

Министерство 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 помещений 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	7
1 ОБЗОР ЛИТЕРАТУРЫ	8
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ	9
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ	13
3.1 Обоснование выбора оборудования для рабочих мест	13
3.1.1 Рабочие станции	13
3.1.2 Принтеры	14
3.2 Настройка оконечных устройств	15
3.2.1 Настройка пользовательских станций	15
3.2.3 Настройка принтеров	22
3.3 Обоснование выбора активного сетевого оборудования	22
3.3.1 Маршрутизатор	23
3.3.2 Коммутатор	24
3.3.3 Файловый сервер	25
3.3.4 Беспроводные точки доступа	25
3.3.5 Контроллер точек доступа	26
3.4 Обоснование выбора пассивного сетевого оборудования	27
3.4.1 Телекоммуникационный шкаф	27
3.5 Обоснование выбора серверного ПО	28
3.6 Настройка активного сетевого оборудования	28
3.6.1 Установка серверного ПО	28
3.6.2 Настройка NTFS/SMB сервера	29
3.7 Разделение сети на внутренние виртуальные подсети	33
3.8 Составление таблицы адресации в ЛКС	34
3.9 Описание и настройка компонентов локальной сети	35
3.9.1 Настройка маршрутизатора	35
3.9.2 Настройка коммутатора	38
3.9.3 Настройка беспроводной точки доступа	40
3.9.4 Настройка контроллера точек доступа	40
4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ	43
ЗАКЛЮЧЕНИЕ	44
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	45
ПРИЛОЖЕНИЕ А	47
ПРИЛОЖЕНИЕ Б	48
ПРИЛОЖЕНИЕ В	49
ПРИЛОЖЕНИЕ Г	50
ПРИЛОЖЕНИЕ Д	51

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 Metro Ethernet. Сети данного типа характеризуются многоточечным подключением в городской сети. Данный тип сети обладает преимуществами, например, лёгкой масштабируемостью, хорошим отношением цена/качество и простотой использования.

Основной задачей компьютерных сетей является обеспечение совместного доступа к данным, поэтому под данную сеть по заданию требуется создать отдельный сервис NTFS/SMB с внутренним сервером. Файловые системы NTFS поддерживаются операционными системами Windows и Linux, однако так как данный формат разрабатывался компанией Microsoft для Windows NT – рекомендуется использовать её. Протокол SMB является протоколом коммуникации, который кроме взаимодействия с некоторым сетевым оборудованием (принтерами, как указано по заданию) 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, написание руководства пользователя, подведение итогов разработанной системы.

1 ОБЗОР ЛИТЕРАТУРЫ

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 3.1.1

Таблица 3.1.1 – 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.

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 3.1.2, а сравнение цветных – в 3.1.3.

Таблице 3.1.2 – 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 3.1.3 – 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 3.2.1 – 3.2.5.

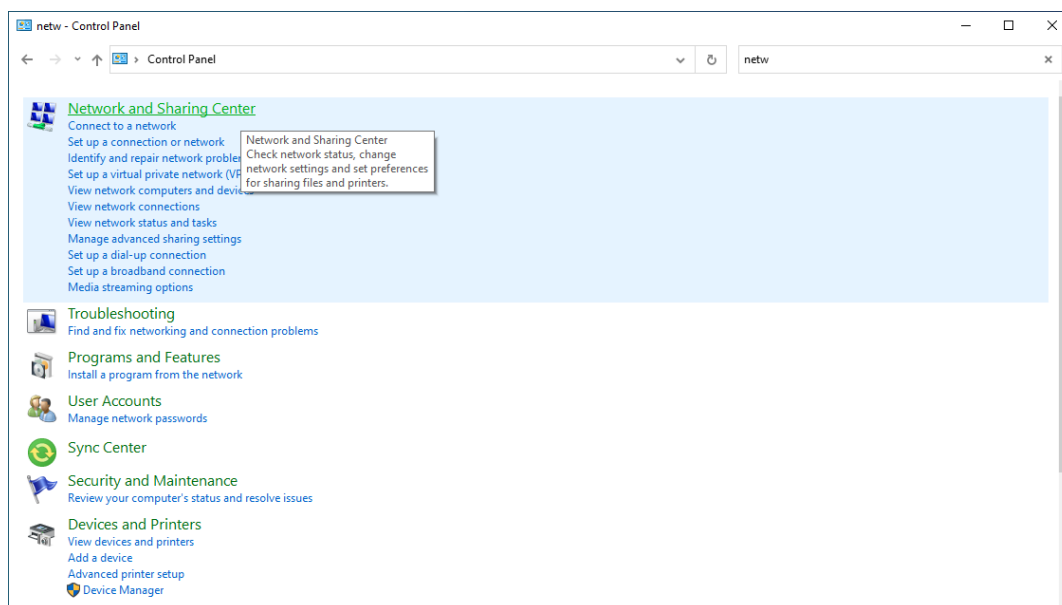


Рисунок 3.2.1 – выбор «Network Sharing Center».

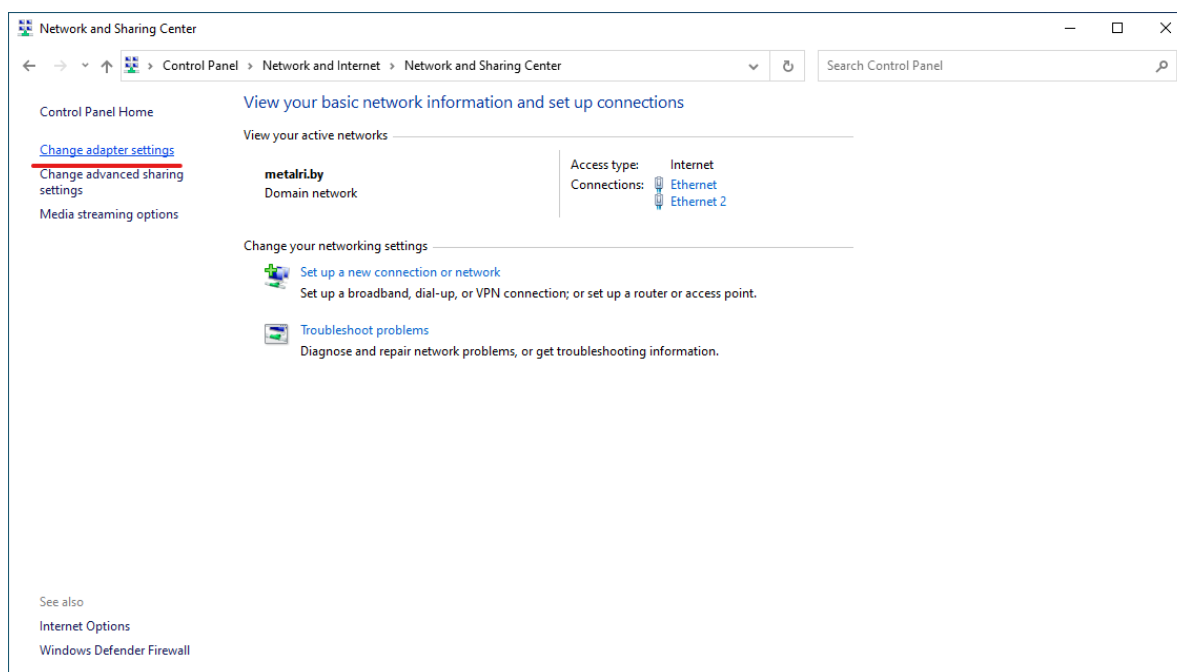


Рисунок 3.2.2 – выбор «Change adapter setting».

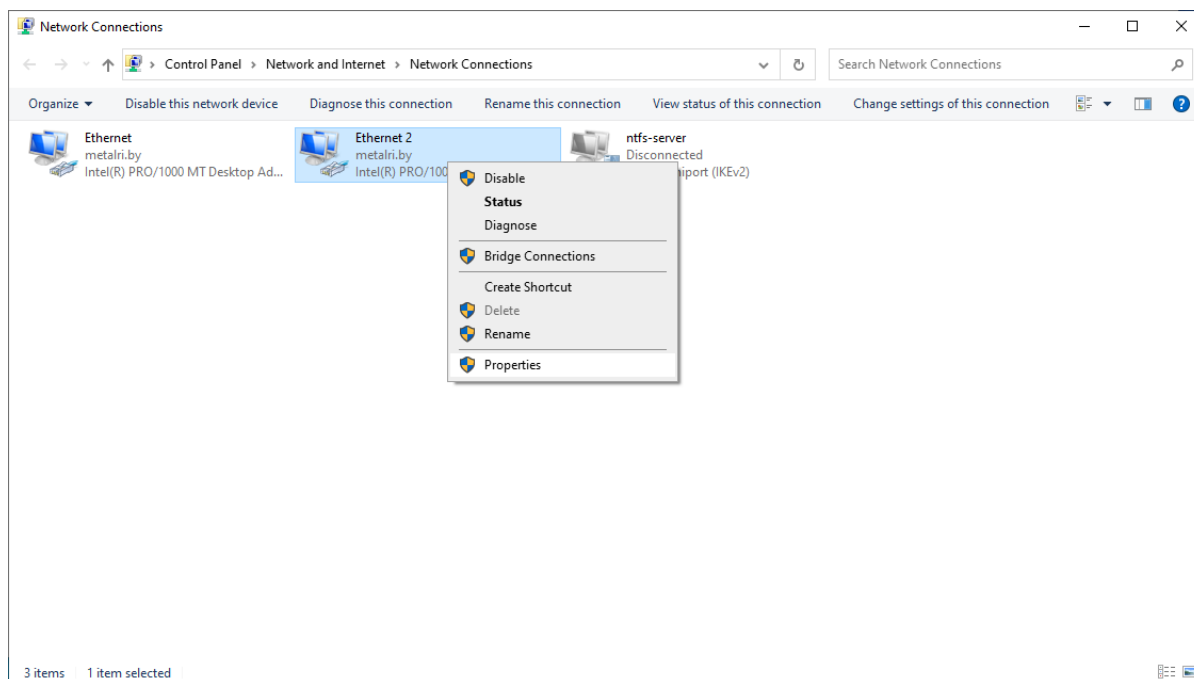


Рисунок 3.2.3 – выбор соответствующего адаптера и его настроек.

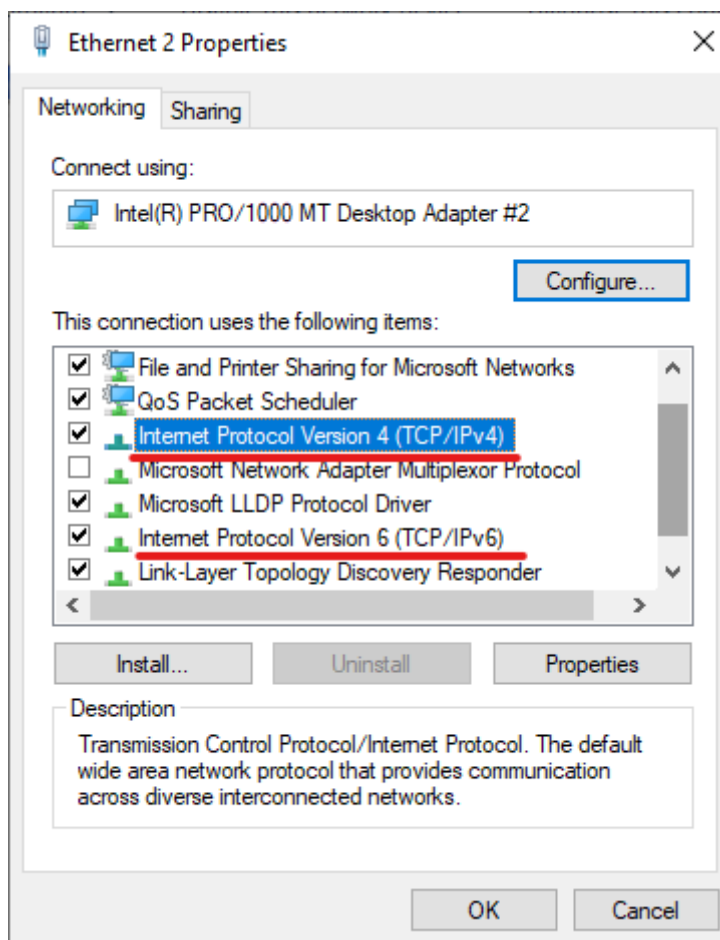


Рисунок 3.2.4 – выбор настроек IPv4 и IPv6.

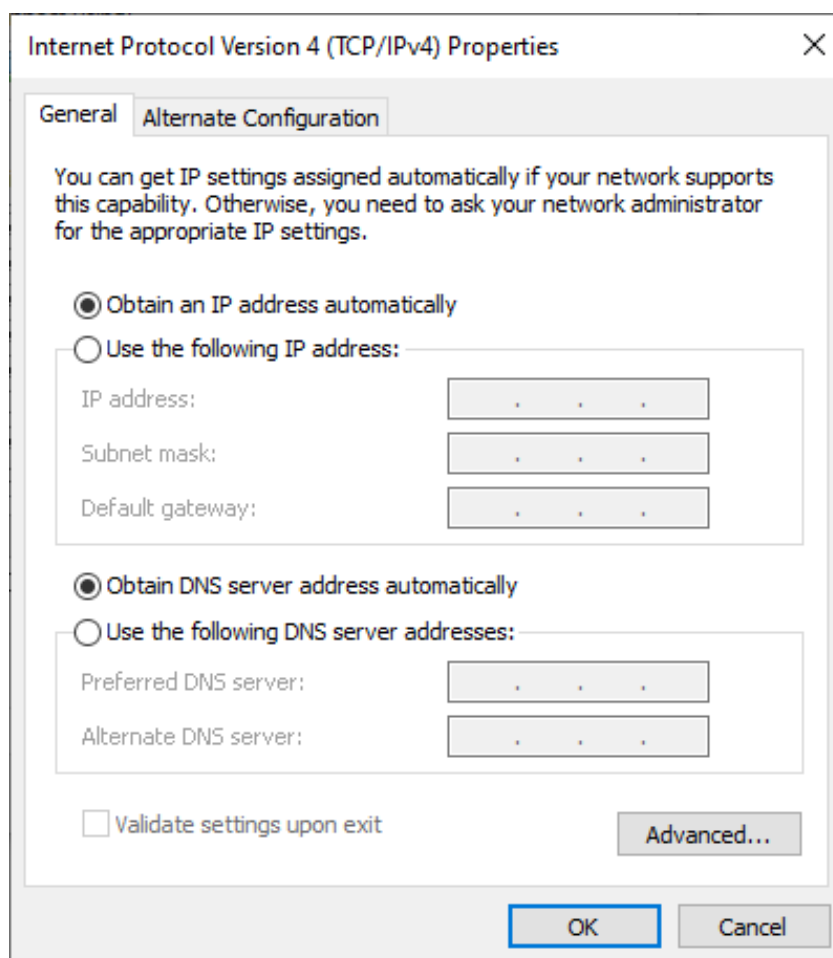


Рисунок 3.2.4 – Настройка IPv4.

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:

- Настройка опции «Log on hours» в соответствии со временем работы компании (рисунок 3.2.5);
- Пользователь должен менять пароль после каждого входа в учётную запись (рисунок 3.2.6);
- Будет использоваться приложение «miniOrange» для двухфакторной аутентификации.

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 3.2.9 – 3.2.11).

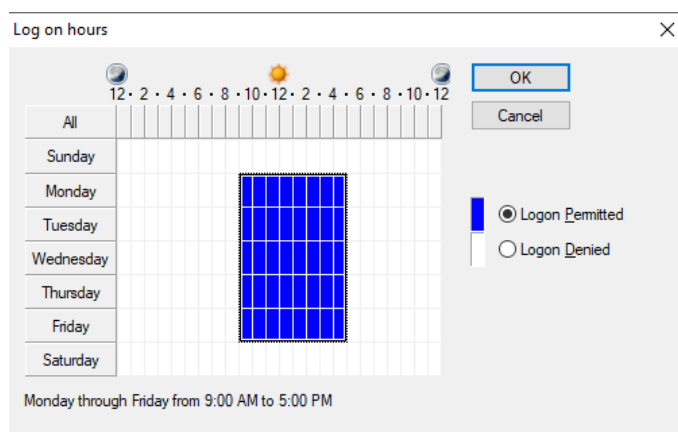


Рисунок 3.2.5 – Настройка опции «Log on hours»

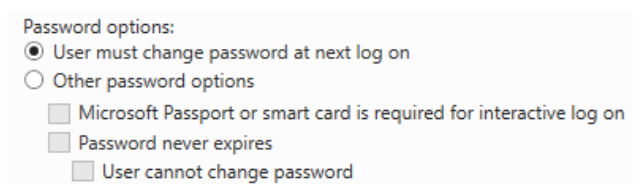


Рисунок 3.2.6 – Настройка повторного изменения пароля

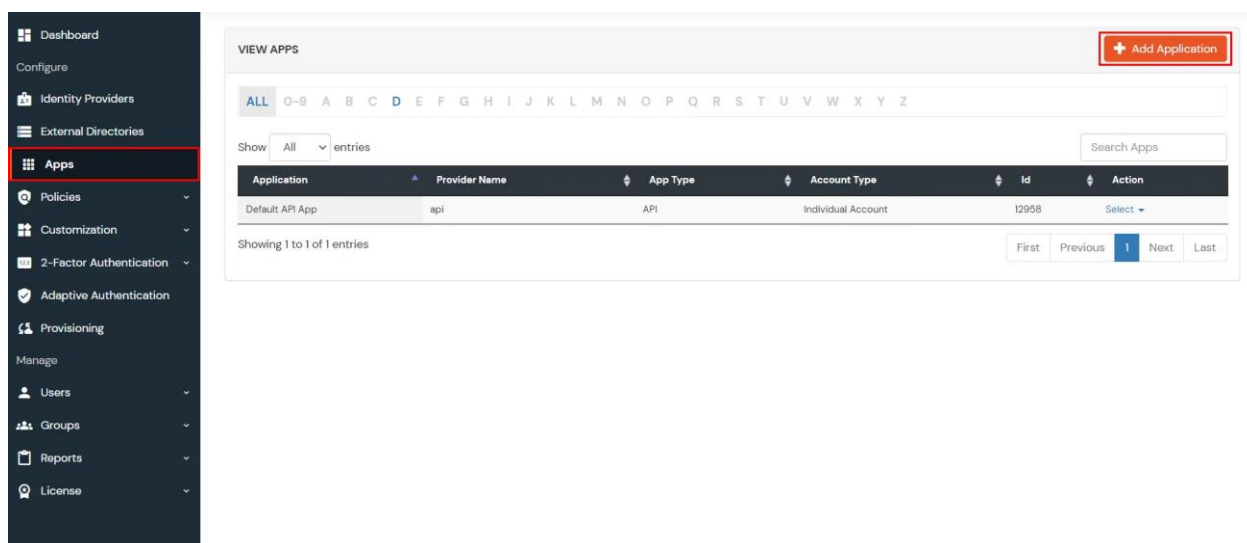


Рисунок 3.2.6 – Добавление нового типа авторизации.

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 3.2.7 – Добавление способа входа.

Dashboard

Configure

Identity Providers

External Directories

Apps

Policies

Customization

2-Factor Authentication

Setup 2FA

Alternate 2FA Login Methods

2FA Options For EndUsers

Assign Hardware Token to Users

Static Code Generation

Adaptive Authentication

Provisioning

Manage

SELECT DEFAULT AUTHENTICATION METHOD

☒ OTP OVER SMS

☐ DISPLAY HARDWARE TOKEN

☐ EMAIL LINK

☐ OTP OVER EMAIL

☐ SMS LINK

☐ OTP OVER SMS AND EMAIL

SELECT ALLOWED 2FA METHODS

☒ OTP OVER SMS

☒ SOFT TOKEN

☒ MICROSOFT AUTHENTICATOR

☒ OTP OVER EMAIL

☐ DISPLAY HARDWARE TOKEN

☐ EMAIL LINK

☒ QR CODE AUTHENTICATION

☐ CALL ME

☒ PUSH NOTIFICATIONS

☒ GOOGLE AUTHENTICATOR

☒ AUTHY AUTHENTICATOR

☒ YUBIKEY HARDWARE TOKEN

☒ SMS LINK

☒ SECURITY QUESTIONS

☒ OTP OVER SMS AND EMAIL

Рисунок 3.2.8 – 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 3.2.9 – Customer Key и API Key со стороны администратора.

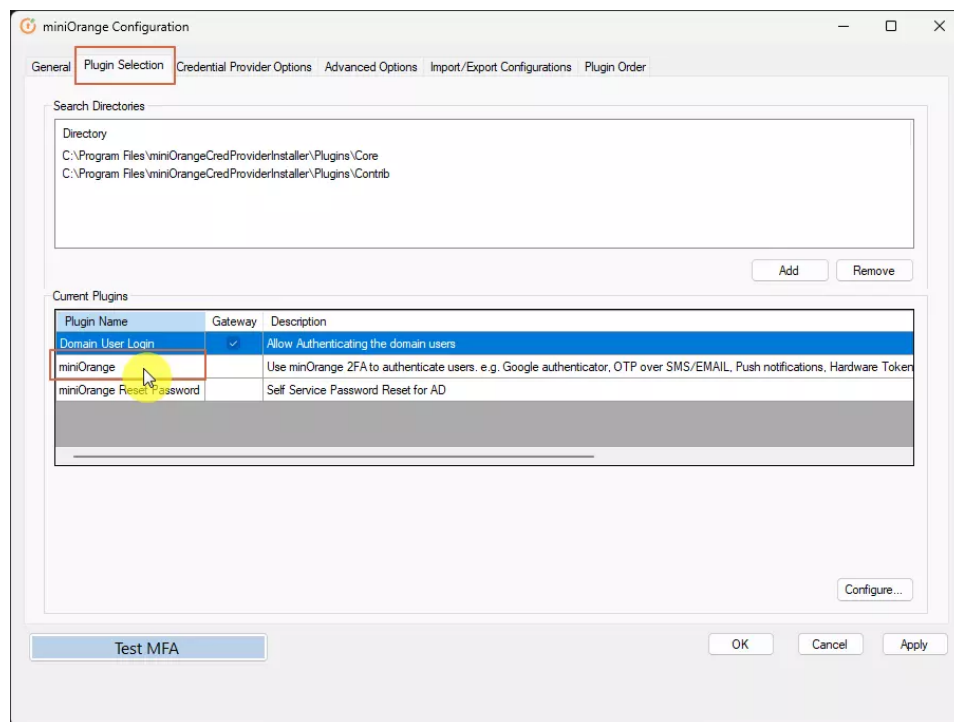


Рисунок 3.2.10 – Включение плагина двухфакторной аутентификации.

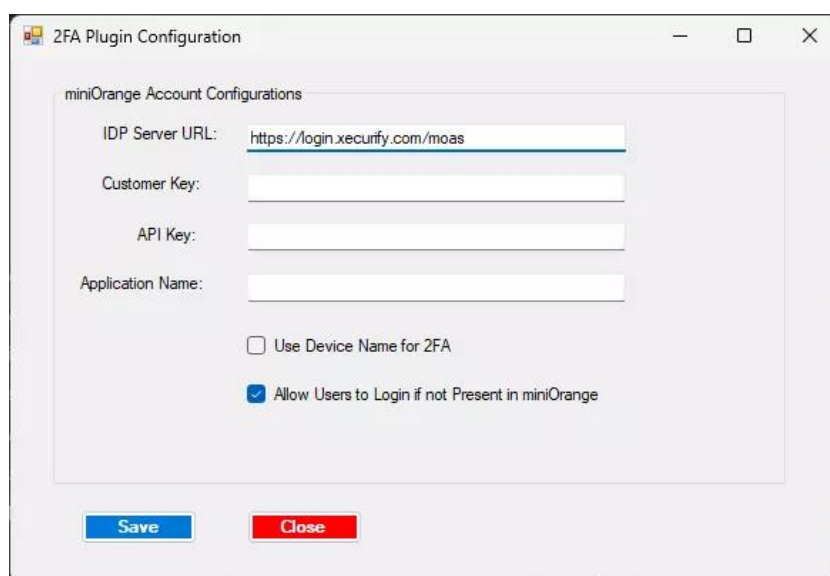


Рисунок 3.2.11 – Меню ввода Customer key и API key.

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 3.2.12). При этом привязывая своё приложение от Google Authenticator или Push Notification.

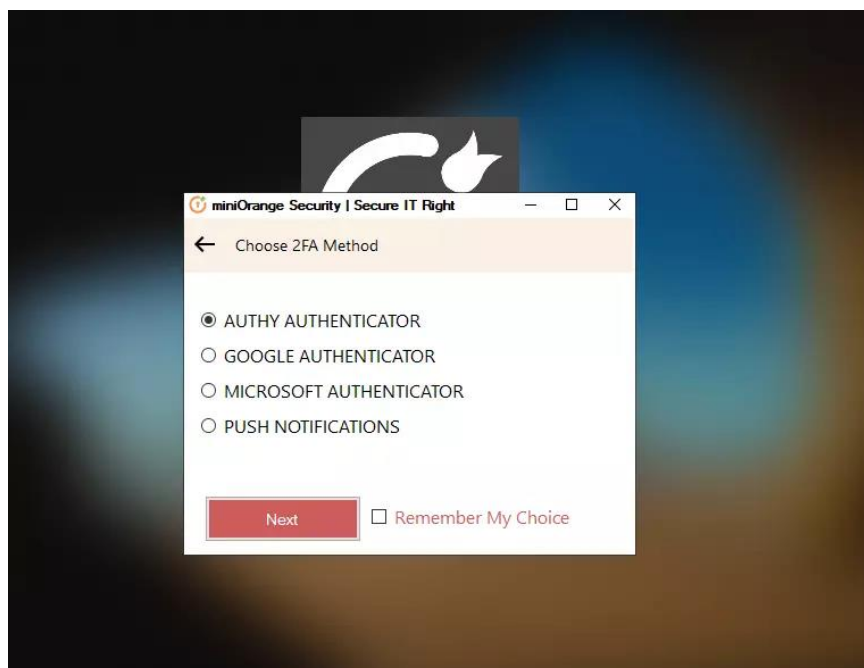


Рисунок 3.2.12 – Меню входа пользователя.

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 [4] 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 [5]. 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 «Д».

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 3.3.1.

Таблица 3.3.1 – 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 [6].

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 3.3.2.

Таблица 3.3.2 – 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 [7]

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 [8] и Lenovo ThinkSystem SR630 V2 [9].

Таблица 3.3.3 – 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.

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 3.3.4 – сравнение беспроводных точек доступа

Модель	Cisco AIR-AP1815I-E-K9	Cisco AIR-AP1852I-E-K9	Cisco C9115AXI-I
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 [10] является наилучшим сочетанием цена/качество. Точка Cisco C9115AXI-I [11] 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 3.3.5 – сравнение контроллеров точек доступа

Модель	Cisco AIR-CT2504-15-K9	Cisco AIR-CT3504-K9
Цена	3308.58 р.	33217.44 р.
Количество поддерживаемых точек доступа	До 75	До 150

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 [12] 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 кабели, 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 3.3.1

Таблица 3.4.1 – количество необходимых креплений

Оборудование	Необходимое количество крепёжных единиц (RU – rack shelf)
Cisco ISR4431/K9	1
Cisco SB SF350-28-K9	1
Dell EMC PowerEdge R440	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 [13]. 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 Установка серверного ПО.

Для начала необходимо установить на сервер Windows Server 2022. Для этого следует:

- 1) Загрузить драйвера с официального сайта Lenovo [14], и следуя по инструкции, обновить серверное ПО;
- 2) Вставить переносно устройство с установщиком Windows Server;
- 3) Перезагрузить сервер. При загрузке нажать F12;
- 4) Выбрать «USB Device»;
- 5) Продолжить установку ОС.

После установки Windows Server – система будет установлена и сервер будет перезагружен. После перезагрузки и нажатия Ctrl+Alt+Delete

администратор сможет войти в систему, введя пароль.

При необходимости – на Windows следует произвести обновление и загрузить драйвера, позволяющие поддержку технологии RAID.

3.6.2 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.

После конфигурации интерфейса необходимо создать сервер. Для этого необходимо:

- 1) Нажать «Manage» в верхнем правом углу и выбрать «Add Roles and Features» (рисунок 3.6.1);
- 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». (рисунок 3.6.3). Нажать «Next»;
- 5) Подтвердить.

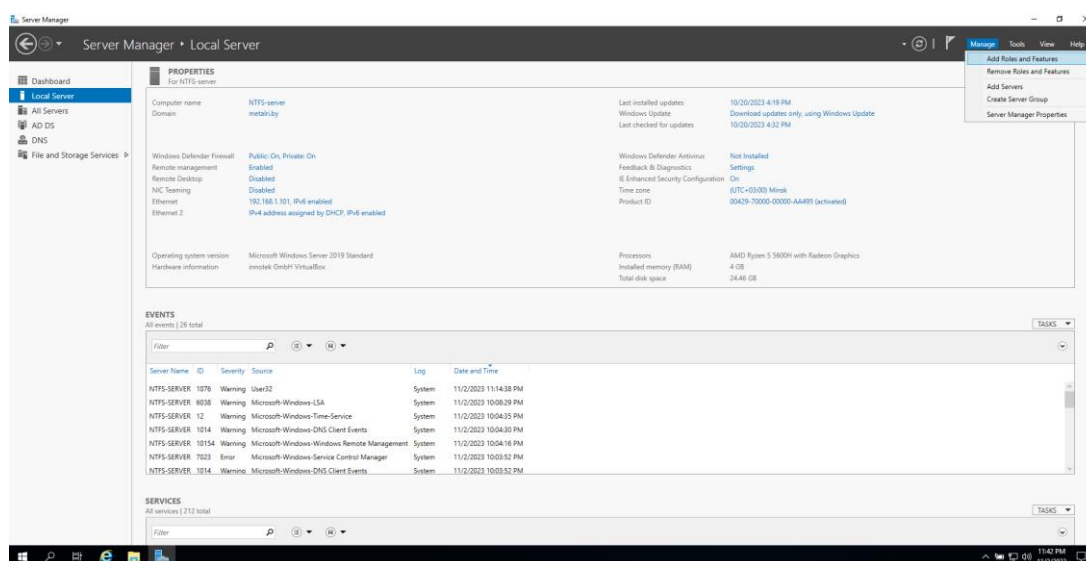


Рисунок 3.6.1 – Выбор «Add Roles and Features».

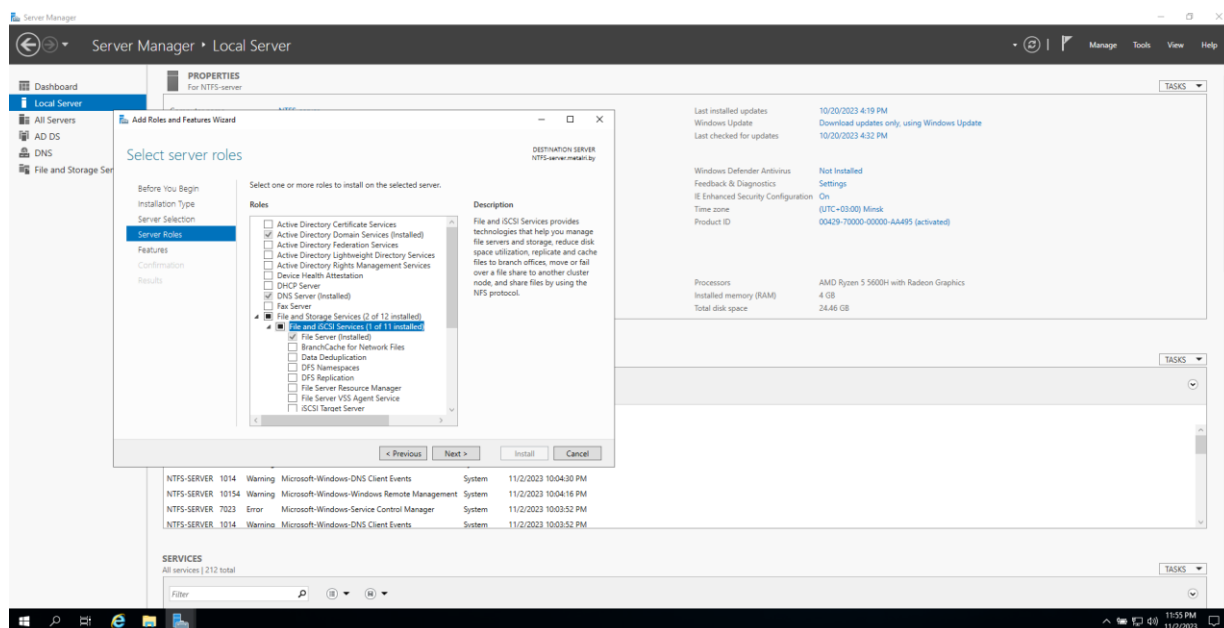


Рисунок 3.6.2 – Выбор «File Server».

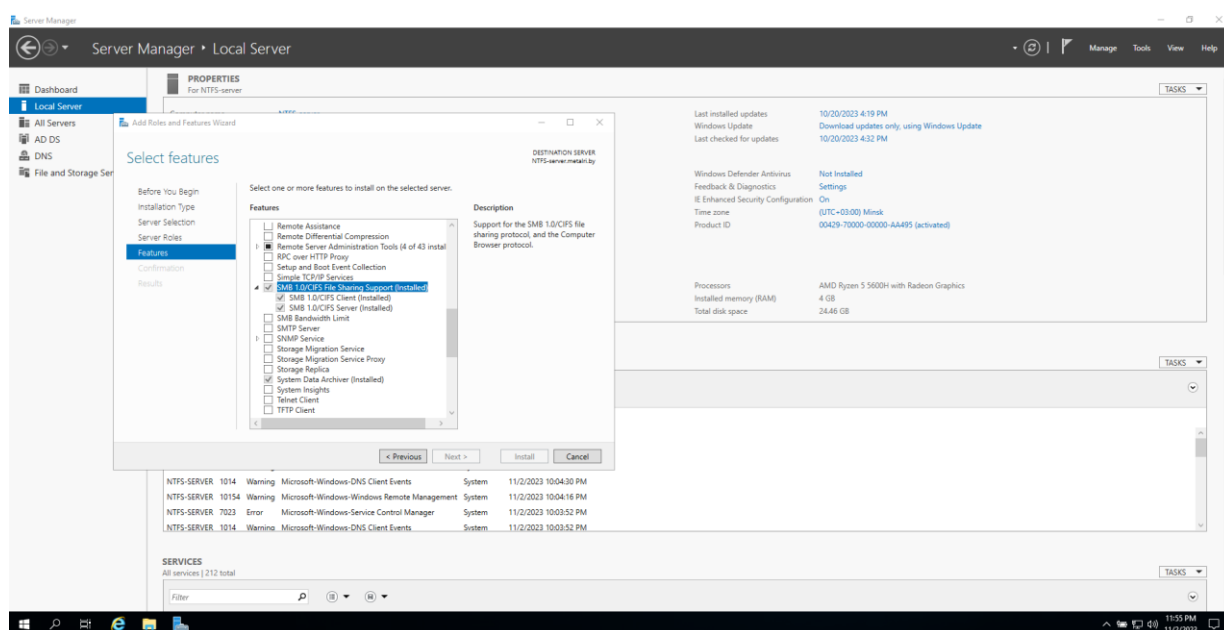


Рисунок 3.6.3 – Выбор «SMB File Sharing Support».

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

- 1) Переходим в «Tools», «Active Directory Users and Computers», «Groups».
- 2) Добавляем новую группу (рисунок 3.6.4). Назначаем имя.
- 3) Переходим во вкладку «Users». Создаём нового пользователя по такому же алгоритму. Назначаем компьютеру пользователя, а пользователю – группу. (рисунок 3.6.5)

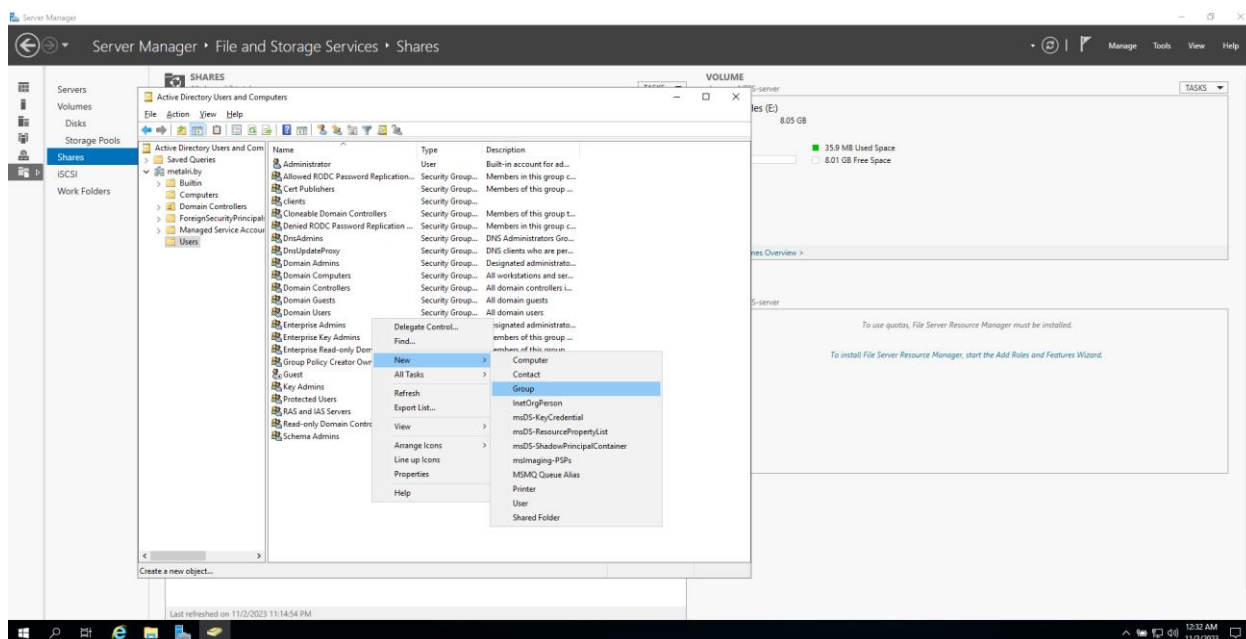


Рисунок 3.6.4 – Добавление новой группы пользователей.

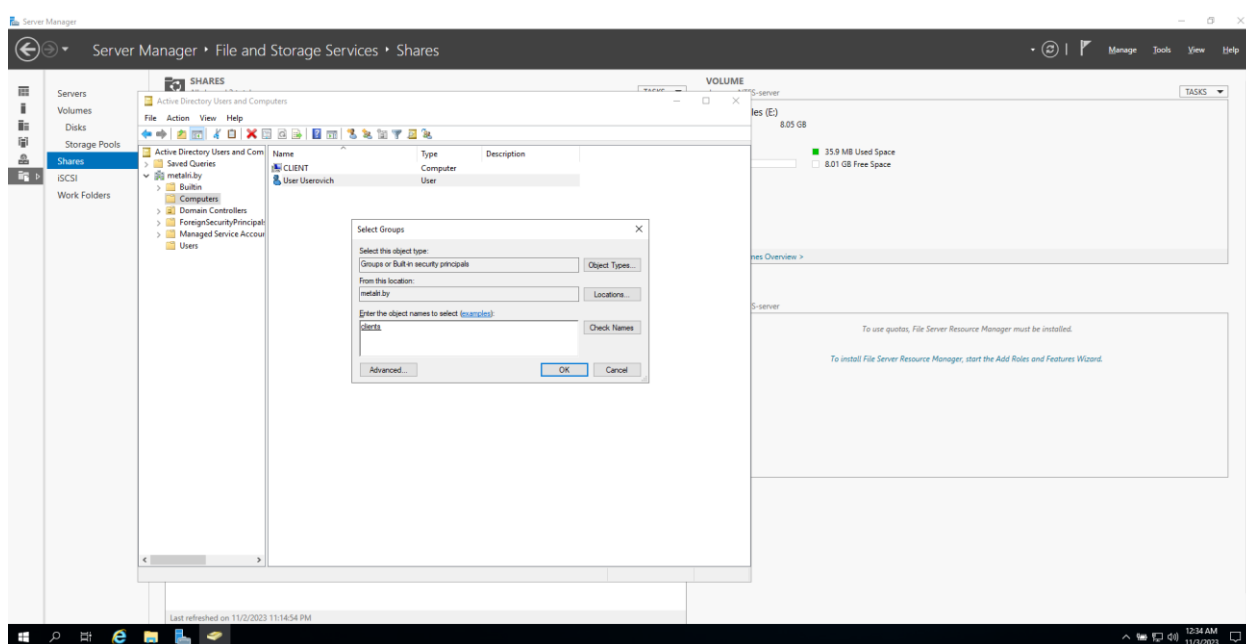


Рисунок 3.6.5 – Добавление назначение пользователя в группу.

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 деления пространства (рисунки 3.6.7 – 3.6.8).

После этого наш сервер готов к работе и политики настроены.

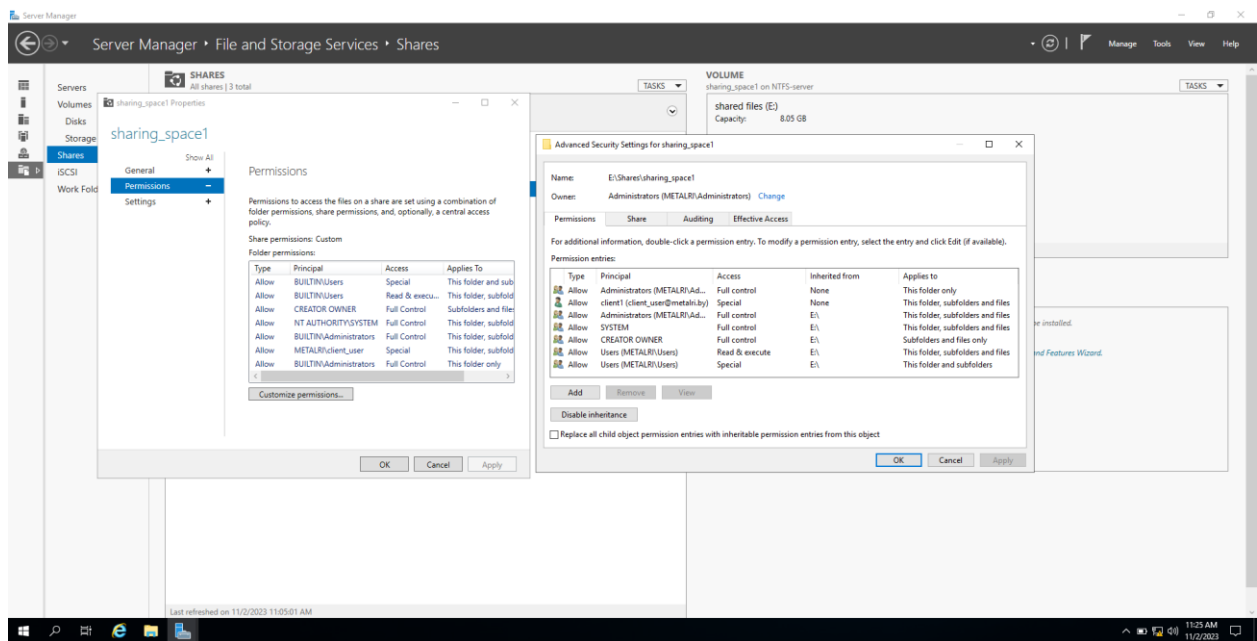


Рисунок 3.6.6 – Конфигурация разрешений.

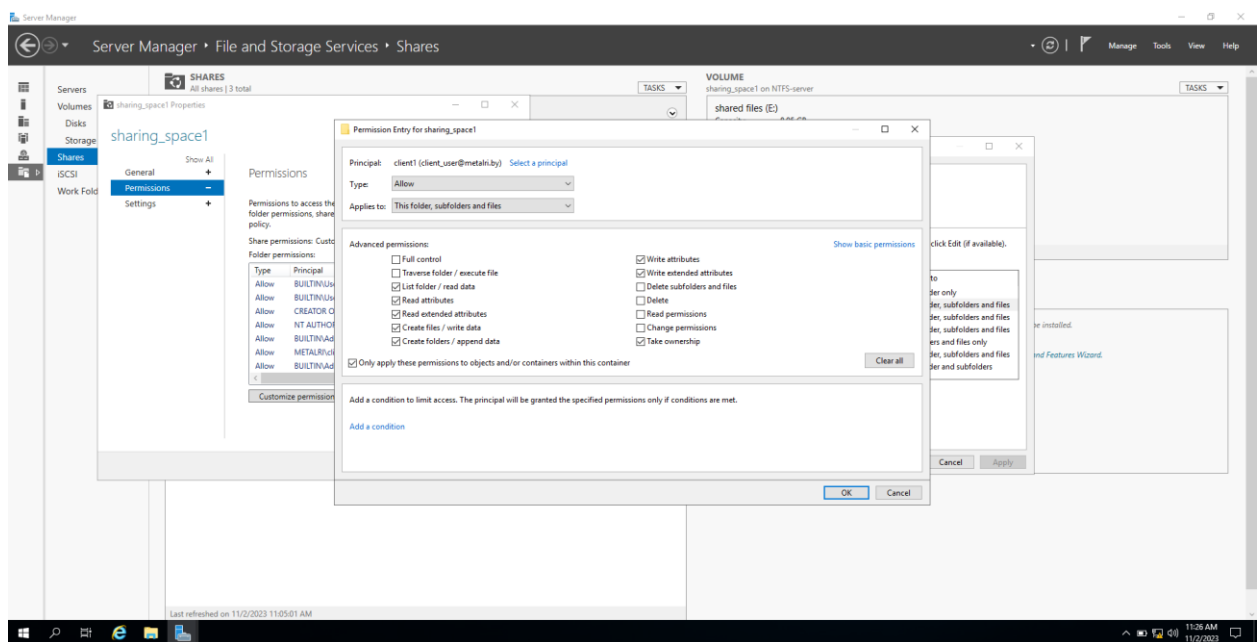


Рисунок 3.6.7 – Конфигурация разрешений.

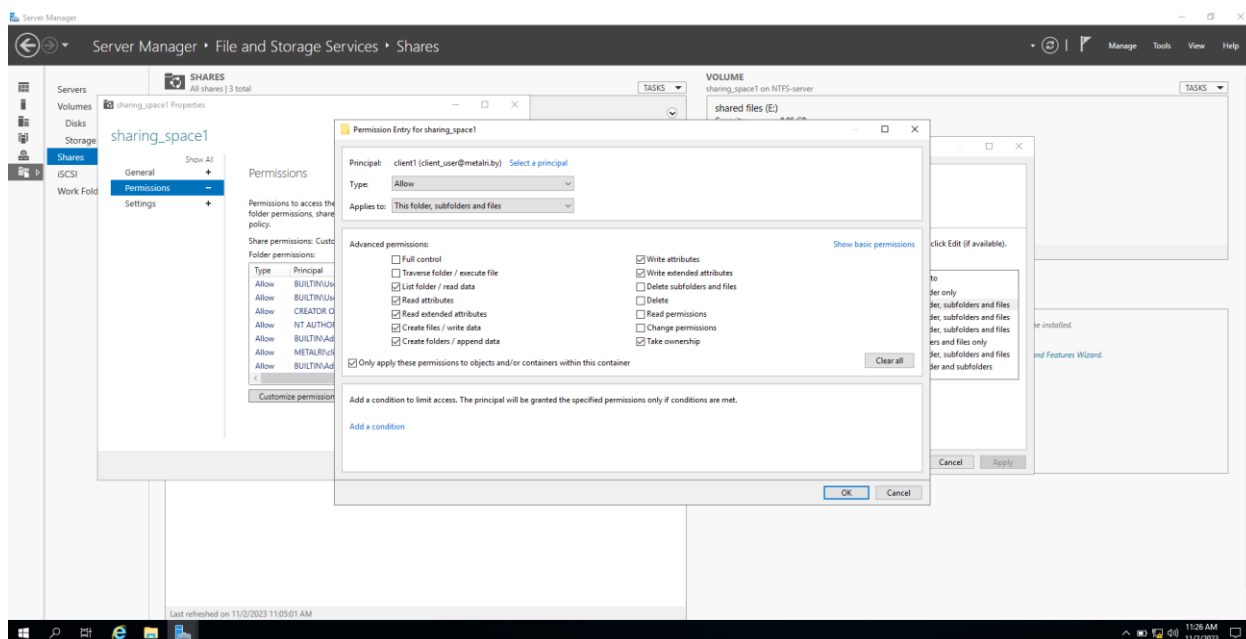


Рисунок 3.6.8 – конфигурация разделяемой политики.

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.

Сопоставления устройств, виртуальных ЛКС, адресов и масок показаны в таблице 3.8.1

Таблица 3.8.1 – таблица адресации в локальной сети

Устройство	VLAN	IP-адрес	Маска подсети
Рабочие станции дирекции и учёного совета	10	192.168.0.11 ... 192.168.0.14 FD10::	255.255.255.0 /64
DHCP-пул мобильных подключений для дирекции и ученого совета		192.168.0.40 ... 192.168.0.50	255.255.255.0
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 FD11::	255.255.255.0 /64
DHCP-пул мобильных подключений для исследовательского и производственного отдела		192.168.1.40 ... 192.168.1.50	255.255.255.0
WLAN-интерфейс WLC		192.168.1.4	255.255.255.0

Продолжение таблицы 3.8.1 – таблица адресации в локальной сети

Рабочие станции бухгалтерии и отдела продаж и обслуживания	12	192.168.2.10 ... 192.168.2.12 FD12::	255.255.255.0 /64
DHCP-пул мобильных подключений для бухгалтерии и отдела продаж и обслуживания		192.168.2.40 ... 192.168.2.50	255.255.255.0
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 FD13::	255.255.255.0 /64
WLAN-интерфейс WLC		192.168.3.4	255.255.255.0
Административный отдел	20	192.168.20.10 FD20::	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 FD30::	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

```
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
```


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 FD10::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 FD11::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 FD12::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 FD13::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 FD20::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 FD30::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#ip nat inside
```

3) Настройка access-листов. Запрещаем трафик между VLAN-ами, кроме трафика между пользователями и сервером.

```
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 10 remark access list for VLAN 10.
Router(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 10 deny 192.168.2.0 0.0.0.255
Router(config)#access-list 10 deny 192.168.3.0 0.0.0.255
Router(config)#access-list 10 permit any
Router(config)#access-list 11 remark Access list for VLAN 11.
Router(config)#access-list 11 deny 192.168.0.0 0.0.0.255
Router(config)#access-list 11 deny 192.168.2.0 0.0.0.255
Router(config)#access-list 11 deny 192.168.3.0 0.0.0.255
Router(config)#access-list 11 permit any
Router(config)#access-list 12 remark Access list for VLAN 12.
Router(config)#access-list 12 deny 192.168.0.0 0.0.255.255
Router(config)#access-list 12 deny 192.168.1.0 0.0.255.255
Router(config)#access-list 12 deny 192.168.3.0 0.0.255.255
Router(config)#access-list 12 permit any
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 g0/0/0.10
Router(config-subif)#ip access-group 10 out
Router(config-subif)#interface g0/0/0.11
Router(config-subif)#ip access-group 11 out
Router(config-subif)#interface g0/0/0.12
Router(config-subif)#ip access-group 12 out
Router(config-subif)#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)#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) 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 server

```

2) 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
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(config)#ip dhcp pool guests
Switch(dhcp-config)#network 192.168.3.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.3.1
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
Switch(dhcp-config)#interface vlan 13
Switch(config-if)#ip address 192.168.3.5 255.255.255.0

```

3) 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

```

4) Назначение ролей портов

```

Switch(config)#interface range gigabitEthernet0/1-3
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 gigabitEthernet0/25-28
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)#interface range gigabitEthernet0/30
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#interface range gigabitEthernet0/31
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: 4-9, 17-20, 23-24, 28-29, 32-39 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.

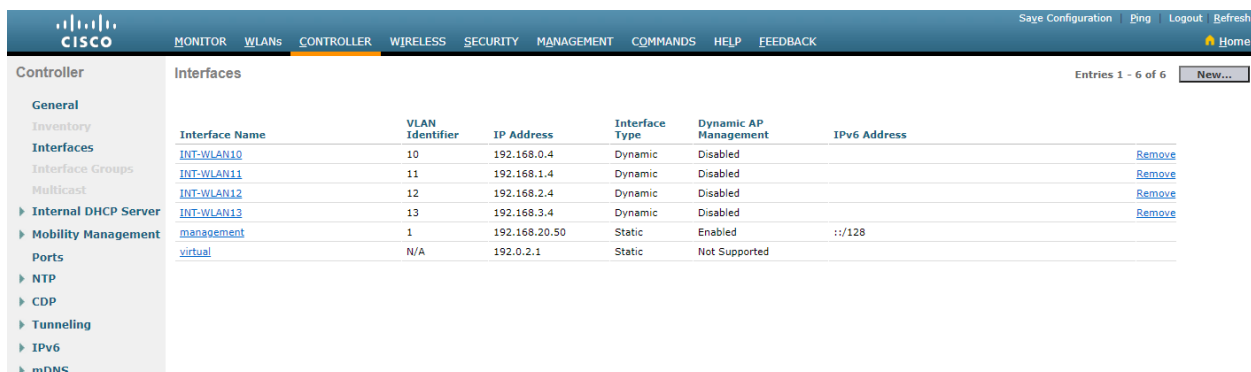
```
AP(config)#capwap ap controller ip address 192.168.20.50
```

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	
INT-WLAN11	11	192.168.1.4	Dynamic	Disabled	
INT-WLAN12	12	192.168.2.4	Dynamic	Disabled	
INT-WLAN13	13	192.168.3.4	Dynamic	Disabled	
management	1	192.168.20.50	Static	Enabled	::1/128
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-scope отображены на рисунке 3.9.4.

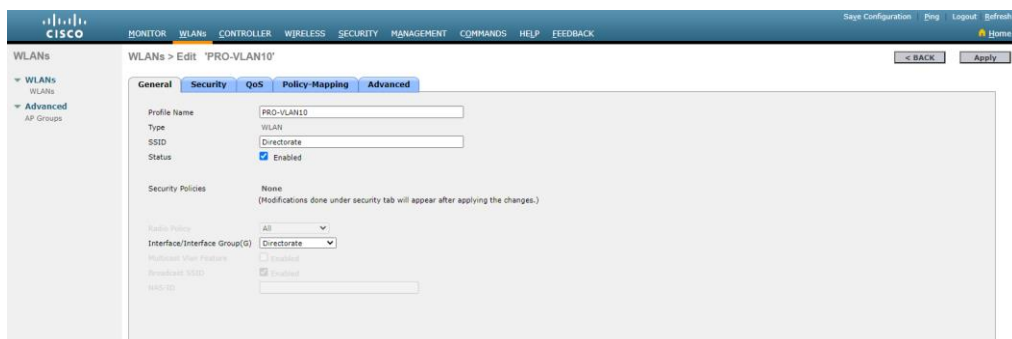


Рисунок 3.9.2 – конфигурация интерфейса и WLAN.

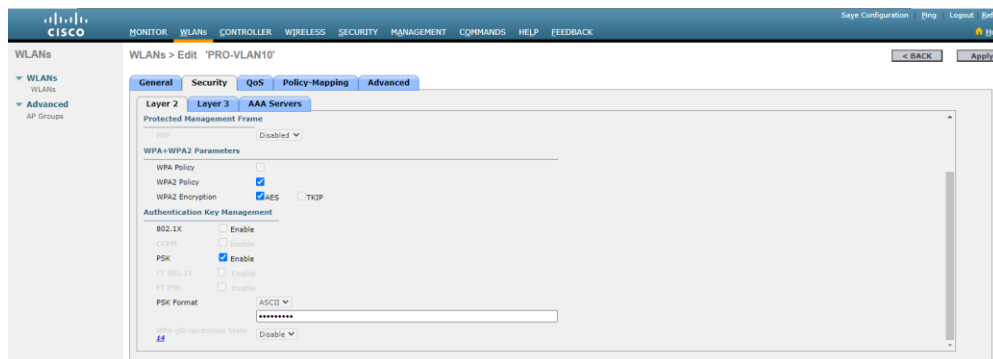


Рисунок 3.9.3 – конфигурация безопасности WLAN.

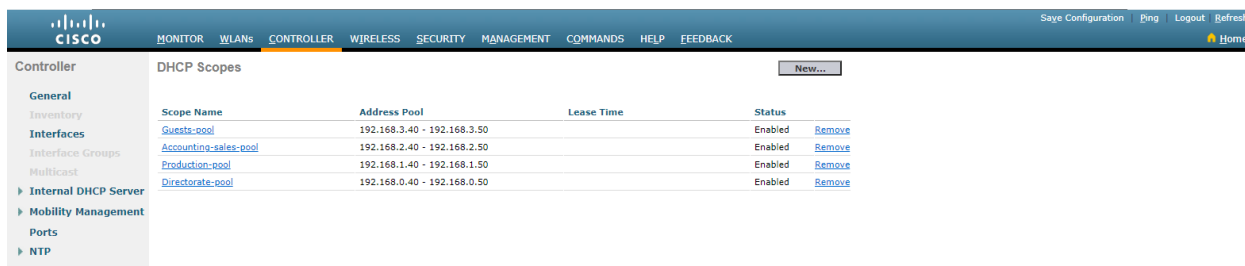


Рисунок 3.9.4 – созданные DHCP-scope.

После назначения пулов необходимо перейти во вкладку «Controller» -> «Interfaces», и во всех интерфейсах адресом DHCP-сервера указать свой же адрес. После данного шага точки, подключаемые к данному контроллеру, будут иметь 4 WiFi сети: Guests, Accounting-Sales, Production, Directorate. 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.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

ЗАКЛЮЧЕНИЕ

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]. – Электронный 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] Драйвера для принтера Kyocera P3145DN [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://www.kyoceradocumentsolutions.eu/en/support/downloads.name-L2V1L2VuL3ByaW50ZXJzL0VDT1NZU1AzMTQ1RE4=.html>
- [5] 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
- [6] Характеристики маршрутизатора Cisco ISR4431 [Электронный ресурс]. – Электронный данные. – Режим доступа: <https://www.cisco-russia.ru.com/routers/cisco-isr4431-v-k9>
- [7] Характеристики маршрутизаторов 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>
- [8] 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
- [9] 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>
- [10] 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
- [11] 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>
- [12] 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

[13] «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>

[14] Драйвера Lenovo ThinkSystem [Электронный ресурс]. – Электронные данные. – Режим доступа: <https://windows-server.lenovo.com/repo/latest/>

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

ПРИЛОЖЕНИЕ А
(Обязательное)

Схема СКС структурная

ПРИЛОЖЕНИЕ Б
(Обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(Обязательное)

План этажа. Схема монтажная

ПРИЛОЖЕНИЕ Г
(Обязательное)

Перечень оборудования, изделий и материалов

ПРИЛОЖЕНИЕ Д
(Обязательное)

Ведомость документов