Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовой работе
«Локальная компьютерная сеть, вариант 20»
по дисциплине
«Аппаратное обеспечение компьютерных сетей»

Выполнил:
студент группы 650503
Юревич А. С.

Руководитель:
Глецевич И. И.

Минск 2019

Вариант	20
Сфера деятельности	Центр обработки данных компании, занимающейся программированием.
Помещение и пользователи	В пристройке к многоэтажному зданию, в которую ведет коридор. 2 комнаты (10 и 30 м^2) вдоль коридора, подсобное помещение (7 м^2).
Оборудование	Оснащение рабочих мест для 3 работающих поочередно администраторов, основной и резервный серверы для одновременного обслуживания до 100 пользователей (тонкие клиенты), принтер.
Подключение к Ethernet	Metro Ethernet.
Адресация	IPv4 (выдана подсеть 172.17.0.0), IPv6 (для некоторых приложений программистов).
Безопасность	Подключение к беспроводной сети только администраторов. Удаленное администрирование.
Финансы	Полноценная коммерческая сеть.
Дополнительные требования заказчика	Обеспечить повышенную пожарную безопасность.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ……..…...…….4
1 ОБЗОР ЛИТЕРАТУРЫ…….……..…….…....5
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ…….…...…….8
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ…….....…...9
3.1 Обоснование выбора активного сетевого оборудования……...…….9
3.1.1 Беспроводная точка доступа Cisco Aironet 1602I…….....10
3.1.2 Коммутатор Cisco SG350XG-24T-K9...…….…..10
3.2 Обоснование выбора серверного оборудования……..……10
3.2.1 Обоснование выбора терминального сервера…….……10
3.2.2 Обоснование выбора RADIUS-сервера и серверного ПО…...…...11
3.3 Организация рабочих мест…….12
3.3.1 Обоснование выбора рабочей станции администратора…….…...12
3.3.2 Обоснование выбора принтера…….……12
3.4 Разделение сети на виртуальные подсети…….13
3.5 Адресация в локальной компьютерной сети……14
3.6 Описание настройки компонентов локальной сети…….…15
3.6.1 Настройка коммутатора……...……..…...15
3.5.2 Настройка удалённого администрирования…….……...16
3.5.3 Настройка серверного ПО…….……..……...17
3.5.4 Настройка беспроводной точки доступа…….……20
3.5.5 Настройка принтера…….……..22
3.5.6 Настройка персональных компьютеров…….…….23
3.7 Переключение основного терминального сервера на резервный……..24
4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ……...……..……25
4.1 Общая организация СКС……..……..25
4.1.1 Обоснование выбора среды передачи данных……25
4.1.2 Обоснование выбора информационных розеток…….…...26
4.1.3 Обоснование выбора кабельного короба……..……...26
4.1.4 Обоснование выбора серверных стоек…….…26
4.1.5 Размещение беспроводной точки доступа……..…….26
ЗАКЛЮЧЕНИЕ.……...…..……..…28
СПИСОК ЛИТЕРАТУРЫ……...…...29
ПРИЛОЖЕНИЕ А…….…….32
ПРИЛОЖЕНИЕ Б……..…….33
ПРИЛОЖЕНИЕ В…….……..34
ПРИЛОЖЕНИЕ Г……..……35

ВВЕДЕНИЕ

Локальная компьютерная сеть (далее – ЛКС) – сеть из нескольких устройств, объединённых между собой при помощи активного и пассивного сетевого оборудования. Локальные сети могут проектироваться в пределах одного помещения, этажа или целого здания. Основная цель объединения рабочих станций и периферийных устройств в общую сеть – одновременное использование различных сетевых ресурсов, удалённый доступ и другое.

Настройкой активного оборудования, общего доступа и ПО, а также контролем физической целостности ЛКС занимается системный администратор. В обязанности администратора также могут входить устранение неполадок и неисправностей в сети, обеспечение информационной безопасности, подготовка и сохранений резервных копий данных, работа на первой линии поддержки (помощь пользователям в решении их проблем с рабочими станциями, так называемый «эникейщик» от англ. *any key*).

Задача данной курсовой работы – спроектировать локальную компьютерную сеть для центра обработки данных компании, занимающейся программированием. Основная цель создания локальной сети – повышение производительности труда, упрощение взаимодействия сотрудников, обеспечение доступа к общим ресурсам для всех станции, подключенных к ЛКС.

Проектирование ЛКС в рамках данной курсовой работы будет сопряжено со следующими подзадачами:

- изучить физические среды передачи данных;
- ознакомиться с принципами проектирования и построения ЛКС в промышленных масштабах;
- проанализировать способы построение физической структуры ЛКС;
- ознакомиться с правилами адресации в сети;
- изучить строение сети Metro Ethernet, её архитектуру и применение;
- изучить способы удалённого администрирования, авторизации пользователей;
- изучить рекомендации по повышению пожарной безопасности ЛКС.

1 ОБЗОР ЛИТЕРАТУРЫ

Основными источниками получения крупного багажа теоретических знаний стали источники [1,2]. Обе книги являются своего рода культовыми пособиями, в которых рассматриваются основы и технологии построения ЛКС, освещаются вопросы основных понятий, моделей и способов построения сетей, организация стека протоколов TCP/IP, создания серверов и служб для IP сетей (например, DHCP, AAA и другие). Оба источника освещают вопросы маршрутизации и коммутации, однако источники [3] и [4] освещают эти вопросы намного шире, так как являются узкоспециализированной литературой по подготовке к сертификационным экзаменам CCNA.

DHCP (сокращение от английского Dynamic Host Configuration Protocol – протокол динамической настройки узла) – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы оконечного устройства в сети TCP/IP.

Помимо книг одним из основных источник стал русскоязычный коллективный блог Хабр (в прошлом Хабрахабр), на котором статьи пишут сами пользователи, основываясь на личном опыте. При написании данного проекта много полезной информации было почерпано из источников [5-11]. В этих источниках описана настройка SSH на устройствах Cisco, настройка беспроводных точек доступа (в частности приведено подробное объяснение работы WPA2 и процесс конфигурации точки доступа с использованием графического интерфейса пользователя), а также описание локальных сетей с тонкими клиентами и терминальным сервером, обслуживающим сеть пользователей.

SSH – это сетевой протокол, позволяющий производить удалённое управление операционной системой. В данном курсовом проекте SSH используется для удалённого администрирования коммутатора.

WPA2 – набор алгоритмов и протоколов, обеспечивающих защиту данных в беспроводных сетях Wi-Fi. WPA2 существенно повышает защищённость беспроводных сетей Wi-Fi по сравнению с прежними технологиями и включает в себя алгоритмы шифрования AES и аутентификации 802.1X. В данном курсовом проекте WPA2 используется для авторизации администраторов в беспроводной сети.

Наиболее подробная теоретическая информация, касающаяся AAA, приведена в источнике [7].

AAA (сокращение от английского Authentication, Authorization and Accounting) – как следует из расшифровки аббревиатуры, система аутентификации, авторизации и учёта событий, встроенная в Cisco IOS. Эта система предоставляет пользователям безопасный удалённый доступ к сетевому оборудованию, например к беспроводным маршрутизаторам. Система занимается сбором и отправкой информации на сервер, аутентификацией пользователей и их авторизацией.

Аутентификация – процесс идентификации пользователя по паре «логин - пароль». Аутентификация определяет, каким образом клиент будет представляться беспроводной точке доступа. Для использования в курсовой работе был выбран протокол EAP, определяющий подлинность подключаемого устройства внешним сервером.

Авторизация – предоставление возможностей пользователю для удалённого доступа.

Аккаунтинг – служба, занимающаяся сборов и отправкой информации на сервер. Используется для составления отчётности, для биллинга (обработка платежей, работа с тарификацией и выставлением счетов пользователям) и для аудита. Может включать в себя различные данные, например время начала и окончания сессии, количество отправленных или полученных пакетов или байт и другое.

Помимо источников [8, 9] создание терминальных сетей подробно описывается в источниках [12, 13]. Информация из источника [12] основывается на реальном практическом опыте одного системного администратора в своей компании по выбору терминального сервера и, во много, основываясь на этот источник был выбран терминальный сервер для данного курсового проекта.

Одним из пожеланий заказчика было обеспечить повышенную пожарную безопасность, для чего было необходимо изучить соответствующие источники. Для выбора кабеля подходящих характеристик были изучены источники [14-17] и [22, 23], в которых описываются технические характеристики витой пары, государственный стандарт на кабельные изделия по требованиям пожарной безопасности, а также правила противопожарной безопасности при проектировании структурированной кабельной системы.

В курсовом проекте используется группа технологий 10Gbase-T, способная дать пропускную способность сети до 10 Гб/с. Для достижения данной скорости в ЛКС необходимо использовать определённый вид обжима витой пары. Информация об обжиме прямой витой пары для 10 Gigabit Ethernet была получена в источнике [18].

В англоязычном источнике [19] описываются технические характеристики сервера IBM x3650 M4, использующемся в курсовом проекте в качестве сервера для обслуживания тонких клиентов. Помимо технических характеристик сервера в данном источнике есть информация о его физических габаритах, что позволяет выбрать серверную стойку под этот сервер.

В источнике [20] описываются характеристики серверной стойки, предназначенной для хранения сервера IBM x3650 M4.

В источнике [21] описывается информационная розетка, которая используется в финальном монтаже локальной сети для подключения оконечных устройств к локальной сети.

В источнике [23] находится краткая информация об огнестойком канальном коробе, применяющемся в курсовом проекте.

Технические характеристики принтера, подключаемого к локальной сети для нужд администраторов, описаны в источнике [24]. Инструкция по подключению принтера к локальной сети находится в источнике [30].

Характеристики используемого коммутатора Cisco SG350XG-24T-K9 описываются в источнике [25].

В источнике [26] описывается беспроводная точка доступа Cisco Aironet 1602I. На этой же странице находится инструкция по первоначальной настройке точки доступа Wi-Fi.

В источниках [27] и [28] описаны технические характеристики двух системных блоков: Jet Office 3i7, используемой в реализуемой ЛКС в качестве RADIUS-сервера, и Irwin Computers Coffee Lake G1-07, который является персональным компьютером для пользования администраторами с целью решения рабочих задач.

В источниках [24 – 28], помимо технических характеристик закупаемого оборудования, приведены цены на оборудование и контактные номера телефонов компаний, реализующих данную продукция для физических и юридических лиц.

В источнике [29] описывается процесс подключения принтера Ricoh к локальной компьютерной сети.

В источниках [30-31] подробно описана структура Metro Ethernet – её особенности и отличительные черты, основные понятия, модели предоставления Ethernet-услуг, практики применения и перспективы для расширения локальной компьютерной сети.

Сегодня классическим подходом к построению Metro Ethernet является функциональная декомпозиция на уровни доступа: опорная сеть (ядро), уровень агрегации и уровень доступа (клиентский уровень). Для обеспечения повышенной надёжности и резервирования широко применяется топологическая модель кольца. Кольца обычно создаются на уровне ядра и на клиентском уровне.

Базовой для построения развитых Ethernet-сетей является технология виртуальных локальных сетей – Virtual Private LAN (VLAN). Данная технология позволяет создавать в едином Ethernet-сегменте независимые логические области, ограничивающие на канальном уровне пределы распространения трафика. В заголовок Ethernet-кадра вводится дополнительная принадлежность к конкретному VLAN. Так получается помеченный кадр, который передаётся по транковым каналам и на выходе из коммутатора (например, на стороне клиентского порта) метка убирается[31].

В источнике [34] приведена справочная информация о переключении сервера на резервный и репликации данных.

Репликация данных – механизм синхронизации содержимого нескольких серверов.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе пояснительной записки описывается структура организации локальной компьютерной сети для центра обработки данных и проводится обоснование её выбора. Со структурной схемой локальной компьютерной сети можно ознакомиться в приложении «А».

Предприятие, занимающееся программированием, представляет из себя различные структурные единицы: отдел программирования, отдел управления персоналом, отдел управления компанией центр обработки данных. В рамках данного курсового проекта описывается проектирование локальной компьютерной сети для центра обработки данных.

Согласно заданию, центр обработки данных занимает два помещения площадью 10 и 30 $м^2$ (серверное помещение, в котором расположено серверное оборудование, и комната администраторов, где организованы их рабочие места). Основная задача центра обработки данных – обслуживание до ста тонких клиентов, что говорит о больших размерах предприятия и больших объёмах трафика, который будет передаваться из ЦОД в остальные отделы компании и обратно.

По данному условию, в локальной сети центра обработки данных входят три административные станции, за которыми поочерёдно работаю три администратора, принтер, основной и резервный сервер для обслуживания тонких клиентов. Для обеспечения доступа к сети с портативных устройств администраторов (смартфоны, ноутбуки) необходимо установить беспроводную точку доступа. Для ограничения доступа к беспроводной сети необходимо установить и организовать работу AAA-сервера.

Локальная сеть состоит из коммутатора третьего уровня, к которому подключены пользовательские станции, принтер, беспроводная точка доступа и серверное оборудование. В связи с большим потоком данных, передаваемым через локальную сеть, необходимо обеспечить пропускную способность на пути от основного и резервного терминального сервера до оконечных пользователей не менее 10 Гб/с.

Учитывая особенности строения Metro Ethernet, коммутатор, являющийся связующим элементом проектируемой локальной компьютерной сети и остальными сегментами сети компании, занимающейся программированием, подключается к остальным коммутаторам в кольцевую топологию. Внутри проектируемой локальной компьютерной сети используется топологическая модель «звезда» - оконечные устройства подключаются к коммутатору, который в свою очередь подключается к сети Metro Ethernet.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

На этапе функционального проектирования в данном разделе описывается функционирование программной и аппаратной составляющей проектируемой ЛКС. Детально изучить топологию и структуру разрабатываемой локальной компьютерной сети можно в приложении «Б».

3.1 Обоснование выбора сетевого оборудования

В сетях происходит пакетная передача данных и важно правильно обработать каждый пакет, узнать источник и пункт назначения пакета, узнать данные, которые он хранит в себе, а также обеспечить целостность пакета и передаваемой им информации и доставить пакет в место назначения. Эту задачу берёт на себя активное сетевое оборудование. Выбор сетевого оборудования очень важен, так как от него зависит правильность функционирования всей локальной сети, поэтому к нему стоит подойти ответственно.

На данный момент компания Cisco предоставляет самый широкий выбор коммутаторов, маршрутизаторов и другого сетевого оборудования. По данным за 2016 год Cisco контролирует 56% рынка активного сетевого оборудования, что говорит о высоком уровне и качестве. Однако за хорошую технику нужно платить: оборудование компании стоит заметно дороже по сравнению с другими устройствами, но эта переплата стоит того, когда дело касается серьёзных коммерческих сетей, где важна скорость работы и отказоустойчивость. С учётом вышеизложенного и пожеланий заказчика в ходе проектирования ЛКС было принято использовать именно оборудование компании Cisco.

Одним из пожеланий заказчика было подключение сервера для обслуживания до 100 тонких клиентов, следовательно в проекте необходимо было предусмотреть высокую пропускную способность пассивного и активного оборудования.

При одновременном подключении ста тонких клиентов к серверу минимальная скорость соединения, которую нужно обеспечить для потоковой передачи, около 15 Мбит/с на одного пользователя [33].

Для обеспечения одновременного обслуживания сотни тонких клиентов потребуется пропускная способность каналов минимум в 1500 Мбит/с. С учётом возможного масштабирования предприятия необходимо обеспечить пропускную способность на пути от терминального сервера до тонкого клиента в 10 Гбит/с, для этого в пределах проектируемой локальной компьютерной сети необходимо выбрать коммутатор с интерфейсами 10 Gigabit Ethernet. Для администраторов, использующих подключение к беспроводной сети, такая скорость является избыточной для повседневного использования, поэтому было принято решение выбрать беспроводную точку доступа с меньшей пропускной способностью.

Исходя из вышесказанного было принято использовать следующее активное сетевое оборудование:

1. Беспроводная точка доступа Cisco Aironet 1602I.
2. Коммутатор Cisco SG350XG-24T-K9.

3.1.1 Беспроводная точка доступа Cisco Aironet 1602I

Беспроводная точка доступа используется для подключения к сети беспроводных устройств по технологии Wi-Fi. Данная точка доступа является одной из самых бюджетных из тех, что предлагает компания Cisco для малого и среднего бизнеса. Она поддерживает используемый в сети протокол аутентификации WPA2, а также настраивается при помощи графического интерфейса пользователя. Основным стандартом для Wi-Fi был выбран стандарт IEEE 802.11n, гарантирующий пропускную способность около 500 Мбит/с, чего хватает для обеспечения доступа администраторов в сеть.

3.1.2 Коммутатор Cisco SG350XG-24T-K9

В Metro Ethernet сетях коммутатор является основным связующим элементом, поэтому выбор коммутатора очень важен при проектировании данной ЛКС входящей в MAN сеть.

Коммутатор Cisco SG350XG-24T-K9 является управляемым коммутатором третьего уровня OSI, предназначенным для организации локальной компьютерной сети средних размеров. Относительная дешевизна, наличие 24 портов 10 Gigabit Ethernet, возможность управления и мониторинга коммутатора через веб-интерфейс, поддержка удалённого администрирования и маршрутизации делают выбор этого коммутатора очевидным и разумным.

3.2 Обоснование выбора серверного оборудования

3.2.1 Обоснование выбора терминального сервера

В настоящее время активно развиваются компьютерные сети, основанные на «тонких» клиентах и терминальном доступе. Это связано с минимальными необходимыми вложениями для создания инфраструктуры.

Работа терминальной сети значительным образом отличается от работы классической компьютерной сети. Терминальный режим подразумевает наличие «тонких» клиентов – это максимально упрощённая версия настольного персонального компьютера. Он значительно меньше по размерам, в нём отсутствуют жёсткий диск, вентиляция, оптический привод. Используются так называемые «холодные» процессоры, которые не требуют активного охлаждения и сильно не нагреваются в процессе работы.

Пользователю на экран приходит лишь изображение экрана, которое обрабатывается на сервере. От пользователя на сервер поступают команды

устройств ввода (клавиатура, мышь), терминальный сервер занимается обработкой полученных данных и, в соответствии с ними, изменением изображения на экране пользователя. На самом сервере хранятся приложения, файловые сервисы, базы данных и другие необходимые пользователям сервисы.

В качестве терминального сервера выбор пал на сервер IBM x3650 M4. В источнике [12] приводится опыт системного администратора, реализующий свою сеть с терминальным сервером и тонкими клиентами. Однако в стандартной конфигурации данный сервер имеет один порт Gigabit Ethernet, пропускной способности которого не хватает для полноценной работы сети. Для обеспечения пропускной способности в 10 Гб/с необходимо докупить и установить в сервер адаптер Intel X540 Dual Port 10Gbase-T. Данный сетевой адаптер содержит два порта 10 Gigabit Ethernet: один основной для непосредственной передачи данных, второй административный для контроля состояния сервера и репликации данных. Также для повышения надёжности данных и увеличения производительности было принято решение организовать RAID-массив из имеющихся в сервере жёстких дисков. Для создания RAID 10 необходимо докупить и установить RAID-контроллер ServeRAID M5110.

По условию задания необходимо приобрести два таких сервера с дополнительными адаптерами и контроллерами: один основной и один резервный. Целесообразно разместить их на разных серверных стойках во избежание порчи одновременно двух серверов.

Наличие резервного сервера – одна из важнейших составных частей обеспечения доступности к сервисам сервера терминалов. Для переключения на резервный сервер в случае отказа основного обычно используются инструменты High Availability (например, Linux-HA и DRBD на UNIX-системах и vGate на ОС Windows). Алгоритм действий, связанных с переключением основного сервера на резервный и наоборот, описаны в разделе 3.7.

3.2.2 Обоснование выбора RADIUS-сервера и серверного ПО

Очевидно, что немаловажную роль в защищённом доступе играет шифрование данных. В настоящее время широко известны технологии WEP, WPA и WPA2. WEP-шифрование использовать категорически не рекомендуется в связи с тем, что оно было скомпрометировано. Разница между WPA и WPA2 лишь в алгоритме шифрования (TKIP или AES). Так как AES является более совершенным алгоритмом шифрования, чем TKIP, было решено выбрать его.

WPA2 Personal и WPA2 Enterprise различаются тем, откуда берутся ключи шифрования. В первом случае используется статический ключ, который задаётся в настройках точки доступа. Такой ключ является общедоступным для всех пользователей точки и может быть легко скомпрометирован, что повлечёт

за собой смену паролей у всех пользователей. Динамический ключ используется для корпоративного применения во избежание таких ситуаций. Ключ может обновляться по ходу работы, при этом не разрывая текущее соединение. За генерацию ключа отвечает дополнительный компонент системы – сервер авторизации. Это может быть RADIUS-сервер, TACACS, TACACS+ и другие.

Использование шифрования WPA2 Enterprise подразумевает наличие в сети RADIUS-сервера. RADIUS-сервер в данной ЛКС используется для хранениях учётных записей администраторов, использующих беспроводной доступ к сети, и обеспечения их доступа к сети.

В рамках проектируемой сети можно обойтись без специализированного сервера, а использовать в его качестве стационарный персональный компьютер, вычислительной мощности которого вполне хватит для обеспечения работы сопутствующего ПО. Выбор пал на бюджетный компьютер Jet Office 3i7, позиционирующий себя как офисный ПК. Процессора Intel Core i3 7100 3900 МГц, 4 Гб оперативной памяти и графического ускорителя Intel HD Graphics 630 будет достаточно для нормальной работы сервера.

В качестве программного обеспечения для настройки AAA-сервера было решено использовать Cisco Secure Access Control Server, так как данное ПО является проприетарным продуктом Cisco с удобным web-интерфейсом и широкими настройками сервера. Процесс настройки RADIUS-сервера описан в разделе 3.6.3.

3.3 Организация рабочих мест

Под рабочим местом следует понимать выделенную часть площади с расположенным на ней технологическим оборудованием и инвентарём, необходимым для выполнения работы. Рабочее место – это первичная ячейка производственной структуры предприятия.

В рамках проекта организация рабочего места не является трудной задачей. Рабочий места администраторов необходимо обеспечить персональными компьютерами и, по требованию заказчика, принтером.

3.3.1 Обоснование выбора рабочей станции администратора

Основной задачей при организации рабочих мест администраторов была обеспечить комфортные условия работы для сотрудников. В первую очередь рабочие станции должны быть оснащены сетевыми адаптерами с возможностью подключения к LAN и быть достаточно мощными для выполнения всех поставленных задач. Исходя из этого выбор пал на компьютеры Irwin Computers Coffee Lake G1-07.

3.3.2 Обоснование выбора принтера

По требованию заказчика в проектируемой локальной сети необходимо наличие принтера для его использования администраторами. Ознакомившись с рынком принтеров был выбран цветной лазерный принтер Ricoh SP C260DNw. Данный принтер имеет возможность быть подключенным к локальной сети либо к беспроводной сети Wi-Fi. Также принтеры компании Ricoh имеют удобный web-интерфейс, попасть в который можно набрав в адресной строке браузера IP-адрес принтера. Он позволяет удалённо посмотреть состояние аппарата, значение счётчиков, а также остаток тонера.

3.4 Разделение сети на виртуальные подсети

Metro Ethernet подразумевает активное использование виртуальных локальных подсетей (далее VLAN). Так как в центре обработки данных есть логическое разделение оборудования на два различных типа – серверное оборудование и оконечное – логично применить VLAN для их разделения. Виртуальные подсети позволяют построить на базе одной физической сети некоторое количество логических подсетей, которые будут существовать независимо друг от друга. Такое разделение на виртуальные локальные подсети позволяет определять некоторые политики безопасности непосредственно для VLAN, а не для каждой станции и сервера по отдельности, а также упрощает понимание устройства и структуры ЛКС за счёт абстрагирования от каждой конкретной станции, позволяя рассматривать их целостно, в совокупности.

Для достижения большей степени административного контроля и логического разделения среды передачи данных было принято решение распределить пользовательские станции и серверы следующим образом:

1. VLAN №99 – административный VLAN, выделенный под рабочие станции, принтер и беспроводной маршрутизатор. В данной структурной единице ЛКС находятся оконечные устройства. К их числу относятся пользовательские станции администраторов, цветной принтер и беспроводной маршрутизатор, обеспечивающий доступ к сети с портативных устройств администраторов (ноутбуки, смартфоны и другие). Все устройства подключены к одному коммутатору. Беспроводные устройства, подключенные к точке доступа, хоть и физически находятся в другой подсети, относятся к виртуальной сети для администраторов.
2. VLAN №10 – VLAN, выделенный под серверное оборудование. В данной виртуальной подсети находятся основной и резервный сервер для обслуживания тонких клиентов, а также AAA-сервер, предназначенный для ограничения доступа к локальной сети. Равно как и устройства в отделе администрирования, все серверы подключены к главному коммутатору.

В связи с маленьким размером проектируемой сети и отсутствием сложных архитектурных условий, лучшим выбором при проектировании сети

будет использование проверенных подходов. Для маршрутизации между различными виртуальными подсетями используется коммутатор третьего уровня. В этой схеме коммутатор выполняет всю маршрутизацию в сети.

3.5 Адресация в локальной компьютерной сети

По условию задания в разрабатываемой ЛКС необходимо осуществить адресацию с применение протоколов IPv4 и IPv6. Протокол адресации IPv4 использует четырёхбайтные адреса, ограничивающие адресное пространство. Традиционно адрес IPv4 записывается четырьмя десятичными числами от 0 до 255, разделёнными точками, через дробь указывается длина маски подсети. Однако данный вид адресации столкнулся с проблемой исчерпания адресов. В ноябре 2019 года были распределены последние IPv4 адреса в Европе, странах бывшего СССР и на Ближнем Востоке. Решить эту проблему призвана новая версия протокола – IPv6. Протокол IPv6 отличается от своего предшественника использованием увеличенной в 4 раза длиной адреса. В связи с исчерпанием IPv4 адресов продвижение новой версии протокола началось активнее.

Сеть разделена на 2 виртуальные подсети:

1. VLAN №99 – административная подсеть.
2. VLAN №10 – серверная подсеть.

IPv6 адреса нужны лишь для некоторых приложений администраторов на их рабочих станциях, поэтому можно назначить эти адреса только на персональных компьютерах администраторов. Так как для администраторов планируется выход только во внутреннюю сеть Metro Ethernet, для их пользовательских станций имеет смысл назначить IPv6 адреса из диапазона Unique Local Unicast.

В таблице 3.3 отображено соответствие оконечного устройства доступному IP-адресу и маскам подсети.

Таблица 3.1 – Соответствие оконечного устройства IP-адресу и маске подсети

Устройство	VLAN	IP-адрес	Маска подсети
1	2	3	4
Рабочая станция #1	VLAN №99	172.17.0.2 fd00:a::2	255.255.255.0 /64
Рабочая станция #2		172.17.0.3 fd00:a::3	255.255.255.0 /64
Рабочая станция #3		172.17.0.4 fd00:a::4	255.255.255.0 /64
Принтер		172.17.0.5	255.255.255.0
Беспроводная точка доступа		172.17.0.6	255.255.255.0
Wi-Fi DHCP Pool		172.17.1.5 … 172.17.1.15	255.255.255.0

Продолжение таблицы 3.1

1	2	3	4
Основной терминальный сервер	VLAN №10	Te0/1: 172.17.2.10 Te0/2: 172.17.2.11	255.255.255.0
Запасной терминальный сервер		Te0/1: 172.17.2.20 Te0/2: 172.17.2.21	255.255.255.0
AAA-сервер		172.17.2.30	255.255.255.0

3.6 Описание настройки компонентов локальной сети

3.6.1 Настройка коммутатора

Для достижения большей степени административного контроля и логического разделения среды передачи данных было принято решение разделить устройства, подключенные к сети, на две группы: серверное оборудование и оборудование администраторов.

Для создания и настройки административного VLAN на коммутаторе необходимо создать его и назначить порты, к которым подключены оконечные устройства, access портами с указанием номера VLAN.

Команды настройки VLAN №99 и VLAN №10 в Cisco IOS по алгоритму, описанному выше, выглядит так:

```
Switch(config)#vlan 99
Switch(config)#interface range Te0/7-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
Switch(config-if-range)#exit
Switch(config)#vlan 10
Switch(config)#interface range Te0/2-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
```

Для настройки Inter-VLAN маршрутизации необходимо разрешить маршрутизацию на коммутаторе и задать ip-адреса на интерфейсах VLAN:

```
Switch(config)#ip routing
Switch(config)#ipv6 routing
Switch(config)#int vlan 10
Switch(config-if)#ip address 172.17.2.1
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#int vlan 99
Switch(config-if)#ip address 172.17.0.1
Switch(config-if)#ipv6 address fd00:A::1/64
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

На интерфейсе Te0/8, к которому подключен принтер через порт f0, можно ограничить пропускную способность интерфейса. Аналогичные операции необходимо произвести с интерфейсами Te0/6-7 и Te0/9-11 коммутатора, которые подключены к портам G0:

```
Switch(config)#interface Te0/8
Switch(config-if)#speed 10000
Switch(config-if)#srr-queue bandwidth limit 1
Switch(config-if)#exit
Switch(config)#interface Te0/6-7,Te0/9-11
Switch(config-if-range)#speed 10000
Switch(config-if-range)#srr-queue bandwidth limit 10
Switch(config-if-range)#exit
```

3.6.2 Настройка удалённого администрирования

Согласно заданию, необходимо настроить удалённое администрирование. На данный момент существует большое количество технологий, позволяющих настроить удалённое администрирование, однако основными в Cisco являются Telnet и SSH.

Telnet получил большое распространение в первую очередь в Unix-подобных системах. Сервис позволяет создать удалённого пользователя при помощи логина и пароля, по которым предоставляется вход в систему. Затем пользователь может удалённо запускать программы или задавать системные команды.

Сетевой протокол SSH (Secure Shell) в отличие от Telnet шифрует все передаваемые данные (в том числе и пароли), что делает его лучшим вариантом, чем Telnet. Шифрование паролей и конфигурационных файлов особенно важно при работе на удалённой пользовательской станции.

Для настройки SSH на коммутаторе необходимо подключиться к нему и выполнить следующие пункты:

1. Установит дату и время (необходимо для генерации ключа).
2. Указать домен и имя устройства.
3. Сгенерировать ключ для SSH.
4. Указать шифрование пароля.
5. Создать пользователя с максимальными привилегиями и задать пароль для привилегированного режима.
6. Активировать протокол AAA.
7. Разрешить компьютерам внутренней сети получать доступ к коммутатору по SSH.
8. Запретить в режиме конфигурирования терминальных линий всё, кроме SSH.
9. Активировать автоматическое поднятие строки после ответа системы на проделанные изменения, позволить входить сразу в

привилегированный режим, настроить автоматическое закрытие SSH сессии через 60 минут.

10. Привязать группу доступа, созданную на шаге 7, к терминальной линии.

Команды настройки SSH приведены ниже:

```
Switch#clock set 00:09:04 03 Dec 2019
Switch #configure terminal
Switch #(config)ip domain name aoks.local
Switch #(config)crypto key generate rsa
Switch #(config)service password-encryption
Switch #(config)username admin privilege 15 secret Tw6QiO0q
Switch #(config)enable secret Tw6QiO0q
Switch #(config)aaa new-model
Switch #(config)access-list 23 permit 172.17.0.0 0.0.0.255
Switch #(config)line vty 0 4
Switch #(config-line)transport input ssh
Switch #(config-line)logging synchronous
Switch #(config-line)privilege level 15
Switch #(config-line)exec-timeout 60 0
Switch #(config-line)access-class 23 in
```

На этом настройка SSH завершена. Для получения удалённого доступа администратору необходимо лишь установить клиент для протоколов удалённого доступа (например PuTTY). Необходимо выбрать тип соединения «SSH» и указать IP-адрес коммутатора в подсети. Также нужно проверить порт – протокол SSH обычно прослушивает соединения на TCP-порту 22. Пример полностью заполненного окна конфигурации представлен на рисунке 3.1.

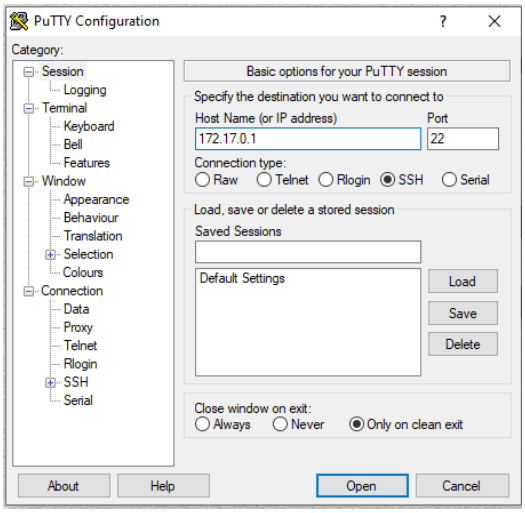

Рисунок 3.1 – Настройка сессии удалённого соединения

3.6.3 Настройка серверного ПО

Учитывая разработку ЛКС для полноценной коммерческой сети целесообразно использовать проприетарный продукт Cisco Secure Access Control Server (ACS) в стеке с ПК Jet Office 3i7. Cisco Secure ACS – программный продукт, конфигурирующийся через веб-интерфейс, позволяющий создавать и управлять мощными, надёжными и отказоустойчивыми системами.

Для настройки AAA на сервере необходимо установить на него Cisco Secure ACS. Установка программы не должна вызвать трудностей. Для перехода к настройкам серверам необходимо в адресную строку браузера ввести IP-адрес сервера, откроется web-интерфейс, после прохождения авторизации в котором будут доступны настройки AAA. Изображение интерфейса представлено на рисунке 3.2.

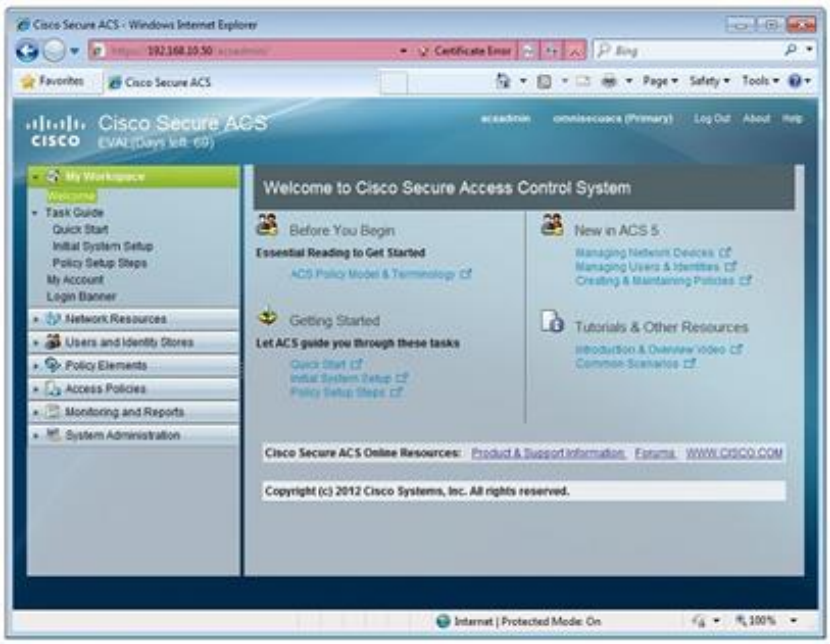

Рисунок 3.2 – Web-интерфейс Cisco Secure ACS

Для настройки сервера RADIUS необходимо перейти во вкладку «Network Resources», выбрать там подкатегорию «AAA», далее «AAA Servers and Groups», затем выбрать «Servers». Откроется список созданных серверов. Для создания нового сервера необходимо нажать кнопку «Add» и настроить новый сервер: выбрать тип сервера «RADIUS», назначить IP сервера 172.17.2.30, проверить порт авторизации и порт аккаунтинга (обычно это 1645 и 1646, стандартные порты для Cisco, рекомендуется использовать именно эти порты) и задайте ключ конфигурации («config_key_XcQ»). По нажатию «ОК» начинается процесс создания сервера, окно становится неактивно. В случае успешного создания сервера окно конфигурирования закроется, новый RADIUS-сервер появится в списке серверов.

Для управления пользователями необходимо нажать на вкладку «Users and Identity Stores», затем «Internal Identity Stores» и «Users». Для создания и добавления пользователя необходимо кликнуть на кнопку «Create» (рисунок 3.3).

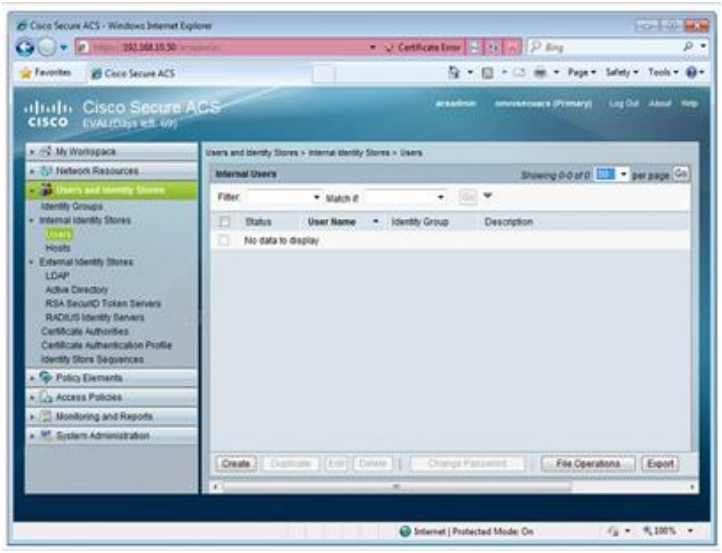

Рисунок 3.3 – Список пользователей в Cisco Secure ACS

Далее необходимо заполнить имя пользователя, выставить статус «Enabled» и ввести пароль пользователя (рисунок 3.4). При необходимости можно заполнить описание пользователя и определить для него группу, но для маленькой сети это имеет не много смысла.

По нажатию на кнопку «Submit» создание пользователя будет завершено, окно будет закрыто, отобразится список всех пользователей (рисунок 3.5). На этом процесс создания пользователя завершается.

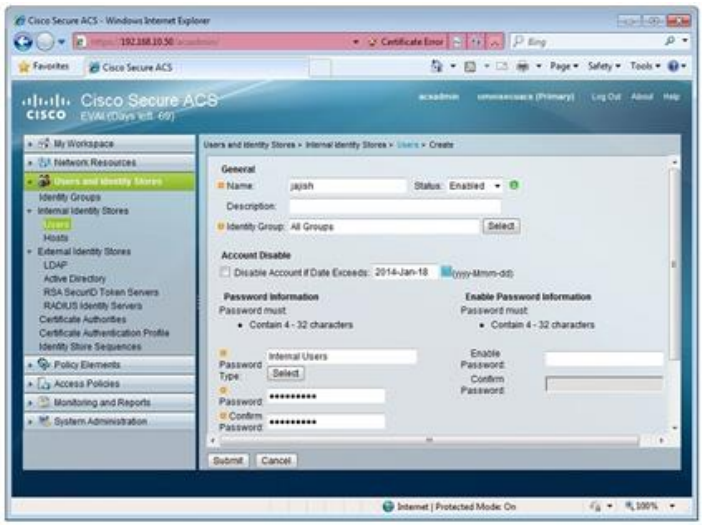

Рисунок 3.4 – Создание нового пользователя в Cisco Secure ACS

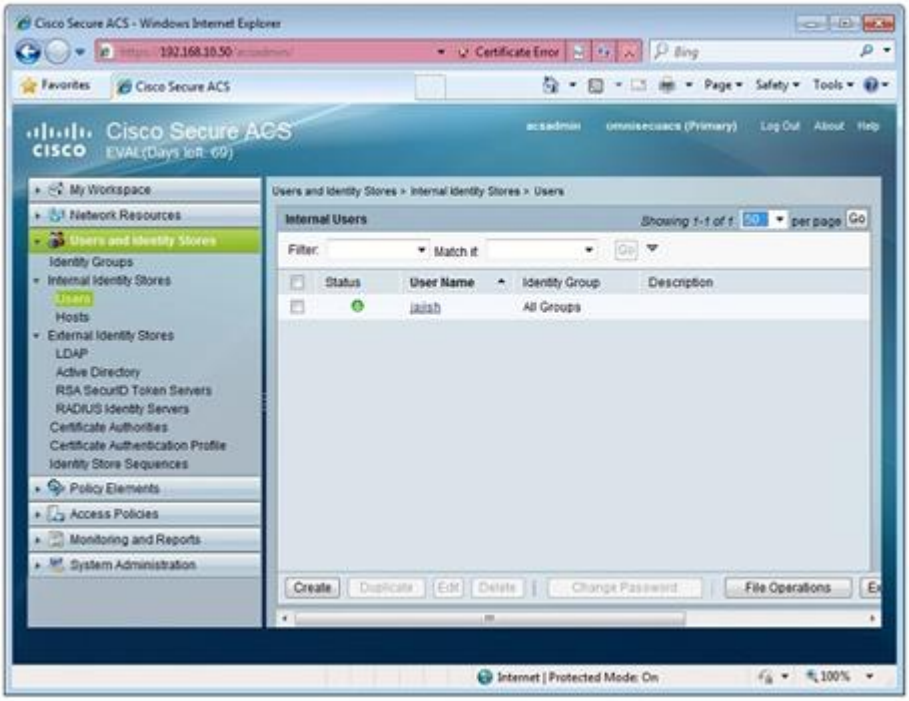

Рисунок 3.5 – Обновлённый список пользователей после создания одного из них в Cisco Secure ACS

3.6.4 Настройка беспроводной точки доступа

Для использования беспроводной точки доступа её необходимо заранее настроить. Для перехода к графическому интерфейсу настройки необходимо в адресной строке браузера ввести IP-адрес точки доступа (172.17.0.6).

На вкладке «General» необходимо ввести SSID точки доступа («Admin Wi-Fi»), VLAN ID (10), шлюз по умолчанию (172.17.0.1), IP-адрес точки доступа в рамках подсети в текстовом поле «Internet IP Address» (172.17.0.6) и адрес внутри WAN в текстовом поле «Router IP Address» (172.17.1.1).

Перейдём к настройке шифрования, для этого нужно перейти на вкладку WLAN и выбрать «Create New». В открывшемся окне нужно выбрать вкладку «Security», в ней «Layer 2». В окне настройки безопасности выбрать тип шифрования «WPA+WPA2», отметить чекбокс «WPA2 Policy-AES» и «802.1X Enable» (рисунок 3.6).

Далее необходимо настроить доступ к AAA-серверу на беспроводной точке доступа. Интерфейс настройки представлен на рисунке 3.6. Для этого, не покидая вкладки «Security», следует нажать на вкладку «AAA Servers», выбрать вид аутентификации «RADIUS Authentication», кликнуть «New», после чего перейти к настройке сервера.

Здесь необходимо указать IP-адрес RADIUS-сервера (172.17.2.30), ввести ключ RADUIS-сервера («config_key_XcQ»), изменить порт по умолчанию на порт 1645, проверить статус сервера и после этого нажать «ОК».

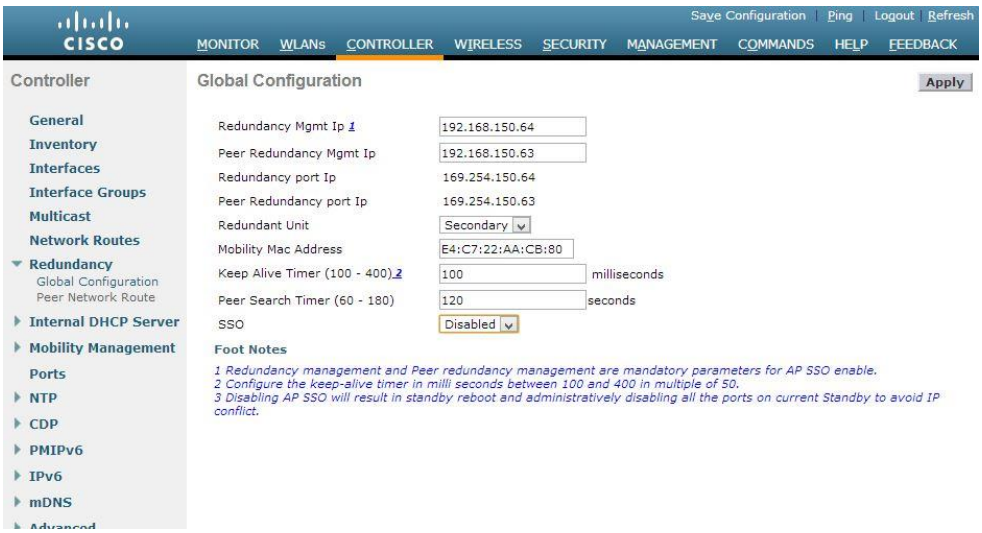

Рисунок 3.6 – Окно настройки WLAN

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

Рисунок 3.7 – Окно настройки RADIUS-сервера

Точка доступа Cisco Aironet 1602I поддерживает протокол DHCP, для его настройки также необходимо воспользоваться графическим интерфейсом пользователя. Во вкладке «General» необходимо пролистать вниз до «DHCP Server Settings». В окне настройки нажать кнопку «Enable» напротив «DHCP Server», выбрать начальный IP-адрес для раздачи (172.17.1.5), и выбрать максимальное количество пользователей (с учётом размеров сети десяти пользователей будет достаточно).

На этом настройка беспроводной точки доступа закончена.

3.6.5 Настройка принтера

Для подключения принтера к локальной сети необходимо подключиться к нему с административной станции при помощи USB-кабеля и запустить установку драйверов с установочного диска, идущего в комплекте. В окне с предложением выбрать тип подключения выберите «Сетевое подключение» (рисунок 3.8).

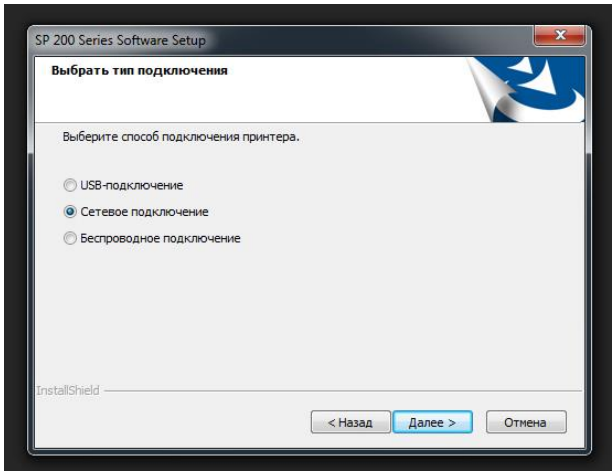

Рисунок 3.8 – Выбор типа подключения принтера

Далее следует перейти к ручной настройке сети принтера. В открывшемся окне необходимо задать наличие/отсутствие DHCP, IP-адрес, маску подсети и шлюз. После настройки принтера можно воспользоваться его web-интерфейсом, введя в адресной строке браузера IP-адрес принтера (рисунок 3.9). В web-интерфейсе информация о количестве тонера, очереди документов и другом.

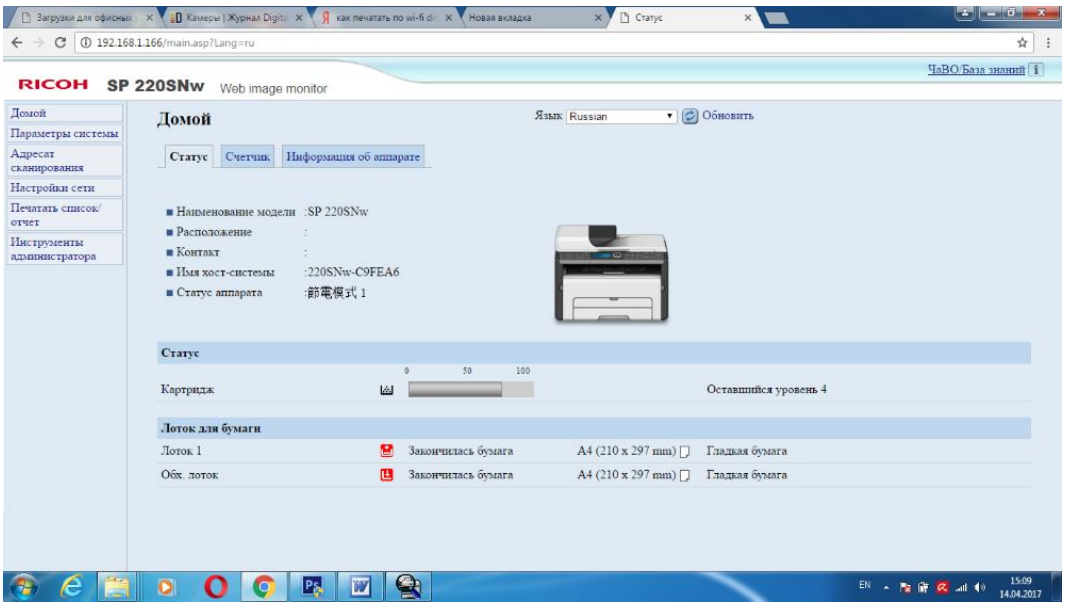

Рисунок 3.9 – Web-интерфейс принтера Ricoh SP C260DNw

3.6.6 Настройка персональных компьютеров

Персональные компьютеры администраторов подключаются посредством Ethernet. Для настройки администраторских ПК необходимо зайти в панель управления, выбрать раздел «Сеть и Интернет», в разделе «Сетевые подключения» нажать кнопку «Изменение настроек адаптера». В открывшемся окне перейти к настройкам Ethernet, нажать на «IP версии 4», на кнопку свойства и задать в открывшемся окне свойств IP-адрес компьютера, маску подсети и основной шлюз. Пример настройки представлен на рисунке 3.10. После успешной настройки изображение красного крестика пропадёт.

Аналогичным образом настраивается и IPv6 адрес, пример настройки на рисунке 3.11.

Процедуру настройки адресов необходимо повторить на всех административных персональных компьютерах согласно таблице адресации.

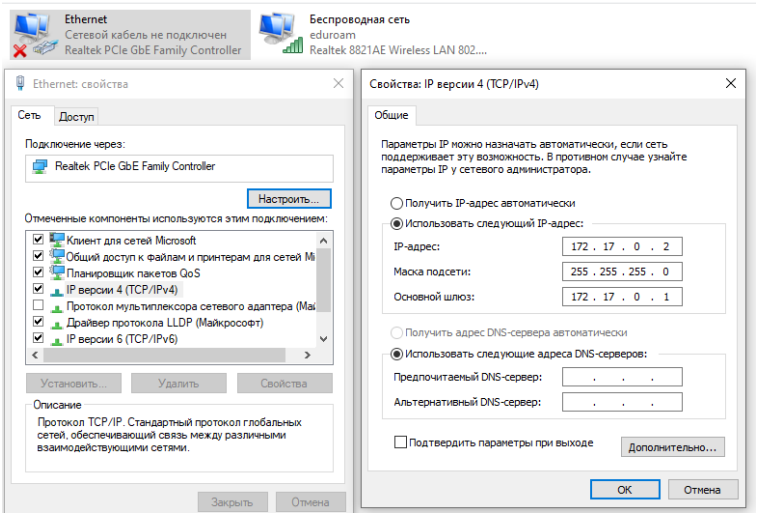

Рисунок 3.10 – Настройка IPv4 на ПК

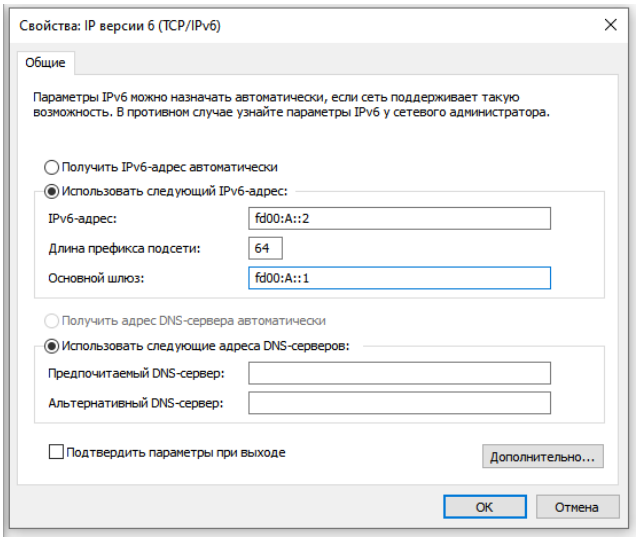

Рисунок 3.11 – Настройка IPv6 на ПК

3.7 Переключение основного терминального сервера на резервный

Переключением на резервный сервер в случае отказа (fail-over) называется процедура включения в систему другого сервера взамен вышедшего из строя. При этом не стоит путать аварийное переключение сервера как реакция на отказ с запланированным переключением (switch-over).

В проектируемой ЛКС используется сервер с двумя портами, один является основным информационным портом, через который идёт трафик для тонких клиентов, второй порт используется для администрирования. IP-адрес информационного интерфейса сбрасывается в случае, если сервер прекращает свою работу по любым причинам.

В ходе работы сервера происходит процесс репликации данных, когда обновление данных на основном сервере также сохраняется на резервном сервере. Процесс репликации происходит раз в 10 минут.

В общем случае процедура переключения на резервный сервер в случае отказа основного состоит из нескольких шагов:

1. Основной сервер пингуется раз в секунду по административному каналу Te0/2 (heartbeat). IP-адрес административного интерфейса основного сервера 172.17.2.11.
2. В случае, если основной сервер перестал пинговаться, репликация данных с основного сервера на резервный прекращается, на основном сервере сбрасывается IP-адрес на информационном интерфейсе (Te0/1), IP-адрес информационного интерфейса резервного сервера (Te0/1) заменяется на IP-адрес информационного интерфейса основного сервера (172.17.2.10). В этот момент пользователи вновь получают доступ.
3. Основной сервер продолжает пинговаться по административному каналу с администраторской станции (порт Te0/2 резервного сервера). При этом для мониторинга работы резервного сервера проверяется доступ также и к нему по IP-адресу 172.17.2.21.
4. В случае, если основной сервер возобновил свою работу, данные с резервного сервера реплицируются на основной, на информационном интерфейсе резервного сервере IP-адрес изменяется на его основной IP-адрес (172.17.2.20), на информационном интерфейсе основного сервера восстанавливается его IP-адрес (172.17.2.10).

Для автоматизации процесса репликации и переключения серверов используется специализированное административное ПО. Примером такого программного обеспечения является vGate. Весь процесс смены сервера в данной программе автоматизирован, достаточно создать два сервера на вкладке «Серверы» нажав кнопку «Добавить сервер», задать для каждого сервера основной и дополнительный адрес, указать зависимость «Резервный сервер» для второго сервера. Смена сервера происходит автоматически.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

В данном разделе описывается практическая реализация ЛКС (прокладка коробов с Ethernet-кабелем, размещение оборудования и сопутствующие мероприятия). Данный раздел сопровождается планом пристройки, в которой располагается центр обработки данных (приложение «В»).

4.1 Общая организация СКС

В проектируемой ЛКС кабельная подсистема реализована с помощью прокладки в кабельном коробе витой пары категории 5е вдоль стены по плинтусу. На коридор и в серверную комнату кабель прокладывается через поперечные отверстия в стене. В коридоре кабельный короб находится под фальшполом. В кабельном коробе кабель идёт до соответствующей ему информационной розетки, через которую происходит подключение оконечных устройств к сети. Сетевые розетки расположены на стене близко к полу и в непосредственной близости к соответствующим устройствам.

Рабочие места администраторов расположены в углу отдела администрирования и оснащены столами (2 прямых и один угловой), креслами, персональными компьютерами.

Между стеной коридора и столом одного из администраторов расположен шкафчик, внутри которого находится коммутатор. Во избежание использования вертикальных кабельных подсистем беспроводную точка доступа расположена на центральном рабочем месте без сопутствующего монтажа. Принтер расположен рядом с одним из рабочих мест и подключен в локальную сеть.

4.1.1 Обоснование выбора среды передачи данных

Кабель «витая пара» имеет несколько категорий, нумеруемых от 1 до 8, которые определяют эффективный пропускаемый частотный диапазон. Пропускную способность в 10 Гб/с на расстоянии менее 100 метров гарантирует витая пара категории 6а и выше. Для соединений с пропускной способностью в 1 Гб/с будет достаточно кабеля пятой категории. В связи с тем, что расстояния внутри проектируемой ЛКС меньше 100 метров, целесообразно использовать «витую пару» вместо оптоволокна.

Одним из пожеланий заказчика является обеспечение пожарной безопасности сети. Исходя из этого пожелания для прокладки кабельной системы необходимо придерживаться ГОСТ 31565-2012 «Кабельные изделия. Требования пожарной безопасности». Наиболее пожаробезопасными кабелями являются кабельные изделия категории FRLSLTx и FRHFLTx.

Исходя из вышеописанного было принято решение организовать кабельную систему на основе кабеля категории 5е для Gigabit Ethernet и Fast

Ethernet соединений и кабеля категории 6a для 10 Gigabit Ethernet соединений в огнестойкой оболочке из низкотоксичного ПВХ пластика пониженной пожарной опасности с низким дымо- и газовыделением категории FRLSLTx.

Все соединения в данной локальной сети реализованы витой парой с коннекторами RJ-45 прямого типа, используемый тип обжима – перекрёстный.

4.1.2 Обоснование выбора информационных розеток

Для подключения устройств к сети необходимо обеспечить доступность устройств к кабелю. Удобно и эстетично организовать доступ позволяет монтаж информационных розеток RJ-45. Недорогим вариантом информационных розеток являются отечественные Этюд Кома-001К, обеспечивающие доступ к сети.

4.1.3 Обоснование выбора кабельного короба

Учесть пожелание заказчика, касающееся пожарной безопасности, труднее при выборе кабельного короба. Большинство производителей делают кабельные коробы из легковоспламеняющегося ПВХ без особого внимания к огнестойкости, однако во время поиска подходящего короба на белорусском рынке были найдены огнеупорные каналы ЭкоПласт МЕХ Е15-Е110. Маркировка «Е15-Е110» означает, что изделие выдерживает напор огня от 15 до 110 минут, чего вполне хватит для удовлетворения потребностей заказчика, касающейся пожарной безопасности.

4.1.4 Обоснование выбора серверных стоек

Для размещения терминальных серверов необходимо приобрести две серверные стойки исходя из размеров терминального сервера (445 мм в ширину, 746 мм в глубину). Под данные габариты подходит двухрамная стойка TWT-RACK2-33U (рисунок 3.8). Стойки нужно приобрести в количестве двух штук. В серверной комнате находятся две такие серверные стойки на расстоянии одного метра друг от друга с расположенными на них основным и запасным серверами для обслуживания тонких клиентов. Рядом с запасным сервером на полу находится RADIUS-сервер.

Для обеспечения пожарной безопасности в отделе администрирования и в серверной комнате в углах помещений расположены углекислотные огнетушители. Углекислотные огнетушители в процессе тушения не наносят ущерб электро- и оргтехнике.

4.1.4 Размещение беспроводной точки доступа

Беспроводной доступ к сети администраторы должны получать из двух помещений: из комнаты администраторов и из серверной комнаты.

Максимально поддерживаемая скорость точкой доступа Cisco Aironet 1602I на частоте 2,4 ГГц – 500 Мбит/с, однако реальная скорость доступа будет меньше.

Учитывая небольшие размеры помещений, а также их близость относительно друг друга предположим, что необходима одна точка доступа для обслуживания администраторов. В приоритете пользования точкой доступа является отдел администрирования. Между кабинетом администраторов и серверным помещением находятся две межкомнатные стены, поэтому необходимо рассчитать затухание радиоволн при размещении точки доступа в кабинете администраторов.

Согласно плану этажа, комнаты разделены коридором площадью 20 м^2 (8 метров в длину и 2,5 метра в ширину). Серверное помещение находится севернее коридора и занимает площадь 10 м^2 (длина 4,5 метра, ширина 2,2 метра), южнее находится кабинет администраторов общей площадью 30 м^2 (длина 5,8 метров, ширина 5,3 метра). Друг от друга комнаты отделяют две межкомнатные стены длиной 4,5 метра.

Затухание радиоволн в беспрепятственной воздушной среде рассчитывается по формуле 4.1 и измеряется в децибелах.

$$L = 32{,}44 + 20\lg(F) + 20\lg(D), \quad (4.1)$$

где F – частота в ГГц, D – расстояние в метрах.

Рассчитаем затухание в администраторском кабинете по формуле 4.1: $L = 32{,}44 + 20\lg(2{,}4) + 20\lg(5{,}8) = 74{,}26$ дБ.

Обеспечение хорошего сигнала точкой доступа Cisco Aironet 1602I необходимо обеспечивать её расположением в непосредственной близи от рабочих мест, чтобы покрыть их сигналом. Учитывая, что помещения разделяют обычные межкомнатные стены, около 30% сигнала будут теряться[35]. При этом доступ к беспроводной сети в кабинете администраторов будет обеспечен.

В результате было решено использовать одну точку беспроводного доступа, которая будет расположена на центральном рабочем месте администратора.

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсового проекта была разработана локальная компьютерная сеть для центра обработки данных компании, занимающейся программирование. По итогу работы была спроектирована завершённая структурированная кабельная система, выбрано необходимое оборудование, произведены все настройки, необходимые для работы оконечных устройств локальной сети. Созданная локальная сеть получилась достаточно простой для её реализации и надёжной.

Полученная сеть полностью удовлетворяет пожеланиям, предъявленным заказчиком:

1. Основное помещение оснащено тремя рабочими местами для администраторов и принтером.
2. Серверная комната оснащена основным и резервным серверами для одновременного обслуживания до 100 тонких клиентов.
3. Реализована возможность подключения к беспроводной сети и ограничение доступа для лиц, не являющимися сотрудниками центра обработки данных.
4. Обеспечено удалённое администрирование коммутатором.
5. Обеспечена повышенная пожарная безопасность сети.

Активное и пассивное сетевое оборудование, а также пользовательские станции, принтер, серверы и другое техническое обеспечение, выбранное для реализации, соответствует стандартам качества, надёжности и зарекомендовало себя как одно из лучших решений для малых и средних локальных компьютерных сетей.

СПИСОК ЛИТЕРАТУРЫ

[1] Сергеев, А. Основы локальных компьютерных сетей / А. Сергеев – М.: Лань, 2016. – 185 с.

[2] Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзэролл – СПБ.: Питер, 2012 – 962 с.

[3] Одом, У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация / У. Одом, пер. с английского ООО «И. Д. Вильямс», М.: 2015. – 736 с., с илюс.

[4] Одом, У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND1 100-101. Академическое издание / У. Одом, пер. с английского ООО «И. Д. Вильямс», М.: 2016. – 903 с., с илюс.

[5] InterVLAN Routing в сети передачи данных [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/138883/ - Дата доступа – 20.12.2019.

[6] Wi-Fi с логином и паролем для каждого пользователя или делаем WPA2-EAP/TLS подручными средствами [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/170949/ - Дата доступа – 20.12.2019.

[7] WPA2-Enterprise, или правильный подход к безопасности Wi-Fi сети [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/150179/ - Дата доступа – 20.12.2019.

[8] Тонкий клиент – что это и с чем его едят [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/76159/ - Дата доступа – 20.12.2019.

[9] Тонкие клиенты как они есть [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/90670/ - Дата доступа – 20.12.2019.

[10] Настройка SSH в Cisco [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/68262/ - Дата доступа – 20.12.2019.

[11] Настройка беспроводных сетей на контроллере Cisco [Электронный ресурс]. – Электронные данные. – Режим доступа: https://habr.com/ru/post/148903/ - Дата доступа – 20.12.2019.

[12] Проект. Терминальный сервер на 100 человек [Электронный ресурс]. – Электронные данные. – Режим доступа: http://itsave.ru/тонкие-клиенты-для-малого-бизнеса/ - Дата доступа – 20.12.2019.

[13] Создание терминальных сетей на базе тонких клиентов [Электронный ресурс]. – Электронные данные. – Режим доступа: https://alex-service.ru/product/clients/ - Дата доступа – 20.12.2019.

[14] Категория пожарной опасности (кабельная маркировка) [Электронный ресурс]. – Электронные данные. – Режим доступа:

https://www.profsector.com/parameter/1228/kategoriya-pozharnoy-opasnosti-kabelnaya-markirovka - Дата доступа – 20.12.2019.

[15] Правила противопожарной безопасности при проектировании СКС [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.xnets.ru/plugins/content/content.php?content.96.8 - Дата доступа – 20.12.2019.

[16] ГОСТ 31565-2012 Кабельные изделия. Требования пожарной безопасности [Электронный ресурс]. – Электронные данные. – Режим доступа: http://docs.cntd.ru/document/1200101754 - Дата доступа – 20.12.2019.

[17] Технические характеристики витой пары [Электронный ресурс]. – Электронные данные. – Режим доступа: https://hobbyits.com/texnicheskie-xarakteristiki-vitoj-pary/ - Дата доступа – 20.12.2019.

[18] Обжим кабеля RJ45 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://day24h.ru/raznoe/obzhim-kabelya-rj45-kompyuter-router-raspinovka-setevogo-kabelya-router-kompyuter.html#_RJ45_RJ45 - Дата доступа – 20.12.2019.

[19] System x3650 M4 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://lenovopress.com/tips0850-system-x3650-m4-e5-2600-v2 - Дата доступа – 20.12.2019.

[20] Стойка двухрамная TWT-RACK2-33U-6x10 M4 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.ttn.by/computers_and_networks/server_equipment/server_cabinets_and_racks/stoyka_dvuhramnaya_twt_twt_rack2_33u_6x10_code430891 - Дата доступа – 20.12.2019.

[21] Розетка компьютерная RJ45 кат. 5e [Электронный ресурс]. – Электронные данные. – Режим доступа: http://wolframbel.by/r-koma-001k/ - Дата доступа – 20.12.2019.

[22] Кабель «витая пара» (LAN) для структурированных систем связи [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.tinko.ru/catalog/product/267136/ - Дата доступа – 20.12.2019.

[23] Огнестойкие кабельные системы [Электронный ресурс]. – Электронные данные. – Режим доступа: http://lebelectro.by/ognestojkie-kabelnye-linii/ognestojkie-kabelnye-kanaly - Дата доступа – 20.12.2019.

[24] Принтер Ricoh SP C260DNw [Электронный ресурс]. – Электронные данные. – Режим доступа: https://catalog.onliner.by/printers/ricoh/spc260dnw - Дата доступа – 20.12.2019.

[25] Коммутатор Cisco SG350XG-24T-K9 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://catalog.onliner.by/switch/cisco/sg350xg24tk9 - Дата доступа – 20.12.2019.

[26] AIR-CAP1602I-R-K9 Cisco WIFI [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.vtkt.ru/catalog/wlanarea/wifiapoints/cisco_aironet_air_cap1602i_wifi_tochka_dostupa_s_3_vstroennymi_antennami/ - Дата доступа – 20.12.2019.

[27] Jet Office 3i7 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://catalog.onliner.by/desktoppc/jets/jet13i7100d8h0mn - Дата доступа – 20.12.2019.

[28] Irwin Computers Coffee Lake G1-07 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://catalog.onliner.by/desktoppc/irwin/coffeelakeg107 - Дата доступа – 20.12.2019.

[29] Инструкция по подключению многофункциональных устройств серии [Электронный ресурс]. – Электронные данные. – Режим доступа: Ricoh SP 220 https://www.ixbt.com/infopages/ricoh-sp-220-325.shtml#ethernet - Дата доступа – 20.12.2019.

[30] Metro Ethernet – услуги для операторов связи в «немаркетинговом» понимании [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.sib.com.ua/arhiv_2009/2009_4/statia%204_6%202009/4_6_2009.htm - Дата доступа – 20.12.2019.

[31] Metro Ethernet. Архитектура и технологии [Электронный ресурс]. – Электронные данные. – Режим доступа: https://nag.ru/articles/reviews/15443/metro-ethernet-arhitektura-i-tehnologii.html - Дата доступа – 20.12.2019.

[32] Переключение на резервный сервер [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.delphiplus.org/mysql-optimizatsiya-proizvoditelnosti/pereklyuchenie-na-rezervnyi-i-vozvrat-na-osnovnoi-server-pri-otkaze.html - Дата доступа – 21.12.2019.

[33] Оценка трафика для RDP сессии пользователя на RDS сервере [Электронный ресурс]. – Электронные данные. – Режим доступа: http://winitpro.ru/index.php/2017/02/15/bandwidth-usage-per-users-on-rds-2012/ - Дата доступа – 20.12.2019.

[34] Процедура переключения на резервный сервер в случае выхода из строя основного [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.vmgu.ru/articles/vgate-r2-server-failover-and-failback - Дата доступа – 22.12.2019.

[35] Коэффициенты затухания сигнала Wi-Fi при прохождении через различные среду [Электронный ресурс]. – Электронные данные. – Режим доступа: https://help.keenetic.com/hc/ru/articles/213968869-Коэффициенты-затухания-сигнала-Wi-Fi-при-прохождении-через-различные-среды - Дата доступа – 23.12.2019.

ПРИЛОЖЕНИЕ А
(обязательное)

Схема СКС структурная

ПРИЛОЖЕНИЕ Б
(обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(обязательное)

Схема СКС. План этажа

ПРИЛОЖЕНИЕ Г
(обязательное)

Перечень оборудования, изделий и материалов