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 114

БГУИР КП 1-40 02 01 01 429 ПЗ

Студент Р.А. Якунин

Руководитель А.В. Русакович

МИНСК 2023

Вариант	114
Объект	небольшая обувная компания
Форма здания, этажи, суммарная площадь помещений в квадратных метрах	п-образная, 1, 330
Количество стационарных пользователей (ПК), количество стационарных подключений, количество мобильных подключений	15, 16, 16
Сервисы (дополнительные подключения)	нет
Прочее оконечное оборудование (дополнительные подключения)	принтеры, сканеры
Подключение к Internet	DOCSIS
Внешняя адресация IPv4, внутренняя адресация IPv4, адресация IPv6	внешний IPv4-адрес автоматически назначает провайдер, публичная подсеть, доступ в Internet, использовать подсеть из блока адресов для Беларуси
Безопасность	IPsec-VPN для удаленного подразделения
Надежность	надежность хранения данных
Финансы	полноценная коммерческая сеть
Производитель сетевого оборудования	Cisco
Дополнительные требования заказчика	экологичность

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В наше время каждое предприятие или компания имеет потребность в локальной компьютерной сети, что является неотъемлемым инструментом для обеспечения гармоничного взаимодействия всех сотрудников компании, обеспечения оперативного доступа к актуальной информации и эффективной совместной работы.

Целью этого курсового проекта является разработка локальной компьютерной сети для небольшой обувной компании. Ключевыми целями в ее разработке являются: реализация всех предопределенных заказчиком требований (бюджет, количество возможных подключений, предпочтения по безопасности и скорости), грамотная реализация архитектуры сети, стабильность и бесперебойность работы для комфортной работы каждого сотрудника.

Для реализации данного курсового проекта следует учесть следующие требования: архитектуру здания, а также плотность и ширину стен для расчета проходимости сигнала по всей площади помещения. Стоит учесть количество стационарных пользователей, количество стационарных подключений, количество мобильных подключений, в том числе прочее оконечное оборудование.

Безопасность компьютерной локальной сети имеет первостепенное значение, поскольку она защищает конфиденциальные данные компании, предотвращает несанкционированный доступ и минимизирует риск утечек информации. Важно обеспечить надежные меры защиты, чтобы сохранить репутацию, уверенность клиентов и предотвратить потенциальные проблемы. Для проектирования данной компьютерной сети особое внимание следует уделить надежности хранения данных, а также стоит учесть требование заказчика в необходимости IPsec-VPN для удаленного подразделения.

При выборе сетевого оборудования будет использоваться производитель Cisco, который является одним из ведущих мировых производителей сетевого оборудования, обладая долгой историей и сильной репутацией. Cisco предлагает широкий спектр продуктов и решений для сетевой инфраструктуры, что позволяет выбрать наилучшие варианты под текущие требования заказчика.

Резюмируя поставленную цель были выделены следующие задачи:

1. Изучить материала по заданию на проект.
2. Разработать структуру сети и структурную схему.
3. Подобрать устройства с обоснованием их выбора.
4. Составить функциональную схемы.
5. Сделать выводы и написать руководство пользователя.

1 ОБЗОР ЛИТЕРАТУРЫ

1.1 DOCSIS

DOCSIS (Data Over Cable Service Interface Specification [1]) – это стандарт, разработанный для передачи данных, голоса и видео по кабельным телевизионным сетям. DOCSIS используется провайдерами кабельного интернета и кабельного телевидения для обеспечения доступа в Интернет и услуги цифрового телевидения.

DOCSIS определяет спецификации для физического уровня (такие как способы модуляции и частотные диапазоны) и уровня канального доступа, а также управления и конфигурации сети. Стандарт DOCSIS разработан для работы с сетями, которые используют коаксиальные кабели.

Эта делится по видам спецификаций. Деление проводится по порядку выхода обновлений с дополнительными функциями. Различия между видами определяются критериями качества обслуживания (QoS), емкостью потока, модуляциями, помехоустойчивостью. EuroDOCSIS – адаптация стандарта под европейскую сетку частот. Скорость передачи данных в разных версиях технологии см. в таблице 1.1.

Таблица 1.1 - сравнение характеристик рассматриваемых точек доступа.

Версия	DOCSIS		EuroDOCSIS	
	Прямой канал (Down) Мбит/с	Обратный канал (Up) Мбит/с	Прямой канал (Down) Мбит/с	Обратный канал (Up) Мбит/с
1.x	42,88 (38)	10,24 (9)	55,62 (50)	10,24 (9)
2.0	42,88 (38)	30,72 (27)	55,62 (50)	30,72 (27)
3.0 4-channel	+171,52 (+152)	+122,88 (+108)	+222,48 (+200)	+122,88 (+108)
3.0 8-channel	+343,04 (+304)	+122,88 (+108)	+444,96 (+400)	+122,88 (+108)
3.1	10000	2000	10000	2000
4.0	10000	10000	10000	10000

1.2 IPsec-VPN

В общем виде VPN представляет собой совокупность технологий управления доступом и контролем, аутентификации, туннелирования, используемых для защиты и безопасной передачи данных через сеть Интернет.

Использование туннелирования обеспечивает безопасность при передаче данных. При этом при передаче пакетов из одной сети сообщения инкапсулируются в пакеты другой сети. Туннелирование необходимо из-за того, что в сетях, использующих протокол IP, имеются уязвимости. Во время разработки протокола IP на его уровне не были предусмотрены какие-либо функции безопасности, что позволят легко подделать и перехватить данные в сетях, использующих данный протокол.

Независимо от того, какую форму VPN выберет организация, конечный результат всегда будет одинаковым. VPN создают «туннели» через незащищенные публичные сети, чтобы установить безопасные соединения с частной сетью. Используя стандартные, но надежные средства безопасности, такие как шифрование данных и аутентификация конечных точек, VPN могут предотвращать несанкционированный доступ к этим туннелям и к сети организации на другом конце.

IPSec (IP Security) является набором протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищенного обмена ключами в сети Интернет. В основном применяется для VPN-соединений организаций.

IPSec-VPN изначально предназначался для подключения типа «точка-точка» и предполагал удаленный доступ к сети через стандартный клиент или приложение. Эти VPN были в основном разработаны для постоянных удаленных сайтов для доступа к одной центральной сети.

Преимуществами IPSec VPN являются, во-первых, постоянная связь между локациями, во-вторых, поскольку IPSec работает на «уровне протокола» Интернета, то любой протокол на основе IP может быть отправлен через сеть. Это означает, что можно использовать IPSec приложений данных, использующих протоколы TCP и UDP.

2 РАЗРАБОТКА СТРУКТУРНОЙ СХЕМЫ

В данном разделе приведено описание структуры локальной компьютерной сети. Схема структурная приведена в приложении А.

Структурное проектирование требуется для схематичного изображения модели локальной компьютерной сети. Структурная схема дает возможность разделить локальную компьютерную сеть на некоторые условный логические блоки взаимосвязанные друг с другом.

Благодаря этому подходу, можно условно составить структуру сети и общий план действий по ее созданию, не углубляясь в физическую реализацию.

В ходе проектирования выделены следующие блоки:

- блок маршрутизации
- блок коммутации
- блок оконечных устройств
- блок точек доступа
- блок мобильных оконечных устройств
- блок выхода в интернет

Всего предполагается организовать 16 стационарных подключений из которых 15 - стационарных пользователей. А также 16 мобильных подключениях. Помимо вышеперечисленных подключений к локальной компьютерной сети будут подключены принтеры и сканеры.

2.1 Блок маршрутизации

Блок маршрутизации представляет важный компонент в инфраструктуре локальной компьютерной сети организации. Этот блок отвечает за маршрутизацию данных внутри организации и обеспечивает доступ к Интернету для всех устройств, подключенных к сети.

Для достижения этой цели можно воспользоваться как L3-коммутатором, так и маршрутизатором. Однако, заказчик поставил требование реализовать технологию IPsec-VPN, которая, доступна только на маршрутизаторах. Таким образом за реализацию маршрутизации был выбран маршрутизатор.

Маршрутизаторы этого блока соединены с поставщиком интернет-услуг, что обеспечивает организации доступ к глобальной сети, а также

связаны с блоком коммутации, обеспечивая передачу данных между всеми устройствами внутри локальной сети.

Таким образом, блок маршрутизации является неотъемлемой частью сети, обеспечивая ее связность, безопасность и доступность. Это позволяет всем устройствам в организации успешно взаимодействовать друг с другом и с внешним миром.

2.2 Блок коммутации

Блок коммутации тесно взаимодействует с остальными компонентами сети, обеспечивая надежную передачу данных внутри организации. Блок коммутации состоит из коммутатора. Взаимодействие блока коммутации с другими сетевыми компонентами включает в себя пересылку данных от маршрутизаторов через коммутаторы к конечным устройствам, а также обеспечение подключения точек доступа для беспроводного доступа к сети.

По блок-схеме, блок коммутации взаимодействует с блоком оконечных устройств. Здесь каждый коммутатор связан с группой стационарных ПК и принтеров, представленных в составе блока оконечных устройств. Коммутаторы в этом контексте обеспечивают связанность и коммутацию данных между персональными компьютерами и принтерами внутри организации. Это обеспечивает сотрудникам возможность обмена информацией, совместной работы в сети и печати документов без затруднений.

Следующим блоком, взаимодействующим с блоком коммутации, является блок точек доступа. Этот блок предоставляет беспроводное подключение для устройств, таких как ноутбуки и мобильные устройства. Коммутаторы активно взаимодействует с точками доступа, обеспечивая беспроводное соединение для сотрудников.

Блок коммутации, таким образом, является неотъемлемой частью сети организации, обеспечивая ее функциональность, расширяемость и эффективность. Все вышеперечисленные блоки тесно взаимодействуют с блоком коммутации, что обеспечивает бесперебойную работу сети и соответствие потребностям современной корпоративной среды.

2.3 Блок оконечных устройство

В контексте локальной компьютерной сети организации, этот блок представляет собой комплекс компьютеров и принтеров, которые соединены

с сетью через коммутаторы. Эти оконечные устройства выполняют разнообразные задачи в сети и активно взаимодействуют между собой, а также с другими компонентами сети. ПК в рамках этого блока являются рабочими станциями для сотрудников организации. Они используются для выполнения различных задач, таких как создание и редактирование документов, отправка и прием электронной почты, использование прикладных программ и доступ в Интернет. Взаимодействие ПК между собой и с другими устройствами включает передачу и прием данных по сети.

ПК взаимодействуют напрямую между собой, используя коммутаторы. Они могут обмениваться данными, использовать общие сетевые ресурсы, такие как общие папки, общие принтеры и сканеры, а также совместно работать над проектами и заданиями. Принтеры и сканеры подключенные к коммутаторам, доступны всем ПК в этом блоке, что упрощает процесс печати документов.

2.4 Блок точек доступа

Блок точек доступа в рамках организации составляет центральную часть беспроводной инфраструктуры, обеспечивая беспроводное соединение для устройств, поддерживающих Wi-Fi технологии.

Точки доступа представляют собой устройства, реализующие технологию Wi-Fi и предоставляющие возможность устройствам подключаться к сети без применения физических соединений. Эти точки доступа размещаются в разных частях здания таким образом, чтобы обеспечивать равномерное охватывание беспроводной сети Wi-Fi внутри помещения. Они соединены с сетевыми коммутаторами и осуществляют связь между беспроводными устройствами и проводной локальной сетью.

Блок беспроводной сети обеспечивает беспроводный доступ к сети для беспроводных устройств, включая ноутбуки, смартфоны, планшеты и другие устройства, поддерживающие технологию Wi-Fi. Эти устройства могут подключаться к беспроводной сети, используя точки доступа, и получать доступ к ресурсам сети, включая доступ в Интернет и общие файлы.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

Данный раздел посвящен проектированию и описанию функциональной схемы, а также выбору оборудования для локальной компьютерной сети, которая будет реализована.

В приложении Б представлена функциональная схема с условно-графическими обозначениями.

3.1 Сведения об используемом оборудовании

При построении локальной компьютерной сети используется следующее оборудование: маршрутизатор, коммутатор, беспроводные точки доступа, моноблоки, также принтер и сканеры.

Также, необходимо учесть, что оборудование должно приобретаться фирмы Cisco, поскольку это требование заказчика.

В следующих подразделах описано обоснование выбора конкретных моделей перечисленного оборудования.

3.1.1 Обоснование выбора пользовательских станций

По заданию требуется обеспечить компьютерную сеть пятнадцатью стационарными пользовательскими станциями. Предполагается использование станций для работы с текстовыми редакторами, редакторами таблиц и прочим офисным программным обеспечением. Как следствие имеет смысл рассматривать сегмент рынка, рекомендованный для офисных решений. Конкретных требований к комплектующим по заданию не наложено, как следствие наиболее удобным решением будет покупка готовых сборок, представленных на рынке широкого потребления. Это исключит надобность в изучении совместимости комплектующих при создании индивидуальной сборки.

Был выбран ПК MultiOffice 5C104FD8H1G103S50H [4] из-за средней цены 1500 BYN, а также приемлемой конфигурации.

Характеристики ПК:

1. Процессор Intel Core i5 10400F с 6 ядрами и тактовой частотой 2900МГц.
2. 8 ГБ DDR4 оперативной памяти с частотой 2666 МГц
3. HDD накопитель емкостью 1000 ГБ и скоростью вращения 7200 RPM.
4. Графического адаптера NVIDIA GeForce GT.

3.1.2 Обоснование выбора пользовательской операционной системы

В качестве операционной системы для пользовательских станций и была выбрана ОС Windows 10. Windows 10 является самой популярной настольной операционной системой. Поэтому большинству пользователей будет удобнее и привычнее работать именно с этой операционной системой.

3.1.3 Обоснование выбора принтера и сканера

В процессе поиска принтера выбор пал на HP OfficeJet Pro 7720 [5]. Он имеет среднюю стоимость 1,500 BYN, а также имеет в себе встроенный сканер, что облегчит работу сотрудникам. HP OfficeJet Pro 7740 струйный принтер, печатающим формат А3. Такой формат будет удобен для самостоятельной печати рекламных баннеров компании.

Для подключения принтер имеет порт Ethernet, USB и возможность подключиться по беспроводному интерфейсу Wi-Fi.

3.1.4 Обоснование выбора модема

В качестве наиболее рационального решения можно было бы рассмотреть возможность отказаться от модема и использовать маршрутизатор с расширением-модемом для DOCSIS, однако подобные маршрутизаторы более не выпускаются производителем CISCO.

Единственным критерием выбора в таком случае остается поддержка модемом технологии DOCSIS. Из-за устаревания технологии выбор модемов на рынке крайне мал, большинство устройств совмещают в себе как функцию модема, так и маршрутизатора или беспроводного маршрутизатора. Так как необходимость в таком дополнительном функционале отсутствует, рациональным выбором будет модель DPC3008 [7] от компании Cisco. Стоимость данной модели составляет 150 BYN.

Технические характеристики:

1. совместимость с DOCSIS 3.0, что позволяет поддерживать более высокие скорости передачи данных по сравнению с более старыми версиями DOCSIS;

2. поддерживает скорость передачи данных до 340 Мбит/сек Download и до 120 Мбит/сек Upload;

3. предоставляет один порт Ethernet, который может быть использован для подключения к компьютеру или маршрутизатору;

3.1.5 Обоснование выбора маршрутизатора

Основными критериями при выборе маршрутизатора являются: достаточное количество портов со стороны LAN, поддержка VPN, поддержка IPv6-маршрутизации.

Требуется 1 порт LAN к коммутатору и 1 WAN для подключения к глобальной сети, однако, учитывая возможность расширении сети, следует рассматривать модели с большим количеством портов. Также учитывая устаревание технологии DOCSIS, не стоит выбирать маршрутизатор с низкой скоростью внешнего подключения, так как при будущей модернизации системы, это может стать причиной общей низкой скорости доступа к сети Интернет из проектируемой локальной компьютерной сети.

Из моделей доступных на территории РБ были выбраны 2 аналога C1121-4P и C1113-8P, их сравнение приведено в таблице 3.1.

Таблица 3.1 – сравнение характеристик маршрутизаторов.

Маршрутизатор	Cisco C1121-4P GE	Cisco C1113-8P GE
Поддержка IPSec	Да	Да
Ethernet порты	4 x 100/1000 RJ-45 Gigabit Ethernet ports 1 x WAN	8 x 100/1000 RJ-45 Gigabit Ethernet ports 2 x WAN
Потребляемая мощность, Вт	58	60
Объем ОЗУ	4 Гб	4 Гб
Поддержка IPv6	Да	Да
Поддержка IPsec VPN	Да	Да
Power over Ethernet (PoE)	Да	Да

Согласно этим критериями была выбрана модель Cisco C1121-4P 4xLAN GbE 1xWAN GbE 1xUSB 3.0 [8], с стоимостью 11,500 BYN.

Выбор пал на него, так как он имеет оптимальное количества LAN портов, в отличии от излишнего количества в аналоге.

3.1.6 Обоснование выбора коммутатора

Для сети потребуется коммутатор с минимум 19 портами, но следует выделить среди критериев выбора большее количество LAN-портов для возможности дальнейшего расширения сети. Так же не имеет смысла рассматривать L3-коммутаторы, так как дополнительный функционал, который отличает их от L2-коммутаторов уже присутствует на

маршрутизаторе. Хоть существующая максимальная скорость восходящего потока низка, стоит предусмотреть в коммутаторах GigabitEthernet порты, так как в перспективе возможен переход сети на более быструю технологию доступа к Интранету.

Сравнение аналогов приведено в таблице 3.2

Таблица 3.2 – сравнение характеристик коммутаторов.

Коммутатор	Cisco C1000-24T-4G-L	Cisco C1000-24T-4X-L
Поддержка IPSec	Да	Да
Ethernet порты	24 x 100/1000 RJ-45 Gigabit Ethernet ports 4 x SFP (Gigabit Ethernet)	24 x 100/1000 RJ-45 Gigabit Ethernet ports 4 x 10 Gigabit Ethernet (10GBase-X)
Power over Ethernet (PoE)	Да	Да
Объем ОЗУ	512 Мб	512 Мб
FLASH	256 Мб	256 Мб

Аналоги имеют одно различие: 4 SFP и 4 10GE порты. Так как ни тот, ни другой тип соединения по заданию не требуется, следует сделать выбор какая из технологий в будущем может оказаться более полезной заказчику.

Согласно этим критериями была выбрана модель Cisco C1000-24T-4X-L [9], стоимость которого равной 10,500 BYN, так как 10GE соединение способно реализовать большую скорость передачи данных при необходимости в будущем использовать устройств, требующих высокоскоростных соединений.

3.1.7 Обоснование выбора точки беспроводного доступа

Для снижения нагрузки на коммутатор и отказа от покупки контроллера точек доступа решено использовать точки доступа со встроенным контроллером.

Имеет смысл рассматривать точки доступа из серий, рекомендованных Cisco для развертывания BSS для малого бизнеса. Такими являются модели серии Cisco Aironet. С учетом вышеописанных требований из данных семейств подходят по требованиям модели C9115AXI-EWC-I и AIR-AP2802I-E-K9.

Сравнение аналогов приведено в таблице 3.3

Таблица 3.3 - сравнение характеристик рассматриваемых точек доступа.

Наименование	C9115AXI-EWC-I	AIR-AP2802I-E-K9
Мощность, Вт	20,4	13,9
Максимальная мощность передачи 2,4 GHz, дБм	23	27
Максимальное количество подключений	Не указана в спецификации	200
Power over Ethernet (PoE)	Да	Да
Протокол безопасности	802.11i, Wi-Fi Protected Access 3 (WPA3), WPA2, WPA	802.11ac, WPA3, WPA2, WPA

В приведен анализ требуемых характеристик вышеуказанных точек доступа. В данном случае ля модели C9115AXI-EWC-I не специфицировано максимальное количество подключений, а также имеет меньшую мощность сигнала, поэтому в качестве точки доступа выбрана модель AIR-AP2802I-E-K9 [10]. Цена устройства составляет 5,600 BYN.

Точка доступа также обладает следующими характеристиками:

1. 1 RJ-45 GigabitEthernet POE порт;
2. Поддержка 2.4 ГГц частот;
4. 1024 Мб FLASH, 2048 Мб объем ОЗУ;

3.1.8 Обоснование выбора расходного материала

Исходя из требования установки оборудования в виде скрытого монтажа были выбраны следующие расходные материалы:

1. информационная розетка Schneider Electric Glossa GSL000181K;
2. витая пара UTP cat.5E 4x2x24AWG;
3. кабельный короб 24x25 «ECOLINE».

Данные расходные материалы понадобятся для объединения всей инфраструктуры сети. Также розетки изготовлены из материалов, способствующих уменьшению отходов и обладающих возможностью повторной переработки, что способствует сокращению воздействия на окружающую среду.

Также все сетевое оборудование поддерживание Power over Ethernet (PoE). Эта технология дает возможность питать устройство посредствам Ethernet кабеля. PoE может снижать потребление энергии за счет сокращения

использования дополнительных кабелей и устройств для подачи питания к устройствам. Одна инфраструктура (Ethernet-кабель) может обеспечивать энергию и данные, что может уменьшить потребление электроэнергии.

3.2 Адресное пространство

Основными требованиями заказчика в проектировании адресного пространства локальной компьютерной сети являются: внешний IPv4-адрес автоматически назначает провайдер, внутренняя IPv4-адресация должна использовать публичную подсети, IPv6-адресация должна быть реализована с использованием подсети из блока адресов для Беларуси.

Исходя из этих требований очевидно, что общение между оконечными и сетевыми устройствами должно происходить посредством публичной IPv4-подсети. А IPv6-подсеть используется для выхода в Internet.

Согласно варианту, существует выбор из семи подсетей. Подсети в нотации Classless Inter-Domain Routing (далее – CIDR) и количество доступных адресов для конечных устройств приведены в таблице 3.4

Таблица 3.4 – предлагаемые подсети в нотации CIDR

№	Адрес подсети	Длина маски в битах	Количество хостов
1	17.128.0.0	9	8,388,606
2	47.174.192.9	19	8,190
3	129.142.160.0	19	8,190
4	152.2.224.0	20	4,094
5	172.201.37.0	25	126
6	97.252.255.0	26	62
7	84.214.211.224	28	14

Локальная компьютерная сеть предусматривает следующее количество устройств:

— маршрутизатор — 1;

— коммутатор — 1;

— точка доступа — 1;

— принтер-сканнер — 1;

— стационарные подключения — 15;

— мобильные подключения — 16.

Общее количество устройств равно 35. Также при выборе подсети следует учесть, что в будущем сеть может быть расширена, поэтому не стоит

выбирать сеть с слишком малым адресным пространством, как у сеть и избыточно большим адресным пространством ввиду его ненадобности.

3.2.1 Внешняя IPv4 адресация

В нашем случае внешний IPv4-адреса назначается провайдером. Для демонстрации настройки оборудования данной локальной компьютерной сети был выбран адрес 18.24.102.1/30. Позже, при реальном воссоздании данной сети, адрес следует заменить на выданных провайдером.

3.2.2 Внутренняя IPv4 адресация

Для внутренней IPv4 адресации нужно использовать публичную подсеть. Под приватными подсетями принято считать:

1. 10.0.0.0/8 (то есть все что начинается на 10.);
2. 172.16.0.0/12 (то есть с 172.16.0.0 по 172.31.255.255 включительно);
3. 192.168.0.0/16 (то есть со 192.168.0.0 по 192.168.255.255 включительно).

Для внутренней адресации IPv4 стоит выбрать подсеть не входящую в эти диапазоны. Исходя из этого была выбрана подсеть 172.201.37.0/25, в рамках которой предусмотрено 126 хостов. Данная подсеть не входит в диапазоны приватных подсетей. Эта подсеть будет полностью покрывать все необходимые проводные и беспроводные подключения, а также имеет запас адресов для будущего расширения сети.

Исходя из ролей пользователей, которые имеют доступ к оборудованию, следует разделить подсеть на 4 подсети.

1. Пользовательская (пользовательские ПК, принтеры-сканнеры)
2. Беспроводная (точка доступа и беспроводные устройства)
3. Удаленные пользователи (для удаленного подразделения)
4. Административный (активное сетевое оборудование)

Схема внутренней адресации IPv4 представлена в таблице 3.5.

Таблица 3.5 — Схема внутренней адресации IPv4

VLAN	Назначение	Адрес подсети	Длина маски подсети, бит	Количество хостов
10	Пользовательский	172.201.37.0	27	30
20	Беспроводной	172.201.37.32	27	30
30	Удаленные пользователи	172.201.37.64	27	30
100	Административный	172.201.37.96	27	30

Маршрутизатор должен иметь доступ к каждой из подсетей, поэтому на его интерфейсе будет присутствовать адреса каждой из подсетей.

Для администрирования сети требуется каждому сетевому устройству выдать адрес из VLAN 100. С ними можно ознакомиться в таблице 3.6.

Таблица 3.6 - Адреса устройств для административной подсети.

Устройство	IP адрес	Маска подсети
Router	172.201.37.97	255.255.255.224
Switch	172.201.37.98	255.255.255.224
Admin-PC	172.201.37.99	255.255.255.224

Для пользовательской подсети требуется назначить адреса приведенные в таблице 3.7

Таблица 3.7 - Адреса устройств для пользовательской подсети.

Устройство	IP адрес	Маска подсети
Router	172.201.37.1	255.255.255.224
PC1	172.201.37.2	255.255.255.224
…	…	…
PC14	172.201.37.15	255.255.255.224
Printer	172.201.37.16	255.255.255.224
Switch	172.201.37.17	255.255.255.224

Для беспроводной подсети назначаем адреса приведенные в таблице 3.8

Таблица 3.8 - Адреса устройств для беспроводной подсети.

Устройство	IP адрес	Маска подсети
Router	172.201.37.33	255.255.255.224
Access Point	172.201.37.34	255.255.255.224
Wareless User1	172.201.37.35	255.255.255.224
…	…	…
Wareless User16	172.201.37.50	255.255.255.224
Switch	172.201.37.51	255.255.255.224

Так же для подсети с удаленными пользователями следует назначить следующие адреса (см. таблица 3.9).

Таблица 3.9 - Адреса устройств для подсети удаленных пользователей.

Устройство	IP адрес	Маска подсети
Router	172.201.37.65	255.255.255.224
Switch	172.201.37.66	255.255.255.224

3.2.3 IPv6 адресация

В соответствии с требованием заказчика, IPv6 адресация должна использовать подсеть из блока адресов для Беларуси и осуществлять доступ в Internet.

Для IPv6-подсети необходимо использовать Global Unicast адреса. При адресации локальной компьютерной сети IPv6 была выбрана подсеть 2001:500:3::/48, которая находится в блоке адресов для Беларуси.

Для адресации устройств эта сеть будет разбита на подсети, при этом subnet id будет выбран в соответствии с номером VLAN. Схема адресации IPv6 представлена в таблице 3.10.

Таблица 3.10 — Схема разбиения на подсети IPv6

VLAN	Назначение	Адрес подсети	Длина префикса
10	Пользовательский	2001:500:3:10::	64
20	Беспроводной	2001:500:3:20::	64
30	Удаленные пользователи	2001:500:3:30::	64
100	Административный	2001:500:3:100::	64

Следуя из данного делегирования сети на подсети следует, что устройствам, в соответствии с их VLAN, выданы адреса по аналогии с адресами IPv4 для сохранения целостной системы адресации и упрощения настройки (см. таблицы 3.11-3.14)

Таблица 3.11 — Схема адресации IPv6 административной подсети

Устройство	IPv6 адрес	Длина префикса
Router	2001:500:3:100::97	64
Switch	2001:500:3:100::98	64
Admin-PC	2001:500:3:100::99	64

Таблица 3.12 — Схема адресации IPv6 пользовательской подсети

Устройство	IPv6 адрес	Длина префикса
Router	2001:500:3:10::1	64
PC1	2001:500:3:10::2	64
…	…	…
PC14	2001:500:3:10::15	64
Printer	2001:500:3:10::16	64
Switch	2001:500:3:10::17	64

Таблица 3.13 — Схема адресации IPv6 беспроводной подсети

Устройство	IPv6 адрес	Длина префикса
Router	2001:500:3:20::33	64
Access Point	2001:500:3:20::34	64
Wareless User1	2001:500:3:20::35	64
…	…	…
Wareless User16	2001:500:3:20::50	64
Switch	2001:500:3:20::51	64

Таблица 3.14 — Схема адресации IPv6 подсети удаленных пользователей

Устройство	IPv6 адрес	Длина префикса
Router	2001:500:3:30::97	64
Switch	2001:500:3:20::98	64

3.3 Конфигурация сетевого оборудования

3.3.1 Настройка VLAN на коммутаторе

Для начала создадим виртуальные сети на коммутаторе. Для этого в режиме глобальной конфигурации задаем VLAN индексы из таблицы 3.3 с помощью команды:

```
Switch(config)#VLAN 10
Switch(config)#VLAN 20
Switch(config)#VLAN 30
Switch(config)#VLAN 100
```

Согласно функциональной схеме из приложения Б на интерфейсах коммутатора GigabitEthernet0/2-14 прописываем команды:

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 10
```

На интерфейсе GigabitEthernet0/15, который идет к компьютеру администратора, прописываем:

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 100
```

На интерфейсе GigabitEthernet0/17, который идет к точке беспроводного доступа, прописываем:

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 20
```

На интерфейсе GigabitEthernet0/18, который идет к маршрутизатору, прописываем следующие команды:

```
Switch(config-if)#switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30,100
```

Так же назначаем каждому VLAN адреса на коммутаторе:

```
Switch(config-if)#int VLAN 10
Switch(config-if)#ip address 172.201.37.17 255.255.255.224
Switch(config-if)#ipv6 address 2001:500:3:10::17/64

Switch(config-if)#int VLAN 20
Switch(config-if)#ip address 172.201.37.51 255.255.255.224
Switch(config-if)#ipv6 address 2001:500:3:20::51/64

Switch(config-if)#int VLAN 30
Switch(config-if)#ip address 172.201.37.66 255.255.255.224
Switch(config-if)#ipv6 address 2001:500:3:30::66/64

Switch(config-if)#int VLAN 100
Switch(config-if)#ip address 172.201.37.100 255.255.255.224
Switch(config-if)#ipv6 address 2001:500:3:100::100/64
```

3.3.2 Настройка маршрутизации между сетями

На маршрутизаторе разбиваем интерфейс, идущий к коммутатору, на 3 подинтерфейса.

Для подсети с стационарными подключениями прописываем:

```
Router(config)#int gigabitEthernet 0/2.10
Router(config-if)#encapsulation dot1q 10
Router(config-if)#ip address 172.201.37.1 255.255.255.224
Router(config-if)#ipv6 address 2001:500:3:10::1/64
```

Для подсети с беспроводными подключениями прописываем:

```
Router(config)#int gigabitEthernet 0/2.20
Router(config-if)#encapsulation dot1q 20
Router(config-if)#ip address 172.201.37.33 255.255.255.224
Router(config-if)#ipv6 address 2001:500:3:20::33/64
```

Для подсети удаленных пользователей прописываем:

```
Router(config)#int gigabitEthernet 0/2.30
Router(config-if)#encapsulation dot1q 30
Router(config-if)#ip address 172.201.37.65 255.255.255.224
Router(config-if)#ipv6 address 2001:500:3:30::65/64
```

Для административной подсети прописываем:

```
Router(config)#int gigabitEthernet 0/2.100
Router(config-if)#encapsulation dot1q 100
Router(config-if)#ip address 172.201.37.97 255.255.255.224
Router(config-if)#ipv6 address 2001:500:3:100::97/64
```

В рамках нашей задачи подсети предприятия не должна пересекаться с беспроводной, так как является гостевой. Также эти подсети должны иметь доступ в интернет. Поэтому для разграничения взаимодействия между подсетями настроим access листы.

Настройка производиться на центральном роутере.

Административный VLAN может общаться с кем угодно, поэтому для него ничего не создаем.ACL для подсети с PC:

```
Router(config)#ip access-list standart PC_VLAN10
Router(config-std-nacl)#deny 172.201.37.32 0.0.0.31
Router(config-std-nacl)#permit any
```

С помощью deny мы запрещаем общаться с подсетью с беспроводными устройствами. С помощью permit разрешает общаться со всем остальными

Привязываем access list к интерфейсу подсети:

```
Router(config)#int GigabitEthernet 0/2.10
Router(config-if)#ip access-group PC_VLAN10 out
```

Параметр out указывает на фильтрацию исходящего трафика. ACL для беспроводной подсети:

```
Router(config)#ip access-list standard Wi-Fi_VLAN20
Router(config-std-nacl)#deny 172.201.37.0 0.0.0.31
Router(config-std-nacl)#permit any
```

Тут запрещаем взаимодействовать с подсетями стационарных устройств. Привязываем к интерфейсу:

```
Router(config)#int GigabitEthernet 0/2.20
Router(config-if)#ip access-group Wi-Fi_VLAN20 out
```

ACL для удаленных пользователей:

```
Router(config)#ip access-list standard RemUs_VLAN30
Router(config-std-nacl)#deny 172.201.37.32 0.0.0.31
Router(config-std-nacl)#permit any
```

Тут запрещаем взаимодействовать с подсетью беспроводных устройств. Привязываем к интерфейсу:

```
Router(config)#int GigabitEthernet 0/2.30
Router(config-if)#ip access-group RemUs_VLAN40 out
```

3.3.3 Настройка административной подсети

Настроим ssh на роутере и коммутаторе. Для этого выполним следующие команды:

```
Router(config)#ip domain-name admin.com
Router(config)#crypto key generate rsa modulus 1024
Router(config)#ip ssh version 2
Router(config)#username admin secret qwerty
Router(config)#line vty 0 4
```

```
Router(config-line)#login local
Router(config-line)#transport input ssh
```

Для доступа в интернет зададим на интерфейс, выходящий в интернет ipv6 адрес:

```
Router(config)#int GigabitEthernet 0/2
Router(config-if)#ipv6 address 2001:500:3::1/64
Router(config-if)#ip address 18.24.102.1 255.255.255.252
Route(config)# ip route 0.0.0.0 0.0.0.0 18.24.102.1
Router(config)#ipv6 route ::/0 2001:500:3::1
```

3.4 Настройка ПК и маршрутизации между ними

Для ПК требуется настроить статическую IPv4 маршрутизацию.

Настройка адресов IPv4 на ПК с Windows производиться по следующему алгоритму:

1. Зайти в свойства Ethernet.

2. Выбрать IP версии 4 (TCP/IP), нажимаем кнопку «Свойства». Делаем поле «Использовать следующий IP-адрес», заполнить поля «IP-адрес» и «Маска подсети» соответствующими адресами из таблицы 3.6.

В поле «Основной шлюз» вводим IPv4 адрес центрального маршрутизатора. Окна настройки представлены на рисунке 3.1.

3. Настройка IPv6 аналогична IPv4, только нужно выбрать IP версии 6 (TCP/IP), и в окне настройки ввести IPv6 адреса ПК и маршрутизатора. Окна настройки представлены на рисунке 3.7.

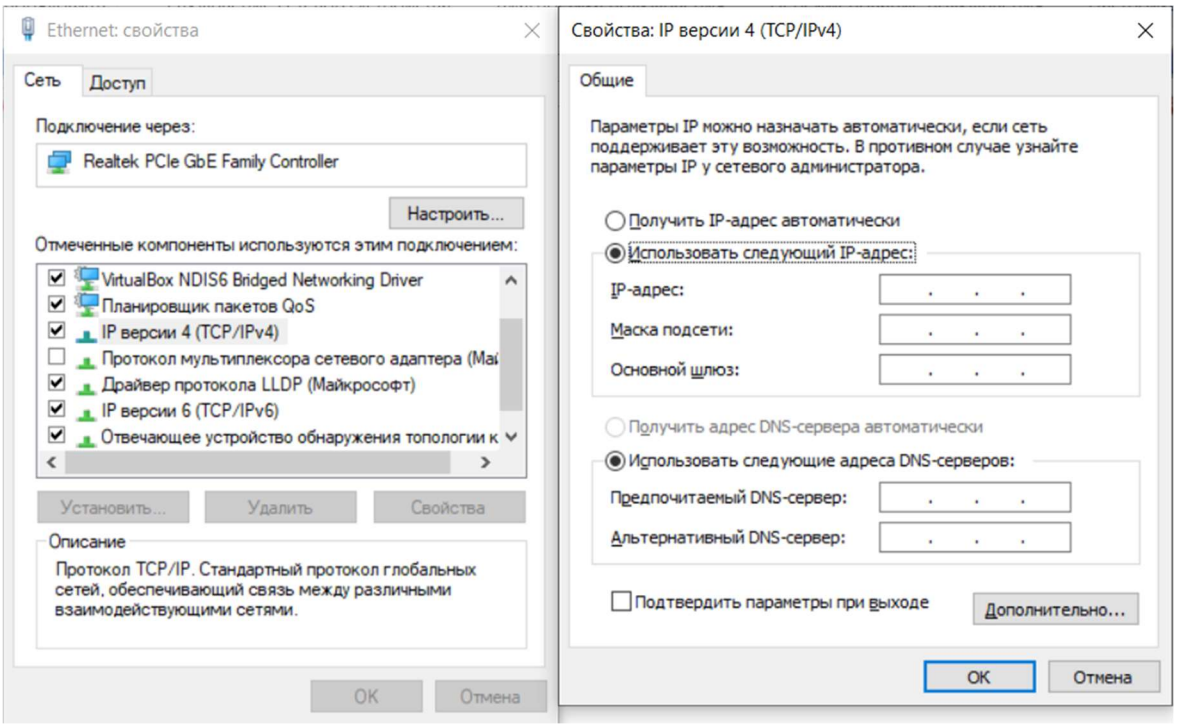

Рисунок 3.1 - Настройка IPv4 на ПК

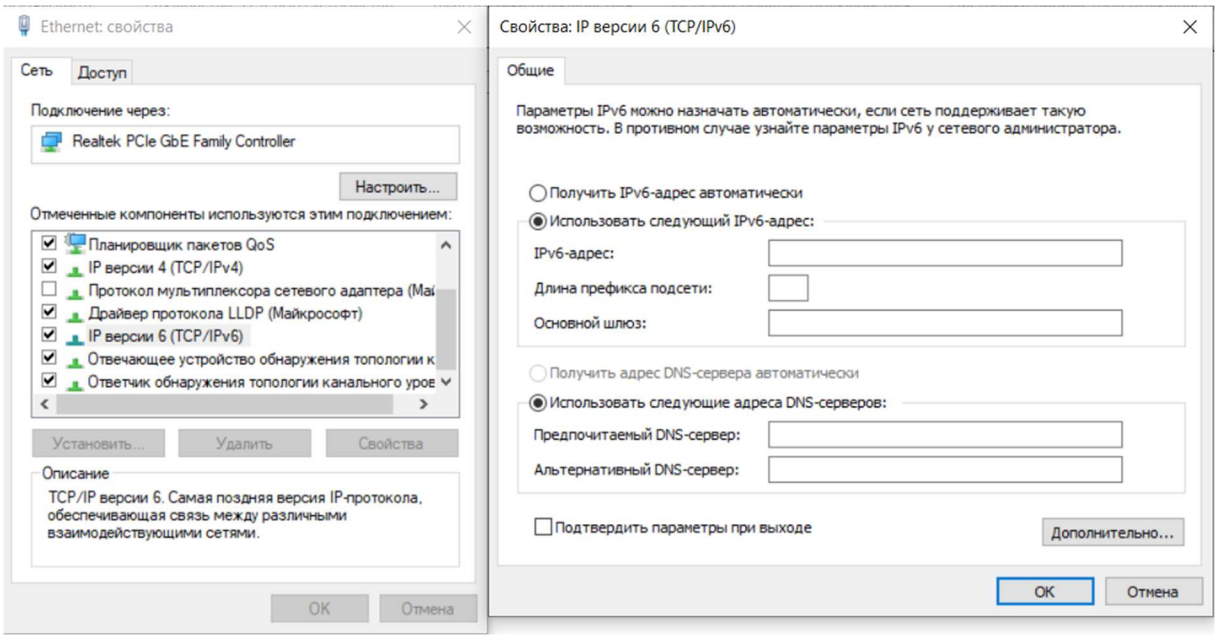

Рисунок 3.2 - Настройка IPv6 на ПК

3.5 Настройка принтера

Настройка принтера включает в себя инструкцию по подключению принтера к проводной сети. Подключение принтера происходит с помощью прямого Ethernet-кабеля.

Чтобы завершить установку принтера, необходимо загрузить драйверы с сайта 123.hp.com (см. рисунок 3.3, 3.4).

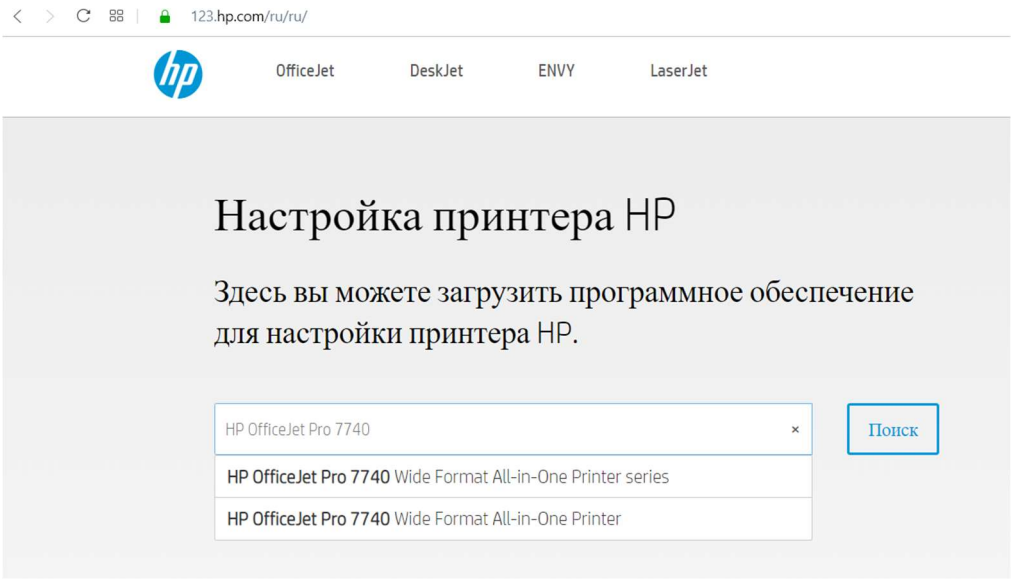

Рисунок 3.3 - Поиск ПО для принтера

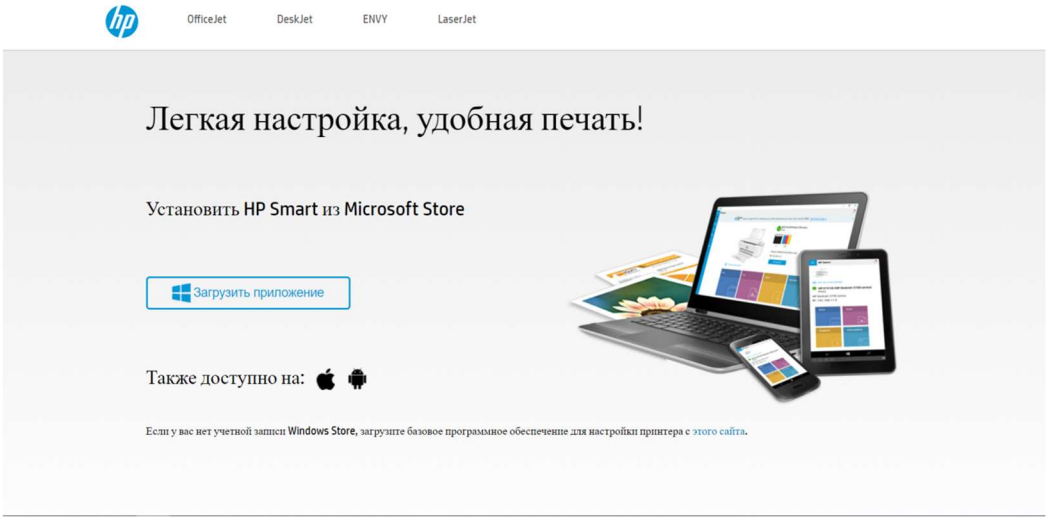

Рисунок 3.4 - Результат поиска ПО для принтера

Предлагаемое ПО (в данном случае - приложение HP Smart) выполнит поиск недавно установленных принтеров. Если используемый принтер не

отображается, нужно нажать на значок «+», а затем следовать инструкциям на экране, чтобы добавить новый принтер.

3.6 Настройка точки беспроводного доступа

Для мобильных устройств адреса из беспроводной сети должны выдаваться автоматически. Поэтому на центральном роутере настраиваем DHCP. Прописываем следующие команды:

```
Router(config)#ip dhcp pool Wi-Fi
Router(dhcp-config)#network 172.201.37.32 255.255.255.224
Router(dhcp-config)#default-router 172.201.37.33
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#domain-name mysite.local
```

И исключаем адрес самой точки доступа.

```
Router(config)#ip dhcp excluded-address 172.201.37.34
```

Так же произведем аналогичную настройку для DHCPv6:

```
Router(config)#ipv6 dhcp pool Wi-Fi-v6
Router(я)# address prefix 2001:500:3:20::/64 lifetime infinite
Router(dhcp-config)#dns-server 2001:4860:4860::8888
Router(dhcp-config)#domain-name mysitev6.local
Router(dhcp-config)# default-router 2001:500:3:20::33
```

Дальше приступаем к настройке Wi-Fi точки доступа. Для интерфейса BVI1 задем IP из подсети, предназначенной для смартфонов.

```
Wi-Fi(config)#ip address 172.201.37.34 255.255.255.224
Wi-Fi(config)#ipv6 address 2001:500:3:20::33/64
```

После задаем и настраиваем SSID. Присвоим сети имя Wi-Fi, задействуем авторизацию с помощью WPA, установим ключ сети ciscocisco

```
Wi-Fi(config)#dot11 ssid Wi-Fi
Wi-Fi(config-ssid)#authentication open
Wi-Fi(config-ssid)#authentication key-management wpa
Wi-Fi(config-ssid)#guest-mode
```

```
Wi-Fi(config-ssid)#wpa-psk ascii ciscocisco
Wi-Fi(config-ssid)#exit
```

Затем настроим радио-интерфейс.

```
Wi-Fi(config)#interface Dot11Radio1
Wi-Fi(config-if)#encryption mode ciphers tkip
Wi-Fi(config-if)#ssid Wi-Fi
Wi-Fi(config-if)#speed basic-54.0 54.0
Wi-Fi(config-if)#station-role root access-point
Wi-Fi(config-if)#no shutdown
Wi-Fi(config-if)#exit
```

3.7 Настройка IPsec-VPN

ISAKMP (Internet Security Association and and Key Management Protocol) и IPSec необходимы для построения и шифрования VPN-туннеля. ISAKMP, также называемый IKE (Internet Key Exchange) является протоколом согласования (negotiation protocol), который позволяет двум хостам договариваться о том, как создать сопоставление безопасности IPsec.

Первым шагом является настройка политики ISAKMP Phase 1

```
Router (config)#crypto isakmp policy 1
Router (config-isakmp)#encr 3des
Router (config-isakmp)#hash md5
Router (config-isakmp)#authentication pre-share
Router (config-isakmp)#group 2
Router (config-isakmp)#lifetime 86400
```

Далее мы собираемся определить Pre-Shared ключ для аутентификации с нашим партнером. При конкретной конфигурации нужно заменить адрес на адрес партнера:

```
R1(config)# crypto isakmp key secret address 1.1.1.2
```

Создаем расширенный ACL:

```
Router(config)#ip access-list extended VPN-TRAFFIC
Router (config-ext-nacl)#permit ip 172.201.37.0 0.0.0.29
172.201.37.96 0.0.0.31
```

Следующим шагом является создание набора преобразования (Transform Set), используемого для защиты наших данных. Назовем его TS.

```
Router(config)#crypto ipsec transform-set TS esp-3des esp-
md5-hmac
```

Создаем Crypto map. Crypto Map является последнем этапом нашей настройки и объединяет ранее заданные конфигурации ISAKMP и IPSec:

```
Router(config)#crypto map CMAP 10 ipsec-isakmp
Router(config-crypto-map)#set peer 1.1.1.2
Router(config-crypto-map)#set transform-set TS
Router(config-crypto-map)#match address VPN-TRAFFIC
```

Последний шаг - применить криптографическую карту к интерфейсу маршрутизатора, через который выходит траффик. Здесь исходящим интерфейсом является FastEthernet 0/1.

```
R1(config)# interface GigabitEthernet0/17
R1(config- if)# crypto map CMAP
```

При этом, на стороне удаленного подразделения системный администраторвведем в маршрутизаторе следующие команды:

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encr 3des
Router(config-isakmp)# hash md5
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 2
Router(config-isakmp)# lifetime 86400
Router(config)# crypto isakmp key share address 18.24.102.1
Router(config)# ip access-list extended VPN-TRAFFIC
Router(config-ext-nacl)# permit ip 172.201.37.0 0.0.0.29
172.201.37.96 0.0.0.31
Router(config)# crypto ipsec transform-set TS esp-3des esp-
md5-hmac
Router(config)# crypto map CMAP 10 ipsec-isakmp
Router(config-crypto-map)# set peer 1.1.1.1
Router(config-crypto-map)# set transform-set TS
Router(config-crypto-map)# match address VPN-TRAFFIC
Router(config)# interface FastEthernet0/1
Router(config- if)# crypto map CMAP
```

3.8 Надежность хранения данных

Так как важным фактором для заказчика является надежность хранения данных, было принято реализовать механизм резервного копирования данных. Существует большое количество различного ПО для этих целей.

«Правило 3-2-1» общепринятая стратегия для резервного копирования данных, которая помогает обеспечить их безопасность и доступность. Это правило гласит:

1. «3 копии данных». Важно иметь не одну, а три копии ваших данных. Это может быть оригинал данных плюс две резервные копии.

2. «2 различных устройства». Копии данных должны храниться на как минимум двух различных устройствах или медиа. Например, оригинальные данные на вашем компьютере, а резервные копии на внешнем жестком диске или в облачном хранилище.

3. «1 копия вне основного места хранения». Хотя бы одна из трех копий данных должна быть храниться вне основного места работы. Это может быть облачное хранилище, отдельный физический носитель (например, внешний жесткий диск) или копия данных на другом географически удаленном сервере.

3.8.1 Интеграция OneDrive

Исходя из того, что пользователи используют операционную систему Windows и формат деятельности подразумевает по большей части офисную работу, следует, что компании потребуется корпоративная подписка Microsoft Office 365 для пользования основных рабочих инструментов (Word, PowerPoint, Excel, Outlook и др.). В план решения для бизнеса в подписку на сервис также входит облачное хранилище на 1 ТБ для каждого пользователя на базе платформы OneDrive.

OneDrive имеет возможность как хранить любые данные пользователя удаленно, так и реализует механизм резервного копирования данных. Это идеально подходит под требования, так как реализует нужный нам функционал(создает резервные копии локально и так же сохраняет их в облаке) и не требует дополнительных финансовых затрат, так как входит в пакет подписки Microsoft Office 365.

Настройка резервного копирования с OneDrive:

1. Установите приложение OneDrive.

2. Откройте параметры OneDrive (щелкните значок «облака OneDrive» в области уведомлений и выберите значок OneDrive «Справка и параметры», а затем — «Параметры».)

3. Перейдите на вкладку «Синхронизация и резервное копирование».

4. Выберите «Управление резервным копированием».

Чтобы начать резервное копирование папки, выберите любую папку с надписью «Не резервное копирование», а затем нажмите кнопку «Сохранить» (изображено на рис. 3.5).

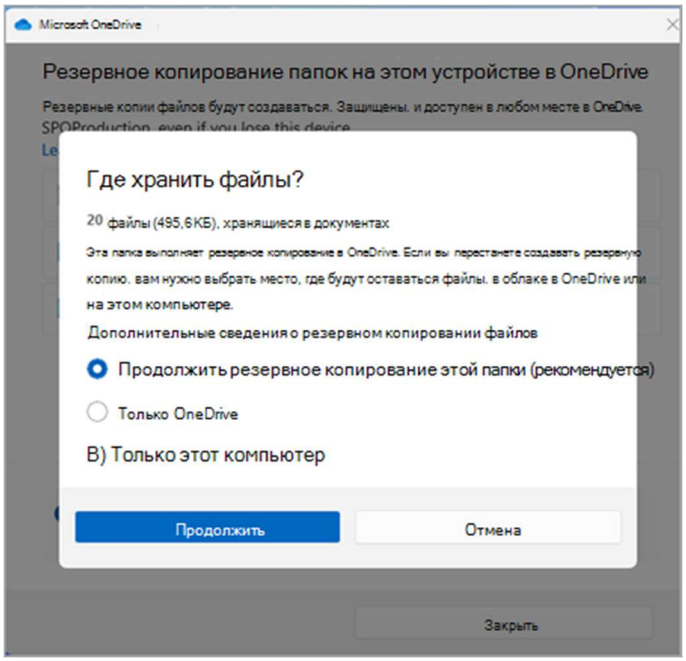

Рисунок 3.5

Также необъемлемым плюсом данного решения является удобный интерфейс пользователя, благодаря которому каждый пользователь без больших знаний в пользовании такого рода ресурсами может без проблем настроить ПО удобным для него образом.

Используя OneDrive создается дополнительная защиты данных от потери. Создание копий файлов локально и в облаке, обеспечит надежность хранения информации. Это гарантирует безопасность и доступность ваших данных в любой ситуации, дает уверенность в их сохранности.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СИСТЕМЫ

В данном разделе находится описание выбора кабелей, монтаж и размещение оборудования, расчет качества связи беспроводной сети для выстраиваемой ЛКС. Планом монтажа оборудования представлен в приложении В. Используемые условно-графические обозначения описаны в левой части схемы. Перечень оборудования, изделий и материалов представлен в приложении Г.

4.1 План помещений

Общая площадь помещений объекта 330 квадратных метров.

В здании 8 комнат: кабинет директора, кабинет дизайнеров, кабинет отдела маркетинга, кабинет колл-центра, склад, рабочее помещение, коридор и санузел.

4.2 Организация СКС

В проектируемой локальной компьютерной сети прокладка кабельной системы будет осуществляются вдоль стен на уровне ниже подоконников, за фальшь-стеной, прокладка кабелей между помещениями производится над фальшь-потолком.

Для всех подключений используется неэкранированная витая пара категории 5е. Для рабочих станций используются информационные розетки, установленные у рабочих мест на высоте 30 см от пола.

Для подведения электричества к сетевым устройствам будет использована технология POE, которая позволяет питать устройства посредствам Ethernet.

В отделе колл-центра будет установлен телекоммуникационный шкаф, в котором будет размещено следующее оборудование: коммутатор, маршрутизатор и модем.

Принтер расположен в кабинете директора и должен быть подключен к информационной розетке, а также дополнительный принтер подключенный посредством USB может располагаться у любой выбранной заказчиком рабочей станции.

В плане монтажа указывается, как и где следует прокладывать кабель, устанавливать информационные розетки.

Согласно схеме, заказчику рекомендуется, что рабочие столы с персональными компьютерами должны располагаться по периметру комнат вблизи розеток.

4.2 Монтаж информационной розетки

Розетку устанавливают в предварительно подготовленное заглубление в стене, где сначала винтом требуется зажать подрозетник, затем прикрепить съемный коннектор, и в конце фиксировать наружную панель. Внешняя розетка обычно имеет сзади коннектор с ножевыми контактами, пробивающими жилы витой пары через изоляцию.

4.3 Подключение принтера-сканнера

Для подключения принтера через Ethernet нужно выполнить следующие действия:

1. Загрузите драйвер.
2. Запустите программу установки драйвера принтера.
3. При появлении диалогового окна [Тип подключения] выберите [Проводное сетевое подключение (Ethernet)]. Нажмите [Далее] и следуйте инструкциям по завершению установки. Пример показан на рисунке 4.1.

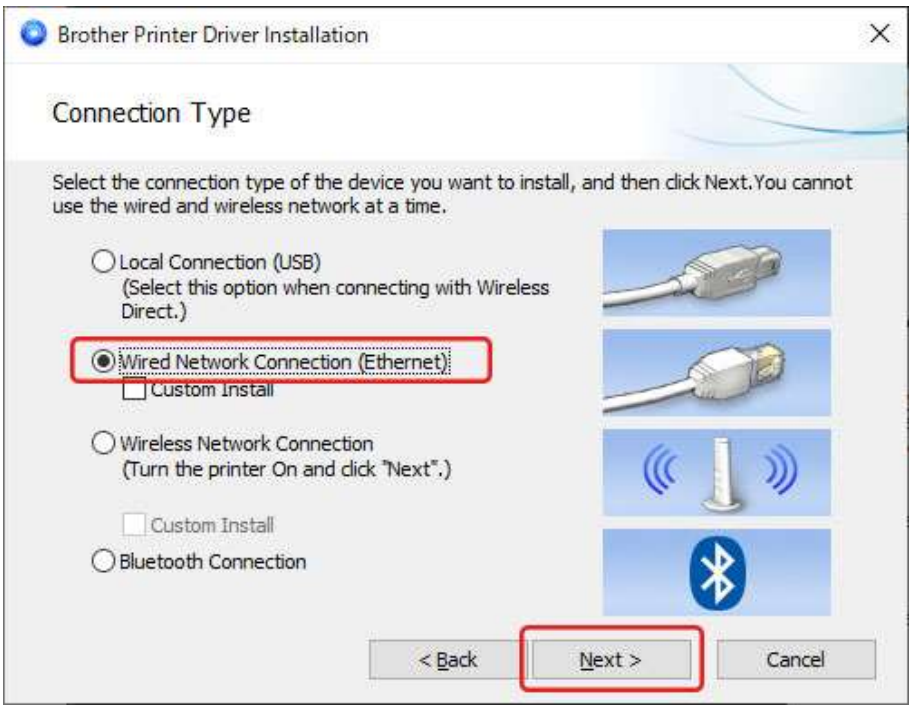

Рисунок 4.1

4. Перед подключением кабеля LAN убедитесь, что принтер выключен.
5. Подключите кабель LAN к порту LAN на задней панели принтера.
6. Подключите кабель LAN к активному порту LAN в сети.
7. Включите принтер.
8. Установите и запустите P-touch Editor для печати.

Для подключения принтера через USB нужно выполнить следующие действия нужно выполнить аналогичные действия, за исключением пункта 3. В нем следует выбрать [Локальное подключение (USB)].

4.4 Расчет качества покрытия беспроводной сетью

Беспроводная сеть должна покрывать всю площадь объекта и обеспечивать до 16 соединений. Внешние стены здания и внутренние этажа состоят из железобетонных блоков, внутренние стены квартир, в свою очередь, выполнены из шлакоблока. Высота этажа составляет 3 метра.

Для расчета затухания радиоволн в беспрепятственной воздушной среде используется упрощенная формула:

$$L = 32.44 + 20 * \lg(F) + 20 * \lg(D)\text{, дБ}$$

где F – частота сигнала (ГГц), D – расстояние (м).

Произведем расчеты покрытия. Точка доступа располагается в геометрическом центре здания (в коридоре) на потолке 3 м. В таком случае, наиболее удаленная точка квартиры располагается на расстоянии 13.6 м:

$$r = \sqrt{\frac{18^2}{2} + \frac{19.5^2}{2} + 3^2} = 13.6 \text{ м}$$

Рассчитаем затухание беспроводного маршрутизатора для используемой частоты: 2.4 GHz.

$$L_{\text{макс. уд.}} = 32.44 + 20 * \lg(2.4) + 20 * \lg(13.6) = 62.7 \text{ дБ}$$

Рассчитанное затухание сигнала удовлетворительно с учетом мощности излучения беспроводного маршрутизатора, равному 27 дБ. Добавим к расчету

затухания сигнала в воздушной среде. Наиболее серьезное препятствие для распространения сигнала представляется в виде стен из шлакоблока. Исходя из планировки помещения, суммарно между каждой комнатой имеется 1 стена из шлакоблока. Препятствие дает затухание $L_{\text{макс. конст.}} = L_{\text{шлакоб. ст.}} = \ 4$ дБ.

Также стоит учесть возможное затухание за счет взаимного размещения оборудования $L_{\text{обор.}} = 5$ дБ.

Тогда максимальное затухание сигнала в помещениях организации составляет:

$$L_{\text{макс.}} = L_{\text{макс. конст.}} + \ L_{\text{макс. уд.}} + \ L_{\text{обор.}} = 4 \text{ дБ} + \ 33.9 \text{ дБ} + 5 \text{ дБ} = 71.7 \text{ дБ}$$

Тогда минимальная мощность сигнала в помещении будет равна:

$$S_{\text{мин}} = \ S_{\text{маршрутизатора}} - L_{\text{макс}} = 27 \text{ дБ} - 71.7 \text{ дБ} = -44.7 \text{ дБ}$$

Такой показатель сигнала является удовлетворительным, что позволяет воспользоваться беспроводным маршрутизатором с мощностью излучения 27 дБ для покрытия всего объекта. Поэтому расположение маршрутизатора считается удачным.

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы была разработана локальная компьютерная сеть для небольшой обувной компании. Также были получены практические и теоретические знания, и навыки проектирования локальной компьютерной сети.

Был исследован рынок сетевого оборудования, стандарты и требования к создаваемой системе. Благодаря этому были получены навыки анализа рынка и выбора подходящего под выданные требования сетевого оборудования.

Результатами проектирования являются структурная, функциональная схемы, план здания предприятия, перечень оборудования и материалов, необходимых для построения и реализации этой локальной компьютерной сети. Сюда вошли маршрутизаторы, коммутатор, рабочие станции, принтер, кабели и другое. А также были графически обозначены правила развертывания данного оборудования на объекте. Оборудование, выбранное в данной работе, удовлетворяет всем требованиям заказчика.

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

Данная курсовая работа подтвердила важность вычислительных сетей во всех сферах человеческой деятельности, позволила восполнить пробелы в знаниях о вычислительных сетях в разработке, структурировании, прикладном использовании и конфигурировании, а также предоставила реалистичную ситуации разработки локальной компьютерной сети для небольшой обувной компании.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

[1] Коротко о главном: DOCSIS — [Электронный ресурс]. — Режим доступа: https://hab r.com/ru/articles/102429/.

[2] Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер - Спб: Питер, 2019. - 992 с.

[3] Н. Г. Рожнова, Н. А. Искра, И. И. Глецевич «Вычислительные машины, Системы и Сети. Дипломное проектирование» - Минск БГУИР 2014 — [Электронный ресурс]. - Режим доступа: https://www.bsuir.by/m/12_100229_1_87625.pdf

[4] Компьютер MultiOffice 5C104FD8H1G103S50H [Электронный ресурс]. – Электронные данные. – Режим доступа:: https://www.markit.by/product/kompyuter-multioffice-5c104f d8h1g103s50h_p126401/

[5] МФУ HP OfficeJet Pro 7720 [электронный ресурс]. - Режим доступа: https://catalog.onliner.by/printers/hp/y0s18a

[6] Чекмарев Ю. В. Локальные вычислительные сети / Ю. В. Чекмарев. - М.: ДМК-Пресс, 2014. - 250 с.

[7] Cisco DPC3008 Cable Modem DPC 3008 Comcast DOCSIS 3.0 [электронный ресурс]. - Режим доступа: https://www.ebay.com/p/1101528304?iid=125943169120

[8] Маршрутизатор Cisco ISR C1121-4P [электронный ресурс]. - Режим доступа: https://www.telestream.by/catalog/setevoe_oborudovanie/marshrutizatory_1/32311

[9] Коммутатор Cisco C1000-24T-4G управляемый 2-го уровня 28-портовый, сертификат СТБ [электронный ресурс]. - Режим доступа: https://server-x.by/kommutator-cisco-c1000-24t-4g-upravlyaemyy-28-ports-c1000-24t-4g-l.html

[10] Точка доступа Cisco Aironet 2800i AIR-AP2802I-E-K9 [электронный ресурс]. - Режим доступа: https://catalog.onliner.by/wirelessap/cisco/aironet2800i

ПРИЛОЖЕНИЕ А

(обязательное)

Схема структурная

ПРИЛОЖЕНИЕ Б

(обязательное)

Схема функциональная

ПРИЛОЖЕНИЕ В

(обязательное)

Схема принципиальная (План монтажа здания)

ПРИЛОЖЕНИЕ Г

(обязательное)

Перечень оборудования

ПРИЛОЖЕНИЕ Д

(обязательное)

Ведомость документов