

аМинистерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Аппаратное обеспечение компьютерных сетей

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовому проекту
на тему
ЛОКАЛЬНАЯ КОМПЬЮТЕРНАЯ СЕТЬ,
ВАРИАНТ 64

БГУИР КП 1–40 02 01 01 064 ПЗ

Студент:

И.А. Григорик

Руководитель:

А.В. Русакович

МИНСК 2023

Вариант	64
Объект	научно-исследовательская организация (металлообработка)
Форма здания, этажи, суммарная площадь одного этажа в квадратных метрах	вытянутая прямоугольная (с соотношением сторон 1:4), 1-3, 410
Количество стационарных пользователей (ПК), количество стационарных подключений, количество мобильных подключений	условный заказчик не уверен, от 10, 20
Сервисы (дополнительные подключения)	файловый сервер NTFS/SMB для внутреннего использования
Прочее оконечное оборудование (дополнительные подключения)	цветные принтеры, принтеры
Подключение к Internet	Metro Ethernet
Внешняя адресация IPv4; внутренняя адресация IPv4; адресация IPv6	непосредственного подключения к провайдеру нет, приватная подсеть, взаимодействие в рамках внутренней сети.
Безопасность	усиленная безопасность в отношении учетных записей пользователей
Надежность	особых требований нет
Финансы	полноценная коммерческая сеть
Производитель сетевого оборудования	условный заказчик не уверен
Дополнительные требования заказчика	нет

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	5
1 ОБЗОР ЛИТЕРАТУРЫ	6
1.1 NTFS/SMB сервер	6
1.2 Двухфакторная аутентификация	7
1.3 Использование VLAN.....	7
1.5 Использование NAT и PAT.....	8
1.6 Использование контроллера точек доступа	9
1.7 Конфигурирование адресов по SLAAC	9
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ.....	11
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ	15
3.1 Обоснование выбора оборудования для рабочих мест	15
3.1.1 Рабочие станции.....	15
3.1.2 Принтеры	16
3.2 Настройка оконечных устройств.....	17
3.2.1 Настройка пользовательских станций	17
3.2.3 Настройка принтеров.....	25
3.3 Обоснование выбора активного сетевого оборудования.....	25
3.3.1 Маршрутизатор	25
3.3.2 Коммутатор.....	26
3.3.3 Файловый сервер.....	27
3.3.4 Беспроводные точки доступа.....	28
3.3.5 Контроллер точек доступа	29
3.4 Обоснование выбора пассивного сетевого оборудования.....	30
3.4.1 Телекоммуникационный шкаф.....	30
3.5 Обоснование выбора серверного ПО	31
3.6 Настройка активного сетевого оборудования.....	31
3.6.1 Настройка NTFS/SMB сервера.	31
3.7 Разделение сети на внутренние виртуальные подсети.....	32
3.8 Составление таблицы адресации в ЛКС.....	33
3.9 Описание и настройка компонентов локальной сети.....	35
3.9.1 Настройка маршрутизатора	35
3.9.2 Настройка коммутатора.....	37
3.9.3 Настройка беспроводной точки доступа	39
3.9.4 Настройка контроллера точек доступа	40
4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ	43
4.1 Обоснование выбора среды передачи данных	43
4.2 Обоснование выбора сетевых розеток	43
4.3 Обоснование выбора кабельного короба.....	44
4.3 Размещение и монтаж активного сетевого оборудования.....	44

4.2.1 Расчёт качества покрытия беспроводной сетью	46
4.3 Размещение и монтаж пассивного сетевого оборудования.....	47
ЗАКЛЮЧЕНИЕ	49
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	50
ПРИЛОЖЕНИЕ А	52
ПРИЛОЖЕНИЕ Б.....	53
ПРИЛОЖЕНИЕ В	54
ПРИЛОЖЕНИЕ Г	55
ПРИЛОЖЕНИЕ Д	56
ПРИЛОЖЕНИЕ Е.....	57
ПРИЛОЖЕНИЕ Ж	58
ПРИЛОЖЕНИЕ З.....	59
ПРИЛОЖЕНИЕ И	60

ВВЕДЕНИЕ

Сетевая инфраструктура является одной из важнейших частей любой современной сферы деятельности. Компьютерные сети нужны практически в любых сферах: от бизнеса и маркетинга, до образования и исследовательских лабораторий. Благодаря компьютерным сетям работа оптимизируется, становится быстрее, легче и надёжнее.

Ключевой частью любой компьютерной сети является выход в интернет. По данному варианту его необходимо реализовать путём использования существующего подключения к транспортной сети Metro Ethernet. Сети данного типа характеризуются как подключениями точка-точка, так и многоточечным подключением в городской сети. Данный тип сети обладает преимуществами, например, лёгкой масштабируемостью, хорошим отношением цена/качество и простотой использования.

Помимо решения основной задачи обеспечения общения между пользователями, частной задачей компьютерных сетей так же является обеспечение совместного доступ к данным, поэтому под данную сеть по требованию условного заказчика необходимо создать отдельный сервис NTFS/SMB с внутренним сервером. Файловая система NTFS поддерживается операционной системой Windows, однако так же, доступ к ней можно получить на базе операционных систем Linux с использованием дополнительных модулей ядра. Данный формат файловой системы разрабатывался компанией Microsoft для Windows NT. Протокол SMB является протоколом коммуникации, который кроме взаимодействия с некоторым сетевым оборудованием и общего доступа к директориям обеспечивает механизм межпроцессорной коммуникации.

Одно из ключевых качеств компьютерных сетей – её безопасность, ибо безопасные сети становятся лёгкой добычей для злоумышленников. По варианту требуется обеспечить усиленную безопасность в отношении учетных записей пользователей.

Количество стационарных пользователей будет определяться разработчиком, соответственно будет выбираться в зависимости от размера и нагрузки на сеть. Количество стационарных подключений – от 10, а количество мобильных в размере 20.

Здание вытянутое, прямоугольное с соотношением 1 к 4, так что располагать рабочие места и сетевое оборудование будет удобно.

Цель проекта: разработка локальной компьютерной сети для научно-исследовательской организации, занимающейся изучением металлообработки.

Задачи: изучение материала и технологий, заданных по заданию; разработка структурной схемы сети; использование устройств и обоснование их выбора, описание настройки устройств, составление функциональной схемы, подведение итогов разработанной системы.

1 ОБЗОР ЛИТЕРАТУРЫ

В ходе выполнения курсовой работы были применены знания, полученные в ходе изучения дисциплин «Теоретические основы компьютерных сетей», «Администрирование компьютерных систем и сетей» и «Аппаратное обеспечение компьютерных сетей». Так же из интернет-источников и книг были подчерпнуты знания и принципы проектирования и администрирования локальных сетей.

1.1 NTFS/SMB сервер

NTFS – самая распространённая файловая система для жёстких дисков или твердотельных накопителей, разработанная Microsoft и используемая по сей день. NTFS, основная файловая система для последних версий Windows и Windows Server, предоставляет полный набор функций, включая дескрипторы безопасности, шифрование, квоты дисков и расширенные метаданные. Его можно использовать с общими томами кластера для обеспечения непрерывно доступных томов, к которым можно получить доступ одновременно из нескольких узлов отказоустойчивого кластера. NTFS позволяет задать разрешения для файла или папки, указать группы и пользователей, доступ к которым требуется ограничить или разрешить, и выбрать тип доступа, чем обеспечивает повышенную безопасность. Из этого можно предположить, что NTFS – подходящая система для использования в качестве основной файловой системы на серверах.

Samba представляет собой программный пакет с открытым исходным кодом, дающий сетевым администраторам возможность гибко и свободно настраивать, конфигурировать и выбирать системы и оборудование, то есть устанавливать на компьютерах UNIX/Linux имитации устройств с Windows. Это упрощает выполнение задач по обмену файлами (как файл-серверам) или задавать параметры печати в качестве принт-серверов.

Samba обеспечивает свободный доступ к:

1. Диска Linux к Windows-компьютерам;
2. Диска Windows к оборудованию с ПО Linux;
3. Принтерам Linux к Windows-компьютерам;
4. Принтерам Windows к Linux-системам.

Собственно, файловый сервер NTFS/SMB представляет собой файловый сервер, работающий под управлением операционной системы Linux или Windows, в задачи которого входит разделение папок и настройка доступа к ним. В конечном итоге и на Windows и на Linux задача настройки сводится к тому, чтобы настроить разделяемое файловое пространство, и настроить правила доступа к нему.

1.2 Двухфакторная аутентификация

Так как по требованию условного заказчика было необходимо реализовать повышенную безопасность в отношении учётных записей пользователей — было принято решение использования двухфакторной аутентификации.

Двухфакторная аутентификация — это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж — это логин и пароль, второй — специальный код, приходящий по SMS или электронной почте. Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя. В общем, суть подхода очень проста: чтобы куда-то попасть, нужно дважды подтвердить тот факт, что вы — это вы, причем при помощи двух «ключей», одним из которых вы владеете, а другой держите в памяти. Данный тип аутентификации практически всегда гарантирует безопасность пользователя, чем и достигается дополнительная ступень безопасности.

Для двухфакторной аутентификации было использовано приложение miniOrange. Данное приложение просто в настройке и поддерживает аутентификацию через Google Authenticator. Его легко настроить, и он будет аутентифицировать пользователей с помощью SMS, push-сообщений, идентификатора устройства или QR-кода.

Следующая принятая ступень — настройка часов использования. Данный механизм позволяет разрешить вход в учётную запись лишь по определённому времени (в большинстве согласуется с рабочим графиком человека). По истечении времени входа пользователя в систему пользователь может продолжать работать на рабочей станции, но не может получить доступ ни к каким сетевым ресурсам, за исключением уже открытых ресурсов, таких как общие ресурсы, к которым обращается пользователь. В Windows Server можно отключить пользователей от всех сетевых ресурсов по истечении их рабочего времени, что является лучшей практикой в защите учётных записей пользователей.

1.3 Использование VLAN

Так же при проектировании сети была произведена процедура разбиения сети на VLAN — виртуальный ЛКС, которые существуют на втором уровне модели OSI. Виланы позволяют строить на базе одной физической сети некоторое количество логических, причем логические сети будут существовать независимо друг от друга, то есть переданный в одной сети пакет никогда не будет принят в другой. VLAN обладают рядом преимуществ, таких как разграничение трафика, адаптация к изменению в сети, логическое

разбиение сети и так далее.

Так же следует упомянуть про маршрутизацию между VLANs. На данный момент распространены два типа маршрутизации: «Router-on-a-Stick», «InterVLAN Routing», и «IVR via L3 Switch». Данные типы маршрутизации разделяются по видам подключения каналов «маршрутизатор-коммутатор». В первом случае канал «маршрутизатор-коммутатор» является trunk-каналом, при чём на маршрутизаторе создаются подинтерфейсы, за счёт которых и происходит маршрутизация между VLANs. Данный способ эффективен для использования в сетях с большим количеством VLANs, так как при втором способе сделать канал «маршрутизатор-коммутатор» намного сложнее. Во втором способе на маршрутизатор от коммутатора идёт количество каналов, равное количеству маршрутизируемых VLANs. При этом каждый канал назначает access-роль, за счёт чего и достигается маршрутизация между интерфейсами. При третьем способе используется L3 коммутатор, в котором создаются виртуальные интерфейсы.

1.5 Использование NAT и PAT

Для того, чтобы дать пользователям доступ в интернет – использовался NAT. NAT используется для маскировки адресов, что зачастую используется при переводе частных адресов в публичные. Это позволяет устройству с частным адресом IPv4 обращаться к ресурсам за пределами его частной сети. NAT в сочетании с частными адресами IPv4 оказался полезным методом сохранения общедоступных IPv4-адресов. Один общедоступный IPv4-адрес может быть использован сотнями, даже тысячами устройств, каждый из которых имеет частный IPv4-адрес. NAT имеет дополнительное преимущество, заключающееся в добавлении степени конфиденциальности и безопасности в сеть, поскольку он скрывает внутренние IPv4-адреса из внешних сетей.

NAT включает в себя четыре типа адресов:

- Внутренний локальный адрес (Inside local address);
- Внутренний глобальный адрес (Inside global address);
- Внешний местный адрес (Outside local address);
- Внешний глобальный адрес (Outside global address);

Модификация NAT – PAT, позволяет транслировать несколько частных адресов на один или несколько публичных. Данная технология используется в большинстве маршрутизаторов, причём как в домашних, так и в коммерческих условиях. Условия трансляции адресов, а точнее транслируемые области, задаются с помощью PAT-листов.

Таким образом, за счёт NAT достигается гибкость сети и минимальное использование адресного пространства.

1.6 Использование контроллера точек доступа

Так как организация условного заказчика является коммерческой, и существует шанс расширения сети – было принято использовать контроллер точек доступа и использовать легковесные точки доступа соответственно.

Контроллер беспроводной сети производит автоматический поиск, централизованную настройку точек доступа, обновление программного обеспечения подключенных точек доступа. WLC может выступать в роли DHCP сервера, для автоматического распределения IP-адресов. Контроллер производит анализ радиочастотного диапазона, регулируя мощность каждой точки доступа, канал, на котором она работает, периодически обновляя данные о состоянии радиоэфира.

Контроллер централизованно авторизует пользователей при подключении к беспроводной сети. Операционная система контроллера управляет всеми беспроводными соединениями, обеспечивает управление ресурсами радио-интерфейсов сети (точками доступа).

В данной курсовой работе контроллер так же играл немаловажную роль в плане настройки бесшовного соединения, авторизации пользователей и разбиения сети на беспроводные локальные сети.

Архитектура сети с центральным контроллером:

- позволяет строить масштабные WiFi сети;
- обеспечивает простоту и удобство администрирования сети, безопасность ее работы.

Легковесная же точка доступа может быть установлена в любом участке сети, подключена к обычному порту доступа ЛВС и при этом предоставлять сервис для нескольких беспроводных сетей (WLAN) одновременно, с разными политиками безопасности: для гостей, для персонала, для технологических устройств. Точка доступа создает туннель (LWAPP, CAPWAP) до контроллера, в котором передает информацию от каждого клиента с меткой идентификатора сети).

1.7 Конфигурирование адресов по SLAAC

Так как всем устройствам необходимо получить IPv6-адрес, то в качестве способа назначения был выбран метод SLAAC. Автоматическая настройка адреса без отслеживания состояния (SLAAC) – это способ получения устройством префикса, длины префикса и адреса шлюза по умолчанию. В основе SLAAC лежит ICMPv6. Данная модель конфигурирования является менее приоритетным, так как данный протокол не позволяет получить адрес DHCP-сервера, который может быть получен лишь путём использования протокола DHCPv6. Однако, так как заказчик в цель поставил IPv6-адресацию в рамках локальной сети – то DHCP сервер нам может быть не так важен, а тем более данный сервер будет найден путём

использования протокола IPv4.

По методу SLAAC узлы конфигурируются по следующим шагам:

1. Узел назначает себе link-local адрес для коммуникации на 3 уровне;
2. Узел выполняет обнаружение дубликатов адресов (DAD), путём отправки сообщения в solicited-группу локальных адресов;
3. Если потенциальный сосед не ответил – то узел считает адрес уникальным и посылает маршрутизатору запрос на получение данного адреса;
4. Узел настраивает свой уникальный адрес и выполняет повторное обнаружение дубликатов;
5. Если дубликат не найден – то узел переходит в активное состояние до момента истечения валидности адреса. Если нет – то пытается выставить адрес заново.

Стоит отметить, что SLAAC так же позволяет работать совместно с DHCPv6, так что при будущем потенциальном расширении сети у сетевого администратора не должно возникнуть трудностей с глобальной IPv6-адресацией.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

Раздел структурного проектирования в контексте данной научно-исследовательской организации представляет собой процесс разработки оптимальной логической инфраструктуры передачи данных, обеспечивающей надежную передачу информации и эффективное взаимодействие между сотрудниками и системами.

Компания использует три этажа по 410 метров квадратных каждый. На данных этажах будут располагаться помещения с различными назначениями: дирекция, учёный совет, административный отдел, исследовательский и производственный отдел, отдел продаж и обслуживания клиентов, бухгалтерия. Данная структура является типовой для научно-исследовательских институтов, поскольку обеспечивает эффективное распределение задач. Так же из данной структуры возможно предположить, что пользовательские станции будут распределены в примерном соотношении:

- 1) Дирекция – 10%;
- 2) Учёный совет – 15%;
- 3) Административный отдел – 10%;
- 4) Исследовательский и производственный отдел – 45%;
- 5) Отдел продаж и обслуживания клиентов, бухгалтерия – 20%.

Для обеспечения доступа выхода в интернет предполагается задействование уже существующего подключения Metro Ethernet. Данное соединение предоставляет скорость до 10 Гбит/с, что является конкурирующей скоростью по сравнению с другими типами подключений, например, GigabitEthernet.

Выход в интернет из данной локальной сети реализован посредством косвенного подключения к Metro Ethernet. Стоит понимать, что прямого подключения к провайдеру нету. Это значит, что между интернетом и локальной сетью есть некая прослойка, недоступная для инженера компьютерной сети, которая в дальнейшем передаёт пакеты в глобальную сеть. Также из этой сети пакеты могут приходить, поэтому блок интернета будет являться как сборщиком информации, так и её провайдером.

Для того чтобы данную информацию маршрутизировать внутри сети и в интернет – используются маршрутизаторы. Данные устройства принимают пакеты и путём использования маршрутной информации направляют их в соответствующие каналы связи.

Чтобы обеспечить взаимодействие локальной сети с интернетом – на границу сети будет поставлен маршрутизатор, который будет выполнять не только цель взаимодействия локальных сетей с интернетом, но также и маршрутизацию между виртуальными локальными сетями. Данный маршрутизатор будет присоединяться к компьютерной сети по принципу «маршрутизатор на палочке» (в оригинале – «router on a stick»). Данный подход характеризуется единственным подключением маршрутизатора к коммутаторам, вместо N подключений маршрутизатора к коммутатору, где N

– количество внутренних разделений внутренних сетей на виртуальные. Так как сеть относительно небольшая – данный подход также поможет сэкономить средства, чтобы не покупать коммутатор третьего уровня.

Таким образом пакеты из интернета будут приходить на маршрутизатор и адресоваться в локальную сеть. В свою же очередь пакеты, которым необходимо выйти за пределы локальной сети будут приходить на маршрутизатор и уходить в интернет за счёт данного соединения. И наконец, пакеты, которым необходимо перейти от одной виртуальной локальной сети в другую виртуальную сеть – будут также приходить на маршрутизатор, обрабатываться и маршрутизироваться. Таким образом, данный блок маршрутизации будет выполнять адресную функцию как внутри сети, так и за пределы сети. Блок маршрутизации было решено поставить на границе сети, чтобы не использовать дополнительных каналов коммутаторов и не усложнять подсеть. Также, так как блок связан с коммутационным узлом, что и позволяет распространяться пакетам по всем виртуальным локальным сетям.

Для взаимодействия пользователей внутри локальных сетей зачастую используют коммутаторы. Они позволяют создавать так называемые виртуальные локальные компьютерные сети. Благодаря большому количеству портов и взаимодействию на другом уровне модели OSI, данные устройства получаются удобными, быстрыми и дешёвыми. В данной компьютерной сети коммутационный узел играет важнейшую роль. Данный узел отвечает за всю передачу пакетов, как из интернета и в интернет, так и между виртуальными сетями. Ключевое соединение данного узла является соединением с устройствами администрирования. Благодаря этому соединению локальную сеть легко администрировать, настраивать и логировать.

Коммутационный блок необходимо подключать ко всем устройствам, так как это позволит распределить виртуальные локальные сети и, соответственно, тегировать весь трафик в один hop, не занимая каналы чужих сетей. Ключевое подключение – подключение к маршрутизатору. Так как данный блок подключён ещё и к блоку стационарных пользователей, и должен как-то взаимодействовать с глобальной сетью – подключение к маршрутизатору должно быть двунаправленным. Соответственно, если пакеты идут за пределы сети – им необходимо получить некую маршрутную информацию, которую должен предоставить маршрутизатор, и прийти обратно к устройствам в виде ответа или же в виде сообщения в другую сеть.

Так как внутри сетей могут возникать перебои или ошибки, вне зависимости от типа сети, её масштаба и сложности, то в каждой компьютерной сети необходим отдел с некими сетевыми администраторами. Сетевые администраторы должны иметь наибольший приоритет в сообщениях и наивысший уровень доступа, так как данные люди считаются квалифицированными специалистами, и могут наравне настраивать, масштабировать и исправлять неисправности компьютерных сетей. Зачастую сетевые администраторы имеют непосредственный доступ ко всему сетевому оборудованию.

В данной сети было решено подключить устройства администрирования сети к коммутационному узлу. Это упростит маршрутизацию данных устройств внутри локальной сети и позволит легко масштабировать их количество. Данные устройства могут настраивать и управлять не только стационарные подключения по типу ПК и серверов, но и беспроводные подключения. Именно поэтому они подключены напрямую к коммутационному узлу, который сможет принимать все административные пакеты. Так же, для этого будет необходимо изолировать административный VLAN. Данный блок было решено не подключать к маршрутизатору из-за плохой масштабируемости системы в будущем и усложнении подключения. Например, если устройств администрирования будет больше, чем 2 – то уже возникнут проблемы, так как обычно на маршрутизаторах располагается примерно 2-3 порта Gigabit или же FastEthernet. Причём необходимо учитывать, что один из портов должен идти на коммутатор, а один – на выход в интернет.

Главная цель создания локальной компьютерной сети – обеспечение взаимодействия между подключёнными абонентами, или же стационарными пользователями. Пользователи могут разбиваться на определённые группы, которые в последующем могут разделяться не только названиями, а также правами доступа, тегированием приоритетом сообщений, т.е. тегированием трафика и другими характеристиками. В данном случае стационарными пользователями будут являться научные сотрудники, бухгалтера и другие сотрудники научно-исследовательского института.

Стационарные пользователи в данной сети отделены от блока устройств администрирования по причинам разного тегирования трафика, уровня доступа и так далее. Данный блок устройств будет представлять собой персональные компьютеры работников научно-исследовательского института. Также подключения пользователей необходимо разграничить от беспроводных подключений, по причине топологической необоснованности данного действия, и от блока стационарных подключений, так как в стационарные подключения входят принтеры и серверы, которые не должны обслуживаться равноправно пользователями.

Пользователи должны быть объединены в некую группу и образовывать локальную сеть. Соответственно, для создания групп используется подключение пользователей к коммутационному узлу. Данное подключение является ключевым в сети, так как оно формирует саму сеть. Подключение должно быть двунаправленным, так как пакеты могут идти как внутрь своей виртуальной локальной сети, так и за её пределы, например в интернет или в другую виртуальную локальную сеть. Также подключение должно быть разграничено с маршрутизатором по причине необходимости работать с другим оборудованием. Так как маршрутизаторы рассчитаны на выдачу информации – они не рассчитаны на подключение множества устройств. Данную проблему решает коммутатор – устройство с множеством подключений, однако без наличия решения задачи адресации.

Кроме подключений обычных проводных пользователей необходимо организовать мобильные подключения, которые будут обеспечивать подключением к сети портативные устройства. Данные подключения являются популярными, так как портативные устройства являются самыми востребованными способами передачи информации на данный момент. Беспроводные подключения также будут являться одной из уязвимостей данной сети, поэтому необходимо приобретать беспроводные точки доступа как минимум с протоколом WPA2.

Блок устройств беспроводного доступа будет подключаться к коммутатору непосредственно. Данный блок не должен обобщаться с блоком стационарных подключений или же с блоком стационарных пользователей, так как данные блоки должны иметь собственный трафик, отделённый и тегами, и соединениями. Блок также не имеет смысла в подключении к маршрутизатору, так как данное подключение будет занимать лишние порты. Беспроводные подключения должны взаимодействовать в дуплексном или полудуплексном режиме, так как пакеты могут браться как из сети интернет, так и из других виртуальных локальных сетей.

Так как на данный момент ни одна компания не обходится без напечатания тех или иных документов – то во всех компаниях сейчас распространены стационарные подключения в виде принтеров. Данные устройства так же входят в состав локальной компьютерной сети, так как покупка и установка одного принтера на одного человека – зачастую невыгодно и неэффективно. Вместо этого часто используется локальное подключение принтера или МФУ, которые могут использоваться несколькими пользователями одновременно. Причём со стороны пользователя – использование офисных устройств с данным подключением отличается только тем, что вместо печати на рабочем месте ставится отдельный блок с офисными устройствами, к которым необходимо подойти и забрать бумаги, отправленные на печать. Зачастую на одну рабочую комнату ставится одно устройство. Так же так как необходимо организовать внутренний NTFS/SMB сервер для файлообмена – то данный блок также необходимо подключить отдельно, не связанно напрямую ни с маршрутизатором, ни с устройствами пользователей, ни с устройствами администрирования, однако все данные блоки должны иметь доступ к серверам.

Для организации данного типа подключения выделяется отдельный блок стационарных устройств. Данный блок также подключается к коммутационному узлу, который будет «раздавать» доступ к данным устройствам всем подключениям от него. Данное подключение должно быть двунаправленным, так как сообщения могут входить как на сервера (в виде файлов, программ и так далее), так и выходить с сервера в локальную сеть (передача данных на компьютеры). На принтеры приходит информация о печати страницы. Однако при отмене печати, малом количестве чернил или другом техническом сбое.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

3.1 Обоснование выбора оборудования для рабочих мест

Под рабочим местом воспринимается пункт, где устанавливается и обслуживается технологическое оборудование, необходимое для выполнения работы.

В рамках данного проекта под рабочим местом воспринимается отдельно выделенная часть площади с персональным компьютером и цветным или же чёрно-белым принтером, как требует заказчик.

3.1.1 Рабочие станции

Основой всех рабочих мест является рабочая станция, которая должна быть надёжным устройством, оборудованной операционной системой и необходимым программным обеспечением. Первое, на что стоит смотреть при выборе станции – наличие соответствующих сетевых адаптеров и характеристики, для выполнения задач предприятия. Так как предприятие является научно-исследовательской организацией, занимающейся металлообработкой (важно не путать с металлургией), следует предположить, что на станциях зачастую придётся использовать САПРы, а также различное требовательное к ресурсам ПО.

Под данные характеристики подходят некоторые офисные компьютеры, например Z-Tech 5-34G-16-120-1000-320-N-190047n [1] или же ASUS D700ME [2]. Данные модели обладают хорошими дискретными видеокартами, соотношением цена/качество, имеют сетевой интерфейс GigabitEthernet, что удовлетворяет всем требованиям. Сравнение данных компьютеров приведены в таблице 3.1.

Таблица 3.1 – Сравнение пользовательских станций

Модель компьютера	D700ME	5-34G-16-120-1000-320-N-190047n
Цена	4 373.27 р.	2701.60 р.
Дата выхода на рынок	2022	2020
Модель процессора	Intel Core i5-10400	AMD Ryzen 5 3400 G
Количество ядер	6	4
Тип и объём оперативной памяти	DDR4, 16 ГБ	DDR4, 16 ГБ
Видеокарта и объём видеопамяти	NVIDIA GeForce RTX 3060, 12 ГБ	NVIDIA GeForce GTX 1660 Ti, 6 ГБ
Конфигурация накопителя	SSD 512 ГБ	HDD 1000 ГБ + SSD 120 ГБ
Порты LAN	1 Gigabit Ethernet	1 Gigabit Ethernet

В данном сравнении компьютер от компании Z-Tech проигрывает по характеристикам видеокарты, а также по процессору и дате выхода на рынок. Несмотря на то, что компьютер от компании Z-Tech выигрывает по конфигурации накопителя и цене, было принято выбрать компьютеры ASUS D700ME, так как у предприятия будет иметься внутренний файловый сервер, а также предприятие является полностью коммерческим проектом, что даёт нам больше воли распоряжения деньгами.

Так же, так как заказчик требует усиленную безопасность в отношении учётных записей пользователей – то каждый ПК будет снабжён счётчиком отпечатка пальца, который будет использоваться при аутентификации пользователя.

3.1.2 Принтеры

По требованию заказчика для данной научно-исследовательской организации необходимо выбрать и купить чёрно-белые, а также цветные принтеры. Так как данное предприятие занимается научной деятельностью, следует предположить, что необходимо использовать высокоточные принтеры, с поддержкой печати графического материала. Также немаловажными характеристиками будут являться: скорость печати, технология (лазерная/струйная), производительность (поддерживаемый объём страниц в месяц). Сравнение чёрно-белых принтеров приведены в таблице 3.2, а сравнение цветных – в 3.3.

Таблица 3.2 – Сравнение характеристик чёрно-белых принтеров

Модель принтера	Kyocera ECOSYS P4060dn	Kyocera ECOSYS P4060dn	Kyocera ECOSYS P3145DN
Цена	22 874.16 р.	1349 р.	2050 р.
Объём оперативной памяти	4 096 Мб	256 Мб	512 Мб
Максимальная скорость печати	60 стр./мин.	35 стр./мин.	45 стр./мин.
Максимальная месячная нагрузка	16000 стр.	20000 стр.	150000 стр.
Максимальное разрешение печати	1200x1200 dpi	1200x1200 dpi	1200x1200 dpi
Формат печати	A3	A4	A4

Исходя из данной таблицы можно предположить, что принтер KYOCERA ECOSYS P3145DN является наилучшим для полноценного коммерческого проекта. Принтер Kyocera ECOSYS P4060dn является чрезмерно дорогим, и в нём нет таковых потребностей. Принтер Kyocera

ECOSYS P4060dn просто проигрывает по характеристикам.

Таблица 3.3 – Сравнение характеристик цветных принтеров

Модель принтера	Epson L1300	Kyocera ECOSYS P5026cdn	HP Color Laser
Цена	2083.62 р.	1863 р.	1399 р.
Технология	Струйная	Лазерная	Лазерная
Объём оперативной памяти	Нет данных	512 Мб	128 Мб
Максимальная скорость печати	32 стр./мин.	26 стр./мин.	18 стр./мин.
Максимальная месячная нагрузка	2500 стр.	50000 стр.	20000 стр.
Максимальное разрешение печати	5760x1440 dpi	1200x1200 dpi	600x600 dpi
Максимальный формат печати	A3	A4	A4

Так как заказчику может быть важно разрешение и формат печати – стоит выбрать принтер Epson L1300. Данный принтер обладает большим разрешением печати при относительно небольшой цене в отличие от конкурирующих принтеров. Также данный принтер лидирует в скорости печати, а месячной нагрузкой можно нивелировать.

3.2 Настройка оконечных устройств

Под настройкой оконечных устройств понимается настройка пользовательских станций, принтеров и цветных принтеров. Данная процедура выполняется с каждым новым подключаемым устройством.

3.2.1 Настройка пользовательских станций

Настройка персональных компьютеров происходит в два шага:

1) Настройка параметров адаптеров:

Персональные компьютеры подключаются посредством Ethernet. Чтобы настроить ПК, необходимо зайти в панель управления, выбрать «Network and Sharing Center», далее «Change adapter settings». После выбора необходимого адаптера и захода в его настройки, необходимо выбрать пункт «Internet Protocol Version 4 TCP/IPv4» и в нём выставить пункт «Obtain IP address automatically». В поле «DNS» следует так же выставить «Obtain DNS server address automatically» Так как в локальной сети IPv4 и IPv6 пулы настроены на коммутаторе и маршрутизаторе – то прописывать IP-адреса, как и DNS-сервер

вручную не требуется. После данных настроек компьютер перезагрузится, и пользователь будет сконфигурирован с ПК администратора.

Полный список действий представлен на рисунках 3.1 – 3.5

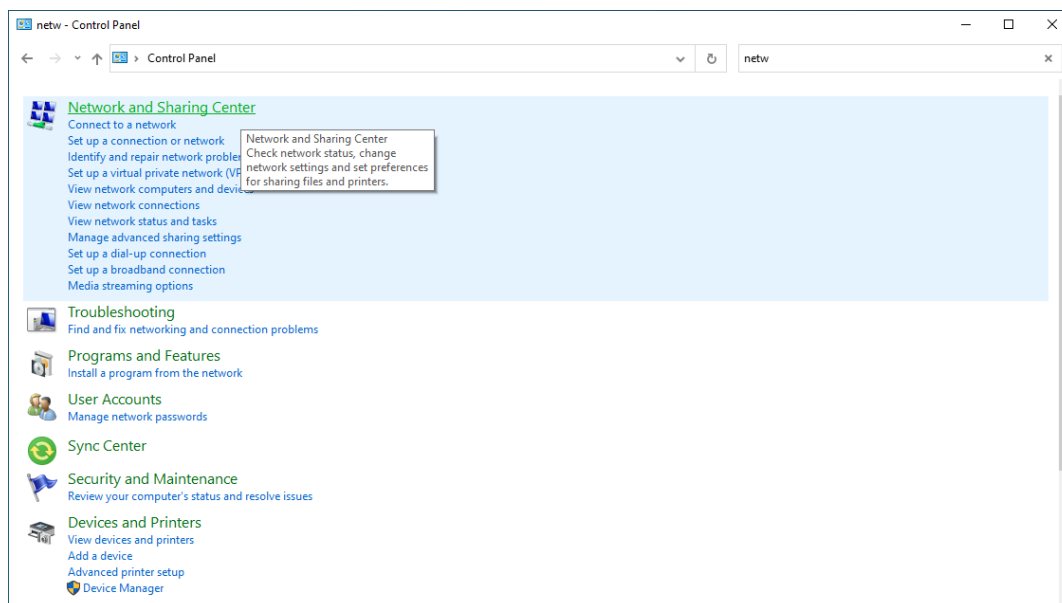


Рисунок 3.1 – выбор «Network Sharing Center»

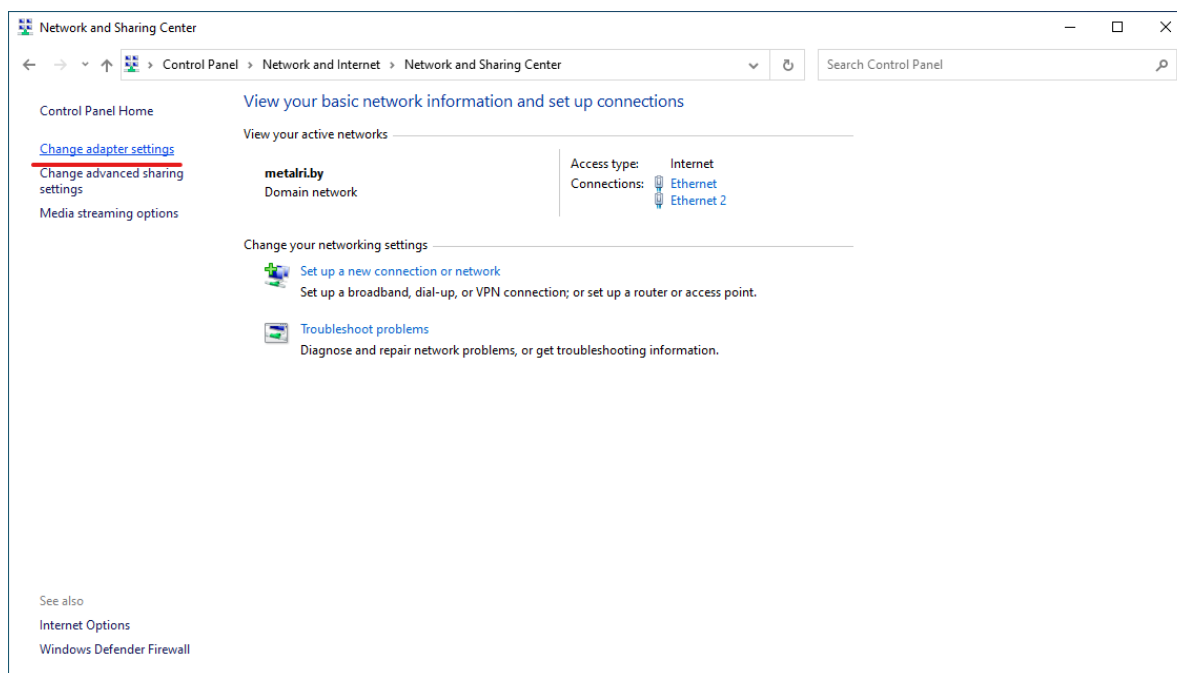


Рисунок 3.2 – выбор «Change adapter setting»

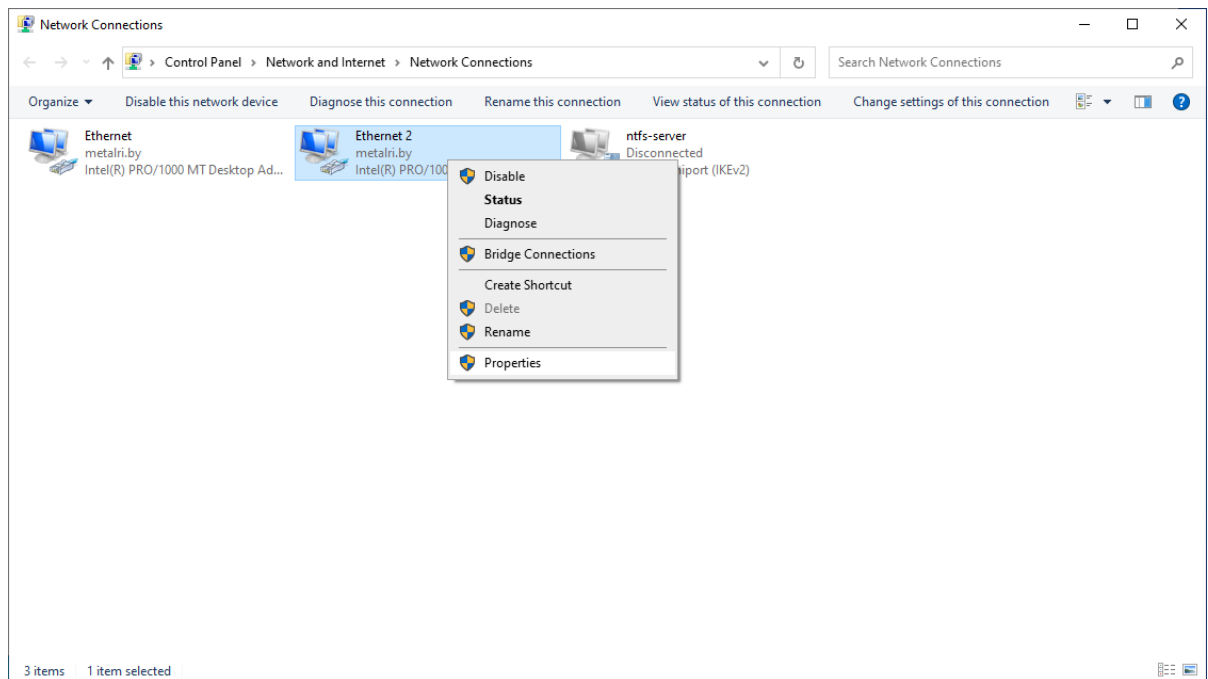


Рисунок 3.3 – выбор соответствующего адаптера и его настроек

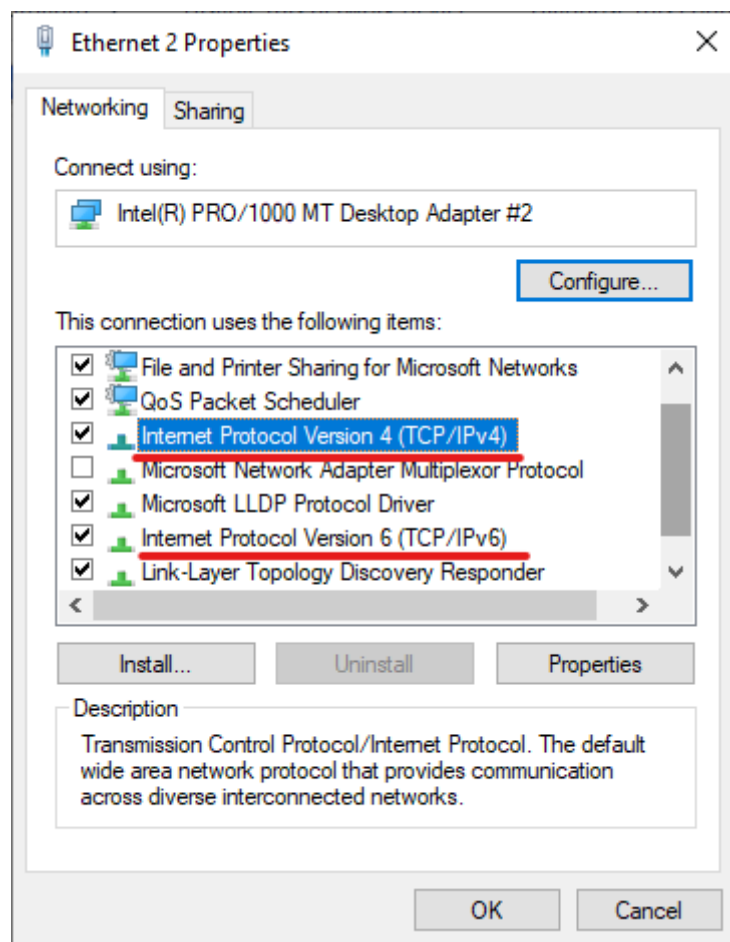


Рисунок 3.4 – выбор настроек IPv4 и IPv6

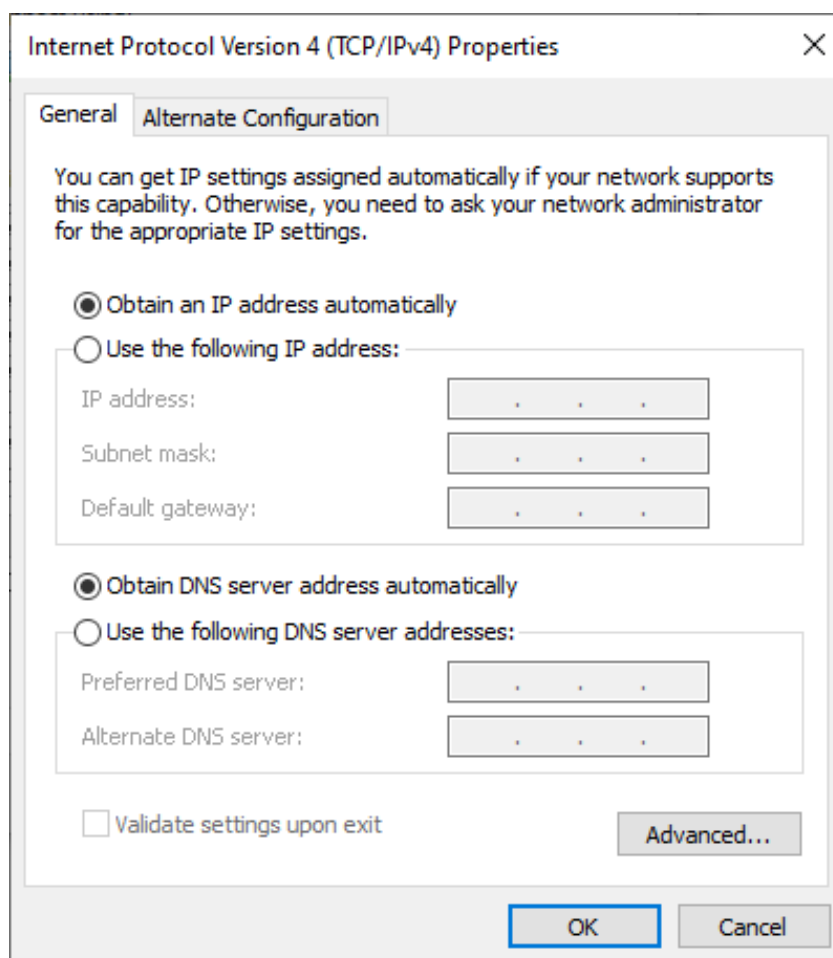


Рисунок 3.5 – Настройка IPv4

После перезагрузки или же выхода и входа в учётную запись, данный пользователь будет иметь доступ к разделяемым ресурсам данной ЛКС.

2) Настройка усиленной безопасности в отношении учётных записей:

Для обеспечения усиленной безопасности в отношении учётных записей пользователей было принято использовать два решения:

- Пользователь должен менять пароль после каждого входа в учётную запись (рисунок 3.6);
- Настройка опции «Log on hours» в соответствии со временем работы компании (рисунок 3.7);

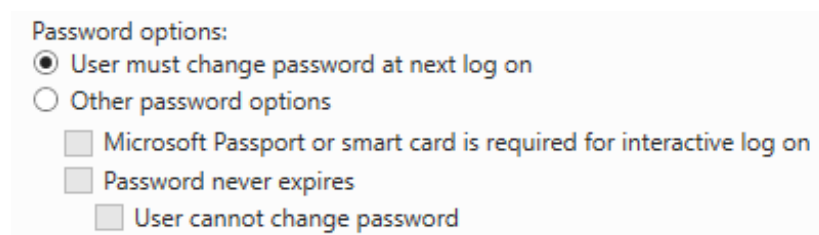


Рисунок 3.6 – Настройка повторного изменения пароля

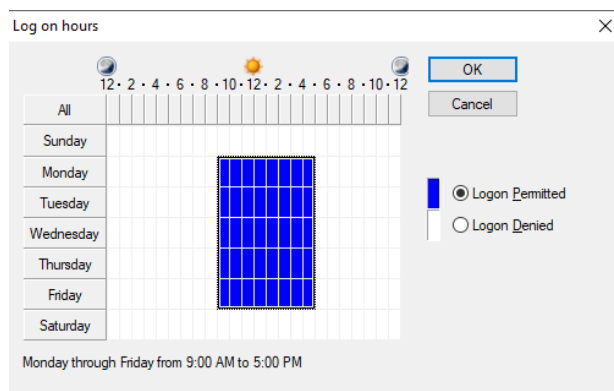


Рисунок 3.7 – Настройка опции «Log on hours»

- Будет использоваться приложение «miniOrange» для двухфакторной аутентификации.

После настройки пункта часов входа в систему следует отключить пользователей от всех сетевых ресурсов по истечении их рабочего времени, выбрав «Политики» в строке меню «Диспетчер пользователей для доменов», выбрав «Учетная запись», а затем выбрав «Принудительное отключение удаленных пользователей от сервера по истечении времени входа в систему» в нижней части диалогового окна «Политика учетной записи».

Для использования приложения miniOrange необходимо зайти на официальный сайт, создать аккаунт администратора один раз. Далее необходимо добавить новый тип авторизации в разделе «apps» (рисунок 3.2.6). Далее необходимо добавить тип «Desktop», «Windows», задать имя аутентификации, имя политики и группы, тип входа и выставить «Two Factor Authentication» (рисунок 3.2.7). Далее в разделе «2FA options for EndUsers» необходимо выставить метод аутентификации для пользователей (рисунок 3.2.8).

На стороне пользователя необходимо загрузить приложение аутентификации с официального сайте [3]. После входа в приложение во вкладке «Plugin Selection» необходимо включить пункт «miniOrange». При этом высветиться окно, в котором необходимо ввести «Customer Key» и «API Key», которые даны в настройках на стороне администратора. Делается данная процедура один раз для каждого пользователя (рисунки 3.8 – 3.13).

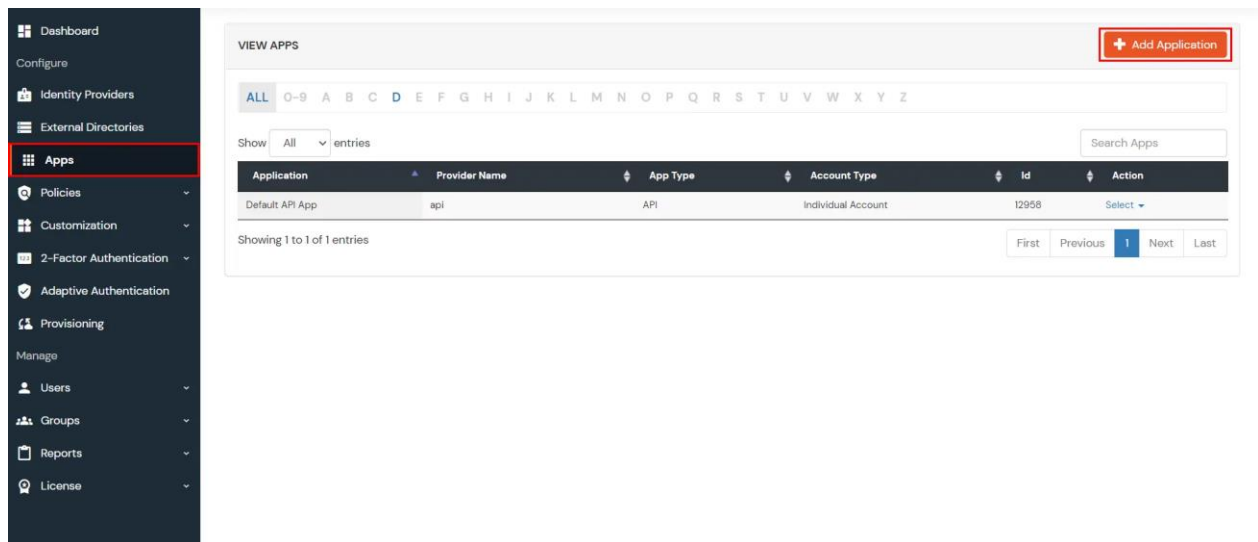


Рисунок 3.8 – Добавление нового типа авторизации

ADD POLICY

*Group Name :

*Policy Name :

*Login Method :

☒ Enable 2-Factor Authentication (MFA)

☐ Enable Adaptive Authentication

(Enable this option if you want to restrict app access based on IP, Device, Time and Location.)

Рисунок 3.9 – Добавление способа входа

SELECT DEFAULT AUTHENTICATION METHOD

☒ OTP OVER SMS ☐ OTP OVER EMAIL

☐ DISPLAY HARDWARE TOKEN ☐ SMS LINK

☐ EMAIL LINK ☐ OTP OVER SMS AND EMAIL

SELECT ALLOWED 2FA METHODS

☒ OTP OVER SMS ☒ PUSH NOTIFICATIONS

☒ SOFT TOKEN ☒ GOOGLE AUTHENTICATOR

☒ MICROSOFT AUTHENTICATOR ☒ AUTHY AUTHENTICATOR

☒ OTP OVER EMAIL ☒ YUBIKEY HARDWARE TOKEN

☐ DISPLAY HARDWARE TOKEN ☒ SMS LINK

☐ EMAIL LINK ☒ SECURITY QUESTIONS

☒ QR CODE AUTHENTICATION ☒ OTP OVER SMS AND EMAIL

☐ CALL ME

Рисунок 3.10 – Выбор метода двухфакторной аутентификации

Product Global Settings

Account Details [🔗](#)

You will need the following information to call our APIs:

Customer Key	123456
Customer API Key	1ABCD234EFGHI567
Customer Token Key	1234ABCD5678EFGH



Рисунок 3.11 – Customer Key и API Key со стороны администратора

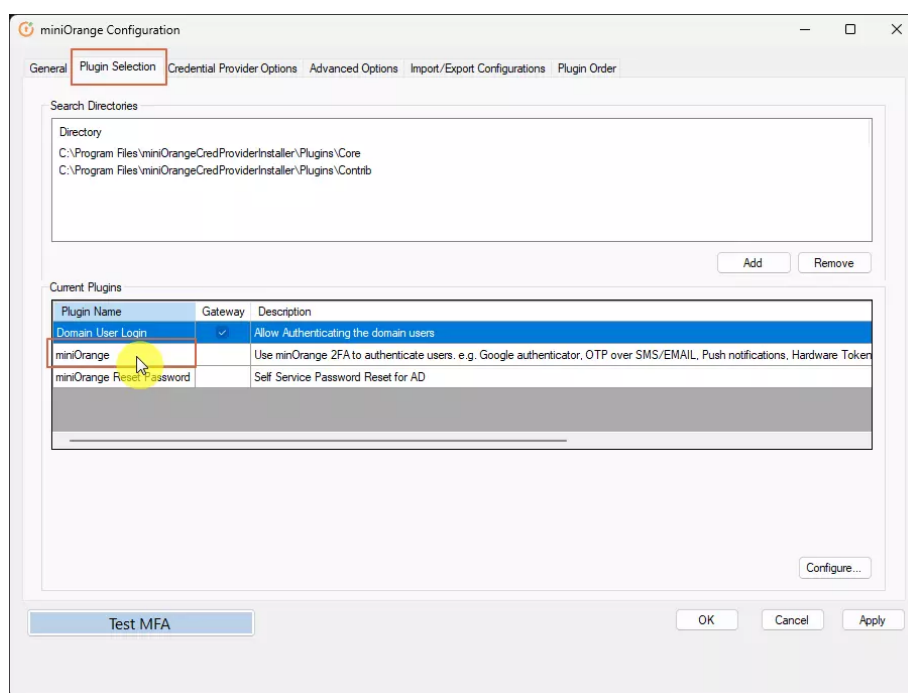


Рисунок 3.12 – Включение плагина двухфакторной аутентификации

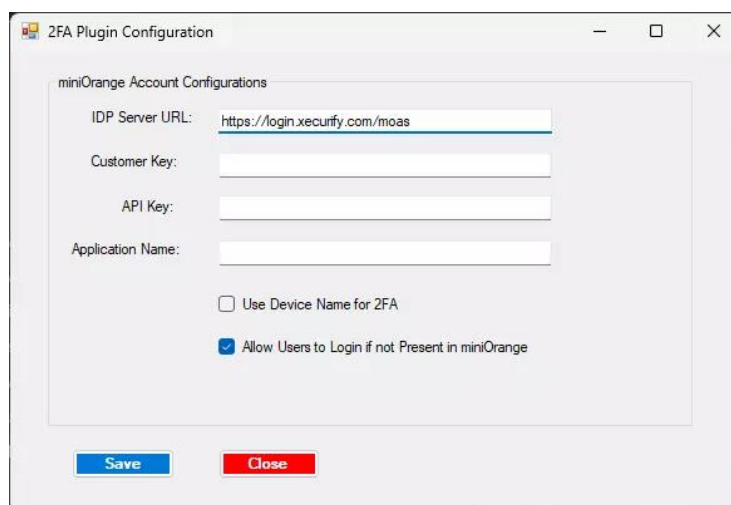


Рисунок 3.13 – Меню ввода Customer key и API key.

После данной настройки и нажатия кнопки «Save» в пункте «Credential Provider Options» необходимо выбрать пункт «Force miniOrange 2FA on Logon».

Таким образом после включения персонального компьютера пользователь будет видеть меню аутентификации (рисунок 3.14). При этом привязывая своё приложение от Google Authenticator или Push Notification.

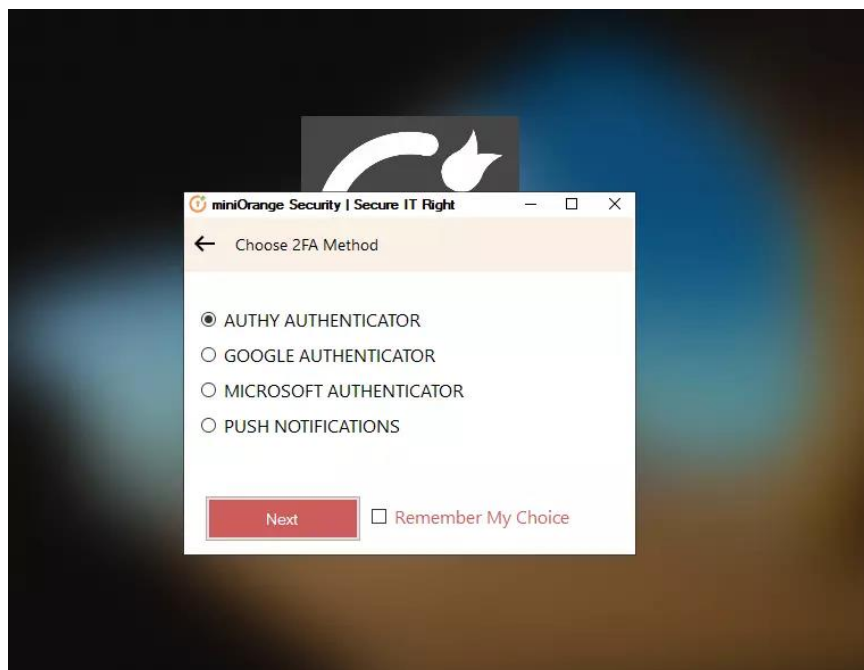


Рисунок 3.14 – Меню входа пользователя.

Последний пункт настройки безопасности – настройка приложения NCheck Bio Attendance, которое позволит настроить дополнительную аутентификацию в виде приложения, блокирующего доступ к ПК до тех пор, пока не будет выполнена биометрическая аутентификация. Так как для биометрии были выбраны сканеры отпечатков пальцев – то рекомендуется использовать их, однако благодаря гибкости приложения можно купить другое оборудование, к примеру веб-камеры, и использовать аутентификацию по лицу.

Весь процесс настройки данного приложения описан на официальном сайте данного приложения [4], так что следует лишь описать основные шаги:

На стороне сервера необходимо:

1. Установить приложение по вышеуказанной ссылке с официального сайта в разделе «Server»;
2. Выбрать пароль для суперпользователя (менеджера), пароль, порт, который будет служить для передачи сообщений.
3. Зайти в меню «конфигурация» и запустить NCheck Bio сервер;

На стороне клиента:

1. Установить приложение по вышеуказанной ссылке с официального сайта в разделе «Client», подраздел «Install Client»;

2. В установленном приложении нажать кнопку «Search Server» и подключиться к серверу;

3. Ввести пароль менеджера (только в первый раз) и сконфигурировать тип биометрии (в данном случае выбрать «Fingerprint», «External Scanner»).

Таким образом, после вхождения в систему путём двухфакторной аутентификации экран пользователя будет блокироваться, и будет ожидаться подтверждение путём сканирования отпечатка пальца.

3.2.3 Настройка принтеров

Для настройки принтеров требуется подключить принтер к пользовательской станции и включить принтер в сеть. Для настройки чёрно-белых принтеров от компании Kyocera следует загрузить с официального сайта Kyocera [5] универсальный драйвер, запустить его и нажать «Express Install». После автоматического поиска принтера и его выбора следует нажать «Install».

Для настройки цветных принтеров от Epson требуется загрузить драйвер с официального сайта Epson [6]. После скачивания и запуска драйверов следует нажать «Ok», после чего драйверы будут установлены на пользовательскую станцию.

3.3 Обоснование выбора активного сетевого оборудования

Активным сетевым оборудованием можно считать оборудование, участвующее в обработке и передаче данных в компьютерных сетях. К данному оборудованию относятся маршрутизаторы, коммутаторы, мосты, сетевые серверы и другие устройства, управляющее трафиком и принимающие решения о маршрутизации данных и усиливающие сигнал для передачи по сети.

Из параметров, предоставленными заказчиком, следует выделить самые главные, коими являются:

- 1) Сеть имеет небольшой масштаб. Как минимум от 10 стационарных подключений и 20 подключений для мобильных устройств;
- 2) Подключение к Internet происходит за счёт Metro Ethernet;
- 3) Необходима поддержка VLAN;
- 4) Необходим файловый NTFS/SMB сервер для внутреннего использования;

Исходя из этих требований и будет подбираться сетевое оборудование.

Полный список используемого оборудования будет предоставлен в приложении «Е».

3.3.1 Маршрутизатор

Маршрутизатор – это сетевое устройство, выполняющее функцию

переадресации приходящих на него пакетов в соответствии с маршрутной информацией. Данное устройство, стоит на границе сетей и передаёт информацию между ними. В дополнение к связи различных сетей, маршрутизатор будет выполнять функцию адресации между виртуальными локальными сетями.

В данной компьютерной сети выбор стоял между двумя маршрутизаторами: Cisco ISR4431/K9 или же Cisco ISR4221/K9. Сравнение данных маршрутизаторов приведено в таблице 3.4.

Таблица 3.4 – Сравнение маршрутизаторов

Модель	Cisco ISR4331	Cisco ISR 4221
Поддержка телефонии и видео	До 100, 360	Отсутствует
Беспроводной модуль LAN-контроллера	Поддерживается	Отсутствует
Поддержка PoE	До 250 Ватт	Отсутствует
Суммарная пропускная способность	До 300 Мбит/с	До 75 Мбит/с
Максимальный объём памяти DDR3	До 16 ГБ	До 4 ГБ
Максимальный объём флеш-памяти	До 16 ГБ	До 8 ГБ
Цена	9312.24 р.	3959.59 р.

Исходя из данного сравнения, логично выбрать маршрутизатор Cisco ISR4331. Данный маршрутизатор обладает рядом преимуществ, таких как большая пропускная способность, объём памяти и поддержка PoE. Далее про конкретные характеристики маршрутизатора [7].

Cisco ISR4431/K9 – это один из маршрутизаторов серии Cisco Integrated Services Router и имеет ряд характеристик, которые делают его хорошим выбором в корпоративных и бизнес-средах. Данный маршрутизатор обладает рядом преимуществ, таких как: наличием 4 RJ-45 Gigabit портов и 4 small form-factor pluggable Gigabit портов, поддержкой PoE, наличием ещё 3 свободных NIM-слотов. Данный маршрутизатор может служить в качестве DHCP-сервера, а также имеет встроенную поддержку NAT.

3.3.2 Коммутатор

Коммутаторы являются базовыми составляющими компьютерных сетей и служат для соединения устройств сети, таких как компьютеры, принтеры, сервера, маршрутизаторы и так далее, между собой.

В данной сети коммутатор служит связующим звеном, позволяющим устройствам обмениваться друг с другом информацией. Общее сравнение

информации приведено в таблице 3.5.

Таблица 3.5 – Сравнение коммутаторов

Модель	Cisco SB SG350-52-K9	Cisco SB SG350-48-K9	Cisco C1000-48T-4G-L
Цена	3796.45 р.	2129.11 р.	8876.00 р.
Уровень (Layer)	2+	2+	2
Порты доступа	Gigabit Ethernet, SFP	Fast Ethernet, SFP	Gigabit Ethernet, SFP
Количество портов доступа	48 GE + 2 Gigabit combo + 2 SFP	48 Fe + 2 GE + 2 SFP	48 GE + 4 SFP
Коммутационная матрица	56 Гбит/с	17.6 Гбит/с	104 Гбит/с
Внутренняя пропускная способность	77.38 милл. пакет. / с	13.09 милл. пакет. / с.	77.38 милл. пакет. / с.
Таблица MAC-адресов	16384 адресов	16384 адресов	16000 адресов
Буфер памяти пакетов	3 МБ	3 МБ	1.5 МБ

По полученным данным следует сделать вывод, что коммутатор Cisco SB SG350-52-K9 является наиболее подходящим под данную задачу. Данные о всех коммутаторах взяты с официального сайта Cisco [8]

Коммутатор Cisco SB SG350-52 обладает рядом преимуществ, таких как:

1. Высокая внутренняя пропускная способность;
2. Высокая коммутационная матрица;
3. Уровень управления – 2+;
4. Относительно низкая цена, по сравнению с другими коммутаторами;
5. В дополнение ко всему – присутствует Web-интерфейс управления.

Данные характеристики позволяют предположить, что данный коммутатор является хорошим выбором для данной компании, так как обеспечивает необходимую работоспособность и масштабируемость сети.

3.3.3 Файловый сервер

Файловый сервер – это оконечное устройство, предназначенное для хранения и обмена файлами в компьютерной сети. Он обеспечивает централизованное хранилище данных и совместный доступ к файлам для пользователей, подключенным к сети. Для сравнения были выбраны сервера Dell EMC PowerEdge R450 [9] и Lenovo ThinkSystem SR630 V2 [10].

Таблица 3.6 – Сравнение серверов

Модель	Dell EMC PowerEdge R450	Lenovo ThinkSystem SR630 V2
Цена	26000 р.	10633 р.
Максимальная оперативная память	1 ТБ	8 ТБ
Поддержка RAID SAS/SATA	SAS/SATA с поддержкой RAID 0/1/5/10/50	SATA с поддержкой RAID 0/1/10/5/50/6/60
Сетевые интерфейсы	2 x GE	4 x GE
Объём внутреннего хранилища	до 488.8 ТБ	до 368.64 ТБ
Форм-фактор дисков	4 x 3.5" или же 8 x 2.5" SAS/SATA HDD/SSD	4 x 3.5" или же 8 x 2.5" SATA/SAS HDD/SSD

Так как сервер от Dell проигрывает по важным характеристикам, таким как максимальный объём оперативной памяти и цена – было решено выбрать сервер от Lenovo. Так же немаловажным фактором стала доступность данного сервера. Подробнее о сервере:

Сервер от компании Lenovo предоставляет поддержку RAID, двух или более процессоров, 32 разъёмов для DDR4 RDIMM, порты для USB и большое количество поддерживаемых операционных систем, в том числе и Microsoft Windows Server с Hyper-V.

Так как сервер обладает удовлетворительными характеристиками, в последующем его можно будет использовать как сервер для управления групповыми политиками и учётными записями пользователей.

В качестве жестких дисков под файловый сервер были выбраны Fujitsu Eternus DX S2 SAS 900GB 10K 2,5, так как данные диски подключаются по SAS-интерфейсу, что является лучшим подключением нежели SATA. Так же данные жёсткие диски обладают большим количеством перезаписей, ёмкостью и скоростью передачи данных.

3.3.4 Беспроводные точки доступа

Беспроводная точка доступа используется для интеграции беспроводных и традиционных проводных сегментов сети. В настоящее время точки доступа – это мосты, которые являются беспроводными маршрутизаторами.

Таблица 3.7 – Сравнение беспроводных точек доступа

Модель	Cisco AIR-AP1815I-E-K9	Cisco AIR-AP1852I-E-K9	Cisco C9115AXI-I
1	2	3	4

Продолжение таблицы 3.7 – Сравнение беспроводных точек доступа

1	2	3	4
Цена	2534.79 р.	3105.81 р.	8 943.48 р.
Поддерживаемые стандарты	802.11a/b/g/n/ac	802.11a/b/g/n/ac	До 802.11ax
Максимальная скорость передачи данных	1 Гб/с	2 Гб/с	3.4 Гб/с
Поддержка Ethernet-подключения	До 3 GE	1 x GE	1 x Multi-Gig E
USB-порт	-	1	1
Опция питания	AC/DC или PoE	AC/DC или PoE+	PoE или Cisco UPoE+

Из данной таблицы можно предположить, что точка Cisco AIR-AP1852I-E-K9 [11] является наилучшим сочетанием цена/качество. Точка Cisco C9115AXI-I [12] обладает немного лучшими характеристиками в плане Ethernet-подключения и максимальной скорости передачи, однако данная точка дороже почти в три раза, соответственно, её выбор будет необоснованным.

AIR-AP1852I-E-K9 – точка доступа от компании Cisco, которая поддерживает проводное Gigabit-соединение, и так же беспроводное подключение 802.11ac. Так же точка имеет Console-порт, через который можно настраивать конфигурацию, поддержку PoE+, протокол WPA2, и выбранный контроллер точек доступа.

3.3.5 Контроллер точек доступа

Контроллер точек доступа является централизованным устройством для настройки и администрирования точками доступа. Благодаря контроллеру возможно реализовать бесшовное подключение к Wi-Fi и настроить аутентификацию для подключения к сети.

Таблица 3.8 – Сравнение контроллеров точек доступа

Модель	Cisco AIR-CT2504-15-K9	Cisco AIR-CT3504-K9
1	2	3
Цена	3308.58 р.	33217.44 р.
Количество поддерживаемых точек доступа	До 15	До 150

Продолжение таблицы 3.8 – Сравнение контроллеров точек доступа

1	2	3
Количество поддерживаемых клиентов	До 1000	До 3000
Максимальная пропускная способность	1 Гб/с	3 Гб/с
Поддержка стандартов Wi-Fi	До 802.11ac	До 802.11ac

Из данного сравнения можно сделать вывод, что характеристики контроллера точек доступа Cisco AIR-CT2504-15-K9 [13] хуже, однако так как цена данного контроллера в 10 раз ниже, и, по требованию заказчика, количество поддерживаемых клиентов покрывается в разы, было принято выбрать данный контроллер. Так же данный контроллер поддерживает до 16 виртуальный ЛКС и имеет консольный порт для настройки и администрирования.

Стоит дополнить, что точки доступа могли бы быть выбраны от дочерней компании Cisco – Cisco Meraki, однако данные точки доступа были отключены 21 декабря 2022 года и их использование не является возможным.

3.4 Обоснование выбора пассивного сетевого оборудования

Пассивное сетевое оборудование отличается от активного тем, что не получает питания непосредственно от электросети и передаёт сигнал без его изменения или усиления. Таким оборудованием являются кабеля, информационные розетки, телекоммуникационные шкафы и так далее.

3.4.1 Телекоммуникационный шкаф

Телекоммуникационный шкаф является местом расположения всего активного сетевого оборудования, которому необходимо соответствующее крепление. Подбираться телекоммуникационный шкаф должен по количеству необходимых креплений. Количество необходимых креплений приведено в таблице 3.9.

Таблица 3.9 – Количество необходимых креплений

Оборудование	Необходимое количество крепёжных единиц (RU – rack shelf)
1	2
Cisco ISR4431/K9	1
Cisco SB SF350-28-K9	1

Продолжение таблицы 3.9 – Количество необходимых креплений

1	2
Lenovo ThinkSystem SR630 V2	1
Cisco AIR-CT2504-15-K9	1
Всего	4

В итоге нужен шкаф, который будет иметь вместимость минимум 4RU. Таковым является шкаф SYSMATRIX MR 6812.933. Шкаф имеет 12 креплений, что является достаточным. К тому же, шкаф является напольным, что при общем весе примерно в 50 кг без источника бесперебойного питания и батарей может являться слабой стороной настенных шкафов. Данный шкаф позволяет разместить всё необходимое оборудование и, при надобности, расширить сеть.

3.5 Обоснование выбора серверного ПО

Так как по условиям заказчика необходимо реализовать поддержку файлового NTFS/SMB сервера для внутреннего использования, то было принято решение использовать отдельный физический сервер, с возможным расширением в будущем.

В качестве операционной системы была выбрана Windows Server 2022 Standard с категорией Desktop Experience для настройки и администрирования, как файлового сервера, так и пользовательских групп. Windows Server была взята 2022 года, так как эта в данной версии сделали упор на улучшении SMB [14]. Так же на данный момент это является новейшей версией Windows Server.

В качестве ресурса управления NTFS-сервером было принято использовать уже существующую на данной ОС утилиту: «Server Manager», в которой можно легко создавать и настраивать разделяемые пространства.

Так же это позволяет нам использовать утилиту «Active Directory», которая позволяет настраивать групповые политики в отношении пользователей.

3.6 Настройка активного сетевого оборудования

3.6.1 Настройка NTFS/SMB сервера.

После загрузки сервера необходимо сконфигурировать его сетевой интерфейс, подобно пользовательскому. В качестве шлюза по умолчанию назначить IP маршрутизатора, а в качестве IP назначить адрес из виртуальной ЛКС, назначенной под сервера. Так как это делается аналогично пользовательскому оборудованию – то приводить подробное описание этому не требуется. Дополнительные изображения конфигурации файлового сервера представлены в приложении «З».

После конфигурации интерфейса необходимо создать сервер. Для этого необходимо:

- 1) Нажать «Manage» в верхнем правом углу и выбрать «Add Roles and Features»;
- 2) Нажать «Next», перейти на «Server Roles»;
- 3) В «Server Roles» выбрать «File and storage Services», «File Server» (рисунок 3.6.2). Нажать «Next»;
- 4) Выбрать «SMB File Sharing Support». Нажать «Next»;
- 5) Подтвердить.

После данного этапа необходимо провести настройку группы пользователей. Для этого:

- 1) Переходим в «Tools», «Active Directory Users and Computers», «Groups».
- 2) Добавляем новую группу. Назначаем имя.
- 3) Переходим во вкладку «Users». Создаём нового пользователя по такому же алгоритму. Назначаем компьютеру пользователя, а пользователю – группу.

Теперь надо создать и сконфигурировать разделяемое пространство. Переходим во вкладку «File and Storage Servers» в «Server Manager».

Выбираем новое пространство, локацию и имя разделяемого пространства. Далее – конфигурируем разрешения (рисунок 3.6.6). Добавляем ранее созданную группу пользователей и конфигурируем сначала её разрешения на другие папки, созданные не этой пользовательской группой, далее её политику разделения пространства.

После этого наш сервер готов к работе и политики настроены.

Со стороны клиента можно проверить работоспособность:

- 1) Создать файл с компьютера администратора.
- 2) Создать файл с пользователя клиента.
- 3) С компьютера пользователя попытаться модифицировать/удалить файл, созданный с компьютера администратора.
- 4) С компьютера администратора попытаться модифицировать/удалить файл, созданный пользователем.

Если групповые права на разделяемые пространства сконфигурированы верно – то пользователь не сможет ни удалить, ни модифицировать файл, созданный администратором. Администратор же, в свою очередь, сможет и удалять, и модифицировать файлы, созданные пользователем.

3.7 Разделение сети на внутренние виртуальные подсети

Данную компьютерную сеть было решено разделить на некоторое количество виртуальных локальных сетей с целью оптимизации трафика, увеличения общей производительности, а также повышения безопасности сети.

Данную подсеть было решено разделить на X виртуальных ЛКС:

1) VLAN 10 – дирекция, учёный совет. В него будут входить 4 персональных компьютера, 1 на дирекцию и 3 на учёный совет;

2) VLAN 11 – исследовательский и производственный отдел. В него входит 7 персональных компьютеров;

3) VLAN 12 – бухгалтерия и отдел продаж и обслуживания клиентов. В него входит 3 персональных компьютеров, 2 на отдел продаж и обслуживания клиентов, 1 на бухгалтерию;

4) VLAN 13 – гостевые мобильные подключения.

5) VLAN 20 – административный отдел (административный VLAN). На данный момент в него входит 1 персональный компьютер, с возможностью конфигурирования сервера, а также контроллер точек доступа;

6) VLAN 30 – многофункциональный сервер.

В конечном итоге, в сети будет 15 стационарных пользователей.

Маршрутизация между виртуальными сетями будет осуществляться за счёт маршрутизатора, подключенного по принципу router on a stick, так как под заданное количество виртуальных ЛКС маршрутизация Cisco IVR не подходит, в связи с большим количеством VLAN-ов.

3.8 Составление таблицы адресации в ЛКС

Так как внутренняя подсеть является приватной, то и адреса стоит брать из приватного пула IPv4. Из-за того, что приватных адресов в варианте из лабораторных работ нет, используем ближайшие к ним.

IPv6 адресация в рамках внутренней сети, значит следует использовать уникальные локальные IPv6-адреса, с префиксом FD00::/7 [15]. В качестве длины префикса будет использоваться значение 64, а в качестве постфикса – преобразованный MAC-адрес в нотации EUI-64. Для упрощения получения IPv6-адресов на оконечных устройствах будет использоваться принцип SLAAC, а не DHCPv6. При данном методе устройство будет получать адрес от маршрутизатора, который периодически будет отправлять ICMPv6 сообщения всем устройствам, под управлением IPv6. Так как адрес DNS-сервера будет сконфигурирован на IPv4 – то на IPv6 данная конфигурация будет необязательной.

Сопоставления устройств, виртуальных ЛКС, адресов и масок показаны в таблице 3.10

Таблица 3.10 – Адресация в локальной сети

Устройство	VLAN	IP-адрес	Маска подсети
1	2	3	4
Рабочие станции дирекции и учёного совета	10	192.168.0.11 ... 192.168.0.14 FD::10:EUI-64	255.255.255.0 /64

Продолжение таблицы 3.10 – Адресация в локальной сети

1	2	3	4
DHCP-пул мобильных подключений для дирекции и ученого совета	10	192.168.0.40 ... 192.168.0.50 FD::10:EUI-64	255.255.255.0 /64
WLAN-интерфейс WLC		192.168.0.4	255.255.255.0
Рабочие станции исследовательского и производственного отдела	11	192.168.1.11 ... 192.168.1.17 FD::11:EUI-64	255.255.255.0 /64
DHCP-пул мобильных подключений для исследовательского и производственного отдела		192.168.1.40 ... 192.168.1.50 FD::11:EUI-64	255.255.255.0 /64
WLAN-интерфейс WLC		192.168.1.4	255.255.255.0
Рабочие станции бухгалтерии и отдела продаж и обслуживания		192.168.2.10 ... 192.168.2.12 FD::12:EUI-64	255.255.255.0 /64
DHCP-пул мобильных подключений для бухгалтерии и отдела продаж и обслуживания	12	192.168.2.40 ... 192.168.2.50 FD::12:EUI-64	255.255.255.0 /64
WLAN-интерфейс WLC		192.168.2.4	255.255.255.0
DHCP-пул гостевых мобильных подключений	13	192.168.3.40 ... 192.168.3.50 FD::13:EUI-64	255.255.255.0 /64
WLAN-интерфейс WLC		192.168.3.4	255.255.255.0
Административный отдел	20	192.168.20.10 FD::20:EUI-64	255.255.255.0 /64
Контроллер точек доступа		192.168.20.50	255.255.255.0
DHCP-пул для точек доступа		192.168.20.50 ... 192.168.20.60	255.255.255.0
Многофункциональный сервер	30	192.168.30.10 FD::30:EUI-64	255.255.255.0 /64

3.9 Описание и настройка компонентов локальной сети

3.9.1 Настройка маршрутизатора

Для подключения станции, с которой будет происходить настройка к маршрутизатору необходим консольный кабель RJ45-DB9, если на компьютере есть COM-порт, или же RJ45-USB, с эмулятором терминала, по типу PuTTY.

По правилам хорошего тона назначим нашим подинтерфейсам маршрутизатора IP-адреса, оканчивающиеся на «1», так как данные адреса будут служить маршрутом по умолчанию для окончного оборудования.

1) Настройка канала между маршрутизатором и коммутатором, настройка пароля

```
Router(config)#enable password kBv724]xZgE4
Router(config)#password complexity enable
Router(config)#password complexity not-current
Router(config)#password complexity not-username
Router(config)#password complexity min-length 9
Router(config)#password again 7
Router(config)#int g0/0/0
Router(config)#ipv6 unicast-routing
Router(config-if)#speed 1000
Router(config-if)#duplex full
Router(config-if)#no shutdown
Router(config-if)#ipv6 enable
Router(config-if)#no shutdown
```

2) Маршрутизация между VLAN:

```
Router(config)#int gig0/0/0.10
Router(config-subif)#description Sub-interface for Directorate
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.0.1 255.255.255.0
Router(config-subif)#ipv6 address FD00:0000:0000:10::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#ip nat inside
Router(config-subif)#int gig0/0/0.11
Router(config-subif)#description Sub-interface for Production
department
Router(config-subif)#encapsulation dot1Q 11
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#ipv6 address FD00:0000:0000:11::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#ip nat inside
Router(config-subif)#int gig0/0/0.12
Router(config-subif)#encapsulation dot1Q 12
```

```

Router(config-subif)#description Sub-interface for accounting
and salesman departments
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#ipv6 address FD00:0000:0000:12::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#ip nat inside
Router(config-subif)#int gig0/0/0.13
Router(config-subif)#encapsulation dot1Q 13
Router(config-subif)#description Sub-interface for guests
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#ipv6 address FD00:0000:0000:13::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#ip nat inside
Router(config-subif)#int gig0/0/0.20
Router(config-subif)#description Sub-interface for
administrators
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#ipv6 address FD00:0000:0000:20::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#ip nat inside
Router(config-subif)#int gig0/0/0.30
Router(config-subif)#description Sub-interface for servers
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#ipv6 address FD00:0000:0000:30::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#ip nat inside

```

3) Настройка access-листов. Запрещаем трафик между локальными пользователями и гостевыми подключениями.

```

Router(config)#access-list 80 permit 192.168.0.0 0.0.255.255
Router(config)#access-list 80 remark Access list for overloaded
NAT.
Router(config)#access-list 13 remark Access list for VLAN 13.
Router(config)#access-list 13 deny 192.168.0.0 0.0.0.255
Router(config)#access-list 13 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 13 deny 192.168.2.0 0.0.0.255
Router(config)#access-list 13 permit any
Router(config)#interface g0/0/0.13
Router(config-subif)#ip access-group 13 out

```

4) Настройка NAT

```

Router(config)# int g0/0/1
Router(config-if)# ip address 6.0.0.2 255.192.0.0
Router(config-if)# ip nat outside
Router(config-if)# no shutdown
Router(config)#ip nat pool out_addr_pool 6.0.0.2 6.0.0.2 netmask
255.192.0.0

```

```
Router(config)#access-list 80 permit 192.168.0.0 0.0.255.255
Router(config)#ip nat inside source list 10 pool out_addr_pool
overload
```

5) Создание DHCP-пулов для беспроводных подключений

```
Router(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.39
Router(config)#ip dhcp excluded-address 192.168.0.51
192.168.0.255
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.39
Router(config)#ip dhcp excluded-address 192.168.1.51
192.168.1.255
Router(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.39
Router(config)#ip dhcp excluded-address 192.168.2.51
192.168.2.255
Router(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.39
Router(config)#ip dhcp excluded-address 192.168.3.51
192.168.3.255
Router(config)#ip dhcp pool WLAN-10
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool WLAN-11
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool WLAN-12
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool WLAN-13
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns-server 8.8.8.8
```

3.9.2 Настройка коммутатора

Для подключения станции, с которой будет происходить настройка, к коммутатору, необходим консольный кабель RJ45-DB9, если на компьютере есть COM-порт, или же RJ45-USB, с эмулятором терминала, по типу PuTTY.

Настройка коммутатора будет происходить в несколько шагов:

1) Конфигурация пароля

```
Switch (config)#enable password 28a{A0II]>Dv
Switch (config)#password complexity enable
Switch (config)#password complexity not-current
Switch (config)#password complexity not-username
```

```
Switch (config)#password complexity min-length 9
Switch (config)#password again 7
```

2) Создание VLAN

```
Switch(config)#vlan 10
Switch(config-vlan)#name directorate
Switch(config-vlan)#vlan 11
Switch(config-vlan)#name production
Switch(config-vlan)#vlan 12
Switch(config-vlan)#name accounting-sales
Switch(config-vlan)#vlan 13
Switch(config-vlan)#name guests
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name admins
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name servers
```

3) Настройка DHCP-сервера для персональных компьютеров

```
Switch(config)#ip dhcp excluded-address 192.168.0.0 192.168.0.10
Switch(config)#ip dhcp excluded-address 192.168.0.30 192.168.0.39
Switch(config)#ip dhcp excluded-address 192.168.0.51
192.168.0.255
Switch(config)#ip dhcp excluded-address 192.168.1.0 192.168.1.10
Switch(config)#ip dhcp excluded-address 192.168.1.30 192.168.1.39
Switch(config)#ip dhcp excluded-address 192.168.1.51
192.168.1.255
Switch(config)#ip dhcp excluded-address 192.168.2.0 192.168.2.10
Switch(config)#ip dhcp excluded-address 192.168.2.30 192.168.2.39

Switch(config)#ip dhcp excluded-address 192.168.2.51
192.168.2.255
Switch(config)#ip dhcp excluded-address 192.168.3.30 192.168.3.39
Switch(config)#ip dhcp excluded-address 192.168.3.51
192.168.3.255
Switch(config)#ip dhcp pool directorate-wired
Switch(dhcp-config)#network 192.168.0.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.0.1
Switch(config)#ip dhcp pool production
Switch(dhcp-config)#network 192.168.1.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.1.1
Switch(config)#ip dhcp pool paperwork
Switch(dhcp-config)#network 192.168.2.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.2.1
Switch(dhcp-config)#interface vlan 10
Switch(config-if)#ip address 192.168.0.5 255.255.255.0
Switch(dhcp-config)#interface vlan 11
Switch(config-if)#ip address 192.168.1.5 255.255.255.0
Switch(dhcp-config)#interface vlan 12
Switch(config-if)#ip address 192.168.2.5 255.255.255.0
```

4) Настройка канала между маршрутизатором и коммутатором

```
Switch(config)#interface gigabitEthernet0/48
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#switchport trunk allowed vlan 10,11,12,13,20,30
Switch(config-if)#duplex full
Switch(config-if)#speed 1000
Switch(config-if)#mdix auto
```

5) Назначение ролей портов

```
Switch(config)#interface range gigabitEthernet0/1-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#interface range gigabitEthernet0/10-16
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 11
Switch(config-if-range)#interface range gigabitEthernet0/20-22
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 12
Switch(config-if-range)#interface gigabitEthernet0/25-30
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan 10-13,20,30
Switch(config-if-range)#switchport trunk native vlan 20
Switch(config-if-range)#power inline auto
Switch(config-if-range)#interface range gigabitEthernet0/31
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#interface gigabitEthernet0/32
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10-13,20,30
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#interface gigabitEthernet0/40
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
```

После назначения access-ролей свободными остаются порты: 5-9, 17-20, 23-24, 33-39 и 41-47. Сделано это с целью возможности дальнейшей масштабируемости сети и подключения нового оконечного или сетевого оборудования.

3.9.3 Настройка беспроводной точки доступа

К точке доступа можно подключиться так же, как и к другому сетевому оборудованию – используя Console-порт, подключая к разъёму RS-232 на компьютере, или же используя кабель RJ45-to-USB и программу-эмулятор терминала.

Так как беспроводные точки доступа и контроллер точек находятся в

разных виртуальных ЛКС – необходимо использовать какой-либо протокол обнаружения. Так как для точек серии 1800 Cisco рекомендует использовать протокол CAPWAP, вместо LWAPP – было принято использовать его. Так же стоит явно сконфигурировать код страны. Данный этап не обязателен, но рекомендуем компанией Cisco. Так как Беларусь относится к израильскому региону – следует поставить его.

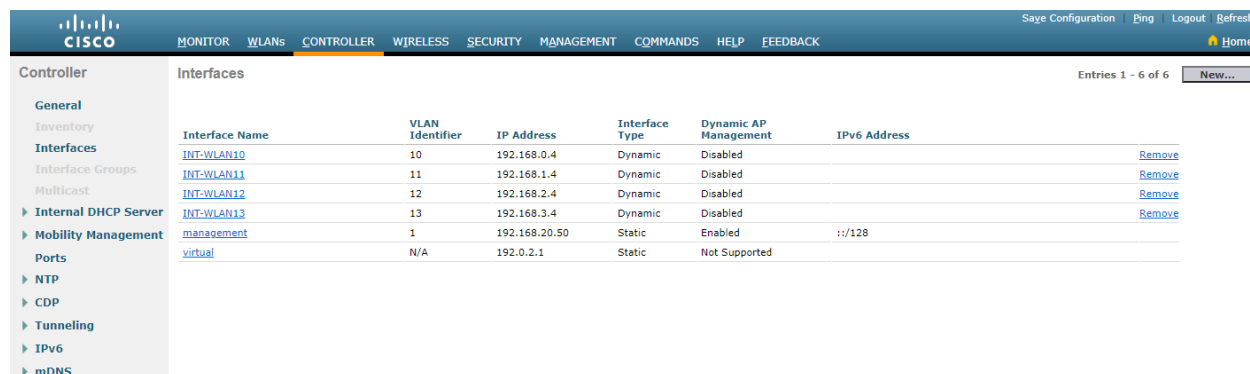
```
AP(config)#capwap ap controller ip address 192.168.20.50
AP(config)#ap country IL
```

Так как для точек доступа на WLC будет настроен внутренний DHCP-сервер – настраивать IP и DG на точках доступа не нужно.

3.9.4 Настройка контроллера точек доступа

Для первоначальной настройки требуется подключить компьютер к беспроводному контроллеру и на назначение адреса поставить «DHCP». После назначения адреса и Default Gateway – следует перейти в браузер и ввести адрес Default Gateway. После долгой загрузки высветиться окно первоначальной настройки контроллера, в которой надо будет ввести имя сети, Default Gateway, Management IP, VLAN ID, выбрать тип аутентификации, имя сети и виртуальный IP.

После необходимо создать все интерфейсы для VLAN. Делается это во вкладке «Controller» -> «Interface» -> «New...». Созданные интерфейсы отображены на рисунке 3.9.1



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address	
INT-WLAN10	10	192.168.0.4	Dynamic	Disabled		Remove
INT-WLAN11	11	192.168.1.4	Dynamic	Disabled		Remove
INT-WLAN12	12	192.168.2.4	Dynamic	Disabled		Remove
INT-WLAN13	13	192.168.3.4	Dynamic	Disabled		Remove
management	1	192.168.20.50	Static	Enabled	::/128	
virtual	N/A	192.0.2.1	Static	Not Supported		

Рисунок 3.9.1 – Созданные интерфейсы.

Далее следует перейти во вкладку «WLANs», создать новый WLAN и конфигурировать его, включив и назначив соответствующий интерфейс (рисунок 3.9.2), назначить тип «Security» (рисунок 3.9.3).

Далее необходимо перейти во вкладку «Controller» и создать DHCP-scope. После создания необходимо зайти в DHCP-scope и сконфигурировать «Pool Start Address», «Pool End Address», «Network», «Mask» и «Default Router».

Созданные DHCP-score отображены на рисунке 3.9.4.

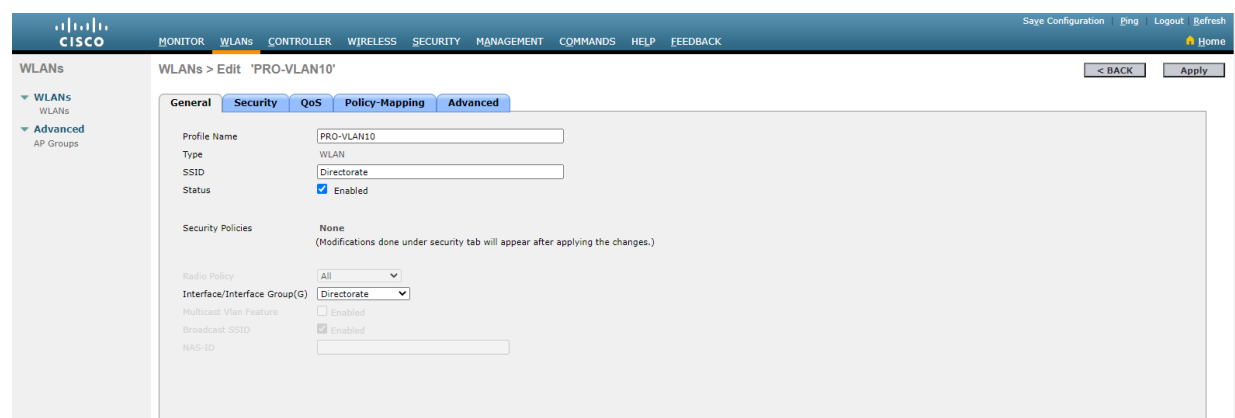


Рисунок 3.9.2 – Конфигурация интерфейса и WLAN.

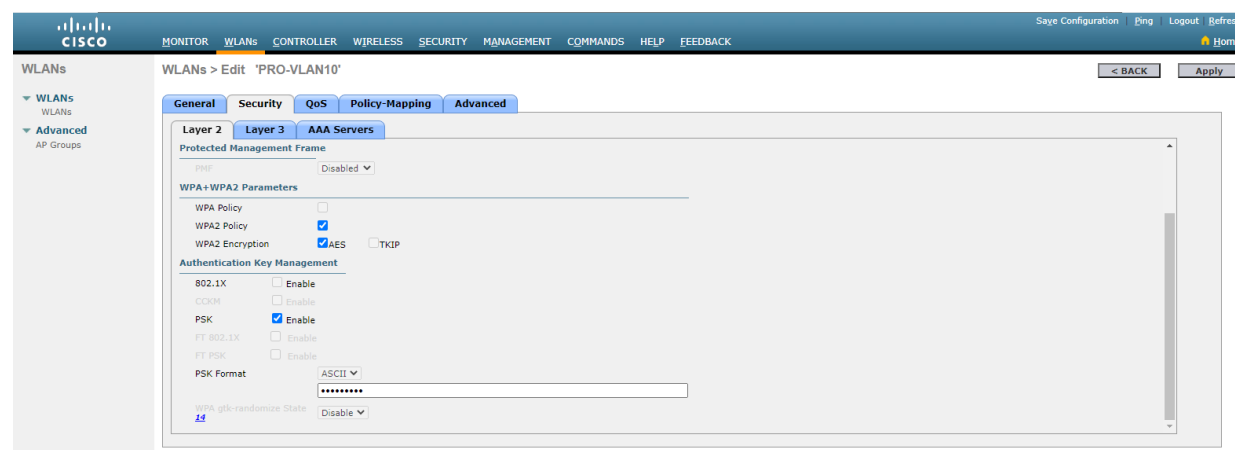


Рисунок 3.9.3 – Конфигурация безопасности WLAN.

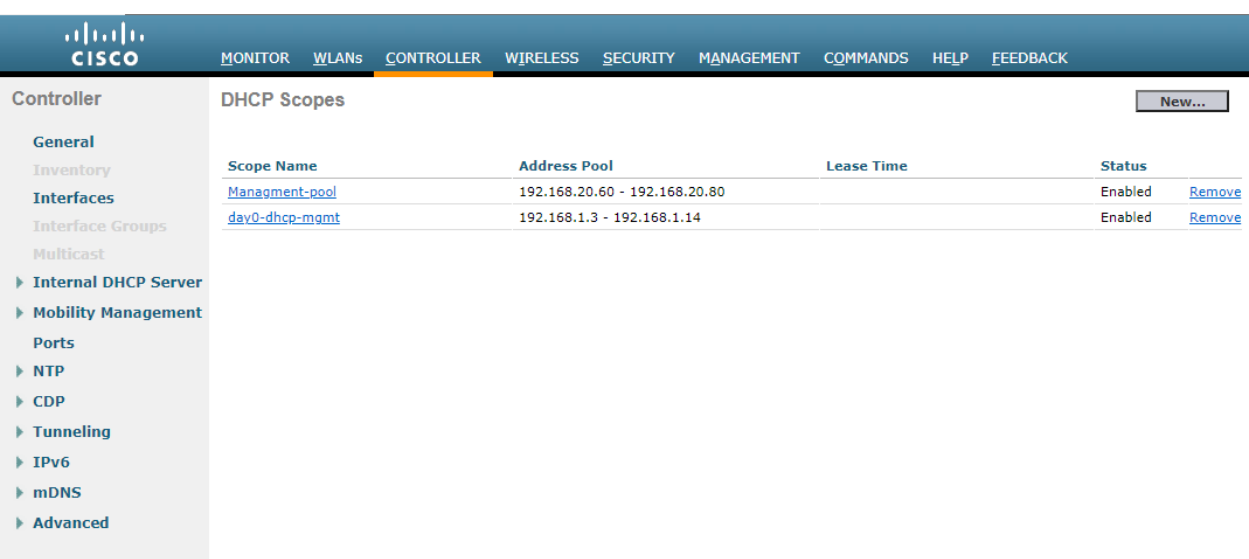


Рисунок 3.9.4 – Созданные DHCP-score.

После назначения пулов необходимо перейти во вкладку «Controller» -> «Interfaces», и во всех интерфейсах адресом DHCP-сервера указать адрес подинтерфейса на маршрутизаторе. После данного шага точки, подключаемые к данному контроллеру, будут иметь 4 WiFi сети: Guests, Accounting-Sales, Production, Directorate. Если к точкам не подключается окончательное оборудование – следует перейти в пункт «Wireless»->«Country» и сконфигурировать страну, если это не было сделано раньше на точках доступа.

Так же рекомендуется включить роуминг. Для этого на переходим в пункт «WLANs» и нажимаем на WLAN ID конкретного WLAN, на котором будет включаться функция роуминга. Далее переходим во вкладку «Advanced» и в секции «11k» выставяем пункты «Neighbor List» и «Neighbor List Dual Band» (рекомендуется производителем). Так же следует выставить пункт «Assisted Roaming Prediction Optimization», для увеличения точек доступа в роуминге и оптимизации для устройств, не поддерживающих стандарт роуминга 802.11k. Таким образом после выставления этих пунктов на всех WLAN будет реализован беспроводной роуминг.

Пароли к данным сетям настраиваются в контроллере точек доступа. При подключении к какой-либо из сетей устройство будет автоматически назначать адрес из ранее созданного пула адресов и ассоциировать себя с VLAN этого пула.

Так же стоит отметить, что настройки локальной сети были эмулированы в среде Cisco Packet Tracer, и рабочие конфигурации активного сетевого оборудования находятся в приложении «И».

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

В данном разделе описывается выбор пассивного сетевого оборудования и практическая реализация ЛКС (прокладка коробов с Ethernet-кабелями, размещение оборудования и сопутствующие мероприятия). Данный раздел сопровождается планами этажей, в которых размещается научно-исследовательская организация.

4.1 Обоснование выбора среды передачи данных

Так как и в рабочих станциях, и в коммутаторе используется формат Gigabit Ethernet – то следует выбрать кабель категории как минимум 5е, который поддерживает передачу 1 Гб/с на расстоянии до 100 метров.

Так как далее рассчитывать расстояние не имеет смысла, по причине поддержки расстояния до 100 метров всеми категориями кабелей – то было принято было выбрать категорию 5е.

Далее необходимо выбрать кабельную защиту. Так как в канале в какой-то момент будет идти минимум 15 кабелей (выход из коммутатора на 3 этаже в спуск кабельного канала), а также факт, что кабели выходят из средней лаборатории на втором этаже, в которых возможна генерация различных шумов и помех, то следует использовать экранированную витую пару. Для данного случая следует использовать витую пару категории F/UTP. Так же нужно помнить, что данный кабель нуждается в заземлении системы, ибо без заземления в его использовании не имеется никакого смысла.

4.2 Обоснование выбора сетевых розеток

Так как никаких требований в плане пыле- и влагостойкости не указано, то можно было предположить, что розетки не требуют никакой дополнительной защиты. Однако, так как на втором этаже размещаются лаборатории компании, занимающейся изучением металлов, следует предположить, что в данных помещениях может быть повышенный уровень пыли, причём металлической, что может плохо повлиять на работоспособность системы. Из этого следует вывод, что розетки необходимо выбирать по стандарту IP, причём версия IP должна защищать от мелкой оседающей пыли, что должно соответствовать минимум степени IP50. Также следует помнить, что витая пара экранирована и требует заземления, следовательно необходимо брать FTP-розетку. Под данные характеристики подходит розетка от компании 3М: Volition RJ45 K5e FTP.

Так же и ПК стоит снабдить особыми пылевыми фильтрами-чехлами, которые будут крепиться на корпус компьютера. Так как корпуса различаются по размерам и форматам – стоит взять любые фильтры, подходящие по размеру, степень защиты которых минимум IP50.

4.3 Обоснование выбора кабельного короба

Для монтажей в большинстве используют кабельные коробки. Для правильного подбора данного короба необходимо его рассчитать.

Наружный диаметр кабеля cat5e F/UTP – 6.33мм [16]. Для начала необходимо рассчитать площадь сечения кабеля: $S_{сеч} = \frac{1}{4}\pi d^2 = 31.47$.

Далее необходимо рассчитать площадь поперечного сечения короба, при этом учитывается, что сумма сечений проводов и кабелей, рассчитанных по их наружным диаметрам, включая изоляцию и наружные оболочки, не должна превышать: для глухих коробов 35 % сечения короба в свету; для коробов с открываемыми крышками 40 %. Из этого составим формулу 4.1:

$$S_N = \frac{N \cdot S_{сеч}}{0,4}, \quad (4.1)$$

В данной формуле S_N – расчётная площадь поперечного сечения короба для N кабелей, N – количество кабелей.

Далее из плана этажа необходимо взять место, с наибольшим количеством кабелей. Таковым будет являться переход из телекоммуникационного шкафа третьего этажа в спуск кабельного канала. При этом будет идти 15 кабелей. Подставив в формулу, получим, что площадь поперечного сечения будет 1268,8мм. Из этого получим, что размеры короба должны быть минимум 30х43. При этом чаще всего форм-фактор кабельных каналов идут 40х16, 40х25, 40х40, так что кабельный канал будет подбираться из расчёта на будущее, 40х40.

4.3 Размещение и монтаж активного сетевого оборудования

Активное сетевое оборудование, использующееся в данной сети, будет располагаться на третьем этаже здания, в серверном шкафу (кроме точек доступа). Серверный шкаф является шкафом напольного типа, соответственно, не имеет никаких ограничений по высоте крепления. Сам шкаф рекомендуется размещать на третьем этаже здания, рядом с пунктом администрирования. Так же имеется возможность установить шкаф на первом этаже в кладовой, при этом организация компьютерной сети никак не поменяется, однако следует понимать, что располагать шкаф на третьем этаже крайне не рекомендуется из-за шанса попадания в него металлической пыли.

В шкафу будут крепиться маршрутизатор, коммутатор, сервер и контроллер точек доступа. Компьютер сетевого администратора может подключаться как напрямую к разъёму коммутатора в шкафу (что не рекомендуется), так и через сетевую розетку, отведённую от шкафа. Далее приводится комплекс «хороших практик», которые используются при наполнении телекоммуникационного шкафа.

Для крепления оборудования в шкаф понадобится:

1. Отвёртка крестовая;
2. Винты, шайбы и гайки (если не идут в комплекте);
3. Бухта витой пары;
4. Кремпер для обжима проводов;
5. Тестер;
6. Горизонтальные и вертикальные органайзеры, хомуты;
7. Силовые кабели различной длины.

Для того, чтобы закрепить необходимое оборудования, сначала рекомендуется составить схему расположения. Так как больше всего проводов будет идти от коммутатора, а между маршрутизатором и коммутатором будет лишь один провод – лучше всего расположить коммутатор над или под маршрутизатором, и так как больше маршрутизаторов или коммутаторов нет – над коммутатором можно расположить горизонтальный органайзер. Далее, в нашем случае с любой из сторон от органайзера, можно поместить оставшееся сетевое оборудование. Сзади так же следует в тот же слот установить горизонтальный органайзер, если шкаф это поддерживает, и вертикальный, для прокладки силовых кабелей. Схема расположения оборудования представлена на рисунке 4.1. Сверху стоит маршрутизатор, за ним идёт коммутатор, органайзер, контроллер точек доступа и сервер соответственно.

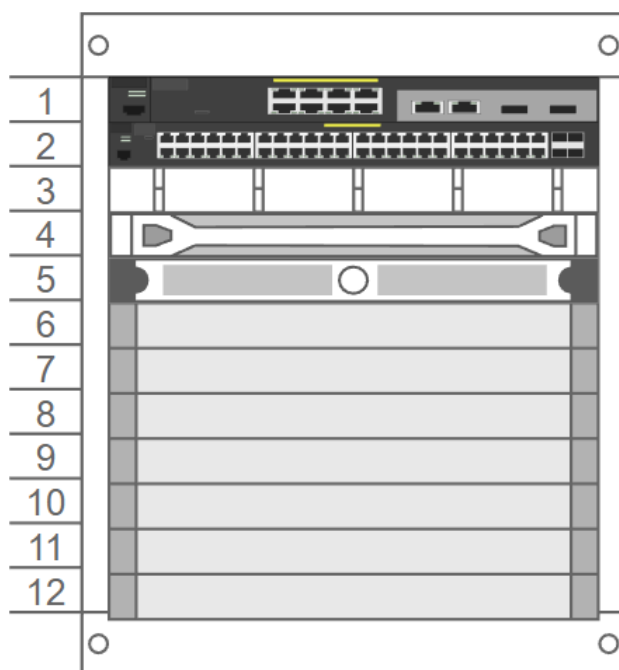


Рисунок 4.1 – Схема расположения оборудования в шкафу

Так же требуется провести определённую процедуру с сервером. Для сервера рекомендуется прикрепить наклейку с написанным MAC-адресом, а

также номера корзин в дисках и серийные номера дисков, установленных в слоты сервера.

На кабели рекомендуется клеить бирки, обозначающие куда и откуда идёт кабель. Так же стоит не забывать про заземление стоек. Сам шкаф рекомендуется располагать на расстоянии 20-30 см от стены.

Точки доступа же, в отличие от всего остального активного сетевого оборудования, располагаются на каждом из этажей. На каждый этаж идёт по 2 точки доступа. Точки доступа крепятся к потолку с помощью специального кронштейна, который идёт в комплекте. Для крепления необходимо провести кабель Ethernet в кронштейн, прикрепить кронштейн к потолку, используя специальные отверстия и прикрепить точку доступа к кронштейну. Стоит понимать, что точки доступа могут крепиться к разным потолкам по разным методам. Полную инструкцию, включая вышесказанную, можно найти в списке использованных источников под номером 17.

Отдельно стоит упомянуть расчёт покрытия беспроводной сетью.

4.2.1 Расчёт качества покрытия беспроводной сетью

Беспроводная сеть должна покрывать всю площадь здания, и может даже выходить за его пределы. Внешние стены помещений состоят из кирпича, влияние на пропускную способность которого равно примерно 6 dB [18]. Пол же будет. Для того, чтобы рассчитать, эффективно или нет располагать точки доступа – необходимо рассчитать расстояние от источника сигнала до наиболее удалённой точки.

Так как здание прямоугольное, можно предположить, что использование Яги-антенн будет эффективно. Однако, требуется опровергнуть или подтвердить данное утверждение. Если располагать Яги-антенну на первом этаже около лестницы, чтобы она покрывала всё помещение, и чтобы диаграмма направленности покрывала сопутствующие углы помещения, что является примерно 32 градуса, то следует воспользоваться формулой 4.2:

$$L = -(32.44 * 20 \lg(F) + 20 \lg(D) + const) + F_{yagi} + F_{AP} + N * 5 \quad (4.2)$$

где F – частота в ГГц (2.5/5), D – расстояние между источником сигнала и приёмником, F_{yagi} – частота усиления Яги-антенны, F_{AP} – частота усиления точки доступа (равно 22), N – количество стен, через которые проходит сигнал, $const$ – константная величина затухания (примерно равна 5 dB), L – затухание сигнала в dB.

По данной формуле получим, что затухание на первом этаже, при использовании Яги-антенны с усилением в 12 dB составит -79.29 dB, так как сигнал будет проходить через монолитную стену, а также в других точках – через металлические двери. На втором этаже затухание будет равно -95,29 dB, без условия прохождения через двери, что уже не соответствует типичной

чувствительности приёмника. На третьем этаже затухание будет равно -83,29 dВ. Из данных расчётов можно сделать вывод, что использование Яги-антенн в данном проекте не обосновано и является неэффективным способом покрытия беспроводной сетью.

Теперь же можно предположить, что на этаж должно приходиться две точки доступа, стоящие на расстоянии 10.5 метров от стен и примерно 20 метров друг от друга. Результаты данного расчёта будут приведены в таблице 4.1, в которой маркировка точек доступа будет указана аналогично маркировке приложениям «В», «Г» и «Д» соответственно. Расчёты будут производиться по формуле 4.3.

$$L = -(32.44 * 20 \lg(F) + 20 \lg(D) + 5) + F_{AP} - N * 5 \quad (4.3)$$

Где F – частота в ГГц (2.5/5), D – расстояние между источником сигнала и приёмником, F_{AP} – частота усиления точки доступа (равно 22), N – количество стен, через которые проходит сигнал, $const$ – константная величина затухания (примерно равна 5 dВ), L – затухание сигнала в dВ.

Таблица 4.1 – расчёт затухания сигналов для точек доступа

Точка доступа	Затухание 2.4 ГГц	Затухание 5 ГГц
AP1.1	-64.49	-70.87
AP1.2	-59.49	-65.87
AP2.1	-64.49	-70.87
AP2.2	-64.49	-70.87
AP3.1	-58.38	-64.76
AP3.2	-59.49	-65.87

Усиление сигнала точками доступа – 20 + 2 dВ [19]. Соты точек доступа были разделены на расстояние 12 метров. При этом точка охватывает свою половину этажа и покрывает её сигналом, достаточным для его приёма мобильными подключениями.

4.3 Размещение и монтаж пассивного сетевого оборудования

Все кабели идут в отдельном кабельном коробе, исключая кабели, идущие по фальш-потолку и кабелей в плинтусе. Кабельный короб необходимо располагать на расстоянии не менее 2 метров над полом и не менее 30 см от потолка, за счёт добавления резервного расстояния и в связи с техникой безопасности.

В качестве короба, как было рассчитано выше, следует взять короб размером 40х40. Так как в дополнительных требованиях не присутствует пожаробезопасность и влагостойкость – то можно выбрать самый простой короб размером 40х40, коим является КДК-Д 40х40 Bylectrica.

Так же необходимо понимать, что провода будут идти в распределительную коробку. Единственный фактор, при выборе распределительной коробки – плоскость принимаемого поперечного сечения. В данном случае это принимаемое отверстие должно быть от 40х40мм.

В качестве витых пар были взяты провода ParLan™ F/UTP Cat 5e, так как данная компания имеет бесплатную доставку, гарантию замены брака и хорошие отзывы. Шайбы RJ-45 можно взять любые.

И розетки, и витые пары будут обжиматься по стандарту «Б». Для того, чтобы обжать кабель – необходимо иметь кремпер. Так как кабель имеет защитный слой фольги – то рекомендуется сначала с начала обжимать его как обычный кабель, для расстановки проводов в правильном порядке, а потом снять слой, для дополнительного слоя фольги между кабелями и обмоткой.

Для обжима сетевой розетки потребуется стриппер, кроссировочный нож (или обычный) и, непосредственно, сама розетка. Алгоритм обжима розетки заключается в следующем:

1. Снять часть розетки;
2. Определить стандарт «А» или «Б» (обычно размечены цветами и двумя буквами);
3. Снять изоляцию с кабеля с помощью стриппера;
4. Используя кроссировочный нож, аккуратно отпрессовать провода в необходимую выемку;
5. Соединить вторую часть розетки и прикрепить к стене.

Из личных рекомендаций можно уточнить, что сначала необходимо выставить все провода согласно цветовой схеме над нужными выемками, перепроверить все соединения и лишь потом отпрессовать провода, так как если какой-либо из кабелей не будет стоять на своём месте – придётся переобжимать всю розетку заново.

После обжима всех сетевых кабелей необходимо удостовериться в их работоспособности. Данный шаг рекомендательный, и может пропускаться. Для того, чтобы проверить, правильно ли обжат сетевой кабель или розетка – необходимо воспользоваться кабельным тестером. Для тестирования кабеля необходимо вставить вход и выход кабеля в тестер. При этом, если на экране или светодиодах не будет никакого нарушения или переплетения – то кабель был обжат правильно. Для тестирования розеток необходим тестер с составными частями – приёмник и передатчик соответственно. Если приёмник или передатчик не имеют функции вставки в розетку – то необходимо подключить к ним заранее обжатые и проверенные RJ-45 пары. После подключения необходимо повторить вышеописанную процедуру.

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсового проекта по разработке и реализации локальной компьютерной сети были рассмотрены и реализованы различные аспекты, необходимые для создания эффективной и безопасной инфраструктуры. Проект включает в себя разделы, начиная с обзора литературы, где были рассмотрены такие ключевые темы, как NTFS/SMB сервер, двухфакторная аутентификация, использование VLAN, NAT и PAT, а также контроллеры точек доступа.

Разработанная сеть имеет следующие свойства для удовлетворения нужд заказчика:

- 1) Оснащение достаточным количеством оконечных устройств и наличие некоторого запаса, для подключения новых;
- 2) Разделение сети на VLAN по логической составляющей;
- 3) Наличие различных WiFi сетей, администрируемых с локального контроллера;
- 4) Обеспечено конфигурирование и размещение локального файлового сервера;
- 5) Обеспечен выход в интернет, с использованием PAT, не требуя большого количества публичных IP-адресов;
- 6) Сконфигурирована подсеть для беспроводных гостевых подключений;
- 7) Обеспечена автоматическая настройка IPv4 и IPv6 адресов для конечных устройств;
- 8) Произведено описание и рекомендации к креплению и размещению сетевого оборудования, а также проектировочный расчёт качества покрытия беспроводной сетью.

Полученные результаты обеспечивают надежную и эффективную локальную сеть, готовую к использованию в предполагаемых рабочих условиях.

В заключение хочется отметить, что выполнение данного проекта позволило углубить понимание принципов проектирования и настройки локальных компьютерных сетей, а также приобрести дополнительные теоретические навыки в области выбора оборудования, настройки компонентов и создания структурированных кабельных систем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- [1] Компьютер Z-Tech 5-34G-16-120-1000-320-N-190047n [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://catalog.onliner.by/desktoppc/ztech/ztec534g161201pj>
- [2] Компьютер ASUS D700ME [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.asus.com/displays-desktops/tower-pcs/expertcenter/expertcenter-d7-mini-tower-d700me/>
- [3] Приложение аутентификации от компании miniOrange [электронный ресурс]. – Электронные данные. – Режим доступа: [miniorange.s3.amazonaws.com/public/plugins/idp/mOCredentialProvider.msi](https://s3.amazonaws.com/public/plugins/idp/mOCredentialProvider.msi)
- [4] Инструкция пользователя по использованию NCheck Bio Attendance [электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.ncheck.net/documentation/index.html>
- [5] Драйвера для принтера Kyocera P3145DN [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.kyoceradocumentsolutions.eu/en/support/downloads.name-L2V1L2VuL3ByaW50ZXJzL0VDT1NZU1AzMTQ1RE4=.html>
- [6] Драйвера для принтера Epson L1300 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.epson.co.id/Ink-Tank-Printers/L-Series/Epson-L1300/s/SPT_C11CD1300
- [7] Характеристики маршрутизатора Cisco ISR4431 [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.cisco-russia.ru.com/routers/cisco-isr4431-v-k9>
- [8] Характеристики коммутаторов серии Cisco 350 [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.cisco.com/c/en/us/products/collateral/switches/small-business-smart-switches/data-sheet-c78-737359.html>
- [9] Характеристики сервера Dell EMC PowerEdge R450 [Электронный ресурс]. – Электронные данные. – Режим доступа: http://raid.by/load-file/servers/servers-dell/Dell_EMC_PowerEdge-R450-Spec-Sheet.pdf
- [10] Характеристики сервера Сервер Lenovo ThinkSystem SR630 V2 [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.lenovo.com/us/en/p/servers-storage/servers/racks/thinksystem-sr630-v2/77xx7sr63v2>
- [11] Характеристики точек доступа Cisco серий Aironet [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.router-switch.com/media/upload/product-pdf/cisco-indoor-access-points-comparison-chart.pdf?utm_source=product_pdf&utm_medium=links&utm_campaign=pdf
- [12] Характеристики точек доступа Cisco серий Catalyst [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741988.html>

[13] Характеристики контроллера точек доступа Cisco 2500 [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.cisco.com/c/en/us/products/collateral/wireless/2500-series-wireless-controllers/data_sheet_c78-645111.html

[14] «Что нового» в Windows Server 2022 [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022>

[15] Стандарт адресов IPv6 типа unique-local [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://datatracker.ietf.org/doc/html/rfc4193#section-3.2>

[16] Характеристики кабеля cat-5e F/UTP [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://cabeltorg.by/catalog/kabeli-i-provoda/kabel-f-utp-cat-5e-lszh-4pr-4x2x24awg-0-50-200mhz-cu-305m/>

[17] Инструкция крепления точки доступа Cisco к потолку [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/mounting/guide/apmount.html

[18] Затухание сигнала Wi-Fi в различных материалах [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://fantasylab.ru/tekhnoblog/6-fantasylab/2011-03-20-02-19-00/72-zatukhanie-wi-fi-v-razlichnykh-materialakh.html>

[19] Техническая спецификация точек доступа серии Cisco Aironet 1815 [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1815-series-access-points/datasheet-c78-738243.html>

ПРИЛОЖЕНИЕ А
(Обязательное)

Схема СКС структурная

ПРИЛОЖЕНИЕ Б
(Обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(Обязательное)

План первого этажа. Схема монтажная

ПРИЛОЖЕНИЕ Г
(Обязательное)

План второго этажа. Схема монтажная

ПРИЛОЖЕНИЕ Д
(Обязательное)

План третьего этажа. Схема монтажная

ПРИЛОЖЕНИЕ Е
(Обязательное)

Перечень оборудования, изделий и материалов

ПРИЛОЖЕНИЕ Ж
(Обязательное)

Ведомость документов

ПРИЛОЖЕНИЕ 3

Изображения конфигурации файлового сервера

ПРИЛОЖЕНИЕ И

Рабочие конфигурации в Cisco Packet Tracer