ФГОУ СПО "Салаватский индустриальный колледж"

Пояснительная записка

ОРГАНИЗАЦИЯ КОРПОРАТИВНОЙ СЕТИ НА ОСНОВЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПЕРЕДАЧИ ДАННЫХ

Выполнил Степанов А.З.

Проверил Панова М.А

2011

Содержание

Цель, задач проекта, термины и сокращения

Введение

1. Технологии цифровых и аналоговых линий связи

1.1 Модемная связь

1.2 Цифровые технологии связи

2. Технология DSL

2.1 ADSL

2.1.1 Характеристики

2.1.2 Оборудование

2.1.3Разработка спецификации на оборудование

2.1.4 Применение

2.2 HDSL

2.2.1 Характеристики

2.2.2 Оборудование

2.2.3Разработка спецификации на оборудование

2.2.4 Применение

2.3 VDSL

2.2.1 Характеристики

2.2.2 Оборудование

2.2.3Разработка спецификации на оборудование

2.2.4 Применение

3. Выбор технологии и оборудования для построения корпоративной сети

4. Настройка сетевого соединения, распределения сетевых адресов

5. Обеспечение безопасности ресурсов сети

5.1 Предотвращение неконтролируемого доступа к информации

5.2 Firewall

5.3 Разработка спецификации на оборудование

6. Требования к технологии управления сетью

Заключение

Список использованных источников

Цель, задачи проекта, термины и сокращения

локальный сеть цифровой корпоративный

По заданию необходимо разработать проект объединения 2-х локальных сетей в одну на основе цифровых технологий передачи данных.

Основной целью курсового проекта является приобретение навыков построения локальной вычислительной сети на основе цифровых технологий передачи данных.

xDSL (digital subscriber line) - цифровая абонентская линия

ADSL (Asymmetric Digital Subscriber Line) - асимметричная цифровая абонентская линия)

HDSL (high data rate digital subscriber line) - высокоскоростная цифровая абонентская линия)

VDSL (Very-high data rate Digital Subscriber Line) - сверхвысокоскоростная цифровая абонентская линия

Internet Protocol или IP (internet protocol) - межсетевой протокол

АТС (кириллица) - автоматическая телефонная станция

Bit Error Rate (BER) – частота ошибочных бит

IDSL (ISDN Digital Subscriber Line) - цифровая абонентская линия

RADSL (Rate Adaptive Digital Subscriber Line) - цифровая абонентская линия с адаптацией скорости

SDH (Synchronous Digital Hierarchy) - это технология транспортных телекоммуникационных сетей

ISDN (Integrated Services Digital Network) - цифровая сеть с интеграцией обслуживания.

POTS (Plain Old Telephone Service) - старые обычные телефонные службы

PCI (Peripheral component interconnect, дословно) - взаимосвязь периферийных компонентов

USB (Universal Serial Bus) - универсальная последовательная шина

PPPoE (Point-to-point protocol over Ethernet) - сетевой протокол канального уровня передачи кадров PPP через Ethernet

HTTP (. HyperText Transfer Protocol ) - протокол передачи гипертекста

NAT (Network Address Translation) -"преобразование сетевых адресов

URL (Universal Resource Locator, как правило, произносится "урл") URL – это адрес страницы в интернете

Введение

Корпоративная сеть передачи данных - это телекоммуникационная сеть, объединяющая в единое информационное пространство все структурные подразделения компании. Корпоративная сеть - это основа жизнедеятельности любой организации. Большинство применяющихся сегодня информационных решений носит ярко выраженный распределенный характер и требует наличия на предприятии или в организации высокопроизводительной корпоративной сети передачи данных. Основными задачами корпоративной сети оказываются взаимодействие системных приложений, расположенных в различных узлах, и доступ к ним удаленных пользователей. Поэтому корпоративная сеть, как правило, является территориально распределенной, т.е. объединяющей офисы, подразделения и другие структуры, находящиеся на значительном удалении друг от друга. Часто узлы корпоративной сети оказываются расположенными в различных городах, а иногда и странах.

Современные технологии цифровой передачи данных во многом стирают проблему расстояний и позволяют в рамках единой корпоративной сети организовать:

* единый электронный документооборот;
* общие архивы документов;
* передачу речи;
* передачу данных телеметрии;
* автоматический сбор данных систем видеонаблюдения;
* дистанционный режим доступа к файлам, устройствам печати, к серверам с базами данных;
* сопряжение вычислительных сетей, в том числе, использующие различные сетевые протоколы;
* видеоконференцсвязь;
* подключение к сети Интернет по выделенному каналу связи;
* предоставление доступа к глобальным сетям данных, к финансовым торговым и информационным системам;
* использование услуг IP-телефонии;
* взаимодействие между локальной вычислительной сетью (ЛВС) подразделения и ЛВС центрального офиса.

Вышеперечисленные возможности во многом упрощают внутренние процессы компании, а также дают предприятию ряд преимуществ, по сравнению с конкурентами, а именно:

* простота управления компанией;
* прозрачность работы компании;
* оперативный контроль деятельности всех служб и структурных подразделений;
* быстрая и своевременная реакция на внешние и внутренние изменения;
* доступ ко всем информационным ресурсам предприятия в реальном времени;
* оперативная связь;
* экономия средств на международных и междугородних звонках.

Основная проблема, которую приходится решать при создании корпоративной сети - организация каналов связи. Если в пределах одного города можно рассчитывать на аренду выделенных линий, в том числе высокоскоростных, то при переходе к географически удаленным узлам ситуация осложняется "особенностями национальных телекоммуникаций": недостаточно развитой и изношенной кабельной инфраструктурой, большими расстояниями, наличием сложно преодолимых естественных препятствий. Поэтому зачастую каналы попросту отсутствуют, либо стоимость аренды становится неприемлемой, а качество и надежность их часто оказывается весьма невысокими. [2,1]

В данном курсовом проекте мы рассмотрим наиболее распространенные технологии xDSL и выберем из них наиболее подходящую нам для построения корпоративной сети виртуального предприятия. Так же мы проанализируем и подберем к нашей сети наиболее подходящее нам оборудование.

1. Технологии цифровых и аналоговых линий связи

1.1 Модемная связь

Наиболее распространённый и известный в России способ подключения к Интернету – модемная связь с использованием телефонной линии. К компьютеру подключается модем – устройство для приёма и передачи данных, которое соединяется с обычной телефонной линией. Когда необходимо установить связь, при помощи модема производится набор телефонного номера, по которому отвечает другой модем, установленный у Интернет-провайдера. Между модемами устанавливается соединение и производится передача данных.

Практически всегда модемная связь с использованием телефонной линии применяется для сеансового соединения с Интернетом. Когда сеанс связи заканчивается, модем освобождает телефонную линию, и её можно использовать для иных нужд. Основное достоинство модемной связи – её распространённость и невысокая цена. Если доступна достаточно качественная телефонная линия, доступна и модемная связь – нет необходимости в организации специального канала. Первоначальная цена подключения к провайдеру модемной связи невысока или отсутствует вовсе – требуется лишь приобретение самого модема. Текущая оплата производится по времени соединения; иногда предлагается неограниченный доступ с фиксированной помесячной оплатой.

Однако у модемной связи есть и крупные недостатки, значительная часть их которых связана с плачевным состоянием основной массы российских телефонных линий. Общеизвестная проблема модемной связи – невысокая скорость. Теоретически современные модемы способны обеспечивать передачу данных со скоростью до 56 Кбит/с по направлению от провайдера к пользователю и до 40 Кбит/c – от пользователя к провайдеру. Это заметно меньше, чем возможности большинства современных каналов, однако позволяет одному пользователю достаточно комфортно использовать большинство сервисов в Интернете. Реальная скорость при работе по не очень качественной телефонной линии оказывается заметно меньше.

Надёжность модемной связи зависит от качества передачи сигнала по телефонной линии – и поэтому в России оказывается непредсказуемой. На некоторых линиях не удаётся установить связь вовсе. На других – возможность установления связи и её скорость зависят от ряда случайных факторов (погода, функционирование АТС в данный момент и т.п.) При появлении в линии помех модемы могут на некоторое время прекратить передачу информации или вовсе разорвать связь.

Наконец, установление сеанса связи может быть весьма продолжительным из-за занятости модемных телефонных линий провайдера. Конечно, на каждом телефонном номере провайдера обычно установлено несколько линий и соответственно модемов – но все эти линии могут быть заняты. Кроме того, бывают перегружены каналы связи между телефонными станциями. В обоих этих случаях при наборе номера модемом в ответ приходит сигнал "занято", и набор приходится повторять. Такой "дозвон" вплоть до получения ответа модема провайдера может продолжаться значительное время, иногда – часами. В сочетании с возможностью обрыва связи в любой момент из-за плохого качества линии, долгий дозвон может в некоторых случаях привести к бесполезности подобного подключения.

К основным характеристикам линий связи относятся:

* амплитудно-частотная характеристика;
* полоса пропускания;
* затухание;
* помехоустойчивость;
* перекрестные наводки на ближнем конце линии;
* пропускная способность;
* достоверность передачи данных;
* удельная стоимость.

В первую очередь разработчика вычислительной сети интересуют пропускная способность и достоверность передачи данных, поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети. Пропускная способность и достоверность - это характеристики как линии связи, так и способа передачи данных. Поэтому если способ передачи (протокол) уже определен, то известны и эти характеристики. Например, пропускная способность цифровой линии всегда известна, так как на ней определен протокол физического уровня, который задает битовую скорость передачи данных - 64 Кбит/с, 2 Мбит/с и т. п.

Амплитудно-частотная характеристика, полоса пропускания и затухание.

Степень искажения синусоидальных сигналов линиями связи оценивается с помощью таких характеристик, как амплитудно-частотная характеристика, полоса пропускания и затухание на определенной частоте.

Амплитудно-частотная характеристика показывает, как затухает амплитуда синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всех возможных частот передаваемого сигнала. Вместо амплитуды в этой характеристике часто используют также такой параметр сигнала, как его мощность. Знание амплитудно-частотной характеристики реальной линии позволяет определить форму выходного сигнала практически для любого входного сигнала. Для этого необходимо найти спектр входного сигнала, преобразовать амплитуду составляющих его гармоник в соответствии с амплитудно-частотной характеристикой, а затем найти форму выходного сигнала, сложив преобразованные гармоники.

Пропускная способность (throughput) линии характеризует максимально возможную скорость передачи данных по линии связи. Пропускная способность измеряется в битах в секунду - бит/с, а также в производных единицах, таких как килобит в секунду (Кбит/с), мегабит в секунду (Мбит/с), гигабит в секунду (Гбит/с) и т. д.

Пропускная способность линий связи и коммуникационного сетевого оборудования традиционно измеряется в битах в секунду, а не в байтах в секунду. Это связано с тем, что данные в сетях передаются последовательно, то есть побитно, а не параллельно, байтами, как это происходит между устройствами внутри компьютера. Такие единицы измерения, как килобит, мегабит или гигабит, в сетевых технологиях строго соответствуют степеням ) 0 (то есть килобит - это 1000 бит, а мегабит - это 1 000 000 бит), как это принято во всех отраслях науки и техники, а не близким к этим числам степеням 2, как это принято в программировании, где приставка кило равна 210 =1024, а мега - 220 = 1 048576.

Помехоустойчивость и достоверность. Помехоустойчивость линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде, на внутренних проводниках. Помехоустойчивость линии зависит от типа используемой физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивыми являются радиолинии, хорошей устойчивостью обладают кабельные линии и отличной - волоконно-оптические линии, малочувствительные ко внешнему электромагнитному излучению. Обычно для уменьшения помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают.

Достоверность передачи данных характеризует вероятность искажения для каждого передаваемого бита данных. Иногда этот же показатель называют интенсивностью битовых ошибок (Bit Error Rate, BER). Величина BER для каналов связи без дополнительных средств защиты от ошибок (например, самокорректирующихся кодов или протоколов с повторной передачей искаженных кадров) составляет, как правило,10-4 - 10-6, в оптоволоконных линиях связи - 10-9. Значение достоверности передачи данных, например, в 10-4 говорит о том, что в среднем из 10000 бит искажается значение одного бита.[3,4]

1.2 Цифровые технологии связи

хDSL - семейство технологий, позволяющих значительно расширить пропускную способность абонентской линии местной телефонной сети путём использования эффективных линейных кодов и адаптивных методов коррекции искажений линии на основе современных достижений микроэлектроники и методов цифровой обработки сигнала.

В аббревиатуре xDSL символ "х" используется для обозначения первого символа в названии конкретной технологии, а DSL обозначает цифровую абонентскую линию DSL (англ. Digital Subscriber Line - цифровая абонентская линия). Технологии хDSL позволяют передавать данные со скоростями, значительно превышающими те скорости, которые доступны даже самым лучшим аналоговым и цифровым модемам. Эти технологии поддерживают передачу голоса, высокоскоростную передачу данных и видеосигналов, создавая при этом значительные преимущества как для абонентов, так и для провайдеров. Многие технологии хDSL позволяют совмещать высокоскоростную передачу данных и передачу голоса по одной и той же медной паре. Существующие типы технологий хDSL, различаются в основном по используемой форме модуляции и скорости передачи данных.

Службы xDSL разрабатывались для достижения определенных целей: они должны работать на существующих телефонных линиях, они не должны мешать работе различной аппаратуры абонента, такой как телефонный аппарат, факс и т. д., скорость работы должна быть выше теоретического предела в 56Кбит/сек., и наконец, они должны обеспечивать постоянное подключение.

К основным типам xDSL относятся ADSL, HDSL, IDSL, MSDSL, PDSL, RADSL, SDSL, SHDSL, UADSL, VDSL. Все эти технологии обеспечивают высокоскоростной цифровой доступ по абонентской телефонной линии. Существующие технологии xDSL разработаны для достижения определенных целей и удовлетворения определенных нужд рынка. Некоторые технологии xDSL являются оригинальными разработками, другие представляют собой просто теоретические модели, в то время как третьи уже стали широко используемыми стандартами. Основным различием данных технологий являются методы модуляции, используемые для кодирования данных.

Синхронная Цифровая Иерархия (СЦИ: англ. SDH - Synchronous Digital Hierarchy) - это технология транспортных телекоммуникационных сетей. Стандарты СЦИ определяют характеристики цифровых сигналов, включая структуру фреймов (циклов), метод мультиплексирования, иерархию цифровых скоростей и кодовые шаблоны интерфейсов и т. д.

Система SDH обеспечивает стандартные уровни информационных структур, то есть набор стандартных скоростей. Базовый уровень скорости - STM-1 155,52 Mбит/с. Цифровые скорости более высоких уровней определяются умножением скорости потока STM-1, соответственно, на 4, 16, 64 и т. д.: 622 Мбит/с (STM-4), 2,5 Гбит/с (STM-16), 10 Гбит/с (STM-64) и 40 Гбит/с (STM-256).

ISDN (Integrated Services Digital Network) - цифровая сеть с интеграцией обслуживания. Позволяет совместить услуги телефонной связи и обмена данными.

Основное назначение ISDN - передача данных со скоростью до 64 кбит/с по 4-килогерцовой проводной линии и обеспечение интегрированных телекоммуникационных услуг (телефон, факс, и пр.). Использование для этой цели телефонных проводов имеет два преимущества: они уже существуют и могут использоваться для подачи питания на терминальное оборудование.[6,5]

2. Технология DSL

2.1 ADSL

2.1.1 Характеристики

Технология ADSL в настоящее время является наиболее развитой в семействе xDSL, обеспечивает передачу по электрическому кабелю потоков до 8 Мбит/с в одном направлении (как правило, в сторону пользователя) и до 1,5 Мбит/с - в другом. Технически асимметрия реализуется за счет распределения частотного спектра передачи в пользу потока абонента.

По широкому входящему каналу абонент получает данные из интернет или видеоданные, а исходящий используется для отправки запросов на получение информации. При этом пропускной способности исходящего канала достаточно для передачи электронной почты, факсов и для проведения голосовых переговоров через Интернет.

Указанные выше предельные скорости передачи в прямом и обратном направлении могут быть снижены в зависимости от конкретного типа оборудования, кабеля, требуемой протяженности абонентской линии.

Оборудование ADSL способно автоматически или принудительно конфигурироваться, чтобы на конкретной абонентской линии достичь максимальной скорости передачи с минимальным коэффициентом ошибок.

Несомненным плюсом технологии ADSL является то, что при ее использовании нет необходимости организации отдельного "физического" канала от АТС до пользователя, можно использовать уже имеющуюся телефонную линию. Здесь необходимо заметить, что организация стандартной выделенной линии не подразумевает выдачу телефонного номера (и услуги телефонной связи) на него.

Именно таким образом ADSL может обеспечить, например, одновременную высокоскоростную передачу данных, передачу видеосигнала и передачу факса. И все это без прерывания обычной телефонной связи, для которой используется та же телефонная линия. Технология предусматривает резервирование определенной полосы частот для обычной телефонной связи (или POTS - Plain Old Telephone Service). Удивительно, как быстро телефонная связь превратилась не только в "простую" (Plain), но и в "старую" (Old); получилось что-то вроде "старой доброй телефонной связи". Однако, следует отдать должное разработчикам новых технологий, которые все же оставили телефонным абонентам узенькую полоску частот для живого общения. При этом телефонный разговор можно вести одновременно с высокоскоростной передачей данных, а не выбирать одно из двух. Более того, даже если у вас отключат электричество, обычная "старая добрая" телефонная связь будет работать по-прежнему и с вызовом электрика у вас никаких проблем не возникнет. Обеспечение такой возможности было одним из разделов оригинального плана разработки ADSL. Даже одна эта возможность дает системе ADSL значительное преимущество перед ISDN.

Для того, чтобы оценить скорость передачи данных, обеспечиваемую технологией ADSL, необходимо сравнить ее с той скоростью, которая может быть доступна пользователям, использующим другие технологии. Аналоговые модемы позволяют передавать данные со скоростью от 14,4 до 56 Кбит/с. ISDN обеспечивает скорость передачи данных 64 Кбит/с на канал (обычно пользователь имеет доступ к двум каналам, что в сумме составляет 128 Кбит/с). Различные технологии DSL дают пользователю возможность передавать данные со скоростью 144 Кбит/с (IDSL), 1,544 и 2,048 Мбит/с (HDSL), "нисходящий" поток 1,5 - 8 Мбит/с и "восходящий" поток 640 - 1500 Кбит/с (ADSL), "нисходящий" поток 13 - 52 Мбит/с и "восходящий" поток 1,5 - 2,3 Мбит/с (VDSL). Кабельные модемы имеют скорость передачи данных от 500 Кбит/с до 10 Мбит/с (при этом следует учитывать, что полоса пропускания кабельных модемов делится между всеми пользователями, одновременно имеющими доступ к данной линии, поэтому число одновременно работающих пользователей оказывает значительное влияние на реальную скорость передачи данных каждого из них). Цифровые линии Е1 и Е3 имеют скорость передачи данных, соответственно, 2,048 Мбит/с и 34 Мбит/с.

В новом стандарте ADSL 2 реализованы скорости 10 Мбит/с "нисходящего" и 1 Мбит/с "восходящего" потока при дальности до 3 км, а в технологии ADSL 2+, стандарт которой должен быть утверждён в 2003 году, фигурируют скорости "нисходящего" потока в 20, 30 и 40 Мбит/с (соответственно по 2,3 и 4 парам).[7]

2.1.2 Оборудование

С точки зрения пользователя все ADSL модемы можно делятся на четыре группы

* внутренние PCI модемы
* внешние модемы с интерфейсом USB
* внешние модемы с интерфейсом Ethernet
* внешние маршрутизаторы (роутеры) с интерфейсом Ethernet

Внутренние ADSL модемы по сравнению с внешними имеют те же достоинства и недостатки, что и модемы классические. С одной стороны, они не занимают место на столе, не требуют отдельного блока питания и заметно уменьшают количество проводов, но, с другой стороны, для установки требуют вскрытия системного блока (что не всегда возможно, если блок находится на гарантии и опечатан), а также не могут работать без драйверов, а потому, как правило, подходят только для пользователей MS Windows (как и в случае с классическими PCI модемами, для альтернативных систем драйвера существуют далеко не всегда, да и качество их обычно оставляет желать лучшего). Настройка модема осуществляется с помощью специальной утилиты, поставляемой вместе с драйверами.

Внешние USB модемы обеспечивают такую же функциональность, как и внутренние модемы. Они обладают всего двумя разъемами – USB и разъемом для подключения телефонной линии и, как правило, двумя индикаторами – один светодиод показывает, что модем включен, а другой – что установлено ADSL соединение. Как и PCI модемы, они могут работать только в мостовом режиме – даже если для модема заявлена поддержка PPPoE, то на практике это будет означать попросту наличие собственного PPPoE клиента в его драйвере. Опять же, для работы модему требуются драйвера, а для настройки – специальная утилита, так что пользователям систем, отличных от MS Windows, стоит как минимум предварительно выяснить наличие и качество работы драйверов под их ОС, а еще лучше – обратить внимание на модемы с интерфейсом Ethernet.

Более универсальны ADSL модемы с интерфейсом Ethernet – для работы с ними от операционной системы требуется лишь поддержка протокола TCP/IP и любой сетевой карты с интерфейсом 10Base-T ("витая пара"), к которому и подключается модем. Настройка модема также не требует каких-либо специальных драйверов или утилит – она производится из любого броузера (модем имеет собственный HTTP-сервер и web-интерфейс для конфигурирования), а многие модемы поддерживают и подключение по telnet для сторонников командной строки.

Теоретически такой модем можно подключать даже напрямую к хабу или свитчу, на котором организована домашняя локальная сеть, однако практически в этом, как правило, нет никакого смысла – эти модемы не поддерживают ни трансляции сетевых адресов (Network Address Translation, сокращенно NAT), ни каких-либо методов авторизации (PPPoE либо PPPoA), они могут лишь выполнять функции конвертера между интерфейсами ATM и Ethernet. Таким образом, основное их преимущество над USB-модемами заключается в наличие интерфейса, поддерживаемого всеми современными ОС и, соответственно, в отсутствии необходимости в каких-либо специфических драйверах.

Наиболее распространенным способом подключения сетей к интернету в условиях, когда провайдер предоставляет только один IP-адрес, является использование трансляции сетевых адресов (NAT). В этом случае компьютерам внутри сети раздаются так называемые частные IP-адреса (часто их еще называют "серыми") – эти адреса могут использоваться любым желающим, но только в пределах локальной сети, в глобальной же Сети они не имеют какого-либо смысла. Очевидно, что по этой причине компьютеры с частными IP-адресами могут быть доступны только из той локальной сети, в которой они расположены за ее пределами такая адресация теряет всякий смысл; поэтому для обеспечения доступа в интернет устанавливается сервер, имеющий сразу два адреса – "серый", соответствующий локальной сети, и "белый", доступный снаружи для всех желающих. Если же на сервер из локальной сети поступает пакет, идущий наружу – сервер подменяет в нем "серый" адрес отправителя на собственный "белый" адрес и отправляет дальше, одновременно запоминая, с какого "серого" адреса этот пакет пришел, чтобы, когда из интернета придет ответ на него, переправить этот ответ отправителю исходного пакета. Этот механизм и называется трансляцией сетевых адресов и обеспечивает наиболее прозрачный и наименее зависимый от используемых приложений и операционных систем способ подключения локальных сетей к интернету.

Разновидность ADSL модемов, имеющих встроенную поддержку NAT, называется ADSL маршрутизаторами, либо роутерами. Кроме собственно NAT, большинство ADSL маршрутизаторов поддерживают также PPPoE и PPPoA протоколы (то есть способны при необходимости самостоятельно авторизоваться у провайдера, без установки PPPoE-клиента на пользовательский компьютер), способны работать DHCP-сервером, автоматически раздавая IP-адреса и базовые настройки подключенным к ним компьютерам, а также имеют в своем составе DNS-сервер и файрволл. Иначе говоря, ADSL маршрутизатор способен легко заменить отдельный сервер, полностью обеспечивая функционирование и доступ в интернет небольшой локальной сети. Конечно, для сколько-нибудь серьезной сети возможностей модема не хватит – в нем нет подсчета трафика для каждого из компьютеров сети, фильтрации URL'ов, кэширующего прокси-сервера и многого другого, однако для небольшой домашней сети, состоящей обычно максимум из трех-четырех компьютеров (например, один настольный компьютер и два ноутбука), такой модем является практически идеальным решением.

Как и рассмотренные выше Ethernet ADSL модемы, маршрутизаторы подключаются через интерфейс Ethernet, причем в данном случае возможность подключить их к свитчу или хабу напрямую становится куда более заманчивой. Настройка модемов также осуществляется через web-интерфейс с помощью любого броузера, но многие модели поддерживают и такие протоколы, как telnet и SNMP. Зачастую Ethernet ADSL модемы оказываются упрощенными версиями ADSL маршрутизаторов, возможности которых ограничены программно – сравните, например, D-Link DSL-300G и DSL-500G.

Весьма привлекательны ADSL маршрутизаторы и для домашних пользователей, имеющих только один компьютер. Во-первых, такой роутер за счет использования NAT позволяет отгородить компьютер от сети, полностью защитив его от червей, подобных MSBlast – дело в том, что к компьютеру, имеющему "серый" IP-адрес, невозможно получить прямой доступ из Интернета, ибо в качестве получателя пакета обязательно должен быть указан адрес "белый", то есть адрес маршрутизатора. Способа же указать маршрутизатору извне, что этот пакет должен предназначаться для какого-либо из подключенных к нему локальных компьютеров, в общем случае не существует – поэтому все попытки атак будут приходиться на маршрутизатор, которому они не смогут причинить ни малейшего вреда хотя бы потому, что стоящая на нем ОС не имеет ничего общего с Windows. Кроме того, ADSL маршрутизатор является полностью самостоятельным устройством

Внешние маршрутизаторы со встроенными свитчами и точками доступа Wi-Fi ADSL маршрутизаторы со встроенными свитчами, точками доступа Wi-Fi, принт-серверами и т.д. Такой маршрутизатор позволяет организовать небольшую домашнюю сеть без использования какого-либо дополнительного оборудования, что не только весьма удобно, но и обходится дешевле покупки двух или трех отдельных устройств. Та же часть устройства, что отвечает за ADSL и доступ в интернет, ничем не отличается от таковой в обычных ADSL маршрутизаторах. [7]

# 2.1.3 Разработка спецификации на оборудование

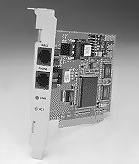


Рисунок 1 - PCI ADSL-модем Cisco 605

Основные характеристики

- Автоматическая установка скорости интерфейса (Rate-adaptive DSL) в зависимости от качества линии обеспечивает ее максимальное возможное значение. Максимальная скорость передачи данных к абоненту - 7 Мбит/с, а от абонента - 1Мбит/с. Для кодирования сигнала используется технология амплитудно-фазовой модуляции без несущей (CAP, Carrierless Amplitude Phase)

- В Windows 95/98, Windows NT 4.0 и 5.0 обеспечена поддержка драйвера NDIS для установки протокола PPP поверх ATM поверх DSL (RFC 1483)

- Светодиодные индикаторы приема/передачи данных и состояния линии ADSL

- Совместимость со стандартом PCI Plug-and-Play для упрощенной установки и конфигурирования

- Благодаря совместимости с технологией Cisco QuickDial время освоения ADSL уменьшается до секунд

- Разъем RJ-11 ADSL для подключения к цифровой линии

- Встроенный телефонный порт, снабженный микрофильтром EZ-DSL

- PPP-окончание для прозрачного доступа в удаленные корпоративные локальные сети и Интернет

- Поддержка уровня AAL5 ( ATM adaptation layer) и формата ячеек Raw Cell.

- Использование технологии Cisco EZ-DSL обеспечивает максимальную скорость линии DSL с учетом ее качества, определяемого автоматически (Rate Adaptive DSL)

- Полная совместимость с мультиплексорами доступа Advanced DSLAM серий Cisco 6100 и Cisco 6200.

Маршрутизаторы Cisco 2800 серии имеют возможность одновременного обеспечения большого количества сервисов с большой скоростью на нескольких соединениях T1/E1/xDSL. Маршрутизаторы предлагают встроенное ускорение шифрования и слоты DSP (voice digital-signal-processor); систему предотвращения вторжений (IPS) и функции межсетевого экрана; опциональную встроенную систему обработки вызовов и поддержку голосовой почты; высокую плотность интерфейсов для большого количества требований проводных и беспроводных соединений; достаточную производительность и плотность слотов для будущего расширения сети и требований современных приложений.

Таблица 1 – Спецификация Cisco 2800

|  |  |
| --- | --- |
| Размеры (ширина x глубина x высота) | 4.37 x 44.5 x 41.9 |
| Вес, кг: | 6.2 |
| Тип установки, особенности конструкции: | Установка в 19 дюймовую стойку, размер 1 RU  Возможность установки на стену отсутствует |
| Параметры питания: | Входное напряжение AC: 100 - 240 В AC, автоматическая регулировка  Входная частота AC: 47 - 63 Гц  Входной ток AC: 2 А (110 В), 1 А (230 В) |
| WAN/LAN-интерфейсы: | 2 x RJ-45 10/100 FE |
| Другие интерфейсы: | 1 x консольный порт (до 115.2 кбит/с)  1 x AUX порт (до 115.2 кбит/с)  1 x USB 1.1 |
| Слоты расширения: | 2 x PVDM (DSP)  4 слота для интерфейсных карт:  2 x HWIC/VWIC/WIC/VIC - 400 Мб/сек (полудуплекс) или 800 Мб/сек (общая), поддержка PoE  1 x VWIC/WIC/VIC  2 x AIM  Слоты для сетевых модулей: 0  Слоты для Extension-Voice-Module (EVM): 0 |
| Управление: | Cisco Router и Security Device Manager (SDM)  Функция расширенной установки  Поддержка CiscoWorks  Cisco AutoInstall  Cisco IOS Embedded Event Manager (EEM) |

2.1.4 Применение

Основная область применения ADSL, скоростной доступ в Интернет. Также имеется возможность подключаться к корпоративным локальным сетям, различным мультимедийным программам. Например, слушать музыку или смотреть фильмы и другие видеоматериалы on-line, то есть в реальном времени, без предварительной закачки данных на компьютер(Рисунок 2).

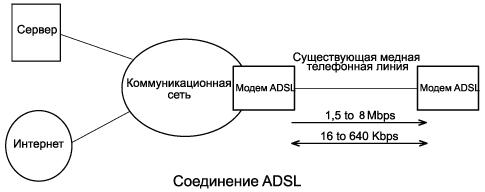


Рисунок 2 – Технология ADSL

2.2 HDSL

2.2.1 Характеристики

Технология HDSL предусматривает организацию симметричной линии передачи данных, то есть скорости передачи данных от пользователя в сеть и из сети к пользователю равны. Благодаря скорости передачи (1,544 Мбит/с по двум парам проводов и 2,048 Мбит/с по трем парам проводов) телекоммуникационные компании используют технологию HDSL в качестве альтернативы линиям T1/E1. (Линии Т1 используются в Северной Америке и обеспечивают скорость передачи данных 1,544 Мбит/с, а линии Е1 используются в Европе и обеспечивают скорость передачи данных 2,048 Мбит/с.) Хотя расстояние, на которое система HDSL передает данные (а это порядка 3,5 - 4,5 км), меньше, чем при использовании технологии ADSL, для недорогого, но эффективного, увеличения длины линии HDSL телефонные компании могут установить специальные повторители. Использование для организации линии HDSL двух или трех витых пар телефонных проводов делает эту систему идеальным решением для соединения УАТС, серверов Интернет, локальных сетей и т.п. [7]

2.2.2 Оборудование

HDSL модем HTU-2. В HTU-2 используется технология HDSL, повышающая обычную дальность передачи для цифровых интерфейсов nх 64 Кбит/с. Применяется линейное кодирование 2B1Q, техника коррекции линии и адаптивной фильтрации, а также эхоподавление для компенсации дефектов линии, ответвлений и смешанной кабельной разводки. Это обеспечивает высокую устойчивость к фоновому шуму и возможность передачи по нескольким линиям HDSL в одном и том же физическом кабеле. HTU-2 повышает до 4.8 км дальность действия при передаче по четырехпроводному медному кабелю (0.5 мм) и до 9 км - с повторителем.

HTU-2 поддерживает изменения приоритизации, что позволяет пользователю выбирать, какие временные интервалы останутся активными при отказе одной из пар.HTU-2 поддерживает передачу со скоростью, равной любому кратному 64 Кбит/с вплоть до 2.048 Мбит/с. HTU-2 работает в дуплексном режиме при передаче по четырехпроводному кабелю и может использоваться в качестве оконечного устройства на абонентском шлейфе или для двухточечных соединений в приложениях для комплекса зданий. Поддерживаемые цифровые интерфейсы: V.35, X.21, RS-530, V.36/RS-449 или Ethernet через встроенный мост/маршрутизатор.

HTU-2 может работать с HTU-E1 для связи между цифровыми интерфейсами в помещении пользователя и магистралью Е1 в центральном офисе.

Плата HTU-2 может обеспечить дистанционную подачу электропитания для повторителя HDSL или удаленного модема HTU-2/P. Для реализации этой возможности по спецзаказу поставляется HTU-2/PF. Управляющая и диагностическая информация передаются одновременно по встроенному каналу управления без помех потоку данных. Возможны непрерывный контроль за работой, управление и диагностика местных и удаленных устройств с передней панели или с помощью управляющего порта. Устройство выпускается в отдельном конструктивном исполнении или в виде платы для установки в стойке LRS-24 с центральным управлением SNMP. HTU-2 может работать с модулем DHL/E1/2W DXC или с модулями HS-H2 или MHL-2E1/2T1 Megaplex.

HDSL-маршрутизатор Intel 9545. Маршрутизатор может использоваться в качестве устройства подключения к Интернету, а также для подсоединения офисов к частным корпоративным сетям. Его пропускная способность в обоих направлениях составляет 1,5 Мбит/с.

Машрутизатор 9545 HDSL предназначен для установки в телефонных сетях на основе медного кабеля. Он может быть вынесен на расстояние до 3,6 км от центрального офиса.

В состав устройства входит встроенный интерфейс HDSL, а также модули CSU/DSU (Channel Service Unit/Digital Service Unit -- модуль обслуживания канала/цифровой служебный модуль). Такое сочетание компонентов позволило объединить в одном устройстве функции маршрутизации и клиентского подключения, отказавшись тем самым от установки маршрутазаторов HDSL и модулей связи в каждом бизнес-подразделении.

В Express 9545 предусмотрена поддержка стандарта Embedded Operation Channel (встроенный канал управления), благодаря чему поставщик услуг может отправить такой маршрутизатор на узел клиента, который самостоятельно подключит полученное устройство. После установки конфигурирование системы и управление ею можно будет осуществлять из центрального офиса. [7]

2.2.3 Разработка спецификации на оборудование

WATSON 3 - модем, обеспечивающий высокую дальность, превосходящую аналогичные системы передачи, а так же высокие показатели помехозащищенности и электромагнитной совместимости.

Основан на CAP64 технологии, и поддерживает скорость 2,048 кБит/с для линий связи большой протяженности. С WATSON 3 HDSL операторы могут обеспечить высокоскоростной доступ в Интернет, соединить локальные сети (ЛВС) или соединить существующие медные сети доступа и магистральные ВОЛС. [7]

Сравнительные характеристики модемов WATSON 3 Table Top, CAPSPAN-2000 Standalone и LGHD-2000D Standalone указаны в таблице 2.

Таблица 2 - Сравнительные характеристики оборудования HDSL

|  |  |  |  |
| --- | --- | --- | --- |
| Оборудование | LGHD-2000D Standalone | CAPSPAN-2000 Standalone | WATSON 3 Table Top |
| Питание | 220 В, 50Гц | 220 В, 50Гц | 40-60 В, адаптер220 В |
| Потребл. мощность | 9 Вт | 12 (8) Вт | 6 Вт |
| Дистанционное питание | нет | есть, 180 В пост. | 120 В пост. |
| Управление | С локальной клавиатуры и ЖКИ, RS-232 (VT100) только на корзине, ПО для Windows | RS-232 (VT100) | RS-232 (VT100), централизованное сетевое управление через X.25 или Ethernet, протоколы SNMP, SMIP, частные протоколы TMS Nokia, XMP Bosch E1, V.35, V.36, X.2, (2 порта N\* 64 до 1 Мбит/с каждый, ISDN PRi, Ethernet (Bridge) |
| Интерфейсы | E1 (T1), V.35 | E1 (T1), V.35 | E1(1+1) |
| Резервирование по пользовательскому интерфейсу | нет | нет |  |
| Защита по HDSL тракту | нет | нет | при обрыве одной пары сохраняется половина временных интервалов |
| Режим работы | 2 пары | 2 пары | 2 пары или 1 пара (половина потока) |

2.2.4 Применение

Основной областью применения HDSL является соединения линий местных телефонных сетей или выделенные линии связи, где нужна очень высокая скорость, например, в офисных зданиях, где больше количество абонентов одновременно вынуждены связываться друг с другом.

Существует еще усовершенствованный вариант данной технологии, который называется HDSL2. При всех преимуществах HDSL, второй версии хватит одной телефонной линии – двух медных проводов. Но пока широкого распространения HDSL2 не получил(Рисунок 3). [8]

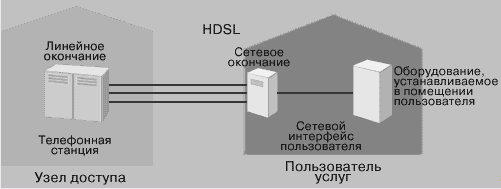


Рисунок 3 – Технология HDSL

2.3 VDSL

2.3.1 Характеристики

Технология VDSL является наиболее "быстрой" технологией xDSL. Она обеспечивает скорость передачи данных "нисходящего" потока в пределах от 13 до 52 Мбит/с, а скорость передачи данных "восходящего" потока в пределах от 1,5 до 2,3 Мбит/с, причем по одной витой паре телефонных проводов. Технология VDSL может рассматриваться как экономически эффективная альтернатива прокладыванию волоконно-оптического кабеля до конечного пользователя. Однако, максимальное расстояние передачи данных для этой технологии составляет от 300 метров до 1300 метров. То есть, либо длина абонентской линии не должна превышать данного значения, либо оптико-волоконный кабель должен быть подведен поближе к пользователю (например, заведен в здание, в котором находится много потенциальных пользователей). Технология VDSL может использоваться с теми же целями, что и ADSL; кроме того, она может использоваться для передачи сигналов телевидения высокой четкости (HDTV), видео по запросу и т.п. [8]

2.3.2 Оборудование

VDSL модем City-Netek CN-501 LT/RT

Используя данные модемы, можно соединить две Ethernet точки на расстояниях до 1500 метров по витой паре (начиная от 3-ей категории) на скоростях до 12.5 Mbps в режиме FullDuplex. У устройства есть VDSL порт, 10/100BaseTX Ethernet порт (обычный и uplink) и POTS/ISDN splitter, к разъему которого, собственно говоря, и подключается аналоговый или ISDN телефон. Устройство имеет порт RS232, через который Вы можете конфигурировать Ваш модем и/или обновлять прошивку модема. Модемы могут быть двух видов – ведомый (RT) и ведущий (LT). Ведущий позволяет удаленно конфигурировать ведомый. Для настроек модема (через RS232 интерфейс) используется прилагаемая программа, которая позволяет модифицировать целый ряд параметров. В частности, Вы можете уменьшить скорость работы модема, но при этом поднять расстояние, на котором этот модем работает. К примеру, на 4 Mbps модем должен "пробивать" расстояние в 2.5 км.[8]

VDSL коммутатор City-Netek CN-5412

VDSL коммутатор, в качестве оконечных абонентских устройств для которого используются те же самые CN-501 модемы. Данный коммутатор поддерживает VLAN, одновременную передачу VDSL и голоса, имеет на борту 12 VDSL портов и 4-е Ethernet. Имеет консольный выход для управления через терминал.[8]

2.4.3 Разработка спецификации на оборудование



Рисунок 4 – Управляемый VDSL IP концентратор

На рисунке 4 показан DYNAMIX DV-24 - управляемый VDSL коммутатор, который позволяет строить высокоскоростные сети с возможностью управления. Он обеспечивает поддержку 24 VDSL каналов через POTS/ISDN соединения и имеет два порта Gigabit Ethernet для подключения к сети провайдера либо агрегирования нескольких аналогичных концентраторов (uplink). Концентраторы DYNAMIX DV-24 поддерживают технологию QAM 4 и обеспечивают симметричную скорость соединения до 25Mbps на канал. В качестве оконечного оборудования могут использоваться модемы DYNAMIX VCS и DYNAMIX VC-S4.

Особенности:

* Совместим с IEEE 802.3 & 802.3u Ethernet стандартами и ETSI, ITU, ANSI стандартами
* Одновременная передача голосового и VDSL трафика, встроенные в концентратор сплиттеры
* Симметричная скорость 5M/15M/25Mbps на канал при расстоянии 1.7 / 1.1/ 0.6 км
* Два порта Gigabit Ethernet (RJ-45) с Auto MDI/MDIX
* Один порт для консольного управления
* Поддержка SNMP (SNMP v1 RFC-1493 Bridge MIBs:RFC-1643 Ethernet MIB, RFC-1213 MIB II) / HTTP / Telnet и консольного управления
* Поддержка качества передачи голоса на основе контроля соотношения сигнал-шум
* Поддержка управления контролем потока на основе IEEE802.3x для полного дуплекса (Full Duplex) и Back Pressure для полудуплекса (Half Duplex)
* Поддержка безопасности - 802.1v VLAN ( протокол базирующихся)
* RMON groups 1, 2, 3, 9 (RFC-1757 RMON MIB)
* Поддержка 802.1p Class of Service
* Поддержка 802.3ad port trunking и LACP (Link Aggregation Control Protocol)
* Поддержка GARP/GVRP IEEE-802.1p/q VLAN
* Поддержка 802.1D Spanning Tree Protocol (STP)
* Поддержка Multicast IP таблицы/IGMP v2, BOOTP/DHCP Client, контроля полосы пропускания
* Поддержка "зеркалирования" портов
* Защита от широкополосного шторма (Broadcast Storm)
* Спектральная совместимость с XDSL, ISDN (2B1Q/4B3T), HomePNA оборудованием
* Защита VDSL портов.

Спецификации:

Техническая спецификация

VDSL интерфейс :

- 24 порта VDSL (RJ-21 разъем) и 24 портов POTS (RJ-21 разъем) -Встроенные POTS/ISDN сплиттеры -Частота VDSL передатчика : 0.9MHz ~ 3.9MHz, приемника: 4MHz~7.9MHz LAN интерфейс :

- два 10/100/1000Mbps Ethernet порта ( RJ-45) с Auto MDI/MDIX Светодиодные индикаторы :

Power, POST, Link/Active/Speed Status для Ethernet портов, Link для VDSL портов Протоколы :

- Поддержка spanning tree протокола (IEEE 802.1d) - Поддержка 802.1p Class of Service

- Поддержка безопасности - 802.1v VLAN ( протокол базирующихся)

- Поддержка 802.3ad port trunking и LACP (Link Aggregation Control Protocol)

- Поддержка GARP/GVRP IEEE-802.1p/q VLAN - Поддержка 802.1D Spanning Tree Protocol (STP)

- Поддержка Multicast IP таблицы/IGMP v2 с 512 группами - Поддержка "зеркалирования" портов - Защита от широкополосного шторма ( Broadcast Storm) Управление:

- Консольное, Telnet, Web и SNMP управление; - SNMP: SNMP v1 RFC-1493 Bridge MIBs:RFC-1643 Ethernet MIB, RFC-1213 MIB II - RS-232 консольный порт : DB-9 Pin Female / 9600bps - Питание: от внешнего AC 85-265 В/50-60Hz/1A источника

Физические параметры

- Размер 432 x 299 x 66 mm

- Рабочая температура: 0°C- 50°C

- Температура хранения: -20°C - 65°C

- Влажность: 10% - 90% (без конденсата)

2.3.4 Применение

С помощью оборудования Ethernet - over - VDSL решается задача соединения двух локальных Ethernet - сетей, расположенных на расстоянии до 1,5 километров со скоростью 11 Мбит/с (напомним, расстояние может быть увеличено до 3 километров с некоторым уменьшением скорости).

Для решения этой задачи между сегментами ЛВС должен лежать прямой некоммутируемый провод, категории не ниже 3 (телефонный кабель ТПП). Разумеется, если качество кабеля (диаметр жилы, категорийность и. д.) улучшается, предельные дальности увеличиваются. В этом случае используются два модема Ethernet - over - VDSL, локальный (CN-501LT) и удаленный (CN-501RT), включенные по топологии "точка - точка", которые имеют разъем RJ-45 для включения в сегмент Ethernet - сети, разъем RJ-11, для подключения к VDSL - линии, и в том случае, когда для передачи данных используется существующая работающая телефонная линия, разъем RJ-11 для подключения телефонии и встроенный сплиттер для разделения двух телекоммуникационных сервисов - передача голоса и данных(Рисунок 5).[8]

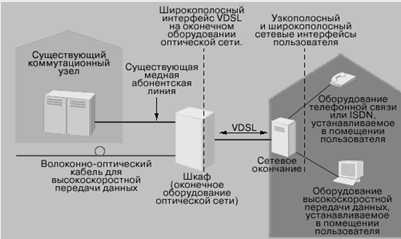


Рисунок 5– технология VDSL

3. Выбор технологии и оборудования для построения корпоративной сети

Исходя из рассмотренных данных и показаний, оптимальным будет выбор ADSL технологии объединения 2-х локальных сетей. ADSL обладает множеством преимуществ:

- Использование самых обычных витых пар медных проводов телефонных кабелей.

- Высокая скорость передачи данных в сравнении с другими распространенными технологиями.

- Полоса пропускания линии принадлежит пользователю целиком.

- Возможность пользоваться обычной телефонной связью одновременно с цифровым каналом компьютерной сети.

- Не требует прокладки специальных кабелей, а использует уже существующие двухпроводные медные телефонные линии. [9]

Построение корпоративных сетей и анализ требований. На этом этапе формулируются основные деловые цели предприятия, для которого разрабатывается проект, например, сокращение производственного цикла, более оперативный прием заказов или повышение производительности труда за счет более эффективного взаимодействия сотрудников, то есть те цели предприятия, которые в настоящий момент, при существующих средствах и технологиях не вполне достигаются. Осуществляется поиск аналогичных систем, анализируются их сильные и слабые стороны, определяется возможность использования удачного опыта для проектируемой системы.

Разработка бизнес-модели и Построение корпоративных сетей. Бизнес-модель можно по-другому назвать функциональной моделью производства, она описывает деловые процедуры, последовательность и взаимозависимость всех выполняемых на предприятии работ. При этом внимание концентрируется не на компьютерной системе, а на деловой практике.[10]

Разработка технической модели и Построение корпоративных сетей. Техническая модель описывает в достаточно общих терминах, какое компьютерное оборудование нужно использовать, чтобы достичь целей, определенных в бизнес-модели. Для построения технической модели необходимо провести инвентаризацию всего имеющегося оборудования, определить требования к новой системе (при этом требования должны быть сформулированы не с технической точки зрения, а с позиций руководителей и конечных пользователей сети), на основании этого определить, что из существующего оборудования может быть использовано в новой системе. Далее необходимо определить полный функциональный набор необходимых аппаратных средств без конкретизации марок и моделей оборудования.

После того, как выбрана техническая модель, описывающая сеть в общих терминах, создается так называемая физическая модель, которая является подробным описанием конкретных продуктов, их количества, технических параметров и способов взаимодействия.

Оборудование для построения ADSL-сети

Cisco 6200 Series Advanced DSL Access Multiplexer (DSLAM) (рисунок 6) - 14-ти слотовый мультиплексор для абонентского доступа с поддержкой до 80-ти абонентских линий ADSL на скорости до 7Мбит/с.

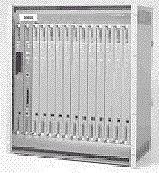


Рисунок 6 – Cisco 6200 Series Advanced DSL Access Multiplexer (DSLAM)

The 605 Personal PCI ADSL Modem - внутренний модем PPP/ATM для установки в PCI-слот компьютера, позволяет пользователю принимать информацию от узла провайдера на скорости до 7Мбит/с.

Cisco 626 ATM25 ADSL Modem – внешний ADSL модем.

Из вышеописанных оборудований для объединения 2-х локальных сетей в одну будет использоваться ADSL модем марки Cisco 626 ATM25 ADSL и ADLS мультиплексор марки Cisco 6200 Series Advanced DSL Access Multiplexer. ADSL модем будет использован для выхода в интернет. Для обеспечения совместного доступа сети интернет необходим интернет шлюз(прокси-сервер) куда и будет подключен ADSL модем.

На рисунке 7 показана примерная схема подключения отдаленных офисов в общую корпоративную сеть.

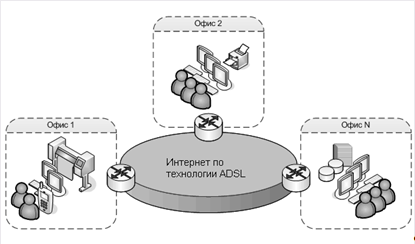


Рисунок 7 – Корпоративная сеть на основе ADSL технологии

4. Настройка сетевого соединения, распределения сетевых адресов

В первую же очередь необходимо подключить само устройство.



Рисунок 8 – Соединение xDSL

Для настройки сетевого соединения необходимо открыть свойство подключения(Рисунок 9).

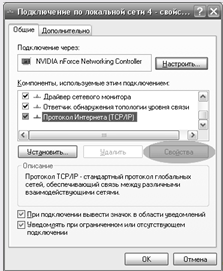


Рисунок 9 – Свойства подключения устройства

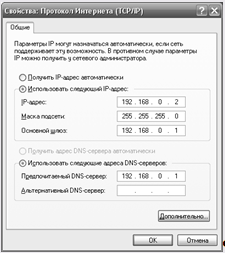


Рисунок 10 – Протокол TCP/IP

Установите следующие настройки:

IP-адрес:192.168.0.2

Маска подсети:255.255.255.0

DNS:192.168.0.1

Такие настройки были выбраны из-за того что они являются стандартными. Диапазон IP адресов 192.168.0.0 выделены для образовательных учреждений и корпоративных сетей, это сделано для того что бы IP адреса не совпадали в интернете.

Распределение сетевых адресов. Диапазон адресов следует разбить на участки, которые будут применяться для различных целей.

1. 192.168.0.1 - 192.168.0.5 – для сервера

2. 192.168.0.6 - 192.168.0.15 – для активного оборудования, коммутатора

3. 192.168.0.20 - 192.168.0.100 – для автоматизированных рабочих мест.

5. Обеспечение безопасности ресурсов сети

5.1 Предотвращение неконтролируемого доступа к информации

Предотвращение неавторизованного доступа к сетевым ресурсам означает, прежде всего, невозможность физического доступа к компонентам сети - рабочим станциям, серверам, сетевым кабелям и устройствам, и т.п. Когда сетевое соединение выходит за пределы зоны влияния, например в точке подключения к внешнему провайдеру интернета, то контроль за физическими аспектами сети теряется. Оборудование в помещении компании должно находиться под пристальным наблюдением.

Серверы, на которых хранятся важные или уязвимые данные, не должны стоять открыто на столе или в незапертой комнате, куда может зайти кто угодно. Аналогичным образом должны защищаться маршрутизаторы, концентраторы, коммутаторы и другие устройства. Комнаты с компьютерами должны закрываться на замок или находиться под круглосуточным наблюдением. Если кто-то из сотрудников компании работает круглосуточно, то это комнату закрывать не обязательно - но только в том случае, если персонал не дежурит по одному. В идеале доступ в подобные помещения должен контролироваться, например, путем регистрации в журнале. Резервные носители, такие как ленты или перезаписываемые компакт-диски, должны быть защищены так же, как и исходные данные. Недопустимо хранить резервные копии на сервере или рабочей станции, оставлять картриджи и CD на столе или в незапертом ящике. [13]

5.2 Firewall

Firewall - это программа, представляющая собой защитный барьер между компьютером и внешним миром. Хакеры используют специальное программное обеспечение для сканирования интернета и поиска незащищенных компьютеров. Такие программы посылают маленький пакет данных компьютеру. Если на компьютере нет Firewall, то он автоматически отвечает на принятое сообщение, и это означает для хакера, что система открыта и может быть взломана. Firewall распознает такие случаи и не отвечает на подобные сообщения. Таким образом, хакеры даже не могут узнать, что компьютер подключен к сети.

Внутри локальной сети, которую от внешних угроз защищает корпоративный Firewall, рабочая станция остается беззащитной. Настройки общего Firewall, не позволяют разрешить или запретить активность тех или иных приложений, которые запущены на рабочей станции, а так же предотвратить распространение вирусов. При помощи специальных типов атак злоумышленник может в локальной сети получить любые данные, которые передаются по сети с Вашего компьютера. Переговоры по ICQ, почтовые пароли, письма и любая другая конфиденциальная информация может быть перехвачена до того, как она дойдет до получателя. Даже в случае если используются защищенные соединения (SSL), все равно есть известные способы получать перехваченные данные сразу в расшифрованном виде.

Классификация firewall'ов и определение политики firewall'а

Классификация firewall'ов. Исследуются существующие технологии firewall'ов: пакетные фильтры, stateful inspection firewall'ы, прокси прикладного уровня. Рассматривается сервис NAT. Приводятся примеры использования firewall'ов различного типа: выделенные прокси серверы, host-based firewall'ы, персональные firewall'ы.

Различные типы окружений firewall'а. Рассматриваются различные типы окружений, в которых может функционировать firewall. Приведены основные принципы построения окружения firewall'а. Дается определение DMZ сети. Исследуются различные топологии DMZ сетей с использованием firewall'ов разного типа. Разбирается взаимное расположение конечных точек VPN и firewall'ов. Вводятся понятия интранет, экстранет. Задаются принципы создания политики firewall'а.

Пример пакетных фильтров в ОС FreeBSD 6.0. Рассматриваются пакетные фильтры, реализованные в ОС FreeBSD 6.0: IPF и IPFW. Приводится синтаксис каждого из этих пакетных фильтров и возможности поддержки состояния ТСР соединения в них. Приводится порядок прохождения пакета через правила пакетного фильтра. Изучается применение функции трансляции сетевых адресов (NAT). Приведены примеры набора правил в IPF и IPFW.[14,13]

5.3 Разработка спецификации на оборудование

Спецификация PIX Firewall 515

Таблица 3- Спецификация PIX Firewall 506 и 515

|  |  |  |
| --- | --- | --- |
| Характеристики | Модель | |
| PIX Firewall 506 | PIX Firewall 515 |
| Корпус (модуль) | монтируемый в 19-ти дюймовую стойку или отдельный модуль | монтируемый в 19-ти дюймовую стойку или отдельный модуль |
| Процессор | 200 MГц Intel Pentium MMX | 200 MГц Intel Pentium MMX |
| Оперативная память | 32 Mб | 64 Mб |
| Flash память | 16 Mб | 16 Mб |
| Консольный порт | RJ-45 | RJ-45 |
| Загрузка/Обновление | только TFTP | только TFTP |
| Failover порт \* | Disabled | DB-25 EIA/TIA-232 |
| H x W x D (см.) | 4.1 x 42.5 x 30 | 4.1 x 42.5 x 30 |
| Напряжение | 100-240 В | 100-240 В |
| Частота питания | 50-60 Гц | 50-60 Гц |
| Сила тока | 1.5-0.75 А | 1.5-0.75 А |

Таблица 4 - Эксплуатационные параметры PIX Firewall 506 и 515

|  |  |  |
| --- | --- | --- |
| Характеристики | Модель | |
| PIX Firewall 506 | PIX Firewall 515 |
| Температура хранения | от -25 до +70ºC | от -25 до +70ºC |
| Относительная влажность | от 20 до 95% | от 20 до 95% |
| Стандарты EMI | CE, VCCI class II, FCC, BCIQ, Austel | CE, VCCI class II, FCC, BCIQ, Austel |
| Рабочая\_температура | от -5 до +45ºC | от -5 до +45ºC |

6. Требования к технологии управления сетью

Международная Организация по Стандартизации (ISO) внесла большой вклад в стандартизацию сетей. Модель управления сети этой организации является основным средством для понимания главных функций систем управления сети. Эта модель состоит из 5 концептуальных областей:

- Управление эффективностью

- Управление конфигурацией

- Управление учетом использования ресурсов

- Управление неисправностями

- Управление защитой данных

- Управление эффективностью

Цель управления эффективностью - измерение и обеспечение различных аспектов эффективности сети для того, чтобы межсетевая эффективность могла поддерживаться на приемлемом уровне. Примерами переменных эффективности, которые могли бы быть обеспечены, являются пропускная способность сети, время реакции пользователей и коэффициент использования линии.

Управление эффективностью включает несколько этапов:

Сбор информации об эффективности по тем переменным, которые представляют интерес для администраторов сети.

Анализ информации для определения нормальных (базовая строка) уровней.

Определение соответствующих порогов эффективности для каждой важной переменной таким образом, что превышение этих порогов указывает на наличие проблемы в сети, достойной внимания.

Управляемые объекты постоянно контролируют переменные эффективности. При превышении порога эффективности вырабатывается и посылается в NMS сигнал тревоги.

Каждый из описанных выше этапов является частью процесса установки реактивной системы. Если эффективность становится неприемлемой вследствие превышения установленного пользователем порога, система реагирует посылкой сообщения. Управление эффективностью позволяет также использовать проактивные методы. Например, при проектировании воздействия роста сети на показатели ее эффективности может быть использован имитатор сети. Такие имитаторы могут эффективно предупреждать администраторов о надвигающихся проблемах для того, чтобы можно было принять контрактивные меры.

Управление конфигурацией

Цель управления конфигурацией - контролирование информации о сете- вой и системной конфигурации для того, чтобы можно было отслеживать и управлять воздействием на работу сети различных версий аппаратных и программных элементов. Т.к. все аппаратные и программные элементы имеют эксплуатационные отклонения, погрешности, или то и другое вместе, которые могут влиять на работу сети, такая информация важна для поддержания гладкой работы сети.

Чтобы обеспечить легкий доступ, подсистемы управления конфигурацией хранят эту информацию в базе данных. Когда возникает какая-нибудь проблема, в этой базе данных может быть проведен поиск ключей, которые могли бы помочь решить эту проблему.

Управление учетом использования ресурсов

Цель управления учетом использования ресурсов - измерение параметров использования сети, чтобы можно было соответствующим образом регулировать ее использование индивидуальными или групповыми пользователями. Такое регулирование минимизирует число проблем в сети (т.к. ресурсы сети могут быть поделены исходя из возможностей источника) и максимизировать равнодоступность к сети для всех пользователей.

Как и для случая управления эффективностью, первым шагом к соответствующему управлению учетом использования ресурсов является измерение коэффициента использования всех важных сетевых ресурсов. Анализ результатов дает возможность понять текущую картину использования. В этой точке могут быть установлены доли пользования. Для достижения оптимальной практики получения доступа может потребоваться определенная коррекция. Начиная с этого момента, последующие измерения использования ресурсов могут выдавать информацию о выставленных счетах, наряду с информацией, использованной для оценки наличия равнодоступности и оптимального коэффициента использования источника.

Управление неисправностями

Цель управления неисправностями - выявить, зафиксировать, уведомить пользователей и (в пределах возможного) автоматически устранить проблемы в сети с тем, чтобы эффективно поддерживать работу сети. Т.к. неисправности могут привести к простоям или недопустимой деградации сети, управление неисправностями, по всей вероятности, является наиболее широко используемым элементом модели управления сети ISO.

Управление неисправностями включает в себя несколько шагов:

* Определение симптомов проблемы.
* Изолирование проблемы.
* Устранение проблемы.
* Проверка устранения неисправности на всех важных подсистемах.
* Регистрация обнаружения проблемы и ее решения.

Управление защитой данных

Цель управления защитой данных - контроль доступа к сетевым ресурсам в соответствии с местными руководящими принципами, чтобы сделать невозможными саботаж сети и доступ к чувствительной информации лицам, не имеющим соответствующего разрешения. Например, одна из подсистем управления защитой данных может контролировать регистрацию пользователей ресурса сети, отказывая в доступе тем, кто вводит коды доступа, не соответствующие установленным.

Подсистемы управления защитой данных работают путем разделения источников на санкционированные и несанкционированные области. Для некоторых пользователей доступ к любому источнику сети является несоответствующим. Такими пользователями, как правило, являются не члены компании. Для других пользователей сети (внутренних) несоответствующим является доступ к информации, исходящей из какого- либо отдельного отдела. Например, доступ к файлам о людских ресурсах является несоответствующим для любых пользователей, не принадлежащих к отделу управления людскими ресурсами (исключением может быть администраторский персонал).

Подсистемы управления защитой данных выполняют следующие функции:

* Идентифицируют чувствительные ресурсы сети (включая системы, файлы и другие объекты)
* Определяют отображения в виде карт между чувствительными источниками сети и набором пользователей
* Контролируют точки доступа к чувствительным ресурсам сети
* Регистрируют несоответствующий доступ к чувствительным ресурсам сети.[15]

Заключение

Цель курсового проекта заключалась в организации корпоративной сети для виртуального предприятия. Были рассмотрены вопросы:

- цифровые и аналоговые линии связи

- преимущества и недостатки основных цифровых технологий связи, характеристики и оборудование для рассматриваемой технологии;

Выбрана технология для построения корпоративной сети.

Технология корпоративной сети:

Была выбрана технология ADSL, так как она обладает множеством преимуществ:

1. Использование самых обычных витых пар медных проводов телефонных кабелей.

2. Высокая скорость передачи данных в сравнении с другими распространенными технологиями.

3. Полоса пропускания линии принадлежит пользователю целиком.

4. Возможность пользоваться обычной телефонной связью одновременно с цифровым каналом компьютерной сети.

5. Не требует прокладки специальных кабелей, а использует уже существующие двухпроводные медные телефонные линии.

Исходя из поставленных задач, анализируя решенные задачи, с помощью выбранной нами технологи и оборудования для виртуальной корпоративной сети, можно придти к выводу, что все поставленные цели курсового проекта были достигнуты.

Список использованных источников

1 Сайт Интернета www.elecom.ru

2 Сайт Интернета www.mariupol.net

3 Сайт Интернета www.xdsl.ru

4 Сайт Интернета www.ixbt.com

5 Сайт Интернета www.sovtel.ru

6 Сайт Интернета athena.vvsu.ru

7 Сайт Интернета www.godynamix.ru

8 Сайт Интернета www.irs.ru

9 Сайт Интернета www.erudition.ru

10 Сайт Интернета www.agfirewall.ru

11 Сайт Интернета www.mark-itt.ru

12 Сайт Интернета www.komcinet.ru

13 К. Закер – Компьютерные сети. Модернизация, поиск неисправностей.

14 М. Кульгин – Компьютерные сети. Практика построения.

15 Олифер В.Г., Олифер Н.А Компьютерные сети. Принципы, технологии, - протоколы. - СПб: Питер, 2006. - 958 с.