Содержание

Введение.....2

1. Теоретические основы построения локальных сетей.....3

1.1 Моделирование структуры сети.....8

1.1.1 Особенности пакета моделирования сети Cisco Packet Tracer.....8

1.2 Выбор кабеля.....15

1.3 Адресация в сети предприятия.....16

1.4 Установка серверного оборудования.....20

1.4.1 Установка основной серверной ОС и FTP сервера.....20

1.5 Установка серверных приложений.....24

1.6 Способы доступа к узлу интернет.....30

1.7 Коммутируемый доступ.....34

1.8 Доступ по выделенной линии.....35

1.9 Разработка узла доступа в интернет.....35

2. Проектирование компьютерной сети для предприятия ООО РА «Арт-График».....45

2.1. Анализ предприятия ООО РА «Арт-График».....45

2.1.1 Описание структуры предприятия ООО РА «Арт-График».....45

2.2 Моделирование физического объекта предприятия.....47

2.3 Структура сети.....49

2.4 Проектирование доступа в интернет для предприятия.....53

2.5 Структура сети.....47

2.5.1 Оценка расходов на проектирование локальной сети.....71

Заключение.....72

Список использованных источников.....73

Введение

Рекламное агентство — это, как правило, многопрофильное предприятие, которое решает многоплановые задачи в рамках рекламного обслуживания: проводит исследование проблем, обусловливающих стратегию, тактику и концепцию рекламных кампаний, осуществляет их обоснование, детализацию и финансовый расчет, разрабатывает рекламную идею, создает рекламную продукцию, размещает ее в средствах распространения рекламы, контролирует эффективность рекламы.

Структура рекламного агентства полностью отражает цели работы агентства и объем предоставляемых им услуг. Многообразие агентств предопределяет и такое же разнообразие организационных структур каждого агентства. Однако несмотря на различия, существуют и единые общие методологические подходы к организации работы любого рекламного агентства. В крупных агентствах сильнее ощущается необходимость объединить различных специалистов в отделы и более четко разграничить сферы ответственности. Актуальность данного исследования заключается в возможности предложить модель развития информационной инфраструктуры. Важным аспектом является построение локальной сети и обеспечение скоростного доступа в глобальную сеть.

Объектом исследования является проектирование компьютерной сети.

Предметом исследования является IT-инфраструктура малого предприятия.

Для достижения поставленной цели необходимо решить следующие задачи:

- выбрать стандартную технологию для построения сети;
- подобрать сетевое оборудование;
- спроектировать схему прокладки кабеля;
- выполнить расчета экономического эффекта от создания и эксплуатацию локальной сети.

Вывод: Реализация предложенного проекта позволит сократить бумажный документооборот внутри организации, повысить производительность труда, сократить время на обработку информации.

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ

1.1 Моделирование структуры сети

Компьютерной сетью можно считать соединение двух и более компьютеров с помощью кабеля или телефонной линии и модема, при котором становится возможен обмен данными между ними. Компьютеры, расположенные в одном помещении или здании и связанные между собой, называют локальной компьютерной сетью (LAN – Local Area Network). Количество компьютеров, подключенных к такой сети, ограничивается возможностями применяемой кабельной системы и сетевого оборудования. Несколько локальных компьютерных сетей при объединении образуют кампусную сеть (CAN – Campus Area Network), например, локальные сети расположенных по соседству зданий или корпусов одного предприятия или учебного заведения. MAN (Metropolitan Area Network) – сеть уже городского масштаба, к которой могут быть подключены несколько кампусных или локальных сетей предприятий и организаций. WAN (Wide Area Network) – широкомасштабная сеть, охватывающая, например, несколько городов, область или край.

CAN (Global Area Network) – глобальная компьютерная сеть – это объединение нескольких широкомасштабных компьютерных сетей, например, в масштабе страны. И, наконец, сетью всех сетей является Интернет, в состав которого входят Всемирная Компьютерная Паутина (World Wide Web), система электронной почты и другие системы хранения и передачи информации.

Монтаж сети ЛВС на предприятии даёт следующие преимущества:

1. возможность совместного использования сотрудниками элементов ЛВС;
2. быстрый доступ к необходимой информации;
3. надёжность хранения и резервирования данных, защищённую информацию;
4. возможность использования современных технологий в повседневной работе (доступ в Интернет, электронный документооборот и т.д.)

Чтобы обеспечить стабильность работы всех имеющихся на предприятии отделов и служб, необходимо, чтобы ЛВС соответствовала определённым требованиям:

1. Эффективность (минимальные затраты при высоком качестве);
2. Возможность модернизации (при необходимости к ЛВС можно подключать дополнительное оборудование, не меняя технических или программных параметров сети);
3. Гибкость (выход из строя одного элемента сети не должен прерывать работы всей ЛВС).

Локальная вычислительная сеть, помимо самих компьютеров сотрудников, состоит из множества взаимосвязанных элементов. Это сетевые кабели, маршрутизаторы, контроллеры, панели и пульты управления.

Не существует универсальной структуры ЛВС. Каждый проект монтажа ЛВС – это эксклюзивный продукт, разрабатывающийся в соответствии с особенностями конкретного предприятия. Однако есть три основных вида структуры ЛВС.

ЛВС типа «Звезда»

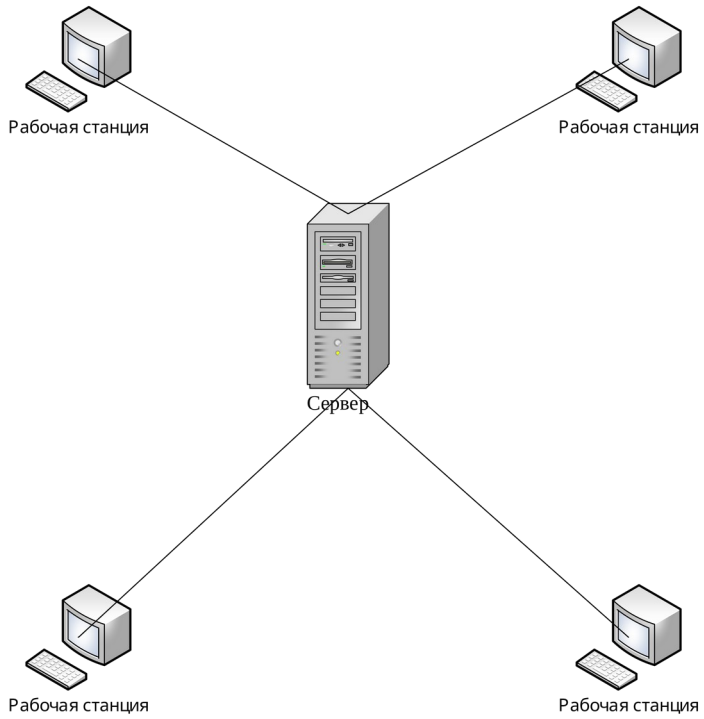


Рисунок 1.2 - Схема соединения «Звезда»

Преимущества ЛВС топологии «Звезда» заключается в том, что можно подключать к сети новые узлы, не прерывая работу остальных элементов. А единственный недостаток ощущается тогда, когда HUB выходит из строя. При этом нарушается работоспособность всей ЛВС. Возможность подключать новые станции, не прерывая работу всей системы, а также

относительно низкая себестоимость данного вида ЛВС обеспечили такой системе популярность.

ЛВС типа «Кольцо»

При такой структуре ЛВС все компьютеры связаны между собой последовательно. Сигнал передаётся в одном направлении по кольцу, при этом каждый компьютер играет роль усилителя. Недостаток такой структуры – сравнительно низкая скорость передачи данных от одного компьютера к другому, а также нарушение работы всей ЛВС при поломке хотя бы одного подключенного к ней компьютера.

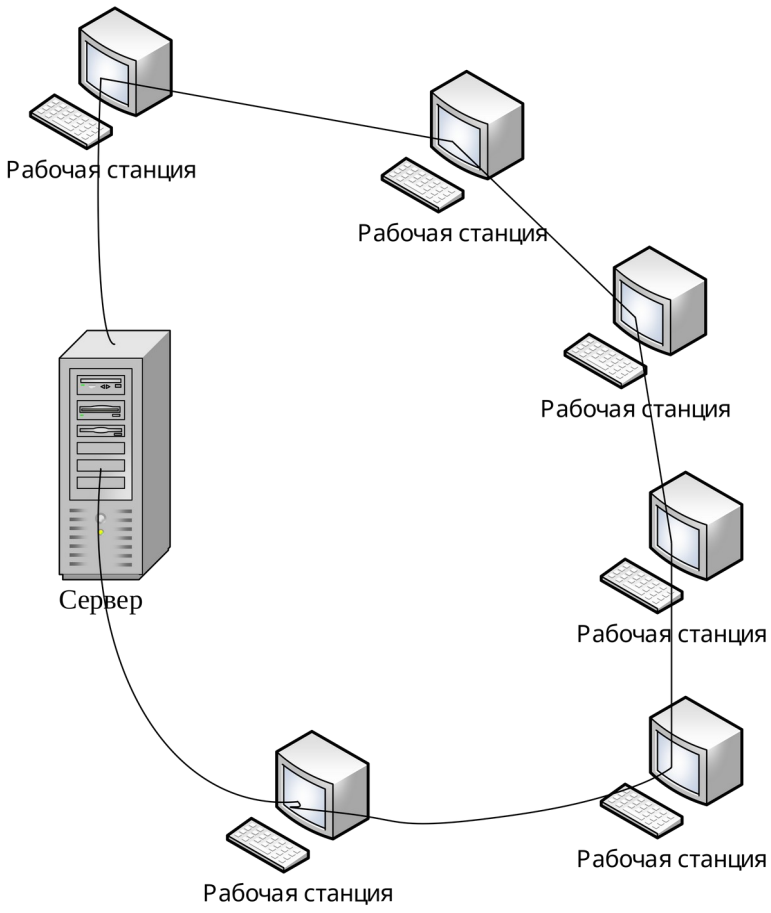


Рисунок 1.3 - Схема соединения «Кольцо»

При «шинной» топологии ЛВС каждый компьютер подключается к общему кабелю – шине передачи данных. Основной недостаток – зависимость связи всех компьютеров от одного кабеля. Когда ЛВС проектируется по такой топологии, необходимо обеспечить неуязвимость шины, на этой составляющей экономить нельзя. Кроме того, если возникает

необходимость подключить новый компьютер, на время монтажных работ связь компьютеров через ЛВС также придётся прерывать.[3]

Монтаж древовидной компьютерной сети

Несмотря на то, что в каждой топологии ЛВС есть свои недостатки, можно реализовать проект, который будет полностью соответствовать индивидуальным требованиям предприятия. В сложных многоуровневых ЛВС, как правило, используется не одна топология. Так, например, компьютеры отдела бухгалтерии соединяются между собой по типу «Звезда», компьютеры отдела закупок подключены последовательно, а все ПК двух отделов подключаются к общей шине. Такая топология называется древовидной. При этом компьютеры каждого отдела (или этажа) могут иметь отдельный сервер. Разделение всех компьютеров, входящих в ЛВС, по древовидной топологии – решение, обеспечивающее удобное администрирование всей системы.

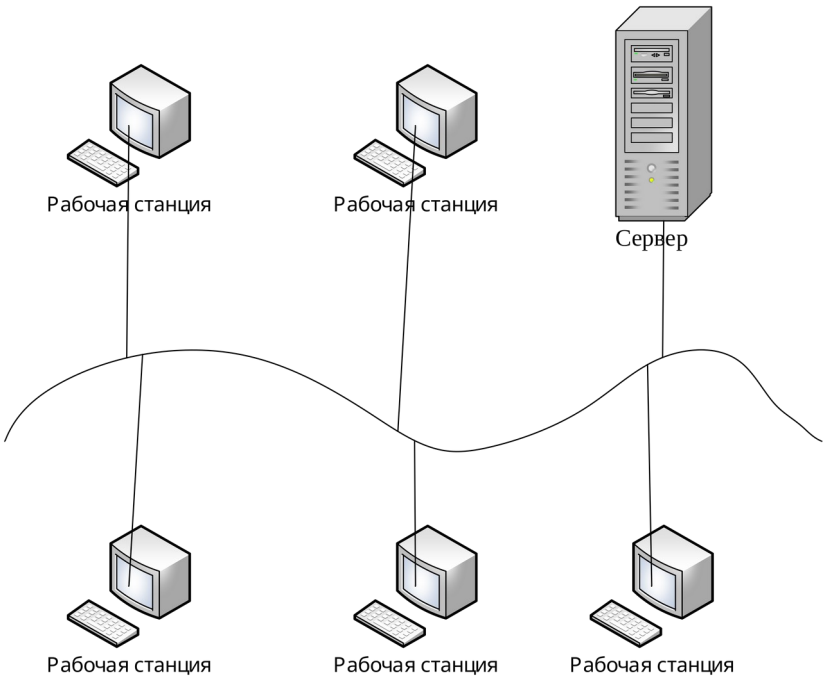


Рисунок 1.4 - Схема соединения «Шина»

Современные же технологии позволяют организовать работу предприятия на основе беспроводной сети (WiFi). В этом случае все вышеперечисленные недостатки организации сетевой инфраструктуры исключаются. Единственной проблемой организации беспроводной сети на предприятии может быть особое физическое расположение компании (например, вблизи защищённых государственных правительственных

объектов), когда использование беспроводной радиосвязи запрещено или ограничено.

Вне зависимости от выбранного способа организации локальной вычислительной (компьютерной) сети, необходимо учитывать, что работоспособность, функциональность, безотказность ЛВС зависят не только от топологии, но и от надёжности оборудования, на основе которого будет строиться сеть, и от квалификационного уровня специалистов, занимающихся монтажом и настройкой ЛВС. Это очевидно, что монтаж и должны проводиться компетентными специалистами.

1.3 Обзор и анализ сетевого оборудования и операционных систем

1.3.1 Обзор сетевых кабелей и компонентов кабельной системы

Для локальных сетей существует три принципиальные схемы соединения: с помощью витой пары, коаксиального или волоконно-оптического кабеля. Для передачи информации так же могут использоваться спутники, лазеры, микроволновое излучение и т.п., но подобная экзотика выходит за область рассмотрения этого курсового проекта.

1.3.2 Витая пара

Витая пара в настоящее время является самой распространённой средой передачи и представляет собой пару свитых проводов. Кабель, составленный из нескольких витых пар, как правило, покрыт жёсткой пластиковой оболочкой, предохраняющей его от воздействия внешней среды и механических повреждений. Схема витой пары представлена на рис. 2.1

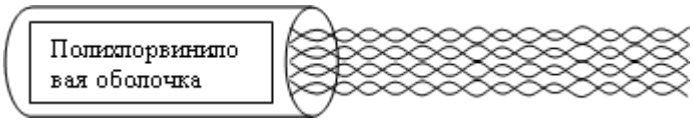


Рисунок 2.1. Кабель из витых пар

В нормальных условиях витая пара поддерживает скорость передачи данных от 10 до 100 Мбит/с. Однако ряд факторов может существенно снизить скорость передачи данных, в частности, потеря данных, перекрёстное соединение и влияние электромагнитного излучения.

Для уменьшения влияния электрических и магнитных полей применяется экранирование (кабель из витых пар покрывается фольгой или оплёткой). Но после экранирования витой пары в значительной степени увеличивается затухание сигнала. Под затуханием сигнала подразумевается его ослабление при передаче из одной точки сети в другую. Экранирование изменяет сопротивление, индуктивность и ёмкость таким образом, что линия становится склонной к потере данных. Подобные потери могут сделать витую пару нежелательной и ненадёжной средой передачи. И экранированная, и неэкранированная витая пара используется для передачи данных на несколько сотен метров.

В соответствии со спецификациями ассоциации электронной и телекоммуникационной промышленности вводится пять стандартных категорий кабеля из витых пар. При определении категорий кабеля используется только неэкранированная витая пара (UTP).

- Кабель первой категории используется для передачи голосовых данных. С начала 80-х годов кабель CAT 1 используется в основном в качестве проводки телефонных линий. Кабель первой категории не сертифицирован для передачи данных любого типа и в большинстве случаев не рассматривается как среда для передачи цифровых данных.

- Кабель второй категории используется для передачи информации со скоростью не более 4 Мбит/с. Этот тип проводки характерен для сетей устаревшей сетевой топологии, использующих протокол с передачей маркера. Кабель тактируется частотой 1 Мгц.

- Кабель третьей категории в основном используется в локальных сетях с устаревшей архитектурой Ethernet 10base-T и сертифицирован для передачи данных со скоростью до 16 Мбит/с. Кабель тактируется частотой 16 МГц.

- Кабель четвёртой категории используется в качестве среды соединения сетей с кольцевой архитектурой или архитектурой 10base-T/100base-T. Кабель CAT 4 сертифицирован для передачи данных со скоростью до 16Мбит/с и состоит из четырёх витых пар. Тактируется частотой 20 МГц.

- Кабель пятой категории является самой распространённой средой передачи для Ethernet. Кабель поддерживает скорость передачи данных до 100Мбит/с и используется в сетях с архитектурой 100base-T и 10base-T. Кабель тактируется частотой 100 МГц.

1.3.3 Коаксиальный кабель

Коаксиальный кабель является широко распространённой и достаточно удобной средой передачи данных. Такое название кабель получил вследствие того, что состоит из двух проводников. Один проводник (цельная или витая жила) экранируется вторым, который тоже может быть сплошным или переплетённым. Проводники, как правило, разделены слоем диэлектрического материала. Сам кабель покрыт пластиковой оболочкой. Коаксиальный кабель лучше защищён от помех и позволяет увеличить длину сегмента сети. Использующие коаксиальный кабель сети стандартов 10base-2 приблизительно 180 м. На рис. 2.2 и 2.3 показан коаксиальный кабель в разрезе.

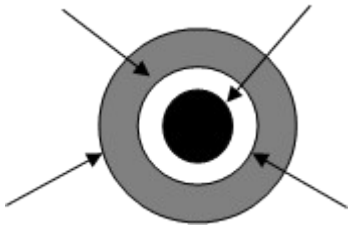


Рисунок 2.2. Сечение коаксиального кабеля.

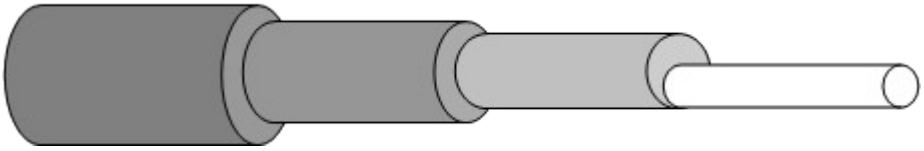


Рисунок 2.3. Продольный разрез коаксиального кабеля.

С увеличением диаметра коаксиального кабеля пропускная способность повышается. Однако одновременно с этим увеличиваются затраты на выполнение проводки из такого кабеля, поскольку необходимо использовать специальные инструменты. Характерные свойства коаксиального кабеля:

- Он менее подвержен влиянию шума по сравнению с витой парой.

- Кабель состоит из двух концентрических проводников, разделённых слоем диэлектрического материала.

- Импеданс коаксиального кабеля может быть равен 75 Ом (кабель толщиной ½ дюйма) или 50 Ом (кабель толщиной 3/8 дюйма).

1.3.4 Волоконно-оптический кабель

Это тонкая и гибкая среда, позволяющая передавать данные в виде световых волн по стеклянному «проводнику» или кабелю. Волоконно-оптические линии связи используются на расстояниях свыше одного километра. Характерной их особенностью является высокая защищённость от несанкционированного подключения (что не удивительно, поскольку для передачи данных не используются электрические сигналы). Существует две разновидности кабеля: одномодовый и многомодовый.

Устройство волоконно-оптического кабеля

Коаксиальный и волоконно-оптический кабель устроены почти одинаково. Сердечник последнего состоит из сплетения тонких стеклянных волокон и

заключён в пластиковую оболочку, отражающую свет обратно к сердечнику. Плакирование покрыто концентрическим защитным слоем пластика. На рис. 2.4 показано устройство волоконно-оптического кабеля.

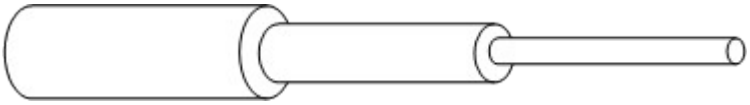


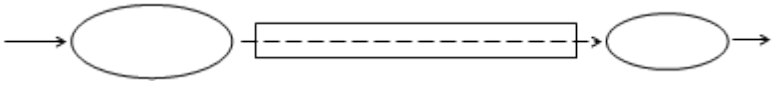
Рисунок 2.4. Волоконно-оптический кабель

Все данные в компьютере представляются с помощью нулей и единиц. Все стандартные кабели передают бинарные данные с помощью электрических импульсов. И только волоконно-оптический кабель, используя тот же принцип, передаёт данные с помощью световых импульсов. Источник света посылает данные по волоконно-оптическому «каналу», а принимающая сторона должна преобразовать полученные данные в необходимый формат (см. рис. 2.5).

Одномодовый и многомодовый кабель

В относительно тонком волоконно-оптическом канале свет будет распространяться вдоль продольной оси канала. В учебниках физики этот эффект упоминается в следующей формулировке – «импульсы света распространяются в осевом (аксиальном) направлении». Именно это и происходит в одномодовом кабеле (см. рис. 2.6).

Однако преимущества этого типа передачи ограничены. С целью устранения подобных ограничений стали выпускать подобный кабель. Но тут возникла другая проблема – лучи света имеют свойство входить в канал под различными углами волны проходят различное расстояние и прибывают к получателю в разное время. Этот эффект, проиллюстрированный на рис. 2.7, получил название модальной дисперсии.



Источник света Волоконно-оптический кабель Приёмник 1

Рисунок 2.5. Принцип работы волоконно-оптического кабеля.

Оболочка Плакирование

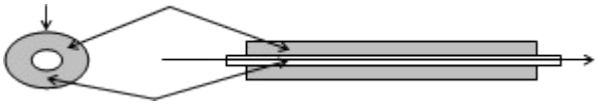


Рисунок 2.6. В тонком кабеле свет распространяется по одномодовому пути

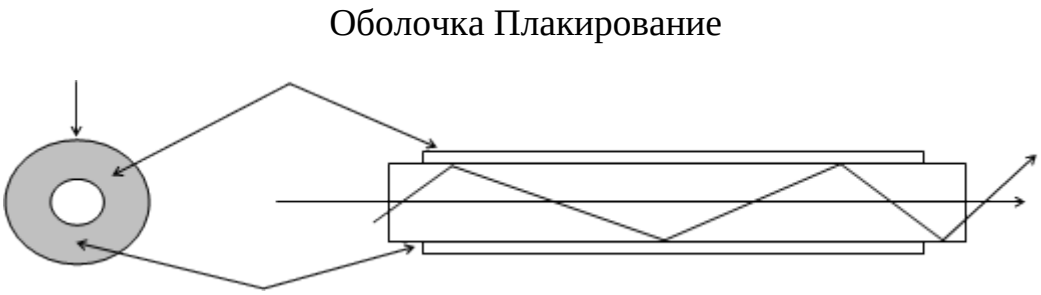


Рисунок 2.7. В толстом кабеле неаксиальные лучи подвержены модальной дисперсии

Чем больше количество мод света в канале, тем уже полоса пропускания. В дополнение к тому, что различные импульсы достигают получателя практически одновременно, усиление дисперсии приводит к наложению импульсов и введению получателя в «заблуждение». В результате снижается общая пропускная способность. Одномодовый кабель передаёт только одну моду световых импульсов. Скорость передачи данных при этом достигает десятков гигабит в секунду. Одномодовый кабель в состоянии поддерживать несколько гигабитных каналов одновременно, используя для этого световые волны разной длины. Следовательно, пропускная способность многомодового волоконно-оптического кабеля ниже, чем у одномодового.

Простейший способ уменьшения дисперсии – нивелирование волоконно-оптического кабеля. В результате лучи света синхронизируются таким образом, что дисперсия на стороне приёмника уменьшается. Дисперсия также может быть уменьшена путем ограничения количества длин световых волн. Оба метода позволяют в некоторой степени уменьшить дисперсию, но не в состоянии привести скорость передачи данных в соответствие с одномодовым волоконно-оптическим кабелем.

В США широко используется многомодовый волоконно-оптический кабель 62.5/125. Обозначение «62.5» соответствует диаметру сердечника, а обозначение «125» – диаметру плакирования (все величины приведены в микронах). Из одномодовых распространены кабели с маркировкой 5-10/125. Ширина полосы пропускания обычно приводится в МГц/км. Хорошей моделью взаимоотношений полосы пропускания и дальности передачи служит резиновый жгут – с увеличением расстояния полоса пропускания сужается (и наоборот). В случае передачи данных на расстояние 100 метров полоса частот многомодового кабеля составляет 1600 Мгц при длине волны 850 нм. Аналогичная характеристика одномодового кабеля составляет приблизительно 888 ГГц.

Основные характеристики волоконно-оптического кабеля:

- Абсолютный иммунитет к электромагнитным излучениям.

- Возможна передача данных на расстояние до 10 км.

- В лабораторных условиях реально достичь скорости передачи до 4 Гбит/с.

- В качестве источника света может использоваться светоизлучающий диод или лазер.

1.3 Адресация в сети предприятия

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

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

Выделение диапазона адресов осуществляется бесплатно, но организация получившая адреса, должна реально подтвердить их использование через определённый промежуток времени.

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

Групповые адреса

Если данные должны быть переданы на несколько устройств (например, просмотр видео с одной Web-камеры на различных компьютерах или одновременное разворачивание образа операционной системы на несколько систем), то уменьшить нагрузку на сеть может использование групповых рассылок.

Для этого компьютеру присваивается еще один IP-адрес из специального диапазона: с 224.0.0.0 по 239.255.255.255, причем диапазоны 224.0.0.0— 224.0.0.255 и 239.0.0.0—239.255.255.255 не могут быть использованы в приложениях и предназначены для протоколов маршрутизации3 и т. п. Назначение адресов групповой рассылки производится соответствующим программным обеспечением.

Если коммутатор имеет функции работы с групповыми рассылками (поддержка IGMP snoophing, P1M DM/PIM SM), то передаваемые на адреса групповой рассылки данные будут поступать только на те порты, к которым подключены устройства, подписавшиеся на соответствующие рассылки. В результате сетевой трафик может быть существенно снижен по сравнению с вариантом передачи таких данных каждому устройству сети независимо.

Распределение IP-адресов сети малого офиса

В сетях предприятий обычно задействованы диапазоны IP-адресов, выделенные для локального использования. Часть адресов закрепляется статически, часть — раздается динамически с помощью DHCP (Dynamic Host Configuration Protocol, динамический протокол конфигурации сервера).

Статические адреса закрепляются:

1. за шлюзом, для которого обычно используют адрес xxx.xxx.xxx.1, но это традиция, а не правило;
2. за серверами DNS, DHCP, WINS;
3. за контроллерами домена;
4. за серверами сети (например, централизованные файловые ресурсы, почтовый сервер и т. п.);
5. за станциями печати, имеющими непосредственное подключение к сети;

6. за управляемыми сетевыми устройствами (например, сетевыми переключателями, SNMP-управляемыми источниками аварийного питания и т. п.).

Рабочие станции традиционно используют динамические адреса. При этом часть динамических адресов выдается для локального использования, а часть предназначается для внешних клиентов, "гостей" сети.

Большинство сетевых устройств (роутеров) выдают ip адрес из сети 192.168.0.1/24. В этом примере значение до косой черты — это ip адрес, после — маска сети. Существует таблица масок сети, составленная для удобства инженера, она приведена в таблице 2.2, а Маска «24» сообщает нам о том, что в сети 192.168.0.1 может находиться 254 хоста. В случае если нам нужно меньше или больше хостов в одной сети и можно применить маску.

Таблица 2.2 – Таблица адресов

СЕТЬ	МАСКА	КОЛ-ВО ХОСТОВ	BROADCAST
192.0.0.8	255.0.0.0 (8)	16777214	192.255.255.255
192.168.0.0	255.255.0.0(16)	65534	192.168.255.255
192.168.0.0	255.255.240.0(20)	4094	192.168.15.255
192.168.0.0	255.255.248.0(21)	2046	192.168.7.255
192.168.0.0	255.255.252.0(22)	1022	192.168.3.255
192.168.0.0	255.255.254.0(23)	510	192.168.1.255
192.168.0.0	255.255.255.0(24)	254	192.168.0.255
192.168.0.0	255.255.255.128(25)	126	192.168.0.127
192.168.0.0	255.255.255.192(26)	62	192.168.0.63
192.168.0.0	255.255.255.224(27)	30	192.168.0.31
192.168.0.0	255.255.255.240(28)	14	192.168.0.15

192.168.0.0	255.255.255.248(29)	6	192.168.0.7
192.168.0.0	255.255.255.252(30)	2	192.168.0.3
192.168.0.0	255.255.255.254(31)	2	—
192.168.0.0	255.255.255.255(32)	1	—

В нашей сети будет несколько сегментов. Предположим, что у нас в офисном здании работает около сотни работников. Для такого количества пользователей, находящихся в 11 помещениях, нам достаточно 254 хоста. Среди трех сегментов сети разделим сеть на две части по 127 хостов, отдел материально-технического обеспечения и сеть инженерного отдела необходимо определить в одну группу хостов. Таблица коммутации сети представлена в приложении 2.

1.4 Установка серверного оборудования

1.4.1 Установка основной серверной ОС и FTP сервера

FTP-сервер

Gene6 FTP Server - один из лучших FTP-серверов с расширенным администрированием и высоким уровнем безопасности передаваемых данных. Программа позволяет открывать доступ к данным для конкретных пользователей или групп пользователей через их учетные записи, управлять правами доступа для файлов и каталогов и ограничивать доступ по IP-адресам. При этом может быть создано нескольких виртуальных узлов FTP и ограничено число соединений (для IP, домена, пользователя), а также установлены сроки действия учетных записей. Предусмотрена и возможность более тонкой настройки прав доступа конкретных пользователей, для которых несложно, например, определить максимальный размер закачиваемых на FTP-сервер файлов, сделать какие-то файлы в открытой папке заблокированными или наоборот, доступными, определить лимиты скорости при скачивании и закачивании файлов, установить интервалы времени доступности FTP-сервера и т.д. Имеется поддержка ODBC баз данных, возможно сжатие передаваемых данных (MODE Z), а для

обмена важными файлами может использоваться 128-битное SSL-шифрование. В реальном времени ведется подробная статистика активности на FTP-сервере, записываемая в log-файлы и визуально отображаемая в текстовом и графическом виде.

Предусмотрены средства удаленного администрирования, позволяющие добавлять, изменять, удалять учетные записи пользователей, а также изменять все доступные настройки доменов удаленно (как если бы администратор находился у компьютера, на котором запущен сервер). Существует возможность делегировать администрирование другому администратору посредством создания новой учетной записи пользователя с ограниченными правами администратора. Подключение удаленного администрирования шифруется при помощи SSL и запускается на собственном настраиваемом порте.

Программа (имеется русскоязычная версия) представлена в двух редакциях: Standard и Professional.

Программа включает два модуля - движок FTP-сервера и FTP-Администратор. Движок FTP-сервера работает как системная служба (то есть автоматически запускается при загрузке Windows), интерфейса не имеет и отвечает за включение/отключение сервера, FTP-Администратор обеспечивает доступ к настройкам сервера и запускается через меню Пуск. Значок FTP-сервера всегда находится в системном трее, и по виду этого значка несложно понять, когда сервер включен, когда отключен, и когда на него зашел какой-нибудь пользователь.

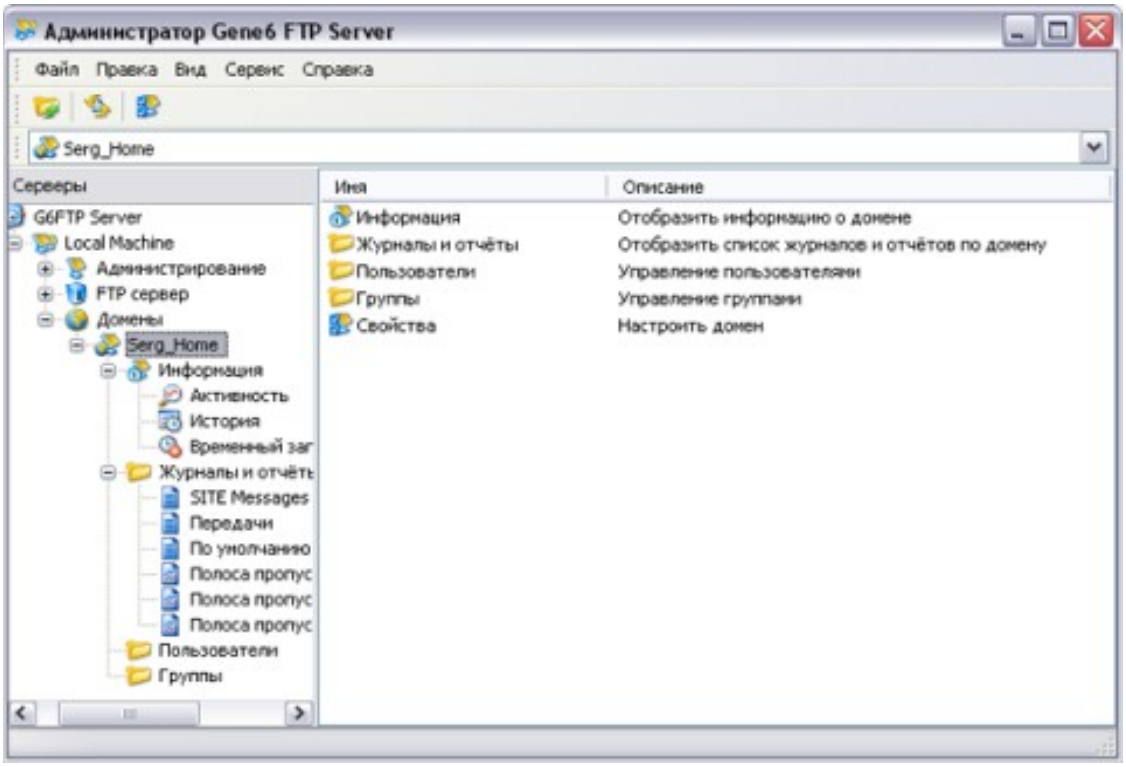


Рисунок 2.9 – Интерфейс Gene6 FTP Server

Установка Windows Server 2008 R2

Операционная система Windows Server 2008 предоставляет системному администратору широкий набор инструментов для решения задач управления. Основными из этих инструментов являются следующие:

• консоль управления (Microsoft Management Console, MMC);

• мастера (Wizards);

• утилиты командной строки.

Консоль управления MMC2 представляет собой унифицированную среду для выполнения административных задач. Администратор, имея в распоряжении такую среду, может помещать в неё одну или несколько утилит, называемых оснастками (snap-in), для решения текущей проблемы. Консоль управления позволяет одинаково отображать любые оснастки и использовать для управления ими похожие приемы. Таким образом, смысл применения консоли управления в том, чтобы сделать среду выполнения административных утилит единообразной и удобной. С той же целью в Windows Server 2003 применяются мастера. Мастер представляет собой программу, которая проводит администратора по всем этапам решения какой-либо задачи. На каждом этапе возможен выбор одного или нескольких

способов решения или параметров настройки. Часто также мастера предоставляют возможность выбора параметров по умолчанию.

Использование мастеров позволяет сократить время установки и настройки компонентов операционной системы или время решения другой административной задачи. Кроме того, параметры по умолчанию чаще всего обеспечивают вполне работоспособный режим, хотя, возможно, и не самый эффективный. Утилиты командной строки являются самыми старыми инструментами администрирования, ведущими свою историю от первых операционных систем без графического интерфейса. В то время альтернативы утилитам командной строки не было. Сегодня большинство задач управления можно решить без использования утилит, однако многие администраторы считают, что утилиты командной строки удобнее графического интерфейса.

Кроме того, такой вид утилит, как утилиты диагностики стека протоколов TCP/IP, не имеют стандартного графического аналога (эти утилиты рассматриваются во второй лекции). Большинство административных задач возможно решить, используя любой из представленных инструментов – консоль управления, мастер или утилиту командной строки. Выбор инструмента обусловливается, в основном, личными предпочтениями системного администратора. Интерфейс Windows Server 2008 представлен на рисунке 2.9

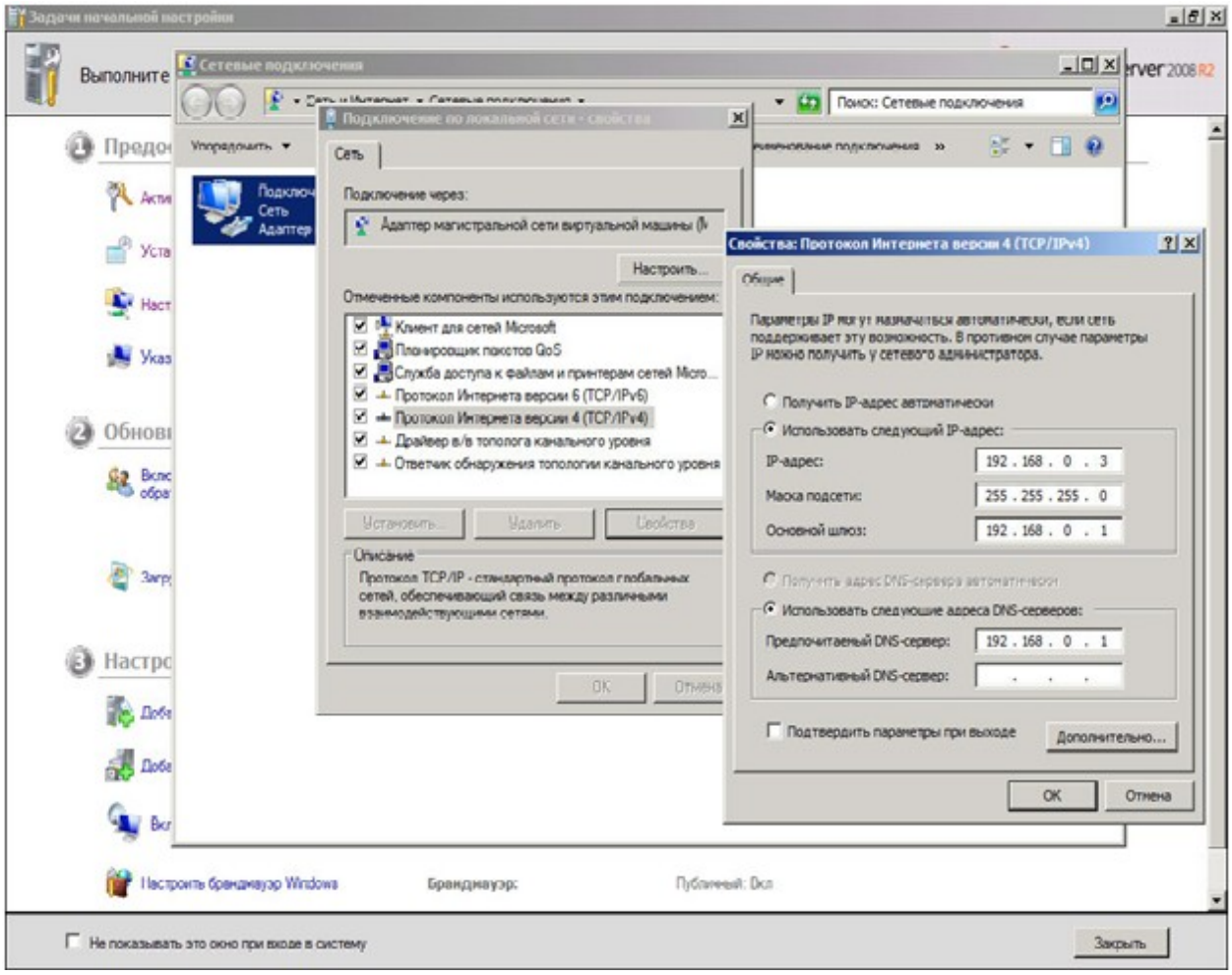


Рисунок 2.10 – Windows Server 2008 R2

1.6 Способы доступа к узлу интернет

Описание узла Интернет начинается с описания основных сервисов, которые он будет предоставлять, затем производится описание основных модулей узла, которые реализуют ту или иную услугу, и в итоге предоставляется обоснование выбора конкретной аппаратной или программной платформы для каждого функционального модуля.

Описание услуг

При планировании входа на рынок услуг предлагается начать с предоставления базовых услуг по предоставлению доступа в сеть Интернет, и затем постепенно вводить дополнительные услуги, такие как VoIP, web-hosting, colocation, и двигаться, таким образом, в сторону контент-провайдинга. Базовые услуги будут обеспечивать стабильный доход

компании, а дополнительные доходы позволят создать центры генерации прибыли.

Базовые услуги

Базовые услуги провайдера — это фундамент его развития, как в плане наращивания его технических мощностей, так и в плане увеличения клиентской массы. Набор базовых услуг провайдера обязательно должен быть не хуже, чем у других операторов рынка, поскольку выбор клиента во многом зависит от ассортимента стандартных услуг, предлагаемых провайдером.

В настоящее время таким набором услуг Интернет-провайдера являются: Коммутируемый доступ в сеть Интернет

1. Доступ в Интернет по выделенной линии
2. Электронная почта
3. Электронные новости
4. Размещение персональной странички в Интернет
5. Регистрация доменного имени

Дополнительные услуги

Одной из самых популярных дополнительных услуг среди Интернет-провайдеров является в настоящее время услуга Интернет-телефонии. Клиентам этой услуги предоставляется возможность совершать междугородние и международные звонки по существенно более низким тарифам, по сравнению с тарифами обычных операторов. Успешное внедрение различных методов оплаты напрямую зависит от правильного выбора платформы биллинга (автоматизированной системы расчетов) услуг Интернет-телефонии и здесь необходимо уделить особенное внимание вопросам интеграции уже используемых АСР с АСР, обслуживающей комплекс устройств VoIP.

Не менее популярны и услуги, связанные с размещением web-серверов клиентов на территории провайдера. Эти услуги подразделяются, как правило, на два класса: размещение виртуальных серверов (web-hosting) и размещение физических серверов (co-location).

Кроме этих, широко распространенных дополнительных услуг можно предложить внедрение новых, совершенно не представленных на московском и российском рынках. Эти услуги базируются на гибкости предлагаемого оборудования узла: Услуги по организации и управлению политиками

безопасности сетей клиентов Услуги по защите от всплесков трафика Услуги по гарантированному предоставлению определенного уровня качества сервиса, предоставлению временных дополнительных мощностей во время периодов пиковой нагрузки Услуги по динамической репликации

Также в качестве перспективной услуги можно рассматривать создание виртуальных частных сетей клиентов.

Региональный оператор Интернет имеет иерархическую структуру узлов Интернет, состоящую из центрального узла и узлов операторов. Центральный узел предоставляет услуги не только своим абонентам, но и периферийным компаниям – провайдерам.

Типовой узел оператора выполняет следующие функции:

1. Обеспечение доступа абонентов к сети Интернет через коммутируемые и выделенные линии,
2. Предоставление возможности использования сервеа электронной почты, сервера новостей, сервера FTP и сервера WWW типового узла,
3. Предоставление абонентам возможности регистрации собственных доменов второго или третьего уровня с использованием для поддержагния домена сервера DNS типового узла,
4. Проверка и санкционирование доступа абонентов к различным информационным ресурсам (IP соединению, электронной почте, новостям, FTP, WWW и т.п.),
5. Регистрация событий – попыток получения абонентами IP соединения и доступа к информационным ресурсам,
6. Контроль информационной безопасности,
7. Начисление оплаты за используемые абонентом информационные ресурсы,
8. Маршрутизация трафика между центральным узлом, службами и пользователями.

Структура типового узла интернет представлена на рисунке 3.1

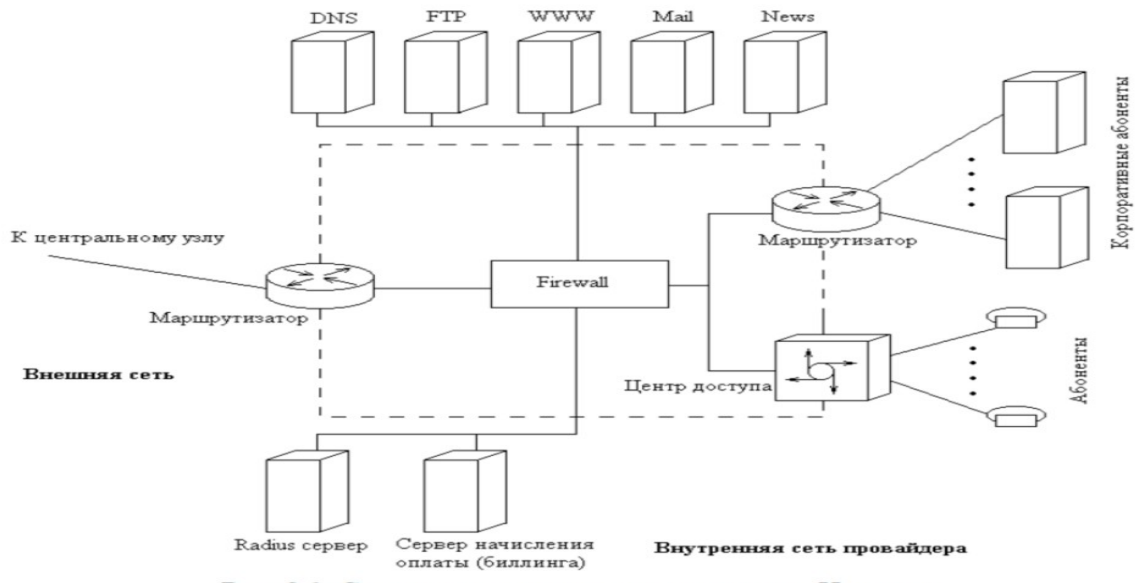


Рисунок 3.1 - Структура типового узла интернет

В основу функциональной схемы положено разделение на внешние (незащищѐнные) и внутренние (защищѐнные) сети, для чего предлагается использование межсетевого экрана Firewall.

Разделение требуется по следующим причинам:

1. Необходимо защитить внутреннюю локальную сеть провайдера со стороны Интернет;
2. Необходимо защитить серверы провайдера (DNS, WWW, FTP, Mail, News и т.д.) как со стороны Интернет, так и со стороны своих абонентов, предоставив в то же время возможность санкционированного доступа к серверам для получения услуг;
3. Необходимо предоставить своим абонентам некоторый уровень защиты от несанкционированного вмешательства в их работу со стороны Интернет.

Основным устройством для построения узла Интернет является маршрутизатор доступа.

При выборе маршрутизатора доступа первоочередное внимание следует обращать на такие факторы, как надежность, управляемость, расширяемость, гибкость, спектр предлагаемых технологий и поддерживаемые протоколы. Для построения узла Интернет можно использовать продукты компаний 3Com, Advanced Computer Communications, Cisco Systems, Xyplex, IBM, группы сетевых продуктов Digital Equipment, Bay Networks, Compatible Systems и TimePlex.

Свой выбор, скорее всего, придется ограничить одним поставщиком, и отнюдь не из-за проблем совместимости. Заставить работать вместе продукты различных производителей - задача вполне решаемая. Однако конфигурация - вот что почти наверняка заставит ограничиться одним поставщиком. Как правило, каждый производитель исповедует свой собственный подход к конфигурации маршрутизаторов. Это касается различий не только в командах и графическом интерфейсе, но и в самой концепции и терминологии.[6]

1.7 Коммутируемый доступ

Основным и наиболее доступным способом соединения с сетью Интернет является "доступ по коммутируемому соединению", или "dial-up access". Он использует в качестве среды передачи данных уже существующие каналы связи - телефонную сеть общего пользования. (Рисунок 3.2)

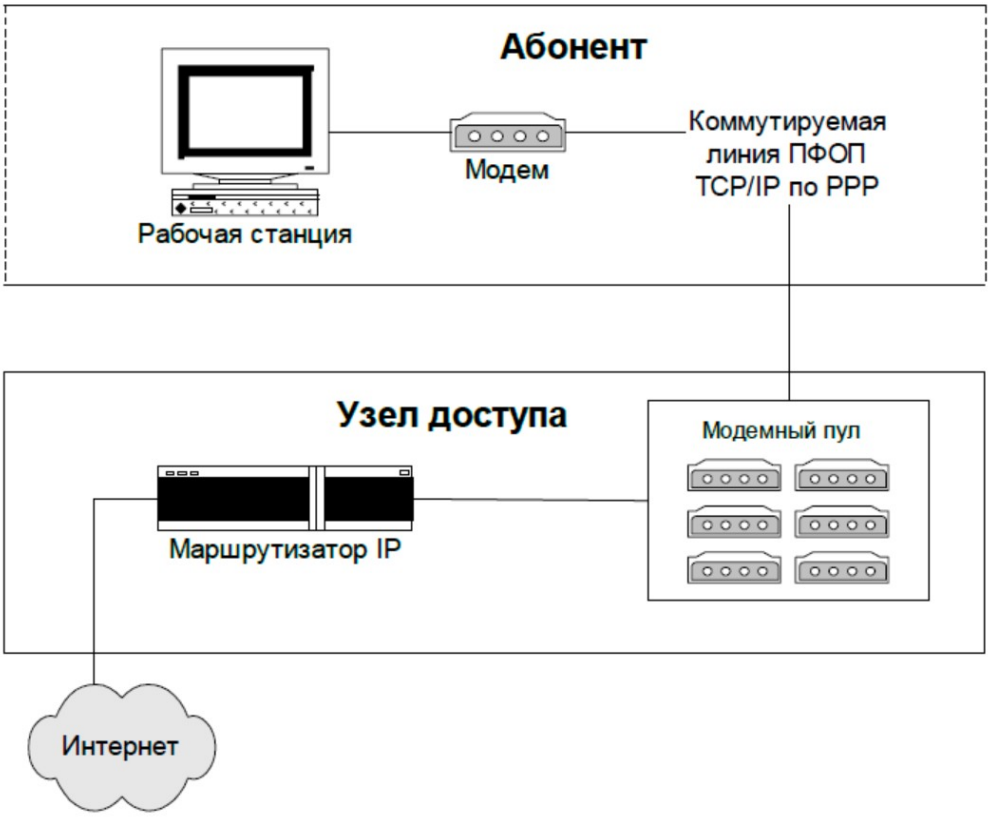


Рисунок 3.2 - Схема коммутируемого доступа через модем

Канал связи между провайдером и клиентом устанавливается при помощи коммутирующего оборудования АТС. Перед началом работы необходимо установить соединение, а после окончания работы разорвать. Пользователю разрешается вести передачу в полосе частот 300Гц-3400Гц, то есть на частоте передачи голоса. Всѐ остальное отсекается на АТС полосовым фильтром. Коммутируемый канал обеспечивается телефонной сетью. Он может быть устроен самыми разными способами и обеспечивает связь на любые расстояния. То есть, коммутируемый канал - это некий интерфейс, предоставляемый

пользователю телефонной сетью и обеспечивающий заданные параметры сигнала (уровень, полосу, отношение сигнал/шум). Средства же, которыми происходит доставка сигнала между абонентами, от пользователя скрыты.

1.8 Доступ по выделенной линии

Следующим по значимости способом соединения с Интернет является доступ по —выделенной линии", или "leased line". В качестве среды передачи данных также используется телефонная сеть общего пользования. В отличие

от коммутируемой линии выделенная всегда готова к работе (не требуется время на установление соединения). Возможно построение выделенной линии тональной частоты, но на практике такой вариант не используется. Таким образом, выделенная линия - непосредственное электрическое соединение посредством одной или нескольких пар медного кабеля диаметром от 0,4мм и выше в обход коммутационной аппаратуры АТС. Поэтому еѐ часто называют физической линией. Скорость и дальность связи по выделенной линии полностью определяются ее электрическими характеристиками. (Рисунок 3.3)

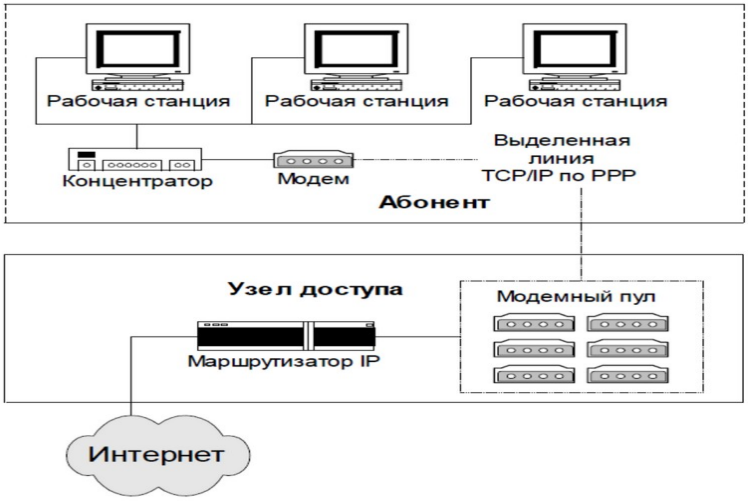


Рисунок 3.3 - Выделенный кабель

1.9 Разработка узла доступа в интернет

Организация интернет-доступа.

Организация доступа в Интернет на современном предприятии это не просто установка маршрутизатора. Для обеспечения непрерывных и качественных бизнес-процессов в компании необходимо настроить подключение внутренней офисной сети к провайдерам Интернета с использованием различных каналов и протоколов передачи данных. Нужно сразу задуматься о том, как организовать доставку трафика клиент-банков, IP-телефонии, почтового сервера, баз данных и сайтов. Будут ли работать пользователи напрямую, через прокси-сервер и в чем отличие. Потребуется ли хождение внешнего трафика внутрь сети, если кто-то из сотрудников работает через VPN с домашнего компьютера или из командировки. Если используется служба доменов Active Directory, то логично ее использовать в целях аутентификации пользователей для интернет-доступа. Нужны резервирование каналов, публикация веб-сервисов или почтовых служб,

расширенная маршрутизация, портмаппинг, приоритезация и много других умных слов.

Прямой доступ. Работа через NAT.

Самым простым и надежным способом подключения внутренних компьютеров к всемирной паутине является NAT – трансляция адресов и портов наружу при прохождении трафика через шлюз. В этом случае каждый компьютер в сети работает напрямую, служба NAT прозрачно транслирует во внешнюю сеть все его запросы. Это самый универсальный способ предоставления доступа в Интернет, когда не нужно дополнительно настраивать программы, а Интернет как бы «сразу есть» на любом компьютере. Traffic Inspector помогает настроить службу NAT для Microsoft Windows, а также может быть установлен на уже настроенную сеть. Достаточно создать пользователей (либо подключить их из домена) и выбрать способ их авторизации.

Работа через прокси-сервер.

Другой способ доступа в Интернет – через прокси-сервер. В этом случае все запросы транслируются сервером на уровне протоколов приложений и требуют поддержки клиентских программ. Прокси-сервер в Traffic Inspector поддерживает все необходимые протоколы и может работать через HTTP, HTTPS, FTP и SOCKS. Есть возможность использовать «прозрачный» режим работы с сайтами, когда настройка клиентских браузеров не производится, но все веб-запросы все равно проходят через прокси-сервер. Преимущества работы через прокси-сервер состоят в возможности кэширования посещаемых ресурсов и блокировке элементов сайта (баннеров, мультимедиа, видео, флеш и т.д.). Для комфортной работы в Интернете и надежного контроля трафика рекомендуется использовать совместный доступ: прокси-сервер для сайтов и NAT для других служб. [7]

Способы аутентификации. Active Directory и VPN.

Использование Traffic Inspector подразумевает создание для каждого пользователя отдельной учетной записи. Если домен уже настроен учетные записи пользователей можно подгрузить из Active Directory.

Traffic Inspector позволяет идентифицировать клиента разными способами: по имени и паролю, через домен, по IP и MAC, VLAN и через VPN. Контроль трафика осуществляется по всем пользователям, а доступ и ограничения

могут быть настроены по группам, например, разделив сотрудников и руководство.

Специально для идентификации пользователя создана удобная программа-агент, которая упрощает авторизацию и служит для отображения баланса и расходов трафика и управления экономией (персональной фильтрацией и кэшированием на прокси-сервере). Пользователи также могут использовать веб-вариант этого агента. В этом случае его не нужно устанавливать – он сможет работать на любой операционной системе через браузер.

В 90-х годах прошлого столетия стало очевидно, что дефицит IP-адресов в адресном пространстве глобальной сети не за горами. Количество отдельных «хостов», подключенных к Интернету росло и продолжает расти быстрыми темпами. Назрела необходимость каким-то образом обеспечить доступ к глобальным ресурсам всё большему количеству компьютеров и одновременно упростить их индексацию. В 1994-м году группой разработчиков сетевых технологий Network Working Group был предложен метод, с помощью которого решалась задача экономии IP-адресов. В этом документе участники группы NWG опубликовали описание, как актуальности, так и возможного решения проблемы с помощью объединения отдельных IP-адресов в группы. В том же году была разработана технология NAT (Network Address Translation - преобразование сетевых адресов). Подробное описание принципов работы NAT вы найдете по этому адресу. И хотя разработчики заявили, что NAT временное решение проблемы, технология прижилась, не смотря на некоторые свои недостатки.

Внедрение NAT позволяет решить следующие вопросы.

1. Обеспечение корпоративных и частных локальных сетей большим количеством внутренних IP-адресов. При этом не возникает конфликтов между одинаковыми IP-адресами разных организаций.
2. Обеспечение безопасности всех узлов локальной сети, путем скрытия внутренних IP-адресов от внешней сети. Своего рода FireWall.
3. Организация доступа к Интернету всем компьютерам локальной сети через единый шлюз, используя единственный IP-адрес.

NAT

Современные реализации NAT позволяют решать многие другие задачи касающиеся администрирования сетей, например: контроль и учет трафика конечных пользователей Интернета, мониторинг и ведение статистики. В

Windows XP также встроена своя реализация механизма преобразования сетевых адресов. Аппаратная реализация NAT применяется в ADSL-модемах, различных маршрутизаторах и коммутаторах.

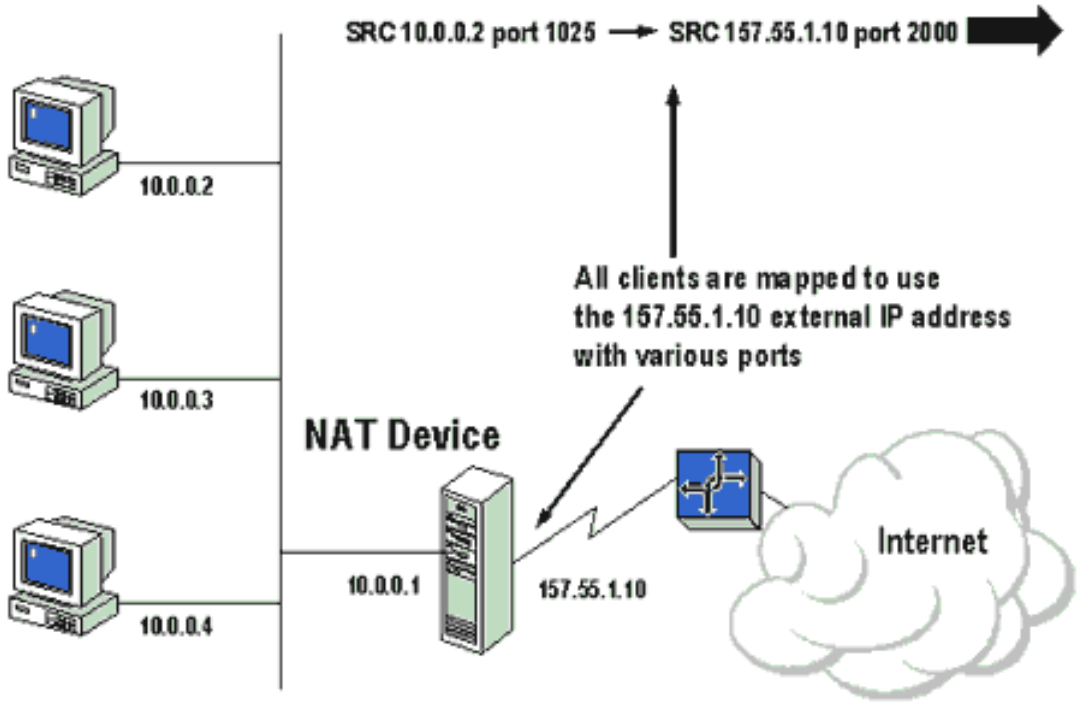


Рисунок 3.1 - Схема технологии NAT

Основные принципы работы технологии NAT заключаются в следующем. В модуль NAT встроена таблица, которая ведет запись о каждом соединении. В ней содержатся IP-адреса и номера портов источников и приемников пакетов информации. С помощью этой таблицы NAT преобразовывает адреса. Для прояснения работы NAT рассмотрим следующий пример.

Есть локальная сеть с одним общим выходом в Интернет. Один из компьютеров устанавливает соединение. Связь проходит через маршрутизатор. Адрес компьютера - 10.78.78.4, порт - 777. Адрес WWW-сервера - 192.155.28.28, порт - 44. Маршрутизатор использует единый для всех «хостов» локальной сети адрес - 10.78.78.1. Пакет, проходя через NAT от локального компьютера к веб-серверу меняет свой адрес с 10.78.78.4 на 10.78.78.1 и порт с 777 на 242, например (для каждого соединения NAT открывает свой порт). В таблице NAT добавляется запись о пакете - IP-адрес и номер порта. Пакет отсылается на удаленный сервер. Обратный пакет содержит адрес получения 10.78.78.1 и порт 242. В таблице NAT происходит поиск данных, соответствующих соединению через порт 242, затем пакет получает IP-адрес компьютера 10.78.78.4 и порт 777 и доставляется до места назначения.

Многие программы раньше не использовали технологию NAT для соединения с глобальной сетью, из-за чего возникали трудности. Несмотря на это, метод получил распространение и постоянно совершенствуется его программная и аппаратная реализация. Наверняка, со временем и NAT уступит свое место более универсальным и продвинутым механизмам, ведь Интернет-технологии развиваются в бешеном ритме.

Система преобразования сетевых адресов

Система преобразования сетевых адресов, разработанная компанией Cisco, используется устройством (брандмауэром, маршрутизатором или компьютером), соединяющим внутреннюю сеть с остальным миром. Преобразование сетевых адресов может иметь разные формы и может работать разными способами:

1. Статическое преобразование сетевых адресов - преобразование незарегистрированного IP адреса в зарегистрированный IP адрес по принципу «один к одному». Особенно полезно, когда требуется доступ к устройству из-за пределов локальной сети.
2. Динамическое преобразование сетевых адресов - преобразование незарегистрированного IP адреса в зарегистрированный IP адрес из группы зарегистрированных IP адресов.
3. Перегрузка - форма динамического преобразования, преобразующая много незарегистрированных IP адресов в один зарегистрированный адрес за счет использования различных портов. Эту процедуру еще называют PAT (Port Address Translation, преобразование портов и адресов), одноадресным NAT или мультиплексированным NAT на уровне портов.
4. Совпадение - когда используемые в вашей сети адреса являются зарегистрированными IP адресами, используемыми в другой сети, маршрутизатор должен вести таблицу преобразования таких адресов, перехватывать их и заменять зарегистрированными уникальными IP адресами. Важно отметить, что маршрутизатор NAT должен преобразовывать «внутренние» адреса в зарегистрированные уникальные адреса, а также «внешние» зарегистрированные адреса в адреса, которые являются уникальными в частной сети. Такая операция может осуществляться с использованием статического преобразования сетевых адресов, либо сервиса доменных имен (DNS) и внедрения динамического преобразования сетевых адресов.

Внутренняя сеть обычно представляет собой локальную сеть (LAN, Local Area Network), которую иногда называют тупиковым доменом (stub domain). Тупиковый домен - это локальная сеть, внутри которой используются IP адреса. Большинство сетевого трафика в тупиковом домене локальное и не выходит за пределы внутренней сети. Тупиковый домен может содержать как зарегистрированные, так и незарегистрированные IP адреса. Разумеется, все компьютеры, которым присвоены незарегистрированные IP адреса, для связи с остальным миром должны пользоваться преобразованием сетевых адресов.[8]

Настройка преобразования сетевых адресов

NAT можно настраивать различными способами. В приводимом ниже примере маршрутизатор NAT настроен так, что преобразует незарегистрированные (внутренние, локальные) IP адреса, применяемые в частной (внутренней) сети, в зарегистрированные IP адреса. Эта процедура выполняется каждый раз, когда устройству с незарегистрированным адресом во внутренней сети требуется связаться с сетью общего пользования (внешней). Схема представлена на рисунке 3.2.

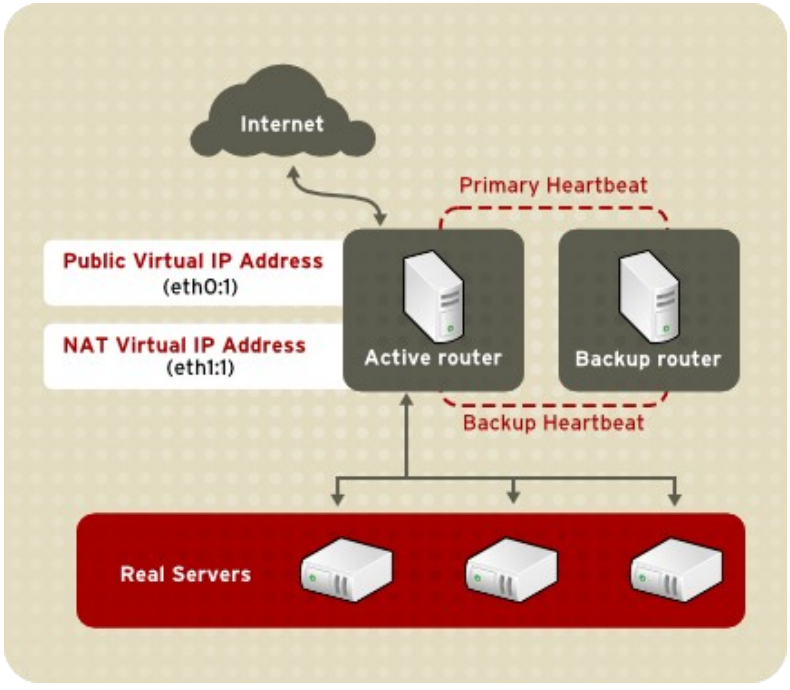


Рисунок 3.2 - Схема преобразования сетевых адресов

Интернет-провайдер закрепляет за вашей компанией ряд IP адресов. Адреса из закрепленной группы являются зарегистрированными IP адресами и называются внутренними глобальными адресами. Незарегистрированные,

частные IP адреса разделяются на две группы. Одна небольшая группа (внешние локальные адреса) используется маршрутизаторами NAT. Вторая, значительно большая группа, которую называют внутренними локальными адресами (inside local addresses), используется в тупиковом домене. Внешние локальные адреса используются для формирования уникальных IP адресов устройств, называемых внешними глобальными адресами, для выхода в публичную сеть.

1. Большинство компьютеров тупикового домена обменивается информацией друг с другом, используя внутренние локальные адреса.
2. Некоторые компьютеры тупикового домена часто связываются с устройствами за пределами локальной сети. Эти компьютеры имеют внутренние глобальные адреса, которые не требуют преобразования.
3. Когда компьютеру тупикового домена с внутренним локальным адресом нужно связаться с компьютером за пределами локальной сети, пакет направляется к одному из маршрутизаторов NAT.
4. Маршрутизатор NAT сверяется с таблицей маршрутизации для выяснения, есть ли запись для адреса назначения. Если такая запись имеется, маршрутизатор NAT преобразует пакет и создает для него запись в таблице трансляции адресов. Если адреса назначения в таблице маршрутизации нет, пакет игнорируется.
5. Используя внутренний глобальный адрес, маршрутизатор отправляет пакет к пункту назначения.
6. Компьютер в публичной сети отправляет пакет в частную сеть. Адресом отправителя пакета является внешний глобальный адрес. Адресом назначения является внутренний глобальный адрес.
7. Маршрутизатор NAT сверяется с таблицей трансляции адресов и определяет, что здесь имеется адрес назначения, соотносящийся с компьютером в тупиковом домене.
8. Маршрутизатор NAT преобразует внутренний глобальный адрес пакета во внутренний локальный адрес и отправляет пакет к соответствующему компьютеру.

Перегрузка NAT

Перегрузка NAT использует функцию пакета протоколов TCP/IP, мультиплексирование, позволяющую компьютеру создавать с одним или несколькими удаленными компьютерами несколько одновременных соединений с применением различных портов TCP или UDP. Пакет IP содержит заголовок, в котором имеется следующая информация:

1. Адрес источника - IP адрес компьютера-отправителя, например, 201.3.83.132
2. Порт отправителя - номер порта TCP или UDP, назначенный компьютером-отправителем для данного пакета, например, порт 1080
3. Адрес получателя - IP адрес компьютера-получателя, например, 145.51.18.223
4. Порт назначения - номер порта TCP или UDP, который компьютер-отправитель требует открыть у компьютера-получателя, например, порт 3021.

Адреса указывают две машины на каждом конце, а номера портов обеспечивают уникальный идентификатор для соединения между двумя компьютерами. Комбинацией этих четырех чисел определяется одно соединение TCP/IP. В каждом номере порта используется 16 бит, а это значит, что возможно 65 536 (216) значений. На практике, с учетом того, что разные производители сопоставляют порты немного по-разному, можно ожидать, что доступными будут приблизительно 4 000 портов.

2. Реализация компьютерной сети для предприятия ООО РА «Арт-График»

2.1. Анализ предприятия ООО РА «Арт-График»

2.1.1 Описание структуры предприятия ООО РА «Арт-График»

Общество с ограниченной ответственностью рекламное агентство «Арт-График» было создано в начале 2001 года. Рекламно-производственная компания «Арт-График» занимается разработкой и изготовлением наружной и внутренней рекламы на различных носителях.

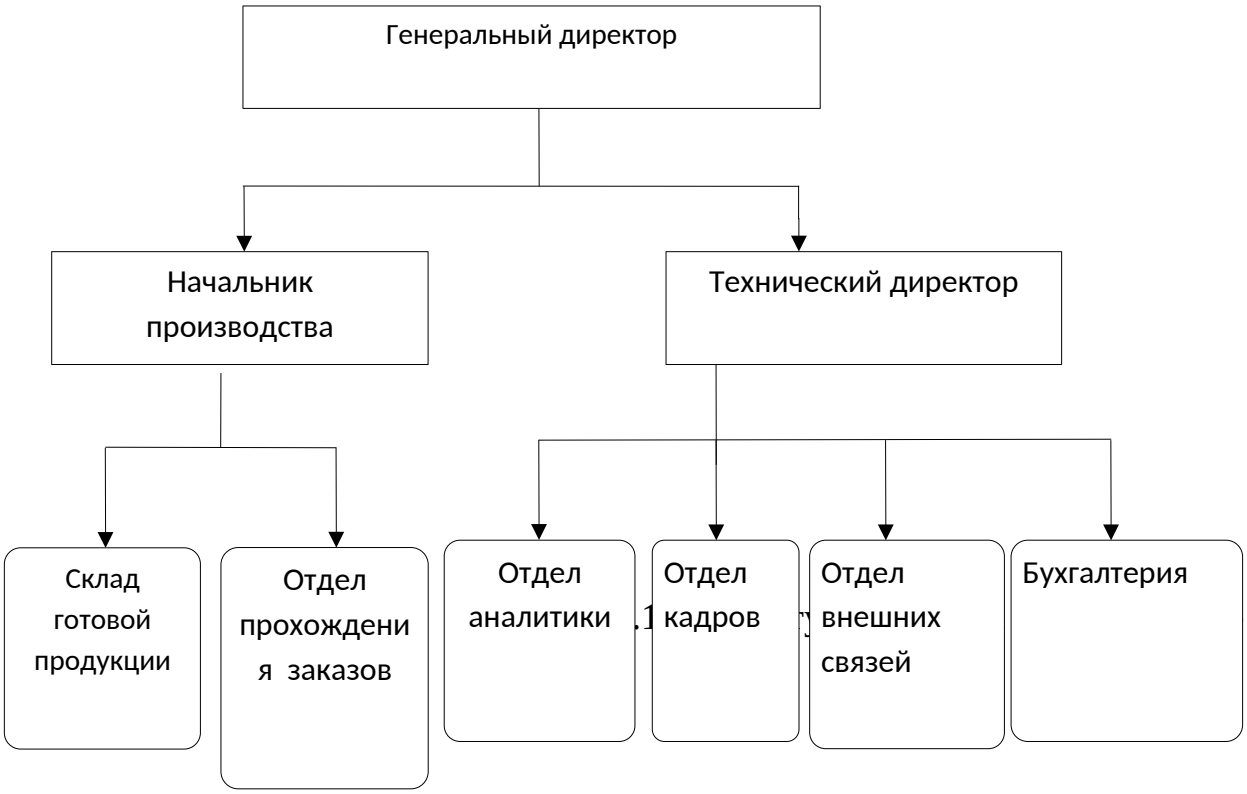
За годы активной деятельности компания заняла прочные позиции на рекламном рынке г. Санкт-Петербурга и Ленинградской области в разработке дизайна и изготовлении наружной рекламы.

Имеется собственная производственная база, позволяющая изготавливать рекламные конструкции любой сложности.

Руководство предприятия:

Генеральный директор – Свояков Алексей Юрьевич;

Технический директор – Алушин Алексей Викторович



Существуют разнообразные организационные схемы рекламных агентств – специализированные в узких областях рекламной деятельности и полносервисные, предоставляющие заказчикам весь комплекс работ в области маркетинговых коммуникаций. С первого взгляда может показаться, что все работающие в рекламном агентстве занимаются исключительно творческой работой. На самом деле больше 2/3 штата вообще не решают творческих задач. Круг их занятий совершенно иной: работа с СМИ, исследовательская работа, работа с подрядчиками и клиентами и т.п.

Сегодня ни одно предприятие невозможно представить без высокотехнологичного информационного оснащения. Без компьютера не обходится ни бухгалтер, ни менеджер. И, конечно, удобно, когда все имеющиеся на предприятии компьютеры связаны между собой единой системой – локальной вычислительной сетью, или ЛВС, входящей в состав единой информационной инфраструктуры.

2.4 Моделирование физического объекта предприятия

Площадь ООО РА «Арт-График» 202 м^2. Офис предприятия занимает 1 этаж здания и состоит из 13 комнат и 1 коридора и одного цеха площадью

52 м^2. В помещении сметного отдела находится 3 компьютера, офисная техника, мебель. Общая длинна кабеля 132 м. В таблице 2.1 представлены данные о помещении ООО РА «Арт-График».

Таблица 2.1 – Данные о помещении

Тип помещения	Площадь, м^2	Содержимое	Кол-во компьютеров	Длина кабеля, м
Отдел МТР	12	Мебель, офисная техника, маршрутизатор отдела	4	12
Техническое помещение	9	Прокси-сервер с МСЭ, сервер-интернет, погран. Маршрутизатор	0	15
Кабинет руководства отделов	12	Мебель, офисная техника,	4	25
Кабинет директора	12	Мебель, офисная техника, сейф, отдельный стол для переговоров.	1	5
Сметный отдел	12	Мебель, офисная техника	3	20
Отдел ДОУ	12	Мебель, офисная техника	2	10
Инженерный отдел	30	Мебель, офисная техника	9	10
Финансовый отдел	15	Мебель, офисная техника	6	10
Отдел ВС	12	Мебель, офисная техника	3	5
Отдел аналитики	12	Мебель, офисная техника	3	15
Бухгалтерия	12	Мебель, офисная техника	3	15

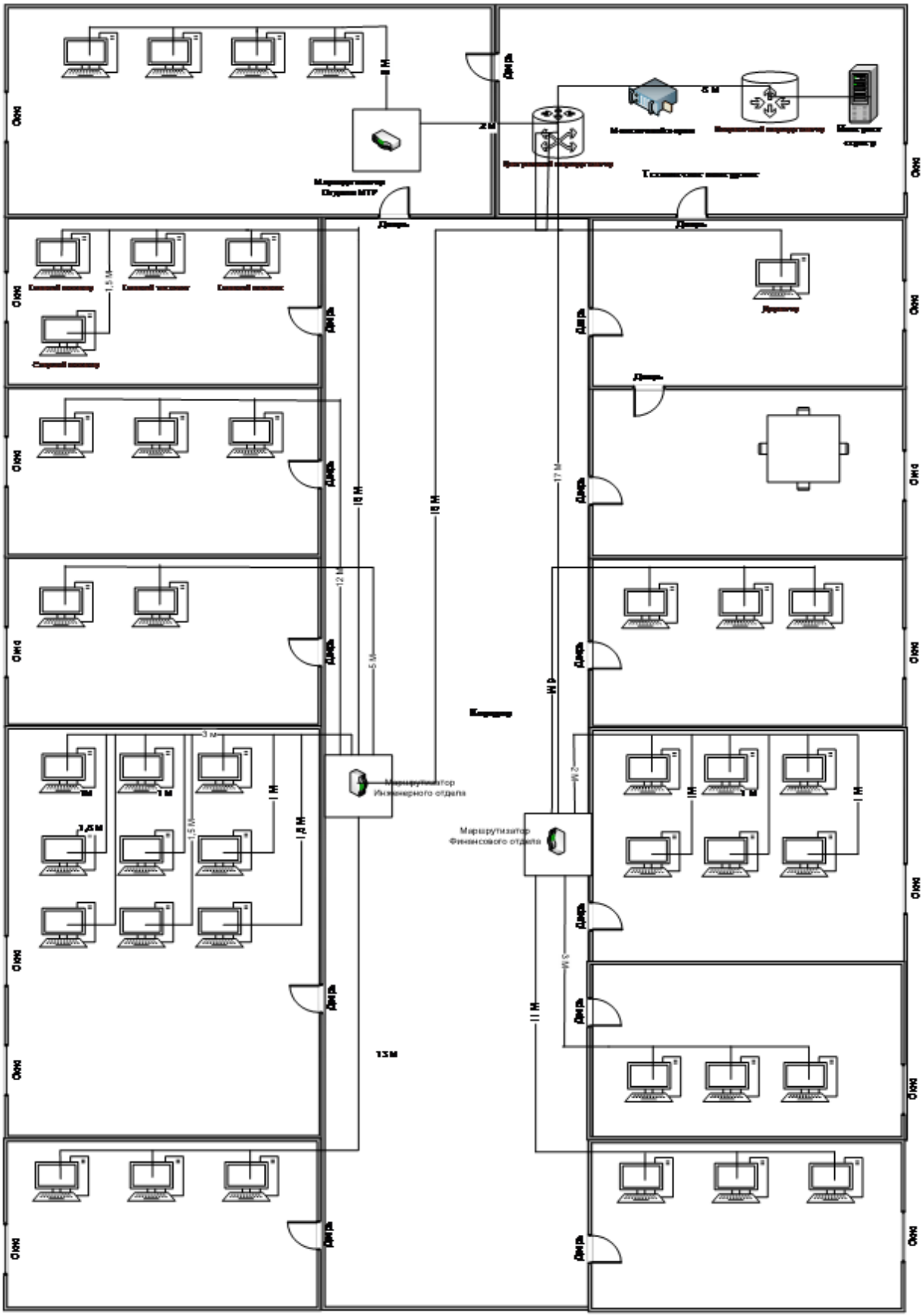


Рисунок 2.7 – Физическая структура сети предприятия

2.5 Структура сети

Структура сети предприятия ООО РА «Арт-График» отражает организационную структуру предприятия. На предприятии 43 компьютера 42 из них (кроме компьютера генерального директора) разделенных на 3 сегмента локальной сети,

1. 1 сегмент сети (инженерный)

- 3 компьютера сметного отдела
- 2 компьютера документационного обеспечения
- 9 компьютеров инженерного отдела
- 3 компьютера бухгалтерии
- Компьютер главного технолога
- Компьютер старшего по разработкам
- Компьютер главного механика
- Компьютер главного инженера

2. 2 сегмент сети (экономический)

- 3 компьютера отдела внешних связей
- 4 компьютеров бухгалтерии
- 3 компьютера отдела кадров
- 3 компьютера планового отдела
- 3 компьютера бухгалтерии
- 3 компьютера отдела аналитики

3. 3 сегмент сети (материально-техническое обеспечение)

- 4 компьютера отдела

На рисунке 1.5 представлена топология 3 сегмента сети, на рисунке 1.6 топология 1 сегмента сети, на рисунке 1.7 представлена топология 2 сегмента сети, в приложении 1 общая схема всех сегментов сети

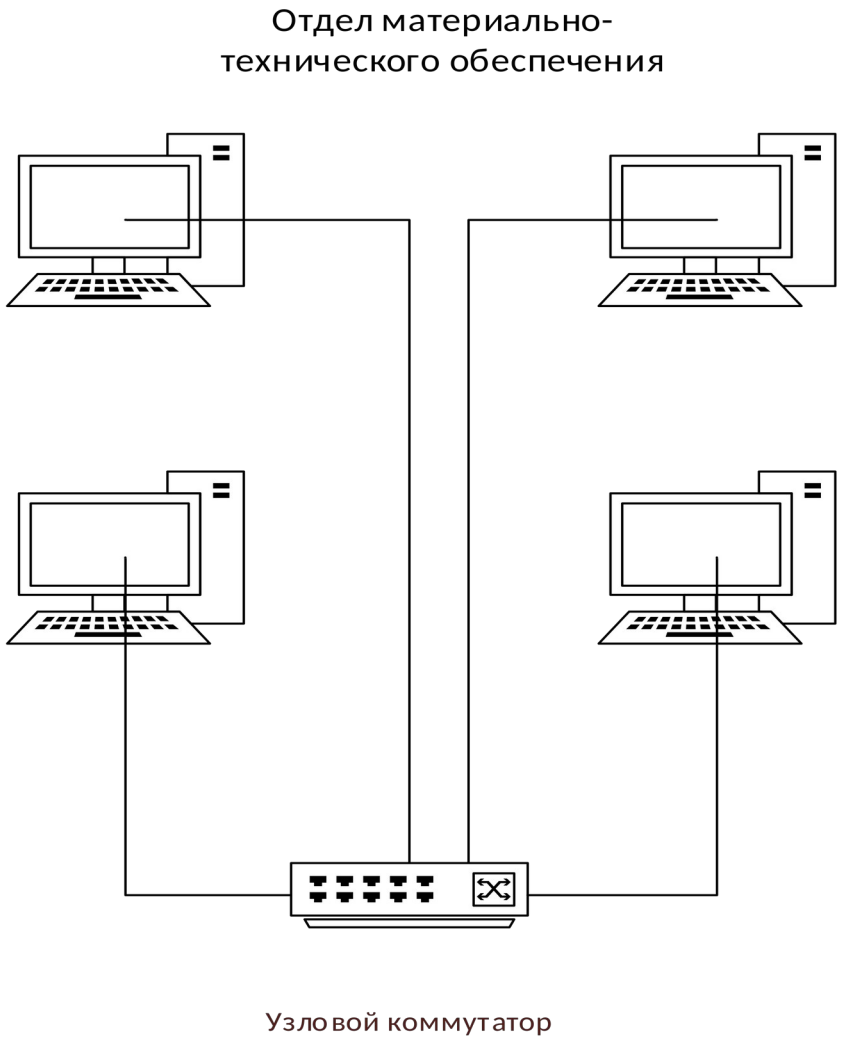


Рисунок 1.5 - 3 Сегмент сети

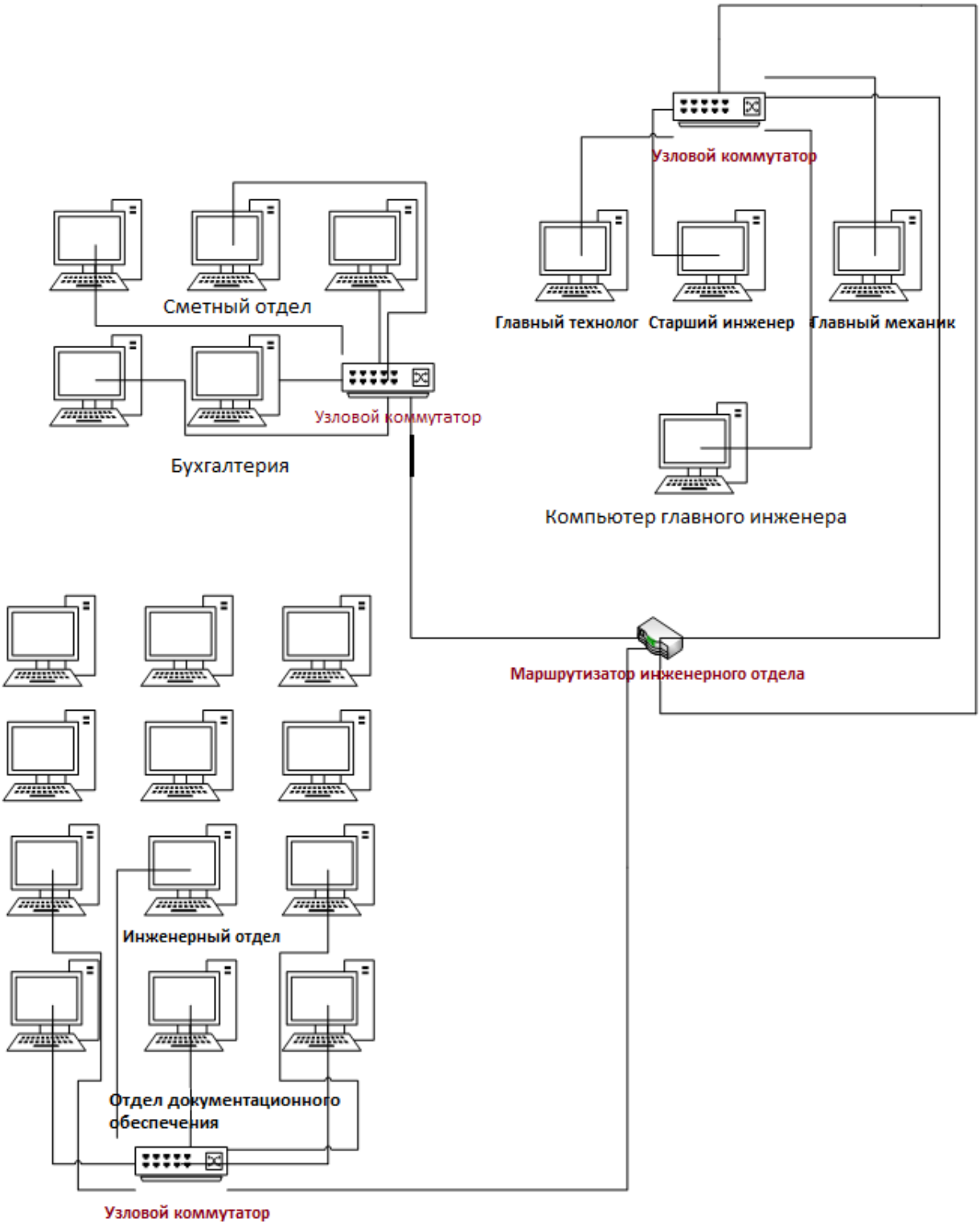


Рисунок 1.6 - 1 Сегмент сети

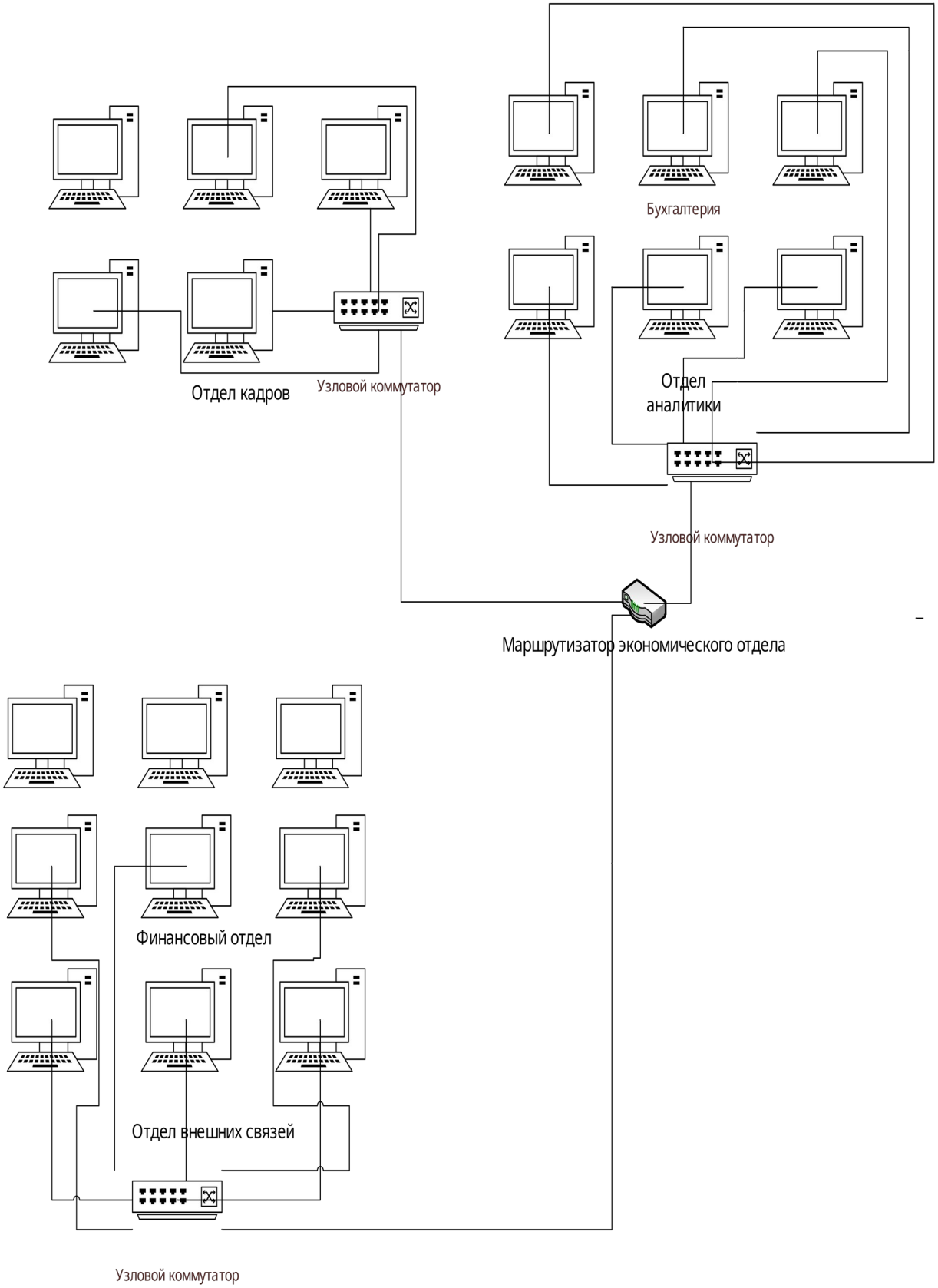


Рисунок 1.7 - 2 сегмент сети

2.6 Проектирование доступа в интернет для предприятия ООО РА «Арт-График»

2.4.2 Установка соединения через NAT

У нас есть компьютер (для простоты обозначения назовём его SERVER) с двумя сетевыми адаптерами, первый подключен к интернету, второй находится в локальной сети. В данном пункте будет продемонстрирована настройка NAT на компьютере под управлением Windows Server 2012. Для того что бы добавить на сервере роль NAT для начала нужно запустить “Диспетчер сервера” (Пуск -> Администрирование –> Диспетчер сервера).

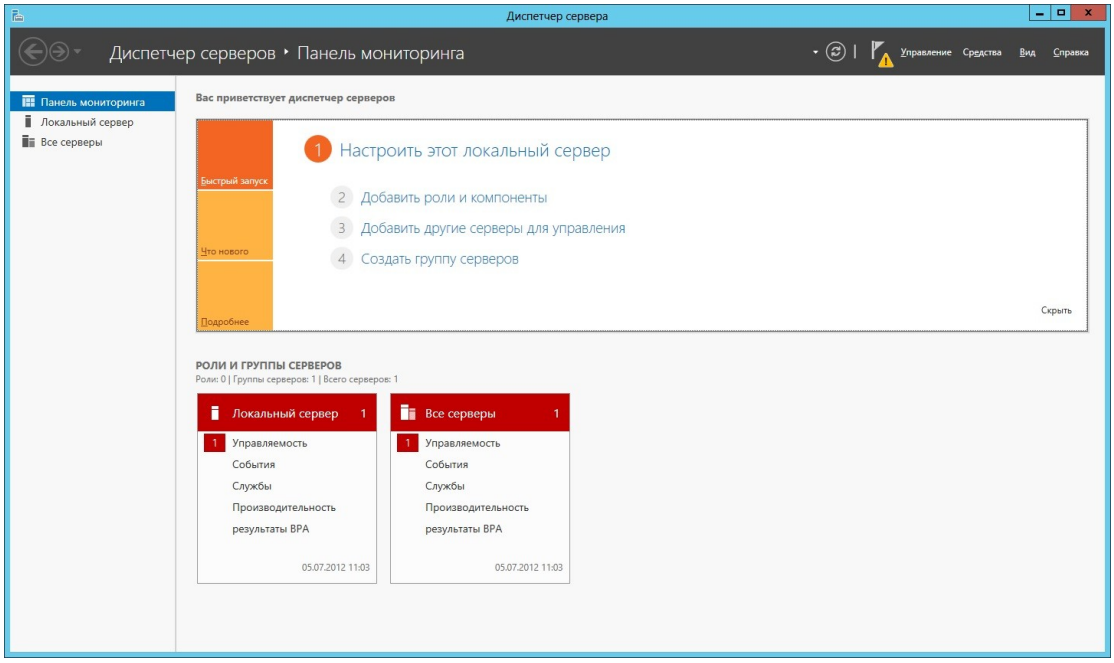


Рисунок 3.3 - Диспетчер сервера

Из диспетчера сервера Windows мы можем управлять нашим сервером добавляя или удаляя роли. Нажмите “Добавить роли и компоненты” после чего откроется мастер добавления ролей на первой странице которого вам напомнят что необходимо проверить перед началом работы. Нажимаем “Далее” и мастер нам предложит выбрать тип установки, нам даётся два варианта “установка ролей и компонентов” или “установка служб удалённых рабочих столов”, нас интересует первый вариант, выбираем жмём “Далее”. На этой странице мастер спросит нас куда мы хотим добавить роль, на сервер или виртуальный жёсткий диск, выбираем сервер и нажимаем “Далее”.

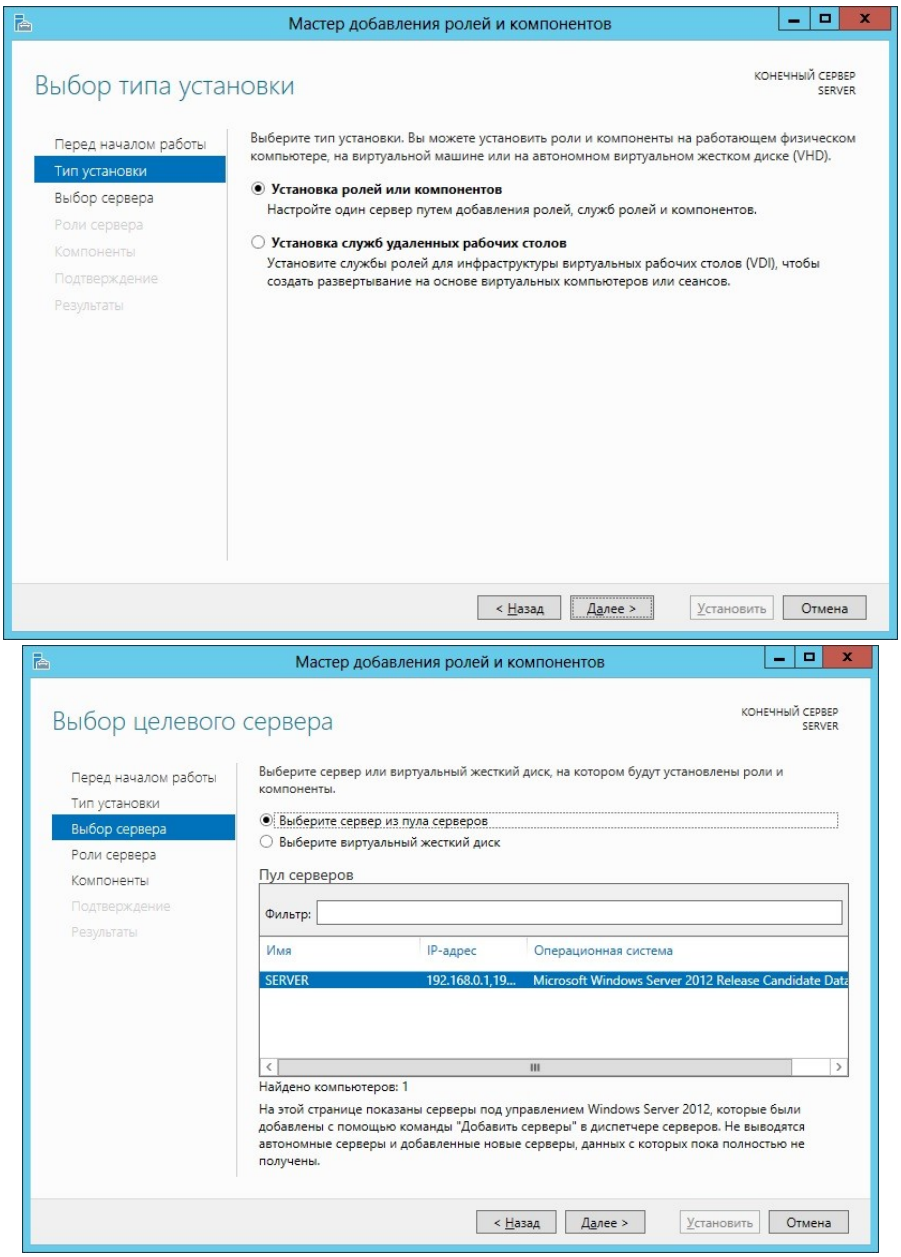


Рисунок 3.4 - Выбор типа установки и выбор сервера

Теперь мастер предлагает выбрать нам роль которую мы хотим установить на сервер, ставим галочку напротив “Удалённый доступ” и тут же выскакивает окно в котором мастер сообщает нам что для установки этой роли необходимо установить дополнительные средства, нажимаем “Добавить компоненты” окно дополнительных компонентов исчезает и мы жмём “Далее”.

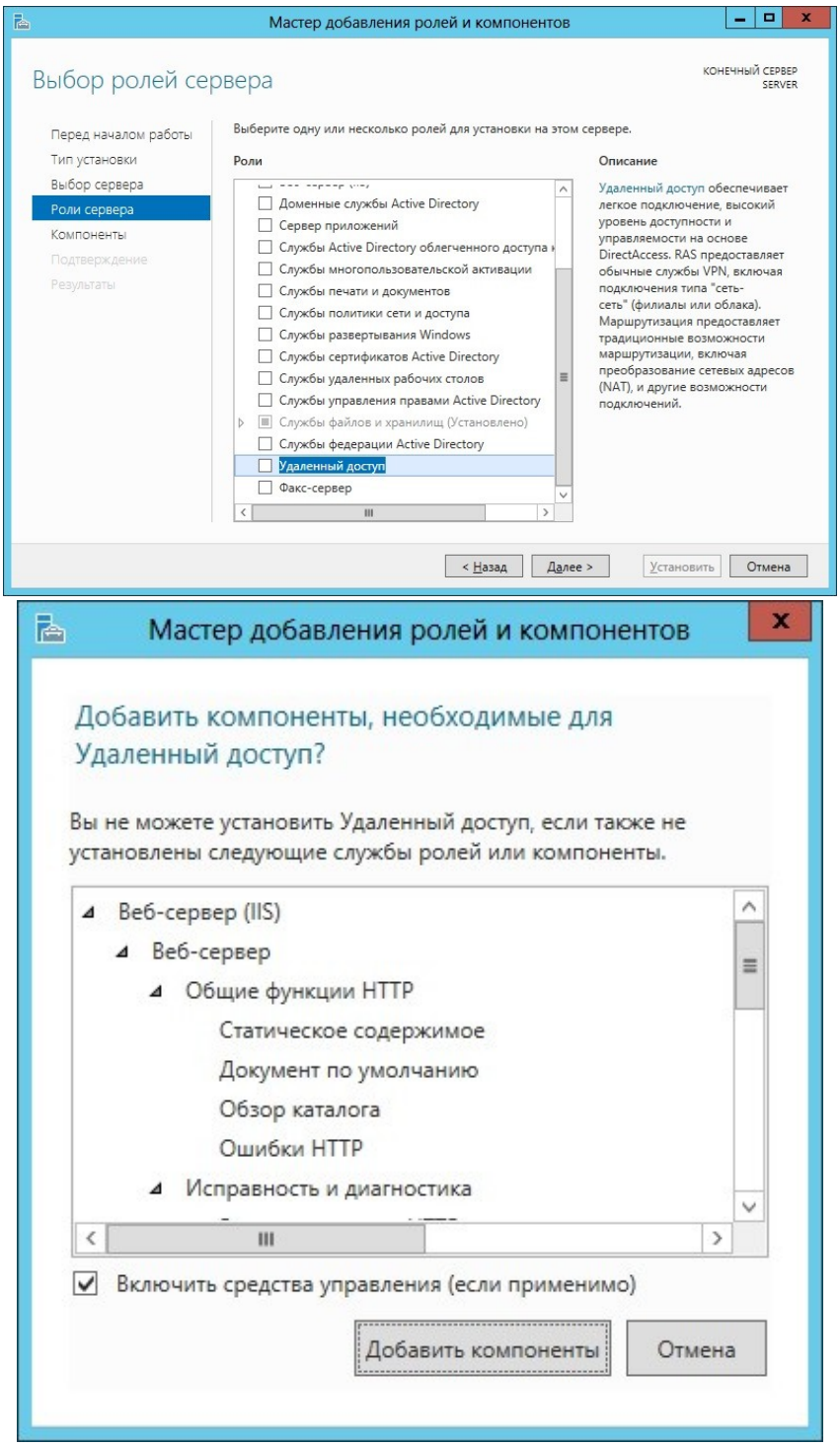


Рисунок 3.5 - Роли сервера сервера и компоненты

Следующим шагом мастер предлагает нам добавить компоненты сервера, здесь нам ничего выбирать не нужно так что просто жмём “Далее” и на следующей странице мастер показывает нам описание роли “ Удалённый доступ” в очередной раз нажимаем “Далее”.

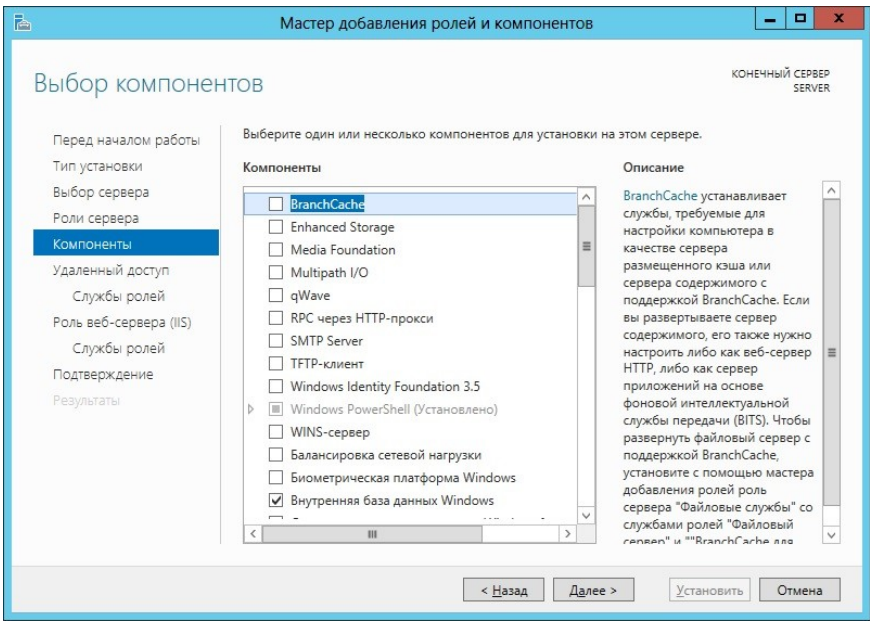


Рисунок 3.6 - Выбор компонентов и удаленный доступ

Теперь мастер предлагает выбрать “службы ролей для установки удалённый доступ”, выделяем галочкой “Маршрутизация” и жмём далее.

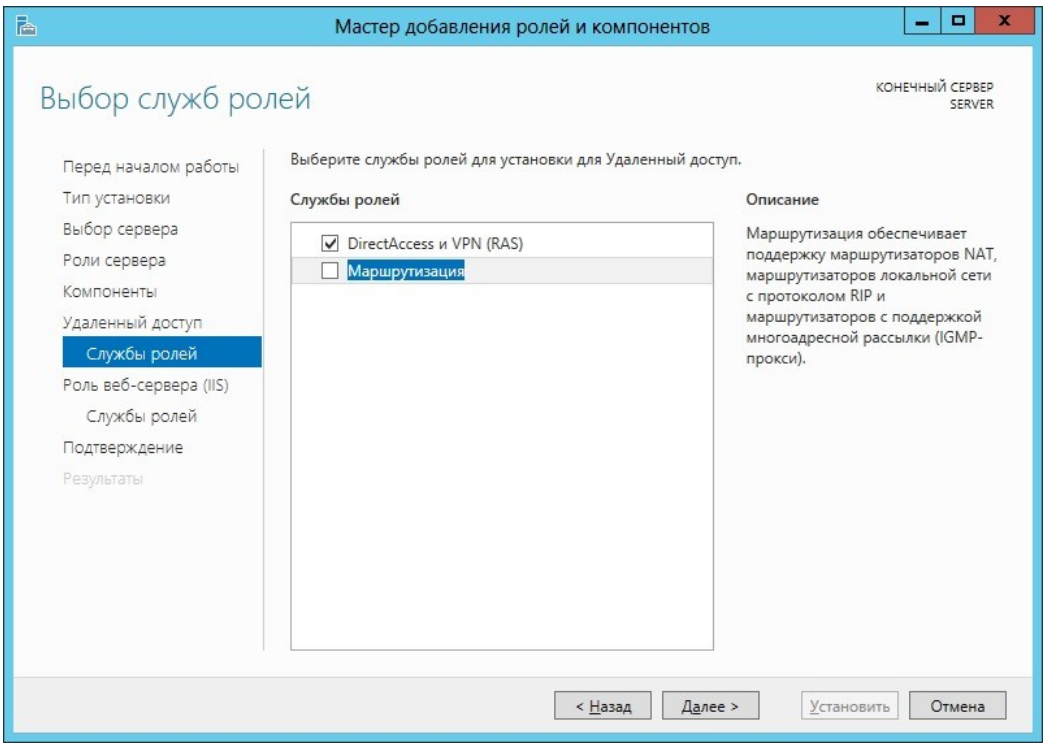


Рисунок 3.7 - Выбор служб и ролей

Следующим шагом, мастер покажет нам описание роли “Веб сервер IIS”, эта роль является обязательной и без неё роль “Удалённый доступ” не может быть добавлена. Нажимаем “Далее”, на следующей странице можно выбрать службы для роли “Веб сервер IIS”, снова нажимаем “Далее”.

На этом шаге мастер показывает нам какие роли и службы будут установлены на сервер, так же сверху можно поставить галочку которая отвечает за немедленную перезагрузку сервера по окончанию установки, если это требуется. После того как будет нажата кнопка “Установить” начнётся процесс установки роли на сервер.

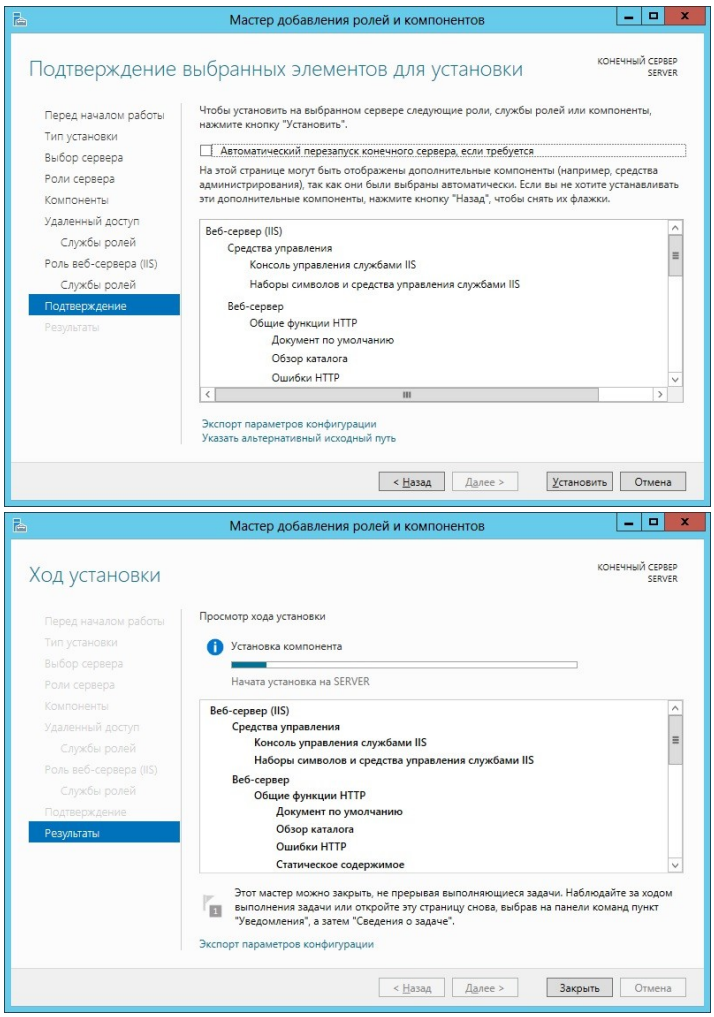


Рисунок 3.8 - Результат установки

После того как мастер закончит установку новой роли на сервер нажмем “Закрыть”.

Установка NAT

После того как роль была установлена нам следует настроить NAT, для этого мы запускаем оснастку “Маршрутизация и удалённый доступ” (Пуск -> Администрирование -> Маршрутизация и удалённый доступ). Затем вызываем контекстное меню и выбираем “Настроить и включить маршрутизацию и удалённый доступ” после чего запускается “мастер настройки сервера маршрутизации и удалённого доступа” он то нам и поможет настроить NAT.

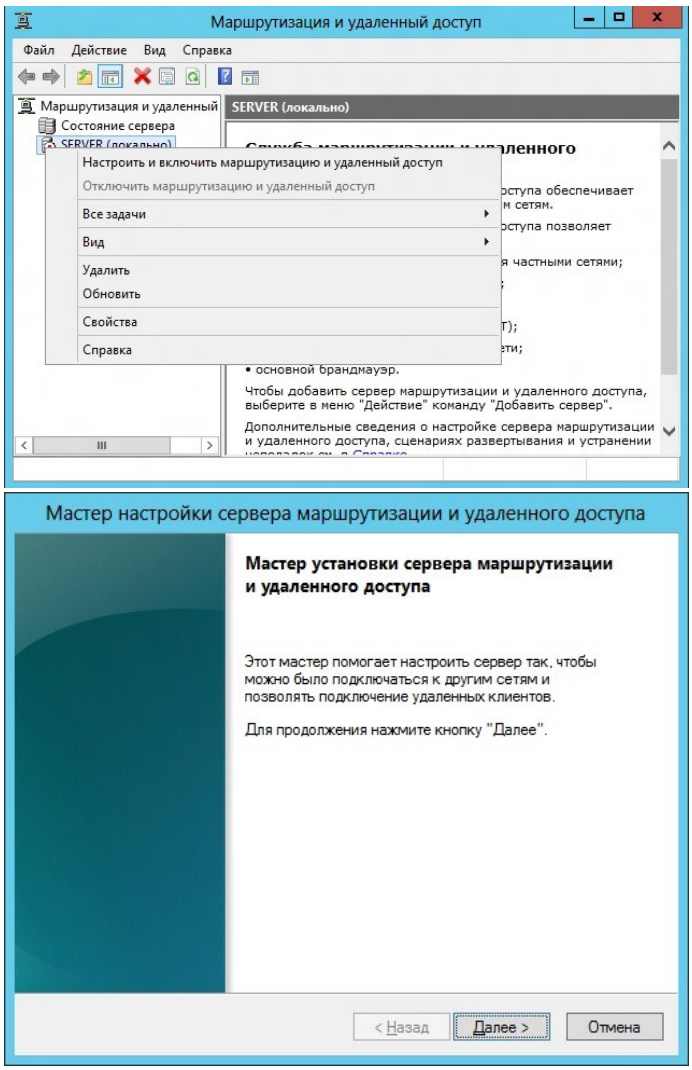


Рисунок 3.9 - Мастер настройки NAT

На первой странице мы увидим краткое описание мастера и нажмём “Далее”. На втором шаге мастер предлагает нам выбрать одну из служб которые будут запущены на сервере, выбираем “преобразование сетевых адресов (NAT)” и жмём “Далее”. После чего мастер нам предложить выбрать сетевое соеденение которое смотрит в интернет (для наглядности я назвал свои сетевые подключения соответственно). Так же нам предлагается вариант подключения по требованию, его следует выбирать если вы осуществляете выход в интернет с помощью модема или подключения которое необходимо активировать в ручную. Выбираем нужное подключение и жмём “Далее”.

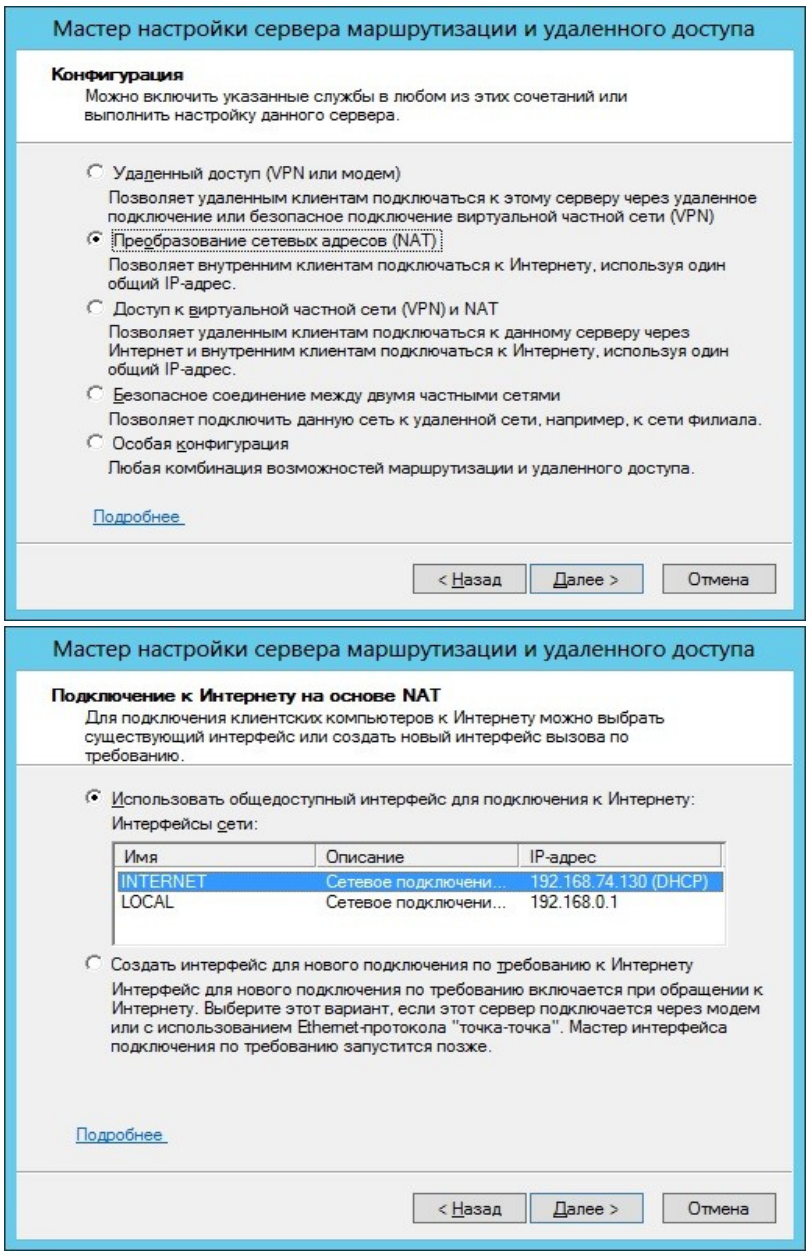


Рисунок 3.10 - Подключение к интернету на основе NAT

На этом этапе мастер предупреждает что ему не удалось обнаружить в нашей локальной сети службы DNS или DHCP и предлагает нам два варианта развития событий:

1. Включить базовые службы назначения адреса и сопоставления имён
2. Установить службы сопоставления имён и адресов позднее

Нам подходит первый вариант, т.к. в нашей сети не установлены службы преобразования имён DNS и все имена будут преобразовывать DNS сервера нашего провайдера. Второй вариант подойдёт тем у кого в сети есть свой DNS сервер. Выбираем первый вариант и нажимаем “Далее”. На следующей странице мастер сообщит вам в каком

диапазоне будет работать NAT, этот диапазон мастер составил исходя из конфигурации вашего сетевого подключения смотрящего в локальную сеть (у меня это подключение называется LOCAL). Нажимаем “Далее” и видим завершающий этап мастера “сервера маршрутизации и удалённого доступа”. На этом экране мастер показывает для какого подключения настроен NAT и на какой диапазон адресов этот NAT будет вещать. Нажимаем “Готово”, мастер внесёт нужные изменения после чего завершит свою работу и перед вами предстанет оснастка “Маршрутизация и удалённый доступ” с настроенным NAT.

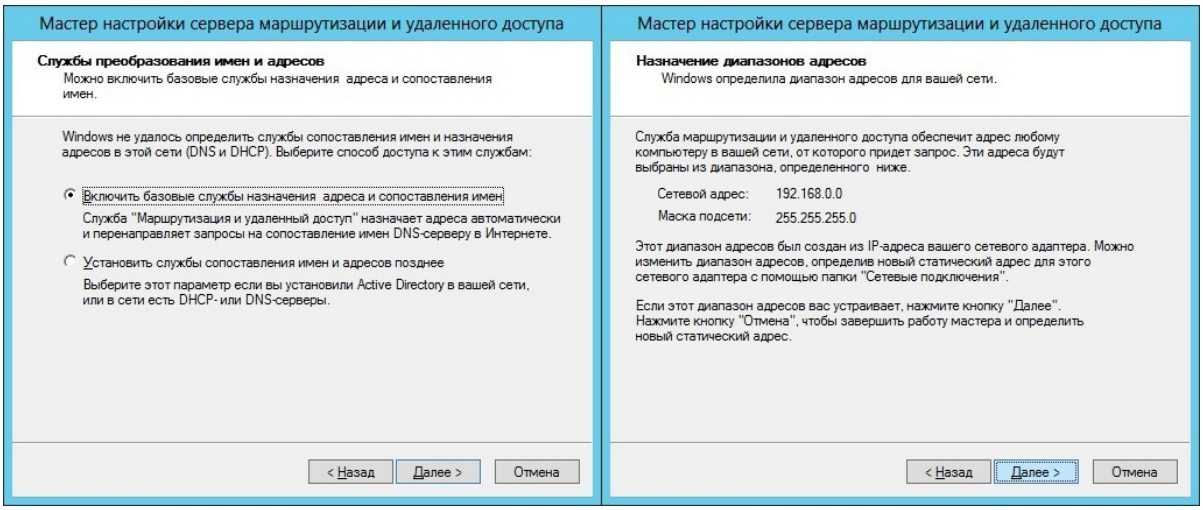


Рисунок 3.11 - Включение базовой службы назначения адреса и сопоставления имен

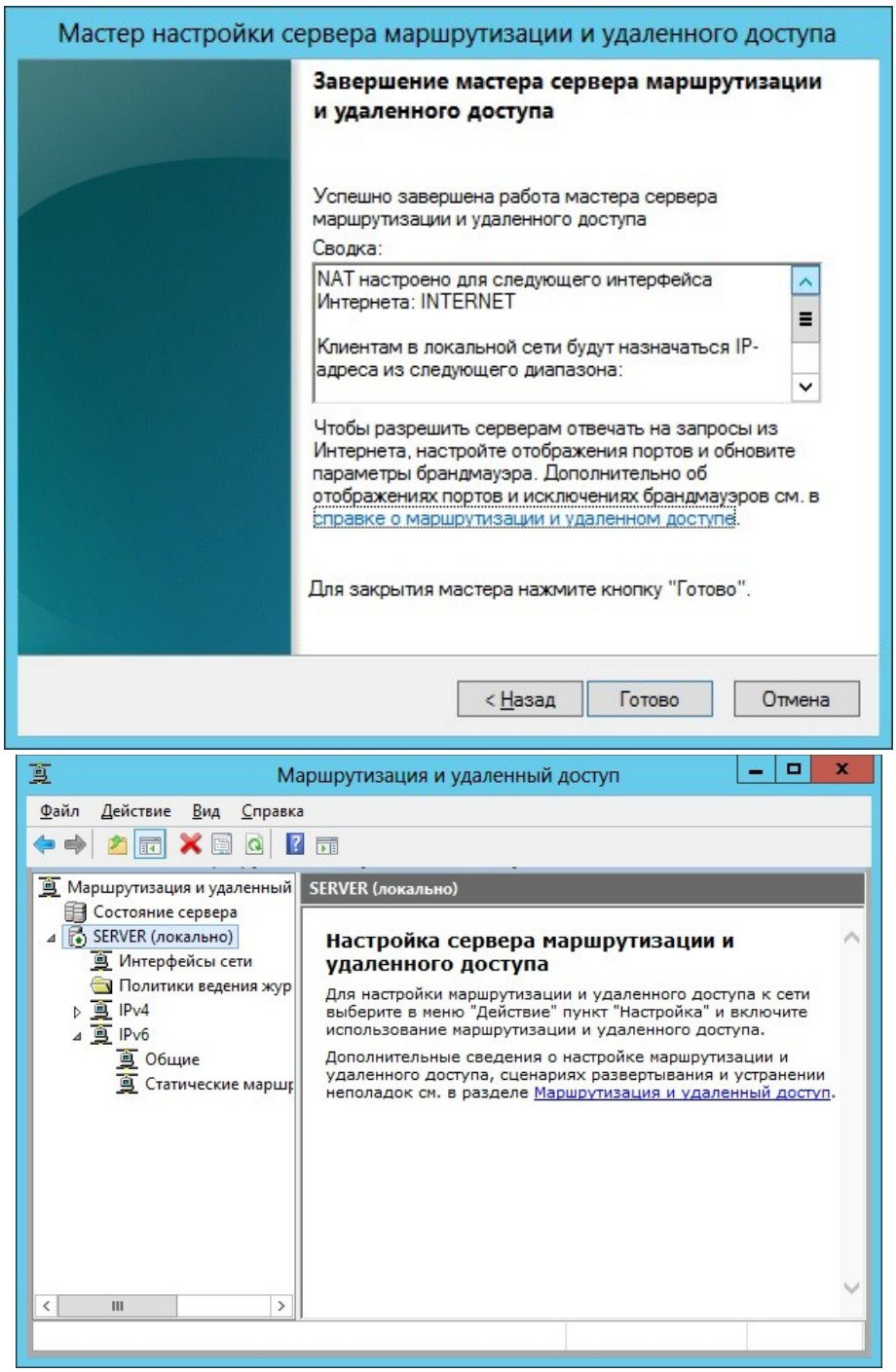


Рисунок 3.12 - Завершение установки

Настройка клиентской машины

Всё дело в том что нужно настроить сетевое подключение для компьютеров которым вы планируете разрешить доступ в интернет(для простоты обозначения назовём эти компьютеры клиентскими). Для того что бы настроить сетевое подключение на клиентском компьютере нам нужно открыть папку “Сетевые подключения” (Пуск -> Панель управления -> Центр управления сетями и общим доступом -> изменение параметров адаптера). Далее если у вас несколько подключений на клиентском компьютере,

выбираем то которое смотрит в локальную сеть, вызываем контекстное меню и нажимаем “свойства”. Выбираем “Протокол Интернета версии 4 (TCP/IPv4)” и нажимаем свойства.

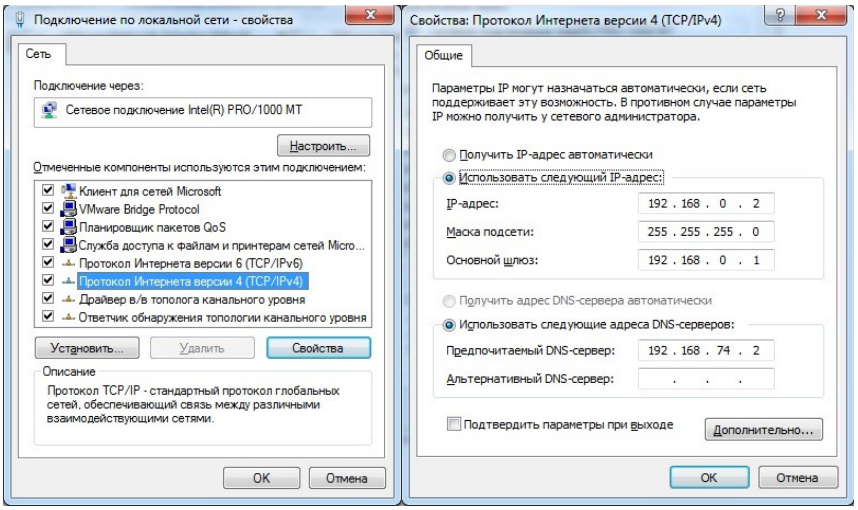


Рисунок 3.13 - Настройка подключения по локальной сети

В после “Основной шлюз” указываем IP адрес SERVER (Компьютер на котором запущен NAT), а в поле “Предпочитаемый DNS-сервер” указываем DNS сервер провайдера(его можно посмотреть в сведениях подключения к интернету на SERVER). После чего нажимаем “OK”, затем ещё раз “OK”. Подключение применит новые настройки и на клиентском компьютере появится доступ в интернет.

1) При установке Traffic Inspector на сервер выберем тип установки "Сервер".

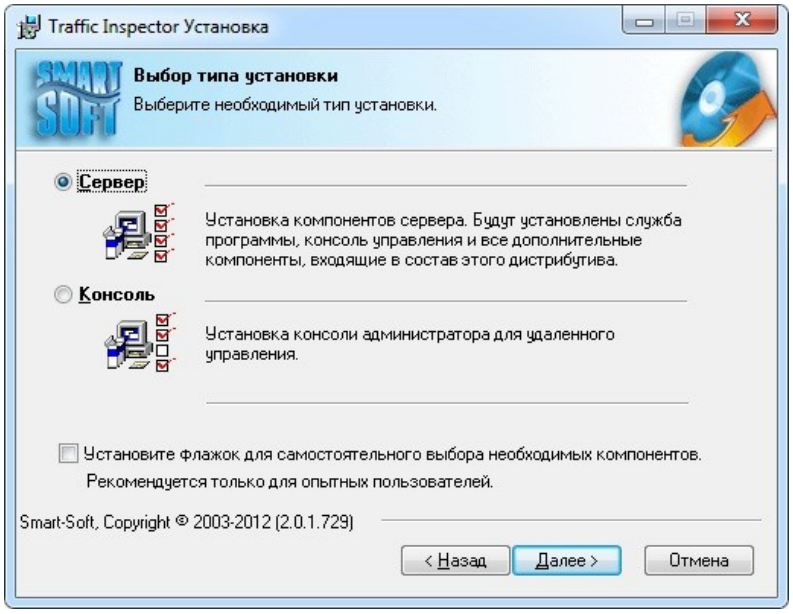


Рисунок 3.14 - Тип установки

2) После установки запустим консоль управления Traffic Inspector (Программы/Traffic Inspector/Администрирование).

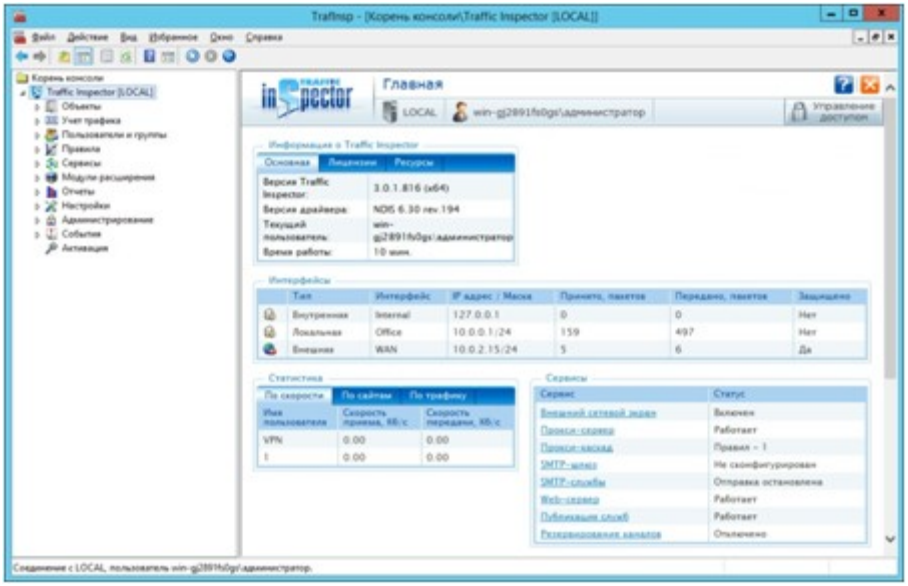


Рисунок 3.15 - Консоль установки

3) После установки программы Traffic Inspector, зайдите в "Консоль администратора" и запустите "Конфигуратор". Вариант применения выберем "Сервер - сетевой шлюз".

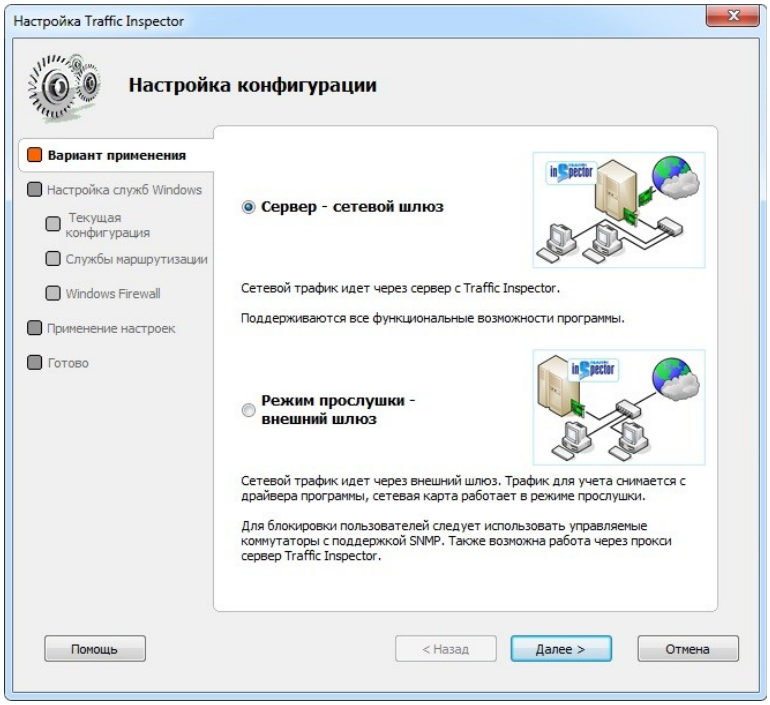


Рисунок 3.16 - Настройка конфигурации

4) В разделе "Службы маршрутизации" выберем "Используется NAT от службы Internet Connection Sharing (ICS)".

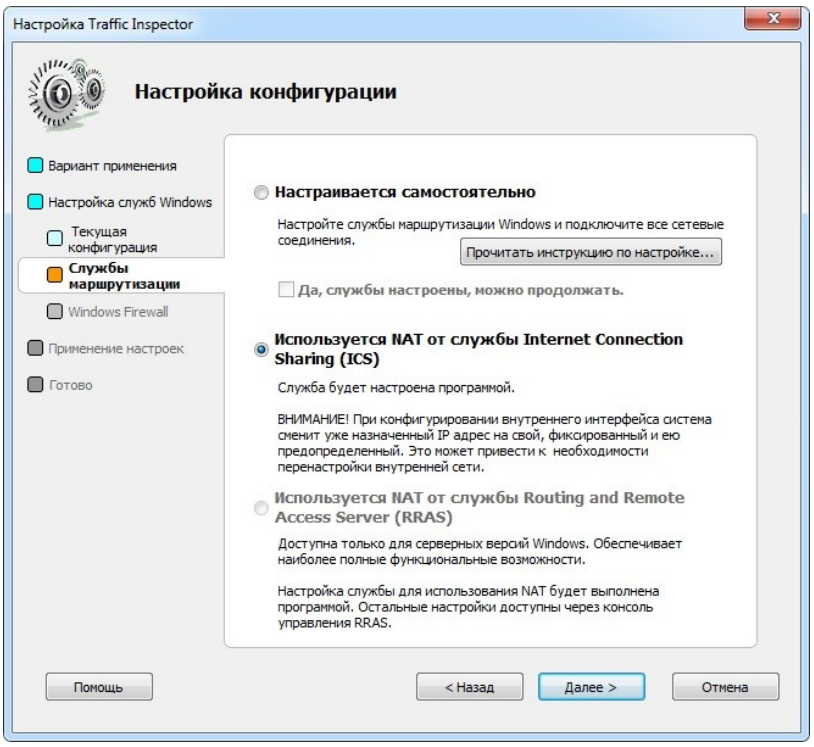


Рисунок 3.17 - Раздел служба маршрутизации

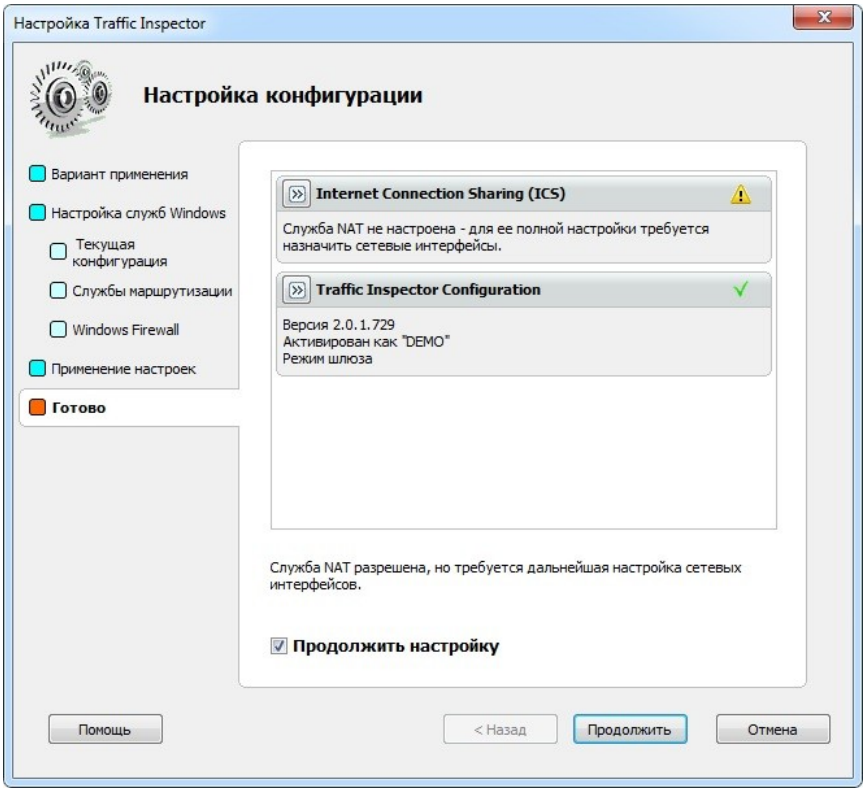


Рисунок 3.18 - Окончание настройки

5) В мастере "Настройка служб Traffic Inspector" выберем необходимые настройки и используемые службы.

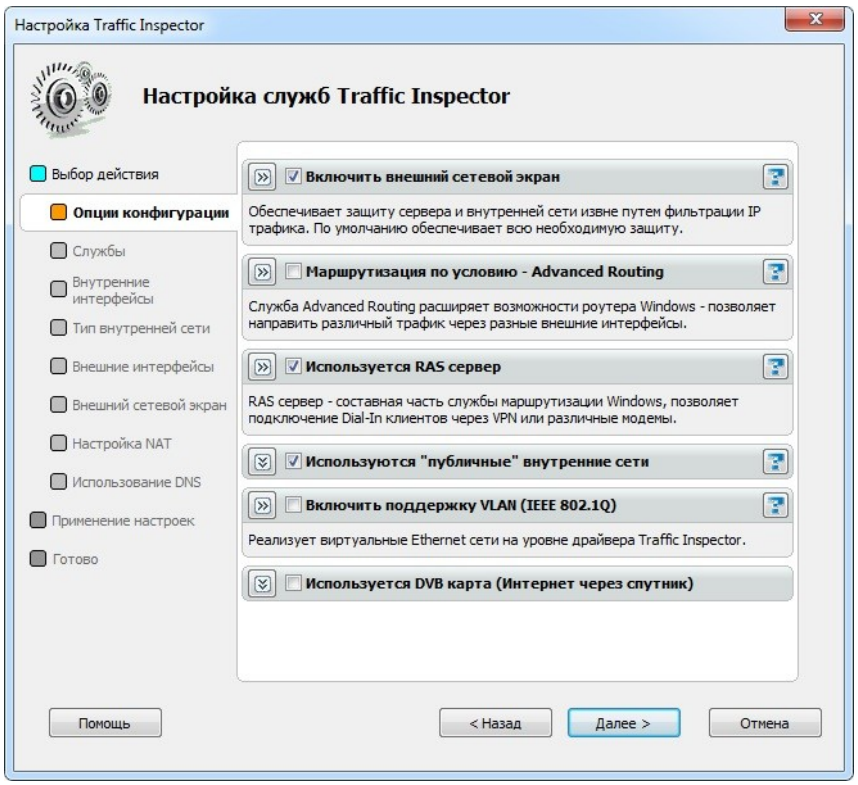


Рисунок 3.19 - Настройка служб Traffic Inspector

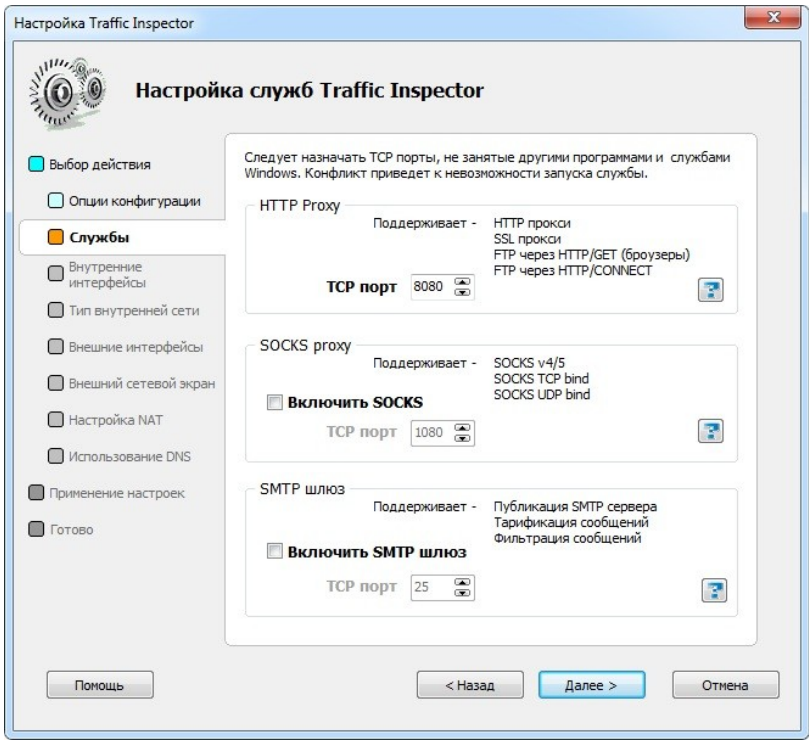


Рисунок 3.20 - Службы Traffic Inspector

6) Выберем сетевой интерфейс внутренней сети.

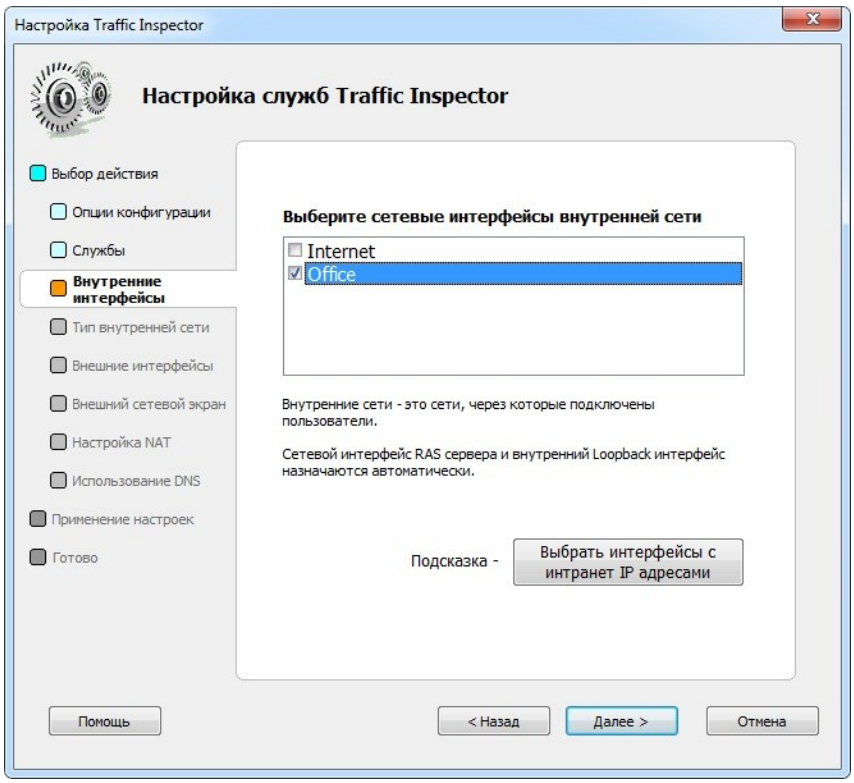


Рисунок 3.21 - Сетевой интерфейс Traffic Inspector

8) Выберем публичные сети (если выбрана публичная сеть, на внутреннем интерфейсе будет включен сетевой экран).

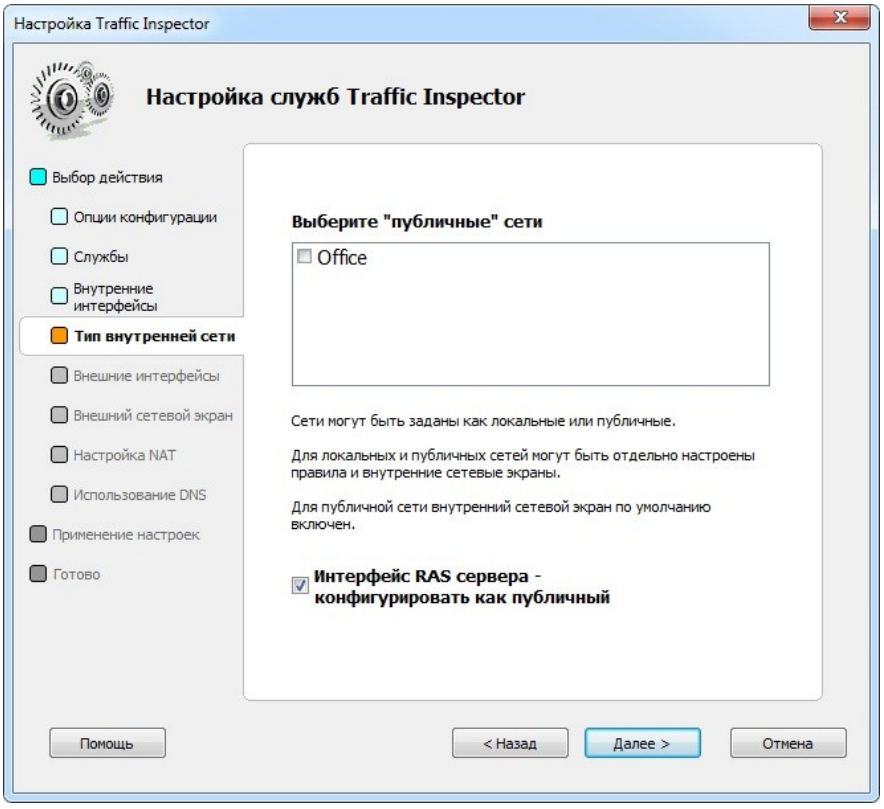


Рисунок 3.22 - Тип внутренней сети

9) Выберем сетевой интерфейс внешней сети.

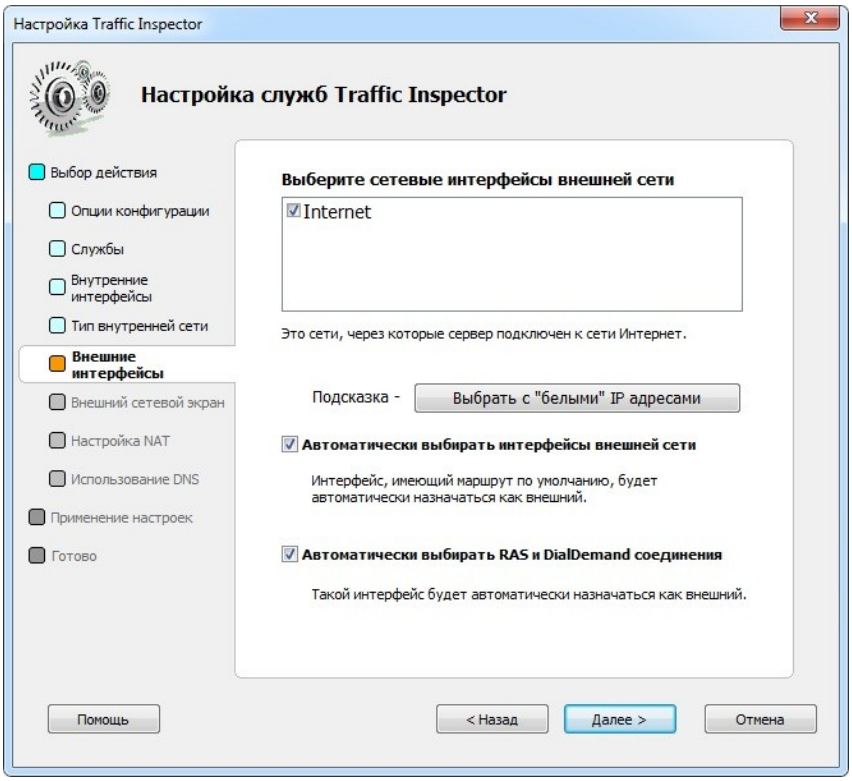


Рисунок 3.23 - Внешние интерфейсы

10) Выберем интерфейсы для настройки NAT необходимо обратить внимание, что если подключение происходит через VPN или PPPoE или Dial-Up, то и указывать нужно именно его, а не сетевое подключение).

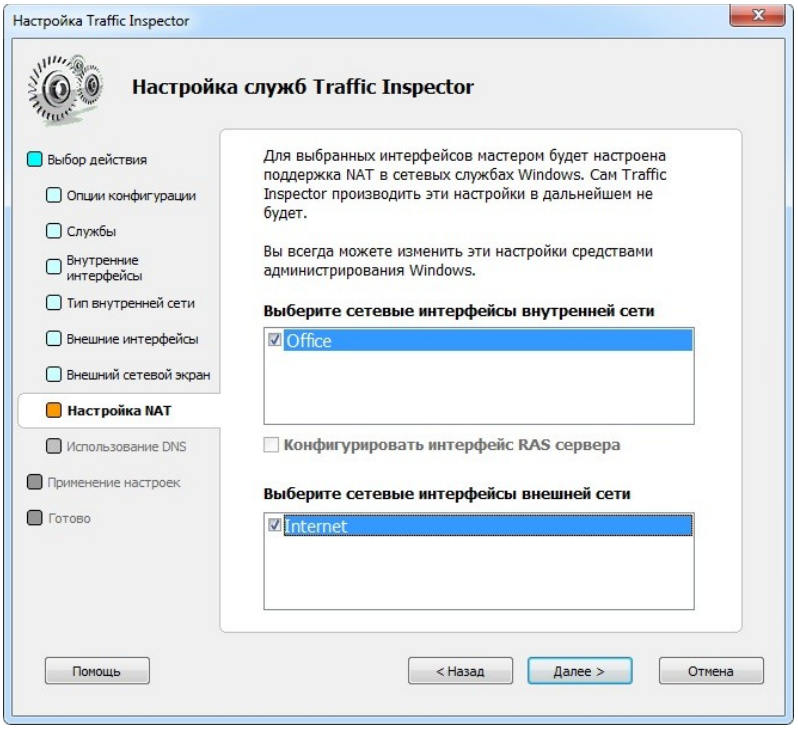


Рисунок 3.24 - Настройки NAT

11) Настройка Конфигурации и Служб Traffic Inspector завершена. Нажмите "Готово".

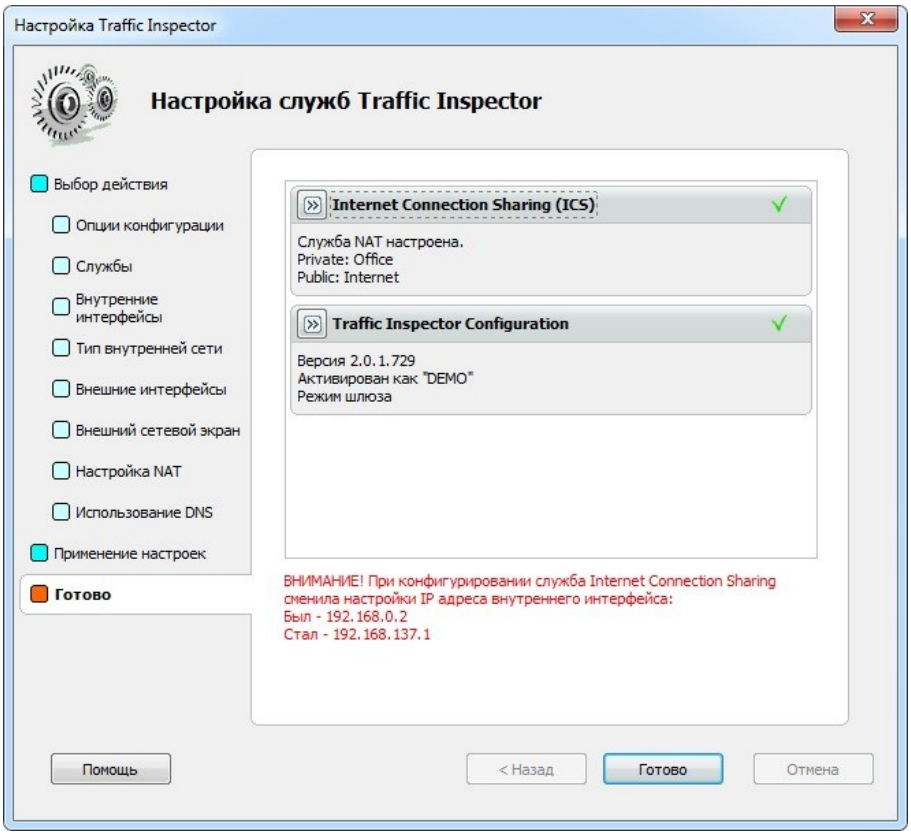


Рисунок 3.25 - Завершение настройки

12) Выбираем "Нормальный" режим использования DNS. Подробности о других режимах можно посмотреть в справке. Жмем «Далее».

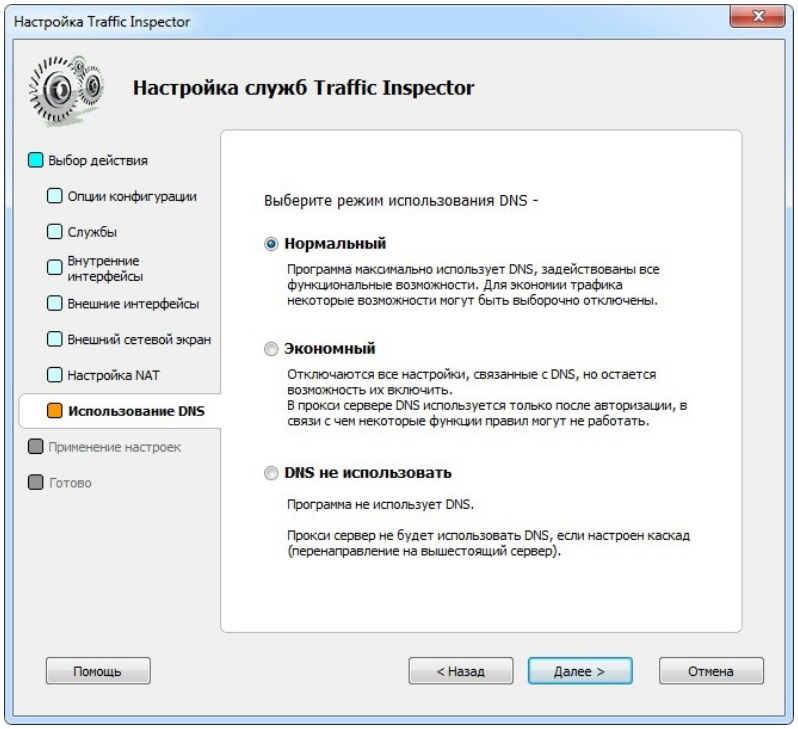


Рисунок 3.26 - Тип DNS

13) Применение установленной нами конфигурации.

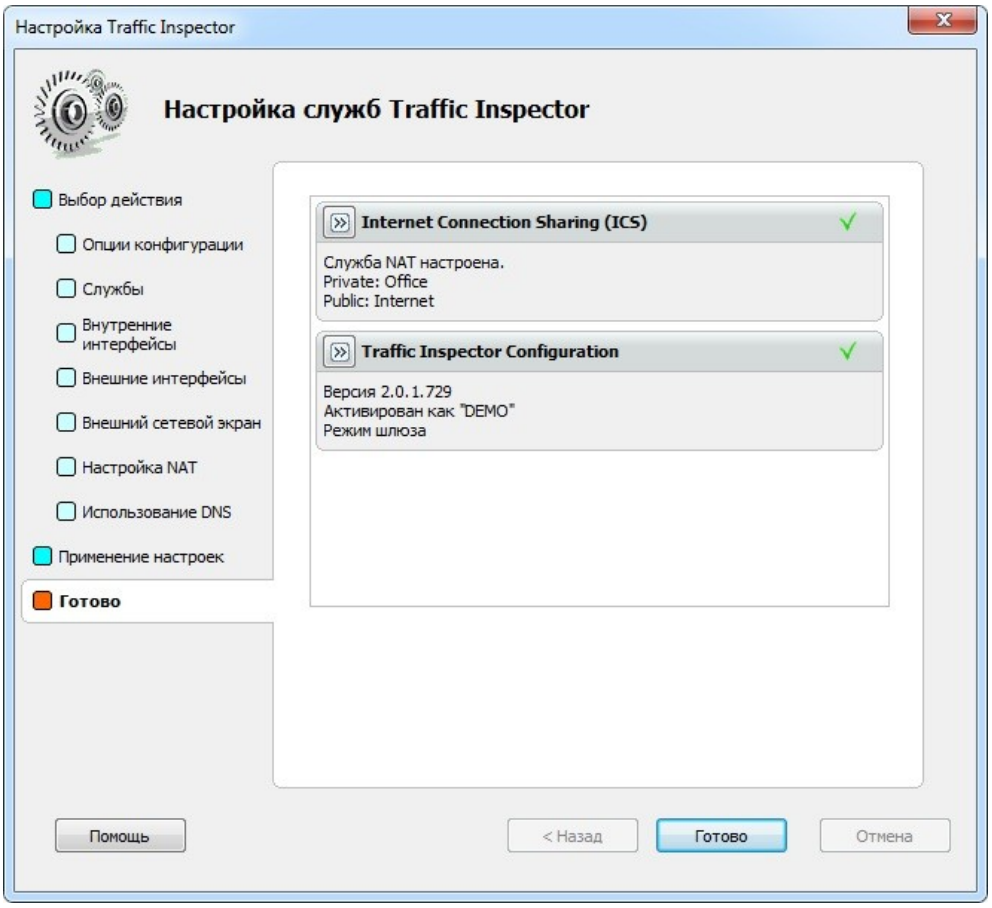


Рисунок 3.27 - Режим шлюза и служба NAT

14) После конфигурирования Traffic Inspector в консоли у нас должны отобразиться интерфейсы внутренней и внешней сетей.

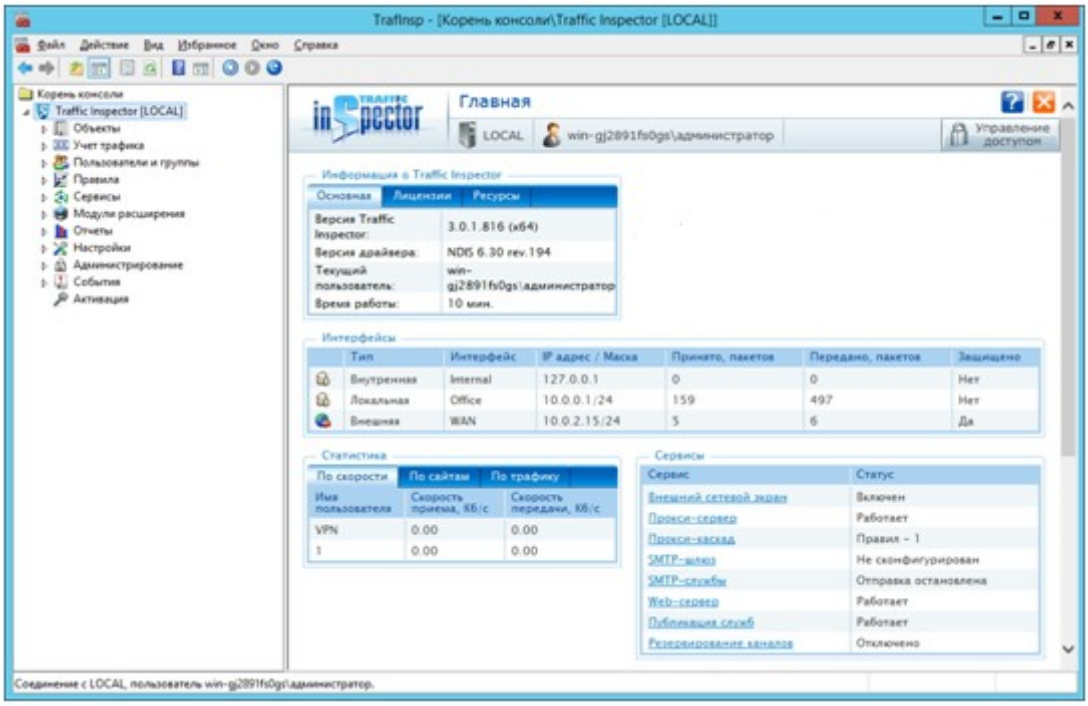


Рисунок 3.28 - Корень консоли Traffic Inspector

15) Раскроем вкладку "Traffic Inspector" и выберем "Управление пользователями". В появившемся окне (см.рис) выберем "Создать пользователя".

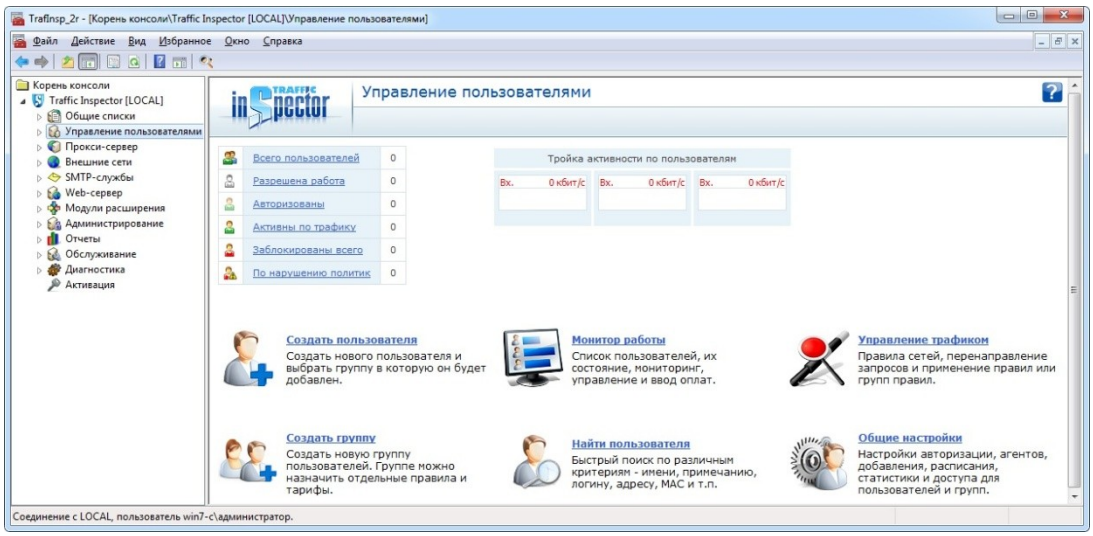


Рисунок 3.29 - Управление пользователями

16) В окне добавления клиента мы можем задать его имя, способ авторизации, время доступа и другие необходимые нам параметры (подробнее см. в справке, она доступна в любом окне консоли по нажатию F1).

17) Чтобы клиент мог пользоваться Интернетом он должен авторизоваться. Авторизация может быть разной в зависимости от выбранного способа (логин, IP, MAC и.т.п). Отдельно стоит отметить возможность авторизации через клиентского агента. В нем пользователь может видеть свой баланс, а также переключать режимы кэширования и блокировки. Агента можно загрузить с встроенного Веб-сервера программы, который доступен по адресу http:\\<имя сервера>:8081, где "имя сервера" - это сетевое имя или IP компьютера на котором установлен Traffic Inspector (в нашем случае http:\\192.168.137.1:8081). В настройках агента необходимо указать имя сервера или IP адрес его внутреннего интерфейса (в нашем случае 192.168.137.1).



Рисунок 3.30 - MyServer

2.5 Оценка расходов на проектирование IT-инфраструктуры предприятия

2.5.1 Оценка расходов на проектирование локальной сети и доступа в интернет

Расходы на комплектующие изделия определяются прямым счётом по форме, приведённой в таблице 4.1. Список используемого оборудования и материалов для создания ЛВС. Транспортные расходы принимаются в размере 13–15% от общей стоимости готовых изделий.

Таблица4.1 – Расчёт покупных изделий

№ п/п	Наименование материалов	Единица измерения	Количество	Цена, руб.	Сумма, руб.
1	Сервер Pentium IV 3000	шт.	1	75 000	75 000
2	Коммутатор 3COMBaselineSwitch 2948-SFPPlus	шт.	1	42 888	42 888
3	Маршрутизатор HP MSR900	шт.	1	28 310	66 700
4	Рабочие станции	шт.	28	11 600	324 800
5	Кабель 10 Base T Level 5	метр	600	4	2 400
6.	Розетки RJ45	шт.	30	40	1 200
7.	Короб	метр	150	80	12 000
8.	Програмный пакет Traffic Inspector NAT	шт.	1	3 480	3 480
9.	Microsoft Office	шт.	28	7 250	203 000
	Итого			**705 365**	

Заключение

В рамках дипломной работы были достигнуты следующие основные результаты:

1. Произведен анализ структуры предприятия ООО «Арт-График», его деятельности, а также характеристики его подразделений.
2. Поставлена цель внедрения, а также определены основные требования проектирования IT-инфраструктуры для данного предприятия.
3. Рассмотрены технологии доступа для организаций и произведен их сравнительный анализ.
4. Обоснован выбор оборудования для подключения, программного обеспечения.
5. В специальной части была произведена разработка схемы локально вычислительной сети предприятия.
6. Рассмотрена установка оборудования и настройка соответствующего программного обеспечения.

Задача создания компьютерной сети ООО «Арт-График», для данной организации выполнена.

Список использованных источников

1. А.В. Гаврилов «Локальные сети ЭВМ». - М.: Издательство «Мир», 2007
2. Парфенов Ю.А. Кабели электросвязи / Ю.А. Парфенов. – М.: Эко-трендз, 2003.
3. Сайт компании deps /Практика проектирования пассивных оптических сетей
4. Портнов Э. Л. Оптические кабели связи и пассивные компоненты волоконно-оптических линий связи / Э.Л. Портнов. – М.: Горячая линия – Телеком, 2007.– 464 с.
5. Цех сетей передачи данных ОАО «Ростелеком», 2013
6. Шварц, М. Сети связи: протоколы, моделирование и анализ: в 2"х ч. Ч. I: пер. с англ. – М.: Наука, 1992.
7. Орлов С. Оптика вплотную с клиентами / С. Орлов // LAN. – 2003. – №5. – С. 50-60.
8. Сайт фирмы ООО "БиС-Пром", раздел виды работ [Электронный ресурс], режим доступа: http://bisprom/builidng/, свободный
9. ГОСТ Р 15971-08. Системы обработки информации. Термины и определения
10. Минаев И.Я. 100% самоучитель. Локальная сеть своими руками (+ CD ROM) / - М.: СПб. [и др.] : Питер, 2010. - 368 с.
11. Москвин Э. К. Локальная сеть без проводов / Э.К. Москвин. - М.: НТ Пресс, 2010. - 128 с.
12. Назаров, С. В. Администрирование локальных сетей Windows NT / 2000 / .NET / - М.: Финансы и Статистика, 2011. - 480 с.
13. Нанс Б.А, Компьютерные сети / - М.: Наука, 2014. - 400 с.
14. Новиков, Ю.В., Аппаратура локальных сетей: функции, выбор, разработка / - М.: Высшая школа, 2011. - 288 с.
15. Поляк-Брагинский А.Н., Локальная сеть под Linux. - М.: БХВ-Петербург, 2011. - 240 с.
16. Пятибратов А.П., Вычислительные системы, сети и телекоммуникации / - М.: Огни, 2010. - 400 с.
17. Рассел Д., Локальная вычислительная сеть / - М.: Книга по Требованию, 2012. - 102 с.
18. Расстригин Л.А., Вычислительные машины, системы, сети… / - Л.: Наука, 2015. - 224 с.
19. Росс К. Компьютерные сети / К. Росс, Дж. Куроуз. - М.: СПб: Питер; Издание 2-е, 2013. - 768 с.

20. Свами М. В. Графы, сети и алгоритмы / - Москва: Гостехиздат, 2010. - 979 с.
21. Соколов А.В., Защита информации в распределенных корпоративных сетях и системах / - М.: ИЛ, 2015. - 656 с.
22. Стефанюк В.Л., Локальная организация интеллектуальных систем / - Москва: Огни, 2014. - 949 с.
23. Хепп К., Аналитические свойства амплитуд рассеивания в локальной квантовой теории поля/ - Москва: Мир, 2012. - 318 с.
24. Гук М., Аппаратные средства локальных сетей / - М.: СПб: Питер, 2012. - 574 с.
25. Браун Стивен. Виртуальные частные сети: Пер. с англ./ –М.: «Лори». – 2001.
26. Вакка Д. Безопасность Intranet: Пер. с англ./ –М.: «Бук Медиа Паблишер». –2015.
27. Дунаев С. INTRANET – технологии. WebDBC. CGI. CORBA 2.0. Netscape. Suite. IntraBuilder. Java. JavaScript UveWire./ –М.: «Диалог-МИФИ». –1997.
28. Микита Р.М., Рогозов Р.М., Свиридов А.С., Стукотий Л.Н. Концепция построения информационной модели предприятия, 2010.
29. Научные основы организации управления и построения АСУ / Под ред. В.Л. Бройдо, В.С. Крылова. - М.: Высшая школа, 2006.

Карта сети предприятия ООО «Арт-График» **Приложение 2**

