

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ВОЛОГОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА АВТОМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

СЕТИ ЭВМ И ТЕЛЕКОММУНИКАЦИИ

Методические указания к курсовому проекту

Электроэнергетический факультет, ФЗДО

Специальности: 220201 - управление и информатика в технических системах
230101 - вычислительные системы, сети и комплексы

Вологда
2006

УДК 681.374.1

Сети ЭВМ и телекоммуникации. Методические указания к курсовому проекту.
– Вологда: ВоГТУ, 2006- 26с.

Приводится техническое задание на проектирование корпоративной вычислительной сети для различных организаций, а также методические указания по последовательности выполнения шагов проектирования с их подробным описанием.

Утверждено редакционно-издательским советом ВоГТУ

Составитель: А.А.Суконщиков, к.т.н., доцент

Рецензент: А.М. Водовозов зав. кафедрой Управляющие
вычислительные системы доцент, к. т. н.

КУРСОВОЙ ПРОЕКТ.

По дисциплине «Сети ЭВМ и телекоммуникации» студенты выполняют курсовой проект, который состоит в разработке проекта корпоративной сети предприятия. Разработка состоит из нескольких подразделов, которые необходимо выполнить последовательно. Каждый студент выполняет свой вариант, который будет определяться последовательным номером студента в списке группы. Во всех вариантах заданий предусматривается наличие филиалов, один из них в другом городе, другой в этом же, для обоих необходимо обеспечить удаленный доступ к корпоративной сети. Кроме того каждый вариант должен учитывать выход в Интернет, организацию почтового сервера, Веб - сервера, прокси - сервера, серверов баз данных, файл-серверов (PDC,BDC) и серверов для других сетевых приложений.

Варианты заданий по разработке корпоративной сети в следующих организациях. Номер варианта соответствует номеру студента в списке группы (см. таб. 1.1):

Таблица 1.1

NN варианта	Предметная область
1	Информационная система для автоматизации организационно-распорядительного документооборота производственного предприятия.
2	Информационная система для автоматизации документооборота оперативного управления производственного предприятия.
3	Информационная система для автоматизации документооборота подсистемы сбыта производственного предприятия.
4	Информационная система для организационно-распорядительного документооборота учреждения
5	Информационная система для факультета университета
6	Информационная система для кафедры университета
7	Информационная система для торгового предприятия
8	Информационная система для авиапредприятия
9	Информационная система для лечебного учреждения (больницы)
10	Информационная система для лечебного учреждения (поликлиники)
11	Информационная система для банка
12	Информационная система для культурно-спортивного центра

13	Информационная система для издательства с филиалами в других городах
14	Информационная система для автотранспортного предприятия
15	Информационная система для предприятия связи
16	Информационная система для железнодорожного вокзала
17	Информационная система для школы (колледжа, гимназии)
18	Информационная система для выставочного центра
19	Информационная система для центра службы занятости
20	Информационная система для акционерного общества, имеющего филиалы в других городах
21	Информационная система для небольшой финансовой компании
22	Информационная система для небольшой инвестиционной фирмы
23	Информационная система для архитектурной организации
24	Информационная система для машиностроительного предприятия
25	Информационная система для строительного треста
26	Информационная система для гостиницы
27	Информационная система для милиции

Количество зданий и их размер (в метров) в каждом вариантах также определяется последней цифрой шифра в зачетной книжке студента, при этом организация занимает только 4 этажа в представленных ниже зданиях (первый и последний):

1. Два двухэтажных здания - 20х250.
2. Два четырехэтажных здания - 26х200
3. Два семиэтажных здания - 10х150
4. Два девятиэтажных здания - 30х100
5. Три двухэтажных здания - 20х220
6. Три четырехэтажных здания - 24х200
7. Три семиэтажных здания - 20х90
8. Три девятиэтажных здания - 16х70
9. Четыре двухэтажных здания - 20х10
10. Четыре трехэтажных здания - 20х150.

Высота этажа для всех вариантов (а также подвала и чердака) ровно 3 метра. Форма зданий различна. Расстояние между зданиями определяется по последней цифрой шифра в зачетной книжке студента:

- | | | | | |
|-----------|-----------|-----------|-----------|------------|
| 1. 100 м. | 2. 130 м. | 3. 150 м. | 4. 200 м. | 5. 180 м. |
| 2. 80 м. | 7. 170 м. | 8. 300м. | 9. 400м. | 10. 330 м. |

Правила оформления пояснительной записки

Пояснительная записка пишется чернилами на одной стороне листа бумаги формата А4. Общий объем 25 - 30 страниц. С левой стороны листа должны быть поля шириной 20 мм, листы подшиваются в папку вместе с диаграммами, схемами и другими иллюстрациями. Все схемы, формулы, графики должны быть пронумерованы и снабжены подписями и ссылками в тексте. Допускается подготовка пояснительной записки с использованием компьютера. Материалы в пояснительной записке следует располагать в следующем порядке:

- титульный лист;
- задание на проектирование;
- содержание;
- введение;
- схема информационных потоков на предприятии и расчет объема потоков между отделами;
- схема информационных потоков с учетом размещения информационных ресурсов на серверах;
- проектирование структурной схемы вычислительной сети;
- разработать защиту сети от несанкционированного доступа;
- организация связи с филиалами;
- распределение адресов рабочих станций с учетом структурной схемы;
- выбор сетевых протоколов;
- выбор топологии сети , среды передачи, метода доступа, активного и пассивного оборудования корпоративной сети ;
- выбор сетевой операционной системы и клиентской операционной системы, сетевое прикладное обеспечение;
- разработка имитационной программы корпоративной сети и анализ полученных результатов при разных трафиках;
- разработка плана монтажной прокладки соединений сети и расположения сетевого оборудования в зданиях организации и разработка кабельных трасс между зданиями;
- смету разработки проекта сети;
- заключение;
- список используемых источников;

- приложения.

В пояснительной записке должны быть выдержаны единые обозначения и единые размерности для используемых параметров. Допускаются только общепринятые сокращения слов, терминов, обозначений. Законченная пояснительная записка подписывается студентом и руководителем проекта. Изложение должно быть ясным и четким, без повторений, количество иллюстраций - минимальным, но достаточным для пояснения изложенного.

Состав графической части курсового проекта, который приводится в приложении:

- гистограмма информационной нагрузки на предприятии (плакат) – 1 лист;
- логическая структура вычислительной сети (плакат) – 1-2 листа;
- схема структурная вычислительной сети (плакат) – 1-2 листа;
- план размещения оборудования и монтажных соединений сети (чертеж) – в зависимости от количества этажей и зданий;
- схема кабельных трасс (чертеж) – 1 лист;
- состав и структура программного обеспечения сети (стеки протоколов, системное программное обеспечение – клиентская и серверная части) – 1 лист.

Разработка возможных вариантов конфигурации ЛВС

Сетевую архитектуру можно понимать как поддерживающую конструкцию или инфраструктуру, лежащую в основе функционирования сети. Данная инфраструктура состоит из нескольких главных составляющих, в частности компоновка или топология сети, кабельная проводка и соединительные устройства - мосты, маршрутизаторы и коммутаторы. Проектируя сеть, необходимо принимать во внимание каждый из этих сетевых ресурсов и определить, какие конкретно средства следует выбрать и как их надо распределить по сети, чтобы оптимизировать производительность, упростить управление оборудованием и оставить возможности для последующего роста. В курсовом проекте следует создать свою конфигурацию сети в соответствии с конкретным заданием. Рассмотрим, какие вопросы должны быть решены в разделах курсового проекта.

Введение

Во введении необходимо отметить актуальность проектирования и внедрения корпоративной сети (КС) в данной организации. Какие плюсы при внедрении КС возникают на предприятии.

1. Схема информационных потоков на предприятии и расчет объема потоков между отделами.

Схема информационных потоков представляется в виде диаграммы (графа), в которой вершины состояний отражают отделы, а дуги информационные потоки.

В первой главе необходимо провести организационный анализ структуры предприятия (фирмы)- выделить отделы, операции в отделах, необходимая информация для отделов, передача информации между отделами, виды информации, предварительные объемы обмена информации. Выделяем на информационной схеме преимущественные объемы связей между отделами, что может учитываться при выборе и анализе пропускного канала между данными отделами, которые отразим на схеме магистральные потоки информации. Определяем, как идет распределение трафика между отделами в сети. В таблице 1.2 для примера показан средний объём информации за один рабочий день (8 часов) в Мбайт, отправляемый и принимаемый подразделениями фирмы, а также между отделами центра и филиалами. Необходимо заметить, что трафик складывается из собственно рабочей информации плюс 10% служебной информации, также учитываем (условно), что при передаче по сети информации она увеличивается в 1,7 раза за счет помехоустойчивого кодирования.

Таблица 1.2

	Отделы получают информацию													
		1	2	3	4	5	6	7	8	9	10	Филиал1	Филиал2	Σисх. инф.
отделы отсылают информацию	1	20	15	3	15	15	15	8	8	5	30	8	-	122
	2	15	30	30	8	15	15	15	15	8	15	8	8	152
	3	15	15	-	3	8	8	8	8	8	15	8	8	104
	4	15	15	3	20	8	8	8	8	8	8	-	-	81
	5	15	50	-	8	180	50	50	15	-	40	20	8	256
	6	15	15	-	8	15	20	-	-	15	-	8	8	84
	7	15	15	-	8	15	-	40	60	-	-	20	8	141
	8	15	15	-	8	15	-	60	40	30	-	20	8	171

	9	15	15	-	8	-	15	-	30	20	-	8	-	91
	10	15	15	30	8	15	-	-	-	-	40	8	8	99
	Филиал1	8	8	8	-	20	8	20	20	8	8	-	-	108
	Филиал2	-	8	8	-	8	8	8	8	-	8	-	-	56
	Σвход. инф.	143	186	82	74	134	127	177	172	82	124	108	56	

Предпроектное обследование предприятия. В этом разделе необходимо привести результаты исследования внутренних и внешних информационных потоков предприятия, которые должны обрабатывать проектируемые сети (обычно в виде гистограммы максимально суммарной почасовой информационной нагрузки в течение рабочего цикла (дня) предприятия). Гистограмма должна быть оформлена в виде плаката.

По структурно-организационной схеме предприятия, рис 1.1,а, для каждого рабочего часа определяется информационная нагрузка каждой информационной связи каждого структурного подразделения (отдела) предприятия.

Информационная нагрузка одной информационной связи определяется по результатам анализа документооборота в обоих направлениях между данным подразделением и каждым подразделением, непосредственно с ним связанным. Исходным носителям информации считается стандартный лист формата А4, содержащий 2000 алфавитно-цифровых знаков и пробелов. При 8-битном кодировании информационная емкость такого листа составляет $E=200*8=16000$ бит.

Информационная часовая нагрузка одной организационной связи равна:

$$IH_{cs} = \frac{E * (n_1 + n_2)}{3600} \frac{бит}{сек} \quad (1.1)$$

где E – информационная емкость стандартного листа документа;

n1 – число листов, поступающих в данное подразделение за час;

n2 – число листов, отправляемых данными подразделениями в час.

Информационная часовая нагрузка организационных связей определяется по формуле 1.1 для всех подразделений предприятия. При этом не учитываются информационные связи с теми подразделениями, для которых расчет уже производился.

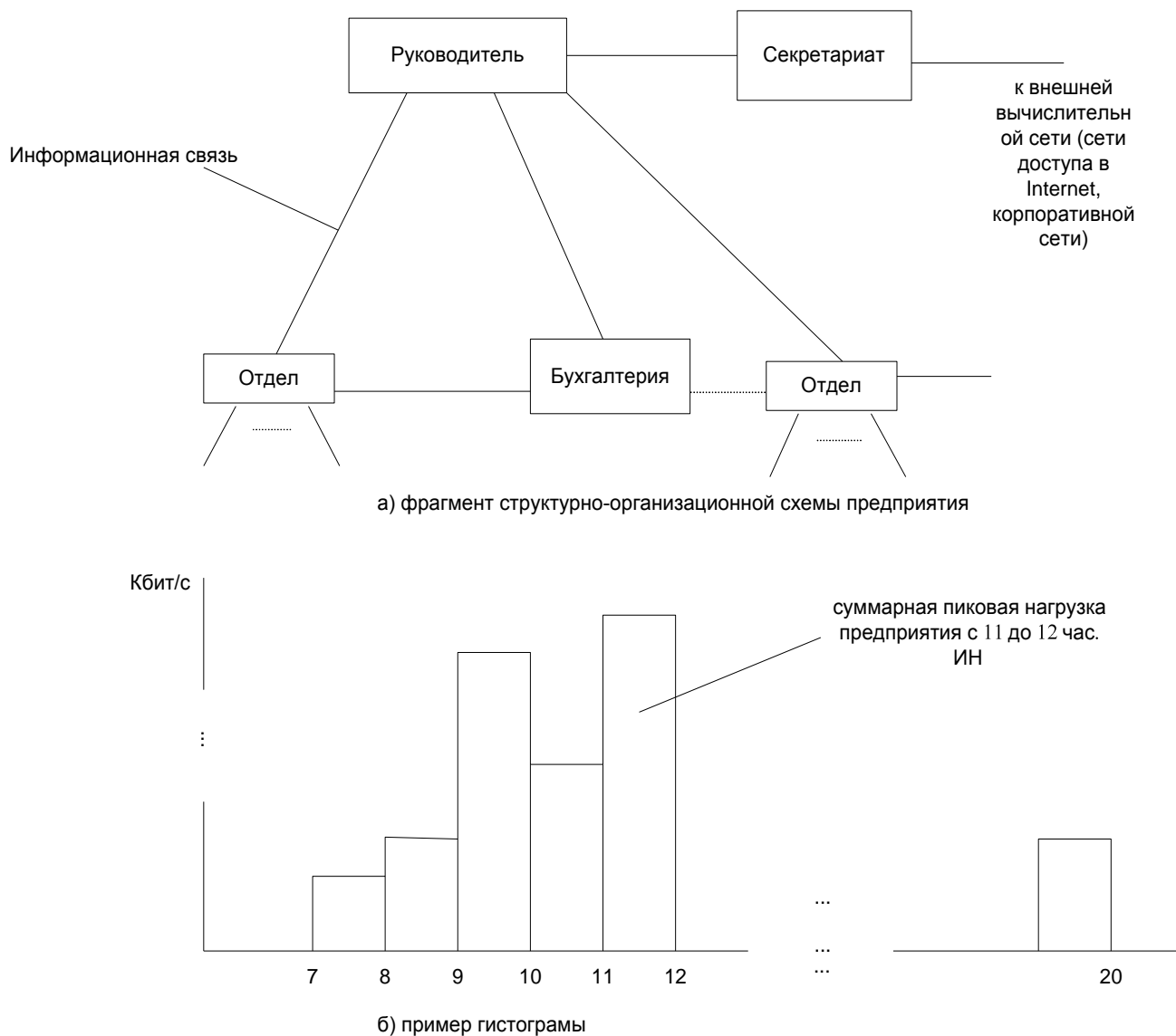


Рис 4.1. К построению гистограммы информационной нагрузки.

Суммарная часовая информационная нагрузка всех организационных связей предприятия равна:

$$ИН_{\Sigma} = ИН_{св} * N \frac{бит}{сек} \quad (1.2)$$

где N – число организационных связей в схеме предприятия.

На гистограмме, рис 4.1.б для каждого рабочего часа показывается значение $ИН_{\Sigma}$, и выбирается максимальное значение $ИН_{\Sigma}$, макс для рабочего дня (цикла) предприятия, которое является исходным для определения потребной полезной пропускной способности базовой технологии проектируемой сети.

Общая пропускная способность C_p сети определяется по формуле:

$$C_p = k_1 * k_2 * ИН_{\Sigma, макс} \quad (1.3)$$

где $k_1=(1,1\div 1,5)$ – коэффициент учета протокольной избыточности стека протоколов, измеренного в практикуемой сети; для стека TCP/IP $k_1\approx 1,3$;

k_2 – коэффициент запаса производительности для будущего расширения сети, обычно $k_2\approx 2$.

Логическое проектирование ВС. Определяется логическая структура ВС (для ЛВС – на основе расчётов коэффициента загрузки, для КВС – на основе анализа внешних информационных потоков); выполняется логическое структурирование ЛВС и окончательно выбираются сетевые технологии; разрабатывается логическая схема ВС.

Необходимые расчеты для ЛВС выполняются в следующей последовательности:

Определение коэффициента нагрузки неструктурированной локальной вычислительной сети:

$$\rho_n = \frac{C_p}{C_{\max}}; \quad (1.4)$$

где C_{\max} – максимальная пропускная способность базовой технологии сети.

Проверка выполнения условия допустимой нагрузки ЛВС (домена коллизий):

$$\rho_{n \text{ (д.к.)}} \leq \rho_{\text{доп}} = 0,35 \quad (1.5)$$

где $\rho_{n \text{ (д.к.)}}$ – коэффициент нагрузки неструктурированной сети или домена коллизий – логического сегмента ЛВС.

Примечание: Если условия (1.5) не выполняются необходимо выполнить логическую структуризацию ЛВС:

последовательно разделять сеть на логические сегменты (домены коллизий) по Нл.с. компьютеров в каждом логическом сегменте, проверяя на каждой итерации выполнение условия (1.5):

$$\rho_{\text{д.к.}} = \frac{N_{\text{л.с.}} \cdot C_i}{C_{\max}} \leq \rho_{\text{Ethernet}} = 0,35$$

Определение межгруппового трафика и трафика к серверу:

$$C_{\text{меж.гр}}^n = C_{\text{серв}} = 0,5 \cdot C_{\Sigma}^n$$

Определение коэффициента нагрузки по межгрупповому трафику и трафику к серверу:

$$\rho_{\text{меж.гр.серв}} = \frac{C_{\text{меж.гр}}^n}{C_{\max}} \leq \rho_{\text{Internet}} = 0,35 \quad (1.6)$$

Если условие (1.6) не выполняется, принять значение Смакс для межгруппового обмена в сети равным следующей по производительности разновидности базовой технологии. Например, для Ethernet, Fast Ethernet, Gigabit Ethernet, до тех пор, пока условие (1.6) не будет выполнено.

2. Схема информационных потоков с учетом серверов.

Один из основных принципов технологии «клиент - сервер» заключается в разделении функций стандартного диалогового приложения на четыре группы, имеющие различную природу.

1 группа. Это функции ввода и отображения данных.

2 группа. Объединяет чисто прикладные функции, характерные для данной предметной области (например, для инвестиционной системы – открытие счета, перевод денег, и т.д.)

3 группа. Фундаментальные функции хранения и управления информационно - вычислительными ресурсами (базами данных, файловыми системами и т.д.)

4 группа. Служебные функции, осуществляющие связь между функциями первых трех групп.

В соответствии с этим в любом приложении выделяются следующие логические компоненты:

- компоненты представления, реализующий функции первой группы;
- прикладной компонент, поддерживающий функции второй группы;
- компонент доступа к информационным ресурсам, поддерживающий функции третьей группы, а также вводятся и уточняются соглашения о способах их взаимодействия (протокол взаимодействия).

Выделяют четыре подхода, реализованные в следующих технологиях:

- файловый сервер;
- доступ к удаленным данным;
- сервер баз данных;
- сервер приложений;

Файловый сервер (FS). Этот подход является базовым для локальных сетей ПК. Один из компьютеров в сети назначается файловым сервером и предоставляет другим компьютерам услуги по обработке файлов. Файловый сервер работает под управлением сетевой операционной системы и играет роль компонента доступа к информационным ресурсам (т.е. к файлам). На

других ПК в сети функционирует приложение, в кодах которого совмещены компонент представления и прикладной компонент. Протокол обмена при такой схеме представляет собой набор вызовов, обеспечивающих приложению доступ к файловой системе на файл-сервере.

Сервер баз данных (DBS) – технология, реализуемая в реляционных СУБД. Ее основу составляет механизм хранимых процедур – средство программирования SQL – сервера. Процедуры хранятся в словаре баз данных, разделяются между несколькими клиентами и выполняются на том же компьютере, где функционирует SQL-сервер. В сервере баз данных компонент представления выполняется на компьютере – клиенте, в то время как прикладной компонент оформлен как набор хранимых процедур и функционирует на компьютере-сервере БД. Там же выполняется компонент доступа к данным, т.е. ядро СУБД.

На практике используются смешанные модели, когда целостность базы данных и некоторые простейшие прикладные функции обеспечиваются хранимыми процедурами (DBS – технология), а более сложные функции реализуются непосредственно в прикладной программе, которая выполняется на компьютере – клиенте (RDA – технология).

Сервер приложений (AS) представляет собой процесс, выполняемый на компьютере – клиенте, отвечающий за интерфейс с пользователем (т.е. реализует функции первой группы).[5]

Прикладной компонент реализован как группа процессов, выполняющих прикладные функции, и называется сервером приложения.

Доступ к информационным ресурсам осуществляет менеджер ресурсов (например, SQL-сервер). Из прикладных компонентов доступны такие ресурсы, как базы данных, очереди, почтовые службы и др. AS, размещенная на компьютере, где функционирует менеджер ресурсов, избавляет от необходимости направления SQL-запросов по сети, что повышает производительность системы.

Технологии RDA и DBS опираются на двухзвенную схему разделения функций:

- в RDA прикладные функции отданы программе – клиенту (прикладной компонент комбинируется с компонентом представления);
- в DBS ответственность за их выполнение берет на себя ядро СУБД (прикладной компонент интегрируется в компонент доступа к информационным ресурсам).

В AS реализована трехзвенная схема разделения функций. Здесь прикладной компонент выделен как важнейший изолированный элемент приложения. Сравнивая модели, можно заметить, что AS обладает наибольшей гибкостью и имеет универсальный характер.[5]

Определим, какие сервера нужны для полноценного функционирования сети. Построим схему информационных потоков с учетом серверов.

Во-первых, необходим файл-сервер для обработки потоков информации между отделами, для организации внутреннего документооборота.

Во-вторых, для организации доступа в Internet необходим проxy-сервер.

Proxy – Server – это сервер, который выступает в качестве «представителя» настоящего сервера в сети. Все запросы к настоящему серверу в действительности поступают сначала на Proxy – Server, который таким образом получает возможность отвергнуть нежелательные запросы, предотвращая непосредственный доступ на сервер и к его данным. Proxy – Serverы организуют собственный кэш для хранения данных. При выполнении первоначального запроса на данные сервера, передаваемые через Proxy – Server, данные сохраняются в кэше Proxy – Serverа. Повторные запросы могут использовать данные, хранящиеся в кэше, что сокращает объем передачи данных с основного сервера.[5]

В-третьих, для возможности пользования электронной почтой необходим почтовый сервер, для хранения Web-страниц - Web-сервер.

В-четвёртых, для печати любых документов необходим доступ сотрудников к принтеру. В каждом подразделении будет хотя бы один сетевой принтер подключенный через Print-Server.

В-пятых, начальники подразделений и некоторые сотрудники для обмена служебными документами в системе документооборота, подключены к внутренней электронной почте (через Exchange-Server).

Exchange Server – поддерживает службы обмена сообщениями и различные приложения для интеграции рабочих групп, существующих в локальной сети. Кроме обеспечения работы электронной почты, это положение может быть использовано для организации общедоступных каталогов Web, для организации общих дискуссий с использованием Outlook в качестве конечного интерфейса.

Объем почтовых сообщений в большинстве случаев незначителен, поэтому загруженность сервера складывается из интенсивности обмена почтовой информацией между внешними и локальными пользователями.

В-шестых, сотрудники всех отделов должны иметь доступ к внутреннему серверу баз данных, содержащему рабочую информацию, применяемую внутри фирмы (это СУБД 2), а для удобства работы «медленных» клиентов (филиала например) с данной БД – сервер приложений.

В-седьмых, так же необходим сервер баз данных с информацией о клиентах и сотрудниках предприятия (это СУБД 1).

Кроме всех вышеперечисленных, для защиты сети и ее нормальной работы необходимы следующие сервера: межсетевой экран, антивирусный сервер, главный и резервный контроллеры домена и т.д. О них пойдет речь далее – при выборе программного обеспечения сети.

Таким образом, в состав сети необходимо включить следующие сервера:

1. Сервер Базы Данных 1 (СУБД 1) база, содержащая оперативную текущую информацию;
2. Сервер Базы Данных 2 (СУБД 2) архив и информационная база;
3. Файловый сервер документов и информации (FILE-Server);
4. Print – сервер;
5. Проxy – сервер;
6. Почтовый (E-Mail) сервер;
7. WEB – сервер;
8. Сервер приложений для работы медленных клиентов с СУБД 2;
9. Сервер внутренней почты Microsoft Exchange. внутри сети.

Схема информационных потоков с учетом серверов показана на рисунке 2.1.

Отделы обозначены на схеме соответствующими цифрами.

Для нормального функционирования сети также необходимы еще 2 сервера: PDC- (Primary Domen Controller) и BDC-сервера (BackUp Domen Controller) - для сохранения всех учетных записей это службы ОС. Установим PDC на проxy-сервер, а BDC – на файл-сервер. В состав каждого контроллера домена входят службы DNS и DHSP. DHSP предназначена для динамического распределения IP-адресов машин. DNS содержит таблицы соответствия имен компьютеров в сети их IP- адресам. DNS-внешний (на проxy-сервере) необходим для внешнего доступа к сети. DNS-внутренний (на файл-сервере) предназначен для работы внутренних пользователей. Некоторые из этих серверов можно совместить: Print-сервер и сервер баз данных 1; антивирусный сервер и сервер баз данных 2 ; почтовый, WEB-сервер, проxy-сервер и сервер приложений. Сервера БД выбираются исходя из задач и программного обеспечения, с помощью которого пользователи будут решать эти задачи.

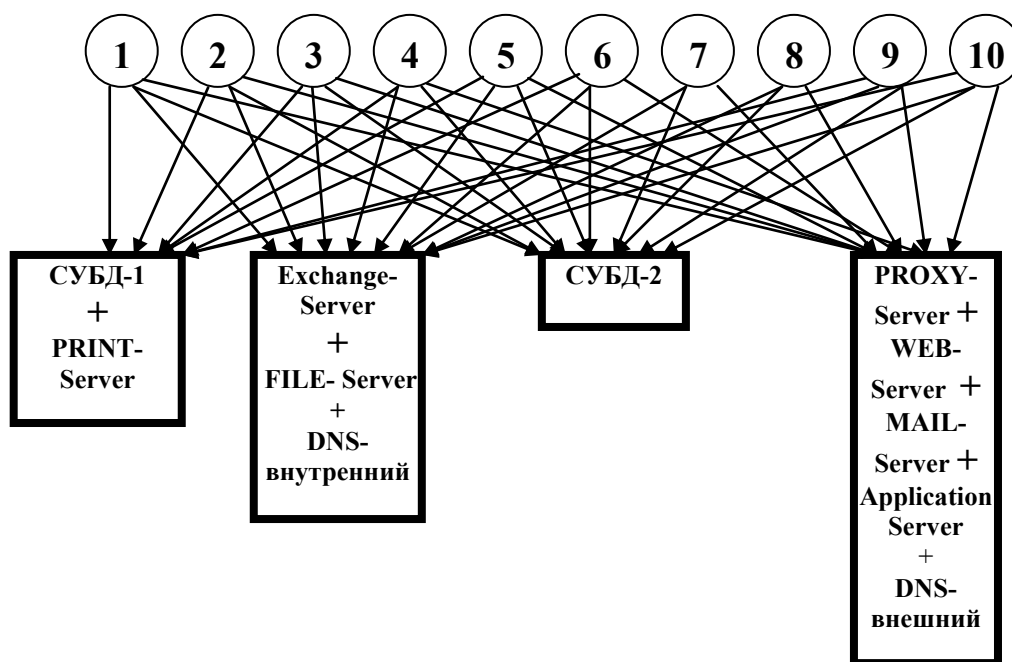


Рис. 2.1.

3. Проектирование структурной схемы корпоративной сети.

Исходя из схемы информационных потоков, разделения этих потоков, и схемы информационной потоков с учетом серверов, также зная расположение зданий и их габариты составим структурную схему корпоративной сети (В ПРИЛОЖЕНИИ) и приводим ее краткое описание.

4. Разработка защиту сети от несанкционированного доступа.

Подключение компьютеров к сети позволяет организовать общий доступ к файлам и принтерам на других компьютерах, подключение к базам данных, а также обмен электронной почтой.

Политика сетевой безопасности каждой организации должна включать две составляющие:

- Политика доступа к сетевым сервисам.
- Политика реализации межсетевых экранов.

Политика доступа к сетевым сервисам должна быть уточнением общей политики организации в отношении защиты информационных ресурсов в

организации. Для того чтобы межсетевой экран успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Таковой считается политика, при которой найден гармоничный баланс между защитой сети организации от известных рисков и необходимостью доступа пользователей к сетевым сервисам. В соответствии с принятой политикой доступа к сетевым сервисам определяется список сервисов Интернета, к которым пользователи должны иметь ограниченный доступ. Задаются также ограничения на методы доступа, необходимые для того, чтобы пользователи не могли обращаться к запрещенным сервисам Интернета обходными путями.[4]

Для обеспечения безопасной работы и защиты от несанкционированного доступа необходимо иметь:

1. Политику пользователей для защиты на внутреннем уровне.
2. Использование межсетевого экрана для защиты локальной сети от внешних несанкционированных воздействий.

Контроль прав доступа производится разными компонентами программной среды - ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением (таким как монитор транзакций) и т.д.

Основные требования по безопасности данных, предъявляемые к БД и СУБД, во многом совпадают с требованиями, предъявляемыми к безопасности данных в компьютерных системах – контроль доступа, криптозащита, проверка целостности, протоколирование и т.д. Большинство современных СУБД имеют встроенные средства, позволяющие администратору системы определять права пользователей по доступу к различным частям БД, вплоть до конкретного элемента.[4]

Для организации защиты на внутреннем уровне необходимо определить какие группы пользователей, к каким ресурсам имеют тот или иной вид доступа (результаты свести в таблицу).

Тоже самое необходимо проделать и при настройке межсетевого экрана для внешних пользователей (т.е. построить матричную модель защиты защиты).

Таким образом, для нашей локальной сети, необходимо на административном уровне разработать политику доступа и разграничения доступа к информационным ресурсам данной сети.

5. Организация связи с филиалами.

В этом разделе необходимо описать выданный преподавателем тип связи с филиалами по следующим разделам: теоретическое описание выданного метода, аппаратура, которая позволяет организовать данную связь на приемной и передающей стороне.

6. Распределение адресов рабочих станций с учетом структурной схемы.

В данном разделе необходимо разделить сеть на несколько подсетей исходя из структурной схемы сети. Определить IP – адреса для подсетей (для серверов и ПК), маску и широковещательные адреса. Для распределения адресов использовать внеклассовую модель.

7. Выбор сетевых протоколов.

Выбрать сетевые протоколы, которые будут использоваться в разработанной сети и каких функции на основе данных протоколов будут выполняться.

8. Выбор топологии сети, среды передачи, метода доступа, активного и пассивного оборудования корпоративной сети.

8.1. Виды используемых кабелей.

В качестве средств коммуникации наиболее часто используются витая пара, радиоканал и оптоволоконные линии. При выборе типа кабеля учитывают следующие показатели:

1. Стоимость монтажа и обслуживания;
2. Скорость передачи информации;
3. Ограничения на величину расстояния передачи информации (без дополнительных усилителей–повторителей (репитеров));
4. Безопасность передачи данных.

Главная проблема заключается в одновременном обеспечении этих показателей, например, наивысшая скорость передачи данных ограничена максимально возможным расстоянием передачи данных, при котором еще обеспечивается требуемый уровень защиты данных. Легкая наращиваемость и простота расширения кабельной системы влияют на ее стоимость и безопасность передачи данных.

8.2. Выбор типов кабелей для сети.

Чтобы выбрать тип кабеля, а значит и тип сетевой технологии и, соответственно, оборудование, нужно знать какая нагрузка будет на этот канал связи. Протяженность этого канала и условия окружающей среды, в которой этот канал будет находиться.

Рассчитаем нагрузку на каналы связи. Для этого необходимы данные из таблиц в первой главе, а также структурная схема сети.

8.3. Выбор коммутаторов.

Коммутаторы (Switch) – это:

1. Многопортовое устройство, обеспечивающее высокоскоростную коммутацию пакетов между портами.
2. В сети с коммутацией пакетов - устройство, направляющее пакеты, обычно на один из узлов магистральной сети. Такое устройство называется также коммутатором данных.

Коммутатор предоставляет каждому устройству (серверу, ПК или концентратору), подключенному к одному из его портов, всю полосу пропускания сети. Это повышает производительность и уменьшает время отклика сети за счет сокращения числа пользователей на сегмент. Как и двухскоростные концентраторы, новейшие коммутаторы часто конструируются для поддержки 10 или 100 Мбит/с, в зависимости от максимальной скорости подключаемого устройства. Если они оснащаются средствами автоматического опознавания скорости передачи, то могут сами настраиваться на оптимальную скорость - изменять конфигурацию вручную не требуется. Как работает коммутатор? В отличие от концентраторов, осуществляющих широковещательную рассылку всех пакетов, принимаемых по любому из портов, коммутаторы передают пакеты только целевому устройству (адресату), так как знают MAC-адрес (Media Access Control) каждого подключенного устройства (аналогично тому, как почтальон по почтовому адресу определяет, куда нужно доставить письмо). В результате уменьшается трафик и повышается общая пропускная способность, а эти два фактора являются критическими с учетом растущих требований к полосе пропускания сети современных сложных бизнес приложений.

Коммутация завоевывает популярность, как простой, недорогой метод повышения доступной полосы пропускания сети. Современные коммутаторы нередко поддерживают такие средства, как назначение приоритетов трафика

(что особенно важно при передаче в сети речи или видео), функции управления сетью и управление многоадресной рассылкой.

Для выбора коммутаторов предварительно необходимо вычислить минимальное количество портов у каждого из них. На каждом коммутаторе необходимо предусмотреть запасные порты, чтобы в случае отказа одного из используемых, можно было в кратчайшие сроки устранить неполадку и задействовать один из резервных портов. Такой подход имеет смысл для портов под УТР-кабель. Для оптических портов это неактуально, так как они отказывают крайне редко.

Количество портов рассчитывается по следующей формуле:

$$N = 1.5 * N_k + 1,$$

где: N – требуемое количество портов; N_k – количество занятых портов.

И округляется в большую сторону в зависимости от стандартных количеств портов на коммутаторах.

Далее можно перейти к выбору конкретных моделей коммутаторов. Будем брать по возможности коммутаторы и сетевые карты одной фирмы-производителя. Это позволит избежать конфликтов, а также упростить настройку сети.

8.4. Выбор сетевых адаптеров.

Сетевые интерфейсные платы (NIC, Network Interface Card) устанавливаются на настольных и портативных ПК. Они служат для взаимодействия с другими устройствами в локальной сети. Существует целый спектр сетевых плат для различных ПК, имеющих определенные требования к производительности. Характеризуются по скорости передачи данных и способах подключения к сети.

Если рассматривать просто способ приема и передачи данных на подключенных к сети ПК, то современные сетевые платы (сетевые адаптеры) играют активную роль в повышении производительности, назначении приоритетов для ответственного трафика (передаваемой/принимаемой информации) и мониторинге трафика в сети. Кроме того, они поддерживают такие функции, как удаленная активизация с центральной рабочей станции или удаленное изменение конфигурации, что значительно экономит время и силы администраторов постоянно растущих сетей.

8.4. Выбор конфигурации серверов и рабочих станций.

Главным требованием к серверам является надежность. Для повышения надежности будем выбирать машины с RAID контроллером. Он может работать в двух режимах: «зеркала» и в «быстром режиме». Нас будет интересовать первый режим. При этом режиме данные записываемые на жесткий диск одновременно записываются и на другой второй аналогичный жесткий диск (дублируются). Так же для серверов необходимо большее количество оперативной памяти (сколько памяти требуется выяснить не возможно, так как нам неизвестны реальные размеры баз данных и объемы хранимой на жестких дисках информации). Также на сервере совершается обработка запросов(серверы баз данных) пользователя, следовательно нужно выбирать марку и частоту процессора лучше (больше), чем на рабочих станциях.

9. Выбор сетевой операционной системы и клиентской операционной системы, сетевое прикладное обеспечение.

В данном разделе показать по каким критериям было выбрано то или иное программное обеспечение, привести краткое описание выбранного программного обеспечения.

10. Разработка имитационной программы корпоративной сети и анализ полученных результатов при разных трафиках.

Существует довольно значительное количество программ, автоматизирующих процессы разработки и исследования аналитических моделей вычислительных систем и сетей. Рассмотрим одну из них, достаточно простую и удобную в использовании - GPSS/PC. GPSS/PC предназначена для имитационного моделирования производственных систем. В системе GPSS/PC языком моделирования является GPSS. Поскольку целью построения любой модели является исследование моделируемой системы, интерпретатор GPSS/PC автоматически собирает стандартную статистику по каждому типу объектов, занятых в модели.

Для моделирования возьмем упрощенную структурную схему сети. Моделирование производим исходя из нагрузки на конечные коммутаторы 2 машины на один коммутатор ,то есть каждый отдел заменяется двумя ПК. Для того чтобы промоделировать сеть, необходимо знать, какие задержки возникают в ее устройствах. Задержки можно рассчитать по формулам.

Для расчета задержек в канале:

$V(\text{объем пакета})/V(\text{скорость передачи})$

Для оптоволокна получим: $512\text{байт} * 8 / 1 \text{ Гбит} = 0,000004$;

Для витой пары: $512\text{байт} * 8 / 100 \text{ Мбит} = 4 * 10^{-5} = 0,00004$;

Для расчета задержек в коммутаторе:

$V(\text{объем пакета}) / V(\text{скор. Передачи}) * N$ (количество портов).

Вычислим задержку:

Для 16-ти портового: $512 * 8 / 100000000 * 16 = 0,00000256$;

Для 24-х портового: $512 * 8 / 100000000 * 24 = 0,000001706$.

Расчет задержек на серверах:

Задержка при обращении к НЖМД + задержка при обработке процессором;

$(512 * 8 / 10000000 * 8) + (512 * 8 / 2,4 \text{ ГГц} * 32) = 0,00005$.

Для рабочих станций (у них частота процессора 1800 МГц) задержка будет примерно в 2 раза выше, чем на серверах: примерно 0,0001.

Кроме того учитывая объемы передаваемой информации необходимо рассчитать время генерации пакетов для станций (Generate) для трех случаев: минимальной нагрузки, средней и максимальной и провести моделирование для всех трех случаев. Учесть также и обмен данными не только между ПК и серверами, но и между самими серверами.

В приложении представить программу моделирования и три результата моделирования. По результатам моделирования сделать вывод.

11.Разработка плана монтажной прокладки соединений сети и расположения сетевого оборудования в зданиях организации и разработка кабельных трасс между зданиями.

Важную роль играет длина здания, в котором компьютеры располагаются в разных концах здания. Fast Ethernet использует экранированный кабель из скрученных пар проводников (STP), как указано в спецификации IEEE 802.3u для 100BASE-T. Стандарт рекомендует использовать кабель категории 6 с четырьмя парами проводников, помещенных в пластиковую оболочку. Кабели категории 6 сертифицированы для полосы пропускания 100 МГц. В 100BASE-TX одна пара используется для передачи данных, вторая - для обнаружения коллизий и приема.

Установка разъемов. Для минимизации переходных помех не допускать раскручивания пар при установке разъемов RJ-45 более 1.5 см.

Прокладка витой пары производится по коробам, которые расположены на стенах на высоте более 2 метров.. Так как оптоволокну придется протягивать между зданиями, используем самонесущий оптоволоконный кабель (возможно использование троса или прокладка в телефонной канализации). Так же необходимо учесть провис кабеля, плавность закруглений – до 5% от общей длины кабеля. Привести схемы монтажных соединений и кабельных трасс в приложении.

12. Смета разработки проекта.

В данном разделе должны быть приведены все оборудование (пассивное и активное) и программное обеспечение, которое было выбрано в ходе проектирования.

Заключение

В ходе выполнения курсового проекта была разработана корпоративная сеть для представленной организации. Были определены информационные потоки между отделами: это рабочая информация баз данных, электронная почта и прочий трафик Internet. Далее с учетом информационных потоков выбраны сервера и построена схема информационных потоков с учетом серверов. Определена топология сети - «звезда-шина». Сетевая технология – Fast Ethernet +Gigabit Ethernet; выбрано активное и пассивное сетевое оборудование, сетевая и клиентские операционные системы и сетевое прикладное обеспечение, разработана защита сети от несанкционированного внутреннего и внешнего доступа. Составлен план монтажной прокладки соединений сети и расположения сетевого оборудования. В завершение проекта составлена смета разработки проекта сети. Произведено моделирование сети на языке имитационного моделирования GPSS.

Литература

1. Головин, Ю.А. Информационные сети и телекоммуникации: учебное пособие. Часть 1 / Ю.А. Головин, А.А. Суконщиков. – Вологда: ВоГТУ, 2001.- 144 с.

2. Олифер, В.Г. Компьютерные сети: принципы, технологии, протоколы /В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 1999. – 672 с.
3. Кульгин, М. Технологии корпоративных сетей: энциклопедия /М.Кульгин. – СПб.: Питер, 1999. – 704 с.
4. Новиков, Ю.В. Аппаратура локальных сетей: функции, выбор, разработка / Ю.В.Новиков, Д.Г. Карпенко. – М.: Эком, 1998. – 288 с.
5. Максимов, Н.В. Компьютерные сети /Н.В. Максимов, И.И. Попов. – М.: Форум; Инфра -М, 2005. – 335 с.
6. Спортак, М. Компьютерные сети: энциклопедия пользователя. Книга 2: Networking.Essentials : пер. с англ. / М. Спортак. – Киев: Диасофт, 1999. – 432 с.
- 7.Найк, Д. Стандарты и протоколы Интернета: пер. с англ. / Д.Найк. – М.: Microsoft Press;Русская редакция, 1999. – 384 с.
- 8.Лагутенко, О.И. Модемы: справочник пользователя / О.И. Лагутенко. – СПб.: Лань, 1997. – 368 с.
- 9.Олифер, В.Г. Новые технологии и оборудование IP – сетей / В.Г.Олифер, Н.А.Олифер. – СПб.: Питер, 2000. – 372 с.
- 10.Шатт, С. Мир компьютерных сетей: пер. с англ. / С. Шатт. – Киев: ВНУ, 1996. – 288 с.
11. Щербо, В.К. Стандарты вычислительных сетей. Взаимосвязи сетей: справочник / В.К. Щербо. – М.:КУДИЦ –ОБРАЗ, 2000. – 272 с.
12. Спортак, М. Компьютерные сети: энциклопедия пользователя. Книга 1: High Performance Networking : Пер. с англ. / М. Спортак. – Киев: Диасофт, 1998. – 432 с.
13. Гук, М. Аппаратные средства локальных сетей / М.Гук. - СПб.: ПИТЕР, 2002. - 435 с.