1. ВВЕДЕНИЕ

В настоящее время все современные крупные компании (со штатом сотрудников от 100 человек) проводят четкую политику развития IT структуры компании. Основной частью этой структуры является разработка и внедрение корпоративной сети. Обычным явлением для крупной корпоративной сети является наличие централизованного администрирования всех филиалов, а также построение распределенной сети, позволяющей связывать между собой как различные филиалы, так и отдельных работников. Так же для таких организаций свойственно формирование отдельных групп пользователей, имеющих уникальные способы доступа (через беспроводные сети, через выделенные каналы и т.п.).

Настоящая курсовая работа предназначена для создания проекта корпоративной сети крупной компании CorpKAM.

2. АНАЛИЗ ИСХОДНЫХ ДАННЫХ

2.1 Исходные данные

2.1.1 Структура компании



Рис.1 Структура подразделений корпорации CorpKAM

Корпорация имеет главный офис (здание А) и два филиала:

* производство продукции Manufacture (M) – здание B;
* отдел исследований и новейших разработок Research (R) – здание C;

Структура здания А:

1 этаж. Подразделения корпорации:

* отдел кадров и подготовки специалистов Human Resource (HR);
* отдел маркетинга Sales (S);
* служба информационных технологий и технической поддержки Information Technologies (IT).

2 этаж. Подразделения:

* руководство корпорацией Executive (E);
* бухгалтерия Accounting (Acc);
* отдел экономики и планирования Business (Bus).

На 3, 4, и 5 этажах расположено проектное отделение, при этом:

3 этаж. Проектный отдел Project 1 (P1);

4 этаж. Проектный отдел Project 2 (P2);

5 этаж. Проектный отдел Project 3 (P3).

Для 2-х групп сотрудников отдела маркетинга необходимо организовать защищенную беспроводную сеть с выходом в интернет.

Структура здания B:

В - одноэтажное здание, где производятся изделия двух типов, одно из них на площадях М1, другое - на площадях М2. Кроме того, имеется автоматизированный склад готовой продукции Production (P). Филиал Manufacture (M) (здание В) расположен в другом городе, удаленном на значительное расстояние, и соединен с главным офисом каналом Т1.

Структура здания С:

Здание С связывается с главным офисом через Internet маршрутизаторами с функцией “дозвон по требованию”, используя подключение ADSL.В двухэтажном здании С филиала отдел Research занимает два этажа, при этом на 1 этаже расположена рабочая группа Research 1 (R1), на 2 этаже группа Research 2 (R2).

Также имеется небольшой штат сотрудников корпорации в Европе, которые соединяются с главным офисом по каналам ISDN. Несколько сотрудников работают в своих домашних офисах SOHO, подключающихся к главному офису по коммутируемым каналам связи PSTN Dial-up 56 Кб/с.

Рис 2. Схема расположения корпорации CorpKAM



2.1.2 СОСТАВ ИСХОДНЫХ ДАННЫХ ТРЕБОВАНИЙ

Для определения исходных данных определяем, что номер варианта N=5.

В качестве исходных данных берется достаточность полосы пропускания каналов передачи данных (Т1, ISDN, ASDL) для обеспечения сетевого трафика с удовлетворительным клиентским откликом.

Критерием расположения серверов является минимизация служебного трафика.

Основные технологии - Ethernet по стандарту 100/1000BASE-T (на витой паре cat5 и выше) и FDDI.

Каждое подразделение корпорации имеет свой конфиденциальный сервер приложений, доступ к которому могут иметь только сотрудники соответствующего подразделения.

Для внешних IP\_интернет адресов используется диапазон адресов (Public\_IP) 131.107.х.0/24, где х=50\*G+N G={1, 2, 3} – номер группы, N- номер варианта. Таким образом, имеем x=50\*1+5=55 и диапазон 131.107.55.0/24.

Для диапазона внутренних адресов (Private\_IP) используется зарезервированный ICANN диапазон адресов 10.55.0.0/16

Величины K = 5, L = 1, N = 5, G = 1.

Таблица 1 Поэтажное расположение рабочих групп и количество рабочих станций трёх проектных отделов в здании А

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ОТДЕЛ | Project 1 |  | Project 2 |  | Project 3 |  |
| ЭТАЖ | Число рабочих групп (комнат) | Число рабочих станций в группе, не более | Число раб. гр. | Число раб. ст. | Число раб. гр. | Число раб. ст. |
| Этаж 1 | 20 | 10 |  |  |  |  |
| Этаж 4 |  |  | 13 | 16 |  |  |
| Этаж 5 |  |  |  |  | 9 | 17 |

В таблице 3 приведены данные по количеству рабочих групп и рабочих станций в одноэтажном здании филиала В Manufacture.

Таблица 2 Количество рабочих групп и рабочих станций в одноэтажном здании филиала В Manufacture

|  |  |  |
| --- | --- | --- |
| ОТДЕЛ | Manufacture | |
| Подразделение | Число рабочих групп (комнат) | Число раб. станций в группе, не более |
| M1 | 25 | 10 |
| M2 | 16 | 22 |
| P | 10 | 37 |

Таблица 4 Поэтажное число групп и рабочих станций в здании С филиала Research

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ОТДЕЛ | Res 1 | | Res 2 | |
| ЭТАЖ | Число рабочих групп (комнат) | Число рабочих станций в группе, не более | Число раб. групп | Число раб. ст. |
| Этаж 1 | 9 | 20 |  |  |
| Этаж 2 |  |  | 6 | 10 |

Таблица 5 Данные общекорпоративных служб

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Служба | Human Resource, IT gr., Sales Manag. | | Accounting | | Business | |
| Параметр К | Число рабочих групп (комнат) | Число рабочих станций в группе, не более | Число раб. гр. | Число раб. станций в раб. гр. | Число раб. гр. | Число раб. ст. в раб. гр. |
| 5 | 5 | 8 | 4 | 13 | 3 | 7 |

Детально проработать реализацию служб и протоколов VPN-L2TP/IPSec, используя для построения сети оборудование фирмы 3Com.

## Требования

При выполнении работы выполните также следующие требования:

* в качестве службы каталогов корпоративной сети использовать Active Directory;
* предоставить доступ к размещенному в головном офисе Web и FTP серверам корпорации CorpKAM как пользователям Интернета, так и пользователям внутренней корпоративной сети (intranet) в любое время в любой день недели;
* изолировать корпоративную сеть от Интернета, кроме Web и FTP-сервера;
* изолировать внутреннее пространство имен;
* защитить все данные, пересылаемые между головным офисом и филиалом Research;
* каждое подразделение должно иметь свой конфиденциальный сервер приложений;
* обеспечить защиту конфиденциальных данных при пересылке в подразделениях корпоративной сети с использованием IPSec;
* обеспечить защиту конфиденциальных данных при пересылке через Интернет с использованием VPN;
* обеспечить защищенные подключения к корпоративной сети удаленных пользователей по телефонным линиям (ASDL/ISDN);
* обеспечить защиту беспроводных сетей WLAN;
* обеспечить проведение аудио и видеоконференций (\*);
* обеспечить надежную работу соединений путем введения дополнительных, резервных маршрутных подключений (\*);
* предусмотреть меры по снижению сетевого трафика, вызываемого потоковыми аудио и видеоконференциями (\*);
* выполнить оценку стоимости оборудования и сопутствующего ПО.

\* - необязательное (но желательное) для выполнения.

3. ФИЗИЧЕСКОЕ ПРОЕКТИРОВАНИЕ СЕТИ

В физическое проектирование сети включается подбор оборудования, проектирование расположения оборудования на этажах, а также выбор ПО, которое будет использовано при построении сети.

3.1 Геометрические характеристики зданий

Для правильной оценки количества устанавливаемого оборудования и монтируемых линий необходимо иметь представление о геометрических параметрах здания, в котором осуществляется монтаж. Так как ТЗ не содержит данных для этого, примем, что:

- здания имеют форму параллельного параллелепипеда;

- если не оговорено иное, то каждое подразделение располагается на своем этаже;

- расчет выполняется из наихудших условий труда – что бы рабочее место каждого сотрудника удовлетворяло минимальным санитарным нормам (4 м/человека);



- ввиду того, что размер одной РГ меняется по заданию от 7 до 22 РС в РГ, то будем считать, что площадь РГ с запасом в 50% на расширение сети равна 1,5\*22\*4=132 м. Учитывая возможности по расширению, а также то, что человеку реально нужно дял организации рабочего места больше 4 м, будем считать, что в РГ 30 РС.



- распределение оборудования по этажу выполняется так, что бы обеспечить подключение РГ в любой точке этажа.

Для геометрических расчетов применим следующую методику расчета, основанную на геометрической оптимизации.

3.1.1 Модель рабочей группы (РГ)

Под РГ понимается комната здания (или несколько смежных комнат здания), в которой расположены РС. Так как порядок расположения РС неизвестен, то считаем, что они равномерно распределены по комнате (смежным комнатам). Для простоты расчетов считаем, что РГ имеет прямоугольную форму. Как будет показано ниже, можно при решении задачи о средней длине ЛС внутри РГ можно перейти от прямоугольной формы РГ к квадратной без потери общности. Так же не известно расположение РГ друг относительно друга, поэтому считаем, что на каждую РГ выделяется один коммутатор (или коммутационный узел из нескольких коммутаторов).

В силу того, что по заданию РГ размещены на существенном расстоянии друг от друга, необходимо предусмотреть возможность их объединения коммутаторами горизонтального подуровня ГП. Введем в рассмотрение модель такого подключения.

Допустим, что от коммутатора РГ к коммутатору ГП идет одна или несколько ЛС, объединенных в один канал связи КС. Необходимо установить, как именно геометрически расположить коммутаторы и линии связи, что бы общая стоимость такого подключения была минимальной. Для простоты модели, а так же исходя из реальных конструкций зданий, считаем, что ЛС можно прокладывать только под прямым углом (рисунок 1).



Рисунок 1. Модель №1 подключения РГ к ГП

На рисунках 1 и 2 X и Y – расстояние между коммутаторами ГП и РГ по длине и ширине здания соответственно, N\*M – габариты РГ, W и L – габариты прямоугольной области, противоположными точками которых являются коммутатор ГП и наиболее удаленная от него РС РГ. Габариты W и L описывают так называемую зону охвата коммутатора ГП и будут использованы в п. 3.1.2 при построении математической модели ГП.

При таком расположении коммутатора РГ в РГ имеем среднюю длину ЛС между РС и коммутатором как:

(1)



Считается, что длина ЛС изменяется от 0 (РС расположена около коммутатора) до (N+M) – (РС расположена в противоположном углу от коммутатора РГ).

Рассмотрим другое расположение коммутатора РГ (рисунок 2). Коммутатор РГ расположен в центре РГ. Это увеличивает расстояние до коммутатора ГП на (N+M)/2, а средняя длина ЛС внутри РГ равна:

(2)



Получается, что расположение коммутатора не влияет на среднюю длину ЛС внутри РГ, но влияет на длину ЛС между коммутаторами РГ и ГП, увеличивая ее с (N+M) метров до 1.5\*(N+M) метров.



Рисунок 2. Модель №2 подключения РГ к ГП.

Для снижения стоимости РГ и стоимости ее подключения к ГП необходимо

и



Так как мы не можем повлиять на габариты РГ, то мы можем только минимизировать длину ЛС между коммутаторами РГ и ГП, поэтому для дальнейшей работы выбираем модель РГ №1.

Из формул (1) и (2) видно, что



зависит не от конкретных значений габаритов РГ, а от периметра РГ, поэтому можно заменить при расчете средней длины ЛС в РГ N+M на 2Z, то есть представить РГ в виде квадрата со стороной Z.

В допущениях приведены оценки габаритов РГ. Если взять в первом приближении, что РГ имеет квадратную форму, то сторона квадрата Z будет составлять примерно 11-12 метров. Реально получается, что Z не менее 15-17 м (увеличение номинальных габаритов РГ на 25-30 % позволяет учесть особенности индивидуальной проводки внутри каждой РГ, в том числе проводку в коробах, под потолком, петли в коробах и т. д.).

Установим зависимости между величинами X, Y и Z для того, что бы в дальнейшем оценивать суммарную длину ЛС, используемых при подключении РГ к коммутатору ГП.

Исходя из того, что сеть должна иметь минимальную стоимость, то выбираем в качестве ЛС коммутатора ГП и РГ UTP cat5. Это накладывает ограничения на величины X+Y<=90м. Формально для UTP cat5 максимальная длина составляет 100м, однако IEEE рекомендует брать эту величину не более 90 м для гарантированно устойчивой работы. Исходя из соображений экономии (КС коммутатора ГП и РГ будет содержать гораздо меньше кабелей, чем КС РС внутри РГ) неравенство преобразуем в равенство X+Y=90. Таким образом, имеем, что

(3)



Полученные зависимости (3) позволяют оценить, можно ли вообще подключить РГ к ГП, и если да, то определить, какая будет суммарная длина ЛС. Оценим длину ЛС, необходимых для образования РГ и ее подключения к коммутатору ГП

(4)



Выводы

1) Средняя длина ЛС внутри РГ не зависит от габаритов РГ, а зависит только от периметра РГ (1). Поэтому можно взять в качестве математической модели РГ квадрат со стороной Z=(N+M)/2. Если Z<15, то для расчета необходимо взять Z=15.

2) Оценка совокупной длины ЛС, необходимой для образования РГ и подключения ее к коммутатору ГП, производится по формуле (4).

3.1.2 Модель горизонтального подуровня (ГП)

Для ГП этажа характерно, что имеется небольшое количество межэтажных переходов (1-2 на здание), к которым необходимо подвести коммуникации со всего этажа. Так как в задании не уточнено, каким именно межэтажными переходами обладает здание и как они расположены, то считаем, что переход делают при монтаже сети. Так как это достаточно долгая и дорогостоящая процедура, то считаем, что межэтажный переход у нас один и находится примерно в центре этажа.

Как было определено в предположениях, сеть ГП должна обеспечить подключение РГ в любой точке этажа. При такой неопределенной ситуации относительно расположения РГ единственно верное решение – обеспечить на уровне проекта возможность подключения РГ к ГП в любой точке.

Для того, что бы обеспечить такую возможность, необходимо, что бы в зону охвата коммутаторов ГП попали все РС этажа любой подгруппы. Коммутаторы ГП предлагается объединять конструктивно общей шиной, то есть когда у каждого коммутатора, кроме оконечных, один порт используется для подключения других коммутаторов, расположенных «левее», а другой – для подключения коммутаторов, расположенных «правее». С точки зрения эксплуатации это одна высокоскоростная шина, на которой организованы точки доступа – коммутаторы ГП. Такая схема показала свою эффективность на практике, и поэтому при разработке модели ГП будем придерживаться ее.

Рассмотрим модель ГП, которая позволит нам оценить, сколько коммутаторов необходимо использовать в ГП, что бы стоимость ГП была минимальной (с учетом того, что в ГП входит все РГ). На рисунке 3 схематично изображена зона охвата одним коммутатором ГП.



Рисунок 3. Модель зоны охвата коммутатора ГП

Обозначения величин соответствует обозначениям на рисунках 1 и 2. Зоной охвата коммутатора ГП считаем прямоугольник 2W\*2L. Теперь рассмотрим, какие данные можно получить на основании такой модели.

1) Можно получить размеры зоны охвата коммутатора ГП, если знать габариты РГ и длину ЛС между коммутаторами ГП и РГ. Если считать, что Z=(N+M)/2, для образования ЛС между коммутаторами используется кабель UTP cat5 (п. 3.1.1), а решение будет эффективно при (п. 3.1.1). Если при этом учесть, что минимальное значение Z=15 (п. 3.1), то получим, что



(5)



Формула (5) устанавливает, что W+L=120, то есть экономическая эффективность вводит ограничение на периметр зоны охвата. Это позволяет при одном известном габарите вычислить другой. В частности, если использовать UTP cat5, то максимальное значение величины W составляет 105 метров (120-105=15 метров сторона квадрата РГ). Эта величина превышает технологический предел использования кабелей UTP cat5 в 90 метров. Таким образом, мы можем использовать любое значение величины W, допустимое технологией передачи данных.

Получаем, что нам необходимо минимизировать периметр РГ при сохранении ее площади. Из геометрии известно, что прямоугольник с минимальным периметром и заданной площадью – это квадрат. Таки образом, берем, что РГ – квадрат со стороной 15 м. Для здания А максимальное число РГ на этаж составляет 20, для здания B – 25, для здания С – 9. Определим, какой минимальной площади должны быть этажи зданий, чтобы выполнялись требования санитарных норм (п. 3.1). Получаем, что площадь здания A равна 20\*225=4500 м2, здания В 25\*225=5625 м2, здания С – 9\*225=2025 м2.

2) На основании модели можно рассчитать, сколько коммутаторов ГП необходимо для покрытия прямоугольного помещения произвольных габаритов. Основная задача в этом случае – минимизировать количество коммутаторов ГП с соблюдением требования по периметру зоны охвата и расстояния между соседними коммутаторами РГ. Последнее требование связано с тем, что эти коммутаторы потребуется соединять между собой для построения магистрали ГП. Слишком большие расстояния потребуют применять дорогие ВОЛС и соответствующее оборудование. Поэтому задача минимизации стоимости ГП может рассматриваться только с учетом совокупной стоимости ЛС, оборудования и проведения работ по монтажу.

3.1.3 Принятые габариты зданий

Рассмотрим нашу задачу для каждого здания. Как было показано выше, зона охвата описывается выражением (5), при условии, что W,L<=90 и W+L<=120. Площадь зоны охвата равна 4WL. Необходимо этими зонами охвата покрыть весь этаж здания, площадь которого для каждого здания определена выше.

Для здания А: имеем S=4500 м2, для простоты будем считать, что здание имеет форму прямоугольника 50\*90м. Тогда получаем, что W=90/2=45 и L=50/2=25. Условие W+L=70<=120 выполняется и из этого следует, что при заданных габаритах здания достаточно иметь один коммутатор ГП, к которому будут подключаться РГ.

Если взять другие габариты здания, то результат может быть другим. Например, если габариты здания 20\*180, то W=20/2=10, L=180/2=90. Условие W+L=100<=120 так же выполняется, что позволяет нам использовать так же один коммутатор ГП.

Для здания B: имеем S==5625 м2, для простоты будем считать, что здание имеет форму прямоугольника 45\*125м. Тогда получаем, что W=125/2=62,5 и L=45/2=22,5. Условие W+L=85<=120 выполняется и из этого следует, что при заданных габаритах здания достаточно иметь один коммутатор ГП, к которому будут подключаться РГ.

Если взять другие габариты здания, то результат может быть другим. Например, если габариты здания 90\*62,5, то W=90/2=45, L=62,5/2=31,25. Условие W+L=96,25<=120 так же выполняется, что позволяет нам использовать так же один коммутатор ГП.

Для здания С: имеем S=2025 м2. Очевидно, что для покрытия такой площади хватит одного коммутатора ГП.

На основании проведенных выкладок можно сделать вывод о том, что ГП всех зданий будет состоять из ЛС UTPcat5 и использовать один коммутатор ГП и по одному коммутатору РГ на РГ. Соответственно, без информации о положении РГ на этаже невозможно выполнить чертежи расположения коммутационного оборудования РГ, а можно выполнить только чертеж расположения коммутационного оборудования ГП и ВП.

Согласно расчетам, проведенным в пп. 3.1.1-3.1.2, для дальнейших расчетов примем:

- габариты здания А 50\*90 м2, число этажей 5;

- габариты здания В 45\*125 м2, число этажей 3;

- габариты здания С 27\*75м2, число этажей 2.

3.2 Установка требований к сети и подбор оборудования

3.2.1 Требования к оборудованию и ЛС по пропускной способности и надежности

По заданию базовой технологией для построения сети является технология Ethernet 100/1000Base TX и технология FDDI. Так как FDDI нуждается в специфичном оборудовании, а средой передачи является ВОЛС, то рассматривать ее имеет смысл только тогда, когда предъявляются высокие требования по отказоустойчивости, а требования к пропускной способности не очень высокие.

Для современных РС на рынке наиболее распространены сетевые карты Ethernet 100Base TX. Пропускной способности этой технологии вполне хватает, что бы покрыть требования практически всех пользователей.

В дальнейшем будем считать, что на одну РГ требуется один коммутатор РГ, который обеспечивает подключение всех РС, входящих в РГ по заданию + желательно иметь 50% запаса по количеству портов на развитие сети, по технологии Ethernet 100Base-TX, подключение к коммутатору ГП по технологии Ethernet 1000Base-TX. Требования к надежности канала между коммутаторами РГ и ГП достаточно низкие, резервирования обычно не требуется. В случае, если это обусловлено характером работ группы в сети (например, бухгалтерия или руководство организации), можно предусмотреть «холодное» резервирование, протянув еще одну ЛС UTP cat5, и в случае отказа основной ЛС в короткие сроки (до 10-15 минут) вручную восстановить работоспособность сегмента сети.

Выше показано, что на ГП требуется разворачивать только один коммутационный узел. Число РС по заданию, подключаемых к коммутационному узлу ГП, сильно колеблется в зависимости от условий применений от 120 до 550 (с учетом масштабирования на 50%). Поэтому в зависимости от конкретных условий необходимо применять либо простые коммутаторы, либо коммутаторы 3-го уровня, обеспечивающих блокирование ШВТ. Скорость коммутации должна составлять 1000 Мбит/с, так как через коммутатор ГП будет вестись работа с серверами приложений подразделений, служебными серверами, а так же связь с другими объектами структуры сети. Требования к надежности самого коммутатора и ЛС, образующей идущей от ГП к ВП, предъявляются высокие, так как в случае отказа ЛС или коммутатора от сети отделяется большое количество пользователей. Поэтому целесообразно подготовить либо «горячую» замену вышедшей из строя ЛС, либо применить агрегирование канала, повысив пропускную способность сегмента (по технологии PortTrunking или другой аналогичной). В обоих случаях требуется, что бы коммутаторы поддерживали указанные режимы работы.

Все серверы здания, находящиеся в серверной комнате, объединяются в одну РГ с подключением к коммутатору ГП на скорости 1000 Мбит/с. Так как это ответственные РС, то для них организуется «холодное» резервирование ЛС с коммутатором РГ.

Вертикальная подсистема стягивается в точку. Она представлена коммутатором 3-го уровня, к которому подключается коммутаторы ГП, а так же коммутатор с серверной РГ. Все подключения выполняются на скорости 1000 Мбит/с с «горячим» резервированием или агрегированием ЛС.

Для организации беспроводного доступа требуются точки доступа WiFi.

3.2.2 Выбор конкретного оборудования и комплектующих сети согласно требованиям

В качестве источника данных о стоимости сетевого оборудования фирмы 3Com, а так же о доступности на российском рынке возьмем данные Internet – магазинов www.levovosd.ru и www.apitcom.ru. Здесь будет рассмотрено только оборудование, характеристики которого влияют на качество сети. Расходные материалы и технически простые изделия (кабели, разъемы, пачкорды, пачпанели, шкафы и т.п.) не рассматриваются, так как их расход (количество) сильно зависит от конкретной геометрии зданий или отдельных комнат. Так же здесь не будет рассматриваться специфичное оборудование (маршрутизаторы ADSL,T1,Dial-Up и пр.), так как требования к ним будут сформированы ниже при описании соответствующих разделов.

В качестве коммутатора РГ возьмем 3COM Switch 4210 26-Port. Он имеет 24 порта Ethernet на 100 Мбит/с и 2 порта на 1000 Мбит/с. Коммутатор является управляемым (через консоль и Web-интерфес), поддерживает QoS. Наличие 2-х портов позволяет при росте рабочей группы подключить такой же коммутатор на скорости 1000 Мбит/с, используя один порт для подключения к коммутатору ГП, а другой для дополнительного коммутатора. Так же поддерживается PortTrunking, что позволит при необходимости использовать оба порта для подключения к коммутатору ГП. Имеется поддержка VLAN.

В качестве коммутатора ГП возьмем Baseline Switch 2916-SFP Plus. Он является коммутатором 2-го уровня, но поддерживает до 256 VLAN с группировкой портов, Port Trunking до 8-ми транков и до 8 портов в транке. Данный коммутатор применяется в тех случаях, когда число РГ на этаже не превышает 14. В случае, когда необходимо подключить большее число РГ, можно поставить дополнительный коммутатор.

В качестве коммутатора ВП, выполняющего роль ядра сети, возьмем модуль 3Com Switch 8800 48-Port 10/100/1000BASE-T IPv6. Это устройство обеспечивает коммутацию 3-го, поддержку VLAN, стекируемость и внешнее управление. Для маршрутизации доступны протоколы RIP, OSPF, IGMP, PIM(SM,DM), VRRP, BGP4, IS-IS. Устройство является стекируемым.

В качестве типового сервера (подходящего для решения большинства задач) возьмем 2U HP ProLiant DL380 G5. У него достаточно гибкий набор изменяемых параметров, возможность монтирования в стойку и дублирующий блок питания горячей замены.

В качестве ИБП берем APC SUA3000RMI2U. Он обладает достаточной мощностью в 3000ВА для обеспечения аварийной остановки серверов. Имеет возможность монтажа в стойку. Число ИБП определяется в каждом конкретном случае, исходя из анализа того, сколько нужно времени, чтобы выполнить безопасную остановку серверов или подготовить источники резервного питания к работе. Однако бесперебойное питание необходимо обеспечить для всех серверов всех зданий.

В качестве рабочей станции можно использовать любое оборудование на базе IBM PC, комплектация которого зависит от характера решаемых задач. Ориентировочная стоимость 1000-1500$.

3.3 Выбор пользовательского ПО

Все ПО можно разделить на 2 большие группы: служебное ПО, предназначенное для обеспечения работоспособности сети, и прикладное ПО пользователей.

При выборе ПО следует учитывать возможность применения не только коммерческого ПО, но и свободного, распространяемого по GNU-лицензии или подобным им. Бесплатная поддержка такого ПО практически не проигрывает корпоративной, при необходимости практически всегда можно заключить договор на поддержку с третьей стороной. Особенно на это следует обратить внимание при выборе ПО для конечных пользователей, так как именно в этом случае наиболее велики отчисления за лицензирование и поддержку.

ПО пользователей может быть разнонаправленным, однако при его выборе необходимо руководствоваться тем, что по заданию основными пользовательскими ОС являются 98, NT Prof, XP Prof, 2000 Prof. При выборе ОС следует иметь ввиду, что свободная продажа и техническая поддержка осталась только для XP Prof, поэтому на новые РС имеет смысл устанавливать только эту ОС. Дополнением к ОС является пакет офисного ПО OpenOffice.org 3.0, распространяемый по GNU лицензии и являющийся хорошей альтернативой пакету MS Office. В качестве почтового клиента можно использовать OpenWebMail (http://openwebmail.org/). Специализированное ПО, которое устанавливается в соответствии с требованиями конкретного пользователя, определяется в процессе эксплуатации и не может быть определена на этапе проектирования сети.

Системное ПО строится на основе Windows 2003 Server. Эта ОС имеет несколько редакций: Web, Datacenter, Enterprice, Standart. Редакции Web и Datacenter имеют достаточно простую комплектацию, поэтому их рассматривать не будем. Редакция Enterprice отличается от Statndart только добавлением следующих служб и компонент:

- поддержка процессоров Itanium;

- горячее добавление ОЗУ;

- поддержкой службы сертификатов и смарт карт;

- служба кластеров;

- каталог сессий служб терминалов;

- поддержка внешних хранилищ данных.

Проанализировав имеющиеся аппаратное обеспечения, структуру сети и требования по безопасности, приходим к выводу, что достаточно возможностей Windows 2003 Server Standart Edition. Указанные ОС применяется для развертывания всех серверных приложений сети, за исключением отдельно оговоренных случаев.

4. ЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ СЕТИ

В логическое проектирование сети включается выделение логических частей сети, описание настройки оборудования и настройка используемых сетевых служб (DNS, AD, DHCP).

3.1 Выделение подсетей и распределение IP адресов по подсетям

Выделение IP адресов в пределах всей организации целесообразно сделать динамическим (с применением DHCP)

3.1.1 Выделение подсетей и распределение IP адресов по подсетям здания А

Здание А согласно заданию имеет 5 этажей. Нижние 2 этажа имеют в своем составе несколько подразделений, 3, 4 и 5-й этажи имеют по одному подразделению на этаже. Выявим число РС на каждом этаже и необходимое количество IP адресов, необходимых для работы на основании данных таблиц 1,2 и 5.

В здании А так же помимо указанных подразделений будут находится общекорпоративные серверы, серверы подразделений, серверы демилитаризованной зоны и прочее общекорпоративное служебное оборудование в отдельно выделенном помещении, находящемся на 1-ем этаже. Учтем так же, что по заданию для использования во внутренней сети доступны адреса с диапазоном 10.55.0.0/16.

Таблица 6 Распределение IP адресов по зданию А

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Этаж | Подразделение | Число РС (с запасом 50%) | Выделяемое число IP адресов | Общее число IP на этаже |
| 1 | Отдел кадров (Human Resource) | 40(60) | 64(10.55.0.192/26) | 256 |
| 1 | Отдел маркетинга Sales (S) | 40(60) | 64(10.55.0.128/26) |
| 1 | Отдел IT | 40(60) | 64(10.55.0.64/26) |
| 1 | Корпоративные сервера | 30(45) | 64(10.55.0.0/26) |
| 2 | Руководство Executive (E) | 15(23) | 32(10.55.1.0/27) | 192 |
| 2 | Бухгалтерия Accounting (Acc) | 52(78) | 128(10.55.1.128/25) |
| 2 | Отдел экономики Business (Bus) | 21(32) | 32(10.55.1.32/27) |
| 3 | Проектный отдел Project 1 (P1) | 200(300) | 512(10.55.2.0/23) | 512 |
| 4 | Проектный отдел Project 2 (P2) | 208(312) | 512(10.55.4.0/23) | 512 |
| 5 | Проектный отдел Project 3 (P3) | 153(230) | 256(10.55.6.0/24) | 256 |

При таком разделе внутри здания А для использования остаются свободными диапазоны 10.55.1.96/26 (64 адреса) и 10.55.7.0/24 (256 адресов). Остальные адреса внутреннего диапазона выделяются зданиям B и C.

Свободные диапазоны адресов будут распределяться по мере возникновения необходимости. В частности, для сотрудников, использующих беспроводной доступ к корпоративной сети, будут выделены адреса из этого диапазона, что позволит соответствующим образом настроить сетевой фильтр и понизить риски при работе в беспроводных сетях. Размер свободно диапазона позволяет обеспечить свободным доступом весь отдел маркетинга, что снимает ограничения на численность группы.

Cервера приложений и подразделений, а также сервера служб DNS, FTP, RAS/VPN, Mail, Web устанавливаются в серверной и на них устанавливаются статические IP адреса (путем привязки их MAC адреса к IP адресу, выдаваемому DHCP). Для серверов DHCP (основного, резервного и транслирующих) задаются настоящие статические IP адреса, в противном случае работа сети будет невозможна. Размещение серверов подразделений в серверной увеличивает объем межэтажного трафика, однако повышает физическую безопасность серверов от НСД и упрощает обслуживание.

Для внешнего FireWall-а обеспечивается выделение статических адресов из пула внешних адресов 131.107.55.0/24(256 адресов). Из этого же пула адресов обеспечивается выделение адресов firewall-а здания С, которое подключается к главному филиалу через Internet с помощью технологии ADSL и для сотрудников, которые получают доступ по ISDN, то есть для всех РС, которые подключаются к основному филиалу через публичные сети (или WireWall-ы, через которые они выходят в internet с поддержкой NAT), должны быть выделены статические внешние адреса.

3.1.2 Выделение подсетей и распределение IP адресов по подсетям здания B

Так как здание B соединено с головным зданием А через канал Т1 с пропускной способностью всего в 1,544 Мбит/с, то необходимо организовать в сети здания В собственные внутренние сервера, синхронизируемые с общекорпоративными серверами в здании А.

Таблица 7 Распределение IP адресов по зданию В

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Этаж | Подразделение | Число РС (с запасом 50%) | Выделяемое число IP адресов | Общее число IP на этаже |
| 3 | M1 | 250(375) | 512(10.55.8.0/23) | 1568 |
| 2 | M2 | 352(528) | 512(10.55.10.0/23) |
| 1 | P | 370(555) | 512(10.55.12.0/23) |
| 1 | Корпоративные сервера | 15(45) | 32(10.55.14.0/27) |

В виду возможности дальнейшего роста производственных мощностей резервируем для здания всю сеть 10.55.14.0.0/23 (512 адресов), из которой используется уже диапазон 10.55.14.0/27 (32 адреса) под серверы здания B.

Так как сеть здания В должна быть достаточно самостоятельно, то в ней необходимо развернуть собственные сервера DNS, DHCP, основной и резервный контролер домена, а так же сервера приложений и подразделений.

3.1.3 Выделение подсетей и распределение IP адресов по подсетям здания С

Так как здание B соединено с головным зданием А через канал ADSL, чья пропускная способность до 6,1 Мбит/с с дозвоном по требованию, то необходимо организовать в сети здания С собственные внутренние сервера, синхронизируемые с общекорпоративными серверами в здании А только при установлении канала связи.

Таблица 7 Распределение IP адресов по зданию C

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Этаж | Подразделение | Число РС (с запасом 50%) | Выделяемое число IP адресов | Общее число IP на этаже |
| 1 | R1 | 180(240) | 256(10.55.16.0/24) | 256 |
| 2 | R2 | 60(90) | 256(10.55.17.0/24) | 288 |
| 2 | Корпоративные сервера | 15(45) | 32(10.55.18.0/27) |

В виду возможности дальнейшего роста мощностей резервируем для здания всю сеть 10.55.18.0/24 (256 адресов), из которой используется уже диапазон 10.55.18.0/27 (32 адреса) под серверы здания C.

Так как сеть здания C должна быть достаточно самостоятельно, то в ней необходимо развернуть собственные сервера DNS, DHCP, основной и резервный контролер домена, а так же сервера приложений и подразделений.

3.2 Размещение серверов DNS

Структуры AD, DNS и DHCP достаточно сильно взаимосвязаны, особенно AD и DNS, поэтому их развертывание следует рассматривать в комплексе. В частности, DNS желательно развертывать одновременно с AD, так как в этом случае гарантируется их совместимость и облегчается процесс взаимной настройки.

Прежде чем приступать к проектированию структуры Active Directory, рассмотрим сначала реализацию DNS. Предполагается применить нестандартный подход, а именно – использовать т. н. разделение DNS (split-brain DNS). Разделенный DNS делает ресурсы доступными, прозрачными и независимыми по расположению для внешних и для внутренних пользователей. Под прозрачностью понимается, что пользователю не нужно использовать различные имена или перенастраивать клиентские приложения на использование разных имен в зависимости от его местоположения в настоящий момент.

Разделение DNS работает за счет того, что используется 2 или больше доступных серверов DNS, предназначенных для этого имени домена. Один или больше серверов отвечают за разрешение имен для хостов внутренней сети, другие же (один или больше) серверы отвечают за разрешение имен для хостов в Internet.

Сервер DNS, ответственный за разрешение имен во внутрикорпоративной сети, содержит записи DNS, которые отображают имена серверов в их внутренние IP-адреса, которые и используются во внутренней сети. DNS-сервер; ответственный за разрешение имен для внешних пользователей, отображает имена во внешние IP-адреса, обеспечивая доступ к корпоративным ресурсам снаружи.

Внутренние серверы DNS размещаются в Intranet за сетевым экраном (firewall), а внешние серверы DNS устанавливаются в демилитаризованной зоне (DMZ) или в Internet. При этом только внутренние клиенты имеют доступ к внутреннему серверу DNS, хранящему адресную информацию о компьютерах внутренней сети. Запросы внешних клиентов о доменных Internet-именах и адресах организации выполняются внешним DNS-сервером. Любые запросы, идущие из Internet в Intranet, запрещены. Если на внутренний DNS-сервер приходит запрос о разрешении имени Internet, которого нет в локальном кэше, то запрос отправляется на внешний DNS-сервер. На внешнем сервере DNS разрешаются только запросы, исходящие из внутренней сети.

Зоне DNS в домене AD свойственны две особенности. Во-первых, AD сохраняет в DNS большое количество данных. Во-вторых, значительная часть этой информации носит конфиденциальный характер. В частности, в зоне домена AD хранятся имена и адреса контроллеров домена. Структура с разделением DNS позволит скрыть эту информацию от посторонних глаз.

Для корпорации CorpKAM необходимо зарегистрировать домен второго уровня. Например, corpkam.ru. Для обеспечения автономности сетей отдельных филиалов и рационального обмена служебной информацией через WAN, выделим в домене corpkam.ru. два дочерних поддомена: manuf. corpkam.ru. и res.corpkam.ru соответственно для зданий B и C.

Согласно рекомендации технического задания, DNS-сервер вместе с основным контроллером домена AD будут базироваться на платформе Windows 2003 Enterprice Server. Для обеспечения надежности с ним в паре будет работать еще один сервер (Secondary), который сможет обеспечивать работоспособность сети в случае выхода из строя первого сервера. В нашем случае оценивая вариант выхода из строя только первичного сервера, ввиду конкретно его технических или программных неисправностей, целесообразным будет размещение вторичного сервера в том же здании.

Получив запрос на преобразование имени, основной DNS-сервер сначала обращается в кэш. Если имени в кэше нет, а DNS-сервер содержит зоны, то сервер пытается преобразовать имя, проверяя зоны. Сервер обращается к ретранслятору (установленному в DMZ) или в Интернет лишь в том случае, если не может найти нужный адрес в кэше или в зонах. Главная особенность разделенной DNS заключается в том, что DNS-сервер больше доверяет информации из зон, чем данным, извлеченным из Интернета.

Для функционирования такой структуры необходимо на внутреннем DNS-сервере в качестве forwarder’а установить внешний DNS-сервер, а на внешнем DNS-сервере установить либо режим рекурсивного запроса к DNS провайдера, либо итеративный опрос DNS-серверов, начиная с корневых (root-hints). Форвардинг запросов будет осуществляться на кэширующий сервер, что позволит благодаря использованию кэша снизить нагрузку при обработке «внешних» запросов, так как в основной массе запросы будут касаться разрешения имен машин корпоративной сети.

В реализации структуры DNS главного здания участвуют 3 DNS-сервера: внутренний, внешний и сервер провайдера. Внутренний сервер отвечает за зоны main. corpkam.ru (куда входят все отделы здания А), proj.corpkam.ru (планируется создать специальный домен для проектов в Active Directory). Внешний сервер устанавливается в качестве forwarding-сервера для внутреннего для того, чтобы перенаправлять запросы, не разрешенные с помощью кэша. Внешний DNS-сервер, в свою очередь, отправляет рекурсивные запросы к DNS-серверу провайдера.

DNS-серверы в зданиях B пересылают неразрешённые запросы на DNS-сервер здания A.

Для того чтобы из здания C можно было разрешать имена компьютеров, располагающихся в здании B без нагрузки на DNS-серверы здания А, необходимо на DNS-сервере здания C создать так называемые зоны-заглушки или упрощённые зоны (stub-zone). Упрощенная зона представляет собой копию зоны, содержащую только те ресурсные записи, которые необходимы для локализации DNS-серверов, являющихся носителями полной версии зоны. Основное назначение упрощенной зоны – идентификация DNS-серверов, которые способны выполнить разрешение доменных имен, принадлежащих к этой зоне.

Таким образом, на DNS-сервере здания C будет создана stub-zone для каждой из зон здания A и для зоны здания B. А в качестве forwarder-DNS выступит DNS-сервер провайдера.

На всех внутренних DNS-серверах следует включить режим Dynamic DNS Updates, для того, чтобы узлы могли регистрировать свои записи в соответствующих зонах. Поскольку мы используем ADIZ, рекомендуется также включить режим безопасных обновлений (secure updates). В этом режиме администратор AD может определять, кому и какие действия разрешается выполнять над ресурсными записями DNS.

3.3 Размещение серверов WINS

Согласно заданию на курсовую работу, среди рабочих станций в сети корпорации есть машины под управлением ОС Windows 98, которые используют имена NetBIOS. Поэтому наряду с DNS в проектируемой сети должна быть реализована служба разрешения имен NetBIOS. Для этой цели необходимо установить серверы WINS.

Сервер WINS рассчитан на высокую нагрузочную способность и может один обслуживать компанию с 10-15 тысячами компьютеров. Имена NetBIOS являются 16-байтными адресами, которые однозначно идентифицируют узлы в сети. Этот адрес имеет длину в 15 знаков и 16-тый используется для однозначной идентификации службы, запущенной на системе, такой, например, как службы Сервера или Рабочей Станции. Основная цель использования WINS – это разрешение имен NetBIOS в IP-адреса. Как и в случае NT 4, системы, настроенные на использование службы WINS, при загрузке будут регистрировать свои имена NetBIOS и соответствующие им IP-адреса. В целях повышения надежности установим в главном здании 2 WINS-сервера, а в зданиях филиалов – по одному WINS-серверу.

Сервер WINS можно задействовать совместно с сервером DNS для разрешения имен NetBIOS. Для этого на сервере DNS используются записи типа WINS. Если сервер DNS снабжен адресом сервера WINS (при помощи записи WINS), то сервер DNS будет пытаться опрашивать сервера WINS для разрешения имен, не найденных в собственной базе данных.

Обычно серверы WINS можно разместить на контроллерах домена. Например, если AD спланирована так, что имеется корневой домен, не содержащий пользователей и применяемый лишь как держатель имени домена и административных групп, то его контроллеры домена не очень загружены и могут выполнять дополнительные функции.

3.4 Размещение серверов DHCP

Каждому хосту, подключенному к сети на базе TCP/IP, должен быть назначен уникальный IP-адрес. Протокол DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) был разработан как средство динамического выделения хостам IP-адресов. Протокол DHCP является открытым промышленным стандартом, упрощающим управление сетями на базе TCP/IP. Этот протокол также может быть использован для централизованного управления процессом настройки стека протокола TCP/IP на клиентских машинах (речь идет о таких параметрах, как адрес шлюза по умолчанию или адрес DNS-сервера).

В спецификации протокола DHCP определяются два участника: DHCP-сервер и DHCP-клиенты. Служба клиента DHCP запрашивает у DHCP-сервера параметры для настройки стека протоколов TCP/IP. Служба сервера DHCP обрабатывает клиентские запросы, осуществляя выдачу в аренду IP-адреса из некоторого диапазона. Каждый адрес выделяется на определенный срок. По окончании этого срока хост должен либо продлить срок аренды, либо освободить адрес. Все удовлетворенные запросы пользователя фиксируются службой сервера DHCP в собственной базе данных. Подобное решение позволяет предотвратить выделение одного IP-адреса двум хостам. Одновременно с выдачей IP-адреса DHCP-сервер может также предоставить клиенту дополнительную информацию о настройках стека протоколов TCP/IP, такую как маска подсети, адрес шлюза и адреса серверов DNS и WINS.

В составе Windows Server 2003 реализован как DHCP-клиент (который устанавливается по умолчанию), так и DHCP-сервер (который может быть установлен и сконфигурирован администратором при необходимости).

Запрос к серверу DHCP посылается клиентом широковещательно, следовательно, не может выйти за пределы локальной подсети. Чтобы клиент из подсети, не соединенной непосредственно с DHCP сервером, мог получать от него IP адреса, необходимо убедиться, что маршрутизатор (в нашем случае, коммутатор 3 уровня), объединяющий подсети, поддерживал направление широковещательных сообщений DHCP, то есть поддерживал стандарт RFC 1542. В противном случае необходимо будет установить в каждой из подобных подсетей агент ретрансляции DHCP (DHCP Relay Agent) или сервер DHCP. Агент ретрансляции DHCP – это хост, который прослушивает подсети на наличие широковещательных сообщений DHCP/BOOTP и переадресовывает их на некоторый заданный DHCP-сервер. Использование агентов ретрансляции избавляет от необходимости устанавливать сервер DHCP в каждом физическом сегменте сети. Агент не только обслуживает прямые локальные запросы клиента DHCP и перенаправляет их на удаленные DHCP-серверы, но также возвращает ответы удаленных DHCP-серверов клиентам.

Используемый для объединения подсетей коммутаторы ГП Baseline Switch 2916-SFP Plus не поддерживает стандарт RFC 1542, поэтому агент ретрансляции необходим в каждой подсети ГП (один на этаж). Для них должны быть выделены статические IP –адреса из пула, выделенных для серверной комнаты.

Для повышения надежности во всех зданиях корпорации будем использовать по 2 DHCP-сервера в связи с довольно большим числом рабочих станций в них и для повышения надежности.

Для того чтобы DHCP-сервер начал корректно работать, необходимо на нем настроить области (т. н. scopes). Область DHCP – административная группа, идентифицирующая полные последовательные диапазоны возможных IP-адресов для всех клиентов DHCP в физической подсети. Области определяют логическую подсеть, для которой должны предоставляться услуги DHCP, и позволяют серверу задавать параметры конфигурации, выдаваемые всем клиентам DHCP в подсети. Область должна быть определена прежде, чем клиенты DHCP смогут использовать сервер DHCP для динамической конфигурации TCP/IP.

В главном здании выделим 9 областей в соответствии с числом отделов. Пусть области отделов HR, Sales, IT, Exec, Bus, Acc, Project 1, Project 2 обслуживаются одним DHCP-сервером, а области отдела Project 3 – другим. В этом случае между серверами будет соблюдена пропорция 80/20 по количеству обслуживаемых рабочих станций, как и рекомендует Microsoft.

Настройка DHCP областей на каждом сервере включает следующее:

- Начальный адрес (start IP address);

- Конечный адрес (End IP address);

- Маска подсети (Subnet mask length);

- Исключения (Exclusions)

- Резервирование (Reservation).

Рассмотрим настройку DHCP-области на примере отдела HR (ей соответствует диапазон 10.55.0.192/26): начальным адресом будет являться 10.55.0.192, конечным - 10.55.0.255. Маска подсети – 26 (то есть, 255.255.255.192), а диапазон статических адресов определим следующий: 10.55.4.1 – 10.55.4.10.

В здании B отдадим под управление одному DHCP-серверу отделы M1 и M2, а второму серверу – отдел P. Опять будет соблюдена пропорция количества обслуживаемых серверами рабочих станций 80/20, обеспечена некоторая отказоустойчивость.

В здании C выделим области (scopes) в соответствии с отделами R1 и R2.

Наличие двух серверов DHCP в сети может при определённых условиях привести к её частичной или полной неработоспособности. Подобное было возможно в более старых ОС из-за того, что практически любой мог активизировать свой сервер DHCP. Для того чтобы этого не случилось, необходимо авторизовать установленные DHCP-серверы в Active Directory. В этом случае при попытке запустить службу DHCP происходит обращение к Active Directory, где просматривается список адресов IP для всех авторизованных в домене серверов DHCP. Если адреса рассматриваемого сервера нет, то служба DHCP будет автоматически на нем терминирована.

сервер пользователь филиал сеть беспроводный

3.5 Разработка структуры Active Directory(AD)

Active Directory – это служба каталогов в Windows 2003 Server. Active Directory содержит каталог, в котором хранится информация о сетевых ресурсах и службы, предоставляющие доступ к этой информации. Ресурсы, хранящиеся в каталоге, такие, как данные, сведения о принтерах, серверах, базах данных, группах, службах, компьютерах, политике безопасности, – называются объектами (object). Active Directory встроена в Windows 2003 Server и обеспечивает:

- упрощенное администрирование;

- масштабируемость;

- поддержку открытых стандартов;

- поддержку стандартных форматов имен.

Active Directory иерархически упорядочивает ресурсы в домене – логическом объединении серверов и других сетевых ресурсов в единое имя домена. Домен является основной единицей репликации и безопасности в сети Windows 2003.

Логическая часть Active Directory включает в себя лес, деревья, домены и OU (организационные подразделения, ОП). Физическая часть – сайты и контроллеры домена. Пространство имен Active Directory будет базироваться на ранее описанной структуре доменных имен службы DNS.

Один домен способен поддерживать до 10 миллионов объектов каталога. Согласно этому утверждению, можно было бы для всей корпорации создать один домен. Однако при создании доменов следует руководствоваться другими критериями – не только количеством объектов, которые могут быть созданы в Active Directory.

Первый критерий – административная политика. Необходимо так спроектировать систему, чтобы ей было проще управлять.

Второй критерий – безопасность. Внутри домена действуют правила безопасности, не распространяющиеся за его пределы.

Третий критерий – размер. Управлять доменом с огромным числом пользователей может оказаться значительно сложнее, чем несколькими доменами с меньшим числом объектов.

Несмотря на то, что у однодоменной структуры есть свои преимущества (простота управления; меньшая стоимость; меньшее число администраторов; предельная емкость, равная емкости леса доменов), предпочтение при проектировании Active Directory в корпорации CorpKAM отдадим многодоменной структуре. А именно – лесу.

Одной из причин, по которым выбирается структура с несколькими доменами, является как раз безопасность. Если в организации существуют ОП, требования к безопасности которых существенно отличаются от остальных, то такие подразделения лучше выделить в отдельные домены. Проблема безопасности также тесно связана с полномочиями администраторов. Если взять администраторов единственного домена (а значит, и корневого домена в лесу), то по умолчанию они включены в такие группы как Domain Admins, Schema Admins, Enterprise Admins. Последние два наделены огромными полномочиями в рамках леса, которые нужны далеко не всем администраторам. Чтобы у администратора не было возможности самостоятельно включить себя в группу с обширным списком прав, целесообразно создавать корневой домен пустым – в котором нет пользователей, но есть учетная запись администратора предприятия. В остальных хранятся учетные записи пользователей и администраторов домена.

Создание пустого корневого домена для хранения в нем учетных записей администратора предприятия обязательно при наличии более чем одного дочернего домена или нескольких деревьев в лесу. В нашем случае дочерних доменов планируется создать как минимум 2 (для зданий B и C), поэтому создадим пустой корневой домен.

Пустой корневой домен играет и ещё одну важную роль. Это своего рода «хранитель имени» организации. Так как корневой домен дает имя всему лесу, то никакие изменения в нижележащей доменной структуре не отражаются в имени леса. Можно легко добавлять новые домены в лес или удалять их из леса.

Еще один положительный фактор наличия пустого корневого домена в том, что в нем нет значительных нагрузок на контроллеры, и надежность их от этого возрастает. Поэтому в этом домене можно разместить глобальный каталог и мастера схемы и именования доменов, которые можно будет задействовать для восстановления системы.

Естественно, у структуры леса с пустым корневым доменом есть и недостаток – необходимость использовать 2 дополнительных сервера в качестве контроллеров домена. Но аппаратные требования к таким контроллерам невысоки, поэтому не будем принимать во внимание указанный недостаток.

Развертывание сетевой структуры начнем с пустого корневого домена corpKAM.ru. Дочерние домены будут выделены соответственно для главного здания (main.corpkam.ru), здания B (manuf.corpkam.ru) и здания C (res.corpkam.ru). Также предполагается создать еще один дочерний домен с особой политикой безопасности (например, для проектов). Конфигурация этого домена будет меняться в зависимости от текущих проектов. Назовем его, например, proj.corpkam.ru.

Заканчивая проектирование логической структуры Active Directory, надо сказать об организационных подразделениях (ОП), которые используются:

- для делегирования административных полномочий;

- для разграничения групповой политики;

- для рассортировки объектов;

- для ограничения числа объектов в контейнерах;

- для помощи в миграции.

Предполагается для каждого отдела создать ОП. Таким образом, в здании A будет 9 ОП, в здании B – 3 ОП, и в здании C – 2 ОП. В домене проектов (proj.corpiso.ru) организационные подразделения будут создаваться в соответствии с текущими проектами компании.

Перейдем к физической структуре Active Directory. Начнем её рассмотрение с сайтов. Сайт – это часть физической структуры Active Directory, совокупность одной или нескольких IP-подсетей, соединенных высокоскоростными каналами связи. Основная задача сайта – обеспечивать хорошее сетевое соединение.

Проектируемую корпоративную сеть можно представить как 3 области с качественными линиями связи LAN (они соответствуют сетям головного офиса и двух филиалов), которые соединены между собой линиями связи WAN, имеющими другое качество и пропускную способность. Следовательно, целесообразно представить физическую структуру сети в виде трех сайтов. Каждый сайт соответствует одному зданию корпорации. Отдельный сайт в Active Directory может включать несколько доменов. Сайт в здании A будет включать в себя 3 домена: пустой корневой, домен здания A и домен проектов. В зданиях B и C сайты будут содержать по одному домену.

Как только будет завершена работа по созданию сайтов, рабочие станции при входе домен будут регистрироваться на контроллере домена, входящем в данный сайт, а не посылать запросы через WAN. Репликацию же контроллеров доменов можно настроить с помощью сайтов. Таким образом, у администраторов есть удобный механизм контроля и регулирования межсайтового трафика.

Теперь необходимо определить, какое количество контроллеров нужно разместить в каждом домене. Для каждого домена нужен как минимум один контроллер. Однако в крупных сайтах одного контроллера на домен может оказаться недостаточно. В случае недоступности единственного контроллера в сайте весь трафик регистрации в сети будет направлен по каналу. Время регистрации может заметно возрасти. Наличие нескольких контроллеров домена в крупном сайте дает некоторые преимущества. Одно из них – повышение надежности.

Проектируя AD для крупного предприятия, стоит подумать об оптимальном расположении мастеров операций.

Мастер схемы (Schema Master) — единственный во всем лесу мастер операций, ответственный за внесение изменений в схему. Изменения в схему может вносить администратор с полномочиями Schema Admins. Так как эта группа располагается только в корневом домене леса, то целесообразно и мастер схемы держать там же. В нашем случае пустой корневой домен — идеальное место для мастера схемы. Компьютер с мастером схемы не несет особой нагрузки, так как схема модифицируется крайне редко. Мастер схемы по умолчанию размещается на самом первом контроллере домена в лесу. В силу его небольшой загруженности его можно там и оставить.

Мастер доменных имен(Domain Naming Master) также один на весь лес. Он отвечает за добавление в лес новых доменов, кроме существующих, и за добавление/удаление объектов кросс-ссылок на внешние каталоги. Эти операции может выполнять только администратор с правами Enterprise Admins, следовательно, как и мастера схемы, мастер доменных имен разместим в пустом корневом домене. Мастер доменных имен отвечает за то, чтобы имена доменов в лесу были уникальны. Когда добавляется новый домен, этот мастер обращается к серверу ГК в поисках такого имени. Именно поэтому он должен располагаться на одном сервере с сервером ГК. Компьютер, на котором располагается мастер доменных имен, не несет практически никакой нагрузки, так как домены в лес добавляются нечасто. Это позволяет поместить его на одном компьютере с мастером схемы. Он должен быть доступен из любой точки сети.

Имитатор PDC (PDC Emulator)прежде всего нужен для клиентов старого типа (ранее Windows 2000), так как, с их точки зрения, он играет роль главного контроллера домена. Помимо этого, он выполняет роль master browser для приложений, использующих NetBIOS. Он отвечает за срочное тиражирование изменений в AD, таких как смена паролей или блокировка учетных записей. Кроме того, он отвечает за аутентификацию пользователей, сменивших пароль.

Следует учитывать, что для каждого домена должен быть свой имитатор PDC и имитатор PDC должен быть всегда доступен для других контроллеров в домене, а также в больших доменах имитатор PDC несет повышенную нагрузку и его целесообразно размещать на отдельном сервере.

Мастер относительных идентификаторов (Relative Identifier Master) хранит общий пул идентификаторов домена и выдает их контроллерам по мере необходимости, при этом обеспечивается уникальность RID в домене, переносит объекты из одного домена в другой: при переносе между доменами у учетной записи меняется DN и SID, а уникальный ID остается неизменным. Компьютер, выполняющий данную роль, относительно не загружен, поэтому может располагаться на тех же контроллерах, где и другие мастера доменных операций.

Мастер инфраструктуры (Infrastructure Master) периодически проверяет ссылки на отсутствующий на данном контроллере домена объект в доступной ему реплике базы AD. Для этого он обращается к ГК и проверяет, не изменились ли у объекта с данным GUID его DN и SID. Если они изменились, то соответствующие изменения вносятся в локальную реплику и тиражируются на остальные контроллеры в домене.

Если мастер инфраструктуры находится на том же компьютере, что и ГК, то он не функционирует. Это связано с тем, что компьютер, исполняющий роль ГК, хранит реплики всех объектов в лесу, а значит, нет ссылок на отсутствующие объекты. Если все контроллеры в домене являются ГК, то надобности в мастере инфраструктуры нет, и он может не работать. Таким образом, мастер инфраструктуры должен быть один в каждом домене, не должен располагаться на сервере ГК и должен быть слабо загружен и может располагаться на одном сервере с другими мастерами в домене.

Учитывая все сказанное выше, предлагаем следующую схему размещения мастеров: в каждом домене устанавливается как минимум два сервера-контроллера домена, причем на первом сервере размещается ГК и мастер относительных идентификаторов. Этот же сервер выступает в роли форпоста при междоменной репликации. На втором сервере устанавливается имитатор PDC и мастер инфраструктуры.

Для поддержки целостности информации в сети, необходимо организовать репликацию AD. В Windows 2003 действует модель multi-master (нескольких главных), означающая, что на любом контроллере домена можно производить обновления в Active Directory. Однако, вместе с усложнением репликации в Windows 2003 Active Directory, здесь так же присутствует возможность более простого контроля процесса репликации, через использование сайтов, site links (связей сайтов) и работы по расписанию. В среде Active Directory контроллерам домена нет необходимости связываться с одним главным контроллером домена для получения изменений. Вместо этого, они создают связи друг с другом для отслеживания, какой контроллер домена будет выступать в качестве источника репликации изменений. Эти взаимоотношения называются connection objects (объекты-подключения). Процесс, который создает объекты подключения между контроллерами домена, запускается на всех контроллерах домена автоматически и называется Knowledge Consistence Checker (KCC - дословно: служба проверки непротиворечивости знаний). КСС стартует каждые 15 минут и вносит изменения в топологию объектов-подключения, если это необходимо (например, если какой-либо из контроллеров домена временно недостижим).

Внутрисайтовая репликация:

1. RPC over IP – Remote Presage Call over IP – асинхронный трафик, несжимаемый, не требует сертификатов.
2. SMTP- асинхронный, сжатый, требует сертификата

Active Directory реплицирует информацию в пределах сайта чаще, чем между сайтами, сопоставляя необходимость в обновленной информации каталога с ограничениями пропускной способности сети.

В пределах сайта Active Directory автоматически создает топологию репликации между контроллерами одного домена с использованием кольцевой структуры. Топология определяет путь передачи обновлений каталога между контроллерами домена до тех пор, пока обновления не будут переданы на все контроллеры домена.

Для обеспечения репликации между сайтами нужно предоставить сетевые соединения в виде связей сайтов. Active Directory использует информацию о сетевых соединениях для создания объектов соединений, что обеспечивает эффективную репликацию и отказоустойчивость.

3.6 Организация беспроводного доступа к сети (WLAN)

Две независимые группы сотрудников отдела маркетинга работают на ноутбуках и для них необходимо создать беспроводную сеть WLAN.

Беспроводные локальные сети кратко обозначаются аббревиатурой WLAN (Wireless Local Area Network). Самым распространенным на сегодняшний день стандартом беспроводных сетей является Wi-Fi. Он соответствует спецификации IEEE 802.11, которая, в свою очередь, имеет несколько модификаций, обозначаемых буквами a, b, g и n. Беспроводные сети претерпели много модификаций, сейчас наиболее распространены сети, поддерживающие протокол спецификации IEEE 802.11g, обеспечивающие в зоне прямой видимости скорость передачи данных до 54 Мбит/с. Для работы с WiFi необходимо выбрать протоколы аутентификации.

Операционные системы семейства Windows Server 2003 поддерживают протокол MS-CHAP v2, обеспечивающий взаимную проверку подлинности, создание более надежных начальных ключей шифрования данных для MPPE (Microsoft Point-to-Point Encryption) и разные ключи шифрования для отправки и приема данных. Чтобы свести к минимуму риск раскрытия пароля во время обмена паролями, из протокола исключена поддержка старых методов обмена паролями MS-CHAP. Поскольку версия MS-CHAP v2 обеспечивает более надежную защиту, чем MS-CHAP, при подключении сначала предлагается использовать именно ее (если она доступна), а затем уже MS-CHAP. Протокол MS-CHAP v2 поддерживается на компьютерах, работающих под управлением Windows XP, Windows 2000, Windows 98, Windows Millennium Edition и Windows NT 4.0. Компьютеры, работающие под управлением Windows 95, поддерживают MS-CHAP v2 только для подключений VPN, но не для подключений удаленного доступа.

Из-за нецелесообразности использования центра сертификации выбираем метод аутентификации EAP-MS CHAP V2, который является самым распространенным, наиболее дешевым и достаточно надежным.

Для организации доступа используется точка доступа WiFi 3CRWE454G75. Она поддерживает стандарт IEEE 802.11g и WPA, в состав которого входит EAP, выступающий каркасом для различных протоклов аутентификации, в том числе и MS CHAP V2.

3.7 Организация DMZ

Суть DMZ заключается в том, что она не входит непосредственно ни во внутреннюю, ни во внешнюю сеть, и доступ к ней может осуществляться только по заранее заданным правилам межсетевого экрана. В DMZ нет пользователей – там располагаются только серверы. Демилитаризованная зона, как правило, служит для предотвращения доступа из внешней сети к хостам внутренней сети за счет выноса из локальной сети в особую зону всех сервисов, требующих доступа извне.

В состав DMZ входят:

- сервера DMZ: Mail, Web, ftp, внешний DNS и RAS;

- средства изоляции (межсетевые экраны);

- коммутационное оборудование DMZ (коммутатор РГ и прочее оборудование, обеспечивающее связь с другими зданиями и сотрудниками корпорации по выделенным каналам).

В качестве серверов Mail, Web и ftp берем свободное ПО, распространяемое по лицензии GNU(или схожим). В частности, в качестве ОС используем FreeBSD, ориентированную на работу в сети. Для этой ОС существуют все указанные сервера в виде свободно распространяемых продуктов, поэтому их выбор должен осуществляться при консультации с отделом эксплуатации сети. Например, в качестве Web – сервера может быть развернут Apach вместе с PHP и MySQL или PostgreSQL. Поддержка мировым сообществом этих продуктов достаточно сильная. Тоже самое относится и большинству других решений для указанных серверов.

Для снижения стоимости DMZ следует физически разместить сервера, выполняющие схожую по нагрузке работу, на одном физическом сервере. Для этого развернем на одном сервере Mail и ftp, а на другом Web сервер.

Отдельно ставится сервер RAS на основе Windows Server 2003, так как он призван обеспечить доступ к сети для удаленных пользователей. Развернуть его на FreeBSD не получится. В добавок, служба DNS должна быть связана со службой AD, поэтому ее также лучше развернуть на сервере с OC Windows 2003 Server.

Для защиты проникновения через демилитаризованную зону в корпоративную сеть используются межсетевые экраны. Существуют программные и аппаратные экраны. Для программных требуется отдельная машина. Для установки аппаратного брандмауэра (программируемого моста) нужно лишь подключить его в сеть и выполнить минимальное конфигурирование. Обычно программные экраны используются для защиты сетей, где нет необходимости производить много настроек, связанных с гибким распределением полосы пропускания и ограничения трафика по протоколам для пользователей. Если сеть большая и требуется высокая производительность, выгоднее становится использовать аппаратные межсетевые экраны.

1) При достаточном финансировании используются 2 firewall-а – один отделяет DMZ от внешней сети, другой- DMZ от локальной сети

2) При ограниченном финансировании используется более дешевый вариант: использованию одного сервера с тремя сетевыми интерфейсами. Тогда один интерфейс «смотрит» в Интернет, второй – в DMZ и третий – в локальную сеть.

При реализации такого варианта необходимо обратить внимание на его недостатки:

- Снижение надежности сети. В случае зависания или перезагрузки сервера ресурсы, находящиеся в DMZ, будут временно недоступны пользователям;

- В случае его выхода из строя все то время, которое вы потратите на замену, локальная сеть организации будет практически неработоспособна;

- Слабая защита от вмешательств извне.

Если используются два межсетевых экрана, то все эти недостатки частично или полностью можно устранить. В случае выхода из строя одного из них в течение буквально нескольких минут сеть из варианта «1» можно превратить в вариант «2», добавив в сервер еще одну сетевую карту и произведя соответствующие изменения в настройках. К тому же безопасность сети при использовании двух межсетевых экранов повышается. Например, если взломщик сумел проникнуть на сервер, подключенный к WAN и DMZ, то ему не будут доступны ресурсы локальной сети.

Остановимся на втором варианте при использовании программного firewall. В качестве ОС для firewall выбираем FreeBSD, в качестве программного firewall – пакет Smoothwall. В коммерческой версии этот продукт обладает мощным набором настроек и предоставляет большие возможности по фильтрации пакетов. Так же он предоставляет возможность организации NAT(п. 3.7.1), что важно для внешнего FireWall-a.

Оборудование, которое потребуется для такой организации DMZ, следующее:

- 5 серверов;

- 1 коммутатор ГП;

- коммутационное оборудование в составе маршрутизаторов 5680 и OfficeConnect ADSL Wireless.

3.7.1 Распределение внешних IP адресов, использование NAT

Технология NAT позволяет выполнять трансляцию адресов из локальных в глобальные через подмену портов. Подмена должна происходить до попадания в WAN, то есть внутри DMZ.

Для обеспечения доступа к серверам DMZ им должен быть назначены внешние IP адреса из доступного по заданию диапазона. Для обеспечения подключения пользователей через Dial-Up (п. 3.7.3) реализацию технологии NAT необходимо сделать на внешнем firewall. Так же необходимо назначить статические внешние IP адреса на все сетевые интерфейсы внутреннего firewall, кроме связанного с локальной сетью.

3.8 Подключение филиалов и удаленных пользователей

Согласно заданию на курсовую работу, все три здания корпорации CorpKAM географически разнесены, поэтому необходимо определить, каким образом будет происходить подключение филиалов к главному зданию A.

3.8.1 Подключение здания В по каналу Т1

Здание В расположено в другом городе, удалённом на значительное расстояние от главного офиса. Для его подключения арендуется канал T1. Для обеспечения репликации сайтов и зон DNS, целесообразно подключить выделенный канал к коммутатору, соединяющему корпоративные серверы в демилитаризованной зоне. На стороне здания B используется специальный маршрутизатор 5680, имеющий возможность подключения каналов T1. В здании А стоит аналогичный маршрутизатор.

Канал T1 - первичный канал иерархии PDH - является основным каналом, используемым во вторичных сетях телефонии, передачи данных и ISDN. Структура систем передачи T1 включают три уровня эталонной модели OSI: физический, канальный и сетевой. Физический уровень описывает электрический интерфейс потока T1, а также параметры сигнала T1.

Канальный уровень описывает процедуры мультиплексирования и демультиплексирования каналов более низкого уровня иерархии (ОЦК 64 кбит/с и каналов ТЧ) в поток T1, цикловую и сверхцикловую структуру потока T1, встроенные процедуры контроля ошибок и т.д. Наконец, сетевой уровень описывает процедуры управления каналами T1 в первичной сети, а также контроль параметров ошибок на сетевом уровне. Этот уровень является относительно неполным и включает всего лишь несколько процедур. Основным же для рассмотрения систем передачи T1 является структура канального уровня. Рассмотрим более подробно структуру каждого из трех уровней систем T1.

Используемые типы кодирования: HDB3 (стандартизирован), либо AMI.

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень цифровой иерархии | Скорости передачи, соответствующие различным системам цифровой иерархии, кбит/с |  |  |
|  | Американский стандарт(Tx) | Японский стандарт(DSx)Jx | Европейский стандарт(Ex) |
| 1 (первичный) – T1 | 1544 (24 канала) | 1544 (24 канала) | 2048 (30 каналов по 64kbps) |
| 2 (вторичный) – T2 | 6312 (96 каналов) | 6312 (96 каналов) | 8448 (120 каналов по 64kbps) |
| 3 (третичный) – T3 | 44736 (672 канала) | 32064 (480 каналов) | 34368 (480 каналов по 64kbps) |
| 4 (четвертичный) - T4 | 274176 (4032 канала) | 97728 (1440 каналов) | 139264 (1920 каналов по 64kbps) |
| 5 (пятеричный) | \*не используется\* | 397200 | 564992 |

Таким образом, выбранный маршрутизатор подключается к одному из портов коммутатора, объединяющего серверы в демилитаризованной зоне здания А. Поскольку для соединения филиала В с главным офисом не используется никакая публичная сеть, то на этом канале организовывать VPN с целью защиты данных не будем.

3.8.2 Подключение здания С по каналу ADSL

Филиал Research (здание C) связывается с главным офисом через Internet маршрутизаторами с функцией «дозвон по требованию», используя подключение ADSL. Выбранный маршрутизатор OfficeConnect ADSL Wireless не поддерживает функцию «дозвон по требованию», поэтому для обеспечения автодозвона будет использоваться сервер двумя сетевыми интерфейсами с ОС FreeBSD через пакет PPPD. Помимо маршрутизации, эта машина будет выполнять роль межсетевого экрана, для чего на ней будет установлен пакет Smoothwall. Выбранный маршрутизатор имеет средства для организации VPN-туннелей с аппаратным шифрованием данных по протоколам WPA/WPA2 шифрование 128- bit с TKIP/AES wireless encryption, 40/64-bit и 128-bit WEP шифрование. Для сохранения конфиденциальности данных, передаваемых между зданиями A и C, организуем VPN-туннель.

ADSL (Asymmetric Digital Subscriber Line - Асимметричная цифровая абонентская линия) входит в число технологий высокоскоростной передачи данных, известных как технологии DSL (Digital Subscriber Line - Цифровая абонентская линия) и имеющих общее обозначение xDSL.

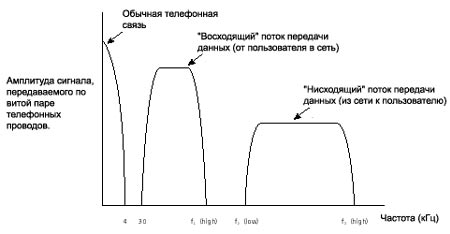


Рисунок 4. Распределение частот в ADSL

ADSL является асимметричной технологией - скорость "нисходящего" потока данных (т.е. тех данных, которые передаются в сторону конечного пользователя) выше, чем скорость "восходящего" потока данных (в свою очередь передаваемого от пользователя в сторону сети).

Технология ADSL использует метод разделения полосы пропускания медной телефонной линии на несколько частотных полос (также называемых несущими). Это позволяет одновременно передавать несколько сигналов по одной линии. Кроме этого может применяться технология эхокомпенсации (Echo Cancellation), при использовании которой диапазоны "восходящего" и "нисходящего" потоков перекрываются (смотрите рисунок 5) и разделяются средствами местной эхокомпенсации.

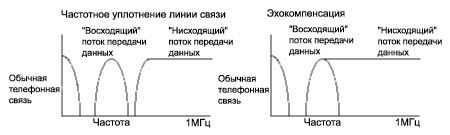


Рисунок 5. Частотное уплотнение линии связи и эхокомпенсация

Для защиты данных при передаче через публичную сеть используется VPN, описание которого приведены ниже в п.3.8.4.

3.8.3 Подключение сотрудников корпорации в Европе по каналам ISDN

Аббревиатура ISDN расшифровывается как цифровая сеть с интеграцией услуг (Integrated Services Digital Network). Технология ISDN базируется на пользовательских каналах со скоростью 64 Кбит/с (так называемых B-каналах) и на отдельном служебном канале (D-канале).

Канал "B" (Bearer) - канал для передачи голоса, данных, видео c пропускной способностью 64 Кбит/с. Он предоставляется "чистым", т.е. вся его полоса пропускания доступна для передачи информации, а вызовы, сигнализация и другая системная информация передается по D-каналу.

Канал "D" (Delta) - служебный канал для передачи управляющих сигналов с пропускной способностью 16 (BRI) или 64 (PRI) Кбит/с. Один канал типа "D" обслуживает 2 или 30 (Европа) В-каналов и обеспечивает возможность быстрой генерации и сброса вызовов, а также передачу информации о поступающих вызовах, в том числе о номере обращающегося к сети абонента.

BRI (Basic Rate Interface) - стандартный базовый интерфейс с пропускной способностью 144 Кбит/с (EuroISDN); он объединяет два канала "B" и один канал "D". К интерфейсу BRI можно подключить до восьми различных ISDN-устройств. При этом каждому устройству выделяется свой индивидуальный номер (multiple subscriber numbers). Очень важная особенность ISDN состоит в том, что для установки BRI-розетки оператору обычно не требуется прокладывать новую телефонную пару - используется обычная линия ТСОП.

Физическим уровнем интерфейса BRI, определяющего правила взаимодействия конечных пользователей и коммутатора ISDN, служит обычная витая пара, которая работает в дуплексном режиме передачи данных, - так называемый U-интерфейс.

PRI (Primary Rate Interface) - этот интерфейс объединяет несколько B-каналов (например, в Европе - 30 В-каналов с общей полосой пропускания 2,048 Мбит/с). В отличие от BRI, он поддерживает только одно оконечное устройство. Но подключив, например, локальную АТС или маршрутизатор c поддержкой ISDN, можно разбить PRI на множество BRI-интерфейсов. В настоящее время для предоставления офисам PRI-сервиса широко используется абонентская цифровая линия на одной (SDSL) или двух (HDSL) телефонных парах.

По сравнению с традиционными аналоговыми сетями, ISDN имеет ряд преимуществ:

* экономия времени благодаря быстрому соединению между абонентами (менее 1 секунды внутри города и не более 10 секунд при междугородном вызове);
* два полноценных городских номера по одной паре проводов, вместо одного, как при аналоговом подключении;
* возможность подключить до 8 различных устройств (компьютер, факс, телефон, видеотелефон и др.), два, из которых могут работать одновременно;
* великолепное качество связи, отсутствие прерываний и посторонних шумов на линии;
* высокая скорость соединения с сетью Интернет - гарантированные 128 Кбит/с до провайдера, вместо негарантированных при аналоговом подключении 51200 Кбит/с (в лучшем случае);
* широкий спектр различных дополнительных услуг (более надежное определение номера вызывающего абонента (CLIP), мультиплексирование абонентских номеров (MSN), мини-АТС, переадресация по различным критериям, 3-х сторонняя конференция и т.д.).

По одной физической паре пользователь получает две независимые цифровые линии по 64 Кбит/c (вместо одной, как аналоговом подключении), которые он может использовать для:

* подключения двух обычных или специальных цифровых телефонов;
* одновременного подключения телефона и ISDN-устройства передачи данных на скорости 64 Кбит/c;
* подключения ISDN-устройства передачи данных на скорости 128 Кбит/c (для подключения к сети Интернет или организации внутрикорпоративной сети).

Кроме этого:

* ISDN может работать со всеми типами информации, включая голос, текст, изображение, аудио- и видеоинформацию;
* ISDN позволяет объединить компьютерные сети компании, имеющей рассредоточенные офисы в как пределах города (звонок бесплатный), так и за его пределами (поминутная оплата за межгород, соединение по требованию - DDR) с гарантированной (в отличие от сети "Интернет") скоростью 64 или 128 Кбит/c;
* стоимость ISDN-оборудования значительно меньше, чем стоимость модемов для выделенных линий;
* абонент получает шестизначный номер городской телефонной сети и имеет возможность пользоваться услугами междугородной связи.

Для защиты данных при передаче через публичную сеть используется VPN, описание которого приведены ниже в п.3.8.4.

3.8.4 Подключение сотрудников по каналам Dial-Up

Согласно заданию несколько привилегированных сотрудников работают в своих домашних офисах SOHO, подключающихся к главному офису по коммутируемым каналам связи Dial-up. Подключение этих клиентов будем осуществлять по VPN на основе службы RAS ОС Windows 2003 Server, так как подключение будет производится через общедоступные телефонные сети. Проверку подлинности удаленных пользователей в этом случае сначала выполняет сторонняя организация (в процессе предоставления доступа по телефонной линии), а затем их аутентифицирует VPN-сервер удаленного доступа (при подключении к частной сети).

При организации VPN могут использоваться усовершенствованные версии протоколов РРР (Point-to-Point Protocol), РРТР (Point-to-Point Tunneling Protocol) и L2TP (Layer 2 Tunneling Protocol). Для обеспечения безопасности конфиденциальных данных будем применять шифрование на основе протокола IPSec в туннелях L2TP, которые являются более надежными, чем туннели PPTP.

VPN-подключение состоит из следующих компонентов:

* VPN-сервер - компьютер, принимающий VPN-подключения от клиентов VPN.
* VPN-клиент - компьютер, инициирующий VPN-подключение к серверу VPN. VPN-клиентом может быть отдельный компьютер или маршрутизатор.
* Туннель - часть подключения, содержащая инкапсулированные данные. Можно создать туннель и передавать по нему данные без шифрования. Это не является VPN-подключением, поскольку личные данные передаются через общедоступную сеть в незащищенном, легко доступном для чтения виде.
* VPN-подключение - часть подключения, содержащая зашифрованные данные.
* Туннельные протоколы - протоколы, используемые для управления туннелями и инкапсуляции личных данных. Операционные системы семейства WS2003 поддерживают туннельные протоколы PPTP и L2TP.
* Туннелированные данные - данные, обычно передаваемые при помощи частного подключения «точка-точка».
* Транзитная объединенная сеть - общедоступная сеть, по которой передаются инкапсулированные данные. В операционных системах семейства WS2003 транзитная объединенная сеть всегда является сетью IP. Транзитной объединенной сетью может быть Интернет или частная интрасеть на основе IP-протокола.

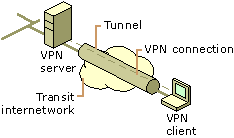


Рисунок 6. Организация VPN-тоннеля

Протоколы туннелирования:

РРТР и L2TP позволяют зашифровать мультипротокольный трафик, а затем инкапсулировать его в IP-заголовок, который будет послан по объединенной IP-сети организации или общественной объединенной IP-сети типа интернета. Основаны на протоколе РРР, следовательно имеют функции для управления сеансом, назначения адресов и маршрутов.

Режим туннелирования IPSec (IPSec ТМ) позволяет зашифровывать IP-пакеты и затем инкапсулировать их в IP-заголовок, который будет послан по объединенной IP-сети организации или открытой объединенной IP-сети типа интернета.

Технология IPSec TM не рекомендуется для VPN-подключений удаленного доступа, потому что она не содержит никаких стандартных методов для аутентификации пользователей, назначения IP-адресов и назначения адреса сервера имен. Возможно использовать технологию IPSec TM для межсайтовых VPN-подключений на компьютерах с системой WS2003.

PPTP (Point-to-Point Tunneling Protocol) —является расширением протокола PPP и использует механизмы проверки подлинности, сжатия и шифрования этого протокола. Протокол PPTP и метод шифрования MPPE (Microsoft Point-to-Point Encryption) обеспечивают основные необходимые для виртуальных частных сетей службы инкапсуляции и шифрования частных данных. Кадр PPP зашифровывается по методу MPPE с использованием ключей шифрования, созданных в процессе проверки подлинности по протоколу MS-CHAP, MS-CHAP v2 или EAP-TLS.

Кадр PPP, содержащий IP - датаграмму заключается в оболочку с заголовком GRE (Generic Routing Encapsulation) и заголовком IP. В заголовке IP-адреса источника и приемника соответствуют VPN-клиенту и VPN-серверу.



Рисунок 7. Структура кадра PPP

L2TP (Layer Two Tunneling Protocol) — это туннельный протокол на основе RFC, являющийся промышленным стандартом. L2TP использует средства шифрования, предоставляемые методом IPSec. Комбинацию L2TP и IPSec называют L2TP/IPSec. Комбинация L2TP/IPSec обеспечивает работу служб VPN, выполняющих инкапсуляцию и шифрование частных данных.



Рисунок 8. Структура кадра L2TP

Инкапсуляция пакетов L2TP/IPSec выполняется в два этапа.

1. Инкапсуляция L2TP - кадр PPP (IP-датаграмма или IPX-датаграмма) заключается в оболочку с заголовком L2TP и заголовком UDP.

2. Затем полученное L2TP-сообщение заключается в оболочку с заголовком и трейлером IPSec ESP (Encapsulating Security Payload), трейлером проверки подлинности IPSec, обеспечивающим целостность сообщения и проверку подлинности, и заголовком IP. В заголовке IP-адреса источника и приемника соответствуют VPN-клиенту и VPN-серверу.

Сообщение L2TP шифруется с использованием стандарта DES или 3DES при помощью ключей шифрования, созданных в процессе согласования IKE (Internet Key Exchange).

Преимущества протокола L2TP/lPSec в сравнении с РРТР

1. Метод IPSec ESP дает аутентификацию источника данных каждого пакета, целостность данных, защиту от атак воспроизведения и конфиденциальность данных (шифрование). В противоположность этим свойствам, протокол РРТР обеспечивает только конфиденциальность данных в каждом пакете.
2. Подключения L2TP/IPSec обеспечивают более сильную аутентификацию, требуя как аутентификации на уровне компьютера через сертификаты, так и аутентификации на уровне пользователей через аутентификационный протокол РРР.
3. В протоколе L2TP/IPSec пакеты РРР, обмен которыми происходит в процессе аутентификации на уровне пользователей, никогда не посылаются в незашифрованной форме, потому что процесс РРР-подключения происходит после установления соглашения по безопасности IPSec. В случае перехвата РРР-пакеты опознавательного обмена для некоторых типов аутентификационных РРР-протоколов могут использоваться для автономных словарных атак и определения пользовательских паролей;
4. Связка L2TP\IPSec может работать в двух режимах – с использованием цифровых сертификатов и с использованием предварительных ключей. Сертификаты дают гибкую возможность по организации доступа, однако требуют развертывания службы сертификатов. Применение предварительных ключей делает сертификаты не нужными, однако требует применения для всех клиентов одинакового ключа. Для автоматического обновления требуется применение Диспетчера подключений (Connection Manager).

Преимущества протокола РРТР по сравнению с протоколом L2TP/IPSec

1. Протокол РРТР не требует инфраструктуры сертификатов. Протоколу L2TP/IPSec требуется инфраструктура предварительного установления общих секретов или инфраструктура сертификатов для выдачи компьютерных сертификатов VPN-серверу и всем компьютерам VPN-клиентов. В случае использования предварительных ключей это ограничение снимается.
2. Клиенты РРТР могут находиться за транслятором сетевых адресов (NAT), если транслятор NAT имеет редактор для РРТР-трафика. Клиенты или VPN-серверы, базирующиеся на протоколе L2TP/IPSec, не могут располагаться позади NAT-устройства, если только поддержка VPN в нем не установлена отдельно.

Существует несколько способов защиты конфиденциальности данных, пересылаемых между клиентами и VPN-сервером удаленного доступа:

- проверка подлинности удаленных пользователей;

- шифрование конфиденциальных данных;

- применение политик удаленного доступа.

Чтобы обеспечить доступ к ресурсам частной сети только уполномоченным удаленным пользователям, в проекте следует предусмотреть аутентификацию, или проверку подлинности, удаленных пользователей. В этом случае для входа в систему пользователям необходимо ввести реквизиты: имя пользователя, пароль и имя домена. Проверка реквизитов может выполняется на основе:

- локальных учетных записей, хранимых на VPN-сервере удаленного доступа;

- учетных записей Active Directory, хранимых на контроллерах домена.

В проектируемой сети будем осуществлять аутентификацию и авторизацию пользователей на основе учетных записей Active Directory. Доступ к ресурсам удаленному пользователю будет предоставляться на основании принадлежности его к определенной группе, авторизованной для доступа к данному ресурсу внутренней сети. В целях безопасности реквизиты удаленных шифруются при пересылке между клиентом и сервером удаленного доступа.

В корпорации CorpKAM для организации VPN выбираем связку протоколов L2TP\IPSec c использованием предварительных ключей, так как он позволяет обойтись без организации системы сертификации, что упрощает построение сети, однако снижает безопасность организованного подключения через VPN.

3.9 Обеспечение возможности проведения аудио и видео конференций

Для обеспечения видео и аудио конференций необходимо использовать возможности оборудованию по обеспечению QoS. Применяемые коммутаторы и маршрутизаторы имеют такую возможность, поэтому все, что необходимо сделать – это настроить соответствующим образом QoS на каждом устройстве.

5. ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы был разработан эскизный проект сети корпорации CorpKAM. Была спроектирована физическая структура сети здания каждого из филиалов. При выборе сетевого оборудования отдавалось предпочтение продукции компании 3Com, которую отличает высокая надежность и приемлемое соотношение цена/качество. К тому же, использование сетевого оборудования одного производителя гарантирует совместимость.

В процессе проектирования физической структуры сети зданий учитывались правила построения структурированных кабельных систем.

Также в ходе курсовой работы была спроектирована как логическая, так и физическая структура службы каталогов – Active Directory. Был определен состав доменов, число контроллеров в каждом из них и роли, выполняемые ими. Для корректной репликации данных главного каталога, домены были включены в состав сайтов.

Служба DNS интегрирована в Active Directory. В целях безопасности внутреннюю и внешнюю среды обслуживают разные DNS-серверы. Выбранное количество и размещение внутренних и внешних серверов DNS позволяет быстро обслужить запросы и минимизировать трафик WAN.

В целях безопасности в проекте широко применяются межсетевые экраны. Для организации конфиденциального удаленного доступа к ресурсам сети используется технология VPN на основе протокола туннелирования L2TP\IPSec.