

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	5
1 ОБЗОР ЛИТЕРАТУРЫ	6
1.1 Общие сведения о локальной компьютерной сети	6
1.2 Основные характеристики локальных сетей	6
1.3 Топологии локальных сетей	7
1.4 Коммутация компьютерных сетей	8
1.5 Маршрутизация компьютерных сетей	9
1.6 Технологии подключения к Internet	10
1.7 Технология Wi-Fi	11
1.8 Адресация в локальной компьютерной сети	11
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ	13
2.1 Основные характеристики компании	13
2.2 Топология локальной компьютерной сети	14
2.3 Логическая структура проектируемой сети	15
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ	16
3.1 Обоснование выбора сетевой операционной системы	16
3.2 Администрирование, серверная часть сети	17
3.3 Обоснование выбора активного сетевого оборудования	19
3.3.1 Коммутатор	20
3.3.2 Маршрутизатор	21
3.3.3 Беспроводная точка доступа	21
3.3.4 Принтеры	23
3.4 Адресация локальной сети	25
3.5 Настройка VLAN	26
3.6 Настройка доступа в Internet	27
3.7 Настройка web-сервера	28
3.8 Настройка сервера резервного копирования	28
3.9 Настройка беспроводной точки доступа	30
3.10 Настройка персональных компьютеров	31
3.11 Настройка принтеров	31
4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ ..	33
4.1 Организация рабочих мест	33
4.2 Изделия и материалы	33
4.3 Монтаж устройств	34
ЗАКЛЮЧЕНИЕ	35
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	36
ПРИЛОЖЕНИЕ А Схема структурная	37
ПРИЛОЖЕНИЕ Б Схема СКС функциональная	38
ПРИЛОЖЕНИЕ В План первого этажа	39
ПРИЛОЖЕНИЕ Г План второго этажа	40
ПРИЛОЖЕНИЕ Д Перечень оборудования, изделий и материалов	41
ПРИЛОЖЕНИЕ Е Ведомость документов	42

ВВЕДЕНИЕ

В данной курсовой работе предполагается реализовать локальную компьютерную сеть для компании по разработке Java-приложений.

Компьютерные сети являются одним из важнейших столпов любой современной сферы деятельности. Буквально всё: заводы, аграрные предприятия, компании, школы, научные лаборатории и игровые студии – нуждается в компьютерных сетях. Именно благодаря им человечество способно практически моментально обмениваться информацией и данным, что существенно ускоряет двигатель прогресса и повышает общую образованность населения.

Одной из главных особенностей компьютерных сетей является то, что они представляют собой систему, характеристики которой в целом значительно превышают соответствующие характеристики простой суммы составляющих элементов сети при отсутствии связи между ними. Для современных компаний безопасный и стабильный доступ к глобальной сети является «жизненно необходимым». В настоящее время использование вычислительных сетей даёт предприятию многочисленные возможности. Конечной целью использования вычислительных сетей на предприятии является повышение эффективности его работы, которое может выражаться, например, в увеличении производительности внутренних процессов предприятия, и как следствие – повышение прибыли.

Безусловно, вычислительные сети имеют и свои проблемы, например, сложности с совместимостью программного обеспечения, проблемы с транспортировкой сообщений по каналам связи с учётом обеспечения надёжности и производительности, но главным доказательством эффективности является бесспорный факт их повсеместного распространения. Всё больше и больше появляются крупные сети с сотнями рабочих станций и десятками серверов. Естественно, с другой стороны, обеспечение безопасности и работоспособности компьютерных сетей может быть довольно дорогостоящим, поэтому всегда стоит находить компромисс между всеми этими составляющими, так как не всегда затраченные средства на создание и поддержку компьютерной сети будут превышать полезность ее работы.

Целью данной курсовой работы является разработка архитектуры компьютерной сети для компании по разработке Java-приложений. Рассматриваются следующие пункты: планирование топологии, выбор оборудования для создания сети, размещение данного оборудования в помещениях, а также его последующее соединение и настройка.

Подводя итог, в век информации любому бизнесу необходимо использовать компьютерные сети в той или иной мере, чтобы оставаться конкурентоспособным, в особенности компаниям, функционирующим в IT-сфере.

1 ОБЗОР ЛИТЕРАТУРЫ

При написании данной работы были использованы научная и учебно-методическая литература, справочный и практический материал и схемы сетевого аппаратного обеспечения, находящиеся в открытом доступе. Исходя из полученных данных далее представлено описание основных компонентов и понятий, необходимых для разработки и исправного функционирования данного проекта.

1.1 Общие сведения о локальной компьютерной сети

Компьютерная сеть позволяет соединить несколько различных устройств в одну систему, внутри которой может происходить обмен данными. Главными элементами таких сетей являются компьютеры, но в них также могут участвовать и принтеры, сетевое оборудование, серверы, хранилища, телевизоры, телефоны и другие устройства. Все эти устройства называются оконечными узлами. Но в сети также присутствуют и промежуточные элементы – это различные маршрутизаторы, роутеры, модемы, точки беспроводного доступа, коммутаторы. Всё это соединяется между собой с помощью так называемой сетевой среды. Сетевая среда — это оптоволоконные кабели, радиоволны Wi-Fi, витые пары, с помощью которых все устройства подключаются к сети и взаимодействуют между собой [1].

Компьютерные сети бывают локальными (LAN) и глобальными (WAN). Первые располагаются на ограниченной территории, зачастую в пределах одного здания, а вторые могут распространяться на куда большую площадь – расстояние между узлами может составлять сотни и тысячи километров. В данному курсовом проекту разрабатывается локальная сеть на двух этажах бизнес-центра.

Стоит отметить, что различия между локальными и глобальными компьютерными сетями потихоньку стираются. Это связано с улучшением и тех, и других. Возможно, в ближайшем будущем между ними уже не будет значительной разницы [2].

1.2 Основные характеристики локальных сетей

Локальная сеть подходит для использования на ограниченной территории – например, в квартире, офисе или целом здании, но не более. Она обеспечивает быструю передачу данных между узлами сети. Это позволяет пользователю LAN, например, использовать удалённый диск со скоростью, сравнимой с использованием HDD на своём компьютере.

В локальных сетях используются высококачественные линии связи. Наиболее распространены сейчас медные витые пары и оптоволоконные кабели. Это даёт возможность отказаться от подтверждения получения пакета, модуляции и некоторых других методов, которые снижают скорость передачи и усложняют использование сети.

Локальная сеть предполагает совместное использование каналов. Это означает, что одним и тем же каналом связи могут пользоваться разные узлы сети.

Всё вышеперечисленное даёт локальной сети ряд преимуществ:

- быструю передачу данных;
- относительную простоту настройки;
- низкая сложность методов передачи;
- возможность использования дорогой сетевой среды.

Но у локальной сети присутствует серьёзный минус – слабая масштабируемость. Вместе с увеличением количества узлов и протяжённости линий резко снижается скорость передачи данных [3].

1.3 Топологии локальных сетей

Топология – это то, как и в каком порядке устройства сети связываются между собой и передают данные. Рассмотрим возможные виды физической топологии, указав плюсы и минусы каждого [4]:

1 Шинная. Эта физическая топология появилась раньше всех. Она работает по следующему принципу – к одному длинному кабелю с помощью трансиверов подсоединяются все устройства сети. Любой сигнал или пакет данных, отправленный одним из компьютеров сети, направляется на все остальные. Только после приёма пакета элемент сети проверяет, ему ли адресовано «сообщение». Если да, то продолжает обработку. А если нет – отбрасывает и заканчивает работу с этим пакетом. Сейчас такую топологию почти не применяют из-за низкой отказоустойчивости. Любое повреждение основного кабеля приводило к полной неисправности всей сети.

2 Кольцевая. Каждый компьютер подключается к двум соседним, и в итоге должно получиться замкнутое кольцо. При такой топологии компьютер передаёт данные в одну сторону, а принимает с другой. Это означает, что пакет данных, который направлен, например, из первого компьютера кольца к четвёртому, должен пройти ещё промежуточные узлы в виде второго и третьего. А если второй компьютер захочет что-то отправить первому, то пакету данных придётся совершить полный круг – и подойти к первому элементу узла с другой стороны. Минусы очевидны – низкая отказоустойчивость, низкая скорость работы, частые ошибки. Здесь, как и при шинной топологии, при поломке кабеля на одном участке сеть приходит в негодность.

3 Звёздная топология. Все элементы сети подключаются к центральному, который играет роль ретранслятора. Многие локальные сети сейчас работают именно с такой топологией, используя в качестве центра «звезды» коммутатор. Главным плюсом здесь является высокая отказоустойчивость при лёгкой установке. Даже если один из элементов сетевой среды выйдет из строя, то вся сеть продолжит работать. Доступ к ней потеряет только то устройство, у которого разорвалось соединение с ретранслятором. Однако

если сломается центральное звено, то вся сеть перестает быть работоспособной.

4 Полносвязная. Эта топология – самая отказоустойчивая. Каждый элемент сети напрямую связывается со всеми остальными. Чтобы прекратить работу сети, нужно вывести из строя все кабели. Главный минус — высокая стоимость такого подключения.

5 Неполносвязная. Данная топология представляет собой упрощённую версию полносвязной. Вместо того, чтобы соединять все конечные устройства со всеми, пропускается несколько кабелей таким образом, чтобы все элементы сети имели доступ друг к другу. Результатом является высокая отказоустойчивость, достигаемая за счёт меньших затрат.

6 Смешанная или древовидная. Эта топология наиболее распространена в крупных компаниях. Она представляет собой древовидную структуру – очень разветвлённая и состоящая из отдельных «ветвей» или площадок. Обрыв связи ограничит доступ только нескольким или даже одному элементу сети, не затронув сеть целиком. Такая система очень гибкая – она позволяет настраивать каждую площадку нужным образом, основываясь на других топологиях.

1.4 Коммутация компьютерных сетей

В традиционных телефонных сетях, связь абонентов между собой выполняется с помощью коммутации каналов связи. В начале коммутация телефонных каналов связи выполнялась вручную, далее коммутацию выполняли автоматические телефонные станции (АТС).

Аналогичный принцип используется и в вычислительных сетях. В качестве абонентов выступают территориально удаленные вычислительные машины в компьютерной сети. Физически не представляется возможным предоставить каждому компьютеру свою собственную не коммутируемую линию связи, которой они пользовались бы в течении всего времени. Поэтому практически во всех компьютерных сетях всегда используется какой-либо способ коммутации абонентов (рабочих станций), выполняющий возможность доступа к существующим каналам связи для нескольких абонентов, для обеспечения одновременно нескольких сеансов связи.

Коммутация – это процесс соединения различных абонентов коммуникационной сети через транзитные узлы. Коммуникационные сети должны обеспечивать связь своих абонентов между собой [5].

Рабочие станции подключаются к коммутаторам с помощью индивидуальных линий связи, каждая из которых используется в любой момент времени только одним, закрепленным за этой линией, абонентом. Коммутаторы соединяются между собой с использованием разделяемых линий связи (используются совместно несколькими абонентами).

Три основные наиболее распространенные способы коммутации абонентов в сетях:

– коммутация каналов (circuit switching) - подразумевает образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами. Отдельные каналы соединяются между собой специальной аппаратурой – коммутаторами, которые могут устанавливать связи между любыми конечными узлами сети. В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал;

– коммутация пакетов (packet switching) – это особый способ коммутации узлов сети, который специально создавался для наилучшей передачи компьютерного трафика. Опыты по разработке самых первых компьютерных сетей, в основе которых лежала техника коммутации каналов, показали, что этот вид коммутации не предоставляет возможности получить высокую пропускную способность вычислительной сети. При коммутации пакетов все передаваемые пользователем сети сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами.;

– коммутация сообщений (message switching) – разбиение информации на сообщения, каждый из которых состоит из заголовка и информации. Это способ взаимодействия, при котором создается логический канал, путем последовательной передачи сообщений через узлы связи по адресу, указанному в заголовке сообщения. При этом каждый узел принимает сообщение, записывает в память, обрабатывает заголовок, выбирает маршрут и выдает сообщение из памяти в следующий узел.

1.5 Маршрутизация компьютерных сетей

Маршрутизация служит для приема пакета от одного устройства и передачи его по сети другому устройству через другие сети. Маршрутизаторы направляют трафик во все сети, составляющие объединенную сеть [6].

Для маршрутизации пакета маршрутизатор должен владеть следующей информацией:

- адрес назначения;
- соседний маршрутизатор, от которого он может узнать об удаленных сетях;
- доступные пути ко всем удаленным сетям;
- наилучший путь к каждой удаленной сети;
- методы обслуживания и проверки информации о маршрутизации.

Маршрутизатором, или шлюзом, называется узел сети с несколькими IP-интерфейсами (содержащими свой MAC-адрес и IP-адрес), подключенными к разным IP-сетям, осуществляющий на основе решения задачи маршрутизации перенаправление дейтаграмм из одной сети в другую.

Маршрутизаторы представляют собой либо специализированные вычислительные машины, либо компьютеры с несколькими IP-интерфейсами, работа которых управляется специальным программным обеспечением.

1.6 Технологии подключения к Internet

В современном мире трудно оспорить важность постоянного, надежного и доступного соединения с сетью Интернет. Теперь выход в Интернет нужен не только дома, со стационарного компьютера, но и особое значение приобретает выход в сеть с мобильных устройств. Обеспечивают всестороннюю связь устройства с интернет, технологии подключения интернета. На сегодня это шесть активно используемых технологий [7]:

- ADSL;
- DOCSIS;
- FTTP;
- PON;
- интернет мобильных устройств;
- интернет через спутник.

Например, в домах распространена технология домашнего интернета FTTP либо PON, а в транспорте мобильный интернет.

Технология PON наиболее передовая технология передачи Интернет сигнала. Оптическое волокно предоставляет возможность передавать данные большого объема и с большой скоростью, в том числе такие требовательные к стабильности сигнала, как голос и видео, но оптический кабель стоит дорого, и выделять для каждого абонента отдельное волокно – несет огромные траты для большинства провайдеров. Мало того, многие абоненты не используют весь потенциал выделенного оптоволокна, и большая его часть "простаивает".

Поэтому была разработана PON-технология – для максимально эффективного и экономного использования возможностей оптоволоконной сети. Основным преимуществом Passive Optical Network является организация подключения нескольких десятков абонентов к сети по одному оптоволокну. Реализовано это с помощью разделения передачи пакетов во времени (протоколы TDM и TDMA), а также разделения приема и передачи данных в разных волновых диапазонах [8].

В данной технологии сигнал адаптируется терминалом OTN, который ставится каждому конечному потребителю, например, в квартиру. Данная технология не имеет ограничений по скорости передачи данных, но разделена на классы: APON/ BPON (Broadband PON) – 155 Мбит/с, EPON (Ethernet PON) 1000 Мбит/с, GPON (Gigabit PON) – скорость от 600 Мбит/с до 2,5 Гбит/с.

У любой технологии имеются свои недостатки, к рассматриваемой относятся следующие:

1. Поломка абонентского терминала может привести к неработоспособности всей подсети. Сети PON менее надежны, и обрывы связи в них случаются чаще.

2. Сети PON более уязвимы: каждое устройство в подсети фактически получает весь трафик, включая пакеты, не предназначенные для этого устройства. Обычно они шифруются, тем не менее технология повышает риск взлома трафика другого человека.

3.Поскольку световой сигнал в сплиттере просто делится без усиления, мощность его с каждым делением снижается. Поэтому размер PON-сетей ограничен: на один оптический терминал (OLT — Optical Line Terminal) допускается максимум 128 абонентских устройства (ONT / ONU — Optical Network Terminal / Optical Network Unit).

4.При полной загрузке (128 активных пользователей) реальная скорость подключения невысока – максимум 20 Мбит/с.

Приведенные выше недостатки следует учитывать при проектировании и разработке сети, что позволит системному администратору в кратчайшие сроки устранить возникающие проблемы.

1.7 Технология Wi-Fi

Wi-Fi – это самая популярная, доступная и востребованная технология передачи данных в беспроводных компьютерных сетях. При наличии подключения к интернету технология Wi-Fi позволяет распределить интернет-трафик между максимально возможным числом пользователей и/или устройств [9].

За время своего существования с 1996 года Wi-Fi (точнее IEEE 802.11), как и любая технология, прошла несколько стадий своего развития. Соответственно появлялись и различные ее версии. Тестирование на совместимость и сертификацией беспроводных устройств, занимается отдельная организация WECA (Wireless Ethernet Compatibility Alliance) более известная как Wi-Fi Alliance.

Основные характеристики радиоволны, а значит и сигнала Wi-Fi - это ее длина и частота (частотный диапазон). Последний параметр означает частоту переменного тока, необходимую для получения волны нужной длины и используется для классификации радиоволн. Другое определение частоты - это количество волн, проходящих через определенную точку пространства в секунду [10].

Для данной технологии используются дециметровые и сантиметровые волны ультравысокой и сверхвысокой частоты (УВЧ и СВЧ) в частотных диапазонах 2,4 ГГц, 5 ГГц и других редко используемых: 900 МГц, 3,6 ГГц, 10 ГГц, 24 ГГц. Главное преимущество Wi-Fi-связи отражено во втором ее названии - беспроводная связь. Именно отсутствие проводов вкупе со все возрастающей скоростью передачи данных является ключевым моментом при выборе этого способа соединения. Технология Wi-Fi в современном мире используется повсеместно от частных квартир до огромных торговых залов.

1.8 Адресация в локальной компьютерной сети

В локальных сетях используется принцип адресации. Для передачи данных в локальных и глобальных сетях устройство-отправитель должно знать адрес устройства-получателя. Поэтому каждый сетевой компьютер имеет уникальный адрес: физический или аппаратный (MAC-адрес); сетевой

(Internet Protocol, IP); символьный (обычное имя компьютера или полное доменное имя) [11].

Самым распространённым способом является адресация по сетевому адресу, или IP-адрес используется в сетях TCP/IP при обмене данными на сетевом уровне.

Присваивается IP-адрес компьютеру либо вручную (статический адрес), либо компьютер получает его автоматически с сервера (динамический адрес). Статический адрес прописывается администратором сети в настройках протокола TCP/IP на каждом компьютере сети и жестко закрепляется за компьютером.

В присвоении статических адресов компьютерам есть определенные неудобства:

- администратор сети должен вести учет всех используемых адресов, чтобы исключить повторы;
- при большом количестве компьютеров в локальной сети установка и настройка IP-адресов отнимают много времени.

Наряду с перечисленными неудобствами у статических адресов есть одно немаловажное преимущество: постоянное соответствие IP-адреса определенному компьютеру. Это позволяет эффективно применять политику IP-безопасности и контролировать работу пользователей в сети. К примеру, можно запретить определенному компьютеру выходить в Интернет или определить с какого компьютера выходили в Интернет.

Если компьютеру не присвоен статический IP-адрес, то адрес назначается автоматически. Такой адрес называется динамическим адресом, т. к. при каждом подключении компьютера к локальной сети адрес может меняться. К достоинствам динамических адресов можно отнести:

- централизованное управление базой IP-адресов;
- надежная настройка, исключая вероятность дублирования IP-адресов;
- упрощение сетевого администрирования.

Динамический IP-адрес назначается специальной серверной службой DHCP (Dynamic Host Configuration Protocol). Серверная служба DHCP, которая распространяет (сдает в аренду) IP-адреса называется DHCP-сервер. Компьютер, получающий (арендующий) IP-адрес из сети, называется DHCP-клиент.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данной курсовой работе необходимо организовать локальную компьютерную сеть в двухэтажном здании компании по разработке Java-приложений. В разделе описывается структура объекта – IT-компании, определяется общая схема автоматизации, топологии и структура будущей локальной компьютерной сети. Структурная схема представлена в приложении А.

2.1 Основные характеристики компании

Согласно заданию, компания располагается в отдельном двухэтажном здании, которое включает в себя второй этаж, отведенный для разработчиков, и первый для организации рабочего процесса.

Первый этаж включает в себя следующие помещения:

- кабинет директора, в котором находятся одно стационарное и три мобильных подключения;
- комнату для собеседований – 10 мобильных подключений;
- служебное помещение;
- серверную.

Второй этаж является рабочим местом для разработчиков и тестировщиков ПО. Для продуктивной работы в трёх комнатах – 20, 25, 25 м² соответственно – заявлено 14 стационарных и 14 мобильных подключений.

Важным параметром при проектировании локальной компьютерной сети является оборудование, которое будет использоваться компанией. В данном случае сотрудниками используются ПК с web-камерами, личные ноутбуки, личные смартфоны, имеется web-сервер, обычный и цветной принтеры.

Для подключения к Internet используется технология GPON, следовательно, от общего кабеля в помещение протягивают персональный оптический кабель. Его подсоединяют к терминалу, модему типа ONT (Optical Network Terminal). Терминал устанавливают максимально близко к отверстию, через которое протянуто волокно. Кабель нежелательно тянуть далеко, потому что он очень хрупкий, а восстанавливать его сложно и затратно. Важное условие монтажа линии GPON – наличие рядом с дверью розетки для подключения модема.

В плане финансовых затрат имеется возможность выбирать качественное, быстрые и, следовательно, дорогостоящее оборудование с целью достижения максимального комфорта работы сотрудников компании.

Адресация представлена двумя версиями IP – IPv4 и IPv6.

Адрес IPv4 является публичным адресом, выданным провайдером. Публичные IP-адреса – это то, что отличает все устройства, подключенные к общедоступному Интернету. Именно этот адрес каждый провайдер Интернет-услуг использует для пересылки интернет-запросов.

Адрес IPv6 – публичная сеть от провайдера.

Безопасность компьютерных сетей особенно важна в таких компаниях и фирмах, где персонал работает над проектами, имеющими конфиденциальную составляющую. Чтобы уберечь работников и компанию в целом от хакерских атак, взломов, утечек информации, особое внимание нужно уделить защите компьютерной сети. К безопасности проектируемой локальной сети требования не выставлены, однако, используется сервер для резервного копирования, локальная сеть разделена на подсети, а также имеется возможность использовать Firewall для защиты подключения к Internet.

2.2 Топология локальной компьютерной сети

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи. Важно отметить, что понятие топологии относится, прежде всего, к локальным сетям, в которых структуру связей можно легко проследить. В глобальных сетях структура связей обычно скрыта от пользователей и не слишком важна, так как каждый сеанс связи может производиться по собственному пути.

Топология определяет требования к оборудованию, тип используемого кабеля, допустимые и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети.

В данной курсовой работе топология сети – «звезда» – самая распространённая и технологичная система создания сетей. Командует всем сервер, контроллер или коммутатор, а все компьютеры как лучи подсоединены к нему. Общение между ними происходит только через центральное устройство. Топология сети, в которой все компьютеры присоединены к центральному узлу стала основой для построения современных офисных локальных сетей.

В качестве узла используются активные или пассивные коммутаторы. Пассивный – это устройство соединения проводов не требующая питания. Активный коммутатор соединяет схему проводной или беспроводной технологией и требует подключения к питанию, он может усиливать и распределять сигналы. Топология сети «звезда» обрела популярность благодаря множеству достоинств:

- высокая скорость и большой объём обмена данными;
- повреждение передающего кабеля или поломка одного элемента (кроме центрального) не снижает работоспособность сети;
- широкие возможности для расширения, достаточно смонтировать новый кабель или настроить доступ на коммутаторе;
- простая диагностика и ремонт;
- легкий монтаж и сопровождение.

Как и большинство сетей, соединение звезда имеет ряд недостатков, все они связаны с необходимостью использования центрального коммутатора:

- дополнительные затраты;
- поломка коммутатора приводит к неработоспособности всего оборудования;
- число подключаемых устройств и объём передаваемой информации зависит от его характеристик.

Несмотря на недостатки звезда широко используется при создании сетей на больших и маленьких предприятиях.

2.3 Логическая структура проектируемой сети

Логическая структура сети данного курсового проекта основывается на использовании Virtual LAN (далее VLAN). Виртуальные сети созданы, чтобы реализовать сегментацию сети на коммутаторах, т.е. на втором уровне модели OSI. Создание VLAN, которые представляют собой логическое объединение групп рабочих станций сети, является одним из основных методов защиты информации и повышения производительности сетей пакетной коммутации на коммутаторах.

Обычно VLAN группируются по функциональным особенностям работы, независимо от физического местоположения пользователей. Обмен данными происходит только между устройствами, находящимися в одной сети VLAN. Виртуальные сети логически сегментируют всю сеть на широковещательные домены так, чтобы пакеты пересылались только между портами, которые назначены на ту же самую VLAN.

В разрабатываемой сети используются следующие подсети:

- административная подсеть, позволяющая сетевому или системному администратору управлять локальной сетью компании;
- подсеть для стационарных подключений – организована с целью создания стабильного рабочего процесса на стационарных устройствах компании;
- подсеть для мобильных подключений – аналогична предыдущей, но нацелена на мобильные подключения, например, личные ноутбуки или мобильные телефоны сотрудников;
- подсеть для резервного копирования, представляющая собой Backup-сервер для увеличения надежности сети и обеспечения сохранности данных.

Использование других логических отделов на данном момент не целесообразно, все необходимые функции с достаточной безопасностью и удобством можно реализовать в вышеперечисленных VLAN.

В связи с небольшим размером компании и отсутствием сложных архитектурных условий, лучшим выбором при проектировании сети будет использование архитектуры «router-on-a-stick». Роутер на палочке – это термин, часто используемый для описания схемы, состоящей из маршрутизатора и коммутатора, которые соединены с использованием одного канала Ethernet. В этой схеме на коммутаторе настроено несколько VLAN и маршрутизатор выполняет всю маршрутизацию между различными VLAN.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе детально описывается функционирование программной и аппаратной составляющей разрабатываемой локальной сети. Функциональная схема структурирования кабельных сетей представлена в приложении Б.

3.1 Обоснование выбора сетевой операционной системы

Финансовые возможности заказчика позволяют разработать полноценную коммерческую сеть. Наиболее надежным и гибким вариантом является использование оборудования американской компании Cisco. Обоснование выбора данного бренда представлено следующими критериями:

1 Охват. У решений Cisco нет конкурентов по этому параметру. Наиболее широкая линейка по всем сетевым решениям, от рынка SOHO до провайдерских решений, от небольших, но функциональных маршрутизаторов, до систем управления сетями крупных предприятий.

2 Надежность. Надежность Cisco проверена годами успешной эксплуатации.

3 Гибкость. Одно и то же оборудование, в зависимости от операционной системы и оснащении модулями, может выполнять совершенно различные функции: защитные, шлюза унифицированных коммуникаций, сервисные... Это, в свою очередь, позволяет не покупать оборудование, а просто написать несколько соответствующих команд.

4 Взаимозависимость. Разное оборудование, выполняющее разные функции, могут зависеть друг от друга и управлять друг другом. Это позволяет сделать сеть «живым» организмом, а не набором разрозненных устройств.

5 Отладка. Очень важно для настройки и настройщиков: широчайшие возможности по поиску неисправностей, встроенные практически во все устройства Cisco.

6 Интеллектуальность. Все устройства Cisco содержат широкий спектр технологий, протоколов, идеологий, как стандартных, так и своих собственных, позволяющих расширить возможности сети.

7 Производительность. Компания Cisco является лидером во многих сегментах рынка и должна соответствовать этому высокому званию. Поэтому появляются уникальные решения, типа CRS.

8 Централизация. Устройствами Cisco можно управлять не по одиночке, а используя мощные комплексы, например, Cisco Security Manager. Также централизованно можно собирать всевозможнейшую статистику и анализировать её – MARS.

Для работы с устройствами Cisco используется собственная операционная система – Cisco IOS (от англ. Internetwork Operating System – Межсетевая Операционная Система) – семейство операционных систем, используемых в большинстве роутеров и коммутаторов производства Cisco Systems (ранние коммутаторы использовали CatOS). IOS - это комплекс для

управления маршрутизаторами, коммутаторами, межсетевыми и телекоммуникационными функциями, интегрированный в мультизадачную операционную систему. Хотя IOS и базируется на ядре с совместной многозадачностью, многие функциональные возможности системы переносятся на другие ядра, такие как QNX и Linux, например, продукты безопасности ASA.

Управление устройствами с IOS происходит при помощи интерфейса командной строки (CLI), при подключении при помощи консольного кабеля, по Telnet, SSH либо при помощи AUX порта.

3.2 Администрирование, серверная часть сети

Для постоянного функционирования локальной сети используется сервер – это специализированный программно-аппаратный комплекс, предназначенный для обслуживания сети организации. Серверы решают множество различных задач: начиная с простого файлового хранилища с защитой от потери информации или управлением доступом к сети Интернет, до задач по обработке данных.

На начальном этапе развития компании в роли сервера может выступать обычный ПК с установленным специализированным ПО, обычно данного решения достаточно при штате сотрудников менее 20 человек, но всё зависит от сферы деятельности организации, а в IT-сфере данные – самый дорогой актив компании. С ростом организации повышенное требование предъявляется к надёжности работы сети и сохранности данных, что нельзя обеспечить средствами обычного ПК. Хотя профессиональное и потребительское оборудование во многом схоже, именно упор на некоторые функции и качества позволяет отнести аппаратное обеспечение к профессиональному уровню. Например, домашний ПК должен быть быстрым, тихим, с возможностью модернизации и, конечно, за разумные деньги. Он проработает несколько лет, при этом зачастую будет простаивать по несколько часов, и у пользователя будет возможность заменить вышедший из строя компонент или просто убрать накопившуюся пыль. К серверам предъявляются иные требования: здесь на первом месте стоят надёжность, доступность в режиме 24/7, техническое обслуживание без остановки работы.

В данной курсовой работе используется стоечный сервер Cisco UCS серии C, которые можно использовать в качестве полноценных автономных машин или интегрировав их в Cisco UCS (Unified Computing System). В разрабатываемой сети выбран первый вариант, и серверы будут управляться при помощи встроенного в сервер контроллера Cisco Integrated Management Controller (CIMC).

На момент проектирования сети на официальном сайте cisco.com предложено шесть стоечных серверов:

- стоечный сервер UCS C125 M5;
- стоечный сервер UCS C220 M5;
- стоечный сервер UCS C240 M5;

- стоечный сервер UCS C240 SD M5;
- стоечный сервер UCS C480 M5;
- стоечный сервер UCS C480 ML M5.

Первые сервера из представленного списка являются бюджетными и подходят для малого бизнеса, последние, в свою очередь, используются как системы управления предприятием, что на данный момент является избыточным. Золотой серединой являются сервера модели C240, конкретно в курсовом проекте будут использоваться стоечный сервер UCS C240 SD M5 – для администрирования сети и для создания web-сервера. Основные характеристики выбранного оборудования представлены в таблице 3.1 и внешний вид представлен на рисунке 3.1.

Таблица 3.1 – Характеристики сервера UCS C240 SD M5

Процессоры	Два Intel® Xeon® Scalable processors (Second Generation)
Память	24 DDR4 DIMM ячейки: 8, 16, 32, 64, и 128 GB и до 2933 MHz Поддержка Intel® Optane™ PMem (128G, 256G, 512G)
Расширение PCIe	6 PCIe 3.0 + один дополнительный 12-Gbps контроллер RAID и один дополнительный слот mLOM
Внутреннее хранилище	До 6 2,5-дюймовых дисков NVMe, SAS или SATA.
Встроенные карты сетевого интерфейса (NIC)	Два порта 10GBASE-T Intel x550 Ethernet
Питание	Резервные источники питания переменного тока мощностью 1050 Вт с возможностью горячей замены



Рисунок 3.1 – Стоечный сервер UCS C240 SD M5

Для резервного копирования данных компания Cisco предлагает сервер хранилищ данных S3260 M5. Данное оборудование позволит сохранять данные компании и, в случае выхода из строя какого-либо административного оборудования, позволит восстановиться практически без потерь. Внешний вид хранилища представлен на рисунке 3.2. Основные характеристики следующие:

- двойные серверные узлы на базе процессоров Intel® Xeon® Scalable 2-го поколения и процессоров Intel Xeon Scalable;
- постоянная память Intel® Xeon® Optane™ DC;
- общее хранилище данных до 960 терабайт;
- расширение ввода-вывода для сторонних карт расширения PCIe;
- управление хранилищем на основе политик.



Рисунок 3.2 – Сервер хранилищ данных S3260 M5

Согласно заданию, в здании имеется серверная, следовательно, описанные выше сервера необходимо установить в специальную серверную стойку. Для этого используется стойка Cisco серии R. Стандартные стойки и стойки расширения Cisco серии R идеально подходят для установки Cisco UCS с одной или несколькими стойками на объектах заказчиков. Предварительная проверка продуктов Cisco UCS в стойках не от Cisco приводит к аннулированию гарантии Cisco UCS.

Данная стойка предусматривает систему охлаждения и функции оптимизации прокладки кабелей, источники питания и стабилизаторы для стоек, обеспечивает простую установку и использование, стабилизирующие ножки для безопасной установки ИТ-оборудования, предусматривает варианты укладки кабелей без инструментов и U-маркировку.

3.3 Обоснование выбора активного сетевого оборудования

В данном подразделе описывает выбор активных компонентов сети, такие как маршрутизатор, коммутатор, точка беспроводного доступа и рабочие станции. Полный перечень оборудования представлен в приложении Д.

3.3.1 Коммутатор

Коммутаторы являются базовыми составляющими компьютерной сети большинства предприятий. Данное устройство в курсовом проекте работает на втором уровне модели OSI. Существует различные виды коммутаторов для самых разнообразных сетей: модульные, неуправляемые и управляемые, подробнее о коммутаторах описано в разделе 1.

Далее будут рассматриваться только управляемые коммутаторы, по той причине, что необходимо создать и настроить VLAN в разрабатываемой сети.

Управляемые коммутаторы предоставляют самый широкий спектр функций и гарантируют самую удобную работу с приложениями, самый высокий уровень безопасности, самый точный контроль и управление сетью. Именно поэтому управляемые коммутаторы часто внедряют в качестве коммутаторов агрегации/доступа в очень крупных сетях или в качестве коммутаторов уровня ядра в относительно небольших сетях.

Компания Cisco предлагает большой выбор коммутаторов для локальной сети среднего количества конечных устройств. В серии устройств Cisco 350 Series Managed Switcher присутствуют все параметры, удовлетворяющие требованиям проектируемой сети, например, большое количество портов – 48, Power of Ethernet для питания беспроводной точки доступа без необходимости использования отдельной розетки.

Полноценное название выбранного коммутатора – Cisco SG350-52P 52-Port Gigabit PoE Managed Switch. Характеристики данного устройства представлены в таблице 3.2, внешний вид представлен на рисунке 3.3.

Таблица 3.2 – Основные характеристики коммутатора SG350-52P

Количество портов	48 RJ-45, 2 SFP, 2 Gigabit Cooper/SFP combo
Питание для PoE	375 Вт
Температура работы	От 0 до 45 С
Акустический шум(при 40 С)	54.2 dB
Охлаждение	Три кулера
Потребляемая мощность	110 В = 62.4 Вт, 220 В = 61.8 Вт



Рисунок 3.3 – Коммутатор SG350-52P

3.3.2 Маршрутизатор

Для построения локальной сети на основе таблицы маршрутизации и организации доступа в Internet по кабелю или беспроводной технологии Wi-Fi необходимо выбрать маршрутизатор. Согласно модели OSI, последний работает на третьем уровне и является точкой выхода данных из локальной сети в Internet.

Как и в случае с коммутаторами Cisco предлагает широкий выбор оборудования. В разрабатываемом проекте для IT-компании следует обратить внимание на возможность шифрования, поддержку VPN, брандмауэра и прочих утилит для обеспечения максимальной защищенности данных, а также стабильной и быстрой работы сети.

Популярным и надежным решением для маршрутизации сетей является оборудование Cisco 4000 серии. Имеется четыре вида аппаратной конфигурации: ISR4221, ISR4331, ISR4431, ISR4461. Для текущего заказчика, а также с учетом финансовых возможностей, идеальным решением будет использование ISR 4451. Данный маршрутизатор включает в себя:

- широчайший спектр функций для настройки различных протоколов и зависимостей;
- имеет шифрующую пропускную способность равную 7 Гбит/с;
- пропускную способность 10 Гбит/с;
- поддерживает PoE.

Для реализации подключения к сети интернет через GPON в данном маршрутизаторе предоставляются два SPF+ порта, которые являются универсальными для любого вида оптических кабелей. Поскольку SFP поддерживает скорость передачи данных только до 4.25Gbps, для передачи данных со скоростью до 16Gbps используется модуль SFP+. Спецификации SFP+ основаны на SFF-8431. В современных приложениях модуль SFP+ обычно поддерживает 8Gbps Fibre Channel, 10 Gigabit Ethernet и стандарт оптической транспортной сети OTU2.

Внешний вид данного устройства представлен на рисунке 3.4.



Рисунок 3.4 – Маршрутизатор Cisco ISR 4451

3.3.3 Беспроводная точка доступа

Кабельные сети не могут покрыть все пространства, где необходим или желателен высокоскоростной интернет. Кроме того, на них влияет топология,

относительная сложность монтажа и ограниченность конечных пользователей сети. Также имеется необходимость подключения личных ноутбуков и мобильных телефонов. При таких обстоятельствах оптимальным решением является использование WLAN.

WLAN (Wireless Local Area Network) – это точка доступа к интернету, современная технология передачи информации посредством радиосигналов, без наличия кабельных соединений. Наличие специальных модулей в смартфонах, планшетах, ноутбуках или стационарных ПК позволяет пользователям получать устойчивый сигнал в границах покрытия

Для реализации WLAN необходимо выбрать точку доступа, которая подключается к проводной сети и преобразует сигнал в беспроводной посредством технологии Wi-Fi.

Характеристиками для выбора оборудования на данный момент является: поддержка основных частот: 2.4 ГГц и 5 ГГц; стандарта Wi-Fi, скорость передачи данных, количества антенн, количество одновременной передачи нескольких потоков, а также стандарты безопасности.

Компания Cisco предоставляет широкий выбор оборудования с новейшими технологиями для самых различных целей, например, расположение точки на улице или для промышленных сред. В данной курсовой работе целесообразно использовать точку доступа серии Catalyst 9100. Имеется пять вариантов аппаратной конфигурации: Catalyst 9105, Catalyst 9115, Catalyst 9120, Catalyst 9124, Catalyst 9130. Последняя точка доступа имеет наилучшие характеристики для использования ее в IT-сфере.

Точки доступа Cisco® Catalyst® 9130AX Series – это следующее поколение корпоративных точек доступа. Они устойчивы, безопасны и интеллектуальны. К сети подключается большое количество устройств от личных ноутбуков до мобильных телефонов сотрудников. Точки доступа Cisco Catalyst серии 9130AX обеспечивают удобство работы в любом месте для всех, с высоким масштабированием и непревзойденной производительностью в различных сетевых развертываниях. Выходя за рамки стандарта Wi-Fi 6 (802.11ax), серия 9130AX обеспечивает интегрированную безопасность, отказоустойчивость и операционную гибкость, а также улучшенный сетевой интеллект.

В данном оборудовании используется технология MIMO (Multiple Input Multiple Output) – это технология, используемая в беспроводных системах связи, позволяющая значительно улучшить спектральную эффективность системы, максимальную скорость передачи данных и емкость сети. Главным плюсом в выборе данной технологии является способность устройства обслуживать большое количество пользователей, что идеально подходит под критерии IT-компаний, где большинство сотрудников имеет несколько мобильных гаджетов.

Имеется возможность вещания в двух частотных диапазонах: 2.4 ГГц и 5 ГГц. Преимущество 5 ГГц сетей заключается в большей скорости соединения и менее "зашумленном" диапазоне, а первое очень сильно зависит

от второго. 5 ГГц точек доступа меньше, они дороже, сигнал затухает быстрее, поэтому соседние сети меньше будут влиять проектируемую сеть. Также здесь нет других источников помех, характерных для 2.4 ГГц диапазона, например, СВЧ-печей и Bluetooth-устройств.

Внешний вид точки доступа изображен на рисунке 3.5.



Рисунок 3.5 – Cisco Catalyst серии 9130AX

3.3.4 Принтеры

Принтер – одно из самых необходимых вещей в офисном помещении. Без него не обойдется даже самый маленький офис, ведь печатать приходится ежедневно. Не любое печатающее устройство подойдет для офиса. Есть некоторые критерии, которым следует придерживаться при его выборе.

1Количество.Первое, о чем следует подумать – объем печати. Недооценка данного параметра повлечет за собой лишнюю переплату.

2Качество. При печати текста особой разницы между принтерами нет. А вот картинки и фотографии – для них требуется более высокое разрешение, которое скажется на конечной цене аппарата.

3Сканирование, копирование. Если эти функции необходимы, следует присмотреться к многофункциональным устройствам – МФУ – гибридам сканера, принтера и копира в одном корпусе.

4Наличие цветной печати. Некоторые документы требуют цветной печати для точного отображения информации.

5Форматы. Поддержка печати множества форматов бумаги позволит использовать гибки использовать один принтер для решения множества задач.

6Тип печати. Существует две основные категории принтеров: лазерный и струйный.

Как уже упоминалось ранее, финансовые возможности соответствуют для разработки полноценной коммерческой сети, следовательно, имеется возможность рассматривать наилучшие вариант из представленных выше критериев оценки.

Одним из таких является HP PageWide Color 755dn. Максимальный формат печати – А3. Устройство отличается высокой производительностью – до 75 тысяч страниц в месяц. Способен выдавать до 41 страниц за минуту. Обработывает любые виды печатных носителей, включая плотные конверты, открытки, грубую бумагу и бумагу из вторсырья. Обладает высокой энергоэффективностью, что позволяет снизить затраты на электроэнергию, имеет поддержку Mac OS, Windows, Linux. Не имеет Wi-Fi модуля для беспроводной печати, однако, имеется возможность подключить в коммутатор через Ethernet. Внешний вид принтера представлен на рисунке 3.6.



Рисунок 3.6 – Принтер HP PageWide Color 755dn

Данный принтер установлен на первом этаже, где находится кабинет директора. В помещение для совещаний установлен черно-белый принтер KYOCERA ECOSYS P3150dn, который имеет сравнительно низкую себестоимость печати, большой ресурс картриджей и прочих узлов, скоростная печать, объем встроенной памяти может быть расширен до 2 ГБ, возможность дооснащения лотками. Из минусов – нет модуля Wi-Fi.

Внешний вид принтера представлен на рисунке 3.7.



Рисунок 3.7 – Принтер KYOCERA ECOSYS P3150dn

3.4 Адресация локальной сети

Для взаимодействия оконечных устройств, а также для доступа в Internet в курсовой работе используется принцип адресации. В разделе 1 описаны виды адресации, на основе этих сведений используются статическая адресация для стационарных устройств, что позволит лучше отслеживать их работу и обеспечить надежную защиту коммерческой тайны и динамическую адресацию для мобильных устройств, чтобы избавить сетевого администратора и сотрудников от необходимости согласовывать каждое новое беспроводное подключение.

Выбор IP-адреса подсети обусловлен рекомендуемыми диапазонами значений для локальных компьютерных сетей. При назначении маски подсети следует учитывать возможное будущее количество добавленных оконечных устройств, что предупредит надобность заново переписывать статическую маршрутизацию. В реализуемом проекте решено использовать маску подсети равную /24, а также установить третье число в IP-адресе соответствующим номеру VLAN, в которой используется данный диапазон.

Диапазон адресов для назначения представлен в таблице 3.3.

Таблица 3.3 – Диапазон адресов локальной компьютерной сети

Назначение VLAN	VLAN ID	IP адрес подсети	Маска подсети
Административный	2	172.16.2.0	/24 (255.255.255.0)
Рабочий стационарный	3	192.168.3.0	/24 (255.255.255.0)
Рабочий мобильный	4	192.168.4.0	/24 (255.255.255.0)
Резервного копирования	5	172.16.5.0	/24 (255.255.255.0)

Ввиду того, что провайдером выделена публичная подсеть IPv6, для выбора конкретных значений адресов используется таблица доступных блоков IPv6 адресов для Беларуси. Для каждого хоста будет выбран global unicast IPv6 адрес из подсети, выданной провайдером, 2a03:c740:1::/64.

3.5 Настройка VLAN

Благодаря популярности оборудования Cisco в свободном доступе имеется большое количество руководств для настройки сети, что достаточно упрощает администрирование сети. Для настройки VLAN используются представленные ниже команды. Переходы в командные режимы Cisco IOS опущены, однако текущий режим при написании команды оставлен. В квадратные скобки заключено обобщённое название параметра.

Создание VLAN'a с идентификатором [ID] и задание имени для него:

```
sw1(config)# vlan [ID]
sw1(config-vlan)# name [VLAN Name]
```

Удаление VLAN'а с идентификатором 2:

```
sw1(config)# no vlan [ID]
```

Порты коммутатора, поддерживающие VLAN'ы, (с некоторыми допущениями) можно разделить на два множества:

- тегированные порты (или транковые порты, trunk-порты в терминологии Cisco).

- нетегированные порты (или порты доступа, access-порты в терминологии Cisco);

Тегированные порты нужны для того, чтобы через один порт была возможность передать несколько VLAN'ов и, соответственно, получать трафик нескольких VLAN'ов на один порт. Информация о принадлежности трафика VLAN'у, как было сказано выше, указывается в специальном теге. Без тега коммутатор не сможет различить трафик различных VLAN'ов.

Настройка access портов:

- назначение порта коммутатора в VLAN:

```
sw1(config)# interface [Port N]
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan [VLAN ID]
```

- просмотр информации о VLAN'ах:

```
sw1# show vlan brief
```

Создание статического транка:

```
sw1(config)# interface [Port N]
sw1(config-if)# switchport encapsulation dot1q
sw1(config-if)# switchport mode trunk
```

В стандарте 802.1Q существует понятие native VLAN. Трафик этого VLAN передается нетегированным. по умолчанию это VLAN 1. Однако можно изменить это и указать другой VLAN как native.

Настройка [VLAN IDk] как native:

```
sw1(config-if)# switchport trunk native vlan [VLAN IDm]
```

Теперь весь трафик принадлежащий VLAN'у IDm будет передаваться через транковый интерфейс нетегированным, а весь пришедший на транковый интерфейс нетегированный трафик будет промаркирован как принадлежащий VLAN'у IDm (по умолчанию VLAN 1).

Настройка VLAN на маршрутизаторах Cisco:

```
R1(config)#interface [Port N]
R1(config-if)#ip address [IP] [mask]
R1(config-if)#ipv6 address [IP] [mask]
```

3.6 Настройка доступа в Internet

В данной курсовой работе внутренняя сеть использует локальную IPv4 адресацию, которая требует трансляции адресов для доступа в глобальную сеть Интернет.

При динамической трансляции создаётся пул возможных внутренних адресов и устанавливается критерий соответствия, для определения того, какие внутренние IP-адреса должны транслироваться с помощью NAT.

Для указания частных IP-адресов, подлежащих трансляции, динамическая трансляция NAT использует списки управления доступом ACL, а также определяет пул зарегистрированных открытых IP-адресов, которые будут выделяться для этого. Алгоритм настройки динамической трансляции следующий:

1. Настроить интерфейсы, которые будут находиться во внутренней подсети, с помощью команды `ip nat inside`.

2. Настроить интерфейсы, которые будут находиться во внешней подсети, с помощью команды `ip nat outside`.

3. Настроить список ACL, соответствующий пакетам, поступающим на внутренние интерфейсы, для которых должна быть применена трансляция NAT.

4. Настроить пул открытых зарегистрированных IP-адресов с помощью команды режима глобального конфигурирования: `ip nat pool (name) (first address) (last address) netmask (mask)`.

5. Включить динамическую трансляцию NAT, указав в команде глобального конфигурирования: `ip nat inside source list (№ acl) pool (pool name)`.

Пример настройки NAT представлен ниже.

Настройка интерфейса в сторону частной сети, в данном случае используется интерфейс, который подключен к коммутатору:

```
Router(config)#interface [interface №]
Router(config-if)#ip address [IP] [mask]
Router(config-if)#no shutdown
Router(config-if)#ip nat inside
Router(config-if)#exit
```

Следующий этап – настройка интерфейса в сторону провайдера, т.е. интерфейс, в который подключается оптоволоконный кабель:

```
Router(config)#interface [interface №]
Router(config-if)#ip address [IP] [mask]
Router(config-if)#no shutdown
Router(config-if)#ip nat outside
Router(config-if)#exit
```

Настройка динамической адресации NAT:


```

Router(config)#ip nat pool [pool name] [first address]
[second address] netmask [mask]
Router(config)#access-list 1 permit [subnet IP] [subnet
inverted mask]
Router(config)#ip nat inside source list 1 pool inPool
Router(config)#ip route 0.0.0.0 0.0.0.0 [IP]

```

Последней командой является назначение статического маршрута в сторону провайдера.

3.7 Настройка web-сервера

Как правило, сервер отдает в сеть свои ресурсы, а клиент эти ресурсы использует. Также, на серверах устанавливаются специализированное программное и аппаратное обеспечение. На одном компьютере может работать одновременно несколько программ-серверов. В разрабатываемом курсовом проекте предполагается реализовать Web-сервер.

Веб-сервер – сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-поток или другими данными. Cisco HTTP (WEB) сервер – позволяет создавать простейшие веб-странички и проверять прохождение пакетов на 80-ый порт сервера.

Для настройки Web-сервера используется Cisco IOS, пример настройки представлен ниже:

```

ip http server
ip http authentication {aaa | enable | local | tacacs}
ip http accounting commands level {default | named-
accounting-method-list}
ip http port port-number
ip http path url
ip http access-class access-list-number
ip http max-connections value
ip http timeout-policy idle seconds life seconds requests
value

```

Данные команды выполняются в режиме конфигурации.

3.8 Настройка сервера резервного копирования

Резервное копирование – это создание копии ваших файлов и папок на дополнительном носителе информации (внешнем жестком диске, CD/DVD-диске, флэшке, в облачном хранилище и т.д.). Резервное копирование необходимо для восстановления данных, если они повредились или разрушились в основном месте их хранения.

Резервное копирование и восстановление конфигурации – конфигурация и файл IOS маршрутизатора или коммутатора могут быть скопированы на FTP или TFTP-сервер. В приведенном ниже примере описывается использование FTP-сервера.

Создайте FTP-сервер с идентификацией по идентификатору пользователя по ID и пароля для обеспечения доступа исключительно администратора сети.

```
R1(Config)#archive
R1(Config-archive)# path ftp://[server IP]/r1-config (name of
the file will be created as - r1-config-1...2)
R1(Config-archive)# write memory (To save the config file on
ftp during write memory command applied)
R1(Config-archive)# time-period 60 mins (auto save the
running config on to FTP after 1 hour)
R1# show archive (To check the configuration file backup)
```

Для восстановления конфигурации используется команда:

```
R1# configure replace ftp://[server IP]/r1-config-3 (name of
the desired file)
```

Касательно данных с рабочих станций сотрудников: для ОС Windows имеется множество популярных утилит для автоматического запланированного копирования на локальный сервер, например Exiland Backup или ArcGIS. Интерфейс первой утилиты представлен на рисунке 3.8.

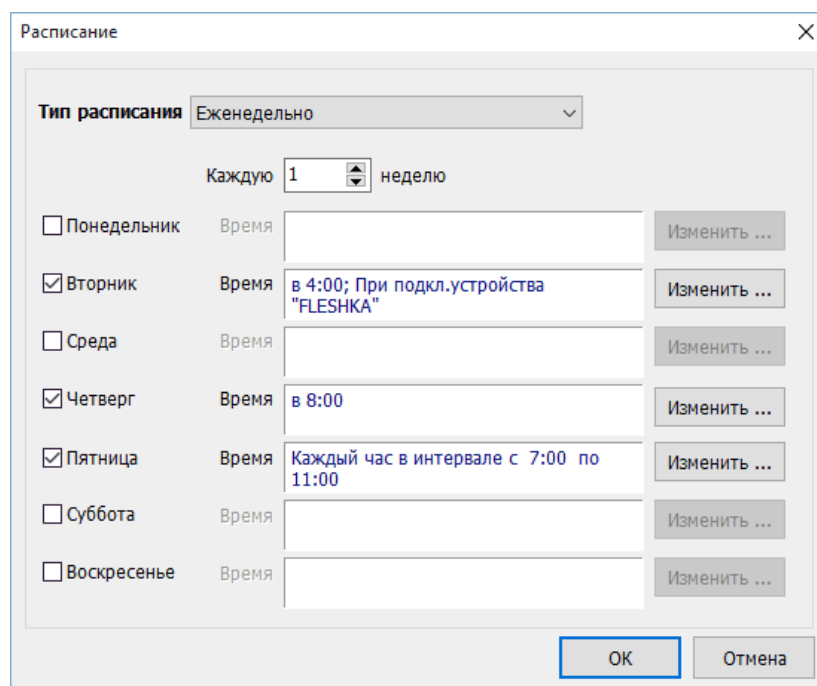


Рисунок 3.8 – Интерфейс утилиты резервного копирования ExilandSoft

Альтернативным вариантом является копирование файлов через SSH с помощью командной строки. Ниже представлены примеры команд. Данный способ нацелен на более продвинутых пользователей ОС Windows.

Скопировать файл по SSH на сервер:

```
pscp [путь к файлу] [имя пользователя]@[имя сервера/ip-адрес]:[путь к файлу]
```

Скачать файл по SSH с сервера командой:

```
rsync [имя пользователя]@[имя сервера/ip-адрес]:[путь к файлу]  
[путь к файлу]
```

Увидеть список папок и файлов на сервере через rsync.exe:

```
rsync -ls [имя пользователя]@[имя сервера/ip-адрес]:[путь]
```

3.9 Настройка беспроводной точки доступа

В данной курсовой работе используется две беспроводные точки доступа Cisco Catalyst серии 9130AX. Для использования беспроводной точки доступа её необходимо заранее настроить. Для перехода к графическому интерфейсу настройки необходимо в адресной строке браузера ввести IP-адрес точки доступа (172.16.4.1).

На вкладке «General» необходимо ввести SSID точки доступа («Admin Wi-Fi»), VLAN ID, шлюз по умолчанию (172.16.4.0), IP-адрес точки доступа в рамках подсети в текстовом поле «Internet IP Address» (172.16.4.1) и адрес внутри WAN в текстовом поле «Router IP Address».

Перейдём к настройке шифрования, для этого нужно перейти на вкладку WLAN и выбрать «Create New». В открывшемся окне нужно выбрать вкладку «Security», в ней «Layer 2». В окне настройки безопасности выбрать тип шифрования «WPA+WPA2», отметить «WPA2 Policy-AES» и «802.1X Enable». Графический интерфейс данной процедуры представлен на рисунке 3.9.

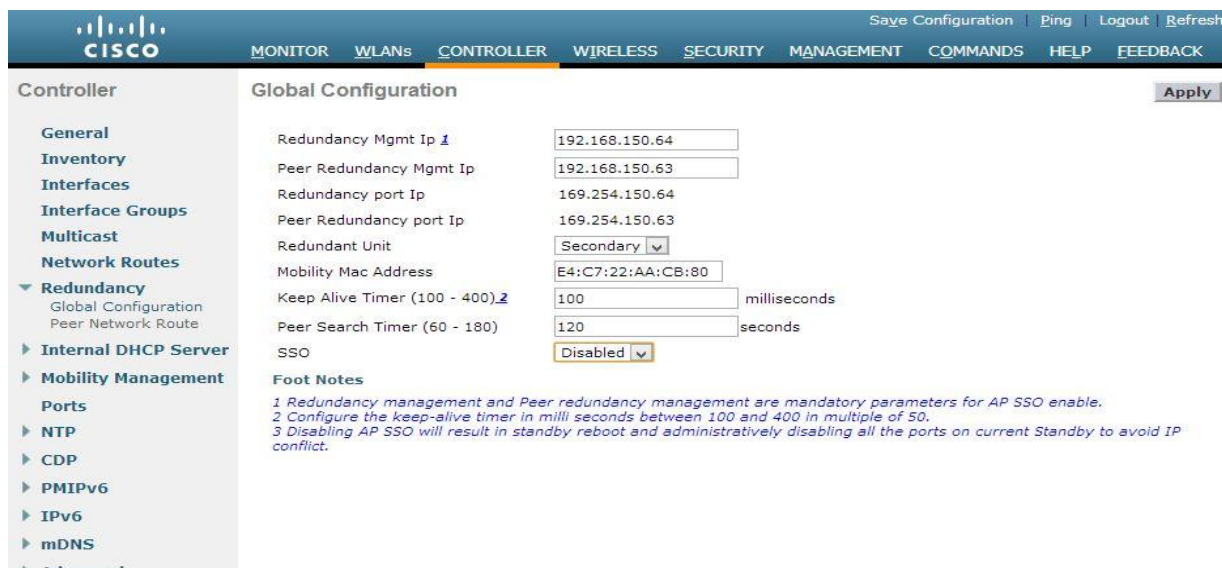


Рисунок 3.6 – Окно настройки WLAN

Для автоматического назначения IP-адресов подключаемым устройствам нужно настроить работу DHCP. DHCP – это протокол, позволяющий раздавать IP-адреса подключаемым устройствам. Он позволяет упростить процесс выдачи адресов, перекладывая эту работу на сторону сервера.

Точка доступа Cisco Catalyst 9130AX поддерживает протокол DHCP, для его настройки также необходимо воспользоваться графическим интерфейсом пользователя. Во вкладке «General» необходимо опуститься до пункта «DHCP Server Settings». В окне настройки нажать кнопку «Enable» напротив «DHCP Server», выбрать начальный IP-адрес для раздачи (172.16.4.2), и выбрать максимальное количество пользователей – для проектируемой сети имеется возможность установить данное значение в 252. Вторая точка доступа настраивается автоматически согласно параметрам, заданным выше.

3.10 Настройка персональных компьютеров

Персональный компьютер администратора подключаются посредством Ethernet. Для настройки администраторского ПК необходимо зайти в панель управления, выбрать раздел «Сеть и Интернет», в разделе «Сетевые подключения» нажать кнопку «Изменение настроек адаптера». В открывшемся окне перейти к настройкам Ethernet, нажать на «IP версии 4», на кнопку свойства и задать в открывшемся окне свойств IP-адрес компьютера, маску подсети и основной шлюз.

Пример настройки представлен на рисунке 3.7. Аналогичным образом настраивается и IPv6 адрес. Для настройки стационарных устройств сотрудников используется такой же принцип.

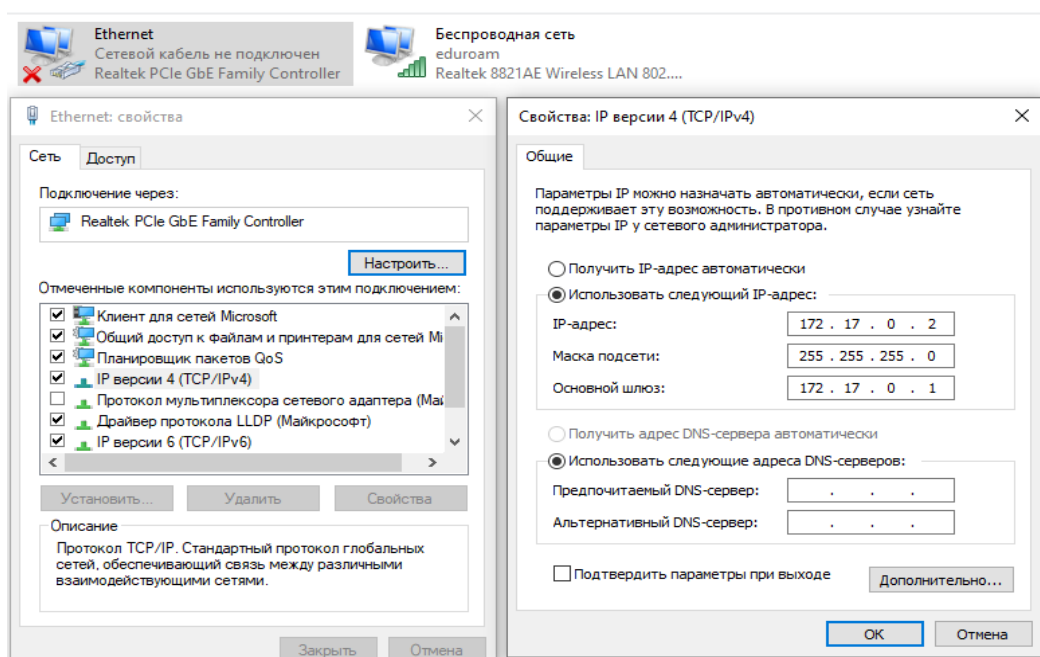


Рисунок 3.7 – Настройка IPv4 на ПК

3.11 Настройка принтеров

Настройка принтера включает в себя инструкцию по подключению принтера к проводной сети. Подключение принтера происходит с помощью прямого Ethernet-кабеля.

Выбранные принтеры являются достаточно популярными и обладают огромной базой различных руководств. Для настройки принтера Принтер HP PageWide Color 755dn следует выполнить следующие пункты:

1.Подключить кабель Ethernet к порту Ethernet (1) и к сети. Порт представлен на рисунке 3.8.

2.Включить устройство.

3.Открыть панель инструментов (потянуть вниз вкладку панели инструментов, расположенную в верхней части любого экрана, или коснуться полосы в верхней части главного экрана).

4.На панели инструментов нажать (Ethernet), чтобы отобразить IP-адрес. Нажмите Печать сведений, чтобы напечатать страницу с IP-адресом.

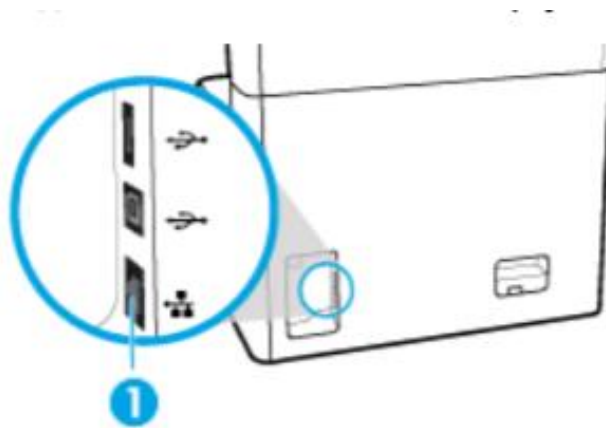


Рисунок 3.8 – Порт для подключения кабеля Ethernet

Принтер KYOCERA ECOSYS P3150dn оборудован сетевым интерфейсом, совместимым с такими сетевыми протоколами, как TCP/IP (IPv4), TCP/IP(IPv6), NetBEUI и IPSec. Он позволяет выполнять сетевую печать в Windows, Linux, Macintosh.

Настройку данного принтера следует начинать с подключения Ethernet-кабеля в соответствующий порт. Следующим этапом является настройка через экран принтера:

- через главное Меню зайти на настройки IPv4;
- возможен выбор адресации: DHCP или статический IP-адрес, по причине того, что в данной курсовой работе принтерам присвоен статический адрес, то выбирается второй пункт;
- задается IP-адрес принтера, маска подсети шлюз по умолчанию и необходимо отключить функцию DHCP и Auto-IP;
- последним шагом является перезагрузка принтера и Перезапуск сети в пункте Сеть.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

В данном разделе описывается проектирование структурированной кабельной системы разрабатываемой локальной сети, обосновывается выбор пассивного сетевого оборудования, а также сопутствующих компонентов системы. План первого и второго этажа представлены в приложениях В и Г, соответственно. Перечень оборудования, изделий и материалов находится в приложении Д.

4.1 Организация рабочих мест

Под рабочим местом понимается часть производственной площади с размещенным на ней технологическим оборудованием и инвентарем, необходимыми для эффективного выполнения поставленных перед работником задач. Рабочее место является первичной ячейкой производственной структуры компании.

Организация рабочего места в данной курсовой работе представляет из себя наличие персональных компьютеров и возможности подключения беспроводных устройств сотрудников к сети компании. Далее оба устройства должны иметь возможность выхода в глобальную сеть Интернет. В качестве персонального компьютера для работы с Java-приложениями и удобного выхода в сеть, может использоваться любая машина, имеющая среднюю производительность, и качественную сетевую карту. Также одним из условий было наличие web-камер, установленных на мониторах сотрудников.

Для подключения ПК к локальной сети достаточно подсоединить в разъем сетевой карты подведенную к рабочему месту витую пару прямого типа RJ-45. Работники могут подключиться по беспроводному каналу в помещениях своих отделов на втором этаже.

По условию требовалось установить в здание два принтера, один чёрно-белый, а второй цветной – оба аналогично подключены витой парой прямого типа RJ-45, как и пользовательские станции.

4.2 Изделия и материалы

Основным типом соединения в построенной топологии является витая пара прямого типа RJ-45. Из-за топологии звезда кабеля потребовалось довольно много. На все соединения около 200 м кабеля. Ещё пять было добавлено в перечень с учётом на обрезки и порчу кабеля.

Витая пара – это вид кабеля связи, представляющий из себя одну или несколько пар изолированных проводников, скрученных между собой и покрытых пластиковой оболочкой. Свивание проводников производится с целью повышения связи проводников одной пары. Благодаря этому электромагнитная помеха одинаково влияет на оба провода пары и компенсирует сама себя. Для снижения связи отдельных пар кабеля в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом.

В данной курсовой работе используются кабели FTP категории 6. Используются они по той причине, что разъёмы активного и серверного оборудования поддерживают Gigabit Ethernet. Также из-за прокладки в одном коробе нескольких кабелей им желательно экранирование. Данного кабеля необходимо 200 м из-за топологии звезда, требующей обширного количества кабеля. Ещё пять метров добавлено с учётом обрезков и порчи кабеля при монтаже. Полная модель кабеля - витая пара FUTP Cat 6e RJ-45. Витые пары помещены связками или по одному, в зависимости от расположения в здании по чертежу, внутрь монтажного короба. Параметры короба - материал ПВХ, размер 100х40. Короб проложен вдоль стен, внизу или вверху в зависимости от проектировки помещения.

4.3 Монтаж устройств

Для соединения административной рабочей станции Admin's PC с Cisco-маршрутизатором используется консольный кабель Cisco DB9 - RJ45. Его достаточно в количестве 5 метров единым кабелем. Активное сетевое оборудование, а именно: коммутатор, маршрутизатор, стоечный сервер, сервер хранилищ данных – расположены в серверной стойке в служебном помещении. Данное размещение позволит администратору успешно отлаживать сетевые устройства, а также обеспечить их долговременную работоспособность ввиду наличия вентиляции и охлаждения в стойке.

Волоконно-оптического кабеля используется 10м для подключения GPON-модема к внешней магистрали. Его модель Gembird CFO-LCLC-OM2-10M.

Все кабели «расходятся» из серверной на первом этаже, где расположена серверная стойка. В необходимых местах необходимо просверлить стены для удобной прокладки кабеля. Беспроводные точки доступа закреплены на стенах, на высоте 1.5 метра. К ним ведут спуски или подъёмы в кабельных каналах в зависимости от того, внизу или вверху стены находится ближайший короб с необходимой витой парой, идущей к главному маршрутизатору.

ЗАКЛЮЧЕНИЕ

За время проектирования курсовой работы была разработана локальная компьютерная сеть в соответствии с листом задания, позволяющая выполнять различные функции для успешной и стабильной работы компании по разработке Java-приложений в сфере IT.

Для написания данной курсовой работы было определено различие LAN и WAN сетей; после изучения различных топологий и заданных условий была выбрана топология звезда; обусловлен выбор сетевого оборудования из перечня, предлагаемого каталогом компании Cisco.

Следующим этапом является настройка разрабатываемой локальной сети. Для достижения этой цели необходимо использовать документацию Cisco, представленную на упомянутом выше сайте. Настройка сети проводилась по методу «сверху-вниз» – этот подход обуславливается настройкой сперва маршрутизатор, как верхней точки всей топологии, далее прописывается конфигурация коммутатора и, в заключение, проводится настройка оконечных устройств. Для моделирования работы возможно использовать программу Cisco Packet Tracer, в которой возможно назначить каждому устройству свой IP-адрес, смоделировать разрабатываемую сеть и проверить последнюю на работоспособность.

В заключение проектировки сети, необходимо соединить устройства физически на плане здания при помощи кабелей. С этой целью были изучены различные категории пассивного сетевого оборудования и пересмотрев топологию было выявлено, что достаточно использовать RJ-45 прямого типа категории 6 с FTP типом защиты. По заданию, провайдером проведен оптоволоконный кабель, который требует соответствующего порта на маршрутизаторе и, логично, самого кабеля. С целью удобства обустройства рабочего места администратора, последнему выделено специальное помещение – серверная. Данное решение обуславливается удобством настройки сети, а также, с ростом компании, возможности добавлять дополнительное оборудование без существенных перенастроек, переноса оборудования и, как следствие, меньших экономических затрат.

В курсовой работе представлены необходимое оборудование, структурная, функциональная схемы, планы этажей и спецификация оборудования и материалов, необходимых для построения локальной вычислительной сети.

В заключение справедливо отметить, что в данной работе требования, предъявляемые заказчиком, выполнены в полном объеме, выбранное оборудование соответствует всем стандартам качества, надежности и зарекомендовало себя как одно из лучших во множестве организаций. Разработанная топология сети останется актуальной в течение долгого периода времени, а предусмотренная гибкость позволит беспрепятственно расширять IT-компанию.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Локальная компьютерная сеть – разбираемся, что это [Электронный ресурс] – Электронные данные. – Режим доступа: <https://itmaster.guru/nastrojka-interneta/chto-takoe-lokalnaya-set.html> – Дата доступа 20.09.2021.

[2] Сергеев, А.С. Основы локальных компьютерных сетей: справочное пособие / А.С. Сергеев – М.: Энергоатомиздат, 2016. – 212 с.

[3] Настраиваем локальную сеть дома: оборудование, доступ к общим папкам и принтерам [Электронный ресурс] – Электронные данные. – Режим доступа: <https://club.dns-shop.ru/blog/t-280-marshrutizatoryi/31650-nastraivajem-lokalnuu-set-doma-oborudovanie-dostup-k-obschim-pa/> – Дата доступа 25.09.2021.

[4] Таненбаум, Э. Компьютерные сети 5-е изд. / Э. Таненбаум, Д. Уэзеролл – М.:Перо, 2016. – 312 с.

[5] Способы коммутации и передачи данных в сетях [Электронный ресурс] – Электронные данные. – Режим доступа: <https://pc.ru/docs/network/switching-methods> – Дата доступа 26.09.2021.

[6] Основные принципы работы сетевой маршрутизации [Электронный ресурс] – Электронные данные. – Режим доступа: <https://pc.ru/docs/network/routing> – Дата доступа 01.10.2021.

[7] Технологии подключения интернета [Электронный ресурс] – Электронные данные. – Режим доступа: <https://webonto.ru/tehnologii-podkljuchenija-interneta/> – Дата доступа 03.10.2021.

[8] Способы коммутации и передачи данных в сетях [Электронный ресурс] – Электронные данные. – Режим доступа: <https://lantorg.com/article/tehnologiya-pon-chto-eto> – Дата доступа 03.10.2021.

[9] Что такое вай фай (Wi-Fi)? Технология, фото и применение [Электронный ресурс] – Электронные данные. – Режим доступа: <https://wigid.ru/wi-fi/besprovodnaia-set-wi-fi> – Дата доступа 07.10.2021.

[10] Подробно о свойствах WiFi сигнала [Электронный ресурс] – Электронные данные. – Режим доступа: <https://lantorg.com/article/chto-takoe-wifi-podrobno-o-svoystvah-wifi-signala> – Дата доступа 10.10.2021.

[11] Адресация в компьютерных сетях [Электронный ресурс] – Электронные данные. – Режим доступа: <http://blogsisadmina.ru/seti/adresaciya-v-kompyuternyx-setyax.html> – Дата доступа 12.10.2021.

Технология PON – что это такое и зачем она нужна? [Электронный ресурс] – Электронные данные. – Режим доступа: <https://club.dns-shop.ru/blog/t-290-drugoe-setevoe-oborudovanie/48306-tehnologiya-pon-chto-eto-takoe-i-zachem-ona-nujna/> – Дата доступа 15.10.2021.

Куроуз, Д. Компьютерные сети. Нисходящий подход: справочное пособие / Д. Куроуз, К. Росс – Минск: Друк, 2016. – 276 с.

ПРИЛОЖЕНИЕ А
(обязательное)

Схема структурная

ПРИЛОЖЕНИЕ Б
(обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(обязательное)

План первого этажа

ПРИЛОЖЕНИЕ Г
(обязательное)

План второго этажа

ПРИЛОЖЕНИЕ Д
(обязательное)

Перечень оборудования, изделий и материалов

ПРИЛОЖЕНИЕ Е
(обязательное)

Ведомость документов