СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc152164031)

[1 ОБЗОР ЛИТЕРАТУРЫ 4](#_Toc152164032)

[2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 5](#_Toc152164033)

[2.1 Выбор топологии сети 6](#_Toc152164034)

[3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 8](#_Toc152164035)

[3.1 Обоснование выбора активного сетевого оборудования 8](#_Toc152164036)

[3.1.1 Маршрутизатор D-link DSA-2006 8](#_Toc152164037)

[3.1.2 Коммутатор D-Link DGS-1250-28XMP 9](#_Toc152164038)

[3.1.3 Точка доступа D-Link DWL-8620AP 10](#_Toc152164039)

[3.1.4 Контроллер точек доступа D-Link DWC-1000 С1 12](#_Toc152164040)

[3.1.5 Рабочая станция HP Slim S01-aF0020ur 376B6EA 13](#_Toc152164041)

[3.1.6 Сервер Dell PowerEdge R250 Rack Server 14](#_Toc152164042)

[3.1.7 МФУ Xerox B215 с факсом 15](#_Toc152164043)

[3.1.8 Проектор Rombica Ray Box B1 (MPR-L770) 15](#_Toc152164044)

[3.2 Пассивное сетевое оборудование и кабеля 16](#_Toc152164045)

[3.2.1 Выбор телекоммуникационного шкафа 16](#_Toc152164046)

[3.2.2 Выбор кабеля 16](#_Toc152164047)

[3.2.3 Выбор коннектора, короба и розетки 16](#_Toc152164048)

[3.3 Обоснование выбора ПО 17](#_Toc152164049)

[3.4 Адресация в локальной компьютерной сети 18](#_Toc152164050)

[3.5 Настройка сетевого оборудования 19](#_Toc152164051)

[3.5.1 Настройка маршрутизатора 19](#_Toc152164052)

[3.5.2 Настройка коммутаторов 23](#_Toc152164053)

[3.5.3 Настройка контроллера и точек доступа 26](#_Toc152164054)

[3.5.4 Настройка RADIUS-сервера 29](#_Toc152164055)

[3.5.5 Настройка МФУ с факсом 30](#_Toc152164056)

[3.5.6 Настройка веб-сервера 31](#_Toc152164057)

[3.5.7 Настройка ПК 33](#_Toc152164058)

[4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ 36](#_Toc152164059)

[ЗАКЛЮЧЕНИЕ 37](#_Toc152164060)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 38](#_Toc152164061)

[ПРИЛОЖЕНИЕ А 39](#_Toc152164062)

[ПРИЛОЖЕНИЕ Б 40](#_Toc152164063)

[ПРИЛОЖЕНИЕ В 41](#_Toc152164064)

[ПРИЛОЖЕНИЕ Г 42](#_Toc152164065)

[ПРИЛОЖЕНИЕ Д 43](#_Toc152164066)

# ВВЕДЕНИЕ

В рамках данного курсового проекта рассматривается разработка и проектирование корпоративной сети для небольшой обувной компании. Компьютерные сети в обувных компаниях используются для управления за-пасами, обработки онлайн-заказов, обмена данными между отделами и роз-ничными точками, а также для обеспечения взаимодействия с клиентами и поставщиками.

Объект располагает г-образным одноэтажным зданием общей пло-щадью 330 квадратных метров. На текущий момент, в организации 15 ста-ционарных пользователей и предусмотрено 16 стационарных подключений, а также 16 мобильных подключений. Для обеспечения внутреннего и внеш-него взаимодействия с клиентами и партнерами, компания использует web-сервер. Кроме того, в инфраструктуре присутствуют принтеры, включая цветные модели.

Цель данной курсовой работы - создание оптимальной и эффективной сетевой инфраструктуры, обеспечивающей надежное подключение к интернету через Multigigabit Ethernet, используя статический внешний IPv4-адрес и публичную подсеть для внутренней адресации IPv4. Подключение к сети Internet предусмотрено по протоколу IPv6, и для этого будет использо-ван блок адресов, специфичный для Беларуси.

Этот проект предназначен, прежде всего, для руководства и IT-специалистов обувной компании, чтобы они могли обеспечивать беспере-бойную и надежную работу всей сети. Проектирование сети будет основано на оборудовании производителя Cisco. Помимо этого, особое внимание будет уделено вопросам безопасности: протоколирование всех сессий доступа из сети Internet и в неё. Несмотря на отсутствие специфических требований к надежности, основной акцент сделан на создании полноценной коммерческой сети. В будущем, организация может расширяться, поэтому стоит учесть это при построении сети.

В ходе данного курсового проекта необходимо решить следующие задачи: разработка структуры сети, подбор необходимого сетевого и око-нечного оборудования, которое будет решать поставленные задачи, настройка и конфигурация устройств, а также разработка функциональной схемы. Эти данные и разработанные решения смогут значительно улучшить работу и подойдут для широкого круга организаций, стремящихся к современным стандартам сетевой инфраструктуры для бизнес-решений.

# 1 ОБЗОР ЛИТЕРАТУРЫ

Для выполнения данной курсовой работы были использованы статьи, видео-уроки, научная и учебно-методическая литература, документация и материалы, представленные на сайтах и форумах, специализирующихся на сетях.

Книга Эндрю Таненбаума «Компьютерные сети» [8] предоставила подробный разбор всех аспектов и уровней организации сетей.

На страницах книги «Компьютерные сети. Принципы, технологии, протоколы» [4] структурирована и детально подана информация об управлении локальными сетями для малого и крупного бизнеса.

Книга «Основы локальных компьютерных сетей» [8] предоставляет основы построения локальных компьютерных сетей.

Официальные инструкции D-Link [3] и [5] описывают построение проводных и беспроводных локальных сетей среднего размера.

Источник [2] предоставил подробную информацию о VLAN, о их настройке на коммутаторах D-Link, о принципе работы коммутатора с виртуальными сетями, о настройке маршрутизации между виртуальными сетями посредством маршрутизатора. Также предоставил информацию о «port-security, native VLAN» и примеры настройки простых и сложных локальных сетей с использованием VLAN.

При настройке точки беспроводного доступа возникли проблемы в понимании BVI интерфейса. В поисках информации по нему пришлось прошерстить источник [6].

Источник [7] – документация по установке принтера.

Источник [9] – гайд по установке Nginx web-сервера

.

# 

# 2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе будет рассмотрена структура локальной сети для небольшой обувной компании. Данный раздел сопровождает чертеж схемы СКС структурной (приложение «А»).

В одноэтажном здании Г-образной формы, площадью 330 м², расположена небольшая обувная фабрика. В здании присутствует ограниченный доступ для посетителей. Сетевая инфраструктура организована для обеспечения эффективной работы производственных и административных процессов.

На входе в здание расположен ресепшн (вахта) с компьютером и принтером. В центральной части здания, вдоль основного коридора, размещены рабочие места для административного персонала. Столы для рабочих мест организованы вдоль стен с учетом прокладки подпольного кабеля для стационарных подключений.

В одном из углов здания размещена небольшая комната для принтеров, подключенных к внутренней сети. Это обеспечивает удобство печати документов для сотрудников.

В зоне производства предусмотрены рабочие места с компьютерными станциями для управления производственными процессами. В каждой производственной зоне установлена по одной WiFi-точке доступа для обеспечения мобильной связи сети.

Конференц-зал, расположенный в другом углу здания, оснащен проектором с HDMI-подключением и несколькими розетками RJ-45 для проводного подключения к сети.

В последней части здания находится серверная комната со всей коммутацией, обеспечивающая стабильную работу внутренней и внешней сети. Серверная оборудована web-сервером организации с доступом изнутри и снаружи.

Для сети предусмотрено 16 стационарных подключений и 16 мобильных подключений, что соответствует количеству сотрудников фабрики и их потребностям в подключении. В качестве протокола безопасности используется WPA2-Enterprise. Гостевой WiFi не предусмотрен, учитывая конфиденциальный характер работы фабрики.

Сеть должна быть отказоустойчивой, с коммерческим уровнем защиты, обеспечивать удобство эксплуатации пользователями и легкость администрирования.

В данном разделе будет рассмотрена структура локальной сети для небольшой обувной компании. Данный раздел сопровождает чертеж схемы СКС структурной (приложение «А»).

В одноэтажном здании, площадью 330 м2, присутствует небольшая обувная компания, которая имеет ограниченный доступ для посетителей, но при этом требует хорошего системного комплекса для обеспечения медицинских исследований. На первом этаже у входа будет ресепшен (вахта) с ПК собственным принтером. Далее по обе стороны коридора, проходящего по центру, будет опенспейс, где исследователи будут сидеть за ПК, столы для рабочих мест располагаются с двух сторон вдоль прокладки подпольного кабеля. Далее по коридору будет располагаться комната для принтеров, работающих по внутренней сети, дабы сотрудники могли удобно печатать свои отчеты. В конце коридора будет располагаться две переговорные с проекторами и розетками под RJ-45. Подключение к проекторам будет происходить по HDMI. В самом конце коридора будет находиться серверная комната со всей коммутацией и web-сервером организации, к которому будут иметь доступ как внутри, так и извне. Необходимо обеспечить как стационарное, так и беспроводное подключения WiFi во всех помещениях для внутреннего использования.

В структурном проектировании необходимо учитывать возможное количество подключений и от данных параметров отталкиваться в проектирование сети.

Максимальное стационарных подключений: 50 станций. Беспроводных подключений: 30. Будем предполагать, что работа этой лаборатории секретна и не предполагает присутствие посетителей, поэтому гостевой WiFi избыточен, как протокол безопасности используем WPA2-Enterprise.

В главном зале – опенспейсе – расположится две точки доступа WiFi. В переговорных будет проведено как минимум 6 розеток для подключения в сеть, для удобства работы на собраниях.

Требования обозначены так, что сеть должна иметь резервные подключения для обеспечения надежности, а также сеть должна быть коммерческого уровня: то есть обеспечивать как удобную эксплуатацию пользователями, так и иметь удобное администрирование, иметь многоуровневую защиту и отказоустойчивость.

## Выбор топологии сети

Выбранная физическая топология проектируемой сети – «звезда».

Логическая структура сети будет построена на использовании Virtual LAN. Виртуальные сети позволяют построить на базе одной физической сети некоторое количество логических.

Все стационарные станции, а также точки для беспроводного доступа будут подключены к коммутатору. Коммутатор в свою очередь будет подключен к маршрутизатору, который и будет обеспечивать выход в интернет и маршрутизацию внутри VLAN.

Маршрутизатор, коммутатор, web-сервер, контроллер беспроводных точек будут находиться в закрытом служебном помещении, что обеспечит дополнительную защиту от физического взлома посторонними лицами. Точек беспроводного доступа будет несколько.

В рамках данного проекта сеть предприятия будет разделена на 5 подсетей:

1. Подсеть административная.
2. Подсеть производственная.
3. Подсеть мобильных точек.
4. Подсеть для внутренних устройств и ПК.
5. Подсеть для Web-сервера, с выходом в интернет.

# 3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описывается функционирование аппаратной и программной части локальной компьютерной сети, обоснование выбора аппаратной части и описание основных настроек всех устройств.

## 3.1 Обоснование выбора активного сетевого оборудования

В данном подразделе курсового проектирования приводится описание всего выбранного сетевого оборудования и обоснование конкретного выбора. При выборе данного вида оборудования необходимо было руководствоваться такими параметрами как производительность, надёжность, бюджетность и, самое главное, оборудование должно отвечать всем необходимым требованиям заказчика. Выбор был сделан в пользу следующего активного сетевого оборудования (см. Приложение Г):

1 Маршрутизатор D-link DSA-2006.

2 Коммутатор D-Link DGS-1250-28XMP.

3 Точка доступа D-Link DWL-8620AP.

4 Контроллер точек доступа D-Link DWC-1000 С1.

5 Рабочая станция HP Slim S01-aF0020ur 376B6EA.

6 Сервер Dell PowerEdge R250 Rack Server 1U.

7 МФУ Xerox B215 с факсом.

8 Проектор Rombica Ray Box B1 (MPR-L770).

### 3.1.1 Маршрутизатор D-link DSA-2006

При выборе маршрутизатора, выбор пал на маршрутизатор D-link DSA-2006 ввиду его небольшой стоимости и характеристик, полностью удовлетворяющих потребности заказчика. Данный маршрутизатор оснащен встроенным сетевым экраном, что позволит нам предоставить доступ определенным VLAN без использования дополнительного оборудования.

Для настройки маршрутизатора DSA-2006 используется простой и удобный встроенный web-интерфейс (доступен на двух языках – русском и английском). Мастер настройки позволяет быстро перевести DSA-2006 в режим маршрутизатора (для подключения к проводному или беспроводному провайдеру), точки доступа, повторителя или клиента и задать все необходимые настройки для работы в выбранном режиме за несколько простых шагов.

Также DSA-2006 поддерживает настройку и управление с помощью мобильного приложения D-Link Click'n'Connect для устройств под управлением ОС Android, что может позволить быстро изменить настройки конфигурации даже неопытным пользователям.

Таблица 3.1 – Характеристика маршрутизатора D-link DSA-2006

|  |  |
| --- | --- |
| Процессор | Intel Atom C2358 (1,74 ГГц, двухъядерный) |
| Оперативная память | 2 ГБ, DDR3 |
| Flash-память | 4 ГБ, eMMC |
| Интерфейсы | * 6 портов 10/100/1000Base-T * 2 порта USB 2.0 * Консольный порт с разъемом mini-USB |
| Типы подключения WAN | * Мобильный интернет * PPPoE * IPv6 PPPoE |
| Функции | Поддержка VLAN, DHCP, VRRP, статическая маршрутизация, RIP v1/v2, NAT |
| Размеры | 278 x 183 x 44 мм |
| Вес | 1.7 кг |
| Питание | 100-240 В переменного тока, внутренний источник питания |
| Макс. мощность | 20 Вт |

### 3.1.2 Коммутатор D-Link DGS-1250-28XMP

Сетевой коммутатор – активное сетевое устройство, предназначенное для соединения нескольких узлов вычислительной сети между собой. Соединение происходит в пределах одного или нескольких сегментов сети.

Настраиваемый коммутатор DGS-1250-28XMP, оснащенный 24 портами 10/100/1000Base-T с поддержкой PoE и 4 портами 10GBase-X SFP+, поддерживает технологию D-Link Green и расширенные функции управления и безопасности, обеспечивая высокую производительность и масштабирование сети. Функции управления включают SNMP, управление на основе Web-интерфейса, утилиту D-Link Network Assistant и интерфейс командной строки (CLI).

24 порта данного коммутатора поддерживают стандарт IEEE 802.3at PoE. Каждый порт PoE подает питание мощностью до 30 Вт при общем бюджете коммутатора 370 Вт, что позволяет пользователям подключать к DGS-1250-28XMP устройства, совместимые со стандартом 802.3at. Это позволяет размещать оборудование в труднодоступных местах вне зависимости от расположения электрических розеток и минимизировать прокладку кабеля.

Коммутатор DGS-1250-28XMP поддерживает полный набор функций уровня 2, включая IGMP Snooping, Port Mirroring, Spanning Tree Protocol (STP) и Link Aggregation Control Protocol (LACP).

Функция управления потоком IEEE 802.3x позволяет оптимизировать нагрузку на коммутатор для повышения надежности передачи данных. Поддерживая скорость на каждом из медных портов до 2000 Мбит/с в режиме полного дуплекса, коммутатор обеспечивает высокую производительность, необходимую для подключения рабочих мест. Коммутатор поддерживает функцию диагностики кабеля и функцию Loopback Detection.

Функция Loopback Detection используется для определения петель и автоматического отключения порта, на котором обнаружена петля.

Функция диагностики кабеля предназначена для определения состояния витой пары, а также типа неисправности кабеля.

Коммутатор DGS-1250-28XMP поддерживает управление с помощью утилиты D-Link Network Assistant или через Web-интерфейс. Утилита обеспечивает автоматическое обнаружение и отображение на экране коммутаторов D-Link серии Smart, принадлежащих одному и тому же сегменту сети L2. Благодаря этой утилите пользователю не нужно менять IP-адрес своего компьютера, что упрощает начальную установку коммутатора. Пользователю доступна расширенная конфигурация и основные настройки обнаруженных устройств, например смена пароля и обновление программного обеспечения. Коммутатор DGS-1250-28XMP также поддерживает интерфейс командной строки (CLI) и SNMP.

Таблица 3.2 – Характеристика коммутатора DGS-1250-28XMP

|  |  |
| --- | --- |
| Процессор | 800 МГц |
| Оперативная память | 2 ГБ |
| Flash-память | 64 МБ |
| Интерфейсы | * 24 порта 10/100/1000Base-T с поддержкой PoE * 4 порта 10GBase-X SFP+ * Консольный порт с разъемом RJ-45 |
| Размер таблицы MAC-адресов | 16K записей |
| VLAN | 802.1Q |
| Бюджет мощности PoE | 370 Вт (макс. 30 Вт на порт PoE) |
| Размеры | 440 x 267 x 44 мм |
| Вес | 3,95 кг |
| Питание | 100-240 В переменного тока, 50/60 Гц |
| Макс. мощность | 28.86 Вт (функция PoE выключена)  463,76 Вт (функция PoE включена) |

### 3.1.3 Точка доступа D-Link DWL-8620AP

Точка доступа ‑ это беспроводная базовая станция, предназначенная для обеспечения беспроводного доступа к уже существующей сети или создания новой беспроводной сети. В качестве точки доступа была выбрана D-Link DWL-8620AP.

Унифицированная беспроводная точка доступа D-Link DWL-8620AP предназначена для организации масштабируемых беспроводных сетей на предприятиях малого и среднего бизнеса. DWL-8620AP поддерживает стандарт беспроводной связи 802.11ac Wave 2 и одновременную работу в двух диапазонах частот 2,4 ГГц и 5 ГГц, что позволяет применять точку доступа для решения широкого ряда сетевых задач, в том числе требовательных к пропускной способности.

Точка доступа DWL-8620AP может работать как в автономном режиме, так и под управлением унифицированных беспроводных контроллеров D-Link, что нам подходит. Благодаря удобному управлению и высокой скорости соединения устройство легко интегрируется в любую существующую сетевую инфраструктуру, которая в дальнейшем может быть масштабирована в соответствии с требованиями пользователя.

Беспроводная точка доступа DWL-8620AP поддерживает технологию MU-MIMO (Multi-User Multiple Input Multiple Output), благодаря которой устройство может одновременно передавать данные нескольким клиентам через разные антенны. Это позволяет более эффективно использовать радиоканал для передачи данных и значительно увеличивает общую пропускную способность сети. DWL-8620AP поддерживает технологию 4x4 MU-MIMO, обеспечивающую максимальную производительность беспроводной сети.

Таблица 3.3 – Характеристика точки доступа D-Link DWL-8620AP

|  |  |
| --- | --- |
| Интерфейсы | * IEEE 802.11b/g/n 2,4 ГГц * IEEE 802.11a/n/ac Wave 2 5 ГГц * 2 порта LAN 10/100/1000Base-T (порт LAN1 с поддержкой PoE 802.3at) * Консольный порт с разъемом RJ-45 |
| Антенна | Четыре внутренние всенаправленные антенны с коэффициентом усиления    – 3 dBi для диапазона 2,4 ГГц    – 4 dBi для диапазона 5 ГГц |
| Схема MIMO | MU-MIMO 4x4 |
| Сетевое управление | * Web-интерфейс (HTTP/HTTPS) * Telnet/SSH * Интерфейс командной строки (CLI) |
| Безопасность беспроводного соединения | Поддержка до 32 SSID, 16 SSID на радиодиапазон  Поддержка 802.1Q VLAN  Изоляция клиентов  Аутентификация: WPA, WPA2 Personal/Enterprise  Шифрование: AES, TKIP  Обнаружение несанкционированных точек доступа  Фильтрация по МАС-адресам |
| Размеры | Диаметр 220 мм, высота 47 мм |
| Вес | 0,79 кг (без кронштейна)  0,84 кг (с кронштейном) |
| Питание | * Адаптер питания:   Выход: 12 В постоянного тока 2,5 А   * Питание по кабелю Ethernet (PoE) 802.3at |
| Макс. мощность | 24,24 Вт |

### 3.1.4 Контроллер точек доступа D-Link DWC-1000 С1

Контроллер точек доступа - это устройство не является маршрутизатором или межсетевым экраном, или даже коммутатором - это устройство управляет точками доступа. Это может быть, как отдельное сетевое устройство в виде небольшой или большой коробочки, или может быть в виде облачного сервиса.

Беспроводной контроллер DWC-1000 осуществляет централизованное управление устройствами в беспроводной сети LAN. Устройство является полнофункциональным и экономичным решением для сетей малого и среднего бизнеса благодаря возможности управления от 6 до 24 беспроводными точками доступа для DWC-1000 аппаратной версии A1 и от 12 до 66 точками доступа для DWC-1000 аппаратной версии С1, а также благодаря возможности объединения до 4 контроллеров в общую группу (кластер). В нашей реализации будет использоваться аппаратная версия С1 контроллера.

Функции автоматического обнаружения точек доступа и централизованного управления позволяют приобрести систему корпоративного класса без затрат на выполнение масштабных и сложных конфигураций. Благодаря надежной и многофункциональной системе безопасности DWC-1000 обеспечивает защиту от потенциальных атак неавторизованных пользователей и устройств в беспроводной сети.

 Функции централизованного удаленного управления обеспечивают автоматическое обнаружение совместимых беспроводных точек доступа D-Link, их добавление в список управляемых точек доступа и быструю настройку с теми же параметрами, что и у предыдущих точек доступа. Благодаря возможности объединения контроллеров в кластер, администраторы могут выполнить настройку и управление всей группы с помощью одного контроллера. Ведение наблюдения за точками доступа и подключенными станциями в режиме реального времени обеспечивает эффективное использование сетевых ресурсов. Предупреждения об опасности и сбор статистики значительно упрощают управление и позволяют оптимизировать сетевую производительность.

Таблица 3.4 – Характеристика контролера точек доступа D-Link DWC-1000 С1

|  |  |
| --- | --- |
| Процессор | Cavium 7020 (800 МГц, двухъядерный) |
| Память | 1024 МБ, DDR II |
| Flash-память | 128 МБ, NOR-Flash |
| Интерфейс | * 4 порта 10/100/1000Base-T * 2 порта 10/100/1000Base-T Option1 * 2 порта USB 2.0 * Консольный порт RJ-45 |
| Максимальное количество точек доступа на устройство | По умолчанию: 12  После обновления: 66 |
| Количество пользователей, одновременно проходящих аутентификацию на адаптивном портале | 1024 |
| Размеры | 280 х 180 х 44 мм |
| Вес | 0,79 кг (без кронштейна)  0,84 кг (с кронштейном) |
| Питание | Внешний источник питания: 12 В переменного тока / 2,5 А |
| Макс. мощность | 12,6 Вт |

### 3.1.5 Рабочая станция HP Slim S01-aF0020ur 376B6EA

В качестве рабочей станции было принято решение выбрать HP Slim S01-aF0020ur 376B6EA. Причиной выбора стало то, что данная рабочая станция имеет относительно невысокую цену и хорошую комплектацию: современный процессор AMD Athlon Silver 3050U 2020 года выпуска, у который имеет 2 ядра и который может развивать тактовую частоту процессора 2300 МГц. Оперативной памяти объемом 8 ГБ и типом DDR4 вполне достаточно для запуска и корректной работы необходимого программного обеспечения.

Кроме того, в данном системном блоке уже присутствует твердотельный накопитель объемом 256 ГБ, который отличается лучшей скоростью записи и чтения данных, в отличие от жестких дисков.

А для работы в сети есть 1 интерфейс GBit и 1 Wi-Fi интерфейс.

На рабочей станции уже остановлена ОС Windows 10, которая является самой популярной операционной системой для ПК на данный момент [4].

Таблица 3.5 – Характеристика HP Slim S01-aF0020ur 376B6EA

|  |  |
| --- | --- |
| Процессор | AMD Athlon™ 3050U (2,3 ГГц с возможностью увеличения до 3,2 ГГц, 4 Мбайт кэш-памяти L3, 2 ядра) |
| Память | Память DDR4-2400 SDRAM, 8 Гбайт (1 x 8 Гбайт) |
| Внутреннее хранилище | Твердотельный накопитель PCIe® NVMe™ M.2, 256 Гбайт |
| Видеокарта | AMD Radeon™ |
| Порты | 4 разъема SuperSpeed USB Type-A со скоростью передачи данных 5 Гбит/с; 1 комбинированный разъем для наушников и микрофона |
| Сетевой интерфейс | Встроенный сетевой адаптер 10/100/1000 GbE |
| Беспроводная сеть | Комбинированный модуль Realtek 802.11a/b/g/n/ac (1x1) Wi-Fi и Bluetooth 4.2 |
| Размеры | 95 x 303 x 270 мм |
| Вес | 3,02 кг |
| Питание | Адаптер питания переменного тока Smart 65 Вт |
| Операционная система | Windows 10 |

### 3.1.6 Сервер Dell PowerEdge R250 Rack Server

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-потоком или другими данными. В качестве веб-сервера будет использоваться Dell PowerEdge R250.

Dell PowerEdge R250, оснащенный процессором Intel Xeon E-2300, представляет из себя мощный сервер для обычных бизнес-приложений с повышенным спросом на производительность. Он поддерживает скорость DDR4 3200 МТ/ с и модули DIMM емкостью 32 ГБ, можно доставить памяти до 128 ГБ для рабочих нагрузок с интенсивным использованием памяти.

Кроме того, для достижения существенного улучшения пропускной способности, PowerEdge R250 поддерживает PCIe Gen 4 и обеспечивает повышенную тепловую эффективность для удовлетворения растущих требований к мощности и теплу. Это делает PowerEdge R250 идеальным сервером в стойке для критически важных для бизнеса рабочих нагрузок, облачных инфраструктур и операций с торговыми точками в форм-факторе 1U для малого и среднего бизнеса внутри и за пределами центра обработки данных.

Таблица 3.6 – Характеристика Dell PowerEdge R250 Rack Server 1U

|  |  |
| --- | --- |
| Процессор | Intel® Pentium G6405T 3.5GHz, 4M Cache, 2C/4T, No Turbo (35W), 2666 MT/s |
| Память | 8GB UDIMM, 3200MT/s, ECC |
| Внутреннее хранилище | 1TB 7.2K RPM SATA Entry 3.5in Hard Drive Cabled |
| Сетевой интерфейс | On-Board Broadcom 5720 Dual Port 1Gb LOM |
| Размеры | 42.8 x 482 x 598.64 мм |
| Вес | 3,02 кг |
| Питание | 450 W Bronze 100-240 V AC, cabled |
| Операционная система | Ubuntu |

### 3.1.7 МФУ Xerox B215 с факсом

В качестве принтера, сканера либо ксерокса было принято решение использовать выбрать МФУ Xerox B215. Данное устройство, как и большинство уже выбранных устройств, входит в диапазон устройств невысокой ценовой категории, что соответствует условиям заказчика.

Данное МФУ так же можно использовать в качестве факса, что избавляет от покупки еще одного устройства. Настройка МФУ может быть произведена благодаря 3.5-дюймовому сенсорному экрану, расположенному в верхней части корпуса.

Таблица 3.7 – Характеристика МФУ Xerox B215 с факсом

|  |  |
| --- | --- |
| Поддерживаемые ОС | Windows, Mac, Linux |
| Функции | * Печать * Сканирование * Копирование * Факс |
| Дисплей | Сенсорный экран 3.5 дюйма |
| Сетевой интерфейс | Ethernet, WiFi |

### 3.1.8 Проектор Rombica Ray Box B1 (MPR-L770)

По заданию необходим проектор способный выводить изображение на экран. Для данных целей решено использовать проектор Rombica Ray Box B1 (MPR-L770).

Основные характеристики:

– Технология проецирования: LCD;

– Источник света: Светодиоды;

– Ресурс источника света: 30000 часов;

– Физическое разрешение: 1280х720;

– Соотношение сторон: 16:9;

– Подключение: HDMI.

## 3.2 Пассивное сетевое оборудование и кабеля

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.

### 3.2.1 Выбор телекоммуникационного шкафа

Помещение имеет большую площадь относительно количества работников, поэтому есть возможность организовать полноценную серверную комнату. Из соображений безопасности, а также требования к физической защите оборудования было решено разместить сетевое оборудование в телекоммуникационные шкафы.

Для размещения маршрутизатора, коммутаторов, контроллера точек доступа, веб-сервера был выбран телекоммуникационный шкаф TWT-CBWL-12U-6x4. Он имеет возможность крепиться на стене, имеет высоту 12 монтажных единиц и в комплекте поставки находится все необходимое оборудование.

### 3.2.2 Выбор кабеля

В задании не указано спецефических требований по защите от помех, в связи с чем будут использоваться неэкранированные UTP кабеля.

Всё оборудование будет работать со скоростью 1Гбит/с, в связи с чем был выбрана витая пара категории 5e. Для нее характерны стандарты 10/100/1000BASE-T и дальность до 100 м при использовании 1000BASE-T.

По итогу всех требований был выбран следующий кабель: UTP CAT5e, REXANT 4PR 24AWG.

### 3.2.3 Выбор коннектора, короба и розетки

В характеристиках кабеля указан лишь диаметр проводника – 24AWG, поэтому для расчёта размера короба возьмем максимальный диаметр кабеля как 6мм. В большинстве мест нам нужно проложить либо 1, либо 3, либо 4, либо 26, 27 кабелей, поэтому возьмем короба размерами 40x25 идущие от шкафа и 20x10 идущие непосредственно к розеткам.

Возьмем следующие короба:

– ECOLINE 40x25 мм;

– ECOLINE 20x10 мм.

Также возьмем коннекторы Geplink GL4701 RJ45 и розетки PST00 39047.

## 3.3 Обоснование выбора ПО

В нашей сети необходимо специальное ПО для трех задач: 1 – работы Web-сервера для доступа клиентов внутри локальной сети и извне; 2 – работы авторизации пользователей при подключении к нашим точкам доступа посредством сервера RADIUS; 3 – предостережение атак вирусов, защита от вирусов.

Для решения этих задач было принято сконфигурировать веб-сервер на сервере, а RADIUS-сервер на локальном ПК администратора, что будет стоять в серверной.

Для веб-сервера было решено использовать Nginx как HTTP-сервер. Его преимущества:

– Обслуживание статических запросов, индексных файлов, автоматическое создание списка файлов, кэш дескрипторов открытых файлов;

– Ускоренное обратное проксирование с кэшированием, распределение нагрузки и отказоустойчивость;

– Ускоренная поддержка FastCGI, uwsgi, SCGI и memcached серверов с кэшированием, распределение нагрузки и отказоустойчивость;

– Модульность, фильтры, в том числе сжатие (gzip), byte-ranges (докачка), chunked ответы, XSLT-фильтр, SSI-фильтр, преобразование изображений; несколько подзапросов на одной странице, обрабатываемые в SSI-фильтре через прокси или FastCGI/uwsgi/SCGI, выполняются параллельно;

– Поддержка SSL и расширения TLS SNI;

– Поддержка HTTP/2 с приоритизацией на основе весов и зависимостей.

Для RADIUS-сервера принято использовать пакет FreeRadius для ОС Linux на административном ПК. Это альтернатива других коммерческих RADIUS серверов, поскольку он модульный и функциональный на сегодняшний день. Кроме того, он входит в пятёрку RADIUS серверов мира с точки зрения развёртывания и количества пользователей, которых этот сервер авторизует ежедневно.

Может работать на встраиваемых системах с небольшим количеством памяти, обслуживая несколько миллионов пользователей. FreeRADIUS быстрый, гибкий, настраиваемый, а также поддерживает больше протоколов аутентификации, чем многие коммерческие серверы. Сервер поставляется вместе с инструментом управления через веб-интерфейс dialupadmin, который написан на PHP. В настоящее время FreeRADIUS используется как основа для разработки коммерческих RADIUS серверов

Для защиты от вирусов принято решение использовать Avast Antivirus. Avast имеет дополнительную систему безопасности (программа сначала запускает запрашиваемый файл в безопасной виртуальной среде – так называемой песочнице – внимательно анализируя его работу и только после успешного прохождения такого теста допускает его к системным ресурсам Windows).

Особенности Avast:

– Защита: AV-Test – 6 из 6, AV-Comparatives – 3 звезды и эффективность 99,7%;

– Потребление ОЗУ: 117,5 Мб;

­– Высокая популярность (400 миллионов пользователей) позволяет разработчикам быстро реагировать на угрозы;

– Есть независимая от браузера защита от опасных URL-адресов;

– Полная защита от опасных URL только в Chrome и Firefox;

– Множество дополнительных функций;

## 3.4 Адресация в локальной компьютерной сети

Внутренняя сеть будет разделена на 4 подсети. Назначение и адреса подсетей указаны в таблице 3.8.

Таблица 3.8 – Схема адресации подсетей

|  |  |  |  |
| --- | --- | --- | --- |
| Назначение | VLAN | Адрес подсети | Маска подсети |
| 1 | 2 | 3 | 4 |
| Административная | 33 | fd88:9:128:33::/64 | |
| 192.168.33.0 | 255.255.255.128 |
| Внутренние устройства | 100 | fd88:9:128:100::/64 | |
| Стационарные ПК | 192.168.100.0 | 255.255.255.192 |
| Внутренняя беспроводная | 20 | fd88:9:128:20::/64 | |
| 192.168.20.0 | 255.255.255.0 |
| Для Web сервера | 5 | fd88:9:128:5::/64 | |
| 192.168.5.0 | 255.255.255.0 |

Всем устройствам будут присвоены приватные IPv4 адреса и local unicast IPv6. Поскольку у нас по заданию нет требования использовать IPv6 за пределами внутренней сети, то мы можем использовать адреса из диапазона unique-local, а адресация будет проходить без проблем, т.к. устройства соединены между собой коммутаторами L2. Будем использовать головную часть адресов подсетей IPv6 равной fd88:9:128::/48.

Подробная адресация указана в таблицах 3.9 - 3.12.

Таблица 3.9 – Адресация административной подсети

|  |  |  |
| --- | --- | --- |
| Устройство | IPv4 Адрес | IPv6 Адрес |
| 1 | 2 | 3 |
| Маршрутизатор | 192.168.33.1 | fd88:9:128:33::1 |
| VLAN-шлюз | 192.168.33.126 | fd88:9:128:33::126 |
| Контроллер точек доступа | 192.168.33.30 | fd88:9:128:33::30 |
| ПК админа | 192.168.33.10 | fd88:9:128:33::10 |
| Веб-сервер | 192.168.33.40 | fd88:9:128:33::40 |

Таблица 3.10 – Адресация стационарных ПК и внутренних устройств

|  |  |  |
| --- | --- | --- |
| Устройство | Адрес IPv4 | Адрес IPv6 |
| 1 | 2 | 3 |
| ПК | 192.168.100.2-52 | fd88:9:128:100::2-52 |
| Принтеры | 192.168.100.55-56 | fd88:9:128:100::55-56 |
| VLAN-шлюз | 192.168.100.62 | fd88:9:128:100::62 |

Таблица 3.11 – Адресация беспроводной сети

|  |  |  |
| --- | --- | --- |
| Устройство | Адрес IPv4 | Адрес IPv6 |
| 1 | 2 | 3 |
| VLAN-шлюз | 192.168.20.254 | fd88:9:128:100::254 |
| Точки доступа | 192.168.20.2-3 | fd88:9:128:100::2-3 |
| Контроллер | 192.168.20.4 | fd88:9:128:100::4 |
| Остальные устройства | 192.168.20.5-35 | fd88:9:128:100::5-35 |

Таблица 3.12 – Адресация подсети Web сервера

|  |  |  |
| --- | --- | --- |
| Устройство | Адрес IPv4 | Адрес IPv6 |
| 1 | 2 | 3 |
| VLAN-шлюз | 192.168.5.254 | fd88:9:128:100::254 |
| Web сервер | 192.168.5.3 | fd88:9:128:100::3 |

## 3.5 Настройка сетевого оборудования

Приступим к настройке нашего активного сетевого оборудования.

### 3.5.1 Настройка маршрутизатора

Перед настройкой маршрутизатора, необходимо включить питание и подключиться к одному из портов Ge3-6. Далее необходимо убедиться, что Ethernet-адаптер Вашего компьютера настроен на автоматическое получение IP-адреса (в качестве DHCP-клиента). Как только вы получили по DHCP конфигурацию, можно переходить к web-интерфейсу.

Стандартные значения для этого роутера:

– Доменное имя устройства: dlinkrouter.local;

– IP-адрес устройства: 192.168.10.1;

– Имя пользователя: admin;

– Пароль: admin.

Запустите web-браузер. В адресной строке web-браузера введите доменное имя маршрутизатора (по умолчанию – dlinkrouter.local) с точкой в конце и нажмите клавишу Enter. Вы также можете ввести IP-адрес устройства (по умолчанию – 192.168.10.1).

Если устройство еще не было настроено или ранее были восстановлены настройки по умолчанию, при обращении к web-интерфейсу открывается страница изменения настроек по умолчанию.

Необходимо ввести пароль администратора в поля «Новый пароль» и «Подтверждение пароля» (см. рисунок 3.1). После авторизации будет предложено изменить настройки по умолчанию.

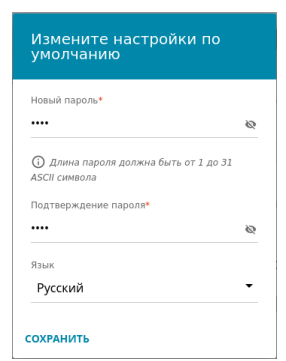


Рисунок 3.1 – Смена стандартных настроек

После того, как мы оказались авторизованы в web-интерфейсе, можно приступать к конфигурированию.

#### 3.5.1.1 Настройка WAN-соединения

По заданию, провайдер автоматически назначает нам внешний IPv4-адрес. В таком случае провайдер выдаст нам DNS, по которому наш маршрутизатор будет стучаться за IPv4-адресом. Иных требований по технологии соединения нет, поэтому будем использовать стандартное соединение Gigabit Ethernet.

Чтобы настроить WAN-соединение, нужно:

1 Перейдите на страницу «Настройка соединений / WAN».

2 Нажмите кнопку «ДОБАВИТЬ (+)».

3 На открывшейся странице на вкладке «Главные настройки» выбрать необходимое значение в раскрывающемся списке «Тип соединения».

4 Выбрать «Динамический IPv4»

5 Если провайдер предоставил адрес DNS-сервера, сдвинуть переключатель «Получить адрес DNS-сервера автоматически» влево и заполнить поле «Первичный DNS» (с.м. рисунок 3.2).

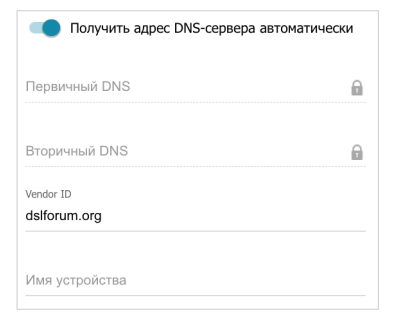


Рисунок 3.2 – Панель ввода DNS провайдера

#### 3.5.1.2 Настройка NAT

Для того, чтобы использовать один WAN ip-адрес для всех устройств локальной сети, которые могу выходить в интернет, необходимо зайти в раздел “Разное” и сдвинуть соответствующий переключатель вправо, рисунок 3.3:

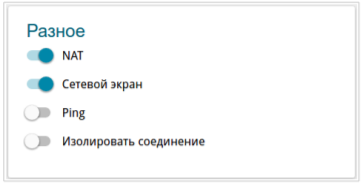


Рисунок 3.3 – Раздел Разное

#### 3.5.1.3 Настройка IPv6

Чтобы настроить адресацию IPv6 необходимо изначально на маршрутизаторе перейти во вкладку IPv6 раздела IP, выставить режим адресации “Статический” и присвоить маршрутизатору IP-адрес FD00::1 и префикс 64, рисунок 3.4:

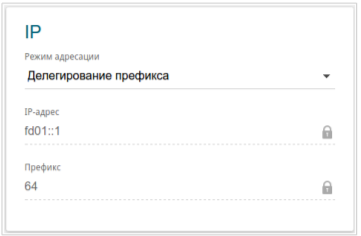


Рисунок 3.4 – Настройка IPv6 на маршрутизаторе

#### 3.5.1.4 Настройка межсетевого экрана

Воспользуемся межсетевым экраном [6] на маршрутизаторе, чтобы доступ в интернет имели веб-сервер. Для настройки межсетевого экрана подключаемся к web-интерфейсу машрутизатора [7] по ip-адресу 192.168.10.1.

Далее нужно перейти в раздел “Межсетевой экран” (см. рисунок 3.5):

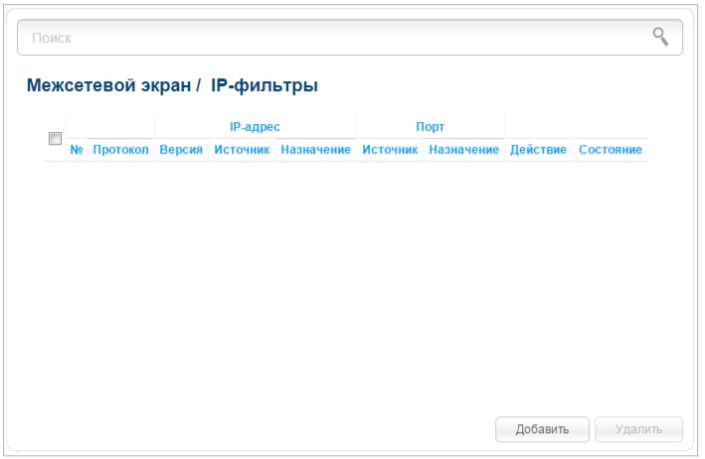
****

Рисунок 3.5 – Страница Межсетевой экран / IP-фильтры

Нам нужно ограничить доступ к административному VLAN извне.

После нажатия на кнопку «Добавить» попадаем на страницу, где вводим ip-адрес шлюза VLAN33 в поле «IP-адрес назначения», в поле «IP-адрес источника» выбираем «public», и в поле «Действие» выбираем «Запретить» и нажимаем кнопку «Применить». Также можно настроить по какому программному порту назначения или источника будет разрешен трафик, и еще можно выбрать по какому протоколу работать (см. рисунок 3.6):

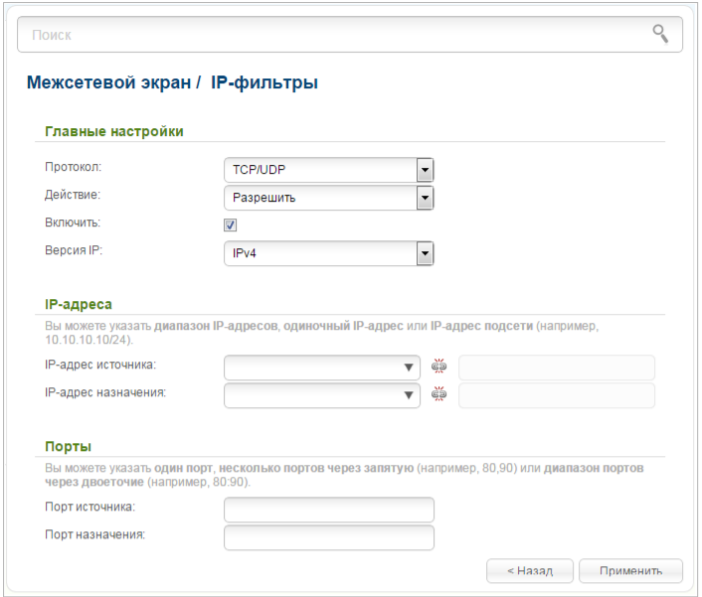


Рисунок 3.6 – Страница добавления правила для обработки сетевых пакетов

Таким образом мы должны настроить:

1 Разрешить адресам из VLAN 100 доступ к VLAN 5 для доступа к Web-серверу по http и https.

2 Разрешить адресам из VLAN 33 доступ к VLAN 5 для доступа к Web-серверу по http и https.

3 Разрешить адресам из VLAN 20 доступ к VLAN 5 для доступа к Web-серверу по http и https.

4 Запретить извне доступ к VLAN 33.

### 3.5.2 Настройка коммутаторов

Для корректной работы сети в первую очередь необходимо настроить VLAN. Для этого используем утилиту SmartConsole [5], отличается простотой использования.

При подключении коммутатора к любой рабочей станции, данная утилита сама находит коммутатор в сети. После чего мы можем добавить необходимые VLAN и сконфигурировать порты.

Переходим на вкладку 802.1Q VLAN, где мы видим кнопку “Add VID”:

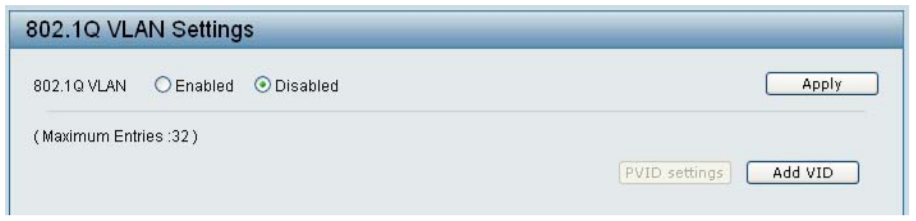


Рисунок 3.7 – Вкладка 802.1Q VLAN

После нажатия на кнопку открывается окно, где можно добавить VLAN. Тут отмечаем порт, через который будут проходить тегированные пакеты. Также соответствующих полях вводим VID и имя для создания каждого VLAN.

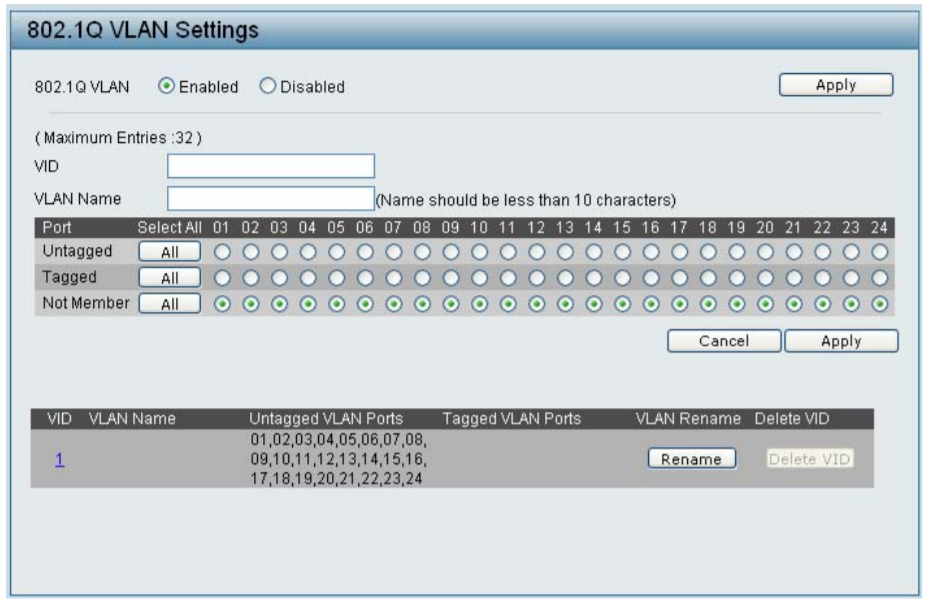
****

Рисунок 3.8 – Создание VLAN

Далее отмечаем порты, которые принадлежат определенному VLAN и нажимаем кнопку “Apply”. После чего у нас появится сконфигурированный VLAN, как на рисунке 3.9:

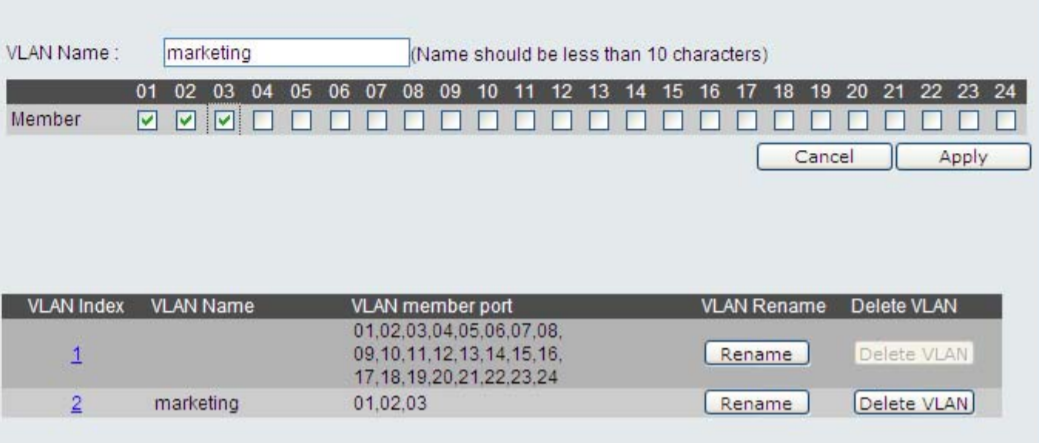


Рисунок 3.9 – Пример созданного и сконфигурированного VLAN

После этого необходимо настроить VLAN на маршрутизаторе для взаимодействия подсетей между собой. На странице “Дополнительно / VLAN” необходимо создать и отредактировать группы портов для виртуальных сетей (см. рисунок 3.10):

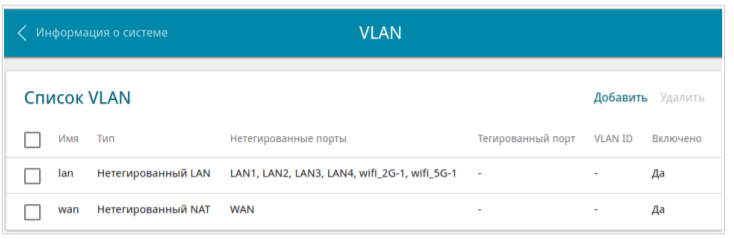


Рисунок 3.10 – Страница Дополнительно / VLAN

Необходимо нажать кнопку “Добавить” и на открывшейся странице нужно ввести VLAN ID, название и выбираем подключенные порты для каждого VLAN в нашей локальной сети (см. рисунок 3.11):

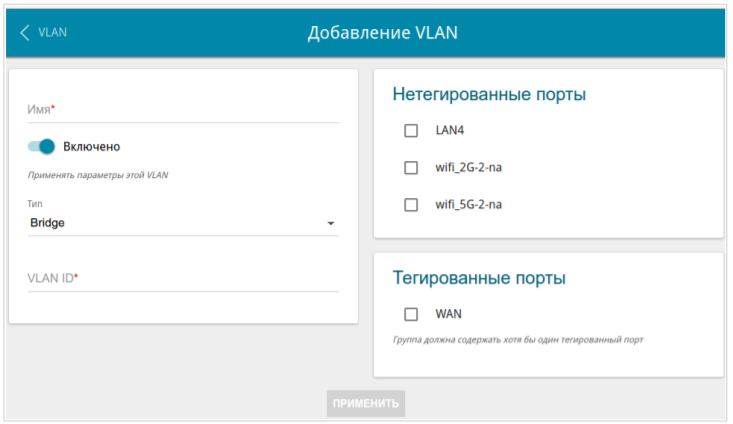


Рисунок 3.11 – Страница создания группы портов для VLAN

Также, необходимо настроить резервирование на коммутаторах.

Настроим на коммутаторе, смотрящим в маршрутизатор LACP, предварительно соединив его дополнительными связями с нижележащими коммутаторами. Необходимо войти в web-interface коммутатора.

Далее, необходимо перейти во вкладку « DGS-1210 > L2 Functions > Link Aggregation > Port Trunking». На этой вкладке необходимо выбрать какие порты объединять в транк и в какую группу их определить.

Можно выбрать ID группы агрегации, тип протокола LACP или Static, ну и выбрать собственно порты (см. рисунок 3.12). Данный процесс необходимо повторить и на нижележащих коммутаторах. В нашем случае:

– на root: ID 1 = G13, G14; ID 2 = G15, G16;

– на нижележащих: на одном ID 1, на другом – ID 2, порты – G0, G1.

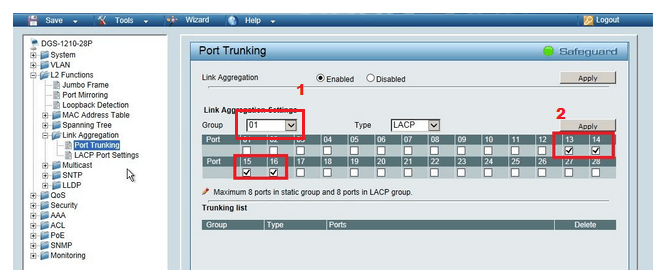


Рисунок 3.12 – Настройка LACP

### 3.5.3 Настройка контроллера и точек доступа

В первую очередь необходимо войти в web-interface WLC. Для этого подключимся к контроллеру, настроим на компьютере адрес из подсети 192.168.10.0/24.

В браузере перейти по http://192.168.10.1 и залогиниться (пароль и пользователь: admin, см. рисунок 3.12).

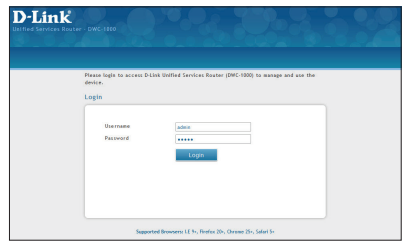


Рисунок 3.12 – Авторизация в WLC

Далее, заходим по «Wireless > Access Point > Discovered AP List». В этом меню покажутся найденные точки доступа.

Кликнув правой кнопкой мыши по найденным точкам доступа можно перейти к настройке отдельной точки (см. рисунок 3.13).

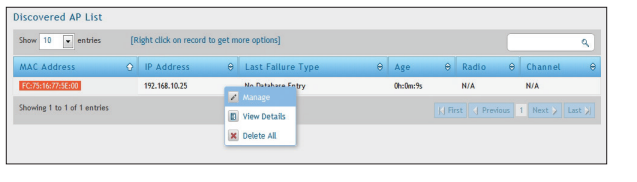


Рисунок 3.13 – Выбор точки доступа для настройки

Далее, выскочит меню настройки точки доступа (см. рисунок 3.14).

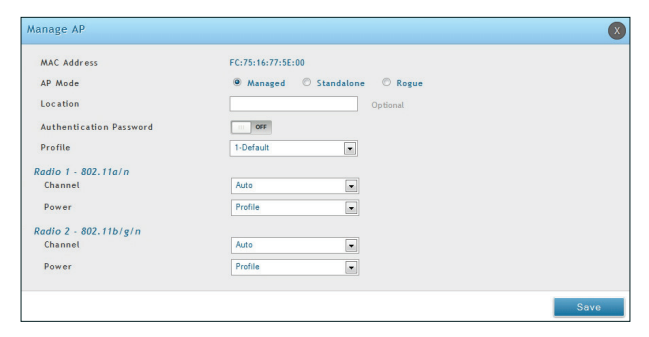


Рисунок 3.14 – Пример окна настройки

Нас интересуют следующие поля:

– AP Mode – режим точки доступа, тыкаем Managed.

– Аутентификация – Если режим точки доступа = управляемый, включите, чтобы потребовать пароль для аутентификации.

– Профиль – Если режим точки доступа = Управляемый, выберите профиль, который будет применен для настройки точки доступа.

– Радио – Если режим точки доступа = управляемый, отображается режим беспроводной радиосвязи, используемый точкой доступа. Поля – ниже появятся после того, как вы выберете режим управляемой точки доступа.

– Канал – если режим AP = управляемый, это рабочий канал для радио.

– Мощность – если режим AP = управляемый, это процент мощности, используемой для радио.

Далее необходимо настроить SSID на контроллере:

– Заходим в «Wireless > Access Point > AP Profile > AP Profile SSID». Тут появится список WLAN-ов настроенных на контроллере.

– Выберите свой стандартный SSID и щелкните правой кнопкой мыши. Вызовется меню как на рисунке 3.15.

Тут настраиваем для безопасности WPA2-Enterprise.

Чтобы использовать SSID с проверкой подлинности RADIUS, выполните следующую процедуру:

1 Перейдите на страницу Безопасность > Аутентификация> Внешний сервер аутентификации> RADIUS-сервер.

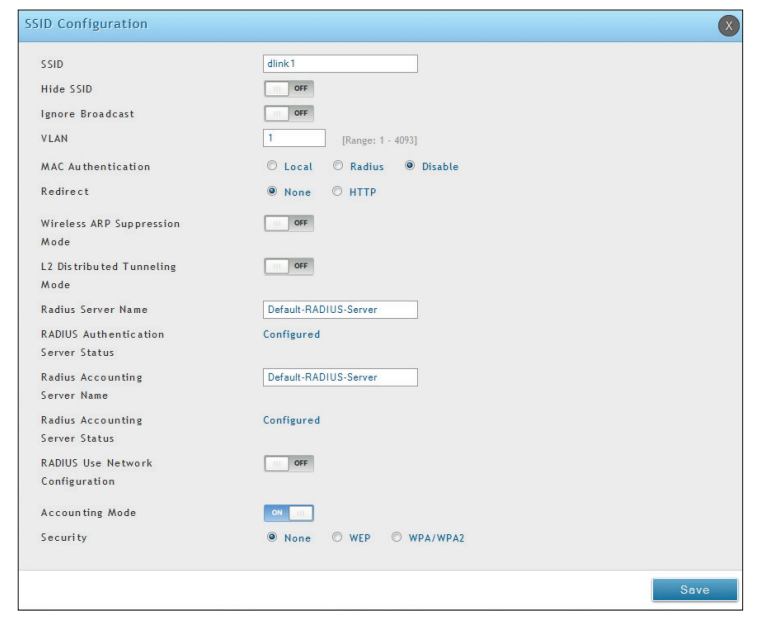


Рисунок 3.15 – Настройка SSID

Тут будут поля:

* Проверка сервера – Нажмите, чтобы проверить соединение между контроллером и вашим RADIUS-сервером.
* Сервер аутентификации IP-адрес – IP-адрес вашего сервера аутентификации RADIUS.
* Порт аутентификации ­– Номер порта аутентификации RADIUS для отправки сообщений RADIUS.
* Секрет – Введите секретный ключ, который позволяет устройству входить в настроенный сервер RADIUS. Он должен соответствовать секрету на сервере RADIUS.
* Тайм-аут – Установите тайм-аут в секундах. Контроллер должен дождаться от вета от RADIUS-сервера. Повторяет количество попыток, которые контроллер сделает с сервером RADIUS, прежде чем отказаться.

2 Заполните поля, приведенные ниже, и нажмите Сохранить. Ваша точка доступа будет настроена на использование

сервера аутентификации RADIUS.

3 Нажмите Проверка сервера, чтобы проверить соединение между DWC-1000 и вашим RADIUS-сервером. (см. рисунок 3.16)

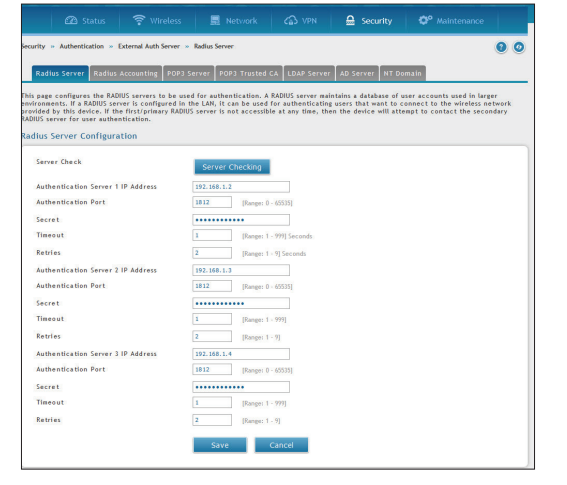


Рисунок 3.16 – настройка RADIUS

Далее переходим во вкладку Wireless -> Local Network -> DHCP Server и производим настройку DHCP пула. Для этого в поле DHCP выбираем Enable, далее в поле Start IP Address вписываем адрес начала пула (например, 192.168.20.5), а в поле End IP Address адрес конца пула (например, 192.168.20.35), указываем маску подсети и нажимаем Apply.

### 3.5.4 Настройка RADIUS-сервера

Установите пакет freeradius. В терминале введите команду:  
$ sudo apt install freeradius

Добавьте информацию о маршрутизаторе, который будет использовать RADIUS-сервер для аутентификации клиентов.

Откройте файл /etc/freeradius/3.0/clients.conf. В конце файла добавьте строки:

$ sudо gedit /etc/freeradius/3.0/clients.conf

client 192.168.20.4 {

secret = dlinkpassword

shortname = WLC

}

Создайте и заполните файл /etc/freeradius/3.0/dictionary.dlink:

$ sudо gedit /etc/freeradius/3.0/dictionary.dlink

VENDOR dlink 171

BEGIN-VENDOR dlink

ATTRIBUTE dlink-privelege-level 1 integer

END-VENDOR dlink

В конфигурационный файл /etc/freeradius/3.0/dictionary в конце файла добавьте строку:

$ sudо gedit /etc/freeradius/3.0/dictionary

$INCLUDE /etc/freeradius/3.0/dictionary.dlink

Настройте базу учётных записей пользователей. На коммутаторах с D-Link-like CLI существует четыре уровня прав доступа — Admin, Operator, Power User и User. Соответственно, в конфигурационном файле RADIUS-сервера необходимо создать пользователей для каждого уровня доступа — admin, operator, power\_user, user и enable. Пользователь enable необходим для получения прав администратора при выполнении команды enable admin. Откройте файл /etc/freeradius/3.0/users. В начале файла добавьте:

$ sudо gedit /etc/freeradius/3.0/users

admin Cleartext-Password := “admin\_password”

dlink-privelege-level = 5

enable Cleartext-Password := “enable\_password”

dlink-privelege-level = 5

operator Cleartext-Password := “operator\_password”

dlink-privelege-level = 4

power\_user Cleartext-Password := “power\_user\_password”

dlink-privelege-level = 6

user Cleartext-Password := “user\_password”

dlink-privelege-level = 3

Перезапустите RADIUS-сервер:

$ sudo systemctl restart freeradius.service

Чтобы протестировать аутентификацию пользователей локально на RADIUS-сервере, введите команду:

$ sudo radtest admin admin\_password 127.0.0.1:18120 0 testing123

### 3.5.5 Настройка МФУ с факсом

Настройка МФУ происходит с помощью подключения Ethernet-кабеля к сети.

Настройки TCP/IP:

1 На панели управления принтера выберите Устройство > Сеть >

2 Выберите «Включение TCP/IP».

3 Для IPv4 и IPv6 нажмите «Включить».

4 Нажмите на «X».

Чтобы вернуться в главное меню, нажмите кнопку «На главную».

Настройка сетевого адреса вручную:

1 На панели управления принтера выберите Устройство > Сеть > Настройки TCP/IP.

2 Выберите «Динамическая адресация DHCP».

3 Нажмите «Отключено», затем выберите «X».

4 Нажмите «Настройки TCP/IP».

5 Нажмите «IPv4», затем введите IPv4-адрес, затем нажмите «Подтвердить». Для параметра «Адрес шлюза» укажите адрес, затем нажмите «Подтвердить». Для параметра «Маска подсети» введите адрес и нажмите «Подтвердить».

6 Нажмите на «X».

7 Чтобы вернуться в главное меню, нажмите кнопку «На главную».

### **3.5.6 Настройка веб-сервер**а

Установите на сервер пакет Nginx:

$ sudo apt update

$ sudo apt install nginx

$ sudo service nginx start

$ sudo systemctl enable nginx

Проверьте, что Nginx запущен и установлен в старт-ап:

$ sudo systemctl is-enabled nginx

$ sudo service nginx status

Для настройки работы Nginx, необходимо закинуть файл со своим конфигом в папку /etc/nginx/conf.d.

Например:

upstream apache{

        server apache-app:80;

}

server {

        server\_name "" $server\_addr;

        listen 80; # managed by Certbot

        root /home/nginx-user/public\_html;

        index index.html;

        location /info.php {

                proxy\_pass http://apache/$uri;

                proxy\_set\_header X-Real-IP $remote\_addr;

                proxy\_set\_header X-Forwarded-for $remote\_addr;

                proxy\_set\_header Host $host;

                proxy\_connect\_timeout 60;

                proxy\_send\_timeout 90;

                proxy\_read\_timeout 90;

                proxy\_redirect off;

                proxy\_set\_header Connection close;

                proxy\_pass\_header Content-Type;

                proxy\_pass\_header Content-Disposition;

                proxy\_pass\_header Content-Length;

        }

        location /application {

                proxy\_pass  http://app;

                proxy\_set\_header X-Real-IP $remote\_addr;

                proxy\_set\_header X-Forwarded-for $remote\_addr;

                proxy\_set\_header Host $host;

        }

        location ~ "\.mp3" {

            try\_files $uri =404;

        }

        location /secondserver {

            rewrite ^ https://www.youtube.com/watch?v=dQw4w9WgXcQ;

        }

        location /roundrobin {

                proxy\_pass http://balance;

                proxy\_set\_header X-Real-IP $remote\_addr;

                proxy\_set\_header X-Forwarded-for $remote\_addr;

                proxy\_set\_header Host $host;

        }

        location ~ "^.\*/(?<angle>0|90|180|270|360)?/(?<file>\w+)\.(?<format>jpg|jpeg)$" {

                alias /home/nginx-user/public\_html/data/Images/$file.$format;

                add\_header Capture1 $angle;

                add\_header Capture2 $file;

                add\_header Capture3 $format;

                add\_header Capture4 $uri;

                image\_filter test;

                image\_filter rotate $angle;

                image\_filter\_buffer 8M;

        }

        location ~ "^/(?<file>\w+)?\.(png)$" {

                root /home/nginx-user/public\_html/data/Images/;

                add\_header Capture1 $file;

                add\_header Capture2 $uri;

                image\_filter test;

                image\_filter\_buffer 8M;

        }

        location /monitoring {

                root /home/nginx-user/public\_html/;

                index monitoring.html =404;

                add\_header Refresh 1;

        }

    }

upstream app {

        server localhost:8080;

}

server {

        listen 8080;

        server\_name "" $server\_addr;

        root /home/nginx-user/public\_html/;

        index app.html;

}

Этот конфиг-файл поднимает Nginx, который слушает порт 80 запросы по HTTP, после чего в зависимости от URL возвращает тот или иной контент.

### 3.5.7 Настройка ПК

Для настройки адресов IPv6 на пользовательских станциях необходимо открыть свойства подключения по локальной сети на панели управления Windows. Далее нужно открыть свойства IPv6 и на каждой пользовательской станции ввести соответствующий IPv6-адрес, маску 64 и адрес шлюза. Аналогичные манипуляции для настройки IPv4 в этом же окне. (см. рисунок 3.17).

В качестве средства предостережения вирусных атак принято установить на все ПК антивирусную систему Avast.

Для установки на ПК, нужно перейти на сайт https://www.avast.ru/installation-files#pc. Отсюда скачиваем подходящий для нашей системы установочный файл, в нашем случае для Windows 10. В ходе установки можно решить, какие дополнения вы хотели бы установить (см. рисунок 3.18).

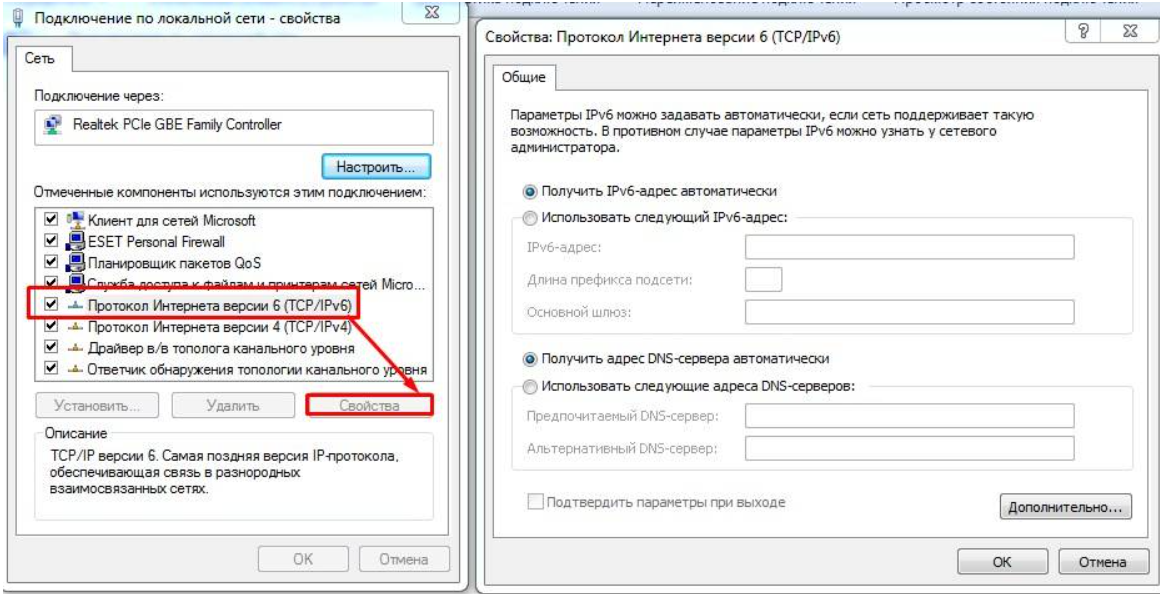


Рисунок 3.17 – Настройка IPv6 и IPv4 на пользовательских станциях



Рисунок 3.18 – Установка Avast

После установки необходимо настроить параметры сканирования и очистки журналов. Вкладка с «Обслуживанием» позволяет задать параметры автоматической очистки и лимит карантина. В принципе, рекомендуется увеличить размер карантина на несколько порядков, т.к не всё и не всегда может туда поместиться со значением по умолчанию (см. рисунок 3.19).

В мониторинге состояния рекомендуется поставить все галочки по той простой причине, что это увеличит общую безопасность и избавит Вас от лишних телодвижений по обновлению и защите антивируса (см. рисунок 3.20).

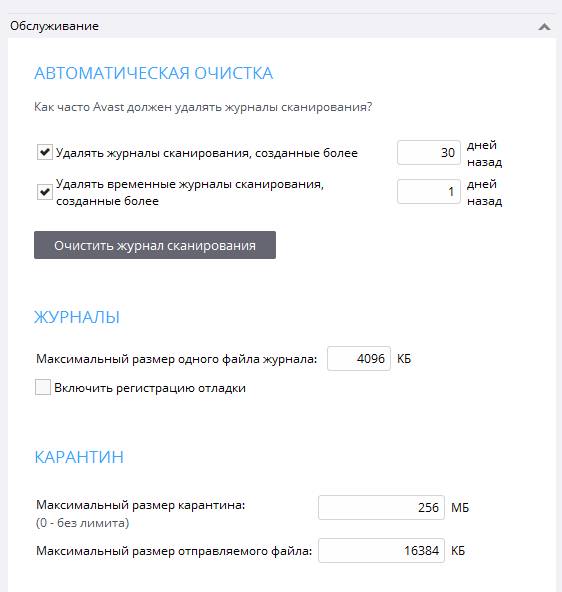


Рисунок 3.19 – Настройка параметров карантина и удаления журналов

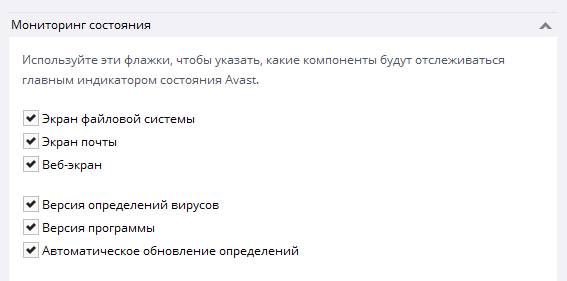


Рисунок 3.20 – Настройка мониторинга состояния

# 4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

В данном разделе находится описание практической части того, что было сказано выше в предыдущих разделах. В разделе структурированной компьютерной сети будет описано как будет происходить монтаж и размещение оборудования.

Во всех кабинетах будет использоваться неэкранированная витая пара (см. п. 3.2.2).

В здании имеется следующие комнаты:

– Кабинет 101 – проходная, пост охраны. Рассчитано, что здесь находится 1 рабочее место под ПК и 1 сетевой принтер;

– Кабинет 102 – опенспейс, основное место работы компании. Рассчитано, что тут будет работать 36 человек, столы располагаются над подпольной проводкой кабеля, также на потолке протянуты в коробе под фальш потолком кабеля к точкам доступа;

– Кабинет 103 – кухня, предполагается подключение мобильных пользователей, в случае долгого перерыва или просто от желания поработать на кухне с хорошими скоростям;

– Кабинет 104а и 104б – переговорные, располагается по 6 рабочих мест, кабельная система проведена к ним в коробе под фальш полом;

– Кабинет 105 – принтерная, располагаются сетевые принтеры, 3 подключения;

– Кабинет 106 – серверная, тут располагается телекоммуникационный шкаф со всем оборудованием.

В плане здания можно увидеть как прокладывается кабель и местоположение сетевого оборудования. План СКС можно детально изучить на чертеже плане этажа в приложении В.

# ЗАКЛЮЧЕНИЕ

В ходе выполнения данной курсовой работы была разработана и спроектирована локальная компьютерная сеть для небольшой организации, занимающейся торговлей запчастями автомобилей. Были получены теоретические и практические навыки по проектированию локальных компьютерных сетей.

Было изучено большое количество документации и советов с форумов официального производителя изучаемых устройств, а также были изучены рекомендации на сайте производителя сетевого оборудования.

В итоге, была спроектирована компьютерная сеть. Выполнены функциональная и структурная схемы, а также был реализован на бумаге план нашего единственного этажа. Про проектирование подбор оборудования полагался полностью на разработчика. Все эти доводы и причины выбора текущих устройств был обоснован и указан в пояснительной записке.

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

В результате проектирования топологии было изучены подходы к проектированию, найден оптимальный подход, что помогло построить локальную сеть грамотнее.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Таненбаум, Э. Компьютерные сети/ Э. Таненбаум, Д. Уэзеролл. – 5-е издание – Санкт-Петербург [и другие]: Питер, Питер Пресс, 2017. – 955с
2. Росс Дж. WI-FI. БЕСПРОВОДНАЯ СЕТЬ / Дж. Росс – М.: НТ Пресс, 2007. — 320 с. — ISBN 978-5-477-00665-6
3. Рожнова Н.Г. Вычислительные машины, системы и сети. Дипломное проектирование / Н.Г. Рожнова, Н.А. Искра, И.И. Глецевич – Минск БГУИР 2014
4. Популярные ОС [Электронный ресурс]: – Режим доступа: https://ddr5.com.ua/rejting-operaczionnyh-sistem-2020-2021/ – Дата доступа: 05.11.2021
5. Утилита SmartConsole [Электронный ресурс]: – Режим доступа: https://ftp.dlink.ru/pub/Switch/DES-1100-24/Description/ – Дата доступа: 01.12.2021
6. Межсетевой экран [Электронный ресурс]: – Режим доступа: https://ru.wikipedia.org/wiki/Межсетевой\_экран/ – Дата доступа: 24.11.2021
7. Руководство по настройке роутера [Электронный ресурс]: – Режим доступа: https://ftp.dlink.ru/Router/DIR-825\_AC\_E1A/Descriptopn – Дата доступа: 12.12.2021
8. Настройка МФУ в сети [Электронный ресурс]: – Режим доступа: http://www1.hp.com/ctg/Manual/c04403458/ – Дата доступа: 05.12.2021
9. Веб-сервер и реверс-прокси Nginx [Электронный ресурс]: – Режим доступа: https://nginx.org/ru/ – Дата доступа: 05.12.2021

# **ПРИЛОЖЕНИЕ А**

(обязательное)

Схема СКС структурная

# **ПРИЛОЖЕНИЕ Б**

(обязательное)

Схема СКС функциональная

# ПРИЛОЖЕНИЕ В

(обязательное)

План этажа

# ПРИЛОЖЕНИЕ Г

(обязательное)

Перечень оборудования, изделий и материалов

# ПРИЛОЖЕНИЕ Д

(обязательное)

Ведомость документов