети на основе сервера.Выделеннымназывается такой сервер, который функционорует только как сервер (исключая функциии клиента или рабочей станции). Они специиально оптимизированы для быстрой обработки запросов от сетевых клиентов и для управления защитой файлов и каталогов.С увелечением размеров сети и объёма сетевого трафика (время обмена информацией.) необходимо увеличить количествосерверов.

Специализированные серверы.

Круг задач, выполняемых сервирами многообразен и сложен.Чтобы приспособиться к возрастающим потребностям пользователей, серверы в больших сетях стали специализированными.Например, в сети Windows NT существуют различные типы серверов.

Файл-серверы и доступом пользователей к файлам. П-С управляют доступом пользователей к принтерам.Например, чтобы работать с текстовым процессором, вы должны его сначала запустить на своем компьютере. Документ текстового процессора, хранящийся на файл-сервере, загружается в память вашего компьютера и, таким образом, вы можете работать с этим документом на своём компьютере. Файл-сервер предназначен для хранения файлов и данных.

Серверы приложений.

Серверы приложений хранят большие обьёмы информации в структурированом виде. В файли или приный сересрах данные целиком копируются на запрашивающий компьютер. А в сервере пересылаются только результаты запроса.

Приложение- клиент на удаленном компьютере получает доступ к данным, хранимым на сервере приложений. Однако вместовсей базыц данных на ваш компьютер с сервера загружаются только результаты запроса. Например, вы можете получить список работников, поступивших на работу в 1990 г. и т.д.

Почтовые серверы

Почтовые серверы управляют передачей электронных сообщний между пользователями сети.

Факс-серверы

Управляют потокам входящих и исходящих факситильных сообщений через один или несколько факс-модемов.

Коммуникационные серверы

Управляют потоком данных и почтовых сообщений между этой сетью и другими сетями или удаленными пользователями через моден и телефонную линию.

Сервер служб каталогов.

Предназначен для поиска, хранения и защиты информации всети. Windows NT server объединяет компьютеры в логические группы-долины (domain) система защиты которых наделяет пользователей различными правами доступа к сетевому ресурсу.

Значение програмного обеспечения.

Сетевой сервер и опреционная система работают как единое целое. Без ОС даже самый мощный сервер представляетт собой груду железа. А ОС позваляет реализовать потенциал аппаратных ресурсов сервера.

Некоторые ОС, например, Windows NT NT server, были созданы специально для того, чтобы использовать приимущества наиболее

передовых серверных технологий. Так Windows NT server поддерживает файлы сервера размером до 16 эксабант (эб) 1 эксабайт = 1 миллиард гигабайт.

Преимущества сетей на основе сервера.

Разделение ресурсов

Администрирование и управление доступом к данным осуществляется централизованно. Ресурсы как правило, расположены также централизованно, что облегчает их поиск и поддержку.Защита

Основным аргументом при выборе сети на основе сервера является, как правило, защита данных. В таких сетях, как Windows NT server, проблемами безопасности может заниматься один администратор, он формирует политику безопасности ии применяет её в отношении каждого пользователя сети.

Резервы копирование данных

Поскольку в сетях на основе сервера информация расположена централизованно, нетрудно обеспечить её регулярное резервное копиравание.

Избыточность

Благодаря избыточным системам данные на сервере могут дублироваться в реальном времени, поэтому в случае повреждения основной области хранения данных информация не будет потеряна легко воспользоваться резервной копией.Количество пользователей Сети на основе сервера способны поддерживать тысячи пользователей.

Аппаратные обеспечение

Так как компьютер не выполняет функций сервера требования к его характиристикам зависят от самого пользователя. Типичный компьютер-клиент имеет,по крацней мере, 486-й процессор и от 8 до16 мбайт оперативной памяти

Комбинированные сети

Существуют и комбинированные типы сетей, совмещающие лучшие качества одноранговых сетей и сетей на основе сервера. Многие администраторы считают, что такая сеть наиболее полно удовлетворяет их запросы, так как в ней могут функционировать оба типа операционных систем. Операционные Системы для сетей на основе сервера, например Windows NT server или Nowell Netware, в этом случае отвечает за совместное использование приложений и данных.

На компьютер -клиентах могут выполняться операционные системы такие, как Windows 95 ,которые будут управлять доступам к ресурсам выделенного сервера и в тоже время предоставлять в совместное использование свои жесткие диски.

Комбинированные сети-наиболие распространенный тип сетей,но для их правильной реализации и надежной защиты необходимы определенные знания и навыки планирования

В одноранговых сетях каждый компьютер функционирует и как клиент и как сервер. Для небольшой группы пользователей подобные сети легко обеспечивают разделение данных и периферийных устройств. Вместе с тем, поскольку администрирование в одноранговой сети сети не централизованное обеспечить развитую систему защиты данных трудно.

Сети на основе сервера наиболее эффективны в том случае,когда совместно используется большое количество ресурсов и данных. Администратор может управлять защитой данных, наблюдая за функционированием сети. В таких сетях может быть один или несколько серверов, в зависимости от объёма сетевого трафика,количество периферитных устройств и т.д. Например, в одной сети могут быть и принт-сервер и коммуникационный сервер, и сервер базы данных.

Контрольные вопросы.

1. Концепции построения сети.
2. Локальные вычислительные сети.
3. Расширение компьютерных сетей.
4. Что называется сетью.
5. Принтеры и другие периферийные устройства.
6. Два типа сетей.
7. Одноранговые сети.
8. Сети на основе сервера.
9. Специализированные сети.
10. Значение программного обеспечения.

Ключевые слова:

автономная среда;

принтеры;

факсимальные аппараты;

модемы;

джойстики;

ресурсы;

серверы.

Лекция № 2

Компоновка сети.

Различные способы компоновки сети.

План:

Топология сети

Базовые топологии

Персональная сеть с топологией “шина”

Передача сигнала

Терминатор

Расширение ЛВС

Звезда

Кольцо

Передача маркера

Активные конйетраторы

Комбинированные топологии

Резюме

Топология сети.

Термин "Топология" или "Топология сети", характеризует физическое расположение компьютеров, кабелей и других компонентов сети. Топология - это стандартный термин, который используется при описании основной компоновки сети.

Кроме этого термина, для описания физической компоновкиупотребляется также следующие:

- физическое расположение;
- компоновка;
- диаграмма;
- карта.

Топология сети обуславливает её характеристики. Выбор тойили иной топологии влияет:

- на состав сетевого оборудования;
- характеристики сетевого оборудования;
- возможности расширения сети;
- способ управления сетью.

Чтобы совместно использовать ресурсы или выполнять другие сетевые задачи, Компьютеры должны быть подключены друг к другу. Для этой цели в большинстве сетей применяется кабель. Однако просто подключить компьютер к кабелю, соединяющему другие компьютеры, не достаточно. Различные типы кабелей в сочетании с различными сетевыми платами, сетевыми ОС и другими различными компонентами требуют различного взаимного расположения компьютеров.

Каждая топология сети полагает ряд условий. Например, она может диктовать не только тип кабеля, но и способ его прокладки.

Базовые топологии.

Все сети строятся на основе 3-х базовых топологий :

- шина (bus)
- star (звезда)
- кольцо (ring)

Если компьютеры подключены вдоль одного кабеля, топологияназывается шиной. В том случае, когда компьютеры подключены к сегментам кабеля, исходящим из одной точки, или концентратора,топология называется звездой. Если кабель, к которому подключены компьютеры, замкнут в кольцо, такая топология носит название кольца.

Топологию шина часто называют "линейной шиной". Данная топология относится к наиболее простым и широко распространённым топологиям. В ней используется один кабель, именуемый магистрально или сегментом, вдоль которого подключены все компьютеры сети.

Простая сеть с топологией "шина"

Взаимодействие компьютеров.

В сети с топологией "шина" компьютеры адресуют данные конкретному компьютеру, передавая их по кабелю в виде электрических сигналов.

Чтобы понять процесс взаимодействия компьютеров по шине, необходимо уяснить следующие понятия:

- передача сигнала;
- отражение сигнала;
- терминатор.

Передача сигнала.

Данные в виде электрических сигналов передаются всемкомпьютерам сети; однако информацию получает только тот адрес, котрого соответствует адресу получателя, зашифрованному в этих сигналах. Причём в каждый момент времени только один компьютер может вести передачу. Так как данные в сеть передаются лишь одним компьютером,её производительность зависит от количества компьютеров, подключённых к шине. Чем больше компьютеров, ожидающих передачи данных, тем медленнее сеть.Кроме шага компьютеры, на быстродействие сети влияет множество факторов, в том числе:

- характеристики аппаратного обеспечения компьютеров в сети.
- частота, с которой компьютеры передают данные.
- тип работающих сетевых приложений.
- расстояние между компьютерами 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 компьютер выйдет из строя, это не скажется на работе остальных. В активных топологиях компьютеры генерируют сигналы и передают их по сети.

Отражение сигнала.

Данные, или электрические сигналы, распространяются по всей сети - от одного конца кабеля к другому. Если не принимать никаких специальных действий, сигналы, достигая конца кабеля, будут отражаться и не позволяет другим компьютерам осуществлять передачу. Поэтому, после того, как данные достигнут адресата, электрические сигналы необходимо погасить.

Терминатор.

Чтобы предотвратить отражение электрических сигналов, на аждом конце кабеля устанавливают терминаторы (termihator), поглащающие эти сигналы. Все концы сетевого кабеля д.б. к чему-нибудь подключены, например к компьютеру или баррел-коннектору для увелечения длины кабеля. Компьютеру свободному-неподключенному концу кабеля д.б. подсоединён терминатор, чтобы предовратить отражение электрических сигналов.

Нарушение целостности сети.

Разрыв сетевого кабеля происходит при его физическом разрыве или отсоединения одного из его концов. Прекращение функционирование сети возможно также при отсутствие терминаторов. Сеть "падает".

Сами по себе компьютеры в сети остаются работоспособными, но пока сети не разорванны, они не могут взаимодействовать друг сдругом.

Расширение ЛВС.

Увелечение числа компьютеров охвативаеных сетью, вызывает необходимость расширения. В сети с топологией "шина" кабель обычно удлиняется 2-мя способами.

1. Для соединения 2-х отрезков кабеля можно воспользоваться можно баррел-коннектором. Но злоупотреблять им не стоит, т.к. сигнал при большом кол-ве стыковок искажается и ослабевает. Лучше купить один длинный кабель, чем соединять несколько коротих отрезков.

2. Для соединения 2-х отрезков кабеля служит репитер (repeater). В отличие от коннектора, он усиливает сигнал передпередачей его в следующий сегмент. Поэтому предпочтительнее использовать репитер, чем баррел-коннектор или один длинный кабель сигналы на большие расстояние пойдут без искажений.

Звезда.

При топологии "звезда" все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту, именуемому концентратором (hyb). Сигналы от предающего компьютера поступают через концентратор ко всем остальным. Это топология возникла на заре вычислительной техники, когда компьютеры были подклю чены к центральному, главному компьютеру. В сетях с топологией "звезда" подключение кабеля и управление конфигурацией сети централизованны. Но есть и недастаток: для больших сетей значительно увеличивается расход кабеля. К тому же, если центральныййй компонент выйдет из строя, нарушается работа всей сети. А если выйдет из строя только один компьютер (или кабель, соединяюший его с концентратором) ,то лиш этот компьютер не сможет передовать или приниматть данные по сети. На остальное компьютер в сети это не повлияет.

Кольцо.

При топологие "кольцо" компьютер подключается ккабелю,замкнутому в кольцо. Поэтому у кабеля просто не может быть свободного конца, к которому надо подключать терминатор. Сигналы передаются по кольцу в одном направлении и проходят через каждый компьютер. В отличие от пассивной топологие "шина", здесь каждый компьютер выступает в роли ретера, усиливая сигналы и передавая их следующему компьютеру. Поэтому, если выйдет из строя один компьютер, прекращает функционировать вся сеть.

Передача маркера.

Один из принципов передачи данных в кольцевой сети носит название передачи маркера. Суть его такова. Маркер последовательно, от одного компьютера к другому, передаётся до тех пор, пока его не получит тот, который хочет передать данные. Передающий компьютер изменяет маркер, помещает электронный адрес в данные и посылает их по кльцу. Данные проходят через каждый компьютер, пока не окажутся у того, чей адрес совпадает с адресом получателя, укзанным в данных. После этого принимающий компьютер посылает передающиму сообщение, где потверждает факт прёма данных. Получив потверждение, передающй компьютер создаёт новый маркер и возвращает его в сеть. В кольце диаметром 200 м маркер может циркулировать с частотой 10000 оборотов в секунду.

Концентраторы.

В настоящее время одним из стандартных компонентов етей становится концентратор. А в сетях с топологией "звезда" он служит центральным узлом.

Активные концентраторы.

Генерируют и передают сигналы также, как это делают репитеры. Они имеют от 8 до 12 портов для подключения компьютера.

Пассивные концентраторы.

Они просто пропускают через себя сигнал как узлы коимутации, не усиливая и не восстанавливая его. Пассивные концентраторы не надо подключать к источнику питания.

Гибридные концентраторы.

К ним можно подключать кабели разных типов. Использование коннцентраторов даёт ряд преимуществ. Разрыв кабеля в сети с топологией "линейная шина" приведет к "падению" всей сети. Между тем разрыв кабеля, подключенного к концентратору, нарушит работу только данного сегмента. Остальные сегменты останутся работоспособными.

От сети отключается только компьютер, кабель которого отсоединился или имеет разрыв. Другие преимущества использования концентраторов:

- простота изменения или расширения сети: дастаточно просто пдключить ещё один компьютер или концентратор;

- использование различных портов для подключения кабелей разных тиипов;

- централизованный контроль за работой сети и сетевым трафиком во многих сетях активные концентраторы наделены диагностическими возможностями, позволяющими определить работоспособность соединения.

Комбинированные топологии.

Звезда-шина.

Звезда -шина (star-bus) - это комбинация топологий "шина"и "звезда". Чаще всего это выглядит так: несколько сетей с топологиией "звезда" объединяются при помощи магистральной линейной шины.

Звезда - кольцо.

Эта топология несколько похожа на звезду-шину. Отличие втом, что концентраторы в звезде-шине соединены магистральной линеной шиной, а в звезде-кольце на основе главного концентратора они образуют звез

Резюме.

Топологией называется определённое физическое расположение компьютера. 3 базовых типа топологии: шина, звезда, кольцо. На их основе строятся различные комбинации: например, зведа - шина, звезда - кольцо.

Шина - самая простая и распространенная топология. Все компьютеры соединены одним кабелем. Сигналы предаются всем компьютерам в сети. Чтобы предотвратитть отражение, к концам кабеля подключают терминаторы. Предавать одномоментно может только один

компьютер. Поэтому, чем больше компьютер, тем меньше пропускная способность сети.

В топологии "звезда" каждый компьютер подключён к центральному компоненту-концентратору. Если концентратор выходит из строя, перестаёт функционировать вся сеть.

Контрольные вопросы.

1. Топология сети.
2. Базовые топологии.
3. Шина.
4. Звезда.
5. Кольцо.
6. Концетраторы.
7. Комбинированные сети.
8. Терминатор.
9. Расширение ЛВС.

Ключевые слова

Компоновка;

Диаграмма;

Карта;

Шина;

Звезда;

Кольцо;

Терминатор;

Топология;

Репитер.

Лекция № 3.

Сетевой кабель - физическая среда передачи.

План:

Основные группы кабелей.

Структура коаксиального кабеля.

Типы коаксиальных кабелей

Оборудование для подключения коаксиальных кабелей.

Витая пара.

Неэкранированная витая пар.

Экранированная витая пара.

Оптоволокновый кабель.

Узкополосая передача.

Основные группы кабелей.

На сегодняшний день подавляющая часть сетей использует для соединения провода или кабеля. Они выступают в качестве среды передачи сигналов между компьютерами. Существуют различные типы кабелей. Но в большинстве сетей применяются только 3 основные группы кабелей:

- коаксиальный кабель,
- витая пара: неэкранированная, экранированная,
- оптоволокнолоконный кабель.
- коаксиальный кабель.

Коаксиальный кабель недорог, лёгок, гибок и удобен в применении. Он безопасен и прост в установке. Самой простой коаксиальный кабель состоит медной жилы, изоляции, её окружающей, экрана в виде металической оплетки и внешней оболочки. Если кабель, кроме металической оплётки, имеет и слой фольги, то он называется кабелем с двойной экранизацией. При наличии сильных помех можно воспользоваться кабелем с учетверённой экранизацией. Он состоит из 2-ного слоя фольги и 2-ного слоя металической оплётки.

Структура коаксиального кабеля.

Некоторые типы кабелей покрывает металическая сетка-экран. Сетка защишает передаваемые по кабелю данные, поглощающая внешние электро магнитные сигналы, называемые помехами или шумом. Таким образом экранне позволяет помехам исказить данные. Электрические сигналы, кодирующие данные, передаются по жиле. Жила - это один провод или пучок проводов. Сплошная жила изготавливается, как правило из меди. Жила окружена изоляционным слоем, который отделяет её от металлической оплетки. Оплетка играет роль заземления и защищает жилу от электрических шумов и перекрёстных помех. Перекрёстные помехи -это электрические наводки, вызванные сигналами в соседних проводах.

Проводящая жила и металлическая оплетка не должны соприкасаться, иначе произойдёт короткое замыкание, помехи проникнут в жилу и данные разрушаться. Снаружи кабель покрыт непроводящим слоем - из резины, телефона, пластика. Коаксиальный кабель, более помехоустойчив; затухание сигнала в ней меньше чем в витовой паре. Затухание - это уменьшение величины сигнала при его перемещению по кабелю. Коаксиальный кабель можно использовать при передаче на большие расстояния и в тех случаях, когда высокоскоростная передача данных осуществляется на несложном оборудовании.

Типы коаксоальных кабелей:

- тонкий коаксиальный кабель;
- толстый коаксиальный кабель.

Выбор того или иного типа кабеля зависит от потребностей конкретной сети.

Тонкий коасиальный кабель.

Это гибкий кабель диаметром около 0,5 см. Прост в применении и годится практически для любого типа сети. Подключается

непосредственно к плате сетевого адаптера компьютера. Способен передавать сигнал на расстояние до 185 м, без его заметного жения вызванного затуханием. Для различных типов кабелей любая специальная маркировка. Тонкий коаксиальный кабель относится к группе, которая называется семейством RG-58, его волновое сопротивление 50 Ом. Волновое сопротивление - это сопротивление переменному току. Отличительная способность семейства RG-58 - медная жила. Она может быть иной или состоять из нескольких переменных проводов.

Толстый коаксиальный кабель.

Относительно жёсткий кабель с диаметром около 1 см. Иногда его называют "Стандартной Ethernet", поскольку он был первым типом кабеля, применяемым в Ethernet-популярный сетевой архитектуре. Медная жила этого кабеля толще, чем у тонкого коаксиального кабеля. Чем толще жила у кабеля, тем больше расстояние способен преодолеть сигнал. Следовательно, толстый коаксиальный кабель передаёт сигналы дальше, чем тонкий коаксиальный кабель - до 500 м. Поэтому коаксиальный кабель иногда используют в качестве основного кабеля, который соединяет несколько небольших сетей, построенных на тонком коаксиальном кабеле. Для подключения к толстому коаксиальному кабелю применяется специальное устройство - трансивер.

Трансивер снабжён специальным конкретором, котрый назван весьма впечатляюще - "зуб вампира" или "пронзающий ответитель". Этот "зуб" проникает через изоляционный слой и вступает в непосредственный физический контакт с проводящей жилой. Чтобы подключить трансивер к сетевому адаптеру, надо кабель трансивера подключить к коннектору AVI-порта сетевой платы. Этот коннектор известен так же как DIX-коннектор, или конннектор DB-15.

Сравнение 2-х типов коаксиальных кабелей.

Чем толще кабель, тем сложнее с ним работать. Тонкий коаксиальный кабель гибок, прост в установке и относительно недорог.

Толстый коаксиальный кабель трудно гнуть, и следовательно его сложнее устанавливать. Это очень существенный недостаток, особенно если необходимо проложить кабель по трубам или желобам.

Толстый коаксиальный кабель дороже тонкого, но при этом он передаёт сигналы на большие расстояния.

Оборудование для подключения коаксиального кабеля.

Для подключения тонкого к.к. к Kv используются так называемые BNC- коннекторы. В семействе BNC несколько основных компонентов.

- BNC – коннектор BNC коннектор либо припаивается, либо обжимается на конце кабеля.
- BVC T – коннектор. Соединяет сетевой кабель с сетевой платой компьютера.
- BNC баррел – коннектор. Применяется для сращивания двух отрезков тонкого коаксиального кабеля.
- BNC - терминатор

В сети с топологией "шина" для поглощения "свободных" сигналов терминаторы устанавливаются на каждом конце кабеля. Иначе сеть не будет работать. Классы коаксиальных кабелей и требования пожарной безопасности.

Выбор того или иного класса коаксиальных кабелей зависит от того,где этот кабель будет прокладываться. Существуют два класса коаксиальных кабелей :

- поливинилхлоридные;
- пленумные - для прокладки в области пленума.

Поливинилхлоридные (PVC) - это пластик, который применяется в качестве изолятора или внешней оболочки у большинства коаксиальных кабелей. Кабель PVC достаточно гибок, его можно прокладывать на откратых участках помещений. Однако при горении он выделяет ядовитые газы. Пленум - это небольшое пространство между фальш-потолком и

перекрытием, обычно его используют для вентиляции. Требования пожарной безопасности строго ограничивают типы кабелей, которые могут быть здесь проложены, поскольку в случае пожара выделяемые им дым или газы распространяются по всему зданию. Слой изоляции и внешняя оболочка пленумного кабеля выполнены из специальных огнеупорных материалов, которые при горении выделяют минимальное колличество дыма. Это уменьшает риск химического отравления. Кроме того, эти кабели можно прокладывать открыто, не заключая в трубу. Однако они дороже и жёстче чем PVC.

Некоторые соображения (примечание).

Используйте коаксиальные кабели, если требуется:

- среда для передачи речи, видео и двоичных данных.
- передавать данные на большие расстояния (по сравнению с менее дорогими кабелями).
- знакомая технология, предлагающая достаточный уровеньо защиты данных.

Витая пара.

Самая простая витая пара - это 2 перевитых вокруг друг друга изолированных медных провода. Существуют 2 типа тонкого кабеля: неэкранированная пара (VTP) и экранированная витая пара (STP)

Несколько витых пар часто помещают в одну защитную оболочку. Их количество в таком кабеле может может быть разным. Завивка проводов позволяет избавиться от электрических помех, наводимых соседними парами и другими источниками, реле и трансформаторами.

Неэкранированная витая пара.

Широко используется в ЛВС, максимальная длина сегмента составляет 100 м (328 футов). Состоит из 2-х изолированных медных проводов. Существует несколько спецификаций, которые регулируют колличество витков на единицу длины - в зависемости от назначения кабеля.

Существует 5 категорий кабелей VTP

Категория 1.

Традиционный телефонный кабель, по которому можно передавать только речь, но не данные. Большинство телефонных кабелей, произведённых до 1983 года, относятся к категории 1.

Категория 2.

Кабель, способный передавать данные со скоростью до 4 Мбит/с. Состоит из 4-х витых пара.

Категория 3.

Кабель, способный передавать данные со скорость 10 Мбит/с. Состоит из 4-х витых пар с 9 витками на метр.

Категория 4.

Кабель, способный передавать данные со скоростью 16 Мбит/с. Состоит из 4-х витых пар.

Категория 5.

Кабель, способный передавать данные со скоростью 100 Мбит/с, состоит из 4-х витых пар медного провода.

Большинство телефонных систем используют неэкранизированную витую пару. Это одна из причин её широкой популярности. Причём во многих зданиях, при строительстве, VTP прокладывают не только для сегодняшних нужд телефонизации, но и, предусматривая запас кабеля, в расчёте на будущие потребности. Если провода расчитаны на передачу данных, их можно использовать и в компьютерной сети. Однако надо быть осторожным, так как обычный телефонный провод не имеет витков и его электрические характеристики могут не соответствовать тем, которые требуются для надёжной и безопасной передачи данным между компьютерами.

Одной из проблем для всех типов кабелей являются перекрёстные помехи - неэкранированная витая пара особенно страдает от перекрёстных помех. Для уменьшения их влияния используют экран.

Экранированная витая пара.

Такой кабель (STP) имеет медную оплётку которая, обеспечивает большую зашщиту, чем неэкранированная витая пара. Кроме того, пары проводов STP обмотаны фальгой. В результате экранированная витая пара обладает прекрасной изоляцией, защищающей данные от помех. Вывод: STP, по сравнению с VTP, меньше подвержена воздействию электрических помех и может передавать данные с более высокой скоростью и на большие расстояния.

Компоненты кабельной системы.

Соединители (connectors)

Для подключения витой пары к компьютеру используются телефонные коннекторы RG-45. На первый взгляд, они похожи на RG-11, но между ними есть отличия. Во-первых, вилка RG-45 больше по размерам и не не подходит для гнезда RG-11. Во-вторых, коннектор RG-45 имеет 8 контактов, а RG-11 только 4. Построить развитую кабельную систему и упростить работу с ней поможет ряд полезных компонентов.

Распределительные стойки и полки.

Они предназначены для монтажа кабеля. Позволяют централизованно организовать множество соединений и при этом занимают мало места.

Коммуникационные панели. (path panels).

Существуют разные типы панелей расширения. Поддерживают до 96 портов и скорость передачи до 100 Мбит/с.

Соединители.

Одинарные или двойные вилки RG-45 подключаются к панелям расширения или нестенным розеткам. Обеспечивают скорость передачи данных до 100 Мбит/с.

Настенные розетки.

К ним можно подключить два или более соединителя. Некоторые соображения. Используйте витую пару, если:

- Вы ограничены в денежных средствах при организации ЛВС.
- Вам нужна достаточно простая установка, при которой подключение компьютеров - несложная операция.
- Не используйте витую пару, если Вы хотите быть абсолютно увере-
- ны в целостности данных, передаваемых на большие расстояния с большой скоростью.

Оптововолокновый кабель.

В оптоволокновых кабелях цифровые данные распортстраняются в виде модулированных световых импульсов. Это относительно надёжный способ передачи, так как электрические сигналы при этом не передаются. Следовательно, оптоволокновые кабели нельзя вскрыть и перехватить данные, от чего незастрахован любой кабель, проводящие электрические сигналы. Оптоволокноввй кабель предназначен для перемещения больших объёмов данных на очень высоких скоростях, так как сигнал в нём практически не затухает и не искажается.

Строение

Оптическое волокно-тонкий стеклянный цилиндр, называемый жилой, покрытый слоем стекла, называемого оболочкой с иным, чем у жилы коэффициентом преломления. Иногда оптоволокно производят из пластика. Но ластик передаёт световые импульсы на меньшее расстояния. Стеклянное оптоволокно передаёт сигналы только в одном направлении, поэтому кабель состоит из 2-х волокон с отдельными коннекторами. Одно служит для передачи, другое - для приёма. Жёсткость волокн увеличена покрытием из пластика, а прочность волокнами кевлара. Кевлартовые волокна распологаются между 2 кабелями, заключённы между в пластик. Предача по оптоволоконному кабелю не подвержена электрическим по схемам ведётся на чрезвычайно высокой скорости (в настоящее время(1995

г.) до 100 Мбит/с, теоритически возможная скорость - 200000Мбит/с). По нему можно можно передавать световой импульс на многие километры.

Некоторые соображения.

- Вы планируете посылать данные с очень высокой скоростью на большие расстояния и по надёжной (защищённой) среде передачи.
- Не используйте оптоволоконный кабель, если : Вы ограничены в денежных средствах.
- Вы не обладаете навыками, необходимыми для правильной установки и корректного подключения оптоволоконных сетей устройств.

Узкополосная передача.

Узкополсные системы передают данные в виде цифрового сигнала одной частоты. Сигналы представляют собой дискретные электрические или световые импульсы. При таком способе вся ёмкость комуникационного канала используется для передачи одного импульса или, другими словами, цифровой сигнал использует всю полосу пропускания кабеля. Полоса-эта разница между максимальной и минимальной частотой, которая может передана по кабелю.

Каждое устройство в сетях с узкополосной передачей посылает данные в обоих направлениях, а некоторые могут одновременно и передавать их и принимать. Узкополосная передача. Двунаправленная цифровая волна. Продвигаясь по кабелю, сигнал постепенно затухает и, как следствие, может исказиться. Если кабель слишком длинный, на дальнем его конце передаваемый сигнал может исказиться до неузнаваемости или просто пропасть. Чтобы избежать этого, в узкополосных системах используют репитеры, которые усиливают сигнал и ретранслируют его в дополнительные сегменты, позволяя тем самым увеличить общую длину кабеля.

Широкополосная передача.

Широкополосные системы передают данные в виде аналогового сигнала, который использует некоторый интервал частот. Сигналы представляют собой непрерывные (а не дискретные) электромагнитные или оптические волны. При таком способе сигналы передаются по физической среде в одном направлении. Ели обеспечить необходимую полосу пропускания, то по одному кабелю одновременно может идти вещание нескольких систем, таких, как кабельное телевидение и передачи данных. Каждой передающей системе выделяется часть полосы пропускания. Все устройства связанные с данной системой (например компьютеры), должны быть настроены таким образом, чтобы работать именно с выделенной частью полосы пропускания.

В узкополосных системах для восстановления сигнала используют репитеры, а в широкополосных - усилители. В широкополосной системе сигнал передаётся только в одном направлении, поэтому, чтобы все устройства могли и принимать и передавать данные необходимо обеспечить 2 пути для прохождения сигнала. Разработано 2 основных решения:

- разбить полосу пропускания на 2 канала, которые работают с различными частотами; один канал для передачи сигналов, другой для приёма.
- использовать 2 кабеля; один кабель предназначен для передачи сигнлов, другой для приёма.

Контрольные вопросы

1. Какие основные группы кабелей вы знаете.
2. Классы коаксиальных кабелей.
3. Витая пара.
4. Перечислить ряд полезных компонентов.
5. Оптоволокновый кабель.
6. Узкополосная передача.
7. Широкополосная передача.
8. Экранированная витая пара.
9. Неэкранированная витая пара.

Ключевые слова

Экрнирование;

перекрестные помехи;

затухание;

пленум;

коаксиальный кабаль;

витая папра;

оптоволокновый кабель.

Лекция № 4

Беспроводные сети.

План:

Беспроводная среда.

Типы беспроводных сетей.

Локальные вычислительные сети.

Способы передачи.

Радиопередача в узком спектре.

Передача “точка-точка”.

Мобильные сети.

Сотовые сети.

Беспроводная среда

Беспроводная среда постепенно входит в нашу жизнь. Как только технология окончательно сформируется, производители предложат широкий выбор продукции по приемлемым ценам, что приведет к росту спроса на нее, и к увеличению объема продаж. В свою очередь, это вызовет дальнейшее совершенствование и развитие беспроводной среды.

Словосочетание "беспроводная среда" может ввести в заблуждение , поскольку означает полное отсутствие проводов в сети. В действительности же это не так. Обычно беспроводные компонентывзаимодействуют с сетью, в которой- как среда передачи - используется кабель. Такая сеть со смешанными компонентами называется гибридной.

Возможности

Идея беспроводной среды весьма привлекательна, так как ее компоненты:

- 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.

Применение

Трудность установки кабеля - фактор, который дает беспроводной среде неоспоримое преимущество. она может оказаться 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 или зданиях;
- в помещениях, планировка которых часто меняется;
- в строениях (например, памятниках архитектуры или истории),где прокладывать кабели нежелательно.

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 компьтеров в качестве среды

передачи сигналов выступают AT&T, MCI, Sprint, местные телефонные компаниии 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.

Точка доступа

Трансивер, называемый иногда точкой доступа, обеспечивает обмен сигналами между компьютерами с беспроводным подключением и остальной сетью. В беспроводных ЛВС используются небольшие настенные трансиверы. Они устанавливают радиоконтакт между переносными устройствами. Такую сеть нельзя назвать полностью беспроводной именно изза использования этих трансиверов.

Способы передачи

Беспроводные локальные сети используют четыре способа передачи данных:

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

Инфракрасное излучение

Все инфракрасные беспроводные сети используют для предачи данных инфракрасные лучи. В подобных системах необходимо генерироватьочень 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.

Как говорит само название, 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 тем, что требует прямой видимости между передатчиком и приемником. Если по какимлибо причинам луч будет прерван, это прервет и передачу.

Радиопередача в узком спектре

Этот способ напоминает вещание обыкновенной радиостанции. Пользователи настраивают передатчики и приемники на определенную частоту. при этом прямая видимость необязательна, площадь вещания

составляет около 46 500 м 42 (500 000) квадратных футов).Сигнал высокой частоты, который используется, не проникает через металлические или железобетонные преграды. Связь относительно медленная 4 (около 4,8 Мбит/с).

Радиопередача в рассеянном спектре

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 течении предопределенного промежутка времени настроены на установленный интервал, после чего переключаются на другой интервал. переключение всех 0 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 43,2 км на открытом пространстве и до 120 м внутри здания. Это тот случай, когда технология позволяет получить по настоящему беспроводную сеть.

Передача "точка- точка"

Данный способ передачи несколько выходит за рамки существующего определения сети. Технология передачи "точка- точка" предусматривает обмен данными только между компьютерами, в отличие от взаимодействия между несколькими компьютерами и периферийными устройствами. Однако, чтобы организовать сеть с беспроводной передачей, надо использовать дополнительные компоненты, такие, как одиночные и хост-трансиверы. Их можно устанавливать как на одиночных компьютерах, так и на компьютерах, подключенных к сети. Эта технология, основанная на последовательной передаче данных, обеспечивает:

- высокоскоростную и безошибочную передачу, применяя радиоканал “точка- точка”;
- проникание сигнала через через стены и перекрытия;

- скорость передачи от 1,2 до 38,4 Кбит/с на расстояние до 60 м внутри здания и на 530 м - в условиях прямой видимости. Подобные системы позволяют передавать сигналы между компьютерами, между компьютерами и другими устройствами, например принтерами или сканерами штрих кода.

Расширенные локальные сети

Некоторые типы беспроводных компонентов способны функционировать в расширенных ЛВС так же, как и их аналоги- в кабельных сетях. Беспроводной мост, например, соединяет сети, находящиеся друг от друга на расстоянии до 3 миль.

Многоточечное беспроводное соединение

Компонент, называемый беспроводным мостом, 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 зданиями.

Беспроводные мосты дальнего действия

Если расстояние, которое "покрывает" беспроводной мост, недостаточно, можно установить мост дальнего действия. Для работы с сетями Ethernet и Token Ring на 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.

Такая форма связи удобна, но и довольна 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 беспроводной сети применяются беспроводные адаптеры, использующие технологию сотовой связи. Небольшие антенны, установленные на переносных компьютерах, связывают их с окружающими радиоретрансляторами.

Пакетное радиосоединение

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

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

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

Сотовые сети

Сотовые цифровые пакеты данных 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.

Микроволновые системы

Микроволновая технология помогает организовать взаимодействие между зданиями в небольших, компактных системах, например в университетских городках. На сегодняшний день микроволновая технология - наиболее распространенный в Соединенных Штатах метод передачи данных на дальние расстояния. Он идеален при взаимодействии - в прямой видимости - двух точек, таких, как:

- спутник и наземная станция;
- два здания;
- любые объекты, которые разделяет большое пространство (например, водная поверхность или пустыня). Микроволновая система состоит из следующих компонентов.
- Двух радиотрансиверов. Один для генерации сигналов (передающая станция), а другой для приема (приемная станция).
- Двух направленных антенн.

Они нацелены друг на друга так, чтобы осуществить прием сигналов, передаваемых трансиверами. Эти антенны часто устанавливают на вышки, чтобы покрыть большие расстояния.

Контрольные вопросы.

1. Беспроводная среда?
2. Различие между баспроводными средами передачи?
3. Типы беспроводных сетей?
4. Перечислите типы инфрокрасных сетей?
5. Какая технология похажа на инфрокрасную сеть?
6. Мобильные сети?
7. В каких средах используются мобильные сети? Перечислить.

Ключевые слова.

Беспроводная среда;

Мобильные сети;

Локальные сети;

Радиопередача;

Сотовые сети;

Приемник;

Микроволновая система

Лекция № 5

Платы сетевого адаптера.

План:

Назначение платы сетевого адаптера.

Примечание.

Базовый порт ввода/вывода.

Базовый адрес памяти.

Выбор трансивера.

Назначение платы сетевого адаптера

Платы сетевого адаптера выступают в качестве физического интерфейса, или соединения, между компьютером и сетевым кабелем. Платы выставляются в слоты расширения всех сетевых компьютеров и серверов. Чтобы обеспечить физическое соединение между компьютером и сетью, к соответствующему разъему, или порту, платы (после ее установки) подключается сетевой кабель.

***Назначение платы сетевого адаптера*:**

- подготовка данных, поступающих от компьютера, к передаче по сетевому кабелю;
- передача данных другому компьютеру;
- управление потоком данных между компьютером и кабельной системой.

Плата сетевого адаптера, кроме того, принимает данные из кабеля и переводит их в форму, понятную центральному процессору компьютера. Плата сетевого адаптера состоит из аппаратной части и встроенных программ, записанных в ПЗУ. Эти программы реализуют функции подуровней Управление логической связью и Управление доступом к среде Канального уровня модели OSI. Подготовка данных Перед тем, как послать данные в сеть, плата сетевого адаптера должна перевести их из формы, понятной компьютеру, в форму, в которой они могут передаваться

по сетевому кабелю. Внутри компьютера данные передаются по шинам. Как правило, это несколько проводников, расположенных близко друг к другу. Так как линий несколько, то и биты данных могут передаваться по ним группами, а не последовательно. Шины, которые использовались в первых персональных компьютерах IBM, были известны как 8- разрядные шины: они могли передавать группы по 8 битов данных. IBM PC/AT имеет 16-разрядную шину, это означает, что она способна передавать сразу 16 би ов. Многие овременные компьютеры оснащены уже 32 разрядной шиной. Часто говорят, что данные по шине компьютера передаются параллельно, так как 16 битов или 32 бита движутся параллельно друг другу. Представьте, что 16 разрядная шина - это 16- пол сная автострада, по которой рядом (параллельно) движутся 16 машин, каждая из которых перевозит 1 бит. В сетевом кабеле данные должны перемещаться в виде потока битов. При этом говорят, что происходит последовательная передача, потому что биты следуют друг за другом. Иными словами, кабель- это дорога с одной полосой. По таким "дорогам" данные в каждый момент времени движутся в одном направ-лении. Плата сетевого адаптера принимает параллельные данные и организует их для последовательной, (побитовой), передачи. Этот процесс завершается пере-водом цифровых данных компьютера в электрические и оптические сигналы, которые и передаются о сетевым кабелям. Отвечает за это преобразование трансивер. Сетевой адрес помимо преобразования данных, плата сетевого адаптера должна указать свое местонахождение, или адрес, чтобы ее могли отличить от других плат. Сетевые адреса должны быть определены комитетом IEEE. Этот комитет закрепляет за каждым производителем плат сетевого адаптера некоторый интервал адресов. Производители "зашивают" эти адреса в микросхемы. Благодаря этому каждая плата, а следовательно, каждый компьютер имеют уникальный адрес в сети. При приеме даннах от компьютера и подготовке их к

передаче по сетевому кабелю плата сетевого адаптера участвует также в других операциях.

1. Компьютер и плата сетевого адаптера должны быть связаны друг с другом, чтобы осуществлять передачу данных (от компьютера к плате). Если плата может использовать прямой доступ к памяти, компьютер выделяет ей некоторую область своей памяти.

2. Плата сетевого адаптера запрашивает у компьютера данные.

3. Шина компьютера передает данные из его памяти плате сетевого даптера.

Часто данные поступают быстрее, чем их способна передать плата сетевого адаптера, поэтому они временно помещаются в буфер. Передача и управление данными Перед тем как послать данные по сети, плата сетевого адаптера проводит электронный диалог с принимающей платой, во время которого они "обговаривают":

- максимальный размер блока передаваемых данных;
- объем данных, передаваемых без подтверждения о получении;
- интервалы между передачами блоков данных;
- интервал, в течении которого необходимо послать подтверждение;
- объем данных, который может принять каждая плата не переполняясь;
- скорость передачи данных;

Если новой (более сложной и быстрой) плате необходимо взаимодействовать со старой (медленной) платой, они должны найти общую для обеих скорость передачи. Схемы некоторых современных плат сетевого адаптера позволяют им приспособиться к медленн й скорости старых плат. Каждая плата оповещает другую о своих параметрах, принимая чужие параметры и подстраиваясь к ним. После того как все детали определены, платы начинают обмен данными. Параметры

конфигурации, Параметры платы сетевого адаптера должны быть корректно установлены, чтобы ее работа протекала правильно. В их число входят:

- прерывание;
- базовый адрес порта ввода/вывода;
- базовый адрес памяти;
- используемый трансивер.

Примечание.

Параметры платы сетевого адаптера иногда устанавливаются в программном обеспечении, но они должны совпадать с установками, заданными на плате перемычками или DIP - переключателями. Дополнительную информацию о настройке платы с помощью переключателей можно получить из ее документации. Прерывание Линии запроса прерывания - это физические линии, по которым различные устройства (например, порты ввода/вывода, клавиатура, драйверы дисков и платы сетевого адаптера) могут послать микропроцессору компьютера запросы на обслуживание, или на пре ы-вание. Линии запроса прерывания встроены в аппаратуру компьютера, они имеют различные уровни приоритетов, что позволит процессору определить наиболее важный из запросов. Посылая компьютеру запрос, плата сетевого адаптера использует прерывание - электрический сигнал, который направляется центральному процессору компьютера. Все устройства в компьютере должны пользоваться разными линиями запроса прерывания, ил прерыванием (IRQ). Линия запроса прерывания задае-тся при настройке устройства. (Примеры см. в таблице.) В большинстве случаев платы сетевого адаптера используют прерывание IRQ3, IRQ5,IRQ10 или IRQ11. Если есть выбор, рекомендуем отдать предпочтение IRQ5, тем более что это значение установлено по умолчанию во многих системах. Чтобы оп еделить, какие значения прерывания установлены по умолчанию в Вашей системе, воспользуйтесь диагностическими программными утилитами, например

Microsoft Diag-nostic (MSD). Если ни IRQ3, ни IRQ5 не доступны, выберите другой доступный номер прерывания (никакое другое устройство Вашего компьютера не должно его использовать) из таблицы. IRQ Компьютер с процессором 80286 (или выше)

Базовый порт ввода/вывода

Базовый порт ввода/вывода определяет канал по которому курсируют данные между устройством компьютера (например, платой сетевого адаптера и его центральным процессором. Для центрального процессора порт выглядит как адрес. Каждое устройство системы должно иметь уникальный адрес базового порта ввода/вывода. Адреса портов (в шестнадцатеричном формате), предс-тавленные в следующей таблице, если они не заняты, могут быть выделены плате сетевого адаптера. Здесь перечислены адреса портов и соответствующие им устройства. Сверьтесь с документацией компьютера чтобы уточнить занятые адреса.

Базовый адрес памяти

Базовый адрес памяти указывает на ту область памяти компьютера (RAM), которая используется платой сетевого адаптера в качестве буфера для ходящих и исходящих кадров данных. Этот адрес иногда называется начальным адресом RAM. Часто базовым адресом памяти у платы сетевого адаптера является D8000. (Для некоторых плат последний нуль не указывается: Вместо D80000 пишется D800.) Запомните, необходимо выбрать базовый адрес памяти , не занятый другим устройством.

Примечание.

У плат сетевого адаптера, которые не используют оперативную память системы, отсутствует такой параметр, как базовый адрес памяти. Некоторые платы сетевого адаптера имеют параметр, позволяющий выделить определенный объем памяти для хранения кадров данных. Например, есть платы, в которых вы можете выделить 16 Кб или 32 Кб памяти. Чем больше памяти Вы выделяете, тем выше скорость сети , но тем меньше памяти остается для других целей.

Выбор трансивера

Плата сетевого адаптера может иметь и дополнительные параметры, их также необходимо задать при конфигурировании. Например, некоторые платы поставляются с внешним и встроенным трансивером- Вы должны задать тот трансивер, который будет использован. Выбор часто производится с помощью перемычек небольших соединителей, которые, связывая два вывода, определяют, какая цепь будет использоваться платой.

Совместимость.

Чтобы обеспечить совместимость компьютера и сети, плата сетевого адаптера должна отвечать следующим требованиям:

- соответствовать внутренней структуре компьютера (архитектуре шине данных);
- иметь соединитель (он должен подходить к типу кабельной системы) для подключения сетевого кабеля.

Например, плата, которая должна работать в компьютере Apple в сети с топологией "шина", не будет работать в компьютере IBM в сети с топологией "кольцо". Сеть топологии "кольцо" требует плату, которая физически отличается от применяемой в сети топологии "шина", к тому же Apple использует другой метод взаимодействия по сети и внутреннюю системную шину.

Контрольные вопросы.

1. Основные характеристики ифункции платы сетевого адаптера?
2. Типы разъемов для подключения кабеля?
3. Сетевой адрес?
4. Передача и управление данными?
5. Сетевые кабели и соединители?
6. Какие соединители используются в телефонных сетях?
7. Назначение платы сетевого адаптера.

Ключевы слова.

Прерывание;

трансчивер;

мышь;

шина;

коннектор;

серверкоаксиальный кабель;

неэкранированная витая пара.

Лекция № 6

Сетевые модели OSI и IEEE Project 802

План:

Работа сети.

Модель OSI.

Многоуровневая архитектура.

Прикладной уровень.

Представительский уровень

Сеансовый уровень.

Трнспортный уровень.

Сетевой уровень.

Канальный уровень.

Физический уровень.

Работа сети

Работа сети заключается в передаче данных от одного компьютера к другому. В этом процессе можно выделить несколько конкретных задач:

- распознать данные;
- разбить данные на управляемые блоки;
- добавить информацию к каждому блоку, чтобы указать местонахождение данных;
- указать получателя;
- добавить информацию синхронизации и информацию для проверки ошибок;
- поместить данные в сеть и отправить их по заданному адресу.

Модель OSI

В 1978 году International Standards Organization (ISO) был выпущен на бор спецификаций, описывающих архитектуру сети с неоднородными уст ройствами. Исходный документ относился к открытым системам, чтобы

все они могли использовать одинаковые протокол и стандарты для обмена ин формацией.

Примечание.

Каждый профессионал в области компьютерных сетей должен знать основные организации, разрабатывающие сетевые стандарты и их вклад в развитие сетей. В 1984 году ISO выпустила новую версию своей модели , названную эталонной моделью взаимодействия открытых систем (Open System Interconnection reference model, OSI). Версия 1984 года стала международным стандартом: именно ее спецификации используют производители при разработке сетевых продуктов, именно ее придерживаются при разработке сетей. Эта модель широко распространенный метод описания сетевых сред. Являясь многоуровневой системой, она отражает взаимодействие программного и аппаратного обеспечения при осуществлении сеанса связи, а также помогает решить разнообразные проблемы.

Многоуровневая архитектура

В модели OSI сетевые функции распределены между семью уровнями Каждому уровню соответствуют различные сетевые операции, оборудование и протоколы. На каждом уровне выполняются определенные сетевые функции, которые взаимодействуют с функциями соседних уровней, вышележащего и нижележащего. Например, сеансовый уровень должен взаимод йствовать только с Представительским и Транспортным уровнем и т.п. Все эти функции подробно описаны. Нижние уровни 1-й и 2-й - определяют физическую среду передачи данных и соответствующие задачи (такие, как передача битов данных через плату сетевого адаптера и кабель). Самые верхние уровни определяют, каким способом осуществляется доступ п иложений к услугам связи. Чем выше уровень, тем более сложную задачу он решает. Каждый уровень предоставляет несколько услуг (т.е. выполняет несколько операций), подготавливающих данные для доставки по сети на другой компьютер. Уровни отделяются

друг от друга границами- интерфейсами. Все запросы от одного уровня к другому передаются через интерфейс. Каждый уровень использует услуги нижележащего уровня.

7.Прикладной уровень.

6.Представительский уровень.

5.Сеансовый уровень.

4.Транспортный уровень.

3.Сетевой уровень.

2.Канальный уровень.

1.Физический уровень.

Взаимодействие уровней модели OSI

Задача каждого уровня - предоставление услуг вышележащему уровню, маскируя детали реализации этих услуг. При этом каждый уровень на одном компьютере работает так, будто он напрямую связан с таким же уровнем на другом компьютере. Однако в действительностисвязь осуществляется между смежными уровнями одного компьютера - программное обеспечение, работающее на каждом уровне, реализует определенные сетевые функции в соответствии с набором протоколов. Перед подачей в сеть данные разбиваются на пакеты . Пакет (packet) это единица информации, передаваемая между устройствами сети как единое целое. Пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне к пакету до авляется некоторая информация, форматирующая или адресная, которая необходима для успешной передачи данных по сети.

На принимающей стороне пакет проходит через все уровни в обратном порядке. Программное обеспечение на каждом уровне читает информацию пакета, затем удаляет информацию, добавленную к пакету на этом же уровне отправляющей стороной, и передает пакет следующему уровню. Когда пакет дойдет до Прикладного уровня, вся адресная информация будет удалена и данные примут свой первоначальный вид.

Таким образом, за исключением самого нижнего уровня сетевой модели, никакой другой уровень не может непосредственно послать информацию соответствующему уровню другого компьютера. Информация на компьютера- отправителе должна пройти через все уровни Затем она передается на компьютера- получатель по сетевому кабелю и опять проходит через все слои, пока не достигнет того же уровня, с которого она была послана на компьютера отправителе. Например, если Сетевой уровень передает информацию с компьютера А, она спускается через Канальный и Физический уровни в сетевой кабель, далее по нему попадает в компьютера В, где поднимается через Физический и Канальный уровни и достиает Сетевого уровня.

В клиент- серверной среде примером информации, переданной Сетевым уровнем компьютера А Сетевому уровню компьютера В, мог бы служить адрес и, очевидно, информация контроля ошибок, добавленные к пакету.

Взаимодействие смежных уровней осуществляется через интерфейс. Интерфейс определяет услуги, который нижний уровень предоставляет верхнему, и способ доступа к ним. Поэтому каждому уровню одного компьютера окажется, что он непосредственно взамодействует с таким же уровнем другого компьютера.

Далее описывается каждый из семи уровней модели OSI и определяются слуги, которые они предоставляют смежным уровням .

Прикладной уровень

Уровень 7, Прикладной (Application) - самый верхний уровень модели OSI. Он представляет собой окно для доступа прикладных процессов к сетевым услугам. Этот уровень обеспечивает услуги, напрямую поддерживающие приложения пользователя, такие, как про раммное обеспечение для передачи файлов, доступа к базам данных и электронная почта. Нижележащие уровни поддерживают задачи,

выполняемые на Прикладном уровне. Прикладной уровень управляет общим доступом к сети, потоком данных и обработкой ошибок.

Представительский уровень

Уровень 6, Представительский (Presentation), определяет формат, используемый для обмена данными между сетевыми компьютерами. Этот уровень можно назвать переводчиком. На компьютере- отправителе данные, поступившие от Прикладного уровня, на этом уров е переводятся в общепонятный промежуточный формат. На компьютере- получателе на этом уровне происходит перевод из промежуточного формата в тот, который используется прикладным уровнем данного компьютера. Представительский уровень отвечает за преобраз вание протоколов, трансляцию данных, их шифрование, смену или преобразование применяемого набора символов (кодовой таблицы) и расширение графических команд. Представительский уровень, кроме того, управляет сжатием данных для уменьшения передаваемых битов.

На этом уровне работает утилита, называемая редиректором (redirector). Её назначение - переадресовать операции ввода/вывода к ресурсам сервера.

Сеансовый уровень

Уровень 5, Сеансовый (Session) позволяет двум приложениям на разных компьютерах устанавливать, использовать и завершать соединение, называемое сеансом. На этом уровне выполняются такие функции, как распознавание имен и защита, необходимые для связ двух приложений в сети. Сеансовый уровень обеспечивает синхронизацию между пользовательскими задачами посредством расстановки в потоке данных контрольных точек. Таким образом, в случае сетевой ошибки, потребуется заново передать данные, следующие за последней контр льной точкой . На этом уровне выполняется управление диалогом между взаимодействующими процессами, т.е. регулируется, какая из сторон осуществляет передачу, когда, как долго и т.д.

Транспортный уровень

Уровень 4, Транспортный (Transport), обеспечивает дополнительный уровень соединения - ниже сеансового уровня. Транспортный уровень гарантирует доставку пакетов без ошибок, в той же последовательности, без потерь и дублирования. На этом уровне сообщен я переупаковываются: длинные разбиваются на несколько пакетов, а короткие объединяются в один. Это увеличивает эффективность передачи пакетов по сети. На Транспортном уровне компьютера-получателя сообщения распаковываются, восстанавливаются в пер оначальном виде, и обычно посылается сигнал подтверждения приема. Транспортный уровень управляет потоком, проверяет ошибки и участвует в решении проблем, связанных с отправкой и получением пакетов.

Сетевой уровень

Уровень 3, Сетевой (Network), отвечает за адресацию сообщений и перевод логических адресов и имен в физические адреса. Одним словом исходя из конкретных сетевых условий, приоритета услуги и других факторов здесь определяется маршрут от компьютератправителя к компьютеру получателю. На этом уровне решаются также такие задачи и проблемы, связанные с сетевым трафиком, как коммутация пакетов, маршрутизация и перегрузки. Если сетевой адаптер маршрутизатора не может передавать большие блоки данных, посланные компьютером-отправителем, на Сетевом уровне эти блоки разбиваются на меньшие. А сетевой уровень компьютера получателя собирает эти данные в исходное состоние.

Канальный уровень

Уровень 2, Канальный, осуществляет передачу кадров данных от Сетевого уровня к Физическому. Кадры - это логически организованная структура, в которую можно помещать данные. Канальный уровень компьютера- получателя упаковывает “сырой” поток битов, поступающих от Физического, в кадры данных. Управляющая информация используется

для маршрутизации, а также указывает на ти пакета и сегментацию . Данные - собственно передаваемая информация. CRC(остаток избыточной циклической суммы)- это сведения, которые помогут выявить ошибки, что, в свою очередь, гарантирует правильный прием информации. Канальный уровень (Data link) обеспечивает точность передачи кадров между компьютерами через Физический уровень. Это позволяет Сетевому уровню считать передачу данных по сетевому соединению фактически безошибочной. Обычно, когда Канальный уровень посылает кадр, он ожидает со стороны получателя подтверждения приема. Канальный уровень получателя проверяет наличие возможных ошибок передачи. Кадры, поврежденные при передаче, или кадры, получение которых не подтверждено, посылаются вторично.

Физический уровень

Уровень 1, Физический, - самый нижний в модели OSI. Этот уровень осуществляет передачу неструктурированного, “сырого” потока битов по физической среде (например, по сетевому кабелю.) Здесь реализуются электрический, оптический , механический и функц ональный интерфейсы с кабелем. Физический уровень также формирует сигналы, которые переносят данные, поступившие от всех вышележащих уровней. На этом уровне определяется способ соединения сетевого кабеля с платой сетевого адаптера, в частности, количество контактов в разъёмах и их функции. Кроме того. Здесь определяется способ передачи данных по сетевому кабелю. Физический уровень предназначен для передачи битов (нулей и единиц) от одного компьютера к другому. Содержание самих битов на данном уровне значения не имеет. Этот уровень отвечает за кодирование данных и синхронизацию битов, гарантируя, что пере анная единица будет воспринята именно как единица, а не как ноль. Наконец, Физический уровень устанавливает длительность каждого бита и способ перевода бита в соответствующие электрические или оптические импульсы, передаваемые по сетевому кабелю.

Контрольные вопросы.

1. Сетевые модели OSI?
2. На каком уровне определяется способ соединения сетевого кабеля с сетевы адаптером.
3. Какие семь уровней модели вы знаете?
4. Опишите взаимодействие уровней модели OSI?
5. На каком уровне находится прикладной уровень? Опишите.
6. Что такое представительский уровень?
7. Что такое транспортный уровень?
8. Что какое сетевой уровень?
9. Что такое сеансовый уровень?

Ключевые слова.

Прикладной;

представительский;

сеансовый;

транспортный;

сетевой;

канальный;

физический;

Лекция № 7

Драйверы

План:

Назначение драйверов.

Сетевая среда.

Драйверы и модель OSI.

Драйверы и сетевое программное обеспечение.

Ввод в действие.

Установка.

Настройка.

Обновление.

Удаление.

Резюме.

Назначение драйверов.

Драйверы (driver) [иногда их называют драйверами устройств (dev ce driver)] - это программное обеспечение, позволяющее компьютеру ра ботать с различными устройствами. Даже если некоторое устройство подключено к компьютеру, операционная система не сможет взаимодейс твовать с ним до тех пор, пока не будет установлен и правильно сконфигурирован драйвер этого устройства. Драйвер - программа, которая "говорит" Компьютеру, как надо управлять или работать с устройством, чтобы оно правильно выполняло все свои функции.

Драйверы существуют почти для каждого типа устройств компьютера и периферии, например:

- устройство ввода (мыши);
- SCSI- и IDE-дисковых контроллеров;
- жестких и гибких дисков;
- устройств мультимедиа (микрофонов, видиокамер, записывающих устройств);

- плат сетевого адаптера;
- принтеров, плоттеров, накопителей на магнитной ленте и т.д.

Как уже говорилось, обычно именно операционная система взаимо действует с драйверами, обеспечивая функционирование устройств. Хоро шим примером использования драйверов может служить драйвер принтера. Принтеры производятся большим количеством фирм и обладают различными функциями и особенностями. Производители компьютеров просто не в состоянии оснастить свои компьютеры программным обеспечением для работы с каждым типом принтера. Вместо этого производители принтеров оздают драйверы для своих принтеров. Чтобы Ваш компьютер мог посылать документы на принтер, сначала надо загрузить драйвер этого принтера, который обеспечит взаимодействие компьютера с этим устройством.

Согласно сложившейся практике, производители периферийных устройств и устанавливаемых в компьютер плат отвечают и за поставку к ним драйверов. Драйверы поставляются на дисках вместе с оборудованием или с операционными системами. Кроме того, они могут быть взяты с таких служб, как The Microsoft Network (MSN) или CompuServe.

К другому типу устройств, требующих наличия драйверов и составляющих пользователям массу неприятностей, относятся дисковые контроллеры. В основном используются два типа контроллеров:

Small Computer System Interface (SCSI);

Integrated Device Electronic (IDE).

SCSI-контроллеры позволяют связывать цепочкой несколько различных устройств, например жестких дисков CD-ROM-дисководов. Этот контроллер, помимо корректного драйвера, требует правильной настройки устройства. Если Вы заменили SCSI-адаптер одного производителя на SCSI-адаптер другого производителя, Вам придется установить корректный драйвер и правильно его сконфигурировать.

Дисковый накопитель типа IDE имеет встроенный контроллер, поэтому его установка и обслужи вание проще.

Сетевая среда

Сетевые драйверы обеспечивают связь между платами етевого адаптера и работающими на компьютере редиректорами. Редиректор - часть сетевого программного обеспечения, которая принимает запросы ввода/вывода, относящиеся к удаленным файлам, и переадресовывает их по сети на другой компьютер. Для установки драйвера часто используется специальная утилита.

Драйверы и модель OSI

Драйверы платы сетевого адаптера располагаются на подуровне Управление доступом к среде (Канальный уровень модели OSI). Подуровень Управления доступом к среде отвечает за совместный доступ плат сете вого адаптера обеспечивает прямую связь между компьютером и самой платой. Это, в свою очередь, связывает компьютер с сетью.

Драйверы и сетевое программное обеспечение

Производители сетевых адаптеров обычно предоставляют драйверы разработчикам сетевого программного обеспечения, которые включают их в состав своих продуктов.

Производители сетевых операционных систем публикуют списки сов местимого оборудования (Hardware Compatibiliti List, HCL) - списки устройств, драйверы которых протестированы и включены в состав опера ционной системы.

Например, HCL для операционной системы Microsoft indows NT Server содержит более 100 моделей плат сетевых адаптеров (от различных производителей), драйверы которых были ротестированы и включены в состав данной операционной системы. Это означает, что в комплект поставки Microsoft Windows NT Server входит более 100 драйверов,

которые позволят ей работать более чем сотней различных плат сетевого адаптера.

И последнее. Даже если драйвер какой-то конкретной платы не был предусмотрен сетевой операционной системой, не расстраивайтесть. Обычно производители плат сетевого адаптера сами включают в комплект поставки диск с драйверами наиболее популярных сетевых операционных систем. Однако перед покупкой платы стоит все-таки убедиться в том, что для Вашей сетевой операционной системы есть драйвер.

Ввод в действие

Ввод в действие и управление драйверами подразумевает их становку, настройку, обновление и удаление.

Установка

В настоящее время наиболее популярные сетевые перационные системы обычно используют для установки интерактивной графический интер фейс. Например, в Microsoft Windows NT Server это делается с помощью утилиты Control Panel.

Настройка

Обычно платы сетевого адаптера имеют несколько параметров, от правильной установки которых зависит корректная работа самого адаптера. Как уже говорилось на занятии , настройку параметров можно осуществить перестановкой перемычек или DIP-переключателей. Однако большинство современных плат сетевого адаптера не имеет ни перемычек, ни DIP-переключателей. Они конфигурируются программно - при установке драйверов или после нее.

Обновление

Время от времени производители вносят в драйверы дополнения или изменения, которые увеличивают прозводительность сетевых компонентов. Эти изменения распространяются или по почте (зарегистрированным пользователем), или через электронную доску объявлений, или с помощью оперативных служб, таких, как The Microsoft

Network (MSN) или CompuServe. Процесс обновления драйверов обычно аналогичен процессу их установки.

Удаление

Иногда может возникнуть ситуация, когда необходимо удалить драйверы. Чаще всего это происходит при конфликте исходных драйверов с новыми. Например, удаляя из системы некоторые оборудование, надо удалить и связанные с ним драйверы, чтобы исключить возможный конфликт этих драйверов с теми, которые будут установлены в последствии. Процесс удаления драйверов обычно аналогичен процессу их установки и обновления.

Резюме

Драйвер - это программа-утилита, позволяющая компьютеру с определенным устройством. Такие устройства, как мышь, исковые накопители, платы сетевого адаптера и принтера, поставляются вместе сосвоими драйверами. Операционная система компьютера не распознает устройство до тех пор, пока не будет установлен необходимый драйвер (если операционная система не поддерживает спецификацию Plug and Play).

Большинство драйверов предоставляется производителями перационных систем. Если же драйвера для какого-то устройства нет, попробуйте найти его на диске, входящим в комплект поставки оборудования. В некоторых случаях драйверы можно получить у оперативных служб типа The Microsoft Network (MSN) или CompuServe.

В сетевой среде каждый компьютер обладает платой сетевого адаптера и соответствующим ей драйвером, благодаря которым компьютер посылает данные по сети. Современные процедуры (с графическим интерфейсом пользователя) облегчают установку драйвера. Эти процедуры аналогичны его установке.

Контрольные вопросы.

1. Драйверы в сетевой среде?
2. Функции драйверов?
3. Назначение драйверов?
4. Установка и удаление драйверов?
5. Драйверы и модель OSI?
6. Что такое драйвер?

Ключевые слова.

Драйвер;

диск;

мультимедия;

микрофон;

видеокамера;

принтер;

плоттер;

магнитная лента;

Лекция № 8

Передача данных по сети

План:

Функции пакетов.

Структура пакетов.

Основные компоненты.

Формирование пакетов.

Адресация пакетов.

Рассылка пакетов.

Резюме.

Функции пакетов

Данные обычно содержатся в больших по размерам файлах. Однако се ти не будут нормально работать, если компьютер посылает этот блок данных целиком. Существует две причины, замедляющие работу сети при передаче по кабелю больших блоков данных.

Во-первых, такой блок, посылаемый одним компьютером, заполняет кабель и "связывает" работу всей сети, т.е. препятствует взаимодействию остальных сетевых компонентов.

Во-вторых, возникновение ошибок при передаче крупных блоков при ведет к повторной передаче всего блока. А если поврежден небольшой блок данных, то требуется повторная передача именно этот небольшого блока, что значительно экономит время.

Чтобы быстро и легко не тратя времени на ожидиния, передавать по сети данные, надо разбить их на небольшие управляемые блоки. Эти блоки называются пакетами или кадрами. Хотя термины "пакет" и "кадр" си нонемичны, полными синонимами они все-таки не являются. Существуют различия между типами сети, которые эти термины отражают.

Пакет - основная единица информации в компьютерных сетях. При разбиении данных на пакеты скорость их передачи возрастает на столько, что каждый компьютер в сети получает возможность принимать и передовать данные практически одновременно с остальными компьютерами. На целевом компьютере (компьютере - получателе) пакеты накапливаются и выстраиваются в должном порядке для восстановления исходного вида данных. При разбиении данных на пакеты сетевая операционная система до бавляет к каждому пакету специальную управляющую информацию. Она обеспечивает:

- передачу исходных данных небольшими блоками;
- сбор данных в надлежащем порядке (при их получении);
- проверку данных на наличие ошибок (после сборки).

Структура пакетов.

Пакеты могут содержать несколько типов данных:

- информацию (например, сообщение или файлы);
- определенные виды данных и команд, управляющих компьютером (например, запросы к службам);
- коды управления сеансом (например, запрос на повторную передачу для исправления ошибки).

Основные компоненты

Некоторые компоненты являются обязательными для всех типов паке тов:

- адрес источника (sourse), идентифицирующей компьютер отправитель;
- передаваемые данные;
- адрес местоназначения (destination), идентифицирующий компь ютер-получатель;

- инструкции сетевым компонентам о дальнейшем маршруте данных;
- информация компьютеру-получателю о том как объединить передава емый пакет с остальными, чтобы получить данные в исходном виде;
- информация для проверки ошибок, обеспечивающая корректность пе редачи.

Компоненты пакета группируются в три раздела: заголовок, данные и трейлер.

Заголовок

Заголовок включает:

- сигнал, "говорящий" о том, что передается пакет;
- адрес источника;
- адрес местоназначения;
- информацию, синхронизирующую передачу.

Данные

Эта часть пакета - собственно передаваемые данные. В зависимости от типа сети ее размер может меняться. Но для большинства сетей он составляет от 512 байтов (0.5 Кб) до 4 Кб. Так как обычно размер исходных данных гораздо больше 4 Кб, для помещения в пакет их необходимо разбить на меньшие блоки. При передаче объемного файла может потребоваться много пакетов.

Трейлер

Содержимое трейлера зависит от метода связи, или протокола. Впро чем, чаще всего трейлер содержит информацию для проверки ошибок, на зываемую циклическим избыточным кодом (Cyclical Redundancy Check, CRC). CRC - это число получаемое в результате математических преобра зований над пакетом и исходной информацией. Когда пакет достигает места назначения эти преобразования повторяются. Если результат совпадает с CRC - пакет принят без ошибок. В противном

случае - при передаче данные изменились, по этому необходимо повторить передачу пакета.

Формат и размер пакета зависят от типа сети. А максимальный размер пакета определяет, в свою очередь, количество пакетов, которое будет создано сетевой операционной системой для передачи большого блока данных.

Формирование пакетов.

Процесс формирования пакета начинается на Прикладном уровне моде ли OSI, т.е. там, где "рождаются" данные. Информация, которую надо переслать по сети, проходит сверху вниз все семь уровней, начиная с Прикладного. На каждом уровне компьютера-отправителя к блоку данных добавляется информация предназначенная для соответствующего уровня компьютера - получателя. Например, информация добавленная на Канальном уровне компьютера-отправителя, будет прочитана Канальным уровнем компьютера - получателя.

Транспортный уровень разбивает исходный блок данных на пакеты. Структура пакетов определяется протоколом, который использует два компьютера - получатель и отправитель. На Транспортном уровне, кроме того, к пакету добавляется информация, которая поможет компьютеру - получателю восстановить исходные данные из последовательности пакетов. Когда, завершив свой путь к кабелю пакет проходит Физический уровень, он содержит информацию всех остальных шести уровней.

Адресация пакетот.

Большинство пакетов в сети адресуются конкретному компьютеру, и, как результат, только он один реагирует на них. Каждая плата сетевого адаптера "видит" все пакеты, передаваемые по сегменту кобеля, но

только при совпадении адреса пакета с адресом компьютера она прерывает его работу. Используется так же и широковещательная адресация (broadcast addressing). На пакет с таким типом адреса одновременно реагирует множество компьютеров в сети. В крупномасштабных сетях, покрывающих огромные территории (или государства), предлагается несколько возможных маршрутов для передачи данных. Коммутирующие и соединяющие сетевые компоненты используют адресную информацию пакетов для определения наилучшего маршрута.

Рассылка пакетов

Сетевые компоненты используют адресную информацию пакетов и лядругих целей: чтобы направлять пакеты по месту назначению и не допускать их в те области сети, к которым они не относятся. В правильной рассылке акетов ключевую роль играют две функции.

Продвижение пакетов. Компьютер может отправить пакет на следующий подходящий сетевой компонент, основываясь на адресе из заголовка пакета.

Фильтрация пакетов. Компьютер может отбирать определенные пакеты на основе некоторых критериев, например адреса.

Резюме

Прежде чем послать данные в сеть, компьютер-отправитель разбивает их на небольшие блоки, которые легче передавать по сетевому кабелю. Эти пакеты, или порции, - основные единицы сетевых коммуникаций. Они обеспечивают современное взаимодействие сетевых компонентов. Все пакеты содержат следующие обязятельные компоненты: адрес источника, данные, адрес местоназначения, инструкции и информацию для проверки ошибок. Каждый пакет состоит из трех разделов: заголовка (включающего сигнал, который "говорит" о том, что передает пакет; адрес источника; адрес местоназначения; информацию,

синхронизирующую передачу), данных и трейлера (включающего информацию для проверки ошибок - CRC).

Формирование пакета начинается на Прикладном уровне модели OSI и продолжается далее, на всех уровнях, поскольку каждый из них добавляет к пакету свою информацию.

Контрольные вопросы.

1. Пакеты в сетевых коммуникациях?
2. Роль и значение пакетов?
3. Основные части пакетов?
4. Формирование пакетов?
5. Передача пакетов?
6. Какие компоненты пакетов вы знаете?
7. Функции пакетов?

Ключевые слова.

Пакет;

трейлер;

данные;

заголовок;

адресация.

Лекция № 9

Протоколы

План:

Назначение протоколов.

Работа протоколов.

Компьютер-отправитель.

Компбютер-получатель.

Маршурутизируемые и немаршрутизируемые протоколы.

Протоколы в многоуровневой архитектуре.

Стеки протоколов.

Прикладные протоколы.

Трагспортные протоколы.

Сетевые протоколы.

Стандартные протоколы.

Распространенные протоколы

Установка и удаление протоклов.

Резюме.

Литература:

Назначение протоколов

Протоколы (protocols) - это набор правил и процедур, регулирующих порядок осуществления некоторой связи. Например, дипломаты какой либо страны четко придерживаются протокола при общении с дипломатами из других стран. В компьютерной среде правила связи служат тем же целям. Протоколы это правила и технические процедуры, позволяющие несколькимкомпьютерам при объединении в сеть общаться друг с другом.

Запомните три основных момента, касающихся протоколов:

1. Существует множество протоколов. И хотя все они участвуют в реализации связи, каждый протокол имеет различные цели, выполняют резличные задачи, обладает своими преимуществами и ограничениями.

2. Протоколы работают на разных уровнях модели OSI. Функции протокола определяются уровнем, на котором он работает. Если, например, какой-то протокол работает на Физическом уровне, то это означает, что он обеспечивает прохождение пакетов через плату сетевого адаптера и их поступление в сетевой кабель.

3. Несколько протоколов могут работать совместно. Это так называемый стек, или набор, протоколов. Как сетевые функции распределены по всем уровням модели OSI, таки протоколы совместно работают на различных уровнях стека протоколов.Уровни в стеке протокола соответствуют уровням модели OSI. В совокупности протоколы дают полную характеристику функциям и возможностям стека.

Работа протоколов

Передача данных по сети, с технической точки зрения, должна быть разбита на ряд последовательных шагов, каждому из которых соответствует свои правила и процедуры, или протокол. Таким образом, сохраняется строгая очередность в выполнении определенных действий. Кроме того, эти действия (шаги) должны быть выполнены в одной и той же последовательности на каждом сетевом компьютере. На компьютере-отправителе эти действия выполняются в направлении сверху вниз, а на компьютере-получателе снизу вверх.

Компьютер-отправитель

Компьютер-отправитель в соответствии с протоколом выполняет следующие действия :

- разбивает данные на небольшие блоки, называемые пакетами, с которыми может работать протокол;
- добавлять к пакетам адресную информацию, чтобы компьютеру получатель мог определить, что эти данные предназначены именно ему;

- подготавливать данные к пеедачи через плату сетевого адаптера и далее по сетевому кабелю.

Компьютер-получатель

Компьютер-получатель в соответствии с протоколом выполняет те же действия, но только в обратном порядке:

- принимает пакеты данных из сетевого кабеля;
- через плату сетевого адаптера передает пакеты в компьютер;
- удаляет из пакета всю служебную информацию, добавленную компьютером-отправителем;
- копирует данные из пакета в буфер - для их объединения в исходный блок данных;
- передает приложению этот блок данных в том формате, который оно использует.

И компьютеру-отправителю, компьютеру-получателю необходимо выполнять каждое действие одинаковым способом, с тем чтобы пришедшие по сети данные совпадали с отправленными.

Если, например, два протокола будут по-разному разбиваться данные а пакеты и добавлять информацию (о последовательности пакетов, синхронизации или проверки ошибок), тогда компьютер, использующий один из эих протоколов, не сможет успешно связаться с компьютером, на котором работает другой протокол.

Маршрутизируемые и немаршрутизируемые протоколы

До середины 80-х годов большинство локальных сетей были изолированными. Они обслуживали один отдел или одну компанию и редко объединялись в крупные системы. Однако, когда локальные сети достигли высокого уровня развития и объем передаваемой ими

коммерческой информации возрос, ЛВС стали компонентами больших сетей.

Данные, передаваемые из одной локальной сети в другую по одному из возможных маршрутов, называется маршрутизируемыми. Протоколы, которые поддерживают передачу данных между сетями по нескольким маршрутам, называются маршрутизируемыми (routable) протоколами. Так как маршрутизируемые протоколы могут использоваться для объединения нескольких локальных сетей в глобальную сеть, их роль постоянно возраста.

Протоколы в многоуровневой архитектуре

Несколько протоколов, которые работают в сети одновременно, обеспечивают следующие операции с данными:

- подготовку;
- передачу;
- прием;
- последующие действия.

Работа различных протоколов должна быть скоординирована так, чтобы исключить конфликты и незаконченные операции. Этого можно достичь с помощью разбиения на уровни.

Стеки протоколов

Стек протоколов (protocol stack) - это комбинация протоколов. Каждый уровень определяет различные протоколы для управления функциями связи или ёе подсистемами. Каждому уровню присущ свой набор правил. Так же как и уровни в модели OSI, нижние уровни стека описывают правила взаимодействия оборудования, изготовленного разными производителями. А верхние уровни описывают правила для проведения сеансов связи и интерпретации приложений. Чем выше

уровень, тем сложнее становиться решаемые им задачи и связанные с этими задачами протоколы.

Привязка

Процесс, который называется привязка, позволяет с достаточной гибкостью настраивать сеть, то есть сочетать протоколы и платы сетевых даптеров, как того требует ситуация. Например, два стека протоколов, PX/SPX и TCP/IP, могут быть привязаны к одной плате сетевого адаптера. Если на компьютере более одной платы сетевого адаптера, то стек ротоколов может быть привязан как к одной, так и к нескольким платам етевого адаптера.

Порядок привязки определяет очередность, с которой операционная система выполняет протоколы. Если с одной платы сетевого адаптера связано несколько протоколов, то порядок привязки определяет очередность, с которой будут использоваться протоколы при попытках установить соединение. Обычно привязку выполняют при установки операционной системы или протокола. Например, если TCP/IP - 1-й протокол в списке привязки, то именно он будет использоваться при попытки установить связь. Если попытка неудачна, компьютер попытается установить соединение, использую следующий по порядку протокол в списке привязки.

Привязка (binding) не ограничивается установкой соответствия стека протоколов плате сетевого адаптера. Стек протоколов должен быть привязан (или ассоциирован) к компонентам, уровня которых и выше, и ниже его уровня. Так, TCP/IP наверху может быть привязан к Сеансовому уровню NetBIOS, а внизу - к драйверу платы сетевого адаптера. Драйвер, в свою очередь, привязан к плате сетевого адаптера.

Стандартные стеки.

В компьютерной промышленности в качестве стандартных моделей протоколов разработано несколько стеков. Вот наиболее важные из них:

- набор протоколов ISO/OSI;
- IBM System Network Architecture (SNA);
- Digital DECnet;
- Novell NetWare;
- Apple AppleTalk;
- набор протоколов Интернета, TCP/IP.

Протоколы этих стеков выполняют работы, специфичную для своего уровня. Однако коммуникационные задачи, которые возложены на сеть, приводят к разделению протокола на три типа:

- прикладной;
- транспортный;
- сетевой.

Прикладные протоколы

Прикладные протоколы работают на верхнем уровне модели OSI. Они обеспечивают взаимодействие приложений и обмена данными между ними. К наиболее популярным прикладным протоколам относятся:

APPC (Advanced Program-to-Program Communication) одноранговый SNA-протокол фирмы IBM, используемый в основном на AS/400;

FTAM (File Transfer Access and Management) - протокол OSI доступа к файлам;

X.400 - протокол CCITT для международного обмена электронной почты;

X.500 - протокол CCITT служб файлов и каталогов на нескольких системах;

SMTP (Simple Mail Transfer Protocol) - протокол Интернета для обмена электронной почтой;

FTP (File Transfer Protocol) - протокол Интернета для передачи файлов;

SNMP (Simple Network Management Protocol) - протокол Интернета для мониторинга сети и сетевых компонентов;

Telnet - протокол Интернета для регистрации на удаленных хостах и обработки данных на них;

Microsoft SMBs (Server Message Blocks, блоки сообщения сервера) и клиентские оболочки или редиректоры;

NCP (Novell NetWare Core Protocol) и клиентские оболочки или редиректоры фирмы Novell;

Apple Talk и Apple Share - набор сетевых протоколов фирмы Apple;

AFP (Apple Talk Filling Protocol) - протокол удаленного доступа к файлам фирмы Apple;

DAP (Data Access Protocol) - протокол доступа к файлам сетей DECnet.

Транспортные протоколы

Транспортные протоколы поддерживают сеансы связи между компьютерами и гарантируют надежный обмен данных между ними. К популярным транспортным протоколам относятся:

TCP (Transmission Control Protocol) - TCP/IP-протокол для гарантированной доставки данных, разбитых на последовательность фрагментов;

SPX - часть набора протоколов IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange) для данных, разбитых на последовательность фрагментов, фирмы Novell;

NWLink - реализация протокола IPX/SPX от фирмы Microsoft;

NetBEUI [NetBIOS (Network Basic Input/Output System) Extended User Interfase - расширенный интерфейс пользователя] – устанавливает сеансы связи между компьютерами (NetBIOS) и предоставляет верхним уровням транспортные услуги (NetBEUI);

ATP (Apple Talk Transacition Protocol), NBP (Name Binding Protocol) протоколы сеансов связи и транспортировки данных фирмы Apple.

Сетевые протоколы

Сетевые протоколы обеспечивают услуги связи. Эти протоколы управляют несколькими типами данных : адресацией, маршрутизацией, проверкой ошибок и запросами на повторную передача. Сетевые протоколы, кроме того, определяют правила для осуществления связи в конкретных сетевых средах, например Ethernet или Token Ring. К наиболее популярным сетевым протоколам относятся :

- IP (Internet Protocol) - TCP/IP-протокол для передачи пакетов;
- IPX (Internetwork Packet Exchenge)- протокол фирмы NetWare для передачи и маршрутизации пакетов;

* NWlink - реализация протокола IPX/SPX фирмой Microsoft;
* NetBEUI - транспортный протокол, обеспечивающий услуги транспортировки данных для сеансов и приложений NetBIOS;
* DDP (Datagram Delivery Protocol) - AppleTalk - протокол транспортировки данных.

Стандартные протоколы

Модель OSI помогает определить, какие протоколы нужно использовать на каждом уровне. Продукты от разных производителей, которые соответствуют этой модели, могут вполне корректно взаимодействовать друг с другом.

ISO, IEEE, ANSI (American National Standarns Institute), CCITT(Comite Consultatif Internationale de Telegraphie et Telephonie), сейчас

называемый INU (International Telecommunication Union), и другие организации по стандартизации разработали протоколы, соответствующие некоторым уровням модели OSI.

IEEE-протоколы Физического уровня:

802.3 (Ethernet).

Это сеть "логическая шина", скорость передачи данных - 10 Мбит/с. Данные передаются по кабелю каждому компьютеру, но принимают их только те, кому они адресованы. Протокол CSMA/CD регулирует трафик сети, разрешая передачу только тогда, когда кабель не занят и другой компьютер не передает информацию.

802.4 (передача маркера).

Это сеть типологии "шина", использующая схему передачи маркера. Каждый компьютер принимает данные, но реагируют на них только те, кому они адресованы. Маркер, передаваемый от компьютера к компьютеру, определяет тот компьютер, которому разрешена передача.

802.5 (Token Ring).

Это сеть "логическое кольцо", скорость передачи данных - 4 или 16 Мбит/с. Хотя эта сеть и называется кольцом, выглядит она как звезда, поскольку все сетевые компьютеры подключены к концентратору (MAU). Впрочем, кольцо реализуется внутри концентратора. Маркер, передаваемый по кольцу, определяет тот компьютер, которому разрешена передача.

IEEE - протокола Канального уровня поддерживают связь на подуровне Управления доступом к среде. Драйвер управления доступом к среде - это драйвер устройства, расположенный на подуровне Управления доступом к среде. Этот драйвер называют также драйвером платы сетевого адаптера. Он предоставляет низко уровневый доступ к сетевым адаптерам, обеспечивая поддержку передачи и некоторые основные функции по управлению адаптером.

Протокол управления доступом к среде определяет, какой именно компьютер может использовать сетевой кабель, если несколько компьютеров одновременно пытаются получить к нему доступ. CSMA/CD, протокол 802.3, разрешает компьютеру начинать передачу лишь тогда, когда на данный момент нет других передающих компьютеров. Если два компьютера начинают передачу одновременно, происходит своего рода столкновение - коллизия (collision). Протокол обнаруживает коллизию и запрещает передачу до тех пор, пока кабель не освободится. Затем, через случайный интервал времени, каждый компьютер вновь пытается начать передачу.

Распространенные протоколы

Среди множества протоколов наиболее популярны следующие:

- TCP/IP;
- NetBEUI;
- X.25;
- Xerox Network System (XNS);
- IPX/SPX и NWLink;
- APPC;
- Apple Talk;
- набор протоколов OSI;
- DECnet.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) - промышленный стандартный набор протоколов, который обеспечивает связь в гетерогенной (неоднородной) среде, т.е. обеспечивает совместимость между компьютерами разных типов. Совместимость - одно из основных преимуществ TCP/IP, поэтому большинство ЛВС поддерживает его. Кроме того, TCP/IP предоставляет доступ к ресурсам

Интернета, а также маршрутизируемый протокол для сетей масштаба предприятия. Поскольку TCP/IP поддерживает маршрутизацию, он обычно используется в качестве межсетевого протокола. Благодаря своей своей популярности TCP/IP стал стандартом де-факто для межсетвого взаимодействия.

К другим специально созданным для набора TCP/IP протоколам относятся:

SMTP (Simple Mail Transfer Protocol) - электронная почта;

FTP (File Transfer Protocol) - обмен файлами между компьютерами, поддерживающими TCP/IP;

SNMP (Simple Network Management Protocol) - управление сетью.

TCP/IP имеет два главных недостатка: размер и недостаточная скорость работы. TCP/IP - относительно большой стек протоколов, который может вызвать проблемы у MS-DOS клиентов. Однако для таких операционных систем, как Windows NT или Windows 95, размер не является проблемой, а скорость работы сравнима со скоростью работы протокола IPX.

NetBEU

NetBEUI - расширенный интерфейс NetBIOS. Первоначально NetBIOS и NetBEUI были тесно связаны и рассматривались как один протокол. Затем некоторые производители ЛВС так обособили NetBIOS, протокол Сеансового уровня, что он уже не мог использоваться наряду с другими маршрутизируемыми транспортными протоколами. NetBIOS (Network Basic Input/Output System - сетевая база системы ввода/вывода) это IBM интерфейс сеансового уровня с ЛВС, который выступает в качестве прикладного интерфейса с сетью. Этот протокол предоставляет программам средства для осуществления сеансов связи с другими сетевыми программами. Он очень популярен, так как поддерживается многими приложениями. NetBEUI - небольшой, быстрый и эффективный

протокол Транспотрного уровня, который поставляется со всеми сетевыми продуктами фирмы Microsoft - MS - NET.

К преимуществам NetBEUI относится небольшой размер стека (важно для MS-DOS компьютеров), высокая скорость передачи данных по сети и совместимость со всеми сетями Microsoft. Основной недостаток NetBEUI - он не поддерживает маршрутизацию. Это ограничение относится ко всем сетям Microsoft.

X.25

X.25- набор протоколов для сетей и коммуникацией пакетов. Его использовали службы коммуникации, которые должны были соединять удаленные терминалы с мэйнфреймами.

XNS

Xerox Network System (XNS) был разработан фирмой Xerox для двоих сетей Ethernet. Его широкое использование началось с 80-х годов, но постепенно он был вытеснен протоколом TCP/IP. XNS - большой и медленный протокол, к тому же он применяет значительное качество широковещательных сообщений, что увеличивает трафик сети.

IPX/SPX и NWLink

Internetwork Packet Exchange/Sequential Packet Exchange (IPX/SPX)-стек протоколов, используемый в сетях Novell. Как и NetBEUI, относительно небольшой и быстрый протокол. Но, в отличие от NetBEUI, он поддерживает маршрутизацию. IPX/SPX - "наследник" XNS.

NWLink - реализация IPX/SPX фирмой Microsoft. Это транспортныймаршрутизируемый протокол.

APPC

APPC (Advanced Program-to-Program Communication) – транспортный протокол фирмы IBM, часть System Network Architecture (SNA). Он позволяет приложениям, работающим на разных компьютерах, непосредственно взаимодействовать и обмениваться данными.

AppleTalk

Apple Talk - Собственный стек протоколов фирмы Apple omputer,позволяющий компьютерам Apple Macintosh совместно использовать файлы и ринтеры в сетевой среде.

Набор протоколов OSI

Набор протоколов OSI - полный стек протоколов, где каждый протокол соответствует конкретному уровню модели OSI. Набор содержит маршрутизируемые и транспортные протоколы, серии протоколов IEEE Project 802, протокол Сеансового уровня, Представительского уровня и несколько протоколов Прикладного уровня. Они обеспечивают полнофункциональность сети, включая доступ к файлам, печать и эмуляцию терминала.

DECnet

DECnet - собственный стек протоколов фирмы Digital Equipment Corporation. Этот набор аппаратных и программных продуктов реализует архитектуру Digital Network Architecture (DNA). Указанная архитектура определяет сети на базе локальных вычислительных сетей Ethernet, сетей FDDI MAN (Fiber Distributet Data Inerface Metropolitan Area Network) и глобальных вычислительных сетей, которые используют средства передачи конфиденциальных и общедоступных данных. DECnet может использовать как протоколы TCP/IP и OSI, так и свои собственные. Данный протокол принадлежит к числу маршрутизируемых.

Несколько раз DECnet обновляется; каждое обновление называется фазой. Текущая версия DECnet Phase V. Используются как собственные протоколы DEC, так и достаточно полная реализация набора протоколов OSI.

Установка и удаление протокола

Установка и удаление протокола выполняется аналогично установке и удалению драйвера. Основные (для конкретной операционной системы) протоколы автоматической подключаются при первоначальной установке

самой системы. Например, в Windows NT Server 3.51 протоколом по умолчанию является TCP/IP.

Чтобы установить протокол, например NWLink, после инсталляции операционной системы, надо воспользоваться специальной утилитой. Так, в Windows NT Server эта утилита через последовательность диалоговых окон позволяет:

- установить новый протокол;
- изменить порядок установленных протоколов в списке привязки;
- удалить протокол.

Резюме

Протоколы в сетевой среде определяют правила и процедуры передачи данных. Передача данных по сети состоит из ряда шагов, Которые должны выполнятся в неизменном порядке. Компьютер отправитель и компьютер-получатель используют протоколы для следующих процедур:

- разбиение данных на пакеты;
- добавление к пакету адресной информации;
- подготовки пакетов к передаче;
- приема пакетов, передаваемых по кабелю;
- копирование данных из пакета для сборки исходных блоков данных;
- передачи этих восстановленных блоков в компьютер.

Чтобы обеспечить в сети связь, одновременно работают множество протоколов. Эти протоколы находятся в стеке на разных уровнях. Существует несколько стеков, которые используются в качестве стандартных протоколов. Наиболее известный среди них построены в соответствии с уровнями модели OSI.

Протоколы устанавливаются и удаляются аналогично тому, как устанавливаются и удаляются драйверы. Чаще всего они устанавливаются автоматически при инсталляции операционной системы. Однако иногда надо установить новый протокол, изменить порядок следования протоколов в списке привязки или удалить протокол. Для этого обычно используется специальная утилита.

Контрольные вопросы.

1. Протоколы в сетевой среде?
2. Понятие протокол?
3. Назначение протоколов?
4. Источники протоколов?
5. Взаимодействие протоколов в сетях?
6. Включение и отключение поддержки протоколов?
7. Что такое стеки протоколов?
8. На каком уровне работает прикладные протоколы?
9. Транспортные протоколы?
10. Стандартные протоколы?

Ключевые слова.

Протокол;

буфер;

прикладной уровень;

стек;

привязка;

транспортный уровень;

сетевой уровень;

Лекция N10

Передача данных по кабелю

План:

Назначение методов доступа.

Управление трафиком.

Основные методы доступа.

Множественый доступ с контролем несущей и обнаружением коллизий.

Состязательный метод.

Некоторые соображения.

Множественный доступ с контролем несущей и предотвращенимем коллизий.

Доступ с передачей маркера.

Доступ по приоритету запроса.

Состязание приоритетов запроса.

Некоторые соображения.

Резюме.

Лттература:

Назначение методов доступа

.

Метод доступа - набор правил, которыео, как компьютер должен отправлять и принимать данные по сетевому кабелю.

Управление трафиком

В сети несколько компьютеров должны иметь совместный доступ к кабелю. Однако, если два компьютера попытаются одновременно передавать данные, их пакеты "столкнутся" друг с другом и будут испорчены. Это так называемая коллизия.

Чтобы передать данные по сети от одного пользователя к другому или получить их с сервера, должно быть несколько способов:

- поместить данные в кабель без "столкновения" с уже передаваемыми по нему данными;

- принять данные с достаточной степенью уверенности в том, что при передаче они не были повреждены в результате коллизии.

Все сетевые компьютеры должны использовать один и тот же метод доступа, иначе произойдет сбой сети. Отдельные компьютеры, чьи методы будут доминировать, не дадут остальным осуществить передачу.

Методы доступа служат для предотвращения одновременного доступа к кабелю нескольких компьютеров, упорядочивая передачу и прием данных по сети и гарантируя, что в каждый момент времени только один компьютер может работать на передачу.

Основные методы доступа

Существует три способа предотвратить одновременную попытку ис пользовать кабель. Другими словами, три основных метода доступа к нему.

- Множественный доступ с контролем несущей:
  с обнаружением коллизий;
  с предотвращением коллизий;
- Доступ с передачей маркера.
  Только компьютер, получивший маркер, может передавать данные.
- Доступ по приоритету запроса.

Множественный доступ с контролем несущей и обнаружение коллизий

При множественном доступе с контролем несущей и обнаружением кол лизий (сокращенно CSMA/CD) все компьютеры в сети - и клиенты, и серверы - "прослушивают" кабель, стремясь обнаружить передаваемые данные (т.е. трафик).

1. Компьютер "понимает", что кабель свободен (т.е. трафик отсутс твует).

2. Компьютер может начать передачу данных.

3. Пока кабель не освободится (в течение передачи данных), ни один из сетевых компьютеров не может вести передачу.

Вы, вероятно, помните: если два (или более) компьютеров попытаются вести передачу данных одновременно, это приведет к коллизии. Тогда эти компьютеры приостанавливают передачу на случайный интервал времени, а затем вновь стараются "наладить" связь.

Вдумайтесь в название этого доступа (хотя оно и немного длинновато). Компьютеры как бы " прослушивают" кабель, отсюда - контроль несущей. Чаще всего сразу несколько компьютеров в сети "хотят" передать данные, отсюда-множественный доступ. Передавая данные, компьютеры "прослушивают" кабель,чтобы, обнаружив коллизии, некоторое время пе реждать, а затем возобновить передачу, отсюда-обнаружение коллизий.

В то же время способность обнаружить коллизии-причина, которая ограничивает область действия самого CSMA/CD. Из-за ослабления сигнала при расстояниях свыше 2500 м (1.5 мили) механизм обнаружения коллизий не эффективен. Если расстояние до передающего компьютера превышает это ограничение, некоторые компьютеры могут не "услышать" его и начнут передачу данных, что приведет к коллизии и разрушению пакета данных.

Состязательный метод

CSMA/CD известен как состязательный метод, поскольку сетевые компьютеры "состязаются" (конкурируют) между собой за право передавать данные. Он кажется достаточно громоздким, но современные реализации CSMA/CD настолько быстры, что пользователи даже не задумываются над тем, что применяют состязательный метод доступа.

Некоторые соображения

Чем больше компьютеров в сети, тем интенсивнее сетевой трафик. При интенсивном трафике число коллизий возрастает, а это приводит к замедлению сети (уменьшению ее пропускной способности). Поэтому в не которых ситуациях метод CSMA/CD может оказаться недостаточно быстрым.

После каждой коллизии обоим компьютерам приходится возобновлять передачу. Если сеть очень загружена, повторные попытки могут опять привести к коллизиям, но уже с другими компьютерами. Теперь уже четыре компьютера (два - от первой неудачной попытки и два - от второй неудачной попытки первых) будут возобновлять передачу. Результат может оказаться тем же, что и в предыдущем случае, только пострадавших компьютеров станет еще больше. Такое лавинообразное нарастание повторных передач может парализовать работу всей сети.

Вероятность возникновения подобной ситуации зависит от числа пользователей, пытающихся получить доступ к сети, и приложений, с ко торыми они работают. База данных, например, сеть используют интенсивнее, чем тестовые процессоры.

Сеть с методом доступа CSMA/CD, обслуживающая многих ользовате лей, которые работают с несколькими системами управления базами данных (критическое число пользователей зависит от аппаратных

компьютеров, кабельной системы и сетевого программного обеспечения), может практически "зависнуть" из-за чрезмерного сетевого трафика.

Множественный доступ с контролем несущей и предотвращением коллизий

Множественный доступ с контролем несущей и предотвращением коллизий (сокращенно CSMA/CA) не так популярен, как CSMA/CD или передача маркера. используя CSMA/CA, каждый компьютер перед передачей данных в сеть сигнализирует о своем намерении, поэтому остальные компьютеры "узнают" о готовящейся передаче и могут избежать коллизии.

Однако широковещательное оповещение увеличивает общий трафик сети и уменьшает ее пропускную способность. Отсюда - CSMA/CA работает ме леннее, чем CSMA/CD.

Доступ с передачей маркера

Суть доступа с передачей маркера заключается в следующем: пакет особого типа, маркер (token), циркулирует по кольцу от компьютера к компьютеру. Чтобы послать данные в сеть, любой из компьютеров сначала должен дождаться прихода свободного маркера и захватить его.

Когда какой либо компьютер "наполнит" маркер своей информацией и пошлет его по сетевому кабелю, другие компьютеры уже не могут передавать данные. Так как в каждый момент времени только один компьютер будет использовать маркер, то в сети не возникнет ни состязание, ни коллизий, ни временных пауз.

Доступ по приоритету запроса

Доступ по приоритету запроса - относительно новый метод доступа, разработанный для стандарта сети Ethernet со скоростью передачи данных 100 Мбит/с - 100 VG-AnyLAN. Он стандартизован IEEE в категории 802.12.

Этот метод доступа основан на том, что все сети 100 VG-AnyLAN строятся только из компьютеров и оконечных узлов. Компьютеры управляют доступом к кабелю, последовательно опрашивая все узлы в сети и выявляя запросы на передачу. Компьютер, должен знать все адреса, связи и узлы и проверять их работоспособность. Оконечным узлом, в соответствии с определением 100 VG-AnyLAN, может быть компьютер, мост, маршрутизатор или коммутатор.

Состязание приоритетов запроса

Как и при CSMA/CD, при доступе по приоритету запроса два компь ютера могут бороться за право передать данные. Однако только последний метод реализует схему, по которой определенные типы данных - есливозникло состязание, - имеют соответствующий приоритет. Получив одновременно два запроса, концентратор в начале отдает предпочтение запросу с более высоким приоритетом. Если запросы имеют одинаковый приоритет, они будут обслужены в произвольном порядке.

В сетях с использованием доступа по приоритету запроса каждый компьютер может одновременно передавать или принимать данные, пос кольку для этих сетей разработана специальная схема кабеля. В них применяется восьмипроводной кабель, по каждой паре проводов сигналы передаются с частотой 25 МГц.

Некоторые соображения

В сетях, где реализован доступ по приоритету запроса, связь уста навливается между компьютером-отправителем, компьютером и компьюте ром-получателем. Такой вариант более эффективен, чем CSMA/CD, где пе редача осуществляется для всей сети. В среде с доступом по приоритету запроса каждый концентратор "знает" только те оконечные узлы и репитеры, которые непосредственно подключены к нему, тогда как в среде с CSMA/CD каждый концентратор "знает" адреса всех узлов в сети.

К преимуществам метода доступа по приоритету запроса (в сравнении с CSMA/CD) относятся:

* Использование четырех пар проводов.

Четыре пары проводов позволяют компьютеру одновременно передавать и принимать данные.

* Передача через компьютер.

Передача не вещается на все компьютеры в сети. Компьютеры, централизованно управляемые концентратором, не соревнуются за права доступа к кабелю.

Резюме

Чтобы избежать коллизий и разрушений пакетов данных, необходимо управлять трафиком в сети. Метод доступа - набор правил, которые оп ределяют, как компьютер должен отправлять и принимать данные по сетевому кабелю. Эти правила помогают предотвратить одновременный доступ к кабелю нескольких компьютеров. Существует три основных подхода:

* "прослушивание" кабеля и обнаружение коллизий;
* доступ с передачей маркера;
* доступ по приоритету запроса.

Используя CSMA/CD, компьютеры "прослушивают" кабель и - при от сутствии несущей - передают данные. Обнаружение коллизий - состяза тельный метод доступа (компьютеры соревнуются за право передавать

данные). Если сетевой трафик достаточно интенсивен, CSMA/CD работает медленно. При предотвращении коллизий (CSMA/CA) каждый компьютер пе ред началом передачи сигнализирует о своем намерении. Этот метод мед леннее, чем обнаружение коллизий. В сетях с передачей маркера компьютер захватывает проходящий маркер, присоединяет к нему данные и отправляет дальше. Одномоментно только один компьютер может использовать маркер, поэтому коллизий нет. При доступе по приоритету запроса связь осуществляется только между компьютером-отправителем, концентратором и компьютером-получателем. Передачей данных централизованно управляет концентратор, причем на все остальные компьютеры в сети он не вещает.

Контрольные вопросы.

1. Роль методов достпа в передпче по сетевому кабелю?
2. Основные методы доступа.?
3. Что такое состязательный метод?
4. Опищите метод доступа с передачей маркера.
5. Состязание приоритетов запроса?
6. Необходима ли поддержка маршрутизации в сети?
7. Все ли компьютеры используют один и тот же метод доступа?

Ключевые слова

Маркер;

Запрос;

Трафик;

Коллизий;

Кабель;

Сервер;

Концетратор.

Лекция №11

Ethernet,

План:

Обзор.

Происхождение.

Основные характеристики.

Формат кадра.

Стандарты IEEE на 10 Мбит/с.

10BaseT.

10Base2.

10Base5.

10BaseFL.

Стандартные IEEE на 100 Мбит/с.

Спецификации.

Топология.

Сегментация.

Етевые операционные системы и Ethernet.

Литература:

Обзор

Сетевая архитектура (network architecture) - это комбинация стандартов, топологий и протоколов, необходимых для создания работоспособной сети. Данное занятие, представляющеесетевую архитектуру Ethernet, является первым в серии занятий, посвященных сетевым архитектурам.

Происхождение

В конце 60-х годов Гавайский университет разработал глобальную вычеслительную сеть (ГВС) под названием ALOHA. Как Вы помните из ма териала предыдущих занятий, ГВС охватывает большие пространства, чем ЛВС. Университет, располагая обширной территорией,

решил объединить в сеть все имеющиеся в его распоряжении компьютеры. Одним из ключевых аспектов созданной сети явилось использование метода доступа CSMA/CD.

Эта сеть и послужила основой для современных сетей Ethernet. В 1972 году Роберт Меткалф и Дэвид Боггс (Исследовательский центр Пало Альто фирмы Xerox) разработали кабельную систему передачи сигналов, а в 1975 году - первый продукт Ethernet. Первоначальная версия Ethernet представляла собой систему со скоростью передачи 2.94 Мбит/с и объединяла более 100 компьютеров с помощью кабеля длиной в 1 км.

Сеть Ethernet фирмы Xerox имела такой успех, что компания Xerox, Intel Corporation и Digital Equipment разработали стандарт для Ethernet со скоростью передачи 10 Мбит/с. Сегодня ее рассматривают как спецификацию, описывающую метод кабельного соединения и совместного использования компьютеров и информационных систем.

Спецификация Ethernet выполняет те же функции, что Физический и Канальный уровени модели OSI. Эта разработка лежит в основе специфи кации IEEE 802.3.

Основные характеристики

Ethernet - самая популярная в настоящее время сетевая архитектура. Она использует узкополосную передачу со скоростью 10 Мбит/с, топологию "шина", а для регулирования трафика в основном сегменте кабеля - CSMA/CD.

Среда (кабель) Ethernet является пассивной, т.е. получает питание от омпьютера. Следовательно, она прекратит работу из-за физического повреждения или неправильного подключения терминатора.

Сеть Ethernet имеет следующие характеристики:

- традиционная топология - линейная шина;
- другие топологии - звезда-шина;
- тип передачи - узкополосная;
- метод доступа - CSMA/CD;

- спецификации - IEEE 802.3;
- скорость передачи данных - 10 и 100 Мбит/с;
- кабельная система - толстый и тонкий коаксиальный, UTP.

Формат кадра

Ethernet разбивает данные на пакеты (кадры), Формат который отли чается от формата пакетов, используемого в других сетях. Кадры предс тавляют собой блоки информации, передаваемые как единое целое. Кадр Ethernet может иметь длину от 64 до 1518 байтов, но сама структура кадра Ethernet использует, по крайней мере, 18 байтов, поэтому размер блока данных в Ethernet - от 46 до 1500 байтов. Каждый кадр содержит управляющую информацию и имеет общую с другими кадрами организацию.

Стандарты IEEE на 10 Мбит/с

Здесь будут рассмотрены четыре топологии Ethernet со скоростью передачи 10 Мбит/с:

- 10BaseT;
- 10Base2;
- 10Base5;
- 10BaseFL.

10BaseT

В 1990 году IEEE опубликовал спецификацию 802.3 для построения сети Ethernet на основе витой пары. 10BaseT (10 - скорость передачи 10 Мбит/с, Base - узкополосная, T - витая пара) - сеть Ethernet, которая для соединения компьютеров обычно использует неэкранированную витую пару (UTP). Тем не менее и экранированная витая пара (STP) также может применять в топологии 10BaseT без изменения каких-либо ее параметров.

Большинство сетей этого типа строятся в виде звезды, но по системе передачи сигналов представляют собой шину, как и другие конфигурации Ethernet. Обычно концентратор сети 10BaseT выступает

как многопортовый (multiport) репитер и часто располагается в распределительной стойке здания. Каждый компьютер подключается к другому концу кабеля, соединенного с концентратором, и использует две пары проводов: одну - для приема, другую -для передачи.

Максимальная длина сегмента 10BaseT - 100 м (328 футов). Мини мальная длина кабеля - 2.5 м (около 8 футов). ЛВС 10BaseT может обс луживать до 1024 компьютеров.

При скорости передачи выше 10 Мбит/с коммутационные панели перед использованием необходимо тестировать. Новейшие концентраторы обеспе чивают соединение как для толстого, так и для тонкого коаксиального кабеля Ethernet. При такой реализации сети, присоединив мини-трансивер 10BaseT к порту AUI платы сетевого адаптера, несложно перейти от толстого Ethernet к витой паре (10BaseT).

10Base2

В соответствии со спецификацией IEEE 802.3 эта топология называ ется 10Base2 [10 - скорость передачи 10 Мбит/с, Base - узкополосная передача, 2 - передача на расстояние, примерно в два раза превышающее 100 м (фактическое расстояние 185 м)].

Сеть такого типа ориентированна на тонкий каоксиальный кабель, или тонкий Ethernet, с максимальной длиной сегмента 185м. Минимальная длина кабеля 0.5 м (20 дюймов). Кроме того, существует ограничение на максимальное количество компьютеров, которое может быть размещено на 185-метровом сегменте кабеля, - 30 штук.

Компоненты кабеля "тонкий Ethernet":

- BNC баррел-коннекторы;
- BNC Т-коннекторы;
- BNC-терминаторы.

Сети на тонком Ethernet обычно имеют топологию "шина". Стандарты IEEE для тонкого Ethernet не предусматривают использование кабеля трансивера между Т-коннектором и компьютером.

Вместо этого Т-коннектор располагают непосредственно на плате сетевого адаптера.

BNC баррел-коннектор, соединяя сегменты кабеля, позволяет увели чить его общую длину. Например, Вам нужен кабель длиной 30 м, а у Вас есть сегменты тонкого кабеля по 20 и 5 м. Соедините двумя баррел-кон некторами эти сегменты, чтобы получить кабель нужной длины. Однако использование баррел-коннекторов желательно свести к минимуму, поскольку они ухудшают качество сигнала.

Сеть на тонком Ethernet - экономичный способ реализации сетей для небольших отделений и рабочих групп. Используемый в такого типа сетях кабель:

- относительно недорогой;
- прост в установке;
- легко конфигурируется.

По спецификации IEEE 802.3, сеть на тонком Ethernet может поддер живать до 30 узлов (компьютеров и репитеров) на один кабельный сегмент.

Правило 5-4-3

Сеть на тонком Ethernet может состоять максимум из пяти сегментов кабеля, соединенных четырьмя репитерами, но только к трем сегментам при этом могут быть подключены рабочие станции. Таким образом, два сегмента остаются зарезервированными для репитеров, их называют межрепитерными связями. Такая конфигурация известна как правило 5-4-3.

10Base5

В соответствии со спецификацией IEEE эта топология называется 10Base5 [10 - скорость передачи 10 Мбит/с, Base - узкополосная передача, 5 - сегменты по 500 м (5 раз по 100 м)]. Известно и другое ее название - стандартный Ethernet.

Сети на толстом коаксиальном кабеле (толстый Ethernet) обычно ис пользуют топологию "шина". Толстый Ethernet может поддерживать до 100 узлов (рабочих станций, репитеров и т.д.) на магестральный сегмент. Магистраль, или магистральный сегмент, - главный кабель, к которому присоединяются трансиверы с подключенными к ним рабочими станциями и репитерами. сегмент толстого Ethernet может иметь длину 500 м при общей длине сети 2500 м (8200 футов).

Растояния и допуски для толстого Ethernet больше, чем для тонкого Ethernet.

Компоненты кабельной системы:

* Трансиверы.

Трансиверы, обеспечивая связь между компьютером и главным кабелем ЛВС, совмещены с "зубом вампира", соединенным с кабелем.

* Кабели трансиверов.

Кабель трансивера (ответвляющийся кабель) соединяет трансивер платой сетевого адаптера.

* DIX-коннектор, или AUI-коннектор.

Этот коннектор расположен на кабеле трансивера.

* Коннектор N-серии (в том числе баррел-коннектор) и терминаторы N-серии.

Правило 5-4-3

Сеть на толстом Ethernet может состоять максимум из пяти магист ральных сегментов, соединенных репитерами (по спецификации IEEE 802.3), но только к трем сегментам при этом могут быть подключены компьютеры. При вычислении общей длины кабеля "толстый Ethernet" длина кабеля трансивера не учитывается, т.е. в расчет принимают только длину сегмента кабеля "толстый Ethernet".

Минимальное расстояние между соседними подключениями - 2.5 м (около 8 футов). В это расстояние не входит длина кабеля трансивера.

Толстый Ethernet был разработан для построения ЛВС в рамках большого отдела или всего здания.

Комбинирование толстого и тонкого Ethernet

Обычно в крупных сетях совместно используют толстый и тонкий Ethernet. Толстый Ethernet хорошо подходит в качестве магистрали, а для ответвляющихся сегментов применяют тонкий Ethernet. Вероятно, Вы пом ните, что толстый Ethernet имеет медную жилу большего сечения и может передавать сигналы на большие расстояния, чем тонкий Ethernet. Трансивер соединяется с кабелем "толстый Ethernet", AUI-коннектор кабеля трансивера включается в репитер. Ответвляющиеся сегменты тонкого Ethernet соединяются с рапитером, а к ним уже подключаются компбютеры.

10BaseFL

10BaseFL (10 - скорость передачи 10 Мбит/с, Base - узкополосная передача, FL - оптоволоконный кабель) представляет собой сеть Ethernet, в которой компьютеры и репитеры соединены оптоволоконным кабелем.

Основная причина популярности 10BaseFL - возможность кабель между репитерами на большие расстояния (например, между зданиями). Максимальная длина сегмента 10BaseFL - 2000 м.

Стандарты IEEE на 100 Мбит/с

Новые стандарты Ethernet позволяют преодолеть скорость передачи в10 Мбит/с. Эти новые возможности разрабатываются для таких приложений, порождающих интенсивный трафик, как:

- CAD (система автоматического проектирования);
- CAM (системы автоматического производства);
- видео;
- отображение и хранение документов.

Известны два стандарта Ethernet, которые могут удовлетворить воз росшие требования:

- 100BaseVG-AnyLAN Ethernet;

- 100BaseX Ethernet (Fast Ethernet).

И Fast Ethernet, и BaseVG-AnyLAN работают примерно в пять-десять раз быстрее, чем стандартный Ethernet. Кроме того, они совместимы с существующей кабельной системой 10BaseT. Это означает, что перейти от 10BaseT к этим стандартам достаточно быстро и просто.

100VG-AnyLAN

100VG (Voice Grade) AnyLAN - новая сетевая технология, которая сочетает в себе элементы Ethernet и Token Ring. Эта технология, раз работанная фирмой Hewlett-Packard, в настоящее время совершенствуется стандартом IEEE 802.12. Спецификация 802.12 - стандарт передачи кадров Ethernet 802.3 и пакетов Token Ring 802.5.

Эта технология имеет несколько названий:

- 100VG-AnyLAN;
- 100BaseVG;
- VG;
- AnyLAN.

Спецификация

Перечислим возможности некоторых из существующих в настоящее время спецификаций 100VG-AnyLAN:

- минимальная скорость передачи данных 100 Мбит/с;

- поддержка каскадируемой топологии "звезда" на основе витой пары категории 3,4 или 5 и оптоволоконного кабеля;

- метод доступа по приоритету запроса (различаются два уровня приоритетк: низкий и высокий);

- поддержка средств фильтрации персонально адресованных кадров в концентраторе (для повышения степениконфиденциальности);

- поддержка передачи кадров Ethernet и Tocken Ring.

Топология

Сеть 100VG-AnyLAN строится по топологии "звезда", где все компь ютеры соединены с концентратором. Сеть можно расширять,

добавляя "до черние" (child) концентраторы к центральному, "родительскому" (parent), который относится к ним так же, как и к компьютерам, т.е. родительские концентраторы управляют передачей компьютеров, соединенных со своими "детьми".

Некоторые соображения

Представленная технология требует использования специольных кон центраторов и плат. Кроме того, длина кабеля 100BaseVG, по сравнению с 10BaseT и другими реализаторами Ethernet, ограничена: общая длина пары кабелей от концентратора 100BaseVG до компьютеров не мажет превышать 250 м. Чтобы преодолеть это ограничение, надо использовать специальное оборудование. Ограничения длины кабеля приведут к тому, что для 100BaseVG потребуется больше кабельных стоек, чем для 10BaseT.

100BaseX Ethernet

Это стандарт, иногда называемый Fast Ethernet, является расширением существующего стандарта Ethernet. Он строится на UTP категории 5, использует метод доступа CSMA/CD и топологию "звезда-шина" (подобно 10BaseT), где все кабели подключены к концентратору.

Спецификация среды

- 100BaseX включает три спецификации среды передачи:
- 100BaseT4 (UTP категории 3,4 или 5 с четырьмя парами роводов);
- 100BaseTX (UTP или STP категории 5 с двумя парами проводов);
- 100BaseFX (двухжильный оптоволоконный кабель).

Некоторые соображения

Ethernet может использовать несколько протоколов связи, в том числе и TCP/IP, который хорошо работает в операционной среде UNIX. Поэтому Ethernet так популярен в научных и образовательных системах.

Сегментация

Производительность Ethernet можно повысить: разделите перегружен ный сегмент на два, соединенные мостом или маршрутизатором. Трафик в каждом сегменте при этом уменьшается, так как меньшее число компьютеров в сегменте пытается осуществить передачу, и время доступа к кабелю сокращается.

Разделение сегмента - удачный ход при подсоединении к сети новых пользователей или установке новых приложений, интенсивно работающих с сетью (например, баз данных и видеоприложений).

Сетевые операционные системы и Ethernet

Ethernet работает с большинством популярных сетевых операционных систем, в их числе:

- Microsoft Windows 95;
- Microsoft Windows NT Wockstation;
- Microsoft Windows NT Server;
- Microsoft LAN Manager;
- Microsoft Windows for Workgroups;
- Novell NetWare;
- IBM LAN Server;
- AppleShare.

Контрольные вопросы.

1. Сетевая архитектура Ethernet?
2. Стандарты IEEE,определяющие сети Ethernet?
3. Компоненты аспекты реализации IEEE?
4. Что такое 10BaseT?
5. Что такое 10Base2?
6. Что такок 10Base5?
7. Что такое 10BaseFL?
8. Что такое сегментация?

Ключевые слова.

Сеть;

Топология;

Шина;

Звезда;

Сегментация;

Концентратор.

Лекция № 12

Установка сетевой операционной систем

План:

Обзор.

Координация аппаратного и программмного обеспечения.

Многозадачность.

Програмные компоненты.

Клиентское программное обеспечение.

Редиректор.

Периферийные устройства.

Серверное программное обеспечение.

Установка Windows NT Server.

Идентификация сервера.

Роль сервера.

Установка и удаление сетевы служб.

Привязка служб.

Резюме.

Литература:

Обзор

До последнего времени программное обеспечение для работы с сетью персональных компьютеров выступало в качестве дополнения к сужествующим операционным системам. Персональный компьютер, являющийся частью сети, в действительности работал под управлением и автономной, и сетевой операционных систем одновременно.

Для обслуживания всех функций обе операционные системы надо было устанавливать на один и тот же компьютер. Например, Microsoft LAN Manager иногда называли сетевой операционной системой, однако, по

сути, он только обеспечивал работу в сети таких операционных систем, как MS-DOS, UNIX или OS/2.

В современных операционных системах типа Windows NT Server, Windows NT Workststion и Windows 95 автономная и сетевая операционные системы скомбинированы в одну операционную систему, которая поддерживает функционирование как автономного компьютера, как и целой сети. Эта операционная система является основой для деятельности всего программного и аппаратного обеспечения компьютера.

Координация аппаратного и программного обеспечения

Операционная система управляет выделением аппаратных есурсов:

- памяти;
- процессорного времени;
- дискового пространства;
- переферийных устройств.

Операционная система, кроме того, координирует взаимодействие между компьютером и прикладными программами, которые на нем выполняются. Она служит так же основой, на которой строятся такие приложения, как программы обработки текстов и электронных таблиц. Фактически прикладные программы создаются для конкретной операционной системы. Однако поставщики часто указывают, что их приложения написаны так, чтобы полностью использовать дополнительные возможности Window NT Server 3.51.

Многозадачность

Поддержка сетевой операционной системы и сетевой деятельности довольно сложная задача. В связи с этим, выбирая операционную систему для сетевой среды, необходимо принимать во внимание такую ее особенность, как многозадачность (multitasking).

Многозадачная операционная система позваляет выполнять на компьютере более одной задачи одновременно. "Настоящая" многозадачная операционная система может выполнять столько задач,

сколько имеется процессоров. Когда задач больше, чем процессоров, компьютер должен так распоряжаться их временем, чтобы доступные процессоры уделяли некоторую часть времени каждой задаче, переключаясь между задачами, пока все они не будут веполнены. Компьютер под управлением такой операционной системы "выглядит" так, будто он одновременно обрабатывает несколько задач.

Существуют два основных типа многозадачности.

- Вытесняющая (preemrtive) многозадачность

При вытесняющей многозадачности операционная система может получить управление процессором без "согласования" с задачей.

- Невытесняющая (non-preemptive) [кооперативная (cooperative)] многозадачность.

При невытесняющей многозадачности управление процессором никогда не отнимается у задачи, которая сама решает, когда ей освободить процессор. Программы, написаные для операционных систем с кооперативной многозадачностью, должны переодически уступать контроль над процессором другим программам. Но любая из них до тех пор не сможет продолжить работу, пока программа с неприоритетной многозадачностью не уступит управление процессором.

Так как автономная и сетевая операционные системы постоянно заимодействуют друг с другом, система с вытесняющей многозадачностью обладает несомненными преимуществами. Например, такая система может передать управление процессором от локальной задачи к сетевой.

Программные компоненты

До недавнего времени все сетевые операционные системы представляли собой приложения, загружаемые поверх автономной операционной системы. Важнейшее различие между операционной системой Microsoft Windows NT и другими операционными системами как раз в том и состоит, что сетевые возможности встроенные в саму Windows NT.

Сетевая операционная система:

- связывает все компьютеры и переферийные устройства в сети;
- координирует функции всех компьютеров и переферийных стройств в сети;
- обеспечивает защитный доступ к данным и переферийным устройствам в сети.

Сетевое программное обеспечение состоит из двух важнейших компонентов:

- сетевого программного обеспечения, устанавливаемого на компь
- ютерах-клиентах;
- сетевого программного обеспечения, устанавливаемого на компь ютерах-серверах.

Клиентское программное обеспечение

В автономных системах, когда пользователь набирает команду запрос к компьютеру на выполнение некой задачи, этот запрос передаетсячерез локальную шину процессору компьютера. Например, если Вы хотите увидеть содержимое каталога, размещенного на одном из локальных дисков компьютера, процессор интерпретирует запрос, а затем выводит на дисплее содержимое каталога.

Однако в сетевой среде, когда пользователь делает запрос, относя щийся к ресурсам удаленного сервера, этот запрос передается из ло кальной шины компьютера в сеть, к серверу с необходимым ресурсом.

Редиректор

Передача запросов выполняется редиректором (redirector). В зави симости от сетевого программного обеспечения редиректор может назы ваться оболочкой (shell) или запросчиком (requester).Редиректор - это небольшой фрагмент кода операционной системы, который:

- перехватывае запросы в компьютере;

- определяет, должен ли запрос поступить на локальную шину компьютера или его надо переадресовать через сеть другому серверу.

В Windows NT сервер обслуживает подключения, затребованные редиректорами клиентов, и предоставляет им доступ к необходимым ресурсам. Другими словами, сервер обслуживает запросы клиентов.

Обозначение ресурсов

Редиректор должен следить за тем, чтобы обозначения устройств соответствовали определенным сетевым ресурсам.

Допустим, Вы решили реализовать свое право на доступ к совместно используемому каталогу. И здесь окажется, что Ваши возможности целиком зависят от установленной операционной системы. Например, в Windows NT наиболее простой способ подключения к сетевому диску, к которому Вам необходим доступ, - использовать File Manager. Когда Вы указываете сервер и имя совместно используемого каталога, File Manager присваивает одну из букв английского алфавита в качестве обозначения этого каталога, например G. Затем Вы можите обращаться к этому каталогу на удаленном компьютере как к диску G, и редиректор определит его местонахождение.

Периферийные устройства

Редиректоры могут посылать запросы как к компьютерам, так и к периферийным устройствам. Используя редиректор для LPT1 или COM1, можно ссылаться на сетевые, а не на локальные принтеры. Редиректор будет перехватывать любые задания на печать, направляемые в LPT1, и передавать их из локальной машины на указанный сетевой принтер.

Благодаря редиректору пользователь теперь не должен заботиться о реальном местонахождении данных и периферийных устройств или о сложностях подключения.

Серверное программное обеспечение

Серверное программное обеспечение дает возможность всем сетевым компьютерам совместно использовать данные сервера и его периферийные устройства, включая принтеры,плоттеры и диски.

Обычно все компьютеры Windows NT содержат програмное обеспечение и клиента, и сервера. Даже если рабочие станции под управлением Windows NT выступают в роли клиентов, они имеют встроенное программное обеспечение для выполнение функций как клиентов, так и серверов. Запрос содержимого каталога на удаленном жестком диске.

Управление совместно используеиыми ресурсами

Большинство сетевых операционных систем не только предоставляет возможность доступа к совместно используемым ресурсам, но и определяет порядок их совместного использования. Под порядком совместного использования ресурсов имеют в виду:

- предоставление различным пользователям разного уровня оступа к ресурсам;
- координацию доступа к ресурсам,- чтобы исключить ситуацию, когда два компьютера пытаются одновременно получить доступ к ресурсам.

Например, администратор должен ознакомить всех пользователей сети с содержимым конкретного документа (файла)- он дает этот документ (файл) обшедоступным, однако управляет доступом к нему таким оброзом, чтобы:

- некоторые пользователи имели возможность только читать документ;
- другие пользователи имели возможность и читать документ, и вно
- сить в него изменения.

Управление правами доступа

Сетевые операционные системы предоставляют сетевым администраторам и другую возможность: определять, кто может работать ресурсами сети. Сетевой администратор, используя сетевую операционную систему, способен:

- добавить в список пользователей сети и новых пользователей;
- предоставить превелегии отдельным пользователям сети или снять эти превелегии;
- удалить определенных пользователей из списка пользователей, под держиваемого сетевой операционной системой.

Управление сетью

Современые сетевые операционные системы содержат инструмен тальные средства администрирования(administrative tools), которые помогают администраторам проанализировать состояние сети.

Если в сети назревают проблемы, инструментальные средства администрирования могут распознать их признаки и предоставить информацию в виде графиков или в других формах. В ответ администратор сети предпримит конкретирующие действия еще до того, как неполадки нарушат ее функционирование.

Установка Windows NT Server

Программа установки - это приложение, которое выполняет всю работу по установке сетевой операционной системы в различных условиях. Эти условия определяются:

- средой, в каторой производится установка;
- размером сети;
- типом задач, который сервер будет выполнять в сети;
- типом файлов системы, которую будет использовать сервер;

- идентификация сервера;
- операционными системами, установленные на сервере;
- распределением дискового пространства сервера.

Идентификация сервера

Обычно программа установки запрашивает следующие данные об идентификации сервера и сети:

- имя, которое Вы дали своему сегменту сети (например, имя домена или рабочей группы);
- имя Вашего сервера.

Эта информация помогает сетевой операционной системе идентифицировать конкретный сервер и его сетевое окружение, а также отличать их от других компьютеров и сегментов сети. Это важное условие для передачи и приема данных через сеть.

Роль сервера

В процессе установки Вам будет задан вопрос о рали, которую дол жен выполнять устанавливаемый сервер в Ващей сетевой среде.

Например, под оправлением Microsoft NT Server сеть разделяется на облости, называемые доменами. Домен- это логическое обьединение компьютеров,которое значительно упрощает администрирование. Некоторые серверы в доменах следят за всеми пользователями, отвечают за политику безопасности и хранение важной информации о самом домене. Иначе говоря, первый сервер, устанавливаемый в домене,должен выступать главным контролером домена (Primary Domain Controller, PDC). PDC нетолько содержит копию важнейшей информации о домене и проверяет права пользоваталей, но может также выступать как сервер файлов, печати и приложений. Каждый домен обязательно включает один (и только один!) PDC.

Некоторые серверы Windows NT, установленные после PDC, могут быть установлены как резервные контроллеры доменов (Baskup Domain Controller, BDC). BDC - это компьютер, который хранит резервные копии

политики безопасности домена и базу данных домена, а так же проводит аутентификацию входов в сеть. Наличие в доне BDC строго не обязательно, однако рекомендуется иметь как минимум обин BDC. Кроме того, BDC может функционировать как сервер файлов, печати и приложений.

Другие серверы устанавливают как "простые серверы". Их называют просто серверами, они могут выполнять роль серверов файлов, печати и приложений.

Устанавливая серсвр, вы должны указать: является ли он главным сервером, резервным контроллером или просто сервером файлов, печати и приложений.

Разбиение на разделы

Чтобы установить сетевую операционную систему, необходимо указать как будут использоватьсяпространство жестких дисков сервера.

Жеский диск можно разбить на области, называемые разделами (partition). Отдельные разделы Вы можите зарезервировать для некоторых целей.

Во время установки сетевой операционной системы не забудьте создать для нее раздел или указать тот раздел среди существующих, на ко торых она будет установлена.

Конфигурирование платы сетевого адаптера

Во время установки Windows NT Server вам будет предложено выбрать или сконфигурировать плату сетевого адаптера установленно в вашем компьютере. Кроме того, вы должны выбрать протоколы из следующего списка протоколов: TCP/IP, NetBEUI, IPX/SPX.

Установка протокола TCP/IP

Протокол Microsoft TCP/IP в Windows NT служит для поддержки сетей масштаба предприятия. TCP/IP - это:

- стандартный, маршрутизируемый протокол сетей масштаба предприятия для Windows NT;

- архитектура, облегчающая обмен данными в гетерогенных средах;

- доступ во всемирную сеть Интернет и к ее ресурсам.

Установка TCP/IP достаточно проста и понятна. В Control Panel дважды щелкните значок Network, выберите Add Software, а затем - TCP/IP and related components.

Параметры установки

Для установки Microsoft TCP/IP неоходимы следующие три параметра конфигурации: IP-адрес, маска подсети и шлюз по умолчанию.

IP-адрес

IP-адрес - это логический 32-битный адрес, используемый для иден тификации TCP/IP-хоста. Каждый IP-адрес состоит из двух частей: иден тификатора (ID) сети и ID-хоста. ID сети идентифицирует все хост-уст ройства, которые находятся в одной физической сети. ID-хоста иденти фицирует конкретный хост в сети. Каждый компьютер, на котором уста новлен протокол TCP/IP, должен иметь уникальный IP-адрес. Вот пример корректного IP-адреса: 131.107.2.200.

Маски подсети

Маска подсети (subnet mask) используется для выделения части IP-адреса так, чтобы TCP/IP мог отличать ID сети от ID хоста. TCP/IP-хосты могут связываться, используя маску подсети для того, чтобы определить, где находится хост назначения: в лакальной или уда ленной сети. Вот пример корректной маски подсети: 255.255.255.0.

Шлюз по умолчанию

Чтобы обмениваться данными с хостом в другой сети, конфигурация IP-хоста должен быть указан маршрут в сеть назначения. Если не обнаружен предопределенный маршрут, хост использует шлюз для передачи данных хосту назначения. Шлюз по умолчанию используется для пересылки IP-пакетов, которые должны быть переданы в

удаленные сети. Если шлюз по умолчению не указан, возможности связи ограничены локальной сетью.

Конфигурирование TCP/IP вручную

При конфигурирование TCP/IP вручную нужно указать IP-адрес, маску подсети и шлюз по умолчанию. Введите эти параметры для каждой платы сетевого адаптера компьютера который использует TCP/IP.

Автоматическое конфигурирование TCP/IP

Microsoft Windows NT Server поддерживает так называемый динамический протокол конфигурирования хоста (Dynamic Host Configyration Protocol, DHCP). Когда сеть содержит сервер DHCP, клиенты, поддерживающие DHCP (включая Windows NT Workstation и Windows NT Server), могут запрашивать от него данные о конфигурации TCP/IP. Обычно это значительно упрощает настройку параметров TCP/IP на компьютерах-клиентах.

Если вам доступен сервер DHCP, то TCP/IP может быть сконфигурирован автоматически - во время установки TCP/IP активизируйте флажок Enable Automatic DHCP Configuration. Если флажок Enable Automatic DHCP Configuration отмечен клиент DHCP обращается к DHCP-серверу за информацией о параметрах настройки. Автоматическое конфигурирование с использованием DHCP может быть выполнено позднее с помощью значка Network в Control Panel.

Активизироканный флажок Enable Automatic DHCP Configuration избавляет клиента DHCP от какой бы то ни было дополнительной настройки TCP/IP.

Системные требования к серверу

Для нормальной работы с сетевой операционной системой очень важно представлять, какими ресурсами должен обладать сервер. В число системных требований к нему входят такие параметры:

- доступное дисковое пространство;
- тип процессора;

* объем оперативной памяти.

Сетевые службы

Сетевые службы - это приложения сетевой операционной системы, "выдающие жизнь" в сеть. В среде Microsoft Windows NT Server они наз-ся службами.

Программа установки сетевой операционной системы, гарантирует что по умолчаниюбудет установлен минимально необходимый набор сетевых служб (service). Однако в процессе эксплуатации сети иногда возникает потребность установить такие такие службы и функции, которые изначально не были обязательны для сети.

Установка и удаление сетевых служб

Установка и удаление сетевых служб напоминает установку и удаление драйверов. Большенство сетевых операционных систем для этого применяет специальные утилиты с графическим интерфейсом пользователя.

Привязка служб

Связи - это последовательность соединения сетевых компонентов, начиная сетевыми службами и протоколами верхнего уровня модели OSI и заканчивая драйверами плат сетевого адаптера на нижнем уровне. Чтобы службы были доступны всем сетевым компонентам, каждый из них должен быть связан с одним или несколькими сетевыми компонентами, предшествующими ему или следующими за ним.

Резюме

Операционная система является основой для функционирования всего аппаратного и программного обеспечения компьютера. При построении сети необходимо осмыслить взаимодействие между компонентамиоперационной системы, которые выполняют в сети автономные и сетевые задачи. Одно из важнейших свойств - многозадачность, позволяющая компьютеру выполнять несколько

процессов одновременно. Программное обеспечение сетевой операционной системы состоит из 2-х компонентов: программного обеспечения клиента и сервера. Прог аммное обеспечение клиента включает в себя так называемый редиректор. Он перехватывает в компьютере запросы и определяет, где они должны выполняться: на локальном компьютере или на удаленном сетевом. Серверное программное обеспечение "отвечает" за совместное использование ресурсов и координирует различные уровни доступа.

При установке системного сетевого программного обеспечения Вы должны присвоить серверу имя, а также определить его роль в сети. При установке сетевой операционной системы некоторое количество сетевых служб, которые выполняют различные сетевые задачи, настраиваются на автоматический запуск.

Контрольные вопросы.

1. Основные возможности и функции сетевых операционных систем.
2. Установка сетевой операционной системы.
3. Главное особенности установки.
4. Програмные компоненты.
5. Что такое редиректор?
6. Сетевые службы.
7. Серверное программное обеспечение?
8. Идентификация сервера?
9. Параметры установки?

Ключевые слова

Процессор;

Периферийные устройства;

Редиректор;

Идентификация;

Шлюза;

Привязка.

Лекция № 13

Внедрение сетевых приложений.

План:

Сетевые приложения.

Электронная почта.

Функции.

Поставщики услуг.

Связь между стандартами.

Планирование.

Совместно используемые приложения.

Резюме.

Литература:

Сетевые приложения.

Многие компьютерные приложения изначально были разработаны для одиночных пользователей, например текстовые процессоры, электронные таблицы, базы данных и графические редакторы.

Эти приложения являлись своебразными компьютезированными версиями стандартного офисного оборудования, такого, как:

- пишущие машини;
- калькуляторы;
- линейки;
- рейсшины;
- блокноты.

Повсеместное применение сетей вызвало модернизацию этих программ. В результате мы стали пользоваться преимуществами таких сетевых возможностей, как разделение ресурсов и выборочная защита. Однако, несмотря на усовершенствования, они остались все теми же заменителями офисного оборудования.

Тем не менее разработчики программного обеспечения очень быстро

оценили мощный потенциал сетей и начали создавать программы специально для многопользоательской работы. К числу таких программ относятся:

- электронная почта и обмен собщениями;
- планирование;
- групповое программное обеспечение.

Электронная почта.

Электронная почта, или e-mail,- это мощное, изощренное средство, которое позволяет пользователю посылать все, что может быть создано на компьютере, любому другому пользователю, имеющему адрес e-mail. Сообщения элетронной почты обычно включает текст, графику, присоедененные файлы, аудио и видео. Сообщения e- mail легко:

- прочитать и уничтожить;
- прочитать и сохранить;
- прочитать и дать ответ;
- отредактировать и сохранить или переслать другому лицу;
- распечатать.

Системы e-mail обеспечивают моментальную связь между всеми сотрудниами в любой организации, независимо от ее размера.

В отличие от телефонной связи, где существует проблема поиска и ожидания абонента, электронная почта удобна как для отправителя, так и для получателя. Сообщения могут быть посланы в любое время суток, с уверенностью в том, что получатель ознакомится с ними в удобный для себя момент. E-mail может также фиксировать обмен сообщениями по конкретной теме, отражая, таким образом, “историю вопроса”.

Функции

Почтовые ящики.

В системе электронной почты для каждого пользователя администратор создает отдельный почтовый ящик. Почтовый ящик-это место, куда доставляется вся почта, приходящая на имя владельца ящика.

Извещение.

Системы электронной почты могут извещать получателей о том, что на них имя поступило сообщение. При этом компьютер получателя подает звуковой сигнал, визуальный сигнал или тот и другой одновременно.

Подтверждение приема.

Программа электронной почты может информировать отправителя о том, было ли получено и прочитано посланное им сообщение.

Ответ.

Большинство систем e-mail предоставляет адресату возможность ответить на сообщение – простым щелчком кнопки ответа, не вводя полный e-mail адрес. Пользователи могут сохранять сообщения от людей, с которыми они часто связываются, и не заботиться о деталях адресации, если в будущем возникнет необходимость вновь обменяться сообщениями.

Присоединённые файлы.

Современные системы электронной почты позволяют пользователям присоединить к сообщениям не только текстовые файлы. Присоединения могут включать электронные таблицы, базы данных, графику, видео- и аудиозаписи.

Каталоги.

Логически законченные системы e-mail имеют особые каталоги-списки всех пользователей системы. Подобные каталоги обычно содержат опширный массив информации о сетевых пользователях:

- имя;
- местонахождение;
- должность;
- номер телефона;
- комментарии.

Эти данные, доступные всем пользователям системы, могут быть полезны не только в случае обмена сообщениями. Ведь найти номер

телефона, уточнить должность кокого-либо лица или адрес его офиса гораздо бысрее и легче через ситему e-mail, несколько раз нажав на клавиши, чем перелистовать справочник.

Поставщики услуг.

Электронная почта стала доступна и через крупных поставщиков, которые предоставляют пользователям связь и услуги по всему миру. Вот список пяти основных:

- Microsoft (MSN)
- CompuServe;
- America Online;
- MCI MAIL;
- AT&T.

Их ситемы почты превратились в стандартные платформы связи, через которые каждый абонент может связываться с любым другим подписчиком, имеющим в системе почтовый ящик. Этой возможностью пользуются, например, абоненты CompuServe и MCI. Подписка на такие услуги доступна через локальных поставщиков.

Поддержка.

При планировании системы e-mail администратор сети должен позаботиться об её поддержке и обучении пользователей. Некоторые организации на роль администратора электронной почты назначают специального сотрудника, в обязанности которого входит:

- создание, модификация и удаление пользователей и групп;
- управление хранилищем сообщений и папок на почтовом сервере;
- администрирование каталогов электронной почты;
- указание новых почтовых отделений, удаленных пользователей и сетей, с которыми должна обмениваться данными Ваша почтовая система;

- обучение новых пользователей.

Связь между стандартами.

Сети, которые связаны с другими сетями бщей несущей, могут столкнуться с проблемой: как обмениваться сообщениями, если их почтовые системы различны? В этой ситуации сеть должна транслировать входящие сообщения в формат, понятный собственной системе. Устройство, выполняющее преобразование, называется шлюзом. Обычно он представляет собой компьютер, выделенный специально для этой задачи.

Планирование.

Сетевые утилиты планирования помогают пользователям оптимально планировать своё время. Они пригодны как для индивидуального, так и для группового планирования рабочего дня.

Индивидуальное планирование.

Программы планирования – это электронная версия обычного календаря-блокнота, предназначенная для ежедневного, ежемесячного и ежегодного планирования деловых встреч, переговоров и т.д. Хотя планировщики от разных поставщиков имеют свои особенности, все они выполняют стандартные функции: помогают пользователям “ вести” электронный ежедневник, который автоматически напомнит о предстоящем событии. Это избавляет пользователя от необходимости постоянно заглядывать в календарь или держать в памяти тысячи подробностей.

Большинство планировщик следит за календарём и, по мере прлближения события, выводит на экран сообщение-напоминание.

Когда пользователь дополняет расписание очередной записью (например, датой встречи), утилита планирования автоматически проверяет, не намечено ли в электронном календаре на это время другое событие. Если других событий нет, утилита внесет эту встручу в распорядок дня. А в том случае, пользователь попытается назначить на это

же время еще одну встречу, прогамма-планировщик известит его конфликте.

Групповое планирование.

Программа электронного планирования на сетевом уровне решают и такую задачу: автомвтически проверяют расписание всех потенциальных учатниеов втречи и указывают организатору этой встречи, когда у них есть свободное время. Основываясь на информации планировщика, организатор встречи подбирает день и час, когла все свободны, а электронный планировщик автоматически вносит событие в календарь каждого участника.

Затем электронный планировщик будет следить за сроками и напомнит каждому о приближении встречи.

Используя продукты типа Microsoft Schedule+, Вы сможете просматриватьраспорядок дня другого лица, если, конечно, этот человек сделал свой календарь доступным для просмотра. Такая возможность избавит Вас от лишних хлопот. Электрнный планировщик может также предоставить Вам своеобразный отчет о всех и событиях, прошедших за определенный период.

Мультимедиа.

Основные производители группого программного обеспечения включают в свои продукты новейшие технологии, которые значительно расширяют диапозон применения электронных коммуникаций. Причём расширяют на такие области, о которых несколько лет назад ещё никто и не слышал. Современные системы группового программного обеспечения поддерживают мультимедиа, т.е. совмещают в одной системе разнообразные типы данных и информации.

- сканированные изображения;
- факсимальные сообщения;
- речь;
- звук;

- оптическое распознание символов;
- графику;
- видео и видеоконфигурации.

Совместно используемые приложения.

Такие приложения, как текстовые процессы, базы данных и электронные таблицы, подобно любым другим ресурсам, могут совместно использоваться в сети. Это имеет как минимум два достоинства:

- прикладные рограммы обходятся дешевле, так как общая лицензия на 200 пользователей обычно стоит меньше, чем 200 индивидуальных копий приложения;
- существует гарантия, что версия приложения у всех одна и та же.

Тем не менее администратор сети должен знать о некоторых особенностях совместного использования приложений в сети. Компании, совместно использующие приложения, должны приобретать оющую лицензию, которая потверждает законность применения программы. В противном случае любой человек, кроме непосредственного поеупателя приложения, будет использовать программу незаконно.

Администратору сети придется организовать и обучение персонала.Этого требуют, как правило, новые версии текущего приложения и новые программы. Аминистратор должен разъяснить пользователям, что хотя обучение новым приложениям и новым версиям снизит производительность, но только на короткое время. В перспективе они принесут выгоду.

Резюме.

Некоторые прложения былисозданы специально для работы в сетях-электронная почта и обработка сообщений, планирование, а также группа интерактивных приложений реального времени, которые называбтся групповым прграммным обеспечение.

Электронная почта своим рождением обязана простой передаче

сообщений в сети. А сообщения электронной почты могут включать текст и графику, аудио и видео. Пользователи электронной почты обмениваются сообщениями через почтовые ящики. К особенностям электронной почты относятся извещение адресата о приходе сообщений и поддержка функций ответа. Кроме того, пользователи могут присоединять к сообщениям файлы различных типов. Кроме правило, системы электронной почты для каждого пользователя имеют отдельный каталог.

Программы электронной почты и обработки сообщений относятся CCITTX.400 и X.500, простой протокол передачи почты (SMTP) и служба обработки сообщений (MHS). Обмен сообщениями между сетями, использующими различные стандарты, выполняются через шлюзы. Шлюз-это компьютер, предназначенный для преобразования протоколов.

Кроме приложений, специально предназначенных для сетей, совместно могут использоваться в сети и приложения, изначально созданные для автономного выполнения, такие, как базы данных или текстовые процессоры. Администратор сети должен проанализировать различные проблемы, возникающие при установке в сетитаких приложений. Эти проблемы связаны с возможностями сети, коллективным лицензированием, веленим журнала программного обеспечения и обучением пользователей.

Контрольные вопросы.

1. Сетевые приложения.
2. Электронная почта и обмен сообщениями.
3. Планирование.
4. Групповое программное обеспечение.
5. Функции.
6. Связь между стандартами.
7. Планирование.
8. Мультимедиа.

Ключевые слова.

пишущие машинки;

калькулятор;

линейки;

рейсшины;

блокноты;

мультимедиа.

Лекция № 14

Сети с компонентами от разных Производителей.

План:

Типичная сетевая среда.

Решение со сторноны клиента.

Решение со стороны сервера.

Выбор производителя.

Novell.

Apple.

Резюме.

Литература:

Типичная сетевая среда

Сегодня большинство сетей состоит из компонентов от разных производителей. Хотя при реализации таких сетей иногда возникают сложные проблемы, четкое планирование помогает их преодолеть, и сети работают вполне корректно.

Проблемы чаще всего возникают, если в сети выполняются сетевые операционные системы нескольких типов, а также если операционные системы клиентов и редиректоры получены от разных производителей. Иными словами, характер сети меняется, когда программным компонентам от разных производителей приходится работать в одной «упряжке».

Операционная система сервера, операционная система клиента и редиректор должны быть совместимы. Например, если в Вашей сети один клиент работает под управлением Microsoft Windows 95, другой является клиентом для Novell NetWare, третий — Apple Macintosh, а на сервере работает Microsoft Windows NT Server, то и сервер, и клиенты должны найти общий язык, чтобы каждый компонент мог понимать других.

Решение со стороны клиента

В большинстве ситуаций, затрагивающих несколько сетевых операционных систем, ключ к достижению взаи-модействия - редиректор Точно так же, как Ваш телефон для связи с различными абонентами может воспользоваться услугами не одной телефонной компании, компьютеры для связи с различными сетевыми серверами могут иметь несколько редиректоров.

Каждый редиректор обрабатывает только те пакеты, которые передаются на понятном ему языке и по понят-ному ему протоколу. Если Вы знаете, к каким ресурсам Вам необходим доступ, установите соответствующий редиректор - он передаст Ваши запросы по указанному местоназначению.

Допустим, клиенту под управлением Windows NT необходим доступ к серверу Novell. Администратор сети может добиться этого, загрузив на клиенте поверх Windows NT редиректор Microsoft - для доступа к серверам Novell.

Решение со стороны сервера

Второй способ реализовать связь между клиентом и сервером - установка службы на сервере. Такой метод применяется для включения компьютеров Apple Macintosh в среду Windows NT. Microsoft поставляет службу Services for Macintosh, которая позволяет серверу под управлением Windows NT Server взаимодействовать с клиентом Apple.

Если установлена служба Services for Macintosh, пользователи Macintosh получают доступ к ресурсам сервера Windows NT. Эта служба, кроме того, преобразовывает файлы между компьютерами, работающими под управлением Macintosh и Windows NT. Таким образом, пользователи Macintosh и пользователи Windows NT могут сохранить свои собственные интерфейсы для работы с одними и теми же файлами.

Пользователь Macintosh продолжает следовать стандартным процедурам Macintosh и видеть значки Macintosh (такие, как Chooser и Finder), даже если он обращает-ся к ресурсам сервера Windows NT.

Выбор производителя

Основными поставщиками сетевых продуктов являются три фирмы:

- Microsoft,
- Novell,
- Apple

Эти три производителя уже давно осознали: совмес-тимость их продуктов дает значительные преимущества. Поэтому каждый производитель предлагает утилиты, которые:

- позволяют его операционным системам связываться с серверами остальных двух производителей,
- помогают его серверам распознавать клиентов остальных двух производителей.

Microsoft

Microsoft встроила редиректор, распознающий сети Microsoft, в следующие операционные системы своего производства:

- Windows NT,
- Windows 95,
- Windows для рабочих групп

Редиректор автоматически запускается при установке операционной системы. Программа установки загружает необходимые драйверы и редактирует файлы настройки так, чтобы редиректор начал функционировать сразу после включения компьютера

Программное обеспечение редиректора фирмы Microsoft не только предоставляет всем клиентам возможность доступа к ресурсам сети, но и каждому клиенту Windows для рабочих групп и Windows NT - возможность разделять свои собственные ресурсы.

Microsoft в среде Novell

Для подключения клиента под управлением Windows NT Workstation к сети Novell NetWare необходим протокол NWLink и служба Client Service for NetWare (GSNW). Для подключения сервера под управлением Windows NT Server к сети NetWare необходим протокол NWLink и служба Gateway Service for NetWare (GSNW). NWLink - это реализация фирмой Microsoft протокола IPX/SPX. CSNW - это реализация фирмой Microsoft редиректора для доступа к NetWare (в терминах фирмы Novell - «запросчик»). Вместе они составляют законченное решение по подк-лючению Microsoft Windows NT к серверам Novell NetWare.

Для подключения клиента под управлением Windows 95 к сети NetWare необходим протокол IPX/SPX и Microsoft Client for NetWare Networks (клиент для сетей NetWare фирмы Microsoft). Microsoft Service for NetWare Directory Services (NDS - служба каталогов NetWare) - это усовершенствованное программное обеспечение клиента NetWare, осуществляющее поддержку Novell NetWare 4. x Directory Services. Microsoft NDS предоставляет пользова-телям поддержку регистрации и просмотра сети для служб регистрационной базы данных NetWare 2- x, 3-x и 4- x, которые будут выступать как серверы NetWare 4- x NDS.

Клиенты MS-DOS

Поставщики серверных операционных систем предлагают утилиты, которые позволяют клиентам под управлением MSDOS получать доступ к серверам всех трех поставщиков. Эти утилиты можно установить на одной машине; в этом случае один MS-DOSклиент будет работать с серверами всех трех сред.

Novell

Серверы Novell могут распознавать следующих клиентов служб совместного использования файлов и принтеров.

Клиенты NetWare символьного режима под управлением MSDOS или DRDOS могут подключаться:

- к серверам Novell NetWare;
- компьютерам под управлением Windows NT Server

Клиенты Windows NT с запущенным запросчиком Novell NetWare и редиректором Windows NT могут подключаться:

- к серверам Novell NetWare;
- компьютерам под управлением Windows NT Workstation и Windows NT Server

Фирма Novell поставляет запросчики для следующих операционных систем компьютеровклиентов:

- MS-DOS;
- OS/2;
- Windows NT

Apple

В среде Macintosh редиректор фирмы Apple является частью операционной системы Macintosh AppleShare - это сетевая операционная система фирмы Apple; она обеспечивает функции совместного использования файлов. Клиентское программное обеспечение поставляется с каждой копией операционной системы Apple. Существует также сервер печати AppleShare - серверный спулер принтера. Таким образом, компьютеры Macintosh поставляются полностью оборудованными для работы в сетях Apple

Клиенты MS-DOS

Программное обеспечение AppleShare для персональных компьютеров предоставляет клиентам под управлением MS-DOS доступ к серверам файлов и печати AppleShare. С установленным программным обеспечением Ap-pleShare (для персональных компьютеров) и при наличии платы LocalTalk (для персональных компьютеров) пользователи получают доступ к томам сервера файлов (хра-нилищу файлов) и принтерам сети AppleTalk. Плата LocalTalk для ПК содержит микропрограмму, управляющую соединением между сетью AppleTalk и персональным ком-

пьютером. Драйвер LocalTalk для ПК реализует большинство протоколов AppleTalk и взаимодействует с платой для приема и передачи пакетов.

Служба Services for Macintosh

При установленной службе Services for Macintosh сервер Windows NT становится доступным клиентам Macintosh. Благодаря этому продукту клиенты под управлением MS-DOS и Macintosh-клиенты могут совместно использовать файлы и принтеры. Служба Services for Macintosh включает протоколы AppleTalk версий 2. 0 и 2. 1, Local-Talk, Ether-Talk, TokenTalk и FDDITalk. Кроме того, Ser-vices for Macintosh поддерживает принтер LaserWriter® версии 5. 2 или более поздней.

Резюме

Взаимодействие сетевых компонентов от разных производителей может быть достигнуто благодаря мерам со стороны клиента или со стороны сервера. Со стороны клиента можно установить редиректор. Редиректор будет перехватывать запросы к службам и передавать их через сеть соответствующим компонентам сети. Со стороны сервера можно установить службу, которая преобразует сервер так, чтобы клиенту казалось, будто сервер работает под управлением «родной» (для клиента) сетевой операционной системы.

Выбор решения зависит от поставщика, продукты которого Вы используете. Основными поставщиками сетевых продуктов являются фирмы Microsoft, Novell и Apple.

Решения со стороны сервера применяются для включения компьютеров Macintosh в среду персональных компьютеров. При реализации решений со стороны клиентов Вы должны уточнить, существуют ли редиректоры, которые будут:

- выполняться на компьютерах в Вашей сети;
- взаимодействовать с Вашей сетевой операционной системой.

Контрольные вопросы.

1. Особенности сетей?
2. Некоторыепроблемы возникающие при реализации таких сетей, и методы их решения.
3. Какие фирмы являются постовщиками сетей, перечслите?
4. Что делает каждый редиректор?
5. Что такое Apple?
6. Что такое Novell?

Ключевые слова.

Редиректор;

протокол;

служба;

установки;

запросчики.

Лекция № 15.

Сетевая печать.

Среда клиент сервер.

План:

Обзор.

Разрешение совместного использования принтера.

Ввод информации о принторе.

Подключение к принтеру.

Управление совместно используемым принтером.

Управление правам доступа пользователей.

Языки описания страниц.

Удаление администрирование.

Резюме.

Обзор

Чтобы напечатать данные на сетевом принтере, пользователи сети посылают свои данные на сервер печати, который затем передает их на принтер.

Переадресация (redirection) играет важную роль в се-тевой печати, так как каждое задание на сетевую печать должно быть направлено не на локальный принтер, а в сеть Процесс печати состоит из двух этапов

1. Редиректор компьютера передает по сети задание на печать.
2. Сетевое программное обеспечение сервера печати получает по сети задание на печать и добавляет его к остальным заданиям, ожидающим доступа к совместно используемому принтеру, т. е. формирует очередь на печать.

В крайне загруженной среде может быть много документов, ожидающих печати. Чтобы упростить выборку заданий из сети на принтер, сеть использует буферизацию, или spool (simultaneous peripheral operation on line - буферизация входных и выходных потоков).

Спулер - это буфер в оперативной памяти сервера печати, который хранит задание на печать до тех пор, пока принтер не будет готов его выполнить. Так как буфер находится в оперативной памяти, данные из него попадут в принтер быстрее, чем с жесткого диска. Однако, если для печати одновременно послано множество документов и буфер переполняется, часть документов будет «сброшена» на жесткий диск сервера печати, где им придется ожидать возвращения в буфер

Разрешение совместного использования принтера

Простое подключение принтера к сетевому серверу печати еще не делает его доступным пользователям сети: несмотря на то что физически принтер является частью сети, ему еще не присвоен сетевой идентификатор.

Чтобы посылать на принтер свои данные, пользователи должны идентифицировать (т. е. «видеть») принтер со своих компьютеров. Другими словами, сетевая операционная система должна дать принтеру имя и известить о нем и о его доступности все сетевые компьютеры.

Ввод информации о принтере

Каждая сетевая операционная система имеет собственную версию разделения принтера, однако все они тре-буют, чтобы администратор установил драйвер принтера и сообщил сетевой операционной системе некоторые данные об этом принтере.

Такая процедура включает:

- загрузку драйверов принтера, чтобы последний мог работать с сервером печати;
- назначение принтеру (как разделяемому ресурсу) имени, чтобы сети могли идентифициро-вать это имя и получить доступ к принтеру;
- назначение места вывода данных, чтобы редиректор знал, куда необходимо передавать задания на печать;

- установку параметров печати и параметров формата выходных данных, чтобы сетевая операционная система знала, как обрабатывать и форматировать задания на печать.

Утилиты совместного использования принтеров

Совместное использование принтеров может показаться, на первый взгляд, сложным процессом, однако большинство сетевых операционных систем имеет утилиты, которые помогают администраторам вводить информацию Например, в Windows NT Server утилита под названием Print Manager предоставляет окно для настройки принтера

Подключение к принтеру

Сначала Вы должны предоставить принтер в совместное использование, а затем с помощью сетевой операционной системы подключиться к нему Для этого надо знать две вещи.

- имя сервера, к которому подключен принтер;
- имя принтера

Вот почему администратор обязательно вводит имя принтера (во время разрешения его совместного использо-вания) Современные операционные системы, такие, как Windows NT, имеют графический пользовательский интерфейс, который значительно упрощает подключение к принтеру

Управление совместно используемым принтером

Разрешив совместное использование принтера, администратор сети теперь должен и управлять им, и обслуживать его. Администрирование принтера имеет две «облас-ти ответственности»:

- собственно обслуживание принтера,
- управление правами доступа пользователей к принтеру

Обслуживание принтера

Обслуживание принтера подразумевает:

- снабжение принтера бумагой и тонером, очистку принтера от смятой бумаги;
- контроль за выводом на принтер, чтобы предотвратить дублирование заданий на печать и переполнение выходного лотка,
- контроль за работой принтера и вызов технических специалистов в случае возникновения серьезных проблем.

Многие из этих задач являются рутинными и глубоких знаний не требуют. Если рядом с принтером лежит вразумительная инструкция, пользователи обычно не отказываются наполнить пустой лоток бумагой или заменить опустевший картридж с тонером новым.

Однако, если никто не отвечает за функционирование принтера, работа пользователей может осложниться. Ведь часто каждый думает, что кто-то другой должен разбираться с постоянными сбоями принтера. В результате простейшие проблемы мешают нормально работать до тех пор, пока какой-нибудь выведенный из себя доброволец не возьмется за исправление ситуации.

Управление правами доступа пользователей

Принтер рассматривается в ряду любых других совместно используемых ресурсов Поэтому пользователи должны иметь не только права на доступ к нему, им также должен быть присвоен определенный уровень этих прав.

Например, пользователи с соответствующими привилегиями могут манипулировать заданиями на печать, которые передаются на сетевой принтер. Они вправе пере-мещать свои задания в начало очереди, отодвигая задания других пользователей или даже удаляя некоторые из

них совсем. Во избежание конфликтов ограничьте количество пользователей, наделенных такими привилегиями.

Диапазон привилегий, относящихся к печати, зависит от сетевой операционной системы. Сетевые операционные системы содержат утилиты, которые администратор может использовать для назначения соответствующих привилегий печати. Таким образом, именно администратор определяет, какими привилегиями будут обладать пользователи.

В частности, Windows NT Server Print Manager с помощью серии диалоговых окон упрощает администратору управление правами доступа к принтерам.

Языки описания страниц

Сетевой администратор должен знать, как устанавливать и обслуживать сетевой принтер. Но не только. Он должен также выявлять все факторы, от которых может зависеть функционирование и производительность прин-тера. Один из этих факторов - язык описания страниц (Page Description Language, PDL).

Языки описания страниц сообщают принтеру, как должны выглядеть напечатанные документы. На PDL указываются позиции для каждого элемента и параметры печати, такие, как размеры и виды шрифтов, однако сам процесс формирования страницы возлагается на принтер.

Благодаря своему воздействию на печать языки описания страниц очень важны для администраторов. PostScript, например, обеспечивает гибкое управление шрифтами (любого размера) и высококачественную графику. Поэтому PostScript поможет Вам творчески подойти к созданию различных документов.

Удаленное администрирование

Чтобы управлять сетевым принтером, администратору не нужно находиться рядом с сервером печати. Большинство современных сетевых операционных систем предлагает утилиты, которые могут использоваться администрато-ром для управления принтером с любого компьютера в сети.

Итак, с удаленного компьютера администратор может:

- приостановить печать на принтере;
- удалить некоторые задания из очереди на печать;
- изменить порядок заданий в очереди на печать.

В небольших сетях, где все серверы и компьютеры расположены относительно близко друг к другу, такая возможность не столь важна. Однако, если сеть велика и принтер и компьютер администратора находятся в разных частях здания, эта возможность окажется очень полезной.

Для локального и удаленного управления принтером используются одни и те же утилиты. В Windows NT Ser-ver, например, администратор просто выбирает принтер для администрирования, и сетевая операционная система с помощью последовательности диалоговых окон проводит администратора через весь процесс.

Совместное использование факсмодемов

Совместно используемый факс-модем для факсимильной связи означает то же, что совместно используемый прин-тер - для печати. Он обеспечивает доступ к факсу для каждого пользователя сети. Возможность посылать факсы по сети помогает пользователям сберечь время (не надо покидать свое рабочее место) и нервы (не надо разбираться с устройством автономного факсаппарата).

Хорошая служба факс - сервера позволит администратору отмечать все входящие факсы и рассылать их соответствующим пользователям, а

также отбрасывать те из них, которые не представляют интереса, например рек-ламу.

Некоторые утилиты сетевого факса позволяют пользователям связывать свои адреса электронной почты с номером факса. В результате предназначенные им факсимильные сообщения пересылаются автоматически.

Резюме

Чтобы установить в сети совместно используемый принтер, администратору необходимо установить драйверы принтера;

- присвоить принтеру сетевое имя;
- указать местонахождение вывода;
- установить параметры выходного формата

Большинство сетевых операционных систем имеет утилиты, которые проводят Вас через этот процесс. После установки принтера каждый пользователь должен инди-видуально подключиться к нему.

Администратор сети отвечает за поддержку принтера и управление пользователями. Его обязанности достаточ-но разнообразны: начиная с загрузки бумаги в принтер и кончая назначением пользовательских привилегий. Windows NT Server с помощью последовательности диалоговых окон направляет процесс администрирования. Большинство современных сетевых операционных систем позволяет администратору управлять принтером с любого компьютера в сети.

Существуют также факс-серверы для совместно используемых факс устройств. Благодаря им пользователи могут посылать факсы со своих собственных компьютеров. Для маршрутизации входящих факсов применяются различные методы.

Контрольные вопросы.

1. Сместное исподьзование принтера.
2. Краткая характеристика языков описания страниц.
3. Специализированные устройства для совместного ипользования принтеров.
4. Совместное использование факс-модемов.
5. Утилиты совместное использованияпринтеров.
6. Подключение к принтеру.
7. Языки описания страниц.
8. Удаление администрирование.

Ключевые слова.

Сервер печати ;

спулер;

идентификатор;

редиректор;

принтер.

Лекция № 16.

Администрирование сети.

Управление пользователями.

Управление производительностью сети.

План:

Управление сетью.

Области администрирования.

Обязанности администратора.

Создание учётных записей пользователей.

Ввод данных о пользователе .

Установка параметров пользователя.

Пофили.

Учётная запись гостя.

Типы групп.

Блакирование.

Резюме.

Литература:

Управление сетью

Сеть, которая может работать сама по себе, еще не придумана. Время от времени нужно подключатъ новых пользователей, а среди существующих некоторых иногда удалять. Приходиться устанавливать новые ресурсы и предоставлять их в совместное использование,кроме того, предоставлять соответствующие права на доступ к ним. Права доступа – это правила, ассоциированные с ресурсом, обычно каталогом, файлом или принтером.Права регулируют доступ пользователей к ресурсам. Всё это означает, что после установки сетью необходимо управлять.

Области администрирования

Сеиевое администрирование распространяется на пять основных областей, с которыми должен быть хорошо знаком администратор сети:

управление пользователями - создание и поддержка учетных записей пользователей, управление доступом пользователей к ресурсам;

управление ресурсами - установка и поддержка сетевых ресурсов; уаправление конфигурацией - планирование конфигурации сети, ее расширение, а также ведение необходимой документации;

управление производительностью - мониторинг и контроль за сетевыми операциями для поддержания и улучшения производительности системы;

поддержка - предупреждение, выявление и решение проблем сети.

Обязанности администратора

Учитывая области сетевого управления, можно составить список задач, за выполнение которых отвечает администратор сети:

- создание учетных записей пользователей и управление ими;
- защита данных;
- обучение и поддержка пользователей (при необходимости);
- модернизация существующего программного обеспечения и установка нового;
- архивирование;
- предупреждение потери данных;
- мониторинг и управление пространством для хранения данных на сервере;
- настройка сети для достижения максимальной производительности;
- резервное копирование данных;
- защита сети от вирусов;
- решение сетевых проблем;
- модернизация и замена компонентов сети (при необходимости);

- добавление в сеть новых компьютеров.

Создание учетных записей пользователей

Каждому, кто работает в сети, необходимо выделить учетную запись пользователя. Учетная запись состоит из имени пользователя и назначенных ему параметров систему. Эта информация вводится администратором и сохраняется сетевой операционной системой. При попытке пользователя войти в сеть его имя служит для проверки учетной записи.

Все сети имеют утилиты, которые помогают администраторам добавить в базу данных безопасности сети новые учетные записи. Этот процесс иногда называют зданием пользователя». В Microsoft Windows NT Server утилита для создания записей называется User Manager for Domains, она находится группе программ nistrative Tools.

Запустив утилиту **User Manager,** выберите из меню **User** команду New **User...** Появится одноименное окно, в которое можно ввести информацию, необходимую для новой учетной записи пользователя .

Ввод данных о пользователе

Учетная запись содержит информацию, которая определяет пользователя в системе безопасности сети, в том числе:

- имя и пароль пользователя;
- права пользователя на доступ к ресурсам системы;
- группы, к которым относится учетная запись.

Эти данные необходимы администратору для создания новой учетной записи. Поясним назначение некоторых полей, заполняемых при создании новой записи.

- **Username** - тидентифицирует учетную запись пользователя. Имя ользователя не должно совпадать с именем другого пользователя, группы администрируюемого домена или компьютера. Оно может

содержать до 20 любых символов произвол ьного регистра, исключая следующие: « / \:; | =, + * ? < >

- **Full Name** - содержит полное имя пользователя.
- **Description** - содержит текст, описывающий учетную запись или пользователя.
- **Password и Confirm Password** - содержит пароль, максимальная длина которого символов. Регистр символов в данном случае значим: нужно ввести одинаковые пароли в оба поля.

Windows NT Server реализует возможность, имеющуюся в большинстве утилит управления пользователями — копирование учетных записей. С ее помощью администратор создает «модель» пользователя, отдельные параметры и характеристики которой могут потребоваться другим пользователям. Для создания новой учетной записи с этими характеристиками администратор просто копирует эту-образцовую-запись и дает ей новое имя.

Установка параметров пользователя

Большинство сетей позволяет администраторам присваивать пользователям некоторые дополнительные параметры, в том числе:

- время регистрации - чтобы ограничить время, в течение которого пользователь может войти в сеть;
- домашний каталог- чтобы предоставить пользователю место для хранения его личных файлов;
- продолжительность действия учетной записи - чтобы ограничить «пребывание» некоторых пользователей в сети.

Профили

Администратору пригодится в работе и другая возможность - построить для некоторохых пользователей сетевое окружение. Это необходимо, например, для поддержки определенного уровня безопасности или для поддержки пользователей, не овладевших

комьютерами и сетями в такой степени, чтобы самостоятельно работать с этой технологией. Администратор может создать профили (profiles) для управления средой пользоваетелей, в которой они оказываются после входа в систему. К среде относятся сетевые подключения и доступные программы, а также:

- подключения к принтерам;
- настройки Program Manager;
- значки;
- настройки мыши;
- цвета экрана;
- хранители экрана.

К параметрам профилей, кроме того, иногда относятся специальные условия входа в систему и информация о том, где пользователь может хранить свои файлы.

Ключевые учетные записи пользователей

Сетевые операционные системы поставляются с заранее созданными пользовательскими учетными записями некоторых типов, которые автоматически активизируются при установке системы.

Администратор — начальная учетная запись

При установке сетевой операционной системы автоматически создается учетная запись пользователя, обладающего полной «властью» в сети. Именно на него возлагаются следующие функции:

- формирование сети;
- установка начальных параметров защиты;
- создание других пользователей.

В сетевой среде Microsoft этот пользователь носит имя Administrate тор). В среде Novell он известен как Supervisor (Супервизор). Обычно тот, кто установил сетевую операционную систему, первым входит в сеть. Войдя в сеть с учетной записью администратора, он имеет полный контроль сетевыми функциями.

Учетная запись гостя

Другой стандартный пользователь, создаваемый программой установки, называется Guest (Гость). Эта учетная запись предназначена для людей, которые не являются полноправными пользователями сети, однако нуждаются во временном доступе к ней. Некоторые сетевые операционные системы, например Microsoft Wind после установки оставляют учетную запись гостя отключенной. Администратор сети может ее активизировать.

Пароли

Пароли (passwords) обеспечивают безопасность сетевой среды. Поэтому первое, что должен сделать администратор при установке параметров своей учетной записи,-это изменить пароль. Он предотвратит и несанкционированный вход в сеть пользователей с правами администратора, и создание ими других пользователей.

Каждый должен придумать себе уникальный пароль и хранить его в тайне. В особо важных случаях надо обязать пользователей периодически менять свои пароли. Многие сетевые операционные системы предлагают средства, которые автоматически вынуждают пользователей делать это через заданный администратором промежуток времени.

В ситуациях, когда безопасность не столь существенна или когда права доступа ограниченны (как в учетной записи гостя), можно модифицировать учетную запись так, чтобы для входа в сеть конкретного пользователя не требовался пароль.

Администратор, наконец, должен учесть и такой вариант: в систему попытается войти пользователь, уже уволенный из компании. Единственный путь избежать этого-деактивизировать учетную запись бывшего сотрудника как можно быстрее.

Вот некоторые традиционные советы по управлению паролями:

- не используйте очевидные пароли, такие, как дата рождения, имя Вашей супруги (супруга) или ребенка, кличка собаки и т. п.;
- лучшее место для хранения пароля - Ваша память, а не бумажка, приклеенная к монитору;

не забывайте про срок действия Вашего пароля (если конечная дата установлена), чтобы изменить пароль до того, как он перестанет действовать и система будет заблокирована.

Как только пользователи, которым при операциях с паролями помогал администратор, приобретут некоторый опыт, администратор вправе определить приемлемую для них политику защиты паролями.

Учетные записи групп

Сети могут поддерживать тысячи учетных записей (accounts). Бывают случаи, когда администратор должен произвести одни и те же действия над каждой из этих записей или, по крайней мере, над значительной их частью.

Иногда администратор вынужден посылать одно и то же сообщение большому количеству пользователей (извещая их о каком-либо событии) или определять, какие пользователи должны иметь доступ к определенным ресурсам. Для этого администратору необходимо модифицировать каждую учетную запись, изменяя в ней права доступа конкретного пользователя. Если 100 человек нуждаются в разрешении на использование какого-нибудь ресурса, администратор должен по очереди предоставить это право каждому из ста.

Практически все сети решают эту проблему, предлагая объединить отдельные пользовательские учетные записи в одну учетную запись специального типа, называемую группой. Группа (group) - это учетная запись, которая содержит другие учетные записи. Основная причина реализации групп - упрощение администрирования. Группы

предоставляют администраторам возможность оперировать большим пользователей как одним сетевым пользователем.

Если 100 учетных записей объединены в группу, администратор может послать группе одно сообщение, и все ее члены автоматически получат его. Аналогично право на доступ к ресурсу можно присвоить группе, и все ее члены получат его.

Планирование групп

Поскольку группы - очень мощный инструмент администрирования, при планировании сети им необходимо уделять особое внимание. Опытные администраторы знают, что практически не должно быть индивидуальных пользователей сети. Каждый пользователь будет разделять с другими определенные привилегии и обязанности. Привилегии (rights) уполномочивают пользователя на выполнение некоторых действий в системе. Например, он может иметь привилегию проводить резервное копирование системы. Привилегии относятся к системе в целом и этим отличаются от прав. Права (permissions) и привилегии должны быть присвоены группам так, чтобы администратор мог обращаться с ними, как с одиночными пользователями. Группы помогают осуществить следующие действия:

- Предоставить доступ к ресурсам (таким, как файлы, каталоги и принтеры). Правпа предоставленные группе, автоматически предоставляются ее членам.
- Предоставить привилегии для выполнения системных задач [таких, как резервное копирование, восстановление файлов (с резервных копий) или изменение системного времени]. По умолчанию ни одному из пользователей ни одна из привилегий не присваивается. Пользователи получают привилегии через членство в группах.
- Упростить связь за счет уменьшения количества подготавливаемых и передавемых сообщений

Создание групп

Созданние групп подобно созданию учетной записи индивидуального пользователя. Большинство сетей имеет утилиты, с помощью которых администратор может формировать новые группы. В Microsoft Windows NT Server эта программа называется **User** ger **for Domains** и находится в группе программ **Administrative Tools.** Запустив утилиту **User Manager,** выберите из меню User команду **New Local Group....**

Появится одноименное диалоговое окно, предназначенное для ввода информации о новой локальной группе.Поясним назначение полей, заполняемых при создании новых групп.

Group Name - идентифицирует локальную группу. Имя группы не должно совпадать с именем какой-либо другой группы (или пользователя) в администрируемом домене или компьютере. Оно может содержать любые символы произвольного регистра, исключая следующие: ; \ = + *?<>

Description — содержит текст, описывающий группу или пользователей этой группы.

Основное различие между созданием группы и созданием группы индивидуального пользователя состоит в том, что группа должна «знать», какие пользователи являются ее членами. Поэтому задача администратора - выбрать соответствующих пользователей и присвоить их группе.

Типы групп

Microsoft Windows NT Server использует группы четырех типов.

Локальные (local) группы.

Группы этого типа реализуются в базе данных учетных записей отдельного компьютера. Локальные группы состоят из учетных записей пользователей, которые имеют права и привилегии на локальном компьютере, и учетных записей глобальных групп.

Глобальные (global) группы.

Группы этого типа используются в границах всего домена. Глобальные группы регистрируются на главном контроллере домена (PDC) и могут содержать только тех пользователей, чьи учетные записи находятся в базе данных этого домена.

- Специальные (special) группы.
- Эти группы обычно используются Windows NT Server для внутрисистемных нужд.
- Встроенные (built-in) группы.

Некоторые функции групп этого типа общие для всех сетей. К ним от большинство задач администрирования и обслуживания. Чтобы выполнять стандартные операции, администраторы должны создавать учетные записи пользователей и группы с соответствующими привилегиями, однако многие поставщики сетей избавляют администраторов от этих хлопот, предлагая им встроенные локальные или глобальные группы. Встроенные группы делятся на три категории:

- администраторы - пользователи этих групп имеют максимально возможные привилегии;
- операторы - пользователи этих групп имеют ограниченные административные возможности для выполнения специфических задач;
- другие - пользователи этих групп выполняют ограниченные задачи.

Предоставление привилегии группам

Простейший метод предоставить одинаковые права большому количеству пользователей-присвоить эти права группе, а затем добавить в группу пользователей. Аналогично добавляются пользователи во встроенную группу. Например, если администратор захочет, чтобы какой-то пользователь выполнял в сети административные задачи, он сделает этого пользователя членом группы Administrators.

Блокирование и удаление учетных записей пользователей

Иногда администратор должен исключить возможность использования в сети какой- нибудь учетной записи. Этого можно достичь ее блокированием или удаленим.

Блокирование

Если учетную запись заблокировать, она по-прежнему будет находиться в базе данных учетных записей сети, однако никто не сможет использовать ее для входа в сеть. Блокированная учетная запись как бы не существует. Администратору следует отключить учетную запись сразу после того, как пользователь кончил с ней работать. Если станет ясно, что учетная запись вообще болбше не понадобится, ее можно удалить. Для блокировки учетных записей пользователей в Windows NT Server служит окно **User Properties** программы **User Manager.** Чтобы заблокировать пользователя, дважды щелкните имя его учетной записи, установите флажок **Account Disabled,** а затем щелкните **ОК.** Теперь учетная запись заблокирована .

Удаление.

Удаление учетной записи уничтожает информацию о пользователе в базе данных учетных записей сети; пользователь больше не сможет получить доступ к сети.

Учетная запись пользователя должна быть удалена в следующих случаях:

- пользователь уволился из организации;
- кончился срок найма пользователя;
- ользователь сменил рабочее место внутри организации (его доступ к данной сети необходимо закрыть).

Процесс удаления пользователя обычно несложен: надо выбрать имя учетной записи и щелкнуть кнопку в диалоговом окне. В Microsoft Windows NT Server, например, лаления учетных записей пользователей служит программа **User Manager for Domains.** Выберите учетную запись,

которую нужно удалить, затем нажмите клавишу DELETE. Подтвердив, что Вы действительно хотите удалить учетную запись, щелкните ОК - учетная запись будет удалена.

Управление производительностью сети

После установки и запуска сети администратор должен быть уверен в том, что она эффективно работает. Для этого ему приходится следить за производительностью сети и управлять всеми факторами, которые на нее влияют.Масштаб задач по управлению сетью зависит:

- численности и профессионализма сотрудников, которые обеспечивают поддержку сети;
- средств, выделяемых на поддержку сети;
- ожидаемой отдачи от использования сети.

Небольшую одноранговую сеть, состоящую из 10 или 12 компьютеров, может контролировать (визуально) один человек, тогда как для надлежащего мониторинга большой сети или ГВС (глобальной сети) потребуется специальный персонал и соответствующее оборудование. Один из методов обеспечить безотказную работу сети - ежедневно наблюдать за определенными аспектами ее функционирования. Постоянно контролируя сеть, Вы сможете вовремя заметить снижение производительности на любых участках сети.

Узкие места

Большинство сетевых операций складывается из совместных действий несколько устройств. Каждое устройство на выполнение своей части операции требует некоторого го времени. Если какое-либо устройство использует заметно больше проще времени по сравнению с другими, возникают проблемы с производительностью системы в целом. Такое «тормозящее» устройство обычно называют «узким месте». Основная задача мониторинга производительности — выявить и устранить узкие места. Чтобы решать проблемы узких мест (bottleneck),

администратор должен возможность найти сетевые устройства, которые, выполняя свои задачи, расходуют больше времени, чем это допустимо.

Следующие устройства сервера чаще всего являются узкими местами:

- процессоры;
- память;
- сетевые платы;
- контроллеры дисков;
- среда передачи.

Причины, которые приводят к тому, что устройство становится узким местом;

- устройство используется неэффективно;
- устройство работает слишком медленно;
- мощность устройства недостаточна, чтобы выполнять все возлагаемые на него задачи.

Хороший мониторинг распознает эти недостатки и выдает Вам нформацию, которая облегчает поиск проблемного компонента (или компонентов).

Windows NT Performance Monitor

Большинство современных сетевых операционных систем имеет утилиты мониторинга, которые помогают администратору контролировать различные аспекты функционирования сервера. Windows NT Server, например, имеет утилиту под названием Performance Она помогает администратору сети наблюдать и в реальном времени, и в записи:

- за деятельностью процессоров;
- работой жестких дисков;
- использованием памяти;
- использованием сети;

Winows NT Performance Monitor может выполнять следующие действия:

- записывать информацию о производительности сети;

- посылать предупреждение администратору сети;
- запускать другую программу, которая вернет систему в приемлемое состояние.

Используя такие средства, как Performance Monitor, прежде всего установите основные параметры, при которых система функционирует наиболее эффективно. Регистрируя значения этих параметров, Вы сможете составить некоторое представление об удовлетворительных хазрительных характеристиках системы. Теперь у Вас есть основа для сравнения (если что-нибудь изменится либо потребует модернизации или замены). Без базовы характеристик определение и поддержание необходимого уровня производительности - задача сложная.

Простой протокол управления сетью

Программное обеспечение управления сетью, как и большинство сетевых компонентов, подчиняется стандартам, созданным производителями сетевого оборудования. Один из этих стандартов - простой протокол управления сетью (Simple Management Protocol, SNMP). При использовании SNMP программы, называемые агентами, загружаются на каждое управляемое устройство. Агенты собирают статистические данные, контролируя сетевой трафик и функционирование этих ключевых компонентов сети. Собранные сведения хранятся в базе данных управленческой информации (Ma Information Base, MIB).

К компонентам SNMP относятся:

- концентраторы;
- серверы;
- интерфейсные платы;
- маршрутизаторы и мосты;
- другое специальное сетевое оборудование.

Для накопления информации специальная программа (консоль управления) регулярно опрашивает этих агентов и загружает информацию

из их MIB. После накопления необработанных данных программа управления может выполнить еще две задачи:

- представить информацию в форме графиков, схем и диаграмм;
- переслать информацию в указанную базу данных для последующего анализа.

Если любой показатель выйдет за пределы, установленные администратором, чма управления может известить администратора, выдав предупреждение на компьютера или отправив его на пейджер. Затем с помощью консоли управления персонал поддержки может произвести изменения в сети (зависит от компонента).

Полное управление системой

За последнее время размер и сложность сетей резко возросли, поэтому всеобъемлющий контролъ за ними стал более дорогим. В связи с этим производители разработали программы, которые для системного управления делают то же, что для мониторинга систем делают программы контроля производительности. Примером одного из этих прложений - управления целыми системами - является Microsoft Systems Management Server (SMS), программа централизованного управления распределенными системами.

Systems Management Server обеспечивает централизованное администрирование компьютеров в распределенных сетях, а именно: инвентаризацию программного и аппаратного обеспечения;
распространение и установку программного обеспечения;
совместное использование сетевых приложений;
выявлвление причин, которые вызывают проблемы в программном и аппаратном обеспечении.

Systems Management Server дополняет другие приложения системного управления (такие, как User Manager, Registry Editor, Event Viewer и Server Manager), поставляемые с операционными системами Microsoft.

Systems Management Server выполняет следующие функции.

Управляет инвентаризацией.

Systems Management Server делает и сохраняет опись аппаратного и программного обесеспечения каждого компьютера. Опись хранится в базе данных SQL Server. Типичная опись должна отразить тип процессора, количество оперативной памяти, размер жесткого диска, тип операционной системы и список прикладного программного беспечения.

Распространяет программное обеспечение.

Как только опись компьютера будет внесена в базу данных, Systems Management Server непосредственно на клиенте может установить и сконфигурировать новое программное обеспечение или обновить ранее установленные программы. Этот механизм пространения применяется также на компьютерах-клиентах при выполнении команд например, для поиска вирусов.

Управляет совместно используемыми приложениями.

Совместно используемые приложения могут устанавливаться и на сервер, чтобы клиенты могли получить к ним доступ. Когда пользователь входит в сеть, Syster Menegement Server создает на компьютере-клиенте группу программ и добавляет значок для каждого приложения, доступного пользователю. Чтобы запустить совместно изпользуемое приложение, выберите значок из локальной группы программ (однакоимейте в виду: приложение хранится на жестком диске сервера).

Осуществляет удаленное управление и мониторинг сети.

Systems Management Server содержит Help Desk и средства диагностики, которые позволяют управлять удаленными клиентами. В частности, с помощью диагностических утилит Вы сможете просматривать текущую конфигурацию клиентов, а утилиты Help Desk беспечивают непосредственный доступ к удаленному клиенту. Systems Management Server содержит также Microsoft Network Monitor, с помощью которого Вы

сможете анализировать сетевой трафик и находить проблемные участки в Вашей сети.

Документация сети

Отрожать историю сети так же важно, как проводить мониторинг производительности времени. Исследуя работу сети с момента ее создания, Вы сможете:

- выявить глобальные проблемы с оборудованием или производительностью, которые могут быть не замечены при мониторинге в реальном времени;
- установить базовые данные, с которыми будет сравниваться текущая информация.

Резюме

При управлении сетью приходится решать много задач. Одна из наиболее важных среди них-управление производительностью сети. Проводя мониторинг сети, администратор выявляет, во-первых, ее узкие места и, во-вторых, способы увеличения ее производительности. Мониторинг производительности помогает также в планировании и прогнозировании потребностей сети. Чаще всего узкими местами становятся процессор, память, платы сетевых интерфейсов и контроллеры дисков.

Microsoft предоставляет два инструментальных средства, которые помогают администратору в выполнении этих задач. Performance Monitor (входит в комплект постановки Windows NT Server) обеспечивает мониторинг сетевых операций в реальном времени записи. Systems Management Server (приобретается отдельно) оказывает поддержку в более широком диапазоне задач по централизованному управлению всеми компьютерами в распределенной сети.

Важный компонент управления сетью -протокол функционирования сети. История сети является бесценным справочником при решении многих сетевых проблем.

Контрольные вопросы.

1. Задачи и обязанности администратора?
2. Типы учётных записей?
3. Какие пароли вы знаете?
4. Группы?
5. Мониторинг производительности сети?
6. Проблемы защиты сети?
7. Какие две основные модели обеспечения безопассности данных и методов зазщиты физическтх компонентов сети вы знаете?
8. Перечислите дополнительные средства защиты вы знаете?
9. Возможные причины потери данных?
10. Системы и процессы, предпреждения потерю данных.

Ключевые слова.

Администратор;

пароль;

архивирование;

модернизация;

утилиты;

профили;

гость;

оператор;

мониторинг;

конфигурация.

Лекция №17

Защита информации.

План:

Планирование зазщиты сети.

Разработка политики защиты.

Упреждающая защита.

Физическая защита оборудования.

Защита серверов.

Защита кабеля.

Пароль доступа к ресурсу.

Рузюме.

Планирование защиты сети

Работая в сетевой среде, Вы должны быть уверены в том, что секретные данные таковыми и останутся, поскольку лишь пользователи, которые имеют соответствующие полномочия, смогут получить к ним доступ. Однако важно обеспечить защиту не только конфиденциальной информации, но и функционирования сети в целом.

Каждая сеть нуждается в защите от преднамеренного или случайного повреждения. В то же время хороший администратор сети всегда помнит, что при обеспечение безопасности надо знать меру, надо строить защиту таким образом, чтобы люди не испытывали трудности при выполнении своей работы. Короче говоря, пользователи не должны приходить в отчаяние, пытаясь получить доступ к собственным файлам.

Несмотря на то что сети обрабатывают и весьма деликатную, и ценную деловую информацию, об ее защите часто думают в последнюю очередь. Наиболбшю угрозу для безопасности сети представляют:

- несанкционированный доступ;
- электронное подслушивание;
- кража;

- преднамеренное или неумышленное повреждение.

Задача администратора - гарантировать, что сеть будет надежным и безопасным инструментом для ведения бизнеса.

Разработка политики защиты

Для защиты сети необходимо проводить определенную политику, т.е. следовать набору праил и предписаний, - ничто нельзя отдавать на волю случая.

Выработка политики безопасности (security policy) - первый шаг, который должна сделать любая организация, обеспечивая защиту своих данных. Политика устанавливает «генеральную линию», опираясь на которую и администратор, и пользователи вносить изменения, находить выход из нештатных ситуаций при развитии сети, разработка и принятие политики безопасности - важнейший шаг к успешному использованию сети.

Упреждающая защита

Лучшая политика защиты данных имеет предупредительный характер. Предотвращая несанкционированный доступ или действия, Вы сохраните информацию. Однако система основанная на упреждении, требует, чтобы администратор в совершенстве владел средствами и методами, которые помогают сохранить данные в безопасности.

Аутентификация

Перед тем как получить доступ к сети, Вы должны ввести правильные имя пользователя и пароль. Поскольку пароли связаны с учетными записями пользователей, система идентификации паролей является Вашей первой линией обороны против несанкцированного доступа.

Физическая защита оборудования

Обеспечение безопасности данных надо начинать с физической зашиты обордования. На степень физической защиты влияют:

- размер компании;
- характер информации;
- доступные ресурсы.

В одноранговых системах организованная политика защиты оборудования отсутствует, так как пользователи сами отвечают за безопасность своих компьютеров и данных.

Защита серверов

В больших централизованных системах, где число индивидуальных пользователей достаточно велико, а данные компании имеют важное значение, серверы должны быть физически защищены от случайного или преднамеренного вмешательства.

При возникновении проблем с серверами в каждой группе пользователей всегда найдутся желающие продемонстрировать свои технические способности. Одни могут знать, что делают, а другие и нет. Поэтому самое лучшее — тактично уj людей от самостоятельного «исправления» сервера.

Простейшее решение — запереть серверы в специальном помеше-ченным доступом. Но не все организации имеют такую возможность. А серверы хотя бы в кабинете или в большом шкафу смогут все.

Защита кабеля

Медный кабель, например коаксиальный, подобен радиостанции: он излучает электромагнитные сигналы, которые содержат информацию о передаваемых данных. Эту информацию с помощью специального оборудования легко перехватить.

Кроме того, к медному кабелю можно подключиться и похитить информацию непосредственно из сетевого кабеля. Поэтому доступ к

кабельным трассам, по которым передаются важные данные, должен быть ограничен либо узким кругом уролномоченных на работу с кабелем лиц, либо прокладкой его внутри строительных конструкций (в перекрытиях и стенах).

Модели защиты

Защитив физические компоненты сети, администратор должен гарантировать сетевые ресурсы находятся в безопасности от несанкционированного доступа случайного или преднамеренного уничтожения. Политика назначенияпривилегий и прав на доступ к сетевым ресурсам - основа для превращения сети в инструментах успешного ведения бизнеса.

Сейчас широко применяются две модели, которые обеспечивают безопастость информационных и аппаратных ресурсов:

- защита через пароль;
- защита через права доступа.

Эти модели называют также защитой на уровне совместно используемых ресурсов (recource level) (защита через пароль) и защитой на уровне пользователя (user level) (защита через права доступа).

Пароль доступа к ресурсу

Один из методов защиты совместно используемых ресурсов - присвоить пароль каждому общедоступному ресурсу. Таким образом, доступ к ресурсу осуществляется только в том случае, когда пользователь вводит правильный пароль.

Во многих системах ресурсы могут быть предоставлены в совместное использование разными типами прав доступа. В Windows 95, например, к каталогам может быть доступ только для чтения, полный доступ и доступ в зависимости от пароля.

Доступ только для чтения (read only).

Если совместно используемый каталог предоставлен только для чтения, сотрудники, знающие пароль, будут читать в нем все файлы. Они

могут просматривать документы, копировать их на свою машину, печатать, но не могут изменять исходный документ.

Полный доступ (full access).

В случае полного доступа к файлам в совместно используемом каталоге сотрудники, знающие пароль, могут просматривать, модифицировать и удалять в нем любые файлы.

Доступ в зависимости от пароля (depending on password).

Доступ в зависимости от пароля заключается в следующем. Совместно используемому каталогу присваивается пароль двух уровней: доступ только для чтения и полный доступ. Сотрудники, знающие пароль доступа для чтения, могут лишь читать данные, а те, кто знает пароль полного доступа, имеют соответственно полный доступ.

Защита совместно используемых ресурсов паролем — самый простой метод защиты который позволяет любому, кто знает пароль, получить доступ к нужному ресурсу.

Права доступа

Защита через права доступа заключается в присвоении каждому пользователю определенного набора прав. При входе в сеть пользователь вводит пароль. Сервер, проверяя комбинацию имени пользователя и пароля, т.е. проверяя права пользователя в базе данных безопасности, предоставляет или запрещает доступ к сетевым ресурсам. Защита с применением прав доступа обеспечивает более высокий уровень управления доступом к совместно используемым ресурсам, а также более строгий режим безопастности, чем защита паролем. Имея защиту на уровне совместно используемых ресурсов, любой человек может с легкостью передать другому, например, пароль доступа к принтеру. Гораздо менее вероятно, что этот пользователь сообщит кому-нибудь свой персональный пароль.

Так как защита на уровне пользователя более эффективна и может определять различные уровни безопасности, большие организации обычно отдают предпочтение именно этой модели.

Резюме

Планирование сети включает и планирование ее защиты. Необходимый уровень защиты от разных факторов, в том числе от размера фирмы и характера передаваемых данных. Администратор должен оценить потребности сети и выработать политику безопасности.

Существует две модели защиты - защита совместно используемых ресурсов паролем и защита через права доступа. Многие компании применяют обе модели. Защита паролемем сфокусирована на совместно используемых ресурсах. Для доступа к конкретному ресурсу пользователь должен ввести пароль. Защита через права доступа основана на присвоении пользователям некоторого набора прав. При входе в сеть пользователь вводит комбинацию имени и пароля. Эти параметры определяют доступность сетевых ресурсов.

Наиболее эффективный метод присвоения прав -создать группы. Администратор наделяет конкретными правами целые группы пользователей, а не отдельных пользователей.

Дополнительные средства защиты - аудит, бездисковые компьютеры, шифрование данных и защита от вирусов.

Контрольные вопросы.

1. Проблемы защиты сети?
2. Перечислите две основные модели обеспечения данных и методов защиты физических компонентов сети.
3. Физическая защита оборудования?
4. Дополнительные средства защиты?
5. Что такое аудит?
6. Перечислите модли защиты ?
7. что такое права доступа?

Ключевые слова.

Несанкицированный доступ;

электронное подслушивание;

кража;

аутентификация;

аудит;

блокировка;

модификация;

шифрования.

Лекция № 18.

Предупреждение потери данн

План:

Защита данных.

Резервное копирование на магнитную ленту.

Система резервного копирования.

Тестирование и хранение.

Установка системы резервного копирования.

Источник бесперебойного питания.

Уровни.

Резюме.

Защита данных

К числу бедствий можно отнести все, что влечет за собой потерю данных в сети. При чины бедствий самые разнообразные: от дел рук человеческих до природных катаклизмов, в том числе:

- воровство или вандализм;
- пожар;
- отказы источников питания и скачки напряжения;
- отказы компонентов;
- природные явления, такие, как молнии, наводнения, бури и землетрясении
- Остановка сети, вызванная чрезвычайными причинами, всегда бедствие, всегда серьёзное уменьшение производительности. Требуется время на восстановление данных хранилища резервных копий (если у Вас есть резервные копии). Без них последвия будут самыми непредсказуемыми, с огромными финансовыми потерями. Существуют методы и системы, предупреждающие катастрофическую потерю данных:
- резервное копирование на магнитную ленту;

- источники бесперебойного питания (UPS);
- отказоустойчивые системы.

Могут использоваться все эти системы или любая из них, в зависимости от ценности данных и бюджета организации.

Резервное копирование на магнитную ленту

Наиболее простой и недорогой метод предупредить катастрофическую потерю данных-периодическое резервное копирование с последующим хранением копий за пределами организации. Это один из немногих способов гарантировать, что данные остаются в безопасности и пригодны для использования.

Опытные сетевые инженеры знают, что система резервного копирования – первая линия обороны. Надежная стратегия резервирования сводит к минимуму риск потери данных, поддерживая текущую резервную копию в таком состоянии, при котором файлы легко восстанавливаются в случае повреждения оригинальных данных.

Чтобы проводить резервное копирование, необходимо иметь:

- оборудование;
- расписание;
- сотрудника, чья обязанность - реализовать расписание на практике.

Под оборудованием обычно подразумевается один или несколько накопителей на магитной ленте с комплектом лент (или другое устройство массового хранения данных). Любые расходы в этой области могут оказаться мизерными по сравнению с теми финансовыми потерями, которые вызовет разрушение данных.

Система резервного копирования

Общее правило гласит: если Вы не можете в дальнейшем обойтись без чего-то, сделайте его резервную копию. Выбор объектов для резервного копирования - целые диски, отдельные каталоги или файлы - зависит от того, насколько быстро нужно продолжить работу после потери

важных данных, восстановив их. Полное резервное копирование может ускорить восстановление конфигурации диска, однако, если имеются большие объемы данных, требует значительного числа дополнительных магнитных лент. Резервирование отдельных файлов и каталогов потребует меньше лент, однако администратору придется вручную восстанавливать конфигурацию диска.

Критические данные должны резервироваться ежедневно, еженедельно или ежемесячно в зависимости от степени их важности и от того, насколько часто они обновляются. Самое лучшее время для резервного копирования - время наименьшей загрузки системы. Сообщите пользователям, когда будет выполняться резервное копирование, чтобы они не обращались к серверу в этот период.

Тестирование и хранение

Квалифицированные администраторы всегда проверяют систему резервного копирования перед тем, как запустить ее в эксплуатацию. Они выполняют резервное копирование, удаляют информацию, восстанавливают данные, а затем пробуют их использовать.

Администратор должен регулярно тестировать все процедуры резервного копирования, чтобы быть уверенным: все, что должно резервироваться, в действительности резервируется. Чтобы гарантировать быстрое восстановление важных файлов, необходимо также проверять процедуры восстановления.

- В идеале администратор должен делать две копии каждой ленты. Одну он должен хранить на работе, а другую - за пределами организации в безопасном месте. Помните: хранение лент в несгораемом сейфе может уберечь их от пламени, однако высокая температура скорее всего разрушит записанные данные.

Установка системы резервного копирования

Накопители на магнитной ленте могут быть подключены к серверу или к любому компьютеру, причем резервное копирование инициируется с того компьютера, к которому подсоединен накопитель. Если резервное копирование выполняется непосредственно на сервере, операции резервирования и восстановления протекают намного быстрее, так как отсутствует передача данных по сети.

Резервное копирование через сеть - наиболее удобный метод резервирования для множества систем, однако при этом создается значительный сетевой трафик и увеличивается время отклика сети. Сетевой трафик, кроме того, вызывает уменьшение производительности. Это одна из причин, почему так важно проводить резервное копирование во время наименьшей загрузки сервера.

Если несколько серверов расположены компактно, можно уменьшить трафик, вызванный резервным копированием, - поместите в изолированный сегмент компьютер, с которого выполняется резервирование. Этот компьютер подключают к отдельной сетевой плате каждого сервера.

Источник бесперебойного питания

Источник бесперебойного питания (UPS) - это автоматический внешний источник энергии, который поддерживает работоспособность сервера или других устройств в случае сбоев электрической сети. Системы бесперебойного питания используют способность источников бесперебойного питания взаимодействовать с операционной системой, например с Microsoft Windows NT, через специальный интерфейс. Стандартная система бесперебойного питания обеспечивает две важнейшие для сети функции:

- *питание сервера в течение некоторого времени;
- *управление безопасным завершением работы системы.

Источником энергии обычно служат аккумуляторы, однако UPS может быть и ротационной системой, запасающей энергию с помощью большого маховика и двигателем внутреннего сгорания, вращающим генератор переменного тока.

При нарушении питания UPS извещает пользователей о сбое и предупреждает их о необходимости завершить работу. Затем, выждав предопределенный времени, UPS организованно закрывает систему.

При этом хорошо организованная система бесперебойного питания будет предотвращать доступ к серверу дополнительных пользователей, а также пошлет администратору сети сообщение об аварии.

- Отказоустойчивые системы

Отказоустойчивые системы защищают данные, дублируя и размещая их на различных физических носителях (например,на разных дисках). Избыточность (redundancy) данных позволяет осуществлять к ним доступ даже в случае выхода из строя части системы. Избыточность - общий отличительный признак большинства отказоустойчивых систем.

Тем не менее отказоустойчивые системы нельзя использовать как замену регулярного резервного копирование серверов и локальных жестких дисков. Тщательно спланированная стратегия резервного копирования является лучшей страховкой от потери или уничтожения данных.

Отказоустойчивые системы предлагают следующие варианты для обеспечения избыточности данных:

- чередование дисков;
- зеркализацию дисков;
- замену секторов.
-

Уровень 0 — чередование дисков

При чередовании дисков (disk striping) данные делятся на блоки размером 64 кБайт и равномерно распределяются по всем дискам массива. Однако чередование дисков не обеспечивает повышенной надежности, так как не создает избыточности данных. При повреждении любого раздела будут потеряны все данные. Чередование дисков объединяет множество областей неформатированного свободного пространства в один большой логический диск, распределяя хранилище данных по всем дискам одновременно. В Windows NT для чередования дисков необходимо как минимум два физических диска (максимальное число — 32 диска). При чередовании дисков можно использовать разделы дисков нескольких типов: SCSI, ESDI и IDE.

Чередование дисков имеет ряд преимуществ. Во-первых, несколько малых разделов образуют один большой раздел, благодаря чему лучше используется дисковое пространство. Во-вторых, применяя несколько дисковых контроллеров, можно резко увеличить производительность.

Уровень1 - зеркализация дисков

Зеркализация дисков (disk mirroring) - дублирование раздела и запись его копии на другом физическом диске . Поэтому всегда есть две копии данных, причем каждая – на отдельном диске. Любой раздел может быть зеркализирован. Эта стратегия – простейший метод защиты одиночного диска от сбоев. Зеркализация дисков выступает как форма непрерывного резервного копирования , так как при этом поддерживается полная копия раздела с другого диска.

Уровень 2 - чередование дисков с записью кода коррекции ошибок

Блок данных - при записи - делится на части, распределяемые по разным дискам. Одновременно генерируется код коррекции ошибок (ECC), который также записывается на разных дисках. Для кода коррекции

ошибок требуется больше дискового пространства, чем при методе с контролем четности. Хотя последний гораздо эффективней использует дисковое пространство, он уступает в этом отношении уровню 5.

Уровень 3 — код коррекции ошибок в виде четности

Чередование дисков с использованием кода коррекции ошибок, хранящимся в виде четности, подобно уровню 2. Контролем четности называют процедуру проверки ошибок, при которой устанавливается количество единиц в каждой переданной группе битов. Оно должно быть одинаковым - четным или нечетным. В этом случае говорят: данные переданы без ошибок. При этой стратегии метод с кодами ECC заменяется схемой контроля четности, которой необходим только один диск для хранения информации контроля четности. Это приводит к тому, что примерно 85 % дискового пространства используется для хранения непосредственно данных.

Уровень 4 — чередование дисков большими блоками

Эта стратегия, основанная на методе чередования дисков, обеспечивает запись целевых блоков данных на каждый диск в массиве. Отдельный контрольный диск используется для хранения информации о четности. При каждой записи соответствующая информация о четности должна быть прочитана с контрольного диска и модифицирована. Из-за высоких накладных расходов этот метод больше подходит для операций крупными блоками, чем для обработки транзакций.

Уровень 5 — чередование с контролем четности

В настоящее время чередование с контролем четности - наиболее популярный метод построения отказоустойчивых систем. Уровень 5 поддерживает от 3 до 32 дисков и распределяет информацию о четности по всем дискам массива (по всему набору чередования). Данные и информация об их четности всегда размещаются на разных дисках.

Блок информации о четности записывается в каждой полосе (ряде) чередования,распределенной по дискам. Информация о четности помогает

восстановить данные с отказавшего физического диска. Если отказал один диск, для полного восстановления данных достаточно информации, распределенной по оставшимся дискам. RAID4 хранит блок четности на одном физическом диске, тогда как RAID 5 распределяет информацию о четности равномерно по всем дискам.

Резюме

Существует несколько стратегий, способных предотвратить потерю данных при различных бедствиях. Главные среди них - резервное копирование, испольпользование источников бесперебойного питания и отказоустойчивых систем. Администоры должны оценить потребности своих сетей и выбрать соответствующие средства.

Стандартный метод предупреждения потерь данных – регулярное использование накопителей на магнитной ленте для резервного копирования файлов. Известны различные методы резервного копирования. Необходимо вести журнал резервного копирования.

Источник бесперебойного питания — это внешний источник питания, который поддерживает функционирование сервера или других сетевых устройств при сбое во внешней сети. Источником энергии может служить аккумуляторная батарея, ротационная система и т.д.

Отказоустойчивые системы дублируют данные и размешают их на разлиных физических носителях. Эти системы дополняют резервное копирование. Большинство стратегий обеспечения отказоустойчивости классифицируется в системе RAID, включая чередование и зеркализацию дисков. Некоторые современные сетевые операционные системы используют замену секторов. А такие сетевые операционные системы, как Windows NT Server, имеют утилиты для управления механизмами отказоустойчивости.

Контрольные вопросы.

1. Какие причины потери данных ы знаете?
2. Системы и процессы, предупреждения потерю данных вы знаете?
3. Тестирование и хранение?
4. Установка системы резервного копирования?
5. Источник бесперебойного питания?
6. Перечислите уровни чередование дисков?

Ключевые слова.

Оборудование;

сотрудник;

сегмент;

чередование дисков;

зеркализация дисков;

коррекция;

дефект;

сектор.

СОДЕРЖАНИЕ