СОДЕРЖАНИЕ

[**ВВЕДЕНИЕ** 4](#_Toc534718286)

[**1** **ОБЗОР ИСТОЧНИКОВ** 6](#_Toc534718287)

[**1.1 Общие положения** 6](#_Toc534718288)

[**1.2 Требования к локальной вычислительной сети** 7](#_Toc534718289)

[**1.3 Требования к оформлению** 8](#_Toc534718290)

[**2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ** 9](#_Toc534718291)

[**2.1 Разделение сети на структурные единицы** 9](#_Toc534718292)

[**2.2 Выбор топологии сети** 9](#_Toc534718293)

[**2.3 Подсети для лабораторий и преподавательской** 11](#_Toc534718294)

[**2.4 Подсеть для заведующего кафедрой** 11](#_Toc534718295)

[**2.5 Административная подсеть** 11](#_Toc534718296)

[**3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ** 12](#_Toc534718297)

[**3.1 Обоснование выбора сетевой операционной системы** 12](#_Toc534718298)

[**3.2 Обоснование выбора активного сетевого оборудования** 12](#_Toc534718299)

[**3.2.1 Коммутатор Catalyst 2960-L** 12](#_Toc534718300)

[**3.2.2 Маршрутизатор Cisco 4451-X** 13](#_Toc534718301)

[**3.2.3 Беспроводной маршрутизатор Linksys EA6350 AC1200** 14](#_Toc534718302)

[**3.2.4 Сервер Dell PowerEdge T30** 15](#_Toc534718303)

[**3.2.5 Рабочая станция Jet MultiOffice FX430D4S12IS50** 16](#_Toc534718304)

[**3.2.6 Принтер HP OfficeJet 3830** 17](#_Toc534718305)

[**3.3 Обоснование выбора пассивного сетевого оборудования** 17](#_Toc534718306)

[**3.4 Схема адресации** 18](#_Toc534718307)

[**3.5 Административная подсеть** 19](#_Toc534718308)

[**3.6 Настройка подсети для заведующего кафедрой** 20](#_Toc534718309)

[**3.7 Настройка DHCP** 21](#_Toc534718310)

[**3.8 Настройка экспорта рабочего стола** 23](#_Toc534718311)

[**3.9 Настройка доступа в Интернет** 27](#_Toc534718312)

[**3.10 Настройка файлового сервера** 28](#_Toc534718313)

[**3.11 Настройка принтера** 31](#_Toc534718314)

[**3.12 Настройка беспроводного маршрутизатора** 31](#_Toc534718315)

[**3.13 Настройка протоколирования событий** 31](#_Toc534718316)

[**4 ПРИНЦИПИАЛЬНОЕ ПРОЕКТИРОВАНИЕ** 32](#_Toc534718317)

[**4.1 Кабельная подсистема** 32](#_Toc534718318)

[**4.2 Организация рабочих мест** 32](#_Toc534718319)

[**ЗАКЛЮЧЕНИЕ** 33](#_Toc534718320)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 34](#_Toc534718321)

[**ПРИЛОЖЕНИЕ Б** 36](#_Toc534718322)

[**ПРИЛОЖЕНИЕ В** 37](#_Toc534718323)

[**ПРИЛОЖЕНИЕ Г** 38](#_Toc534718324)

# **ВВЕДЕНИЕ**

Компьютерные сети являются одним из важнейших столпов любой современной сферы деятельности. Буквально всё – от заводов, аграрных предприятий и ферм до школ, научных лабораторий и игровых студий – нуждается в компьютерных сетях. Именно благодаря им мир, словно строго выверенный часовой механизм, способен бесперебойно работать и подогревать бурлящий котёл прогресса и человеческой мысли.

Главная задача компьютерных сетей – обеспечение одновременного и совместного доступа к общим ресурсам – будь до данные, вычислительные мощности или конкретные физические устройства. К примеру, принтеры, ёмкости жёстких дисков, виртуальные машины, вычислительное время, и многое другое являются ресурсами.

В реальной жизни существует масса ситуаций, когда к тем или иным ресурсам может понадобиться общий доступ. Например, команде программистов нужен общий доступ к коду одного проекта, банкам нужно иметь связь между собой для правильной обработки транзакций. Интернет – это тоже большая компьютерная сеть. Можно вспомнить облачные вычисления, Big Data, блокчейн – в основе всех них лежат именно компьютерные сети. Другими словами, возможность установить связь между множеством компьютеров имеет огромный потенциал и широчайшее практическое применение.

Конечно, с появлением сетей возникло и множество проблем. Непредвиденные обстоятельства и чрезвычайные ситуации могут вывести из строя или даже уничтожить сетевое оборудование, отрезав доступ к информации, что во многих случаях фактически значит остановку бизнеса. Также очень острой проблемой стоит потеря данных вследствие человеческого фактора или вышеупомянутых чрезвычайных ситуаций.

Неисправность компьютерных сетей влечёт за собой огромные убытки и абсолютно недопустима, поэтому специалисты по всему миру активно разрабатывают контрмеры для минимизации и предотвращения неисправностей компьютерных сетей. Примерами таких решений можно привести резервное копирование и обеспечение резервных путей данных.

Однако риски использования компьютерных сетей не ограничиваются выводом из строя той или иной части системы – взломы и хищение данных представляют собой большую угрозу. Особенно острой ситуация стала с повсеместным распространением глобальной сети Интернет. Часто недобросовестные системные администраторы не принимают должных мер по защите сетей, рабочих станций и серверов, в результате позволяя злоумышленникам получать доступ к частным сетям и данным.

Конечно, с одной стороны, реализация и поддержка компьютерных сетей может показаться очень дорогостоящей, небезопасной и хрупкой – кто-то даже может назвать это лишней уязвимостью бизнеса – но на деле сети открывают целую вселенную новых возможностей, так что затраты с торицей оправдываются полученной выгодой.

В век информации любому бизнесу необходимо использовать компьютерные сети в той или иной мере, чтобы оставаться конкурентоспособным.

Целью данного курсового проектирования является разработка архитектуры компьютерной сети для кафедры коммерческого университета, обучающей математике. В его рамках будут рассмотрены планирование топологии, необходимое оборудование для реализации сети, физическая прокладка проводки в помещениях.

# **ОБЗОР ИСТОЧНИКОВ**

## **1.1 Общие положения**

Локальная вычислительная сеть – это компьютерная сеть, располагающаяся на небольшой территории.

Классифицируются сети в основном по способу администрирования. Сети бывают:

1. Персональные (PAN) – персональные вычислительные сети

предназначены для взаимодействия устройств, принадлежащих одному владельцу. Обычно включают лишь несколько узлов и очень малы по занимаемой площади.

Такие сети чаще всего включают в себя беспроводные клавиатуры, мыши, смартфоны, беспроводную гарнитуру, принтеры, и многие другие устройства.

Самой распространённой технологией подключения в таких сетях является Bluetooth.

1. Локальные (LAN) – локальные сети покрывают группу зданий или

небольшую территорию. Хотя вовсе не обязательно, чтобы узлы сети были физически близко расположены друг от друга. Локальность в данном контексте значит скорее совместное локальное управление.

В локальных компьютерных сетях наиболее распространённым является проводное соединение. Оно может осуществляться через медный кабель, либо через оптоволоконный.

Наряду с проводными соединениями широко используется беспроводные соединения, соответствующие стандарту IEEE 802.11, более известные, как Wi-fi. Беспроводное соединение уступает по скорости проводному, но получило широкое распространение в быту и в бизнесе ввиду своего удобства.

1. Распределённые – распределённые сети позволяют распределить

имеющуюся вычислительную мощность на множество узлов, исключая наличие центрального сервера.

1. Городские (MAN) – городские сети связывают компьютеры в

пределах одного города.

Самый яркий пример подобной сети – сеть кабельного телевидения, в которой после модернизации появилась возможность передавать цифровые данные, и, как следствие, система стала городской (муниципальной) компьютерной сетью.

1. Глобальные (WAN) – глобальные сети связывают компьютеры на

очень больших территориях и включают в себя большое количество узлов. К примеру, Интернет является глобальной сетью.

Также можно классифицировать сети по способу управления:

1. Клиент-сервер – в таких сетях выделяются узлы, выполняющие

управляющие и обслуживающие функции (серверы). Остальные узлы являются терминальными (клиенты). Обычно конечному пользователю доступен именно клиент. В клиент-серверных сетях часто используется топология типа «звезда», когда множество узлов подключено к главному центральному.

1. Одноранговые сети – в одноранговых сетях все узлы равноправны.

Одним из главных плюсов таких сетей является доступность и сохранение работоспособности при любом количестве любых узлов сети [2].

Физически сети состоят из активного и пассивного сетевого оборудования.

Активное сетевое оборудование питается от электрической сети и выполняет функции преобразования и усиления сигнала. В перечень активного оборудования входят маршрутизаторы, коммутаторы, усилители, сервера, рабочие станции, и другие.

Пассивное же сетевое оборудование не питается от сети, не преобразовывает и не усиливает сигнал. Примерами пассивного сетевого оборудования можно привести кабели, розетки, коммутационные панели, кронштейны, кабельканалы, защитные коробы, коммутационные шкафы, и другие [3].

В разделе 3 используемое в курсовой работе оборудование будет рассмотрено более подробно.

## **1.2 Требования к локальной вычислительной сети**

Любая вычислительная сеть должна обеспечивать надёжный и быстрый доступ к любому ресурсы сети для любых её пользователей. Чтобы выполнять эту функцию, локальная вычислительная сеть должна соответствовать приведённым ниже требованиям.

Главное, и самое очевидное требование – собственно, обеспечение пользователям локальной вычислительной сети доступа к общим ресурсам данной сети и её компьютеров. Все остальные требования, хоть тоже являются крайне важными, влияют лишь на качество выполнения этой задачи.

Локальная вычислительная сеть также должна быть производительна – это требование характеризует возможность параллельной обработки задачи сразу несколькими компьютерами в сети.

Немаловажным требованием также является надёжность локальной вычислительной сети. Она, в свою очередь, делится на три критерия:

1. Вероятность доставки пакета без искажений.
2. Доля времени, в течение которого систему можно использовать.
3. Способность защиты данных от несанкционированного доступа.

Не стоит забывать также про отказоустойчивость. Это требование предполагает доступность сети даже при отказе некоторых её элементов. Отказоустойчивость обычно достигается созданием альтернативных путей данных и наличием резервного оборудования, которое заменяет собой основное в случае неисправности.

Прозрачность сети достигается в том случае, если вся сеть видна пользователю как единая вычислительная система, а не как множество отдельных вычислительных устройств.

Очень важна и расширяемость сети. Данное требование предполагает собой простое наращивание размеров сети – добавление новых узлов, пользователей, рабочих станций, замены устаревшего оборудования на более новое, и так далее.

Важным требованием является управляемость сети. Управляемость сети – это возможность контролировать работу всей локальной вычислительной сети из единого центра управления.

Вычислительные сети также должны поддерживать различные типы трафика. Сюда может входить и традиционный поток бит, и видео, и аудио.

Также вычислительной сети будет сложно существовать без совместимости, когда различное аппаратное и программное обеспечение не конфликтуют и способны сосуществовать и обмениваться информацией в одной сети без специальных конвертирующих мер – даже будучи от различных производителей, или под управлением разных операционных систем [4].

## **1.3 Требования к оформлению**

Пояснительная записка и прилагающиеся к ней чертежи должны быть подобающим образом оформлены в соответствии с действующими правилами ГОСТ [1].

# **2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ**

## **2.1 Разделение сети на структурные единицы**

На кафедре присутствуют четыре кабинета с множеством рабочих станций. Все они должны иметь доступ в Интернет и к файловому серверу.

Имеет смысл выделить на каждый кабинет по своей подсети, а также создать административную виртуальную локальную сеть для отслеживания и управления.

Итоговая структурная схема представлена в приложении «А».

## **2.2 Выбор топологии сети**

Сетевая топология – это конфигурация графа, вершинами которого являются конечные узлы сети и коммуникационное оборудование – вычислительные машины и маршрутизаторы соответственно, – а рёбрам – информационные или физические связи между вершинами.

Компьютерные сети весьма и весьма удобно представлять именно в виде графов.

Наиболее вероятные кандидаты для использования в курсовом проекте:

1. Шинная – связь между любыми двумя узлами устанавливается через

один общий путь (шину). Данные, передаваемые одной станцией, становятся доступны для всех других, подключённых к этой шине. Такая топология проста, но влечёт за собой ряд проблем – например, проблему одновременной попытки доступа сразу нескольких узлов к одной и той же шине (рисунок 2.1).

1. Кольцевая – узлы связаны кольцевой линией передачи – к каждому

узлу подключены две линии. Проходя по кольцу, данные становятся доступны всем узлам (рисунок 2.2). Такая топология решает проблему одновременной попытки доступа сразу нескольких узлов к одной и той же шине, однако передача данных от одного узла к другому замедляется, поскольку данные должны пройти через несколько узлов прежде, чем попадут к адресату.

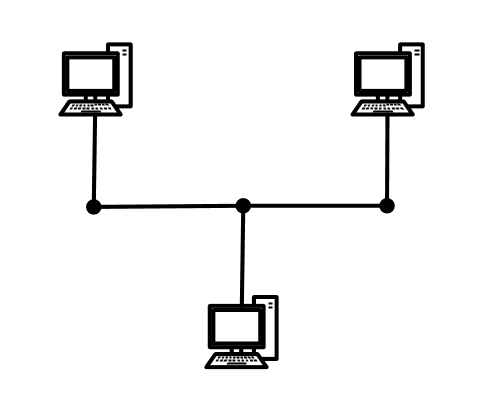
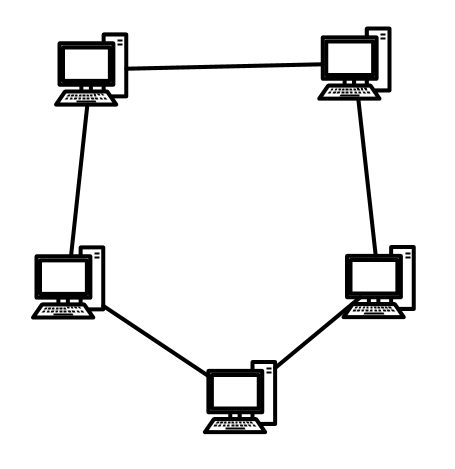
1. Звезда – к центральному узлу подключены все остальные

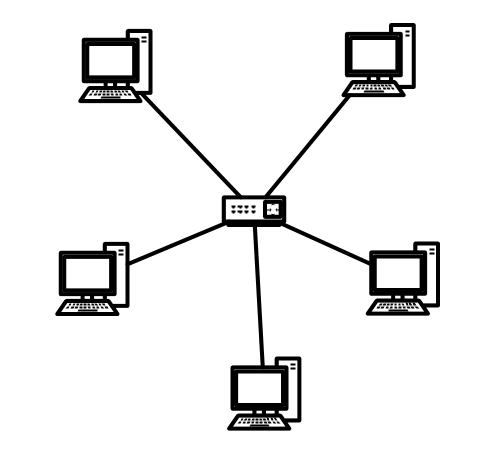
(рисунок 2.3). Основным минусом данной топологии, пожалуй, является большая нагрузка на центральный узел.

Сама топология подразумевает под собой физическое расположение компьютеров, кабелей, маршрутизаторов, коммутаторов и прочих компонентов в сети.

Стоит отметить, что различные типы топологий решают различные типы задач, так что необходимо тщательно подойти к её выбору. Он может зависеть от следующих факторов:

1. Состав имеющегося сетевого оборудования
2. Характеристики сетевого оборудования
3. Возможность расширения сети
4. Способ управления сетью

  
Рисунок 2.1 – Шинная топология  
  
  
Рисунок 2.2 – Кольцевая топология

  
Рисунок 2.3 – Топология «звезда»

На основе данного варианта и вышеприведённого материала, было принято решение использовать топологию «звезда». Она наиболее всего подойдёт поставленной задаче, ввиду наличия центрального сервера.

## **2.3 Подсети для лабораторий и преподавательской**

В данной структурной единице сети выделяются рабочие станции для лабораторий и преподавательской. Каждому кабинету соответствует своя виртуальная локальная сеть.

## **2.4 Подсеть для заведующего кафедрой**

В данной структурной единице сети выделяется рабочая станция для заведующего кафедрой. Она подключена к центральному маршрутизатору через коммутатор.

## **2.5 Административная подсеть**

Данная структурная единица используется для управления всей остальной сетью. Она распространяется на все коммутаторы и центральный маршрутизатор, а также имеет одну рабочую станцию.

# **3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ**

## **3.1 Обоснование выбора сетевой операционной системы**

Так как используемая сетевая аппаратура производится компанией Cisco, операционной системой была выбрана Cisco IOS. Она используется в маршрутизаторах и коммутаторах производства Cisco.

Это многозадачная операционная система, выполняющая задачи маршрутизации, сетевой организации и передачи данных.

Взаимодействие с данной ОС осуществляется посредством командной строки (CLI).

## **3.2 Обоснование выбора активного сетевого оборудования**

Активным оборудование является, если оно содержит электронные схемы, питаемые от электрической сети или других источников, а также выполняющее функции преобразования и усиления сигнала. Такое оборудование может обрабатывать сигнал по установленным алгоритмам.

В сетях данные передаются передаются попакетно. Каждый пакет содержит данные и техническую информацию: сведения об источник и приёмнике, проверку целостности данных, и многое другое. Эта информация делает возможной исправную доставку адресату.

Активное сетевое оборудование не просто улавливает и передаёт сигнал, но и обрабатывает техническую информацию в соответствии со встроенными алгоритмами.

В данном курсовом проекте используется следующее активное сетевое оборудование:

1. Коммутаторы Cisco Catalyst 2960-L
2. Маршрутизатор Cisco 4451-X
3. Беспроводной маршрутизатор Linksys EA6350 AC1200
4. Сервер Dell PowerEdge T30
5. Рабочие станции Jet MultiOffice FX430D4S12IS50

Было решено использовать оборудование компании Cisco, ввиду его надёжности, удобства и множества функций. Полный перечень оборудования представлен в приложении «Г».

## **3.2.1 Коммутатор Catalyst 2960-L**

Сетевой коммутатор – активное сетевое устройство, предназначенное для соединения нескольких узлов вычислительной сети между собой. Соединение происходит в пределах одного или нескольких сегментов сети. Коммутаторы можно рассматривать как многопортовые мосты. Стоит отметить, что работают они на втором уровне модели OSI.

В качестве коммутатора для рассматриваемой в данной работе сети был выбран Cisco Catalyst 2960-L на 24 порта. Модели на 16 портов не хватит для некоторых узлов, а модель на 48 портов показалась избыточной, так что модель на 24 порта оказалась идеальным кандидатом.

Одним из важнейших критериев при выборе была управляемость коммутатора. Все коммутаторы делятся на управляемые и неуправляемые: неуправляемые не располагают своим собственном процессором, так что вносить изменения в их конфигурацию не представляется возможным.

Управляемые же коммутаторы, помимо возможности тонкой ручной настройки, обладают обширным рядом функций: мониторингом сети, механизмами управления трафиком, возможностью создавать виртуальные локальные сети, и многими другими.

Конечно, управляемые коммутаторы на порядок дороже, но полностью оправдывают свою цену широким спектром возможностей.

Cisco Catalyst 2960-L имеет 24 порта Gigabit Ethernet, пассивную систему охлаждения (что позволяет значительно снизить уровень шума от серверной) и возможность ручной конфигурации.

  
Рисунок 3.1 – Cisco Catalyst 2960-L [6]

## **3.2.2 Маршрутизатор Cisco 4451-X**

Маршрутизатор – это специализированный сетевой компьютер, имеющий несколько сетевых интерфейсов. Основная задача маршрутизатора – пересылка пакетов между разными сегментами сети, а также связывание разнородных сетей с различными структурами. Для принятия решений о том, куда пересылать пакеты, используется информация о топологии сети и набор определённых правил. Маршрутизаторы работают на третьем уровне модели OSI.

Cisco 4451-X обладает следующими характеристиками:

Таблица 3.1 – Основные характеристики Cisco 4451-X

|  |  |
| --- | --- |
| Характеристика | Значение |
| Количество сетевых модулей интерфейса (NIM): | 3 |
| Количество портов встроенного коммутатора | 48 |

*Продолжение таблицы 3.1*

|  |  |
| --- | --- |
| 1 | 2 |
| Потребление PoE | 500 Вт |
| Формфактор | 2 RU |
| Тип блока питания | Внутренний; AC, PoE или DC |
| Порт управления | 1 GE |
| Количество USB портов (type A) | 2 |
| Интегрированные WAN порты | 2 PoE GE / SFP; 2 GE / SFP |
| DRAM | 4 GB |
| Flash | 8 GB |
| Поддержка VDSL 2 | Есть |

Cisco 4451-X был выбран потому, что обладает встроенным коммутатором, что позволяет несколько упростить топологию. Также этот роутер обладает поддержкой VDSL2.



Рисунок 3.2 – Cisco 4451-X [5]

## **3.2.3 Беспроводной маршрутизатор Linksys EA6350 AC1200**

Беспроводной маршрутизатор выполняет практически те же функции, что и обыкновенный, а также обладает возможностью беспроводного подключения устройств.

Выбранный для данной курсовой работы маршрутизатор Linksys EA6350 AC1200 обладает следующими характеристиками:

1. Двухполосное вещание (2.4 и 5 Гц), обеспечивающее более

надёжное соединение.

1. Поддержка Gigabit Ethernet.
2. Технология формирования луча, фокусирующая Wifi сигнал на

подключённых устройствах.

1. Поддержка Wireless-AC, обеспечивающая скорости до 867 Мбит/с.

При выборе были важны высокая скорость и надёжность подключения. Linksys EA6350 AC1200 соответствует обоим этим требованиям.



Рисунок 3.3 – Linksys EA6350 AC1200 [7]

## **3.2.4 Сервер Dell PowerEdge T30**

Сервер – это компьютер, выделенный из группы для выполнения сервисных задач без непосредственного участия администратора.

В качестве сервера был выбран Dell PowerEdge T30 Его технические характеристики:

Таблица 3.2 – Основные характеристики Dell PowerEdge T30

|  |  |
| --- | --- |
| Характеристика | Значение |
| Процессор | Intel Xeon E3-1225 v5 3.3 GHz Quad-Core |
| ОЗУ | 8 Гб |
| Жёсткий диск | 1 Тб |
| DVD привод | Есть |

Это далеко не самый мощный сервер, но его более, чем хватит для поставленных задач. При выборе важно было найти относительно современный сервер по доступной цене.

Машина будет использоваться как файловый сервер.

  
Рисунок 3.4 – Dell PowerEdge T30 [8]

Работать сервер будет под управлением Windows Server 2019 – серверной операционной системы, базирующейся на Windows 10. Она выбрана из-за своей простоты в работе.

## **3.2.5 Рабочая станция Jet MultiOffice FX430D4S12IS50**

Рабочие станции будут использоваться преподавателями и студентами для проведения занятий, доступа к Интернету и файловому серверу.

При выборе не стояло каких-либо особых требований, так что была взята доступная станция Jet MultiOffice FX430D4S12IS50. Она имеет следующие технические характеристики:

Таблица 3.3 – Основные характеристики Jet MultiOffice FX430D4S12IS50

|  |  |
| --- | --- |
| Характеристика | Значение |
| Процессор | AMD FX 4300 3.8 ГГц Quad-Core |
| ОЗУ | 4 Гб |
| SSD | 120 Гб |
| Блок питания | 500 Вт |
| LAN | 1 Гигабит |

На кафедре не будет выполняться никакой тяжёлой вычислительной работы, так что выбранные характеристики вполне приемлемы и будут достаточны для обучения математике.

Работать данная станция будет под управлением операционной системы Windows 10 Enterprise. Данная ОС была выбрана из-за своей распространённости на рынке и простоты по сравнению с аналогами.

  
Рисунок 3.5 – Jet MultiOffice FX430D4S12IS50

## **3.2.6 Принтер HP OfficeJet 3830**

Данный принтер отлично подходит для офисов и учебных заведений. Компания HP давно зарекомендовала себя, как ведущий производитель принтеров, так что выбор пал именно на её продукты. Выбрать же именно модель 3830 заставили следующие особенности:

1. Тихий режим
2. Технология Instant Ink
3. Поддержка разных размеров бумаги

  
Рисунок 3.6 – HP OfficeJet 3830 [10]

## **3.3 Обоснование выбора пассивного сетевого оборудования**

Пассивным сетевым оборудованием называется сетевое оборудование, не питающееся от электрической сети, не преобразующее сигнал и выполняющее функции по его усилению.

Примерами такого оборудования можно представить различные кабели, информационные розетки, монтажные шкафы, монтажные стойки, телекоммуникационные шкафы, и многое другое.

Таблица 3.4 – Актуальные категории витых пар

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Категория | Максимальная длина, м | Максимальная скорость, Гбит/с | PoE | Максимальная частота,  МГц |
| Cat-5 | 100 | 0.1 | Есть | 100 |
| Cat-5e | 100 | 1 | Есть | 100 |
| Cat-6 | 100 | 10 | Есть | 250 |
| Cat-6a | 100 | 10 | Есть | 500 |

В данной курсовой работе была использована неэкранированная витая пара категории 5e. Категория обусловлена тем, что всё оборудование использует Gigabit Ethernet.

Экранирование же применяется лишь в специализированных цехах, где велико электромагнитное излучение, либо электромагнитное излучение самой витой пары способно повлиять на работу каких-либо устройств. На кафедре математики нет сильных источников излучения или особо чувствительного оборудования, поэтому экранирование витой пары будет не будет иметь особого смысла.

Других особых требований к пассивному оборудованию нет, так что после анализа имеющихся на рынке вариантов были выбраны витая пара Hyperline UUTP4-C5E-S24-IN-LSZH-GY, коннектор RJ-45 Cabeus 8P8C-SH-С7-TWP, и компьютерная информационная розетка Glossa GSL000181K RJ45 категории 5e.

Все они соответствуют стандартам категории 5е, так что вполне подходят для рассматриваемой сети.

## **3.4 Схема адресации**

По условию даны две подсети:

1. 90.168.1.0 255.255.255.248 (6 хостов)
2. 10.0.10.0 255.255.255.0 (254 хоста)

Имеет смысл разбить подсеть 10.0.10.0 на 8 подсетей, вмещающих по 30 хостов каждая.

Так будет гораздо более удобно настраивать сеть, а также позволит разделить её на участки.

У получившихся подсетей маска изменится на 255.255.255.224. Итоговая схема адресации отражена в таблицах 3.5 и 3.6.

Остальные устройства покрываются с помощью DHCP, о котором будет рассказано ниже.

Итоговая функциональная схема представлена в приложении «Б».

Таблица 3.5 – Схема адресации сетей

|  |  |  |
| --- | --- | --- |
| Назначение | IP адрес | Маска подсети |
| Административная | 10.0.10.224 | 255.255.255.224 |
| Лаборатория 1 | 10.0.10.0 | 255.255.255.224 |
| Лаборатория 2 | 10.0.10.32 | 255.255.255.224 |
| Лаборатория 3 | 10.0.10.64 | 255.255.255.224 |
| Преподавательская | 10.0.10.96  2001:F0C5:1:: | 255.255.255.224  /64 |
| Заведующий кафедрой | 10.0.10.128  2001:F0C5:2:: | 255.255.255.224  /64 |
| Wi-fi | 10.0.10.160 | 255.255.255.224 |
| VDSL2 | 10.0.10.192 | 255.255.255.224 |
| Сервер | 90.126.1.0 | 255.255.255.248 |

Таблица 3.6 – Схема адресации центрального роутера

|  |  |  |
| --- | --- | --- |
| Назначение порта | IP адрес | Маска подсети |
| Сервер | 90.126.1.2 | 255.255.255.248 |
| Лаборатория 1 | 10.0.10.1 | 255.255.255.224 |
| Лаборатория 2 | 10.0.10.33 | 255.255.255.224 |
| Лаборатория 3 | 10.0.10.65 | 255.255.255.224 |
| Преподавательская | 10.0.10.97  2001:F0C5:1::1 | 255.255.255.224  /64 |
| Заведующий кафедрой | 10.0.10.129  2001:F0C5:2::1 | 255.255.255.224  /64 |
| Выход в Интернет | 10.0.10.193 | 255.255.255.224 |

## **3.5 Административная подсеть**

В административной подсети осуществляется управление всей сети посредством программирования центрального маршрутизатора, также выступающего в роли DHCP сервера.

Приступим к настройке виртуальных подсетей для администрирования и кабинетов. Административной подсети необходима виртуальная локальная сеть. Выделим для неё адрес 10.0.10.224/27. Индекс виртуальной локальной сети – 2, имя – VLAN2.

Для создания VLAN необходимо прописать следующие команды на центральном маршрутизаторе и всех коммутаторах (адреса для соответствующих устройств представлены в таблице 3.7):

vlan 2

name VLAN2

ip ad [ip адрес]

Таблица 3.7 – адреса устройств для административной подсети.

|  |  |  |
| --- | --- | --- |
| Устройство | ip адрес | Маска подсети |
| ROUTER | 10.0.10.225 | 255.255.255.224 |
| SWITCH0 | 10.0.10.226 | 255.255.255.224 |
| SWITCH1 | 10.0.10.227 | 255.255.255.224 |
| SWITCH2 | 10.0.10.228 | 255.255.255.224 |
| SWITCH3 | 10.0.10.229 | 255.255.255.224 |
| SWITCH4 | 10.0.10.230 | 255.255.255.224 |

Также необходимо переключить коммутаторы в режим trunk. В этом режиме коммутатор будет пропускать только пакеты из разрешённых администратором подсетей:

switch# conf t

interface [Interface]

switchport mode trunk

switchport trunk allowed vlan 1,2

Также в целях безопасности стоит прописать port-security на интерфейсе, предназначенном для администратора:

switchport port-security

switchport port-security maximum 1

switchport port-security violation restrict

switchport port-security mac-address sticky

## **3.6 Настройка подсети для заведующего кафедрой**

Для данной подсети требуются ipv4 и ipv6. Так как подсеть располагает лишь одной рабочей станцией, смысла в DHCP нет, так что можно обойтись статическими адресами.

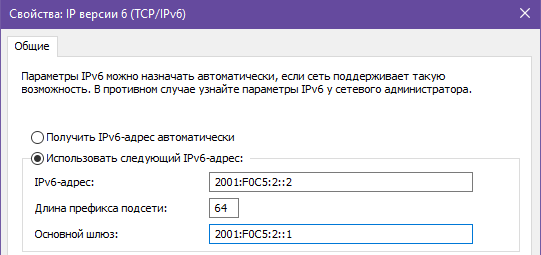
Пропишем на центральном роутере следующее:

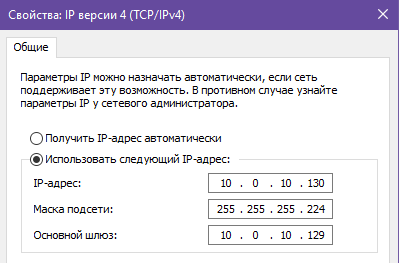
int [Интерфейс, идущий к подсети завкафедрой]

ip ad 10.0.10.129 255.255.255.224

ipv6 address 2001:F0C5:2::1\64

На компьютере заведующего кафедрой следует указать настройки, указанные на рисунках 3.7 и 3.8.

  
Рисунок 3.7 – Настройки ipv6.

  
Рисунок 3.8 – Настройки ipv4

## **3.7 Настройка DHCP**

DHCP – это сетевой протокол, позволяющий компьютерам в сети получать ip и другие параметры для работы в сети автоматически. Это позволяет легко расширять существующие сети и не проделывать большое количество монотонной работы.

Всего для рассматриваемой сети понадобится четыре ipv4 DHCP пула и один ipv6 пул для компьютеров на кафедре.

Для настройки DHCP требуется подключиться к роутеру (выступающему в роли DHCP сервера) и прописать в нём следующие команды:

ip dhcp pool Lab1

network 10.0.10.0 255.255.255.224

default-router 10.0.10.1

exit

ip dhcp pool Lab2

network 10.0.10.32 255.255.255.224

default-router 10.0.10.33

exit

ip dhcp pool Lab3

network 10.0.10.64 255.255.255.224

default-router 10.0.10.65

exit

ip dhcp pool Teachers

network 10.0.10.96 255.255.255.224

default-router 10.0.10.97

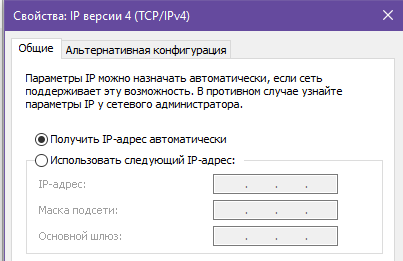
exit

Это создаст четыре DHCP пула для каждого кабинета. Теперь необходимо задать правильные адреса на интерфейсах центрального маршрутизатора. Для этого нужно на каждом интерфейсе, идущему к коммутатору, прописать следующее:

int [Интерфейс]

ip ad [Адрес, ранее указанный в default-router соответствующего пула]

Чтобы на рабочей станции происходило подключение по DHCP, надо отметить автоматическое получение ip в центре управления сетями (рисунок 3.9).

  
Рисунок 3.9 – Получение адреса с использованием DHCP.

По условию, компьютерам на кафедре необходим ipv6. Для его настройки нужно снова зайти в центральный маршрутизатор и прописать следующие команды:

Сперва нужно включить ipv6 маршрутизацию.

ipv6 unicast-routing

Затем надо создать DHCPv6 пул.

ipv6 dhcp pool Teachers\_v6

address prefix 2001:F0C5:1::/64

После этого надо перейти в интерфейс, ведущий к учительской.

int [Интерфейс]

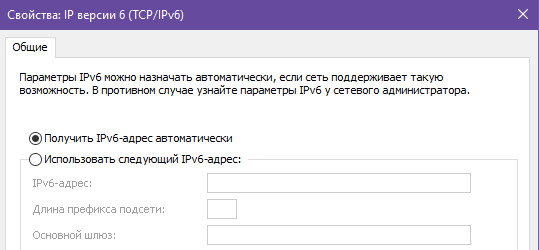
ipv6 ad 2001:F0C5::1/64

ipv6 dhcp server Teachers\_v6

ipv6 nd managed-config-flag

ipv6 nd prefix 2001:F0C5::/64 14400 14400 no-autoconfig

На рабочих станциях в учительской нужно включить автоматическое получение ipv6 в настройках сетей (рисунок 3.10).

  
Рисунок 3.10 – Получение адреса с использованием DHCPv6.

## **3.8 Настройка экспорта рабочего стола**

Для настройки экспорта рабочего стола на компьютеры студентов а лабораториях была выбрана программа iTALC.

Перед установкой следует настроить Windows. Необходимо зайти в настройки брандмауэра и отключить его. После этого нужно настроить параметры общего доступа, разрешив обнаружение и удалённое подключение, что показано на рисунках 3.11 и 3.12.

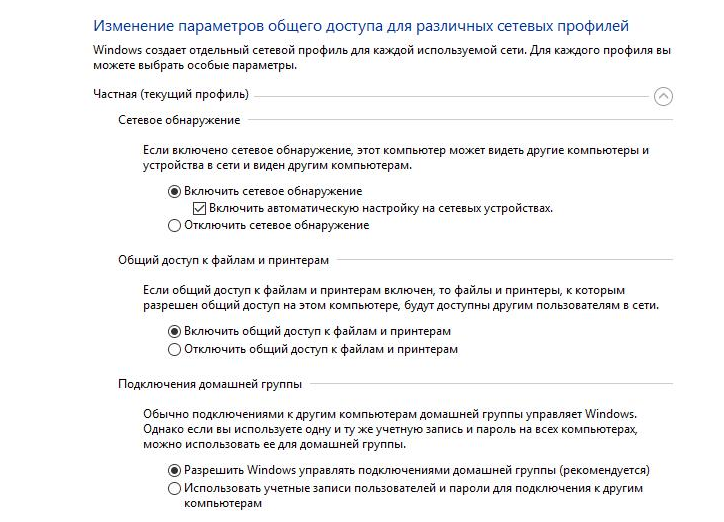


Рисунок 3.11 – Настройка параметров общего доступа

Также необходимо включить доступ к общим папкам.

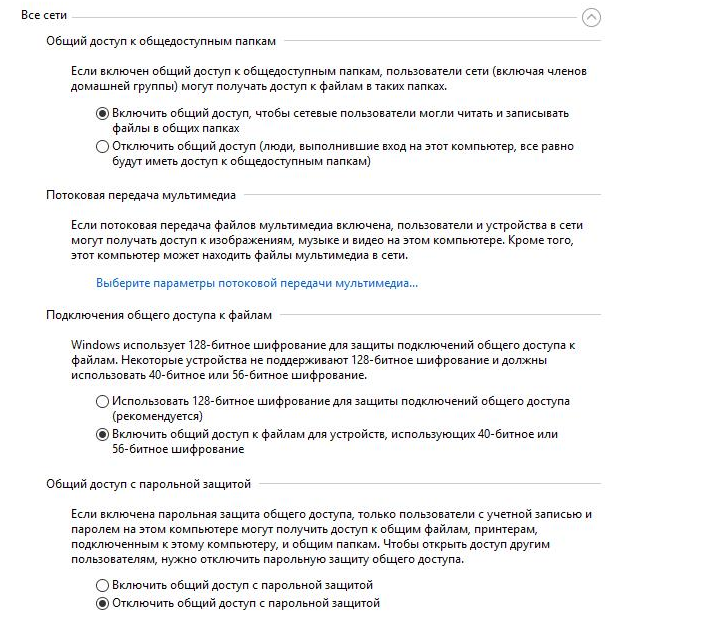


Рисунок 3.12 – Настройка параметров общего доступа

После этого нужно установить iTALC 3 и выбрать пункт VNC Reflector в меню Backend (рисунок 3.13).

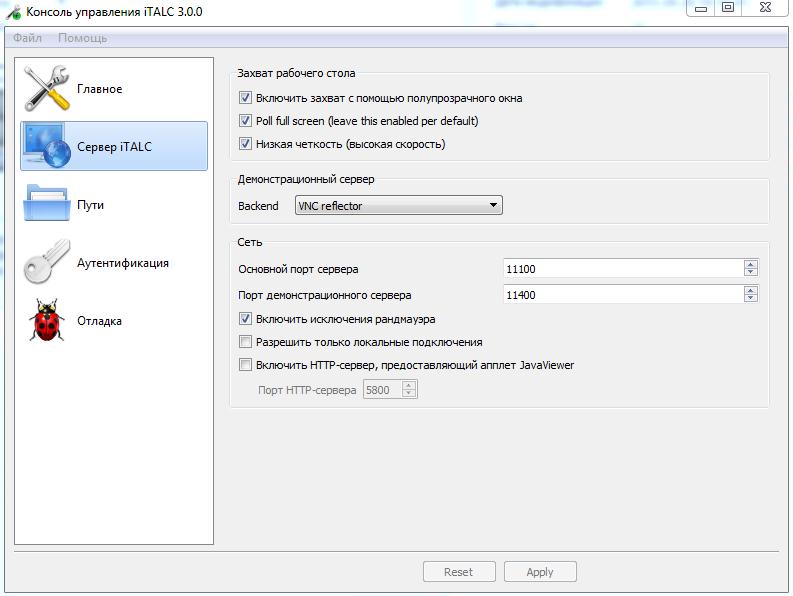


Рисунок 3.13 – Интерфейс iTALC

Далее нужно сгенерировать ключ доступа для учеников на компьютере преподавателя (рисунки 3.14 и 3.15).

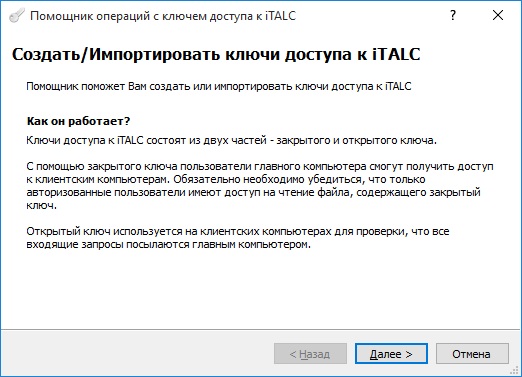
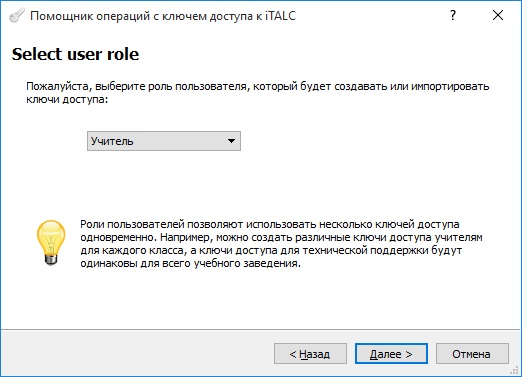
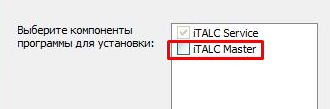


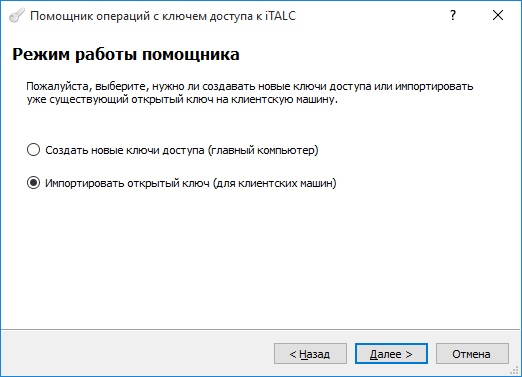
Рисунок 3.14 – Генерация ключа

  
Рисунок 3.15 – Генерация ключа

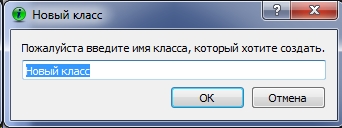
После генерации ключ необходимо загрузить на компьютеры студентов. Далее нужно установить на них iTALC, при этом убрав при установке компонент iTALC Master (рисунок 3.16).

  
Рисунок 3.16 – Параметры установки iTALC на компьютерах студентов

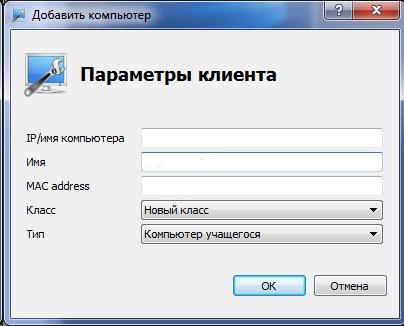
Далее нужно, аналогично главному компьютеру, выставить Backend на VNC Reflector, и после этого импортировать его ключ, что показано на рисунке 3.17.

  
Рисунок 3.17 – Импорт ключа

После этого нужно снова перейти на компьютер преподавателя и создать новый класс (рисунок 3.18).

  
Рисунок 3.18 – Генерация ключа

В нём нужно добавить компьютеры учеников. Так как в сети настроен DHCP, вместо ip адресов следует прописать имена компьютеров (рисунок 3.19).

  
Рисунок 3.19 – Генерация ключа

## **3.9 Настройка доступа в Интернет**

Доступ в Интернет осуществляется посредством VDSL2. Выбранный маршрутизатор обладает одним портом с поддержкой VDSL2. Чтобы его настроить, надо прописать следующие команды:

controller VDSL 0/1/0

operating mode vdsl2

end

int [Интерфейс с поддержкой VDSL]

ip ad 10.0.10.193 255.255.255.224

load-interval 30

no negotiation auto

no sh

Теперь необходимо настроить NAT. Для каждого интерфейса кабинета, заведующего кафедрой, преподавательской, сервера:

ip nat inside

Для Интерфейса, выходящего в Интернет:

ip nat outside

exit

ip access-list standart foxNAT

permit 10.0.10.224 255.255.255.224

permit 10.0.10.0 255.255.255.224

permit 10.0.10.32 255.255.255.224

permit 10.0.10.64 255.255.255.224

permit 10.0.10.96 255.255.255.224

permit 10.0.10.128 255.255.255.224

permit 90.126.1.2 255.255.255.248

permit 10.0.10.160 255.255.255.224

exit

ip nat inside source list foxNAT interface [Интерфейс, выходящий в Интернет] overload

Также надо настроить доступ в Интернет по расписанию. Для этого нужно прописать следующие команды:

time-range NoNoTime

periodic daily 00:00 to 07:59

periodic daily 17:00 to 23:59

periodic weekend 00:00 to 23:59

access-list Internet deny ip host 10.0.10.1 any time-range NoNoTime

access-list Internet deny ip host 10.0.10.33 any time-range NoNoTime

access-list Internet deny ip host 10.0.10.65 any time-range NoNoTime

access-list Internet deny ip host 10.0.10.97 any time-range NoNoTime

access-list Internet deny ip host 10.0.10.129 any time-range NoNoTime

access-list Internet permit ip host any any

Затем нужно зайти в интерфейсы всех лабораторий, преподавательской и кабинета заведующего кафедрой, и прописать:

ip access-group Internet in

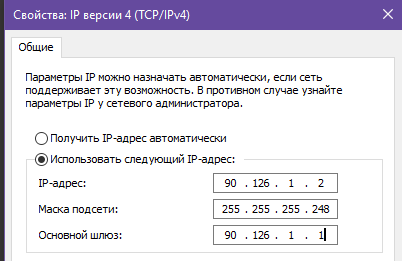
## **3.10 Настройка файлового сервера**

Для начала настроим ip адреса. На центральном маршрутизаторе:

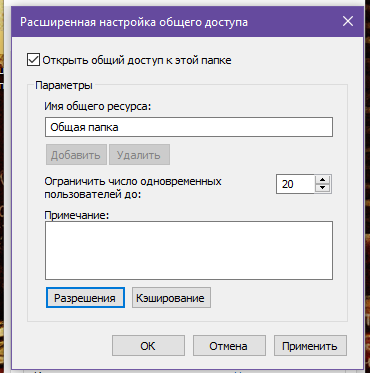
int [Интерфейс]

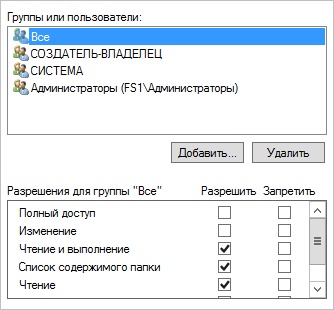
ip ad 90.126.1.1 255.255.255.248

На сервере укажем адрес, показанный на рисунке 3.20.

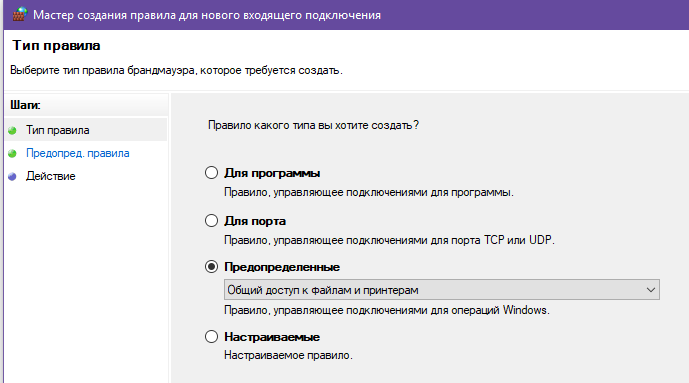
  
Рисунок 3.20 – Адрес сервера

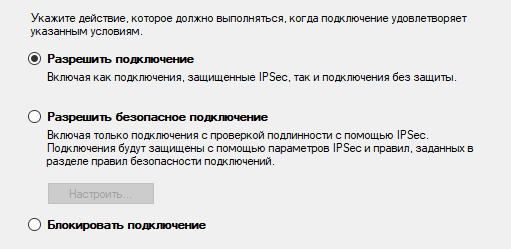
Затем нужно перейти в Диспетчер серверов и добавить роль «Файловые службы и службы хранилища». После этого нужно создать общие папки, к которым будет предоставлен доступ (рисунки 3.21 и 3.22).

  
Рисунок 3.21 – Расширенная настройка общего доступа

  
Рисунок 3.22 – Разрешения общей папки

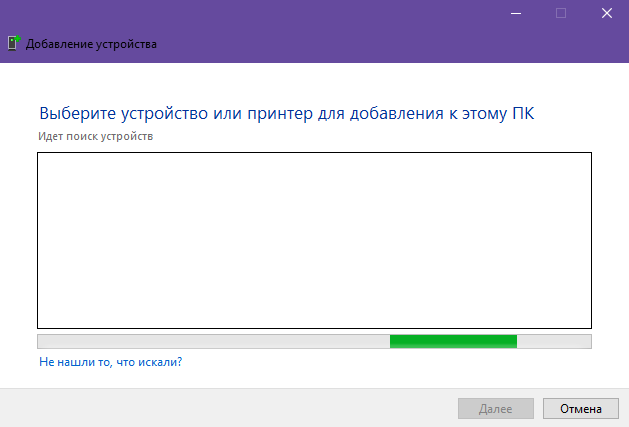
Также нужно создать новое правило в брандмауэре Windows, показанное на рисунках 3.23 и 3.24.

  
Рисунок 3.23 – Создание нового правила

  
Рисунок 3.24 – Разрешения общей папки

## **3.11 Настройка принтера**

Принтер находится в той же локальной сети, что и преподавательская. Чтобы подключиться к нему, нужно зайти в Панель Управления -> Устройства и Принтеры, и нажать на кнопку «Добавить новое устройство». После этого принтер успешно обнаружится (рисунок 3.25).

  
Рисунок 3.25 – Поиск принтера

## **3.12 Настройка беспроводного маршрутизатора**

Чтобы войти в интерфейс беспроводного маршрутизатора, нужно вписать в адресную строку 192.168.0.1. Стандартным логином и паролем будет admin admin соответственно. Сразу после входа нужно сменить их на другие.

После этого в настройках LAN нужно ввести ip локальной сети 10.0.10.160 с маской 255.255.255.224.

Далее нужно включить и настроить DHCP. ip сети -- 10.0.10.160, шлюз -- 10.0.10.161

Затем надо включить беспроводную сеть, выставить в настройках безопасности WPA2/PSK, задать уникальный SSID и пароль, который будет известен только преподавателям.

## **3.13 Настройка протоколирования событий**

Протоколирование будет производиться в буфферном режиме на центральном роутере. Чтобы включить протоколирование, нужно прописать:

logging buffered 64000

# **4 ПРИНЦИПИАЛЬНОЕ ПРОЕКТИРОВАНИЕ**

## **4.1 Кабельная подсистема**

Витая пара проложена при помощи защитных коробов по коридорам помещения. Где возможно, кабель ведётся по плинтусу прямо к информационным розеткам, расположенным в непосредственной близости от оконечных устройств.

Результатом данных операций является план кафедры, представленный в приложении «В».

## **4.2 Организация рабочих мест**

На кафедре три комнаты выделены под лаборатории, суммарно вмещающие 26 рабочих станций для студентов и три – для преподавателей. Одна комната выделена под учительскую, с десятью стационарными рабочими станциями, беспроводным маршрутизатором и принтером. Также выделена комната для заведующего кафедрой с одной рабочей станцией. Под сетевые нужды также выделено помещение – в нём находятся административный компьютер, сервер, беспроводной маршрутизатор, центральный маршрутизатор, коммутаторы и монтажный шкаф с центральным маршрутизатором и коммутаторами.

Две оставшиеся комнаты используются для других целей и не содержат в себе никакого сетевого оборудования.

Подключение сервера и рабочих станций осуществляется посредством выхода неэкранированных витых пар категории 5е с поддержкой Gigabit Ethernet через отверстия в стенах. Все кабели сходятся в защитный пятимиллиметровый пластиковый короб, берегущий их от внешнего воздействия. В конечном итоге он выходит за пределы кафедры и подключается к силовым сетям.

# **ЗАКЛЮЧЕНИЕ**

В ходе выполнения курсовой работы была разработана локальная компьютерная сеть для кафедры, обучающей математике. Также были получены практические и теоретические знания, и навыки проектирования локальной вычислительной сети.

Были исследованы рекомендации производителей, имеющееся на рынке сетевое оборудование, стандарты и требования к создаваемой системе.

В работе были представлены структурная, функциональная схемы, план этажа, спецификация перечня материалов и оборудования, необходимых для построения и реализации сети. Сюда вошли рабочие станции, маршрутизатор, коммутаторы, сервер, и другие. Оборудование, на которое пал выбор, соответствует всем стандартам качества, надёжности, и зарекомендовало себя как одно из лучших в своём классе для множества организаций, предприятий и бизнесов.

Возникшие в процессе проектирования проблемы правильным разбиением сети на структурные единицы, настройкой оборудования, грамотным использованием выданных подсетей и прокладкой кабелей были решены и устранены.

Данная курсовая работа только подтвердила важность вычислительных сетей во всех сферах человеческой деятельности, позволила восполнить пробелы в знаниях о вычислительных сетях, из разработке, структуре, прикладном использовании, а также предоставила реалистичную модель ситуации разработки локальной вычислительной сети для кафедры, обучающей математике.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

[1] Н. Г. Рожнова, Н. А. Искра, И. И. Глецевич «Вычислительные машины, Системы и Сети. Дипломное проектирование» - Минск БГУИР 2014 — [Электронный ресурс]. — Режим доступа:

https://www.bsuir.by/m/12\_100229\_1\_87625.pdf

[2] Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е издание – Санкт-Петербург [и другие] : Питер, Питер Пресс, 2017. – 955 с.

[3] CompBegin [электронный ресурс]. – Режим доступа: http://www.compbegin.ru/articles/view/\_100

[4] Чекмарёв Ю. В. Локальные вычислительные сети / Ю. В. Чекмарёв. – М.: ДМК-Пресс, 2014. – 250 с.

[5] Cisco 4451-X [электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/support/routers/4451-x-integrated-services-router-isr/model.html

[6] Cisco Catalyst 2960-L [электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/products/switches/catalyst-2960-l-series-switches/index.html#~stickynav=1

[7] Linksys EA6350 AC1200 [электронный ресурс]. – Режим доступа: https://www.linksys.com/us/p/P-EA6350/

[8] Dell PowerEdge T30 [электронный ресурс]. – Режим доступа: https://www.dell.com/en-us/work/shop/cty/pdp/spd/poweredge-t30/pet30\_12084\_3?CID=314685&st=%2Bdell+%2Bt30&VEN1=nXBKHWmy%2C73667372921886%2C901qz26673%2Cc%2C&VEN2=bb%2C%2Bdell+%2Bt30&LID=5957867&dgc=st&dgseg=cbg&acd=123092153372795930&VEN3=413004742551081767

[9] Jet MultiOffice FX430D4S12IS50 [электронный ресурс]. – Режим доступа: https://catalog.onliner.by/desktoppc/jets/fx430d4s12is50

[10] HP OfficeJet 3830 [электронный ресурс]. – Режим доступа: https://store.hp.com/us/en/pdp/hp-officejet-3830-all-in-one-printer

**ПРИЛОЖЕНИЕ А**

(обязательное)

Схема СКС структурная

# **ПРИЛОЖЕНИЕ Б**

(обязательное)

Схема СКС функциональная

# **ПРИЛОЖЕНИЕ В**

(обязательное)

План кафедры

# **ПРИЛОЖЕНИЕ Г**

(обязательное)

Перечень оборудования, изделий и материалов