**РЕФЕРАТ**

Объект исследований: Служба по делам детей Северодонецкого городского совета.

Предмет исследования: локальная сеть Службы по делам детей Северодонецкого городского совета.

В первом разделе рассмотрены общие принципы построения локальных сетей, рассмотрена модель эталонная сетевая модель OSI, дана характеристика базовым технологиям ЛВС, сделан обзор типов соединительных линий.

Во втором разделе выполнен анализ предметной области, выбор конфигурации вычислительной сети, спроектирована структурная схема вычислительной сети и схема прокладки кабеля, выполнено планирование комплекса мер по администрированию и поиску неисправностей сети.

В третьем разделе выполнен экономический расчет объекта анализа, а именно расчет на создание проекта ЛВС, расчет материальных затрат, использование ЭВМ, расчет технологической себестоимости ЛВС, расчет капитальных затрат на создание и эксплуатацию ЛВС и экономический эффект от использования ЛВС на данном предприятии.

В четвертом разделе проведены расчеты отопления, вентиляции, природного и искусственного освещения, полученные значения сопоставлены с нормативными.

ЛОКАЛЬНАЯ СЕТЬ, АДМИНИСТРАТОР, РАБОЧАЯ СТАНЦИЯ, СЕРВЕР, АНАЛИЗАТОРЫ, ДИАГНОСТИКА, ТЕСТЕР

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ

1. ОСНОВЫ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ

1.1 Архитектурные принципы построения компьютерных сетей

1.2 Среда передачи данных

1.3 Базовые технологии построения локальных сетей

2. АНАЛИЗ И КОМПЛЕКС МЕРОПРИЯТИЙ ПО ОБСЛУЖИВАНИЮ ЛОКАЛЬНОЙ СЕТИ СЛУЖБЫ ПО ДЕЛАМ ДЕТЕЙ СЕВЕРОДОНЕЦКОЙ ГОРОДСКОГО СОВЕТА

2.1 Административные, технические и программные характеристики Службы по делам детей Северодонецкой городского совета

2.2 Анализ локальной компьютерной сети Службы по делам детей Северодонецкого городкого совета

2.3 Описание комплекса мероприятий по обслуживанию сети

2.3.1 Администрирование локальных сетей

2.3.2 Средства выявления неисправностей

3. ЭКОНОМИЧЕСКИЙ РАСЧЕТ СТОИМОСТИ ОБЪЕКТА АНАЛИЗА

3.1 Расчет затрат на создание проекта ЛВС

3.2 Расчет материальных затрат

3.3 Использование сетевого оборудования

3.4 Расчет технологической себестоимости ЛВС

3.5 Расчет капитальных затрат на создание ЛВС

3.6 Затраты при эксплуатации ЛВС

3.7 Расчет экономического эффекта на создание и эксплуатацию ЛВС

4. ОХРАНА ТРУДА

4.1 Организация рабочего места

4.2 Организация и расчет отопления

4.3 Расчет вентиляции

4.4 Расчет искусственного освещения помещений

4.5 Расчет природного освещения помещений

ВЫВОДЫ

ПРИЛОЖЕНИЕ А. Сравнительный анализ базовых технологий постоения локальных сетей

**1. ОСНОВЫ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ**

* 1. **Архитектурные принципы построения компьютерных сетей**

Сеть – это соединение разного оборудования, а значит, проблема совместимости является одной из наиболее острых. Без принятия всеми производителями общепринятых правил построения оборудования прогресс в деле «строительства» сетей был бы невозможен. Поэтому все развитие компьютерной отрасли в конечном счете отражено в стандартах.

В компьютерных сетях идеологической основной стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода была разработана стандартная семиуровневая модель взаимодействия открытых систем, ставшая своего рода универсальным языком сетевых специалистов.

Организация взаимодействия между устройствами в сети является сложной задачей. Как известно, для решения сложных задач используется универсальный прием – декомпозиция, то есть разбиение одной сложной задачи на несколько более простых задач-модулей. Процедура декомпозиции включает в себя четкое определение функций каждого модуля, решающего отдельную задачу, и интерфейсов между ними.

При декомпозиции часто используется многоуровневый подход. Он заключается в следующем. Все множество модулей разбиваются на уровни. Уровни образуют иерархию, то есть имеются вышележащие и нижележащие уровни. Множество модулей, составляющих каждый уровень, сформировано таким образом, что для выполнения своих задач они обращаются с запросами только к модулям непосредственно примыкающего нижележащего уровня. С другой стороны, результаты работы всех модулей, принадлежащих некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция задачи предполагает четкое определение функции каждого уровня и интерфейсов между уровнями. Интерфейс определяет набор функций, которые нижележащий уровень предоставляет вышележащему. В результате иерархической декомпозиции достигается относительная независимость уровней, а значит, и возможность их легкой замены.

Формальные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называются протоколом. Модули, реализующие протоколы соседних уровней и находящихся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть интерфейсом. Интерфейс определяет набор сервисов, предоставляемый данным уровнем соседнему уровню. В сущности, протокол и интерфейс выражают одно и тоже понятие, но традиционно в сетях за ними закрепили разные области действия: протоколы определяют правила взаимодействия модулей одного уровня в разных узлах, а интерфейсы – модулей соседних уровней в одном узле.

Имея дело с 2-мя протоколами, и каждый из них имеет собственный протокол, который может быть изменен, не зависимо от протокола другого уровня. Эта независимость протоколов друг от друга и делает привлекательным многоуровневый подход.

В начале 80-х годов ряд международных организаций по стандартизации (ISO, ITU-T и некоторые другие) разработали модель, которая сыграла значительную роль в развитии сетей. Эта модель называется моделью взаимодействия открытых систем или моделью OSI. Модель OSI определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

В модели OSI средства взаимодействия делятся на 7 уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с одним определенным аспектом взаимодействия сетевых устройств.

Модель OSI описывает только системные средства взаимодействия, реализуемые операционной системой, системными утилитами, системными аппаратными средствами. Модель не включает средства взаимодействия приложений конечных пользователей.

Самый нижний уровень модели предназначен непосредственно для передачи потока данных. Осуществляет передачу электрических или оптических сигналов в кабель или в радиоэфир и, соответственно, их приём и преобразование в биты данных в соответствии с методами кодирования цифровых сигналов. Другими словами, осуществляет интерфейс между сетевым носителем и сетевым устройством.

На этом уровне работают концентраторы (хабы), повторители (ретрансляторы) сигнала и медиаконверторы.

Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом. К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами. Физический уровень определяет такие свойства среды сети передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передач данных и т. п.

Канальный уровень предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля за ошибками, которые могут возникнуть. Полученные с физического уровня данные он упаковывает во фреймы, проверяет на целостность, если нужно исправляет ошибки (посылает повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием. На этом уровне работают коммутаторы, мосты.

В программировании этот уровень представляет драйвер сетевой платы, в операционных системах имеется программный интерфейс взаимодействия канального и сетевого уровней между собой, это не новый уровень, а просто реализация модели для конкретной ОС. Примеры таких интерфейсов: ODI, NDIS.

3-й уровень (сетевой уровень) модели OSI предназначен для определения пути передачи данных, отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и заторов в сети. На этом уровне работает такое сетевое устройство, как маршрутизатор.

Протоколы сетевого уровня маршрутизируют данные от источника к получателю и могут быть разделены на два класса: протоколы с установкой соединения и без него.

Описать работу протоколов с установкой соединения можно на примере работы обычного телефона. Протоколы этого класса начинают передачу данных с вызова или установки маршрута следования пакетов от источника к получателю. После чего начинают последовательную передачу данных и затем по окончании передачи разрывают связь.

Транспортный уровень модели предназначен для доставки данных без ошибок, потерь и дублирования в той последовательности, как они были переданы. При этом не важно, какие данные передаются, откуда и куда, то есть он предоставляет сам механизм передачи. Блоки данных он разделяет на фрагменты, размер которых зависит от протокола, короткие объединяет в один, а длинные разбивает. Протоколы этого уровня предназначены для взаимодействия типа точка-точка. Пример: TCP, UDP.

Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приема), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных.

Некоторые протоколы сетевого уровня, называемые протоколами без установки соединения, не гарантируют, что данные доставляются по назначению в том порядке, в котором они были посланы устройством-источником. Некоторые транспортные уровни справляются с этим, собирая данные в нужной последовательности до передачи их на сеансовый уровень. Мультиплексирование данных означает, что транспортный уровень способен одновременно обрабатывать несколько потоков данных (потоки могут поступать и от различных приложений) между двумя системами. Механизм управления потоком данных — это механизм, позволяющий регулировать количество данных, передаваемых от одной системы к другой. Протоколы транспортного уровня часто имеют функцию контроля доставки данных, заставляя принимающую данные систему отправлять подтверждения передающей стороне о приеме данных.

Сеансовый уровень модели отвечает за поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды не активности приложений. Синхронизация передачи обеспечивается помещением в поток данных контрольных точек, начиная с которых возобновляется процесс при нарушении взаимодействия.

Представительский уровень отвечает за преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с уровня приложений, он преобразует в формат для передачи по сети, а полученные из сети данные преобразует в формат, понятный приложениям. На этом уровне может осуществляться сжатие/распаковка или кодирование/декодирование данных, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

Данный уровень обычно представляет собой промежуточный протокол для преобразования информации из соседних уровней. Это позволяет осуществлять обмен между приложениями на разнородных компьютерных системах прозрачным для приложений образом. Уровень представлений обеспечивает форматирование и преобразование кода. Форматирование кода используется для того, чтобы гарантировать приложению поступление информации для обработки, которая имела бы для него смысл. При необходимости этот уровень может выполнять перевод из одного формата данных в другой. Уровень представлений имеет дело не только с форматами и представлением данных, он также занимается структурами данных, которые используются программами. Таким образом, уровень 6 обеспечивает организацию данных при их пересылке.

Прикладной уровень, верхний уровень модели, обеспечивает взаимодействие сети и пользователя. Уровень разрешает приложениям пользователя иметь доступ к сетевым службам, таким как обработчик запросов к базам данных, доступ к файлам, пересылке электронной почты. Также отвечает за передачу служебной информации, предоставляет приложениям информацию об ошибках и формирует запросы к уровню представления.

Модель OSI представляет хотя и очень важную, но только одну из многих моделей коммуникаций. Эта модель и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, службами, поддерживаемыми на верхних уровнях, и прочими параметрами.

**1.2 Среда передачи данных**

На сегодняшний день подавляющая часть компьютерных сетей использует для соединения провода или кабели. Они выступают в качестве среды передачи сигналов между компьютерами. Существуют различные типы кабелей, которые удовлетворяют потребности всевозможных сетей, от малых до больших.

В широком ассортименте кабелей нетрудно запутаться. Так, фирма Belden, ведущий производитель кабелей, публикует каталог, где предлагает более 2200 их типов. К счастью, в большинстве сетей применяются только три основные группы кабелей: коаксиальный кабель, витая пара (неэкранированная, экранированная) и оптоволоконный кабель.

Не так давно коаксиальный кабель был самым распространенным типом кабеля. Это объяснялось двумя причинами. Во-первых, он был относительно недорогим, легким, гибким и удобным в применении. А во-вторых, широкая популярность коаксиального кабеля привела к тому, что он стал безопасным и простым в установке.

Самый простой коаксиальный кабель состоит из медной жилы (core), изоляции, ее окружающей, экрана в виде металлической оплетки и внешней оболочки. Если кабель, кроме металлической оплетки, имеет и слой фольги, он называется кабелем с двойной экранизацией. При наличии сильных помех можно воспользоваться кабелем с учетверенной экранизацией. Он состоит из двойного слоя фольги и двойного слоя металлической оплетки.

Некоторые типы кабелей покрывает металлическая сетка — экран (shield). Он защищает передаваемые по кабелю данные, поглощая внешние электромагнитные сигналы, называемые помехами или шумом. Таким образом, экран не позволяет помехам исказить данные.

Электрические сигналы, кодирующие данные, передаются по жиле. Жила — это один провод (сплошная) или пучок проводов. Сплошная жила изготавливается, как правило, из меди.

Жила окружена изоляционным слоем, который отделяет ее от металлической оплетки. Оплетка играет роль заземления и защищает жилу от электрических шумов (noise) и перекрестных помех (crosstalk). Перекрестные помехи — это электрические наводки, вызванные сигналами в соседних проводах.

Проводящая жила и металлическая оплетка не должны соприкасаться, иначе произойдет короткое замыкание, помехи проникнут в жилу, и данные разрушатся. Снаружи кабель покрыт непроводящим слоем — из резины, тефлона или пластика.

Коаксиальный кабель более помехоустойчив, затухание сигнала в нем меньше, чем в витой паре. Затухание (attenuation) — это уменьшение величины сигнала при его перемещении по кабелю.

Как уже говорилось, плетеная защитная оболочка поглощает внешние электромагнитные сигналы, не позволяя им влиять на передаваемые по жиле данные, поэтому коаксиальный кабель можно использовать при передаче на большие расстояния и в тех случаях, когда высокоскоростная передача данных осуществляется на несложном оборудовании.

Существует два типа коаксиальных кабелей:

* тонкий коаксиальный кабель;
* толстый коаксиальный кабель.

Тонкий коаксиальный кабель — гибкий кабель диаметром около 0,5 см (около 0,25 дюймов). Он прост в применении и годится практически для любого типа сети. Подключается непосредственно к платам сетевого адаптера компьютеров.

Тонкий коаксиальный кабель способен передавать сигнал на расстояние до 185 м (около 607 футов) без его заметного искажения, вызванного затуханием.

Производители оборудования выработали специальную маркировку для различных типов кабелей. Тонкий коаксиальный кабель относится к группе, которая называется семейством RG-58, его волновое сопротивление равно 50 Ом. Волновое сопротивление (impedance) — это сопротивление переменному току, выраженное в омах. Основная отличительная особенность этого семейства — медная жила. Она может быть сплошной или состоять из нескольких переплетенных проводов.

Толстый (thick) коаксиальный кабель — относительно жесткий кабель с диаметром около 1 см (около 0,5 дюймов). Иногда его называют «стандартный Ethernet», поскольку он был первым типом кабеля, применяемым в Ethernet — популярной сетевой архитектуре. Медная жила этого кабеля толще, чем у тонкого коаксиального кабеля.

Чем толще жила у кабеля, тем большее расстояние способен преодолеть сигнал. Следовательно, толстый коаксиальный кабель передает сигналы дальше, чем тонкий, — до 500 м (около 1 640 футов). Поэтому толстый коаксиальный кабель иногда используют в качестве основного кабеля (магистрали), который соединяет несколько небольших сетей, построенных на тонком коаксиальном кабеле.

Как правило, чем толще кабель, тем сложнее с ним работать. Тонкий коаксиальный кабель гибок, прост в установке и относительно недорог. Толстый 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 передает сигналы на большие расстояния.

Самая простая витая пара — это два перевитых вокруг друг друга изолированных медных провода. Существует два типа тонкого кабеля: неэкранированная витая пара и экранированная витая пара.

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

Неэкранированная витая пара (спецификация lOBaseT) широко используется в ЛВС, максимальная длина сегмента составляет 100 м (328 футов).

Неэкранированная витая пара состоит из двух изолированных медных проводов. Существует несколько спецификаций, которые регулируют количество витков на единицу длины — в зависимости от назначения кабеля. В Северной Америке UTP повсеместно используется в телефонных сетях.

Неэкранированная витая пара определена в особом стандарте - Electronic Industries Association and the Telecommunications Industries Association (EIA/TIA) 568 Commercial Building Wiring Standart. EIA/TIA 568 — на основе UTP — устанавливает стандарты для различных случаев, гарантируя единообразие продукции. Эти стандарты включают пять категорий UTP.

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

Категория 2.Кабель, способный передавать данные со скоростью до 4 Мбит/с. Состоит из четырех витых пар.

Категория 3.Кабель, способный передавать данные со скоростью до 10 Мбит/с. Состоит из четырех витых пар с девятью витками на метр.

Категория 4. Кабель, способный передавать данные со скоростью до 16 Мбит/с. Состоит из четырех витых пар.

Категория 5. Кабель, способный передавать данные со скоростью до 100 Мбит/с. Состоит из четырех витых пар медного провода.

Большинство телефонных систем использует неэкранированную витую пару. Это одна из причин ее широкой популярности. Причем во многих зданиях, при строительстве, UTP прокладывают не только для сегодняшних нужд телефонизации, но и, предусматривая запас кабеля, в расчете на будущие потребности. Если установленные во время строительства провода рассчитаны 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, какие требуются для надежной и безопасной передачи данных между компьютерами.

Одной из потенциальных проблем для всех типов кабелей являются перекрестные помехи. Вы, должно быть, помните, что перекрестные помехи — это электрические наводки, вызванные сигналами в смежных проводах. Неэкранированная витая пара особенно страдает от перекрестных помех. Для уменьшения их влияния используют экран.

Кабель экранированной витой пары (STP) имеет медную оплетку, которая обеспечивает большую защиту, чем неэкранированная витая пара. Кроме того, пары проводов STP обмотаны фольгой. В результате экранированная витая пара обладает прекрасной изоляцией, защищающей передаваемые данные от внешних помех. Все это означает, что STP, по сравнению с UTP, меньше подвержена воздействию электрических помех и может передавать сигналы с более высокой скоростью и на большие расстояния.

Для подключения витой пары к компьютеру используются телефонные коннекторы RJ-45. На первый взгляд, они похожи на RJ-11, но в действительности между ними есть существенные отличия. Во-первых, вилка RJ-45 чуть больше по размерам и не подходит для гнезда RJ-11. Во-вторых, коннектор RJ-45 имеет восемь контактов, a RJ-11 — только четыре.

Построить развитую кабельную систему и в то же время упростить работу с ней Вам поможет ряд очень полезных компонентов.

* распределительные стойки и полки.
* распределительные стойки и полки предназначены для монтажа кабеля. они позволяют централизованно организовать множество соединений и при этом занимают достаточно мало места.
* коммутационные панели. существуют разные типы панелей расширения. они поддерживают до 96 портов и скорость передачи до 100 мбит/с.
* коннекторы. одинарные или двойные вилки rj-45 подключаются к панелям расширения или настенным розеткам. они обеспечивают скорость передачи до 100 мбит/с.
* розетки

В оптоволоконном кабеле цифровые данные распространяются по оптическим волокнам в виде модулированных световых импульсов. Это относительно надежный (защищенный) способ передачи, поскольку электрические сигналы при этом не передаются. Следовательно, оптоволоконный кабель нельзя вскрыть и перехватить данные, от чего не застрахован любой кабель, проводящий электрические сигналы.

Оптоволоконные линии предназначены для перемещения больших объемов данных на очень высоких скоростях, так как сигнал в них практически не затухает и не искажается.

Оптическое волокно — чрезвычайно тонкий стекляшчьш цилиндр, называемый жилой (core), покрытый слоем стекла, называемого оболочкой, с иным, чем у жилы, коэффициентом преломления. Иногда оптоволокно производят из пластика. Пластик проще в использовании, но он передает световые импульсы на меньшие расстояния по сравнению со стеклянным оптоволокном.

Каждое стеклянное оптоволокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон с отдельными коннекторами. Одно из них служит для передачи, а другое -- для приема. Жесткость волокон увеличена покрытием из пластика, а прочность — волокнами из кевлара. На рисунке представлен пример кевларового покрытия. Кевларовые волокна располагаются между двумя кабелями, заключенными в пластик.

Передача по оптоволоконному кабелю не подвержена электрическим помехам и ведется на чрезвычайно высокой скорости (в настоящее время до 100 Мбис/с, теоретически возможная скорость - 200 000 Мбит/с). По оптоволоконному кабелю можно передавать световой импульс на многие километры.

Выше были рассмотрены кабельные линий связи, но ещё существует проводные (воздушные) линии связи и радиоканалы наземной и спутниковой связи.

Проводные воздушные линии связи представляют собой провода без каких-либо изолирующих или экранирующих оплеток, проложенных между столбами и висящие в воздухе. По таким линиям связи традиционно передаются телефонные или телеграфные сигналы, но при отсутствии других возможностей эти линии используется и для передачи компьютерных данных. Скоростные качества и помехозащищенность этих линий оставляют желать много лучшего. Сегодня проводные линии связи уже почти нигде не встречается.

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приёмника радиоволн. Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапозоном, так и дальностью канала. Диапазоны коротких, средних и длинных волн, называемые также диапазонами амплитудной модуляции по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но работающие на диапазонах ультракоротких волн, для которых характерна частотная модуляция, а также диапазонах сверхчастот (СВЧ). В диапазоне СВЧ (свыше 4ГГц) сигналы уже не отражаются ионосферой Земли и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют либо спутниковые каналы, либо радиорелейные каналы, где это условие выполняется.

* 1. **Базовые технологии построения локальных сетей**

За время, прошедшее с момента появления первых локальных сетей, было разработано несколько сот самых разных сетевых технологий, однако заметное распространение получили немногие. Это связано, прежде всего, с высоким уровнем стандартизации принципов организации сетей и с поддержкой их известными компаниями. Тем не менее, не всегда стандартные сети обладают рекордными характеристиками, обеспечивают наиболее оптимальные режимы обмена. Немаловажно и то, что производители программных средств также в первую очередь ориентируются на самые распространенные сети. Далее будут рассмотрены особенности основных технологий локальных сетей.

Token Ring разработан фирмой IBM. В качестве передающей среды применяется неэкранированная или экранированная витая пара (UPT или SPT) или оптоволокно. Скорость передачи данных 4 Мбит/с или 16Мбит/с. В качестве метода управления доступом станций к передающей среде используется метод - маркерное кольцо (Тоken Ring).

Основные положения этого метода:

* устройства подключаются к сети по топологии кольцо;
* все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);
* в любой момент времени только одна станция в сети обладает таким правом.

В IВМ Тоkеn Ring используются три основных типа пакетов: пакет управление/данные (Data/Соmmand Frame), маркер (Token) и пакет сброса (Аbort).

С помощью пакета управление/данные выполняется передача данных или команд управления работой сети. С помощью типа маркер станция может начать передачу данных только после получения такого пакета. В одном кольце может быть только один маркер и, соответственно, только одна станция с правом передачи данных. Посылка пакета сброса называет прекращение любых передач.

В сети можно подключать компьютеры по топологии звезда или кольцо.

Arknet - простая, недорогая, надежная и достаточно гибкая архитектура локальной сети. Разработана корпорацией Datapoint в 1977 году. Впоследствии лицензию на Аrcnet приобрела корпорация SМС (Standard Microsistem Corporation), которая стала основным разработчиком и производителем оборудования для сетей Аrcnet. В качестве передающей среды используются витая пара, коаксиальный кабель (RG-62) с волновым сопротивлением 93 Ом и оптоволоконный кабель. Скорость передачи данных - 2,5 Мбит/с. При подключении устройств в Аrcnet применяют топологии шина и звезда. Метод управления доступом станций к передающей среде - маркерная шина (Тоken Bus).

Этот метод предусматривает следующие правила:

* все устройства, подключенные к сети, могут передавать данные только получив разрешение на передачу (маркер);
* в любой момент времени только одна станция в сети обладает таким правом;
* данные, передаваемые одной станцией, доступны всем станциям сети.

Передача каждого байта в Аrcnet выполняется специальной посылкой ISU(Information Symbol Unit - единица передачи информации), состоящей из трех служебных старт/стоповых битов и восьми битов данных. В начале каждого пакета передается начальный разделитель АВ (Аlегt Вurst), который состоит из шести служебных битов. Начальный разделитель выполняет функции преамбулы пакета.

В Аrcnet определены 5 типов пакетов:

1. пакет IТТ (Information To Transmit) - приглашение к передаче. Эта посылка передает управление от одного узла сети другому. Станция, принявшая этот пакет, получает право на передачу данных.
2. пакет FBE (Free Buffeг Еnquiries) - запрос о готовности к приему данных. Этим пакетом проверяется готовность узла к приему данных.
3. пакет данных. С помощью этой посылки производиться передача данных.
4. пакет АСК (ACKnowledgments) - подтверждение приема. Подтверждение готовности к приему данных или подтверждение приема пакета данных без ошибок, т.е. в ответ на FBE и пакет данных.
5. пакет NAK (Negative AcKnowledgments) - неготовность к приему. Неготовность узла к приему данных (ответ на FBE) или принят пакет с ошибкой.

В сети Arknet можно использовать две топологии: звезда и шина.

Ethernet – это самый распространенный на сегодняшний день стандарт локальных сетей.

Спецификацию Ethernet в конце семидесятых годов предложила компания Xerox Corporation. Позднее к этому проекту присоединились компании Digital Equipment Corporation (DEC) и Intel Corporation. В 1982 году была опубликована спецификация на Ethernet версии 2.0. На базе Ethernet институтом IEEE был разработан стандарт IEEE 802.3. Различия между ними незначительные.

На логическом уровне в Ethernet применяется топология шина:

* все устройства, подключенные к сети, равноправны, т.е. любая станция может начать передачу в любой момент времени(если передающая среда свободна);
* данные, передаваемые одной станцией, доступны всем станциям сети.

Метод управления доступом (для сети на коаксиальном кабеле) — множественный доступ с контролем несущей и обнаружением коллизий скорость передачи данных 10 Мбит/с, размер пакета от 72 до 1526 байт, описаны методы кодирования данных. Режим работы полудуплексный, то есть узел не может одновременно передавать и принимать информацию. Количество узлов в одном разделяемом сегменте сети ограничено предельным значением в 1024 рабочих станции (спецификации физического уровня могут устанавливать более жёсткие ограничения, например, к сегменту тонкого коаксиала может подключаться не более 30 рабочих станций, а к сегменту толстого коаксиала — не более 100). Однако сеть, построенная на одном разделяемом сегменте, становится неэффективной задолго до достижения предельного значения количества узлов, в основном по причине увеличивающегося количества коллизий.

FDDI (Fiber Distributed Data Interface — распределённый волоконный интерфейс данных) — стандарт передачи данных в локальной сети, протянутой на расстоянии до 200 километров. Стандарт основан на протоколе Token Ring. Кроме большой территории, сеть FDDI способна поддерживать несколько тысяч пользователей.

В качестве среды передачи данных в FDDI рекомендуется использовать оптоволоконный кабель, однако можно использовать и медный кабель, в таком случае используется сокращение CDDI (Copper Distributed Data Interface). В качестве топологии используется схема двойного кольца, при этом данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным, по нему передаётся информация в обычном состоянии; второе — вспомогательным, по нему данные передаются в случае обрыва на первом кольце. Для контроля за состоянием кольца используется сетевой маркер, как и в технологии Token Ring. Поскольку такое дублирование повышает надёжность системы, данный стандарт с успехом применяется в магистральных каналах связи.

Сравнительный анализ существующих технологий представлен в Приложении А.

**2. АНАЛИЗ И КОМПЛЕКС МЕРОПРИЯТИЙ ПО ОБСЛУЖИВАНЮ ЛОКАЛЬНОЙ СЕТИ СЛУЖБЫ ПО ДЕЛАМ ДЕТЕЙ СЕВЕРОДОНЕЦКОЙ ГОРОДСКОГО СОВЕТА**

**2.1 Административные, технические и программные характеристики Службы по делам детей Северодонецкой городской рады**

Проанализируем структуру Службы по делам детей Северодонецкой городского совета. Назначением данной службы является, реализация политики по вопросам социальной защиты детей и предотвращения детской безприглядности и совершения правонарушений детьми. Данная служба является юридическим лицом. В состав данной службы входят такие структурные подразделения как главная бухгалтерия и сектор по вопросу опеки по попечительству. Ниже представлена схема организационной структуры предприятия (см. рисунок 2.1).

Начальник

Главный бухгалтер

Заведующий сектором по вопросу опеки опечительству

Специалист I категории

Специалист

Специалист

Специалист

Рисунок 2.1 - Организационная структура предприятия.

План помещения состоит из следующих кабинетов:

1. кабинет начальника;
2. кабинет бухгалтера;
3. кабинет заведующего по вопросу опеки и попечительству;
4. кабинет специалиста I категории;
5. кабинет специалистов.

Графический план представлен в Приложении Б.

В кабинете начальника расположены такие технические средства как компьютер (1шт), принтер (1шт) и телефон.

В кабинете главного бухгалтера расположены компьютер (1шт) и ксерокс (1шт).

В кабинете заведующего сектором по вопросу опеки и попечительства расположены компьютер (1шт) и сканер (1шт).

В кабинете специалиста I категории расположены компьютер (1шт) и принтер (1шт).

В кабинете специалистов расположены компьютер (1шт) и принтер (1шт).

Компьютер, расположеный в кабинете начальника, имеет такие технические характеристики:

* процессора Intel Core 2 Quad 2.33 Ghz;
* материнская плата - на базе чипсета Intel P35Express + ICH10;
* оперативная память - DDR II 4 GB PC2-6400 800 MHz;
* жесткий диск - 150 GB Serial ATA 16 Mb;
* графический акселератор - NVIDIA 9600GT 512MB/256bit;
* оптический привод DVD -RW/+RW;
* корпус - ATX Middle Tower GIGABYTE GZ-X1 420W (Brand GIGABYTE);
* акустика - STORM U-709A;
* манипулятор «мышь»;
* клавиатура PS/2 A-4 Tech KB(S)-26.

Компьютер, расположенный в кабинете заведующего по делам опеки и попечительства, имеет такие же характеристики как и компьютер, расположеный в кабинете главного бухгалтера:

* процессор – AMD Socket AM2 ATHLON 64 X2 5200+ BOX;
* материнская прлата – MB Asus P4PE-2x;
* оперативная память – DDR 512 PC3200;
* жёсткий диск - USB 2.0 PRESTIGIO Data Safe II 2.5" 160GB USB 2.0;
* оптический привод DVD -RW/+RW;
* корпус ATX 4U 4203, 350 W Black;
* монитор 19" TFT Prestigio P1910;
* манипулятор «мышь»;
* клавиатура PS/2 A-4 Tech KB(S)-720.

Компьютеры,расположеные в кабинетах специалиста I категории и в кабинете специалистов, имеют следующие характеристики:

* процессор – AMD Socket AM2 ATHLON 64 X2 5400+ BOX;
* материнская прлата – ASUS M2A-VM SocketAM2 AMD 690G PCI-E;
* оперативная память – DDR 512 PC3200;
* жёсткий диск - SATA II 160.0g 7200 Samsung 8Mb (NCQ);
* оптический привод DVD -RW/+RW;
* корпус ATX Midle Tower ASUS TA-668, 350W;
* монитор CRT 17" LG F720B FLATRON;
* манипулятор «мышь»;
* клавиатура PS/2 A-4 Tech KB(S)-720.

В работе предприятия используются следующие программные продукты:

* Windows XP Home Edition Russian CD BOX;
* Get Genuine Kit Win XP Pro Russian w/SP 1 License;
* Office Professional Plus 2007 Russian OPL NL;
* Kaspersky Internet Security 2009 5-Desktop 1 year Base Box;
* ABBYY Fine Reader 9.0 Professional Edition;
* RAR Archiver.

Таким образом рассмотрев организационную структуру предприятия можно сказать, что на предприятии осуществляются информационные потоки

- от начальника к главному бухгалтеру и заведующему сектором по вопросам опеки и попечительства в виде приказов;

- от заведующего сектором по вопросам опеки и попечительству к специалисту I категории и трем специалистам в виде приказов;

- от специалиста I категории и специалистов к заведующему сектором по вопросам опеки и попечительства в виде отчетов;

- от главного бухгалтера и заведующего сектором по вопросам опеки и попечительства к начальнику в виде отчетов.

Для обеспечения данного информационного потока в Службе по делам детей Северодонецкого городского совета создана локальная сеть.

**2.2 Анализ локальной компьютерной сети Службы по делам детей Северодонецкого городкого совета**

Проанализировав существующую сеть можно сказать, что

1. используемая технология – Ethernet;
2. среда передачи данных – коаксиальный кабель;
3. сетевое оборудование – GETNET 16 PORT Switch 10/100 GS-D16P;
4. рабочая станция (2шт) имеет следующие характеристики:
   * процессор – AMD Socket AM2 ATHLON 64 X2 5400+ BOX;
   * материнская прлата – ASUS M2A-VM SocketAM2 AMD 690G PCI-E;
   * оперативная память – DDR 512 PC3200;
   * жёсткий диск - SATA II 160.0g 7200 Samsung 8Mb (NCQ);
   * оптический привод DVD -RW/+RW;
   * корпус ATX Midle Tower ASUS TA-668, 350W;
   * монитор CRT 17" LG F720B FLATRON;
   * манипулятор «мышь»;
   * клавиатура PS/2 A-4 Tech KB(S)-720.

Рабочая станция (2шт) имеет следующие характеристики:

* процессор – AMD Socket AM2 ATHLON 64 X2 5200+ BOX
* материнская прлата – MB Asus P4PE-2x
* оперативная память – DDR 512 PC3200
* жёсткий диск - USB 2.0 PRESTIGIO Data Safe II 2.5" 160GB USB 2.0
* оптический привод DVD -RW/+RW
* корпус ATX 4U 4203, 350 W Black
* монитор 19" TFT Prestigio P1910
* манипулятор «мышь»
* клавиатура PS/2 A-4 Tech KB(S)-720

Сервер (1шт) имеет следующие характеристики:

* процессора Intel Core 2 Quad 2.33 Ghz;
* материнская плата - на базе чипсета Intel P35Express + ICH10;
* оперативная память - DDR II 4 GB PC2-6400 800 MHz;
* жесткий диск - 150 GB Serial ATA 16 Mb;
* графический акселератор - NVIDIA 9600GT 512MB/256bit;
* оптический привод DVD -RW/+RW;
* корпус - ATX Middle Tower GIGABYTE GZ-X1 420W (Brand GIGABYTE);
* акустика - STORM U-709A;
* манипулятор «мышь»;
* клавиатура PS/2 A-4 Tech KB(S)-26.

Данная локальная сеть объединяет структурные подразделы предприятия и представлена в приложении Б.

Такая конфигурация сети полностью удовлетворяет требованиям по обеспечению бесперебойного документооборота и по использованию совмесных ресурсов. Так как в сеть объединены 5 компьютеров, будет обеспечено высокое быстродейсвие передачи данных в сети. При моделировании видно, что соединение 100 Мбит/с используется не на полную мощность, что позволит развивать и увеличивать сеть, не задумываясь о скорости передачи данных.

При увеличении числа рабочих станций не нужно будет менять сетевое оборудование, необходимо только добавить отдельные компоненты, такие как дополнительные линии связи, так как свободными остаются еще 11 портов Switch 10/100 GS-D16P.

Данная структура сети полностью удовлетворяет потребностям предприятия, а также предусмотрена возможность расширения. Так как могут возникать неисправности сети, необходимо разработать комплек мер по профилактике и защите сети.

**2.3 Описание комплекса мероприятий по обслуживанию сети**

**2.3.1 Администрирование локальной сети**

Администрирование локальной сети – это обеспечение и контроль физической связи, настройка активного оборудования, настройка общего доступа и определённого круга программ, обеспечивающих стабильную работу сети.

Многие инструменты есть в самой операционной системе, другие разработаны различными программистами. Также перечень инструментов администратора может практически неограниченно расширяться по мере развития сети.

Далее рассмотрены основные инструменты администратора сети:

* команда ping. эта команда есть во всех операционных системах, поддерживающих работу в сети. Особенности работы команды, список её параметров может быть различным у различных систем, но основные функции неизменны. Команда позволяет определить следующие параметры сети: доступность компьютера в сети, работоспособность кабельной линии между компьютерами, качество связи между компьютерами и т.д.
* команда inconfig - команда также запускается при помощи командной строки и позволяет узнать о сетевых настройках компьютера, на котором она запущена.
* программа для сканирования сетей superscan - утилита, позволяющая определить работающие в данный момент компьютеры сети.
* окно управления компьютером – средство, с помощью которого можно контролировать работу пользователей.
* окно просмотр событий, содержащееся в современных операционных системах, содержит сбора информации о происходящих в них событиях, связанных с работой программ, служб и самой системы.

Администратор может совершать действия для организации и контролирования за работой сетью и пользователей, некоторые из них представлены ниже.

Запуск приложений с диска сервера вместо диска рабочей станции представляет собой способ обеспечения стабильной рабочей конфигурации для пользователей и сведения к минимуму нагрузки по администрированию сети. В простейшей форме процесс сводится к установке приложения обычным образом с указанием каталога сетевого диска, вместо локального каталога, в качестве места расположения файлов программы. Однако приложения Windows никогда не отличались простотой, поэтому в реальности этот процесс выглядит намного сложней.

Запуск приложений с диска сервера имеет как достоинства так и недостатки. Положительным фактором, как и в случае с размещением на сервере операционной системы, можно назвать экономию пространства локальных дисков, защиту файлов приложений от повреждения или удаления, а также возможность улучшения и обслуживания единственной копии приложения, а не индивидуальных копий на каждой рабочей станции. Среди недостатков на первый план выступает тот факт, что приложения, размещенные на сервере, обычно работают сравнительно медленнее, чем их локальные аналоги, а также генерируют существенный объем сетевого трафика и не могут функционировать, если сервер неисправен или не доступен по другим причинам.

Есть возможность совместного использования несколькими рабочими станциями приложение, размещенное на сервере, то, как правило, по-прежнему придется привести его полную установку на каждой машине. Это делается для того, чтобы быть уверенными, что каждая рабочая станция имеет соответствующие файлы Windows, установки реестра и пиктограммы, необходимые для работы приложения. Один из способов практической реализации приложения, размещенного на сервере, заключается в проведении полной инсталляции программы на каждую рабочую станцию, с указанием имени одного и того же каталога сервера в качестве места расположения файлов программы в каждом отдельном случае. Таким образом, каждая рабочая станция получит все необходимые файлы и модификации, а на сервере останется всего одна копия файлов приложения.

В большинстве современных сетей Windows как операционная система, так и файлы приложений устанавливаются на локальных дисках рабочих станций. Однако по-прежнему только от администратора сети зависит принятие решений о том, где именно будут храниться файлы данных, создаваемые и изменяемые пользователями. При решении данного вопроса следует обращать особое внимание на некоторые принципиальные моменты, а именно, доступность этих файлов для пользователей и их безопасность. Естественно, пользователи должны получать доступ к своим файлам данных, но существуют также файлы, которые должны совместно использоваться многими пользователями. Важные файлы данных также должны быть защищены от модификации и удаления неавторизованным персоналом и к тому же дублироваться на альтернативном носителе в целях страховки от непредвиденных обстоятельств, например, выхода диска из строя или пожара.

Рабочие файлы могут иметь различный формат, что не может отражаться на том, каким способом их надлежит хранить. Например, документы индивидуальных пользователей, созданные с помощью текстовых редакторов или электронных таблиц, предназначены для использования одним человеком в каждый момент времени, в то время как базы данных поддерживают одновременный доступ несколькими пользователями. В большинстве случаев файлы баз данных хранятся на компьютерах, исполняющих приложения серверов баз данных, поэтому администраторы могут регулировать доступ к ним с помощью разрешений файловой системы и защищать регулярным резервным копирование. Другие типы файлов могут требовать дополнительного планирования.

Наилучшей стратегией для большинства сетей Windows представляется установка операционной системы и всех прочих приложений на локальные диски рабочих станций в сочетании с хранением всех рабочих файлов на серверах сети. Наиболее распространенная практика заключается в создании на сервере индивидуального каталога для каждого пользователя, при чем пользователю предоставляется полный контроль над собственным каталогом. Затем следует сконфигурировать все приложения для хранения рабочих файлов в этом каталоге по умолчанию, чтобы никакой ценной информации не оставалось на локальном диске.

В организации возможность сформировать стабильную и жизнеспособную конфигурацию рабочих станций предоставлена администратору.

Одним из моментов конфигурирования рабочих станций заключается в обозначении диска сервера одной и той же буквой для всех рабочих станций. Если в сети есть серверы приложений, предоставляющие свои ресурсы всем пользователям сети (например, сервер базы данных компании), тогда каждая система сети должна обозначать диск этого сервера одной и той же буквой.

Для реализации стабильного набора букв, соответствующим дискам пользователей, можно применить скрипты входа. Они содержат команды NET USE, отображающие диски определенных серверов при каждом подключении пользователя к сети. Правильное структурирование этих команд позволит создать единый скрипт входа в сеть для многочисленных пользователей.

Для разрешения каждому пользователю возвращать свои собственные конфигурационные установки при регистрации в системе существуют отдельные профили.

Создание профилей пользователей представляет собой метод хранения ярлыков и установок конфигурации рабочего стола индивидуальных пользователей в каталогах, к которым возможно получение доступа в процессе запуска систем. Если профили пользователей хранятся на рабочей станции, то становится возможным её совместная эксплуатация несколькими пользователями, причем без необходимости перезаписывать конфигурационные установки при регистрации в системе. Если же профили хранятся на сервере сети, пользователи смогут получать к ним доступ с любой рабочей станции. Это называется перемещаемым профилем. Кроме того, можно заставить пользователей загружать определенный профиль при каждом входе в систему и запретить им изменять его – это обязательный профиль.

Если в вопросах обеспечения конфигурации рабочих станций предполагается опираться на размещение профилей пользователей на сервере, то следует обязательно предпринять ряд мер для того, чтобы эти профили всегда оставались доступными пользователям, когда бы они не подключались к сети.

Администратор может контролировать реестр рабочей станции. Системный реестр является центральным хранилищем данных о конфигурации в операционных системах Windows, и осуществление контроля над ним есть одна из наиболее важных частей работы системного администратора. Возможность получения доступа к реестру рабочей станции, как удаленно, так и автоматизированном режиме, позволит контролировать практически любой аспект функциональности системы, а также защищать сам реестр от повреждения из-за неавторизованных изменений.

Все 32-битные операционные системы Windows включают возможность проведения системной политики, варианты которой позволяют осуществлять значительный объем контроля над конфигурацией рабочей станции. Определив набор правил системной политики и внедрив его, можно контролировать, к каким именно компонентам операционной системы будет разрушен доступ пользователей, какие приложения эти пользователи смогут запускать, а также какой вид будет иметь их рабочий стол. Правила системной политики представляют собой не более чем набор установок системного реестра, которые упакованы в файл системной политики и хранятся на диске сервера. Когда пользователь подключается к сети, рабочая станция загружает файл системной политики с сервера и применяет зафиксированные там установки к своему системному реестру.

Редактор системной политики представляет собой просто инструмент для создания файлов системной политики, он совершенно не контролирует конкретные варианты политики, которые создает. Сами правила системной политики берут начало из шаблонов системной политики, которые представляют собой файлы формата ASCII, содержащие ключи реестра, возможные значения, пояснительный текст. Все это формирует правила политики.

С помощью системной политики можно ограничить доступ к файловой системе, что представляет собой еще один способ защиты рабочих станций от вмешательств со стороны пользователей. Блокирование этого доступа не допустит перемещение, удаление или изменения файлов, необходимых для функционирования операционной системы рабочей станции.

**2.3.2 Средства выявления неисправностей**

Существует 7 уровней сетевого стека, определенных в эталонной модели OSI.

7.Прикладной (напр. HTTP, SMTP, SNMP, FTP, Telnet, scp, NFS, RTSP, BGP)

6.Представительный (напр. XML, XDR, ASN.1, SMB, AFP)

5.Сеансовый (напр. TLS, SSL, ISO 8327 / CCITT X.225, RPC, NetBIOS, ASP)

4.Транспортный (напр. TCP, UDP, RTP, SCTP, SPX, ATP, DCCP, GRE)

3.Сетевой (напр. IP, ICMP, IGMP, CLNP, OSPF, RIP, IPX, DDP)

2.Канальный (напр. Ethernet, Token ring, PPP, HDLC, X.25, Frame relay, ISDN, ATM, MPLS, Wi-Fi, ARP, RARP)

1.Физический (напр. электричество, радио, оптоволокно)

Нарушения могут возникнуть фактически на любом уровне, и средства, используемые для диагностики проблем на различных уровнях, совершенно различны. Знание доступных средств является существенным моментом в борьбе с неисправностями.

Некоторые возможности по выявлению неисправностей встроены в стандартные операционные системы. Далее рассмотрены некоторые из средств выявления проблем сети, предоставляемые операционными системами, наиболее широко используемыми в современных сетях.

Операционные системы Windows включают различные средства, которые можно применять для управления сетевыми соединениями и выявления связанных с ними проблем. Далее рассмотрены некоторые из них:

1) Команда NET является основным средством управления из командной строки для сетевого клиента Windows. Эту команду можно использовать для выполнения многих сетевых функций, схожих с теми, что позволяют осуществлять графические утилиты, такие как Windows Explorer (проводник Windows). Поскольку NET – утилита командной строки, то существует возможность включать ее в скрипты регистрации и командные файлы. Например, NET можно использовать для входа и выхода из сети, подключения сетевых ресурсов совместного использования, запуска и остановки сервисов, размещения в сети разделяемых ресурсов.

Команда NET реализована как файл с именем NET.exe, который помещается в системный каталог в процессе инсталяции операционной системы. Чтобы использовать эту программу, нужно запустить файл из командной строки, указав подкоманду, которая может иметь дополнительные параметры.

2) NET Watcher (Инспектор сети) – это утилита, включенная в Windows 95/98 и Windows NT Server 4.0 Resourse Kit. которая позволяет отслеживать пользователей сети, подключенных к компьютеру, ресурсы совместного использования, к которым они в данный момент осуществляют доступ, и файлы, открытые удаленными пользователями. Также можно отключать пользователей от ресурсов совместного использования, принудительно закрывать файлы, которые эти пользователи открыли, и создавать или удалять разделяемые ресурсы. NET Watcher обычно применяется для определения, кто из пользователей в данный момент осуществляет доступ к ресурсам совместного использования и файлам данного компьютера. Однако с точки зрения администрирования лучшая возможность этого приложения заключается в том, что оно позволяет соединиться с другими компьютерами в сети и выполнить на них эти действия удаленно.

3) Web Administrator – это дополнение к серверу Интернета (IIS) от Microsoft, которое позволяет управлять многими элементами системы Windows NT 4.0 Server при помощи любого Web-браузера, совместимого с языком Java.

Задачи, которые позволяет решать Web Administrator:

* управления локальными и доменными учетными записями пользователей, групп и компьютеров;
* управление драйверами устройств, установленными в системе;
* просмотр журнала регистрации событий событий NT;
* управление разрешениями общих ресурсов и файлов системы;
* отправление сообщений пользователям, зарегистрировавшимся на сервере;
* удаленная перезагрузка сервера;
* управление очередями печати и их содержимым;
* запуск, остановка и приостановка работы сервисов;
* мониторинг сеансов и отключение пользователей;
* просмотр информации о состоянии сервера и статистики производительности.

4) Microsoft NetMeeting – вообще, это программное средство для содания конференций и коллективной работы, предназначенное для работы через Интернет, но оно также может оказать большую услугу администратору сети. NetMeeting является частью полной установки Internet Explorer 4 и 5, но и помимо этого программа также доступна в отдельно в виде версий для Windows 95/98 и NT/2000. Одна из возможностей NetMeeting называется «общий доступ к рабочему столу», она позволяет удаленному пользователю получить полный контроль над компьютером. Администраторы могут прибегнуть к этой возможности для удаленного конфигурирования системы, установки программного обеспечения и даже для запуска приложений, и все без какого-либо прямого взаимодействия с удаленного компьютера.

Также широко используются утилиты TCP/IP. В следствии того, что TCP/IP стал наиболее распространенным стеком протоколов в сетевой индустрии, поэтому многие задачи администрирования сети и выявления неисправностей включают в себя работу с различными элементами этих протоколов. Так как практически все компьютерные платформы поддерживают TCP/IP, его основные служебные средства были перенесены на множество различных операционных систем, а некоторые из них адаптированы к специальным нуждам. Далее рассматриваются некоторые из этих средств, но в большей степени с точки зрения полезности для администратора сети, нежели чем с позиции составляющих элементов и специфики реализации.

Утилита Ping, несомненно, является наиболее распространенным средством диагностики TCP/IP и включена практически в каждую реализацию протоколов TCP/IP. В большинстве случаев это – утилита командной строки, хотя существует несколько графических версий, а также версии на базе меню. Все они выполняют одни и те же задачи. Основная функция Ping заключается в отправке сообщения другой TCP/IP-системе сети, чтобы определить, правильно ли работает стек протоколов вплоть до Сетевого уровня. Так как стек протоколов TCP/IP функционирует одинаково во всех системах, то можно использовать программу для проверки соединения между двумя любыми компьютерами вне зависимости от процессорной платформы или операционной системы.

Traceroute – утилита, которая обычно реализована как программа командной строки и включена в большинству стеков TCP/IP, хотя иногда она носит другое имя. В системах Unix команда называется traceroute, а реализация для Windows с такими же функциональными возможностями называется Tracert.exe. Назначением этого программного средства являются отображения маршрута, который преодолевают пакеты IP, чтобы достигнуть определенной системы назначения.

Таблица маршрутизации является жизненно важной частью сетевого стека любой системы TCP/IP, даже той, что не выполняет функции маршрутизатора. Система использует таблицу маршрутизации, чтобы определить, каким образом следует передавать каждый пакет. Пакет Route.exe в Windows и команда route, включенная в большинство версий UNIX, позволяет просматривать таблицу маршрутизации и добавлять или удалять записи в ней.

Netstat является утилитой командной строки, которая отображает статистику сетевого трафика для различных протоколов TCP/IP и, в зависимости от платформы, может также выводить на экран другую информацию. Большинство вариантов UNIX поддерживают команду netstat, а операционные системы Windows включают программу Netstat.exe, которая по умолчанию устанавливается вместе со стеком TCP/IP. Параметры командной строки для netstat в разных реализациях могут варьироваться, но одним из основных является параметр –s, который отображает статистику для каждого из основных протоколов TCP/IP.

Не считая общего числа пакетов, принятых и переданных каждым протоколом, netstat предоставляет различную информацию о сбойных ситуациях и других процессах, которая может помочь выявить проблемы сетевого взаимодействия на различных уровнях модели OSI.

Nslookup является утилитой, которая позволяет отправлять запросы непосредственно определенному DNS-серверу, чтобы разрешить имена в IP-адреса или запросить иную информацию. В отличии от других методов разрешения имен, таких как использование Ping, Nslookup позволяет указать, какой из серверов получит команды, что дает возможность определить, правильно ли работает DNS-сервер и содержит ли он верные данные.

Программа Ipconfig является простой утилитой для отображения конфигурационных параметров TCP/IP системы. Это особенно полезно, когда для автоматической конфигурации клиентов TCP/IP в сети используется серверы DHCP, так как для пользователей не существует другого простого способа увидеть, какие установки были назначены их рабочими станциями.

Анализатор сети является мощным инструментом, который может быть легко использован в целях выявления проблем в сети и ее поддержки. Когда программа декодирует пакет, она отображает все его содержимое, включая информацию, которая может быть секретной. Протокол FTP, например, передает пароли пользователя в текстовом виде, и они могут быть легко прочитаны при захвате пакетов анализаторов сети.

Анализаторы сети, иногда называемый анализатором протоколов, представляет собой устройство, захватывающее передаваемый по сети трафик и анализирующее его свойства несколькими различными способами. Основной функцией анализатора является декодирование и отображение содержимого захваченных в сети пакетов. Для пакетов программа выводит информацию, найденную в любом из полей каждого протокольного заголовка, а также данные исходного приложения, переносимые в качестве полезных данных пакета. Анализаторы, к тому же, часто предоставляют статистику о передаваемом по сети трафике, такую как число пакетов, используемых определенным протоколом, и количество трафика, сгенерированного каждой системой в сети. Анализатор сети также является прекрасным средством для обучения. Нет лучшего способа познакомиться с сетевыми протоколами и их функциями, чем увидеть их в действии.

Существуют очень разнообразные анализаторы сети, начиная с отдельных аппаратных устройств, стоящих тысячи долларов, и заканчивая программными продуктами, сравнительно недорогими или бесплатными. Например, Windows NT Server и Windows 2000 Server включают приложение Network Monitor, которое позволяет анализировать сетевой трафик.

По сути, анализатор сети – это приложение, запущенное на компьютере с установленной платой сетевого адаптера. Это объясняет, почему эти устройства могут включать аппаратное обеспечение, либо принимать исключительную форму программы.

Анализатор сети обычно работает, переключая плату сетевого адаптера компьютера, на котором он запущен, в беспорядочный режим работы. Обычно сетевой адаптер исследует адрес назначения в заголовке протокола Канального уровня каждого пакета, достигающего компьютера, и если пакет адресован не этому компьютеру, сетевой адаптер игнорирует его. Это предотвращает обработку центральным процессором системы тысяч посторонних пакетов. Однако когда сетевой адаптер переключен в беспорядочный режим работы, он принимает все пакеты, приходящие в сети, вне зависимости от их адреса назначения, и передает их программе анализатора сети для обработки. Это позволяет системе анализировать не только трафик, созданный системой или предназначенный для системы с запущенным программным обеспечением анализатора, на также трафик, которым обмениваются другие системы в сети.

Когда приложение захватывает из сети трафик, оно сохраняет все пакеты в буфере, к которому в дальнейшем обращается во время анализа. В зависимости от размера сети и интенсивности передаваемого трафика, количество захваченных данных может быть неимоверно большим, поэтому обычно следует задавать размер буфера, чтобы контролировать количество захваченных данных. Также можно применять фильтры, чтобы ограничить типы данных, захватываемых анализатором.

Функции анализаторов протоколов делятся на анализ трафика и анализ протоколов. Каждая из этих функции рассмотрена далее более подробно.

Некоторые анализаторы сети могут отображать статистику о трафике в сети по мере его захвата, такую как количество пакетов в секунду, разбитых по рабочим станциям или протоколам. В зависимости от продукта, также возможно представление этой информации в графической форме. Так информацию можно использовать для определения количества трафика, создаваемого каждого системой сети или каждым протоколом.

Используя это средство, можно определить, какое количество пропускной способности сети расходуется определенным приложением или пользователем. При помощи фильтров захвата можно сконфигурировать анализатор сети для отправки администратору аварийных сигналов при возникновении в сети определенных условий. Некоторые продукты могут генерировать аварийные сигналы, когда трафик определенного типа достигает заданного уровня, например, когда в сети Ethernet возникает слишком много коллизий.

Помимо возможности захвата пакетов из сети, некоторые анализаторы также могут генерировать их сами. Можно использовать анализатор для имитации трафика определенной интенсивности, чтобы проверить рабочее состояние сети или оборудование, чувствительное к нагрузке.

После того как образец трафика помещен в буфер анализатора, можно исследовать пакеты более детально. В большинстве случаев пакеты, захваченные в течении периода взятия образцов трафика, отображаются хронологически в виде таблицы, где перечислены наиболее важные характеристики каждого пакета, такие как адреса системы назначения и источника и основной протокол, использованный для пакета. При выборе пакета из списка отображаются дополнительные панели с содержимым протокольных заголовков и данных пакета, обычно в необработанной и декодированной форме.

Первое применение для инструмента подобного типа заключается в том, что можно увидеть, какие типы трафика присутствуют в сети. Например, если сеть используют каналы связи глобальной сети, которые являются более медленными и дорогими по сравнению с соединениями локальной сети, можно использовать анализатор, чтобы захватить трафик, передаваемый по этим каналам, и убедиться в том, что их пропускная способность не расходуется попусту.

Когда проблема заключается в кабеле, формирующем сеть, требуются различные виды устройств, имеющие название «тестер кабеля». Тестеры кабеля обычно представляют собой удерживаемые в руках устройства, которые присоединяются к сети, чтобы выполнить различные диагностические тесты проводимости сетевого кабеля. Некоторые комбинированные тестеры можно присоединять к различным типам сетевого кабеля, таким как неэкранированная витая пара, экранированная витая пара и коаксиальный кабель, в то время как другие способны проверять только один тип кабеля. Для совершенно различных технологий передачи сигналов, таких как оптоволоконный кабель, необходимо отдельное устройство.

Тестеры кабеля рассчитываются на применение с определенными стандартами кабеля, поэтому они могут определить, соответствует ли производительность кабеля стандарту. Это называется испытанием презвонкой. Во время установки кабеля соответствующий специалист тестирует каждую связь, чтобы убедиться в её правильной работе, и проверяет отсутствие проблем, которые могут быть вызваны качеством самого кабеля или природы его установки.

Помимо проверки жизнеспособности разводки кабельной сети, тестеры кабеля являются хорошим средством для выявления проблем с кабелем. Например, тестер, функционирующий как рефлектометр, может определить обрыв или короткое замыкание в кабеле, передавая высокочастотный сигнал и измеряя количество времени, прошедшее до того момента, как отображенный сигнал вернется обратно. Используя эту технику можно определить, на каком расстоянии от тестера в кабеле произошел обрыв или возникла другая неисправность. Зная, что проблема расположена на расстоянии, например 20 м, можно избежать проверки каждого метра кабеля, идущего до этого места. Некоторые тестеры также могут помочь определить маршрут, по которому кабель проходит через стены или потолки. Для этого используется звуковой генератор, посылающий по кабелю сильный сигнал, который может уловить тестер, если будет расположен поблизости от кабеля.

**ВЫВОДЫ**

В данном дипломном проекте были сформулированы технико-экономическое обоснование анализа ЛВС, спроектирована структурная схема и схема прокладки кабеля ЛВС, спланированы основные мероприятия по обслуживанию сети и произведены экономические расчеты.

В дипломном проекте мною была проанализирована локальная сеть Службы по делам детей Северодонецкого городского совета и описаны основные мероприятия по администрированию и поиску неисправностей сети.

Анализ показал, что целями локальной сети Службы по делам детей Северодонецкого городского совета являются:

* совместная обработка информации;
* совместное использование сетевых ресурсов, таких как локальные диски, сетевой принтер, доступ в Интернет;
* централизованное управление компьютерами;
* централизованное резервное копирование всех данных;
* контроль за доступом к информации.

ЛВС создаст для пользователей новые возможности интегрального характера благодаря прикладным системам ПК и другому оборудованию сети.

Проанализировав сеть Службы по делам детей Северодонецкого городского совета можно сказать, что осуществление настройки сети выполняется с помощью системных средств MS Windows. При выполнении переустановки операционной системы на любой рабочей станции, сеть не утратит свою работоспособность, а лишь временно прекратит доступ к своим ресурсам.

После проделанной работы можно дать следующие рекомендации. В случае расширения средств компьютерной техники существует возможность подключения ее к локальной сети. Внедрение предложенных мероприятий не займут значительных денежных затрат в связи с тем, что такие преобразования уже заложены в структуру существующей локальной сети.

Также мною были расмотрены вопровы администирования сети, такие как настройка сетевого оборудования, настройка совместного доступа к ресурсам сети и выявление неисправностей и устранение сбоев в работе сети. Основой при выявления неисправностей чвляются встроенные утилиты операционной системы Windows. Они позволяют управлять учетными записями пользователей, управлять драйверами сетевых устройств, просматривать жернал событий, управлятьдоступом к общим ресурсам и файлов системы, просматривать информацию о состоянии сервера и статистики его производительности.

Можно сказать, что немаловажным инструментом являются анализаторы сети, которые управляют процессом обмена информации, производя анализ трафика и протоколов.

Большинство неиправностей сети связаны с порчей кабельной системы. Для выявления испорченного учакстка сети используются тестеры кабеля, которые могут определить обрыв или которкое замыкание в кабеле.

Локальная сеть имеет высокие технические характеристики, позволяющие значительно увеличить производительность труда работников предприятия и дает новые возможности для расширения деятельности, что для Службы по делам детей Северодонецкого городского совета особенно важно. Использование данной ЛВС дает годовой экономический эффект в сумме 112 554,42 грн. что разрешит окупить затраты в течение 6 месяцев.

В разделе охраны труда был произведен расчет отопления, вентиляции, природного и искусственного освещений. Сравнив их с нормативными значениями, сделала вывод, что все нормы охраны труда соблюдаются.

**Приложение А. Способы построения локальной сети**

|  |  |  |  |
| --- | --- | --- | --- |
| Параметры сети | Ethernet | Token Ring | Arcent |
| Стандарт | IEEE8023 | IEEE8025 | Datapaint |
| Типология | Шина | Кольцо | Шина |
| Скорость передачи | 100 Мбит/с | 16 Мбит/с | 25 Мбит/с |
| Длина | 5 км | 120 км | 6 км |
| Метод управления | CSMA/CD | Маркер | Маркер |
| Код | Манчестер | Биоразрядный | Arcent |
| Количество обв. | До 1024 | До 260 | До 255 |