СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 4](#_Toc27949770)

[1 ОБЗОР ЛИТЕРАТУРЫ 5](#_Toc27949771)

[2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 7](#_Toc27949772)

[3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 8](#_Toc27949773)

[3.1 Выбор активного сетевого оборудования 8](#_Toc27949774)

[3.1.1 Маршрутизатор Cisco 881-K9 8](#_Toc27949775)

[3.1.2 Коммутатор Cisco WS-C2960-8TC-L 8](#_Toc27949776)

[3.1.3 Беспроводная точка доступа D-link DWL-2600AP 9](#_Toc27949777)

[3.1.4 Повторитель Hikvision DS-1H34-0102P 10](#_Toc27949778)

[3.2 Выбор рабочего оборудования 10](#_Toc27949779)

[3.2.1 Рабочая станция N-Tech King Office M 61367 10](#_Toc27949780)

[3.2.2 Многофункциональное устройство HP LaserJet Pro M28w 10](#_Toc27949781)

[3.2.3 Принтер Xerox Phaser 3260DNI 11](#_Toc27949782)

[3.3 Схема адресации, настройка DHCP и SSH 11](#_Toc27949783)

[3.4 Настройка туннеля IPv6-over-IPv4 14](#_Toc27949784)

[3.6 Настройка прокси-сервера 14](#_Toc27949785)

[3.7 Настройка беспроводной точки доступа 16](#_Toc27949786)

[3.8 Настройка сетевого принтера 18](#_Toc27949787)

[4.1 Кабельная система 19](#_Toc27949788)

[4.2 Организация рабочих мест 19](#_Toc27949789)

[4.3 Защита оборудования от влаги 20](#_Toc27949790)

[4.4 Расчет качества связи для беспроводных точек доступа 20](#_Toc27949791)

[4.5 Монтаж беспроводной точки доступа 21](#_Toc27949792)

[ЗАКЛЮЧЕНИЕ 24](#_Toc27949793)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 25](#_Toc27949794)

[ПРИЛОЖЕНИЕ А 26](#_Toc27949795)

[ПРИЛОЖЕНИЕ Б 27](#_Toc27949796)

[ПРИЛОЖЕНИЕ В 28](#_Toc27949797)

[ПРИЛОЖЕНИЕ Г 29](#_Toc27949798)

[ПРИЛОЖЕНИЕ Д 30](#_Toc27949799)

# **ВВЕДЕНИЕ**

Компьютерные сети прочно вошли в нашу жизнь. Соединение нескольких персональных компьютеров и других цифровых устройств в одну компьютерную сеть позволяет быстро обмениваться информацией, централизованно хранить данные, получать доступ к сети Интернет и совместно использовать такие периферийные устройства, как принтер и сканер. Также это обеспечивает большую вычислительную мощность, так как нагрузку можно распределить между ЭВМ.

Но использование локальных компьютерных сетей сопровождается рядом задач: разработки принципов совместного использования сетевых ресурсов и протоколов, обеспечение защиты данных. В наше время существует множество аппаратного обеспечения (коммутаторы, маршрутизаторы), сетевых операционных систем, а также многочисленные сетевые приложения как для серверов, так и для рабочих станций, которые помогают при решении вышеперечисленных задач.

С распространением во всех сферах деятельности человека компьютерных сетей привело к большому количеству проблем, связанных с неожиданными условиями работы и обстоятельствами, которые имеют все шансы вывести из строя или же, в том числе, и полностью уничтожить сетевое оснащение, отрезав доступ к информации, собственно, что во множестве случаях практически означает остановку работы. Чтобы это предотвратить необходимо обеспечить дополнительную защиту устройств. Кабели, соединяющие устройства можно провести через коробы, а сами устройства поместить в телекоммуникационные шкафы. В связи с этим немаловажной характеристикой любой локальной компьютерной сети является отказоустойчивость, то есть поддержание работоспособности сети даже при поломке некоторых сетевых устройств, входящий в топологию.

# **1 ОБЗОР ЛИТЕРАТУРЫ**

Так как главной задачей данного курсового проекта является разработка локальной сети для научно-исследовательской лаборатории, то необходимо в первую очередь изучить издания по проектированию локальных сетей. Далее приведено описание используемой литературы.

В книге [1] рассказаны основы локальных сетей. В первые три раздела посвящены базовым понятиям сетевых технологий, описанию видов, моделей и способам построения компьютерных сетей. Много внимания уделяется теоретическим и практическим вопросам организации сетей на основе стека проколов TCP/IP. Рассматриваются технологии, обеспечивающие реализацию сетей на основе IPv4 и IPv6. В четвертом и пятых разделах данного пособия посвящено таким общесетевым службам как DNS, электронная почта, FTP, веб, службам удаленной консоли и т.д. Физические основы построения локальных сетей раскрывается с в шестой главе пособия. Рассказывается о технологиях и стандартах кабельной сети Ethernet, беспроводных сетях Wi-Fi, а также виртуальных локальных сетях. Особое внимание уделяется практическому применению и проектированию сетей на основе вышеперечисленных технологий.

В книге [2] рассматриваются вопросы организации сетевых структур, типы, топологии, методы доступа, среда передачи информации, аппаратные компоненты компьютерных сетей, а также методы пакетной передачи данных. В перовой главе описываются общие понятия, основные топологические решения локальных сетей, протоколы и их типы. Вторая глава посвящена средствам и системам связи, в том числе кабельные (витая пара и коаксиальный кабель). Четвертая глава подробнее описывает технологии компьютерных сетей таких как Ethernet и FastEthernet, технические средства, оборудование и программное обеспечение локальных сетей. В пятой главе рассмотрены вопросы адресации внутри локальной сети, стек протоколов TCP/IP, проколы динамической маршрутизации RIP, протоколы транспортного уровня UDP и TCP.

В учебном пособии [3] изложены принципы работы коммутаторов L2 и L3. На практических примерах показаны варианты использования протокола STP. Описаны основные методы работы с коммутаторами: агрегирование каналов связи, обеспечение безопасности и качество обслуживания для интерфейсов, а также принципы статической и динамической маршрутизации.

Во второй главе книги [4] об общих принципах построения сетей. Данная тема освещена примерами построения простейших локальных сетей, состоящих из двух компьютеров. Поднимаются вопросы совместного использования ресурсов, связи с периферийными устройствами, использования средств связи между компьютерами, адресации узлов, коммутации и т.д. Третья глава посвящена принципам коммутации и буферизации пакетов в сети. В четвертой главе авторы подробно останавливаются на модели OSI и ее уровнях. В девятой главе рассказывается о беспроводных средах передачи данных: о преимуществе использования, линях связи, распространении электромагнитных волн. Приводятся примеры использования как, одного источника беспроводной связи и нескольких приемников, так и нескольких источников и нескольких приемников. Глава двенадцатая описывает коммутируемые сети Ethernet. Приведена классификация каналов Ethernet по скорости передачи данных и режимы работы каналов. Часть двадцать восьмой главы посвящена прокси-серверам: их назначению, принципу работы, возможностям фильтрации трафика, блокировки доступа к запрашиваемым пользователем ресурсам и создание списка приложений, которые могут оправлять запрос только через прокси-сервер.

Со второй по пятую главу книга [5] подробно рассказывает о уровнях сетевой модели OSI. Шестая глава посвящена беспроводным и мобильным сетям, описывающим их стандартам, разновидностям, адресации в таких сетях.

В электронном ресурсе [6] указана спецификация маршрутизатора Cisco C881-K9. В нем находится информация о количестве портов для локальных и глобальных сетей, скорости передачи данных через данные порты, способе настройки устройства, поддерживаемых протоколах, способах адресации.

Электронный ресурс [7] является спецификацией коммутатора Cisco WS-C2960-8TC-L. Из него можно узнать информацию о типе данного коммутатора, количестве портов, скорости передачи данных, поддерживаемых стандартах и протоколах.

Электронный ресурс [8] является спецификацией беспроводной точки доступа D-link DWL-2600AP. В нем находится информация о поддерживаемых данным устройством стандартах беспроводной связи.

В электронном ресурсе [9] подробно описана архитектура Router-on-a-Stick. В данной статье приведены примеры настройки маршрутизатора и коммутатора для данной архитектуры, область применения, топологии сети.

В электронном ресурсе [10] описана настройка программного обеспечения Kerio Winroute Firewall в качестве прокси-сервера.

# **2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ**

В соответствии с заданным вариантом необходимо реализовать сеть для научно-исследовательской лаборатории.

По условию задания лаборатория находится в подвальном помещении и делится на две части: исследовательскую и административную. Исследовательская часть состоит из трех помещений: лаборатория (21 м2) и два служебных помещения (10 м2). В административной части находятся три помещения: кабинет директора (10 м2), бухгалтерия (11 м2) и служебное помещение (5 м2).

В лаборатории будут размещены 5 стационарных подключения (4 персональных компьютера (ПК) и один сетевой принтер) и 5 мобильных подключений, а в служебных помещениях исследовательской части по 2 стационарных (2 ПК) и 2 мобильных подключений. В кабинете директора будет расположен один компьютер и один сетевой принтер, а в бухгалтерии один ПК и многофункциональное устройство, подключенное к ПК. По условию задания в служебном помещении административной части размещать какие-либо подключения не надо.

Так как в лаборатории сотрудники используют как рабочие станции, так и личные устройства, то имеет смысл изолировать их друг от друга. Одна из виртуальных подсетей (VLAN 10) будет выделена для рабочих целей, а вторая (VLAN 20) – для личных целей сотрудников. Использование виланов позволяет контролировать трафик, которых проходит через проектируемую сеть. Таким образом пакеты из одной виртуальной сети не смогут попадать в другую.

Структурная схема проектируемой сети представлена в приложении А.

# **3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ**

## **3.1 Выбор активного сетевого оборудования**

В данном курсовом проекте будет использоваться следующие компоненты активного сетевого оборудования:

1. маршрутизатор Cisco Cisco 881-K9
2. коммутатор Cisco WS-C2960-8TC-L
3. беспроводная точка доступа D-link DWL-2600AP

### 3.1.1 Маршрутизатор Cisco 881-K9

Маршрутизатор – сетевое устройство, используемое в компьютерных сетях передачи данных, которое, на основании информации о топологии сети (таблицы маршрутизации) и определённых правил, принимает решения о пересылке пакетов сетевого уровня модели OSI их получателю [2].

Основываясь на топологии сети, приведенной в приложении Б, и условии задания, которое ограничивает бюджет для использующихся компонентов, было решено выбрать маршрутизатор с одним портом для выхода в Интернет, поддержкой адресации IPv4 и IPv6, протоколов TCP/IP, HTTP и возможностью использования маршрутизатора в качестве DHCP-сервера.

Для реализации заданной топологии будет использоваться маршрутизатор Cisco 881-K9. Характеристики выбранного маршрутизатора перечислены в таблице 3.1.

Таблица 3.1 – характеристики маршрутизатора Cisco 881-K9

|  |  |
| --- | --- |
| Интерфейс Ethernet | 1 WAN-порт 10/100 Мбит/с, 4 LAN-порт 10/100 Мбит/с |
| Стандарты и протоколы | 802.1q(VLAN), DHCP, IPv4, IPv6, 6to4 tunneling |
| Рабочая влажность | От 10% до 90% |

### 3.1.2 Коммутатор Cisco WS-C2960-8TC-L

В данном проекте важной составляющей является коммутатор – устройство, предназначенное для объединения компонентов сети между собой.

Коммутаторы подразделяются на управляемые и неуправляемые. Неуправляемые коммутаторы не обладают интерфейсом для настройки и работают по принципу Plug-and-Play, то есть для использования устройства необходимо только подключить его к компонентам сети. Управляемые коммутаторы обладают консольным портом для настройки и расширенным набором функций, протоколами управления благодаря наличию процессора. Так как проектируемая сеть будет разделена на виланы, то необходимо использовать управляемый коммутатор.

В условии задания указано точное число стационарных подключений в научно-исследовательской организации (9 устройств для лаборатории и 3 для администрации), поэтому предпочтительно использовать коммутаторы с небольшим числом портов.

Для реализации проектируемой сети в качестве коммутатора была выбрана модель Cisco WS-C2960-8TC-L. Основный характеристики данной модели перечислены в таблице 3.2.

Таблица 3.2 – характеристики коммутатора Cisco WS-C2960-8TC-L

|  |  |
| --- | --- |
| Интерфейс Ethernet | 8 портов 10/100 Мбит/с |
| Консольный порт | RJ-232 |
| Таблица MAC-адресов | 8К |
| Соответствие стандартам | 802.1d (Spanning Tree Protocol), 802.1Q (VLAN) |
| Управление | Веб-интерфейс, Интерфейс командной строки (CLI) |
| Рабочая влажность | От 10% до 90% |

### 3.1.3 Беспроводная точка доступа D-link DWL-2600AP

Беспроводная точка доступа – устройство, предназначенное для обеспечения беспроводного соединения клиентов к существующей сети. Данная технология чаще всего используется для подключения устройств, не имеющих проводного интерфейса, к локальной сети.

Для реализации заданной сети необходимо использовать пять беспроводных точек доступа: три размещаются в исследовательской части, две в администрации.

Для обеспечения беспроводного доступа всех мобильных устройств к сети исследовательской лаборатории и сети Интернет была выбрана модель D-link DWL-2600AP. Данная модель поддерживает стандарты беспроводной связи 802.11b/g/n, имеет возможность конфигурирования через консольный порт. Для приема и передачи данных используются две внутренние антенны, которые поддерживают 2х2 MIMO. Для авторизации пользователей может использоваться WPA Personal/ Enterprise или WPA2 Personal/ Enterprise. Характеристики приведены в таблице 3.3.

Таблица 3.3 – характеристики WAP D-link DWL-2600AP

|  |  |
| --- | --- |
| Беспроводной интерфейс | 802.11b/g/n 2,4 ГГц |
| Интерфейс Ethernet | 1 порт 10/100 Мбит/с |
| Частота | 802.11b/g/n: 2,4 ГГц - 2,4835 ГГц |
| Режимы работы | Точка доступа, WDS, WDS + AP |
| Рабочая влажность | От 10% до 90% |

*Продолжение таблицы 3.3*

|  |  |
| --- | --- |
| Управление | Интерфейс командной строки (CLI), Веб-интерфейс, GUI, Telnet/SSH |

### 3.1.4 Повторитель Hikvision DS-1H34-0102P

Так как исследовательская и административная части находятся друг от друга на расстоянии 150 м, то необходимо позаботиться о том, чтобы сигнал с коммутатора из исследовательской части достигал маршрутизатора, расположенного в административной части. Коммутаторы и маршрутизатор используют тип соединения 100BASE-TX, максимальная длина передачи сигнала которого составляет 100 м. Очевидно, что этой длины недостаточно. Для решения этой проблемы будет использоваться повторитель сигнала Hikvision DS-1H34-0102P. Из небольшого количества представленных вариантов была выбрана это модель, так как она обладает степенью защиты IP-65, что соответствует защите от струй воды во всех направлениях, и усилением сигнала до 200 м.

## **3.2 Выбор рабочего оборудования**

### 3.2.1 Рабочая станция N-Tech King Office M 61367

При выборе рабочей станции учитывалась специфика задач, решаемых исследовательской лабораторией – проектирование, калибровка и тестирование измерительных приборов. Для этого необходим компьютер с хорошей аппаратной составляющей, поэтому в курсовой работе будет использоваться модель N-Tech King Office M 61367. Процессор Intel Core i5 8400 с частотой 2,8 Ггц и объем оперативной памяти в 8 Гб подойдут для сложных вычислений и обработки больших массивов данных. Характеристики модели приведены в таблице 3.4.

Таблица 3.4 – характеристики компьютера N-Tech King Office M 61367

|  |  |
| --- | --- |
| Модель процессора | Intel Core i5 8400 |
| Тактовая частота процессора | 2800 Мгц |
| Количество ядер | 6 |
| Тип оперативной памяти | DDR4 |
| Объем оперативной памяти | 8 Гб |
| Тип накопителя | HDD |
| Объем накопителя | 1000 ГБ |

### 3.2.2 Многофункциональное устройство HP LaserJet Pro M28w

Для сотрудников администрации было выбрано многофункциональное устройство модели HP LaserJet Pro M28w. Данная модель имеет возможность копирования и печати со скоростью 18 станиц в минуту. Предположительный ресурс картриджа составляет 1000 страниц. Черно-белая печать производится в формате А4, чего будет достаточно для сотрудников администрации. Подключается устройство к компьютеру через USB.

### 3.2.3 Принтер Xerox Phaser 3260DNI

Так как устройство будет подключено к коммутатору, то при выборе модели необходимо учитывать наличие Ethernet интерфейса. Качество печати не играет большой роли при использовании принтера в администрации, поэтому предпочтительно выбирать принтер с лазерной технологией печати. Преимуществом данной технологии являются небольшая стоимость и большой срок годности тонера-порошка и картриджа. Черно-белая печать производится в формате А4 со скоростью 28 страниц в минуту.

## **3.3 Схема адресации, настройка DHCP и SSH**

Адресации в проектируемой локальной сети осуществляется по протоколам IPv4 и IPv6. Выделенная подсеть IPv6 будет разделена на три подсети: подсеть для администрирования сетевого оборудования, подсеть для рабочих станций и подсеть для личных устройств.

Таблица 3.6 – соответствие виртуальной подсети и адресов протокола IPv6

|  |  |
| --- | --- |
| Номер VLAN | Подсеть |
| 2 | FD:0:0:1::/66 |
| 10 | FD:0:0:1:4000::/66 |
| 20 | FD:0:0:1:8000::/65 |

Для того, чтобы реализовать возможность удаленной настройки активного сетевого оборудования, необходимо назначить адреса для всех сетевых устройств из административного вилана.

Таблица 3.7 – адреса протокола IPv6 для устройств в административной сети

|  |  |
| --- | --- |
| Имя хоста | Адрес |
| Router-1 | FD:0:0:1::1/66 |
| Switch-1 | FD:0:0:1::2/66 |
| Switch-2 | FD:0:0:1::3/66 |
| Switch-3 | FD:0:0:1::4/66 |
| Point-1 | FD:0:0:1::5/66 |
| Point-2 | FD:0:0:1::6/66 |
| Point-3 | FD:0:0:1::7/66 |
| Point-4 | FD:0:0:1::8/66 |
| Point-5 | FD:0:0:1::9/66 |

Для обеспечения защищенного доступа к консоли активного сетевого оборудования необходимо настроить административный вилан. Для этого сначала следует на каждом устройстве настроить протокол SSH:

enable

configure terminal

ip domain name [имя домена]

crypto key generate rsa

service password – encryption

username admin privilege 15 password 7 password

line vty 0 4

transport input ssh

logging synchronous

exec–timeout 60 0

exit

Затем на каждом коммутаторе необходимо создать интерфейс для административного вилана:

enable

configure terminal

interface vlan 2

ipv6 address [адрес хоста]

На маршрутизаторе создаем подинтерфейс для административного вилана:

enable

configure terminal

interface f0/1.2

ipv6 address [FD:0:0:1::1/66]

Далее настроим на маршрутизаторе протокол DHCP, который динамически раздает IP-адрес устройству. Первым делом создаем на коммутаторах виртуальные подсети:

enable

configure terminal

vlan 2

name Admin

vlan 10

name Work

vlan 20

name Personal

Далее необходимо настроить интерфейсы каждого коммутатора. Для интерфейсов, связанных с оконечным устройством, настраиваем режим access и дополнительно настраиваем защиту от несанкционированного доступа по данному интерфейсу:

enable

configure terminal

interface [номер интерфейса]

switchport mode access

switchport access vlan [номер виртуальной подсети]

switchport port-security

switchport port-security maximum 1

switchport port-security mac-address sticky

switchport port-security violation restrict

Для остальных интерфейсов настраиваем режим trunk:

enable

configure terminal

interface [номер интерфейса]

switchport mode trunk

switchport trunk allowed vlan 10,20

После этого переходим к настройке маршрутизатора. Для этого нужно выполнить следующие пункты:

1. Создать и настроить пул адресов для виртуальных подсетей:

enable

configure terminal

ipv6 local pool GPvlan10 fd:0:0:1::/65 65

ipv6 dhcp pool vlan10

prefix-delegation pool GPvlan10

ipv6 local pool GPvlan20 fd:0:0:1:8000::/65 65

ipv6 dhcp pool vlan20

prefix-delegation pool GPvlan20

1. Настроить интерфейс, связанный с коммутатором:

enable

configure terminal

ipv6 unicast-routing

interface f0/1

no shutdown

interface f0/1.10

encapsulation dot1q 10

ipv6 dhcp server vlan10

interface f0/1.20

encapsulation dot1q 20

ipv6 dhcp server vlan20

## **3.4 Настройка туннеля IPv6-over-IPv4**

Для обеспечения выхода в Интернет необходимо настроить туннель для инкапсуляции пакетов с протоколом IPv6 в IPv4. Такой туннель настраивается на интерфейсе маршрутизатора, связанным с коммутатором:

interface tunnel 10

tunnel source f0/1.10

tunnel destination 80.94.0.1

tunnel mode ipv6ip

exit

interface tunnel 20

tunnel source f0/1.20

tunnel destination 80.94.0.2

tunnel mode ipv6ip

## **3.6 Настройка прокси-сервера**

При проектировании данной локальной сети необходимо реализовать доступ пользователей в Интернет через прокси-сервер. Для этого будет использоваться комплекс для управления подключением локальной сети к Интернету Kerio Control.

Для начала необходимо скачать Kerio Control с официального сайта производителя и распаковать его. Далее запускается инсталлятор и производится установка программного обеспечения.

При первом запуске программы будет запущен «Мастер настройки». В любой момент времени «Мастер настроек» можно запустить еще раз, выбрав вкладку «Политика трафика» в консоли администратора.

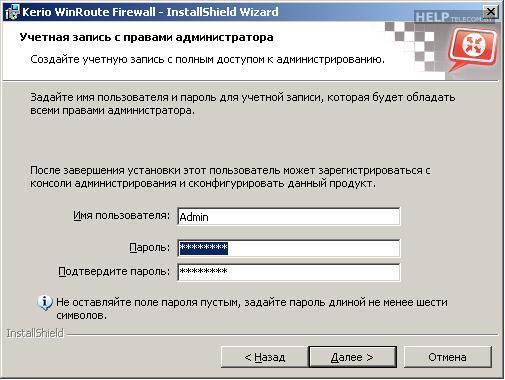


Рисунок 3.1– создание административной учетной записи при установке Kerio Control

Одной из возможностей прокси-сервера является кэширование запросов пользователей. В таком случае при повторном запросе ресурса данные будут загружены не из Интернета, а из сохраненной копи. Данные будут находиться в кэше до тех пор, пока не будут вытеснены более востребованным ресурсом. Это позволяет уменьшить время доступа к запрашиваемым данным. Для настройки кэшируемого прокси-сервера в программе Kerio Control необходимо перейти на вкладку «Кэш» и выбрать те настройки, которые указаны на рисунке 3.2. После этого следует перейти на вкладку «Прокси-сервер» и включить параметры, которые указаны на рисунке 3.3.

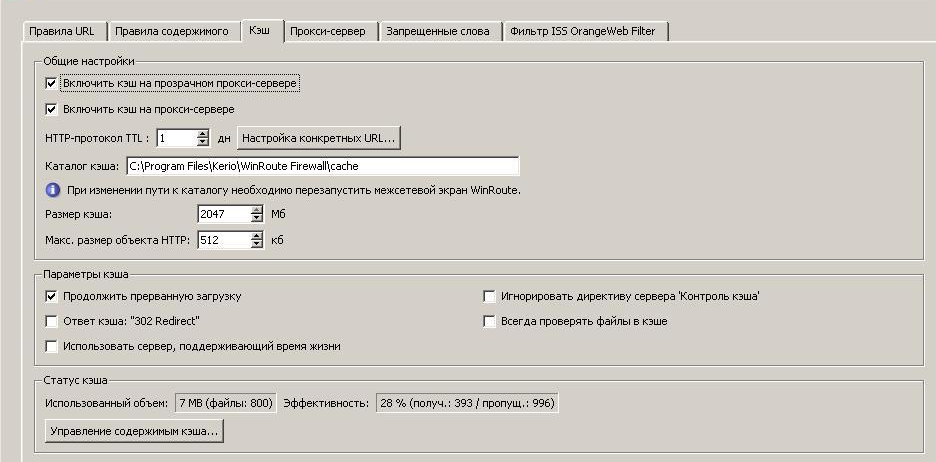


Рисунок 3.2 – настройка кэша для прокси-сервера

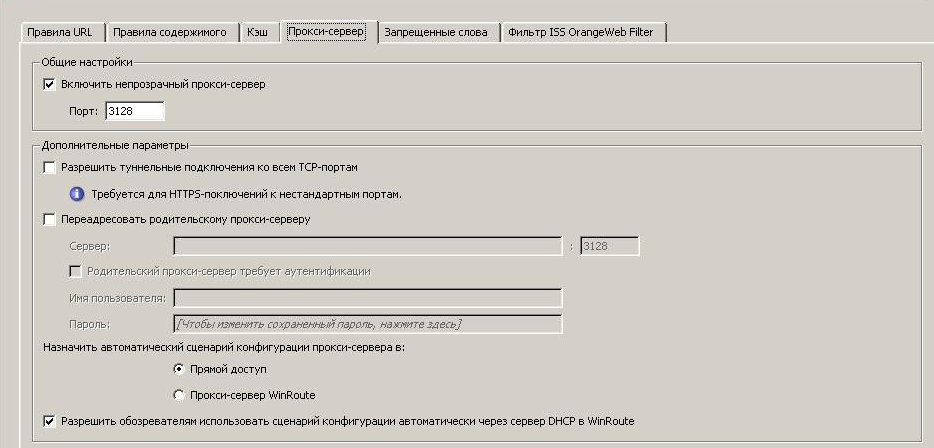


Рисунок 3.3 – настройка прокси-сервера

## **3.7 Настройка беспроводной точки доступа**

Настройка беспроводной точки доступа происходит через web-интерфейс. Подробная инструкция по конфигурированию описана в руководстве пользователя [11].

Для входа на беспроводную точку доступа необходимо подключить ее к компьютеру, в браузере ввести адрес 10.90.90.91 и в появившимся окне ввести логин admin и пароль admin. После успешного подключения появится страница с базовыми настройками точки доступа (рисунок 3.4). Так как маршрутизатор в сети работает как DHCP-сервер, то в настройках следует указать, что беспроводная точка доступа является DHCP-клиентом.

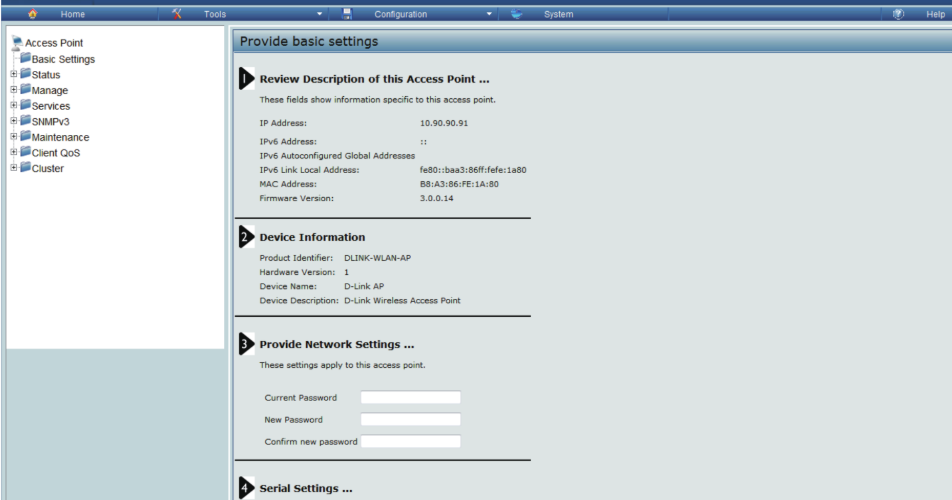


Рисунок 3.4 – базовая настройка беспроводной точки доступа

Для настройки беспроводного интерфейса нужно перейти вкладку «Wireless settings». Появится страница, в которой можно указать протокол беспроводной (рисунок 3.5).

Wireless settings describe aspects of the local area network (LAN) related specically to the radio device in the

access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access

Wireless settings describe aspects of the local area network (LAN) related specically to the radio device in the

access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access

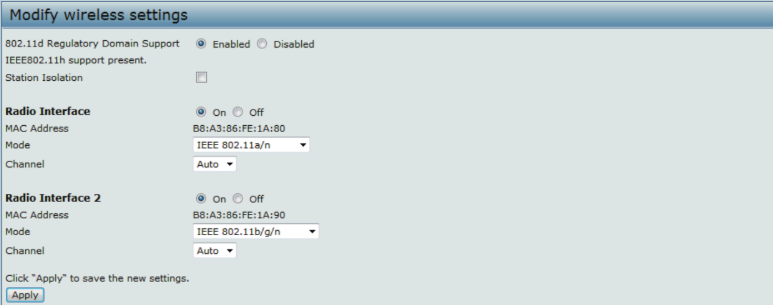


Рисунок 3.5 – настройка беспроводных интерфейсов

Далее необходимо обеспечить защиту доступа к беспроводной сети. В начале необходимо задать SSID (Service Set Indicator) для точки доступа. Сперва следует перейти на вкладку «VAP» и указать SSID (рисунок 3.6). Затем необходимо в пункте «Security» задать в качестве параметра значение «WPA Personal». При данном режиме обязательно указывается пароль, который необходимо будет ввести пользователю при подключении к данной беспроводной точке.

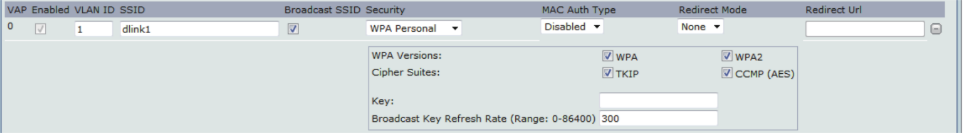


Рисунок 3.6 – настройка SSID для точки доступа

Далее необходимо настроить фильтр MAC-адресов на беспроводной точке доступа. В зависимости от того, как настроить фильтр, можно запретить доступ к точке станциям с указанными MAC-адресами, либо же разрешить доступ только перечисленным устройствам.

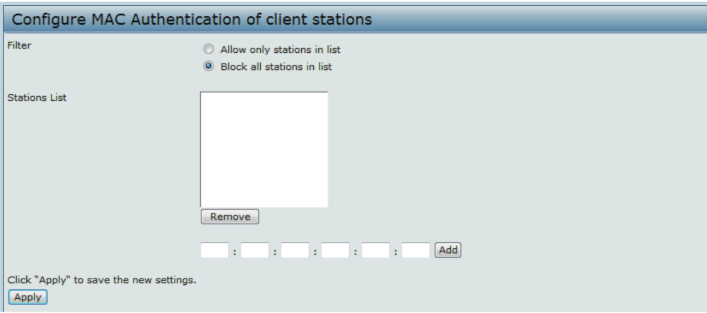


Рисунок 3.7 – настройка фильтра MAC-адресов

Если на вкладке «MAC Authentication» выбрать пункт «Allow only stations in list», то к точке доступа смогут подключаться только станции из списка разрешенных MAC-адресов. Если выбрать пункт «Block all stations in list», то будет заблокированы все устройства из списка. Для подтверждения списка MAC-адресов требуется нажать кнопке «Apply».

Также необходимо настроить SSH на точке доступа. Для этого необходимо перейти на вкладку SSH и выбрать пункт «Enable» в графе «SSH Status». Для подтверждения следует нажать кнопку «Apply».

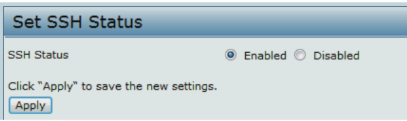


Рисунок 3.8 – настройка SSH на беспроводной точке доступа

## **3.8 Настройка сетевого принтера**

Для настройки принтера необходимо для начала подключить его в информационную розетку. Затем на одном их стационарных компьютеров зайти в «Панель управления» в раздел «Принтеры и сканеры». В появившемся окне выбрать пункт «Добавить принтер или сканер». После того как компьютер выведет список обнаруженных устройств, выбрать принтер и нажать на кнопку «Добавить устройство».

Для предоставления общего доступа к принтеру нужно перейти в свойства устройства. В разделе «Доступ» установить флаг в поле «Общий доступ к этому принтеру». Так как в проектируемой сети подключено два сетевых принтера, то необходимо дать им разные имена (Printer-1 и Printer-2).

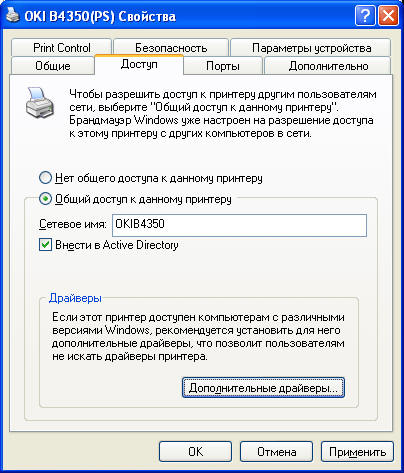


Рисунок 3.7 – настройка сетевого принтера

**4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СИСТЕМЫ**

## **4.1 Кабельная система**

Пассивным является оборудование, не питающееся от электричества и не усиливающее сигнал между устройствами. Таким оборудованием являются кабели, информационные розетки, монтажные шкафы.

В данной курсовой работе будут использоваться неэкранированная витая пара категории 5е Klotz RC5-SB1X, коннектор RJ-45 TWT 8P8C UTP cat 5e, и компьютерная информационная розетка TWT.SM1-45-WH.

В связи с тем, что исследовательская лаборатория находится в подвальном помещении, необходимо использовать сетевой кабель с повышенной защитой от влажности. Для этого была выбрана витая пара Klotz RC5-SB1X. Внутренние многожильные проводники, образующие пары, заключены в полиэтиленовый крестообразный разделитель. Это гарантирует сохранение механической структуры кабеля при мобильном использовании. Дополнительной защитой служит прочная оболочка из специального полимера на основе полиуретана.

Для дополнительной защиты кабельной системы от механических воздействий будут использоваться алюминиевые коробы, через которые будут проводиться кабели.

При проектировании локальной сети кабельная система была реализована с использованием FastEthernet.

## **4.2 Организация рабочих мест**

Исследовательская лаборатория делиться на две части: исследовательская и административная. Исследовательская часть состоит из лаборатории и двух служебных помещений.

В лаборатории расположено пять стационарных устройств (одно из которых сетевой принтер) и 5 мобильных подключений, в служебных помещениях по два стационарных устройства и 2 мобильных подключения.

В административной части находятся кабинет директора, бухгалтерия и служебное помещение. В кабинете директора расположено два стационарных устройств (одно из которых сетевой принтер) и пять мобильных подключений. В бухгалтерии одно стационарное устройство, к которому подключено многофункциональное устройство, и одно мобильное подключение. В служебном помещении не содержится никакого оборудования.

Подключение рабочих станций и принтеров осуществляется через информационные розетки, которые находят возле каждого рабочего места.

## **4.3 Защита оборудования от влаги**

Для обеспечения защиты оборудования будет использоваться телекоммуникационные шкафы. Это не только предотвратит поломку оборудования при повышенной влажности, но и защитит от несанкционированного доступа к сетевому оборудованию, так как телекоммуникационные шкафы закрываются на ключ. Установка оборудования в телекоммуникационный шкаф позволит администраторам быстрее и легче находить неисправности.

При проектировании данной локальной сети будет использоваться телекоммуникационный шкаф LAN-DC-CBP4-42Ux6x10. Данный шкаф имеет кабеля для заземления, а также доступ к устройству с любой стороны.

Поскольку телекоммуникационный шкаф имеет четыре секции, установка коммутаторов, для подключения пользователей, будет произведена в верхнюю секцию. Установка маршрутизатора будет производиться во вторую сверху секцию. Учитывая рекомендации стандарта TAI–942 рекомендуется установить телекоммуникационный шкаф на фальшпол, для того чтобы произвести установку системы кондиционирования воздуха, а также электроснабжения, в том числе и источников бесперебойного электропитания.

## **4.4 Расчет качества связи для беспроводных точек доступа**

При реализации проектируемой сети будут использоваться беспроводные точки доступа, поддерживающие стандарт беспроводной связи 802.11n. Этот стандарт работает на частотах в 2,4 и 5 ГГц. В данном случае точки доступа работают на частоте 2,4 ГГц. Рассчитаем значение затухания радиоволн по формуле:

L = 32,44 + 20lg(F) + 20lg(D), dB, (4.1)

где F – частота в GHz, D – расстояние в метрах

Произведем расчет затухания для самых дальних подключенных устройств в административной и исследовательских частях. Предположим, что в административной части здания точка доступа будет находится в бухгалтерии. Это помещение с размерами 2х5,5 метров, а самое удаленное устройство находится в кабинете директора с размерами 5х2 метров. Если предположить, что точка доступа будет находиться посредине помещения, то расстояние между устройством и точкой доступа приблизительно равно 5 метрам. Подставим значения в формулу 4.1:

L = 32,44 + 20lg(2,4) + 20lg(5) = 32,44 + 7,6 + 13,98 = 54,02 dB

Предположим, что в исследовательской части здания точка доступа будет находится в первом служебном помещении. Это помещение с размерами 5х2 метров, а самое удаленное устройство находится в лаборатории с размерами 3х7 метров. Если предположить, что точка доступа будет находиться посредине помещения, то расстояние между устройством и точкой доступа приблизительно равно 8 метрам. Подставим значения в формулу 4.1:

L = 32,44 + 20lg(2,4) + 20lg(8) = 32,44 + 7,6 + 18,06 = 58,1 dB

В таблице 4.1 приведены типы препятствий и их эффективное расстояние радиочастотного сигнала.

Таблица 4.1 – типы препятствий для радиочастотных сигналов

|  |  |  |
| --- | --- | --- |
| Тип препятствия | Дополнительные потери (dB) | Эффективное расстояние |
| Открытое пространство | 0 | 100% |
| Межкомнатная стена (15,2 см) | 15-20 | 15% |
| Несущая стена (30,5 см) | 20-25 | 10-15% |
| Монолитное железобетонное перекрытие | 20-25 | 10% |

Учитывая, что комнаты разделяют обычные межкомнатные стены, то дополнительные потери составляют 15% от значения изначального сигнала беспроводной точки доступа.

После данных расчетов было стало очевидно, что размещение по одной беспроводной точки в каждой части исследовательской лаборатории будет недостаточно для обеспечения всех беспородных устройств. Поэтому было принято решение о размещении беспроводной точки доступа в каждом помещении организации (кроме служебного помещения в административной части).

## **4.5 Монтаж беспроводной точки доступа**

Для монтажа беспроводной точки доступа сперва необходимо изучить руководство по установке «Quick Installation Guide 802.11n Unified Access Point» [12].

Следующие шаги используются, чтобы установить точку доступа D-Link DWL-2600AP на потолочных перекладинах:

1) зафиксировать два потолочных кронштейна на потолочных перекладинах. Убедиться, что оба кронштейна установлены параллельно друг другу;

2) использовать винты, входящие в комплект, чтобы зафиксировать монтажное кольцо на потолочных кронштейнах;

3) подключить кабель к порту LAN на точке доступа;

4) закрепить беспроводную точку доступа на монтажное кольцо. Повернуть устройство по часовой стрелке, чтобы зафиксировать его в нужном положении.

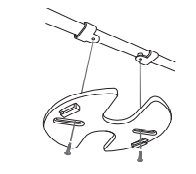


Рисунок 4.1 – фиксация крепежного кольца на потолочных кронштейнах

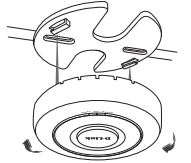


Рисунок 4.2 – крепление беспроводной точки доступа на потолочных перекладинах

Еще одним вариантом монтажа беспроводной точки доступа является монтаж с помощью анкерных болтов:

1. поместить крепежное кольцо на стену или потолок;
2. отметить точки, в которые будут вставляться анкерные болты;
3. просверлить отверстия в отмеченных местах и вставить пластиковые настенные анкеры;
4. использовать винты, которые идут в комплекте;
5. подключить кабель к порту LAN на точке доступа;
6. чтобы прикрепить беспроводную точку доступа к монтажному кольцу для начала следует найти на его правой стороне надпись «Open-Lock». Далее необходимо найти маленькое крепление на точке доступа и приложить его к надписи на монтажном кольце;
7. повернуть точку доступа по часовой стрелке до фиксации устройства. Крепление на устройстве должно указывать на надпись «Close text» на монтажном кольце.

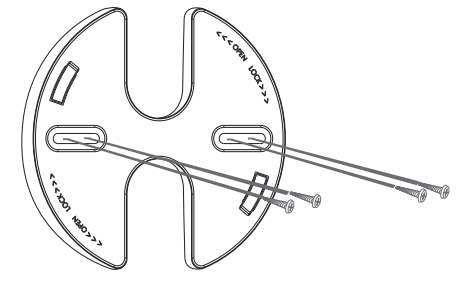


Рисунок 4.3 – крепление монтажного кольца к стене

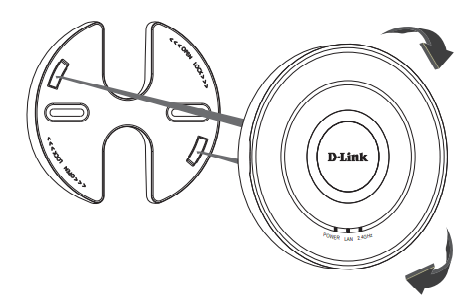


Рисунок 4.4 – крепление беспроводной точки доступа к монтажному кольцу на стене

# **ЗАКЛЮЧЕНИЕ**

При выполнении данной курсовой работы была спроектирована локальная сеть для научно-исследовательской лаборатории. Были учтены все пожелание заказчика, такие как закупка оборудования средней ценовой категории, защита оборудования и кабельной системы от влажности и выход в сеть Internet через собственный прокси-сервер.

В ходе курсовой работы была спроектированы план помещений в лаборатории и топология сети, проанализированы варианты сетевого оборудования и выбраны модели, подходящие к условиям заказчика. Было выбрано такое оборудование, как коммутатор, маршрутизатор, сетевой принтер, многофункциональное устройство, беспроводная точка доступа и рабочая станция.

Данная курсовая работа пополнила знания о взаимодействии активных сетевых устройств друг с другом, настройках оборудования, особенностях использования прокси-серверов, подключении и применении сетевых принтеров, методах защиты от влажности.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

[1] Сергеев, А.Н. Основы локальных компьютерных сетей: Учебное пособие / А.Н. Сергеев. – СПб: Издательство «Лань», 2016. – 184 с.

[2] Максимов Н.В. Компьютерные сети: учебное пособия для студентов учреждений среднего профессионального образования / Н.В. Максимов, И.И. Попов. – М.: ФОРУМ, 2016. – 464 с.

[3] Технологии коммутации и маршрутизации в локальных компьютерных сетях: учебное пособие Е.В. Смирнова [и др.]. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2013. – 398 с.

[4] Олифер В. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов / В. Олифер, Н. Олифер. – СПб: Питер, 2016. – 992 с.

[5] Кроуз Дж. Компьютерные сети: Нисходящий поток / Дж. Кроуз, К. Росс. – Москва: Издательство «Э», 2016. – 912 с.

[6] Спецификация маршрутизатора Cisco С881-K9 [Электронный ресурс] – Электронные данные. – Режим доступа: https://www.router-switch.com/pdf/c881-k9-datasheet.pdf-Дата доступа: 03.12.2019

[7] Спецификация коммутатора Cisco SRW208G [Электронный ресурс] – Электронные данные. – Режим доступа: http://itlogin.co.kr/?module=file&act=procFileDownload&file\_srl=1508&sid=c020e0a067adf10f82c6ce46a8876f53&module\_srl=396-Дата доступа: 03.12.2019

[8] Спецификация беспроводной точки доступа D-link DWL-2600AP [Электронный ресурс] – Электронные данные. – Режим доступа: http://www.dlink.co.in/pdfs/products/DWL-2600AP/DWL-2600AP\_ds.pdf-Дата доступа: 03.12.2019

[9] Архитектура Router-on-a-Stick в сети передачи данных [Электронный ресурс] – Электронные данные. – Режим доступа: https://habr.com/ru/post/138573/-Дата доступа: 30.11.2019

[10] Настройка Proxy/DHCP сервера на базе Kerio Winroute Firewall [Электронный ресурс] – Электронные данные. – Режим доступа: http://help.a1.by/faq/problems/setting\_computer/preferences/~group\_id=2~id=269-Дата доступа: 04.12.2019

[11] Руководство пользователя – Электронные данные. – Режим доступа: https://mcgrp.ru/files/viewer/203430/1 -Дата доступа: 10.12.2019

[12] Краткое руководство по установке – Электронный данные. – Режим доступа: https://mcgrp.ru/files/get/203429 - Дата доступа: 19.12.2019

# ПРИЛОЖЕНИЕ А

(обязательное)

Схема структурная

# ПРИЛОЖЕНИЕ Б

(обязательное)

Схема функциональная

# ПРИЛОЖЕНИЕ В

(обязательное)

План этажа. Администрация

# ПРИЛОЖЕНИЕ Г

(обязательное)

План этажа. Исследовательская часть

# ПРИЛОЖЕНИЕ Д

(обязательное)

Перечень оборудования