СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Компьютерная сеть — это сложная система, включающая тысячи самых разнообразных компонентов: компьютеры разных типов, начиная с настольных и кончая мейнфремами, системное и прикладное программное обеспечение, сетевые адаптеры, концентраторы, коммутаторы и маршрутизаторы, кабельную систему. Основная задача системных интеграторов и администраторов состоит в том, чтобы эта громоздкая и весьма дорогостоящая система как можно лучше справлялась с обработкой потоков информации, циркулирующих между сотрудниками предприятия и позволяла принимать им своевременные и рациональные решения, обеспечивающие «выживание» предприятия в жесткой конкурентной борьбе. А так как жизнь не стоит на месте, то и содержание корпоративной информации, интенсивность ее потоков и способы ее обработки постоянно меняются. Последний пример резкого изменения технологии автоматизированной обработки корпоративной информации у всех на виду - он связан с беспрецедентным ростом популярности Internet в последние годы.

Изменения, причиной которых стал Internet, многогранны. Гипертекстовая служба WWW изменила способ представления информации человеку, собрав на своих страницах все популярные ее виды - текст, графику и звук. Транспорт Internet - недорогой и доступный практически всем предприятиям (и через телефонные сети, и одиночным пользователям) - существенно облегчил задачу построения территориальной корпоративной сети, одновременно выдвинув на первый план задачу защиты корпоративных данных при передаче их через (в высшей) степени общедоступную публичную сеть с многомиллионным "населением". Стек TCP/IP сразу же вышел на первое место, потеснив прежних лидеров локальных сетей IPX и NetBIOS, а в территориальных сетях - X.25.

Популярность Internet оказывает на компьютерные сети не только техническое и технологическое влияние. Так как Internet постепенно становится общемировой сетью интерактивного взаимодействия людей, то Internet начинает все больше и больше использоваться не только для распространения информации, в том числе и рекламной, но и для осуществления самих деловых операций - покупки товаров и услуг, перемещения финансовых активов и т.п. Это в корне меняет для многих предприятий саму канву ведения бизнеса, так как появляются миллионы потенциальных покупателей, которых нужно снабжать рекламной информацией, тысячи интересующихся продукцией клиентов, которым нужно предоставлять дополнительную информацию и вступать в активный диалог

через Internet, и, наконец, сотни покупателей, с которыми нужно совершать электронные сделки. Сюда нужно добавить и обмен информацией с предприятиями-соисполнителями или партнерами по бизнесу. Изменения схемы ведения бизнеса меняют и требования, предъявляемые к корпоративной сети. Например, использование технологии Intranet сломало привычные пропорции внутреннего и внешнего трафика предприятия в целом и его подразделений - старое правило, гласящее, что 80% трафика является внутренним и только 20% идет вовне, сейчас не отражает истинного положения дел. Интенсивное обращение к Web-сайтам внешних организаций и других подразделений предприятия резко повысило долю внешнего трафика и, соответственно, повысило нагрузку на пограничные маршрутизаторы и межсетевые экраны (firewalls) корпоративной сети. Другим примером влияния Internet на бизнес-процессы может служить необходимость аутентификации и авторизации огромного числа клиентов, обращающихся за информацией на серверы предприятия извне. Старые способы, основанные на заведении учетной информации на каждого пользователя в базе данных сети и выдаче ему индивидуального пароля, здесь уже не годятся - ни администраторы, ни серверы аутентификации сети с таким объемом работ не справятся. Поэтому появляются новые методы проверки легальности пользователей, заимствованные из практики организаций, имеющих дело с большими потоками клиентов - магазинов, выставок и т.п. Влияние Internet на корпоративную сеть — это только один, хотя и яркий, пример постоянных изменений, которые претерпевает технология автоматизированной обработки информации на современном предприятии, желающем не отстать от конкурентов. Постоянно появляются технические, технологические и организационные новинки, которые необходимо использовать в корпоративной сети для поддержания ее в состоянии, соответствующем требованиям времени. Без внесения изменений корпоративная сеть быстро морально устареет и не сможет работать так, чтобы предприятие смогло успешно выдерживать жесткую конкурентную борьбу на мировом рынке. Как правило, срок морального старения продуктов и решений в области информационных технологий находится в районе 3 - 5 лет.

Стратегическое планирование сети состоит в нахождении компромисса между потребностями предприятия в автоматизированной обработке информации, его финансовыми возможностями и возможностями сетевых и информационных технологий сегодня и в ближайшем будущем.

1 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

Если в одном помещении, здании или комплексе близлежащих зданий имеется несколько компьютеров, пользователи которых должны совместно решать какие-то задачи, обмениваться данными или использовать общие данные, то эти компьютеры целесообразно объединить в локальную сеть.

Локальная сеть – это группа из нескольких компьютеров, соединенных посредством кабелей (иногда также телефонных линий или радиоканалов), используемых для передачи информации между компьютерами. Для соединения компьютеров в локальную сеть необходимо сетевое оборудование и программное обеспечение.

Назначение всех компьютерных сетей можно выразить двумя словами: совместный доступ (или совместное использование). Прежде всего, имеется в виду совместный доступ к данным. Людям, работающим над одним проектом, приходится постоянно использовать данные, создаваемые коллегами. Благодаря локальной сети разные люди могут работать над одним проектом не по очереди, а одновременно.

Локальная сеть предоставляет возможность совместного использования оборудования. Часто дешевле создать локальную сеть и установить один принтер на все подразделение, чем приобретать по принтеру для каждого рабочего места. Файловый сервер сети позволяет обеспечить совместный доступ к программам.

Оборудование, программы и данные объединяют одним термином: ресурсы. Можно считать, что основное назначение локальной сети – доступ к ресурсам.

У локальной сети есть также и административная функция. Контролировать ход работ над проектами в сети проще, чем иметь дело со множеством автономных компьютеров. Если в учебном классе есть локальная сеть, то она тоже выполняет административную функцию, позволяя контролировать ход занятий учащихся.

Для связи с внешними (периферийными) устройствами компьютер имеет порты, через которые он способен передавать и принимать информацию. Нетрудно догадаться, что если через эти порты соединить два или несколько компьютеров, то они смогут обмениваться информацией между собой. В этом случае они образуют компьютерную сеть. Если компьютеры находятся недалеко друг от друга, используют общий комплект сетевого оборудования и управляются одним пакетом программного обеспечения, то такую компьютерную сеть называют локальной. Простейшие локальные сети

используют для обслуживания рабочих групп. Рабочая группа – это группа лиц, работающих над одним проектом (например, над выпуском одного журнала или над разработкой одного самолета) или просто сотрудники одного подразделения.

Корпоративную сеть целесообразно рассмотреть, как сложную систему, состоящую из нескольких взаимодействующих слоев. В основании пирамиды, представляющей корпоративную сеть, лежит слой компьютеров - центров хранения и обработки информации, и транспортная подсистема (рис. 1), обеспечивающая надежную передачу информационных пакетов между компьютерами.

Рисунок 1

Иерархия слоев корпоративной сети

Над транспортной системой работает слой сетевых операционных систем, который организует работу приложений в компьютерах и предоставляет через транспортную систему ресурсы своего компьютера в общее пользование.

Над операционной системой работают различные приложения, но из-за особой роли систем управления базами данных, хранящих в упорядоченном виде основную корпоративную информацию и производящих над ней базовые операции поиска, этот класс системных приложений обычно выделяют в отдельный слой корпоративной сети.

На следующем уровне работают системные сервисы, которые, пользуясь СУБД, как инструментом для поиска нужной информации среди миллионов и миллиардов байт, хранимых на дисках, предоставляют конечным пользователям эту информацию в удобной для принятия решения форме, а также выполняют некоторые общие для предприятий всех типов процедуры обработки информации. К этим сервисам относится служба WorldWideWeb, система электронной почты, системы коллективной работы и многие другие.

Верхний уровень корпоративной сети представляет специальные

программные системы, которые выполняют задачи, специфические для данного предприятия или предприятий данного типа. Такими системами могут служить системы автоматизации банка, организации бухгалтерского учета, автоматизированного проектирования, управления технологическими процессами и т.п.

Конечная цель корпоративной сети воплощена в прикладных программах верхнего уровня, но для их успешной работы абсолютно необходимо, чтобы подсистемы других слоев четко выполняли свои функции.

Стратегические решения, как правило, влияют на облик сети в целом, затрагивая несколько слоев сетевой "пирамиды", хотя первоначально касаются только одного конкретного слоя или даже отдельной подсистемы этого слоя. Такое взаимное влияние продуктов и решений следует обязательно учитывать при планировании технической политики развития сети, иначе существует большая вероятность столкнуться с необходимостью срочной и непредвиденной замены, например, сетевой технологии, из-за того, что новая прикладная программа испытывает острый дефицит пропускной способности для своего трафика.

Адресация компьютеров в сети

Каждый компьютер, работающий по протоколу TCP/IP, обязательно имеет IP-адрес— 32-битное число, используемое для идентификации узла (компьютера) в сети. Адрес принято записывать десятичными значениями каждого октета этого числа с разделением полученных значений точками. Например: 192.168.101.36.

IP-адреса уникальны. Это значит, что каждый компьютер имеет свое сочетание цифр, и в сети не может быть двух компьютеров с одинаковыми адресами. IP-адреса распределяются централизованно. Интернет-провайдеры дела ют заявки в национальные центры в соответствии со своими потребностями Полученные провайдерами диапазоны адресов распределяются далее между клиентами. Клиенты сами могут выступать в роли интернет-провайдера и распределять полученные IP-адреса между субклиентами и т.д. При таком способе распределения IP-адресов компьютерная система точно знает «расположение» компьютера, имеющего уникальный IP-адрес; ей достаточно переслать данные в сеть «владельца». Провайдер в свою очередь проанализирует пункт назначения и, зная, кому отдана эта часть адресов, отправит информацию следующему владельцу поддиапазона IP-адресов, пока данные не поступят на компьютер назначения.

Выделение диапазона адресов осуществляется бесплатно, но организация получившая адреса, должна реально подтвердить их

использование через определённый промежуток времени.

Для построения локальных сетей организаций выделены специальные диапазоны адресов. Это адреса 10.x.x.x, 192.168.x.x, 10.x.x.x, с 172.16.x.x по 172.31.x.x, 169.254.X.X. Пакеты, передаваемые с указанных адресов, не маршрутизируются (иными словами, не пересылаются) через Интернет, поэтому в различных локальных сетях компьютеры могут иметь совпадающие адреса из указанных диапазонов. Для пересылки информации с таких компьютеров в Интернет и обратно используются специальные программы, «на лету» заменяющие локальные адреса реальными при работе с Интернетом. Иными словами, данные в Сеть пересылаются от реального IP-адреса. Этот процесс происходит «незаметно» для пользователя. Такая технология называется трансляцией адресов.

Кабельная система

Выбор кабельной подсистемы диктуется типом сети и выбранной топологией. Требуемые же по стандарту физические характеристики кабеля закладываются при его изготовлении, о чем и свидетельствуют нанесенные на кабель маркировки. В результате, сегодня практически все сети проектируются на базе UTP и волоконно-оптических кабелей, коаксиальный кабель применяют лишь в исключительных случаях и то, как правило, при организации низкоскоростных стеков в монтажных шкафах.

В проекты локальных вычислительных сетей (стандартных) закладываются на сегодня всего виды кабелей:

- коаксиальный (двух типов):
  Тонкий коаксиальный кабель (thin coaxial cable);
  Толстый коаксиальный кабель (thick coaxial cable).
- витая пара (двух основных типов):
  Неэкранированная витая пара (unshielded twisted pair - UTP);
  Экранированная витая пара (shielded twisted pair - STP).
- волоконно-оптический кабель (двух типов):
  Многомодовый кабель (fiber optic cable multimode);
  Одномодовый кабель (fiber optic cable single mode).

Не так давно коаксиальный кабель был самым распространенным типом кабеля. Это объясняется двумя причинами: во-первых, он был относительно недорогим, легким, гибким и удобным в применении; 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, 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.

Оплетка, ее называют экраном, защищает передаваемые по кабелям данные, поглощая внешние электромагнитные сигналы, называемые помехами или шумом, таким образом, экран не позволяет помехам исказить данные.

Электрические сигналы передаются по жиле. Жила – это один провод или пучок проводов. Жила изготавливается, как правило, из меди. Проводящая жила и металлическая оплетка не должны соприкасаться, иначе произойдет короткое замыкание и помехи исказят данные.

Коаксиальный кабель более помехоустойчивый, затухание сигнала в нем меньше, чем в витой паре.

Затухание – это уменьшение величины сигнала при его перемещении по кабелю.

Тонкий коаксиальный кабель – гибкий кабель диаметром около 5 мм. Он применим практически для любого типа сетей. Подключается непосредственно к плате сетевого адаптера с помощью Т-коннектора.

У кабеля разъемы называются BNC коннекторы. Тонкий коаксиальный кабель способен передавать сигнал на расстоянии 185 м, без его замедленного затухания.

Тонкий коаксиальный кабель относится к группе, которая называется семейством RG– 58. Основная отличительная особенность этого семейства медная жила.

RG 58/U – сплошная медная жила.

RG 58/U – переплетенные провода.

RG 58 C/U- военный стандарт.

RG 59 – используется для широкополосной передачи.

RG 62 – используется в сетях Archet.

Толстый коаксиальный кабель относительно жесткий кабель с диаметром около 1 см. Иногда его называют стандартом Ethernet, потому что этот тип кабеля был предназначен для данной сетевой архитектуры. Медная жила этого кабеля толще, чем у тонкого кабеля, поэтому он передает сигналы дальше. Для подключения к толстому кабелю применяют специальное устройство трансивер.

Трансивер снабжен специальным коннектором, который называется

«зуб вампира» или пронзающий ответвитель. Он проникает через изоляционный слой и вступает в контакт с проводящей жилой. Чтобы подключить трансивер к сетевому адаптеру надо кабель трансивера подключить к коннектору AUI – порта к сетевой плате.

Витая пара – это два перевитых вокруг друг друга изоляционных медных провода. Существует два типа тонкого кабеля: неэкранированная витая пара (UTP) и экранированная витая пара (STP).

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 (двигателями, трансформаторами).

Неэкранированная витая пара (спецификация 10 Base T) широко используется в ЛВС, максимальная длина сегмента составляет 100 м.

Неэкранированная витая пара состоит из 2х изолированных медных проводов. Существует несколько спецификаций, которые регулируют количество витков на единицу длины – в зависимости от назначения кабеля.

1) Традиционный телефонный кабель, по которому можно передавать только речь.

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

3) Кабель, способный передавать данные со скоростью до 10 Мбит/с. Состоит из 4х витых пар с 9-ю витками на метр.

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

5) Кабель, способный передавать данные со скоростью до 100 Мбит/с. Состоит из 4х витых пар медного провода.

Одной из потенциальных проблем для всех типов кабелей являются перекрестные помехи.

Перекрестные помехи – это перекрестные наводки, вызванные сигналами в смежных проводах. Неэкранированная витая пара особенно страдает от этих помех. Для уменьшения их влияния используют экран.

Кабель, экранированной витой пары (STP) имеет медную оплетку, которая обеспечивает большую защиту, чем неэкранированная витая пара. Пары проводов STP обмотаны фольгой. В результате экранированная витая пара обладает прекрасной изоляцией, защищающей передаваемые данные от внешних помех.

Следовательно, STP по сравнению с UTP меньше подвержена воздействию электрических помех и может передавать сигналы с большей

скоростью и на большие расстояния.

Для подключения витой пары к компьютеру используют коннекторы RG- 45.

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 скрыть 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 стеклянный цилиндр, называемый жилой, покрытый слоем стекла, называемого оболочкой, с иным, чем у жилы, коэффициентом преломления. Иногда оптоволокно производят из пластика, он проще в использовании, но имеет худшие характеристики по сравнению со стеклянным.

Каждое стеклянное оптоволокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон с отдельными коннекторами. Одно из них служит для передачи сигнала, другой для приема.

Передача по оптоволоконному кабелю не подвержена электрическим помехам и ведется с чрезвычайно высокой скоростью (в настоящее время до 100Мбит/сек, теоретически возможная скорость – 200000 Мбит/сек). По нему можно передавать данные на многие километры.

Обзор и анализ возможных технологий для решения поставленной задачи

Рассмотрим ряд технологических решений локальных сетей.

Локальная сеть Ethernet.

Спецификацию Ethernet в конце семидесятых годов XX века предложила компания Xerox Corporation. Позднее к этому проекту присоединились компании Digital Equipment Corporation (DEC) и Intel Corporation. В 1982 г. была опубликована спецификация на Ethernet версии 2.0. На базе Ethernet Институтом IEEE был разработан стандарт IEEE 802.3.

На логическом уровне в Ethernet применяется шинная топология:

- 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.

В стандарте Ethernet, помимо топологии шина, используется пассивная звезда и пассивное дерево (сетевое устройство, соединяющие сегменты сети – репитеры, репитерные концентраторы).

Метод доступа Ethernet является методом множественного доступа с прослушиванием несущей и разрешением коллизий (конфликтов) – CSMA/CD (Carier Sense Multiple Access with Collision Detection) и был предложен Xerox в 1975 г.

Поскольку в системе используется топология «общая шина», сообщение, отправляемое одной рабочей станцией, принимается одновременно всеми остальными, подключенными к общей шине. Сообщение, предназначенное только для одной станции, принимается этой станцией и игнорируется остальными. Перед началом рабочая станция определяет, свободен канал или занят. Если канал свободен, станция начинает передачу. Главное требование к такой топологии – отсутствие петель (нет замкнутых путей).

Ethernet не исключает возможности одновременной передачи сообщений двумя или несколькими станциями. Аппаратура автоматически распознает коллизии (конфликты). После обнаружения конфликта станции задерживают передачу на некоторое время. Это время небольшое и для каждой станции свое. После задержки передачи возобновляется. Реально конфликты приводят к уменьшению быстродействия сети только в том случае, если работает порядка 80 – 100 станций.

При увеличении числа пользователей сеть будет работать не столь эффективно. В этом случае оптимальное решение состоит в увеличении числа сегментов для обслуживания групп с меньшим числом пользователей. Передаваемые в сети Ethernet пакеты могут иметь переменную длину.

В качестве сегмента сети может выступать шина или единичный абонент. Для шинных сегментов используют коаксиальный кабель, а для лучей пассивный пассивной звезды – витую пару или оптоволокно (им присоединяют к концентратору одиночные ПК).

- форматы сети Ethernet при скорости 10 Мбит/сек:
- 10 Base-T – витая пара;
- 10 Base5 – толстый коаксиальный кабель;
- 10 Base2 – тонкий коаксиальный кабель;
- 10 Base-FL – оптоволокно.

Развитие технологии Ethernet все больше отходит от первоначального стандарта: используются новые среды передачи, коммутаторы вместо

концентраторов, отказ от манчестерского кода и от метода управления CSMA/CD.

Fast Ethernet

В сети Fast Ethernet применяется та же базовая технология, что и в Ethernet – множественный доступ с контролем несущей и обнаружением конфликтов. Обе технологии основаны на стандарте IEEE 802.3. В результате для создания сетей обоих типов можно использовать одинаковый тип кабеля, сетевые устройства и приложения. Сети Fast Ethernet позволяют передавать данные со скоростью 100 Мбит/сек, т.е. в десять раз быстрее чем Ethernet.

В сети Fast Ethernet в отличие от Ethernet используется только пассивная звезда и пассивное дерево. К тому же в Fast Ethernet более жесткие требования к длине сети, например, увеличение сети в 10 раз приводит к уменьшению в 10 раз допустимой величины прохождения сигнала по сети.

Форматы сети Fast Ethernet при скорости 100 Мбит/сек:

- 100 Base-T4 – счетверенная витая пара;
- 100 Base-TX – сдвоенная витая пара;
- 100 Base-FX – оптоволокно.

Gigabit Ethernet

Продолжение развития сетей Ethernet и Fast Ethernet. Gigabit Ethernet совместимы с сетевой инфраструктурой Ethernet и Fast Ethernet, но функционируют со скоростью 1000 Мбит/сек – что в 10 раз быстрее, чем Fast Ethernet. Сеть Gigabit Ethernet является наследницей сети Ethernet, соответственно берет все достоинства и недостатки этой сети.

Сохранение преемственности сетей Ethernet, Fast Ethernet и Gigabit Ethernet позволяет просто соединить сегменты сетей в единую сеть, при этом переходить к новым скоростям постепенно, вводя гигабитные сегменты только на самых напряженных участках сети.

Сеть Gigabit Ethernet сохраняет метод доступа CSMA/CD, в нем используется те же форматы пакетов и те же размеры, что в Ethernet и Fast Ethernet (это дополнительный плюс в местах соединения с этими сегментами). Единственно, что нужно при соединении сегментов – согласование скоростей обмена, соединение сегментов идет через коммутаторы.

Работа по созданию сети Gigabit Ethernet ведется с 1995 г. В 1998 г. был принят стандарт, получивший название IEEE 802.3z, включивший в себя виды сети Gigabit Ethernet.В 1999 г. принят стандарт IEEE 802.3ab, включивший в себя вид сети Gigabit Ethernet 1000 Base-T.

Виды сегментов сети Gigabit Ethernet:

- 1000 Base-SX – сегмент на оптоволоконном кабеле с длиной волны светового сигнала до 500м, используются лазерные передатчики;
- 1000 Base-LX – сегмент на оптоволоконном кабеле с длиной волны светового сигнала до 1300м, используются лазерные передатчики;
- 1000 Base-CX – сегмент на экранированной витой паре длиной до 25км;
- 1000 Base-T – сегмент на счетверенной неэкранированной витой паре длиной до 100м, используется пятиуровневое кодирование и полнодуплексный режим передачи.

Передача в Gigabit Ethernet производится в полудуплексном режиме и полнодуплексном режиме. Полнодуплексный режим не налагает ограничения на длину сети (кроме ограничений, связанных с затуханием сигнала) и обеспечивает отсутствие конфликтов, этот режим станет в будущем основным для Gigabit Ethernet.

Сеть Gigabit Ethernet с ее огромной пропускной способностью не всегда может решить некоторые задачи, предлагается новая версия – 10 Gigabit Ethernet IEEE 802.3ae, принятая в 2002 г. Ее принципиальные отличия от предыдущих версий: в качестве среды передачи используется только оптоволокно, полнодуплексный режим обмена, единственно, что остается от изначального Ethernet – формат пакета.

На современном этапе формирования и использования ЛВС наиболее актуальное значение приобрели такие вопросы, как оценка производительности и качества ЛВС и их компонентов, оптимизация уже существующих или планируемых к созданию ЛВС. Сейчас, когда локальные вычислительные сети стали важной частью в информационной стратегии множества предприятий, недостаточное внимание к оценке мощности ЛВС и ее планированию привело к тому, что сегодня для поддержки современных приложений в архитектуре клиент- сервер многие сети необходимо проектировать с основы, а во многих случаях и заменять.

Производительность и пропускная способность ЛВС определяется рядом факторов:

– кабельная система;

– сервер и его конфигурация, рабочие станции;

– каналы связи, сетевое оборудование;

– сетевые операционные системы и операционные системы рабочих станций;

– организация распределенного вычислительного процесса;

– защита поддержания и восстановления работоспособности в

ситуациях сбоев и отказов.

В основе работы глобальной сети Интернет лежит набор (стек) протоколов TCP/IP. Стек протоколов TCP/IP — набор сетевых протоколов передачи данных, используемых в сетях, включая сеть Интернет. Название TCP/IP происходит из двух наиважнейших протоколов семейства — TransmissionControlProtocol (TCP) и InternetProtocol (IP), которые были разработаны и описаны первыми в данном стандарте. Протокол IP — это протокол, описывающий формат пакета данных, передаваемого по сети. Протокол TCP — это протокол следующего уровня, предназначеный для контроля передачи и целостности передаваемой информации. Стек протоколов TCP/IP включает в себя четыре уровня: -прикладной уровень (applicationlayer), транспортный уровень (transportlayer), сетевой уровень (Internetlayer), канальный уровень (linklayer). Протоколы этих уровней полностью реализуют функциональные возможности модели OSI. На стеке протоколов TCP/IP построено всё взаимодействие пользователей в IP-сетях. Стек является независимым от физической среды передачи данных. На прикладном уровне (Applicationlayer) работает большинство сетевых приложений. Эти программы имеют свои собственные протоколы обмена информацией, например, HTTP для WWW, FTP (передача файлов), SMTP (электронная почта), SSH (безопасное соединение с удалённой машиной), DNS (преобразование символьных имён в IP-адреса) и многие другие. В массе своей эти протоколы работают поверх TCP или UDP и привязаны к определённому порту, например:на TCP-порт 80 или 8080, FTP на TCP-порт 20 (для передачи данных) и 21 (для управляющих команд), SSH на TCP-порт 22, запросы DNS на порт UDP (реже TCP) 53, обновление маршрутов по протоколу RIP на UDP-порт 520.

Протоколы транспортного уровня (Transportlayer) могут решать проблему негарантированной доставки сообщений («дошло ли сообщение до адресата?»), а также гарантировать правильную последовательность прихода данных. В стеке TCP/IP транспортные протоколы определяют, для какого именно приложения предназначены эти данные. Протоколы автоматической маршрутизации, логически представленные на этом уровне (поскольку работают поверх IP), на самом деле являются частью протоколов сетевого уровня; например OSPF (IP идентификатор 89). Сетевой уровень (Internetlayer) изначально разработан для передачи данных из одной (под)сети в другую. Примерами такого протокола является X.25 и IPC в сети ARPANET. С развитием концепции глобальной сети в уровень были внесены дополнительные возможности по передаче из любой сети в любую сеть,

независимо от протоколов нижнего уровня, а также возможность запрашивать данные от удалённой стороны, например в протоколе ICMP (используется для передачи диагностической информации IP-соединения) и IGMP (используется для управления multicast-потоками). Канальный уровень (Linklayer) описывает, каким образом передаются пакеты данных через физический уровень, включая кодирование (то есть специальные последовательности бит, определяющих начало и конец пакета данных). Ethernet, например, в полях заголовка пакета содержит указание того, какой машине или машинам в сети предназначен этот пакет. Примеры протоколов канального уровня — Ethernet, IEEE 802.11 WirelessEthernet, SLIP, TokenRing, ATM и MPLS.

Обеспечение информационной безопасности в сети

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п. Поскольку утрата информации может происходить по сугубо техническим, объективным и неумышленным причинам, под это определение подпадают также и мероприятия, связанные с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

Переход от работы на персональных компьютерах к работе в сети усложняет защиту информации по следующим причинам:

большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц;

значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть;

уже отмеченные недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на предпродажном этапе, называемом бета- тестированием, а в процессе эксплуатации. В том числе неидеальны встроенные средства защиты информации даже в таких известных и "мощных" сетевых ОС, как Windows NT или NetWare.

Возможна утечка информации по каналам, находящимся вне сети:

хранилище носителей информации, элементы строительных конструкций и окна помещений, которые образуют каналы утечки конфиденциальной информации за счет так называемого микрофонного эффекта, телефонные, радио-, а также иные проводные и беспроводные каналы (в том числе каналы мобильной связи).

Любые дополнительные соединения с другими сегментами или подключение к Интернет порождают новые проблемы. Атаки на локальную сеть через подключение к Интернету для того, чтобы получить доступ к конфиденциальной информации, в последнее время получили широкое распространение, что связано с недостатками встроенной системы защиты информации в протоколах TCP/IP. Сетевые атаки через Интернет могут быть классифицированы следующим образом:

Сниффер пакетов (sniffer – в данном случае в смысле фильтрация) – прикладная программа, которая использует сетевую карту, работающую в режиме promiscuous (не делающий различия) mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки).

IP-спуфинг (spoof – обман, мистификация) – происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя.

Отказ в обслуживании (Denial of Service – DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

Парольные атаки – попытка подбора пароля легального пользователя для входа в сеть.

Атаки типа Man-in-the-Middle – непосредственный доступ к пакетам, передаваемым по сети.

Атаки на уровне приложений.

Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений.

Злоупотребление доверием внутри сети.

Несанкционированный доступ (НСД), который не может считаться отдельным типом атаки, так как большинство сетевых атак проводятся ради получения несанкционированного доступа.

Реализация данной работы, произведенная с учетом всех вышеперечисленных факторов, позволит сократить бумажный документооборот внутри отдела управления организации, повысить производительность труда, сократить время на получение и обработку информации, выполнять точный и полный анализ данных, обеспечивать получение любых форм отчетов по итогам работы. Как следствие, образуются дополнительные временные ресурсы для разработки и реализации новых проектов.

2. ПРОЕКТИРОВАНИЕ ЛВС

Задание: Разработка технического предложения локально-вычислительной сети железнодорожной станции «Новогиреево»

Дано:

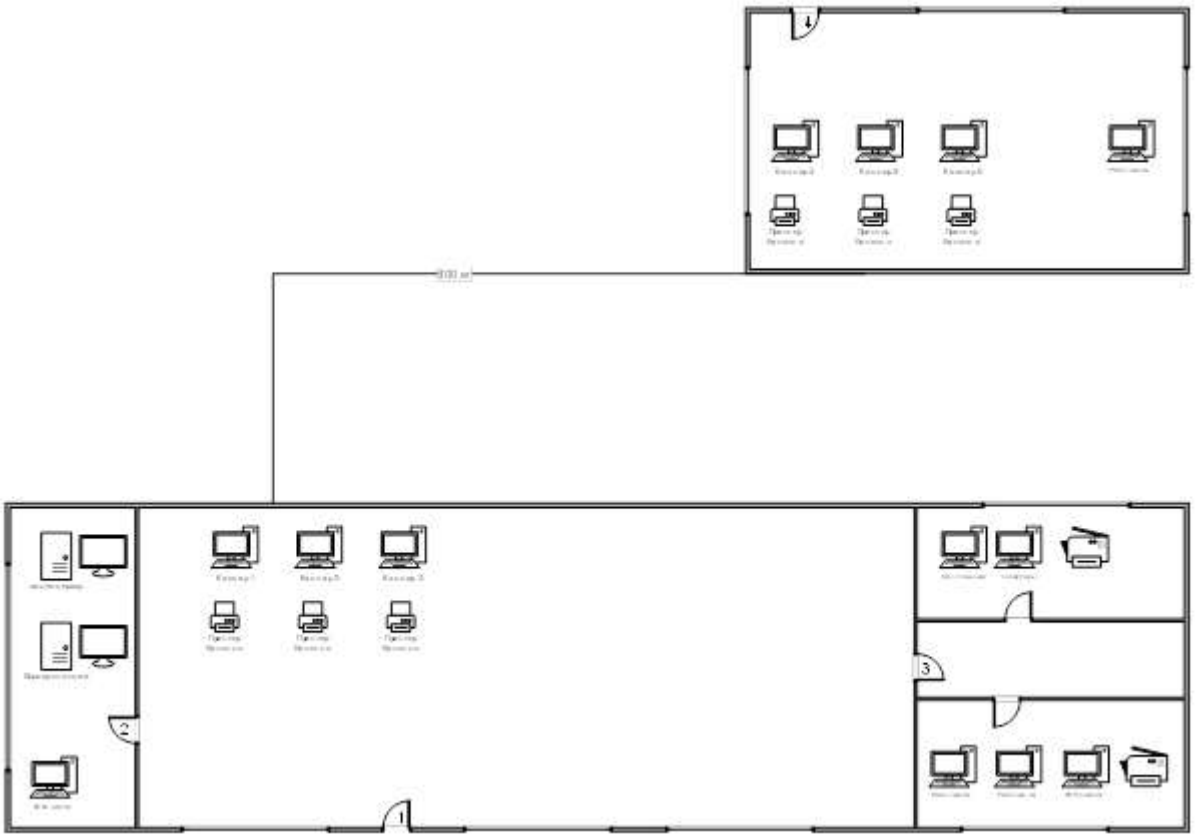
1) В связи с реконструкцией станции Новогиреево, следует разработать систему локально-вычислительной сети. Имеется два помещения: в-первом расположены – [1] зал ожидания и кассы, [2] серверная комната и [3] комната руководства станции; во-втором только кассы;
2) В помещении [4] – 5 компьютеров, 4 из них осуществляют роль касс и 1 для работников станции; в помещении [3] – 5 ПК и 2 МФУ; в серверной – два сервера – сервер станции и сервер видеонаблюдения;

Необходимо:

Организовать полноценную локально-вычислительную сеть с выходом в сеть Интернет, а также предусмотреть возможность совместного использования сетевых ресурсов (принтеров) всеми полномочными пользователями сети.

Рисунок 2

План помещений станции.



Выбор топологии сети

В качестве физической топологии выберем топологию распределенной звезды. В помещениях будет расположено 3 коммутатора, и по 1 модему в каждом здании. Связь между зданиями будет организована посредством VPN. В первом помещении имеется 16 устройств, подключаемых к сети, следовательно коммутатор должен иметь 17 портов, будет применен коммутатор на 24 порта. Во втором помещении имеется 8 сетевых устройств, следовательно коммутатор с учетом запаса нужно использовать на 16 портов. Итого в обоих помещениях в сумме 25 сетевых устройств. Сеть будет состоять из 3 звезд, соединенных между собой посредством модемов и кабеля в первом помещении.

Для соединения сетевых устройств используется кабель UTP и для его соединения с оконечными устройствами понадобится 25 розеток RJ45. Каждое рабочее место должно быть оборудовано минимум двумя розетками электрической сети для питания компьютеров и 1 электрической розеткой бытового применения.

Определение необходимого количества кабеля

Для подсчета длина необходимого кабеля можно использовать 2 метода.

Метод суммирования заключается в подсчете длины трассы каждого горизонтального кабеля с последующим сложением этих длин. К полученному результату добавляется технологический запас величиной до 13%, а также запас для выполнения разделки в розетках и на кроссовых панелях. Достоинством рассматриваемого метода является высокая точность. Однако при отсутствии средств автоматизации и проектировании компьютерных сетей с большим количеством портов такой подход оказывается чрезмерно трудоемким, что практически исключает, в частности, просчет нескольких вариантов организации кабельной системы. Он может быть рекомендован для использования только в случае проектирования сетей с небольшим количеством компьютеров.

Общий расчет кабеля методом суммирования вычисляется по формуле:

$$Li = (l1 + l2 + \cdots + \ln) * 1{,}3 (1)$$

где n – количество компьютеров; l – длина сегмента кабеля;

Ks - коэффициент технологического запаса – 1,3 (13%), который учитывает особенности прокладки кабеля, всех спуски, подъемы, повороты, межэтажные сквозные проемы (при их наличии) и также запас для выполнения разделки кабеля.

Длина кабеля, необходимого для каждого помещения, равна сумме длин сегментов всех узлов этого помещения, умноженного на коэффициент технологического запаса.

Эмпирический метод дает хорошие результаты для кабельных систем с числом рабочих мест свыше 30. Его сущность заключается в применении

для подсчета общей длины горизонтального кабеля, затрачиваемого на реализацию конкретной сети, обобщенной эмпирической формулы.

Согласно этому методу, средняя длина кабеля $L_{ср,}$ принимается равной

$$Lcp = (Lмин + Lмакс) / 2 * 1,1 + X \quad (2)$$

где Lmin и Lmax - длина кабельной трассы от точки ввода кабельных каналов в кроссовую до телекоммуникационной розетки соответственно самого близкого и самого далекого рабочего места, рассчитанная с учетом особенностей прокладки кабеля, всех спусков, подъемов, поворотов, межэтажных сквозных проемов (при их наличии) и т.д.;

Ks - коэффициент технологического запаса – 1,1 (10%);

X = X1 + X2 - запас для выполнения разделки кабеля. Со стороны рабочего места (X1) он принимается равным 30 см. Со стороны кроссовой - X2 – он зависит от ее размеров и численно равен расстоянию от точки входа горизонтальных кабелей в помещение кроссовой до самого дальнего коммутационного элемента опять же с учетом всех спусков, подъемов и поворотов.

Расчет кабель-канала проводится по периметру каждого помещения, затем все суммируется.

Для нашего случая будем использовать эмпирический метод для каждого помещения раздельно.

Расчет длины кабеля для первого помещения.

Для этого помещения максимальный сегмент кабеля имеет длину 22 метров, минимальный – 1 метр. Запас на разделку кабеля положим в 0,4м. Подставим эти значения в формулу (2). Тогда

$$Lcp=(22+1)/2*1.1+0.4=13,05м.$$

В помещении А находится 15 устройств, таким образом необходимая длина кабеля:

$$Lобщ=13,05*17=221,85м.$$

Расчет длины кабеля для второго помещения.

Для этого помещения максимальный сегмент кабеля имеет длину 13 метров, минимальный – 1 метр. Запас на разделку кабеля положим в 0,4м. Подставим эти значения в формулу (2). Тогда

$$Lcp=(8+1)/2*1.1+0.4=5,35м.$$

В помещении Б находится 7 устройств, таким образом необходимая длина кабеля:

$$Lобщ=5,35*8=42,8м.$$

Общая длина кабеля необходимого для обоих помещений составит

LАБ=42,8+221,85=264,65м.

Округлим общую длину кабеля до 265м.

Рассчитаем длину кабель-канала, с учетом того, что ему не нужен запас на разделку.

Lкаб=215,05+39,6=254,65м.

Округлим общую длину кабель-канала до 255 м.

Список необходимого оборудования представлен в таблице 1.

Таблица 1.

Список необходимого оборудования

№ п/п	Оборудование	Количество	Ед. Изм.
1	Коммутатор	3	Шт.
2	Модем	2	Шт.
3	Кабель	265	М.
4	Розетка RJ-45	25	Шт.
5	Патч-корд	25	Шт.
6	Кабель-канал	255	М.

Выбор программного обеспечения

В качестве операционной системы для сервера выберем ОС Windows Server 2019.

Серверная ОС Windows – представитель семейства сетевого ПО Windows Network, разработанное Microsoft одновременно с обычно операционной системой Windows 10. К ее преимуществам относят:

- высокий запас по производительности;
- огромное количество программного обеспечения, доступного для скачивания;
- высокий уровень безопасности (относится как к защите от вредоносного ПО, так и от атак на виртуальные машины);
- возможность индивидуальной разработки ПО (обеспечивается поддержкой контейнеризации Kubernetes, широкими возможностями для масштабирования);
- работа с Windows Subsystem for Linux: позволяет разрабатывать ПО для операционной системы Linux, включая и виртуальные машины.

Серверные ОС Windows Server оптимально подходит для взаимодействия с разноплановым программным обеспечением, файловыми, почтовыми серверами.

Клиентская операционная система осуществляет две основные функции: она предоставляет пользователю ряд тех или иных сервисов и управляет ресурсами компьютера, на котором она выполняется. Собственно, выбор операционной системы и определяется, во-первых, тем, какие у нее имеются ресурсы, а во-вторых, тем, какие сервисы требуются пользователю, — не все операционные системы способны работать с тем или иным аппаратным обеспечением, да и запросы пользователя (в том числе корпоративного) порой бывают столь высоки, что выбор операционных систем, способных их удовлетворить, оказывается весьма невелик.

Перечислим наиболее часто встречающиеся потребности корпоративного пользователя:

Возможность применять офисные приложения (то есть готовить документы с помощью текстовых процессоров, электронных таблиц, средств презентационной графики и т.д.).

Возможность обращаться к ресурсам локальной сети и Интернета (например, к сетевым принтерам, файлам на сетевом диске или на Web-сайтах, к Web-приложениям и почтовым серверам).

Возможность пользоваться корпоративными приложениями, например входящими в состав системы управления предприятием. Последнее нередко косвенно влечет за собой такую потребность, как доступ к той или иной СУБД, — многие системы управления предприятиями используют архитектуру «клиент-сервер», требующую наличия на рабочем месте пользователя клиентской части СУБД, используемой в такой системе.

Надежность, средства защиты данных, устойчивость к сбоям.

Планирование информационной безопасности

Для защиты информации от несанкционированного доступа будет применяться разграничение доступа к ресурсам. С целью защиты компьютеров сети от атак из сети интернет, выход в сеть Интернет организуется через прокси-сервер, а сам сервер оборудован брандмауэром. Как на сервере, так и на рабочих станциях будет установлен антивирус с централизованным управлением через политики сервера. Сервер оборудуется источником бесперебойного питания, позволяющим завершить необходимые рабочие процессы при отключении от сети электропитания.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы был составлен план сети, объединяющей два здания Новогиреевской станции, расположенные на расстоянии 800 м. друг от друга. Были выбраны топологии сети для каждого из зданий, позволяющие обеспечить устойчивую работу сети как в каждом здании, так и объединить оба здания в одну сеть. В зданиях предложен вариант прокладки кабеля, размещения сетевых устройств с целью экономии материальных средств как на прокладку сети, так и на её обслуживание. Сетевое оборудование имеет запас по количеству портов и, при необходимости, позволяет быстро нарастить мощность ЛВС при увеличении количества рабочих мест, либо добавления ещё одного и более зданий.

ОС, выбранная для сервера и рабочих станций, позволяет быстро и с минимальными усилиями провести первоначальную настройку сети, а в дальнейшем её обслуживание и модернизацию.

Краткий план сети, который отражает все выбранные компоненты и характеристики планируемой сети представлен в таблице.

Таблица 2

Краткий план сети

Характеристика	**Значение**
Топология сети	Распределенная звезда
Тип кабеля	UTP
Сетевое оборудование	3 коммутатора, 24 и 16 портов
Оборудование для доступа к VPN	2 модема ВОЛС
Операционная система сервера	Windows Server 2019
Операционная система станций	Windows 11
Сетевой протокол	TCP/IP

Список использованных источников

1. Виснадул, Б.Д. Основы компьютерных сетей: учебное пособие для учрежд. СПО/ Б.Д. Виснадул, С.А. Лупин, С.В. Сидоров; под ред. Л.Г.Гагариной. - М.: ФОРУМ: Инфра М, 2012.
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов/ В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2012.
3. Таненбаум, Э. Компьютерные сети/ Э. Таненбаум, Д. Уэзеролл. - СПб.: Питер, 2014.
4. Канцедал, С.А. Дискретная математика: учебное пособие для студ. учрежд. СПО.- М.: ФОРУМ: ИНФРА-М, 2013.
5. Кочетков, Е. С. Теория вероятностей и математическая статистика: учебник для студ. учрежд. СПО/ Е.С. Кочетков, С.О. Смерчинская, В.В. Соколов. - 2-е изд., испр. и перераб. - М.: Форум: ИНФРА-М, 2014.
6. Новиков, Ф. Дискретная математика: учебник для вузов. — СПб.: Питер, 2011.

Приложение А

Логическая схема организации связей