

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН  
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ**

К защите  
зав. кафедрой

\_\_\_\_\_

«\_\_» \_\_\_\_\_ 2015 г.

**Выпускная  
квалификационная работа бакалавра**

на тему: «Разработка терминальной серверной сети на базе тонких клиентов»

Выпускник \_\_\_\_\_ Юн Д.С.

Руководитель \_\_\_\_\_ Кабильджанов А.С.

Рецензент \_\_\_\_\_ Умеров Х.У.

Консультант  
по БЖД \_\_\_\_\_ Борисова Е.А.

Ташкент 2015

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН  
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ**

**Факультет компьютерный инжиниринг  
Кафедра: Компьютерные системы  
Направление (специальность): 5610600 – Техника и технология оказания  
сервисных услуг**

**У Т В Е Р Ж Д А Ю**

Зав кафедрой \_\_\_\_\_

« \_\_\_\_\_ » \_\_\_\_\_ 2015 г.

**ЗАДАНИЕ**

на выпускную квалификационную работу Юн Д.С.

«Разработка терминальной серверной сети на базе тонких клиентов»

Утверждена приказом по университету 17 января 2015 г. № 159-15

Срок сдачи законченной работы 30 мая 2015 г.

Исходные данные к работе: данные стационарных клиентов, коммутаторов, сервера и веб интерфейса.

Содержание расчетно-пояснительной записки

Введение

1. Системный обзор терминального режима клиент – серверных сетей
2. Аппаратная реализация клиент – серверной сети.
3. Программная реализация клиент – серверной сети.
4. Расчет необходимого трафика сети и пропускной способности
4. Заключение
5. Презентация

Руководитель:

Кабильджанов А.С.

Задание принял:

Юн Д.С.

## Консультанты по отдельным разделам выпускной работы

### График выполнения работы

№	Наименование раздела работы	Срок	Выполнение
1	Введение	10.02.15	
2	Современное состояние клиент – серверных сетей	17.02.15	
3	Проектирование аппаратного обеспечения клиент – серверных сетей	20.02.15	
4	Практическая реализация терминального режима клиент – серверной сети	20.03.15	
6.	Расчеты трафика сети и пропускной способности	20.04.15	
6	Безопасность жизнедеятельности	10.05.15	
7	Заключение	20.05.15	
8	Презентация ВКР	25.05.15	

Выпускник: Юн Д.С.

\_\_\_\_\_ " \_\_\_\_ " \_\_\_\_\_ 2015 г.

Руководитель Кабильджанов А.С.

\_\_\_\_\_ " \_\_\_\_ " \_\_\_\_\_ 2015 г.

# СОДЕРЖАНИЕ

## Введение

<b>Глава I.</b>	<b>Современное состояние клиент – серверных сетей</b>
1.1.	Тонкие клиенты, работающие в терминальном режиме
1.2.	Терминальный режим работы сервера
1.3.	Методы и среды передачи данных
	Выводы по главе I
<b>Глава II.</b>	<b>Проектирование терминального режима клиент – серверных сетей.</b>
2.1.	Аппаратное обеспечение клиент – серверных сетей
2.2.	Выбор среды передачи данных
2.3.	Программное обеспечение клиент – серверных сетей
2.3.	Пропускная способность клиент – серверной сети
	Выводы по главе II .....
<b>Глава III.</b>	<b>Практическая реализация терминального режима клиент – серверных сетей.</b>
3.1.	Реализация терминальной технологии
3.2.	Реализация программного обеспечения
3.3.	Организация внешнего доступа клиент – серверной сети
3.4.	Обеспечение безопасности при работе в Internet
	Выводы по главе III .....
<b>Глава IV.</b>	<b>Безопасность жизнедеятельности.....</b>
4.1.	
4.2.	
	Выводы по главе IV.....
	<b>Заключение.....</b>
	<b>Список литературы.....</b>

## Введение

Для повышения эффективности реализации современных информационных и телекоммуникационных технологий согласно постановлению Президента Республики Узбекистан уделяется большое внимание практическому внедрению терминальному режиму работы сети, что позволит обеспечить тесное информационное взаимодействие между локальными сетями, превратив их в единую систему [1, 2].

Основная задача компьютерных сетей состоит в том, чтобы совместно использовать ресурсы (данные, приложения, периферийные устройства) и осуществлять интерактивную связь как внутри, какой либо фирмы, так и за её пределами.

Функции сети: распределение данных, распределение информационных и технических ресурсов, распределение программ, обмен сообщениями по электронной почте.

Основное отличие ЛВС от глобальных систем заключается в том, что для всех абонентов имеется единый высокоскоростной канал передачи данных, к которому ЭВМ и другое периферийное оборудование подключаются через специальные блоки сопряжения.

Преимущества сети:

- быстрый обмен информацией между пользователями;
- общий для пользователей доступ к ресурсам;
- оптимальное распределение нагрузки между несколькими ПК;
- возможность резервирования данных, повышение устойчивости системы к отказам;
- создание гибкой рабочей среды.

Использование локальных сетей позволяет облегчить доступ к устройствам оконечного оборудования данных установленных в учреждении.

**Цель данной работы** проектирование клиент-серверной сети на примере среднего офиса, расчет параметров этой сети и определение ее соответствия стандартам.

В данной работе будут освещены следующие стороны проблемы:

- анализ современного состояния локальных сетей в офисах;
- определение структуры сети, ее топологии, основных направлений трафика;
- определение технических характеристик используемого сетевого оборудования;
- определение требований к ПО по допускаемому размеру сети, скорости, гибкости и разграничению прав доступа, контролю за обменом информацией;
- определение необходимости и методов подключения к внешним сетям (интернет).

Планирование сети корпорации, состоящей из центрального сервера, и локальных серверов класса SOHO.

Центральный сервер располагается в одном многоэтажном здании, филиал же занимает 2 корпуса. Пользователи и серверы рабочих групп равномерно распределены по этажам. Количество рабочих мест во всех рабочих группах приблизительно одинаковое. Планировка этажей во всех зданиях также одинаковая.

Требования к сети центрального сервера:

- Простота администрирования для пользователей.
- Обеспечение между рабочими группами трафика типа voice over IP
- peer-to-peer.
- Доступ в Интернет через промежуточную сеть PSTN.

Требования к сети филиала:

- Обеспечение большого внешнего трафика к ресурсам центрального офиса при относительно низком уровне внутреннего трафика.
- Обеспечение между рабочими группами низко интенсивного трафика

типа small office peer-to-peer.

- Доступ в Интернет через промежуточную сеть PSTN.

#### **Задачи работы:**

1. Для центрального сервера и локальных серверов разработать терминальную сеть с использованием инструментальных средств приложения

2. Для каждой сети выбрать сетевую технологию и физическую топологию, конкретизировать архитектурные особенности с учетом ролевого распределение компьютеров.

3. Осуществить выбор активного сетевого оборудования (рабочих станций, серверов, коммуникационного оборудования) и выписать его основные характеристики (наименование, тип, производитель, количество портов и т.п.).

4. Установить на серверы приложения и определить виды трафика, создаваемого каждым из них.

5. Осуществить выбор среды передачи и номинальную битовую скорость протокола для линий связи всех уровней, включая магистральные связи и межсетевые телекоммуникации. Длины кабельных сегментов назначить произвольно в рамках технологических ограничений (витая пара до 100 м., оптоволокно до 500 м.).

6. Используя механизм анимации, организовать трафик небольшой интенсивности работающих приложений в каждом из сегментов и оценить степень загрузки магистралей, используя средства статистики. Используя данные усредненной утилизации магистралей и межсетевых телекоммуникаций, рассчитать их полезную пропускную способность.

## **Глава 1. Современное состояние клиент – серверных сетей**

### **1.1. Терминальный режим работы «тонких» клиентов.**

Вычислительные системы имеют два основных вида построения архитектуры: централизованный и распределенный. Распределенная архитектура реализуется на двух- и трехзвенную клиент-серверную сети. Основным различием между ними это при распределенной архитектуре большая часть вычислений проходит на «клиенте», а при централизованной все вычисления выполняются на центральном сервере. Система, основанная на терминалах, представляет собой центральную вычислительную площадку, к которой подсоединяются терминальные клиенты. Причем клиенты могут быть как стационарными, так и мобильными, а подключаться не только через LAN, но и через WAN. На центральной вычислительной площадке находится терминальный сервер, обычно он является сервером приложений, который может быть связан с сервером баз данных. На площадке также может находиться резервный терминальный сервер, обеспечивающий повышенную отказоустойчивость и высокую готовность системы в целом. При централизованной архитектуре особо актуально применение технологии «тонкий клиент».

Иначе говоря, под термином «тонкий клиент» подразумевается достаточно широкий с точки зрения системной архитектуры ряд устройств и программ, которые объединяются общим свойством: возможность работы в терминальном режиме. Таким образом, для работы тонкого клиента необходим терминальный сервер. Этим тонкий клиент отличается от толстого клиента, который, напротив, производит обработку информации независимо от сервера, используя последний в основном лишь для хранения данных.

Аппаратный тонкий клиент (например, Windows- и Linux-терминалы) — специализированное устройство, принципиально отличное от ПК. Он не имеет жёсткого диска, использует специализированную

локальную ОС (одна из задач которой организовать сессию с терминальным сервером для работы пользователя), не имеет в своём составе подвижных деталей, выполняется в специализированных корпусах с полностью пассивным охлаждением.

Для расширения функциональности тонкого клиента прибегают к его «утолщению», например, добавляют возможности автономной работы, сохраняя главное отличие — работу в сессии с терминальным сервером. Когда в клиенте появляются подвижные детали (жёсткие диски), появляются возможности автономной работы, он перестаёт быть тонким клиентом в чистом виде, а становится универсальным клиентом.

Тонкий клиент в большинстве случаев обладает минимальной аппаратной конфигурацией, вместо жёсткого диска для загрузки локальной специализированной ОС используется DOM (Disk On Module) (модуль с разъёмом IDE, флэш-памятью и микросхемой, реализующей логику обычного жёсткого диска — в BIOS определяется как обычный жёсткий диск, только размер его обычно в 2-3 раза меньше). В некоторых конфигурациях системы тонкий клиент загружает операционную систему по сети с сервера, используя протоколы PXE, BOOTP, DHCP, TFTP и Remote Installation Services (RIS).

Иными словами, тонкий клиент представляет собой системный блок, у которого обычно нет жесткого диска, и присутствует только минимальный набор железа, нужный для запуска операционной системы тонкого клиента (далее просто тонкого клиента). К системному блоку подключены питание, мышь, клавиатура, монитор, сетевой кабель. Кроме стандартного набора к тонкому клиенту могут быть подключены другие устройства, при условии, что он сможет их распознать и передать терминальному серверу.

Технически терминальный сервер представляет собой очень мощный компьютер (либо кластер), соединенный по сети с терминальными клиентами - которые, как правило, представляют собой маломощные или устаревшие рабочие станции, либо специализированные решения для

доступа к терминальному серверу. Терминальный сервер служит для удалённого обслуживания пользователя с предоставлением рабочего стола.

В последнее время усложнилась инфраструктура предприятий и организаций, стремительно растёт количество необходимых прикладных программ и приложений, постоянно возрастает уровень требований к мощностям вычислительных ресурсов.

Поэтому целями и задачами использования терминальной технологии на базе использования тонких клиентов является:

- Снижение временных расходов на администрирование;
- Повышение безопасности — снижение риска инсайдерских взломов;
- Снижение затрат на программное и аппаратное обеспечения;
- Снижение расхода электроэнергии;
- Увеличение отказоустойчивости оборудования.

## **1.2. Терминальный режим работы сервера.**

Терминальный режим принципиальным образом отличается от работы обычной компьютерной сети.

После старта тонкого клиента управление передаётся PXE-загрузчику, который находится в ПЗУ сетевой карты. PXE-загрузчик по протоколу BOOTP получает:

- сетевые настройки;
- IP адрес TFTP-сервера;
- путь до образа ОС тонкого клиента для загрузки.

После загрузки ОС тонкого клиента, управление передаётся терминалу.

Затем ОС тонкого клиента при загрузке ещё раз получает настройки сети и IP адрес TFTP-сервера и пытается загрузить конфигурационный файл. Если такой файл есть, то он загружается и применяется, если нет - применяются настройки по умолчанию.

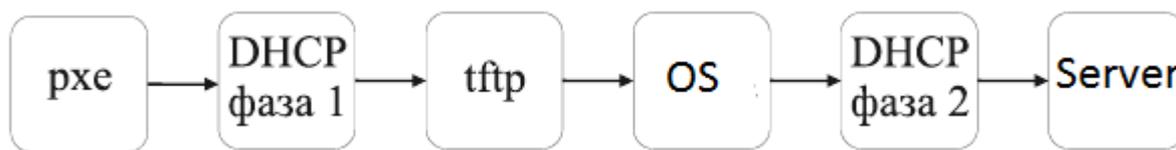


Рис. 1.1. Структурная схема работы клиент – серверной структуры.

Ключевым элементом для организации рабочего места пользователя есть тонкий клиент.

Иными словами, терминальный клиент после установления связи с терминальным сервером пересылает на последний вводимые данные (нажатия клавиш, перемещения мыши) и, возможно, предоставляет доступ к локальным ресурсам. Терминальный сервер предоставляет среду для работы (терминальная сессия), в которой исполняются приложения пользователя. Результат работы сервера передается на клиента, как правило, это изображение для монитора и звук (при его наличии).

Преимущества использования терминальной технологии на базе использования тонких клиентов вместо обычных персональных компьютеров следующие:

- снижение начальных затрат на приобретение, вследствие минимальных требований к конфигурации;
- унификация — все клиенты имеют одинаковый набор программного обеспечения;
- Взаимозаменяемость оборудования
- простота реализации задач — нет необходимости настраивать каждый компьютер по отдельности, так как осуществляется централизованное управление информационным процессом. Все настройки для управления тонкими клиентами системный администратор выполняет централизованно на сервере;

- экономия времени системного администратора, обслуживающего абсолютно одинаковые компьютеры, вероятность поломок которых сведена к минимуму, а все программы установлены на сервере;
- масштабируемость — созданный единожды образ системы для работы всей группы пользователей позволяет поддерживать легко масштабируемую сеть. Можно установить столько ПК, сколько требуется, при этом добавление новых рабочих мест требует минимальных усилий;
- безопасность и отказоустойчивость. Терминал, загружаясь, получает операционную систему «от производителя», настройка которой осуществляется только отделом информационной поддержки. Все модификации операционной системы и прикладного ПО никак не влияют ни на других пользователей, ни на образ, хранящийся на сервере. Вся пользовательская информация хранится на сервере на RAID-массиве и регулярно резервируется, что увеличивает отказоустойчивость;
- защита от утечек информации — нет локальных носителей — нет возможности делать копии документов на съемные носители информации.
- Сверхнизкое энергопотребление.«Холодный» процессор, отсутствие вентиляторов и прочих моторчиков, жестких дисков и приводов, флэш-память с мизерным потреблением – благодаря всему этому тонкий клиент потребляет чрезвычайно мало электроэнергии по сравнению с обычным ПК.
- терминалы практически не подвержены моральному старению, и срок их службы в 2—3 раза больше, чем у персональных компьютеров.

### **Недостатки**

- Концентрация всей функциональности в рамках одного (нескольких) серверов — выход из строя любого элемента между приложением и клиентами (сервер, коммутаторы) приводит к простоям многих пользователей.
- Усиливаются негативные последствия ошибок конфигурации и работы ПО (последствия ошибок сказываются не на отдельных пользователях, а на всех пользователях сервера сразу же)

- Проблемы с лицензированием (некоторое ПО не предусматривает ситуации работы нескольких пользователей на одном компьютере или требует использования более дорогих версий).
- неприменимы ресурсоемкие приложения для работы с графикой и трехмерным моделированием, такие как Photoshop, AutoCAD, 3D StudioMax.

Терминальный режим подразумевает, что на рабочем месте пользователя есть только «фреймы» т.е. изображение результата обработки информации. Все операции по ее обработке и хранению осуществляют сервера приложений. Доступ клиентов к приложениям осуществляется через терминальный сервер с использованием одного из известных протоколов терминального доступа.

### **1.3. Методы и среды передачи данных**

В настоящее время различают три основных метода передачи данных:

- коммутация каналов;
- коммутация сообщений;
- коммутация пакетов.

В качестве методов доступа можно выделить: случайные и детерминированные[5]. Среди случайных методов наиболее известен метод множественного доступа с контролем несущей и обнаружением конфликтов. Англоязычное название метода - Carrier Sense Multiple Access /Collision Detection (CSMA/CD).

Протокол CSMA/CD позволяет устранять коллизии путем выдачи каждой станцией, обнаружившей коллизию с помощью сигнала оповещения. Это заставляет все станции прекращать передачу согласно требованиям стандарта. Поэтому для своевременного обнаружения коллизии станция прослушивает среду на всем протяжении собственной передачи.

1. Станция, собирающаяся передавать, прослушивает среду, и передает, если среда свободна. В противном случае (т.е. если среда занята), переходит к шагу 2. При передаче нескольких кадров подряд станция выдерживает

вает определённую паузу между посылками кадров – межкадровый интервал, причем после каждой такой паузы перед отправкой следующего кадра станция вновь прослушивает среду (возвращение на начало шага 1);

2. Если среда занята, станция продолжает прослушивать среду до тех пор, пока среда не станет свободной, и затем сразу же начинает передачу;

3. Каждая станция, ведущая передачу, прослушивает среду, и, в случае обнаружения коллизии не прекращает сразу же передачу, а сначала передает короткий специальный сигнал коллизии – jam-сигнал, информируя другие станции о коллизии, и прекращает передачу;

4. После передачи jam-сигнала станция замолкает и ждет некоторое произвольное время в соответствии с правилом бинарной экспоненциальной задержки, а затем возвращается к шагу 1.

Сеть строится на основе стандарта 100BASE-TX. Стандарт 100BASE-TX определяет сегмент Ethernet на основе неэкранированных витых пар (UTP) категории 3 и выше с топологией пассивная звезда (Twisted-Pair Ethernet). Данный тип сегмента Ethernet имеет все преимущества и недостатки пассивной звезды. Суммарное количество кабеля, необходимого для объединения такого же количества компьютеров, оказывается гораздо больше, чем в случае шины. С другой стороны, обрыв кабеля не приводит к отказу всей сети, монтаж, а также диагностика неисправности сети проще. В сегменте 100BASE-TX передача сигналов осуществляется по двум витым парам проводов, каждая из которых передает только в одну сторону (одна пара – передающая, другая – принимающая). Кабелем, содержащим такие двойные витые пары, каждый из абонентов сети присоединяется к концентратору (хабу). Концентратор производит смешение сигналов от абонентов для реализации метода доступа CSMA/CD, то есть в данном случае реализуется топология пассивная звезда.

Так как характеристики сети удовлетворяют требованиям для использования витой пары в качестве сетевой среды, то выбран был кабель UTP категории 5E 24AWG. Кабели имеют стандартные разъемы RJ-45.

Данная сеть имеет топологию «многоуровневая звезда», т.к. здесь каждый ПК подключается отдельным кабелем к общему для группы коммутатору, а сам коммутатор совместно с коммутаторами своего уровня к – коммутатору уровнем выше. Всего выделяются три уровня: уровень доступа (УД), уровень распределения (УР) и уровень ядра (УЯ). УР расположен в кроссовой этажа, УЯ – в аппаратной. Такое иерархическое соединение называется «многоуровневая звезда». Особенностью такой топологии является высокая экономичность, т.к. для связи определенного количества узлов используется минимум кабеля.

Если между устройством и коммутатором происходит разрыв соединения, то вся остальная сеть продолжает работать. Правда, если этим устройством был единственный сервер, то работа будет несколько затруднена. При выходе из строя концентратора сеть перестанет работать. Данная сетевая топология наиболее удобна при поиске повреждений сетевых элементов: кабеля, сетевых адаптеров или разъемов. В качестве сетевой технологии для данной сети выбираем технологию Ethernet. В зависимости от скорости передачи данных и передающей среды существует несколько вариантов технологии.

Независимо от способа передачи стек сетевого протокола и программы работают одинаково практически во всех вариантах: 10 Мбит/с Ethernet, быстрый Ethernet (Fast Ethernet, 100 Мбит/с), Гигабит Ethernet (Gigabit Ethernet, 1 Гбит/с), 10 Гигабит Ethernet. Почти все технологии Ethernet используют метод доступа распределенной среды передачи данных.

Выбор технологии Ethernet в качестве базовых технологий осуществлен по ряду причин, выгодно отличающих их от других известных технологий передачи данных: технологии семейства Ethernet, являются наиболее эффективными по показателю быстродействие/стоимость.

## **Выводы к главе 1.**

Терминальный режим работы сервера позволяет организовать взаимодействие клиента и информационного ресурса с помощью терминалов, имеющих упрощенное исполнение и не требующих обслуживания.

В качестве технологии передачи данных выбрана технология Ethernet с методом доступа распределенной среды передачи данных

Для данной работы выбрана топологию “иерархическая звезда”, так как можно логически разделить офис на следующие уровни иерархии: комната – этаж – здание, на каждом из которых будет применяться свой класс сетевого оборудования в соответствии с нагрузкой на уровне.

## **Глава 2. Проектирование терминального режима клиент – серверных сетей.**

### **2.1. Аппаратное обеспечение клиент – серверных сетей.**

Определим количество рабочих мест главного офиса, состоящего из 9 этажей:

$$1512/9 = 168 \text{ рабочих мест.}$$

Всего девять рабочих групп, количество рабочих мест в одной рабочей группе:

$$168/9 = 18 \text{ рабочих мест.}$$

Для построения сети главного офиса необходимо: 1512 ПК, SQL server с встроенным сервером печати, 3 общих сервера (E-mail server, File server, HTTP server), сервер с FireWall +RAS/CS, Web-server, принтер, коммутаторы доступа, коммутаторы распределения, коммутатор ядра. А также маршрутизатор и модем для выхода на внешнюю сеть.

Обоснуем выбор состава активного оборудования для сети главного офиса.

В качестве хостов (оконечных узлов) выберем ПК Think Centre A52 8157-72G фирмы IBM (Нью-Йорк, США).

Основные характеристики:

Модель – Think Centre A52 8157-72G

Тип - бизнес-ПК

Процессор - Intel Pentium IV 1.8 ГГц под socket 775, 800 МГц FSB

Кэш память - уровень 1 - 16 кБ на кристалле, уровень 2 - 2 МБ на кристалле

Материнская плата - 200МГц

Оперативная память - PC4200 DDR2 SDRAM, 512 МБ (расш. до 4 ГБ), 2x240-конт. DIMM (1 не занят)

Жесткие диски - 120.0 ГБ, внутр., Serial ATA 1.0

Оптическое устройство хранения - DVD-RW 5.25" внутр.. АТАPI,  
DVD: 16

Видео - Intel Graphics Media Accelerator 950, на основе чипсета Intel  
GMA 950 чипсет, встроен. • PCI Express x16, 2048x1536/16 млн.

Видеопамять - расш. до 224 МБ, совместно используемая SDRAM

Звук - на основе Analog Devices ADI 1891 HD чипсет, встроен., АС'97,  
Microsoft DirectSound

Данный тип ПК может использоваться для любых приложений  
офисного типа.

В качестве серверов выберем xSeries, фирмы IBM (Нью-Йорк,  
США).

Основные характеристики:

Модель – xSeries

Тип – сервер/базовой производительности

Процессор - Intel Pentium IV 3.0 ГГц под socket 775, 800 МГц FSB

Кэш память - уровень 1 - 16 кБ на кристалле, уровень 2 - 1 МБ на  
кристалле

Материнская плата - 200МГц

Оперативная память – 512 МБ (макс. 16 ГБ) PC3200 DDR2 SDRAM- 6  
(4 не занято), 240-конт. DIMM, код исправления ошибок

Жесткие диски - 120.0 ГБ, внутр., SCSI, 7200 об/мин

Оптическое устройство хранения - DVD-RW 5.25" внутр.. АТАPI,  
DVD: 16

Видео - на основе чипсета Radeon 7000M, встроен. • PCI, 2048x1536/16  
млн., 16 МБ DDR SDRAM

Сетевой адаптер - 10 Мбит/сек., 100 Мбит/сек., 1000 Мбит/сек.,  
Ethernet, Fast Ethernet, Gigabit Ethernet, встроен., IEEE 802.3 (Ethernet), IEEE  
802.3ab (TP Gigabit Ethernet), IEEE 802.3u (Fast Ethernet).

В качестве коммутаторов выберем однотипное оборудование Cisco  
Catalyst 2948G фирмы Cisco (Сан-Хосе, США)

В качестве магистрального коммутатора ядра выберем Cisco Catalyst 4003.

В качестве маршрутизаторов выберем Cisco 4500-RPS-M

Учитывая выбранное активное оборудование сети главного офиса, изобразим логическое общее построение сети главного офиса (рис. 2.1)

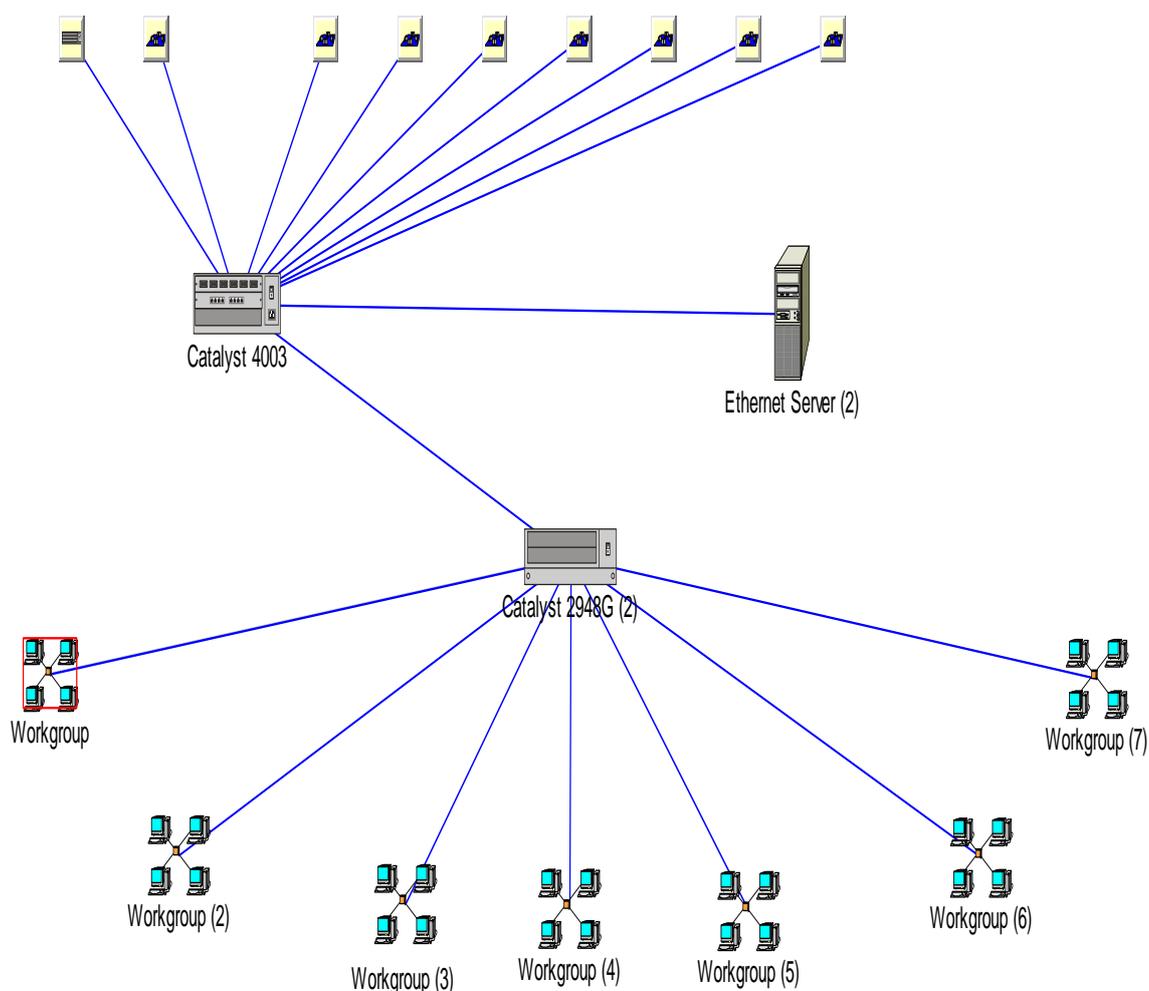


Рис.2.1. Общее построение сети главного офиса.

## 2.2. Выбор среды передачи данных

Для выбора состава оборудования необходимо выбрать среды передачи и необходимый трафик передачи данных.

Нужно рассчитать трафик для:

- коммутатора рабочей группы офиса;
- коммутатора этажа;

- коммутатора ядра офиса

1) Для коммутатора рабочей группы.

Здесь во внимание берется тип трафика, циркулирующий внутри рабочей группы – это LAN peer-to-peer traffic, Voice over IP peer-to-peer, а также трафик к серверам рабочей группы ( SQL- server), т.е. SQL – client трафик, который генерируется ПК к общим серверам (File server, E-mail server, HTTP server).

LAN peer-to-peer traffic – передача данных в одноранговом режиме (точка-точка) (объем сообщения - 10 Кбайт, средняя интенсивность - 20 сообщений в час).

$$\gamma = \frac{10 \cdot 8 \cdot 20}{3600} = 0,45 \cdot 10^{-3} \text{ Мб/с}.$$

Voice over IP peer-to-peer — передача голосового трафика IP-пакетами (объем сообщения - 10 Мбайт, средняя интенсивность — 2 сообщения в час, трафик между рабочими группами).

$$\gamma = \frac{10 \cdot 8 \cdot 2}{3600} = 0,046 \text{ Мб/с}$$

File Server's client - трафик клиента файлового сервера (объем сообщения - 1 Кбайт, средняя интенсивность - 3 сообщения в час).

$$\gamma = \frac{1 \cdot 8 \cdot 3}{3600} = 6,8 \cdot 10^{-6} \text{ Мб/с}$$

E-mail - электронная почта в ЛВС (объем сообщения —10 Кбайт, средняя интенсивность —10 сообщений в час).

$$\gamma = \frac{10 \cdot 10 \cdot 8}{3600} = 0,23 \cdot 10^{-3} \text{ Мб/с}$$

HTTP client – данные гипертекстов (web-страниц) (объем сообщения — 1,5М байта, средняя интенсивность —5 сообщений в час).

$$\gamma = \frac{1,5 \cdot 8 \cdot 5}{3600} = 0,017 \text{ Мб/с}$$

SQL server's client - трафик клиента SQL-сервера (объем сообщения - 0,5 Кбайт, средняя интенсивность - 15 сообщений в час).

$$\gamma = \frac{0.5 \cdot 15 \cdot 8}{3600} \cdot 24 = 0,4 \cdot 10^{-3} \text{ Мб/с}$$

Определим общую загрузку трафиком для порта коммутатора рабочей группы офиса:

$$\gamma_{\text{РГ}} = 0,000434 + 0,067 + 0,00097 + 0,002 + 0,0167 = 0,087104 \text{ Мб/с}$$

Ставим коммутатор, который поддерживает 10 Мбитный порт Ethernet.

2) Для коммутатора этажа.

Здесь во внимание берется тип трафика, который генерируется всеми ПК рабочей группы к общим серверам (File server, E-mail server, HTTP – server(доступ в интернет)), а также трафик Voice over IP peer-to-peer(трафик между рабочими группами).

Voice over IP peer-to-peer — передача голосового трафика IP-пакетами между рабочими группами (объем сообщения - 10 Мбайт, средняя интенсивность — 2 сообщения в час, трафик между рабочими группами).

$$\gamma = \frac{10 \cdot 8 \cdot 2}{3600} * 24 = 1,1 \text{ Мб/с}$$

$$\gamma_{\text{Э}} = (6,8 \cdot 10^{-6} + 0,23 \cdot 10^{-3} + 0,017 + 1,1) * 24 = 26,8 \text{ Мб/с}$$

Ставим коммутатор, который поддерживает 100 Мбитный порт Ethernet.

3) Для коммутатора ядра здания.

Здесь во внимание берется тип трафика, который генерируется всеми ПК этажа к общим серверам (File server, E-mail server, HTTP –server(доступ в интернет)).

$$\gamma_{\text{Э}} = (6,8 \cdot 10^{-6} + 0,23 \cdot 10^{-3} + 0,017) \cdot 24 \cdot 7 = 2,9 \text{ Мб/с}$$

Ставим коммутатор, который поддерживает 10 Мбитный порт Ethernet.

4) Для коммутатора внешней сети.

Здесь во внимание берется тип трафика, который генерируется всеми ПК здания к общим серверам (File server, E-mail server, HTTP –server (доступ в интернет)).

$$\gamma_{\text{К}} = (6,8 \cdot 10^{-6} + 0,23 \cdot 10^{-3} + 0,017) \cdot 24 \cdot 7 \cdot 9 = 26,1 \text{ Мб/с}$$

Можно ставить коммутатор, который поддерживает 100 Мбитный порт Ethernet.

### **2.3. Программное обеспечение клиент – серверных сетей**

На общих серверах устанавливается сетевая ОС Free BSD. На сервере с FireWall и RAS/CS - Windows Server 2003.

Выбор данных ОС подкреплён общей распространённостью, простотой в пользовании, администрированием всей сети и её компонентов при работе с интерфейсом данных ОС.

Протоколы.

Вышеперечисленные ОС могут поддерживать протоколы нижестоящих уровней OSI, а также протоколы своего уровня. А именно: 7-уровень: RTP, HTTP, SMTP, POP-3, NETBIOS и т.д.; 4-уровень: TCP, UDP;

3-уровень: IP, IPX, LRP, RIP, OSPF, BGP и т.д.; 2-уровень: технологии Ethernet, ATM, ISDN и т.д.

Многие приложения требуемые заказчиком автоматически ставятся при установке ОС, а именно: Интернет браузер - Internet Explorer, Outlook Express - для почты, Paint - для обработки графических файлов и т.д. .

Но также необходимо проинсталлировать такие виды приложений для работы с определенным типом трафика.

Для E-mail - The Bat.

Для Voice over IP peer-to-peer - Skype.

Для работы с текстовыми документами, таблицами, базами данных - пакет MS Office, I C.

Для альтернативы веб-браузера - Opera, Fire Fox.

Для альтернативы проводника (explorer) - Total Commander.

Для альтернативы работы с видео (Windows Media) - Light Allow, Jet Audio. Для работы с архивами - WinRAR.

Для защиты ПК от вредоносных программ (вирусов) - Dr.Web.

Все клиентские части серверных программ установлены вместе с ОС

либо в вышеперечисленных приложениях.

Для серверов необходимо поставить серверные части программ.

File Server - файловый сервер. Серверное программное обеспечение управления доступом к файлам и другим дисковым ресурсам сети. Инсталлируется, как правило, на выделенном мощном компьютере, который помимо управления доступом к файлам и другим дисковым ресурсам ЛВС обеспечивает безопасность и синхронизацию. Безопасность понимается в том смысле, что доступ к отдельным файлам могут получить только авторизованные пользователи, обладающие соответствующими правами. Синхронизация заключается в блокировке доступа к файлам и записям, и предназначена для защиты данных от повреждения при одновременной попытке их изменения несколькими пользователями.

E-mail Server - сервер электронной почты. Программа, которая управляет доставкой электронной почты и другой информации. Для работы почтового сервера выделенный компьютер не требуется.

Отдельный сервер для FireWall и RAS/CS - FireWall (Outpost) и служба RAS/CS. Отдельный Web-server - приложение UserGate (доступ в Интернет), FireWall (Outpost).

HTTP-сервер – общие серверы. Они предназначены для предоставления ресурсов web-сайтов. Он взаимодействует с HTTP-клиентом по протоколу передачи гипертекста HTTP. Используется в сетях Intranet, Extranet, поддерживающих архитектуру «клиент-сервер».

SQL Server - SQL сервер. Серверная специализированная программа обращения к БД, поддерживающая язык структурированных запросов. Для работы не требует выделенного компьютера.

На всех серверах настраивается требуемый тип приложения сетевым администратором, путем настройки ОС.

## **2.4. Пропускная способность клиент – серверной сети**

На связи ПК – коммутатор РГ генерируется трафик: LAN peer-to-peer traffic, Voice over IP peer-to-peer, а также трафик к серверу рабочей группы (SQL - server), т.е. SQL – client и трафик, который генерируется ПК к общим серверам (File server, E-mail server, HTTP-server). Соответственно это приложения: Photo Shop, Visio, Corel Draw, Total Commander, Light Allow, Internet Explorer, Jet Audio, MS Word, Excel, Access, Skype, 1С, The Bat.

На связи SQL – server – коммутатор РГ: Internet Explorer.

На связи коммутатор РГ - коммутатор этажа: трафик к общим серверам (File server, E-mail server, HTTP-server), а также трафик Voice over IP peer-to-peer.

Приложения: Skype, The Bat, Total Commander и т.д.

На связи коммутатор этажа – коммутатор здания: трафик к общим серверам (File server, E-mail server, HTTP-server).

Приложения: The Bat, Total Commander и встроенные в ОС приложения.

На связи коммутатор здания – коммутатор кампуса: трафик к общим серверам (File server, E-mail server, HTTP-server).

Приложения: The Bat, Total Commander и встроенные в ОС приложения.

Выход во внешнюю сеть (Интернет) будем организовывать по технологии ADSL 2+.

Данная технология является асимметричной по скорости приема/передачи (24/2 Мбит/с). По одной телефонной линии идет телефонный и информационный трафик. Это осуществляется путем частотного разделения канала с помощью сплитера.

Для реализации этой технологии со стороны абонента нужны: телефонная линия, сплитер, ADSL 2+ модем.

К активному оборудованию относится ADSL 2+ модем. Это - Zyxel P-660RT EE.

Модем P-660RT принадлежит к четвертому поколению ADSL-модемов и предоставляет функциональность, необходимую для подключения уже имеющейся офисной сети к Интернету.

Основные преимущества:

- Высокоскоростной Интернет – до 24 Мбит/с
- Надежное соединение на проблемных линиях
- Свободный телефон;
- Постоянное соединение;
- Не требует установки драйвера;
- Работает с Windows, Mac, Linux;
- Простая настройка;
- Защита от атак из Интернета;
- Сплитер в комплекте.

Данный модем также настраивается в режим маршрутизатора, поэтому отдельного маршрутизатора не требуется.

Для распределенного доступа к сети Интернет также используется Web-server, на котором установлены приложения: Outpost (FireWall), UserGate (программа контроля за доступом к сети Интернет), Dr. Web (антивирусная программа).

Пропускная способность оценивает скорость сетевого протокола и числом передаваемых кадров в секунду. Различают номинальную и полезную скорость протокола.

Нам нужно рассчитать именно полезную пропускную способность протокола.

Для этого:

- запускаем 4 раза режим анимации для нашей сети;
- при длине пакетов в сети:

700 байт, 720 байт, 725 байт, 750 байт находим среднюю длину пакета:

$$\frac{700+720+725+750}{4} = 723 \text{ байт};$$

- теперь определим время передачи кадра длиной 723 байт:

$$t = \frac{723 \cdot 8}{10000000} = 579 \text{ мкс при максимальной скорости } 10 \text{ Мбит/с};$$

- с учетом межкадрового интервала, который составляет 9,6 мкс период следования кадра будет равен:  $9,6 \text{ мкс} + 579 \text{ мкс} = 588,6 \text{ мкс}$ ;

- определим максимальное число кадров передаваемое за 1 секунду:

$$P = \frac{1}{0.0005886} = 1698 \text{ кадров/с};$$

- теперь вычислим полезную пропускную способность протокола без учета времени ожидания доступа у среде. Для этого необходимо от средней длины кадра 723 байт вычесть преамбулу (8 байт) и служебную информацию (18 байт), т.е. определить полезную информацию:  $723 - 18 - 8 = 693$  байт – полезные данные.

$$\text{Тогда } C_{\text{п}} = 693 \cdot 8 \cdot 1694 = 9,4 \text{ Мб/с.}$$

Таким образом, полезная скорость протокола без учета времени ожидания доступа к среде составляет 9,4 Мб/с. Это означает, что вполне достаточно будет использовать 10 Мбитный порт Ethernet.

## **Выводы к главе 2**

Определены: объект исследования, размеры и структура сети, дано обоснование выбора необходимого сетевого оборудования. Общее построение сети главного офиса.

Произведены расчеты по пропускной способности сети, необходимого количества и длины кабельной системы.

## Глава 3. Практическая реализация терминального режима клиент – серверных сетей.

### 3.1. Реализация терминальной технологии

Для реализации в качестве терминальной сети используем топологию «многоуровневая звезда», т.к. здесь каждый ПК подключается отдельным кабелем к общему для группы коммутатору, а сам коммутатор совместно с коммутаторами своего уровня к – коммутатору следующего уровня. Особенностью такой топологии является высокая экономичность, т.к. для связи определенного количества узлов используется минимум кабеля.

Практическая реализация сети этажа представлено на рис. 3.1 и сети рабочей группы на рис. 3.2.

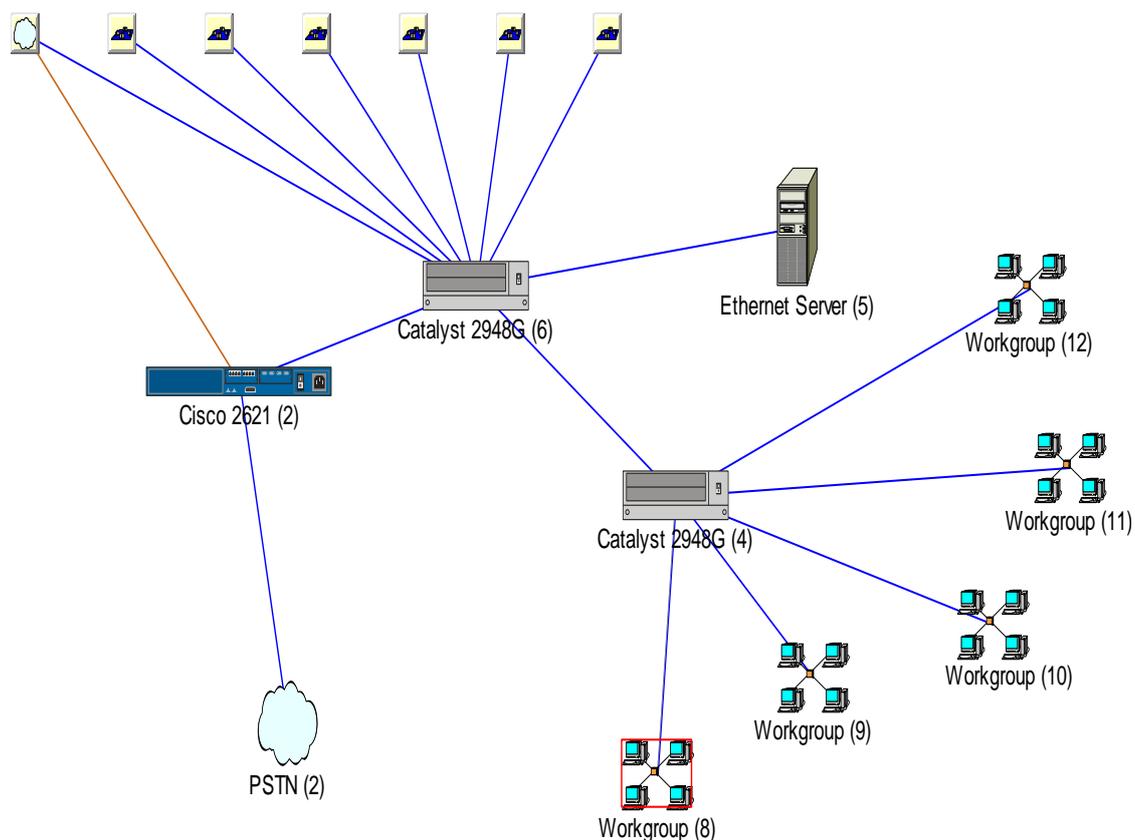


Рис.3.1. Практическая реализация главного офиса.

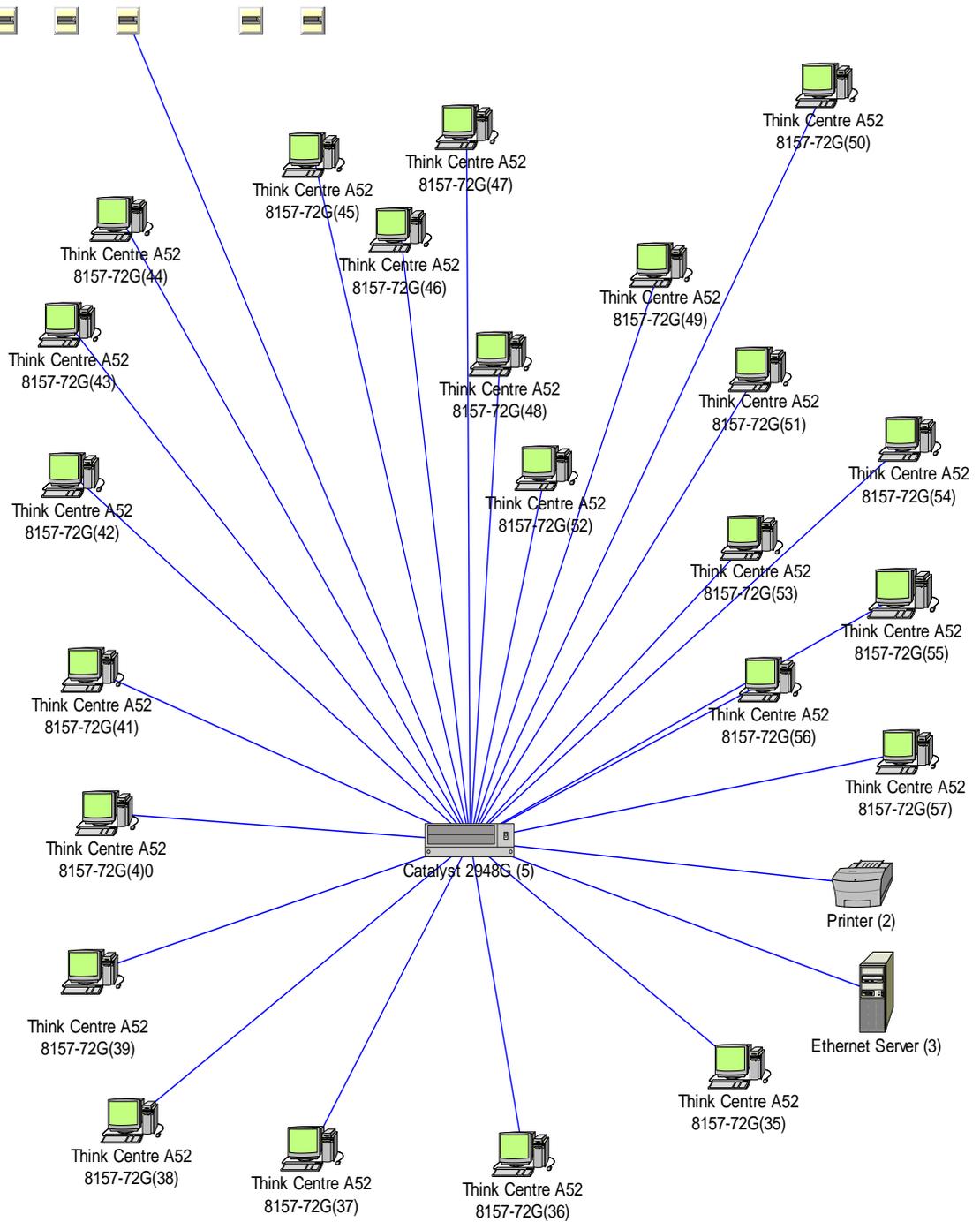


Рис.3.2. Практическая реализация сети рабочей группы.

В качестве технологии используем Ethernet с методом доступа распределенной среды передачи данных.

Достоинство Ethernet: экономичность, расширяемость, простота реализации простых алгоритмов доступа к среде, адресации и передачи данных.

Недостатки: домен коллизий и широковещательный домен, но они могут быть устранены с помощью уровневых сетевых коммутаторов и маршрутизаторов.

Файловый сервер будет реализован на базе ОС Linux, а терминальный – Windows.

Поэтому для реализации терминальной технологии придётся использовать 2 службы и 1 пакет. DHCP – предоставляет клиентам сетевые реквизиты. TFTP – простой способ предоставить доступ к файлам по сети Thinstation – пакет образа тонкого клиента

Дистрибутив «Thinstation» разработан специально для создания тонких клиентов и оснащен всеми необходимыми приложениями, обеспечивающими подключение к сервисам по основным протоколам удаленной работы: Citrix ICA, Microsoft RDP, VNC, NX NoMachine, 2X ThinClient, VMWare View Open client, X11, Telnet, SSH. Систему можно загружать по сети с помощью Etherboot/PXE или внешнего носителя (FDD/CD/HDD/CF/USB-flash). Все настройки производятся централизованно при помощи конфигурационных файлов, что упрощает управление терминалами.

**Thinstation** - мини-дистрибутив Linux, позволяющий превратить старые компьютеры в полноценные бездисковые тонкие клиенты.

Версия Thinstation 2.2.2, в отличие от Thinstation 5.1 менее требовательна к техническому обеспечению, поэтому не стоит забывать про неё при использовании старых машин в качестве тонких клиентов.

### **Установка и настройка DHCP**

Установка DHCPD с последующей автозагрузкой.

```
# yum -y install dhcp
# chkconfig g dhcpd on
vim /etc/dhcpd.conf
```

```
ddns-update-style interim;
ignore client-updates;
authoritative;
# Описание настроек подсети
subnet 192.168.0.0 netmask 255.255.255.0 {
# Диапазон адресов, который будет выдавать DHCP сервер
range 192.168.0.50 192.168.0.254;
# шлюзпоумолчанию
option routers 192.168.0.1;
# маскаподсети
option subnet-mask 255.255.255.0;
# DNS
option domain-name-servers 192.168.0.1;
#Время на которое выдаться IPадрес
default-lease-time 14400;
max-lease-time 86400;
# ПутьдообразаThinstation Linux
filename "/visteh-0.1/pxelinux.0";
# TFTP-сервер
next-server 192.168.0.1;
}
```

```
udp0 0 0.0.0.0:69 0.0.0.0:* 3105/xinetd
```

## Настройки тонких клиентов

Для начала, необходимо распаковать архив с образом тонкого клиента в /var/lib/tftpboot таким образом, чтобы рхе-загрузчик был доступен по пути "/var/lib/tftpboot/visteh-0.1/pxelinux.0". Далее создается общий файл настроек для тонких клиентов:

```
# vim/var/lib/tftpboot/thinstation.conf.network
```

```
# IP адрес терминального сервера
SESSION_0_FREERDP_SERVER=192.168.0.2
# Протокол доступа к терминальному серверу
SESSION_0_TYPE=freerdp
```

## **Настройка разрешения экрана в Thinstation Linux** производится

параметром SCREEN\_RESOLUTION:

```
SCREEN_RESOLUTION="1280x1024"
```

Затем производится указание режима работы монитора и частоты развёртки: инструкции X\_MONITOR\_MODELINE, SCREEN\_HORIZSYNC и SCREEN\_VERTREFRESH.

VGA-режим задается с помощью утилиты 915resolution, которая включена в образ Thinstation Linux. Пример:

Включаем 915resolution

```
INTELWIDESCREEEN_ENABLED=On
```

Параметры, передаваемые утилите при запуске.

- 49 - номер режима
- 1920 1080 - количество точек по горизонтали и вертикали соответственно
- 16 - битность изображения

```
INTELWIDESCREEEN_OPTIONS="49 1920 1080 16"
```

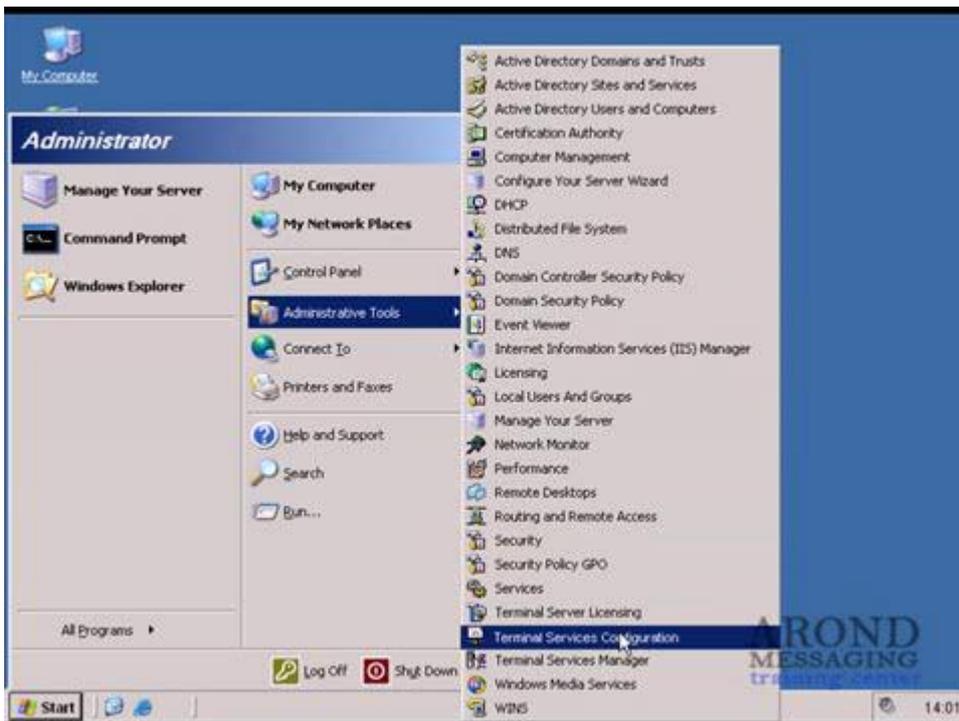
Для более полной информации по параметрам следует набрать команду в консоли тонкого клиента : # 915resolution -h

### **Установка сервера терминалов в Windows Server 2003 R2**

Последовательность операций:

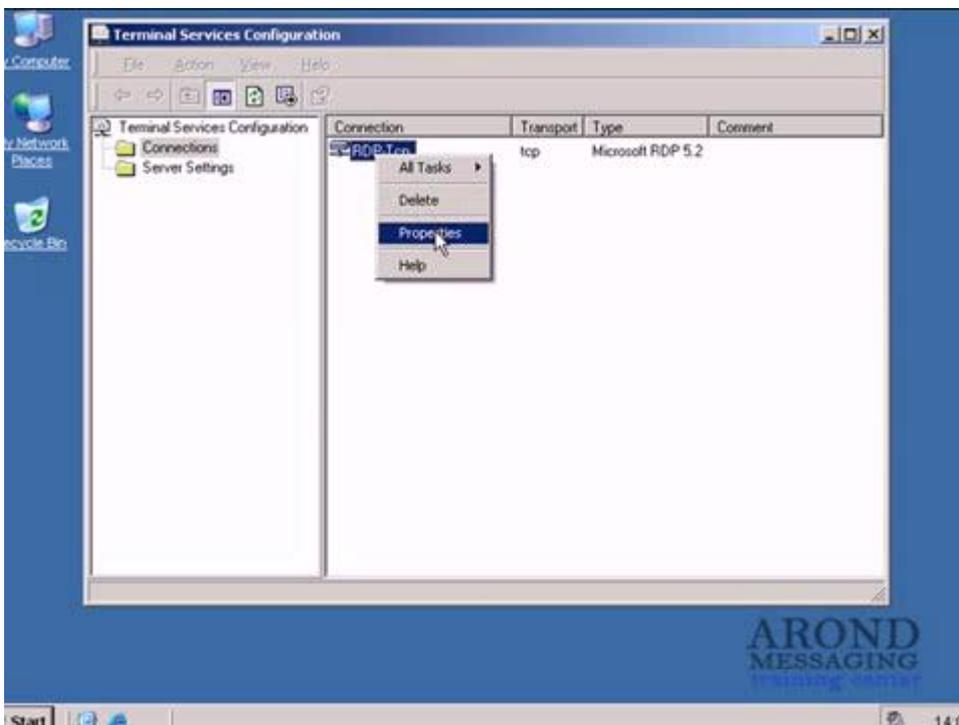
1. «Start» — «Administrative Tools» - «Terminal Service Configuration».

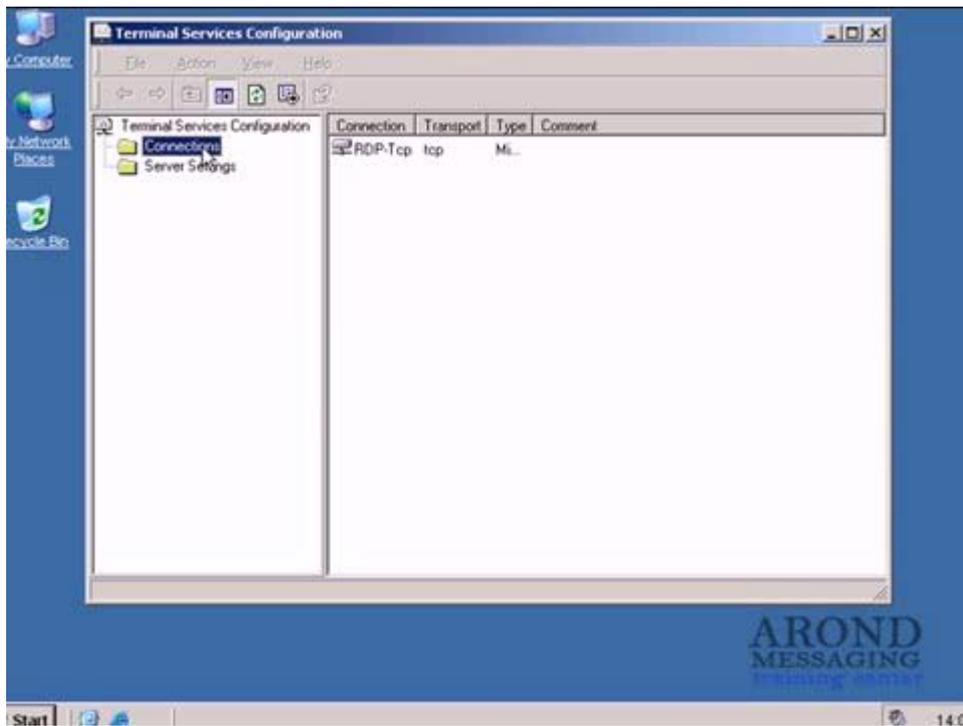
Откроется окно «Terminal Service Configuration».



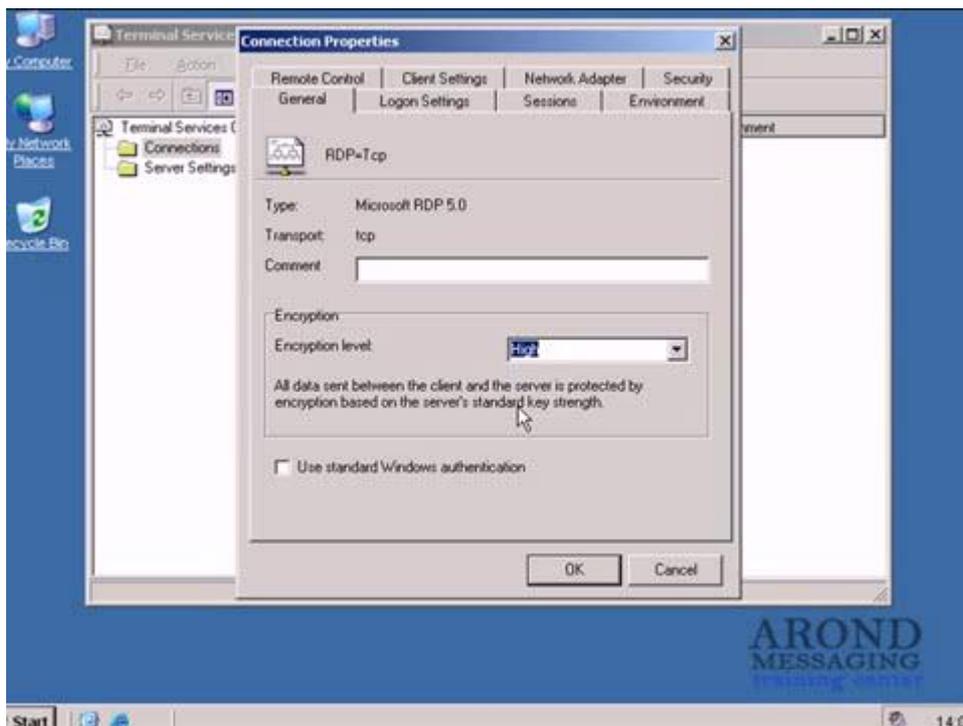
2. Затем загружается «Corrections» в правой части окна.

3. Через свойства RDP-TCP осуществляется нажатие правой кнопки по иконке RDP-TCP и выбора пункта контекстного меню «Property»

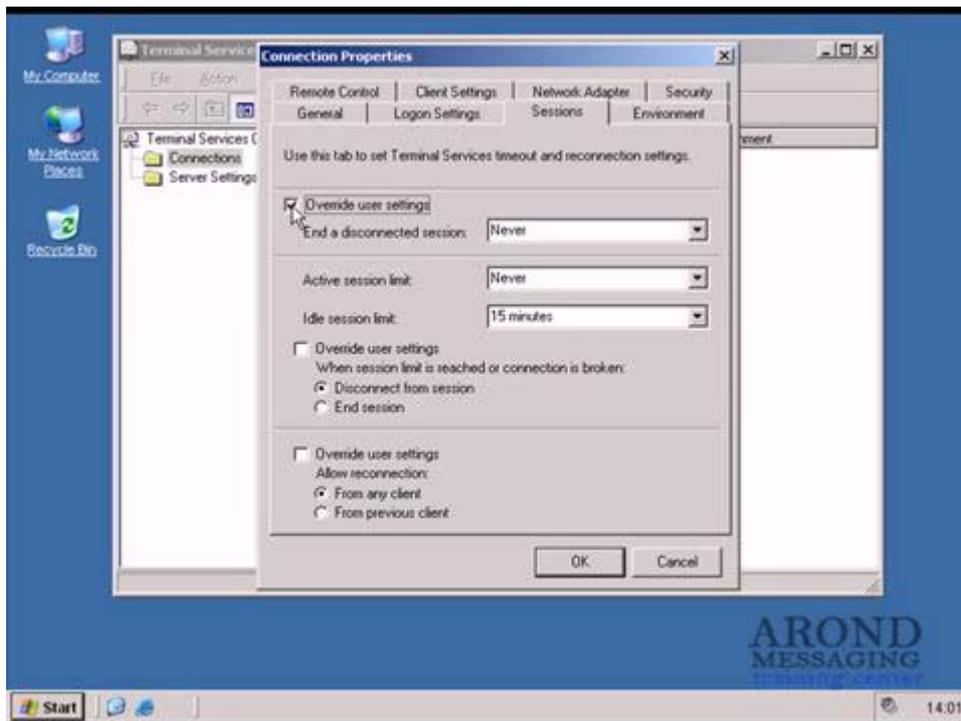




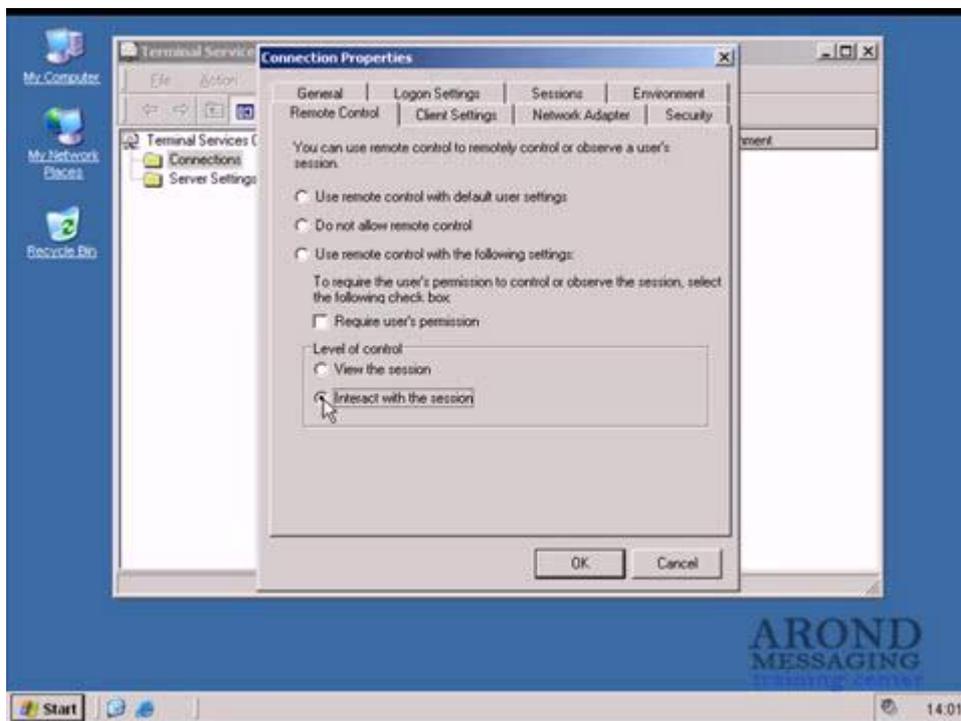
4. На «General» необходимо изменить значение «Encryptionlevel» на «High»



5. На «Sessions» изменяется значение «Idle session limit» на «15 minutes» и активируется опция «Override user settings»



6. На «Remote Control» ставится переключатель в положение «Interactwiththesession»



Установка сервера терминалов закончена.

## **3.2. Реализация программного обеспечения клиента**

### **Операционная система (ОС).**

На рабочих терминалах ПК будет установлена одна из последних версий ОС компании Microsoft – Windows XP.

Выбор данных ОС подкреплен общей распространенностью, простой в пользовании, администрированием всей сети и ее компонентов при работе с интерфейсом данных ОС.

Многие приложения, требуемые заказчиком автоматически ставятся при установке ОС, а именно: Интернет браузер – Internet Explorer, Outlook Express – для почты и т.д.

Но также необходимо проинсталлировать такие виды приложений для работы с определенным типом трафика.

Для E-mail – The Bat.

Для работы с текстовыми документами, таблицами, базами данных – пакет MS Office, 1С, Oracle.

Для альтернативы веб-браузера – Opera.

Для альтернативы проводника (explorer) – Total Commander.

Для альтернативы работы с видео (Windows Media) – Light Allow, Jet Audio.

Для работы с архивами – WinRAR.

Для защиты ПК от вредоносных программ (вирусов) – NOD 32 3.0.

Все клиентские части серверных программ установлены вместе с ОС либо в вышеперечисленных приложениях.

Для серверов необходимо поставить серверные части программ.

E-mail Server — сервер электронной почты. Программа, которая управляет доставкой электронной почты и другой информации. Для работы почтового сервера выделенный компьютер не требуется.

На связи ПК – коммутатор РГ генерируется трафик: LAN peer-to-peer traffic, а также трафик к серверу рабочей группы (FTP - server), т.е. FTP-client и трафик, который генерируется ПК к общему серверу (E-mail server).

Соответственно это приложения: Total Commander, Light Allow, Internet Explorer, Jet Audio, MS Word, Access, 1C, The Bat.

На связи FTP - server – коммутатор РГ: Total Commander, NetLook.

На связи коммутатор РГ - коммутатор этажа: трафик к общим серверам (E-mail server). Приложения: The Bat, Total Commander и т.д.

На связи коммутатор этажа – коммутатор здания: трафик к общим серверам (E-mail server). Приложения: The Bat, Total Commander и встроенные в ОС приложения.

На связи коммутатор здания – коммутатор филиалов: трафик к общим серверам (E-mail server).

Приложения: The Bat, Total Commander и встроенные в ОС приложения.

Для разграничения прав коммутатор использует список контроля доступа (ACL), который может содержать до 256 записей, а также технологию IP-MAC-port Binding, которая позволяет контролировать доступ подключенных к коммутатору устройств в сеть на основе их IP и MAC-адресов, а также порта подключения.

### **3.3. Организация внешнего доступа клиент – серверной сети**

Выход во внешнюю сеть (Интернет) будем организовывать по технологии ADSL. Данная технология является асимметричной по скорости приема/передачи (24/2 Мбит/с). По одной телефонной линии идет телефонный и информационный трафик. Это осуществляется путем частотного разделения канала с помощью сплитера. Для реализации этой технологии со стороны абонента нужны: телефонная линия, сплитер, ADSL модем. К активному оборудованию относится ADSL модем. Это - Zyxel P-660RT EE. Модем P-660RT принадлежит к четвертому поколению ADSL-модемов и предоставляет функциональность, необходимую для подключения уже имеющейся офисной сети к Интернету.

Основные преимущества:

- Высокоскоростной Интернет – до 24 Мбит/с
- Надежное соединение на проблемных линиях
- Свободный телефон;
- Постоянное соединение;
- Не требует установки драйвера;
- Работает с Windows, Mac, Linux;
- Защита от атак из Интернета;

Для распределенного доступа к сети Интернет также используется FireWall.

Для организации удаленного доступа для объединения сетей Главного офиса предполагаемая длительность занятия каналов для этой связи составляет 60 часов в месяц, поэтому будем использовать технологию коммутации пакетов – АТМ ( 2 Мбит/с).

Для организации связи через сеть АТМ со стороны Главного офиса необходимо оборудование, которое поддерживает данную технологию: маршрутизатор, сервер удаленного доступа RAS/CS.

Сервер удаленного доступа RAS/CS идет в комплекте с ОС Windows 2003 Server. Он настраивается сетевым администратором путем настройки конфигурации сетевой ОС. Программное сжатие данных в сервисе удаленного доступа позволяет пользователям существенно увеличить (практически в два раза) пропускную способность своего соединения. Поддержка прикладных программных интерфейсов RAS позволяет пользователям разрабатывать собственные приложения, обладающие возможностями удаленного доступа. Для обеспечения секретности передаваемых данных в сервисе RAS имеется встроенный механизм шифрации данных, основанный на алгоритме открытого ключа RC4 компании RSA Data Security.

Для организации связи через сеть PSTN со стороны Главного офиса необходимо оборудование, которое поддерживает данную технологию: маршрутизатор, сервер удаленного доступа RAS/CS. Маршрутизатор -

модульный маршрутизатор Cisco серии 4500 фирмы Cisco Systems, со вставленной ISDN платой ISDN Interface Processor.

Полная спецификация активного оборудования, используемого для построения клиент – серверной сети.

Таблица 3.1. Спецификация активного оборудования для построения клиент - серверной сети

№	Тип оборудования	Фирма-производитель	Наименование и показатели	Кол, шт
1.	ПК	IBM	Think Centre A52 8157-72G Процессор - Intel Pentium IV 1.8 ГГц под socket 775, 800 МГц FSB Кэш память - уровень 1 - 16 кБ на кристалле, уровень 2 - 2 МБ на кристалле Материнская плата - 200МГц Оперативная память - PC4200 DDR2 SDRAM, 512 МБ (расш. до 4 ГБ), 2x240-конт. DIMM (1 не занят) Жесткие диски - 120.0 ГБ, внутр., Serial ATA1.0 Оптическое устройство хранения - DVD-RW 5.25" внутр.. АТАPI, DVD: 16 Видео - Intel Graphics Media Accelerator 950, на основе чипсета Intel GMA 950 чипсет, встроен. • PCI Express x16, 2048x1536/16 млн. Видеопамять - расш. до 224 МБ, совместно используемая SDRAM Звук - на основе Analog Devices ADI 1891 HD чипсет, встроен., AC'97, Microsoft DirectSound Сетевой адаптер - 10 Мбит/сек., 100 Мбит/сек., 1000 Мбит/сек., Ethernet, FE, GE.	3300
2.	Сервер	IBM	xSeries Процессор - Intel Pentium IV 3.0 ГГц под socket 775, 800 МГц FSB Кэш память - уровень 1 - 16 кБ на кристалле, уровень 2 - 1 МБ на кристалле Материнская плата - 200МГц Оперативная память – 512 МБ (макс. 16 ГБ) PC3200 DDR2 SDRAM- 6 (4 не занято), 240-конт. DIMM. Жесткие диски - 200.0 ГБ, внутр., SCSI, 7200 об/мин Оптическое устройство хранения - DVD-RW 5.25" внутр.. АТАPI, DVD: 16 Видео - на основе чипсета Radeon 7000M, встроен. • PCI, 2048x1536/16 млн., 16 МБ DDR	143

			SDRAM Сетевой адаптер - 10 Мбит/сек., 100 Мбит/сек, 1000 Мбит/сек., Ethernet, FE, GE.	
3.	Коммутатор	Cisco Systems	Cisco Catalyst 2948G внутренняя шина - 22 Гбит/сек, более 10 млн. пакетов в сек. (64-byte packets); скорость обработки пакетов размером 64 байта - 14880 в режиме 10 Мбит/сек, 148800 в режиме 100 Мбит/сек, 1488000 в режиме 1000 Мбит/сек; буфер - 12-МВ разделяемой памяти на все порты; процессор 150 MHz (R5000 RISC); Информация о портах : 48 10BaseT/100BaseTX, 2 1000BaseX GE. Информация о памяти : 64MB DRAM и 16MB flash	143
5.	коммутатор ядра	Cisco Systems	Cisco Catalyst 4003 поддерживает модули: 48-портовый 10/100 FE , 32-порта 10/100 FE плюс два порта GE 6 портов Get, 18 портов GE обрабатывает 18 мил.п/сек и обладает быстродействующей внутренней шиной 24 Гбит/с	1
6.	маршрутизатор	Cisco Systems	Cisco 4500-RPS-M построены на параллельной архитектуре	1
7.	маршрутизатор	Cisco Systems	Модель Cisco 2621 имеет два порта FE 10/100 Мбит/с, двумя слотами WAN, для установки интерфейсных модулей WIC (WAN Interface Card), одним слотом для сетевого модуля и внутренним слотом AIM (Advanced Interface Module)., оборудована высокопроизводительным процессором RISC. Интерфейсы FE маршрутизатора Cisco 2621 обеспечивают поддержку протокола ISL (Inter-Switch Link) для подключения к нескольким VLAN.	4

### **3.4. Проектирование кабельной системы клиент – серверной сети.**

Для прокладки горизонтальных и вертикальных кабелей подсистемы внутренних магистралей проектируемой кабельной системы используются следующие разновидности каналов:

- закрытые металлические лотки за фальшпотолком, предназначенные для прокладки кабелей горизонтальной подсистемы в коридорах;
- декоративные короба (в связи с отсутствием каналов в стенах и в полу рабочих помещений пользователей);
- закладные трубки типа гильз диаметром в свету 32 мм, через которые производится ввод за фальшпотолком рабочих помещений пользователей горизонтальных кабелей, снимаемых с лотка в коридоре;
- вертикальные трубчатые элементы типа рукавов диаметром в свету 80 мм, выполняющие функции каналов стояка и используемые для прокладки по ним кабелей подсистемы внутренних магистралей.

Кроссовая этажа представляет собой служебное помещение, в которое вводятся кабели подсистемы внутренних магистралей СКС и кабели горизонтальной подсистемы. В этом помещении монтируется коммутационное и другое вспомогательное оборудование. КЭ должна быть максимально приближена к вертикальным стоякам, по которым прокладывается кабель магистрали внутренней СКС. Для минимизации длины кабеля и стоимости горизонтальной подсистемы, КЭ размещается по центру обслуживаемой рабочей зоны. Для обеспечения режима контроля доступа комната не должна иметь окон и не должна быть совмещена с другими комнатами.

Согласно стандарту ISO/IEC11801 обслуживаемая площадь на 1 КЭ не должна превышать 1000м<sup>2</sup>.

Волоконно-оптические и электрические кабели подсистемы внешних магистралей обычно прокладываются в телефонной канализации. Глубина закладки кабеля составляет 0,4-1,5м и через каждые 40-100м должны быть смотровые колодцы.

Магистральные кабели подсистемы внутренней магистрали могут прокладываться вертикально и горизонтально. Конструкции прохода горизонтальных участков совмещаются с кабельными трассами горизонтальной подсистемы. Для прохода вертикальных участков применяются стояки или шахты из соотношения 8000мм (8 на 10см ) на 2500м рабочей площади. В указанную площадь включаются все этажи, обслуживаемые кабелями, проходящими по данной трассе.

Кабельные трассы горизонтальной подсистемы, предназначены для прокладки кабеля от кроссовой этажа до рабочего места. В основной части трасса прокладывается горизонтально, но могут встречаться и вертикальные участки (подъемы под потолок, под плинтус, на пересечениях этажных пролетов). Кабели прокладываются в конструкциях пола, под потолком и в кабельных коробах (настенных каналах).

Общим требованием, предъявляемым к этим конструкциям, является необходимость заземления всех металлических элементов.

Для организации ГП и подсистемы рабочих мест (ПРМ) будем применять кабель Cat 5e S-FTP. Это экранированная витая пара с двойным экраном. Он обеспечивает защиту информации и защиту от электромагнитных излучений.

Количество патч-кордов составляет 70% от количества ИР, и из них 5-10% количество шнуров длиной 3 м. Оконечные шнуры для подключения ТА входят в комплект их поставки и в итоговую спецификацию не включаются.

$$N_{\text{пк}3} = 168 * 0,7 * 2 = 235,2 = 236 \text{ шт (длина патч-корда 3 м)}$$

$$N_{\text{пк}5} = 168 * 0,3 * 2 = 100,8 = 101 \text{ шт (длина патч-корда 5 м)}$$

#### **Расчет объема поставки горизонтального кабеля**

Расчет поставки горизонтального кабеля будем проводить эмперическим методом.

$$L_{\text{КП}} = \frac{L_{\text{max}} + L_{\text{min}}}{2} \cdot K_{\rho} + X,$$

где  $L_{КП}$  – кабельный проброс (от ИР до патч-панели);

$K_p$  – коэффициент технического запаса равен 1,1;

$X$  - запас на выполнение разделки кабеля, учитывается с обеих сторон

( $X=0,6$ м)

Чтобы определить  $L_{max}$  и  $L_{min}$  нужно учесть такие данные:

- расстояние от кроссовой до самой удаленной ИР на этаже  $x_1$ ;
- расстояние от кроссовой до самой ближней ИР на этаже  $x_2$ ;
- подъем в монтажном шкафу 3 м;
- шкаф-стена в кроссовой 1м;
- подъем для кабельного лотка в кроссовой 3 м;
- длина ввода в комнату 0,15 м;
- величина спуска в комнату 2.3 м.

$x_1$  и  $x_2$  определим из плана этажа

$x_1=34,05$  м,  $x_2=6$  м.

Тогда  $L_{max} = 3+1+2,3+0,15+34,05=34,45$  м

$L_{min} = 3+1+2,3+0,15+6=11,8$ м

$$L_{КП} = \frac{40,5 + 11,8}{2} \cdot 1,1 + 0,6 = 28,85\text{м}$$

Общее количество кабеля определяется по формуле:

$$L_{общ} = L_{КП} \cdot N_{ИР} \cdot 2,$$

где  $N_{ИР}$  – количество ИР на этаже.

2- двухпортовая ИР.

$$L_{общ} = 28,85 \cdot 168 \cdot 2 = 9694 \text{ м}$$

Общее количество кабеля для всего здания:

$$L_{общ\ кам} = 9694 \cdot 9 \cdot 2 = 174492 \text{ м}$$

$$N_{катушек} = \frac{174492}{500} = 348,98 \approx 349 \text{кат}$$

Необходимо 349 катушек кабеля по 500 м.

К коммуникационному оборудованию СКС относят: патч-панели, розетки, модули для ЛВС – RJ-45, для телефонии – RJ-11, коннекторы RJ-45, организаторы, коммутационные шнуры, организаторы для телефонного кабеля.

Патч-панели – 24 портовые 2U – 126 шт. Розетки – 2-х портовые – 1512шт. Модули RJ-45 – 1512шт. Модули RJ-11 – 1512шт.

Коннекторы RJ-45 – 6066 шт. Организаторы – 126 шт.

Коммутационные шнуры – 3033шт.

Все оборудование СКС внесено в таблицу 7.5.1.

Таблица 3.2. Спецификация оборудования кабельной системы

Тип оборудования	Количество
коммутационный шкаф 42U	16 шт
Короб 32*12,5	2646м
Короб 40*20	5278
Кабель S-FTP Cat 5e	349катушек по 500 м
Патч-панели – 24 портовые 2U	126шт
Розетки – 2-х портовые	1512 шт
Модули RJ-45	1512 шт
Модули RJ-11	1512 шт
Коннекторы RJ-45	6066 шт
Организаторы	126шт
Коммутационные шнуры	3033 шт

### 3.5. Обеспечение безопасности при работе в Internet

При организации доступа к некоторым ресурсам Internet все чаще возникает необходимость во введении некоторых ограничений. Это означает, что среди множества пользователей Internet, владелец ресурса должен определить некоторые правила определения тех, кому доступ разрешен, и предоставить им способ, с помощью которого они могли бы доказывать свою при-

надлежность к легальным пользователям. Следовательно, необходима процедура аутентификация, пригодная для использования в Internet.

Аутентификация с применением сертификатов является альтернативой использованию паролей и представляется естественным решением.

При использовании сертификатов сеть, которая дает пользователю доступ к своим ресурсам, не хранит никакой информации о своих пользователях - они ее предоставляют сами в своих запросах в виде сертификатов, удостоверяющих личность пользователей. Сертификаты выдаются специальными уполномоченными организациями - центрами сертификации. Поэтому задача хранения секретной информации (закрытых ключей) возлагается теперь на самих пользователей, что делает это решение гораздо более масштабируемым, чем вариант с использованием паролей.

Использование сертификатов основано на предположении, что сертифицирующих организаций немного, и их открытые ключи могут быть всем известны каким-либо способом, например, с помощью тех же публикаций в журналах. Когда пользователь хочет подтвердить свою личность, он предъявляет свой сертификат в двух формах - открытой, то есть такой, в которой он получил его в сертифицирующей организации, и в зашифрованной с применением своего закрытого ключа. Сторона, проводящая аутентификацию, берет из открытого сертификата открытый ключ пользователя и расшифровывает с помощью него зашифрованный сертификат. Совпадение результата с открытым сертификатом подтверждает факт, что предъявитель действительно является владельцем закрытого ключа, парного с указанным открытым.

Затем с помощью известного открытого ключа указанной в сертификате организации проводится расшифровка подписи этой организации в сертификате. Если в результате получается тот же сертификат с тем же именем пользователя и его открытым ключом - значит он действительно прошел регистрацию в сертификационном центре, является

тем, за кого себя выдает, и указанный в сертификате открытый ключ действительно принадлежит ему.

Сертификаты можно использовать не только для аутентификации, но и для предоставления избирательных прав доступа. Для этого в сертификат могут вводиться дополнительные поля, в которых указывается принадлежность его владельца к той или иной категории пользователей. Эта категория указывается сертифицирующей организацией в зависимости от условий, на которых выдается сертификат.

При использовании сертификатов отпадает необходимость хранить на серверах корпораций списки пользователей с их паролями, вместо этого достаточно иметь на сервере список имен и открытых ключей сертифицирующих организаций. Может также понадобится некоторый механизм отображений категорий владельцев сертификатов на традиционные группы пользователей для того, чтобы можно было использовать в неизменном виде механизмы управления избирательным доступом большинства операционных систем или приложений.

Механизм получения пользователем сертификата хорошо автоматизируется в сети в модели клиент-сервер, когда браузер выполняет роль клиента, а в сертифицирующей организации установлен специальный сервер выдачи сертификатов. Браузер вырабатывает для пользователя пару ключей, оставляет закрытый ключ у себя и передает частично заполненную форму сертификата серверу. Для того, чтобы неподписанный еще сертификат нельзя было подменить при передаче по сети, браузер зашифровывает сертификат выработанным закрытым ключом. Сервер сертификатов подписывает полученный сертификат, фиксирует его в своей базе данных и возвращает его каким-либо способом владельцу. Очевидно, что при этом может выполняться еще и неформальная процедура подтверждения пользователем своей личности и права на получение сертификата, требующая участия оператора сервера сертификатов. Это могут быть доказательства оплаты услуги, доказательства

принадлежности к той или иной организации - все случаи жизни предусмотреть и автоматизировать нельзя.

После получения сертификата браузер хранит его вместе с закрытым ключом и использует при аутентификации на тех серверах, которые поддерживают такой процесс.

В настоящее время существует уже большое количество протоколов и продуктов, использующих сертификаты. Например, компания Netscape Communications поддерживает сертификаты стандарта X.509 в браузерах Netscape Navigator и своих информационных серверах, а также выпустила сервер сертификатов, который организации могут у себя устанавливать для выпуска своих собственных сертификатов. Microsoft реализовала поддержку сертификатов в версии Internet Explorer 3.0 и в сервере Internet Information Server.

### **Выводы к главе 3**

При разработке программного обеспечения клиент – серверной сети выполнено:

1. Реализована сеть на топологии «многоуровневая звезда».
2. Проведена настройка терминального режима работы сервера и тонких клиентов.
3. Проведена организация внешнего доступа клиент – серверной сети
4. Выбрана спецификация активного оборудования для построения клиент – серверной сети.
5. Произведены расчеты кабельной системы, связывающая главную сеть и ее подсети
6. Обеспечение безопасности при работе в Internet с помощью сертификатов

## **Заключение**

В выпускной работе разработана клиент - серверная сеть, состоящая из главного офиса и внешнего доступа. Сеть построена на коммутированной топологии: коммутаторы доступа, распределения и ядра. Каждый сегмент сети работает по клиент-серверной архитектуре, организованной по топологии – «многоуровневая звезда. Для Главного офиса предоставлен доступ к сети Интернет по технологии ADSL 2+. Отдельные сегменты сети объединены с помощью разных технологий (ATM, ISDN, PSTN). Внутри отделов сеть построена по технологии Ethernet.

Все перечисленные решения позволяют осуществить такие преимущества:

- работа всех приложений указанных в задании ( LAN peer-to-peer traffic, Voice over IP peer-to-peer, SQL – client, File client, E-mail client, HTTP- client);
- коммутационное оборудование фирмы Cisco бесперебойно осуществляет коммутацию всей ЛВС, что позволит продолжить работу информационной инфраструктуры клиент – серверной сети;
- выход в сеть Интернет по технологии ADSL 2+ позволит иметь доступ к этой сети со скоростью 24 Мб/с;
- приведен выбор сетевой операционной системы, поддерживающей стандартные протоколы - ОС Windows Server 2003 Server R2;
- кабельная система категории 5 со стандартными разъемами RJ-45;

## Список используемой литературы

1. Каримов И.А.: Постановление Президента Республики Узбекистан «О мерах по дальнейшему внедрению развитию современных информационно-коммуникационных технологий» / Собрание законодательства Республики Узбекистан, 2012 г., № 13, стр. 139. Ташкент, 2012
2. «Компьютерные сети» В. Г. Олифер, Н. А. Олифер, 2012.
3. «Основы структурированных кабельных систем» П. А. Самарский, 2010
4. «Компьютерная сеть. Проектирование, создание, обслуживание» Штефан Науманн, Хендрик Вер, 2009.
5. Велихов А.В., Строчников К.С. Компьютерные сети. Учебное пособие по администрированию локальных сетей. 3-е издание. - Новый издательский дом, 2005 г.
6. Челлис Дж., Перкинс Ч., Стриб М. Основы построения сетей. Учебное руководство для специалистов MCSE (+CD-ROM). - Лори, 1997 г.
7. Сетевые средства Microsoft Windows NT Server 4.0 - BHV-Санкт-Петербург, 1997 г.
8. Cisco Systems. Руководство по технологиям объединенных сетей. 3-е издание. 2012г.
9. Сайты в Интернете:
  - 1). [www.company.spark.ua](http://www.company.spark.ua)
  - 2). [www.cisco.com](http://www.cisco.com)
  - 3). [www.haker.in.ua](http://www.haker.in.ua)
  - 4). [www.samsungservice.ru](http://www.samsungservice.ru)
5. Для оформления работы использовались такие приложения:
  - 1). Net Cracker Professional4.1.
  - 2).MS Visio 2002.
  - 3). AutoCAD 2008